

État de l'art de l'authentification renforcée

Dominique ALGLAVE

SG/STSI/SDITE
61-65 rue Dutot
75015 PARIS

Pascal COLOMBANI

SG/STSI/SDITE
61-65 rue Dutot
75015 PARIS

Nicolas ROMERO

Pôle de compétence Gestion des Identités
45000 ORLEANS

Sofiane FLIH

SG/STSI
61-65 rue Dutot
75015 PARIS

Résumé

Plusieurs approches différentes concourent à la sécurisation globale du système d'information, et cumulent leurs apports respectifs. Ainsi en est-il du suivi des bonnes pratiques d'une part, de la clarification du périmètre à protéger d'autre part et du renforcement du contrôle à l'accès, c'est à dire la première authentification. En fin de compte, la question de la sécurisation raisonnable, du niveau technologique suffisant, demeure toujours déterminante, ne serait-ce qu'au niveau budgétaire.

L'objectif de cette étude est justement de couvrir tous les types d'authentification allant du support cryptographique physique jusqu'au mot de passe, en abordant également les nouveaux modes d'authentification présentés récemment dans l'offre industrielle, tels que les « grilles dynamiques », les « jetons invisibles » ou les analyses comportementales, afin de permettre une comparaison de ces types après avoir dégagé des critères de comparaison communs. La partie méthodologique vise à exposer les critères et leur pertinence ainsi que leurs limites, tandis que les paragraphes relatifs aux résultats permettent à la fois de disposer d'une description de la technologie en question, puis d'une caractérisation sous forme de notation par critères mais aussi sous forme de radar. Enfin, ce dernier aspect débouche sur des comparaisons entre ces différentes techniques, leurs forces relatives, leurs faiblesses relatives et leur adaptabilité à telle population du ministère plutôt qu'à telle autre.

Ce travail concerne aussi les équipes de développement puisque ce tour d'horizon permet de dégager des concepts innovants dont certains sont partiels et pourraient initier d'autres développements libres de droit dont l'implémentation maîtrisée aurait un coût très faible.

L'outil de constitution des radars sera mis à disposition dès les JRES 2013.

Mots-clefs

Authentification forte, authentification faible, PKI, gestion des identités, vol d'identités, gestion de risques, fédération d'identité, SSO.

1 Introduction

Dans les systèmes d'information intégrant toutes les briques technologiques à l'état de l'art, telles que la fédération d'identité, l'authentification unique (SSO), la faiblesse de l'authentification initiale se propage à l'ensemble du domaine ainsi fédéré. De même la force de l'authentification initiale se propage à l'ensemble du périmètre fédéré dans la mesure où le réseau fédéré est lui aussi sécurisé de manière adéquate. Le renforcement de l'authentification du périmètre du système d'information est donc un enjeu de premier ordre. Cependant, mettre en œuvre ce renforcement n'est pas simple : il requiert de minimiser les changements d'architectures pour éviter des congestions à l'accès du système d'information ; il demande de modifier les habitudes de l'ensemble des usagers des applications ; il suppose un coût variable mais récurrent et couramment exorbitant par rapport aux capacités de budget de la sécurité informatique. Si bien que les points d'achoppements des projets utilisant la cryptographie ne sont plus de l'ordre de la maîtrise théorique ou des applications développées mais bien de la mise en œuvre globale intégrant tous les facteurs du déploiement. L'authentification forte utilise deux facteurs non liés parmi les trois de nature distinctes couramment présentés par 'ce que je suis', 'ce que je possède', 'ce que je sais', alors que l'authentification renforcée recouvre l'utilisation de deux facteurs liés parmi ces trois et présente de nombreux avantages de l'ordre de la facilité du déploiement ou du coût ou de la convivialité.

Etant donné que l'amélioration de l'authentification à l'accès est une étape clé du renforcement de la sécurité de l'ensemble du système d'information par le biais des outils de la fédération d'identité ou de l'authentification unique, il convient de lever les derniers obstacles qui s'y opposent. La seule certitude en la matière est que l'usage du mot de passe statique comme validation de l'identité à l'accès est aujourd'hui un facteur de risque. Mais il est nécessaire de faire l'inventaire des paramètres d'évaluation des techniques alternatives. La caractérisation des mécanismes d'authentification permettra ainsi de définir les étapes des déploiements intermédiaires vers une généralisation de l'authentification forte dans le futur.

Si les acteurs du système d'information sont par ailleurs issus de populations hétérogènes, alors la définition de classes homogènes des modes d'authentification renforcée est essentielle à la réussite de l'entreprise d'amélioration du niveau de sécurité. Le résultat conduira alors à disposer d'un bouquet d'authentification suivant les familles de population, dont les solutions d'authentification forte feront partie et resteront l'objectif à moyen terme.

Il s'agit en conséquence de doter les ministères d'un outil capable d'éviter des erreurs de parcours en choisissant des solutions d'authentification en inadéquation avec les besoins réels. L'objectif pour aujourd'hui est donc : qualifier les différentes technologies puis les différents produits d'authentification disponibles sur le marché, afin de faciliter leurs mises en œuvre éventuelles tant du point de vue des usages que de leur intégration dans les infrastructures existantes. Le cas échéant, d'autres solutions spécifiques peuvent être élaborées à partir de la prise en compte des lacunes des solutions commerciales et permettre ainsi à l'institution de disposer à faible coût de solutions techniques bien adaptées.

