NewP@ss

Nouvelles générations de passeports electroniques

Contenu

1. Résumé

Le projet Newp@ss a atteint ses principaux objectifs. Des plates-formes de pointes sécurisées (microélectronique et logiciel embarqué) adaptées aux passeports électroniques de 3ème et 4ème génération ont été prototypées. Ces nouvelles générations de plates-formes pour passeport électronique sont actuellement en cours de standardisation au sein de l'Organisation de l'Aviation Civile Internationale (OACI). Ces nouvelles plate formes seront utilisables au niveau européen et international et permettront un passage aux frontières rapide, automatisé et sécurisés. Elles pourront également être utilisées pour de nouvelles applications gouvernementales (comme la gestion des visas électroniques par exemple) ou pour des applications privées (accès à des services électroniques proposés par des compagnies aériennes, des hotels, des loueurs automobiles, ...).

Ces plates-formes de passeports sécurisés avancés intégrent l'état de l'art dans le domaine des communications sans contact de proximité (basé sur la norme ISO 14443). Elles possèdent des débits de communications 8 fois plus rapides que la génération de passeport actuellement déployée sur le terrain. Le passeport électronique le plus rapide du monde et les équipements de lecture correspondant ont été prototypés dans le cadre du projet. Les opérations de passage aux frontières automatisées seront accélérés et la sécurité accrue. L'arrivée dans les pays sera facilitée et accélérée grâce au protocole de communication sans contact VHBR.

Des micro-contrôleurs sécurisés ont été développés fournissant une puissance de calcul et de mémoire ainsi que des niveaux de sécurité à l'état de l'art pour des applications de type carte à puce. Des systèmes de lectures performants ont également été prototypés. Avec l'augmentation de la fraude aux documents de voyage et d'identité, un accent particulier a été mis sur les aspects sécurité et de confidentialité avec le développement de nouveaux protocoles cryptographiques (comme le protocole SAC ou EACv2.1). La plate-forme Newp@ss propose un haut niveau de sécurité pour les opérations de contrôle aux frontières.

Le partage d'information au sein du consortium newp@ss a été excellente; plus de 50 rapports ont été partagés et de nouvelles collaborations ont été établies. Les partenaires du projet Newp@ss ont également partagés les connaissances nouvellement générées et les résultats scientifiques dans des revues universitaires et des grandes conférences internationales. En outre, le consortium a contribuer à de nombreuses réunions concernant la sécurité des documents de voyage en contribuant notamment à la nouvelle norme eMRTD LDSv2 qui permettra le stockage de visas électroniques, tampons électroniques ou bien de tickets d'embarquement. Une coopération intensive entre tous les partenaires s'est mise en place au cours du projet. Plus de 14 démonstrateurs, dont 4 démonstrateurs complexes ont été définies dans mode de travail collaboratif afin d'illustrer les cas d'utilisation de contrôle aux frontières et des cas d'utilisation pour les voyageurs fréquents.

Le passeport électronique de 3ème génération prototypé sera distribué sur le marché à partir de cette année et le passeport de 4ème génération à partir de 2018. La technologie VHBR sera améliorée dans les prochaines années et sera vraisemblablement mis en œuvre dans les smartphones et les tablettes. Les protocoles cryptographiques seront réutilisés et améliorés dans d'autres types de documents électroniques tels que les cartes d'identité électronique, les permis de conduire et les cartes de permis de résidence. Ces nouvelles fonctionnalités faciliteront la vie des voyageurs en particulier à l'international, mais aussi à tout moment les citoyens pourront accéder à des services numériques publics ou privés en ligne grace à ces nouvelles générations de documents électroniques.

Ces nouvelles technologies représentent un changement important de modèle et embarquent des

technologies innovantes (interface haute vitesse, multi-applicatif embarqué, plate-forme logicielle sécurisé, applications mobiles et lecteurs, …)

15 partenaires de 5 pays européens ont travaillés sur le projet, et ont abordés l'interopérabilité au niveau de l'application, des outils de test et ont contribués de manière proactive à des actions de normalisation.

Ce projet a contribué au Grand Challenge concernant « la sécurité des consommateurs et des citoyens» et contribuer à la vision, la mission et la stratégie de l'AENEAS et de CATRENE. Tout cela a été rendue possible grâce au soutien du programme CATRENE et à la Direction Générale des Entreprises. Les applications ciblées par le projet newp@ss auront un grand impact économique, social et technique car ils seront intégrés à une grande partie des passeports électroniques de 2015 à 2020. Ce projet répond à nos besoins communs de sécurité et d'interopérabilité au niveau européen et international.

2. Description du projet

2.1. Rappel des objectifs

Le projet newp@ss visait le développement de plates-formes sécurisées pour la future génération de passeports électroniques (microélectronique avancée et logiciels embarqués).

Ces futurs passeports électroniques seront utilisables et reconnus comme document de voyage au niveau européen et international. Ils pourront également être utilisés pour des applications gouvernementales ou des applications à caractère privé.

La 3ème génération (intégrant les protocoles SAC et EAC v2.10) est en cours de déploiement en Europe depuis le début de 2015 et la 4ème génération (avec la mise en œuvre de la nouvelle norme LDS2) sera déployée courant 2018. La technologie développée dans le cadre du projet peut s'appliquer également à d'autres domaines tels que l'e-ID, le programme des voyageurs pre-enregistrer, le vote électronique ou bien encore le permis de conduire électronique.

Le projet visait les objectifs suivants:

- **Développer les technologies matérielles et logicielles** nécessaires pour la **prochaine génération de passeports électroniques**. Cette nouvelle génération intégrera la **nouvelle norme LDS2** (structures de données logiques) en cours de discussion à l'OACI, cela permet un changement fondamental concernant l'utilisation du passeport, lui permettant de devenir une véritable plate-forme multi-applications.

- **Développer les briques technologiques** nécessaires pour atteindre les niveaux de performance et de fonctionnalité demandée par l'OACI et l'UE ou des organismes de réglementation internationaux tels que les **nouveaux protocoles cryptographiques (SAC, EAC v2.1)**, les i**nterfaces sans contact à grande vitesse** (VHDR / VHBR), la biométrie additionnelle.

- **Élaborer des preuves de concepts complets** pour la mise en œuvre des nouveaux e-passeport, résultant d'une combinaison de **microcontrôleurs sécurisés de pointe**, les plates-formes logicielles embarquées basées sur un OS « small footprint », les lecteurs fixes ou mobiles compacts sécurisés.

- **Développer les concepts de sécurité et de confidentialité** nécessaires pour garantir une durée de vie de 5 à 10 ans des plates-formes e-passeport ainsi qu'un bon niveau d'isolation entre les applications.

- **Fournir une suite de tests fonctionnelles et des implémentations de référence**, appropriées pour permettre des tests d'interopérabilité.

- **Valider la preuve de concepts de plates-formes e-passeport** sur des cas d'utilisation dans le domaine de l'e-gouvernement et dans le domaine privée. La mise en place de certains de ces cas d'utilisation implique le développement et la validation des mécanismes de sécurité nécessaires à la bonne gestion des informations d'identification et de sécurité (certificats PKI).

Le projet met à profit les résultats du projet MEDEA + BIOP@ss, impliquant quelques uns des partenaires du consortium et dont certains éléments ont été réutilisés (en particulier les apports du projet aux comités de

normalisation appropriées ainsi que des briques technologiques, le protocole VHBR, spécification de protocole cryptographique, la méthodologie d'évaluation de la sécurité, ...)

2.2. Importance Stratégique pour l'Europe

Ce projet contribue au Grand Challenge "des consommateurs et de la sécurité des citoyens" de l'AENEAS / CATRENE VMS. Les applications ciblées par le projet newp@ss ont à la fois un grand impact économique, social et technique et couvre une grande partie du marché des passeports électroniques de 2015-2020. Il répond à nos besoins de sécurité et d'interopérabilité au niveau européen et international.

Le système européen de passeport électronique est considéré comme une référence dans le monde entier; grâce notamment à la mise en œuvre du nouveau protocole SAC qui est largement encouragé par ce projet et sera déployé en Europe et peut-être également hors Europe. Il permet de promouvoir les normes européennes et l'industrie européenne.

La stratégie numérique de l'union européenne pour répondre aux principaux défis et évolutions de la société de l'information et des médias jusqu'en 2020 vise à améliorer l'efficacité, moderniser l'administration, réduire la bureaucratie et permettre aux citoyens de communiquer avec les différentes autorités administratives plus facilement. Dès que les citoyens auront une carte d'identité nationale électronique ou un passeport électronique, ils seront en mesure d'accéder facilement et avec un haut niveau de sécurité à des services d'une e-administration.

2.3. Importance marché

Ce projet renforce la compétitivité des secteurs de l'industrie européenne suivants:

• **Cartes à puce sécurisé et appareils personnels sécurisés :**

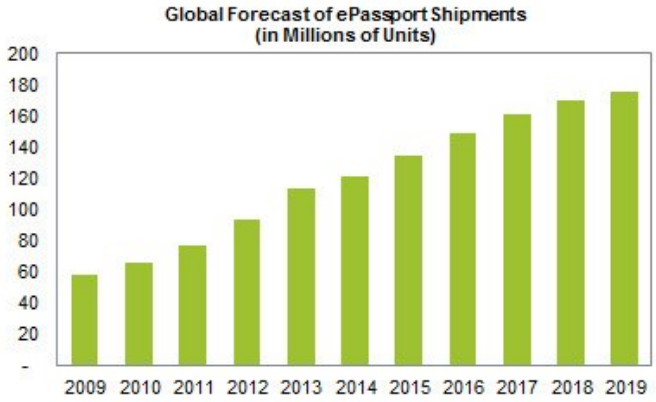
Le projet de newp@ss couvre le développement et le prototypage d'applications telles que les passeports électroniques soutenu par l'OACI et les applications e-Identité et permis de résidence.

• **E-Passeport:**

Depuis 2007, plus de 120 pays ont adoptés la première version passeport définit par l'OACI (la première norme de l'OACI est finalisée depuis 2004).

L'Union Européenne a adopté la biométrie et le protocole sécurisé SAC depuis 2015. Cela représente un marché pour newp@ss de plusieurs centaines de millions d'unités.

Les dernières informations disponibles montrent que le nombre de passeports électroniques délivrés progresse d'année en année:



Source: IHS Technology, August 2014

2.4. Rappel de l'état de l'art au lancement du projet

- **Situation en 2012**

Les documents de voyages et les cartes e-ID permettant l'accès à des services en ligne ont une croissance significative en Europe. Les documents de voyages sont nécessaires pour répondre aux exigences internationales d'interopérabilité de l'OACI, les cartes e-ID sont promues au niveau régional ou national.

- **Documents de voyage**

Les e-passeports (documents de voyage lisibles machine eMRTD) sont basés sur des spécifications définies par l'Organisation de l'Aviation Civile Internationale (OACI), et ils sont introduits dans le but de renforcer la sécurité internationale en offrant des solutions permettant de lutter contre l'immigration illégal, la criminalité transfrontalière et l'usupation d'identité. Les passeports électroniques contiennent un microprocesseur sans contact avec au moins 32 kilo-octets de mémoire, sur lequel on peut stocker les données biographiques du titulaire comme le nom, la date et le pays de naissance, ainsi que l'image du visage du titulaire et des données biométriques. Ces données peuvent être lues à partir du passeport en utilisant un lecteur sans contact.

Depuis Février 2005, la Communauté Européenne a adopté la première phase des spécifications techniques du e-Passport qui fixent au 28 Août 2006 la date limite pour les états membres pour inclure une image biométrique faciale dans leurs passeports électroniques. La deuxième phase est apparue mi-2009 en intégrant l'image d'empreintes digitales stockées dans le passeport électronique européenne. La troisième génération de passeport européen est en cours de normalisation et intègrera le nouveau protocole SAC. Il permet l'échange sans contact sécurisé et protége la vie privée des citoyens européens. Son déploiement a commencé en 2015.

- **e-ID**

Il existe actuellement plusieurs projets d'e-ID nationaux mis en œuvre ou en perspective (Finlande,

Allemagne, Portugal, Belgique, ...) à travers l'Europe. Ils sont principalement basés sur la technologie carte à puce. La norme eIDAS concernant la carte européenne du citoyen est également utilisée dans plusieurs cas. Sous responsabilités nationales, ces programmes devraient permettre le développement d'applications interopérables intersectorielles dans l'UE. Certains pilotes existent déjà (Projet STORK).

- **Situation dans le domaine des technologies**

La plupart des implémentations actuelles de passeport électronique 1ère et 2ème génération sont basés sur des microcontrôleurs 8/16 bits sécurisés classiques, avec environ 70 / 96KB de mémoire non volatile (NVM) et JavaCard 2.2 pile de logiciel embarqué classique. L'interface sans contact actuelle est basée sur la norme ISO 14443 classique. Aujourd'hui, la spécification de l'OACI pour le débit de la liaison sans contact du passeport électronique est de 424 kbps. Il est trop faible pour transférer plus de 100 Ko en 1 seconde et n'est pas adaté aux débits qui seront nécessaires dans le future. Le Projet BIOPASS avait proposé 6,8 Mbps dans la spécification ISO (couche physique du standard) pour l'amendement de la norme de carte de proximité ISO 14-443. Différentes propositions étaient en cours d'examen par les experts de l'ISO et un amendement de la norme VHBR a été réalisé au cours du projet newp@ss.

2.5. Innovations proposées

Innovation majeure proposée dans le cadre du projet

1) **Architecture 32 bits** pour remplacer l'architecture classique des microcontrôleurs sécurisés 8/16 bits afin de remplacer les plate-formes « à contact » classique et d'offrir de nombreuses nouvelles fonctionnalités, y compris:
   - Solutions de gestion de l'alimentation intégrée
   - Mise en place d'un démonstrateur OS multi-tâche avec mise en forme de puissance intégré
   - Sélection, mise en œuvre et intégration de l'architecture mémoire non volatile
   - Mise en oeuvre matérielle d'une interface VHBR de transmission contact et sans contact
   - Authentification basée sur le geste
   - Des solutions innovantes d'inlays et d'antennes

2) Développement de la **LDS2 (Logical Data Structure v2.0)**, développement avancé des plate formes logicielles embarquées permettant le stockage et la vérification de visa électroniques et de tampons électroniques, approche multi-application garantissant une parfaite isolation entre les applications et un niveau de sécurité élevé tel que demandé par la réglementation européenne.

3) Le développement de la technologie **contactless VHBR**. Les demandes techniques de l'ISO concernant l'amendement VHBR ont été intégrées dans un microcontrôleur sans contact et un lecteur. L'amélioration du module de gestion des faibles puissances et la conception pour des puces de dimension réduite a été étudié. Le traitement du signal a été amélioré afin de réduire les limitations inter symbole d'interférence et les limitations liés aux canaux de communication sans-contact de proximité. Des tests d'intégration du VHBR ont également été réalisés à la fois coté puce et côté lecteur / réseau. La compatibilité avec la technologie NFC a également été évaluée.

4) Des **cas d'utilisations avancées** démontrant la possibilité d'utiliser l'e-passeport et les documents d'identité électroniques dans un contexte multi-application, mélangeant des services publics et privés ont été proposés.

Quelques bénéfices quantitatifs:

- Des puces et OS intégrés avec des applications supportant le protocole sans contact de **848 kbps à 6,8 Mbps** ont été prototypés. Ce qui permet d'optimiser les temps de contrôle aux frontières de l'ordre de 30-50% grâce à tous les composants développés dans le projet et à l'automatisation complète de la vérification
- Plate forme matérielle et logicielle possédant des capacités de traitement de **100 Ko de données par seconde** (**~ 16 fois plus rapide que la technologie actuelle**)
- **Amélioration de la sécurité (protocole SAC et EAC v2.1)**

Newp@ss s'est en particulier interessé aux points suivants:

- Les cas d'usage pour le contrôle aux frontières,
- Les fonctions de base comme la vérification électronique des documents,
- Les principales normes : 9303 de l'OACI (Document de Voyage), BIG-EAC, ISO 24727 (biométrie)
- La réglementation principale en Europe : Union européenne (13502/2/07 3rd country nationals)

2.6. Plan d'exploitation / Dissemination des résultats

Les fabricants de cartes à puce impliqués dans le projet (Gemalto, Giesecke & Devrient) utiliseront les composants matériels et logiciels développés dans le cadre du projet en mode «pick and place » pour fournir des e-passeports à faible couts, fiables et interopérables. Ils dériveront des solutions pour le marché cible abordées dans le projet (par exemple, permis de résident et cartes e-ID).

Les fournisseurs de silicium et de composants électroniques (STMicroelectronics, ID3, NXP Semiconductors, Infineon Technologies), impliqué dans le projet fourniront des composants développés dans le projet pour les applications cibles. Basé sur l'expérience acquise et les livrables créés dans le cadre du projet, de nouvelles fonctionnalités seront intégrées dans les futurs produits. ID3 Semiconductors et NXP-F utiliseront les résultats du projet dans leur future génération de lecteurs (y compris les lecteurs mobiles).

Les entreprises de services informatiques impliqués dans le projet seront en mesure de conseiller les sociétés privés ou entités gouvernementales sur la façon de mettre en place des solutions interopérables dans le domaine des demandes de citoyenneté (Evoleo). Ces entreprises cherchent à renforcer les partenariats académique avec les instituts de R & D et les entreprises, qu'elles soient complémentaires ou concurrentes. Elle souhaite être positionnée plus près de l'utilisateur final. Elles prévoient également de définir, d'intégrer et de développer des solutions commerciales sur mesure pour les cas d'utilisation identifiés. Evoleo, par exemple, est axée sur le développement d'un lecteur portable autonome léger qui pourrait être intégré dans les smartphones / tablettes ou des ordinateurs portables et prévoit d'élargir sa gamme de produits et d'exploiter de nouvelles opportunités commerciales.

Le rôle de l'ISEN dans le projet a été de mener les activités tests et de banc d'essais pour certains cas d'utilisation afin de démontrer le potentiel des futurs passeports. Les partenaires ont contribués à la définition de l'architecture logicielle, à sa mise en œuvre et, en conséquence, on pu se former sur les nouvelles normes matérielles et logicielles applicables dans le domaine du passeport électronique. Un autre objectif de l'ISEN, comme de l'Instituts de Technologie, a été la transmission de ses connaissances nouvellement acquise auprès des entreprises locales. Ce transfert a pour objectif de créer des synergies entre les entreprises locales, les autres participants et organes éventuellement externes afin de promouvoir l'utilisation des développements et la recherche de projets à l'avenir.

Les instituts de R & D impliqués dans le projet (CEA-Leti, ISEN, TUG-IAIK, Instituto Telecomunicações) capitaliseront sur les connaissances acquises dans le projet pour fournir des blocs matériels et tireront parti de leurs compétences en matière d'évaluation de la sécurité, selon les schémas de principes nationaux ou privés (RF faible puissance, mise à niveau plate-forme, caractérisation).Les instituts de R & D, dans le cadre de leur mission d'amélioration de la compétitivité des industries nationales ont formés un groupe de personnes qualifiées qui a maintenant une profonde connaissance de la conception, des techniques d'analyse et de mise en œuvre des passeport électronique, Ils prévoient de transférer ces connaissances par des actions de conseil et de formation.

- ***Dissemination des résultats***

Le transfert de connaissances a été organisé à travers des conférences (séances d'information), des séances de travaux associés au projet, des ateliers avec des participants invités provenant d'organismes gouvernementaux et opérateurs d'infrastructures (aéroports, compagnies aériennes ...).

Plusieurs canaux ont été identifiés et exploités à des fins de diffusion en corrélation avec la feuille de route du projet. Une liste de ces canaux de communication a été mise en place. Par exemple, parmi les conférences et possibilités d'exposition qui ont été examinés, on peut mentionner le Forum européen de la nanoélectronique et l'événement annuel World eID.
En dehors de ces canaux, le projet a examiné aussi bien le milieu universitaire et les supports de publication connexes, ce qui a permis notamment aux instituts de recherche de l'université d'élargir la diffusion à un plus large publique des résultats scientifiques obtenus.
Un portail web dédié à newp@ss (http://newpass.av.it.pt/) a servi à des fins de transfert de connaissances, et offert un espace d'échange pour les partenaires afin de partager des documents techniques, échanger des informations sensibles et confidentielles tout au long de la durée de vie du projet.

2.7. Impacts attendus

Chaque citoyen de l'UE a des droits et des devoirs. Beaucoup d'entre eux souhaitent être en mesure d'exercer leurs droits et leurs devoirs partout où ils se trouvent dans l'UE. Le mécanisme pour accéder à ses droits et devoirs doit être simple, facilement compréhensible et accessible à tout moment, n'importe où dans n'importe quel états membres. L'accès aux services publics au niveau pan-européen est un aspect clé de ce projet. Newp@ss soutient cet objectif en fournissant la technologie de base nécessaire à ce déploiement.

La gestion de l'identité est un mécanisme pour identifier qui vous êtes. À l'heure actuelle cela se fait principalement par document papier. La gestion d'identité électronique vient compléter l'identification sur papier par des moyens électroniques, qui apportent l'énorme avantage de rendre disponible un service en ligne à tout moment et n'importe où. Cependant, la mise en œuvre d'un système de gestion d'identité électronique soulève de nombreuses questions technologiques et organisationnelles. La sécurité, la vie privée, la protection des données, l'interopérabilité, l'authentification, l'accès aux services, etc...

Dans le domaine du passeport électronique, tous les acteurs impliqués dans le recrutement, la fabrication de passeport, la personnalisation, les processus de contrôle aux frontières doivent maitriser de nombreuses compétences. Ils seront impliqués dans les déploiements de futures générations de passeport électroniques.

Ces compétences incluent:

- Des techniques d'authentification et de chiffrement avancés
- La mise en œuvre de nouveaux systèmes d'exploitation compatibles SAC et EAC v2.1
- La gestion d'une autorité de certification PKI, responsable de l'enregistrement des clés publiques, de la révocation de certificats, etc.
- La saisie des données biométriques, le stockage et l'adéquation des configurations en conformité avec les normes de sécurité élevées et des politiques de confidentialité strictes
- La maitrise d'équipement de capture, de mise en forme et de préparation des données d'inscription
- L'authentification de l'identité des individus par des entités gouvernementales appropriées. Vérification de la validité des informations fournit par le demandeur
- La mise en place d'une chaîne ou d'un réseau de confiance, notamment à l'international

Les résultats du projet auront de nombreux impacts, notamment en termes de:

- ***Personnalisation:*** plusieurs nouveaux défis pour les personalisateurs de documents d'identités électroniques, principalement autour de la protection de la vie privée et de la sécurité devront être résolus.
- ***Le contrôle des frontières****:* la totalité des lecteurs de contrôle aux frontières devront être compatible et équipés du logiciel d'authentification de documents en lien avec l'autorité de contrôle de passeport (DV, Document Verifier). Dans la pratique, cela signifie que les logiciels des lecteurs devront être mis à jour pour être compatible avec les protocoles nouveau intégrant SAC, LDS2, etc.
- ***Gouvernement et citoyens****:* les nouvelles technologies telles que les cartes à puce, la biométrie et la technologie sans contact ont démontrés leur utilité et sont de mieux en mieux compris, les questions de confidentialité et de sécurité continueront tout de même à être soulevés.
- ***Impacts industriels****:* Les fournisseurs d'accès Internet pourront exploiter le nouveau schéma d'authentification en ligne afin d'offrir des services d'identification sécurisés aux entreprises.

3. Description du consortium

Nom	Pays	Adresse	Grands Comptes	PME
Gemalto	France	6 rue de la Verrerie 92197 Meudon Cedex, France	X	
NXP Semiconductors F	France	NXP Semiconductors 2 Esplanade Anton Philips – Campus EffiScience BP 2000 - 14 906 Caen - France	X	
id3 semiconductors	France	5 rue de la Verrerie F-38120 Le Fontanil Cornillon		X
STMicroelectronics (Rousset) SAS	France	190 Avenue Célestin Coq, F-13106 Rousset Cedex - France	X	
Compuworx	Hungary	2040 Budaors, Szabadsag 141-143		X
Infineon Technologies	Germany	Infineon Technologies AG Am Campeon 1-12, 81726 Munich, Germany	X	
Giesecke & Devrient	Germany	Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81607 Munich, Germany	X	
NXP Semiconductors G	Germany	NXP Semiconductors Germany GmbH Stresemannallee 101 22529 Hamburg, Germany	X	
Infineon Technologies	Austria	Siemensstraße 2 A-9500 Villach	X	
NXP Semiconductors A	Austria	Mikron-Weg 1, 8101 Gratkorn, Austria	X	
EVOLEO Technologies	Portugal	Travessa Sá e Melo, n.º 161, Fracção H, Gueifães 4470-116 Maia, Portugal		X

Instituts	Country	Address
Institute CEA-LETI	France	CEA-LETI MINATEC 17, rue des Martyrs, F- 38054 Grenoble cedex 9
ISEN-Toulon	France	Maison des technologies Place Georges Pompidou F-83000 Toulon
Instituto de Telecomunicações Aveiro	*Portugal*	Campus Universitário de Santiago 3810-193 Aveiro
TU Graz Institute for Applied Information Processing and Communications	*Austria*	University of Technology Inffeldgasse 16a A-8010 Graz

3.1. Gemalto

« Dans un monde numérique de plus en plus connecté, nous contribuons à établir une confiance mutuelle »

- 2.5milliards d'€ de chiffre d'affaires en 2014,
- 46 pays avec un site en activité,
- 14 000 collaborateurs représentant 116 nationalités,

Leader mondial de la sécurité numérique, Gemalto est au cœur de l'évolution du monde numérique. Nous permettons aux entreprises et aux gouvernements du monde entier d'offrir des services numériques pratiques et de confiance à des milliards de personnes. Loin des projecteurs, nous œuvrons pour que vos clients, collaborateurs et citoyens puissent réaliser des transactions bancaires, se connecter ou s'identifier, en toute simplicité et sécurité. Que ce soit pour communiquer, utiliser des services bancaires, travailler en ligne, bénéficier de services de e-gouvernement, accéder aux services du Cloud ou bâtir l'Internet des objets, partout dans le monde et à tout instant, nombreux sont ceux qui font confiance à Gemalto.
Nous maîtrisons la globalité du processus de création de solutions de sécurité numérique pour nos clients et leurs utilisateurs finaux. Nous développons des logiciels et des systèmes d'exploitation sécurisés que nous embarquons dans de nombreux objets, comme les cartes UICC ou SIM, les cartes bancaires, les tokens, les passeports électroniques et les cartes d'identité électroniques. Nous personnalisons ces objets et déployons des plate formes et services pour gérer les données confidentielles qu'ils contiennent sur l'ensemble de leur cycle de vie. Toutes nos activités reposent sur la confiance de nos clients que nous avons su conquérir en gérant leurs données sensibles et en permettant à leurs utilisateurs de profiter de nos solutions en toute sécurité. C'est ainsi que nous remplissons notre mission, en apportant confiance et facilité d'usage au monde numérique.

3.2. STMicroelectronics

STMicroelectronics, une des plus grande société mondiale de semi-conducteur, est un leader global pour le développement et la fabrication de solutions semi-conducteurs couvrant une large gamme d'applications microélectroniques. Une combinaison sans égale d'expertise circuit et système, de fortes capacités de fabrication, de portefeuille de propriété intellectuelle (IP) et de partenaires stratégiques positionne la société sur les solutions de System-on-Chip (SoC), et ses produits jouent un rôle important pour permettre la convergence actuelle des marchés. Les actions de la société sont cotées sur les places boursières de New York, de Paris et de Milan. En 2010 les ventes nettes de la société se sont élevées à 10,35 Md$. Plus d'informations sont disponibles sur le site web de ST (www.st.com).
ST est un leader du marché des composants pour carte à puce depuis 1983 quand ST a introduit le premier circuit pour les cartes téléphoniques prépayées et le premier microcontrôleur sécurisé pour les applications de paiement. Dans le domaine de l'identité électronique, ST a été partenaire des projets Onom@Topic+ et BioP@ss (MEDEA +). ST est très actif dans le domaine du traitement de confiance, et impliqué dans le projet TSC (MEDEA+) ainsi que dans le NFC et les modules de sécurité associés.

3.3. ID3 Technologies

Fondée en 1990 par une équipe de microélectroniciens de STMicroelectronics, id3 Technologies est une société d'étude spécialisée dans la conception et le développement de composants, de systèmes électroniques et d'applications dans les domaines du Sans contact (RFID), de la Biométrie et de la Radiofréquence. ID3 Technologies résout les défis technologiques de ses clients en leur proposant des solutions innovantes et de hautes performances, conçues par son équipe d'experts autour d'un portefeuille unique de technologies. Son réseau de partenaires composé de grands acteurs internationaux et de PME lui donne une très grande réactivité pour prototyper et fabriquer vos produits. Nous traitons chaque jour des affaires impliquant la vie privée et le secret de l'information, nous croyons qu'une éthique claire et forte est

nécessaire pour profiter des innovations majeures apportées par id3 Technologies.
Nous nous sommes engagés dans un processus d'amélioration permanente et d'investissement important dans la R&D pour apporter à nos clients les solutions les plus sûres. Nous pouvons faire face à toutes les inquiétudes puisque nous assurons la fiabilité complète de nos solutions et le secret de l'information.

3.4. CEA-LETI

Institute CEA-LETI is one of the laboratories of the Technological Research Division of CEA.(French Atomic Agency) With more than 1000 experts in the field of microelectronics and microtechnologies, its mission is to successfully complete technological research programs aiming at developing new processes, new components and new smart systems with a view to transfer it to industry. The LETI activities relies on a set of technological platforms (microelectronics, microsystems, optronic components and multimedia) structured around extensive resources (10 000 m² of clean rooms,). The System Design and Integration Department (DSIS) develops know-how in integrated circuit design and skills in development of systems and prototyping applied to the areas of telecommunications, communicating objects and secure components.
The LETI hosts secure components specialists both in the technological and security evaluation areas: micro packaging, architecture and design of secured digital components (asynchronous logic, non-volatile memories, SOC, NOC, ultra-low power radiofrequency transmission, etc.).
The first areas of application are smart cards and electronic tags. Contactless smart cards, RFID tags and the emergence of concepts for communicating portable objects into Internet of Things concept highlighted the need for protection of data owned by the citizen or by companies. Securing of the new information and communication technologies with respect to protection of the private life of individuals has directly affected development of electronic systems. Results of works from LETI teams in contactless physical layer and protocols for very High Data Rate (VHDR) were proposed at ISO standardization committees and are under discussion for the Very High Bit Rate (VHBR) amendment of ISO contactless proximity card standard. Nowadays, the systems R&D activities of CEA-LETI in the RF communications field employ more than one hundred people. Moreover, the LETI operates an ITSEF (Information Technology Security Evaluation Facility) laboratory, specialized in security evaluation of electronic components within the framework of public schemes such as Common Criteria, ITSEC, FIPS, AIS and private schemes such as EMVCo or VISA.

3.5. ISEN

ISEN-Toulon is an engineering high school established in Toulon since 1991, delivering a master degree in electronics and informatics. The cursus is split in three parts : a first two year course in fundamentals (mathematics and physics), then a one year course giving a general overview of electronic and informatics technologies, followed by a last two year course allowing students to follow a more specialized set of modules (digital technologies, networks and systems, business development, innovation management, RFID, NFC,…).
Research activities at ISEN-Toulon have started in 1994 and are organized in five domains:

- Semiconductor devices characterization and reliability for advanced CMOS technologies
- Analogue/digital integrated circuit and secured RF systems for wireless applications design
- Molecular electronics on silicon
- Digital and programmable circuits applications
- Image and signal processing
- Informatics (design, development & validation, integration)
- Since 2000, a large part of these activities are integrated within the IM2NP Laboratory (Institut Matériaux Microélectronique Nanosciences de Provence - UMR CNRS 6242)

- Thanks to its association with IM2NP, ISEN-Toulon has strongly developed human and technical skills in the field of 13.56 MHz contactless systems. Two Ph-D theses have been attended, concerning the modeling of the transmission channel, the optimization of load modulation for multi cards systems and the use of digital multi phases modulations. All these studies have been made in collaboration with ST Microelectronics (Rousset, France).
- These skills are merged in a RF laboratory. The laboratory houses one of the Micro-Packs platforms for certification of functional conformity of products with standard ISOIEC 14443 implementing standard ISO10373-6. This platform, issued from public and private foundings, is dedicated to the R&D cooperations between industrials and universities in PACA area. ISEN-Toulon will be kept valorized in Catrene project.
- One PhD these has joined Isen Toulon in 2010 focused on the innovation and use cases.
- Since 2010, ISEN-Toulon became an associated member of the LSIS , Laboratoire des Sciences de l'Information et des Systèmes

3.6. Infineon Technologies

Infineon Technologies se concentre sur trois défis majeurs auxquels la société moderne est confrontée: l'efficacité énergétique, la mobilité et la sécurité et offre des semi-conducteurs et des solutions systèmes pour l'électronique automobile, le secteur industrielle, le secteur de la carte à puce et ses applications de sécurité. La société est sur le marché des circuits intégrés de haute sécurité depuis 25 ans. Le portefeuille de produits répond à des marchés de volumes élevés tous pertinents, tels que les cartes téléphones GSM, les cartes bancaires, l'identification, les transports et la télévision payante. En 2009, la part de marché selon Frost & Sullivan était de 27%. Infineon Technologies a été le numéro un en terme de volume élevé pendant 13 ans. Dans le domaine des cartes d'identité électroniques nationales et des cartes de sécurité sociale en Europe, ses produits ont été émis en Finlande, en Estonie, en Italie, en Belgique, en Autriche et en Suède, ainsi que récemment pour la nouvelle Carte Nationale d'identité électronique Allemande (NPA). Environ 80% des cartes d'identité électroniques en Europe contiennent un microcontrôleur sécurisé Infineon. Plus de 15 pays ont choisis Infineon pour leur programme de passeport électronique international. (www.infineon.com).

3.7. Giesecke&Devrient

Giesecke & Devrient est un groupe technologique international de premier rang dont le siège se trouve à Munich. Fondée en 1852, l'entreprise a réalisé en 2014 un chiffre d'affaires de 1,83 milliard d'euros en employant 11 450 personnes. La proximité client est assurée au plan international par 58 filiales et coentreprises dans 32 pays.

G&D développe, produit et distribue des produits et solutions pour le paiement, la communication sécurisée et la gestion des données personnelles. Sur ces marchés, le groupe a une position de leader technologique et possède une avance sur ses concurrents. L'entreprise compte parmi ses clients des banques centrales et commerciales, des opérateurs de téléphonie mobile, des entreprises, ainsi que des gouvernements et services publics.

L'activité principale de G&D se divise dans les secteurs principaux suivants :

- Billet de banque

Equipements, solutions et offres de services pour les billets de banque : solutions d'éléments de sécurités pour billets de banque, des substrats des billets, des systèmes d'impression et de traitements des billets de banque ainsi que les caisses centrales et l'ensemble du centre-fort et de la logistique, avec la gestion complète des offres de services de maintenance durant l'utilisation des solutions G&D.

- Sécurité mobile

Produits et solutions de sécurité pour les applications mobiles : gestion des abonnements, paiements sur le Cloud ou cybersécurité, gestion des données, personnalisation, gestion de projet, ainsi que des services de conseil ; cartes SIM, cartes bancaires, cartes d'identité ou de santé, modules M2M et jeton

- Solutions pour les gouvernements

Des solutions complètes pour la production et la personnalisation de passeports, de cartes d'identité, de cartes de santé et de permis de conduire ; systèmes de personnalisation, d'édition et de gestion des documents. Des solutions d'identification des personnes, d'inscription des électeurs et de contrôle aux frontières ; sécurité informatique.

3.8. NXP Semiconductors

NXP Semiconductors provides High Performance Mixed Signal and Standard Product solutions that leverage its leading RF, Analog, Power, Digital Processing and manufacturing expertise. These innovations are used in a wide range of automotive, industrial, consumer, lighting, medical, computing and identification applications. Headquartered in Europe, the company has about 28,000 employees working in more than 25 countries and posted sales of USD 4.4 billion in 2010. News from NXP is located at www.nxp.com.

3.8.1. NXP France

NXP site in Caen, France is dedicated to R&D with more than 500 engineers working on advanced semiconductors-based solutions. More than 80 of these engineers are part of the Identification team that focus on Near Field Communication and on development of contactless readers. NXP-F has a system expertise that covers hardware and software interface topics. The ID team from NXP France was already part of the Biop@ss project where it contributed to (1) the definition of platforms' architecture and specifications, (2) the coupling of NFC IC with other secure technologies (biometrics), and (3) use case definition. Biop@ass was one of the many European (ITEA2 'Smart Urban Spaces' and 'Expeshare'...), as well as national experimentations and projects ('Caen Ville NFC', trial in Nice) related to contactless technologies.
NXP Semiconductors will develop and integrate component solutions with high-speed contactless interfaces such as VHDR. Those solutions / platforms will also embed contact interfaces so that compatibility of card readers with e-ID interoperability platform requirements can be ensured. Such a contact product will also embed secured features such as secured pin-pad.
Thus, new generation of contactless components adapted to ID requirements (compatible to ICAO) is planned and combination with security modules will be targeted.
NXP will provide solutions to manage multiple applications on single secure element architecture.
NXP Semiconductors Germany GmbH.
NXP-D has an outstanding position in automotive semiconductors and is market leader in contact-less identification solutions with the business unit identification in Hamburg. NXP is a top global supplier of chips in eGovernment applications, such as electronic passports, ID cards, or health cards. The activities of NXP Germany comprise design, development and marketing of leading edge RFID, e-government and automotive sensor devices. With over four billion chips sold to date NXP the world's leader in the design of contact-less chips used in secure smart cards and electronic identification schemes

3.8.2. NXP Semiconductors Austria GmbH

The project partner NXP Semiconductors Austria GmbH has a leading position in contactless identification systems for Automotive and Identification markets, with the participating site Gratkorn being the competence center for contactless identification within NXP.

Around 350 employees are working on advanced high performance mixed signal semiconductor solutions, with a focus on R&D and marketing activities.

3.9. TUG-IAIK

L'Institut de Recherche Appliquée en traitement de l'information et des communications de Graz, l'université de Technologie est hautement spécialisée en sécurité informatique. Les principales activités de l'institut sont la recherche, l'enseignement universitaire et des services de conseils pour les organismes publics et les entreprises. Actuellement, environ 50 chercheurs (ETP) sont employés à IAIK, environ un tiers d'entre eux sur la base du budget ordinaire de l'université, le reste est financé par des tiers . Plusieurs aspects de ce domaine exigeant sont couverts, allant de la cryptographie (Prof. Vincent Rijmen) , la vérification formelle et l'informatique de confiance (Prof. Roderick Bloem) pour sécuriser des solutions d'administration en ligne .

3.10. Instituto de Telecomunicações (IT)

IT est une organisation portugaise privée, à but non lucratif appartenant à l'Université Technique de Lisbonne, Université d'Aveiro, Université de Coimbra et Portugal Telecom Inovação, sa mission est de créer et de diffuser des connaissances scientifiques dans le domaine des télécommunications afin d'améliorer l' éducation et la formation, tant au niveaux universitaire et post-universitaire, et d'améliorer la compétitivité de l'industrie portugaise et des opérateurs de télécommunications. L'unité de recherche a été évalué par un groupe d'experts choisis par "Fundação para a Ciência ea Tecnologia" (l'agence nationale pour la recherche), en 1996 et 1999: à la suite de cette évaluation, IT a été sélectionné en 2001 par le gouvernement portugais et obtenu la distinction dr laboratoire associé au gouvernement dans le domaine des télécommunications. Le pôle de Aveiro Elle compte actuellement environ 28 chercheurs doctorants (dont beaucoup détiennent également des postes d'enseignement à l'Université d'Aveiro), ainsi que 78 autres chercheurs, avec une expertise sur la radio, les micro-ondes, l'optique, les réseaux et la conception de circuit intégrés.

3.11. EVOLEO Technologies (EVO)

EVOLEO est une PME fondée en 2007 opérant dans le domaine aérospatial et industriel, investir dans les compétences liées à la conception de systèmes électroniques critiques et très complexes, au-delà de l'automatisation et de contrôle traditionnel. Les principaux clients et partenaires d'Evoleo comprennent des sociétés majeures dans le domaine des chemins de fers, de l'énergie et de l'espace, et sur les projets de l'Agence Spatiale Européenne (ESA). Depuis sa fondation, l'entreprise a développé une expertise dans les différents domaines de l'ingénierie électronique tels que la conception et la mise en œuvre de matériel analogique et numérique, la mise en œuvre de logiciels pour les systèmes embarqués, l'utilisation de systèmes d'exploitation en temps réel, de l'instrumentation et de contrôle et l'ingénierie des systèmes. Un facteur commun à tous ces domaines sont les problèmes de fiabilité et de sécurité, identifier les risques, les échecs et les solutions de contournement. En interne Evoleo possède des compétences dans la mise en œuvre de systèmes multi-core sur FPGA et fin 2010 a coopéré à un projet de l'ESA dans la conception d'une unité d'interface de données pour le contrôle de charge utile du satellite avec le processeur LEON3 et l'OS temps réel RTEMS, impliquant des acteurs clés des solutions informatiques tels Aeroflex Gaisler en Suède. Stratégiquement, Evoleo a décidé d'aller encore plus loin sur le secteurs des transports et de la santé, en mettant l'accent sur la facilité d'utilisation des solutions pour l'utilisateur final en tenant compte des questions de sécurité toujours nécessaires.

4. Durée du projet

Début:	01/12/2012
Fin:	30/11/2015

5. Organisation du projet

SP1 (Gemalto)
Gestion de projet

SP2 (Gemalto)
Specification Plates-formes

- Specification exigences, Architecture, Marketing
- Specifications Plates-formes

SP3 (STMicroelectronics)
Développement Plateformes Matériels
Puces & Lecteurs

- Briques élémentaires pour e-passport
- Development/integration µ-controleurs
- Lecteur sécurisés sans-contacts

SP4 (Giesecke & Devrient)
Développement Plateformes Logicielles
On-Card & Off-card

- Briques logiciels
- Developpement SW « On-card »
- Developpement SW “Off-card” et mécanismes de personalisation

---

SP5 (Infineon Technologies)
Tests et Implementation de Référence
OS & Application

- Méthodes et Outils de génération de tests
- Prototypage d’applications
- Normalisation sans contact haud débit

SP6 (CEA-Leti)
Sécurité

- Sécurité embarquée fonctions “privacy”
- Gestion des risques
- Preparation d’évaluation de sécurité

SP7 (ISEN)
Cas d’usages et démonstrateurs

- Définition de cas d’usages
- Methode d’intégration
- Demonstration préparation/intégration

SP8 (Instituto de Telecommunicacoes)
Dissemination et Normalisation

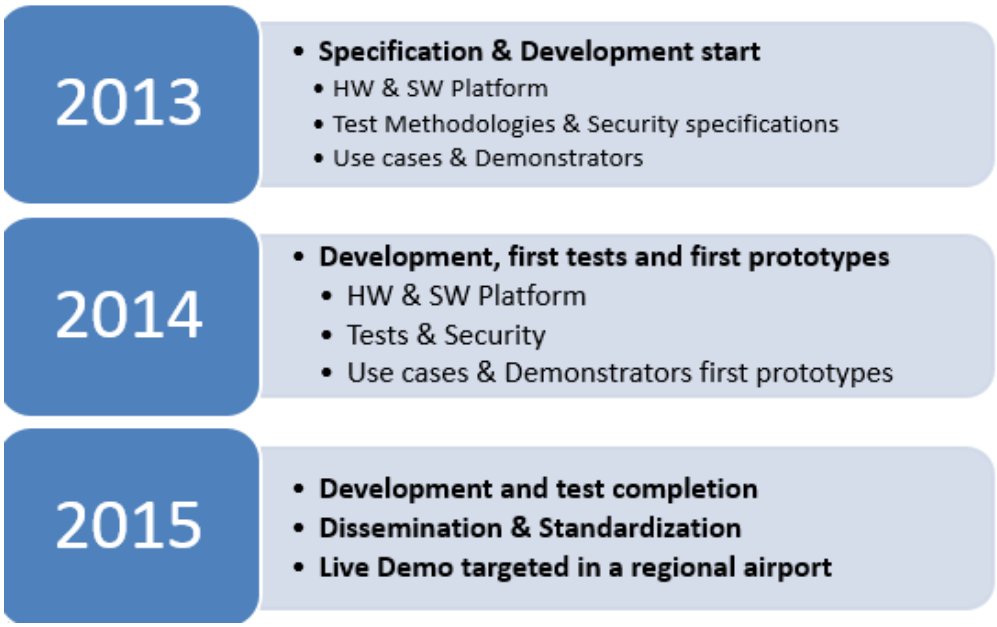
- Dissémination et exploitation
- Normalisation
- Demonstration finale

6. Description du projet

6.1. SP1 – Gestion de projet

Coordinateur	**Gemalto**
Partenaires	Tous
Objectifs	L'objectif de ce groupe de travail était de s'assurer de la cohérence du travail effectué tout au long du projet avec le plan de travail et les délais prévus.Il traite les actions de coordination de projet et les processus nécessaires pour faciliter l'élaboration et la mise en œuvre d'une stratégie globale commune. Le sous projet 1 comprend, de par sa structure de gestion, la responsabilité administrative de communiquer avec l'organisation CATRENE pour : les rapports, la préparation des revues, la participation à des événements CATRENE, etc. et pour communiquer avec les autorités publiques compétentes
Livrables	Promotion du projet et stratégie de communication Rapports semestriels Revue de projet

6.1.1. Principales étapes du projet



6.1.2. Activités par périodes

Les réunions du comité de pilotage du projet (PMB) et du comité technique du projet (PTB):

2012-2013 Réunions PMB-PTB:

Titre	Date	Lieu	Société	Sujet
KoM-PMB-PTB	18 juillet 2012	Meudon	Gemalto	Lancement du projet
PMB-PTB	12-13 novembre 2012	Munich Allemagne	Infineon	Session générale du comité de pilotage du projet.
PMB-PTB	15-16 janvier 2013	Porto Portugal	Instituto Telecom-muniacoes	Session générale du comité de pilotage du projet incluant les questions de communication (site Web). Conclusion du travail des trois derniers mois par sous projet. Discussion sur les cas d'utilisation et les relations entre sous projets. Evaluations conjointes des sous projets 2 et 7 concernant les activités des démonstrateurs.
PMB-PTB	15-16 avril 2013	Graz Austriche	NXP Semi-conductors Austria.	Session générale du comité de pilotage du projet incluant les questions de communication et de diffusion (commentaires sur le site Web) et finalisation du CR. Discussion sur les cas d'utilisation et les relations entre sous projets. Evaluations conjointes des sous projets 2 et 7 concernant les activités des démonstrateurs.
PMB-PTB	25-26 juin 2013	Vantaa Finlande	Gemalto	Session générale du comité de pilotage du projet basée sur les PCA, le plan de communication, le conseil consultatif et les problèmes rencontrés (également la visite de l'usine Gemalto Vantaa). Des sessions techniques par sous projet en mettant l'accent sur les liens avec le sous projet 2 et les sous projets 3 et 7 et des stratégies pour le passeport 4G. (Délimitation US par rapport aux priorités UE).
Gemalto	14-16 octobre 2013	La Ciotat France		Session Catrene Session générale du comité de pilotage du projet basée sur les PCA, le plan de communication, le conseil consultatif et les problèmes rencontrés (également la visite de l'usine Gemalto à Vantaa). Des sessions techniques par sous projet en mettant l'accent sur les liens avec le sous projet 2 et les sous projets 3 et 7 et des stratégies pour le

				passeport 4G..

2014 Réunions PMB-PTB:

Titre	Date	Lieu	Société	Sujet
PMB-PTB	15-16 janvier 2014	Hamburg Allemagne	NXP Semi-conductors Germany	Session générale du comité de pilotage du projet et du comité technique du projet. Conclusion du travail des trois derniers mois par sous projet. Discussion des cas d'utilisation et des relations entre sous projet. Activités des démonstrateurs en relation avec les sous projets 2 et 7.
PMB-PTB	8-9 avril 2014	Caen France	NXP Semi-conductors France	Session générale du comité de pilotage du projet et du comité technique du projet. Conclusion du travail des trois derniers mois par sous projet. Discussion commune concernant les démonstrateurs. Activités des démonstrateurs en relation avec les sous projets 2 et 7.
PMB-PTB	4-5 juin 2014	Porto Portugal	Evoleotech	Session générale du comité de pilotage du projet et du comité technique du projet. Conclusion du travail des trois derniers mois par sous projet. Activités des démonstrateurs en relation avec les sous projets 2 et 7. Evaluation de la nouvelle situation Compuworx
PMB-PTB	30 septembre – 1er octobre 2014	Graz Autriche	Infineon	Session générale du comité de pilotage du projet et du comité technique du projet. Conclusion du travail des trois derniers mois par sous projet. Discussion des cas d'utilisation et des relations entre sous projet. Activités des démonstrateurs en relation avec les sous projets 2 et 7.
PMB-PTB	8-9 décembre 2014	La Ciotat France	Gemalto	Session générale du comité de pilotage du projet et du comité technique du projet. Conclusion du travail des trois derniers mois par sous projet. Activités des démonstrateurs en relation avec les sous projets 2 et 7.

2015 Réunions PMB-PTB:

Title	Date	Location	Company	Subject
PMB-PTB	22-23 janvier 2015	Grenoble France	CEA-Leti	Session générale du comité de pilotage du projet et du comité technique du projet. Conclusion du travail des trois derniers mois par sous projet. Discussion des cas d'utilisation et des relations entre sous projet. Activités des démonstrateurs en relation avec les sous projets 2 et 7.
PMB-PTB	14-15 avril 2015	Munich Allemagne	G&D	Session générale du comité de pilotage du projet et du comité technique du projet. Conclusion du travail des trois derniers mois par sous projet. Discussion commune sur les démonstrateurs. Activités des démonstrateurs en relation avec les sous projets 2 et 7.
PMB-PTB	16 juin 2015	Toulon France	ISEN	Session générale du comité de pilotage du projet et du comité technique du projet. Conclusion du travail des trois derniers mois par sous projet. Préparation de l'examen final.
PMB-PTB	17 juin 2015	Toulon France	ISEN	Revue Finale Internationale Catrene
Revue Finale	26 Novembre 2015	La Ciotat France	Gemalto	Revue Finale France avec la Direction Générale des Entreprises

Modifications demandées au cours du projet

2013

Une demande de modification du projet a été remise au cours du premier semestre 2013, visant à corriger certaines données du projet liées au démarrage tardif de celui-ci en France et aux réponses négatives de financement dans certains pays.

Le CR a principalement fourni de nouvelles informations sur les sujets suivants:

- Mise à jour par chaque partenaire des charges de travail sur la période de juin 2012 à juin 2015
- Mise à jour du FPP en tenant compte du retrait des partenaires espagnols, et de la situation Compuworx en Hongrie.
- Mise à jour de la proposition en tenant compte du départ du partenaire autrichien SIC et de la réduction du budget des autres partenaires de ce pays.
- Mise à jour des changements en tenant compte de l'ensemble des éléments décrit ci-dessus.
- Nomination d'un nouveau chef de projet Gemalto.

Cette demande de modification a été approuvée par la SGA Catrene lors de la réunion à Munich les 28 et 29 mai 2013.

2014:

Une deuxième demande de modification a été remise au bureau Catrene au cours du premier semestre 2014, visant à corriger certaines données du projet liées au démarrage tardif ce celui-ci en France et des réponses négatives de financement dans certains pays.

Le CR a principalement fourni de nouvelles informations sur les sujets suivants:

- Mise à jour par chaque partenaire du tableau des charges de travail sur la période de juin 2012 à juin 2015
- Mise à jour des changements en tenant compte de l'ensemble des éléments décrits ci-dessus.

La demande de modification a été proposée à Catrene SGA pour discussion pendant la réunion de février 2014 et a été officiellement approuvée par l'organisation Catrene.

2015:

Une demande de modification du projet a été envoyée Durant cette période, visant à inclure Compuworx dans le projet.

La demande de modification du projet a été proposée et approuvée par Catrene SGA et discuté pendant la réunion de février 2015.

Principaux Jalons:

Sous Projet	Jalons	Date Prévue (CR #2)	Date Réalisée	Type de deliverable	Livrables prévus
SP2	J1 J2	T4 13 T1 14	T4 13 T1 14	Specification Specification	Specification plate-forme 3G Specification plate-forme 4G
SP3	J3 J4	T2 14 T2 15	T3 14 T2 15	Architecture Matérielle	MCI document d'architecture MCU sécurisés et lecteurs sécurisés
SP4	J5 J6	T4 13 T2 15	T4 13 T2 15	Specification Logicielle	Spécification des briques logicielles Disponibilité des logiciels embarqués (On-Card) et non embarqués (Off-Card)
SP5	J7 J8	T3 13 T4 14	T3 13 T4 14	Specification Outil de test	Etat de l'art spécification et méthode test Rapport logiciel de lecture universel
SP6	J9 J10	T4 13 T2 15	T4 13 T2 15	Specification Assurance Qualité	Specification des fonctions cryptographiques et confidentialités Plates-formes partiellement prêtes pour une évaluation formelle
SP7	J11 J12	T1 14 T2 15	T1 14 T2 15	Use Cases Demonstration	Definition de cas d'usages complexes Demonstration de cas d'usages complexes
SP8	J13	T1 15	T3 15	Atelier	Atelier de dissemination et démonstrations

6.1.3. Résultats obtenus

Livrables:

Livrable	Tâche	Date Prévue (CR #2)	Date réalisée	Type et Contenu
D1	T1	T4 12	T4 12 fait	Rapport Annuel
D2	T1	T2 13	T2 13 fait	Rapport Semestriel
D3	T1	T4 13	T4 13 fait	Rapport Annuel
D4	T2	T2 14	T2 14 fait	Rapport Semestriel
D5	T2	T4 14	T4 14 fait	Rapport Annuel
D6	T2	T2 15	T2 15 fait (anglais) T4 15 (français)	Rapport Final

6.2. SP2 – Spécification des plates-formes

6.2.1. Introduction

Coordinateur	**Gemalto** (Coordinateur du SP)
Partenaires	STM, CEA-Leti, Id3, IFAT, IFX, ISEN, NXP-AT, NXP-F, NXP-G , EVO, IT
Objectifs	L'objectif de cette tâche était de définir les spécifications nécessaires à la réalisation des plates-formes des prochaines générations de passeport électroniques. Ces plate formes devant être conformes à la norme ICAO 9303 LDS2 (Logical Data Structure v2) actuellement en cours de définition à l'OACI

Ce SP a été divisé en 2 tâches:

- **Tâche 1:** Specification fonctionnelle et technique des plates-formes
- **Tâche 2:** Specification de l'architecture de haut niveau des plates-formes.

6.2.2. Activités par périodes et partenaires

2012:

Gemalto
En tant que coordinateur du sous-projet, Gemalto a organisé des réunions et conférences téléphoniques avec l'ensemble des partenaires afin de recueillir les exigences. Gemalto a démarré le livrable D2.1, et produit avec l'ensemble des partenaires la liste préliminaire des exigences concernant les passeports 3G et 4G.

NXP-F
NXP-F a travaillé sur la spécification et l'ingénierie des exigences liées aux lecteurs de puces, pour assurer la compatibilité avec les passeports électroniques et les cartes d'identités électroniques. NXP a également commencé la définition de l'architecture du lecteur de puces.

STM
STM a contribué à la formulation des exigences HW.

CEA-Leti
Aucun travail démarré en 2012.

ID3
Aucun travail démarré en 2012.

ISEN-Toulon
ISEN-Toulon a travaillé sur:

- Les exigences et les tendances des normes actuelles relatives à l'utilisation d'un passeport électronique
- La coopération avec l'aéroport de Toulon Hyères Gemalto et la fourniture des spécifications fonctionnelles pour la 3ème et 4ème génération de passeport électronique
- Une coopération avec NXP-F pour réaliser les spécifications techniques des lecteurs de puce adaptée à la 3ème génération de passeport électronique.
- L'état de l'art sur les outils de caractérisation permettant la validation du protocole de VHBR

Giesecke & Devrient
G&D a démarré la spécification des exigences pour les différentes plates-formes :

- Plates-formes multi-applicatives de 3ème et 4ème génération pour le passeport électronique
- Plate-forme pour équipement mobile basé sur les environements sécurisés d'exécution (« Trusted Execution Environment ») afin de sécuriser les entrées et sorties de données.

NXP-G
Dans le cadre du SP2, NXP-Allemagne a contribué à la spécification des exigences (clarification et formulation). Deux ateliers de travail avec des clients en 2012 ont été utilisés pour collecter les exigences matérielles relatives au futur passeport électronique. Une version préliminaire des exigences matérielles a été soumise au partenaire en décembre 2012.

IFX-IFAT
Infineon a contribué à la formulation des exigences matérielles, en particulier concernant les exigences matérielles liées au protocole SAC pour le passeport de 3ème génération et en termes d'exigences mémoire pour les futures structures de données qui seront stockés sur les puces des passeports de 3ème et 4ème génération et les puces eID possédant des exigences similaires.
IFAT a commencé à évaluer les besoins de puissance et d'énergie pour la mise en œuvre du protocole SAC pour les passeports de 3ème génération. Les premières estimations de besoin de puissance et d'energie liées au VHBR pour les futures applications (par exemple eVisa), ont commencées.

NXP-A
NXP-A a commencé à travailler sur les exigences de certification et les politiques de sécurité (exigences fonctionnelles de sécurité) pour haut niveau de certification Critères Communs.

IAIK
Dans le SP2, IAIK a commencé à étudier les exigences permettant la protection de la vie privée dans le contexte des passeports électroniques et les implications pour la plate-forme matérielle sous-jacente.

Evoleo
Evoleo a commencé l'analyse et la collecte d'informations sur l'état de l'art et les tendances concernant les documents électroniques en termes de spécifications techniques et de sécurité. Les scénarios d'usage possibles de la nouvelle plate-forme et les nouveaux contextes d'usage de services supplémentaires ont également été un sujet d'étude.

IT
IT a commencé l'étude de la documentation disponible auprès des institutions et organisations concernées, afin d'établir l'état de l'art actuel des passeports électroniques (en portant une attention particulière aux activités de l'OACI), et a également commencé une identification des scénarios appropriés pour évaluer la plate-forme sécurisée avancée NewP@ss.

2013:

Gemalto
L'objectif principal pendant le premier semestre 2013 était de recueillir les exigences essentielles pour le passeport 3G (livrable D2.1). Les travaux concernant le passeport 3G s'est terminé par un revue finale le 3 mai 2013. Le second objectif pendant le premier semestre 2013 était de commencer à travailler sur la spécification de haut niveau pour les passeports électroniques 3G (livrable D2.2). Cette tâche était en cours,

et a commencé par une réunion formelle d'examen (7 Juin 2013) avec les partenaires, en acceptant la table des matières. En tant que coordinateur du SP2, Gemalto a contribué et coordonné le travail sur ces documents, et a agi comme l'éditeur principal. Le travail a inclus des réunions en face-à-face et des conférences téléphoniques avec les partenaires.
L'objectif pendant le second semestre 2013 était de créer les spécifications de haut niveau du passeport 3G, en lien avec la spécification des exigences du passeport 3G (livrable D2.2), le travail a été complété par une revue finale le 16 Octobre 2013. Le deuxième objectif pendant le second semestre 2013 était de mettre à jour le document de spécification des exigences existant (livrable D2.1) avec les nouvelles exigences spécifiques au passeport de 4ème Génération, et d'inclure un résumé des cas d'utilisation du passeport de 4ème génération. Aussi ce travail s'est terminé par une revue finale le 18 Décembre 2013. L'objectif restant pour le second semestre 2013 était de mettre à jour le document de spécifications de haut niveau du passeport 3G afin d'inclure les spécificités de l'architecture du passeport 4G. Le travail a été commencé au cours du second semestre 2013.
En tant que coordinateur du SP2, Gemalto a contribué et coordonné le travail sur ces documents, et a agi comme l'éditeur principal. Le travail a inclus des réunions en face-à-face et des conférences téléphoniques avec les partenaires.

NXP-F
NXP a travaillé sur la spécification des exigences (D2.1) en particulier du côté du lecteur et en coopération avec ID3. Plusieurs réunions téléphoniques ont été effectuées afin de discuter, de déterminer et d'examiner les exigences lecteurs.
NXP a également travaillé sur les sujets suivants:

- L'architecture de haut niveau en ce qui concerne les lecteurs (D2.2) pour les passeports 3G en coopération avec ID3. Nous avons harmonisé nos points de vue par le biais d'appels téléphoniques et d'échanges de documents. NXP s'est focalisé sur la spécification matérielle du lecteur et a coopéré avec ID3 sur les aspects logiciels.
- L'analyse et les spécifications des antennes. NXP a fait des études pour être en mesure de trouver des solutions conformes aux normes en tenant compte des contraintes du projet
- L'architecture de CPU

STM
STM a contribué à la spécification des exigences matérielles des passeports 3G et 4G en mettant l'accent sur la plate-forme matérielle du passeport 4G en 2013.

CEA-Leti
Le CEA-Leti a travaillé sur les exigences liées aux protocoles de communication (notamment en vue de préparer l'introduction du VHBR) .et aux exigences matérielles génériques.
Le CEA-Leti a également travaillé sur les exigences de sécurité. Pour le passeport 3G, l'objectif était de reprendre les exigences critères communs et les exigences de l'OACI existantes. Sur le passeport 4G, le Leti a travaillé sur les questions de vie privée, en essayant d'utiliser les exigences communes de critères existants afin de concevoir la base de ce qui pourrait devenir un profil de protection.

ID3
Id3 a travaillé avec NXP sur les exigences de lecteur RFID des passeports de 3ème génération. ID3 a étudié les normes utilisées dans la technologie de lecture des passeports électronique, (en particulier les normes adoptées par l'OACI) de manière à définir les fonctionnalités matérielles et logicielles d'un lecteur de passeport hautement interopérable.
Avec la coopération de NPX-F, ID3 a travaillé sur le document d'architecture de haut niveau concernant la définition du lecteur (D2.2). Id3 s'est focalisé sur les aspects du firmware embarqués d'un lecteur de table.

Un schéma d'architecture de haut niveau a été proposé en exposant tous les briques de logiciels impliqués dans un lecteur USB RFID.
Toutes les ressources impliquées dans le lecteur de table ont été analysées et détaillées:

- exigences USB. (« Pipes », descripteurs et classe dédiée à la norme RFID / PCSC lecteur)
- exigences de frontal RF. (Protocoles RF, le protocole NFC)
- fonctionnalités supplémentaires (ISO 7816 interface)

ISEN-Toulon
L'ISEN-Toulon a travaillé sur les points suivants:

- Sur les exigences liées au lecteur et antennes des passeports electroniques. En conformité avec les nouvelles normes de l'ISO et de l'OACI (recommandations et spécifications)
- Contribution en collaboration avec Gemalto pour 3G spécifications de haut niveau, en fournissant scénario de base 3G-
- Des réunions avec le personnel de l'aéroport de Toulon-Hyères et des observations ethnographiques de divers services de l'aéroport afin de de préparer les recommandations pour le déploiement de démonstrateurs de passeports 3G et 4G dans le contexte de l'aéroport de Toulon-Hyères

Giesecke & Devrient
G & D a contribué à la définition des besoins pour les plates-formes passeports électroniques 3G et 4G. L'accent a été mis sur les plates-formes logicielles et les interfaces pour la partie électronique des passeports 3G et 4G:

- Plate-forme passeport électronique multi-applicatives supportant les spécificités propres à chaque pays
- Interface de l'application pour la plate forme 3G (SAC)

G & D a contribué à la spécification de haut niveau pour la plate-forme de passeport 3G et 4G.
Surtout la spécification de haut niveau pour l'utilisation de smartphones comme dispositifs d'accès sécurisé aux passeports et documents d'identités électroniques.

- Plate-forme périphérique mobile basé sur l'environnement d'exécution de confiance (« Trusted Execution Environment») permettant la sécuriasation des entrées et des sorties.

NXP-G
Le travail sur les livrables du SP2 a continué en 2013, y compris les spécifications 3G et 4G. NXP a contribué à ces documents pour les éxigences et paramètres matériels. Au cours de 2013, l'accent a été mis sur les exigences de la plate-forme matérielle pour le passeport électronique 4G.

IFX-IFAT
IFX a contribué à la formulation des exigences matérielles, en particulier sur l'aspect matériel permettant les calculs liés au nouveau protocole SAC pour les passeports 3G et en termes d'exigences de mémoire pour les futures structures de données devant être stockées sur les puces des passeports électroniques 3G et 4G et les puces eID avec des exigences similaires. Le point ctrique a concerné la taille de la mémoire pour les passeports électroniques 4G concernant l'horodatage, les visas et la biométrie.

IFAT
L'évaluation des besoins de puissance et d'énergie pour la mise en œuvre du SAC pour passeports 3G s'est poursuivie.

NXP-A
NXP-A a terminé son travail sur

- Les exigences de certification et

- Les politiques o de sécurité (exigences fonctionnelles de sécurité) pour les certifications critères Communs

IAIK
Dans SP2, IAIK a poursuivi ses enquêtes sur les technologies d'amélioration de la confidentialité dans le contexte des passeports électroniques.

Evoleo
Evoleo a poursuivi ses analyses et sa collecte des informations sur l'état de l'art et les tendances des documents électroniques en termes de spécifications techniques et de sécurité. Avec une attention plus particulière aux activités de l'OACI.
Les scénarios possibles d'usage des nouvelles plate-formes pour des services supplementaires ont encore été un sujet à l'étude. Les spécifications de la PKI des interfaces d'infrastructure et de la plate forme Logicielle ont également été une contribution pour ce sous projet.

IT
IT a poursuivi sa participation à l'identification de scénarios appropriés permettant l'évaluation des plates-formes sécurisées NewP@ss.
IT a contribué à la définition des exigences du passeport 4G, (dans le livrable D2.1), sur la PKI sur les ordinateur qui hébergerons la PKI des passeports 3G et 4G.
L'evaluation des exigences préliminaires a été réalisée, concernant les aspects sécurité et interface PKI et inclus dans le livrable D2.2. La contribution pour le livrable D2.2 concerne les aspects spécification PKI, les logiciels de la plate-forme hôte, les applications et les interfaces entre l'ordinateur hôte et le lecteur, et l'ordinateur hôte et la PKI.

2014:

Gemalto
L'objectif T1 / 2014 était de mettre à jour le document de spécifications de haut niveau du passeport 3G et de définir les spécificités de l'architecture du passeport 4G. Ce livrable D2.2 a été révisé et publié fin Mars 2014, comme prévu. A ce moment, tous les livrables SP2 prévues (D2.1 et D2.2) étaient prêts et disponible. En tant que coordinateur du SP2, Gemalto a contribué et coordonné le travail sur ces documents, et a agi comme éditeur principal. Le travail a inclus des réunions en face-à-face et des conférences téléphoniques avec les partenaires.

NXP-F
NXP-F a travaillé avec ID3 pour définir les spécifications de lecteur RFID des passeports de 3e et 4e générations. Deux documents ont été livrés à ce sujet:

- exigences techniques pour 3G et 4G passeports
- spécifications de haut niveau pour la 3G et 4G passeports

STM
Aucune activité signalée au cours de la période.

ID3
Id3 a travaillé avec NXP sur les exigences RFID pour lecteur de passeport de 3ème et 4ème génération, (en particulier les normes adoptées par l'OACI) en cours pour définir les fonctionnalités matérielles et logicielles d'un lecteur de passeport hautement interopérable.

Pour ce travail, ID3 a participé à la rédaction de deux documents communs:

- «Les exigences techniques pour 3G et 4G passeports"
- "Spécification de haut niveau pour les passeports 3G et 4G"

Pour le premier semestre de 2014, ID3 a axée ses travaux sur les besoins et les spécifications du lecteur 4G. Les activités d'ID3 sur lot de travail se sont terminées au cours du deuxième semestre.

CEA-Leti

Pendant le premier semestre de l'année 2014, le CEA a contribué à D2.1 et D2.2 livrables en se concentrant sur les exigences de sécurité et les spécifications pour la plate-forme de passeport 4G.
Durant le second semestre de l'année 2014, aucune contribution du CEA le travail était terminé.

