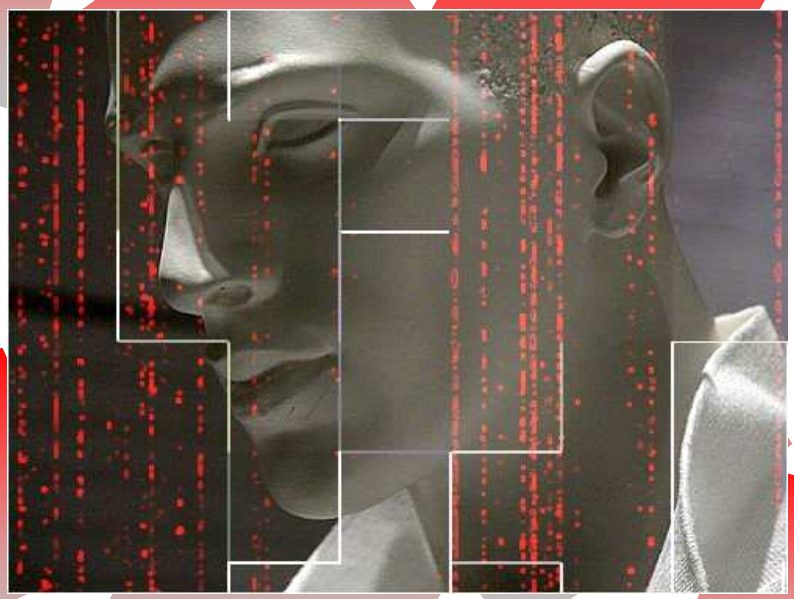
SCIENCE ALLEMAGNE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Dossier d'information du Service pour la Science et la Technologie de l'Ambassade de France en Allemagne – Mars 2009

L'identité électronique sécurisée

Définition, enjeux et développements technologiques en Allemagne



Directeur de publication : Dr. Ing. Jean-François Dupuis
Directeur de la rédaction : Romain Collignon
Traduction : Jana Ulbricht
Photo de couverture : Romain Collignon

Rédaction. Ambassade de France en Allemagne - Service pour la Science et la Technologie
Adresse postale : Pariser Platz 5, D-10117 BERLIN
Tél:+49 30 590 039 000, Fax:+49 30 590 039 265, Internet: www.wissenschaft-frankreich.de, E-mail : sciencetech@botschaft-frankreich.de

Sommaire

Préambule

Ces dernières années, l'émergence et le développement exponentiel des réseaux sociaux et des blogs sur Internet ont conduit à la prolifération massive des données personnelles des internautes. Désormais, chaque utilisateur dispose et doit gérer une véritable « identité numérique » constituée de ses contributions et des traces qu'il répand sur la Toile.

L'utilisation croissante du monde virtuel et l'évolution d'Internet offrant de plus en plus de services aux particuliers, aux entreprises et aux gouvernements amènent irrévocablement à se poser la question de la sécurité de l'information et plus particulièrement de celle relative à la protection des données personnelles.

Une des réponses à cette problématique consiste en la mise en œuvre d'identités numériques s'appuyant sur des technologies d'authentification permettant d'apporter aux utilisateurs la confiance nécessaire dans l'utilisation de l'outil Internet et des réseaux de communication.

Dans ce domaine, l'Allemagne fait figure de précurseur. Si la carte d'identité actuelle permet une identification dans le « monde papier », son pendant dans le monde de l'Internet n'existe toujours pas. C'est pourquoi le gouvernement fédéral allemand a décidé de mettre en place, à partir de novembre 2010, une carte d'identité électronique pour chaque citoyen allemand.

Avec l'arrivée imminente de cette carte, de nombreuses questions se posent quant à la définition de l'identité numérique, à ses enjeux, à ses applications et aux développements scientifiques qui s'y rapportent, mais également aux limites de ce système.

Cependant, dans un monde toujours plus communiquant, prouver l'identité d'une personne n'est pas le seul défi à relever. Il est également nécessaire de pouvoir justifier de l'identité d'objets, de produits et de garantir la propriété intellectuelle grâce à des procédés innovants tels que les filigranes ou les signatures numériques.

La présente édition du Science Allemagne : « L'identité électronique sécurisée », donne un aperçu des développements technologiques en Allemagne dans le cadre de l'introduction de la carte d'identité électronique. Elle offre également une vision des systèmes de sécurité mis en place dans les infrastructures de communication.

Preuve réciproque de l'identité sécurisée grâce à l'introduction en Allemagne de la carte d'identité électronique à partir de 2010

Martin Schallbruch, directeur des technologies de l'information et de la communication (TIC) au Ministère fédéral de l'Intérieur, Berlin

Martin Schallbruch, *diplômé en informatique né en 1965, est responsable, en tant que CIO (Chief Information Officer) auprès du Ministère fédéral de l'Intérieur, de la stratégie et coordination des TIC au sein de l'administration fédérale. Il traite également des questions relatives à la sécurité nationale dans le domaine des TIC. La gestion des passeports et des pièces d'identité, incluant le projet „passeport électronique", est aussi de son ressort.*

L'utilisation des données personnelles relatives à l'identité pour la communication et les transactions sur Internet est actuellement un sujet de plus en plus important dans les discussions sur la sécurité et la protection des données dans les médias numériques. Les acteurs de la sphère politique, de l'administration, de l'industrie et du monde scientifique parlent d'une même voix : la migration croissante de nos activités professionnelles et personnelles dans le monde virtuel apporte certes avec elle un degré de liberté et d'efficacité. Cependant, elle entraîne aussi de nouveaux types et quantité de risques, comme par exemple la multitude des codes PIN et des mots de passe qui doivent être créés et gérés pour chaque service en ligne. L'insouciance des citoyens lorsqu'ils transmettent leurs données et lorsqu'ils choisissent leurs canaux de communication, apporte sa part de risques et elle offre une cible privilégiée aux malfaiteurs.

De ceci résulte une responsabilité de l'Etat de veiller à la création d'une infrastructure sécurisée, fiable et de confiance dans la communication sur Internet. Il peut – et doit – créer des conditions générales appropriées pour les secteurs privé et public, signifiant tout d'abord la mise en place de mesures légales et des garanties de sécurité correspondantes, comme par exemple des procédés de certification. Cependant, l'Etat doit soutenir parfois la commercialisation de certains standards et d'infrastructures TIC, car elle ne peut pas être à la seule charge d'entreprises isolées. En ce sens, la carte d'identité électronique - le projet actuel du Ministère fédéral de l'Intérieur – en est un bon exemple.

Ce projet fait partie des priorités du gouvernement allemand et se trouve au centre de la stratégie E-Identity qui a été définie dans le cadre du programme gouvernemental *E-Government 2.0* en 2006. La nouvelle pièce d'identité sera un catalyseur pour l'e-gouvernance, mais ses effets vont bien au-delà. Elle présente un avantage pratique conséquent pour l'e-business et l'e-gouvernance et ne peut être menée à bien que par une coopération étroite entre l'administration et l'industrie. En 2008, les conditions réglementaires et techniques les plus importantes ont été définies. Les premiers tests de grande envergure sont prévus au cours de l'année 2009. La nouvelle carte d'identité électronique doit être délivrée d'ici fin 2010. Simultanément, de nombreuses applications attrayantes seront mises à disposition au niveau fédéral pour l'utilisation de cette nouvelle pièce d'identité.

Le but initial de ce projet était de transférer les fonctions présentes sur la carte d'identité actuelle du « monde papier » au monde virtuel. Aujourd'hui déjà, la carte d'identité est utilisée au quotidien aussi souvent comme moyen d'authentification dans le domaine privé que dans le domaine administratif. Il suffit de penser à l'ouverture d'un compte bancaire, la clôture de contrats d'assurance et de vente ou bien l'acquisition de biens autorisée à partir d'un certain âge. Tous ces services se trouvent également en ligne. Toutefois, les processus d'identification nécessaires sont aussi variés que le nombre même de prestataires. La carte d'identité électronique doit mettre fin à cet imbroglio de codes PIN et de mots de passe en offrant la possibilité d'une « authentification standard ». Les processus d'inscription et de connexion doivent être transparents pour le citoyen et il doit pouvoir décider en toute connaissance de cause quelles données personnelles il transmet sur Internet. Chacun des *deux* partis d'une communication ou

d'une transaction doit avoir la certitude de l'identité de son interlocuteur.

C'est pourquoi tous les prestataires de service de l'e-gouvernance et de l'e-business souhaitant intégrer la carte d'identité électronique dans leurs processus, doivent demander au préalable des certificats d'autorisation auprès d'une instance publique. Ce n'est seulement qu'après avoir reçu un tel certificat que le prestataire de service sera techniquement autorisé à demander des données personnelles. Là encore, c'est le possesseur de la carte qui contrôle quelles données sont échangées lors de la transaction électronique.

En utilisant par exemple son ordinateur personnel, il verra apparaître : *le prestataire X vous demande vos nom, adresse et âge pour la transaction Y*. Ce n'est qu'avec le code PIN de la carte d'identité que le possesseur donnera en effet accès à ses données. L'utilisation pour le citoyen de la fonction électronique de la carte reste cependant facultative. Lorsqu'ils iront retirer leur carte à la mairie, les citoyens allemands pourront, à ce moment, décider soit directement soit ultérieurement si les fonctions électroniques de la carte doivent être activées. Selon les besoins personnels, une signature électronique individuelle peut être ajoutée en plus à la carte par un prestataire de signatures privé.

Les champs d'application de ses nouvelles fonctions seront multiples. L'e-gouvernance doit en profiter à tous les niveaux fédéraux. Des milliers de processus de demande des données standards – nom, adresse, âge, lieu de naissance – peuvent être automatisés. Des demandes et contrats peuvent être gérés de façon entièrement électronique, puisque la carte d'identité électronique remplie la fonction de signature manuelle et rend cette dernière accessoire. Des serveurs de formulaires et de nombreuses transactions pourront désormais être utilisés en toute sécurité avec cette nouvelle carte. En effet, la signature électronique manquait jusqu'à présent en tant que dernier élément nécessaire à leur mise en place. Il est donc décisif pour la réussite de l'introduction de la carte d'identité électronique qu'elle soit intégrée de façon optimale dans les projets et concepts existants. Ceci vaut de même pour les projets de l'initiative *Deutschland-Online*, avec par exemple la déclaration des véhicules, ainsi que pour les solutions déjà établies telles que l'assurance vieillesse allemande. L'optimisation en masse des procédures permettra la diminution des charges administratives et la concrétisation des objectifs de l'e-gouvernance : disponibilité des services 24h/24, traitement en ligne, suppression des temps de déplacement et des frais d'affranchissement et des consultations personnelles.

Outre son usage dans le commerce en ligne, c'est la confiance apportée par la future carte d'identité dans les processus électroniques qui devient de plus en plus importante. Là où aujourd'hui il existe les procédés les plus variés pour justifier son identité sur Internet – et auparavant par courrier – la carte d'identité électronique peut permettre d'établir un nouveau standard. Ce dernier doit être « appris » seulement une fois et peut être ensuite utilisé quotidiennement dans de nombreux domaines : achats en ligne, enchères en ligne, ouverture de comptes bancaires ou résiliation de contrats d'assurance.

A cette fin, le Ministère fédéral de l'Intérieur est entré en 2008 en dialogue intense avec le syndicat professionnel allemand des TIC – BITKOM – ainsi qu'avec les responsables de la branche. Les premiers projets-pilotes viennent d'être lancés avec, par exemple, le Land de Bade-Wurtemberg (sur le portail Internet du Land), l'Institut Fraunhofer des technologies de l'information sécurisées (SIT) et l'Université technique de Darmstadt. Suite aux consultations parlementaires en cours au sujet de la loi concernant la nouvelle carte d'identité, une série de tests sera lancée en 2009 dans tout le pays avec différentes autorités, entreprises et un grand nombre de volontaires. La phase de préparation montre d'ores et déjà que cette nouvelle carte dispose, même hors du contexte de l'Internet, d'un potentiel d'application bien supérieur à celui initialement prévu. Outre les exemples des distributeurs automatiques de cigarettes, d'autres applications « offline » sont envisagées : les points de vente du loto, les caisses de grandes surfaces pour les contrats de paiements d'acomptes ou les réceptions d'hôtel.

Avec cette nouvelle carte, la justification électronique de l'identité doit augmenter la sécurité et la fiabilité de l'identification et de la communication sur Internet, en établissant une nouvelle infrastructure de sécurité liée à cette carte destinée à tous les secteurs et à chaque citoyen dans le but d'un changement durable de la culture d'Internet.

Contact

Martin Schallbruch
IT-Direktor im Bundesministerium des Innern, Berlin

Téléphone : +49 (0) 301 86810
E-mail : itd@bmi.bund.de

Plus de sécurité dans le monde numérique – Comment les identités électroniques influencent-elles l'organisation de la vie quotidienne du citoyen ?

