



Advanced Revocation Provider (ARP)



Ascertia's Advanced Revocation Provider (ARP) product provides powerful, easy to use, yet sophisticated OCSP and CRL services that enables Windows desktop applications to establish trust for digital certificates. ARP has been designed to integrate with any Microsoft CAPI-based application via a CAPI plugin, and it also exposes a simple API that allows other applications to call the ARP Enterprise Edition Server. Its advanced functionality includes optional central management using Group Policy Objects, the ability to support complex validation policies plus a detailed historical log record of all recent transactions together with an easy to use OCSP request & response viewer.

ARP Architecture

ARP is a validation plugin for Windows CAPI on both desktop and server systems. This validation provider plugin interacts with either a user environment on desktop systems (Standard Edition) or a multi-user environment on a separate centralised server (Enterprise Edition). Both products offer sophisticated OCSP and CRL based validation. Group Policy Objects (GPO) are used to create and manage validation policy settings to provide centralised management and enable policy changes to be rolled out across the enterprise. Policy settings allow the user to be informed only when trust issues arise. A sophisticated history viewer is included as standard within the product.

➔ ARP Standard Edition

Designed to be deployed on corporate desktops ARP SE uses central management settings to determine the validation policy that should be enforced for checking the status of certificates used within any CAPI application.

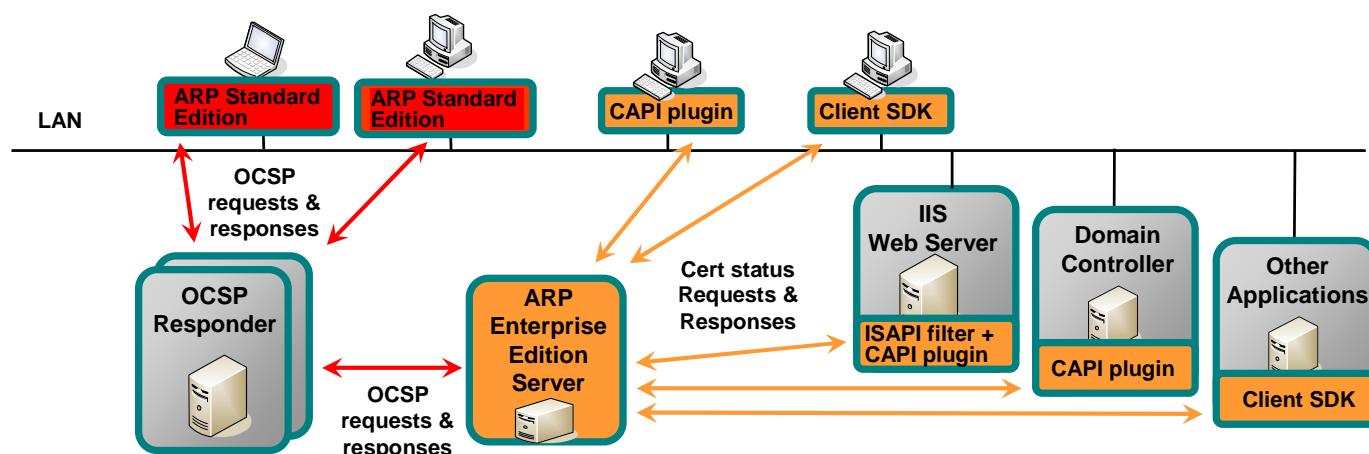
➔ ARP Enterprise Edition

With ARP EE only a very light CAPI plugin (or Client SDK) is deployed to the desktop. ARP EE is deployed on a central server. It receives certificate validation requests from multiple ARP CAPI plugins and creates OCSP requests for forwarding to an OCSP responder, or depending on policy retrieves the relevant CRL. Once the status of the certificate is established, ARP EE Server replies back to the ARP CAPI plugin.

ARP key features at a glance

- ➔ Configure validation policies using both online OCSP servers and published CRLs
- ➔ Support for central policy setting using GPO, GUI locking and silent install
- ➔ Allows an organisation to configure which applications ARP provides validation services for
- ➔ Provides a detailed transaction history viewer with a search facility and OCSP request/response viewer
- ➔ Able to use cached OCSP responses and cached CRLs using configurable cache periods
- ➔ ARP prioritises which method to use for validation, e.g. real-time OCSP, then OCSP Cache, then CRLs
- ➔ Dynamically determines the authoritative responder address using the certificate's AIA extension or using locally configured OCSP responder address(es)
- ➔ Ability to configure multiple OCSP responder and CRL Repository addresses for resilient operations
- ➔ Works behind corporate proxies and firewalls with configurable authentication

ARP Deployment Options



A Sophisticated OCSP Client Provider for Certificate Validation

Simplified Results Windows

To aid end-user understanding ARP provides simple balloon windows with the certificate validation results:



The conditions under which these windows are visible in the system tray is configurable as well as the length of time they appear on the screen. Importantly you can configure ARP to only show validation failures so that users are not shown unwanted pop-up messages.

