## PICS proforma—IEEE Std 1609.2[[1]](#footnote-2)

### Identification

Only the first three items are required for all implementations. Other information may be completed as appropriate in meeting the requirement for full identification.

The terms *name* and *version* should be interpreted appropriately to correspond with a supplier’s terminology (e.g., type, series, model).

|  |  |
| --- | --- |
| Supplier |  |
| Contact point for queries about the PICS |  |
| Implementation name(s) and version(s) |  |
| Other information necessary for full identification, e.g., name(s) and version(s) of the machines and/or operating systems(s), system names |  |

### Protocol summary

|  |  |
| --- | --- |
| Identification of protocol standard | IEEE Std 1609.2 |
| Identification of amendments and corrigenda to this PICS proforma that have been completed as part of this PICS | Amd. : Corr. :  Amd. : Corr. : |
| Have any exception items been required? (See A.1.3; the answer *Yes* means that the implementation does not conform to IEEE Std 1609.2) | □Yes  □No |
| Date of statement (dd/mm/yy) |  |

### Conformance statement

#### Security services

This presents a list of the security functionality that an implementation may claim to support.

| Item | Security configuration (top-level) | Reference | Status | Support |
| --- | --- | --- | --- | --- |
|  | Support secure data service |  | O1 | □Yes □No |
|  | Secure data exchange entity (SDEE) identification | 4.2.2.1 | S1:M | □Yes □No |
|  | Support only one SDEE | 4.2.2.1 | S1.1:C1 | □Yes □No |
|  | Distinguish between SDEEs | 4.2.2.1 | S1.1:C1 | □Yes □No |
|  | Generate secured protocol data unit (SPDU) |  | S1:O2 | □Yes □No |
|  | Create Ieee­­1609­Dot2­­Data containing unsecured data | 4.2.2.2.2 | S1.2:O3 | □Yes □No |
|  | Create Ieee­­1609­Dot2­­Data containing valid Signed­Data | 4.2.2.2.3, 5.2, 5.3.1, 5.3.3, 5.3.7, 6.3.4, 6.3.9, 9.3.9.1 | S1.2:O3 | □Yes □No |
|  | Using a valid HashAlgorithm | 6.3.5 | S1.2.2:M | □Yes □No |
|  | Support signing with hash algorithm SHA-256 | 6.3.5 | S1.2.2:O3a | □Yes □No |
|  | Support signing with hash algorithm SHA-384 | 6.3.5 | S1.2.2:O3a | □Yes □No |
|  | Support signing with other hash algorithm | 6.3.5 | S1.2.2:O | □Yes □No |
|  | Containing a Signed Data payload | 6.3.6 | S1.2.2:M | □Yes □No |
|  | … with payload containing data | 6.3.7 | S1.2.2.2:O4 | □Yes □No |
|  | … with payload containing extDataHash | 6.3.7 | S1.2.2.2: O4 | □Yes □No |
|  | … with generationTime in the security headers | 6.3.9, 6.3.11 | S1.2.2.2: O | □Yes □No |
|  | … with expiryTime in the security headers | 6.3.9, 6.3.11 | S1.2.2.2: O | □Yes □No |
|  | … with generationLocation in the security headers | 6.3.9, 6.3.12 | S1.2.2.2: O | □Yes □No |
|  | … with p2pcdLearningRequest in the security headers | 6.3.9, 6.3.26 | S1.2.2.2: O | □Yes □No |
|  | … with missingCrlIdentifier in the security headers | 6.3.9, 6.3.16 | S1.2.2.2: O | □Yes □No |
|  | … with encryptionKey in the security headers | 6.3.9, 6.3.18 | S1.2.2.2: O | □Yes □No |
