gemalto

Re-Trust Quaterly meeting Architecture Day report

d'Annoville Jerome
Technical Project Manager

06/19/07

Motivations

- Lack of common view on the design
- No time during quarterly meeting for reviews
- Many publications but no specifications
- List features on which there is a consensus
- Topics to be refine
- Feed-back from WP3 to WP2

Results (1/3)

- Added values of HW in the project not clear
  - T3.2 co-obfuscation to clarify
  - Final demonstrator
- TPM = the platform
  - Repository for hashes
  - Unique
- Smartcard (SC) = the user
  - Repository for hashes, Part of the monitor processing
  - Manages user data / credentials
- TPM/SC
  - TPM: not programmable, cannot be tampered
  - SC: programmable, Terminal communication can be eavesdropped

Results (2/3)

- HW Advantage
  - Offload tasks for the server
  - Identification of the platform / user
- Threat
  - User is the main threat
- Monitor
  - Monitor replacement: must be merged with some (application) code
- Platform
  - Trust platform is out of scope
  - Even on a Trusted platform an application can be tampered

Boundaries of trust