D21.2 – Technology Inventory

Document Identification	
Date	16/07/2013
Status	Final
Version	1.0

Related SP / WP	SP 2 / WP 21	**Document Reference**	https://dms-prext.fraunhofer.de/livelink/livelink.exe/overview/3182865
Related Deliverable(s)	D32.1, D22.2	**Dissemination Level**	CO
Lead Participant	IFAG	**Lead Author**	Detlef Houdeau (IFAG)
Contributors	Frank-Michael Kamm (G&D), Detlef Houdeau (IFAG), Lothar Fritsch (NRS), Charles Bastos (ATOS)	**Reviewers**	Christian Wagner (TU Graz), Dr. Anja Lehmann (IBM Zurich)

This document is issued within the frame and for the purpose of the FutureID project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424

Abstract

An extensive survey will be performed to identify the state of the art of eID and related relevant technologies for two factor authentication and signature in the public domain. The regional focus would be on Europe. This survey will consider available technologies and standards and include academic contributions. It will provide a comprehensive overview of the available and relevant technologies. The result of this survey will be documented in D22.1.

Document Information

Contributors

Name	Partner
Detlef Houdeau, Simon Hartmann	IFAG
Alexander Summerer, Frank-Michael Kamm	G&D
Charles Bastos Rodriguez	ATOS
Lothar Fritsch	NRS

History

Version	Date	Author	Changes
0.1	26/03/2013	Detlef Houdeau	Document Structure
0.2	05/04/2013	Detlef Houdeau	Chapter 2.1, 2.2, 2.3, 3.1 and 3.2
0.3	26/04/2013	Alexander Summerer, Frank-Michael Kamm	Chapter 2.5, 2.5.1, 2.5.2
0.4	03/05/2013	Detlef Houdeau	Add into chapter 3.2, 5
0.5	14/05/2013	Frank Michael Kamm	Chapter 2.4
	15/05/2013	Detlef Houdeau	Add into chapter 2.4
0.6NRS	22/05/2013	Lothar Fritsch	Added chapter 3 + references
1.0	29/05/2013	Detlef Houdeau, Simon Hartmann	Clean version
1.0 final	02/07/2013	Detlef Houdeau, Simon Hartmann	Overworked version

Table of Acronyms

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
API	Application Programming Interface
BAC	Basic Access Control; security architecture of ICAO
BioPIN	Biometric Personal Identification Number (e.g. fingerprint)
BSI	Bundesamt für Sicherheit in der Informationstechnik; Federal Office for Security in the Information Technology
BRP	British Residence Permit
B2C	Business to Citizen
CAPI	Crypto-API
CD-ROM	Compact Disc ROM
CNG	Cryptography Next Generation
COS	Card Operation System
CPU	Central Processing Unit
CY	Calendar Year
DAE	Digital Agenda Europe
DES	Data Encryption Standard
DG	Directorate General
EAC	Extended Access Control
EC	European Commission
ECC	European Citizen Card
ECC	Elliptic Curve Calculation
eEHIC	electronic European Health Insurance Card
eGK	elektronische Gesundheitskarte
eIAS	electronic Identification, Authentication, Signature

eMRTD	Electronic Machine Readable Travel Documents
EP	European Parliament
EPAC	European Port Access System
eRP	electronic Residence Permit
EU	European Union
GCS	Generic Cryptographic Service
GSS	Generic Security Service
G2C	Government to Citizen
HPC	Health Professional Card
HPRO	Health Professional
ICAO	International Civil Aviation Organisation
IdM	Identity Management
IMCO	Commission of the European Parliament
IoT	Internet of Things
ITRE	Commission of the European Parliament
JCE	Java Cryptography Extension
MEL	Multos Executable Language
MS	Member States
MW	Middleware
NIST	National Institute for Standardisation and Technology
nPA	neuer Personalausweis; new eID token in Germany
OCF	Open Card Framework
OS	Operation System
PC	Personal Computer
PC / SC	Personal Computer / Smart Card
PIN	Personal Identification Number
PIV	Person Identification (and) Verification

PKCS	Public Key Crypto Standard
PUK	Personal Unblocking Key
ROM	Read Only Memory
RSA	Rivest, Shamir und Adleman; asymmetrical algorithm
SIM	Subscriber Identity Module
SSEDIC	Scoping the Single European Digital Identity Community
SW	Software
TR	Technische Richtlinie; Technical Guideline
UK	United Kingdom
2G	2nd Generation

Table of Contents

1. Introduction

The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

The FutureID infrastructure will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. FutureID will allow application and service providers to easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments.

This will enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers FutureID will provide an integrative framework, which eases using their authentication and signature related products across Europe and beyond.

To demonstrate the applicability of the developed technologies and the feasibility of the overall approach FutureID will develop two pilot applications and is open for additional application services which want to use the innovative FutureID technology.

D21.2 will be an extensive survey on the state of the art of eID and related relevant technologies in Europe. This survey will consider available technologies and standards and include academic contributions.

The report gives an overview on eID programs in Europe in the time window ***CY 1998 – 2012*** in chronological sequence, reflects the availability of standards, HW-technologies, COS-technologies and MW-technologies in this time window and gives an outlook on future technologies along public funding projects in the time window ***CY 2012 – 2015***.

D21.2 is bridged with D32.1 – provides survey of existing eID and credential systems – and is the input for D22.1 – analysis of requirements with regard to the use and business cases.

Future ID is a three-year duration project funded by the European Commission Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424

2. eID Programs in the Time Window CY 1998 - 2012

2.1 Roll out programs in Europe

The following overview in chronologic sequence displays national programs on eID along the application scope

- e-Government services (tax, social, health etc.)
- e-Business services (banks, insurance organization, enterprise and retailer etc.)

with the three core basic pillars

- electronic identification (I)
- electronic authentication (A)
- electronic signature (S)

which is used typical in the acronym eIAS. The overview also reflects programs of the European Commission, which foster eID in the EU-MS in this timeframe.