Björn Donath, Senior Innovation Developer – Imprimerie fédérale, Berlin

*Depuis 2006, **Björn Donath**, ingénieur diplômé de sciences économiques, travaille pour l'imprimerie fédérale à Berlin. Dans un premier temps, il a été responsable de la gestion de projets et du Proposal Management. Début 2008, il a pris la fonction de « Senior Innovation Developer » dans le département de R&D de l'entreprise et est responsable, entre autres, de la gestion de projets et de la coordination des activités de recherche de l'imprimerie fédérale au sein du cluster d'innovation Fraunhofer « Identité sécurisée ». De plus, Björn Donath veille à la coopération du cluster avec les organismes de recherche nationaux et s'occupe de la fondation des futurs laboratoires dans le domaine de l'« identité sécurisée ».*

Le monde a changé. Un deuxième univers a été créé avec Internet, et nous utilisons ses possibilités de communication, d'information et de commerce aussi naturellement que dans le monde réel, et ceci avec l'aide des identités électroniques. Malgré les grandes libertés et chances que nous offrent les nouvelles technologies modernes d'information et de communication, apparaissent également de plus en plus d'inconvénients liés aux chaînes de création de valeur mises en réseau. De nombreuses duperies connues, issues des méthodes commerciales classiques (par exemple l'escroquerie financière, sur les crédits et sur les biens), se sont également répandues aujourd'hui sur Internet, tout comme les nouvelles attaques spécifiques en ligne à l'encontre des données personnelles de l'utilisateur. Les hackers et les usurpateurs d'identité ne causent pas seulement des dommages économiques énormes, ils augmentent également la méfiance des utilisateurs vis-à-vis d'Internet. De ce fait, une infrastructure sécurisée d'Internet devient de plus en plus nécessaire. Les organismes de recherche internationaux ainsi que les prestataires de technologies de haute sécurité sont sollicités pour contribuer à une plus forte sécurité de l'identité numérique par de nouveaux procédés et de nouvelles solutions.

eIdentity – un partenaire fiable au sein du réseau

Malgré ces prédictions alarmistes, nous avons besoin et nous voulons disposer de la rapidité et du confort que nous offrent les infrastructures fiables des TIC. Plus nous utilisons les services du World Wide Web, plus les mécanismes de protection fiables pour nos données personnelles nous sont nécessaires. Avec notre identité électronique (eIdentity ou eID), nous nous créons un partenaire fiable et compatible avec le réseau pour les tâches quotidiennes réalisées en ligne. L'eID doit permettre d'assurer clairement l'identification de l'individu sur Internet aussi bien que dans le monde réel.

Ce n'est qu'avec une identité sécurisée qu'il nous est possible de nous distinguer de la masse et de nous identifier clairement comme un partenaire commercial ou de communication. Cela vaut notamment pour des situations où nous désirons accéder à un service sensible, comme par exemple pour ouvrir un compte bancaire, pour des démarches administratives en ligne ou seulement pour recevoir des informations, des lettres ou des biens sur Internet. Notre identité électronique doit nous suivre partout telle une sorte d'identité itinérante intelligente - *« Identity Roaming »* - même lorsque nous quittons notre pays d'origine.

Dans la communication classique avec un vis-à-vis, nous utilisons des documents d'identité hautement sécurisés comme la carte d'identité ou le passeport. C'est notamment cette fonction que doit satisfaire notre « eIdentity » lors des transactions électroniques, puisque seule l'irréversibilité des personnes, des auteurs ou des expéditeurs permet la création de relations sécurisées. Dans le monde numérique, nous devons également être sûrs que l'expéditeur d'une information est réellement la personne qu'il prétend être. Ceci vaut de même pour les produits coûteux. Nous devons savoir avec certitude qu'il s'agit d'originaux et non de copies.

Ces dernières années, différents mécanismes de sécurité ont été développés afin de satisfaire ce besoin de sécurité naturel. Outre la signature classique et la vérification d'identité à travers les documents personnels, divers mécanismes et codes d'accès ainsi que des processus de signature numérique sont aujourd'hui mis en place. Malheureusement, certains des systèmes disponibles actuellement ne seront plus fiables à l'avenir. Des systèmes insuffisamment protégés contre la contrefaçon, des domaines d'application ou des conditions d'utilisation restreintes entravent le fonctionnement efficace des identités électroniques,

qui mènent souvent les utilisateurs des espaces virtuels dans un vrai chaos d'identité. Nous avons toujours besoin de douzaines de mots de passe, de PIN et de TAN différents pour passer d'une activité sécurisée de banque en ligne à des plates-formes de communication sécurisées ou d'e-commerce. Pourtant, tout le monde sait que des preuves univoques d'identité sont indispensables pour créer des relations commerciales basées sur la confiance.

Des stratégies pour plus de sécurité dans le réseau

Pour cette raison, des concepts et des solutions sont développés dans le monde entier pour la mise en place de stratégies relatives à l'eIdentity. Ainsi, l'Initiative « i2010 » de la Commission européenne fait de la gestion de l'eIdentity une priorité de son plan d'action transfrontalier « eGovernment ». Dans ce contexte, l'Allemagne fait également avancer très activement son programme « eGovernment 2.0 » auquel participent les Länder et les communes.

Même dans le domaine classique des documents ID, il s'est produit un changement radical durant les trois dernières années. Depuis novembre 2005, de nouveaux documents de voyage électroniques (ePass) sont distribués dans tous les Etats membres de l'Union Européenne. Ainsi, les Européens disposent pour la première fois d'une eIdentity officielle qui est acceptée et qui s'utilise de plus en plus, selon les études de marché actuelles, comme pièce d'identité pour le payement de biens et de services à l'étranger ainsi que pour les activités commerciales électroniques. Deux domaines d'application de la gestion d'identité, celle officielle et celle utilisée dans le privé - qui jusqu'alors étaient strictement séparés, s'assimilent progressivement.

La pièce d'identité électronique comme clé de voûte des applications TIC orientées vers l'avenir

L'eID sécurisée sera la clé de voûte pour des relations sécurisées et fiables dans l'espace virtuel – ceci est un fait et l'Allemagne en tient compte avec l'introduction de la carte d'identité électronique à partir de novembre 2010. Dorénavant, les fonctions classiques de la nouvelle carte d'identité établie doivent permettre également une identification et une authentification fiables sur le réseau.

Grâce à la réalisation technique de ce projet TIC le plus grand et le plus exigeant au monde, ce sont plus de 80 millions d'Allemands qui pourront bientôt potentiellement s'identifier en ligne, prouver avec fiabilité leur âge ou s'authentifier clairement auprès des services électroniques. Ceci exigera peu de démarches : une demande de nouvelle pièce d'identité électronique et l' achat d'un lecteur compatible.

Lors de la demande, le titulaire du document décide quelles fonctions il souhaite intégrer à sa carte. En Allemagne, il existe un droit à l'autodétermination des informations personnelles. Il stipule que chaque citoyen peut décider lui-même s'il veut utiliser ou non son eIdentity officielle pour des processus et des applications privés.

Fournisseurs eID – Les garants d'une plus grande sécurité dans le réseau

Du point de vue du droit à la protection des données, les standards de sécurité doivent absolument être étendus de par l'introduction des fonctions électroniques d'identité. Dès que des données personnelles numériques (nom, adresse, date de naissance) sont utilisées pour la première fois avec l'accord du titulaire du document, non seulement auprès des administrations, mais également dans le cadre de secteur privé pour la légitimation et l'authentification, il devient nécessaire de créer des mécanismes de protection hautement sécurisés. Telles les instances publiques actuelles, les partenaires commerciaux et de communication habilités devront disposer de certificats d'autorisation définis précisément, qui seront uniquement délivrés par des centres de confiance autorisés ou de hautes instances de sécurité.

Ainsi, les services des fournisseurs ID hautement spécialisés, certifiés partenaires de confiance, gagneront énormément en importance puisqu'ils permettront un commerce sans duperie et en accord avec la loi. En effet, sans les services des instances de certification qui vérifient et confirment l'identité de façon indépendante, les TIC ne fonctionneraient plus, que ce soit dans les secteurs officiels ou privés. Dans ce contexte, de nouveaux mécanismes e-Ident, qui, comparés au système actuel de Post-Ident, doivent être mis en place pour plus de fiabilité et de confort dans la protection de l'anonymat et de la sphère privée.

Les défis technologiques sont énormes, puisqu'ils relèvent de concepts de cartes d'identification à fonctions multiples comme le système développé pour la carte d'identité. D'une part, un environnement-système entièrement nouveau et unique dans sa complexité sera créé. Ce réseau surpassera de loin les obligations exigées par les infrastructures de l'ePass.

D'autre part, les structures hautement performantes pour les Firewalls doivent garantir une délimitation claire entre les secteurs d'accès officiels et privés. Il s'agit avant tout de la protection efficace des données biométriques, telles que les empreintes digitales numérisées, qui ne doivent être utilisées que par les instances de sécurité mandatées par l'Etat.

Du point de vue technologique, il sera possible de maîtriser ces défis. De plus, un travail intensif de

sensibilisation est nécessaire. Les avantages que présentent la vérification de l'identité électronique et la sécurité qui est offerte par les fournisseurs eID certifiés, doivent, avant tout, être transparents pour l'utilisateur et être en mesure de le mettre en confiance. Des applications accessibles et centrées sur l'utilisateur y contribueront. Elles doivent être mises en place dès aujourd'hui et non dans quelques années. Ceci constitue l'une de grandes missions des sociétés modernes de l'information.

Les identités en ligne et hors ligne en adéquation

Avec l'introduction de la carte d'identité électronique, l'Allemagne et ses partenaires s'aventurent sans aucun doute en terre inconnue. Pourtant, nous devons nous rendre compte que le monde réel et le monde virtuel, que nous distinguons encore aujourd'hui, vont se rapprocher de plus en plus et que les identités en ligne et hors ligne se connecteront également. Car peu importe ce que nous faisons et où nous nous déplaçons, nous agissons toujours en tant que propre individu et ne disposons que d'une seule identité absolue et unique.

La création de standards de sécurité à l'épreuve du temps signifie ainsi que nous devons penser au-delà des fonctionnalités d'un seul document et que nous devons apprendre à envisager, diriger et sécuriser fiablement les structures gigantesques du réseau.

Déjà aujourd'hui, il n'est plus possible de s'abstenir de certaines étapes de la chaîne globale de création de valeur concernant des procédés hautement sécurisés. C'est pourquoi l'imprimerie fédérale ne s'occupe plus uniquement du développement de technologies d'imprimerie innovantes, mais elle conquiert aussi de plus en plus les domaines d'applications innovantes des TIC.

Dans ce but, nous nous penchons aussi bien intensément sur des structures mathématiques et des technologies complexes de logiciel que sur des problèmes de la gestion de l'eID à long terme.

Perspectives

A long terme, seuls les concepts de sécurité garantissant des standards de sécurité interopérables au niveau international, utilisés pour tous les procédés d'interaction réels ou virtuels, de commerce et de communication, seront en mesure de convaincre.

Afin de maîtriser ce défi, l'imprimerie fédérale s'engage dans des groupes de travail et de recherche interdisciplinaires.

Le Cluster d'innovation Fraunhofer «Identité sécurisée» récemment fondé constitue un bon exemple pour cet engagement. Aux côtés de l'imprimerie fédérale sont impliqués onze autres partenaires économiques, cinq instituts de recherche ainsi que les Länder de Berlin et de Brandebourg,.

Participer activement à la conception d'un avenir social et technologique sécurisé nécessite une innovation d'excellence. Ceci signifie pour nous travailler dans une perspective globale et être actif dans tous les sous-domaines des chaînes intégrées de procédés d'identification. Outre le développement continu des documents classiques et électroniques ID, nous offrons également, en coopération avec notre centre de confiance D-TRUST, de nouveaux procédés de gestion fiable de l'eID ainsi que tous les services de certification utiles que peut proposer un fournisseur ID digne de confiance. L'innovation d'excellence signifie également encourager de nouvelles formes de coopération. C'est pourquoi nous disposons de laboratoires d'avenir à sujet spécifique, dans lesquels sont élaborés de nouveaux systèmes pour l'identification, des procédés de fabrication et des matériaux ainsi que d'une culture d'entreprise orientée vers l'avenir.

Si nous déployons notre force d'innovation, notre créativité et notre disponibilité pour créer des réseaux intelligents de façon conséquente pour le développement de scénarios d'application à long terme et juridiquement sécurisés, l'Allemagne et beaucoup d'autres pays de l'Europe vont parvenir à sortir des sentiers battus dans le domaine de la sécurité.

C'est notamment sur le sujet de l'e-identité qu'il est nécessaire d'aller chercher au-delà du territoire national, car les besoins de la communauté internationale des utilisateurs sont identiques dans le monde entier. La garantie des plus hauts standards de sécurité et des identités sécurisées représente un défi global.

Contact

Björn Donath
Bundesdruckerei GmbH Technology – Innovations
http://www.bundesdruckerei.de

Téléphone : +49 (0) 302 598 3046
E-mail : bjoern.donath@bdr.de
Site Internet : http://www.sichere-identitaet.de

Cluster d'innovation Fraunhofer « Identité sécurisée - transparence et authenticité dans les mondes réel et numérique »

Prof. Dr.-Ing. Krüger, Directeur du cluster d'innovation de la société Fraunhofer „Identité sécurisée Berlin-Brandebourg"

*Le **Prof. Dr.-Ing. Jörg Krüger**, né en 1962, a fait des études de génie électronique à l'Université technique (TU) de Berlin. Entre 1992 et 1999, il a travaillé à l'Institut Fraunhofer pour le développement d'unités de production et de techniques de construction (IPK) dans le domaine des techniques de commande.*
Suite à l'obtention de son doctorat en 1998, le Prof. Krüger a fondé l'entreprise „reCognitec", une société de traitement d'images numériques à Kleinmachnow près de Berlin, où il a occupé la fonction de gérant associé.
Au 1er novembre 2003, le Prof. Krüger a ensuite pris la direction du département de technique d'automatisation industrielle à l'Institut des machines-outils et d'exploitation industrielle (IWF) à la TU Berlin. Cet emploi implique également la direction du département de technique d'automatisation à l'Institut Fraunhofer (IPK).

