RSA®

The Security Division of EMC

Livre blanc

RSA Authentication Decision Tree: Choisir la solution d'authentification la mieux adaptée aux besoins de votre entreprise

« Quelle est la solution d'authentification la mieux adaptée à mon entreprise ? »

Partout dans le monde, cette question résonne comme un leitmotiv. Avec l'émergence de nouveaux produits de sécurité qualifiés de « remèdes miracles » par les spécialistes, l'offre de solutions d'authentification est aujourd'hui devenue pléthorique. Aussi, avant de faire leur choix, les entreprises se doivent d'entamer une réflexion globale autour des besoins d'authentification de leurs utilisateurs, des menaces contre lesquelles elles doivent se protéger, de leurs objectifs et des contraintes réglementaires propres à leur secteur.

Pour leur faciliter la tâche, RSA a mis au point un outil d'aide à la décision baptisé Authentication Decision Tree. Son objectif : permettre aux entreprises de cerner, d'évaluer et de choisir la solution d'authentification la mieux adaptée aux besoins de leurs utilisateurs et de leur activité. Grâce à ce cadre décisionnel, elles peuvent affiner leur choix parmi les nombreuses solutions d'authentification disponibles, en fonction de cinq critères clés. Ce livre blanc vous invite à découvrir l'Authentication Decision Tree, avant de passer en revue les cinq critères clés à prendre en compte pour le choix d'une solution d'authentification. Son objectif : vous proposer un guide pratique de sélection d'une solution conciliant vos différents paramètres de risques, coûts et commodité pour l'utilisateur final.

Le besoin d'authentification forte

La protection de l'accès aux informations, et la garantie des identités des utilisateurs demandant cet accès, constituent la base de toute stratégie de sécurité. Jusqu'ici stimulé par le besoin de sécurisation des accès distants aux informations de l'entreprise, l'essor de la demande d'authentification forte à divers niveaux de l'entreprise s'explique aujourd'hui par la convergence de plusieurs facteurs.

Emergence de nouvelles applications métier en ligne. Motivées par le potentiel commercial et les économies réalisables grâce à un accès en ligne aux informations, de nombreuses entreprises migrent une part croissante de leurs applications métier sur le Web.

Augmentation de la demande d'accès distants. La mondialisation de l'économie et la mobilité accrue des personnels ont contraint de nombreuses sociétés à ouvrir le système d'information et donner aux employés accès aux informations, à toute heure du jour et en tout point du globe. Le but : maintenir les niveaux de productivité de leurs collaborateurs distants.

Élargissement des droits d'accès à de nouvelles catégories d'utilisateurs. Sous-traitants, partenaires et fournisseurs exigent aujourd'hui de pouvoir bénéficier d'un accès à la demande aux informations de l'entreprise dont ils ont besoin: prévisionnels de vente, veille concurrentielle, grilles tarifaires, état des stocks et données clients.

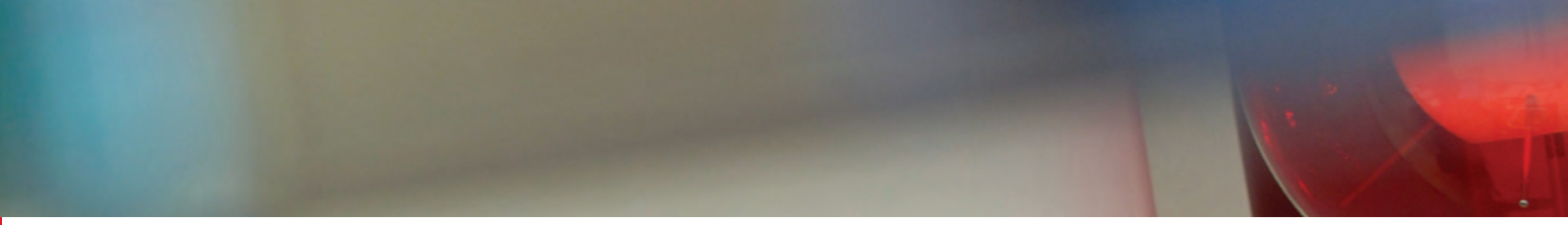
Essor des portails clients. Les clients sont aujourd'hui de plus en plus nombreux à vouloir accéder à leur compte en temps réel pour gérer leurs données en ligne.

Conformité règlementaire. Avec l'intensification de la pression règlementaire ces dernières années, les entreprises sont contraintes d'adopter des mesures de sécurité destinées à bloquer tout accès non autorisé.

Sophistication des menaces. Selon l'utilisateur et la nature de l'information, il existe de nombreuses menaces qui imposent la mise en place de dispositifs d'authentification forte afin de limiter les risques. Ainsi, pour les utilisateurs en entreprise, il convient d'adopter une authentification forte afin d'éviter les risques d'accès non-autorisé à des données sensibles stratégiques pour la vie de l'entreprise et de lutter donc contre les menaces internes. Pour ce qui est des clients, les entreprises doivent leur assurer une protection proactive contre les attaques de type phishing, chevaux de Troie et autres formes de logiciels malveillants (malware).

Authentification des utilisateurs : état des lieux

Malgré les faiblesses communément admises de l'authentification par simple mot de passe, son utilisation continue de prévaloir comme outil dominant de vérification de l'identité des utilisateurs. Bien que considérée comme une méthode d'authentification « gratuite », l'authentification par simple mot de passe se révèle aujourd'hui être très coûteuse sur le plan de la gestion



récurrente et du support. D'après Forrester Research, le coût de main d'œuvre moyen pour la simple réinitialisation d'un mot de passe s'élève à près de 70 dollars US.