2 Méthodologie – élaboration des critères

2.1 Constitution de critères d'évaluations des technologies

Etant donné la diversité des solutions proposées sur le marché depuis trois ans, il est complexe de présenter une grille d'analyse fiable apte à honorer les avantages sans omettre les inconvénients. Il convient donc d'établir une liste de critères en préalable pour couvrir les grandes problématiques communes aux différentes communautés constituant le ministère, puis d'évaluer les types de technologie au regards de ces critères et enfin de montrer les principaux traits issus des choix de certains produits industriels combinant plusieurs technologies. En résultat collatéral de cette étude, il sera possible d'effectuer des comparaisons et éventuellement de concevoir des types technologiques nouveaux répondant mieux encore aux besoins spécifiques du ministère.

2.2 Explication des critères et justification de leur pertinence

La classification des critères part du principe d'un découpage par domaine d'évaluation regroupant des sous critères issus de questions précises. L'explication de ces derniers vient ci-après et demeure une approche subjective.

1. Domaine relatif à la typologie de l'authentification

L'objectif de cet aspect de la caractérisation vise à situer le plus clairement possible le mode d'authentification par rapport aux critères habituellement connus et référencés dans les études classiques de l'authentification. Etant donné l'émergence de nouveaux types, il faut revenir aux fondements de la classification basée sur le facteur de forme physique ou non, sur le partage de secret ou non ainsi que d'autres paramètres permettant de les situer comparativement. Plus la technologie sera forte, plus la note sera valorisée.

On distingue dans ce domaine la valorisation des critères suivants :

- La famille d'appartenance couvrant les possibilités suivantes : simple login et mot de passe, login et mot de passe + Captcha, OTP Matériel, OTP Logiciel, OTP à la demande, grille dynamique, authentification environnementale, authentification par le risque, authentification comportementale, par l'usage de la biométrie, et plus classiquement par les certificats.
- Dès lors, on peut affecter une qualification de faible à très forte en nuancant par des évaluations intermédiaires en fonction des risques identifiés ou constatés. Le qualificatif de très fort étant réservé à l'authentification par certificat sur support cryptographique physique qualifié par les organismes habilités en France dans la mesure où la maîtrise complète des infrastructures et des opérateurs est également assurée (Le cas des commissions d'autorités d'enregistrement de COMODO montre que cette maîtrise des opérateurs et des infrastructures fait partie de l'évaluation de l'offre de sécurité). Viennent ensuite les solutions d'OTP avec support cryptographique physique qui présentent la vulnérabilité de la centralisation des secrets partagés dans un support qui peut ne pas être fort et qui est vulnérable à des attaques internes multiples ou à des pannes potentielles mettant en défaut le fonctionnement de l'authentification. A l'extrême vient le mot de passe simple sans politique de renforcement. Au cas par cas, il est possible de noter chaque technologie en relatif par rapport aux deux extrêmes.
- De manière à compléter le critère précédent, le nombre de facteurs est ajouté à l'étude pour préciser le précédent et donner une indication qui reste décisive dans l'usage tant par les questions de déploiement que d'attaque potentielle.
- La volonté de s'inscrire durablement dans la démarche de l'ANSSI implique de préciser si le produit couvert par le type d'authentification étudié a été qualifié ou s'il entre dans une catégorie du Référentiel Général de la Sécurité.

La typologie de l'authentification permet aux spécialistes de situer d'emblée les difficultés prévisibles dans la mise en œuvre ou l'acceptation des produits qui s'y rattache.

2. Domaine relatif à l'adhérence vis-à-vis des technologies choisies

Le but de ce second domaine vise à souligner le degré d'adhérence technique de certaines solutions vis-à-vis de tout support. Ce groupe de critères vise à déceler d'éventuels coûts cachés dans le déploiement, la maintenance, mais également à identifier une capacité réelle ou au contraire une incapacité de réaction par rapport à un incident technologique majeur. Autrement dit, même si dans les critères précédents le fait qu'il y ait un support physique apporte un avantage en matière de sécurité, si la robustesse de l'ensemble est mise à mal alors le support physique devient une contrainte forte pour la reprise d'activité sécurisée. Il s'agit de mesurer la capacité de résilience. Donc, plus l'adhérence sera forte, plus la note sera dévalorisée :

- La technologie est-elle basée sur un support cryptographique physique, quel qu'il soit ?
- Est-elle utilisable sur un poste en libre-service sans avoir à le personnaliser de manière spécifique ?
- Y-a-t-il une installation d'un pilote logiciel spécifique et dans ce cas, peut-on disposer du support pour tous les type d'OS (y compris pour les tablettes) et tous les types de matériel plus pauvres en connectique ?

