Paper for Consideration by S100TSM9

Proposal for IHO S-100e5 protection scheme policies

Submitted by:	PRIMAR
Executive Summary:	Defines the policies to be adopted by IHO when operating as the S-100e5 Scheme Administrator and the requirements of the scheme administrator application to support that role.
Related Documents:	S-100 5.0.0 part 15
Related Projects:	

Introduction / Background

This document outlines the S-100e5 data protection policies to be adopted by IHO when becoming the S-100e5 Scheme Administrator. It will also form the basis for developing the required application to empower IHO to operate as the S-100e5 Scheme Administrator.

The presented policies are discussed while keeping in mind that the IHO is also scheme administrator for S-63 and S-100e4 protection schemes. These policies shall also be applied for S-63 and S-100e4 where feasible.

PRIMAR Advisory Committee (PAC) has funded a project in 2023 to empower IHO to operate as S-100e5 Scheme Administrator. This will cover all costs for training in standards and operational procedures, upgrade of S-100e5 Scheme Administrator application with digital signing functionality, and provide continued support to IHO after 2023. PRIMAR has provided a similar role and support to IHO for S-63 and S-100e4.

Analysis/Discussion

S-100e5 Scheme Administrator root certificate and certificate durations

1) S-100e5 part 15 introduced changes to the protection scheme. The key lengths were increased to increase protection and make the IHO S-100e5 protection scheme compatible with the IEC 63173-2 SECOM standard. The changes will require IHO to issue a new S-100e5 scheme root certificate. The S-100e5 root certificate is not compatible with S-100e4 or S-63, and there should be no possibilities for misunderstanding since the key lengths/algorithms are different (dependant on stakeholder implementation).

2) The IHO has as the data protection Scheme Administrator (SA) issued the following root scheme certificates:
   - S-63 (renewal date 03 Feb 2033, issued 06 Feb 2013, already renewed once)
   - S-100e4 (renewal date 11 Oct 2051, issued 03 Dec 2019)

The SA root certificate is used by IHO to create protection scheme Data Server certificates. When a root certificate is renewed, all OEM installations must replace the current root certificate with the new IHO root certificate.

3) Commercial root certificates pre-installed with your computer operating system typically have a duration of 20-30+ years. The IHO root certificate shall have a long duration since all OEM installation will be required to install the renewed IHO root certificate. All valid Data Server certificates continue to be valid independent of when IHO decides to renew their root certificate. (IHO has established procedures to secure their private keys required to renew the root certificate.) A renewed IHO root certificate shall be issued minimum 3 years before the current certificate expires to allow for sufficient time to reinstall the certificate on OEM installations. It is recommended that:
   - The S-100e5 root certificate duration is 40 years
   - The renewed S-100e5 root certificate shall be issued minimum 3 years before the current root certificate expires.

4) IHO has issued S-100e4 Data Server Certificates with a duration of 10 years.

5) When a Data Server certificate is issued or renewed, it will only have to be installed with the Data Server. None of the other protection scheme stakeholders will be affected because of the hierarchy structure of the certificates. A renewal of a Data Server certificate shall not have any impacts on the current data server service provision (as long as the Data Server renewal Certificate Signing Request is based on the original internal key pairs). A Data Server certificate can as a consequence have a shorter duration and implicitly also act as certificate revocation when it expires and is not renewed. It is recommended that:
   - The S-100e5 Data Server certificate duration is 5 years

X.509 Certificate information fields

6) IHO shall require that all Data Servers standardize the encoding of X.509 certificate fields in accordance with the document S-100WG7-06.7 S-100 Part 15 Identifiers and Procedures.

7) The IHO S-100e5 root certificate will comply with S-100WG7-06.7 information fields encoding.

IHO digital signature functionality

8) IHO must have functionality to digitally sign relevant standard components, e.g. S-101 Feature and Portrayal Catalogues. The output of the signature process shall be a properly formatted S-100 Exchange Set containing the signed source files.