CY Program on electronic identities:

1998 - **Finland** starts issuing 1st generation eID/eGov-card (FINID);
the eID document is voluntary in Finland;

2000 - **Slovenia** starts issuing 1st generation eHealth Patient Cards (HIC);

- **Poland**, Katowice starts rollout 1st eHealth Patient Card (KUZ);

2001 - **Spain** starts rollout of Health Professional Cards (HPC);

- **UK** starts rollout Health Professional Cards (HPC);

2002 - **Finland** starts with issuing the 2nd generation eID/eGov-card (FINID);

- **Norway** starts issuing of eSig-card for G2C and B2C processes (BUYPASS);

2003 - **European Council** decides and publishes "THESALONIKI Declaration" for identity travel documents with biometric data;

- **Belgium** starts rollout 1st generation national eID card (BELPIC);

- **Estonia** starts with issuing 1st generation national eID card;

- **Italy** starts 1st pilot of eHealth Patient Cards (CRS);

2004 - **EC** starts cross border cost reimbursement program for health service (NetC@rd)

- **Austria** starts rollout of eCard, with eGov, eSign and eHealth services;

- **EC** publishes regulation 2252/2004 for electronic travel documents with biometric data; two steps: CY 2006 face data must store in the electronic Machine Readable Travel Document (eMRTD) in EU-MS; CY 2009 also two fingerprints must be stored in eMRTD in EU-MS;

2005 - **Sweden** starts rollout of eID/eGov-Services card, combined with ICAO-data, ICAO-biometrics and ICAO-security (ICAO-BAC); the eID document is voluntary in Sweden;

- **EC** publishes recommendation 14351/2005, for national electronic ID-Cards; this recommendation addresses only the biometric data and the security architecture on ICAO for travel documents, as defined in the EU regulation 2252/2004.

2006 - **Italy** starts with issuing national eID card (CIE) and eGov/eHealth Service card (CNS);

- **The Netherlands** start rollout national eID card w/ ICAO-data (1st Generation, BAC face photo); eID service in the public or private domain is not possible;

- **Spain** starts rollout national eID cards (DNIe);

2007 - **Serbia** starts rollout of 1st generation national eID card, with eGov-Services;

- **Portugal** starts issuing 1st generation national eID cards, with 5 services in the public domain (PEGASUS);

- **France** migrates to the 2nd generation e-Health (Sesame Vitale 2); the 2nd gen is defined as replacement, if the 1st gen is not anymore valid;

2008
- **EC** publishes regulation 13502/2/07, for electronic Residence Permit (eRP); this address foreigner, which stay for long term (>90 days) in EU-MS.
- **EC** DG INFSO and 17 Member States start eID interoperability project (STORK);
- **EC** DG HEALTH and 12 Member States start e-Health interop. project (epSOS);
- **EC** DG INFSO and 12 Member States start e-Procurement interop. project (PEPPOL);
- **EC** starts feasibility program on federal network on HPC registration (HPRO);
- 1st Rollout of electronic Residence Permit in Europe starts in the **UK** (BRP);

2009
- **EC** publishes the new standard on e-European-Health-Insurance-Card (eEHIC);
- **Italy**, Lombardia starts with roll out of the 2nd generation eID/eGov/eHealth/eTicketing card (CNS);
- **The Netherlands** starts roll out national eID card w/ ICAO-data (2nd Generation, EAC face data and two fingerprint data);
- **Slovenia** starts replacing eHealth Patient Card with the 2nd generation (HIC);
- **Lithuania** starts with issuing 1st generation national eID card, combined with ICAO-data, ICAO-biometrics and ICAO-security (ICAO-BAC); hybrid card with contactless interface for travel document data and contact based interface for eGovernment purposes.
- **Monaco** starts issuing eID card combined w/ ICAO-data, ICAO-biometrics and ICAO-security (ICAO-BAC); hybrid card with contactless interface for travel document data and contact based interface for eGovernment purposes;

2010
- **Swiss** starts roll out of 1st generation e-Health Patient Card (KVG);
- **Swiss** Post starts eSign-card program for G2C and B2B processes (SuisseID); the participation is voluntary for health professionals, hospitals and clinics;

- **Germany** starts roll out of 1st generation national eID cards (nPA); eID service function is optional; citizen can decide eID "on" or "off";

- **EC** publishes the milestone plan for a single European market in CY 2015. A new regulation on electronic identification is scheduled for CY 2013 (KOM(2010)245);

- **Turkey** starts pilot phase of eID service in the city of Bolu;

2011 - **Poland** starts public tender on eID combines with e-Health service (PLID);

- **Ireland** starts pilot rollout of eID (Citizen Service Card);

- **EC** publishes the timetable for stability and growth for the European market. A regulation on electronic identification is scheduled for CY 2013 (KOM(2011)669);

2012 - **Czech Republic** starts issuing eID on voluntary basis;

- **EC** publishes a draft on EU regulation on electronic identification, authentication and signature; two committees of the EP collects reports on the eIAS regulation: ITRE and IMCO. ITRE is responsible for Industry, Research and Energy, IMCO is responsible for International Market and Consumer Protection.

- **Denmark** starts public tender on eID;

- **Croatia** starts a feasibility phase for an eID card program;

- **France** government decides to postpone the eID program and to remove e-service functions from this document in the public domain;

- **Austria** starts to work on the specification for the eID 2G;

- **Poland** federal government decides to split eID and e-Health into two programs;

- **Romania** federal ministry of health starts roll out of e-Health Patient Cards;

- **Bulgaria** starts a feasibility study on eID;

- **Germany** publishes a tender on 2nd generation e-Health Patient Card (eGK/2G) and Health Professional Card (HBA/2G).