3. Domaine relatif à la protection du secret

Les paramètres de ce troisième domaine visent à mettre en exergue un groupe d'événements redoutés et leur probabilité associée. Cet aspect plus précis de l'analyse de risque, faite exclusivement sur la sécurisation périmétrique reposant encore massivement sur l'authentification par mot de passe, traduit une focalisation technique : il s'agit de la sensibilité au vol du secret, et plus particulièrement lorsqu'il est fait à l'insu du porteur. Le fait de focaliser sur ce risque vise à établir les authentifications renforcées comme étape intermédiaire possible vers l'authentification forte référencée dans le RGS. Reste à en voir les nuances et à en accepter ou non les risques résiduels selon les besoins. La protection du secret est notée de plus en plus favorablement selon qu'elle permet de :

- Résister au vol d'identifiant par phishing ou key logger ou encore par observation répétée
- Echapper au vol par interception

- Et surtout de reprendre une activité de manière sûre après attaque massive du système de sécurité ; il s'agit de mettre en valeur la résilience intrinsèque d'une méthode d'authentification en cas de constat de la perte du secret

4. Domaine relatif au coût

Par ce quatrième domaine, l'étude entend prendre en compte les coûts d'infrastructure et de déploiement initial ainsi que les coûts unitaires pour un porteur d'authentification. Par ailleurs, le coût de maintenance annuelle est aussi pris en compte. La précision de ces critères est difficile à obtenir sans avoir lancé un appel d'offre.

5. Domaine relatif à l'intégration

L'intégration d'un projet d'authentification dans la globalité du système d'information - au sens du système qui porte la donnée - est essentielle à sa bonne réussite. Afin de traduire concrètement ces termes il faut prendre en compte d'une part l'intégration technique grâce aux critères suivants :

- L'aisance de l'intégration dans l'infrastructure existante et en particulier dans l'infrastructure d'authentification et de fédération d'identité, notamment par la compatibilité du modèle basé sur CAS, Shibboleth, ou l'architecture de RSA (FIM, Authentication Manager, Access Manager)
- L'indépendance par rapport à certaines technologies propriétaires et la capacité à inter opérer avec tous les références issues des normes ou des solutions industrielles répandues (SAML, LDAP, RADIUS pour les premières, AD, pour les secondes, etc.)
- La capacité à passer dans un mode industriel réparti dans les infrastructures des ministères. Il est visé par ce critère l'indépendance par rapport à un modèle en cloud computing, autant que l'aptitude avérée du support industriel à corriger d'éventuels bugs par la maintenance logicielle ou l'intervention par des correctifs en urgence. De même, la possibilité à mettre en œuvre une solution de haute disponibilité éventuellement sur plusieurs sites demeure un aspect indispensable pour la continuité d'activité.
- L'indépendance vis-à-vis d'une connexion Internet ou de l'accès à un centre de données par Internet ainsi que la couverture géographique (DOM/TOM/COM/URB/RUR) si toutefois le mode de connexion dépendait d'une communication téléphonique.

D'autre part, la notion d'intégration vise également l'évaluation du niveau d'intégration fonctionnelle dans les limites suivantes :

- Le degré d'acceptation et de réception, voire d'adhésion du point de vue fonctionnel au sens de la fonction rendue aux utilisateurs. Il s'agit donc d'étudier l'acceptation de la part des différents agents (du premier degré, du second degré, des agents administratifs ou de laboratoires, mais également des étudiants, des lycéens, des collégiens ainsi que de leurs parents pour d'autres usages potentiels). L'avis des maîtrises d'ouvrages est dans ce sens déterminant.
- L'aisance du déploiement en matière d'organisation des remises, par les autorités locales d'enregistrement ou par des délégations de pouvoir, des paramètres de comptes et d'authentification. Le support physique requiert ici plus de procédures et apporte des contraintes fortes dès qu'il s'agit de grands nombres répartis sur un territoire large. De même, pour une même technologie, si plusieurs éléments secrets sont à configurer, installer ou transmettre, la difficulté apparaît croissante. De plus, les documents de politique d'accréditation qui ouvrent à une homologation vis-à-vis du RGS sont d'autant plus complexes à élaborer. En ce qui concerne l'adaptabilité aux situations rencontrées, les technologies apparaissent très différentes les unes des autres.
- Enfin, du point de vue de l'utilisateur, l'évaluation de l'utilisabilité ou de la facilité d'emploi d'une manière intuitive permet de donner une note de 'convivialité' dans cette phase d'insertion dans le système d'information au sens le plus large.

6. Domaine relatif à la pérennité globale

L'investissement dans un renforcement de l'authentification nécessite d'évaluer le temps d'usage minimal possible de la technologie ainsi mise en place, ne serait-ce qu'en raison du coût pécuniaire et humain qu'il recouvre. Les critères associés sont les suivants :

- La pérennité de la ou des organisations (sociétés industrielles, groupes de travail, comité de normalisation) qui promeuvent le système d'authentification. Si le produit est très innovant et peu partagé, il convient d'évaluer sa disponibilité dans la gamme ou dans l'offre des sociétés qui le développent, ainsi que les questions de maintenance associées aux différents modules, permettant ainsi de garantir les corrections de bugs ou d'attaques éventuels.
- De même, la question de maintenance peut être renforcée par une conformité stricte à une norme ou une interopérabilité de plusieurs constructeurs.

