Future of Cloud-Based Services for Multi-factor Authentication: Results of a Delphi Study

Christian Senk

University of Regensburg
Department of Management Information Systems
93053 Regensburg, Germany
christian.senk@uni-r.de

Abstract. The *Cloud Computing* model potentially leverages the diffusion of strong multi-factor authentication systems. In order to systematically evaluate the future of cloud-based services for multi-factor authentication, a 3-rounded *Delphi* survey with experts in the German-speaking area was conducted. Results indicate the substantially increasing importance of such services in both organizational and user-centric application fields. Furthermore, seven primary success factors have been identified. Most critical are factors regarding the ease of adoption as well as security- and compliance-related issues.

Keywords: Authentication, Delphi Study, Cloud Computing.

1 Introduction

While for many use cases basic password-based user authentication is considered to become too insecure, there are substantial barriers regarding the adoption of strong(er) multi-factor authentication systems. Here, on the one hand side, the *Cloud Computing* model opens up opportunities to lower related barriers and to drive the adoption; on the other hand side, inherent risks might significantly restrict the applicability of related systems. In this context, we investigate following research questions (RQ) to assess the future application of such systems:

- **RQ1:** How will the practical relevance of cloud-based services for multi-factor authentication develop and which authentication methods will prevail?
- **RQ2:** Which are relevant practical application fields for such systems?
- **RQ3:** Which requirements are critical for the diffusion of such systems (referred to as *success drivers*) and should thus be reflected by service providers?

Since for this purpose no comprehensive data is available, an expert survey is conducted applying the *Delphi* method. The remainder of this paper is structured as follows: Section 2 explains the theoretical background and related work. Section 3 lays out the research design including the applied method as well as the justification of its application. The findings are set forth and discussed in section 4. Section 5 finally summarizes this paper and directs future research.

M. Yousif, L. Schubert (Eds.): Cloudcomp 2012, LNICST 112, pp. 134–144, 2013.

2 Theoretical Background and Related Work

This section sets forth the paper's theoretical fundamentals as well as related work in the field of cloud-based authentication services.

2.1 Cloud Computing

According to the *National Institute of Standards and Technology* (NIST), *Cloud Computing* is defined as a "model for enabling convenient on-demand network access to a shared pool of configurable computing resources [...] that can be rapidly provisioned and released with minimal management effort or service provider interaction" [15]. Cloud services refer to resources at the infrastructure, platform or application layer and provide specific advantageous characteristics such as multi-tenancy, easy standardized access through thin clients, scalability of the underlying infrastructure, and automated self-service provisioning [11, 14, 15]. Hence, the most frequently mentioned obstacles are concerns regarding security and compliance, but also issues related to the ease of integration with existing systems and possible lock-in effects [11, 14].

2.2 Authentication

Users can generally be authenticated using knowledge-based, token-based or biometric methods [12]. Most systems implement basic PIN- or password-based mechanisms (knowledge) [4]. However, because of several inherent drawbacks, the strength of authentication of knowledge-based mechanisms is considered to be insufficient for many applications [5, 18]. A possible way to increase this strength is to replace or to supplement existing controls with token-based procedures (e.g. one-time password (OTP) generators) or biometric methods (e.g. face recognition, keystroke dynamics) [4, 8, 12]. The combination of different kinds of authentication methods is referred to as *multi-factor authentication* [4, 12].

2.3 Authentication as a Service

The application of security services according to the *Cloud Computing* model is referred to as *Security as a Service*, SECaaS) and, accordingly, promises additional specific benefits compared to on-premises solutions or traditional security service outsourcing [1, 9, 17]. A study conducted by the author in 2011[1] discovered that statistically, there are three drivers for the adoption of SECaaS:

- **Perceived Ease of Adoption:** Degree to which the adopter believes that the SECaaS adoption is effortless, both technically and organizationally speaking;

[1] Survey was conducted in 2011 in cooperation with the *German Federal Association for Information Technology, Telecommunications and New Media* (BITKOM e.V., see: `http://www.bitkom.de`); detailed data is not published, yet.

