FIDIS

Future of Identity in the Information Society

Title:	"D3.18: Demonstration of a new approach for preserving identity and privacy in mobile transactions using Id-token with Trusted Computing"
Author:	WP3
Editors:	Rani Husseiki, Konstantinos Kolelis (Sirrix AG), Lorenz Mueller (Axsionics)
Reviewers:	Harald Zwingelberg (ICPP)
Identifier:	D3.18
Type:	[Deliverable]
Version:	1.1
Date:	Tuesday, 30 June 2009
Status:	[Final]
Class:	[Public]
File:	fidis-wp3-del3.18_Demonstration_v1.1.doc

Summary

This deliverable considers a possible approach to give the ability for a user to verify that the computing devices she is using are trustworthy (i.e., in a reliable and secure configuration, free of malware, spyware, etc.) in order to preserve her digital identity in mobile transactions on different computing devices.

Through this deliverable, Sirrix and Axsionics give a demonstration of joint solution for this problem. On a high level, our idea is to allow a user to verify the trustworthiness of a platform using an Axsionics personal identity management assistant (Internet Passport, a credit card sized id-token that manages cryptographic keys and identities). Therefore, she will hold her Id-token to the screen of the PC to be verified. The Id-token then – using its unique optical interface - verifies the trustworthiness of the PC. For this purpose, so-called attestation protocols are conceived and prototyped. Those are carried out between the user's PC and a verification server. This is achieved bye means of trusted computing technologies integrated in the user's PC.

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
1.0	10.06.2009	• Initial Release (Rani Husseiki)
1.1	18.06.09	• Integration of review comments

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Introduction)	Rani Husseiki
2 (Motivation)	Rani Husseiki
3 (Demonstrator)	Rani Husseiki
4 (Conclusion)	Rani Husseiki

Table of Contents

1 Executive Summary

This deliverable presents a joint solution for identification with trusted systems that has been developed by Sirrix and Axsionics in the context of FIDIS work package 3. The solution addresses an essential requirement for secure transactions using mobile devices: reliable identification on a trustworthy system.

The joint solution has been conceived and implemented based on technologies developed by both partners.

TURAYA™, a high assurance security kernel architecture developed by Sirrix, allows virtualizating the hardware of a proprietary user's device. This enables multiple operating systems to run concurrently on the same hardware in isolated virtual environments. Trusted Computing technologies integrated in the device allow monitoring the integrity of the software stack running on the device, and therefore its trustworthiness. Integrity measurements can be sent to a central server for verification against trustworthy values.

On the other hand, the AXSionics authentication system, composed of an Internet Passport (id-token), an Integration Link (a flickering code showed on the screen) and a Security Management server (authentication server) enables a reliable identification and authentication of a user to a certain service. However, it assumes the trustworthiness of the user's device, which is not always a valid assumption.

Through their joint solution, Sirrix and Axsionics developed a system that combines the security properties provided by their corresponding technologies implementing a demonstrator that is based on four main components. These interact among each other to provide identification and authorization of a certain user to access a service based on his possession of a token as well as the trustworthiness of his PC's configuration. The components are: an id-token (Internet Passport), a local secure station (the user's PC), a Trusted Computing based verification server (TC verification server), and an Axsionics security management server (Axsionics server).

A set of trust-rules are established in the overall architecture of the demonstrator. These rules prove that a user is able to get access to a certain service and make transactions if and only if he is the true owner of the Internet Passport token, the token is an authentic one which is registered at the Axsionics server, and his device configuration is verified for its trustworthiness by the verification server.

The demonstrator has been successfully built and presented at the FIDIS event at IFIPSec2009.

2 Introduction

In the mobile digital society users will pursue their online activities using different computing devices - some of them are owned and controlled by the user while others are not. For example, a user will check her email and do voice communication on her family PC, use a shared PC at work to check her (business and private) mail and write documents, use an Internet terminal in a hotel to digitally sign a contract she has received by e-mail, communicate peer to peer using her PDA in an ad-hoc networking scenario etc.

In this scenario, insecure computing devices seriously jeopardize a user's privacy and identity. For instance, a device controlled by an attacker can collect the data (documents, e-mails, internet telephony conversations etc.) produced by the user; also, it can impersonate a user by stealing her credentials or by acting on behalf of her in a malicious way while, e.g., she performs bank transactions or signs a digital contract. The need for protection from identity theft and privacy breaches during critical mobile transactions on non-proprietary devices is therefore self-evident.

