

Addressing Data Privacy in Credit Unions

Keys to Securing Member Data and Achieving NCUA 748 Compliance

Executive Summary

Since NCUA 748 was passed in 2001, one of its key principles remains that credit unions must “ensure the security and confidentiality of member records.” While this guiding principle has remained the same, the nature of the threats to this data, and the steps required to protect this data, have changed significantly in recent years. This solution brief looks at the changing nature of security threats, it looks at specific guidelines 748 provides for protecting member information, and it outlines how Ingrian can help address these guidelines, and so ensure data privacy within credit unions.

The National Credit Union Association (NCUA) publishes detailed rules and regulations for Federal Credit Unions. These comprehensive guidelines cover issues such as credit practices, accuracy in advertising, fidelity bond and insurance coverage, and investment and deposit activities. Part 748 of these guidelines are entitled “Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance.” As part of this statute, the NCUA mandates that credit unions develop an information security program, with the following objectives:

“Ensure the security and confidentiality of member information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member.”

Since these guidelines were first passed in 2001, the threats to consumer data—and corresponding steps credit unions need to take to meet these guidelines—have changed significantly. NCUA guidelines specify that security measures must address both internal and external threats. In the past, credit unions have largely been able to address these requirements by building a strong network security perimeter, but the nature of today’s security threats are changing—

requiring a new approach to security.

While traditional technologies like firewalls and intrusion detection systems are a critical part of protecting an enterprise’s network perimeter, they are only part of a complete security picture. Here are a few reasons for this:

- According to Gartner, 75% of external-based attacks are tunneling through applications—and so go undetected by a range of perimeter security mechanisms.
- The ongoing battle of patching known exploits is being lost: According to a study by Symantec, in 2003, 70 percent of all security vulnerabilities were simple for attackers to manage, and this number grew 10% over the previous year.
- Most estimates cite that now over 50% of security breaches are perpetrated by internal staff.
- Even with a fortified network perimeter, storage systems can be breached via insecure storage management interfaces and physical storage systems and data in the databases and applications themselves can be stolen.

As credit unions address these changing dynamics, and so remain compliant with 748, they are beginning to look to ensure data privacy—undertaking the process of selecting and securing critical data inside the enterprise.

While no single vendor or solution can address the entirety of 748 requirements, Ingrian's data privacy solutions address the key fundamental points of data privacy inside an enterprise, and so help ensure credit unions are protected from breaches and are compliant with many of the fundamental requirements of 748 for information security.

With Ingrian DataSecure™ Platforms, companies can secure data within applications, databases, and storage systems. DataSecure gives customers comprehensive controls for protecting sensitive data, delivering such capabilities as granular, field-level encryption; centralized, FIPS-compliant key management; integrated authentication and authorization; and robust logging and auditing.

Below is an overview of Part 748's guidelines for securing member data, and information on how Ingrian DataSecure Platforms address these requirements.

Encrypting Member Information

Appendix A of Part 748 advises "Encryption of electronic member information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access."

Often, organizations deploy security systems to encrypt data in transport between machines, but then have the data stored in the clear. Given the reasons stated above, this approach is no longer enough. DataSecure is a dedicated security appliance that can centralize the encryption of critical data, and ensure that data is secure, both in transit and as it resides in application servers, Web servers,

and databases. Because it manages encryption at the application level, Ingrian delivers a great deal of granularity over what data to encrypt, whether that data is a field or an entire column in a database.

Appendix B to Part 748 defines "sensitive member information to mean a member's social security number, personal identification number (PIN), password, or account number, in conjunction with a personal identifier, such as the individual's name, address, or telephone number." The reality is that this sensitive data may only represent a very small percentage of all the data a credit union must process and store. DataSecure enables organizations to assign varying security values to the data that resides within the enterprise, and to apply granular control over the type of data to encrypt.

Yet the encryption of data is only part of the story. One of the essential components of encryption that is often overlooked is key management, which refers to the way cryptographic keys are generated and managed throughout their life. When evaluating a data privacy solution, it is essential to include the ability to securely generate and manage keys.

