Concept for Trusted Personal Devices in a Mobile and Networked Environment

Frank C. Bormann, Laurent Manteau, Andreas Linke, Jean C. Pailles, Jan van Dijk

Abstract—**In this article we present a concept for Trusted Personal Devices, which are intended to be the common platform for the next generation of Smart Cards and other secure devices in mobile and networked environments. The concept is based on a classification of technical profiles for different potential TPD form factors and applications. Requirements coming from various application areas are considered. A number of use cases have been defined to show innovative features of the TPD. Highlights are the support of Internet connectivity and Web server functionality in a secure and reliable way. In addition, trust establishment and privacy issues are especially considered in the design.**

Index Terms—**Smart Card, SIM, Web server, Security, Trust, Privacy**

I. Introduction

InspireD is a European research project in the IST-FP6 Program "Towards a global dependability and security framework". The acronym stands for "**In**tegrated **s**ecure **p**latform for **i**nteractive T**r**usted **P**ersonal **D**evices". 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**) [1].

TPDs aim to meet the strong demands for privacy, trust, and security among people'sdigital identities in an 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 within existing IT infrastructures, in particular it could act as a secure, portable Web server.

The results presented in this article are based on market and technology watch activities and the ongoing validation of the results from the technical specifications for TPDs. Moreover, experts for social, ethical & privacy issues of new technologies have been consulted.

We present the following results of the TPD concept [2]:

- A **Classification** of TPD profiles, usage functions & privacy issues (Section II),
- an overview of **Application Areas** for TPDs (Section III),
- an overview of **Use Cases** for TPDs (Section IV), and
- technological **Innovations** brought by TPDs (Section V).

II. Classification & Usage of TPDs

Within the RESET project [3], a research roadmap for Smart Card-related technologies has been defined. Based on this roadmap, four potential form factors for **Trusted Personal Devices** can be distinguished: **Smart Card, SIM-Card**, **Mass storage card**, and **USB token**.

Whereas the first two form factors are characterized by an onboard microprocessor and security features, the latter two are well known for their mass storage capability and convenient connectivity to host devices. A main goal is to combine the beneficial properties of the different form factors in one platform for Trusted Personal Devices [2].

InspireD performed a requirement analysis to define the characteristic properties for the different TPD profiles. The results are shown in Figure 1. A cross "X" stands for a characteristic property, whereas an "O" indicates an option.

One can see that for each TPD profile high-density storage is required. ISO 7816 is the standard interface for current Smart Card form factors, but this should be extended by optional interfaces, such as USB, MMC (Multi Media Card), or NFC (Near Field Communication, ISO 14443). The two TPD profiles "System on Smart Card" and "System on Token" have the option for a power supply and an autonomous user interface on board.

To summarize, from an end user perspective, we can define the TPD as follows:

A TPD is a small device belonging to a single person to enable trusted operations with other entities in an Information Technology & Communication infrastructure."

Manuscript received February 7, 2006. This work was supported in part by the European Commission under contract No. 507894

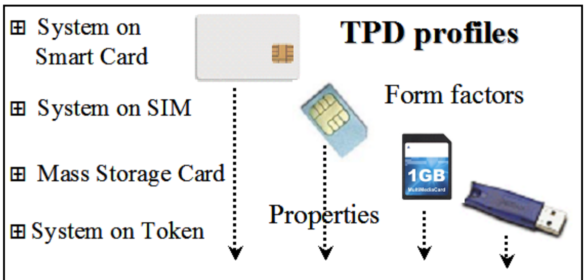
F. C. Bormann is with ORGA Systems enabling services GmbH, 33104 Paderborn, Germany, phone +49 5251 889 3221; fax: +49 5251 889 3239; e-mail: fbormann@orga-systems.com.

L. Manteau is with Gemplus SA, 13705 La Ciotat Cedex, France, e-mail: Laurent.Manteau@gemplus.com

A.Linke is with Giesecke & Devrient GmbH, 81677 Munich, Germany; e-mail: Andreas.Linke@de.gi-de.com

J.C. Pailles is with France Telecom R&D, 14000 Caen, France, e-mail: jeanclaude.pailles@francetelecom.com

Jan van Dijk is professor of communication science at the University of Twente, The Netherlands, e-mail: Jan.vanDijk@utwente.nl



