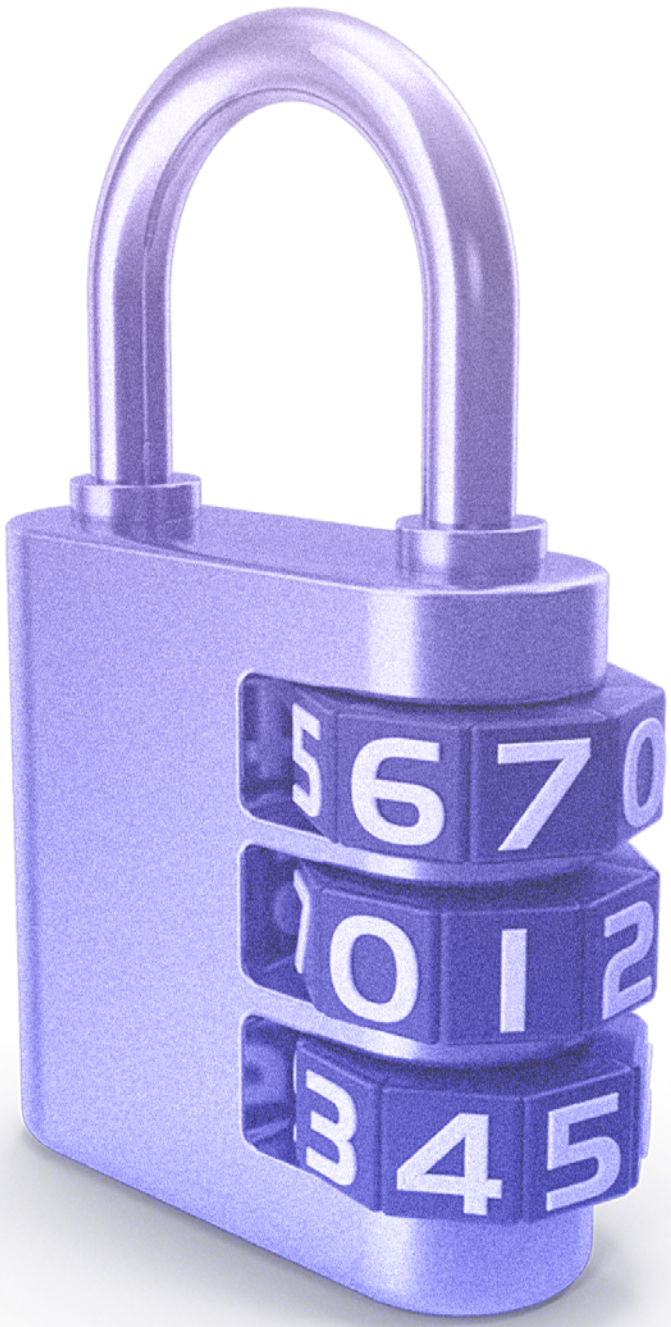
FS-ISAC

Protecting Financial Data With Encryption Controls



September 2024

Overview

Financial services firms and external entities, such as law firms, are targeted by malicious threat actors seeking to steal the sensitive data passing between the organizations.

That data – including consumer information, healthcare information, and material non-public information – can be highly regulated. A breach can result in reputational harm, impaired client relationships, remediation costs, and legal consequences for both sides.

One of the most effective ways to protect that data, whether in storage or in flight, is with encryption controls. Those security measures are implemented by organizations to protect data by turning it into a code that cybercriminals can't read through encryption and decryption processes. These encryption controls must comply with legal requirements and be obtained from reputable sources.

Financial services firms are legally required to have encryption controls, but every organization that deals with sensitive information should as well.

Protecting encryption keys in a Hardware Security Module (HSM) adds a layer of safety. HSMs are physical devices that strengthen encryption practices by generating keys, encrypting and decrypting data, creating and verifying digital signatures (which validate the authenticity and integrity of a digital document), and ensuring the data meets the highest level of verification prior to signature.

These devices also reduce the risk of successful ransomware attacks by keeping cryptographic keys used for data encryption or digital signatures out of threat actors' hands. With HSMs, organizations ensure cryptographic keys remain protected even when other parts of their digital infrastructure are compromised.

