H2.4 The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective

By Harald Zwingelberg and Jan Schallaböck

Editors:	*Harald Zwingelberg (Unabhängiges Landeszentrum für Datenschutz)*
Reviewers:	*Ioannis Krontiris (Johann Wolfgang Goethe – Universität Frankfurt)*
	Robert Seidl (Nokia-Solutions and Networks)
Identifier:	*H2.4*
Type:	*Heartbeat*
Version:	*1.0*
Date:	*31/10/2013*
Status:	*Final*
Class:	*Public*

Abstract

Within the research project Attribute based Credentials for Trust (ABC4Trust) the legal research task concentrated on requirements, concepts and further aspects for privacy-preserving methods for identification and authentication. The European Commission proposed a Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS). The Authors like to use the opportunity to provide insights from a privacy and data protection perspective to for the legislative process based on the expertise gained within the ABC4Trust project. The three core aspects addressed herein are:

I. Emphasize the concept of authentication instead of identification

II. Remove barriers for privacy-preserving eID solutions

III. Clarify applicability of data protection requirements also for eID services

The findings leading to this document has been used to discuss the position with stakeholders in the European parliament and the European Commission.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257782 for the project Attribute-based Credentials for Trust (ABC4Trust) as part of the "ICT Trust and Security Research" theme.

Members of the ABC4TRUST consortium

1.	Alexandra Institute AS	ALX	Denmark
2.	CryptoExperts SAS	CRX	France
3.	Eurodocs AB	EDOC	Sweden
4.	IBM Research – Zurich	IBM	Switzerland
5.	Johann Wolfgang Goethe – Universität Frankfurt	GUF	Germany
6.	Microsoft Belgium NV	MS	Belgium
7.	Miracle A/S	MCL	Denmark
8.	Nokia-Solutions and Networks Management International GmbH	NSN	Germany
9.	Research Academic Computer Technology Institute	CTI	Greece
10.	Söderhamn Kommun	SK	Sweden
11.	Technische Universität Darmstadt	TUD	Germany
12.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany

List of Contributors

Chapter	Author(s)
All Chapters	Harald Zwingelberg (ULD), Jan Schallaböck (ULD)
Appendix	Harald Zwingelberg (ULD), Jan Schallaböck (ULD)

Table of Contents

1 Introduction

The European Commission published a proposal for a "Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market" (herein: eIDAS).[1] The proposal aims at removing existing barriers to the digital development in Europe by providing the legal basis for a mutual recognition of electronic identification and authentication means, as requested within the Digital Agenda.[2] This deliverable provides an analysis of the aforementioned in light of the research conducted by the ABC4Trust consortium.

This analysis has been written by partners of the ABC4Trust (Attribute-based Credentials for Trust) research consortium.[3] ABC4Trust researches privacy preserving solutions to authenticate users only with those attributes necessary for a given purpose. The authors therefore focussed on the aspects related to electronic identification, as addressed by Chapter II of the proposed regulation. In the following we introduce three substantial suggestions for amendments to the regulation to address central aspects to grant more weight to data protection aspects:

- Emphasize the concept of authentication instead of identification (Chapter 2),
- Remove barriers for privacy-preserving eID solutions (Chapter 3),
- Applicability of data protection requirements for eID services (Chapter 4),
- As well as other related aspects (Chapter 5).

Details and suggestions for amending the legal text of the eIDAS regulation are provided in the Appendix of this document.

[1] For the proposal text and other related legislative documents see: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=201689.

[2] Key Action 16 reads: "Propose a Council and Parliament Decision requesting Member States to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services", in A Digital Agenda for Europe, COM (2010) 245 final, online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245:EN:NOT .

[3] The research leading to these results has been funded by the European Commission under grant agreement n° 257782 for the project Attribute-based Credentials for Trust (ABC4Trust) as part of the "ICT Trust and Security Research" theme.

2 Emphasize the concept of authentication instead of identification

The Commission's draft of the eIDAS regulation is focussed on the model of identifying individuals with their full set of personal information provided by the respective national electronic identification scheme (eID). From a data protection viewpoint this model is out-dated. The data protection principle of data minimisation instead requires limiting the processing of personal data to the amount and duration necessary for a given purpose, which in relevant occasions may not be full identification of individuals, as often e.g. prove of age is sufficient. In the view of many European experts upcoming eID solutions should therefore support the privacy-preserving feature of selective disclosure of attributes.[4] The German eID solution which is being rolled out to citizens since 2009, the "new ID-card" ("Neuer Personalausweis", nPa) natively supports data minimisation and even provides a formal process for supporting the enforcement that only the necessary data is transferred to a relying party.[5] To enable such data minimisation eID schemes need to support selective disclosure (see Section 2.1) and this privacy-preserving method must not be excluded but should rather be encouraged by the eIDAS regulation (see Section 2.2).

2.1 Data minimisation and selective disclosure

The concept of selective disclosure allows revealing only parts of the information available in an eID-scheme. In typical implementations the information is split in attribute-value pairs, e.g. name: Johannson, first name: Sven, place of residence: Stockholm, profession: lawyer, date of birth: 1975-02-07, etc. The privacy-preserving principle of attribute selection means that the citizen only discloses those personal data necessary for a specific given purpose. For example in cases where only the verification of the age or the current home address is required, only this information is provided to the relying party. More advanced systems even allow calculating and verifying a proof over an attribute, thus for age verification it is not even necessary to reveal the birth date but it is possible to show that the birth date certified in the eID is above or below eighteen. Supported by technology, they may allow such verifications in a way that the trust in the issuer remains intact as changes to the attribute values are not possible without being detectable. Such technology is not only state of the art, but also readily available, ie. current practise. In fact the current German eID supports this feature and two other, even more advanced solutions are currently piloted within the ABC4Trust project[6] supported by the European Commission.

