

Apple Identity Wallet

Disruption as a catalyst for digital transformation

Artur Burgardt
Maarten Oestreich
Pierre Heugle

Key Facts

- › In context of the continuously growing degree of digitization, the sub-sector of strong identification and authentication of private and legal persons is increasingly being transferred to the digital world. An exponentially growing, cross-industry market potential of digital identity management is evident
- › The market significance of technological progress is underpinned by the regulatory and catalytic influence of the European Parliament and Council in the form of the eIDAS (electronic identification, authentication and trust services) regulation. The existing demand for defined interoperability is further illustrated by the number of national eID schemes already notified or under examination
- › Based on the iOS 13 operating system, which was released on September 19, it is now possible for the first time to read the new ID card via the eID functionality on Apple devices and use the derived identity for digital use cases
- › Taking into account Apple's recently published components in the form of the CryptoKit for the possible establishment of hardware-based wallets as a prerequisite for the secure, local storage of digital identity information, focused market positioning of Apple's login functionality as a primary authentication option, as well as the patent published on 24.10.2019 for the secure storage and reuse of identity information (Identity Credential Verification Techniques), the required core areas of a fully comprehensive identity management system can be provided
- › An active marketing of the new identity card in the form of the eID functionality and the accompanying orientation towards the use of Android and iOS devices leads to an actively promoted customer acceptance of mobile-device-based identification and thus an indirect lowering of the market entry barriers of an Apple / Google Identity Wallet. At the same time, this would lead to / has the potential to cut off the value chain of repeated, eID-based identification, since a digital copy is derived based on initial identity verification and stored in the secure element for reuse
- › With consistent execution of the announced Apple / Google strategy orientation, the use case of recurring digital identity verification, e.g. in the form of Video-Ident, and thus the main business area of current market participants of digital identification solutions will be disrupted
- › Due to existing technological alternatives the window of opportunity for active market participation and profitable provision of identity information (e.g. by the financial and insurance sector) is closing
- › The medium-term complete digitalization of sensitive identity information using the customer-centric, mobile-device-based data storage concept and convenient, integrative reuse without the need for re-identification can have a disruptive effect on the current market situation. Current strategic orientations of the public and private sector should be recalibrated to avoid potential displacement from the exponentially growing and highly profitable identity market

The NFC-interface (Near Field Communication), which will be accessible to third-party applications starting with iOS 13, combined with the patent for the secure storage and reuse of identity information published on October 24, 2019, represents a potential change of mind compared to Apple's previous strategy.

In the area of exponentially increasing, cross-industry digitization, the sub-sector of strong identification and authentication of private and legal persons is increasingly being transferred to the digital world. The progressive development of corresponding services is multifactorial favored by the technological maturity of available digital identification and authentication solutions with regard to the required security and accepted official ID documents as well as by the clear user expectations with regard to digital products without media discontinuity. Based on this, new segments of significant market relevance based on strong identification / authentication are emerging, such as e-health, Internet of Things and smart cities. Within existing industries of sensitive customer identities (e.g. banking, insurance), the possibility of comprehensive, compliance and security conformable digitalization of regulated identity verification processes arise.

In this context, the published iOS 13 operating software represents with regard to the NFC interface (Near Field Communication), which is partially accessible for third party applications, a potential change of mind of Apple's closed ecosystem focused strategy. Based on this approach it is possible for the first time, as already established on Android devices, to read out the identity card via the eID functionality and to use the derived identity for digital application areas. Although the market acceptance of this solution is currently limited due to historically partly complex onboarding processes and only selectively available use cases, the automatic activation of the eID functionality, which has been prescribed by the regulatory authorities since 15.07.2017, and the presumably short-term withdrawal of regulatory conformity of alternative identification methods in form of Video-Ident based methods for AML-compliant (Anti-money laundering) use cases counteracts this deficit. Thus, instead of an extraordinary individual decision, an overarching, presumably prepared strategy orientation becomes apparent by considering the overarching market potential of digital identity management. This hypothesis is strengthened by the announcement of the CryptoKit at the Apple Worldwide Developers Conference 2019 for possible establishment of hardware-based wallets as a prerequisite for the secure, local storage of digital identity information, and the focused market positioning of the Apple login functionality as a primary authentication option. The initial assumption of a dedicated strategy focus is most recently confirmed by the latest Apple patents for the secure storage and reuse of identity information (Identity Credential Verification Techniques - Pub. No. 20190325125, 20190327228). These patents are structured along the sub-areas of secure creation, storage and transmission of digital identity information based on driving license and ID card as official identity document.

