
Processus de sécurité de la clé biométrique STEALTH MXP™

Écrit par
Larry Hamid
Chief Technology Officer
MXI Security



www.mxisecurity.com

Préambule

De nombreuses méthodes matérielles et logicielles de sécurisation ont été employées pour l'authentification forte des individus aux systèmes. Traditionnellement elles existent sous plusieurs formes telles que les cartes à puce, les clefs USB, les lecteurs biométriques et les mots de passe éphémères (One Time Password). Beaucoup de procédés ont été inventés et ajoutés en matière de processus d'authentification afin d'assurer d'autres services de sécurité tels que le référentiel sécurisé d'informations soit personnelles soit d'entreprise ou la conduite d'opérations cryptographiques pour une signature numérique, l'encryptage le décryptage. Malgré la multitude de possibilités et de facteurs formes des jetons qui sont apparus sur le marché elles sont toutes limitées en termes de capacité, d'application et de portabilité, autant d'obstacles sérieux lorsqu'il s'agit de faire face aux nouvelles exigences pour gérer des identités numériques. MXP est la première technologie du genre à comporter des identités diverses, l'authentification, une capacité importante, la flexibilité, la sécurité et la portabilité afin de satisfaire les besoins des systèmes existants ainsi que les demandes, en pleine évolution, de l'industrie de la gestion de l'identité et de la sécurité de l'information.

Identité Numérique

Une identité numérique peut être définie comme un ensemble d'attributs qui caractérisent une personne ou une chose dans le domaine numérique. Un attribut est un énoncé émis au sujet d'une personne ou d'une chose par une personne ou une chose. L'identité numérique comporte plusieurs facettes.

D'une manière générale, chaque entité avec laquelle nous interagissons dans le monde numérique recherche des attributs spécifiques de notre identité. Par exemple, votre banque en ligne vous identifiera par votre numéro de compte bancaire tandis que votre adhésion à une communauté Web peut être votre adresse de courriel. Dans beaucoup de scénarios votre identité pourrait être une information personnelle telle que votre nom, votre adresse ou votre numéro de téléphone. Une fois l'identité confirmée elle peut être employée pour accéder aux services pour lesquels elle est autorisée selon les critères de sécurité du service.

Le nombre d'identités numériques que nous possédons est en augmentation constante. Chaque entreprise utilise beaucoup d'applications qui contribuent à la multiplication d'utilisateurs et de mots de passe que chaque utilisateur doit mémoriser. Les organismes traitent cette question typiquement en déployant les solutions *single sign-on* (SSO). La plupart des produits de SSO maintiennent une banque d'identités numériques, la plupart du temps sous forme de nom de login et de mots de passe. Ceux-ci sont utilisés par les diverses applications qui en ont besoin.

Le Web a été une autre source de prolifération d'identité numérique. Les gens utilisent le Web pour leurs tâches courantes telles que les achats, des opérations bancaires et le divertissement tandis que les entreprises fournissent de plus en plus de services et de contenu à leurs clients, partenaires et employés. Chaque service exige habituellement ses propres identifiants de comptes et mots de passe. La sécurité, la confidentialité et l'interopérabilité des identités numériques constituent les plus grands défis pour l'internet aujourd'hui. On commence à traiter ce problème avec des normes émergentes et des technologies telles que le Web Service Security (WSS) et la Liberty Alliance pour créer une architecture de gestion d'identité connue sous le nom de Federated Identity (Identité Fédérée).

Authentification d'utilisateur

L'authentification de l'utilisateur est le processus utilisé pour identifier un individu afin de s'assurer que l'individu est celui qu'il prétend être. L'authentification d'utilisateur est toujours basée sur au moins un parmi trois facteurs : la connaissance, la propriété et la biométrie.

Par l'utilisation de la connaissance un utilisateur montre qu'il connaît un secret tel qu'un mot de passe. La propriété prouve l'identité basée sur la possession d'un objet particulier tel qu'un badge d'employé ou une carte à puce. En biométrie, des traits physiques ou comportementaux qui sont uniques à un individu sont employés pour confirmer l'identité. Des exemples de traits biométriques sont les empreintes digitales, la structure de l'iris, le spectrogramme vocal et le visage.

