



# InspireD

---

## D8: Security requirements for TPD (abstract)

# Table of Contents

---

<b>1. INTRODUCTION</b> .....	<b>2</b>
<b>2. SECURITY REQUIREMENTS</b> .....	<b>2</b>
2.1 HARDWARE SECURITY.....	3
2.1.1 <i>Security requirements analysis</i> .....	3
2.1.2 <i>Side Channel attacks</i> .....	6
2.1.3 <i>Hardware to software security</i> .....	7
2.1.4 <i>Counter-measures</i> .....	7
2.1.5 <i>Conclusion</i> .....	7
2.2 SOFTWARE SECURITY .....	8
2.2.1 <i>Security Requirements analysis</i> .....	8
2.2.2 <i>Enhanced User Authentication and Trust existing possibilities</i> .....	8
2.2.3 <i>Links with other groups</i> .....	9
<b>3. CONCLUSIONS</b> .....	<b>9</b>

## 1. Introduction

---

The aim of this document is to present an overview on the work done on the “Security requirements for the TPD”. This includes the contribution of the work packages WP1.2 and WP2.5. It also takes into account the exchange of information that occurs between the different groups around security definition and more recently privacy that are integrated in the D8 document.

This document is an abstract of the D8 document which has been realised in the **frame of the EC-funded initiative untitled “Inspired”** (IST-2002-507894). This document is not at all a substitute of the D8. It sums up and puts the emphasis on the main activities done during the past time. In the conclusion, the document describes the different actions that have to be completed before the end of the project.

## 2. Security Requirements

---

The D8 deliverable covers the security aspects related to the TPD; security is a transversal topic that drives all smartcards development and obviously future TPD development as well. Based on this fact, all InspireD partners are concerned and aware of the importance of such deliverable.

The D8 document addresses security-related topics, browsing from hardware-level features to architectural security issues. In its current draft version, it does not cover all raised aspects, and does not propose final solutions yet.

However, several critical aspects are already studied, and early choices and results are reported.

The current version of the D8 has first analyses the early generic requirements and profiles definitions, trying to see the impact they will have in the definition of the TPD security, some early conclusions have been made. Then, a focus has been done on specific topics through collecting and analyzing existing practices in the field of TPD security.

Indeed, it is commonly admitted that security cannot be absolute; neither can it be de-correlated from its applicative field.

In the next phases of the security analysis, a focus will be put and studies will be conducted to see the feasibility of the implementation of some of those requirements in the context of the specific use cases and application areas, taking into account the privacy related issues. These phases will take into account the refinement of the TPD profiles that has been done in parallel by other work group.

A description of the main activities and results is exposed in the following chapters. We have decided to follow the current structure of the D8 document through a first chapter on hardware security and a second chapter on software security. Those chapters will expose the thought processes used.

Due to the size of the corresponding document, a split in two parts had been decided for the last year. That means that this abstract will be related in its next release to the documents D8.1 and D8.2.

## 2.1 Hardware security

### 2.1.1 Security requirements analysis

In the early phase of the project InspireD, a list of functional TPD requirements was gathered and mapped to a number of typical TPD profiles to be investigated.

Given the requirement list, the first task of work package 1.2 was to identify those requirements, which are related to hardware security.

The following requirements were identified as being related to hardware security:

N#	Functional requirements
105	The TPD should ensure third parties (i.e. neither the TPD issuer nor the user) that the TPD is trustworthy, while protecting user privacy by providing: strong user authentication and identification services (e.g. PIN, biometrics...), pseudonymity or anonymity of the user, trusted attestation
107	The TPD should offer an execution environment suitable for applications that exploit secrets, without leaking information. The level of security will be defined during technical studies.
110	The TPD should be suitable for association with trusted computing platforms
112	The TPD should include features for recovery of TPD data, or their migration to another TPD, where they do not compromise the security of either device
125	The TPD should allow a complete contactless transaction time to be consistent with the "swipe mode" typical of transport fare payment. The "less than 150ms" target will be studied, for mutual asymmetric authentication. It may require external power source.
131	The TPD should be able to process content cryptographically at high speed
135	The TPD should be able to output in real-time decrypted content from an encrypted content input, on the host interface, this applying to multimedia content for consumption
136	The TPD should be able to store consumption multimedia content and keep it protected from free access
141	The TPD shall be designed to prevent physical attacks

**Figure 1 – Global requirements related to HW security**

In a second step, the general description was refined to a list of items describing in detail the requirements for security. The following table depicts these detailed requirements as well as their relevance for the different TPD profiles.

