How to Create a slim and comprehensive PP: The Frame Approach

Igor Furgel
T-Systems

14th ICCC

What are we speaking about?

- Motivation
- The ‘frame approach’ as a solution
- Application example: good practice
- Advantages and references

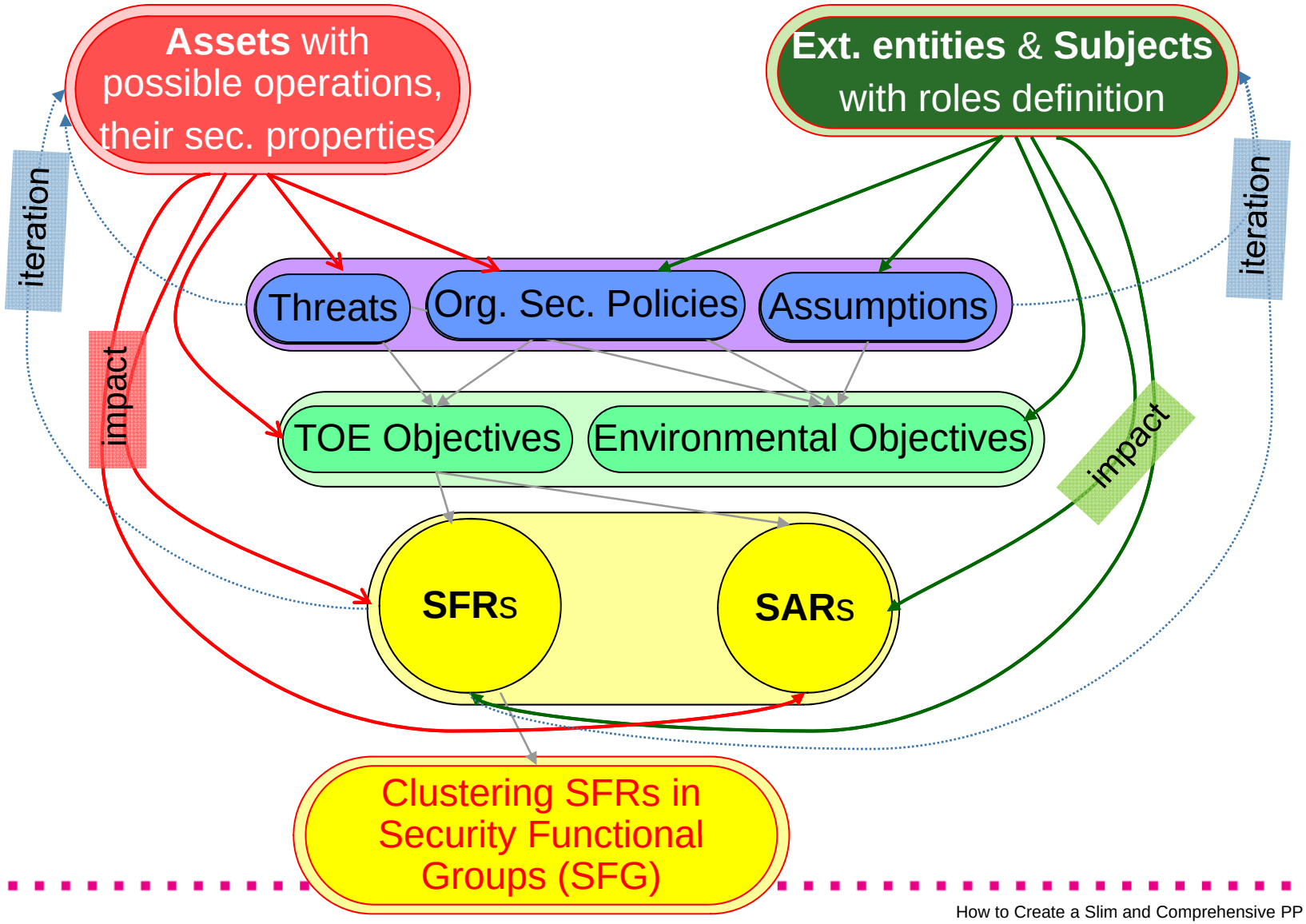
Motivation

- Protection Profiles (PP) have already become a useful and powerful standardisation instrument.
  - It is a good news.
- As a result, there are currently hundreds certified PPs for different IT product classes
- Several PPs are quite extensive:
  - a lot of formal items confuses readers with the question in their eyes at the end of reading:
    - which assets once again should the TOE protect?
    - It is the bad news.

