CRL Monitor

Automated CRL validity checking, alerting and management reporting

ADSS Server is a well-proven, standards-based product that can be deployed on premise for enterprise use or within a managed service as part of a cloud service. It can meet the most demanding needs by providing high throughput and high availability. As a strategic product for Ascertia, it offers support for the latest Windows and Linux operating systems, databases and HSMs.

Certificate Revocation List Overview

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.

Key Features

- **Active monitoring:**
  Monitor your CRLs to ensure that they are "fresh" i.e. not expired and are being updated as expected
- **Integrity Checking:**
  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.
- **Trusted Path Validation:**
  Check 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
- **Notification and Reporting:**
  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
- **Publication and Retention**
  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)

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.

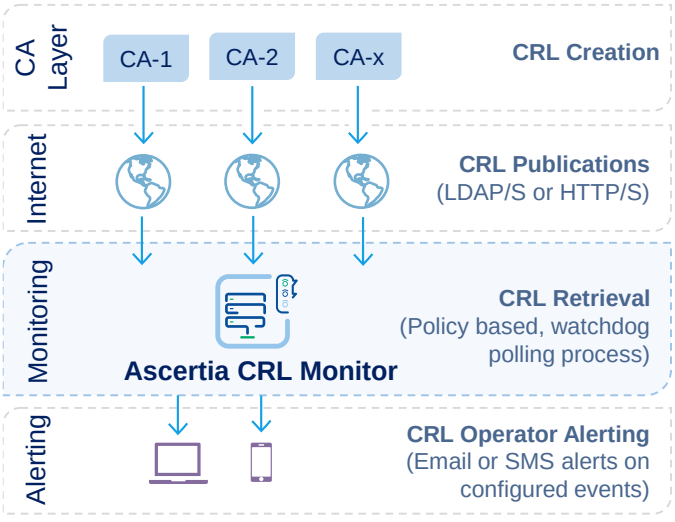
Maximise your CRL Service uptime

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:

Perform Real-time tests

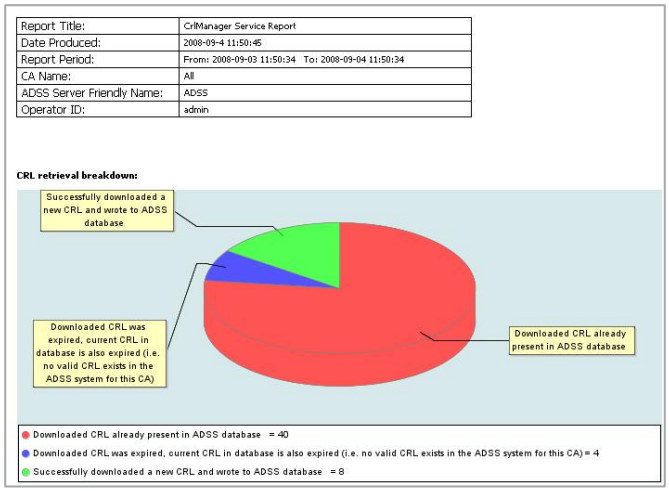
CRL Monitor tests the status of a CRL publishing service by downloading and checking the CRLs at pre-defined intervals. It can check that CRLs are updated as expected before their expiry date, giving service providers valuable hours in which to act to avoid trust issues. This is the only fully effective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

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



Create Detailed Reports

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!



Report Title:	CrlManager Service Report
Date Produced:	2008-09-4 11:50:45
Report Period:	From: 2008-09-03 11:50:34 To: 2008-09-04 11:50:34
CA Name:	All
ADSS Server Friendly Name:	ADSS
Operator ID:	admin

CRL retrieval breakdown:

CA Friendly Name	ADSS Samples Test CA (Configured Local CA)
CA CRL resource URL:	ldap://192.168.0.131:10389/cn=crl1,ou=dev,o=ascertia
First CRL number processed	2
Last CRL number processed	9
Total number of CRLs processed	6
Average CRL size (KBytes)	0.255
Average CRL Entries	2
Average time to download (seconds)	10.31
Average time to check the CRL (seconds)	0.01
Average time to insert the CRL (seconds)	0.67
ALERT SUMMARY	**Number of Alerts Seen**
Downloaded CRL has no issues and is now the current active CRL	6
Downloaded CRL has no issues but is the same as the current active CRL	24
Downloaded CRL has expired and current copy of CRL has also expired	1
Downloaded CRL has expired however the current copy of CRL is still valid	10
Downloaded CRL fails the Trust Manager CRL freshness policy for this CA	18
CRL Download failed because of communication issues	2
Downloaded CRL format is invalid	4
CRL signature fails to verify or is not trusted	8
An internal error has occurred, e.g. database connection failure, etc.	

Perform full CRL checks

Alerts are generated for a wide variety of events 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 CRL signature fails to verify or is not trusted
- The CRL was successfully downloaded, verified and written to the database

Easy Configuration

CRL Monitor has a simple web-based interface to make it easy to manage the trusted CAs and their CRL policies.

Continuous High Availability Monitoring

CRL Monitor is designed to run as a 24x7 service. A Primary and a Secondary server can operate in a high availability configuration.

CRL Archiving and Re-Publishing

CRL Monitor can be configured to keep each CRL it retrieves (if required). Administrators can use this to confirm the CRL in which a target certificate was first revoked.

After CRL Monitor has checked and accepted a CRL it can also optionally re-publish the CRL in another location. It can therefore be used to check CRLs before or after they are published.

Check all CRL resources per CA

CRL Monitor can be configured to check all defined CRL distribution points using either LDAP/S or HTTP/S protocols. This ensures that CRLs in secondary or tertiary locations are also known to be monitored and verified.

Enterprise Architecture

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

- Report on CAs for a selected time-period
- Produce PDF reports or in CSV format
- Provide detailed CRL content viewing and searching
- Provides secure transactions and operational logs
- Provide automated record archiving, system integrity checking and effective Role Based Access Controls

CRL Monitor is a comprehensive solution for actively checking the availability of Certificate Revocation Lists in complex high trust environments.

Secure web-based management is provided as standard together with advanced management configuration options and detailed reporting.

Supported Operating Systems:

Microsoft Server 2022, 2019, 201
Linux RedHat, SUSE, CentOS, Ubuntu

Supported Databases:

Microsoft SQL Server 2022, 2019, 2017
Oracle 19c, 18c
Azure SQL Database (DB-as-a-service)
PostgreSQL 14, 13, 12, 11
MySQL 8, 5
Percona-XtraDB-Cluster 5

Mike Hathaway | Chief Product Officer

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia's PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

For more info
info@ascertia.com
www.ascertia.com