

# Trusted Computing Platform Alliance

## Privacy



*T C P A*  
*Trusted Computing Platform Alliance*



EJA 6/22/00

# What is Trust? What is Privacy?

## The (TCPA) definition of a Trusted Platform

A Trusted Platform behaves the way it is expected to behave for the intended purpose.

“Privacy is the claim of individuals to decide when information about them will be disclosed and under what conditions.”

- Dr. Alan Westin  
Prof. of Public Law and Govt.  
Columbia University

**TCPA must ensure trust while retaining privacy**



*T C P A*  
*Trusted Computing Platform Alliance*



EJA 6/22/00

# Current State

Industry

- Privacy issues still frequent in the news
  - **Key: Privacy mis-steps hurt all companies**
- Privacy is selling point for some products
  - **Key: Well executed privacy is an asset**

Gov.

- FTC now considering legislation
  - To fast-track complaints from TRUSTe, et al
  - **Key: Groups ignoring Privacy Guidelines could invite legislation unfriendly to the industry**



T C P A  
Trusted Computing Platform Alliance



EJA 6/22/00

# TCPA Principles

- Industry-led definition
- Add trust while preserving privacy
  - Owner has ultimate control of private information
  - Owner “opts-in”
  - Privacy-positive design tradeoffs
- Add trust while preserving openness and owner choice
  - Report integrity, not restrict choice / options of the Owner
  - Define mechanisms, not policies



*T C P A*  
*Trusted Computing Platform Alliance*

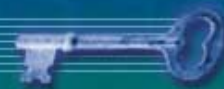


# TCPA and Privacy

- Owner Opt-in
- Owner has ultimate control over private information
- Specific privacy friendly work
  - Multiple identities
  - Identity (Anonymity) protocol



*T C P A*  
*Trusted Computing Platform Alliance*



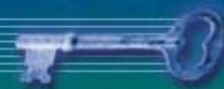


# Owner “opt-in” and Owner Control

- TCPA Subsystem doesn't function until enabled by Owner
  - Owner must create a “subsystem identity” for the TCPA Subsystem to function
- All private information can be erased by the TCPA Subsystem Owner
- Any creation and storage of secret data requires permission of the TCPA Subsystem Owner
  - Any use of secret data requires permission of data owner



*T C P A*  
Trusted Computing Platform Alliance



# Identities

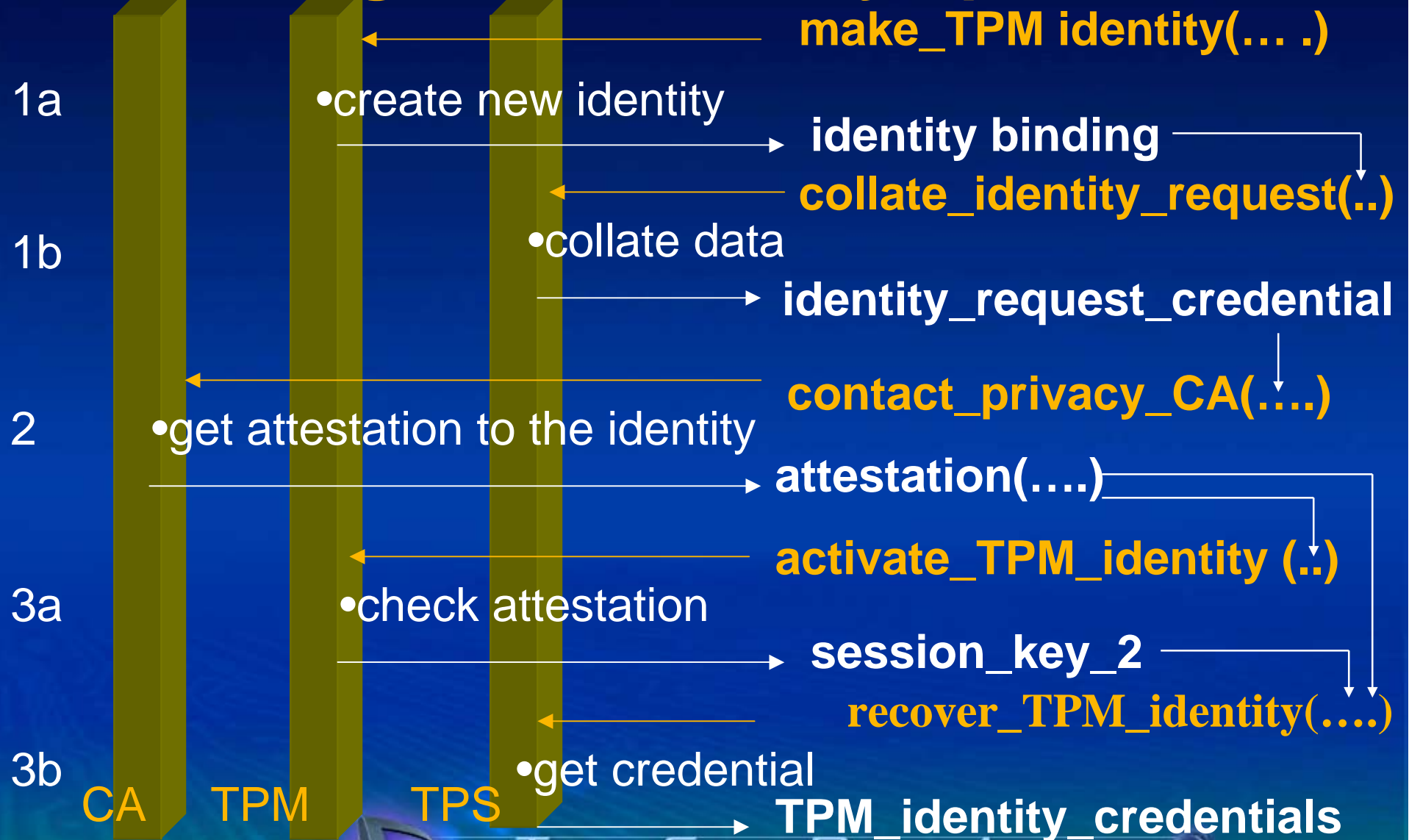
- Creation of all identities is authorized by the TCPA Subsystem Owner
- Owner can create multiple identities
  - to enhance personal security
  - to prevent identity cross-correlation
- Privacy CA endorses validity of each TCPA subsystem generated identity



**T C P A**  
*Trusted Computing Platform Alliance*



# Obtaining a TPM identity - protocol



**T C P A**  
Trusted Computing Platform Alliance





# Summary

- **TCPA actively working to protect privacy**
  - Multiple identities
  - Anonymity protocol
- **Preserving Owner choice and control**



**T C P A**  
*Trusted Computing Platform Alliance*



# Backup



*T C P A*  
*Trusted Computing Platform Alliance*



EJA 6/22/00

# Personally Identifiable

- **Personally identifiable information**
  - *Defined as: “Any collected information or product feature that can be used to identify, contact or locate a person”*
  - **Examples of personally identifiable information :**
    - Name, address, email address, phone number, cell phone ESN, Social Security number, credit card information, etc.
      - And any information linked to the above



*T C P A*  
**Trusted Computing Platform Alliance**



# Entities

**Owner** - controls the TPS

**Challenger** - wants to trust the TPS

**CA** - binds conventional ID to cryptographic ID

**Validation Entity (VE)** - provides proper metrics

**Trusted Platform Module Entity (TPME)** - attests that the  
TPS is genuine

**Conformance Entity (CE)** - attests that design is conformant

**Platform Entity (PE)** - attests that platform conforms to design

**Privacy CA** - attests that an ID belongs to a TPS  
while respecting the privacy of the Owner

**User** - uses the TPS



*T C P A*  
*Trusted Computing Platform Alliance*

