Predictive Assurance

Bundesamt für Sicherheit in der Informationstechnik (BSI)
(Federal Office for Information Security)

9 ICCC – Jeju, Korea
September 2008

Irmela Ruhrmann
Head of Division Certification, Approval and Conformity Testing

Agenda

- Definitions & Objectives
- History
- Current Status
- Additional Sources of Input
- Open Issues
- Outlook

- **Definitions & Objectives**

Predictive Assurance

- Problem: product certificate is frequently obsolete at, or shortly after, the certification date:
  - evaluated configuration not purchasable
  - need to operate product other than in the evaluated configuration
  - patches issued since certification date
- Solution: greater emphasis on the developer's original development process and the update and flaw remediation process
- Goal: Provide a degree of 'predictive assurance' where the conclusions of an evaluation report could remain valid for a much more realistic and usable length of time

Focus of Approach

- Focus on software products
  - Patches are released more often than with hardware
  - Hardware and smartcards development process different from software development
    - more structured, documented design (HDL)
    - security aspects highly important for vendor and considered during design

- **History**

Assurance Maintenance – CC 2.1 (1)

- Concept to assure maintenance as changes are made to the TOE or its environment (CCV2.1), e.g.
  - correction of bugs found in the certified TOE
  - updates to the functionality provided
  - same TOE, but on a different hardware or software
- evidence of assurance maintenance independently checked by an evaluator at certain points

Assurance Maintenance – CC 2.1 (2)

- Flaw Remediation (ALC_FLR) part of Assurance Maintenance

- Security impact analysis
  - security impact of all changes effecting the TOE, performed by developer
  - Important element for Assurance Continuity

