A platform approach to certifying Smart card ICs

Presented by

Mike Paterson, Hitachi Europe Ltd.

Smart Card Security Conference, TOKYO, 29th March 2001

Acknowledgements

This IC Protection Profile is the result of a joint development project between
the Smart card IC manufacturers:

Atmel, Hitachi, Infineon Technologies and Philips Semiconductors

- in collaboration with **debis IT Security Services** and under the German Common Criteria
Evaluation Scheme, administered by the
Bundesamt für Sicherheit in der Informationstechnik

Why we need a new IC PP

- The only established hardware PP has demonstrated the usefulness of a hardware-only approach, but:
  - it was not designed with multi-application cards and downloadable applications in mind
  - it was not designed to be fully modular and easily re-usable

    …in other words, it was not designed to produce results that are movable between different end-products, different labs., or even different certification bodies
- Many of the card vendors and issuers are looking for an improved approach for their multiple hardware evaluation requirements.

Overview

- Benefits
- What the “Platform” concept means
- Relationship with other PPs
- Scope and Concept of the IC Platform PP
- Usage
- Status and Schedule
- Key questions for PP users

Benefits of the IC PP

- Enabling a platform approach for Smart card Certification using the Common Criteria (ISO 15408)
  - more cost effective – one evaluation per platform
  - less time for card evaluation and certification
  - better comparability between platforms, evaluations and results
  - re-use of evaluation efforts, results and certificates
  - modularity simplifies certificate maintenance.

The “Platform” concept…

- The IC platform is the basis for supplying a wide variety of products and services on smart cards and so we want to be able to specify and evaluate its security
- The TOE is defined as a processing unit (CPU), security components, I/O ports, memories and any IC-dedicated software, which:
  - provides functions to the O/S and applications
  - protects user programs and user data (the assets)
  - gives security assurance, based on the correct development and production processes
  - can be easily enhanced with additional features.

…for Modularity…

The Platform approach is designed to be modular…

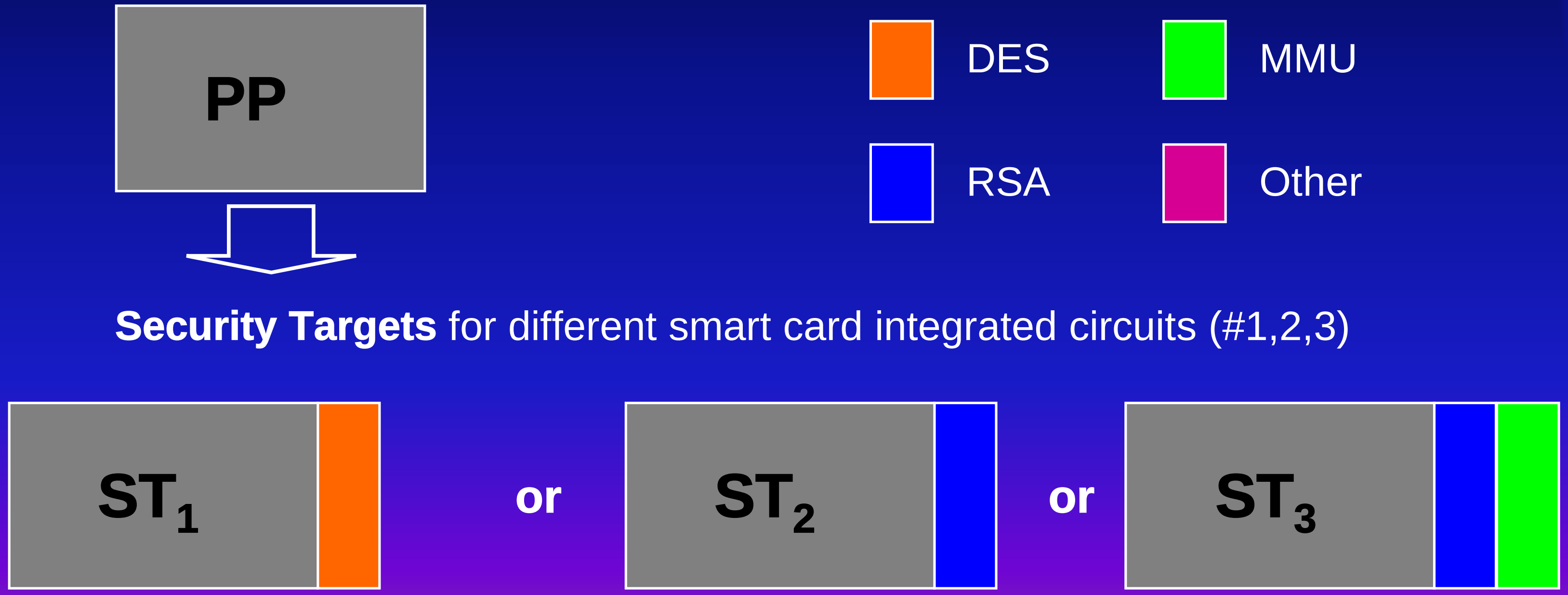
- the Security Target for each IC will be a combination of the requirements of the certified IC Platform PP and a list of functional augmentations