Comment puis-je prouver que mon moi est réellement moi ? Est-ce que ce produit est vraiment authentique ? L'émetteur du message est-il indiscutablement celui qu'il prétend être ? La confirmation sans équivoque de l'identité de personnes, d'objets, d'auteurs et d'émetteurs constitue, dans le monde réel comme dans le monde numérique, la base pour des relations sécurisées. En vue de la numérisation et de l'automatisation croissantes des activités, la question de l'authenticité des identités devient plus importante que jamais. Aujourd'hui, il existe différentes méthodes qui permettent de prouver l'identité. Outre les documents personnels, les signatures traditionnelles et électroniques, seront à l'avenir de plus en plus utilisées des cartes d'accès et de crédit ainsi que des labels et des filigranes. Cependant, tous ces systèmes ne sont pas pérennes – leurs champs d'applications sont restreints, ils ne sont pas suffisamment protégés contre la contrefaçon et ils sont généralement régis par les conditions d'utilisation et d'application mis à disposition par le service.

Les partenaires, membres du Cluster d'innovation Fraunhofer « Identité sécurisée », se sont fixés comme objectif de sécuriser les multiples relations réciproques qui existent entre les gens, les objets et les machines, tout en garantissant et en prouvant leur unicité.

Deux visions orientent le travail du Cluster d'innovation :

Vision Future ID-Card Systems

Les futures cartes d'identité identifieront leur propriétaire de façon incontestable et ne pourront pas être falsifiées. L'utilisateur de cette carte administrera lui-même ses données personnelles et ne mettra à disposition que les paramètres personnels nécessaires à la spécificité du champ d'utilisation de la carte. Le futur système d'identité, comme par exemple la carte d'identité électronique personnelle, permettra d'interconnecter les propriétaires et les objets qu'ils utilisent (véhicules, appareils médicaux) de façon flexible et mobile. Le service utilisé pourra s'adapter aux préférences et aux caractéristiques de l'utilisateur dans la mesure où ce dernier mettra librement à disposition les données liées à son identité pour les besoins correspondants. Les futurs documents personnels seront utilisés aussi bien sous forme physique que sous forme électronique. Ils permettront également l'accès à des services numériques. Afin que cette vision devienne réalité, le Cluster d'innovation « Identité sécurisée » développe de nouveaux systèmes de sécurité, matériaux et technologies avec lesquels les données seront générées, stockées, visualisées et authentifiées.

Vision Future ID-based Communication

L'émetteur et le récepteur d'une information seront identifiés sans la moindre ambiguïté – un prérequis essentiel pour une communication sécurisée. Les émetteurs anonymes et indésirables seront ainsi filtrés. Les voitures du futur reconnaîtront automatiquement les papiers du véhicule, les cartes électroniques seront utilisées à la place des clés de la voiture et les éléments du véhicule seront vérifiés par leur provenance. Afin de concrétiser ces idées, les partenaires du cluster développent entre autres dans l'industrie automobile des méthodes, des procédés et des technologies qui reconnaissent et utilisent les identités électroniques, comme par exemple pour la gestion de l'identité, la communication dans les réseaux de transport et la sécurité des produits.

Dans la région de Berlin-Brandebourg, un large savoir-faire s'est développé ces dernières années autour des

questions relatives à la sécurité de l'identité. Que ce soit sur le plan des autorités fédérales, des organismes publiques, des mondes de la recherche et politique - un grand nombre d'entreprises et d'initiatives ont été mises en place avec pour thème l'« Identité sécurisée », de sorte qu'à l'heure actuelle, dans presque aucune autre région, les connaissances scientifiques et les besoins économiques n'ont autant convergé. En effet, l'imprimerie fédérale (Bundesdruckerei), partenaire économique du cluster, est implantée dans la région. En conséquence, le cluster peut développer de manière ciblée des technologies, des matériaux et des procédés. C'est par un transfert technologique rapide de ces résultats de recherche vers des applications industrielles, que la région renforcera durablement son potentiel économique.

La participation de la société Sagem Orga du groupe français Safran montre que ces questions de sécurité de l'identité ont également une portée internationale. Sagem Orga est l'un des pionniers et leaders mondiaux de l'industrie de cartes à puce. Le portefeuille de Sagem Orga comprend des solutions de matériels informatiques, de logiciels, de conseil et de services autour de la carte, pour les domaines des télécommunications, de la santé, de l'identification et du système bancaire. Dans les télécommunications, les plus grands opérateurs de téléphonie mobile comptent parmi les clients de Sagem Orga. Cet expert de cartes à puce offre des solutions pour l'identification électronique et biométrique, les justificatifs électroniques, cartes de santé, permis de conduire et paiements par virement.

Dans ce contexte, Sagem Orga s'appuie fortement sur les technologies dans le domaine des documents de sécurité, comme l'intégration de puces, de matériaux spécialisés et de procédés de personnalisation optique. Pour tester les innovations technologiques concernées, les méthodes de traitement d'images prennent de plus en plus d'importance. Ceci implique aussi bien des procédés de vérification optique pour des matériaux que la recherche de méthodes de calcul qui sont appropriées aux plates-formes mobiles de traitement d'images.

Les Instituts Fraunhofer :

- Institut Fraunhofer pour le développement d'unités de production et de techniques de construction IPK (direction)
- Institut Fraunhofer de systèmes de communications publics FOKUS
- Institut Fraunhofer des techniques de communication, Institut Heinrich-Hertz HHI
- Institut Fraunhofer de recherche appliquée des polymères IAP
- Institut Fraunhofer de fiabilité et de microintégration IZM

Universités :

- Université libre de Berlin
- Université Humboldt de Berlin
- Université technique de Berlin
- Université de Potsdam
- TFH Wildau

Partenaires industriels :

- Imprimerie fédérale (Bundesdruckerei)
- Corrsys 3D Sensor AG
- Daimler AG
- IABG GmbH
- Nexus Technology GmbH
- Prisma GmbH
- Sagem Orga GmbH
- Telekom AG Laboratories Berlin
- TES Frontdesign GmbH
- Testing Technologies IST GmbH
- Wincor Nixdorf
- XETOS AG

Contact

Prof. Dr.-Ing. Jörg Krüger,
Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik IPK

Téléphone : +49 (0) 303 900 6183
E-mail : joerg.krueger@ipk.fraunhofer.de

Utilisation et administration des identités électroniques sécurisées

Petra Hoepner, Institut Fraunhofer des systèmes de communications publics (FOKUS), Berlin

Petra Hoepner *est chef de projet en R&D et chercheur à l'Institut Fraunhofer FOKUS. Dans la cadre de cette fonction, elle est responsable de la coordination et de la direction de projets nationaux et internationaux ainsi que de la planification et du développement technologiques dans les domaines de la sécurité et de l'e-gouvernement. Petra Hoepner travaille pour l'Institut Fraunhofer FOKUS depuis 1990. En 1980, elle a obtenu son diplôme d'informatique à l'Université technique de Berlin.*

Chacun dispose de plusieurs identités !

Depuis le début de l'industrialisation et avec la plus grande mobilité de l'homme qui s'en est suivi, il est devenu de plus en plus commun qu'une personne utilise les services d'un prestataire pour s'identifier. Il est maintenant nécessaire que cette personne prouve son identité. Depuis les dernières décennies, une quantité de documents personnels a été établie dans cette optique : un coup d'œil dans un porte-feuille dévoile des permis de conduire, des cartes de membres, de crédits et de banques et bien-sûr une pièce d'identité qui sert à justifier son identité, indépendamment du contexte.

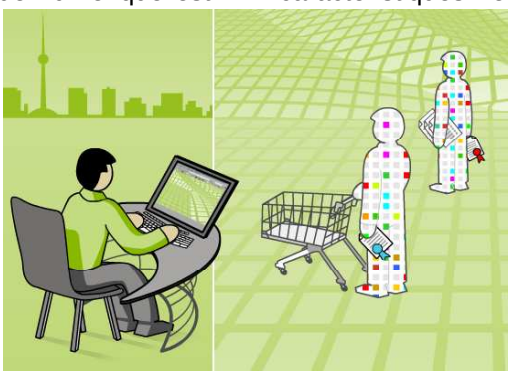
Ceci montre que dans le monde réel et au quotidien avec autrui, nous possédons plusieurs « identités » qui définissent notre « moi ».

Que ce soit en tant que citoyen, client ou voyageur, ces « identités » spécifiques nécessiteront de plus en plus d'être traitées électroniquement. Que ce soit pour les transactions bancaires en ligne, l'utilisation de services administratifs en ligne ou les achats sur Internet, ces procédés de traitement de l'identité étaient jusqu'à aujourd'hui gérés par les prestataires de services eux-mêmes. Et chaque prestataire dispose de son propre procédé.

Lors de l'inscription et de l'authentification, l'utilisateur des services électroniques est soumis aux exigences spécifiques de ces derniers. Un grand nombre de données personnelles de l'utilisateur sont demandées lors de l'enregistrement et ne sont pas forcement nécessaires pour la requête spécifique. L'authentification de l'utilisateur se poursuit dans la plupart des cas avec le couple identifiant/mot de passe. Ceci nous amène à disposer d'un nombre inconsidéré d'IDs différents, d'identifiants et de mots de passe en raison de la multitude d'identités possibles. Aujourd'hui, il existe donc différents certificats d'authentification qui sont utilisés pour l'e-commerce, l'e-business, l'e-gouvernance, l'e-health et autres applications.

Identités numériques et gestion d'identité

L'identité d'un individu dans le monde numérique est représentée par une « identité numérique ». Les identités numériques doivent être créées, gérées et résiliées. Dans son cycle de vie, l'identité numérique est utilisée pour différentes actions et activités remplissant divers objectifs qui ont pour point central commun l'identification de l'individu réel dans le monde virtuel.



Chaque identité se compose de caractéristiques et d'attributs particuliers tels que l'âge, le sexe, la formation professionnelle ou bien encore la durée d'un contrat et autres. Toutes ces caractéristiques ne sont pas pour autant nécessaires dans tous les contextes ou censées être dévoilées. Par exemple, l'employeur connaît la durée de contrat de ses employés, mais ne doit pas forcement être au courant d'informations personnelles telles que l'appartenance à une association. Jusqu'à présent l'enregistrement et l'utilisation des identités étaient faits sans concertation commune. Avec l'augmentation croissante des services en ligne, les identités doivent être gérées sur une même base. L'utilisateur doit pouvoir se mouvoir dans le monde

numérique, ce qui signifie qu'il doit fournir certaines

Une gestion sécurisée de l'identité est indispensable et nécessite une approche globale comprenant les fonctions suivantes :

- Identification et enregistrement des utilisateurs
- Authentification des utilisateurs, Single-Sign-On
- Autorisation des utilisateurs à des accès spécifiques
- Contrôle et validation de la légitimité de l'utilisation
- Gérance des identités des utilisateurs et des autorisations (gérer les cycles de vie, les sessions et le contexte de sécurité)

Dans le domaine de l'e-gouvernance/e-business, la notion de « sécurité » signifie le plus souvent la gestion de signatures électroniques ou l'authentification des acteurs (citoyens, business et administration) lors de l'utilisation des différents services. Par contre, la génération et l'administration par exemple des rôles, des droits, des pseudonymes, des mécanismes de protection des données, ainsi que

informations personnelles tout en restant ciblées.

leur interopérabilité, leur structure et leur réalisation technique, ne sont qu'en partie résolues.

L'interopérabilité entre les différentes approches et technologies dans le secteur de la gestion de l'identité devient de plus en plus importante. Elle comprend des aspects techniques, sémantiques et d'organisation.

En 2010, l'Allemagne disposera d'une pièce d'identité électronique avec une fonction eID comme base de la gestion d'identité sécurisée. Cette pièce d'identité permettra au citoyen de pouvoir s'authentifier en toute sécurité auprès des administrations et de l'industrie pour avoir recours à leurs services. Ceci est le fondement d'une identification et d'une authentification sécurisée qui repose sur les informations confirmées par l'Etat.

L'utilisation aisée et l'intégration des eIDs dans diverses applications ainsi que dans des infrastructures d'identité sont indispensables afin de remplir toutes les fonctions de la gestion de l'identité.

Les développements actuels, regroupés sous le titre de « gestion de l'identité centrée sur l'utilisateur », offrent des solutions potentielles.

