Identity management in cloud computing in conformity with European Union law? – Problems and approaches pursuant to the proposal for a regulation by the European Commission on electronic identification and trust services for electronic transactions in the internal market

Stephan Sädtler[1]

Chair for Public Law, IT-Law and Legal Information Technology,
held by Prof. Dr. Gerrit Hornung, LL.M.,
University of Passau
Innstr. 39
94032 Passau
stephan.saedtler@uni-passau.de

Abstract: On 4 June 2012, the EU Commission submitted a draft of a regulation on "electronic identification and trust services for electronic transactions in the internal market" [EC12][2]. Due to its impact onto the infrastructure of the new German identity card (nPA) it is subject to fierce criticism, particularly from Germany. This essay seeks to address that criticism and to discuss potential approaches, amongst others that of the research project „SkIDentity – Trusted Identities in the Cloud" of the „Trusted Cloud" programme[3], whilst also addressing accompanying questions of law in the context of identity management in cloud computing.

1 Introduction

Data protection and data security in the sector of information technology – and especially in cloud computing – have become a continuous issue due to the rapid technological development and the accompanying variety of applications of IT-systems. With the constant increase of online-based data processing in nearly all areas of life and business and the corresponding potential risks, the demands for security have steadily increased. Driven by that demand, security technology has considerably improved. One accomplishment of that development in Germany was the introduction of the electronic

[1] Stephan Sädtler works as a research assistant at the University of Passau and is a certified specialist lawyer for IT-Law. The essay was originally written in German. The translation was poduced by Ray Migge, a student and lecturer for English constitutional law at the University of Passau, to whom the author feels greatly indepbted. The essay is part of the research project "SkIDentity – Trusted Identities for the Cloud", sponsored by the Federal Ministry of Economics and Technology (fundig plan # 01MD11031).

[2] Hereafter also reffered to as eIAS-R-D.

[3] See http://www.trusted-cloud.de/de/1645.php.

identification (eID) via the new identity card (nPA), as its underlying infrastructure is regarded as highly secure and effectively balances the interests of the user including a high level of data protection and those of the recipient regarding the authenticity of the data (regarding the eID-concept of the nPA see [RHS08][Bo10][Mö11]). Most of the member states have also issued electronic identification means that may prove suitable to strengthen trust in online applications. Currently the implementation of applications deemed secure often fails due to a lack of acceptance of such technologies, which, amongst other factors, is often caused by the significant financial and technical costs for service providers. Mere national approaches to online-applications – often in a cross-border context – are subject to several disadvantages. In the light of that, the efforts aiming at harmonizing the framework for electronic identification whilst respecting the principle of technology neutrality (see [EC12, recital 21]) and specifically the Commission's draft regulation on electronic identification and trust services for electronic transactions in the internal market, appear comprehensible and reasonable/sensible.

In Germany, however, the draft has been the object of justified criticism rather than approval (see [Ho12][SpRo13]; for criticism in the area of trust services see [RoJo13]). Constructive amendments to the proposed regulation are imperative, as calls for improvements have legitimately been raised. As the regulatory aims of the draft are deemed predominantly sensible and sound, it cannot stop there: in the interest of a mutual approach, it is rather necessary to find adequate technical solutions pursuant to the objectives of the European Union legislation.

This essay seeks to cover valid points of criticism along with a discussion on potential technological solutions in the context of cloud computing. It will be limited to the respective provisions on electronic identification in Chapter II, which is independent of the provisions on trust services in connection with electronic signatures, and the accompanying general provisions in Chapter I.

2 General Content of the Provisions on Electronic Identification

Central element of the regulation on electronic identification is the requirement for online service providers in Art. 5[4] to adhere to the principle of mutual recognition and acceptance of electronic identification means which will be notified following a notice to the European Commission in accordance with Art. 7 and the provisions on an independent procedure in Art. 6. Adherence to the principle of mutual recognition and acceptance is compulsory only in so far as an electronic identification by electronic identification means and authentication for an individual online service is required by domestic law or domestic administrative practice. Whilst the far-reaching implications of this provision are formulated unambiguously, the requirements as to application and notification remain largely unclear, as will be shown in the following.

