PKI AS A SERVICE

Secure Enterprise Networks, IT Systems, and IoT Devices

Unlocking Automation and Enterprise Control

For more information contact questions@hydrantid.com or visit www.hydrantid.com

Root and Issuing CA Technical Operations Overview for 2018

As adoption of computers and the Internet has matured, so have users' expectations for security. New regulations and changing attitudes towards corporate responsibility and data protection are driving most organizations to devote considerable attention to computer security. HydrantID provides digital identity and advanced authentication services to help organizations secure data and systems as well as ecommerce transactions. HydrantID's services assist organizations to achieve industry best practices related to encryption and authentication while reducing operating complexity and costs.

In today's world of everything-as-a-service, it's easy to forget that Public Key Infrastructure (PKI) solutions were among the first 'cloud' services available in the market, well before the term Cloud existed in the context of computer services. Organizations all over the world have been buying trusted SSL certificates online since the mid-nineties. Arguably this PKI-based solution was the first security product to be widely sold and adopted globally by organizations of all sizes. A significant contributor to this success is the nature of PKI itself. As the name Public Key Infrastructure suggests, every digital certificate has a 'public' and a 'private' component. When utilizing cloud-based PKI solutions to protect servers and other corporate assets the only information that is sent and stored by our servers is the 'public' data contained in the certificate. Our customers retain the 'private' key and associated sensitive data within their own environments. PKI security was designed to only carry 'public' information and is the bedrock of the secure internet (HTTPS) used to protect millions of financial transactions every day.

The HydrantID cloud-based, commercial Certificate Authority (CA) provides managed PKI services to the enterprise and public sector in the Americas, Asia Pacific and Europe. Through our affiliate partner QuoVadis LTD., the company has operations in Switzerland, Holland, the UK, Germany, and Bermuda. Secure PKI hosting facilities are located in the United States, the Netherlands, Switzerland and Bermuda.

Unlock Your Automation

PKI has the advantage of being a foundational security technology that has been implemented for decades in a wide variety of use cases. This longevity in the market has driven commercial computer hardware, operating system and application providers to enable PKI-specific features in those products. This leads to most enterprises having a strong ecosystem of PKI certificate-aware products already deployed in their infrastructure.

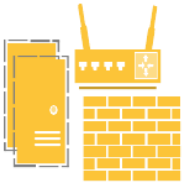
Common PKI Use Cases

Three primary security benefits provided by digital certificates are Authentication, Confidentiality and Integrity:

- Authentication: Digital certificates provide two keys that are mathematically-related, a "private" key that is kept secret and a "public" key that is meant for distribution. During certificate authentication, there is always a step that requires data to be encrypted by one of the keys and decrypted by the corresponding second key. The simplest example of this is visiting a secure website in a browser. When you go to https://hydrantid.com, the browser uses the SSL certificates' public key to compute a secret. The server hosting hydrantid.com must have the corresponding private key to decrypt the secret data.
- Confidentiality: Digital certificate-aware protocols (like SSL and its replacement, TLS) use a combination of symmetric and asymmetric encryption to ensure message privacy. In the hydrantid.com example above, the web browser and hosting server agree on an encryption algorithm and a shared secret key to be used for one session only. All messages transmitted between the web browser and hosting server are encrypted using that algorithm and key, ensuring that the message remains private even if it is intercepted.
- Integrity: Digital certificate-aware protocols provide data integrity by calculating a message digest, also known as a hash value. The contents of the message are "hashed" via an algorithm e.g. SHA-256, that produces a result that can be repeated only if the message contents and algorithm remain unchanged. The digital signature keys are used to "sign" and "verify" the original calculated hash (message digest) to ensure that it was not tampered with during transport.

Where would an enterprise value these benefits? Some common examples are:

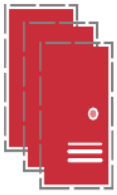
Windows and MacOS computers and servers that are joined to a Microsoft Active Directory domain
Installing digital certificates on each user's computer that is attached to your corporate network provides a method for authentication to ensure only trusted devices are present on your network. For servers, the use of SSL/TLS certificates adds verification and encryption of connections, both internally and externally.