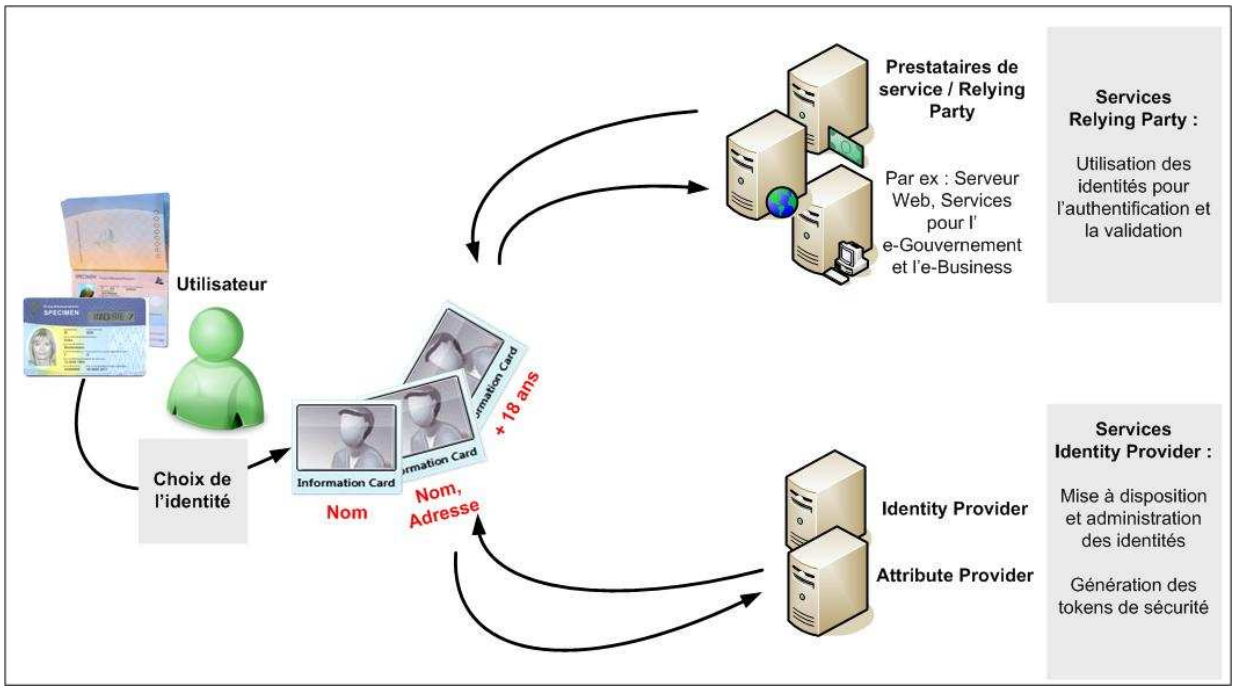
Gestion de l'identité centrée sur l'utilisateur

En ce qui concerne leurs données personnelles, les utilisateurs deviennent de plus en plus prudents en raison notamment de l'augmentation croissante des attaques informatiques (« phishing ») et des virus. Les services en ligne demandent des attributs d'identification, mais exposent rarement leur propre identité. Pour faire face à cette tendance, des relations de confiance appropriées et leurs mises en application techniques sont nécessaires. L'idée principale de cette gestion de l'identité centrée sur l'utilisateur consiste à donner à ce dernier le contrôle total de ses données personnelles et de leur transmission aux services concernés. En prenant l'exemple de l'utilisation des cartes de crédit, des cartes bancaires, des cartes de visites etc., un portefeuille électronique global contenant les « Information Cards (I-Cards) » sera mis à disposition de l'utilisateur.

De la même manière que des cartes classiques, les I-Cards sont représentées par des icônes rectangulaires contenant certaines informations d'identité, comme par exemple :

- l'instance émettrice,
- le nom de la carte, choisi soit par l'émetteur soit par l'utilisateur même
- un arrière plan d'image, choisi soit par l'émetteur ou soit par l'utilisateur même
- les valeurs des attributs de l'identité sur la carte, le plus souvent visibles pour l'utilisateur (par exemple le nom, l'adresse, l'e-mail)

L'objectif des I-Cards est de proposer à l'utilisateur une certaine quantité d'informations variables contenues dans celles-ci qui sont relatives à l'identité. Ainsi, la personne peut choisir d'utiliser celle qui lui convient le mieux suivant son besoin de protection vis-à-vis d'un service ou d'une ressource. Ce système relie donc une interface d'utilisateur graphique avec l'implémentation de la gestion de l'identité centrée sur l'utilisateur. Les composants et l'infrastructure d'identité pour l'utilisation des I-Cards sont représentés sur l'image suivante :



Le laboratoire Secure eIdentity

Le laboratoire Secure eIdentity a été crée afin de pouvoir traiter ces sujets de recherche et de développement liés à l'identité. Au sein de ce laboratoire coopèrent l'imprimerie fédérale, qui est une entreprise leader au niveau mondial dans le domaine des technologies de haute sécurité, l'Institut Fraunhofer FOKUS, un expert pour l'intégration des services dans des architectures orientées vers les services, ainsi que d'autres partenaires. Pour atteindre leurs objectifs concernant la protection des données et de la sécurité des identités numériques dans des processus et systèmes publics et commerciaux, ils y effectuent des recherches et s'occupent du transfert technologique.

Le laboratoire Secure eIdentity sert également de plate-forme et de vitrine pour la gestion de l'identité moderne. Il soutient aussi l'industrie et l'administration par la mise à disposition d'une infrastructure orientée vers les services et les procédés.

Au sein du projet « myID » géré par le Cluster d'innovation de l'Institut Fraunhofer « Identité Sécurisée », différents scénarios sont actuellement mis en place. Ils montrent l'intégration exemplaire des identités numériques (par exemple la carte d'identité électronique) dans des procédés infaillibles et dans la gestion de l'identité et la gestion d'accès ciblée vers les utilisateurs en offrant une haute protection des données.

Conclusion

Pour que les citoyens puissent décider eux-mêmes quelles informations personnelles ils souhaitent transmettre, à qui, quand, pour quel objectif et sur quel laps de temps, il est nécessaire de mettre à leur disposition des technologies appropriées. L'élargissement de la responsabilité personnelle et des droits de participation des citoyens nécessite des technologies soutenant et garantissant la protection des données.

Pour que les citoyens aient confiance dans les eIDs, ils doivent pouvoir décider eux-mêmes de transmettre ou non leurs données personnelles.

Contact

Petra Hoepner
Fraunhofer FOKUS, Berlin

Téléphone : +49 (0) 303 463 7185
E-mail : petra.hoepner@fokus.fraunhofer.de

Sécurité sur le long terme et qualité des documents électroniques officiels grâce à la famille primée de contrôleurs de cartes à puce « SLE 78 » d'Infineon

Dr Heiner Fuhrmann, Government Identification, Chip Card & Security, Infineon Technologies AG, Munich

Dr Heiner Fuhrmann *est ingénieur et docteur en jurisprudence. Depuis le milieu des années 90, il effectue des recherches dans le domaine de la communication sécurisée, de la justice en ligne et du commerce électronique. Dr Fuhrmann a travaillé pour des prestataires de services de certification et de procédures d'attribution électroniques dans le champ d'application de la loi sur la signature. Depuis 2004, il est employé chez Infineon dans le domaine des cartes à puce. Il y est responsable du secteur des produits de contrôleurs sécurisés pour des applications officielles, comme par exemple les passeports, les cartes nationales d'identité, les permis de conduire et les cartes d'assurance maladie.*

Les documents d'identité électroniques passent à l'offensive

Partout dans le monde, les documents conventionnels d'identité sont de plus en plus souvent remplacés par des versions électroniques. Cela concerne une multitude de documents : les passeports, les documents de séjour jusqu'aux cartes d'assurance maladie et sociale en passant par les permis de conduire. Les objectifs généraux du passage aux nouveaux documents sont l'intégration électronique d'un système de contrôle continu des documents ainsi que l'augmentation de la sécurité contre les malveillances. Il est également nécessaire que les composants électroniques conservent une durée de vie égale à celle des documents classiques.

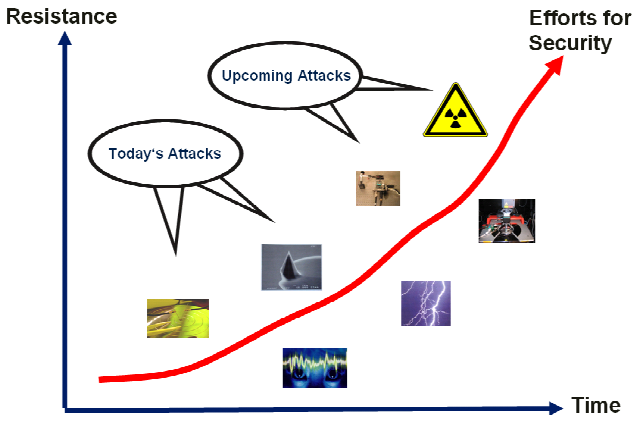
Les fonctions électroniques intégrées dans les documents d'identité sont gérées par des contrôleurs de sécurité spécifiques, similaires à ceux utilisés par exemple pour les cartes bancaires. Les applications des documents d'identité électroniques présentent de grands défis auxquels doit répondre la prochaine génération des contrôleurs.

Exigences relatives à la sécurité et à la durée de vie

Les documents officiels doivent fournir des informations fiables sur l'identité et sur les autorisations qui leur sont liées. Ils sont depuis toujours sécurisés contre les malveillances par des moyens techniques coûteux – dans la plupart des cas par des techniques d'impression coûteuses. Grâce aux fonctions électroniques, la sécurité de ces documents devrait être encore plus augmentée. C'est pourquoi les contrôleurs doivent satisfaire aux exigences élevées des institutions publiques. En tant que composants électroniques, les contrôleurs de cartes à puce suivent d'autres règles que les techniques d'impression traditionnelles utilisées pour la fabrication des documents. Ce sont des systèmes de grande complexité dont la sécurité ne peut être efficacement jugée que par des experts certifiés. Les contrôleurs de cartes à puce sont depuis longtemps utilisés pour des transactions électroniques hautement sécurisées. Pour cette catégorie de produits, la recherche et l'industrie ont créé une méthodologie très pointue pour l'évaluation neutre et objective de la sécurité sous forme de procédés de certification. Sous contrôle de l'Etat, les produits de sécurité sont examinés dans les moindres détails par ces mécanismes dans des laboratoires spécialisés et l'efficacité de leurs défenses contre des attaques potentielles est évaluée. Des certificats de sécurité présentant le critère « Common Criteria » d'un niveau CC EAL 5+ (high) sont exigés pour les contrôleurs destinés aux documents officiels.

A l'aide d'un certificat de sécurité, les contrôleurs de cartes à puce peuvent attester de leur état actuel au moment du contrôle.

Cependant, la nature des attaques évolue et peut forcer les fabricants des contrôleurs de cartes à puce ainsi que les concepteurs des logiciels correspondants, à des adaptations coûteuses de leurs produits.



Graphique 1 : Efforts fournis pour des mesures de défense conventionnelles

Concept de sécurité efficace à long terme

Des contrôleurs de cartes à puce de haute qualité et efficaces à long terme peuvent casser cette spirale d'efforts et établir une base solide pour les documents sécurisés et pour que leurs services associés puissent être garantis sans dysfonctionnement plus de 10 ans. Ceci n'est possible que si les attaques sont combattues à la racine et si leur développement futur est pris en compte. Ce mécanisme est expliqué dans la suite avec l'exemple des attaques par erreur :

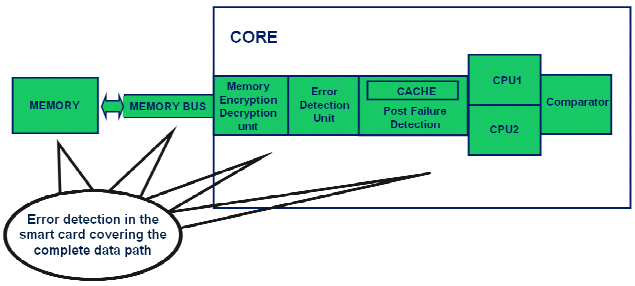
Les *attaques par erreur* (aussi attaques semi-invasives) sont un type d'attaques largement répandu contre lequel les contrôleurs de cartes à puce doivent être préparés. Ces attaques visent à perturber le fonctionnement normal de la puce en influant de l'extérieur. Elles provoquent ainsi un dérèglement du programme ou l'apparition d'états irréguliers dans la puce qui contournent la fonction de protection du programme. Afin de réaliser un dérèglement ciblé, il est possible d'utiliser différents effets physiques, comme par exemple les rayonnements laser, thermique, radioactif, les impulsions électriques et les variations spécifiques de fréquence du signal.

Les mesures classiques contre ces actions extérieures malveillantes reposent essentiellement sur des réseaux denses de capteurs de sécurité qui surveillent si une influence potentiellement malveillante agit sur le contrôleur. Cette manière de procéder nécessite des améliorations en continu : parallèlement à la miniaturisation des attaques, les réseaux de capteurs doivent être de plus en plus dense. De nouvelles attaques physiques (par exemple le rayonnement alpha à la place du rayonnement laser) remettent même en question le principe d'action des capteurs.

Au lieu de détecter les mécanismes physiques impliqués lors d'attaques, il est aussi possible de surveiller les données à protéger contre des changements non-autorisés. Si l'on réussit à reconnaître une portion d'information qui a été modifiée de façon non-autorisée, les conséquences des attaques par erreur sont détectées par n'importe quels canaux d'attaque.

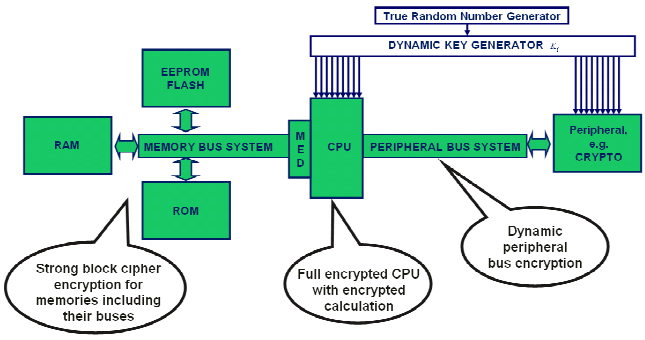
Infineon *Integrity Guard*

Infineon a suivi cette méthode de détection avec sa famille de contrôleurs « SLE 78 » basée sur le concept de sécurité primé *Integrity Guard.* Sur toute la puce, chaque bit est surveillé par divers mécanismes afin de détecter s'il a subi une modification non autorisée. Toutes les mémoires, les bus de données et aussi les unités de calcul (CPU) sont donc contrôlés. Par exemple, des opérations de calcul sont ainsi réalisées séparément sur deux unités de calcul. Les résultats sont ensuite comparés afin de s'assurer qu'aucune manipulation n'a été faite.



