Security Certificate Exchange (SCX)

Odette Recommendation – Version 1.0

Security Certificate Exchange (SCX) – Recommendation

	Executive Summary

Problem Statement

The use of Security Certificates has become an important part of data exchange in the automotive industry. They are used to provide proof of identity of the partners, allow encryption/ decryption/integrity-check of files and ensure non-repudiation of the data exchange.
However, the large number of Security Certificate providers has made it increasingly difficult to properly manage the exchange, validation and installation of these certificates.

The SCX project team has analysed the business requirements and technical opportunities and developed a recommendation to establish trust between the business partners and enable the automated exchange and renewal of Security Certificates.

Technical Solution

The technical basis for the recommendation is a Trust Service Status List (TSL). Such a list contains details of Security Certificate providers (aka Certificate Authorities, CA) and their status. For the automotive industry, a positive identification is recommended, i.e. the list contains the trustable CAs. The list is being published and updated on the internet and can be easily accessed by enabled software systems. To ensure the integrity of the TSL the list has to be signed with a digital signature of the institution creating and maintaining the TSL.

Business partners receiving Certificate information from other partners may now automatically check the trustability of the issuing CA.

All recommended parts of the trust system are based on international standards (namely ISO – International Standardisation Organisation, ETSI – European Telecommunication Standards Institution, RFC -Internet and ITU - International Telecommunication Union standards)

Organisational Solution

1. According to the various security levels that different business processes may require there can be several trust lists, each of them containing details of the issuing CAs complying with the security level's policy requirements.
   So far, two levels are identified:
   a. Basic – The issuing CA is an authenticated business entity and operates a PKI.
   b. OFTP2 – The issuing CA is listed in the Basic TSL (i.e. fulfils the basic requirements) and additionally complies with the OFTP2 Security Certificate Policy requirements.

2. The industry partners participating in the project (OEM, supplier, solution provider) consider it crucial that the TSL and the related service are provided by a neutral body. They recommend Odette to be this trust guardian and to provide the service to the automotive industry community.

3. For operational and administrative purposes it is recommended to establish two bodies:
   a. SCX Administration – the body which is responsible for running and maintaining the service. The Odette central office should fulfill this role.
   b. SCX Committee – the body which deals with exception situations. Especially in the situation where a CA is found to be no longer compliant with the security level, the SCXC shall take decisions on necessary corrective actions on behalf of the automotive community. The committee shall consist mainly of representatives of OEMs and suppliers.

4. The service is provided on an open basis. Every interested CA can apply to be listed on Odette TSLs. Odette will do the necessary validation of the existence of the CA. The compliance to the so far defined security levels will be verified by self-assessment of the applying CA.

5. The establishment and maintenance is provided as a service for the membership of Odette and the whole automotive community. However, Odette will not take over legal responsibilities.

Conclusion

With the provision of the trust service Odette strengthens its position as an Organisation of the automotive industry for the automotive industry.

Acting as a trust guardian Odette provides an essential service to the business partners in the automotive industry. This service is in line with Odette's mission as 'business enabler' for electronic data exchange in the European automotive industry.

The recommendation enables especially the large scale implementation and use of the OFTP2 file transfer protocol for secure data transfer over the Internet.

Security Certificate Exchange (SCX) – Recommendation

Table of Contents

I. Introduction

1) Objective

Secure data exchanges with business partners, using OFTP2 and other B2B tools, rely heavily on the use of Security Certificates which can provide proof of identity of the partners, allow encryption, support integrity-check of files and ensure non-repudiation of the data exchange.

The massive rise in the day to day use of B2B processes and the number of exchanges of confidential and critical data between partners in the automotive industry coupled with an unknown number of Security Certificate providers has made it increasingly difficult to properly manage the exchange, installation and checking of these certificates.

Odette has therefore decided to recommend a standardised solution for security certificates exchange between Odette member companies.
The recommendation is aimed at PKI application users in the European automotive industry and the providers of their security certificates.
Use outside the EU and in other industry sectors is also possible and is encouraged.

The design goals of this recommendation were:

- use self-regulation within Odette member companies to replace expensive and time consuming processes
- enable an automatic trust decision and ensure a specified security level without security know how on end user level
- enable an automatic and quick security certificate exchange by defining an exchange channel
- minimize manual processes (e.g. checking policies should be only done once for all members)
- base the solution on existing standards
- minimize barriers to implementing the solution (e.g. for small partners)

2) Scope of this Document

This document is a recommendation for certificate exchange which defines

- processes, interfaces and protocols for certificate exchange / trust / verification,
- processes to achieve accepted minimum security level(s) and
- requirements for the setup and operation of a trust service (to be provided by Odette).

