CMS Topaz™
CASE STUDY

CertBRIDGE by GEOBRIDGE:

A Case Study of Embedded PKI and CMS Topaz

GEOBRIDGE Corporation

Partner: GEOBRIDGE

Website: www.geobridge.net

Country or Region: United States

Industry: Information Security

Partner Profile

GEOBRIDGE is a leading information security solutions and compliance provider that has supported hundreds of clients in securing their business operations and managing compliance regulations.

Business Situation

GEOBRIDGE, manufacturer of key management solutions, studied ways to remove common barriers of entry for real-time enablement of POI devices, by providing customers with a compliant trust model for remote key loading, delivered via cloud service.

Solution

The CertBRIDGE platform enables GEOBRIDGE to leverage best practice security tools and first-rate subject matter expertise to deliver a fully managed Certificate Authority service to the marketplace, leading to reduced costs and accelerated time-to-market for its financial services customers.

GEOBRIDGE Corporation, the manufacturer of the KeyBRIDGE™ platform, in partnership with CSS, known for its PKI Operations and Cloud PKI solutions, has released CertBRIDGE™ 1.0, enabling Point of Interaction (POI) manufacturers to offer remote key loading to their customers.

Certified Security Solutions (CSS) is a cyber security company that builds and supports platforms enabling secure commerce for global businesses connected to the Internet. CMS Topaz provides enterprise application service providers with a reliable and highly scalable PKI identity platform that can be easily embedded to enable secure operations of applications, devices and services.

Direct Key Injection and Remote Key Loading

Since 1997, GEOBRIDGE has been enabling direct key injection for hundreds of POI devices. More recently, GEOBRIDGE has worked with a number of POI manufacturers to support their proprietary remote key loading techniques with the KeyBRIDGE™ appliance. There are two primary techniques in the marketplace, both with distinct advantages, and both supported by the new CertBRIDGE platform:

- **Symmetric Protection of Symmetric Keys:** This technique lends itself to large batch processing, with pre-ordered payloads managed carefully through common or proprietary terminal management systems. This technique relies on the presence of a symmetric key loaded by the manufacturer at the time of device building. CertBRIDGE establishes and ensures mutual authentication prior to the delivery of this sensitive payload.
- **Asymmetric Protection of Symmetric Keys:** This technique applies to single device key loading in real-time, by leveraging mutual authentication techniques enabled by a carefully managed Public Key Infrastructure and Certificate Authority. Asymmetric protection of symmetric keys relies on the presence of a pre-loaded key pair used to perform mutual authentication. While this method is effective, it comes with complexity of implementation for those unable to efficiently roll out and sustain the required infrastructure.

CertBRIDGE: A New Solution

For decades, secure key delivery solutions have been either symmetric or asymmetric. Both GEOBRIDGE and CSS have invested considerable resources in providing clients the most secure key management available while supporting adherence to compliance requirements. The CertBRIDGE platform has enabled GEOBRIDGE and CSS to combine best practice security tools to deliver a single robust solution to the marketplace, supported by first-rate subject matter expertise, reduced costs, and accelerated time-to-market for solution providers.

CertBRIDGE has been designed to satisfy industry and government compliance requirements associated with real-time remote key distribution for POI manufacturers. Unique features and specialized functions of new equipment are only impactful when a solution can be deployed in a timely manner. Moreover, total cost of ownership is often calculated by considering the cost of repair and re-keying obligations. Shipping costs, along with revenue lost during a shipping cycle, are major drivers for more efficient solutions. As a result, real-time key loading techniques are necessary to support the demands of the industry.

The single greatest challenge of enabling real-time key loading is the establishment of a compliant trust model. This is the purpose of PKI. By relying on a Certificate Authority (CA), an effective PKI solution will establish trust by eliminating opportunities for corruption by systems or people. A compliant PKI solution leverages physical infrastructure along with meticulous processes, procedures, and subject matter expertise.

The Reliance on Public Key Infrastructure

Deploying and properly managing a PKI is not a trivial matter. The cost, time, and expertise needed to manage a solid PKI is staggering, forcing many organizations to put critical PKI operations on the back burner. From services to resource salaries and hardware, in-house PKI can have an annual maintenance cost of anywhere from $300,000 to more than $1 million.

Some of the components that must be managed on an ongoing basis include:

- Segregated physical security infrastructure, as per compliance guidelines
- Establishing an offline root with associated procedures
- Tracking of certificates, locations, and expirations
- Monitoring and reporting, with automatic notification and escalation
- Proper documentation for change control and employee turnover
- Management of CA and CRL health and uptime

> “The single greatest challenge of enabling real-time key loading is the establishment of a compliant trust model. This is the purpose of PKI. An effective PKI solution will establish trust by eliminating opportunities for corruption by systems or people. A compliant PKI solution leverages physical infrastructure along with meticulous processes, procedures, and subject matter expertise."

In addition, poor operating procedures tend to worsen over time, resulting in widening security gaps and increased risk levels. Because PKI is a mature technology, assumptions are often made that it is as secure today (and tomorrow) as it was when built. These assumptions exist even as new demands are placed on the PKI, which were not accounted for during its design and deployment. As a result, organizations often make PKI management and operations decisions that put critical information at risk.

Compliance mandates, recurring organizational turnover, the need to maintain strong cryptography standards, and an organization's need to focus on its core business are all reasons to evaluate whether building and managing PKI in-house is truly the most effective way to secure an application service. Secure deployment of PKI must also extend beyond initial implementation to ongoing management and growth, in order to ensure all business and compliance goals are met and sustained.