IC Platform Protection Profile

Smart card Integrated Circuit
mandatory requirements

IC Functional Augmentations

Smart card Integrated Circuit
additional features, e.g.:



PP

🟧 DES

🟩 MMU

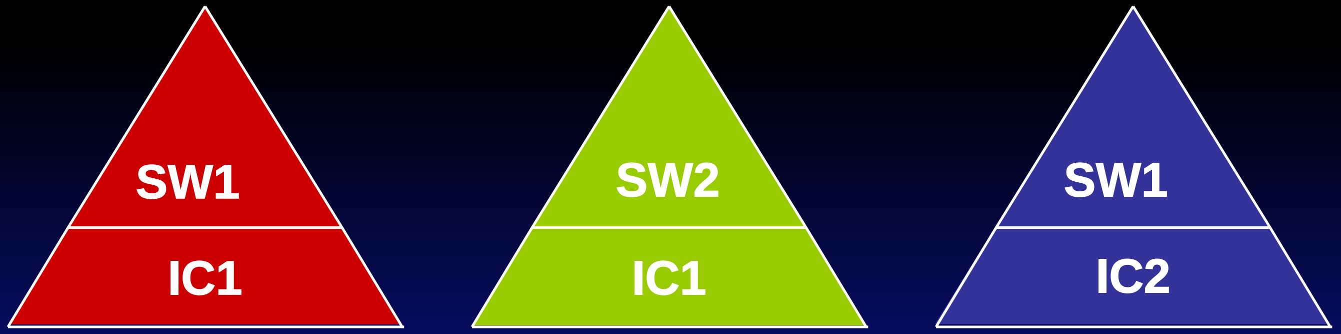
🟦 RSA

🟪 Other

Security Targets for different smart card integrated circuits (#1,2,3)

…Re-use and Flexibility (1)

today



SW1
IC1
1st Evaluation

SW2
IC1
2nd Evaluation

SW1
IC2
3rd Evaluation

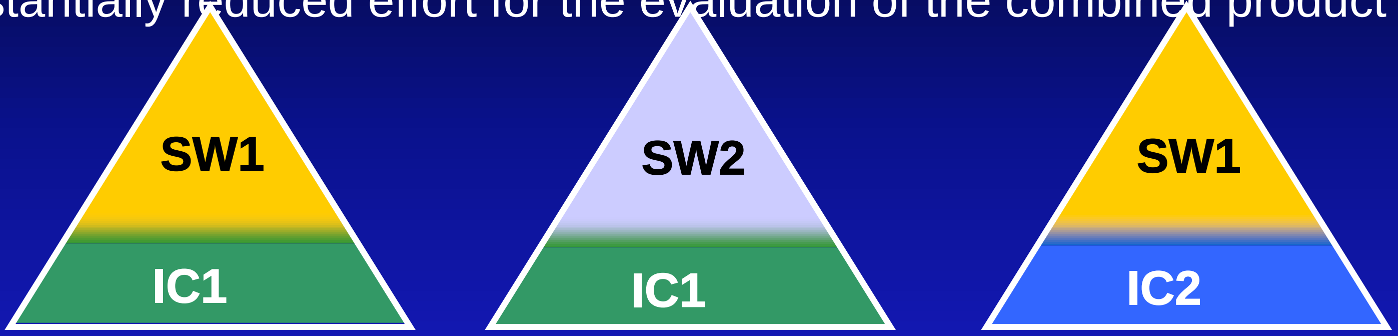
- Today, you can in theory re-use evaluation results
- In practice there are too many constraints:
  - same Evaluation lab. and Certification Body
  - same hardware and software developers
  - no effective separation between h/w and s/w

⇨ **THREE FULL EVALUATIONS ARE USUALLY REQUIRED**

…Re-use and Flexibility (2)

- Separate evaluations for h/w & s/w, with a clear description of the interfaces
- Re-use of results for different combinations of:
  - h/w, s/w, labs. and certification bodies
- Substantially reduced effort for the evaluation of the combined product