ISEN-Toulon

Sur la deuxième année du projet, l'ISEN-Toulon a travaillé sur ces points suivants:

- Les exigences techniques pour le passeport 3G et 4G, (livrable D2.1). La contribution ISEN concerne les démonstrateurs 3G développés et les cas d'utilisation pour le passeport 4G.
- Spécification de haut niveau pour les passeports 3G et 4G; (livrable D2.2). La contribution ISEN concerne la spécification de l'antenne lecteur des passeports.

IFX / IFAT

Pendant T1-2014, IFX a contribué à la formulation des exigences matérielle, en particulier sur l'aspect matériel pour le support des calculs associé au protocole SAC des passeports 3G et également en termes d'exigences de mémoire pour les futures structures de données devant être stockées sur les puces des passeports électroniques 3G et 4G, les cartes d'identité électroniques et les permis de résidences possédant des exigences similaires. L'accent a été mis sur la taille de la mémoire nécessaire aux passeports électroniques 4G pour permettre la gestion de l'horodatage, les visas et la biométrie et le support de l'écriture électronique basé sur EAC 2.0 et la lecture électronique basé sur SAC. Le résultat de la réunion de l'OACI TAG 22 de mai à Montréal, le Canada a reflété ce travail.

Giesecke & Devrient

G & D a finalisé la contribution à la spécification de haut niveau pour la plate-forme de passeport 3G et 4G et la spécification de haut niveau pour l'utilisation de smartphones comme dispositifs d'accès sécurisé aux documents d'identité et aux passeports électroniques.

NXP-G

NXP Allemagne a participé activement aux activités de clôture du SP2 (effective par décision lors de la réunion du consortium à Caen, France (8-9 Avril 2014)).

NXP-A

Aucune activité signalée au cours de la période.

IAIK

Aucune activité signalée au cours de la période.

Evoleo

Pendant T1-2014, les spécifications de hauts niveaux liés à l'ordinateur hôte et a la PKI ont été identifiées comme les applications lecteur 3G / 4G fonctionant dans l'ordinateur hôte. Les interfaces entre le dispositif de lecteur et le PC hôte et l'interface entre le PC hôte et la PKI ont également été précisées.
Aucune activité signalée pendant le second semestre 2014.

IT
Durant cette période, IT a affiné sa contribution initiale aux exigences du passeport 4G (livrable D2.1), concernant la PKI et l'ordinateur hôte 3G / 4G. Une révision de la contribution d'IT au livrable D2.2 a également été achevée, liées aux spécifications de la plate-forme logicielle pour la PKI et à l'ordinateur hôte, ainsi que des applications et des interfaces entre l'ordinateur hôte et le lecteur, et l'ordinateur hôte et PKI, pour les passeports électroniques 4G. Pendant H2 2014, IT a utilisé les exigences et les spécifications de SP2 définis, comme référence pour les développements du SP4 et SP7, y suivi les activités de normalisation de la LDS2.

2015:

Gemalto
Tous les livrables du SP2 prévues (D2.1, D2.2) sont terminés depuis Mars 2014. En tant que coordinateur du SP2, Gemalto a suivi l'activité de normalisation des futurs passeports (LDSv2) et analyser les éventuelles mises à jour dans les livrables du SP2. Les contributions réelles à la normalisation ont été discutées dans le contexte du SP8.

NXP-F
Aucune activité signalée au cours de la période. SP2 terminé.

STM
Aucune activité signalée au cours de la période. SP2 terminé.

ID3
Aucune activité signalée au cours de la période. SP2 terminé.

CEA-Leti
Aucune activité signalée au cours de la période. SP2 terminé.

ISEN-Toulon
Aucune activité signalée au cours de la période. SP2 terminé.

IFX / IFAT
Aucune activité signalée au cours de la période. SP2 terminé.

G&D
Aucune activité signalée au cours de la période. SP2 terminé.

NXP-G
Aucune activité signalée au cours de la période. SP2 terminé.

NXP-A
Aucune activité signalée au cours de la période. SP2 terminé.

IAIK
Aucune activité signalée au cours de la période. SP2 terminé.

Evoleo
Aucune activité signalée au cours de la période. SP2 terminé.

IT
Aucune activité signalée au cours de la période. SP2 terminé.

6.2.3. Coopération

- **Au sein du SP**
  - Très bonne coopération avec des informations reçus de la part de tous les partenaires.
  - Des conférences téléphoniques régulières entre les partenaires actifs ont été organisées.
  - Des points périodiques avec les coordinateurs des autres sous projets ont été organisés
  - Les réunions SP2 suivantes ont notamment été organisées:
    - **12 Novembre 2012**, Munich: Discussion des principes généraux sur la façon de travailler et de coopérer et quelles sont les contributions des partenaires.
    - Des conférences spécifiques SP2 entre les partenaires (toutes organisées par Gemalto)
    - **23 Novembre 2012**: Première rencontre avec Gemalto, ST, NXP-F, ISEN, IFX, G & D, NXP-G et IT. Discussion et accords sur le calendrier des livrables, 3G et 4G définition, catégories d'exigences, coopération avec d'autres SPs.
    - **30 Novembre 2012 & 4 Decembre 2012**: Poursuite de la définition des besoins avec un plus petit groupe (Gemalto, G & D, NXP-G, NXP-A, IAIK et IFX).
    - **10 Decembre 2012**: Travail de définition des exigences, l'ISEN rejoint le groupe pour faire un point sur la première rencontre avec l'aéroport de Toulon.
    - **19 Decembre 2012:** définition des besoins avec NXP-G, IT, Evoleo, STM, IAIK, Gemalto.
    - **3 Mai 2013:** Revue de cahier des charges 3G avec G & D, le CEA-Leti, IT, Gemalto
    - **7 Juin 2013:** Revue de spécification 3G avec Evoleo, IT, le CEA-Leti, NXP-G, F-NXP, ID3, IFX-A, IFX-G, G & D, Gemalto
    - **9 Septembre 2013:** SP2-SP7 cas d'utilisation atelier spécifique 4G (conf appel)
    - **16 Octobre 2013:** Spécification de haut niveau 3G (D2.2) revue de document (La Ciotat)
    - **18 Decembre 2013:** Exigences 4G (D2.1) revue de document (Conf appel)
    - **Janvier-Mars 2014**: conférence téléphonique avec les partenaires pour préparer la spécification de haut niveau 4G
    - **26 Mars 2014** (organisé par Gemalto): Revue des spécifications 4G avec Gemalto, G & D, NXP-G, ID3, IT, ISEN, NXP-F et IFX-A.

  - Les livrables D2.1 et D2.2 actuelles sont le résultat de l'effort conjoint de tous les partenaires actifs qui ont apporté leur contribution à ces documents.
  - Plusieurs conférences téléphoniques SP2, des ateliers et des documents revus au cours des années 2012-2014

- **Avec les autres Sous Projets**
  - **SP3**: Les specifications 3G / 4G ont alimentés le travail d'architecture matériel.
  - **SP4**: Une coopération étroite et de l'alignement a été nécéssaire lors de la création du SP4 Spécification Logicielle (D4.1, D4.2 et D4.3) et de la spécification SP2 de haut niveau (D2.2). Des contributions directes au SP4 Spécification Logicielle (D4.1, D4.2, D4.3) et D4.8 / D4.9 (Wafer / post-issuance personnalisation).
  - **SP5**: Contribution aux livrables liés aux tests (D5.4)
  - **SP6**: Alignement en ce qui concerne les aspects de sécurité des passeports 3G / 4G
  - **SP7**: Très proche coopération pour la définition des cas d'utilisation et démos 3G / 4G
  - **SP8**: Contributions aux activités de normalisation

6.2.4. Résultats obtenus

Livrables:

Livrable	Tâche	Date prévue (CR #2)	Date réalisée	Type et Contenu
D2.1	T2.1	T2 13	T2 13 fait	Specification des exigences fonctionnelles et techniques – Passeport 3G
D2.2	T4.2	T4 13	T4 13 fait	Specification de l'architecture de haut niveau (incluant les options pour les démonstateurs) – Passeport 3G
D2.1	T4.3	T4 13	T4 13 fait	Specification des exigences fonctionnelles et techniques – Passeport 4G
D2.2	T4.2	T1 14	T1 14 fait	Specification de l'architecture de haut niveau – Passeport 4G

Résultats principaux:

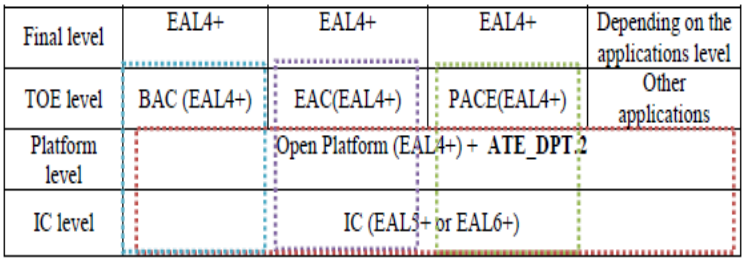
- **Année 2013 livrables = exigences fonctionnelles et techniques**
  - SP2-SP7 Ateliers cas d'usage (Mars 2013) -> entrée nécessaire pour les spécifications
  - SP2-SP7 Ateliers cas d'usage (Sept 2013) specifique au passeport 4G
  - SP2 D2.1 *terminé* (specification fonctionnelle 3G + 4G) -> documents d'entrée pour tous les autres SP
- **Année 2014 livrables = architecture**
  - SP2 Liverable D2.2 *terminé* (specification architecture 3G + 4G)
  - Contribution au SP4 : Livrables D4.1, D4.2, D4.3
- **Demonstrations (2013-2015)**
  - 3G ePassport: **Demonstration SAC avec CAN** (dernière réunion 2013)
  - 4G ePassport: **Demonstration LDSv2 eVisa/eTravelStamp read/write demonstration** (Hambourg Réunion Newp@ss, Janvier 2014)
  - 4G ePassport: **Demonstration technologie LDSv2+VHBR technology** (Graz Reunion Newp@ss, Octobre 2014)
  - 4G ePassport: **Demonstration Border Control avec LDSv2 eVisa and eTravelStamp** (Munich Réunion Newp@ss, Avril 2015)

Principales exigences passeport 3G:

- **Composant:**
  - ISO 7816 contact interface with T=0, T=1
  - ISO/IEC 14443 contactless interface typeA&B, T=CL, speeds 106-848kbps
  - CC certified at least in EAL5+ level
  - At least 400kB (code memory) and 80kB (non-volatile storage)
  - Crypto coprocessor/acceleration: DES, AES, ECC(up to 544b) and RSA (up to 4096b)
- **Lecteur:**
  - Contact reader chip:ISO/IEC7816, 5,0V (class A), 3,0V (class B), 1,8V (class C)
  - Contactless reader chip: support for NFC forum standard, ISO18092, ISO/IEC 14443 PCD standard (A and B), 106-848kbps

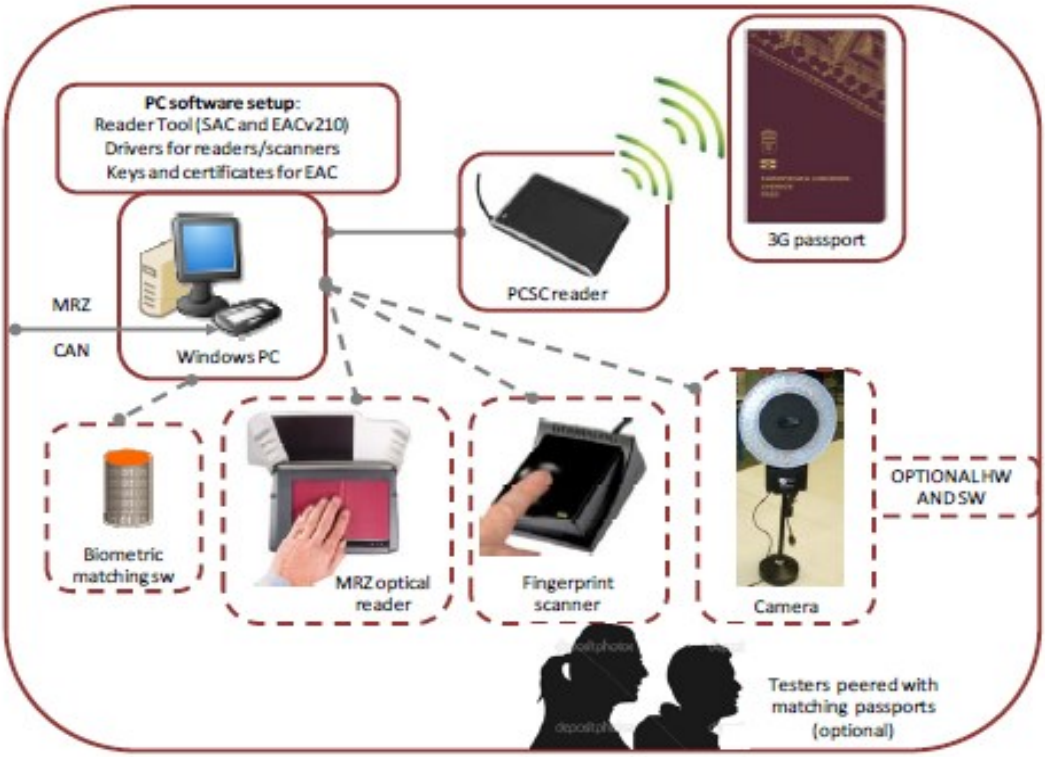
- Other: USB powered, USB2.0 host interface with host computer, interface to a secure element (e.g. for key storage) SAM, SIM or embedded SE

- **Plate-forme MRTD SE**:
  - Support multiple applications & interfaces
  - Support of crypto primitives (see list in the document) with sufficient performance
  - CC security certification (at least EAL4+ level)

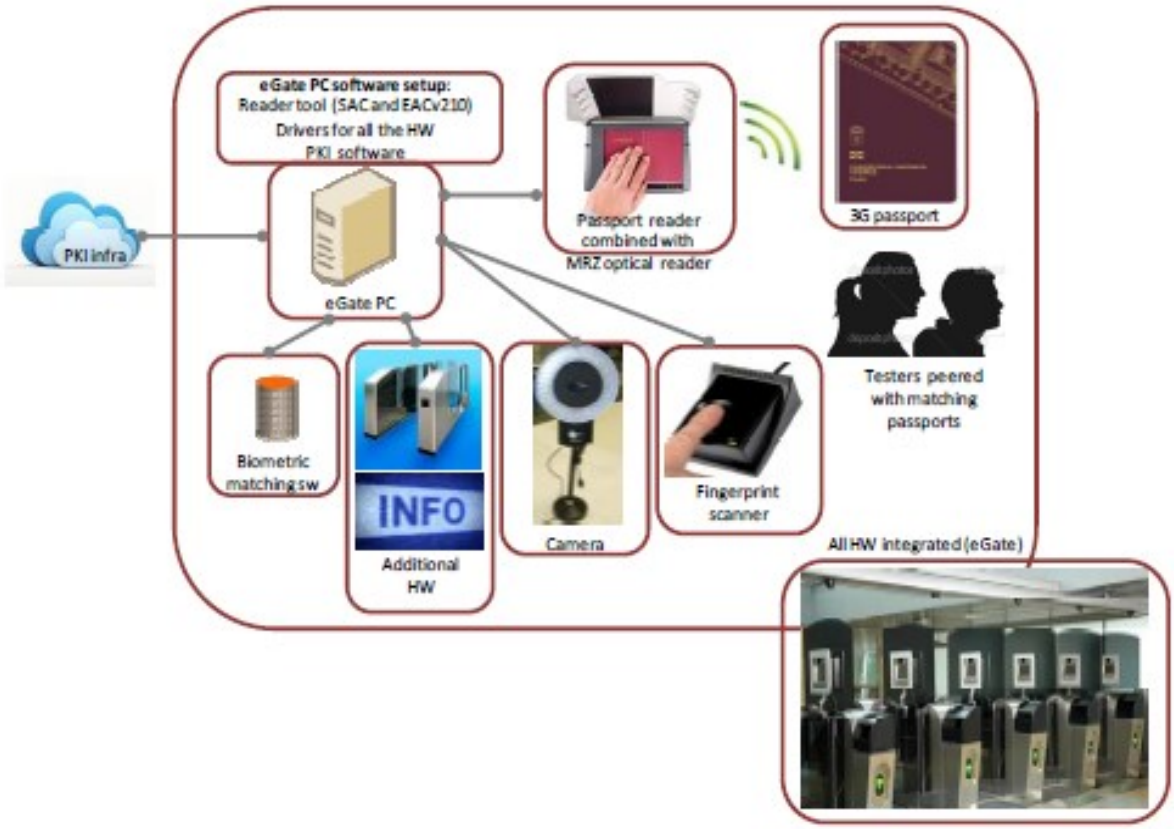


- **Application MRTD SE:**
  - Compliance with BAC, SAC, EACv210 (part1&3), and related test specifications
  - Compliancy with RF contactless communication standards [ISO14443]
  - Implement T=0, T=1, T=CL (type A+B)
  - Certification CC v3.1
    - ✓ EAL4+ certified with BAC protection profile [BAC-PP]
    - ✓ At least in EAL4+ level, with EAC protection profile [EAC-PP]
    - ✓ At least in EAL4+ level, with PACE/SAC protection profile [PACE-PP]
- **Plate-forme Lecteur:**
  - The host computer communicates with the reader using PC/SC middleware.
  - The reader device
    - ✓ shall be seen by USB host as USB CCID device
    - ✓ Embeds no ICAO protocols: Host computer takes in charges ICAO protocols such as SAC, BAC, EAC, and AA
- **Security et Certification:**
  - 3G passport shall conform[Open Platform_PP], [BAC_PP],[EAC_PP], [PACE_PP], at least in EAL4+ level
- **Tests**: voir livrables SP5.

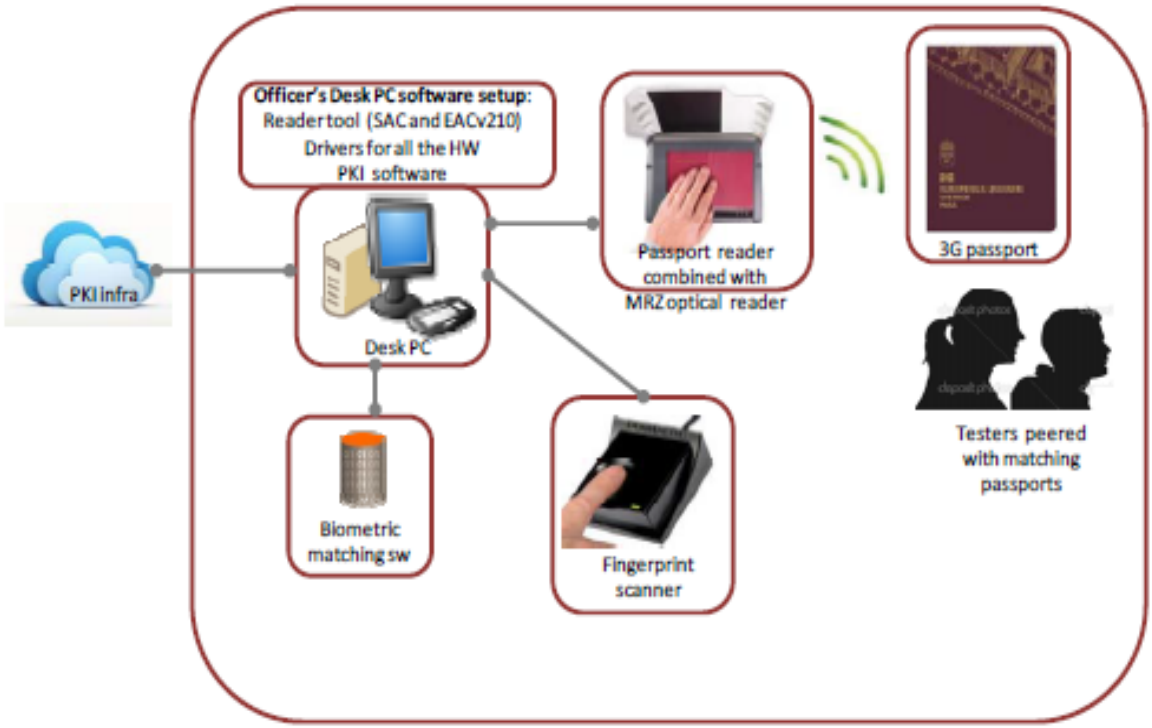
Cas d'usage 3G – "standalone":



Cas d'usage 3G – "Airport eGate":

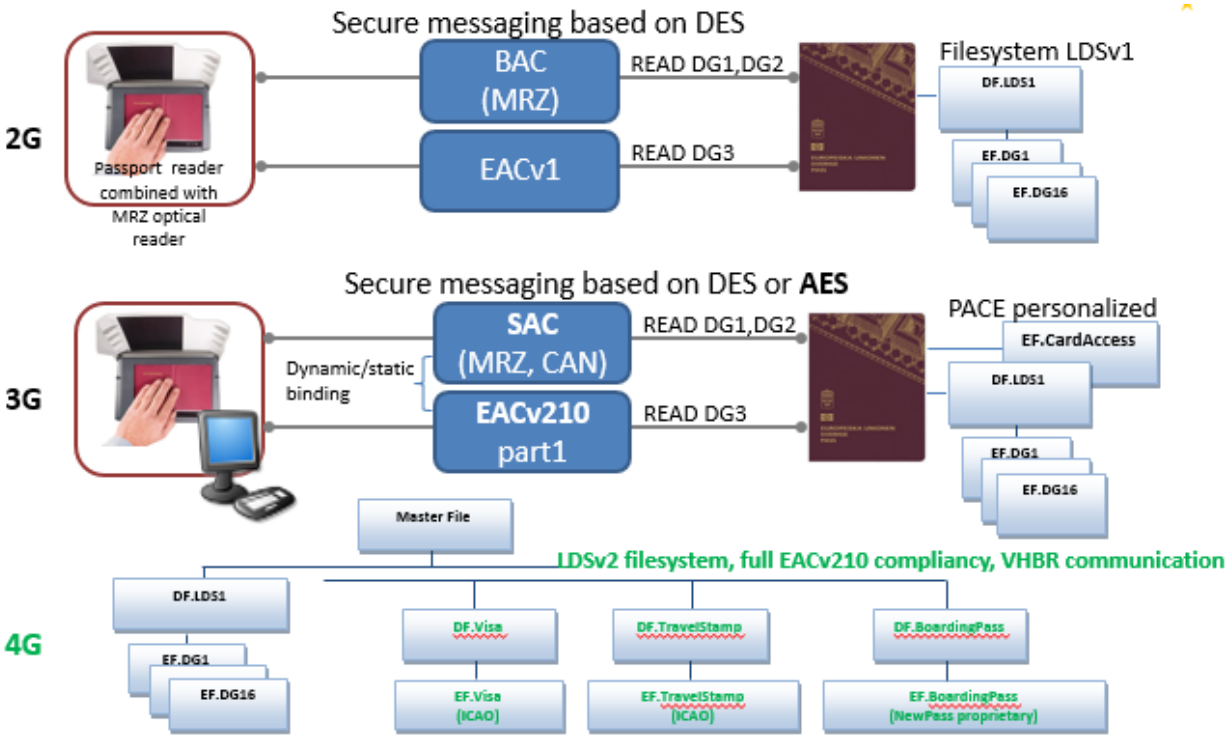


Cas d'usage 3G – "Border control desk":



Cas d'usage 3G – « Portable devices »:

Application MRTD SE:



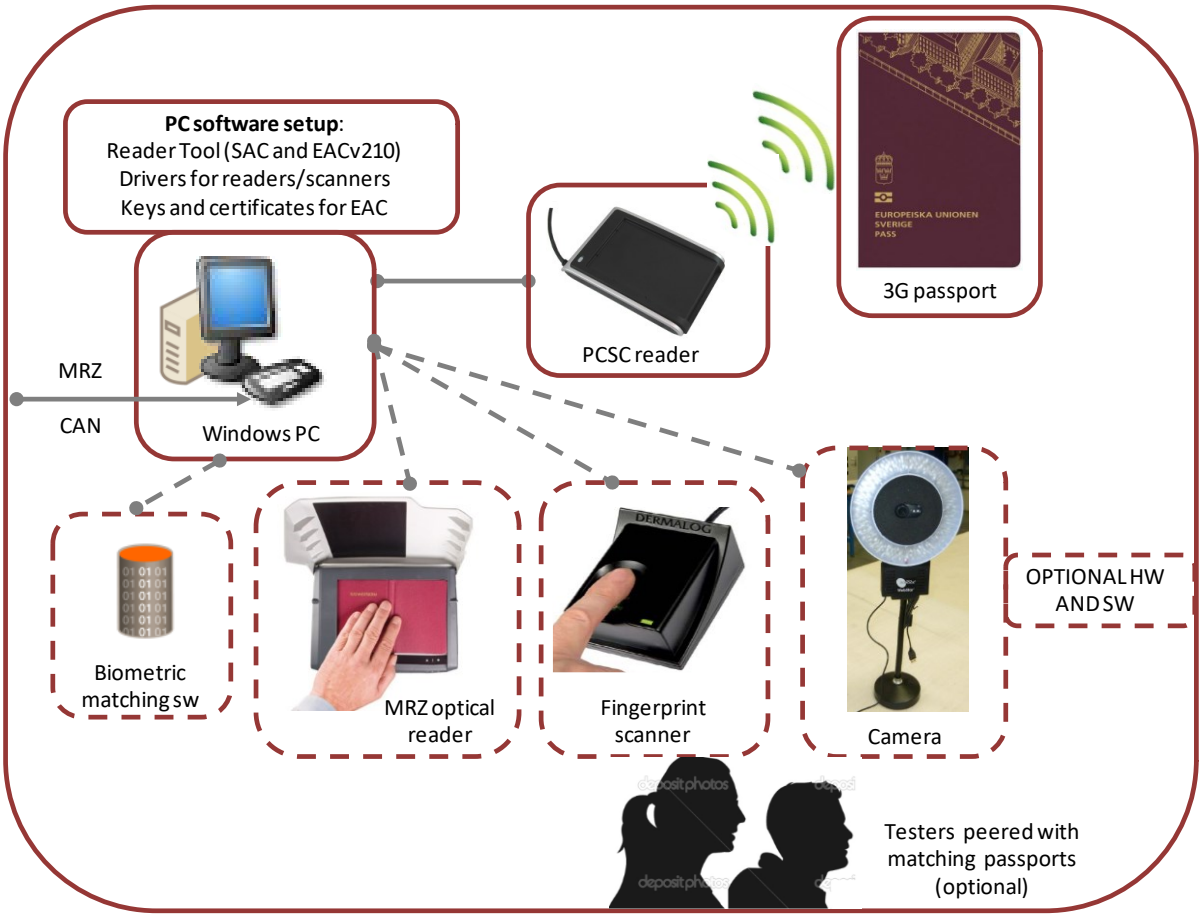
Lot de travaux SP2:

Reqs & Specs	ePassport	Reader + Host computer	PKI infra
HW	MRTD SE chip + antenna	Reader HW + antenna	No contribution
SW platform	MRTD SE platform (VHBR)	Reader platform Host computer platform	No contribution
Application	MRTD SE application (LDSv2, full EACV210, VHBR)	Reader application run in **host computer**, managing SAC/EAC/LDSv2 , interfacing PKI	Functionality reuse from ICAO, 2G/3G PKIs and LDSv2 adoption
Security	Chip+platform+appl. certification, chip+platform security (JC,GP),application security (SAC, EACv210, LDSv2)	The new crypto and authentication protocols are implemented in the application level	Advanced PKI-based security solution to support new 4G applications, based on LDSv2
Testing	WP5 (VHBR, EACv210, LDSv2)	WP5 (VHBR)	No contribution

Demonstrateurs 3G ePassport (CAN):

Description generale

Architecture Générale



Scenario d'usage:

- Saisie du CAN
- Execution du PACE ou BAC
- Lecture LDS1
- Affichage du temps de lecture et des informations lues

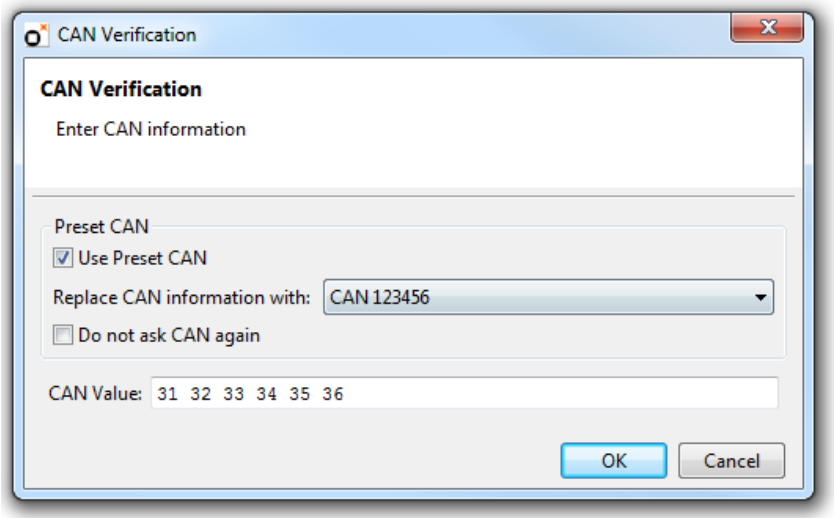


Figure 1 – Saisie du CAN

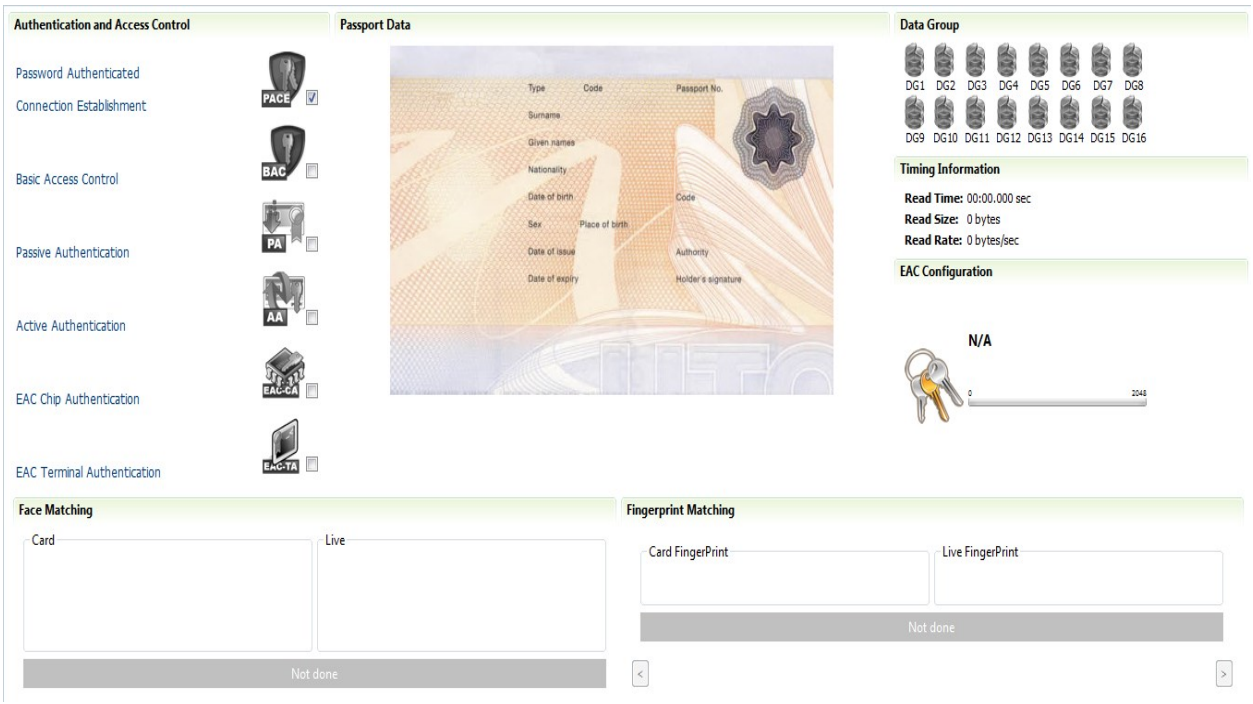


Figure 2 – Selection du Protocol de sécurité (BAC, PACE, PA, EAC …)

```
2015-05-05 16:05:42,239 [INFO ] - *** Password Authenticated Connection Establishment is  successful. ***
2015-05-05 16:05:42,240 [INFO ] - Selecting folder : #A0000002471001
2015-05-05 16:05:42,249 [DEBUG] - Reading EF.COM ...
2015-05-05 16:05:42,267 [INFO ] - LDSReaderCardService : Warning during unwrapping SM: tag 85 should be used instead of tag 87 (iso7816_C_9)
2015-05-05 16:05:42,275 [INFO ] - EF.COM (25 bytes) read successfully in 25 ms.
2015-05-05 16:05:42,275 [DEBUG] - Reading EF.SOD ...
2015-05-05 16:05:42,338 [INFO ] - EF.SOD (885 bytes) read successfully in 61 ms.
2015-05-05 16:05:42,338 [DEBUG] - Reading EF.DG14 ...
2015-05-05 16:05:42,375 [INFO ] - EF.DG14 (431 bytes) read successfully in 37 ms.
2015-05-05 16:05:42,376 [INFO ] - Generating ECDH keypair ...
2015-05-05 16:05:42,397 [INFO ] - Executing PHASE2 ...
2015-05-05 16:05:42,417 [INFO ] - Ephemeral public key:
04 CD 95 3A B8 EB 42 31 18 A1 67 B6 29 B8 D9 9C
42 7A 2F 30 A9 CF B4 2D 8B 32 7A 7E 98 C8 FE C9
FC 0B AD 96 2B 69 48 CC 1A 54 2D D5 D8 4A 83 11
99 7D 93 D3 02 98 BB 84 53 38 B5 D0 50 4C 54 9A
AD
2015-05-05 16:05:44,890 [INFO ] - MSE Set KAT IS public key done.
2015-05-05 16:05:44,891 [DEBUG] - CA Encryption Key : A1 FA 50 8D D4 2F 1E 42 A8 C2 E4 A6 A3 01 BA 45

2015-05-05 16:05:44,892 [DEBUG] - CA Integrity Key : 7B 0C 6D 4E 0A AF 97 7B C5 B3 EF 2E 0D CD 9F A3

2015-05-05 16:05:44,892 [INFO ] - Chip Authentication algorithm : EC  (256)
2015-05-05 16:05:44,893 [INFO ] - *** Chip Authentication is  successful. ***
2015-05-05 16:05:44,902 [DEBUG] - Reading EF.DG1 ...
2015-05-05 16:05:44,917 [INFO ] - LDSReaderCardService : Warning during unwrapping SM: tag 85 should be used instead of tag 87 (iso7816_C_9)
2015-05-05 16:05:44,930 [INFO ] - EF.DG1 (93 bytes) read successfully in 27 ms.
2015-05-05 16:05:44,930 [DEBUG] - Reading EF.DG2 ...
2015-05-05 16:05:45,653 [INFO ] - EF.DG2 (11368 bytes) read successfully in 721 ms.
2015-05-05 16:05:45,654 [DEBUG] - Reading EF.CVCA ...
2015-05-05 16:05:45,673 [INFO ] - EF.CVCA (13 bytes) read successfully in 19 ms.
2015-05-05 16:05:45,674 [INFO ] - Retrieval provider ::com.gemalto.tools.epassport.keyservice.eac.LocalIKD
2015-05-05 16:05:45,674 [INFO ] - Retrieving CVCA ::FRCVCATT256
2015-05-05 16:05:45,675 [INFO ] - Retrieving CVCA certificate with holder reference : FRCVCATT256
2015-05-05 16:05:45,675 [INFO ] - CVCA certificate [FRCVCATT256,FRCVCATT256] found.
2015-05-05 16:05:45,724 [INFO ] - Signature Algorithm SHA256WITHECDSA initialized for External Authentication
2015-05-05 16:05:45,744 [DEBUG] - Signature  : 30 45 02 20 71 DC C7 1B BE E7 C6 55 FD 4F 39 3C
83 32 0F B6 14 D4 AA 5A 20 66 73 C0 B7 A1 F9 3D
```

```
7F CB 79 36 C9 48 60 FD D3 9C B5 5B DA 4B 73 DB
F6 33 12 20 77 98 F8 D2 CD 95 3A B8 EB 42 31 18
A1 67 B6 29 B8 D9 9C 42 7A 2F 30 A9 CF B4 2D 8B
32 7A 7E 98 C8 FE C9 FC
2015-05-05 16:05:50,771 [INFO ] - Signature Algorithm SHA256WITHECDSA initialized for External Authentication
2015-05-05 16:05:50,798 [DEBUG] - Signature  : 30 46 02 21 00 EE EA 13 47 B7 5D 0F E9 9B F3 B5
3C D6 EC 36 BB CF 5E 34 9B 71 F2 E8 D7 B4 C7 46
3F B6 8F 29 01 02 21 00 B8 E8 0E DD 0B B8 D2 FE
65 61 F0 1C 19 E6 2A C6 CE 50 98 FA A8 CD 6E DA
77 0D 4D 73 7B 4B 6A 98
2015-05-05 16:05:50,799 [INFO ] - Signature tmp:30 46 02 21 00 EE EA 13 47 B7 5D 0F E9 9B F3 B5
3C D6 EC 36 BB CF 5E 34 9B 71 F2 E8 D7 B4 C7 46
3F B6 8F 29 01 02 21 00 B8 E8 0E DD 0B B8 D2 FE
65 61 F0 1C 19 E6 2A C6 CE 50 98 FA A8 CD 6E DA
77 0D 4D 73 7B 4B 6A 98
2015-05-05 16:05:50,799 [INFO ] - sig length :64; prev sig length :72
2015-05-05 16:05:50,799 [INFO ] - Signed data for External Authentication:
EE EA 13 47 B7 5D 0F E9 9B F3 B5 3C D6 EC 36 BB
CF 5E 34 9B 71 F2 E8 D7 B4 C7 46 3F B6 8F 29 01
B8 E8 0E DD 0B B8 D2 FE 65 61 F0 1C 19 E6 2A C6
CE 50 98 FA A8 CD 6E DA 77 0D 4D 73 7B 4B 6A 98

2015-05-05 16:05:53,271 [INFO ] - External authentication done
2015-05-05 16:05:53,272 [INFO ] - Terminal Authentication algorithm : EC SHA256 (256)
2015-05-05 16:05:53,272 [INFO ] - *** Terminal Authentication is  successful. ***
2015-05-05 16:05:53,273 [DEBUG] - Reading EF.DG3 ...
2015-05-05 16:05:54,639 [INFO ] - EF.DG3 (20213 bytes) read successfully in 1365 ms.
2015-05-05 16:05:54,639 [DEBUG] - Reading EF.DG15 ...
2015-05-05 16:05:54,672 [INFO ] - EF.DG15 (165 bytes) read successfully in 32 ms.
2015-05-05 16:05:54,673 [INFO ] - Document Signer (DSCA) from EF.SOD: CN=TEST DSCA FRA ECDSA256,C=FR
2015-05-05 16:05:54,675 [INFO ] - Looking for Coutry Signer (CSCA) certificate: C=FR, CN=TEST CSCA FRA ECDSA256...
2015-05-05 16:05:54,676 [INFO ] - CSCA certificate not found
2015-05-05 16:05:54,716 [INFO ] - *** Passive Authentication is  successful. ***
2015-05-05 16:05:54,716 [INFO ] - Passport read successful. [Total bytes read :35204 bytes, total time : 34 ms.]
2015-05-05 16:05:54,995 [INFO ] - Retrieving CVCA certificate with holder reference : FRCVCATT256
2015-05-05 16:05:54,995 [INFO ] - CVCA certificate [FRCVCATT256,FRCVCATT256] found.
2015-05-05 16:05:54,996 [INFO ] - LDS processing finished successfully.
```

Figure 3 - Run your transaction with a 3G ePassport

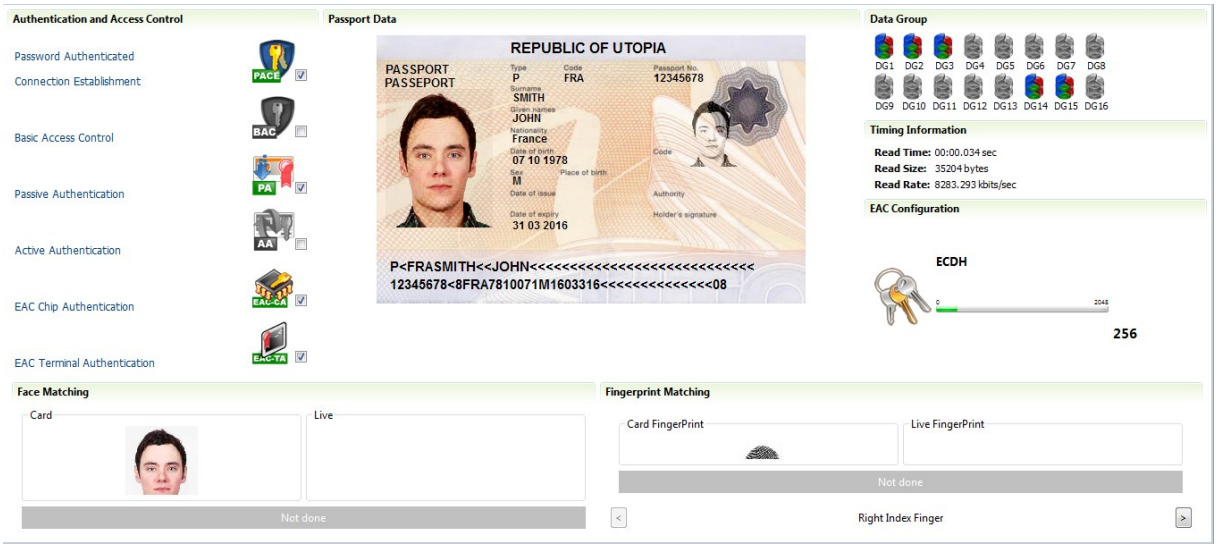


Figure 4 – Affichage des résultats (biographic & biometric data display)

Caractéristiques techniques

Matériel:

- Standard keyboard and display
- Any contactless reader, which is PC/SC compatible and compliant to ISO14443 Type A and B
- MRZ optical reader (conditional)
- Fingerprint scanner (conditional)
- Camera (conditional)
- PC, running Windows XP or Windows 7

Logiciel:

- Drivers for the readers, scanners and camera (according to the selected setup)
- Biometric data (facial image/fingerprints) matching software (conditional)

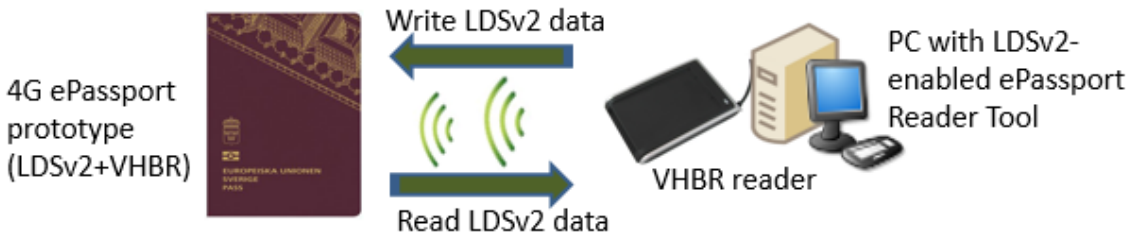
Autre:

- Keys and public key certificates needed for EAC transaction
- 3rd generation eMRTD, supporting SAC, EACv210 part 1, BAC and LDSv1

Demonstateur 4G ePassport (LDS2 / VHBR)

Description Générale

Architecture Générale:



Scénario d'usage:

- Saisie du CAN
- Execution PACE or BAC
- Lecture LDS1
- Lecture LDS2
- Affichage du temps de lecture et des informations lues
- Lecture / Ecriture eVisa
- Lecture / Ecriture travel stamps
- Lecture / Ecriture Boarding Pass

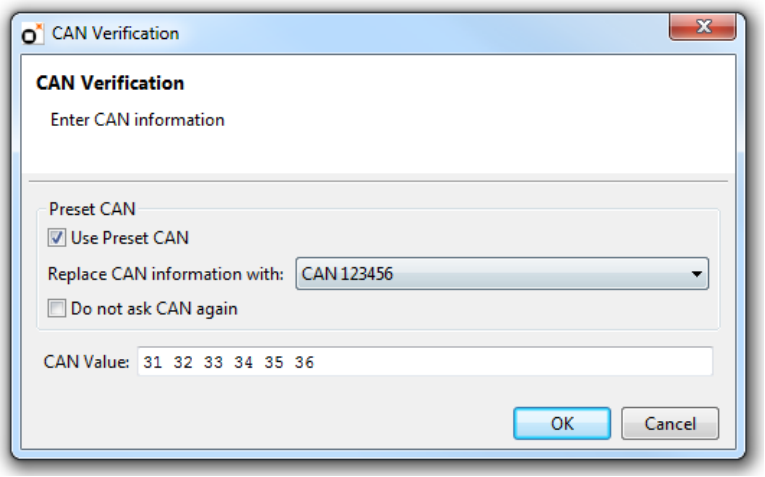


Figure 5 - Saisie du CAN

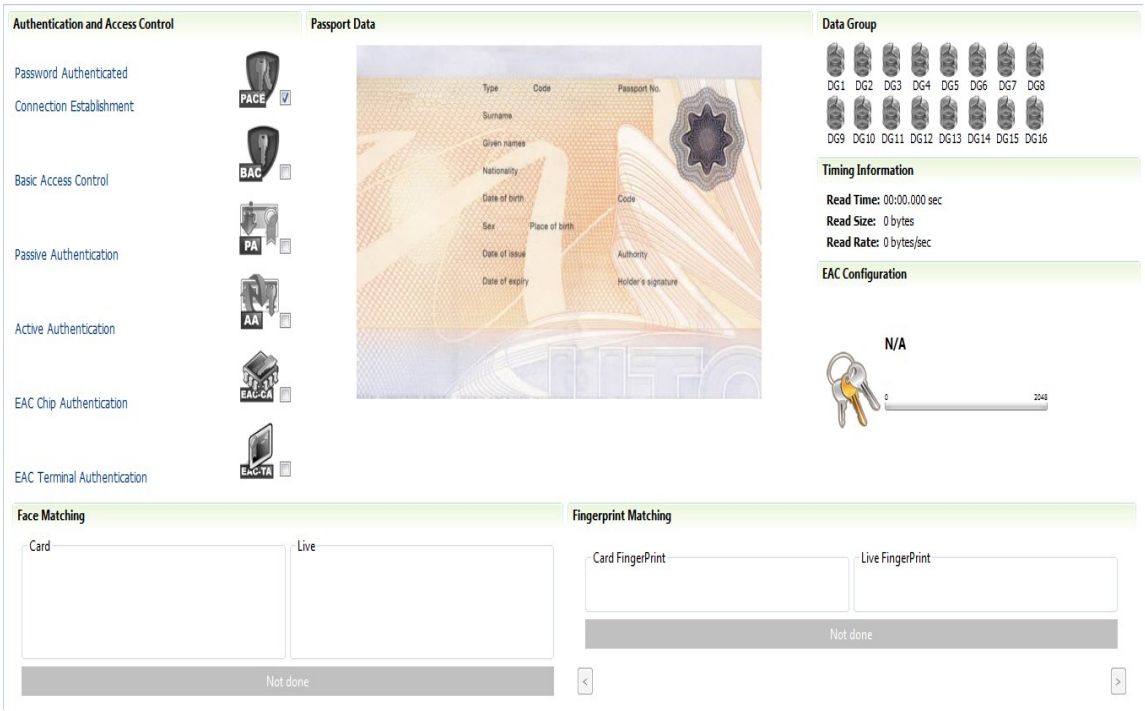


Figure 6 - Selection du Protocol de sécurité (BAC, PACE, PA, EAC …)

```
2015-05-05 16:05:42,239 [INFO ] - *** Password Authenticated Connection Establishment is  successful. ***
2015-05-05 16:05:42,240 [INFO ] - Selecting folder : #A0000002471001
2015-05-05 16:05:42,249 [DEBUG] - Reading EF.COM ...
2015-05-05 16:05:42,267 [INFO ] - LDSReaderCardService : Warning during unwrapping SM: tag 85 should be used instead of tag 87 (iso7816_C_9)
2015-05-05 16:05:42,275 [INFO ] - EF.COM (25 bytes) read successfully in 25 ms.
2015-05-05 16:05:42,275 [DEBUG] - Reading EF.SOD ...
2015-05-05 16:05:42,338 [INFO ] - EF.SOD (885 bytes) read successfully in 61 ms.
2015-05-05 16:05:42,338 [DEBUG] - Reading EF.DG14 ...
2015-05-05 16:05:42,375 [INFO ] - EF.DG14 (431 bytes) read successfully in 37 ms.
2015-05-05 16:05:42,376 [INFO ] - Generating ECDH keypair ...
2015-05-05 16:05:42,397 [INFO ] - Executing PHASE2 ...
2015-05-05 16:05:42,417 [INFO ] - Ephemeral public key:
04 CD 95 3A B8 EB 42 31 18 A1 67 B6 29 B8 D9 9C
42 7A 2F 30 A9 CF B4 2D 8B 32 7A 7E 98 C8 FE C9
FC 0B AD 96 2B 69 48 CC 1A 54 2D D5 D8 4A 83 11
99 7D 93 D3 02 98 BB 84 53 38 B5 D0 50 4C 54 9A
AD
2015-05-05 16:05:44,890 [INFO ] - MSE Set KAT IS public key done.
2015-05-05 16:05:44,891 [DEBUG] - CA Encryption Key : A1 FA 50 8D D4 2F 1E 42 A8 C2 E4 A6 A3 01 BA 45

2015-05-05 16:05:44,892 [DEBUG] - CA Integrity Key : 7B 0C 6D 4E 0A AF 97 7B C5 B3 EF 2E 0D CD 9F A3

2015-05-05 16:05:44,892 [INFO ] - Chip Authentication algorithm : EC  (256)
2015-05-05 16:05:44,893 [INFO ] - *** Chip Authentication is  successful. ***
2015-05-05 16:05:44,902 [DEBUG] - Reading EF.DG1 ...
2015-05-05 16:05:44,917 [INFO ] - LDSReaderCardService : Warning during unwrapping SM: tag 85 should be used instead of tag 87 (iso7816_C_9)
2015-05-05 16:05:44,930 [INFO ] - EF.DG1 (93 bytes) read successfully in 27 ms.
2015-05-05 16:05:44,930 [DEBUG] - Reading EF.DG2 ...
2015-05-05 16:05:45,653 [INFO ] - EF.DG2 (11368 bytes) read successfully in 721 ms.
2015-05-05 16:05:45,654 [DEBUG] - Reading EF.CVCA ...
2015-05-05 16:05:45,673 [INFO ] - EF.CVCA (13 bytes) read successfully in 19 ms.
2015-05-05 16:05:45,674 [INFO ] - Retrieval provider ::com.gemalto.tools.epassport.keyservice.eac.LocalIKD
2015-05-05 16:05:45,674 [INFO ] - Retrieving CVCA ::FRCVCATT256
2015-05-05 16:05:45,675 [INFO ] - Retrieving CVCA certificate with holder reference : FRCVCATT256
2015-05-05 16:05:45,675 [INFO ] - CVCA certificate [FRCVCATT256,FRCVCATT256] found.
2015-05-05 16:05:45,724 [INFO ] - Signature Algorithm SHA256WITHECDSA initialized for External Authentication
2015-05-05 16:05:45,744 [DEBUG] - Signature  : 30 45 02 20 71 DC C7 1B BE E7 C6 55 FD 4F 39 3C
83 32 0F B6 14 D4 AA 5A 20 66 73 C0 B7 A1 F9 3D
```

```
7F CB 79 36 C9 48 60 FD D3 9C B5 5B DA 4B 73 DB
F6 33 12 20 77 98 F8 D2 CD 95 3A B8 EB 42 31 18
A1 67 B6 29 B8 D9 9C 42 7A 2F 30 A9 CF B4 2D 8B
32 7A 7E 98 C8 FE C9 FC
2015-05-05 16:05:50,771 [INFO ] - Signature Algorithm SHA256WITHECDSA initialized for External Authentication
2015-05-05 16:05:50,798 [DEBUG] - Signature  : 30 46 02 21 00 EE EA 13 47 B7 5D 0F E9 9B F3 B5
3C D6 EC 36 BB CF 5E 34 9B 71 F2 E8 D7 B4 C7 46
3F B6 8F 29 01 02 21 00 B8 E8 0E DD 0B B8 D2 FE
65 61 F0 1C 19 E6 2A C6 CE 50 98 FA A8 CD 6E DA
77 0D 4D 73 7B 4B 6A 98
2015-05-05 16:05:50,799 [INFO ] - Signature tmp:30 46 02 21 00 EE EA 13 47 B7 5D 0F E9 9B F3 B5
3C D6 EC 36 BB CF 5E 34 9B 71 F2 E8 D7 B4 C7 46
3F B6 8F 29 01 02 21 00 B8 E8 0E DD 0B B8 D2 FE
65 61 F0 1C 19 E6 2A C6 CE 50 98 FA A8 CD 6E DA
77 0D 4D 73 7B 4B 6A 98
2015-05-05 16:05:50,799 [INFO ] - sig length :64; prev sig length :72
2015-05-05 16:05:50,799 [INFO ] - Signed data for External Authentication:
EE EA 13 47 B7 5D 0F E9 9B F3 B5 3C D6 EC 36 BB
CF 5E 34 9B 71 F2 E8 D7 B4 C7 46 3F B6 8F 29 01
B8 E8 0E DD 0B B8 D2 FE 65 61 F0 1C 19 E6 2A C6
CE 50 98 FA A8 CD 6E DA 77 0D 4D 73 7B 4B 6A 98

2015-05-05 16:05:53,271 [INFO ] - External authentication done
2015-05-05 16:05:53,272 [INFO ] - Terminal Authentication algorithm : EC SHA256 (256)
2015-05-05 16:05:53,272 [INFO ] - *** Terminal Authentication is  successful. ***
2015-05-05 16:05:53,273 [DEBUG] - Reading EF.DG3 ...
2015-05-05 16:05:54,639 [INFO ] - EF.DG3 (20213 bytes) read successfully in 1365 ms.
2015-05-05 16:05:54,639 [DEBUG] - Reading EF.DG15 ...
2015-05-05 16:05:54,672 [INFO ] - EF.DG15 (165 bytes) read successfully in 32 ms.
2015-05-05 16:05:54,673 [INFO ] - Document Signer (DSCA) from EF.SOD: CN=TEST DSCA FRA ECDSA256,C=FR
2015-05-05 16:05:54,675 [INFO ] - Looking for Coutry Signer (CSCA) certificate: C=FR, CN=TEST CSCA FRA ECDSA256...
2015-05-05 16:05:54,676 [INFO ] - CSCA certificate not found
2015-05-05 16:05:54,716 [INFO ] - *** Passive Authentication is  successful. ***
2015-05-05 16:05:54,716 [INFO ] - Passport read successful. [Total bytes read :35204 bytes, total time : 34 ms.]
2015-05-05 16:05:54,995 [INFO ] - Retrieving CVCA certificate with holder reference : FRCVCATT256
2015-05-05 16:05:54,995 [INFO ] - CVCA certificate [FRCVCATT256,FRCVCATT256] found.
2015-05-05 16:05:54,996 [INFO ] - LDS processing finished successfully.
```

Figure 7 - Transaction avec un ePassport 4G

```
2015-05-05 16:39:02,917 [INFO ] - Selecting folder : #A0000002471002
2015-05-05 16:39:03,658 [INFO ] - Reading file 01 12 (47470 bytes)
2015-05-05 16:39:04,304 [INFO ] - Reading file 01 13 (42636 bytes)
2015-05-05 16:39:04,966 [INFO ] - Reading file 02 24 (44643 bytes)
2015-05-05 16:39:05,417 [INFO ] - Successfully read EF.Visa, EF.TravelStamp and EF.BoardingPass
2015-05-05 16:39:05,417 [INFO ] - Operation took 2.738218925 seconds
```

Figure 8 – Temps de lecture ePassport

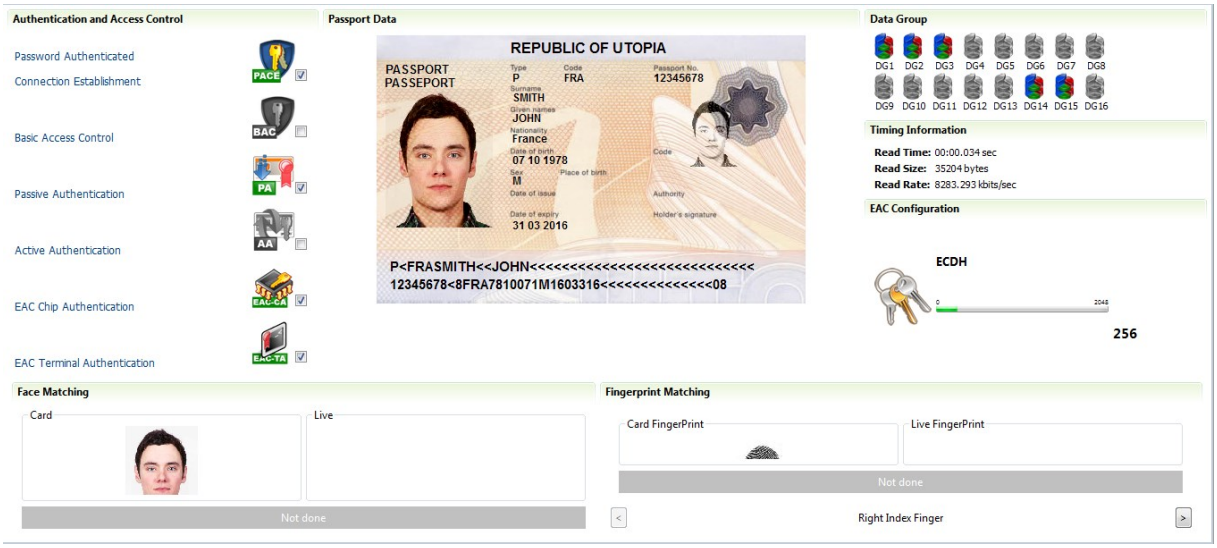


Figure 9 – Affichage des résultats (biographic & biometric data display)

Nous avons également la possibilité de lire les tampons d'horodatage, les Visa de voyage et ticket d'enregistrement:

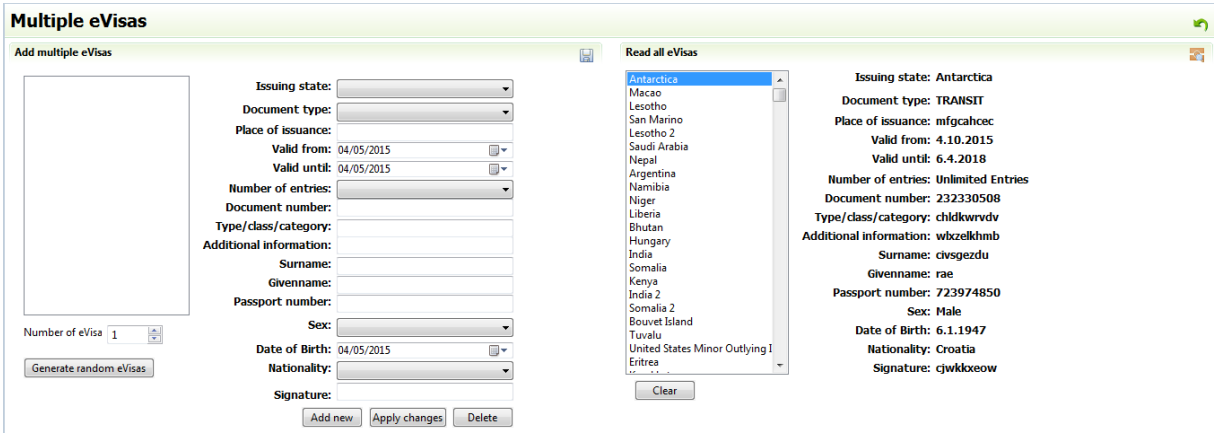


Figure 10 - Lecture/Ecriture eVisa

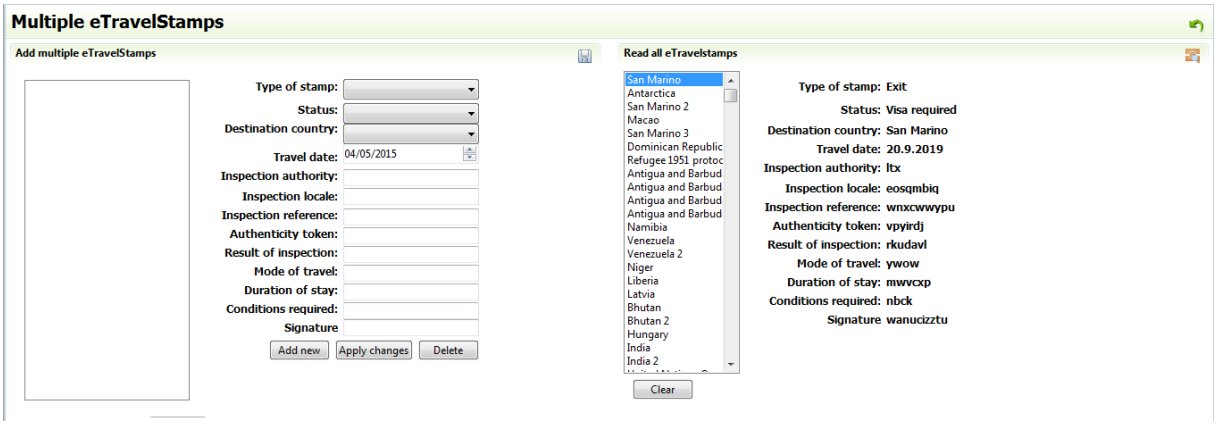


Figure 11 - Lecture/Ecriture eTravel stamps

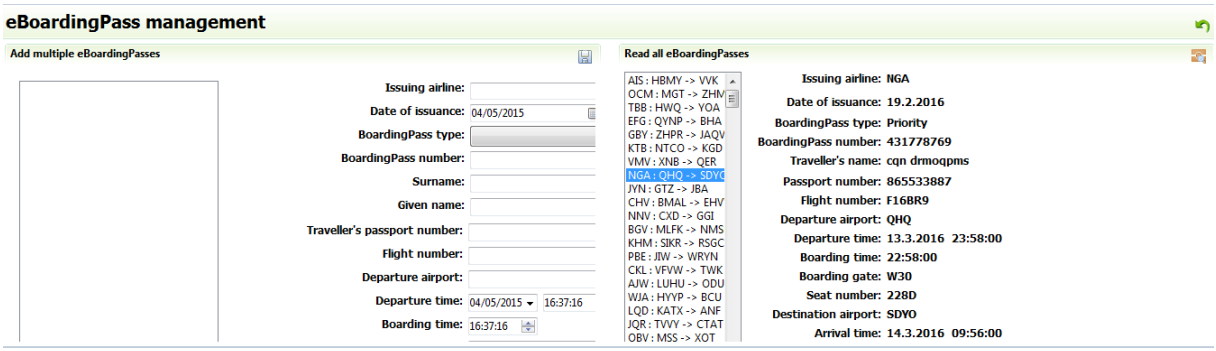


Figure 12 - Lecture/Ecriture eTravel stamps

Caractéristiques Techniques

Matériel:

- Standard keyboard and display
- VHBR reader with communication speed at least 1.6 Mbit/s from card to reader (optional)
- PC, running Windows XP or Windows 7
- MRZ optical reader (conditional)
- Fingerprint scanner (conditional)

- Camera (conditional)

Logiciel:

- Drivers for the readers, scanners and camera (according to the selected setup)
- Biometric data (facial image/fingerprints) matching software (conditional)

Autres:

- Keys and public key certificates needed for EAC transaction
- 4th generation eMRTD, supporting SAC, full EACv2, LDSv1 and LDSv2

6.3. SP3 - Développement Plates formes Matérielles

6.3.1. Introduction

Coordinateur	**STMicroelectronics**
Partenaires	CEA-Leti, Gemalto, G&D, Id3, IFAT, IFX, ISEN, NXP-F, NXP-G
Objectifs du SP	Le but de ce sous projet était de développer les microcontrôleurs sécurisés sans contact et les lecteurs de cartes associés qui étaient nécessaires pour les nouvelles générations de passeport électronique (mais qui peuvent être aussi utilisé pour d'autres produits d'identité électronique). Les microcontrôleurs et lecteurs visés doivent s'adaptera certaines caractéristiques qui pourraient être demandées par les états ; ça peut être le cas pour certaines variations d'interface sans contact (VHBR, NFC…) ou a plus haut débit, ainsi que pour de nouveaux protocoles cryptographiques ou des capacités de traitements biométriques enfouis. Dans tous les cas, la priorité a porté sur les problématiques de consommation et en particulier celles des dispositifs dédiés à la sécurité Du coté des microcontrôleurs, l'approche c'est concentrée sur des architecture à base de processeurs 32 bits, qui fournissent une capacité de traitement et un espace mémoire adressable en ligne avec le niveau de performances requis pour les applications a très haut niveau de sécurité. Néanmoins, les contraintes énergétiques (en particulier pour le fonctionnement en mode sans contact) nécessitent des concepts optimisés de gestion des alimentations, par exemple, pour supporter des architectures multiprocesseurs. Le support de logiciels embarqués multi-applications, des concepts de gestion mémoire avancés multiples et des schémas de synchronisation ont aussi été étudiés. Du coté des lecteurs, les briques développées visent principalement la performance globale et une interopérabilité accrue.

Ce Sous Projet est divisé en trois tâches principales:

- **Tâche 1:** Briques technologiques de base *(Robustesse, basse consommation, sans contact à haut débit)*
- **Tâche 2:** Développement de MCU sans contact sécurisé *(Architecture & Sécurité, suivi de l'intégration et du test)*
- **Tâche 3:** Développement de lecteur sans contact sécurisé *(Architecture & Sécurité, suivi de l'intégration et du test)*

6.3.2. Activités par périodes et partenaires

2012:

ST (Coordinateur)

Un travail initial a démarré sur la brique d'interface sans contact plus particulièrement pour une implémentation robuste et à faible consommation. Pour le microcontrôleur sécurisé, le travail d'intégration des différents besoins est en cours ainsi que les premiers choix architecturaux. La conception initiale de certaines briques de base a débuté (mémoire non volatile, dispositifs sécuritaires…) afin de finaliser les options (performance, surface…). La coopération avec l'ISEN a débuté sur les interface sans contact a faible

consommation d'énergie.

ST a aussi coordonné les activités et livrables du SP3 durant la période.

CEA-Leti

Le CEA-Leti a raffiné son programme de travail sur les spécifications et le développement au sein du projet de l'interface sans contact à haut débit. Il y a deux objectifs principaux ; D'abord le CEA-Leti va améliorer la brique existante telle que développée dans le programme BioP@ss pour intégrer les récents amendements du standard VHBR. Ensuite, le CEA-Leti va proposer et développer une nouvelle architecture pour la brique à intégrer coté carte (passeport) et qui sera conforme au nouveau standard au-delà de 6.8Mbps jusqu'à 27Mbps.

Gemalto

Pas d'activité durant cette période.

Giesecke & Devrient

Pas d'activité durant cette période.

Id3

Pas d'activité durant cette période.

IFAT

IFAT a réalisé des simulations intensives de consommation sur le microcontrôleur sécurisé 32 bit pour obtenir une cartographie de référence en vue de l'analyse de l'impact des mécanismes sécuritaires de vérification d'intégrité.

IFX

Coté IFX, les premières études conceptuelles pour des mécanismes matériels de contrôle d'intégrité pour les microcontrôleurs sécurisés 32bits ont débuté. Des estimations de circuit supplémentaire ont été générées sur des modèles abstraits pour comparer les différentes options et en extraire des informations pour l'analyse de faisabilité.

