Les 14es Rencontres de l'ARCSI « L'épopée de la carte à puce et son avenir »

Gérard Peliks et Joël Hosatte

Le jeudi 20 octobre 2022, l'ARCSI tenait son colloque annuel - ses 14es Rencontres- dans un endroit prestigieux, un amphi de la BnF - Bibliothèque nationale de France - dans le 13e arrondissement de Paris.

Les messages de bienvenue et les hommages à nos illustres disparus

À 09 h 00 tout est prêt pour accueillir les participants. Après un petit-déjeuner café, jus de fruit, croissants, nous entrons dans l'amphi où Jean-Louis Desvignes, président de l'ARCSI, présente le sujet de la journée : « L'épopée de la carte à puce et son avenir ».

Ce sujet a été choisi et développé par le comité scientifique de l'ARCSI, en hommage à Michel Ugon, véritable inventeur de la carte à microprocesseur, décédé le 28 décembre 2021 dans l'oubli des médias, alors que des milliards de cartes à puces dans le monde sont basées sur ses travaux. L'ARCSI tenait à rendre hommage à cet illustre ingénieur que nous étions fiers de compter dans nos rangs.

Jean-Louis Desvignes donne la parole à Kevin Riffault, directeur général de la BnF, notre hôte qui nous souhaite la bienvenue.

Kevin Riffault nous exprime son intérêt et celui de la BnF pour des associations qui, comme l'ARCSI, œuvrent pour faire connaître une avancée technologique majeure, comme ce sera le cas au cours de la journée en abordant différents aspects en particulier historique, sociologique et technique. Il nous souhaite une excellente journée.

Jean-Louis remercie M. Riffault d'avoir accepté notre venue à des conditions privilégiées et d'être venu nous accueillir personnellement. Il lui remet la médaille de l'ARCSI ainsi que le superbe catalogue de l'exposition des Archives nationales sur le secret de l'État à laquelle l'ARCSI avait fortement participé

Jean-Louis Desvignes remercie les partenaires de cet évènement : Thales, Idemia, La Banque Postale, la BnF, TheGreenBow et Citalid.

Avant de présenter le programme de la journée, Jean-Louis informe l'assemblée de la disparition d'un autre membre de l'ARCSI, Hervé Lehning, qui nous a quittés quatre jours plus tôt après de longs mois d'hospitalisation. C'est une perte énorme pour notre association. Hervé Lehning, normalien, agrégé de mathématiques, membre du CA de l'ARCSI, avait introduit l'association au Salon de la Culture et des Jeux Mathématiques, tenu chaque année, fin mai, place Saint-Sulpice. Il organisait le stand de l'ARCSI qui pour la première fois en 2022 s'est tenu sans lui. Hervé Lehning est l'auteur de livres qui font référence sur les mathématiques et la cryptologie, comme

« Le Livre des Nombres », « La Bible des Codes Secrets » ou encore « Toutes les mathématiques du monde ». Jean-Louis offrira certains de ces livres en cadeau aux divers intervenants. Un hommage lui est rendu dans ce bulletin.

Jean-Louis présente le programme général de la journée, le passé le matin, avec la formidable épopée de la carte à puce sous un éclairage historique, technique, normatif et industriel, et l'avenir de cette technologie, le « *Secure element* », dans le courant de l'après-midi, jusqu'à la clôture de l'évènement vers 19 h 00.

Il nous apprend que l'une de nos stars, Jean-Jacques Quisquater, a connu plusieurs déboires logistiques qui l'empêchent d'être parmi nous ce matin, mais que les efforts conjugués de nos spécialistes Christophe et Laurent et de l'équipe technique de la BnF nous permettront de l'entendre par visioconférence l'après-midi. Il s'ensuit quelques décalages sans conséquence dans le programme.

La première table ronde : L'hommage à Michel Ugon

Jean-Louis prononce un émouvant hommage de l'ARCSI à Michel Ugon, un homme attachant, dont l'intelligence n'avait d'égal que l'humilité et qui a su convaincre le monde industriel des atouts que présentait la carte à microprocesseur qui allait s'appeler la « carte à puce », la vraie carte à puce, celle avec un processeur de calcul, pas celle qui n'était qu'une carte à mémoire. Puis sans tarder, il appelle la première table ronde pour l'hommage à Michel Ugon.

Pierre Paradinas, Carlos Martin, Joël Hosatte et Dominique Decavèle

Présidée par Jean-Louis Desvignes, elle réunit quatre experts qui ont bien connu Michel Ugon : Pierre Paradinas, Carlos Martin, Joël Hosatte et Dominique Decavèle.

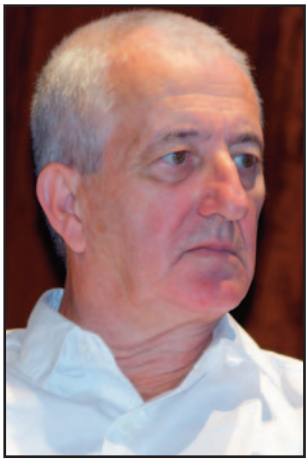
À tour de rôle, ceux-ci indiquent les circonstances dans lesquelles ils ont côtoyé Michel Ugon et tous soulignent ses grandes qualités humaines et professionnelles. Il a été un ingénieur fort apprécié et très écouté !