- **Perceived Usefulness:** Degree to which the adopter believes that the adoption increases its performance; this includes cost- and quality-related benefits;
- **Trust:** Degree to which the adopter believes that the adoption is free of risks, which includes mainly security-related but also social and strategic risks.

Below, cloud-based systems for (strong) user authentication are referred to as *Authentication as a Service* (AaaS). Such systems are operated and maintained by *Authentication Service Providers* (ASP) in order to determine a user's identity by specified means and to assert this to respective target systems. Here, it must be noted that AaaS regards user authentication *from* the cloud and not *within* existing cloud systems [e.g., 2]. The results of the aforementioned survey emphasizes the relevance of AaaS. Of 164 participating organizations, 12.8% plan to invest in cloud-based services for multi-factor authentication within the next three years. In the medium and long run further 7.9% intend to use such systems. Findings of Forrester Research support this. According to a survey among 324 IT security decision-makers conducted in 2008, 75% were planning or considering changes or upgrades to their customer authentication processes; 72% showed general interest in AaaS [7].

3 Research Design

In the first part of this section, the basic content-related concept of the study is laid out which includes a total of 50 hypotheses (H). The applied methodology is introduced and justified afterward.

3.1 Concept

RQ1: Development (H1-H4). We initially argue that the relevance of AaaS is induced by an increasing demand for strong (multi-factor) authentication and a hypothesized decreasing significance of inherently weak knowledge-based authentication methods (H2). Thus, we not only expect the increasing importance of such systems (H1) but also of strengthening biometric (H3) and token-based authentication methods (H4) required to implement AaaS systems. To investigate this development, we intend to evaluate the general relevance of AaaS as well as authentication approaches today, short-, medium- and long term.

RQ2: Application Fields (H5-H19). Since the respective type of an AaaS consumer implicates different individual requirements (e.g. regarding service level agreements (SLA), interface design), one must differentiate whether it is an organization that adopts such a service or a private person employing it autonomously. Based on related literature [e.g., 4, 12, 14], we identified possible networked application fields which were then hypothesized regarding their potential relevance for AaaS employments (see result tables 2 & 3).

RQ3: Success Factors (H20-H50). Since the success of AaaS solutions directly depends on its adoption, we systematize possible success factors according to the aforementioned adoption drivers. Furthermore, to enable deeper insights, we differentiate success factor candidates at the different levels of an AaaS solution. This includes the *system* implementation itself, one or more implemented authentication *methods*, and organizational attributes specific to a *provider* (ASP), offering at least one system. All hypothesized items are derived from related literature [e.g., 3, 6] (see result tables 4, 5 & 6).

3.2 Applying the Delphi Method

The *Delphi* method can be defined as a structured group communication process which allows individuals to deal with complex problems and has proven to be a popular instrument in IS research and technology forecast [13, 16]. Here, classical studies are characterized by the following attributes [10]: (1) Survey of selected experts; (2) use of standardized questionnaires; (3) anonymity of individual responses; (4) calculation of statistical group answers; (5) iteration of the survey; (6) provision of the group answers (controlled feedback) to the respondents.

The novelty, complexity and specificity of this paper's research object requires the involvement of declared experts in related fields (e.g. *Cloud Computing*). Compared to alternative approaches like group discussions or expert surveys, the *Delphi* method tends to reveal more reflected and thus better expert judgment [10]. Major drawback, on the other hand side, is a higher expenditure of time due to additional survey rounds conducted [10]. Essential for a high quality of a *Delphi* study's generated results is the selection of experts with an appropriately deep understanding of the research topic [10]. Related literature suggests a panel size of 10-18 individuals or more which are selected non-randomly by the *Delphi* monitoring team [10, 13, 16]. The panel should furthermore be composed interdisciplinary to cover a more faceted set of expert opinions [10].