Sirrix and Axsionics decided to address this problem by conceiving a joint solution, which was then implemented in the scope of a demonstrator. The solution presents a modern approach for solving the problem by giving the ability for a user to verify that the computing device she is using is trustworthy (i.e. has a reliable and secure configuration, free of malware, spyware, etc…). This guarantees the preservation of the user's digital identity, and the security of the user's transaction on this computing device. Both the user and the service provider would be able to establish trust in the user's platform with regard to its capability to ensure authenticity of the user and security of the transaction.

In fact, Sirrix has developed a trusted computing scheme that allows verifying the trust status of a local computer that is connected to a Trusted Computing (TC) verification service. For a user that intends to use the local computer however it is impossible to verify the trust status of the computer in question without the possibility to get the verification status report from the TC verification service over a secure channel. The display of the local machine which shall be verified can not serve for this purpose because, if corrupted, the attacker may also fake the verification message.

To solve this problem, Sirrix and Axsionics conceived a joint solution. On a high level, the idea is to allow a user to verify the trustworthiness of the platform she is using, and to guarantee that her identity is safe from impersonation. A user would possess a unique and private Axsionics "Internet Passport" (a credit card sized computing device that manages cryptographic keys and identities). The computing device includes the TURAYA^{TM} Security Kernel developed by Sirrix, which integrates Trusted Computing (TC) technologies. A verification server is able to verify the trustworthiness of the device by means of attestation protocols which are based on TC technologies. A series of communication protocols performed between the PIMA, the computing device (PC), the verification server and the Axsionics server will prove the trustworthiness of the PC to the PIMA owner, and will prove the identity of the PIMA owner to verification server.

This deliverable presents the motivation behind the demonstrator, as well as the concept, technical specifications, usage scenario and effectiveness of the solution. The concept has been modelled and implemented as a demonstrator based on a combination of technologies provided by both Sirrix and Axsionics. The demonstrator has been successfully presented during the FIDIS event at the IFIPSec 2009 security conference.

3 Motivation

3.1 Security Requirements in E-commerce Scenarios

We start by conceiving a motivation scenario that led Sirrix and Axsionics to work on the joint solution, and which is at the basis of evaluation of the proposed architecture. The solution considers, as explained below, a trustworthy identification of the user to a trustworthy computing device he is using to perform a security-critical transaction.

In a typical e-commerce scenario, mutual verification of identities between the service provider and the user is crucial. This is achieved by means of authentication protocols, which allow verifying that:

- Service Provider A (e.g. Bank) is really talking to **Mr.** Smith and not **Mrs.** Smith

AND

- that Mr. Smith is really talking to Service Provider A (e.g. Bank)

The aim of this mutual authentication process is to guarantee that neither of the two parties is subject to impersonation, i.e. an attacker is assuming his identity in order to fraudulently act on behalf of the real identity holder.

Another crucial security requirement in a typical e-commerce scenario is the verification of a willful act when a transaction is requested. This is usually achieved by means of an authorization process that allows verifying that:

- It is really the willful act of Mr. Smith to transfer x$ from his account to account xyz of Mrs. Johns in Bank B and to confirm it

or e.g.

- It is really the willful act of Mr. Smith to change conditions of his online contract

or e.g.

- It is really the willful act of Mr. Smith to open, download or print specific information…

The aim of this authorization process is to guarantee that the person claiming the identity of the transaction requester – which has already been authenticated – is truly and willingly requesting this particular transaction, and is not subject to, e.g., man-in-the-middle attacks.

3.2 Available Technologies

The solution conceived and implemented by Sirrix and Axsionics is based on technologies developed by both partners whose combination helped achieve an overall solution that addresses the security requirements mentioned in the previous section. In the following, we give an overview of the technologies provided by both partners.

3.2.1 TURAYA™

The TURAYA™ High Assurance Security Kernel (HASK) [Tura09] developed by Sirrix, which leverages virtualization and Trusted Computing technologies, constitutes a crucial part of the solution. The HASK installed on a computing device allows running several operating systems concurrently on top of it, and in separate virtual environments (compartments), which all share the same hardware components. The HASK integrates security services that ensure mandatory security control on the compartments, and guarantee enforcement of security policies. The isolation of these environments is a key security aspect of TURAYA™. It allows, e.g. running an online banking application in a separate compartment whose configuration[4] can be verified by the HASK security services against trustworthy values. Trusted Computing technology is also supported by the HASK in order to allow measurements[5], persistent storage, and remote attestation[6] [Remo05] of compartment configurations to other devices or entities, e.g. a verification server. This is achieved by means of a Trusted Platform Module (TPM), which is a secure hardware chip integrated in the computing device of the user, and whose specification is defined by the Trusted Computing Group (TCG).