Pierre a côtoyé Michel Ugon en 1988, ce dernier étant membre du jury de sa thèse de doctorat sur la Biocarte (intégration d'une carte à microprocesseur dans un réseau professionnel de santé). Une relation sincère est née entre eux deux. Pierre a rencontré à nouveau Michel Ugon à Marseille en 1993, à l'occasion d'une conférence qu'il faisait sur la carte santé. Michel Ugon l'attendait au fond de la salle et ils ont discuté dans un coin du salon du peu de compréhension des responsables sur ce que pouvaient apporter les cartes à microprocesseurs.

Carlos a fréquenté longuement Michel Ugon lors du processus de certification des cartes à puces. Le succès de cette entreprise doit beaucoup à leur volonté commune d'aboutir, et à l'adhésion de Michel Ugon aux orientations données par le SCSSI et à l'énergie qu'il a alors déployée pour convaincre ses pairs.

Joël rapporte ici une anecdote que lui a confiée Michel Ugon. Au début de sa coopération avec Motorola, les directions avaient souhaité un protocole d'accord préalable, afin de régler les éventuels litiges entre les deux sociétés, en cas d'échec des discussions techniques. Exaspéré par la lenteur des juristes, il commença son travail sans attendre. Eh bien, quelques semaines plus tard, les techniciens avaient achevé leur coopération fructueuse, rendant caduque la nécessité du protocole juridique, alors que les juristes divergeaient encore sur leur texte !

La naissance d'une industrie à travers les applications de la carte, les brevets, les standards et les relations avec l'industrie des technologies de l'information



Pierre Paradinas

Jean-Louis Desvignes donne la parole au professeur Pierre Paradinas du Conservatoire National des Arts et Métiers – CNAM – Il est enseignant et titulaire de la chaire des Systèmes Embarqués, directeur du développement technologique à l'INRIA.

Il revient d'abord sur son histoire personnelle : au milieu des années quatre-vingt, le monde de la carte à puces était très petit, tous se connaissaient, et c'est naturellement que Michel Ugon fut membre de sa thèse de doctorat en informatique, sur la Biocarte, puis il aborde son exposé.

L'épopée de la carte à microprocesseur fut une prodigieuse aventure menée par de grands experts. Pierre Paradinas cite notamment le professeur Jean-Jacques Quisquater de l'université catholique de Louvain qui a grandement contribué à introduire la cryptologie dans la carte, Jean-Jacques Quisquater, qui interviendra l'après-midi par visioconférence.

L'histoire de la carte à microprocesseur est multiple, c'est celle des brevets (qui a inventé la carte ?), celle des normes (qui a dicté sa loi ?), celle des entreprises (qui a gagné la bataille ?) et celle des logiciels dans et autour de la carte.

Des centaines de brevets ont été déposées autour de la carte à puce, dont certains sont toujours actifs. La carte à puce est vraiment une aventure collective, mais qui en est à l'origine ? En France, les premiers brevets sont ceux de Moreno (1974), Ugon

(1977) et Guillou (1979). Mais il existe des brevets antérieurs aux États-Unis (Pomeroy – 1967 ; Halpern – 1972), au Japon (Arimura – 1972) et en Allemagne (Dethloff – 1977). Pierre donne le contenu des brevets et attire notre attention sur celui de Michel Ugon, le seul à donner le moyen d'assurer la sécurité de la carte : une consommation de courant identique, que l'opération requise soit autorisée ou non.

In fine, Innovatron (Moreno) et Bull CP8 (M. Ugon) réussirent à faire reconnaître leurs brevets et toucheront des royalties de l'ensemble de l'industrie. Mais l'adoption de cette invention passe par les normes et standards.

Française ou Allemande la première carte à puce ?

De nombreuses normes ont été publiées et encore davantage discutées, les deux pays les plus actifs étant la France et l'Allemagne, mais aussi la Grande Bretagne, les États-Unis et le Japon, ainsi que des industriels comme Visa et MasterCard. Michel Ugon, au nom de Bull CP8, a œuvré pour que la carte à microprocesseur devienne la norme ISO 7816. qui décrit en quatre parties adoptées de 1987 à 1995 ses dimensions, la place des contacts, les protocoles de communications. L'ISO 7816-3 conserve la trace des belles bagarres entre la France et l'Allemagne au sein de l'ETSI, avec la variante T=0 pour la France et T=1 pour l'Allemagne.

