Certificate Automation Rollout for Enterprises

GETTING STARTED WITH THE CONNECTOR MODEL OF PKI-AS-A-SERVICE (PKIAAS)

Maintaining certificates is more than a hassle; between lost revenue and high IT costs, expired certificates deeply affect an organization's bottom line. Automating certificates has become critical for enterprises seeking a seamless, secure online presence. There are a number of certificate automation models available to establish this critical PKI infrastructure and secure communications between machines, network and mobile devices, virtual servers, and the Internet of Things. This technical guide provides the basics on how they work, and dives into the details of rolling out the connector model of certificate management — like HID PKIaaS.

WHITE PAPER

The Case for Connectors

HID PKIaaS leverages a connector model of certificate automation. With this method, certificate utilities that already exist in the market are added to a platform (such as ACME clients) or are embedded in popular enterprise platforms (like Microsoft Intune). Unlike agent or agentless models, the connector model does not rely on the introduction of a "command and control" platform solely for the management of certificates.

Since the connector model is not a command and control environment, it does not require that a central management console be installed and maintained by your IT team to prevent failures. The connectors work autonomously to request and install certificates independent of one another, with a lightweight browser-based certificate portal providing the traditional certificate management functions like manual issuance, revocation, reporting and account management. This approach does not require privileged local system credentials and decentralizes the mechanics of managing certificates, which eliminates the management console from being an enterprise-wide, central point of failure. It also reduces the dependency on a single vendor, as most connectors are not proprietary to HID Global and can be simply re-configured for use with other certificate service providers.

AUTOMATED CERTIFICATE MANAGEMENT

The ongoing work of securing servers and applications with digital certificates presents a perfect opportunity for automation. Ensuring that keys and certificates are generated and installed correctly becomes easier to manage when purpose-built utilities are deployed. In addition, installing and configuring automated certificate utilities, like the widely-available Automated Certificate Management Environment (ACME) clients, ultimately saves a great deal of time compared to installing certificates manually. With HID PKIaaS, you control which processes are automated.

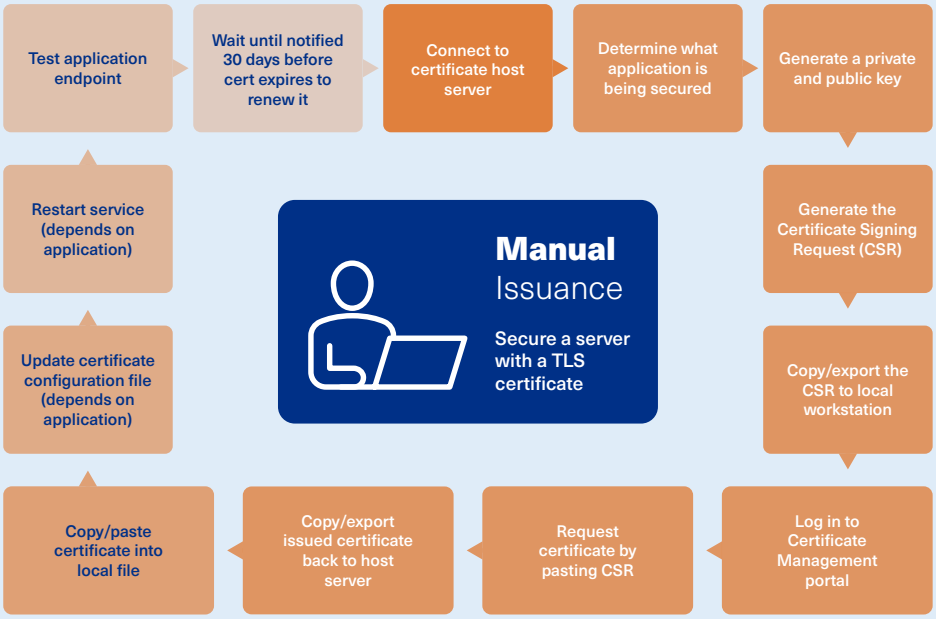
CERTIFICATE MANAGEMENT MODELS

There are three models of certificate management:

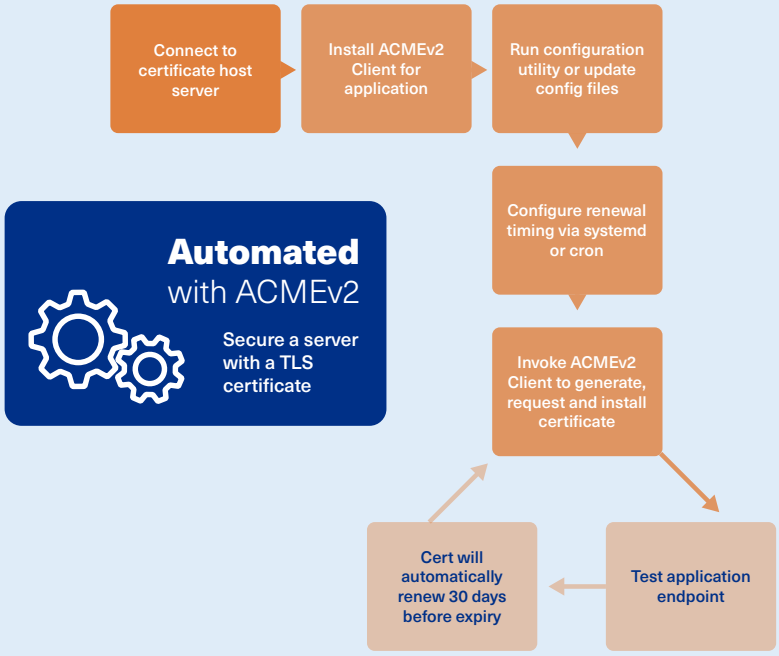
- Agent: Installs software on a computer that lets the service know when a certificate is about to expire
- Agentless: Pushes data to a computer for automatic updates
- Connector: Uses technology agnostic open-source tools

For more information on certificate management options, read our eBook: **PKI Automation Strategies: Finding the Perfect Fit for Your Organization**

The traditional method of securing a server requires multiple steps for each and every certificate:



With ACME clients, certificates can be replaced with a simple command, and most applications can be automatically configured to use the certificate without human intervention. This leads to significant time savings and fewer service interruptions due to expired certificates.