Network devices such as routers, firewalls, load balancers and SSL Inspectors
Installing digital certificates from your own dedicated, branded CA provides a method for authentication and encryption between devices and protects against impersonation by providing your own trusted certificate chain.

Smartphones, tablets, smartcards and other user devices Installing digital certificates from your own dedicated, branded CA on user devices, either personal or corporate-provisioned using a Mobile Device Management platform and Wireless Gateway provides an option for seamless wireless authentication to your network.

MacOS computers managed with OSX Profile Manager
Much like that for Windows domain-joined computers, installing digital certificates from your own dedicated, branded CA on each user's computer that is attached to your corporate network provides a method for authentication to ensure only trusted devices are present on your network.



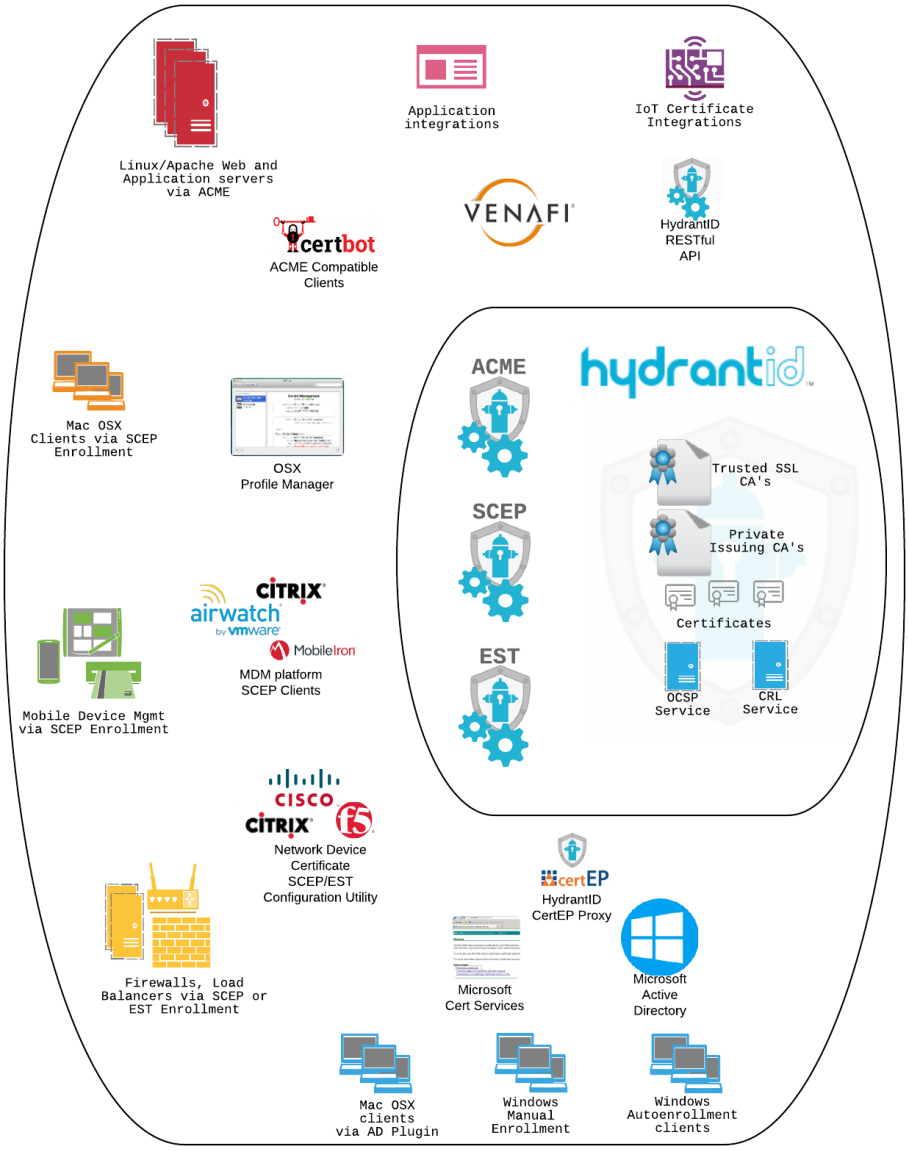
Microsoft IIS, Linux and Apache Web and Application Servers
Installing trusted SSL/TLS certificates (such as Extended Validation certificates) for external-facing Web services provides additional verification and security for your customers and other website visitors. Internal servers benefit from SSL/TLS certificates issued from your own dedicated, branded CA to protect internal connections and services.

