Sterling B2B Integrator

Online Certificate Status Protocol (OCSP) Support

Version 5.2.2

Sterling B2B Integrator

Online Certificate Status Protocol (OCSP) Support

Version 5.2.2

Note
Before using this information and the product it supports, read the information in "Notices" on page 23.

Contents

Chapter 1. Online Certificate Status Protocol (OCSP) Support in Sterling B2B Integrator

The Online Certificate Status Protocol (OCSP) is a set of ASN.1 defined data structures for requesting and receiving information about certificate revocation status. These data structures can be sent and received by many transport protocols in principle. In practice, HTTP is used.

An OCSP client sends questions and processes responses. An OCSP responder answers questions and generates responses.

Chapter 2. OCSP Client Functionality

An OCSP client implementation consists of the following:

- Data structures for managing information about OCSP responders
- Functionality for generating OCSP requests
- Functionality for processing OCSP responses
- Functionality for transmitting OCSP requests and receiving OCSP responses

Chapter 3. How Sterling B2B Integrator Performs an OCSP Check

An OCSP check for a certificate in Sterling B2B Integrator is determined when the OCSP check within Sterling B2B Integrator is implemented as a part of internal system APIs used by services for getting certificates and keys from the database. OCSP checks are performed by Sterling B2B Integrator when methods are called to get certificates and keys from the objects that encapsulate them in the database.

About this task

The following steps describe how the OCSP check is implemented in Sterling B2B Integrator:

Procedure

1. The system checks the object that encapsulates the certificate to determine if OCSP checking is enabled. This allows the system to determine with no additional database calls whether to attempt an OCSP check.
2. If OCSP checking is enabled, the system retrieves the encoded issuer name from a certificate.
3. The system hashes the encoded issuer name with SHA1.
4. The system attempts to find an authority configured in the system that has a name whose hash matches that of the certificate. If no authority is found, no check is performed.
5. If an authority is found, the system checks the OCSP policy for the authority. If the policy permits or requires OCSP checks, see the CERT_AUTHORITY table for more information. The system attempts to find an OCSP responder for the authority.
6. If an OCSP responder is found for the authority, an OCSP check is attempted. If no OCSP responder is found for the authority, one of the following happens:
   - If the authority policy is set to always check, an exception is thrown and the check fails.
   - If the authority policy is to only check when a responder is configured, no check is performed.

Chapter 4. Database Tables

Two new database tables have been added to manage OCSP-related information:

- CERT_AUTHORITY
- OCSP_RESPONDER

CERT_AUTHORITY

The CERT_AUTHORITY table maintains information about certificate authorities.

Column	Type	Description
OBJECT_ID	VARCHAR (255)	This is a GUID that constitutes a unique ID for a record. This is the primary key. Cannot be null.
NAME	VARCHAR (255)	A name for a record. Null allowed.
CREATE_DATE	DATETIME	A create date for a record.
MODIFIED_DATE	DATETIME	The date a record was last modified.
MODIFIED_BY	VARCHAR(255)	Information about who modified a record.
ISSUER_NAME	BLOB	The RDN of the authority taken from its certificate.
HASH_ALG	VARCHAR(128)	The hash algorithm used to compute name and key hashes. Only SHA1 is supported.
RDN_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the DER encoded issuer RDN taken from the authority's certificate. This column is indexed.
KEY_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the encoded public key in the issuer's certificate
CERT_OID	VARCHAR(255)	The OBJECT_ID of the authority's certificate in the CA_CERT_INFO table. Each authority must have a CA certificate in the database. Nulls not allowed.

OCSP_POLICY	VARCHAR(128)	The OCSP policy for the authority. This consists of two comma separated values. The values describe when to use OCSP and what to check. Possible values are: **OCSP_When** • never – never use OCSP • resp – use OCSP only if a responder is configured when a request is made • always – always use OCSP when a request is made. This requires a responder to be configured and will cause certificate checking to fail if no responder is configured **OCSP_What** • none – never check any certificates • end-user- Check only end user certificates • both – check both end-user and intermediate certificates. Currently not supported • Null is not allowed in this column
CRL_POLICY	VARCHAR(128)	Currently not used.
LOCK_ID	INTEGER	Used by the system to lock rows in the table.
CREATETS	TIMESTAMP	The timestamp of record creation for a row in the table.
MODIFYTS	TIMESTAMP	The last modification time for a row in the table.
CREATEUSERID	VARCHAR(40)	The user ID that created a row in the table.
MODIFYUSERID	VARCHAR(40)	The user ID that modified a row in the table.
CREATEPROGID	VARCHAR(40)	The name of a program or object that created a row in the table.
MODIFYPROGID	VARCHAR(40)	The name of a program or object that modified a record in the table.