#	Description	X-Ref to WP02	M3 : System on Token		M4 : Combi SoT		M8 : System on Card		S3 : System on SIM		S4 : Contact MSC	
			HW	SW	HW	SW	HW	SW	HW	SW	HW	SW
<b>Protection against invasive attacks</b>												
1	The TPD should have protection mechanisms against identification/localisation of critical blocs & shielding	136, 141	1	0	1	0	1	0	1	0	1	0
2	The TPD should have shields protecting against EM emanation (active shields)	107, 141	1	0	1	0	1	0	0	0	0	0
3	The TPD should have protection against Probing / Forcing	107, 136, 141	1	0	1	0	1	0	1	0	1	0
4	The TPD should have protection against optical inspection	107, 136, 141	1	0	1	0	1	0	1	0	1	0
5	The TPD should have protection against Laser Cutter Attack	107, 136, 141	1	0	1	0	1	0	1	0	1	0
6	The TPD should have protection against Emission Microscopy	107, 136, 141	1	0	1	0	1	0	0	0	0	0
7	The TPD should have protection against Etching		1	0	1	0	1	0	1	0	1	0
<b>Protections against non-invasive attacks</b>												
8	The TPD should remove attacker's ability to synchronise with any internal event	107	1	1	1	1	1	1	1	1	1	1
9	The TPD should have Protection against timing analysis	107	1	1	1	1	1	1	1	1	1	1
10	The TPD should provide countermeasures against Simple Power Analysis.	107	1	0	1	0	1	0	1	0	1	0
11	The TPD should provide countermeasures against Differential Power Analysis.	107	1	0	1	0	1	0	1	1	1	1
12	The TPD should provide countermeasures against Simple Electromagnetic Analysis.	107	1	0	1	0	1	0	1	1	1	1
13	The TPD should provide countermeasures against Differential Electromagnetic Analysis.	107	1	0	1	0	1	0	1	1	1	1
14	The TPD should provide countermeasures against accoustic cryptanalysis.	107	0	0	0	0	0	0	0	0	0	0
15	The TPD should facilitate countermeasures against hybrid attacks [i.e. combination of side-channel information and cryptanalytic analysis]		1	1	1	1	1	1	1	1	1	1
<b>Protection against semi-invasive attacks</b>												
16	The TPD should have protection against faults through the IOs	107, 141	1	0	1	0	1	0	1	0	1	0
17	The TPD should have resistance against Spike and Glitch Attacks	107, 141	1	1	1	1	1	1	1	1	1	1
18	The TPD should have resistance against Optical/Light Attacks	107, 141	1	1	1	1	1	1	1	1	1	1
19	The TPD should have resistance against Alpha-Radiation Attacks	107, 141	1	1	1	1	1	1	0	0	0	0
20	The TPD should have resistance against Temperature Variation Attacks	107, 141	1	1	1	1	1	1	1	1	1	1
21	The TPD should have resistance against Power Supply Attacks	107, 141	1	1	1	1	1	1	1	1	1	1
22	The TPD should have resistance against Clock Variation Attacks	107, 141	1	1	1	1	1	1	1	1	1	1
23	The TPD should have resistance against Electromagnetic Induction	107, 141	1	1	1	1	1	1	1	1	1	1
24	The TPD should have resistance against UV Radiation Attack		1	1	1	1	1	1	1	1	1	1

