



## CRL Monitor

Automated validity checking and reporting



ascertia

Certificate Revocation Lists (CRLs) contain vital information on the revocation status of digital certificates and as such the availability of valid CRLs is essential for normal operation of trust infrastructures. CRLs also form the legal basis for checking the validity and trustworthiness of issued certificates and therefore directly impact the liability model of a PKI system.

A major problem for providers and their customers is that the availability and integrity of CRLs is in many cases simply not monitored. It is left to internal or external users to report any failures, by which time the damage has generally already occurred. Ascertia believes that it is crucial that these critical information files are regularly and automatically checked to ensure their integrity, validity, trustworthiness and freshness. A PKI provider should be able to prove compliance with their certificate practice statements, especially in case disputes arise with relying parties.

Ascertia CRL Monitor provides automated monitoring for multiple CRL issuers, it provides effective management reporting, failure alerting through email and SMS and other advanced options. CRL Monitor is an essential tool that helps prevent infrastructure failures having a very substantial downstream impact on service users.

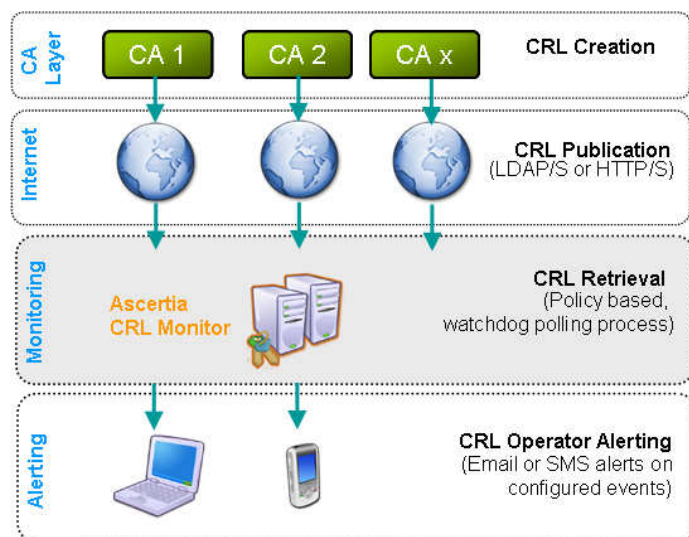
### Automated CRL monitoring

Ascertia CRL Monitor provides an automated test service that enables an administrator to easily detect CRL publishing failures or irregularities. It is a must have product for any organisation providing PKI services. With CRL Monitor, you can identify issues and fix unexpected conditions before your users report them to you!

CRL Monitor is also very useful for organisations that consume CRLs, i.e. relying party organisations. They can monitor the service and easily compare this with the Service Level Agreement (SLA). Key management reports can be produced at any time for any registered CA.

### Maximise your CRL Service uptime

CRL Monitor provides immediate real-time feedback on CRL issues as they arise. Where PKI services are used it is often assumed that they are functioning correctly and will continue to do so - this is often not the case. Use CRL Monitor to check for expected and unexpected behaviours:



### Why use CRL Monitor

- ➔ Monitor your CRLs to ensure that they are "fresh" i.e. not expired and are being updated as expected
- ➔ Check CRLs for their integrity and availability, i.e. that there is no file corruption either through a publishing failure, an operational issue or even an attack on the core trust infrastructure
- ➔ Check that the correct CA has signed production CRLs, includes support for verifying indirect CRLs
- ➔ Check CRLs from multiple issuers and URL locations at regular pre-configured intervals on a per CA basis
- ➔ Ensure high availability by using multiple monitors to ensure there is no single point of failure
- ➔ Select which members of staff receive error and summary reports by email and/or phone SMS
- ➔ Produce management reports to provide evidence of SLA performance
- ➔ Be able to download CRLs and publish them locally to avoid single point failures and reduce network bandwidth for large enterprises
- ➔ Retain a secure and searchable archive of all CRLs that were retrieved, for management information and dispute resolution purposes
- ➔ CRL Monitor is a service module within ADSS Server and is thus available on Windows and Unix systems
- ➔ CRL Monitor is an essential part of the Ascertia ADSS OCSP Server product that has been tested and certified by the US DoD JITC.  
[http://jitc.fhu.disa.mil/pki/pke\\_lab/ocsp\\_testing/details/ascertia\\_trustfinder\\_ocsp\\_5\\_0.html](http://jitc.fhu.disa.mil/pki/pke_lab/ocsp_testing/details/ascertia_trustfinder_ocsp_5_0.html)

### Perform Real-Time Tests

CRL Monitor tests the status of a CRL publishing service by downloading and checking the CRLs at pre-defined intervals. It can check that CRLs are updated as expected before their expiry date, giving service providers valuable hours in which to act to avoid trust issues. This is the only fully effective way to ensure a PKI is operating as it should.

Multiple CAs can be monitored using specific CRL polling and validation policy settings.

