Multi-Level Certifications
Using Lower EALs as Project Milestones

Bertolt Krüger, SRC Security Research & Consulting GmbH
Christian Tobias, Utimaco Safeware
ICCC 2008, Jeju, South Korea

SRC security consulting

utimaco® safeware

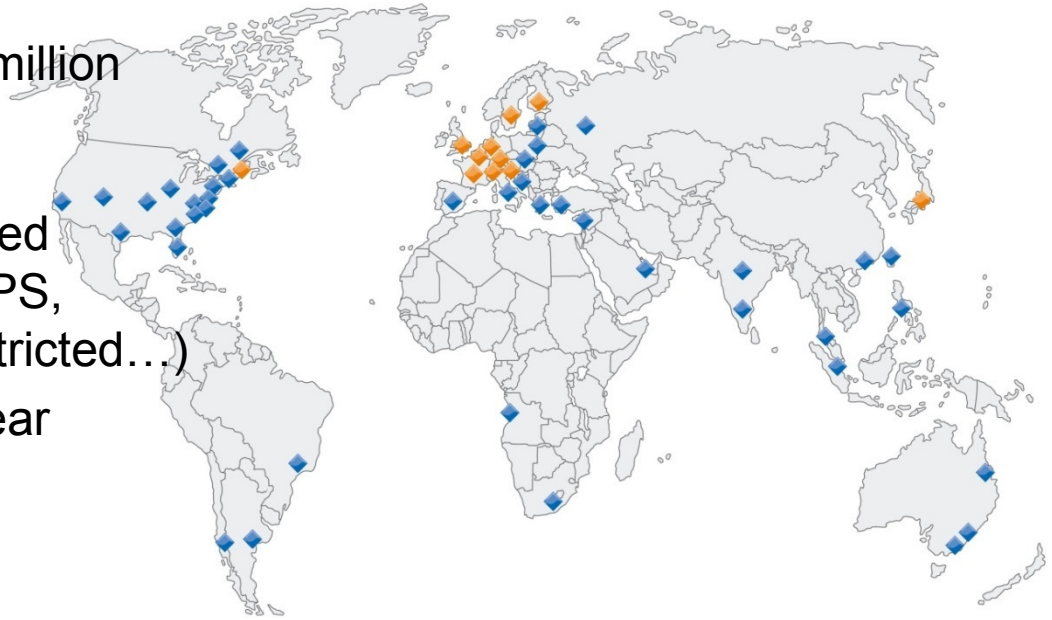
Highlights

- CC Market Requirements for Full Disk Encryption (FDE) Products
- Conflict of Goals for Vendors
- Proposed Approach: Multi-Level Certifications
  - Introduction and Organisation
  - Impact on project schedule and budget
  - Challenges
- Wrap-up and Discussion

Utimaco Safeware

Celebrating 25 Years of Protecting Information Worldwide

- Founded in 1983
- Revenue FY 2007/08: €55.9 million
- 300+ employees worldwide
- Committed to provide evaluated and certified solutions (i.e. FIPS, Common Criteria, NATO Restricted…)
- About 3-5 certifications per year
- Certifications in Germany, Japan und the US.



SRC Security Research and Consulting GmbH

- Background
  - Founded in August 2000 by German financial industry
  - Employees: 52
  - Headquarter: Bonn, Germany
- Consultancy on Secure Systems throughout the lifecycle
  - Independent
  - Customer- and project-oriented solutions
  - Through highly qualified consultants
  - With international focus
- Some fields of expertise
  - Common Criteria evaluation facility
  - Specialist for payment schemes, in particular smart card based
  - Information Security Management Systems
  - Ethical Hacking and Forensics
  - Auditor according to Payment Card Industry (PCI) Standards (PED, DSS, PA-DSS)
- More information available at: http://www.src-gmbh.de

General Conditions for Vendors

- Certain markets require a (Common Criteria) Certificate
  - The Time-to-Certificate is one of the most critical parameters for vendors.
- Often heard critical comments regarding CC
  - Takes too long
  - Is too expensive
- Conflict of goals

