Hewlett Packard Enterprise

Data sheet

HPE SecureData Sandbox

HPE Security–Data Security

Business Benefits

Easily accessed virtual machine

- Deployment and configuration time reduced to a few minutes
- Copy-paste code from tutorial code snippets, sample code, and sample data sets
- Prepackaged Eclipse project that enables local build and remote debugging and execution

Scenario focused tutorials

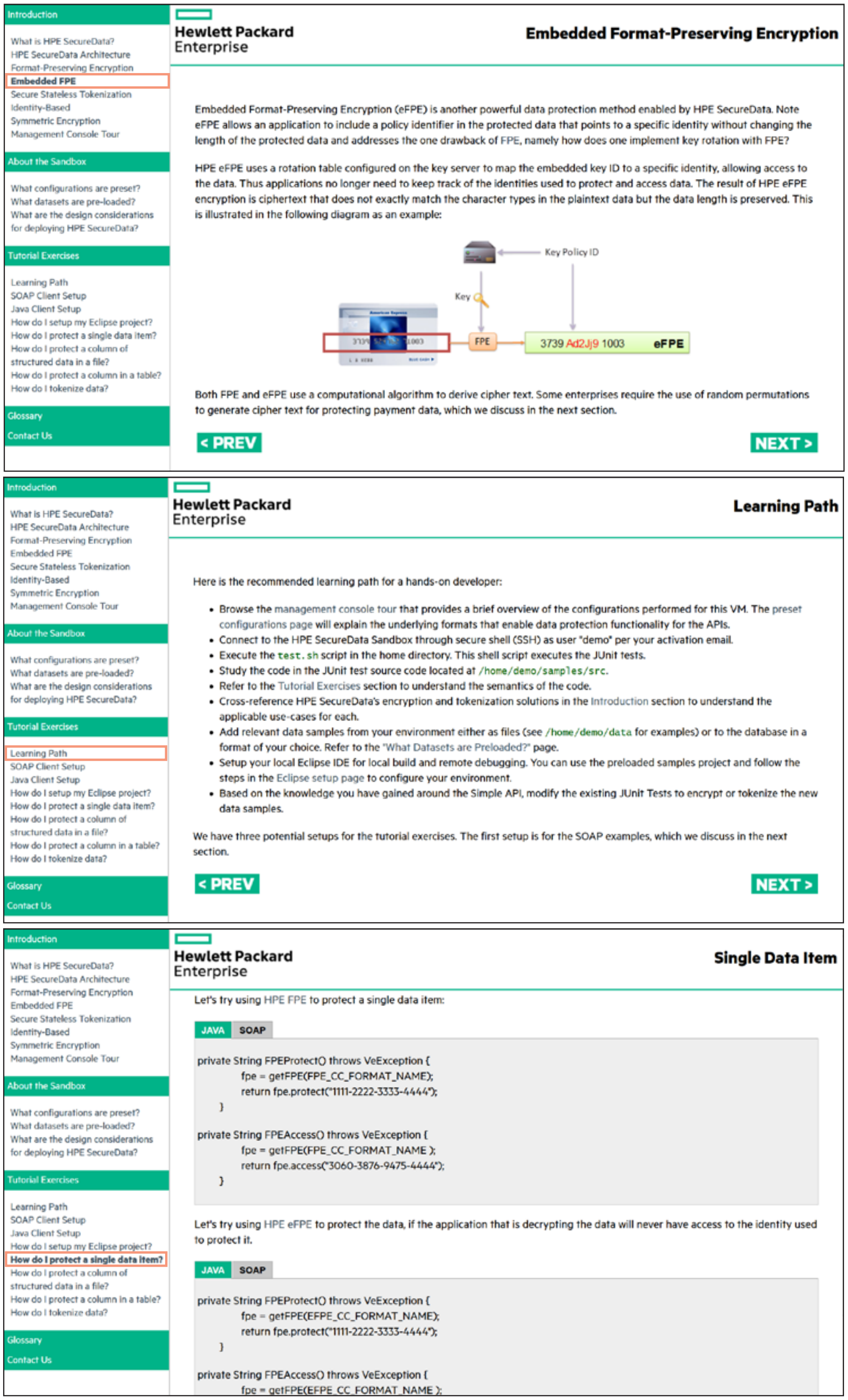
- Show how HPE FPE, HPE eFPE, HPE IBSE and HPE SST work in realistic use-cases
- Column protection in files
- Securing data in database columns
- Data protection and de-identification

Challenge

With the accelerating frequency of data breaches, and the over-arching need to meet compliance regulations, it is imperative for organizations to efficiently evaluate solutions before the internal procurement process. HPE SecureData Sandbox provides an easy, step-by-step way for security architects and developers to "roll up their sleeves" and experience data-centric security. HPE SecureData Sandbox is ideal for organizations looking to gain valued insight into our data-centric solution without disrupting operations or installing new systems or hardware.

The Solution–HPE SecureData Sandbox

The solution includes market-leading HPE Format-Preserving Encryption, HPE Secure Stateless Tokenization, HPE Stateless Key Management, and data masking that secure the entire lifecycle of sensitive data as it moves through the enterprise and beyond. It also extends data protection beyond organizational borders, enabling the protection of data shared with partners, suppliers, and outsourcers.