- For this reason, a clear, transparent and standardised praxis for the development of comprehensive, non-confusing and certifiable PPs is helpful and indispensable
- This talk deals with the concrete working praxis ensuring comprehensiveness and clearness of the resulting PP

The ‘Frame Approach’: Stick to Ariadne’s Thread

Do not be frightened ☺



The ‘Frame Approach’: Stick to Ariadne’s Thread

- APE_INT
  - Define physical and logical TOE scope

- APE_SPD
  - Make a slim, but technically sound choice of
    - **assets**,
    - possible **operations** on them and
    - their **security properties**

    to be protected and maintained by the PP security policy
  - Determine the minimal necessary set of
    - **subjects** and
    - **external entities**

    pertained to the set of the assets
  - Define {threats, OSPs and assumptions} directly derived from and exactly aligned with the assets, operations, their security properties, subjects and external entities

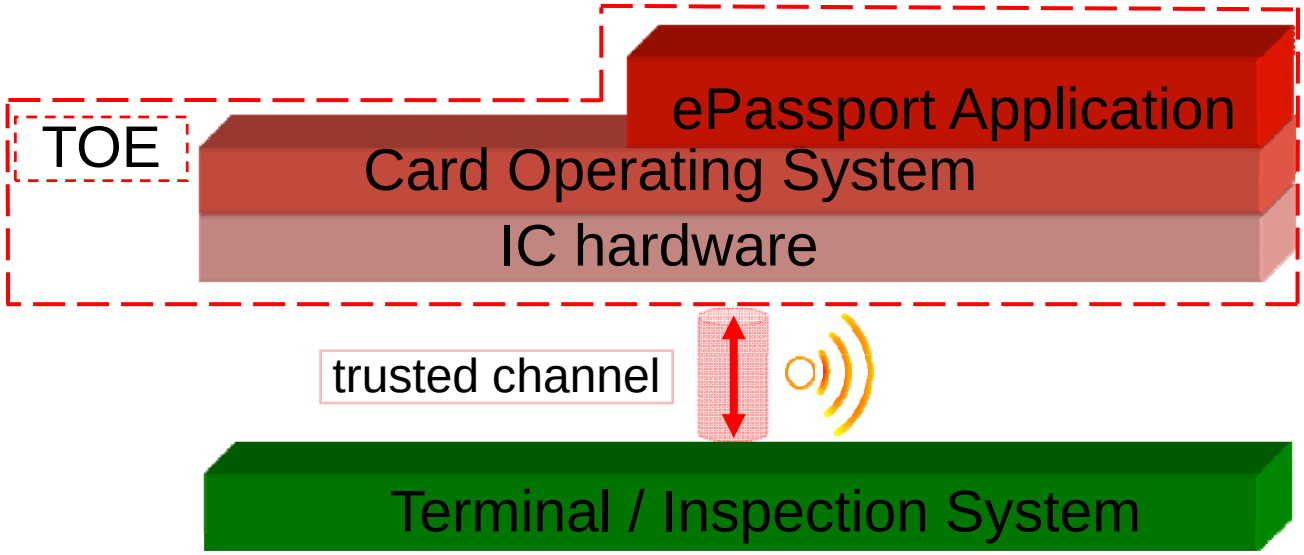
The ‘Frame Approach’: Stick to Ariadne’s Thread

- APE_OBJ
  - Precisely align TOE Security Objectives with the security properties of the assets
- APE_REQ
  - Complete CC operations like *assignment*, *selection* and *refinement* in single SFRs only using the assets, possible operations on them, their security properties and subjects as defined in APE_SPD
  - Cluster single SFRs in Security Functional Groups (SFG) in a logical way:
    - each Group supports a dedicated TOE security service as stated in the logical TOE scope in APE_INT
- READY.