#	Description	X-Ref to WP02	M3 : System on Token		M4 : Combi SoT		M8 : System on Card		S3 : System on SIM		S4 : Contact MSC	
			HW	SW	HW	SW	HW	SW	HW	SW	HW	SW
<b>Cryptographic Algorithms &amp; Performances</b>												
25	The TPD should perform consistency tests for internally generated public and private keys.	105	0	1	0	1	0	1	0	1	0	1
26	The TPD must use publicly known approved cryptographic algorithms. This is a recommendation which should not inhibit the use of proprietary algorithms whenever required.	125	1	1	1	1	1	1	1	1	1	1
27	The TPD should have a cryptoprocessor for up to 2048 RSA with key generation	110, 125	1	0	1	0	1	0	1	1	1	1
28	The TPD should have a cryptoprocessor for up to 2048 RSA with encryption/decryption	110, 125	1	0	1	0	1	0	1	1	1	1
29	The TPD should have a cryptoprocessor for up to 2048 RSA with digital signature	110, 125	1	0	1	0	1	0	1	1	1	1
30	The TPD should have a cryptoprocessor for up to 256-bit ECC encryption/decryption/signature		1	0	1	0	1	0	0	0	1	1
31	The TPD should have a cryptoprocessor for Vernam One Time Pad	110, 125							0	0	0	0
32	The TPD should have a cryptoprocessor for SHA1	110, 125	0	1	0	1	0	1	0	1	0	1
33	The TPD should have a cryptoprocessor for 3DES	125, 135	1	0	1	0	1	0	1	1	1	1
34	The TPD should have a cryptoprocessor for AES	125, 135	1	0	1	0	1	0	1	1	1	1
35	The TPD should have a true random number generator		1	0	1	0	1	0	1	0	1	0
36	The TPD should have a pseudorandom number generator		0	1	0	1	0	1	0	1	0	1
37	A standardised choice of random number tests, approved in the context of formal evaluation/certification, should exist and be supported by the TPD		1	1	1	1	1	1	1	1	1	1
38	The TPD should offer the possibility to generate a public key pair [in particular for RSA and ECC] without ever releasing the private key part [i.e. keep the private key confidential at all times].		1	1	1	1	1	1	1	1	1	1
39	The TPD should provide a hardware accelerator to facilitate the implementation of random number tests		0	0	0	0	0	0	0	0	0	0
<b>Secure Management</b>												
40	The hardware should have mechanisms that allow the operating system to restrict the access to secret data and keys.	105	1	1	1	1	1	1	1	1	1	1
41	The TPD should provide the possibility of testing the quality of the random numbers generated at any time		1	1	1	1	1	1	1	1	0	0
42	Lifecycle Management (Testmode / Usermode / End of Life)		1	0	1	0	1	0	1	0	1	0
43	The TPD should have counter-measures against tearing attacks		0	1	0	1	0	1	0	1	0	1
<b>Biometric Authentication Mechanisms</b>												
44	Communication between the TPD and the fingerprint sensor shall be secured and ensure data integrity and confidentiality.	115, 112	0	1	0	1			0	0	1	1
45	Biometric authentication should always be performed either on the biometric sub-device, or on the TPD. In that case the TPD shall perform match on card verification. The biometric template shall be securely (data integrity and confidentiality) transferred	115	0	1	0	1			0	0	1	1

Figure 2 – Security requirements mapped to profiles

For the first draft of the document focus was put on the different possible kind of physical attacks and their impact thus counter-measures were proposed.

As it's these threats and the way to prevent from them is the main security focus regarding hardware we wrote a chapter for each of them.

## 2.1.2 Side Channel attacks

This chapter will describe the state of the art on side-channel attacks. This gives a first overview of the public state-of-the-art, while introducing the reader to this specific domain in smartcard and TPD security.

The idea of hardware "cryptanalysis" or side channel attack came up concretely around 1998 with Paul Kocher. Their basic observation is that, at some point, such transformations have to be implemented as a program that will run on some specific devices (a processor chosen for the application or some tailored piece of hardware). This might allow recovering the secret parameter involved in the computation thanks to the specific features of the device. Such attacks are much less general than classical cryptanalysis (since it involves characteristic of the implementation), but often prove to be much more powerful. As such, side channel attacks should be seriously taken into account.

