Data Sheet

KeyBRIDGE POI Solution

KeyBRIDGE POI supports more than 350 devices from renowned manufacturers of POI systems.

KeyBRIDGE POI (Point of Interaction) Solution

GEOBRIDGE Corporation has a large footprint in the payment processing industry for over two decades. The knowledgeable and skilled GEOBRIDGE team has developed the remarkable KeyBRIDGE 4100 POI to be a state of the art key injection appliance, keeping up with the technology of the very dynamic payment industry.

KeyBRIDGE POI supports both DUKPT and Master/Session methodologies and key loading, while enabling customers to load and support EMV keys. Additional terminal-specific functionality is also supported through the KeyBRIDGE injection dashboard for each supported device. Custom wiring diagrams detail all of the necessary features and functions of KeyBRIDGE-certified point-of-interaction terminals so that users have all of the necessary details to properly load each device.

Some of the standard product features are:

- Centralized and secure key storage
- Detailed key inventory
- POI key erasure functionality to clear production keys from POS devices prior to transporting
- Ability to update the System Master Key (SMK) for periodic key rotation
- Supported keys include:
  - Double & triple-length TDES keys
  - 128, 192 & 256-bit AES keys
  - Single & double length Master/Session keys
  - RSA key pairs and certificates
  - ECC key pairs and certificates

GEOBRIDGE by utimaco

Compliance at the Highest Level

GEOBRIDGE participates and monitors both national and international standards. The KeyBRIDGE platform was designed with compliance and security standards being the most important consideration in our development. Our customers can always look to us for guidance and be assured that the KeyBRIDGE complies with the following industry standards:

Supported standards:

- **ANSI X9.24-1-2017:**
  Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
- **ANSI X9.24-2-2016:**
  Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
- **ANSI X9.24-3-2017:**
  Retail Financial Services - Symmetric Key Management Part 3: Derived Unique Key per Transaction
- **ANSI X9.TR 39-2009:**
  TG-3 Retail Financial Services Compliance Guideline Part 1: PIN Security and Key Management
- **ANSI X9.TR 31-2018:**
  Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
- **ANSI X9.TR 34-2012:**
  Interoperable Method for Distribution of Symmetric Keys Using Asymmetric Techniques Part 1: Using Factoring-Based Public Key Cryptography Unilateral Key Transport
- **ANSI X9.97-2009:**
  Financial services – Secure Cryptographic Devices (Retail) Part 1: Concepts, Requirements and Evaluation Methods
- **ANSI X9.52-1998:**
  Triple Data Encryption Algorithm Modes of Operation
- **Payment Card Industry (PCI) PIN Security Requirements**
- **FIPS 140-2:**
  Security Requirements for Cryptographic Modules, Security Level 3, Certificate #2434

Role Based Access Controls

When it comes to security on the KeyBRIDGE platform, one of the most important aspects is Access Controls. The KeyBRIDGE solution enforces the concepts of dual control and split knowledge, with extensive audit logging to capture each action that is performed. All activities can be reliably traced to at least two unique personnel. Additionally, the KeyBRIDGE appliance architecture is rooted in role-based access to ensure appropriate controls and restrictions for performing sensitive functions. The four user roles in KeyBRIDGE are:

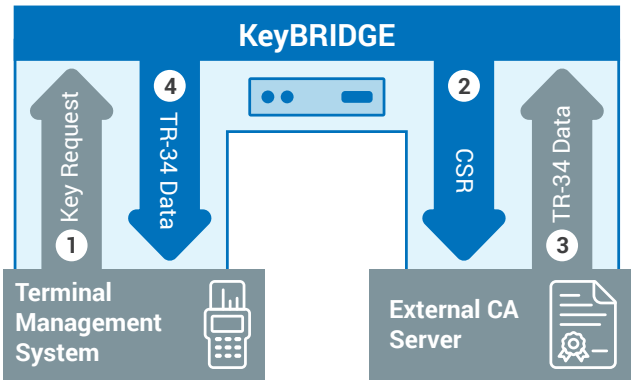
- **Manager**
- **Key Custodian**
- **Supervisor**
- **Operator**

The assigned role will dictate the access and capabilities of a given user. Each role has specified privileges to allow access based on the need to know of the user.

State of the Art Technology

One of the newest features on the KeyBRIDGE is the ARCK™ API, (API for Remote Centralized Key Management). This is a simple JSON Schema RESTful API that allows for new schemas to be included for support in rapid fashion. Basic key generate, import, export, and delete, along with a suite of administrative and audit functions that are all available as GET and POST commands. Additionally, KeyBRIDGE now supports the ability to serve as the client, allowing for KeyBRIDGE to POST keys to designated endpoints.

The API can even be used for the purposes of issuing Cryptographic Signing Requests to third party Certificate Authorities. The KeyBRIDGE architecture supports the ability to define custom APIs for automated key exchanges to external systems and applications. Baseline key exchange formats leverage X9 TR-34 key payload formats, but APIs may be tailored to support specific requirements of the receiving system. The APIs leverage TLS 1.2 for secure data transport and built-in certificate management supports full trust chain validation for each communicating device.