Strong Security

ARP can be configured with the following security checks:

- ➔ Replay checks by using the optional nonce extension
- ➔ Use of OCSP over SSL
- ➔ OCSP request signing
- ➔ Ability to set clock tolerance levels
- ➔ Ability to set OCSP/CRL cache periods
- ➔ Ability to verify OCSP responder's own cert chain
- ➔ Ability to verify if CA has authorised the OCSP responder

History Viewer

ARP comes with a detailed history viewer which retains recent validation transactions - be they checked via OCSP or CRLs. Users are able to review all recent validation requests and responses using a plain English interface e.g.

- Which application checked which certificate, when, what was the result for the certificate chain
- View the validation transaction details and see the request response messages in English

Transaction Id	Target Alias	Issuer Alias	Application Name	Request Type
70	Ascertia Testing	ARP Central Bank	WINWORD.EXE	Revocation Checking
69	ARP Central Bank	Identrus Root Prep...	WINWORD.EXE	Revocation Checking
68	Ascertia Testing	ARP Central Bank	WINWORD.EXE	Revocation Checking
67	ARP Central Bank	Identrus Root Prep...	WINWORD.EXE	Revocation Checking
66	Ascertia Testing	ARP Central Bank	WINWORD.EXE	Revocation Checking
65	ARP Central Bank	Identrus Root Prep...	WINWORD.EXE	Revocation Checking
64	Ascertia Testing	ARP Central Bank	WINWORD.EXE	Revocation Checking
63	ARP Central Bank	Identrus Root Prep...	WINWORD.EXE	Revocation Checking
62	Ascertia Testing	ARP Central Bank	WINWORD.EXE	Revocation Checking
61	ARP Central Bank	Identrus Root Prep...	WINWORD.EXE	Revocation Checking

Sequence Id	Certificate Alias	Certificate Type	Revocation Type	Revocation Status
1	Ascertia Testing	End Entity	OCSP	Good
2	Central Arptest OC...	OCSP Responder	OCSP	Good
3	PTE Root OCSP Re...	OCSP Responder	OCSP	Good

Highly configurable Policy Engine

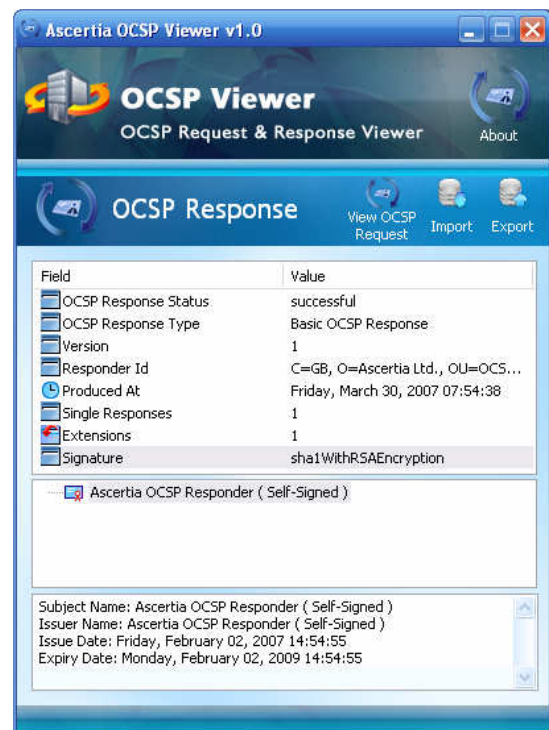
ARP can use the AIA extension and/or multiple defined addresses to find an authoritative OCSP responder. Cached OCSP responses can also be used.

Similar options are available for processing CRLs. ARP has advantages for CRL users in terms of the visual warning on the user interface, i.e. configuring ARP to pop-up only when "Not Trusted" certificates are found. In these circumstances Windows alone would provide no further details, and no record of the validation attempt!

ARP allows users to visually see issues and then review the history of prior transactions so that meaningful dialogues can be held with support desk staff to identify and correct any issues arising.

OCSP Transaction Viewer

By simply clicking on one of the above transactions within the History Viewer, an end-user can see the full OCSP request/response transaction:



Technical Summary

System Requirements:	Windows 2000 / 2003 Server Windows XP using ARP SE and multiple other environments using ARP EE
Interfaces and Protocols:	RFC 2560 (OCSP), TLS/SSL, Communication through proxy, PFX/PKCS#12 for OCSP request signing, X.509v1 and v3 certificates, X.509v1 and v2 CRLs, Indirect CRLs

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 1256 895416 US: +1 508 283 1890
40 Occam Road, Guildford, Surrey, GU2 7YG, UK
© Copyright Ascertia Limited 2009. All Rights Reserved, E&OE