Report on Standardization Contribution

SP1, Task 13.4: Contributing to Standardization

Document Identification	
Date	07/08/2014
Status	Final
Version	1.5

Related SP / WP	SP 1, WP 13	**Document Reference**	D13.4.2
Related Deliverable(s)	13.3	**Dissemination Level**	PU
Lead Participant	G&D	**Lead Author**	Dr. Jens Urmann
Contributors	IBM, IFAG, TUG	**Reviewers**	FhG IAO

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.

1. Executive Summary

This deliverable reports on the standardization activities of contributing FutureID partners within the context of the FutureID project. The contributions focus on the following objectives:

- **Harmonization of existing ID card standards**: Existing standards and specifications for Machine Readable Travel Documents (such as ePassports), ISO compliant Driving Licenses and EU Driving Licenses make use of different cryptographic protocols for the very same use cases. To reduce this complexity FutureID partners actively support the adoption of already widely deployed Travel Document protocols for Driving Licenses. To reduce this complexity even further, FutureID partners contribute to test standards which enhance the interoperability of implementations. This complexity reduction will support the fulfilment of FutureID's objectives.

- **Pushing the privacy topic for next generation ID cards**: Use cases and requirements for the privacy friendly usage of Driving Licenses as ID cards in the future have been collected and specified. These serve as input for the next step, the standardization of the privacy-friendly techniques which will be standardized for ID cards in general and not for Driving Licenses. This approach has been chosen in order to avoid the errors made for existing standards, i.e. the usage of different protocols for the same use cases, but different types of ID cards.

- **Pushing the standardization of IC managed devices**: These devices (displays, keyboards, batteries…) are under the control of the IC and may be on card or off-card, e.g. part of the mobile phone. This topic allows for new use cases and enhances security as well as privacy of existing use-cases.

This document D 13.4.2 is an updated version of the previous deliverable D 13.4.1, integrating the additional standardization activities that occurred within the last 6 months. It will be continued as a continuously updated document for the future reporting periods as well.

2. Document Information

2.1 Contributors

Name	Partner
Dr. Detlef Houdeau	IFAG
Dieter M. Sommer	IBM
Prof. Dr. Peter Lipp	TUG
Dr. F.-M. Kamm	G&D
Dr. Jens Urmann	G&D

2.2 History

Version	Date	Author	Changes
0.1	03.02.2014	F.-M. Kamm	Initial version
0.2	18.02.2014	Jens Urmann	Included input from IFAG, TUG and G&D
0.3	20.02.2014	Jens Urmann	Added - further input from IBM - remark about new privacy work item in WG4 - clause 1 "Executive Summary" - clause 7 "Summary/Conclusions"
1.0	21.02.2014	F.-M. Kamm	Minor modifications, compilation int. reviewer version.
1.1	13.03.2014	F.-M. Kamm	Integrate reviewer comments
1.2	02.07.2014	Jens Urmann	Update for the next reporting period
1.2.1	23.07.2014	Detlef Houdeau	Additional updates
1.3	24.07.2014	Jens Urmann	Consolidated input from partners
1.4	25.07.2014	F.-M. Kamm	Internal reviewer version.
1.5	07.08.2014	Jens Urmann	Resolved comments of the internal review and included further input by FutureID partners

2.3 Table of Acronyms

AdES	Advanced Electronic Signatures
BAC	Basic Access Control
BAP	Basic Access Protection
EAC	Extended Access Control
EAP	Extended Authentication Protocol
eIDAS	electronic Identification, Authentication and trust Services
eMRTD	electronic MRTD
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute
EU	European Union
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ICBWG	Implementation and Capacity Building Working Group
ICC	Integrated Circuit Card
IEC	International Electrotechnical Committee
ISO	International Organisation for Standardization
JTC	Joint Technical Committee
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
NTWG	New Technology Working Group
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number

SC	Standardization Committee
SCA	Signature Creation Application
STF	Specialist Task Force
SVA	Signature Verification Application
TAG	Technical Advisory Group
TF	Task Force
WG	Working Group

3. Table of Contents

4. Project Description

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 who want to use the innovative *FutureID* technology

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

5. Role of Standardization for FutureID

One of the key challenges of FutureID is managing the complexity and large variety of eID systems in Europe. Not only national eID cards shall be supported by the FutureID infrastructure but other types of "secondary" eIDs as well, like health cards, driver's licenses, resident permits, etc. This complexity is reflected in several parts of the system architecture and the system components layout, e.g. the modular approach of the client architecture or the technical design of the Universal Authentication Service.

Among several organizational, political and socioeconomic aspects, one of the main reasons for this large variety of existing eID solutions within Europe is the lack of widely accepted and implemented standards. Although already many eID standards for hardware, interfaces, protocols, security, etc. have been defined on European or global level, many of them still allow a large variety of options, variations and parameter choices or simply lack unambiguity that limit interoperability in actual implementations. In addition, different types of eIDs have different usage scenarios, operational environments and requirements regarding privacy, security, roll-out costs, etc. For certain areas, gaps in standardization still exist and need to be addressed (see deliverable D13.3).