...in future



SW1

IC1

SW2

IC1

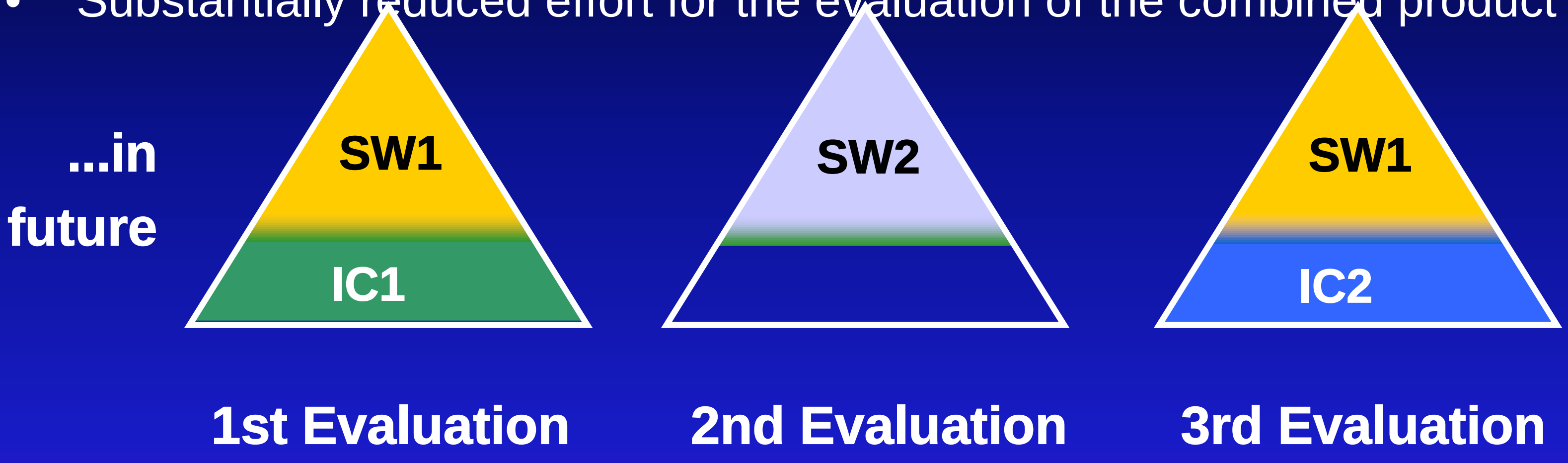
SW1

IC2

1st Evaluation **2nd Evaluation** **3rd Evaluation**

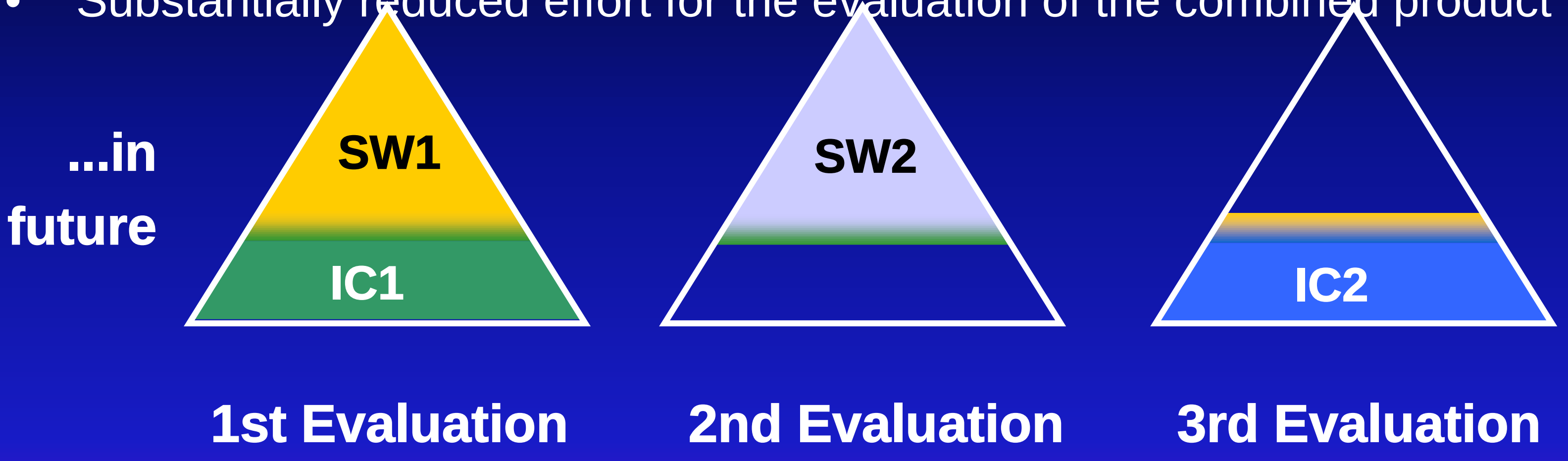
…Re-use and Flexibility (2)

- Separate evaluations for h/w & s/w, with a clear description of the interfaces
- Re-use of results for different combinations of:
  - h/w, s/w, labs. and certification bodies
- Substantially reduced effort for the evaluation of the combined product