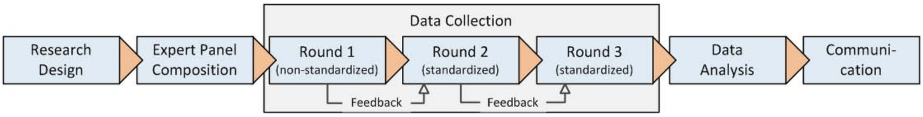

Fig. 1. Process Model of the Study

The study follows the process depicted by figure 1. In a first step, the research questions were specified, related contents systematized and a measurement model derived. Afterward, potential experts were identified and selected to join the expert panel. The expert panel was initially questioned in a non-standardized form (Round (R) 1), and then in two successive standardized survey rounds (R2 and R3) with controlled feedback. After completion, the data was analyzed and key findings were distributed to all active panel members.

4 Findings

Below, the outcome of the conducted survey is laid out.

4.1 Composition of Expert Panel

Potential experts were appealed, informed about this study and its objective, and invited to apply via e-mail reasoning why and how they could contribute to this topic[2]. Then, the panel was composed. Of 39 candidates 36 experts were selected. All experts provide at least 3 years of experience in related fields. R1 was completed by 34 and R2 by 32 persons. The last round revealed 24 responses. This corresponds to a total panel mortality rate equals 33.3%. The final panel was composed almost equally of experts of the fields *consumer* (34.5%), *provider or developer* (34.5%), and *research* (31.0%)[3]. Details about the panel composition and its development are depicted by figure 2.

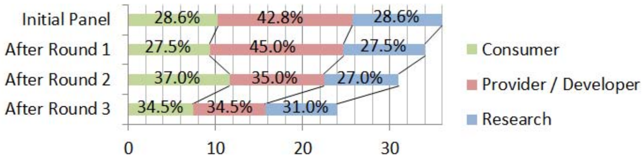

Fig. 2. Composition of the Expert Panel

4.2 Data Collection

The data collection was carried out from January to April 2012. The first round revealed 34 responses to two open questions regarding the most important (1) *application fields* and (2) *success factors* as perceived by the experts. The unstructured answers were mapped to the existing measurement model. This first (non-standardized) round was conducted via e-mail or telephone interview and was used both to double-check the completeness of the designed model and to determine the intuitively most named items. Afterward, the measurement model was translated into a standardized online questionnaire for R2 and pre-tested by 10 IT security master students and the research team of the partner project *SkIDentity*[4]. To provide for feedback in the 2nd (and 1st standardized) survey round the previously most named items were highlighted accordingly. R2 and R3 were conducted consecutively online including both open and closed questions. The survey of R3 contained the visualized statistical group answers of R2. Furthermore, after R2, we removed non-significant items.

[2] For this, IT professionals of the network of BITKOM e.V. were contacted. Additionally, declared experts were directly addressed via XING, see `http://www.xing.de`.

[3] Multiple answers were permitted.

[4] See, `http://www.skidentity.com/`

4.3 Results

Subject of this sub-section is the description and analysis of the gathered data.

RQ1: Development. The development of the significance of AaaS and (independently) general authentication approaches is illustrated by figure 3. Though the relevance of AaaS is evaluated to be rather low within the next three years, in the medium to long run the panel forecasts a significant increase and a respective high importance (Median=4)[5]. A congruent development is expected for token-based authentication methods, indicating the dependence of AaaS on such methods. This is supported by the evaluation of implementable authentication procedures. The panel was asked to rank the five most relevant methods regarding the implementation of AaaS in the medium and long term. Here, token-based methods performed clearly better than all other biometric or knowledge-based procedures, both for private and business user-centric applications. Table 1 summarizes the results ordered by average rank (business). The data also suggests a significant decrease of the relevance of knowledge-based methods from currently *very high* to *medium*. The importance of biometrics correlates negatively and increases from *very low* to *medium* and even subtends the curve for knowledge-based procedures. H1–H4 are supported.

