CEF DIGITAL
European Commission

DG CONNECT
Digital Single market

eIDAS
Cooperation Network

Peer Review DE

PEER REVIEW REPORT – German eID

Version :	V1.0
Status :	Final
Dissemination Level :	Coordination Network
Due date of peer review report :	16th June 2017
Actual submission date :	Date of submission to EC (after the opinion of the CN on 28 June 2017)
Organisation name of lead partner for this peer review report:	Freek van Krevel (NL)
Experts participating:	AT (R. Posch, P. Kustor, E. Aigner, H. Leitold, A. Tauber. D. Klauser, G. Ebil, A. Banfield-Mumb-Mülheim, B. Karning, G. Schmied), BE (C. Mahieu, F. Leysens, L. Wijns, J. Colpaers, G. Vanlint), BG (S. Kirov, I. Nedelcheva), CZ (P. Tiller, R. Piffl), DK (M. Park Andersen), EE (A. Mõltik, S. Leskov, V. Kaljukivi, A. Poola, R. Süld, M. Heidelberg, L. Kask, E. Adams, M. Erlich, M. Arm, M. Pedak), EL (A. Stasis, L. Demiri, V. Kalogirou, D. Kontogioris, V. Dalakou), ES (F. José Jara González, J. Crespo, R. Perez Galindo, E. de la Calle Vian, C. Gómez Muñoz), FR (C. Anderson, R. Santini, E. Jaulmes, V. Lancino, Q. Dusoulier, Y. Tourdot, H. Pujol, C. Menseau), HR (D. Bozic, B. Zeba, M. Loborec. J. Sulik), IT (S. Arbia, A. Florio, S. Ianniello), LI (M. Skarohlid, S. Näscher) LT(V. Krasauskas, D. Vezikauskiene, A. Kudalevas), LU (L. Antunes, D. Struck), LV (E. Vismanis, U. Aptis, I. Balodis, G. Zarins, D. Telnovs, K. Teters), MT (A. Camilleri), NL (B. Hulsebosch, J. Verschuren, H. Congleton), NO (J. Berge Holden, T. Alvik, J. Binningsbo), PL (R. Poznanski), SE (F. Ljunggren, M. Dandoy) , SI (A. Žužek Nemec, S. Zorc, D. Petrović, A. Pelan, R. Ponikvar), SK (R. Magna, J. Hruz), UK (A. Cooper, J. White, Katherine Attwood, C. Porteous)
Partner(s) contributing :	AT, BE, CZ, DK, EE, EL, ES, FR, HR, IT, LI, LT, LU, LV, NL, NO, PL, SE, UK

Abstract:

In line with the European Commission's aims to set up a Digital Single Market and to increase trust in digital services, the eIDAS Regulation 910/2014 seeks to enable European citizens to carry out transactions electronically and adopt new services. This peer review process report provides observations on the German electronic identification (eID) scheme. Consistent with the eIDAS regulation, Member States have formulated an opinion on the German eID through examining documentation on the scheme and through interaction with German experts on the scheme. Various aspects have been studied in depth to come to a well-founded conclusion on the reliability of the German eID in the eIDAS infrastructure. Those aspects concern the following elements: enrolment, electronic identification means management and authentication, middleware and management and organisation. Participating Member States (MSs) of this peer review have concluded that the declared Level of Assurance (LoA) high, complies with the eIDAS Implementing Regulation 2015/1502 and therefore have sufficient trust in the German eID to use it in the eIDAS infrastructure.

Executive Summary

In line with the European Commission's aims to set up a Digital Single Market and to increase trust in digital services, the eIDAS Regulation 910/2014 seeks to enable European citizens to carry out transactions electronically and adopt new services. This peer review report provides observations on Germany's eID scheme by participating Member States.

The eIDAS Regulation 910/2014 seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities. The Regulation will increase the effectiveness of public and private online services, electronic business and electronic commerce in the Union. As celebrated by Vice-President of the European Commission Andrus Ansip in his correspondence to Member States on 4th May 2017, Germany is the first country to pre-notify their eID scheme. According to Vice-President Ansip Germany is also the first Member State to take the major step to move "from a patchwork of national online markets to an integrated Digital Single Market, where commercial and public services can flow easily and seamlessly across borders and therefore make the most of the opportunities brought by digitisation."

Consistent with the regulation other Member States have volunteered to engage in a process of peer review. As outlined in Article 7 of the eIDAS Implementing Decision 2015/296 peer review acts as "a mechanism for cooperation between Member States designed to ensure interoperability and security of notified electronic identification schemes." This report provides the conclusions of this peer review of Germany's eID scheme covering aspects ranging from enrolment, electronic identification means management and authentication, middleware and management and organisation.

The objective of this document is to provide information about the peer review process and to enable the Cooperation Network to provide an opinion on the German electronic identification scheme and its interoperability and security. The peer review process should be considered as a mutual learning process that helps to build trust between Member States. This document contains observations and a conclusion made by experts of participating Member States in the peer review. Therefore this peer review process report can be seen as a starting point to establish trust in the German electronic identification scheme in relation to the eIDAS infrastructure.

Main topics

This document has been categorised into four topics. This has been done to cluster subjects and to assure that the experts only have to formulate an opinion on their area of expertise. Regarding the first topic about enrolment the following aspects of the German eID have been reviewed: identity proofing procedures, controls, document acceptation, delivery and activation, legal representation, information material / terms & conditions, pseudonyms and document numbers.

