Reuse of evidences and evaluation results

Carolina Lavatelli, Trusted Labs
(on behalf of ISCI)
Contents

- Reuse concepts
- ISCI project: goals and approach
- Work in progress
- Next steps
Reuse concepts

- The subject has been addressed ten years ago in Reuse of Evaluation Results and Evidences [CCMB-2002-08-009-002]
  - states the principle of avoiding the analysis where no direct or indirect change arises
  - aims at reducing costs and delays for developers and evaluators
- Central to the scalability of the Common Criteria evaluation framework
Reuse concepts

- Reuse scenarios: using a previously completed evaluation for
  1. The re-evaluation or assurance maintenance of the TOE by another lab (same CCRA scheme or not)
  2. The evaluation of a compound TOE
- The recommendation is to perform the delta analysis of the previous and the new security targets to derive the impact of changes
- Implementation details left open
ISCI project: goals and approach

- ISCI is involved in improving usability of CC in the field of smartcards and similar devices
- ISCI has developed the «reuse» methodology for the composite evaluation of an «application» on top of a certified «platform»
- In the context of NFC deployment the aim is to improve evaluation of Java Card applications that will run on many platforms
  - Supported by standardized functional and security specifications for Java Card and GlobalPlatform technologies
P1 and P2 are GlobalPlatform-enabled Java Cards
P1 and P2 are certified against PP (U)SIM
A is a Java Card application
Goals

- Ease Java Card application evaluation process when the same application is evaluated in more than one certified platform
- Harmonize the understanding of reuse across certification schemes and labs
Approach

- Build a set of supporting documents
  - **for developers**: to prepare the evidences related to a given application that would be evaluated on top of different platforms
  - **for the first evaluator of the application**: to standardise the outcome regarding the platform-dependent and – independent features
  - **for the second and further evaluators of the application**: to standardise the reuse from the first evaluation
Foreseen supporting documents

- Developers’ guidance on reuse
- CEM for Reuse – first evaluation
- CEM for Reuse – further evaluations
- Template of “ETR for Reuse”

Edition will be made on a need-to-have basis
Progress status

« Delta analysis of security targets »

▪ General method for any 2 standard STs
  ▪ Refined method for any 2 composite STs
    ▪ Refined method for any 2 composite STs for the same application on top of two different platforms
  ▪ Impact of the analysis on reusability

► Input to supporting documents
► To be published by end of the year
Progress status (suite)

- Template of « ETR for Reuse »
  - Table of contents
  - Expected information, hints and examples
    - Under development

- CEM for Reuse – first evaluation
- CEM for Reuse – further evaluations
- Developers’ guidance on reuse
  - Formally not started yet although the discussions address the topics altogether
Next steps

- Consolidate the impact of moving an application from one platform to another and the consequences on the evaluation tasks

- Extend the analysis to « similar » applications on « similar » platforms

- Provide the supporting documents for pilot evaluations
Funding

- French INOSSEM project (2012-2013)
  - « Provide industry solutions to ensure security interoperability and portability between multi-applicative secure elements (e.g. (U)SIM) »
  - Partners: ANSSI, Gemalto, Genigraph, GREYC (Univ. Caen), Morpho, Oberthur, Oppida, Orange, SERMA Technologies, SFR, THALES, Trusted Labs, XLIM (Univ. Limoges)
Thank you!

Carolina Lavatelli
carolina.lavatelli@trusted-labs.com