Therefore, it is reasonable for FutureID to support ongoing standardization activities for eID systems in order to help reducing this complexity and variety and ensure that implementations are compliant to the underlying standards and specifications. These activities are typically a prerequisite for a further harmonization of eIDs in Europe. At the same time, FutureID may develop new solutions and approaches for privacy-friendly eIDs that should be addressed in the standardization groups. By implementing a FutureID solution in a European or global standard, the exploitation of FutureID results in actual products will become much more realistic and feasible.

Within this task, several FutureID partners have participated in various standardization bodies and their corresponding working groups in the eID context to further harmonize the eID landscape and to join forces on supporting and promoting FutureID. This report will summarize the main activities of the partners since project start. In future editions, it will be updated every six months to cover new developments in this field.

For better readability, the activities are structured along standardization bodies and their working groups.

6. Standardization Bodies

6.1 International Civil Aviation Organisation (ICAO)

The International Civil Aviation Organization (ICAO) has set up a program on Machine Readable Travel Documents (MRTD) such as ePassports. This program is supported by the Technical Advisory Group on MRTD (TAG/MRTD) which consists of government and private sector experts and is appointed by the ICAO Secretary General. TAG/MRTD has the following tasks [ICAO]:

- establish policy recommendations and proposals and
- develop, establish and maintain MRTD standards and specifications

TAG/MRTD has two working groups:

- "The New Technologies Working Group (NTWG): responsible for research, analysis and reporting on new technologies available today or in the future for use in MRTDs, including the development of MRTD specifications contained in Document 9303; and
- The Implementation and Capacity Building Working Group (ICBWG): assists the Secretariat and its international and regional partners in implementing all the education, promotion, assistance and capacity building demands channeled through the ICAO Secretariat." (source: [ICAO])

For the participation of FutureID partners in these groups see Figure 1.

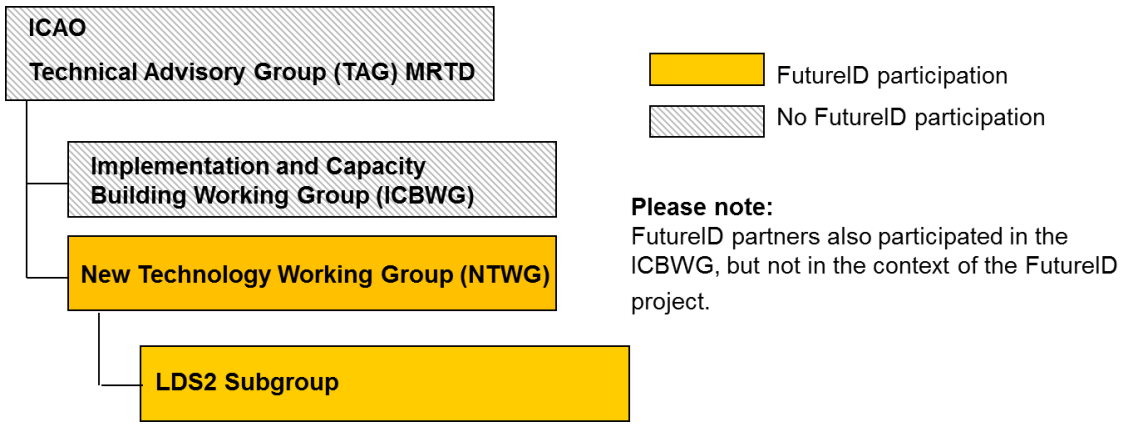

Figure 1 FutureID partner standardization activities in ICAO

For the development of standards and specifications TAG/MRTD has a liaison with ISO/IEC JTC 1 / SC17 / WG3; see clause 6.2.1. Required standards and specifications are often drafted by WG3 (and also other ISO/IEC standardization bodies) according to the TAG/MRTD requirements in coordination with the NTWG. These specifications are finally approved by TAG/MRTD. For a list of ICAO approved standards and specifications on MRTDs please refer to [ICAO Download].

A current work topic is the second version of the Logical Data Structure (LDS2) which supports in addition to LDS1 the following use cases; see [TAG/MRTD/21-WP/6]:

- Travel Stamps (Entry / Exit Records)
- Visa
- Additional Biometrics for facilitated travel programs

For the authorization to write LDS2 data and to read additional biometrics the Extended Access Control (EAC) protocol shall be applied.

Many national eID cards used as secure token follow the ICAO standard in terms of security, logical data set and biometric data. Examples are Monaco, Lithuania, Sweden, Kosovo, Germany, The Netherlands, Albania, Turkey and until 2015 Italy.

In the reporting period the following ICAO meetings were attended by FutureID partners:

- ICAO NTWG, 15.-17. October 2013, Berlin, Germany
- ICAO NTWG LDS2 sub workgroup meeting, 13.-14. January 2014, The Hague, Netherlands
- ICAO TAG22 meeting, 21.-23. May 2014, Montréal, Canada

Based on the last TAG meeting ICAO will publish a new version 0.9 of the Technical Report "Logical Data Structure 2.0 – Optional Expanded Chip Functionality". Two protocol aspects are defined: writing data in LDS2.0 with EAC and reading data from LDS2.0 with Supplemental Access Control, i.e. the PACE protocol.

