



Solution Brief



2012

SecurIT TrustBuilder® Certificate Validation Server for IBM Tivoli Access Manager

Solution Brief

SecurIT TrustBuilder Server

SecurIT TrustBuilder Server is a stand-alone, redundant server that provides a pluggable platform for application independent security services. The services provided by the TrustBuilder Server can best be summarized as Identity Data Services (IDS).

An IDS provides a central service point for all information required to fulfil Authentication and Authorization requests. On the one hand it acts as an AAA (Authentication, Authorization and Accounting) server, but it also behaves as a PDP (Policy Distribution Point), whereby data can be stored locally or retrieved in real time from back-end resources.

SecurIT TrustBuilder Server is a natural evolution of TrustBuilder for WebSEAL, the version running on WebSEAL and providing authentication services to IBM Tivoli Access Manager (ITAM). Whereas the WebSEAL version hooks into the CDAS interface only, TrustBuilder Server is able to work with both the CDAS and EAI interfaces provided on ITAM.

SecurIT TrustBuilder has already been applied in multiple customer projects for various purposes, such as:

- Authentication Server for OTP¹ (e.g. VASCO Digi-Pass or Radius)
- Authentication Server for eID²
- Validation Server for certificates (eID, CRL, OCSP)
- User Provisioning Server for self-registration
- Signature Validation Server
- Authorization Server for Web Services
- ...

These are but examples of how TrustBuilder can be used. The underlying architecture of the server allows for many other applications. More information on this architecture can be found in the following papers published on the SecurIT web site:

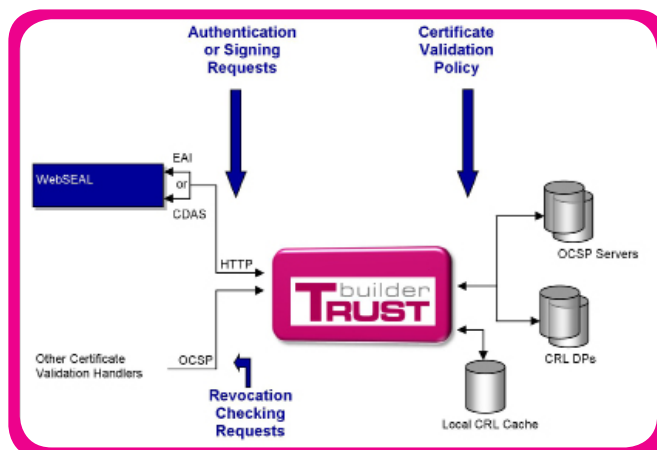
[DataSheet TAMEb TrustBuilder](#)
[Solution Brief Authentication](#)
[Solution Brief Transaction Signing and Validation](#)

SecurIT TrustBuilder Validation Server

The SecurIT TrustBuilder Validation Server is a pre-configured instance of the TrustBuilder Server. It addresses an increasing need to perform certificate validation and revocation checking in an integral way. It can receive certificate validation requests for the purpose of Authentication or Digital Signing from ITAM.

In case of authentication with an SSL certificate, the CDAS interface has to be used, whereas challenge-response type signed tokens can be handled via the EAI interface as well.

The SecurIT TrustBuilder Validation Server groups together all TrustBuilder Connectors that are required to provide a local, replicated certificate status store that



can be used by Resource Managers that require up-to-date status information on certificates.

The server provides real-time certificate validation services, such as:

- Verify the issuer's signature
- Check the certificate validity
- Retrieve attributes in a readable format
- Check the Revocation status on-line and/or with a local store
- Map the certificate attributes to a known Identity

The local store is kept up-to-date in the background by means of scheduled CRL and delta-CRL updates. This schedule is driven by an update policy that can be configured by CA or even by DP (Distribution Point).

A Validation Policy can dictate to use online OCSP validation and/or may allow for local store usage. This policy can be pre-configured, derived from content of the certificate or depend on the classification of the calling Resource Manager (e.g. applications dealing with high-value/high-risk transactions might require real-time validation of certificates).

As an example, a policy could dictate that OCSP validation by the issuing CA has to be used, but in case this service is not reachable, the local CRL store can be used if last updated successfully within a given time frame.

TrustBuilder Validation Server also provides an OCSP Server interface at the Security Services Layer, turning it into an OCSP Caching Server.

¹ OTP = One Time Password

² eID = electronic Identity Card