|  | … … with a PublicEncryptionKey | 6.3.9, 6.3.18, 6.3.19 | S1.2.2.2.8:O5 | □Yes □No |
|  | … … with a SymmetricEncryptionKey | 6.3.9, 6.3.18, 6.3.20 | S1.2.2.2.8:O5 | □Yes □No |
|  | Support a SignerIdentifier | 6.3.25 | S1.2.2:M | □Yes □No |
|  | … of type self | 6.3.24 | S1.2.2.3:O6 | □Yes □No |
|  | … of type digest | 6.3.27 | S1.2.2.3:O6 | □Yes □No |
|  | … of type certificate | 6.4.2 | S1.2.2.3:O6 | □Yes □No |
|  | … … maximum number of certificates included in the SignerIdentifier | 6.3.25 | S1.2.2.3.2  1:M  > 1:O | Enter number: (  ) |
|  | Support a Signature | 6.3.29 | S1.2.2:M | □Yes □No |
|  | … an ecdsa256Signature | 6.3.30 | S1.2.2.4:O6a | □Yes □No |
|  | … … using NIST p256 | 6.3.30 | S1.2.2.4.1:O7 | □Yes □No |
|  | … … using Brainpool p256r1 | 6.3.30 | S1.2.2.4.1:O7 | □Yes □No |
|  | … … with a x-only *r* value | 6.3.23 | S1.2.2.4.1:O8 | □Yes □No |
|  | … … with a compressed *r* value | 6.3.23 | S1.2.2.4.1:O8 | □Yes □No |
|  | … … with an uncompressed *r* value | 6.3.23 | S1.2.2.4.1:O8 | □Yes □No |
|  | … an ecdsa384Signature using Brainpool p384r1 | 6.3.31 | S1.2.2.4:O6a | □Yes □No |
|  | … … with a x-only *r* value | 6.3.23 | S1.2.2.4.1:O8 | □Yes □No |
|  | … … with a compressed *r* value | 6.3.23 | S1.2.2.4.1:O8 | □Yes □No |
|  | … … with an uncompressed *r* value | 6.3.23 | S1.2.2.4.1:O8 | □Yes □No |
|  | Determine that certificate used to sign data is valid (part of a consistent chain, valid at the current time and location, hasn’t been revoked) | 5.2 | S1.2.2:M | □Yes □No |
|  | Determine that the generation location is consistent with the region in the certificate | 5.2.3.2.2, 6.4.17 | S1.2.2.5:M | □Yes □No |
|  | Support a circularRegion | 6.4.17, 6.4.18 | S1.2.2.5.1:O9 | □Yes □No |
|  | Support a rectangularRegion | 6.4.17, 6.4.20 | S1.2.2.5.1:O9 | □Yes □No |
|  | Maximum number of rectangularRegions supported | 6.4.17, 6.4.20 | S1.2.2.5.1.2  8:M  > 8:O | Enter number: (  ) |
|  | Support a polygonalRegion | 6.4.17, 6.4.21 | S1.2.2.5.1:O9 | □Yes □No |
|  | Maximum number of points in a polygonalRegion | 6.4.17, 6.4.21 | S1.2.2.5.1.3  8:M  > 8:O | Enter number: (  ) |
|  | Support identifiedRegion | 6.4.17, 6.4.22 | S1.2.2.5.1:O9 | □Yes □No |
|  | Maximum number of identifiedRegions supported | 6.4.17, 6.4.22 | S1.2.2.5.1.4:  8:M  > 8:O | Enter number: (  ) |
|  | Support IdentifiedRegion of type CountryOnly | 6.4.22, 6.4.23 | S1.2.2.5.1.4:O10 | □Yes □No |
|  | Support IdentifiedRegion of type CountryAndRegions | 6.4.22, 6.4.24 | S1.2.2.5.1.4:O10 | □Yes □No |
|  | Support IdentifiedRegion of type CountryAndSubregions | 6.4.22, 6.4.25 | S1.2.2.5.1.4:O10 | □Yes □No |
|  | List of supported IdentifiedRegions[[2]](#footnote-3) | 5.2.3.4, 6.4.22 | S1.2.2.5.1.4:M | Provide as Additional Information |
|  | Determine that the certificate has the proper appPermissions | 6.4.8, 6.4.28 | S1.2.2.5: M | □Yes □No |
|  | Maximum number of PsidSsp in the appPermissions sequence | 6.4.8, 6.4.28 | S1.2.2.5.2  8:M  > 8:O | Enter number: (  ) |
