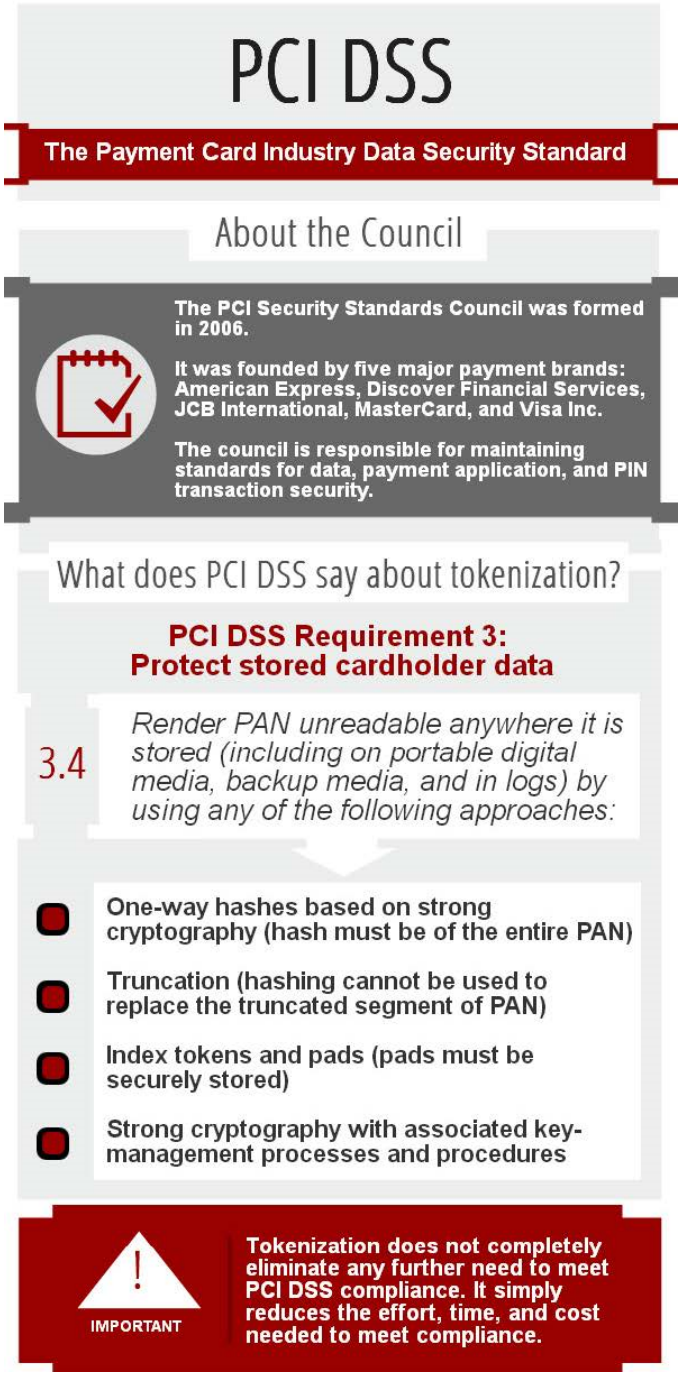
Vaultless Tokenization Overview

VAULTLESS TOKENIZATION FROM FUTUREX

Every year, financial institutions and other enterprise organizations are charged with safeguarding increasing volumes and types of sensitive data, both of their own and of their clients. This seemingly endless stream of sensitive data continues to grow, and the cost and resource dedication associated with adequately securing it is generally accepted as part of the cost of doing business in the information age. This is especially true for financial institutions responsible for handling credit, debit, and prepaid card numbers in accordance with Payment Card Industry Data Security Standard regulations. However, there are steps that these organizations can take to ease their compliance burdens while at the same time keeping their data secure. Tokenization is one of these steps. Tokenization is a method of replacing sensitive data, such a Primary Account Number (PAN), with randomly generated replacement data known as a token. This whitepaper explains the basic concepts behind tokenization and how Futurex's vaultless tokenization solution allows organizations to reduce the scope and cost of regulatory compliance by vastly reducing, and completely eliminating in some cases, the presence of clear-text cardholder data from their processing infrastructure and storage environments.