OCSP_RESPONDER

The OCSP_RESPONDER table maintains information about OCSP responders.

Column	Type	Description
OBJECT_ID	VARCHAR (255)	This is a GUID that constitutes a unique ID for a record. This is the primary key. Cannot be null.
NAME	VARCHAR (255)	A name for a record. Null allowed.
CREATE_DATE	DATETIME	A create date for a record.
MODIFIED_DATE	DATETIME	The date a record was last modified.
MODIFIED_BY	VARCHAR(255)	Information about who modified a record.
ISSUER_NAME	BLOB	The RDN of the authority taken from its certificate.
HASH_ALG	VARCHAR(128)	The hash algorithm used to compute name and key hashes. Only SHA1 is supported.
RDN_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the DER encoded issuer RDN taken from the authority's certificate. This column is indexed.
KEY_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the encoded public key in the issuer's certificate
CERT_OID	VARCHAR(255)	The OBJECT_ID of the authority's certificate in the CA_CERT_INFO table. Each authority must have a CA certificate in the database. Nulls not allowed.
CACHE_TTL	VARCHAR(64)	The time in seconds to allow OCSP responses to live in the internal response cache If the column is NULL, OCSP responses will only be cached for 1 second, which in practice means not at all.
TRANS_PROF_OID	VARCHAR(255)	OBJECT_ID of a profile in the GIS database. You have to create a profile for the OCSP responder that includes the correct URL for the responder.

COMM_BP	VARCHAR(255)	Name of a business process to use to communicate with the OCSP responder. This has to be a business process that does HTTP communication. Services in the business process have to be configured to not require or present HTTP headers when sending and receiving, respectively. The process HTTPClientSend that comes with the system can be used and is recommended
COMM_WAIT	VARCHAR(24)	The number of seconds to wait for communication with the OCSP responder to take place before inferring that something is wrong.
LOCK_ID	INTEGER	Used by the system to lock rows in the table.
CREATETS	TIMESTAMP	The timestamp of record creation for a row in the table.
MODIFYTS	TIMESTAMP	The last modification time for a row in the table.
CREATEUSERID	VARCHAR(40)	The user ID that created a row in the table.
MODIFYUSERID	VARCHAR(40)	The user ID that modified a row in the table.
CREATEPROGID	VARCHAR(40)	The name of a program or object that created a row in the table.
MODIFYPROGID	VARCHAR(40)	The name of a program or object that modified a record in the table.
SEND_NONCE	VARCHAR(8)	Indicates whether to send a nonce with OCSP requests. Valid values: • true • false
REQ_NONCE	VARCHAR(8)	Indicates whether to require a nonce in OCSP responses. The system only recognizes the requirement for nonces on responses if it is required to send them in requests (SEND_NONCE=true). Valid values: • true • false

RESP_CERT_IN_CA_STORE	VARCHAR(8)	Indicates whether the certificate used to verify signatures on OCSP responses is in the CA store. Valid values: • true • false - The trusted store is checked.
RESP_CERT_OID	VARCHAR(255)	The object ID of the certificate used to verify signatures on OCSP responses. This is the object ID of a record in the CA_CERT_INFO or TRUSTED_CERT_INFO table.

Chapter 5. OCSP Configuration

About this task

When configuring the system, you can create as many authorities and responders as you like.

To configure the system to use OCSP:

Procedure

1. Check the certificate for the certificate authority who issues the certificates you want to check in with OCSP into Sterling Integrator to verify it is a CA certificate.
2. List the CA certificates in the system and get the object ID for the certificate you just installed.
3. If the authority's OCSP response signing certificate is different than the authority's certificate issuing certificate, check the authority's OCSP response signing certificate into Sterling Integrator as a Trusted certificate.
4. If you checked in an additional OCSP signing certificate, list the Trusted certificates in the system and get the object ID for the certificate you just installed.
5. Go to the bin directory of the Sterling Integrator installation.
6. Start the database if necessary.
7. Start the bash or sh shell.
8. Source the file tmp.sh
9. Create an authority using the utility in the class com.sterlingcommerce.security.ocsp.SCICertAuthority.
10. Create an OCSP responder using the utility in the class com.sterlingcommerce.security.ocsp.SCIOCSPResponder
11. Update the certificates for the authority or individual certificates to enable OCSP. The utility com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo will configure all trusted and system certificates for an authority. The utility com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo will configure one system certificate. The utility com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo will configure one trusted certificate.

