Title:	"D3.14: Model implementation for a user controlled biometric authentication"
Author:	WP3
Editors:	Lorenz Müller (AXSionics), Els Kindt (KU Leuven)
Reviewers:	Harald Zwingelberg (ICPP), Marit Hansen (ICPP)
Identifier:	D3.14
Type:	Deliverable
Version:	1.0
Date:	Thursday, 06 August 2009
Status:	Final
Class:	Public
File:	fidis_deliverable_wp3_14_V1_0_final

Summary

Biometric systems vary widely in their set-up, architecture and purpose (security, convenience, forensic etc.). The objective of this deliverable is a proof of concept for a trusted authentication system that uses biometrics in a divided control scheme. In this scheme the biometric data is encapsulated in a personal token controlled by the user but the implementation of the biometric processing is in the tamper resistant token is controlled by the operator. The proof of concept is achieved through a practical application of a distributed biometric authentication and transaction verification system in a field test setup to demonstrate the usability of the theoretical framework elaborated in D3.10.

The field test is based on a small but still representative sample of users from different European countries. The test participants are authenticated through their biometrics without any disclosure of biometric data to an operator (application of the proportionality principle).

The theoretical basis for this demonstrator system is based on the divided control model using encapsulated biometric data and processing that has been described in D3.10. This implementation was recommended as preferred model for privacy-enhancing biometric applications. It relies on functional requirements in terms of conformity with the existing legal privacy framework and recommendations for biometric systems in the EU and in Switzerland. This field test serves as experimental verification of the theoretical models.

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	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	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	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	21.3.2008	• Planning of the deliverable with first content list (Lorenz Müller, Els Kindt)
0.2	31.8.2008	• Setup of test system (Lorenz Müller, Marcel Jacomet, Andreas Eicher)
0.3	30.11.2008	• Definition of field test protocol (Lorenz Müller, Els Kindt, other contributors)
0.4	30.4.2009	• Field test closed, collection of results (Lorenz Müller, all contributors)
0.5	20.5.2009	• Commented content list of deliverable report (Lorenz Müller, Els Kindt)
0.6	8.6.2009	• Field test results, technical, usability, legal and privacy aspects (Els Kindt, Lorenz Müller)
0.7	17.6.2009	• Preliminary draft of deliverable report (Lorenz Müller, Els Kindt)
0.8	23.7.2009	• Final draft of deliverable for reviewers (Lorenz Müller)
0.9	Begin of August	• Corrections and final review (Lorenz Müller, Els Kindt)
1.0	5.8.09	• Final deliverable

Foreword

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

Chapter	*Contributor(s)*
1 (Introduction)	Lorenz Müller, Els Kindt
2 (Fieldtest planing)	Lorenz Müller, Els Kindt, Martin Meints, Denis Royer
3 (Fieldtest run)	All contributors
4 (Result evaluation)	Lorenz Müller, Els Kindt
5 (Conclusion)	Lorenz Müller
Annex	Lorenz Müller, Els Kindt

Table of Contents

1 Executive Summary

In previous deliverables (D3.2, D3.10) the FIDIS consortium elaborated a comprehensive theoretical framework for the use of biometrics in compliance with technological possibilities, legal constraints, ergonomic expectations and economic feasibilities. The advantages and disadvantages of different architectural and conceptual models have been evaluated under the above aspects. A critical point in all implementations is the storage and the control of the biometric reference data of the enrolled biometric subjects. Two models have been forwarded as recommendations for best practice implementations of the storage and usage of the biometric data for the enrolment and recognition processes.

In the shared control model biometric data are stored in a centralised or distributed database, under the control of different organisations that supervise the biometric processing to be compliant with the proportionality principle for personal data processing. Such models with access to all reference templates in the recognition process may be necessary to guarantee the uniqueness of the identity claimed by the biometric subject. Such implementations are necessary to prevent individuals from using several identities in a certain application context.

In the divided control model the biometric data are stored and processed in a personal device provided or accepted by the organisation that requests authentication through a biometric recognition. Thus the processing itself is controlled by the organisation but the biometric data and the usage of the device is controlled by the individual subject. The biometric data and processing is encapsulated in the personal device and never leaves the device and no biometric information besides the fact that a certain recognition process was successful is disclosed to the operator or a third party. Systems based on models with encapsulated biometrics guarantee the uniqueness of a biometric subject that may claim a certain identity. They cannot guarantee that a certain individual has an unique identity. Thus they are not suitable for forensic applications. But implementations based on the divided control model are recommended for the protection of the identity of individuals from theft or abuse. The preferred implementation is in a user centric Personal Identity Management Assistant (PIMA) device.

The purpose of this deliverable is to check the technical feasibility, the organisational practicability and the user acceptance of the divided control model within a field test. Such a test is indicated as the usage of a biometric device is still new for most persons and thus the acceptance is not granted by itself. In addition the best ergonomics of a biometric device used by individuals in the field is not yet known and user may be reluctant to such a personalized model with an initial usage learning threshold. These open points of the recommended implementation model have to be elucidated in practice with an existing PIMA. Such a credit card sized device with encapsulated biometrics is built by one of the FIDIS partner organisation (AXS Internet Passport). In the field test the device was distributed to a selected sample of 30 test persons from Germany, Belgium, the Netherlands and Switzerland. It was used to protect their OpenID identifiers previously established by the test persons. The OpenID is a widely accepted Internet identity credential that allows accessing various accepting web sites with the same authentication process. Also the access to the FIDIS internal web site is available for OpenID identifiers.

The field test lasted for 4 months starting at begin of the year 2009. All test persons performed the initial enrolment of their biometrics into the AXS Internet Passports and the initial binding of their card with the OpenID identifier provided by a Swiss OpenID operator without additional help or support. These settings for the field test simulate a realistic distribution process of such an encapsulated PIMA for commercial applications. The test persons reported their personal concerns about the usage of biometrics and their real life experience with the mean of a questionnaire and with personal comments.

In parallel to the practical field test all legal constraints for the application of biometrics in such a usage model have been carefully evaluated for all four countries in which field test persons were involved. The various data protection laws request in most cases a special treatment of biometric data and the consent of the biometric subjects. Additional requirements have been fulfilled by specific contracts for the test operators and a consent form for the test persons.

The result of the test shows that the divided control model is accepted by the majority of the test persons. But a certain reluctance towards biometric recognition remains present within a about a third of the test population. The practical test showed that ergonomic aspects are predominant for the user experience and convenience is in most cases higher rated than security even for biometric applications. It is an intrinsic fact of any biometric system that the most critical process is the initial enrolment and thus the establishment of reference templates. The later performance of the biometric recognition processes heavily depend on the quality of these initial reference data. In the field test this most critical step was done by the inexperienced user right after he or she received the device. The enrolment process therefore caused the highest level of non satisfaction and frustration within the field test user community. The application of the divided control model using a PIMA that is distributed to inexperienced users has to plan the initial enrolment process very carefully to avoid poor performance and user frustration. The field test however also showed that the learning curve for the use of a personal biometric device is very steep. Almost all users claimed to have no usage problems in the subsequent authentication processes once they completed the enrolment. In general the understanding of the constraints of an authentication protocol based on a biometric measurement is not high even in the IT educated population.

The conclusion of the field test is that the divided control model is apt for applications where the identities of individuals have to be protected. The ergonomic design of the PIMA device and of the enrolment protocol is crucial for the user acceptance and the system performance. The legal aspects of a deployment of a biometric system have to be carefully evaluated and are different from country to country. In general the divided control model bears less legal problems than systems with centralised biometric data storage. Taking all aspects into account the used implementation of biometrics in a system-on-card model with divided control can be considered as best practice for secure and privacy protecting biometric authentication in E-commerce applications.

2 Introduction

2.1 Overview of the document

This report discusses the way biometrics can be applied for the purpose of biometric user recognition in the verification mode[1] in real life systems in accordance with all requests coming from data protection and privacy considerations. The findings of the report describe the goals, the setup and the result of a practical field test using a device that verifies the legitimacy of its user through fingerprint recognition.

In the introduction the recommended implementation of biometrics as described in a previous Fidis deliverable [Fidis310] is recapitulated with emphasis on the practical implications coming from the legal, technical and privacy protection requirements. An important enabler or disabler of biometric applications is the reliability, the ergonomics and the economics of the biometric verification process in an identity based application. All these aspects are, at least partially, covered by the setup and concept of the field test. The applied methods are described in the last section of the introduction.

The third chapter describes the concrete outcomes of the field test that shall emerge from the evaluation process of the test results. The used instruments for the test data acquisition, the protection of the participants of the field test and the legal framework are presented. In the first part of the chapter a detailed description of the field test setup and especially of the processing architecture of the underlying authentication system is presented with emphasis on the implemented biometrics. In the second part of the chapter we present the standards and constraints from a legal point of view that governs the realisation of the field test.

The following chapter describes the realization of the field test with the applied test protocol and the collection of the raw data.

One chapter is dedicated to the observations made by the participants during the field test and the evaluation of the collected data. The summary data are extracted from the returned questionnaires, the comments of the tester and the observed usage of the test device during the field test period.

The report ends with a final conclusion comparing the practical results with the principal findings and recommendations of the previous Fidis report D3.10 [Fidis310].

In the annex the used questionnaires, the compiled responses, the usage statistics and the legal framework documents are attached to allow further evaluation of the data and further usage of the legal models developed for the purpose of the field test but with a more general application potential.

[1] In biometrics two operational modes are defined: In the verification mode a biometric subject claims a certain identity and his biometric data sample are just compared with the reference template that corresponds to the claimed identity. In the identification mode a subject delivers just a biometric data sample that then is compared with all other samples in the database to define his identity. In the limiting case that only one person is registered in the database, for instance in a personal token, the two modes become the same [Fidis310].

2.2 Fidis recommended implementations of biometrics

In the report D3.10 *Biometrics in Identity Management* [Fidis310] several aspects concerning security of the biometric data, privacy protection in connection with biometrics and request on biometric systems from legal and ergonomic considerations have been discussed. The differences, the threats but also the advantages of biometric applications compared to traditional authentication methods have been presented. The main findings were

- A clear distinction of the different operation modes is necessary. It is relevant whether a biometric system operates in the identification or in the verification mode. The identification mode applied to many individuals automatically requests some centralised processing of biometric data. The collected biometric data captured from individuals have to be compared with all previously stored reference templates to decide if the biometric subject corresponds to some registered individual. In the verification mode however more distributed architectures with local capture and processing of biometric data are possible as the actual captured biometric sample data has only to be compared with a clearly identified reference template of the individual that claims a certain identity. The two modes, identification and verification, merge in the case of a system that recognises only one individual. Such a system can be implemented in a mobile device that represents an identifier for a partial identity of an individual. If the biometric data in addition is securely protected inside the device we speak about encapsulated biometrics.
- An intrinsic problem of the application of biometric methods in the recognition of individuals is the occurrence of measurement and evaluation errors. Such errors may lead to a false acceptance of an individual to have a certain identity or to the false rejection of an individual negating his true identity. For practical applications of a biometric system it is important to distinguish between the technical notion of false matching (FMR) or false non matching rates (FNMR) that characterises the performance of a certain biometric system for the comparison of one captured query template with one stored reference template and the notion of false acceptance (FAR) and false rejection rate (FRR) that characterises the performance of the full recognition process with all steps until a system makes the final acceptance or rejection decision. For a given biometric system the correlated relation between the FMR and the FNMR are represented by the ROC curve (Receiver Operation Characteristics). The performance parameter (FRR, FAR) of a biometric recognition system may deviate by orders of magnitude from the corresponding technical values depending on the recognition protocol, e.g. when several capture attempts are allowed before a final decision is taken or when the comparison process uses several reference templates covering the intrinsic variations of the single measurement processes. The relevant values for a practical implementation are always the FRR and the FAR, the FNMR and the FMR have only a technical importance as they define the principal recognition potential of a certain biometric method.
- A further problem of the collection of biometric data is the limited possibility to revoke or change void data. Biometric data often remain linked to the delivering individual during his whole lifetime and the raw data may even disclose health related information [Fidis310]. This quality of biometric data may generate an inacceptable hazard to the privacy of individuals and therefore biometric systems should be designed in a way that such threats on the biometric data are avoided. For this a classification grid for biometric systems has been developed that classifies biometric

systems according their control scheme. The most important criterion of the classification is the possession of control over the collected biometric data and the possession of control over the processing protocol and algorithms. Depending on the field of applications different control schemes (operator control, shared or divided control, user control) are possible. The legal principle of proportionality applied on the collection and processing of biometric data leads to the recommendation to favour control schemes that limit the disclosure of biometric raw data to the operator whenever possible. One scheme that realizes this request is the divided control model where the operator controls the processing method and protocol and the user controls the biometric data and the capture of these data. A system with encapsulated biometrics is in accordance with this preferred control model. There are however situations where a centralised control is unavoidable. Such cases especially occur in forensic applications or in applications where identities have to be mapped on individuals (necessity of negative identification proving that an individual has not a claimed identity or detection of multiple identities established by an individual for fraudulent purposes).

- For practical applications based on biometric authentication the convenience for the user and the cost effectiveness for the operator are very important. The implementation of biometric systems must take these constraints into account. Actually biometrics bear the potential for an enhanced user convenience for authentication processes as the user does not need to perform in cumbersome protocols linked to some personal secret, like PIN or long passwords combined with dedicated tokens with inserted smart cards or scratch lists. There are biometric methods like fingerprint or signature recognition that are well accepted by users and that have been technically developed in a way to allow a cost effective deployment. To really take advantage of a certain biometric authentication system its usage by different operator organisations would be highly beneficial. This for instance can be realised by integrating biometrics into a Personal Identity Management Assistant (PIMA) device of a user centric identity management system [Fidis31]. The user establishes authentic communication channels with all operators that accept his PIMA as an authenticating device. Such a user centric identity federation concept is realized by the AXS-Authentication System presented in the D3.10 report and used for the purpose of the field test. The PIMA in this system is the AXS Internet Passport with a fingerprint recognition System-on-Card that was also presented in the D3.10 report. The advantage for the user is that he does not need to learn different authentication procedures for each connection to another operator. The advantage for the accepting operator is that he does not need to roll out and handle an own authentication infrastructure with proprietary hardware devices and/or smart cards. He just can use the existing infrastructure already in the hand of the user to take advantage of the biometric authentication capability of the PIMA of the user. This model makes economical sense for the operator as he has only to cover marginal costs to participate in such a user centric authentication system (cost of the additional secure channel between him and the user). The total cost of a user centric identity management is shared among all participating organisations, the initial investment in the infrastructure is typically covered by ISP or telecom organisations.
- In the same report the legal constraints for the application of biometric systems have been compiled and presented. As a crucial point evolves the proportionality principle which states that only user data should be collected by an operator that are mandatory

for the specific application. Biometric data used to link a person to a specific identity or identity credential of a commercial application should be used in a very restrictive way so that no unintended and not consented use of such data is possible. The corresponding legal boundary conditions for the collection of biometric data thus can be very restrictive in certain countries. The legal findings relevant for the practical applications and especially for the field test in the four countries are entirely covered in the specific section below.