[4] Art. without reference to a law or regulation are those of the eIAS-R-D.

2.1 Scope of Application

2.1.1 National eIDs

The first alternative of Art. 2 (1) restricts the regulation's applicability to electronic identification which is provided by, on behalf or under the responsibility of a Member State. It is complemented by Art. 6 (1)(a), which requires the implementation of electronic identification means by, on behalf or under the responsibility of an individual Member State.

Whilst the nPA is within the scope of application as it is issued by the Federal Republic of Germany, other identification means, e.g. electronic cards of the telematics infrastructure[5] of the health care services or the identification authentication according to § 6 De-Mail-G are difficult to define as being within the scope of application. At best, they could fall within the second and third alternative of Art. 6 (1)(a), i.e. "[…] issued […] on behalf of or under the responsibility of the notifying member state […]".

The application of Art. 6 (1)(a) to the electronic health data card appears reasonable as it is based on a legal requirement in accordance with § 291a SGB V; however, responsibility lies not with the state but with health insurance funds and companies, which in accordance with § 291a (7) and § 291b SGB V have entrusted the German company "Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik)" with their responsibility. Indicative of public responsibility is the supervision and authorisation by the German Federal Ministry for Health and Social Insurance (e.g. § 291b (2)). Furthermore, the shareholders of gematik are largely publically financed. Including the private sector in the process of the issuance of electronic identification means does not preclude an assumption of a public responsibility (see [EC12, recital 14]). A serious counter-argument can be found, though, in the wording of the explanatory memorandum to the regulation: "Most EU Member States have introduced some form of electronic identification system" (see [EC12, explanatory memorandum, 3.3.2]). It suggests that the underlying presumption of the draft was the existence of a single national main identification scheme in the context of the regulation per individual Member State.

Even more questionable is whether the identification verification in accordance with § 6 De-Mail-G is within the scope of application of the draft. De-Mail services do not operate on behalf of the Member States. Although these services are subject to accreditation pursuant to § 17 De-Mail-G, a responsibility by the state as outlined in the draft must nonetheless be dismissed, as the accreditation does not entail any liability by the state. The wording of the draft provides a further argument in favour of such result as it requires the issuance of identification means as a pre-condition for notification of electronic identification schemes in Art. 6 (1)(a).

It is fair to conclude, that merely the nPA falls unambiguously within the scope of application of the eIAS-R-D, whilst it remains questionable whether that is the case for

[5] http://www.gematik.de/cms/de/egk_2/egk_3.jsp.

other German electronic identification schemes. That would be changed by the amendment proposed in the draft report by the European Parliament Committee on Industry, Research and Energy on 4 April 2013, which suggested at least a change to the wording of Art. 6 (1)(a) to "[…] either issued by the Member state, or issued by another entity as mandated by the Member State or issued independently but recognised by the notifying Member State […]" [EPC13, p. 12] and Art. 2 (1), thereby covering eID-schemes which are merely recognised by Member States. Both, the health data card and the De-Mail verification scheme indubitably fall within that category. However, it would thwart all efforts to notify merely the main identification scheme of any individual Member State.

2.1.2 Restriction to Public Services?

The recitals of the regulation give the impression that only public online services shall be subject to the principle of mutual recognition and acceptance. Recital 11 primarily refers to "[…] cross-border online services offered by the Member States […]". Services provided by the private sector are explicitly excluded as it refers to only those services provided by Member States. Furthermore, recital 9 manifests the aim to overcome obstacles in interactions with public authorities. Pursuant to recital 14, the decision on whether the private sector may be involved in the issuance of electronic identification means shall be left to the individual Member States. Apart from the imprecise wording of that provision it seems to contradict the aim, proclaimed in the very same recital, of diminishing the discrimination between public and private sectors. The wording of Art. 5 itself however does not contain any such restriction as it includes all online services requiring an electronic identification for access (hence, also private applications, for which such an identification is required by law). Merely the referral to the "administrative practice" is directed towards the public sector. Whether that is applicable also to the first alternative remains unclear. Should the regulation seek to target the public sector only, a clarification as to that effect is indispensable.