Graphique 2 : Détection globale des erreurs par l'Integrity Guard

Le concept de sécurité *Integrity Guard* de la famille de contrôleurs « SLE 78 » comprend une multitude de mesures adaptées contre les attaques actuelles et futures, comprenant un cryptage complet de toute la voie de transmission des données, assurant ainsi qu'à aucune position, les données soient disponibles en texte clair. Avec sa famille « SLE 78 », Infineon a poussé ce principe à l'extrême et crypte, outre les contenus de mémoire, le cache et les bus de données, même les calculs du processeur.



Graphique 3 : Cryptage complet par l'Integrity Guard

Dans sa globalité, l'*Integrity Guard* atteint un niveau de sécurité sur le long terme qui n'a jamais été réalisé et offre une plate-forme de sécurité idéale pour des documents d'identité électroniques fiables.

Efficacité énergétique et qualité

Les documents d'identité électroniques ne sont pas seulement déterminés par leur sécurité. Ils doivent en plus remplir leurs fonctions sans défaut pour une durée supérieure à 10 ans, et ceci indépendamment de l'environnement et de manière à assurer des accès électroniques rapides et aisés pour tous les utilisateurs.

Aujourd'hui, un grand nombre de documents d'identité électroniques est équipé d'interfaces sans fil. La communication s'effectue ici en approchant le document le long d'un appareil spécifique grâce à un champ électromagnétique sans contact électrique. D'une part, ce mécanisme permet d'interagir facilement sans que les documents ne soient

introduits dans l'appareil de lecture. D'autres part, il évite les contacts de surface qui limitent la durée de vie du document.

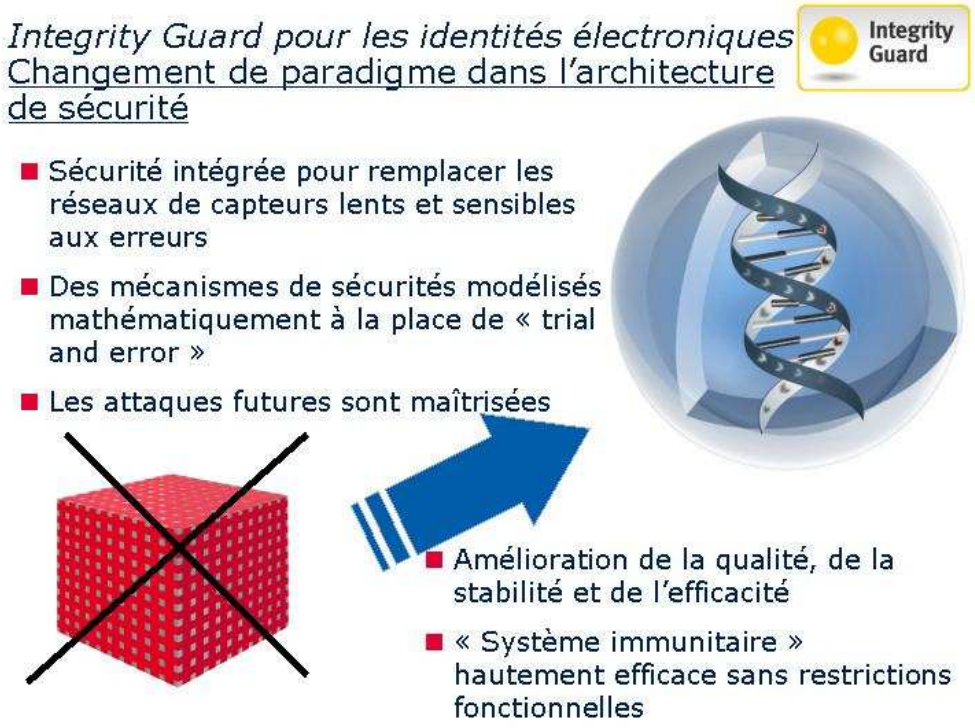
Lors des connexions sans fil, les contrôleurs intégrés dans les documents d'identité doivent être alimentés en énergie à travers le champ électromagnétique créé par les appareils de lecture. De plus, ils doivent garantir une communication fiable malgré les influences perturbatrices lors de l'utilisation. Puisque les exigences élevées relatives à la sécurité (décrites ci-dessus) exigent des opérations de calcul complexes dans les contrôleurs, une optimisation constante de l'efficacité énergétique est indispensable.

Toute l'architecture de la famille de contrôleurs « SLE 78 » a été conçue de fond en comble dans cette perspective. Une douzaine de mécanismes spécifiques veillent à ce que seuls les composants nécessaires au fonctionnement du système soient alimentés en énergie. Ils utilisent chaque fraction d'énergie disponible dans les champs électromagnétiques variables et permettant ainsi une communication stable et sécurisée à travers l'interface sans fil. Les propriétés fondamentales du concept de sécurité *Integrity Guard* assurent la stabilité du système dans sa globalité, et offre avec la famille « SLE 78 » une fiabilité et une robustesse de son fonctionnement jamais atteintes.

Changement de paradigme vers un système immunitaire robuste

Avec le concept d'*Integrity Guard* intégré à la famille de contrôleurs « SLE 78 », Infineon est parvenu à créer un changement de paradigme dans le domaine du hardware sécurisé. Les anciens contrôleurs de cartes à puce, tels des chevaliers moyenâgeux, devaient être régulièrement équipés de nouvelles armures coûteuses (sous forme de capteurs). Ceux-ci étaient pour le système une source potentielle d'erreurs nécessitant une maintenance lourde et ils provoquaient un ralentissement du système. L'*Integrity Guard* remplace cette armure par une sorte de système immunitaire robuste qui reconnaît les erreurs à l'intérieur du système et s'y opposent. Telles des cellules somatiques naturelles, ce système est capable de réagir de façon flexible aux nouvelles menaces, tout en évitant les effets secondaires non-souhaités qui handicapent le système lors de son activité normale. Ainsi, les exigences élevées des documents officiels telles que la durée de vie, la qualité et le fonctionnement sans fil ou l'efficacité énergétique peuvent être entièrement satisfaites, sans oublier les besoins en sécurité très prononcés.

Fin 2008, Infineon a reçu le Sesame Award pour le hardware le plus innovant dans l'industrie des cartes à puce grâce à sa famille de contrôleurs « SLE 78 » équipée d'*Integrity Guard.* Infineon a écrit ainsi un nouveau chapitre pour l'histoire commençante des identités électroniques sécurisées.



Contact

Dr. Heiner Fuhrmann
Infineon Technologies AG
Chip Card & Security

Téléphone : +49 (0) 892 342 3037
E-mail : heiner.fuhrmann@infineon.com
Site Internet : http://www.infineon.com/security

Technologies pour l'identité sécurisée – Technologies d'affichage pour les cartes multifonctions

Armin Wedel, Directeur du département des systèmes polymères fonctionnels à l'Institut Fraunhofer de recherche appliquée des polymères, Potsdam

*Né en 1960, le **Dr. Armin Wedel** a étudié la physique à l'Université de Rostock. Depuis 1992, il travaille en tant que scientifique et directeur de projets à l'Institut Fraunhofer de recherche appliquée des polymères à Potsdam. Son domaine de recherche concerne le développement de technologies pour la fabrication d'OLEDs et de cellules photovoltaïques organiques, ainsi que le développement d'électrets et de polymères ayant des propriétés piézo- et pyroélectriques.*

La protection des identités couplée à un mécanisme fiable d'identification et d'authentification de personnes, de biens et de propriété intellectuelle, est la condition de base essentielle pour la capacité d'action d'une société à l'échelle globale connectée. Les nouvelles technologies pour une identité sécurisée permettent de gagner clairement en sécurité à travers le développement de produits et d'applications innovants. Autour de ce sujet sont réunis au sein d'un même cluster cinq instituts Fraunhofer, cinq universités et 12 entreprises dans la région de Berlin-Brandebourg.

Puisque la capitale régionale Berlin-Brandebourg représente le siège du Parlement et du gouvernement fédéraux, des ambassades, des autorités fédérales et des organes constitutionnels, nombre d'organismes, d'institutions et d'infrastructures, ainsi que les processus impliqués dans les affaires et l'administration doivent satisfaire, dans cette région, aux exigences de sécurité. La politique s'en est également rendu compte et soutient financièrement des initiatives de recherche et de développement, notamment dans le domaine de la sécurité.

La présence d'un environnement scientifique très performant est une condition essentielle pour le développement positif de l'industrie de la sécurité au niveau local. En ce qui concerne le développement, la production et l'application de produits et de solutions dans le domaine de la sécurité, la capitale régionale fait partie des sites les plus importants et les plus performants en Allemagne et en Europe. La proximité géographique d'un même contenu thématique, les courtes distances entre la recherche, le développement, l'application et la demande, ainsi que les coopérations et les partenariats public/privé réussis, ont permis de créer une infrastructure qui n'a pas son égal en Allemagne.

Le paysage économique, avec ses produits et/ou ses services dans le secteur de la sécurité, est très diversifié et bien positionné dans la région de Berlin-Brandebourg. Plus de 260 entreprises représentant environ 10.000 employés travaillent dans le domaine de la sécurité et réalisent un chiffre d'affaires annuel de 1,3 milliard d'euros (état en 2006). Afin de partager un échange d'expériences et de savoir dans les domaines clés de la sécurité civile, un certain nombre de ces entreprises se sont organisées en réseau (SeSamBB, SecTec, etc).

Les domaines phares du secteur de la sécurité dans le Land de Berlin-Brandebourg reposent sur le développement de solutions pour la protection de l'identité de personnes, de produits, de propriété intellectuelle et de communication. A cette fin, des mécanismes, des matériaux et des technologies innovants sont élaborés.

L'imprimerie fédérale de Berlin compte parmi les acteurs principaux dans ces domaines clés. Depuis quelques années, elle entretient une coopération intensive avec différents instituts Fraunhofer dans le Land. Le succès de cette coopération est visible au travers des trois laboratoires communs en service ainsi que des deux prochains en phase de planification. Les Security Labs sont utilisés comme centres d'application et de prestation de services au sein des instituts Fraunhofer. Ils doivent multiplier les résultats d'une recherche innovante dans la sécurité et créer des synergies dans les domaines apparentés. A l'avenir, ces laboratoires pourront servir de comités de certification pour certaines technologies de sécurité.

Pour l'imprimerie fédérale, les méthodes et mécanismes de gestion de l'identité constituent la technologie d'avenir des années futures. C'est pourquoi l'un des objectifs de cette entreprise consiste à faire de la région Berlin-Brandebourg une plate-forme pour les technologies de sécurité civile et à soutenir son importance en tant que centre de compétences européen. Les points importants pour y arriver sont l'autoinitiative de tous les partenaires impliqués et la forte volonté de redéfinir et de réorienter les thèmes d'avenir, tout ceci en coopération avec la société Fraunhofer et avec d'autres institutions et entreprises au sein du cluster d'innovation « Identité sécurisée ». Dans ce contexte, l'imprimerie fédérale, en coopération avec l'Université

Libre de Berlin, a déjà créé en 2007 une chaire de professeur « Secure Identity ».

L'objectif des travaux communs de recherche et de développement est de pouvoir offrir des technologies, des mécanismes et des produits qui permettent de justifier sans ambiguïté l'identité de personnes, d'objets et de la propriété intellectuelle, tant dans le monde réel que dans le monde virtuel. Dans ce but, l'Institut Fraunhofer de la recherche appliquée des polymères (Fraunhofer IAP) à Potsdam développe des éléments de sécurité innovants. Grâce à leur intégration dans des documents (par exemple des cartes d'identité), il est possible d'utiliser de nouvelles fonctionnalités dans une carte à puce (Smartcard) à base de polymères. A cette fin, des symboles lumineux flexibles à base de diodes électroluminescentes organiques (OLEDs) sont développés. Ils sont fabriqués grâce à des technologies spécifiques et permettent une auto-identification du document.

Les technologies de base pour la production d'OLEDs sont très largement connues à l'Institut Fraunhofer IAP. Cependant, la structuration géométrique des OLEDs, l'augmentation de leur efficacité, de leur luminosité et la prolongation de leur durée de vie représentent toujours des défis dans l'utilisation d'une Smartcard.

La structuration est réalisée au cours d'étapes de photolithographie pour la superposition des couches ou par la séparation structurée des matériaux en combinaison avec des électrodes structurées.

Actuellement, différents procédés d'impression pour la production d'OLEDs à base de polymères sont testés dans le monde entier ou ont déjà été intégrés dans des dispositifs-pilotes et de fabrication.

Alors que les procédés, comme l'impression sérigraphique et de gravure, sont au stade de développement pour cette application, le développement à l'Institut Fraunhofer IAP dans le domaine des imprimantes à jet d'encre est déjà plus avancé.

