

Blog Post

N° 4/2018

Key Success Factors for e-Identity Systems

*Recommendations for an accepted, competitive and
enduring e-identity solution*

Dr. Andreas Windisch

ASQUARED

asquared Blog Post N° 4/2018

March 2018

Copyright © asquared GmbH

Digital identities are on everyone's lips and currently there are a large number of different approaches across Europe. Based on Kim Cameron's Laws of Identity, we present nine success factors for e-identity systems. This will be the key to establishing an accepted, competitive and enduring solution: In addition to the acceptance on the service provider and customer sides, it is about the development of innovative business areas to create added value.

Introduction

US-american providers have been established as identity providers for years (e.g. Facebook, Google, LinkedIn). The accounts can already be used to log in comfortably on various pages, without having to register again. So far, however, they are focusing on "elementary identities". Asian companies such as Tencent have achieved considerable reach in their home markets, especially with WeChat, and are in the process of expanding their accounts to recognized electronic identities and rolling out functionality globally; Germany was chosen as the first particularly interesting internationalization target.

In response, and not least because of the changing regulatory requirements for data protection - essentially the European Data Protection Regulation and the new e-Privacy Directive - digital identities and possible e-identity systems (infrastructures, platforms, schemes etc.) are on everyone's lips. In Europe, e-identity systems are springing up: from government solutions as a digitization drive for existing identity means to smaller start-ups, solutions based on innovative technology or solutions from individual industries to cross-industry cooperation approaches. In some European countries, this process has been taking place in a very differentiated manner for many years, but in Germany it is still coming to terms. Our blog post "E-Identity Solutions in Europe" gives a summarising Europe-wide overview.

It remains exciting which of the systems can prevail with a view to market acceptance. To assess this question, Kim Cameron's Laws of Identity can be consulted. Back in 2005, Kim Cameron compiled a list of digital identity laws that explain the success or failure of digital identity systems. We applied these rules to the current circumstances in 2018, assessing whether they continue to be valid and, based on this, derive a list of key success factors for modern e-identity systems, which must be taken into account by e-identity system providers.

The Laws of Identity by Kim Cameron

Kim Cameron is an Identity Architect at Microsoft and has played a leading role in developing a variety of identity-relevant Microsoft products. Many years ago, he addressed the challenge that the Internet has been developed without any explicit way of knowing who interacts with whom, which is why digital service providers have always used a variety of workarounds.

„[...] Today's Internet, absent a native identity layer, is based on a patchwork of identity one-offs.“

Kim Cameron, Microsoft Corporation, 2005

In *The Laws of Identity*, in 2005, he highlighted the relevance of a broad identity layer, while outlining the challenges of establishing such a layer. Back then, Cameron was sure that "a single simplistic digital identity solution as a universal panacea was not realistic."

Instead, a unifying identity metasytem is needed to address digital identities, which defines common standards and loosely couples different identity solutions from different application contexts.

To define such an identity layer, Cameron has compiled 7 Laws for digital identities and recommends that they be strictly followed in order to create an identity metasytem that is widely and universally accepted.

Key success factors for e-identity systems

Based on our experience in the field of digital identities and our assessments of the current market conditions, we have analysed the applicability and relevance of Cameron's Laws of Identity and derived a total of nine key success factors for e-identity systems on this basis.

Compared to Cameron's recommendations, we have slightly expanded one point (Success Factor 6) and separately highlighted two points that are critical for success from our perspective (success factors 8 and 9). The remaining points, as we see it, remain valid. The following figure summarizes those key success factors in a condensed form, the following paragraphs explain these a little more detailed and evaluate them against the background of the status quo of the given market situation.

Key Success Factors for E-Identity-Systems



Based on Kim Cameron's Laws of Identity
Source: asquared / as of March 2018
ASQUARED

Figure 1: Nine key success factors for e-identity systems / as of March 2018

Success Factor 1 – User control and consent

The success of an e-identity system largely depends on the user's trust. Trust is created here by the overarching commitment of the identity system to place the user as the ultimate controlling decision-maker in divulging his information. The users expect to decide self-determined which information about them is revealed to whom and why. Those approvals are familiar from the app stores of for example Apple and Google, where you confirm for each app to be downloaded, which data and functionalities shall be released. In addition, it makes sense to provide the user with an "approval manager", that lists the approvals issued in the past and allows to recall them for future inquiries.

