Data Sheet: Voltage SecureData

Voltage SecureData includes:

Voltage SecureData Management Console:
Enforces data access and key management policies and eliminates need to configure each application because flexible policies are centrally defined and reach all affected applications.

Voltage Key Management Server:
Eliminates need 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, which eliminates need to implement monolithic cryptographic libraries and permits centralized encryption and tokenization services to 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.

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.

Voltage SecureData Command Line:
Scriptable tool for bulk encryption to easily integrate encryption into existing operations.

End-to-End Data Protection For the Way Your Business Works
A Unique Data-Centric Approach to Encryption, Tokenization, Data Masking and Key Management.

The Current Climate in Data Security
While complying with privacy regulations might meet immediate audit goals, many companies are finding that compliance mandates are a rear-guard effort that provides no more protection than patches to a leaky boat. 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 from the moment of capture across the information life-cycle. Online data (consisting of various types of servers and applications) is the most frequently compromised asset, accounting for nearly all (99.9 percent) of the 285 million records breached in the last year.

What’s more, the costs of passing audit and maintaining compliance are becoming even 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. Additionally, past attempts to protect data end-to-end have required significant changes to systems – at great cost to the organization. The prevalence of legacy systems that host vast amounts of private information spanning decades only complicates matters.

A Unique Approach to End-to-End Encryption
Voltage SecureData is an end-to-end data protection framework that delivers rich encryption, tokenization, data masking and key management services – without the cost and complexity of traditional solutions. Voltage SecureData 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 mainframe, open systems, and application servers through native encryption and tokenization option for Service Oriented Architecture environments, which eliminates need to implement monolithic cryptographic libraries and permits centralized encryption and tokenization services to enterprise applications and middleware.

Data Sheet: Voltage SecureData™

© 2009 Voltage Security, Inc. All rights reserved. Voltage Security is a registered trademark of Voltage Security, Inc. Voltage SecureData is a trademark of Voltage Security, Inc. Other names and brands may be claimed as the property of others.

About Voltage Security
Voltage Security®, Inc., is the world leader in providing data-centric encryption and key management solutions for combating new and emerging security threats. Voltage customers represent a wide variety of industries including payments, financial, insurance, medical, e-commerce. Offerings include Voltage SecureFile™, Voltage SecureData™, Voltage SecureData Payments™, Voltage SecureData Web™, Voltage SecureFile™ and Voltage Cloud Services™. The company has been issued several patents based upon breakthrough research in mathematics and cryptographic systems. To learn more about Voltage customers please visit voltage.com/customers.
Voltage SecureData protects information in compliance with PCI DSS, HIPAA, GLBA, state or national privacy regulations to quickly pass audit and additionally implements full end-to-end data protection to prevent data breaches — all without the IT organization having to completely redefine the entire infrastructure and IT processes or policies. On average, Voltage SecureData requires less than 0.1 FTE per data center for ongoing management.

**The Voltage Security Approach - How We Do It**

**Format Preserving Encryption™** : Encryption and Masking

Traditional encryption approaches create enormous system-level 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, data of birth or salary fields, is encrypted in place.

Past encryption methods significantly alter the original format of data, producing a different output. 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 1-2 lines of code. Whole systems can be rapidly protected in just days at a significantly reduced cost.

Voltage SecureData FPE also encrypts data with the access policy information — true data-centric protection where the data policy travels with the data itself — and supports regular AES, 3DES, RSA, SHA-1 and traditional cryptographic functions for backwards compatibility. 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. Ad-hoc secure end-to-end communications networks can be established instantly: seamless secure collaboration from the enterprise to, say, ten thousand brokers is possible without disrupting or slowing down existing business interactions while remaining privacy regulation compliant.

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 at a Point of Sale (POS) device where offline data protection or one way data protection from POS to the back end is desired — without complex and costly processes to manage symmetric keys such as key injection.

Voltage Identity-Based Encryption obviates the need for certificates, or identity is used as a public key as a means to replace the need for certificates, all made possible by remarkable algorithms of recent invention.

- **George Peabody, Mercator Group**

**Role-Based Stateless Key Management: Transparent, Dynamic,لو.role-based**

Key Management has been the industry’s biggest operational headache when managing encryption: 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 the 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:

- Easily recovering long-since archived data because keys can always be recovered.
- Automating supervisory or legal e-discovery requirements through simple application APIs, both native and as 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.

**Tokenization: Format-Preserving Tokens**

Voltage SecureData takes a similar approach to tokenization by eliminating the need for expensive heavy lifting to support a range of tokenization services such as single field tokenization and de-tokenization, bulk tokenization and de-tokenization, and the validation and issuance of tokens. Like traditional tokenization solutions, Voltage SecureData connects to any database for secure token storage, recovery and lookup. Unlike these solutions, however, Voltage SecureData leverages its own database independent FIPS certified encryption and stateless Key Management eliminating the need to store and manage keys, and providing full automatic key rollover. Voltage SecureData Format Preserving Tokens inherit the rich APIs and authentication and authorization framework from the Voltage SecureData platform.

