FFIEC Security Guidelines

How to make the e-Banking authentication guidelines work for your organization

WHITE PAPER

Introduction

As attacks targeting online banking (e-banking) applications grow more sophisticated and more frequent, financial institutions need to strengthen their defenses. In response to these changing demands, the Federal Financial Institutions Examination Council (FFIEC) released revised security guidelines for secure banking authentication. How do you respond to these new guidelines in a way that will work best for your organization—especially as ever-more stringent security mechanisms are being subverted by ever-more sophisticated criminals and attacks?

As attacks targeting online banking (e-banking) applications grow more sophisticated and more frequent, financial institutions need to strengthen their defenses.

The Critical Imperatives for Financial Institutions

Given the frequency of breaches making headlines, it's clear that, as consumers, none of us is immune. The risks grow for those high-wealth consumers and corporate banking accounts, entities whose large resources and transaction volumes make them even more lucrative, and thus frequent, targets for criminals. Given the increase in malware and high-profile breaches, robust, continuous, and adaptable security is of paramount importance.

Traditional authentication measures are not enough to protect against fraudulent transactions. To meet their budget and profit objectives, address risk management and compliance requirements, and provide superior consumer service, it is vital for financial services institutions to ensure compliance with FFIEC security guidelines and provide optimal security. To do so, they must employ a number of key principles and best practices in order to secure online consumer identities, transactions, and data.

Adapt Authentication Mechanisms to Specific Use Cases and Risk Levels

In e-banking, different customers are vulnerable to different risks, depending on the type of transactions they conduct and the value associated with those transactions. Given the disparity in the risk levels of the different e-banking applications deployed, the authentication approaches employed should also vary substantially as well.

Security teams can choose from a broad array of mechanisms and form factors. These alternatives provide security management with a host of benefits and trade-offs, factors that will determine their suitability for a given use case. For example, for a secure loan application, more rudimentary identity verification would suffice, which could help streamline authentication logins for users and limit security expenses. On the other hand, with such high-value transactions as wealth management, security teams should adopt solutions that offer the highest levels of security and performance. These solutions should verify identities, accounts, and data input, and offer expedited transaction and data validation processing.

Layered Security Approach

Rather than relying on a single point of failure that can compromise the entire business, organizations need to treat authentication as part of a multi-layered security framework.

User Identity Verification

To safeguard their online businesses for meeting FFIEC security guidelines, financial services institutions need foolproof mechanisms for ensuring that users conducting transactions are, in fact, who they claim to be. Consequently, as a first line of defense, strong, multi-factor authentication is a critical requirement for verifying users' identities before they can access financial services portals.

Once users have been authenticated, additional safeguards need to be employed before transactions are conducted. Even if the identity of a user is validated, the transaction that ultimately is executed may still be unauthorized or fraudulent. For example, several malware and man-in-the-browser attacks have effectively changed the transaction without the customer or the bank detecting the alteration. A customer can ask to transfer $100 but the malware can change the sum to $20,000 and divert the transfer to another account.

Especially as they seek to guard against man-in-the-middle and man-in-the-browser attacks, additional transaction security mechanisms need to be employed. The key is to implement a complete, end-to-end approach in order to protect the identity and the transaction itself. To do so, organizations need to implement transaction signing that ensures that the customer-initiated transaction has not been altered or compromised in any way. This is especially critical for higher value corporate customer services, as well as such consumer applications such as wealth management, high-volume transfers, and online trading.

Financial institutions can use an array of approaches to secure these types of transactions:

- **Challenge-response via personal questions.** Here, a user would execute a transaction on a bank's online portal. The bank could then prompt the user to submit the middle name of his or her father. If the name submitted matches the record, the transaction would be confirmed.
- **Challenge-response via one-time password.** In this case, a user would also initiate a transaction on an online portal. When the bank receives the transaction, they would send the transaction details and a one-time passcode to the user's mobile phone via SMS. Once the user approves the transaction by submitting the required passcode, the bank would confirm the transaction.
- **Digital signature.** In this example, a user would view a document or transaction, and then a signing process would be initiated in which the user is prompted for token or PIN credentials. Once the credential has been validated by a trusted certificate authority, the recipient would view the signed document or transaction.

