GEOBRIDGE Corporation

Newsletter
Oct 2016

The LMK Rotation

Creating a new LMK is no more challenging than the creation of any other key type. However, rotating all of the keys in an organization's payment environment from encryption under the old LMK to encryption under the new LMK while logging all activities and ensuring that the key is translated properly is a much more daunting task.

A leading financial card services provider who has been a client of GEOBRIDGE for ten years, was audited in the Spring of 2016. One of the findings was to rotate the Thales payShield 9000 HSM's LMK that had been in place for several years. The client utilized five different applications connecting to a farm of payShield 9000 HSMs. The client had over 1000 different keys representing ten distinct key types across the five applications. Like every project in the payment world, this one had to be completed within a very short timeframe.

The client contacted GEOBRIDGE's Professional Service team to help provide a solution. As part of the rotation, the team recommended to rotate the LMK but also to translate the existing key inventory from variant to key block due to the PCI PIN Control Objective that will enforced in January of 2018.

After two weeks of project planning, GEOBRIDGE's team went onsite to oversee the translation activities. As part of the service, the team used a KeyBRIDGE™ 3100 appliance with the Third Party HSM integration module.

With the KeyBRIDGE 3100 appliance, the client:

- Created their own KeyBRIDGE master key, which they continue to retain.
- Logically separated the keys within the KeyBRIDGE appliance according to application name and relationship.
- Automatically logged and uniquely named all keys, while validating key check values.
- Translated all keys from encryption under old LMK to encryption under the KeyBRIDGE SMK.
- Translated the full key inventory for use under the new LMK.

Benefits of using the GEOBRIDGE KEES™ Service:

- All keys were successfully translated from the old Variant LMK to the new Key Block LMK.
- All activities were automatically logged with unique user IDs, and RBACs permissions.
- All HSMs are loaded with the new LMK.
- The client is now prepared to operate in both variant and key bundling modes.
- The client has now created a full inventory key escrow, encrypted by a 256-bit AES Key. The encrypted key inventory is now saved off to the network, and the master key components are stored securely in the client's key custodian safes.
- All activities onsite were successfully completed within three (3) days.

A seemingly impossible task with unrealistic timelines was completed ahead of schedule while also preparing for future compliance mandates, all as a result of GEOBRIDGE KEES™ Professional Services team and the KeyBRIDGE platform.

CertBRIDGE™

GEOBRIDGE announces CertBRIDGE™, a Managed Service Certificate Authority.

- Cost-effective solution for deploying your own Certificate Authority.
- Allowing clients to deploy their own unique security schemes onto their own devices.
- Enabling unique remote key delivery techniques with Asymmetric cryptography.
- Flexible delivery model enhancing delivery and reduced deployment time.
- Architected to allow you to maintain complete control of your Root CA and PKI recovery materials.
- Highly customizable Public Key Infrastructure with no per-certificate costs.
- Ensuring High Availability and effective Disaster Recovery.
- Leveraging subject matter expertise of GEOBRIDGE to meet cryptographic compliance mandates.
- Contact sales@geobridge.net for additional information.

20110 Ashbrook Place, Suite 275
Ashburn, VA 20147

Telephone: (703) 857-2100
Fax: (703) 724-4137

www.GEOBRIDGE.net
sales@GEOBRIDGE.net

Ask the Assessor

Dear GEOBRIDGE Assessor,

What types of logs will the auditors be asking for during a review of my Key Management activities?

This question may seem pretty obvious, but interestingly enough many organizations fall short in journaling all their key management activities. They miss documenting relevant information that can result in an unsatisfactory rating on a TR-39 or PCI PIN audit. Detailed and comprehensive logs are critical part of the auditor's review for any organization that manages encryption keys. However, your logs are not just to impress the auditors during an assessment. If logs are reviewed on a regularly scheduled basis they will provide companies with valuable information that can aide in their security, as well as help to improve upon the existing key management procedures.

The documented procedures created for key management should detail what information should be included in your logs when encryption keys are created, stored, distributed, and finally destroyed. In other words, **the entire key life cycle**. Logs are the audit trails which should be used for Individual Accountability, Reconstruction of past events, Intrusion Detection and Problem Identification. Proper training of what to log, and how to log, must be done with all Key Management personnel to ensure completeness, accuracy and consistency of logging is maintained with everyone involved.

