Product Brochure

KeyBRIDGE TokenBRIDGE Secure and Easy-to-Manage Tokenization

Creating Trust in the Digital Society

utimaco® 40 YEARS

Unique Tokenization with the Proven Data Security Standard and High Availability (HA)

As more and more sensitive data is transferred and stored electronically, the communication networks over which it travels and the databases that store it become tempting targets for criminals. The spate of announcements detailing the consumer community victims of the latest attacks is almost routine. In response, industries such as the payment industry and enterprises have struggled to protect the data it manages, with varied success. Regulations mandated by the industries, such as PCI-DSS and GDPR, are industry standards that attempt to articulate best practices for how merchants, processors, and financial institutions should protect their cardholder data for the banking and financial services (BFS) and similarly for enterprises respectively.

Data protection under strict regulations is a **requirement of all industries**.

Data protection under strict regulations is a requirement of all industries. For example, there is a necessity for industries like automotive, IoT and manufacturing to share only relevant data with 3rd parties covering sensitive data. Various government agencies hold a lot of public information. For making public improvement decisions, they need to share the data or combine it with other publicly available data. Protecting sensitive data during these transfers is the topmost priority for government agencies. Similarly, almost all industries share, store, and process sensitive data, and the risk faced while transferring the sensitive data back and forth multiplies.

While encryption is available as one solution to data protection, industries are also looking for alternative solutions to implement based on their requirements. In such cases, tokenization is the required solution to solve business problems.

Tokenization (replacing a sensitive data element with one that has no exploitable value) can reduce the complexity of the data protection solution because the cryptography and key management required to implement a tokenization solution are hidden behind the Token Vault.

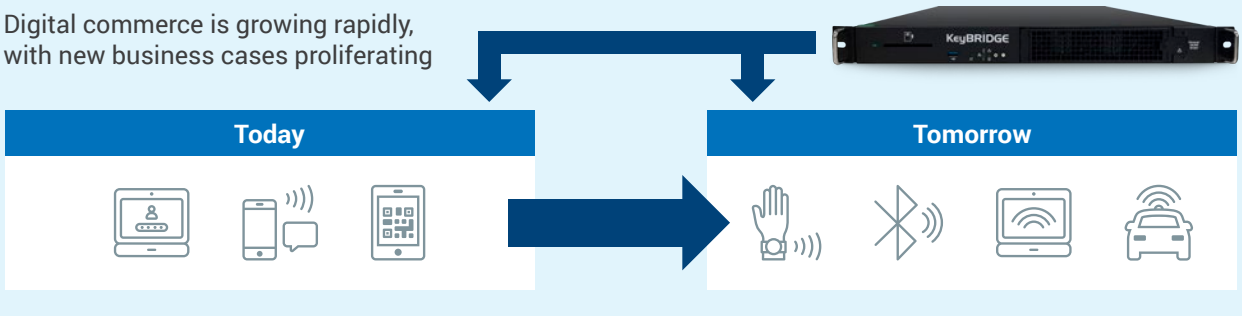
UTIMACO
KeyBRIDGE TokenBRIDGE

Reliable Security
Provides a complete solution with a built-in HSM, database, and token management system

Meet Compliance Standards
PCI HSM v3 and FIPS 140-3 L3 Certified

Easy Crypto Management
Enables Detailed Token Inventory

Full Control over Your Keys
Provides Centralized Key Storage



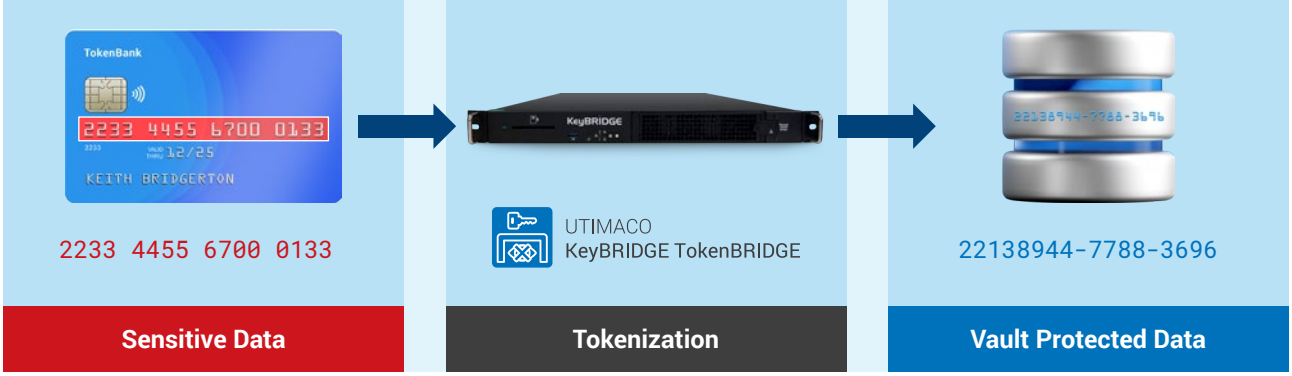
TokenBRIDGE licensed on the KeyBRIDGE appliance, implements a secure, easy-to-manage Token Vault, the core of any tokenization solution. The KeyBRIDGE TokenBRIDGE appliance is an ideal solution to the Token Vault requirement and how it assists in achieving PCI DSS compliance and General Data Protection Regulation (GDPR).