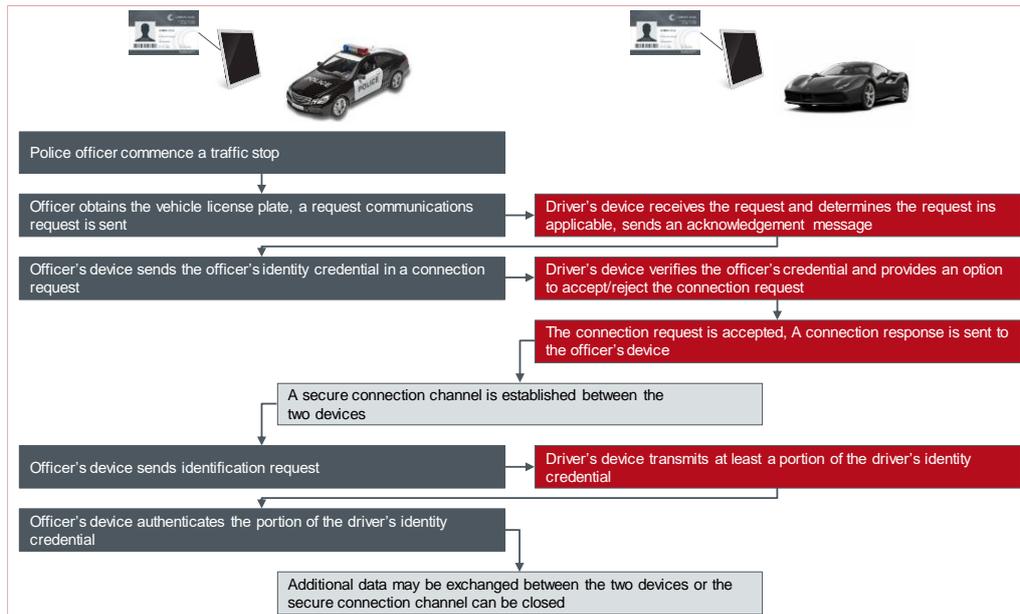


Figure 1 - Apple patent excerpt - sample process for identity provision and verification

Hereby the required components for a comprehensive identity management system in form of strong identity validation, local data storage and downstream authentication could be combined. This approach not only allows Apple to establish themselves as a digital identity provider, but also to fulfill the necessary technical prerequisites for the targeted positioning within the profitable e-Health sector. The Supervisory Board of Apple Inc. determined to extend the group strategy by e-health components for hardware, software and services. Meanwhile, the company's CEO, Tim Cook, postulates this aspect as the company's greatest future value driver and at the same time the greatest contribution to the society; he speaks of the global community. In this context in 2018, three functionalities of the Apple Watch (ECG sensor, pulse sensor for detecting atrial fibrillation, fall sensor) were simultaneously approved by the Food and Drug Administration of the United States FDA, or are currently undergoing final testing.

In addition to Apple, the technology company Google, as the main player, is also driving technological progress of secure and convenient customer identification and authentication. During the developer conference Google I/O 2019 the ambition of comprehensive transfer of electronic identities to Google devices and offering the utilization of these via a dedicated API was communicated. As initial step the system should be able to provide qualifying proof of possession of a driving license in accordance with ISO 18013-5. The definition of related standards has been actively supported and co-developed by Google for years.

Exponentially growing, cross-industry market potential of digital identity identified

Considering the exponentially growing market potential of identity-based use cases, the early strategic orientation of global technology companies Apple and Google is fully replicable. The e-health industry segment reached a market value of 142 billion dollars in 2018. Based on current assumptions the 200 billion dollar value should be exceeded in 2020 (see Figure 2).

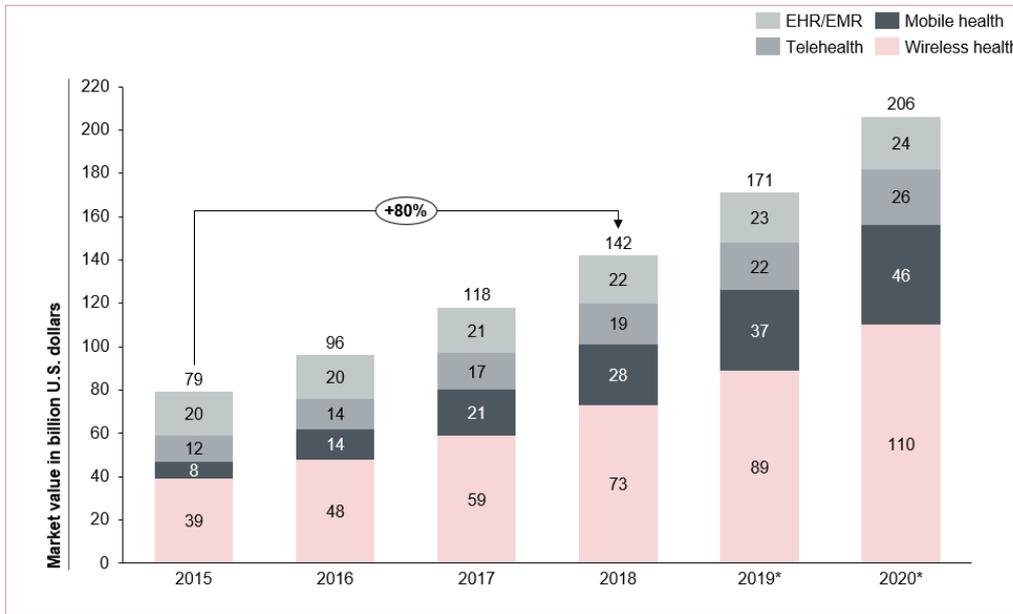


Figure 2 - Market value of the global digital healthcare market from 2015 to 2020 in billions of US dollars (* forecast 2019, 2020)

As an addition example for the significant potential of the digital identity market 94 billion dollars revenue was generated globally in 2018 within the identity-based IoT industry, leading to 50% increase over the last 4 years (see Figure 3). Based on the current forecasts, the number of installed IoT devices will increase accordingly by 133% over the next 5 years (see Figure 4).