For the topic eID means management and authentication the following subjects have been discussed: unique identifier, how the revocation and reactivation system works, ID means characteristics and cryptography. Since a pseudonym is linked to an ID card and not to a person, information was provided regarding the linking of the existing records of citizen to a new

pseudonym for relying parties. It was explained that for sector relying parties of a receiving Member State the same pseudonym is created even if multiple middleware instances are operated.

The third topic, middleware, consists of the following subjects: deployment, documentation, and maintenance, responsibilities and security and access certificates and private sector relying party deployment. Two options are available for MS to implement the middleware: either the middleware is bundled by CEF/DIGIT together with its eIDAS node reference node implementation, or a virtual machine (VM) can be provided including the eIDAS middleware

For the fourth topic, management and organisation, the peer review has been focused on gaining insight into how all participants providing services related to the eID scheme in a cross-border context have in place documented information security management practices, policies, approaches to risk management, and other recognised controls, so as to provide assurance (commensurate to LoA high) that effective controls are in place.

As a conclusion based on the complete provided documentation and on the convincing answers received for the four topics above the experts participating in this peer review trust in the level of assurance the German eID scheme proclaims it has, LoA high, and that this eID scheme complies with the eIDAS Implementing Regulation 2015/1502.

The next step is for the rapporteurs and coordination team to present the peer review report on the German eID scheme for the Cooperation Network. After this presentation the German eID scheme can officially be notified.

Content

List of Abbreviations

Abbreviation	Explanation
AufenthG	Residence Act (Aufenthaltsgesetz)
AufenthV	Ordinance Governing Residence (Aufenthaltsverordnung)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CN	Cooperation Network
COM	European Commission
eAT-PP	BSI: Common Criteria Protection Profile BSI-CC-PP-0069 Electronic Residence Permit Card (RP_Card PP)
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
eIDAS Arch	eIDAS Technical Subgroup: eIDAS Technical Specifications – Interoperability Architecture
eIDAS Attributes	IDAS Technical Subgroup: eIDAS Technical Specifications – Attribute Profile
eIDAS CN	European Commission implementing decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
eIDAS IF	European Commission implementing regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
ePA-PP	BSI: Common Criteria Protection Profile BSI-CC-PP-0061, Electronic Identity Card (ID_Card PP)
EU	European Union
ICAO 9303	ICAO: Doc 9303, Machine Readable Travel Documents, Part 3
IF Mapping	BSI: German eID based on Extended Access Control v2 – Fulfilment of interoperability requirements according to (EU) 2015/1501
ISO/IEC 14443	ISO/IEC: ISO/IEC 14443 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards
ISO/IEC 7816	ISO/IEC: ISO/IEC 7816 – Identification cards – Integrated circuit cards
LoA	Level of Assurance

LoA Mapping	BSI: German eID based on Extended Access Control v2 – LoA mapping
MRED	BSI: Common Criteria Protection Profile BSI-CC-PP-0087, Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP)
MS	Member States (of the EEA)
MW	Middleware
PauswG	Act on identity cards and electronic identification (Personalausweisgesetz)
PauswG_AMD	Government draft for an Act on the promotion of electronic identification
PauswV	Ordinance on identity cards and electronic identification (Personalausweisverordnung)
PP-Chip	Eurosmart: Security IC Platform Protection Profile, BSI-PP-0035
PP-IS	BSI: Common Criteria Protection Profile for Inspection Systems, BSI-CC-PP-0064
PP-0083	BSI: Common Criteria Protection Profile BSI-CC-PP-0083 Standard Reader – Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control
VM	Virtual machine

List of Country Codes

Country	Country code	Country	Country code
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Latvia	LV
Czech Republic	CZ	Luxembourg	LU
Cyprus	CY	Hungary	HU
Denmark	DK	Malta	MT
Germany	DE	Netherlands	NL
Estonia	EE	Norway	NO
Greece	EL	Poland	PL
Spain	ES	Portugal	PT
Finland	FI	Romania	RO
France	FR	Sweden	SE
Croatia	HR	Slovenia	SI
Ireland	IE	Slovakia	SK
Italy	IT	United Kingdom	UK

History

Version	Date	Changes made	Modified by
0.1	19.05.2017	Update paragraphs	Hanna Congleton
0.2	23.05.2017	Revisions + lay-out	Katherine Attwood, Hanna Congleton & Freek van Krevel
0.4	23.05.2017	Revisions conference call	Hanna Congleton
0.5	24-05-2017	Revisions based on comments rapporteurs and COM	Hanna Congleton
0.6	29-05-2017	Revisions based on input rapporteurs	Fabrice Leysens, Herbert Leitold, Fredrik Ljunggren, Katherine Attwood, Hanna Congleton
0.7	31-05-2017	Revisions based on comments rapporteur	Hubert Pujol
0.8	01-06-2017	Revisions/editorial remarks Coordination Team	Katherine Attwood, Freek van Krevel
0.9	14-06-2017	Revisions based on review cycle and input rapporteurs	Fabrice Leysens, Herbert Leitold, Hubert Pujol, Fredrik Ljunggren, Hanna Congleton
1.0	16-06-2017	Revisions based on extra information given by Germany	Fabrice Leysens, Hanna Congleton

1. Introduction

1.1 Scope and Objective of Peer review report

Objective

Peer review is a mechanism for cooperation between Member States designed to ensure interoperability and security of notified electronic identification schemes.[1] The specific objective of the present peer review process is to enable the Cooperation Network to provide an opinion on the German electronic identification scheme and its interoperability and security[2].