Common Enterprise Automation Requirements

Connector solutions, including HID PKIaaS, meet all the requirements common to most enterprise applications.

Specific Requirement	HID Global PKIaaS
Supports ACME API Version 2	All ACME connectors listed below are version 2 and support external account binding.
Public Reachable ACME Endpoint	The ACME service endpoint hosted by HID PKIaaS is publicly accessible with valid authentication credentials.
Uses ACME Generic Tooling (e.g. certbot, k8s Cert-Manager)	HID PKIaaS supports any ACME version 2-compliant tooling.
Validation via HTTP or DNS	Generic tooling is supported, though because HID PKIaaS pre-verifies any domains associated with your account, the authorization and challenge portions of the ACME protocol are bypassed by the ACME server. This allows the HID PKIaaS ACME API to be used by hosted private PKI CAs without opening any incoming firewall connections.
Short-Lived Certificates (a Few Months)	Certificate lifetimes are configurable.
Low Pricing for Basic TLS Certificates	HID PKIaaS does not utilize per-certificate pricing and will set a subscription threshold high enough to meet your needs.

Automation on Kubernetes	Cert-manager is supported. The integration closely follows the configuration found at **cert-manager.io/docs/configuration/acme.** A few specific items need to be configured, including:
	• A secret created in the cert-manager namespace with the "HAWK Key" for accessing ACM. The value provided should be Base64 encoded if loading from a YAML file
	• For kind: ClusterIssuer, under spec.acme:
	  • Email : set this to the email address of the user registered in the ACM system
	  • Server: set this to the specific policy id being referenced. For example, it would be (replace "<policy_id>" with value that HID PKIaaS Support can provide once policies are created for your account)
	  • ExternalAccountBinding.keyID: set this to the "HAWK ID" of the credential for accessing the ACM environment
	  • KeySecretRef: set this to the reference for the Base64 encoded secret created in cert-manager namespace
	• For kind: certificate
	  • Array of dnsNames to use in certificate

Choosing the Right Connector for Your Platform

The following table describes the connector we recommend for each of your enterprise platforms:

Platform	Connector	In App or Add-on	License	Notes
Microsoft Intune	Dynamic SCEP	In App	Microsoft Intune	This integration uses the native Intune Dynamic SCEP API
F5 Load Balancer	F5-AWS	Add-on	Open source, HID PKIaaS subscription	This was created specifically to demonstrate F5 automation capabilities
Windows IIS	Lego version 2.0.0+	Add-on	Open source, HID PKIaaS subscription	**https://go-acme.github.io/lego/** Utilizes HID Global-created Powershell scripts and the ACME Lego client
Apache	Certbot version 0.32.0+	Add-on	Open source, HID PKIaaS subscription	**https://certbot.eff.org/**
Nginx web servers	Certbot version 0.32.0+	Add-on	Open source, HID PKIaaS subscription	**https://certbot.eff.org/**
Tomcat/Jetty applications servers (Java Keystore)	Certbot version 0.32.0+	Add-on	Open source, HID PKIaaS subscription	**https://certbot.eff.org/** Keystore creation and automation is accomplished using provided shell scripts.
Unix / Linux	Certbot version 0.32.0+	Add-on	Open source, HID PKIaaS subscription	**https://certbot.eff.org/**
Ubuntu	Certbot version 0.32.0+	Add-on	Open source, HID PKIaaS subscription	**https://certbot.eff.org/**
Windows Auto enrollment	Autoenrollment Proxy	Add-on	Open source, HID PKIaaS subscription	Must be installed on one or more domain-joined servers
Azure	Certify the Web	Add-on	Open source, HID PKIaaS subscription	**https://certifytheweb.com/** Easily install and auto-renew SSL/TLS certificates from ACME certificate authorities for your IIS/Windows servers
AWS	Certbot version 0.32.0+	Add-on	Open source, HID PKIaaS subscription	**https://certbot.eff.org/**
OpenStack	Openshift-ACME	Add-on	Open source, HID PKIaaS subscription	**https://github.com/tnozicka/openshift-acme** Openshift-acme is ACME Controller for OpenShift and Kubernetes clusters. It will automatically provision certificates using ACME v2 protocol and manage their lifecycle including automaticn renewals.
Jetstack	Cert-manager	Add-on	Open source, HID PKIaaS subscription	**https://cert-manager.io/docs** Cert-manager is a native Kubernetes certificate management controller

Simplify PKI Management with Cloud-based Automation

HID Global provides encryption and authentication services to help companies secure computer and network devices, IoT systems and e-commerce transactions. HID Global focuses on helping companies achieve industry best practices related to authentication and encryption, while reducing operating complexity and costs. HID Global's cloud-based, PKI-as-a Service offering allows organizations to obtain authentication and encryption services on-demand, in real-time. An industry-leading fixed-price subscription model eliminates financial and operational barriers that start-ups and Fortune 500 companies alike face in creating strong security practices.

For more information about automating your PKI, visit our **solutions page**.

hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 | Latin America: +52 (55) 9171-1108
For more global phone numbers click here

2022-08-01-iams-certificate-automation-rollout-enterprise-wp-en PLT-05787
part of ASSA ABLOY