L'apparition sur le marché de nouvelles méthodes d'authentification complique encore la tâche des entreprises au moment du choix d'une stratégie d'authentification forte. Au sein des grands groupes, les authentificateurs matériels restent la solution privilégiée pour sécuriser l'accès aux ressources de l'entreprise. Toutefois, la mobilité accrue des collaborateurs et l'utilisation répandue des téléphones mobiles et autres assistants personnels (PDA) entraîne une hausse de la demande d'authentificateurs logiciels. Sur les portails grand public, l'authentification basée sur le risque et l'authentification sur base de connaissances sont plébiscitées pour leur simplicité d'utilisation et leur évolutivité sur des bases d'utilisateurs de masse.

Devant l'étendue de l'offre, les entreprises peinent à déterminer l'orientation de leur stratégie d'authentification. Elles ont en effet le choix entre plusieurs solutions d'authentification en fonction de critères comme le type d'utilisateurs, l'importance des données à protéger, la portabilité et la qualité d'expérience utilisateur. Pour les aider à évaluer ces différentes options et à trouver celle en phase avec les besoins de leurs utilisateurs et de leur activité, RSA a mis au point l'Authentication Decision Tree.

Facteurs critiques à intégrer dans l'élaboration d'une stratégie d'authentification

L'élaboration d'une stratégie d'authentification appropriée repose sur l'analyse de cinq facteurs clés :

- L'importance des données à protéger
- Le niveau d'authentification utilisateur à appliquer
- L'usage prévu
- Les besoins des utilisateurs finaux
- L'environnement technique

L'importance des données à protéger

Le premier critère à prendre en compte concerne l'importance des données à protéger et le coût résultant d'un accès non autorisé à ces données. Données propriétaires, coordonnées bancaires, numéros de carte de crédit, dossiers de santé ou toute information d'identification personnelle : toutes ces données peuvent être considérées comme appartenant à la catégorie des informations sensibles. Tout accès non autorisé à ce type d'information peut avoir de lourdes conséquences financières, à l'image des coûts qu'un établissement bancaire devra supporter en cas de transferts de fonds non autorisés effectués à partir des comptes de certains clients – sans parler du déficit d'image pour la société en question. Plus les informations ont une valeur importante, plus le risque est élevé pour l'entreprise en cas d'accès non autorisé, et plus la solution d'authentification devra être forte.

Le niveau d'authentification utilisateur à appliquer

L'étude des catégories d'utilisateurs et du type d'informations auxquelles ces utilisateurs ont accès permet de déterminer le niveau d'authentification à appliquer par l'entreprise. De fait, les entreprises n'ayant pas le pouvoir d'imposer une authentification à leurs clients, elles privilégieront pour le choix de la solution des critères de commodité et de facilité d'adoption par les clients. En revanche, pour leurs collaborateurs et partenaires, les entreprise auront davantage de contrôle sur les types d'authentification à mettre en place et considéreront donc en priorité des critères comme la portabilité, le coût total de possession (TCO) et les coûts de gestion.

L'usage prévu

Le déploiement d'une solution d'authentification répond souvent à plusieurs objectifs. En d'autres termes, l'entreprise pourra décider d'aller au delà de la simple vérification d'identité et de mettre en place des niveaux d'authentification supplémentaires, en fonction de l'utilisateur et des types d'opérations effectuées. Par exemple, un établissement financier cherchant à réduire ses pertes dues à la fraude pourrait implémenter une solution de surveillance des transactions sur les transferts à haut risque. Autre exemple : pour ses collaborateurs amenés à échanger des informations sensibles (RH, paye, données financières, etc.), une société pourra exiger la mise en place d'une solution d'authentification comportant un dispositif de cryptage des fichiers et des e-mails.

Les besoins des utilisateurs finaux

Pour le déploiement d'une solution d'authentification sur une population d'utilisateurs finaux, de multiples critères devront être pris en compte en fonction des profils. Du point de vue des utilisateurs, les entreprises devront intégrer les critères de simplicité d'utilisation et de volonté d'adoption, ainsi que le type d'informations auxquelles l'utilisateur aura accès. Du point de vue de l'entreprise, d'autres paramètres devront être ajoutés à l'équation : coût total de possession (TCO), besoins de formation, évolutivité de la solution pour la prise en charge de nouveaux utilisateurs, et mobilité.

L'environnement technique

Dernier point, l'environnement technique de déploiement permet de déterminer d'autres facteurs comme le niveau d'authentification à appliquer. Ainsi, dans un environnement où les postes de travail sont fortement contrôlés et équipés d'anti-virus à jour, les critères de sécurité ne seront pas aussi stricts que dans un cadre où l'environnement utilisateur est moins contrôlé et où une majorité de la population utilisateurs accèderaient au réseau à distance des quatre coins du globe.

Autre critère technique à prendre en compte : le parc de matériels utilisateur pour l'accès. Dans un environnement applicatif d'entreprise ou orienté client, les utilisateurs finaux sont susceptibles d'accéder à l'information à partir d'un large éventail de périphériques – ordinateurs fixes et portables, PDA, téléphones mobiles ou autres bornes d'accès. Le type de périphérique utilisé permet alors de déterminer les formes des facteurs d'authentification proposés aux utilisateurs finaux.

L'Authentication Decision Tree

Émergence de nouvelles méthodes et technologies d'authentification, augmentation de la valeur des données, demandes d'accès aux réseaux et aux applications provenant de nouvelles catégories d'utilisateurs, prolifération de menaces sophistiquées, complexification du contexte règlementaire… les effets conjugués de tous ces éléments contraignent les entreprises à réévaluer leur stratégie d'authentification en place.

