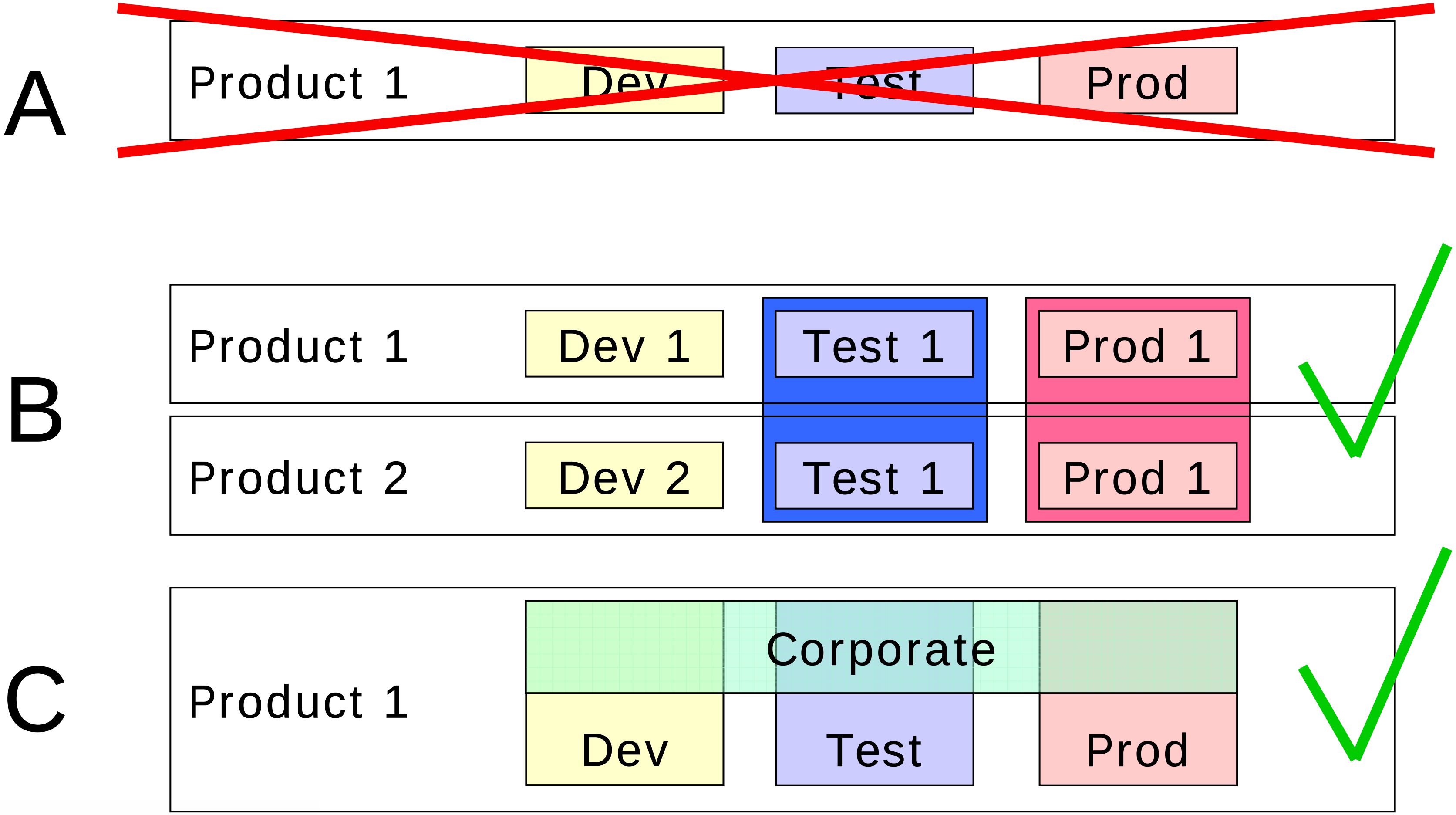
How to Write Site Security Targets

Gerald Krummeck – atsec, Germany/USA
Frank Sonnenberg – BSI, Germany
Thomas Borsch – BSI, Germany
Dirk Jan Out – TNO, Netherlands
Thomas Schröder – T-Systems, Germany

How to Write
Site Security Targets

- Situation – the network
- Strategy – defining the SST realms
- Carving – shaping the Site
- Authoring – writing the SST
  - SSTs and STs
  - Authoring the document
- Evaluation – AST report
- Lessons learned (so far)