Full Disk Encryption Market

- Certifications (CC and FIPS 140) are required in many calls for tender.
- Market situation:
  - 6 Products with CC certificate
    - EAL 4: 3 products
    - EAL 3: 1 product
    - EAL 2: 1 product
    - EAL 1: 1 product
  - 2 CC certifications in progress (EAL 4)
  - 2 well-known vendors ignoring CC

Market Situation for Utimaco

- SafeGuard Easy is a full disk encryption solution with a strong certification history.
- Gradual deplacement of SafeGuard Easy by the newly developed product suite SafeGuard Enterprise.
- CC Certification of SafeGuard Enterprise is a market need.
- Conflict of objectives:
  - EAL 4 is needed to be competitive.
  - A CC certificate is needed as soon as possible.

Approach to Resolve this Conflict

- Assumptions:
  - EAL 4 is about 1.5 – 2 times as time-consuming as EAL 3
  - The Low Level Design (LLD) is the main reason for this difference
- Solution: Do a multi-level certification!
  - Step 1: EAL 3+
    - Can be obtained significantly faster
    - Sufficient to open part of the FDE market
    - Sufficient to start national approvals
  - Step 2: EAL 4
    - Obtained via a re-certification
    - Sufficient to address all of the FDE market

Comparison of Assurance Requirements

Assurance Class	EAL 3	EAL 4
ACM_AUT	-	1
ACM_CAP	3	4
ACM_SCP	1	2
ADO_DEL	1	2
ADO_IGS	1	1
ADV_FSP	1	2
ADV_HLD	2	2
ADV_IMP	-	1
ADV_LLD	-	1
ADV_RCR	1	1
ADV_SPM	-	1

AGD_ADM	1	1
AGD_USR	1	1
ALC_DVS	1	1
ALC_LCD	-	1
ALC_TAT	-	1
ATE_COV	2	2
ATE_DPT	1	1
ATE_FUN	1	1
ATE_IND	2	2
AVA_MSU	1	2
AVA_SOF	1	1
AVA_VLA	1	2

- All components depending on the LLD are marked in orange.
- All components that can be covered in EAL 3+ are marked in blue.

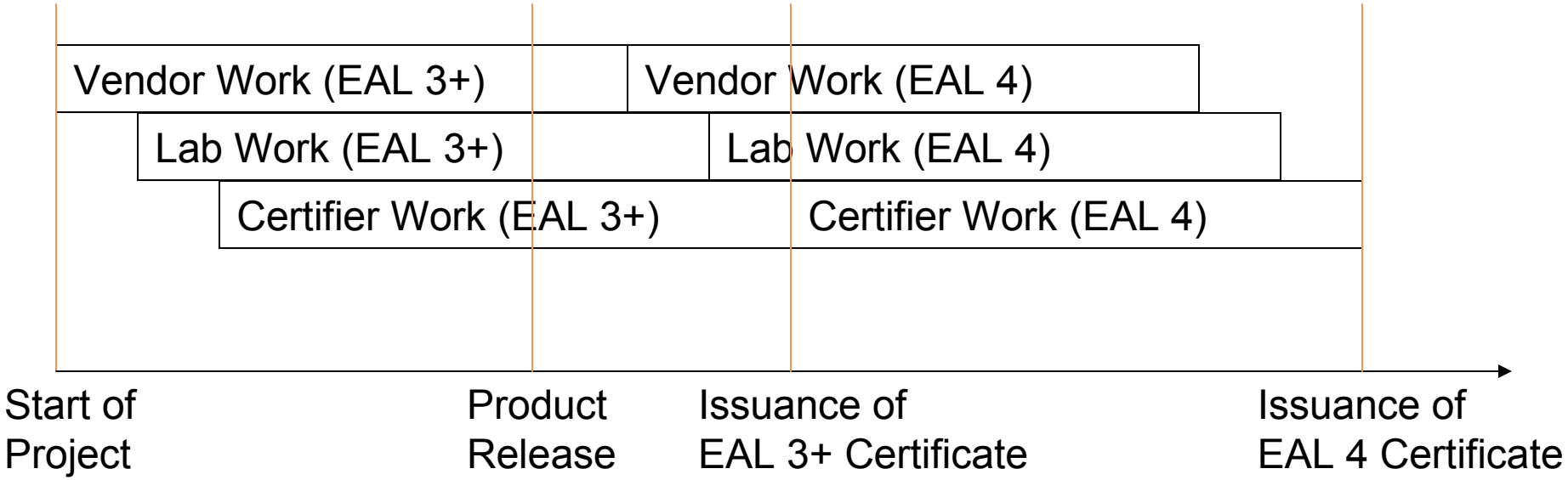
How Realistic is this Approach?