## Continuous Monitoring

CRL Monitor runs continuously and can operate in a high availability configuration using multiple CRL Monitor instances. When used like this if the current master CRL Monitor instance fails then the next available slave instance automatically assumes control and continues to retrieve and check the defined CRLs, ensuring that monitoring is not affected by a single point of failure.

## CRL Archiving

It is often necessary to keep an archive of all the CRLs that have been issued, either for historical digital signature verification or to resolve disputes that may arise in future.

CRL Monitor not only keeps an archived copy of each CRL it retrieves but also provides management and searching capability over the entire CRL dataset. This simply and easily allows administrators to determine within which CRL a particular certificate was first identified as revoked.

## Enterprise Architecture

CRL Monitor has been designed by security experts to provide a secure and reliable trust monitoring system:

- ➔ Report on a particular CA, or all registered CAs
- ➔ Report on a selected time period
- ➔ Produce PDF reports or in tabular form for input into a spreadsheet
- ➔ Provide detailed CRL content viewing and searching
- ➔ Provide secure operator authentication and optional dual control capability
- ➔ Maintain secure, protected transactions logs and operator activity logs
- ➔ Provide automatic database record archiving
- ➔ Provide automatic system integrity checking

## Multiple CRL resources per CA

For high availability PKI environments, CRL Monitor can be configured to use multiple CRLs distribution points (LDAP or HTTP) for each CA, allowing it to access alternate locations should the primary resource become unavailable. As an option all defined URLs can be checked and verified.

System Requirements:	Windows 2003, 2008 (32 & 64bit) Windows XP Unix (Solaris, Linux)
Databases:	SQL Server 2005, 2008 Oracle 10g, 11g, MySQL 5, PostgreSQL 8
Standards, Interfaces and Protocols:	X.509v1 and v3 certificates X.509 v1 and v2 CRLs LDAP and HTTP for CRL retrieval Support for TLS/SSL, proxy servers (including digest authentication)

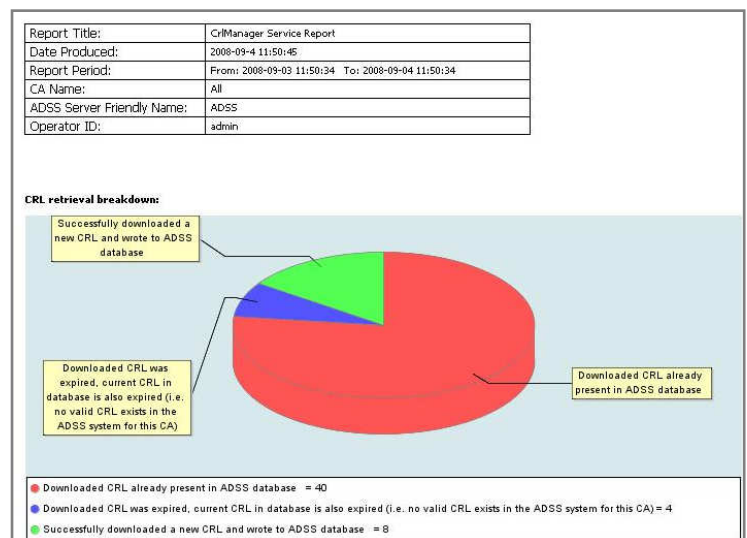
## Perform full CRL checks

CRL Monitor can be configured to generate alerts when a wide variety of events occur, including:

- ➔ The CRL has expired
- ➔ The CRL is too old for the defined freshness policy
- ➔ The CRL could not be fetched / downloaded
- ➔ The structure or format of the CRL is incorrect
- ➔ The CA signature on the CRL fails to verify or is not trusted
- ➔ The CRL was successfully downloaded, verified and written to the database

## Create Detailed Reports

CRL Monitor maintains logs on all CRL operations completed so that detailed reports can be produced for specific dates. CRL Monitor also provides CRL retrieval statistics in tabular and graphical formats.



## Additional CRL Publishing

CRL Monitor allows valid CRLs that it has downloaded to be re-published in a location where other systems and users can access them. This may be at a central location or a remote location. Used locally this enables remote systems to minimise network bandwidth and ensure maximum availability.

Network configurations of local clients (such as Ascertia's ADSS Server and ARP products) can use local CRL resources to advantage rather than accessing CRLs locations. Government systems in particular are concerned about disaster recovery and operational continuity and CRL Monitor can play an important role here.

## Easy Configuration

CRL Monitor has an advanced web-based GUI to help set-up trusted CAs and their CRL processing policies.

Ascertia Limited  
 Web: [www.ascertia.com](http://www.ascertia.com)  
 Email: [info@ascertia.com](mailto:info@ascertia.com)  
 Tel: +44 1256 895416 US: +1 508 283 1890  
 40 Occam Road, Guildford, Surrey, GU2 7YG, UK  
 © Copyright Ascertia Limited 2010. All Rights Reserved, E&OE