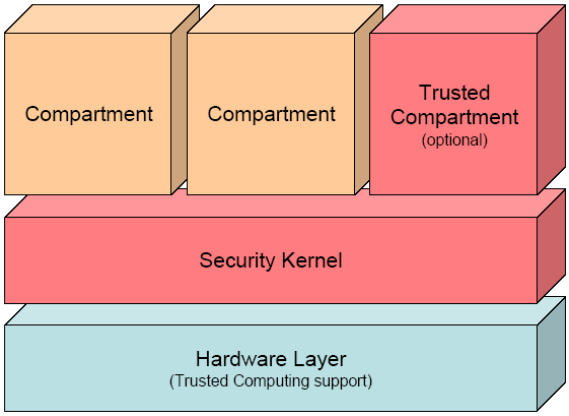

Fig. 1: Security Architecture of the user's computing device

The TURAYA™ solution also features a "Trusted Object Manager" (TOM) which is responsible for remotely configuring devices equipped with TURAYA™ HASK. This server handles compartments and their security configurations. A user with a device equipped with TURAYA ™ system will be able to download these security critical compartments to his device from the TOM. Therefore, a secure banking-software-compartment (which is basically a minimal operating system with only online-banking software installed on it) can be downloaded to the device, leaving the option for the user to install other legacy OSes and applications within other compartments.

---

[4] *The term configuration follows the terminology of the Trusted Computing Group and means the integrity state of a platform or software component, e.g., taken during an integrity measurement and being represented as hash value of a program binary.*

[5] *Cryptographic SHA-1 based hash values of binaries.*

[6] *Attestation protocols allow a platform to provide evidence of its integrity, and therefore its trustworthiness with respect to well defined policies, to remote parties*

This aspect of the TURAYA ™ solution, though essential to the overall concept, is however not included in the demonstrator. Nevertheless, the TURAYA™ solution provides the following relevant and crucial components for the joint solution:

- **Remote Attestation Service:** one of the HASK security services which are relevant and crucial for the joint solution. This service allows the HASK to generate a cryptogram including *fingerprints* of the measurements of a certain compartment, which are values saved in so-called Platform Configuration Registers (PCR) of the TPM. This cryptogram can then be sent to another entity for verification.
- **Verification Server**: a server that handles trustworthy PCR values (i.e. PCR values reflecting measurements of trustworthy configurations of compartments). This server can check an attestation cryptogram obtained from a certain device, and verify the included PCR values against a list of trustworthy PCR values registered at the server. If a matching occurs, the server can confirm the trustworthiness of the corresponding compartment.

3.2.2 AXSionics Authentication System

On the other hand, the AXSionics identification solution [Axsi09] presents the other crucial part of the overall solution. It consists of:

A personal identity management assistant (PIMA) which is a credit card sized computing device that manages cryptographic keys and identities.

- **AXSionics Internet Passport™**: a personal identification device of a credit card size with Display, Fingerprint reader and optical interface.
- **AXSionics Integration Link:** an optical communication channel which is based on a flickering image generated by the screen of the computing device and intercepted by the Internet Passport to produce the secret message.
- **AXSionics Security Manager:** server software which encrypts the messages and manages the credentials of the users.

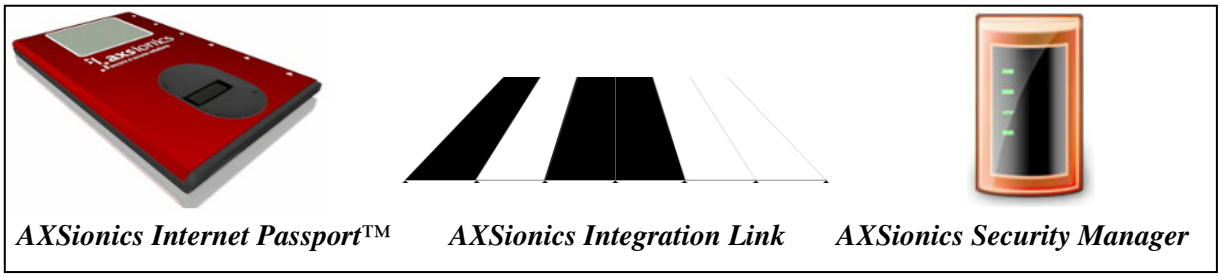

Fig.2: Components of the AXSionics Authentication System Solution

The AXSionics authentication solution features the following:

Trusted display: Submitted transaction details are encrypted – decryption on the token display only after successful owner's authentication

Communication Channel: is under full control of the 2 communicating parties (no 3rd party involved).

