Doubtless Identification and Privacy Pre-serving of User in Cloud Systems

Antonio González Robles[1] · Norbert Pohlmann[1] ·
Christoph Engling[2] · Hubert Jäger[3] · Edmund Ernst[3]

[1]Institute for Internet Security
Westfälische Hochschule, Gelsenkirchen
{gonzalezrobles | pohlmann}@internet-sicherheit.de

[2]Institut für Rechtsinformatik, Universität des Saarlandes
christoph.engling@uni-saarland.de

[3]Uniscon GmbH
{hubert.jaeger | edmund.ernst}@uniscon.de

Abstract

Present paper addresses the common challenge of compliant verification of electronic identities (eID) with legal certainty. The latter is of particular importance for banks, financial institutions, and public authorities. To ensure confidentiality, provider-proof cloud systems are a technical solution. However, they must also ensure privacy for communication from system to system.

With this document, we shall highlight, based on said challenge, our motives and pinpoint the objective of the Verifi-eID research project and its implementation. We shall then address legal considerations, followed by commonly applied provider-proof cloud security and identification measures. Lastly, we shall illuminate a possible solution, followed by a summary.

1 Motives

When information is exchanged or business is done online, being able to identify all users unequivocally and securely is imperative [Kros14]. Certified security allows bank customers, for example, to be able to verify whether they are actually accessing the proper website when conducting financial transactions. In turn, banks verify clients' actual IDs up front via prior face-to-face identification by demanding their user IDs and passwords, followed by re-mote access user confirmation for transaction. In doing so, banks inevitably recognize the mandatory user information and transaction content. Yet today's customary cloud computing authentication methods have multiple serious drawbacks: Large-scale cloud providers can all access a user's confidential data, not to mention metadata. The latter even includes file names and types. Providers are also able to distinguish who accesses which files. Normally, providers cannot exclude that internal staff, e.g. a system administrator, accesses data without authorization. Storing or processing confidential or personally identifiable third-party data, in particular, does not comply with strict German data privacy legislation.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2015), 1-11

In contrast, provider-proof cloud services pose an advantage. These exclude any possible staff access via technical means. In other words, provider employees have no way of access-ing entrusted data or metadata at any time whatsoever. The downside, however, is that these providers cannot know the accessing person's actual identity and, consequently, une-quivocally verify digital IDs beyond doubt. Yet this is indispensable, for example, for financial transactions.

The objective of the Verifi-eID project, which is supported by the German Federal Ministry of Education and Research and conducted by the Westfälische Hochschule Gelsenkirchen, the University of Saarland and the IT security and provider-proof cloud experts Uniscon, is to find a way in which users can remotely authenticate their ID with the requested due privacy and manage assigned documents (files, images, etc.) safely in compliance with applicable law alike.o have consistency throughout the papers in the book please use for the Title and Headlines uppercase first letters in important Words and lowercase letters for fill words.

2 Verifi-eID Project Mission

Named project partners' mission is to provide a solution enabling provider-proof service us-ers to be able to trust digital IDs. The focus of research is a method in which parties can une-quivocally verify each other's identity securely and without having to reveal their identity to the cloud provider, so that their privacy is ensured.

Instead of the cloud provider, identity verification is performed by a reliable third party (Trusted Third Party). What's more, the Verifi-eID system must also be able to verify online IDs of legal entities and digital objects, such as files or images. In addition, the target solution must provide compliant legal certainty upon ID verification. The procedures and methods in development are integrated into a demonstrator, in order to test how the technically and legally secure solution can be used by the applicant.

3 Legal Considerations

Compliant and legally certain implementation per demonstrator must consider several legal aspects. These concern – besides German privacy law – also European identification direc-tives and, finally, law of evidence regulations.