According to the well-recognized principle of data minimisation relying parties may only ask for the necessary personal data. This principle is inter alia laid down in Art. 6 (1) (b) and (c) of Directive 95/46/EC and also immanent to the Commission's draft of a General Data Protection Regulation.[7] All relying parties in Member States are thus already required to structure their processes in a manner that only the necessary personal data is processed for a specific service. Thus, asking relying parties to consider what categories of data are actually necessary and limiting the processing to these categories

[4] This is supported by a survey among eID experts done by the SSEDIC project: "With regard to the disclosure of user attributes 90% of the experts support the principle of minimum disclosure (by agreeing with the statement 'The user should be able to disclose only the minimum number of attributes required for a transaction and without giving away unneeded data')." cf, [SS11], p. 32 et seq.

[5] For details on how the necessity of attributes may be assesses see: [Zw11] pp. 151, 156 et seq.

[6] See: https://www.abc4trust.eu.

[7] For the proposed draft and legislative documents see: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=201286

is not a new requirement by any means, but should be practice in all public and private entities to comply with the existing European data protection law.

In the area of electronic identification, adhering to the principle of data minimisation was admittedly difficult, as established eID solutions often forced the users to disclose all information contained within a certificate, as otherwise the proofing mechanism, often relying on a digital signature for the whole set of data, would have been invalidated. With the availability of privacy-preserving eID solutions no reasons remain to continue forcing persons to provide fully identifying sets of personal data where a limited disclosure, pseudonymous use or even an anonymous proof of certain attributes is sufficient. A series of institutions, including the European Data Protection Supervisor (EDPS) as well as numerous researchers and other constituencies therefore support the request to introduce selective disclosure in upcoming eID solutions and to pave the way for this within the eIDAS regulation.[8]

2.2 Introducing Privacy-preserving authentication to eIDAS

Consequently, we suggest amendments to the eIDAS regulation that broaden the scope of the draft by incorporating electronic authentication with selected attributes. In this proposal authentication is defined as the basic use case: A user, to whom an eID has been issued (the holder), is providing information on attributes regarding his person. Electronic identification is a sub-case of authentication, where the set of attributes provided contains the information necessary to identify the holder, e.g. the relevant set of name and address for issuing a summons to appear before court. Being aware of the different definitions for the terminology 'authentication' in the scientific disciplines concerned with eIDs, it was necessary to clearly define authentication as the process of providing information on specific attributes. Authentication then can be further differentiated into four levels with raising intensity and raising invasiveness in terms of the holder's privacy:

- **Unlinkable authentication** – the holder remains anonymous and only provides e.g. information on age, place of living or belonging to a particular group or profession.
- **Context specific authentication** – the provided information allows verifying that the same person has electronically authenticated in the same context in a previous transaction. This type of authentication supports the pseudonymous use of services.[9]
- **Conditional electronic identification** –the process of an electronic authentication using person identification data in electronic form unambiguously representing a natural or legal person in such a manner that the relying party can access and disclose the identifying information only under specified conditions. This case allows to preserve the privacy of users and to reduce the risk of accidentally exposing personal data to third parties. While the relying party can be certain of being able to identify an acting individual, the identifying information is not disclosed until really needed. But the disclosure can only be conducted under the said conditions, e.g. in case of fraud or other means of abuse. There are several technical or organisational approaches available to do this, namely the inspector approach in ABC4Trust[10], and the proposed amendment, however, does not suggest a particular solution.

  Privacy-preserving attribute-based credentials as researched and developed within ABC4Trust support conditional identification by way of the "inspection mechanism", which

[8] [EDPS13], consideration n° 28; [Sp13] p. 145; [Qu13] position paper of Hessian DPA, p. 4; numerous European eID experts support selective disclosure as a necessary feature according to a survey of the SSEDIC project, infra footnote 4.

[9] The notion of „pseudonymous" here is used in a way, where only the data subject has the knowledge to uncover the pseudonym and link it to herself. The concept often is not sufficiently differentiated from cases where the another party can do so, which often is the case when ex-post pseudonymisation is applied but the information on the link between person and its pseudonym is stored separately.

[10] See: [Ca11] Chapter 2.6, pp. 21-22.

allows the relying party to cryptographically verify that it actually possesses the identifying information already without decrypting it.[11] Traditionally this task is also achieved by replacing the identifying bits of information into a separated and protected environment, while the original data only contains a link to the former. Sometimes such a process also is described as pseudonymisation, but it should not be confused with the use of the term in the way it was introduced for "context specific authentication", as above.

- **Unconditional electronic identification** –the process of an electronic authentication providing person identification data in electronic form unambiguously representing a natural or legal person in a way that the relying party direct learns the identifying attribute values.

Introducing authentication as a conceptual approach would require a series of amendments with clarifications and definitions including editorial follow-up changes in several articles, but does not have an impact of the viability of the original use cases for the directive, but rather extends it. In addition the process of validating received information formerly named 'electronic authentication' is now defined clearer as 'electronic validation'. The necessary changes to the text of the regulation are laid down in the Appendix to this text.

3 Remove Barriers for privacy-preserving eID solutions

The eIDAS regulation as a legal framework applicable in many Member States with different cultural and sociological backgrounds and varying developments in the area of eIDs should be as technology neutral as possible. In particular it must preserve an option for more privacy-preserving solutions – be it for existing eID schemes or those that are still under development to be open for innovation in this area. Within a mid- to long-term perspective the regulation must be open for changes and adaptations and should preferably even encourage the technological advancement of national eID solutions. Otherwise the requirement of mutual recognition and acceptance may lead to a 'race to the bottom' as the cheapest, easiest and potentially most privacy invasive solution may be preferred by relying parties or other stakeholders not primarily interested in and concerned with preserving privacy and citizen's rights.

The proposed Article 6 (1) (d) eIDAS has two major obstacles for privacy-preserving eID solutions. The first sentence suggests an architectural set up and corresponding data flows which are not state of the art in data protection (see Section 3.1). The second sentence prevents that relying parties may be imposed with technical requirements which is, however, a severe hindrance for advancing eID solutions (see Section 3.2).

