PRIMAR®

PRIMAR S100 part 15 Data Protection

Operated by the Norwegian Mapping Authority, Hydrographic Service

FREEDOM TO CHOOSE

Digital Signatures

- An attachment to a digital file which is a unique representation of the file content and the identity of the file creator
- Provides authenticity, integrity and non-repudiation to files
- S-100 part 15 provides mechanisms for defining and exchanging digital signatures with exchange set files

Digital Signatures - Requirements

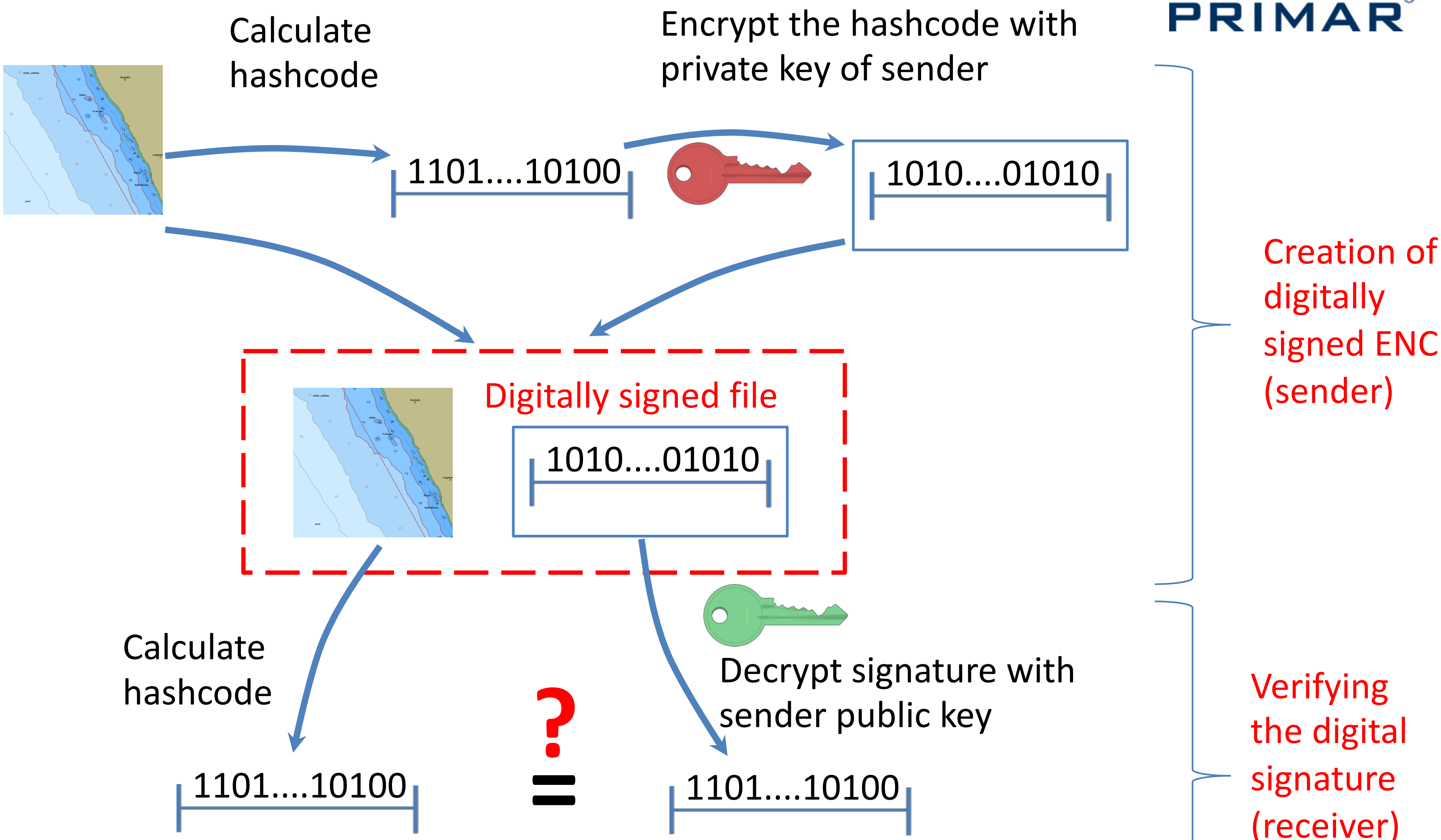
- Uses a *Private* and *Public key* pair which is mathematically related to each other
- Private Key
  - Only accessible for the signer and is used to generate the digital signature attached to the digital file
- Public Key
  - Created by the signer and mathematically related to the Signer´s Private Key
  - Used by the recipient to authenticate the signer and verify the digital signature attached to the file
- Public Keys are shared using *Digital Certificates*