Le paysage est encore plus complexe au niveau des industriels, avec les pionniers français Bull CP8 et Schlumberger, mais aussi les acteurs du paiement (Allemagne) et du silicium (Motorola, SGS Thomson puis Gemplus, sans oublier l'Allemand Siemens/Infineon). La Direction Générale des Télécommunications (DGT) lance une expérimentation à Vélizy au début des années quatre-vingt, et les banques françaises le projet IPSO qui réunit les travaux de Philips à Caen, Bull CP8 à Blois et Schlumberger à Lyon. La carte Bull CP8 sera généralisée en 1986, mais le marché peine à décoller en France comme à l'étranger.

En parallèle, la DGT active le projet Télécarte qui, par son succès, induit le développement d'un tissu industriel en France (SGS Thomson, Schlumberger, Gemplus…) et en Allemagne (Infineon…) avec des exportations. Le projet Télécarte a été terminé en France en 2014.

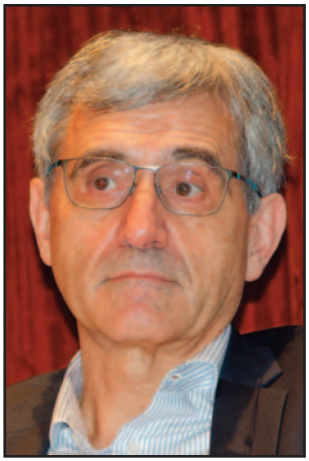
Les archives de Bull CP8 relatent sa dimension internationale, avec ses nombreux partenariats, mais le décollage est difficile, en particulier pour les cartes de paiement. La fin des années quatre-vingt et quatre-vingt-dix ont été les « années folles », le professeur Jean-Jacques Quisquater, membre de l'ARCSI pourra en témoigner. Les progrès technologiques, le logiciel Java en 1996, les clés publiques… offrent une opportunité salutaire, que les industriels saisissent en prenant en main leur devenir au sein du Java Card Forum.

Le marché décolle dans les années 2000, grâce aux télécoms et à la carte SIM. Les données d'Eurosmart, dont Michel Ugon a été le premier président, indiquent 1 100 000 000 (un milliard et cent millions) de cartes vendues en 1998, 5,5 milliards en 2010 et plus de 9,5 milliards de Secure éléments en 2020.

Michel Ugon, qui a porté la voix de la sécurité dans le domaine des cartes à puce, Louis Guillou et Jean-Jacques Quisquater peuvent être fiers de leurs contributions. En revanche, honte aux industriels et aux médias de ne pas avoir rendu hommage à Michel Ugon quand il est monté, en décembre 2021, vers les étoiles. L'ARCSI a tenu, par ces 14es Rencontres, à honorer celui qui fut un de nos éminents membres.

L'heure est aux questions du public. Il y en eut peu, les participants restant bouche bée devant un spectacle si instructif et si bien conduit. Geneviève Bouché, une des participantes et vice-présidente de l'association Forum ATENA interroge les intervenants sur un point qui lui tient à cœur : la souveraineté de la France face à cette technologie qui change tant de choses dans notre vécu quotidien. Elle évoque l'appel d'offres du ministère de la Santé, la carte vitale et celle des professionnels de santé.

Présentation de la mise en place du schéma français d'évaluation et de certification des technologies de l'Information. Application à la carte à puce.


Carlos Martin

Carlos Martin monte à la tribune. Carlos a été responsable du centre d'évaluation et de certification du SCSSI (Service Central de la Sécurité des Systèmes d'Information), ancêtre de l'ANSSI, dirigé alors par le général Jean-Louis Desvignes. Carlos a participé, pour la France, à l'élaboration des « Critères Communs » Europe/États-Unis (qui allaient devenir la norme ISO 15 408). Responsable ensuite à la Banque de France de la sécurité des moyens de paiement, puis RSSI de Carrefour France, il est aujourd'hui RSSI du Groupe La Banque Postale. C'est à l'époque où il s'occupait de certification qu'il a rencontré Michel Ugon qui a tout de suite adhéré au processus d'évaluation et de certification, et qu'il n'a eu de cesse de valoriser en étendant sa certification à l'ensemble des étapes de la fabrication de ses cartes. Carlos a su créer un collectif de personnalités œuvrant sur ces technologies.

Au premier congrès de l'ARCSI, à Rennes, en 2006, eut lieu un fort intéressant échange entre Michel Ugon et Louis Guillou à propos du brevet Guillou/Quisquater sur le *zéro knowledge*. Peu de temps après Michel Ugon commença hélas à avoir des problèmes de santé.

Carlos nous explique le schéma français d'évaluation et de certification des technologies appliquées au domaine de la carte à puce, depuis les ITSEC Européens jusqu'aux Critères Communs. Il cite l'organisme qui accrédite les laboratoires d'évaluation candidats : le COFRAC (comité français d'accréditation), avant que le SCSSI leur délivre leur agrément pour devenir centres d'évaluation : les CESTI. C'est sur eux que s'appuie le SCSSI (aujourd'hui l'ANSSI) pour délivrer les certificats en France, comme le fait le BSI en Allemagne, le CESG en Grande Bretagne, le NIST aux US, etc. Pour les cartes à puce, en France les CESTI sont le CEACI, le CEA/LETI et la SERMA. Il indique les différentes étapes à franchir pour obtenir une certification à différents niveaux de E1 à E6 pour les ITSEC et de EAL1 à EAL7 (*Evaluation Assurance Level*) pour les Critères Communs. 18 technologies de cartes à puces sont certifiées aujourd'hui. Il indique ces étapes depuis la description de la cible jusqu'à la certification et sa maintenance.

