Voltage security

DATA SHEET
Voltage SecureData Enterprise

# End-to-end Data Protection for the Way Your Business Works

A DATA-CENTRIC APPROACH TO ENCRYPTION, TOKENIZATION, DATA MASKING AND KEY MANAGEMENT

## The Current Climate in Data Security

With ever-increasing competitive and cost pressures, enterprises are driving toward greater use of cloud services and Big Data analytics to extract more value from corporate and customer information. At the same time, concerns for effective data security and compliance with privacy regulations can often cause delays in adoption of these valuable technologies. With data in constant motion and with rising threats to sensitive data from both inside and outside the business, companies need to be able to protect data end-to-end, from the moment of capture across the information lifecycle including testing and production. What's more, the costs of passing audit and maintaining compliance are becoming more unpredictable – especially in an environment of increasing regulations, outsourcing and cloud computing. There is a strong desire to reduce audit scope wherever possible to contain cost.

Voltage SecureData Enterprise provides a comprehensive approach to enterprise data protection. It is the only comprehensive data protection platform that secures data as it is captured, processed, and stored across a variety of devices, operating systems, databases, and applications used by enterprises, merchants, and service providers. Voltage SecureData Enterprise includes market-leading Voltage Format-Preserving Encryption (FPE), Voltage Secure Stateless Tokenization (SST) technology, Stateless Key Management, and data masking to address the entire lifecycle of sensitive data as it moves through the enterprise and beyond. It also extends data protection beyond organizational borders, enabling protection of data shared with partners, suppliers, and outsourcers.

## Highlights

- **Reduce audit scope, costs, system impact and resources.** Eliminate sensitive data from production and test systems and enable end-to-end data protection in 60 days or less. Satisfies compliance requirements for privacy regulations.
- **Avoid brand-damaging, costly breaches.** Move beyond compliance to easily weave data protection across mainframe, open systems, devices and platforms.

## A Unique Approach to End-to-end Encryption

Voltage SecureData Enterprise brings a unique, proven data-centric approach to protection – where the access policy travels with the data itself – by permitting data encryption and tokenization without changes to data format or integrity, and eliminating the cost and complexity of issuing and managing certificates and symmetric keys. As a result, companies like RLI and Heartland Payment Systems have achieved end-to-end data protection across mainframes and open systems in both production and test/development systems, in 60 days or less.

## Immediate Integration of Data Security

Voltage SecureData Enterprise can immediately integrate with virtually any application, ranging from decades-old custom applications to the latest enterprise programs. SDKs/APIs and command line tools enable encryption and tokenization to occur natively on the widest variety of platforms, including Linux, mainframe and mid-range. APIs enable broad integration into portfolios including ETL, cloud, SEIM/SIM, databases and applications, and Big Data with native on-node cluster-wide data-masking, encryption and decryption.

Voltage SecureData Enterprise protects information in compliance with PCI DSS, HIPAA, GLBA, state and national privacy regulations, allowing organizations to quickly pass audit and additionally implement full end-to-end data protection to reduce risk impact of data breaches – all without the IT organization having to completely redefine the entire infrastructure and IT processes or policies. On average, Voltage SecureData Enterprise requires less than 0.1 full-time employee (FTE) per data center for ongoing management.

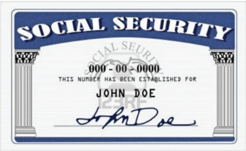
# The Voltage Security Approach—How We Do It

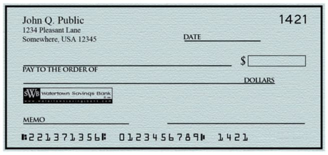
## Voltage Format-Preserving Encryption: Encryption and Masking

Traditional encryption approaches have enormous impact on data structures, schemas and applications. Voltage SecureData Format-Preserving Encryption (FPE), a mode of the industry-proven Advanced Encryption Standard (AES), overcomes this challenge by encrypting data while preserving its original format and without sacrificing encryption strength. Structured data, such as Social Security, Tax ID, credit card, account, date of birth or salary fields, can be encrypted in place.

Traditional encryption methods significantly alter the original format of data. For example, a 16-digit credit card number encrypted with AES produces a long alphanumeric string. As a result, database schema changes are required to facilitate the original format. Because Voltage SecureData FPE maintains the format of the data being encrypted, no database schema changes and minimal application changes are required – in many cases only the trusted applications that need to see the clear data need a single line of code. Tools for bulk encryption facilitate rapid de-identification of large amounts of sensitive data in files and databases. Whole systems can be rapidly protected in just days at a significantly reduced cost.