"CertBRIDGE, powered by CMS Topaz, eliminates common challenges inherent in PKI and overcomes the barriers to successful adoption within the Point of Interaction (POI) industry."

An effective and compliant PKI infrastructure can be cost prohibitive when considering these and other requirements factors. Requirements and associated costs have prevented the adoption of more efficient techniques and are consequently limiting competition in the Point of Interaction (POI) industry. Leveraging a dedicated PKI service for these operations is often the simpler, safer, and most sustainable option. CertBRIDGE, powered by CMS Topaz, eliminates these challenges inherent in PKI and overcomes the barriers to successful adoption.

How Does CertBRIDGE Enable Real-time Remote Key Distribution?

The CertBRIDGE platform changes the current model. CertBRIDGE is a managed, plug-and-play Certificate Authority. For a fraction of the cost of establishing an effective and compliant internal PKI, customers can rely on CSS physical security and subject matter resources for maintaining control of their CA and public key infrastructure. CertBRIDGE enables POI manufacturers to offer real-time remote key loading techniques.

The CSS SaaS Offering

CMS Topaz provides enterprise application service providers with a path to easily embed reliable and scalable PKI into their applications and services. Courtesy of a cloud hosted PKI-as-a-Service offering (PKIaaS), CMS Topaz delivers digital certificates and addresses all compliance mandates. It also eliminates the need to host, manage, and support the PKI environment and CAs as an organization.

With many years of experience operating and managing PKI deployments, a PKI professionally managed by CSS is designed to meet the immediate and long-term security needs of a business that requires PKI with a secure and auditable operation plan. It allows businesses to have full confidence in their technology investment without allocating critical resources to its many administrative demands.

CMS Topaz now brings this expert PKI experience and operational efficiency directly to cloud applications and services, so that they benefit from the security of digital certificates without the need for their operators to assume management responsibilities of the PKI.

CertBRIDGE is powered by CMS Topaz.

CMS Topaz™
for Cloud Apps

CertBRIDGE Availability and Powerful Outcome

There are many financial advantages to leveraging CertBRIDGE, including the ability to perform remote key loading while eliminating associated PKI management costs. CertBRIDGE benefits from CMS Topaz powering its Certificate Authority and digital certificates, with unlimited scalability and a High Assurance security level.

CertBRIDGE is a licensed feature available on the KeyBRIDGE™ platform. KeyBRIDGE™ is the appliance the POI industry has trusted since 2004 for the agnostic, secure loading of payment-related keys. KeyBRIDGE™ facilitates the signing of a certificate for a POI public key. Many devices are capable of generating their own public and private key pairs. In cases where devices are incapable of generating their own public and private key pairs, KeyBRIDGE™ produces the keys using its certified FIPS 140-2 level 3 random number generator. When devices do generate their own key pairs, the POI will connect directly to a KeyBRIDGE™ appliance and provide its certificate signing request within the business's secure facility.

CertBRIDGE maintains an organization's Certificate Authority from a secure remote location. KeyBRIDGE™ connects to the Certificate Authority via a secure TLS 1.2 connection utilizing mutual authentication to fulfill the certificate-signing request and return the certificate, signed by your Certificate Authority. All activities are automatically logged providing you with end-to-end auditability and inventory management.

With the trust model established, devices can be connected to the Internet and make real-time queries to receive an initial key load by providing a signed certificate used to establish mutual authentication. Key Distribution Hosts like KeyBRIDGE™ can facilitate this mutual authentication and deliver the requested key(s) back to the original POI device in real-time by leveraging industry standard TR-34 techniques for the asymmetric distribution of symmetric keys.

CertBRIDGE delivers:

- A secure, compliant and cost-effective PKI Infrastructure for remotely injecting encryption keys into devices with an organization's own Certificate Authority.
- Architecture that allows an organization to maintain complete control of their Root CA and PKI recovery materials.
- The ability to generate and store keys in a compliant hardware platform.
- Automated and simplified key management activities, resulting in cost savings.
- The capability to track and revoke certificates through Certificate Revocation Lists (CRLs).
- Unique remote key delivery techniques with Asymmetric cryptography.
- Guaranteed high availability and effective disaster recovery.
- GEOBRIDGE expertise on hand to meet cryptographic compliance mandates.
- Devoted PKI expertise for implementation and management.
- Constant monitoring with guaranteed response time.

About GEOBRIDGE

Established in 1997, GEOBRIDGE Corporation 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 an active participant in many standards-based organizations, sought after to provide industry leading subject matter expertise for Cryptographic Key Management, Payment Security, and Compliance related services. GEOBRIDGE's client list includes Fortune 500 companies, financial institutions, healthcare organizations and government clients across North America and around the globe. GEOBRIDGE leverages their team's expertise in data protection, program development, enforcement and governance to help architect solutions to help mitigate risk for clients. Visit www.geobridge.net for more information.

About Certified Security Solutions (CSS)

As the market leader in enterprise and IoT digital identity security for data, devices, and applications, CSS is a cybersecurity company that builds and supports platforms to enable secure commerce for global businesses connected to the Internet. Headquartered in Cleveland, Ohio, with operations throughout North America, CSS is at the forefront of delivering innovative software products and SaaS solutions that are secure, scalable, economical, and easy to integrate into any business. Visit www.css-security.com for more information.

Contact Us

css-security.com

877.715.5448