



InspireD

D1: TPD Functional requirements - abstract

Table of Contents

1. INTRODUCTION	2
2. TPD REQUIREMENTS	2
2.1 BACKGROUND AND PROCESS	2
2.2 TPD PROFILES	3
2.3 CHOICE CRITERIA	4
3. CONCLUSIONS	4
4. GLOSSARY	4

1. Introduction

This document is an abstract of the deliverable **D1 “TPD Functional requirements”** realized within the InspireD project (IST-2002-507894).

“**InspireD**” is a European research project in the IST-FP6 Program “Towards a global dependability and security framework”. The acronym stands for “**I**ntegrated **s**ecure **p**latform for **i**nteractive **T**rusted **P**ersonal **D**evelopments”. The project vision is that the next generation of Smart Cards should be based on a new common platform approach for **Trusted Personal Devices (TPD)**.

TPDs aim to meet the strong demands for privacy, trust, and security among our digital identities in the increasing number of mobile devices and the emergence of a pervasive networking environment. Firstly, to establish trust, TPDs rely on security technology based on strong cryptography and supported by a dedicated hardware. Secondly, the TPD is meant to be a personal belonging, i.e., a TPD is under the control of a person in addition to a solely issuer-centric approach in current Smart Card applications. Thirdly, the TPD is to be employed as a device in the IT infrastructure, in particular it could act as a secure, portable Web server.

The TPD represents a major evolution of smart card technologies and is intended to enlarge the scope of the card and its value for both the card issuer and its end user. The set of requirements listed in this document address both generic requirements for the TPD platform as well as specific requirements driven from the 4 specific applications listed in the project’s Description of Work (DoW), which cover the following 4 domains:

- mobile phone
- data rights management and content protection for digital TV
- digital ID market
- on-line services

In order to address specific requirements of different possible types of TPDs and to avoid unneeded constraints to specific categories of TPDs, the concept of TPD Profiles is introduced to provide first level description of the different families of TPDs, and to allow the association of specific requirements to these specific families.

Each item of the requirements list is then applied to an explicit particular set of TPD profiles.

The set of requirements specified in this document cover 3 domains:

- 1) Functional requirements, which define functions of the TPDs that are considered required;
- 2) Interoperability requirements, which define how multi-vendor interoperability is handled;
- 3) Legal requirements, which refers to government or European regulations potentially applicable to the TPD.

The extensive tables of requirements, profiles and classes are not provided in this abstract.

More details on the InspireD project can be found in the Web at www.inspiredproject.com

2. TPD requirements

2.1 Background and process

TPD requirements are based on the results of the RESET programme and on the experience of the smart card manufacturers. They have concluded that the smart card business needed a major overhaul of its technology foundations in order to take advantage of increased silicon resources, and overcome limitations related to:

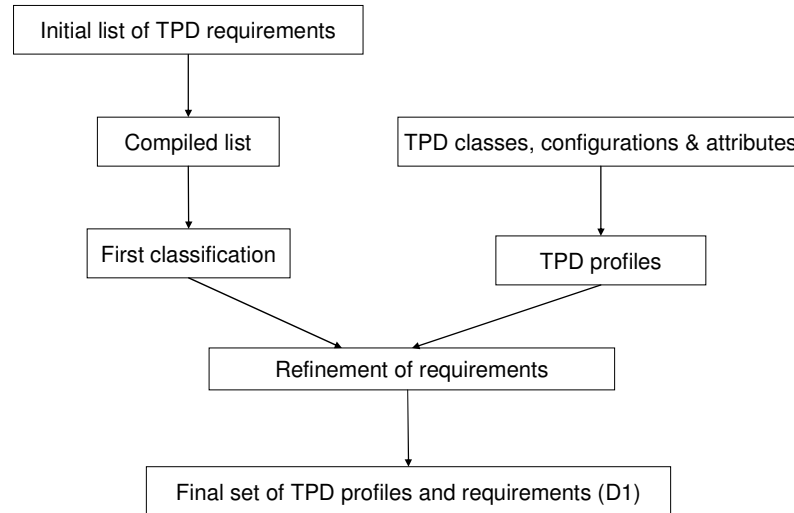
- Interfaces,
- the execution environment,

- the application models.