[11] See: [Ca11] pp. 86 et seq.

3.1 eIDAS must be open for alternative architectural designs and data flows

Reading the present Article 6 of the regulation, it appears to suggest a centralized service for the technical implementation. Under such a solution the holder needs to provide identifying data to the relying party and the relying party is then validating the 'identification data *received*' (emphasis added) with the "authentication possibility online", a service to be provided by the notifying Member States. The resulting data flows in such a constellation are shown in Figure: below:

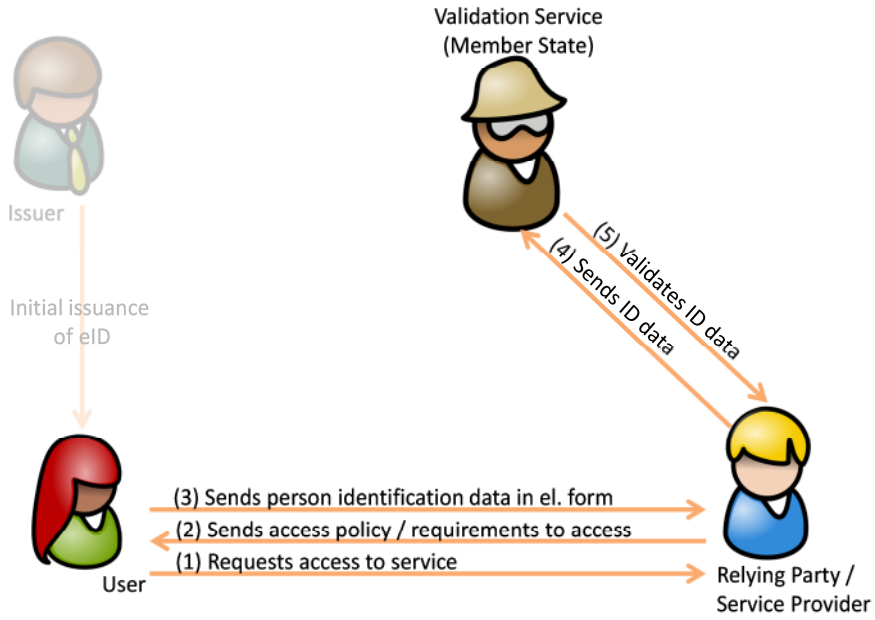

Figure: Data flow as suggested by Article 6 (1) (d)

A clarification is necessary as this architectural approach is not state of the art nor sufficiently technological neutral. The current text version effectively prevents existing implementations following other (better) approaches from being used. But above all it exposes relevant risks for the privacy of citizens, lowering trust and thus poses potential obstacles for the adoption by users and relying parties. From a data protection perspective the following privacy risks can be observed:

- The validation service may profile the user.
- The validation service learns about the relying parties' customers (business secrets).
- The validation service becomes a hot-spot with many personal data processed. From an IT-security point of view, such a centralized database is critical and a potential target for attacks.
- The relying party receives information on all attributes of the eID unless the national eID system natively supports selective disclosure.
- The user does not have any transparency and control over the data exchanged between the relying party and the validation service.
- The member states are burdened with the costs of making available such a service.

Two alternative architectures should be considered. First, in a slightly more privacy-preserving solution, the validation service may act as privacy proxy, providing the feature of selective disclosure to users. The data flow would be different, while the same actors are in place. In this scenario the *user* would contact the validation service to get a signed or sealed certificate on the necessary attributes

which may then be presented to the relying party. The relying party and the validation service would not directly interact.

However, at least on a mid- to long-term perspective the directive should aim for users to authenticate and identify them directly towards a relying party or another user by presenting only the necessary attributes. In the meantime Members States should be allowed and encouraged to support foreign relying parties in order to enable end-to-end authentication for citizens of the respective Member State. For this the notifying Member States, cf. Art. 6 eIDAS, must then provide the necessary specifications and at least an open reference implementation, support and other means to validate electronic authentications done with the notified eIDs free of charge, but they do not need to provide validation service themselves. In the latter case the further costs of operating the system would reside with the relying parties, which appears adequate, however.

While such an approach could and should be made mandatory, a voluntary approach might be more acceptable for some member states. Relying parties could then voluntarily opt for supporting such technology, either by using and hosting the reference implementation or reimplementing the specification themselves. Such an approach would allow open the field for innovation and give relying parties and member states the option to improve the way eIDs work without the need for new regulation.

The suggested amendments address these aspects and open the eIDAS regulation for technological advances.

3.2 Imposing proportionate technical requirements on relying parties

Encouraging the further development of privacy-preserving eID solutions is not sufficient, if the later deployment is prevented by the eIDAS regulation. The second sentence of Article 6 (1) (d) reads: "Member States shall not impose any specific technical requirements on relying parties established outside of their territory intending to carry out such authentication." This effectively prevents all eID systems from exposing requirements regarding some specific technical implementation on the side of the relying party. Recital 15 further specifies that this refers to any "specific hardware or software to verify and validate the notified electronic identification."

As stated in the section above, it would be preferable from a data protection and privacy by design perspective to have established a process for authentication end-to-end completely omitting entities in the middle such as the validation services currently proposed as an interim solution. However, such proactive solutions will likely require at least some specified software installed on the client of the relying party, if not impose some hardware requirements. Usually it is necessary to install some cryptographic libraries for the validation process and another component to arrange the communication with the other party, e.g. a browser plug-in. The current text prevents that relying parties are demanded to foresee these requirements. While a voluntary adaptation is possible, it should be further encouraged.

If should be noted that also the solution proposed in the Commission draft necessarily imposes technical requirements upon relying parties. In any case it is necessary to understand the underlying protocols, e.g. the relying parties' computer must "know" how to handle and where to send the identification data for validation. This will also require some set up, the installation of a browser plug-in, update of cryptographic libraries and installation of the issuers root certificates.