Tokenization turns sensitive data into an unrecognizable string of characters that are rendered unusable without the tokenization system in place and, if stolen, provides no value to cybercriminals.

Industries

- Banking and Financial Services
- Automotive and Integrated Mobility
- Manufacturing and IoT
- Retail
- Cloud / Cloud Service Providers
- Government and Public Sector
- Telecommunications
- Energy and Utilities
- Logistics and Transportation
- Many more

TokenBRIDGE Solution



Key Features

Random and Format-Preserving Tokenization

TokenBRIDGE allows the creation of highly scalable, flexible, and customizable tokens in any format, enabling to securely store and access tokens and their sensitive data within a single, centralized location. It provides vault-based tokenization with a true token vault. The tokens are generated based on a true hardware-based, FIPS-certified Random Number Generator.

High Physical and Logical Security

TokenBRIDGE allows a role-based access control (RBAC) enforced with dual control and split knowledge. Also, it is possible to organize the tokens by creating a logical relationship structure for more compliant handling. TokenBRIDGE provides a physically secure enclosure. It means that opening or penetrating the enclosure automatically erases the System Master Key (SMK), preventing access to the entire token database.

TokenBRIDGE Maximizes Availability

TokenBRIDGE also offers a High Availability (HA) option, permitting multiple appliances to be integrated into a self-replicating network. Appliances may be separated geographically, allowing tokens issued by one appliance to be recovered on another.

Easy Integration into Existing Crypto Environment

TokenBRIDGE provides Simple JSON Schema RESTful API-driven functionality. No client is needed to deploy or maintain. TokenBRIDGE works as an appliance that can be easily integrated as part of a mesh IT network.

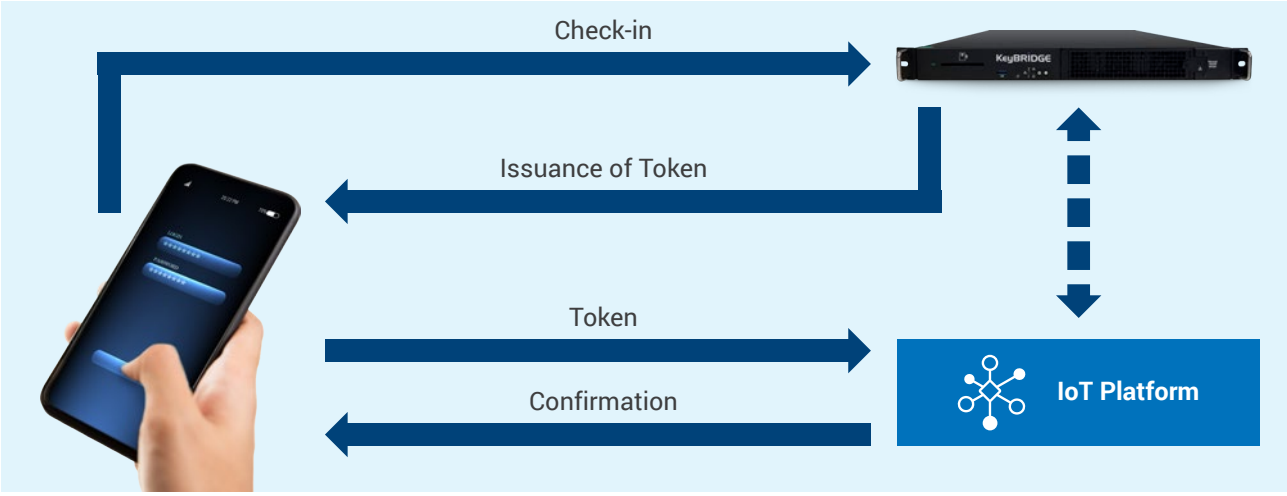
Other Features

- **Remote communications protected by TLSv1.2** with only high strength cipher suites, utilizing mutual authentication with client profile connections authenticated by their certificates.
- **Remote Management** permits appliance maintenance and configuration without requiring physical proximity.
- **Automates activity tracking within the system**, capturing token activity details and user activity, as well as comprehensive audit logging of all sensitive functions.
- **Configurable network settings** enable access to shared network storage for secure file storage and access.
- **Configurable automated** daily backup function.