Application Integrations
Business automation tools such as ServiceNow can be integrated with both our trusted SSL and private CA services to provide workflow automation customized for your unique requirements. Key Management platforms like Venafi provide a wide range of certificate automation capabilities to simplify the rollout and management of certificates in complex environments.

Internet of Things devices and Gateways
A less common use case for the average enterprise. Digital certificates can be issued from your own purpose-built, IoT-specific CA via our RESTful Certificate API to enable devices, gateways and management systems to provide a full chain of trust for authentication to ensure only trusted devices are present on your network.

How Do I "Unlock Automation" For These Use Cases?

For each use case listed above, it's important to understand what vendor products, platforms and technologies are being utilized in your enterprise that are "certificate-aware". This diagram shows some common examples used by our customers.



This table provides details for each use case. The middle column lists some platforms already present in many of our customers' networks that can be used to enable automated

or assisted PKI rollouts. The last column lists the service hosted or provided by HydrantID that provides the channel between your enterprise and HydrantID PKI services:

Use Case	Enabled By	HydrantID Service
Windows and MacOS computers and servers (Microsoft IIS) that are joined to a Microsoft Active Directory domain	• Microsoft Active Directory • Microsoft CertSrv • Microsoft Autoenrollment	**Secardeo CertEP** (A cert request proxy that is installed in your enterprise domain)
Network devices such as routers, firewalls, load balancers and SSL Inspectors	• Device Configuration software • Venafi Trust platform	**SCEP** (Simple Certificate Enrollment Protocol) and **EST** (Enrollment over Secure Transport)
Mobile Device Management solutions for Smartphones, tablets, smartcards and other user devices	• Airwatch by VMWare • MobileIron • Citrix ZenMobile • Other MDM software	**SCEP** (Simple Certificate Enrollment Protocol) or **Secardeo CertEP** (A cert request proxy that is installed in your enterprise domain)
MacOS computers managed with OSX Profile Manager	• OSX Profile Manager • JAMF Now • JAMF Pro	**SCEP** (Simple Certificate Enrollment Protocol)
Linux and Apache Web and Application Servers	• CertBot • Other ACME-compliant clients	**ACME** (Automated Certificate Management Environment)
Application Integrations	• Venafi Trust Platform • Secardeo CertEP • Any third-party API-aware application	**Certificate API** (A RESTful API that enables the request, status, download and revocation of certificates from HydrantID-managed CA services)

Your Own Private CA

HydrantID offers two Managed PKI models: A Private PKI (Private Root) for organizations that need full control over certificate policies and root key distribution (Figure 1); and the Dedicated Issuing CA (Shared Root) that provides a low-cost alternative for organizations that just need digital certificates to secure internal servers and other resources (Figure 2).