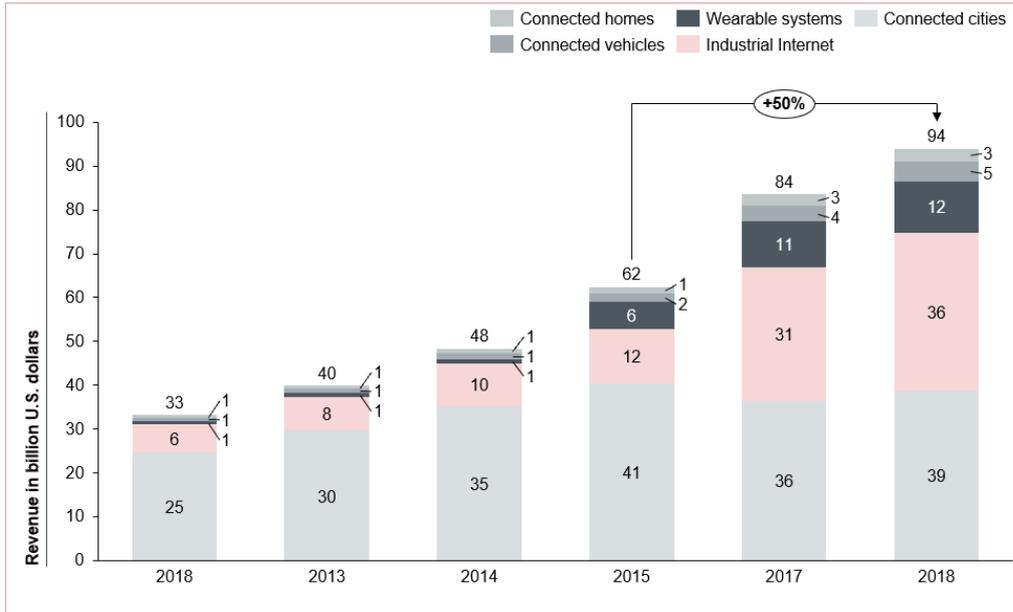


Figure 3 - Revenue of Internet of Things subsystems worldwide from 2012 to 2018 (in billion U.S. dollars)

For possible management and administration of the variety of connected devices (expected 62 billion in 2024 – see figure 4) in respect to required identity assignment and fraud prevention related identity management systems, including associated technologies, standards and interoperability concepts are rising on the global market.

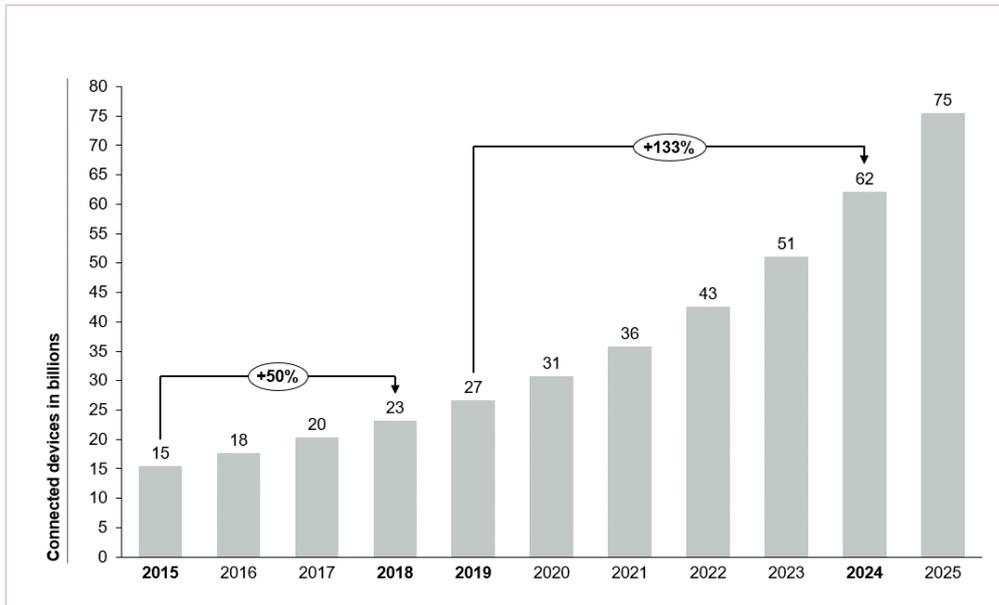


Figure 4 - Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)

The significantly increasing market potential of digital identities is evident not only in emerging business areas (e.g. e-health, Internet of Things), but also within already established segments such as the banking and payment sector.