The peer review process should be seen as a mutual learning process that helps to build trust between Member States. Since trust in the eIDAS architecture will be based on confidence of MSs in eID architecture schemes, it is vital to have a successful notification of national eID architectures.

Experts of participating MS have identified areas of interest and reported their observations in this document. Based on those observations, information is gathered by rapporteurs on each topic and an overview of interesting matters is provided. The German eID scheme has been discussed in depth and the input of German experts have been required for any questions about the German eID infrastructure.

The peer review aims to come to observations on the level of trust that is experienced by other Member States concerning the assurance level of the German scheme. In other words this peer review report aims to indicate, how the eID means complies with the eIDAS regulation and to discuss the acceptance of the level of assurance of the German eID.

Scope

The security and interoperability of the German eID scheme regarding the eIDAS regulation are in scope for this peer review process. This implies that matters that are an issue only on a national level are out of scope for this peer review. Questions that have gone beyond the scope of the peer review process, have been discussed by the peer review participants because the experts of this peer review believed that this could benefit other MS and the CN.

1.2 Methodology of Work

The scope of the peer review was determined using Article 10, paragraph 3 of the Commission Implementing Decision (EU) 2015/296 which states “peer reviewing may include, but is not limited to, one or more of the following arrangements: (a) the assessment of relevant documentation; (b) examination of processes; (c) technical seminars; and (d) consideration of independent third party assessment.”

As such it was set out in the 6th Cooperation Network meeting on 3 April 2017 that the peer review of Germany’s eID scheme would be led by a team of coordinators, who would then organise

[1] Article 7(1) of COMMISSION IMPLEMENTING DECISION (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

2 Article 14 (i) of the same Decision

Member States around topics of interest. Rapporteurs would be appointed to lead each topic and their observations would be based on: a description of the German eID scheme provided by Germany, a German self-assessment of its eID scheme against relevant requirements of the eIDAS regulation and underlying implementing acts, discussions with technical experts from Germany and a visit to Berlin to participate in technical workshops and working group sessions.

Several Member States have indicated they would like to work across several topic groups, or desired to participate in one topic, and provide input to other topics. Member States could indicate, if they wanted to play an active or a passive role. 'Active' indicates that a MS wishes to contribute actively to the topic in the creation of questions and writing the report. An 'observer' status means that a MS wished to follow the proceedings and offer comments on the report.
As noted in Article 7, paragraph 2 of (EU) 2015/296, "Participation of the peer Member States [is] voluntary. The Member State whose electronic identification scheme is to be peer reviewed may not refuse the participation of any peer Member State in the peer reviewing process". At the 6th Cooperation Network the following Member States expressed interest in participating in the review: AT, BE, CZ, DK, EE, EL, ES, FR, HR, IT, LT, LU, LV, NL, NO, PL, SE and the UK.

From these Member States, three Member States highlighted that they would like to be part of the Coordination Team: FR, NL and UK. As such these Member States have made up the Coordination Team and have organised the logistical and practical aspects of process. They have acted as the contact point for both the European Commission and Germany. Moreover, these countries coordinated messages and facilitated the creation of a working collaborative space alongside the European Commission in which to conduct the peer review. They also coordinated the production of this report and ensured the rapporteurs had enough information from which to draw their observations in their topics.

In terms of topics and areas of interest, four topics were created and rapporteurs assigned. These were arranged as follows:

Topic 1: Enrolment
Rapporteur: Fabrice Leysens (BE)
Active MSs: BE, CZ, FR, EL, HR, LT, LU, LV, NO, SE, UK
Observers: AT, BG, EE, ES, FI, IT, LI, MT, SI, SK

Topic 2: eID means management and authentication
Rapporteur: Herbert Leitold (AT) and Hubert Pujol (FR)
Active MSs: CZ, DK, HR, EE, IT, NL, PL, SE, UK, AT, FR
Observers: BE, ES, FI, LI, LU, LT, LV, NO, SI, SK

Topic 3: Middleware
Rapporteur: Herbert Leitold (AT) and Hubert Pujol (FR)
Active MSs: BE, CZ, EE, IT, NL, NO, SE, UK, AT, FR
Observers: DK, ES, FI, LT, LU, PL, SI, SK

Topic 4: Management and Organisation
Rapporteur: Fredrik Ljunggren(SE)
Active MSs: ES, FR, LU, UK, BE
Observers: EE, FI, IT, LT, SI, HR, CZ, NO, AT

The Coordination team set up a weekly conference call to discuss progress with the Rapporteurs and to ensure any constraints were flagged and could be facilitated. Rapporteurs were able to provide a weekly update on their topics. Any possible areas of overlap have been addressed. It also provided a feedback facility to ensure all members could agree to the outputs and format of the Peer Review document.

Questions on the update mechanism and related information channels have been raised by the peer review panel. The main communication channel supported by the Member State whose electronic identification scheme is to be peer reviewed, was email and was maintained to distribute information on pre-releases, releases and updates.

