Paper for Consideration by S-100TSM7

S-100/S101 Exchange Catalogue Digital Certificate and Signature exchange

Submitted by:	ECC
Executive Summary:	This is a discussion paper related to exchange and encoding of Data Server Certificates and dataset digital signatures.
Related Documents:	
Related Projects:	

Introduction / Background

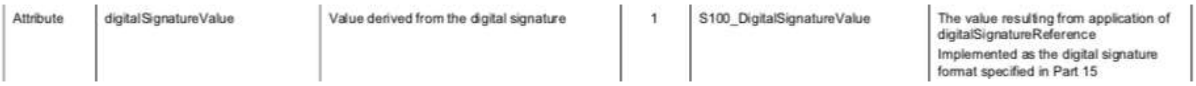
Electronic Chart Centre (ECC) has started to develop support for data protection in accordance with S-100 Part 15 which was published in December 2018.

We have in our development identified possible shortcomings in the encoding of digital certificates and signatures when exchanging dataset files. This document proposes a change to how certificate and signature information is encoded. If approved, it will require changes to S-100, S-100 part 15 and S-101.

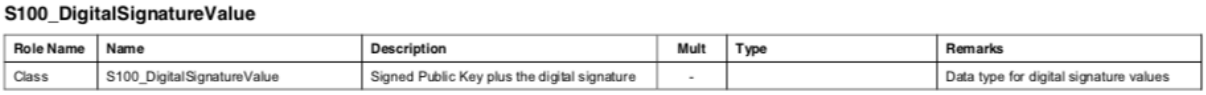
Analysis

IHO will operate as S-100 Scheme Administrator (SA) for the S-100 data protection scheme. PRIMAR has in its S-101 project developed for IHO a S-100 Scheme Administrator (SA) application with functionality to verify Certificate Signing Requests (CSR) from Data Servers and issue S-100 Data Server Certificates. The IHO and the SA application will not digitally sign a Data Server´s public key. The Data Server Certificate contains information to identify the Data Server organisation, validity period for the Data Server certificate, and all the parameters required to extract the Data Server public key and use it in the authentication of dataset files included in the exchange set (P,Q,G,Y parameters for the DSA algorithm).

The S-100/S-101 defines the following record construct to exchange signature information for a file included in the exchange set:



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

We have identified the following challenges with this encoding.

The specifications assume that only the IHO signature of the Data Server public key will be encoded together with the Data Server signature for an exchange file will be encoded in the datasetDiscoveryMetadata or supportFileDiscoveryMetadata records. This raises the following problems:

1. The IHO as S-100 protection Scheme Administrator will only issue Data Server Certificates, ref S-100 part 15. IHO will not create or issue Data Server Signed Public Keys as currently described in the S-100/S-101 standards. (The Certificate contains the Data Server public key together with all relevant DSA parameters)

2. To enable a data recipient to successfully authenticate a file using the defined DSA algorithm (ref S-100 part 15), the recipient must obtain a copy of the Data Server P,Q,G and Y parameters. These parameters are only included in a Data Server Certificate. Since S-100 only defines a mechanism to exchange a Data Server public key (Y parameter) it will be impossible for the recipient to authenticate any of the files included in the exchange set.

3. A separate exchange mechanism must be established to deliver Data Server Certificates to the data recipient. The recipient must have a copy of the Certificates for all Data Servers which have applied a digital signature to the files included in the exchange set. Authentication as defined today will NOT work unless alternative proprietary methods are established to send the Data Server Certificate to the recipient.

We propose to make the following changes to S-100/S-100 part 15 and S-101 to establish a formal mechanism to support authentication of files included in the exchange set. An example of the encoding is provided below:

a) A new record structure is defined in the S100_ExchangeCatalogue to support the encoding of all Digital Certificates (public keys with parameters) required to authenticate all the datasets included in the exchange set. Each Data Server Certificate will be defined once with an ID and referenced whenever a file signature is defined. See attached example where two Certificates are defined (PRIMAR and Norwegian Hydrographic Service).
b) The new Certificate record can hold multiple Data Server Certificates (multiplicity 0..n)
c) The recipient system can now use the pre-installed IHO root public key to authenticate all the included Data Server Certificates. If authentication fails, the exchange files signed by that Data Server shall not be used. For all certificates which authenticates successfully, the OEM system can verify the certificate validity period and extract the P, Q, G and Y parameters for later use when dataset files are to be authenticated and imported into the system.
d) When a dataset file is defined in datasetDiscoveryMetadata or supportFileDiscoveryMetadata record, only the ID of the Data Server is included together with the signature of the file. This enables multiple digital signatures to be attached to a dataset file; e.g. HO, RENC etc. The OEM system can now use the P,Q,G and Y parameters extracted from the authenticated Data Server Certificate to be used for the dataset file authentication.
e) This mechanism assumes that IHO will be the only scheme administrator and that all Data Server Certificates can be authenticated using the IHO public key.

Example of encoding:

Definition of two Data Server Certificates (including their P,Q,G and Y parameters)

```
<S100XC:S_100ExchangeCatalogue
.....
<S100XC:S_100exchangeCertificates>
            <S100:dataServer id="PRIMAR">
                        <S100:dataServerCertificate>
                                    -----BEGIN CERTIFICATE-----
                                    MIIE/zCCBLygAwIBAgIFAIDJF8swCwYJYIZIAWUDBAMCMF4xDDAKBgNVBAMMA0VD
                                    QzEMMAoGA1UECwwDRUNDMQwwCgYDVQQKDANFQ0MxEjAQBgNVBAcMCVN0YXZhbmdl
                                    cjERMA8GA1UECAwIUm9nYWxhbmQxCzAJBgNVBAYTAk5PMB4XDTE5MDMyMjE1MDAz
                                    NloXDTI5MDMyMjE1MDAzNlowDTELMAkGA1UEBhMCTk8wggG3MIIBKwYHKoZIzjgE
                                    ATCCAR4CgYEAqFb4BB9rXOXDwDiZb/X8EmQz57+053Eztt7/nojM6voUpi5MDTyv
                                    vsHKoTcEsX/otrRcrUXukTBhvUL3naeOBX3Y21zKfZ+ApfclNJ8ZuCCy/0Ok+w9q
                                    8w38NWYv+P37681zdYRz/ZwjjfOLAloWKc7EnOVyLa3elS/Uu6/BCSMCFQDKR2Dy
                                    Gpdury5G24RCr1U4/alfpwKBgDx9ga+CbcPxRdQrpMdCzS+KQCRQURFs0i6gTAuj
                                    9AVjnlTMYm6Vb6czys1toMi0TwMihz5t5Gx2cdFPb9s0iZCNUFjsYCNlILe/DhNQ
                                    eey9xxIDVBZQgUlOplsV40h9W7nQemkR3YQgiGboZ0wLtCx1l/yrBBQTEG7hiGKa
                                    ZCymA4GFAAKBgQCRrtoLPJcM9fjBFqyyf7WAhUkSqwNFGzJTf9i8MAiOGh9EREU8
                                    oJ8fM4WBG/KzbuKjddZADoiYR3u0WbR+TGHra0pdGqSLLVV2ECjX8glkffe9yWYN
                                    wT9saKvv3ErQKrxlk2H5869qVOFSxloLF1Y9QwdWKVGUg0yeF5LHNb11V6OCAlUw
                                    ggJRMAkGA1UdEwQCMAAwggHIBgNVHQ4EggG/BIIBuzCCAbcwggErBgcqhkjOOAQB
                                    MIIBHgKBgQCoVvgEH2tc5cPAOJlv9fwSZDPnv7TncTO23v+eiMzq+hSmLkwNPK++
                                    wcqhNwSxf+i2tFytRe6RMGG9Qvedp44FfdjbXMp9n4Cl9yU0nxm4ILL/Q6T7D2rz
                                    Dfw1Zi/4/fvrzXN1hHP9nCON84sCWhYpzsSc5XItrd6VL9S7r8EJIwIVAMpHYPIa
                                    l26vLkbbhEKvVTj9qV+nAoGAPH2Br4Jtw/FF1Cukx0LNL4pAJFBREWzSLqBMC6P0
                                    BWOeVMxibpVvpzPKzW2gyLRPAyKHPm3kbHZx0U9v2zSJkI1QWOxgI2Ugt78OE1B5
                                    7L3HEgNUFlCBSU6mWxXjSH1budB6aRHdhCCIZuhnTAu0LHWX/KsEFBMQbuGIYppk
                                    LKYDgYUAAoGBAJGu2gs8lwz1+MEWrLJ/tYCFSRKrA0UbMlN/2LwwCI4aH0RERTyg
                                    nx8zhYEb8rNu4qN11kAOiJhHe7RZtH5MYetrSl0apIstVXYQKNfyCWR9973JZg3B
                                    P2xoq+/cStAqvGWTYfnzr2pU4VLGWgsXVj1DB1YpUZSDTJ4Xksc1vXVXMHgGA1Ud
                                    IwRxMG+hYqRgMF4xDDAKBgNVBAMMA0VDQzEMMAoGA1UECwwDRUNDMQwwCgYDVQQK
                                    DANFQ0MxEjAQBgNVBAcMCVN0YXZhbmdlcjERMA8GA1UECAwIUm9nYWxhbmQxCzAJ
```

```
                BgNVBAYTAk5PggkAyzpT6dnxR9swCwYJYIZIAWUDBAMCAzAAMC0CFDab/4/TogEF
                VsD5bmpM5/55jNC3AhUArgJQIr6BpBcl0Lc7vdvsAdpkQ2A=
                -----END CERTIFICATE-----
            </dataServerCertificate>
        </S100:dataServer>

        <S100:dataServer id="Norwegian Hydrographic Service">
            <S100:dataServerCertificate>
                -----BEGIN CERTIFICATE-----
                .......
                .......
                -----END CERTIFICATE-----
            </dataServerCertificate>
        </S100:dataServer>
</S100XC:S_100exchangeCertificates>
```

Encoding of digital signatures for each file:

```
<S100XC:datasetDiscoveryMetadata>
        <S100XC:fileName>101NO002A4804.000</S100XC:fileName>
        ....
    <S100XC:dataProtection>1</S100XC:dataProtection>
        <S100XC:protectionScheme>S-100<S/100XC:protectionScheme>>
    <S100XC:digitalSignatureReference>dsa</S100XC:digitalSignatureReference>
    <S100XC:digitalSignatureValue dataServerId="PRIMAR">
        302C021433796C6647CC1C55A67DC72FA7C6E157A6594B2B02145D3768B44F3A6ABA11A77178B738AD3B6A0
DE344
        </S100XC:digitalSignatureValue>
        ....
```

Discussion

The current encoding of digital signatures in S-100 will not work because:

- Mechanisms for exchange of Data Server Certificates must be established outside the scope of S-100
- Encoding of only a Data Server Public Key in S-100 exchange set is insufficient for enabling a recipient to perform an authentication of a file. The P, Q, G and Y parameters must be provided and is provided in the Data Server Certificate
- The IHO as S-100 Scheme Administrator does not sign Data Server public keys as defined in S-100, only issue Data Server Certificates

By using the proposed mechanism as shown in the example, a dataset file can be digitally signed by multiple Data Servers (e.g. HO, RENC). Defining all relevant Certificates once as metadata initially in the catalogue file and only use their IDs for reference when encoding a digital signature will contribute to reducing the overall size of the catalogue file. File size does not have to be an issue, but creating large exchange sets with 20-30.000 files where certificate information must be repeated every time a signature is defined can introduce some excess file overhead. Other information in the exchange records can also introduce overhead; e.g. the volume of information included when defining organisations and their contact detail or number of coordinates required to define the dataset bounding polygon.

An alternative mechanism will be to update the current definition of signatures to enforce a Data Server Certificate must be included whenever a digital signature is encoded. This will however introduce a lot of file overhead and repetition of the certificate information for every file included in the exchange set. PRIMAR can create exchange sets with 20.000 dataset files and updates where the PRIMAR certificate msut be encoded once for each file instead of using a ID reference to the proper certificate definition. This will require some rewording of text in S-100, S-101 and S-100 part 15.

Conclusions

A mechanism for a proper definition and exchange of certificate information is included in the proposal.

An alternative approach using the existing record structures but with appropriate rewording of the text can also be used.

Action Required of S-100TSM7

The S-100TSM7 is invited to:

- Discuss the proposal within this paper and decide whether it could be forwarded to S100WG5 for further consideration and approval