The following aspects are not yet defined:

- processes for end user or machine certificate exchange.
- requirements for the setup and operation of a certificate/CRL proxy for user/machine certificates by Odette.

These aspects may be covered in a subsequent version of the recommendation.

Out of scope of this recommendation is the specification of application specific requirements (e.g. specific certificate policies for OFTP2).

This recommendation does not cover issues related to signing documents from a legal or financial point of view. i.e. legal non-repudiation requirements (e.g. with qualified signature in contracts) are not covered.

3) References

- OFTP2 RFC 5024
- Odette S2R Recommendation
- ETSI TS 102 231: Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider status information
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- PKCS #7: Cryptographic Message Syntax - Version 1.5

4) Definitions / Abbreviations

Confidentiality	Information is only available to authorized persons.
Availability	Data / IT systems are accessible and usable in the manner agreed upon with the service provider (dependable, fail-safe)
Integrity	Information is unaltered (correct), exact and complete. It is not changed, deleted or destroyed without intention or proper justification.
Non-Repudiation	Non-repudiation is the concept of ensuring that content cannot later be denied by either of parties' involved (content commitment). There is also a legal definition of this term, giving legal right after signing a message with non-repudiation. In this document only the technical aspect is used.
Encryption	Encryption denotes the usage of a cryptographic algorithm to protect information confidentiality.
(Digital) signature	(Digital) signature denotes the usage of a cryptographic function to protect the integrity of data. In this context integrity refers to the content of the data. In addition, the integrity of the data origin can also be protected (non-repudiation).
Public Key Cryptography	Public Key Cryptography denotes functions with which every user possesses a so-called key pair composed of a Public Key and Private Key. With the usage of the freely accessible public key, data can be encrypted for a user and its signatures can be validated. Only with the user's private key the decryption process or signature creation can be performed.
(Security) Certificates	Certificates are the public keys of the users signed by a reliable authority (the certificate authority CA). Certificates prevent faking a public key within Public Key Cryptography. Certificates issued for a natural person are called Personal Certificates, in contrast to machine or group certificates. They are based on X.509.
CA Certificate	A certificate of a certificate authority. The CA Certificate is needed to check a security certificate that has been issued by this certificate authority.
Root Certificate	A CA certificate is called root certificate when this certificate has not been issued by another CA and therefore is self signed. A root certificate represents the trust root of a whole PKI.
Public Key Infrastructure (PKI)	Public Key Infrastructure (PKI) denotes the infrastructure used to issue, distribute and validate certificates as well as any associated processes.
Certificate Authority (CA)	An authority issuing certificates (see also Security Certificates).
Certificate / CRL Proxy	A certificate / CRL proxy is a store and forward service used to connect to separate (company) directories (e.g. LDAP) via one interface.
OFTP2	Odette File Transfer Protocol Version 2
OID	Object identifier according to ISO/IEC 9834 series.
OSCAR	Odette System of Coding and Registration, a unique code assigned to business entities
SCX	Security Certificate Exchange
S2R	Security and Risk Reduction
TSL	Trust Service Status Lists
SCXC	Security Certificate Exchange Committee
SCXA	Security Certificate Exchange Administration
URL	Uniform Resource Locator

II. Trust Model

1) Principles

The trust model will be based on Trust Service Status Lists (TSL) and a governing trust agency.

A TSL is an arbitrary list of CA certificates that conform to the policy of this list. A TSL is cryptographically secured by a signature of the trust agency. Multiple lists for different application specific security policies are possible. The TSLs vary in provided security level and the list joining process.

The trust agency is responsible for maintaining the lists and for publishing them. In this recommendation, the role of the trust agency is fulfilled by Odette as a non-profit activity..

The user can download the TSLs from the Odette web server. Based on the registered CAs in a TSL trust decisions can be automated. Since the setup of trust has been done centrally by Odette and the TSLs themselves are signed with a certificate, the system will also reduce the effort required for each participant to trust another PKI. Also, by maintaining a defined standard of evaluation and acceptance of CAs it is possible to reduce security risks that can be caused by negligence in an environment, where all the trusts have to be set up individually.

2) TSL Format

The TSL contains a list of trusted CA certificates that can be used to verify the end certificates to be trusted. If the CA is not a root CA, then all CA certificates in the PKI hierarchy above the trusted CA are also included in the TSL. The trusted issuing CA of each CA hierarchy is always listed before the other CAs which are lower in the hierarchy.

The TSL-format is defined in the ETSI standard TS 102 231. The detailed implementation is described in the “SCX - Implementation Guidelines” which is annexed to this Recommendation.

3) TSL Types

For each specific application and required security level, a separate TSL policy and related TSL can be generated.

There is only one predefined TSL, called TSL Basic. All other TSLs are derived from the TSL Basic and contain a subset of its trusted CA certificates.