Les Profils de Protection, ainsi que les masques, l'encartage et l'échange de données, doivent être inclus dans la cible à évaluer, pour que celle-ci soit acceptée par l'ANSSI.

Le point de vue du GIE Carte Bancaire

Dominique Decavèle

Dominique Decavèle s'exprime à son tour. Il est un ancien du GIE Carte Bancaire qui était pour la France, au début des années 1980, le seul client de cartes à puce. Mais les banques ne voyaient pas d'un bon œil qu'il n'y ait qu'un seul fournisseur de distributeur de billets. IBM, entre autres industriels, est venu, en France, sur ce marché émergent.

En 1974, Roland Moreno avait montré une puce, mais qui était bien trop épaisse pour tenir sur une carte et entrer dans un distributeur de billets. Il avait déposé un brevet sur la protection des données de l'objet portable par un code confidentiel. Ce n'était qu'une carte à mémoire. C'était surtout à l'époque une solution qui cherchait un problème.

En 1977, Michel Ugon qui travaillait chez Bull dépose un brevet qui mettait en avant la capacité de traitement plutôt que la simple existence d'une mémoire. C'est devenu la technique Bull CP8 et là on peut parler de cartes à microprocesseurs. Bien des problèmes avaient enfin trouvé une solution.

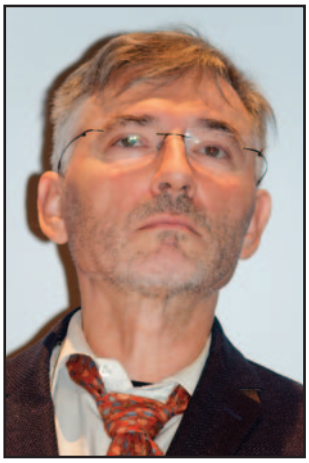
En 1978, la Direction Générale des Télécommunication, ancêtre de France Telecom lance avec dix banques françaises le GIE Carte bancaire. En 1979, Louis Guillou et Jean-Jacques Quisquater mettent l'accent sur la cryptographie embarquée.

Les cartes sans contact furent brevetées en 1980, puis des éléments de cryptographie furent intégrés dans les cartes à puce dès 1981 et firent également l'objet de brevets.

Dominique Decavèle évoque alors l'aventure de la Yescard, 1998-2001, qu'a permise une erreur de conception dans le protocole d'échange entre la carte et le terminal. La validité de la transaction était contrôlée par la carte, qui répondait par OUI ou NON. Pour les petits montants (600 F), la vérification en ligne n'était pas effectuée, la banque émettrice de la carte était informée en différé, la nuit, à la fin de chaque journée. Cette défaillance qui ne pouvait porter sur de gros montants sembla mettre la fraude informatique à la portée des pirates et plongea le GIE Carte Bancaire dans la tourmente. Informé de la faille, il a préféré une solution judiciaire à la solution technique plus contraignante. Quelle belle transition vers l'intervenant suivant, Serge Humpich, qui fut classé du côté des attaquants !

Pour bien avancer il faut reculer

Serge Humpich, ingénieur électronicien passionné, a été développeur de code notamment pour les salles de marché. Il nous explique que pour bien aller de l'avant, il faut savoir parfois prendre du recul sur « comment les choses se sont déjà passées », autant que sur le fonctionnement plus général de la société. Il nous fait part des motivations qui l'ont toujours guidé depuis qu'il était étudiant et, au fil du temps, des manquements qu'il a pu constater ou subir dans les processus de décision.


Serge Humpich

Il se défend d'avoir attaqué la carte bancaire comme il peut le lire parfois. Il s'y est intéressé par la passion de faire une activité suivie, technique, épanouissante sur la durée. C'est la recherche faite sans aucune documentation technique sur des programmes écrits en assembleur et son aspect minutieux qui l'intéressait, et non l'objectif final. Profondément surpris par l'absence de sécurité qu'il constate dans l'emploi de la carte bancaire, il veut simplement le prouver concrètement. Il retire, en démonstration publique, plusieurs carnets de tickets de métro des distributeurs de billets de la RATP. Il est finalement arrêté et condamné à une peine de prison avec sursis. Serge Humpich souhaite ne pas s'étendre davantage sur cet épisode, M. Decavèle nous ayant expliqué il y a quelques minutes la faille dans le protocole qui permettait les « yescard ».