Let us begin with the legal basics of identification. The German Act on Identity Cards and Electronic Identification (Personalausweisgesetz, PAuswG) provides a foundation for the dig-ital identification of persons. However, it is arguable whether the Trusted Third Parties (TTP) concept may be implemented pursuant to this act. Under Section 21 (2) No. 2 PAuswG, au-thorized access to nPA (new German ID card) data is not granted, if the purpose consists of "commercial transmission of the data" [Möll11, marginal number 15]. The German identity card and electronic identification law provides no direct solution to identification of digital objects. Yet, since ID cards are designed as "secure signature creation devices", files can be signed modification-proof. On the other hand, the purpose of said signature is to identify its creator, and this allows the cloud provider to draw conclusions.

The EU Regulation (EU) No. 910/2014 (i.e., eIDAS-VO), in force since 9/17/2014, introduces a new method of identification. Its actual directives come into effect as of 7/1/2016. The Regulation

is directly enforceable, applicable and legally binding in the respective EU mem-ber countries [Roßn15, p. 359].

The so-called electronic seals mentioned in Section 3 nos. 25-27 of Regulation (EU) No. 910/2014 are new. Named seals are pseudonymous (alias) "signatures" that may be used by legal entities only [Roßn13, p. 70; Quir13, p. 22]. They do not concurrently describe who the corporate body is but rather only ensure the data's authenticity [Sosn15, p. 831]. To date, this was not possible under German law. The Regulation provides that electronic seals are categorized according to degree of trustworthiness: simple, advanced, and qualified electronic seal. As with signatures, said seals can be verified by Trusted Third-Party (TTP) services (Section 3 No. 16 Regulation (EU) No. 910/2014). Trusted services (which the Regu-lation refers to as "Trusted Service Providers") evidently implement the TTP concept in per-son, since the Regulation does not stipulate any restrictions, as is the case with the German Act on Identity Cards and Electronic Identification (Personalausweisgesetz, PAuswG). To pro-vide compliant legal certainty, identification (authentication) must even withstand court-ordered inspection [Borg11, p. 243]. Prima facie evidence is a possibility. The latter (rebut-table presumption) specifies that, to prove a position, one may infer from previous experi-ence. A good example is rear-end collision: The mere fact that a vehicle collision accident occurred from the rear indicates that the back driver either didn't keep a safe distance or was distracted. No such wealth of experience with identification exists to date. However, owing to how the new ID card is devised, regular presumption, that authentication is merely possible upon possession of an ID and knowledge of the PIN, is justifiable [Borg11, p. 234; Borg10, p. 3338]. For this reason, authentication is only performable by the owner of the card or a third party given the respective PIN [Borg11, p. 234; Borg10, p. 3338].

Yet this is only applies to a limited extent for activity carried out after identification and, hence, situations in which the ID is used to prove that the identified user is the actual author of the respective activity [Borg11, p. 247 ff.]. Consequently, the integrity (i.e. authenticity in terms of authorship / lack of modification) of digital objects cannot be verified reliably per prima facie evidence if the files are not signed. For the time being and pursuant to Regula-tion (EU) No. 910/2014, the aforementioned principles of prima facie evidence are transfer-able to signatures and seals. However, since the Regulation also dictates that the EU mem-ber states must, in turn, recognize the IDs of other EU countries, it remains questionable whether prima facie evidence of definitely national design is sustainable. Moreover, pursu-ant to Section 25 and 35, qualified electronic signatures and seals are subject to special evi-dence provisions. According to Section 2, a qualified electronic seal shall enjoy "the pre-sumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked". Thus, Regulation (EU) No. 910/2014 provides an im-portant and applicable legal basis for legally certain identification of individual persons, legal entities, and data.

