Implementation Primer

Implementation Guidelines for Creating a Secure Browser Authentication Solution to Combat Man-in-the-Browser Threats
# Implementation Guide: Secure Browser on NG-FLASH

## Table of Contents

- Introduction ........................................................................................................... 1
- NG-FLASH Solution Framework: Protection against MitM and MitB .................. 4
- How To .................................................................................................................. 5
  - Overview ............................................................................................................ 5
  - System Requirements: ....................................................................................... 5
  - How to set autorun ............................................................................................ 7
**Introduction**

The success of multi-factor authentication implementations in addressing security threats and attacks, such as eavesdropping, password guessing, phishing, social engineering, Man-in-the-Middle (MitM) and the like, is well known. This has also challenged hackers and cybercriminals to continue developing new kinds of attacks in their ongoing quest to steal data and identities, and commit fraud. SafeNet is currently experiencing increasing interest from the market for Man-in-the-Browser (MitB) solutions, not only in the European and American online banking markets, but worldwide.

Today, the most common type of attack is the Man-in-the-Middle (MitM) attack. Basically, a MitM attack takes place when an attacker intercepts communications between two parties, such as a customer and a financial organization, without their knowledge. By doing so, the attacker becomes "the man in the middle." As a proxy, the MitM can both capture and manipulate the contents of the messages relaying between the two parties without their knowledge.

As MitM attacks have evolved, attackers have developed new social engineering tactics, using malware to capture and manipulate personal information relayed between two parties. A MitB attack is of this very nature and is designed to intercept data as it passes over a secure communication taking place through the browser between a user and an online application. A Trojan is embedded in a user’s browser application and can be programmed to trigger when a user accesses specific online sites, for example an online banking site. Once activated, a man-in-the-browser Trojan can intercept and manipulate, on-the-fly, any information a user submits online to the banking application. The information being manipulated could be the amount of money being transferred or the accounts between which it is being transferred; all without the knowledge of the end user or banking counterpart, who both see the transaction as mutually approved. This makes this type of attack very pervasive as it proliferates through the Internet, with devastating effects for the end users, as well as the financial institutions.

**The most effective defense against MitB attacks is achieved in two different ways:**

(i) Protecting transactions by providing a safe browser with real-time identity validation and digitally-signed transactions on a multi-factor authentication device loaded with digital certificates, and

(ii) Transaction verification achieved through out-of-band (OOB) technology, in which a user’s identity is verified through a separate channel, such as a telephone.

This rest of this document will discuss how SafeNet’s NG-FLASH hybrid authenticator platform can be used to create a clientless, secure browser solution for MitM and MitB threats for complete online transaction protection.
NG-FLASH Solution Framework: Protection against MitM and MitB

In the previous section, it was established that one of SafeNet’s approaches for protecting transactions in online services is to provide a totally safe browser environment with real-time identity validation through the use of a multi-factor authentication device. SafeNet’s eToken NG-FLASH combines the high security of smart card-based technology with the benefits of encrypted flash memory in a single USB token device, enabling secure access to networks and applications, secure online transactions, data encryption, and secure mobile mass data storage—all in one compact USB token.

SafeNet’s eToken NG-FLASH is a platform that can effectively meet the criteria required for addressing MitM and MitB threats, as described in the following paragraphs:

- **Two-factor Certificate-based Authentication (CBA) for addressing MitM and other existing threats**: OTP authenticators can effectively address threats from password guessing and phishing but have limitations addressing MitM attacks. The method that provides protection against all of these types of attacks is smart card-based authentication. MitM attacks can be thwarted by using SSL with server authentication (i.e., using a server certificate), and then authenticating the client over the SSL connection. However, the limitation is that this only works if the server certificate is valid, which is not always the case. For example, many users fail to correctly validate server certificates and will click through warnings. Thus, although SSL with server authentication makes MitM attacks harder to carry out, they are still possible by using phishing or other methods. The only method of authentication that provides complete protection against these attacks is SSL used in conjunction with client authentication (meaning that the client/user also has a digital certificate).

- **Trusted browser that is ‘read-only’ for thwarting MitB threats**: In order to prevent MitB attacks, the browser configuration must be trusted and free of infections from malware. This browser must reside on the token in ‘read-only’ mode, such that any malicious software, plug-ins, or sniffers are precluded from compromising any digital signature or authentication sessions. In addition, browsers should be loaded, modified, and unloaded on the authenticator through correct authorizations only.

Firefox is the most common portable browser platform available today that allows for the creation and use of portable configurations out-of-the-box. The inherent PKCS11 capability of Firefox allows for easy integration with smartcards and smartcard-based USB tokens, which is another important consideration in favor of Firefox. The standards-based Firefox browser can, therefore, be utilized for delivering Web-based applications hosted on the NG-FLASH for an effective MitB solution. (Section 3 of this document provides detailed steps on how to create this solution using the NG-FLASH platform and relevant tools.)

More advanced portability options than the ones enabled by Firefox are also available with third-party solution providers, such as Ceedo. Using such portable solutions might provide protection against malware on host computers that may attack the run-time browser process in execution on the host computer of the token-resident safe browser.

The following chart presents a summary of possible technology solutions and the threats they can avert:

<table>
<thead>
<tr>
<th>Technology Solution</th>
<th>Eavesdropping</th>
<th>Phishing</th>
<th>Pharming</th>
<th>MitM</th>
<th>MitB</th>
<th>MitB (run-time malware)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBA</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NG-FLASH + Portable Firefox Browser</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NG-FLASH + third-party advanced portability solutions</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

The NG-FLASH platform, because of its flash storage capabilities, also allows for ease-of-use in terms of plug-and-play usage of the tokens out-of-the-box. PKCS11 drivers for the smartcard, which when loaded on NG-FLASH, enable the token to work in a clientless mode without the need for installing a client on every computer the token is used from. This also enables the smartcard chip in the token to only accept authentication and digital signature instructions from the trusted, read-only browser application residing on the token.

