



VeriSign Quick Take

FFIEC Guidance on “Authentication in an Internet Banking Environment”

+ News

The Federal Financial Institutions Examination Council (FFIEC), which is comprised of the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and several other federal agencies, released guidance for US Financial Institutions (FI's) on the topic of authentication for their Internet customers.

+ Analysis

This was a compelling follow-up to previous guidance issued by the FFIEC and recent guidance issued by the FFIEC-member, FDIC.

The guidance makes definitive steps towards the elimination of single-factor authentication (i.e., username/passwords) by financial institutions for the retail and commercial customers. Single-factor authentication was called “inadequate” in protecting certain high-risk transactions. It correlates account fraud and identity theft to single-factor (e.g., ID/password) authentication exploitation.

Its recommendation for FI's was to provide authentication techniques employed by the financial institution that are appropriately matched to the risks associated with those products and services. Specifically, it identified “high-risk transactions involving access to customer information or the movement of funds to other parties” as the scope of the affected areas for FI's. Therefore, FI's need to clearly understand their respective business processes and the associated risks each of these potentially hold as it relates to identity theft and fraud.

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. The timing of the guidance recommended compliance by year-end 2006, which may drive the need for proven technologies like OTP and PKI for the immediate term, as they are available now and have been proven in retail banking internationally for years.

Finally, it was suggested that the appropriate methods be taken to ensure the identity of the applicant can be sufficiently verified in addition to ensuring the proper credential strength used for accessing the system.



Where it all comes together.™



+ Recommendation

Financial institutions should pursue the following steps:

1. Assess the various business processes that may involve transfer of funds or access to customer information to determine the risk profile.
2. Provide the appropriate level of identity verification and multi-factor authentication corresponding to the risk profile. Formally evaluate the range of different technologies and pilot as soon as possible to achieve compliance by the desired timeline in 2006.
3. Get involved with industry groups like FSTC and OATH to develop the long term roadmap and solutions.

+ Industry Involvement

Requirements and standards are being developed to address the needs of the guidance and can benefit from input from FI's, vendors and solution providers.

The Financial Services Technology Consortium (FSTC)'s "Better Mutual Authentication" project: VeriSign and 15-20 other FI's and vendors are working collaboratively to define requirements on behalf of FI's to authenticate the customer to the FI and the FI back to the customer. This project will be used to specify solutions that will address the FFIEC guidance and any possible regulation might arise in the future.

Groups like OATH (openauthentication.org) are critical for taking these requirements and facilitating them into standards that can be adopted by products. OATH and the FSTC are actively collaborating to identify how best to partner to address the very important segment of the strong authentication market. OATH welcomes all members from the financial industry and vendors associated with authentication technologies.

+ Additional Information

FFIEC guidance: http://www.ffiec.gov/pdf/authentication_guidance.pdf

FDIC FIL: <http://www.fdic.gov/news/news/financial/2005/fil5905.html>

FSTC Better Mutual Authentication Project: http://fstc.org/projects/project_home.cfm

OATH Open Authentication Project: <http://openauthentication.org>

VeriSign Unified Authentication: <http://www.verisign.com/products-services/security-services/unified-authentication/index.html>

Visit us at www.Verisign.com for more information.