2.3 Processus de comparaison des types d'authentification par élaboration de RADARS

La comparaison de plusieurs types de technologie et in fine de plusieurs produits industriels est rendue possible par la mise au point des critères précédemment étudiés. Toutefois, cet objectif de vouloir mettre en relief les avantages de certains types par rapport à d'autres appelle des remarques et demande des précautions d'usage.

En effet, les critères étant définis en début de processus, la portée de l'étude n'est réelle que dans la mesure où ces critères sont pleinement partagés, pertinents et réels sur l'ensemble des technologies ainsi que dans les conclusions de l'étude. Il n'est donc pas possible d'en changer en cours d'étude ni d'en ajouter pour certaines technologies au risque de ne rien comparer.

Dès lors, la prise en compte de la spécificité des besoins pour tel groupe d'utilisateurs demande à affiner l'approche des critères. Cette approche doit être faite de manière uniforme pour ce groupe sans modifier la liste des critères de l'ensemble de l'étude et sans modifier l'évaluation de l'apport fonctionnel selon ces critères. Autrement dit, telle technologie dispose de tel avantage selon un critère précis mis en exergue, et quel que soit la communauté qui l'utilise, cet avantage demeure considéré comme tel, y compris par rapport à toutes les autres technologies. La prise en compte de l'aspect spécifique des besoins du groupe d'utilisateurs considéré se manifeste donc par un autre biais qui est la pondération relative des critères dans le contexte d'usage de ces technologies pour cette communauté précise ; ces pondérations demeurent fixes pour toute l'étude dédiée à ces types d'usage et seront éventuellement différentes pour un autre type d'usage. Ainsi la forme des radars peut varier d'une étude contextualisée à une autre.

Enfin, le choix d'usage d'une technologie par rapport à une autre sera plus évident pour une même communauté professionnelle si une pondération des critères a été élaborée pour cette population sur le périmètre de l'étude en fonction des risques identifiés pour le système d'information considéré.

3 Relevé des caractéristiques distinctives des types d'authentification étudiés

L'offre industrielle s'est étoffée depuis trois ans tant en nombre d'industriels présents sur ce nouveau marché qu'en types de technologies. Un découpage de cette typologie est présenté ci-dessous avec une brève description pour chacun des types dans ce qu'ils ont de plus significatif du point de vue de cette étude comparative.

3.1 Authentification forte par certificat sur support cryptographique physique

L'authentification par certificat dont le bi-clés est tiré sur le support cryptographique physique, quel que soit le facteur de forme et avec les procédures de remise en face à face, est de loin celui qui donne le plus de garanties d'authentification mais il présente la difficulté de déploiement sur une population nombreuse et périmètre géographique étendu. Par ailleurs, il demande un déploiement sur les postes (pilote de la carte à puce) et représente un investissement financier plus élevé. Il peut permettre d'être conforme au RGS si le produit de support est qualifié. Parmi les points forts, il faut noter la possibilité de réaliser les opérations cryptographiques (dont l'authentification du système d'exploitation du poste, la signature ou le chiffrement) en mode déconnecté (sans OCSP dans ces cas).

3.2 Authentification forte par certificat dans un magasin cryptographique non physique

Par contre, l'authentification par certificat dont le bi-clés est tiré sur le support cryptographique non physique, dans un magasin cryptographique logiciel même avec les procédures de remise en face à face, ne donne pas les mêmes garanties d'authentification et demande une étude de qualification prévue par le RGS notamment pour les certificats une étoile. Par exemple, les magasins cryptographiques de Microsoft pour les systèmes d'exploitation depuis XP ont fait l'objet d'articles dans la presse spécialisée de manière à illustrer la possibilité d'extraire les bi-clés et les certificats à l'insu de leur porteur. Des outils logiciels ont été diffusés depuis (voir le n° MISC n°66 – Mars Avril 2013 – Utilisation avancée de Mimikatz – p.8 et suivantes). Dès lors, les mécanismes de révocation (CRL ou même OCSP) sont eux aussi mis en échec et aucune autre protection ne pourrait contribuer à empêcher l'usage de ce certificat dérobé. L'impact de cette menace est donc très élevé. Une manière de renforcer ce service d'authentification peut être de le coupler avec un élément secret séquestre en base centralisée et de rendre l'usage du certificat plus robuste, après interrogation par un client logiciel de la base en question. Mais alors, la dépendance vis-à-vis des pilotes logiciels ainsi que de la connexion vient contrebalancer le gain en sécurité.

3.3 Authentification par génération d'authentifiant à partir d'un secret partagé sur support cryptographique physique ou logiciel sur un support tiers

L'authentification par gestion d'un secret cryptographique partagé entre le porteur et la base centralisée permet de déployer l'usage d'authentification par mot de passe à usage unique, bien connue sous le nom d'OTP (pour One Time Password). Plusieurs implémentations du générateur de mot de passe sont envisageables, les unes par logiciel, d'autres par matériel offrant des capacités variables de résistance au vol.

