Digital Certificate (X.509)

PRIMAR®

- S-100 part 15 uses the X.509 to define Scheme Administrator (IHO) root certificate and Data Server Certificates
- X.509 certificate contains all the information required by the recipient to validate and make use of the content
  - Issuing organisation (root or certificate authority)
  - Subject organisation
  - Certificate validity period
  - Subject public key information

Version
Serial Number
Signature Algorithm Identifier
Issuer Name
Validity Period
Subject Name
Public Key Information
Issuer Unique ID
Subject Unique ID
Extensions

Current definition signatures S-100

- Defined in datasetDiscoveryMetadata and supportFileDiscoveryMetadata

Attribute	digitalSignatureValue	Value derived from the digital signature	1	S100_DigitalSignatureValue	The value resulting from application of digitalSignatureReference Implemented as the digital signature format specified in Part 15

S100_DigitalSignatureValue

Role Name	Name	Description	Mult	Type	Remarks
Class	S100_DigitalSignatureValue	Signed Public Key plus the digital signature	-		Data type for digital signature values

- Catalogue file only contains the subject PUBLIC KEY and its file SIGNATURE
- Limitations:
  - Impossible to identify subject organisation
  - Impossible to validate validity period
  - Is it a public key with all required DSA parameters?
  - Non-compatibility with authentication developments E-Navigation
  - Does not support a future implementation of certificate revocation list (CRLs)

Proposal 1: Certificate Inclusion

PRIMAR®

- The *digital certificate* should be included in the exchange set (not only the public key)
  - Supports de-facto certificate management
- Better support for adding more participants (Data Servers) to the protection scheme

Proposal 2: Certificate Definition

- Propose to define all referenced Data Server Certificates as exchange metadata with an ID reference
- Propose to use the ID reference when a dataset signature is defined
- PRIMAR can produce exchange sets containing 15-20.000 dataset files (S-57)

Example encoding

<S100XC:S_100ExchangeCatalogue
.....
<S100XC:S_100exchangeCertificates>
<S100:dataServer id="PRIMAR">
<S100:dataServerCertificate>
-----BEGIN CERTIFICATE-----
MIIE/zCCBLygAwIBAgIFAIDJF8swCwYJYIZIAWUDBAMCMF4xDDAKBgNVBAMMA0VD
QzEMMAoGA1UECwwDRUNDMQwwCgYDVQQKDANFQ0MxEjAQBgNVBAcMCVN0YXZhbmdl
cjERMA8GA1UECAwIUm9nYWxhbmQxCzAJBgNVBAYTAk5PMB4XDTE5MDMyMjE1MDAz
…..
BgNVBAYTAk5PggkAyzpT6dnxR9swCwYJYIZIAWUDBAMCAzAAMC0CFDab/4/TogEF
VsD5bmpM5/55jNC3AhUArgJQIr6BpBcl0Lc7vdvsAdpkQ2A=
-----END CERTIFICATE-----
</dataServerCertificate>
</S100:dataServer>
….
….
<S100XC:datasetDiscoveryMetadata>
<S100XC:fileName>101NO002A4804.000</S100XC:fileName>
....
<S100XC:dataProtection>1</S100XC:dataProtection>
<S100XC:protectionScheme>S-100<S/100XC:protectionScheme>></S100XC:protectionScheme>
<S100XC:digitalSignatureReference>dsa</S100XC:digitalSignatureReference>
<S100XC:digitalSignatureValue
dataServerId="PRIMAR”>302C021433796C6647CC1C55A67DC72FA7C6E157A6594B2B02145D3768B44F3A6ABA11A
77178B738AD3B6A0DE344
</S100XC:digitalSignatureValue>
....