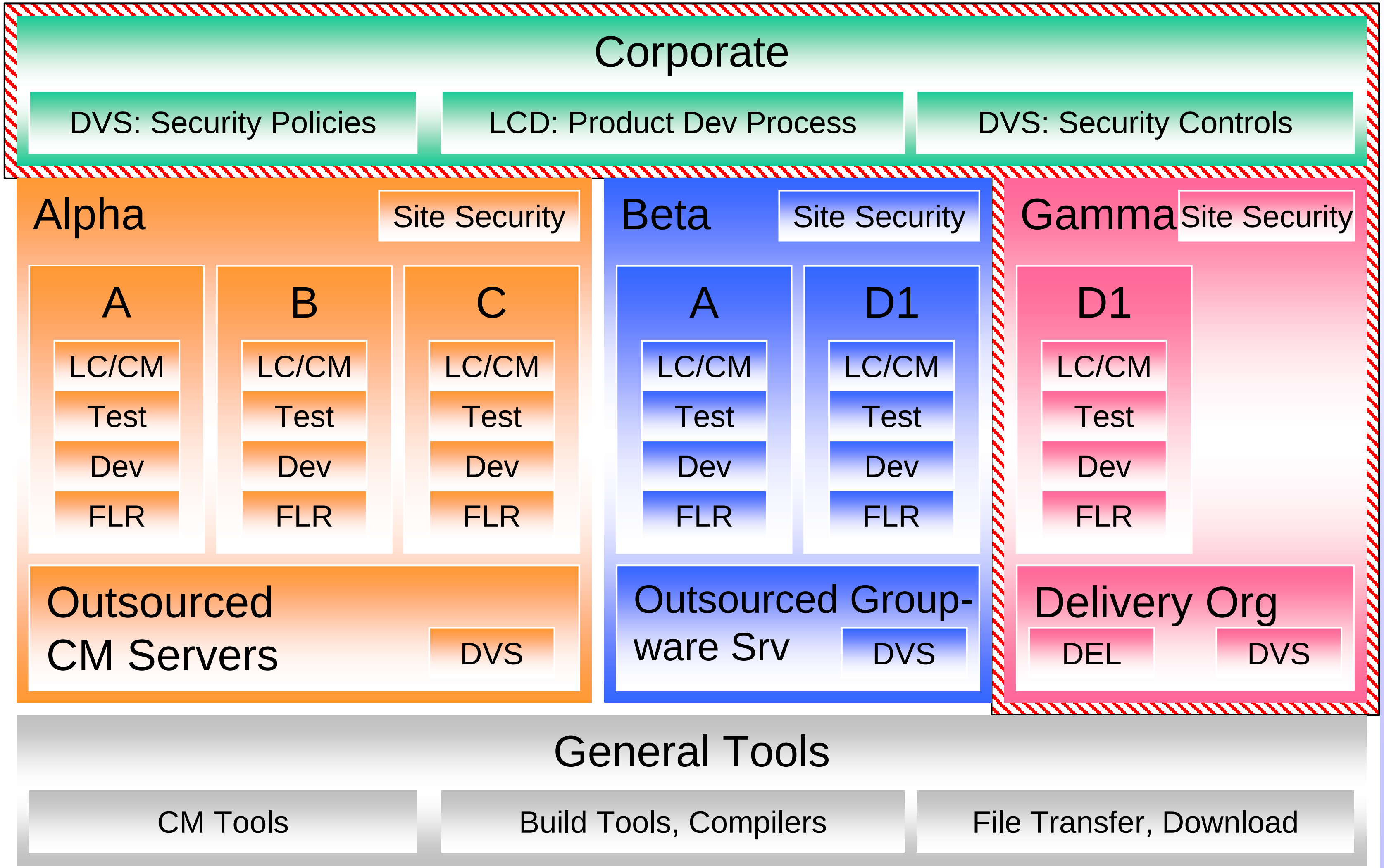
Site Certificates ... for whom?