Par rapport à l'infrastructure de gestion de clés publiques, l'infrastructure de gestion de clé privées souffre de plusieurs inconvénients qui sont inhérents à la centralisation du secret : le service d'authentification dépend d'un point unique de défaillance (SPOF), qui même s'il est répliqué demande à être synchronisé de manière fine quant à la base de temps et la base des comptes. L'autre point marquant réside dans la protection de ces secrets ou des séquestres qui peut être lacunaire (attaque du serveur central ou attaque de la base de recouvrement chez le tiers de confiance doté de celle-ci). Dans les deux cas, des renforcements sont possibles mais des exemples récents ont montré que lors d'une défaillance de grande ampleur¹, la résilience est difficilement compatible avec le renforcement de la sécurité. En effet, pour permettre le second, il est courant de mettre en œuvre des supports cryptographiques physiques effectuant la génération des mots de passe à usage unique et d'être ainsi doté des attributs de l'authentification forte. De surcroît, il s'agit bien dans ce cas de l'authentification du porteur du token, qui doit par ailleurs connaître le code pin. Mais, en cas de compromission massive, la gestion de ceux-ci demande le retour en usine pour un changement des secrets embarqués – ce qui est coûteux en temps, en moyen, en personne – et la résilience est ainsi mise en doute.

Parmi les méthodes récemment apparues au titre de l'authentification renforcée, la possibilité de disposer de logiciels OTP embarqués sur des supports mobiles pourrait permettre de pallier tous ces inconvénients et permettrait de demeurer dans le groupe de l'authentification forte au regard des trois critères (ce que je sais, ce que je possède, ce que de connais), bien que la sécurité d'un support mobile ait été mise en cause à de multiples reprises ces dernières années. Reste pourtant la difficulté d'unifier une flotte de mobiles pour une population nombreuse. Cet aspect, qui relève d'un autre volet de la gestion du système d'information, n'est pas encore optimisé d'un point de vue technique et économique. Si le support mobile est d'une origine externe au périmètre du système d'information professionnel, la maîtrise est encore moins assurée.

D'autres technologies émergentes relevant du secret partagé sont apparues récemment et offre un traitement différencié de ces désagréments. Toutefois, le niveau de sécurité en est amoindri. Elles sont décrites ci-après.

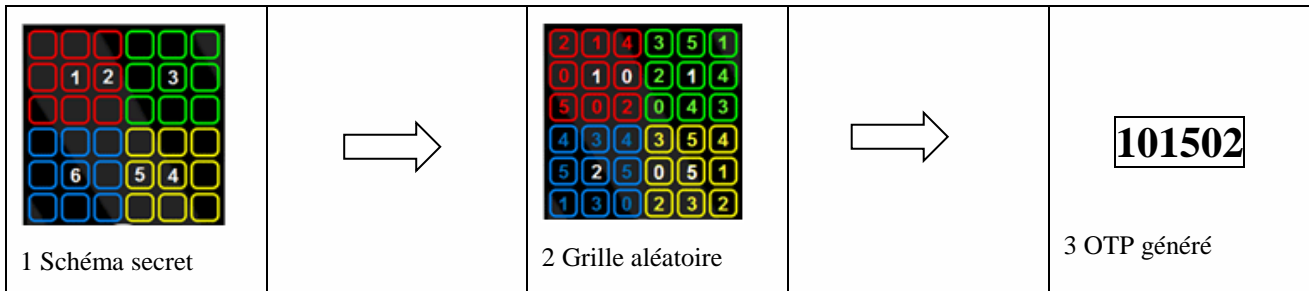
3.4 Authentification par grille

Ce moyen d'authentification peut être divisé en deux parties : d'une part une grille de caractères (généralement des chiffres) générée aléatoirement, d'autre part un schéma secret choisi par l'utilisateur qui représente une suite de position sur la grille. En superposant le schéma à la grille, on obtient une suite de caractères qui fait office d'OTP. Dans ce cas, la capture du mot de passe à usage unique n'est d'aucun effet sur la sécurité comme pour l'OTP en général. Aucun