The new General Data Protection Regulation and the e-Privacy Directive alone require these principles, although not in full swing. The e-identity systems hence need to provide additional functionalities, that go beyond the mere case-related approval of information disclosure, in order to give the user control over his data and thus to increase the confidence in the e-identity system and - more importantly - to preserve it.

This necessity is now internalized by (almost) all established players. Google and Facebook, for example, have been trying for many months to bring the topic of data protection and privacy as well as the self-determination of users regarding their data in the foreground. Both have launched different transparency offensives in 2017 and 2018, in order to educate the users about it, now offer various configuration options and want to expand them further. In China, they seem not to be that progressive: there are already the first pilots to use the messaging service WeChat as electronic identity means; Privacy and privacy are unclear. Interesting especially when the service comes to Germany.

Success Factor 2 – Minimum disclosure, constrained use

When dealing with personal or identifying information, the "need to know" and "need to retain" principles must always be applied. Their compliance is already required in the BSI IT Baseline Protection Catalogue and is mandatory at the latest by the General Data Protection Regulation.

For e-identity systems, however, these principles have a particularly high status, as they also apply to the disclosure of data to service providers and must be complied with. Cameron referenced the example of age verification, in which only an affirmation of belonging to an age group should be transmitted, instead of the concrete date of birth or the avoidance of concrete one-to-one identifiers that can be used across all contexts.

„Aggregation of identifying information also aggregates risks. To minimize risk, minimize aggregation.“

Kim Cameron, Microsoft Corporation, 2005

In principle, the data may only be provided for specific applications and for a specific purpose. Depending on the application, only the least identifying data must always be passed on in order to maximize user's privacy.

Success factor 3 - Reliable limitation to justifiable parties

The e-identity system must ensure that all parties involved have a necessary and legitimate claim to be part of the identity value chain. This can be the identity provider who provides personal data to the e-identity system or the service provider who receives this data. The user must always be able to rely on the fact that these parties are the actual parties as well as that only the released data is provided and that data is used for the purpose it has been approved for.

The former is no longer a major problem today by using PKI infrastructures and certificates etc. The latter can be solved by explicit agreements between the parties with regard to data transfer and data use. In accordance with success factor 1, the granted usage rights of disclosing individual data per specific transaction could be logged in the "Release Manager" for maximum transparency and traceability.

The e-identity system receives certain know-your-customer obligations to directly sanction individual infringements within the system, thereby reducing the risk to all other parties.

Success factor 4 - Consideration of directed identities

The concept of directed identities distinguishes the visibility and communication direction of identity entities. Omnidirectional identities are those that are publicly known and visible or accessible and that invite to communicate: it can be a beacon in a physical shop, a card reader, or even a webshop online.

While this omnidirectional identity makes sense for public parties, it must be strictly avoided for private identities. Communication may only be initiated with reliable and trusted parties, ideally after the user's consent (unidirectional identity). Strictly speaking, NFC- or RFID-enabled payment cards and older national ID cards are negative examples, since information identifying the user (their account data or personal data) can be read out without a check of the issuing authority or explicit consent of the user taking place.

Especially for higher value identification use cases, only unidirectional identities for private parties in accordance with success factor 1, i.e. under the control and consent of the user, shall be allowed for.

Success factor 5 - Pluralism of operators & technologies

An e-identity system is only as valuable as the context in which it is used. The multiplicity of these contexts and their specific characteristics make the standardization in a comprehensive system and its acceptance on the user side difficult. Cameron is even clearer:

„One reason there will never be a single, centralized monolithic system is because the characteristics that would make any system ideal in one context will disqualify it in another.“

Kim Cameron, Microsoft Corporation, 2005

An e-identity system must be polycentric and polymorphic, according to Cameron. It must be an association of several specific e-identity systems and therefore exist in different forms depending on the context; a metasystem as a system of systems.

