hydrantid™

Secure Enterprise Networks, IT Systems, and IoT Devices

Unlocking Automation and Enterprise Control

Automating Certificates With Your Own Private PKI

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.

PKI Basics

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.

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.

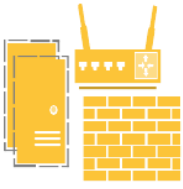
Common PKI Use Cases

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:

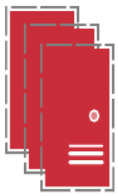
Windows and MacOS computers and servers that are joined to a Microsoft Active Directory domain
Installing digital certificates on each user's computer that is attached to your corporate network provides a method for authentication to ensure only trusted devices are present on your network. For servers, 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.



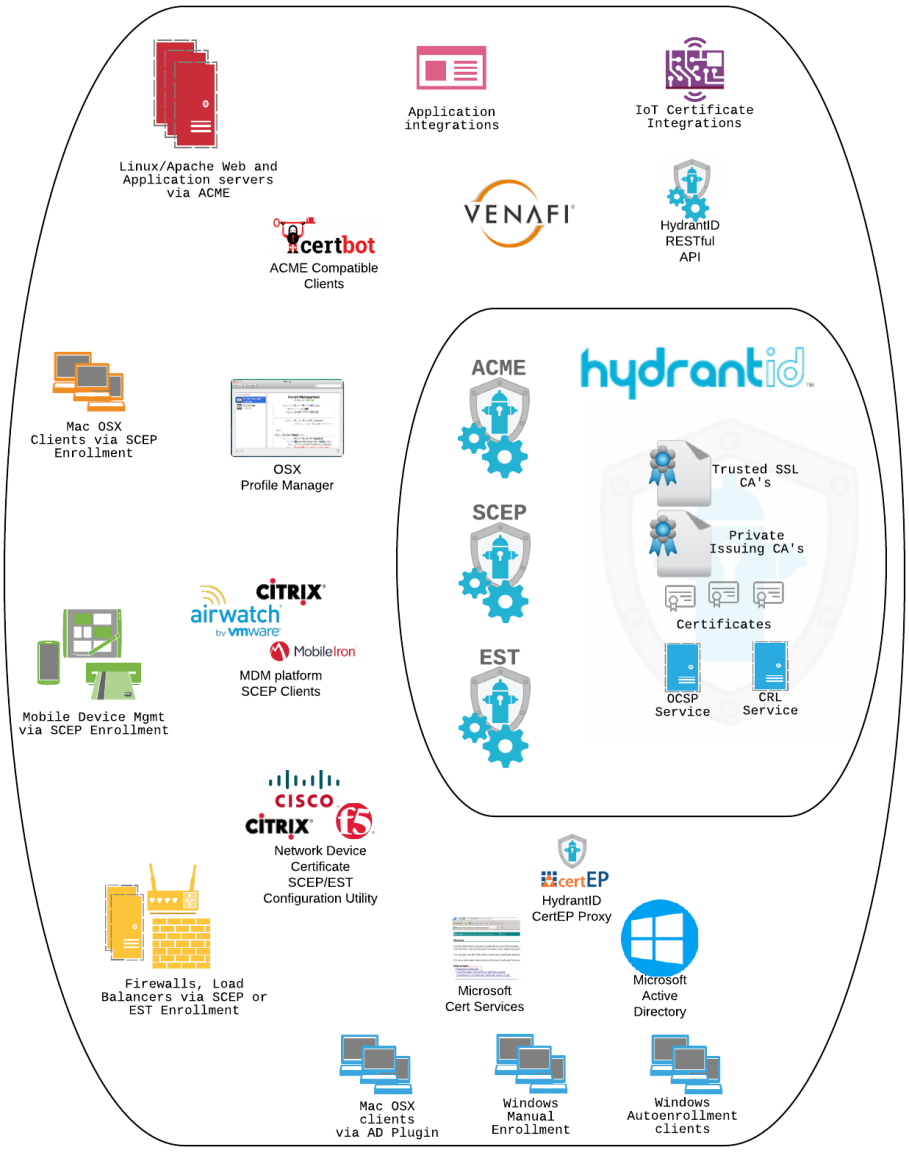
Microsoft IIS, Linux and Apache Web and Application Servers
Installing trusted SSL/TLS certificates (such as Extended Validation certificates) for external-facing Web services provides additional verification and security for your customers and other website visitors. Internal servers benefit from SSL/TLS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

- Private PKI (Private Root) for organizations that need full control over certificate policies and root key distribution (Figure 1)
- 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).