> *"We needed fast deployment in an environment that is reluctant to change, but we were able to move through very quickly. We were able to get PCI compliant, which is a very big win for us, and improve our security and the additional controls around the data as it's being moved, and we have very few support calls."*
>
> *- Tim Masey*
> *Director of Enterprise Information Security, AAA - The Auto Club Group*





| | Credit Card<br>0012 3456 7890 0000 | Tax ID<br>000-00-0000 | Bank Account<br>800N2982K-22 |
|---|---|---|---|
| FPE | 2724 9283 2943 2838 | 982-28-7723 | 709G9242H-35 |
| AES | 8juYE62W%UWjaks&<br>dDFeruga2345^WFL | lja&2924kUEF65%Qa<br>rotugDF2390^32KNq | Hiu97NMko2^Ku}o{3<br>5RJ434DQNmnSDre |

Voltage SecureData FPE also integrates access policy information in the ciphertext, providing true data-centric protection where the data policy travels with the data itself. Voltage SecureData FPE de-identifies production data and creates structurally valid test data so developers or users can perform QA or conduct data analysis – all without exposing sensitive data.

## Identity-Based Encryption: Simplified Public Key Encryption

Voltage Identity-Based Encryption (IBE) enables unstructured data such as files and bulk data to be secured on-the-fly for any system, recipient or group in an ad hoc manner without the traditional problem of having to issue and manage encryption keys for every endpoint.

When combined with FPE, IBE provides end-to-end protection in a distributed environment to allow encryption of data at the point of capture – for example, a Point-of-Sale (POS) device, where offline data protection or one-way data protection is required, from the POS to the back end – without complex and costly processes, such as key injection, to manage symmetric keys.

## Stateless Key Management: Transparent, Dynamic, Role-based

Key management has been the industry's biggest operational headache when managing encryption, and the operational barrier that has made the large-scale deployment of encryption impractical. Most data encryption products require significant administrative overhead and add significantly to IT management costs – by including the need for a key database to store a copy of every key ever issued, and having to make changes according to how that database behaves.

Voltage Stateless Key Management securely and mathematically derives any key, as required by an application, once that application and its users have been properly authenticated and authorized against a centrally managed policy. Voltage Stateless Key Management reduces IT costs and eases the IT administrative burden by:

- Eliminating the need for a key database, as well as the corresponding hardware, software and IT processes required to protect the database continuously or the need to replicate or back-up keys from site to site.
- Easily recovering archived data because keys can always be recovered.
- Automating supervisory or legal e-discovery requirements through simple application APIs, both native and via web services.
- Maximizing the re-use of access policy infrastructure by integrating easily with identity and access management frameworks and dynamically enforcing data-level access to data fields or partial fields, by policy, as roles change.

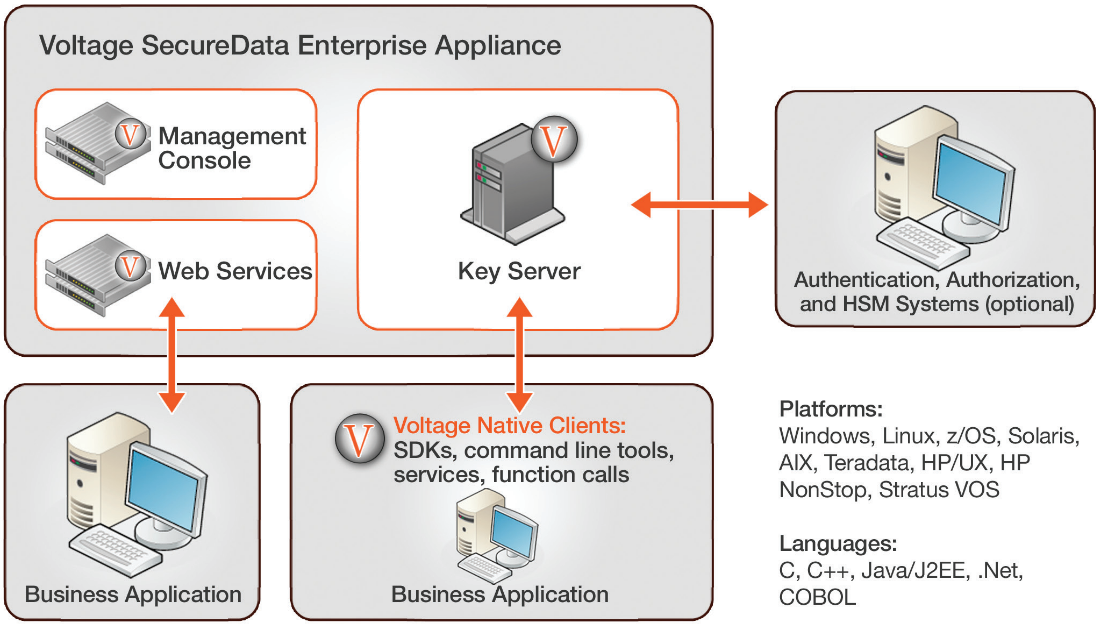
## Voltage Secure Stateless Tokenization (SST) Technology