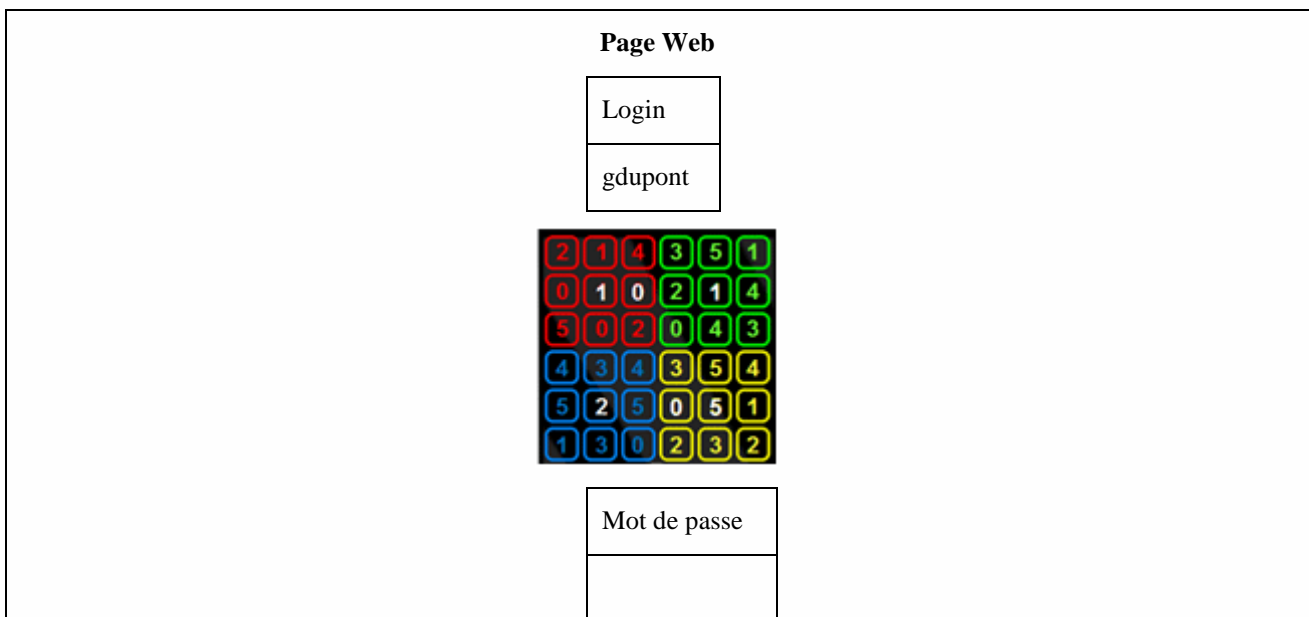
¹ <http://www.usinenouvelle.com/article/contre-le-piratage-rsa-va-remplacer-ses-cles-securid.N153386>

support matériel ni logiciel n'est à déployer. De même le partage de postes est possible sans surcoût et la résilience est élevée puisque le changement d'algorithme peut être effectué de manière centralisée. Alors que l'intégration fonctionnelle est similaire à celle des autres technologies, l'intégration technique est dépendante du degré d'industrialisation des fournisseurs. Il s'agit donc bien d'une authentification du porteur et non de celle de la machine ou du support délivrant le mot de passe à usage unique. Par contre, l'observation répétée peut mettre à mal cette technologie si toutefois ce facteur n'a pas été pris en compte dès la conception.

Ci-dessous le principe de choix de la grille par l'utilisateur Georges Dupont :



Et son utilisation lors de la connexion à une application web ; dans un premier temps, le fait de donner le login 'gdupont' permet à la base d'authentification de proposer une grille dynamique affectée à ce login précis :



Dans un second temps, la lecture des codes, avec pour masque la grille initialement fixée, permet de taper le code dans le champ 'mot de passe', comme l'indique le schéma ci-dessous. Il s'en suit que des observations répétées pourraient mettre à mal la grille choisie. Dès lors, cette proposition d'authentification pourrait convenir à un renforcement de l'authentification, en tant que première authentification, mais probablement pas comme seule et unique authentification pour l'ensemble du SI. A partir de cet exemple précis, d'autres conceptions de mise en œuvre de ces grilles dynamiques pourraient être proposées en dissociant la page de connexion de la page d'affichage de la grille ou en mutualisant cette page de grille aléatoire pour un ensemble de personnes s'y réfèrent. Ces différenciations d'une authentification par grille restent à explorer de manière à durcir la sécurité qui en résulte.

Page Web

Login
gdupont

2	1	4	3	5	1
0	1	0	2	1	4
5	0	2	0	4	3
4	3	4	3	5	4
5	2	5	0	5	1
1	3	0	2	3	2

Mot de passe
101502

3.5 Authentification par ‘invisible token’

Le jeton immatériel et invisible (ou ‘invisible token’ en anglais) utilise la technologie HTML5 pour générer un OTP via le navigateur à partir de plusieurs paramètres et d’une fonction cryptographique chargée par le navigateur. Parmi les paramètres figurent notamment une clé chiffrée et enregistrée, lors de l’enrôlement du système, dans l’arborescence des fichiers de celui-ci. C’est l’utilisation de ce paramètre dans le calcul cryptographique qui permet de réaliser l’authentification qu’elle soit par défi-réponse ou génération de jeton OTP basée sur d’autres calculs. Il s’agit donc d’un enrôlement de machine et non de personnes. Cette solution a l’avantage d’être relativement indépendante de la plateforme utilisée puisqu’elle utilise la technologie des navigateurs, avec la réserve toutefois de valider la solution pour chaque flotte identifiée – il sera problématique de traiter les postes échappant à toute maîtrise. Toutefois, il faut noter que c’est uniquement la machine (voire même uniquement le navigateur) qui est authentifiée et non l'utilisateur.

3.6 Authentification comportementale

Ces méthodes d’authentification sont basées sur la reconnaissance de schémas propres à l'utilisateur. On peut notamment citer l’analyse de la frappe au clavier ou bien la cohérence des heures et lieux de connexion au système. Cette méthode est généralement considérée comme un renforcement d’un autre mode d’authentification préalable.