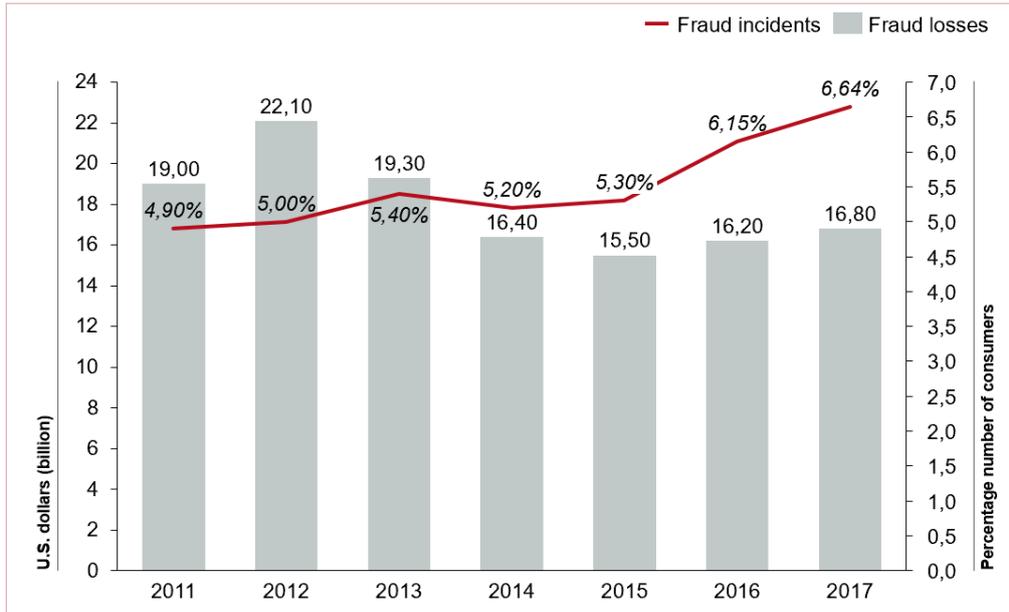


Figure 5 - Fraud Incidence Rate and Dollar Amount Losses, 2011-2017

In summary, 61% (~ U.S. \$13.48 billion) of the fraud damage suffered in the United States in 2018 is due to identity theft. Considering significantly increasing CNP fraud rates (Card not present, +94% in 2017 compared to 2014 - see Figure 6), the establishment of technologically sophisticated identity management systems and modern authentication methods is the main driver to minimize and control the risk potential arising from digital identity theft.

At the same time, the derived process chains (e.g. know-your-customer) can be fully digitized, streamlined and optimized based on emerging, regulatory compliant identification solutions within the strictly regulated financial industry.

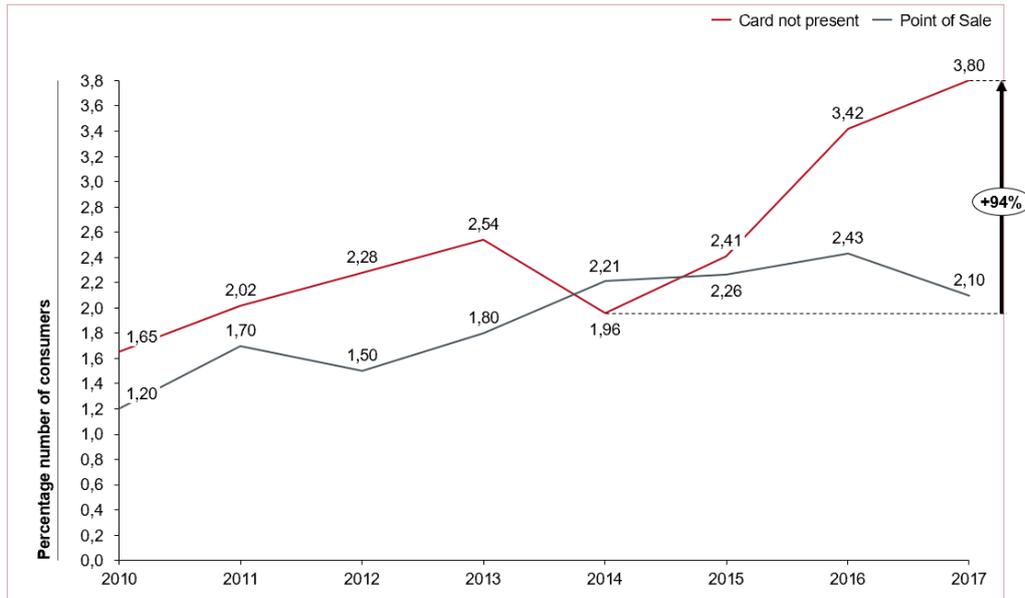


Figure 6 – Consumers who had a card misused for POS and CNP Transactions 2010 - 2017

The European-wide eIDAS (electronic identification, authentication and trust services) regulation serves as a catalyst for the digital identity market

The exponentially growing market potential of digital identities is underpinned by the regulatory and catalytic influence of the European Parliament and Council in form of the eIDAS (electronic identification, authentication and trust services) Regulation (EU) No. 910/2014. This allegation repeals the Signature Directive 1999/93/EC and promotes the removal of digital barriers for Europe-wide citizen identification in the field of public services in form of establishing inter-state interoperability. Hereby the European market potential of digital use cases based on strong customer identification / authentication should be raised. Due to the eIDAS regulation is a directly applicable law on the national market within the European union since July 2016 (Art. 52), the derived national requirements must be implemented in all 28 EU member states. The existing demand for defined interoperability is further illustrated by the number of national eID schemes already notified or under examination, which must be accepted by all member states latest 12 months after notification on every national market in area of national online services of public authorities (Regulation No. 910/2014 - Chapter II, Article 6).