4 Cloud Service Provider Security Measures

If personal data is stored or processed in a cloud, a German customer must be able to reas-sure himself locally in advance (i.e. in the data center), and on a regular basis thereafter, that compliance is observed pursuant to Germany's Federal Data Privacy Act (Federal Ministry of Justice and Consumer Protection 2003). After all, it is risky for a user to outsource data to online services and data centers, where it is stored and may be accessed by third-party beneficiaries. Cloud applications that process data, e.g. within the framework of software as a service (SaaS), and are used by

parties obliged to legal confidentiality, in particular, provide information during processing. After all, a cloud provider can access a database through the application server.

4.1 Common Security Technologies

Security aware cloud application providers apply both technical and organizational measures, to safeguard against internal and external attacks via web application. Organiza-tional measures, such as the two-man rule or role based access control, are often applied for data that is unencrypted during processing (e.g. the German DE-Mail).

End-to-end content encryption is also often applied as a technical measure, to complicate access pursuant to § 203 of the German Penal Code StGB (e.g. Wuala).

Named protection measures prevent access to content. They do not prevent access to metadata.

Hitherto existing Unicast systems must disclose the recipient's e-mail address to the provid-er, for the provider to be able to forward data correctly. Hence, communication service pro-viders are able to access connection data. Yet connection data is defined as personal and personally identifiable data. In other words, it, too, is subject to data privacy.

4.2 Advanced Technologies

To date, there are four state-of-the-art privacy protecting technologies:

- Accurate adherence to organizational protection measures, to protect metadata
  (Example: IT baseline protection catalogues based on this method)
- The Multicast approach
  (Example: The FreenetFreenet project[1])
  This approach is currently rather suited for narrow band applications, since it requires high processing power and high access availability from its network users.
- Application of mix networks
  (Example: The security software TOR[2]TOR)
  Owing to long transmission delays, this approach is currently also rather suited for narrow band applications.
- Sealed Cloud technology, which is based on three essential requirements: Performance, necessary security, and convenience.
  (Example: The web service IDGARD[3])

We shall take a closer look at the latter approach in the following. What makes Sealed Cloud technology so unique, is that a set of purely technical measures prevents access to content and metadata. Mere organizational measures along the first line of defense no longer sufficiently protect against external cybercrime or internal attacks. Hence, IT security experts recommend excluding the human risk factor. The following sub-chapter commits itself to cloud provider "proofness".

1 e. g. http://www.freenet.de, abgerufen am 21.07.2015 15.00.
2 e. g. https://www.torproject.org, abgerufen am 21. 07.2015 15.06.
3 e. g. https://www.idgard.de, abgerufen am 21.07.2015 15.07.

4.2.1 4.2.1 Cloud Provider-proofness per Sealed Cloud

The technical measures, developed to meet the aforementioned four basic requirements (performance, necessary security, convenience), consist of the following:

- **Security Measures during Data Connection to the Data Center**
  In order to avoid having to install special software, user device to Sealed Cloud connection occurs via classic SSL encryption. Only strong ciphers (encryption algorithms, e. g. AES 256), i.e. with long keys and no known implementation weakness, are accepted in the process. Since no private key should be accessible on the server side, it is calculated on demand. A browser add-on and apps for mobile devices protect against man-in-the-middle attacks and alert the user of fake digital certificates. With a one-time password generator or a numerical code sent via text message, user data is protected per 2-factor authentication.
- **Security Measures against Data Access during Processing**
  Components that process unencrypted data are located in the so-called data clean-up area. Mechanical cages are equipped with electromechanical locks for the purpose. Further, all electronic interfaces are limited to granting only the user access; direct administrator access is not possible. None of the underlying components dispose of persistent memory. The electronic interfaces and electromechanical components of the cages dispose of numerous sensors that instantly trigger an alarm upon attempted access. This alarm instantly triggers data clean-up. In other words, user sessions on the respective servers are automatically routed to unconcerned segments, and all data in the affected segments is deleted. To ensure deletion, power to the servers is disconnected for 15 seconds. Accordingly, a respective procedure occurs before technical maintenance.
- **Security Measures during Storage**
  The principle of sealing also includes special key distribution. According to the scientific project report [Jaeg13], the provider disposes of no decryption key, neither for database protocol decryption, nor for decipherment of data in the file systems.
  The keys for the protocols in the database are derived from user name and password hashtags. The instant the hash values are determined, user name and password are dismissed. At the end of a session, the determined hash value is also deleted. An exclusively volatile meta-mapping server operates within the data clean-up area, so that no application usage information can be deducted from the foreign keys in the database. The application is able to map data structures within the server yet without the infrastructure provider or the application provider being able to access them. Any access attempt automatically triggers the mentioned data clean-up. However, since the server disposes of volatile memory only, high availability postulates, first of all, redundant configuration in a cluster and, secondly, in the event that the entire infrastructure should fail, gradual data restoration per active user sessions.
- **Further Metadata Protection Measures**
  Communication regarding traffic is intensity dependently "randomly delayed", so that no metadata conclusions may be drawn from the traffic. In addition, communicated file siz-

