ActivID® Validation Authority

Scalable, Secure and Cost Effective Digital Certificate Validation

In today's digital world, it's of utmost importance to be able to verify the identity of a person, device or a website.

A digital certificate provides a secure way to authenticate the identity of a person or computer, but it's equally critical for organizations to be able to ensure the validity of the digital certificate and regularly check for status changes and revocation.

Traditionally, the certificate validation could be done in two ways. In the first one, a trusted authority periodically publishes a signed master list of all valid or revoked certificates. The downside of this approach is that the Certificate Revocation List (CRL) often rapidly grows to an unusable size.

The second approach requires direct communications to a secured, trusted authority that can verify the validation status of each certificate. Known as traditional On-line Certificate Status Protocol (OCSP), this approach requires each validation server to be protected against both physical and network attacks. The added security risks and associated costs make this approach unacceptable for most medium and large Public Key Infrastructure (PKI) environments.

HID's ActivID Validation Authority provides a revolutionary new approach for digital certificate validation, called Distributed OCSP, to offer radically improved security at a fraction of the total cost.

KEY BENEFITS

The ActivID Validation solution, comprising the ActivID Validation Authority, the ActivID Validation Responder and the ActivID Validation Client, introduces a distributed infrastructure for certificate validation that improves upon any CRL or Traditional OCSP scheme in the following areas:

Security – ActivID Validation Responders have no private keys, so are less vulnerable to exploitation. They cannot provide false responses, even if compromised. Additionally, they use FIPS 140-2 certified cryptography.

Scalability – ActivID Validation Responders can be rapidly deployed in any number of locations and scale to meet the needs of hundreds of remote sites.

Availability – ActivID Validation Responders can be easily replicated in many locations for high availability, with excellent survivability under attack.

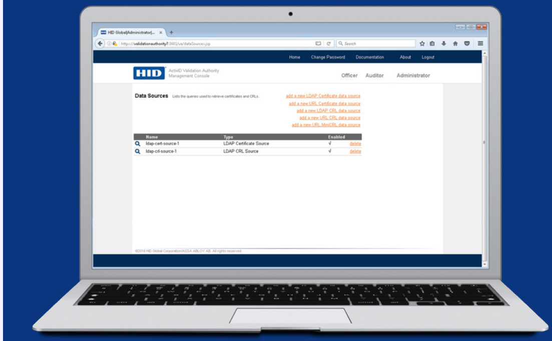
Performance – ActivID Validation Responders can be placed close to relying parties to deliver extremely low latency for OCSP responses.

Cost effective – ActivID Validation Authority licensing allows for unlimited Validation Responder deployments at a fraction of the cost of the Traditional OCSP model. In addition, there are no per-transaction costs.

Delegated validation – ActivID Validation Authority supports the Server-based Certificate Validation Protocol (SCVP), to confirm the authenticity of the issuing Certificate Authority (CA). This is especially relevant in a federated PKI comprising multiple CAs in which each party requires the ability to validate the status and authenticity of other's credentials.

Ease of management – The ActivID Validation Responders represent stateless, appliance-grade functionality, guaranteeing that only the central ActivID Validation Authority requires management.

Standards compliant – ActivID Validation Authority integrates seamlessly with existing PKI products from HID Global and other vendors, through standards, such as X.509, OCSP, SCVP, LDAP and RESTful API.


HID Global|Administrator|...
https://validationauthority7:3601/va/dataSources.jsp
Search
Home
Change Password
Documentation
About
Logout
HID
ActivID Validation Authority
Management Console
Officer
Auditor
Administrator

Data Sources Lists the queries used to retrieve certificates and CRLs.

add a new LDAP Certificate data source
add a new URL Certificate data source
add a new LDAP CRL data source
add a new URL CRL data source
add a new URL MiniCRL data source