However, as the recognition and acceptance is mandatory in other Member States overstraining requirements on the side of relying parties should be prevented. Therefore the verification means must be available free of charge or licence costs and any additional technological and implementation requirements must be proportionate for the relying party in the light of the benefits for the privacy of the citizens. The European Commission may decide on the proportionality of the requirements given due consideration to the position of relevant stakeholders such as the European Data Protection

Supervisor and the Article 29 Working Party. As a general guideline a solution only requiring a browser plug-in or add-on available for broadly deployed browsers and / or additional cryptographic libraries should be considered proportionate. Where possible such solutions should be standardized to avoid too many different solutions within the union. Further considerations for the proportionality could include:

- the solution is standardised,
- cryptographic libraries must be available as source code,
- different operating systems are supported.

Such a solution would prevent that relying parties are overstrained with implementation requirements. To open the eIDAS regulation for privacy-preserving solutions it must be possible to notify eID schemas that place some proportionate requirements on the relying party.

4 Applicability of data protection requirements for eID services

The proposal contains a reference to the Directive 95/46/EC in Article 11 thus within chapter III on trust services. Such a reference is missing in the appropriate section on eIDs and thus may cause the misinterpretation that the rules on data protection do not apply in this area. However, issuers, validation services and relying parties are all processing personal data of the holder of the eID, who is the data subject in the sense of the Privacy Directive, 95/46/EC. At least a clarifying statement is advisable here and can easily be accomplished by moving the reference to data protection legislation from Article 11 to the first chapter of the regulation making it applicable to all subsequent chapters. Further issuers and validation services are consequently to be added as addressees of the norms.

In addition it must be prevented that validation services use their central position within the currently proposed data flow to profile the citizen's behaviour. Validation services therefore must not collect or retain personal data beyond the absolutely necessary extend. Potential liability of validation services does not permit excessive storage of data. Here the current draft needs further clarification for what and to which extend notifying Member States, issuers and validation services are supposed to be liable. It would be preferable to define liability in a way that it does not require log files and protocols of validation processes. This is a rather relevant clarification, as European citizens may publicly reject the approach taken, if new profiling opportunities are introduced, rendering the whole legislative approach ineffective. However, as lined out above, instead of a legislative approach, by means of a prohibition, an architectural approach as lined out above in Chapter 3 may be necessary to gain the relevant trust from citizens for using the service.

5 Other related aspects

While focussing on the three core aspects above minor amendments are suggested quasi en-passant, some of which are highlighted in the following sections.

5.1 Difference in security levels of national eID solutions

To prevent that eID schemas with a low assurance level, e.g. username and password, must be accepted where the Members State requires a higher level such as a secure physical token a clarification has been suggested for Art. 5. It should only be possible to require other Member States to recognize and accept eID solutions with the same or higher assurance level. As a similar

requirement exists for the recognition and acceptance of electronic signatures in Article 20 (4) eIDAS a comparable corrective measure must be included for eIDs as well.[12]

5.2 Recognition and acceptance

In Article 5 the object of the mandatory recognition and acceptance requires adjustments. Member States may have eID schemes with different assurance levels in place. It should be self-evident that only electronic authentication means with the same or higher assurance level are eligible for a mandatory recognition by other Member States.
Likewise Member States may foresee a separation of sectors for the application of their eID solutions, e.g. between public, health and financial sectors. This separation may be foreseen as an organisational measure for data protection and IT-security. Such considerations must not be prevented by enforcing recognition and acceptance of foreign eIDs from another sector as is currently proposed, even if these meet the required assurance level.
Both clarifications require further definitions with implementing acts. Existing international standards such as ISO/IEC 29115 Entity Assurance Authentication may provide helpful guidance in this context.

5.3 Liability

A clarification is necessary regarding the reference to liability in Article 6 (1) (c) and (e) of the proposed eIDAS directive. Currently the Article reads as if it is may be about the correctness of the provided data. But it may also be understood in a way that the electronic authentication means and any information provided with it is clearly linked to a single person. Thus the member state vouches only for the fact, that for each authentication means there is only one single person but a single person may have several authentication means (e.g. an eID-token and an eHealthCard, or several ePassports). Independent of what is intended a clarification should be made. In any case it should be added that Member States and issuers are only liable for the correctness of the data or the link to a single person at the time of issuance.

This decision does indirectly influence data protection considerations as a stricter liability may lead to the necessity that validation services and issuers retain log data as a proof for potential liability cases.

6 Conclusion and outlook

While use by the private sector is not directly in scope of the eIDAS regulation it can, however, be assumed that it will impact the future eID landscape in Europe and pave the road also for those eID systems that will be used by the private sector. Some of the privacy–preserving concepts described within this paper should be considered for eID solutions, even independently from a potential notification under the eIDAS regulation, but they also should seen by Member States as desirable features for upcoming eID schemes.

The authors have presented the ideas stated herein on several occasions throughout summer 2013. The notion of allowing selective disclosure of attributes as direct means to enable data minimisation has been brought to the attention to the specialists and regulators in the field. The idea of conditional

[12] [Du12], p. 6.

identification, which allows data minimisation by selective disclosure of attributes also for all those cases where the knowledge of the full identity of the users is only needed under certain specific circumstances, has caught the interest of the audience and the authors are encouraged to continue looking into the involved aspects.

In the meantime a series of potential use cases for conditional identification have been identified, which we plan to analyse under technical, legal and privacy perspectives. The two ABC4Trust pilots are already deploying the inspection feature and will be further assessed with legal considerations.

Another interesting use case is, again, the cross-border use of eIDs: It is unlikely that all relying parties will deploy the necessary hard- and software to interpret all existing eID solutions in Europe. Services transforming foreign eID claims into something "understandable" for the relying party are therefore necessary.[13] Such services could quite easily integrate selective disclosure of attributes by not showing all attribute-value pairs obtained from the source credential towards the relying party. However, this raises new liability questions for the providers of such services. Thus necessary evidence must be available in case of disputes arising. Instead of retaining all information from source credentials and replies to relying parties with the transformation service, which would enable profiling of user interests or identifying the customer relations of relying parties, using conditional identification may offer a solution in these cases. The necessary evidence would then be forwarded in encrypted form to the relying party who could retain the information on behalf of both parties while the decryption key remains either with the transformation service or a trusted third party.

Such potential use cases will allow for and also ask for further legal evaluation of possibilities and opportunities for privacy-enabling deployments, as next steps of research to be conducted.

[13] For cross-border uses of eIDs the projects STORK, https://www.eid-stork.eu/, and STORK 2.0, https://www.eid-stork2.eu/, propose solutions to verify claims on behalf of relying parties with the eID solutions available to the user. The project FutureID, http://www.furuteid.eu/, broadens the scope to include further services including the transformation of claims and allowing e.g. selective disclosure of attributes.

Appendix A The suggested amendments in detail

Article	Commission's proposal	Proposed amendment	Explanation
Article 1	Subject matter		
Article 1(1)	This Regulation lays down rules for electronic identification and electronic trust services for electronic transactions with a view to ensuring the proper functioning of the internal market.	This Regulation lays down rules for **electronic authentication,** electronic identification and electronic trust services for electronic transactions with a view to ensuring the proper functioning of the internal market.	Introducing the term "authentication" as a basic, broader concept behind identification, to allow for usage of eIDs beyond identification, but to prove an attribute.
Article 1(2)	This Regulation lays down the conditions under which Member States shall recognise and accept electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State.	This Regulation lays down the conditions under which Member States shall recognise and accept electronic **authentication** means of natural and legal persons falling under a notified electronic **authentication** scheme of another Member State.	See above.
Article 2(1)	This Regulation applies to electronic identification provided by, on behalf or under the responsibility of Member States and to trust service providers established in the Union	This Regulation applies to **electronic authentication and** electronic identification provided by, on behalf or under the responsibility of Member States and to trust service providers established in the Union	Se above.
Article 2(2)	This Regulation does not apply to the provision of electronic trust services based on voluntary agreements under private law.		
Article 2(3)	This Regulation does not apply to aspects related to the conclusion and validity of contracts or other legal		

Article	Commission's proposal	Proposed amendment	Explanation
	obligations where there are requirements as regards form prescribed by national or Union law.		
Article 3	Definitions For the purposes of this Regulation, the following definitions shall apply:		
Article 3(1) (new)		**'Transaction' means the particular session or contact between the person and a relying party;**	Justification: The definition of transaction is necessary prerequisite for the subsequent definitions. The limitation to a session excludes e.g. a longer lasting contractual relationship with several contacts between the parties. The latter is considered a relation and covered by the context specific electronic authentication below. A session rather refers to the attention span of a person for a specific task, e.g. visiting a particular website.
Article 3(1a) (new)		**'unlinkable electronic authentication' means the process of using data in electronic form describing attributes of a natural or legal person where the provided attributes and any additionally available information do not allow to link the transaction to a person or any other transaction;**	Justification: For many use cases establishing a direct link to a person is unnecessary and under data protection considerations in general and the data minimisation principle in particular undesired or even non-compliant, Art. 6 (1)(b) and (c) of Directive 95/46/EC. For instance – an online service may need to know that a customer is over 18 years old, but not the name, address or exact birthdate, in order to ascertain that the customer may access a particular service or order particular goods. In this case an anonymous

Article	Commission's proposal	Proposed amendment	Explanation
			proof of the necessary personal attributes is sufficient, allowing the customer to remain anonymous.
Article 3(1b) (new)		**'context specific electronic authentication' means the process of using data in electronic form describing attributes of a natural or legal person where the provided attributes allow verification that the same person has electronically authenticated in the same context in a previous transaction;**	Justification: This introduces the notion of acting under a computer created identifier or self-chosen name, often also connoted with the term of a pseudonym. But due to the ambiguity of the term the latter should be avoided. It accepts the necessity in practice to securely re-identify that the same person is acting. On the internet the proof of a pre-existing relation is often done with a rather insecure solutions, e.g., with shared secret such as username and password. Electronic authentication means may highly add to security and trust in this area. But where it is sufficient to verify that the same person is acting this must not lead to a complete identification of the holder with their real name, birthdate etc. Rather solutions allowing for a secure re-recognition should be used. Context may be understood inter alia as bound to a specific role of the person authenticating, e.g. acting as private user or in a professional context, or bound to a relation with the other party, e.g. the username for a particular online service.
Article 3(1c) (renumbered)	'electronic identification' means the process of an electronic authentication	'electronic identification' means the process of an electronic authentication using	Justification: Identification is an electronic authentication with

Article	Commission's proposal	Proposed amendment	Explanation
	using person identification data in electronic form unambiguously representing a natural or legal person;	**identification data** in electronic form unambiguously representing a natural or legal person **(a) where the identification data can only be used by the relying party for identifying the person if specified conditions are met (conditional electronic identification) or** **(b) where the identification data can be used by the relying party for identifying the person (unconditional electronic identification);**	identification data' (cf. Art. 3 (4b) below) thus where the chosen set of attributes unambiguously represents a person such as such as name, address, birth date, registration number, etc. allowing the identification of the natural or legal person. Terminology aligned and adjusted in accordance with the definition given in Art. 3 (4a) (new), below. Conditional electronic identification supports the numerous cases in which a direct identification is unnecessary for the regular course of affairs but where identification is necessary in exceptional cases, e.g. fraud or other means of abuse. Once the condition is given the relying party may obtain or decrypt the identification data. This allows providing WiFi access to foreigners without learning their identity but in case of criminal actions done the identity of the WiFi user would be at the disposal of the provider. Unconditional electronic identification mans that the relying party receives the information in readable format. Unconditional identification may be necessary as it is required by law (e.g. to prevent money laundering) or for

Article	Commission's proposal	Proposed amendment	Explanation
			the conclusion of contracts where the identity of the acting person is of relevance.
Article 3(2)	'electronic identification means' means a material or immaterial unit containing data as referred to in point 1 of this Article, and which is used to access services online as referred to in Article 5;	'electronic **authentication** means' means a material or immaterial unit containing data as referred to in point 1a of this Article, and which is used to access services online as referred to in Article 5;	Justification: This is a follow-up change due to introducing the concept of authentication as the more generic process with identification as the specific form with identification data.
Article 3(3)	'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to persons as referred to in point 1 of this Article;	'electronic **authentication** scheme' means a system for electronic **authentication or** identification under which electronic authentication means are issued to persons as referred to in point 1 of this Article;	Justification: This is a follow-up change due to introducing the concept of authentication as the more generic process with identification as the specific form with identification data.
Article 3(4)	'authentication' means an electronic process that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data;	***'electronic validation*** means an electronic process that allows the validation of the electronic identification **or electronic authentication** of a natural or legal person; or of the origin and integrity of an electronic data;	Justification: Keeping the terminology established in science and literature for differentiating between electronic authentication and identification (see Article 3 (1a), 3 (1b) and 3 (1c) above the process of verifying the validity of provided attributes requires an alternative terminology other than authentication. Electronic validation has been chosen according to the existing wording of Art. 6 (1) (d).
Article 3(4a) (new)		**'identification data' means any set of attributes the knowledge of which allows to**	Justification: This definition describes identification data in a functional

Article	Commission's proposal	Proposed amendment	Explanation
		get hold of a single person, e.g. the set of name and an address allowing for service of documents or any information leading to these information, e.g. a unique person number;	manner. A comprehensive list of attributes has intentionally been omitted as Member States may consider different attributes mandatory for a clear and unambiguous identification.
Article 3(4b) (new)		**'issuer' means an entity who vouches for the validity of one or more attributes of a person, by issuing an electronic identification means to a holder;**	Justification: Necessary definition to directly address "issuers" with the data protection requirements, see Art. 4a below.
Article 3(4c) (new)		**'validation service' means the entity responsible for an authentication possibility ensured by a notifying Member State according to Art. 6 (1) (d);**	Justification: Necessary definition to address "validation services" with the data protection requirements, see Art. 4a below.
Article 3(4d) (new)		**'holder' means a natural or legal person to whom an electronic authentication means is issued;**	Justification: Missing definition.
Article 3(4e) (new)		**'relying party' means a natural or legal person to whom the holder of an electronic authentication means verifies attributes;**	Justification: The draft already referred to relying parties in Article (1) (d) without a proper definition.
Article 4	Internal market principle		
Article 4a(new)		Data processing and protection	Justification: The reference to the data protection legislation of the Union appears only after the chapter on electronic identification, which may mislead the interpreter of the law to believe that it is not meant to apply with equal weight on the electronic identification chapter of the regulation. This seems to be a editorial, but

Article	Commission's proposal	Proposed amendment	Explanation
			necessary adjustment. Therefore this proposal is to move the reference from Article 11 to article 4a(new). See also amendments to Article 11.
Article 4a(1)(new)		**Trust service providers, issuers, validation services, relying parties and supervisory bodies shall ensure fair and lawful processing in accordance with Directive 95/46/EC when processing personal data**	Justification as above: The reference to the data protection legislation of the Union appears only after the chapter on electronic identification, which may mislead the interpreter of the law to believe that it is not meant to apply with equal weight on the electronic identification chapter of the regulation. This seems to be a editorial, but necessary adjustment. Therefore this proposal is to move the reference from Article 11 to article 4a(new). See also amendments to Article 11.
Article 4a(2)(new)		**Trust service providers, issuers, validation services shall process personal data according to Directive 95/46/EC. Such processing shall be strictly limited to the minimum data needed to issue and maintain a eID or certificate, validate an electronic authentication or to provide a trust service.**	Justification as above: The reference to the data protection legislation of the Union appears only after the chapter on electronic identification, which may mislead the interpreter of the law to believe that it is not meant to apply with equal weight on the electronic identification chapter of the regulation. This seems to be a editorial, but necessary adjustment. Therefore this proposal is to move the reference from Article 11 to article 4a(new). See also amendments to Article 11.
Article 4a(3)(new)		**Trust service providers, issuers, validation services shall guarantee the confidentiality and integrity of data related to a person to**	Justification as above: The reference to the data protection legislation of the Union appears only after the chapter

Article	Commission's proposal	Proposed amendment	Explanation
		whom the eID is issued or the service is provided.	on electronic identification, which may mislead the interpreter of the law to believe that it is not meant to apply with equal weight on the electronic identification chapter of the regulation. This seems to be a editorial, but necessary adjustment. Therefore this proposal is to move the reference from Article 11 to article 4a(new). See also amendments to Article 11.
Article 4a(4)(new)		**Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent issuers or from indicating in electronic authentication means a pseudonym instead of or in addition to the holder's name or prevent trust service providers indicating in electronic signature certificates a pseudonym instead of the signatory's name.**	Justification as above: The reference to the data protection legislation of the Union appears only after the chapter on electronic identification, which may mislead the interpreter of the law to believe that it is not meant to apply with equal weight on the electronic identification chapter of the regulation. This seems to be a editorial, but necessary adjustment. Therefore this proposal is to move the reference from Article 11 to article 4a(new). See also amendments to Article 11. Additionally, the text concerning electronic authentication means clarifies that issuers should not be prevented from providing further attributes enabling selective disclosure of individual attributes, including pseudonyms in the sense of context specific electronic authentication.

Article	Commission's proposal	Proposed amendment	Explanation
Article 4a(5)(new)		**Validation services must not collect or retain data beyond the extent necessary for the process of validation. Validation services must not profile holders. Data must not be retained for the sole purpose of providing proof in liability cases.**	Justification: This requirement results from the data minimisation principle. In particular it prevents that the validation services collects and retains data and may create profiles about the online behaviour of citizens. It further prevents that validation services may collect a list of customers of a particular relying party and thus protects the business interests of the relying parties as well. The potential liability must not lead to an uncontrolled collection of personal data. And the suggested solution does not conflict with the liability of the Member States set forth in Article 6 (1) (e). The unambiguous attribution of the data to a single individual may still be ensured at the time of issuance or verification as requested. As proof in potential proceedings on liability questions the sealed or signed proof provided by the validation service will suffice. As generally the provisions on liability in Art. 6 require clarification and rephrasing such changes may require follow-up changes of this norm necessary.
Article 4a(6)(new)		**Issuers and relying parties may only ask for as much personal data as is necessary to**	Justification: This is a principle that is in either case mostly applied by

Article	Commission's proposal	Proposed amendment	Explanation
		establish that the attributes of the individual that they are interacting with are the appropriate ones for the purpose at hand.	service providers, and is an integral part of the data minimisation principles and the values enshrined in the data protection legislation of the Union and the member states.
Article 5	Mutual recognition and acceptance When an electronic identification using an electronic identification means and authentication is required under national legislation or administrative practice to access a service online, any electronic identification means issued in another Member State falling under a scheme included in the list published by the Commission pursuant to the procedure referred to in Article 7 shall be recognised and accepted for the purposes of accessing this service.	Mutual recognition and acceptance When an electronic **authentication** using an electronic **authentication** means and **verification** is required under national legislation or administrative practice to access a service **of the same sector** online, any electronic **authentication** means issued in another Member State falling under a scheme included in the list published by the Commission pursuant to the procedure referred to in Article 7 **of the same or higher assurance level issued** shall be recognised and accepted for the purposes of accessing this service. Where a Member State separates between sectors of applicability for eIDs it may limit recognition and acceptance of notified electronic authentication means to the sector of origin.	Justification: Follow-up changes in diction. To prevent a race to the bottom and undermining security concepts Member States should not be forced to accept electronic authentication means with a lower assurance level. E.g. it would be inappropriate force Member States to allow access with a username and password secured eID towards services that require two factor authentication with a secure token to access under national law of the Member State. Likewise where Member States foresee a separation of sectors, e.g. between public, health and financial sectors, these data protection and security considerations must not be negated by enforcing the recognition and acceptance of foreign eIDs from another sector even if these meet the required assurance level. Implementing acts: It will be necessary to define with implementing acts a

Article	Commission's proposal	Proposed amendment	Explanation
			systematic of sectors based on factually existing separations in the Member States. For assurance levels such systems already exist as a basis, e.g. the ISO/IEC 29115 standard.
Article 6	Conditions of notification of electronic identification schemes	Conditions of notification of electronic **authentication** schemes	Justification: Follow-up changes.
Article 6(1)(a)	Electronic identification schemes shall be eligible for notification pursuant to Article 7 if all the following conditions are met: (a) the electronic identification means are issued by, on behalf of or under the responsibility of the notifying Member State;	Electronic **authentication** schemes shall be eligible for notification pursuant to Article 7 if all the following conditions are met: (a) the electronic authentication means are issued by, on behalf of or under the responsibility of the notifying Member State;	Justification: Follow-up changes.
Article 6(1)(b)	the electronic identification means can be used to access at least public services requiring electronic identification in the notifying Member State;	the electronic **authentication** means can be used to access at least public services requiring electronic **authentication** in the notifying Member State;	Justification: Follow-up changes.
Article 6(1)(c)	the notifying Member State ensures that the person identification data are attributed unambiguously to the natural or legal person referred to in Article 3 point1;	the notifying Member State takes necessary means to ensure that the information on personal attributes issued in an electronic **authentication** means unambiguously attributes to the holder and that the information on personal attributes are correct at the time of issuance.	Justification: All electronic authentication means should be clearly bound to the person they have been issued to. A clear linkability to the holder by means of the data provided to the relying party is, however, only necessary in the case of electronic identification.
Article 6(1)(d)	the notifying Member State ensures the availability of an authentication possibility online, at any time and free of charge so that any relying party can validate the	the notifying Member State ensures the availability of ***an authentication possibility free of charge***. For this Member States must either provide for an authentication possibility	Justification: This establishes clear requirements for what an authentication service is and could be, and further details the mechanism

Article	Commission's proposal	Proposed amendment	Explanation
	person identification data received in electronic form. Member States shall not impose any specific technical requirements on relying parties established outside of their territory intending to carry out such authentication. When either the notified identification scheme or authentication possibility is breached or partly compromised, Member States shall suspend or revoke without delay the notified identification scheme or authentication possibility or the compromised parts concerned and inform the other Member States and the Commission pursuant to Article 7;	online or otherwise provide all necessary specifications and reference implementations for relying parties to verify an electronic authentication or an electronic identification with proportionate effort. ~~**Member States shall not impose any specific technical requirements on relying parties established outside of their territory intending to carry out such authentication.**~~ When either the notified identification scheme or authentication possibility is breached or partly compromised, Member States shall suspend or revoke without delay the notified identification scheme or authentication possibility or the compromised parts concerned and inform the other Member States and the Commission pursuant to Article 7; ***other affected parties shall be notified in accordance with the obligations laid out in Article 15(2).***	whereby cooperation around development of appropriate technological standards and requirements could be undertaken. The validation solution may be set up as a validation service online. Together with the amendment to Article 4a (5) the suggested solutions should reasonably prevent profiling attempts or that centralized databases are built with the validation service. Allowing and encouraging further development of privacy-preserving solutions prevents a 'race to the bottom' in terms of data protection and security aspects in the eID area. Also in the light of technological neutrality such a path for upcoming solutions must remain open. Therefore only few necessary cornerstones may be demanded including a clear reference to data protection requirements. As privacy-preserving solutions allowing for an end-to-end authentication demand for some technical requirements on the relying parties' side, it must be possible to require that proportionate action is taken by relying parties, e.g. installing a browser plug in or running software

Article	Commission's proposal	Proposed amendment	Explanation
			of a USB stick without further installation. This is a very important but not invasive amendment to the regulation as also the current draft necessarily requires that the relying party understands the authentication process, thus has some software installed. Revocation: The revocation of a service must be possible without creating linkability of the electronic authentication means, in particular unique serial numbers send with each authentication must not be used.
Article 6(1)(d-a)(new)		**Validation services must provide at the discretion of the holder a signed or sealed proof of attributes selected by the holder.** **In case of an anonymous authentication the provided proof must not be linkable to the person authenticated or to any other proof provided.** **In cases of context specific electronic authentication linkability is permissible only within the specific context.**	Justification: This paragraph addressed particular duties of the validation services. If and as long as third parties are involved in the authentication process entity should be deployed for the benefit of data protection. In particular where the eID solutions of the Member States do not (yet) support attribute selection the involved third party could and should act as a privacy proxy concealing unnecessary information from the relying party. Demanding validation services to provide proof over individual attributes is a direct consequence of

Article	Commission's proposal	Proposed amendment	Explanation
			the principle of data minimisation applicable to all relying parties within the European Union. To prevent any form of profiling the provided proofs must not be linkable, thus must not contain serial numbers or other means that would allow identify a person authenticating even for the issuer or validation service itself. Also it should not be possible for relying parties to see that the same person has authenticated before. Providing selective disclosure of attributes by the validation services may give valuable impulses for future development of the national eID solutions within the notifying Member States and lead towards the acceptance of more privacy preserving eID solutions in a mid- or long term. The selection is to the discretion of the holder as it is up to the data subject to decide which information to disclose.
Article 6(1)(e)	the notifying Member State takes liability for: – (i) the unambiguous attribution of the person identification data referred to in point (c), and – (ii) the authentication possibility specified in point (d).	the notifying Member State takes liability for: – (i) that the data provided for the electronic authentication means are unambiguously ***verifying the attributes of*** a single natural or legal person – (ii) the authentication possibility specified in	*Justification: This again removes the emphasis from an unambiguous identification to the attribution credentials model of authentication individuals with the right amount of information at the right time.* It is necessary to clarify what the

Article	Commission's proposal	Proposed amendment	Explanation
		point (d).	liability is about. Currently the article reads as if it is not about the correctness of the data but that the electronic authentication means and any information provided with it is clearly attributed to a single person. Thus the member state vouches for the fact, that for each authentication means there is only one single person but a single person may have several authentication means (e.g. an eID-token and a eHealthCard, or several ePassports). If this is what is meant a clarification should be added as the current version may mislead a hasty reader to believe that the Member State vouches for the correctness of the provided identity information.
Article 6(2)	Point (e) of paragraph 1 is without prejudice to the liability of parties to a transaction in which electronic identification means falling under the notified scheme are used.	Point (e) of paragraph 1 is without prejudice to the liability of parties to a transaction in which electronic **authentication** means falling under the notified scheme are used.	Justification: Follow-up amendment.
Article 7	Notification 1. Member States which notify an electronic identification scheme shall forward to the Commission the following information and without undue delay, any subsequent changes thereof:	Notification 1. Member States which notify an electronic authentication scheme shall forward to the Commission the following information and without undue delay, any subsequent changes thereof:	
Article 7(1)(a)	a description of the notified electronic identification scheme;	a description of the notified electronic **authentication** scheme;	
Article 7(1)(b)	the authorities responsible for the notified	the authorities responsible for the notified	

Article	Commission's proposal	Proposed amendment	Explanation
	electronic identification scheme;	electronic **authentication** scheme;	
Article 7(1)(c)	information on by whom the registration of the unambiguous person identifiers is managed;		
Article 7(1)(d)	a description of the authentication possibility;		
Article 7(1)(e)	arrangements for suspension or revocation of either the notified identification scheme or authentication possibility or the compromised parts concerned.	arrangements for suspension or revocation of either the notified **authentication** scheme or authentication possibility or the compromised parts concerned.	

Appendix B References

[Ca11] J. Camenisch, I. Krontiris, A. Lehmann, G. Neven, C. Paquin, H. Zwingelberg and K. Rannenberg, "D2.1 Architecture for Attribute-based Credential Technologies – Version 1" Deliverable, version 1, 2011. Available at: https://abc4trust.eu/download/ABC4Trust-D2.1-Architecture-V1.2.pdf (2013-10-30).

[Du12] J. Dumortier, and N. Vandezande, Niels "Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market," ICRI Research Paper No. 9, September 26, 2012. Available at SSRN: http://ssrn.com/abstract=2152583 or http://dx.doi.org/10.2139/ssrn.2152583.

[EDPS13] European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Commission proposal for a Regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market (ElectronicTrust Services Regulation), 2012, Official Journal 2013/C 28/04. Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-09-27_Electronic_Trust_Services_EN.pdf.

[Qu13] Gisela Quiring-Kock: Stellungnahme des Hessischen Datenschutzbeauftragten zum „Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt", COM(2012) 238 final, 2012. Available at: http://www.datenschutz.hessen.de/download.php?download_ID=255.

[Sp13] Gerald Spindler, Matti Rockenbauch: Die elektronische Identifizierung - Kritische Analyse des EU-Verordnungsentwurfs über elektronische Identifizierung und Vertrauensdienste, in Mulimedia und Recht (MMR), 2013, pp. 139-148. Available at: http://beck-online.beck.de/Default.aspx?typ=reference&y=300&z=MMR&b=2013&s=139&n=1.

[SS11] SSEDIC, "Year 1 eID adoption Survey," 2011. Available at: http://www.eid-ssedic.eu/images/stories/pdf/SSEDIC%20D2.3.1%20eID%20Adoption%20Survey%20Y1%20v1.1.pdf (2013-10-30).

[Zw11] Harald Zwingelberg: Necessary Processing of Personal Data: The Need-to-Know Principle and Processing Data from the New German Identity Card, in: Simone Fischer-Hübner et al. (eds.), Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology Vol. 325, Springer, 2011, Available at: http://link.springer.com/chapter/10.1007%2F978-3-642-20769-3_13.