|  | Maximum supported length of the full chain (sending) | 5.1.2.2 | S1.2.2.5:  2:M  >2:O | Enter number: (  ) |
|  | Determine that key and certificate used to sign are a valid pair | 5.3.7 | S1.2.2:M | □Yes □No |
|  | Support signing with explicit certificates | 6.4.6 | S1.2.2.5:O11 | □Yes □No |
|  | Support signing with implicit certificates | 5.3.2, 6.4.5 | S1.2.2.5:O11 | □Yes □No |
|  | Generate elliptic curve digital signature algorithm (ECDSA) keypairs using a high-quality random number generator | 5.3.6 | S1.2.2.4.1: M | □Yes □No |
|  | Create Ieee­­1609­Dot2­­Data containing EncryptedData | 4.2.2.3.2, 5.3.4, 6.3.32 | S1.2:O2 | □Yes □No |
|  | Generate Elliptic Curve Integrated Encryption Scheme (ECIES) ephemeral keypairs using a high-quality random number generator | 5.3.4, 5.3.5, 5.3.6 | S1.3.3: M | □Yes □No |
|  | Maximum number of recipients supported | 6.3.32 | S1.2.3  8:M  > 8:O | Enter number: (  ) |
|  | Containing PreSharedKeyRecipientInfo | 6.3.33, 6.3.34 | S1.2.3.2:O12 | □Yes □No |
|  | Containing symmRecipientInfo | 6.3.33, 6.3.35 | S1.2.3.2:O12 | □Yes □No |
|  | Containing certRecipientInfo | 6.3.33, 6.3.36 | S1.2.3.2:O12 | □Yes □No |
|  | Containing signedDataRecipientInfo | 6.3.33, 6.3.36 | S1.2.3.2:O12 | □Yes □No |
|  | Containing rekRecipientInfo | 6.3.33, 6.3.36 | S1.2.3.2:O12 | □Yes □No |
|  | Support public-key encryption | 0 | S1.2.3:O13 | □Yes □No |
|  | … using ECIES-256 | 0 | S1.2.3.4:M | □Yes □No |
|  | … … using NIST p256 | 0 | S1.2.3.4.1:O14 | □Yes □No |
|  | … … using Brainpool p256r1 | 0 | S1.2.3.4.1:O14 | □Yes □No |
|  | Support encrypting to an uncompressed encryption key | 6.3.18 | S1.2.3.4.1:O15 | □Yes □No |
|  | Support encrypting to a compressed encryption key | 6.3.18 | S1.2.3.4.1:O15 | □Yes □No |
|  | Support encrypting to an encryption key included in an explicit cert | 6.3.18 | S1.2.3.4.1:O16 | □Yes □No |
|  | Support encrypting to an encryption key included in an implicit cert | 6.3.18 | S1.2.3.4.1:O16 | □Yes □No |
|  | … using a different algorithm introduced at a later date | 6.3.38 | S1.2.3.4:O | □Yes □No |
|  | Support symmetric encryption | 6.3.39 | S1.2.3:O13 | □Yes □No |
|  | … using AES-128 | 5.3.8, 6.3.39 | S1.2.3.5:M | □Yes □No |
|  | … using a different algorithm introduced at a later date | 6.3.36 | S1.2.3.5:O | □Yes □No |
|  | Receive secured protocol data unit (SPDU) |  | S1:O2 | □Yes □No |
|  | Support preprocessing SPDUs | 4.2.2.3.1 | S1.3.2.3.1, S3.3  S3.4:M | □Yes □No |
|  | Verify Ieee­­1609­Dot2­­Data containing Signed­Data | 4.2.2.3.2, 5.2, 5.3.1, 5.3.3, 5.3.7, 6.3.4, 6.3.9 | S1.3:O17 | □Yes □No |
|  | Using a valid HashAlgorithm |  | S1.3.2:M | □Yes □No |
|  | Verify signed data using HashAlgorithm SHA-256 | 6.3.5 | S1.3.2.1:O17a | □Yes □No |
|  | Verify signed data using HashAlgorithm SHA-384 | 6.3.5 | S1.3.2.1:O17a | □Yes □No |
|  | Verify signed data using another HashAlgorithm | 6.3.5 | S1.3.2.1:O | □Yes □No |
|  | Containing a Signed Data payload | 6.3.6 | S1.3.2:M | □Yes □No |
|  | … with payload containing data | 6.3.7 | S1.3.2.2:O18 | □Yes □No |