The Voltage Secure Stateless Tokenization (SST) technology is an advanced, patent pending, data security solution that provides enterprises, merchants and payment processors with a new approach to help assure protection for payment card data. Voltage SST technology is offered as part of the Voltage SecureData Enterprise data security platform that unites market-leading encryption, tokenization, data masking and key management to protect sensitive corporate information in a single comprehensive solution.

Voltage SST technology is "stateless" because it eliminates the token database which is central to other tokenization solutions, and removes the need for storage of cardholder or other sensitive data. Voltage has developed an approach to tokenization that uses a set of static, pre-generated tables containing random numbers created using a FIPS random number generator. These static tables reside on virtual "appliances" – commodity servers – and are used to consistently produce a unique, random token for each clear text Primary Account Number (PAN) input, resulting in a token that has no relationship to the original PAN. No token database is required with SST technology, thus improving the speed, scalability, security and manageability of the tokenization process.

## Voltage SecureData Enterprise Architecture

All Voltage solutions share a common infrastructure, including the same centralized servers and administration tools. This enables Voltage customers to choose an appropriate combination of techniques to address their use cases, across diverse environments, while avoiding the costs and complexities of deploying and managing multiple products.



Voltage SecureData Enterprise Appliance
Management Console
Web Services
Key Server
Authentication, Authorization, and HSM Systems (optional)
Business Application
Voltage Native Clients: SDKs, command line tools, services, function calls
Business Application

**Platforms:**
Windows, Linux, z/OS, Solaris, AIX, Teradata, HP/UX, HP NonStop, Stratus VOS

**Languages:**
C, C++, Java/J2EE, .Net, COBOL

## Voltage SecureData Enterprise includes:

- **Voltage SecureData Management Console:** Enforces data access and key management policies, and eliminates the need to configure each application, because flexible policies are centrally defined and reach all affected applications.
- **Voltage Key Management Server:** Eliminates the requirement to store or manage keys because keys are dynamically derived; seamlessly integrates with existing Identity Management and Authorization Systems and permits FIPS 140-2 Hardware Key Management through Hardware Security Modules.
- **Voltage SecureData Web Services Server:** Centralized web services encryption and tokenization option for Service Oriented Architecture environments, enterprise applications and middleware.
- **Voltage SecureData Simple API:** Maximizes efficiency on a broad range of application servers through native encryption on HP/UX, HP NonStop, Solaris, Linux, AIX, Windows, CentOS, Teradata, and a variety of POS devices.
- **Voltage SecureData z/Protect:** Maximizes CPU performance on mainframe systems through native z/OS support for encryption and tokenization.
- **Voltage SecureData z/FPE:** Mainframe data processing tool to fast track integration into complex record management systems such as VSAM, QSAM, DB2 and custom formats. De-identify sensitive data for production as well as test use.
- **Voltage SecureData Command Line:** Scriptable tool to easily integrate bulk encryption and tokenization into existing batch operations. Performs operations on files and databases.

> “*Voltage SecureData Enterprise tokenization appears to be every bit as effective as conventional tokenization solutions. Moreover, Voltage SecureData would provide higher performance and greater security. Therefore, it is Coalfire’s opinion that Voltage SecureData tokenization solution, when properly implemented, would promote a merchant’s PCI compliance goals and effectively reduce its PCI audit scope.*”
>
> *– PCI DSS Scope Reduction Analysis by Coalfire Systems, Inc.*

### About Voltage Security

Voltage Security®, Inc. is the leading data protection provider, delivering secure, scalable, and proven data-centric encryption and key management solutions, enabling our customers to effectively combat new and emerging security threats. Leveraging breakthrough encryption technologies, our powerful data protection solutions allow any company to seamlessly secure all types of sensitive corporate and customer information, wherever it resides, while efficiently meeting regulatory compliance and privacy requirements.

For more information, please visit **www.voltage.com**.