Cependant, face à une telle profusion de solutions et au buzz qui entoure certaines technologies d'authentification, les entreprises ont souvent du mal à y voir clair. Les solutions biométriques bénéficient par exemple d'une couverture médiatique inversement proportionnelle à leur déploiement effectif. En effet, avec leurs systèmes de lecture coûteux et encombrants, ces solutions se révèlent au final peu conciliables avec les solutions d'accès mobile ou distant, et difficilement généralisables au grand public.

Le niveau de contrôle de l'environnement utilisateur constitue un critère essentiel dans le choix de la méthode d'authentification la plus appropriée.

L'Authentication Decision Tree de RSA a été conçu pour permettre aux entreprises d'évaluer objectivement leur besoins utilisateurs et métier au regard de l'offre existante. Le but : faciliter le processus décisionnel. L'intérêt d'un tel arbre décisionnel provient du manque actuel d'une solution universelle adaptée à tous les scénarios, à toutes les contraintes des entreprises et à l'ensemble des besoins de sécurité des utilisateurs. Aujourd'hui, les entreprises peuvent s'appuyer sur cet outil pour choisir la solution d'authentification la plus appropriée, voir panacher plusieurs solutions, en tenant compte des différents critères de risques, de coûts et de commodité pour l'utilisateur.

Authentication Decision Tree : mode d'emploi

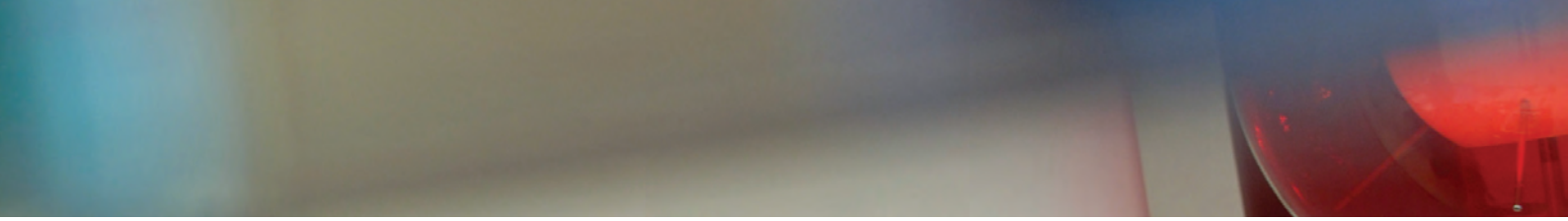
Pour déterminer la ou les solutions les mieux adaptées à votre entreprise, l'Authentication Decision Tree de RSA analyse plusieurs critères :

- Le niveau de contrôle de l'environnement utilisateur
- Les méthodes d'accès utilisées
- La demande d'accès aux applications et aux données, en tout lieu et à tout moment
- La nécessité de crypter les disques, les fichiers ou les e-mails
- La prévention de la fraude

Le niveau de contrôle de l'environnement utilisateur

Le niveau de contrôle de l'environnement utilisateur constitue un critère essentiel dans le choix de la méthode d'authentification la plus appropriée. L'entreprise a-t-elle le droit d'installer un logiciel sur le système de l'utilisateur ? Peut-elle imposer le système d'exploitation sur lequel l'utilisateur doit travailler ? Tels sont les exemples de questions à se poser.

Mais pourquoi est-ce si important ? La compatibilité des solutions d'authentification avec les systèmes d'exploitation (OS) n'étant pas universelle, il est par conséquent primordial de s'interroger sur le niveau de contrôle de l'entreprise sur l'OS. En entreprise, la direction des services informatiques (DSI) contrôle les systèmes d'exploitation installés sur les équipements des utilisateurs. Ce n'est, en revanche, pas le cas des OS des utilisateurs externes (clients ou partenaires) – d'où la nécessité de proposer des méthodes d'authentification différentes pour ces groupes d'utilisateurs.



Les méthodes d'accès utilisées

Les méthodes d'accès jouent un rôle essentiel dans l'élaboration d'une stratégie d'authentification. Certaines méthodes d'authentification ne fonctionnent que pour l'accès aux applications Web, tandis que d'autres peuvent être utilisées pour l'accès à des applications hors ligne. La prise en compte de l'utilisateur, de ses droits d'accès et du type d'utilisation prévu influencent directement les méthodes d'authentification retenues.

La demande d'accès aux applications et données, en tout lieu et à tout moment

La mondialisation de l'économie et la mobilité accrue des collaborateurs ont fait exploser la demande d'un accès permanent aux données, partout dans le monde. La continuité d'activité repose aujourd'hui en grande partie sur l'ouverture d'un accès sécurisé aux données de l'entreprise. Pour les collaborateurs ou les partenaires, l'accès 24h/7j aux données de l'entreprise en tout point du globe constitue un critère essentiel au maintien de leur productivité. Côté clients, ce type d'accès compte pour beaucoup dans le niveau de satisfaction. Quelques exemples de questions à se poser pour l'évaluation de certains critères clés :

- Devons-nous mettre en place un accès utilisateur à partir d'une grande variété de sites distants ?
- Devons-nous mettre en place un accès utilisateur à partir de systèmes hors de notre contrôle (bornes publiques, systèmes d'accès dans les hôtels, stations de travail partagées, etc.) ?
- Devons-nous mettre en place un accès utilisateur à partir de divers terminaux (PDA et téléphones mobiles) ?

Cryptage des disques, fichiers ou e-mails

Dans l'évaluation de leur stratégie d'authentification, les entreprises devront tenir compte des autres objectifs métier impactés par la méthode d'authentification choisie. Ainsi, prenons l'exemple d'un organisme de santé soumis aux règlementations HIPAA. Ce type de structure a pour obligation de crypter des données de santé protégées ou toute autre information d'identification personnelle d'un patient lors des différents transferts d'informations d'un service à l'autre. Dans notre exemple, l'établissement de santé pourra exiger des personnes détentrices des droits d'accès à ces informations qu'elles y accèdent uniquement à partir de machines réputées sûres.

