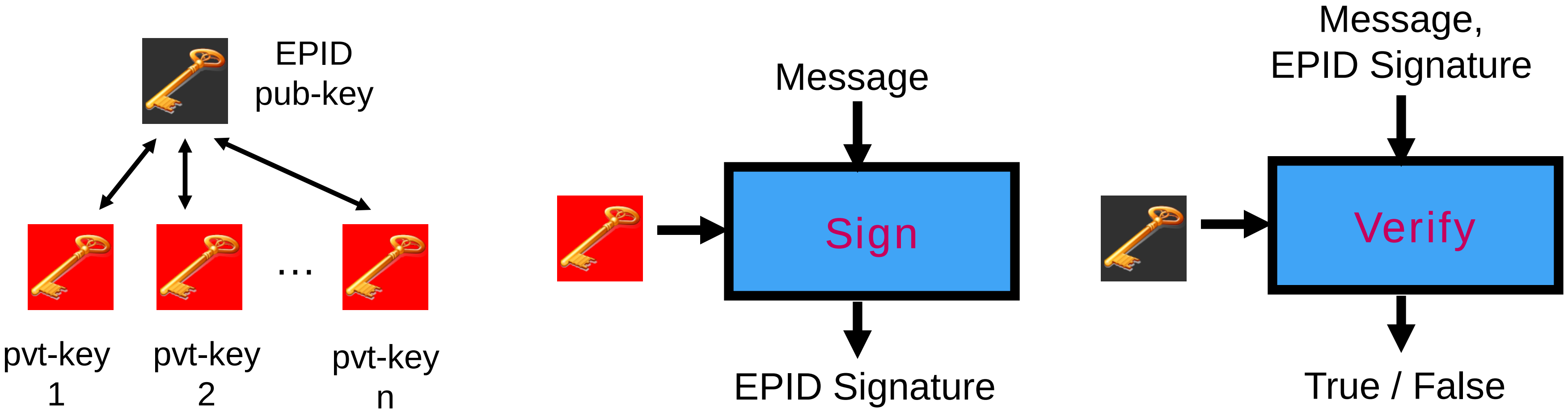
Enhanced Privacy ID (EPID)

Ernie Brickell and Jiangtao Li
Intel Corporation

Agenda

- EPID overview
- EPID usages
  - Device Authentication
  - Government Issued ID
- EPID performance and standardization efforts

Overview of EPID



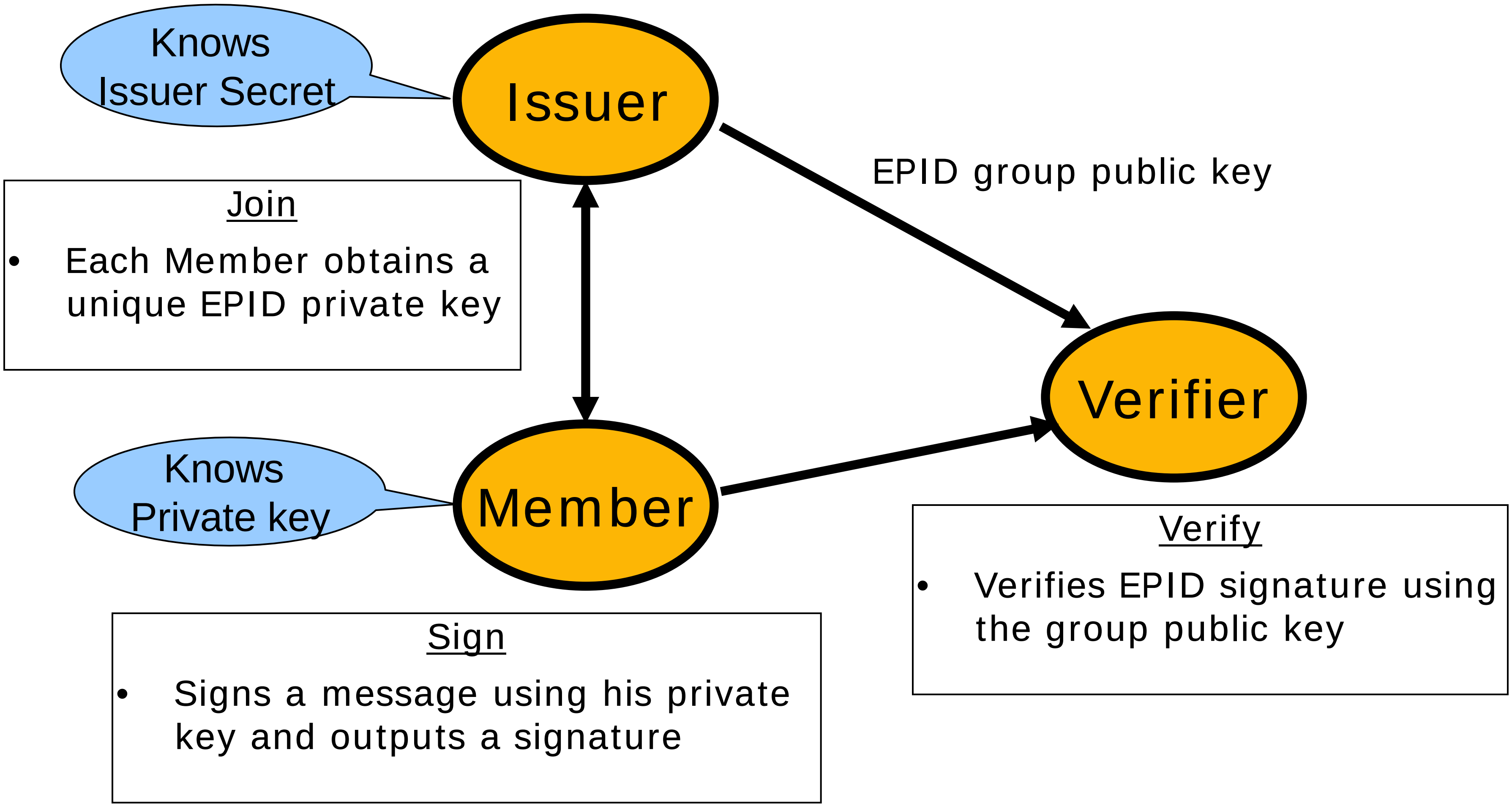
- EPID is a digital signature scheme with special properties
  - One group public key corresponds to multiple private keys
  - Each unique private key can be used to generate a signature
  - Signature can be verified using the group public key