One of the principal conclusions of D3.10 is that the best solution to solve the problem of information leakage from biometric data in templates and from the processing of captured biometric data is user control and encapsulation of the whole biometric system into a tamper resistant device. Such a system-on-card solution will be used for the field test.

2.3 Field test environment - OpenID

The general field test environment shall permit using the AXS Internet Passport in multiple applications and especially for the access to the internal Fidis homepage. To achieve this operational goal many sites that accept an authentication with the AXS Internet Passport have to be available. This condition is easily fulfilled if the AXS Internet Passport is combined with an OpenID [OpenID] Identifier. The OpenID standard[2] is a world wide single sign on scheme that follows a simple protocol:

1. In an initial step the user has to enrol at an OpenID Identity Provider. For this he delivers a set of identifying credentials, agrees with the provider on an authentication procedure and receives from him the OpenID Identifier which is basically an URL that links to the authentication procedure of the OpenID Identity Provider (OpenIDprovider).
2. To authenticate at the site of an acceptor, called relying party, of the OpenID Identifier the following authentication protocol runs:
    a. The user requests access to the Web Site of the relying party that offers authentication via an OpenID Identifier
    b. The user enters his OpenID Identifier into the OpenID login form of the relying party
    c. The relying party transforms the OpenID identifier into a canonical URL form and request this URL to connect him with the OpenID identity Provider

[2] Wikipedia explains the OpenID standard as follows:

"OpenID is an open, decentralized standard for user authentication and access control, allowing users to log onto many services with the same digital identity. As such, it replaces the common login process that uses a login-name and a password, by allowing a user to log in once and gain access to the resources of multiple software systems.

An OpenID is in the form of a unique URL, and is authenticated by the user's 'OpenID provider' (that is, the entity hosting their OpenID URL). The OpenID protocol does not rely on a central authority to authenticate a user's identity. Since neither the OpenID protocol nor Web sites requiring identification may mandate a specific type of authentication, non-standard forms of authentication can be used, such as smart cards, biometrics, or ordinary passwords.

OpenID authentication is used and provided by several large websites. Organizations like AOL, BBC, Google, IBM, Microsoft, MySpace, Orange, PayPal, VeriSign, Yandex, Ustream and Yahoo! act as providers."

d. The relying party and the OpenID Identity Provider establish a secure communication channel and the relying party then connects the access requesting user directly to the OpenID Provider authentication server.
e. The OpenID Identity Provider authenticates the user by the means he has implemented; in the case of the field test setup this is the AXS-Authentication System where the user needs the Internet Passport.
f. Upon correct authentication of the user the OpenID Identity Provider redirects the user to the web site of the relying party. In parallel he delivers some identifying user credentials for the relying party over the established secure channel.
g. Upon reception the relying party grants the user access to his resources.

The sent credentials identifying the user may include some or all of the credentials that the OpenID Identity Provider collected during the initial establishment of the user account when he delivered the OpenID identifier. The fact that this credential delivery could be considered as a privacy hazard is not relevant for the findings of the field test as it is a standard procedure of the OpenID scheme outside the sphere of influence of the field test definition. Furthermore most OpenIDproviders allow the user to choose which data should be transferred to the relying party - at least the Swiss Identity Provider Clavid that has been elected for the field test provides this option.

3 Field test objectives and instruments

The purpose of the field test is to check

- the technical feasibility of a robust and stable implementation of encapsulated biometrics in a personal device with divided control of the biometrics,
- the acceptance of the user to use biometrics to authenticate towards such a personal device,
- the ergonomics of the used AXS Internet Passport and the user felt performance of the biometric authentication process and
- the user demand for such an authentication scheme applicable in multiple contexts.

3.1 Evaluation goals and instruments

The specific goals are the elicitation of

- the user concern and beliefs in relation with the privacy of biometric data in an encapsulated biometric system
- the user requests on convenience for authentication systems
- the general attitude of users towards biometric authentication in civil applications
- the security consciousness of the user when he submits sensitive data over the Internet
- the ability to correctly perform a biometric enrolment outside of a environment with supervised guidance
- the understanding to use a PIMA with biometrics in multiple application settings
- the willingness to learn new technical operations for the purpose of authentication and
- the legal constraints and boundary conditions.

3.2 Description of the AXS-Authentication System (AXS-AS)

The **AXS Authentication System™ (AXS-AS)** is an authentication management infrastructure that allows the delivery of identity based services over the Internet. The AXS AS includes the following functional components:

- **AXS Internet Passport**
  PIMA that can read encrypted messages sent by a server directly from a computer screen of a local Internet access device (PC, PDA, phone etc) through an optical interface. It displays the message content upon biometric authentication of the user to assure that only the legitimate user has access to the message. The Internet Passport has 112 free preinitialised channels for connections to various business applications that accept the AXS-AS for identity assurance services.
- **AXS Integration Link (AXS-IL)**
  Interfacing SW components installed in the Business Application of the identity based value service Provider. The AXS-IL consists of the flickering code generator that transforms a binary message in a flickering code in the web browser of the user that can be read by the AXS Internet Passport.
- **AXS Security Manager (AXS-SM) server**
  The AXS-SM server administers the secure channels between the business application of a service Provider and the AXS Internet Passports. Upon request of the business application through a Web Service call by the AXS-IL the AXS-SM server generates and delivers an encrypted message dedicated to a specific AXS Internet Passport. The

message is then forwarded by the web server of the business application to the user Internet access device in form of a flickering code. An AXS-SM server may provide secure channels for an unlimited number of business applications and Internet Passports. The AXS-SM server is typically operated by an identity service operator.

- **AXS Credential Manager (AXS-CM)**
  The AXS-CM server distributes the initial credentials (keys) for the opening of secure channels between card and provider to the AXS-SM servers that are attached to it. It receives these initial credentials for all cards that are distributed over its domain of attached servers and business application portals. Such a tree is called an AXS domain and the domain over which an AXS Internet Passport is distributed is called the home domain as the AXS-CM delivers the channel credentials for this card inside and outside the domain. The AXS-CM is operated by a broker which is typically a ISP or a telecom company with a network infrastructure.
- **AXS Domain Router (AXS-DR)**
  The AXS-DR is a directory server that allows to identify the home domain of an AXS Internet Passport. When a user wants to use his Internet Passport with a business application of a Provider that is not attached to the tree of the card's home domain the AXS-CM of this foreign tree has to ask for a credential to open a secure channel into the card at its home domain. The AXS-CM of the foreign domain identifies through the AXS-DR the home domain and requests from the corresponding AXS-CM a credential set to open a secure channel to the Internet Passport in question. This architecture allows a seamless roaming of the AXS Internet Passport between domains. For the user the AXS Internet Passport becomes a universally applicable PIMA. However certain brokers may restrict the roaming from and to their domain tree according their security policy.

The domain tree and logical connection architecture is sketched in Fig. 1.

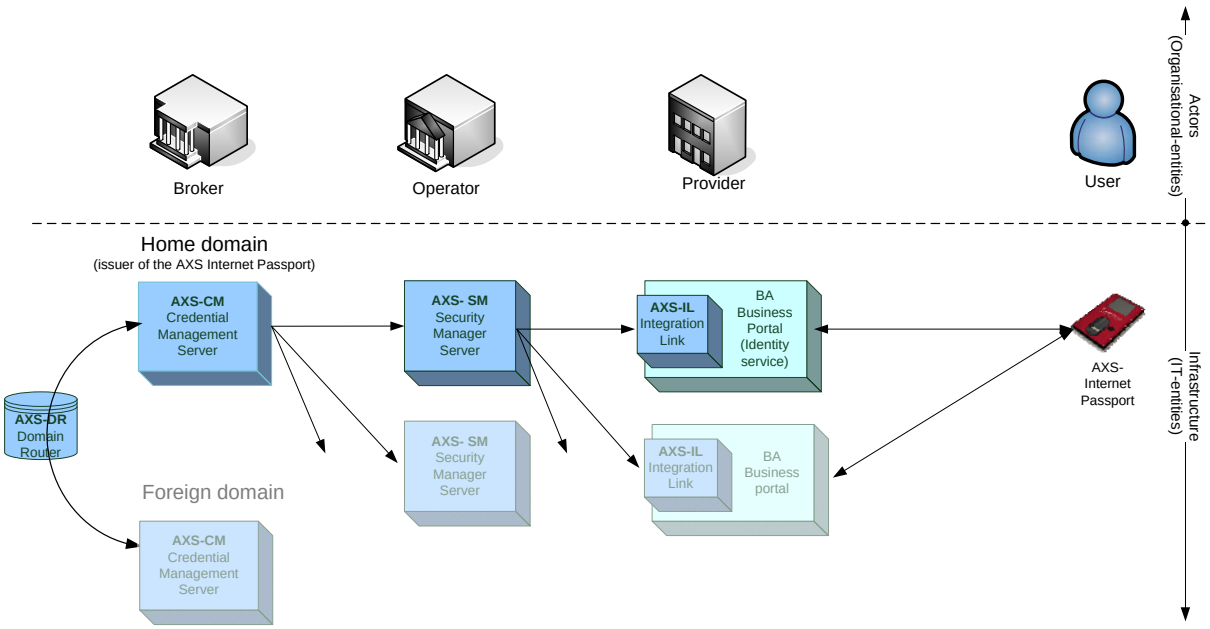


Figure 1: AXS-AS system architecture with components and indicated domain tree

The user's AXS Internet Passport offers a trusted display, independent from the local computing infrastructure. The AXS Security Manager software must be installed in the secure zone of an identity service operator. The AXS Integration Link interfaces to the identity management system of the service provider and calls the AXS-Security Manager over Web services. The **Flickering Code Generator** (**FCG**) methods are integrated in the web presentation of the operator and transform the encrypted message in an optical code in the browser of the user's Internet access device. The integration schematic is presented in Fig. 2.

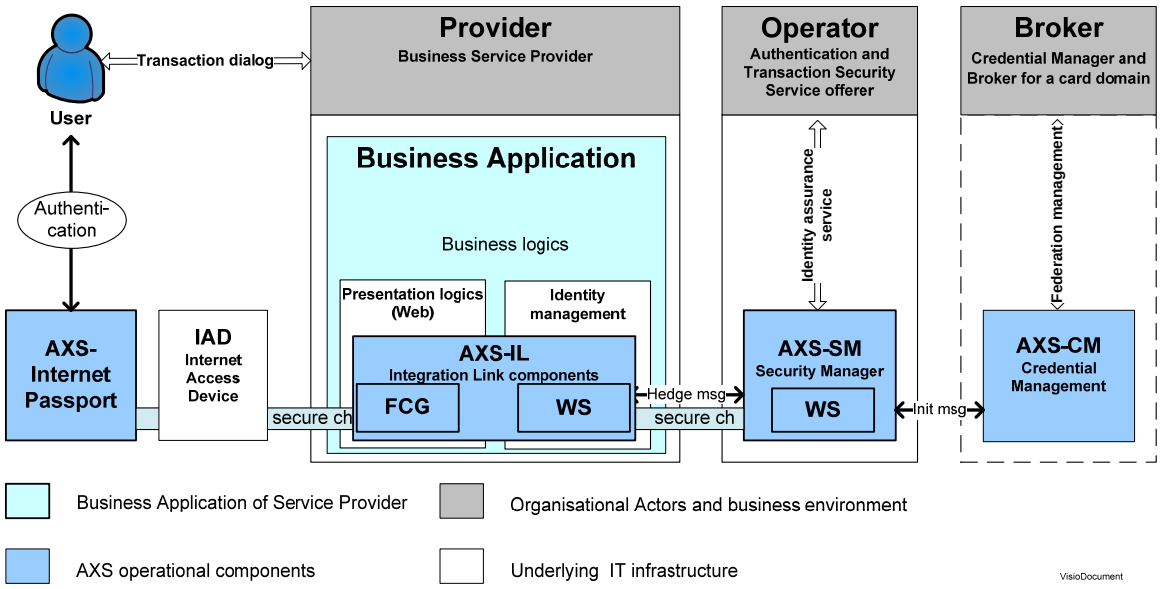


Figure 2: Integration of the AXS-AS in an existing IT infrastructure

For the purpose of the field test the following functions in relation to the AXS-AS were defined

- Provider of the identity assurance service is Clavid AG
  Clavid installed in their OpenID business application the workflow to initialse and use the AXS Internet Passport in connection with the OpenIDs provided by them.
- Operator of the AXS Security Manager and Credential Manager server is AXSionics
  AXSionics has an own domain and operates such servers for various attached provider of identity based services and directly also for business application providers.

An OpenID identity verification with the AXS Internet Passport consist of the following steps (bold printed steps are specific for the field test scheme):

- The user types his OpenID identifier into the login page of an OpenID acceptor (relying party)
- The acceptor (Relying Party) links the OpenID to the original OpenIDprovider which in this case is the Clavid server and connects the user to the OpenIDprovider
- **The Clavid server links the submitted OpenID identifier with the AXS Internet Passport number and request an authentication message**
- **The OpenID verification process request an authentication credential from the user and displays the flickering code**

- **The user reads with his AXS Internet Passport the flickering code, authenticates himself towards the card with his fingerprint biometrics and receives via card display the identity verification code**
- **The user enters the one time code which is submitted to the AXS-SM server for verification**
- **The AXS-SM server delivers the identity verification result to the OpenID identification server**
- The OpenID application forwards the identity credentials to the OpenID acceptor (Relying Party)
- According the result the acceptor (Relying Party) grants access to the user.

The operational architecture for the OpenID verification protocol of the field test is presented in Fig 3.

