



Enhanced Privacy ID: Hardware Attestation Beyond TPM

Ernie Brickell, Chief Security Architect, Intel Corporation

Jiangtao Li, Research Scientist & Security Architect, Intel Labs

Presented by Jiangtao Li (jiangtao.li@intel.com)

TRUST workshop on Anonymous Digital Signatures (AnonSig'10)

Overview of Enhanced Privacy ID (EPID)

- Direct Anonymous Attestation (DAA)
 - A crypto scheme for providing anonymous signatures
 - DAA is designed specifically for the Trusted Platform Module (TPM)
 - RSA based DAA scheme adopted by TCG TPM Spec v1.2
- EPID is an extension of DAA
 - Flexible key generation and signature creation options
 - Additional revocation capabilities
 - Support both RSA and pairing based schemes
- Applications of EPID beyond TPM
 - Hardware authentication without revealing identity
 - Anonymous attestation of hardware-based trusted platforms
 - E-commerce, content protection, identity cards

Motivation Example: Hardware Attestation

Hey, I am trusted platform. Here is the proof and a measure of my environment. Please give me your protected resource.



A Platform

The proof convinces me that the platform is indeed trusted. I trust the platform to provide the measurement of the environment. I trust the environment to protect my resource. I will send you the resource.

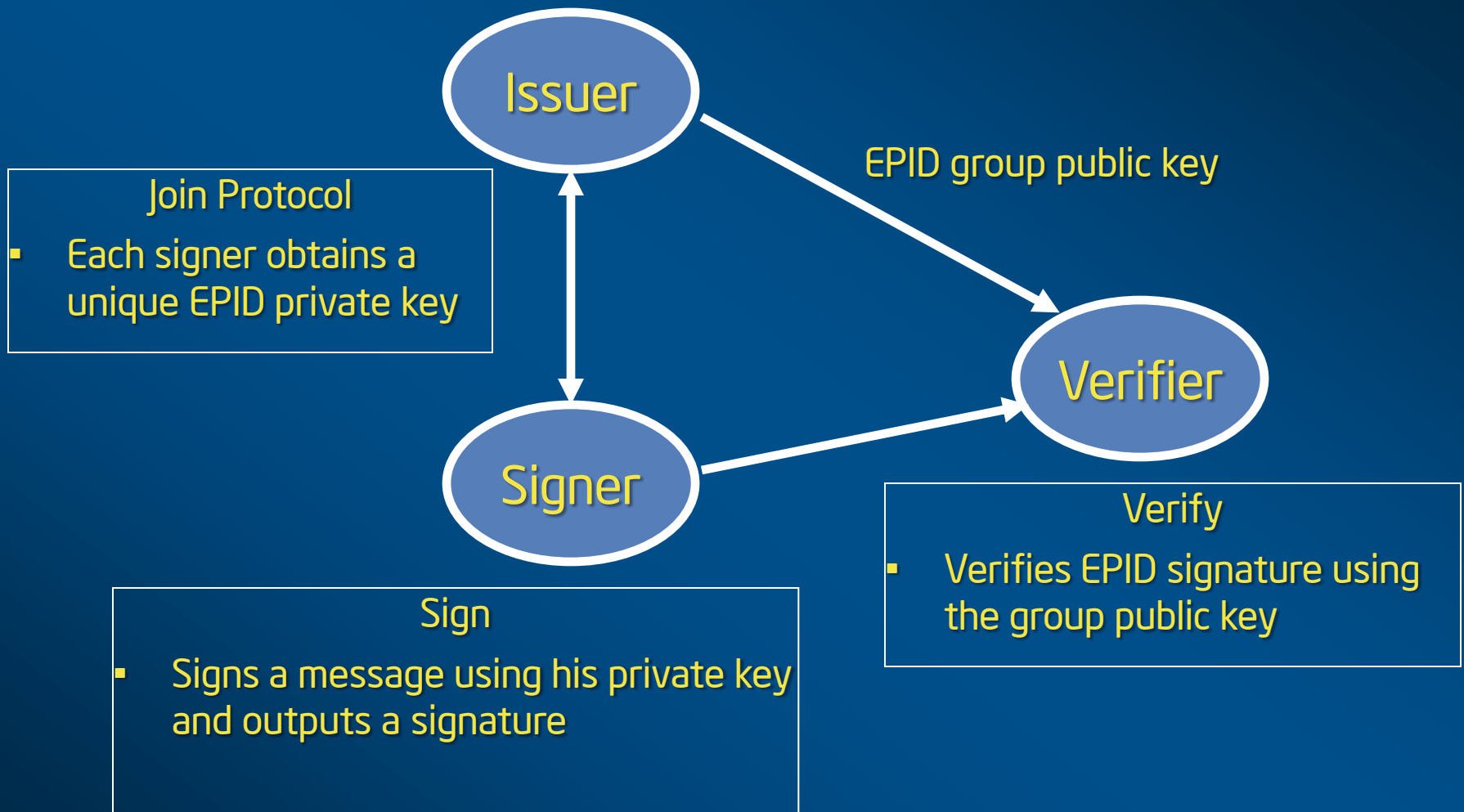


A Service Provider

Attestation

- The platform can be a laptop, smart phone, netbook, smart card, or TPM.
- The service provider does not need to know or care the identity of the platform, it only needs know whether the platform is trusted.
- DAA/EPID can be used authentication and attestation while preserving the privacy of the platform.

What is EPID



Privacy Features of DAA/EPID

- EPID signatures are anonymous
- EPID signatures are untraceable
 - Nobody including the issuer can open an EPID signature and identify the signer of the signature
 - This is the main difference between group signature schemes
 - This feature provides maximum privacy to the end users
- Two modes of EPID signatures
 - Random base: signatures are unlinkable
 - Name base: multiple signatures presented to same verifier are linkable, but still unlinkable for different verifiers
- Signer and verifier may negotiate mode