While the addition of a challenge-response mechanism can offer some benefits, the strength of security provided will vary according to the approach. Given its use of personal information, which can be obtained through social engineering and other means, the first approach outlined above presents more vulnerabilities than an approach that generates one-time passcodes or that leverages digital signatures.

In addition, multi-layered security defenses are vital. Rather than relying on a single point of failure that can compromise the entire business, organizations need to treat authentication as part of a multi-layered security framework.

Given financial institutions' sensitive information assets, they need to also employ encryption to secure those assets. That way, if unauthorized users do somehow gain access to sensitive information repositories, they won't be able to use that information. Further, when encryption is employed, strong security of cryptographic keys is also essential. This often should include the use of hardware security modules (HSMs) that store cryptographic keys in secure, purpose-built devices, and that encrypt the keys themselves so the highest level of security is realized. Further, the same HSMs used for safeguarding the cryptographic keys can be used to validate the transaction itself.

Audit, Assessment, and Adaptability

Traditionally, within any large financial institution, a host of varying use cases and systems may be in play, and it is imperative for security administrators to select the type of authentication solution that best meets the needs of each specific use case. Consequently, security administrators may need to employ a range of authentication mechanisms within their organizations. However, from a budget, security, and time management perspective, organizations simply can't afford to manage each type of authentication mechanism through a different management platform. It's essential to use a central, unified platform that can support many different authentication mechanisms.

Having a centralized system in place for rotating and safeguarding keys, securing the applications, and protecting user transaction data helps streamline security administration, and enables timely audits and system assessments.

In addition, it is also critical to centrally manage the application servers and databases that allow these online banking transactions to take place. Having a centralized system in place for rotating and safeguarding keys, securing the applications, and protecting user transaction data helps streamline security administration, and enables timely audits and system assessments.

Finally, to adapt to the ongoing evolution in malware and other threats, financial institutions need to leverage a transaction infrastructure that can seamlessly evolve along with changing threats. To adapt efficiently, organizations need to be able to strengthen the authentication security mechanisms employed—without being forced to change the back-end infrastructure.

SafeNet: Fully Trusted Authentication for FFIEC Compliance

SafeNet solutions deliver the capabilities financial institutions need to safeguard e-banking transactions. At the same time, SafeNet gives customers a wide range of options that offer improved visibility and unparalleled agility for adapting to changing needs and tailoring levels of security to levels of risk. Only SafeNet delivers a fully trusted environment that gives customers these capabilities:

- **Complete token control.** SafeNet offers customers the option of creating and controlling their own token data. As a result, customers can enjoy greater flexibility and control, and won't be exposed if the solution vendor experiences a compromise.
- **Broad authentication options.** SafeNet delivers the broadest choice when it comes to authentication methods—enabling any enterprise to effectively address the needs of all use cases and risk levels. The SafeNet authentication portfolio includes hardware tokens, software authentication, OOB, one-time password solutions, transaction signing, and more.
- **Centralized management.** SafeNet Authentication Manager is a solution that can centrally manage all SafeNet authentication solutions, including OTP, certificate-based, transaction signing, and more. Whether financial services institutions adopt multiple authentication approaches incrementally, or in parallel, they can rely on SafeNet Authentication Manager to meet their long-term needs.
- **Support for innovation and evolution.** SafeNet uniquely supports customers in their ability to flexibly and nimbly adapt to changing risks, transactions, and customer needs.
- **Layered data protection.** SafeNet offers a broad range of solutions that enable organizations to employ multi-layered security. With SafeNet HSMs and data encryption appliances, administrators can encrypt and secure sensitive data, as well as the associated cryptographic keys.

Conclusion

In their effort to combat online fraud, financial services institutions need to employ increasingly sophisticated, yet practical and cost-effective, security solutions. With SafeNet, financial services institutions can leverage an array of flexible and sophisticated security products that safeguard e-banking transactions against today's sophisticated and evolving threats.

About SafeNet, Inc.

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies, and in over 100 countries, trust their information security needs to SafeNet.

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