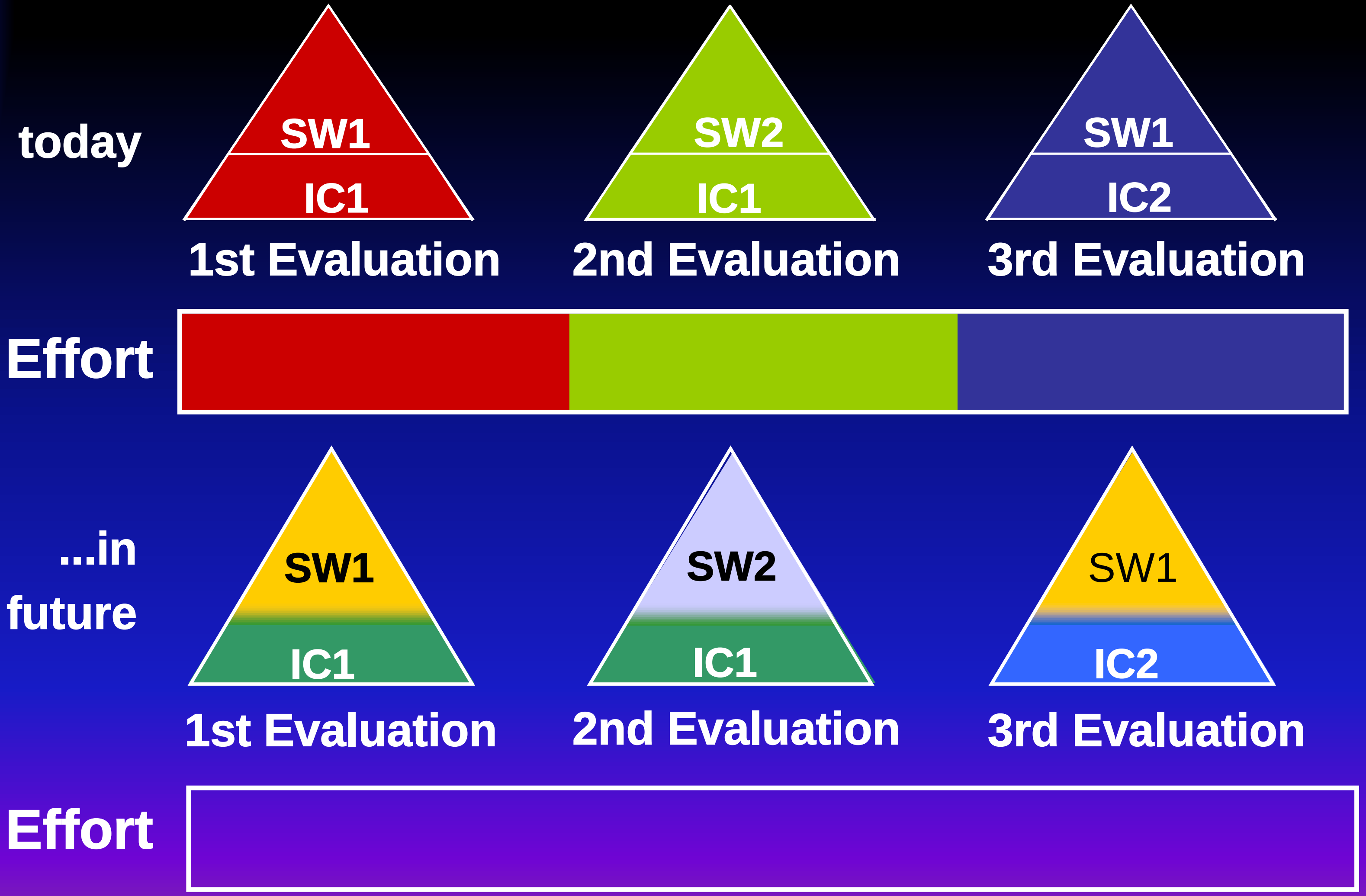
…Re-use and Flexibility (2)

- Separate evaluations for h/w & s/w, with a clear description of the interfaces
- Re-use of results for different combinations of:
  - h/w, s/w, labs. and certification bodies
- Substantially reduced effort for the evaluation of the combined product



Certifying a new product will not require the re-evaluation of previously certified parts (i.e. IC1 or SW1)