Example: ePassport: APE_INT: Physical Scope

Terminal

TOE



Example: ePassport: APE_INT: Logical Scope (BSI-CC-PP-0068)

- TOE major security features
  - User Data in the TOE:
    Only terminals possessing authorisation information can get access to the user data stored in the TOE and use security functionality of the ePass
  - User Data in the communication channel:
    Verifying *authenticity* and *integrity* as well as securing *confidentiality* of user data in the communication channel between the TOE and the inspection system
  - Averting of inconspicuous tracing of the ePass
  - Self-protection of the TOE

ePassport: APE_SPD: Definition of Assets

Object No.	Primary asset (user data)	Definition incl. operations	Generic security property to be maintained
1	user data stored in the TOE	All data stored in the context of the ePassport application. This asset can be *read out* solely by inspection system	confidentiality integrity authenticity
2	user data transferred TOE <=> inspection system	All data being transferred in the context of the ePassport application between the TOE and an authenticated terminal. This asset can be *exchanged* by the TOE with inspection system	confidentiality integrity authenticity
3	ePass tracing data	Technical information about the current and previous locations of the ePass gathered by inconspicuous recognising the TOE. This asset can be *gathered* by a terminal	unavailability

ePassport: APE_SPD: Definition of Assets

Object No.	**Secondary** asset (TSF-data)	Definition	Generic security property to be maintained
4	Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way This asset can be *maintained* by the TOE	availability (in the sense of 'existence')
5	TOE secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality This asset can be *used* by the TOE	confidentiality integrity
6	TOE non-secret cryptographic material	Permanently or temporarily stored public cryptographic keys and other non-secret material (signatures) used by the TOE in order to enforce its security functionality This asset can be *used* by the TOE and *read out* by inspection system	integrity authenticity

ePassport: APE_SPD: Definition of Subjects

Ext. Entity No.	Subject No.	Role	Definition
1	1	ePass holder	A person for whom the ePass Issuer has personalised the ePass
2	-	ePass presenter	A person presenting the ePass to a terminal and claiming the identity of the ePass holder
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless interface (the default terminal role).
4	3	Inspection system	A terminal of an inspecting authority verifying the ePass presenter as the ePass holder by comparing the real biometrical data of the ePass presenter with the stored biometrical data of the ePass holder
13	-	attacker	A threat agent trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most *high* attack potential.

ePassport: APE_SPD: Derivation of Threats

- **T.Forgery**: Forgery of Data (⇨ integrity)
  - An attacker alters the user data or/and TSF-data stored in the TOE or/and transferred between the TOE and the inspection system, so that the inspection system perceives these modified data as authentic one.

- **T.Eavesdropping** on communication TOE ⇔ inspection system (⇨ confidentiality)
  - An attacker is listening to the communication between the TOE and the inspection system in order to gain the user data transferred between the TOE and the inspection system.

- **T.Skimming**: Capturing Card-Terminal Communication (⇨ authenticity)
  - An attacker imitates an inspection system in order to get access to the user data stored in or transferred between the TOE and the inspection system via the contactless interface of the TOE.

ePassport: APE_SPD: Derivation of Threats

- **T.Tracing**: Tracing ePass (⇨ unavailability)
  - An attacker tries to *gather* TOE tracing data (i.e. to trace the movement of the ePass) unambiguously identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE.
- **T.Physical_Tampering** (⇨ genuineness)
  - An attacker may physically modify the TOE in order to alter (i) its security functionality (hardware and software part, as well), (ii) the user data or the TSF-data stored in the TOE.

- **OSPs should**
  - mainly be derived from the external entities as defined above, and
  - reflect responsibilities concerning technical, organisational and legal infrastructures necessary for issuing and operating the TOE (e.g. issuing and verifying PKI branches)
- **Assumptions should**
  - be derived from the external entities as defined above, and
  - reflect the expected behaviour of human users necessary for issuing and operating the TOE

ePassport: APE_OBJ: Derivation of Security Objectives

- **OT.Data_Integrity**
  - For each asset, the TOE shall preserve its integrity according to Table 1 (user data) and Table 2 (TSF data)
- **OT.Data_Authenticity**
  - For each asset, the TOE shall preserve its authenticity according to Table 1 (user data) and Table 2 (TSF data)
- **OT.Data_Confidentiality**
  - For each asset, the TOE shall preserve its confidentiality according to Table 1 (user data) and Table 2 (TSF data)
- **OT.Tracing**
  - For ePass tracing data, the TOE shall preserve its unavailability according to Table 1 (user data)
- **OT.TOE_Genuineness**
  - The TOE shall ensure to be operational, only if its genuineness is available according to Table 2 (TSF data)