At this point, however, it is necessary to make a conceptual distinction as to whether the entirety of the identifying information is centralized in a monolithic system or merely the authentication information (logins) and possibly elementary identifying information. Cameron is particularly referring to the first case. In the second case, only user authentication is standardized and identifying information, which is relevant in almost all contexts, is kept in a monolithic system, while information and features that go beyond that,

if necessary, can also be accessed in a polycentric manner on specific e-identity systems. In this case, provision should be made to ensure acceptance of the system for contextual use cases, cf. success factor 8 "context-specific persona concept".

By contrast, established players such as Google, Facebook or LinkedIn are monolithic systems which process and maintain the personal data in each case in a central system (even if this is technically realized with a large number of systems). This works great for elementary and unverified identity data. As soon as it goes beyond that, the weaknesses of these approaches become clear. For example, verified information or context-specific attributes would have to be integrated into the central system, and users would always have to be willing to maintain all the data in just that one place (Facebook? Google?). This willingness will not exist in every context.

Success factor 6 - Human integration, seamless & secure

Cameron's Law 6 "Human Integration" focuses in particular on securing the integration of humans, i.e. on challenges of cross-channel and cross-platform user authentication with the aim of avoiding identity fraud. This point is inevitably correct but has lost some of its attention in recent years due to a large number of new and sufficiently reliable security mechanisms and concepts (especially biometrics). The balance remains: Ease of use against risk.

The security of a system regarding the integration of the user can be achieved in different ways: technically, organizationally or procedural. For all considerations, it is important to ensure the smoothest possible integration. Can bulky multiple factor authentication potentially be avoided? Are concepts of background security applicable, such as passive behavioural methods? May the authentication method used be standardized across all contexts and thus the concept of providing a "master key" actually be realized?

Success factor 7 - Consistent user experience

There is no need to say much about the imperative for a simple, consistent and unified user experience for digital products. For example, as today's payment process is largely minimized to a one-click process, identification processes should also be as simple, lean and frictionless as possible.

However, uniformity plays an important role in e-identity systems due to the different contexts in which they are used. The user guidance and the user experience should always be assignable and recognizable and follow the same or at least similar patterns, regardless of the specific usage scenario; be it when logging in on a news website online,

in the online identification carried out as part of opening a bank account or even during user authentication to open the doors of a rental vehicle.

Users need to be aware that they are using the respective e-identity system and what action (e.g. authentication) is required of them. The user experience should not fundamentally differ when logging in to a website from logging in to a vehicle (in the rental process). The consideration of the success factor 5 "Pluralism of operators and technologies" may create special challenges at this point.

Success factor 8 - Context-specific persona concept

The motivation of today's e-identity systems is mainly to create an identity standard for many (ideally all) digital use cases. Due to the variety of different contexts, along with different perceptions of the users, the acceptance of using a single identity for all these use cases will be very low. The daily search on the Internet or the login on new and previously unknown websites may lead to disturbing emotions when using the officially verified identity and possibly with deposited means of payment. You may want to use the service with a strongly reduced or even deliberately false identity, and that even starts with the e-mail address. It is not for nothing that providers of fake mail accounts are enjoying high popularity. If the e-identity system is applicable across all contexts, users will want to choose the identity with which they are actually under way. Possible contextual identities can be roughly summarized as follows:

Fundamental Persona Concept

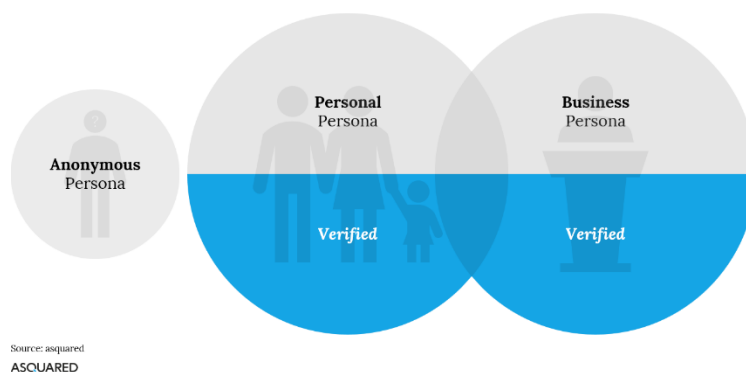


Figure 2: Illustration of fundamental persona concept

Anonymous persona - an identity with self-declared identity data that does not necessarily correspond to reality, aiming at not disclosing any real identity data. These are used, for example, for websites and services subject to registration, but where this identity data is not at all relevant to business. An example is the frequent need to specify an e-mail address.