6.2 ISO/IEC JTC 1 / SC 17 "Cards and Personal Identification"

The Standardisation Committee (SC) 17 of the ISO/IEC Joint Technical Committee (JTC) 1 is the standardisation body in charge of the fundamental standards in the field of smart card technology. The standards developed by SC17 and its working groups cover among others the card body (WG1), communication protocols for contact (WG4) as well as contactless interfaces (WG8), a standardised command set (WG4), and biometrics for smart cards (WG11). Almost all smart cards deployed make use of these standards including GlobalPlatform and Java Cards

which make use of the standardised communication protocols but often apply proprietary commands.

In addition SC17 standardises applications in the field of ID cards for Machine Readable Travel Documents such as ePassports (WG3 together with ICAO, the International Civil Aviation Organisation) and Driver Licences (WG10). Driver Licences and ePassports are the only types of standardised ID cards that are issued worldwide. For this reason FutureID partners participate in the standardisation of the corresponding smart card applications. The main objectives are

- a harmonisation between these application standards so that the same (security) mechanisms are applied and
- availability of unambiguous standards and test specifications so that implementations become interoperable.

Figure 2 provides an overview over the SC17, its working groups and the participation of FutureID partners. Please note that FutureID partners also participate in ISO/IEC JTC 1 / SC17 itself as well as WG1 and WG8, but not in the context of the FutureID project.

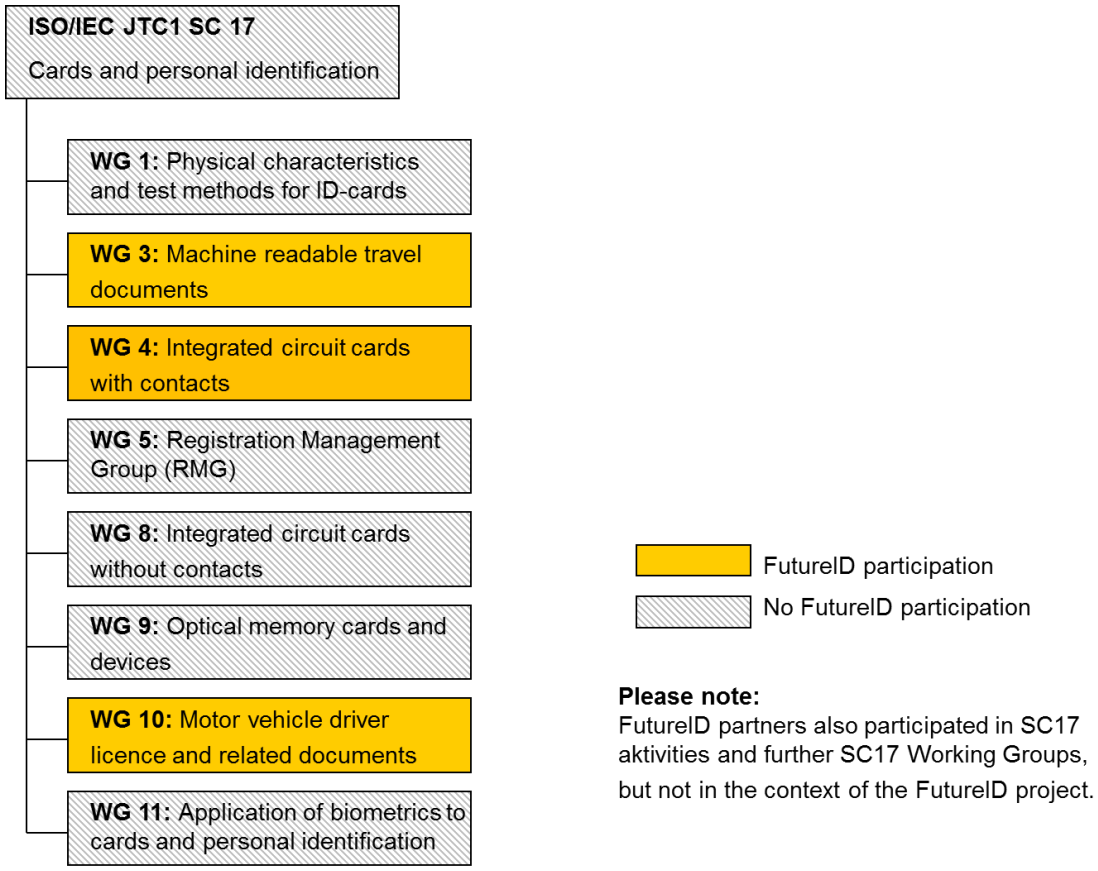

Figure 2 FutureID partner standardization activities in ISO/IEC JTC 1 / SC 17

6.2.1 Working Group 3 "Machine Readable Travel Documents"

Working Group 3 has a liaison with ICAO's TAG/MRTD and works on standards and specifications for Machine Readable Travel Documents (MRTDs); see clause 6.1. WG3 works on many different topics and therefore most of the work is done in Task Forces; see Figure 3 for the WG3 structure and the participation of FutureID partners in the context of this project. Please note that FutureID partners participate also in further Task Forces, but not in the context of the FutureID project as the topics are not relevant for the FutureID project, e.g. the development of a test standard for the durability of the Passport booklet.