We give a classification of these attacks according to the way they handle the device under attack.

The literature has taken the habit to classify side channel along two orthogonal axes according to the handling of the device by the attacker:

- Invasive / semi-invasive/ non-invasive
- Active / passive attacks.

**Invasive attacks:** *Provide the attacker with access to the components of the chip. This requires depackaging the chip in order to observe, manipulate or interfere with the inside of the system. The hardware is definitively damage.*

**Non-invasive attacks:** *Use information available from the outside of the chip, without the need to open it.*

**Semi-invasive attacks:** *These attacks require de-packaging the chip but do not require electrical contact with the metal surface of the chip.*

**Active attacks:** *try to tamper with the correct behaviour of the device, for example by inducing fault during the computation.*

**Passive attacks:** *in this scheme, the attacker will observe the device while it is properly functioning without disturbing it.*

Afterwards, different sections present the known side channel attacks, for each of them the way to perform them (the protocol) and a sample is given. Namely you will find:

- Timing attacks
- Power analysis (SPA, DPA, HO Power attacks...)
- Electromagnetic Analysis (SEMA, DEMA)
- Acoustic crypto-analysis
- Fault attacks
- Cache attacks
- Attacks against fingerprint sensors

### 2.1.3 Hardware to software security

Security is a global approach; especially in the context of small tamper-resistant devices like TPD, security has to be tackled at each stage of its development and at each level of its architecture.

The previous section shows how complex the physical or so-called invasive, semi-invasive or non-invasive attacks are. Beyond the understanding of techniques used in such attacks, some generic counter-measures will be proposed later. If physical counter-measures -which are implemented in hardware with sensors, shields, etc...- are a first answer to the problem, they cannot obviously answer to all attacks or threats. This is due to the fact that such techniques have limitations, as well as to the nature of attacks themselves.

Combination of hardware and software counter-measures is straightforward at this stage; many software techniques have been already introduced in the previous section, and will be addressed and described here in a dedicated manner.

Here it will be question of low level software techniques which are usually hardware dependent, although their base concepts can be generalized; better than listing exhaustively such techniques, the goal is really to understand the concepts behind.

Some attacks or classes of attacks will serve as examples and will be referred to.

Management of sensitive data processing will be depicted.

The aim is to insure: consistency, integrity, confidentiality...

### 2.1.4 Counter-measures

In this section, after generic existing countermeasures will be explained, then we will go through the attacks defined previously and propose some countermeasures for each.

Both hardware and software counter-measures (with their efficiency) will be given in order to prevent the previous listed attacks (the same plan is kept).

As well we decided to add a measurement bench because an important element to ensure tamper resistance and test the efficiency of implemented countermeasures is the systematic analysis and evaluation of measurements.

To this end, a measurement bench is needed, whose set-up and software enables an automated and reproducible execution of attacks by measuring power consumption and/or electromagnetic radiation.

For these measurements, several items are necessary, for instance measuring probes for electromagnetic radiation, a high-precision adjustment bench, and equipment for shielding, etc.

### 2.1.5 Conclusion

The D8 document being split between hardware security requirements and software ones was the first step. Enlarging this work will lead to our concern the D8.1 document.

While keeping improving the mentioned contributions (reverse engineering, focus on fault attacks...) the following of that will be the study of new hardware design to avoid those attacks or at least reduce their efficiency. As well cryptographic algorithms and implementation of them will be developed so as to be resistant against side-channel attacks.

Biometry new hardware definition will be the core of a new chapter.

Then focus will be put on vulnerability risks analysis for new identified TPD features and the conclusion of that work will be a kind of Security Guideline.