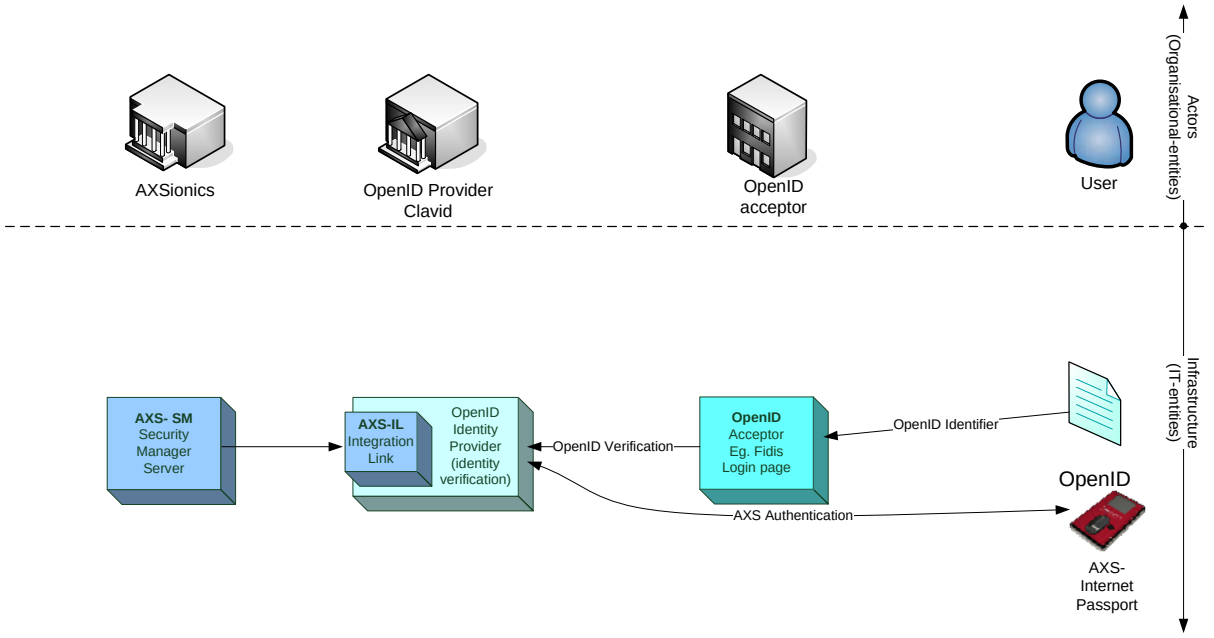


Figure 3: Combination of the OpenID scheme with the AXS-AS

3.2.1 The AXS Internet Passport

The principal component of the AXS-AS is the AXS Internet Passport. It is a credit card shaped Personal Identity Management Assistant (PIMA) that receives messages over an optical interface, recognises it's owning user through a 1-, 2 or 3-factor authentication protocol and informs its user over an integrated graphical display.

For this it has a fingerprint sweep sensor that serves also as input pad to enter for instance a PIN code. The card has an optical interface with 6 channels that reads flickering messages from any screen displays. It informs the user over an internal graphical OLED display with a resolution of 128 (W) x 96 (H) pixels. It has in addition a Mini-USB 2.0 interface that serves on one side to reload the accumulator of the token (reload necessary after approx. 200 transactions).. The token is started and stopped by pressing the power button.

One main novelty of the AXS AS is the optical interface. All tokens have this interface to read a flickering code displayed on the screen of the local client. The optical interface works with a wide variety of screens in almost any parameter settings. The bandwidth of the optical

interface depends on the characteristics of the screen, the graphic card and the available graphic driver software of the local computer. A typical value is 150 baud (bits/sec).

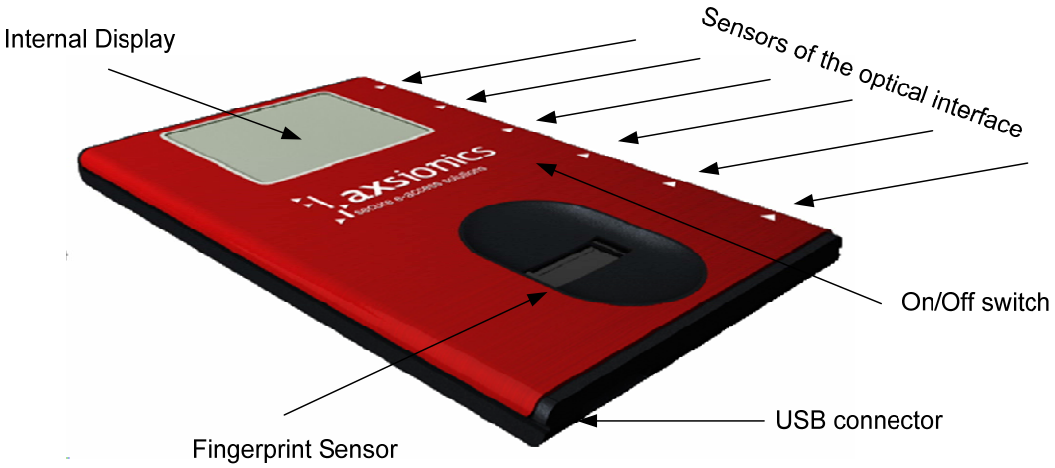


Figure 4: The AXS Internet Passport is a PIMA with a system-on-board biometrics, an optical interface for data input and graphical display for data output.

All critical data and computations are embedded in the secure processing platform inside the card which is a certified[3] (CC EAL 4+) microprocessor with a SAM 7 architecture. The security processor executes the cryptographic operations in an integrated secure and fast crypto coprocessor. All data, also the biometric data are enclosed in the tamper resistant memory of the microprocessor.

Another important novelty is the intrinsic user side identity federation capability. Each AXS Internet Passport has 128 preinstalled independent secured channels that can be activated to communicate with different service providers attached to any AXS-SM servers. This setting allows to use the AXS Internet Passport in principle for all identity based services a user wants to get access to. For the attachment to the OpenID Identifier only one of these channels was used.

3.2.2 Characteristics of the biometrics in the AXS-AS

The AXS Internet Passport adopts the divided control model for the biometric processing combined with an encapsulated implementation of the biometric procedures. The whole biometric processing is realised as system-on-card inside the AXS Internet Passport. The storage of the biometric reference templates, the measurement and the decision about the biometric application usage are under the sole control of the user. The way the data are processed and the recognition decision are under the control of the AXS-AS and thus the card issuing operator. Due to the encapsulated implementation of the data and the processing algorithms the user can not trick the card into a wrong authentication and therefore the operator still can trust the delivered result of the authentication process as long as the answer code that the user has to return is onetime and unique. On the other side the user knows that the full biometric process remains in his hand and the operator will never get access to his

[3] Common Criteria is a standard for security certification of IT infrastructure. It defines different certification levels, so called Evaluation Assurance Levels (EALx). See http://www.commoncriteriaportal.org/thecc.html

biometric data. With this scheme the proportionality principle for personal data processing can be fulfilled even when biometric data are used for purely commercial applications.

The whole implementation is protected in a tamper resistant processor in the AXS Internet Passport. Such an implementation reduces to a great extent the threats to the data or the processing of a biometric system often cited by critics.

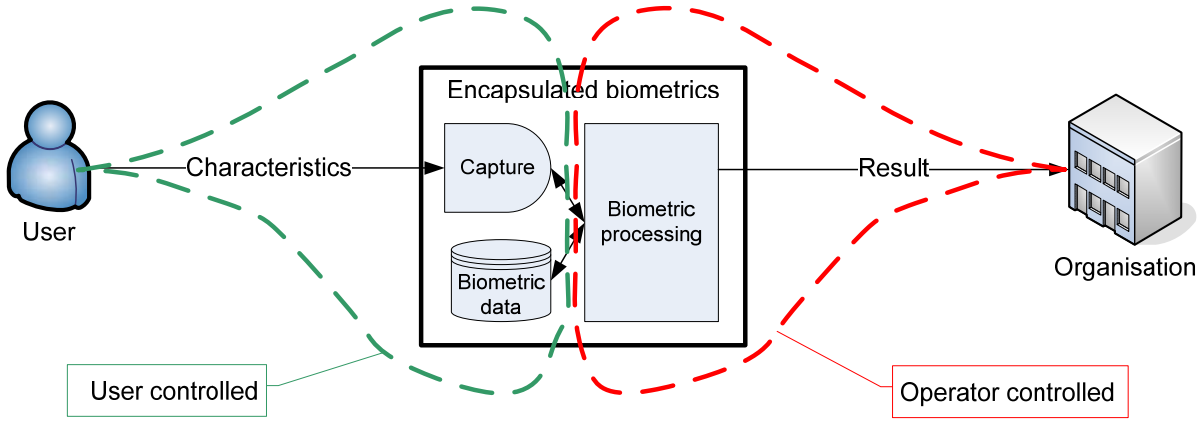


Figure 5: Scheme of the divided control model fora biometric system

3.2.3 Security and functional requirements for the test environment

For the field test the following usage requests were fulfilled:

- Each user can establish an OpenID identifier and link it with his AXS Internet Passport in an easy way at the site of the OpenID Provider Clavid.
- The provided OpenID identifier shall work with all or at least almost all OpenID accepting sites
- The AXS authentication process shall start seamless right after the submission of the OpenID identifier into the login web page of an acceptor (Relying Party)
- The user shall be able to unlink his OpenID from the AXS Internet Passport but the AXS Internet Passport will remain linked biometrically to him or her

The following data protection and security measures were applied for the field test using OpenID and the AXS Internet Passport:

- No name of testers will be recorded by the test organizer (with the exception of voluntary supplied Email addresses)
- All statistical raw data collected during the field test are classified at the security level 3 (only internal use at AXSionics). Only compiled statistics will be published
- The test users were urged to chose a non speaking OpenID identifier name
- The Relying Party (processor) will only collect the non personal OpenID identifier to make the access log statistics with success and failure log
- After the end of the field test all statistical raw data at the processor and the controller and the test agent institutions will be discarded. Only compiled data will be kept for future research purposes.

- All published statistical data are anonymized in the sense that no link between a user, the AXS Internet Passport number and the usage statistics can be reconstructed.

The fulfilment of the usage and security requirements have been realised and tested before the start of the field test with the Fidis internal homepage as Relying Party, the OpenID Provider (Clavid) and AXSionics as the processing operator of the AXS-AS in the field test.

A detailed user instruction has been produced to guide the user through the OpenID identifier ordering process, the personalization of the AXS Internet Passport, the link of the Passport with the OpenID identifier and the usage of the OpenID for the access to the Fidis web page.

3.3 Legal and operational aspects of the biometric field test setup

The legal compliance requirements were also an important aspect of the biometric field test setup.

3.3.1 General

Limitation of number of participating Fidis partners - For legal compliance purposes, the number of participating Fidis members has been limited and was restricted to the countries where the data protection legislation requirements could be managed with the help of the test agents. These test agents would coordinate some compliance aspects, such as the assistance to and the organisation of a notification to the data protection authorities if needed, the provision of information to the data subjects, the request for free, informed and specific consent and the collection of the anonymous questionnaires.

For these reasons, the countries and test agents were the following : Germany, with test agent ICPP, Belgium, with test agent ICRI, the Netherlands with test agent TILT and Switzerland with test agent AXSionics. AXSionics combined this role of test agent with the responsibility of controller of the processing of personal data for the test (see below).

Role of the test agents : no processing of data - The test agent needed to identify a certain number of participants in their country for testing the AXS-Internet Passport (in connection with websites that use OpenID) and for filling in the questionnaire. The test agents would be more a contact person for the participants in the test. They did not process any data. They have only collected the questionnaires (in paper form) which were fully anonymous and not part of any file system and which they forwarded to AXSionics, the controller. The test agents had no access to any personal data whatsoever.

Applicable law - It was reviewed and concluded that in this set up, the data protection legislations of Germany, Switzerland, Belgium and the Netherlands would apply to the field test.

3.3.2 Summary of the demonstrator set up and the applicable legislation

The field test was organized by AXSionics established in Switzerland for test and research purposes. In particular the test included the evaluation of the proof of concept and the field demonstrator of the AXS Internet Passport on which biometric fingerprint would be locally stored for authentication (in particular verification) purposes of the user of the card, and the proper functioning of the related applications developed by AXSionics, in particular the interface between the card and the OpenID authentication application programs (which is available with Clavid), and user feedback (by questionnaires).

Personal data of the data subjects (who were the involved researchers and volunteers of Fidis partners) was limited: fingerprint (biometric) data stored and used on the card (under the control of the user), account data for the OpenID and communications on authentication attempts. AXSionics determined the means (i.e. the use of the AXS Internet Passport) and the purposes (i.e. validation of the demonstrator and the use of the AXS Internet Passport) of the use of personal data in the field tests. AXSionics was therefore the controller of the field tests.

As a result, Swiss federal data protection[4] was applicable to the field test organized by AXSionics established in Switzerland where AXSionics would distribute in the framework of its activities AXS Internet Passports for the field test amongst its researchers.

AXSionics also distributed AXS Internet Passports for the field test to researchers of the Fidis consortium partners in Belgium, the Netherlands, and Germany.

Although AXSionics has no establishment in any of these countries, the possibility that the local data protection laws[5] apply to the deployment of the AXS Internet Passport in these countries was taken into account (see art. 4 1 c of the Directive 95/46/EC as implemented in the concerned member states[6]). For this reason, it was also advised to limit the number of countries of the participating researchers.

3.3.3 Brief recapitulation of some of the legal requirements complied with under the applicable legislation

AXSionics had to comply with the above mention data protection legislations for the field tests and demonstrator.

Without mentioning all legal requirements (reference is made to other relevant Fidis deliverables, including D3.2 and D3.6, and the texts of the national applicable laws), the most important requirements which are important for the practical preparation and compliance of the field test are summarized hereinafter.

Legal basis : free, informed and specific consent - One of the legal basis on which the test could rely for the processing of personal data considering the context, is the free, specific and informed consent. Specific information is to be provided as specified in the applicable laws

---

[4] The Swiss (federal) data protection legislation dates of 19 June 1992 (with important modifications entering into force on 1st of January 2008) and is available in English at http://www.edoeb.admin.ch/org/00828/index.html?lang=en and in German at http://www.admin.ch/ch/d/sr/2/235.1.de.pdf .

[5] The *Belgian (federal) data protection legislation* dates of 8 December 1992 (with modifications). An unofficial translation is available at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

The *German (federal) data protection legislation* dates of 18 May 2001. An unofficial translation is available at http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzFederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/BundesdatenschutzgesetzFederalDataProtectionAct.pdf . The *Dutch data protection legislation* dates of 6 July 2000 and an unofficial translation is available at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

[6] Although is was agreed that the cards would become property of the data subjects in order to minimize the risks of data abuse, the cards are likely to remain 'equipment' used in Belgium, the Netherlands, etc; the question will remain whether this is for the use of AXSionics or the data subject ; because of the purposes of the test and the demonstrator, it will remain difficult to argue that these local data protection laws would not apply upon using the card (compare opinion about applicability of the laws on data processing with 'cookies' send by US companies to pc's owned by data subjects).

which were taken in a cumulative way into account when the consent was prepared and drafted. The possibility that biometric data include information about health was also taken into account. The consent also included reference to the user questionnaires. A draft proposed consent was discussed amongst all involved parties, agreed and finalized for use in the test. The consent was also preceded with extensive information about the processing aspects of the demonstrator. This information and consent is set forth in the Annex.

Notification obligation - The processing of personal data shall in principle be notified in the countries where the local data protection laws apply (see above) and require such notification. For the test purposes, exemptions could apply.

Switzerland: The processing of biometric data was in principle subject to notification.[7] However, there is an exemption if there is an independent data protection official appointed (see art. 11 a 5 e) or a certification (see art. 11 a 5 f in combination with art. 11).