WHAT IS VAULTLESS TOKENIZATION?

Tokenization is a method of protecting sensitive data, often cardholder credentials, using cryptographically generated substitute characters as placeholder data. These characters, known as tokens, have no intrinsic value, thus they are useless if stolen. However, tokens can be decrypted in a hardware security module (HSM) to retrieve the original clear-text data when needed. This procedure is known as detokenization.

While the security benefits offered by tokenization are relatively easy to understand, those with heavy involvement in compliance and auditing operations may see a deeper and more profound benefit in the reduction in compliance scope made possible by tokenization. As tokenized data is random and contains no value, it is typically not subject to the same compliance requirements as clear-text payment data.

For financial institutions, tokenization offers an opportunity to significantly reduce PCI DSS compliance scope and cost by tokenizing as much cardholder data as possible. This potentially de-scopes substantial portions of production environments from compliance audits. On-premises tokenization from Futurex offers these organizations a significant return on investment manifested in both resources and time saved, and even greater efficiencies are possible by integrating VirtuCrypt's cloud tokenization services.

Futurex solutions are designed from the outset with turnkey implementation in mind and vaultless tokenization is no exception. From the initial stages of product conception, vaultless tokenization is geared towards easy implementation and integration into a variety of client environments. This is accomplished through robust formatting and customization options that enable tokenized data to conform to existing data entry and storage formatting parameters. Simply put, tokenization can be implemented in both on-premises and cloud environments with no changes to existing database schemas and no downtime.

VAULTED VERSUS VAULTLESS TOKENIZATION

Futurex offers an advanced method of tokenization known as vaultless tokenization. Legacy methods of "vaulted" tokenization require large databases mapping tokens to their corresponding clear data. In this model, detokenization requires the database to be queried with a token to retrieve the original data.

There are implementation, security, and compliance drawbacks to the vaulted tokenization model. Token vaults represent a single point of failure in tokenization infrastructures, and they also represent a high-risk target for theft, since they contain clear cardholder data, which is also within the scope of PCI compliance. Furthermore, large token vaults often present complex implementation problems, particularly in distributed, worldwide deployments.

Vaultless tokenization is safer and more efficient. Futurex's primary tokenization platform, the Key Enterprise Management Server (KMES) Series 3, uses a FIPS 140-2 Level 3 and PCI HSM compliant Secure Cryptographic Device to generate tokens using standards-based algorithms, which have been reviewed by experts. This method allows for a vaultless method of tokenization that eliminates the need for a vault or master token database. The encryption and key management techniques used in Futurex's KMES Series 3, as well as through VirtuCrypt's cloud-based tokenization services, provide strong cryptography to secure data at rest, also allowing for both single and multi-use tokens.

INTEGRATION INTO THE HARDENED ENTERPRISE SECURITY PLATFORM

Futurex's Hardened Enterprise Security Platform, together with the VirtuCrypt Cloud, forms the industry's only unified, end-to-end payment security platform capable of securing all facets of transaction processing.

What sets Futurex's vaultless tokenization apart from others in the marketplace is the Hardened Enterprise Security Platform, Futurex's complete product line of payment processing HSMs, key management solutions, cryptographic management platforms, and cloud-based services. These devices are built on Futurex's Base Architecture Model, a common code base that ensures all devices are fully interoperable, scalable, and easily expanded over time.

With this shared code and API functionality, organizations using Futurex products can integrate tokenized data end-to-end throughout their cryptographic ecosystem. For example, cardholder data can be encrypted at the initial point of capture using Point-to-Point Encryption (P2PE), decrypted within the secure boundary of a Futurex HSM and re-encrypted using a transfer key for payment validation by the processer, while simultaneously having a token generated for storage and future use.

