

brightsight®



your
partner
in security
approval



Monique Bakker
+ 31 15 269 2502
bakker@brightsight.com
www.brightsight.com

Unravel smart card composite requirements

A practical guide to CCDB-2007-09-
001

Presentation content

- Introduction on the composite product evaluation document
- Role of the user guidance in a composite evaluation
- Simplifying ASE_COMP activities
- Simplifying ADV_COMP activities
- Conclusion

CCDB-2007-09-001

'The Composite product evaluation for smart card and similar devices' in essence asks the following two questions.

- Does the embedded smartcard software implement the recommendations of the underlying hardware correctly and completely?

- Is the complete composite product resistant against attackers with a high attack potential?

CCDB-2007-09-001

- ❑ Required evidence from the platform evaluation :
 - ❑ Platform security target
 - ❑ Platform open samples for testing
 - ❑ Platform user guidance
 - ❑ Platform ETR_COMP
 - ❑ Platform certification report
- ❑ Required evidence from the composite evaluation:
 - ❑ Design compliance evidence
 - ❑ Composite configuration evidence
 - ❑ Delivery and acceptance procedures
 - ❑ All evidence for the composite (application) evaluation, including security target, design documentation and security architecture description.

- ❑ JIL attack potential document

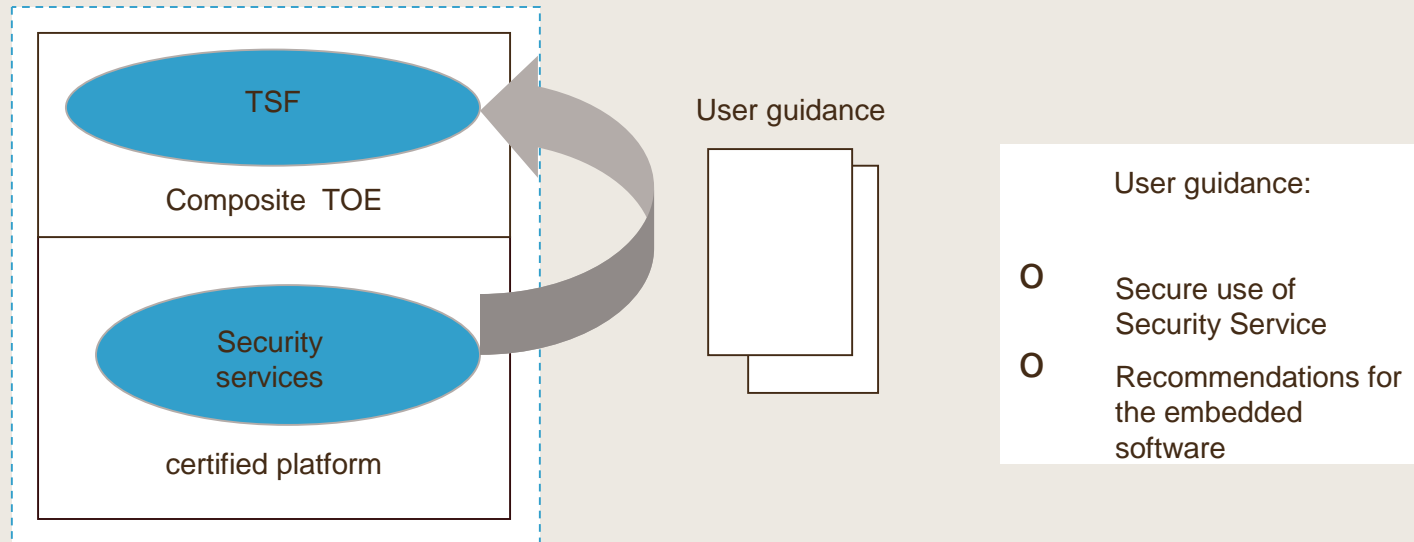
Scope of the presentation

- Concentrate on the SFRs

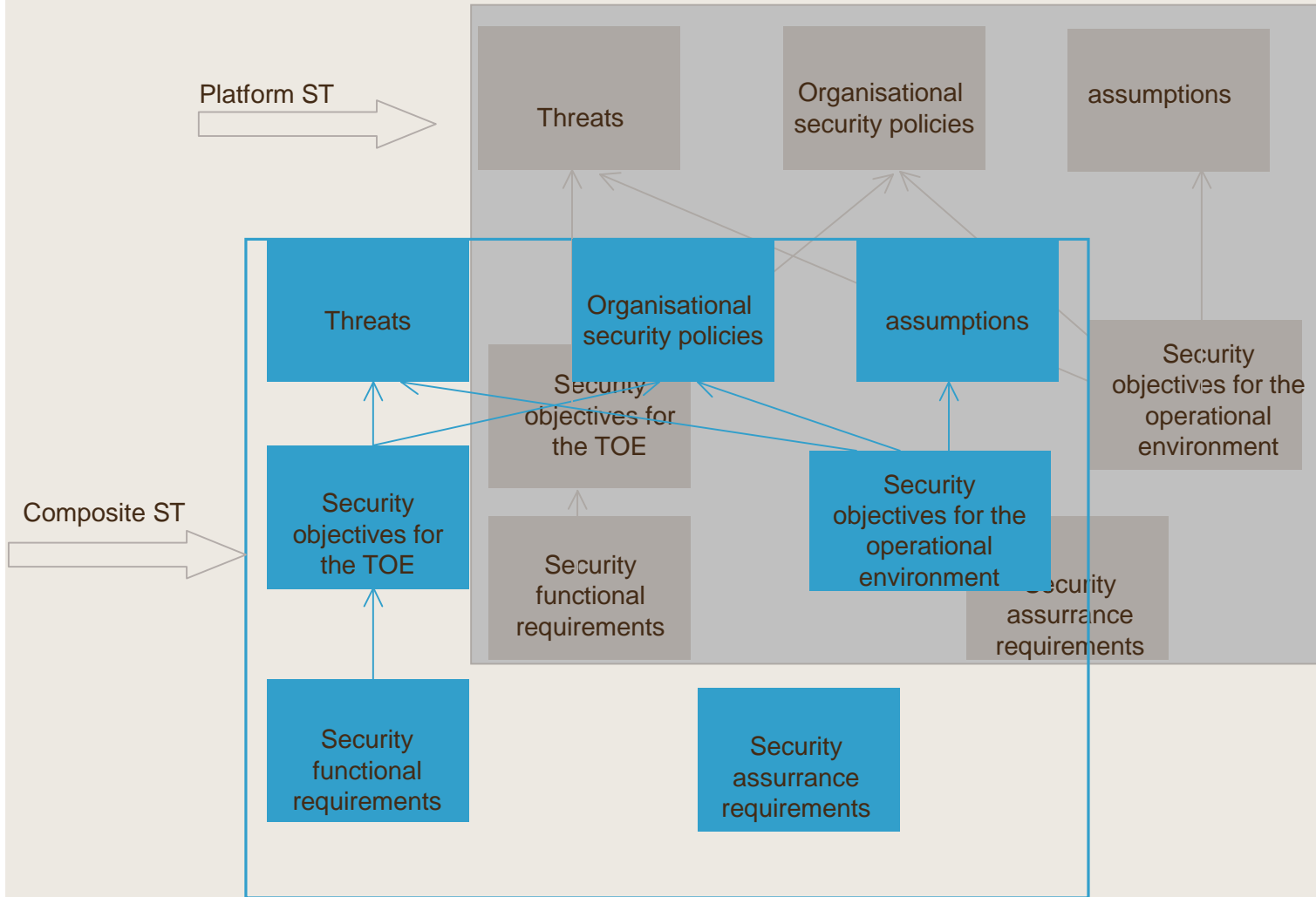
ASE Comp

ADV Comp

The role of the user guidance

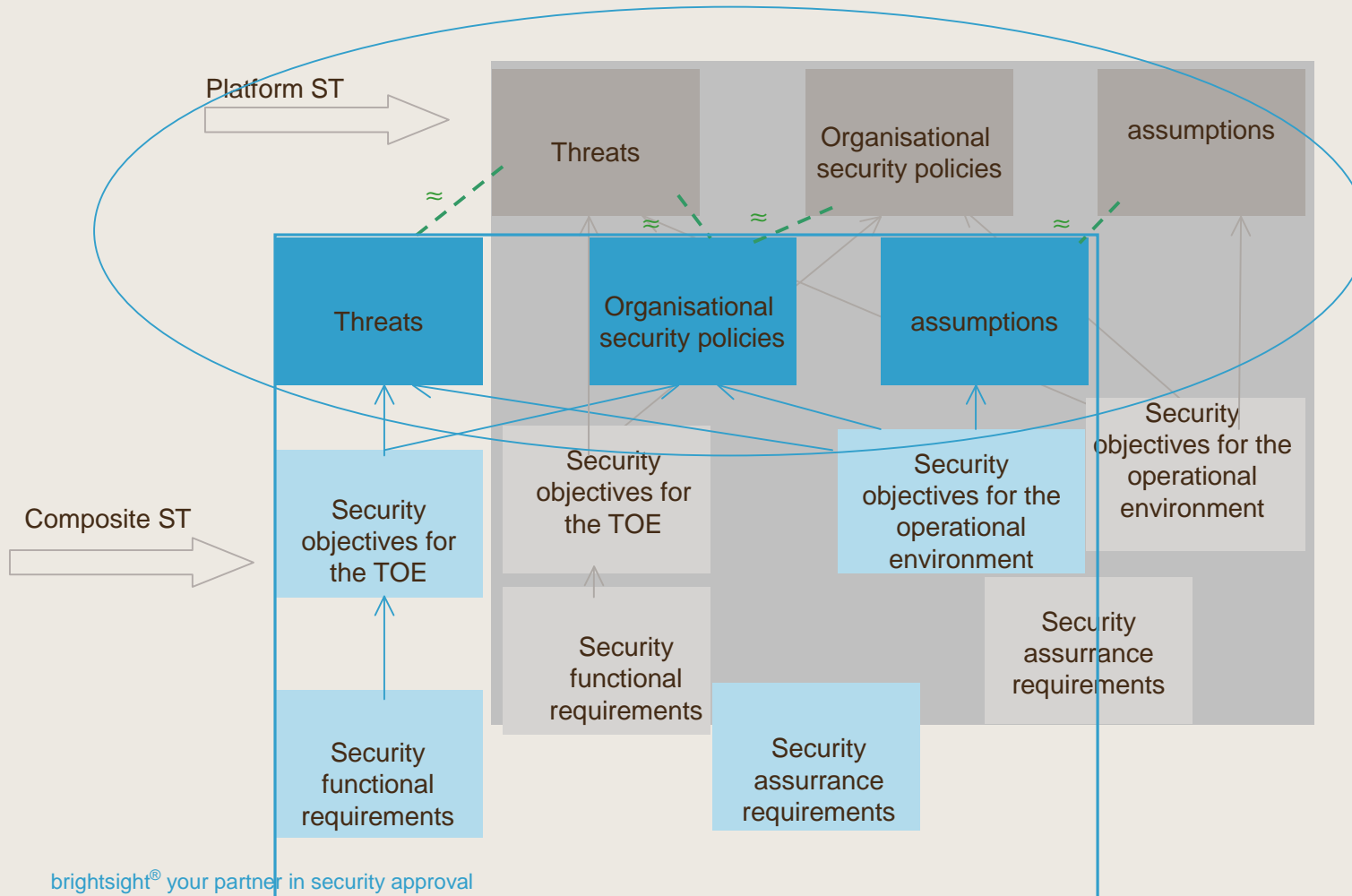


ASE_COMP activities



ASE_COMP activities

The SPD for the composed TOE is consistent with that specified in the component TOEs



