Dealing with Risk and Compliance to secure your growth

16th May 2018

John Bycroft, SVP Sales Europe

comforte

Top drivers for Data Security Investment

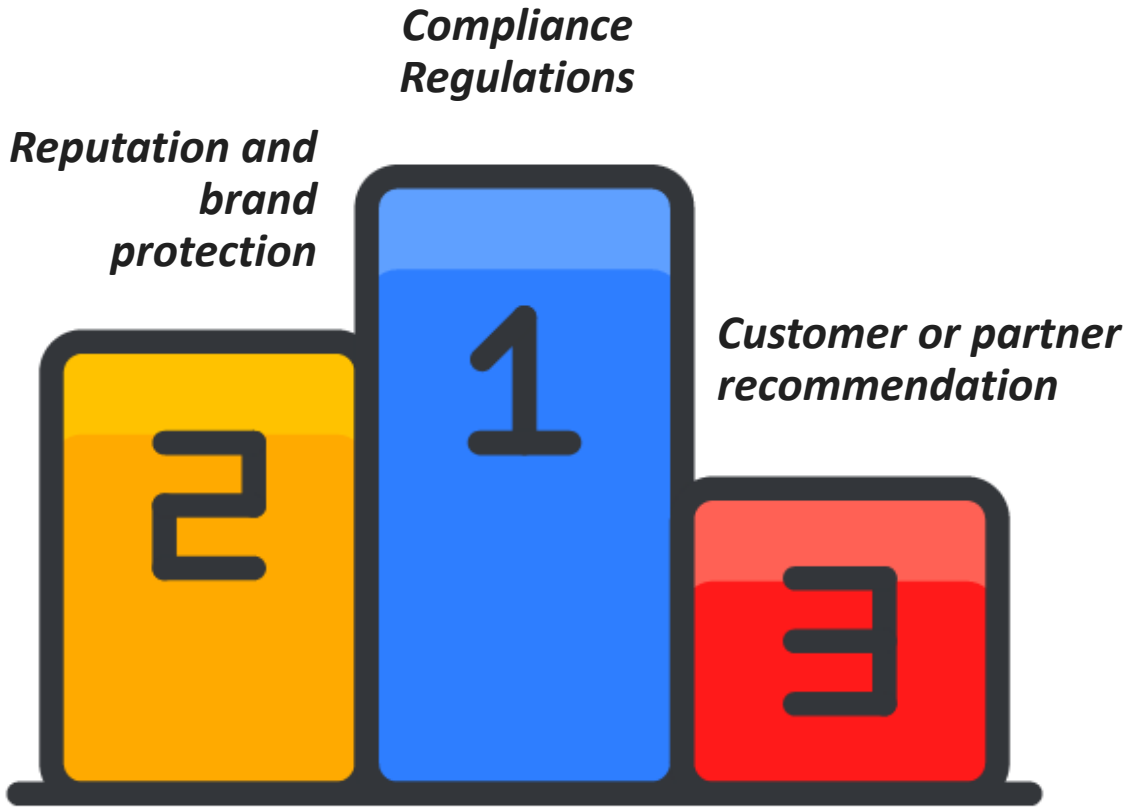
Reputation and brand protection

Compliance Regulations

Customer or partner recommendation

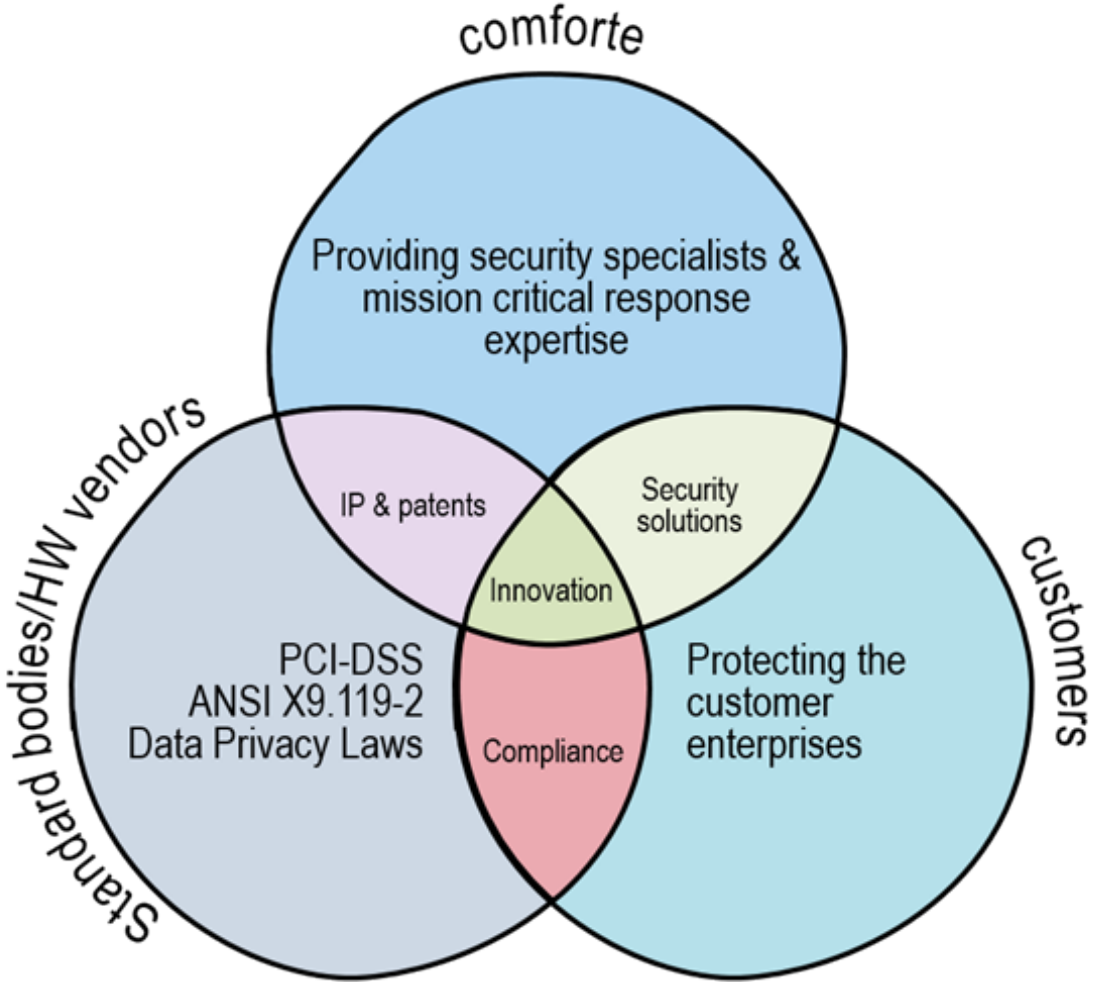
http://www.infosecurity-magazine.com/news/research-data-breaches-up-security/
https://www.bloomberg.com/news/articles/2017-03-02/world-s-biggest-banks-fined-321-billion-since-financial-crisis

Top drivers for Data Security Investment



http://www.infosecurity-magazine.com/news/research-data-breaches-up-security/
https://www.bloomberg.com/news/articles/2017-03-02/world-s-biggest-banks-fined-321-billion-since-financial-crisis

Comforte and Security



So what can you do?