Protecting information defends both the financial firm and the external service supplier. So, in an ever-evolving threat landscape, it's in everyone's best interest to use the security controls that keep data safe.

To that end, FS-ISAC drafted this guidance. In it, you'll find:

- Real-world threats and the impact of HSM devices
- Practical encryption challenges facing IT teams
- Security guidance for cloud based systems
- A due diligence questionnaire to detect security gaps – and potential regulatory issues – in external entities' storage and encryption
- A list of resources that strengthen cybersecurity

This document is designed for firms entrusted with sensitive information. Consumer trust fuels financial services and many other industries – and safeguarding data is crucial to maintaining that trust.

Risks and HSMs

HSMs put barrier after barrier between the data and the hacker. Threat actors are incentivized to go after easy wins, so every obstacle reduces risk to financial services firms and their partners. HSMs can help fulfill differing regulatory obligations as well. Below are a few ways HSMs solve for today's risks.

Risk: Threat actor attempts to gain access to a client's financial data in a law firm.

HSM risk mitigation: The HSM encrypts the key to the data and keeps the key out of the web server's memory. So even if the hacker accesses the server, they can't find or use the sensitive data.

Risk: Migrating a trading firm's workload to the cloud can expose data and create vulnerabilities in identity access management.

HSM risk mitigation: HSMs store and hide keys in cloud environments, and separate decryption keys from encrypted data. Access to data in flight or storage is only available through a tightly controlled network interface.

Risk: Employees' Internet-of-Things (IoT) devices – including mobile phones, cars, and watches – can be exploited to launch attacks and compromise networks.

HSM risk mitigation: HSMs reduce the risk of unauthorized access and data breaches via IoT devices by storing cryptographic keys and enabling device authentication and secure communication.

Risk: A consulting firm's information security regulations differ from those of the financial sector.

HSM risk mitigation: A HSM's secure platform for key management and cryptographic operations can fulfill regulatory mandates in multiple sectors. (As a rule, the HSM should be accredited to FIPS 140-2 Level 3 with tamper detection circuitry.)

IT Considerations

Encryption and Cloud-Based Systems

Key storage is a very important aspect of cryptographic controls, and the relevant key(s) must be generated, stored, and managed within a HSM that complies with regulations for the entire key lifecycle. That has particular relevance in the cloud-based systems that businesses are using more and more often.

Most major cryptography service providers (CSPs) in cloud-based systems offer a compliant HSM solution. However, in many cases, HSM solutions cannot integrate with common components used for TLS termination/SSL offload, which means some architectural changes may be required.

If this is the case, work with the cloud service provider to architect a solution that works for both financial services firms and their external partners. It is also important to note that the location of data, keys, and HSM must be located within the same environment. If the system is hosted in the cloud, a cloud-based HSM option is necessary. If a system is hosted in a traditional data center or co-location facility, select an HSM located in the same physical environment.

Issues Associated with Encryption

Sending sensitive information without encryption across an external, untrusted network connection increases risk exposure. However, once encryption is implemented as a control, if a technology problem should arise, any portion of the flow could become unusable due to the inability to decrypt for use. Even if availability issues do not occur, encryption can add significant latency, especially TLS connections.

Due Diligence

The following questions are designed for organizations external to financial services firms. The answers can help financial institutions better understand the cybersecurity maturity and encryption controls of their external partners and highlight cybersecurity gaps that could lead to a breach.

Document Storage and Transmission

> How do you store and transmit the financial institution's documents internally and externally?

Encryption Controls

Encryption Controls and Configuration

> Do you use HSM, TLS, or a cloud-based offerings? Describe how these controls are configured and how data flows through the control architecture.

> Is data at rest encrypted? If so, is the encryption on-premises or cloud-based? Is internal network traffic encrypted or in the clear?

> Unique file-level encryption offers better protection. Is encryption applied at the digital file level or the storage container level?

Encryption Key Storage and Management

> How are encryption keys stored? Are they in a HSM? Is the HSM accredited to FIPS 140-2 Level 3 with tamper detection circuitry?

Financial firms should require external entities to have Level 3 to prevent breaches, not just detect them as with Level 2.