Result of ASE_COMP

- A set of **relevant SFRs** realised by Security Services in the certified platform reused in in the composite TOE
 - In **USE_CASE A** the relevant SFRs comprise the SFRs that implement security services that are used in ADV_ARC as security mechanism to explain how the TOE protects itself from tampering and bypassing
 - In **USE_CASE B** the relevant SFRs are identical to a subset of SFRs presented in the composite ST and (partly) will also be used in ADV_ARC in the role of security mechanism.

ADV_COMP

- The evaluator shall examine the rationale for design compliance to determine that all applicable requirements on the application, imposed by the underlying platform are fulfilled by the composite product
 - evidence compliance 1:
 - 100% match all requirements are followed
 - evidence compliance 2:
 - Recommendation is not followed because it is not applicable
 - Recommendation is not followed and an alternative solution is implemented

ADV_COMP and ADV_ARC

- Content of ADV_ARC
 - Security domain separation
 - Secure initialisation
 - Protection from tampering
 - Non-bypassability

- JIL Security architecture requirements
 - “Cooperation of security mechanisms” in JIL ADV_ARC
 - “JIL Application of Attack Potential to Smart Cards” shall be considered

ADV_COMP and ADV_ARC

□ Content of ADV_ARC

- Security domain separation

□ Secure initialisation

- *The sequence at startup follows the recommendations of the HW platform*
- *Composite specific steps at startup*

□ Protection from tampering and Non-bypassability

- **ETR for Composition - JIL Application of Attack Potential for Smart Cards**