Key Generation Options

- Interactive join
 - Signer runs a join protocol with Issuer to obtain a private key
 - Signer's private key is unknown to the issuer
- Non-interactive join
 - Issuer generates all private keys offline
 - Issuer delivers a unique private key to each signer
 - Issuer deletes the private keys after provisioning
- Motivation for offline key generation
 - Efficient and scalable
 - Impossible to run interactive join protocol at manufacturing line
 - For hardware authentication (instead of user authentication), issuer has no incentive to impersonate a signer

Performance Optimizations for Signer

- Outsourcing the signing operation
 - Signer can outsource most of the signing operation to a helper
 - The helper can assist the signer on signature computation but cannot create signatures himself
 - In DAA context, signer is TPM and helper is host platform
- Pre-computation
 - Most of the computation in a signature generation can be pre-computed before knowing what message is going to be signed
- These optimizations are optional

Revocations in EPID

- Private key revocation (same as in DAA)
 - If a private key is corrupted and is published widely over the Internet, the issuer can revoke the private key
 - Revocation check is performed locally by the verifier
- Signature based revocation
 - If a private key is corrupted and is used in a malicious transaction, the issuer can revoke the key that signed the transaction without knowing the key
 - In signing algorithm, each signer needs to prove in zero-knowledge that he did not create the revoked signatures

EPID Scheme for Bilinear Maps

- EPID scheme derived from
 - Boneh, Boyen, and Shacham group signature scheme (2004)
 - Furukawa and Imai group signature scheme (2006)
- Security assumptions
 - Strong Diffie-Hellman (q-SDH) assumption for security
 - Decisional Diffie-Hellman (DDH) assumption for anonymity
- Efficiency of EPID scheme
 - Private key is 128-byte on 256-bit Barreto-Naehrig curve
 - Signature is 352-byte on 256-bit Barreto-Naehrig curve
 - Sign takes 4 EXPs
 - Verify takes 1 pairing + 3 EXPs
 - Each revoked private key, verifier computes 1 EXP
 - Each revoked signature, signer computes 3 EXPs, verifier computes 2 EXPs

