

EAB Research Project Conference

Security Evaluation of ABC Systems

Günter Schumacher, European Commission Joint Research Centre

An ABC System is...

- An automated door **system**?
- A security **concept** built upon an automated door?
- A traveller **service** built upon an automated door?



Relevant questions to ABC

- How much of the border control process is delegated to the machine?
- How are those elements protected?
- How is the relation between perceived uncritical with critical parts?
- . . .

In any case, an ABC system...

- is a security related system,
- needs careful design methodology, and
- requires assessment against security objectives

Different views to security

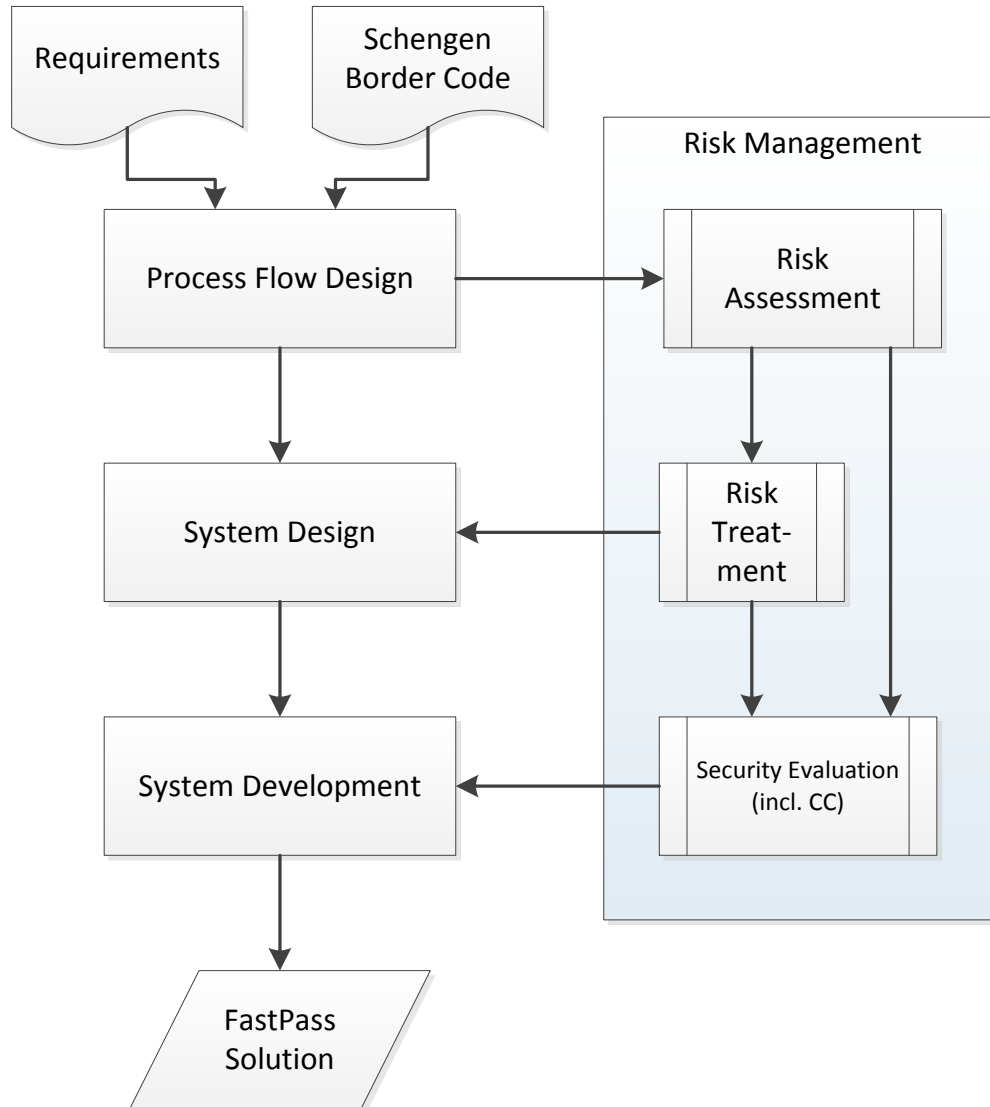
- product oriented
- development process oriented
- business process oriented

FastPass work on ABC security

- **Methodology**
 - ✓ Security Assessment Methodology
 - ✓ Privacy Impact Assessment Methodology
- **Evaluation**
 - ✓ Security assessment
 - ✓ Privacy Impact Assessment
- **Documentation**
 - ✓ Recommendations and Best Practice Report

Security Assessment Methodology

- Detailed consideration of **alternative approaches**
 - Common Criteria (ISO 15408)
 - Commercial Product Assurance (U.K. certification scheme)
 - ISO 27000 (Information Security Management)
 - Technische Richtlinie (German BSI)
- Synthesis of **model to be adopted**: *Security Risk Management according to ISO 27001/27005 plus optional CC conformant Protection Profiles for certain components*
- Exploiting Risk Analysis and Assessment as important FastPass **design tool**





Clear benefits:

- Evaluation not an “a-posteriori” activity but an interactive task with the development
- Shares concepts and considerations with privacy impact assessment

Data Protection Impact Assessment (DPIA)

Two complementary aspects to be addressed for a research project:

-  The personal data processing operations supporting the research (the way the research is conducted)
-  The development of new capabilities or technologies (the result of the research)

DPIA – Guiding Principles

- **(New) General Data Protection Regulation:**
 - Article 33
 - European Parliament first reading adopted last March

- **Adoption of concept developed for Smartgrids:**

The Expert Group 2 of the Smart Grid Task Force, chaired by JRC received a two years mandate on 1st February 2012 in order to develop a proposal for Privacy and Data Protection Impact Assessment template for Smart Grids (DPIA template).

The Adopted Process

- Step 1** - Pre-assessment and criteria determining the need to conduct (or not) a DPIA;
- Step 2** - Initiation;
- Step 3** - Identification, characterisation and description of the systems / applications processing personal data;
- Step 4** - Identification of relevant risks;
- Step 5** - Data protection risk assessment;
- Step 6** - Identification and Recommendation of controls and residual risks;
- Step 7** - Documentation and drafting of the DPIA Report;
- Step 8** - Reviewing and maintenance.

FastPass DPIA tool under development

Objective of the tool :

- It **supports the assessment** of the system
- Takes into account that DPIA is not a check list but a **documented process**
- Taking into account of the **controls already implemented** or planned

Work in progress

- Security evaluation:
 - Completion of risk management plan
 - Detailed discussion of list of vulnerabilities (currently some 80) in relation to design options
 - Internal and external review of relevant documentation
- Data protection impact assessment:
 - Elaboration of the adoption of DPIA developed for smart metering
 - Development of “DPIA tool” to facilitate individual steps

First documentation available by 1st half of 2015