Personal persona - an identity based on real personal data. These are initially self-explanatory, but the user has a vested interest in providing real data because they are required in the business process. Example: name and delivery address for e-commerce orders. Using these, fraud cases are fundamentally unavoidable. However, if the identity data are verified by a certified authority, they can also be used for higher-value applications. If even certified means of identity are integrated (for example, the digital identity card), business cases are also possible which require AML-compliant identifications.

Business Persona - is an identity that essentially provides identifying information about a person in his professional context, such as the current employment situation or even the stations of professional career, as well as professional contact information. There is an intersection with the personal persona - at least with the name attribute. Again, these identities could be verified. This way, for example, branch- or company-wide networks could be formed, company purchases could be pooled or internal services could be used (use of department vehicles or similar).

It is very likely that more differentiated personas will emerge. Depending on the scope of the e-identity system, there will be users who will use all personas, others use only a specific persona focussing on a specific context etc. The users have the choice and can determine which of their identities should be used and how much information is revealed about their identity.

An e-identity system should consistently implement the Persona concept, thereby highlighting the self-determination of users in line with Success Factor 1 "User Control and Consent".

Success factor 9 - Omnipresent applicability

An e-identity system may fulfil all previously mentioned success factors; however, as long as it does not gain a pervasive market reach, it will not succeed. In order to be established as a de-facto identity standard, an omnipresence for the users should be aimed and this across all contexts and channels.

Cross-context presence

As with almost all new product placements, the challenge lies - but here with particular relevance - in the solution of the famous hen-egg problem. The first 8 success factors mainly focus on user acceptance. In order to be listed as an identification instrument with as many acceptance points as possible across all contexts, the acceptance requirements on the part of the respective service provider must also be taken into account. These include in particular:

- 1 *Functionality per context* - The different contexts in the different sectors or industries place different demands on the features of the identity solution. The functionality of a specialized AML- or LOA4-compliant solution is not required for a variety of everyday online applications. A pure single-sign-on solution, on the other hand, is insufficient for eGovernment applications. It is therefore important to establish solutions with a modular and diversified range of functions.
- 2 *Potential (realistic) user reach* - For a new product it is always difficult to initially score with high numbers of users. However, it is all the more important not to allow any hurdles of acceptance for users and to avoid excluding certain user groups. In the case of identity solutions and the associated need for trust, independence from individual providers is an important success factor. Likewise, the simplicity of user registration; Ideally, existing identities can be reused. The participation of large companies with a large customer base alone is no guarantee for success. Again and again you hear "we bring in X m. customers directly". Still, the users decide and want to be convinced. Thus, establishing new digital solutions in hitherto untapped contexts with direct added value for the customer is the way to go.
- 3 *Costs* - Other non-functional killers of reach are the costs and organizational hurdles (see point 4). Identity solutions are not praiseworthy, whenever it is just about unverified identity data (single sign-on, self-declared data). Only LOA4-functionalities can be calculated realistically. For e-identity systems, therefore, the identity functionality alone will not allow for a dark green business case. For service providers, it will have to be almost free of charge and it is important to use alternative business models.
- 4 *Contracts and SLAs etc.* - Ideally, participation in an e-identity system requires only one participation contract. In reality, however, this will not be so easy due to the pluralism of operators (success factor 5) or, depending on the shareholder structure, due to the competition and antitrust laws. In this case, however, it will be essential to ensure that market-driven concentrator and facilitator models exist to facilitate contractual onboarding, especially for medium-sized and smaller players.