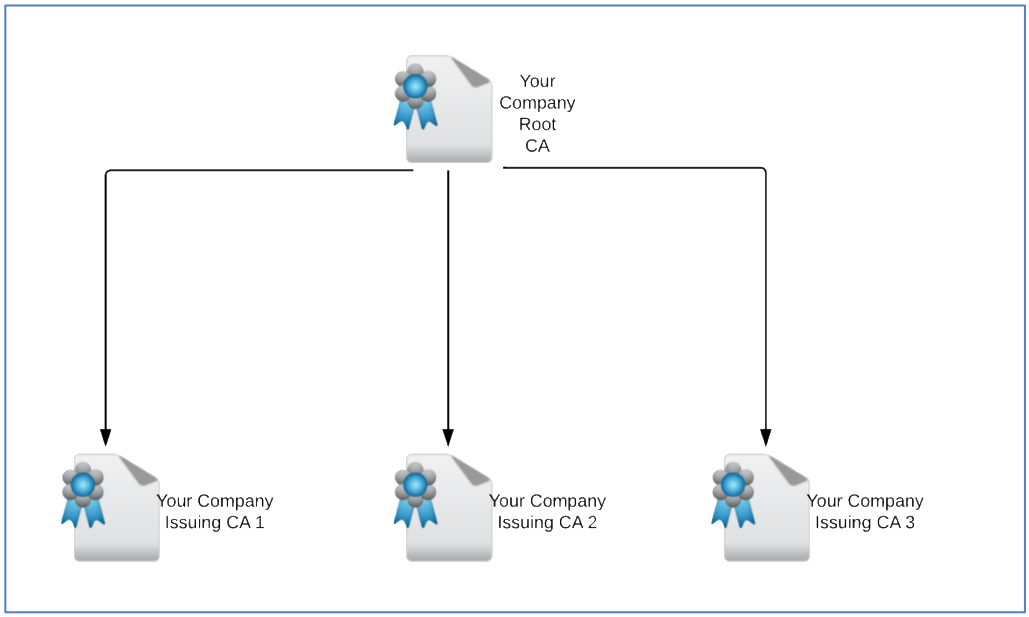


Figure 1: Private PKI Hierarchy

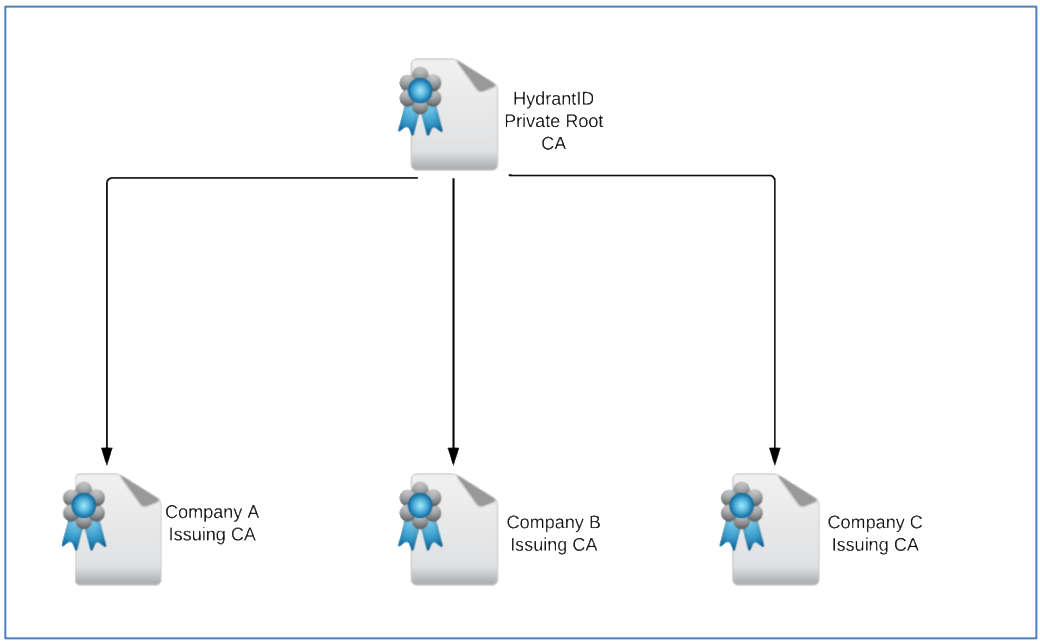


Figure 2: Dedicated ICA Hierarchy

HydrantID also delivers Enterprise Trusted Certificate Services for providing SSL/TLS, Extended Validation, Code Signing, S/MIME and other pre-trusted certificates. You can find out more about each of these services at https://www.hydrantid.com.

All our PKI solutions provide the necessary documentation, set-up and on-going CA operations to free your staff to focus on your core business. We provide scalable, secure and

geographically-distributed implementations for Managed PKIs and leverage highly-secure and audited technical facilities and expertise to deliver all our services.

HydrantID charges a fixed annual subscription fee for the operation of our PKI solutions, with the subscription tailored to each customer's specific requirements. All of our services can be included in a single subscription and new services can be added at any time.