This provides the following security guarantees with respect to a transaction:

- Authenticity: transaction details can only be sent from an authenticated sender
- Integrity/Privacy/Secrecy: transaction details are sent encrypted (no plain text over the web from a trusted sender)
- Freshness: transaction details can not be replayed

3.3 Technical Requirements

3.3.1 Hardware requirements

Generally, a hardware security anchor that is able to store and communicate encrypted integrity measurements should exist at least on the user's device in order for a verification server to establish remote trust in the device. A TPM, such as the one supported by TURAYA™, would be a suitable component. TPMs are nowadays included in business notebooks as well as many desktop computers. Hence, schemes based on this technology are legitimately considered as feasible and deployable on mainstream devices.

On the other hand, id-token such as the ones proposed by Axsionics are also indispensable. Since these hardware components present unique features, they seem necessary as a function component supporting the overall concept of our solution.

Authentication and Verification servers do not need any specific hardware components, although TPM support by these servers might be beneficial if they are required to prove the trustworthiness of their configurations e.g. to user devices. However, this is not a considered requirement in our scenario.

3.3.2 Software requirements

In order to integrate the above-described technologies in a comprehensive solution, several software components need to be available.

In particular, a security kernel is necessary to allow several virtual machines – proprietary as well as security-critical – to run on mainstream user devices.

An integrity measurement architecture including software components that allow performing sequential measurements of loaded software. Specifically, a protected pre-BIOS called the Core Root of Trust for Measurement (CRTM), and a support software called TCG Software Stack (TSS) which performs various functions like communicating with the rest of the platform or with other platforms, need to be included.

Moreover, security services supporting "remote attestation" and "verification" should be included on the device side and server side respectively.

4 Demonstrator

The demonstrator that Sirrix and Axsionics implemented presents a joint solution stemming from a combination of the technologies explained above. The solution has been conceived so as to address the security requirements for preserving the identity of a user as well as the authenticity and security of a transaction he is willing to perform from his personal device.

4.1 General Concept

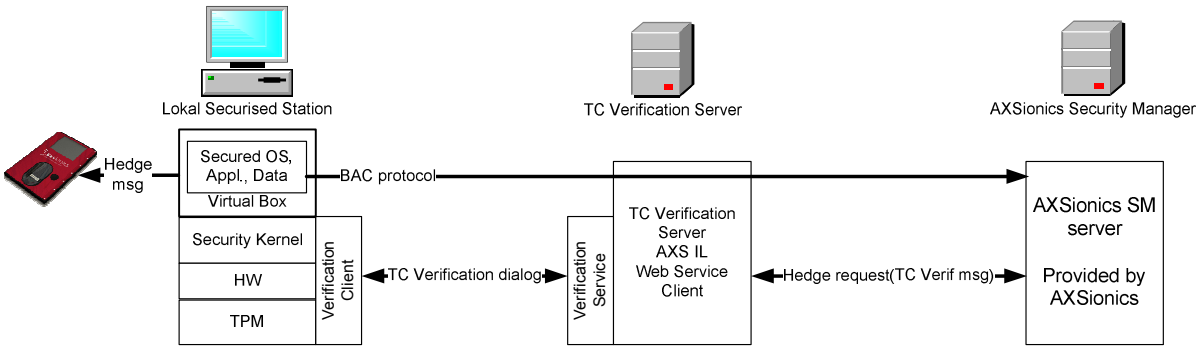

Fig.3: General Architecture of the joint solution

The architecture depicted above includes four entities which we describe as follows:

1. **The Internet-Passport (IP)**: private card for a user, with a unique serial number.
2. **The Local Secure Station:** computing device (PC) of the user, on which the TURAYA™ HASK is installed, including a "Remote Attestation Service" (Verification Client). One compartment including the secured OS and online-banking application runs on top of the HASK. A TPM chip is also available on the PC.
3. **TC Verification Server:** A server that handles the verification of compartment configurations obtained from a Remote Attestation Service (Verification Service).
4. **AXSionics Security Manager:** A security management server handling authentication credentials of users who possess an Internet Passport, and can be installed by any enterprise.