ISEN-Toulon

ISEN Toulon a travaillé sur l'expression des besoins et les tendances des standards actuels correspondants aux usages des passeports électroniques. D'autre part la coopération avec NXP-F a débuté autour des études des spécifications techniques des antennes pour la 3ème génération de passeport électronique.

NXP-F

NXP F a travaillé, dans la Tâche 3.1, sur des briques technologiques pour les lecteurs. Une étude a débutée sur les choix de processeurs et d'architecture ainsi que les optimisations potentielle. La spécification de l'interface entre le SAM et le clavier de saisie sécurisée de PIN est en cours. La coopération avec l'ISEN sur les antennes a débuté et un programme de travail agréé.

NXP-G

Les activités, au sein des Tâches 3.1 et 3.2, ont débutées conformément aux plans. Pour la Tâche 3.1, l'évaluation de plusieurs cœurs de processeur dans les nœuds technologiques visés a débuté. Cette étude est une comparaison quantitative de leurs performances intégrant les contraintes de durcissements sécuritaires et pour un budget énergétique contraint. L'intégration avec les autres éléments du système

(MMU et coprocesseurs) est aussi investiguée, pour permette un haut niveau de parallélisme des traitements.

L'activité de la Tâche 3.2 dépend en partie des travaux de la Tâche 3.1. Pour l'instant, l'intégration de l'interface sans contact à haut débit a été évaluée sur la base des mises à jour du standard ISO 14443. Ceci suppose de retravailler les structures de bus interne du microcontrôleur car, sans évolution, des goulots d'étranglement vont limiter la bande passante. En conséquence les investigations sur les architectures des bus et de l'unité de gestion de mémoire ont débutées.

2013:

ST (Coordinateur)

Au sein de la Tâche 3.1, ST a focalisé son travail sur l'évaluation et la conception de l'interface sans contact en privilégiant la très faible consommation. ST a poursuivi la coopération avec ISEN-Toulon sur ce sujet ainsi que sur certaines briques d'IP analogues pour les circuits futurs. Les études incluent aussi l'interface sans contact à haut débit (type ASK). Un effort particulier a été fait sur la modélisation du sous-système complet incluant les interactions avec l'antenne pour simuler un comportement complet avant réalisation du circuit. Ce travail sera poursuivi pour affiner les options d'architecture et d'implémentation de l'interface sans contact.

En parallèle, sur la base de l'architecture de microcontrôleur sécurisé 3G, ST a débuté (au sein de la Tâche 3.2) la définition et la conception des éléments nécessaire à l'intégration d'une première plate forme en fin 2013. Ce travail a été complété par l'évaluation initiale des mécanismes de sécurité à implémenter.

ST a aussi coordonné les activités et livrables du SP3 durant la période.

CEA-Leti

Durant le premier semestre 2013, le CEA-Leti s'est concentré sur deux sujets ; D'abord, l'évaluation de l'architecture matérielle pour générer les signaux RF modulants le 13.56MHz tant pour la solution ASK que pour la solution PSK. Ensuite la finalisation des spécifications détaillées de l'interface VHBR (contrôle digitaux, étages de modulation et circuits RF). La conception de l'amplificateur et de l'antenne sont en cours sur la base des derniers amendements de la norme ISO14443-3 relatifs à la constellation de symboles pour l'émission.

Gemalto

Gemalto a contribué à la Tâche 3.2 au travers de la spécification de besoins (pour la partie matérielle sous-jacente) du SP2.

Giesecke & Devrient

Les travaux sur les afficheurs sur carte ont débuté en Décembre 2013.

Id3

Id3 a étudié la solution de transceiver proposé par NXP comme Element central du lecteur. Une attention particulière a été portée sur les éléments périphériques du microcontrôleur.
Durant le second semestre, Id3 a réalisé une évaluation technique du VHBR. Une réunion avec le CEA-Leti a eu lieu pour évaluer les travaux existants sur le VHBR et les réutilisations potentielles dans le cadre de ce projet. Id3 a aussi évalué les solutions VHBR disponible sur le marché.
Pour préparer l'architecture du lecteur VHBR, Id3 a étudié les contraintes spécifiques à cette fonctionnalité. L'aspect vitesse a retenu l'attention ; l'architecture du lecteur VHBR a été élaboré pour assure l'homogénéité du débit de données. Ce travail a permis de proposer une architecture cohérente pour un lecteur VHBR

évitant tout goulot d'étranglement. Cette architecture a été décrite au sein du livrable D3.3.1.

IFAT
IFAT a réalisé des simulations intensives de consommation sur le microcontrôleur sécurisé 32 bit pour obtenir une cartographie de référence en vue de l'analyse de l'impact des mécanismes sécuritaires de vérification sans impact négatif sur le niveau de sécurité comme défini dans le standard ISO 15408.

IFX
IFX a travaillé sur les études conceptuelles pour des mécanismes matériels de contrôle d'intégrité pour les microcontrôleurs sécurisés 32bits. La priorité a été mise sur le développement d'un mécanisme de signature du flux d'instructions et sur une implémentation efficiente de vérification en temps réel de l'intégrité.

ISEN-Toulon
ISEN Toulon a travaillé sur la partie RF du l'interface VHBR et défini un plan de travail avec ST. ISEN-Toulon a aussi travaillé sur les antennes avancées et le sous-système RF, plus particulièrement sur des solutions reconfigurables

NXP-F
NXP F a continué le travail, dans la Tâche 3.1, sur différentes briques technologiques pour les lecteurs. Une étude a débutée sur les choix de processeurs et d'architecture ainsi que les optimisations potentielle. La spécification de l'interface entre le SAM et le clavier de saisie sécurisée de PIN est en cours. La coopération avec l'ISEN sur les antennes a débuté et un programme de travail agréé. Plusieurs études sur le choix de CPU ont été conduites pour déterminer l'architecture du circuit pour lecteur et complété par une analyse de la stabilité des échanges entre l'hôte USB (quand le lecteur sans contact est connecté à un PC) et l'interface RF. Une analyse de transfert de données a été réalisée avec la comparaison différents types de transferts entre le CPU et les interfaces avec et sans contact. Des simulations (au niveau System C) ont été réalisées pour comparer les performances du CPU avec différents type de contrôle d'accès mémoires
NXP-F a poursuivi sa coopération avec l'ISEN-Toulon sur les antennes. Un premier document de synthèse a été produit.

NXP-G
NXP-G a progressé sur les briques technologique de base au sein de la Tâche 3.1.
Une modélisation système de m'architecture du microcontrôleur avec l'interface VHBR a été réalisée confirmant les points prioritaires sur l'optimisation de la consommation de de la bande passante.
Plusieurs concepts d'architecture pour de futurs accélérateurs cryptographiques ont été développés pour comparer leurs avantages respectifs en termes de performances et de ressources (surface, consommation, sécurité et vitesse d'exécution). L'évaluation de ces résultats est en cours pour recommander un choix en vue de prochaines intégrations et industrialisations.
Des études d'architecture coté CPU ont été menés. Ce travail est une comparaison quantitative et qualitative de leurs performances pour différentes configurations. Alors que les évaluations théoriques se poursuivent, une implémentation prototype a été préparée.

2014:

ST (Coordinateur)

Au sein de la Tâche 3.1, le travail de conception est terminé pour les blocs analogues spécifiques à faible consommation et sur pour l'interface sans contact. Ceci inclus la brique VHBR ASK et les dispositifs de vérification d'intégrité du code exécuté et complète la contribution de ST au livrable D3.1.1.

Pour la Tâche 3.2, ST a fabriqué un premier prototype d'une plate forme sans contact basée sur l'architecture visée pour les microcontrôleurs sécurisés 3G/4G (incluant 480Koctets de mémoire Flash haute densité et un processeur 32bits cadencé au maximum a 28MHz). Ceci complète la contribution de ST au livrable D3.2.2. Cette plate forme intègre certains mécanismes sécuritaires du type de ceux définis dans le SP6. Un premier travail dévaluation du circuit a débuté, pour analyser en priorité l'interface sans contact (les performances en consommation et communication principalement).

ST a aussi coordonné les activités et livrables du SP3 durant la période.

CEA-Leti

Durant le premier semestre 2014, le CEA-Leti a travaillé sur l'architecture système d'une carte d'émission VHBR, principalement le contrôle digital, l'étage de modulation et le circuit RF. La conception de l'amplificateur et de l'antenne sont en cours sur la base des derniers amendements de la norme ISO14443-3 relatifs à la constellation de symboles pour l'émission.

CEA-Leti a travaillé à la conception et le développement des modules de base pour un lecteur VHBR implémentant la totalité du dernier amendement (amd5) de la norme ISO 14443-2. Ce lecteur inclut les circuits de modulation et de démodulation pour les deux solutions ASK et PSK. Ce développement permettra de tester le futur circuit RF côté carte. Il sera aussi la base d'une démonstration VHBR complète.

Par ailleurs le CE-Leti, a débuté la conception de l'interface RF destiné aux futurs microcontrôleurs sécurisés. Ce circuit implémentera la totalité du standard VHBR incluant les deux solutions ASK et PSK. La fin de conception est envisagée au printemps 2015 et les premiers prototypes à l'automne. De nombreuses simulations du traitement de signal destiné au bloc de réception ont été réalisées pour déterminer le meilleur compromis entre les performances de modulation et démodulation, la consommation et la surface.

Gemalto

Gemalto a contribué à la Tâche 3.2 au travers de la spécification de besoins (pour la partie matérielle sous-jacente) du SP2. Gemalto a aussi revu et commenté les documents produit durant la période.

Giesecke & Devrient

G&D a analysé les différentes technologies d'afficheur et de clavier compatibles avec une intégration dans une carte. Les principaux critères concernent la durée de vie, la robustesse et la très faible consommation. Pour l'intégration du logiciel G&D coordonne les activités au sein du comité de standardisation ad hoc (ISO/IEC JTC 1 SC 17 WG 4).

G&D a étudié l'intégration d'une LED dans le corps de la carte pour visualiser des données cachées lorsque la carte est activée par le champ d'un lecteur. Des prototypes ont été préparés.

Id3

Id3 a étudié et proposé une architecture originale pour les lecteurs sans contact compatibles 4G : un circuit RF dédié et un puissant microcontrôleur. Id3 a procédé à un suivi permanent des solutions VHBR disponibles sur le marché. Un circuit particulier a été identifié et étudié. Pour le circuit microcontrôleur, Id3 a réalisé une analyse comparatives des contrôleurs présents sur le marché, et retenue une première sélection sur la base des caractéristiques décrites dans les spécifications. L'accès direct aux mémoires (DMA) a été une des caractéristiques principales analysée en détails. Dans un deuxième temps, des tests comparatifs on été réalisés sur les microcontrôleurs présélectionnés les plus adaptés à un future lecteur VHBR, qui ont permis de retenir 3 solutions. Un lecteur VHBR existant a été identifié, acquis et est en cours d'évaluation

Durant l'année, Id3 a conçu et intégré un premier prototype de lecteur VHBR. Ce développement est basé sur l'architecture décrite dans le livrable D3.3.1. Parmi les tâches principales réalisées ou en cours, on notera le développement de la plate forme matérielle, un premier niveau de logiciel embarquée et des simulations

d'antenne VHBR, toujours en cours. Pour la plate forme matérielle, Id3 a intégré une première carte incluant l'interface VHBR associée à un microcontrôleur avec interface USB. Cette plate forme a permis de supporter le développement des logiciels embarqués spécifiques aux protocoles RFID et VHBR. Les activités de test de l'ensemble ont débutées. Les variations d'antennes ont été simulées, avec le logiciel EM Simulator, pour obtenir une solution offrant une bande passante suffisante. Ces dernier travaux ont été réalisés en coopération avec l'ISEN-Toulon et vont permettre de partager certain résultats.

IFAT/IFX

IFAT/IFX ont poursuivi l'analyse d'impact des mécanismes sécuritaires de vérification (sans détériorer le niveau de sécurité, comme défini dans le standard ISO 15408) sur la base des simulations intensives de consommation sur le microcontrôleur sécurisé 32 bit. La priorité a été donnée d'abord sur l'intégrité du code exécutable, activité qui s'est terminée en Juin 2014, pour traiter ensuite l'intégrité des données.

ISEN-Toulon

Durant cette année, l'ISEN-Toulon a principalement travaillé sur la faisabilité d'un amplificateur à faible bruit (LNA) dédiée au sous-système VHBR ainsi qu'à la faisabilité d'un démodulateur VHBR. D'autres études se sont poursuivies sur le développement des antennes, permettant une bonne communication entre systèmes VHBR et non VHBR. Pour assurer une bonne interopérabilité et des performances comparables entre les premières générations de passeports électroniques et les troisième et quatrième générations, ce travail inclus aussi la faisabilité d'un réseau d'accord flexible en fonction du débit souhaité. Ces activités ont représenté la contribution de l'ISEN-Toulon au livrable D3.1.1.

NXP-F

NXP-F a travaillé à l'optimisation de l'interface du lecteur (avec ou sans contact) pour les performances (antenne permettant une augmentation de la distance de fonctionnement) et pour la sécurité (claviers protégé et module de sécurité).

D'autre part NXP-F a continué les travaux sur plusieurs briques du contrôleur pour lecteur sans contact. L'évaluation des processeurs est terminée, de même que la comparaison des solutions de transfert de donnes entre le processeur et les interfaces avec ou sans contact. Enfin, l'analyse comparative des différents mécanismes d'accès mémoire (registre tampon, mémoire cache, mécanisme prédictif…) est terminée. Ces éléments ont été inclus comme contribution aux livrables D3.1.1 et D3.3.1.

NXP-G

NXP-G a poursuivi ses travaux sur les briques technologiques de base au sein de la Tâche 3.1. L'architecture cible retenue pour les microcontrôleurs intégrant une interface VHBR a été vérifiée et validée. Le budget énergétique et l'optimisation de la bande passante ont été confirmés par des simulations intensives. Les résultats montrent que solution industrielle issue de ces travaux, devra retenir un compromis entre le débit de communication, l'énergie disponible et les fréquences de travail du processeur et des crypto-processeurs.

Les concepts d'architecture pour les futurs crypto-processeurs ont été évalués. En préparation de futures intégrations dans des produits commerciaux, les différentes conditions d'opération ont été définies pour atteindre les objectifs visés.

Quant aux études d'architecture des processeurs, elles sont terminées, et des éléments de cœur ont été fabriqués sous forme de prototypes et leur validation a débutée.

2015:

ST (Coordinateur)

Au sein de la Tâche 3.1, ST a terminé l'évaluation de la nouvelle interface VHBR confirmant les performances en débit ainsi qu'en consommation (Contribution au livrable D.3.1.2). L'activité de ST dans cette Tâche 3.1 est terminée.

Dans la Tâche 3.2, le prototype de plate forme sans contact pour les passeports 3G/4G (incluant 480Koctets de mémoire Flash haute densité et un processeur 32bits cadencé au maximum a 28MHz) a été entièrement évalué (terminant ainsi la contribution de ST au livrable D3.2.3.). Cette plate forme inclus des mécanismes de sécurité comparables à ceux étudiés dans le SP6. Cette évaluation a confirmé les fonctionnalités du circuit, en particulier, la gestion d'accès mémoire, les capacités de traitement, les traitements cryptographiques sécurisés à et les performances de l'interface VHBR. Ce travail est maintenant terminé.

ST a aussi coordonné les activités et livrables du SP3 durant la période.

CEA-Leti

Le premier semestre de 2015 a vu la conception mixte (analogue/digital) du circuit d'interface VHBR pour le PICC. Sur la base de l'architecture étudiée en 2014 et le prototype intégré en FPG et présenté en démonstration lors de la revue finale, l'architecture et les algorithmes ont été finalisés. Le lancement de la fabrication d'un prototype silicium a été décalé à Septembre. Ce circuit intégre un récepteur RF en quadrature innovant, permettant une consommation très réduite et un sous système de traitement de signal digital pour réduire les effets de distorsion liés au facteur de couplage des antennes. Comme ce circuit est conçu pour supporter l'intégralité de la norme ISO/ISE 14443-2 (Amd 3 et Amd 5) pour les modulations ASK et PSK, des fonctions de test spécifiques ont été ajoutées pour vérifier (voire contourner en cas de fonctionnement incorrect ou bloquant) les briques élémentaires analogues et le bloc de traitement digital. Ces fonctions pourront introduire un supplément de consommation, mais jugé acceptable au vu de la capacité à valider et caractériser un circuit aussi innovant. Le rapport de développement a été intégré au livrable D.3.1.3.

Toujours basé sur le récent amendement 5 à la norme ISO/ISE 14443-3 (Amd 5), le CEA-Leti a intégré, dans le cadre de la Tâche 3.3, une carte lecteur sans contact pour une architecture VHBR supportant à la fois la modulation et démodulation ASK et PSK. Ce développement a été validité et sera l'outil de base pour la validation, prévue en fin d'année, du prototype d'interface VHBR (coté PICC).

Gemalto

Comme contribution au livrable D3.2.4, Gemalto a réalisé une analyse détaillée des afficheurs compatibles pour une intégration dans des cartes ou des documents électroniques (comme le passeport). Un ensemble se besoins particuliers doit être adressé lorsqu'un afficheur, ou de manière plus générale, une interface doit être intégrée dans une carte.

Giesecke & Devrient

En 2015 G&D a analysé des dessins et des matériaux permettant l'intégration de sous-systèmes dans la carte.

Comme rapporté dans le livrable D3.2.4, G&D a donc étudié l'intégration d'une LED dans le corps de la carte pour visualiser des données cachées lorsque la carte est activée par le champ d'un lecteur. Des prototypes ont été préparés.

Id3

Durant l'année 2015, Id3 a travaillé, sur l'intégration et l'amélioration en termes d'interopérabilité du lecteur VHBR et sur sa caractérisation.

Durant l'année, Id3 a conçu et intégré un premier prototype de lecteur VHBR basé sur une plate forme matérielle (associant l'interface VHBR à un microcontrôleur avec interface USB), un premier niveau de logiciel embarquée et des simulations d'antenne VHBR. Id3 continu le développement de ce lecteur VHBR pour

supporter toutes les technologies RFID. L'effort porte sur l'amélioration matérielle et logicielle visant une interopérabilité maximale entre cartes et lecteur. Pour ce faire plusieurs dessin d'antenne ont été testés et comparés. Ces travaux ont été rapportés dans le livrable D3.3.2.

Id3 a débuté une large activité de caractérisation du lecteur. Les objectifs de ces travaux sont multiples : dans un premier temps il d'agit de vérifier les caractéristiques du lecteur et de s'assurer de leur conformité avec les normes visées ainsi qu'avec les directives EMC ; des tests ont été réalisés sur la plate forme matérielle, en particulier sur l'antenne et le spectre d'émission. Dans un second temps, la caractérisation du lecteur a porté sur les performances électriques, plus particulièrement la distance de fonctionnement et le débit de communication. Pour effectuer ces mesures, Id3 a développé des outils matériels et logiciels, en particulier un robot a été utilisé pour effectuer automatiquement l'ensemble des présentations de cartes face au lecteur. Le détail de ces travaux a été rapporté dans le livrable D3.3.3.

IFAT/IFX

IFAT/IFX ont évalué les prototypes de microcontrôleur 32 bits avec mécanismes de vérification d'intégrité, tant sur les aspects consommation que résistance sécuritaire, permettant de confirmer les résultats de simulations. Cette activité est maintenant terminée.

ISEN-Toulon

Pour assurer une bonne interopérabilité et des performances comparables entre les premières générations de passeports électroniques et les troisièmes et quatrièmes générations, l'ISEN-Toulon a développé, durant cette dernière année, réseau d'accord différentiel permettant de transférer plus d'énergie vers l'antenne du lecteur. Ce circuit d'accord permet de travailler sur la totalité de la bande de fréquence VHBR en assurant l'intégrité du signal transmis.

En parallèle, l'ISEN-Toulon a terminé une série de mesures intensives des réponses de la carte sans contact communicant à différentes vitesses. Ces réponses seront vues par les antennes des lecteurs pour les différents facteurs de qualité des débits VHBR standardisés.

NXP-F

NXP-F a travaillé à l'optimisation de l'interface du lecteur (avec ou sans contact) pour les performances (antenne permettant une augmentation de la distance de fonctionnement) et pour la sécurité (claviers protégé et module de sécurité).

D'autre part NXP-F a poursuivi les travaux sur plusieurs briques du contrôleur pour lecteur sans contact. Ces éléments ont été inclus comme contribution aux livrables D3.1.1 et D3.3.1. L'évaluation des processeurs est terminée, de même que la comparaison des solutions de transfert de donnes entre le processeur et les interfaces avec ou sans contact. Enfin, l'analyse comparative des différents mécanismes d'accès mémoire (registre tampon, mémoire cache, mécanisme prédictif…) est terminée.

NXP-G

NXP-G a terminés les derniers travaux durant cette période du projet. Les résultats d'évaluation ont été finalisés et diffusés en interne pour préparer la future industrialisation des résultats du projet. Les documents ont étés terminés et les résultats archivés.

Comme rapporté dans le livrable D3.1.3, NXP-G a complété les études sur les architectures de CPU et sur les accélérateurs cryptographiques avancés.

Pour les architectures de CPU, les équipes ont principalement comparé trois processeurs (les processeurs Cortex M0 et Cortex M3 de la société ARM et un cœur propriétaire NXP). Le budget énergétique et l'optimisation de la bande passante ont été confirmés par des simulations intensives. Les résultats montrent que solution industrielle issue de ces travaux, devra retenir un compromis entre le débit de communication,

l'énergie disponible et les fréquences de travail du processeur et des crypto-processeurs.

Les concepts d'architecture pour les futurs crypto-processeurs ont visés les configurations et la flexibilité (tant au niveau matériel que logiciel embarqué ou microcode) tout en maintenant un haut niveau de résistance sécuritaire. Plusieurs concepts de crypto-processeur ont été étudiés et évalués. Même si capacité de reconfiguration devrai devenir la norme du futur à moyen terme, tous les exemples d'implémentation on clairement montrés une évaluation de performance (temps de transaction) inversement fonction du niveau de reconfiguration.

Comme rapporté dans le livrable D3.2.4, NXP-G a aussi travaillé sur une authentification à base de reconnaissance de geste en utilisant une matrice de capteurs capacitifs enfouis dans le corps de la carte.

6.3.3. Coopération

Tous les partenaires du sous projet ont contribué aux travaux avec de bons échanges techniques. Des réunions de synchronisations des activités du sous projets se sont tenues en parallèle de chaque réunion de consortium.

- **Coopérations au sein du Sous Projet**
  - **ISEN / ST :** travail de conception et d'évaluation brique VHBR
  - **IFX / NXP / ST:** évaluation conjointe des architectures MCU
  - **Id3 / ISEN :** simulation d'antennes lecteur & circuit d'accord large bande
  - **Id3 / IFX & Id3 / ST :** démonstrations VHBR
- **Coopérations avec les autres Sous Projets**
  - **SP2 & SP4:** échanges sur les spécifications
  - **SP5:** test et conformité VHBR (CEA-LETI / ISEN)
  - **SP6:** échanges sur les dispositifs sécuritaires
  - **SP7:** démonstrations (Principalement communications à haut débit)
    - ✓ Lecteur Id3 avec carte à base de composant Infineon
    - ✓ Passeport à base de MCU sécurisé ST et lecteur
    - ✓ Lecteur à haut débit (VHBR) à base de composant NXP

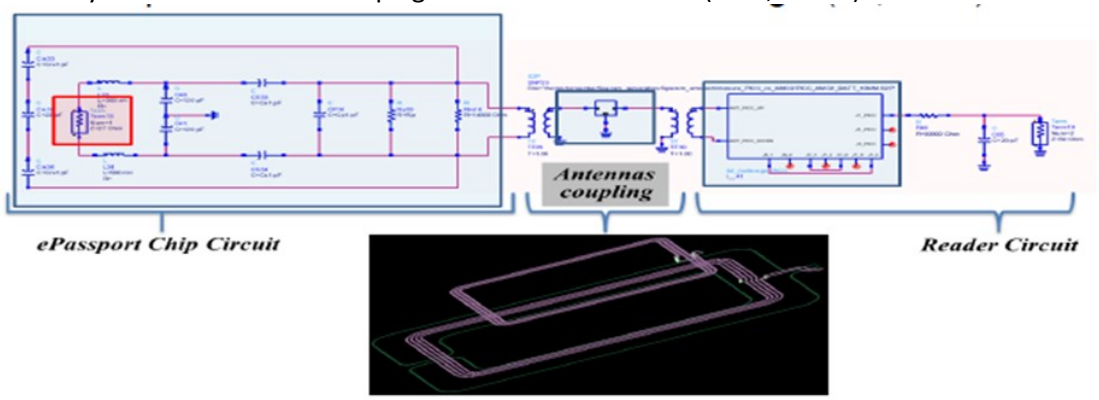
6.3.4. Résultats obtenus

Livrables:

Livrable	Tâche	Plan (CR #2)	Statut	Type et Contenu
D3.1.1	T3.1	T1 14	Livré T1 14	Rapport initial sur les briques technologiques de base
D3.1.2	T3.1	T4 14	Livré T4 14	Rapport d'évaluation des briques technologiques de base
D3.1.3	T3.1	T2 15	Livré T2 15	Rapport sur de futures briques technologiques de base
D3.2.1	T3.2	T2 14	Livré T3 14	Architecture de MCU sans contact sécurisé
D3.2.2	T3.2	T3 14	Livré T3 14	Prototype de MCU sans contact sécurisé
D3.2.3	T3.2	T2 15	Livré T2 15	Evaluation de MCU sans contact sécurisé
D3.2.4	T3.2	T2 15	Livré T2 15	Rapport sur des extensions de briques Matérielles / Logicielles
D3.3.1	T3.3	T1 14	Livré T1 14	Architecture de Lecteur sans contact sécurisé
D3.3.2	T3.3	T2 14	Livré T4 14	Démonstrateur de Lecteur sans contact sécurisé
D3.3.3	T3.3	T2 15	Livré T2 15	Evaluation de Lecteur sans contact sécurisé

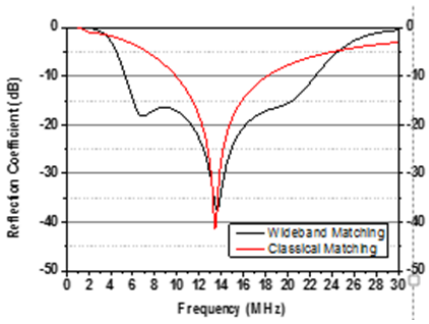
Résultats principaux:

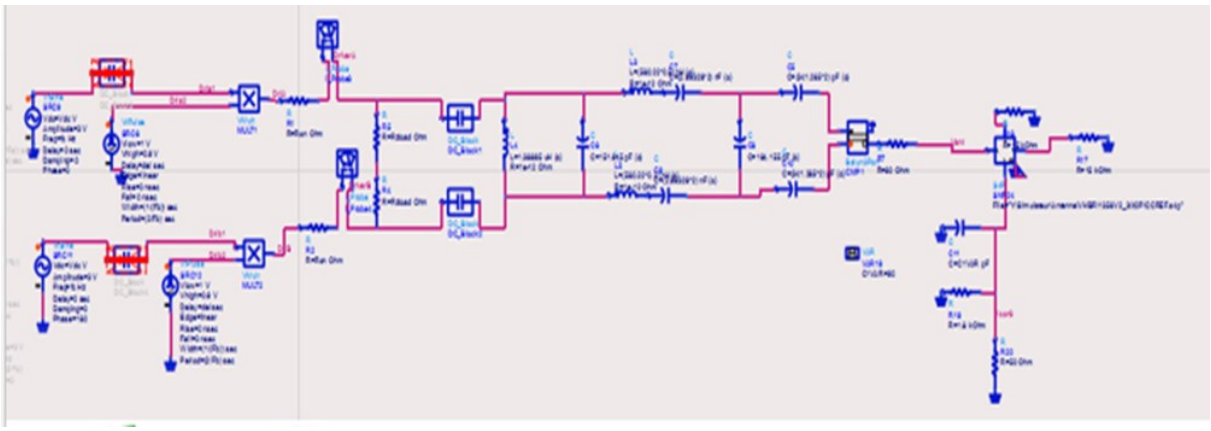
- **Tâche 1: Briques technologiques de base**
  - **Etudes préliminaires d'interface sans contact à haut débit**
    - ✓ Mesures sur le circuit VHBR actuel pour préparer de nouvelles architectures (CEA-Leti)
    - ✓ Analyse de la norme VHBR pour le test (avec le SP5) et la conformité
    - ✓ Etudes initiales pour une interface VHBR ASK à faible consommation (ST, ISEN)
    - ✓ Analyse et simulation de couplage d'antennes avancées (ISEN, NXP-F)



  - **Interface VHBR ASK à faible consommation (ST)**
    - ✓ Intégré dans le prototype de MCU sans contact
    - ✓ Transfer jusqu'à 3.4 Mbps (Rx) & 6.8 Mbps (Tx)

  - **Circuit d'adaptation large bande (ISEN-id3):**
    - ✓ Même facteur de qualité qu'un circuit d'adaptation classique
    - ✓ Coefficient de réflexion optimisé pour les bandes de fréquences VHBR

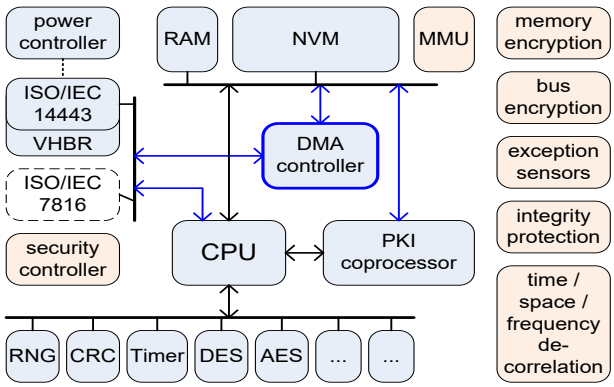




- **Impact du taux de transfert de données sur l'architecture lecteur (NXP-F)**
  - ✓ Mesures de comparaison entre différents scenarii, supportant la conclusion qu'un bus direct AHB-master est préférable à une solution BMA
    - Marge plus importante en bande passante au niveau de la RAM
    - Problème potentiel de latence avec la combinaison BMA/USB pour les hauts débits (12Mbps) avec une horloge système réduite (13.56MHz)

- **Architecture d'accélérateur cryptographique (NXP-G)**
  - ✓ Modélisation et prototypage d'un coprocesseur AES (résistance accrue à l'injection de fautes).
  - ✓ Architecture basée sur des calculs sur une transformée mathématique des données

- **Etude sur les architectures CPU (NXP-G)**
  - ✓ Finalisation de recommandations pour l'architecture CPU basé sur l'intégration du VHBR et la modélisation de la bande passante.

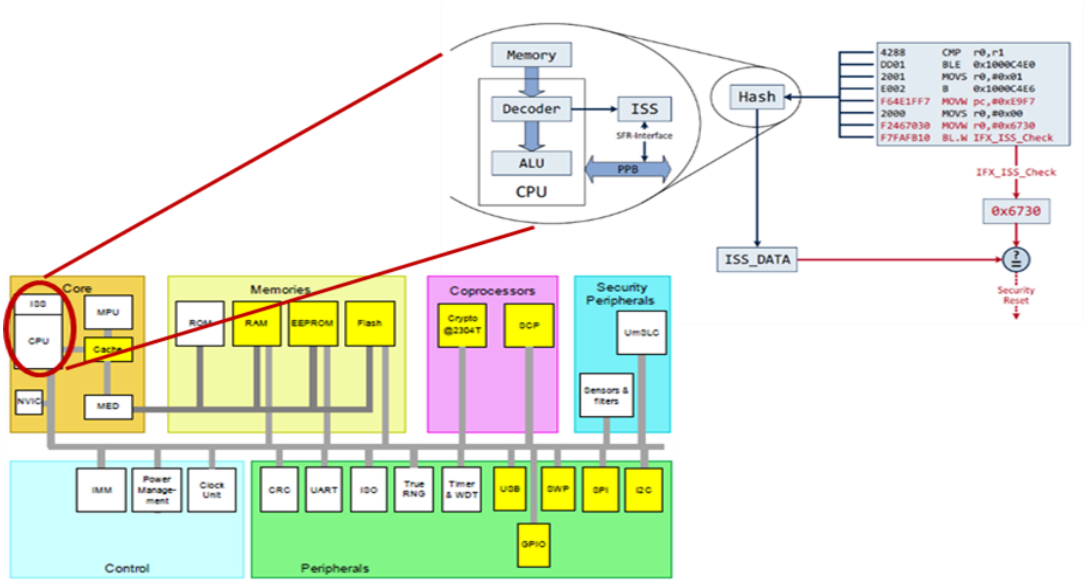


- **Récepteur VHBR ASK/PSK pour carte en CMOS 65 nm (LETI)**
  - ✓ Jusqu'à 6,8 Mbps (ASK), 27 Mbps (PSK) / 4mm² / 0.5mA (cible)
  - ✓ Définition d'architecture complexe → retard → Tape out Sep. 2015

- **Tâche 2: Développement de MCU sans contact sécurisé**

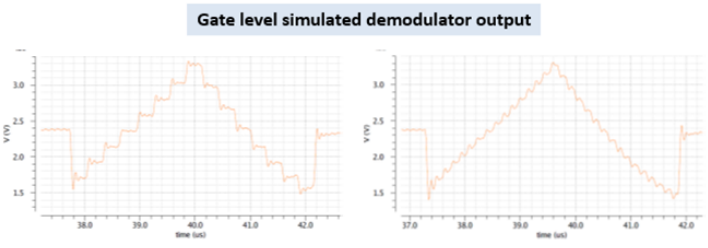
  - **Architecture de haut niveau & dispositifs sécuritaires principaux**
    - ✓ Spécifications architecturales du modem VHBR (Leti)
    - ✓ Architecture initiale de MCU sécurisé incluant les capacités 4G (Tous)
    - ✓ Comparaison architecturale (qualitative/quantitative) des CPU (NXP-G)

- **Mécanismes d'intégrité pour MCU 32 bits et consommation (IFX)**
  - ✓ Premier silicium avec dispositif d'intégrité de code disponible



  - ✓ Tests fonctionnels, résistance aux fautes, consommation évaluée
- **Premier MCU sécurisé évalué - 3G avec capacités 4G (ST)**
  - ✓ CPU 32 bit sécurisé, 480 KOctets Page Flash NVM, compatible CCEAL6+
  - ✓ Horloge interne à 28Mhz (sélection de fréquence pour consommation)
  - ✓ Interface sans contact:
    - ISO/IEC 14443 (type A & B) et ISO/IEC 18092 (Détection automatique de RF)
    - Transfer Haut Débit (VHBR): ASK testé jusqu'à 3.4 Mbps (Rx) & 6.8 Mbps (Tx)
- **Extensions Matérielles / Logicielles**
  - ✓ Intégration LED dans la carte (démonstration G&D)
    - Visualisation d'impression dans la carte
  - ✓ Authentification à base de geste (démonstration NXP)
    - Utilise une matrice de capteurs capacitifs (9)

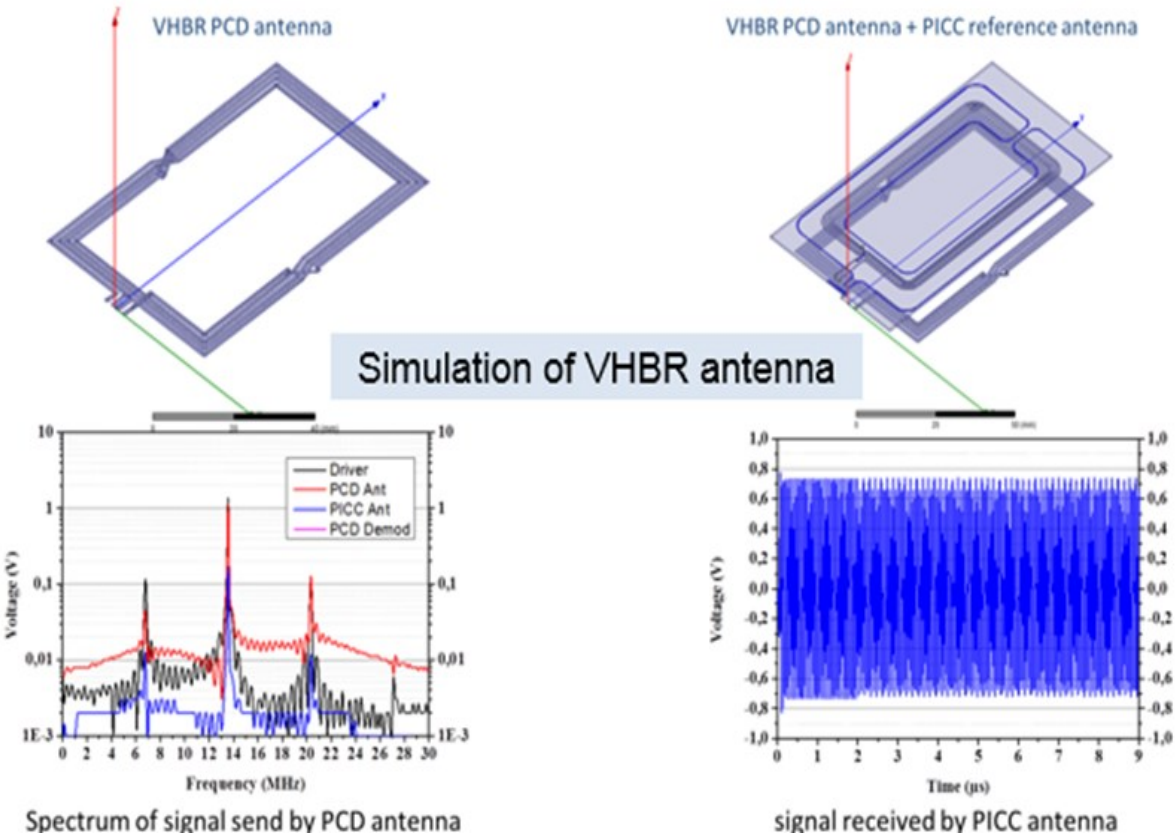
- **Tâche 3:** Développement de lecteur sans contact sécurisé
  - **Développent lecteur ASK/PSK VHBR (CEA)**
    - ✓ Pour évaluer le circuit test VHBR (carte)
    - ✓ RF basée sur des composants discrets



Bit rate 10.17Mb/s (3fc/4)

Bit rate 27.12Mb/s (2fc)

- **Simulation d'antennes VHBR (ISEN, Id3, CEA)**



- **Intégration & implémentation du Lecteur (id3)**
  - ✓ Développement d'une plate forme matérielle
    - Incluant l'interface VHBR et un microcontrôleur avec interface USB
    - Développent du logiciel embarqué pour la communication RF / VHBR

Démonstrateur technologique VHBR PSK

Introduction et motivation

Ce démonstrateur technologique a pour but de réaliser la transmission de données en VHBR entre un lecteur et une carte, modulées selon les amendements 3 et 5 de la norme ISO/IEC 14443-2. Ce lien apparaît comme la partie la plus délicate de la norme VHBR puisque le récepteur de la carte doit rester compatible avec les contraintes de coût et de consommation, malgré l'accroissement important du débit (jusqu'à 27 Mbps en modulation de phase, PSK). Du point de vue du projet, ce travail vient en complément des travaux sur la technologie VHBR dans le projet puisque les autres partenaires ont axé leurs travaux sur le lien inverse, entre la carte et le lecteur.

La démonstration envisagée au démarrage du projet était de faire migrer un démonstrateur VHBR existant au CEA-LETI pour la rendre compatible avec les couches basses de la norme ISO/IEC 14-443. Ce démonstrateur, dont des photos sont présentées sur la Figure 13, est un démonstrateur applicatif capable de mettre en œuvre un lien VHBR bidirectionnel pour transférer des fichiers d'imagerie médicale entre un lecteur et une carte. Ce démonstrateur ayant été terminé avant la publication de la norme ISO/IEC 14443, le schéma de modulation est propriétaire et montre des limitations en terme de débit atteignable ; cela justifie l'objectif du CEA-LETI de concevoir un circuit VHBR respectant le standard et mettre à jour ce démonstrateur initial en y intégrant le circuit fait dans NewP@ss.

Figure 13: Démonstrateur du CEA-LETI au démarrage du projet

Ces plans ont été modifiés car nous avons malheureusement dû repousser la phase de fabrication du circuit pour plusieurs raisons. En particulier, les spécifications définitives de la norme ont été publiées après le démarrage du projet et nous avons préféré attendre qu'elles soient figées pour démarrer le travail. Nous avons par ailleurs sous-estimé la durée nécessaire à mettre au point l'architecture du récepteur. Nous avons dû en effet revisiter l'état de l'art des récepteurs VHBR qui reposent sur un comparateur de phase car ce dernier s'est avérée d'une part incompatible avec l'approche bi mode (modulation de phase ou d'amplitude) que nous avons adoptée et d'autre part incapable de fournir un signal exploitable pour les algorithmes que nous avons choisis.

Pour ce circuit, nous avons développé un frontal analogique en quadrature original que nous avons breveté. Enfin, pour des raisons de rationalisation des coûts d'accès à la technologie TSMC CMOS, nous avons modifié notre choix initial d'une technologie CMOS 40 nm en CMOS 65 nm, repoussant la date d'envoi en fonderie au 14 Octobre 2015.

Description du démonstrateur technologique

Le démonstrateur technologique regroupe les travaux faits sur :

- la conception du circuit de réception VHBR pour la carte (décrit ci-dessous)
- la carte d'émission développée dans le sous-projet 3. Testée dans le sous-projet 5, cette carte d'émission joue le rôle d'un outil de test pour le circuit de réception en émulant le lecteur. Elle est capable d'émettre des paquets de données formatés et modulés selon les spécifications des amendements 3 et 5 de la norme ISO/IEC 14443-3, soit en modulation de phase ou d'amplitude.

Les spécifications du circuit de réception VHBR pour la carte sont regroupées dans le tableau ci-dessous :

	Spécifications		
	Implémentation ou valeur min	Valeur max.	Commentaires
Modulation de phase, PSK (Mbps)	10.17	27.12	
Modulation d'amplitude, ASK (Mbps)	1.7	6.78	
Implémentation couches supérieures VHBR	Non (ASK, PSK)		
Taille du circuit	3.4 mm²		
Objectif de consommation du circuit (mA)	0.5		Spécifications du circuit de récupération de puissance
Technologie	TSMC 65 nm		
Boitier	QFN 48		

Le circuit est un récepteur analogique et numérique (architecture mixte) capable de recevoir des paquets d'un lecteur modulés en ASK ou PSK. Puisque ce travail est très exploratoire, une très grande place du circuit a été accordée au test des fonctions unitaires de la chaine de traitement. Il est important de noter que si la partie analogique est compatible avec les 2 modulations, la partie numérique a été réalisée pour traiter des signaux modulés en phase uniquement. Les traitements pour la modulation ASK étant plus simples, nous avons choisi de les omettre dans la conception.

Le frontal analogique est un récepteur en quadrature innovant, permettant une consommation très réduite, pour lequel le CEA a fait deux demandes de brevets. Il produit des échantillons numérisés qui sont traités par la partie numérique, elle-même organisée autour d'une mémoire partagée pour pouvoir faire traiter séquentiellement les échantillons reçus. L'architecture du circuit est présentée sur la Figure 14.

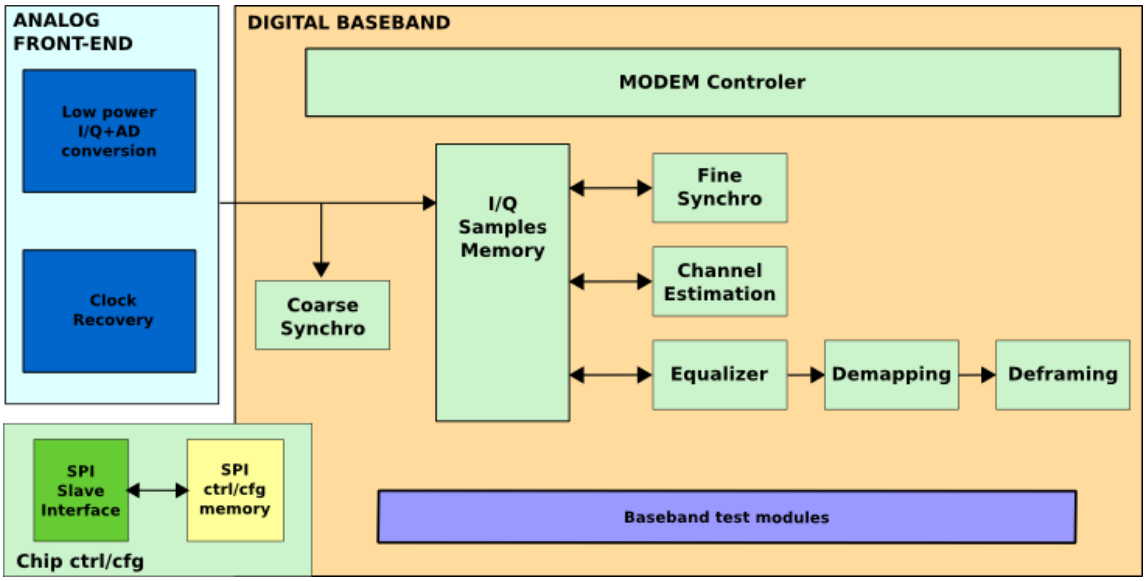


Figure 14: Architecture mixte du récepteur VHBR

Le circuit a été envoyé en fonderie chez TSMC par le biais d'Europractice à la date du 14 Octobre 2015. C'est un circuit de 3.4 mm² dont le padring est composé de 60 pads et il a été conçu pour pouvoir utiliser un boitier de test de type QFN à 48 pins. Le layout du circuit est présenté sur la Figure 15 et le schéma de bonding sur la Figure 16. Comme c'est un circuit très exploratoire, ce circuit doit pouvoir être testé de manière intensive pour valider chacun de ses blocs. Plus de la moitié de la surface est ainsi dédiée aux modules et interfaces de test ; la partie analogique représentant un tiers de la surface et la partie numérique moins de 10 %.

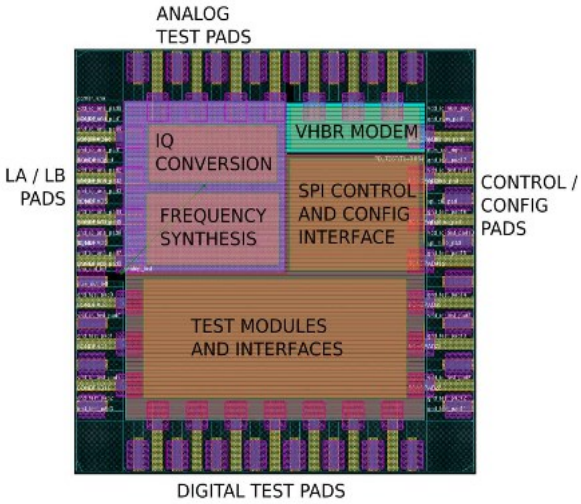


Figure 15: Layout du circuit VHBR envoyé en fonderie

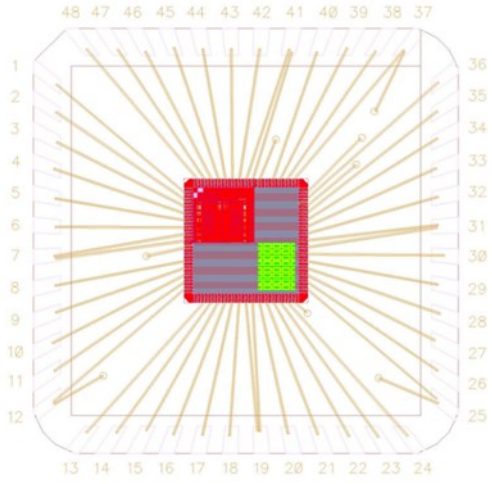


Figure 16: Schéma de bonding du circuit VHBR

Les travaux liés à la carte de test ont débuté en Octobre 2016, de manière à pouvoir tester le circuit quand il reviendra de fonderie (date estimée deuxième quinzaine de décembre).

Démonstration de VHBR sur la nouvelle génération de MCU

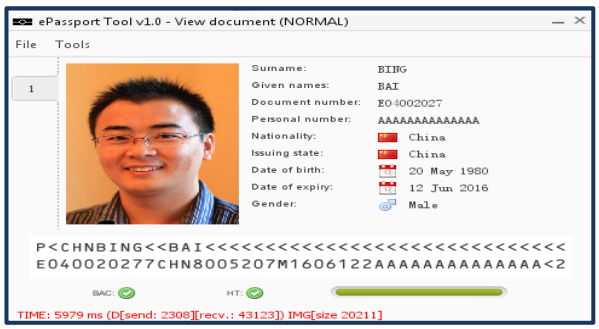
Description générale:

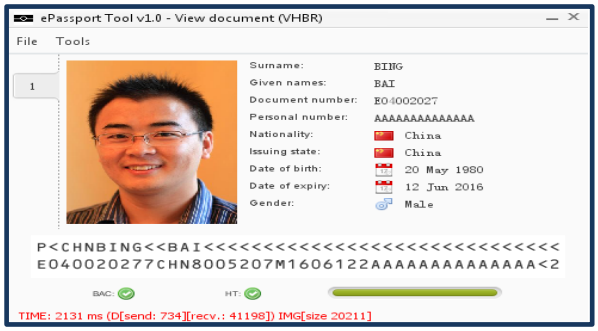
ST a développé un premier MCU sécurisé pour les applications de passeport électronique 3G avec les principales capacités pour le 4G. Ce composant inclus :

- un CPU 32 bit sécurisé, 480 KOctets Page Flash NVM, compatible CC EAL6+
- une horloge interne à 28Mhz (sélection automatique de fréquence pour consommation)
- une interface sans contact:
  - ISO/IEC 14443 (type A & B) et ISO/IEC 18092 (Détection automatique de RF)
  - Transfer Haut Débit (VHBR): ASK testé jusqu'à 3.4 Mbps (Rx) & 6.8 Mbps (Tx)

Démonstration

La démonstration prévoit la lecture des données du passeport (comme lors d'un contrôle) avec la communication standard et avec la communication VHBR en utilisant le composant développé dans le cadre du projet NewP@ss intégré dans le format passeport et un lecteur (d'un partenaire asiatique de ST).





Temps actuel:
5.98 secondes

Temps VHBR:
2.13 secondes

Les résultats montrent un gain du temps total d'un facteur 3 pour la lecture des données.

Démonstration d'affichage du code CAN

Description générale:

L'intégration d'un clavier ou d'un afficheur dans une carte ou un document d'identité électronique est couteuse et complexe. Les composants utilisés doivent répondre aux critères de flexibilité, de fiabilité et de durée de vie de la carte ou du document. Dans quelques cas d'usage, en particulier pour le passeport électronique un afficheur complet ne semble pas nécessaire.
En fait, la connaissance du "Card Access Number" (CAN) ou de la "Machine Readable Zone" (MRZ) d'un passeport pourrait être utilisée pour suivre à la trace le porteur. Le CAN et la MRZ doivent donc être traités comme des informations confidentielles et protégés contre des lectures non autorisées. Au lieu d'utiliser un afficheur, une solution alternative pour protéger certaine informations imprimées sur la carte ou le document peut être utilisée ; l'idée de base est d'utiliser un matériau qui devient transparent lorsque éclairé par une LED placée dans le corps de carte ou de document. Cette LED serai alimenté par le champ électrique d'un lecteur.

Concept:

Une LED est placée à l'intérieur de la carte ou du document électronique dans un feuillet transparent qui agit comme un guide pour distribuer la lumière horizontalement dans la carte ou le document. Ce feuillet et la LED sont placés entre deux couches de matériau opaque de telle sorte que la LED ne soit pas visible. Quand la LED est éteinte, seuil l'impression à la surface de la carte est visible. Quand la LED est allumée, le changement de couleur et de luminosité est bien visible, et permet de révéler des caractères cachés.

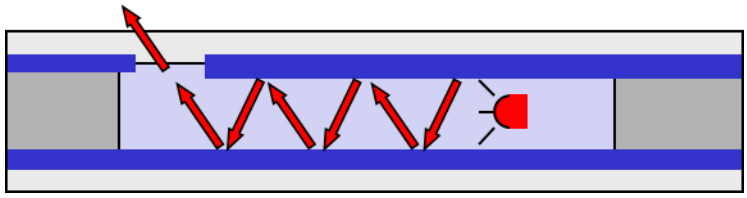


Figure 17 – Coupe de la carte/document à LED intégrée

Cas d'usage:

Dans le cadre du projet NewP@ss un prototype de carte a été développé. Ce prototype intègre en caractères cachés le code CAN dans une carte d'identité. Quand la carte entre dans le champ électrique d'un lecteur, l'énergie reçue permet d'allumer la LED, ce qui rend la surface de la carte transparente et révèle donc le code CAN.

Figure 18 – Carte à LED, révélant le code CAN par illuminations

Figure 19 – Carte avec LED éteinte / allumée

Démonstration d'authentification à base de geste

Description générale:

NXP a étudié et développé une solution de matrice de capteurs capacitifs qui peuvent s'intégrer dans le corps d'un carte ou d'un passeport, sr le même support que l'antenne de communication. Une telle technologie peut être utile pour autoriser la vérification de futurs passeports électroniques à l'aide de smartphones NFC.

Comme la lecture de la zone MRZ ne peut être assurée dans ce cas, les informations nécessaires pour établir la communication sécurisée (numéro du document, date de naissance…) doivent être saisies manuellement avec des risques d'erreurs. Cette technologie peut être une solution alternative.

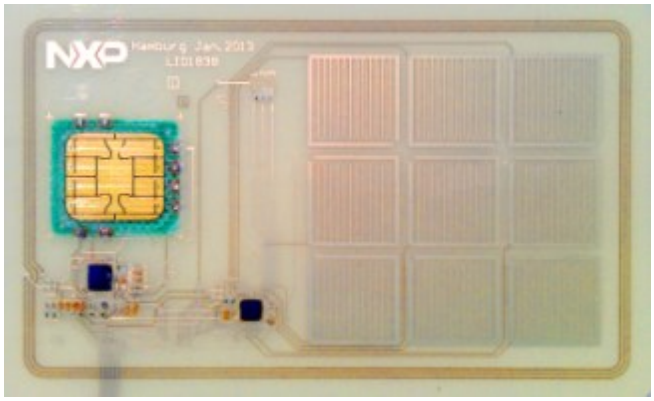
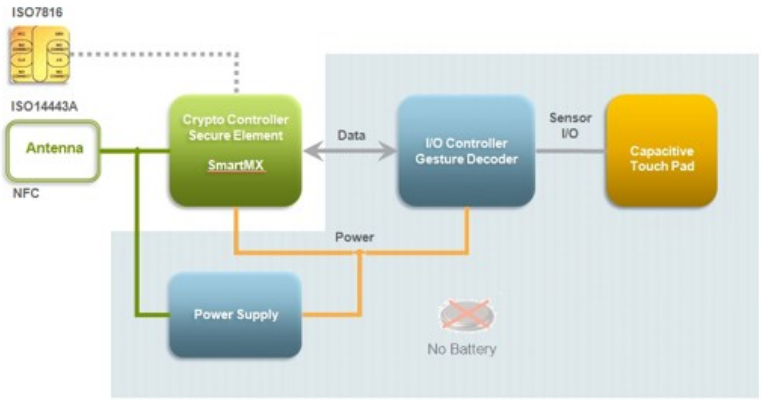


Figure 20 – Carte avec matrice de capteurs capacitifs

Architecture:

Un microcontrôleur sécurisé standard comme ceux utilisés, dans les passeports, n'ont pas assez d'entrées sorties pour supporter une matrice de capteurs capacitifs. Un petit MCU générique (sans sécurité particulière) est donc nécessaire, ainsi que quelques composants passifs standards, pour évaluer les signaux des capteurs capacitifs.



Il a été démontré, au cours du projet, que le fonctionnement sans contact est également possible en dépit du bilan de puissance en plus exigeant, car l'énergie récupérée à partir du champ électromagnétique ISO 14443 doit maintenant alimenter à la fois le microprocesseur sécurisé et le microcontrôleur secondaire.

De la même manière, cette technologie peut être intégrée avec l'antenne dans la couverture du passeport électronique. La matrice de capteurs est couverte par la couche imprimée du document, certaines marques devraient être incluses dans la conception graphique du passeport électronique pour visualiser la zone de capteurs. Le réseau de capteurs capacitifs ne serait utilisé que pour une inspection mobile quand les capacités d'OCR ne sont pas disponibles.

Démonstrateur de lecteur VHBR (Id3)

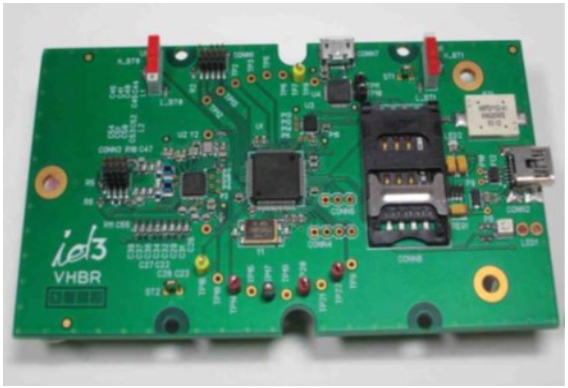
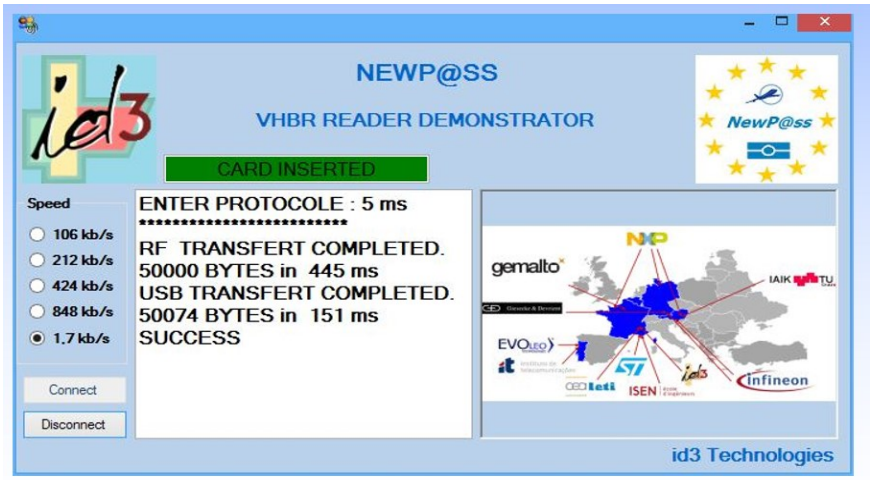


Figure 21: Lecteur VHBR Id3

Figure 22: Carte VHBR Infineon

Cas d'usage

- Détection de la présence d'une carte sans contact
- Téléchargement de 50Koctet de données et affichage
- Mesure des temps de transfert



Conclusion

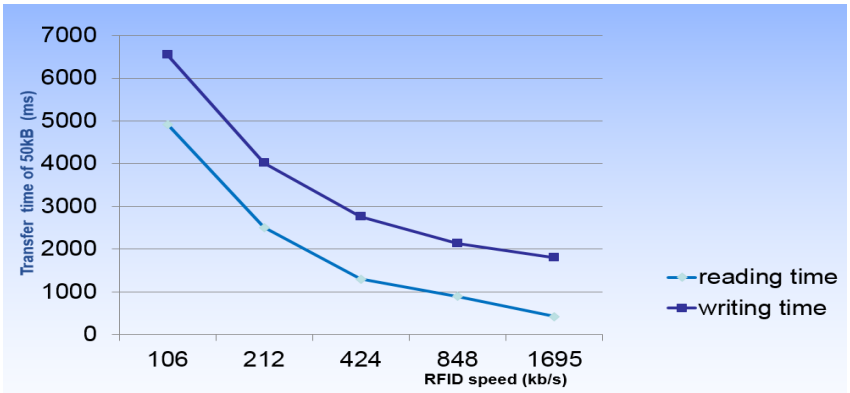


Figure 23: Performances du lecteur VHBR – Temps de transfert vs. débit

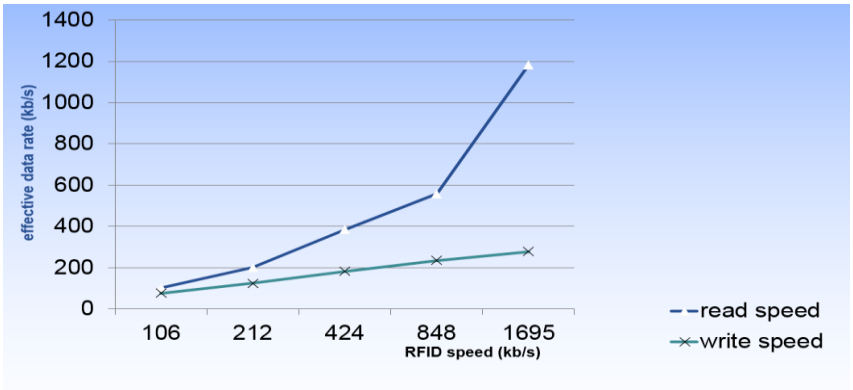


Figure 24 : Performances du lecteur VHBR : Taux de transfert effectifs

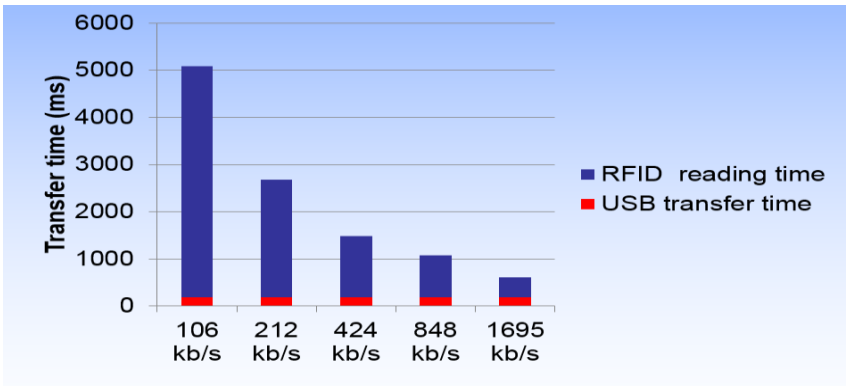
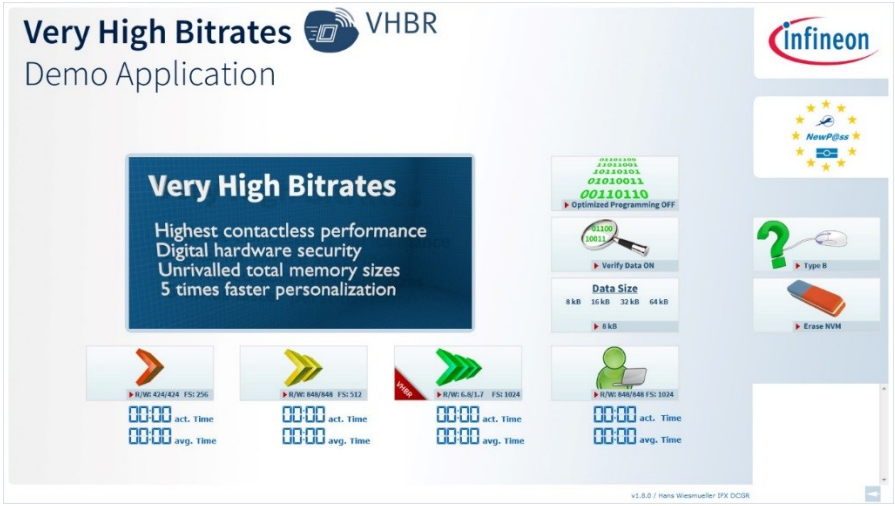


Figure 25: Performances du lecteur VHBR : Répartition des temps de transfert (lecture de 5OKo)

- Amélioration du débit : les temps de transfert varient d'un facteur 10 entre 106Kb/S et 1.7 Mb/s
- Limitations : la démonstration est peu réaliste car un transfert d'un large volume de données implique souvent des traitements cryptographiques coté lecteur et coté carte/document, qui limitent les performances.

Démonstration d'application VHBR



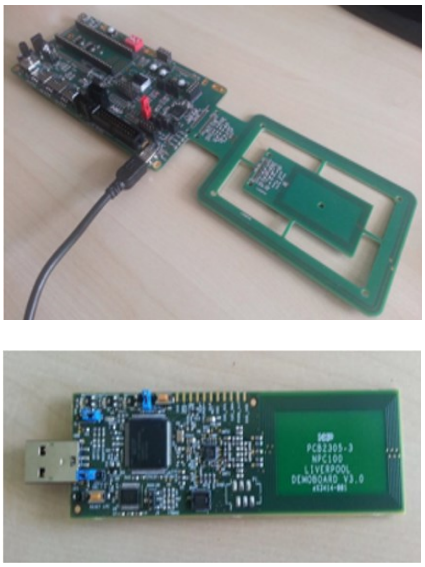
La norme VHBR autorise des vitesses de communication pour les passeports et autre documents d'identité électroniques qui permettent le transfert de large volume de données comme nécessaire pour les futures

applications.

Avec le standard ICAO LDS2.0 en cours de définition, des champs de données additionnels tels que les visa électronique ou les tampons d'horodatage devraient faire partie de la transmission aux points de contrôle.

Le démonstrateur présente une accélération d'un facteur 8 et plus par rapport aux passeports actuels, et réduit aussi les temps de latence par utilisation de trames de données plus grandes.

Démonstrateur de lecteur VHBR (NXP-F)



Hardware : NXP-F VHBR Reader

Software : GoldenReader execution

Ce démonstrateur est équipé d'un contrôleur NFC de NXP destiné aux lecteurs avec ou sans contacts. A l'aide des multiples interfaces, il est possible de tester les fonctionnalités matérielles et logicielles de composant. La présence de deux antennes de tailles différentes pour s'adapter à divers environnements de test.

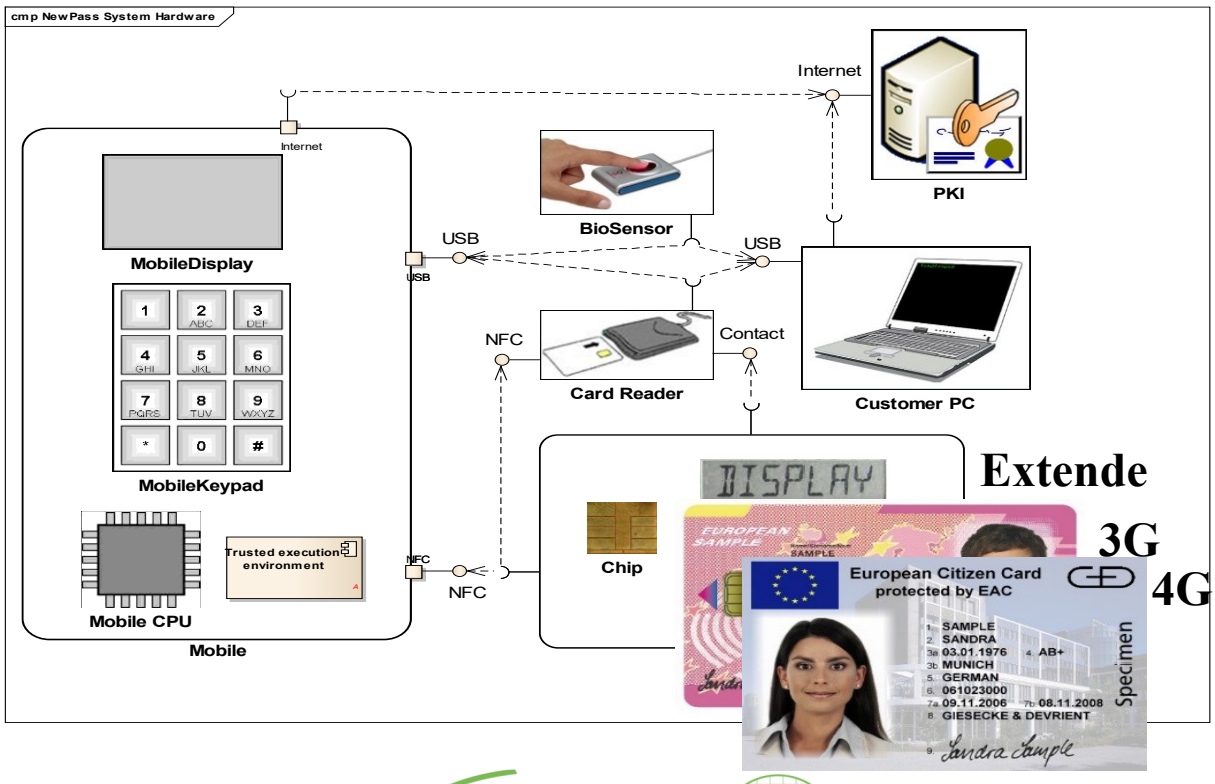
6.4. SP4 – Développement plate forme logicielle

6.4.1. Introduction

Coordinateur	**Giesecke & Devrient**
Partenaires	Gemalto, STM, id3, G&D, EVO, IT, NXP-F, NXP-G, IFX-G IFX-A, SIC
Objectifs du sous-projet	L'objectif de ce sous-projet est le développement du logiciel embarqué (en se basant sur la technologie e-passport actuelle et sur le nouvel LDS2). Les fonctions basiques nécessaires pour les e-passport de troisième et quatrième génération seront implémentées. Un soin particulier sera apporté afin de conserver une structure logicielle permettant une interopérabilité complète de toutes les plate formes visées (au niveau applicatif) et de s'assurer de la capacité de la plate forme à fonctionner en mode multi-applications. Ce sous-projet couvre également les aspects nécessaires au développement de logiciel « off-card » tel que le logiciel du lecteur ou des infrastructures PKI.