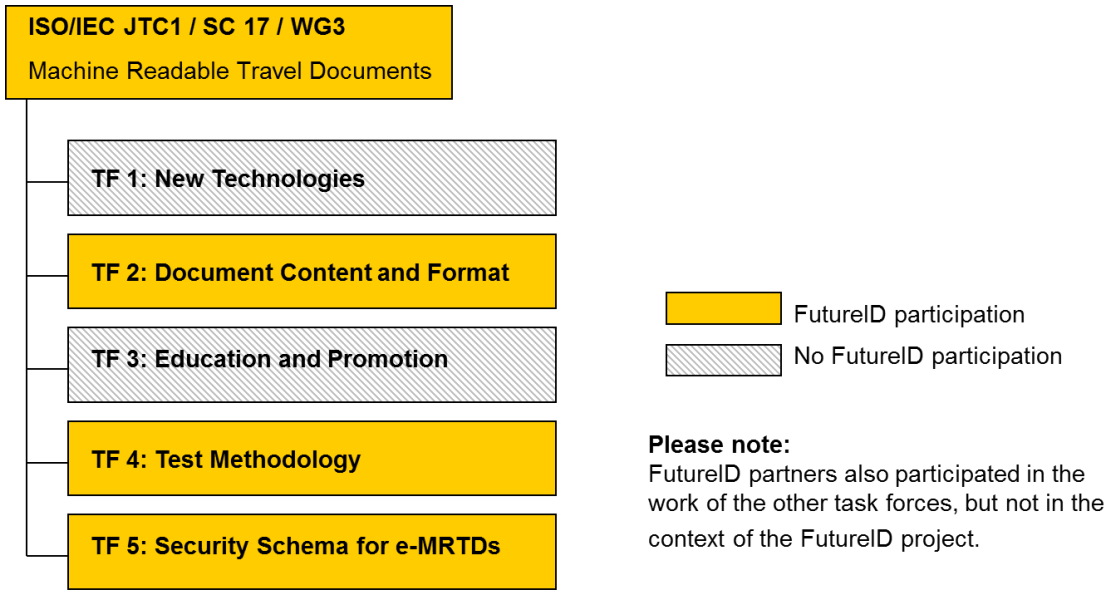

Figure 3 FutureID partner standardization activities in ISO/IEC JTC 1 / SC 17 / WG3

In the reporting period FutureID partners contributed to the following issues:

- Revision of ICAO's Document 9303 (Doc9303): Doc9303 part 1 to 3 is the main specification of ICAO on MRTDs; currently the sixth edition is publicly released [Doc 9303]. The supplement to Doc9303 [Supplement] provides updates and clarifications to Doc9303 and Technical Reports specify further topics. WG3 TF2 is working on the 7th edition of Doc9303 part 1 – 12 which will incorporate the input of the 6th edition, the latest version of the supplement and several Technical Reports. As members of the Review Board FutureID partners reviewed the first draft versions of part 10 and 11 on the Logical Data Structure including basic card mechanisms respectively the security mechanisms such as the cryptographic protocols.
- eMRTD test specifications: To ensure interoperability ICAO publishes also test specifications for eMRTDs which are drafted by WG3 Task Force 4. FutureID partners commented on errors in the test specification for the application protocol and LDS [eMRTD-test-3] which resulted in a new version of the specification. This new version is not yet approved by TAG/MRTD. In addition FutureID partners commented on errors in the EACv1 test specification TR-03105-3.2 (version 1.3) that is used for European eMRTDs. Some of these comments have been resolved in the update of the test specification [TR-03105-3.2].
- Contributions in TF5 to the latest versions of the supplement [Supplement] and the latest version of the Technical Report on Supplemental Access Control [TR-SAC] which has been approved by TAG/MRTD. Compared to the previous version this Technical Report specifies an additional flavor of the PACE protocol that provides not only a key agreement between

the chip and the reader, but also an authentication of the eMRTD chip in the same protocol (PACE with Chip Authentication Mapping PACE-CAM).

In the reporting period FutureID partners actively participated in the following ISO/IEC JTC1 / SC17 / WG3 and joint task force meetings:

- 04.06.2013 – 06.06.2013, London, United Kingdom
- 30.09.2013 – 02.10.2013, Singapore
- 14.04.2014 – 16.04.2014, Tokyo, Japan

6.2.2 Working Group 4 "Integrated Circuit Cards with Contacts"

While the name of the group suggests that WG4 is only working on contact oriented cards, WG4 actually works on the fundamental card issues of contact as well as contactless cards with the exception of contactless communication protocols which are standardized in WG8. One work item that was initiated in 2010 deals with **ICC managed devices**, i.e. devices which are under the control of the ICC's IC. These devices may reside on the card itself or outside the card, e.g. in a mobile phone. Examples are devices for

- input and / or output purposes such as keypads, (touch) displays, microphones, loudspeakers,
- communication purposes such as LEDs and optical sensors,
- support purposes such as power supplying devices (e.g. batteries)

WG4 develops the [ISO/IEC 18328] standard series in the context of this work item. This series as well as related standards and specifications will allow the support of use cases in a standardized and secure way, e.g.