## 2.2 Software security

For such device, software security is very important to give confidence in the use of the TPD in the different use cases exposed in the document D5.1. It is crucial for a portable device that will be in charge of the security of personal and sensitive data to be able to protect its contents but also to exchange data in a secure way, with the prior knowledge of its holder.

In this context, a specific emphasis was put on enhanced user authentication mechanisms, on trusted platform components, the later being closely linked to the TCG initiative (Trusted Computing Group) which aims at defining specifications for trust establishment in several environments (PC, handsets, etc).

Privacy is not treated as a separate point but appears at different levels in the whole document. It was a deliberate choice, according to the main target of the InspireD project. It is to develop a Trusted Platform Device that integrates security and which aim is to secure holder's personal and sensitive data from any threats: direct attack on the protocols to get secret information or tentative to track the holder. In this context, privacy is one of the centric point to address through all the recommendations. That's why it appears directly or indirectly in the different topics mentioned in this document such as anonymous protocol, relations between TPD and TPM, secure channels,....

### 2.2.1 Security Requirements analysis

The first approach consists in looking at the 164 requirements early defined for the TPD and to see what the impacts on the security are, what are the main points to focus on.

As a matter of fact, privacy and authentication issues are, as already mentioned, first points to address. The approach consists in a reminder of the properties around those two items, before going more in deep in the privacy enhancements for authentication protocols. An example of the importance of such topics and the duality of the holder is illustrated through the authentication of a person by his passport at the border: on one hand the user wants to be granted full access to certain resources and on the other hand he wants his privacy to be protected, possibly to remain completely anonymous. That's why the information he reveals in the course of the authentication must not be read by unauthorised entities and it must be made sure that the data is not abused for purposes not required by the process.

### 2.2.2 Enhanced User Authentication and Trust existing possibilities

After the previous topics around privacy and authentication, we then focus on the way to establish a secure link between the two entities involved in the communication (to be extended), or the way to perform alternative authentication such as biometry techniques for example.

A particular attention was also paid to techniques or recommendations that support those techniques, as for example legal signature functions, contactless. One more time, privacy is present here, with the particular point on contactless, through the recommendation of use of sure algorithm for signature. It will also be completed by recommendations to establish a secure channel, the issue of the key establishment that come with.

It allows to directly pointing out a specific item when speaking about secure channel: Trust. How could you establish a trusted relation with another entity?

That's why this document makes a particular point on the complementarities between a TPD (portable device in charge of the security of the personal and sensitive data) and the TPM (a fixed machine that could be trusted). An illustration done on the SIM use case came to get more in depth in this scheme. It also a possibility to emphasis the role and the importance played by a TPD/SIM when used with a mobile trusted platform.

In correlation with these properties of trust, it clearly appears that to get confidence in a TPD, it is important to get confidence in its all life cycle. By saying that one means that it is a point to develop secure channel with a trusted entities, to define anonymous protocols to perform authentication, but it is another to guarantee the security of the data stored inside the TPD during its all life: from its personalisation until its end of life. As it rapidly appears through discussion that a unique model of life cycle management won't answer the requirements of all the use cases, the solution was to present the different possibilities that could be used depending on the context.

### 2.2.3 Links with other groups

As mentioned the WP1.2 and 2.5 are transversal groups dedicated to security. But security is something that should be intimately mixed with the specification, the design and the coding done for a device. That's why a special care was brought to the participation to the other part of the project documentation. A wide part of this job of advices is directly indicated in the corresponding documents (on the communication, on the operating system as for example), a few part of them are related in this document, more as a track of the job done.

## 3. Conclusions

---

This document is rich in security aspects and technologies; it already browses some of the main subjects that are currently being tackled by the industry.

Besides, special care will be brought on the user authentication issue as well as on the trusted platform components issue, both having privacy-related aspects.

In parallel, improved coordination and synchronisation is achieved with other software groups in the InspireD project, so that at any stage of their own work security conclusions, advice, guidance or specifications will be available for them to integrate.

During the last year of the project a special care will be given to the feasibility of the recommendations done in this document or directly in the design documents. This will be achieved through our participations in different demonstrators.