Cross-channel presence

In addition to cross-context presence, a cross-channel presence is also indispensable for the far-reaching applicability of an e-identity system. Multi cross and omnichannel availabilities are the keywords here. This way only, it can be ensured that a system actually will find extensive applicability.

New business models in particular are increasingly tailored to mobile applicability, e. g. in the mobility context or in stationary commerce. High availability of systems is nowadays assumed to be complied to anyway, but in mobile applications of e-identity systems,

permanent availability is a particular issue, which is why the solutions should also include mechanisms that enable offline capability.

In this context, the system must always be open to third parties and offer appropriate integration options. The functionality must be integrable into third-party apps or into other systems (e.g. cash register or production systems).

Conclusion

Based on Kim Cameron's Laws of Identity, we have summarized nine success factors for today's e-identity systems. These relate to both user acceptance and acceptance by service providers; Adhering to them will be key to establishing a widely accepted and competitive solution, even for non-European competition.

In this context, it will be very interesting to see how the announced initiatives are positioned and which of the points are being considered. But it will also be particularly exciting to find out which of the points are not explicitly addressed and to see how they are resolved instead.

In addition to these system-specific target systems, the biggest challenge for all service providers is to close existing digitalization gaps by formulating innovative use cases (also using potentially available e-identity systems), thus providing users with a clearly perceivable added value. Omnipresent digital identities are an enabler for cross channel and cross domain approaches. The combination of existing use cases, which only allow additional services to the established products, will only be possible with a minimum of cross-provider and cross-industry cooperation. But as soon as this becomes reality, it will finally be really exciting for the user.

Sources

- 1 Kim Cameron, The Laws of Identity, 11.05.2005,
<http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>
- 2 Asquared - Innovations- und Technologie-Blog, E-Identity-Lösungen in Europa – Ein europäischer Vergleich, 15.02.2018,
<https://asquared.company/blog/e-identity-loesungen-in-europa-ein-europaeischer-vergleich-686/>
- 3 Meedia, Transparenz-Offensive: Facebook startet neue Kampagne zu Datenschutz und Privatsphäre, 29.01.2018,
<http://meedia.de/2018/01/29/facebook-startet-neue-kampagne-zu-daten-schutz-und-privatsphaere/>
- 4 Datenschutzbeauftragter INFO, WeChat Goes West – Chinas Überwachungs-App kommt, 16.01.2018,
<https://www.datenschutzbeauftragter-info.de/wechat-goes-west-chinas-ueberwachungs-app-kommt/>
- 5 The Verge, How WeChat came to rule China - The multipurpose messaging app is becoming the nation's ID system, 01.02.2018,
<https://www.theverge.com/2018/2/1/16721230/wechat-china-app-mini-programs-messaging-electronic-id-system>
- 6 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), 27.04.2016,
<http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32016R0679>
- 7 Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 44, Gesetz zur Anpassung des Datenschutzrechts, an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG-EU), 05.07.2017,
https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBL#_bgbl_%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf

Authors



Dr. Andreas Windisch is Managing Director at asquared. As a certified computer scientist and with a doctorate in engineering, he acted in leading positions in automotive, technology and consulting firms and disposes of many years of experience in the field of IT transformation management - especially in the banking and financial services sector.



About asquared

Asquared is a Berlin-based consulting firm. Our work focuses on developing practical solutions for the regulatory, technologically and/or socially induced change, associated with direct application and confirmation in an industrial environment.

Our attention is focused on business and technology and their interaction. Reaching from the reorientation of strategies, over the (re)design of products and services to the operationalization - our work focuses on shaping change. On all levels.

We present selected insights of our theoretic and practical research work to a broader audience in the form of publications and lectures.

asquared GmbH


Pappelallee 78/79


10437 Berlin - Germany

Phone +49 (0) 30 22 66 79 60


E-Mail contact@asquared.team

 asquared.company

 asquared.blog

 twitter.com/asquaredgmbh

 [instagram.com/asquaredgmbh](https://www.instagram.com/asquaredgmbh)

 [linkedin.com/company/asquared](https://www.linkedin.com/company/asquared)