Open standards for Security and Certification

Contribution to a Permanent Certification Structure

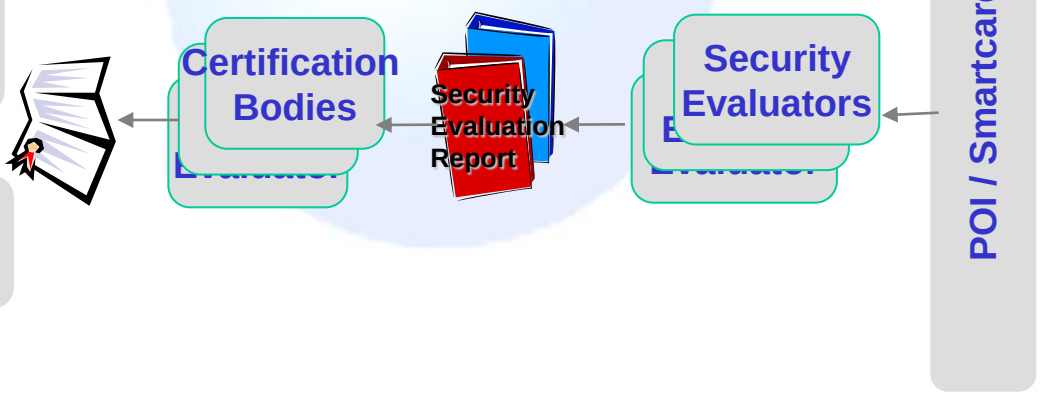
First Ideas

22 December, 2011

The Target Solution

Acceptance of 1 Certificate for multiple approval

Permanent Structure



How to maintain and monitor a certification infrastructure

Two processes must be covered

1) Maintenance of the infrastructure

2) Operation of the infrastructure

How to maintain and monitor a certification infrastructure

1) Maintenance of the infrastructure

- An activity, which is event driven
  - New requirements occur
    - Volume
    - New attacks
    - Oversight
    - Business / changes in risk management
    - CC scheme requirements
- New PPs or PP Releases may be the consequence
  - To organize and coordinate, how the new PPs are implemented in the certification infrastructure (not in the products!)

How to maintain and monitor a certification infrastructure

2) Operation of the infrastructure

- Continue to work on OSeC “success factors”
  - Exchange and evaluate experiences with the ETR for Risk / Interpretations
  - Exchange and evaluate different views on the acceptance of a certificate
  - Agree on common publications of market relevant information
    - Certificate life cycle management
  - Solve Conflicts
  - Agree and organize common communication with stakeholders
  - Agree and organize communication with the CC organization
- Case related business / to learn from each other
- Increasing convergence will be achieved where appropriate