Intel® Enhanced Privacy ID

- Intel implements EPID in Intel P55 Ibex Peak chipsets
 - Based on bilinear maps
 - Private keys are generated offline in a secure facility
 - Private keys are provisioned to chipsets at manufacturing line
 - Signatures are generated by chipset w/o help from host
- We expect a wide variety of applications to launch over the next couple of years to utilize this EPID scheme
- EPID signature generation takes about 1 second
- EPID signature verification takes less than 100 ms



Backup

References of EPID

- E. Brickell and J. Li. Enhanced Privacy ID from bilinear pairing. Cryptology ePrint Archive. <http://eprint.iacr.org/2009/095>.
- E. Brickell and J. Li. Enhanced Privacy ID: A remote anonymous attestation scheme for hardware devices. Intel Technology Journal: Advances in Internet Security, 13(2), 2009.
- E. Brickell and J. Li. A Pairing-Based DAA Scheme Further Reducing TPM Resources. TRUST'10, June 2010.
- E. Brickell and J. Li. Enhanced Privacy ID from Bilinear Pairing for Hardware Authentication and Attestation. IEEE PASSAT'10, August 2010.

Cryptographic Background

- Bilinear maps
 - Let G_1 and G_2 be two multiplicative groups of prime order p
 - Let g_1 and g_2 be the generators of G_1 and G_2 , respectively
 - We say $e : G_1 \times G_2 \rightarrow G_T$ if
 1. For $u \in G_1, v \in G_2$, any integers a, b , $e(u^a, v^b) = e(u, v)^{ab}$
 2. $e(g_1, g_2) \neq 1$
 3. There exists an efficient algorithm for compute $e(u, v)$
- Zero-Knowledge (ZK) Proof of knowledge
 - E.g., $PK\{ (x) : T_1 = g_1^x \wedge T_2 = g_2^x \}$
 - x is only known to the prover
 - T_1, T_2, g_1, g_2 are known to both the prover and verifier
 - The verifier is convinced the equations hold after the proof

EPID Scheme in Details

■ Setup

- Chooses a bilinear group pair G_1 and G_2 of prime order p
- Let $e: G_1 \times G_2 \rightarrow G_T$ be a computable bilinear map function
- Chooses $g_1, h_1, h_2 \leftarrow G_1$ and $g_2 \leftarrow G_2$
- Chooses a random $\gamma \in \mathbb{Z}_p$, and computes $w = g_2^\gamma$
- The group public key is (g_1, g_2, h_1, h_2, w)
- The issuer's private key is γ

■ Non-interactive Join

- Issuer chooses a random $f, x \leftarrow \mathbb{Z}_p$
- Issuer computes $A = (g_1 h_1^f)^{1/(x+\gamma)}$
- (A, x, f) is Signer's private key

Note: A valid private key satisfies equation $e(A, g_2^{x+w}) = e(g_1 h_1^f, g_2)$

EPID Scheme in Details (cont.)

■ Sign

- Chooses B randomly in G_1 or computes $B = \text{Hash}(\text{verifier's bsn})$
- Computes $K = B^f$ and
$$\text{PK}\{ (A, x, f) : e(A, g_2^{xw}) = e(g_1 h_1^f, g_2) \wedge K = B^f \}$$
- For each revoked signature which contains a (B_i, K_i) pair, computes
$$\text{PK}\{ (f) : K = B^f \text{ and } K_i \neq B_i^f \}$$

■ Verify

- Verifies B and $K \in G_1$
- Verifies the ZK proof
$$\text{PK}\{ (A, x, f) : e(A, g_2^{xw}) = e(g_1 h_1^f, g_2) \wedge K = B^f \}$$
- Verifies that $K \neq B^{f_i}$ for each f_i in revoked private keys
- For each (B_i, K_i) pair from revoked signatures, verifies
$$\text{PK}\{ (f) : K = B^f \text{ and } K_i \neq B_i^f \}$$