Specific TSLs will be named with the naming schema “TSL_[name].TSL”, where [name] identifies the recommended usage of the TSL, e.g. a specific application such as “OFTP2” or a specific security level such as “qualified signature”.

A unique OID for each TSL-Type will be created.

OID Schema:

OID 1.3.177 = Odette OID branch

OID 1.3.177.509 = Odette PKI branch

OID 1.3.177.509.1 = TSL Branch
OID 1.3.177.509.1.A.B.C.D = full TSL Identifier

Where A: TSL-Policy branch: 0=TSL Basic, x=1..n : [application x]
B: Class branch = 0; reserved for future use

C: Major version (policy requirement change)
D: Minor version (non policy requirement change, e.g. bug fix)

The existing reserved policy branches (including position A, B) are listed in the Annexe "SCX- TSL Applications".

4) TSL Policy

The policy of each TSL must be described in a related policy document with the same name as the TSL in the following naming schema "POL_[name].TXT". The document format is ASCII (ISO-8859-1, Latin 1).

The TSL policy has mandatory elements and can be extended with additional elements. Mandatory elements of a policy are:

- Certificate Usage: Describes what certificates can be used for that are issued by CAs registered on this TSL.
- Certificate Requirements: Minimum requirements of certificates issued by CAs to be registered on the TSL
- CA Requirements: Minimum requirements for the CAs to be registered on the TSL
- Legal binding statement of TSL: Defining the legal binding of the TSL itself.
- Subscribing process: Process used to audit or verify CAs subscribing to the TSL. Detail processes:
  - Policy compliance
  - Authentication
  - Authorisation
- Security Trust Level Description: Describes the level of trust that a CA and it's certificates can earn after being registered on this list.

Unless otherwise stated, any TSL provided by Odette is provided without any liability, especially regarding correctness and availability.

To avoid organisational overhead it is recommended to use self-commitments instead of auditing policy constraints. In case of malpractice of any CA on a TSL, a process of revocation will be initiated.

TSL Basic contains all the certificates of CAs registered at the SCX service. The policy of TSL Basic (POL_Basic.TXT) is:

- Certificate Usage: no stipulation, no usage restrictions
- Certificate Requirements: no stipulation, no requirements
- CA Requirements: no stipulation, no requirements
- Legal binding statement of TSL: no legal binding
- Subscribing process:
  - Policy compliance: none
  - Authentication: SCXA determines CA owners identity by organisational documentation issued by or filed with the applicable government agency or any other competent authority that can confirm the identity (e.g. registration in Odette OSCAR system).

  - Authorisation: SCXA requests signed self-commitment of subscriber to be authorised to register the CA
- Security Trust Level Description: For all CAs on TSL Basic an identity check for the CA owner has been performed. No checks of CA infrastructure performed, no statement of IT-security level of CA operation is possible. Authorisation checking for CA owner is done by self-commitment.

5) TSL Authenticity and Integrity

The TSLs are signed with a signing certificate of Odette. Odette will publish the certificates (multiple for backup reasons) to be used for signing TSLs in a list under the name “TSL_signing.P7B” (see RFC 2315).

Before using the signing certificate to verify the authenticity and integrity of TSLs the signing certificates have to be validated.

Odette will use commercial certificate service providers to obtain TSL signing. As a backup measure, the TSL_signing.P7B contains additional certificates that will be used in an emergency situation (e.g. revocation of the primary signing certificate). Any valid certificate in the TSL signing certificate list could be used by Odette to sign lists.

III. Service Description

1) Organisation

a) Service Governance Model

The following roles are defined for the governance of the security certificate exchange service

Role	Abbreviation	Function	Assigned by
Security Certificate Exchange Committee	SCXC	Management of security certificate exchange service, handling of feature requests, handling of complaints, decision on removing participants from the list, which do not longer comply with the policy rules. .	Assigned and mandated by the Odette Technology Committee.
Security Certificate Exchange Administration	SCXA	Technical execution of SCX service complying with SCXC process descriptions and SCXC single decisions.	Assigned and mandated by the Odette Central Office.

b) Contact points

SCXC, SCXA contact points are published at www.odette.org/TSL/contacts.html

2) TSL Distribution

TSLs will be published on the Odette web server with the URL www.odette.org/TSL/ (prefix URL) followed by the TSL name, e.g. for the basic TSL the URL will be www.odette.org/TSL/TSL_Basic.XML.

Policies and TSL signing certificates will also be published under the same prefix URL, e.g. www.odette.org/TSL/POL_Basic.TXT and www.odette.org/TSL/TSL_signing.P7B

Each TSL contains a validity period. Before the end of the validity period a new TSL with extended validity period will be published under the same URL. A TSL can be used offline only during the stated validity period. If two valid TSLs are available the latest published TSL should be used.