Experience gained used as input for predictive assurance

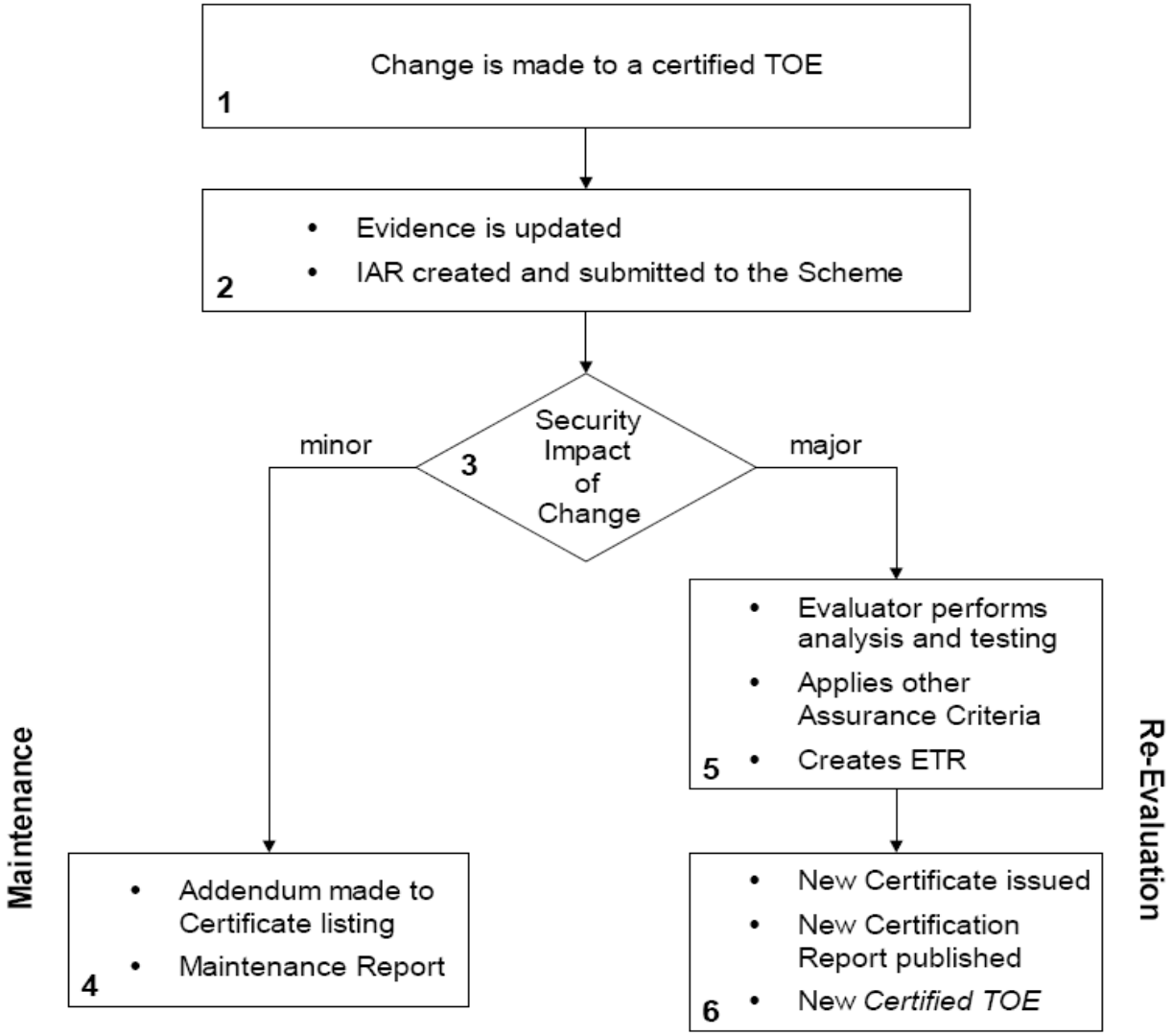
- **Current Status**

Assurance Continuity

CCDB Document 2004-02-09 “Assurance Continuity: CCRA Requirements”

- Assurance Continuity provides an approach to extend the validity of a certificate for a limited scope of changes without re-evaluation
- Developer has to maintain all developer evidence, conduct and record appropriate testing and confirm that previous analysis results have not been affected by changes to the TOE
- Results have to be described in an impact analysis report and presented to the CB

Assurance Continuity Paradigm
CCDB-2004-02-09



Assurance Continuity

CCRA requirements:

- Guidance on characterisation of change - minor/major
- Guidance on performing impact analysis
- Requirements for content and presentation of the impact analysis report (IAR)

- Maintenance approach successfully used in practice for hardware and software products, e.g.
  smartcard controller, printer controller, digital tachograph component, data diode, firewall, certificate manager
- Some applications for maintenance were disapproved - recertification instead

Assurance Continuity

Characterisation of change - minor/major

minor change:

- Impact is sufficiently minimal that it does not affect the assurance of the TOE
- Evaluator activities do not need to be independently re-applied - developer is expected to have tested the changes as part of his standard regression testing

major change:

- Impact is substantial enough that it does affect the assurance of the TOE
- Independent re-application of the evaluator activities is needed

Assurance Continuity

Examples for minor/major changes

minor change:

- Changes to the IT-environment that do not affect assurance
- Editorial changes to the assurance evidence
- Changes to TOE that do not affect assurance

major change:

- Changes to the claimed set of assurance requirements
- Changes to the claimed set of functional requirements
- Use of procedures in the development environment not assessed in the original evaluation

Surveillance

Process to monitor ongoing security performance of certified products in respect to

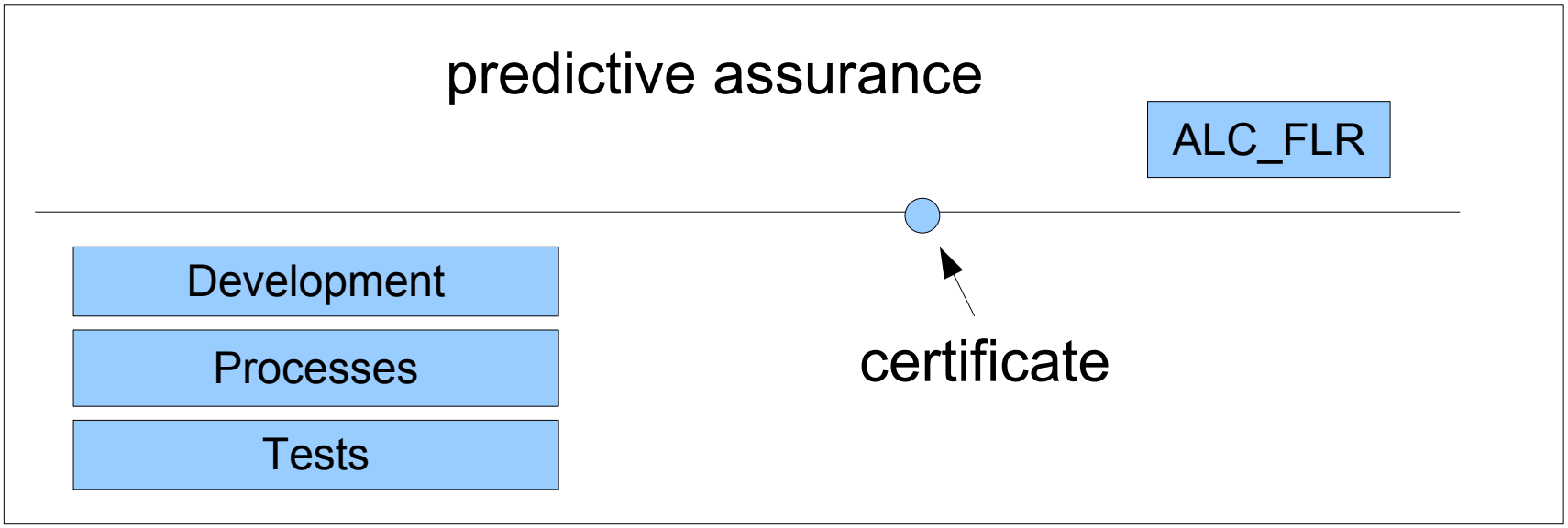
- Validity of Guidance documentation
- (Public) vulnerabilites