- Display the data to be signed on an ICC's display or a display under the control of the IC
- Use dynamic values for the Card Access Number in the context of the PACE protocol. (This number is currently static and printed on the card body.)
- Secure PIN/password entry

Another work item that was initiated in 2013 deals with **ICC protocols and services ensuring privacy**. The use cases and requirements specified in WG10 for next generation Driving Licenses will serve as input for this new work item. WG4 will specify protocols that can be adopted by different applications. A FutureID partner has started discussions also on privacy credentials in this work item.

In the reporting period FutureID partners participated in the following ISO/IEC JTC 1 / SC 17 / WG4 meetings and contributed to the development of the standard series:

- 27.01.2014 – 31.01.2014, London, United Kingdom

Please note that further FutureID partners attend the WG4 meeting regularly and also act as editor for the ISO/IEC 18328 standard series, but not in the context of the FutureID project. Nevertheless also these FutureID partners disseminate the FutureID requirements and results in their WG4 contributions.

6.2.3 Working Group 10 "Motor vehicle driver licence and related documents"

ISO/IEC JTC1 SC17 WG10 "Motor vehicle driver licence and related documents" works in the field of Motor vehicle driver licences standardization with and without a chip. The standard series [ISO/IEC 18013] covers the following parts:

- Part 1: physical document including layout and physical security features
- Part 2: machine readable technologies including logical data structure of the card application
- Part 3: protocols for access control, data integrity and verification that the chip is authentic which must be supported by the card operating system / the card application
- Part 4: test cases for part 2 and 3

For the FutureID project the Logical Data Structure (LDS) and the cryptographic protocols are relevant, especially as Driver's Licences are the most widely issued ID cards – although not yet with a chip. The card body topics are out of the scope of the FutureID project.

FutureID partners actively contributed to the group with the following objectives:

- Harmonization of the cryptographic protocols standardized in WG10 and WG3 for Driver's Licenses respectively eMRTDs
- Harmonization of the EU Driving License and the ISO/IEC 18013 series
- Error correction in ISO/IEC 18013-3 and ISO/IEC 18013-4
- Privacy for the future international driver’s license with a current focus on use cases and requirements

Harmonisation of the cryptographic protocols for Driver Licences and eMRTDs

The use case "electronic inspection of a Driver's Licence" corresponds to the use case "electronic inspection of an electronic Machine Readable Travel Document" (eMRTD, e.g. an ePassport), but Driver's Licences and eMRTDs apply different cryptographic protocols: While the ISO/IEC 18013 series specifies the Basic Access Protection (BAP) with 4 configurations and the Extended Access Protection (EAP) protocol, eMRTDs make use of Basic Access Control (BAC)

which corresponds to BAP configuration 1, Password Authenticated Connection Establishment (PACE) and in Europe also Extended Access Control version 1(EACv1). An initiative has been started in WG10 to adopt the eMRTD protocols (EACv1, PACE) for Driver Licences by means of Amendment 2 "Extended Access Control v1" and Amendment 3 "PACE" to ISO/IEC 18013-3. This initiative is in line with the adoption of the EACv1 protocol instead of EAP for the European Driving Licence, see below.

The EACv1 Amendment on ISO/IEC 18013-3:2009 is finalized and will be published by ISO. For the draft of the PACE Amendment a subset of the PACE protocol as specified by ICAO's [TR-SAC] has been chosen for driving licences.

In addition an amendment to the test standard ISO/IEC 18013-4 for the EACv1 and the PACE protocol is under development. FutureID partners actively supported this initiative by preparing a first draft of ISO/IEC 18013-4 Amendment 1 for EACv1. This amendment may also be used for functional tests of the European Driving Licence in order to issue the required Functional Certificate, see [EU 383/2012].

This harmonization between Driver Licenses and eMRTDs will help to reduce the complexity and variety of the ID card standardization landscape and make the realization of the FutureID objectives more realistic. The WG10 documents on EACv1 and PACE refer to the eMRTD documents and only specify the differences in order to avoid that these protocols evolve independently for Driving Licenses and eMRTDs and become incompatible in the future.