ePassport: APE_REQ: SFRs Alignment with Assets and Subjects

FDP_ACF.1/TRM	
FDP_ACF.1.1	The TSF shall enforce the Terminal Access Control SFP to objects based on the following: 1. Subjects: a. Terminal, b. Inspection system; 2. Objects: a. User Data stored in the TOE; 3. Security attributes: a. Authentication status of terminal
FDP_ACF.1.2	R.1: An inspection system is allowed to *read out* User Data stored in the TOE
FDP_ACF.1.4	R.2: Any terminal being not authenticated as inspection system is not allowed to access any User Data stored in the TOE

ePassport: APE_REQ: SFRs Alignment with Assets and Subjects

FTP_ITC.1/PACE	
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and **inspection system** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure
FTP_ITC.1.2	The TSF shall permit **the inspection system** to initiate communication via the trusted channel
FTP_ITC.1.3	The TSF shall **enforce** communication via the trusted channel for any user data transferred between the TOE and the inspection system

APE_REQ: Security Functional Groups

? Why voluntary clustering single SFRs?

- ! Because the usual alphabetic arrangement does not reflect a logical context of SFRs and a PP does not contain TSS
- ! For a consumer, it is very difficult to re-assemble the logical context of SFRs by analysing dependencies and other rationale parts

➢ Security Functional Groups (SFG) reflect SFRs in the context of the security services expected of the TOE

➢ SFG may be used by an ST author for orientation while developing TOE Summary Specification

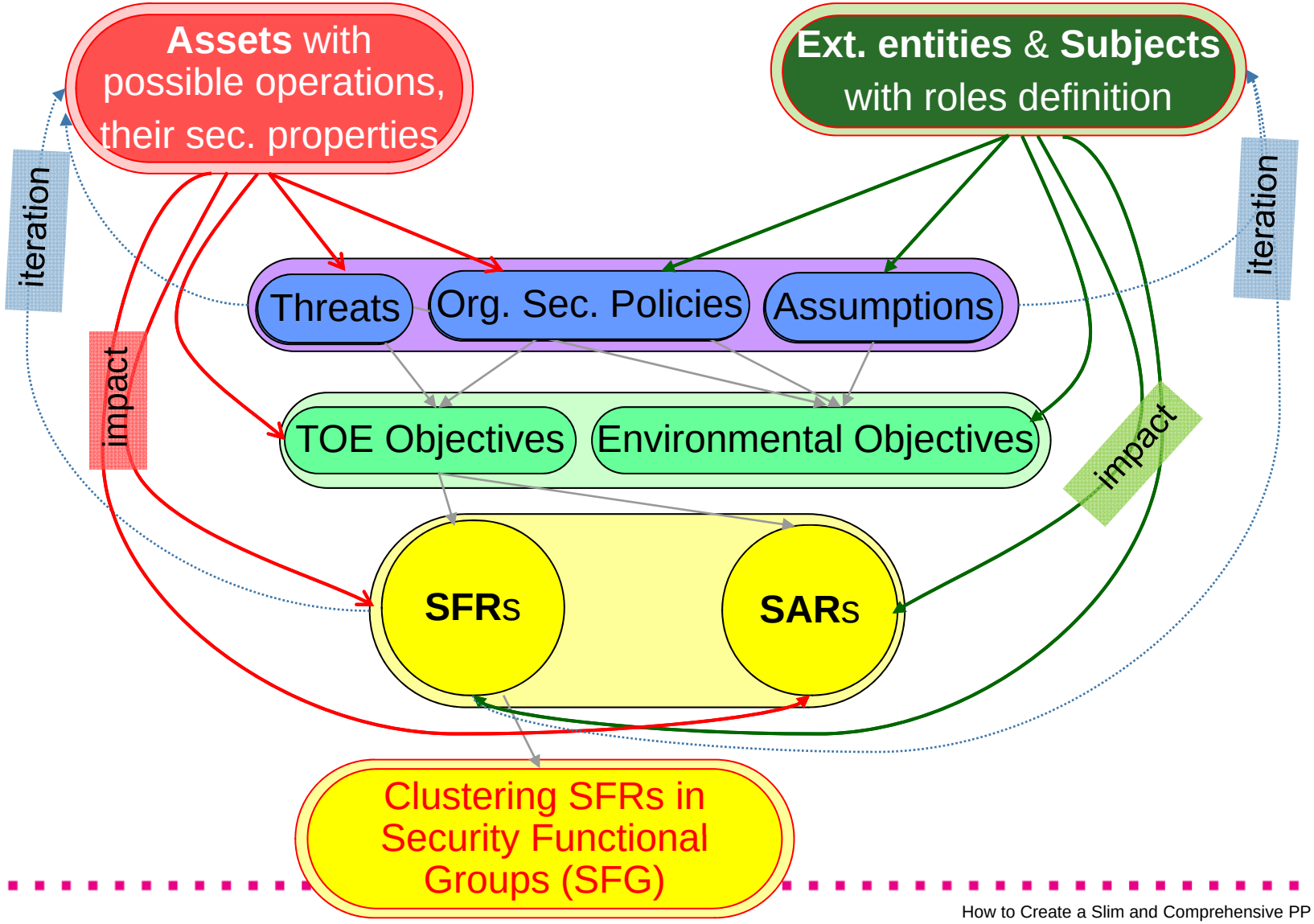
ePassport: APE_REQ: Security Functional Groups