Special Application of Automotive/IoT Industry

Along with the increase in IoT devices, IoT security management is a crucial point to consider. To provide the ultimate security to devices, TokenBRIDGE enables to trust the devices connecting to the IoT platform. TokenBRIDGE as a connecting point between the IoT platform and devices ensures that the data is trustful and the devices are authenticated by creating an air-gapped solution.

For example, a smartphone can be authenticated using the token from TokenBRIDGE before it is used to unlock the car. For this, the IoT platform can send the smartphone request to prove its identity and integrity with TokenBRIDGE. The smartphone would check in to TokenBRIDGE and verify its identity/ integrity. On successful validation, a valid token will be issued by TokenBRIDGE that the smartphone can validate with the IoT platform. The IoT platform can check the token's authenticity and confirm that the smartphone is valid to unlock the car. Using a token also allows a more straightforward mechanism to add and revoke privileges.



UTIMACO's TokenBRIDGE solution is well-designed to accommodate all the requirements that are put forward by new regulations like WP. 29. WP.29 is the UN World Forum dedicated to technical regulations applied to the broad automotive sector, addressing the safety and environmental performance of wheeled vehicles, their subsystems, and parts. Some of the requirements and risks defined by WP. 29 for vehicle security are listed below along with solutions from TokenBRIDGE.

WP. 29: Harmonization of Vehicle Regulations: Requirements that manufacturers have to follow:

Requirement	TokenBRIDGE Solution
#3.3b: The manufacturer shall ensure that any material made open for inspection at the time of type approval remains available for at least a period of 10 years counted from the time when production of the vehicle type is definitively discontinued.	TokenBRIDGE can create the tokens of data for 10 years to place in a logical order and with the de-tokenization capability.
#7.2.2.2h: Cyber Security Management System to provide relevant data to support analysis of attempted or successful cyber-attacks	TokenBRIDGE creates tokens that can be used to provide the relevant data for analysis.
#7.2.2.4 b: The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring includes the capability to analyze and detect cyber threats, vulnerabilities, and cyber-attacks from vehicle data and vehicle logs. This capability shall respect the privacy rights of car owners or drivers, particularly with respect to the consent.	TokenBRIDGE creates tokens that can be used to hide sensitive information.
#7.3.5: The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications, or data.	TokenBRIDGE can create the tokens of data to place in a logical order and with the de-tokenization capability.

How and where can TokenBRIDGE help to mitigate the risks mentioned in WP.29?

Risk	Requirement from WP.29	TokenBRIDGE Solution
#3.5: Information breach by unintended sharing of data (e.g., admin errors, storing data in servers in garages)	Security Controls are applied to back-end systems to prevent data breaches.	TokenBRIDGE security by design helps revoke compromised tokens without impacting and searching internal records.
#7.1: Interception of information / interfering radiations / monitoring communications	Confidential data transmitted to or from the vehicle shall be protected.	Tokens from TokenBRIDGE will help to transfer the confidential data.
#12.1: Compromise of over-the-air software update procedures. This includes fabricating the system update program or firmware	Secure software update procedures shall be employed.	Software updates can be done through the tokens.
#19.1: Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software)	Access control techniques and designs shall be applied to protect system data/ code.	Copyrights or proprietary data should be protected with tokens, so even if it is stolen, it is useless to attackers.
#19.2: Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.	Through system design and access control, it should not be possible for unauthorized personnel to access personal or system-critical data.	TokenBRIDGE security by design where a token can be easily revoked centrally including sensitive data available to authorized parties.
#20.1: Illegal/unauthorized changes to a vehicle's electronic ID	Access control techniques and designs shall be applied to protect system data/ code.	Sensitive data is maintained only at the backend. There are no copies making it easier to control data originality.
#31.1: Information breach. Personal data may be breached when the car changes user (e.g., is sold or is used as a hire vehicle with new hirers)	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data.	TokenBRIDGE uses token which meets the security by design GDPR requirement.