Serge Humpich parle ensuite d'un sujet plus général, qui l'a aidé à douter de la fiabilité des cartes bancaires. Par des exemples précis, il montre que de l'État aux particuliers, dans les entreprises ou même dans l'éducation, tout le monde pense pouvoir encadrer les ingénieurs, décider à leur place et même leur expliquer comment travailler. Pourquoi n'a-t-on pas le même respect de leurs compétences que pour les médecins, comme lors de la crise sanitaire Covid 19 ? Cela amène régulièrement de petites et grandes catastrophes industrielles. C'est un fait de société qu'il ne s'explique pas et dont on n'entend jamais parler.

Vous trouvez que c'est mal ce qu'il a fait ? Un conseil, ne lui cherchez pas trop des noises, comme il me l'a dit le soir, au dîner, Serge est un adepte du Krav Maga 😊

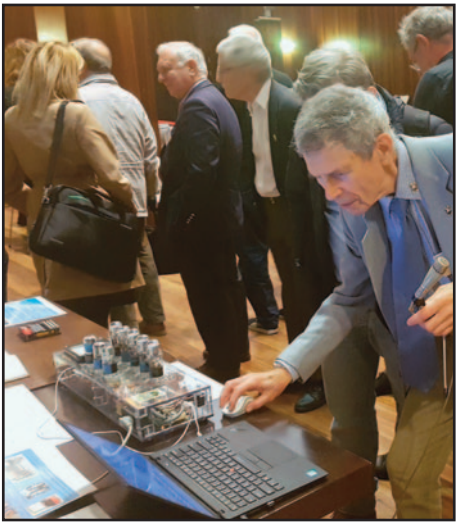
Pause déjeuner

À 13 h 00, un déjeuner nous attend à la sortie de l'amphi, offert par l'ARCSI.

On décompresse, on discute entre nous et avec les intervenants, le repas est somptueux, servi par un personnel très classe. Christian Lixi, un des organisateurs de l'évènement, secrétaire général de l'ARCSI, est aux petits soins pour nous. Portant deux bouteilles de vin, l'une de vin rouge, l'autre de vin blanc, il remplit les verres et veille à ce que tout le monde soit satisfait, et nous avions de quoi l'être !

Dans la salle se trouvent aussi le stand de l'ARCSI et ceux des partenaires de l'évènement. Sur celui de l'ARCSI, notre ami ARCSIste américain, Jon Paul nous accueille et nous engage à suivre la démonstration du premier convertisseur analogique/digital de l'histoire, le « quantificateur » du système de cryptophonie SIGSALY utilisé par Roosevelt et Churchill. Il montre également un simulateur de machine à chiffrer Enigma, qu'il a conçu, petite merveille d'électronique de la taille d'un smartphone.

Jean-Louis Desvignes et Jon Paul sur le stand de l'ARCSI



Jon Paul présente le « quantificateur » du système de cryptophonie SIGSALY

Après le repas, introduction à la cryptographie solide

Jean-Jacques Quisquater en visioconférence

Le professeur Jean-Jacques Quisquater, membre de l'Académie Royale de Belgique, éminent cryptologue et bien sûr membre de l'ARCSI, a connu la veille plusieurs déboires logistiques qui l'ont empêché de venir de Bruxelles. Il apparaît en petite vignette, par visioconférence, au-dessus de ses diapositives, sur le grand écran de l'amphi de la BnF. Jean-Jacques est notamment le co-inventeur du schéma d'identification Guillou/Quisquater des cartes à puce.

C'est à Louis Guillou (CCETT/EPT) que revient le plaisir d'avoir fait se rencontrer Michel Ugon, qui était alors chez Bull CP8, et Jean-Jacques, qui lui était chez Philips Research Lab. C'était au début des années quatre-vingt. Bien que concurrents au départ, leurs relations ont très vite été suivies et fructueuses, pour culminer en 1990 où Louis, Michel et Jean-Jacques étaient tous trois membres du Comité de programme du premier séminaire international ACSA 90 (Accès conditionnel pour les services audiovisuels), tenu à Rennes en juin.

On doit à Jean-Jacques l'introduction du chiffrement sérieux dans la carte, d'abord symétrique avec le DES. Jean-Jacques explique que Louis Guillou est indirectement responsable de son exploit. Celui-ci a expliqué en réunion que mettre le DES dans une carte était impossible vu la taille de l'algorithme et les capacités des composants disponibles. Jean-Jacques a alors considéré qu'un défi lui était lancé ! Au

terme d'un travail acharné et grâce à l'aide des équipes Philips de Hambourg, il a réussi à faire rentrer cet algorithme « au chausse-pied » dans une carte TB 100 de TRT. Le chiffrement asymétrique RSA viendra plus tard. Puis ce furent le projet CORSAIR en 1988 suivit du projet FAME en 1995 qui sert encore de principe de base, de nos jours. Ceci est expliqué dans un article du magazine Pour la science : « Comment on a sécurisé la carte à puce » de Jean-Jacques Quisquater et Jean-Louis Desvignes.

