



Meeting and surpassing FFIEC Authentication Guidelines Painlessly

This document describes how your organization can quickly and painlessly comply with the Federal Financial Institutions Examination Council guidelines for Authentication in an Internet Banking Environment as defined in the document published October 2005.

There are three specific items that are relevant to Authentication Compliance

- Requirement: Two factor or other controls reasonably calculated to mitigate risks**
- Requirement : Customer education**
- Suggestion: Mutual authentication**

Two factor or other controls reasonably calculated to mitigate risks

The document states: “Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.”

Customer education

The document states: “Financial institutions have made, and should continue to make, efforts to educate their customers. Because customer awareness is a key defense against fraud and identity theft, financial institutions should evaluate their consumer education efforts to determine if additional steps are necessary. Management should implement a customer awareness program and periodically evaluate its effectiveness.”

Mutual authentication

The document states: “Financial institutions can aid customers in differentiating legitimate sites from spoofed sites by authenticating their Web site to the customer. Techniques for authenticating a Web site are varied. The use of digital certificates coupled with encrypted communications (e.g. Secure Socket Layer, or SSL) is one; the use of shared secrets such as digital images is another. Digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defense against phishing and similar attacks.”



Complying with FFIEC guidelines, using CallingID's Safety Seal

CallingID offers an unobtrusive, easy to implement, server-based software solution that meets and exceeds the compliance recommendations. Specifically, it offers a client-less server-based approach to mutual authentication and employs strong ID/Password authentication in a manner that protects users from key loggers, when they enter passwords. and against man-in-the-middle exposures.

CallingID provides the following controls:

1. Mutual authentication verifies the site to the user utilizing a shared secret of digital images that the user chooses. This ensures the users that this site is the correct site before they provide their password.
2. An encrypted protocol between the user's machine and the server eliminates man-in-the-middle exposure, ensuring the users that no unknown server is between them and the target server.
3. Password protection from key logger and other spyware techniques is a standard feature. It always assumes that spyware might be installed on the user's machine and always takes evasive action. It simply spoofs any potential key-logger by providing a random entry in the expected password location and transferring the hidden encrypted password (PKI using a combination of one time encryption key and a shared secret key) to the server. .
4. To facilitate user education the software separates the username and password presentation. Upon entering the user name a shared secret is provided to the users to assure them that this is the target site and then the password is solicited. In addition, the user is provided with the ability to periodically, randomly, verify that this site is or is not the site they believe it to be and to use real-time training and testing based on their own practice. These functions are provided in a manner that the banks can tailor to their specific touch and feel.
5. For risk management CallingID provides an automatic audit system to determine the risk associated with each user when he logs into his account, without any need to store passwords or shared secrets in the CallingID components.

The combination of these five controls provides a viable and perhaps even more robust alternative to the often inconvenient two factor authentication techniques, without the accompanying complexities. It ensures the bank's clients that they have actually connected with the target site. CallingID also recommends that banks use a certificate to authenticate the site to the user.

On the technical side, CallingID's software provides the bank with a clientless, easy to implement tool that can easily be implemented with very little client education and minimal administration.