> Ignore the issue or…

> Hope that it does not happen to you

> Do something

PROTECT YOUR DATA WITH TOKENISATION

> “Data protection with tokenisation is proving to be more effective than network perimeter defenses or intrusion detection and is endorsed by the most well-known and respected compliance standards worldwide”

PCI DSS 3.2	ASC X9 Standard 119-2	GDPR
Render Primary Account Number (PAN) unreadable anywhere it is stored (clause 3.4)	Defines the minimum security requirements for implementing tokenisation	Data security measures should allow Pseudonymizing (tokenising or encrypting) of personal data

According to Gartner Research, tokenisation has emerged as a best practice for protecting sensitive fields or columns in databases during the past few years.

Tokenisation (data security)

> Is the process of substituting a sensitive data element (e.g. PAN) with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value.

> The token is a reference (i.e. identifier) that maps back to the sensitive data through a tokenisation system like comForte‘s SecurDPS

tokenisation – the concept

Target format configurable in tokenisation engine.
Important to have a distinguish-method for online migration

Various mechanisms possible to perform actual tokenisation

comForte Tokenisation Engine

> Stateless/Vaultless tokenisation

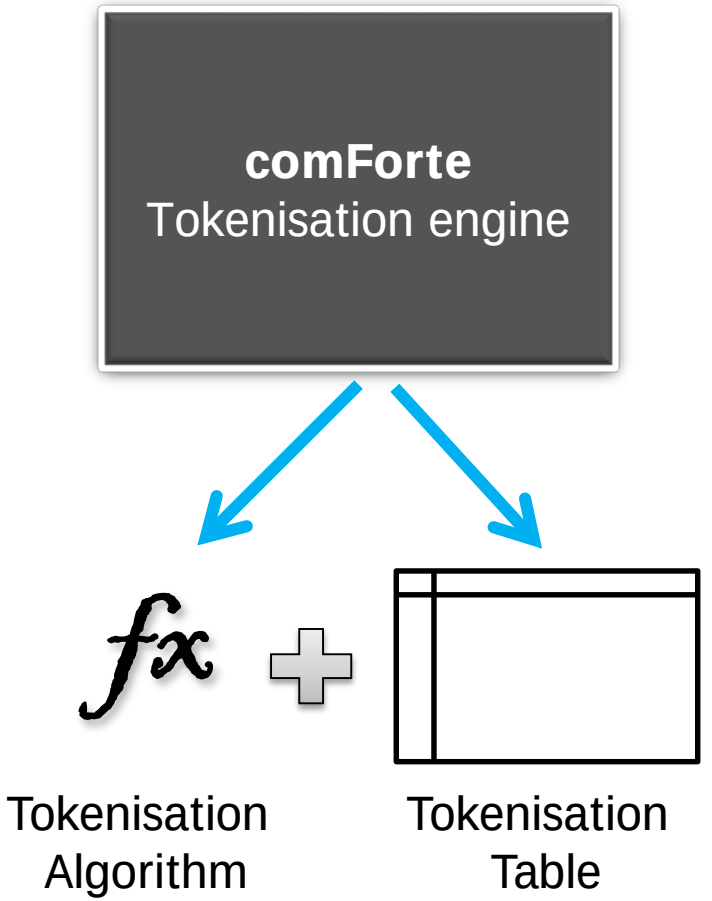
> Security validated by independent cryptologists

> High performance

> Collision-free

> Patented technology based on unbalanced Feistel networks

> Linearly scalable



Enterprise Tokenisation system is mission-critical

Looking for:

> Availability

> Scalability

> Reliability

> Security

> Easy Integration

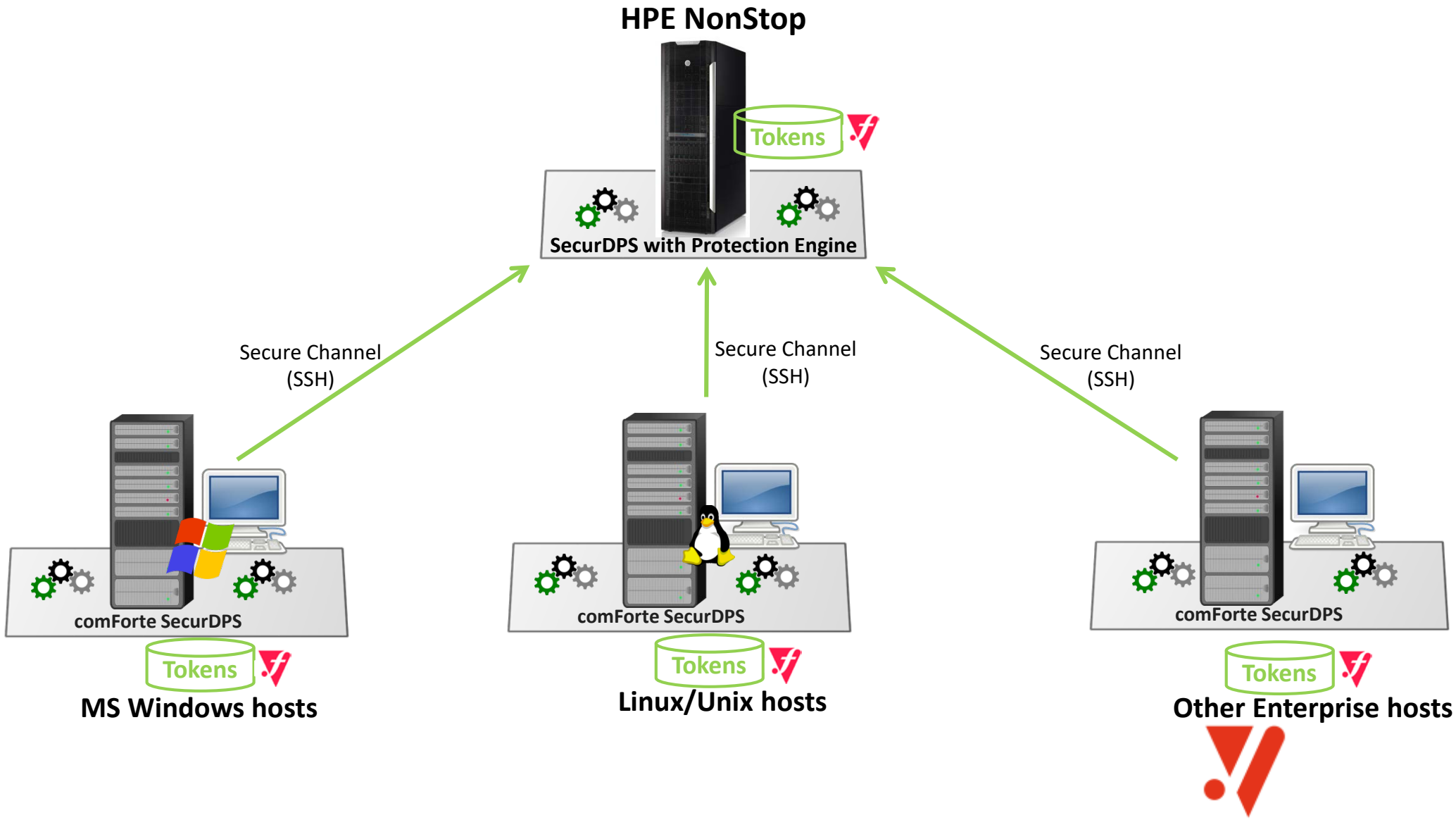
> Fault-Tolerance

> Performance

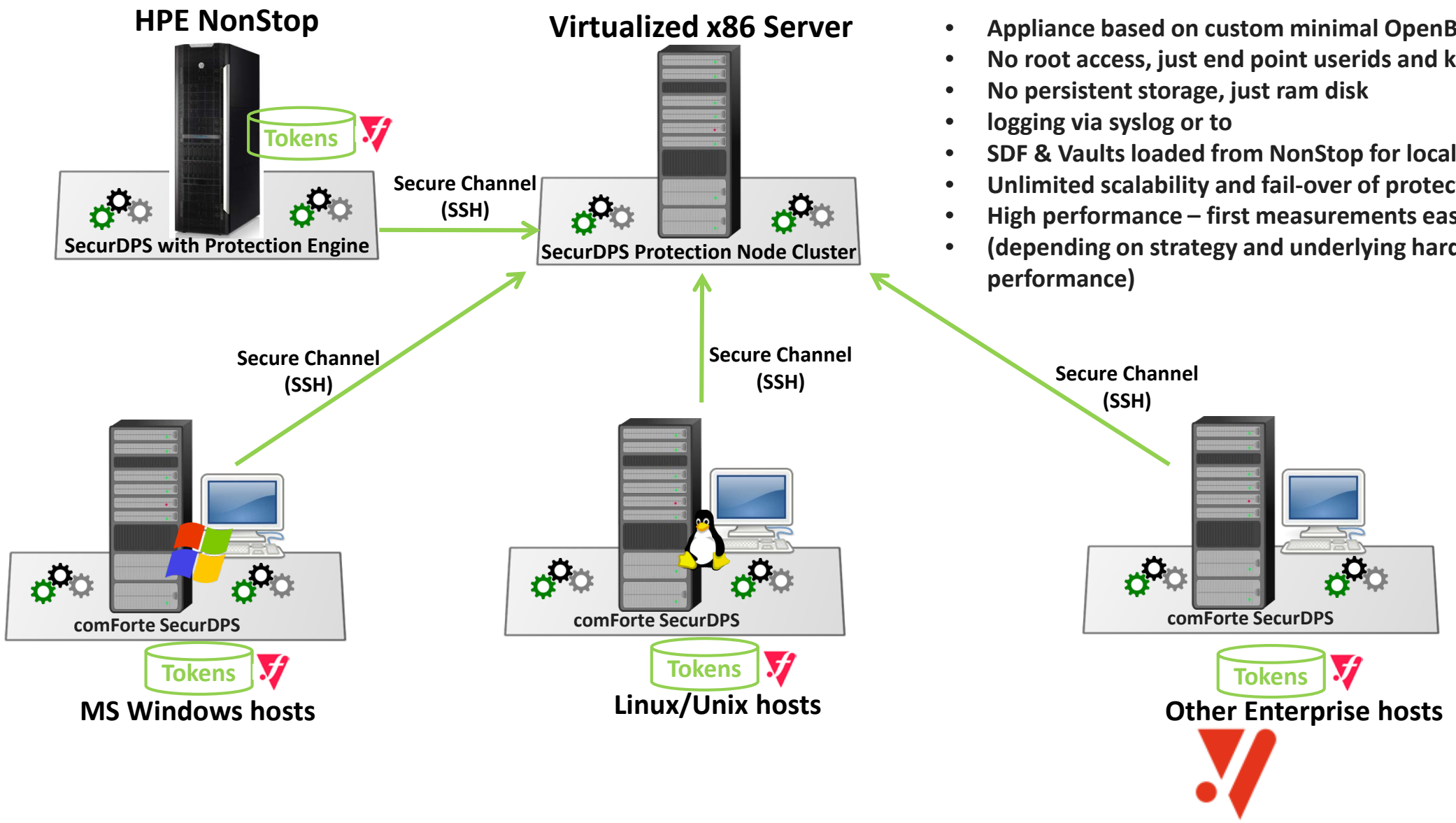
…while keeping effort for tokenisation services management and consumers low

SecurDPS framework

NonStop as the tokenisation server

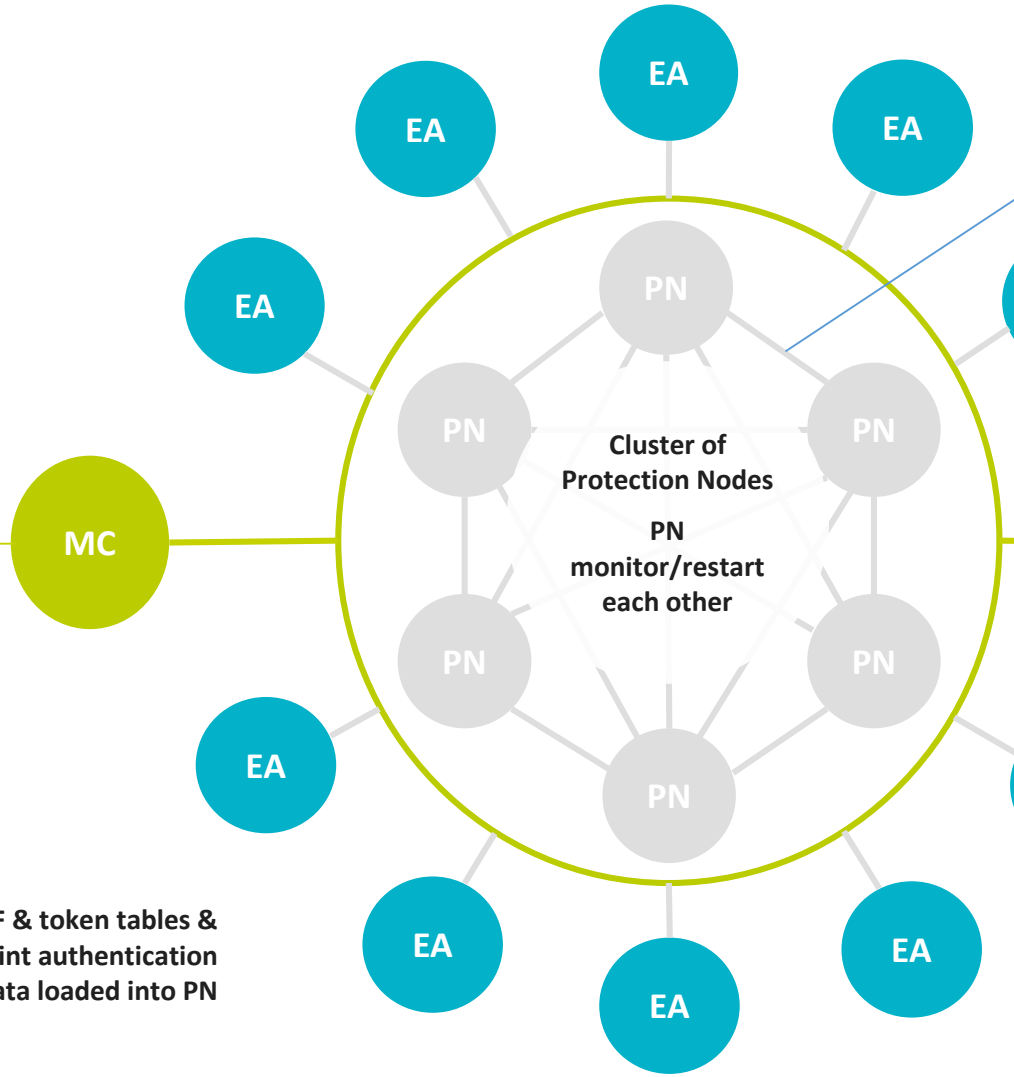


Today - Satellite Protection Node Appliance



- Appliance based on custom minimal OpenBSD
- No root access, just end point userids and keys
- No persistent storage, just ram disk
- logging via syslog or to
- SDF & Vaults loaded from NonStop for local processing
- Unlimited scalability and fail-over of protection nodes
- High performance – first measurements easily 100k TPS
- (depending on strategy and underlying hardware performance)

COMFORTE DATA PROTECTION CLUSTER - ARCHITECTURE YOU CAN RELY ON



Failure of single PN will be transparent for enterprise application (EA) connectors, other PN will take over

Management Console (MC) configures SDF (configuration file) and generates token tables

MC can be stopped after cluster startup!