Enhanced Privacy ID (EPID)

- Direct Anonymous Attestation (DAA)
  - A crypto scheme for providing anonymous signatures
  - DAA is designed specifically for 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
  - Pairing based EPID scheme has improved efficiency

What is EPID



Join

- Each Member obtains a unique EPID private key

Sign

- Signs a message using his private key and outputs a signature

Verify

- Verifies EPID signature using the group public key

Privacy Features of DAA/EPID

- EPID key issuing can be blinded
  - Issuer does not need to know Member Private Key
- EPID signatures are anonymous
- EPID signatures are untraceable
  - Nobody including the issuer can open an EPID signature and identify the member
  - This is the main difference between group signatures
- Unlinkability property depends upon Base
  - Signature includes a pseudonym B^f where
    - B is base chosen for a signature and revealed during the signature
    - f is unique per member and private
  - Random base: Pseudonym R^f where R is random
    - signatures are unlinkable
  - Name base: Pseudonym N^f all where N is name of verifier
    - Signatures still unlinkable for different verifiers
    - Signatures using common N are linkable

Revocations in EPID

- Private key revocation (Revealed Key List)
  - Ex: Private key is corrupted and is published
  - Revocation check performed by verifier

- Verifier Local Revocation using name base
  - Ex: Verifier can revoke a Pseudonym for his name (N^f)
  - Revocation check performed by verifier

- Signature based revocation (Signature Revocation List)
  - Issuer and/or verifier decide that they no longer want to accept signatures from whatever signed a “revoked” message with pseudonym B^f
  - For each future signature,
    - Member signs as normal
    - Member proves he didn’t sign the revoked message
      - Member proves his pseudonym with base B is not B^f
  - Retains same anonymity and unlinkability properties

More on signature based revocation

- Signature Revoke list
  - $K_i = B_i^{fi}$ for many pseudonyms
- Member produces a pseudonym $K = B^f$ in a signature
- The Member performs a Not My Pseudonym Proof, for each pseudonym in Signature Revoke list, i.e., for each (B_i, K_i), the member proves that $K_i \neq B_i^f$
- Signature Revoke list signed by Revocation authority and checked by Member device

Agenda

- EPID overview
- EPID usages
  - Device Authentication
  - Government Issued ID
- EPID performance and standardization efforts

Uses of EPID – Device Authentication

- Device authentication
  - Prove: This is an approved device (and SW environment) for this purpose
  - Only reason to revoke a device EPID key is if the EPID key has been physically removed from the device
- Example: Device which generates, stores, and uses keys in a protected environment
  - Used to establish login keys with many institutions
  - Institution knows that login keys are protected
  - Member knows that a compromise at one institution does not affect his security or privacy at any other institution

Use Name Base or Random Base?