In this model, data remains encrypted throughout the payment process, which potentially eliminates clear-text cardholder data from the merchant network entirely. This serves as a sophisticated, yet easily implemented, tool for reducing compliance scope. Furthermore, tokenization combines with other Futurex encryption technologies to create the industry's only end-to-end payment security solution that secures all facets of transaction processing.

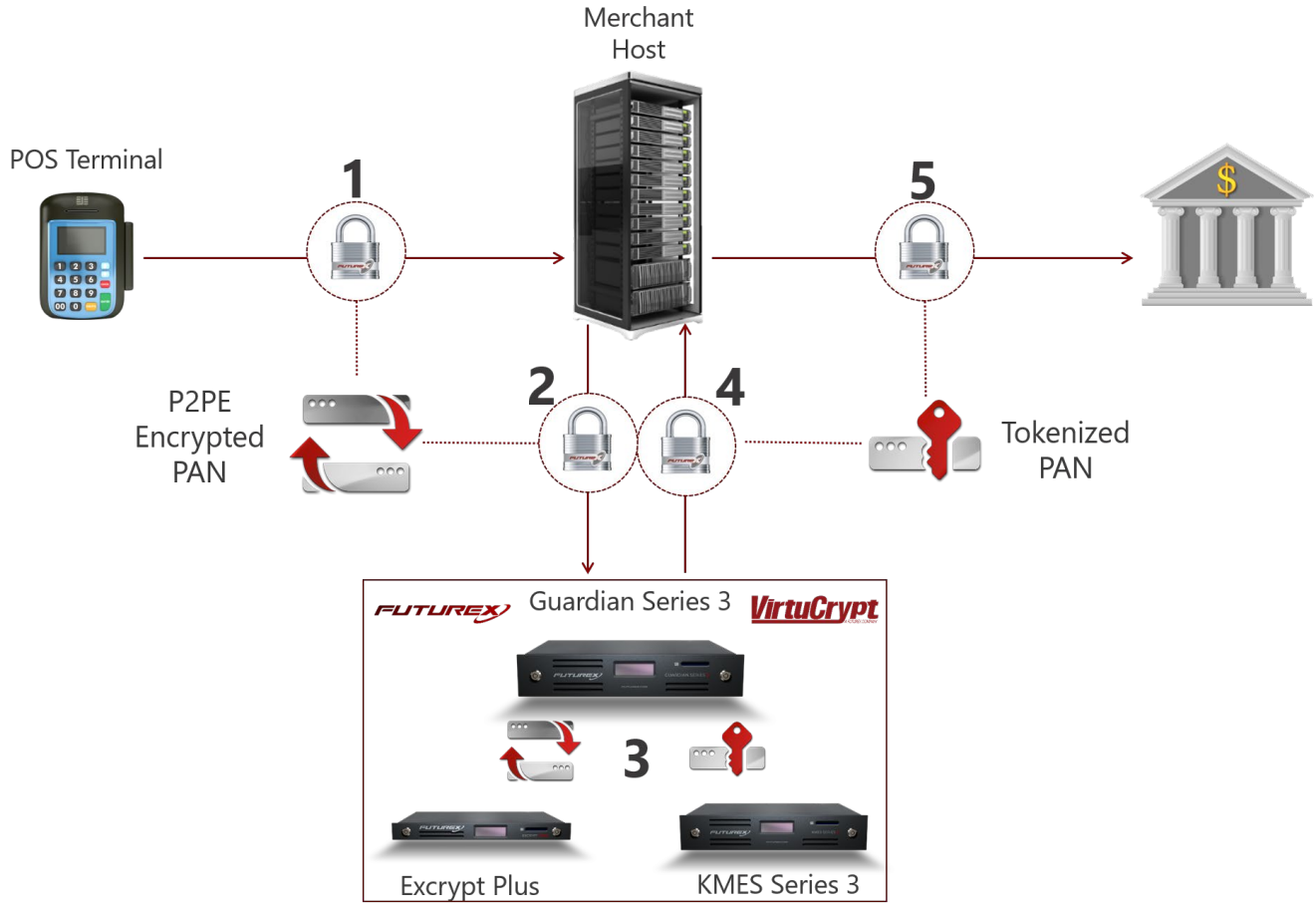
THE KMES SERIES 3

Futurex's vaultless tokenization is powered by the KMES Series 3, a robust, easy-to-use solution for managing large volumes of tokens, keys, certificates, and other cryptographic objects. The KMES is compliant with all major security standards for HSMs including PCI HSM and FIPS 140-2 Level 3.

The KMES Series 3 is powered by a high performance cryptographic module and has the capability to rapidly generate tokens through its easy-to-use interface and REST API. The process of creating tokens can be fully automated, so once the functionality is set up within the host system, an organization can be on its way to secure data storage and reduced PCI compliance scope and cost.