4.1.1 General Workflow

The general workflow of the solution includes the following steps:

1) TPM checks the status of the local machine and delivers the encrypted status vector to the TC Verification Server via a "TC Verification dialog".
2) The TC Verification Server request a hedge message from the AXS Security Manager Server (Verification ticket), which includes the result of the verification server (success/failure) as well as a fresh password for authentication to the online-banking

service. The Verification Server sends back the obtained hedge to the local machine in form of a flickering code.

3) The user reads the flickering code on his PC screen with his AXS Internet Passport and receives the true verification ticket which includes the trust status of his local machine, and the authentication password. She uses the password for authenticating herself on the authentication page on his screen.

4.1.2 Trust Model

The following trust model applies to the process described above:

1. The TPM is trusted to generate a verification vector that truly reflects the configurations of the compartment in which the online-banking application is running. Therefore, if the Verification Server verifies this vector through the Remote Attestation Service, the result of this verification is guaranteed to reflect the trustworthiness of the user's PC.
2. The information included in the hedge message (i.e. the success/failure of the attestation, and the authentication PIN on success) is coded into a flickering code:
    a. That is only readable by this specific Internet Passport.
    b. Whose decoded information is only shown on the Internet Passport display after the owner has authenticated herself to her token using her fingerprints for authentication.
3. The flickering code includes a PIN only if the verification performed by the server is successful, i.e. the user's device is trustworthy. This PIN is the only means for authentication to the online-banking service.

These rules prove that a user is able to get access to a certain service and make transactions if and only if he is the true owner of the Internet Passport token, the token is an authentic one which is registered at the Axsionics server, and his device configuration is verified for its trustworthiness by the Verification Server.

4.2 How the solution works

This section explains the technical details of the solution, including the communication protocol between the four entities of the architecture, and the processes that are carried out due to the user actions.

User starts the local machine (his PC)

- TURAYA™ HASK starts the remote attestation process by invoking the TPM to generate a verification cryptogram which is sent to the TC Verification Service via the Remote Attestation service.

- An https secure connection is established between the local machine and TC Verification Service Web server.
- A web browser is opened with an entry mask for the Internet Passport number PPN (a unique serial number printed on the Internet Passport card, and which is registered at the AXSionics server).

User enters the PPN of his card in the entry mask

- TC Verification Service checks if the received PPN corresponds to an authentic Internet Passport that is registered at the AXSionics server. This is done by verifying that a Basic Access Control (BAC) channel is available for this particular Internet Passport at the server.
- TC Verification Service checks the verification cryptogram retrieved from the user's PC via the Remote Attestation service against trustworthy values. If a matching occurs, the verification result is "success" otherwise "failure". In both cases, the Verification Server generates a "hedge request message" containing the result, as well as the PPN of the Internet Passport that started the challenge. This message is sent to the AXSionics SM server via a Web Service call.
- The AXSionics SM generates the BAC message which includes the result of the Remote Attestation process (i.e. "success or failure"), and if it is a success, a BAC Response code (PIN to be used by the user for authentication to the service). This generation algorithm of this BAC message guarantees that it can only be read by the Internet Passport corresponding to the PPN that has been received in the "hedge request message". The BAC message is sent back to the TC Verification Web client.
- The Flickering Code generator in the TC Verification Web server transforms the BAC message string in a flickering code and sends it to the user's PC to be displayed on his screen.

User reads flickering code with his Internet Passport

Internet Passport receives the BAC message over the secure channel allocated to the TC Verification Service; it then requests the user to authenticate herself with a combination of up to three fingerprints.

User authenticates herself at the Internet Passport (Finger Authentication)

Internet Passport authenticates user and shows then the verification message ("success/failure") and if it a success, the BAC response code in addition.

User enters BAC-response code in the authentication browser

- The TC Verification Service receives the response and forwards it by a second Web Service call to the AXSionics SM server.
- The AXSionics SM server verifies the user response and gives the authentication status back to the TC Verification Service.

- The TC Verification Service may allow the user the access to the local machine (this step is an option to restrict access, but it is not mandatory).

The figure below shows the protocol messages exchanged between the user and the different entities of the solution architecture.