- **EC** starts the initiative for a new interoperability program called eSens, which will be started in CY 2013;

Note:

a) The electronic residence permit card in Europe could support eID services if member states decide this. The responsible EU regulation 13502/2/07 was published on 7th of March 2008.

b) The EU regulation on electronic identification, authentication and signature is one pillar on the Digital Agenda of Europe (DAE) to foster one single European market by CY 2015. Existing eID solutions of EU-MS should be going into a notification process of the EC. Notified eID - token or - solutions should be accepted in all other EU-MS. It is expected, that this new regulation would be signed up from the EU parliament by December 10th of CY 2013.

c) Only Germany issues eID token, which like e-Government or e-Business use the contactless interface according ISO 14443 for e-Services. All other states use the contact interface according ISO 7816 for this purpose.

d) Only Estonia uses e-Signature in a mandatory way. All other states have this service function voluntary.

e) The combination with ICAO-functionality, - data set and - electrical security support travel function on secure token can be used for automatic border control programs. The ICAO frame included the biometric data set and electronic security is not usable for any kind of e-Services like e-Government and/or e-Business.

f) For user verification only PIN (and PUK) is in use. Biometric data, e.g. BioPIN are not in place.

g) Today in eight states in Europe ID-documents are not mandatory (e.g. Sweden, since CY 2005) or not in use (e.g. UK since CY 1951).

h) Most of this public programs offer three elements for the citizens:
   - Secure token, mainly issued from the municipality;
   - Qualified and/or certified card reader – called client service platform (e.g. Italy);
   - MW on CD-ROM (e.g. in Estonia) or for download (e.g. Germany);

i) End of CY 2012 round130 million eID cards are issued. In reflection of a total population of round 500 million citizens in the EU-MS, more than 25% of the citizens have an electronic ID document.

j) Only The Netherlands has started a national eID program without any e-service based on a two factor authentication.

Summary:
Electronic ID documents in Europe show a heterogeneous landscape of roll outs. The oldest program was started 1998 in Finland and the youngest in 2012 in Ireland. Over the time span of 15 years between the 1st roll out and the last roll outs many aspects where standardized on security, technology and application. Future ID should be able to support eID architecture with a broad span of age. The next chapter shows the development of the standardization.

2.2 Availability of standards

A complete overview on international standards on smart cards on interfaces and APIs, on security evaluation and credentials and protocols are displayed in D35.1. Two standards should be highlighted in this report, because these are key pillars for harmonization of technology as well for interoperability of components and solutions. These two documents (specification and standard) are:

- European Citizen Card, CEN 15480
- Card API, ISO 24727

The first standard called in a short name ECC, was started Q1 CY 2004 and finished Q4 CY 2007. The understanding of this time line is important for the view on standardized or not standardized eID token for the citizens in Europe. Some impacts on this:

a) States in Europe, which have started eID programs before this application standard was available, have no chance to use this standard.

b) States in Europe, which start eID programs after Q1 CY 2007, have the possibility to use this standard or parts of the standard.

c) ECC harmonize principles on three elements:
   - Identification (I)
   - Authentication (A)
   - Signature (S)

d) ECC is “tool box” with option on
   - Card interface
   - Authentication protocol
   - Data group
   - Signature protocol

- Access condition to the data group
- Pseudonymity
- And many others

A detail description is available in D32.1

e) EEC Standard has four pillars
Part 1: “Physical card”
Part 2: “Logical card”
Part 3: Data elements
Part 4: Test methods

Some examples

Finland has started the first roll out on eID of all states in Europe in CY 1998. The specification phase and pilot phase was started 1995. At this time an international standard like the ECC was not available. The result is, the FINID is complete outside of this standard and is technical not compatible with any other eID programs in Europe.

Sweden has started the roll out of the eID token in July 2005. At this time only part 1 and part 2 of the ECC-Standard were available. The eID token could be classified as pre-standard version.

Germany has started the roll out of the eID token by November 2010. The ECC-standard was completed, published and usable. The German eID card is fully ECC-compatible. Profile 1 of the ECC-Standard is equal to the new eID card called nPA.

The second standard: Card API is also used as middleware (MW). This MW is needed as logical element for the communication between the smart card and the card terminal. In the last 10 years many various MW-solution were provided from national security labs, like RSA in USA (e.g. PKCS#11), from Microsoft (MS CAPI and CNG), from JAVA (OCF) and from governments, e.g. US Government (GSS API and GCS API) and from the security industry.

Since 2004 a new international standard for MW is deployed under ISO, called ISO 24727. Such standard would be the silver bullet for interoperability of smartcards providing identification, authentication and digital signature. ISO 24727 was pushed by three government stakeholders

- US NIST (National Institute for Standardisation and Technology);
  Main focus: PIV-Card in the US

- Ministry of Health in Australia;
  Main focus: e-Healthcare Card in Australia

- Germany BSI (Federal Ministry of Security in the Information Technology);
  Main focus: eID token in Germany – called nPA.

Since 2009 all relevant parts of ISO 24727 are stabile. The first implementation in Europe is done along the German national eID card program, called AusweisApp (BSI TR 3112) from 1st of November 2010. In this national program the ISO 24727 for MW is linked to the European Citizen Card Standard CEN TC 15480 for Smart Card OS.

Some impacts on the timetable of the availability of this standard:

a) Most of the eID programs in Europe run outside of ISO 24727. Today only Germany is complete in line with ISO 24727.
b) The development time window CY 2004 – CY 2007 of this standard is similar to the ECC-standard, but different standardization organisation (CEN versus ISO) and different key drivers (CEN = industry stakeholder, ISO = government stakeholder) were involved in the work process.

Summary:
Future ID must support a broad range of eID schemes in Europe, mostly not based on an application standard such as European Citizen Card and Middleware. The late availability of the application standard is the cause and effect of the heterogeneous landscape of eID schemes in Europe. Future ID can help to find a way for technical interoperability on infrastructure of the eID programs in 16 EU-MS.
A detailed gap analysis of relevant standards would be shown in D13.3. A comprehensive requirement list is addresses in D35.1.

2.3 Availability of secure HW-technologies

For eID tokens in Europe only processor chips are required. At the first roll out on eID in Europe in CY 1998 a processor chip in 0.6 µm technology was available with 8 bit architecture and a crypto co-processor for asymmetric encryption like RSA. Three years later in CY 2001 the next technology step was made on 0.25 µm and the crypto co-processor supported Elliptic Curve Calculation (ECC). In CY 2003 the 8 bit architecture of the processor chip was changed to 32 bit architecture. CY 2005 with 0.22 µm the next technology step was on the market. CY 2006 beside ROM (Read Only Memory) also Flash as electronic storage media was available. CY 2009 the next technology step was achieved with 0.09 µm. Since CY 2010 the next level of HW-security was ready, called integrity guard, which captures double CPU, means one operational CPU and one for monitoring the work of the other CPU.