...Re-use and Flexibility (3)



today

SW1
IC1
1st Evaluation

SW2
IC1
2nd Evaluation

SW1
IC2
3rd Evaluation

Effort

...in future

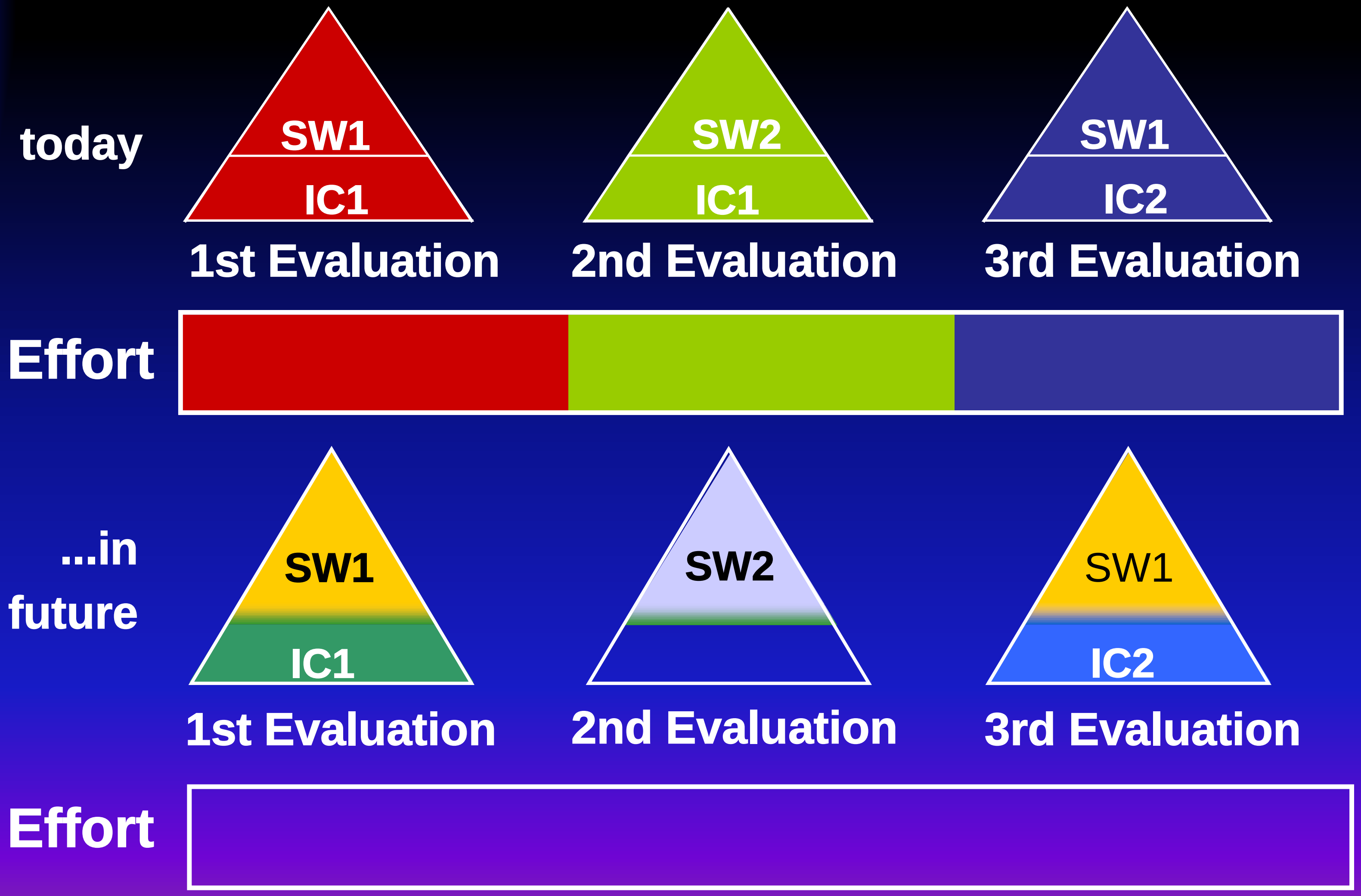
SW1
IC1
1st Evaluation

SW2
IC1
2nd Evaluation

SW1
IC2
3rd Evaluation

Effort

…Re-use and Flexibility (3)



