HID Account Certificate Manager

Manage the Lifecycle of Digital Certificates Across an Enterprise

SECURITY CHALLENGES

In this increasingly digital era, the number of devices and applications for network, mobile and IoT platforms continues to grow at an exponential rate. The growth has resulted in the use of Public Key Infrastructure (PKI) to secure these devices with strong authentication and robust encryption.

Keeping up with the devices' scale and agility creates a challenge for security teams. In order to tackle these challenges, organizations have increased their reliance on encryption and expanded "Encryption Everywhere" using PKI but have maintained control of "trust" by not outsourcing it as typically required by leading PKI service providers.

Organizations have complex network footprints including different networks, domain names, subdomains and websites making it impossible to track and manage TLS/SSL certificates manually through traditional methods.

HID ACCOUNT CERTIFICATE MANAGER

HID Account Certificate Manager (ACM) is designed by PKI experts to allow security administrators to eliminate manual processes for tracking, installing and renewing TLS/SSL certificates as it reduces cyber risks associated with mis-managed certificates. It supports automated certificate installation on typical enterprise network ecosystems consisting of diverse devices.

ACM automates the distribution and management of digital certificates onto devices using protocols such as ACMEv2, SCEP, EST and Microsoft auto-enrollment. It leverages core operating system components for certificate lifecycle automation, reducing the need to install and manage any agents on devices. In addition, ACM provides functionality consistent with the "four-eyes" principle of role-based access control.

ACM provides the scalability required for agile organizations by using elastic cloud services to support issuing millions of certificates with high availability. It empowers administrators with reports and information dashboards to display what matters the most. A RESTful API enables organizations to programmatically request, search, report and export certificates and management data.

KEY FEATURES

- **Certificate Lifecycle Management –** Provides digital certificate lifecycle management across the entire enterprise through a single cloud-based web portal.
- **Automation –** Allows administrators to automate certificate management through ACMEv2, SCEP, EST and Microsoft auto-enrollment protocols, eliminating resource intensive manual certificate installation.
- **One Interface for Management (Public or Private Trust Certificates) –** Provides a single pane of glass to manage all enterprise public or private trust digital certificates reducing the risk of certificate-related outages.

HID Account Certificate Manager

THE SOLUTION IS DESIGNED TO:

- Support private or public trusted device or TLS/SSL certificates – from DV, OV or EV validation
- Provide administrators ability to automate monitoring, notification, installation and renewal of digital certificates to any devices on the network such as network devices, servers, mobile devices, web servers, Windows/Mac computers
- Streamline certificate management with a self-service portal, workflow controls, user activity monitoring, standard protocol support and RESTful APIs for automation

BENEFITS INCLUDE:

- Reduction of cyber risk by tracking and managing all TLS/SSL certificates across the enterprise
- Elimination of resource-intensive manual certificate tracking and lifecycle management
- Elimination of human error by the automatic deployment and management of certificates to prevent outages
- A solution with the ability to keep up with the growing and changing nature of business that scales with your demand
- A single portal to manage the entire certificate portfolio to avoid unexpected certificate issues
- The instant enrollment, approval, issuance, revocation and renewal of all certificates
- Keeps track of digital certificates across the enterprise
- Out-of-the-box integration with enterprise tools such as ServiceNow and MDM platforms
- Support for ACMEv2, SCEP, EST and Microsoft auto-enrollment protocols for certificate management automation
- Guaranteed SLA of 99.99%

Account Certificate Manager Features	• Full certificate lifecycle management for web server, network, mobile and IoT devices • Centralized monitoring, reporting and alerting on certificate expiration • Single pane of glass for certificate inventory and management with ability to initiate request and renewal process with role-based access control • Agentless installation and management of certificates by leveraging default operating systems and application tools • Easily integrates with enterprise applications by leveraging RESTful APIs • Interactive reports and dashboards with support for data export • Multi-factor authentication for enhanced security • Support for multiple certificate policies to meet organizational requirements
Out-of-the-box Integration and Automation Support	• Microsoft auto-enrollment Proxy • Microsoft Active Directory • Mobile Device Management Platform such as VMWare Airwatch, Citrix, MobileIron, Microsoft Intune • Compatible with any ACMEv2 client such as Certbot, Lego • ServiceNow Ticketing System • Venafi Platform

COMPLETE CONTROL WITH ACCOUNT CERTIFICATE MANAGEMENT

HID Account Certificate Management (ACM) offers complete control, delegated administration, on-demand auditing and reporting. Automate and scale certificate provisioning for every system and device.

Learn more about how ACM supports PKI-as-a-Service and Enterprise SSL.

HID
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

2021-06-30-iams-hid-account-certificate-manager-ds-en PLT-04947

Part of ASSA ABLOY