Federal Office
for Information Security

German eID based on Extended Access Control v2

Fulfilment of interoperability requirements according to (EU) 2015/1501

Version 1.0

20 February 2017

1 Introduction

This document describes how the **German eID** scheme (i.e. the **German eID based on Extended Access Control v2**) meets the interoperability and minimum technical and operational security requirements of Commission Implementing Regulation (EU) 2015/1501.

2 Interoperability requirements

Article	Requirement	Description
Art. 4	**Mapping of national assurance levels** The mapping of national assurance levels of the notified electronic identification schemes shall follow the requirements laid down in Implementing Regulation (EU) 2015/1502. The results of the mapping shall be notified to the Commission using the notification template laid down in Commission Implementing Decision (EU) 2015/1505.	The German eID scheme meets all requirements of the eIDAS level of assurance '**high**' laid down in the Commission Implementing Regulation (EU) 2015/1502. The results are stated in the German notification form. The detailed mapping is given in [LoA Mapping].
Art. 5	**Nodes** 1. A node in one Member State shall be able to connect with nodes of other Member States. 2. The nodes shall be able to distinguish between public sector bodies and other relying parties through technical means. 3. A Member State implementation of the technical requirements set out in this Regulation shall not impose disproportionate technical requirements and costs on other Member States in order for them to interoperate with the implementation adopted by the first Member State.	The German eID system is integrated into the eIDAS Interoperability Framework [eIDAS IF] in accordance with the eIDAS Technical Specifications of the eIDAS Technical Subgroup [eIDAS Arch], [eIDAS SAML], [eIDAS Attributes], [eIDAS Crypto]. The integration architecture distinguishes between receiving and sending nodes. Due to the nature of the German eID system, the sending side is deployed via the middleware integration model [eIDAS Arch]. Thus, Germany does not operate a sending node, but provides an eIDAS-Middleware to be operated within the other Member State. The cross-border interface of the German eIDAS-Middleware is implemented according to the eIDAS technical specifications. It was already successfully piloted with another MS in the operational system. The middleware is able to distinguish between public-sector bodies and other relying parties. To get access to personal data stored on the German eID, service providers need an authorisation certificate installed in the middleware. For public-sector

Article	Requirement	Description
		services, Germany will provide the necessary authorisation certificates to each Member State free of charge. Non-public-sector services obtain an authorisation via the standard procedure at the Issuing Office for Authorisation Certificates in accordance with [PAuswG][1] and [PAuswV]. On the receiving side, the deployment is done via the decentralised integration model, i.e. each German service provider operates (or subcontracts) an eIDAS Connector. While service providers are part of the German eID infrastructure, they are not part of the notified German eID scheme, since they have no role in cross-border use of the German eID. Hence, these roles are not considered in the following.
Art. 6	**Data privacy and confidentiality** 1. Protection of privacy and confidentiality of the data exchanged and the maintenance of data integrity between the nodes shall be ensured by using best available technical solutions and protection practices. 2. The nodes shall not store any personal data, except for the purpose set out in Article 9(3).	The German eIDAS-Middleware is implemented according to the eIDAS technical specifications. In particular, these specifications include state-of-the-art crypto requirements for the protection of privacy and confidentiality of data [eIDAS Crypto]. The German eIDAS-Middleware does not store any personal data, except for the purpose set out in Article 9(3).
Art. 7	**Data integrity and authenticity for the communication** Communication between the nodes shall ensure data integrity and authenticity to make certain that all requests and responses are authentic and have not been tampered with. For this purpose, nodes shall use solutions which have been successfully employed in cross-border operational use.	The German eIDAS-Middleware is implemented according to the eIDAS technical specifications. In particular, these specifications include state-of-the-art crypto requirements for the integrity of data [eIDAS Crypto].
Art. 8	**Message format for the communication** The nodes shall use for syntax common message formats based on standards that have already been deployed more than once between Member States and proven to work in an operational environment. The syntax shall allow: (a) proper processing of the minimum set of person identification data uniquely representing a natural or legal person; (b) proper processing of the assurance level of the electronic identification means;	The German eIDAS-Middleware is implemented according to the eIDAS technical specifications. In particular, these specifications include a common message format that has been shown to work in an operational environment [eIDAS SAML].

[1] The notification of the German eID will be based on an amendment of the [PAuswG] which is currently in the legislative process and will enter into force before notification; cf. [PAuswG_AMD].

Article	Requirement	Description
	(c) distinction between public sector bodies and other relying parties; (d) flexibility to meet the needs of additional attributes relating to identification.	
Art. 9	**Management of security information and metadata** 1. The node operator shall communicate the metadata of the node management in a standardised machine processable manner and in a secure and trustworthy way. 2. At least the parameters relevant to security shall be retrieved automatically. 3. The node operator shall store data which, in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident. The data shall be stored for a period of time in accordance with national requirements and, as a minimum, shall consist of the following elements: (a) node's identification; (b) message identification; (c) message data and time;	The German eIDAS-Middleware is implemented according to the eIDAS Technical Specifications. In particular, these specifications include requirements for the communication of metadata [eIDAS Arch]. Furthermore, the eIDAS-Middleware will provide a logging mechanism that enables storing the relevant data as listed in Article 9.
Art. 10	**Information assurance and security standards** 1. Node operators of nodes providing authentication shall prove that, in respect of the nodes participating in the interoperability framework, the node fulfils the requirements of standard ISO/IEC 27001 by certification, or by equivalent methods of assessment, or by complying with national legislation. 2. Node operators shall deploy security critical updates without undue delay.	Security critical updates of the German eIDAS-Middleware will be provided without undue delay. Requirements for the operation of sending nodes are not applicable.
Art. 11	**Person identification data** 1. A minimum set of person identification data uniquely representing a natural or a legal person shall meet the requirements set out in the Annex when used in a cross-border context. 2. A minimum data set for a natural person representing a legal person shall contain the combination of the attributes listed in the Annex for natural persons and legal persons when used in a cross-border context. 3. Data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters.	The German eID is used for the identification of natural persons. The Minimum Data Set provided by the German eID is described in Section 5 of [German eID]. The German eIDAS-Middleware is implemented according to the eIDAS technical specifications, which ensures in particular that data are transmitted based on original characters and, where appropriate, also transliterated into Latin characters.

References

LoA Mapping	BSI: German eID based on Extended Access Control v2 - LoA mapping
eIDAS IF	Europäische Kommission: DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1501 DER KOMMISSION vom 8. September 2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
eIDAS Arch	eIDAS Technical Subgroup: eIDAS Technical Specifications - Interoperability Architecture
eIDAS SAML	eIDAS Technical Subgroup: eIDAS Technical Specifications - SAML Message Format
eIDAS Attributes	eIDAS Technical Subgroup: eIDAS Technical Specifications - Attribute Profile
eIDAS Crypto	eIDAS Technical Subgroup: eIDAS Technical Specifications - Crypto requirements for the eIDAS Interoperability Framework
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG)
PAuswG_AMD	Government draft for an Act on the promotion of electronic identification
PAuswV	Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung - PAuswV)
German eID	BSI: The German eID based on Extended Access Control v2 - Overview of the German eID system