Belgium : The demonstrator had to be notified to the Belgian DPA. There were no exemptions which applied. The existing exemptions for access control or membership seemed not to apply (biometric data is not mentioned). The notification was done electronically before the start of the processing and confirmation of the notification from the Data Protection Authority was received.

Germany: There was an exemption of notification if a data protection official was appointed which had been the case for all German institutions that participated in the study.

The Netherlands: There is a Dutch exemption of notification for research.[8]

Other: Other measures were taken to comply with the applicable local data protection legislation, including

- appointment of a data protection official by AXSionics (in which case no notification is required under Swiss Data protection law (see art. 11 a 5.e));
- all steps to fully inform and to ask the free consent of volunteers in conformity with all locally applicable laws (see information and consent form as mentioned above and as shown in the Annex) ;
- two processor agreements with the processors of the data (the Clavid operator and the Fidis server site operator) were drafted and concluded ;
- AXSionics collected and evaluated the data for strictly the purpose of the Fidis D3.14 report and destroys the raw data afterwards (supervision by the data protection official). The raw data also include the report on OpenID access to the internal Fidis site with Clavid OpenIDs ;
- minimisation of the data collection. As only data was collected that had been necessary for the test purpose;
- In order for the research demonstrator to qualify under the Dutch exemption of notification of the research, all personal data collected under the demonstrator in all countries will be deleted at the latest 6 months after collection (see 'Exemption 28

[7] See art. 11a.3 of the Swiss data protection legislation : ' wenn (…) regelmässig besonders schützenswerte Personendaten (..) bearbeitet werden'.

[8] See 'Exemption 28 (Art. 30 Exemption Decree)', available (in Dutch) at http://www.cbpweb.nl/HvB_website_1.0/vwc28.htm).

(Art. 30 Exemption Decree)', available (in Dutch) at http://www.cbpweb.nl/HvB_website_1.0/vwc28.htm).

- The AXS Internet Passport remained in the hand of the data subjects after the test. The data subjects could at their choice continue their usage or not at their own discretion. They may also unregister or not their account at Clavid at their own discretion.

3.3.4 Positioning of the demonstrator

The demonstrator system provides a privacy enhancing solution for various (legal and privacy) concerns relating to a application that uses biometric data. These concerns relate, as mentioned, to risks of leakage of sensitive information, the use of biometric data for identification purposes without knowledge of the data subject, the use as unique identifier and use for purposes other than those originally intended. All these risks are considerable in centrally controlled biometric data applications. In general, biometric systems as authentication means are moreover far more complex than for example the use of a password or PIN check.[9] A biometric system always requires that (i) biometric characteristics are previously to the authentication, captured from the data subject, processed and stored for comparison and that (ii) the same characteristics are for comparison captured from the data subject and processed again. In a centralised biometric application infrastructure, the data subject looses control over his or her biometric data, stored in various places and processed by the various components of the system of which the data subject is not or almost not informed.

The control by the data subject over biometrics that are stored on a token, however, would mean that the data subject would control the biometric data and the usage of the biometric device.[10] The data subject would in principle know (and control) when the biometric information is used (e.g., for comparison), and also by whom. Subject to the further technical specifications, the data would also not leave the card. Ownership of the token, would in principle not be of primary importance, but may enhance the control of the data subject over his or her biometric information.[11]

This control by the data subject is not specifically mentioned in the Directive 95/46/EC. However, the Directive aims at transparency for the data subject and user controlled biometric authentication means certainly increases such transparency. Moreover, the Directive clearly requires purpose limitation and data minimisation which are advanced by a user-controlled biometric system. The biometric data locally stored, upon the condition that it does not leave the card, will also not leak sensitive information (such as health related information), be used as unique identifier or for surveillance purposes. Errors, because of the local storage, are also reduced. The architecture of the demonstrator and the technical specifications therefore could be qualified as privacy enhancing; If the data subject has the choice to use the biometric

---

[9] See also 'Biometrics' in *The Future of Identity in the Information Society. Challenges and Opportunities*, K. Rannenberg *e.a.* (eds.), Dordrecht, Springer, 2009, p. 147.[Future]

[10] Reference is also made to previous ideas to give the citizen more control over personal data, for example, in the Netherlands, where it was pleaded some time ago to give citizens the right to control a so-called 'digital safe' (digital kluisje)with their personal data. It would contain not only basic (identity) information such as name and address, but also other personal data, such as health or financial data. Such 'digital safe' would preferably be held in a webbased application. See *GBA-commissie wil digital kluisje*, 30 March 2001, available at http://www.computable.nl/artikel/nieuws/146476/250449/gbacommissie-wil-digitaal-kluisje.html

[11] For example, because the token is not to be returned and no biometric data will leave the possession of the data subject.

enhanced digital identity assistant or not, the right of the data subject to object against the processing of biometric data are also respected. Because these technical measures limit considerably the risks of abuse of biometric data, the risks for the data subject become more limited. Because of the advantages that biometric data may offer in authentication applications which require increased security, the use of biometric data may be considered to fulfil the proportionality criterion for such purposes of verification. Whether the data subject is able to exercise his or her right to alternative means, will depend on the practical implementation.

The demonstrator with a user-controlled biometric architecture is also in line with the user-controlled and user-centric identity management concepts and systems mentioned by many to solve the increasingly complicated problems of loss of privacy, e.g. by data breaches. Such systems are being developed for the enhancements of the (data protection) rights of the users.[12] Although the demonstrator is based on the divided control model [Fidis310], whereby the identity or service provider will control the processing of the data, the data subject will retain full control over his or her biometric data which will not be shared or disclosed outside the card.[13]

The concept is also in line with the right to privacy. The fundamental right of respect for one's privacy[14] includes the aspect that a person has rights (of control) over personal information. In a pioneering work of 1967[15], Alan F. Westin defined privacy as 'the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others.' (stress added). Westin stressed privacy as a form of autonomy, in particular, the ability to control the flow of information about oneself. In his view, an individual should be able to decide between or to remain 'in solitude, intimacy, anonymity, (…)'. Westin has further defined this aspect of privacy as follows : 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others' (stress added).[16] Arthur R. Miller[17] also stated shortly thereafter that 'the basic attribute of an effective right to privacy [is] the individual's ability to control the flow of information concerning or describing him [..]' (stress added) The personal information that one want to control will in the first place concern information which closely relates to the person and are regarded as intimate, and which a person would want to keep for him- or herself or at least to restrict the collection, use and circulation thereof. Examples include information about one's

---

[12] See, for example, other projects, such as Prime and Primelife, in particular the Prime white paper, v. 3, 15 May 2008 available online: https://www.prime-project.eu/prime_products/whitepaper/index.html.

[13] This model is therefore also referred to as a user-controlled biometric authentication system, although – contrary to the model of e.g., Prime – the data subject will not have control over the other components of the identity management system, while retaining control over the *biometric* data.

[14] For example, as laid down in Article 8 of the European Convention on Human Rights of 1950.

[15] A. Westin, *Privacy and Freedom*, New York, Atheneum, 1967.

[16] A. Westin, *o.c.*, p. 7.

[17] Arthur R. Miller published in 1971 in the United States the book 'The Assault on Privacy', in which he examined the effect of the technological revolution (of that time) on individual privacy. He made various proposals to reconcile technology with society values, which aroused discussion and controversy. See A. Miller, *The Assault on Privacy : Computers, Data Bases and Dossiers*, Ann Arbor, University of Michigan press, 1971.

health or sex life, but could also include biometric information because of its unique characteristics which are linked with an individual.

Do user-centric solutions imply that the data subject would become controller of the processing ? The use of the term 'control' by the user is not to be confused with the concept of control by the data controller in the data protection legislation. This concept of control by the data controller refers to the control over the 'means used' and the 'purposes of the processing' of the personal data. The entities which decide over these aspects, are under the present data protection legislation considered responsible for the data processing and shall comply with all data protection legislation obligations. This does not change with user-controlled or user-centric biometric systems. For example, if a banking company would want the users of online banking applications to be more securely authenticated, the bank will in most cases take the decision about the use of for example the (biometric) token for the purposes of the authentication of its clients. The bank will hence remain the controller of the processing.

In other settings, even an ISP or telecom organisation could be the controller of the identity management system.[18]

Finally, technology alone will not be sufficient to enhance the data protection and privacy rights of the data subjects. Additional organizational and compliance measures remain necessary, such as the provision of sufficiently detailed and understandable information about the processing, the organisation of alternative means and choice thereof and the internal but independent control of the directive's application or, where necessary, a notification to the data protection authorities.

4 Demonstrator system and field test

The demonstrator system consists of an OpenID established at the site of the OpenID identity provider Clavid and an AXS Internet Passport that is used for the identity verification whenever a user uses his OpenID Identifier.

The field test was done with 30 test persons equally distributed in the participating countries Belgium, Germany, Holland and Switzerland and administered by a local country test agent who selects the field test participants[19]. All the test persons were accepted as users on the internal Fidis web site. Each test person had to establish an OpenID Identifier and use this identifier for the login into the Fidis internal homepage. We expected that the test persons also use their OpenID Identifier for logins into further web sites that also accept OpenID.

4.1 OpenID Identity Provider

The OpenID Identifier suitable for the field test has to be established by a OpenID identity provider who has implemented the authentication protocol of the AXS Internet Passport in his OpenID identity verification check procedure. Such an OpenID identity provider is the Swiss company Clavid [Clavid]. Clavid provides special secured OpenID identifiers that use a

[18] The fact that AXSionics was in the field test controller of the processing does not change this fact. It is clear that AXSionics was only controller because of the demonstration purposes of the field test organized by AXSionics.

[19] There were 30 test persons, 4 test agents and the field test organizer that used the Clavid service during the field test period.

strong authentication protocol for the identity verification of the user. Any relying party web site that offers authentication through OpenID then can take advantage of the strong authentication achieved with the AXS Internet Passport.

4.2 Field test communication architecture

The communication architecture for the field test authentication with the Internet Passport at all Relying Parties accepting OpenIDs is sketched in the following figure:

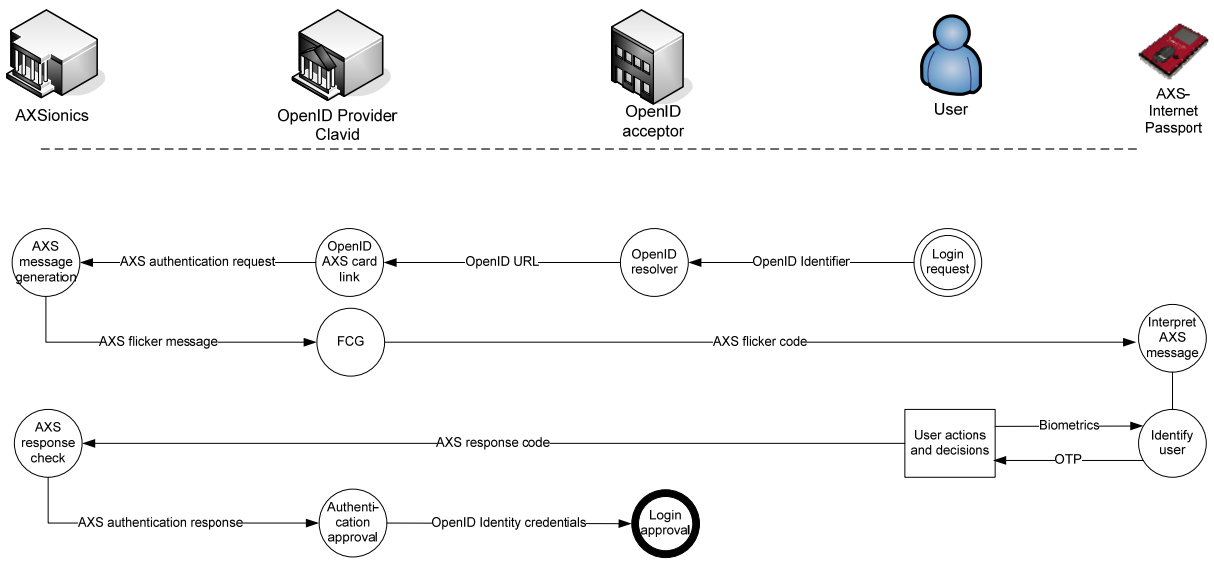


Figure 6: Dataflow for the authentication using OpenID combined with the AXS AS

4.3 Field test setup

The field test separated in the three phases

- **Preparation**
  The preparation included:
  - Define and establish the detailed concept and schedule to run the field test
  - Recruit a suitable OpenID Provider and support him to make the necessary technical developments to allow the link of the OpenID with the AXS Internet Passport via the AXS Authentication System
  - Find country agents among the Fidis collaborators for the administration of the field test in the participating countries of Fidis partners (Germany, Belgium, Holland Switzerland)
  - Recruit 6 to 8 test users in all participating countries over the country agents
  - Develop a questionnaire that reflects the open questions for which answers were needed to achieve the field test goals
  - Investigate about legal constraints for the usage of biometric authentication means and take corresponding actions, e.g. naming of a data protection officer
  - Develop the consent forms and documents for the users and operators that comply with the legal constraints in each country

  - Develop a detailed user guidance (document, video clips) for the requested user actions during the AXS Internet Passport personalization and the registration at the Clavid Identity Provider
- **Execution**
  The execution included:
  - Anonymous distribution of the AXS Internet Passports, the legal forms, the instructions and the questionnaires to the test users via the country agents
  - Support, consulting and controlling of the test users by the country agents to follow the test protocol
  - The execution of the below presented test protocol by the test users during the runtime of the field test
  - The collection of the questionnaires
- **Evaluation**
  The evaluation included:
  - Collection of all user feedbacks during the field test run
  - Retrieval and statistical evaluation of the questionnaires
  - Report

The field test run was initially scheduled for fall 2008 with a runtime of 3 months. Due to some technical problems related with the linkage of the Internet Passport with the OpenID Identifier the schedule had to be shifted to the first 4 months of the year 09. The collection of the field test questionnaires was completed by mid June 09.

4.3.1 Test protocol and User actions in the field test

In the field test setup the test user had to follow a certain test protocol

- **Receive the test material from a local test agent**
  The test material consist of the packed AXS Internet Passport, a test user consent form, a customised user instruction for the field test and a questionnaire
- **Fill out and return the test user consent form**
  The consent form makes the user aware of the potential threats that could emerge from the use of a biometric system and is a waiver for the field test organisers
- **Establish an OpenID account**
  The user registers at Clavid to receive an OpenID identifier and gets his personal protected OpenID identity account
- **Personalize the AXS Internet Passport**
  The Web Site of Clavid supports the user in the fingerprint enrolment process when the user personalizes his AXS Internet Passport
- **Link the AXS Internet Passport with the OpenID identifier**
  The user defines in his protected OpenID account that she wants to use her AXS Internet Passport whenever she uses the OpenID issued by Clavid at any accepting site
- **Use his AXS Internet Passport for all OpenID authentications**
  The OpenID authentication consist then of the standard challenge response protocol for authentication that runs with the AXS Internet Passport. The user authenticated himself with the OpenID – AXS Internet Passport combination as often as possible at the Fidis web site and at any other web site that accepts the OpenID identifier
- **Report experience**
  The user had to complete the field test questionnaire and send it back, optional he or

she communicated further personal experience or comments directly or through the test agent to the field test organizer.