9) When IHO issue digitally signed files, it shall always and only be in accordance with S-100e5 data protection. The motivation behind the requirement is to encourage all stakeholders to implement support for S-100e5. (Even though IHO already can sign files in accordance with IHO S-100e4, the functionality shall be disabled in next software upgrade and never be used.)

10) It is recommended that the IHO never uses the scheme root keys (root certificate) when it digitally signs files. The IHO should become a Data Server and use the IHO Data Server keys (certificate) when it digitally signs files. It is important to distinguish between IHO's role as a certificate authority from its role as digitally signing. This harmonises with common practice within commercial cryptography.

11) The IHO shall only publish the scheme root certificates (S-63/S-100e4/S-100e5) on their website. This should not have any implications for stakeholders on the operation of the protection scheme:
    - The scheme participants (especially OEMs) shall have functionality to install root certificates, and never from certificates encoded and provided in exchange sets.
    - The hierarchy of certificates will ensure that files signed with IHO data server keys are authenticated using the pre-installed IHO scheme root certificate. The certificate identity and issuer organisation are obtained from the X.509 certificate information fields.
    - If an organisation has not yet developed support for S-100e5 data protection, it can as an interim measure still utilise and access the files provided by IHO in digitally signed exchange sets. Since the signature information is only encoded in the exchange set catalogue file and not in a data files itself, the files can be processed without considering authentication. This is not a recommended procedure, and the organisation should carefully consider risks and how it obtained a copy of the exchange set!

<u>Transition S-100e4 to S-100e5</u>

12) IHO will be required to support earlier versions of the protection scheme until only S-100e5 is fully operational (e.g. IHO announces that S-100e4 support is discontinued, service providers do not have any customers using S-100e4 compliant systems, no HOs produce S-100e4 dataset, or IMO requires upgrade to S-100e5). IHO and stakeholders should endeavour to make the transition period from S-100e4 to S-100e5 as short as possible, and encourage and focus on the adoption and use of S-100e5 services among all stakeholders/end-users.

13) If a Data Server is going to introduce S-100 services today, it will be forced to deliver S-100e4 compliant services since there are no known users with S-100e5 compliant systems in the market today. Several OEMs have obtained the required from IHO information to start developing support for S-100e5.

14) As soon as IHO becomes operational as S-100e5 Scheme Administrator, it should immediately enforce that all new Data Servers for an interim period should receive both S-100e4 and S-100e5 Data Server Certificates. It implies that a new Data Server always must create two Certificate Signing Request (CSR) files to obtain both a S-100e4 and S-100e5 Data Server Certificate.

15) IHO should approach all existing S-100e4 Data Servers and invite them to obtain a S-100e5 Data Server Certificate.

Conclusions

It is recommended that IHO adopt the following certificate policies which will be reflected in operational procedures and their Scheme Administrator application:

a) The IHO shall issue a S-100e5 root certificate at earliest convenience in 2023 to encourage stakeholders to develop support for S-100e5. The S-100e5 root certificate shall be published on the IHO web site.

b) The IHO S-100e5 root certificate shall have a duration of 40 years. Any renewed S-100e5 root certificate shall be issued minimum 3 years before the current root certificate expires. IHO will establish appropriate procedures to secure its private key information.

c) S-100e5 Data Server certificates shall be issued with a duration of 5 years.

d) All S-100e5 certificates shall encode the X.509 information fields in compliance with document S-100WG7-06.7 S-100 Part 15 Identifiers and Procedures

e) IHO will obtain a separate IHO S-100e5 Data Server certificate which will only be used when IHO needs to digitally sign files.

f) New IHO Data Servers will for an interim period receive both S-100e4 and S-100e5 Data Server certificates. IHO will contact existing S-100e4 Data Servers to issue a S-100e5 Data Server certificate.

g) IHO will only issue digitally signed files which are compliant with the S-100e5 protection scheme. The signed files will be delivered in a S-100e5 compliant exchange set.

h) IHO shall work with protection scheme stakeholders to encourage and ensure a rapid transition to S-100e5.

Action Required of S100TSM

The S100TSM is invited to:

- Note the paper and discuss proposed protection policy.