Components	SC	SIM	MSC	Token
High density memory	X	X	X	X
Co-processor	O	O	O	O
Biometric Sensor			O	O
Display	O			O
Knobs	O			O
Host Interfaces				
ISO 7816	X	X		
USB	O	O	O	X
MMC			X	
ISO 14443 / NFC	O	O		O
User Interfaces				
Host-based	X	X	X	X
Autonomous	O			O
Power Supply				
Off-board	X	X	X	X
Onboard	O			O

Figure 1: TPD Profiles, Form Factors, and Properties

Besides the form factors and the characteristic properties, TPDs can be distinguished to bear different **usage functions**:

- ***Access***: access to specific areas (or countries), buildings, means of transport, services, institutional resources and entitlements (such as voting);
- ***Payment***: financial transactions on the move with banks or other financial institutions and with retailers;
- ***Commerce:*** transactions of goods, services, discounts, and special offers for preferred customers on the move;
- ***Mobile information and communication***: exchange and retrieval of information and messages on the move, which are usually received, processed and stored in fixed, more or less private and secured places (home, work, school).

Regarding the first three functions (***access***, ***payment***, and ***commerce***) the main power, initiative, responsibility and determination of usage conditions should be with the host, which is in general the TPD issuer. The TPD user is a guest to the space, service, property, etc. of the host. A guest has to be identified or authenticated to get access, make transactions, and the like. The fourth usage function, however (***mobile information and communication***) should remain within the personal space, power, initiative, responsibility and determination of the TPD user. This is the reign of a fast growing ubiquitous, mobile personal domain. The virtual "alter ego" of the mobile user of information and communication technology is carried from private or fixed spaces (home, work) into mobile more or less public spaces (currently present in laptops, PDAs, multimedia mobile phones and others). The initiative to get access from this personal domain to external resources, contacts and information comes from the user. Here the external provider is not a host but a guest that is invited to this mobile personal domain on the conditions of the user knowing what the legitimate requests of the guest are. Thus, for the fourth usage function (***mobile information and communication***) the TPD should be a truly trusted personal device. TPDs with the other three functions should of course also be trusted by users – but in another way or at another level, because they are "less personal", as they cannot work at all without an external technological and organizational access and provisioning system.

TPDs offering one or more of the four different usage functions require different things to be protected by legal and technical means. Liabilities, responsibilities, security and even privacy enhancing technologies (PETs) will acquire different shapes [4]. For the ***access*** function, authentication or identification of the user is crucial. Reconciling privacy preserving authentication methods with a PKI and (partly) blind digital signatures can be proposed here [5]. In the ***payment*** and ***commerce*** area**,** transactions should be strongly protected on the initiative and main responsibility of the supplier. With ***mobile information and communication*** TPDs, contents should be protected on the initiative and responsibility of the user first of all. However, access to resources protected by institutions (employers) and content providers (intellectual property rights) comes on their initiative and responsibility. PETs (other than signatures) and regulatory protections of privacy are far more complicated in the last three functions than in the first function (***access***).

TPDs can be either specialized, i.e., offer only one or two specific usage functions, or multi-functional, i.e., combine even more of the four different usage functions. The choice of the functionality provided by a TPD is the most important strategic choice in the design of TPDs. It has far-reaching consequences in terms of security, privacy, personal autonomy, responsibility and regulation. The more of these four functions are integrated in a single TPD, the more its applicability and partly its convenience increases (less TPDs to carry, but more weight and complexity). However, simultaneously its security, privacy, autonomy of use, individual responsibility and simplicity of regulation decreases. This is because the risks, complexity, and necessity of informed consent by a multitude of parties grow in multifunctional TPDs.

III. Application Areas

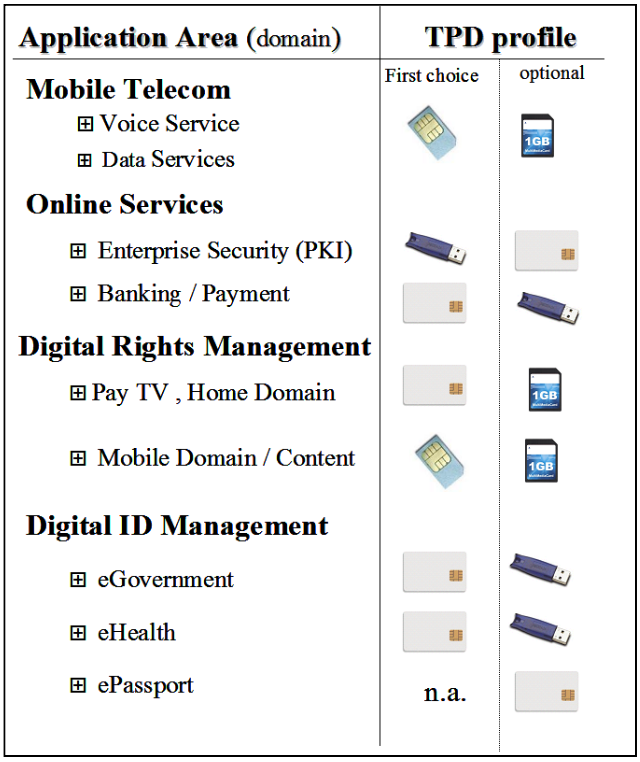
The classification of TPD application areas is based on the current market segmentation for Smart Cards.