The very same applies to the proposed requirement of an electronic identification by electronic identification means and authentication. The strict wording would lead to an applicability of the regulation only where the use of online services without an electronic identification and authorisation is excepted. The aforementioned draft report by the European Parliament Committee on Industry, Research and Energy would substitute the term "required" by "available". That alteration appears advisable in the light of the foregoing. However, it would extent the scope of application significantly.

2.2 Conditions for Notification in Art. 6 (1)(d)

Pursuant to sentence 1 and 2 of Art. 6 (1)(d) electronic identification schemes shall be eligible for notification only on the premise of the notifying Member State guaranteeing the availability of an authentication possibility online, at any time and free of charge, enabling the validation of personal identification data whilst refraining from imposing specific technical requirements on relying parties established outside of the notifying Member State's territory. According to recital 15, that provision shall "rule out any specific national technical rules requiring non-national parties to […] obtain specific

hardware or software to verify and validate the notified electronic identification." Such restrictions of specific technical requirements do not apply to the user (holder) of the identification means [EC12, explanatory memorandum, 3.3.2].

As suggested previously, the driving force for that approach is the principle of interoperability of the various existent schemes. Obliging service providers to implement various differing eID-infrastructures would entail immense technical and financial costs, the avoidance of which could be achieved only by refraining from cross-border transactions. Small businesses and minor public authorities would simply not be able manage these costs.

However, the obligation on Member States to provide possibilities to validate person identification data free of charge leads to the question of who will assume responsibility for the costs of that infrastructure. Insofar as it is intended that costs shall be passed on to the users, the concept might fail due to a lack of acceptance by the users. That problem could at least theoretically be solved by public funding. However, it appears unlikely that safe infrastructures could be established without any specific technical requirements for service providers. In a secure infrastructure, a service provider will only be able to read received data with an appropriate software. It appears the principle of interoperability has been given unacceptable precedence over the principle of security.

3 Consequences for the nPA

In the literature, the draft faced fierce criticism for the requirements as the notification in Art. 6 (1)(d) would basically represent the end for electronic identification of the nPA [Ho12, p. 634] or would at least be in stark contrast to the data protection friendly concept of the nPA (critical also [RoJo13, p. 68] [SpRo13, p. 147 et seqq.]). In fact, the nPA infrastructure involves considerable specific technical requirements and financial costs for service providers: According to § 18 (4) PAuswG, the specific bilateral relationship of the nPA-infrastructure requires a service provider according to § 2 (3) PAuswG, to use a valid authorisation certificate to be able to read the data of the German identity card. The certificate is issued on the basis of an authorisation by the contracting authority (Vergabestelle für Berechtigungszertifikate) in the Federal Office of Administration (Bundesverwaltungsamt). It is to be issued if the requirements in § 21 (2) PAuswG are met, which principally serve the principle of data protection and ties the issuance of the certificate to a pre-validation of the service provider and its object of business (see in detail [Mö11][Bo10, p. 3365 et seqq.]).

The service provider requires a specific technical infrastructure comprising hard- and software to be able to read the data. The considerable costs of the infrastructure must be borne by the service provider. As a service provider aiming at the issuance of an authorisation certificate is classified as a relying party pursuant to Art 6 (1)(d), the nPA-infrastructure imposes specific technical requirements on it. The basic concept of the nPA-infrastructure thereby does not meet neither requirement of the regulation: it does not provide possibilities of authentication and validation free of charge nor does it

refrain from imposing specific technical requirements on relying parties. Hence, it is not notifiable under Art.6 (1)(d).