es are increased to the next higher standard size, so that metadata cannot be computed through time or size correlation, either.

5 Identification in a Cloud Scenario

Today's cloud systems offer services on behalf of a company, so their employees or custom-ers can use the externally hosted service. They also offer cloud services to customers (single users or huge user groups, such as those of companies) directly. Using and offering cloud services entails several implications. The first requires that the cloud provider identify and unequivocally authenticate the user during registration and, in the latter case, usage of the service. The second implication demands user privacy is not breached in a cloud context (i.e. remaining operator-proof). Identification of cloud users opposite cloud service providers is mandatory.

Rapid development of cloud system technologies entails multiple features: cloud service us-ers can, among others, invite new users that are not yet registered to the pertinent service in question. This requires that registered users must also be able to securely identify the us-ers they invite to the (hired) cloud service.

This allows us to arrive to the following crucial conclusions: It is imperative, first of all, that the user is identified securely opposite the cloud service provider and, secondly, towards a further still registered cloud service user. Last but not least, the cloud system operator should not be able to compromise both users' privacy.

The following sub-chapters are committed to the applied identification methods of cloud service users opposite cloud service providers, on the one hand, and other cloud service us-ers (still registered users and new ones), on the other hand. This is followed by a conclusion listing the challenges that result from the aforementioned so-called "crucial aspects".

5.1 User Identification opposite Cloud Service Providers

Current advanced technology based cloud systems offer identification and authentication methods that go beyond using only username and password. They offer modern two-factor authentication that ensures legitimate access to resources. These methods are, for example, based on SMS pass codes with one-time password generators or PIN protected smart cards.

Further far-reaching ID and authentication methods applied, e.g. in cloud (operator-proof) systems, consist in the Vodafone Secure SIM (VSS) and the German National Identity Card (neuer deutscher Personalausweis, nPA) using pertinent pseudonym (alias) eIDs. Recommendable German National Identity Card (nPA) based identification and authentication solutions are listed on the website of the German Federal Ministry of the Interior. These are, among others, the Trusted Cloud project SkIDentity and the provider OpenID.[4]

Identification and authentication per Vodafone Secure SIM (VSS) and the German National Identity Card (nPA) entail further-reaching implications insofar, as that they certify that the electronic identity used is assigned to a true existing legal entity or person. Mobile phone operators have been registering customers long since to mobile numbers, which comes along with face-to-face

4 http://www.personalausweisportal.de

identification per official state-issued ID. What's more, legal entities (persons) are also officially granted German IDs, used by the systems to rely on commensurate pseudonym (alias) eIDs.

Owing to strict German legislation (§ 19 PAuswG, the Act on Identity Cards and Electronic Identification, also known as Personalausweisgesetz) (German Federal Assembly 2009; Federal Ministry of Justice and Consumer Protection 2009), cloud system providers currently dispose of no scientifically and technologically proven method with which to remotely access a user's physical (legal) identity during initial registration. Thus, cloud providers can merely verify whether the same electronic identity (eID) is used persistently, without knowing the actual identity, disclosed by an unequivocal combination of first name, last name, birthdate, birthplace, address, etc.