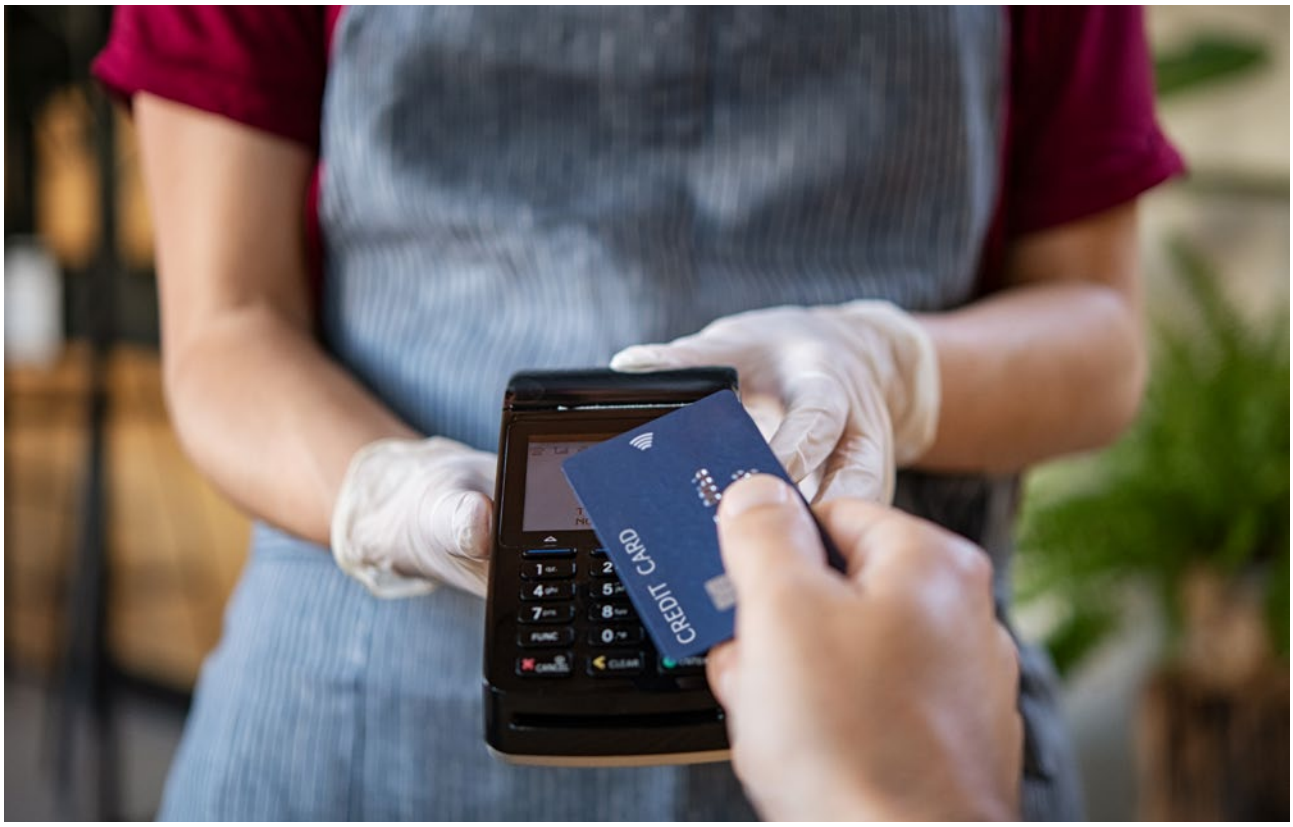
How can TokenBRIDGE help to meet PCI-DSS requirements?

Requirement 3: 'Protect Cardholder Data' and the Capabilities of TokenBRIDGE

The purpose and intent of Requirement 3 is to set standards for protecting cardholder data in storage. Clearly, the best solution is not to store cardholder data unless essential and for the shortest possible time. But if an attacker manages to breach all other safeguards and does get access to stored data, that data should be in a form useless to him. By replacing the data with a token, the attacker cannot use the token to create fraudulent transactions.

TokenBRIDGE stands apart

While most other tokenization solutions rely upon software-based encryption and software-based random number generation, these solutions remain susceptible to the same types of attacks that a nefarious actor would employ to breach other safeguards. Using a FIPS-certified Random Number Generator and a FIPS-certified hardware solution, an attack is far more likely to be thwarted.



Relevant requirement 3 subsections, and how TokenBRIDGE helps to satisfy the requirements.