Ce sous-projet est divisé en quatre tâches :

- **Tâche 1** : Briques logicielles de base *(algorithmes biométriques, développement des primitives cryptographiques basiques et des piles de protocole, http sans contact, modules du lecteur NFC)*
- **Tâche 2 :** Développement du logiciel embarqué sur la carte *(Implémentations des plate formes 3G et 4G, Système d'exploitation Multi-thread adapté au passeport électronique pour des applications multiples)*
- **Tâche 3** : Middleware hors carte *(Logiciel embarqué dans le lecteur, infrastructure gérant les accréditations, intégration appareils mobiles)*
- **Tâche 4** : Personnalisation renforcée *(pré-personnalisation des cartes à base de wafer et personnalisation de l'application, personnalisation après déploiement)*



6.4.2. Activités par périodes et partenaires

2012:

Gemalto
Gemalto a travaillé sue la tâche 4.1 et développer les protocoles cryptographiques sur les courbes elliptiques, incluant SAC et EACv210.

NXP-France
NXP France a travaillé à la définition des spécifications du logiciel embarqué du lecteur. Cela inclut le découpage fonctionnel des différentes fonctions du firmware et la description structurelle des sous-systèmes firmware.

Id3
Id3 a commencé des recherches bibliographiques sur la reconnaissance de l'iris et commence à évaluer diverses solutions techniques : traitement de l'image de l'iris, correspondance de l'iris.

Giesecke & Devrient
G&D a commencé la définition de l'architecture système pour les plate formes passeport électronique afin qu'elles supportent les cas d'usage 3G et 4G. L'implémentation du protocole de la plate forme 3G (SAC support) a commencé. Toutes les activités relatives aux passeports sont synchronisées avec les activités internationales de normalisation au sein de ISO/IEC JTC 1 SC17 et GlobalPlatform.
La définition de l'architecture du système pour les appareils mobiles garantissant des entrée/sorties sécurisées a commencé.

Infineon
IFX+IFAT ont contribué au SP4 pendant la réunion de kick-off et les sessions de travail du SP4. La re-planification et les ressources ont été planifiées en interne pour préparer la revue des spécifications SW D4.4 du T4.2.

NXP-Germany
Pour la tâche 1, la modélisation du système a commencé avec pour objectif l'optimisation du firmware et du software des composants pour leur utilisation dans des appareils mobiles en incluant la fonction NFC. Dans ce domaine, il y a un potentiel important d'amélioration du débit de données.
Pour la tâche 2, les activités se sont concentrées sur les mécanismes de personnalisation. Pour les plates formes futures intégrant de la mémoire flash pour les données et le code, des changements et une extension du modèle de cycle de vie pour le logiciel embarqué sont requis. Cela affecte également les mécanismes d'authentification pendant la production. Jusqu'à présent, les modèles pour les transitions de plusieurs états en production et l'administration de clés et de cryptogrammes individuels ont été investigués.

Evoleo
Evoleo a analysé l'état de l'art de l'infrastructure de gestion de la cryptographie, des protocoles et des identifiants devant être utilisés avec la plate forme Newp@ss.

IT
Une étude préliminaire de la littérature a commencé sur l'état de l'art concernant la cryptographie basique et les piles protocolaires, ainsi que les concepts d'infrastructure appliqués à la nouvelle génération de passeports devant être utilisés dans Newp@ss.

2013:

Gemalto
Gemalto a finalisé sa contribution sur la tâche T4.1 (Basic SW bricks) en participant à l'écriture du livrable D4.1 (Basic SW bricks specification). Cette contribution inclut la description complète des protocoles cryptographiques spécifiques à la 3G et 4G : SAC, EACv210 partielle et EACv210 complète, incluant les versions à venir des protocoles CAv2 and TAv2 d'authentification circuit et d'authentification du terminal. Gemalto continue son travail sur les livrables D4.2 et D4.3.

NXP-France
NXP France a finalisé les spécifications du logiciel embarqué du lecteur IC. Cela inclut le découpage fonctionnel des différentes fonctions du firmware et la description structurelle des sous-systèmes firmware.

Id3
ID3 a continué son travail sur la standardisation des briques logicielles biométriques. Plus particulièrement, le standard BIOAPI a été étudié.
Id3 a commencé un travail de recherche sur la reconnaissance biométrique multimodale (reconnaissance faciale et empreinte digitale).
Pendant le deuxième semestre, Id3 a décrit au sein du document D4.1 sa contribution concernant les briques logicielles disponibles pour la reconnaissance biométrique. En parallèle, Id3 continue ses recherches sur la reconnaissance faciale : un premier prototype d'algorithmes, basé sur des technologies d'apprentissage machine, montre la reconnaissance un à un. Les études se concentrent sur tous les aspects du traitement de l'image faciale : alignement, normalisation, mesure de la différence par rapport à un modèle.

Giesecke & Devrient (WP coordinateur)
G&D a fourni un modèle d'architecture système pour les plates formes passeport électronique afin de supporter les cas d'usage 3G et 4G. De plus, G&D a fourni les spécifications des briques logicielles pour les algorithmes cryptographiques (partie du livrable D4.1). L'implémentation du protocole de la plate forme 3G (SAC support) a été achevée. L'implémentation de la plate forme 4G, basée sur le protocole EAC V2 a été commencée. Toutes les activités relatives aux passeports sont synchronisées avec les activités internationales de normalisation au sein de ISO/IEC JTC 1 SC17 et GlobalPlatform.
La définition de l'architecture du système pour les appareils mobiles garantissant des entrée/sorties sécurisées a continué.
Les premiers démonstrateurs pour la plate forme du passeport 3G sont disponibles.

NXP-Germany
Les tâches ont bien progressé et continuent à être exécutées selon le plan. Les options d'implémentation du protocole HTTP ont été investiguées. Les critères et les conditions aux limites pour l'usage de téléphones mobiles NFC pour l'inspection des passeports 3G et 4G ont été formulés et cela a conduit à de premiers résultats.

Infineon
Aucune activité importante sur cette période

Evoleo
Evoleo a analysé l'état de l'art de la cryptographie et des protocoles devant être utilisés pour Newp@ss.
Le middleware hors-carte, sur le lecteur et le système de gestion des identités sont les sujets en cours de développement.

IT
Une étude a été menée sur l'état de l'art concernant la cryptographie basique (courbe elliptique), les piles de protocoles (systèmes sur et hors carte), les concepts PKI (Public Key Infrastructure) appliqués à la nouvelle génération de passeports, devant être utilisés dans Newp@ss.
IT travaille actuellement sur la définition du software en lien avec l'ordinateur hôte et sur l'intégration de plusieurs périphériques, tels que le lecteur de cartes et les capteurs biométriques. IT travaille également sur les interfaces entre l'ordinateur hôte et le KPI ainsi que les mécanismes gérant les méthodes et protocoles de sécurité.

2014:

Giesecke & Devrient (SP coordinateur)
G&D a édité les documents D4.2 et D4.3.
Les contributions suivantes ont été fournies par G&D :

- 3G chipcard platform
- Extended chipcard platform
- Java Card
- Mobile Platform (Trusted Execution Environment, Open Mobile API)

L'implémentation du protocole de la plate forme 4G (EAC V2 support) a été achevée. L'application 3G est disponible. Les activités pour l'application 4G ont commencé. Les premiers prototypes de plate forme 4G ont été montrés en décembre lors de la revue Catrene.
Toutes les activités relatives aux passeports sont synchronisées avec les activités internationales de normalisation au sein de ISO/IEC JTC 1 SC17 et GlobalPlatform.
Une carte de développement d'une plate forme mobile pour les activités « secure mGovernment » utilisant l'environnement TEE (Trusted Execution Environment) a été sélectionnée et les activités de développement de l'implémentation PACE ont commencé. Des études au sujet de la personnalisation post-délivrance ont bien progressé. Les premiers résultats ont été documentés dans un premier jet du document D4.9.

Gemalto
Gemalto a contribué à l'écriture des livrables D4.1 et D4.2. Cela comprend la description des composants et des applications 4G ainsi qu'une description détaillée du système d'exploitation Multi-application, incluant les cartes, les protocoles de communication, les protocoles de cryptographie, le gestionnaire de mémoire et les drivers. Gemalto a travaillé sur les tâches suivantes :

- **Tâche 1 :** La description et le développement des primitives basiques de cryptographie et des piles de protocoles sont faits
- **Tâche 2 :** Les applications 3G ont été implémentées et démontrées et les applications 4G ont été spécifiées et le premier prototype a été montré. La spécification et l'implémentation du système d'exploitation multi-applications est également prêt.
- **Tâche 4 :** Des investigations et l'implémentation du concept de pré-personnalisation des wafers ont été menées. Des investigations concernant la personnalisation après émission des passeports sont également en cours. Le travail concernant les livrables D4.8 et D4.9 est en cours pour une livraison en T1/2015

NXP-France
NXP France a travaillé sur le lecteur de carte et le logiciel embarqué du circuit IC, gardant en mémoire les recommandations du NFC Forum concernant les contraintes et les standards à respecter.

ID3

Dans ce sous-projet, Id3 a mené deux actions :

- Des recherches sur la biométrie multimodale
- Le développement d'un logiciel embarqué pour le lecteur VHBR.

Concernant les activités biométriques, Id3 s'est concentré sur le portage des algorithmes de reconnaissance faciale pour des systèmes Android. Une application de reconnaissance faciale vient d'être livrée par Id3 et fonctionne sur tablette et smartphone.
Concernant le développement du logiciel VHBR, cette activité vient juste de commencer. L'étude concerne le développement du logiciel embarqué pour un prototype de lecteur VHBR. A terme, ce logiciel dédié au microcontrôleur du lecteur prendra en charge les principaux protocoles RFID, incluant le VHBR.

IFX / IFAT

IFX a contribué au livrable D4.2 (on-card SW specifications) en décrivant les circuits 3G et 4G et en estimant la taille mémoire nécessaire pour les fonctions LDS2.0 eVisa et eStamps.
IFAT a commencé une analyse de l'impact hardware basée sur les propositions de protocoles de préservation de la vie privée tel que recherchés par TUG-IAIK, qui vise les générations de passeports électroniques et e-ID après 4G.
Cette analyse de l'impact hardware prend en compte les contraintes dérivées à partir d'algorithmes et de protocoles « pairing-based ».

NXP-Germany

Le travail de préparation pour l'évaluation des mécanismes de personnalisation a commencé pendant cette période. L'expérience acquise pendant la production de générations de passeports électroniques présents et passés a été utilisée pour déduire les paramètres les mieux adapté aux circuits 3G et 4G. L'objectif est de définir les paramètres qui permettront une pré-personnalisation spécifiquement pour les passeports électroniques 4G.

Evoleo

Evoleo a analysé l'état de l'art des piles de protocoles cryptographiques devant être utilisé dans Newp@ss.
Le middleware hors-carte, sur le lecteur et la spécification du système de gestion des identités ont été réalisés en se concentrant sur le système Newp@ss avec un PC hôte. L'interface et les drivers pour le lecteur de cartes et les capteurs biométriques ainsi que le PKI ont été mis en avant. L'application principale du PC hôte et l'utilisateur s'interfacent facilement.
Les outils sont écrits en Java et utilisent Javascript. L'accès à la carte à puce est fourni au travers d'une version améliorée d' »OpenCard Framework ». Les pilotes sont inclus pour la plupart des cartes à puce ISO 7816-4, des lecteurs de cartes PC/SC et CT-API. La plate forme fournit le support cryptographique complet utilisé communément par les cartes à puce.
OpenSCDP est l'outil utilisé dans les projets cartes majeurs et par un grand nombre de compagnies tierces dans leurs produits respectifs.
Au deuxième semestre, le développement s'est concentré sur la technologie OpenSCDP pour créer une brique logicielle écrite en Java pour l'outil du lecteur. Cela a consisté à implémenter puis à intégrer deux composants.
L'émulation du passeport électronique est également un sujet investigué et développé pour ajouter plus de possibilités de démonstrations du software.

IT

Un middleware hors-carte pour le lecteur et la technologie PKI ont été définies, implémentées et intégrées.
Ce développement a été fait sous Open Smart Card Develop Platform (OSCDP), basé sur du Java et adressant :

l'authentification et les processus d'autorisation PKI (ex : EACv2, authentification passive) ; génération de certificat : PKD ; GUI pour les systèmes d'inspection. Pour cela, IT a également identifié des briques logicielles potentiellement en relation avec le PKI pour un usage dans une prochaine génération de passeport électronique.
IT a également travaillé sur l'interface entre l'ordinateur hôte et le PKI, ainsi que sur les mécanismes pour gérer les protocoles et les mécanismes de sécurité, en suivant le plan décrit dans les livrables D4.1 et D4.3.
De plus, IT travaille sur les aspects du « Universal Reader Tool » enlien avec le PKI, qui peut être developpé en utilisant OpenSCDP.
Le nouveau PKI pour le passeport électronique 4G a été développé et proposé. Le modèle de PKI actuel doit d'abord être adapté pour se conformer avec la technologie 3G, bien que de tels changements n'affecteront pas les passeports électroniques actuels (2G).
Le nouveau PKI pourra fournir l'authentification pour les nouvelles fonctions du passeport électronique 4G, telle que l'écriture des tampons des douanes et des visas électroniques sur les passeports électroniques.

2015:

Giesecke & Devrient (WP coordinateur)
En 2015, G&D a finalisé la plate forme pour le passeport 4G et l'application faisant partie du développement logiciel sur carte (D4.6). G&D a également finalisé diverses activités du D4.7.
Toutes les activités relatives aux passeports sont synchronisées avec les activités internationales de normalisation au sein de ISO/IEC JTC 1 SC17 et GlobalPlatform.
De plus, G&D a coordonné et contribué au travail de personnalisation post-délivrance du document (D4.9), activité terminée en T1/2015.

Gemalto
Gemalto a terminé l'écriture des chapitres qui lui étaient attribués : D4.1 (Basic SW bricks specifications), D4.2 (On-card SW specifications) and D4.3 (off-card middleware SW specification). Gémalto a également implémenté les plates formes et applications 3G et 4G (faisant partie du D4.6).
Gemalto a coordonné et finalisé le travail du livrable D4.8 (Wafer Personalization Concept) et a contrbué au livrable D4.9 (Post Issuance Personalization).

NXP-France
NXP France a continué son travail sur le lecteur de carte et le logiciel embarqué du circuit IC, gardant en mémoire les recommandations du NFC Forum concernant les contraintes et les standards à respecter.

ID3
ID3 a continué à travailler sur deux actions commencées l'année précédente :

- Des recherches sur la biométrie multimodale
- Le développement d'un logiciel embarqué pour le lecteur VHBR.

Concernant les activités biométriques, Id3 s'est concentré sur le portage des algorithmes de reconnaissance faciale pour des systèmes Android. Concernant la reconnaissance des empreintes digitales, Id3 a maintenu ses activités de recherche. De nouveaux algorithmes ont été étudiés pour améliorer l'interopérabilité, la vitesse et la précision de la reconnaissance.
Concernant le développement du logiciel VHBR, l'activité continue. Une première livraison du logiciel VHBR a été faite et permet une communication à une vitesse allant jusqu'à 1.7 Mbits/s.

IFX / IFAT

Aucun rapport d'activité fait pour cette période H1/2015

NXP-Germany
NXP-Germany a contribué au livrable D4.8 "Wafer personalization concept" ainsi qu'au livrable D4.9 "Post-issuance personalization". Des activités de clôture de ce sous-projet ont également été menées.

Evoleo
Au premier semestre 2015, les briques software pour le système d'inspection et le simulateur ePP ont été développées et testées. Les technologies utilisées étaient basées sur les technologies Java et openSCDP. Le logiciel IS a pu être intégré et interagir avec l'infrastructure PKI, le simulateur ePP et les échantillons 4G ePP de Gemalto.
Le simulateur ePP peut simuler les passeports électroniques 3G et 4G, tout en permettant de recréer différents scénarios de protocoles de communication sécurisée et de structures de données LDS.

IT
IT a développé le "TS Signer PKI". IT a travaillé sur le mécanisme permettant d'apposer des tampons et sur les interfaces de connexions entre l'IS et le PKI. IT a développé le mécanisme de sécurité pour la connexion SSL ainsi que la page web pour TS-Signer. IT a également développé le mécanisme pour générer la chaine de certificat et la fonction test pour TS-Signer.

6.4.3. Coopération

- **Dans le sous-projet**
  - Une bonne coopération a eu lieu avec de bonnes contributions reçues de tous les partenaires.
  - Les réunions du SP4 ont eu lieu aux dates suivantes pendant la période couverte par ce rapport:
    - 12 Novembre 2012, Munich: Méthode de travail, coopération, contributions de chaque partenaire
    - 15 Janvier 2013, Porto: Adaption du planning des fournitures
  - Des groupes de travail ont été organisés en parallèle des réunions du consortium
  - Des modèles de documents pour les spécifications logicielles des fournitures D4.x ont été proposés et approuvés par les partenaires
  - Une forte coopération a eu lieu entre tous les partenaires du sous-projet pour finaliser les fournitures D4.2 et D4.3 dans les temps.
  - Plusieurs réunions et conférences téléphoniques ont eu lieu
  - Une répartition des rôles entre GTO, G&D, NXP-G and NXP-F pour les fournitures D4.8/D4.9 a été faite
- **Avec les autres sous-projets**
  - **SP2**: Coopération étroite entre les spécifications logicielles du SP4 (D4.2, D4.3) et les spécifications haut niveau du SP2 (D2.2)
  - **SP5**: Contribution et alignement pour la mise en place de test et implémentation de référence
  - **SP6**: Alignement sur les primitives cryptographiques, protocoles d'authentification et aspects concernant la certification
  - **SP7**: Prise en considération des démonstrateurs et planning des contributions nécessaires
  - **SP8**: Utilisation des résultats pour la standardisation, en particulier pour les standards du passeport électronique 4G (e.g. LDS2, ISO/IEC JTC SC17)

6.4.4. Résultats obtenus

Fournitures:

Fourniture	Tâche	Date prévues (CR #2)	Date livraison	Type et Contenu
D4.1	T4.1	T4 13	T4 13 livré	Spécifications des briques logicielles de base
D4.2	T4.2	T1 14	T2 14 livré	Spécifications logicielles sur-carte (possible mise à jours à T0+12)
D4.3	T4.3	T1 14	T2 14 livré	Spécifications middleware off-card
D4.4	T4.2	T2 14	T3 14 livré	Revue des specifications logicielles sur-carte en lien avec l'impact materiel
D4.5	T4.1	T2 15	T2 15 livré	Briques logicilles de base disponibles
D4.6	T4.2	T2 15	T2 15 livré	Logiciel sur-carte disponible
D4.7	T4.3	T1 15	T1 15 livré	Logiciel hors-carte disponible
D4.8	T4.4	T1 15	T1 15 livré	Concept de personalisation des plaques
D4.9	T4.4	T1 15	T1 15 livré	Personalisation après fourniture

Résultats clé:

- Toutes les fournitures prévues ont été livrées
  - Différents démonstrateurs en lien avec le SP4 sont disponibles. Ils ont pu démontrer les progrès accomplis dans le sous-projet et ont servi de preuves aux concepts suivants:
    - Démonstrateur LDS-2
    - Utilisation d'un environnement d'exécution digne de confiance pour un lecteur de passeport mobile sécurisé.
    - Communications en mode VHBR entre le lecteur id3 et les cartes sans contact Infineon
    - PKI de Signature numérique au format LDS2 – Signature des enregistrements de voyage en 4G

- **Tâche1: Briques logicielles**
  - Développement, validation et maintenance des protocoles nécessaires basés sur la cryptographie de courbe elliptique (Gemalto, G&D)
  - Travail de recherche sur la reconnaissance biométrique multimodale (Id3)
  - Travail sur la modélisation au niveau système pour l'optimisation de temps de transfert dans les communications à base de NFC vers des microprocesseurs sécurisés (NXP-F)
  - Analyse de l'état de l'art de la cryptographie, couches protocoles et infrastructure de gestion des données d'identification pour l'utilisation des nouvelles générations de passeports électroniques (Evoleo, IT)
  - Identification et implémentation de briques logicielles en lien avec le PKI pour utilisation dans la prochaine génération de passeports électroniques (Evoleo, IT)
  - Implémentation de couche HTTP (NXP-G)
  - Mise à jour de librairie Crypto sur-carte (IFX)
  - Algorithmes biométriques (id3)

- **Tâche 2: Développement de logiciel sur carte**

- Conception et développement pour la mise en place des plates formes multi applicatives basées sur la plate forme JavaCard v2.2.x et JavaCard 3.0.x classic (Gemalto, G&D)
- Le passeport 3G et l'applet ont été mis en place
- La plate forme 4G est prête, une application prototype supportant LDS2 est disponible (G&D)
- Conception et implémentation d'un OS Multi Application OS (Gemalto)
- Routines bas niveau pour la gestion optimisée d'interface sans contact avec VHBR (IFX)

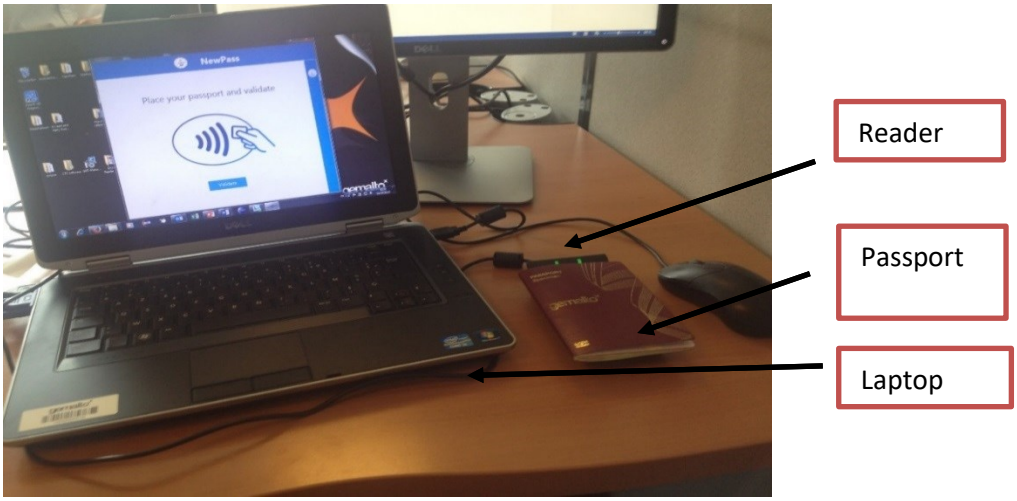
- **Tâche 3: middleware hors carte**
  - Spécifications pour logiciel embarqué associé à la puce du lecteur (NXP)
  - Définition de l'architecture système pour l'utilisation d'appareils portables pour utilisation sécurisées des entrées-sorties et pour des applications egov sécurisées (G&D)
  - Le middleware hors carte pour lecteur ainsi que la technologie PKI ont été conçus et développés.
    - La plate forme OSCDP (Development under Open Smart Card Develop Platform) basée sur le langage de programmation Java adresse:
      - ✓ Les processus PKI d'authentification et d'autorisation (e.g. EACv2, authentification passive)
      - ✓ La génération de certificat
      - ✓ PKD
  - Intégration des briques logicielles et déploiement de PKI LDS2 (IT, Evoleo)
    - Processus d'autorisation PKI
    - Génération de certificat et gestion de signature de documents de voyage
    - Signature de nouvelles données d'enregistrement de voyages par TS-signer, qui est l'entité finale de la signature numérique PKI LDS2.
  - Investigation sur l'utilisation de téléphones portables NFC pour l'inspection des passeports électroniques (NXP-G)
  - Une application de reconnaissance faciale a été délivrée par id3 et tourne sur tablette et smartphone
  - Une première version d'un firmware VHBR a été réalisée et permet la communication jusqu'à 1.7Mbits/s. (id3)
  - L'application PACE-Trusted a été réalisée (G&D)

- **Tâche 4: Personnalisation améliorée**
  - Investigations et implémentations pratiques du concept de pré-personnalisation de plaques (NXP-G)
  - Investigations sur la personnalisation après fourniture (Gemalto).
  - Les livrables relatifs à la personnalisation améliorées ont été fournis (NXP-G, Gemalto, G&D)

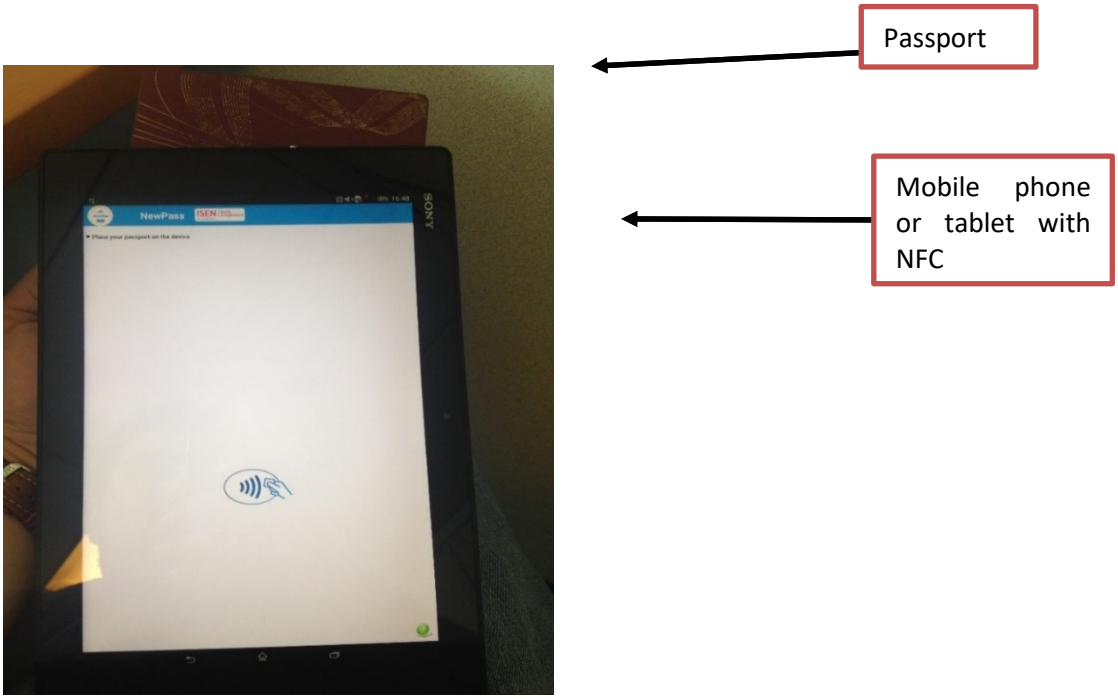
Démonstrateur 4G ePassport "open source" (LDS2 / VHBR)

Description générale

Laptop general architecture:



Laptop general architecture:



Scénario:

- Entrer MRZ ou CAN
- Faire tourner PACE ou BAC
- Lire LDS1
- Lire LDS2
- Imprimer l'information et le temps de lecture

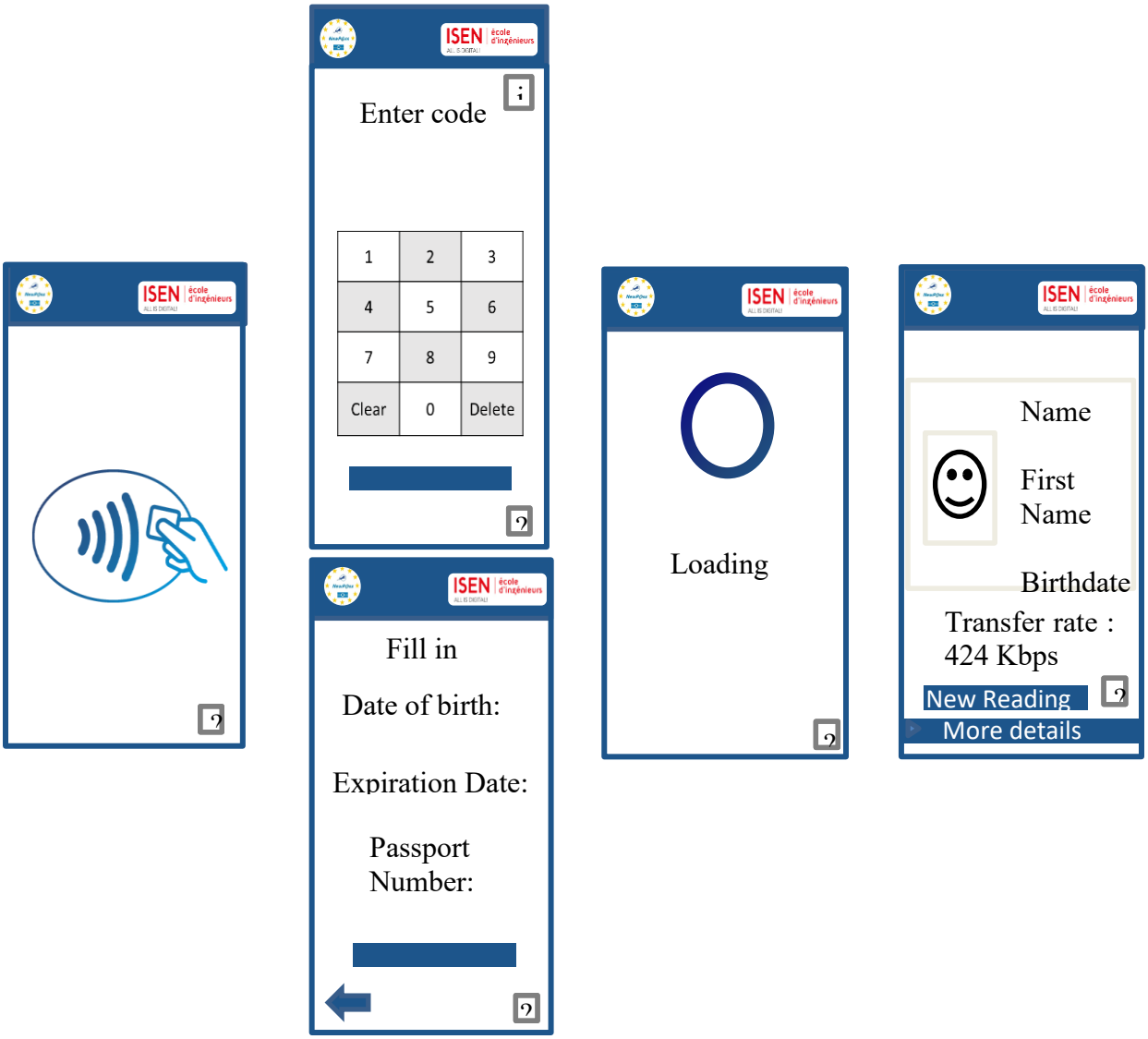


Figure 24 - Application scenario

Caractéristiques techniques

Matériel:

- Clavier standard et écran
- Lecteur sans fil compatible PC/SC compatible et ISO14443 Types A et B
- PC, tournant sur Windows XP ou Windows 7

Logiciel:

- Pilotes pour le lecteur

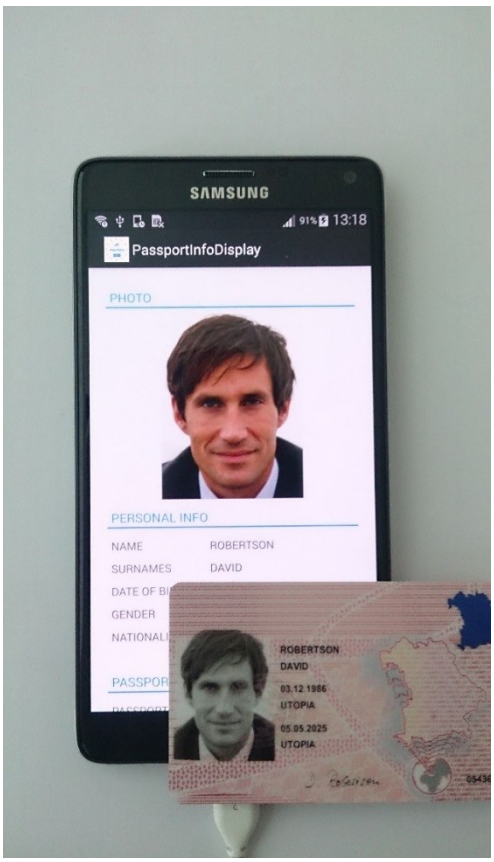
Autres:

- Clés et certificats nécessaires pour une transaction EAC
- 4ème génération eMRTD, supportant SAC, full EACv2, LDSv1 and LDSv2

Démonstrateur TEE-CAN

Description générale

Pour des services eGov, le détenteur de la carte a besoin d'entrer son code pin lui permettant d'accéder à la carte.
Normalement c'est fait en utilisant un lecteur de carte dédié comportant des touches pour rentrer le code pin., Dans un scénario basé sur un smartphone un lecteur de carte n'est pas nécessaire.
A la place, l'environnement d'exécution sécurisé ainsi que l'interface utilisateur sécurisée peuvent être utilisés.
G&D a développé un prototype comme preuve de concept pour le projet NewP@ss.



Démonstrateur PKI LDS2

Description générale

Un citoyen finlandais a assisté à une réunion au Canada et arrive à l'aéroport de Porto au Portugal. Au poste frontière de l'aéroport de Porto, les douaniers doivent vérifier d'abord le dernier enregistrement de voyage inclus dans l'eMRTD. Cet enregistrement est celui qui a été créé à l'aéroport canadien. Ensuite un nouvel enregistrement de voyage est créé et inscrit sur l'eMRTD par le service des douanes de l'aéroport de Porto.

Selon notre scénario l'Etat ayant délivré l'eMRTD est la Finlande, l'Etat ayant signé le dernier enregistrement est le Canada et l'Etat qui accueille et signe le nouvel enregistrement de voyage est le Portugal.
Ainsi pendant les opérations de lecture/écriture, les composants des PKIs LDS2 sont les suivants :

- Le PKI d'autorisation LDS2 finlandais
- Le PKI d'autorisation LDS2 portugais
- Le PKI de signature numérique LDS2 canadien
- Le PKI de signature numérique LDS2 portugais

De plus le service des douanes de l'aéroport de Porto est responsable de la lecture du dernier enregistrement de voyage du eMRTD et de l'écriture du nouvel enregistrement dans l'eMRTD.
Ainsi le service des douanes de l'aéroport de Porto doit interagir directement ou indirectement avec des composants des PKIs LDS2 ci-dessus afin de réaliser les opérations de lecture et d'écriture correctement.

La figure 25 montre le diagramme séquentiel qui présente les interactions entre le service de douane et l'eMRTD finlandais ainsi que les interactions entre le service de douane et les composants requis des PKIs LDS2 ci-dessus pendant les opérations de lecture et d'écriture des enregistrements de voyage depuis/vers l'eMRTD finlandais.

Opération de lecture

Etape 1: L'eMRTD finlandais s'offre au service de douane de l'aéroport de Porto et le protocole SAC, supporté à la fois par l'eMRTD et le service des douanes est alors activé. Le protocole SAC permet de vérifier que le service des douanes est autorisé à accéder aux données stockées (c'est-à-dire le dernier enregistrement de voyage).De plus le protocole SAC permet l'établissement d'un canal sécurisé pour la communication entre l'eMRTD et le service des douanes. (**Procédure d'établissement SAC**)

Etape 2: Le service des douanes à l'aéroport de Porto demande et reçoit le dernier enregistrement de voyage stocké dans l'eMRTD. (**Messages 1 & 2**)

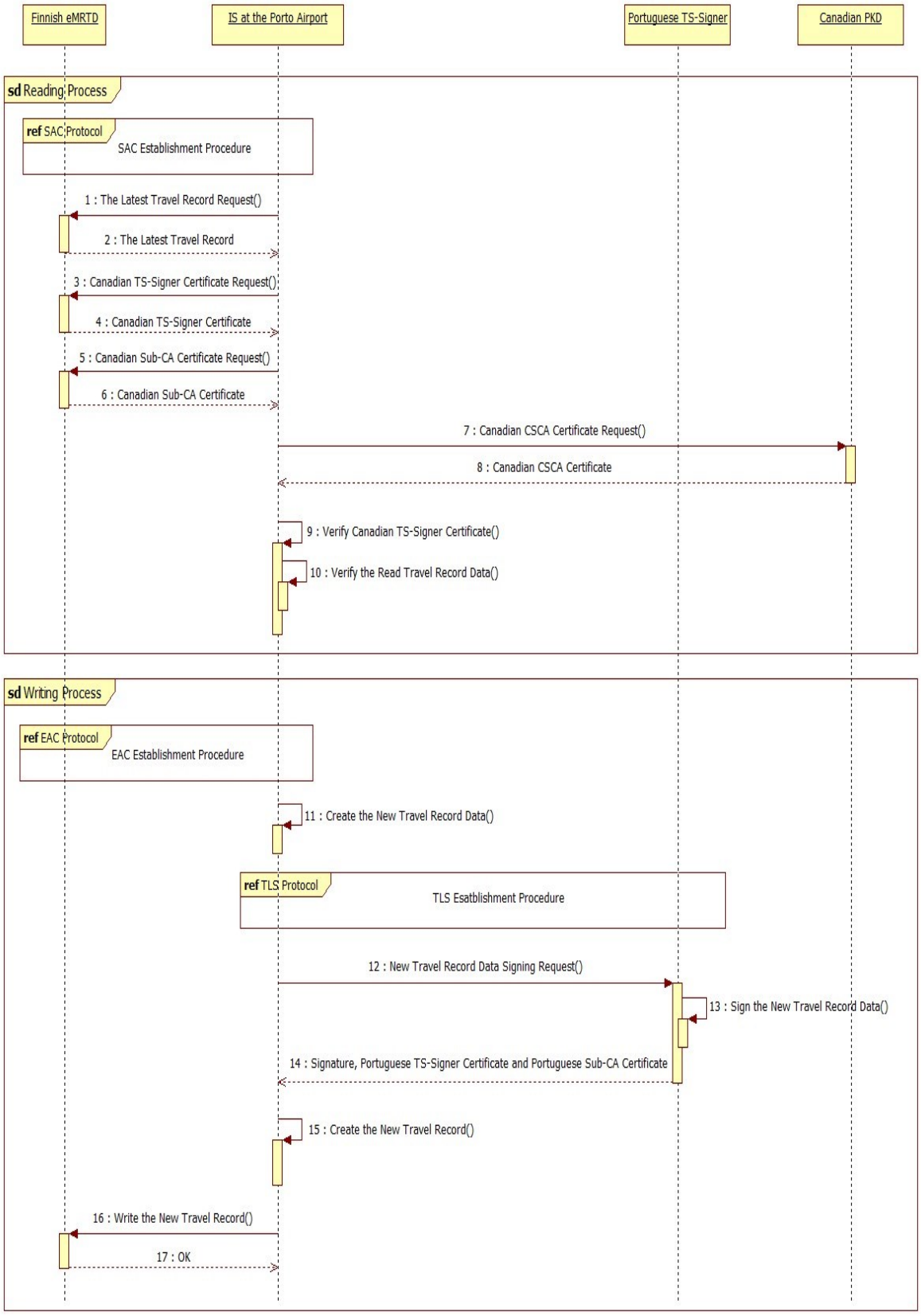


Figure 25 – Diagramme séquentiel des interactions entre le service des douanes et l'eMRTD finlandais ainsi que les interactions entre le service des douanes et les composants requis des PKIs LDS2 pendant les operations de lecture et d'écriture de/vers le eMRD

Etape 3: Sur la base des références incluses dans l'enregistrement de voyage le service des douanes de l'aéroport de Porto demande et reçoit le certificat TS-Signer canadien et le certificat canadien Sub-CA du eMRTD. Ces deux certificats ayant été inscrits sur l'eMRTD par l'aéroport canadien.
(**Messages 3, 4, 5 & 6**)

Etape 4: Pour des raisons de vérification le service des douanes de l'aéroport de Porto demande aussi le certificat canadien CSCA qui est délivré par le CSCA du PKI canadien de signature numérique au format LDS2. En raison du fait que le CSCA canadien est le certificat approuvé du PKI canadien de la signature numérique au format LDS2 et du PKI Canadien au format LDS1 le service des douanes de l'aéroport de Porto demande et reçoit le certificat CSCA canadien du PKD Canadien. Pour notre implémentation nous avons considéré que le service des douanes a déjà obtenu le certificat CSCA canadien.
(**Messages 7 & 8**)

Etape 5: Le service des douanes vérifie le certificat canadien TS-Signer en utilisant le certificat sub-CA et le certificat CSCA Canadien. (**Message 9**)

Etaoe 6: Enfin, après la vérification du certificat TS-Signer Canadien le service des douanes de l'aéroport de Porto vérifie l'authenticité et l'intégrité des données lues dans le dernier enregistrement de voyage reçu du eMRTD à l'étape 2. A ce stade l'opération de lecture est terminée. Les prochaines étapes concernent l'opération d'écriture. (**Message 10**)

Opération d'écriture

Etape 7: L'opération d'écriture commence avec l'interaction entre le service des douanes de l'aéroport de Porto et l'eMRTD finlandais afin que le protocole EAC s'établisse. Le protocole EAC assure une authentification mutuelle entre le service des douanes et l'eMRTD et il permet au service des douanes de prouver à l'eMRTD qu'il est habilité à écrire de nouveaux enregistrements de voyage. L'exécution du protocole EAC requiert des certificats délivrés par les PKI d'autorisation finlandais et portugais au format LDS2. Par conséquent le service des douanes interagit avec les composants de ces deux PKIs afin d'obtenir les certificats requis. En particulier le service des douanes interagit avec les CVCA finlandais du PKI d'autorisation finlandais au format LDS2 et avec le CVCA portugais du PKI d'autorisation portugais au format LDS2. Les interactions entre le service des douanes et les composants appropriés du PKI d'autorisation finlandais LDS2 et du PKI d'autorisation portugais LDS2 ne sont pas décrits pour des raisons de limitation de place. Par ailleurs pendant l'implémentation nous avons considéré que le service de douane avait déjà obtenu les certificats requis pour l'établissement du protocole EAC. **(EAC Establishment Procedure)**

Etape 8: Le service des douanes de l'aéroport de Porto crée les données du nouvel enregistrement de voyage suivant la structure des enregistrements. (**Message 11**)

Etape 9: Le service des douanes de l'aéroport de Porto établit une connexion TLS avec le TS Signer portugais. (**TLS Establishment Procedure**)

Etape 10: Le service des douanes de l'aéroport de Porto envoie les données du nouvel enregistrement de voyage au TS-Signer portugais. (**Message 12**)

Etape 11: Le TS-Signer portugais crée la signature des données du nouvel enregistrement de voyage en les signant numériquement. Le TS-Signer Portugais est l'entité finale du PKI de signature numérique au format

LDS2. En outre le TS-Signer portugais stocke son propre certificat délivré par le Sub-CA portugais ainsi que le certificat Sub-CA portugais délivré par le CSCS portugais. (**Message 13**)

Etape 12: Le TS-Signer Portugais envoie la signature numérique des données du nouvel enregistrement de voyage, le certificat TS-Signer ainsi que le certificat du TS-Signer portugais et le certificat Sub-CA portugais au service des douanes de l'aéroport de Porto. (**Message14**)

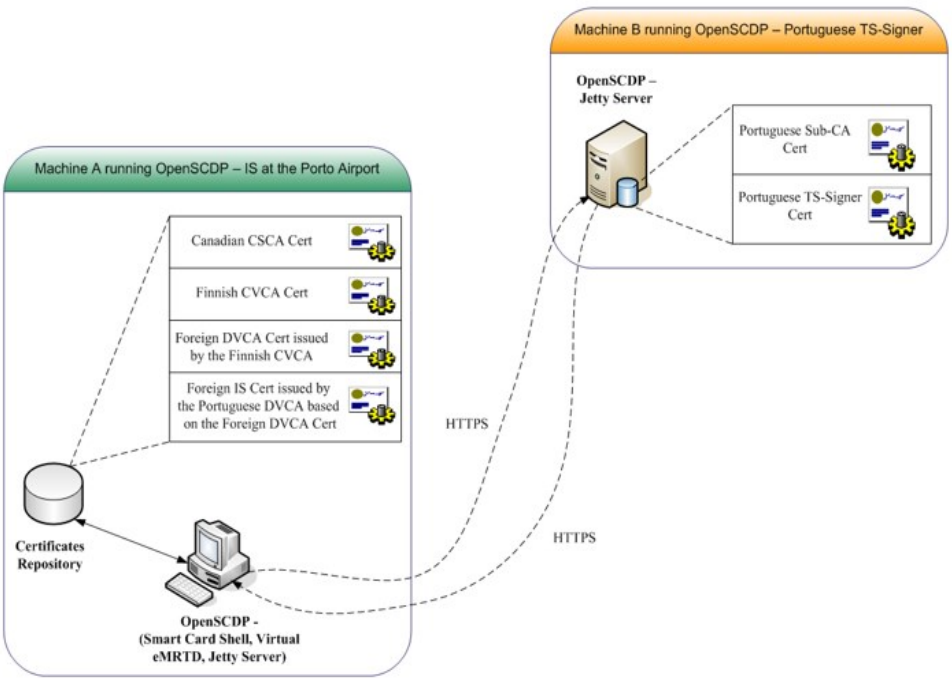
Etape 13: A la réception de la signature numérique des données du nouvel enregistrement de voyage, le certificat du TS-Signer portugais et le certificat Sub-CA portugais, le service des douanes crée le nouvel enregistrement de voyage. En particulier le service des douanes ajoute aux données du nouvel enregistrement de voyage créé à l'étape 8 les éléments suivants: a) la signature numérique reçue des données du nouvel enregistrement de voyage et b) les références au certificat du TS Signer portugais et du certificat portugais Sub-CA dans le compartiment de certificat du eMRTD finlandais. (**Message 15**)

Etape 14: Le service des douanes de l'aéroport de Porto inscrit le nouvel enregistrement de voyage, créé à l'étape 13, dans l'eMRTD finlandais. De plus le service des douanes inscrit le certificat du TS-Signer portugais et le certificat sub-CA portugais reçus du TS-Signer à l'étape 13 dans le fichier de stockage des certificats de l'eMRTD finlandais. Si l'opération d'écriture s'est accomplie avec succès le message OK est renvoyé au service des douanes. (**Messages 16 & 17**)

Mise en place du démonstrateur

Nous avons pris en consideration deux types différents d'implémentation. Le premier type d'implémentation est basé sur l'eMRTD virtuel OpenSCDP et le second type est basé sur un eMRTD 4G réel fourni par Gemalto.

Implémentation basée sur l'e-MRTD virtuel OpenSCDP :



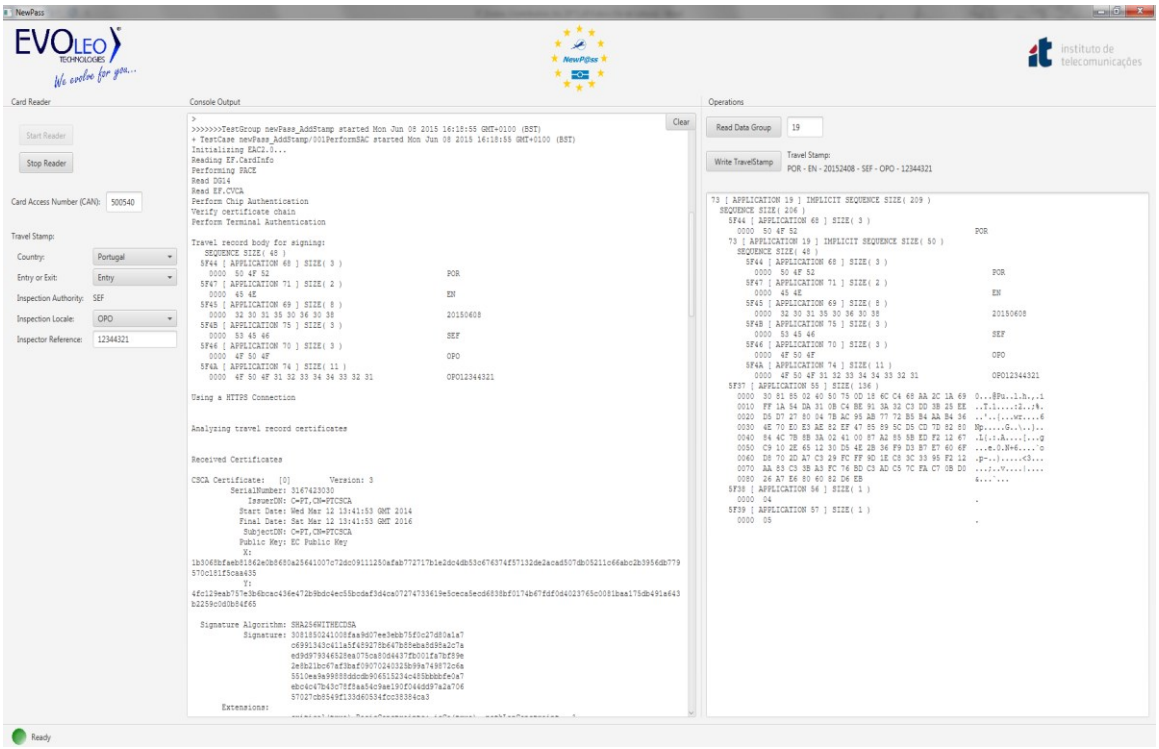
La mise

en place de ce type d'implémentation consiste à utiliser deux machines exécutant OpenSCDP. La machine A exécute la fonctionnalité du service des douanes de l'aéroport de Porto et la machine B exécute la fonctionnalité du TS-Signer Portugais.
Tous les certificats requis pour la vérification du Certificat Canadien TS-Signer à l'étape 5 et pour la vérification de l'authenticité et de l'intégrité des données de l'enregistrement de voyage à l'étape 6 sont stockés localement dans la Machine A et sur l'eMRTD virtuel. En particulier, pour la vérification du certificat du TS-Signer canadien, le certificat canadien CSCA requis est stocké dans la machine A et le certificat Sub-CA requis est stocké sur l'e_MRTD virtuel qui joue le rôle de l'eMRTD finlandais.
Le certificat TS-Signer canadien qui est aussi utilisé pour la vérification de l'authenticité et de l'intégrité des données de l'enregistrement de voyage est stocké dans l'eMRTD virtuel.

De plus, les certificats (le certificat CVCA finlandais, le certificat DVCA délivré par le CVCA Finlandais et le certificat du service des douanes délivré par le DVCA Portugais sur la base du certificat DVCA) que la machine A (c'est à dire le service des douanes de l'aéroport de Porto) requiert pour l'établissement du protocole EAC à l'étape 7 sont stockés localement dans la machine A.
Finalement, le certificat Portugais TS-Signer et le certificat portugais Sub-CA qui sont inscrits par la Machine A sur l'e-MRTD en étape 14 sont stockés localement sur la Machine B (c'est à dire le TS-Signer Portugais). Ces certificats sont envoyés de la Machine B vers la Machine A à l'étape 12.

La description qui suit montre des captures d'écran des résultats des éléments développés pour chacune des étapes décrites ci-dessus.

L'Interface Graphique Utilisateur du service des douanes est montrée sur la figure suivante : sur la partie gauche il est possible de choisir le pays du service des douanes que l'on simule, au milieu une console de sortie et à droite les informations avec possibles opérations de lecture écriture vers les groupes de données au format LDS2.



Opération de lecture

Etape 1: Le protocole SAC a été établi entre l'eMRTD finlandais virtuel et le service des douanes à l'aéroport de Porto.

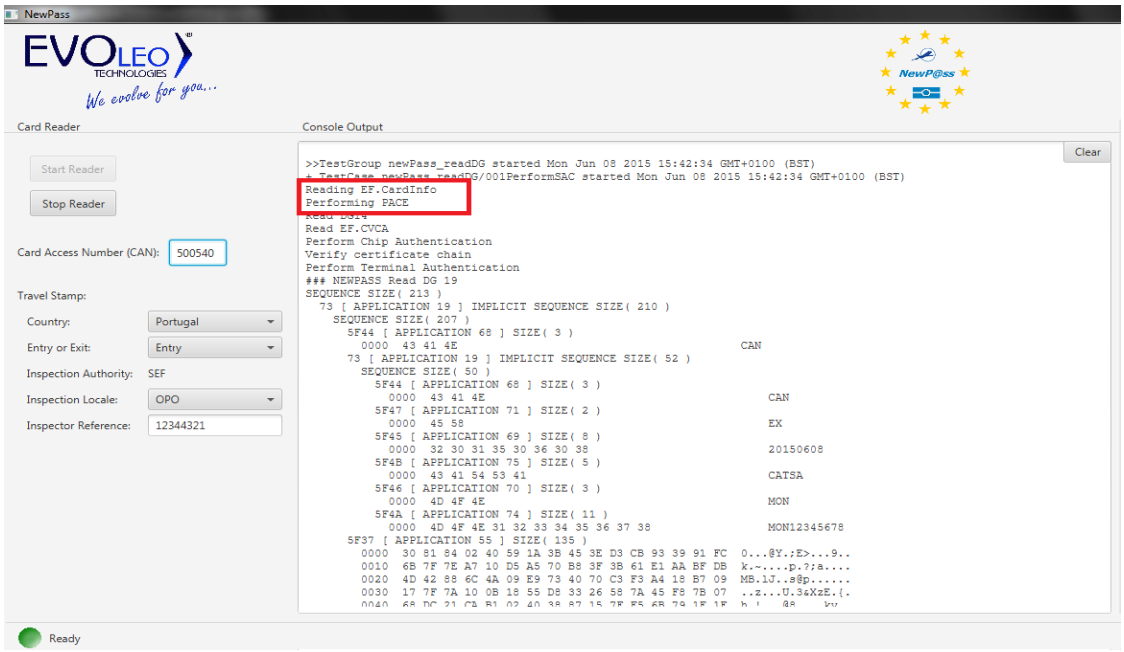


Figure 26 - SAC protocol implementation

Etape 2: Le dernier enregistrement de voyage reçu du service des douanes à l'aéroport de Porto.

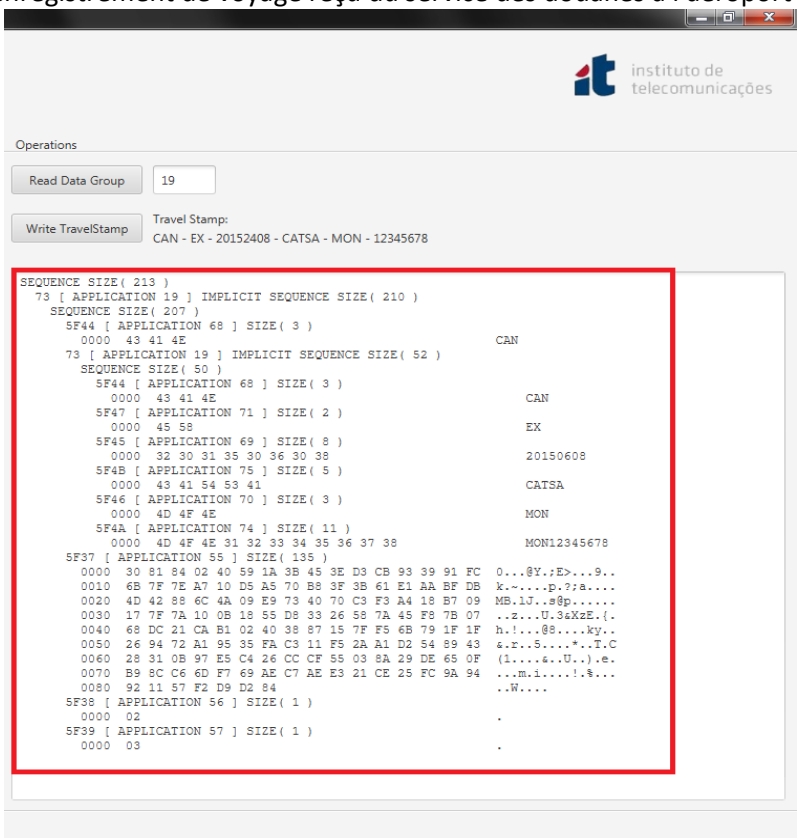


Figure 27 - Last Travel record written in the eMRTD

Etape 3: Le certificat canadien TS-Signer et le certificat Sub-CA canadien reçus de l'eMRTD virtuel.

Etape 4: Le certificat Canadien CSCA qui est stocké sur la Machine A (c'est à dire le service des douanes de l'aéroport de Porto)

Etape 5: Le certificat canadien TS-Signer est vérifié par le service des douanes.

Etape 6: L'authenticité et l'intégrité des données de l'enregistrement de voyage lu sont vérifiées par le service des douanes.

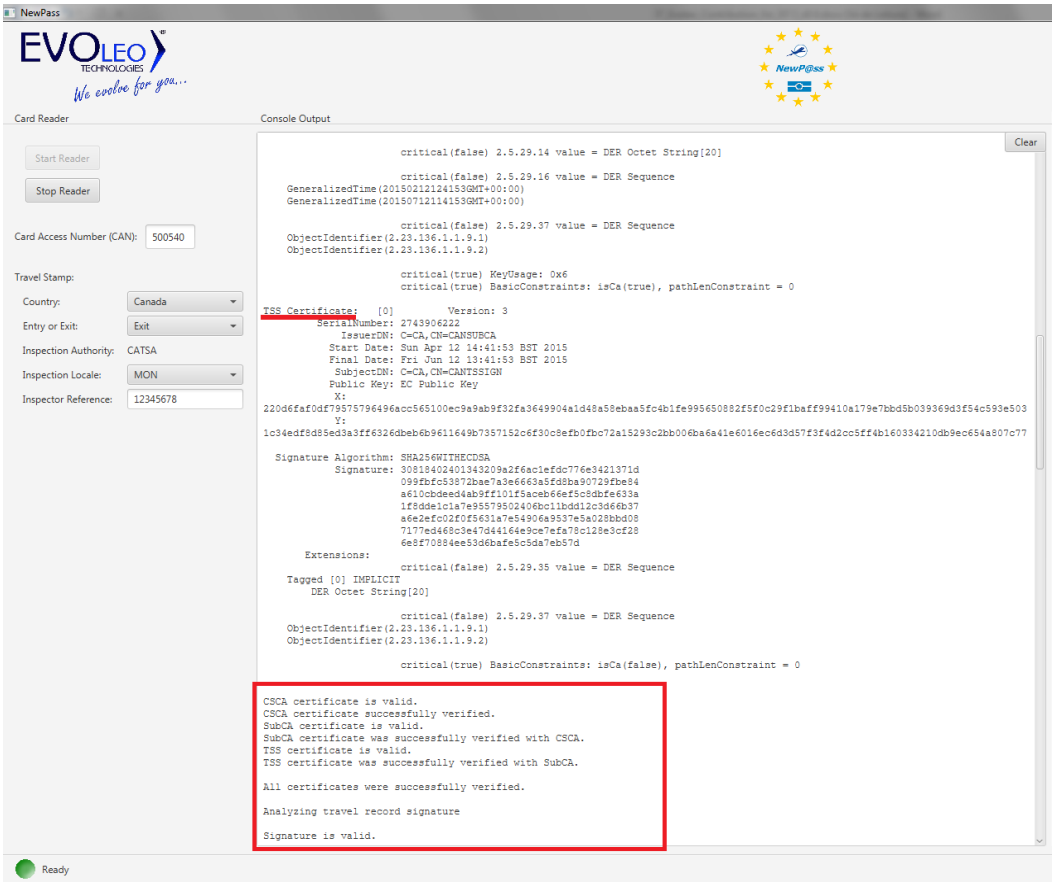


Figure 28 - Travel record validation

Opération d'écriture

Etape 7: Le protocole EAC a été établi entre l'eMRTD finlandais virtuel et le service des douanes de l'aéroport de Porto.

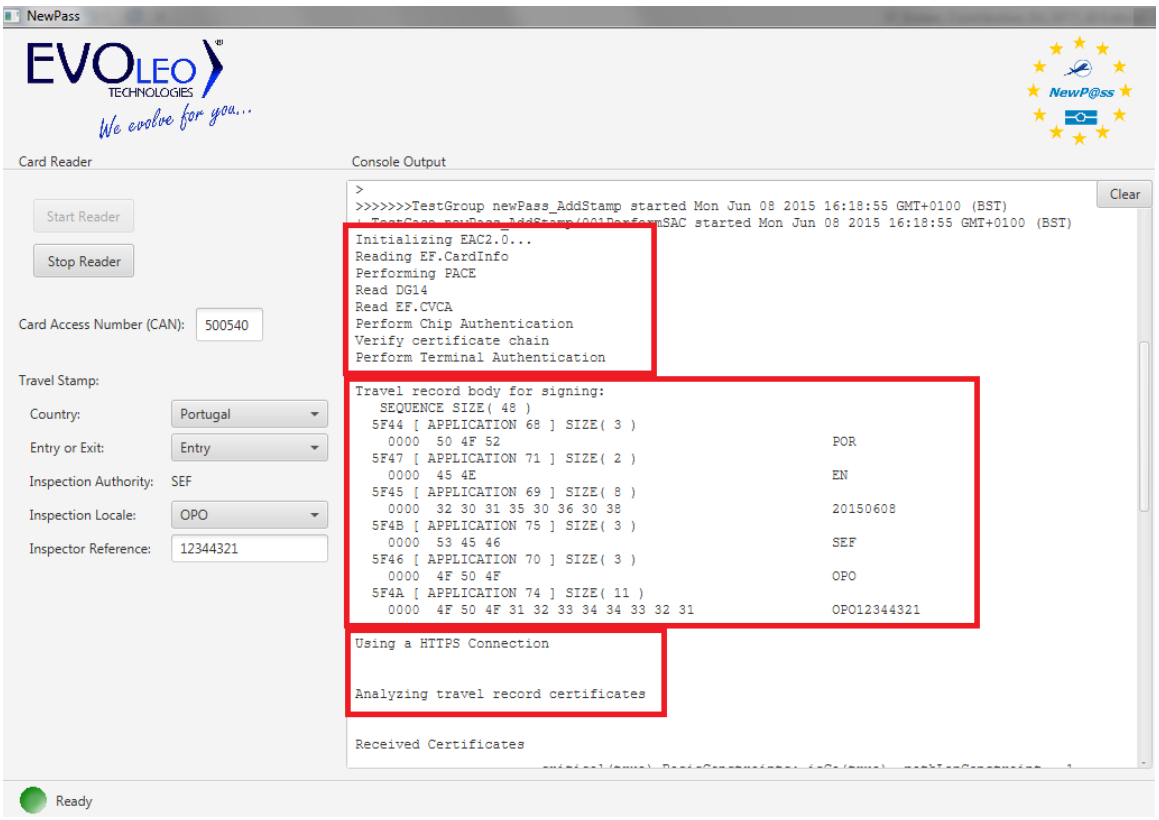


Figure 29 - EAC protocol implementation, followed by the new Travel Record and TS-Signer TLS connection

Etape 8: Les données du nouvel enregistrement de voyage sont créées par le service des douanes de l'aéroport de Porto suivant la structure des enregistrements de voyage.

Etape 9: Une connexion TLS a été établie entre le service des douanes de l'aéroport de Porto et le TS Signer portugais (c'est-à-dire Machine B) à.

Etape 10:La demande est envoyée au TS-Signer Portugais pour la signature des données du nouvel enregistrement de voyage.

Etape 11: La signature des données du nouvel enregistrement de voyage, le certificat TS-Signer portugais et le certificat Sub-CA portugais.

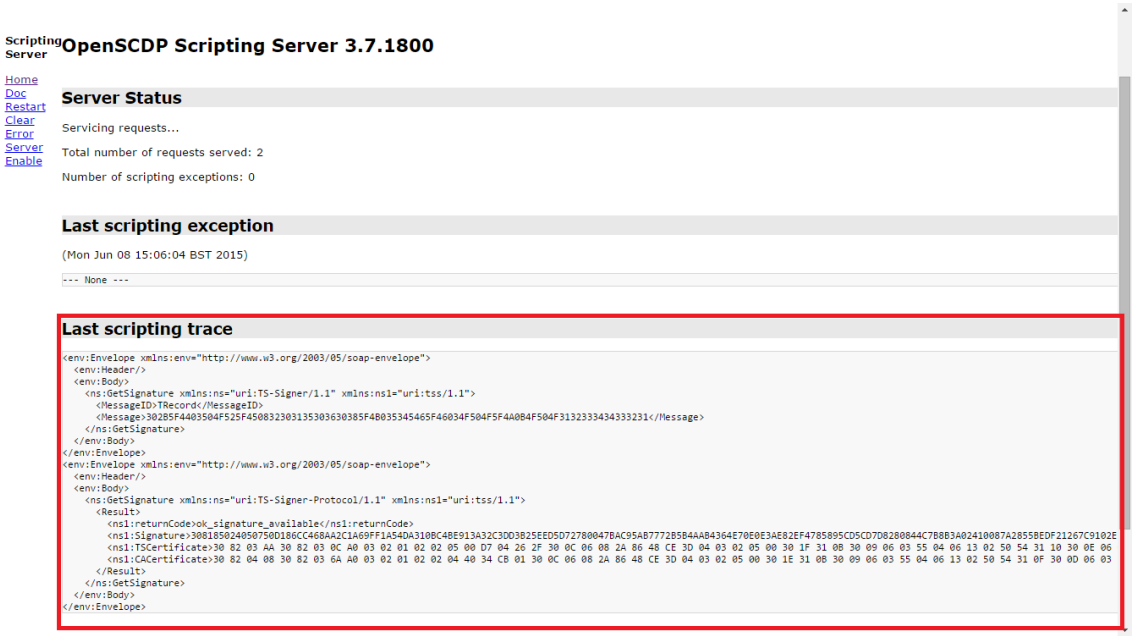


Figure 30 - TS-Signer response message

Etape 12: Réponse du TS-Signer portugais au service des douanes de l'aéroport de Porto qui inclut la signature numérique des données du nouvel enregistrement de voyage, le certificat TS-Signer portugais et le certificat Sub-CA portugais.