The test user can keep the personalized AXS Internet Passport with the recorded biometric fingerprint data. The security concept of the AXS Internet Passport does not allow the deletion of biometric data which are enclosed inside the passport. Any manipulation on the biometric data, including the deletion or alteration by the user, could create a threat for the identity of the user.

4.3.2 Raw data - usage statistics

All the 30 test users personalized their Internet Passports at the Clavid AXS initialisation service. Fig. 7 and 8 show the usage statistics of the AXS Internet Passports during the field test period 1.1.09 – 31.5.09.

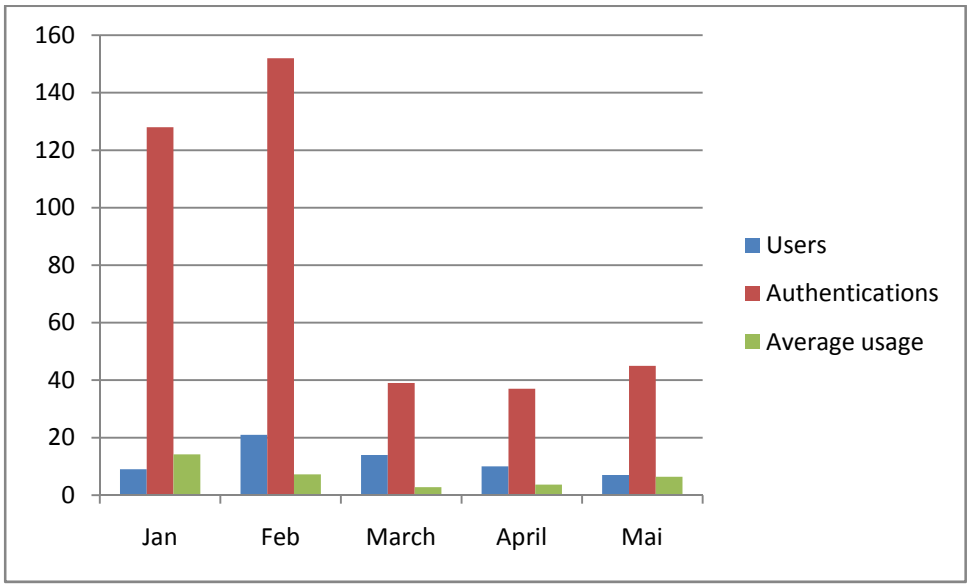


Figure 7: The usage statistics over the test period (not all test persons started test usage at the same time; each individual test period lasted 3 month; some of the users continued to use the AXS Internet Passport after the test)

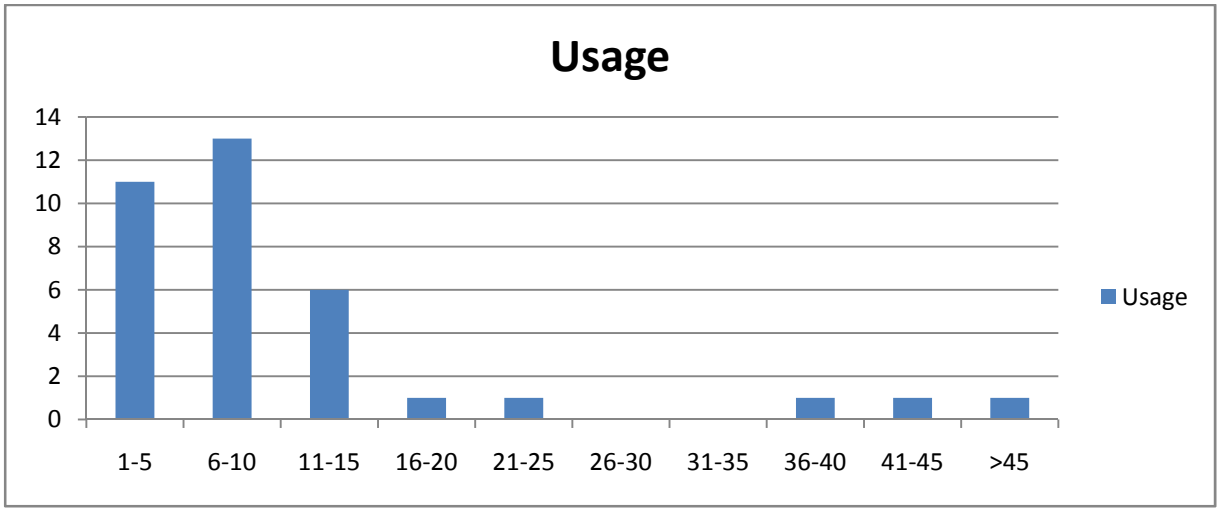


Figure 8: Individual usage statistics. The average usage per month was 6.6 authentications per person , but with large individual fluctuations and a diminution over time

Some of the test users started the field test later and some stopped it after the completion of the test protocol (which originally was configured for a 3 month test). Taking the effective test period into account the average usage over the full test period was 6.6 authentications/month. But there were quite large fluctuations, some test persons did not use their AXS Internet Passport anymore after the first month, some others continued to use it at a relative high frequency.

It stands out that many test persons used the AXS authentication with the OpenID mainly in the beginning of the test period. This is understandable as the test persons were interested by the novelty of the biometric recognition and the possibility of the OpenID identity management. Once this novelty effect had passed the number of authentications dropped to a level which actually is probably typical for the usage of the OpenID access to acceptor sites. After the first two months we observed approx. 2 authentications per person/per month. Part of this usage drop may also be explained by the fact that the test setup explicitly requested the usage of the OpenID Identifier for the access to the Fidis internal web site. No other suggestion was made and most of the test persons will not access the Fidis internal website at a very high frequency.

4.3.3 Raw data – questionnaires and user comments

During the field test the users completed a questionnaire that was developed to clarify the user attitude towards biometrics and privacy and to collect the feedback on usability and ergonomics of the AXS Internet Passport. The questionnaire included the following sections:

- **Test participant profile**
  with general information about age, gender, technology affinity and usage environment
- **Attitude towards biometrics and privacy protection**
  with questions that reveal the basic attitude of the user to the usage of biometrics and the protection of privacy
- **First impressions**
  with questions to be filled out right after the reception of the AXS Internet Passport

- **Getting started**
  with questions about the initial user experience and the personalization process
- **Using the card**
  with questions about the ergonomics and the understanding of the usage procedures especially of the biometrics in the daily applications
- **Documentation**
  with questions about the user behaviour relative to written or shown usage guidance

The detailed list of questions in the questionnaire is presented in the annex. The return rate of the questionnaires was 69 %, with responses from participants of all countries

5 Evaluation of field test results

The 22 participants of the field test that returned the questionnaire represented a good mix of persons

- All countries of the field test participants were represented
- More than a third of the responding persons were females
- The age mixture showed a ratio between younger (below 40 - 72 %) and older (above 40 – 28 %) persons that is close to a typical value for Internet users[20]
- About half of the sample persons indicated that they have an IT background.[21]
- A third had already some usage experience with fingerprint biometrics

Although the small sample does not allow a profound quantitative analysis of the user behaviour and acceptance, some significant qualitative patterns can be clearly identified.

5.1 Attitude towards biometrics and privacy in the Internet

Privacy and identity theft were indicated as the main worries on the Internet.[22] Almost all participants, except one, indicated that privacy was of high or at least relevant importance in identity management systems. Identity theft and profiling were mentioned as the major privacy risks. It is noteworthy that security (in the sense of data protection) was not perceived as a major privacy risk of identity management systems (rather identity theft and profiling).

As to biometrics, there was equally a mix of persons who had some previous experience with biometrics (8 persons) while others did not (13 persons). A large majority, with the exception of 3 persons, considered data protection important for biometrics. At the same time, the awareness of data protection legislation ranged from high (6 participants) to low (9 participants) while the remaining persons could not give an opinion on that or had no awareness at all. Profiling and identity abuse were mentioned as one of the main privacy risks of biometrics.

As to the expectations on biometrics, 13 participants referred to security, while 16 participants mentioned convenience (several aspects could be named). Only 2 persons had no expectations at all and 5 persons mentioned different aspects.

The fact that convenience from biometrics is higher rated than security or privacy was surprising for the field test organizers but it is in accordance with the experience made with first deployments of the AXS-AS in commercial environments. For some test users convenience is even attractive to trade against privacy. While 11 participants stated that they would not give up privacy for convenience, 8 indicated that they might sometimes and 3 agreed therewith.

Biometrics only is considered for about a third of the test sample (6) a valuable option for authentication in any situation; another third (7) does not consider biometrics as a valuable authentication method. The remaining persons make it dependent from the application.

---

[20] Combining the percentage of users for a certain age group with the age pyramid shows that in western countries typically 30 % of the Internet users are over 40 years old (see http://tips.vlaurie.co/2009/02/02/age-distribution-of-american-online-users and http://www.nationmaster.com/country/us/Age_distribution)

[21] *12 indicated that they had an IT background while 7 stated no on this point and 3 were unknown.*

[22] 11 indicated privacy as worries, while 9 mentioned ID theft.

5.2 Findings about usability, convenience and ergonomics

The questions related to the user experience were grouped (see 4.3.3) in four sections covering the lifecycle of the AXS Internet Passport in the hand of the users during the field test plus questions about the finger usage preference.

Delivery and first contact

The feedback on the delivery and the first contact with the biometric card was largely positive; only one person had a negative impression. But beside some minor issues concerning the packaging there was a substantial group (6) which did not understand the purpose of the PIMA token. It is also striking that half of the test persons did not consult the user guide upon reception of the card.

Personalisation and registration at the OpenID provider

The personalization act included the enrolment of 3 fingers and the entry of a 6 digit PIN code. For each fingerprint the user had to enter 3 good quality reference templates sweeping over the fingerprint sensor. For the PIN capture the user had to enter twice the same number using the fingerprint sensor to navigate over of virtual keypad which is shown on the graphical display of the card. Both action request a certain ability to use the fingerprint sensor in the correct way (slight pressure, continuous movements). It turned out that this basic motor skill was one of the biggest ergonomic hurdle. The difficulty was emphasised by the fact that the first time the sensors were used the device requested already a high quality fingerprint capture. Although the problem was expected and training material has been provided in form of pictures, videos and explanations two thirds of the users had problems to enter the reference templates of the fingerprints and still over half of the test persons did not understand how to do so or had difficulties to enter the PIN codes[23]. Although many users had problems to complete the personalization in a first trial, all test persons finally succeeded to personalize the card but some of them needed multiple trials. One of these users returned the following comment:

"It takes a lot of time and effort to get the device to accept you as the user (i.e. the personalization process). Swiping fingers sounds easy but turned out to be quite a challenge. Funny enough, after personalizing the device I experienced no problems when swiping fingers to get access to the Fidis website. This really strikes me as odd. How can I have so much trouble entering my fingerprints and so little applying them? Now that this initial hurdle has been taken, it turns out to be an easy to use device."

The problem of the initial personalization of a personal device with biometrics is imminent as long as the personalization process occurs remotely in the field. Practical and economical constraints urge organisations that will deploy such devices to find solutions for a more convenient remote personalization. Technically it is possible to improve the reference template capture in a way that no higher quality of the captured data is requested for the first reference template registration which reduces the problem to some extent. Further technical and organisational measures to reduce the initial difficulties of the user are recommended.

[23] 15 users declared to have problems with the fingerprint reference template enrollment; 14 users had problems or did not understand immediately how to enter the PIN; only 8 users declared to personalize the PIMA without problems.

Once the personalisation has been completed the user had to link his AXS Internet Passport with the previously created OpenID identifier. This link was performed online on the OpenID account management site at Clavid. Also this step was not performed without difficulties[24]. The main problem was the long reading time over the optical interface necessary to complete the secure channel allocation to the OpenID provider within the AXS Internet Passport.

Usage experience

In general the usage of the card for the authentication of the delivered OpenID Identifier did not cause any basic problems. Most of the test persons understood the logic and processing protocol for the secure authentication process (Fig.6). There were however several critical statements concerning the higher process complexity for the user compared with a simple 1-factor authentication like Username/PW. Two statements from test user illustrate this retention:

"However, when comparing the time it takes me to log into a website using the passport and using a traditional username and password combination, the latter is far quicker."

"The login and authentication procedure is - unfortunately - still quite complex, especially when compared to its biggest competitor: username and password, thus probably limiting the actual adaption of the card as part of day-to-day authentication."

Part of this reluctance to adopt a strong authentication using the AXS Internet Passport comes from the use of the optical interface which in some cases had too long transmission times for the authentication message. The problem was greatly reduced for some replacement cards with improved optical interface compared to the first supplied cards. But there are principal objections against any additional processing for the authentication:

"My overall impression of the AXSionics authentication system is an unique roundabout way off getting access in a complex way to websites with a simple OpenID.

People request enhanced privacy and security but they are not willing to accept additional operational complexity for the day-to-day life. It is clear that this lack of acceptance is partly due to the fact that all sites which accept OpenID (inclusive the Fidis internal web site) do not protect a high financial value neither for the operator nor the user. The use of multifactor authentication should therefore be restricted to the access control to high value sites.

The AXS Internet Passport in principle allows choosing a staggered authentication level with 1-factor (card present only), 2-factor (card and biometrics) and 3-factor (card, biometrics and PIN). This adjustment feature was not used in the field test to force the test users as often as possible into a biometric authentication with a 2- or 3-factor protocol. In a productive environment the security level for the authentication should be adapted to the security needs of the accessed site. In most cases of access control to typical Internet sites (accessible by OpenID) a 1-factor authentication is largely sufficient. The card just returns the access code read over the optical interface without a biometric recognition of the actual user. The use of an additional hardware based token for the authentication process however will always reduce the convenience of a username/PW only authentication, at least as long as the UserID/PW is readily available for the user. As soon as a higher protection is also in the interest of the user

[24] 9 persons claimed that they did not succeed with the registration at the first time.

(e.g. protection of online e-banking transactions) the acceptance of additional steps in the authentication process will probably be higher.

