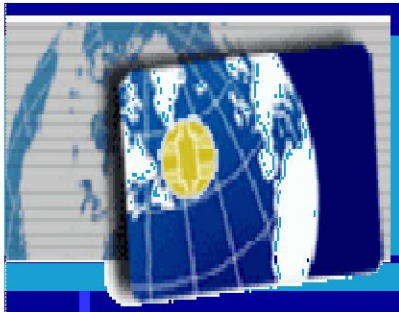


ISCI - International Security Certification Initiative

Common Criteria works!

(How the Smart Card industry uses the CC)

9th ICCC

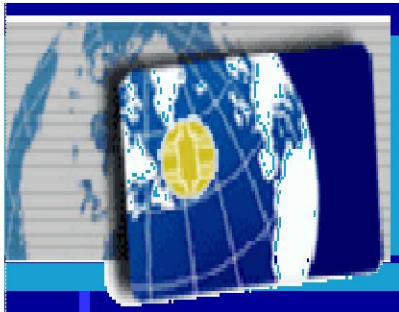
Jeju, 25 September 2008

ISCI-WG1

speaker: Tyrone Stodart

Presentation overview

- ISCI - a Eurosmart Initiative
- Steps to working with CC
  - Protection Profiles
  - Evaluation Guidance
  - Optimise Re-use
  - Develop solutions for key issues
  - Continuous Improvement
- Conclusion



ISCI - a Eurosmart initiative

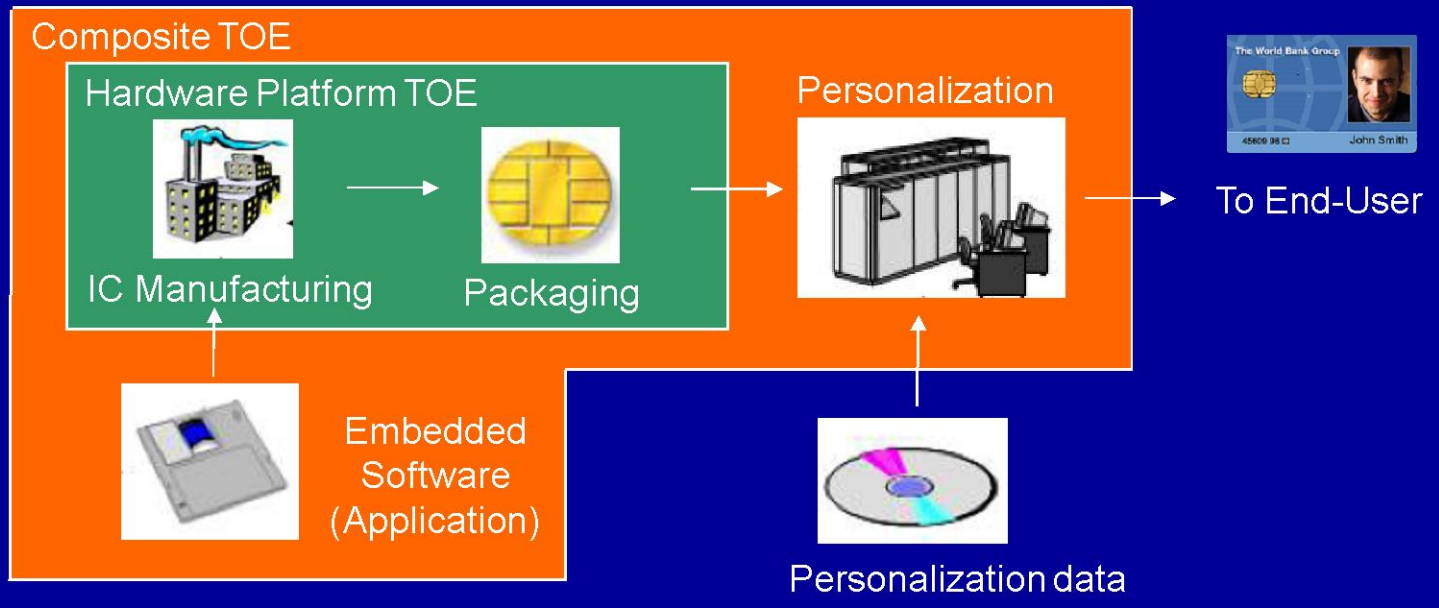
- Eurosmart,
  - International non-profit association founded in 1995 in Brussels
  - 27 companies of the Smart Security industry (smart card manufacturers, semiconductors, terminals, issuers)
  - Promotion and standardization of smart secure devices and smart secure systems
  - Harmonization of security evaluation schemes
- ISCI created by Eurosmart
  - Purpose: To define, support and promote a universal framework for security evaluation and certification methods, tools and procedures, based on internationally accepted standards.
    - Fair, high quality, comparable, standardised evaluations.
  - To involve all actors within the evaluation process, with the goal to improve smart card evaluation time & cost
  - To provide supporting documents to guide smart card evaluations

