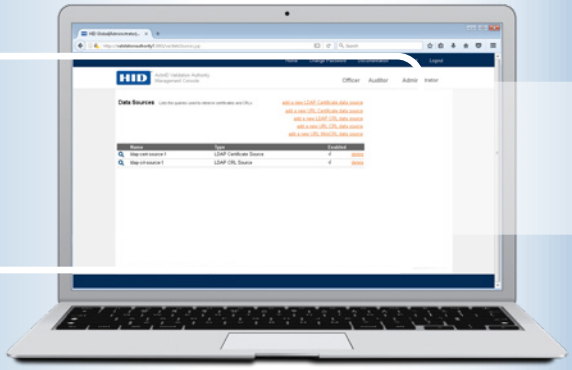
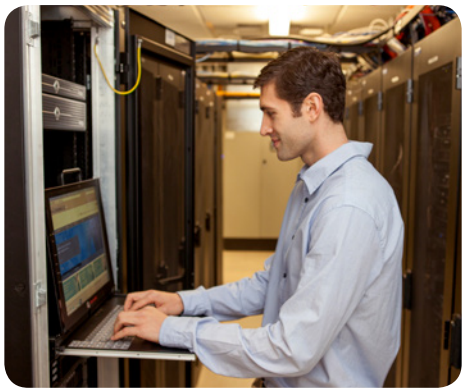
IDENTITY & ACCESS MANAGEMENT

ActivID® Validation Authority





DIGITAL CERTIFICATE VALIDATION IN A SCALABLE, SECURE AND COST EFFECTIVE MANNER

A digital certificate provides a secure way to authenticate the identity of a person or computer. Unfortunately, authentication alone does not determine whether that certificate is still valid. It's critical to check for status changes and revocation. Classically, there have been two approaches to certificate validation. In the first, a trusted authority periodically publishes a signed master list of all valid or revoked certificates. Unfortunately, this 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. This approach, known as Traditional On-line Certificate Status Protocol (OCSP), requires each validation server to be protected against both physical and network attacks. These security risks and associated costs make this approach unacceptable for most medium and large Public Key Infrastructure (PKI) environments.

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

HID GLOBAL'S ACTIVID VALIDATION SOLUTION INCLUDES:

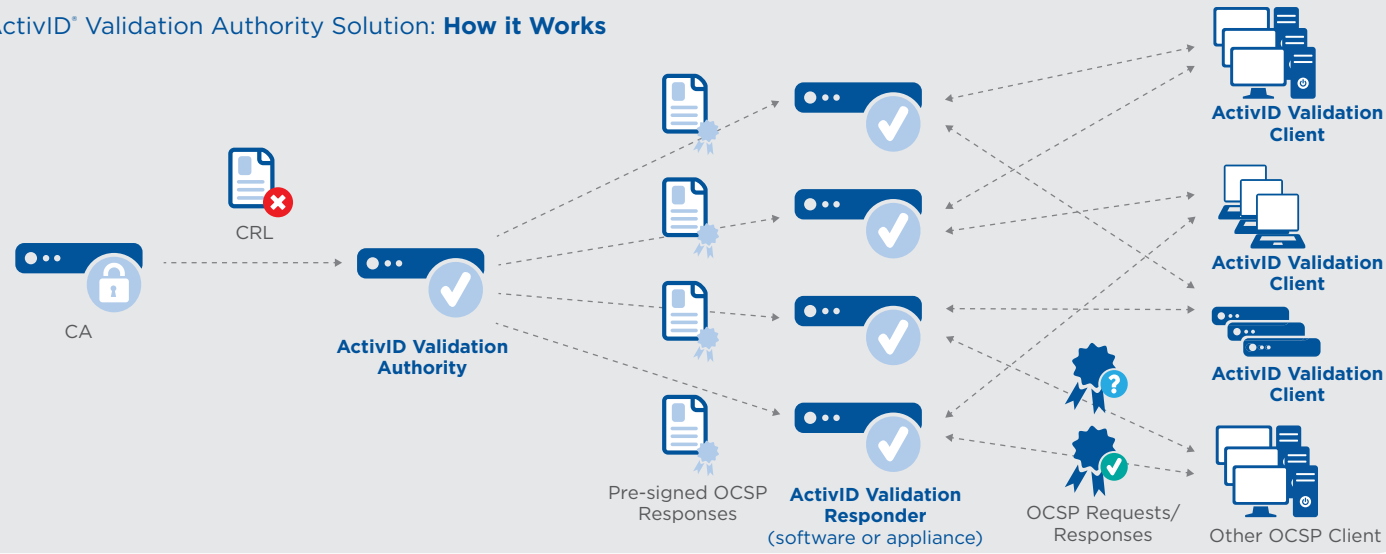
- ActivID Validation Authority
- ActivID Validation Responder
- ActivID Validation Clients, that can be deployed on user desktops (ActivID Desktop Validation Client) or on servers (ActivID Server Validation Extension™)

Key Benefits

The ActivID Validation solution 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 and LDAP.

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



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.

SPECIFICATIONS

Platforms	Microsoft Windows Server® 2012, 2012 R2 and 2016 (64-bit) Red Hat® Enterprise Linux v6.x and 7.x (64-bit)
Databases	Microsoft SQL Server™ 2014, 2016 and 2017 Oracle 12c PostgreSQL 9.x
Certificate authorities	All industry standards-compliant certificate authorities
Hardware Security Modules (HSMs)	Gemalto/SafeNet® Network HSM and PCIe HSM SafeNet Assured Technologies Luna SA for Government Thales nShield™ Connect, Connect+ and Connect XC and nShield Solo and Solo+ AEP Networks Keyper Enterprise and Keyper Plus
Standards Compliance	RFC 6960 (OCSP) RFC 5055 (SCVP) – support for Delegated Path Discovery (DPD) and Delegated Path Validation (DPV) FIPS 201 Certified

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 5081 1650

2018-11-19-activid-validation-authority-ds-en PLT-01536

An ASSA ABLOY Group brand