Digital Certificate

- Provides a trusted infrastructure to exchange and verify a user´s public key
- Digital Certificate is a file which enables recipient to verify identity of user and safely access his public key
- Digital Certificate Issued by a trusted Certificate Authority which certifies the association of a user with a public key
- IHO operates as S-63 and S-100 Certificate Authority

- Serial number
- User identity
- User public key
- Certificate Authority
- Validity period
- Digital signature of CA
- ....

Create and verify digital signature



Calculate hashcode

1101....10100

Encrypt the hashcode with private key of sender

1010....01010

Digitally signed file

1010....01010

Creation of digitally signed ENC (sender)

Calculate hashcode

Decrypt signature with sender public key

1101....10100

?
=

1101....10100

Verifying the digital signature (receiver)

If the calculated hashcode does not match the result of the decrypted signature, the ENC is either changed after signing or was not signed with sender private key (initial verification of public key is a separate process)

IEC authentication requirements

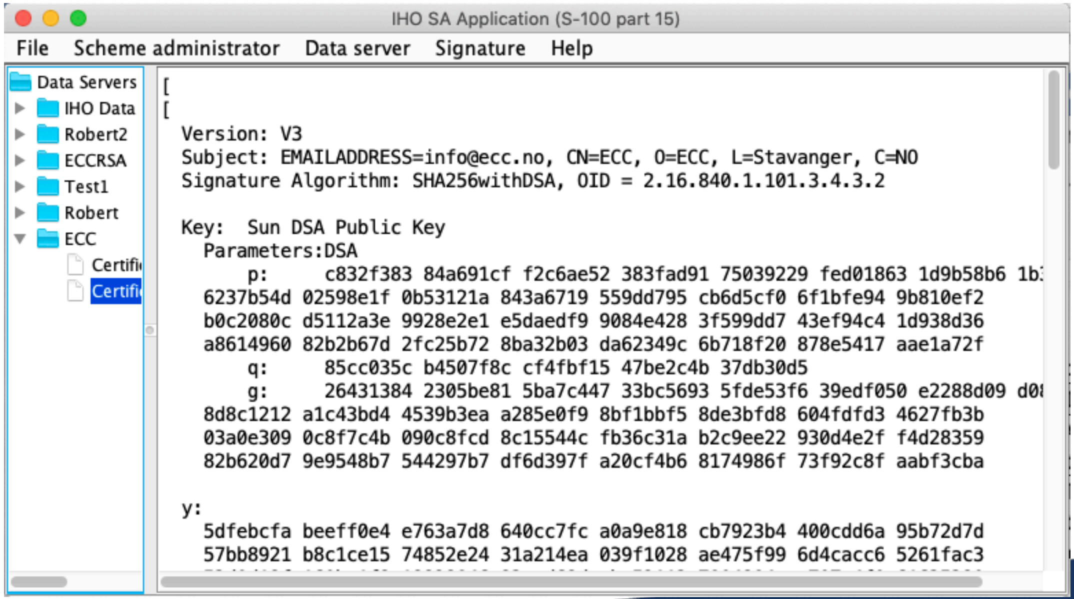
- All data products/files sent to a vessel must support authentication (digital signatures) to increase cyber security
  - S-100 part 15 provides the mechanisms to support authentication
    - S-10X Product Specifications must define how Digital Signatures and if encryption is used
  - S-63 only supports authentication of ENC cell and update files.
    - Discussion in progress for authentication of other files….

PRIMAR S-10X Development Projects

- New S-100 Part 15 – Data Protection Scheme
  - Defines recommended algorithms and data formats for encryption and digital signatures for S-10x products
- PRIMAR is developing S-100 based services
  - Continue existing S-57/S-63 ENC services
  - S-101 ENC distribution services
  - Integrated dual-fuel S-57/S-101 ENC distribution services
  - S-102 bathymetric data distribution services
- PRIMAR S-10X services will be protected and all files will be digitally signed

IHO S-100 Scheme Administrator Application

- PRIMAR S-101 project has developed IHO S-100 Scheme Administrator application
  - Verify Data Server Certificate Signing Requests (CSR)
  - Create S-100 Data Server Digital Certificates
  - Functionality to digitally sign IHO files
- Pre-requisite for anyone wishing to digitally sign S-10X data files



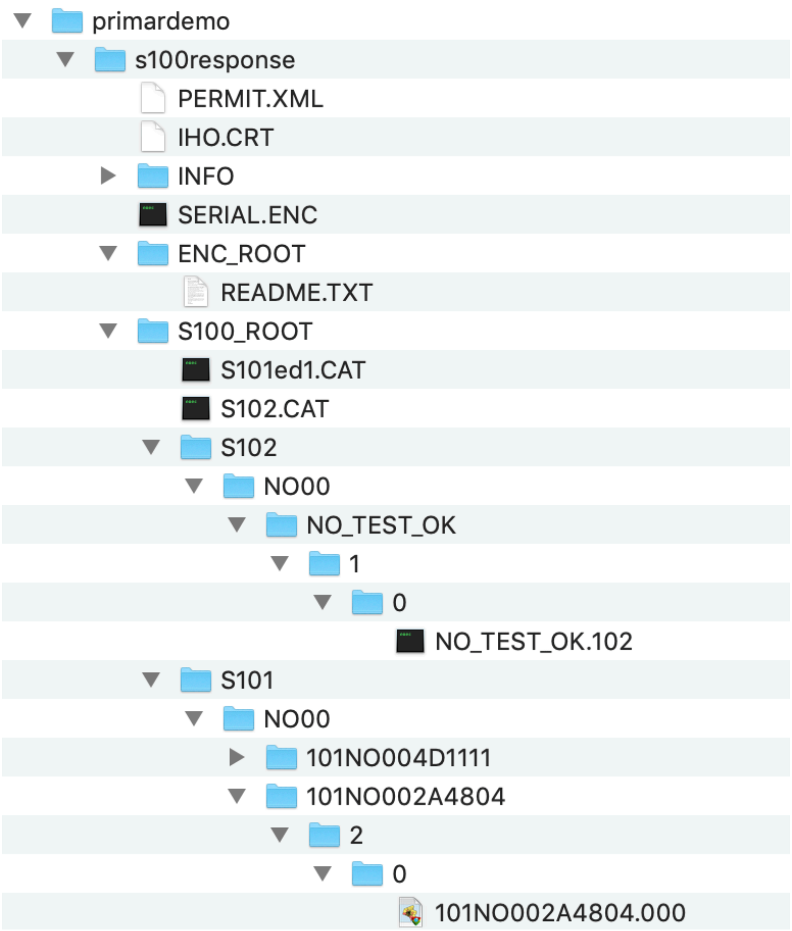
```
[
[
  Version: V3
  Subject: EMAILADDRESS=info@ecc.no, CN=ECC, O=ECC, L=Stavanger, C=NO
  Signature Algorithm: SHA256withDSA, OID = 2.16.840.1.101.3.4.3.2

  Key:  Sun DSA Public Key
    Parameters:DSA
        p:     c832f383 84a691cf f2c6ae52 383fad91 75039229 fed01863 1d9b58b6 1b
    6237b54d 02598e1f 0b53121a 843a6719 559dd795 cb6d5cf0 6f1bfe94 9b810ef2
    b0c2080c d5112a3e 9928e2e1 e5daedf9 9084e428 3f599dd7 43ef94c4 1d938d36
    a8614960 82b2b67d 2fc25b72 8ba32b03 da62349c 6b718f20 878e5417 aae1a72f
        q:     85cc035c b4507f8c cf4fbf15 47be2c4b 37db30d5
        g:     26431384 2305be81 5ba7c447 33bc5693 5fde53f6 39edf050 e2288d09 d0
    8d8c1212 a1c43bd4 4539b3ea a285e0f9 8bf1bbf5 8de3bfd8 604fdfd3 4627fb3b
    03a0e309 0c8f7c4b 090c8fcd 8c15544c fb36c31a b2c9ee22 930d4e2f f4d28359
    82b620d7 9e9548b7 544297b7 df6d397f a20cf4b6 8174986f 73f92c8f aabf3cba

  y:
    5dfebcfa beeff0e4 e763a7d8 640cc7fc a0a9e818 cb7923b4 400cdd6a 95b72d7d
    57bb8921 b8c1ce15 74852e24 31a214ea 039f1028 ae475f99 6d4cacc6 5261fac3
```

PRIMAR S-100 Data Protection

PRIMAR®

- PRIMAR S-10X services will be protected and all files will be digitally signed using S-100 part 15
- Internal testing
  - Digital signatures S-101 and S-102 datasets
  - Encryption S-101 and S-102 datasets
  - Integrated dual-fuel S-57 and S-101 exchange sets

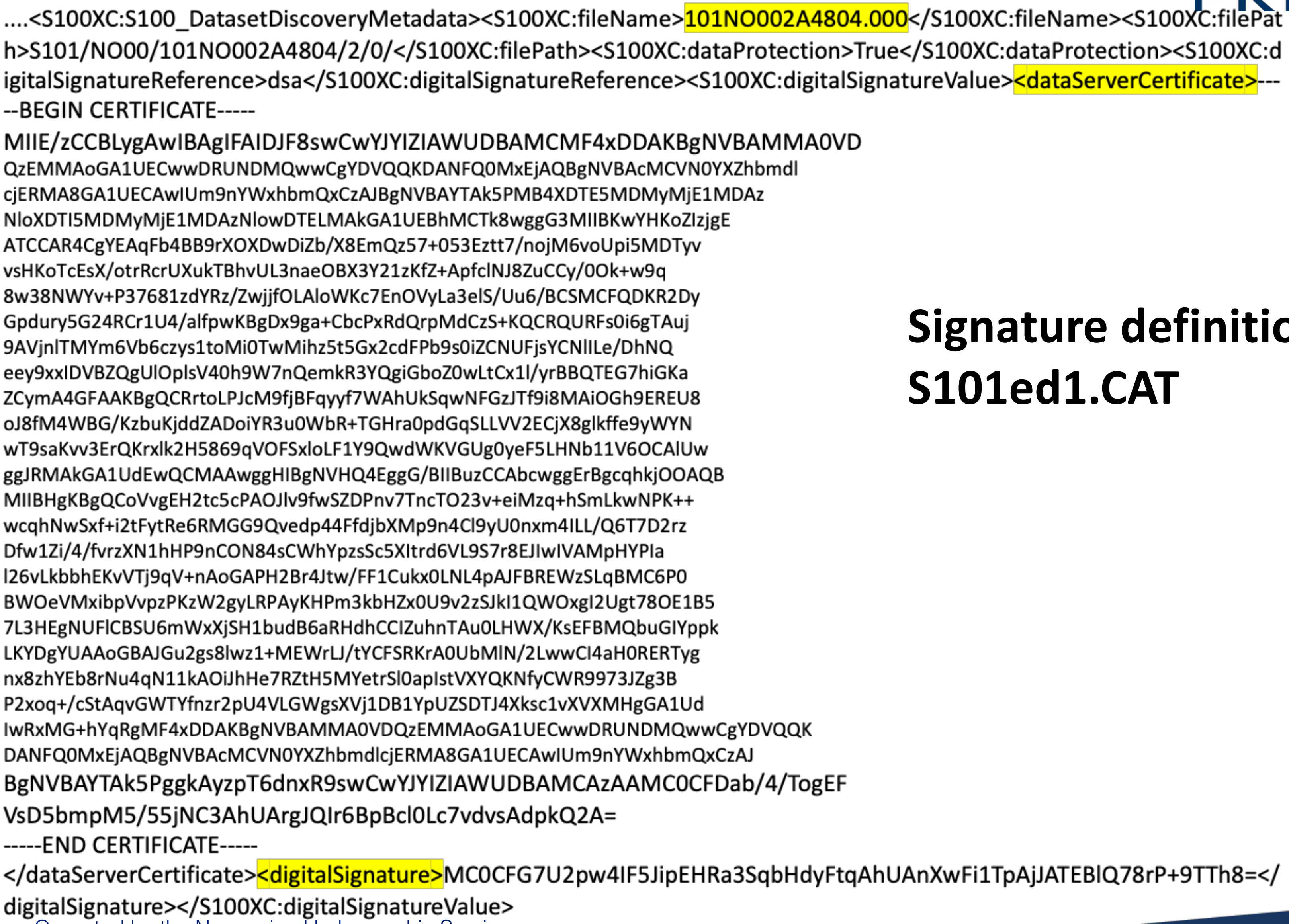
Data Protection Sample Data



```
▼ primardemo
  ▼ s100response
      PERMIT.XML
      IHO.CRT
    ▶ INFO
      SERIAL.ENC
    ▼ ENC_ROOT
        README.TXT
    ▼ S100_ROOT
        S101ed1.CAT
        S102.CAT
      ▼ S102
        ▼ NO00
          ▼ NO_TEST_OK
            ▼ 1
              ▼ 0
                  NO_TEST_OK.102
      ▼ S101
        ▼ NO00
          ▶ 101NO004D1111
          ▼ 101NO002A4804
            ▼ 2
              ▼ 0
                  101NO002A4804.000
```

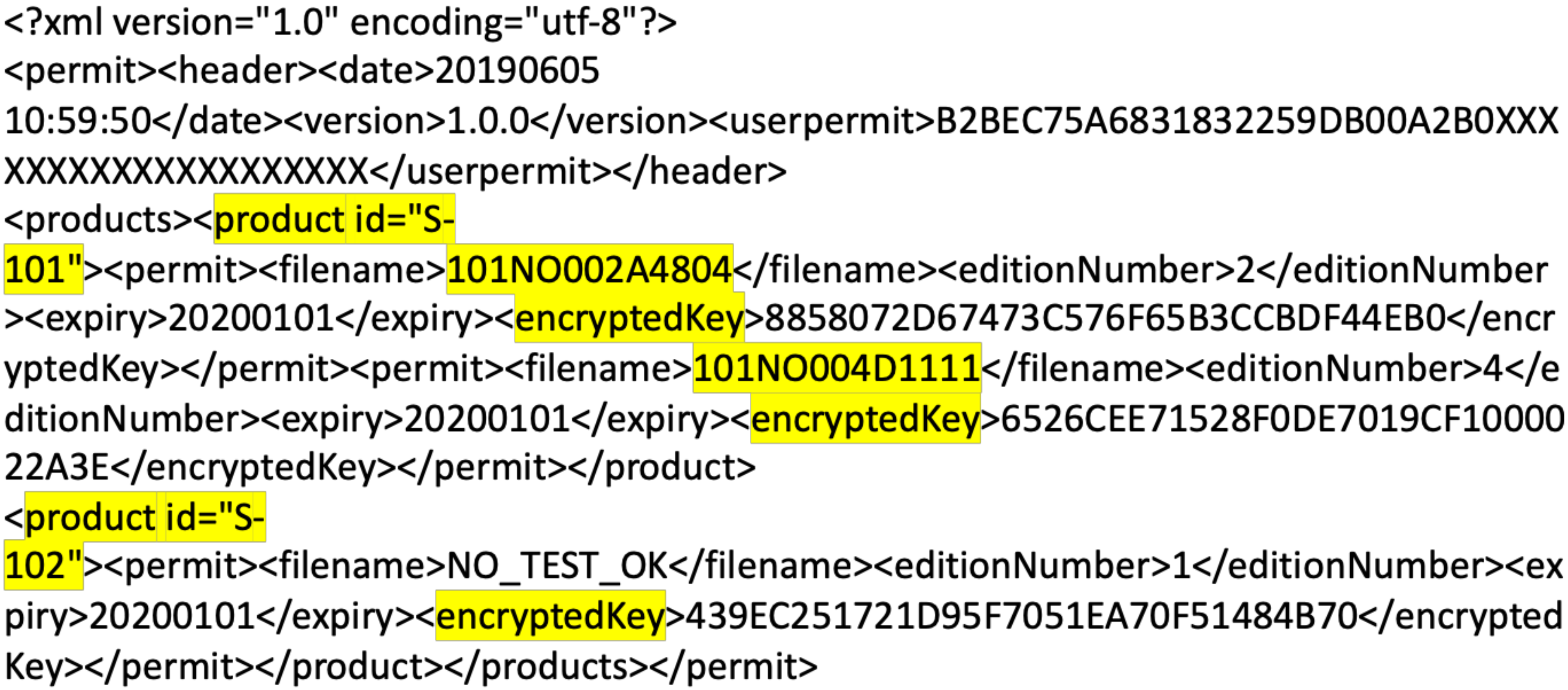
- (Demo)
- Testing S57, S101 and S102 services; integrated and/or separated
- Review of data structures in S100 part 15
- Inclusion of MD_ files in S101
- File naming conventions
- Use official IHO S-100 root certificate

Signature definition in S101ed1.CAT



```
....<S100XC:S100_DatasetDiscoveryMetadata><S100XC:fileName>101NO002A4804.000</S100XC:fileName><S100XC:filePat
h>S101/NO00/101NO002A4804/2/0/</S100XC:filePath><S100XC:dataProtection>True</S100XC:dataProtection><S100XC:d
igitalSignatureReference>dsa</S100XC:digitalSignatureReference><S100XC:digitalSignatureValue><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><digitalSignature>MC0CFG7U2pw4IF5JipEHRa3SqbHdyFtqAhUAnXwFi1TpAjJATEBlQ78rP+9TTh8=</
digitalSignature></S100XC:digitalSignatureValue>
```

Permit Example



```
<?xml version="1.0" encoding="utf-8"?>
<permit><header><date>20190605
10:59:50</date><version>1.0.0</version><userpermit>B2BEC75A6831832259DB00A2B0XXX
XXXXXXXXXXXXXXXX</userpermit></header>
<products><product id="S-
101"><permit><filename>101NO002A4804</filename><editionNumber>2</editionNumber
><expiry>20200101</expiry><encryptedKey>8858072D67473C576F65B3CCBDF44EB0</encr
yptedKey></permit><permit><filename>101NO004D1111</filename><editionNumber>4</e
ditionNumber><expiry>20200101</expiry><encryptedKey>6526CEE71528F0DE7019CF10000
22A3E</encryptedKey></permit></product>
<product id="S-
102"><permit><filename>NO_TEST_OK</filename><editionNumber>1</editionNumber><ex
piry>20200101</expiry><encryptedKey>439EC251721D95F7051EA70F51484B70</encrypted
Key></permit></product></products></permit>
```

Follow-up activities

- Identified S-100 part 15 document improvements/ clarifications
  - Detailed example data required
- Make verified testdata freely available (S-101, S-102++)
  - Current plan is to publish PRIMAR testdata on Github until alternative IHO source is available
  - Testdata mandatory for software developers to develop support for S-10x products
- Provide data protection input to S-100 part 15, S-101 and S-102 working groups