As part of the Peer Review, Germany also invited participating Member States to travel to Berlin for two days of workshops (including presentations and discussions) at the Ministry of the Interior and a site visit to the Bundesdruckerei. This was particularly useful and insightful and has aided the topic groups to understand in depth and discuss in detail the subject matter in hand. The questions and answers are listed in the appendix.

This report will be submitted to the Cooperation Network in order to discuss the compliance of the German eID scheme in relation to eIDAS and, in particular, the level of assurance it proclaims to have: LoA high.

1.3 Relations to the CN Environment

This peer review process must be seen in the light of the cooperation of the Member States with the exchange of information and sharing of best practices that aims to achieve the mutual recognition that will facilitate “cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.” ((EU) No 910/2014 Recital 9)

Germany is the first Member State to pre-notify their eID scheme and, in doing so, paved the way toward achieving the benefits of the eIDAS regulation. It is vital to note that this report should not be seen in isolation, but instead a step towards achieving the Regulation’s aims.

The participation peer member states have not only gained experience in the German eID solution, but also in conducting a peer review. For conducting this peer review a template, common working space and telephone arrangements have been created.

This way of working could further serve as an example on which to base further peer reviews.

Part of the experience is to have a better notion on the sovereignty aspect, as the aim of the Regulation is not to intervene with regard to electronic identity management systems and related infrastructures established in Member States. Consequently, part of the learning experience is to keep discussions focused on the access to cross-border online services offered by Member States, and in addition the required secure electronic identification and authentication to achieve interoperability.

1.4 Relations to the External Environment: outside CN

The executive summary of this peer review report can be considered as a means to communicate findings of interesting aspects of the German eID scheme in relation to the eIDAS infrastructure. Decision makers, the media and any other stakeholder can use this summary as a source of information regarding the security and interoperability of this eID. It can be seen as a result of an intensive investigation of the eID scheme to support the opinion of the Cooperation Network.

The information provided in the summary of this document will be the foundation of trust of the EEA-countries in the German eID means. With faith in the reliability of this eID a first step is made in the direction of interoperability of the eIDAS infrastructure.

1.5 Quality Management

Category	Remarks	Checked by
Conformance to Peer review eIDAS CN template	OK	F. van Krevel
Language & Spelling	OK	F. van Krevel
Delivered on time	OK	F. van Krevel
Each technology description contains the correct elements	OK	F. van Krevel
Contents is fit for purpose	OK	F. van Krevel
Contents is fit for use	OK	F. van Krevel
Commitment within Member States participating in the peer review	OK	F. van Krevel

Table 2: Quality Checklist

1.6 Legal Issues

When conducting the peer review and producing the report the following legal issues have had to be borne into consideration. As stated in Art. 7, paragraph 4 of the Commission Implementing Decision (EU) 2015/296:

> "Any information obtained through the peer reviewing process shall be used solely for this purpose. Representatives of the Member States conducting the peer review shall not disclose any sensitive or confidential information obtained in the course of the peer review to third parties."

As such rapporteurs have treated such information sensitively and with due confidence and any sensitive or confidential information has been removed from the version of the report that will be published publicly. The peer review did not take into account any classified information.

Equally all experts from Member States had to flag any possible conflict of interest as mandated in Art.7, paragraph 5, Commission Implementing Decision (EU) 2015/296 where it cites "Peer Member State shall reveal any possible conflict of interest which representatives nominated by them to take part of the peer review activities might have."

Finally when determining the scope and arrangement of the peer review, Art. 10, paragraph 3 of the Commission Implementing Decision (EU) 2015/296 was consulted, which posits:

> "Peer reviewing may include, but is not limited to, one or more of the following arrangements: (a) the assessment of relevant documentation; (b) examination of processes; (c) technical seminars; and (d) consideration of independent third party assessment."

1.7 Structure of the document

This peer review has been divided into four topics. During a CN meeting in April the CN cooperation decided on the scope of the peer review by agreeing on what topics and subtopics should be considered while conducting the peer review. Each topic has covered several interesting features of the German eID scheme. The topics will be dealt with by providing a summary of the observations per area.

This report gives an overall description of the main subjects that were discussed within the following four topics, but does not intend to provide all the details given by Germany.
Each chapter summarises the questions and answers in a narrative style in order to provide context to the proposed conclusions.

The topics of the peer review are the following:

1. Enrolment. This topic concerns application, registration, identity proofing and verification of a person and finally binding between the electronic identification means of natural persons.

2. Electronic identification means management and authentication. This is about electronic identification means characteristics, design, issuance, delivery, activation, suspension, revocation, reactivation, renewal and replacement.

3. Middleware: the German eID scheme works through MW.

4. Management and organisation. This topic deals with general provisions on management and organisation, published notices, user information, information security management, record keeping, facilities, staff, technical controls, compliance and auditing.

By combining the information that has been gathered in the topics a conclusion will be formulated.

2. Topic 1: Enrolment

2.1 Purpose of this document

The topic area of, enrolment, mainly covered the following aspects of the German eID scheme

- Identity proofing: procedures, controls, document acceptance
- Delivery and activation
- Legal representation
- Information material / terms & conditions
- Pseudonyms and document numbers

2.2 Scope

2.2.1 Identity proofing

The first subject covered in this topic was related to **identity proofing** processes with a focus on the **resident permit** but not limited to it. In this context Germany has been asked to provide additional information about the **procedures and controls** in place that guarantee someone's identity can be established with a high level of assurance (LoA).

In Germany, different kind of documents can be recognised as *identity evidence*. For foreigners, authorities can verify the presented documents against samples provided in various databases and check the plausibility of the person's information in the *foreigners' records*. Additional methods and procedures to detect fraud are also in place.

If a foreigner's claimed identity cannot be verified with a sufficient degree of certainty the Resident Permits will be issued with no activated certificate. In such a case the electronic identification function will not be available.

Staff at foreigners' authorities responsible for verifying identity documents are trained and can assert that a document is recognized and can provide an initial assessment of possible forgery or falsification. They may also use document readers to detect anomalies.

Remote identification is not allowed.

The answers provided by Germany are satisfactory and the related processes are considered sufficient.

The review panel did however formulate the following observation: it was said during the peer-review meeting that one issuing officer can carry out the whole process of registration, enrolment and issuing of an eID card. Reviewers mention that controls such as the 4-eyes principle or separation of duties could reduce the risk of fraud. However it should also be said that the envelope containing the activation code is not conveyed through the registration office, hence the principle of four eyes could be said to be met as it is independently sent to the applicant (at least for an eID, but not for the physical ID document).

Other questions were related to the **delivery and activation process** *.e.g.* how does an applicant apply for possession of an eID or a resident permit and how is it activated?

For applicants living in Germany a letter with the PIN code is sent to the applicant's address and the ID card or the Resident Permit has to be retrieved at the issuing authority.

For Germans living abroad the procedure may vary depending of the country. In some countries (whitelists maintained by the Foreign Office) cards may be sent to the applicant but never with or within the same envelope as the PIN letter. Additional details have been requested about this exception process rather marginal in the whole eID scheme: it appears that the eID card can only be sent if the applicant has mandated the responsible mission abroad. The delivery is done using registered mail with return receipt to ensure the card is delivered to the applicant

The answers provided by Germany are satisfactory and the related processes are considered sufficient.

The review panel did however make the following observation: when both PIN letter and card are delivered via mail it might increase the risk that a third person could obtain both credentials. Authorities in charge of the maintenance of the whitelist should consider the maturity level (adequate training and qualifications) of the postal services in those countries as a determinant criteria. Facing the very small target group and there are still various certainties to prevent abuse, the risk is negligible.

Members States also had questions about a specific case: under what conditions is **representativeness** allowed when applying for an eID or resident permit and how does it work? Again Germany provided information about the procedures and controls in place.

It can be seen from the provided answers that the German legislation covers cases of minors and other situations involving someone legally incapable where representativeness may apply. Application processes for both type of cards have been considered.

The answers provided by Germany are satisfactory and the related processes are considered adequate.

2.2.2 Application & registration

Beside identity proofing and representativeness Member States have requested some details on how the German authorities guarantee that someone who receives an eID is aware of the terms and conditions related to its use and other **recommended security precautions**.

The answers provided indicate that such aspects are covered by German law. In addition a brochure containing the relevant information and precautions is also available for citizens.

The answers provided by Germany are sufficient and satisfactory.

Finally Member States have requested clarifications about the '**pseudonym**' and identification numbers.

The unique identifier that will be sent with the minimum dataset is a pseudonym cryptographically generated from one "card" and for a specific Service Provider. The pseudonym will change when a new card is delivered (the German eID has a duration limited to 10 years). Each Member State will be considered as a Service Provider and will thus receive its own pseudonym for a same person. The document number will not be sent to other member states.

The answers provided by Germany are satisfactory.

2.3 Conclusion for the Enrolment topic

Member States actively involved in reviewing this topic conclude that the declared LoA - high - complies with the eIDAS Implementing Regulation 2015/1502 for the current topic.

3. Topic 2: Electronic Identification means management and authentication

3.1 Purpose of this document

This chapter addresses questions raised within the topic of electronic identity means management and authentication covering the following aspects of the German eID scheme

- Unique identifier
- How the revocation and reactivation system works
- ID means characteristics and cryptography

3.2 Scope

3.2.1 Unique identifier

One subject raised was the use of **pseudonyms** as unique identifier. The review panel understands that the German eID scheme creates card-specific and application-specific pseudonyms that change for a citizen when an eID card gets replaced. Thus, the unique identifier provided by the German eID scheme is **not lifelong-persistent**, which regardless is not a requirement under the eIDAS regulation.

Questions and discussion during the peer review were mainly to seek clarification on **what optional data is available** and under what conditions some of this data might not be transmitted. Such clarification was sought to get a better understanding on how the **matching with existing records** and the **linking of successive eIDs of a citizen** at the relying party could work.

For the German eID, the minimum data set (first name and family name, date of birth, and unique identifier) is always available, as required by Implementing Regulation (EU) 2015/1501.

As optional data the place of birth is always available. In addition, the address and the birth name can be provided, subject to some considerations to be taken into account by a relying party : the address is mainly meant for postal delivery, less for assisting unique identification. It is only available if the citizen has permanent residence in Germany. The address may change and it can be updated on an existing card if the citizen moves. The birth name is available on ID cards from Q2/2012 onwards and on residence cards from Q4/2014.

While optional data not required for unique identification (e.g. address) may be deselected by the citizen in the authentication process the minimum data set, however, will always be transmitted and authentication would fail if a citizen deselects one of these data fields for the minimum dataset.

Some more specific questions were related to whether auxiliary information is available to assist the reliable linking of a citizen’s pseudonym of a replaced eID with the pseudonym of her predecessor eID.

The explanation by the German colleagues showed that no information in excess of the minimum data set and the optional data exists or may be used for identifying card replacements and thus a change of pseudonyms. However, the minimum data set together with the place of birth as optional data even for bigger cities makes it unlikely that two persons have the same data set, although such cases cannot be excluded.

For public sector relying parties of a receiving Member State the same pseudonym is created even if multiple middleware instances are operated.

The answers provided by Germany are satisfactory and led to the clarification provided above.

3.2.2 Revocation and reactivation

Questions in this area were along two directions: firstly, the review panel sought a better understanding on **how revocation of an eID works**, like if the card gets lost or stolen, what the related processes and its security measures are, and who can initiate such revocation. Secondly, as the German eID scheme allows for **reactivation of a previously revoked card**, the issue was where clarifying explanations are given in the processes and what conditions apply to reactivate.

A German eID can be revoked by the card holder themselves through a hotline or a competent authority. The main protection is to authorise this through a revocation password. The German colleagues pointed to the balance needed between protection against unauthorized revocation by others versus keeping revocation easy for the legitimate eID holder to prevent misuse of his/her eID.

The issuing authority can also revoke the eID if it becomes aware of lost or stolen cards or that the card holder passed away.

Technical details on the revocation system, its security measures, and on distributing the revocation lists to the middleware components were given at the peer review meeting and through accompanying documentation.

The German eID scheme allows reactivation of a revoked card only if the eID holder presents the physical card and if no new card has yet been issued. No time limits for such reactivation are in place.

The answers provided by Germany are satisfactory and the related processes are considered sufficient.

3.2.3 ID means characteristics and cryptography

The review panel received a set of questions on **technical details** meant **to learn and get a better understanding** of the German eID scheme.

The German eID is characterised by end-to-end cryptographic protection for the whole path from the eID card to the middleware operated by the eIDAS connector. Mutual authentication is provided where the eID card verifies an authorisation certificate issued to the middleware operator (at the relying party or a centralised eIDAS connector), vice versa the middleware verifies the eID card. The related PKI has been described in detail in the documentation and was discussed during the peer review. It is comparable and partly identical to the PKI architecture for travel documents.

A set of questions raised by the peer review panel was related to **PIN management**: The process distinguishes a transport PIN to activate the eID once, and an authentication PIN used as second factor to the card, i.e. two-factor authentication by possession (of the card) and by knowledge (of the PIN) is implemented. A PIN Unlocking Key is provided to the card-holder only for resetting the PIN retry counter, but not to set a new PIN. Forgotten PINs can only be reset at specific municipal offices where processes to have the citizen identified by municipal officer are in place.

German eID card chips undergo a **Common Criteria certification** to insure protection against an attacker with high potential. The certification lifecycle ensures that chip-generations get periodically re-certified as long as such chips are being issued. Monitoring of security relevant aspects continues beyond, as the chip has a lifetime of up to ten years. eID clients, i.e. the software used to access the eID card, are certified against national technical guidelines.

The answers provided by Germany are satisfactory and the related processes are considered sufficient.

3.3 Conclusion for the eID means management and authentication topic

Member States actively involved in reviewing this topic conclude that the declared LoA - high - complies with the eIDAS Implementing Regulation 2015/1502 for this topic.

4. Topic 4: Management and organisation

The Working Group (WG) for Topic 4 focuses on the management and organisational aspects in providing assurance on the security of the eID scheme. This topic corresponds to section 2.4 of the implementing regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification. DE has prepared a set of documents for the peer-review, whereas the documents "*Overview of the German eID system*" and "*LoA mapping: Mapping of the characteristics of the German eID scheme to the eIDAS Level of Assurance*" are the most relevant for the WG.

4.1 General provisions

The German national eID scheme is provided by the German federal government and governed by federal law and subordinate regulations. All entities providing services for the scheme are either public authorities or private entities contracted by such authorities, which has a direct responsibility to fulfil certain functions in the scheme as stipulated in section 7 of the Act on Identity Cards and Electronic Identification (Personalausweisgesetz, PAuswG).

4.2 Published notices and user information

In the documentation provided by Germany for the peer-review, it is stated *"[...] all terms and conditions are defined by national laws and decrees and as such publicly available. The laws and degrees also cover the applicable rules for data privacy, thus the German eID includes a privacy policy*". In addition, a brochure containing information on how the citizen can use the eID is provided both on-line at the official web page and in printed form.

4.3 Information security management

According to the eIDAS regulation, all participants providing a service related to electronic identification in a cross-border context shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for electronic identification schemes in the respective Member States that effective controls are in place. Such information security management system shall adhere to proven standards and principles.

In the documentation provided by Germany, it is stated that the scheme is governed by national law and subordinate guidelines. Of particular importance are the standards developed by the Bundesamt für Sicherheit in der Informationstechnik (BSI), which provides the foundation for the management practices and risk management. The management standard BSI 100-2 ("IT-Grundschutz Methodology") defines an approach to develop an IT Security Plan ("IT-Sicherheitskonzept"). It outlines a structured approach to identifying assets, classification of such assets based on their respective criticality in each of the security disciplines (confidentiality, integrity and availability) and is accompanied with catalogues of threats and controls. Consequently, Bundesministerium des Innern, has developed such a IT Security Plan for the eID scheme, based on this methodology. The IT Security Plan is not a classified document (although not public), and has been shared with a few members of the WG on a need-to-know basis for the purposes of this peer review.

The Bundesministerium des Innern is responsible for the German eID scheme, and the IT Security Plan is applicable to all relevant IT components and the entities providing such services of the scheme. The overall approach to information security management is very similar to that of the International Information Security Management (ISMS) Standard ISO/IEC 27001:2013.

Private entities involved in the providing of the German eID are also required to be certified according the ISMS standard ISO/IEC 27001. The scope of the ISMS to be certified is determined through the analysis provided in the IT Security Plan, and cover all assets identified as critical.

4.4 Record keeping

The obligations of the Identity Card Register and the Issuing Authorities pertaining to record keeping are regulated through §23 [PAuswG] and §4 [PAuswV]. As the eID scheme is designed so that there exists no central repositories for authentication information, it has been concluded by DE that no other stipulations than the General Data Protection Rules (GDPR) are needed.

4.5 Facilities and staff

Personnel holding critical roles in the enrolment, identity proofing, verification and issuing of the eIDs are employed according to certain dedicated job profiles. The local authorities in the federal states are responsible for establishing training programmes and conducting training courses with the relevant staff. The Federal Ministry of the Interior has, to aid the local authorities, issued comprehensive training material in the form of a handbook.

The IT Security Plan specifically identifies facilities that are potentially critical assets, and address the need for protection of such facilities. It is assumed that each responsible entity conducts its own risk assessment and implements the risk-mitigating controls determined to be required.

4.6 Technical controls

Much like the implementing regulation (EU) 2015/1502, the IT Security Plan does not set out requirements for specific technical controls, but rather provides appropriate input to each entities' own risk analysis. This input includes which information assets needs to be protected and in what aspect (confidentiality, integrity and/or availability). The WG notes that it is in each entities' own discretion to design risk mitigating controls, define appropriate risk acceptance levels and to accept residual risk.

Certain control areas are however identified in the IT Security Plan, which should, as such, be included in the risk analysis and managed. For example, the IT Security Plan specifically requires compliance with BSI TR-03104 for the secure communication between the local authority providing the registration services and the issuer of the eID means. That is determined to address the requirement for secure communication between these entities.

It has further been described to the WG, that the cryptographic keys used for issuing eID means are generated, stored and used within Hardware Security Modules (HSMs) approved by the BSI. The approval process includes a security evaluation and covers the security of the RNG (DRG.4), tamper resistance (high attack potential) and side channel resistance for the relevant algorithms (high attack potential).

4.7 Compliance and audit

The IT Security Plan requires each entity providing services under the eID scheme to conduct a self-assessment (a GAP-analysis) of the compliance to the requirements. In addition, any private entity contracted to provide a service in the eID scheme is required to be certified according to the ISMS standard ISO/IEC 27001:2013. This implies an external audit, where a re-certification is conducted every three years, with annual surveillance audits.

As the scope of the ISMS shall include the stakeholders, dependencies and assets identified in the IT Security Plan, it has been concluded by the WG that such external audit can be considered to fulfil the audit requirement of section 2.4.7 of 2015/1502 for level high.

For public authorities, the requirement of a certified ISMS does not apply. Instead, such authorities are supervised by the Federal States. The form of supervision may differ depending on the circumstances within the issuing authorities. Measures include formalised processes which are defined in procedural guidelines. IT security and data protection officers are responsible for the compliance monitoring.

As the German eID scheme is directly managed by a government body, the requirement of the regulation is that it should be supervised according the national law. The WG is confident that the authorities and agencies taking part in the providing of the German eID scheme are in full compliance with the applicable laws and other regulations.

4.8 Conclusion

It is the WGs opinion that the notified scheme complies with the requirements of section 2.4 of 2015/1502 for level high.

5. Topic 3: Middleware

5.1 Purpose of this document

This topic addresses middleware, mainly covering the following aspects of the German eID scheme

- Deployment, documentation, and maintenance
- Responsibilities and security
- Access certificates and private sector relying party deployment

5.2 Scope

5.2.1 Deployment, documentation, and maintenance

With Germany following a **decentralised deployment model** also known as the **middleware model**, the relying party (the eIDAS connector) operates the components needed to initiate communication with the eID client and to establish a secure cryptographic channel with the eID card.

Germany therefore provides a software component, the “eIDAS middleware” , which is operated in the receiving Member State, in which a German citizen wants to authenticate in.

In a common eIDAS setup, the German middleware is deployed by a central eIDAS connector serving this Member State’s public sector relying parties, or directly at a (private sector) relying party. The peer review clarified how this middleware will be provided by Germany. Two options are foreseen: the middleware will be bundled by CEF/DIGIT together with its eIDAS node reference node implementation, or a virtual machine (VM) including the eIDAS middleware can be provided.

The documentation specific to the eIDAS middleware has been completed and provided in the course of the peer review process. The eIDAS middleware used by other Member States shows some differences to the eID service used by German relying parties. Clarification was sought in the documentation.

Maintenance of software releases follows industry practices. Germany aims to align the eIDAS middleware release cycles with the CEF/DIGIT releases of the eIDAS reference implementation.

5.2.2 Responsibilities and security

Explanations on **requirements** to be met when operating the middleware, **liability and responsibilities** have been asked for. Although just partly in scope of the peer review process, Germany has openly responded to these questions, which helped the peer review panel understand in greater depth the topic covered.

Germany feels responsible and liable for the functionality of the middleware it provides. The organisations operating the eIDAS middleware – central eIDAS connectors or relying parties – are responsible for correct deployment and operation. The eIDAS middleware is provided under an EUPL open source license, which also defines responsibilities.

Following some reference made to requirements for German relying parties on operating an eID server, the German colleagues explained that no requirements in excess of the requirements defined under the eIDAS interoperability service apply.

To increase confidence in the eIDAS middleware Germany informed the peer review panel that a penetration test is ongoing, organisations operating the eIDAS middleware are of course free to analyse the software or to carry out penetration tests themselves.

5.2.3 Access certificates and private sector relying party deployment

The operation of the eIDAS middleware to use the German eID requires **authorisation**. Technically this is implemented by Germany issuing authorisation certificates to relying parties. Validity of the authorisation certificate is checked by the eID card during the citizen authentication process.

For public sector relying parties the authorisation certificate is issued free of charge to Member States. This certificate is used to serve all public services of a Member State. If a Member State operates several eIDAS middleware instances, like for load balancing or when deploying several eIDAS Connectors, authorisation certificates are issued so that the same pseudonym is generated as unique identifier (cf. topic 2 on eID means management and authentication).

The German eID scheme can be used by private sector relying parties conditional to them applying for authorisation at and receiving an authorisation certificate from the German competent authority. This is comparable to procedures German private sector relying parties have to follow. Private sector relying parties may use the eIDAS middleware provided by Germany.

5.3 Conclusion for the middleware topic

Member States actively involved in reviewing this topic conclude that the declared LoA - high - complies with the eIDAS Implementing Regulation 2015/1502 for the current topic.

6. Conclusion

The observations per topic will be discussed in this chapter and a final overall conclusion will also be given in this chapter.

Enrolment: the following aspects of the German eID have been discussed: identity proofing: procedures, controls, document acceptation, delivery and activation, legal representation, information material / terms & conditions, pseudonyms and document numbers. Member States actively involved in reviewing the topic conclude that the answers provided by Germany are satisfactory and the declared LoA - high - complies with the eIDAS Implementing Regulation 2015/1502.

Interesting subjects of topic two (eID means management and authentication) are: the unique identifier is not lifelong persistent, options for additional attributes for the dataset which is normally minimal (though eIDAS complaint), end-to-end cryptographic protection from eID card to middleware and the chip in the ID card which undergoes Common Criteria certification. It was found by that the declared LoA high is indeed met.

The German national eID scheme is provided by the German federal government and governed by federal law and subordinate regulations. All entities providing services for the scheme are either public authorities or private entities contracted by such authorities, which has a direct responsibility to fulfil certain functions in the scheme as stipulated in section 7 of the Act on Identity Cards and Electronic Identification (Personalausweisgesetz, PAuswG). The Bundesministerium des Innern is responsible for the German eID scheme, has taken a structured approach to establish a common framework for the management of information security aspects and risks pertaining to the eID scheme.

In the topic middleware it was discussed that Germany provides an eIDAS middleware software component for MS to install so a secure cryptographic channel can be established with the eID client and the public service provider. Germany feels responsible and liable for the functionality of the middleware it provides. The organisations operating the eIDAS middleware are responsible for correct deployment and operation. The eIDAS middleware provided by Germany may also be used by private sector relying parties.

As a conclusion the experts participating in this peer review trust in the level of assurance the German eID scheme proclaims it has, LoA high, and that this eID scheme complies with the eIDAS Implementing Regulation 2015/1502.

The next step is for the Cooperation Network to present the peer review report on the German eID scheme for the Cooperation Network. After this presentation the German eID scheme can officially be notified.

References

BSI “German eID: Revocation and Pseudonyms”, 2 May 2017 (Slides presented by Germany at the Berlin kick-off meeting)

BSI “Technical Guideline TR-03130-3eID-Server – Part 3: eIDAS-Middleware-Service for eIDAS-Token” Version 1.05, May 2017 (Documentation provided by Germany after the Berlin kick-off meeting)

BSI “Three Steps to integrate the German eIDAS-Middleware”, draft 2. May 2017, (Documentation provided by Germany after the Berlin kick-off meeting)

Files provided by Germany, can be found on the pre-notification Germany page:

- Notification form
- Letter German Minister of the Interior DE
- Letter German Minister of the Interior EN
- German eID 01 Whitepaper final
- German eID 02 LoA Mapping final
- German eID 03 IF Mapping final
- German eID 04 SuppDoc final
- German eID 04 SuppDoc v1_1 draft

Files on Germany Peer Review:
- Technical guideline TR-03130-3 Middle Ware
- Act on Identity Cards and Electronic Identification
- Security Framework Strategy Outline