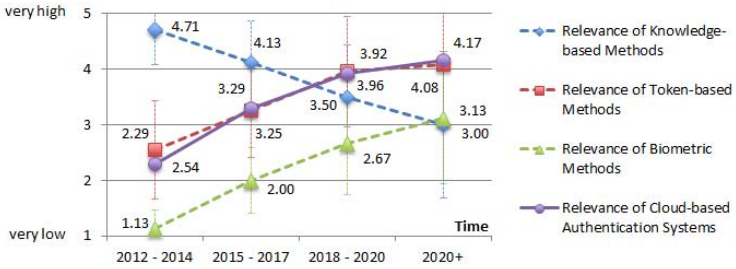

Fig. 3. Development of the Relevance of Authentication Methods and AaaS (n=24)

RQ2: Application Fields. Possible application fields were rated by the panel on a 5-point *Likert* scale with following semantics: [1] *absolutely not relevant*, [2] *rather not relevant*, [3] *neutral*, [4] *rather relevant*, [5] *absolutely relevant*. Regarding organizational application fields, the data indicates the significant relevance of AaaS for the authentication of partners or corporate customers in a federation, the enhancement of *Identity & Access Management* (IAM) systems, the protection of outsourced or cloud applications, and the authentication of private end users in the public sector. An item was rated to be relevant for a median greater than or equal to 4. Statistical details are summarized in table 2. Of 24 experts, 58% name legal or regulative requirements as primary reason for the adoption of AaaS. Business partner demands are secondary (25%). The evaluation of the extent of pain implicated by these drivers was approached looking

[5] For all tests regarding median values, in this and the following section, the (non-parametric) *One-Sample Wilcoxon Signed Rank Test* was applied with $\alpha = 5\%$.

Table 1. Ranking of Authentication Methods regarding AaaS Application

Authentication Method	Type	∅ Rank Business	∅ Rank Private
Hardware-based security token with dedicated reading device	Token	2.52	4.78
Hardware-based security token for OTP	Token	3.30	5.50
Password-protected private keys and certificates	Token	4.28	6.65
Software token (e.g. OTP via smartphone appl.)	Token	5.09	2.72
Text-based password or PIN	Knowledge	8.74	7.04
Fingerprint recognition	Biometrics	9.96	9.72
Keystroke dynamics (text-dependent)	Biometrics	10.07	10.72
Face recognition	Biometrics	10.43	10.02
Voice recognition (text-independent)	Biometrics	10.57	10.11
Keystroke dynamics (text-independent)	Biometrics	10.63	9.70
Hand vein structure recognition	Biometrics	10.65	16.00
Dynamic signature recognition	Biometrics	10.76	10.35
Social knowlegde-based procedures	Knowledge	10.89	10.20
Graphical passwords	Knowledge	10.63	9.50

at the relative value of strong authentication. In this regard, the panel was asked to estimate the average value of strong user authentication proportionally to the value of the respective transaction or business application to be protected. The result was 14.54%. Furthermore, the data indicates that AaaS is most relevant for web-enabled applications involving high protection needs. Regarding even higher security needs (*critical*), applications AaaS is not feasible due to inherent cloud challenges.

The user-centric adoption of AaaS shows promise for the protection of (semi-) critical processes both for private and public applications. Table 3 lists all rated items and the corresponding test results.

