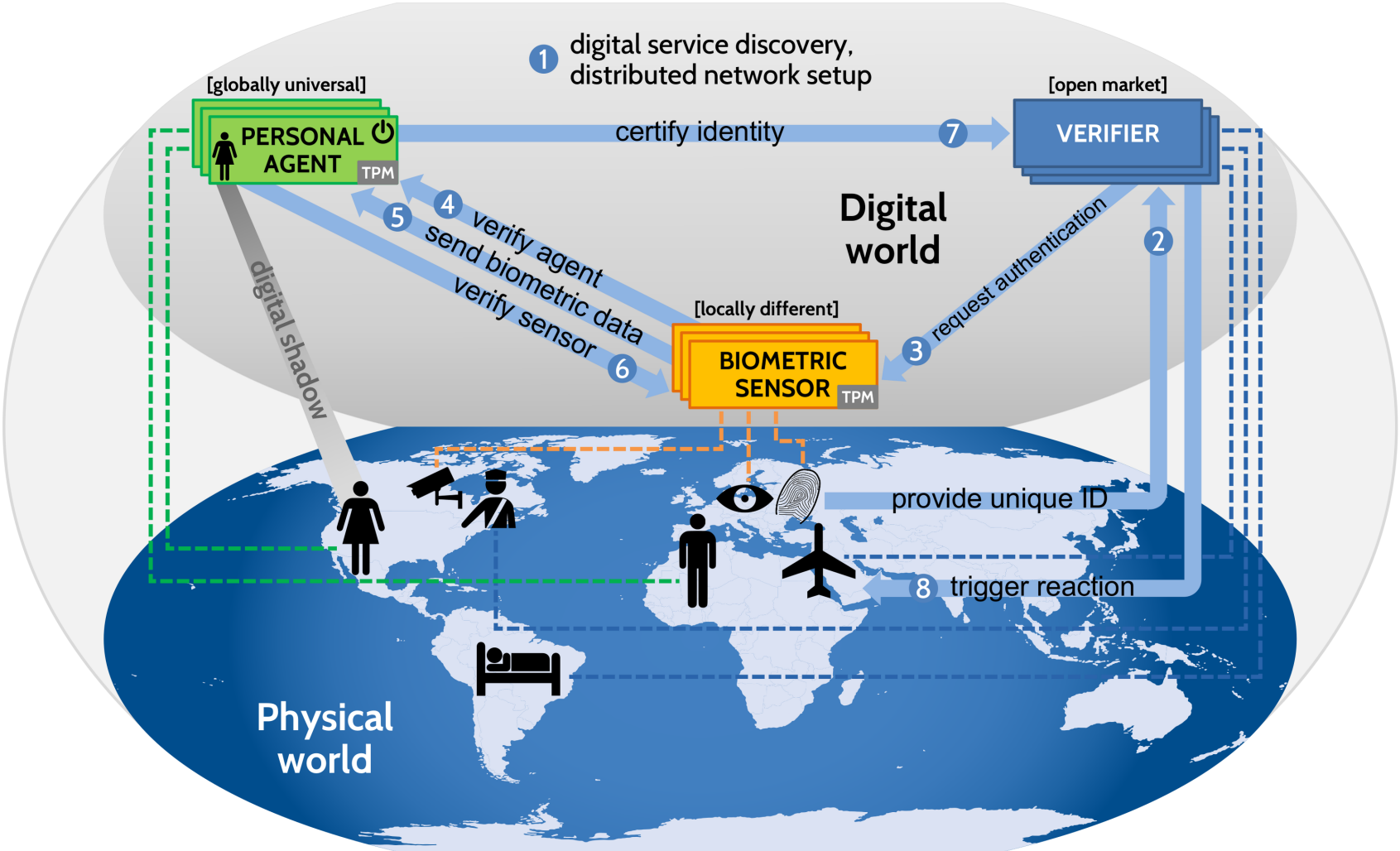
# Digital Shadow: Biometric Sensor

## Master's Thesis Seminar

Michael Preisach

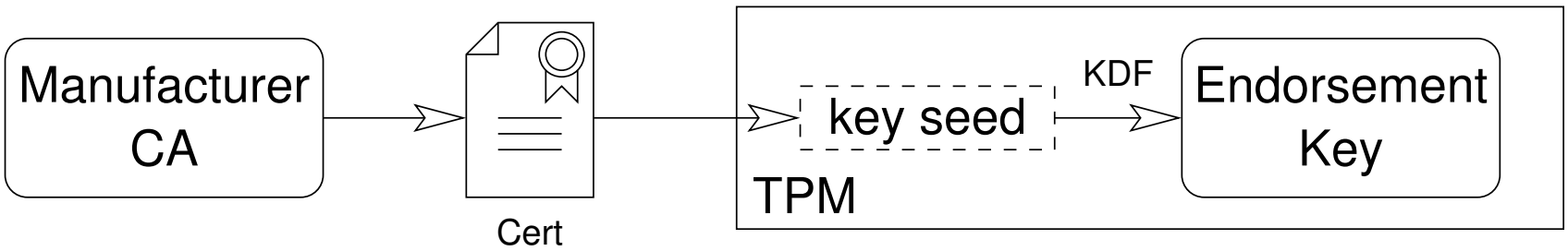
November 19, 2019

# Project Overview Digital Shadow



# Chain of Trust

- Manufacturer of TPM creates certificate
- Core Root of Trust: key seed
- `tpm2_CreatePrimary` to generate new EK



# Chain of Trust - Platform Configuration Register (PCR)

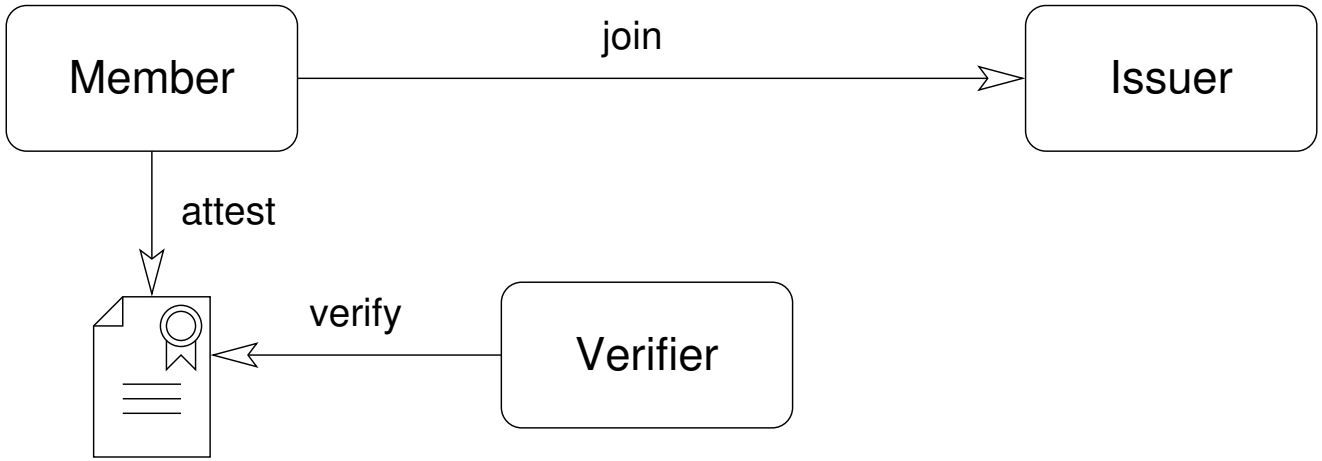
- Booting with TPM2 (PCR0-7)
  - PCR0 EFI Boot Services, EFI Runtime Services, Platform Firmware
  - PCR1 ACPI, SMBIOS, ...
  - PCR2 Option ROMs, Drivers from disks, ... (not relevant)
  - PCR4 EFI/Legacy os Loader
  - PCR5 EFI Partition, GPT, OS Partition Table
- Grub2.04 supports TPM2 (PCR8,9) [1]
  - PCR8 Kernel-, Module- and all other commands
  - PCR9 All files read by GRUB
- Linux uses PCR10-15