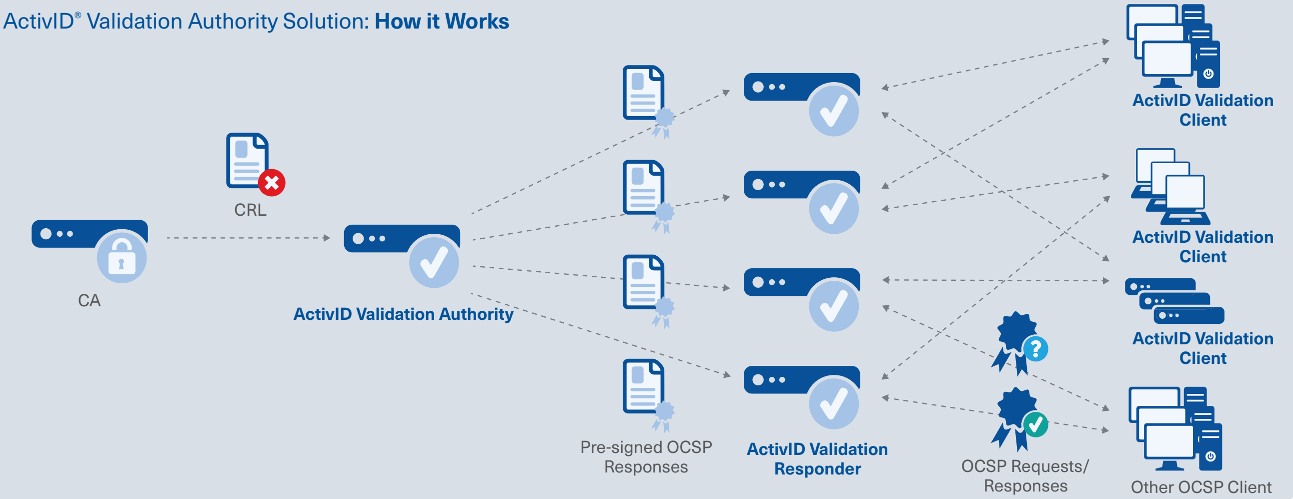
Name	Type	Enabled	
ldap-cert-source-1	LDAP Certificate Source	✓	delete
ldap-crl-source-1	LDAP CRL Source	✓	delete

©2016 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

HID'S ACTIVID VALIDATION SOLUTION INCLUDES:

- ActivID Validation Authority
- ActivID Validation Responder
- ActivID Validation Clients, that can be deployed on user desktops (ActivID Desktop Validation Client) or on servers (ActivID Server Validation Extension™)

ActivID® Validation Authority Solution: **How it Works**


CRL
CA
ActivID Validation Authority
Pre-signed OCSP Responses
ActivID Validation Responder
OCSP Requests/ Responses
ActivID Validation Client
ActivID Validation Client
ActivID Validation Client
Other OCSP Client

OPTIONAL COMPONENT

ActivID Validation Authority also offers Smart Data Bridge™ which constantly monitors data sources for certificate status updates, and pushes these changes to the ActivID Validation Authority whenever they occur.

	ActivID® Validation Authority
Platforms	Microsoft Windows Server® 2012, 2012 R2 2016 and 2019 (64-bit) Red Hat® Enterprise Linux 7.x, and v8 (64-bit)
Database	Microsoft SQL Server™ 2014, 2016, 2017, and 2019 Oracle 12c, and 19c PostgreSQL 9.x, and 12.1
Certicate Authorities	All industry standards-compliant certificate authorities
Hardware Security Modules (HSMs)	AEP KeyPer® Enterprise / Plus Thales (formerly Gemalto SafeNet) Network HSM / PCIe HSM Thales Trusted Cyber Technologies (formerly SafeNet Assured Technologies) Luna SA for Government Entrust Datacard (formerly Thales) nShield™ Connect / Connect+ / Connect XC / Solo / Solo+
Compliance and Standards	RFC 6960 (OCSP) RFC 5055 (SCVP) – support for Delegated Path Discovery (DPD) and Delegated Path Validation (DPV) FIPS 201 Certified

HID
hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800 | Latin America: +52 55 9171 1108
For more global phone numbers click here