Audit Console creates a solid audit trail and allows real-time insights into key questions around enterprise data protection

SDF & token tables & endpoint authentication data loaded into PN

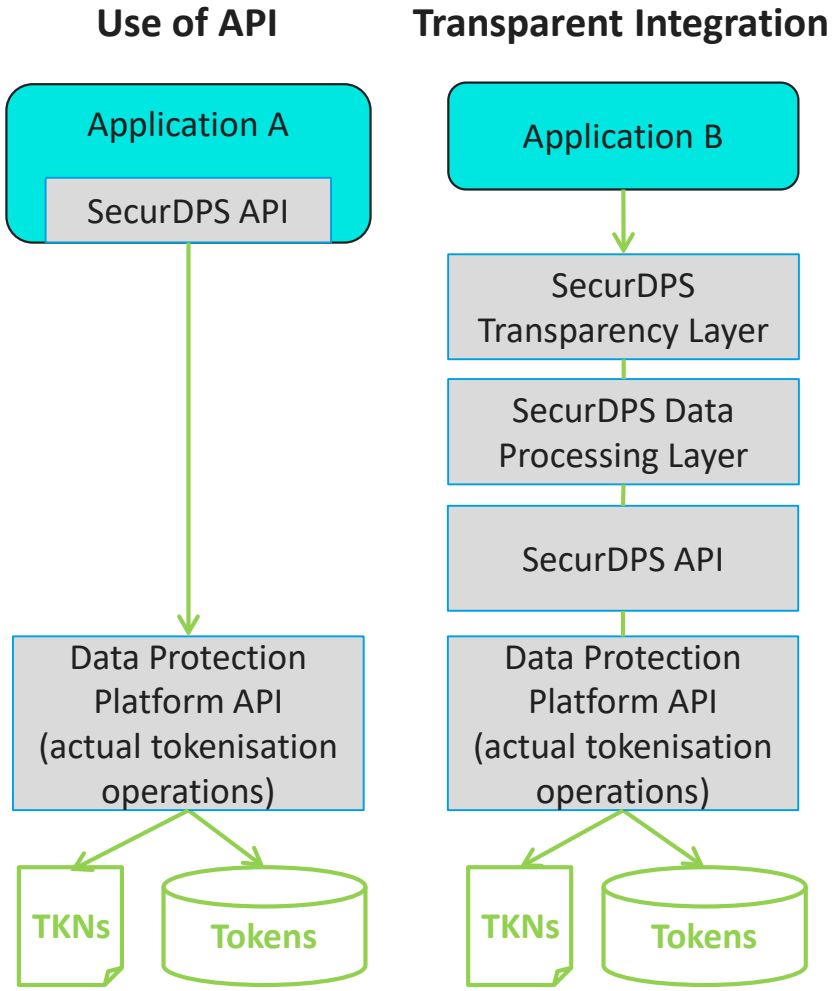
In environments with NonStop (optional), NS can run as MC and/or PN

SecurDPS – Integration Capabilities

SecurDPS integration can be done by:

- Transparent Integration capabilities
  - No code change required
  - Full support of HP NonStop, and can also cover common use cases for Windows and Linux/Unix
  - Allows for protecting files that are accessed by 3rd party applications that cannot be changed, such as file transfers clients, operating systems tools etc.
  - Data processing layer provides capabilities to locate and replace sensitive data in the intercepted I/O stream
  - Transparency allows for migrating from non-tokenised to tokenised without interruption of service

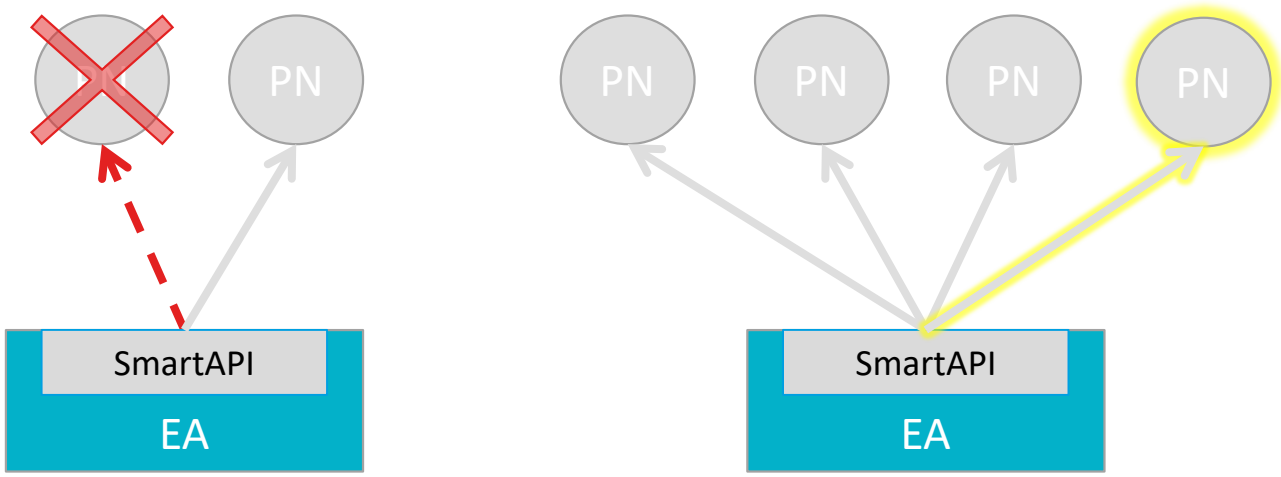
- API access for explicit control of protection engine
  If tight integration with the application is desired



SecurDPS SmartAPI – Not just a Simple API

SecurDPS makes high availability tokenization easy

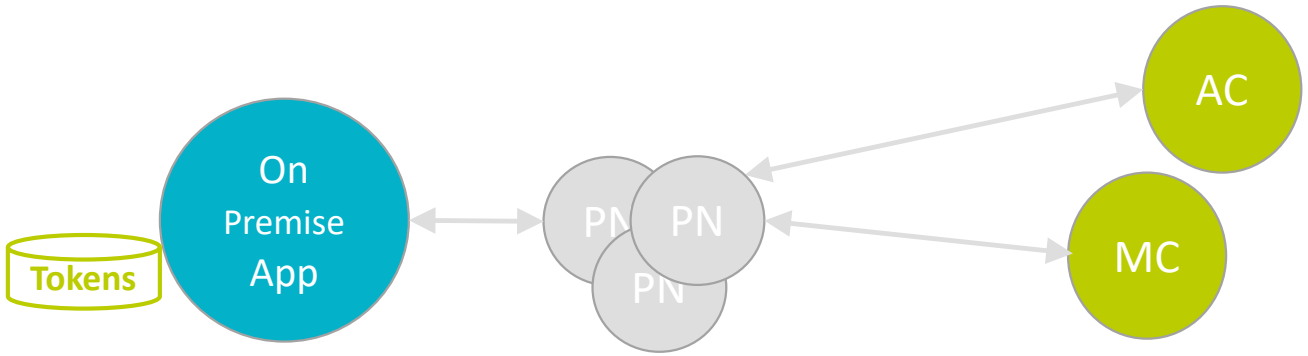
> Automatic failover
> Automatic load balancing
> Automatic (re)distribution
> Automatic integrity assurance
> Automatic scaling