Overall in the smart card industry all three years the next generation of processor chip is deployed. Three corner stones are constantly modified

- Increase performance, e.g. migrate from 8 bit to 32 bit
- Increase security, e.g. change from DES to AES; RSA to ECC
- Increase memory size, e.g. 136k ROM to 400k Flash
- Decrease chip size

In a typical lifecycle of an eID token of 10 years three technology steps on HW are made. With the calculation that all 5 years the next generation of eID token could be required the total time window of 15 years means five technology steps on HW would be realized.

Along the last 15 years the security of HW increases from time to time. First attacks on HW were focused on electronic signal run time on the chip. The next levels of attacks were addresses on the side channel. Since five years light attacks and since 3 years laser flash attacks and the combination of electronic and light attacks were in the tool box of attackers. Every new attack can create a new countermessurement. E.g. light attacks generate light sensors on the chip. An active shield on the chip avoids local needle attacks and the dual CPU approach change from extrinsic security of the HW to the intrinsic security. The high numbers of various attacks fasten the speed of development and the development of a new secure IC family all three years in this particular smart card market.

2.4 Availability of secure COS-technologies

2.4.1 Role of the Card Operating System

While the FutureID project focuses mainly on technologies located above the Card Operating Systems (COS) level, i.e. middleware and applications, it is worth looking at some fundamental properties of COS that are used for eID systems. These underlying COS security functions in conjunction with a tamper-proof hardware (see section 2.3) are responsible for the high trust level that can be achieved when authenticating to FutureID with an eID hardware token. The design of secure COS is optimized with respect to suppressing information leakage by side-channel attacks and therefore provides high confidence that secret eID credential information cannot be read out, forged or copied. Thus the COS in conjunction with secure hardware is the main factor in providing the high trust level for eID authentication.

Most eID specifications do not include the use of a specific COS but rather concentrate on specifying the required functionality and security. It is then the decision of the chip card manufacturer to choose an appropriate COS which provides the required security and functionality within a competitive cost range and the required certification targets. The latter influences the choice of hardware which on the other hand has an impact on the choice of the most suitable COS.

Since smartcards cover a broad range of applications, like payment, ticketing, authentication (incl. eIDs) and mobile communication (SIM card), there exists no universal standard OS like in the case of PCs or mobile phones. The required functionality typically differs significantly between the applications and the main limiting factors are the available hardware resources, especially the size of memory. Due to the strong memory limitations of typically only a few 100 kB, most COS are specifically tailored for a type of application.

Over the years, COS have undergone a similar development like other OS for specialized applications. While the first COS were rather a collection of function libraries than real operating

systems, they developed to monolithic OS and later to layered OS, including even multitasking capabilities for more complex hardware. The actual size of the linked object code typically varies between a few 10 kB and about 500 kB.

Main functions of a COS are:

- Control of data flow to and from a smart card,
- Management of the file system on the card,
- Control of the program code flow,
- Execution and management of cryptographic functions,
- Management of the card command execution,
- Management of access rules and security counters (e.g. retry counter),
- Memory management.

Since security is one of the main assets of smartcards, the COS focuses on providing an appropriate security level in conjunction with a secure hardware. This includes the suppression of side-channel attacks (like timing attacks or power analysis attacks), the execution of “atomic functions” (i.e. routines which cannot be brought into an insecure state by interrupting the execution) and the management of secure counters, like the PIN retry counter. Secure management of memory, especially non-volatile flash memory is also one of the important security roles of the COS.

For eID applications, the level of security that is provided by the COS directly translates into the trust level of authentications that can be reached with the eID. With appropriate measures against side channel attacks it will become practically impossible to read out cryptographic secrets and therefore to copy or modify eIDs.

2.4.2 Types of COS

COS can typically be divided into two main groups:

- File-based COS,
- Application-based COS.

The file-based COS manage a file system that contains elementary files (EF) and dedicated files (DF), which are comparable to files and folders on PC-based OS. The actual application consists of a specific file structure and according access rules that are managed by the COS. In this case the application uses the general functionality provided by the COS (e.g. authentication,

cryptographic algorithms, …). The COS also supports the management of several applications on one card.

Application-based COS provide a universal API (application programming interface), that allows to execute programme code (applets) on top of the COS. This program code can also be provided by a third party. A typical example for this class is the Java Card OS, which provides a Java-based API for applets. In this case the COS is a specific implementation of the Java Card API specifications and provides functionality to manage the installation and execution of several applets on a card.

Depending on the underlying specifications, the COS can also be divided into

- Proprietary COS,
- Open COS.

In case of the proprietary COS, the chip card manufacturer controls the specifications, the range of functionality and the implementation of the COS. By adapting the COS to the respective applications, the proprietary COS typically provide an optimum performance on limited hardware resources in terms of memory usage and operation timing. On the other hand, in case of the open COS, the specifications and the range of functionality are described by industry standards or open standards. The chip card manufacturer only controls the specific implementation of a given specification. These COS offer a higher flexibility in terms of application programming but typically have a higher resource need.

The term “open COS” is somewhat misleading, since only the specifications are open. The actual software implementation is nevertheless proprietary (other than in open source OS, like Linux) and different COS fulfilling the same API specifications might differ in terms of security, depending on the quality of the actual implementation. On the other hand, the “proprietary” COS may nevertheless fulfil certain industry standards or international standards like the ISO/IEC 7816 series to provide the required interoperability.

An important aspect of COS is the management of card applications, especially when the cards are already distributed. This includes the secure installation and removal of applications as well as the separation of application data and maintaining access rights across applications. A framework for managing these topics is provided by the Global Platform specifications. These specifications are independent of the actual COS and therefore can be supported by proprietary COS as well as by open COS.

Another security relevant aspect that could also play a major role for eID systems is the patching of COS parts in the field, i.e. after the cards have been deployed. Especially the eID systems with their long lifetime might require a COS patch during their lifetime when new types of attacks become relevant. The smartcard manufacturers currently develop technologies that allow a secure in-field patching.

2.4.3 Examples of COS

The following list can give a brief overview of some commercial COS implementations. It does not represent a complete list of all available COS.

Application-based COS

- **Java Card** (available in many different implementations, like SkySIM from G&D), allows execution of Java Card programme code.
- **Multos** ("multiapplication operating system"), specified by Maosco Consortium, specifications partially confidential. Programme code typically written in C and translated into MEL (multos executable language).
- **BasicCard**, developed by Zeitcontrol, contains Basic interpreter for execution of programme code.