The validity period for a TSL is defined to be 90 days. 30 days before the end of the validity period a new TSL is published by default, so that there is a 30 day overlapping period. The publication of a follow up TSL can be brought forward, e.g. for publication of important changes such as removing a revoked CA.

To support easy update checking for brought forward TSL publications, an update information file TSL_[name].UPD will also be published. This file is an ASCII text file containing the latest publication update time in the format “ccyy-mm-ddThh:mm:ssZ” (e.g. “2008-09-15T14:20:30Z”) as a string in the first line.

To avoid a denial of service of the Odette web server, mass downloading directly after planned publication (30 days before end of validity period) or after publication of a new update information, is not allowed. The download has to be scheduled at a random time within a 24 hour time window after publication time. If the download fails, the rescheduling has again to be at a random time in a 24 hour time window. If download is not possible after 5 attempts because of service unavailability, then Odette should be contacted for advice.

All published TSLs are archived by SCXA.

3) Service Availability

The service is offered at the best effort of Odette. No specific service availability level is guaranteed.

4) Creation of new List Type

Any Odette member can request the creation of a new list type. The request to SCXC must contain the following information:

- Proposed name of the list
- Use case of the list
- Policy of the list

The SCXC will circulate the request to an appropriate recipient list (e.g. Odette Members or Odette Workgroup) with a due date for comments. After the due date the SCXC decides about creation of the requested list type on basis of feedback. SCXC will then reserve a unique OID for the new list type.

5) List Type Modification

Any Odette member can request a list type modification. Only use case and policy can be changed, name and OID (except version) are fixed. A list type modification could affect the members of a TSL, e.g. if a policy is tightened.

There will be a request for comments process analogous to that in the creation of a new list type.

SCXC decides if the list type modification requires:

a) Replacing the old list by a new list with the same name, but with a different use case and/or policy.

or

b) Creating a new list with a new name parallel to the old list.

Alternative a) will apply for minor changes or fixes, alternative b) will apply when use case and/or policy has major deviations.

For alternative b) an overlapping phase can be defined, after which the old list will be discontinued.

6) Termination of a List Type

Any Odette member or the SCXC itself can request a list type termination. There will be a request for comments process analogous to that in the creation of a new list type.

The SCXC decides about termination of a list type.

7) List Administration Process

a) Subscribing

An application to subscribe can be made by any authorised person of any company for self operated CAs or for CAs operated on their behalf. Applications must be sent to SCXA.

The application must contain:

- CA certificate
- CA owner: company name, address
- Administrative contact person of CA: name, address, e-mail, FAX and telephone number
- All higher certificates in the hierarchy, if CA is not a root CA
- Names of TSL(s), to which subscription is requested

SCXA performs the following processing:

- Check authorisation of the person applying to subscribe
- Carry out the subscribing procedure for TSL_Basic, if CA is not included in TSL_Basic. This does not apply to subscriptions for TSL_TEST.
- Do necessary additional policy checks of TSL [name]
- If the subscribing procedure completes successfully, an update of the TSL(s) will be published

b) Unsubscribing

An application to unsubscribe can be done by the administrative contact persons of registered CAs. Applications must be sent to SCXA.

The application must contain:

- CA certificate
- Name of TSL(s), from which unsubscription is requested

SCXA performs the following processing:

- Check authorisation of the person applying to unsubscribe
- Verify authenticity of the unsubscribe request
- If the unsubscribing procedure completes successfully, an update of the TSL(s) will be published

c) Revocation

If an Odette member has concerns about malpractice of a CA on a TSL, e.g. not complying to the given TSL policy, a revocation request can be sent to SCXC.

SCXC verifies the request (according to the TSL policy) and asks the CA owner to conform to the policy. If the malpractice is not stopped after a SCXC given due date, SCXA will remove the CA from the TSL.

IV. TSL Usage for PKI enabled Software Products

When using TSLs in PKI enabled software products, the following rules must be followed:

- The policy must be checked that it fits to the planned usage.
- The OID of the TSL must be checked for validity for this use case.
- Download regulations (e.g. time frames and random time windows) must be followed. Use update descriptor file to avoid unnecessary downloads.
- The TSL must be checked for integrity with the given signature and the given signing certificate.
- The validity period of the TSL must be checked.
- The validity of the signing certificate must be verified, including a CRL check if it is an online-application.

V. Annexe

1) Version History

Edition	Author	Modification Description	Release Date
Version 1.0	SCX Project Team		16.01.2009

2) Contact

Odette International Limited
Forbes House
Halkin Street
London
SW1X 7DS
UK

Tel: +44 207 344 9227
Fax: +44 207 235 7112
E-mail: info@odette.org

3) Annexe Documents

SCX - Implementation Guideline
SCX -TSL Applications