Discussions on IHO Security Scheme Revocation

- **Options and recommendations -**

IHO Security Schemes

- IHO is the Scheme Administrator (SA) for all their security schemes. It is in practice the same role and function as a commercial Certificate Authority (CA)
- IHO is the custodian and SA for the following security schemes:
    - S-63: Security scheme developed for use with S-57 datasets. Approximately 400+ OEMs and 77 Data Servers registered, but several stakeholders are inactive or have not implemented support for S-63 applications/services. Many end-user installations.
    - S-100e4: Security scheme developed for use with S-100e4 and compliant product specifications. 37 OEMs and 77 Data Servers registered, but several stakeholders are inactive or have not implemented support for S-100e4 applications/services. Limited number of end-user installations
    - S-100e5.1: Security scheme developed for use with S-100e5.1 and compliant product specifications. 37 OEMs (common for all S-100 schemes) and 2 Data Servers registered. None of the Data Servers have developed support S-100e5.1 services and they have indicated they instead will develop support for S-100e5.2 security scheme. No end-user installations.
    - S-101e5.2: Security scheme developed for use with S-100e5.2 and compliant product specifications. 37 OEMs (common for all S-100 schemes) and 2 Data Servers registered. It is expected that this edition of S-100 will become the de-facto standard for every stakeholder to support in the near future. Currently no end-user installations, but service providers and end-user installations are expected to grow.
- None of the IHO protection schemes are backward compatible because of changes in algorithms and key lengths. (Note that the S-100 schemes are all sharing and using the same OEM credentials issued by IHO)
- IHO security schemes have defined 3 stakeholders: Scheme Administrator (IHO), Data Servers and OEMs
- Stakeholders must sign either a Data Server Agreement or OEM Agreement with IHO to become a member of the security scheme. All rights and obligations are defined in these agreements.

Security scheme revocation

- Revocation implies withdrawing a stakeholder's credentials required to participate in the security scheme. There can be many reasons for revocation, e.g. information has been compromised or stakeholder has violated terms and conditions for participation.
- Revocation within the IHO security scheme implies establishing a combination of procedures, functionality, and legal clauses to withdraw:
    - Data Server Certificates for one or all security schemes
    - OEM credentials (M_ID/M_KEY) for S-63 and/or S-100
- Revocation of any of the IHO SA root certificates is considered a special case. It will have a consequence for all Data Servers for that protection scheme which will have to get a new Data Server Certificate signed with the new SA root private key. IHO has

successfully been able to safeguard its SA private keys for the last 20+ years and it is assumed adherence to the same procedures will continue to protect the IHO root keys. It is envisaged that more automated revocation procedures can be established and operated with the introduction of S-100e6 and that root certificate revocation procedures can be formalised with S-100e6.

- Will need to come up with a revocation procedure which can be used for all security schemes and for all categories of stakeholders
- Several technologies exist and are in use within the commercial digital certificate industry:
    - Certificate Authority (IHO) can issue a Certificate Revocation List (CRL) which is distributed every time it is updated. The CRL can be distributed to OEMs who will distribute it to their end-user installations, or Data Servers can be required to distribute and include the CRL to end-users as a new element in their service provision
    - The Online Certificate Status Protocol (OCSP) is an internet standard that allows to check the validity status of X.509 digital certificates. It overcomes some of the distribution and delay issues associated with CRLs and enables a real-time status check of digital certificates (good, revoked or unknown)
    - OCSP Stapling overcomes some of the limitations associated with OCSP and the online connectivity requirement. OCSP Stapling allows the owner of a digital certificate to obtain a digitally signed and time-stamped OCSP certificate status response from a CA which is operating a OCSP service. The stapling response can be attached with the certificate and used to indicate certificate is valid and has not been revoked. Many commercial CAs use OCSP staples with 7 days validity period, but this can be configured by the OCSP operator using the response values thisUpdate, nextUpdate, producedAt. Within our domain procedures must be established on how to interpret the validity of a certificate and supplied dates in the staple response with when the dataset was digitally signed and exchange set created. We are trying to adapt (or circumvent) the certificate validity check feature of OCSP Stapling by interpreting information in such a way that a certificate could have been valid when a dataset and staple was created, and the public key can be used to authenticate the dataset – even though if the certificate later has been revoked or the OCSP Staple has expired because of transmission time.
- The use of CRLs and OCSP is not applicable for the revocation of OEM credentials since these technologies only apply to digital certificates. OEM revocation is only achievable using legal clauses in the above referenced agreements and assigning specific obligations on scheme stakeholders. If later editions of S-100 introduce the use of digital certificates for all stakeholder participants including end-users, a common and shared revocation procedure can be established for the IHO protection schemes.

S-63 security scheme revocations

- *Data Server Certificates*: They are issued by the Scheme Administrator and are encoded in a non-standardised and proprietary format. They contain no information

about subject organisation, issuer, or certificate duration. Certificates never expire. Data Server revocation is only achievable by either of the following methods or a combination of them:

a) Publish a copy of the Data Server Certificate to be revoked and send it to all OEMs and encourage them to distribute it to all their end-user installations. OEMs must develop additional S-63 functionality to check if Data Server Certificates have been revoked, and not import any datasets signed by such Data Servers. To make this an obligation on the OEM might require updates to the OEM Agreement.
b) IHO to issue a Circular Letter to all HOs, RENCs, and registered Data Servers to inform them about the identity of the Data Server organisation to be revoked. The Circular Letter will encourage these organisations to discontinue any dataset deliveries to the revoked Data Server. Registered security scheme participants (e.g. RENCs) shall discontinue dataset deliveries to the revoked Data Server organisation. To make this an obligation on the Data Servers might require updates to the Data Server Agreement.