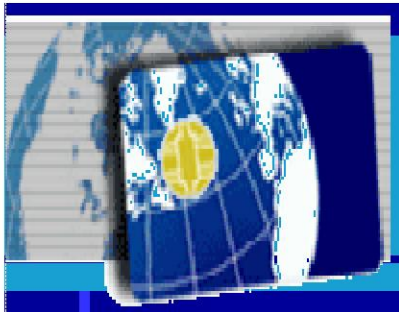
ISCI contributors

- Two working groups
  - WG1 for methodology
  - WG2 for technical issues - known as JHAS
- ISCI-WG1 Contributors
  - Smart card manufacturers, developers, Issuers, IC manufacturers
  - Evaluation laboratories
  - Certification Authorities

Protection Profile Development – A simplified lifecycle

- Smart card evaluations use a number of PP's to 'build' a complete product.
  - Security IC PP - used for the IC, the 'hardware platform' for the application.
  - The system PP - depends on the application for the product. Used for the composite evaluation of application on hardware platform.



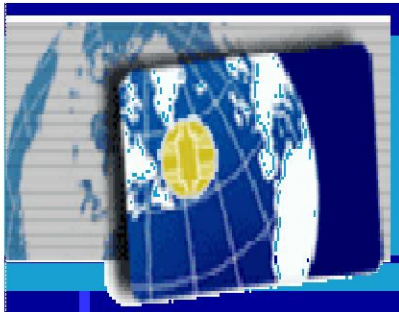


Protection Profile Development - problem

- For CC v2, two IC protection profiles used.
  - PP9806 was used under the French Scheme (DCSSI)
  - BSI-PP-0002 was used under the German Scheme (BSI).

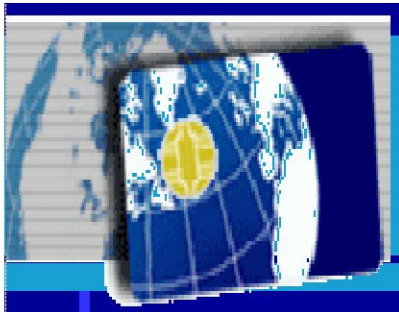
This led to some difficulties in composite evaluation,

- Misalignment between IC PP claims and composite PP claims



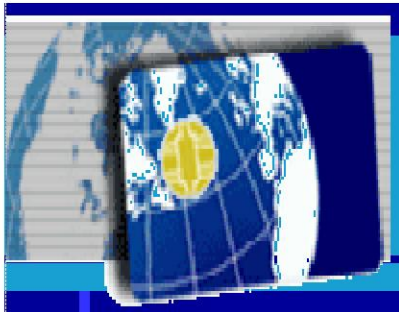
Protection Profile Development - Progress

- Proposal for CCv3.1:
  - Generate one IC protection profile accepted by all developers and the 'foundation' for composite protection profiles.
  - Ensure that sufficient hardware developers were involved in the editing process.
  - Give composite product venders, evaluation labs and certification bodies opportunity to provide feedback to draft versions via ISCI and JHAS.
- Result
  - 5 hardware vendors worked on the 'Security IC Protection Profile', edited by T-Systems and evaluated by Brightsight. It was certified in August 2007 and is currently the de-facto standard.