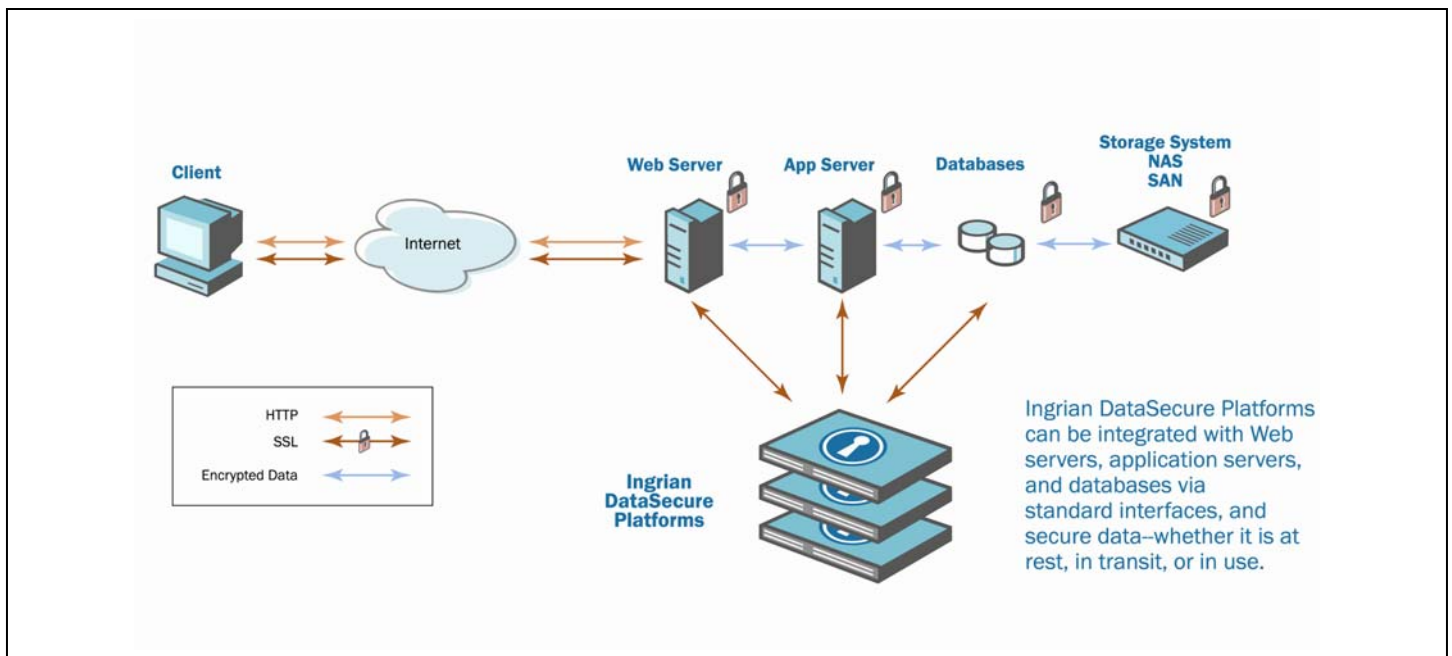
DataSecure centralizes all of the tasks of key management on a single platform and effectively automates administrative key management tasks, which leads to enhanced security, improved operational efficiency, and reduced cost of management. DataSecure also offers an automated and secure mechanism for key rotation, replication, and backup. DataSecure eliminates the security and administrative shortcomings of server-based key management

because it centralizes cryptographic processing on a secure appliance. What makes the platform secure? For starters, unlike servers, no one can "log on" to the Ingrian platform and search for the secret keys. All keys are stored encrypted and integrity checked within the platform, and are never available in plain text to anyone. Furthermore, the keys can only be created and managed by administrators. All communication between servers and Ingrian platforms takes place over a secure SSL connection and all cryptographic keys are stored away from the servers on the DataSecure platform. For an additional level of key storage security, customers can choose a DataSecure platform containing a FIPS 140-2 Level 3-compliant hardware security module, which supports U.S. government requirements to ensure that the storage media itself is extremely tamper resistant.