[1] www.gnu.org/software/grub/manual/grub/grub.html#Measured-Boot

# Problem: Create Trust between BS and PA

- Network discovery
- **No Knowledge about BS**
  - **Hardware**
  - **Software**
  - **Am I talking to a valid BS**
  - Correct client to certify identity for given biometric data
- **BS faces same problem with PA**
- Establish a secure channel to submit sensitive data

# Solution: Direct Anonymous Attestation (DAA)

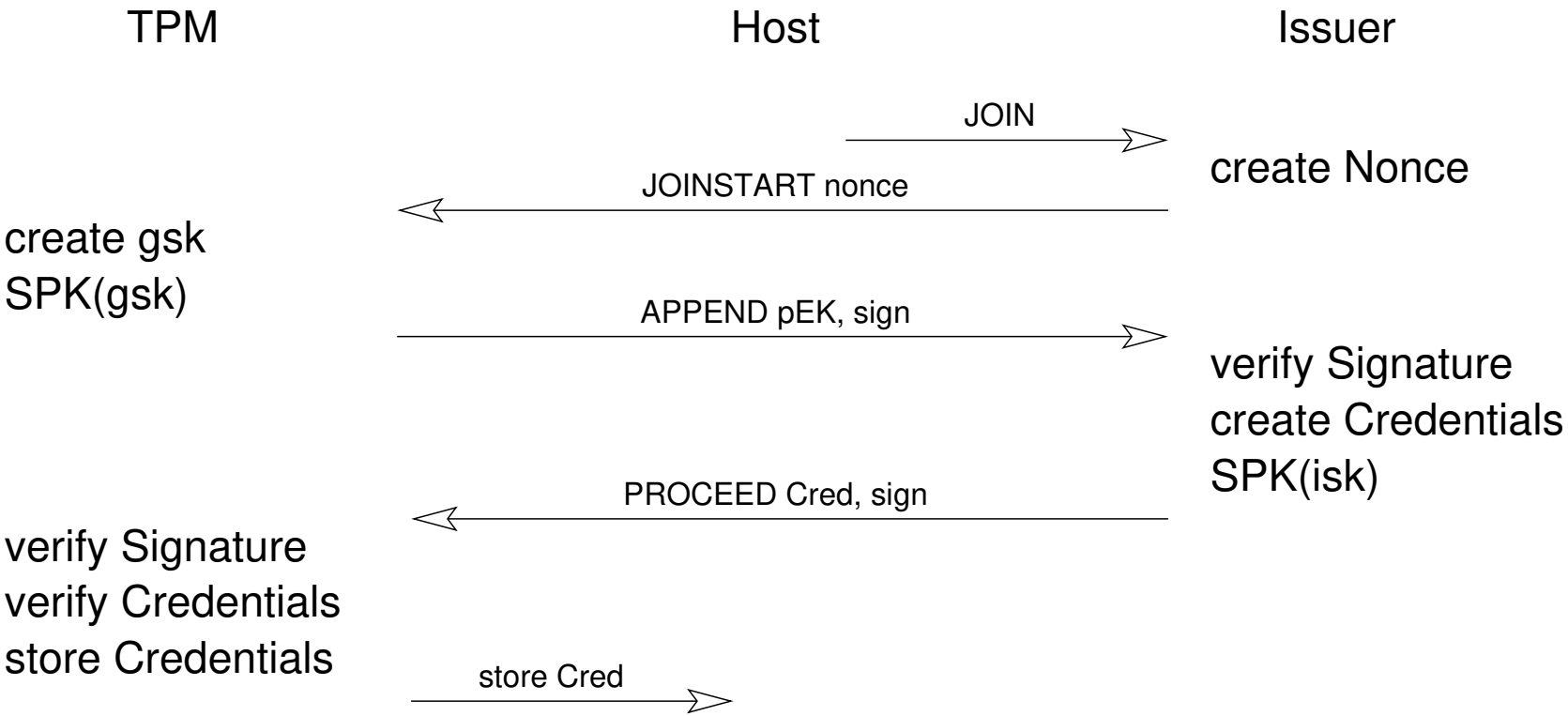



- based on group signatures
- Zero Knowledge Proof to verify group membership
- defines 3 Parties
  - *Issuer*: provides public key for a group (e.g. all Biometric Sensors) and manages group memberships
  - *Member*: holds a group private key to sign messages (e.g. a Biometric Sensor)
  - *Verifier*: knows the group public key and is able to verify correctness of signature (e.g. Personal Agent)

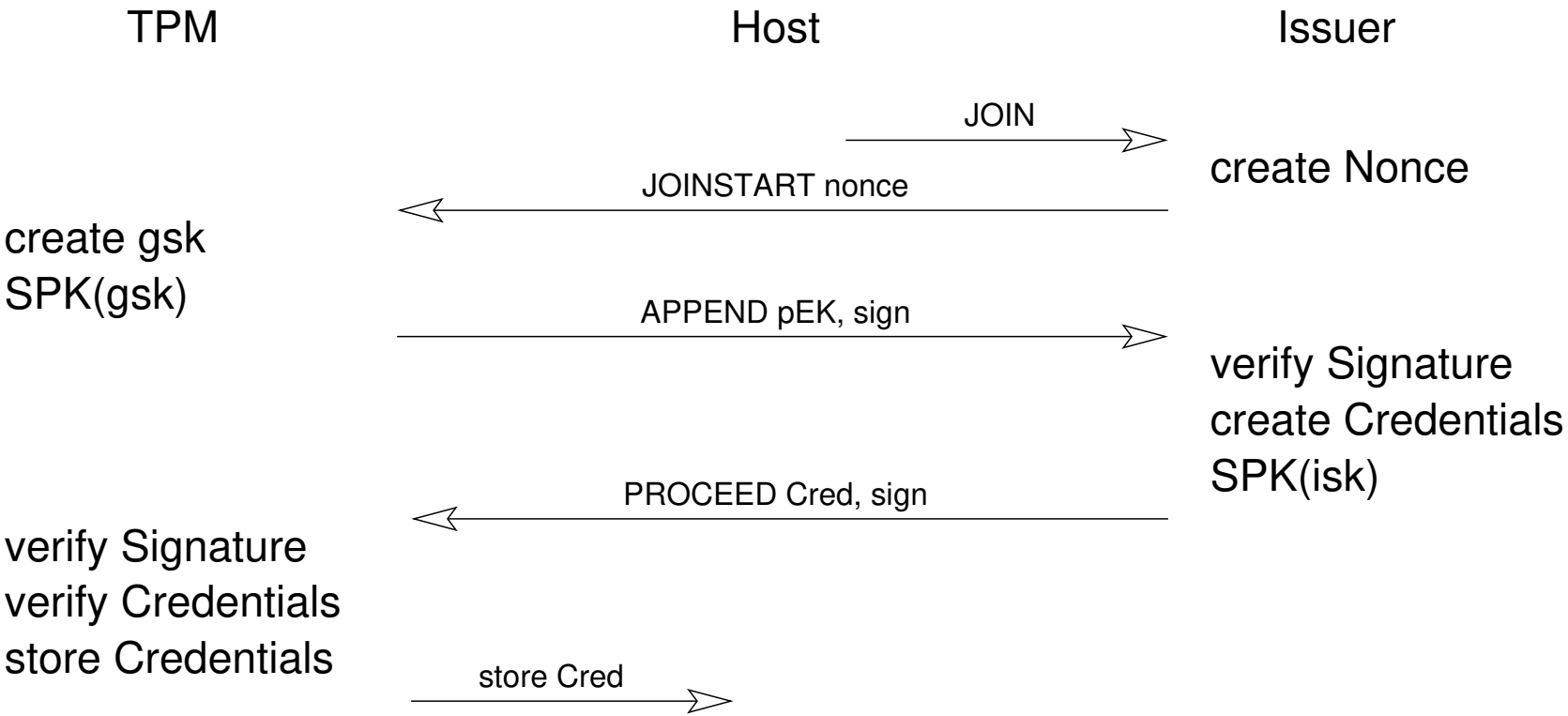
# ECDAA Setup

- Choose TPM-supported pairing-firendly Elliptic Curve: FP256BN
- Generate Issuer keypair
- $isk = (x, y)$
- $ipk = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, X, Y)$
- Publish ipk

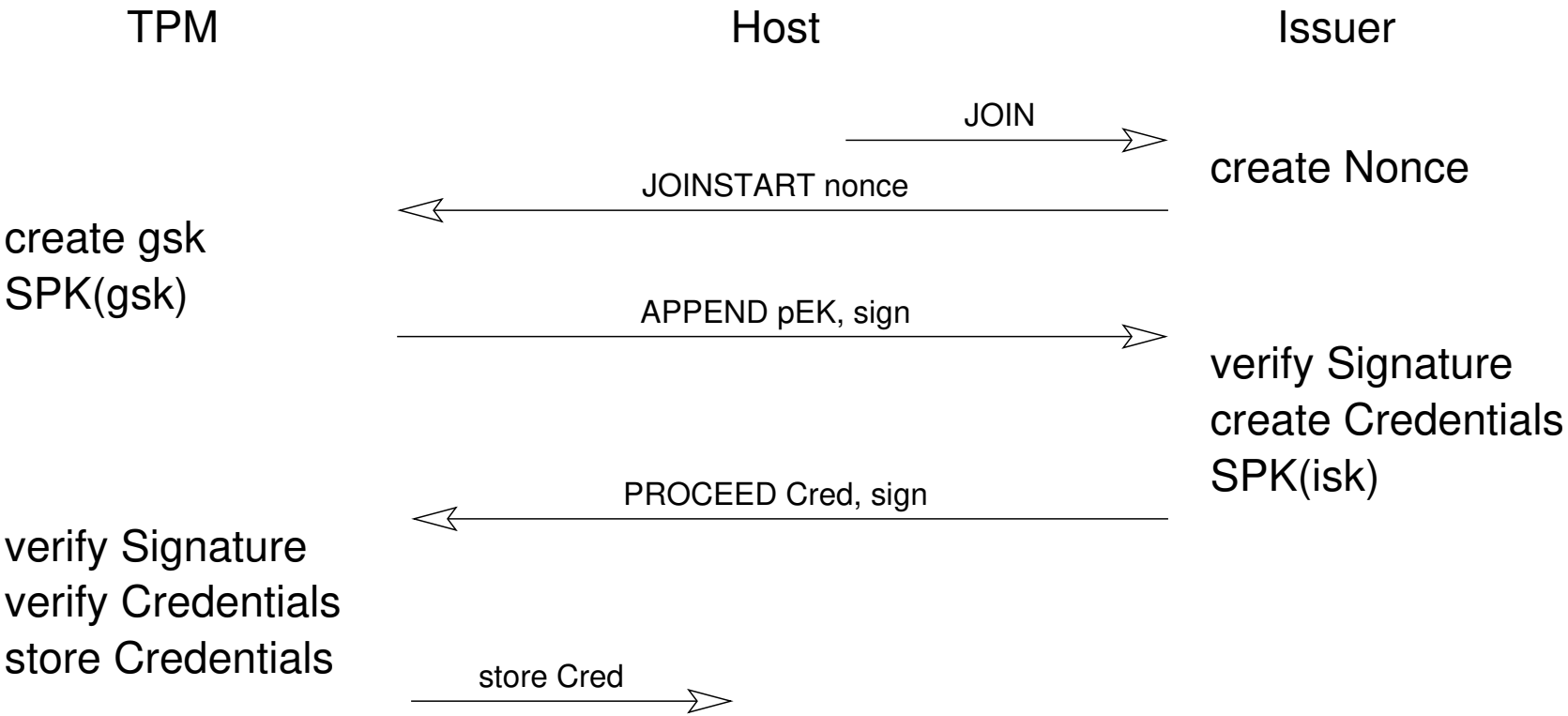
# ECDAA Member Join



# ECDAA Member Sign



# ECDAA Member Verify



# DAA Setup: Issuer creates Bilinear Group and Keys

$$q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e$$

- $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$: groups of prime order $q$
- $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$: generator points
- $e$: bilinear map with properties
  - *Bilinear*: For all $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$, for all $a, b \in \mathbb{Z}$, $e(P^a, Q^b) = e(P, Q)^{ab}$
  - *Non-degenerate*: There exists some $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$ such that $e(P, Q) \neq 1$, where 1 is the identity of $\mathbb{G}_T$
  - *Efficient*: There exists an efficient algorithm for computing $e$
- Choose secret key $x \leftarrow \mathbb{Z}_q$, $y \leftarrow \mathbb{Z}_q$
- generate public key $X = g_2^x$, $Y = g_2^y$
- $ipk = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, X, Y)$
- $isk = (x, y)$

# Bilinear Maps - Sign Messages

- Simplified Example: $\mathbb{G}_1 = \mathbb{G}_2$
- $pk = (q, \mathbb{G}_1, \mathbb{G}_T, g_1, g_T, e, X, Y)$
- Given message $m$

*Signer:*

- Compute Signature $\sigma(a, b, c)$
  - $a \in \mathbb{G}_1$
  - $b = a^y$
  - $c = a^{x+mxy}$
- Send(m, $\sigma$)

*Verifier:*

- Check, that

$$\underline{e(a, Y)} = e(a, g^y) = e(a^y, g) = \underline{e(b, g)}$$

$$\underline{e(X, a) \cdot e(X, b)^m} = e(g, a)^x \cdot e(g, a)^{xym}$$

$$= e(g, a)^{x+xym} = \underline{e(g, c)}$$

# Bilinear Maps: Zero Knowledge Proofs

- Do the same as before, but choose to additional random variables $r$ and $r'$

# DAA Join: Member joins to Issuer's Group

| TPM | | Host | | Issuer |
|---|---|---|---|---|
| | | | $\xrightarrow{\text{JOIN}}$ | $n \leftarrow \{0,1\}^{ln}$ |
| $gsk \leftarrow \mathbb{Z}$ | $\xleftarrow{\text{n}}$ | | $\xleftarrow{\text{n}}$ | |
| $Q \leftarrow g_1^{gsk}$ | | | | |
| $\pi_1 \rightarrow SPK\{(\alpha) : g_1^{\alpha}\}$ | $\xrightarrow{Q,\pi_1}$ | | $\xrightarrow{Q,\pi_1}$ | verify $\pi_1$ |
| | | | | $r \leftarrow \mathbb{Z}_q$ |
| | | | | $a \leftarrow g_1^r$ |
| | | | | $b \leftarrow a^{x+ym}$ |
| | | | | $c \leftarrow a^x \cdot Q^{rxy}$ |
| | | | | $d \leftarrow Q^{ry}$ |
| | | | | $\pi_2 \leftarrow SPK\{(t) :$ |
| | | $e(a,X) \cdot e(c,Y)$ | $\xleftarrow{a,b,c,d,\pi_2}$ | $b = g_1^t \wedge d = Q^t\}$ |
| verify $\pi_2$ | $\xleftarrow{b,d,\pi_2}$ | $\stackrel{?}{=} e(b,g_2)$ | | |
| store$(gsk,b,d)$ | $\xrightarrow{JOINED}$ | store$(a,b,c,d)$ | | |