Introduction
What is HPE SecureData?
HPE SecureData Architecture
Format-Preserving Encryption
Embedded FPE
Secure Stateless Tokenization
Identity-Based
Symmetric Encryption
Management Console Tour
About the Sandbox
What configurations are preset?
What datasets are pre-loaded?
What are the design considerations
for deploying HPE SecureData?
Tutorial Exercises
Learning Path
SOAP Client Setup
Java Client Setup
How do I setup my Eclipse project?
How do I protect a single data item?
How do I protect a column of
structured data in a file?
How do I protect a column in a table?
How do I tokenize data?
Glossary
Contact Us
Hewlett Packard
Enterprise

Embedded Format-Preserving Encryption

Embedded Format-Preserving Encryption (eFPE) is another powerful data protection method enabled by HPE SecureData. Note eFPE allows an application to include a policy identifier in the protected data that points to a specific identity without changing the length of the protected data and addresses the one drawback of FPE, namely how does one implement key rotation with FPE?

HPE eFPE uses a rotation table configured on the key server to map the embedded key ID to a specific identity, allowing access to the data. Thus applications no longer need to keep track of the identities used to protect and access data. The result of HPE eFPE encryption is ciphertext that does not exactly match the character types in the plaintext data but the data length is preserved. This is illustrated in the following diagram as an example:

Both FPE and eFPE use a computational algorithm to derive cipher text. Some enterprises require the use of random permutations to generate cipher text for protecting payment data, which we discuss in the next section.

Learning Path

Here is the recommended learning path for a hands-on developer:

- Browse the management console tour that provides a brief overview of the configurations performed for this VM. The preset configurations page will explain the underlying formats that enable data protection functionality for the APIs.
- Connect to the HPE SecureData Sandbox through secure shell (SSH) as user "demo" per your activation email.
- Execute the `test.sh` script in the home directory. This shell script executes the JUnit tests.
- Study the code in the JUnit test source code located at `/home/demo/samples/src`.
- Refer to the Tutorial Exercises section to understand the semantics of the code.
- Cross-reference HPE SecureData's encryption and tokenization solutions in the Introduction section to understand the applicable use-cases for each.
- Add relevant data samples from your environment either as files (see `/home/demo/data` for examples) or to the database in a format of your choice. Refer to the "What Datasets are Preloaded?" page.
- Setup your local Eclipse IDE for local build and remote debugging. You can use the preloaded samples project and follow the steps in the Eclipse setup page to configure your environment.
- Based on the knowledge you have gained around the Simple API, modify the existing JUnit Tests to encrypt or tokenize the new data samples.

We have three potential setups for the tutorial exercises. The first setup is for the SOAP examples, which we discuss in the next section.

Single Data Item

Let's try using HPE FPE to protect a single data item:

```
private String FPEProtect() throws VeException {
            fpe = getFPE(FPE_CC_FORMAT_NAME);
            return fpe.protect("1111-2222-3333-4444");
      }

private String FPEAccess() throws VeException {
            fpe = getFPE(FPE_CC_FORMAT_NAME );
            return fpe.access("3060-3876-9475-4444");
      }
```

Let's try using HPE eFPE to protect the data, if the application that is decrypting the data will never have access to the identity used to protect it.

```
private String FPEProtect() throws VeException {
            fpe = getFPE(EFPE_CC_FORMAT_NAME);
            return fpe.protect("1111-2222-3333-4444");
      }

private String FPEAccess() throws VeException {
            fpe = getFPE(EFPE_CC_FORMAT_NAME );
```

Figure 1. What's in the HPE SecureData Sandbox?

What is it?

HPE SecureData Sandbox is a self-contained, virtual, portable environment that consists of a full complement of the HPE SecureData appliance and affiliated APIs. The HPE SecureData Sandbox is a complete trial with preconfigured data format types, integrated key management, tutorials, videos, and sample code. You simply register and get started.

About HPE SecureData

HPE SecureData is a complete framework including integrated key management, interfaces to enterprise systems for authentication and authorization, compatibility with event logging and SIEM systems, and a rich set of developer APIs across all leading enterprise application operating systems and development environments.

HPE SecureData provides data protection for structured and unstructured data at the field level through:

- HPE Secure Stateless Tokenization (SST), which protects fields such as credit cards or Social Security numbers using tokenization without the complexity of managing token databases, while reducing PCI DSS scope.
- HPE Format-Preserving Encryption (FPE) based on AES-FF1 mode per NIST draft standard SP800-38G, which protects data fields or sub-fields while preserving format under policy control.
- HPE Embedded Format-Preserving Encryption (eFPE) which protects data fields or sub-fields using FPE with policy information encapsulated in the encrypted data field to enable data to "self describe" its protection policy to applications.
- HPE Identity-Based Symmetric Encryption (IBSE) which protects bulk data using traditional AES in CBC mode per FIPS 197 to secure files or fields with traditional block ciphers.

HPE SecureData Use Cases

- Protection of data in live applications and databases for short time-to-success privacy compliance and data breach risk reduction using encryption and tokenization.
- Protection of data in test and development environments—creating test data sets from live data, which inherits the properties of the live data without exposing it.
- Protecting data in payments transactions for PCI Scope reduction. HPE SecureData can be extended to devices, smartphones, and browser applications with additional add-ons.
- Protecting data in cloud applications, enabling hybrid cloud deployments or all-cloud applications for SaaS, PaaS, and IaaS without increasing risk, data exposure, or introducing data residency risks for data moving to, processed in, or stored inside cloud ecosystems.

How do I access the HPE SecureData Sandbox?

Access is quick and easy. Reach out to your local HPE Security Voltage sales representative, sales engineer, or visit **https://www.voltage.com/products/data-security/hp-securedata-sandbox/**

Sign up for updates

Hewlett Packard
Enterprise

4AA6-0862ENW, February 2017, Rev. 1