The resulting growth of digital customer data usage and communication is supported by the EU-DSGVO and e-Privacy regulation, focusing on customer-centric data protection and transparent information utilization and provisioning.

eIDAS notification status overview



eIDAS notification status per state

State	Level of Assurance	Status
Belgium	High	Notified
Croatia	High	Notified
Czechia	High	Notified
Estonia	High	Notified
Germany	High	Notified
Italy - eID	High	Notified
Italy - SPID	Low - high	Notified
Latvia	(High)	Pre-notified
Luxemburg	High	Notified
Portugal - eID	High	Notified
Portugal - Mobil	(High)	Peer-reviewed
Portugal - Attribute	(High)	Pre-notified
Span	High	Notified
Netherlands	Substantial – high	Notified
UK	Low – substantial	Notified
Slovakia	(High)	Pre-notified
Denmark	tbd	Pre-notified

Figure 7 - Status eID schemes notification procedure

Globally operating, technology-driven and cross-industry oriented platforms are predestinated to drive the market for digital identity management systems based on an already significant customer base

Derived from the described demand for digital, strong customer identification and authentication, three forms of possible business models arise within the digital identity management ecosystem:

- **Identification / authentication solution provider:** Company specializing in research, development and provision of digital solutions for identity verification (e.g. video and call center agent- / video and algorithm-based verification, NFC-specific use of the ID card/ eID functionality) based official identity documents (e.g. ID card, passport) and downstream customer authentication (e.g. face / voice recognition)
- **Identity Orchestrator:** Consolidation of existing identification and authentication solutions via a central, consolidated API to simplify the integrations of multiple identification and authentication methods.
- **Identity management systems:** Systems designed for the potential storage, administration and distribution of digital identities, which partially include existing, commercially available identification solutions and cooperate with other identity orchestrators. Here, a distinction can be made between concepts of centralized and decentralized data storage.

In this context, the business models described are synergistically interdependent and pursue a differentiated strategy orientation.

-
- The identification / authentication solution providers focus on optimizing existing and developing new, more convenient identification and authentication methods (e.g. algorithm-based document recognition, voice recognition, behavior metrics).
 - The identity orchestrators are focusing on the disproportionately growing number of integrated identification and authentication methods
 - The identity management systems are targeting the highest possible cross-industry market acceptance for possible reuse of stored identities along all common security levels / levels of assurance (ISO/IEC 29115)

Due to possible direct or implicit integration of identification/authentication solution providers and repeatable reuse of only once verified identities, identity management systems, as an infrastructural anchor of digital actions offer probably the most significant market potential.

In this context, globally operating, cross-industry technology companies are predestined to push the market for digital identity management systems based on an already significant customer base. The initial step is to position the mandatory creation of a low-threshold identity for the possible product usage. As soon as a significant market acceptance of the established product is achieved, established identities will be offered as a source for authentication in third-party applications, so the company is able to increase their visibility as an identity administrator and provider. By positioning further cross-industry offerings the required omnipresence of digital identities and associated increase of customer trust can be established. As a final step the company establishes itself as a digital identity management system by integrating further identification / authentication solution providers, which creates a strong customer loyalty to the already widely accepted ecosystem.