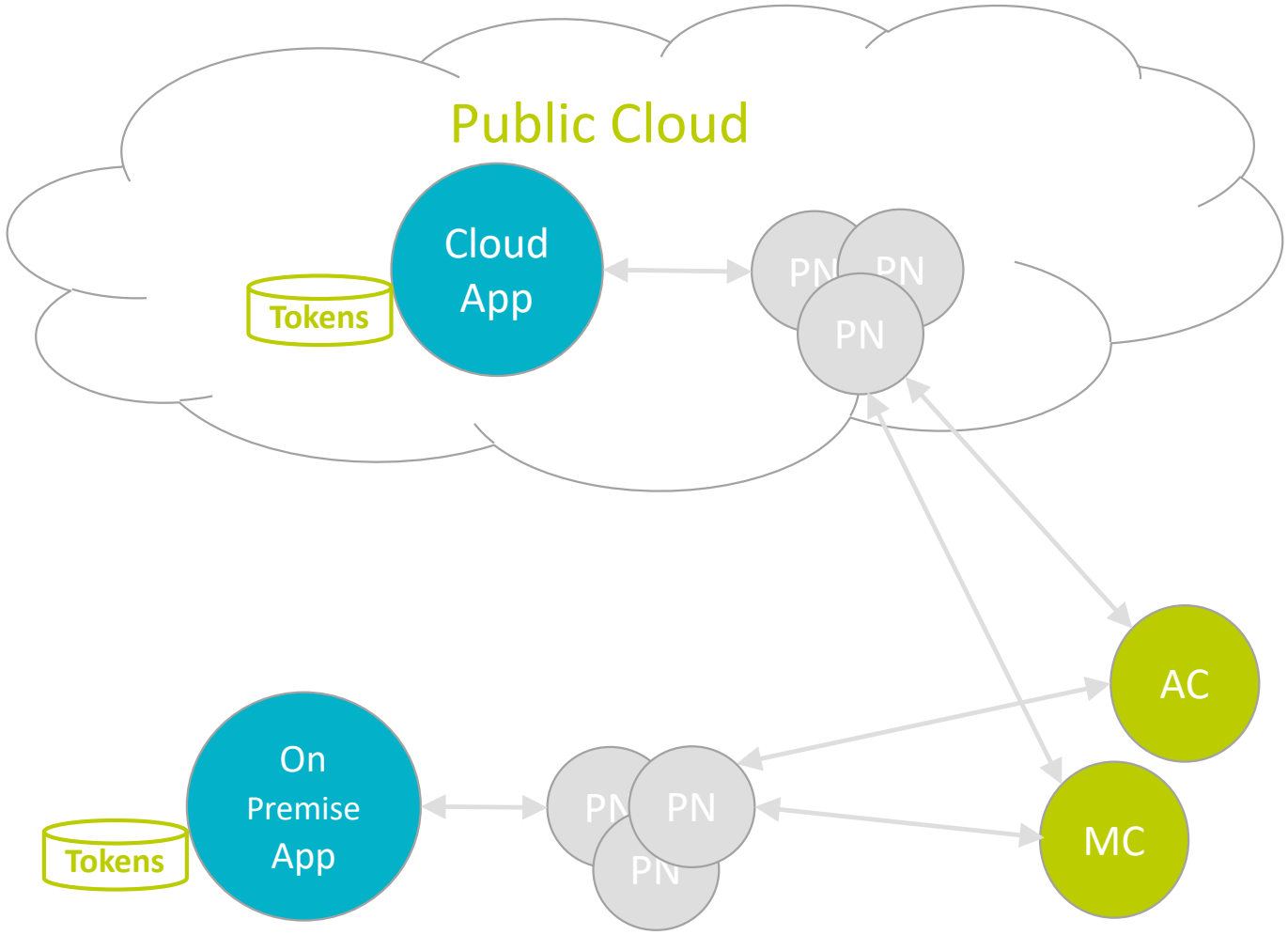
All transparent to the Enterprise App!