File-based COS

- STARCOS (G&D)
- CardOS (Siemens, now Atos)
- Cryptoflex, Cyberflex (Gemalto)
- SIMply CDMA, Micardo (Morpho)
- SIMtonIC, SIMphonIC (Oberthur)

When the first national eID programmes came up, secure tokens with specific COS where requested. This was the case in 1998 in Finland (FINID) as first program in Europe and in the same year in Malaysia (MyKAD) in Asia. These COS were not a derivate of COS for banking card or for SIM-cards.

With increasing numbers of public eID programmes having all different architectures and security requirements, the demand for specific COS increased. On the other hand, standardization efforts like the European Citizen Card specification tried to harmonize the eID landscape in terms of COS functionality. When this trend continues it allows establishing COS-families with modular architectures for eID applications.

Today, proprietary COS are used in Germany, Italy, Austria, Belgium, Finland, Spain and Ireland. Open COS, based on Java Card OS, are used in Czech Republic, Latvia, Portugal, Sweden and Monaco.

2.5 Availability of secure MW-technologies

Contrary to the Card Operating System that has been described in the previous section, the middleware infrastructure lies directly in the focus of FutureID. Since existing eID implementations in various European countries differ in terms of hardware and COS specifications, their middleware architecture is different as well. Therefore, one of the main challenges of FutureID is to integrate this broad variety also on the middleware level. This is especially challenging since the middleware architecture also differs significantly between PC-based systems and mobile devices.

The concrete impact of middleware specifications on FutureID is discussed in detail in the respective deliverables of SP3 (client development), especially of work packages 31 (IFD-layer), 32 (eID services) and 33 (eSign services). Therefore, this section will concentrate on providing a broad overview over existing middleware concepts.

2.5.1 PC-based devices

The following overview describes the various middleware components for the Service Access Layer (SAL) and Transport Layer (TL) on PC-based devices.

Service Access Layer:

PKCS#11 is a token-based interface for cryptography operations, defined by the RSA Laboratories, which is typically supported by native applications. This interface allows the usage of keys on a Smart Card and the execution of crypto operations inside the Smart Card. The crypto operations and key storages on the Smart Card side are typically realised by Applets which are implemented by different vendors. A vendor realising a Crypto Applet typically provides a corresponding PKCS#11 library which can be linked by application. PKCS#11 libraries are typically based on PC/SC in order to perform an APDU communication.

ISO/IEC 24727 defines an international standard middleware framework which can be used by PC applications to perform signature operations and authentication procedures based on Smart Cards. The ISO/IEC 24727 is split in different parts. ISO/IEC 24727 part 3 defines a service access layer which includes authentication protocols and an interface for applications.

The **eCard-API** is a German national standard for a middleware framework, defined by the BSI, leveraging operations based on different card systems like health cards and ID cards used by German citizens. The eCard-API is split in different layers (Application-Layer, Identity-Layer, Service-Access-Layer, Terminal-Layer) and is based to the international middleware standard ISO24727.

Transport Layer:

ISO/IEC 24727 defines an international standard middleware framework which can be used by PC applications to perform signature operations and authentication procedures based on Smart

Cards. The ISO/IEC 24727 is split in different parts. ISO/IEC 24727 part 2 realizes a transport layer for an APDU communication.

PC/SC, as an industry standard, is providing a native interface for PC applications. This standard defines an interface and system for performing an APDU-based communication to Smart Cards. Moreover it defines an architecture on how different PC/SC drivers can be integrated into the PC/SC system. The PC/SC system includes a core component, the resource manager, which manages and synchronizes the communication channels between PC applications and Smart Cards. Libraries implementing the PC/SC standards are typically pre-installed on PC operating systems.

2.5.2 Mobile Devices

Due to the different architecture of mobile devices compared to PC-based devices, the middleware structure is also different than on a PC-like device.

Service Access Layer:

The **SIMalliance Open Mobile API** as specified by the SIMalliance is an API that allows applications on mobile devices to access various kinds of secure elements in a standardized way. These elements can be SIM cards, secure microSD cards or other kinds of secure tokens embedded in or attached to the mobile device. The API definition is independent of a specific platform or programming language and could therefore be implemented on any type of device and operating system. The OpenMobile API consists of a transport layer and a service layer. The transport layer allows an APDU-based communication to Secure Elements available in a device. The service layer defines a set of high level APIs for typical operations on a Secure Element. The current service layer covers APIs for file read/write operations, secure storage operations, PIN verification and Secure Element discovery. The Open Mobile API service layer is optional and can be implemented by different vendors.

PKCS#11 is a token-based interface for cryptography operations, defined by the RSA Laboratories, which is typically supported by native applications. This interface allows the usage of keys on a Secure Element and the execution of crypto operations inside the Secure Element. The crypto operations and key storages on the Secure Element side are typically realised by Applets which are implemented by different vendors. A vendor realising a Crypto Applet typically provides a corresponding PKCS#11 library which can be linked by application. For mobile devices there is typically no PC/SC support.

The platform Android provides a **JCE interface** (Java Cryptography Extension) for Android applications which allows cryptographic operations. The execution of cryptographic algorithms is realised by a specific JCE crypto provider module which has to be chosen by the application. A JCE crypto provider module could use a Secure Element as crypto engine and key storage and uses the Open Mobile API in order to perform the communication to the Secure Element. The crypto engine and key storage is typically realised by a Secure Element Applet (Crypto Applet)

providing an APDU-based interface to select keys and execute cryptographic operations. Since this APDU interface is typically vendor specific the vendor of the Crypto Applet has to provide a corresponding JCE crypto provider module which allows the usage of its Crypto Applet.