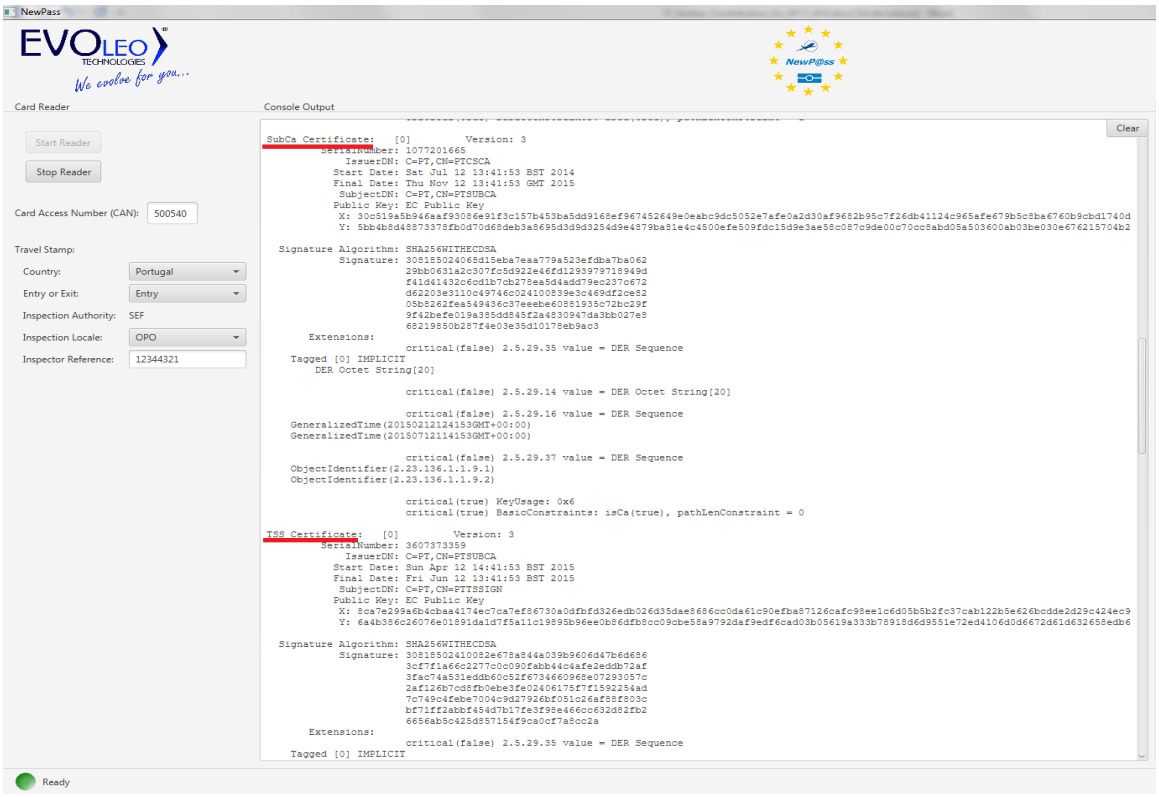


Figure 31 - Portuguese Sub-CA and TS-Signer certificates

Etape 13: Nouvel enregistrement de voyage

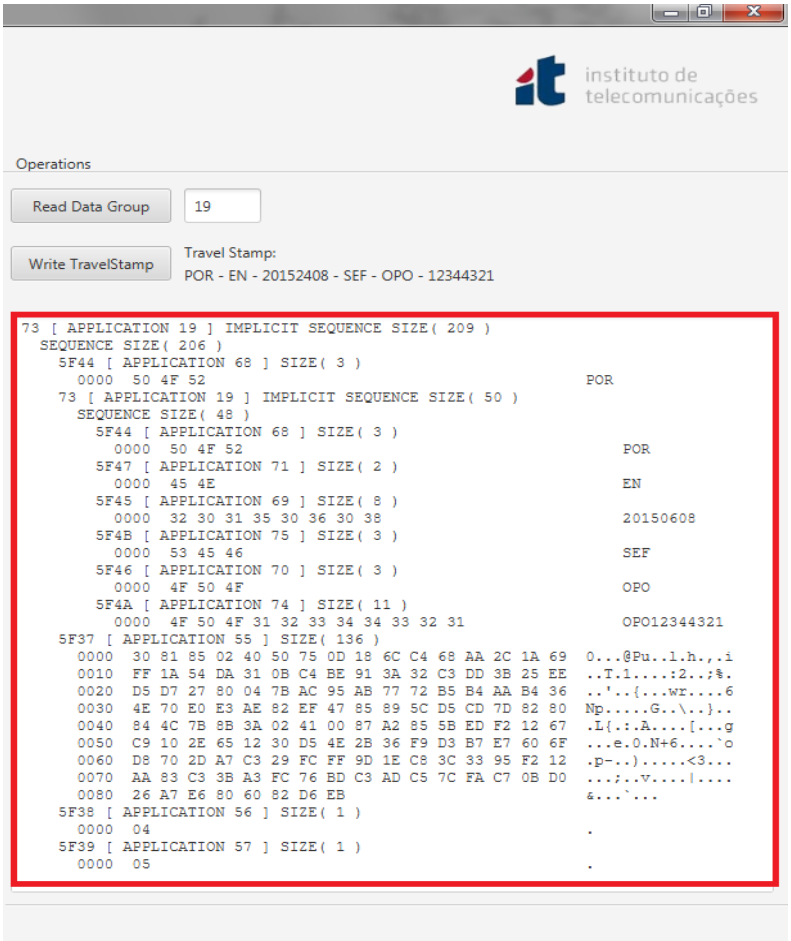


Figure 32 -Tthe new Travel Record, with signature and certificates indexes

6.5. SP5 - Test et implémentations de référence

6.5.1. Introduction

Coordinateur	**Infineon Technologies Austria AG (IFAT)**
Partners	IFX, Gemalto, G&D, ST, NXP-A, NXP-G, NXP-F, IT, EVO, ISEN, CEA-LETI, TUG-IAIK
SP Objectives	L'objectif de ce sous-projet est de développer de nouvelles méthodologies et des programmes de test afin de tester des implémentations de référence ; les résultats devront fournir une base pour les tess de conformité des produits futurs avec les spécifications des standards internationaux comme pour les tests d'interopérabilité. Les résultats inclueront la consolidation des méthodologies de test qui seront proposées aux comités de standardisation appropriés Mettre en œuvre le développement du matériel et l'implémentation des logiciels de test concurremment aux activités de standardisation sera un challenge majeur pour ce sous-projet

Le SP se compose de trois tâches :

- **Tâche 1:** Méthodologie et outils pour la génération et l'automatisation des tests (définition d'une méthodologie de test, Evaluation/définition des programmes de test, développement/évolution des programmes de test, Développement d'un outil de debug à partir de simulateur, Développement d'un environnement de tests pour les tests de conformité).
- **Tâche 2**: Application et déploiement *(ndustrialisation des plates formes de démonstration, Développement d' un outil lecteur Universel, Démonstration de nouvelles fonctions e-passeport).*
- **Tâche 3:** Activités de standardization(Spécification de test du VHBR, Spécification de test EMD*)*

6.5.2. Activités par périodes et partenaires

2012:

Gemalto
Gemalto a travaillé sur la tâche T5.1 pour définir les tests liés au nouveaux protocoles SAC et EACv210, et a aussi évalué les suites de tests relativesau passeport 3G. Les activités de normalisation de Gemalto sont rapportées dans SP8.

NXP-F
NXP France a développé des outils pour la production et l'automatisation de test pour la famille de puce lecteur (tâche 1). L'accent a été particulièrement mis sur le développement de deux outils. L'un des outils permet de piloter l'IC en mode DfT (conception pour le test). L'autre outil permet la gestion de toutes les mesures nécessaires pour valider et qualifier l'IC. NXP France s'est porté volontaire pour être le coordinateur du livrable D5.1.

ST
Pas encore commencé.

ISEN-Toulon
Dans lrSP5 l'ISEN-Toulon a travaillé sur l'état de l'art des outils de caractérisation permettant la validation du protocole de VHBR et la façon de caractériser les différents éléments de lecteurs et de passeports électroniques afin d'assurer les meilleures performances de chaque partie.

CEA-Leti
Pas encore commencé.

Giesecke & Devrient
G & D a commencé à enquêter sur les stratégies de test pour les nouvelles fonctionnalités de la plate-forme 3G de passeport électronique.

IFX
Pas encore commencé.

NXP-G
Les tâches de NXP Allemagne pour le SP5 étaient en préparation. Conformément à la planification de l'effort, aucun effort significatif n'a été dépensé dans le cadre SP5 en 2012. Les travaux de préparation pour les tâches 1 et 3 ont commencé. Les efforts dépendent des livrables du SP2, qui ont bien progressé.

IFAT

Au cours de la réunion de l'ISO / CEI à la Nouvelle Orléans au 09/2012 les définitions de VHBR ont été transférées au status FDIS de vote. Le code source de l'outil de détermination de forme d'onde a été adapté. Enfin, l'amendement 8 de la spécification de test ISO / CEI 10373-6 a été modifié suite à de nouveaux apports en termes de « cadres avec correction d'erreur ».

NXP-A
Pas encore commencé.

TU Graz / IAIK
Nous avons développé des méthodes pour générer des cas de test à partir de modèles formels apatrides afin d'atteindre une couverture de test à l'égard des différents critères d'évaluation. Cela inclut des conditions modifiées et une décision pour la couverture des tests, ceci est nécessaire dans les normes pour les systèmes critiques de sécurité. Nous avons également commencé avec un outil prototypé mettant en œuvre ces méthodes.

IT
Pas encore commencé.

Evoleo
Pas encore commencé.

2013:

IFAT (SP coordinateur)
IFAT a développé des bancs d'essai pour le VHBR et pour l'EMD et a pris la responsabilité du livrable D5.1 "Rapport sur les essais de méthodologies et définition de suites de tests."
IFAT a participé à la réunion ISO / CEI à Tokyo, au Japon 06/2013. Pour les « cadres avec correction d'erreur » (Amendement 4 sein de l'ISO / CEI 14443-4) la résolution de vote DIS a été faite. Pour les méthodes de test VHBR PSK (amendement 5 sein de l'ISO / CEI 10373-6) la résolution de vote DIS a été faite également.

Gemalto
Gemalto a terminé sa partie sur la tâche T5.1 en contribuant aux chapitres convenus dans livrables D5.1 et D5.2. La contribution sur le livrable D5.1 décrit les méthodes d'essai pour les protocoles SAC, LDS2, BAC et EAC. La contribution sur le livrable D5.2 décrit les tests nécessaires pour la plate-forme logicielle de passeport électronique. En outre, une description détaillée du passeport électronique tests d'interopérabilité a été ajoutée en D5.2 par Gemalto. Concernant la tâche T5.3 (activités de normalisation), voir le rapport ci-dessous SP8.

NXP-F
NXP France a développé des outils pour la production et l'automatisation de test pour la famille de puce lecteur (tâche 1). L'accent a été particulièrement mis sur le développement de deux outils. L'un des outils permet de piloter l'IC en mode DfT (conception pour le test). L' autre outil permet la gestion de toutes les mesures nécessaires pour valider et qualifier l'IC. Les outils ont été testés, et le débogage est utilisé pour valider certains sous ensemble du contrôleur contact (avant le lecteur ciblé encore en développement)
En raison du départ de Cathy Demoment la responsabilité de D5.1 a été remis à l'IFAT.

ST
ST a travaillé plus spécifiquement sur les essais pour la communication sans contact ainsi que la caractérisation approfondie des paramètres liés. L'accent a été fait sur la capacité de simuler le banc d'essai complet avec des modèles de circuits potentiels afin d'améliorer la prévisibilité des résultats des tests. Les travaux se poursuivent également sur les tests et les essais VHBR normalisation à l'ISO.

ISEN-Toulon

• A développé des bancs d'essai RF (impédances, spectres, etc ...) pour caractériser les différents éléments du système de contact en temps réel (puce, antenne, emballage.).
• Contribution à la spécification d'une communication VHBR et non VHBR et la façon de le caractériser (livrables D5.1 et D5.2).
• A développé des bancs d'essai pour VHBR.

CEA-Leti

Le CEA-Leti a travaillé sur la synthèse des projets de documents de normes pour la communication de VHBR (ISO-14443) et pour les définitions de tests (ISO 10373-6). La synthèse de ces documents et de leurs interdépendances a été intégrée dans livrables D5.1 et D5.2.

IFX

Pas encore commencé.

Giesecke & Devrient

G & D ont commencé à installer l'environnement des essais pour les passeports 3G. En outre, G & D ont étudié comment les résultats des tests peuvent être réutilisés pour une prochaine certification Critères Communs.

NXP-G

Développement d'un outil de débogage simulateur base (tâche 1) qui a fait de bons progrès, avec des résultats intermédiaires disponibles en interne. Les activités de normalisation (tâche 3) ont continué à fonctionner.

NXP-A

Fourni un modèle formel pour la génération de cas de test et supporte la méthodologie des cas de test ainsi que le développement de l'outil. Les cas de test sont générés automatiquement lorsqu'ils sont exécutés sur un applet pare-feu Java Card.

TU Graz / IAIK

Nous avons développés des méthodes pour générer des cas de test à partir de modèles formels apatrides pour atteindre une couverture de test à l'égard des différents critères d'évaluation. Cela inclut des conditions modifiées et une décision pour la couverture des tests, ceci est nécessaire dans les normes pour les systèmes critiques de sécurité. Nous avons également commencé avec un outil prototypé mettant en œuvre ces méthodes. Les premiers résultats ont été acceptés pour publication à la conférence VALID 2013. Nous avons également commencé les recherches sur les méthodes pour l'achèvement de la suite de tests.

IT

Responsable de la rédaction livrable "D5.2 - Enquête sur les spécifications de test". Il a proposé une première Table des matières pour D5.2, basée sur la norme ISO / IEC FCD 10373-6 documentation standard. Des conférences téléphoniques dédiées ont été organisées, avec tous les partenaires impliqués dans la tâche 5.3, afin de discuter le contenu de D5.2, la structure finale et de déterminer la contribution de chaque partenaire. Toutes les contributions ont été compilées et intégrées dans le livrable par IT, en prenant soin de tout le travail d'édition nécessaire. D5.2 livrable a été libéré à la date prévue (de T3-2013).

Evoleo

Evoleo a contribué à l'enquête des spécifications de test et les méthodologies liées principalement au PCD / lecteur. Les spécifications des tests et VHBR EMD sont également un sujet qu' Evoleo a exploré.

2014:

IFAT (SP coordinateur)
IFAT a travaillé sur la mise en œuvre de nouvelles fonctions e-passeport dans un test-logiciel.
IFAT a participé à la 42e réunion de l'ISO / IEC JTC1 / SC17 / WG8 / TF2 à Kochel am See (Allemagne: 28, 29 et 30 Janvier 2014) et la réunion 43ème ISO / IEC JTC1 / SC17 / WG8 / TF2 à Neuchâtel, (Suisse: 8 et 9 Avril 2014).
IFAT a participé la 42e réunion de l'ISO / IEC JTC1 / SC17 / WG8 / TF2 à Kochel am See (Allemagne: 28, 29 et 30 Janvier 2014), la réunion 43ème ISO / IEC JTC1 / SC17 / WG8 / TF2 à Neuchâtel (Suisse : 8 et 9 Avril 2014), la 44nd ISO / IEC JTC1 / SC17 / WG8 et ISO IEC JTC1 SC17 / WG8 / Réunion / / TF2 à Salamanque Espagne (22 au 26h de Septembre 2014), la 45nd ISO / IEC JTC1 / SC17 / WG8 et ISO SC17 IEC JTC1 / WG8 / Réunion / / TF2 à Hiroshima Japon (23 au 27 février 2015).

Gemalto
Gemalto a terminé sa partie sur la tâche T5.1 en contribuant aux livrables D5.1 et D5.2. Pendant S1 / 2014, le travail sur la tâche T5.2 a été lancé avec la planification du livrable D5.4 Rapport sur les outils de lecture des passeports 3G / 4G.
Gemalto a terminé le travail sur D5.4 livrable (Rapport sur les outils de lecture 3G & 4G passeports électroniques) et a publié le document en Septembre 2014, agissant comme l'éditeur principal du document.

NXP-F
NXP France a développé des outils pour la production et l'automatisation de test pour la famille de puce lecteur (tâche 1). L'accent a été particulièrement mis sur le développement de deux outils. L'un des outils permet de piloter l'IC en mode DfT (conception pour le test). L'autre outil permet la gestion de toutes les mesures nécessaires pour valider et qualifier l'IC. Les outils ont été testés, et le débogage est utilisé pour valider certains sous ensembles de contrôleurs contact (avant le lecteur ciblé encore en développement)
En raison du départ de Cathy Demoment la responsabilité de D5.1 a été remis à l'IFAT.

ST
ST a poursuivi son travail sur les essais et méthodes d'essais des communication sans contact, ainsi que le suivi et la contribution à la normalisation des tests VHBR.

CEA-Leti
Au cours du premier semestre de 2014, le CEA a poursuivi le développement de la partie de lecteur de la plate-forme d'essai. Après avoir étudié les différentes architectures de modulateur, une carte d'émission (newp @ ss TX) a été développée. Elle comprend les blocs suivants: convertisseur D / A (AD9740), modulation IQ (multiplicateur), génération d'horloge, alimentation. La carte a été fabriquée et les premiers essais seront effectués au début de Juillet. Tout d'abord en émettant des symboles aléatoires puis en incrémentant le débit binaire. La constellation de sortie sera analysée et confrontée à la norme ISO1443-2 AM5. Les spécifications de l'antenne ont été calculées sur les contraintes de la norme. D'autres expériences portent sur l'impact de l'antenne : on émet des symboles aléatoires et on analyse les constellations après l'émission de l'antenne.
Le CEA-Leti a travaillé sur la conception et le développement du lecteur spécification complète de VHBR. La première version sera mise en place comme un outil de test pour valider les communications sans contact avec la puce de silicium VHBR. Avec cet outil de test, à la fois ASK et des liens de communication PSK seront expérimentés et validés
.

ISEN-Toulon

ISEN a travaillé sur la livrables D5.1 et D5.2.
ISEN a développé des outils pour la caractérisation de la puce sans contact du passeport électronique. ISEN a continué à développer le banc de caractérisation dédiée au système VHBR.
Le banc d'essai de VHBR est composé d'un assemblage ISO 10373-6 PCD avec un réseau d'adaptation approprié pour les systèmes de VHBR et une plate-forme National Instrument pour le conditionnement de signal. Le banc PCD VHBR dispose d'un réseau d'adaptation spécifique, qui optimise la communication sur la largeur de bande de fréquence globale.
La plate forme national instrument permet de générer et d'analyser des signaux RF en conformité avec les spécifications ISO 10373-6. L'émetteur peut générer des signaux quasi-idéaux avec une très faible vitesse de balayage (comme exposé ci-dessous), ce qui permet d'effectuer quelques tests avec plus de contraintes que les exigences ISO 10373-6.
Le récepteur peut effectuer des analyses sur les couches basses et couches hautes. Une première version de ce banc d'essai a été réalisée, sa validation serait faite lors de la caractérisation de passeport VHBR. Des études ont également commencé sur un des outils d'analyse pour les besoins de EMD.

IFX

IFX a participé à la fourniture du SAC pour les tests des OS sans contact dans le cadre les logiciels IFAT

Giesecke & Devrient

G & D a terminé la configuration de l'environnement des essais pour les passeports 3G. L'installation pour tester les passeports 4G progressait. La plate-forme de passeport 3G a passé avec succès les tests internes de G & D.

NXP-G
Le développement d'un outil de débogage base sur simulateur (tâche 1) a été achevé dans le cadre du projet. La validation en ce qui concerne l'efficacité et la facilité d'utilisation a continué au cours de la période considérée. Sous la tâche 2, NXP-G a continué à développer un outil de démonstration pour la fonctionnalité entrée / sortie de timbre en 4G pour passeports électroniques; cependant, le résultat n'a pas été obtenu entièrement pour l'instant.

TU Graz / IAIK
En collaboration avec NXP-A, nous nous sommes concentrés sur l'augmentation de suite de tests basés sur des techniques d'exécution concolique. Nous avons amélioré un outil existant, ce qui peut générer des suites de tests à partir de zéro, de sorte qu'il prend la suite de test générée par notre prototype et le programme en cours de test en entrée et augmente cette suite de tests pour satisfaire la couverture de la branche sur les parties souhaitées du code source. Nous avons évalué cet outil sur le code source industriel et nous avons pu améliorer considérablement la couverture de code. Les travaux ont permis dans le document «Automatisation des essais Suite Augmentation" par Roderick Bloem, Robert Könighofer, Franz rock et Michael Tautschnig de publier au QSIC2014. Nous travaillons actuellement sur un outil de génération des cas de tests abstraits à partir d'un modèle formel donné afin de parvenir à une couverture souhaitée sur elle.

IT

Elle a contribué au délivrable D5.4, lié à la tâche 5.2 et à une enquête sur l'état de l'art des outils de lecteur universel. Actuellement, il existe plusieurs solutions de logiciel de lecteurs de passeports électroniques.

Comme prévu, les solutions logicielles ouvertes / libres sont à la traîne par rapport aux logiciels commerciaux. Néanmoins, les anciennes solutions ont l'avantage d'être ouvertes, permettant ainsi de nouvelles implémentations. D'autre part, les lecteurs commerciaux ont l'avantage d'être des produits finaux, ce qui permet un déploiement immédiat et un soutien supplémentaire.

Evoleo

Evoleo a contribué à l'étude du cahier des charges et des méthodologies tests, principalement liés au PCD / lecteur. Les spécifications des tests et VHBR EMD ont également été un sujet qu Evoleo a exploré.
Evoleo a également contribué à la définition de l'outil de lecteur universel correspondant à de nouveaux passeports électroniques avec de nouvelles spécifications techniques. Cet outil de lecteur universel permettra de valider les passeports électroniques, mais aussi leurs spécifications techniques associées à des normes.
L'outil Lecteur Universel peut être développé en utilisant une plate-forme open source tel que la plate-forme ouverte Smart Card développement (OpenSCDP).
Le OpenSCDP est une collection d'outils pour le développement, le test et le déploiement de la carte à puce et les applications d'infrastructure à clés publiques. Il utilise les capacités de la plate-forme mondiale de script, le profil et la technologie de messagerie pour offrir une flexibilité inégalée et la vitesse de développement.
L'évaluation des technologies candidates à la création de l'outil « lecteur universel » a été effectuée, l'outil choisi est le Open Smart Card Platform Development (OpenSCDP).
Les contributions à D5.4 ont été préparées et ont continuées en ligne avec le logiciel qui est en cours de développement.

2015:

IFAT (SP coordinateur)

IFAT a travaillé sur la mise en œuvre de nouvelles fonctions e-passeport dans un test-logiciel.
IFAT a participé à la 45nd ISO / IEC JTC1 / SC17 / WG8 et ISO SC17 IEC JTC1 / WG8 / Réunion / / TF2 à Hiroshima Japon (23 au 27 février 2015)

Gemalto

Gemalto a également testé en interne sa plate forme 4G pour passeport électronique et ses applications associés à l'aide des logiciels de lecture des passeports 3G et 4G développés dans le cadre du projet.

NXP-F

NXP France a développé des outils pour la production et l'automatisation de test pour la famille de puce lecteur (tâche 1). L'accent a été particulièrement mis sur le développement de deux outils. L'un des outils permet de piloter l'IC en mode DfT (conception pour le test). L'autre outil permet la gestion de toutes les mesures nécessaires pour valider et qualifier l'IC. Les outils ont été testés, et le débogage est utilisé pour valider certaines sous développement contrôleurs de contact (avant le lecteur ciblé encore en développement)
En raison du départ de Cathy Demoment la responsabilité de D5.1 a été remis à l'IFAT.

ST

Alors que l'activité spécifique a été rempli pour ST dans ce sous-projet, ST a continué sa contribution à des travaux de normalisation des tests VHBR au sein de l'ISO / IEC JTC1 / SC17 / WG8 / TF2.

Cea-Leti

Au cours de l'année dernière (2014), le CEA a développé un outil de lecteur de test qui fera partie du démonstrateur technologique SP7 VHBR. La carte personnalisée (newp @ ss TX) est composée des blocs suivants: convertisseur D / A (AD9740), modulation IQ (multiplicateur), génération d'horloge, alimentation. Des expériences ont été menées pour évaluer l'impact des effets de couplage sur la distorsion du signal lors de l'utilisation PSK. Le niveau maximum de distorsion spécifié dans la norme ISO 14443-2 amd5 en termes de l'interférence entre symboles (ISI) a été comparé aux résultats obtenus avec le conseil TX utilisant des antennes avec des facteurs de qualité (4 et 10). Les résultats montrent que la mise au point par LETI du TX est conforme aux spécifications pour de faibles débits de données (jusqu'à 13,56 MHz) pour le facteur de qualité le plus bas. Néanmoins, la communication pourrait encore être établie pour des débits de données plus élevés ou des facteurs de qualité supérieure à condition que le récepteur développé en SP3 soit en mesure d'atténuer ces distorsions en utilisant un simple égaliseur, ouvrant la porte à l'atténuation ISI équilibré entre PCD et PICC.

ISEN-Toulon

ISEN a travaillé sur la livrables D5.1 et D5.2.

ISEN a développé des outils pour la caractérisation de la puce sans contact du passeport électronique. ISEN a continué à développer le banc de caractérisation dédiée au système VHBR.

Le banc d'essai de VHBR est composé d'un assemblage ISO 10373-6 PCD avec un réseau d'adaptation appropriée pour les systèmes de VHBR et une plate-forme National Instrument pour le conditionnement de signal. Le banc PCD VHBR dispose d'un réseau d'adaptation spécifique, qui optimise la communication sur la largeur de bande de fréquence globale.

La plate forme national instrument permet de générer et d'analyser des signaux RF en conformité avec les spécifications ISO 10373-6. L'émetteur peut générer des signaux quasi-idéaux avec une très faible vitesse de balayage (comme exposé ci-dessous), ce qui permet d'effectuer quelques tests avec plus de contraintes que les exigences ISO 10373-6.

Le récepteur peut effectuer des analyses sur les couches basses et couches hautes. Une première version de ce banc d'essai a été réalisée, sa validation serait faite lors de la caractérisation de passeport VHBR. L'Isen-toulon a développé un outil d'analyse pour les besoins EMD. Cet outil est basé sur la plate forme ISEN et des travaux portent sur l'IHM pour une meilleure expérience utilisateur.

IFX

IFX a participé à la fourniture du SAC pour les tests des OS sans contact dans le cadre les logiciels IFAT

G&D

La plate forme de test 4G a passé avec succes les tests internes G&D.

NXP-G

Au cours de la période considérée, les activités de clôture ont été menées. Les résultats ont été archivés et indexés pour diffusion interne éventuelle et en cas d'industrialisation.

TU Graz / IAIK

En collaboration avec NXP-A, nous avons développé des méthodes pour calculer automatiquement les données de test de haute qualité à partir de modèles de haut niveau qui sont donnés comme des systèmes à états finis. Nos méthodes prennent en charge diverses mesures de couverture tels que la couverture de l'Etat, la couverture de bord et de la couverture / état de la décision modifiée (MC / DC) sur les bords de

gardes. Nous avons mis nos méthodes dans un outil de preuve de concept de génération de cas d'essais et nous l'avons appliqué dans une étude sur l'implémentation de cache sécurisé de cas. Ce travail a abouti dans le document «Étude de cas: Test automatique de cas de production pour une mise en œuvre Cache sécurisé" par Roderick Bloem, Daniel Hein, Franz Rock, et Richard Alexander Schumi. Ce document a été publié à la 9ieme International Conference on Tests & Proofs (TAP'15). (TAP'15).

IT

Pas d'activité dans cette période

Evoleo

En H1-2015, Evoleo a contribué aux spécifications de l'outil de lecteur universel et utilisé comme entrée pour les briques de logiciels en cours de développement sur SP4.

6.5.3. Coopération

- **Au sein du SP5**
  - Bonne coopération, bons éléments reçus de tous les partenaires.
  - Conférence téléphonique régulière pour échanger les connaissances et préparer les livrables D5.1, D5.2, D5.3 et D5.4
  - Bonne répartition de la charge de travail.
- **Avec les auttres SP**
  - **SP7** (Use Cases & Demonstrators to Platform Software Development)
  - La méthodologie de tests fut incluse dans les recommandations des plates formes (**SP2**) et le developpement des plates formes matérielles (**SP3**).
  - Les activités de standardisation du **SP5** (VHBR et EMD) furent des entrées pour le **SP8.**

6.5.4. Résultats obtenus

Livrables:

Livrable	Tâche	Date prévue (CR #2)	Date réalisée	Type et contenu
D5.1	T5.1	T3 13	T3 13 Livré	Rapport sur les méthodologies de test (responsable: NXP-F)
D5.2	T5.3	T3 13	T3 13 Livré	Etude des spécifications de test (responsable: IT)
D5.3	T5.1	T1 15	T1 15 Livré	Rapport sur l'outil de génération de test et de débug basé sur simulateur (responsable: NXP-G)
D5.4	T5.2	T4 14	T4 14 Livré	Rapport sur l'outil de lecteur de e-Passeport 3G & 4G (responsable: Gemalto)
D5.5	T5.3	T2 15	T2 15 Livré	Spécifications de test VHBR et EMD (responsable: IFAT)

- ## *Principales réalisations:*

- Vue d'ensemble sur les méthodologies de test pour les passeports électroniques et lecteurs
- Dévelopement de banc de test relatif au VHBR (Very High Bit Rate), aux perturbations électromagnétiques (EMD, ElectroMagnetic Disturbance)
- Génération de cas de test automatique pour les passeports électroniques et automatisation de génération de test inclusive pour les puces de lecteurs.
- Veille sur les spécifications de test, y compris les normes internationales, les spécifications de la BSI pour passeport électronique et ISO / CEI pour pour lecteur.
- Introduction aux tests d'interopérabilité.
- **SP5 Point de départ:**

  - **1G & 2G ePassport**
    - 1G ePasseport électronique intègre le protocole de sécurité BAC, et contient l'image du visage du titulaire

• Des données biométriques supplémentaires (empreintes digitales) ajoutées au passeport électronique 2G et intègration des protocoles de sécurité BAC et EAC.

- **3G & 4G ePassport**

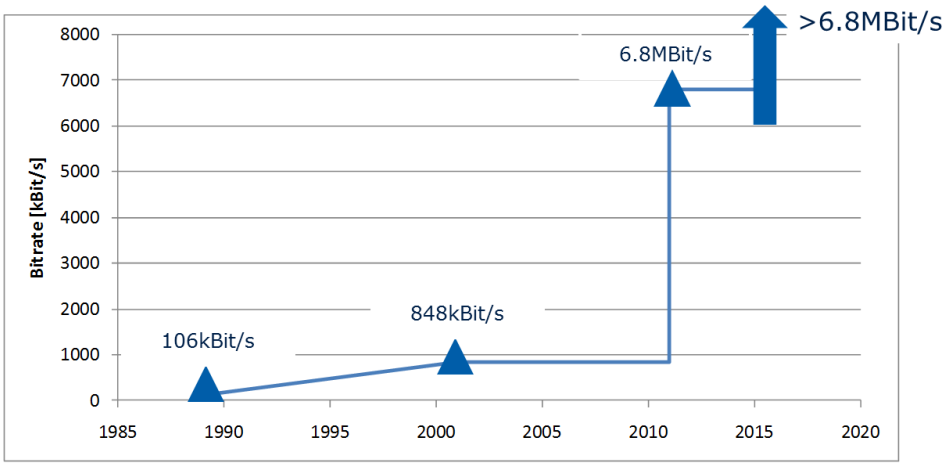
• 3G e-Passport intègre des protocoles de sécurité SAC et EACv210, et contient l'image faciale et les empreintes digitales du titulaire

• 4G e-Passport integre (au moins) le LDSv2 (de Evisa finalement pas défini, eTravelStamp, eBoardingPass), EACv210 totale et VHBR

- **Etat de l'art de la liste des outils de lecteurs universels de passeports électroniques**

Caractéristiques / Outil pour lecteur ePassport	Affichage des données biographiques	1G ePassport BAC	2G ePassport EACv1.11	3G ePassport EAC v2.1	3G ePassport SAC	4G ePassport LDS2 eVisa	LDS2 – Time Stamping (horodatage)
Gold Reader Tool Platinum Edition	X	X	X	X	X	..	..
Keolabs – URT	X	X	X	X	X	..	..
Collis eMRTD Test Tool	X	X	X	X	X	..	..
JMRTD	X	X	X	X	..	..	..
wzPASS	X	X	X	..	..	..	..
ePassport Viewer / pyPassport	X	X	X	..	..	..	..
NFC Passport Reader	X	X	X	..	..	..	..

- Développements sur les stratégies de test pour l'avenir 3G et 4G plate-forme, la modélisation formelle des caractéristiques du test, le test de l'interface haut débit.
- Fin 1980 : Premiers produits sans contact (de proximité)
- Milieu des années 90 : Début de standardisation des débits jusqu'à 848 kbps(ISO/IEC 14443)
- Début 2010 : Premier travaux de standardisation VHBR (ISO/IEC 14443)
- Amendement de ISO14443-2 pendant NewP@ss
- ISO 10373 définit l'ensemble des méthodes de tests qui doivent être appliquées aux cartes d'identification ainsi qu'au lecteur pour garantir leur interopérabilité
- Développement d'un outil de lecture 3G / 4G, un générateur de l'outil de test et un outil de débogage base sur simulateur. Le "lecteur outil 3G / 4G" est le nouveau nom de "Lecteur outil universel".

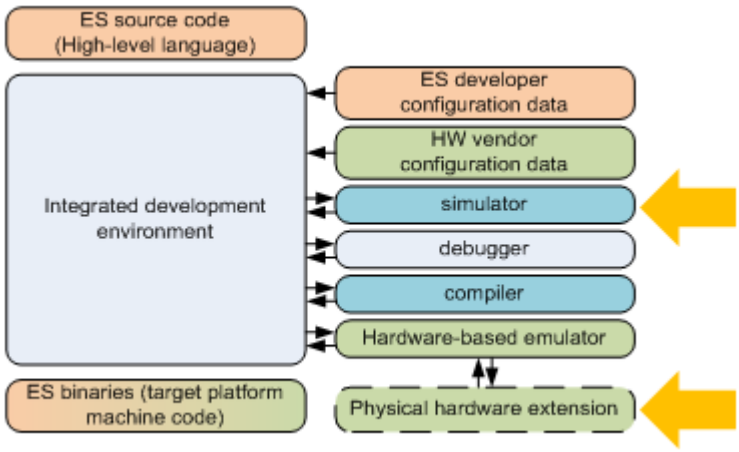


Outil de debogage base sur simulateur

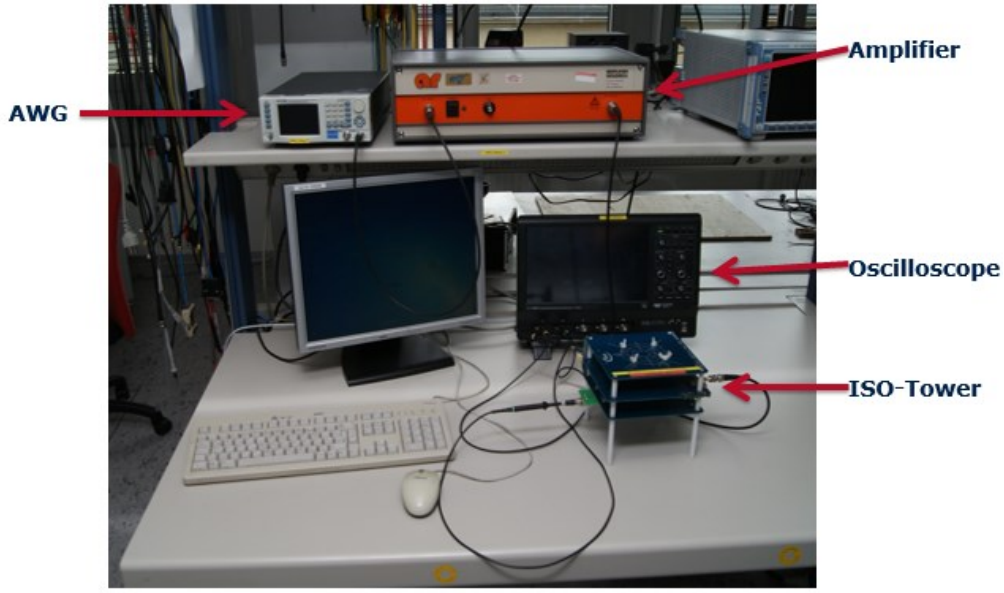
Description générale

Objectif:

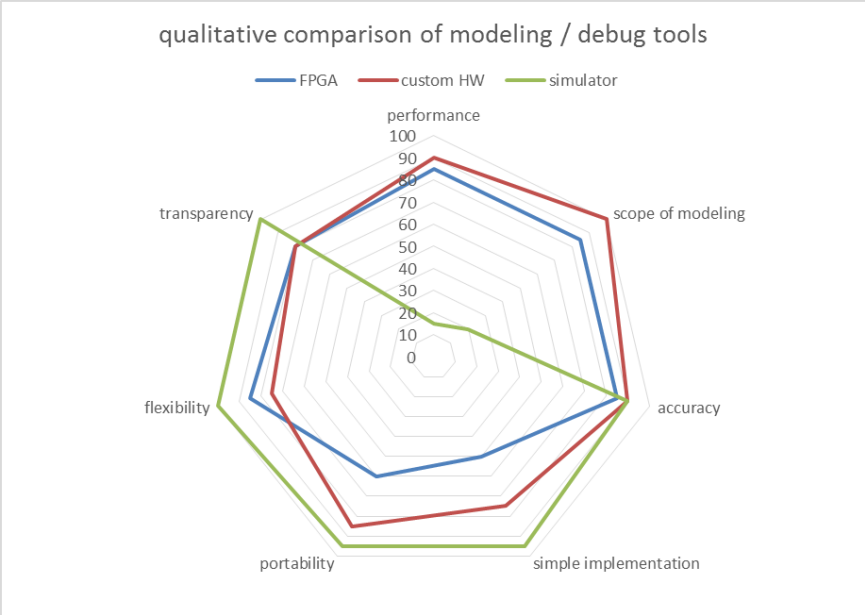
- L'implémentation de logiciel embarqué dans les ePasseports repose sur des outils de développement spécifiques au système d'exploitation
- D5.3 traite de l'architecture de ces outils de développement
- Travaux de simplification de l'architecture de la suite d'outils en effectuant les debuggages sur les outils logiciels (ceux basés sur simulateurs) plutôt que sur le matériel (basé sur les couches physiques)



Architecture Générale :



Conclusion



- **Les propriétés** du debugger basé sur simulateur est comparé avec **deux méthodes de debugs matérielles**

- **Resultats :** Le debogger basé sur simulateur a un **profil de fonctions différent** de ceux basés sur le debugage matériel
  - Performance dégradée (plus lente)
  - Difficulté de modeliser l'ensemble de la plate forme

- Peut être un **remplacement**, mais les éléments de l'ensemble des outils devront être **optimisés** différemment d'aujourd'hui

Banc de test VHBR

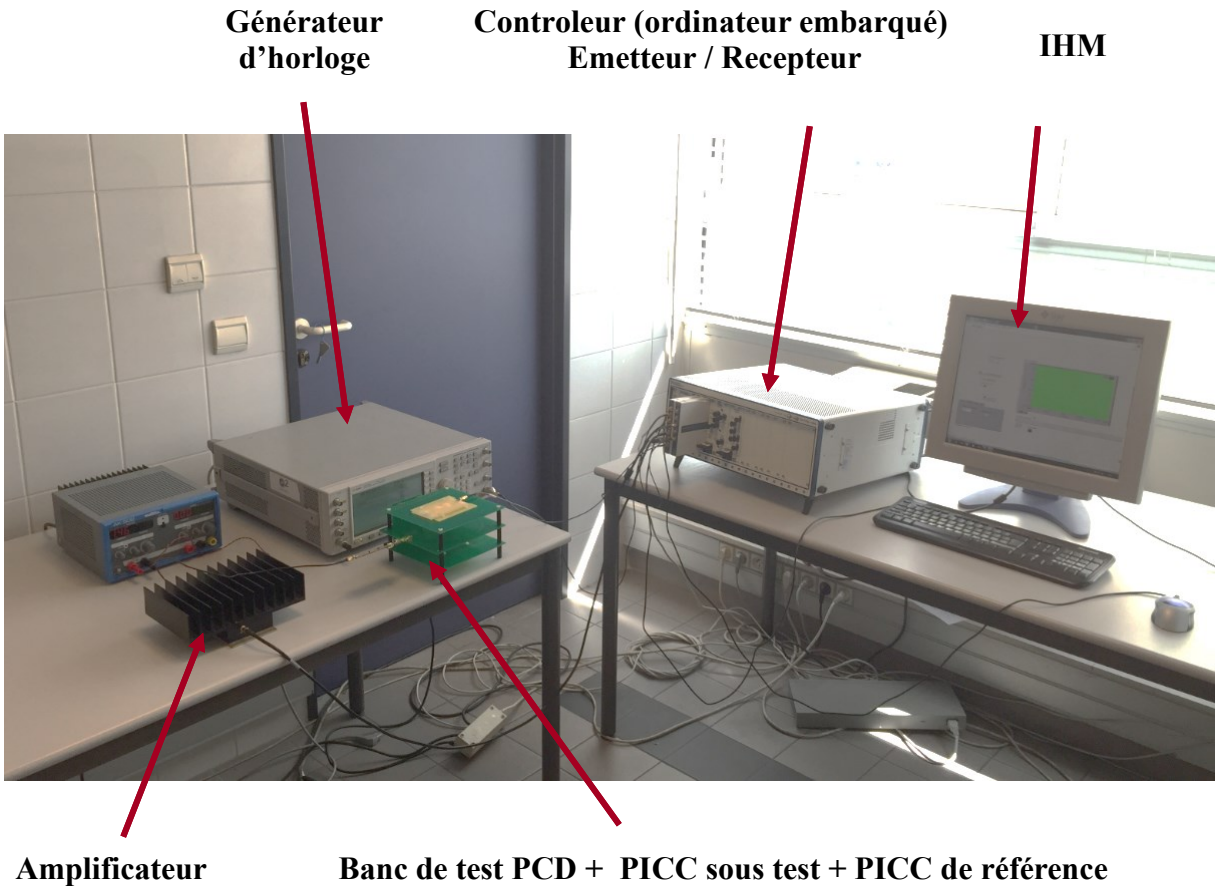
Description Générale

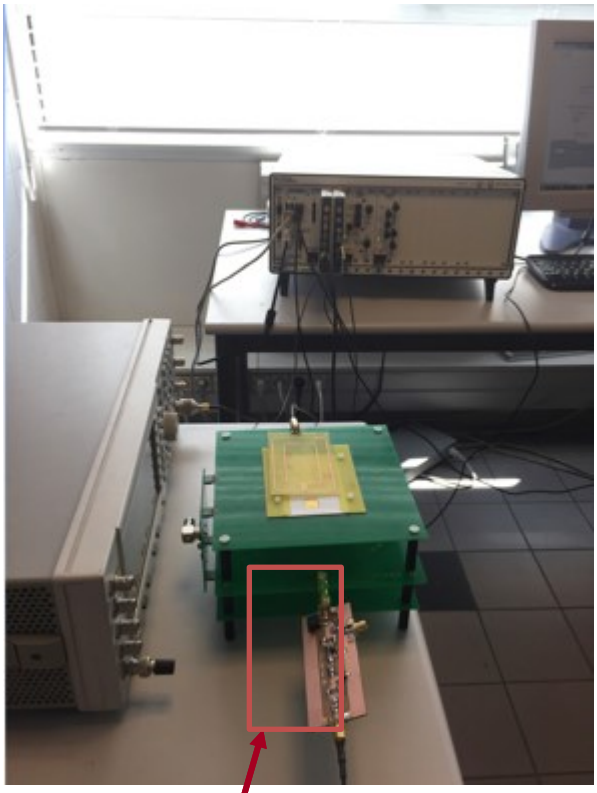
Objectif :

- Génèrer des trames VHBR avec le banc de test
- Evaluateur de lecteur avec un robot 5 axes
- banc de test de puce PICC

Communication VHBR avec le banc de tests

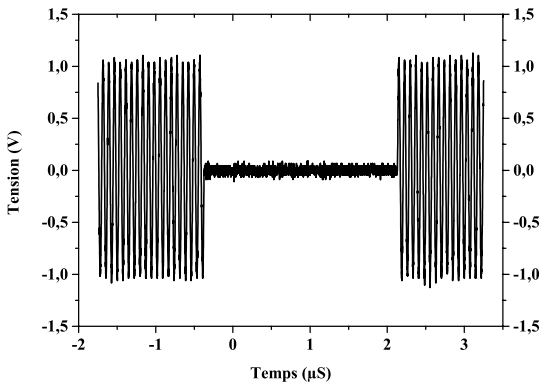
Architecture générale :





Réseau d'adaptation large bande

Fonctionnalités du banc de test:



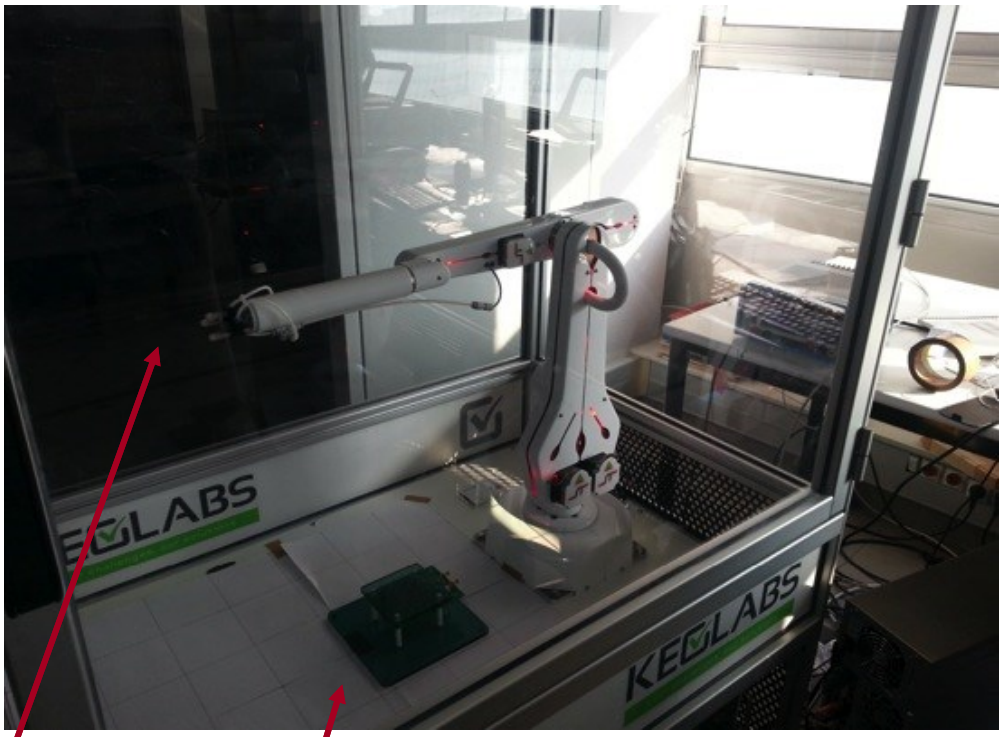
- Génère les signaux avec les caractéristiques voulues (temps de montée, profondeur de modulation, etc.)
- Démodules les réponses PICC
- Peux émuler les formes d'onde de PCD

Robot de test PCD 5 axes

Objectif :

- **Robot 5 axes** spécialement développé pour les **caractérisations sans contact**
- Les déplacements et le lecteur sont controlés par du **code python**
- Une interface graphique permet à l'utilisateur de **charger et effectuer les tests à la volée**.

Architecture globale :



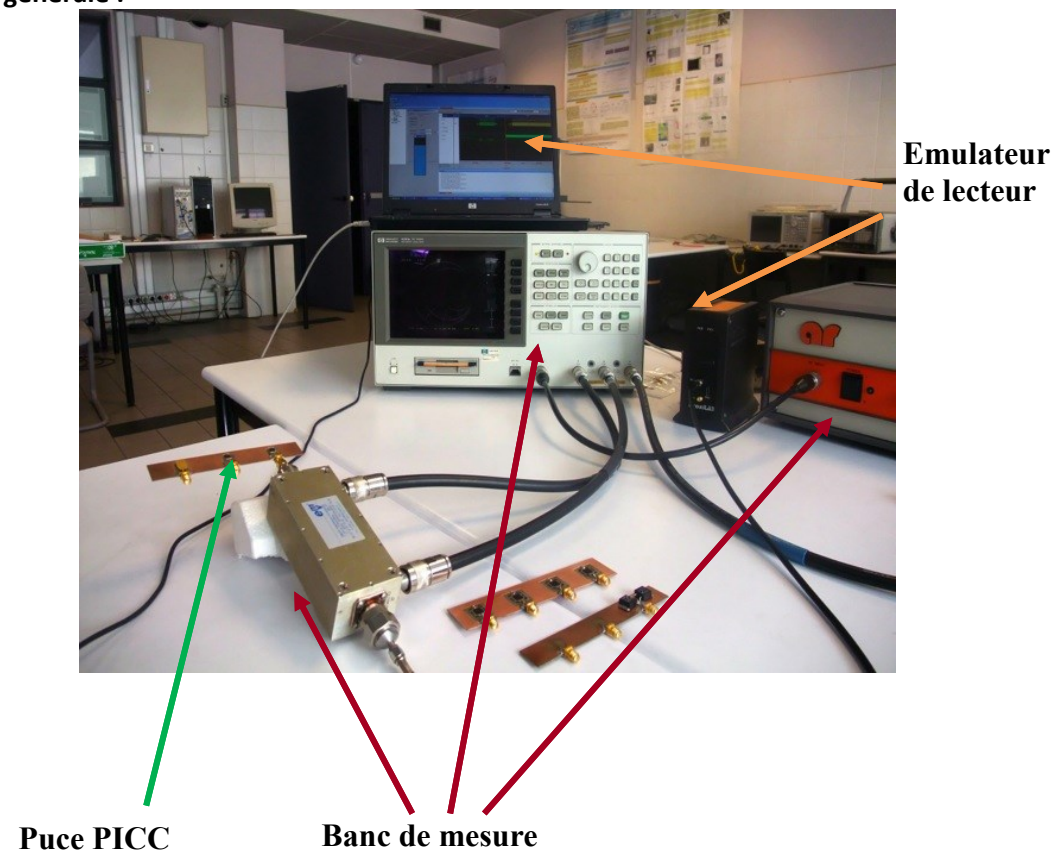
PICC reference **PCD sous test**

Fonctionnalités du banc de test:

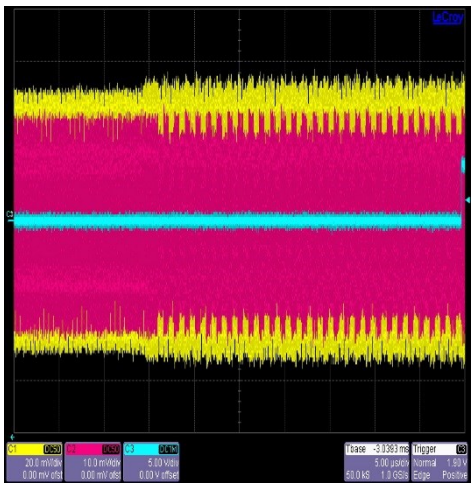
- Gère avec precision le placement des PICC
- Communique avec un lecteur grâce au protocole PCSC
- Permet d'évaluer le volume opératoire d'un lecteur

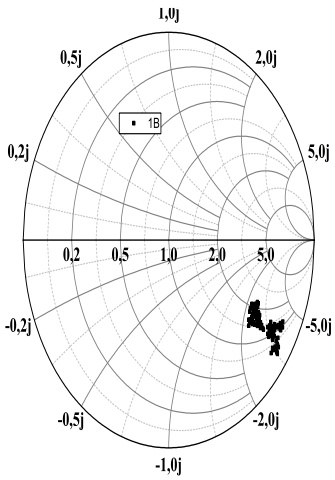
Banc de test de puce

Architecture générale :



Fonctionnalités du banc de test :





- Mesure les impédances de puces sur une large gamme de puissance
- La vitesse d'analyse permet de mesurer l'impédance d'une puce lors d'une communication
- Evalue la consommation d'une puce lors de l'analyse d'une trame PCD.

6.6. SP6 – Securité

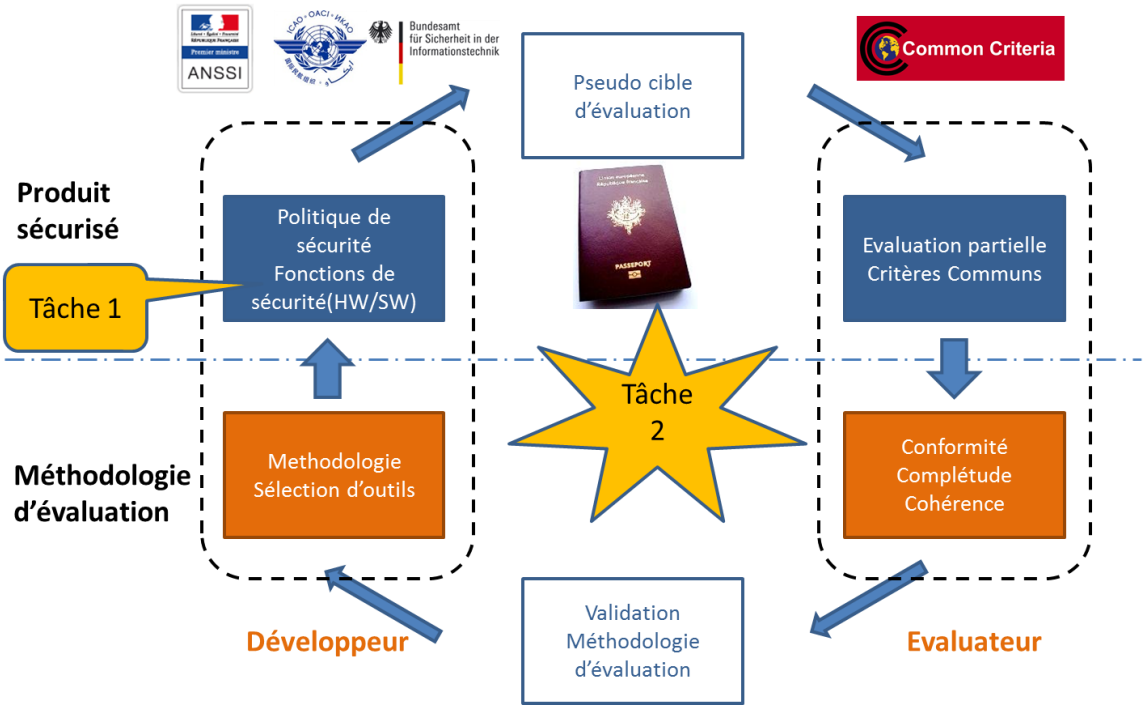
6.6.1. Introduction

Coordinateur	**CEA-Leti**
Partenaires	EVO, Gemalto, G&D, IFX, IFAT, ISEN, IT, NXP-A, NXP-G, ST, TUG-IAIK
Objectifs	L'objectif de ce sous-projet est de réaliser toutes les études transverses nécessaires à ce que les plates-formes issues du projet NewP@ss puissent atteindre le plus haut niveau de sécurité requis par l'OACI, l'UE et d'autres organismes de réglementation internationaux pour supporter les applications cibles. En particulier les MCU pour la 3ème et 4ème génération de passeports électroniques avec mise en œuvre du protocole SAC seront étudiés, en vue de leur future certification dans le cadre des Critères Communs et selon les profils de protection existants ou à venir. Au-delà du travail de R & D réalisé par les SP3, SP4 et SP5 sur les fonctionnalités de base, matérielles et logicielles, il est de la plus haute importance de développer des protections spécifiques contre les attaques malveillantes et de les tester. Le but de ce sous-projet est premièrement d'identifier les vulnérabilités et les menaces potentielles, et, deuxièmement, de spécifier, développer et valider les fonctions de sécurité de la future plate-forme de passeport 3G et 4G.

Ce SP est divisé en deux tâches clés :

- **Tâche 1:** *Fonctions de sécurité intégrées pour l'authentification et préservant la vie privée (développement de protections avancées pour un cycle de vie du MCU sécurisé supérieur à dix ans: Optimisation des algorithmes cryptographiques retenus, intégrité des plates-formes 32 bits, évaluation des schémas de signature de groupe, anonymat et technologies de protection de la vie privée, nouvelles fonctions de sécurité intégrées, gestion des certificats et de la PKI)*

- **Tâche 2:** *Gestion des risques et évaluation de la sécurité (certification au plus haut niveau de sécurité: gestion des risques pour l'analyse de la sécurité de base des plates-formes cibles, méthodologie formelle pour la génération automatique de certains documents requis par les Critères Communs, évaluation sécuritaire partielle pour l'évaluation de la méthodologie)*



6.6.2. Activités par périodes et partenaires

2012:

Gemalto
Gemalto a travaillé sur la tâche T6.1 et optimiser l'efficacité des protocoles cryptographiques nécessaires aux futures générations de passeports électroniques.

STMicroelectronics :
Pas d'activité

CEA-Leti (SP coordinateur)
Activité technique non démarrée. Tâche de coordination du SP6 démarrée.

ISEN-Toulon
Pas d'activité.

IFX
IFX a commencé l'analyse des différentes solutions candidates pour la protection de l'intégrité des données au cours du stockage, du transport et de l'exploitation des plates-formes de contrôleurs sécurisés 32 bits. Les évaluations des contributions potentielles des composants matériels à la mise en œuvre du SAC pour la 3G génération de passeports électroniques ont été réalisées et de leur impact sur la sécurité a été étudié.

Giesecke & Devrient
G&D a commencé l'analyse de la sécurité de la mise en œuvre du SAC pour la 3e génération de passeports électroniques.

NXP-G

Pas d'activité.

IFAT
IFAT a commencé l'analyse des schémas de signature de groupe anonyme en se basant sur les premiers résultats fournis par TU Graz / IAIK, et en prenant surtout en compte le nombre de multiplications de points de courbe elliptique nécessaires. Ces schémas ont également été évalués sous l'aspect des opérations d'appairement nécessaires et si ces opérations coûteuses doivent être effectuées à l'intérieur du contrôleur de sécurité ou non.

NXP-A
NXP-A a commencé à évaluer les méthodes et les outils de modélisation pour les hauts niveaux de certifications des Critères Communs. Les premières ébauches de modèles sont en cours de conception.
Grâce à un financement national NXP-A ne contribue plus à la tâche 1.4, mais contribuera à la tâche 2.2.

TU Graz / IAIK
Dans le SP6, TU Graz/IAIK a commencé à travailler sur les méthodes de préservation de la vie privée. En particulier, différents schémas de signature de groupe ont été comparés par rapport à leurs coûts de mise en œuvre en termes de performances et de leurs tailles de signature. En outre, TUG a commencé à mettre en œuvre le candidat le plus prometteur sur une plate-forme de prototype RFID.

Evoleo
Evoleo a commencé l'évaluation des schémas de PKI existants en fonction des demandes futures, des cas d'utilisation, et en particulier sur la recherche sur les exigences supplémentaires dues à l'aspect multi applications de la 4G.

IT
IT a commencé les travaux de recherche sur des solutions de gestion de clés sécurisées qui répondent efficacement pour la gestion des clés des autorités de certification, pour les clés d'authentification active et contre les attaques de déni de service. Une attention particulière a été accordée aux normes et activités de l'OACI. Un état de l'art sur des sujets pertinents connexes sera bientôt entrepris, à savoir sur les menaces de clonage liées au circuit intégré, sur les authentifications passive et active, et également sur les menaces à la vie privée liées à l'écoute des communications non protégées de la puce , et par utilisation des attaques par force brute sur communications cryptées du circuit intégré.

2013:

CEA-Leti (SP coordinateur)
Le CEA-Leti a continué à travailler sur les méthodes formelles et a débuté une étude sur la possibilité de réduire la charge de travail de l'évaluation formelle et le besoin de spécialistes qualifiés de très haut niveau pour les développeurs, les évaluateurs et les certificateurs, tout en restant cohérent et compatible avec les exigences des Critères Communs.
En poursuite de la collaboration avec le SP2, les spécifications des exigences pour l'évaluation de la sécurité des prochaines générations de passeports électroniques (3G / 4G) ont été abordées, avec un accent mis particulièrement sur la 4G.
Le CEA-Leti en tant que coordinateur du SP a également géré la coordination de la rédaction et de l'édition du livrable D6.1.1.

Gemalto

Gemalto a continué à travailler sur la tâche T6.1 pour optimiser les performances des protocoles cryptographiques du standard (SAC, EAC). Les contributions sur les aspects de la vie privée ont aussi été lancées.

Sur T6.1, Gemalto a travaillé principalement sur les tâches suivantes:

- Analyse de l'état de l'art, évaluation des références existantes et des recherches sur la protection de la vie privée
- Étude de l'évaluation Critères Communs et protection de la vie privée
- Premiers résultats dans le cadre GlobalPlatform concernant la vie privée
  - o Principe mix-and-match pour les plates-formes multi-applicatives
  - o Définition du cadre de base de la protection de la vie privée et architecture associée
- Définition des objectifs de sécurité du passeport électronique 3G
  - o Amélioration de l'OS de la plate-forme pour atteindre au moins le niveau EAL4 + en accord avec le profil de protection PP-SUN Open Configuration
  - o Applications logicielles du passeport électronique EAC / SAC certifiées au niveau EAL4 + selon les profils de protection PP-MRTD-EAC et PP-MRTD-SAC
  - o Mise en œuvre de contre-mesures de sécurité à l'état de l'art sur la plate-forme SW du passeport électronique 3G
- Définition de nouvelles fonctions intégrées de sécurité pour le passeport électronique 4G (cible pour 2015)
  - o Définition des objectifs de sécurité du passeport 4G, y compris de nouveaux mécanismes de confidentialité et LDS2
  - o OS de la plate-forme amélioré et certifié pour atteindre au moins le niveau EAL4 + et peut-être plus
  - o Applications logicielles du passeport électronique avec EAC / SAC certifiés au niveau EAL4 + ou plus
  - o Contribution à l'analyse de l'évaluation des risques par rapport aux attaques invasives ou non invasives potentielles
  - o Evaluation de la plupart des techniques de gestion des certificats compatibles avec les schémas multi-applications
- Les cibles de sécurité correspondantes au passeport 3G ont été diffusées sur le site français de l'ANSSI

ST

En 2013 ST a travaillé principalement sur la tâche 1, sur des études en cours pour améliorer l'efficacité et la sécurité des accélérateurs matériels AES de nouvelle génération. Certains travaux ont été entrepris aussi pour l'utilisation de courbes elliptiques adaptées à la cryptographie dans le contexte du passeport électronique.

En parallèle, un travail plus profond a été fait sur l'intégrité des plates-formes 32 bits, avec un accent sur l'intégrité du code. Un mécanisme matériel spécifique de traitement temps réel a été étudié pour la signature et la vérification des points de vérification locaux et globaux. Ceci afin de détecter (et de réagir) en temps réel en cas de perte dans l'intégrité du code / des données en cours d'exécution. Ce travail se poursuivra avec une mise en œuvre et une validation dans le cadre du SP3.

ISEN-Toulon

Pas d'activité.

IFX

IFX a réalisé l'analyse des différents candidats pour la protection de l'intégrité des données au cours du stockage, du transport et de l'exploitation des plates-formes de microcontrôleurs sécurisés 32 bits. L'accent est mis sur les possibilités d'accès à la puce par des pays tiers par rapport aux contraintes de protection de

la vie privée.

Giesecke & Devrient
G&D a travaillé sur les mécanismes de sécurité qui peuvent être utilisés par un dispositif implémentant un Trusted Execution Environment (TEE) pour communiquer avec un élément sécurisé tel un passeport électronique. Les cas d'utilisation principaux sont l'affichage des données sécurisées et l'obtention des informations de l'utilisateur comme les codes PIN. Les résultats de cette recherche font partie du livrable D6.1. La définition de l'API du canal sécurisé du TEE est actuellement pilotée par G&D au sein de GlobalPlatform.

NXP-G
Les activités concernant la recherche sur la sécurité et les algorithmes cryptographiques se poursuivent conformément au plan.
Des progrès satisfaisants ont été accomplis dans la sélection des candidats pour de nouveaux mécanismes de protection de la mémoire. Les résultats d'une étude interne sont disponibles et une recommandation claire pour les futures étapes d'industrialisation devrait être apportée.
Un autre sujet de discussion concerne les aspects de sécurité des logiciels embarqués (firmware), y compris les concepts de bootloader pour le chargement du code de programme dans la mémoire non volatile. Alors que le nouveau profil de protection Common Criteria BSI-PP-0084 établit certains termes de base et les conditions aux limites, beaucoup de travail reste à faire dans la définition des mesures de sécurité adéquates pour la reconfiguration et le chargement post-délivrance du code et des données.

IFAT
IFAT a fait l'analyse des schémas de signature de groupe anonymes qui se basent sur les premiers résultats de TU Graz / IAIK, en particulier en tenant compte du nombre de multiplications de point de courbe elliptique nécessaires
.

NXP-A
Dans le SP6, NXP-A a continué l'évaluation des méthodes et des outils de modélisation. Sur la base des résultats d'une première évaluation, une méthodologie pour la conception par modèles formels a été développée en vue des certifications de sécurité selon les Critères Communs de haut niveau. En outre, NXP-A a commencé à travailler sur la modélisation formelle de l'OS et sur la sécurité de l'application et la génération automatique de documents en étroite collaboration avec IAIK / TU Graz. Le premier projet d'un modèle pourrait être vérifié pour satisfaire aux exigences de sécurité énoncées dans la cible de sécurité. Une partie du travail a été présenté à l'IECON 2013.

TU Graz / IAIK
Dans le SP6, IAIK / TU Graz a poursuivi ses recherches dans le domaine des technologies de l'amélioration de la confidentialité. Plus précisément, ont été implémentés deux schémas de signature de groupe basés sur un concept d'appairement. TUG/IAIK a commencé à mettre en œuvre et à optimiser le calcul d'appairement afin de répondre aux exigences des dispositifs RFID. En outre, IAIK / TUG a travaillé en étroite collaboration avec NXP Autriche sur la préparation de l'évaluation Critères Communs EAL6. Cela comprend l'élaboration d'un modèle formel et la génération automatique de documents.

IT
IT a réalisé une recherche sur des solutions sécurisées de gestion de clés qui répondent efficacement aux besoins des Autorités de Certification de clés, aux clés d'authentification active, aux clés des signataires de

documents, aux attaques de déni de service, à la gestion de certificats, aux Autorité de Certification des Pays signataires. Une attention particulière a été accordée aux normes et aux activités de l'OACI.
Une étude bibliographique sur d'autres sujets pertinents a également été réalisée, à savoir sur les menaces de clonage liées au circuit intégré, sur l'authentification passive et active, et également sur les menaces sur la vie privée liées à l'écoute de la communication non protégés de la puce et en utilisant des attaques par force brute sur les communications cryptées du circuit intégré. En outre, IT a lancé une recherche sur l'état de l'art sur les menaces cryptographiques, notamment sur l'implémentation des algorithmes mathématiques.
IT a contribué au livrable D6.1.1 en ce qui concerne l'évaluation des certificats du schéma PKI, particulièrement pour les implémentations de la 4G, compte tenu des solutions sécurisées de gestion des clés, comme étudié précédemment. Une attention particulière a été accordée aux normes et aux activités de l'OACI, et aussi aux recommandations pertinentes du BSI.
.

Evoleo
Evoleo a effectué l'évaluation des schémas de PKI existants compte-tenu des demandes des futurs cas d'utilisation, en particulier la recherche sur les exigences supplémentaires dues à l'aspect multi-applications de la plate-forme 4G.
Des contributions ont été rédigées pour le livrable D6.1.1, liées à l'infrastructure PKI, couvrant les principales entités de la PKI et les données échangés entre ces entités.
Les schémas de PKI ont été évalués sur le cadre des recommandations de l'OACI et du BSI.