3.7 Authentification par mot de passe

Moyen d’authentification le plus répandu, le mot de passe n’offre aujourd’hui plus une sécurité suffisante. La force d’un mot de passe est directement liée à sa longueur et aux types de caractères utilisés. Les mots de passe considérés sûrs sont donc peu pratiques d’utilisation (difficulté de mémorisation, longueur de la saisie), ce qui encourage les comportements pouvant entraîner sa compromission. Outre les attaques par recherche exhaustive ou dictionnaire, les mots de passe sont vulnérables aux méthodes d’ingénierie sociale (“phishing”) et à la saisie de frappe (“keylogging”). Répondre de la maîtrise d’une base de mot de passe et de son degré de compromission n’est pas aisé.

3.8 Authentification par identification d’éléments matériels liés aux supports de communication

Généralement associé à l’image de l’ADN, l’identification d’un grand nombre de caractéristiques matérielles des supports de communication peut fournir les éléments nécessaires à une authentification renforcée. Toutefois, ce mécanisme requiert l’installation d’un module logiciel qui préempte beaucoup d’information sur les supports utilisés et n’authentifie pas le porteur à proprement parlé.

4 Comparaisons de types d'authentification – adéquation aux besoins des différentes communautés professionnelles

4.1 Etudes de cas de solutions industrielles – superposition des radars

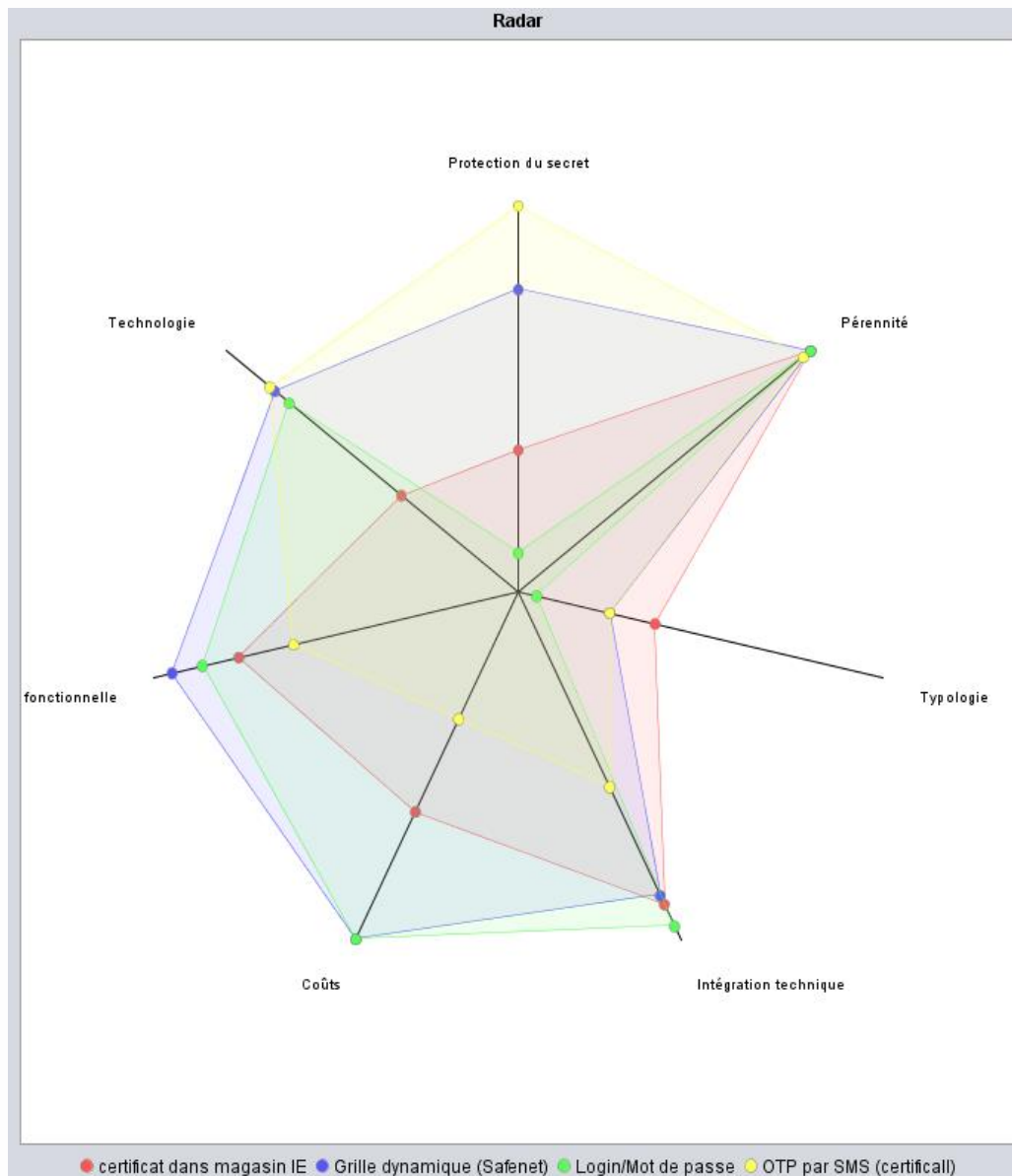
Les études effectuées ont donné lieu à la constitution de nombreux radars de manière à évaluer les (très) nombreuses implémentations industrielles des technologies considérées. Les graphiques qui suivent visent à présenter certaines d'entre elles. Les solutions industrielles présentent souvent un panel de plusieurs technologies exposées précédemment et sont donc polymorphiques. De manière à clarifier la comparaison qui suit, une seule technologie à la fois est utilisée. Une liste non exhaustive de solutions étudiées est présentée ci après, d'autres études sont en cours :