One final note, any handwritten logs should be kept in a hard bound notebook, not a spiral or loose-leaf. This ensures pages cannot be easily removed or substituted fraudulently.

Additional information can be found in the SP800-14 NIST special publication on securing computer systems. It covers audit trails from a high-level perspective.

Have a question for our Assessors?

Send an email to support@GEOBRIDGE.net and include "Ask the Assessor" in the email subject. Your question may be featured in our next newsletter.

Partner Highlight - Infinite Peripherals

In August 2016, GEOBRIDGE announced the integration that enables KeyBRIDGE™ users to support the Infinea® mPOS and Infinea® BluePad devices.

IPC's NFC-enabled products simplify adoption of new contactless payments, such as Apple Pay™, and its Infinea® mPOS line facilitates EMV payments with a contact chip card reader and PIN entry. Anticipating trends and pre-empting solutions for a constantly evolving business landscape, IPC's enterprise mobility solutions also optimize operations in healthcare, hospitality, transportation, warehouse and logistics, entertainment and security. For more information, please visit ipcmobile.com.

Employee Highlight

Donna Gem, CTGA joined GEOBRIDGE in April. She is now Director of Solutions Delivery. Donna came from JP Morgan Chase Commerce Solutions (fka, Chase Paymentech), and brings with her over 24 years as a subject matter expert for encryption key management related to PIN debit, EBT, EMV, E2E, and P2P keys. Additionally her vast knowledge and experience includes:

- ANS X9-F6 committee member
- PCI PIN and TR39 Security expertise
- Providing guidance to development teams in interpreting key management processes and appropriate use of keys to protect sensitive data.
- Assisting third party encryption vendors (ESOs) to ensure compliance with all industry standards.
- Continuous improvement for the implementation methodology, documentation and the key management processes based on updated industry standards.
- Extensive work in with encryption keys utilizing the KeyBRIDGE™ appliance.

20110 Ashbrook Place, Suite 275
Ashburn, VA 20147

Telephone: (703) 857-2100
Fax: (703) 724-4137

www.GEOBRIDGE.net
sales@GEOBRIDGE.net

In the News

The Number of EMV Chip Payment Cards in Global Circulation Increases to 4.8 Billion.

Global technical body EMVCo in June reported sustained growth in the worldwide adoption of EMV chip technology. Official figures of aggregated data show that by the end of 2015, the number of EMV payment cards in global circulation increased, year on year, by 1.4 billion to 4.8 billion.

In addition, EMVCo reports that 35.8% of all card-present transactions conducted globally between January and December 2015 used EMV chip technology*, up from 32% for the same period in 2014.

The latest statistics highlight that EMV chip card adoption rates continued to increase in all the mature regions by the end of 2015:

- Europe Zone 1, EMV chip card adoption rate: 84.3% (up from 83.5% in 2014)
- Canada, Latin America and the Caribbean, EMV chip card adoption rate: 71.7% (up from 59.5% in 2014)
- Africa and the Middle East EMV chip card adoption rate: 61.2% (up from 50.5% in 2014)
- Europe Zone 2 EMV chip card adoption rate: 52.3% (up from 40.4% in 2014)
- Asia Pacific EMV chip card adoption rate: 32.7% (up from 25.4% in 2014)

Europe Zone 1 maintained the highest percentage of EMV chip transactions, which accounted for 97.3% of card-present payments. 87.9% of card present transactions were EMV chip-enabled in Canada, Latin America and the Caribbean, while in Africa and the Middle East, usage accelerated to 87.1%.

In Europe Zone 2, EMV chip transactions reached 71.8% of card present payments. Significant advancements were also made in Asia Pacific, with the percentage of card-present EMV chip transactions rising to 40.3%, marking a nearly 50% increase from 2014.

In the United States the EMV transition started to accelerate in 2015 and is continuing apace in the first half of 2016.

