Système navigateur portable sécurisé

Système intégré utilisant l'authentificateur SafeNet eToken NG-FLASH avec le navigateur portable embarqué

BREVE SUR LA SOLUTION

Avantages

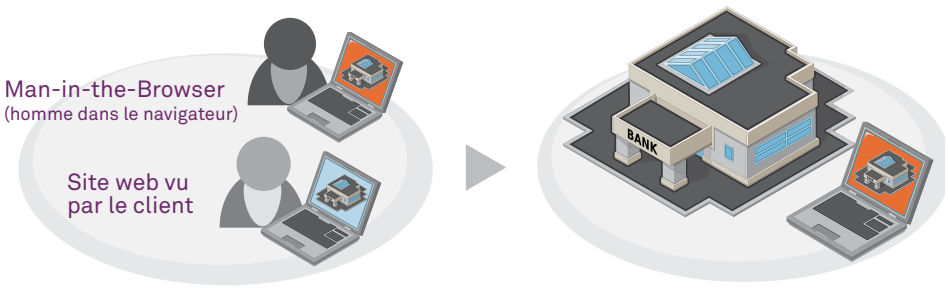
- **Accès sécurisé en ligne et protection d'identité avec un seul appareil:** comprend une carte à puce embarquée ; ainsi le eToken NG-FLASH fonctionne comme une plate-forme bancaire en ligne sécurisée et comme un dispositif d'authentification forte
- **Accès fiable:** navigateur web portable fonctionnant à partir de la mémoire en lecture seulement de l'appareil, ce qui garantit un accès sécurisé aux applications web
- **Facilité d'utilisation:** le client de la banque le branche simplement dans son ordinateur, entre un mot de passe et le navigateur sécurisé se lance

Combattre les attaques Man-in-the-Browser (MiTB) (homme dans le navigateur) avec un système intégré associant l'authentification forte à base de certificat de SafeNet avec un navigateur portable embarqué

La menace Man-in-the-Browser (homme dans le navigateur)

La banque en ligne est devenue une pratique courante au sein du grand public et des entreprises, offrant commodité et accessibilité aux utilisateurs et opportunité de revenus accrus pour les institutions financières. La très large adoption de telles pratiques suppose que l'accès à ces applications en ligne soit sûr et que les communications entre le client de la banque et la banque elle-même soient fiables et sécurisées. Cependant, en raison des pertes financières importantes résultant du cybercrime sous la forme d'attaques par vol d'identité, pharming et phishing (hameçonnage), les clients et les organisations ont fait une pause dans ces pratiques, en exigeant des mesures renforcées de sécurité comme l'authentification multi-facteurs, de manière à identifier sans ambiguïté l'utilisateur.

Dans le jeu du chat et de la souris du cybercrime, les criminels ont réagi à ces mesures de sécurité en développant des attaques plus élaborées sous la forme de logiciels malveillants, appelés aussi malwares (maliciels), résidant localement sur un PC hôte et permettant aux pirates de manipuler les sessions bancaires actives et d'effectuer des transactions frauduleuses à partir de l'ordinateur de l'utilisateur. L'attaque Man-in-the-Browser (MiTB) (homme dans le navigateur) est une attaque de ce type, neutralisant les mesures traditionnelles de sécurité en compromettant le navigateur en ligne du client pour avoir accès à ses identifiants et donc à son compte bancaire. Le malware MiTB manipule de manière discrète et malveillante les transactions souhaitées par l'utilisateur. Par exemple, dans le cas d'un transfert de fonds, le client verra toujours, via des écrans de confirmation, le paiement exact tel qu'il est manipulé dans le navigateur. Mais la banque recevra des instructions de transaction données par le malware MiTB, qui seront modifiées de manière malveillante, par exemple avec un numéro de compte bancaire destinataire différent, un montant de transfert différent, etc. Ni la banque, ni le client n'auront connaissance de la transaction altérée, jusqu'à ce qu'il soit trop tard.