Table 2. Organizational Application Fields

Application	Mean	SD	Median	Min	Max	H
Authentication of partners or corporate customers	4.08	0.78	4	3	5	H10+
Authentication of private end users in the public sector	4.08	0.97	4	1	5	H12+
Protection of outsourced (cloud-) applications	4.00	0.83	4	2	5	H9+
Functional extension of IAM systems	3.75	0.74	4	2	5	H6+
Protection of network access points	3.75	0.99	4	1	5	H8-
Composition to more significant business service	3.67	1.05	4	1	5	H13-
Protection of infrastructure resources	3.58	1.25	4	1	5	H5-
Authentication of private customers for commercial use cases	3.58	0.93	4	1	5	H11-
Dedicated protection of internal applications	3.08	0.83	4	1	4	H7-

Table 3. User-centric Application Fields

Application	Mean	SD	Median	Min	Max	H
(Semi-) critical public applications (e.g. e-Government)	4.21	1.02	4	1	5	H15+
(Semi-) critical private applications (e.g. e-Banking)	4.13	1.03	4	2	5	H16+
Private cloud storages and synchronisation services	3.63	1.06	4	1	5	H18-
Innovative / future applications (e.g. e-car infrastructures)	3.46	1.06	3	2	5	H19-
Global user-centric web single sign-on	3.13	1.15	3	1	5	H14-
Less critical processes or applications (e.g. social networks)	2.68	1.14	3	1	4	H17-

RQ3: Success Factors. For the determination of the success factors, the panel had to rate each hypothesized item on a 5-point *Likert* scale with following semantics: [1] *absolutely not critical*, [2] *rather not critical*, [3] *neutral*, [4] *rather critical*, [5] *absolutely critical.* An item is considered to be a *weak* success factor [+] when its median is significantly equal to or greater than 4.0, a *moderate* success factor [++] when it is (additionally) equal to or greater than 4.5, or a *strong* success factor [+++] for a median equals 5.0. The remaining items were evaluated to be no success factor at all [o] causing the falsification of the corresponding hypotheses. The factors already eliminated after R2 are also enlisted (labelled [*]). The analysis of all success factor candidates is summarized by table 4 (*method*-related), table 5 (*system*-related) and table 6 (*provider*-related)

Table 4. Evaluation of Factors at the Method Level

Factor	Mean	SD	Median	Min	Max	Relevance	H
Ease of use and user acceptance	4.88	0.34	5	4	5	+++	H22+
Transparency & data protection performance	4.29	0.81	4,5	3	5	++	H23+
Independence from dedicated hardware or software	4.00	0.78	4	2	5	+	H20+
Security and strength of the authentication	3.96	0.75	4	2	5	+	H24+
Time-efficient usability	3.92	0.65	4	2	5	+	H21+
Reachability of confidentiality	3.42	1.06	3,5	2	5	o	H27-
Reachability of non-repudiation	3.33	1.01	3	2	5	o	H26-
Scalability of the strength of authentication	3.17	0.76	3	2	5	o	H25-

Table 5. Evaluation of Factors at the System Level

Factor	Mean	SD	Median	Min	Max	Relevance	H
Transparency and usability of the system	4.50	0.51	4,5	4	5	++	H31+
Data security from the consumers' point of view	4.42	0.72	5	3	5	++	H32+
Service access and use by any device	4.29	0.81	4,5	3	5	++	H37+
Ease of technical service integration	4.29	0.62	4	3	5	++	H29+
Comprehensibly secure system interfaces	4.00	0.78	4	2	5	+	H34+
High availability and immediate service recovery	3.96	0.69	4	3	5	+	H33+
Low total costs for service use	3.92	0.72	4	3	5	+	H28+
Reachability of a high strength of authentication	3.83	0.64	4	2	5	+	H36+
Ability to scale and to customize function range	3.50	0.83	3	2	5	o	H38-
Existing integration with relevant target systems	3.42	1.06	3,5	2	5	o	H30-
Management and provisioning of user attributes	3.25	0.94	3	2	5	o	H39-
Ability to (ex-)port user application data*	3.10	0.98	3	2	5	o	H35-
Usability in private and business environments*	2.87	1.18	3	1	5	o	H40-