- *What is provided by the underlying hardware platform*
- security mechanisms and security services support against attacks
 - *Security recommendations of the HW platform are reflected in these mechanisms*

□ JIL Security architecture requirements

□ Cooperation of security mechanisms

- *Security services acting as security mechanisms of the underlying HW platform and thus relevant SFRs*

Result of ADV_COMP

- Design compliance is fully reflected in ADV_ARC
 - The TOE is protected against an attack:
 - Through platform mechanism + relevant security service when the user guidance is followed
 - Through platform mechanism+ user guidance recommendations that are followed by the application (embedded software)
 - Additional mechanism implemented
 - Relevant platform SFRs implement security services that are used as security mechanisms in the descriptions of ADV_ARC

ADV_IMP and ADV_TDS contribute in showing that
the description faithfully describes what is implemented

Conclusion

- Platform ST and Composite ST (ASE_COMP)
 - Identify relevant SFRs
 - Check that objectives for the environment and security assurance fits

- Design compliance, user guidance (ADV_COMP)
 - What is provided by the platform -> ETR for Composition (ADV_ARC)
 - Cooperation of security mechanisms -> security services in the role of security mechanism of the platform (ADV_ARC)
 - Followed recommendations contribute to protection against attacks -> (ADV_ARC)

brightsight®

Questions?



Contact information

Monique Bakker

Jan Blonk

Olaf Tettero

Bright sight BV

Delftechpark 1

2628 XJ Delft

The netherlands

Tel., : +31-152692500

Fax : +31-152692555

E-mail: info@brightsight.com

url: www.brightsight.com