Controlling Access through Authentication and Authorization

Appendix A also advises credit unions to consider "access controls on member information systems, including controls to authenticate and permit access only to authorized individuals."

Authentication and authorization is a critical component of any data privacy solution deployed within an enterprise. DataSecure's robust authentication and authorization capabilities allow the enterprise to restrict which applications and business processes can access sensitive data in the clear. With DataSecure, organizations gain a strong layer of security with granular access controls for both data and the keys used to unlock that data.



Once a user is authenticated, DataSecure enables administrators to restrict user access to only designated keys and specific cryptographic functions, enabling further restriction of users and segmentation of data security.

Logging and Monitoring Security Activities

A fundamental aspect to achieving data privacy in a credit union is the task of monitoring and logging all attempts to access or manipulate sensitive data. Largely, this is the only way administrators can be sure that critical data is in fact secured. Being able to log and monitor this activity is also a fundamental requirement for compliance. Specifically, Appendix A urges

“Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems.”

When encrypting data within an enterprise, one has to consider the fact that data, keys, and logs will be accessed, encrypted, managed, and generated on multiple devices and in multiple locations. With DataSecure, administrators can centrally log and audit access to data and keys, and so gain a range of benefits:

- By leveraging a single and centralized interface, the cost of management is reduced.
- Security is enhanced because administrators gain a centralized mechanism with which to view information as attempted attacks occur.
- Organizations can more effectively ensure compliance with logging and auditing requirements as set forth by the NCUA as well as other governmental and industry legislation.

Employing Administrative Controls

An additional issue outlined in Appendix A is the need to secure the administration of sensitive data. The rule recommends the implementation of “dual controls procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information.”

As mentioned above, because it centralizes all cryptographic processing on to a single, secure appliance, DataSecure streamlines security administration and it yields significant improvements in security. In addition, Ingrian delivers comprehensive capabilities for managing client and administrative access to the DataSecure platform. Access to keys and cryptographic functions are defined using an easy-to-manage, role-based access system.

The only way to access the DataSecure platform is at the administrator level, via a secure Web-management console, a command line interface over SSH, or a direct console connection. In any case, the platform can be configured so that individual administrators are granted access only to areas for which they are responsible. For example, one administrator might only be given access to network configuration, while another might only be given access to certificate management. This level of granular access control enables customers to control and closely monitor administrator operations. All actions performed by all users and administrators are also securely logged, stored, and available for reporting purposes.

Access control can be taken to the highest level by using Ingrian's smart cards and readers, which involve multiple administrators sharing parts of a "group key" required to perform sensitive administrative functions—such as backup and restore operations. This additional level of security makes it impossible to corrupt the system if a smart card is lost or stolen because multiple smart cards must be used together to gain platform access.

About Ingrian Networks

Ingrian Networks brings complete data privacy to the enterprise. Ingrian DataSecure Platforms ensure that sensitive information is impervious to attacks, whether data is at rest, in transit, or in use. Ingrian DataSecure Platforms offer intelligent, granular control over what data is protected, they adhere to open standards and are cost effective to deploy, and they deliver comprehensive security capabilities. For all these reasons, Ingrian is the smart choice for addressing one of today's most critical security threats: data left unprotected within the enterprise. Ingrian is a privately held company backed by such investors as American Express (NYSE:AXP), Globespan Capital Partners (formerly JAFCO Ventures), HighBAR Ventures, Partech International, and Prism Venture Partners. For more information, visit www.ingrian.com.

© Copyright 2004 Ingrian Networks. The Ingrian Logo, Ingrian, and DataSecure are trademarks of Ingrian Networks. All other brand names are trademarks of their respective holders.