Optional package for 3S signing using asymmetric keys

The 3S signing, which is comprised of an asymmetric endorsement key pair, a certificate and a 3S signing functionality, enables a 3S instance to cryptographically prove its identity to external entities.

It is a required capability for different use cases, including secure provisioning of the 3S in a non-secure environment, e.g. further provisioning of a device (containing an SoC with a 3S) during manufacturing or over the air (OTA) after such device has been shipped.

P_Endorsement_Key

Definition:

The 3S stores an asymmetric key pair to enable endorsement. This key pair can either be unique per TOE instance or shared among multiple TOE instances (e.g. group attestation keys that offer a level of anonymity).

The asymmetric key pair can be either (1) generated by each TOE instance or (2) injected into the TOE.

P_Endorsement_Key defines the policy for the generation and protection of the endorsement key pair.

Description:

The P_Endorsement_Key policy requires the TOE to ensure that:

- The TOE protects the stored private key against leakage.
- The TOE protects the stored asymmetric key pair against manipulation.
- There is a guaranteed protection and seclusion on the use of the stored private key within the TOE boundary (e.g. limited to 3S signing functionality).
- There is an assurance as to the probability of key pair duplication between different 3S instances, when generated either by the TOE or during manufacturing prior to injection. For example, an individual endorsement key may have a cryptographic negligible probability while a group key may have a non-negligible probability.
- If the key pair is injected into the TOE, the injection process includes protection against leakage and manipulation of the key pair, at the injection source and in transit to the TOE.

Notes:

The policy covers any asymmetric key scheme and does not specify a certain implementation.

The security target will describe:

- The choice of on-device or off device key generation and injection.
- The level of key uniqueness assurance (i.e. probability of having duplicate key pairs).

P_Endorsement_Certificate

Definition:

The 3S also includes an endorsement certificate from a certificate issuer, enabling authentication of the public endorsement key.

P_Endorsement_Certificate defines the policy for the provisioning and protection of the endorsement certificate.

Description:

The P_Endorsement_Certificate policy requires the TOE to ensure that:

- The certificate injection process includes protection against manipulation at the certificate issuer source and in transit to the TOE.
- The certificate injection process includes protection against forgery of the certificate issuer.
- The stored certificate is protected against manipulation.

Notes:

The policy covers any certificate scheme or issuer and does not specify a certain implementation.

P_TOE_Signing

Definition:

The TOE offers signing functionality utilizing the endorsement keys and the endorsement certificate.

The TOE signing functionality is available to users, i.e. 3S applications outside the TOE boundary.

Description:

The P_TOE_Signing policy requires the TOE to ensure that:

- 3S signing functionality protects TOE users from forgery. E.g. prevent a TOE user from creating a signature identical to a signature created by another TOE user, by including the identity of the user in the signature.

Notes:

The policy covers any signing functionality and does not specify a certain implementation.