|  | … with payload containing extDataHash | 6.3.7 | S1.3.2.2:O18 | □Yes □No |
|  | … with generationTime in the security headers | 6.3.9, 6.3.11 | S1.3.2.2:O | □Yes □No |
|  | … with expiryTime in the security headers | 6.3.9, 6.3.11 | S1.3.2.2:O | □Yes □No |
|  | … with generationLocation in the security headers | 6.3.9, 6.3.12 | S1.3.2.2:O | □Yes □No |
|  | … with missingCertIdentifier in the security headers | 6.3.9, 6.3.26 | S1.3.2.2:O | □Yes □No |
|  | … with missingCrlIdentifier in the security headers | 6.3.9, 6.3.16 | S1.3.2.2:O | □Yes □No |
|  | … with encryptionKey in the security headers | 6.3.9, 6.3.18 | S1.3.2.2:O | □Yes □No |
|  | … … with a PublicEncryptionKey | 6.3.9, 6.3.18, 6.3.19 | S1.3.2.2.8:O19 | □Yes □No |
|  | … … with a SymmetricEncryptionKey | 6.3.9, 6.3.18, 6.3.20 | S1.3.2.2.8:O19 | □Yes □No |
|  | Support a SignerIdentifier | 6.3.25 | S1.3.2:M | □Yes □No |
|  | … of type self | 6.3.24 | S1.2.2.3:O6 | □Yes □No |
|  | … of type digest | 6.3.27 | S1.3.2.3:O20 | □Yes □No |
|  | … of type certificate | 6.4.2 | S1.3.2.3:O20 | □Yes □No |
|  | … … maximum number of certificates included in the SignerIdentifier | 6.3.25 | S1.3.2.3.2  1:M  > 1:O | Enter number: (  ) |
|  | Support a Signature | 6.3.29 | S1.3.2:M | □Yes □No |
|  | … a ecdsa256Signature | 6.3.30 | S1.3.2.4:O20a | □Yes □No |
|  | … … using NIST p256 | 6.3.30 | S1.3.2.4.1:O21 | □Yes □No |
|  | … … using Brainpool p256r1 | 6.3.30 | S1.3.2.4.1:O21 | □Yes □No |
|  | … … with a x-only *r* value | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | … … with a compressed *r* value | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | … … with a compressed *r* value and fast verification | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | … … with a uncompressed *r* value | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | … … with a uncompressed *r* value and fast verification | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | … an ecdsa384Signature using Brainpool p384r1 | 6.3.31 | S1.3.2.4:O20a | □Yes □No |
|  | … … with a x-only *r* value | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | … … with a compressed *r* value | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | … … with a compressed *r* value and fast verification | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | … … with a uncompressed *r* value | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | … … with a uncompressed *r* value and fast verification | 6.3.23 | S1.3.2.4.1:O22 | □Yes □No |
|  | Signed­Data verification fails if the certificate is not valid (part of a consistent chain, valid at the current time and location, hasn’t been revoked) | 5.2, 6.4.2 | S1.3.2:M | □Yes □No |
|  | Reject data based on generation location being inconsistent with certificate | 6.4.8, 6.4.17 | S1.3.2.5:O | □Yes □No |
|  | … using a circularRegion | 6.4.17, 6.4.18 | S1.3.2.5.1:O23 | □Yes □No |
|  | Support a rectangularRegion | 6.4.17, 6.4.20 | S1.3.2.5.1:O23 | □Yes □No |
|  | Maximum number of rectangularRegions supported | 6.4.17, 6.4.20 | S1.3.2.5.1.2  8:M  > 8:O | Enter number: (  ) |