Table 6. Evaluation of Factors at the Provider Level

Factor	Mean	SD	Median	Min	Max	Relevance	H
Market visibility and reputation of the ASP	4.42	0.65	4,5	3	5	++	H45+
(External) Auditability	3.92	0.78	4	3	5	+	H47+
Flexible and customer-oriented licensing models	3.88	0.85	4	2	5	+	H41+
Transparent spec. of legal consequences & effects	3.83	0.70	4	3	5	+	H44+
Location of the ASP and its infrastructure	3.79	1.06	4	1	5	o	H50-
Comprehensive certification	3.71	0.95	4	2	5	o	H46-
Differentiated & standardized SLA	3.67	0.64	4	3	5	o	H42-
Customer support	3.58	0.72	4	2	5	o	H48-
Ability to customize SLA*	3.10	0.72	4	1	5	o	H43-
Synergy effects with other services*	2.70	0.72	4	1	5	o	H49-

including descriptive statistics as well as the evaluation of the relevance of each item and of the corresponding hypothesis[6]. The most substantial and only *strong* success factor is *User acceptance and Ease of Use* of an implemented authentication method. Furthermore, six *moderate* success factors have been identified, four at the system level and each one at the method and provider level.

4.4 Discussion and Implications

According to the experts' judgement, AaaS is a significant future technology for both private users and organizations in order to increasingly replace or supplement existing password-based authentication with stronger methods. Primary authentication methods will be token-based; biometric ones are evaluated to be rather supplementary even in the medium to long run. Considering the determined success factors, possible reasons might, for instance, include an expected lower end user acceptance or data protection-related concerns [e.g., 4, 12]. However, actual reasons must be investigated in more detail and in regard to specific use cases.

Private user-centric applications include public fields such as e-Government and rather critical private web-based services such as e-Banking. Here, mainly soft tokens and device-dependent hard-tokens will be used for the implementation of AaaS. Expert feedback furthermore indicates that services for public applications will mainly be based on electronic identity cards (eID) while private scenarios will utilize more ubiquitous soft-token-based methods. For organizational and business user-centric applications, hardware tokens based on dedicated reading devices promise highest security [4] and are despite of involved costs clearly most important for the implementation of AaaS systems.

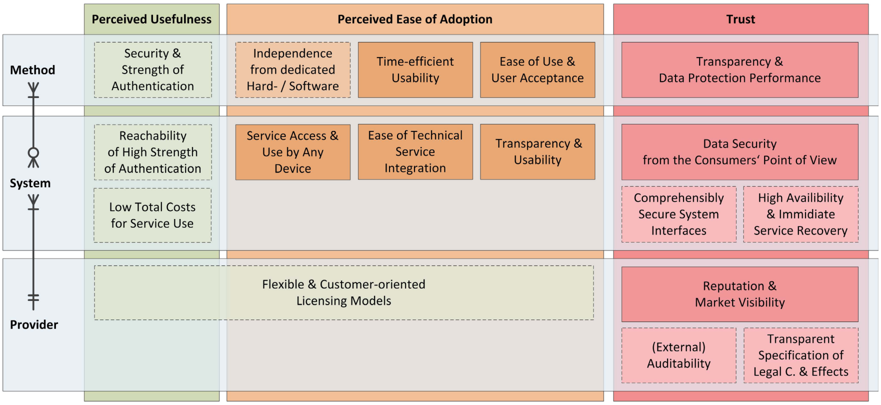
Perceived Usefulness
Perceived Ease of Adoption
Trust
Method
Security & Strength of Authentication
Independence from dedicated Hard- / Software
Time-efficient Usability
Ease of Use & User Acceptance
Transparency & Data Protection Performance
System
Reachability of High Strength of Authentication
Service Access & Use by Any Device
Ease of Technical Service Integration
Transparency & Usability
Data Security from the Consumers' Point of View
Low Total Costs for Service Use
Comprehensibly Secure System Interfaces
High Availibility & Immidiate Service Recovery
Provider
Flexible & Customer-oriented Licensing Models
Reputation & Market Visibility
(External) Auditability
Transparent Specification of Legal C. & Effects

Fig. 4. Systematization of determined Success Factors

[6] [+] support, [-] falsification of a hypothesis.