today

SW1
IC1
1st Evaluation

SW2
IC1
2nd Evaluation

SW1
IC2
3rd Evaluation

Effort

…in future

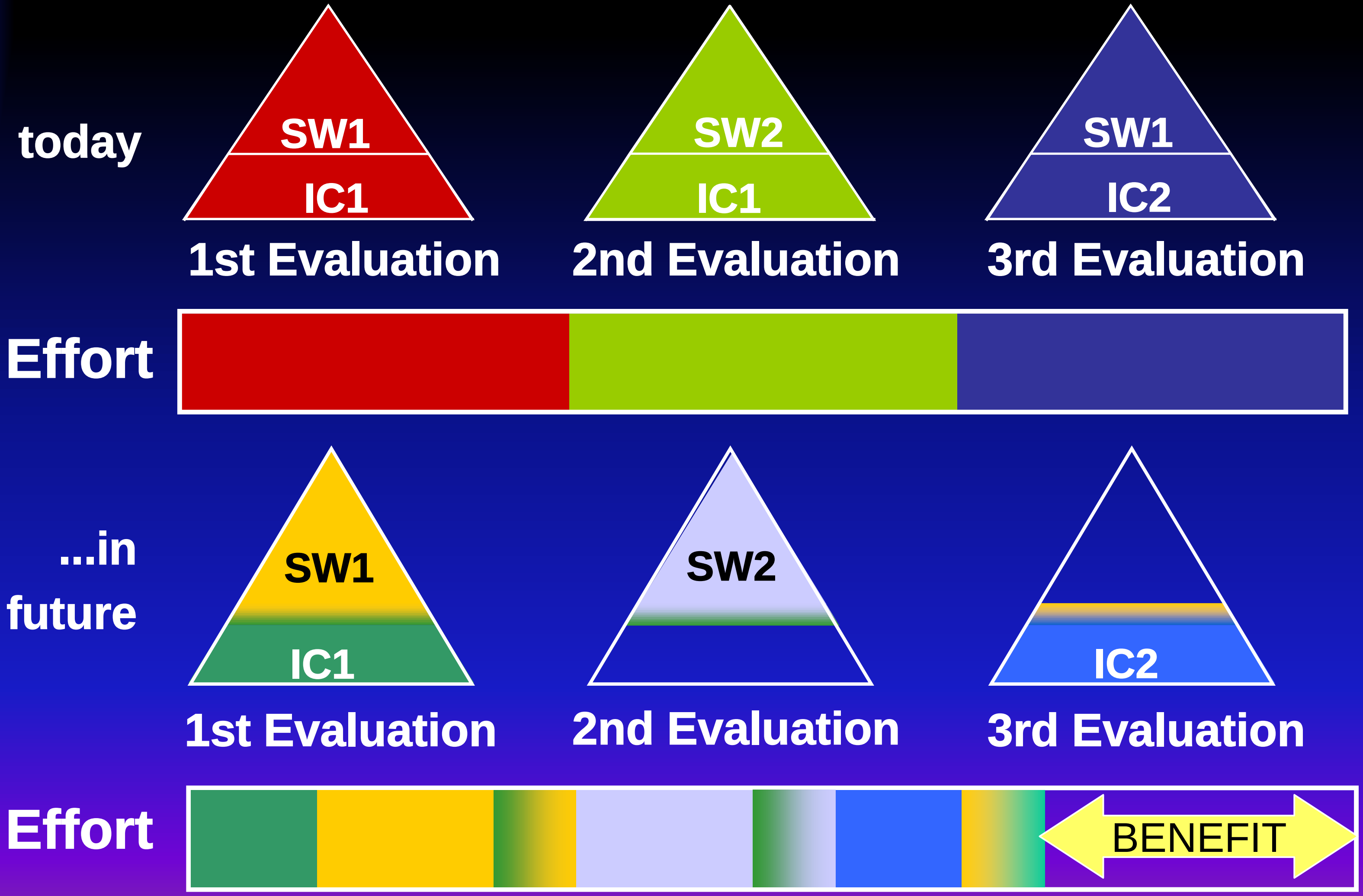
SW1
IC1
1st Evaluation

SW2
2nd Evaluation

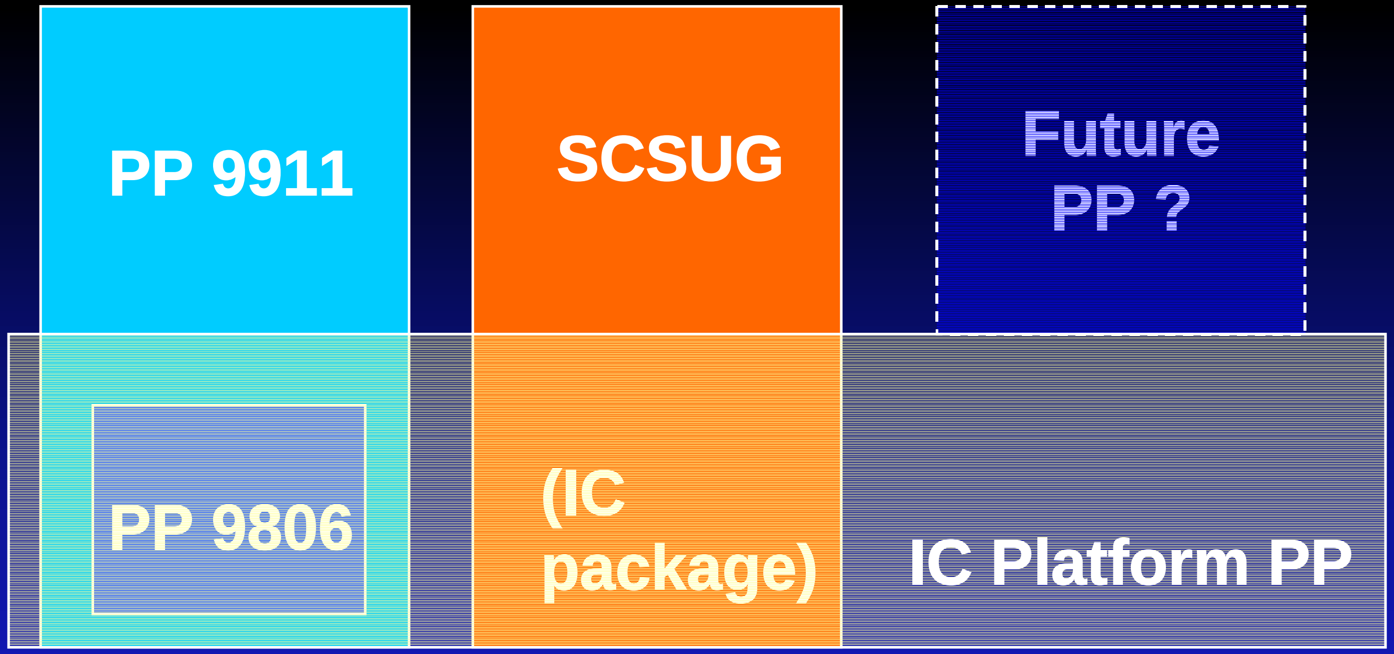
SW1
IC2
3rd Evaluation

Effort

…Re-use and Flexibility (3)

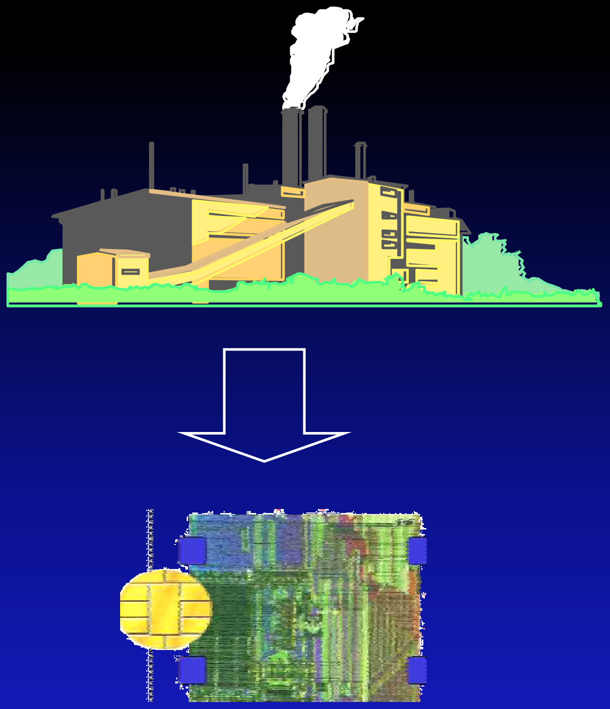


Relationship with other PPs



- The IC Platform Protection Profile is designed to cover:
  - PP/9806
  - The IC package, from the SCSUG PP

Scope and Concept of the PP



Confidentiality and integrity of the TOE during design and manufacture are covered by refinements to the assurance requirements.

Threats against the TOE itself, throughout its lifecycle, are covered by objectives for the TOE (and therefore by functional requirements)