Mobile Telecommunication is currently by far the biggest market segment for Smart Cards. According to Eurosmart [6], over 1 billion SIM cards were shipped worldwide in 2004. Besides the standard USIM application for mainly voice-oriented services, there are more and more data service applications on hold to be deployed. It is assumed that the role of SIM as a business enabler for the network operator will be sustained and enhanced by new features. The use of Mass Storage Cards is an option for special businesses dealing with huge amounts of personal data on a TPD.

Online Services are gathering the market segments banking (280 million Smart Card units in 2004) and enterprise security (12 million units in 2004). Online Services are covering all kinds of transmission of data in fixed networks. In the Enterprise Security domain (PKI), the TPD profile “System on Token” will play a major role, whereas in banking applications, it will be more likely the Smart Card profile.

In the application area **Digital Rights Management**, we can distinguish between the home and the mobile domain. In 2004, 55 million Smart Cards were issued for Pay-TV applications in the home domain. It is expected that with the evolution of wireless networks there will be a strong growth in the mobile domain. Besides TV content, other digital content like games, music, or sensitive documents will require protection in the future in both domains. All TPD profiles are relevant in this context. In the Pay-TV domain, the Smart Card profile is dominant, whereas in the mobile domain, the SIM is more likely to be applied.

The application area of **Digital ID Management** is covering the market segments eGovernment and eHealth with a total shipment of 45 million units in 2004. This application area is related to online services, but is in general on a large scale (e.g., as a nationwide ID) and requires biometrics and physical access control mechanisms at certain places. In **Digital ID Management**, the dominating TPD profile is the System on Smart Card. Especially in eHealth applications with a need to store a high volume of data, alternatives like tokens are currently discussed.



Application Area (domain)	**TPD profile**	
	First choice	optional
Mobile Telecom		
⊞ Voice Service ⊞ Data Services		
Online Services		
⊞ Enterprise Security (PKI)		
⊞ Banking / Payment		
Digital Rights Management		
⊞ Pay TV , Home Domain		
⊞ Mobile Domain / Content		
Digital ID Management		
⊞ eGovernment		
⊞ eHealth		
⊞ ePassport	n.a.	

Figure 2: Relation of TPD profiles and Application Areas

A mapping of the identified TPD profiles to the application areas is shown in Figure 2. The TPD profile column is separated into two sub-columns: in the first sub-column, the form factor considered as the most important candidate for the corresponding application area is shown. In the second sub-column, optional TPD form factors are shown.

For each application area, the anticipated future use of TPDs has been extensively discussed. Typical use cases have been formulated to focus on innovative features of the TPD and to guide the technical specifications. These use cases and innovative features are described in the remainder of this article.

IV. USE CASES

The range of typical TPD use cases has been discussed with user panels, gathering 25 members of different industries deploying Smart Cards and related devices. In a refinement process, a focus was put on the question what kind of information is being protected by the TPD. Basically, the user panels came to the conclusion that digital identities, digital usage rights, and other sensitive personal information the user does not want to disclose without need are ideally protected with a TPD.

An overview of all identified TPD use cases is shown in Figure 3 on the next page. The use cases in bold have been selected to be of major importance for the TPD concept definition and are further explained below.

A. Authentication Gateway – Single Sign On (SSO)

The use case **Authentication Gateway – Single Sign On (SSO)** applies the TPD as a trusted “man in the middle”. After an enrolment phase in a secure environment, the TPD can use the credentials to access different online services with the informed consent of the user. Besides the digital identifiers, privacy policies should be stored and managed on the TPD. From a business perspective, the TPD takes over the role of an identity provider for the user. In addition to the approach of the Liberty Alliance [7] for federated ID management, the requirement to store identity-related information in a central location has to be validated for the TPD itself by bearing a Web server functionality. The following issues have been raised in the discussion with the user panel and will be considered in the ongoing specification and implementation work:

- How to provide a backup function for credentials in case the TPD gets stolen or lost?
- Who issues the TPD? There is an underlying concept of an “open source” TPD, which the user can buy on his own initiative. But even in this case a priori a TPD must be trusted at least by one user and one certification party.
- How can the issuer be changed during the lifecycle of the TPD?