|  | Support a polygonalRegion | 6.4.17, 6.4.21 | S1.3.2.5.1:O23 | □Yes □No |
|  | Maximum number of points in a polygonalRegion | 6.4.17, 6.4.21 | S1.3.2.5.1.4  8:M  > 8:O | Enter number: (  ) |
|  | Support identifiedRegion | 6.4.17, 6.4.22 | S1.3.2.5.1  8:M  > 8:O | Enter number: (  ) |
|  | Maximum number of identifiedRegions supported | 6.4.17, 6.4.22 | S1.3.2.5.1.6:  8:M  > 8:O | Enter number: (  ) |
|  | Support IdentifiedRegion of type CountryOnly | 6.4.22, 6.4.23 | S1.3.2.5.1.6:O24 | □Yes □No |
|  | Support IdentifiedRegion of type CountryAndRegions | 6.4.22, 6.4.24 | S1.3.2.5.1.6:O24 | □Yes □No |
|  | Support IdentifiedRegion of type CountryAndSubregions | 6.4.22, 6.4.25 | S1.3.2.5.1.6:O24 | □Yes □No |
|  | List of supported IdentifiedRegions and the accuracy of each | 5.2.3.4, 6.4.22 | S1.2.2.5.1.4:M | Provide as Additional Information |
|  | Reject data if the certificate does not have the proper appPermissions | 6.4.8, 6.4.28 | S1.3.2.5:M | □Yes □No |
|  | Maximum number of PsidSsp in the appPermissions sequence | 6.4.8, 6.4.28 | S1.3.2.5  8:O  > 8:O | Enter number: (  ) |
|  | Determine that the assuranceLevel is an acceptable level | 6.4.8, 6.4.27 | S1.3.2.5:O | □Yes □No |
|  | Maximum supported length of the full chain (receiving) | 5.1.2.2 | S1.2.2.5:  2:M  >2:O | Enter number: (  ) |
|  | Support verifying SPDUs signed with explicit authorization certificates | 6.4.5 | S1.3.2:O25 | □Yes □No |
|  | Support verifying SPDUs signed with implicit authorization certificates | 5.3.2, 6.4.5 | S1.3.2:O25 | □Yes □No |
|  | Support explicit certificate authority (CA) certificates | 6.4.2, 6.4.6 | S1.3.2:M | □Yes □No |
|  | Support receiving implicit CA certificates | 6.4.2, 6.4.5 | S1.3.2:O | □Yes □No |
|  | Signed­Data verification fails in the following circumstances: | 6.3.4 | S1.3.2:M | □Yes □No |
|  | … SPDU-Parsing: Invalid Input | 6.3.4 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Parsing: Unspported critical information field | 6 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Parsing: Certificate not found | 4.3, 6.3.13, 6.3.14, 6.3.15 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Parsing:Generation time not available | 4.3, 6.3.13, 6.3.14, 6.3.15 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Parsing:Generation location not available | 4.3, 6.3.13, 6.3.14, 6.3.15 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Certificate-Chain: Not enough information to construct chain | 5.1.2 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Certificate-Chain: Chain ended at untrusted root | 5.1.2 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Certificate-Chain: Chain was too long for implementation | 5.1.2 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Certificate-Chain: Certificate revoked | 5.1.2 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Certificate-Chain: Overdue CRL | 5.1.2 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Certificate-Chain: Inconsistent expiry times | 5.1.2 