P_Endorsement_Key

Definition:

The 3S stores an asymmetric key pair to enable further secure provisioning in a non-secure environment, e.g. during device manufacturing or over the air. 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:

This policy requires the TOE to ensure that:

- The private key is protected against leakage.
- The key pair is protected against manipulation.
- There is a guaranteed protection and seclusion on the use of the private key within the TOE boundary.
- There is an assurance as to the probability of key pair duplication.
- If the key is injected into the TOE, the injection process includes protection against leakage and manipulation of the key pair, from 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.
- 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:

This policy requires the TOE to ensure that:

- The certificate injection process includes protection against manipulation and forgery of the certificate issuer and transit to the TOE.
- The 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 within 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.

Notes:

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