That leads to the much criticised and contradictory result that institutions that accept the nPA will also have to accept the electronic IDs of other Member States although they do not provide the same level of data protection (as those IDs are covered by the principle of mutual recognition in Art. 5), whilst the nPA would not have to be accepted by other Member States (as it is not notifiable under Art. 6). The consequence is that the more secure an ID is, based on specific technical components, the less probable its notifiability is. That would defeat the proclaimed objective of creating trust in online services.

4 Approaches to the Problem

4.1 "Gateway-Approach" by the STORK-Project[6]

The contradiction of Art. 6 (1)(d) to the proclaimed aim of enhancing trust in electronic identification and authentication could be resolved by differentiating between specific technical requirements on the one and general technical requirements in the sense of requirements generally applicable on the other hand. Such generally applicable requirements could be defined by the EU Commission, which would receive the authority in Art. 8 (3) to pass delegated legislation on technical minimum standards. That interpretation of the draft and Art. 6 (1)(d) would allow the existence of a homogeneous scheme based on a high level of protection. The technical harmonisation of various eID-schemes within the EU will be as difficult, though, as would be a safe scheme without specific technical requirements.

From a technological perspective, the factually sole solution would be an intermediate institution independent of any relying party, which would coordinate all schemes and would make obsolete the utilisation of differing system components by service providers. This so-called gateway-approach or proxy-approach was developed by the STORK[7] research project, whose main component was a central Gateway in each member state. Should the draft of the regulation have meant to provide for such system [Be13], it would have required a more precise wording that would have had to regulate the specification of general criteria. The aforementioned proposal would provide such system and would eliminate the provision regarding cost free authentication and validation possibilities.[8]

Apart from that though, the approach faces major objections due to data protection concerns. Technically, it would be possible for the intermediate institution to collect and store all user identification data and information on its specific use. That would allow a

[6] See https://www.eid-stork.eu/; in this context also [Be13].
[7] Another approach developed by the STORK-project is the middelware-approach, which would intends the setup of a middleware-software at the service provider. However, as it would also involve specific technical requirements, it neiter would be covered by the current requirements of Art. 6 (1)(d).
[8] According to [ECP13, p. 16] requirements shall be admissable, which have been defined by the Commission in a special procedure.

single institution to create a comprehensive user profile. It must be kept in mind, though, that the use of external identity providers is not uncommon: Even the technical guideline on the eID-service of the nPA-infrastructure explicitly allows outsourced eID-services (see [BSI12, 2.4.2]). The external service provider is responsible for the reading, authenticating and forwarding of nPA data including the result of the validation process to the actual service provider. The external provider thereby manages the authentication certificate of the original service provider. The difference to a central identification provider is that the external provider is not responsible for the entire identification management of a Member State. Furthermore, the external service provider is providing the data processing services pursuant to § 11 BDSG and thereby is subject to a duty to comply with the controlling service provider's instructions.

4.2 SkIDentity-Project

The research project SkIDentity could provide some relief as it might assist in ensuring that the nPA-infrastructure meets the notification requirements whilst overcoming the disadvantages of a central gateway-approach: The project aims at bridging cloud-applications and safe electronic identification means, such as the nPA and the German health data card. It seeks to overcome hurdles for small and medium sized businesses and local authorities, such as the lack of adjustment of cloud-service infrastructures to the specific needs of eIDs and the resulting complications, such as technical compatibility issues, unsolved questions of data protection and questions of law (see [HH+11, p. 297]). Integral part of the SkIDentity-infrastructure is a so-called identity-broker, which would connect the various identification services with the cloud-service providers. Whilst the identity provider would process the actual authentication, the identity-broker merely bundles these services and makes them available to cloud-service providers in a single interface, a so-called cloud-connector. Such single interface makes specific technical requirements in the sense of differing requirements obsolete. The applicability of the concept is not limited to cloud services but can be extended to any internet service.