"The global adoption of the EMV Specifications is imperative to the development of a more secure and interoperable payments industry," comments Mike Matan, current Chair of the EMVCo Executive Committee. EMVCo welcomes engageme with interested parties from across the payments ecosystem and supports a number of initiatives to enable the payments community to be actively involved in developing, enhancing and evolving future specifications."

**The data is reported individually by American Express, Discover, JCB, MasterCard, UnionPay and Visa to a neutral third party and aggregated confidentially for the noted period.*

Article Source: PaymentWeek

Did you know?

- GEOBRIDGE has partnered with Vormetric, a Thales company, to apply GEOBRIDGE experience and expertise of integrating best of breed hardware based cryptographic security with Vormetric data security product offerings.
- GEOBRIDGE offers online and offline RKL solutions to support Device Manufacturers with the KeyBRIDGE™ 3100 platform.
- KeyBRIDGE 3100 appliance has now certified the following devices on the platform:
  - Blue Bamboo: P200
  - AMP: 3000, 5000, 7000 and 9000
  - Infinite Peripherals: mPOS and BluePad 50
  - Topaz: T-PP
  - Anywhere Commerce: Nomad 2.0 and Nomad 2.0 BlueFin
  - VeriFone: e355, MX915 Moneris, UX300 Moneris
  - PAX: D200, Px5 and Px7
  - XAC: 8006L1 (USB and Serial), xCE200T (Serial) xCE25M and xCE50
  - Spectra: T-1000
  - Ingenico: iPP320-Moneris (Serial and USB), iPP320 PayTrace (Serial and USB) and iCMP Moneris
- KeyBRIDGE 2100 appliance is end of support: December 31st, 2016.
- GEOBRIDGE KEES™ Service can augment or satisfy your organizations' Disaster Recovery Requirements with Escrow and Exchange Services.

Upcoming Events

ANS X9-F6 All Committees Meeting

Atlanta, Georgia
October 17th-21st, 2016

2016 Strategic Leadership Forum

The Breakers, Palm Beach, Florida
October 19th-21st, 2016

Money 20/20 Conference

Las Vegas, Nevada
October 23rd-26th, 2016

20110 Ashbrook Place, Suite 275
Ashburn, VA 20147

Telephone: (703) 857-2100
Fax: (703) 724-4137

www.GEOBRIDGE.net
sales@GEOBRIDGE.net

The Purpose of FIPS 140 - What is Compliant?

The National Institute of Standards and Technology (NIST) issues the 140 Publication Series to coordinate the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the United States federal government.

FIPS 140 does not purport to provide sufficient conditions to guarantee that a module conforming to its requirements is secure, still less that a system built using such modules is secure. The requirements cover not only the cryptographic modules themselves but also their documentation and (at the highest security level) some aspects of the comments contained in the source code.

If you are a POI Acquirer, Key Injection organization, or a merchant processor, GEOBRIDGE can provide assistance with the applicable compliant device for you. Please contact us if you need guidance with your hardware security.

FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

- FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must be "production-grade" and various egregious kinds of insecurity must be absent.
- FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
- FIPS 140-2 Level 4 makes the physical security requirements more stringent, and requires robustness against environmental attacks.

Source: NIST Federal Information Processing Standards Publications

About GEOBRIDGE Corporation

Established in 1997, GEOBRIDGE emerged as one of the first information security solutions providers to support cryptography and payment applications for payment processors, financial institutions and retail organizations. Today, GEOBRIDGE is a leading information security solutions and compliance provider that offers Network Security, Cryptography and Key Management, Payment Security and Compliance solutions and services. Our client list includes Fortune 500 companies, financial institutions, healthcare organizations and government clients across North America and around the globe. GEOBRIDGE leverages our team's expertise in data protection, program development, enforcement and governance to help architect solutions to help mitigate risk for our clients. To learn more about GEOBRIDGE, contact us at sales@GEOBRIDGE.net

GEOBRIDGE Corporation

Newsletter
Oct 2016

20110 Ashbrook Place, Suite 275
Ashburn, VA 20147

Telephone: (703) 857-2100
Fax: (703) 724-4137

www.GEOBRIDGE.net
sales@GEOBRIDGE.net