L'efficacité de l'authentification de l'utilisateur augmente sensiblement par l'emploi combiné de deux ou de plusieurs facteurs. Par exemple, le fait d'exiger à la fois un code PIN et une carte à puce (connaissance et propriété) a comme conséquence une authentification plus forte que la simple exigence de la propriété d'une carte à puce. Beaucoup d'organisations ont mis en application l'authentification forte en déployant les cartes à puce, des lecteurs biométriques et un mot de passe éphémère (OTP ou *one time password*).

De nouvelles initiatives de régulations sont actuellement l'objet de législation telles que Sarbanes-Oxley, HIPAA et Gramm-Lixivient-Bliley. Ces normes augmentent la responsabilité des individus et des organismes à l'égard de leurs actions touchant à l'accès et l'utilisation d'informations sensibles. Un tel niveau de responsabilité exige un lien fort entre l'individu à son identité numérique.

En tenant compte du nombre toujours croissant de nos identités numériques et du nombre de plus en plus important de services dont l'accès dépend de ces identités, sans oublier la tendance à l'augmentation de la responsabilité légale pour ses actions à l'intérieur des entreprises, il est évident que l'authentification forte et fiable des individus est un aspect important de l'infrastructure d'identité numérique.

Fournisseurs d'identité et jetons de sécurité

Un fournisseur d'identité est une entité qui définit et distribue des identités numériques. Les compagnies de carte de crédit, les gouvernements et les entreprises sont des exemples de fournisseurs d'identité car ils communiquent des identités à leurs usagers, clients ou citoyens. Les individus sont également considérés comme des fournisseurs d'identité dans la mesure où ils créent leur propre identité chaque fois qu'ils adhèrent à un site Web.

Pour être utile dans une transaction numérique, l'identité doit être affirmées d'une manière ou d'une autre. Le mécanisme utilisé est de mettre des affirmations d'identité dans ce qu'on appelle un jeton de sécurité (*security token*). Les jetons de sécurité sont considérés comme fiables par des personnes qui en dépendent grâce à une relation de confiance entre l'utilisateur et l'instance émettrice et peuvent être vérifiées par des méthodes cryptographiques. Les jetons de sécurité existent sous beaucoup de formats selon le système employé. Par exemple les certificats X509 donnent les informations d'identité aux systèmes de PKI. Les jetons SAM confirment les identités demandées dans un contexte WS-Trust, Le One-Time-Passwords (OTP ou mots de passe éphémères) sont employés par des serveurs d'accès à distance, alors que les username et les mots de passe peuvent être fournis aux systèmes anciens, aux dialogues de login et dans les pages Web.

Les jetons de sécurité sont publiés après l'authentification réussie du sujet. Parfois c'est le fournisseur d'identité qui effectue l'authentification comme dans le cas d'un site Web qui vérifie un nom et un mot de passe d'utilisateur. Alternativement, l'authentification peut être déléguée à une autre entité digne de confiance. Par exemple, une carte à puce peut générer un jeton X509, qui pourrait contenir votre identité numérique publiée par une autorité telle que votre employeur. L'opération de signature de la carte à puce fournit la preuve que l'utilisateur possède la clef privée. La personne concernée peut également vérifier la validité du certificat en faisant confiance à l'Autorité de Certification (*Certificate Authority*).

Le processus de publication d'un jeton de sécurité à l'aide d'un dispositif tel que Stealth MXP est illustré ci-dessous.