L'introduction dans les cartes à puce du chiffrement symétrique, le DES d'IBM, et d'un coprocesseur pour faire du chiffrement asymétrique RSA sont deux premières mondiales réalisées par Jean-Jacques.

Jean-Jacques termine en nous parlant aussi des algorithmes postquantiques dont les puces des cartes devront être équipées ; en effet, quand de puissants ordinateurs quantiques seront mis au point, le chiffrement asymétrique d'aujourd'hui deviendra obsolète, car les clés pourront être cassées dans un temps « raisonnable ».

La saga de la carte à puce continue sous le signe du « Secure Element »

Il est 15 h 30, il a été question du passé de cette formidable aventure, jetons maintenant un coup d'œil sur le futur de la carte à puce.

Présent et futur de la carte SIM – De la carte physique à la eSIM ; de la eSIM à la iSIM

Philippe Lucas

Philippe Lucas, executive vice-président chez Orange Innovation Devices and Partnerships nous parle de la vision d'Orange sur l'évolution de la SIM vers la eSIM (ou embeded SIM).

Au début des années quatre-vingt-dix, la surface d'une puce SIM prenait beaucoup de place. L'évolution s'est faite vers une mini SIM en 1996, une micro SIM en 2003, puis une nano SIM en 2012. L'évolution a continué vers la eSIM, miniaturisée et pré intégrée dans un équipement mobile. Afin d'offrir à l'utilisateur la possibilité de changer d'opérateur et répondre aux besoins de l'Internet des objets, la eSIM est configurable à distance et présente un mécanisme de téléchargement à partir d'Internet. Il y a possibilité de recevoir des profils tout au long de sa durée de vie, comme le type et les conditions d'abonnement avec un opérateur. Un QR code permet aussi de changer de profil.

La eSIM est dotée des mêmes éléments de sécurité que la SIM, c'est donc une grande évolution de la SIM. Elle est devenue indépendante d'un terminal particulier.

Chaque opérateur certifie sa eSIM. Les besoins d'hétérogénéité ont conduit à un marché M2M (*Machine to Machine*) où tout est contrôlé à distance, et à un marché grand public où le besoin de miniaturisation est important.

La eSIM est vue comme une évolution importante pour Orange car elle permet plus de flexibilité pour ses clients que la SIM. Son téléchargement pour faire une personnalisation est agile et instantané. Orange est le premier opérateur à proposer

ainsi des cartes qui peuvent être personnalisées et son marché s'étend en Afrique et au Moyen Orient. Ses partenariats avec en particulier Google et son Wear OS, avec Apple et Samsung qui introduisent la eSIM dans les montres cellulaires en font un leader sur le plan mondial. Les projections dans l'avenir laissent penser que, dans l'Europe de l'Ouest, vers 2026, 65 % des smartphones seront équipés de eSIM et 100 % vers 2030.

Une nouvelle évolution s'annonce pour la eSIM : la iSIM qui sera intégrée dans les processeurs et permettra ainsi d'optimiser l'espace dans les matériels qui en seront équipés, et d'améliorer leur design. Cependant, la question de la certification du composant devient un problème plus complexe et non résolu !

Il est 16 h 15, Jean-Louis Desvignes remercie le conférencier et lui remet son cadeau puis c'est le temps de la pause-café de l'après-midi ; on se retrouve à l'extérieur de l'amphi, les rafraichissements et le café sont les bienvenus, les conversations s'animent, des rendez-vous sont pris, on profite de ces derniers moments d'échange mais l'heure tourne il est déjà 16h 45.

Vite ! Retourner dans l'amphi pour ne rien rater de la suite : un exposé à trois voix.

L'évolution vers le « Secure element », composant essentiel de la carte à puce

La certification des cartes à puce

Claire Loiseau

Claire Loiseau, travaille dans le domaine de la certification depuis 1994. Elle est aujourd'hui présidente de Internet of Trust, qui offre à ses contractants son expertise pour les accompagner dans le processus de certification.

Elle commence par nous parler de la certification de la carte à puce dont la première certification « Critères Communs » a été attribuée à la carte Bull CP8. Ces certifications atteignent aujourd'hui les niveaux EAL4 jusqu'à EAL6 et pour quelques éléments le niveau maximum EAL7 où les spécifications formelles sont généralisées. Plus de 25 certifications Critères Communs ont été obtenues par les grands constructeurs comme Gemalto et Samsung.

Les PP – Profils de Protection - sont des éléments minimas à intégrer dans une cible de sécurité pour obtenir une certification Critères Communs. Concernant les cartes à puce, ils sont nombreux. Claire cite le Profil de Protection pour les JavaCards, pour les plateformes de gestion des cartes. Elle explique aussi le mécanisme de la certification : définition d'un catalogue d'attaques, des schémas pour y répondre, comment les tests doivent se dérouler…

Les innovations et les nouveaux usages

Deuxième des trois intervenants, Philippe Proust, de Thales Gemalto nous présente quelques innovations et nouveaux usages.