5.2 User Identification opposite Other Users

Nowadays, cloud system providers offer the user (customer) the feature to be able to invite external users, i.e. users that are not yet registered with said provider, to join the hired ser-vice. As in the preceding sub-chapter, for user-to-user communication, it is also imperative that the user inviting the third party is able to unequivocally identify this latter user. Current methods commonly used for this purpose are based on identification via SMS and/or e-mail.

This kind of identification merely ensures that one existing user simultaneously applies a mobile number and e-mail and that these are allocated to the assigned account pertinent user invitation. From then on, the inviting user has the certainty that the same still regis-tered user accesses the service for collaboration at all times.

The inviting cloud service user does not receive any information relating to the true legal en-tity (person) behind the mobile phone number and e-mail account. However, in certain cas-es, the user may want certainty as to the real identity in terms of personal information, such as first name, last name, birthdate, birthplace, address, etc. In the latter event, as in 5.1, it is necessary that users be (ideally mutually) identifiable unequivocally

The consideration in present sub-chapter leads to an additional problem. It pertains to the privacy between communicating users. The user ID methods mentioned in 5.1 depend on the cloud service provider. Therefore, the privacy of the two users is not protected.

5.3 Subsequent Challenges

The goal of present subchapter is to summarize the resulting and yet to be achieved objec-tives.

Security considerations examined to date as per provider-proof cloud systems, as well as the imperative of unambiguous user identification opposite cloud providers, comprise the fol-lowing issues, which must be solved in the course of the project:

- Unequivocal identification
- of users by cloud providers
- of users by other users
- Privacy protection of multiple users opposite cloud providers

Measures to be taken to solve the above are highlighted in chapter 6, "Solution".

6 Solution

Secure cloud services allow its users to identify themselves via user name and password and, optionally, 2-factor authentication (2FA). Named second factor may consist, e.g., in a pass code, which is sent to the user via SMS or another channel. However, the second factor may also be a one-time, non-recurring password created by the one-time password generator or smart card the user possesses. The latter communicate per SAML protocol or similar standard solutions with the ID provider on the one hand and, on the other hand, with the respective cloud service.

With the Sealed Cloud based Web service IDGARD, provided by the corporate business partner Uniscon, the second factor consists either of a one-time password generator the size of a credit card (IDGARD Login Card), an SMS Pass Code, or a Vodafone Secure SIM (VSS) and its respective connection via SAML protocol. What's more, nPA connection per 2FA alias was also demonstrated at the CeBIT 2012 fair by means of the Trusted Cloud project SkIDentity. The Institute for Internet Security works with the first OpenID provider[1] disposing of nPA based authentication per alias. The public is offered this service at www.personalausweisportal.de[2].

The basic structure of the solution is depicted in Figure 1 and relies on a Trusted Third Party, to protect user privacy.

