



ARP-OCSP compared with OCSP toolkits

As trust solution experts we keep being asked to explain the benefits that ARP SE and ARP EE bring to an organisation rather than using cheaper or even open source OCSP programming toolkits. The answer is all about management and flexibility. Using a toolkit approach each business application that needs to understand OCSP protocols would have to be programmed (a) to use the toolkit and (b) to understand and take responsibility for all the various options that are needed for high-availability, logging, key management, effective response verification, results review and auditing. Programming toolkits typically just provide an API to the bare OCSP protocol. ARP provides the following extended trust logic and usage features:

- ❖ Simple Deployment
 - ➔ Ability to pre-configure and centrally update ARP settings using Windows Group Policy Objects
 - ➔ Simple installation process, including silent install through Active directory
 - ➔ Options include a Microsoft CAPI Revocation Provider to OCSP enable any CAPI application
 - ➔ Very high level C++ and .NET level clients APIs also exist and Java can be provided
 - ➔ Standard Edition software for desktops and Enterprise Edition software for server-side applications like Windows Domain logon, IIS other web-servers, application servers or Citrix.
- ❖ Powerful validation policy capability:
 - ➔ provides both OCSP and CRLs mechanisms, able to set the priority for these mechanisms
 - ➔ ability to use AIA or over-ride addresses for multiple OCSP responders for high availability
 - ➔ ability to use CDP or over-ride addresses and to define multiple locations for high availability
 - ➔ ability to use cached OCSP responses and/or CRLs either after failure or before query
 - ➔ provides clock tolerance features to stop small clock variations causing validation failures
 - ➔ able to validate OCSP responder certs automatically, including the CA's authority to respond
 - ➔ ability to use OCSP request signing keys within the Windows keystore
- ❖ Communications:
 - ➔ Ability to handle SSL communications with OCSP responder
 - ➔ Ability to communicate through proxies (using IE proxy settings or its own)
- ❖ Transaction logging:
 - ➔ Ability to record all validation transactions including details of the calling application
 - ➔ Ability to automatically trim logs and set debug logging levels
- ❖ Management & Usability:
 - ➔ Ability to configure which applications can invoke ARP
 - ➔ Detailed history viewer including search and filter capabilities for OCSP/CRL transactions
 - ➔ OCSP request/response transaction viewer so that messages can be reviewed in English
 - ➔ Simple pop-up messages in system tray to alert desktop users as to the certificate trust status
 - ➔ Ability to configure which pop-up alert messages are shown to user, e.g. only certs which are marked as "revoked" or "unknown" or only end-entity certs and not CA certs, etc.

All of these features are valuable differentiators for ARP. Building basic OCSP functionality into a single application might not appear too hard using a toolkit, however implementing even some of the advanced options list above is not straightforward. The complexity increases when these tools need to support multiple applications on multiple systems. The clear conclusion is that ARP offers far better value - for business continuity as well as development and operations staff.



Identity Proven, Trust Delivered