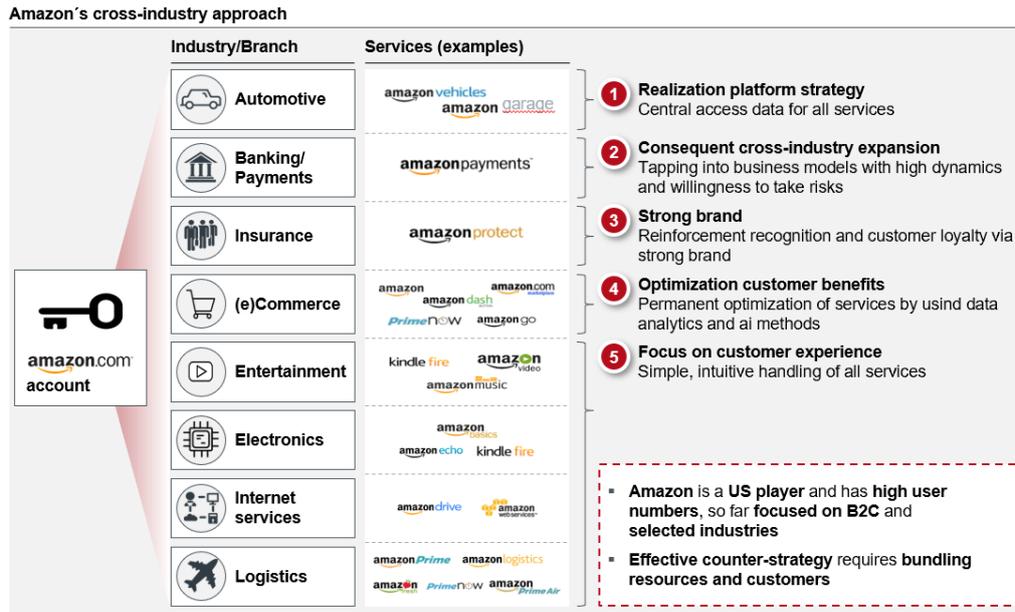


Figure 8 - The degree of penetration achieved is clearly visible on Amazon

This strategic approach can be exemplarily illustrated by Amazon, which currently offers various services and products using the same identity within 8 different industries with a total global turnover of ~140 billion USD in 2016.

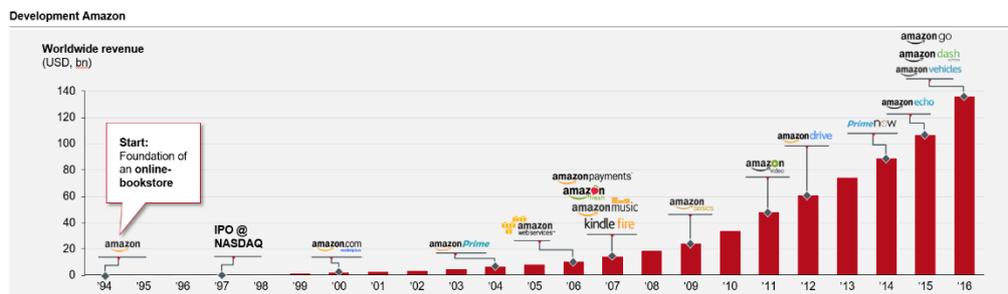


Figure 9 - Worldwide turnover of Amazon 1994 - 2016 in billion U.S. dollars

Further international platform providers in the form of Google, Apple, Facebook and Alibaba were also able to increase the number of customers significantly over the last few years while pursuing a similar strategic orientation.

Comparable market potential can also be identified at globally operating card schemes which, on the one hand, utilize sustainable identification/authentication methods in form of self-optimization to counter growing number of digital fraud and, on the other hand, are able to offer the identification/authentication solutions fully integrated within the existing worldwide payment network by only minimal strategy adjustments.

In this context, MasterCard has announced a digital identity initiative for joint development of future-oriented identity management innovations in cooperation with Microsoft (December 2018)

and Samsung (May 2019). The existing concept focuses on decentralized data storage and central market and network orchestration.

The planned Apple / Google strategy of local identity storage and direct information transfer leads to the disruption of existing value chain of repeated, eID-based identification.

Considering Apple's product and communication focus towards the identity-sensitive e-health market, the provision of cryptographic technologies in form of the CryptoKit for possible establishment of hardware-based wallets as a prerequisite for the secure, local storage of digital identity information and the market-aggressive positioning of Apple's login functionality, the partial accessibility of the NFC interface for identity verification and the patent application of secure storage and reusability of identity information is the next logical step for strong positioning on the profitable identity market.

This approach leads to the possibility to read out required identity information from the national ID card via integrated eID functionality on iOS devices and therefore to fully digitalize sensitive use cases relying on regulatory compliant identities. In this context, the entire process can be classified as highest security level eIDAS high based on the European eIDAS regulation and utilized within the public sector.

Due to established components as decoupled chips (secure element) within modern mobile devices for secure storage of sensitive information, established CryptoKit, the Apple login functionality and the comprehensive concept of digital identity wallet, the necessary prerequisites for comprehensive identity digitization and reuse are already in place.

In this context the respective local, heterogeneous regulatory and security requirements for digital identification of the private and public sectors as well as various technological characteristics of official identity document (ID card, passport) have to be considered. Therefore, no comprehensive product of digital identification within the closed Apple ecosystem can be provided without external support by national structures. To mitigate this situation, global technology providers can benefit from required local market knowledge through active cooperation with local solution providers and government institutions to establish a fully digital identity.

On one hand side further concepts and platforms of centralized / decentralized, server-driven data management (e.g. netID, Verimi) exist in the digital identity management market segment, on the other hand side however the advantages of device-based identity systems in form of higher self-determination and convenience surpass often server-based approaches.

In context of the governmental goal to increase the market acceptance of the eID functionality the risk of indirect but active marketing of the Apple / Google Identity Wallet, due to promoting the mobile device as valid and officially accepted entry point for secure digital identities has to be considered. As soon as the described condition has been realized, Apple / Google will be able to choose relatively compared to the eID functionality a more convenient, probably software-based identification method and apply for the eIDAS notification within a selected country with lower security requirements. Regardless of national security guidelines and potential strategic goal to

position own, governmentally promoted identification solutions, the notified solution must be accepted also on the local market within Europe due to the nature of European law. Due to in respect to the Apple Identity Wallet a digital copy will be derived and stored within the secure element for recurrent re-use, this concept additionally cuts off the value chain of repeated, eID-based identification.