- Security Functional Groups are aligned with the TOE logical scope defined in APE_INT above; but SFGs may be not limited to it

Security Functional Group	Security Functional Requirements
Access control to the User Data stored in the ePass	FDP_ACC.1/TRM, FDP_ACF.1/TRM: access control
Identification and authentication of users and components	FIA_UID.1/PACE, FIA_UAU.1/PACE: I&A of inspection system (as a prerequisite for AC)
Secure data exchange between the ePass and the inspection system	FTP_ITC.1/PACE: trusted channel
Averting of inconspicuous tracing of the ePass	FTP_ITC.1/PACE: trusted channel FIA_AFL.1/PACE: reaction to unsuccessful authentication attempts
Self-protection of the TOE	FPT_PHP.3: resistance to physical attack FPT_FLS.1: preservation of secure state

The ‘Frame Approach’: Stick to Ariadne’s Thread

☺ You are not frightened!



Advantages of the Frame Approach

- Benefits
  - A stable frame: Precise understanding of **what** is protected **at the very beginning** of a PP
  - Sticking to this frame throughout the PP
  - Slim (volume reduction of 20-25%) and technically sound PP due to ‘moving’ within the frame
  - **the set of SFRs becomes transparently and clearly aligned with the sets of assets and subjects** in the SPD-statement
  - Easy deriving TOE Summary Specification for ST
  - The PP becomes comprehensive, transparent and non-confusing for its readers. And even remains certifiable ☺
- As an universal, **TOE-type-independent** approach, this praxis significantly facilitates gaining these benefits

PP References Exploiting the Frame Approach

- A high **efficiency** of the frame approach has **successfully** been ‘tested’ for several certified PPs:
  - Machine Readable Travel Document using Standard Inspection Procedure with PACE(PACE PP), BSI-CC-PP-0068-V2-2011 (and ANSSI)
  - Digital Tachograph – Smart Card (Tachograph Card), BSI-CC-PP-0070-2011
  - Electronic Residence Permit Card (RP_Card PP), BSI-CC-PP-0069-2010,
  - Digital Tachograph - Vehicle Unit (VU PP), BSI-CC-PP-0057-2010,
  - Electronic Identity Card (ID_Card PP), BSI-CC-PP-0061-2009
  - Mobile Synchronisation Services (MSS PP), BSI-CC-PP-0048-2008

- The next PP is coming up for
  - EURO-MILS: Secure virtualisation for trustworthy applications in critical domains

Thank you for your attention!

Dr. Igor Furgel

T-Systems International GmbH
Security Analysis & Testing

Vorgebirgsstr. 49
53119 Bonn

+49 228 98415120
igor.furgel@t-systems.com