THE BIG PICTURE

When taking a holistic approach to cryptographic security for payment processing, Futurex tokenization can be used in conjunction with other encryption technologies, allowing organizations to potentially eliminate all clear-text cardholder data from their networks. For example, when a card is presented at a POS terminal, the PAN is immediately encrypted using Point-to-Point Encryption. When the encrypted PAN makes its way to the HSM, it can be decrypted within the secure cryptographic device boundary, tokenized, and then processed through the card issuer using the tokenized data. Under this model, the combination of POS encryption and tokenization allows for secure transaction processing and storage of cardholder credentials for future use, without ever placing cardholder data in the clear.



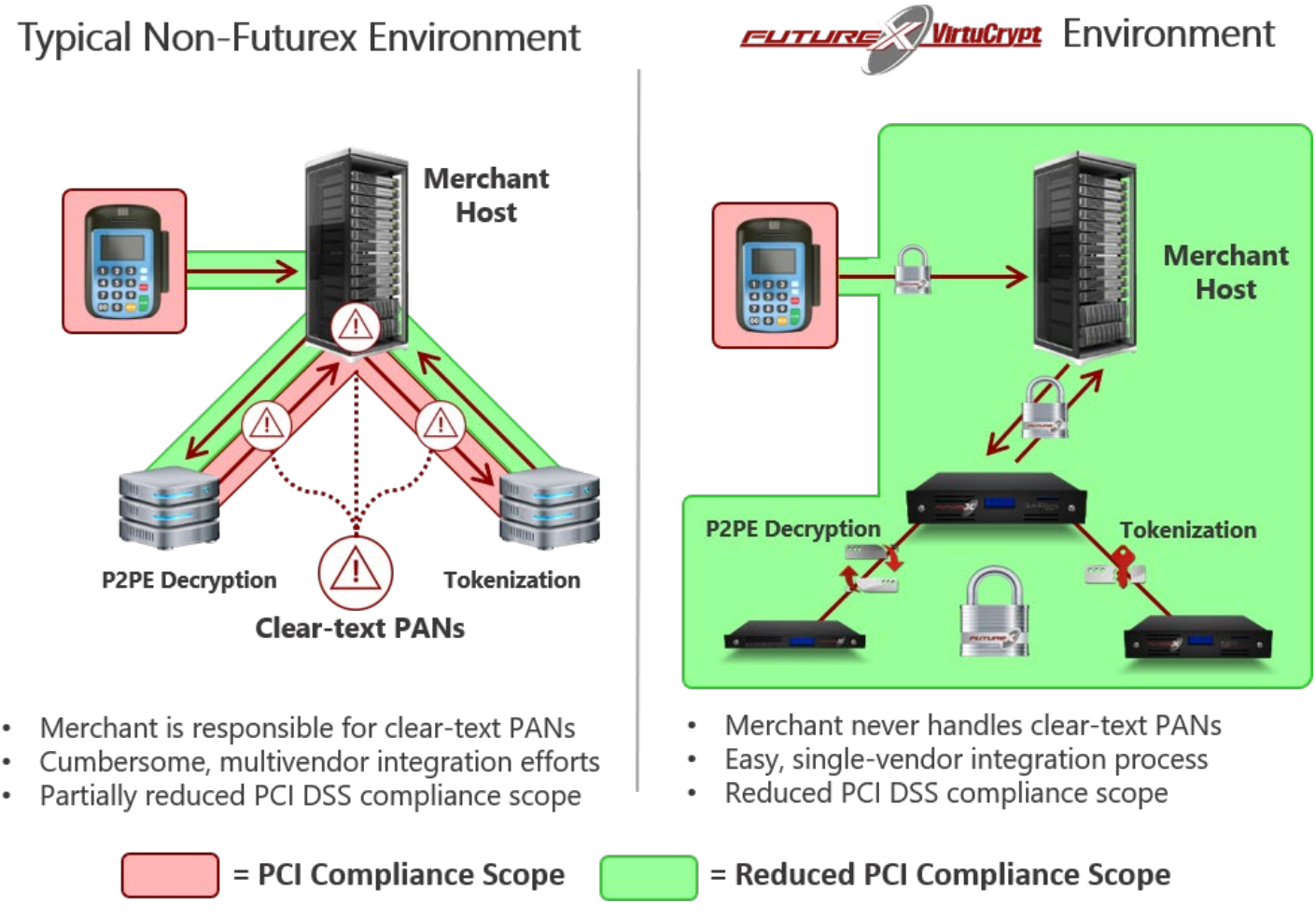
Payment Processing Using P2PE in Conjunction with Tokenization from Futurex