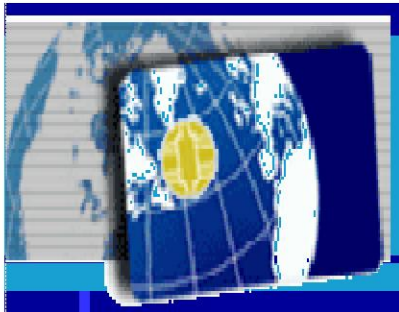
Evaluation Guidance

- 'State-of-art' testing for security evaluations is critical for products being evaluated at AVA_VLA.4/AVA_VAN.5.
- JHAS' role is to provide supporting documentation to encourage consistency in rating attacks
  - 'Application of Attack Potential to Smart cards'
    - Specific information in calculating attack potential 'points' for smart card related attacks (public document).
  - 'Attack methods for Smart cards and Similar Devices'
    - A 'catalog' of attacks with some non-proprietary information on how to perform the attacks (not public).
- JHAS is now working on a test vehicle
  - to determine whether new and existing evaluation labs have the technical capabilities to perform smart card security evaluations.



Optimise Re-use

- The smart card community is active in optimising re-use of evaluation efforts to reduce time and money spend.
  - Evaluation laboratories and Certification bodies have been supportive.
  - These efforts have focussed on formal aspects of the CC, in particular documentation and procedural/process.
  - Site audit activities have also been considered, generally for re-use by a single developer.
    - Developments ongoing regarding product independent site certification
      - useful where more than one developer relies on the site security of a provider (such as packaging site). Presented in Track C 24th August 16:00-17:00.
  - The aim is for an evaluation with high re-use to have costs almost as low as those of a 'black-box' evaluation.



Develop solutions for key issues

- Document has been developed within the community to help in evaluations:

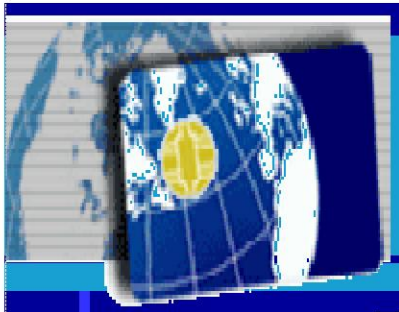
- 1) How to apply CC to smart cards and ICs
  - Rational for Smart Card and Similar Devices
  - Guidance for smart card evaluation
  - Application of CC to Integrated Circuits
  - Application of Attack Potential to Smartcards

- 2) How to perform 'composite' evaluations.
  - Mandatory Guidance has been developed to perform a composite evaluation of an application running on certified hardware, where evidence from the hardware evaluation is provided to optimise re-use and allow the application evaluator to analyse the security measures of the composite product
    - Composite Product Evaluation for Smart cards and Similar Devices
    - ETR-template for composition v1-0.

  - Have recently discussed possible CCv3.1 transition issues for composite evaluation

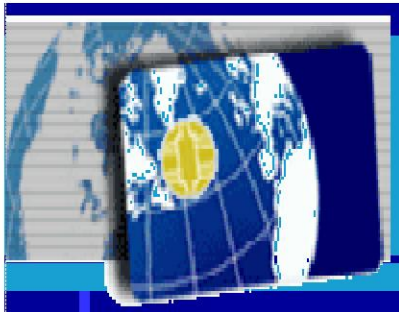
Develop Solutions for Key Issues (2)

- ADV_ARC
  - A new family in CCv3.1 which looked difficult to manage.
  - Transition guidance task
    - Provide guidance for a developer with existing CCv2.3 evaluated products with guidance and a template in order to create suitable ADV_ARC documentation for CCv3.1
    - Discussions between developers, evaluators and certification bodies to understand the requirements and best approach
      - What do the certification bodies want to see?
      - What is useful to the evaluators?
      - What can the developers provide?
        - ideally re-use existing CCv2.3-like material.