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Certificate-Chain: Inconsistent start times | 5.1.2 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Certificate-Chain: Inconsistent chain permissions | 5.1.2 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Crypto: Verification failure | 5.3.1 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Consistency: Future certificate at generation time | 5.2.3 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Consistency: Expired certificate at generation time | 5.2.3 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Consistency: Expiry date too early | 5.2.3 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Consistency: Expiry date too late | 5.2.3 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Consistency: Generation location outside validity region | 5.2.3 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Consistency: Unauthorized PSID | 5.2.3 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Internal-Consistency: Expiry time before generation time | 6.4.8, 6.4.14, 5.2.3 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Internal-Consistency: extDataHash doesn’t match | 5.2.3 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Local-Consistency: PSIDs don’t match | 5.2.3 | S1.3.2.10:O | □Yes □No |
|  | … SPDU-Local-Consistency: Chain was too long for SDEE | 5.2.3 | S1.3.2.10:M | □Yes □No |
|  | … SPDU-Relevance: SPDU Too Old | 5.2.4 | S1.3.2.10:O | □Yes □No |
|  | … SPDU-Relevance: Future SPDU | 5.2.4 | S1.3.2.10:O | □Yes □No |
|  | … SPDU-Relevance: Expired SPDU | 5.2.4 | S1.3.2.10:O | □Yes □No |
|  | … SPDU-Relevance: SPDU Too Distant | 5.2.4 | S1.3.2.10:O | □Yes □No |
|  | … SPDU-Relevance: Replayed SPDU | 5.2.4 | S1.3.2.10:O | □Yes □No |
|  | Decrypt Ieee­­1609­Dot2­­Data containing EncryptedData | 4.2.2.3.3, 5.3.5, 6.3.32 | S1.3:O17 | □Yes □No |
|  | Generate ECIES keypairs using a high-quality random number generator | 5.3.4, 5.3.5, 5.3.6 | S1.3.3: M | □Yes □No |
|  | Maximum number of RecipientInfos supported in an incoming EncryptedData | 6.3.32 | S1.3.3:  8:M > 8:O | Enter number: (  ) |
|  | Containing symmRecipientInfo | 6.3.33 | S1.3.3.2:O26 | □Yes □No |
|  | Containing certRecipientInfo | 6.3.33 | S1.3.3.2:O26 | □Yes □No |
|  | Containing signedDataRecipientInfo | 6.3.33 | S1.3.3.2:O26 | □Yes □No |
|  | Containing rekRecipientInfo | 6.3.33 | S1.3.3.2:O26 | □Yes □No |
|  | Containing pskRecipientInfo | 6.3.33, 6.3.36 | S1.3.3.2:O26 | □Yes □No |
|  | Support decrypting using a public-key algorithm | 0 | S1.3.3:O27 | □Yes □No |
|  | … using ECIES-256 | 0 | S1.3.3.3:M | □Yes □No |
|  | … … using NIST p256 | 0 | S1.3.3.3:O28 | □Yes □No |
|  | … … using Brainpool p256r1 | 0 | S1.3.3.3:O28 | □Yes □No |
|  | … using a different algorithm introduced at a later date | 6.3.38 | S1.3.3.3:O | □Yes □No |
|  | Support decrypting using a symmetric algorithm | 6.3.39 | S1.3.3:O27 | □Yes □No |
|  | ... using AES-128 | 6.3.39 | S1.3.3.4:M | □Yes □No |
|  | … using a different algorithm introduced at a later date | 6.3.36 | S1.3.3.4:O | □Yes □No |