Chapter 6. OCSP Configuration Scripts

The following scripts run the OCSP configuration utilities. There is a Unix/Linux and Windows version of each script. The scripts take the same command-line arguments as the utility programs they invoke. The scripts are located in the bin directory of the product install. The information about the command-line arguments is repeated in this section describing the scripts.

ManageCertAuthority.sh and ManageCertAuthority.cmd

Argument	Description
-a, -l, -d, -u2	Operation to perform: • -a - add • -l - list • -d - delete • -u2 - update existing database record with newly computed key and RDN hashes The –l option takes no additional arguments. The –d option takes a single argument: the object ID of the record to delete
Name	Name of the authority. Required with -a.
Modified_by	User who modified or created the identity. Required with –a.
Hash_alg	Hash algorithm for the authority. Only the value “SHA1” is supported. Required with –a.
Certificate_id	Object ID of the CA certificate associated with the authority. Required with –a.

OCSP_policy	The OCSP policy string for the authority. This is a comma-delimited string as described in the section on the CERT_AUTHORITY table. Required with –a. For the first element of the string, the following are permitted: • never – never use OCSP • resp – use OCSP only if a responder is configured when a request is made • always – always use OCSP when a request is made. This requires a responder to be configured and will cause certificate checking to fail if no responder is configured For the second element of the string, the following are permitted: **OCSP What** • none – never check any certificates • end-user- Check only end user certificates • both – check both end-user and intermediate certificates. Currently not supported. Examples: • never,none • always,end-user
Crl_policy	CRL policy string for the authority. Required with –a. A value is required for this argument, but it is not currently used. “None” is acceptable.
Object_ID	An object ID to use when creating this record. Optional with -a. Required with -u2.

ManageOCSPResponder.sh and ManageOCSPResponder.cmd

Argument	Description
-l	Gets a list of the currently configured OCSP Responders. This option takes no additional arguments.
-d	Deletes the configured OCSP Responder with the provided object ID for responders configuration data. This option takes object_id as an additional argument.
-u2	Updates existing records in the database with the correct information about the public key of the authority certificate and the subject DN of the authority certificate. This needs to be run against all existing records for both Cert Authority and OCSP Responders, or you need to delete and recreate the records to get the proper information into the database. This option takes object_id as an additional argument.

-a	Adds configuration data for a new OCSP Responder to be used for checking the status of certificates issued by the provided authority. Additional arguments are name, modified_by, hash_alg, authority_cert_oid, response_signing_cert_oid, resp_signing_cert_in_ca_store, cache_ttl, trans_prof_oid, comm_bp, comm_wait, send_nonce, require_nonce, and object_id.
name	(Required with -a) Name of the authority.
modified_by	(Required with -a) User who modified or created the identity.
hash_alg	(Required with -a) Hash algorithm for the authority. Only the value “SHA1” is supported.
authority_cert_oid	(Required with -a) Object ID of the CA certificate associated with the authority.
response_signing_cert_oid	(Required with -a) Object ID of the certificate that the provider of the OCSP services used to sign the response providing the status for the certificates. This certificate must be added to the CA Digital Certificate store or the Trusted Digital Certificate store. This is the System Certificate ID for the certificate as it appears in the store.
resp_signing_cert_in_ca_store	(Required with -a) Flag indicating if the previous value for the response_signing_cert_oid argument is found in the CA Digital Certificate Store in Sterling B2B Integrator.
cache_ttl	(Required with -a) The time-to-live in seconds for OCSP responses in the internal cache.
trans_prof_oid	(Required with -a) The object ID of a transport configured for communicating with the OCSP responder.
comm_bp	(Required with -a) Name of a business process to use to communicate with the OCSP responder. This has to be a business process that does HTTP communication. Services in the business process have to be configured to not require or present HTTP headers when sending and receiving, respectively. The process HTTPClientSend that comes with the system can be used and is recommended.
comm_wait	(Required with -a) The number of seconds to wait for communication with the responder until inferring that an error has occurred.
send_nonce	(Required with -a) Indicates if a NONCE value will be sent to the OCSP service. The NONCE value is used to prevent replay attacks by some OCSP providers.
require_nonce	(Required with -a) Indicates if the server should require that the OCSP service provide a NONCE value in the response.
object_id	(Optional with -a) An object ID to use when creating this record.