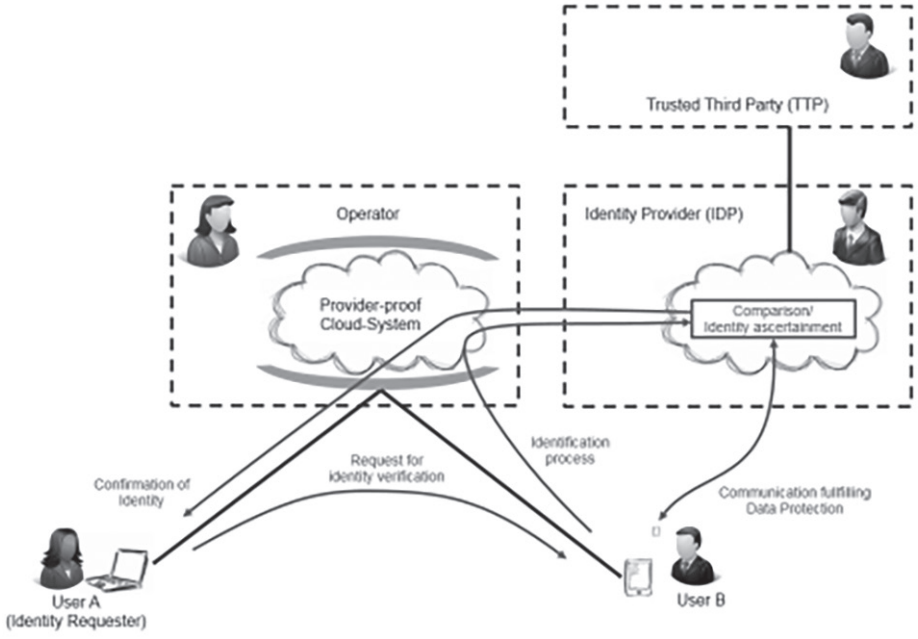

Figure 1: Verification scenario. The uniqueness of this scenario is a situation often to be expected in the future, in which the cloud service provider cannot and does not wish to identify Users A and B yet named users must be able to verify each other's identity reciprocally.

However, said authentication method merely proves that the digital ID logon is invariably performed by the very same user. It does not substantiate whether first name, last name, address, or place and date of birth provided by the user are actually identical to the data that identifies the user unequivocally.

A fundamental security measure consists in meticulously detailed rights management for compliant ID verification of digital objects. The exact technical measures can only be developed in the course of the research project. Yet two basic principles of Sealed Cloud technology are essential. They are combined with further measures, to verify an unequivocally identified user whose privacy is protected.

6.1 Privacy by Design

The principle "privacy / data protection by design" is based on the insight that building in privacy features from the very beginning of the design process is preferable to attempting to adapt a product or service at a later stage. Involving them in the design process considers the full lifecycle of said data and its usage.

- Minimize: The most basic privacy design strategy is MINIMIZE, which states that the amount of personal data that is processed should be restricted to the minimum amount possible.
- Hide: This strategy states that any personal data and respective interrelationships should be hidden from plain view.
- Separate: States that personal data should be processed in a distributed fashion, in separate compartments, whenever possible.
- Aggregate: this fourth design pattern states that personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
- Demonstrate: This strategy requires a data controller, in order to be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

6.2 Trusted Third-Party Identity Verification

Use of pretty much any Internet service on the market requires application of a digital Trust-ed Identity (TId) [GoRoPo14], since this postulates identification of the actual person. The definition of Trusted Identity requires that the accompanying legal identity (person) must match unambiguously. Customary user name / password based authentication to determine the identity of a person is generally based on information provided by the user himself. Ap-plied procedures are often based on e-mail, SMS, or sometimes even postal verification. Yet these procedures are unsatisfactory and far from meeting the offered services' security re-quirements. Subsequential user identities are often referred to as soft digital identities.

With common cloud concepts and traditional Internet services, the legal person and service provider are only close to each other in exceptional cases, so that personal face-to-face identification opposite the service provider is rarely feasible. Identification serves to verify identity describing attributes. Personal identification relies on visual verification of an official state-approved identity card issued by the respective state for a verifiable natural citizen. In Europe, commonly used national IDs provide electronic identities (eIDs) that unify associated attributes pursuant to ISO/

EC 24760 and, in this case, unequivocally represent the natural person. Said attributes consist, among others, of first name, last name, birthdate, birthplace, postal address, etc.

Electronic identification that relies on the new German ID card (neuer Personalausweis, nPA) is of special interest, because it incorporates two essential requirements that must be met, to be able to refer to an identity as digital Trusted Identity (TId). The first implies that the registration process, performed by a trustworthy entity, ensures verification of the natural person. The second is the feasibility of secure, strong user-side attribute authentication which qualifies the eID.