Photo 1 : Clavier OLED

Les OLEDs sont minces, très légères, économiques en énergie et lors de leur production. Elles présentent de plus un plus grand angle de vision, une image plus nette et peuvent être imprimées. La combinaison d'OLEDs avec des éléments électroniques polymères permet de réaliser des écrans complètement flexibles. Les OLEDs peuvent également être combinées avec d'autres éléments fonctionnels comme des claviers souples. Ces nouveaux claviers OLED sont composés de deux couches superposées – un niveau intégrant l'élément OLED mince et l'autre réalisant la fonction de clavier. Ces nouvelles applications demandent des étapes technologiques innovantes, comme par exemple le développement de schémas pour l'affichage ou pour les surfaces lumineuses, la structuration de l'empilement des couches et l'encapsulation efficace des éléments.

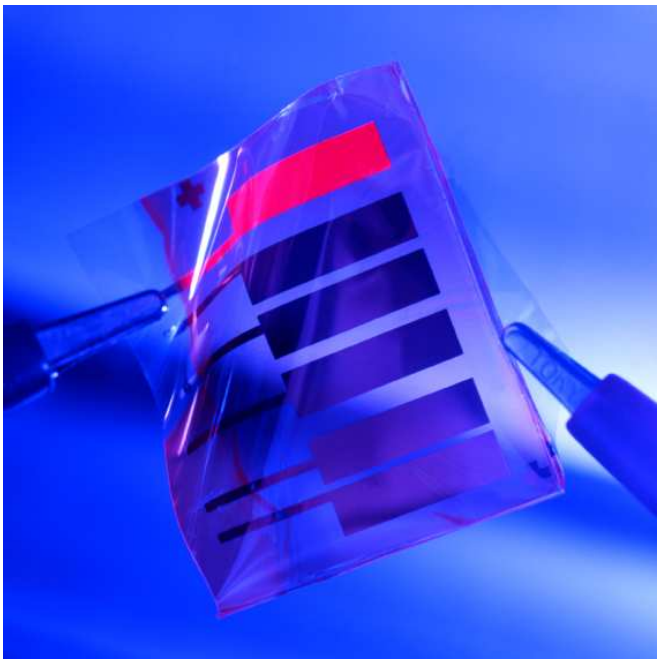


Photo 2 : Feuille d'affichage OLED

Le transistor organique d'effet de champ (OFET) est un composant de base de l'électronique. Les OFETs sont des composants qui utilisent un matériau organique comme semiconducteur. Parmi les circuits électroniques simples, on compte les circuits logiques, les oscillateurs et les circuits redresseurs. Au sein de ses activités de développement, l'Institut Fraunhofer IAP travaille sur des systèmes de matériaux organiques agencés spécifiquement, qui se composent d'un semiconducteur organique et d'un diélectrique polymère. D'autres exigences sont la maniabilité dans l'air des supports souples et l'augmentation de leur performance. Pour remplir ces exigences, il est absolument nécessaire de consacrer une grande partie des travaux de développement dans la corrélation entre les semiconducteurs organiques et les diélectriques organiques. Le semiconducteur organique et le diélectrique organique doivent ainsi être considérés et développés ensemble

dans un système. Grâce au développement et à la mise en œuvre à l'Institut Fraunhofer IAP de nouveaux concepts de synthèse de polymères semiconducteurs conjugués, des OFETS présentant une mobilité de porteurs de charge élevée ont pu être réalisés.

Les couleurs peuvent également être utilisées comme élément de sécurité. Par expérience, la couleur d'un matériau est indépendante de sa température. Seuls quelques matériaux, qualifiés de thermochromes, montrent un changement continu ou brutal de couleur à la suite d'un changement de température. Ces matériaux sont développés à l'Institut Fraunhofer IAP. Ces changements peuvent aussi bien être réversibles qu'irréversibles et ouvrent également la voie à de nouvelles applications dans les techniques de sécurité.

Grâce aux matériaux polymères thermochromes, les intensités de couleur se laissent aussi bien commuter que contrôler de manière ciblées par la température. Ainsi, les effets de commutation thermochromes peuvent avoir lieu entre 2 couleurs (bleu-rouge ou jaune-noir) mais également de façon graduelle (sans couleur-rouge-jaune-vert) grâce à un profil de température prédéterminé.

Contact

Dr. Armin Wedel
Fraunhofer Institut für Angewandte Polymerforschung (IAP)

Téléphone : +49 (0) 331 568 3910
Fax : +49 (0) 331 568 1910
E-mail : armin.wedel@iap.fraunhofer.de
Site Internet : http://www.sichere-identitaet.de

Signatures numériques à l'épreuve du temps

Johannes Buchmann et Erik Dahmen. Université Technique de Darmstadt, Département Informatique, Informatique théorique - Cryptographie et calcul formel.

Johannes Buchmann *est professeur d'informatique et de mathématiques à l'Université technique de Darmstadt (TU Darmstadt) et co-auteur du Journal of Cryptology. En 1993, il a reçu le prix Leibniz de l'Agence de moyens pour la recherche allemande (DFG), le prix allemand le plus renommé pour les scientifiques. En 2006, il a été récompensé par le prix Karl-Heinz-Beckurts pour ses recherches sur les signatures numériques sécurisées à l'épreuve du temps ainsi que sur leurs applications.*

Erik Dahmen *travaille comme scientifique dans le groupe de recherche du Prof. Dr Buchmann. En 2006, il est diplômé en mathématiques à la TU Darmstadt. Erik Dahmen est auteur de plusieurs publications sur les signatures numériques à l'épreuve du temps.*
En 2008, le Prof. Dr Johannes Buchmann et Erik Dahmen ont reçu la deuxième distinction du prix allemand de sécurité des TIC pour leurs recherches sur les signatures numériques.

Les signatures numériques sont un outil essentiel pour la protection des infrastructures actuelles des TIC. Les signatures numériques sont des mécanismes cryptographiques qui permettent de prouver l'authenticité et l'intégrité des données électroniques. En contrôlant l'authenticité, la personne recevant des données peut vérifier si l'expéditeur est réellement la personne qu'elle prétend être. Dans ce contexte, les signatures numériques sont comparables aux signatures manuscrites. En contrôlant l'intégrité des données, le récepteur peut vérifier si ces dernières ont été modifiées lors de l'envoi de l'expéditeur au récepteur.

Parmi les grands champs d'application, les mises à jours de logiciels (updates) contiennent des signatures numériques qui visent à combler les lacunes de sécurité, régulièrement repérées dans les applications logicielles et les systèmes d'exploitation. Par exemple, les mises à jour automatiques pour Microsoft Windows XP sont signées numériquement. Ainsi, le système d'exploitation peut vérifier si la mise à jour a réellement été émise par Microsoft et si, lors de son transfert, elle a pu être modifiée, comme par exemple dans le cas d'introduction de virus. Les signatures numériques sont également utilisées dans les smartphones, tels que l'iPhone d'Apple. Pour qu'une application puisse être utilisée sur un iPhone, celle-ci doit être signée de façon numérique par Apple. Ainsi, seules les applications approuvées par Apple peuvent être installées. De cette manière, l'utilisateur ne télécharge pas par erreur un logiciel malveillant sur son téléphone. Le passeport électronique allemand – l'ePass – est un autre exemple d'application des signatures numériques. Dans ce cas, les signatures numériques sont non seulement utilisées pour l'authentification du passeport, mais également pour la vérification de son appareil de lecture.

Les mécanismes impliqués dans la signature numérique utilisent une clé double se composant d'une clé privée et d'une clé publique. La clé privée est utilisée pour créer les signatures numériques. Elle est exclusivement accessible à l'émetteur, c'est-à-dire au signataire. La clé publique, quant à elle, sert à la vérification des signatures numériques. Elle est accessible aux plate-formes spécialisées pour tout contrôle potentiel de la signature. Une des propriétés importantes de la signature numérique est une déduction très peu probable de la clé privée à partir de la clé publique. C'est pour cette raison que la clé publique peut être mise à la disposition de tout le monde.

Les premiers mécanismes de signature numérique sont apparus à la fin des années 70 jusqu'au milieu des années 80. A l'époque, les mécanismes qui s'étaient imposés, reposaient sur l'insolubilité des problèmes de calcul issus de la théorie des nombres. Le mécanisme de signature Merkle, proposé par Ralph Merkle, avait été ignoré bien qu'il ne présentait que peu de paramètres de sécurité. Les mécanismes basés sur des problèmes liés à la théorie des nombres s'étaient avérés plus efficaces. Aujourd'hui, ces mécanismes font référence et sont en réalité les seuls mécanismes de signature numérique qui soient vraiment mis en pratique.

Au cours des années, ces mécanismes de signature se basant sur des problèmes liés à la théorie des nombres ont été fréquemment mis à mal. Parmi les attaques les plus dangereuses sont comptées celles que peuvent potentiellement provoquer les ordinateurs quantiques. Dès qu'il sera possible de construire des ordinateurs quantiques de grande taille, tous les mécanismes de signature utilisés jusqu'à aujourd'hui deviendront non sécurisés. Cependant, les ordinateurs quantiques ne représentent pas le seul danger. D'autres idées innovantes, grâce auxquelles les problèmes de calcul liés à la théorie des nombres deviennent résolubles, peuvent apparaître à tout moment. Ainsi, la sécurité des mécanismes courants de signature, et toutes les infrastructures TIC installées dans le monde entier, reposent sur des bases fragiles. Vu notre dépendance à ces infrastructures, ce problème présente un enjeu très

important. Des alternatives sécurisées à long terme et des applications pratiques sont nécessaires de toute urgence.

En ce qui concerne la sécurité sur le long terme, le mécanisme impliqué dans la signature Merkle proposait déjà, au début des années 70, une telle alternative. Le mécanisme Merkle ne dispose justement que de peu de paramètres de sécurité : en effet, seule une fonction de hachage cryptographique résistante aux collisions est nécessaire. Cette condition est d'ailleurs minimale, car tout mécanisme de signature utilise une fonction hachage. Contrairement aux problèmes de calcul liés à la théorie des nombres insolubles, il existe un grand nombre de fonctions de hachage cryptographiques. Chaque nouvelle fonction de hachage mène à une nouvelle variante du mécanisme de signature Merkle. Si la fiabilité d'une variante est remise en cause, la fonction de hachage utilisée peut être remplacée par une autre plus sécurisée et rendre ainsi le mécanisme de signature de nouveau sûr. D'autre part, la sécurité des fonctions de hachage n'est menacée que de façon insignifiante par les ordinateurs quantiques. La version originale du mécanisme de signature Merkle représente donc une base solide pour créer un mécanisme de signature sécurisé à long terme.

Ces dernières années, nombre de scientifiques ont travaillé sur les grands problèmes d'efficacité liés au mécanisme de signature Merkle et ils ont réussi à en améliorer les performances. La discipline de Prof. Dr. Buchmann y a d'ailleurs fortement contribué. Ces améliorations rendent le mécanisme de signature Merkle aussi compétitif que ceux utilisés aujourd'hui. Grâce à une combinaison des différentes améliorations, le mécanisme de signature Merkle est devenu le *Generalized Merkle Signature Scheme* (GMSS). Le schéma GMSS représente donc aujourd'hui un mécanisme de signature sécurisé sur le long terme et ouvre à différentes application pratiques.

Le paragraphe suivant décrit le mécanisme de signature Merkle, esquisse les améliorations qui le rendent plus applicable et qui l'ont mené finalement au schéma GMSS. Une description détaillée se trouve dans le livre Post-Quantum Cryptography[1].

Le mécanisme de signature Merkle et ses améliorations

Le mécanisme initial de signature Merkle (MSS) demande une fonction de hachage, un mécanisme de signature unique et un nombre naturel $h \geq 2$. Le nombre h détermine le nombre de signatures vérifiables avec la clé MSS publique, soit 2^h.

[1] Bernstein, Buchmann, Dahmen (Eds.). *Post-Quantum Cryptography*, Springer, 2009, ISBN: 978-3-540-88701-0.

Afin de pouvoir générer les clés doubles (composées d'une clé de signature et d'une clé de vérification), le signataire produit 2^h . d'une signature unique. Il construit ainsi un arbre de hachage binaire, aussi appelé arbre de Merkle, d'une hauteur de h nœuds. Les feuilles de l'arbre de Merkle constituent les valeurs hachées de la clé de vérification. Chaque nœud interne représente la valeur de hachage provenant de la liaison avec ses deux enfants. La clé MSS publique constitue la racine de l'arbre de hachage et la clé privée représente la suite des clés de signature unique, voir l'illustration 1.

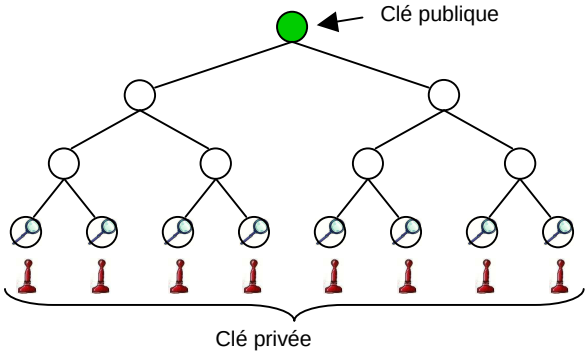


Illustration 1 : Création des paires de clés selon Merkle.

Lors de la signature, les clés de signature sont utilisées l'une à la suite de l'autre. La signature d'un document *d*, produite avec l'*i*ème clé de signature, se compose de la signature unique liée au document, de l'*i*ème clé de vérification, de l'index *i* et d'un chemin d'authentification qui permet à l'appareil de contrôle de vérifier la validité de l'*i*ème clé de vérification en relation avec la clé publique. Le chemin d'authentification pour l'*i*ème clé de vérification est composée des frères et sœurs de tous les nœuds se trouvant sur le chemin de l'*i*ème feuille de Merkle en remontant jusqu'à la racine de l'arbre, voir l'illustration 2.