Functionality, Security and Usability

Both the Dedicated Issuing CA and Private PKI offerings share a common set of functionality that one would expect from our world-class service:

- All Issuing CA private keys are generated and maintained in FIPS 140-2 Level 3 certified Hardware Security Modules
- All Issuing CA private keys are replicated to a geographically-diverse backup site
- Validation Authority service with both CRL publishing and OCSP responders
- OCSP stapling support
- Certificate management web console
- Optional Web Service API for automation
- Automated key management and Active Directory/Autoenrollment support via third-party key and certificate management solutions such as Venafi and Secardeo
- Includes ability to manage Subject Alternative Name (SAN) fields
- Supports multiple certificate policies/types (SSL/TLS, UCC, wildcard, device, S/MIME, encryption, signing, etc.)
- Supports multiple Administrators and rights delegation
- Support for privileged and least privileged accounts as well as organization and department separation

Our service uses Policy Templates to control the types of certificates issued to your account. We provide a number of pre-configured templates that cover the more popular types of certificates (SSL/TLS, UCC, wildcard, device, S/MIME, encryption, signing, etc.). These can be used as a starting point for further customization to meet your business needs.

Moving up to our Private PKI offering adds the features necessary for organizations that want full control over branding, policies and certificate hierarchy:

- Offline private root key(s) and certificate(s)
- Scripted, recorded Key Generation ceremony
- Offline root storage- HSM, security world and card sets, safe in multiple geographically-diverse locations
- Custom Certificate Policy and Certificate Practice Statement (optional)
- Existing Certificate Policy and Certificate Practice Statement review and mapping
- OCSP responder service using software signing keys

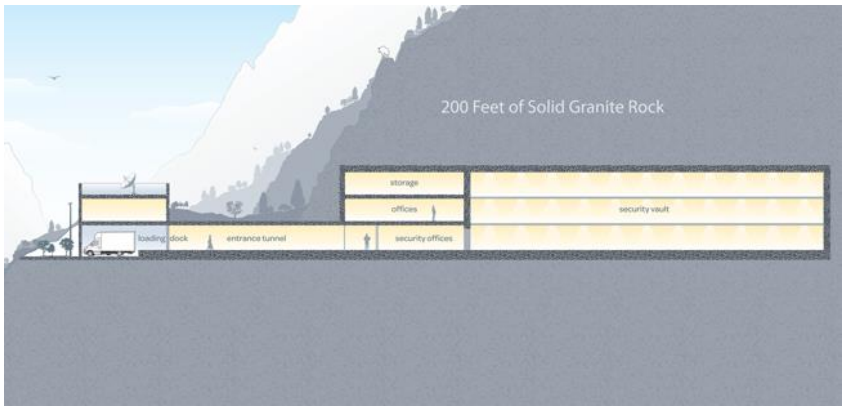
We work closely with our customers to determine the best PKI architecture for their needs. As part of our Private PKI service we offer a workshop that is used to determine:

- CA Naming
- Certificate Policy requirements
- Scope of certificate usage
- Web Services Configuration
- User acceptance testing criteria
- Internal audit and reporting requirements

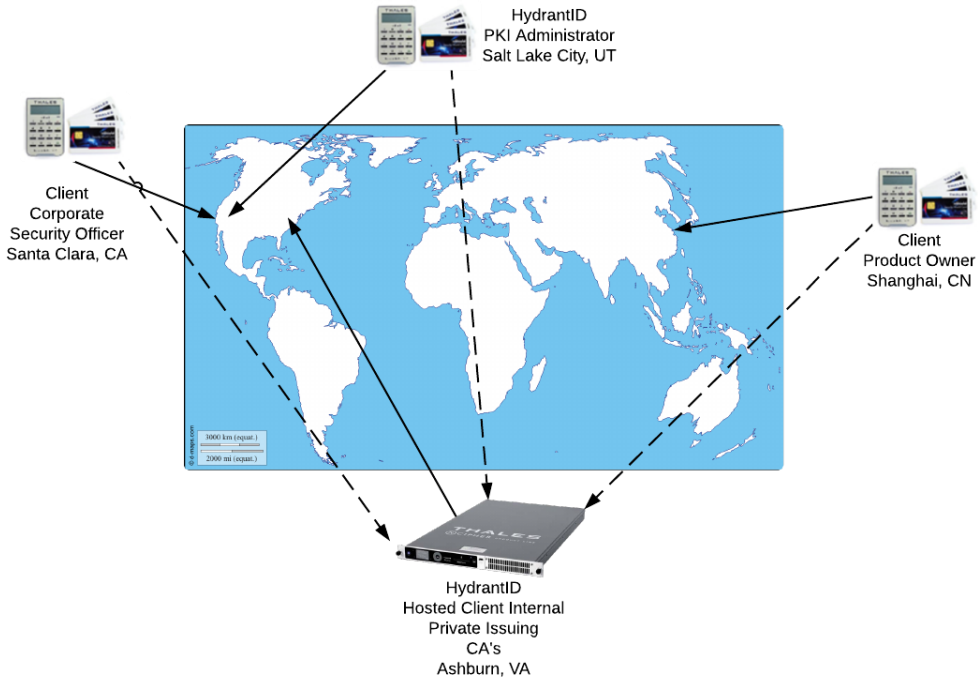
The results of the Workshop are used to create a customized Private Root Hierarchy document that covers the PKI hierarchy design, branding, policy identifiers and certificate types required to deliver a fully-functional PKI service. This becomes the blueprint for generating the private keys and associated certificates.