at certain intervals, e.g. 6 months, 1 year

Implemented in France mainly for smartcard products

Flaw Remediation (ALC_FLR)

- ALC_FLR can be implemented for finished products, whereas predictive assurance has to be implemented in the development process



- ALC_FLR one important element of predictive assurance

- **Other Sources of Input**

Security Development Lifecycle[1]

- Process used by Microsoft in software development on top of regular SW development process
- Important Aspects:
  - Security Training of Development Teams e. g. Security Design Best Practices
  - Use of Security Development Tools and Best Practices
  - Security Documentation
  - Security Penetration Testing
  - Security Reviews

[1] Source: The Security Development Lifecycle – Michael Howard and Steve Lipner

Low Level Assurance Scheme in BSI

- certificate with time limit on validity, EAL 1+
- development environment is “trustworthy”, evaluated in baseline certification
  - ALC aspects
  - process view as in ISO 9000
- minor security relevant changes within period of validity: certificate valid for those changes
- after period of validity: quality check by CB, may involve lab
  - period of validity extended or re-certification

US/UK Evidence Based Trial

Development and Trial of Assurance model for large software products

Results will be used for development of supporting documents or as input for CC V4.0

- **Open Issues**

Test Requirements (Tools)

- What type of tests are required by the developer for predictive assurance?
  - Penetration tests?
  - Evaluator tests?
  - Suggestion: extensive test suite (FUN, PEN) agreed by evaluator and CB in baseline certification - performed after each change
- Dependence on EAL level as ATE and AVA_VAN is involved

Site Certification

- Generic approach to evaluate site aspects independently from specific product
- Definition of evaluation depending on Site and Site Security Target (SST)
  - compulsory elements
  - optional elements (e.g. inclusion of TAT, FLR possible)
- Process could be used as a basis and supplemented by requirements and methodology for predictive assurance

Period of Validity

- Criteria for re-evaluation:
  - new security functions
  - new security objectives
  - new threats
  - change in development process
    question: how much change is allowed?
- Definite timeline comparable to Assurance Maintenance

Relation to Re-evaluation

- Re-evaluation will be facilitated if predictive assurance is used in baseline certification
- Problem to apply predictive assurance in re-evaluation if not applied in baseline certification
- Predictive assurance as mandatory requirement a problem as it cannot be applied retrospectively

- **Outlook**

Planning of Lead Nation Project (1)

Lead: GE
Contributing Nations: UK, US, SP, KR, NO, SE

- Review existing scheme activities
- Review sources of input as mentioned above
- Address open issues
- Analyse how surveillance could be used for general software case
- Review all suggestions against CCRA priciples
- Identify any conflicts with related certification principles - e.g. EN 45011

Planning of Lead Nation Project (2)

- Define detailed development plan
- Specify assurance model, roles and responsibilities to be applied
- Specify assurance sources required – e.g. technical activities, development practices, testing, vulnerability assessment etc.
- Produce a generic form of developers approach in respect to security
- Examine the possibility of 'ramping up' for vendors coming into the certification process
- Suggest suitable approaches for trialling
- Engage with representative set of vendors

Planning of Lead Nation Project (3)

- Propose how to incorporate into Supporting Documents/ CC/CEM taking account of the principle of not changing approach for smartcards and similar devices
- Define the general criteria for evaluators to define constraints and applications of the predictive assurance phase
- Suggest suitable triggers for re-evaluation
- Trial the above in an evaluation
- Ensure that the level of predictive assurance varies appropiately with assurance level (especially time of validity)
- Ensure that evidence from processes examined in predictive assurance support the Evidence based Approach

Contact

Federal Office for Information Security
(BSI)

Certification
Godesberger Allee 185-189
53175 Bonn
Germany

Tel: +49 22899-9582-111
Fax: +49 22899-10-9582-5477

zerti@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de