Prévention de la fraude

Dans le cadre de la lutte anti-fraude, certaines méthodes d'authentification sont requises pour la surveillance des transactions et des actions effectuées par un utilisateur bien que celui-ci ait été authentifié initialement lors de sa connexion. Si ce scénario concerne essentiellement les services financiers, d'autres secteurs d'activité commencent à faire l'objet d'attaques – par phishing et malware – perpétrées par des malfaiteurs dans le seul but de collecter des données personnelles qui serviront à usurper des identités pour commettre des fraudes à but lucratif.

Une multitude de possibilités d'authentification

Authentification par mot de passe

Il s'agit d'une authentification mono-facteur utilisée pour vérifier l'identité des utilisateurs. Même si ce système ne représente aucun coût d'achat initial, les coûts de gestion courante et de support à long terme (pour la réinitialisation d'un mot de passe, par exemple) peuvent s'avérer prohibitifs pour l'entreprise. Facilement piratables ou communiqués à des tiers sans autre forme de précaution, les mots de passe n'offrent pas un niveau de sécurité suffisant.

Authentification basée sur les connaissances

Ce type d'authentification permet d'authentifier une personne sur la base de certaines informations personnelles corroborées par un processus d'interrogation interactif en temps réel. Les questions posées à l'utilisateur se basent sur l'analyse d'informations contenues dans plusieurs bases de données publiques. Ces questions – inconnues jusqu'alors de l'utilisateur – lui sont posées de manière aléatoire.

Authentification basée sur les risques

Baptisée RBA (Risk-Based Authentication), cette technologie d'authentification mesure plusieurs indicateurs de risques en arrière-plan afin de vérifier l'identité des utilisateurs et/ou d'authentifier leurs activités en ligne. Ces indicateurs portent sur certaines caractéristiques des équipements, les profils comportementaux des utilisateurs et des paramètres de géolocalisation d'adresses IP. Plus le niveau de risque présenté est élevé, plus la probabilité de fraude sur l'identité ou l'action observée est grande. Si le moteur d'analyse des risques (Risk Engine) établit que la requête d'authentification comporte un risque supérieur aux seuils acceptables, l'authentification RBA suggère de monter d'un cran la procédure d'authentification. Dans ce cas, l'utilisateur pourra être invité à répondre à certaines questions spécifiques ou à communiquer un code d'autorisation envoyé sur son mobile (SMS) ou par e-mail.

Authentification par mot de passe à usage unique

Solution d'authentification à deux facteurs la plus utilisée, l'authentification par mot de passe à usage unique – également appelée authentification OTP (One-Time Password) – s'appuie sur une information que vous connaissez (un code ou un mot de passe) et un objet que vous possédez (un authentificateur). L'authentificateur génère un nouveau mot de passe à usage unique (ou code OTP) toutes les 60 secondes, rendant ainsi la tâche impossible à toute personne autre que l'utilisateur légitme , de saisir le bon code à un moment donné.

Pour accéder aux informations ou aux ressources protégées par un mot de passe à usage unique, les utilisateurs doivent associer leur code confidentiel (ou code PIN, Personal Identification Number) au code qui s'affiche sur l'écran de leur authentificateur (token code) au moment de l'authentification. Résultat : l'identité de l'utilisateur est pleinement validée grâce à ce code à usage unique.

Cette technologie se décline sous plusieurs formes :

- **Authentificateurs matériels.** Généralement, ces authentificateurs matériels (ou « key fobs » en anglais) se présentent sous la forme de petits appareils portables qui peuvent être accrochés à un porte-clés. Il s'agit de la solution idéale pour les utilisateurs qui privilégient les solutions « tangibles » ou qui doivent pouvoir accéder à leur compte utilisateur en différents endroits.
- **Authentificateurs logiciels (pour PC, clés USB ou autres terminaux mobiles) :** Généralement, les authentificateurs logiciels sont proposés sous la forme d'une application ou d'une barre d'outils installée de manière sécurisée sur le poste de travail, l'ordinateur portable ou l'appareil mobile de l'utilisateur.
- **Authentification on-demand.** Ce type d'authentification repose sur l'envoi d'un mot de passe à usage unique « à la demande » par SMS sur le terminal mobile ou à l'adresse e-mail enregistrée de l'utilisateur. À réception de ce code OTP, l'utilisateur le saisit avec son code PIN pour pouvoir accéder au réseau de l'entreprise ou à une application en ligne.

L'authentification par mot de passe à usage unique s'appuie sur une information que vous connaissez (un code PIN ou un mot de passe) et un objet que vous possédez (un authentificateur).

Certificats numériques

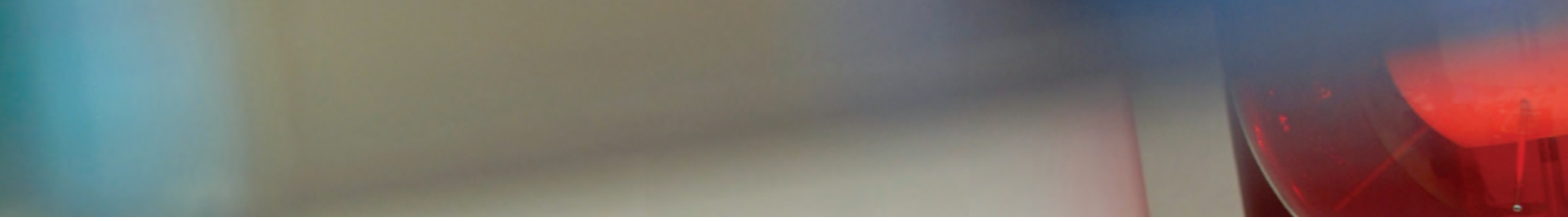
Un certificat numérique est un document électronique unique qui contient les éléments d'identification de la personne ou de la machine à laquelle il est associé. Ce certificat peut être stocké sur un poste de travail, une smart card ou une clé USB. Pour une authentification forte à deux facteurs, le certificat numérique peut être verrouillé sur une smart card ou une clé USB, exigeant que l'utilisateur saisisse un code PIN pour déverrouiller le certificat et utiliser l'habilitation. Ce certificat numérique permet ensuite d'authentifier l'utilisateur qui souhaite accéder au réseau ou à une application. Le rôle des certificats numériques ne se limite pas uniquement à authentifier les utilisateurs. Ils peuvent également servir à l'activation de signatures numériques ou au cryptage d'e-mails.