Private PKI Service Key Generation and Storage

The Private PKI Root CA keys are created during a CA Webtrust-compliant key generation ceremony attended by a business and technical representative of your company. This is designed explicitly around providing full accountability, the highest level of security for the Root CA private keys and maintaining multi-person control of all critical key generation assets. Using non-networked dedicated equipment, the key ceremony is performed in a maximum security digital records and microfilm storage vault located inside a solid granite mountain. This vault, built to Department of Defense specifications, is used to secure dedicated Customer and HydrantID safes containing the Hardware Security Modules and associated activation data. On-going storage and maintenance activities like Key and Certificate Rollover, CRL generation and OCSP Signing certificate renewal are included in our service offering.



For companies or organizations that may need the ability to create PKI hierarchies "on-demand" but still enforce multi-person control and full accountability we also offer a Remote Key Generation Ceremony capability. For more information, please contact your HydrantID representative.



Root and Issuing Key Portability

The Private PKI Root CA will be generated on a dedicated Thales Edge HSM. Upon termination of the contract, these components and any "k-of-n" smartcards and activation data will be provided to the Customer in a secure manner agreed upon by both parties.

The Issuing CA private keys will be hosted on shared HSMs. Upon termination of the contract, these key blobs will be merged into a migration Security World and the "k-of-n" smartcards and activation data will be provided to the Customer in a secure manner agreed upon by both parties.

Key Sizes and Algorithm Support

Although our Dedicated ICA and Private PKI offerings are not governed by an industry group, we encourage our customers to follow best practices for key size and hashing algorithm choices. This currently is a baseline of 2048-bit keys for device and user certificates and 4096-bit keys for Issuing and Root CA's. We have the ability to issue a wide range of key sizes and hash algorithms for cases where your organization needs a custom solution.

Our standard Cryptographic provider is RSA#nCipher Security World Key Storage Provider which is compatible with SHA-256, SHA-384 and SHA-512. We also support:

- Asymmetric public key algorithms: RSA (1024, 2048, 4096), Diffie-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH

- Symmetric algorithms: AES, ARIA, Camellia, CAST, DES, RIPEMD160 HMAC, SEED, Triple DES

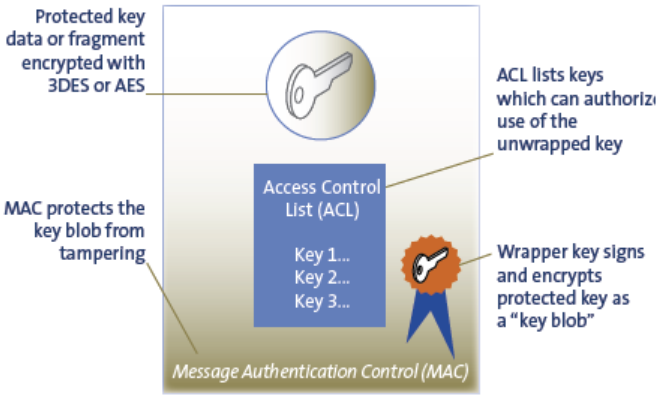
- Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit)

- Full Suite B implementation with fully licensed Elliptic Curve Cryptography (ECC) including Brainpool and custom curves