The diagram above illustrates a complete payment processing solution where cardholder credentials can be completely secured at rest and in motion using a combination of P2PE and vaultless tokenization. The example above consists of a Guardian Series 3 cryptographic management platform, seamlessly paired with an Excrypt Plus for P2PE and KMES Series 3 for vaultless tokenization and key management. Steps 1-5 in the diagram are outlined below:

1. The PAN is encrypted at the Point of Sale terminal using Point-to-Point Encryption.
2. The encrypted PAN is sent back to Futurex Excrypt Plus HSM.
3. Under the secure TLS-encrypted management of the Guardian Series 3, the encrypted PAN is decrypted by the Excrypt Plus HSM and then tokenized by the KMES Series 3. This process can be performed on-premises using the hardware outlined here, or entirely in the cloud using VirtuCrypt services.
4. The tokenized PAN is sent back to the merchant host.
5. The tokenized PAN can then be used for the remainder of transaction processing and business applications.

THE FUTUREX ADVANTAGE

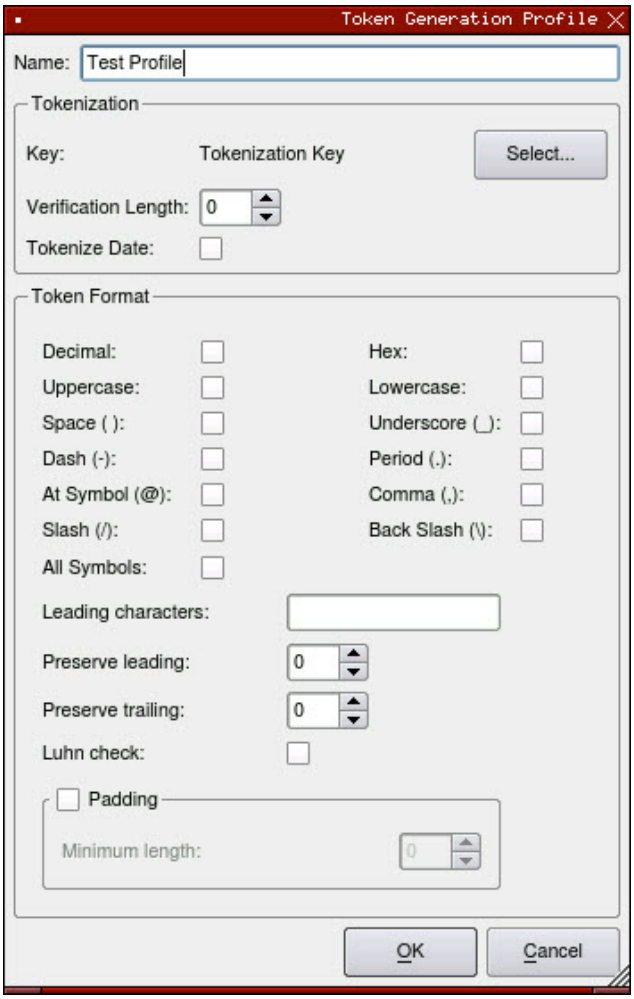
Futurex is the only hardened security provider to offer end-to-end protection for both P2PE and tokenization. No other provider offers vaultless tokenization functionality that integrates with other encryption operations to offer full lifecycle protection of payment data. Futurex makes this possible using the KMES Series 3 for key management and tokenization; the Excrypt Plus and Excrypt SSP Enterprise v.2 for payment processing and validation; the Guardian Series 3 for centralized management, monitoring, alerting, and disaster recovery; and the Excrypt Touch for turnkey, compliant remote management. These devices create a secure cryptographic environment that allows organizations to completely remove the presence of clear-text PANs and payment credentials from their infrastructure.



Typical P2PE/Tokenization Environment vs. the Hardened Enterprise Security Platform

A MULTITUDE OF OPTIONS

Futurex places a high priority on keeping its solutions highly adaptable and open to customization. This is especially true with vaultless tokenization, which offers Futurex's clients an array of customization options. Users can specify what data types are supported, formatting options, data padding, and even to what extent each user group can detokenize data. Moreover, the KMES Series 3 supports token generation profiles, so multiple sets of options and parameters can be saved and used on demand.



CUSTOMIZED TOKENIZATION PARAMETERS

Organizations have a wide range of options for the types of data they tokenize. Customizable token parameters include options for spacing, character casing, hexadecimal, symbols, slashes, underscores, dashes, periods, commas, and more. Additionally, administrators have the option to preserve certain original characters if desired. This is commonly done in the payments industry, where the last four or first four digits of PANs are typically standardized according to the card issuer. This allows financial institutions to save time resources by only tokenizing the specific characters unique to each cardholder.

The tokenizing party also has the option of adding a Luhn check to their tokens. A Luhn Check is a checksum concealed in the token, which allows merchants or card issuers to verify a token's authenticity.

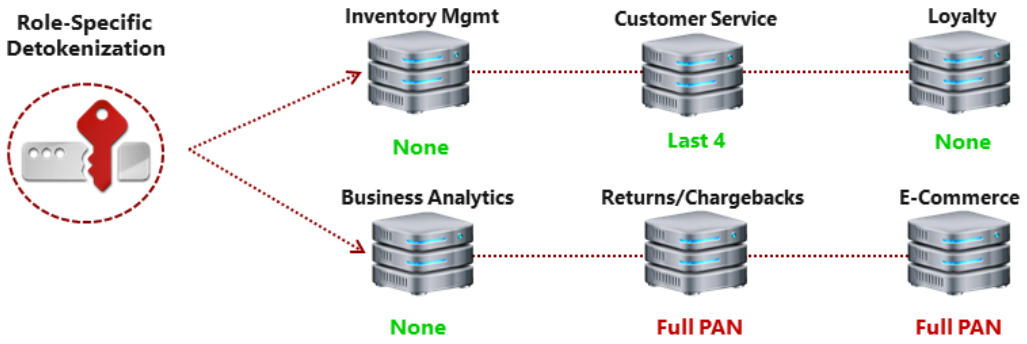
FORMAT-PRESERVING ENCRYPTION (FPE)

To aid in adoptability and integration, Futurex tokenization uses standards-based format-preserving encryption algorithms, which means that tokenized information can be integrated into existing environments with no database changes. FPE allows organizations to tokenize data in the same format as the original data. Take for example a PAN, the most common use case for tokenization. A PAN is typically between 8 and 19 numeric digits, and when using format-preserving encryption, the token will have the same number of digits. For organizations with strict database schemas, format-preserving encryption ensures tokenized data be integrated without making database changes.

In addition to format preservation, the KMES Series 3 hardware and VirtuCrypt tokenization services allow the inclusion of data padding. Data padding is a practice that involves adding extra bits to a strand of data so that it conforms to a standardized length or alignment. Standardized data length throughout database can make storage and querying more efficient. The KMES has leading and trailing padding built into its tokenization options.

CUSTOMIZED, ROLE-SPECIFIC DETOKENIZATION

The security principle of *least privilege* dictates that organizations limit unnecessary exposure to sensitive data to solely what an employee needs to do their job. Any additional access is an unnecessary exposure of sensitive data. Intelligence agencies have operated under this principle of "need to know access" for years. This reduces the risk of data breaches of both the accidental and intentional varieties. Customizing detokenization output based on user group or application role is one way to accomplish this.



Role-Specific Detokenization

With the customization options available in the KMES Series 3 and VirtuCrypt cloud, administrators can control exactly how much detokenized data any one employee or application is able to view. For example, loyalty applications may find a partially detokenized account number, perhaps just the last four digits of a credit card number, sufficient to do their job, while an e-commerce application would likely require a fully detokenized account number for repeat purchases. Still other applications, like business analytics, may be able to use the token itself as an identifier without any need to ever detokenize it. Futurex's vaultless tokenization allows these options to be customized for all parties and managed from a central location.

BATCH TOKENIZATION AND MIGRATION

Futurex's vaultless tokenization offering supports large-scale batch tokenization for integration into existing environments. Similarly, Futurex also supports token migration for clients with an existing tokenization solution. This token migration is accomplished with a purpose-built transfer application that securely migrates existing tokenized data into Futurex's tokenization infrastructure. In addition to tokenization, this application will also transfer existing encryption keys, if applicable, from the client's tokenization environment into the Futurex Hardened Enterprise Security Platform. These keys are secured under a key exchange key (KEK) to protect and simplify the transfer process.

THE VIRTUCRYPT HARDENED ENTERPRISE SECURITY CLOUD

For organizations preferring cloud functionality over on-premises hardware, VirtuCrypt offers cloud access to tokenization-as-a-service functionality. This is especially well-suited for organizations looking to provide tokenization to their own clients. VirtuCrypt is a cloud-based provider of advanced data encryption and processing solutions. All VirtuCrypt services are powered by Futurex hardware, which includes the KMES Series tokenization platform. As such, all the functionality, features, and benefits discussed throughout this whitepaper are also available through the VirtuCrypt Cloud.

All VirtuCrypt Services are accessible and manageable through the VirtuCrypt Intelligence Portal (VIP) Dashboard. The VIP Dashboard is a secure, intuitive web application for organizations to review all information related to their VirtuCrypt infrastructure.

Looking Toward the Future: The Anticipated Impact of Tokenization

Tokenization is currently used primarily in financial transaction environments to secure electronic, card-based payments. The widespread adoption of tokenization in this industry has ushered in substantial increases in security and an overall reduction in compliance costs for organizations around the world.

The proven success of tokenization has applications across multiple industries and sectors. It can be expected that a wide range of organizations, from healthcare providers to government agencies, will take advantage of the myriad of benefits of using this versatile and powerful technology.

With the cross-industry application of the KMES Series and VirtuCrypt Hardened Enterprise Security Cloud, organizations can expand their tokenization infrastructure to encompass a broad array of data types in addition to payment card data. As standards and best practices continue to evolve, Futurex will remain at the forefront of innovation, enabling our customers to safeguard their most sensitive data.

FUTUREX.COM

OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163

FUTUREX ENGINEERING CAMPUS