Le client effectue le transfert, mais le malware Man-in-the-Browser modifie la destination et/ou le montant

Demande vue par la banque

Spécifications de eToken NG-FLASH

Systèmes d'exploitation
- Serveur Windows 2003/R2, serveur Windows 2008/ R2, Windows 7, Windows XP/Vista (32 et 64 bits)

Options de mémoire flash:
- 2 Go, 4 Go, 8 Go, 16 Go

Algorithmes de sécurité embarqués:
- RSA 1024 bits / 2048 bits, DES, 3DES (Triple DES)

Algorithme de cryptage flash embarqué:
- AES256

Certifications sécurité:
- Critères communs EAL4 (carte à puce)

Dimensions:
- 69,5 x 28,5 x 11,5 mm
- (2,74 x 1,12 x 0,45 pouces)

Assistance spécifications ISO :
- Assistance pour spécifications ISO 7816-1 à 4

Poids
- 11 g

Température opératoire:
- 0° C à 70° C (32° F à 158° F)

Température de stockage:
- -40° C à 85° C (-40° F à 185° F)

Taux d'humidité:
- 0-100 % sans condensation

Connecteur USB:
- USB type A; prend en charge USB 1.1 et 2.0 (vitesse maximum et vitesse élevée)

Coque du boîtier dur:
- plastique moulé

Conservation des données dans la mémoire sur carte à puce:
- Au moins 10 ans

Nombre de réécritures de la mémoire sur carte à puce:
- Au moins 500 000

Le système

L'authentificateur à base de certificat eToken NG-FLASH USB de SafeNet avec navigateur portable embarqué est un système de sécurité du poste ou terminal à empreinte zéro, sécurisant l'accès aux applications bancaires en ligne et protégeant l'identité à partir d'un seul appareil. Utilisant un navigateur Web portable incorporé fonctionnant à partir de l'unité mémoire en lecture seule de l'appareil, le système de navigation sécurisé eToken NG-FLASH redonne confiance dans l'application du navigateur et empêche les attaques MiTB de se produire. Il offre une solution d'accès sécurisée qui vous suit partout ; ainsi les clients de la banque peuvent avoir accès à leurs applications en ligne où qu'ils se trouvent et sans problème.

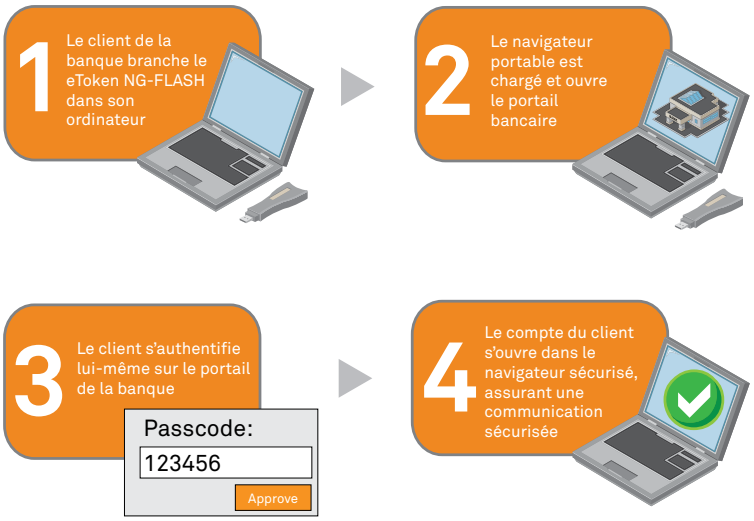
eToken NG-FLASH protège l'accès de l'utilisateur aux applications bancaires en assurant:

- **1. Intégrité du navigateur** - L'utilisation d'une application navigateur portable à partir du token eToken NG-FLASH garantit qu'une image du navigateur propre et non infectée est utilisée. En mémorisant le navigateur sur une partition mémoire en lecture seule de l'appareil eToken, on protège le navigateur contre la violation et l'infection à partir de malwares (maliciels).
- **2. Protection pendant le traitement par le navigateur** - Dans le cas d'intégration avec un navigateur tiers renforcé, des mesures de protection de la mémoire et du traitement empêchent le malware résidant déjà sur le PC d'infecter le navigateur au moment de l'exécution et empêche la manipulation des données sensibles pendant le fonctionnement du navigateur.
- **3. Authentification multi-facteurs** - Vérifie directement l'identité de l'utilisateur via ses identifiants et sécurise le canal de communication entre le navigateur et l'application Web en utilisant le système d'authentification à base de certificat client SSL de SafeNet.