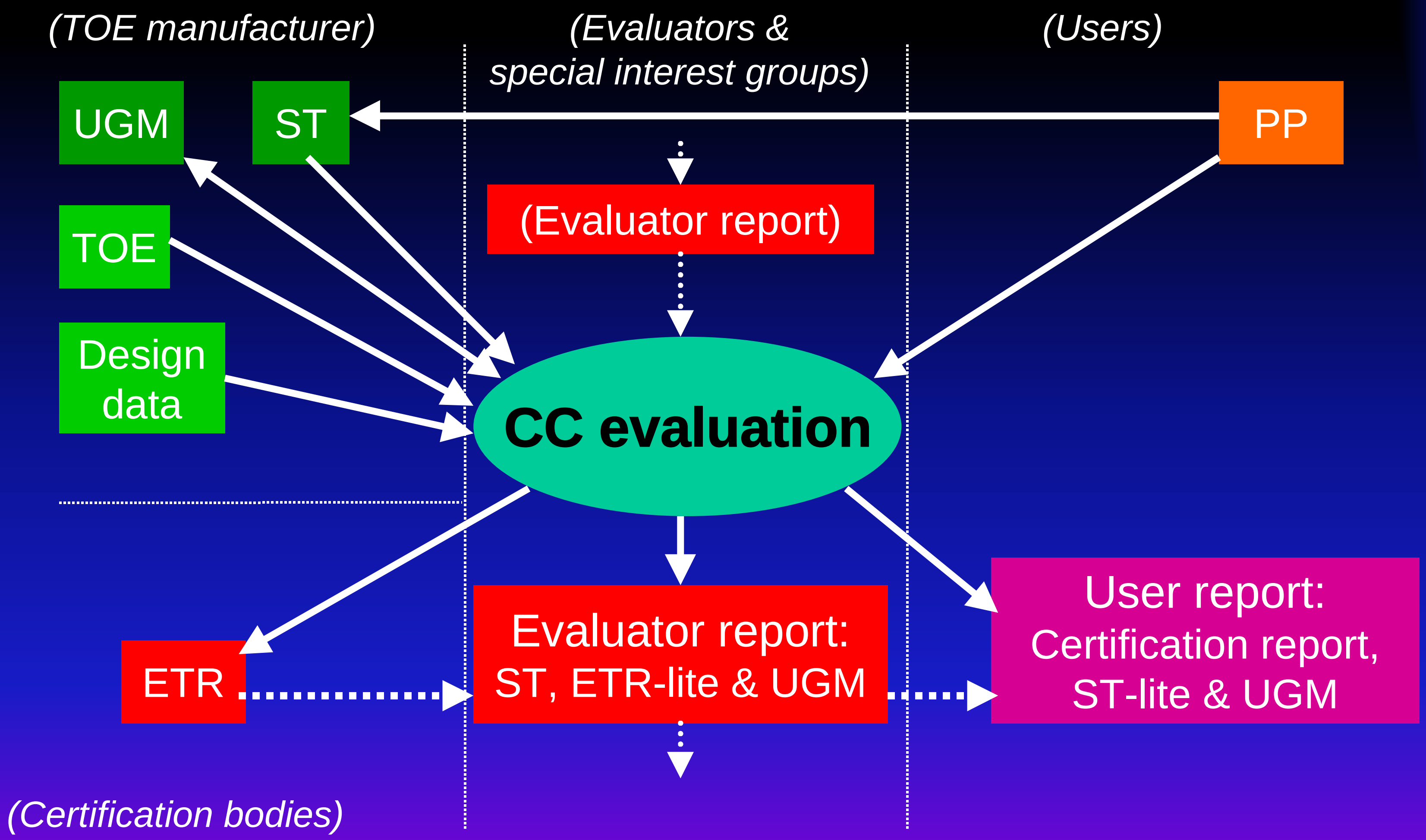
- A generic approach to describing threats ensures the validity of the PP, even if new attacks occur
- The evaluation scheme must ensure that a ‘state-of-the-art’ set of attack methods is always used

Usage

- The modularity and re-use can only happen if:
  - the individual evaluations are planned as modular ones, from the outset
  - the documentation available for re-users is adequate
  - true and effective mutual recognition is achieved

- A model for modular evaluations has been proposed by the major smart card IC manufacturers…

Model for evaluation re-use



Definitions and Assumptions for effective re-use

- User Guidance Manual
  - information required for a software developer to make correct and optimum use of the security features of the TOE
- ETR-lite
  - an approved subset of the Evaluation Technical Report (ETR), sufficient for a second evaluator to integrate the results
- ST-lite
  - an approved subset of the Security Target, suitable for general publication
- Principal assumptions
  - harmonisation of lab. accreditation requirements
  - agreement on the contents of ETR-lite and ST-lite documents

Status of the PP

- Start of process: February 2000
- Agreement on PP development: June 2000
- Presentation of Platform concept: October 2000
- First draft issued for comment: B/December 2000
- Final draft issued for comment: E/March 2001
- Deadline for comments: E/April 2001

- Goal for submission to certifier: B/May 2001
- Goal for certification of PP: June 2001

Key questions for PP users

- Does the PP address the security threats that your application requires?
- Is the PP re-usable and transportable between:
  - different O/S and applications software,
  - different Evaluation Labs.,
  - different Certification Bodies?
- Is the PP internationally recognised?
- What will be your cost and effort to update an evaluation?

In conclusion

- We believe that this new PP can help to make the Common Criteria more practical and effective for smart card developers, because of:
  - maximum re-use and modularity under the CC scheme
  - faster, incremental evaluations
  - extensive consultation with smart card IC users and…
  - a lower cost per product

The latest draft of the IC Platform Protection Profile can be downloaded from:

http:¥¥www.bsi.de/cc/pplist.htm

And finally…

- Thanks to my colleagues at Atmel, Hitachi, Infineon and Philips for the strong collaboration to make this new IC Platform Protection Profile a useful and effective new standard for the smart card market, and
- …thanks to debis IT security services and Bundesamt für Sicherheit in der Informationstechnik for their help in developing this Protection Profile

Thank you

Atmel, Hitachi, Infineon Technologies and Philips Semiconductors