The InspireD project will deliver a set of technologies applicable to a range of products, with finished product deployment in the 2007 – 2010 time window.

Most TPD requirements apply to platform services, regardless of the application. TPD requirements are based on a consensus of smart card manufacturers or vision.

The process for the collection of requirements was as follows:



Process for collection of requirements

Figure 1

2.2 TPD profiles

The TPD profiles have been classified by:

- classes,
- sub classes,
- and configuration items

The classes correspond to two ways of using the TPD: the resident or static class and the itinerant or mobile class. The static TPD needs to be inserted in a host device most of the time for regular use, while mobile devices are inserted on host devices from time to time only, for a user triggered operation, for example.

Static TPDs include the following sub-classes:

- SIM
- MSC (Mass Storage Card)
- TPM (Trusted Personal Module)

Mobile TPDs include the following sub-classes:

- Token (with non-ISO7816 form factor)
- Smart Card

Then the profiles are further classified under configuration choices, which contain specific attributes, under specified configuration items.

Configuration items include:

- Components: which include either single (mC) microcontroller or multiple components like silicon (cpu, memory) and peripherals
- Host interface: which can be contact and contact-less
- User interface: this can be either autonomous or host-based whether the TPD relies on a host or not for the provision of user interface resources.

- Power supply: which can be on-board or off-board

Then the attributes are the different possibilities applying to a particular configuration item, such as different kinds of components, standards for an interface, etc.

2.3 Choice criteria

The following elements were used as choice criteria in order to be able to focus on a representative list of requirements:

- Platform flexibility for applications
- Smooth integration into IT system
- Trust and security
- Mobility enhancement
- Interoperability
- Privacy enhancement
- Performance
- Application-specific requirements

Requirements have been grouped in the following three categories:

- **Functional requirements** of the TPD as a platform
- **Interoperability requirements**, which translate onto whether or not agreement and publicity on specifications of some interfaces exist or if the system remains proprietary
- **Legal requirements**, which refer to compliance with expected legislation or other kind of regulations with potential impact on the proposed technical solutions;

3. Conclusions

Requirements for the TPD have been defined in this document to address both generic requirements for the TPD platform as well as specific requirements driven for 4 specific application domains. As some requirements are very specific to particular applications, they will be handled by special interest groups within the project

TPD Profiles were introduced which are now used as reference for the rest of the developments within the InspireD project.

The TPD requirements in this document result from a long process of formal requirements gathering among partners with a consensus objective. As part of the project, and in order to drive the architecture definition, the consortium will complete the list of TPD features, using the defined requirements, feedback from designers, and a will to focus on the most innovative and useful features.

The requirements list is very wide in scope. The objective was to take the time of a technical analysis before deciding whether one particular requirement should be dropped. The list should be considered as a wish list rather than absolute requirements, and the base for specific technical investigation and feasibility/cost analysis. Some requirements may be dropped after technical analysis, and the key innovative feature set will be defined to address innovative aspects of the platform architecture. Technical work will focus on the features addressing the requirements considered the most important.

4. Glossary

Combi:

Refers to the combination of a contact and a contact-less interface. Applies to chips (combi-chip) or cards (combi-cards).

Host, Host device:

The Host, or Host Device is a device that directly communicates with the TPD, without intermediate device. This definition implies that a device communicating remotely across a network with the TPD is not a host device to the TPD. The TPD host device holds the low layer interface to the TPD, and at least the physical layer. In addition, in many cases, the host device provides the power supply and the user interface resources to the TPD. Certain types of TPD may communicate with several hosts, alternatively or at the same time.

SVP:

Secure Video Processing. SVP is a video content protection platform defined by the SVP forum. See <http://www.svp-cp.org> for more details.

TCG:

TCG, the Trusted Computing Group is a set of companies cooperating to define specifications for the definition of trusted computing platforms. The Trusted Computing Platform is typically a PC, PDA or phone with download capabilities, where a trusted computing module (TPM) is added on the main board to provide security functions in association with the main (un-trusted) CPU. The TPM was initially defined by for the PC an older forum, the Trusted Computing Platform Association. The TCG has taken the responsibilities and extended the scope and membership of TCPA, which is no longer active. See www.trustedcomputing.org for more details.