Transport Layer:

The SIMalliance standard **Open Mobile API** defines a transport interface which allows an APDU-based communication to Secure Elements available in a device. For a device application it is possible to establish a dedicated communication channel which is uniquely assigned by the API implementation to a logical channel of the Secure Element and a Secure Element Applet. The Open Mobile API implementation manages the different communication channels between device applications and SE Applets and assures that resources are allocated and de-allocated correctly. Moreover it controls the APDU communication by considering restrictions and access control policies which might be defined in the targeted Secure Element. The SIMalliance Open Mobile API is defined in an agnostic way and could be implemented in different mobile platforms. First implementations of the Open Mobile API are already available on different Android handsets. On the most Android handsets the OpenMobileAPI implementation is realised as a system service, preinstalled in the devices, which can be used by Android applications to perform an APDU communication towards SE Applets. The Android application has to use an OpenMobileAPI library which realises the communication to the system service realising the resource management. The system service uses different drivers to accomplish the communication to the different Secure Elements.

2.5.3 Conclusions

All the mentioned middleware components provide an infrastructure which already allows for a highly secure usage of hardware-based secure elements. With the support of cryptographic functionality, APDU commands can be sent to Smart Cards and security critical operations can be performed directly on the card. Using secure messaging, the communication between the card and the middleware can be encrypted. Nevertheless, security issues remain. For example, if the transport layer is located in an insecure environment it could be manipulated or be replaced by a malware component. Therefore, the end points of secure communication have to be defined carefully (see for example deliverable D22.2) and the surrounding client platform has to be as trustworthy as possible (see for example deliverable D35.1).

3. Future Technology Concept in the Time Window CY 2012 – 2015

3.1 Technology trends from research

This chapter is based on two pillars, with

- Funded projects with technology focus
- Funded projects with application focus

3.2 Funded projects with technology focus

BioP@ss: biometric authentication for internet services with secures token [2]; EU-funding under MEDEA+/CATRENE; start CY 2008 is looking on implementation of new aspects along the European Citizen Card standard [3]. This project was led by Gemalto, with 9 Companies from 6 EU-MS. Project finished January 2010. According to [17], the project produced the following new technologies:

- It has developed advanced chip cards and embedded software for next-generation biometrics-enhanced passports and identity cards as well as access to pan-European public services. Contactless card scanning and very high speed data interfacing will reduce queues at airports and frontier posts while boosting European security.
- Advances in BioP@ss included match-on-card technologies and the further development of security chips and encryption technologies, and security software for personal computers. Data transfer rates between cards and readers have been increased more than tenfold – from 800 kb/s to 10 Mb/s. Moreover, a new chip-card operating system makes it possible to use future e-ID documents on the Internet without any additional software components on the PC

With the focus on COS BioPass would be a mirror public funding project to FutureID.

TURBINE: Tr**u**sted **R**evocable **B**iometric **I**de**n**titi**e**s was working on improving the quality and reliability of fingerprints for use in e-ID applications started 2008 with a consortium of 10 partner organizations [4]. Project finished 2011. It has developed security methods for trustworthy handling of biometric reference patterns. One of the outcomes is a technology for encryption and on-device verification of biometric reference patterns that can resolve privacy issues with biometric reference patterns [18].

Based on the fact, that FutureID is not reflecting any biometric technologies there is no overlap to TURBINE.

ABC4Trust: **A**ttribute-**b**ased **C**redentials **for Trust** is a project which addresses the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials [5]. This project has started 2009, captures 12 partners from 5 EU-MS and is headed from University in Frankfurt, Germany. It focuses on architecture, and more important, on a standard for identity-related attributes that are used in conjunction with e-ID. The standard description of attribute classes is expected to provide handling of privacy issues that arise with attribute disclosure.

FutureID could benefit from this work, as it provides a specification of pseudonymizable attribute types versus identifiable identity attributes.

PrimeLife: Bringing sustainable privacy and identity management to future networks and services; a funding project under FP7, starting in 2008, runtime 40 months, headed from IBM, with 15 partner from 5 states (included USA) [6]. PrimeLife aimed at the provision of better privacy over person's whole life. Research focused on data handling, policy enforcement and specification, and on the improvement of cryptographic protocols for attributes. The project produced, among other results, a number of articles on policy-enforcement mechanisms, and on trusted user interface metaphors for users of privacy technology.

PrimeLife could be classified as Complementary public funding project to FutureID with the focus on privacy and data protection of person related data.

PICOS: Privacy and Identity Management for Community Services, an FP7 project with focus on the mobile community. This project has started 2008 with 11 partners from 7 countries, headed from University in Frankfurt, Germany [7]. PICOS researched the integration of mobile social media with privacy technology in sample application areas. The prototypes and trials included user-friendly mobile user interfaces that underwent extensive end-user testing in selected target communities. An interesting result is the privacy threat model for data portability in social network applications [19].

With the focus on mobile user interface PICOS could deploy interest inputs for FutureID.

GINI-SA: **G**lobal **I**dentity **N**etworking of **I**ndividuals - **S**upport **A**ction, is an FP7-funding project, starting 2010, duration 24 months with 8 partners from 6 EU-MS, headed from IKED, Sweden [8], with focus on user-centric identity management services. Among its many outcomes is a gap analysis for future research [20].

GINI-SA could be seen as complementary public funding project to FutureID, cause the user centric identity management is the scope.

uTRUSTit: Usable Trust on the Internet of Things, an FP7 project exploring how small devices can communicate trust and security properties of IoT infrastructure to users of varied capabilities. The project built prototypes for smart home and smart office technology with various remote functionalities and a multitude of possible access configurations. Extensive user trials

with special user groups and prototype development based on special-needs persons are some of the highlighted results of the project [23].

Partial aspects of the outcome of uTRUSTit could be on interest for Future ID.

e-Me: The Norwegian VERDIKT project on usable authentication for social media investigated usability and e-inclusion issues with identity management technology used for access to social media. The project developed various alternative authentication prototypes, and tested them with special-needs user groups. One of the project's conclusions is the suggestion of an adaptive multi-modal and multi-channel identity management strategy that accommodates many users and that provides alternative authentication methods that adapt to changes in people's capabilities [24].

The multi channel identy management of e-ME could support FutureID.

PETweb II: The Norwegian VERDIKT project aimed at the conceptualization of privacy risk in identity management technology. It analysed the inherent risks in IdM base technologies, and developed two alternative risk assessment methods. One method focuses on technology-inherent risk factors for information privacy and security, while the second method investigates stakeholder incentives to keep to policies or to ignore them in a wider context [25].

PET web II could be classified as complementary public funding project with the focus on risks along identity management.

