Hewlett Packard Enterprise

Data Sheet

HPE SecureData Enterprise

End-to-end Data-centric Security for the Way Your Business Works

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.

The Current Climate in Data Security

With ever-increasing competitive and cost pressures, enterprises are driving toward greater use of low-cost cloud services such as Azure and AWS, Hadoop and Big Data analytics to extract more value from corporate and customer information. At the same time, concerns for effective enterprise data security and compliance with privacy regulations can often cause delays in adoption of these valuable technologies.

HPE 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, mission-critical systems, and applications used by enterprises, merchants, and service providers. HPE SecureData Enterprise includes market-leading HPE Format-Preserving Encryption (FPE), HPE Secure Stateless Tokenization (SST) technology, HPE 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. HPE SecureData Enterprise solves the issue of advanced threats attacking data as it is stored, processed and moved across different systems end-to-end, without the need to expose live data in the gaps between or across systems.

A Unique Approach to End-to-end Encryption

HPE 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, leading companies in financial services, insurance, retail, health care, transportation, telecom and other industries 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

HPE SecureData Enterprise can immediately integrate with virtually any application, ranging from decades-old custom applications to the latest enterprise programs. Powerful, centrally managed, policy-controlled APIs and command line tools enable encryption and tokenization to occur on the widest variety of platforms, including Linux, mainframe and mid-range. APIs enable broad integration into portfolios

Industry Standard Format-Preserving Technologies

HPE Format-Preserving Encryption (FPE) is currently being published as a standard by NIST as FFX Mode AES - NIST SP800-38G. The work HPE Security - Data Security is doing with NIST, ANSI, IEEE, IETF, and independent security assessment specialists, stands unique in the market, enabling trust in HPE SecureData data-centric encryption, tokenization, and masking. HPE Security - Data Security engineers and cryptographers have brought remarkable technical breakthroughs to market, complete with published security proofs, cryptanalysis, and academic validation. Standards Bodies where HPE SecureData protection technology breakthroughs are published include:

including ETL, cloud, SEIM/ SIM, databases and applications, network appliances and API brokers such as F5 load balancing, and Hadoop with native on-node cluster-wide data-masking, encryption and decryption.

HPE SecureData Enterprise protects information in compliance with PCI DSS, HIPAA, GLBA, state, national and European data 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, HPE SecureData Enterprise requires less than 0.1 full-time employee (FTE) per data center for ongoing management.

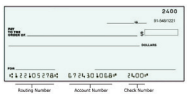
HPE SecureData - Data Security Approach—How We Do It

HPE Format-Preserving Encryption: Encryption and Masking

Traditional encryption approaches have enormous impact on data structures, schemas and applications. HPE 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 HPE 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.

HPE FPE also integrates access policy information in the ciphertext, providing true data-centric protection where the data policy travels with the data itself. HPE 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. The HPE SecureData Enterprise management console enables easy control of policy and provides audit capabilities across the data life cycle--even across thousands of systems protected by HPE SecureData.



122105278 674301068

First Name: Gunther
Last Name: Robertson
DOB: 20-07-1966
SSN: 934-72-2356

FPE AES-FF1 mode	**122105278827572346**	**First Name:** Uywjlqo **Last Name:** Muwruwwbp **SSN:** 298-24-2356 **DOB:** 18-06-1972
Regular AES-CBS mode	8juYE%UkFa2345^WFLE	lja&3k24kQotugDF2390^32 0OWioNu2(*872weW aasIUahjw2%quiFIWUYBw3 Oiuqwriuweuwr%oIU Ow1@

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

HPE 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. HPE 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.

"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

HPE Secure Stateless Tokenization (SST) Technology

The HPE 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. HPE SST technology is offered as part of the HPE 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.

HPE 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. HPE SST 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 HPE SST technology, thus improving the speed, scalability, security and manageability of the tokenization process.

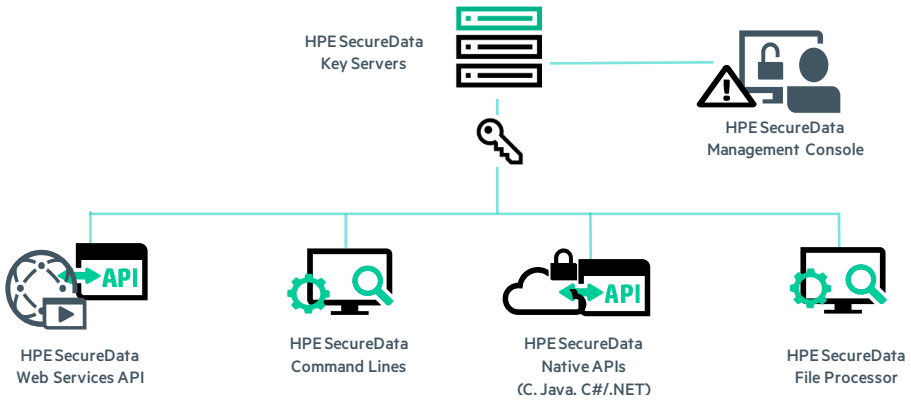
Name	SS#	Credit Card#	Street Address	Customer ID
James Potter	385-12-1199	37123 456789 01001	1279 Farland Avenue	G8199143
Ryan Johnson	857-64-4190	5587 0806 2212 0139	111 Grant Street	S3626248
Carrie Young	761-58-6733	5348 9261 0695 2829	4513 Cambridge Court	B0191348
Brent Warner	604-41-6687	4929 4358 7398 4379	1984 Middleville Road	G8888767
Anna Berman	416-03-4226	4556 2525 1285 1830	2893 Hamilton Drive	S9298273