Harmonization of the EU Driver License and ISO/IEC 18013

The EU Driving Licence as specified in the directives [EU 383/2012], [EU 2011/94/EU] and [EU 2006/126/EC] is not compliant to the existing ISO/IEC 18013 standard series, but specifies several deviations, e.g. the EACv1 protocol is used instead of EAP and data groups (files) contain other data. As already mentioned WG10 is working on the adoption of the EACv1 protocol including a test specification. In addition WG10 started to work on a Technical Report (not standard!) for the EU Driving Licence which will point out the differences to the standard and also specify the changes required in the ISO/IEC 18013-4 test standard so that this test standard can also be applied to an EU Driving Licence as required by the directive [EU 383/2012]. This activity will reduce the differences between the EU Driving Licence and the international standard and help to ensure that implementations of the EU Driving Licence are compliant to the EU directives.

Mobile Driving Licence

Since springtime SC17 WG10 TF14 (Mobile Driving Licence) has start the standardization work on driving license data set stored and displayed in mobile devices such as smart phones. This request was triggered from two states in the US, Florida and Georgia. A 1st principal scheme for one possible solution on the overall architecture was shown along SECURE DOCUMENT WORLD conference in May in London. The standardization work is at this time in a very early work phase. Various technical options are in discussion.

Error correction in ISO/IEC 18013-3 and ISO/IEC 18013-4

For the fulfilment of FutureID objectives unambiguous standards and implementations that are compliant to these standards are of vital importance. For this reason FutureID partners have reported several errors and ambiguities in the ISO/IEC 18013 standard part 3 and 4 by means of Defect Reports. These defects have been resolved in the reporting period and Technical Corrigenda of the standard have been published.

Privacy

FutureID is driving the discussions related to privacy of future ISO/IEC international driver's licenses. This has so far addressed an elaboration of use cases from which requirements have been derived. The latest result is a draft document on requirements related to current and future use cases for the international driver's license. This document serves as input for the new WG4 work item on ICC protocols and services ensuring privacy [ISO/IEC 19286].

In the reporting period the following ISO/IEC JTC1 / SC17 / WG10 meetings were attended by FutureID partners:

- 27.02.2013 – 01.03.2013, Kahului, USA
- 17.06.2013 – 19.06.2013, Gémenos, France
- 30.09.2013 – 02.10.2013, Singapore
- 25.02.2014 – 27.02.2014, San José, Costa Rica
- 16.06.2014 – 17.06.2014, Berlin, Germany

In addition FutureID partners participated in Task Force conference calls in between the meetings.

6.3 ISO/IEC JTC 1/SC 27 "IT Security techniques"

This ISO SC is titled “IT Security techniques” and comprises 5 Working Groups. FutureID is contributing to Working Groups 2 “Cryptography and security mechanisms” and 5 “Identity management and privacy technologies” of ISO/IEC JTC 1/SC 27 in the context of privacy-preserving identity management. A Joint Study Period on “A privacy-respecting identity management scheme using attribute-based credentials” has been started. A first call for contributions for this Joint Study Period ends on August 1, 2014 and will be responded to with a contribution from a FutureID partner.

The intention of the contributions in WGs 2 and 5 is to bring privacy credentials closer towards practice.

6.4 European Mandate M/460 – Electronic Signature

Mandate M/460 is a European Commission initiative, backed by the member states, to deliver a coordinated response on the subject of the deployment of European Digital Single Market. Signatures, identification and secure electronic authentication should help securing e-business transactions and e-services in Europe.

The aim of the Mandate is to create the conditions for achieving the interoperability of eSignature at a European level, by defining and providing a rationalized European eSignature standardization framework. Electronic signature, as standardized in this mandate, are a core functionality to eIDs and thus important to FutureID. A harmonized framework of standards for electronic signatures makes integration of signature implementations, which follow these standards, easier.

In the context of the European Mandate M/460 FutureID partners are members of the ETSI Specialist Task Force (STF) 457 and 458 and are involved in creating the following European Norms and specifications:

- [ETSI EN 319 102] Electronic Signatures and Infrastructures (ESI) – Procedures for Signature Creation and Validation: This draft specifies procedures for creating (Advanced) electronic signatures and establishing whether an (Advanced) electronic signature is technically valid with special consideration on signature validation of "old" electronic signatures, where certificates may have expired or been revoked or even the usage period of algorithms have been exceeded. It does so by capitalizing on security measures that have been applied by e.g. the signer or previous verifiers and ensures that such signatures still can be validated.
- [ETSI PSR4ESCV] Policy and Security Requirements for Electronic Signature Creation and Validation: This document provides general security and policy requirements that should be considered when implementing Signature Creation Applications (SCA) and

Signature Validation Applications (SVA). The goal of the document is to help on one hand the developer of such an application to implement all critical points and on the other hand an evaluator (for a self-evaluation or an evaluation by a third party) to have a list of criteria against which to check the implementation.

- [SR 019 020] Advanced Electronic Signatures in Mobile Environment: The present document provides the framework for further standardisation for the creation and validation of advanced electronic signatures (AdES) in mobile environments (i.e. in environments where mobile devices are supported by networked services for signature creation and/or validation) taking into account recent improvements in the capabilities of mobile devices and their overlap with the capabilities of other computing devices. It identifies the recommended scope of such standards and any suggested provision thought appropriate to these standards.

Members of the FutureID-consortium also actively commented on published drafts to help ensuring their correctness as well as that needs of FutureID are met.