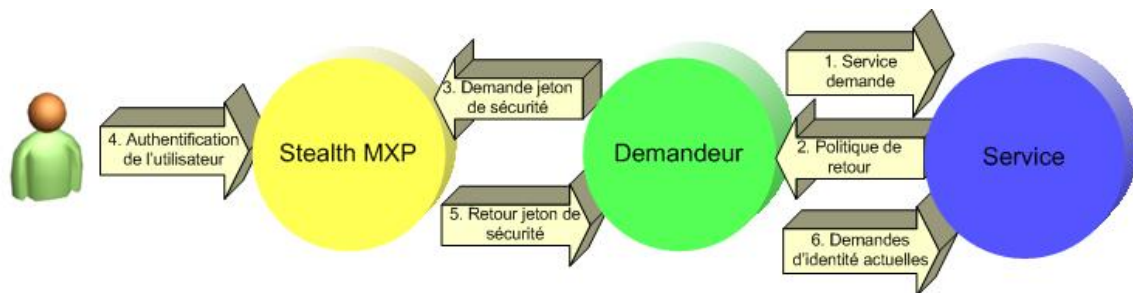


Figure 1: Flux du Jeton de Security sur Stealth MXP

Microsoft InfoCard et PSTS

Microsoft a récemment dévoilé sa technologie InfoCard en tant qu'élément d'un méta-système d'identité. InfoCard permet à l'utilisateur de visualiser et de contrôler l'utilisation de ses identités numériques, fournit une expérience cohérente et constante à travers les systèmes et technologies multiples et fournit un environnement plus sûr pour des consommateurs où des attaques telles que le « phishing » sont atténuées.

InfoCard représente les identités numériques sous la forme de cartes d'informations qui peuvent être présentées visuellement aux utilisateurs d'une manière constante. Des services différents cherchent des affirmations d'identité différentes selon leurs politiques de service. Par exemple, les affirmations que vous fournissez à une institution financière sont différentes de ce que vous fourniriez pour une communauté en ligne telle qu'un groupe de discussion un service de jeu.

Pendant une transaction le système d'InfoCard interprétera une politique de service et affichera les identités numériques qui conviennent à ce service, permettant à l'utilisateur de choisir celui qu'il souhaite utiliser. Une fois les informations confirmées, elles sont insérées dans un jeton SAML, éliminant le besoin de remplir un formulaire Internet. Cette facilitation de contrôle pour l'utilisateur, combinée avec la sécurité du système d'InfoCard, est considérée généralement comme crucial au succès de l'identité numérique sur Internet.

MXI et Microsoft développent conjointement un standard, appelé Portable Security Token Service (PSTS) qui indique comment les InfoCards pourront être gérées sur les dispositifs portatifs qui sont capables de publier un jeton SAML.

Défis actuels

Tout dispositif qui va être utilisé aujourd'hui et à l'avenir comme technologie numérique efficace d'identité doit faire face à un grand nombre de défis.

Identités multiples et formats

La capacité de transporter de multiples identités différentes et de les fournir dans plusieurs formats différents est difficile à réaliser. C'est une question qui n'a pas été vraiment été adressée dans la conception actuelle des jetons.

Les cartes à puce ont une capacité réduite avec comme résultat un nombre limité de paramètres numériques susceptibles d'être maintenues. Les cartes plus grandes atteignent aujourd'hui seulement 64K à 128K octets pour le code et les données. Après la place prise par le code, il ne reste seulement la place que pour une demi-douzaine de paramètres PKI. En terme de formats, les cartes à puce sont habituellement compatibles X509 mais ne produisent pas des jetons SAML. Il est intéressant de remarquer que les solutions SSO ont utilisés les cartes à puce intensivement pour stocker également des paramètres d'applications tels que des usernames et des mots de passe dans des containers sécurisés.

Bien plus limitées dans leur portée pour l'identité numérique sont les jetons OTP. Bien qu'elles fournissent une authentification forte on pourrait maintenir que les jetons OTP ne fournissent pas d'identités numériques réelles puisqu'elles ne donnent aucune affirmation additionnelle autre que les données d'authentification. De par le fait qu'ils soient liés à un serveur d'authentification, les jetons OTP ne servent, en réalité, qu'à authentifier une identité a un système.

Un aspect intéressant des cartes à puces, est que leur facteur de forme permet d'autres moyens physiques pour l'authentification et identité. Souvent une carte à puce se double d'un badge dans une entreprise, car, portant une image de l'employé, elle permet l'inspection et la vérification manuelle de l'identité de l'utilisateur par un autre individu tel qu'un garde de sécurité. Il est facile d'y intégrer des puces RFID ou des codes à barres pour permettre l'accès physique à des locaux. Les cartes à puce ont donc la polyvalence au delà de l'identité numérique en intégrant aussi des systèmes d'accès logiques.