Documentation

A quite well known fact came also out of the field test. People don't like to read manuals or instruction guides independent of how much didactical effort is put in their design. Most of the test persons declared that the User Guide and the additional test user instruction was helpful (16 useful; 3 not useful), but most of them only read it after they stocked somewhere in the initialisation process. Many users mentioned that the online instruction immediately present and accessible online on the site, where a specific action was requested, was helpful. In general the biggest usage problems with the AXS Internet Passport were related with the sweeping of the fingerprint over the sensor and the correct positioning of the card on the screen to read the flicker code. Both actions are difficult to explain but are very easily understood when an animation shows how to do it. For such kind of problems classical forms of documentation can not be helpful. Animated online clips would better fit the needs of the user.

Fingerprint preferences

The used fingers enrolled by the test persons (see annex) shows a very biased distribution towards the index and middle finger and reflects the typical preference for the right hand in the population. This result suggest that the choice of the finger for the authentication does not have a high entropy. It therefore makes little sense to include such a choice in a security concept, e.g. by adding a fingercode. Originally the AXS Internet Passport allowed such a fingercode and it was still present in the field test personalization scheme. It however was not used in the authentication for the just mentioned reason.

5.3 Privacy aspects encountered within the field test

An important aspect of the field test arrangement is as to whether the participants were convinced that they had more control over the biometric data that they provided. 13 of the participants were convinced on that point, while 9 were not. This fact shows that it is difficult to persuade persons through technical measures of a certain fact. Even the fact that it is physically impossible that the token discloses the fingerprint data to an outside instance was not sufficient to convince all persons that their biometric data are well protected.

Some also commented that (more detailed) information about the processing of the biometric data would preferably also be given (and repeated) during the (enrolment and) verification process. One aspect of a PIMA was not exploited explicitly in the field test. It concerns the possibility to use different pseudonyms that all retrieve to the same person. This potential to protect an individual from profiling attacks intrinsic by the user-side identity management approach was pointed out by one of the test persons:

"Only after logging into the clavid -site I found that I could create several personas. This is what would be helpful for someone who would like to manage his online presence, but it was never explained in any of the instructions that this could be done, or what the benefit of his would be. In other words: one of the biggest selling points of the AXS-AS solution is never pointed out to the inexperienced user."

In principle the concept of the AXS Internet Passport also allows completly anonymous authentication. This usage option was not available to the test persons but in view of the above user comment should be made available in future editions.

5.4 Recommendations based on the findings of the field test

The running experience and the result of the evaluation of the different feedbacks allow to convey the following recommendations for a PIMA based authentication system with encapsulated biometric and with the divided control scheme:

- The usability and ergonomics of the personalization and authentication process is preponderant over all other aspects
- The lack of usage experience and the request for high quality reference templates rise a critical initial threshold for the personalization process, which can lead to a high user frustration. An initialization scheme with distributed MIMA in the field has to take this danger into account. The initial usage threshold should be reduced as far as possible.
- Although people rate privacy and security very high they are unwilling to accept any additional inconvenience compared to the simplest authentication methods. Biometric authentication should therefore only be used in specific situation where the user has a high consciousness of the potential security threats. The applied authentication process in a PIMA should be customisable to the specific application.
- Biometrics is well accepted as soon as the initial usage difficulties are mastered. Biometrics even can add to the ergonomics as one has not to memorize cumbersome passcodes. There remains however a reluctance concerning biometric data. Irrational fears about the loss of biometric data are forwarded even by persons with a high level of technical understanding. A transparent and reliable communication about the usage of biometric data should be provided by the editor of a PIMA device.
- Classical approaches for the user information like user guides or manuals deliver not the necessary information for the operation of a biometric system. The user has to learn a specific motion sequence and adopt the right motor skills to deliver a biometric template capture. This is best learned in an interactive way with the biometric system itself with corrective user feedback in combination with animations that show how the right movements look like.
- The usage of pseudonyms in the Internet that all are securely linked to the same person could provide a higher level of privacy and protection against identity fraud. In such a scheme that is supported by a PIMA the user has not to reveal any other information than the fact that behind a certain pseudonym stands always the same real person. This setting would come close to the real world situation where people are accustomed (e.g. in a warehouse) to interact with other persons without revealing their identity. The possibility to link identity secured pseudonyms to a personal card like the AXS Internet Passport should be exploited and made available to all users.
- During the full field test no false acceptance has been communicated. It seems likely that the biometric performance in a personal biometric system has to be tuned for a minimal false rejection rate. The probability of a false acceptance is greatly reduced by the typical operational setting of a PIMA where only one person has access to the biometric device. The FAR has just to be small enough that a finder of a lost or stolen token is refused at a sufficiently high probability.

The overall results of the field test are helpful for the design and optimisation of biometric PIMA. Some of the findings have already been implemented in replacement tokens during the second part of the field test and showed the improvement potential.

6 Conclusions

The deliverable D3.14 allowed to test and to verify the previously elaborated [Fidis310] and propagated concept of divided control over an encapsulated biometric authentication system. The concept was realised in a PIMA, the AXS Internet Passport, with a user centric on-board identity management [Prime]. The concrete application was the securing of a self defined OpenID Identifier with the strong authentication of the AXS Internet Passport. For this the OpenID identifier for each test user had to be defined at the Swiss OpenID provider Clavid that installed the option to link the AXS Internet Passport with the OpenID identifier established through his service. The technical realisation of this link, the preparation of the user interface, the definition of the ergonomic workflow and the preparation of the user instruction material lasted longer than originally foreseen. Also the production and the operational preparation of the test cards took more time than originally scheduled. Therefore the field test had to be rescheduled from fall 2008 to spring 2009.

The field test involved 30 test persons and 5 supporting agents each using the PIMA at least during a 3 months period to the begin of the year 2009. The test user were urged to use the OpenID identifier secured by the AXS Internet Passport for all sites that accept OpenID authentication even if such sites often do not protect content with a high financial value (typical sites are the Fidis internal homepage, social network sites, online info systems with registration etc). The intent was to gain as much as possible practical experience with the frequent usage of biometrics for authentication purposes.

The preparation of the field test also included a rigorous assessment of the legal situation for systems and organisations that process biometric data. This work resulted in a set of accompanying legal documents for the organisers, the processing institutions and the involved test persons. The legal situation is quite heterogeneous within the European Community and therefore the field test was restricted to test users in four countries where the legal situation was manageable with limited costs (Belgium, Netherlands, Germany, Switzerland).

With an anonymous questionnaire addressing the attitude of the test users towards privacy, biometrics and their ergonomic experience with the test setup the users gave their feedback to the field test organizers. The evaluation of the 22 returned questionnaires and of the spontaneous feedback from the users showed that greatest care has to be applied to the usability and the ergonomics of a biometric system that is distributed in the field. In theory people rate privacy and security high, but in the daily practice ergonomic and convenience aspects prevail. This contradiction between behaviour and claim can also be observed on a much wider scale in the privacy neglecting usage of social network sites by most persons. A deployment of secure biometric authentication systems has to take this attitude into account and therefore the use of biometric in the authentication process should be sparse and restricted only to situations where a high security consciousness is already available by the application circumstances (eg. financial transactions, health information etc).

In the ideal case the applied authentication protocols is dynamically adaptable to the concrete value protection situation. For the access to a social network site a 1-factor authentication is sufficient, but for the access to the private bank account the user will accept a 2- or 3-factor authentication with biometrics. This means that the PIMA needs a sufficient flexibility and intrinsic intelligence to adapt to this customisation need for the different sites that are accessed within a user centric federation scheme. The AXS Internet Passport allows the

definition of the authentication level for each individual authentication process. This feature should be used to meet the expectations on convenience of the user.

The question of the economics of a biometric system integrated in a PIMA according the divided control model could not be addressed within the settings of the field test. Market evaluations in other contexts done by AXSionics however show that the market is very sensitive on the price of security solutions. Biometric authentication is only accepted if it has only a marginal impact on the total cost of ownership for an organization that deploys such a system. Exceptions are organizations that operate in domains with extremely high security request mainly in the field of national defense.

With these findings the original goals of the field test have been achieved[25]. The recommendations for the use of biometrics made in previous deliverables based on principal considerations about privacy protection, security and legal constraints have to be completed with a recommendation that usability and convenience are at least equally important in practice. The divided control model and the encapsulation of biometrics within a PIMA remains still the preferred implementation for non forensic biometric authentication applications. An individual device that is often used by the same user in different situations is better adapted to the convenience needs than a centralised biometric authentication scheme with very limited possibilities for an individualised customisation. The usage learning process seems to be very important for the acceptance by the user and such a learning can best be achieved on a personal frequently used system.

[25] The economic aspect was not directly covered by the field test

7 Bibliography

[AXS] Authentication and transaction security in E-business; L. Müller., Proc. Of the 3rd IFIP WG; Karlstad, S.Fischer et al (eds); Springer, 2007; p.175

[Clavid] Clavid ag, Zug, Switzerland; http://www.clavid.com

[Fidis31] Structured Overview on Prototypes and Concepts of Identity Management Systems, M. Bauer, M. Meints; D3.1 Fidis WP3; 2005

[Fidis32] A study on PKI and biometrics, M. Gasson, M. Meints, K. Warwick; D3.2 Fidis WP3, 2005

[Fidis310] Biometrics in identity management, E. Kindt, L. Müller; D3.10 Fidis WP3, 2008

[Future] The Future of Identity in the Information Society; Challenges and Opportunities; K. Rannenberg et al., Dordrecht, Springer, 2009

[OpenID] An introduction in the OpenID standard can be found on the online encylopedia Wikipedia: http://en.wikipedia.org/wiki/OpenID

[Prime] PRIME - Privacy and Identity Management for Europe, European Research project on solutions for privacy enhancing identity management; see also https://www.prime-project.eu/about;

[Westin] Privacy and Freedom, A. Westin; New York, Atheneum, 1967

Annex 1: Returned questionnaires

The following questionnaire was the main feedback vector for the test persons to communicate their experience and opinion to the field test organizers:

Questionnaire for the field test of Fidis Deliverable 3.14

The questionnaire was elaborated by the participating Fidis partners in view of their interest about the collected feedback from the users. The full questionnaire is printed below:

****

Questionnaire for the field test of Fidis Deliverable 3.14

Your honest and constructive answers provide the editors of the D3.14 report with real end user feedback for a system that has been described in the Fidis report D3.10 as a model for best practice applying biometrics for authentication purposes.

It will also help the Fidis partner AXSionics to improve the quality of its products and services.

Your answers will be treated strictly confidential. The participation in the field test is compliant with the data protection laws of the concerned countries.

The questionnaire should be completed in the first half of the field test period and sent back to the test agent (the one which gave you the *AXSionics Internet Passport* **and the questionnaire) before**

End of February 2009

In the second half of the field test period you will get a second *AXSionics Internet Passport* **with a modified user interface for testing[26].**

Thank you for participating in this project.

The editors

Lorenz Müller (AXSionics AG), Els Kindt (KU Leuven)

[26] This second passport will be delivered to a selected sample of test persons in Sept 2009. The results of this continuation can not be covered in this report.

0. User and system information

Please note:

- Complete the following section before you start unpacking and using your AXSionics Internet Passport.
- Please write legibly and use print letters. Thank you.

Test participant information Please tell us a little about yourself			
Country:		**Sex:**	o Female o Male
Age:	o less than 40 o over 40	**Internet:**	o frequent user o rare user
Profession:	o with technical or IT background o with no technical background		
System information Please tell us about the computer system you use			
System:	o Laptop o Desktop	**Monitor type:**	o LCD o CRT o Plasma
Monitor dimension:	Diagonal in inches or cm. Example: 19"	**Monitor resolution:**	In pixels. Example: 1024 x 768
Web browser:	o Firefox o Internet Explorer o Opera o Safari o Other (name it):		
Have you used fingerprint sensors before?	o No o Yes		
If Yes, what type of sensor and where?	o Touch o Swipe Where (name it):		

1. General questions about attitude to identity, privacy protection and biometrics

My opinion Your attitude, your expectations and your concerns are valuable inputs to evaluate the field test results	
1.1 What do you expect from using biometrics?	Expected type of answer
1.2 What are your main worries about making yourself known on the internet?	
Privacy Your attitude, your expectations and your concerns are valuable inputs to evaluate the field test results	
1.3 How important is the protection of your privacy in identity management systems?	Comment freely. Also, report any problems you may have experienced.
1.4 What is in your opinion the major privacy risk of identity management systems?	Comment freely. Also, report any problems you may have experienced.
1.5 Is giving up privacy an option for more convenience?	Expected type of answer
1.6 Are you aware of the details	Expected type of answer

of data protection legislation?	
Biometrics Your attitude, your expectations and your concerns are valuable inputs to evaluate the field test results	
1.7 Have you used biometric applications before?	Comment freely. Also, report any problems you may have experienced.
1.8 What do you think are the main privacy risks of biometrics?	Comment freely. Also, report any problems you may have experienced.
1.9 How do you valuate the importance of the protection of your biometric data?	Comment freely. Also, report any problems you may have experienced.
1.10 Would you be prepared to use your biometric without an additional factor such as a pin code?.	

2. First impression

Please complete this section **as soon as possible** after you unpacked your AXS Internet Passport (also referenced as the card).

Receiving the AXSionics Internet Passport Please tell us about your first impression of the card	
2.1 What was your first impression of the card when you received the box?	Please use 3-6 descriptive key words
2.2 Was it easy to open the box?	Comment freely. Also, report any problems you may have experienced.
2.3 Was it easy to get the content out of the box? Did something fall out unexpectedly?	Comment freely. Also, report any problems you may have experienced.
2.4 Did you easily find all the content of the box? Did you miss anything in particular?	Comment freely. Also, report any problems you may have experienced.
2.5 Did the card fulfill your expectations? What could be improved, and how?	Comment freely. Also, report any problems you may have experienced.
Getting started and proceeding Please tell us how clear the next steps to take were after opening and unpacking the box	
2.6 Was it clear what to do next after unpacking the content?	Comment freely. Also, report any problems you may have experienced.
2.7 Was the quick guide helpful in explaining the next steps?	Comment freely. Also, report any problems you may have experienced.
2.8 Was the purpose of the card clear?	Comment freely. If NO, please explain why not. Where would you look for this information?

2.9 Did you easily find the address of the web page that you needed to call to get started?	Comment freely. If NO, please explain why not.
2.10 Did you read or consult the quick guide *before* you powered ON the card?	Comment freely. If NO, please explain why not.
2.11 Did you read or consult the quick guide *after* you powered ON the card?	Comment freely. If YES, please explain why.

3. Initialisation

Please complete this section **as soon as possible** after the personalization and registration step.