#### Certificate revocation list (CRL) verification entity

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Security configuration (top-level) | Reference | Status | Suppport |
|  | Support CRL Validation Entity | 7 | O1 | □Yes □No |
|  | Correctly verify received CRL | 7.4 | S2:M | □Yes □No |
|  | …using hash ID-based revocation | 5.1.3.5 | S2.1:O29 | □Yes □No |
|  | … of type fullHashCrl | 7.3.2 | S2.1.1:M | □Yes □No |
|  | … of type deltaHashCrl | 7.3.2 | O | □Yes □No |
|  | … using linkage-based revocation | 5.1.3.4 | S2.1:O29 | □Yes □No |
|  | … of type fullLinkedCrl | 7.3.2 | S2.1.2:M | □Yes □No |
|  | … of type deltaLinkedCrl | 7.3.2 | O | □Yes □No |
|  | … containing individual linkage values | 7.3.6 | S2.1.2:M | □Yes □No |
|  | … containing group linkage values | 7.3.6 | O | □Yes □No |

#### Peer-to-peer certificate distribution (P2PCD) functionality

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Security configuration (top-level) | Reference | Status | Support |
|  | Support P2PCD | 8 | O | □Yes □No |
|  | Number of supported SDEEs | 8.2.6 | S3.3:  1:O  > 1:O | Enter number: (  ) |
|  | Support out-of-band P2PCD operations | 8 | S3:O30 | □Yes □No |
|  | Support SSME and SDS operations for out-of-band P2PCD in the requester role | 8.2.4.1.1 | S3.2:O | □Yes □No |
|  | Under at least one condition, trigger request processing on receiving a trigger SPDU | 8.2.4.1.1 | S3.3:M | Enter description of at least one condition under which request processing is triggered ( ) |
|  | Do not trigger request processing on receiving a trigger SPDU for which a request is already active | 8.2.4.1.1 | S3.3:M | □Yes □No |
|  | Number of simultaneously active P2PCD learning requests | 8.2.4.1.1, 8.2.6 | S3.3:  1:O  > 1:O | Enter number: (  ) |
|  | When request processing is triggered, include a P2PCD learning request in the next SPDU for the trigger SDEE except in the following exception cases | 8.2.4.1.1 | S3.3: M | □Yes □No |
|  | Do not include a P2PCD learning request if a learning request for the same certificate has been received within p2pcd\_observedRequestTimeout | 8.2.4.1.1 | S3.3.4:O | □Yes □No |
|  | Only include one P2PCD learning request no matter how many learning requests have been triggered | 8.2.4.1.1 | S3.3.4: M | □Yes □No |
|  | Receive notifications from a P2PCDE that a P2PCD learning response has been received and use those to update the list of known certificates. | 8.2.4.1.1 | S3.3: M | □Yes □No |
|  | Support SSME and SDS operations for out-of-band P2PCD in the responder role | 8.2.4.2.2 | S3:O30 | □Yes □No |
|  | Trigger response processing on receiving a P2PCD learning request | 8.2.4.2.2 | S3.4:M | □Yes □No |
|  | Number of simultaneously active P2PCD learning responses | 8.2.4.2.2, 8.2.6 | S3.4:  1:O  > 1:O | Enter number: (  ) |
|  | Do not trigger response processing if less than p2pcd\_responseActiveTimeout has passed since last triggered | 8.2.4.2.2 | S3.4: M | □Yes □No |
|  | Trigger sending response after random backoff time unless threshold number of responses have been observed | 8.2.4.2.2 | S3.4: M | □Yes □No |
|  | Increment number of responses observed based on input from P2PCDE | 8.2.4.2.2 | S3.4: M | □Yes □No |
|  | Support P2PCDE operations for P2PCD | 8.2.4.2.2 | S3:O30 | □Yes □No |
|  | Receive responses and provide to SSME | 8.2.4.1.1, 8.2.4.2.2, 8.3.1 | S3.5: M | □Yes □No |
|  | Send responses when triggered by SSME | 8.2.4.2.2, 8.3.1 | S3.5: O | □Yes □No |
|  | Send responses over WSMP | 8.2.4.2.2 | S3.5.2: M | □Yes □No |
|  | Support inline P2PCD operations | 8 | S3:O30 | □Yes □No |
|  | Support inline P2PCD requester operations | 8.2.4.1.2 | S3.6:O | □Yes □No |
|  | Support inline P2PCD responder operations | 8.2.4.2.3 | S3.6:M | □Yes □No |

1. Copyright release for PICS proforma: Users of this standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS. [↑](#footnote-ref-2)
2. This list might or might not include an indication of the accuracy of the internal representation of each identified region. [↑](#footnote-ref-3)