- Do you use cryptography supporting AES-256 at the document level or at the storage library level?
- Are you using entropic encryption or software algorithms to generate encryption keys? Natural phenomena-based random number generation is the higher security standard.

Custody and Management of Encryption Keys

- Who holds the encryption keys – you, the financial institution, or a service provider?
- How is key management performed?

Multi-Factor Authentication and Access

- Do you have multi-factor authentication (MFA) in place for all systems and data related to a financial institution?[1] Have you assessed the residual risk after MFA has been applied to determine if additional countermeasures are required?
- Have you determined who is a high-risk user or the high-risk transaction type and applied sound risk management to those elements?

External Entity Due Diligence

Entities external to financial services should be utilizing an HSM if any of the following statements are true:

- Your company uses any certificates issued by a trusted third-party Certificate Authority (i.e., Digicert, Entrust, etc.) to facilitate encryption of financial firm data in transit (i.e. HTTPS, SMTP, S/MIME).
- Your company uses a VPN (Virtual Private Network) that protects financial firm data in transit.
- Your company uses certificates/private keys to sign code.
- Your company uses certificates/private keys to sign documents.
- Your company manages an internal certificate authority (iCA) with associated root and intermediate certificates for internal PKI (public key infrastructure).
- Your company uses keys to sign an authorization request, assertions, or authorizations or to decrypt authorizations, assertions, or authorizations used in access identity (SAML, OAUTH, S/MIME/ DKIM, Seed Auth Server, Kerberos, etc.).
- There are instances of two-factor/biometric authentication information/smart card logon/ FIDO, etc. that leverage private/secret keys.
- Your company encrypts data at rest in databases or other storage systems.
- Your company stores archived data for extended periods of time.
- Your company has any encryption keys that encrypt other encryption keys.
- Your company uses passphrases as part of any cryptographic function/operation.
- Your company manages PIN security.
- Your company installed or used private/ secret encryption keys within a production environment across multiple environment instances.
- There are instances of Europay, Mastercard, and VISA (EMV) Integrated Circuit Card (ICC) keys.
- There are cases where there are more than 50 encryption keys for data at rest.

Conclusion

In today's digital landscape, where sensitive data is constantly at risk from increasingly sophisticated threat actors, employing strong cryptography along with a HSM is a critical component of proactive threat management.

By knowing the risks and working together, financial institutions and external entities can form a powerful bastion of cyber defense against threat actors trying to exploit and capture client data. Employing the right tools and best practices helps everyone protect their data assets and those of their clients. It also enables businesses that run on trust to uphold the confidence of their stakeholders in an increasingly interconnected world.

Additional Cybersecurity Resources

Legal Services

Legal Services ISAO

Architecture, Infrastructure, and Operations

FFIEC Information Technology Examination Handbook, Architecture, Infrastructure and Operations, June 2021

Federal Information Processing Standards (FIPS)

FIPS 140-2 & 140-3: Security Requirements for Cryptographic Modules

FIPS 180-4: Secure Hash Standard

FIPS 186-5: Digital Signature Standard

FIPS 197: Advanced Encryption Standard (AES)

FIPS 198-1: Keyed-Hash Message Authentication Code (HMAC)

National Institute of Standards and Technology (NIST) Special Publications

SP 800-38 Series: Modes of Operation, Cipher-based Message Authentication Code (CMAC), Counter with Cipher Block Chaining-Message Authentication Code (CCM), Galois/Counter Mode (GCM) & GMAC, XEX-based Tweaked-codebook mode with Ciphertext Stealing (XTS-AES), Key Wrapping

SP 800-56 Series: Pair-Wise Key-Establishment Schemes

SP 800-57 Part 1: Recommendation for Key Management

Request for Comments (RFC) Standards

RFC 5246: Transport Layer Security (TLS) Protocol Version 1.2

RFC 8446: Transport Layer Security (TLS) Protocol Version 1.3

ISO/IEC Standards

ISO/IEC 18033-1:2021 - Encryption algorithms

ISO/IEC 18033-2:2006 - Asymmetric ciphers

ISO/IEC 18033-3:2010 - Block ciphers

Endnotes

1 https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf