Security Methodology

J.d'Annoville

Post review Meeting

December 15, 2008

Agenda

- Methodology

  - Assets
  - Threats
  - Risks evaluation
  - Vulnerability

- Integrated in Deliverable 3.2 – September 2008
  - Actors, roles & use-cases

Asset

- To be protected
  - Confidentiality
  - Authenticity
  - Integrity

- Master keys, application object code, …

Threats

- Abuse the asset
  - Functionnal attack
  - Environmental manipulation
  - …
- Ex: t_code_corruption, t_code_substitution, t_authentication_keys_abuse, t_PIN_checking_bypass

- Not formal approach, only obvious threats described

Risks

- Analyse if various threats may occur
- Ranking
- Criticality
  - potential damage caused on assets

gemalto^x

Vulnerability

- Theoretical work
  - Formalize secure software development techniques
- Risk sort by categories
- Actions to mitigate the risks

Thank You

Questions?