SetSystemCertOCSPInfo.sh SetSystemCerOCSPInfo.cmd

This utility will set the OCSP information in the database for a single system certificate

Argument	Description

This utility will set the OCSP information in the database for a single system certificate

-o, -n	How to interpret the second argument: -o object_ID -n name
Object_ID/Name	Object ID or name of the authority as determined by argument 1.

SetSystemCertOCSPInfo.sh and SetTrustedCertOCSPInfo.cmd

This utility will set the OCSP information in the database for a single trusted certificate

Argument	**Description**
-o, -n	How to interpret the second argument: -o object_ID -n name
Object_ID/Name	Object ID or name of the authority as determined by argument 1.

Chapter 7. Run an OCSP Script

About this task

Use the following example to learn how to run the OCSP configuration scripts. These scripts assume that you have already checked in the CA certificates for the authority, started the database, are in the bin directory of your Sterling B2B Integrator installation and have sourced the file tmp.sh in the bin directory.

After getting the object ID of the CA certificate from the authority, in Sterling B2B Integrator from the Administration menu, select **Trading Partners > Digital Certificates-CA**. Select a certificate. The Certificate Summary dialog box appears with the certificate information, including its object ID.

Complete the following steps to run an OCSP Script:

Procedure

1. Run a command similar to the following to create an authority in the system:

   ```
   ./ManageCertAuthority.sh -a VPCA admin SHA1
   "sedna:a1807c:11dc6d53ba4:-7b4b" "always,end-user" "none"
   ```

2. After creating an authority, and creating a profile for communicating with an OCSP responder, run a command similar to the following to create an OCSP responder in the system:

   ```
   ./ManageOCSPResponder.sh -a VPCA admin SHA1
   "sedna:a1807c:11dc6d53ba4:-7b4b" "2400" "a1807c:11dc79aacbd:-7570"
    HTTPClientSend 3600
   ```

3. Run a command similar to the following to list all of the authorities in the system:

   ```
   ./ManageCertAuthority.sh -l
   ```

   Return output for each authority displays:

   ```
   CERT_AUTHORITY:
   OBJECT_ID: sedna:1ded0fd:11dc9d22929:-7fbd
   NAME: VPCA
   CREATE_DATE: 2008-11-23
   MODIFIED_DATE: 2008-11-23
   MODIFIED_BY: null
   ISSUER_NAME: Country=US, StateOrProvince=Dublin,
   OrganizationUnit=GIS Development,
   Organization=Sterling,
   CommonName=Test CA
   HASH_ALG: SHA1
   RDN_HASH: 24E63F8AE9F51497529EA0CC34467A4680737A9F
   ENCODED_RDN_HASH: JOY/iun1FJdSnqDMNEZ6RoBzep8=
   KEY_HASH: C96F2FF442EBFA07672DCEC49B729D4D24898313
   ENCODED_KEY_HASH: yW8v9ELr+gdnLc7Em3KdTSSJgxM=
   CERT_OID: sedna:a1807c:11dc6d53ba4:-7b4b
   OCSP_WHEN_POLICY: always
   OCSP_WHAT_POLICY: end-user
   CRL_POLICY: null
   ```

4. Use a command similar to the following to enable OCSP for all trusted and system certificates issued by the authority:

   ```
   ./SetAuthorityCertsOCSPInfo.sh -o
   "sedna:1ded0fd:11dc9d22929:-7fbd" yes
   ```

Chapter 8. OCSP Check Logic

About this task

The following steps describe the logic of OCSP checking in Sterling B2B Integrator:

If the certificate status is ok, the OCSP check succeeds. Otherwise, it fails.

Procedure

1. If an existing response whose time-to-live has not expired is found, than that response is used as the OCSP response.
2. If no existing response is found in the cache or the time-to-live has expired for a response in the cache, an OCSP request is created.
3. If the system creates an OCSP request, it launches the business process configured for the OCSP responder to send the request and get the response. Requests will include a nonce value if the responder was configured to have one sent.
4. If the business process completes successfully, the system attempts to parse its primary document as an OCSP response. The business process used to send OCSP requests and receive OCSP responses strips the HTTP headers from the response.
5. If the primary document can be parsed as an OCSP response, the system checks the status of the response.
6. If the response status indicates that the request generated a valid response, the system attempts to verify the signature on the OCSP response using the certificate configured for the OCSP responder.
7. If the signature is verified and the responder was configured to require nonce, the system attempts to get and check the nonce from the response.
8. If all other verifications passed, then the system looks for certificate status information for the certificate for which the request was constructed and sent.
9. If the status information is found, then the system updates the internal cache for an existing OCSP response for the certificate.

Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2011. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2011.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Product Number:

Printed in USA