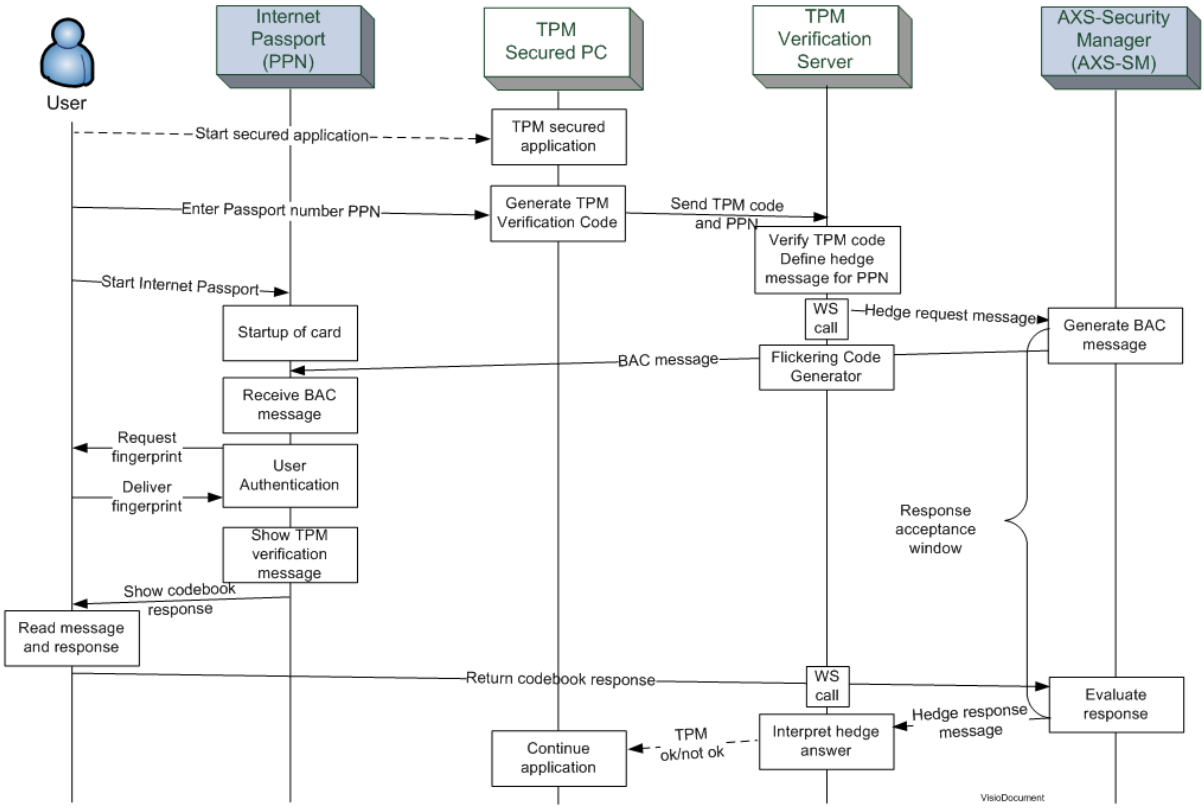

Fig.4: protocol messages between the entities of the architecture

5 Conclusion

The joint solution by Sirrix and Axsionics has been conceived and implemented in order to combine identification techniques with trusted systems. This is an essential requirement for achieving trustworthy schemes for performing transactions using private computing devices, such as a home PC. The solution is based on technologies developed by both partners. This helped us implement a demonstrator showing the effectiveness of our solution.

The demonstrator is based on four main components which interact among each other to provide identification and authorization of a certain user to access a service based on his possession of a token as well as the trustworthiness of his PC's configuration. The components are: an id-token (Internet Passport), a Local Secure station (the user's PC), a Trusted Computing based verification server (TC verification server), and an Axsionics security management server (Axsionics server).

A set of trust-rules are assumed in the overall architecture of the demonstrator. These rules prove that a user is able to get access to a certain service and make transactions if and only if she is the true owner of the Internet Passport token, the token is an authentic one which is registered at the Axsionics server, and her device configuration is verified for its trustworthiness by the Verification Server.

The demonstrator has been successfully built and presented at the FIDIS event at IFIPSec2009.

6 Bibliography

[Tura09] Turaya Security Kernel, Sirrix AG,http://www.sirrix.de/media/downloads/54926.pdf

[Axsi09] The Internet Passport - new biometric platform for end-point authentication and transaction security, Axsionics, http://www.axsionics.ch/ tce/frame/main/410.htm

[Remo05] Remote Attestation and Peer-to-Peer Networks, Ville Likitalo, http://www.tml.tkk.fi/Publications/C/18/likitalo.pdf