- 2 Core Questions:
  - How much longer will the 2-step approach take (compared to a direct EAL 4 certification)?
  - How much more will it cost?

Estimated Lab Costs (before project start)

	Difference in project runtime	Difference in lab costs
Lab 1	30 %	≈ 37 %
Lab 2	0 %	< 3%
Lab 3	40 %	≈ 18 %

Ideal Timeline

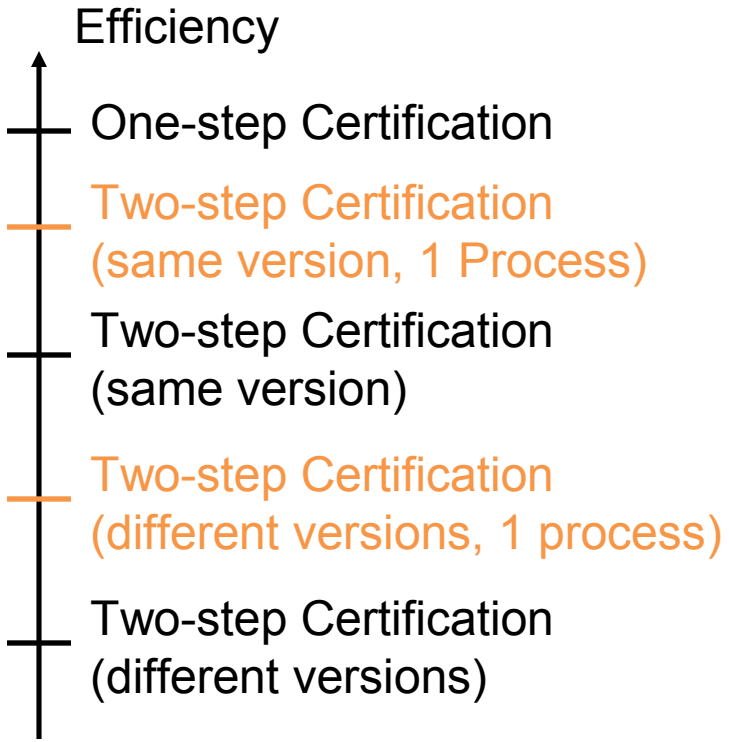


Delays are Expensive

- If the certification takes longer than expected (standard case?), a newer product version can be submitted.
- In the two-step process this is possible without limitations in the first phase only.
- If the product version is changed in the second phase, version-specific work (e.g. independent testing) has to be redone.
  - Project schedule and budget are at risk.

Comparison of Efficiency

- Two certification processes are necessary to reach final goal.
- Administrative Overhead.
- A multilevel certification in only one process would reduce that overhead.



- Adoption of Multi-Level Certifications by Certification Bodies or the CC in general would help minimize the overhead and increase the efficiency of the process.

Challenge: Publication

- Certification bodies publish lists of products in evaluation.
- A Re-Certification cannot be started officially before the base certification is finished.
- At project start only the base certification will be published not indicating the targeted EAL correctly.

Wrap-up

- CC Certification processes are very time-consuming.
- If a CC certificate is finally issued, the certified version may not even be the newest product version.
- The presented approach
  - leads to a significant shorter time-to-certificate,
  - can be used without changing the CC certification process and
  - leads to an (administrative) overhead.
- Appeal to the Certification bodies: adopt this process

Thank you for your attention!

Any Questions?

Dr. Bertolt Krüger
SRC Security Research and Consulting

Bertolt.Krueger@src-gmbh.de
+49 228 2806 122

Dr. Christian Tobias
Utimaco Safeware AG

Christian.Tobias@utimaco.de
+49 6171 88 1711