Personalization (making the connection between you and the card) Please tell us about your experience during the personalization process	
3.1 Was the purpose of the personalization process clear?	Comment freely. If NO, please explain why not.
3.2 Did you easily find the serial number of your card?	Comment freely. If NO, please explain why not.
3.3 Was it clear how to enter the serial number into the web page form?	Comment freely. If NO, please explain why not.
3.4 Was the purpose or the concept of the finger code well described?	Comment freely. If NO, please explain why not. Where would you look for this information? **This question was not evaluated, because the concept was not applied**
3.5 Were you able to enter the finger code into the web form without any problems?	Comment freely. If NO, please explain why not. **This question was not evaluated, because the concept was not applied**
3.6 Was the purpose of the flickering clear?	Comment freely. If NO, please explain why not.
3.7 Was it clear how to scan in the flickering from the computer monitor?	Comment freely. If NO, please explain why not.
3.8 Was the purpose or the concept of the PIN code well described?	Comment freely. If NO, please explain why not. Where would you look for this information?
3.9 Were you able to enter the PIN code on the card without any problems?	Comment freely. If NO, please explain why not.
3.10 Was the purpose of the response code displayed on the card clear?	Comment freely. If NO, please explain why not. Where would you look for this information? **This question was not evaluated, everybody understood the concept**
3.11 Was the response code displayed on the card easy to read?	Comment freely. If NO, please explain why not. **This question was not evaluated**

3.12 Were you able to complete the personalization process without any problems?	Comment freely. If NO, please explain why not.
3.13 Did the card accept your fingerprints easily during the enrollment?	Comment freely. If NO, please mention the amount of trials until the successful entry of the reference templates..
3.14 Are you convinced that your biometric data remains under your full control?	Comment freely. If NO, please explain why not.
Registration (making a connection between the card and the online service) Please tell us about your experience during the registration process	
3.15 Was the purpose of the registration process clear?	Comment freely. If NO, please explain why not.
3.16 Did you understand the concept of the finger code?	Comment freely. If NO, please explain why not. **This question was not evaluated, because the concept was not applied**
3.17 Were you able to complete the registration process without any problems?	Comment freely. If NO, please explain why not.

4. Using the card

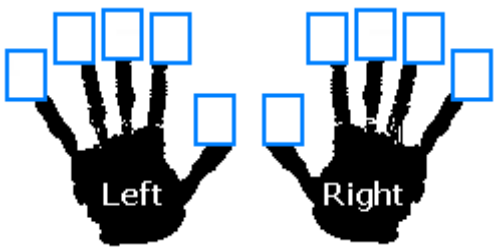
Please complete this section **some days after you started using your AXS-Card** (typically after 10 authentications with the card).

Authentication (you using the card with an online service, e.g. Fidis internal) Please tell us about your experience during the authentication process	
4.1 Was the purpose of the authentication process clear?	Comment freely. If NO, please explain why not.
4.2 Were you able to complete the authentication process without any problems?	Comment freely. If NO, please explain why not.
Optical interface (scanning in a flickering from the computer monitor) Please tell us about your experiences when scanning in a flickering	
4.3 Was the flickering acceptable to your eye?	Comment freely. If NO, please explain why not.
4.4 Was it clear how to position the card on the monitor to successfully scan the flickering?	Comment freely. If NO, please explain why not.
4.5 What is your perception of the time it took to scan in one flickering?	Comment freely.

4.6 Was the content of the *quick guide* helpful in explaining how to scan in a flickering?	Comment freely. If NO, please explain why not.
4.7 Was the information on the *web pages* helpful in explaining how to scan in a flickering?	Comment freely. If NO, please explain why not.
4.8 In general, what did you have most difficulties with when scanning in a flickering?	Comment freely.
Fingerprint sensor (sweeping a finger) Please tell us about your experiences you had when swiping a finger	
4.9 Was the fingerprint sensor pleasant to use? Did it feel "natural" to use it?	Comment freely. If NO, please explain why not.
4.10 Was it clear where to position the card in order to best swipe a finger?	Comment freely. If NO, please explain why not.
4.11 Was the content of the *quick guide* helpful in explaining how to swipe a finger?	Comment freely. If NO, please explain why not.
4.12 Was the information on the *web pages* helpful in explaining how to swipe a finger?	Comment freely. If NO, please explain why not.
4.13 Did you activate the fingerprint viewer application on the card to train swiping a finger?	Comment freely. If NO, please explain why not.
4.14 In general, what did you have most difficulties with when swiping a finger?	Comment freely.
Fingerprint sensor (entering a PIN code) Please tell us about your experiences you had when entering a PIN code	
4.15 Was the content of the *quick guide* helpful in explaining how to enter a PIN code?	Comment freely. If NO, please explain why not.
4.16 Was the information on the *web pages* helpful in explaining how to enter a PIN code?	Comment freely. If NO, please explain why not.
4.17 Did you activate the Pong game on the card to train navigating with the fingerprint sensor?	Comment freely. If NO, please explain why not.
4.18 In general, what did you have most difficulties with when entering a PIN code?	Comment freely.

5. Documentation

Please complete this section **as soon as possible** after you started using your AXS-Card.

Quick guide Please tell us your opinion about the quick guide	
5.1 Did you carefully read the entire quick guide?	Comment freely. If NO, please explain why not.
5.2 Was the content of the quick clear and concise?	Comment freely. If NO, please explain why not.
5.3 Did the quick guide explain well how to scan in a flickering or how to enter a finger print correctly?	Comment freely. If NO, please explain why not.
5.4 Was the content of the quick guide helpful in solving any problems you may have had?	Comment freely. If NO, please explain why not.
5.5 What could be improved in terms of presentation, layout, content organization, etc.?	Comment freely.
Web pages (information guiding you through the different steps) Please tell us your opinion about the information on the web pages guiding you through the process of activating the card	
5.6 Did you carefully read the instructions on the web pages?	Comment freely. If NO, please explain why not.
5.7 Was the content of the web pages clear and concise?	Comment freely. If NO, please explain why not.
5.8 Did the web pages explain well how to scan in a flickering or how to enter a finger print?	Comment freely. If NO, please explain why not.
5.9 Was the content of the web pages helpful completing the tasks?	Comment freely. If NO, please explain why not.
5.10 What could be improved in terms of presentation, layout, content organization, etc.?	Comment freely.
User behavior (for our statistics) Please tell us about your [unconscious] preferences	
5.11 What is the hand you preferably use?	o Left o Right
5.12 Please indicate the fingers you used to personalize your card and the order you entered them by writing a number (1 for the first finger, 2 for the second, etc.) in the box above the corresponding finger. Do not mention your personal finger code.	

Compiled answers from 22 test users

In total 34 test users (DE 7, BE 6, NL 5, CH 2, unknown 2) participated in the field test and 22 of them returned the questionnaire. The results of the questionnaires have been compiled and are presented in the following table. For the evaluation occasionally several answer fields with related context questions have been combined. The numbers in the evaluation table rely to these questions in the above listed questionnaire.

Questionnaire Evaluation Results							
0. Personal questions							
	CH	DE	BE	NL			
Country	4	7	6	5			
	F	M					
Sex	8	14					
	< 40	>40					
Age	16	6					
	Yes	No	Uknown				
IT Background	12	7	3				
	Yes	No	Uknown				
FP sensor experience	8	13	1				
1. General Questions							
	Security	Convenience	Other	None	Privacy	Reliability	
Expectation on biometrics (1.1)	13	16	5	2	1	1	
	Fraud	Privacy	ID theft	Other	Profiling	Abuse	None
Worries on the Internet (1.2)	5	11	9	4	3	1	1
	High	Medium	Low				

Importance of privacy in IMS (1.3)	19	2	1				
	Profileing	Identity theft	Others	Security	Revocability		
Major privacy risk of IMS (1.4)	12	11	4	1	1		
	Yes	No	Sometimes				
Privacy vs convienience (1.5)	3	11	8				
	High	Low	Unknown	No			
Awareness of data protection legislation (1.6)	6	9	4	1			
	Yes	No					
Previous experience with biometrics (1.7)	8	14					
	Dissemination	Abuse	Profiling	Other	Revocability	Theft	Fraud
Main privacy risks of biometrics (1.8)	3	6	5	4	6	3	2
	High	Low					
Importance of biometric data protection (1.9)	19	3					
	Yes	No	Depends	Uknown			
Biometric only for authentication (1.10)	6	7	8	1			
2. First Impression							
	Positiv	Negativ	Unclear				
Reception of card, fullfil expectations (2.1; 2.5)	18	1	3				
	Easy	Difficult	Easy but cable difficult to find		Unclear		
Unpacking (2.2; 2.3; 2.4)	8	1	12		1		
	Clear	Not clear	Help from QG	Help from UI			
Next steps (2.6; 2.7; 2.9)	20	2	9	2			

	Consulted	Not consulted	Consulted after power on
Usefulness of Quick Guide (2.10; 2.11)	11	4	7
	Clear	Not clear	
Purpose of card clear (2.8)	16	6	
3. Initialisation			
	Clear	Not clear	
Purpose of personalization process (3.1)	20	2	
	Clear	Not clear	Clear with issues
Finding and entry of serial number (3.2; 3.3)	19	1	2
	Clear	Not clear	Clear with issues
Purpose and read flickering (3.6; 3.7)	9	7	6
	Clear	Not clear	Entry problem
Purpose and entry of PIN code (3.8; 3.9)	8	12	2
	Yes	No	
Personalization without problems (3.12)	8	14	
	Easy	Difficult	
Fingerprint enrollment (3.13)	7	15	
	Convinced	Not convinced	
Control of biometric data (3.14)	13	9	
	Clear	Not clear	
Purpose of registration (3.15)	18	4	
	Yes	No	
Success of registration (3.17)	13	9	
4. Using the card			

	Clear	Not clear		
Purpose of authentication (4.1)	21	1		
	Yes	No		
Sucess of authentication (4.2)	15	7		
	Yes	No		
Acceptance of flickering (4.3)	21	1		
	Clear	Not clear		
Optical interface -Scan the flickering (4.4; 4.6; 4.7; 4.8)	18	4		
	Acceptable	Too long	Requires exercise	
Temporal ergonomics of flickering (4.5)	15	5	2	Responses range from extremely slow to very fast
	Clear	Not clear		
Fingerprint reading (4.9; 4.10; 4.11; 4.12; 4.13; 4.14)	18	4		
	Clear	Not clear		
Entry of PIN code (4.15; 4.16; 4.17; 4.18)	21	1		
5. Documentation				
	Useful	Not useful	Not used	
Quick Guide (5.1; 5.2; 5.3; 5.4; 5.5)	16	3	3	QG does not really help for fingerprint entry problems
	Useful	Not useful	Not used	
Web instruction (5.6; 5.7; 5.8; 5.9; 5.10)	16	2	4	

Fingerprint preference	Small finger	ring finger	middle finger	index	thumb
Left			3	9	1
Right	3	9	14	18	3

Annex 2: Usage statistic

Raw data of test user statistics with anonymized user identifiers is presented in the table below. In total 35 users (30 test persons, 5 test agents) participated in the field test. The test persons are enumerated by letters A-Z,a-i. The listed usage statistics shows the usage of each test person over the time period from January to Mai (left 3 columns) and the usage of the different users over the test period (right 3 columns) grouped from month to month:

Ordered according users			Ordered according month		
User	Month	responses	User	Month	responses
a	April	9	N	Jan	4
A	Mai	2	S	Jan	1
b	Jan	46	T	Jan	6
b	Feb	11	U	Jan	17
b	March	4	V	Jan	2
b	April	4	W	Jan	15
b	Mai	12	b	Jan	46
B	Feb	3	e	Jan	11
c	Mai	9	h	Jan	26
C	Feb	13	B	Feb	3
C	April	1	C	Feb	13
d	Feb	5	D	Feb	6
d	March	1	F	Feb	10
D	Feb	6	G	Feb	8
e	Jan	11	J	Feb	7
E	April	1	K	Feb	3
f	Feb	12	L	Feb	6
f	April	1	M	Feb	1
F	Feb	10	N	Feb	3
F	March	1	O	Feb	15
g	Feb	9	P	Feb	12
G	Feb	8	Q	Feb	3
G	March	1	R	Feb	11
h	Jan	26	U	Feb	2
h	Feb	10	W	Feb	2
h	March	3	b	Feb	11
h	April	3	d	Feb	5

H	March	5	f	Feb	12
i	Mai	2	g	Feb	9
I	April	9	h	Feb	10
I	Mai	1	F	March	1
J	Feb	7	G	March	1
K	Feb	3	H	March	5
L	Feb	6	L	March	2
L	March	2	N	March	1
M	Feb	1	O	March	1
N	Jan	4	P	March	1
N	Feb	3	Q	March	6
N	March	1	W	March	1
O	Feb	15	X	March	5
O	March	1	Y	March	7
O	April	5	b	March	4
O	Mai	1	d	March	1
P	Feb	12	h	March	3
P	March	1	C	April	1
P	April	1	E	April	1
Q	Feb	3	I	April	9
Q	March	6	O	April	5
R	Feb	11	P	April	1
S	Jan	1	Z	April	3
T	Jan	6	a	April	9
U	Jan	17	b	April	4
U	Feb	2	f	April	1
V	Jan	2	h	April	3
W	Jan	15	A	Mai	2
W	Feb	2	I	Mai	1
W	March	1	O	Mai	1
W	Mai	18	W	Mai	18
X	March	5	b	Mai	12
Y	March	7	c	Mai	9
Z	April	3	i	Mai	2

Annex 3: Legal framework documents

To be compliant with general data protection rules of the countries concerned by the field test, two legal forms have been prepared.

One is a Test User Consent form for the test users to be signed if they agree before the field test in which they obtain detailed information and provide their free, specific and informed consent with the fact that biometric data are processed during the field test.

The second form is a Controller-Processor Agreement form. Individual agreements have been concluded between AXSionics, as the field test controller, and the organizations that process data of the field test on behalf of AXSionics for the purposes of the test. These organizations are the Fidis Web site operator and the OpenID identity provider, each of these two organizations signed such an agreement form. Through this form the organizations that contribute to the field test through data processing in any form declare their consent to process the data in accordance with the applicable data protection laws as a processor and only for purposes of the test.

Test User Consent form

The following form was signed by all test users:

****

Legal notice and consent form, including specific information, consent and agreement form for the field test of the AXS- card for deliverable D3.14

(This legal notice is to be submitted to the individual researchers of the Fidis partners– participants in the AXS -card demonstrator, who are interested to participate in the AXS-card field test, and, upon agreement, is to be returned duly signed in writing, to AXSionics, Neumarkstrasse 27, 2503 Biel, Switzerland, before the start of the field test).

Information about the use of the AXS-card for the Future of the Identity in the Information Society (FIDIS) field test and the processing of your personal data, including biometric data

You, being a research member of one of the FIDIS institutions of the FIDIS project (see www.fidis.net)**,** are hereby informed of the details of the field test for FIDIS Deliverable 3.14, involving a model implementation test of the AXS-card for a user controlled biometric authentication. You are fully free to participate in the test or not. *Only* in case you agree with the information and the consent drafted below, you are invited to sign and date this form for consent and agreement and to return it to AXSionics.