- Revocation of OEM credentials:
  a) Inform all Data Servers that an OEM with listed M_IDs/M_KEYs are to be revoked from the security scheme and all dataset permit services to any systems from this OEM shall be discontinued. To make this an obligation on a Data Server might require updates to the Data Server Agreement. The Data Servers can upon request from IHO provide information on how many end-user installations will be affected by such a decision.

Recommendations:

- Data Server revocation is achieved using method (2) described above, and OEM revocation is achieved using method (a) above.
- This will limit the need for software development to possibly a limited number of active Data Servers, and not affect all the OEMs and their end-user installations. It is also assumed it can be implemented through administrative procedures within Data Servers. It is envisaged these revocation procedures must be properly defined in Data Server/OEM Agreements.
- The use of S-63 security scheme will eventually be discontinued and replaced with a S-100 security scheme. It will be critical to find procedures which will require have the least impact on stakeholder operations or require additional OEM development and updating of all their S-63 compliant installations.

S-100e4/e5 security schemes revocations

- *Data Server Certificates*: They are issued by the Scheme Administrator and are compliant with the ITU X.509 standard and have a specific duration (S-100e4: 2 years, S-100e5.1: 2 years, S-100e5.2: 1 year). Data Server Certificates must be renewed before expiration for the certificate to remain valid, and for the OEM application to validate the certificate and assume the Data Server is a legitimate member of the associated security scheme. (It is assumed that the OEM must have functionality to check if the Data Server Certificate has expired, the OEM application shall not accept the certificate and extract the public key and use it for dataset

authentication). Data Server revocation can be achieved by either of the following methods or a combination of them:

1) IHO in its role as Scheme Administrator can based on updated conditions defined in the Data Server Agreement refuse to renew a Data Server Certificate from an organisation that is to be revoked from the corresponding S-100 security scheme. This will automatically happen when a certificate expires within1-2 years, depending on the certificate duration implemented for the applicable S-100 security scheme. This should not have any development impact on an OEM since it is assumed they will automatically reject all expired Data Server Certificates.
2) Many reasons can be applicable for a need to immediately revoke a digital certificate; Data Server private key has been compromised (impersonation) or severe violations of the Data Server Agreement. For this to be effective, the Scheme Administrator must issue either a CRL or establish an OCSP Stapling service. This will require that:
    a. IHO SA establish CRL and/or OCSP stapling services
    b. The S-100 standard and part 15 implements support for attaching an OCSP Staple to the certificate definitions in an Exchange Set
    c. OEMs must develop functionality to support whatever certificate revocation services provided by IHO SA
    d. The IEC 61174 must be amended to define appropriate compliance tests for certificate revocation

    This option will probably require standard developments and coordination between several authorities. It will not be sufficient for IHO SA to issue CRLs since there is not a requirement on anyone to make use of its content unless a requirement to do so is defined.
3) IHO to issue a Circular Letter to all HOs, RENCs, and registered Data Servers to inform them about the identity of the Data Server organisation to be revoked. The Circular Letter will encourage these organisations to discontinue any dataset deliveries to the revoked Data Server. Registered security scheme participants (e.g. RENCs) shall discontinue dataset deliveries to the revoked Data Server organisation. To make this an obligation on the Data Servers might require updates to the Data Server Agreement.

- Revocation of OEM credentials can be achieved by:
    a) Inform all Data Servers that an OEM with listed M_IDs/M_KEYs are to be revoked from the security scheme and all dataset permit services to any systems from this OEM shall be discontinued. To make this an obligation on a Data Server might require updates to the Data Server Agreement. The Data Servers can upon request from IHO provide information on how many end-user installations will be affected by such a decision.

Recommendations:

- Data Server revocation is achieved using method (3) described above, and OEM revocation is achieved using method (a) above. This will probably have the least impact on current stakeholders. It will also ensure that both the S-63 and all of the S-100 security schemes are using a similar revocation procedure
- This will reduce the need for software development to possibly a limited number of active Data Servers, and not affect all the OEMs and their end-user installations. It is

also assumed it can be implemented through administrative procedures within Data Servers. It is envisaged these revocation procedures must be properly defined in Data Server/OEM Agreements.

- It is however recommended that a proper certificate revocation service is established by IHO when a new S-100e6 standard is published. This will give sufficient time to support Exchange Set definition of OCSP Staples and definition of compliance testing requirements. If work is scheduled now to update the Data Server and OEM Agreements it will be recommended to include terms and obligations to in the future support any revocation services to be implemented for Data Servers and OEMs.
- When S-100e6 is introduced with standardised Data Server certificate revocation services, IHO as SA should also consider offering automated Data Server Certificate renewal services similar to what commercial CAs offer. This can reduce the workload on IHO SA staff. It will still be possible to pause renewal of certificates.
- If IHO S-100e6 will uniquely identify all security scheme stakeholders and end-users using Digital Certificates, a properly operated revocation service should be operated by IHO, ref also IEC 63173 SECOM.