B. *Anonymous Service Access - Direct Anonymous Attestation (DAA)*

The use case **Anonymous Service Access – Direct Anonymous Attestation (DAA)** is focusing on privacy issues when accessing online services. The assumed situation is that the user wants to access high value content on a Web server for a certain period (e.g., for one month), without being tracked or identified for each usage session during this period. In this case, credentials exchanged via TLS/SSL cannot be used, because they can disclose the user identity via the given certificate.

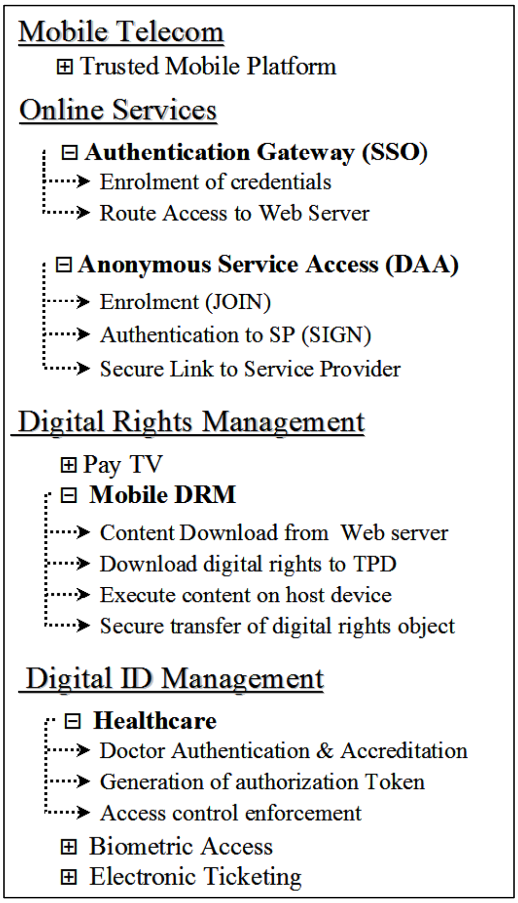

Mobile Telecom
⊞ Trusted Mobile Platform
Online Services
⊟ Authentication Gateway (SSO)
Enrolment of credentials
Route Access to Web Server
⊟ Anonymous Service Access (DAA)
Enrolment (JOIN)
Authentication to SP (SIGN)
Secure Link to Service Provider
Digital Rights Management
⊞ Pay TV
⊟ Mobile DRM
Content Download from Web server
Download digital rights to TPD
Execute content on host device
Secure transfer of digital rights object
Digital ID Management
⊟ Healthcare
Doctor Authentication & Accreditation
Generation of authorization Token
Access control enforcement
⊞ Biometric Access
⊞ Electronic Ticketing

Figure 3: Use Cases per Application Area

A proposed approach here is to apply a dedicated anonymous attestation functionality: After a JOIN function during the enrolment, a separate key will be generated for each session with a SIGN function provided by the TPD. This generated key cannot be used to identify the user in the session; it only states that the user is valid (i.e., "joined the process before").

One has to differentiate between the anonymity of the procedure provided by the cryptographic functions of the TPD (JOIN, SIGN) and the anonymity of the channel. A problem with the latter could occur if there is a collusion between the network operator and the service provider, e.g., if the network operator sends user-related identity information to the service provider based on the knowledge of the network IP address of that user. However, such issues are usually highly regulated. To achieve channel anonymity, different approaches can be used, e.g., purchasing prepaid handsets without the need to provide personal data.

The functions JOIN and SIGN are defined in detail by the Trusted Computing Group [8]. The InspireD consortium is proposing a lightweight implementation of these functions in the TPD based on partial blind signatures.

Other applications, in which these functions can be used, are electronic bidding and voting, where in the latter case also the control of the unicity of the vote is necessary.

In the user panel, the following two further issues have been discussed:

1. The InspireD approach is different to other privacy preserving services (such as the Liberty Alliance), because the service providers are not a priori trusted. Thus, the user only provides the necessary information, e.g., payment for a JOIN process.
2. For all payment-related processes, money-laundering laws have to be preserved, in particular when providing an anonymous service for payments. This is not only valid for high value transactions, but also when small amounts are paid in high volumes very fast. Thus, as a consequence, the SIGN function cannot be used along with a payment process.