FPE FPE SST FPE FPE

Name	SS#	Credit Card#	Street Address	Customer ID
Kwfdv Cqvzgk	161-82-1292	37123 786354 51001	2890 Ykzbpoi Clpppn	S7202483
Veks lounrfo	200-79-7127	5587 0856 7634 0139	406 Cmxto Osfalu	B0928254
Pdnme Wntob	095-52-8683	5348 9209 2367 2829	1498 Zejojtbbx pqkag	G8265029
Eskfw Gzhqlv	178-17-8353	4929 4333 0934 4379	8261 Saicbmeayqw Yotv	G3951257
Jsfk Tbluhm	525-25-2125	4556 2545 6223 1830	8412 Wbbhalhs Ueyzg	B662594

HPE SecureData Enterprise Architecture

HPE SecureData solutions share a common infrastructure, including the same centralized servers and administration tools. This enables HPE SecureData 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.



HPE SecureData Enterprise includes:

- **HPE 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. Manages data format policies, business rules enforcement over data access, integration with enterprise authorization and authentication systems and connectivity to enterprise audit and security event monitoring systems. It also manages data security policies such as the choice of HP FPE, file encryption and data masking.

"HPE SecureData Enterprise tokenization appears to be every bit as effective as conventional tokenization solutions. Moreover, HPE SecureData would provide higher performance and greater security. Therefore, it is Coalfire's opinion that HPE 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 System, Inc.

- **HPE Key Management Server:** Eliminates the need for traditional complex storage-based key management and storage because keys are dynamically derived; seamlessly integrates with existing Identity Management and Authorization Systems and Key Management using FIPS 140-2 certified Hardware Security Modules.
- **HPE SecureData Web Services Server:** Centralized web services encryption and tokenization option for Service Oriented Architecture environments, enterprise applications and middleware.
- **HPE SecureData Simple API:** Maximizes efficiency on a broad range of application servers through native encryption on HP/UX, HPE NonStop, Solaris, Stratus OS, Linux (Red Hat, SUSE), AIX, Windows, CentOS, Teradata, and a variety of payment terminal devices.
- **HPE SecureData Command Lines:** Scriptable tools easily integrate bulk encryption, tokenization and file encryption into existing batch operations and applications.
- **HPE SecureData File Processor:** Aggregates support for both tokenization and encryption of sensitive data elements. It provides a unique value to the customer as a single client converging both web services and native API interfaces. The converged clients expand the support for new file types by decoupling input file processing from the underlying encryption and tokenization operations. Delivers high performance data de-identification, with parallel multi-threaded processing of sensitive data elements simultaneously protecting data fields across columns.
- **HPE SecureData Enterprise also supports mainframe, Big Data, and payment security ecosystems:**
  - **HPE SecureData z/Protect:** Maximizes CPU performance on mainframe systems through native z/OS support for encryption and tokenization.
  - **HPE 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.
  - **HPE SecureData for Hadoop Developer Templates:** Provides templates to enable customers to integrate HPE FPE and HPE SST technologies into their Hadoop instances. Templates come ready to use out-of-the-box for Sqoop, MapReduce and Hive, and can be quickly expanded to integrate into other technologies in the Hadoop stack such as Flume.
  - **HPE SecureStorage:** Data-at-rest encryption for Linux with HPE Stateless Key Management.
  - **HPE SecureData Web and Optional Add-ons:** Secures data end-to-end from browser applications and forms to secure back-end applications, extending end-to-end security beyond transport encryption such as SSL and TLS.
  - **HPE SecureData Terminal SDK and Host SDK:** Provide market-leading P2PE payments security.
- **HPE Professional Services:** Available to help clients scope projects, to combat advanced threats, reduce compliance burden and to quickly solve difficult data privacy challenges.

Learn more at:

voltage.com

http://hpe.com/software/datasecurity

Hewlett Packard Enterprise

4AA6-0208ENW, November 2015, Rev. 1