Pluralité de normes

Beaucoup de normes de sécurité ont été développées pour répondre à la question de l'inter-opérabilité des applications et dispositifs. PKCS #11 et MS CAPI sont deux spécifications qui définissent une interface standard pour les services cryptographiques. Ils ont été employés sur une large échelle pour la gestion de dispositifs émetteurs de jetons de sécurité X509. On propose des extensions de ces normes afin de traiter d'autres objets de sécurité tels que des One-Time-Passwords (mots de passe éphémères).

W-Trust est le nom d'un jeu de spécifications qui est en cours de devenir une norme, à travers OASIS, permettant de définir des services de jetons de sécurité et de traiter la question de l'interopérabilité des jetons de sécurité. Cette norme sera employée très largement pour toute implémentation de Web Services Security, y compris le système InfoCard de Microsoft. Sous l'égide de WS-Trust, les spécifications PSTS sont employées pour permettre à des utilisateurs de se déplacer au sein d'un méta-système d'identité.

Les dispositifs d'identité doivent se connecter à travers les multiples normes existantes et émergentes s'ils veulent maximiser leur utilité et interopérabilité.

La portabilité

La portabilité a été difficile à réaliser. Beaucoup de dispositifs numériques d'identité sont physiquement, mais non logiquement portatif. La réalité d'aujourd'hui est que la plupart des dispositifs vous laissent seulement les utiliser dans les zones où vous avez déployé le logiciel associé au dispositif. C'est le talon d'Achille des cartes à puce. Malgré son faible encombrement ce qui est un élément favorable, la carte à puce doit elle aussi apporter des modules de gestion de périphérique, des lecteurs de cartes et du logiciel intermédiaire propriétaire afin de permettre son utilisation nomade. Des efforts énormes de définition de normes ont été lancés au cours des dernières années afin de traiter l'interopérabilité et la portabilité des cartes à puce. Dans la plupart des cas, la portabilité de carte à puce est limitée à l'errance à l'intérieur d'une organisation. Dépasser ces cadres stricts d'opérationnalité entraîne des difficultés bien supérieures.

La question de la portabilité a été résolue par une classe particulière de dispositifs d'authentification. Il s'agit de jetons OTP avec une alimentation à piles et fonctionnant sans connectivité entre le dispositif et système sur lequel agit l'utilisateur. C'est pourquoi ce sont les dispositifs de choix des entreprises, en particulier lorsqu'on ajoute une authentification forte, bâtie sur deux facteurs, pour l'accès à distance. Puisque aucun logiciel n'est exigé dans le système, ces jetons OTP permettent la mobilité totale aux utilisateurs à distance.

On doit également rester circonspect sur la prétention de beaucoup de fournisseurs de jetons USB au sujet de la portabilité.

Bien que les systèmes de protection USB n'exigent pas de lecteurs, ils peuvent avoir besoin d'un module de gestion de périphérique (driver) ou de privilèges d'administrateur pour opérer. Assez souvent ce besoin n'est pas évident car les dispositifs sont fréquemment évalués sur des machines où les privilèges d'administrateur sont présents permettant l'accès à des fonctions étendues et à des composants à installer silencieusement, donnant de ce fait un faux sens de la portabilité.

Beaucoup d'environnements d'entreprise ne donnent pas aux utilisateurs des privilèges d'administrateur sur leurs postes de travail. Ceci est également vrai pour les kiosques et les PC dans les cybercafés. La vraie portabilité doit être complètement transparente.

Sécurité et confidentialité

La sécurité et la confidentialité sont toujours des conditions essentielles pour tout dispositif de contrôle d'identité numérique. Avec l'augmentation de la pression due à la réglementation légale concernant l'accès à l'information et son utilisation, les organisations doivent s'assurer plus que jamais que les contrôles appropriés soient en place pour empêcher les accès non autorisés. Une infrastructure d'identité forte constitue la première étape pour assurer cette maîtrise là où toute fausse affirmation d'identité peut avoir des répercussions légales.