SecurDPS deployment options

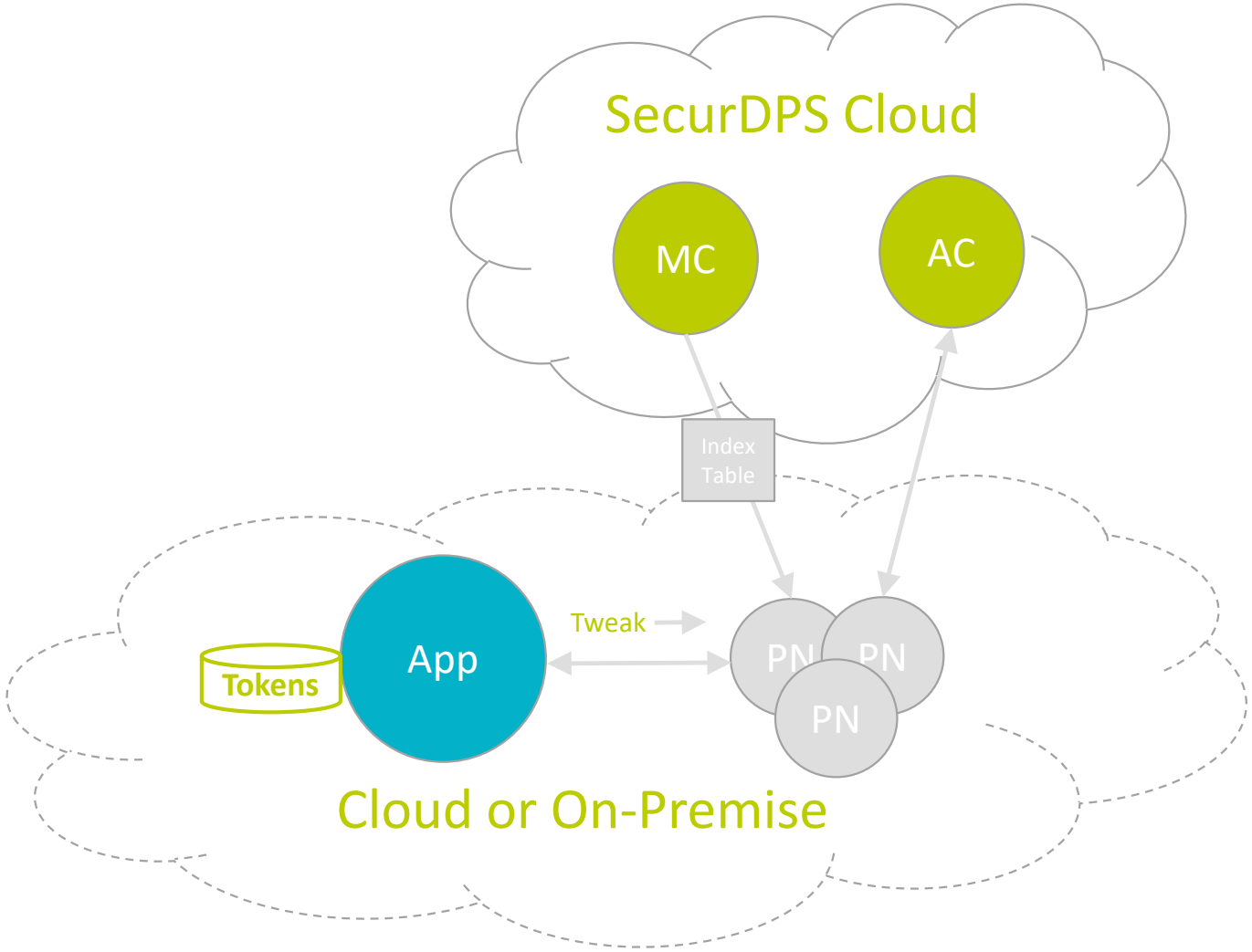
SecurDPS Enterprise On-Prem



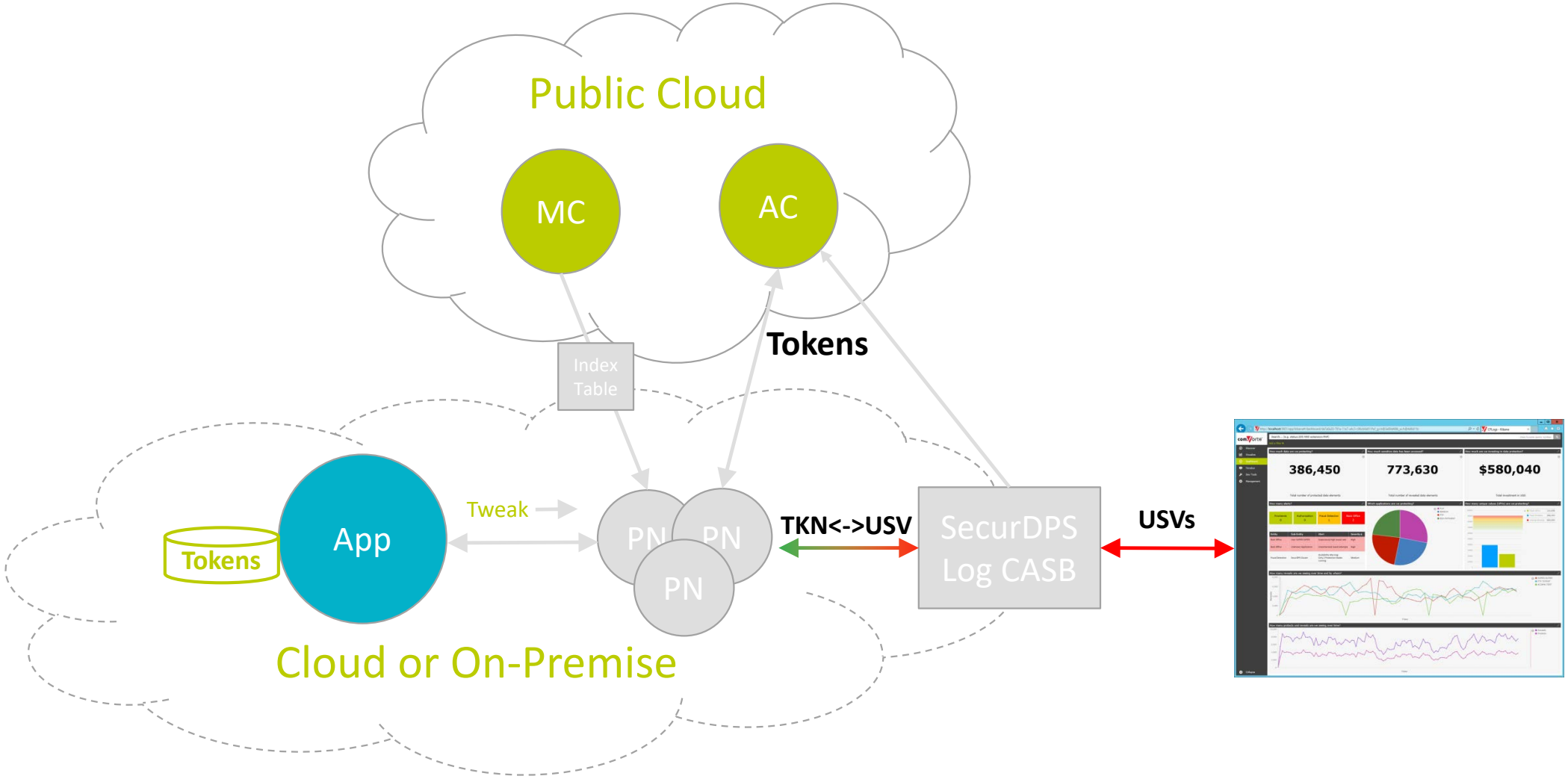
SecurDPS Enterprise Hybrid with on-prem and cloud app