The Network

Product	Evaluation Aspect					
	ADV	AGD	ATE	DEL	SRV	FLR
A 1	Alpha S 1	Alpha S 1	S 1	Gamma	Beta	Alpha S 1
A 2	Alpha	Alpha	Alpha	Gamma	Alpha Beta	Alpha
A 3	Alpha S 2	Alpha	Alpha	Gamma	Alpha Beta	Alpha Delta
A 4	Beta Delta S 3	Beta Delta S 3	Beta Delta S 3	Gamma	Beta S 3	Beta Delta S 3
B 1	Alpha S 4	Alpha	Alpha S 4	Gamma	Alpha	Alpha S 4
C		Alpha	Alpha		Alpha	
D 1	Kappa Beta Gamma	Kappa Gamma	Kappa Beta	Gamma	Kappa	Kappa Beta Gamma

Shaping the Sites



Corporate

DVS: Security Policies

LCD: Product Dev Process

DVS: Security Controls

Alpha

Site Security

A: LC/CM, Test, Dev, FLR

B: LC/CM, Test, Dev, FLR

C: LC/CM, Test, Dev, FLR

Outsourced CM Servers

DVS

Beta

Site Security

A: LC/CM, Test, Dev, FLR

D1: LC/CM, Test, Dev, FLR

Outsourced Group-ware Srv

DVS

Gamma

Site Security

D1: LC/CM, Test, Dev, FLR

Delivery Org

DEL

DVS

General Tools

CM Tools

Build Tools, Compilers

File Transfer, Download

Authoring an SST

- SST content
- Comparing STs and SSTs
- What to put into the the SST

SST Content

1. Introduction
2. Conformance Claim
3. Security Problem Definition
4. Security Objectives
5. Extended Components Definition
6. Security Requirements
7. Site Summary Specification
8. Rationale

Comparing STs and SSTs

- SST borrows model, terminology and structure from ST
  - Well-known model (threats, OSPs, objectives, security requirements, and description of requirement fulfillment)
  - ST becomes SST, TSS becomes SSS
- No security functional requirements (SFRs)
  - Since the SST is not tied to a product, SFRs are irrelevant
- Emphasis on processes in Site Security Specification

Introduction

- SST reference
  - Title, version, date, author, address
- Site description
  - Physical scope: map
  - Logical scope: life cycle parts (development, testing, production, delivery)
  - Justification: why this combination?

Conformance Claim

- Conformance to CC V3.1
- No extended security assurance requirements (chapter 5)
- List of security assurance requirements (chapter 6)

Security Problem Definition: Threats

- Physical and logical security
  - Physical access to restricted areas
  - Logical access to critical IT systems
  - Access to restricted information
- Development process
  - Modification of code, design or guidance docs
  - Development mixup through missing synchronization or in wrong development branch
  - Bypass of verification/review steps in development process
- Delivery
  - Manipulation of delivery package (or its contents) during transmission or delivery

Security Problem Definition: OSPs

- P.CLASSIFICATION
  - Proper classification of all code and documents

Security Objectives

- All objectives derived 1:1 from threats
- P.CLASSIFICATION mapped to
  - O.CLASSIFICATION and
  - O.INFO_ACCESS (controlled access to restricted information)

- **Threats, OSPs, and objectives are boilerplate**
- **Upgrade required for confidentiality of development environment (mostly for hardware development)**

Security Requirements

ALC_CMC.4	Production support, acceptance procedures, and automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer-defined life-cycle model
ALC_TAT.1	Well-defined development tools

Application notes: used to clarify applicability of requirements to different environments within the site

Site Summary Specification

- Structured for easy mapping of security requirements

ALC_DVS

- General security regulations
  - Corporate standards
- Physical security
  - Fences, CCTV, secure areas, guards, badges, fire alarms, etc.
- Personnel security
  - Hiring and leaving, training, information, incident reporting
- Logical security
  - Classification, access to IT systems, hardening, secure communications (teleworking)

Site Summary Specification

ALC_LCD

- Development life cycle
  - Life-cycle-model, processes

ALC_CMC, ALC_CMS

- Configuration management
  - Processes, tools

Don‘t focus on the configuration list, but how it is produced!

Site Summary Specification

ADO_DEL

- Delivery procedures
  - Physical delivery
  - Electronic delivery

SST Evaluation

- Straightforward task
- Things to look for:
  - Site description must define boundaries that are precise enough for splicing in TOE evaluation
  - Site security specification (SSS) should be self-sufficient; other evaluators may not have access to all evaluation evidence

Other evaluators must be able to use the SST in their evaluations without re-evaluating the SST or re-reading all the evidence

Lessons learned so far

- SST concept fits nicely into current CC model
- Formal content of SST
  - may be questionable, because requirements are derived from other evaluations
  - allows authoring and evaluation without significant overhead
  - allows SST to stand on its own as a complete and consistent document
- Customers and evaluators quickly get used to the concept:

Can‘t we do this as a site certification?