Famille	Description
OTP par téléphone, sms ou message vocal ou mail	Authentification sur challenge téléphonique : la sécurité est apportée par le fait que c'est toujours le système qui appelle sur des numéros préenregistrés. Avec code pin ou simple confirmation
Multiple (OTP logiciel, OTP physique installés, etc.)	Authentification par OTP sur divers supports physiques ou logiciels
OTP logiciel / à la demande + authentification du support	Authentification multiple
OTP visuel	Challenge-response : le système demande certaines lettres d'une réponse enregistrée par l'utilisateur, directement sur la page de login ou SMS/email
OTP matériel	Token USB sans drivers à lecture de code temporaire
Biométrie	Authentification via frappe au clavier plus autres facteurs (adresse IP, heure de connexion, version du navigateur...)
Carte à puce multiservices	RFID, OTP, certificats spécifiques (signature, chiffrement, authentification) sur le même support. Conforme au RGS, présente tous les services d'OTP, de carte à puce comme support pour la signature, l'authentification, le chiffrement, ainsi que la reconnaissance visuelle (carte agent), l'identification par RFID ou par bande magnétique.
Token USB/Certificat	Carte à puce mono usage sous un seul facteur de forme
Marquage de nombreuses caractéristiques des supports physiques des systèmes connectés	Identification des équipements électroniques par une combinaison unique de facteurs
Grilles Dynamiques	Elaboration d'un OTP à partir d'une forme choisie à l'origine
Risk-Based/Adaptive Authentication	Authentification comportementale basée sur les usages statistiques moyens(horaire de connexion, adresse ip de provenance, usage de la connexion, etc.)

Parmi les industriels rencontrés figurent Nexims – Certificall, RSA – Securid, IN-WEBO, Login People - ADN du Numérique, CA – ArcotId, SafeNet – GrIDSure / eToken PRO Smart Card, Winfrasoft – PINgrid / PINpass / PINphrase, AuthenWare - Identity Authentication, Google - Google Authenticator, Gemalto, Yubico – YubiKey, etc.

L'outil développé par Pascal Colombani et Sofiane Flih peut être fourni sur demande et permet d'être enrichi en critères supplémentaires. Il conduit à superposer des radars pour visualiser l'écart par rapport à un idéal recherché et permet de disposer d'un cadre d'évaluation commun. Cet outil traduit une méthodologie comparative mise en commun pour évaluer et visualiser les évaluations des technologies à venir et des implémentations de celles-ci dans le

Ci-dessous un exemple des cas à étudier.



4.2 Conséquences des évaluations

Le résultat de ces études montre que les différentes technologies d'authentification renforcée ne sont pas du tout équivalentes. Bien plus, elles s'adaptent en fait à des populations très ciblées aux problématiques spécifiques qu'il faut préalablement avoir bien analysées de manière à répondre aux besoins réels. L'objectif étant clairement de permettre de reprendre la maîtrise de la sécurité périmétrique progressivement et sans modification du parc applicatif, puis dans un second temps, à moyen terme de permettre de converger vers une authentification forte au sens du RGS, tel qu'il est défini aujourd'hui. L'étude a également permis d'aborder la question de la mise en place de tels bouquets d'authentification sans perturber l'existant tant sur le plan du parc applicatif que sur le plan des infrastructures d'authentification déjà en place : le fait d'adjoindre un accès, annexe à ceux existants, muni à la fois de ce nouveau type d'authentification renforcée et de la fonction de fédération d'identité SAML V2, permet de doter un système d'information d'une nouvelle porte d'entrée dont les propriétés de confiance se propagent à l'ensemble de la fédération sans altérer l'existant, d'une manière très simple.

Annexe

Bibliographie

Voir le rapport de stage de Sofiane FLIH sur le sujet de l'authentification renforcée et la constitution de l'outil d'évaluation qui sera publié en janvier 2014.

Deux articles connexes nous ont été signalés durant l'étude par Dominique Launay sans que l'on ait pu les exploiter étant donné leur approche différente de la problématique de l'authentification renforcée mais également faute de temps :

- le premier : une évaluation comparative de méthodes d'authentification web aborde le thème sous l'angle de la maturité technologique de sécurité des grandes familles d'authentification renforcée, sans orientation sur la constitution de radars ni la prise en compte des aspects d'architecture d'intégration. Cet article est très élaboré dans son étude et mérite une lecture approfondie qui reste à faire.

<http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf>

- Le second concerne une évaluation d'un produit d'un l'industriel par Surfnet qui est l'équivalent de RE-NATER aux Pays-Bas. Au-delà du cas précis de ce produit, c'est la méthodologie qui est à analyser. Dans cet article également, une étude fouillée serait à faire pour continuer la présente étude et l'enrichir.

http://www.surfnet.nl/documents/rapport_201105_evaluation_vasco_dp_nano_1_0_0.pdf