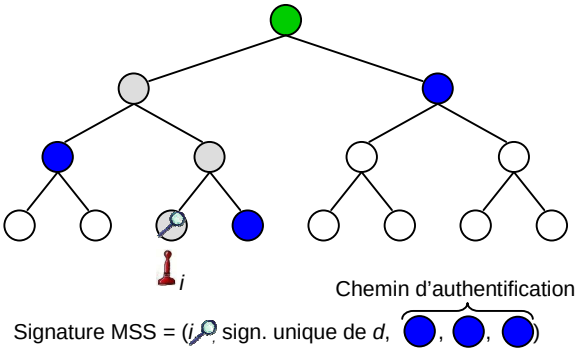


Illustration 2 : Production de signature de Merkle.

Afin de vérifier une signature Merkle, le contrôleur vérifie d'abord la validité de la signature liée au document au moyen de l'*i*ème clé de vérification contenue dans la signature. Il contrôle ensuite l'authenticité de la clé de vérification grâce au chemin d'authentification : le contrôleur reconstruit le chemin de l'*i*ème feuille jusqu'à la racine de l'arbre de Merkle et

compare la valeur de la racine calculée avec celle de la clé publique du signataire. La signature est valable si la racine calculée correspond à la clé publique du signataire et si la vérification de la signature unique est validée.

Nous allons maintenant aborder les limitations du schéma MSS initial et décrire les améliorations grâce auxquelles le schéma GMSS a pu être élaboré.

Dans le mécanisme initial de Merkle, la clé privée est une combinaison de toutes les 2^h clés de signature. Dans la pratique, un tel nombre de clés ne peut pas être mémorisé. C'est pourquoi les clés de signature sont désormais produites par un pseudo-générateur de nombres aléatoires. Ensuite, il suffit d'utiliser le seed du pseudo-générateur de nombres aléatoires comme clé privée. La longueur du seed correspond à la longueur de sortie de la fonction de hachage utilisée, par exemple 160 bits pour l'algorithme de hachage sécurisé (SHA1). Ce mécanisme réduit fortement l'espace mémoire nécessaire pour la clé privée. De plus, le temps de calcul n'augmente que très peu, puisque les pseudo-générateurs de nombres aléatoires utilisés sont très efficaces.

Pour la production d'une signature, le calcul des chemins d'authentification est de loin la partie qui exige le plus de temps. Plusieurs ressources à ce sujet sont disponibles dans la littérature. Cependant, la plupart des approches ont des durées d'exécution très variables. Pour certaines feuilles, le calcul du chemin d'authentification est très rapide et pour d'autres, il prend beaucoup de temps. Récemment, un algorithme de calcul des chemins d'authentification a été présenté. Il garantit des durées d'exécution stables et nécessite pour cela une durée moyenne d'exécution équivalente à celle de l'algorithme le plus performant connu jusqu'ici. Pour des arbres d'une taille de 20 noeuds, la durée d'exécution du cas le plus défavorable est réduite d'environ 15%.

Pour calculer la clé publique, l'arbre de Merkle doit être construit entièrement. Cela nécessite le calcul de $2^{h+1} - 1$ nœuds. Pour des arbres dont la taille dépasse les 20 noeuds, cette solution n'est pas envisageable. Et pourtant, pour de nombreuses applications, il est nécessaire de pouvoir produire plus de $2^{20} = 1.048.576$ signatures avec une seule clé double. De telles applications se trouvent dans les serveurs de banque en ligne par exemple. Les gens doivent s'authentifier pour chaque activité de banque en ligne et créer une signature à cette fin. Le mécanisme de Tree-Chaining résout ce problème. A travers ce mécanisme l'arbre entier de Merkle est découpé en plusieurs arbres partiels plus petits qui sont calculés l'un après l'autre et séparément de façon indépendante. Si on découpe un arbre de Merkle d'une hauteur de 40 nœuds en arbres partiels d'une hauteur de 20 noeuds, seulement $2 \cdot (2^{21} - 1)$ nœuds seront nécessaires (au lieu des $2^{41} - 1$ nœuds) afin de calculer la clé publique. Grâce au mécanisme de Tree-Chaining, il est donc possible de construire efficacement plus de 2^{20} signatures avec une clé double.

Le mécanisme de Tree-Chaining présente cependant un inconvénient : en plus de la signature liée au message, ce mécanisme doit également transmettre les signatures liées aux racines de certains arbres partiels. Cela entraîne des signatures de plus grande taille. Ce problème est résolu grâce au calcul distribué des signatures. L'idée est de distribuer le calcul des différentes signatures des racines des arbres partiels sur plusieurs étapes de signature. Ainsi, la génération d'une signature en devient extrêmement efficace. Au moyen du mécanisme de signature unique Winternitz, cet avantage temporel est transformé en avantage de mémoire utilisée. La combinaison du calcul distribué de la signature et du mécanisme de signature Winternitz permet de réduire considérablement la taille des signatures des racines des arbres partiels et de les calculer malgré tout de façon efficace.

Le tableau 1 montre les temps de calcul et la mémoire utilisée pour une implémentation Java d'un schéma GMSS, c'est-à-dire un schéma MSS comportant toutes les améliorations décrites ci-dessus. L'algorithme de hachage sécurisé (SHA1) a été utilisé en tant que fonction de hachage. Les temps de calcul ont été mesurés à l'aide d'un processeur AMD Athlon 64 X2 5200+. Le tableau montre les temps et la mémoire nécessaires pour différents nombres de signatures par clé publique et un ensemble de deux paramètres visant à équilibrer différemment la mémoire et le temps de calcul.

Nombre de signatures	Signature	Signer	Vérification
2^{20}	1.268 Bytes	12,8 ms	11,5 ms
	1.768 Bytes	2,9 ms	2,1 ms
2^{30}	1.468 Bytes	25,0 ms	10,9 ms
	1.968 Bytes	5,6 ms	2,3 ms
2^{40}	2.072 Bytes	17,8 ms	17,2 ms
	2.672 Bytes	4,0 ms	3,8 ms

Tableau 1 : Temps et mémoire du schéma GMSS

Ce tableau confirme que le schéma GMSS est un mécanisme sécurisé de signature pratique et sécurisée sur le long terme. Son avenir dépend maintenant de la standardisation et des applications qu'on lui trouvera.

Contacts

Prof. Dr. Johannes Buchmann
TU Darmstadt
Téléphone : +49 (0) 615 116 3416
E-mail : buchmann@cdc.informatik.tu-darmstadt.de

Erik Dahmen
TU Darmstadt
Téléphone : +49 (0) 615 116 5416
E-mail : dahmen@cdc.informatik.tu-darmstadt.de

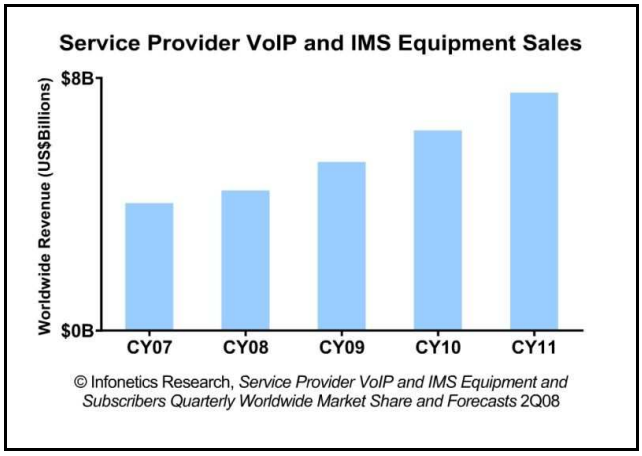
Signatures numériques pour la communication VoIP

M. Kuntze et M. El Khayari, scientifiques à l'Institut Fraunhofer des technologies de l'information sécurisées (SIT), Darmstadt

Nicolai Kuntze *est né en 1978 et a étudié l'informatique à l'Université technique de Darmstadt. Depuis 2005, il s'occupe, au sein de l'Institut Fraunhofer SIT, de plusieurs aspects relatifs à la sécurité des technologies de l'information. Ses spécialités de recherche se trouvent en l'occurrence dans les domaines de l'informatique de confiance (Trusted Computing) ainsi que dans la sécurité de la VoIP.*

Rachid El Khayari *est né en 1982, a étudié l'informatique à l'Université technique de Darmstadt et a essentiellement orienté son mémoire sur les aspects de sécurité de la VoIP.*
Depuis janvier 2009, il travaille dans le domaine des systèmes mobiles sécurisés à l'Institut Fraunhofer SIT.

La voix sur réseau IP (VoIP), également nommée téléphonie par Internet, a conquis d'emblée le monde des affaires. Les analystes estiment un taux de croissance annuel de 20 à 45% et pronostiquent en particulier une forte poussée jusqu'en 2011, comme le montre le graphique 1. Dans quelques années, selon leurs estimations, la moitié des communications professionnelles se fera par Internet. Le succès de la VoIP ne se restreindra pas seulement au réseau câblé, mais se répercutera aussi sur le langage convergent (discussions) et la transmission de données via la prochaine génération de téléphones mobiles. Les économies financières pouvant être réalisées grâce à la VoIP et une connexion Internet haut-débit présentent un effet irrésistible sur les PME et d'autres organisations encore plus grandes. La concentration des technologies de l'information et de la communication (TIC), allant de paire avec la VoIP, réduit aussi les coûts d'exploitation au niveau de l'organisation. Or, comme toute technologie convergente, la VoIP peut hériter des faiblesses des mondes de l'information et de la communication. Tel l'Hydre de Lerne, les risques liés à la sécurité de la VoIP sont multiples.



Graphique 1 : Pronostiques de croissance pour la VoIP

L'enjeu

Un des problèmes fondamentaux auquel la VoIP doit faire face est la confidentialité du contenu de la conversation. Le transport des données vocales implique de nombreux nœuds de connexion augmentant la probabilité de piratage de la conversation par rapport au réseau de téléphone PSTN. Sur ce dernier, un attaquant avait besoin d'un accès direct à la ligne de communication désirée. Il existe heureusement, dans ce domaine de sécurité des TIC, des méthodes qui ont déjà fait leurs preuves. Elles offrent un large spectre de contre-mesures, allant des W(V)LANs, en passant par des réseaux privés virtuels (VPN), jusqu'au cryptage End-to-End des conversations VoIP à l'aide de technologies telles que par exemple le protocole SRTP.

D'autres problèmes sont plus compliqués, puisqu'ils sont directement liés à la définition particulière de la communication vocale. Premièrement : la VoIP peut être bombardée de publicité par le manque de légitimation de l'appelant – appelé le SPIT (SPAM over Internet Telephony). Les appels SPIT automatisés peuvent être crées à moindres coûts, ce qui pourrait encourager le spamming et rendre la VoIP inutilisable. Deuxièmement : la confidentialité des flux de données par VoIP doit être renforcée, puisque les conversations sur une base IP peuvent être aisément utilisées de façon mal attentionnée et à moindre coût. Troisièmement : les données vocales, qui seront stockées à long terme dans des archives numériques, peuvent être victimes de falsifications. Ce problème peut s'avérer gênant pour les organisations d'archivage – comme par exemple les centres d'appels – qui ont des intérêts propres dans la préservation du contenu des conversations en cas d'utilisation ultérieure, en tant que justificatif par exemple. Une solution complète à ce problème se fait toujours attendre. Pour l'instant, seule l'incorporation de simples paquets de données, comme par exemple dans le cadre du protocole Secure Real-time Transport Protocol (ou SRTP), permet de protéger la confidentialité.

La technologie VoIPS

La technologie VoIPS résout simultanément les trois problèmes précédemment mentionnés – grâce à une méthode ouverte, qui est compatible avec les importants standards VoIP SIP et RTP. Le sigle VoIPS signifie "Voice-over-IP Signatures". La VoIPS sécurise des discussions grâce à la signature électronique de la communication numérique à base de paquet. Signer une conversation par VoIP signifie sécuriser la confidentialité et l'authenticité des flux de données des deux côtés et sa séquence temporelle. Ces deux conditions combinées créent le cadre de protection de la conversation. La VoIPS est très apparentée aux protocoles SIP/RTP, qui interviennent lors d'une communication VoIP et qui offrent un haut niveau de sécurité. En activant eux-même leurs signatures, les utilisateurs inconnus autorisent la conversation. La VoIPS instaure ainsi une nouvelle mire pour la justification des données numériques. La confidentialité des conversations enregistrées, la sécurité sur l'identité des interlocuteurs et leur consentement – ces trois éléments sont inclus dans la signature et permettent légalement les contrats reconnus et oraux entre deux partenaires inconnus au téléphone.