Mode de fonctionnement

Servant de première couche de défense contre le vol de mot de passe, l'hameçonnage et les attaques MITM, le système de navigation sécurisé eToken NG-FLASH permet une session SSL sécurisée avec le site web de la banque, en utilisant l'authentification par certificat client. L'utilisation de l'authentification SSL protège contre l'hameçonnage et les attaques MITM. La carte à puce sur le token protège la sécurité et l'intégrité de la clé privée grâce à un système certifié FIPS 140-2, garantissant que la clé ne peut pas être volée par un malware fonctionnant sur le PC.

La composante navigateur portable du système utilise un navigateur standard ou un navigateur sécurisé tiers mémorisé sur la mémoire en lecture seule du eToken NG-FLASH. Le navigateur, avec sa fonction PKI, peut s'intégrer facilement avec la carte à puce eToken NG-FLASH et assure la configuration, dès la sortie de la boîte, pour créer un système de navigation portable intégré empêchant de manière interactive les malwares d'infecter le navigateur et prévenant donc les attaques MITB.



Visitez www.SafeNet-Inc.com/Financial-Services pour des informations sur ces ressources supplémentaires:

- Pour savoir comment mettre en œuvre un système de navigateur sécurisé : Lire notre brochure “Implementation Guidelines for Creating a Secure Browser Solution to Combat Threats” (Guide pour créer un système de navigateur sécurisé pour combattre les menaces)
- Consultez la démonstration rapide pour voir comment une attaque MitB se produit et comment on peut la prévenir
- Lire notre livre blanc “Top Online Banking Threats” (Principales menaces pour la banque en ligne)

Caractéristiques et avantages

eToken NG-FLASH de SafeNet avec un navigateur portable tiers

Caractéristiques	Benefits
Mémoire en lecture seulement sur le eToken NG-FLASH	L’utilisateur peut mémoriser une image propre du navigateur portable et d’un eToken PKI Client portable
Carte à puce intégrée avec certification FIPS 140-2	Empêche les clés d’authentification d’être copiées ou volées en utilisant une protection matérielle, et respecte les normes de sécurité les plus élevées conformément à FIPS
Authentification par certificat client SSL	Utilise les identifiants du certificat client mémorisés sur la carte à puce pour se protéger contre les attaques par phishing (hameçonnage) et MITM (homme dans le navigateur)
Protection immédiate sans installation requise	Assure une navigation sécurisée, même sur une machine infectée ou non sécurisée, en lançant le navigateur dès le branchement dans le eToken NGFLASH ; par de droits d’administrateur requis
Protection interactive intégrée	En utilisant un navigateur tiers renforcé, on élimine les menaces des malwares (maliciels) et des autres attaques malveillantes grâce à une technique intelligente les bloquant à leur point d’entrée

La famille SafeNet des systèmes d’authentification

Les systèmes d’authentification de SafeNet comprennent des authentificateurs à base de certificat, à base d’OTP (mot de passe valable une seule fois), de logiciel, et de solutions hybrides. Tous les authentificateurs, avec les plates-formes de gestion de SafeNet et les applications de sécurité, vous assurent les avantages suivants:

- Effectuer les transactions de manière sécurisée et efficace ce qui ouvre de nouvelles opportunités sur le marché grâce à des produits innovants permettant un accès sécurisé à distance et grâce à des applications telles que la signature numérique et l’authentification avant lancement.
- Diminution du risque grâce à des systèmes d’authentification forte empêchant la fraude et le vol des données, et respectant la réglementation de l’industrie.

A propos de SafeNet

SafeNet est un des leaders mondiaux en matière de sécurité des données. Fondée il y a 25 ans, la société assure une sécurité totale en utilisant ses technologies de cryptage pour protéger les communications, les droits de propriété intellectuelle et les identités numériques, et elle offre toute la gamme des produits, notamment systèmes logiciels, systèmes matériels et puces (circuits intégrés). UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco Systems, Microsoft, Samsung, Texas Instruments, les Départements américains de la Défense et de la Sécurité intérieure, le U.S. Internal Revenue Service (service de collecte des impôts américains) et bien d’autres clients font confiance à SafeNet pour garantir la sécurité de leurs données. En 2007, SafeNet a été rachetée par Vector Capital. Pour plus d’informations, rendez-vous sur www.safenet-inc.com.

Les meilleurs tokens dans le guide des produits réseau

2009 WindowSecurity.com Reader’s Choice Premier choix des lecteurs

Classification 5 étoiles “Le meilleur achat”

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected