Voltage Secure Stateless Tokenization

CyberRes
Voltage

An independent analysis of the capabilities and security of the

CyberRes Voltage Secure Stateless Tokenization solution

Date: May 2022

FOREGENIX

Foregenix Inc.
Boston, MA 02109

T: +1 877 418 4774
info@foregenix.com
www.foregenix.com

Executive Summary

CyberRes, a Micro Focus line of business, engaged Foregenix to perform an analysis of the Voltage Secure Stateless Tokenization (SST) solution and provide feedback on the strengths and weaknesses. The Foregenix SST evaluation process not only included a deconstruction analysis of the tokenization engine, but also interviews with developers to ensure a complete and accurate understanding of the technology. Foregenix also established a test environment to evaluate the token generation and data protection process of the SST engine.

Following a review of the Voltage SST design, several obvious advantages surfaced. Because the mapping table is static, there are no performance issues as the volume of tokens increase. The mapping table remains fixed regardless of the number of tokens that might be generated by the system. This design also enables virtually endless scalability because multiple instances of the Voltage SST solution can be deployed across geographically diverse regions without the need to replicate data beyond the initial setup of the configuration parameters and mapping table.

Foregenix's performance tests for generating varying types of tokens using sample data sets (payment card data, U.S. Social Security numbers, name and address information, and healthcare records) revealed microsecond response times for both token generation and data reconstruction.

Following a detailed analysis of the CyberRes Voltage SST solution, Foregenix determined that SST maintains the highest levels of security through the use of strong, standards-based, reversible table-based tokenization. By eliminating the database used in traditional tokenization solutions, the Voltage SST solution provides enterprise-level performance, security, and scalability that cannot be matched by legacy platforms.

Introduction

Many people do not realize that the concept of tokenization has been used for hundreds of years across a host of different situations. We have all seen movies where gamblers are playing high-stakes poker games. Players sit around a poker table sizing up their competition, trying to determine who has the best hand and how much to wager. In the old Western movies, large stacks of cash would be placed at the center of the table following each gambler's wager, which presented some unique opportunities for thieves and villains. Soon casinos began using poker chips as a substitute for cash at poker tables. Players exchange cash for poker chips at a secured counter with a trusted teller. Each casino issues their own poker chips, which are marked with unique designs such that they can only be used at that specific casino. The poker chips thus have a monetary value, but only in the context of the casino that issued them.

Modern-day tokenization in the digital world operates in much the same way. The protection of sensitive data through tokenization is accomplished by substituting the original sensitive data with a token that supports the business processes, but without exposing the sensitive data to unauthorized parties and unnecessary risks. This whitepaper reviews traditional tokenization technologies and describes how Voltage Secure Stateless Tokenization (SST) 3.0 performs in comparison.

FOREGENIX

Foregenix Inc.
Boston, MA 02109

T: +1 877 418 4774
info@foregenix.com
www.foregenix.com

Tokenization Overview

Tokenization is simply a method of replacing sensitive information with a surrogate value (a "token") that allows users to interact with the token as opposed to the original sensitive information, thereby eliminating the exposure of sensitive data to typical security risks and compliance implications (Illustration #1). The token value can be used for referencing financial transactions, U.S. Social Security numbers, protected healthcare information, or other protected data sets such that the original sensitive data is not exposed. Think of a token as a unique pointer to the sensitive data.

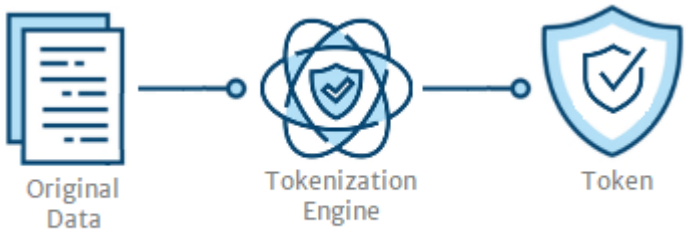

Illustration #1

Typically, these token values are only used within the confines of known, trusted entities and platforms such that, when needed, the original sensitive data can be referenced or reconstructed. If the token value is compromised by an attacker, the original sensitive data is still protected, and the token value cannot be used within other environments for malicious intent. The token has no value on its own: it only has value when it is used within secured and isolated environments to reference or reconstruct the original sensitive data.

Traditional Tokenization

Tokenization solutions deployed over the last several decades have typically used the database tokenization model. With this type of solution, a large database is maintained that maps the token values to the original sensitive data set being protected. The image shown below (Illustration #2) depicts a very simple example of tokenization based upon a database substitution model. While the database model provides a tokenization solution to protect data, it is plagued with several shortcomings. First, the database tokenization model does not scale well within large enterprise environments. As the database grows to support more token values, system performance degrades. This performance degradation can be especially problematic for real-time processing environments such as those that support credit card authorizations, where sub-second response times are critical. Second, business continuity, disaster recovery, and data replication and synchronization become challenging for large database tokenization environments. Scalability and reliability are difficult to maintain as the environment grows. Third, the database containing the sensitive data becomes a high value target for attackers because of the volume of sensitive data that it contains. Security controls and increasing compliance requirements for protecting large database environments can become more difficult than simply protecting the original sensitive data as it is being stored, processed, or transmitted.

Illustration #2

Foregenix Inc.
Boston, MA 02109

T: +1 877 418 4774
info@foregenix.com
www.foregenix.com

Voltage Secure Stateless Tokenization (SST) v3.0

CyberRes, a Micro Focus line of business, engaged Foregenix to perform an analysis of Voltage SST 3.0 and provide feedback on the strengths and weaknesses of the solution. The Foregenix SST evaluation process not only included a deconstruction analysis of the tokenization engine, but also interviews with developers to ensure a complete and accurate understanding of the technology. Foregenix also established a test environment to evaluate the token generation and data protection process of the SST engine.

Initially, it is important to understand the overall design of Voltage SST and that unlike traditional tokenization solutions, the Voltage SST solution leverages a dramatically different architecture that does not use a database. Sensitive data sets are transformed into token values using complex computational processes based on validated NIST standards.

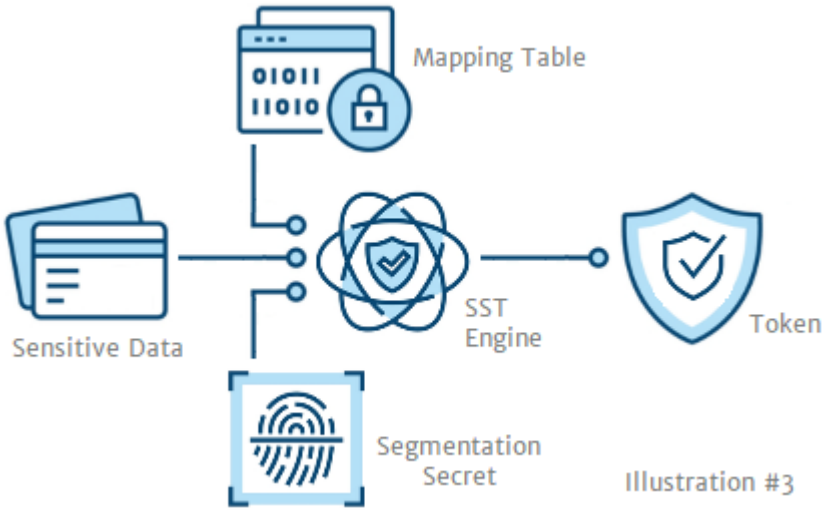

Illustration #3

Before diving into more detail on the Voltage SST transformation engine, it is important to understand the additional components used to generate the token. The image below (Illustration #3) depicts the core components used in the token generation and data reconstruction processes and can be used as a reference for the discussion that follows. The tokenization engine leverages several different inputs to generate the token value. The original sensitive data set along with configuration parameters, a mapping table, and a segmentation secret are passed to the tokenization engine to generate the token value. First, the configuration parameters define the method used by the tokenization engine, most notably the character set and size limits used by the format-preserving function of SST. Next, the tokenization engine uses data elements within the mapping table combined with the segmentation secret to generate tokens. The mapping table is pseudo-randomly generated when the SST instance is initialized, ensuring that every deployment leverages unique data for token generation. This mapping table is approximately 240KB in size and is used to computationally map data sets to generated token values, thereby eliminating the need to maintain large, traditional databases. Finally, the segmentation secret allows clients to create their own tokenization segments (virtual token environments), whereby the same originating data input would produce a different token value. This function can be especially useful for clients who have different business segments where token values need to remain independent.

Foregenix Inc.
Boston, MA 02109

T: +1 877 418 4774
info@foregenix.com
www.foregenix.com

Secure Stateless Tokenization Findings

Following an overview of the SST design, several obvious advantages begin to surface. Because the mapping table is static, there are no performance issues as the volume of tokens increase. The mapping table remains fixed regardless of the number of tokens that might be generated by the system.

This design also enables virtually endless scalability because multiple instances of the SST solution can be deployed across geographically diverse regions without the need to replicate data beyond the initial setup of the configuration parameters and mapping table.

Foregenix's performance tests for generating varying types of tokens using sample data sets (payment card data, U.S. Social Security numbers, name and address information, and healthcare records) revealed microsecond response times for both token generation and data reconstruction (Illustration #4).

Sensitive Data Type	Sensitive Data	Desensitized/Tokenized Data
Credit Card number	1111-2222-3333-4444	1111-22**87-9581**-4444
U.S. Social Security number	999-88-7654	**740-36**-7654
Address	1234 Maple Street	**7321 Uqhap Fbzira**
Phone number	415-555-1234	**819-913-0471**

Illustration #4

The SST solution simplifies the complexity of back-office platforms, and CyberRes Voltage provides a suite of source code examples that demonstrate the integration of the tokenization engine into many different platform environments including Java, Microsoft .Net, and the C programming language.

Security and Compliance Implications

Now that we have described the overall process for how Voltage SST generates tokens, we will dive into a bit more detail regarding the security and compliance of the SST solution.

As described above, SST uses a process known as reversible, format-preserving, table-based tokenization. This means that the process used to create the token maintains a predefined character set (format-preserving) for the token value, and it can be reversed to reconstruct the original sensitive data.

However, unlike traditional encryption that uses a key for encryption and decryption routines, Voltage SST uses the pseudo-randomly generated mapping table in addition to the segmentation secret to generate tokens and to reconstruct the original sensitive data. This is a topic where many people, especially security consultants, begin to confuse the compliance implications of reversible table-based tokens versus encrypted data. However, in terms of PCI DSS, for example, as well as many other compliance standards, the distinction between a reversible table-based token and traditional data encryption is academic and largely irrelevant in the context of data reconstruction/decryption isolation. A clarifying example: in either case, an end-user or merchant has no means of reconstructing the original

Foregenix Inc.
Boston, MA 02109

T: +1 877 418 4774
info@foregenix.com
www.foregenix.com

sensitive data from the token provided by the tokenization service provider (TSP). The merchant is isolated both from the TSP tokenization platform and from all sensitive materials used during the data reconstruction process. Also, the chosen NIST-standard algorithms mean it is computationally infeasible to compromise the original sensitive information from the token value outside of the Voltage SST environment. The Payment Card Industry (PCI) Security Standards Council (SSC) defines computationally infeasible as "*the principle that the best-known cryptanalytic attack cannot succeed within a practical length of time (e.g., decades), because it requires excessive computational resources [*that either do not exist or cannot be constructed*]. The recovery of the original PAN should be computationally infeasible knowing only the token, a number of tokens, or a number of PAN/token pairs.*"

Tokenization Product Security Guidelines

(https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf)

PAN Protection Requirements FAQ 1117

(https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/Are-truncated-Primary-Account-Numbers-PAN-required-to-be-protected-in-accordance-with-PCI-DSS)

Using Voltage SST helps organizations remove sensitive data from their environments while maintaining existing business systems and processes. The removal of sensitive data from the environment not only reduces security risks, but also supports reduced compliance requirements for system platforms that only use SST tokens.

HIPAA § 164.310(d)(1) Device and Media Controls
Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

HIPAA § 164.312(a)(1) Access Control
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

HIPAA § 164.312(c)(1) Integrity
Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

PCI DSS v4.0
Requirement 3.5.1 PAN is rendered unreadable anywhere it is stored
Requirement 4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks

One of the inherent protections of format-preserving tokenization, as shown in illustration #4, is simply that sensitive data is not easily compromised given that all attempts to reconstruct the data from the token result in data

Foregenix Inc.
Boston, MA 02109

T: +1 877 418 4774
info@foregenix.com
www.foregenix.com

sets with the appearance of the original sensitive data. It would be difficult for an attacker to know when the sensitive data had been successfully reconstructed.

Key Voltage Secure Stateless Tokenization 3.0 features include:

- reversible, table-based tokenization
- architected based on industry standards from PCI, NIST, and ANSI
- enterprise-grade performance, security, and scalability

Conclusion

The value of substituting tokens, such as casino chips, for valuable assets has been proven many times across a wide array of environments. Today, the use of tokens as a replacement for sensitive data continues to show the value in protecting valuable data assets.

Following a detailed analysis of the CyberRes Voltage SST solution, Foregenix determined that SST 3.0 maintains the highest levels of security through the use of strong, standards-based, reversible table-based tokenization.

By eliminating the database used in traditional tokenization solutions, the CyberRes Voltage SST solution provides enterprise-level performance, security, and scalability that cannot be matched by legacy platforms.

About CyberRes

CyberRes is a Micro Focus line of business. CyberRes brings the expertise of one of the world's largest security portfolios to help customers navigate the changing threat landscape by building both cyber and business resiliency within their teams and organizations. CyberRes helps enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility. CyberRes Voltage privacy-enabling technologies discover, analyze, and protect sensitive data, and continuously monitor and manage the data life cycle. Manage data minimization, protection, deletion, and other disposition with Voltage. Pseudonymize or anonymize personal data for usability with persistent protection in cloud data analytics, workload migration, third-party data sharing, and more.

Micro Focus is one of the world's largest enterprise software providers. Micro Focus generates $3.0 billion in annual revenue and serves over 40,000 customers worldwide, including 98 Fortune 100 companies. Micro Focus delivers mission-critical technology and supporting services that help thousands of customers worldwide manage core IT elements of their business so they can run and transform—at the same time.

Foregenix Inc.
Boston, MA 02109

T: +1 877 418 4774
info@foregenix.com
www.foregenix.com

About Foregenix

Foregenix is a global leader in Digital Forensics, Incident Response, compliance services, and cybersecurity. With our mix of technology and experience, we protect our clients' data, reputation, and consequently their brands against threat actors around the globe. Foregenix offers a broad portfolio of essential cybersecurity services, ranging from penetration testing, digital forensics, as well as providing guidance and assessment services against other PCI standards such as DSS, SSF, P2PE, CPSA, and others. Foregenix delivers more PCI P2PE assessments than any other QSAC in the world.

About the Author

Bryan Bell is a Principal Consultant for Foregenix. Bryan brings more than 30 years' experience in information security and technology, cryptography, network and systems design, and application development to the cybersecurity industry. Bryan's career opportunities have allowed him to work with and learn from some of the premier thought leaders in the industry. He is considered one of the foremost experts in cryptography and key management. Bryan also serves as a member of the PCI SSC Encryption Task Force.

CISSP, HCISPP, CFCP, CSSLP

PCI QSA (DSS, P2PE, PA-P2PE, SSA, SSLCA, TSP, 3DS, QPA)

ISO 27001 Lead Auditor + ISO 27001 Lead Implementer