Overall national characteristics will be probably not considered by global technology providers as Apple / Google as long as further, overarching technological and regulatory alternatives are available on the European market. Therefore short-term, active and join cooperation models oriented towards the best possible convenience / security balance have to be initiated by local government in order to avoid medium-term, technology-driven displacement.

Based on announced Apple / Google strategy, use cases of recurring digital validation, e.g. in the form of video identification, and thus the main business area of current market participants of digital identity validation is no longer applicable

In addition to emerging challenges within the public sector in the context of the outlined strategic orientation of global technology providers, the sustainability of current market participants of digital identity validation (e.g. via video identification) must be scrutinized. Due to the Apple / Google solution approach of device-based data storage and reuse, initial identity check to derive digital identity will still be needed, but the use case of recurring digital validation, e.g. in the form of video identification and thus the main business area of current market participants will be dropped. Therefore, it will be necessary to either position oneself as a preferred Apple / Google supplier or to shift the business to the surrounding value-added services.

Due to technological alternatives, the window of opportunity for active market participation and profitable provision of identity information by the financial and insurance sector is closing.

As the identity stored on the secure element can be derived from an initial check of official identity document (e.g. ID card, passport), but also from existing sources of already verified identities, the market relevance of further companies with identity-sensitive use cases (e.g. banks, insurance companies) should be considered in respect to the short-term realization of the Apple / Google strategy orientation. Due to the medium-term reuse of already stored identities and the possibility of initial customer verification in cooperation with established identification service providers, the window of opportunity for active market participation by the financial and insurance sector is closing.

Due to the current mobile device market penetration as a gateway to the digital world and control of security-relevant features by technology providers / manufacturers the availability of sovereign identities, regulated by the public sector should be achieved in cooperation with the private sector

The identification and recognition of persona in the physical / analogous world is a sovereign task regulated by legal authorities. The increasing demand for regulatory compliant, strong

identification in the digital world has been met by the government through the eID initiative. However, as explained at the beginning of this article, there are still practical barriers that stand in the way of widespread use, respectively the firm establishment of such identification as a central element.

The gravitational effect of the hardware providers must also be faced by institutions of the legislature, as they cannot be circumvented in the market of mobile devices as the entry gate for underlying identity management. This is because the increasing availability of mobile devices with corresponding security hardware (secure element) for strong authentication with simultaneous high convenience (biometrics) leads to extensive acceptance by the customers and thus by the citizens of the state.

A joint cooperation model should be defined in order to secure the medium-term control sovereignty of the state (see cooperation project OPTIMOS 2.0). This is necessary because a unilateral approach, as in the example described above, can lead to a lack of recognition of the system or to regulatory uncertainty and potential location arbitrage. A short-term joint approach can ensure the necessary consideration of national self-interests. When deriving a corresponding approach, system-related interoperability must be fundamentally guaranteed with regard to standardized data formats, portability between devices and uninterrupted access via different access channels. More importantly, however, such a system must take into account the framework of sovereign and supranational requirements and interests and ensure its continuous compliance. This applies all the more so because currently no uniform consensus on technical organizational requirements and the required security levels for national and European recognition (eIDAS) exists.

Until now, manufacturers have kept access to the security hardware and system-integrated applications of their components at arm's length for economic and strategic reasons. Approval was only granted for selected partners and promising use cases; for example, the identification and authorization of the active persona as a central infrastructure for digital services such as mobile payments. A service that has already advanced to a fixed business repertoire of hardware providers.

The momentum based on the current paradigm shift of the large hardware providers is a good opportunity to create a trend-setting basis for technical and regulatory standards in a cooperative approach. The active participation of public authorities in corresponding pilot projects is of fundamental importance. These can be driven by innovations of private initiatives in order to achieve prototypical implementations in the short term, which ensure practical applicability by means of iterative procedures.

These can be supported by the state in order to secure its own medium-term sovereignty obligations. To ensure recognition on the user side, the state can provide a "guarantee" for the system, positioning the infrastructure as an anchor of trust, established by the public sector.

For the possible realization of the described cooperation approach it is recommended to evaluate and if necessary, initiate dedicated security measures:

- Dynamization of structures trapped in cultural and historical patterns of experience based on cyclical rotations within established committees

-
- Establishment and piloting of public - private partnership models in more agile contexts with shorter terms, more precise target parameters and attractive but stricter bonus and malus regulations
 - Overarching technical exchange between administrative and industrial structures in communicatively protected spaces (e.g. Chatham House Rules) in order to stimulate the free exchange of information and experience and to be able to validate self-referential arguments, especially with regard to confidential information distributed among a small number of experts, without consequences

Identification providers offer bridging technology between analogue identities (sovereign document) and digital services; with increasing availability of digital identities a shift to value-added services is necessary to maintain further relevance

Up to now, identification providers have provided the bridge technology between analog identity (sovereign document) and digital authentication. However, driven by the increasing availability of digital identities based on the ecosystems of mobile device providers, the market will be subject to significant change in the medium term.

