## IEEE 1609.2 security profile proforma[[1]](#footnote-2)

### Instructions for completing the IEEE 1609.2 security profile proforma

The developer of an IEEE 1609.2 security profile may specify the profile by completing this proforma. The main part of the proforma is a fixed questionnaire, divided into entries. Answers to the questionnaire items are to be provided in the center column, and any elaboration necessary is to be provided in the rightmost column. The entries in the value column are either drawn from the list of permitted values given above, or are “n/a”.

### IEEE 1609.2 security profile proforma

#### IEEE 1609.2 security profile identification

|  |  |  |
| --- | --- | --- |
| Field | Value | Notes |
| *Name* |  |  |
| *PSIDs* |  |  |
| *Other considerations* |  |  |

#### Sending

|  |  |  |
| --- | --- | --- |
| Field | Value | Notes |
| *Sign Data* |  |  |
| *Signed Data in Payload* |  |  |
| *External Data* |  |  |
| *External Data Source* |  |  |
| *External Data Hash Algorithm* |  |  |
| *Set Generation Time ­­in­ Security Headers* |  |  |
| *Set Generation Location in Security Headers* |  |  |
| *Set Expiry Time ­in ­­Security ­Headers* |  |  |
| *Signed SPDU Lifetime* |  |  |
| *Signer Type Self* |  |  |
| *Signer ­Identifier ­Policy ­Type* |  |  |
| *Simple­ Signer ­Identifier ­Policy: Minimum Inter ­Cert­ Time* |  |  |
| *Simple­ Signer ­Identifier Policy: Exceptions* |  |  |
| *Simple­ Signer ­Identifier Policy: Signer Identifier Cert ­Chain Length* |  |  |
| *Text­ Signer­ Identifier­ Policy* |  |  |
| *Sign With Fast Verification* |  |  |
| *EC Point Format* |  |  |
| *p2pcd\_flavor* |  |  |
| *p2pcd\_maxResponseBackoff* |  |  |
| *p2pcd\_responseActiveTimeout* |  |  |
| *p2pcd\_requestActiveTimeout* |  |  |
| *p2pcd\_observedRequestTimeout* |  |  |
| *p2pcd\_currentlyUsedTriggerCertificateTime* |  |  |
| *p2pcd\_responseCountThreshold* |  |  |
| *Repeat Signed SPDUs* |  |  |
| *Time Between Signing* |  |  |
| *Encrypt Data* |  |  |

#### Receiving

|  |  |  |
| --- | --- | --- |
| Field | Value | Notes |
| *Use Preprocessing* |  |  |
| *Verify Data* |  |  |
| *Maximum Full Certificate Chain Length* |  |  |
| *Relevance: Replay* |  |  |
| *Relevance: Generation Time in Past* |  |  |
| *Validity Period* |  |  |
| *Relevance: Generation Time in Future* |  |  |
| *Acceptable Future Data Period* |  |  |
| *Generation Time Source* |  |  |
| *Relevance: Expiry Time* |  |  |
| *Expiry Time Source* |  |  |
| *Consistency: Generation Location* |  |  |
| *Relevance: Generation Location Distance* |  |  |
| *Validity Distance* |  |  |
| *Generation Location Source* |  |  |
| *Additional Geographic Consistency Conditions* |  |  |
| *Identified Region Representation Accuracy* |  |  |
| *Overdue CRL Tolerance* |  |  |
| *Relevance: Certificate Expiry* |  |  |
| *Encrypted Data* |  |  |

#### Security management

|  |  |  |
| --- | --- | --- |
| Field | Value | Notes |
| *Signing Key Algorithm* |  |  |
| *Encryption Algorithm* |  |  |
| *Implicit or Explicit Certificates* |  |  |
| *EC Point Format* |  |  |
| *Supported ­Geographic ­­Regions* |  |  |
| *Maximum Full Certificate ­Chain­ Length* |  |  |
| *Use Individual Linkage ID* |  |  |
| *Use Group Linkage ID* |  |  |
| *Signature Algorithms in Chain or CRL* |  |  |

#### Other

|  |  |  |
| --- | --- | --- |
| Field | Value | Notes |
| *Fields that may be subject to policy update* |  |  |

1. Copyright release for 1609.2 security profile proformas: Users of this standard may freely reproduce the 1609.2 security profile proforma in this annex so that it can be used for its intended purpose and may further publish the completed 1609.2 security profile. [↑](#footnote-ref-2)