Requirement	TokenBRIDGE Solution
Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.	TokenBRIDGE can create a PAN token that is either entirely random or an EMV payment token that uses a different PIN. In either case, the PAN token is useless to an attacker.
Render PAN is unreadable anywhere it is stored (including on portable digital media, backup media, and in logs).	Once tokenized, the original PAN is only recoverable by authorized entities. Consequently, any database backups that include the token are likewise protected.
Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	Because the token is a random number and not the encrypted PAN, no complex key management procedures are required, simplifying the implementation.
Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	Substituting random tokens for cardholder data obviates the need for keys. Consequently, TokenBRIDGE installation and ongoing maintenance are significantly simplified.
Production data (live PANs) are not used for testing or development.	Utilizing a token instead of a live PAN will assist in supporting this requirement, particularly that TokenBRIDGE can produce tokens that will satisfy Luhn and Reserved Luhn checks.
Insecure cryptographic storage.	TokenBRIDGE stores all data utilizing FIPS 140-2 Level 3 hardware while leveraging AES 256-bit encryption.
Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	TokenBRIDGE allows for user-definable formats to produce any type of token. TokenBRIDGE stores all data utilizing FIPS 140-2 Level 3 hardware while leveraging AES 256-bit encryption.
Physically secure all media.	TokenBRIDGE allows for the storage and subsequent encrypted backup of any data. TokenBRIDGE stores all data utilizing FIPS 140-2 Level 3 hardware while leveraging AES 256-bit encryption.
Implement audit trails to link all access to system components to each individual user. Including all 10.3 requirements: • User ID • Type of event • Date/Time • Success/Failure • Origination event • Identity of affected data, component, or resources	TokenBRIDGE is equipped with audit log functionality beyond repudiation, logging all token distribution and de-tokenization requests to an individual end-point.
A list of all such devices and personnel with access.	TokenBRIDGE utilizes unique connection profiles for each endpoint while enforcing TLS 1.2 mutual authentication requirements.

Technical Details

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) autosensing

Electrical Characteristics

- **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

Cryptographic Algorithms

- **Asymmetric algorithms/lengths:**
  RSA: 1024, 2048, 3072, 4096 Bits
  ECC: NIST, SEC 2 and Brainpool elliptic curves, 160 – 571 Bits
- **Symmetric algorithms/lengths:**
  DES, TripleDES; AES 128, 192, 256 Bits
- **Hash Functions:**
  SHA1, SHA224, SHA256, SHA384, SHA512 Bits
- **Message Authentication:**
  CMAC, HMAC
- **Compliance with all relevant industry standards:**
  - **NIST SP 800-90A Rev. 1:** Recommendation for Random Number Generation Using Deterministic Random Bit Generators
  - **ANSI X9.119-2017:** Requirements for Protection of Sensitive Payment Card Data – Part 2: Implementing Post-Authorization Tokenization Systems
  - **ANS X9.97-2009:** Financial Services – Secure Cryptographic Devices (Retail) Part 1: Concepts, Requirements, and Evaluation Methods
  - **NIST SP 800-67:** Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
  - **ISO 13491-1:** Banking – Secure Cryptographic Devices (Retail), Part 1 Concepts, Requirements, and Evaluation methods.
  - **Payment Card Industry PIN 2.0 Security Requirements**
  - **Payment Card Industry (PCI) PTS HSM:** Modular Security Requirements Version 3
  - **FIPS 140-2:** Security Requirements for Cryptographic Modules, Security Level 3
  - **FIPS 197:** Advanced Encryption Standard (AES), November 26, 2001

About UTIMACO

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).

UTIMACO develops on-premises and cloud-based hardware security modules, solutions for key management, data protection, and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems. UTIMACO is one of the world's leading manufacturers in its key market segments.

500+ employees around the globe create innovative solutions and services to protect data, identities and communication networks with responsibility for global customers and citizens. Customers and partners in many different industries value the reliability and long-term investment security of UTIMACO's high-security products and solutions.

Find out more on utimaco.com

Headquarters Aachen, Germany

Headquarters Campbell, USA

Contact us

EMEA

UTIMACO IS GmbH

Germanusstrasse 4
52080 Aachen,
Germany

+49 241 1696 200

info@utimaco.com

Americas

UTIMACO Inc.

900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

+1 844 UTIMACO

info@utimaco.com

APAC

UTIMACO IS Pte Limited

6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapore 038986

+65 6993 8918

info@utimaco.com

For more information about UTIMACO® products, please visit:

utimaco.com

Creating Trust in
the **Digital Society**

utimaco®