Named Verifi-eID project shall investigate a solution that unequivocally verifies actual user identities and relies on a digital Trusted Identity, as provided by the new German ID (nPA). The nPA applies pertinent eID, ensures cloud system provider-proofness and, what's more, expanding user-to-user privacy, in order to exclude the cloud provider. The elaborated solu-tion will be at least on a par with locally performed face-to-face identification.

7 Conclusion

The project's target solutions for legally certain, compliant ID verification in provider-proof clouds tap the full potential of cloud computing user groups that don't exploit today's ser-vices due to data privacy concerns. Verifi-eID allows users to exchange confidential business data online or even store and process particular personally identifiable data (e.g. that of medical practices or law firms) per cloud computing.

Acknowledgment

This work is part of the project "Rechtssichere Verifikation elektronischer Identitäten in be-treibersicheren Cloud-Systemen" (Verifi-eID)", which is funded by the German Federal Ministry of Education and Research (BMBF). The content of this article is solely in charge of the authors and reflects in no way the BMBF's opinion.

References

[Borg11, p.] Borges, Georg: Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, 2011 , Baden-Baden (Nomos).

[Bogr10, p.]Borges, Georg.: Der neue Personalausweis und der elektronische Identitätsnachweis, NJW 2010, 3334-3339. [FelPoh10] Security Analysis of OpenID, followed by a Reference Implementation of an nPA-based OpenID Provider. In: Norbert Pohlmann, Helmut Reimer und Wolfgang Schneider (Eds.): ISSE 2010 Securing Electronic Business Processes.

[FelPoh10] Security Analysis of OpenID, followed by a Reference Implementation of an nPA-based OpenID Provider. In: Norbert Pohlmann, Helmut Reimer und Wolfgang Schneider (Eds.): ISSE 2010 Securing Electronic Business Processes.

[GoRoPo14]González Robles, Antonio; Pohlmann, Norbert: Identity Provider zur Verifikation der vertrauenswürdigen digitalen Identität. In: Peter Schartner und Peter Lipp (Hg.): DACH Security 2014. Bestandsaufnahme – Konzepte – Anwendungen – Perspektiven. New edition. Frechen: Horster, Patrick.

[Jaeg13] Jäger, Hubert, et al.: A Novel Set of Measures against Insider Attacks – Sealed Cloud, in: Detlef Hühnlein, Heiko Roßnagel (Ed.): Proceedings of Open Identity Summit 2013, Lecture Notes in Informatics, Volume 223.

[Kros14] Kroschwald, Steffen: Verschlüsseltes Cloud Computing. In: Zeitschrift für Datenschutz (ZD) 2014, p. 75-80.

[Möll11, marg. nr] Möller, Jan: Kommentierung zu § 21 PAuswG in: Hornung, Gerit/Möller, Jan (Hrsg.): Passgesetz Personalausweisgesetz – Kommentar, 2011, München (C.H. Beck).

[Quir13, p.] Quiring-Kock, Gisela: Entwurf EU-Verordnung über elektronische Identifizierung und Vertrauensdienste – EU-weite Interoperabilität – Anspruch und Wirklichkeit, DuD 2013, 20-24.

[Roßn15, p.] Roßnagel, Alexander: Der Anwendungsvorrang der eIDAS-Verordnung – Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar?, MMR 2015, 359-364.

[Roßn13, p.] ders.: Entwurf einer EU-Verordnung über elektronische Identifizierung und Vertrauensdienste – Neue Regeln für elektronische Sicherheitsdienste, ZD 2013, 65-725.

[Sosn14, p.] Sosna, Sabine: EU-weite elektronische Identifizierung und Nutzung von Vertrauensdiensten – eIDAS-Verordnung – Ein Überblick über die wichtigsten Inhalte und deren Konsequenzen für Unternehmen, CR 2014, 825, 831.