In the reporting period the following ETSI ESI meetings were attended by FutureID partners:

- ETSI ESI #43, Barcelona, Spain, May 5-7
- ETSI ESI Meeting on the Impact of the EIDAS-Regulation, Milan, Italy, April 22-23
- ETSI ESI #42, Vienna, Austria, Feb. 3rd-5th 2014
- ETSI ESI #41, London, United Kingdom, Nov. 18-20, 2013
- ETSI ESI #40, Bilbao, Spain, Sept. 16-18, 2013
- ETSI ESI #39, Miedzyzdroje, Poland, June 3-5, 2013
- ETSI ESI #38, Barcelona, Spain, Mar 11-14 2013

The new eIDAS regulation on e-services and e-signature cross border has passed the EU Parliament on 3rd of April 2014 and the EU Council on 23rd of July. Since springtime 2014 the smart security industry is creating a new European Citizen Card Profile along the eIDAS-token-specification in CEN TC224 WG15.

6.5 GlobalPlatform Card Specification Working Group

GlobalPlatform [GP]describes itself as "*a cross industry, non-profit association which identifies, develops and publishes specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology. GlobalPlatform's objective is to create a standardized infrastructure that accelerates the deployment of secure applications and their associated assets, such as data and cryptographic keys, while protecting them from physical or software attacks*" (source: GlobalPlatform homepage).

The GlobalPlatform Task Forces specify requirements which serve as input for the working groups of the GobalPlatform Committees which prepare technical specifications. The GlobalPlatform Card Committee prepares specifications for Secure Elements such as smart

cards, the Device Committee specifies Trusted Execution Environments for Mobile Devices and the Systems Committee specifies the corresponding background systems, see Figure 4.

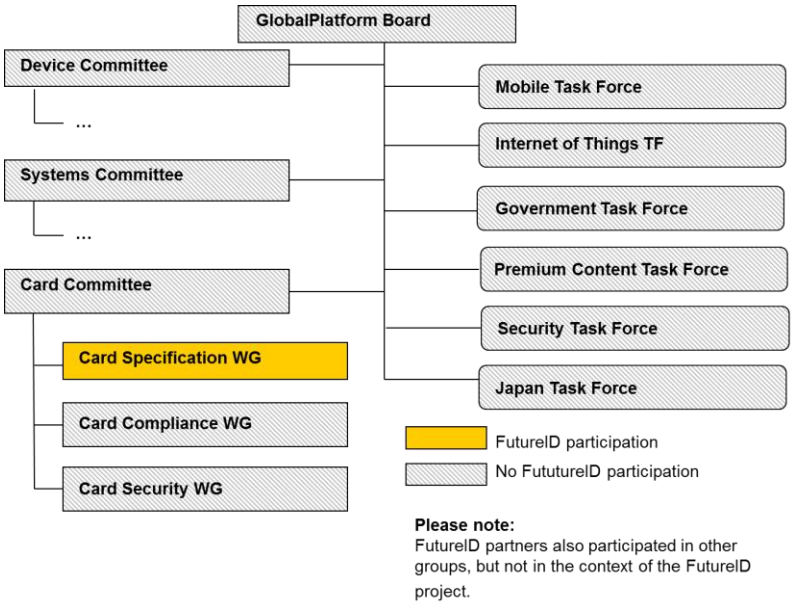

Figure 4 FutureID partner standardization activities in GlobalPlatform

The GlobalPlatform Government Task Force has specified requirements for supporting privacy friendly mechanisms on a GlobalPlatform compliant smart card [GP Privacy Req]. Based on these requirements the GlobalPlatform Card Specification Working Group enhances the GlobalPlatform Card Specification by a privacy framework that prevents leakage of privacy relevant information and provides support for the PACE as well as the EACv1 and EACv2 protocols. This framework is supposed to make the implementation and deployment of applications easier which make use of these protocols.

The group is currently working on a Committee Draft of the Privacy Framework [GP Privacy Framework].

In the reporting period the following GlobalPlatform Card Specification Working Group meetings with the privacy framework on the agenda were attended by FutureID partners:

- 23.06.2014 – 25.06.2014, Munich, Germany

In addition FutureID partners participated in conference calls concerning the privacy framework. Please note that other GlobalPlatform Card Specification Working Group topics are out of the scope of the FutureID project.

7. Summary/Conclusions

The **harmonization of existing ID card standards** is progressing rather well: Stable drafts amendments for the EACv1 and the PACE protocol that are already used for eMRTDs are available for the ISO/IEC Driving Licenses standard. In addition a very first draft for an EACv1 amendment of the ISO/IEC Driving License test standard is available. For the PACE protocol no draft amendment of the ISO/IEC Driving License test standard is yet available. These amendments refer to the existing eMRTD specifications and only specify the differences for Driving Licenses. The optimal solution would be to have a common protocol and test standard for EACv1 as well as PACE which could be applied to eMRTDs, Driving Licenses and other ID cards without any changes. This solution seems currently not to be feasible as several standardization bodies and other parties are involved with different rules and regulations. This makes it difficult to agree on a common standard, to correct errors in time and to include further developments.

In addition Defect Reports and comments on errors and ambiguities in existing standards including test standards have been filed and partially already accepted, so that new versions and Technical Corrigenda have been published. Other comments still have to be resolved. More comments will probably follow.

The **standardization of privacy friendly techniques** for next generation ID cards has been started: Use cases and requirements for Driving Licenses have been systematically collected and specified. Use cases and requirements for other document types still have to be collected and specified. The standardization of privacy friendly techniques for ID cards has only just begun and experience has shown that it will take years to see a published standard. On the positive side the lessons from existing conflicting ID card standards have been learned: The privacy friendly techniques will not be standardized separately for different types of ID cards, but there will be a common standard and the different types of ID cards can build upon this standard.

The **standardization of IC managed devices** is going on for a while and makes progress. There is a lot of interest from other standardization bodies such as GlobalPlatform in this ISO/IEC standard which is a very good sign for the acceptance of this standard.

8. References

[Doc 9303] Machine Readable Travel Documents – 6th edition, 2006, International Civil Aviation Organization, Part 1 – 3, see http://www.icao.int/Security/mrtd/Pages/Document9303.aspx

[eMRTD-test-3] Technical Report – RF Protocol and Application Test Standard for eMRTD – Part 3: Tests for Application Protocol and Logical Data Structure, ISO/IEC JTC1 SC17 WG3 TF4 for ICAO, see http://www.icao.int/Security/mrtd/Pages/Technical-Reports.aspx for the released versions

[ETSI EN 319 102] Electronic Signatures and Infrastructures (ESI) – Procedures for Signature Creation and Validation, ETSI, 15.12.2013, public draft

[ETSI PSR4ESCV] Policy and Security Requirements for Electronic Signature Creation and Validation, draft, February 2014

[EU 2006/126/EC] Directive 2006/126/EC of the European Parliament and the Council of 20 December 2006 on Driving Licences (Recast)

[EU 2011/94/EU] Commission Directive 2011/94/EU of 28 November 2011 amending directive 2006/126/EC of the European Parliament and of the Council on driving licences

[EU 383/2012] Commission Regulation (EU) No 383/2012 of 4 May 2012 laying down technical requirements with regard to driving licences which include a storage medium (microchip), European Commission

[GP] GlobalPlatform homepage, see http://www.globalplatform.org/

[GP Privacy Framework] GlobalPlatform Card Technology, Card Specification – Privacy Framework, draft

[GP Privacy Req] GlobalPlatform Government Task Force – Privacy Framework Requirements, Version 1,0, January 2013, see http://www.globalplatform.org/documents/GP_PrivacyFrameworkRequirements_v1.0.pdf

[ICAO] ICAO homepage, see http://www.icao.int/

[ICAO Download] ICAO approved standards and specifications on MRTDs, see http://www.icao.int/Security/mrtd/Pages/Downloads.aspx

[ISO/IEC 18013] Information technology – Personal Identification – ISO compliant driving licence

Part 1: Physical characteristics and basic data set, 2005

Part 2: Machine-readable technologies, 2008 and Technical Corrigendum 1, 2011

Part 3: Access Control, authentication and integrity validation, 2009
Technical Corrigendum 1 2011
Technical Corrigendum 2 2013
Amendment 1 Scanning Area Identifier – Optional machine readable zone
Amendment 2 Extended Access Control v1 (awaiting publication)
Amendment 3 PACE (draft)

Part 4: Test methods 2011
Technical Corrigendum 1, 2013
Amendment 1 EACv1, PACE and one-line MRZ (draft)

Technical Report: Differences between ISO/IEC18013 and EU Driving Licence (draft)

[ISO/IEC 18328] Identification cards – ICC-managed devices -
Part 1: General framework (draft)
Part 2: Physical characteristics and related test methods (draft)
Part 3: Organisation, security and commands for interchange (draft)

[ISO/IEC 19286] Identification cards – Integrated circuit cards – Protocols and services ensuring privacy, Working Draft

[SR 019 020] Advanced Electronic Signatures in Mobile Environment, ETSI, November 2013, Version 0.0.3p draft

[Supplement] Supplement to Doc 9303, ISO/IEC JTC1 SC17 WG3 for the International Civil Aviation Organization, see http://www.icao.int/Security/mrtd/Pages/Document9303.aspx for the released version

[TAG/MRTD/21-WP/6] Revision of the Logical Data Structure Technical Report - Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) – Twenty First Meeting – Montréal, 10 to 12 December 2012

[TR-SAC] Technical Report Supplemental Access Control for Machine Readable Travel Documents, ISO/IEC JTC1 SC17 WG3 TF5 for the International Civil Aviation Organization, see

http://www.icao.int/Security/mrtd/Pages/Technical-Reports.aspx for the released version

[TR-03105-3.2] Machine Readable Travel Documents – Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control v1 (EACv1), Tests for Security Implementation, Bundesamt für Sicherheit in der Informationstechnik, AFNOR, see https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03105/index_htm.html