2014:

CEA-Leti (SP coordinateur)
Durant l'année 2014, le CEA, en tant que coordinateur du SP6, a contribué à la coordination des séances de travail du SP6 lors des réunions du PTB et des conférences téléphoniques, et à la coordination de la finalisation du livrable D6.2.1 qui a été publié fin Juillet.
Les travaux techniques consacrés au développement de la méthodologie formelle ont été réalisés en collaboration avec NXP-A en tant que développeur. Le CEA-Leti, en tant que centre d'évaluation de la sécurité, a validé la démarche par vérification de modèle proposée par NXP-A pour la conception de la puce sous méthodologie formelle. Cette méthodologie constitue une avancée majeure pour réduire les coûts de développement et d'évaluation, tout en préservant la confiance apportée par les techniques formelles. Pour évaluer cette méthodologie dans le schéma des Critères Communs, le CEA-Leti a travaillé avec l'organisme de certification français, l'ANSSI, pour valider le processus de certification complet.
Des travaux préliminaires ont également été entamés avec Gemalto sur la méthodologie de composition à utiliser pour traiter la certification sécuritaire des futurs passeports électroniques3G et 4G, en tant que nouvelles plates-formes ouvertes pour les applications gouvernementales et privées.

Gemalto
Gemalto a contribué au livrable D6.2.1 sur les aspects évaluation sécuritaire des OS des passeports 3G.

ST
ST a évalué les aspects de sécurité concernant l'intégrité des données / code des circuits plus spécifiquement en introduisant des mesures qui permettent de définir un niveau mesurable de l'intégrité ainsi que les statistiques associées.

ISEN-Toulon

L'ISEN a travaillé pour le livrable D6.2.1 sur la partie gestion des risques des plates-formes cibles.
L'ISEN a commencé à travailler sur une plate-forme dédiée à la communication VHBR pour la mesure de l'immunité vis-à-vis d'un déni de service provoqué par un brouillage RF.

IFX
IFX a fait l'analyse des différents candidats pour la protection de l'intégrité des données au cours du stockage, du transport et de l'exploitation des plates-formes de microcontrôleurs sécurisés 32 bits. L'accent est mis sur l'accès via l'interface sans contact de la puce par un pays tiers par rapport aux contraintes de la vie privée.

Giesecke & Devrient
La définition de l'API du canal sécurisé de la TEE est arrivée à maturité; la plupart des commentaires formulés ont été traités avec succès. Le concept d'évaluation de la plate-forme 3G et 4G a été mis en place en interne.

NXP-G
Les activités concernant les travaux sur les algorithmes cryptographiques et de sécurité ont été achevées en ce qui concerne le projet pour NXP-G. Les travaux concernant les aspects de sécurité des logiciels embarqués ont encore progressé. Ceci inclut les méthodes d'authentification pour le boot loader de la mémoire flash. Un aspect particulièrement intéressant était le compromis entre la taille du bootloader, le renforcement de la sécurité et la performance. Selon le cas d'utilisation de la cible et de l'environnement, des solutions architecturales très différentes peuvent en résulter.

IFAT
IFAT a poursuivi ses analyses des systèmes de signature de groupe anonyme, en particulier par rapport à l'impact sur la sécurité du matériel pour la préservation de la vie privée

NXP-A
NXP-A a poursuivi ses travaux sur la méthodologie formelle pour la conception de puces pour préparer l'évaluation de sécurité de plus haut niveau des Critères Commons. NXP-A a proposé un exemple pour une pseudo évaluation de la politique de sécurité Critères Communs au CEA-Leti afin d'évaluer la méthodologie formelle utilisée par NXP-A et de vérifier la pertinence et la cohérence du vérificateur de modèle par rapport à des approches fondées sur la preuve de théorème. NXP-A a évalué en outre l'utilisation du modèle formel de la politique de sécurité dans le processus de développement, par exemple, dans le test.

TU Graz / IAIK
Dans le SP6, IAIK / TU Graz a terminé la recherche sur les technologies d'amélioration de la confidentialité. Un bloc de traitement de base pour améliorer la performance de la révocation à l'appartenance au groupe dans le cadre de schémas de signature de groupe a été publié à l'ISC 2014. Ce bloc permet à une autorité compétente de relier deux signatures de groupe.
En outre, le travail publié à CHES 2014 a servi de base pour l'étude de faisabilité afin d'examiner l'applicabilité des schémas de signature de groupe sur les dispositifs contraints. Cette étude de faisabilité a été réalisée sur un ARM Cortex M0 + @ 6,78 MHz.
De plus, TUG a montré la faisabilité de résoudre le problème du logarithme discret d'un 113-bit Koblitz Curve avec une mise en œuvre de FPGA à grande vitesse. Les résultats correspondants ont été publiés au SAC 2,014.

IT
IT a affiné sa contribution au livrable D6.1.1, en ce qui concerne l'évaluation des certificats et des schémas de PKI, en particulier pour les implémentations 4G concernant des solutions sécurisées de gestion de clés qui répondent efficacement aux clés des Autorités de Certification, aux clés des authentifications actives, des signataires de documents, aux attaques par déni de service , à la gestion des certificats, aux autorités de

certification des états et aux clés de signature et de révocation de documents.
IT a également contribué au livrable D6.2.1, en ce qui concerne l'évaluation des certificats PKI et schémas associés, en particulier pour la 4G, afin de pouvoir servir de référence pour les deux derniers livrables. En outre, il a inclus l'évaluation des menaces / analyse dans sa contribution, en utilisant le "Microsoft Threat Modeling Tool", en modélisant les scénarios décrits dans le livrable D2.1 pour les applications 3G / 4G. La modélisation des menaces est une technique de modélisation de sécurité centrée sur l'identification des menaces potentielles ainsi que sur la détermination des techniques de protection appropriées pour lutter efficacement contre les menaces identifiées. Une illustration d'un modèle de menace a été élaborée dans ce cas pour le démonstrateur aéroport 3G.
Outre la modélisation et l'analyse de la menace, IT a effectué l'identification des menaces et des attaques principales, telles que le skimming, le clonage, l'usurpation d'identité, l'écoute, la lecture non autorisée de la puce, la modification de la puce, et le déni de service. Les principales solutions envisagées sont: Puces non traçables; Authentification passive; Authentification active; Contrôle d'accès de base (BAC); et extension du contrôle d'accès (EAC).
Après avoir déjà fait une recherche sur la technologie PKI pour le passeport électronique, y compris sur l'état de l'art des principes fondamentaux de la PKI et de la PKI de l'OACI, IT a conçu une solution de PKI pour passeport électronique 4G, qui est mise en œuvre dans le cadre du SP4, et sera démontrée dans le champ d'application de SP7.

Evoleo
Evoleo a continué à faire l'évaluation exhaustive des schémas de PKI existants en fonction des demandes futures pour certains cas d'utilisation, en particulier concernant la recherche sur les exigences supplémentaires dues à l'aspect multi- applications de la 4G.
De nouvelles contributions ont été apportées pour le livrable D6.1.1, liées à l'infrastructure PKI, et couvrant les principales entités de la PKI et les informations échangées entre ces entités.
Les schémas de PKI ont été évalués sur le cadre des recommandations de l'OACI et BSI.

2015:

Cea-Leti (SP coordinateur)
Au cours l'année 2015, le CEA, en tant que coordinateur du SP6, a contribué à la coordination des séances du SP6 dans les réunions PTB et les conférences téléphoniques, et à la coordination de la finalisation des deux derniers livrables du SP6, D6.1.2 et D6. 2.2, qui ont été publiés fin juin. Il a aussi contribué aux présentations du SP6 au cours de la revue CATRENE du 17 juin et de la revue DGE du 26 novembre.

Des résultats techniques consacrés au développement de la méthodologie formelle ont été obtenus en collaboration avec NXP-A en tant que développeur. Le CEA-Leti comme centre d'évaluation de la sécurité, a validé la démarche de vérification de modèle proposé par NXP-A pour la conception de la puce avec une méthodologie formelle. Cette méthodologie constitue une avancée majeure pour réduire les coûts de développement et d'évaluation, tout en préservant la confiance apportée par les techniques formelles. Pour évaluer cette méthode, dans le schéma Critères Commons, le CEA-Leti a collaboré avec l'organisme de certification français, l'ANSSI, pour valider le processus de certification complet. Après plusieurs discussions avec des experts techniques de l'ANSSI pendant les premiers mois de 2015, l'organisme de certification français a finalement accepté et validé cette méthodologie pour le niveau de sécurité le plus élevé dans le cadre du système d'évaluation Critères Commons : EAL7. Ainsi, une certaine harmonisation au niveau des Critères Communs pour les organismes de certification allemands et français a été réalisée pour le plus haut niveau de certification.

Les travaux ont également continué avec Gemalto sur la méthodologie de composition à utiliser pour traiter l'évaluation sécuritaire des passeports électroniques 3G et 4G, en tant que nouvelles plates-formes ouvertes pour les applications gouvernementales et privées. Les conclusions de cette étude préliminaire montrent que beaucoup de travail de spécification et de normalisation reste à entreprendre au niveau de tous les acteurs afin de clarifier et d'introduire de la cohérence et de la compatibilité entre les schémas de certification publics et privés pour le passeport électronique 4G multi-application.

Gemalto
Gemalto a contribué au livrable D6.2.1 sur les aspects évaluation sécuritaire pour les passeports électronique de 4ème génération.

ST
Les travaux de ST concernant l'intégrité du code et des données ainsi que les métrique associées ont été achevés.

ISEN-TOULON
L'ISEN a travaillé sur le livrable D6.2.1. La contribution ISEN concerne la gestion des risques des plates-formes cibles.
L'ISEN a achevé ses travaux sur le développement d'un banc de test dédiée à la communication VHBR et à sa sensibilité au déni de service par brouillage RF.

IFX
Pas d'activité en 2015

G&D
Pas d'activité en 2015

NXP-G
Au cours de la période considérée, les activités de clôture ont été menées. Les résultats ont été archivés et indexés pour diffusion interne et industrialisation éventuelle.

IFAT
IFAT a poursuivi ses analyses des systèmes de signature de groupe anonymes, en particulier par rapport à l'impact sur la sécurité du matériel pour la préservation de la vie privée.

NXP-A
NXP-A a poursuivi ses travaux sur la méthodologie formelle de la conception de puces pour préparer les plus hauts niveaux d'évaluation sécuritaire des Critères Communs. NXP-A a proposé un exemple pour une pseudo évaluation de la politique de sécurité Critères Communs au CEA-Leti afin d'évaluer la méthodologie formelle utilisée par NXP-A et vérifier la cohérence et la cohérence de vérificateur de modèle plutôt que des approches fondées sur les preuves de théorèmes. NXP-A a évalué en outre l'utilisation du modèle formel de politique de sécurité dans le processus de développement, par exemple, dans le test.

TU Graz / IAIK
IAIK / TU Graz a terminé ses travaux concernant le SP6 à la fin de l'année 2014.

IT
IT a contribué au livrable D6.2.2, sur l'analyse de la sécurité de la communication entre le système

d'inspection et le signataire du LDS2 dans le schéma PKI de la signature numérique du LDS2.
La signature numérique PKI LDS2 est utilisée par l'État signataire pour assurer l'intégrité et l'authenticité des trois types d'objets LDS2 de données (c'est-à-dire visas de séjours, tampons électroniques et données biométriques supplémentaires) qu'il écrit dans les documents de voyages électroniques par le biais de ses propres systèmes d'inspection autorisés (SI).
L'analyse de la sécurité informatique est axée sur la communication entre une machine d'inspection autorisée située dans un aéroport de l'état signataire, et le signataire du LDS2 de l'état signataire.

En raison de la vulnérabilité du protocole standard SSL / TLS, la communication entre le SI et le signataire du LDS2 peut être une cible intéressante pour les cybercriminels contre les applications de passeports 4G. L'analyse de la sécurité s'est focalisée sur les attaques potentielles de type Man-in-the-Middle (MITM) et les attaques par déni de service (DoS), les attaques contre la communication basée sur TLS SSL entre le SI et le signataire du LDS2.

Evoleo
Au cours de 2015, Evoleo a contribué au livrable D6.2.1 avec l'état de l'art des schémas de PKI et contribué à la mise en œuvre du PKI pour la démonstration SP7
.

6.6.3. Coopération

- **Interne SP6**
  - Bonne coopération en sessions plénières et surtout en bilatéral
  - Conférences téléphoniques plus techniques en complément des réunions PTB SP6
  - Réunions et travaux bilatéraux:
    - **NXP-A et TUG-IAIK** sur les méthodologies formelles pour la conception de puce
    - **NXP-A et CEA-Leti** sur les méthodologies formelles pour l'évaluation sécuritaire des puces
    - **Gemalto et CEA-Leti** sur l'évaluation en composition
    - **IFX et ST** sur l'intégrité des plates formes 32 bits
    - **IAIK et IFX** sur les signatures de groupe
    - **IT et Evoléo** sur la PKI

- **Avec les autres SPs**
  - **SP2:** Contribution aux spécifications des évaluations sécuritaires
  - **SP2:** Alignement avec les besoins et les spécifications proposées
  - **SP3 and SP4:** Alignement en fonction des primitives cryptographiques, des protocoles d'authentification et des aspects certification (HW and SW)
  - **SP5:** Banc d'essais pour validation de vulnérabilités
  - **SP8:** Propositions pour standardisation

6.6.4. Résultats obtenus

Livrables:

Livrable	Tâche	Statut T4 15	Echéance (Last FPP)	Titre
D6.1.1	T1	Livré	T4-13	Specific cryptographic specifications available Flexible privacy architecture
D6.1.2	T1	Livré	T3-15	New embedded protections for security enhancement
D6.2.1	T2	Livré	T2-14	Formal methodology for certification available and Critical paths for formal evaluation identified (4G)
D6.2.2	T2	Livré	T3-15	Platform qualified for evaluation

Principaux résultats:

Tâche 6.1 Fonctions de sécurité embarquées pour l'authentification et la protection des données privées

T1.1 Optimisation des algorithmes cryptographiques

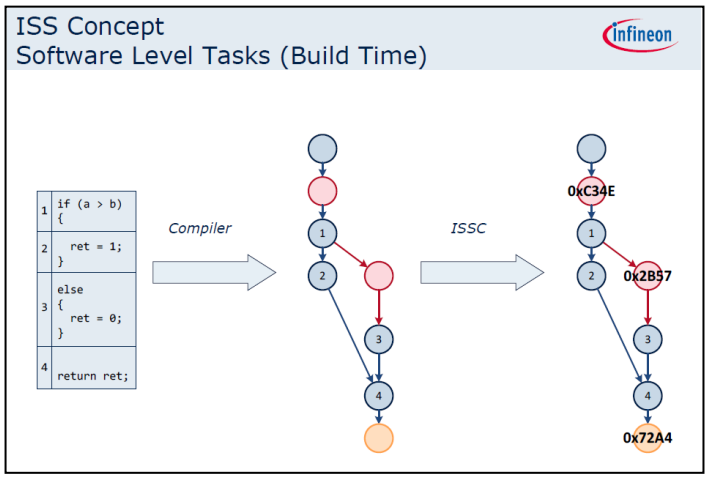
- ✓ **NXP-G**
  - Optimisation continue de l'implémentation des algorithmes pour réduire la consommation et accélérer les temps de calcul
  - Sécurisation des téléchargements de logiciels embarqués après délivrance
- ✓ **TUG-IAIK**
  - Implémentation efficace des courbes elliptiques (ASM)
  - Performance des multiplications sur différents MCU
- ✓ **GTO**
  - Optimisation SW/HW des variantes du protocole PACE
  - Analyse des contremesures avec/sans authentification du terminal

Processor	Version	Program Memory [Bytes]	Data[a] Memory [Bytes]	Chip Area ROM [GE]	Chip Area RAM [GE]	Chip Area Core [GE]	Chip Area Total [GE]	Power @10 MHz [µW]	Energy [µJ]	Runtime @10 MHz [ms]
secp160r1										
ATmega	ASM	8,358	402	11,807	3,754	6,140	21,701	545	503	923
MSP430	ASM	4,788	290	7,796	3,250	7,003	18,048	583	337	578
CortexM0+	ASM	4,256	404	8,270	4,308	15,262	27,840	718	202	281
ATmega	ISE	5,828	402	8,202	3,754	7,039	18,995	666	218	327
MSP430	ISE	3,898	286	6,363	3,225	7,197	16,786	794	194	245
CortexM0+	ISE	3,088	408	6,416	4,334	18,700	29,450	1,306	161	123
secp192r1, NIST P-192										
ATmega	ASM	10,238	462	11,807	4,107	6,140	22,054	556	839	1,509
MSP430	ASM	5,408	330	8,202	3,475	7,003	18,679	581	533	918
CortexM0+	ASM	4,860	448	8,270	4,560	15,262	28,092	716	329	459
ATmega	ISE	6,564	462	10,040	4,107	7,039	21,186	670	336	502
MSP430	ISE	4,142	330	7,796	3,475	7,197	18,468	801	283	353
CortexM0+	ISE	3,164	444	6,416	4,535	18,700	29,652	1,318	241	183
secp224r1, NIST P-224										
ATmega	ASM	12,570	526	15,484	4,485	6,140	26,109	571	1,326	2,321
MSP430	ASM	6,294	374	10,040	3,750	7,003	20,792	584	819	1,403
CortexM0+	ASM	5,672	496	8,270	4,838	15,262	28,369	716	496	693
ATmega	ISE	7,600	526	10,040	4,485	7,039	21,564	664	500	754
MSP430	ISE	4,588	370	7,796	3,725	7,197	18,718	805	419	521
CortexM0+	ISE	3,352	492	6,416	4,812	18,700	29,929	1,330	334	251
secp256r1, NIST P-256										
ATmega	ASM	16,112	590	17,029	4,838	6,140	28,006	548	1,914	3,493
MSP430	ASM	8,378	418	11,878	4,000	7,003	22,881	580	1,286	2,217
CortexM0+	ASM	7,168	540	10,123	5,089	15,262	30,475	719	771	1,073
ATmega	ISE	9,596	590	11,807	4,838	7,039	23,684	655	779	1,190
MSP430	ISE	6,168	416	10,040	3,975	7,197	21,212	791	717	907
CortexM0+	ISE	4,124	536	8,270	5,064	18,700	32,034	1,339	546	408

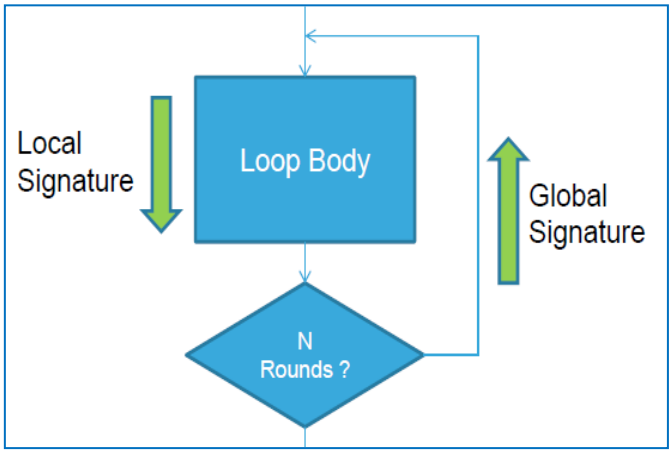
[a] Including Stack.

T1.2 Intégrité de la plate forme 32 bit

- ✓ **IFX**
  - Intégrité du code par Instruction Stream Signatures (ISS)
  - Intégrité des données par combinaison de chiffrement mémoire et de mécanismes de redondance
  - Protection des chemins de données: détection d'erreurs, correction d'erreurs et chiffrement temps-réel



- ✓ **ST**
  - Conception et implémentation d'une protection mémoire unifiée.
    - Niveau de protection identique pour tous les types de mémoire (R/W ECC).
    - Niveau de protection évolutif et implémentation personnalisée
    - Accès mémoire sécurisé de bout-en-bout:
      En conjonction avec Enhanced Code Signature (ECS)
  - Concept intégré sur silicium



T1.3 Signatures de groupe

- ✓ **IFAT et TUG-IAIK**
  - Implémentation optimisée de l'appairement (bloc de base)
  - Implémentation SW (optimisée sur Cortex-M0+)
  - Extension HW (multiplication-accumulation MAC)
  - Concept « Drop-in » (entre CPU et RAM)

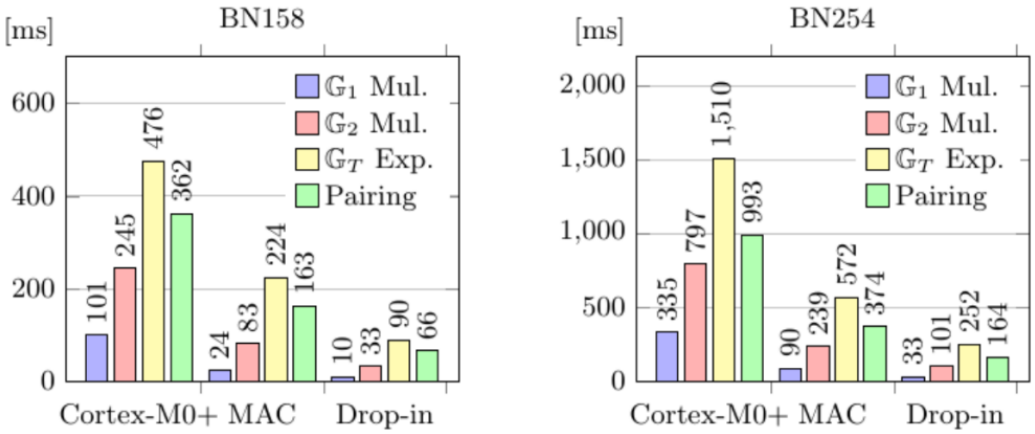
  - Performance avec implémentation optimisée (ARM Cortex M0+ sur Xilinx Spartan-3 FPGA @ 6.78 MHz)

Signature generation with software implementation

Security Level	Curve	Execution Time
80-bit	158-bit BN curve	13.7 sec
128-bit	254-bit BN curve	43.1 sec

Signature generation with drop-in concept

Security Level	Curve	Execution Time
80-bit	158-bit BN curve	2.0 sec
128-bit	254-bit BN curve	5.5 sec

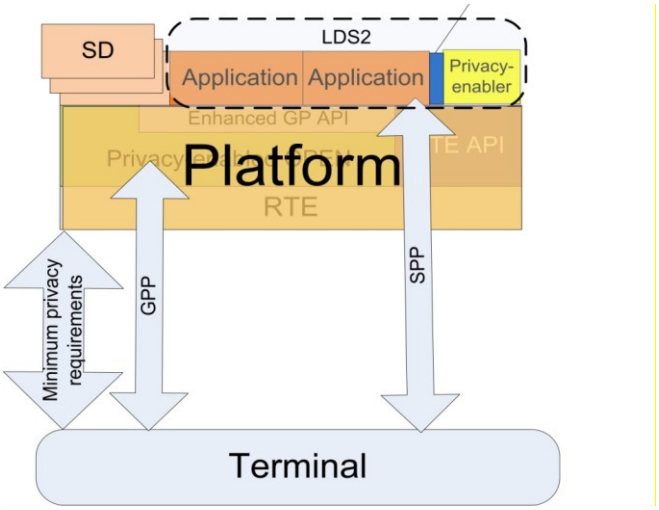


Group operations at 48 MHz

T1.4 Technologies pour anonymat et données privées

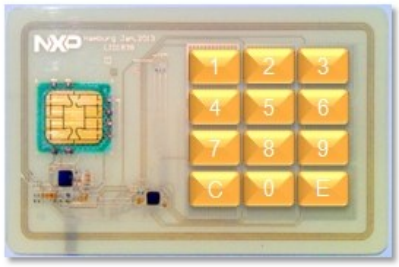
- ✓ **IFX/IFAT**
  - Etudes sur protocoles de type Attribute Based Encryption
  -
- ✓ **ST**
  - Analyse sur implémentation HW des algorithmes proposés
  - Objectif: exécution rapide avec sécurité de bout-en-bout

- ✓ **GTO**
  - Dans le contexte ISO SC17 WG4 :
    - Amélioration du protocole ERA/eIDAS avec un schéma de PIA générique (Annexe dédiée) applicable aux protocoles de protection des données privées decrits dans l'ISO/IEC 19286 (ICC protocols and services ensuring privacy).
    - ISO 7816 part- 8 et part-15 modifiées pour supporter les caractéristiques de protection des données privées du TR eSign
  - CEN : nouvelle initiative sur le Privacy by Design (PbD) :
    - CEN/CENELEC a décidé récemment de démarrer un nouveau comité CEN/CLC JWG 8 sur 'la gestion de des données privées dans les produits et les services'. Secrétariat AFNOR sous la responsabilité du CN SSI.
    - Participation de Gemalto à un sous-groupe dédié aux 'derived credentials' et aux protocoles ABC (Attribute Based Credentials) sous le CN SSI
  - ISO SC27 WG5:
    - Suivi et contribution au Privacy Framework series (i.e. ISO/IEC 29134 et ISO/IEC 29xxx) qui devrait correspondre à un nouveau projet de réglementation par la CE sur le 'Privacy by Design'
  - GlobalPlatform HW:
    - Minimum Privacy (noyau)
    - Global Privacy (plate forme entière)
    - Local Privacy (spécifique à l'application, ie LDS2)

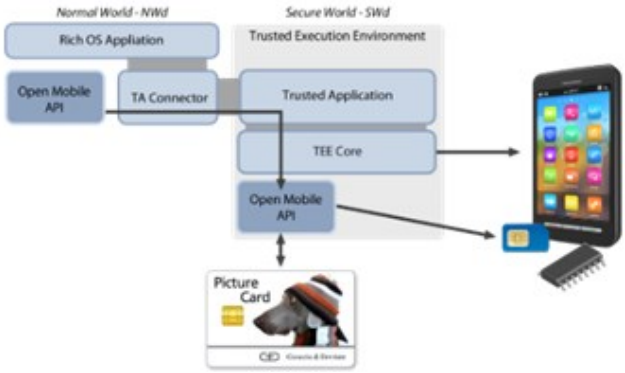


T1.5 Nouvelles fonctions de sécurité embarquées

- ✓ **NXP-G**
  - Matrice de capteurs embarquée sur carte pour amélioration de la sécurité
  - Capture du geste du porteur de la carte



- ✓ **G&D**
  - Le protocole du canal sécurisé entre un SE et un TEE a été défini.
  - Contribution à GlobalPlatform pour le (Secure Channel Protocol 11): Authentication, secure channel and commands

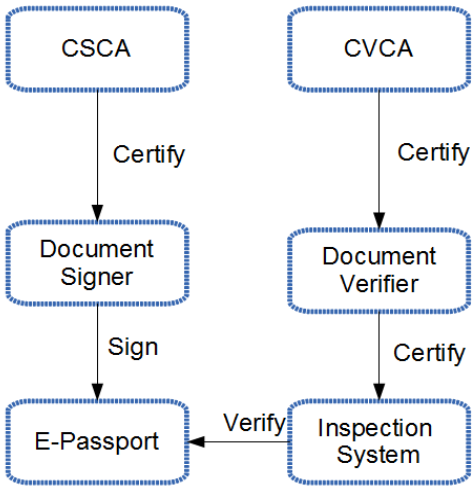


- ✓ **GTO**
  - Nouveau besoin d'authentification entre un passeport électroniqueet un terminal: (Sécurité/Privacy: authentification puce, untraceability, unlinkability, …)

T1.6 Gestion des certificats et PKI

- ✓ **IT+EVO**

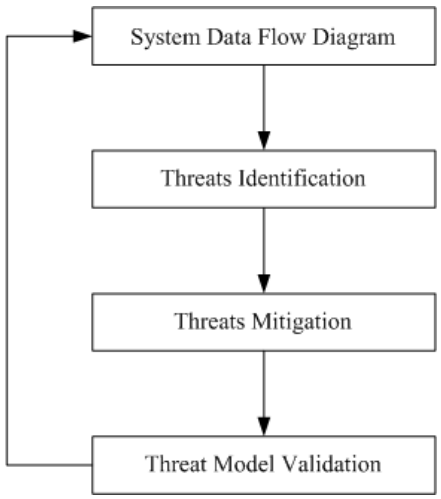
  - Etat de l'art en technologie PKI pour ePassport
  - Fondamentaux de la PKI
  - Analyse de l'état de l'art de la PKI ICAO
  - Conception d'une PKI pour ePassport 4G



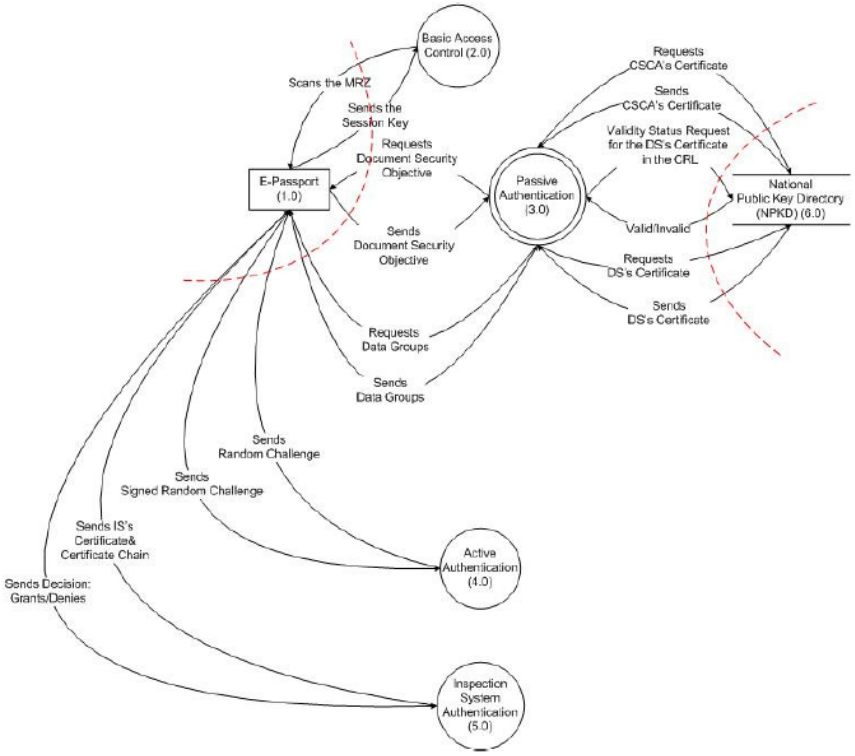
Tâche 6.2 Gestion des risques et évaluation sécuritaire

T2.1 Gestion des risques

- ✓ **NXP-G**
  - Gestion des risques pour attaques sur les blocs HW contrôlant l'exécution du code
  - Analyse des protections HW embarquées
- ✓ **IT+EVO**
  - Identification des principales menaces et attaques
    - Ecoute, clonage, Usurpation d'identité, lecture puce non autorisée, modification de la puce, déni de service
  - Identification des solutions de protection
    - Puce non traçable, authentification passive, authentification active, BAC, EAC
  - Modélisation des menaces et analyse sur un passeport électronique 3G (DFD)



  - Méthodologie générale



- Data Flow Diagram de l'application 3G aéroport.

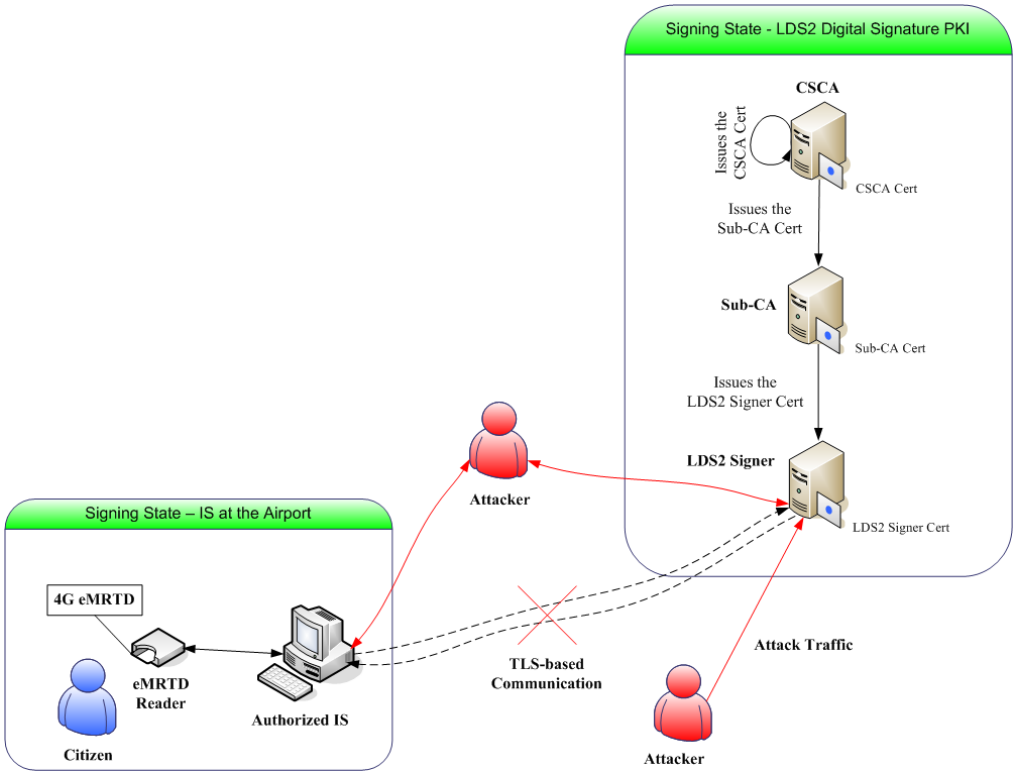
- Analyse de la sécurité de la communication entre la machine d'inspection (IS) et le LDS2 Signer de la signature numérique du LDS2

  - Communication TLS entre l'IS et le LDS2 Signer à cause de la sensibilité des données échangées entre les deux entités.

  - Recherche sur les attaques contre la couche de communication TLS entre l'IS et le LDS2 Signer

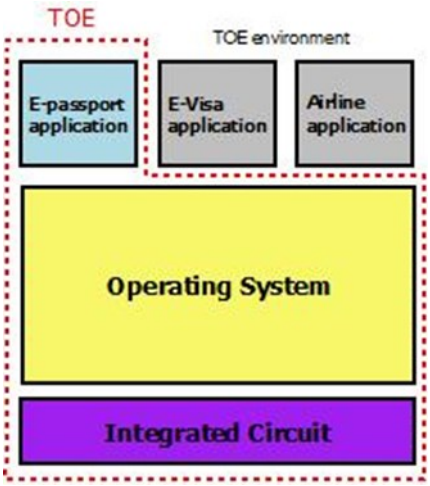
    1. Attaque de type Man-in-the-Middle (MITM)

    2. Attaque de type Déni de Service (DoS)



✓ **GTO**

- Analyse de risque sur les données privées sur un passeport électronique multi-application
  - Intégrité
  - Confidentialité
  - Menaces sur données privées
- Impact sur la rédaction de la cible de sécurité, sur les guides de conception et le processus de vérification de l'application

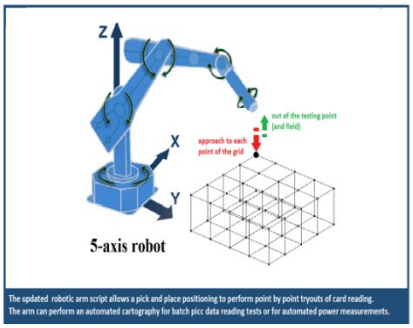


✓ **CEA-LETI**

- Analyse des vulnérabilités du lien sans contact
- Impact sur le processus d'évaluation de la sécurité du passeport électronique

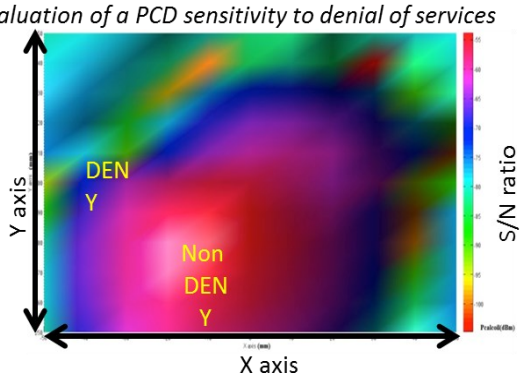
✓ **ISEN**

- Développement d'un banc de test sans contact VHBR vis-à-vis du déni de service



- Robustesse vis-à-vis des sources de bruit RF

Evaluation of a PCD sensitivity to denial of services



- Automatisation:
  - Gestion précise du placement du PICC
  - Communication vers PC avec protocole PCSC
  - Évaluation du volume d'opération du PCD
  - Évaluation de la sensibilité du PCD et du PICC au brouillage pour déni de service (DoS)

T2.2 Développement de méthodologies formelles

✓ **NXP-A en coopération avec TUG-IAIK**

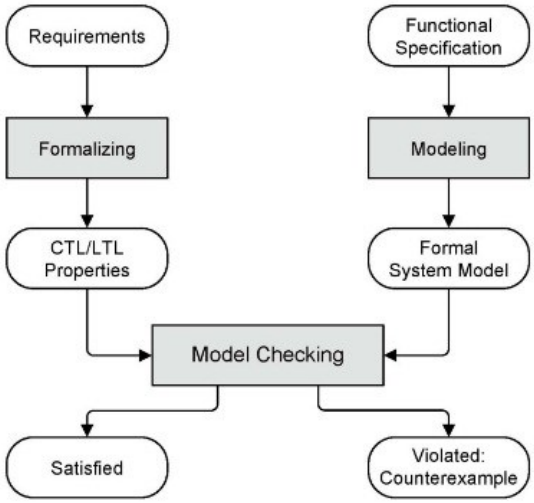
- Implémentation d'un modèle formel pour l'OS et l'application en utilisant les diagrammes d'états UML
- Les diagrammes d'états UML permettent l'intégration de modélisation formelle dans le processus de conception
- Proposition de réutiliser les diagrammes d'état UML pour les spécifications fonctionnelles (FSP) comme demandé par les Critères Communs
- Traduire la Politique de Sécurité de la Cible de Sécurité en formules de logique temporelle (SPM)
- Utiliser un vérificateur de modèle pour prouver que le diagramme d'états UML satisfait les formules décrites en logique temporelle.

T2.3 Validation partielle de méthodologies formelles

✓ **CEA LETI**

- Analyse de la méthodologie proposée par NXP-A basée sur la vérification de modèles
  - Evaluation partielle de l'exemple proposé par NXP-A: Politique de contrôle d'accès simplifié
    - Un Super Utilisateur peut créer/détruire une application sur une carte avec sa propre clé
    - Le client peut incrémenter/décrémenter une valeur dans l'application
  - La conception du contrôle d'accès est modélisée sous forme de diagramme d'états UML (Outil de CAO COSIDE)
  - L'outil apporte la preuve que les spécifications fonctionnelles satisfont la politique de sécurité décrite sous forme de formules de logique temporelle
- Validation de la méthodologie et compatibilité avec le schéma français de certification

- Principal intérêt: Niveau de description très proche de celui de la conception et peut être réalisé par un ingénieur concepteur de base
- Pseudo évaluation par le CEA-Leti et transmission d'un pseudo RTE au certificateur (ANSSI)
- Après de longues discussions validation de la méthodologie par l'ANSSI (certificateur CC)



✓ **CEA LETI & GEMALTO**

- Analyse en évaluation composite d'un passeport électronique 4G
- Nécessité d'une analyse des exigences sécuritaires
  - Aspect très spécifique d'un passeport électronique 4G multi-application: cohabitation d'applications gouvernementales et privées: visas de séjour, tampons électroniques, réservation d'hôtels, paiement électronique,…
  - Analyse des développements et des certifications des applications après délivrance
    - Isolation des applications: gouvernementales et accès aux données personnelles aux seules autorités
  - Analyser si le schéma utilisé en Télécom peut être transposé au passeport électronique, voire adapté
- Etude des exigences environnementales

- Nécessité d'une clarification sur le schéma des autorités de vérification: organisation gouvernementale afin de centraliser les certificats et la gestion des clés
- Nécessité de sonder la position des états

Dissémination:

- **NXP-A**
  - Présentation au 'SystemC AMS – COSIDE User Group Meeting': 'Formal Verification of UML Statechart Diagrams with COSIDE®'
- **CEA-LETI**
  - Présentation de la méthodologie formelle utilisant les diagrammes d'états UML proposée par NXP-A à l'ANSSI pour validation par l'autorité de certification française
- **Giesecke & Devrient**
  - Contribution à GlobalPlatform (Secure Channel Protocol 11): canal sécurisé entre au element de sécurité (SE) et un TEEE
- **GEMALTO**
  - Contribution à l' ISO SC17 WG4 : PET for ISO/IEC 19286
  - Contribution au CEN on Privacy by Design (PbD) & Attribute Based Credentials (ABC) protocols
  - Contribution à l'ISO SC27 WG5 : Privacy Framework (PbD)
- **NXP-A et TUG-IAIK** sur méthodologie formelle pour conception de puce
- **NXP-A etCEA-Leti** sur méthodologie formelle pour évaluation sécuritaire
- **Gemalto et CEA-Leti** pour évaluation en composition
- **IFX, IAIK et ST** sur la plate forme 32 bit

6.7. SP7 – Cas d'usage et démonstateurs et des applications des plate-formes techniques

6.7.1. Introduction

Coordinateur	ISEN
Partenaires	Gemalto, G&D, EVO, IT, NXP-F, id3, IFX
Objectifs	Le présent sous-projet porte sur la démonstration des applications pour les plates-formes techniques NewpP@ss, dans les contextes suivants : - Des cas d'usage unitaires qui permettront de démontrer certaines briques technologiques significatives développées dans le projet - Des cas d'usage réels définis avec l'aéroport de Toulon Hyères qui permettront de mettre en avant les résultats du projet dans un contexte de contrôle aux frontières ainsi que dans un contexte de l'infrastructure aéroportuaire. À la fin du projet, une vitrine complète, adaptée pour faire une promotion d'envergure du projet dans des endroits similaires sera élaborée. - Autres cas d'usage complexes démontrant l'utilité des résultats du projet dans d'autres domaines d'application (des compagnies aériennes, des programmes de fidélité ...)

Le sous-projet est découpé en 3 tâches :

- **Tâche 1:** Définition des cas d'usage unitaires *(Description de l'usage unitaire pour effectuer des tests techniques, enquête qualitative pour étudier les pratiques usuelles de l'aéroport, Définition de 2 cas d'usage de base et plusieurs cas d'usage plus complexes autour de la prestation de services aux voyageurs)*
  Tâche 2: Définition de la méthodologie d'intégration *(Évaluation de l'infrastructure actuelle de l'aéroport pour la vérification de l'identité, conception d'une vision de haut niveau des processus à mettre en œuvre)*
- **Task 3:** Démonstration des cas d'usage complexes *(Architecture de l'infrastructure, des API et des interfaces pour préparer l'intégration, le déploiement de l'infrastructure technique et la mise en œuvre des cas d'usage sélectionnés)*

6.7.2. Activités par périodes et partenaires

2012:

Gemalto
Gemalto a commencé à travailler sur la définition des cas d'usage avec de l'aéroport de Toulon-Hyères. Gemalto a également activement participé aux négociations préliminaires avec l'aéroport.

NXP-F
L'activité n'a pas commencé.

ID3

Id3 a commencé à étudier les cas d'usage de la biométrie impliquant la technologie de reconnaissance (identification des briques technologiques à mettre en œuvre).

INFINEON
L'activité n'a pas commencé.

ISEN-Toulon
ISEN-Toulon a négocié la participation de l'aéroport de Toulon-Hyères. La première version de l'étude quantitative concernant les besoins des aéroports européens a réalisée. Les premières rencontres face-à-face avec les parties prenantes de l'aéroport sont en cours

Giesecke & Devrient
L'activité n'a pas commencé.

ST Microelectronics
L'activité n'a pas commencé.

Evoleo
L'activité n'a pas commencé.

Instituto de Telecomunicacoes
L'activité n'a pas commencé.

2013:

ISEN-Toulon (Coordinateur du sous-projet)
Lors de la session de co-design qui a eu lieu le 7 mars à Meudon, les participants du sous-projet ont élaboré un scénario de «voyage idéal». Pour évaluer la faisabilité du scénario, ISEN-Toulon a mené des observations sur le terrain et a effectué des entretiens avec différents services de l'aéroport de Toulon-Hyères durant la période entre octobre et décembre 2013, y compris:
• Réservation de billets d'avion / enregistrement
• Parking
• Contrôle de sureté
• Contrôle aux frontières
Des entrevues avec d'autres services (bagages, l'aviation générale) sont actuellement en cours de négociation avec l'aéroport. ISEN-Toulon a effectué une étude de 3 aéroports français: Lille, Marseille et Nice et a négocié l'accès aux services VIP de l'aéroport de Nice.
Durant le 4ème trimestre, ISEN-Toulon a organisé et modéré des conférences téléphoniques pour préparer deux ateliers de co-design dédiés à l'élaboration de deux cas d'usages du passeport 4G. Le premier atelier a eu lieu à Hambourg le 16 Janvier 2014. Le deuxième a eu lieu à l'aéroport de Toulon-Hyères le 29-30 Janvier. Les livrables produits sur cette période sont les suivants : retranscriptions des interviews, photos des installations et des services aéroportuaires, des protocoles et des présentations pour animer les sessions de co-design à Hambourg et à l'aéroport de Toulon-Hyères

Gemalto
Gemalto a affiné avec d'autres partenaires les cas d'usage des passeports 3G. Ce travail comprenait un atelier d'une journée, le 21 Mars 2013 à Meudon, hébergé par Gemalto, consacré à la définition des cas d'usage des

passeports 3G. Le travail de définition des cas d'usage des passeports 4G a commencé au cours de cet atelier. Il s'est poursuivi lors d'un atelier dédié le 9 Septembre 2013 (via une conférence téléphonique), en se focalisant sur les cas d'usage LDSv2 spécifiques au passeport 4G : visa électronique, tampon électronique, biométrie supplémentaire et d'autres usages commerciaux. Les résultats de l'atelier sont visibles dans un rapport séparé situé sur le site newp@ss, et en partie dans SP2, livrable D2.2. Le travail sur des cas d'usage du passeport 4G a été poursuivi dans le cadre des ateliers à l'aéroport de Toulon-Hyères (29 et 30 janvier 2014).

NXP-France
NXP France a participé à la définition des cas d'usage de base et des cas d'usage complexes, en particulier au cours de la réunion qui a eu lieu à Paris en Avril. Le questionnaire élaboré pour le personnel de l'aéroport a été relu.

ST
ST a suivi les propositions initiales des cas d'usage et a contribué à l'affinement des démonstrateurs proposés dans le cadre de l'aéroport de Toulon.

ID3
Id3 a contribué à la définition des cas d'usage des passeports de 3ème et 4ème génération. En particulier, Id3 a participé à la réunion de travail avec l'ISEN-Toulon, Gemalto et G & D sur ce sujet. ID3 a régulièrement participé aux conférences téléphoniques et aux réunions consacrées à la définition de cas d'usage. Pour améliorer sa compréhension de l'utilisation du passeport électronique et de partager ses connaissances sur les technologies RFID, ID3 a été impliqué dans les réunions organisées par l'ISEN. Particulièrement, ID3 était présent à la réunion à l'intérieur de l'aéroport de Toulon Hyères. Le but de cet événement était de comprendre le point de vue du personnel de l'aéroport sur les questions relatives aux technologies de passeport électronique. ID3 continue à participer à des études prospectives sur l'utilisation de l'e-passeport de demain

IFX, IFAT
L'activité n'a pas commencé

NXP-G
NXP a continué à contribuer dans les activités du SP7 en participant à la définition de cas d'usage et des activités de démonstration à l'aéroport de Toulon. Le matériel et les logiciels pour réaliser les démonstrations ont été planifiés et préparés. Le travail progresse comme prévu.

Giesecke & Devrient
G&D a contribué à la définition des cas d'usage etaux démonstrateurs dans l'environnement de l'aéroport de Toulon et a assisté à l'atelier de co-design à l'aéroport de Toulon. Par ailleurs, G & D a fourni un premier démonstrateur unitaire illustrant le passeport 3G.

Evoleo
Evoleo a travaillé sur l'identification des scénarios appropriés pour évaluer la plate-forme sécurisée NewP@ss. L'évaluation et la participation des managers de l'infrastructure d'aéroports nationaux est en cours pour explorer les capacités et les démonstrateurs possibles qui s'appuieraient sur des scénarios réels.

IT
IT a suivi les activités de définition et d'implémentation des cas d'usage, notamment sur terrain de test de l'aéroport de Toulon-Hyères. IT, avec Evoleo, a initié des négociations avec les Autorités de certification du

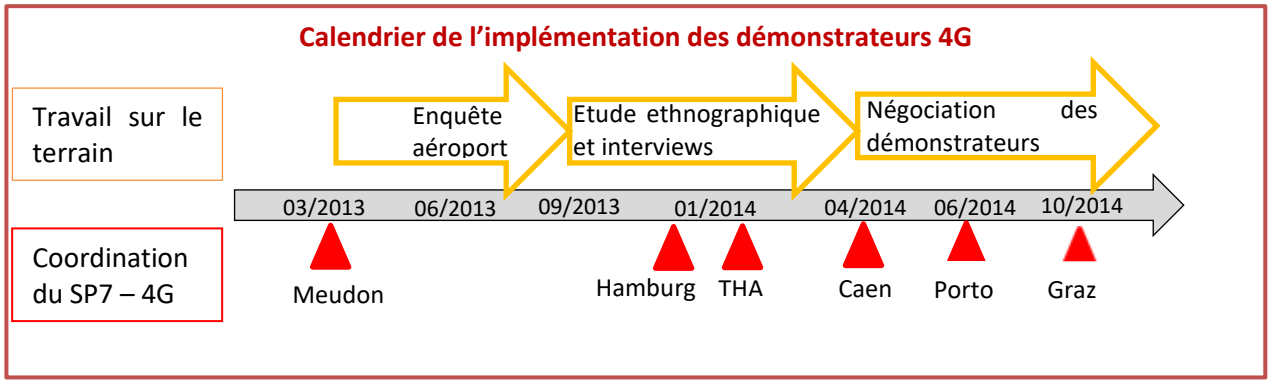
Pays de Vérification/ Vérificateur de documents Portugais, les autorités de contrôle aux frontières (SEF - "Serviço de Estrangeiros e Fronteiras"), et avec l'aéroport de Portugal afin d'évaluer la possibilité d'accéder à un terrain de test local. Celui-ci pourrait s'appuyer sur l'installation principale à Toulon-Hyères, en se focalisant sur un aspect particulier, représentant un plus grand intérêt pour les acteurs nationaux mentionnés.
Evoleo et IT ont sollicité trois aéroports portugais (ANA) pour répondre à l'enquête en ligne menée par l'ISEN-Toulon.

2014:

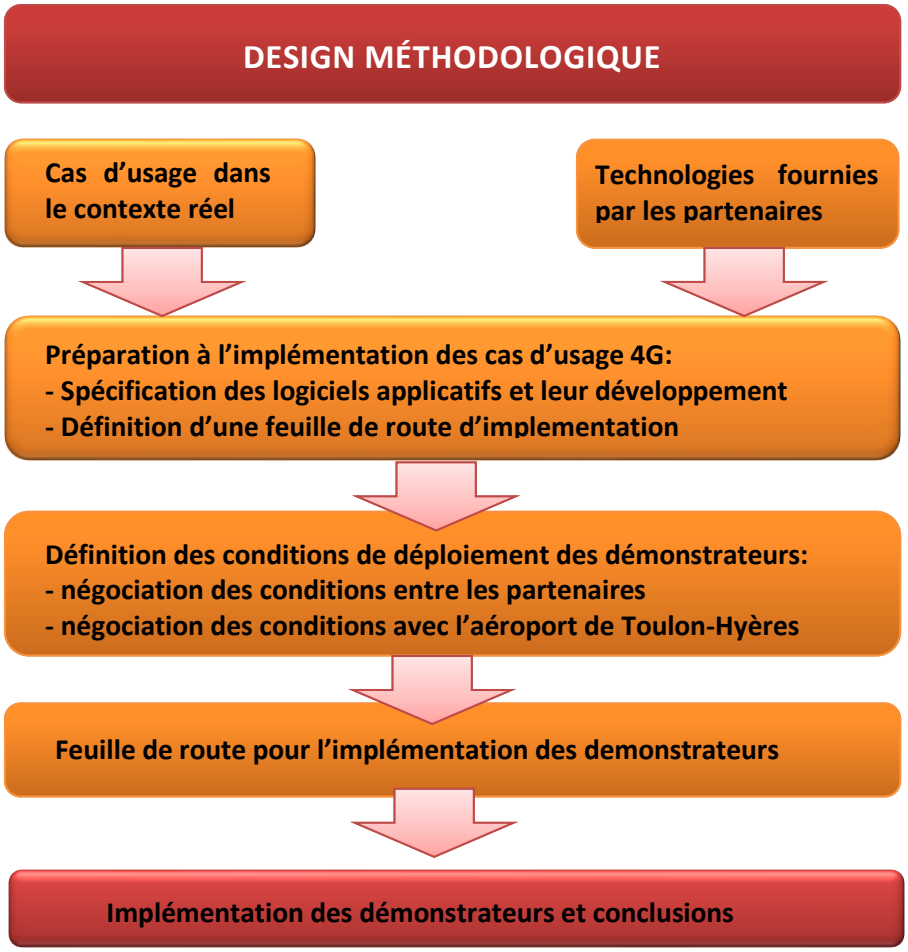
ISEN-Toulon (coordinateur du SP)
Pendant le premier semestre, l'ISEN Toulon a coordonné l'activité du SP7 et a édité 2 livrables. En plus, l'ISEN organisé et coordonné plusieurs ateliers entre les partenaires, présentés dans le tableau ci-dessous :

Hamburg: 16 janvier	Travail sur les cas d'usage spécifiques aux passeports de 4-ème génération (4G)
Toulon-Hyères: Atelier SP7 , 29-30 janvier	Visite des infrastructures de l'aéroport de Toulon-Hyères, et atelier de co-codesign avec le personnel de l'aéroport afin d'envisager des cas d'usage les plus avancés
Caen Workshop, April 9th	Description et présentation des preuves de concept des briques technologiques développées par les partenaires du projet
Porto Workshop, June 6th	Sélection des briques technologies qui seront intégrés dans les démonstrateurs finaux

Au cours du deuxième semestre, l'ISEN-Toulon a poursuivi la coordination de l'activité du SP7. Durant le troisième trimestre, des modifications ont été apportées dans le cadre méthodologique de la préparation du démonstrateur, suite à la réunion qui s'est déroulé à Graz le 30 septembre et le 1 octobre.



La méthodologie de travail est décrite dans le schéma ci-dessous:



A partir des cas d'usages définis lors des sessions de brainstorming, des briques technologiques fournis par les partenaires ainsi que du design de l'environnement sociotechnique (effectué durant le premier semestre 2014), l'ISEN a proposé une feuille de route pour la mise en œuvre des démonstrateurs qui identifie clairement les étapes et l'agenda du travail.

Le travail s'organiserait autour de deux axes : i) préparation des démonstrateurs et ii) la préparation de l'événement de démonstration. La feuille de route sera affinée courant le premier semestre 2015, en s'appuyant sur les contributions et les suggestions des partenaires.

L'ISEN et Gemalto ont commencé une collaboration portant sur la réalisation de logiciels applicatifs pour la démonstration des solutions développées par les partenaires. L'ISEN a coordonné la production d'APIs pour la démonstration des fonctionnalités du passeport 3G. L'ISEN initié la négociation concernant le développement de logiciels à des fins de démonstration conjointement entre les différents partenaires: ISEN, Gemalto, Compuworx et Evoleo. Le travail sera poursuivie et s'intensifiera courant le premier semestre 2015.

ISEN a proposé un cadre pour la négociation des conditions de déploiement des démonstrateurs. Les informations fournies par les partenaires ont été recueillies et synthétisée.

Gemalto

Gemalto a travaillé avec d'autres partenaires pour compléter les cas d'usage du passeport 4G et pour

préparer les démonstrateurs finaux. Ce travail a notamment été effectué au travers des conférences téléphoniques et dans le cadre des réunions de coordination du projet.
Gemalto a participé dans chaque atelier SP7 arrangés lors des réunions de coordination du consortium : le 30 Septembre – 1 Octobre 2014 (Graz) et le 9-10 décembre 2014 (St Cyr Sur Mer). Comme résultat de ces ateliers, une liste de briques technologiques fournie par chaque partenaire et un plan de démonstrateurs unitaires ont été établis pour la fin de l'année 2014. Un planning initial de réalisation de démonstrateurs finaux basé sur les briques technologiques identifiés a été défini.
Gemalto a également démontré les technologies suivantes :

- Passeport éléctronique 3G: SAC avec CAN (lors de la réunion de coordination d'Octobre 2013 à la Ciotat)
- Passeport éléctronique 4G: LDSv2 visa électronique et tampon électronique, démonstration de lecture et d'écriture (lors de la réunion du consortium de Janvier 2014 à Hambourg)
- Passeport éléctronique 4G: démonstration LDSv2+VHBR (réunion de revue de décembre 2014, à St-Cyr-Sur-Mer)

NXP-France
NXP a commencé le travail d'intégration de ses derniers circuits intégrés dans la carte du lecteur de démonstration.

ST
ST a contribué à la définition des cas d'usage des passeports 3G / 4G, et a commencé la préparation d'un démonstrateur de technologie VHBR (vs. norme RF) basé sur le circuit étudié dans le SP3, associé au lecteur VHBR d'ID3.

ID3
ID3 a participé aux conférences téléphoniques consacrées à l'organisation des démonstrateurs. Comme deuxième activité, ID3 a commencé à préparer la conception de son démonstrateur technique. Celui-ci portera sur la démonstration de la technologie VHBR embarquée sur un lecteur en cours de conception.

IFX, IFAT. IFX a soutenu les activités de développement des cartes et des lecteurs VHBR pour des démonstrations des briques autonomes. IFX est en train d'étudier des options de démonstration supplémentaires.

CEA-Leti
CEA-Leti a travaillé sur la spécification d'adaptation du lecteur VHBR et du front –end silicium RF développés dans le SP3 pour être intégrés dans un démonstrateur technologique.

Giesecke & Devrient
G&D a fourni des briques technologiques et est en train de finaliser des briques qui pourraient être intégrés dans des démonstrateurs complexes :

- Passeport 3G (brique)
- Passeport 4G (brique)
- Demonstrateur LDSv2 pour l'entrée/sortie du territoire (démonstrateur unitaire)
- Demonstrateur de l'environnement sécurisé pour mGouvernement (démonstrateur unitaire)

La planification de l'architecture pour le démonstrateur LDSv2 a commencé.

Jusqu'à présent, les démonstrateurs technologiques suivants ont été réalisés par G&D :

- Lecteur mobile d'un document : application Android capable de lire les données du passeport 3G

- Démonstrateur LDSv2 dans un contexte de passage aux frontières (entrée et sortie du territoire) en utilisant des passeports 4G
- Le corps de la carte avec LED pour cacher les données

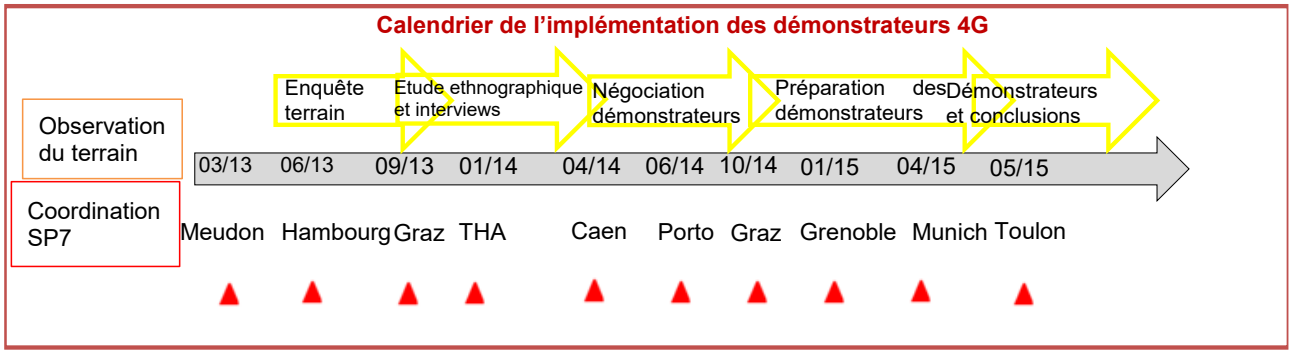
NXP-G
Pas d'activité déclarée pour cette période

Evoleo
Evoleo a travaillé sur l'évaluation et le choix des scénarios appropriés pour mettre en avant le fonctionnement de la plate-forme sécurisée. L'évaluation et l'implication des gestionnaires d'infrastructures aéroportuaires nationaux continue, pour explorer les possibilités et les démonstrateurs possibles dans le contexte réel.
Un démonstrateur de l'infrastructure PKI est en cours de développement en étroite coopération avec IT. Le démonstrateur est composé d'un lecteur/système d'inspection et d'une infrastructure PKI, interagissant l'un avec l'autre. Il reste à explorer la démonstration de la lecture d'un échantillon de passeport électronique en interaction avec l'architecture PKI. L'émulation d'un passeport électronique est étudiée, comme une option supplémentaire pour le démonstrateur.

IT
IT a continué à suivre les activités liées à la définition de scénarios de démonstration et des cas d'usage, notamment dans le contexte de l'aéroport de Toulon-Hyères. IT a travaillé en étroite collaboration avec Evoleo sur les aspects démonstration SP7, à savoir la mise en œuvre de l'infrastructure PKI 4G et de ses mécanismes. Ce démonstrateur sera d'abord envisagé comme un démonstrateur unitaire et par la suite sera intégré avec d'autres démonstrateurs des partenaires.
Le démonstrateur conjoint d'IT/Evoleo vise à démontrer comment un voyageur est authentifié dans le système de contrôle d'un aéroport d'un pays B et ses données de voyage sont signées et inscrites sur son passeport 4G. Le démonstrateur prend en compte deux types de mise en œuvre différents. Le premier mode de réalisation est basé sur le document électronique virtuel fourni par le logiciel OpenSCDP, et le second utilise un réel passeport électronique 4G.

2015:

ISEN-TOULON (coordinateur SP7)
Pendant le premier semestre 2015, ISEN-Toulon a coordonné l'activité du SP7. Le déroulement du travail est illustré par le schéma ci-dessous :



ISEN-Toulon et Gemalto ont coordonnés et contribués aux travaux de préparation des démonstrateurs technologiques et de cas d'usage complexes avec d'autres partenaires. Deux livrables, D7.3 et D7.4, résumant ce travail, ont été édités durant cette période. ISEN-Toulon a également participé à un groupe de discussion dédié à des cas réels. ISEN-Toulon a présenté deux démonstrateurs:

- Banc d'essai sans contact pour les applications VHBR
- Des applications de cas d'usage commerciales, en étroite collaboration avec Gemalto

Gemalto

Gemalto a travaillé avec d'autres partenaires pour compléter les cas d'usage du passeport 4G et la démonstration finale. Le travail de coordination entamé en 2014 s'est poursuivi et s'est intensifié en 2015, au travers des conférences téléphoniques régulières et des ateliers collaboratifs dédiés à la préparation des démonstrateurs.

Comme résultat, le démonstrateur final intégrant des briques technologiques identifiées a été produit. Avant la réunion de revue finale, Gemalto a démontré le cas d'usage de contrôle de passage aux frontières, à l'ISEN Toulon sur une période de 20 mai au 4 juin 2015, impliquant des élèves et le personnel de l'ISEN (voir la figure 10 « Démonstrateur de contrôle de passage aux frontières »). Ce démonstrateur a ensuite été démontré lors de la revue finale du 17 juin, et a en plus démontré l'interopérabilité des échantillons de passeports 4G de Gemalto et de G&D.

De 2013 à 2015, Gemalto a produit les démonstrateurs suivants:

- Passeports électronique 3G : démonstration des protocoles SAC avec CAN (réunions à la fin de 2013)
- Passeport éléctronique 4G: LDSv2 visa électronique et tampon électronique, démonstration de lecture et d'écriture (lors de la réunion du consortium de Janvier 2014 à Hambourg)
- Passeport éléctronique 4G: démonstration LDSv2+VHBR (réunion de coordination à Graz en octobre 2014 et réunion de revue de décembre 2014 à St-Cyr-Sur-Mer)
- Passeport éléctronique 4G : démonstrateur de passage aux frontières avec LDSv2 visa électronique et tampon électronique (réunion à Munich en avril 2015 ; démonstrateur test à l'ISEN en mai-juin 2015 ; et la revue finale du projet 2015, incluant également l'interopérabilité avec les échantillons fournis par G&D)

NXP-France

NXP a commencé le travail d'intégration de ses derniers circuits intégrés dans une carte du lecteur de démonstration.

ST

ST a finalisé un démonstrateur de la communication VHBR (vs. norme RF) basée sur le circuit étudié dans le SP3 associé au lecteur VHBR. Ce démonstrateur a été présenté lors de la revue finale. ST a également travaillé avec Id3 pour évaluer les communications sécurisés MCU avec le lecteur d'Id3.

ID3

Pendant le premier semestre, ID3 a conçu un démonstrateur technologique qui illustre le fonctionnement du lecteur de VHBR. Une application logicielle fonctionnant sur PC a été spécialement conçue à cette occasion. Le démonstrateur effectue un téléchargement d'une image stockée dans une carte sans contact. La démo permet de comparer les temps de transfert en mode VHBR par rapport à la vitesse de la RFID. Ce démonstrateur a été réalisé en collaboration avec ST, Infineon et ISEN.

CEA-Leti

Durant le premier semestre de 2015, le CEA-Leti a mis au point un prototype permettant de valider la partie numérique du circuit VHBR NewP@ass, réalisé dans le SP3. Ce prototype, fait sur une carte FPGA du commerce, a été présenté lors de la revue CATRENE de fin de projet, en juin 2015 à Toulon. Même s'il reposait sur un frontal RF très largement sur-dimensionné par rapport à celui intégré dans le circuit VHBR, le développement de ce prototype a permis néanmoins de valider l'étude système et l'architecture numérique du récepteur, ainsi que d'établir un lien VHBR jusqu'à 27 Mbps en modulation de phase.

Durant le deuxième semestre de 2015, le CEA-Leti a développé la carte de test du circuit VHBR NewP@ss, en vue de son intégration dans le démonstrateur technologique VHBR du SP3 (cf. synthèse de l'activité du SP3). Le synoptique de la carte de test est donné sur la **Figure 26**. La carte de test est une carte mezzanine connectée à une carte mère FPGA, elle-même développée dans un projet précédent. La carte mère offre l'infrastructure matérielle et logicielle pour s'interfacer avec un banc PXI, notamment pour le test des modules RF du circuit NewP@ss. Par ailleurs, le FPGA est aussi envisagé pour implémenter tout ou partie de la chaine numérique au cas où le circuit ne soit pas totalement fonctionnel et qu'il faille « by-passer » une partie de la chaine de réception. Alternativement, le FPGA permettra aussi de tester des algorithmes numériques différents s'il s'avère que les signaux produits pas le frontal RF ne peuvent pas être traités directement par les blocs numériques intégrés dans le circuit (non-linéarités du frontal plus importantes, distorsions importantes sur le signal reçu, etc.).
La carte de test elle-même est connectée à la carte mère par un connecteur numérique, par lequel transiteront les signaux nécessaire à la configuration des registres de tests ainsi que les entrées/sorties numériques du circuit VHBR NewP@ss (appelé NP1 DUT sur la Figure 26). Les entrées/sorties de tests analogiques seront disponibles sur des points de test situés sur la carte. Le circuit sera mis en œuvre grâce à un socket, permettant la réutilisation de la carte de test pour la validation séquentielle des échantillons du circuit reçus du fondeur. Enfin, il faut noter que la carte de test offre deux options pour le conditionnement (redressement) des signaux reçus à l'antenne. Un cavalier permettra de sélectionner soit un circuit intégré pré-existant au projet soit un pont redresseur réalisé en composants discrets.