Up to now, identification services have been graded between different identification levels, which have been classified according to the balance between security and convenience (e.g. photo-ident, AI (artificial intelligence)-ident, video-ident). However, the previously conflicting dimensions of security and convenience can increasingly be realized together by establishing digital identities that are directly integrated into the mobile devices.

This change holds potential for established identification providers to proactively offer their own know-how and proven solutions for onboarding new, device-based products. This act can be carried out at short notice in order to adapt their own product portfolio to the emerging changes. However, in order to avoid a potential displacement from the market, more far-reaching adjustments are necessary. The current environment can be used for both horizontal and vertical integration in order to be able to offer value-added services in the future. This includes, for example, the aggregation of different countries in order to be able to serve them in parallel and to standardize technically different procedures that have been used up to now. An extension to KYC processes, such as sanction and PEP checks, but also company identification and qualified electronic signatures, is also possible. This shift of business towards downstream processes can be seen as a necessary lever to avoid direct competition and ensure medium-term market relevance.

In order to avoid direct market displacement and ensure medium-term participation in the digital identity market, identity holding companies should define a proactive, platform-driven market strategy in cooperation with international technology service providers

In established markets with legislatively anchored requirements with regard to the collected, identity-related data, companies are currently addressing the re-use of the internally available data foundation. This applies in particular to companies with business activities in the banking or insurance sector. Driven by the rapid development of services in the field of identification and authentication management, these companies are under pressure to position themselves with new products in the medium term. However, this is driven by the per se high quality of the existing customer and user data. This information is predestined to be used for subsequent complementary business cases such as credit transactions or to be used additively for public services within the framework of eGovernment initiatives.

As a reference various BankID procedures could be highlighted, which are characterized by high convenience and accessibility and thus a high degree of attractiveness in the Scandinavian region. What these companies have in common is that they already have a corresponding infrastructure for secure retrieval (SCA / Strong Customer Authentication) to map corresponding business processes internally.

The use of existing, identification-related data offers a significantly higher level of convenience for the end user compared to re-identification. As long as their use is authorized for the allocated services, corresponding services can be implemented quickly and pragmatically.

Using this advantage, identity management companies, especially in the finance and insurance industry, have to realize the current window of opportunity for profitable market participation of identity management in the form of an open market strategy. A contrary approach of closed systems and internal use of customer information for analysis purposes will always be regulated by the derived distribution of own products without the possibility of direct profit based on retained identities. Additively, this approach will be continuously undermined by liberalizing market forces. Thus, to avoid medium-term market displacement in the field of digital identity management, it is necessary to pursue a federal platform economy and API / open banking strategy. As a prerequisite for active market participation and the possible offer of identity information, the necessary operational measures must be defined in advance. On the one hand, the legacy systems, which have grown organically in a variety of ways, must be aligned in the direction of standardized technologies (e.g. OAuth 2.0, OpenID Connect) to ensure the necessary interoperability, and on the other hand, the identity silos, which are isolated / loosely coupled within an identity management system, primarily within large companies due to partially separately established sub products, must be consolidated (e.g. keycloak, Auth0, Okta).

Conclusion

The medium-term comprehensive digitalization of sensitive identity information utilizing customer-centric, device-based data storage concept and convenient reuse without the need for re-identification has a disruptive effect on the current market. Current strategic orientations of the public and private sector need to be recalibrated to avoid potential displacement from the exponentially growing and highly profitable identity market. In this context, it will be crucial to define pro-active cooperation models with global technology providers or shift business models towards comprehensive value-added services.

Sources

1. Statista 2019 – Value of global digital health market by major segment 2015-2020
2. Statista 2019 – Internet of Things Dossier
3. Javelin Strategy & Research - 2018 Identity Fraud: Fraud Enters a New Era of Complexity
4. Apple Patent 24.10.2019 - Identity credential verification techniques



Artur Burgardt is Managing Partner at CORE. At CORE, Artur was able to establish expertise developing comprehensive digital products, steering agile implementation projects and defining technology-driven digitalization strategies based on various large-scale projects within finance, insurance and public sector. During last years he was focusing on building up digital identity-based platforms utilizing modern technologies / standards and establishing related market strategies for private and public sector.

Mail: artur.burgardt@core.se



Maarten Oestreich is Senior Expert Manager at CORE. His main areas of expertise include digital identities, authentication procedures, IT management, product management, requirements engineering, agile methods and design thinking / user-centered innovation. His experience includes the development and implementation of a micro-service-based system landscape for mission-critical processes in an international insurance company.

Mail: maarten.oestreich@core.se



Pierre M. Heugle is Transformation Associate at CORE. He holds a Master in Business Administration and International Project Management. His main areas of expertise are Project Management, Business Intelligence and Process & Quality Management. Pierre's experience includes designing and implementing a BI-based reporting system and managing development teams for various project management tools.

Mail: pierre.heugle@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
<https://core.se/>
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
<https://core.se/>
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
<https://core.se/>
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
<https://core.se/>
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai | UAE Emirates
<https://core.se/>
Phone: +97 14 323 0633