SHS Version 1.2 CA

The Swedish Agency for Public Management oct 2003

This version:
http://www.statskontoret.se/shs/pdf/1.2ca.pdf

Latest version:
http://www.statskontoret.se/shs/pdf/shs-ca.pdf

Previous versions:
http://www.statskontoret.se/shs/pdf/1-1ca.pdf
http://www.statskontoret.se/shs/pdf/1-0ca.pdf

Editors:
Björn Scharin, Anders Lindgren, Jan Lundh, Christer Marklund

Content

Figures

1 Introduction

This document is a technical overview of certificate aspects in the SHS concepts. It describes how and where certificates are used and specifies the certificate format.

1.1 Audience

This document is intended for technical SHS administrators, developers and architects that need an overview of how SHS make use of cryptographic methods for authentication, signing and encryption.

1.2 Document history

Version	Date	Change	By	Approved
1.0.1	2003-01-21	First draft based on SHS 1.0 Documentation CA and the English draft document SHS CA version 1.05 from Björn Scharin.	Björn Scharin/ Anders Lindgren	
1.0.2	2003-01-28	Updated draft Document structure	Anders Lindgren	
1.0.3	2003-01-31	Update based on review comments	Anders Lindgren	
1.1	2003-02-06			Christer Marklund
1.2	2003-10-09	Updated for SHS 1.2	Anders Lindgren	Jan Lundh

2 Certificates

Two main certificate categories are used in SHS systems

- Server certificates issued to SHS servers connected business systems and web servers communicating with SHS servers for authentication of the actual server systems and session encryption (SSL).
- In addition the connected business applications use certificates issued to users, groups and organisations for document signing and SHS message encryption.

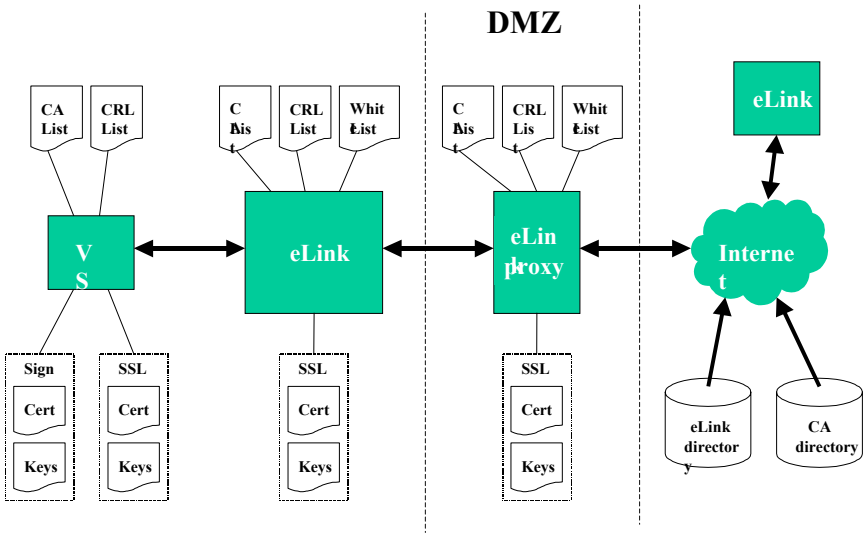

Figure 1 Certificate usage overview

2.1 Server certificate

The server certificates adhere to common Internet praxis and de-facto standard for WWW-server certificates and identifies a specific server such as www.rsv.se.

The use of server certificate within the SHS scope is both the authentication (to prove the servers identity) and encryption (to protect the actual data messages transferred over Internet).

2.2 SHS specific certificates

SHS certificates shall be used by SHS nodes, connected business systems and when web servers are communicating with SHS servers. The SHS certificate shall adhere to general de facto standards in order to minimize the specific requirements on certificate formats and practices.

The SHS certificates shall be based on RFC3280[1].

The following attributes are mandatory for SHS certificates:

certificateSerialNumber
issuerName
- countryName
- organizationName
- commonName

startDate
expireDate
subjectName
- countryName
- organizationName - Organisational number and optionally department identifier
- commonName - server or application name

[1] RFC3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

3 SHS Requirements on Certificate Authorities

This section describes the basic requirements on Certificate Authorities that provide SHS certificates. The exact security requirements are not governed by SHS but rather the owners of connected business applications.

3.1 Certificate distribution and key generation

Both local and CA based key generation should be supported. Therefore SHS certificates should allow distribution in one of the following ways:

- PKCS#10 - certification request syntax (local key generation)
- PKCS#12 – Personal information exchange syntax (certificate, keys, secrets etc when keys generated by the CA).

3.2 Revocation of SHS certificates

Maximum update interval for CRL's is 12 hours. Actors (owners of connected business applications) may have demands for shorter intervals.

3.3 Cross certification

Cross certification is currently not used. The application servers must be capable of handling more than one trusted root server. Organisations that use SHS must define which certificate authorities it trusts.

3.4 Access Control

SHS servers support access control based on certificate information. This access control allows the SHS node to check incoming sessions against a list of trusted server certificate identities. This functionality is known as "white lists" and may be compared to the techniques used by financial institutions that only allows specific certificate holders (normally the certificates issued by the institute) to access the system.