Both Private and Dedicated PKI root keys will be generated on a Thales Edge FIPS 140-2 Level 3 validated Hardware Security Module (HSM). This HSM enforces multi-person control for sensitive processes, such as configuring a new HSM module or activating a key for use. This is commonly known as "k of n", or having a "quorum." The basic premise of k of n is to divide the interactions needed to access information among multiple entities. In the case of an HSM connected to a CA, multiple smartcards need to be connected to the HSM to generate or activate the use of the CA private key. The cards or token can then be separated, distributed, and securely stored to help enforce these processes. The Thales Security World allows for physically splitting key management responsibilities. Split responsibility is a widely accepted control within most security policies. Through its multi-party "k-of-n" control functionality, important key functions, procedures or operations can mandate that more than one person is required to perform these tasks. Instead, a quorum of key holders (the "k" in the "k-of-n") must authorize the actions of the console operator.

The Security World construct also supports scalability by providing a secure and tightly managed process for provisioning identical Issuing CA keys to additional Thales HSMs. Backups are accomplished by making copies of the Issuing CA application "key blob" and moving them to physically and geographically-diverse locations. The Security World construct ensures that the "key blob" is worthless without the "k-of-n" smartcards and a properly-initialized HSM. The following was provided by Thales for reference:

Key Access and Storage
An application "key blob" consists of the key material, the key's Access Control List (ACL), and a cryptographically strong checksum, all encrypted with a 3DES or AES key. In the case of a card set-protected application key, the 3DES or AES wrapper key used is stored via secret-sharing across the Operator Card set and is known as a Logical Token. In the case of a module-protected application key, the 3DES or AES key used is the Security World Module Key, stored in the HSM's nonvolatile memory.

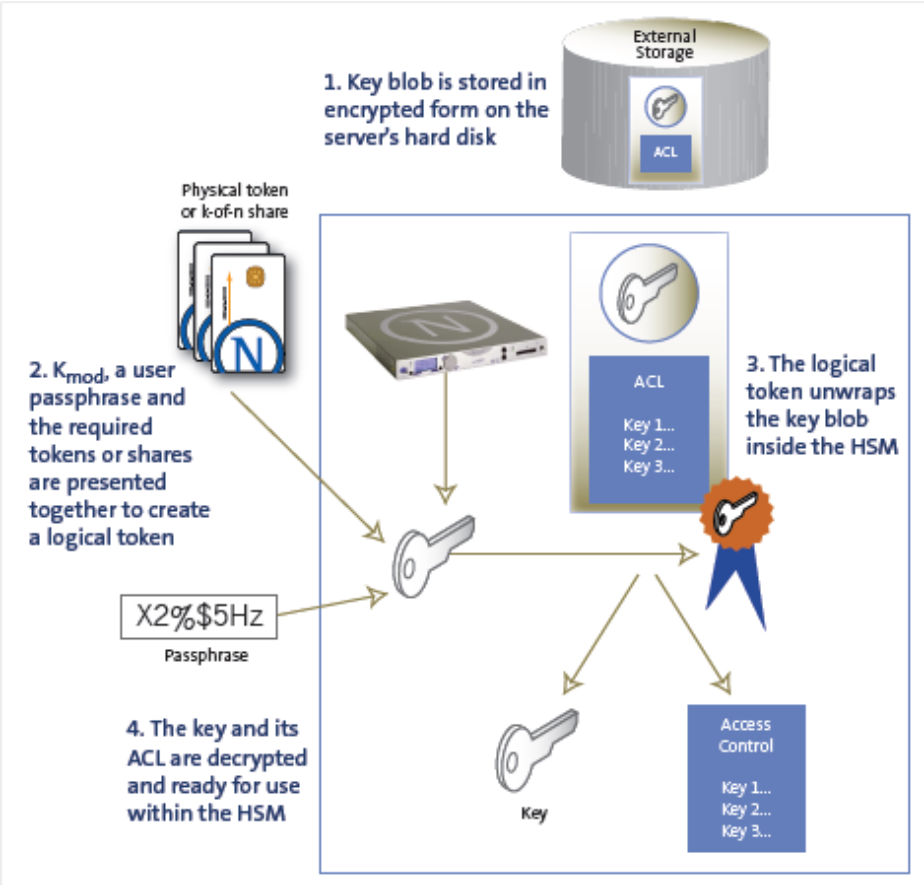


Key Storage

The Security World Module Key is itself stored in a blob on the host file system; the key data, ACL and checksum are encrypted with a 3DES or AES Logical Token stored on the ACS. This allows the Administrator Card Holders to load the Security World Module Key into additional HSMs. The security world module key can be loaded on both dedicated Thales nShield HSMs and on Thales netHSMs.