3.3 Funded projects with application focus

PEPPOL: e-Signature Services feasibility study cross border; focus on B-2-B; it is a public funded project; started 2008 (**P**an-**E**uropean **P**ublic e-**P**rocurement **O**n-**L**ine), where 8 countries looking at using e-ID to facilitate online authentication of transactions [9]. 25 Trust Centers participate on this feasibility project. Project was extended to open PEPPOL, which runs until 2014. PEPPOL facilitates the pre-award and post-award procurement process with standardised components by focusing on the most complex eProcurement elements. The project uses existing e-ID technology.

PEPPOL shows no overlap with FutureID, cause e-procurement cross border is not relevant in FutureID.

ICT/LSP **epSOS**: **S**mart **O**pen **S**ervices for **E**uropean **P**atients, a public funded project, started 2008 and has 26 members from 12 countries for developing a practical e-Health framework infrastructure that will enable secure access to patient health information, patient summaries and e-Prescriptions between different European healthcare systems [10]. This project is extended to 2014. All pilot cases move to STORCK_2. epSOS. It implements patient identity validation, patient consent management, health professional identification and access control mechanisms based on specific policies for medical and patient data sharing and transmission.

With the scope on e-helath service cross border epSOS has no overlap with FutureID.

NetC@rds: Cross border cost reimbursement of health services, a public funded project, too, started 2004 to introduce a pilot on eEHIC (electronic European Health Insurance Card, previous E111 document); It is an application by a consortium of 16 EU-MS in 2010 [11]. The project aims at the implementation of an infrastructure for the European Citizen Health Insurance Card service for patients and medical professionals. The service can be provided via an eye-readable EHIC, a national health insurance electronic card, or via certain national e-ID chip cards issued by the responsible government authorities of the participating partners. An on-line verification provides assurance to support acceptance procedures for both health insurances and health care providers. The NETC@RDS application is thus expected to improve administrative healthcare services across member states and mobility of European citizens to national healthcare system.

The scope of Net Card with cost reimbursement is complete outside of the scope of FutureID.

HPRO: is investigating the creation of a federated network of health professional registration; the feasibility study; by a French and Belgian consortium started in 2008 for 18 months to allow free movement of clinicians and recognition of their expertise by different health authorities based on interoperable use of electronic health professional cards. [12]. The main objectives of the HPRO card will be to facilitate the free movement of health professionals in Europe while protecting patients from the small number of professionals that could be subject to severe disciplinary sanctions. In the future, the card could have other possible applications such as validation of continuing education, and access to medical records.

HPRO is focused on a small use group, concrete on health professionals in Europe. FutureID is focused on the citizens in Europe.

EPAIC and EPAIC II: an initiative and working group (The PortIDS Consortium) to increase the security at sea ports in Europe, starting 2008; is looking at the development of a **E**uropean **P**ort **A**ccess **I**dentification **C**ard [13]. The project carried out a thorough stakeholder analysis of European port, shipping, and logistics stakeholders, the regulation, and the security considerations of access control and ID needs in Europe's ports.

EPAIC addresses only worker at seaports. This is not the scope of Future ID.

eCodex: Improve cross border access and exchange of information about legal proceedings of other countries in Europe [14]. 16 states with their related Ministry of Justice are participating, headed by Ministry of Justice in Germany. Start was Dec 2010 and the finish is scheduled for Nov 2013. The total budget is defined with 14 million EUR. The project discusses issues of document security and data privacy, and explicitly provides e-ID and authentication requirements for legal proceedings over borders in Deliverable 4.1.1 [21]. The project maps

requirements into STORK and PEPPOL. Confidentiality, access control, and digital signatures are core applications for e-ID and related services in eCODEX.

There is no overlap between eCOdex and FutureID, cause eCOdex is focused on information exchange in the legal domain cross border.

eSens: The project is an ICT PSP Large Scale Pilot. The project focuses on a basic cross sector service interoperability. 20 national consortia with an overall budget of 12 million EUR work on the project. The start is spring time 2013 [15]. The objective of WP 6.3 - Identity, Trust and Security - is to integrate the existing solutions and to extend them to create re-usable generic blocks for cross-sector authentication and creation/validation of e-ID and e-Signatures. Examples of possible extensions are modular solutions for usage of e-ID and e-Signatures in modern environments (such as the mobile and cloud-based ones), including certified attributes too. Additionally, this WP will also look at issues of cross-sector / cross-border service security mechanisms and trust establishment, needed when services based on different technical and legal regulations are interconnected.

eSens is of interest for FutureID, because identify, trust and security of cross border e-services is also addressed as well as the integration of existing solutions.

SSEDIC: Platform for all the stakeholders of e-ID to work together and collaborate to prepare the agenda for a proposed single European digital identity community as envisaged by the Digital Agenda Europe. Start was in 2010, duration 36 months [16]. SSEDIC will create, among other expected results, at the technical level an electronically retrievable roadmap of critical actions, milestones and timelines. This roadmap will outline how to achieve the vision of the Single European Digital Identity Community.

The output of SSEDIC would be used along the requirement aspects of FutureID as defined for D22.1, D22.2, D22.3, D22.4, D22.5, D22.6 and S22.7.

ICT/LSP **STORK**: (**S**ecure iden**t**ity acr**o**ss bo**r**ders lin**k**ed) e-ID/eGovernment Services cross border project funding; started 2008 is working on electronic gateways for identity credentials to be authenticated across the EU; this program, called STORK_1, finished by end of 2011 [1]. 15 EU-MS have participated on STORK_1. STORK_2 was started in June 2012, having 58 partners from 19 EU MS with a total budget of 18 million €. Runtime would be three years. The project is coordinated by Atos.

3.4 Most relevant trends in the context of FutureID

This section lists interesting technology trends for FutureID from the projects listed above. Those technologies and trends can inspire FutureID and enhance the project's technology base and specification work.

- Trustworthy biometric authentication: BioP@ss' advanced on-chip biometric matching technology is an interesting option to ease the PIN security issues, and to bridge the gap between a secure device and its user when FutureID needs to establish the presence of a person, and not just the presence of keys and authentication factors. Combined with the TURBINE approach of protected biometric reference patterns, FutureID could demonstrate advanced trusted biometrics with built-in privacy protection.