C. *Digital Rights Management – Mobile Domain*

The use case **Digital Rights Management – Mobile Domain** is about protecting multimedia content and restricting its usage with digital rights. An extension to OMA DRM 2.0 is proposed to securely store and manage digital rights directly on a TPD [9] [10]. This function provides a number of convenient usage options for the user:

(a) It is possible to plug the TPD into different host devices for content usage on different platforms.
(b) It is possible to set up a connection to a networked remote TPD for content usage on a local end device.
(c) It is possible to actually transfer digital rights from one TPD to another ("fair use"), where the target TPD may belong to another user as well as another issuer.

D. *Healthcare – Digital ID Management*

The use case **Healthcare – Digital ID Management** is dealing with storing and retrieving medical data on a TPD with the local enforcement of an appropriate access control policy. A Web service architecture is proposed for the TPD to make it accessible for the doctors, healthcare organisations, and the user.

V. Innovations

From the description of the use cases, it is obvious that different innovative TPD features are required when looking for an interoperable solution.

The key innovation for the TPD is that it will be integrated in the information and communication infrastructure as a **networking element.** The basis for this is the use of standard

Internet protocols like TCP/IP when communicating with the TPD. Above that, HTTP or secure HTTPS will be used to exchange information, and a Web service architecture can be built on top of this. XML processing and Web service protocols like SOAP are key functions treated in the TPD application framework, which is currently being specified.

An innovation closely related to the networking is the use of standard **communication interfaces** on the physical layer in addition to ISO 7816, like USB. The vision is that no dedicated hardware or software is needed on a host device to communicate with the TPD. The user experience should be that people just connect the TPD to the preferred host device and open a standard browser to interact with it.

In some use cases (e.g., eHealth), **mass storage** with more that 1MB up to several GB of memory capacity with personal information is required to be stored in the TPD onboard. Therefore, new storage technologies like flash memory should be accessible by the TPD on board.

The support of (contactless) **near field communication** and **biometric** TPD holder verification are additional innovations shown in dedicated use cases.

A special **privacy** innovation will be brought in with cryptographic functions on the TPD, enabling direct anonymous attestation (DAA) for anonymous access to dedicated online services.

VI. Conclusion & Outlook

From the use cases, a detailed list of innovative TPD features on each design level (hardware, software, and API) is derived for proof-of-concept implementations. The impact of the technological features has been discussed in a dissemination event with over 50 attendees from research organizations, different industries, and public services.

The finalization of the **common platform** specifications for TPDs is envisioned for the second half of 2006. To summarize, a TPD from a technical point of view can be seen as follows:

A TPD is a secure, portable, personal Web server
with optional near field communication
and support of biometric authentication.

As a next step, the proof-of-concept implementations of the innovative TPD features are prepared and demonstrated to show the feasibility of the specifications within the InspireD project in 2006 [1]. It is planned to validate the results in a second public user panel and to continue the discussion on the impact of the new technology in another dissemination event.

References

[1] IST-2002-507894, “InspireD: Integrated secure platform for Trusted Personal Devices”, http://www.inspiredproject.com

[2] InspireD, “TPD concept defintion”, Deliverable D5.1, IST-2002-507894-InspireD, December 2005. to be published on http://www.inspiredproject.com

[3] RESET, “Roadmap for European research on smartcard related technologies”, Deliverable D5, IST-2001-39046-RESET., May 2003, http://www.ercim.org/reset/Resetfinal.pdf

[4] Stephen T. Kent, Lynette I. Millet, “Who goes there? Authentication through the lens of privacy”, http://www7.nationalacademies.org/cstb/pub_authentication.html

[5] IST-2002-507591, “PRIME: Privacy and Identity Management for Europe”, Description of Work, http://www.prime-project.eu.org/

[6] Eurosmart, “The Voice of the Smart Card Industry”, http://www.eurosmart.com/

[7] Liberty Alliance Project, http://www.projectliberty.org/

[8] Trusted Computing Group, https://www.trustedcomputinggroup.org/home

[9] Frank C. Bormann, Stephan Flake, Jürgen Tacken, Carsten Zoth, “Towards the Integration of Trusted Personal Devices into Mobile DRM Systems”, submitted for the IST Mobile & Wireless Communication Summit 2006, Myconos, Greece

[10] Open Mobile Alliance, http://www.openmobilealliance.org/