From a legal perspective, the identity-broker is to not be understood as a natural or legal person. It could be managed by an identity provider as well as by a fourth entity, independent from user, cloud-service provider and identity provider. Thereby, a system would be established that could be used by a cloud-service provider as a relying party without specific technical requirements and free of charge and at the same time remove all data protection concerns about a centralized identity provider by separating the identity provider from the institution that communicates with the user and the cloud-service provider.

5 Questions of Law

Nonetheless, the SkIDentity-project also raises questions of law, which need to be addressed in the context of technical design that conforms to legal requirements.

5.1 Personal Identity Card Law

It remains questionable whether the SkIDentity-infrastructure can be reconciled with the strict requirements of the German personal identity card law. It depends largely on whether an entity independent of the cloud-service provider and involved in the identity management process of reading identification data will be able to obtain an authentication certificate pursuant to § 21 PAuswG for the purpose of identity transfer. It would need to meet the requirements in § 21 (2) PAuswG and § 29 PAuswV. It is questionable whether the entity would make business-related transmissions according to § 21 (2)(1) Nr. 2 part of its objects of business, as § 21 (2)(1) Nr. 2 PAuswG renders it, unlawful.

The determination of business-related transmissions as an exclusion characteristic is based on § 29 BDSG (see [BT08, p. 43]), which by way of example determines advertisements, the practice of credit agencies and address trading to be such transmissions and therefore addresses services whose object of business is the commercialisation of the value of information of data. The exclusion of such transmissions shall prevent that the electronic identification scheme be used as a tool to collect data for address pools or other business entities dealing with data, thereby diminishing the trust of citizens in electronic identification schemes, as the use of such schemes could, for example, lead to an increase of unwanted promotional mailings (see [BT08, p. 43]).

Even though it involves the transmission to cloud-service providers, the aim and actions of a potential identity-broker are different, as the identity-broker would also act in the interest of the users. The object of the transmission would be authentication and not the commercialisation of the data, which makes it fundamentally different from § 29 BDSG and § 21 (2)(1) Nr. 2 PAuswG. Furthermore, § 21 (2) PAuswG must be read in the light of the right to informational self-determination. As far as the freedom and rights of the user are duly taken into account within an infrastructure, it must be rendered admissible as long as it does not compromise the security and safety of the infrastructure.

The same interpretation must be applied to § 29 (1) Nr. 1 PAuswV, according to which the reading of data performed for third parties is prohibited due to data security and protection concerns. In the light of the informational self-determination, such restriction should not be applicable to the provision of data to the owner of IDs. Originally, the section included such a restriction but recently had been amended to exclude ID owners from the restriction.[9]

It follows, that it certainly is possible to design a SkIDentity-infrastructure that would involve an identity-broker managed by an independent party with the aim of independently analysing nPA-data, and which would conform to the requirements of the personal identity card law. As a precondition, the user must retain exclusive control over his personal data without compromising the safety and reliability of the infrastructure. Technical assistance by the provider of broker services does not affect the owners' control. Legal literature proposed an example scenario involving an online data-safe

[9] See Art. 2 Nr. 3 PassVuaÄndG of 20.02.2013, BGBl. (2013) I, p. 330 (Nr.10).

provided by the identity-broker, in which nPA data and the authentication result could be stored and within which the ID owner could independently manage the stored data (see [Mö11, § 21, para. 15]). Should data be transferred to cloud-service providers using this method, the exclusion characteristics of the personal identity card law would not be applicable. Neither would it be rendered an evasion of the system of authentication certificates (in a similar context discussed by [Sch10, p. 55]) as the entity responsible for the management of the data would still require such certificate. The cloud-service provider would also still be bound to the general data protection law. The legal relationship between the service provider and the owner of the certificated furthermore could be subjected to civil agreements, barring the service provider e.g. from § 29 BSGD activities. This technical approach is not limited to the nPA-infrastructure but could be applied to a variety of eIDs.

5.2 Further Requirements of the eIAS-R-D

Nonetheless, the imprecise wording of the draft leaves some fundamental questions regarding the requirements of the eIAS-R-D unanswered: Should the term "specific technical requirements" be read strictly or should there not follow a clarification to allow general technical requirements (defined, for example, by the Commission), factually no eID-scheme would be notifiable.

Further clarification is also needed regarding the "relying parties". As identity provider and identity-broker are neither the final recipient nor end-user of the data it would be reasonable to not classify them as relying parties for the purpose of the regulation. Should that be seen different – e.g. because an identity provider or broker under certain circumstance should be liable to the cloud-service provider and therefore must be able to rely on the hard- and software of the user – the notification requirements would not be met by the nPA-regulation as it cannot be designed to exclude specific technical requirements for the identity provider and for the broker provider.

It remains questionable whether that would even sufficiently ensure a possibility for authentication and validation pursuant to Art. 6 (1)(d). Besides, the provision would require the cooperation of the ID owner and the owner's approval of the involvement of another identity.

5.3 Adequate Level of Confidence

Furthermore, it must be ensured technologically that the level of security of and confidence in the infrastructure matches that of a bilateral relationship. That could be accomplished by making the relationship between the owner of the certificate and the cloud-service provider similar to that between the owner of the certificate and the external eID-service (see [BSI12, 2.4.2]). That question is of special relevance where the authentication entails specific legal consequences, e.g. in § 3a (2) VwVfG. The provision was amended due to the E-Government-Initiative and in its new version provides for a substitution of the written form by filling out electronic forms (see [BT12, p. 13]). So far, the written form could only be substituted by using a qualified electronic signature pursuant to the signature law – as is still the case in civil law transactions pursuant to

§ 126a BGB. It would have to be evaluated in how far the legal requirements would still be met in an extended nPA-infrastructure.

5.4 Downside to the Principle of Mutual Acceptance

5.4.1 Lack of Requirements regarding Data Protection and Security

As the aforementioned approach focussed on the notifiability of eID-systems, its implementation left unsolved existent problems regarding the mutual acceptance of foreign notified authentication means: Primarily, a lack of requirements for data protection and security persists. Accepting the nPA in EU-Member States whilst requiring Germany to accept as equivalent to the nPA such identification means with a lower level of security does not render German nor European legal transactions any more secure than they have been so far. However, the approach taken in the regulation might be helpful: Art. 6 (1)(e) makes Member States liable for the unambiguous attribution of the person identification data pursuant to Art. 3 (1) (which is a requirement for notification pursuant to Art. 6 (1)(c)) and for the provision of an authentication possibility pursuant to Art. 6 (1)(d). Potential liability for failure is a distinct incentive for Member States to ensure a high level of security as every Member State seeks to avoid liability (compare also [Bo13]). How effective that approach will be depends on the interpretation of the provisions on liability. The characteristic of unambiguous attribution has been construed narrowly (see [SpRo13, p. 144 et seqq.]). That provision could also, however, be construed in a wider sense, thereby assuming liability for any data leaks. That interpretation would lead to a significantly higher level of data protection and security. However, the afore-criticised exclusion of specific technical requirements for relying parties contradicts an assumption of comprehensive liability. Nonetheless, the liability approach could prove to be an effective measure. However, it would require more precision and reconciliation with the requirements of Art. 6 (1)(d).

5.4.2 Other eIDs

Applying the regulation to the identification means used in the telematics infrastructure of the German health data card would take that infrastructure ad absurdum: Notified identification means of other Member States would have to be accepted within that infrastructure. The evidence suggests that it is practical to exclude identification means used in individual sectors from the scope of application of the regulation. It must also be considered, that the German health data card, although it does represent a means of authentication, is an integral part of the telematics infrastructure that was designed to enhance the use of the electronic health data card. Apart from authentication, the card can serve the function of storing various other health data. Requiring another identification means would diminish the health data card's central role in the telematics infrastructure – apart from the questions as to data security that would be raised by such a requirement.