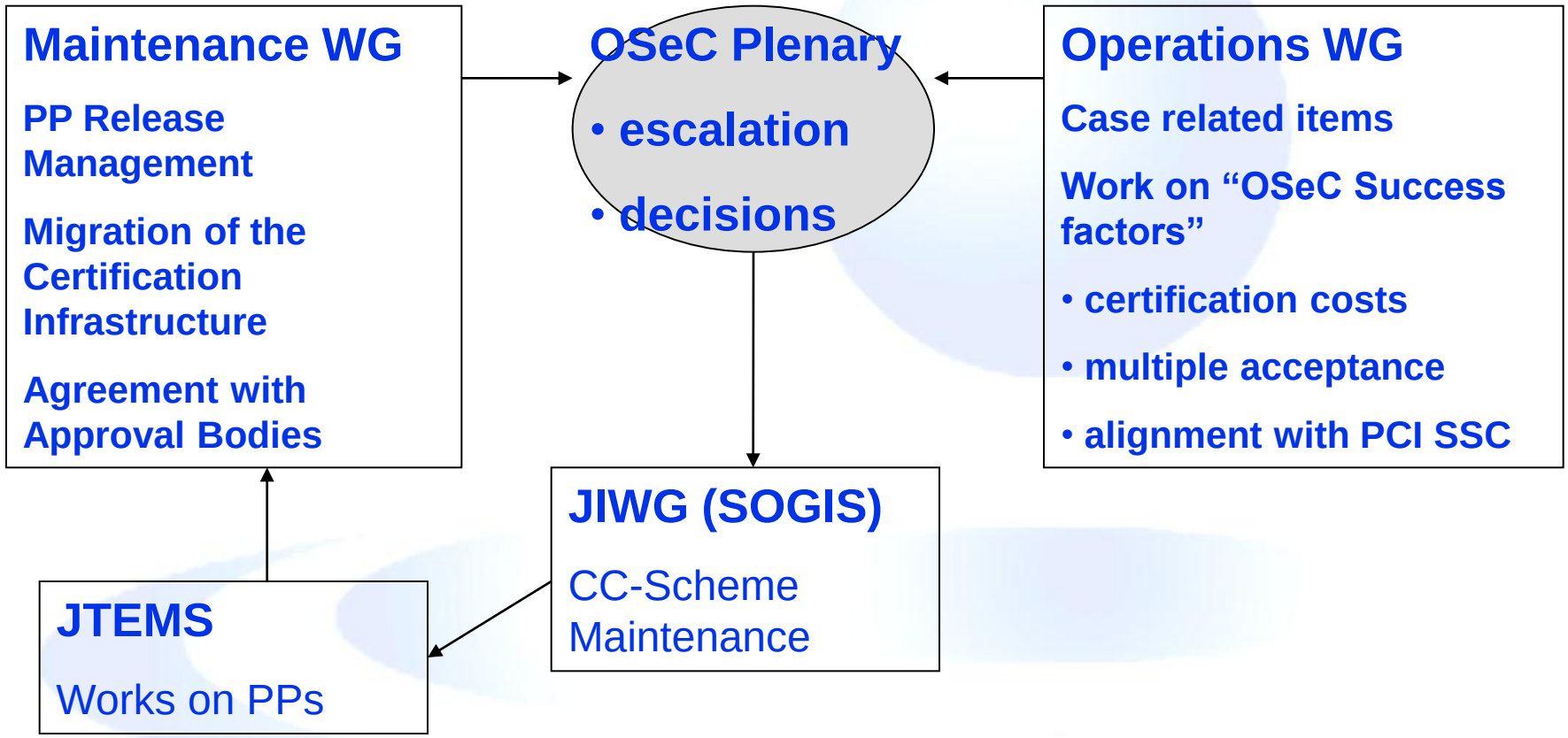
Matching OSeC with other Working Groups

- EPC SCCMB
  - Issue rules for the recognition of certification bodies and laboratories
  - Light oversight and monitoring of SEPA implementation based on the Volume's high level requirements
  - No decision making power regarding the implementation of the maintenance and operation of the certification processes,
  - may ask questions to let OSeC explain its decisions
- EPC CSG
  - Maintenance of the Volume / high level requirements / OSeC representative
  - Security Expert Team SET / OSeC representative
- CAS
  - Standardization / Harmonization of security requirements for cards and terminals
  - Dedicated to contribute to OSeC considering the integration in the OSeC organisation

Matching OSeC with other Working Groups

- OSeC Organisation
  - Scope: Steering the CC Certification of e.g. cards and POI compliant with the Volume's high level requirements
  - Uses the existing CC Certification Infrastructure. Maintains and develops OSeC specific certification issues of this infrastructure in close cooperation with the existing CC Scheme
  - Enables communication and settings of the participating approval bodies regarding maintenance and operations based on the OSeC pilot
  - Includes CAS as a Standardization Expert group for security requirements
  - Engages with JIWG and its groups to maintain the PPs and related CC topics
    - Translation of the CAS requirements into CC PPs
    - Acts on the request of CAS (tbd)
  - Contributes actively to the CSG / SET

Structure of the OSeC Organisation



Prerequisite

- The permanent structure will respect
  - Approval bodies' individual responsibility for risk management
  - Acceptance of the initial approval will be agreed within OSeC, roll out approval handling will be done by the approval bodies in their own responsibility