Certificate serial numbers should be used to support the white list requirement of uniquely identifiable certificates.

4 Detailed Certificate Description

This section describes certificate formats in detail.

4.1 Web server certificate format

Web server certificates are used for authentication and session encryption (SSL). These are de facto standard certificates from trusted CA providers. Used by all types of servers (SHS, business application and proxies)

4.1.1 Certificate fields

Field	Mandatory/ Optional	ASN.1 Type	Comments
Version	M		=2 (X.509 v.3)
SerialNumber	M		
Signature	M		- sha-1WithRSAEncryption - optionally md5WithRSAEncryption
Issuer	M	utf8String	Attributes: - *countryName* according to ISO 3166-1 A2, (ex. =SE) - *OrganizationName* (Official name according to national company registry.) - *OrganisationalUnit* (Optional) - *SerialNumber* (ex. Official organisation number or DUNS number) - *CommonName* (shall include name of CA and name of certificate policy) (ex. ”<OrganisationName> <policy name>”) *OrganizationName* and *serialNumber* = unique identifier
Validity	M	UTCTime	notBefore and notAfter

Subject	M	utf8String	Attributes: - *CountryName* (Country code, ex. SE) - *OrganizationName* - *OrganizationalUnitName (optional)* - *SerialNumber* - *Location (optional)* - *email address (optional)* - CommonName (DNS host name)
subjectPublicKeyInfo	M		
issuerUniqueIdentifier	---		
subjectUniqueIdentifier	---		

4.1.2 Standard-extensions

Field	Critical	Mandatory/ Optional	ASN.1 type	Comments
authorityKeyIdentifier	non-critical	M		SHA-1 (hash of CA public key)
subjectKeyIdentifier	non-critical	M		SHA-1 (hash of subject public key)
keyUsage	critical	M		Permitted usage: -KeyEncipherment -DigitalSignature
privateKeyUsagePeriod		---		
certificatePolicies	non-critical	M		
policyMappings		---		
subjectAltName	non-critical	O		
issuerAltName		---		
subjectDirectoryAttributes	Non-critical	O		
basicConstraints	Non-critical	O		
nameConstraints		---		

policyConstraints		---		
cRLDistributionPoints	Non-critical	M		
extKeyUsage	Non-critical	O		

4.1.3 Private extensions

Field	Critical	Mandatory/ Optional	Comments
AuthorityInfoAccess	Non-critical	O	If OCSP are used
biometricInfo	non-critical	O	
qcStatements	non-critical	O	
cardNumber	non-critical	O	

4.2 SHS Signature and encryption certificate format for applications

This section describes certificate characteristics of certificates used by SHS connected applications for message encryption (end-to-end) and signing.

Note! *The key usage extension support is unclear and needs further investigation.*

4.2.1 Certificate fields

Field	Mandatory/ Optional	ASN.1 Type	Comments
Version	M		=2 (X.509 v.3)
SerialNumber	M		
Signature	M		- sha-1WithRSAEncryption
Issuer	M	utf8String	Attributes: - *countryName* according to ISO 3166-1 A2, (ex. =SE) - *OrganizationName* (Official name according to national company registry.)

			- *OrganisationalUnit* (Optional) - *SerialNumber* (ex. Official organisation number or DUNS number) - *CommonName* (shall include name of CA and name of certificate policy) (e.g. "<OrganisationName> <policy name>") *OrganizationName* and *serialNumber* = unique identifier
Validity	M	UTCTime	notBefore and notAfter
Subject	M	utf8String	Attributes: - *CountryName* (Country code, ex. SE) - *OrganizationName* - *OrganizationalUnit (optional)* - *SerialNumber (optional)* - *Location (optional)* - *email address (optional)* - CommonName (Application or server name)
subjectPublicKeyInfo	M		
issuerUniqueIdentifier	---		
subjectUniqueIdentifier	---		

4.2.2 Standard-extensions

Field	Critical	Mandatory/ Optional	ASN.1 type	Comments
authorityKeyIdentifier	non-critical	M		SHA-1 (hash of CA public key)
subjectKeyIdentifier	non-critical	M		SHA-1 (hash of subject public key)

keyUsage	critical	M (O)[2]		Permitted usage: - nonRepudiation - digitalSignature - keyEncipherment
privateKeyUsagePeriod		---		
certificatePolicies	non-critical	M		
policyMappings		---		
subjectAltName	non-critical	O		
issuerAltName		---		
subjectDirectoryAttributes	Non-critical	O		
basicConstraints		O		
nameConstraints		---		
policyConstraints		---		
cRLDistributionPoints	Non-critical	M		
extKeyUsage	Non-critical	O		

4.2.3 Private extensions

Field	Critical	Mandatory/ Optional	Comments
AuthorityInfoAccess	Non-critical	O	If OCSP are used
biometricInfo	non-critical	O	
qcStatements	non-critical	O	
cardNumber	non-critical	O	

[2] The keyUsage extension is currently not supported by some of the implementations.