Philippe Proust

Entré chez Gemplus en 1993, devenu Gemalto, et lors du rachat de Gemalto par Thales, Philippe a continué sa carrière chez ce dernier industriel.

Pour infliger moins de plastiques qui polluent les océans, la carte à puce va utiliser des produits bio dégradables qui remplaceront les PVC. Certaines seront en métal, en acier inoxydable. Les cartes parleront via les smartphones, pour indiquer par exemple le montant d'une transaction, une fois celle-ci validée. L'authentification biométrique deviendra la règle, grâce à des capteurs sans contact.

Et cela sera réalisé grâce aux « *Secure Elements* » qui contribueront grandement à l'évolution des SIM vers les eSIM puis vers les iSIM. Des alliances s'annoncent comme le Titan Security de Google. Au-delà des cartes à puce, les véhicules connectés seront largement équipés de eSIM, jusqu'à 5 par véhicule, dont un *Secure Element* qui rendra les véhicules communicants avec l'application CAR2CAR.

Et dès que la mémoire RAM pourra être plus importante sur les puces, on prévoit l'intégration d'algorithmes de cryptographie postquantique.

Évolutions techniques et usages du Secure Element

Yves Portalier

Troisième intervenant, Yves Portalier, senior vice-président IDEMIA France. IDEMIA est issue du rapprochement de deux entreprises françaises Morpho (anciennement Safran Identity) et Oberthur Technologies. Grâce à ses technologies, IDEMIA fournit à ses clients des solutions pour créer des identifiants, vérifier des identités et les analyser et ainsi fluidifier toutes les applications faisant usage de l'identité.

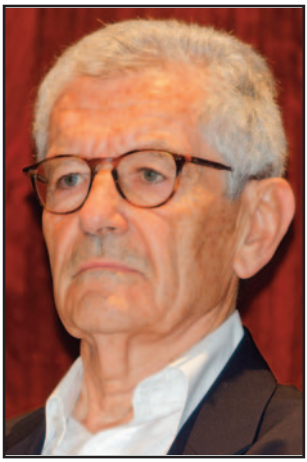
Yves nous présente l'évolution du *Secure Element* et des services associés. Depuis des années, la carte SIM fournit une solution sécurisée pour l'identité des utilisateurs sur les réseaux télécoms. Elle fait désormais partie d'un écosystème de services sécurisés gérant à distance l'identité numérique de l'abonné, jusqu'aux solutions IoT Safe (Internet des objets) définies par la GSM Association.

L'évolution vers des écosystèmes complexes sécurisés engendrerait une fragmentation néfaste du marché s'il n'y avait des initiatives fortes de standardisation. C'est ce qui a été fait pour l'eSIM et le « *subscription manager* » en impliquant toutes les parties prenantes. Par exemple dans le secteur automobile, 70 % des véhicules neufs seront livrés en 2030 avec une connectivité intégrée, permettant aux constructeurs de multiplier les services déployés. Cela implique une évolution profonde des rôles et responsabilités des différents acteurs, afin d'assurer l'interopérabilité entre la composante embarquée et le reste en ligne.

Ouvrir le monde, le rendre plus sûr, tel est le credo affiché par Idemia.

Les 3 exposés terminés, Jean-Louis Desvignes remet un livre cadeau à chaque intervenant. Place maintenant à une intervention avant une dernière table ronde.

La carte à puce et la Défense



Joël Hosatte

Jean-Louis Desvignes, président de l'ARCSI présente le vice-président de l'ARCSI, Joël Hosatte, qui est Ingénieur général de l'armement (IGA) en retraite et qui, pendant de nombreuses années, a œuvré à la réalisation de nombreux équipements assurant la sécurité des communications de nos armées et de nos gouvernants.

Pour mieux comprendre l'usage des cartes à puce dans la Défense, Joël remonte au contexte des années quatre-vingt. L'informatique et les télécommunications étaient deux domaines séparés. Il faut attendre mars 1986 pour que les responsabilités sécurité des deux domaines fusionnent au sein du SCSSI, ancêtre de la DCSSI devenue l'ANSSI.

À partir de 1982, Joël a présidé un nouveau groupe de coordination sécurité de la DGA, qui fut baptisé Groupe de coordination sécurité des systèmes d'information, appellation SSI qui fut reprise 4 ans plus tard à la création du SCSSI et qui perdure aujourd'hui. Il en revendique en quelque sorte la paternité.

Les équipements de chiffrement utilisaient des algorithmes symétriques, mis à la clé manuellement. Le principal risque de sécurité était la compromission des clés par les personnels, lors de leur transport ou leur mise à la clé. Les solutions pour réduire les conséquences d'une compromission (cloisonnement des réseaux et crypto-période courte) augmentaient en fait le nombre de personnes ayant à manipuler les clés, donc paradoxalement le risque de compromission !

C'est dans ce contexte que Michel Ugon est venu présenter son **C**ircuit **P**ortatif des années **8**0 ; à noter au passage l'origine du nom de la carte CP8 et de la société Bull CP8. Cette carte avait toutes les qualités requises pour maintenir le secret des clés.