Le vol d'identité est le délit qui connaît la croissance la plus rapide sur internet. Ceci constitue une menace pour l'utilisation de service et de vente en ligne dans la mesure où les utilisateurs commencent à prendre conscience de l'existence de cette menace. Un des principes de base de l'affirmation de l'identité est la révélation minimale d'informations. C'est-à-dire, seulement les éléments d'identité exigés pour accéder à un service devraient être fournis et aucun autre. La protection des identités numériques est critique au succès de l'e-commerce et à l'utilisation de l'Internet pour des transactions commerciales.

Le logiciel est beaucoup plus vulnérable aux attaques que le matériel. Il est souhaitable de disposer d'un maximum de fonctions critiques pour la sécurité dans les jetons matériels eux-mêmes. En particulier, l'authentification forte devrait être mise en application à l'intérieur du matériel lui-même pour protéger les données d'authentification contre les attaques. De même la protection par le matériel des secrets et des clefs est également cruciale afin de sécuriser les identités contenues dans le dispositif et donc aussi les actifs auxquels ces identités permettent d'accéder.

L'avantage MXP

Le diagramme ci-dessous illustre l'utilisation de Stealth MXP dans le cadre d'interfaces d'identités digitales.

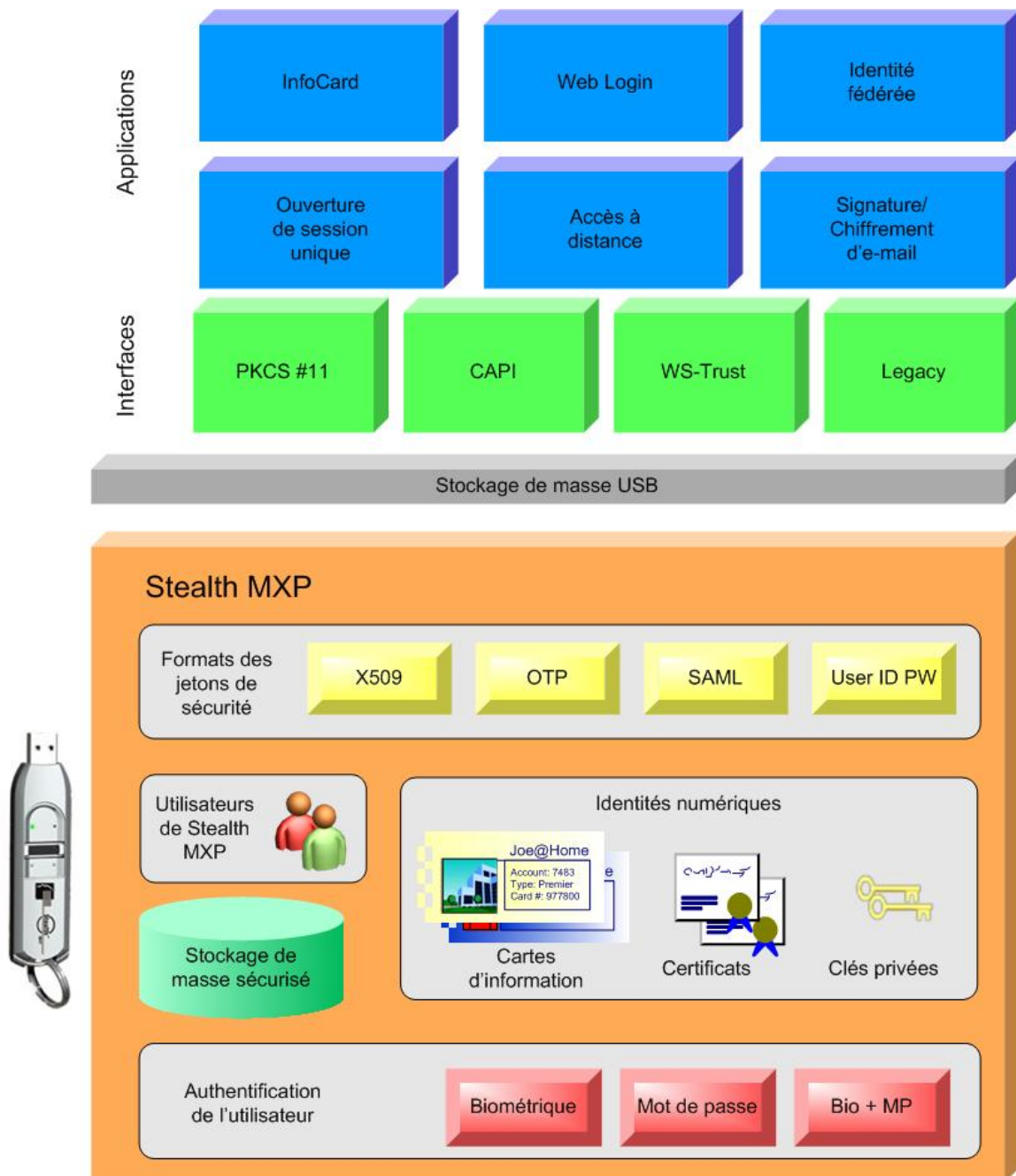


Figure 2: Stealth MXP et la couche d'identité digitale

Quant à la capacité, le système d'InfoCard exige qu'une paire unique de clés RSA soit produite pour chaque paire composée d'une authentification numérique et un service cible. Lorsqu'il existe de nombreuses identités numériques et services cible, les combinaisons possibles montent rapidement en nombre. Stealth MXP a la capacité de gérer des centaines d'affirmations de clés et d'identités numériques tout en fournissant une réponse rapide.

Stealth MXP sait générer beaucoup de formats, y compris le username et les mots de passe pour des systèmes anciens, des certificats x509 et la preuve pour des systèmes PKI, les One-Time-Passwords (mots de passe éphémères) pour des serveurs d'authentification, et peut produire des dispositifs SAML contenant des affirmations d'identité demandées par une personne utilisant WS-Trust. L'interopérabilité et la présentation de ces formats aux systèmes s'effectuent à travers des interfaces standard.