A Logical Token remains in the HSM and on the smartcards and is never passed to the host even in encrypted form. Additional encryption of the Shares of a Logical Token ensures that the passphrases (if set) are required to assemble the Shares into the original 3DES or AES key, and in the case of Operator Cards, to ensure that the card set is used only in HSMs possessing the Security World Module Key.

OCS-protected application keys with Recovery enabled are also stored in a Recovery Blob alongside the main working blob. The Recovery Blob is encrypted using an RSA key pair known as the Recovery Encryption Key. The private half of the Recovery Encryption Key is again stored as a blob protected by a Logical Token stored on the ACS. This allows the Administrator Card Holders to perform the recovery from lost or unusable Operator Cardsets as shown below.



Access to cryptographic keys

Accessing Your PKI Services

We provide an easy-to-use web-based certificate portal that provides a single interface for your account setup, management and reporting needs for both Managed PKI and Trusted SSL certificates in one place. The portal is accessed using any standard web browser and does not require any additional client-side software. This also provides customers the ability to distribute the administration of certificate lifecycles across their organizational with customizable administrator roles. We also provide online training and an Administrator guide that explains the account settings and ability to delegate specific permissions to other Administrators.

Performance, Availability and Scalability

Customers of our PKI offerings rely on two primary services for day-to-day operations: Certificate Issuance and Certificate Validation.

Certificate issuance is a multithreaded service with three primary stages:

- Request submittal: Incoming certificate requests from our portal or API are accepted by a request queue. This provides an auto-scaling method to handle highly-variable peaks in certificate request volumes.
- Request processing: Requests may be subject to a variety of rules processing before being signed by the CA (Certificate Authority). Examples are name constraints, policy enforcement and external dependencies that must be verified prior to the certificate being issued and returned to the requesting customer. The complexity of the certificate to be generated, e.g., key size, number of SAN (Subject Alternative Name) fields, etc., can also increase the issuance time.
- Signed Certificate Return: How the signed certificate is returned depends on the request method. For portal users, an email is generated by our system and sent to the Requestor and other account administrators. A status indicator is also set in the portal. The certificate may be downloaded in both PEM and DER formats, without or without the full certificate chain. For API users, a polling mechanism is used for API-generated requests and third-party integrations. These services poll at frequent intervals and download the certificate as soon as it is available.

Certificate validation information is provided by Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) servers. All Dedicated ICA's and Private PKI's are configured to publish a CRL each time a certificate is revoked and at a specified interval. They are published to a hosted location and can be downloaded as needed. OCSP services provide near real-time revocation status information and is included in both our service offerings. We also support OCSP Stapling which allows a server protected by a certificate to request status information and pass it on to connecting clients. This greatly reduces WAN traffic for busy sites and reduces page load times.

Both CRL and OCSP information may served out of the United States, the Netherlands, Germany, Bermuda and/or Swiss data centers on a round-robin DNS basis with multiple servers in each location. This load balancing method ensures that any interruption at any location is covered by another data center.

Incoming connections to these services are a shared resource and are sized to provide ample bandwidth for all customers on our platform. Capacity is managed by HydrantID and will be added as necessary without our customers incurring additional bandwidth charges.

We maintain Service Level Agreements with all our customers to ensure that our Issuance and Validation systems are available and responsive when you need them. HydrantID operates a multi-location Support desk to provide 24 hour/7 days a week support for solving outages and other high-priority issues. A customer-specific support group is established in our ticketing system and key HydrantID contacts for support issues and escalation are provided at service initiation. We support the use of S/MIME for authenticated and encrypted communications, and maintain a list of authorized customer representatives to authenticate service requests and confirmations.