Joël présente alors de nombreux équipements de chiffrement voix et données qui utilisèrent la carte pour leur mise à la clé. Ce fut d'abord en matière de téléphonie la CHS, première Cryptophonie de Haute Sécurité numérique avec vocodeur, chiffre numérique et modem à 2400b/s qui ne sera guère utilisée que par les militaires, les autorités gouvernementales rechignant à utiliser un équipement encombrant et n'assurant pas un confort d'écoute suffisant. La génération suivante, le DCS 500 de Sagem fut mieux acceptée, mais il fallut tout de même rogner la carte qui dépassait de l'équipement pour éviter qu'un Président agité manipule cette carte pendant ses conversations interrompant celles-ci. Il faudra attendre le début du XXI^{e} siècle pour voir l'équipement de cryptophonie TEOREM de Thales utiliser la carte à puce comme l'élément tangible d'une véritable infrastructure de gestion de clés (PKI).

En matière de chiffrement des données, l'équipement de chiffrement de paquets X.25 Capucine fut également équipé d'un lecteur de carte de même que les chiffreurs IP qui suivirent.

Enfin, concernant les cartes nominatives, Joël nous présente une relique, son ancienne carte d'adhérent à notre association : une carte à puce ! Sous l'impulsion de son dynamique président de l'époque, Pierre Bénéteau, l'Association des Réservistes du Chiffre s'était déjà ouverte aux personnels de la SSI, mais avait conservé son sigle : ARC. La puce donnait un air de modernité indéniable. En fait, la carte ne comportait pas de puce, juste le connecteur pour le décor !

Joël conclut son exposé en mentionnant le projet des États-Unis de doter d'une carte à puce chaque agent fédéral. La grande NSA avait demandé en 2000 à Jean-Louis, alors directeur du modeste SCSSI, son aide pour engager le processus de certification de cette carte. Jean-Louis intervient alors pour préciser qu'il s'était naturellement empressé de répondre favorablement à cette demande, d'autant plus facilement qu'il quittait ses fonctions le mois suivant.

La carte survivra si elle sait gérer sa disparition !

La dernière table ronde s'installe, avec les intervenants de l'après-midi, présidée par le professeur Pierre Paradinas. Le professeur François Pellegrini de l'université de Bordeaux et vice-président de la CNIL conclura cette journée haute en émotions et connaissances partagées.

François Pellegrini et Yves Portalier

Trois facteurs sont réunis pour permettre à une carte à puce d'assumer son rôle

- L'identification du possesseur ;
- sa connaissance d'un secret (mot de passe, code PIN) pour s'authentifier ;
- et bien sûr la possession de la carte.

La carte pourra survivre si le possesseur peut apporter les éléments de preuve qu'il est bien celui qu'il prétend être (par exemple par la biométrie), et s'il est aussi capa-

ble de faire disparaître ces éléments. Prouver son identité c'est bien ; ne pas avoir à prouver son identité c'est bien aussi. Les « *Secure Elements* » seront ici indispensables. Les cartes faites en matière bio ou en métal devront se substituer aux cartes en plastique qui sont mauvaises pour la planète. Il faudra anticiper la venue des cartes iSIM, qui devront être très sécurisées et qui prendront le pas sur les cartes eSim qui remplacent déjà les cartes SIM.

En conclusion, François Pellegrini précise que bien entendu on ne pourra pas laisser sans contrôle les données confidentielles. Si on veut garder la maîtrise des équipements, lors des transferts de données d'un équipement à un autre, il faudra éviter de passer par des intermédiaires. Chiffrer les données sensibles est-ce LA solution ? Le problème est qu'il faudrait aussi éviter que puisse être prouvée, dans certains cas, la présence d'une personne à un endroit donné.

Le problème de la sécurité par rapport à la sûreté est évoqué. Un citoyen est en droit de ne pas être entièrement soumis à l'État et la souveraineté numérique est un facteur essentiel.

Jean-Louis Desvignes termine cet évènement en remerciant les intervenants, les participants restés nombreux et les sponsors. Il est 19 h 00 passé, l'amphi se vide après cette journée bien remplie.

Et tout se termine par un repas

Et pour finir une Guinguette !

À l'EP7, guinguette numérique et gourmande, restaurant sympa située non loin de la BnF, avec quelques intervenants et organisateurs de l'évènement, nous nous retrouvons, autour d'un convivial dîner dans une ambiance un peu bruyante.

Malgré cela, les échanges passionnés continuent, des projets s'échafaudent, des rendez-vous sont pris. À côté de nous coule la Seine et avec elle, déjà le souvenir de cette mémorable journée. Bien sûr, pour l'ARCSI, cet évènement n'est qu'une continuation des activités multiples de l'association. Voyez sur le site de l'ARCSI (`www.arcsi.fr`), vous aurez une idée de ce que notre si chère association propose et réalise.