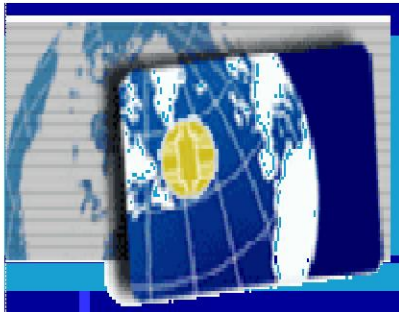
Develop Solutions for Key Issues (3)

- Security Architecture requirements (ADV_ARC) for smart cards and similar devices is now available as a trial document for future CCv3.1 evaluations
- Once it has been confirmed as a useful guide, or revised as necessary, it will be published fully.



Continuous Improvement

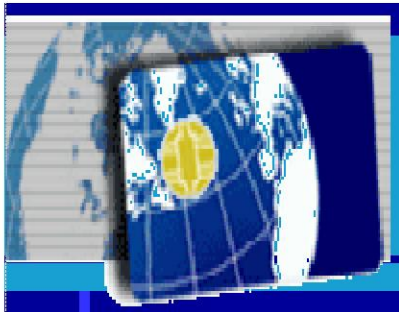
- CC is a moving target
  - Existing guidance and mandatory documents are maintained
    - Ongoing for documentation developed for CCv2.3
  - 'Maintain' newer guidance for ADV_ARC based on results of use 'in-the-field'.
- Smart card evaluation is a moving target
  - Attack Methods document
    - requires regular review to consider new attack methodologies, equipment ratings, etc.
  - Consider the impact of new uses for smart card and security product on CC evaluations,
    - New application protection profiles required ?
- Continue 'optimisation'
  - After a few evaluations under CCv3.1 have been completed, there may be opportunities to increase re-use or further optimise non-value-add activities
    - focus on providing a cost-effective but high-assurance CC process.



Conclusions

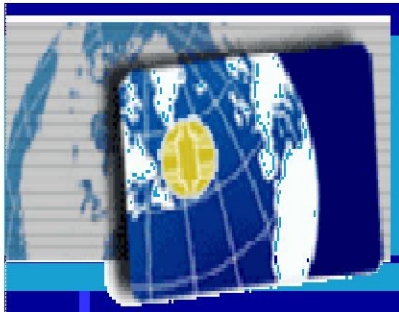
- Different stakeholders in the smart card community have successfully worked together to define standards and provide solutions to shared problems encountered in CC evaluations.

- Actively managed groups of interested parties meet together to discuss issues, and spend time and effort to solve them and publish solutions that have benefited the community.



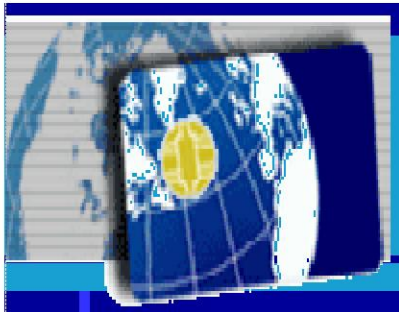
Proposal

- It is clear that other industries within the CC have shared difficulties in evaluating and certifying their products
  - There is a strong benefit if developers, evaluators, certification bodies and other stakeholders work together to provide solutions to shared issues.
    - Develop Protection Profiles that
      - Allow developers to make good security products with the right security for the end-product
      - Provide the user with the security that they require
      - Are reasonable to evaluate against.
    - Develop guidance for particular issues for your products.



Final thoughts

- Discussing issues within an industry does not mean you have to give away secrets
- No company benefits from developers, evaluators or certification bodies re-interpreting the CC every time for the same issue.
- CC does have a high overhead, and if this overhead is minimised, this allows all industry members to compete based on the value-add of the product, not on their skill in negotiations with evaluators or certification bodies.
- There are no industry-specific 'supporting documents' for products other than smart card!
- The smart card industry do not want to see CCv4.0 unless there are clear benefits in terms of cost and time reduction for the same security assurance as CCv2.3/3.1. The community hope for a stable CCv3.1 for at least 5 years, with any fixes for problems experienced in guidance, or in worst case small change releases.



Questions?