6 Conclusion

The imprecise and in part contradictory wording of the eIAS-R-D raises various questions with an impact onto safe identity management in cloud computing by electronic identification means. They are of particular relevance for the nPA-infrastructure leading to justified criticism of the draft. The German health data card scheme is also imperilled by the regulation.

As it appears that the decision on passing the regulation has already been made, it is imperative to develop solutions that are reconcilable with the intentions and aims of the regulation. According to the current wording, only the approach of an intermediate entity for the management of identities appears to be a viable solution. As a central gateway approach is rendered questionable because of data protection concerns, the implementation of an eID-broker mediating between various eID-services at least theoretically appears to be the better option. Although that concept appears reconcilable with the content and rationale of the regulation, further amendment of the wording is necessary. The proposal by the European Parliament Commission on Industry, Research and Energy aiming at the elimination of the requirement to provide said services free of charge and at the modification of the technical requirements provides a first and valid starting point. Moreover, further questions must be addressed in the context of designing technology in conformity with the law. Further, there remain imperfections as to the security and protection of data, which could generally be addressed by a concept of Member State liability. It remains to be seen whether the critical voices will be heard during the forthcoming deliberations.

References

[Be13] Bender, J.: at, Sichere Identifizierung und Vertrauensdienste in Europa. Recht und Technik für sichere elektronische Transaktionen, Stuttgart, 02/03.05.2013.

[Bo10] Borges, G.: Der neue Personalausweise und der elektronische Identitätsnachweis, NJW 2010, p. 3334-3339.

[Bo13] Borges, G.: at, Sichere Identifizierung und Vertrauensdienste in Europa. Recht und Technik für sichere elektronische Transaktionen, Stuttgart, 02./03.04.2013.

[BSI12] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie eID-Server, V.1.6, BSI TR-03130, Bonn 20.04.2012.

[BT08] Deutscher Bundestag: Drucksache 16/10489, Berlin 07.10.2008.

[BT12] Deutscher Bundestag: Drucksache 17/11473, Berlin 14.11.2012.

[EC12] European Commission: 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, COM(2012) 238 final, Brussels 04.06.2012.

[EPC13] European Parliament Committee on Industry, Research and Energy: Draft Report on the 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, Brussels 04.04.2013.

[Ho12] Hornung, G.: Brüsseler Angriff auf den neuen Personalausweis?, MMR 2012, p. 633-634.

[HH+11] Hühnlein, D.; Hornung, G.; Roßnagel, H.; Schmölz, J.; Wich, T.; Zibuschka, J.: SkIDentity – Vertrauenswürdige Identitäten für die Cloud. In: Schartner, P.; Taeger, J. (Ed.): D-A-CH Security 2011. Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven, Klagenfurt 2011, p. 296-303.

[Mö11] Möller, J.: §§ 18-21 PAuswG. In: Hornung, G.; Möller, J.: PassG PAuswG, Kommentar, München 2011.

[RHS08] Roßnagel, A.; Hornung, G.; Schnabel, C.: Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht, DuD 2008, p.168-172.

[RoJo13] Roßnagel, A.; Johannes, P. C.: Entwurf einer EU-Verordnung über elektronische Identifizierung und Vertrauensdienste. Neue Regeln für elektronische Sicherheitsdienste, ZD 2013, p. 65-72.

[Sch10] Schulz, S. E.: Grundbegriffe des Identitätsmanagements. Postfach- und Versanddienst, Identitätsbestätigungsdienst und Dokumentensafes. In: Schliesky, U. (Ed.), Technikgestütztes Identitätsmanagement. Rechtsfragen und Lösungsvorschläge dargestellt am Beispiel der De-Mail und elektronischer Dokumentensafes, Kiel 2010.

[SpRo13] Spindler, G.; Rockenbauch, M.: Die elektronische Identifizierung. Kritische Analyse des EU-Verordnungsentwurfs über elektronische Identifizierung und Vertrauensdienste, MMR 2013, p. 139-148.