- Issue with Random Base
  - A single HW reverse engineered key could be used to get many different accounts with the same institution
- Recommendation: Use Name Base for registration for an account
  - Ex:
    - CitiBank
      - Permanent Name Base is okay
    - Netflix
      - Could change the Name Base daily
        - Reverse engineered key cannot be used by two different platforms during the same day

Example use of signature based revocation

- Member registers with CitiBank
  - EPID Signs a message with pseudonym (CitiBank^f)
    - {Here is a public verification key V where my device securely holds the corresponding private key *[S]*}
- Suppose *S* is found in a piece of malware
- The pair of the above EPID signature and *S* is convincing evidence that the device has been reverse engineered
- Then the pseudonym (CitiBank^f) can be revoked and added to signed Signature Revoke List

Uses of EPID – ID Card

- Government issued ID card
  - Only prove minimal necessary information
    - Age
    - Not on watch list
  - Random base sufficient for many instances
  - Multiple reasons for revocation and/or watch of EPID key
- Potential watch list
  - During Issuing, a random base pseudonym established (R^f)
  - If individual ever put on government watch list, (R^f) is put on watch list
  - Watch list used as revocation list
  - Watch list also signed by Revocation Authority

Revocation (and Watch) List

- Revocation List Verification Public Key
  - Embedded in EPID token
  - Verifies revocation list was signed by Revocation Authority
  - Keeps the EPID Token from responding to an unauthorized revocation list
- Local Audit of Revocation / Watch
  - User Token will know if his private key is ever on a revocation /watch list
  - User would not know unless User Token informed the user
  - Policy enforced by the user token determines when the user is informed
    - A Max time could be in the user token.

Comparisons vs. PKI and DAA

	PKI	DAA with Random B	DAA with Named B	EPID	Group Signatures
Unique Public Key	Yes	No	No	No	No
Unique Private Key	Yes	Yes	Yes	Yes	Yes
Anonymous	No	Yes	Yes	Yes	Yes
Untraceable	No	Yes	Yes	Yes	No
Unlinkable	No	Yes	No	Yes	Yes
Check for revealed private key	Yes	Yes	Yes	Yes	Scheme specific
Revoke the signer of a signature	Yes	No	Yes	Yes	Yes
Member Auditability of Revocation	No	No	No	Yes	No

Agenda

- EPID overview
- EPID usages
- EPID performance and standardization efforts

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
  - Sign takes 4 multi-exponentiations (EXPs)
    - Less than 20ms with 256-bit BN curve
  - 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
    - Less than 10ms per signature
  - Almost all signing and revoke signature can be pre-computed before message to be signed is known

Re-issuing

- If Revealed list or Signature Revocation List gets too big, then Member can join a new group.
  - Member proves to Issuer that he is not revealed or on Signer Revocation List
  - Issuer then provides Member a membership in a new group
  - Probably use Issuer Pseudonym in the reissuing
    - Protects against a compromised key that is not yet revealed

Standardization

- ISO – EPID included in
  - ISO/IEC 20008: Anonymous Digital Signatures
    - Full EPID scheme included in 1st committee draft of ISO 20008-2
  - ISO/IEC 20009: Anonymous Entity Authentication
    - EPID based key exchange protocol (DAA-SIGMA protocol) included in 1st committee draft of ISO 20009-2
- TCG – DAA (EPID without signature revocation) included in TPM 2.0
  - TPM portion of the EPID signing algorithm standardized in TPM spec v0.86
  - Host portion of the EPID signing algorithm to be standardized in TCG PC client specification

Backup

Cryptographic Assumptions of EPID

- q-SDH assumption: Given (g_1, g_1^{r}, $g_1^{r\wedge 2}$, ..., $g_1^{r\wedge q}$, g_2, g_2^{r}), where g_1, g_2 are generators of G_1, G_2, respectively, it is hard to compute an (A, x) pair such that $A = g_1^{1/(x+r)}$
- DDH assumption: it is hard to distinguish two distributions (g^a, g^b, g^{ab}) and (g^a, g^b, g^c), where a, b, c are randomly chosen from Z_q.

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. A Pairing-Based DAA Scheme Further Reducing TPM Resources. TRUST 2010.
- E. Brickell and J. Li. Enhanced Privacy ID from Bilinear Pairing for Hardware Authentication and Attestation. IEEE PASSAT 2010.
- E. Brickell and J. Li. Enhanced Privacy ID from Bilinear Pairing for Hardware Authentication and Attestation. IJIPSI 2011.
- Other EPID related publications
  - E. Brickell and J. Li. ACM WPES 2007
  - E. Brickell, L. Chen, and J. Li. TRUST 2008
  - E. Brickell, L. Chen, and J. Li. IJIS 2009
  - E. Brickell and J. Li. Intel Technology Journal 2009
  - J. Walker and J. Li. INTRUST 2010