Additional features that can be licensed include:

- **Remote Audit Management:** (ARCK™ API) enables the remote access by management to perform audit and statistic reporting.
- **SCD Component Entry:** Allows users to securely enter TDES or AES components through a separate, removable Secure Cryptographic Device (SCD) and send them encrypted to the KeyBRIDGE appliance for storage and use.
- **Network Support:** Allows users to save data such as audit logs, key inventory and system backups from the KeyBRIDGE appliance to a network drive.
- **Custom PED Key Export:** Allows users to define a specific format for the export file(s) containing POI keys, as well as allows users to change the names associated with POI models.
- **Custom Key Usage:** Allows users to define additional Key Usages and determine the permissible characteristics of those Custom Key Usages.
- **Custom Key Attributes:** Allows users to create up to 12 custom attributes at the key level.
- **Real-Time DID Back-Up:** Perform real time backups of your DID counters ensuring that no future keys end up as duplicates for previous deployments.
- **Certificate Management:** KeyBRIDGE allows for the centralized management of X.509 and PKCS #7 certificates.
- **Securing Secret Data:** KeyBRIDGE allows users to securely store secret data such as HSM master key components, passwords, PINs, safe combinations, access codes, and derivation data. Virtually any piece of information that is frequently stored in physical safes can be securely stored and tracked within KeyBRIDGE.

Beneficial and Effective Audit Logging

The KeyBRIDGE appliance logs every user action regardless of status (pass or fail). Each record in the system audit log will contain the following information:

- A unique audit record ID
- Date and timestamp
- User IDs
- Function performed
- Relationship
- POI Terminal Details (injection only)
- Key Serial Number – KSI & DID portion only (injection only)
- Status: Pass or Failure
- Additional discretionary data (function specific)

Managers may view all audit records and select specific records to be printed or saved to a USB drive or shared network resource using the search filter and selecting the appropriate records. Other roles may only view audit records. The KeyBRIDGE appliance limits the size of audit logs and requires periodic archival. The range of records may be chosen by either a date or an absolute number. Once the range is chosen, it will be saved to a file on a USB drive or shared network resource. The appliance will assign a batch ID. The appliance will maintain an archive record batch log to keep a record of archive activity.

Customer Commitment

Secret Data

Each secret is owned by a designated Key Custodian Group. Retrieval of the secure data requires dual control access from two key custodians assigned to the group to which the secret data is associated. Once the credentials have been validated, the secret data may be printed to a secure form.

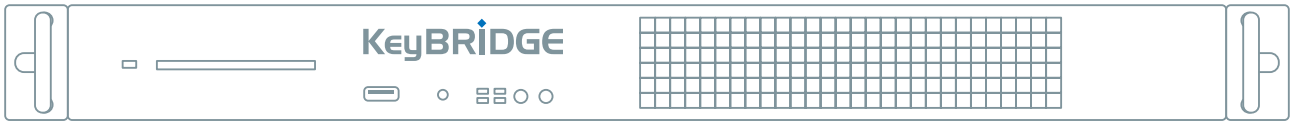
Listening to our Customers

GEOBRIDGE believes our customers know their day-to-day environment, and understand what it takes to refine productivity in doing key injections. That's why many of our KeyBRIDGE version releases include enhancements that are driven by customer feedback and recommendations. When our customers tell us about their ideas for making process improvements to the KeyBRIDGE, we listen. Furthermore, customers that have annual support contracts, receive their KeyBRIDGE updates at no additional costs.

Support Going Above and Beyond

GEOBRIDGE customers are our most vital asset, and so we believe support begins from initial KeyBRIDGE implementation and continues with ongoing maintenance of the appliance. The GEOBRIDGE team provides white glove support while working with customers around the globe to provide exceptional technical support for all of our products and services.

Technical Specifications



KeyBRIDGE 4100

Physical Dimensions

- **Height:** 1.75 inches (4.4 cm)
- **Width:** 17.2 inches (43.8 cm)
- **Depth:** 21.3 inches (54.2 cm)
- **Weight:** 25 pounds (11.3 kg)
- **Controls:** Power on/off switch, unit ID switch

Connectivity

- **Communications Ethernet:** TCP/IP, TLS 1.2 (only)
- **LAN Connection:** 10/100/1000BASE-T (RJ45) auto-sensing

Electrical

- **Rated input voltage:** 100 to 240 VAC
- **Rated input current:** 5 A at 100 VAC 3 A at 240 VAC
- **Rated input frequency:** 50 Hz to 60 Hz
- **Rated input power:** 300 W

Operating Environment

- **Temperature:** 10°C to 35°C (50°F to 95°F)
- **Relative humidity:** 5% to 80% Non-condensing

Certification/Compliance

- **Safety / Emissions:** UL62368-1 + CB62368-1/60950-1, CE/FCC, RCM #1 Australia

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. Guided by the credo that information security solutions should support, rather than dictate, business requirements, GEOBRIDGE continues to find new mechanisms that leverage our customers' security measures to better meet their business needs. Today, GEOBRIDGE is a leading information security solutions and compliance provider that supports a diverse global client base in retail, financial services, manufacturing and key injection facilities.

GEOBRIDGE brings together a team of highly skilled and highly experienced Network Security Architects, Application Developers, Cryptographic Key Management Experts and Project Management professionals who are fully invested in satisfying the security and compliance requirements of our customers.

Contact

GEOBRIDGE Corporation

20110 Ashbrook Place, Suite #125,
Ashburn, Virginia 20147

+1 571.799.0145

Sales@geobridge.net

For more information about GEOBRIDGE products, please visit:

geobridge.net