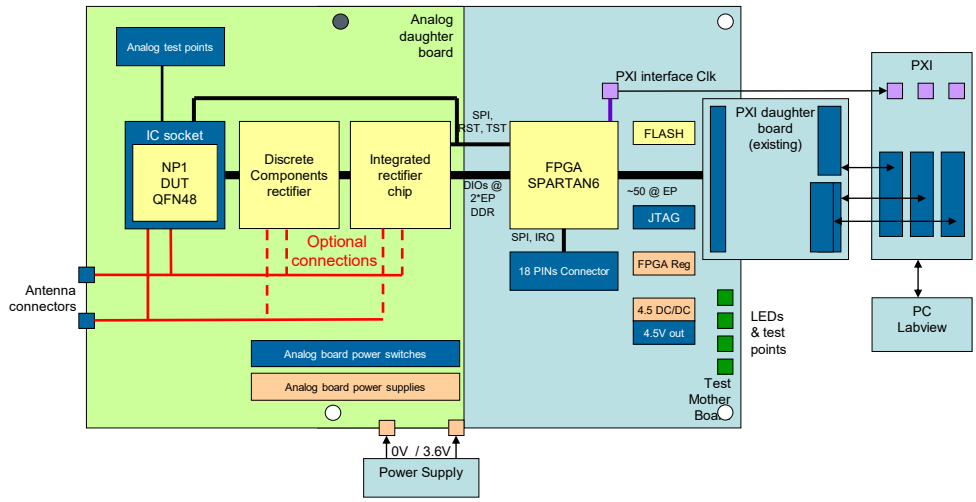


Figure 26: synoptique de la carte de test du circuit VHBR

A l'heure où ce rapport est écrit, la carte de test est en train d'être finalisée. Le schéma du PCB de la carte de test est donné sur la **Figure 27**. Nous prévoyons de l'envoyer en fabrication à la fin de l'année 2015 pour pouvoir en disposer au retour des circuits mis en boitier et réaliser les tests dans le premier trimestre de 2016.

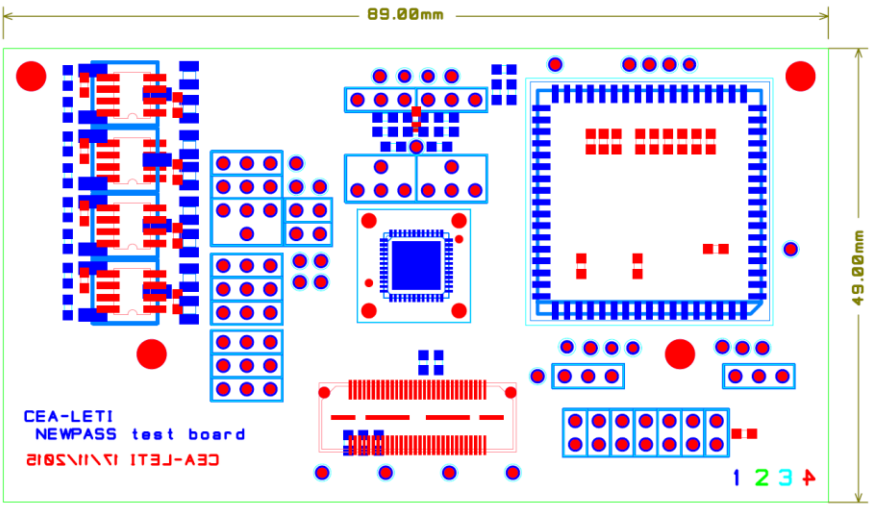


Figure 27: Schéma du PCB de la carte de test du circuit VHBR.

Compuworx

Compuworx a développé une application pour les terminaux de point de vente. Ce logiciel "CWBase" est en mesure de gérer les cartes à puce par le biais du NFC. La mise en œuvre du protocole BAC / PACE n'était pas terminée à l'heure de rédaction du rapport. Compuworx a développé une application smartphone "CWNewp@ss" capable de lire des données des cartes du passeport via NFC (en utilisant le logiciel open source JMRTD, basé sur l'implémentation Java). A l'heure actuelle, l'application Android n'est pas en mesure d'écrire dans le passeport.

IFX, IFAT

IFX a soutenu les activités de développement des cartes et des lecteurs VHBR pour des démonstrations des briques autonomes. IFX est en train d'étudier des options de démonstration supplémentaires.

G&D

G&D a développé les démonstrateurs suivants:

- Démonstrateur LDSv2, en collaboration avec Gemalto (G&D a fourni des échantillons du passeport 4G)
- Le démonstrateur de l'entrée/sortie du territoire avec les échanillons du passeport LDSv2
- Demonstrateur d'environnement sécurisé pour mGouvernement (démonstrateur unitaire)
- Le corps de la carte avec un éclairage LED pour cacher les données

NXP-G

NXP a préparé le démonstrateur du capteur capacitif sur le corps de la carte du passeport, présenté lors de la session de revue finale à l'ISEN Toulon. À cette occasion, un logiciel hébergé sur un téléphone mobile NFC a dû être adapté pour être compatible avec une version plus récente du firmware de la carte. Des échantillons

de cartes de nouvelle génération ont été préparés et configurés pour la démo. Le démonstrateur consistait à simuler une inspection d'un passeport électronique avec un téléphone mobile standard, via la procédure BAC. Dans cette démonstration, l'inspection a été initiée non pas par la transmission des données MRZ hors bande pour initier l'échange de clés de session, mais physiquement sur la bande (mais logiquement hors bande) et la transmission électronique après l'autorisation de l'utilisateur par un mouvement de doigt exécuté sur la carte.

Evoleo

Courant le premier semestre 2015, Evoleo a développé le démonstrateur d'une infrastructure PKI (en coopération avec IT) avec un logiciel de système d'inspection, fonctionnant avec un simulateur d'un passeport électronique. Le démonstrateur a porté sur la démonstration de la structure de données LDSv2 avec un utilisateur voyageant dans différents pays et obtenant des tampons de passage aux frontières écrits dans le passeport, signés par l'infrastructure PKI.

IT

IT a travaillé en collaboration étroite avec Evoleo sur les aspects de démonstrateurs du SP7, en particulier sur l'implémentation de l'infrastructure PKI et des mécanismes nécessaires pour le passeport 4G. Ce démonstrateur unitaire illustre comment un voyageur est authentifié par le système de contrôle d'un aéroport d'un pays B et ses données de voyage sont signés et écrits sur son passeport électronique 4G. Le démonstrateur utilise le passeport virtuel (Virtual eMRTD) fourni par OpenSCDP

6.7.3. Coopération

- **Entre les partenaires du sous-projet**
  - Sessions de co-design afin de concevoir des cas d'usage complexes **le 21 mars 2013 à Meudon**
  - Télé-conférences de coordination régulières
  - Enquête qualitative diffuse par tous les partenaires du SP7
  - Session de co-design **le 29-30 janvier 2014 à l'aéroport Toulon-Hyères**
  - Session de coordination **le 7-8 avril 2014 à Caen** et **le 4-5 juin à Porto**
  - Sessions de coordination: tous les trois mois, avec une session dédiée au SP7 dans le cadre des réunions de coordination du consortium
  - Pendant la période du second semestre 2014, les partenaires se sont focalisés sur la finalisation de démonstrateurs 4G unitaires et, à partir de la fin de l'année, ont entamé la collaboration pour préparer les demonstrateurs de cas d'usage complexes, nécessitant des assemblages de briques technologiques apportées par les différents partenaires. Quelques tests d'interopérabilté ont été effectués pendant la réunion du consortium à Graz le 30 septembre – 1 octobre et à St Cyr le 10 décembre. La coopération s'est intensifiée en 2015.
  - Télé-conférences de coordination: tous les 15 jours en 2013 et 2015
  - Démonstrateur du côntrole de passage aux frontières conjointement implémenté par Gemalto, G&D and ISEN-Toulon
  - Cooperation implémenter les démonstrateurs technologiques: ST, Infineon & ISEN-Toulon; ID3 & ST; G&D & Gemalto
- **Avec les autres sous-projets**
  - **SP 2, 3, 5**: Consultations techniques afin d'élaborer des cas d'usage
  - **Les coordinateurs des autres SP coordinateurs** sont invités à participer dans les sessions de co-design
  - Les cas d'usage sont communiqués à **tous les SP**

- **SP2 and SP4**: Consultations techniques pour concevoir l'architecture technique des démonstrateurs; le coordinateur du SP2 a coordonnée les aspects techniques du démonstrateur de passage aux frontières.

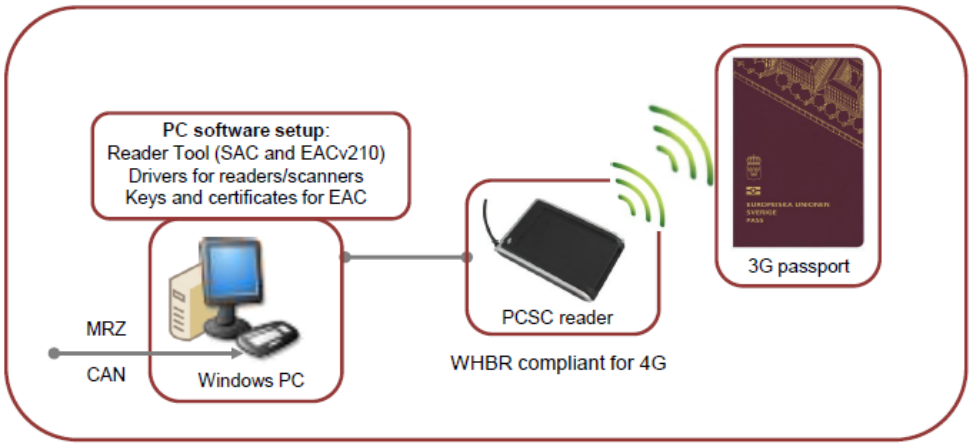
6.7.4. Résultats

Livrables

Deliverable	Related Task	Due date (CR #2)	Delivered or Expected date	Type et contenu
D7.1 v1	T7.1	T2 13	T2 13 fait	Definition des cas d'usage unitaires (Possible update at T0+15)
D7.1 v1	T7.1	T1 14	T1 14 fait	Definition des cas d'usage complexes (Aéroport de Toulon Hyères et autres aéroports)
D7.2	T7.2	T2 14	T2 14 fait	Architecture du système, interfaces, et schéma d'implémentation sur l'aéroport de Toulon Hyères
D7.3	T7.4	T1 15	T1 15 fait	Cas complexes : Version 1.0 du logiciel pour le démonstrateur
D7.4	T7.4	T2 15	T2 15 fait	Démonstration de tous les cas d'usages et conclusions pour l'implémentation finale

Résultats principaux :

- **Le cas d'usage unitaire défini** (Meudon, 21 Mars 2013) – Cas d'usage du passeport 3G



- **Enquête qualitative** élaborée
- **Les cas d'usage pour la structure des données LDS2 du passeport 4G,** compatibles aux normes ICAO (Meudon, 9 Septembre 2013)

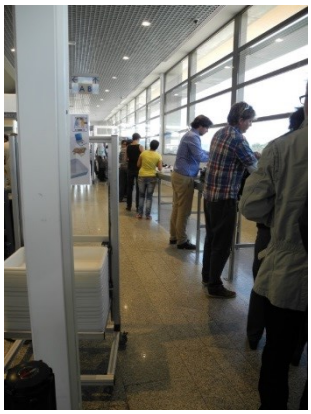
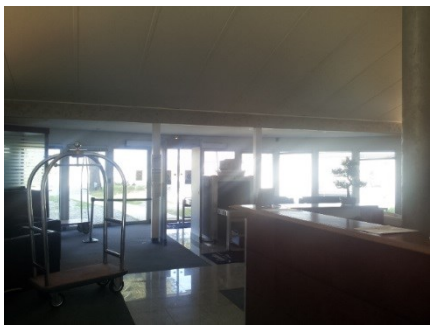
Use case: VISA information

- *What*: Storage, evidence, and retrieval of visa information / approvals from States
- *Why:* replaces the current stickers and stamps, better processing time in the border (no need to browse through the passport pages), can use the same MRZ (one scan is enough), standardized data content & format
- *By who:* embassy (write), border control (read)
- *When:* visa application, border crossing
- *How:*
- *Pros:*
- *Cons:*
- *To consider: storage & nbr of records*

Use case: Travel Stamp

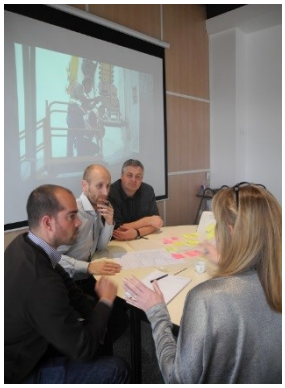
- *What*: Storage, evidence, and retrieval of entry / exit records (travel stamps) from States
- *Why:* provide evidence that a person has legally entered/exited a State, provide risk assessment of a traveler through the travel history, provide standardized data content & format
- *By who: border control inspection system (read/write)*
- *When: border control*
- *How:*
- *Pros:*
- *Cons:*
- *To consider: storage & nbr of records, completeness of records*

- **Etude ethnographique** de l'aéroport Toulon Hyères (Hyères, 11 Octobre 2013)
  - Quelques propositions d'usage du passeport:
    - A l'étape de réservation de billets, afin d'éviter des erreurs de frappe et la saisie de données trop laborieuse
    - A l'étape de contrôle de sûreté, afin de facilité le travail des agents de sûreté
    - Services aux jets privés (aviation civile)

- **Définition de cas d'usage** avec l'aéroport de Toulon Hyères (Session de co-design le 29-30 janvier 2014)
  - 2 scénarii complexes définis:
    - ✓ **Voyage Parfait d'un voyager d'affaires**
    - ✓ **Couple de retraités voyageant à l'extérieur de l'espace Schengen**





- **Démonstrateurs**
  - **Gemalto**
    - Premières transactions avec le passeport électronique 4G, avec la technologie VHBR et la structure de données LDS2 .
  - **ID3**
    - Lecture de passeport RFID, inspection du document de voyage et l'authentification biométrique basée sur la reconnaissance faciale
  - **G&D**
    - Le corps de la carte d'un document électronique avec LED integer afin de cacher les données imprimées sur la carte (dans le cadre du SP3)
    - Démonstrateur de la structure des données LDS 2 basées sur le système de contrôle de passage aux frontières (entrée/sortie) (dans le cadre du SP4)

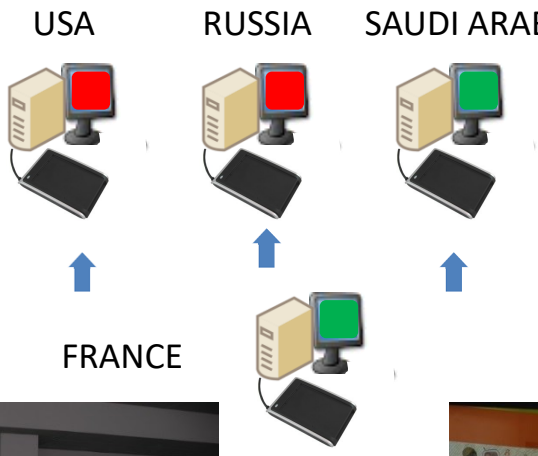
- **Matrice de coordination entre les partenaires pour l'intégration des briques techniques et l'implémentation des démonstrateurs**

Entreprise	Briques disponibles	Briques demandées	Contribution
Gemalto	Passeport électronique sur la puce VHBR (incluant LDSv2)	Puces VHBR compatibles pour le passeport (au moins 1.6 Mbit/s carte -> lecteur)	NXP, ST & Infineon ont aussi des puces
	LDSv2 logiciel applicatif (CST) compatible avec VHBR et la structure de données LDSv2 non-standardisé	Lecteur VHBR compatible avec les cartes (au moins 1.6 Mbit/s carte -> lecteur)	Lecteur développé en interne ID3 peut fournir un lecteur
ISEN	Protocol VHBR ISO 14443 prêt fin décembre 2014	Protocol applicative protocol (crypto, LDS2, stand ICAO)	Lecteur ID3 ou Duali + échantillons du passeport 3 G fournis par Gto ou G&D
	Antenne VHBR pour les lecteurs et les cartes prêt fin décembre 2014, sous condition d'avoir des puces et des cartes	Passeport électronique et lecteur	Puces et échantillons fournis par ST ou NXP ou Infineon
Evoleo/IT	4G/LDSv2 PKI et mécanisme associé	Échantillons de passeports (x3), certificats, données biometriques	Echantillons de cartes avec LDS2 fournis par G&D et Gto
ST	Norme de standard VHBR : Test ISO OS ou ICAO OS?	Lecteur VHBR	Duali
	Cartes VHBR compatibles avec la norme de standard ID1 type A, B	Logiciel pour passeport électronique	Collaboration avec Gto ou G&D: à négocier
NXP-F	Lecteur 4G, démonstrateur unitaire, sous condition d'avoir développé notre propre puce VHBR	Cartes –> collaboration avec ID3	
ID3	Démonstrateur d'analyse d'un document d'identité électronique	Passeport électronique 3G avec code CAN	Cartes 3&4G fournies par Gto ou G&D

- "NewP@ss bénévolat": logiciel open source et application mobile pour lire les passeports 3G/4G dans le cadre d'un projet étudiant ISEN
  - Logiciel open source élargi aux cas d'usage complexes
- **Identification des démonstrateurs technologiques des partenaires**

- Technological demonstrators identifiedG

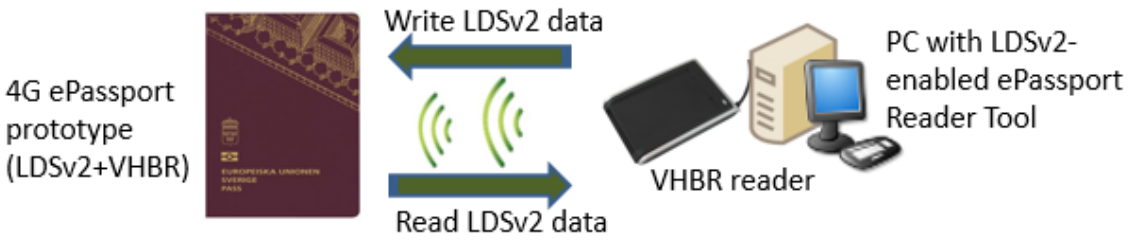
- **Configuration et test du cas d'usage de contrôle de passage aux frontières**
  - Lecture des passeports et écriture dans les passeports – premiers retours de usagers



Démonstrateur du passeport 4G, contrôle de passage aux frontières (Visa et tampon électroniques)

General description

General architecture:



Scénario d'usage:

- Taper CAN
- Effectuer PACE
- Vérifier la validité du passeport
- Effectuer EAC
- Ecrire le tampon de sortie
- Ecrire le tampon d'entrée
- Ecrire le visa

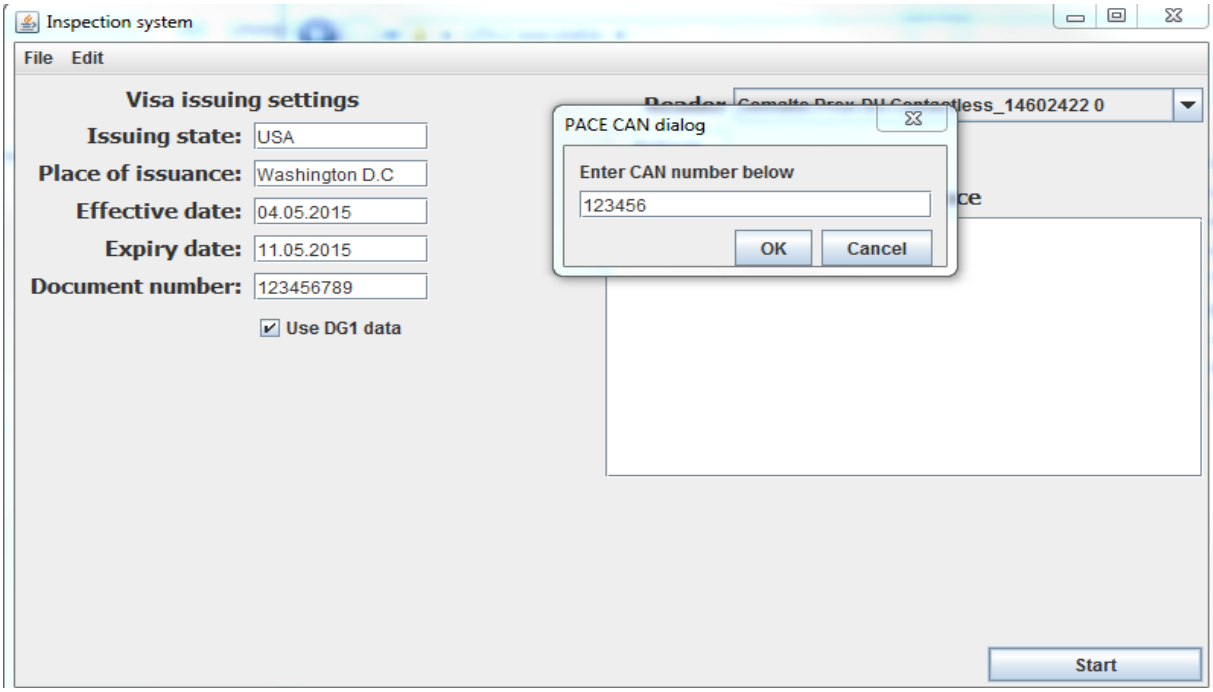


Figure 35 – Entrer le code CAN

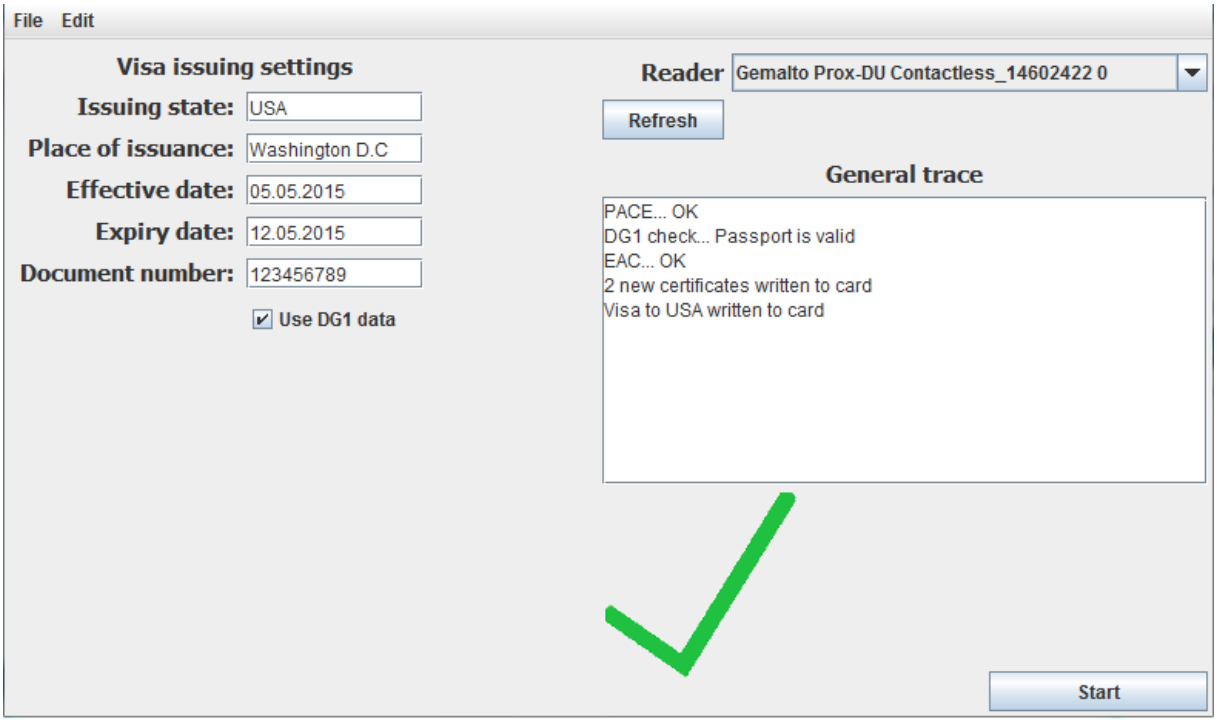


Figure 36 – Ecrire un visa

Il s'agit de la même procédure d'écriture lors de l'écriture d'un tampon d'entrée ou de sortie:

Figure 37 – Ecrire un tampon de voyage

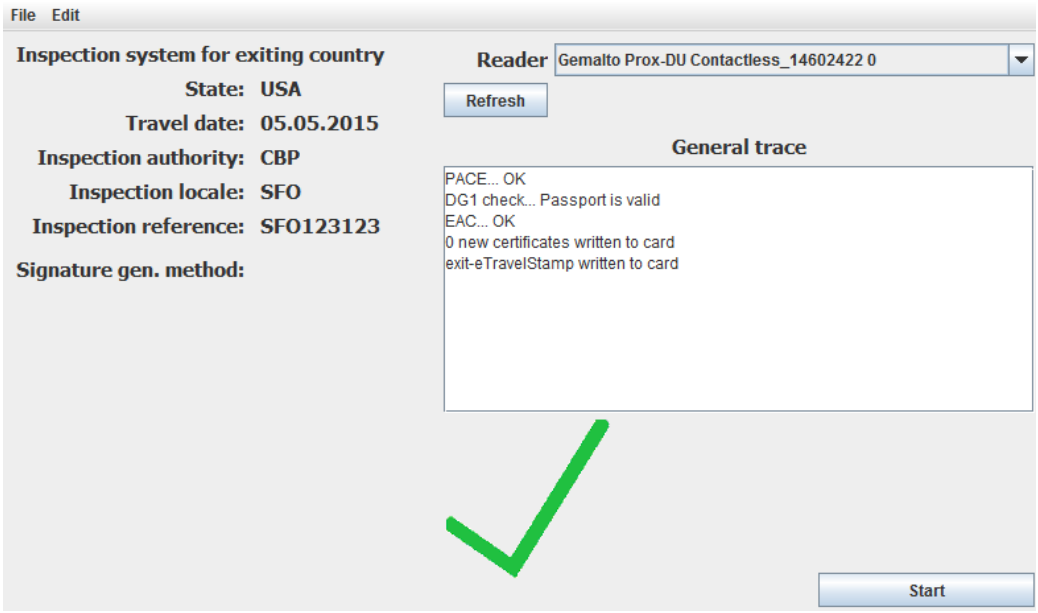


Figure 38 – Ecrire un tampon de voyage

Caractéristiques techniques

MAtériel:

- Clavier et écran standard
- Lecteur VHBR
- PC, Windows XP ou Windows 7

Logiciel:

- Pilotes pour les lecteurs

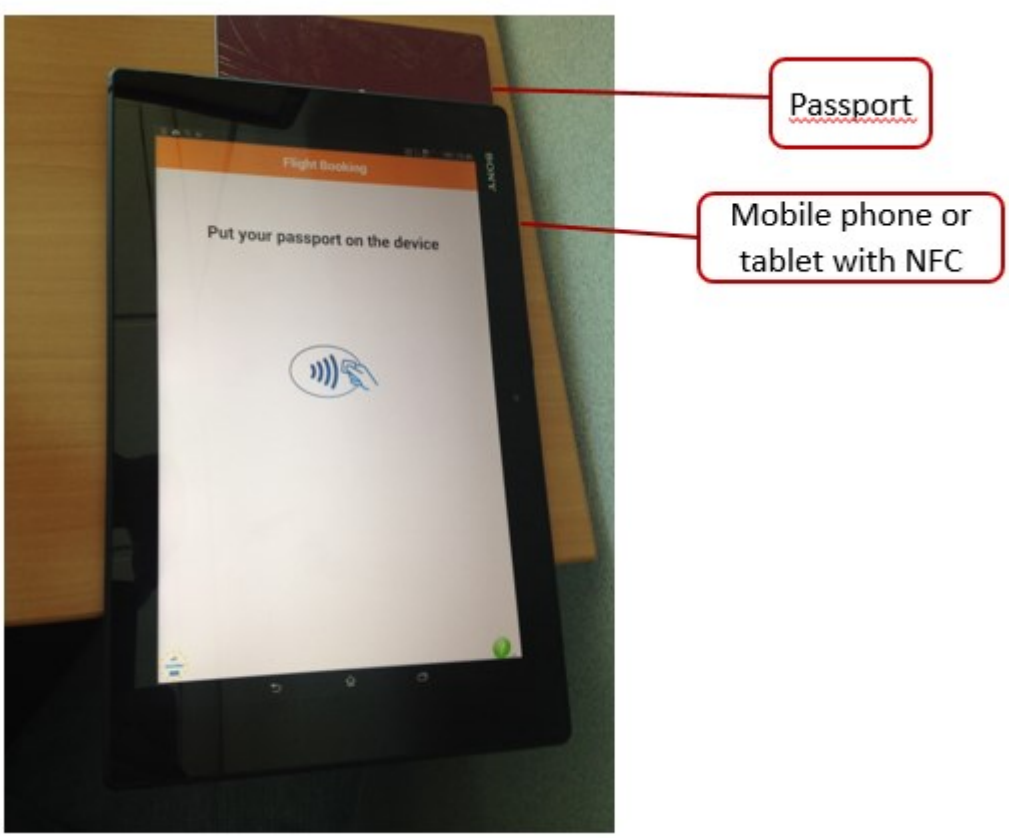
Autres:

- Clés et certificats de clés publics pour la transaction EAC
- Document de voyage électronique 4ème génération, compatible avec SAC, EACv2, LDSv1 et LDSv2

Réservation de vols

Description générale

Architecture générale:

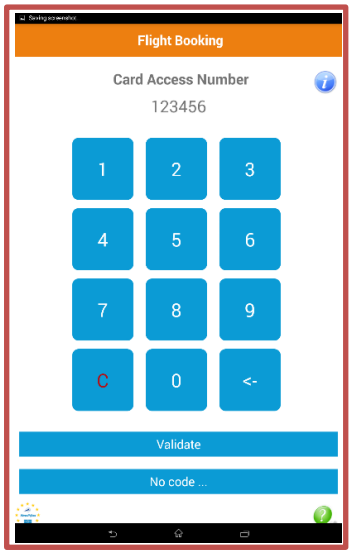


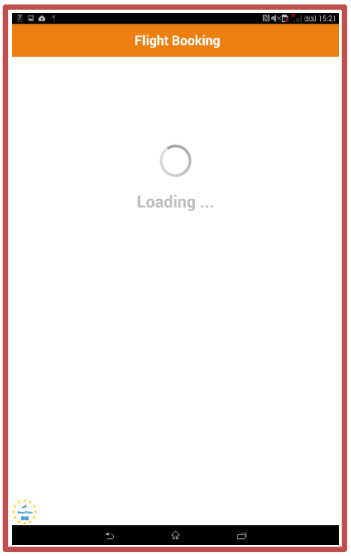
Scénario d'usage:

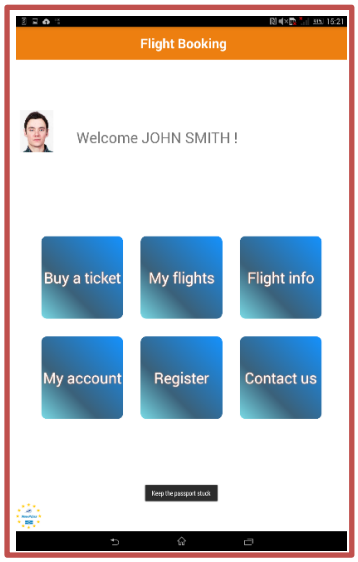
- Entrer CAN ou MRZ
- Effectuer PACE ou BAC
- Log in
- Acheter un billet
- Remplissage de forme automatique

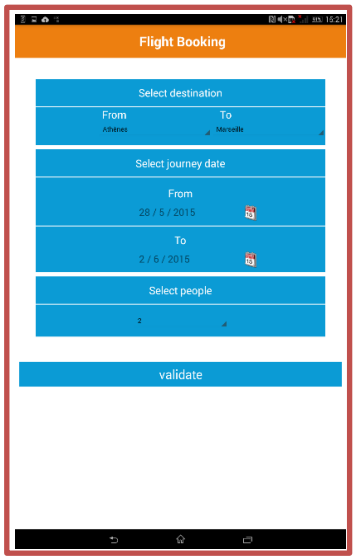

Flight Booking


Flight Booking
Put your passport on the device

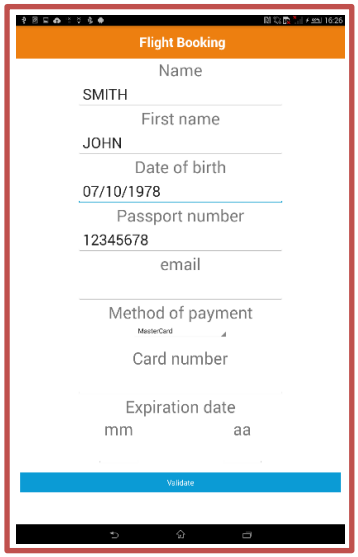

Flight Booking
Card Access Number
123456
1
2
3
4
5
6
7
8
9
C
0
<-
Validate
No code ...

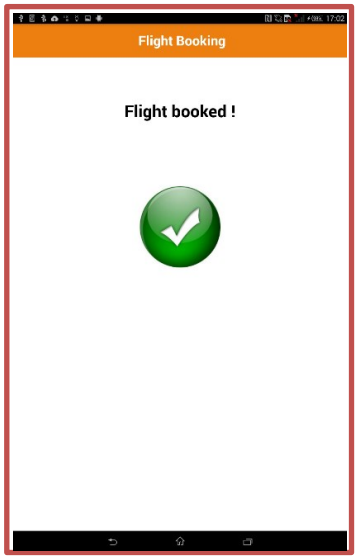

Flight Booking
Loading ...


Flight Booking
Welcome JOHN SMITH !
Buy a ticket
My flights
Flight info
My account
Register
Contact us


Flight Booking
Select destination
From
To
Select journey date
From
28 / 5 / 2015
To
2 / 6 / 2015
Select people
validate


Flight Booking
depart
arrivée
A partir de
06:55
20:10
2300€
07:46
20:42
2460€
08:23
21:17
2670€
09:58
22:03
2440€
11:26
00:04
2620€
13:04
01:08
2330€
14:24
02:12
2760€

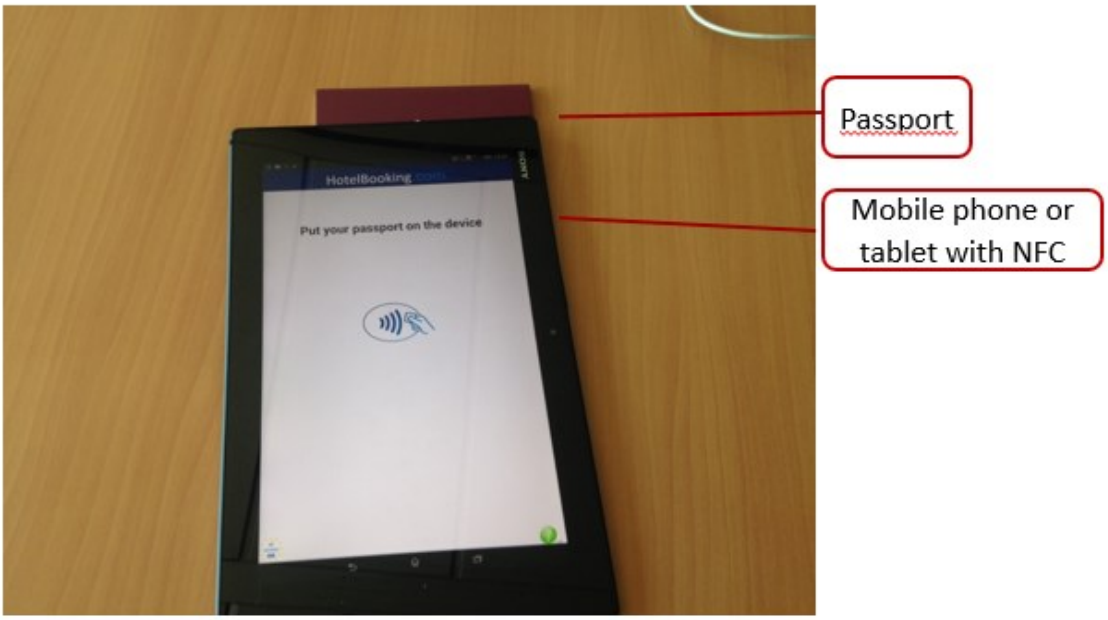

Flight Booking
Name
SMITH
First name
JOHN
Date of birth
07/10/1978
Passport number
12345678
email
Method of payment
Card number
Expiration date
mm
aa


Flight Booking
Flight booked !

Réservation d'un hôtel

Description générale

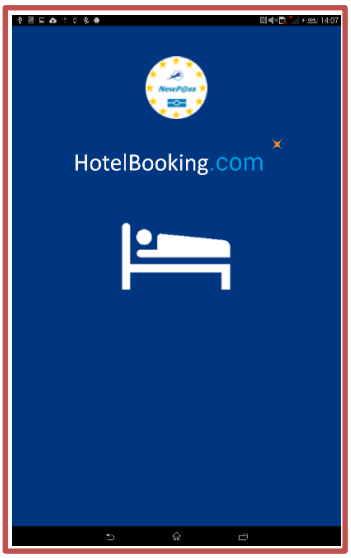
Architecture générale :



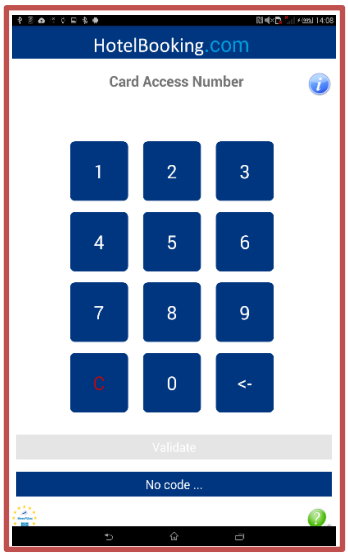
Scénario d'usage:

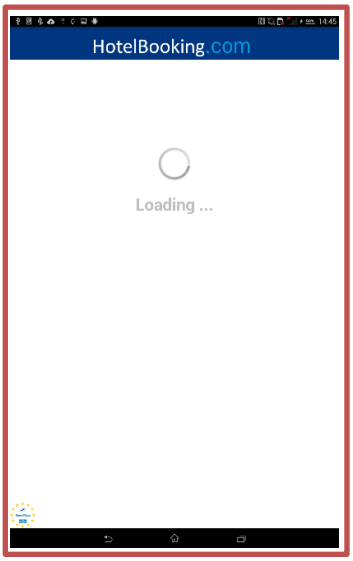
- Entrer CAN ou MRZ
- Effectuer PACE ou BAC
- Log in
- Réserver un hôtel
- Remplissage de forme automatique

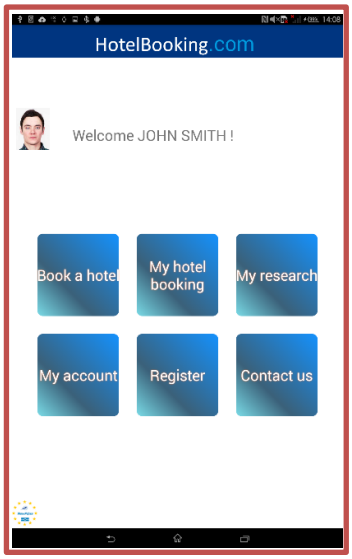
•

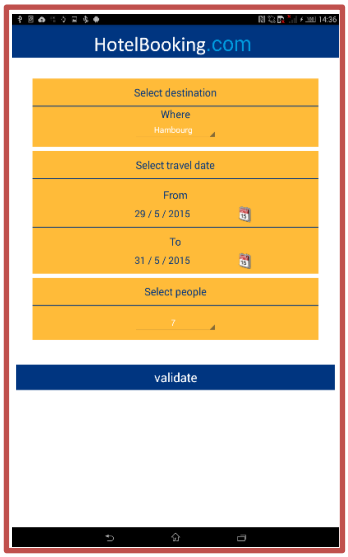

HotelBooking.com


HotelBooking.com
Put your passport on the device

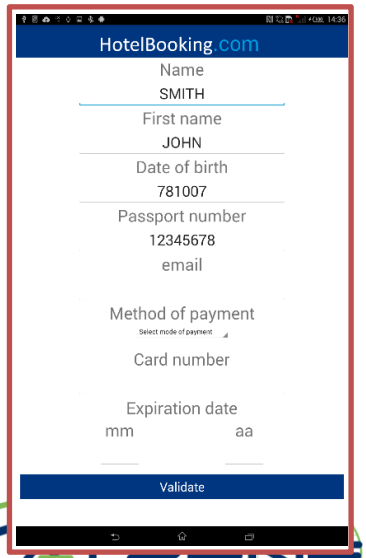

HotelBooking.com
Card Access Number
1
2
3
4
5
6
7
8
9
C
0
<-
Validate
No code ...

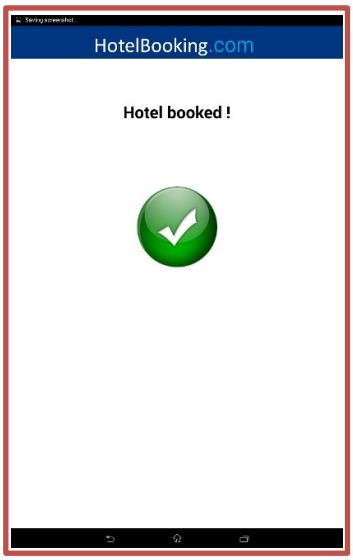

HotelBooking.com
Loading ...


HotelBooking.com
Welcome JOHN SMITH !
Book a hotel
My hotel booking
My research
My account
Register
Contact us


HotelBooking.com
Select destination
Where
Hambourg
Select travel date
From
29 / 5 / 2015
To
31 / 5 / 2015
Select people
validate


HotelBooking.com
A partir de
70€
A partir de
76€
A partir de
98€
A partir de
84€
A partir de
88€
A partir de
97€

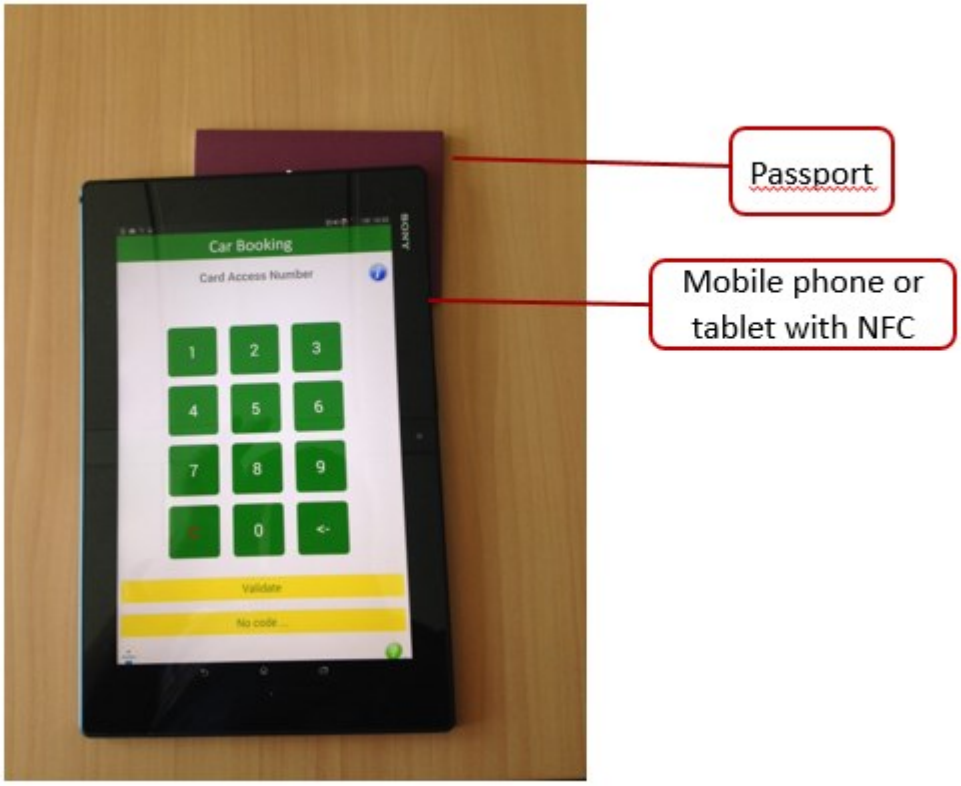

HotelBooking.com
Name
SMITH
First name
JOHN
Date of birth
781007
Passport number
12345678
email
Method of payment
Card number
Expiration date
mm
aa
Validate


HotelBooking.com
Hotel booked !

Réservation d'un voiture

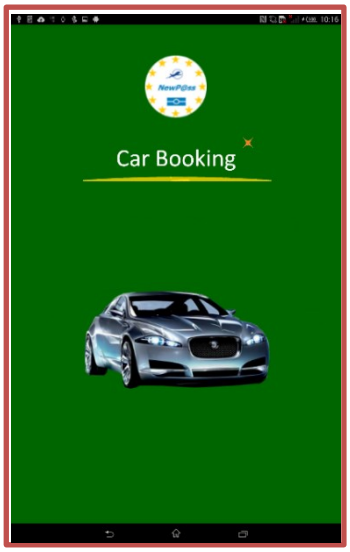
Description générale

Architecture générale:

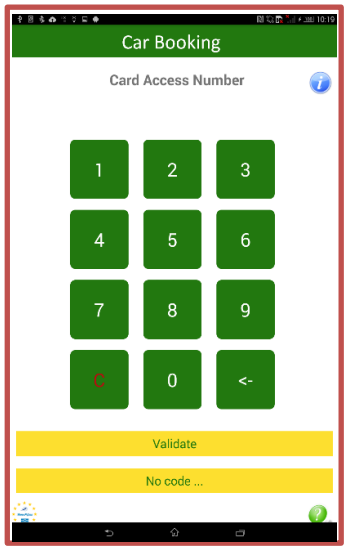


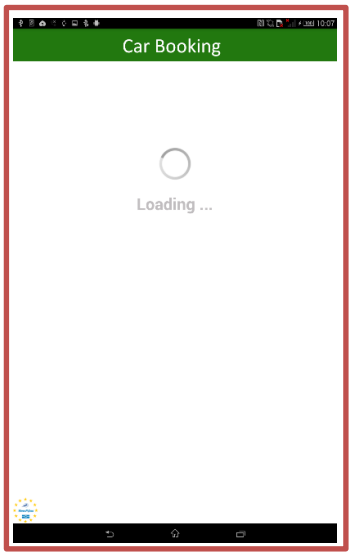
Scénario d'usage:

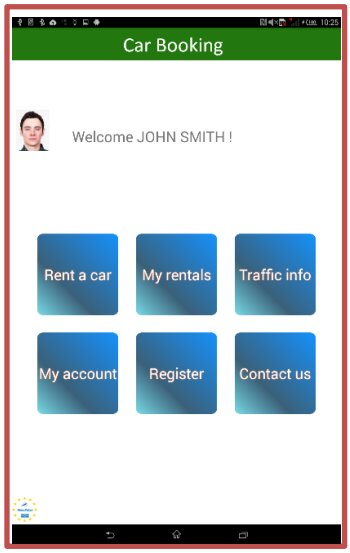
- Entrer CAN ou MRZ
- Effectuer PACE ou BAC
- Log in
- Réserver une voiture
- Remplissage de forme automatique

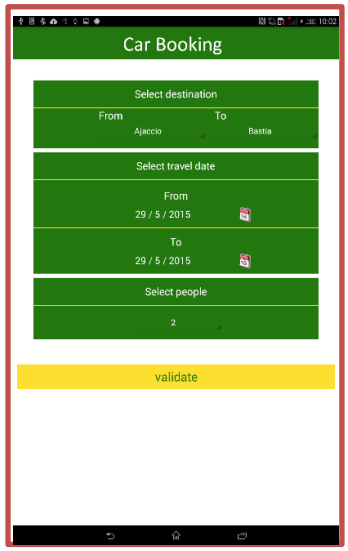

Car Booking


Car Booking
Put your passport on the device

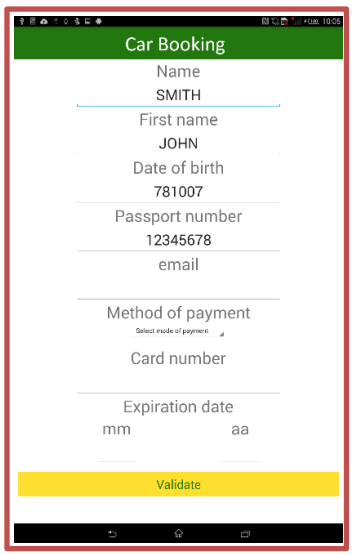

Car Booking
Card Access Number
1
2
3
4
5
6
7
8
9
C
0
<-
Validate
No code ...

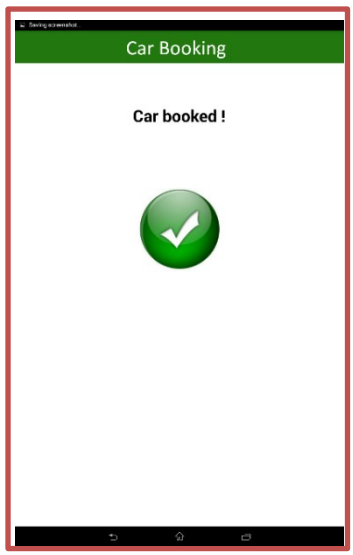

Car Booking
Loading ...


Car Booking
Welcome JOHN SMITH !
Rent a car
My rentals
Traffic info
My account
Register
Contact us


Car Booking
Select destination
From
Ajaccio
To
Bastia
Select travel date
From
29 / 5 / 2015
To
29 / 5 / 2015
Select people
2
validate


Car Booking
A partir de
70€
A partir de
76€
A partir de
98€
A partir de
84€
A partir de
88€
A partir de
97€
A partir de


Car Booking
Name
SMITH
First name
JOHN
Date of birth
781007
Passport number
12345678
email
Method of payment
Card number
Expiration date
mm
aa
Validate


Car Booking
Car booked !

6.8. SP8 Diffusion et Normalisation

6.8.1. Introduction

Pilote du projet	**Instituto Telecommunicacoes (IT)**
Partenaires	Gemalto, STMicroelectronics, ID3 Technologies, CEA-LETI, NXP-F-G-A, IFAT, G&D, Evoleo, IAIK
Objectifs du SP	Diffuser les concepts du projet newp@ss, les connaissances acquises au cours du projet, et les résultats scientifiques dans des revues universitaires et les grandes conférences internationales. Montrer les concepts de la plate-forme newp@ss lors d'expositions internationales clés et de réunions industriels. Promouvoir les technologies de newp@ss dans les organismes de normalisation appropriées. Organiser des ateliers spécialisés et des événements : exposition / démos finale;Décrire les plans d'exploitation des technologies newp@ss dans les produits commerciaux afférent à chaque partenaire.

Ce sous projet (SP) est divisé en 3 tâches principales:
• **Tâche 1:** Diffusion et exploitation (Diffuser les résultats du projet à travers le site internet officiel et public ; publier dans des revues académiques, conférences et congrès ; élaborer les plans d'exploitation des résultats du projet pour chaque partenaire)
• **Tâche 2:** Activités de normalisation (Participer dans les consortiums et les groupes de travail de normalisation)
• **Tâche 3:** Présentation des démonstrateurs finaux (Présenter des cas d'usage, des démonstrateurs ou des réalisations majeures, aux parties prenantes majeures : gouvernement, les agences de l'UE)

6.8.2. Activités par périodes et partenaires

2012:

Activités de diffusion par partenaire

Gemalto et les partenaires ont participé au forum européen de nanoélectronique se déroulant à Munich du 20 au 22 novembre. Un poster a été présenté à cette occasion.
IT et les partenaires ont défni la structure et le contenu d'un site internet permettant à la fois la gestion interne du projet et la diffusion des résultats du projet à un public plus large. L'adresse publique est http://newpass.av.it.pt.
Une liste initiale des événements préliminaires où le projet pourrait fournir une contribution a été préparée par le PMB.
Un comité consultatif du projet regroupant les représentants du BSI allemand et l'ANSSI français et ANTS a été créé. Ce comité se réunit au moins une fois par an avec l'équipe du projet pour discuter des progrès techniques, mais aussi fournir une orientation stratégique pour évaluer les résultats du projet par rapport aux priorités nationales ou internationales.

Activité de normalisation par partenaire

Gemalto

Des activités préliminaires de diffusion ont déjà commencé au second semestre 2012 au cours de plusieurs réunions pertinentes de manière à offrir de la visibilité au projet.

- Participation à l'AFNOR dans la commission « carte et technologie » CN17 ge3
- Participation au comité de normalisation ISO WG3 dans le pôle « force d'action 4 » (Evolution des tests pour les couvertures de passeport)
- Participation aux réunions de l'OACI GTR LDS2, pour la stratégie d'orientation pour développer les spécifications techniques de LDS2 basée sur les exigences gouvernementales
- Participation aux réunions ISO SC17 WG3
- Participation aux réunions de l'ISPRA EU article 6

ST

Les activités de diffusion n'ont pas encore commencées.
Concernant les activités de normalisation, ST suit les activités suivantes

- ISO/IEC JTC1/SC17/WG8 (Norme VHBR)
- ISO/IEC 15408
- Spécifications GlobalPlatform
- ETSI SCP
- ST est aussi membre de l'alliance française de la Confiance Numérique

CEA-LETI

Le CEA-Leti est impliqué dans le processus de normalisation de la technologie VHBR avec le bureau de normalisation locale française AFNOR. Cette activité est réalisée au sein du comité SC17 du groupe de travail WG8 qui est directement liée à la commission WG8 / SC17 à l'ISO. Tous les documents publiés depuis le WG8 / SC17 sont étudiés afin d'avoir une vue d'ensemble de la future norme, et éventuellement de proposer des améliorations précises.

IFX

Les activités de diffusion n'ont pas encore commencées.
Les participations aux activités de normalisation n'ont pas encore été identifiées.

Giesecke & Devrient

Les activités de diffusion n'ont pas encore commencées.

- Participation à l'ISO/IEC JTC1/SC17/WG3 : passeport électronique, LDS1+, LDS2
- Participation à l'ISO/IEC JTC1/SC17/WG4 : interface des cartes à puce, ISO/IEC 7816, protocole d'affichage
- Participation au comité GlobalPlatform : environnement d'exécution sécurisé, APIs, profil de protection
- Participation à la force d'action gouvernementale relative à la GlobalPlatform: Spécifications des plates formes gouvernementales

NXP-G

Les activités de diffusion n'ont pas encore commencées.

IFAT
Les activités de diffusion n'ont pas encore commencées.
Les participations aux activités de normalisation n'ont pas encore été identifiées.

NXP-A
Les activités de diffusion n'ont pas encore commencées.
Les participations aux activités de normalisation n'ont pas encore été identifiées.

IT
IT synthétise toutes les activités de normalisation des partenaires afin de maximiser les entrées du projet vers des organismes internationaux.

Id3
Les activités de diffusion n'ont pas encore commencées.

2013:

Activités de diffusion par partenaire

IT (pilote du SP)
IT a réalisé le site officiel du projet newp@ass et en assure la maintenance. L'activité du site est nourrie à partir des données fournies par tous les autres partenaires. IT a également mis en place un système de dépôt de fichiers pour le partage de documents entre tous les partenaires. Cette infrastructure informatique est hébergée sur des serveurs dans ses installations. IT a également constitué une liste des adresses de messagerie de tous les partenaires pour faciliter la communication interne.
En activité complémentaires, IT a présenté brièvement sur un programme de la radio nationale portugaise le projet Newp@ss.

Gemalto
Des activités de diffusion préliminaires ont eu lieu, notamment, en fournissant une visibilité certaine du projet dans plusieurs réunions pertinentes. Une proposition de présentation du projet pour l'édition de la conférence « e-ID World » en septembre 2013 a été faite et acceptée par le comité du programme du congrès.

NXP-A
Les premiers résultats de travaux de recherche du SP6 ont été présentés et publiés lors la conférence IECON 2013. Conjointement avec UT et IAIK, les résultats des SP5 et SP6 ont été publiés pour le salon « VALID 2013 ».
NXP-G
Au nom du consortium, NXP (Mario Stolz, membre du PMB) a présenté un aperçu du projet newp@ss, dans au cours du forum « Security Document World« (SDW) se déroulant le 21 et 22 mai 2013 à Londres, au Royaume-Uni. Environ 120 participants provenant des gouvernements, des autorités de police, du contrôle des frontières et des affaires intérieures ministères ont suivi l'exposé, intitulé «newp@ss – œuvrer vers l'évolution passeport électronique du futur ".
Au cours de 2013, seules des activités mineures ont eu lieu. NXP a surveillé les activités de normalisation relatives au projet newp@ss et a référencé le projet dans les discussions avec les parties prenantes externes, le cas échéant.

TU Graz/IAIK
Les premiers résultats de travaux du SP5 ont été acceptés pour une publication à la conférence VALID 2013. Les activités de diffusion n'ont encore commencées.

Activité de normalisation par partenaire

Gemalto

- Participation à l'AFNOR dans la commission « carte et technologie » CN17 ge3 (document de voyage et permis de séjour)
- Participation au comité de normalisation ISO WG3 dans le pôle « force d'action 4 » (Evolution des tests pour les couvertures de passeport)
- Participation aux réunions de l'OACI GTR LDS2, pour la stratégie d'orientation pour développer les spécifications techniques de LDS2 basé sur les exigences du gouvernement
- Participation aux réunions ISO SC17 WG3
- Participation aux réunions de l'ISPRA EU art6

NXP-F
NXP France est actif au sein du Forum NFC et aux comités de normalisation ETSI SCP. Ces normes relatives à la technologie NFC sont également indirectement liées aux lecteurs de passeports électroniques, car il est prévu que les lecteurs soient dotés d'une compatibilité NFC et d'avoir des téléphones mobiles agissant en tant que lecteurs de passeports électroniques. En outre, depuis le 2ème trimestre 2013, une attention particulière est faite aux spécifications proposées par GlobalPlatform relative à la certification d'éléments sécurisés embarqués. NXP est un membre actif du groupe en charge de définir les extensions HCI, qui sont nécessaires pour veiller à ce que les applications hébergées sur l'élément sécurisé embarqué puissent être gérés à distance.

ST

- Participation in ETSI SCP
- Participation à ISO/IEC JTC1/SC17/WG8 (Norme VHBR)
- Participation à ISO/IEC 15408
- Participation à l'association GlobalPlatform

ST est aussi membre de l'alliance française de la Confiance Numérique, consortium français de promotion de solutions d'identité numérique.

Id3 Technologies
Actuellement, Id3 ne participe à aucune activité de normalisation en rapport au projet Newp@ss.

ISEN-Toulon
Actuellement, ISEN Toulon ne participe à aucune activité de normalisation en rapport au projet Newp@ss. ISEN Toulon a prévu de publier dans des revues scientifiques spécialisées ses premiers résultats concernant les bancs de test RF.

CEA-Leti
Le CEA-Leti participe au processus de normalisation VHBR l'interface sans contact, avec le bureau de normalisation locale française AFNOR et au niveau international (ISO). Cette activité est réalisée dans le SC17 du comité de l'WG8 du groupe de travail qui est directement liée à la commission WG8 / SC17 à l'ISO. Tous

les documents publiés depuis le WG8 / SC17 ont été étudiés afin d'avoir une vue d'ensemble de la future norme, et éventuellement de proposer des améliorations précises. Le CEA-Leti a prévu de poursuivre les activités de normalisation de la technologie VHBR tant que tous les amendements sur cette technologie ne sont pas arrêtés. A la suite de quoi, le CEA-Leti publiera dans les journaux scientifiques spécialisés, une partie de ses travaux sur développement d'une fonction VHBR pour carte à puce.

IFX

En février 2013, IFX a participé au groupe de travail de l'OACI TF5, qui est en charge de la définition de la nouvelle structure de donnée des passeports (ICAO_LDS2.0) ainsi que la normalisation ICAO_CAN.
En mai 2013, IFX a participé à la première mondiale sur le test de l'interopérabilité ICAO_SAC à Londres, RU.
Le 4 octobre 2013, IFX également participé au groupe de travail TF5 à Berlin, en Allemagne, sur le thème «1er enquête sur l'impact de la structure de donnée LDS2. 0 sur le matériel et le logiciel".

Giesecke & Devrient

G & D contribue aux activités de normalisation suivant:

- Normalisation des passeports électroniques (ISO / CEI JTC 1 SC17 GT3 et DIN NIA 17-03)
- Environnement d'exécution sécurisé, définition de l'interface utilisateur de confiance et Profil de protection selon des critères communs (commission GlobalPlatform), fonctions de gestion d'administration, des API de fonctions internes supplémentaires, API des éléments sécurisés et du canal sécurisé.
- CEN TC 224 GT 16: Définition de nouveaux protocoles d'authentification

NXP-G

- Participation à la norme ISO / IEC JTC1 / SC17 / WG8 TF2 relative à la modulation PSK, aux débits élevés (> 13,56 Mbps)
- Participation à la norme ISO / IEC 15408 relative à la certification de la sécurité.
- Participation à la norme ISO / CEI (divers comités) relative aux activités d'affichage sur les cartes.
- Participation aux comités standardisation de GlobalPlatform relatifs l'architecture sécurisée, à la reconfiguration après délivrance du passeport, et au fonctionnement parallélisé
- Participation au groupe de travail TF5 à l'OACI: Suivi et participation à définition de la structure de donnée LDS 2.0

IFAT

IFAT participe aux réunions de normalisation relative à la technologie VHBR ISO / IEC 14443.

NXP-A

Actuellement, NXP-A ne participe à aucune activité de normalisation en rapport au projet Newp@ss

IT

En tant que pilote du SP8, IT collecte les informations auprès des partenaires concernant leur participation à des activités de normalisation et constitue la liste de comités de normalisation où chaque partenaire contribue.
IT ne participe à aucune activité de normalisation en rapport au projet Newp@ss.

Evoleo

Actuellement, Evoleo ne participe à aucune activité de normalisation en rapport au projet Newp@ss

TU Graz / IAIK

TU Graz /IAIK ne participent à aucune activité de normalisation en rapport au projet Newp@ss.

2014:

Activités de diffusion par partenaire

IT (pilote du SP)
IT maintient le site newp@ss, avec les entrées produites par tous les partenaires. Le système de dépôt de fichier, crée par IT, pour le partage de documents entre tous les partenaires, a son serveur hébergé dans ses installations. Cette infrastructure fournit un soutien aux partenaires ayant des difficultés d'accès ou d'exploitation. Onze listes d'adresses de courrier électronique, également établies par IT, sont intensivement utilisées par les partenaires. Ces listes sont également activement maintenues par IT durant 2014.

Une brève présentation de newp@ss, faite par Mr Joaquim Bastos (IT), a été diffusé le 15 Février 2014, au cours d'un programme de la radio nationale portugaise (RTP / RDP Antenne 1, "Cliquez sur" programme), L'interview en portugais, est disponible en radiodiffusion sur le site Web de la RTP (http://www.rtp.pt/play/p384/e144301/click).

IT a produits 2 articles relatifs au projet Newp@ss pour les conférences suivantes

- E. Alireza, A. Nascimento, J. Rodriguez, J. C. Neves, "An Efficient MAC-Signature Scheme for Authentication in XOR Network Coding", in Proceedings of the Nineteenth IEEE Symposium sur les ordinateur et les communications (ISCC 2014), Funchal, Madeira, Portugal, du 23 au 26 Juin, 2014.

- J. Bastos, G. Mantas, J. C. Ribeiro, J. Rodriguez, "Towards an Advanced PKI-based Security Solution for Next Generation e-Passport and Associated Applications: The NewP@ss Approach", 8e conférence international sur l'internet sans fil Symposium sur Communication sans fil et véhicule (WiCON 2014), Lisbon, Portugal, du 13 au 14 novembre 2014.

Gemalto
Des activités de diffusion préliminaires ont eu lieu, notamment, en fournissant une visibilité certaine du projet dans plusieurs réunions pertinentes. Un passeport prototype de 3eme génération a été présenté durant la session de test d'interopérabilité qui s'est tenue en juin 2014 à Barcelone.

Le projet a été présenté aux instances ou événement suivant :
- Forum mondial d'identité électronique (eID), en septembre 2014
- ANTS (agence Nationale des Titres Sécurisés) Octobre en 2014

Id3 Technologies
Id3 a participé au forum Secure document world (SDW). A cette occasion, ID3 a montré une présentation animée des principaux objectifs du projet. La présentation, une animation Prezi, peut être vue sur le lien suivant:
http://prezi.com/m6agj7vgaxiu/?utm_campaign=share&utm_medium=copy
Id3 a participé au salon Cartes 2014. A cette occasion, ID3 a présenté les activités du projet Newp@ss sur son stand d'exposition.

TU Graz/IAIK
Des résultats ont été acceptés pour des événements scientifiques clés. (CHES, Ares). D'autres publications sont encore à l'étude et en cours de préparation en vue de soumission.

Les articles scientifiques suivants ont été présentés durant la période en cours :

- Spreitzer R., Schmidt J.-M., "Group-Signature Schemes on Constrained Devices: The Gap Between Theory and Practice", Atelier sur la Cryptographie et sécurité sur les systèmes informatiques (CS2), Vienne, Autriche, Janvier 2014.
- Wenger E., Wolfger P.: “Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster”, SAC 2014.
- Unterluggauer T., Wenger E.: “Practical Attack on Bilinear Pairings to Disclose the Secrets of Embedded Devices”, ARES 2014.
- Unterluggauer T., Wenger E.: “Efficient Pairings and ECC for Embedded Systems”, CHES 2014.
- Slamanig D., Spreitzer R., Unterluggauer T.: « Adding Controllable Linkability to Pairing-Based Group Signatures For Free“, ISC 2014.

Les autres partenaires n’ont pas reporté d’activité de diffusion sur la période en cours.

Activité de normalisation par partenaire

Gemalto
Pendant l’année, Gemalto a contribué à diverses réunions liées au projet newp@ss relatives la sécurisation des documents de voyage lisible par machine. (MRTD)

Gemalto a rencontré le sous-groupe gouvernemental de l'OACI dédié à l’orientation de la norme relative à structure de donnée logique (LDS2) aux Pays-Bas à La Haye en Janvier 2014 pour relancer le processus gouvernemental sur la décision concernant le niveau de contrôle d'accès par les autorités et des organisations spécifiques.

La réunion a été l'occasion de mettre à jour le plan de déploiement de la LDS2 ainsi que les cas d'utilisation. La révision entière a été validée lors de la réunion de l'OACI GTR à Paris en avril. Les principales décisions sont résumées dans le livrable D8.2 « Rapport de diffusion et le rapport de normalisation ».

Pendant le second semestre, Gemalto a contribué à diverses réunions liées à newp@ss portant sur la sécurisation des documents et normes MRTD. Le sous-groupe gouvernemental de l'OACI dédié à orientation de la norme LDS2, a été rencontré à Kuala Lumpur en Novembre 2014. La réunion a été l'occasion de mettre à jour le plan de déploiement de la LDS2 et les cas d'utilisation. La révision entière a été validée lors de la réunion de l'OACI en novembre au même endroit. Les principales décisions sont résumées dans le livrable D8.3 « rapport diffusion et de normalisation » actuellement en cours de préparation.