Figure 4 systematizes the determined success factors. While boxes for *strong* and *moderate* success factors feature solid lines, weak items are labelled with a broken line. The figure points out that, according to expert judgement, factors regarding the ease of adoption and the reduction of involved risks are more important than items related to the perceived usefulness of AaaS. These should be regarded by service providers in order to provide attractive authentication products to the market. Here, particularly the importance of security-related factors is supported by related literature and current research [e.g., 11, 14].

All in all, due to the size, quality and composition of the expert panel, we assume reliable results of this *Delphi* study for the German-speaking area.

5 Conclusion

This paper systematically investigates the development, relevant application fields and success drivers of cloud-based services for multi-factor authentication. For this purpose, a 3-rounded *Delphi* survey was conducted with 24 experts of the German-speaking area. The results indicate the significantly increasing importance of such services for both organizational and user-centric applications. Certain application fields were identified to be less or not relevant from a practical point of view. Moreover, seven success factors regarding applied authentication methods, the cloud service design and provider attributes have been identified. Authentication service providers might use these results to effectively direct development, certification or marketing programs. Future research should focus on security controls of such services and on system and interface design.

References

[1] Allen, J., Gabbard, D., May, C.: Outsourcing Managed Security Services. Security improvement module. Carnegie Mellon University, Software Engineering Institute (2003)

[2] amazon web services: AWS Multi-Factor Authentication (2012), `http://aws.amazon.com/de/mfa/`

[3] Braz, C., Robert, J.M.: Security and usability: the case of the user authentication methods. In: Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine, IHM 2006, pp. 199–203. ACM, New York (2006)

[4] Clarke, N.L.: Transparent User Authentication - Biometrics, RFID and Behavioural Profiling. Springer (2011)

[5] Cowan, N., Morey, C.C., Chen, Z., Gilchrist, A.L., Saults, J.S.: Theory and measurement of working memory capacity limits, pp. 49–104. AP (2008)

[6] Cranor, L., Garfinkel, S.: Security and Usability. O'Reilly Media, Inc. (2005)

[7] Forrester Research: Authentication-As–A-Service: A commissioned study conducted by Forrester Consulting on behalf of VeriSign (2009), `http://www.verisign.co.uk/static/auth-as-a-service.pdf`

[8] Gomi, H.: An authentication trust metric for federated identity management systems. In: Cuellar, J., Lopez, J., Barthe, G., Pretschner, A. (eds.) STM 2010. LNCS, vol. 6710, pp. 116–131. Springer, Heidelberg (2011)

[9] Gupta, A., Zhdanov, D.: Growth and sustainability of managed security services networks: an economic perspective. Economics of Information Security, 1–35 (2007)

[10] Häder, M.: Delphi-Befragungen: Ein Arbeitsbuch. VS Verlag für SW (2009)

[11] Höfer, C., Karagiannis, G.: Cloud computing services: taxonomy and comparison. Journal of Internet Services and Applications, 1–14 (2011)

[12] Jain, A., Flynn, P., Ross, A. (eds.): Handbook of Biometrics. Springer, New York (2007)

[13] Linstone, H., Turoff, L., Turoff, M.: The Delphi Method: Techniques and Applications (2002)

[14] Mather, T., Kumaraswamy, S., Latif, S.: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc. (2009)

[15] Mell, P., Grance, T.: The NIST Definition of Cloud Computing. National Institute of Standards and Technology 53(6), 50 (2009), http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[16] Okoli, C., Pawlowski, S.D.: The Delphi method as a research tool: an example, design considerations and applications. Information & Management 42(1), 15–29 (2004)

[17] Senk, C., Holzapfel, A.: Market overview of security as a service systems. In: Pohlmann, N., Reimer, H., Schneider, W. (eds.) ISSE 2011 Securing Electronic Business Processes (2011)

[18] Smith, R.E.: Authentication: From passwords to public keys. Addison-Wesley, Boston (2002)