**“Configuring a new application or set of applications for encryption simply takes moderate configuration and we’re up in running in a matter of weeks. We had not established a standard (for encryption), and now we have one with Voltage.”**

- **Dallas Pettingill, Assistant Vice-President of IT Governance, RLJ Financial Group**
Voltage SecureData protects information in compliance with PCI DSS, HIPAA, GLBA, state or national privacy regulations to quickly pass audit and additionally implements full end-to-end data protection to prevent data breaches — all without the IT organization having to completely redefine the entire infrastructure and IT processes or policies. On average, Voltage SecureData requires less than 0.1 FTE per data center for ongoing management.

The Voltage Security Approach - How We Do It

**Format Preserving Encryption™** : Encryption and Masking

Traditional encryption approaches create enormous system-level 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, data of birth or salary fields, is encrypted in place.

Past encryption methods significantly alter the original format of data, producing a different output. 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 1-2 lines of code. Whole systems can be rapidly protected in just a significantly reduced cost.

Voltage SecureData FPE also encrypts data with the access policy information — true data-centric protection where the data policy travels with the data itself — and supports regular AES, 3DES, RSA, SHA-1 and traditional cryptographic functions for backwards compatibility. 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. Ad-hoc secure end-to-end communications networks can be established instantly: seamless secure collaboration from the enterprise to, say, ten thousand brokers is possible without disrupting or slowing down existing business interactions while remaining privacy regulation compliant.

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 at a Point of Sale (POS) device where offline data protection or one way data protection from POS to the back end is desired — without complex and costly processes to manage symmetric keys such as key injection.

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

Key Management has been the industry’s biggest operational headache when managing encryption: 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 the 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 long-since archived data because keys can always be recovered.

- Automating supervisory or legal e-discovery requirements through simple application APIs, both native and as 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.

**Tokenization: Format-Preserving Tokens**

Voltage SecureData takes a similar approach to tokenization by eliminating the need for extensive heavy lifting to support a range of tokenization services such as single field tokenization and de-tokenization, bulk tokenization and de-tokenization, and the validation and issuance of tokens. Like traditional tokenization solutions, Voltage SecureData connects to any database for secure token storage, recovery and lookup. Unlike these solutions, however, Voltage SecureData leverages its own database independent FIPS certified encryption and stateless Key Management eliminating the need to store and manage keys, and providing full automatic key rollover. Voltage SecureData Format Preserving Tokens inherit the rich APIs and authentication and authorization framework from the Voltage SecureData platform.
Voltage SecureData includes:

Voltage SecureData Management Console:
Enforces data access and key management policies and eliminates need to configure each application because flexible policies are centrally defined and reach all affected applications.

Voltage Key Management Server:
Eliminates need 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, which eliminates need to implement monolithic cryptographic libraries and permits centralized encryption and tokenization services to 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.

Voltage SecureData z/FPE:
Mainframe data processing tool to fast track integration into complex record management systems such as VSAM, QSAM, DB11 and custom formats.

Voltage SecureData Command Line:
Scriptable tool for bulk encryption to easily integrate encryption into existing operations.

The Current Climate in Data Security
While complying with privacy regulations might meet immediate audit goals, many companies are finding that compliance mandates are a rear-guard effort that provides no more protection than patches to a leaky boat. 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 from the moment of capture across the information life-cycle. Online data (consisting of various types of servers and applications) is the most frequently compromised asset, accounting for nearly all (99.9 percent) of the 285 million records breached in the last year.

What’s more, the costs of passing audit and maintaining compliance are becoming even 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. Additionally, past attempts to protect data end-to-end have required significant changes to systems – at great cost to the organization. The prevalence of legacy systems that host vast amounts of private information spanning decades only complicates matters.

A Unique Approach to End-to-End Encryption
Voltage SecureData is an end-to-end data protection framework that delivers rich encryption, tokenization, data masking and key management services – without the cost and complexity of traditional solutions. Voltage SecureData 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 mainframe, open systems and devices in 60 days or less.

data protection across mainframe, open systems, devices and platforms

About Voltage Security
Voltage Security®, Inc., is the world leader in providing data-centric encryption and key management solutions for combating new and emerging security threats. Voltage customers represent a wide variety of industries including payments, financial, insurance, medical, e-commerce. Offerings include Voltage SecureMail®, Voltage SecureData™, Voltage SecureData Payments™, Voltage SecureData Web™, Voltage SecureFile™ and Voltage Cloud Services™. The company has been issued several patents based upon breakthrough research in mathematics and cryptographic systems. To learn more about Voltage customers please visit voltage.com/customers.

Secure Content Technologies
Tel: +1.513.779.1165
kgreer@securecontenttechnologies.com
www.securecontenttechnologies.com