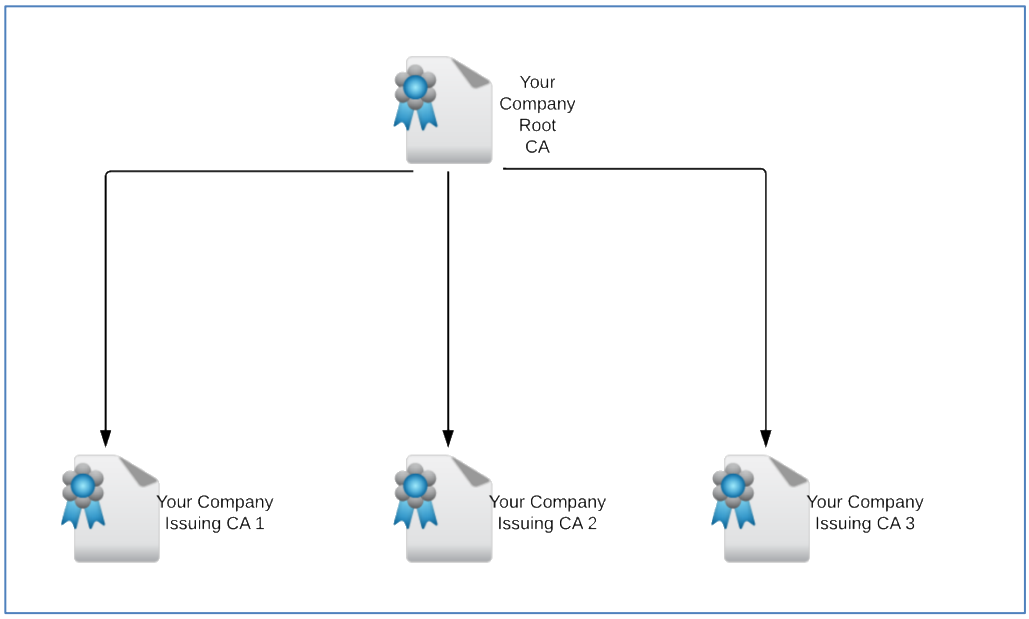


Figure 1: Private PKI Hierarchy

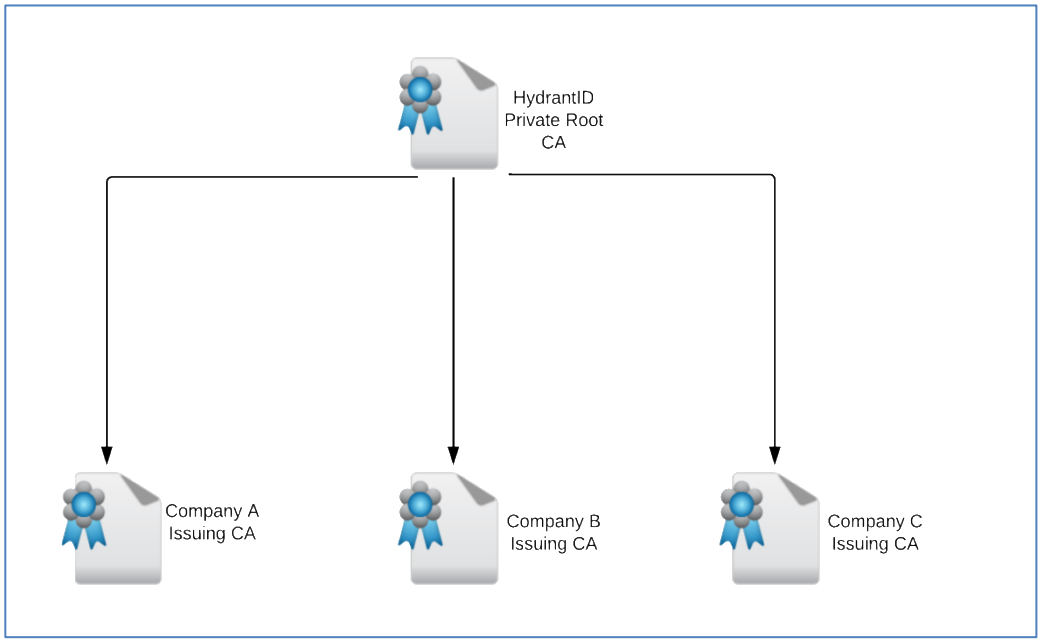


Figure 2: Dedicated ICA Hierarchy

Benefits and Cost Structure

All of 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 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.

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.

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.

Additional Services

HydrantID also delivers Enterprise Trusted Certificate Services for providing SSL/TLS, Extended Validation, Code Signing, S/MIME and other pre-trusted certificates, all for one low subscription fee, and no per certificate pricing. Certificates are issued on-demand and in real time. Find additional information for these services at: https://www.hydrantid.com.

About

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.

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