About the user controlled biometric authentication. The AXS-card has been developed by AXSionics Neumarktstrasse 27, CH – 2503 Biel, Switzerland. The AXS-card is designed to provide for increased security for accessing identity information in a specific identity management system that works in combination with the AXS-card (e.g., an OpenId account). The increased security is effectuated because for accessing the identity information, you need not only to possess the AXS-card, but it will also be verified (authenticated) whether the actual user is the owner of the card (and not a thief of the card). For this purpose, fingerprint of the user of the AXS-card will be verified against previously stored fingerprint information of the owner of the card. Hence, the AXS-card provides for a so-called ‘trusted authentication system with biometrics’. The fingerprint information of the user of the card will only be stored on the AXS-card (and nowhere else nor will it leave the card) and the user will decide when its fingerprint information will be processed and that it is for use of the card (user controlled

biometric authentication). A detailed description of the functional and technical requirements of the AXS-card as proof of concept of encapsulated biometrics is set forth in FIDIS deliverable D3.10, which can find on www.fidis.net.

About the use of the fingerprint (biometric characteristic). By swiping your fingerprint over the biometric sensor on the AXS-card, a feature vector derived from your fingerprint will be stored in template format on the card for later verifications. This is also called the enrolment phase. Each time you swipe your fingers over the sensor on the card in order to authenticate yourself, a feature vector derived from the fingerprint will temporarily be stored for comparison purposes**.** This is also called the verification phase. Data or information about your fingerprints will never leave the card. When developing the AXS-card, the privacy and identity protection recommendations as developed in FIDIS were applied as much as possible. Because fingerprint information could be used for various purposes, including identification and re-use for other purposes as initially meant, the fingerprint information is *only stored on the card* where it is under the control of the user. In addition, not an image of the fingerprint, but a representation of the characteristics of the fingerprint in a table form (feature vector) with relevant location specifications, a so-called *template*, is stored on the card, and this only for verification purposes. The use of a template should prevent that information relating to health or race that may be contained in the fingerprint image would become apparent. However, possible information relating to health or race in templates is still to be further researched and may therefore not be fully excluded with the use of such template. Although the field test does certainly not intend to process such information relating to health or race, your consent with the possible processing of such data will be requested. Furthermore, only the result of the fingerprint verification and comparison ('match'), whether the authentication has been proven successful or not, and no biometric data, will be communicated for access purposes to the OpenId identity provider and the management system hosted by the service provider. A detailed description of the specific privacy and identity recommendations for identity systems using a encapsulated biometric recognition system using fingerprints are set forth in FIDIS deliverable D3.10, available on www.fidis.net.

About the operational aspects of the field test. For testing the AXS-card, it will be required that the user generates an OpenID at the OpenId provider Clavid in Switzerland at www.clavid.com. In addition, the user will need to register its fingerprint information on the AXS-card and will need to register the AXS-card (only, not the fingerprint) with the generated OpenID at Clavid. Detailed instructions on (i) how to proceed to get an OpenID, and on (ii) getting started with the AXS-card are hereby provided in attachment. Subsequently, the user shall use its OpenID in combination with the AXS-card for the FIDIS login at the FIDIS internal webpages and for login at other service providers using OpenID. The user shall hereupon provide written feedback to AXSionics about the use of the card by way of answers in a questionnaire evaluating the instructions and useability of the AXS-card. More detailed instructions on (iii) the use of the AXS-card for accessing any application using OpenID as identity management application, as well as (iv) an example of the questionnaire can be found in attachment.

In order to minimize the data, the user does not need to mention name or any reference number on the questionnaire.

Security measures. By way of security measures implemented, the AXS-card is a tamper resistant token where the full processing and storage of the biometric data takes place under the control of you. The token hardware and its integrated functions are produced by AXSionics and no one can change these functions at reasonable costs. In this sense, the operational functionalities are controlled by AXSionics and not by a third party. You, as user of the card decides if you want to use the card. You control the physical device with the stored biometric data, which is an autonomous personal token with sufficient computing, electrical power and hardware resources to perform the full biometric processing in the token. The AXS-card provides cryptographically secure communication channels with the central authentication system, for this field text with Clavid. Only digital identity credentials without any biometric information can leave the token to confirm a successful verification of the

identity claim of the user. The whole implementation is protected in a tamper resistant processor on the token. Such an implementation reduces to a great extent the threats to a biometric system.

About the use of the AXS-card and the data processed

If your are interested and willing to deploy the AXS-card enabling biometric authentication for accessing the Fidis internal webpages site and other sites, operating OpenID, for test purposes and in the framework of FIDIS deliverable D3.14, you are invited to indicate that you would like to receive an AXS-card.

You are the full and only possessor of the AXS-Card that you will receive and that you should at all times keep under your only control. The AXS-card will store your fingerprint template for later verification and authentication purposes when accessing an OpenID application. Upon communication between the card and the application server, only the fact that the card has recognized its user will be sent by the card to the application server. Traffic data, which is data processed for the authentication and the conveyance of the communication, including IP number and the date and time of the communications, between the AXS-card, the identity provider Clavid and the service providers using OpenId will also be processed. Never give the card to someone else. At the end of the field test, the AXS-card will become yours upon your choice, and will not have to be retuned to AXSionics.

The site which operates the interface with the AXSionics AXS-card for OpenId applications, Clavid**,** Baarerstrasse 2, 6300 Zug, Switzerland, will be a processor in the field test. Clavid will collect and process information on behalf and upon further instructions of AXSioncis about the use of a given AXS-card, such as the number of authentication attempts including time and IP number, and the authentication results transmitted by the card. This information will be communicated to AXSionics alone and not to third parties. Furthermore, this information will be processed likely in combination with the registered data provided by you in connection with OpenId, which includes a reference to your chosen name or pseudonym, your e-mail address, part of your AXS-cardnumber and an OpenId identifier. The participating Fidis partner being operator of the Fidis internal Web site, Mobile Business & Multilateral Security chair, Güneburgplatz 1, 60629 Frankfurt/Main, Germany, will also be a processor in the field test, and will collect and process information on behalf and upon further instructions of AXSioncis about the use of a given AXS-card, such as the number of authorized accesses and attempts accessing the internal webpages with OpenID, including time and IP number of the attempts and an OpenId identifier.

About the questionnaires relating to the use of the AXS-card

AXSionics will invite users of the AXS-card to complete a questionnaire (see above). Any and all information collected by AXSionics through the questionnaires distributed amongst the users of the AXS card and returned by the Fidis partner will be on a no name basis and the information provided should in principle not be linkable to a particular user.

Free, Specific, and informed consent. I understand and agree by signing below that the above described categories of personal data, in particular (a) fingerprint (s) in the form of a template exclusively stored on the AXS-card under my control for verification and authentication purposes, and (b) personal data, including traffic data such as IP number and time and date of communications and data relating to (un)successful user controlled biometric authorization with the AXS-card and processed by the OpenId identity provider Clavid, in combination with OpenID registration and account information, which includes a reference to my chosen name or pseudonym, my e-mail address, part of my AXS-cardnumber and an OpenId identifier, and (c) data, including traffic data such as IP number and time and date of communications and data relating to access (attempts) to OpenID applications of service providers, including the FIDIS internal webpages, and (d) completed written answers to the questionnaire about the use of the card sent to AXSionics, will be processed by AXSionics, the controller, with registered address in Switzerland, Neumarktstrasse 27, 2503 Biel, solely for test and research purposes, in particular for the evaluation of the proof of concept and the field demonstrator of the AXS-card as user controlled biometric authentication as part of FIDIS

research and as described above and the evaluation of ergonomics and acceptance of the test users (market analysis)**.** These personal data, including the traffic data, will only be processed for the duration of the test of the AXS-card in the framework of the Fidis project, that will end by [date].

The representative of AXSionicis in [country], is [organization] (Contact person: [person], at [Email]).

The identity provider Clavid, and the Fidis partner being operator of the Fidis internal Web site, Mobile Business & Multilateral Security chair, Güneburgplatz 1, 60629 Frankfurt/Main, Germany, will be processors of the data and will process that data only on behalf and according to the instructions of AXSionics.

I further understand and agree that, to the extent biometric fingerprint data could reveal information concerning health or race, such data exclusively and securely stored on the AXS-card which I shall hold all times under my control and any other data provided as answer in the questionnaires, which could reveal information relating to health, will be processed, without supervision of a professional of the art of healing, but exclusively for the same testing and researching of the biometric authentication process, system and usability of the AXS-card. By signing this consent, I expressly agree with the processing of such data concerning health or race and which may be contained in a fingerprint template, but which will never leave the AXS-card.

I am informed and take note that I have access to my personal data and the right of correction. For such purpose, I can contact the representative of AXSionics in Belgium, ICRI, and its contact person mentioned above, or if I would prefer, AXSionics represented by Dr. Lorenz Müller lorenz.mueller@axsionics.ch. I can also delete at all times my biometric data from the card. After the end of the field test, I agree to either return the AXS-card to AXSionics or, in case I decide to keep the card, that the use of the AXS-card is my sole responsibility.

I understand and agree that personal data relating to the authentication and access (attempts), but excluding any and all biometric data which is exclusively and securely stored on the AXS-card, may also be sent to third countries, outside the European Union, in particular (only for participants outside Switzerland), Switzerland, where AXSionics is registered, as well as where the identity provider, Clavid, is registered but which provides an adequate level of protection.

In using the AXS-card for connecting to service providers of my choice using OpenID, personal data relating to the authentication and access (attempts), including traffic data and data relating to my OpenID account information, as mentioned above, but excluding any and all biometric data, may also be sent to these service providers (internet sites). The processing of such data falls outside the control of AXSionics and solely these service providers (internet sites) are responsible for the processing of these data and for which they become controller. I understand and agree that such service providers and internet sites using an OpenID access control application, may also be established in countries which do not provide for an adequate level of protection, for example in the United States. I understand however that I am able to choose such internet sites using OpenId that I want to access at my own risk and I agree with any transfer of my data relating to the authentication and access (attempts) using the AXS-card to such sites and countries that I would choose and which may not provide an adequate level of protection.

For consent and approval :

Name, Date, Signature :

Annexes :

1. Detailed instructions on (i) how to proceed to get an OpenID, and on (ii) getting started with the AXS-card;

2. Detailed instructions on (iii) the use of the AXS-card for accessing any application using OpenID as identity management application, as well as (iv) an example of the questionnaire.

Controller-Processor Agreement form

The following generic form was adapted to the data processing organisations of the field test. It was signed by Clavid, as provider of the OpenID identifiers, and by JWG University, as provider of the access through OpenID to the internal Fidis Web site. AXSionics, as controller of the field test was the agreement partner.

**********:

Agreement

Between :

AXSionics AG, Neumarkstrasse 27, 2503 Biel, Switzerland, duly represented by Dr. Lorenz Müller, Chief Technology Officer and Frank Barker, Chief Executive Officer,

Hereinafter : the Controller,

And :

[Data processing operator], duly represented by _____(name and function),

Hereinafter : the Processor,

Whereas

Parties are research partners in the FIDIS (Future of Identity in the Information Society) project, a NoE (Network of Excellence) supported by the European Union under the 6th Framework Programme for Research and Technological Development within the Information Society Technologies (IST) ;

Parties agreed to collaborate in the field test of the AXS-Card developed by AXSionics, which is a proof of concept of encapsulated biometrics as described in FIDIS deliverable D3.10. (hereinafter 'the fieldtest');

The field test is planned for FIDIS deliverable 3.14, the details thereof as further described in the FIDIS workplan 4, D3.14.

AXSionics will take the responsibility for the field test, in particular the acquisition, the management and processing of certain personal data, including details about trusted authentication for accessing the OpenID identity management, for the above mentioned testing purposes, during the fieldtest, as the controller of the personal data;

The processor agrees to collect, to process and/or to receive personal data on behalf of the controller for the above testing purposes in accordance with the instructions of the controller and in compliance with the applicable data protection laws;

Therefore, it has been agreed as follows :

Article 1 – Definitions

1.1. 'Personal Data' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such date (hereinafter Directive 95/46/EC). Biometric data will *not* be included in the Personal Data to be processed by the processor.

'the Controller' shall have the same meaning as in Directive 95/46/EC.

'the Processor' shall have the same meaning as in Directive 95/46/EC and means the entity who agrees to collect, to process or to receive personal data in relation with the field test, and intended for processing on behalf of the Controller in accordance with his instructions, the terms of this Agreement and the applicable data protection laws.

'Field test' shall mean the demonstrator field test as described and planned for FIDIS deliverable 3.14 ;

Article 2 - Subject

2.1 The Controller requests the Processor, who accepts and agrees, to process on his behalf and in compliance with his instructions Personal Data as specified and agreed for the Field test.

2.2 Parties agree that the specifications and the instructions for the processing of the Personal Data for the testing purposes of the Field test are further described by the project proposal for the deliverable 3.14 (attached in appendix 1), the internal project documents and additional documentation that parties may agree upon from time to time.

Article 3 – Warranties and obligations of the Controller

The Controller agrees and warrants that he has instructed and throughout the duration of the Personal Data processing services will instruct the Processor to process the Personal Data only on the Controller's behalf and in accordance with the applicable data protection laws.

The Controller will instruct the Processor on the technical and organizational security measures as specified in Appendix 2, to be implemented by the Processor. Parties agree and belief that to the best of their knowledge these measures are adequate to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, having regard to the state of the art and the cost of their implementation.

Article 4 – Warranties and obligations of the Processor

4.1. The Processor agrees and warrants that he has followed and throughout the duration of the Personal Data processing services will follow the instructions of the Controller to process the Personal Data and will process the Personal Data only on the Controller's behalf and in accordance with the applicable data protection laws. The Processor will process the data only in the manner permitted for the Controller itself. The Processor agrees that it shall render the Personal Data anonymous as soon as the research purpose permits it. Until such time, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately.

4.2. The Processor further agrees that he shall not apply or use the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties, even not for their preservation. The Processor shall at all times keep the Personal Data confidential and request its agents to keep the Personal Data confidential as well.

4.3. Processor undertakes and warrants that he will implement the technical and organizational security measures specified in Appendix 2 before the start of processing the Personal Data and guarantees to take the agreed data security measures.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to his processing of the Personal Data for the Field test and to abide by the advice of the supervisory authority with regard to the processing of this Personal Data.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access by third parties, and (3) any request received from the data subjects.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

Article 5 – Term and Termination

The Agreement is concluded for a period and the time required for the testing of the AXS-card in the framework of FIDIS. The agreement ends latest at [date].

Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.

Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or processed for the Field test and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the

Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

Article 6 – Applicable law, Mediation and Jurisdiction

6.1. The laws of the Switzerland, where the Controller is established, shall apply to this Agreement.

In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled in due time, either party may bring the dispute to a competent court in Switzerland.

Done in _____, on _____ (date), in two copies, each party having received one.

The Processor [Signatures]

The Controller [Signatures]

Appendices