SecurDPS Hybrid Cloud Deployment – no PANs to cloud



SecurDPS Hybrid Cloud Deployment



comForte - contacts

John Bycroft

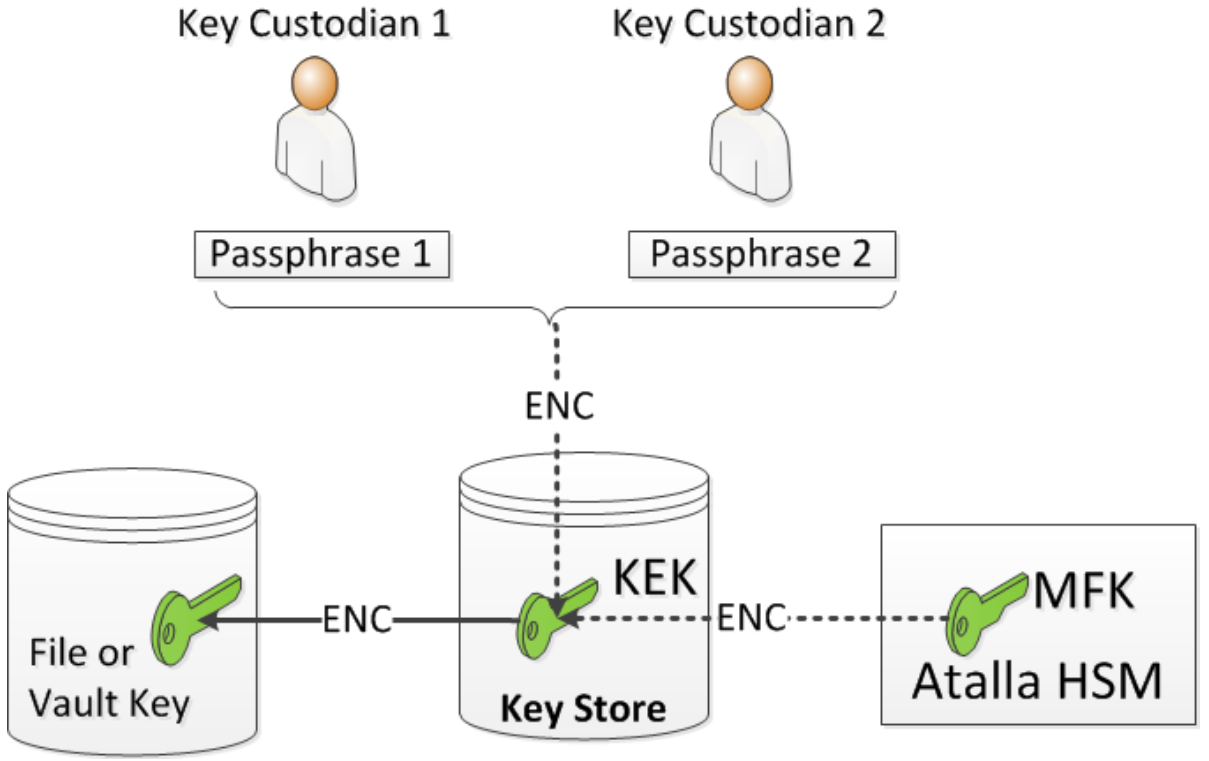
SVP Sales EMEA

Tel: +44 118 909 9076

Email: j.bycroft@comforte.com

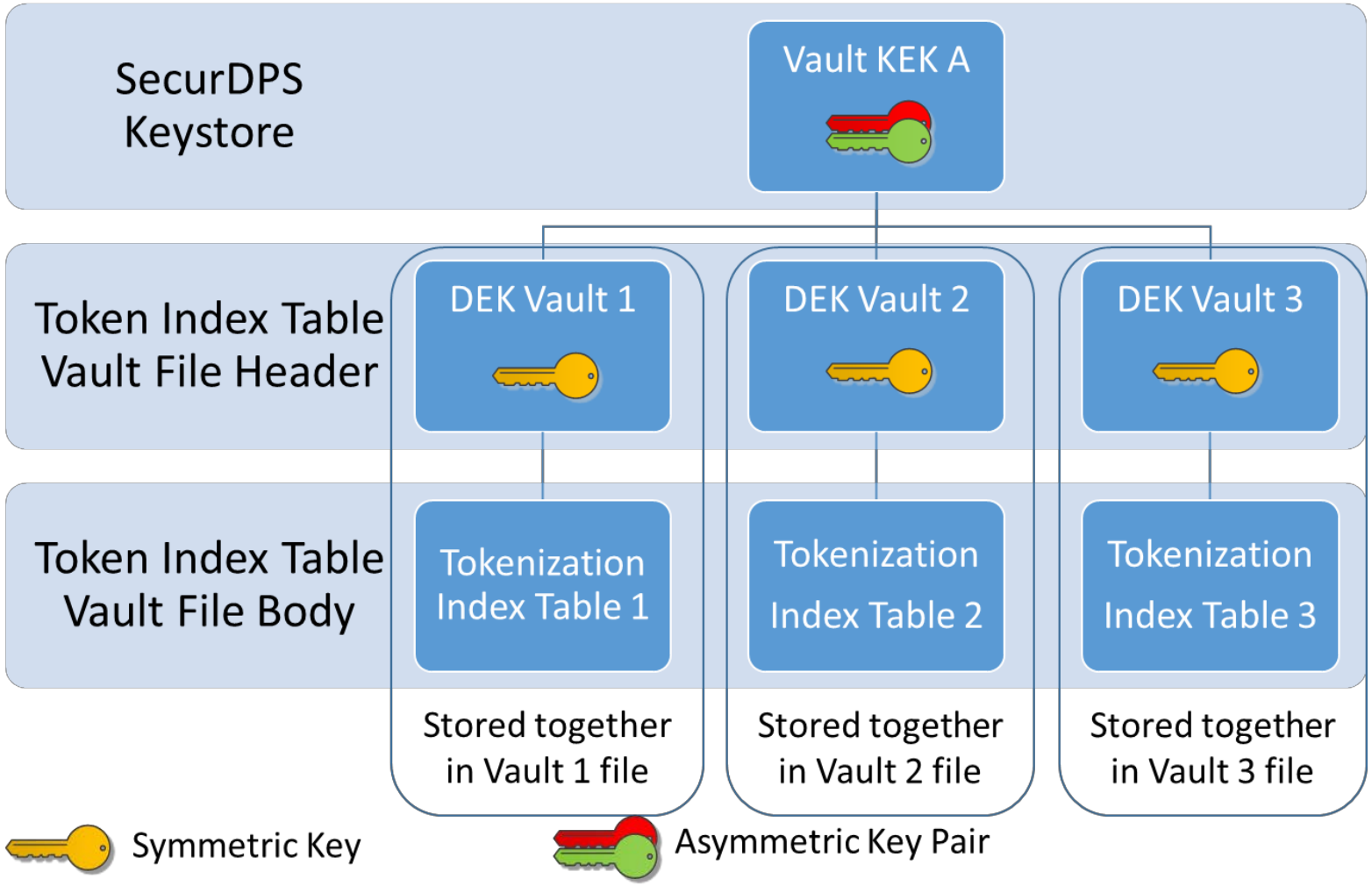
Security specials

Key protection & HSM integration



- Multiple layers of key encryption
- Optional vendor agnostic HSM integration
- Optional Key custodians for split knowledge / dual control
  - Key custodians can authorise key usage for unattended startup

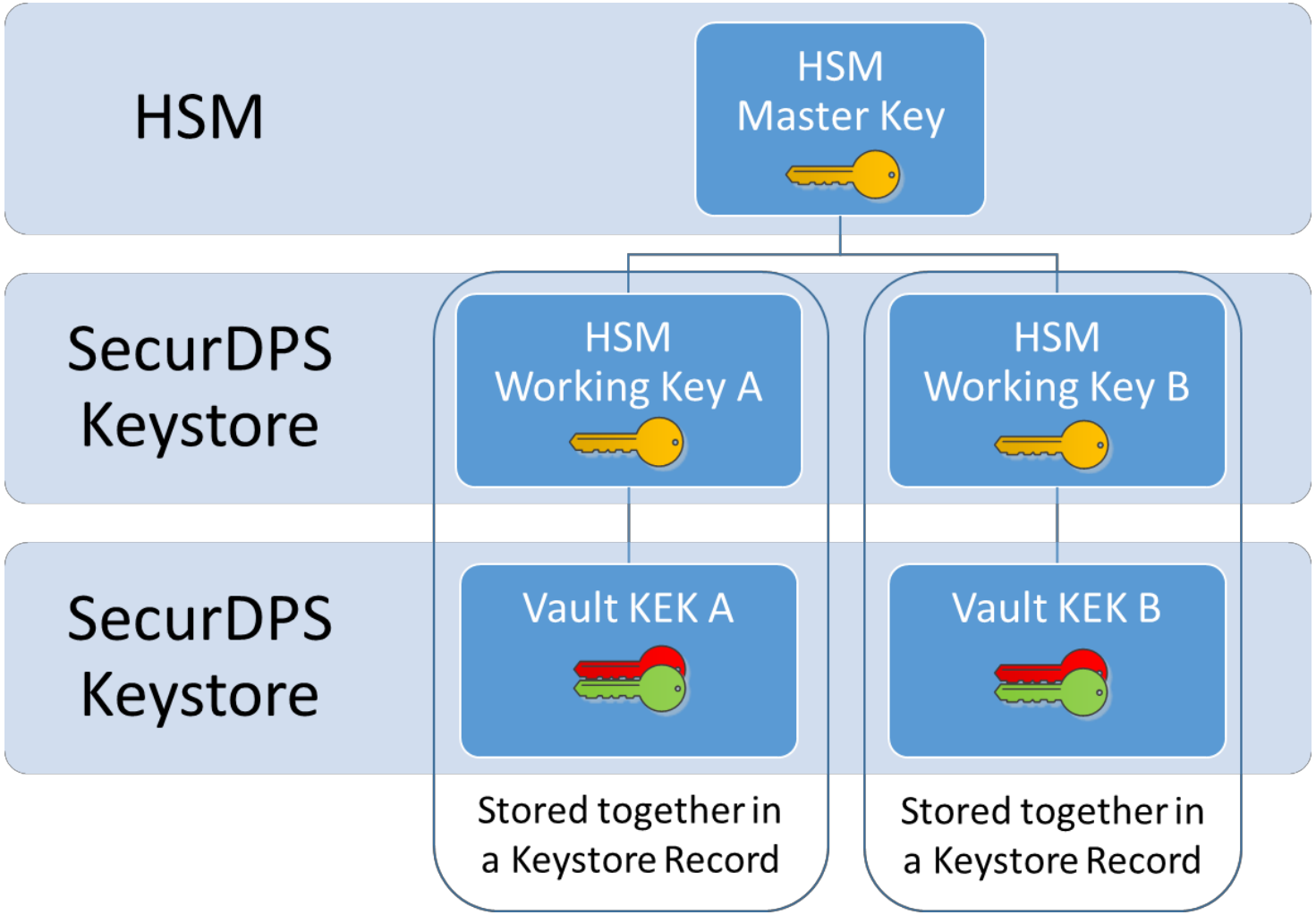
SecurDPS Key hierarchy



The types of the keys and the supported algorithms are as follows:

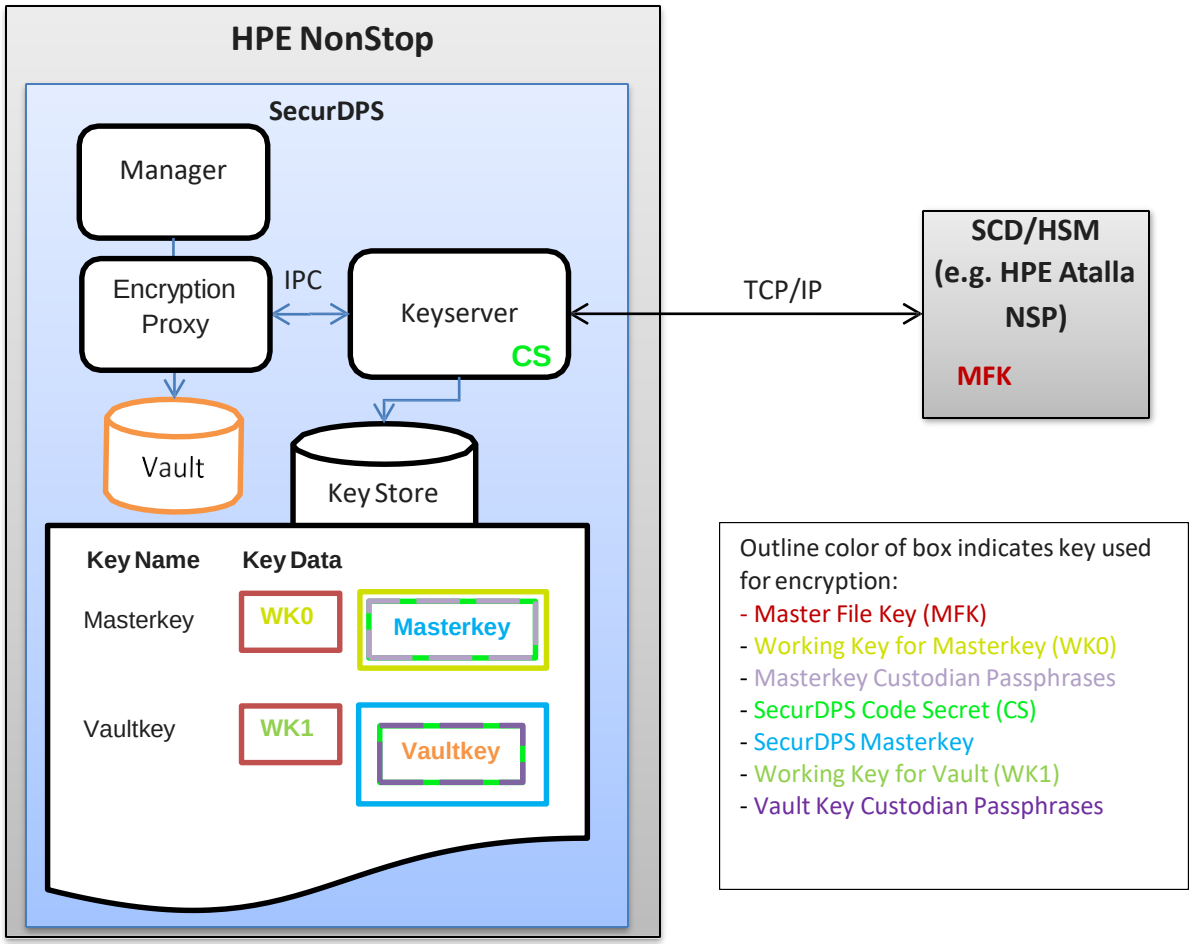
Key/Secret	Type	Supported Algorithms	Purpose and Usage
Vault KEK	Asymmetric	RSA OAEP 2048, 3072[1], 4096[1] Bits	Encrypt a DEK.
DEK	Symmetric	cbc-aes-256-sha-128 cbc-aes-256-sha-256 cbc-aes-256-sha-512	Encrypt a file.
Index Table	Large Random Table	ANSI X9.119-2-2017 i.e. comForte Tokenization Algorithm	Tokenize a sensitive data string (such as the PAN).

Key hierarchy with a HSM



Combining the Encryption Key Protection Layers (example NonStop)

- As a result, the keys in the key store can be protected by multiple optional key encryption layers:
  - **Encryption with a secret derived from the obfuscated code secret and the custodian's passphrases (if the key is under custodian control)**
  - **Encryption with an HSM/SCD working key**
  - **Encryption with the key store Masterkey.**
- Obviously, for the SecurDPS Masterkey itself layer 3 is not available. The diagram depicts an overview of this multi-layer approach.



Keys types and supported algorithms for Key Protection

Key/Secret	Type	Algorithms	Purpose and Usage
Obfuscated Code Secret	Symmetric	DES-EDE3-CBC AES-256-CBC[2]	Encrypt a key in the Keystore.
Custodian Passphrases	Symmetric	PBKDF2	Authenticate Custodians Derive the KEK for encrypting a key in the Keystore.
PBKDF2 Derived Key	Symmetric	DES-EDE3-CBC AES-256-CBC[2]	Encrypt a key in the Keystore
Keystore Masterkey	Asymmetric	RSA OAEP 2048, 3072[2], 4096[2]	Encrypt all keys in the Keystore
HSM working key	Symmetric	Depends on HSM	Encrypt a key in the key store
HSM master key	Depends on HSM	Depends on HSM	Encrypt an HSM key

SDF (Security Definition File) - Main Types of Objects

Opject type	Meaning
audit-collectors	An audit collector is a process belonging to the SecurDPS runtime environment which collects audit log messages received from one or multiple Managers.
applications	Identifiable processes communicating with Manager.
vaults	A vault in this context is an object controlling the translation of plain to protected data and vice versa. If SecurDPS is configured to perform data protection, at least one vault must be configured. It is possible to configure multiple vaults
Strategies	Specifies the details of how SecurDPS performs the data protection. At least one strategy referencing a previously configured vault must be configured for performing data protection. If necessary more than one strategy referencing the same or different vaults may be specified
files	ll the files containing data to be protected. At least one file object needs to be defined per file type, i.e. a set of file that share the same record format
fields	A field defines the properties of a data element in a file record, a message or a SQL table column. It may appear as part of the description of files, records, servers, request and replies
iso8583-schemas	This section defines ISO8583 field data format and structure to allow parsing of ISO data. This schema definition allows for defining both known and custom ISO data
base24-tokens	This section defines BASE24 token meta-data that describes fields to be tokenized within a specific token structure much like the iso8583-schemas

comForte - contacts

John Bycroft

SVP Sales Europe

133a Finchampstead Road,

Wokingham, Berkshire. RG40 3EX

Tel: +44 118 909 9076

Email: j.bycroft@comforte.com