Stealth MXP fournit une authentification forte des utilisateurs se servant d'un mot de passe, d'empreintes digitales ou des deux facteurs ensemble. Ces mécanismes d'authentification se produisent entièrement dans le dispositif en fournissant une sécurité maximale du processus d'authentification et assurent un lien le plus fort possible entre un utilisateur de MXP et ses clés et identités numériques. D'ailleurs, le dispositif a également des possibilités de génération de clés pour s'assurer que les clés privées restent toujours secrètes à l'intérieur du matériel.

Stealth MXP est le premier dispositif de son genre à réaliser la portabilité à 100%. Le protocole de communication n'exige aucun driver additionnel et n'utilise aucune commande étendue qui exigerait des privilèges d'administrateur sur la machine.

En fait, le protocole de la Stealth MXP a été incorporé aux spécifications de PSTS principalement pour sa capacité de réaliser la portabilité complète. Ceci permet la réalisation de transactions Internet sécurisées en utilisant un dispositif portatif avec toute machine équipée du système d'InfoCard.

En conclusion

Stealth MXP comporte des services supplémentaires qui complètent sa fonctionnalité en tant que dispositif total de sécurité. Il peut à la fois fournir des services cryptographiques génériques liés aux utilisateurs authentifiés et garantir un stockage de masse avec encryptage transparent des informations confidentielles. Il comporte également des fonctions administratives qui lui permettent d'être contrôlée dans un environnement d'entreprise où des politiques de sécurité sont définies et imposées par l'organisation. Alternativement Stealth MXP peut être contrôlé par des individus pour un usage dans leurs propres environnements personnels.

Un dispositif adapté aux demandes extensibles d'identités numériques doit être souple dans sa capacité à gérer les identités numériques et les formats de jetons de sécurité. Il doit également assurer l'interopérabilité, la portabilité et la sécurité. Ce sont les éléments qui font que Stealth MXP s'annonce comme le dispositif qui répond aux exigences numériques d'identité d'aujourd'hui et demain.