En parallèle, le comité de normalisation ISO SC17 GT3 a eu une réunion à Salamanque. Dans le groupe de travail TF5, mis à jour les versions officielles des spécifications de LDS2. Les exigences sont divisées en 3 parties et de prendre une partie de la 3 principale 9303 série fait partie de 10, 11 et 12:

- **La structure de données:**
  - 9303 Part10 LDS - § LDS_2.0 data structure
- **Procédure du système d’inspection et protocole d’accès sécurisé:**
  - 9303 Part11 LDS - § LDS_2.0 procédure d’inspection
- **Infrastructure à clé publique**:
  - 9303 Part12 LDS - § LDS_2.0PKI Version préliminaire 2.0

Gemalto a également participé aux réunions suivantes :

- 2014-01-17, and 2014-3-12 Gemalto, (national) **AFNOR Standard CN17 ge3**: **Réunion plénière**

- 2014-04-01 to 03, Gemalto, (international) Siège de la gendarmerie française: réunion OACI NTWG
- 2014-04-14 to 20, Gemalto, (international) **Tokyo: ISO SC17 WG3 Réunion plénière**
- WG3 et ses cinq (5) groupes de travail ont fourni une assistance technique à l'OACI dans de nombreux domaines au cours de la dernière année pour NTWG, ICBWG, LDS2 and the PKD.
- 2014-05-14, Gemalto, (national) **AFNOR Standard CN17 ge3**
- 2014-06-04, Gemalto, (national) AFNOR comité stratégique COS CN17
- *2014-08-26, Gemalto, (international) réunion **OACI RFI à Montréal***
- *2014-09-03, Gemalto, (national)* comité stratégique ***AFNOR standards:** statu sur les normes internationales et européenne (art6, ICAO LDS2, ISO, PKD, …)*
- *2014-09-16, Gemalto, (national) **AFNOR Standard CN17 ge3-ge10*** **Réunion plénière** – *documents de voyage & permis de séjour : statut sur les réunions international et européenne (art6, ICAO LDS2, ISO, PKD, …) – Convergence de normes pour le passeport electronique–*
- *2014 29/09-01/10 Gemalto, (international) **SALAMANCA: ISO SC17 WG3*** Réunion plénière *et groupe de travail*
- *2014-10-01 to 03, Gemalto, (international) **SALAMANCA: ISO SC17*** Réunion plénière
- *2014-10-30, Gemalto, (national) **ANTS/AFNOR**:* Atelier "programme TRIP" Examen des travaux en cours sur passeport électronique, Validation de commentaires /Mise à jour de la LDS2 suite à la réunion de Salamanque.
- *2014-11-11 to 13, Gemalto, (international) **OACI NTWG**, Kuala Lumpur.* Programme trip : Détails pour les membres et rapport par pays, RFI participation et conclusion. Mise à jour sur la reconnaissance faciale et sur les permis de séjour,
- *2014-11-21, Gemalto, (national) **ANTS**: Atelier du programme TRIP sur les orientations françaises et application mobile*
- *2014-12-01 to 05, Gemalto, (international) **ICAO ICBWG**, BRASILIA*
- *2014-12-15, Gemalto, (national) **AFNOR Standard CN17 ge3**:* Réunion plénière – *documents de voyage &permis de séjour : statut sur réunions Internationales & EU (art6, ICAO LDS2, ISO, PKD, …)*
- *2014-12-16, Gemalto, (national) **ANTS/art6**: atelier de travail*

NXP-F

Aucune activité sur la période.

ST

ST poursuit ses participations dans la norme ISO / IEC JTC1 / SC17 / GT8 (processus de normalisation de l'ISO 14443 VHBR) et ISO / IEC 15408. Les activités sont en cours au sein du comité GlobalPlatform ETSI SCP

CEA-Leti

Durant le second semestre 2014, le CEA-Leti a participé au Salon Cartes 2015. A cette occasion, le CEA LETI a fait la promotion du projet de newp@ss et de la technologie VHBR sur son stand d'exposition.
Le travail technique de l'ISO SC17 / GT08 sur VHBR est maintenant terminée pour l'ISO 14 443-2 amd5.

ISEN-Toulon

Comme activité de diffusion, ISEN a introduit la technologie de passeport dans ses activités d'enseignement. Un projet d'ingénierie pour les étudiants M2 a été lancé en octobre 2014, avec l'aide de Gemalto. Le groupe a développé des logiciels libres pour la lecture de passeports 3G et 4G, sur la base déjà disponibles des logiciels JMRTD disponible en open source. Une assistance ponctuelle a été donnée par G & D.

IFX

En février 2013, IFX a participé à Singapour, au groupe de travail de l'OACI TF5, qui est en charge de la définition de la nouvelle structure de donnée des passeports (ICAO_LDS2.0) ainsi que la normalisation ICAO_CAN.

Le 4 octobre 2013, IFX également participé au groupe de travail TF5 à Berlin, en Allemagne, sur le thème «1er enquête sur l'impact de la structure de donnée LDS2. 0 sur le matériel et le logiciel".
En juin 2014, IFX a participé au second test mondial d'interopérabilité ICAO_SAC à Madrid.

ICAO_NTWG_TF5	LDS2.0, CAN	Mark Stafford, USA
SC17 WG10	eDL	Manfred Roth, Deutschland
SC17 WG15	eDAS token	Detlef Houdeau, Deutschland
SC17 WG04	Display	Manfred Roth, Deutschland

Giesecke & Devrient
G&D a contribué aux activités de normalisation suivantes:

- Normalisation du passeport electronique (ISO/IEC JTC 1 SC17 WG3 and DIN NIA 17-03)
- • Environnement d'exécution sécurisé, définition de l'interface utilisateur de confiance et Profil de protection selon des critères communs (commission GlobalPlatform), fonctions de gestion d'administration, des API de fonctions internes supplémentaires, API des éléments sécurisés et du canal sécurisé.
- Primitives cryptographiques supplémentaires pour les protocoles cryptographiques efficaces utilisés dans les passeports électroniques (Forum Java Card)
- Concepts de certification pour les applets JavaCard (GlobalPlatform GT sécurité de la carte)
- Amélioration des certifications des critères communs composites (ISCI)
- Discussion sur les nouveaux chemins d'attaque et de leurs évaluations selon les critères communs (JIL / ARP)
- Communication sans contact avec les puces RFID (ISO/IEC JTC1 SC17 WG8)

NXP-G
Pendant H2 / 2014, des activités mineures ont eu lieu. NXP a fait de la veille normative en rapport au projet newp @ss. Un nouveau projet de LDS2.0 a été mis au point, mais pas encore diffusé.

IFAT
IFAT a participé à la 42ème édition de la réunion de ISO/IEC JTC1/SC17/WG8/TF2 à Kochel en Allemagne, du 28 au 30 janvier 2014 ainsi qu'à la 43ème édition de la réunion de l'ISO/IEC JTC1/SC17/WG8/TF2 à Neuchâtel en Suisse du 8 au 9 avril 2014.
IFAT a également participé à la 44ème édition des réunions ISO/IEC JTC1/SC17/WG8 et ISO/IEC JTC1/SC17/WG8/TF2du 22 au 26 septembre 2014 à Salamanque en Espagne ainsi qu'à à la 45ème édition des réunions ISO/IEC JTC1/SC17/WG8 et ISO/IEC JTC1/SC17/WG8/TF2 à Hiroshima au Japon du 23 au 26 février 2015.

IT
En tant que pilote du SP8, IT collecte les informations auprès des partenaires concernant leur participation à des activités de normalisation et constitue la liste de comités de normalisation où chaque partenaire contribue.
IT ne participe à aucune activité de normalisation en rapport au projet Newp@ss.

2015:

Activités de diffusion par partenaire

IT (Pilote du SP)
Toutes les activités de diffusion et de normalisation menées par des partenaires newp@ss ont été recueillies, compilées et répertoriées par IT (rédacteur) dans livrable D8.3. Le site newp@ss, créé et géré par informatique, a été tenu à jour, également avec ces informations compilées. IT assure le support à tous les partenaires ayant des difficultés d'accès ou d'exploitation concernant le dépôt de fichiers newp@ss utilisé pour le partage de documents. Onze listes d'adresses de courrier électronique, également établie par IT, sont intensivement utilisées par les partenaires. Ces listes sont également été activement maintenues par IT durant 2015.

TI et Evoleo ont participé à l'organisation d'un atelier - Redes de Veiculos nas Sociedades do Futuro, le 3 Juin, à Castelo Branco, Portugal, où a été présenté un démonstrateur commun sur un stand d'exposition: " NewP@ss 4G PKI Travel records demo "

Gemalto
Dans la première moitié de 2015, Gemalto a continué ses activités de diffusion vers des groupes de normalisation liés au passeport électronique (voir D 8.4 pour plus de détails).

Id3 Technologies
ID3 participé à deux expositions au cours des six premiers mois de 2015. À ces occasions, ID3 a présenté les activités newp@ss sur son stand.
• Cartes Sao Paulo exposition du 14 au 16 Avril à 2015.
• Cartes et paiement Moyen-Orient Dubaï 14 et 15 mai à 2015.

Id3 commence la promotion du nouveau lecteur de VHRB conçu pendant projet NewP@ss. L'ambition d'ID3 est de proposer cette nouvelle génération de lecteur RFID VHBR en plus de lecteurs RFID actuels sur le marché.

TU Graz/IAIK
Roderick Bloem, Daniel Hein, Franz Rock, Richard Alexander Schumi: «Case Study: Automatic Test Case Generation for a Secure Cache Implementation", TAP en 2015.

CEA-LETI
CEA Leti a en cours deux demandes de brevet. Ils décrivent l'architecture du récepteur VHBR défini et mis en œuvre dans l'ASIC réalisé dans SP3.

- P. Courouve, J.-B. Doré and M. Pezzin : "Very high datarate RFID receiver", n° FR 1556536. 09/07/2015
- P. Courouve, J.-B. Doré and M. Pezzin : « Quadrature demodulator for very high datarate RFID receiver », n° FR 1556537. 09/07/2015

CEA-LETI a contribué à la diffusion de la méthodologie formelle pour les concepteurs, développé par NXP-A pour le processus d'évaluation de sécurité. Cette méthodologie est basée sur le modèle de contrôle et est une approche plus rentable que des théorèmes trop sophistiqué de preuve. Une présentation de cette méthodologie a été réalisée par le CEA-Leti à l'ANSSI, organisme de certification français de critères communs, afin d'avoir la possibilité de l'utiliser dans le système d'évaluation des critères communs.

Activité de normalisation par partenaire

Gemalto

Au cours de la période en cours, Gemalto a contribué à diverses réunions en rapport aux activités du projet newp@ss, notamment concernant la sécurité des documents et normes MRTD.
Le sous-groupe gouvernemental de l'OACI dédié à l'orientation de la norme LDS2, s'est réuni à Bruxelles en Juin 2015, avec la participation active de Gemalto.
Ces réunions ont été l'occasion de mettre à jour le plan de déploiement de la LDS2 et les cas d'utilisation associés. Toute la révision a été validée lors de la réunion de l'OACI GTR tenue en Novembre dans le même lieu.

Gemalto a participé aux réunions suivantes en 2015

- 2015-01-19/21, Gemalto, (international) réunion **ISO SC17 WG3 TF5 adhoc LDS2,** Berlin

Réunion ISO LDS2 dédiée à l'examen des commentaires d'experts sur la partie 3 du sous projet de norme (par exemple les mécanismes d'accès, de protocoles sécurisés et la PKI). Discussion portant sur la simplification des mécanismes d'authentification et de réduire le nombre de configuration et les options. Proposition de suppression du protocole RSA. Une discussion lancée sur les prochaines étapes et un possible démonstrateur / pilote a été approuvé par le groupe

- 2015-04-01, Gemalto, (national) **AFNOR Standard CN17 ge3-ge10** Réunion plénière - document de voyage et permis de séjour

Statut sur les réunions international et européenne (art6, ICAO LDS2, ISO, PKD, …) – Convergence de normes pour le passeport electronique–

- 2015-04-27/ 30, Gemalto, (international) **Leiden NL: ISO SC17 WG3 réunion plénière et groupe de travails**

  WG3 et ses cinq (5) groupes de travail ont fourni une assistance technique à l'OACI dans de nombreux domaines au cours de la dernière année pour NTWG, ICBWG, LDS2 et PKD.

  - TF1 Révision de la structure de données logiques (LDS), meilleures pratiques dans la gestion d'identité nationale, Maintenance du Document 9303, Normes pour urgence / passeports temporaires, étude sur l'utilisation des codes à barres
  - TF2 rédaction de nouvelles éditions de l'OACI Doc 9303 ED7 - nouvelle version pour publication en Juin
  - TF3 Problématique d'application, Renforcement des capacités de vérification des identités et de la sécurité aux frontières
  - TF4 Essais de durabilité 18745-1, tests d'interface RF 18745-2, tests d'application 18754-3 et Profil d'application préparés par le groupe de travail "sans contact" GT8
  - - TF5 LDS / Maintenance PKI, Révision de la structure de données logiques (LDS), finalisation de la "La structure de données logiques LDS2. Proposition v1" de la LDS2 a été publiée

- 04.05.2015 / 8, Gemalto, (internationale) de l'OACI ICBWG, Australie (aucune présence physique)

Gemalto adressée une contribution non officiel au groupe de travail sur un guide pour l'évaluation de la sécurité et la gestion et la délivrance des documents de voyage pour les Etats

- 2015-05-26, *Gemalto, (national)* ***AFNOR Standard CN17 ge3-ge10*** **Réunion plénière** – *documents de voyage & permis de séjour : statut sur les réunions international et européenne (art6, ICAO LDS2, ISO, PKD, …)*

- 02/06/2015, Gemalto, (internationale) de l'OACI GTR LDS2, Bruxelles. Réunion gouvernementale consacré à l'examen de l'état des travaux en cours et les prochaines étapes sur la partie stratégique. Révision complète du mécanisme d'accès. Examen des stratégies de déploiement par les états membres. Proposition de lignes directrices pour un démonstrateur / pilotes. Rédaction d'un papier blanc sur les démarches à destination du conseil approbation du GT.

- 2015-06-3/5, Gemalto, (international) **ICAO NTWG board**, Bruxelles

Suivi discussions sur les technologies MRTD et LDS2

NXP-F
Pas d'activité sur la période en cours

ST
ST poursuit ses participations dans la norme ISO / IEC JTC1 / SC17 / GT8 (processus de normalisation de l'ISO 14443 VHBR) et ISO / IEC 15408. Les activités sont en cours au sein du comité GlobalPlatform ETSI SCP.

CEA-Leti
Durant le second semestre 2014, le CEA-Leti a participé au Salon Cartes 2015. A cette occasion, le CEA LETI a fait la promotion du projet de newp@ss et de la technologie VHBR sur son stand d'exposition.
Le travail technique de l'ISO SC17 / GT08 sur VHBR est maintenant terminée pour l'ISO 14 443-2 amd5.

ISEN
Comme une activité de diffusion, ISEN introduit la technologie de passeport dans ses activités d'enseignement. Un projet d'ingénierie pour les étudiants M2 a été lancé en Octobre 2014, avec l'aide de Gemalto. Le groupe a travaillé sur développement des logiciels open source pour la lecture de passeports 3G et 4G, sur la base déjà disponibles logiciel open source JMRTD. Le projet a pris fin avec succès en mars 2015, avec la mise à disposition de deux logiciels en open source (pour PC et smartphones) permettant de lire des passeports de génération 3 et 4 à partir du protocole PACE.

Pendant le premier semestre 2015, ISEN-Toulon a participé et coordonné un groupe de discussion consacré à la présentation et à l'évaluation de la prochaine génération de passeport.

IFX
Pas d'activité sur la période en cours

G&D
G&D a contribué aux activités de normalisation suivantes:

- Normalisation du passeport electronique (ISO/IEC JTC 1 SC17 WG3 and DIN NIA 17-03)
- Environnement d'exécution sécurisé, définition de l'interface utilisateur de confiance et Profil de protection selon des critères communs (commission GlobalPlatform), fonctions de gestion d'administration, des API de fonctions internes supplémentaires, API des éléments sécurisés et du canal sécurisé.
- Primitives cryptographiques supplémentaires pour les protocoles cryptographiques efficaces utilisés dans les passeports électroniques (Forum Java Card)

- Concepts de certification pour les applets JavaCard (GlobalPlatform GT sécurité de la carte)
- Amélioration des certifications des critères communs composites (ISCI)
- Discussion sur les nouveaux chemins d'attaque et de leurs évaluations selon les critères communs (JIL / ARP)
- Communication sans contact avec les puces RFID (ISO/IEC JTC1 SC17 WG8)
- API additionnelles sur les courbes elliptiques pour la carte JAVA CARD classique0

NXP-G
Pas d'activité sur la période en cours

IFAT
IFAT a participé à la 42ème édition de la réunion de ISO/IEC JTC1/SC17/WG8/TF2 à Kochel en Allemagne, du 28 au 30 janvier 2014 ainsi qu'à la 43ème édition de la réunion de l'ISO/IEC JTC1/SC17/WG8/TF2 à Neuchâtel en Suisse du 8 au 9 avril 2014.
IFAT a également participé à la 44ème édition des réunions ISO/IEC JTC1/SC17/WG8 et ISO/IEC JTC1/SC17/WG8/TF2du 22 au 26 septembre 2014 à Salamanque en Espagne ainsi qu'à à la 45ème édition des réunions ISO/IEC JTC1/SC17/WG8 et ISO/IEC JTC1/SC17/WG8/TF2 à Hiroshima au Japon du 23 au 26 février 2015.

IT
En tant que pilote du SP8, IT collecte les informations auprès des partenaires concernant leur participation à des activités de normalisation et constitue la liste de comités de normalisation où chaque partenaire contribue.
IT ne participe à aucune activité de normalisation en rapport au projet Newp@ss.

6.8.3. Coopération

- **Interne au SP8**
  - continu entre T8.1 et T8.2, où la diffusion et l'exploitation suivent de près la normalisation, et ont également contribué à ses activités connexes.
  - nécessaire pour avoir une coopération étroite entre T8.3 et T8.2 de manière à se conformer pleinement aux normes internationale, où l'implication des partenaires dans les activités pertinentes peut avoir un impact significatif
- **Avec les autres SP**
  - Essentiellement avec la plupart des autres SP (SP3, SP4, SP5, SP6, SP7), pour la diffusion des résultats, de l'exploitation et de la normalisation des objectifs obtenus, et aussi concernant les démonstrateurs et l'événement final T8.3
- **Entre les partenaires du consortium**
  - **Participation conjointe à des conférences internationales, expositions et événements.**
  - Publication de travaux communs du champ d'application du projet newp@ss mettant en avant les principales réalisations via des conférences ou des revues spécialisées
  - Promotion conjointe des aspects clés dans les organismes de normalisation appropriées

6.8.4. Résultats obtenus

Livrables:

Livrable	Tâche	Date planifiée (CR#2)	Date de livraison	Type et contenu
D8.1	T8.1 + T8.2	T2 13	T2 13 fait	Rapport de diffusion et de normalisation
D8.2	T8.1 + T8.2	T2 14	T2 14 fait	Rapport de diffusion et de normalisation
D8.3	T8.1 + T8.2	T2 15	T2 15 fait	Rapport de diffusion et de normalisation
D8.4	T8.1 + T8.3	T2 15	T3 15	Atelier avec les responsables et organismes gouvernementaux et de l'UE

- **Livrable "D8.1 – rapport de diffusion et de normalisation", document abouti, incluant la première année complète d'activité**
  - Contient les actions de diffusion réalisées par partenaires
  - Contient la compilation des participations des partenaires au sein des comités de normalisation sous forme de 2 listes (national et international)
- **Livrable "D8.2 – rapport de diffusion et de normalisation", document abouti, incluant les activités jusqu'au 1er semestre 2014**
  - Contient les actions de diffusion réalisées par partenaire
  - Contient la mise à jour des participations des partenaires au sein des comités de normalisation
  -
- **Livrable "D8.3 – rapport de diffusion et de normalisation", document abouti, incluant les activités jusqu'au 1er semestre 2015**
  - Contient la liste des actions de diffusion et de normalisation de tous les partenaires.
  - Contient la mise à jour des participations des partenaires au sein des comités de normalisation

Réalisations clés:

- **T8.1 plan de diffusion et d'exploitation**
  - **Site web Newp@ss (http://newpass.av.it.pt/)**
    - Mises à jour fréquentes dans la zone publique, notamment dans la page des événements où la participation et l'organisation d'événements sont annoncées
    - Page publique, permettant l'accès aux documents publics générés dans le cadre du projet, y compris les publications, les résultats attendus et les contributions de normalisation
    - **Zone publique**
      - ✓ **Identification du projet, coordonnées des contacts clés**
      - ✓ **Accueil avec un aperçu général du projet**
      - ✓ **Description** des objectifs généraux et de la pertinence stratégique du projet
      - ✓ **Partenaires** avec une carte de l'Europe contenant tous logos et les lieux d'implantation
      - ✓ **Autorités,** liste des autorités nationaux concernées, leur logo et leur adresse internet
      - ✓ Événements, où la participation et l'organisation d'événements sont annoncées
      - ✓ **Public**, permettant l'accès aux documents publics générés dans le cadre du projet, y compris les publications, les résultats attendus et les contributions de normalisation

- **Zone privée**
  - ✓ accès au dépôt de fichier en partage / serveur de référentiel, et les archives des listes d'adresse de courrier électronique
  - ✓

- **T8.2 Effort de normalisation**
  - l'implication des partenaires dans les comités de normalisation a été compilée dans le livrable D8.1 sous forme de deux tableaux, national et international
    - ✓ CEA-Leti, Gemalto, G&D, IFAT, NXP-F, NXP-G and ST sont activement impliqués
    - ✓ Evoleo, ISEN, IT, NXP-A, Id3 et TUGraz/IAIK ne participent aucune activité de normalisation en rapport au projet

  - **Comités internationaux**
    - ✓ ISO JTC1 SC17, SC27, and ISO/IEC 7816
    - ✓ ICAO NTWG and ICBWG
    - ✓ GlobalPlatform groupe de travail gouvernemental, carte et comité sur les dispositifs
    - ✓ Commission européenne DG Home art6
    - ✓ CEN/TC 224
    - ✓ ETSI SCP
    - ✓ NFC Forum; Java Card Forum
    - ✓ ISCI and JHAS

  - **Comités nationaux**
    - ✓ Agence française de normalisation AFNOR CN17 et CN37, ainsi que (ACN, ACSIEL et COFIS/CICS)
    - ✓ Austrian Standards Institute K001.AG6, AG17 and AG31
    - ✓ German DIN NA 043-01-17

  - Participation continue aux activités de normalisation
  - CEA-Leti participe au processus de normalisation de la technologie VHBR (ISO / IEC 14443), au niveau national et international, à savoir dans l'AFNOR et ISO
  - Gemalto a contribué aux normes de l'OACI sur la structure de données logiques LDS2, approuvées par l'organisme français de normalisation AFNOR et les autorités françaises (diapositives D8.1)
    - ✓ Contribution a également présenté au comité de normalisation ISO GT3 et au comité européen DG Home art6
    - ✓ Contribution réalisée avec la participation du laboratoire Keolabs
  - **G&D** contribue à ISO/IEC JTC1 SC17 WG3 et au DIN NIA 17-03
    - ✓ Également au comité GlobalPlatform, relative aux dispositifs, ainsi qu'au CEN TC 224 WG 16

  - **IFAT** participe à l'ISO/IEC JTC1/SC17/WG8 14443 pour la technologie VHBR
  - **IFX** participe à OACI NTWG, en charge de la LDS2

  - **NXP-F** porte une attention particulière aux certifications des éléments sécurisés, relatif à la GlobalPlatform ainsi qu'au forum NFC et ETSISCP

  - **NXP-G** participe à ISO/IEC JTC1/SC17/WG8 and 15408
    - ✓ Egalement à l'association GlobalPlatform et à OACI NTWG TF5 et LDS2

- **ST** participe à ISO/IEC JTC1 (VHBR), à ISO/IEC 15408, au sein du comité « appareil » de GlobalPlatform à ETSI SCP et à CAN

- La participation aux activités de normalisation assure que les développements du projet sont basés sur les normes internationales pertinentes

- Les résultats du projet sont promus dans les organismes de normalisation compétents, contribuent au processus de normalisation, à savoir dans les décisions techniques

- La liste compilée des participations aux organismes de normalisation des partenaires sera utilisée pour évaluer la meilleure façon pour le projet d'avoir le plus d'impact dans la normalisation, et de trouver des moyens pour les partenaires à coopérer à son égard

NewP@ss - International Standardization Committees Coverage	
Standardization Committee	**Partners**
ISO JTC1 SC17/WG3/ MRTD e-Passport Plenary TF1 NTWG- TF2 co edition TF3 communication TF4 Tests TF5 PKI, PKD, LDS2	Gemalto G&D
ISO JTC1 SC17/WG4 chip cards Generic std	Gemalto G&D
ISO JTC1 SC17/WG8/TF2 and TF3 Contactless cards	Gemalto ST IFAT NXP-G (focus PSK) CEA-Leti
ISO JTC1 SC27 Plenary Security WG1 Information Security Mgt. Sys. WG2 Cryptography & Security WG3 Security Evaluation (15408)	Gemalto ST NXP-G
ISO/IEC 7816 Display protocols	Gemalto G&D
ISO/IEC (various committees) Display-on-card	Gemalto NXP-G
ICAO NTWG LDS2 sub-group	Gemalto NXP-G IFX G&D
ICAO ICBWG	Gemalto

NewP@ss - International Standardization Committees Coverage	
Standardization Committee	**Partners**
Global Platform Device Committee Card Com Government Task Force For MRTD usage	Gemalto ST NXP-G G&D
European Commission DG Home art6 ISPRA Visa, Passport, Residence Permit, SPOC/PKI infrastructure	Gemalto
CEN/TC 224 Plenary	Gemalto
CEN/TC 224 WG15 with SW partners intent to promote projects results for finalizing all SCC parts	Gemalto
CEN/TC 224 WG16 with SW partners intent to promote projects results for enhancing eSignK and secure protocols	Gemalto G&D
CEN/TC 224 WG17 EU protection Profile	Gemalto
CEN/TC 224 WG18 EU Biometrics	Gemalto
ETSI SCP SWP/HCI (REQ, TEC, TEST)	ST NXP-F
ETSI SCP eUICC (REQ, TEST)	ST NXP-F
NFC Forum NCI	NXP-F ST
NFC Forum Devices Working Group	IFX ST
NFC Forum EMVCo alignment meetings	IFX ST

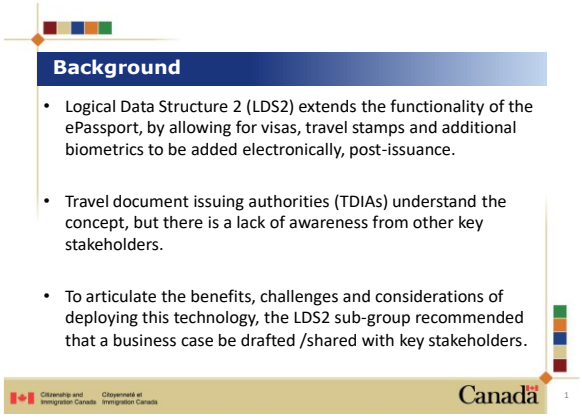
NewP@ss - National Standardization Committees	
French AFNOR committees	**Partners**
AFNOR CN17 COS Strategic orientation committee	Gemalto
AFNOR CN17 ge3 MRTD, Residence Permit, Visa	Gemalto
AFNOR CN17 ge4 Generic Standard 7816.x	Gemalto
AFNOR CN17 ge8 Contactless cards	Gemalto CEA-Leti
AFNOR CN17 cde ECC standards	Gemalto
AFNOR CN37 Biometrics	Gemalto
Alliance pour la Confiance Numerique (ACN)	ST
Austrian Standards Institute	
K001.AG6 Mirror Committee to JTC1/SC6	IFAT
K001.AG17 Mirror Committee to JTC1/SC17	IFAT
K001.AG31 Mirror Committee to JTC1/SC31	IFAT
German committees	
DIN NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA) -NA 043-01-17-08 UA Unterausschuss Kontaktlose Chip-Karten	IFX
DIN NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA) -NA 043-01-17 AA Arbeitsausschuss Karten und pers˙nliche Identifikation	IFX
DIN NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA) -NA 043-01-17-03 UA Maschinenlesbare Reisedokumente	G&D

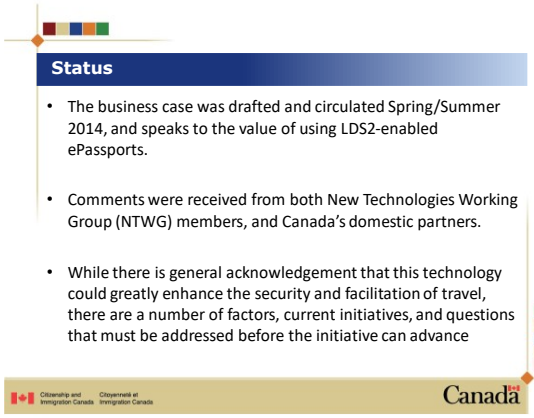
- **T8.3 Réunion final de présentation des démonstrateurs**

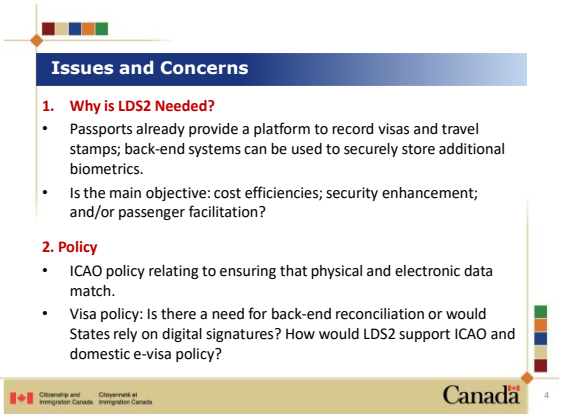
  - L'aéroport de Saragosse s'étant retiré du consortium, a impliqué la nécessité de trouver un aéroport alternatif pour les démonstrateurs finaux
    - ✓ l'aéroport de Toulon Hyères a été abordé comme solution de remplacement pour les démonstrateurs finaux du projet et a accepté de remplacer l'aéroport de Saragosse
  - ISEN-Toulon a mené une enquête sur le terrain à l'aéroport de Toulon Hyères et a produis un questionnaire en ligne
    - ✓ Etude qualitative sur les fonctionnalités et services envisagés dans les aéroports modernes, permettant d'être promus par chaque membre du consortium
  - réunion sur place avec les partenaires les plus impliqués dans les démonstrateurs
    - ✓ Atelier spécifique SP7 le 29 et 30 janvier 2014
    - ✓ Découverte des sites opérationnels et atelier de co-conception avec le personnel de l'aéroport pour spéculer sur les cas d'utilisation les plus avancés.
  - En lien direct avec les activités du SP7.
  - Evénement pour présenter les résultats du projet aux parties prenantes externes, par exemple, FRONTEX, fonctionnaires de l'UE, etc.
  - Prise en compte d'un calendrier favorable pour planifier cet événement final, pour attirer davantage d'intérêt si possible ; contribuer à augmenter l'effet de la diffusion de cette initiative.
  - Gemalto avait menées déjà quelques actions envers les fonctionnaires et les agences de l'UE
  - Possibilité d'organiser un atelier d'une demi-journée avec des projets connexes en cours (projet Eureka ou FP7), éventuellement avec des représentants du cluster EUREKA et l'UE
    - FastPass, ABC4EU, Fidelity, Idea4SWift, Origins…

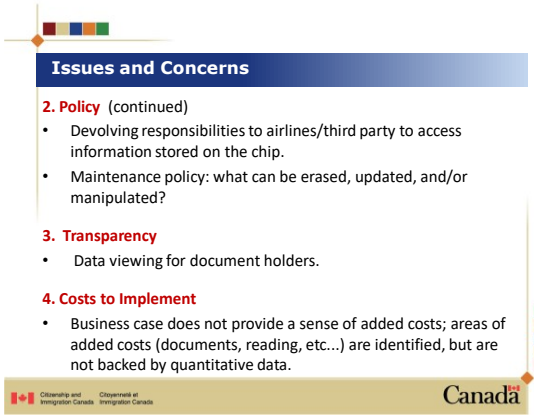
Durant le premier semestre 2015, Gemalto a contribué à diverses réunions dans la portée de newp@ss, à savoir concernant la sécurité des documents et normes MRTD.
Notamment, Gemalto a participé activement à 2 réunions avec le sous-groupe gouvernemental de l'OACI dédié à orientation de la norme sur la LDS2. La première réunion s'est tenue à Kuala Lumpur en Novembre 2014 et la seconde à Bruxelles en Juin 2015.

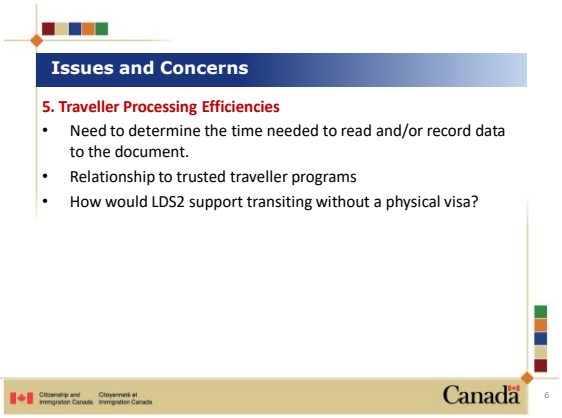
Ces réunions ont été l'occasion de mettre à jour le plan de déploiement de LDS2 et les cas d'utilisation associés. La révision intégrale a été validée lors de la réunion de l'OACI GTR tenue en novembre dans le même lieu. Les principales décisions sont résumées ici après, illustrées dans les diapositives présentées ci-après.

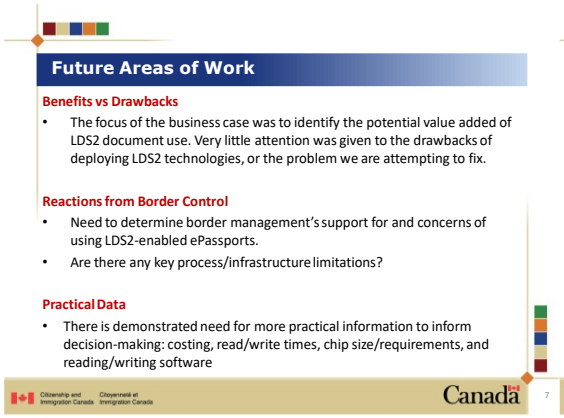


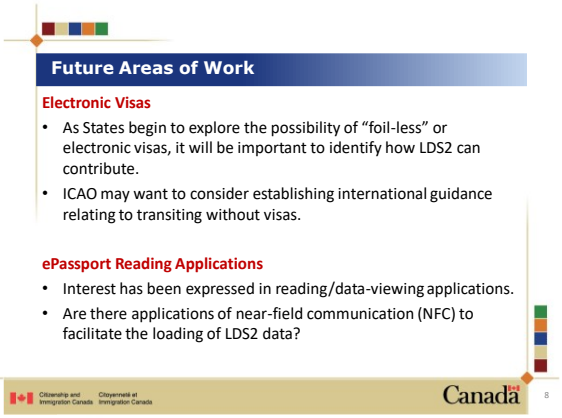








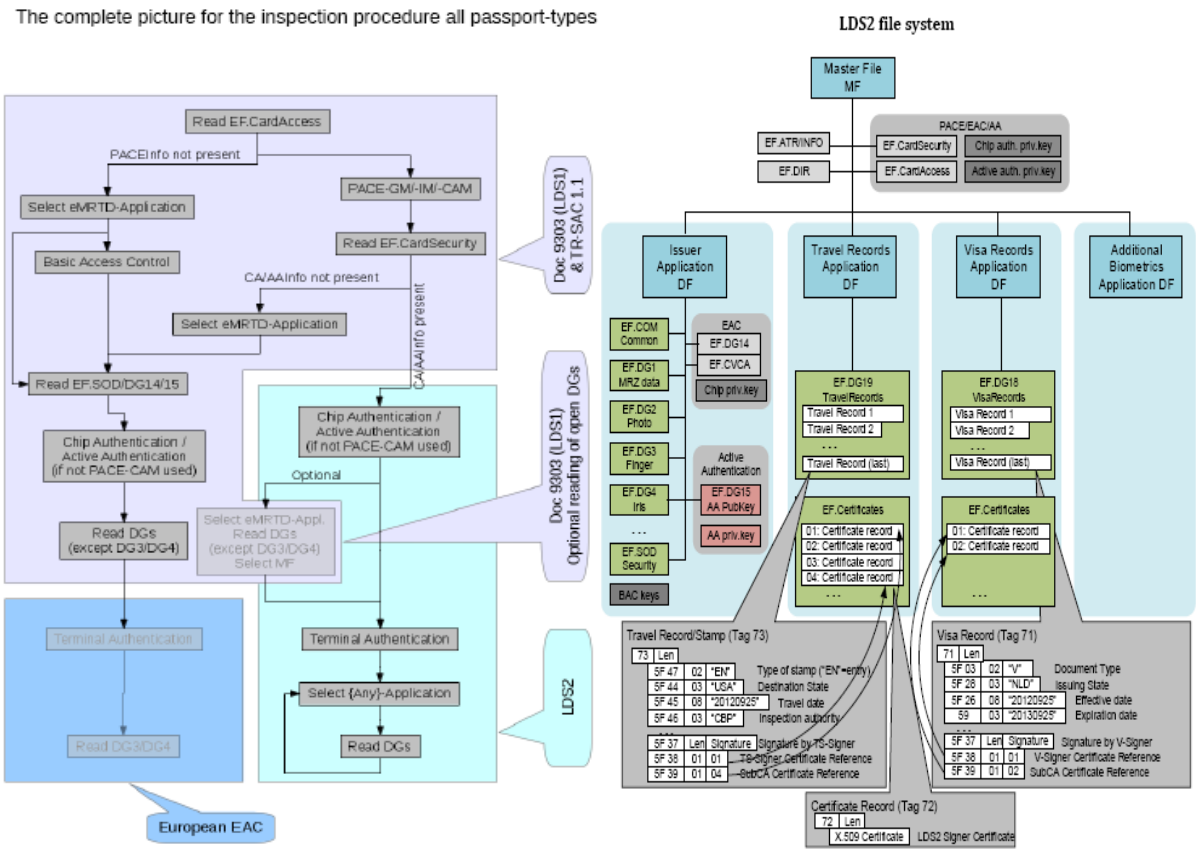




En outre, le comité de normalisation ISO SC17 GT3 s'est réuni à Salamanque en Octobre 2014. Au sein du groupe de travail TF5, les spécifications préliminaires de la LSD2 ont été mises à jour. Les exigences sont réparties en trois parties

- La structure de données :
  - 9303 Part10 LDS - § LDS_2.0 data structure
- Les protocoles d'accès sécurisés et la procédure du système d'inspection:
  - 9303 Part11 LDS - § LDS_2.0 procédure d'inspection
- L'infrastructure à clé publique:
  - 9303 Part12 LDS - § LDS_2.0PKI Version préliminaire 2.0

Le contenu de ces trois documents est résumé dans les présentations ci après. Les projets préliminaires sont disponibles dans le dépôt de fichier newp@ss, pour usage interne uniquement, dans le cadre du projet.
Une nouvelle mise à jour de la procédure d'inspection LDS2 a eu lieu en mai 2015 l'Autorité BSI allemand étant rédacteur en chef de cette sous-partie.



Toutes les activités de normalisation pertinentes dans lesquelles les partenaires de newp@ss ont participé à la période de déclaration se référant sont répertoriées comme suit:

2014-08-26, Gemalto, (international) réunion OACI **à** Montréal
L'objectif était de proposer des évolutions futures possibles des technologies aux représentants du gouvernement. Gemalto a été choisi pour montrer 3 nouvelles technologies.

2014-09-03, Gemalto, (national) Comité stratégique normes AFNOR
Statu sur les normes internationales et européennes en cours (art6, ICAO LDS2, ISO, PKD, …)

2014-09-10/11, G&D, (international) Groupe de travail GlobalPlatform TEE Spec, Sophia-Antipolis

- API préliminaire pour les traitements biométriques des empreintes
- Architecture préliminaire relative à l'exécution en environnement sécurisé
- API 1.1 pour des éléments sécurisés lors de l'exécution en environnement sécurisé
- Commentaire sur l'API relative au traitement d'une connexion en environnement sécurisé.

2014-09-16, Gemalto, (national) **AFNOR Standard CN17 ge3-ge10** réunion plénière – documents de voyage et permis de séjour.
Statut sur les réunions international et européenne (art6, ICAO LDS2, ISO, PKD, …) – Convergence de normes pour le passeport electronique–

2014-09-29/10-01, Gemalto, (international) **ISO SC17 WG3 réunion plénière et groupe de travail à**

Salamanque

WG3 et ses cinq (5) groupes de travail ont fourni une assistance technique à l'OACI dans de nombreux domaines au cours de la dernière année pour NTWG, ICBWG, LDS2 et PKD.

- TF1 Révision de la structure de données logiques (LDS), meilleures pratiques dans la gestion d'identité nationale, Maintenance du Document 9303, Normes pour urgence / passeports temporaires, étude sur l'utilisation des codes à barres
- TF2 rédaction de nouvelles éditions de l'OACI Doc 9303 ED7 - nouvelle version pour publication TF2
- TF3 Problématique d'application, Renforcement des capacités de vérification des identités et de la sécurité aux frontières
- TF4 Essais de durabilité 18745-1, tests d'interface RF 18745-2, tests d'application 18754-3
- TF5 LDS / Maintenance de la PKI, révision de la structure de données logique (LDS), liste des déviations, cartographie authentifiés et étude de LDS2

2014-10-01/03, Gemalto, (international) **ISO SC17 réunion plénière à Salamanque**
Examen de tous les groupes de travail de l'ISO GT1 à GT11 dans le contexte des cartes et des systèmes d'intégration de solutions, y compris passeport et cartes.

2014-10-30, Gemalto, (national) **ANTS/AFNOR** Atelier programme TRIP
Examen sur les travaux en cours sur passeport électronique et validation des commentaires. Mise à jour de la LDS2 suite à la réunion de Salamanque.

2014-10-10, Gemalto, (international) **ICAO NTWG LDS2**, Kuala Lumpur
Réunion gouvernementale consacrée à l'état des travaux et aux étapes suivantes sur les aspects stratégiques. La participation des agents des services frontaliers sont nécessaires pour les prochaines étapes.

2014-11-3/6, G&D, (international) **comité GlobalPlatform, TEE Spec WG** and **Admin Fwk Sub Group**

- API pour les traitements biométrique des empreintes digitales
- API des éléments sécurisés
- Admin Fwk.

2014-11-11/13, Gemalto, (international) OACI **NTWG**, Kuala Lumpur
Nouveaux détails du programme TRIP pour membres. Mise à jour sur la reconnaissance faciale, mise à jour des visas européens des permis de séjour.
Examen des thèmes de la réunion ISO SC17 GT3 sur l'ensemble des TM. Mise à jour au sein du groupe de travail 8 sur le sans contact.

2014-11-21, Gemalto, (national) **ANTS**: Atelier de travail sur le programme TRIP
Usage d'applications/ preuve de concept sur mobile avec des passeports électronique. (Orientation française).

2014-12-1/5, Gemalto, (international) **ICAO ICBWG**, Brasilia
Nouveaux détails sur les exigences du programme TRIP
Examen de stratégie de OACI pour 2013-2016 /mise à jour du business plan.
Feuille de route du passeport electronique, schéma de conformité des MRTD.
Examen du guide pour l'évaluation de la sécurité, la gestion et la délivrance des documents de voyage et des conseils fournis aux états.
Sous-groupe sur la convention des documents voyage.
Evolution du passeport électronique déploiement mondial et faiblesses/ Date limite d'examen.

Aide aux programme Brésilien / document brésilien / réunion de l'industrie.

- **2014-12-15**, Gemalto **AFNOR Standard CN17 ge3-ge10** Réunion plénière - document de voyage et permis de séjour

Statut sur les réunions international et européenne (art6, ICAO LDS2, ISO, PKD, …)

2014-12-16, Gemalto, (national) **ANTS/art6** Atelier.

2015-01-13/15, G&D, (international) Groupe de travail GlobalPlatform TEE Spec, Londres

- API pour les traitements biométrique des empreintes digitales
- Admin Fwk.

- 2015-01-19/21, Gemalto, (international) réunion ISO SC17 WG3 TF5 adhoc LDS2, Berlin
  Réunion ISO LDS2 dédiée à l'examen des commentaires d'experts sur la partie 3 du sous projet de norme (par exemple les mécanismes d'accès, de protocoles sécurisés et la PKI). Discussion portant sur la simplification des mécanismes d'authentification et de réduire le nombre de configuration et les options. Proposition de suppression du protocole RSA. Une discussion lancée sur les prochaines étapes et un possible démonstrateur / pilote a été approuvé par le groupe.

2015-01-21, G&D, (international) Groupe de travail **JHAS,** Bruxelles
Scénarios d'attaque pour les cartes à puce

- mise à jour du taux de perturbation d'attaque cryptographique sur 3DES
- Problématique des sécurités des mobiles (élément sécurisé + contrôleur NFC)
- Changements logiciel-matériel.

2015-02-12, G&D, (international) sous-groupe ISCI MSSR, Bruxelles

- Critères communs de certification de sécurité.

2015-03-4/5, G&D, (international) Groupe de travail **GlobalPlatform TEE,** La Ciotat

- Configurations
- E&P Groupe de conformité des entrées
- API des éléments sécurisés
- API des connexions

2015-03-19, G&D, (international) Groupe de travail **JHAS,** Bruxelles

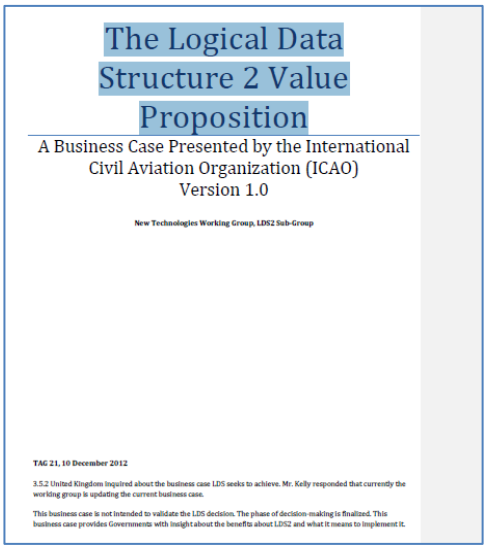
- présentation Eurosmart concernant le coût des réunions JHAS
- Attaque partielle (Perturbation Triple DES plus DES cracker)
- Réutilisation des IP (présentation de Broadcom)
- Sous groupe des éléments sécurisés et du contrôleur NFC et de sécurité des mobiles
- Sous groupe des attaques de patron.
- Sous groupe des échantillons découvert.

2015-04-01, Gemalto, (national) **AFNOR Standard CN17 ge3-ge10** Réunion plénière - document de voyage et permis de séjour
Statut sur les réunions international et européenne (art6, ICAO LDS2, ISO, PKD, …) – Convergence de normes pour le passeport electronique.

2015-04-27/ 30, Gemalto, (international) **Leiden NL: ISO SC17 WG3 réunion plénière et groupe de travails**

WG3 et ses cinq (5) groupes de travail ont fourni une assistance technique à l'OACI dans de nombreux domaines au cours de la dernière année pour NTWG, ICBWG, LDS2 et PKD.

- TF1 Révision de la structure de données logiques (LDS), meilleures pratiques dans la gestion d'identité nationale, Maintenance du Document 9303, Normes pour urgence / passeports temporaires, étude sur l'utilisation des codes à barres
- TF2 rédaction de nouvelles éditions de l'OACI Doc 9303 ED7 - nouvelle version pour publication en Juin
- TF3 Problématique d'application, Renforcement des capacités de vérification des identités et de la sécurité aux frontières
- TF4 Essais de durabilité 18745-1, tests d'interface RF 18745-2, tests d'application 18754-3 et Profil d'application préparés par le groupe de travail "sans contact" GT8
- - TF5 LDS / Maintenance PKI, Révision de la structure de données logiques (LDS), finalisation de la "La structure de données logiques LDS2. Proposition v1" de la LDS2 a été publiée
(Page de couverture ci dessous):



The Logical Data Structure 2 Value Proposition

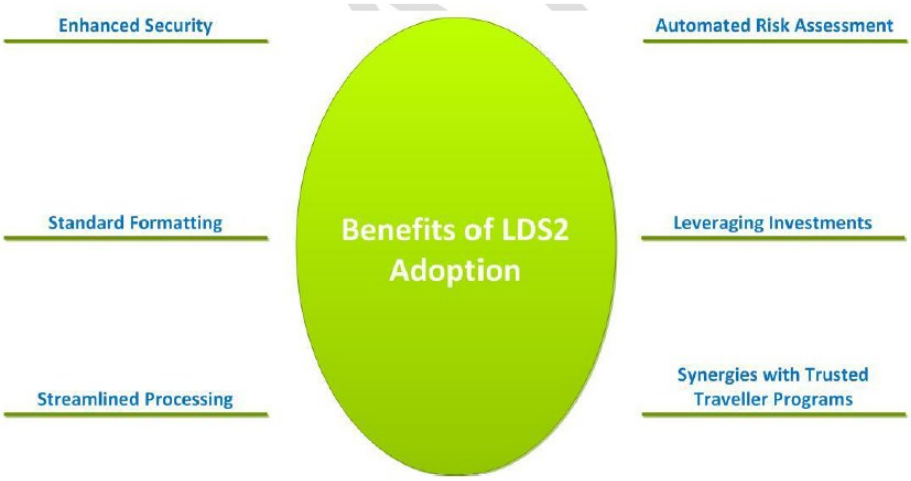
A Business Case Presented by the International Civil Aviation Organization (ICAO)
Version 1.0

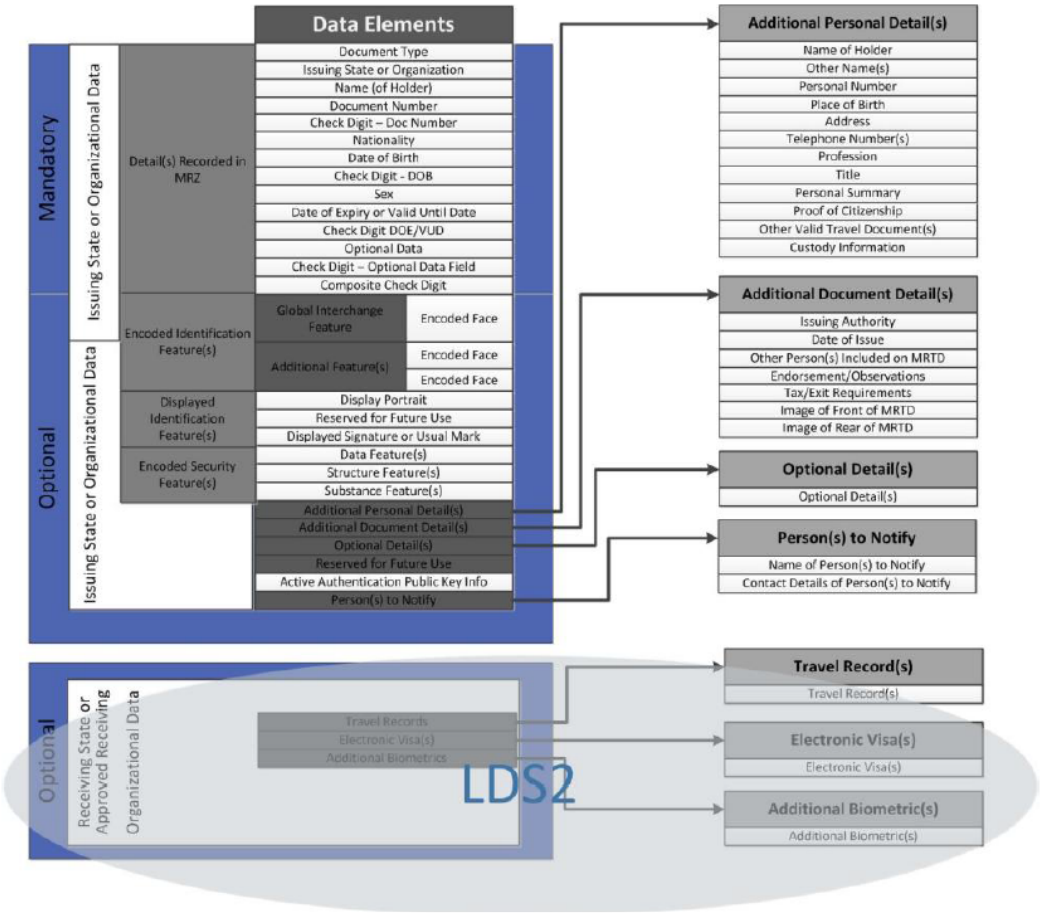
New Technologies Working Group, LDS2 Sub-Group

TAG 21, 10 December 2012

3.5.2 United Kingdom inquired about the business case LDS seeks to achieve. Mr. Kelly responded that currently the working group is updating the current business case.

This business case is not intended to validate the LDS decision. The phase of decision-making is finalized. This business case provides Governments with insight about the benefits about LDS2 and what it means to implement it.





- 04.05.2015 / 8, Gemalto, (internationale) de l'OACI ICBWG, Australie (aucune présence physique) Gemalto adressée une contribution non officiel au groupe de travail sur un guide pour l'évaluation de la sécurité et la gestion et la délivrance des documents de voyage pour les Etats

- 2015-05-26, *Gemalto, (national)* ***AFNOR Standard CN17 ge3-ge10*** **Réunion plénière** – *documents de voyage & permis de séjour : statut sur les réunions international et européenne (art6, ICAO LDS2, ISO, PKD, …)*

- 02/06/2015, Gemalto, (internationale) de l'OACI GTR LDS2, Bruxelles. Réunion gouvernementale consacré à l'examen de l'état des travaux en cours et les prochaines étapes sur la partie stratégique. Révision complète du mécanisme d'accès. Examen des stratégies de déploiement par les états membres. Proposition de lignes directrices pour un démonstrateur / pilotes. Rédaction d'un papier blanc sur les démarches à destination du conseil approbation du GT.

- 2015-06-3/5, Gemalto, (international) **ICAO NTWG board**, Bruxelles

Suivi discussions sur les technologies des MRTD et de la LDS2

Diffusion

- Gemalto a participé au Forum européen de nanoélectronique en 2012, et a monté un poster de présentation de newp@ss à Munich du 20 au 22 novembre en Allemagne.

- *Présentation du projet Newp@ss par Gemalto à l'agence nationale des titres sécurisés, tutelle du ministère de l'intérieur à Paris le 11 février 2013.*

- NXP-G (Mario Stolz), "Newp@ss - œuvrer vers l'évolution passeport électronique du futur" au World Document Security (SDW) 2013, 21-22 mai à Londres, Royaume-Uni

- *Présentation du projet newp@ss par* Gemalto au congrès mondial de l'eID et au forum «**Chip to Cloud Security » du 25 au 27 s**eptembre 2013 à Nice en France

- TUG-IAIK / NXP-Un document accepté à la 5ème conférence sur "Advances in System Testing and Validation Lifecycle" (VALID 2013) du 27 octobre au 1er novembre à Venise en Italie

- R. Bloem, R. Koenighofer, F. Roeck, K. Greimel, "*Model-Based MCDC Testing of Complex Decisions for the Java Card Applet Firewall*"

- • NXP- Document accepté à la 39e conférence annuelle de l'IEEE Industrial Electronics Society (de IECON 2013), 10 au 13 novembre, à Vienne, en Autriche.
- K. Greimel, N. Seßler, T. Klotz, "*Model Checking Specifications of Smart Cards*"

- TU Graz-IAIK, présentation d'un article de conférence : "Case Study: Automatic Test Case Generation for a Secure Cache Implementation", 9e Conférence internationale sur Tests & Preuves (TAP 2015), Juillet 22-24 L'Aquila, en Italie
- Gemalto, présentation d'un démonstrateur : "NewP@ss Border control demo", ISEN Toulon, du 20 mai au 4 juin 2015, à Toulon, France.

- IT and Evoleo, présentation d'un démonstrateur sur un stand d'exposition: "NewP@ss 4G demo PKI Travel records demo", atelier sur « *Redes de Veículos nas Sociedades do Futuro* », le 3 juin à Castelo Branco au Portugal.

- Gemalto, présentation: "NewP@ss project and technology", ISEN Toulon, le 20 mai à Toulon, France.

- ISEN, formation dédiée des étudiants : "projet étudiant sur un logiciel en open source de lecture de document MRTD ", ISEN Toulon, du 1er octobre 2014 au 15 mai 2015 à Toulon, France.

- id3 présentation sur un stand d'exposition: "NewP@ss et id3 VHBR", salon Cards & Payments Middle East 2015, du 12 au 13 mai à Dubaï aux Emirats Arabes unis.

- id3 présentation sur un stand d'exposition: "NewP@ss et lecteur id3 VHBR", salon Cards Payment & Identification 2015, du 14 au 16 avril à São Paulo au Brésil.

- IFAT, présentation: "Trends in der Forschung für kontaktlose Anwendungen", 8. Dresdner RFID-Symposium (2014), du 4 au 5 décembre à Dresde en Allemagne.

- Infineon, présentation: "Border Control, new standards (e.g. LDS2.0) and new technologies (e.g. VHBR)", 3ème Conférence sur la coopération technique et le renforcement des capacités de gestion des frontières – Systèmes d'information de gestion frontalière du 2 au 4 Décembre 2014 à Bangkok en Thaïlande.

- Gemalto, poster and présentation sur un stand d'exposition: "NewP@ss progress", Forum européen de la nanoélectronique 2014, du 26 au 27 novembre à Cannes, France

- IT, présentation d'un article de conférence:: "Towards an Advanced PKI-based Security Solution for Next Generation e-Passport and Associated Applications: The NewP@ss Approach", 8e Conférence internationale de l'Internet sans fil - Symposium sur Wireless and Vehicular Communication (WICON 2014), 13-14 novembre à Lisbonne, Portugal.

- TU Graz-IAIK, conférence: "Designing Secure Smart Cards", 13e conference sur les applications avancées et la recherche sur les carte à puce, du 5 au 7 Novembre à Paris, France.

- id3, présentation sur un stand exposition : "NewP@ss activities", Cartes 2014, du 4 au 6 Novembre à Paris, France
- CEA-Leti, présentation sur un stand exposition : "NewP@ss - Next générations of e-passeport", Cartes 2014, du 4 au 6 Novembre à Paris, France.

- NXP-A, présentation: "Formal Verification of UML Statechart Diagrams with COSIDE®", SystemC AMS – réunion COSIDE du groupe d'utilisateur le 16 octobre 16, à Munich en Allemagne.

- TU Graz-IAIK, présentation d'un article de conférence : "Adding Controllable Linkability to Pairing-Based Group Signatures For Free", Conférence international sur la sécurité de l'information (ISC 2014), du 12 au 14 Octobre, à Hong Kong

- TU Graz-IAIK, conférence: "Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster", 18e Atelier sur la cryptographie à courbe elliptique (ECC 2014), du 8 au 10 Octobre, à Chennai, en Inde

- TU Graz-IAIK, présentation d'un article de conférence : "Automating Test-Suite Augmentation", 14e Conférence internationale sur la qualité des logiciels (QSIC 2014), du 2 au 3 Octobre, à Allen à Dallas, Texas, aux états Unis

- TU Graz-IAIK, présentation d'un article de conférence : "Efficient Pairings and ECC for Embedded Systems", 16e Atelier international sur le matériel cryptographique et Systèmes Embarqués (CHES 2014), Septembre 23-26 Busan, en Corée

- Gemalto, présentation: "NewP@ss progress", congrès mondial World e-ID 2014, du 22 au 25 septembre à Marseille, France

- G&D, présentation: "Trusted Government", congrès mondial World e-ID 2014, du 22 au 25 septembre à Marseille, France

- TU Graz-IAIK, présentation d'un article de conférence: "Practical Attack on Bilinear Pairings to Disclose the Secrets of Embedded Devices", Conférence internationale sur la disponibilité, la fiabilité et la sécurité (ARES 2014), du 8 au 12 septembre à Fribourg, Suisse

- TU Graz-IAIK présentation d'un article de conférence: "Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster", Atelier international sur les zones sélectionnées en cryptographie (SAC 2014), du 14 au 15 Août à Montréal, Québec, Canada

- TU Graz-IAIK, conférence: "Implementation Security", IPICS 2014 - Programme intensif sur Information & Communication de sécurité, du 7 au 18 Juillet sur l'île de Lesbos en, Grèce

- Gemalto, poster and présentation sur un stand d'exposition: "NewP@ss progress", Forum européen de la nanoélectronique 2015, du 30 novembre et 1er Décembre à Berlin, Allemagne

- The consortium has won the "most innovative catrene project award" during the European Nanoelectronics Awards in Berlin December 1st

- **Action de diffusion – <u>46</u> <u>au total</u> (<u>*8 durant 2015*</u>)**
  - Présentations et conférence : 22
  - Article de conférence présenté : 13
  - Poster et stand d'exposition : 6
  - Démonstrateur : 4
  - Formation dédiée : 1
  - Revues 1 (en cours de soumission)
  - brevets 2 (en cours de soumission)
    - 2 sur récepteur analogique numérique VHBR (CEA-Leti)

7. Soutien des autorités nationales

Le projet a été soutenu par les autorités nationales de l'Autriche, de la France, de l'Allemagne et du Portugal et de la Hongrie. Le soutien du public est nécessaire pour la réussite du projet pour les principales raisons suivantes:

Risque scientifique et technique: Les risques techniques et scientifiques sont minimisés par la convergence des intérêts des gouvernements partout dans plusieurs pays européens pour le type de plate-forme que ce projet vise (également soutenu par les politiques générales de l'UE). Les études préliminaires qui ont été effectuées dans l'ex-projet BIOP@ss ont créé toutes les technologies de base pour assurer que les partenaires puissent atteindre leurs objectifs dans newp@ss en bénéficiant de la dynamique créée et le cadre de la coopération déjà créé entre un noyau solide de partenaires. Le soutien public permettra d'accélérer l'obtention de résultats, de minimiser les risques et les coûts liés de la R & D.

Impact attendu sur le secteur public et sur le contexte économique associé : La réalisation de la plate-forme ciblée dotée d'un noyau intégré interopérable de services e-administration soutenue par des composants dans l'art de l'art qui permettent une multi-utilisation efficace mettra à profit le déploiement dans l'e-déplacement et les services connexes. Les résultats du projet permettront d'accélérer la disponibilité d'une société de l'information européenne, bénéfique aux autorités publiques, aux citoyens, et une abondance des acteurs de la technologie d'approvisionnement du secteur public ou fortement relié à lui (aéroports, compagnies aériennes ou de voyage, prestations électroniques .. .). La preuve inhérente des concepts livrés seront encore susceptibles d'être exportés en dehors de l'Europe, comme l'a déjà démontré en particulier si l'approbation des résultats du projet par l'OACI, Chapitre 6 UE, CEN et canal ISO

Activité de normalisation prévue : Dans le secteur public, le projet va apporter des contributions à plusieurs initiatives de normalisation tels que ceux concernés par e-Voyage (OACI, UE Chapitre 6), et l'ISO classique ou CEN comités techniques (ISO / IEC SC17 WG4 7816- 11, la norme ISO / CEI 19794, [OACI], documents ISO SC17 GT3 de voyage, ISO SC17 GT10 permis de conduire, etc. ...), ou ceux qui traitent avec carte électronique de la citoyenneté (CEN / TC 224 WG15, parties 2, 3 et 4 et WG16 et WG17).

Coopération entre les partenaires européens: Un tel projet, porté seulement au niveau national, n'aurait pu satisfaire les exigences d'interopérabilité dans les segments cibles. À cette fin, une coopération technique avec des partenaires de différents pays européens a été nécessaire; sinon le projet aurait produit des résultats qui aurait été non-applicable au-delà d'un cadre limité / nationale.

8. Personnes à contacter

Prénom	Nom	Téléphone	E-mail	Adresse complète
Jean-Pierre	Tual	+33 155016160	jean-pierre.tual@gemalto.com	6 rue de la Verrerie F-92197 MEUDON Cedex
Michael	Guerassimo	+33 442364846	michael.guerassimo@gemalto.com	Avenue Pic de Bertagne 13881 Gemenos Cedex

9. Annexe

9.1. Glossaire

Acronymes et abréviations:

1G ePassport	Passeport électronique intégrant le protocole de sécurité BAC, et contient l'image du visage du titulaire
2G ePassport	Passeport électronique intégrant les protocoles BAC et EAC, et contient l'image faciale et les empreintes digitales du titulaire
3G ePassport	Passeport électronique mettant en œuvre les protocoles de sécurité SAC et EACv210, et contiennt l'image faciale et les empreintes digitales du titulaire
4G ePassport	Passeport électronique mettant en oeuvre (au moins) LDSv2, EACv210 complète et VHBR
AA	Authentification active
AES	standard de cryptage avancé
AHB	bus haute performance
ALU	Unité logique et arithmétique
BSI	Bureau fédéral allemand de la sécurité de l'information
ASK	Modulation d'amplitude
ARM	Advanced RISC Machine (machine avancé à jeu d'instruction réduit)
BAC	Contrôle d'accès basique
CA	Autorité de certification
CA	Authentification de composant (concept du protocole EAC)
CAN	Numéro d'accès à la carte
CCEAL	Critère commun EAL
CEN	Commission de normalisation européenne
Contact-less	Sans contact
CPU	Unité centrale de calcul
CSCA	Pays signat un CA
CVC	Code de validation de carte
CVCA	Pays vérifiant un CA
CWA	accord d'atelier CEN
DES	standard de cryptage de donnée (triple DES)
DF	Fchier de donnée
DGx	groupe de donnée (fichier x) défini par OACI contenant des données
DoS	Deéni de service
DSA	Standard de signature numérique
DV	Verification de document
DVCA	Autorité de certification de vérification de document
EAL	Niveau d'assurance d'évaluation (1 à 7)
EAC	Control d'accès étendu V1.11 (passeport de 2e génération ou permis de séjour)
ECC	Carte de citoyenneté européenne
ECC	Cryptographie à courbes elliptiques
ECS	Code de signature amélioré

EF	fichier élémentaire
EMD	Perturbation électromagnétique
FAR	Taux de fausse acceptation
FGPA	Réseau de porte programmable (circuit logique programmable)
FRR	Taux de fausse rejection
HTML	Langage signalétique hyper texte
HW	Matériel (composant ou carte électronique)
[IAS]	Identification, authentification, signature numérique
IC	Circuit intégré
[ICAO]	organisation de l'aviation civile internationale
ICC	Carte circuit intégré
IEC	Commission électronique internationale
IFD	Interface de dispositif
IOP	Interopérabilité
IS	Système d'inspection
ISS	Station spatiale internationale
ISO	Organisation internationale de normalisation
LDS	Structure de donnée logique
MAC	Contrôle d'accès au support
MCU	Microcontrôleur
mEAC	Contrôle d'accès étendu modulaire
MF	Fichier maître
MITM	Attaque de l'homme du milieu
MoC	Technologie de comparaison (empreinte ou autre) embarqué sur carte à puce
MoT	Technologie de comparaison (empreinte ou autre) embarqué sur terminal
MRTD	Document de voyage lisible à la machine
MRZ	Zone lue par la machine
NFC	Communication en champ proche
NIST	Institut national de norme et de technologie
NVM	Mémoire non volatile
OCR	Reconnaissance optique de caractère
OLED	Diode organique électroluminescente
OS	Système d'exploitation
OSCDP	Plate forme ouverte de développement sur carte à puce
PA	Authentification passive
PACE	Protocole d'authentification pour l'établissement de connexion
PCD	Dispositif de couplage de proximité (= lecteur sans contact)
PICC	Carte à puce sans contact (tel que les ePasseports)
PCB	Circuit imprimé
PASC	Connexion sécurisé par authentification de mode passe
PBM	Mécanisme basé sur des mots de passe
PCA	Accord de consortium
PCSC	PC / carte à puce

PKD	Répertoire à clé publique
PKI	Infrastructure à clé publique
PIA	Autorité d'assurance et de retraite
PMB	Conseil de gestion du projet
PTB	Conseil technique du projet
PP	Profile de protection
PSK	Modulation de phase
PSO	Réalisation d'opération de sécurité
RAM	Mémoire à accès aléatoire
RF	Fréquence radio
RFID	Radio identification
RSA	Algorithme de chiffrement asymétrique
RTL	Niveau de transfert registre
SE	Elément sécurisé
SAC	Control d'accès supplémentaire
SHA	Fonction de hachage cryptographique
SMD	Composant monté en surface
SPI	liaison série synchrone
SPM	Security Policy Model
SW	Logiciel
TA	Authentification du terminal
TEE	Environnement d'exécution sécurisé
TS	Système terminal
VHDR	Débit de donnée très élevé (>848 bits /s)
VHBR	Débit de binaire très élevé (>848 bits /s)