Il est également possible d'associer les certificats numériques aux systèmes d'authentification OTP à l'aide d'un authentificateur hybride. Cet authentificateur hybride stocke alors plusieurs habilitations pour optimiser l'expérience utilisateur. Exemple classique d'utilisation d'un authentificateur hybride certificat/OTP : le déverrouillage d'un disque dur crypté à l'aide d'un certificat numérique, suivi d'une procédure d'authentification sur un VPN à l'aide d'un mot de passe à usage unique.

Analyse des attributs d'authentification

Une fois les impératifs métier et les besoins des utilisateurs évalués, l'entreprise peut définir sa stratégie d'authentification à partir de l'offre disponible. Il s'agit alors de trouver le compromis idéal entre plusieurs variables :

- Niveau de sécurité
- Schéma d'utilisation classique
- Contraintes côté client
- Portabilité
- Usages multiples
- « Challenges » des utilisateurs
- Contraintes de diffusion
- Configuration système requise
- Coût



L'Authentication Decision Tree de RSA permet aux entreprises de comparer les différentes méthodes d'authentification conçues pour répondre à leurs besoins. Cette matrice décisionnelle évalue de manière objective les solutions d'authentification leaders du marché.

Même si le coût représente un critère important, les entreprises devront tenir compte d'autres facteurs dans le choix de la solution la mieux adaptée. Elles ont en effet trop souvent tendance à se focaliser sur le coût d'acquisition.

Or, l'exemple de l'authentification par simple mot de passe suffit à prouver que le prix d'achat ne peut constituer à lui seul un critère de choix. Si les mots de passe sont « gratuits » en termes de coût d'acquisition, ils se révèlent étonnamment coûteux en termes de gestion courante et de support.

Le tableau comparatif des pages 8 et 9 analyse chaque option d'authentification au regard des neuf variables précitées.

Scénario d'utilisation de l'Authentication Decision Tree

Profil de l'entreprise

Un grand organisme de santé gérant plusieurs hôpitaux régionaux et centres spécialisés desservant plus de 1,5 million de patients.

Groupes d'utilisateurs

Médecins, organismes payeurs et complémentaires santé, patients, fonctions administratives

Impératifs métier et besoins des utilisateurs

Constamment en mouvement, les médecins et personnels soignants se déplacent d'un site à l'autre et doivent garder un accès permanent aux dossiers médicaux de leurs patients par le biais de leur Blackberry ou de tout autre terminal mobile. Ce dispositif leur garantit un accès instantané et sécurisé aux dossiers médicaux dès qu'ils en ont besoin, pour une qualité de soins optimale.

De leur côté, les organismes payeurs et les complémentaires santé doivent pouvoir accéder aux dossiers des patients, à leur historique médical et aux services dont ils ont bénéficié pour pouvoir régler les factures ou solutionner les différends.

Quant aux fonctions administratives des établissements de santé, elles doivent en permanence pouvoir accéder aux dossiers médicaux protégés et aux informations d'identification personnelle des patients. De l'agent administratif jusqu'à la personne chargée de la facturation, l'accès aux informations du patient est un critère de performance essentiel au bon déroulement des missions de chacun.

Enfin, les patients ont accès à leurs données personnelles et à leur historique médical par le biais d'un portail Web. Outre les fonctions de mise à jour de leurs données personnelles, ils bénéficient également de plusieurs services pratiques en ligne : prise de rendez-vous, demandes de renouvellement d'ordonnance et règlements des prestations de santé.

Solutions d'authentification possibles

Face à la multiplicité des besoins des utilisateurs et à la diversité des systèmes auxquels ils doivent pouvoir accéder, cet organisme de santé se doit de passer en revue un très large éventail de solutions d'authentification :

Personnels soignants : authentification par mot de passe à usage unique via un logiciel conçu pour les terminaux mobiles

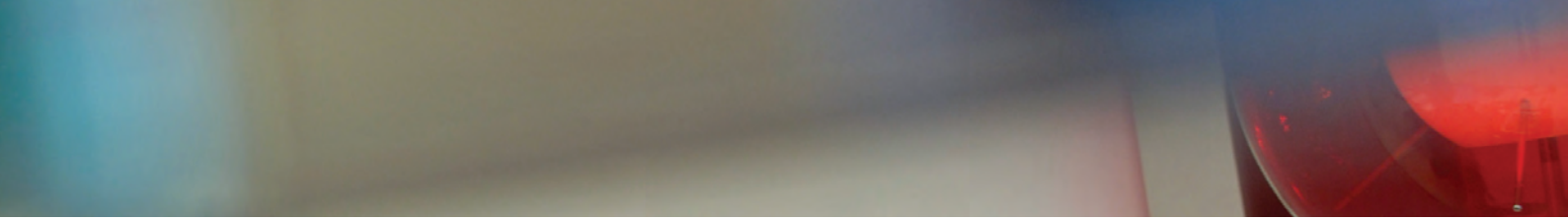
Organismes payeurs et complémentaires santé : tokens matériels

Fonctions administratives : tokens matériels

Patients : authentification basée sur les risques

Les entreprises ont en effet bien trop souvent tendance à se focaliser sur le coût d'acquisition. Or l'exemple de l'authentification par simple mot de passe suffit à prouver que le prix d'achat ne peut constituer à lui seul un critère de choix.