In summary, the combination of a hardened read-only browser, a smartcard, and zero reliance on a workstation footprint on an eToken NG-FLASH can make this a secure, user-friendly MitB solution.
The future versions of this document will also provide ways of creating a High-Assurance NG-FLASH MitM-MitB solution by using a SafeNet HSM, which provides additional security authorizations through signing the browser application that is loaded on the eToken NG-FLASH, and, subsequently, signature verification for the browser application every time it is launched.

The benefits of using eToken NG-FLASH in creating a MitM/MitB solution are as follows:

- Defense against all known threats, such as Man-in-the-Middle, Man-in-the-Browser, and malware, through a smart card-based secure browser solution with locked-down configuration
- High-assurance login mechanism using digital signatures—applications can verify the integrity of the transaction cryptographically and check the status of the certificate in real-time
- Stronger security and more user-friendly than out-of-band solutions—possible with One-Time Passwords (OTP's) and software authenticators

How to Implement Firefox Mobile Browser on the eToken NG-FLASH

This section describes the steps that are needed to implement Firefox Mobile Browser on an eToken NG-FLASH device.

Firefox Portable is an easy-to-use portable version of Firefox. It has been optimized to run Firefox from any CD-ROM, DVD, USB Drive, or hard drive. No installation is required. Firefox Portable can run from the eToken NG-FLASH device and use the eToken smart card capabilities for PKI Operations without installing any PKI client software. It is only required that the host OS will have USB CCID drivers that are available by default on Windows Vista and later versions.

System Requirements

Windows 2000/XP/Vista/7, Wine on Linux/UNIX

Installation Process

1. Download Firefox Portable (www.portableapps.com)

2. Extract the files on your eToken NG-FLASH device partition.


5. Click **Tools | Options | Advanced**, and then click the **Encryption** tab. Click **Security Devices**.

6. Click **Load**. Enter a name for this module (i.e., eToken).
Do not click on Browse to select the eToken PKCS11 module (eTpks11.dll) from the Firefox Portable Directory; only enter ‘eTpks11.dll’ without a path. Since your removable device partition might change between hosts, it is necessary that the search only be conducted in the Firefox Portable Directory.

7. Click OK. The eToken PKCS11 module is now ready for use.

8. Note that you are not logged into your eToken at this time. You can do so by clicking the Login button, after which you will be prompted for your eToken password.

The next step is to install a certificate on your token from your CA. During certificate enrollment, you will need to select your eToken as the device to generate the RSA key pair and on which to store the certificate. Please make sure that your Root CA certificate is also installed.

9. You are now ready to use the certificate for your own purposes, depending on the certificate usage (ssl, s/mime, etc.).

How to Set AutoRun

If you place your CD in the drive and it does not autoplay, there could be several reasons:

- If the CD does not contain a file called autorun.inf in the root directory, it is not designed to autoplay.
- If there is a syntax error in the autorun.inf file, the CD will not autoplay.
- If the autorun.inf file instructs the system to open a program, but the program cannot be located in the path provided, the CD will not autoplay.
- If your Registry is set to inhibit autoplay on the CD drive, it will not autoplay. Right-click on the CD’s icon. If the word “Autoplay” does not appear in the drop down menu, the CD is not enabled for autoplay.

If your autorun CD will not autoplay, it could be that your Registry autorun setting has been turned off. There is always a risk when you attempt to make modifications to your Registry, especially if it is an unfamiliar task.

Tweak UI provides a user-friendly interface to make common Registry changes with minimum risk.

Tweak UI is available for download and installation from the Microsoft PowerToys for Windows XP Web page at http://www.microsoft.com/windowsxp/pro/downloads/powertoys.asp. From the right side of the page, select and download Tweak UI to your hard drive. Open Windows Explorer or My Computer, and then locate and double-click the TweakUI.exe file and follow the instructions to install it on your system.

To run Tweak UI for Windows XP, go to Start | Programs and locate it in the folder Powertoys for Windows XP. When you run Tweak UI, you can locate the autoplay settings in the dialog box as follows:

![Tweak UI](image)

Check the box next to your CD drive in the listing and click Apply.
Also ensure that all CD and DVD drives are set for Autoplay, as illustrated here:

You can confirm that your CD drive is set to Autoplay. If the CD is already in the drive, open Windows Explorer, right-click on the icon for the drive and you should see the following in the drop-down menu:

Next, eject the CD, leave it in the tray and close the door. The CD will autoplay if the autorun.inf file is present on the CD and is correctly constructed.
Remote management of browser updates

One of the following two strategies are reasonable for updating the portable Firefox browser image on the NG-FLASH token:

(i) SafeNet’s Token Management System allows provisioning of NG-FLASH tokens, whereby the CD ROM partition of the token can be configured and loaded with the required software; in this case, the desired portable Firefox image.

(ii) Creation of an update agent that resides on the NG-FLASH token, which is configured to download browser updates made available from a pre-defined web site or URL. The update agent will automatically check the URL or site for available updates, and then download and refresh the browser image on the NG-FLASH tokens. In the future, a configurable update agent would be made available to customers.

For more information about SafeNet’s Authentication solutions, please visit www.SafeNet-Inc.com/authentication.