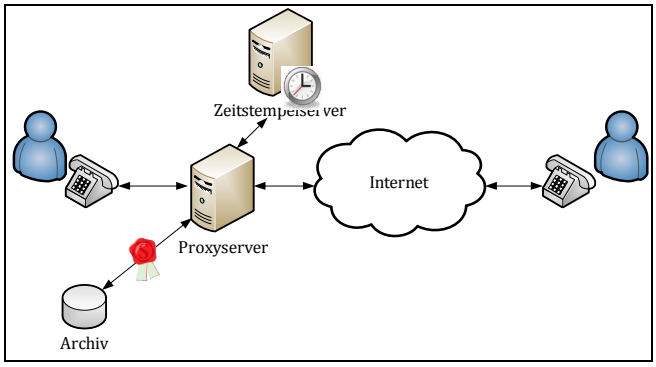


Illustration 2 : Vue globale de l'archivage VoIPS

La technologie brevetée peut être utilisée pour chaque communication numérique et n'est pas seulement limitée à une seule entreprise fournisseuse de la technologie. Le contenu de la communication numérique est morcelé en paquets et envoyé aux récepteurs respectifs. La VoIPS se base sur cette forme de communication à base de paquet. Les paquets peuvent se perdre, de même des ralentissements peuvent survenir et ainsi entraîner une baisse de la qualité dans la communication. Les précautions suivantes sont prises afin d'éviter ces inconvénients.

Sans modifier le flux des paquets de données, des intervalles signés numériquement sont introduits à la suite d'un certain nombre de paquets. Afin de traiter les pertes éventuelles de paquets, il existe un protocole d'échange d'accusés de réception qui montre que les paquets sont bien arrivés à leur destinataire. Ce schéma fondamental d'intervalles est appliqué pour les deux axes de communication – de A vers B et de B vers A. Ainsi, ceci garantit qu'aucun des deux interlocuteurs ne peut intentionnellement détourner des paquets et nier par la suite le contenu de la communication.

Jusqu'ici, les paquets sont protégés par des intervalles de signature par VoIPS à chacune des interfaces. Ensuite, il s'agit de garantir la cohérence des intervalles afin d'éviter que ces derniers soient rajoutés ou enlevés. Pour se faire, les intervalles sont imbriquer pour parvenir à une chaîne cryptographique. Les intervalles et l'imbrication offrent une forte protection de la sécurité lors de la communication.

Dans le domaine de l'archivage des communications téléphoniques, l'Institut Fraunhofer SIT, en collaboration avec Artec IT Solutions, veut rendre commercialisable la VoIPS dans les 18 prochains mois. Artec, une entreprise située à Karben près de Francfort, a déjà développé des produits dans le domaine de l'archivage de mails et de documents sécurisés. Grâce à une coopération avec l'Artec et l'Université de Kassel, l'Institut Fraunhofer SIT veut accélérer ce développement. Outre le développement de la technologie et des produits, une autre priorité est la recherche juridique, qui est réalisée à l'Université de Kassel par l'équipe du professeur Rossnagel.

Le sujet de l'archivage est d'une utilité et d'un intérêt particuliers pour certains groupes tels que les banques et autres institutions financières, les administrations et le gouvernement ainsi que les centres d'appels. L'enregistrement des communications téléphoniques compte parmi les applications les plus importantes dans le domaine des télécommunications. Le premier archivage d'une communication vocale, montré dans l'illustration 3, a été présenté en 1911 par Thomas A. Edison.

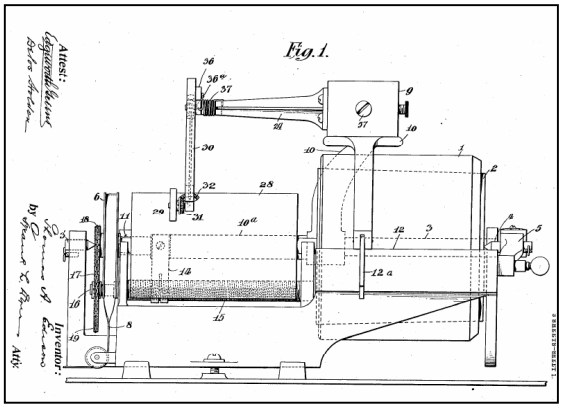


Illustration 3

Un autre objectif consiste à transformer le dispositif d'archivage des mails – EMA - de l'entreprise Artec IT

Solutions, déjà établi sur le marché, en une archive de communication complète.

D'ores et déjà, d'importants prestataires européens de technologie pour les centres d'appels ont manifesté leur intérêt pour la VoIPS comme standard dans le domaine de la sécurité de la communication.

Contact

Nicolai Kuntze
Fraunhofer SIT, Darmstadt

Téléphone : +49 (0) 615 186 9276
E-mail : nicolai.kuntze@sit.fraunhofer.de

Filigranes - Protection des médias numériques

M. Steinebach est directeur du groupe de recherche pour la protection des informations multimédias à l'Institut Fraunhofer des technologies de l'information sécurisées (SIT) et directeur du laboratoire expérimental du Centre de recherche de sécurité avancée à Darmstadt (CASED).

***Martin Steinebach**, né en 1971, a étudié l'informatique à l'Université technique de Darmstadt entre 1992 et 1999. En 2003, il a obtenu son doctorat sur les filigranes numériques pour les médias. Depuis début 2005, il est membre du groupe de travail d'antipiraterie de l'Association des éditeurs et libraires allemands. Depuis début 2006, il est porte-parole du groupe de stéganographie et de filigranes de la section sécurité des GI.*

Les mécanismes numériques de réalisation de filigrane intègrent dans les médias numériques (images, sons et vidéos) des informations non-perceptibles qui peuvent par exemple spécifier l'auteur d'une œuvre ou les numéros de transaction. Ainsi, ces mécanismes permettent d'attribuer une identité personnelle et facile à utiliser dans les copies numériques d'une œuvre. Celles-ci sont d'habitude non distinguables.

Dans le domaine du téléchargement sur Internet, les filigranes numériques se sont révélés, dans les années passées, comme une alternative aux systèmes DRM - Digital Rights Management (gestion des droits numériques - GDN). Le développement du filigrane est lié à deux raisons : d'une part, les DRM compliquent l'utilisation des biens numériques et mènent à une augmentation des demandes en service de la part des clients, alors que les filigranes ne sont quant à eux pas perceptibles par l'utilisateur. D'autre part, les filigranes numériques permettent également de garantir une protection après la transition du média numérique dans le monde analogique. En effet, ils demeurent toujours lisibles dans le matériel protégé comme par exemple lors de l'impression d'une image marquée par un filigrane ou l'enregistrement analogique par un microphone. A l'inverse, les DRM échouent dans ce domaine à cause de cette „lacune analogique" : les médias ainsi protégés peuvent être librement copiés lors du passage du numérique à l'analogique.

C'est avant tout la robustesse croissante vis-à-vis des copies analogiques qui rend les filigranes numériques attractifs pour la protection des médias ou des biens qui ne sont pas, en premier lieu, de nature numérique. Ils représentent une technologie qui reprend le principe de base des codes barres (et de marqueurs visuels semblables), c'est-à-dire qu'ils justifient l'intégrité des informations relatives aux biens tout en gardant l'information invisible dans l'image en question.

Les filigranes numériques offrent la possibilité d'identifier des copies et de les traquer. Ils n'empêchent aucunement la réalisation de copies, car ils ne font qu'intégrer des informations dans les médias, sur lesquels aucune action n'est possible. Sans un environnement approprié et des mécanismes supplémentaires de soutien, aucun contrôle des copies ne peut être garanti par les filigranes.

D'un point de vue technique, le filigrane numérique est un signal qui intègre des informations non perceptibles et en même temps non modifiables. Il est contenu dans un signal porteur au moyen d'un algorithme d'intégration utilisant une clé secrète. Pour chaque algorithme d'intégration, il existe également un algorithme de requête qui permet d'identifier le filigrane inséré dans les données marquées lorsque la clé secrète est disponible. Ce schéma intégré représente ainsi les informations dissimulées. En général, il s'agit des données relatives à l'auteur (identité de la source), au client (identité du destinataire) ou des métadonnées qui peuvent par exemple décrire l'identité de l'œuvre elle-même.

Il existe plusieurs critères de distinction entre les différents procédés de réalisation de filigrane qui sont : la robustesse et la transparence, également nommée la non-perceptibilité. La robustesse décrit la résistance de l'information contenue dans le filigrane vis-à-vis des modifications subies par les données ou par le traitement des médias. L'impression, le scannage ou la reprise de photos, mais aussi les conversions des couleurs, l'agrandissement, la réduction ainsi que la découpure des images sont des exemples contre lesquels les filigranes doivent être robustes. L'information est dite transparente (non-perceptible) si une 'ouïe ou une vue moyenne' ne peut faire la différence entre les données marquées et l'original.

D'autres caractéristiques de ces procédés sont la quantité d'informations qui peut également être intégrée dans les filigranes, la sécurité vis-à-vis des attaques ciblées et la rapidité suivant laquelle un filigrane peut être intégré.

Travaux au centre CASED

Dans les prochaines années, au sein du centre CASED (Center for Advanced Security Research), soutenu par le Land de Hesse, va faire progresser la sécurité des TIC dans de nombreux domaines. Dans celui des filigranes numériques, les activités principales seront concentrées sur l'augmentation immédiate de la sécurité des filigranes contres les attaques connues. L'accent sera mis sur la recherche, la réalisation et l'évaluation d'approches fondées à partir d'idées fondamentales déjà connues, mais dont l'application pratique n'est pas encore déterminée.

L'augmentation de la sécurité des filigranes numériques individuels sera prioritaire. Ils sont utilisés par exemple pour l'identification d'un client lors d'achats sur Internet afin d'éviter des attaques groupées. Ces attaques ont lieu lorsque plusieurs clients informatiques coopèrent avec leurs copies marquées individuellement en produisant par exemple une valeur moyenne des copies et en créant ainsi une nouvelle copie avec un filigrane détruit.

Il existe des préparatifs afin d'instaurer des mesures de prévention qui sont déjà pris en compte. Ils portent, entre autres, sur les sujets suivants : les algorithmes pour la réalisation d'empreintes digitales d'identification du client ; les approches visant d'un côté la réalisation des variations de données afin de baisser la qualité du média lors d'attaques groupées et de l'autre côté l'amélioration de la fiabilité pour reconnaître les empreintes digitales à l'aide d'une variation de l'intensité du filigrane ; les approches s'intéressant à l'augmentation de la sécurité des empreintes digitales grâce à une combinaison de l'attribution de la clé et des empreintes digitales afin de garantir conjointement la traçabilité de l'attaquant en minimisant les informations contenues dans le filigrane.

Dans les prochaines années, l'objectif de la recherche dans le domaine des filigranes numériques sécurisés au sein du CASED, en coopération avec des partenaires et des clients, est d'optimiser les procédés pour la réalisation des empreintes digitales afin de minimiser la complexité lors de la création des variantes. L'exactitude de la lecture des procédés de filigrane augmentera grâce à l'optimisation de la synchronisation et à une analyse des médias marqués afin d'évaluer la qualité attendue du filigrane.

En particulier, les procédés de filigrane et d'empreintes digitales doivent être plus étroitement liés afin de garantir une utilisation optimale de toutes les ressources et des potentiels technologiques fondamentaux.

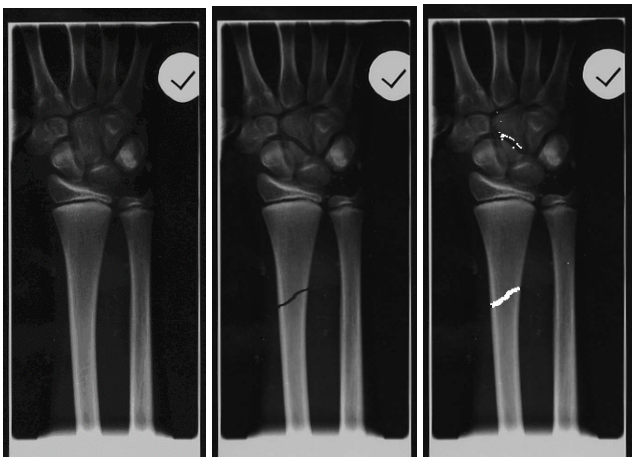
Un exemple d'application « eHealth »

L'amélioration de la sécurité des services des TIC dans le secteur de la santé est un domaine d'application dans lequel le CASED joue un rôle particulier. Là aussi, les filigranes numériques peuvent apporter une aide précieuse.

La possibilité de lier l'identité du médecin traitant et du patient directement dans un fichier médiatique, par exemple dans une radiographie, améliore la fiabilité des processus lors du traitement. Les risques de confusion sont écartés : les médias peuvent ainsi être assignés automatiquement aux médecins et aux cas médicaux, même lorsque étiquetage manuscrit est incorrect. Cela peut également servir à garantir l'anonymat du patient. Un médecin peut transférer une radiographie à ses collègues, afin qu'ils effectuent des expertises supplémentaires, sans pour autant que le nom du patient soit mentionné. Ensuite, les filigranes intégrés dans les images ainsi que leurs expertises pourront être reconnectés avec l'identité du patient.

Outre la protection des identités, il est également possible de protéger l'intégrité des supports. Un filigrane intégré dans un média permet de savoir si ce dernier a été modifié grâce à un processus comparable à celui utilisé dans les signatures numériques.

Les filigranes offrent toutefois l'avantage de pouvoir distinguer un traitement autorisé et dans le cas d'une manipulation, en retrouver la localisation exacte.



A gauche : image originale ; **Au centre :** manipulation de l'image par une fracture de l'os gauche, ajoutée ultérieurement ; *A droite* : localisation de la manipulation dans l'image reconnue grâce au filigrane (couleur blanche)

Contact

Dr. Martin Steinebach
Fraunhofer SIT, Darmstadt
http://www.sit.fraunhofer.de
http://www.cased.de

Téléphone : +49 (0) 615 186 9349
E-mail : Martin.Steinebach@sit.fraunhofer.de