	Authentification par mot de passe	Authentification basée sur les connaissances	Authentification basée sur les risques	Authentification par mot de passe à usage unique (OTP) : tokens matériels	Authentification hybride : OTP et certificat numérique	
Niveau de sécurité	Mono facteur, facilement piratable, transmissible...	Renforcé (mono facteur) Connaissances singulières	Deux facteurs, ou plus, selon le niveau de risque évalué	Deux facteurs : code PIN + code affiché sur le token	Deux facteurs : code PIN + code affiché sur le token ou certificat	
Schéma d'utilisation classique	Non réglementé Applications peu stratégiques	Inscription de nouveaux utilisateurs Accès d'urgence, réinitialisation du code PIN	Applications à usage public ou accès à un VPN SSL	Accès des collaborateurs nomades	Collaborateurs intra-entreprise et en déplacement	
Contraintes côté client	Aucune	Aucune	Aucune	Aucune	Middleware pour les fonctions connectées	
Portabilité	Universelle	Universelle	Applications Web	Universelle	Universalité de l'authentification OTP	
Usages multiples	Non	Non	Plate-forme dédiée à la surveillance des transactions et à la détection des fraudes	Non	Cryptage de fichiers/e-mails Signature numérique Accès distant	
« Challenges » des utilisateurs	Oublis fréquents et problèmes de sécurité (mots de passe inscrits sur un bout de papier)	Minimes	Minimes à importants	Minimes	Minimes	
Contraintes de diffusion	Aucune	Aucune	Aucune	Attribution et envoi de tokens	Logiciel client certificat Token	
Configuration système requise	Annuaire d'utilisateurs	Service par abonnement	Serveur d'authentification Agents personnalisés Applications Web Option de service d'abonnement	Serveur d'authentification Agents d'applications	Autorité de certification Serveur d'authentification	
Coût	Faible coût d'acquisition, mais coûts de support élevés	Modérés	Faible coût, induit un certain niveau d'intégration d'applications	Coût d'achat important, mais faibles coûts de gestion	Coûts d'infrastructure et de gestion supérieurs	



	OTP : tokens logiciels installés sur PC	OTP : tokens logiciels sur clés USB	OTP : tokens logiciels sur terminaux mobiles	Code OTP transmis à la demande	Certificats numériques
	Deux facteurs, niveau de sécurité élevé : code PIN + token	Deux facteurs, niveau élevé (avec éventuellement protection biométrique)	Deux facteurs, niveau élevé : code PIN + code token	Deux facteurs, niveau élevé : code PIN + code envoyé par SMS	Verrouillable par code PIN, pour une authentification à deux facteurs
	Accès des collaborateurs nomades	Accès des collaborateurs nomades	Accès des collaborateurs nomades	Utilisateurs occasionnels ou temporaires Accès d'urgence Second facteur d'authentification IDA	Authentification des utilisateurs intra-entreprise ou authentification de machine
	PC compatible	Clé USB compatible	Plate-forme compatible	Tout équipement pouvant recevoir des e-mails ou des SMS	Conteneur ou périphérique (USB, smart card ou poste de travail)
	Fonctionne uniquement sur le système attribué	Fonctionnement universel, à condition d'avoir un port USB libre	Fonctionnement universel	En fonction de la couverture du service	En fonction du conteneur – une smart card nécessite un lecteur ou un port USB
	Non	Stockage de fichiers	Non	Non	Oui – authentification, signature numérique et cryptage
	Minime	Minime	Minime	Processus en deux étapes	Minime
	Attribution et transmission du logiciel et des seeds	Attribution et transmission du logiciel et des seeds	Attribution et transmission du logiciel et des seeds	Aucune	Aucune
	Serveur d'authentification Agents d'applications	Serveur d'authentification Agents d'applications	Serveur d'authentification Agents d'applications	Serveur d'authentification Agents d'applications Envoi de SMS	enrôlement des utilisateurs ou envoi automatique de certificats sur la machine client
	Inférieur aux tokens matériels	Élevé – terminal + token	Inférieur aux tokens matériels	Inférieur aux tokens matériels ou logiciels	Gestion du cycle de vie à prendre en compte

Les solutions RSA

Depuis plus de 20 ans, RSA est le leader des solutions d'authentification forte à deux facteurs. RSA propose aux entreprises de toutes tailles un large éventail de solutions d'authentification forte leur permettant de concilier leurs impératifs de maîtrise des risques, de coûts et de commodité pour l'utilisateur final.

RSA® Identity Verification

RSA Identity Verification fait appel à une technologie d'authentification basée sur les connaissances pour valider l'identité des utilisateurs en temps réel. RSA Identity Verification pose à l'utilisateur toute une série de questions spontanées, s'appuyant pour cela sur des informations recueillies dans des dizaines de bases de données publiques. En quelques secondes à peine, RSA Identity Verification confirme l'identité de l'utilisateur, sans aucun échange préalable avec ce dernier.

RSA Identity Verification améliore également la précision du niveau d'authentification grâce à son module Identity Event. Pour une procédure encore plus sécurisée et adaptée à la nature spécifique du risque, le module Identity Event mesure le niveau de risque associé à une identité, puis adapte automatiquement le degré de difficulté des questions en temps réel. Parmi les événements d'identité évalués :

- **Les recherches dans les sources d'information publiques.** Tout accès suspect aux rapports d'information publique d'un utilisateur donné.
- **La vélocité d'une identité.** Tout volume d'activité élevé associé à une personne, dans plusieurs entreprises.
- **La vélocité d'une adresse IP.** Plusieurs requêtes d'authentification générées à partir de la même adresse IP.

RSA® Authentication Manager Express

RSA® Authentication Manager Express est une plate-forme d'authentification forte multi-facteurs adaptée aux besoins des PME et entreprises de moins de 2 500 utilisateurs. Authentication Manager Express se déploie sur les VPN SSL et les applications Web leaders du marché pour garantir une authentification forte et un accès sécurisé aux applications et données protégées.

Authentication Manager Express s'appuie sur la technologie RBA (Risk-Based Authentication) développée par RSA, un système perfectionné qui mesure plusieurs indicateurs de risques en arrière-plan afin d'authentifier les identités des utilisateurs. Pour déterminer le niveau de risque associé à chaque demande d'accès, RSA Authentication Manager Express passe plusieurs paramètres d'identification au crible :

- Ce que connaît l'utilisateur (nom d'utilisateur et mot de passe, par exemple)
- Ce que possède l'utilisateur (ordinateur portable ou PC de bureau, par exemple)
- Ce que fait l'utilisateur (authentification ou activité récente sur son compte, par exemple)

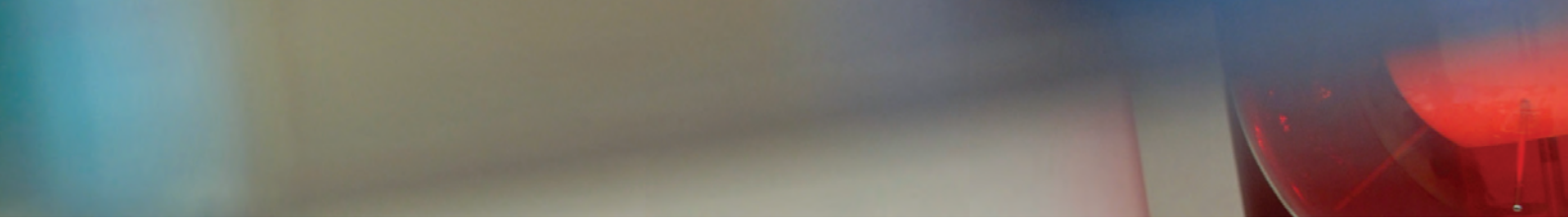
Lorsqu'une demande d'accès ne remplit pas les conditions d'authentification requises, RSA Authentication Manager Express peut déclencher des méthodes d'authentification additionnelles. Ceci est notamment le cas lorsqu'un utilisateur distant se connecte à partir d'une machine non reconnue, et jamais utilisée auparavant pour accéder au réseau. RSA Authentication Manager Express propose deux méthodes d'authentification supplémentaire : l'authentification hors bande par SMS et les réponses à certaines questions « challenge » spécifiques.

Livré sur une appliance prête à l'emploi (plug and play), RSA Authentication Manager Express prend en charge jusqu'à 2 500 utilisateurs.

RSA® Adaptive Authentication

Associant authentification multi-canaux et détection des fraudes, RSA® Adaptive Authentication est une plate-forme économique qui protège l'ensemble de la base d'utilisateurs. Adaptive Authentication introduit de manière active des identifiants supplémentaires par simple ajout d'un cookie et/ou d'un objet flash partagé (également baptisé « cookie flash »), qui sert ensuite d'identifiant unique du périphérique d'un utilisateur donné. La surveillance et l'authentification des activités des utilisateurs en fonction des niveaux de risques, des politiques internes et de la segmentation des utilisateurs permettent d'offrir un niveau de protection conjuguant puissance et commodité. Incluant la technologie RBA développée par RSA, Adaptive Authentication traque plus d'une centaine d'indicateurs (identification de matériel, géolocalisation des adresses IP, profils comportementaux, etc.) afin d'identifier les fraudes potentielles. Chaque activité se voit attribuer un niveau de risque. Plus ce niveau est élevé, plus le risque d'activité frauduleuse est important.

Adaptive Authentication propose un dispositif de surveillance actif en arrière-plan et totalement transparent pour l'utilisateur. Dès lors qu'une activité est jugée à haut risque, l'utilisateur est challengé pour fournir d'autres preuves de son identité. Dans la plupart des cas, ce



challenge consiste soit à répondre à une série de questions précises soit à faire une authentification téléphonique hors bande (un appel téléphonique est passé à l'utilisateur légitime qui doit confirmer les actions en cours, par exemple une demande de transfert, si ce n'est pas le cas la transaction est stoppée). Avec un taux de challenge utilisateur faible et un taux de complétude élevé (la technologie RBA suffit généralement à authentifier l'utilisateur sans autre forme d'identification) Adaptive Authentication offre un excellent niveau de protection pour un confort d'utilisation maximal – deux avantages qui destinent tout naturellement cette solution à des déploiements couvrant de larges bases d'utilisateurs.

RSA Adaptive Authentication est proposé en déploiement sur site ou en mode SaaS (Software as a Service). Cette solution particulièrement évolutive peut prendre en charge plusieurs millions d'utilisateurs.

RSA SecurID® Authentication

Solution OTP leader du marché, RSA SecurID® fait intervenir deux facteurs d'authentification : quelque chose que vous connaissez (un code PIN ou un mot de passe) et quelque chose que vous possédez (un authentificateur ou token). La solution d'authentification RSA SecurID fonctionne en associant une clé symétrique unique (ou « seed record ») à un algorithme éprouvé afin de générer un nouveau mot de passe à usage unique (ou OTP, One-Time Password) toutes les 60 secondes. Une technologie brevetée synchronise chaque authentificateur avec le serveur de sécurité, pour un niveau de sécurité optimal.

Pour accéder aux ressources protégées par le système RSA SecurID, les utilisateurs doivent associer leur code confidentiel (ou code PIN, Personal Identification Number) avec le code qui s'affiche sur l'écran de leur authentificateur (token code) à ce moment précis. Résultat : l'identité de l'utilisateur est pleinement garantie grâce à ce mot de passe unique et utilisable seulement une fois. Pour mieux répondre aux besoins des entreprises et de leurs utilisateurs, l'authentification RSA SecurID est disponible dans plusieurs formats :

Authentificateurs matériels.

Particulièrement ergonomiques, ces authentificateurs matériels (ou « key fobs » en anglais) se présentent sous la forme de petits appareils portables qui peuvent être accrochés à un porte-clés. Il s'agit de la solution idéale pour les utilisateurs qui privilégient les solutions « tangibles » ou qui doivent pouvoir accéder à leur compte utilisateur en différents endroits.

Authentificateur hybride avec certificats numériques

L'authentificateur RSA SecurID 800 est un petit appareil hybride qui allie la simplicité et la portabilité de l'authentification SecurID à la puissance et la flexibilité d'une smart card, le tout au format d'une clé USB. Cet authentificateur gère les certificats numériques standards pour le cryptage de disques et de fichiers, l'authentification, la signature et d'autres applications. L'enregistrement des habilitations de domaine sur un périphérique de sécurité physique permet de renforcer la sécurité du processus d'authentification par simple mot de passe. En associant plusieurs habilitations et applications sur un seul et même support physique, RSA SecurID 800 offre une clé maîtresse qui permet de garantir une authentification forte dans un environnement informatique hétérogène, tout en conciliant simplicité et transparence pour l'utilisateur.

Authentificateurs logiciels

Les authentificateurs logiciels RSA SecurID utilisent le même algorithme que les authentificateurs matériels RSA SecurID. Leur avantage ? Ils évitent aux utilisateurs d'avoir à transporter avec eux un appareil dédié. Au lieu d'être stockée sur un support SecurID, la clé symétrique est conservée en toute sécurité sur le PC, le smartphone ou la clé USB de l'utilisateur.

Terminaux mobiles

Les authentificateurs logiciels RSA SecurID sont disponibles sur toute une panoplie de plates-formes de smartphones, dont BlackBerry®, Microsoft Windows® Mobile, Java™ ME, Palm OS and Symbian OS ainsi que les téléphones UIQ.

Pour plus d'informations sur l'utilisation de l'Authentication Decision Tree afin d'évaluer les solutions d'authentification les mieux adaptées à vos besoins, contactez votre conseiller commercial ou les partenaires de notre réseau de distribution, ou rendez-vous sur www.rsa.com.

Postes de travail Microsoft Windows®

Le token RSA SecurID pour postes de travail Windows réside sur un PC et peut être intégré automatiquement aux principaux clients d'accès distant.

Barre d'outils token OTP

RSA SecurID Toolbar Token conjugue l'aspect pratique des fonctions de saisie semi-automatique des applications Web avec la sécurité des dispositifs anti-phishing.

On-demand (envoi par SMS ou e-mail)

RSA On-demand Authentication envoie un mot de passe à usage unique « à la demande » par SMS sur le terminal mobile ou à l'adresse e-mail enregistrée d'un utilisateur. À réception de ce code OTP, l'utilisateur le saisit avec son code PIN pour accéder au réseau de l'entreprise ou à une application en ligne.

RSA® Certificate Manager

RSA® Certificate Manager est une solution d'autorité de certification en ligne dont les fonctionnalités principales permettent d'émettre, de gérer et de valider des certificats numériques. Outre son serveur Web sécurisé et son puissant moteur de signature permettant de signer numériquement les certificats des utilisateurs, la solution comprend un référentiel de données intégré pour pouvoir stocker des certificats, des données système et des informations relatives au statut des certificats. RSA Certificate Manager est la première solution certifiée Common Criteria et Identrust.

Basé sur des standards ouverts, Certificate Manager est interopérable avec des centaines d'applications standards. La solution peut être donc exploitée sur de nombreuses autres applications (navigateurs Web, clients de messagerie et VPN) garantissant un retour sur investissement maximal. La solution permet également de stocker les habilitations dans les navigateurs, sur des smart cards et tokens USB. Ainsi, les certificats numériques RSA peuvent être combinés avec l'authentificateur hybride SecurID 800 pour consolider plusieurs habilitations sur un seul et même appareil. Résultat : une expérience utilisateur parfaitement fluide. Parmi les autres composants intégrés dans RSA Digital Certificate, on trouve RSA Registration Manager, RSA Validation Manager, RSA Key Recovery Module et RSA Root Signing Services.

A propos de RSA

RSA, la Division Sécurité d'EMC, est le premier éditeur de solutions de sécurité, de gestion des risques et de la conformité. RSA contribue au succès des plus grandes entreprises mondiales, les aidant à relever leurs défis de sécurité les plus complexes et les plus sensibles : gestion des risques organisationnels, protection des accès mobiles et du travail collaboratif, preuves de conformité, et sécurisation des environnements virtuels et Cloud Computing.

RSA apporte la visibilité et la confiance à des millions d'identités utilisateurs, aux transactions qu'elles réalisent et aux données qu'elles génèrent. Pour cela, l'entreprise associe des contrôles stratégiques métiers – assurés par les technologies de certification des identités, de DLP (prévention des pertes de données), de chiffrement et tokenization, de protection contre la fraude et de SIEM – avec des fonctions leaders d'eGRC (Gouvernance d'entreprise) et des services de consulting.

www.rsa.com

DECTR WP 1210