- Policy enforcement mechanisms: FutureID can add value to e-ID transactions by binding transactions to certain policies. CA and signature policies, professional role policies, privacy policies, and complementary obligations describing data processing consent and data processor obligations when handling identity attributes have been developed in PrimeLife. In particular, some results have specified how large data processing systems can enforce data handling policies using trusted hardware [22].

- Identity attribute specification: ABC4TRUST works on the specification and standardization of identity attributes with particular focus on technologies for anonymous credentials. FutureID could benefit from this work, as it provides a specification of pseudonymizable attribute types versus identifiable identity attributes.

- Requirements and gaps: The GINI gap analysis document is a valuable source for technology gaps for future research and prototyping. The applied projects and cross-border trials listed in section 3.3 provide a large body of valuable application requirements that the FutureID infrastructure should be usable against.

- Usability, Accessibility and e-Inclusion: From PICOS, e-ME and uTRUSTit, FutureID can gain insights on accessibility issues, e-inclusion strategies and pitfalls for both IdM technology usage and user interfaces used on the client software. The e-Me concept of multi-modal, multi-channel IdM should be most inspiring to the FutureID project.

- Privacy risk assessment and privacy impact: PETweb II's model for IdM-technology-based privacy risk should be adapted to FutureID. In addition, as FutureID as agnostic to applications using its infrastructure, a basic understanding of both user and application stakeholder's basic interests in sticking to policies, contracts and procedures and their incentives to violate them for profit will be valuable for making decisions about the core security functions of FutureID.

3.5 Outlook on future technologies for e-ID

Today, FutureID focuses strongly on the existing base of smartcard-based e-ID. The main reason for this is certainly the existing regulatory framework for government e-ID, electronic signatures, and the respective vendor base for the base technologies. However, the devices used to interact with digital applications are changing. FutureID should expect three major trends on the e-ID market for the near and mid-term future:

1. Mobile phones will take over e-ID functionality. Based on various technological options (SIM cards, secure hardware and operating system, or secure elements), identity credentials and cryptographic operations will be carried out on people's smart phones. The phones then either user local communication with a PC, or direct communication with application-specific web services or terminals to identify their users. Transaction partners will, in increasing volumes, become automated systems on the Internet of Things rather than large e-government interaction systems. Identity credentials related to credit cards, bonus programs of organizational memberships will compete with CA-based identity credentials.

2. Alternative and supplementary authentication factors will materialize. Today, mobile phones are already used as an additional authentication channel by many e-ID consuming applications – either to send one-time codes to the phone, or to establish identities by checking the phone directory. Technologies for transaction confirmation with automated calls, and voice-recognition based mobile authentication are under development. Location-fencing is another authentication factor that became widely available due to GPS receiver availability on smart phones. E-inclusion requirements and accessibility design might require the implementation of a portfolio of complementing authentication factors for specific user communities. In consequence, FutureID should prepare for alternatives to security-evaluated terminals with small pin pads and small screens as the only precondition for secure use of signature technology and high levels of identity assurance.

3. Quality and privacy management of e-ID ecosystems: Identity attributes may change over a person's lifetime. FutureID and its contributing identity providers should be prepared to update and downstream-enforce identity attribute updates while staying compliant to privacy policies and obligations. In addition, users have strong privacy rights including the revocation of data processing consent. EU data protection legislation is under way to require a "right to be forgotten", which implies that any information system accumulating personal data will need to be able to correct, remove, and delete data on request, or automatically. The FutureID infrastructure will connect many e-ID providers into a large identification and identity attribute exchange infrastructure, which in turn in the role of an identity intermediary will connect its users to a large application space. With the above data quality issues and privacy rights in mind, FutureID faces a non-trivial task for data flow management, policy versioning, and attribute management over its user's whole lifetime.

4. Conclusion

D21.2 – the technology inventory is an extensive survey of the state of the art technologies, standards and implemented programs on eID in the public domain. D21.2 mirrors the development of international standards, technologies and implementation in states in Europe in the time window 1998 – 2012. The document gives an overview on all relevant international public funding programs as known today and finishes with the relevant trends in the context of FutureID.

5. Bibliography

[1] www.eid-stork.eu

[2] www.biopass.eu

[3] CEN TC 224

[4] www.turbine-project.eu

[5] www.abc4trust.eu

[6] www.primelife.ercim.eu

[7] www.picos-project.eu

[8] www.gini-project.eu

[9] www.peppol.eu

[10] www.epsos.eu

[11] www.netcards-project.com

[12] www.hprocard.eu

[13] www.ec.europa.eu/transport/modes/maritime/studies/maritime_en.htm

[14] www.e-codex.eu

[15] www.esens.eu

[16] www.eid_ssedic.eu

[17] EURKA Success story: The Future of airport passport control, 2011-10-14, published on http://www.eurekanetwork.org/showsuccessstory?p_r_p_564233524_articleId=1196552&p_r_p_564233524_groupId=10137, viewed in May 2013.

[18] Practical Guidelines for the privacy friendly processing of biometric data for identity verification, 12/07/2011, http://www.turbine-project.eu/dowloads/TURBINE_KUL_ICRI-D1_4_3_BEST_PRACTICES_R2_3.pdf, accessed May 2013

[19] Weiss, S., “Privacy Threat Model for Data Portability in Social Network Applications”, Proceedings of the 14th Americas Conference on Information Systems (AMCIS), Toronto, Canada, 2008.

[20] Deliverable D2.2 of the GINI support action: Technology Gaps for Longer-Term Research, October 17, 2011; http://www.gini-sa.eu/images/stories/D2.2%20-%20Technology%20Gaps%20for%20Longer-Term%20research%20-%202011.10.17.pdf, accessed in May 2013

[21] e-CODEX Delvierable 4.1.1: e-Identity: Inventory and Requirements Documents, 16.10.2011 http://www.e-codex.eu/news-and-media/media/deliverables.html?eID=dam_frontend_push&docID=144, accessed May 2013

[22] Casassa Mont, M.; Pearson, S.; Bramhall, P., Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. In Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03), IEEE Computer Society: 2003; p 377.

[23] www.utrustit.eu

[24] www.jus.uio/ifp/english/research/projects/nrccl/e-me/

[25] petweb.nr.no