techconsult
The IT Market Analysts

Security & Digital Identities in a Digitalised World

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Information on the study

Produced by:

techconsult
The IT Market Analysts

Contact:

Techconsult GmbH
Email: info@techconsult.de
Phone: +49 561 8109 0
Fax: +49 561 8109 101
Web: www.techconsult.de

In collaboration with:

eco ASSOCIATION OF THE INTERNET INDUSTRY

Content

Prof. Dr. Norbert Pohlmann
Board Member for IT Security at
eco – Association of the Internet Industry

Foreword

Digital credentials could soon replace many physical documents in a secure and trustworthy digital manner, and could greatly simplify processes in public administration, in business, and in society as a whole. The first digital identities available in mobile phones, such as the digital vaccination certificate, represent only the first step taken. A well-functioning infrastructure for digital identities will elevate digitalisation in many processes, offer significantly improved privacy protection, have major economic relevance and, above all, create a high level of acceptance for the digital future. The outcome will be greater trust, based on an open digital identities ecosystem. With digital processes building on each other in a secure and trustworthy form, the advantages for companies, public authorities and citizens are very clear.

Secure digital identities instead of insecure user accounts

In order to unfold the positive effects of digital identities on digitalisation, we need a sovereign European ecosystem which enables issuance and verification on the strength of the Self-Sovereign Identity (SSI). In such a user-centric ID system, all users can manage their identity data and verifiable digital credentials in a sovereign mode. This means that people can decide independently and on a sovereign basis as to when to provide the necessary identity data to which application. Blockchain technology offers an ideal and suitable trust service for the realisation of digital identities. The stakeholders are in the position to verify the authenticity and origin as well as the integrity of the digital identity data and credentials, without blockchain knowing the actual identity or the digital credentials of the users.

Together with techconsult, we have investigated how far companies and the public sector are on this path in Germany and what challenges still await us in order to make new digital applications safer and easier for us all to use.

I wish you an exciting read!

Prof. Dr. Norbert Pohlmann
Board Member for IT Security at
eco – Association of the Internet

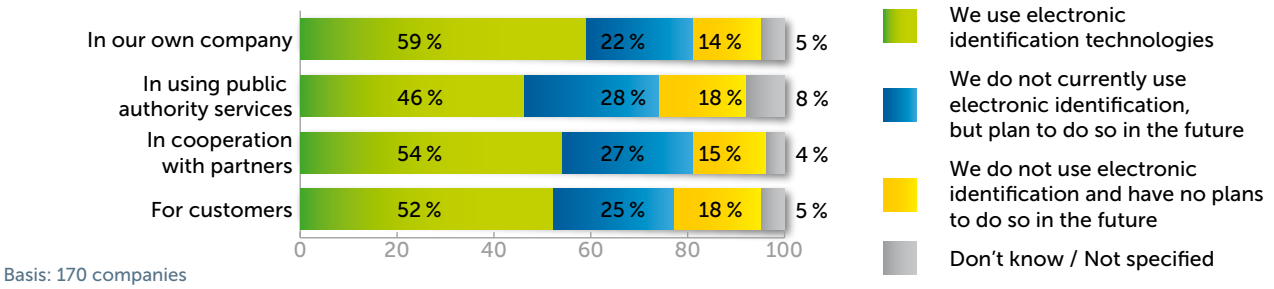
Introduction

As digitalisation steadily advances in all fields of life, it is essential to have secure electronic identification vis-à-vis public authorities and private companies on the Internet. In this context, digital identities constitute a core element of digitalisation. In observing communications, online shopping or official administration procedures, it is clear that a growing number of services are nowadays conducted online and will further burgeon in the future. In order to avail of these services, citizens currently are compelled to have innumerable user accounts – a new one for each service. And these digital identities must be secure, because identities are a lucrative commodity for cybercriminals. To counteract such threats, endeavours are being made to create secure digital identities. For example, the EU Commission wants to provide one secure digital identity for everyone in Europe. With such a central digital identity, people should be able to use a single identity to access the widest possible range of private and public services.

But what is the current situation regarding the use and offers of identity-based services? What characteristics must a single secure digital identity have in order to persuade users to avail of these services? Which official administration services would citizens and companies use if they were available? What prevents citizens and companies from availing of e-government? What requirements must be met to make online services attractive?

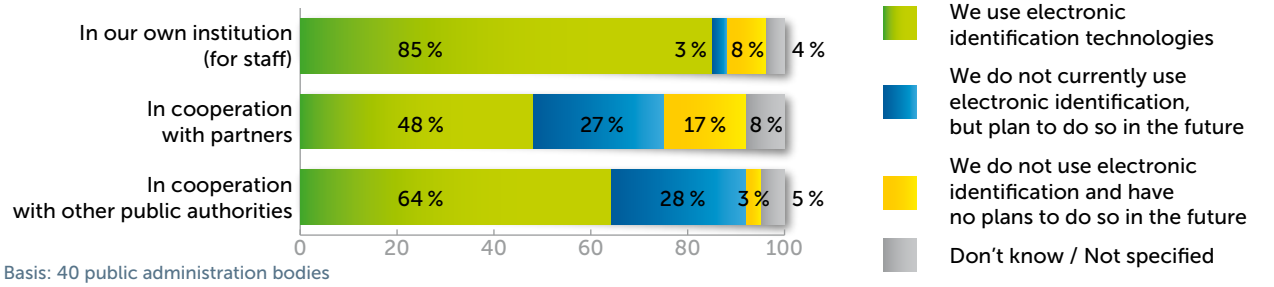
With a view to addressing these and further questions, this study is based on a survey undertaken in Germany on the assessments of digital identities. In total, 170 companies from all sectors and of all sizes, 40 public authorities, and 300 citizens aged 16 and over took part in the survey. The core questions focused not only on the status quo of the current services offered on the basis of secure digital identities in companies and public authorities, but also on the future potential of this technology and challenges in the course of its implementation.

Use of technologies for unambiguous electronic identification – **Companies**



Basis: 170 companies

Use of technologies for unambiguous electronic identification – **Public authorities**



Basis: 40 public administration bodies

Digital Identities: Status Quo, Outlook, Requirements

Deployment of technologies for electronic identification

Technologies for the unambiguous identification of persons, such as the German electronic ID function (eID) or the European eIDAS equivalent, can be availed of by companies in dealings with their customers, in cooperation with partners, in the use of public authority services, and within their companies for their own staff.

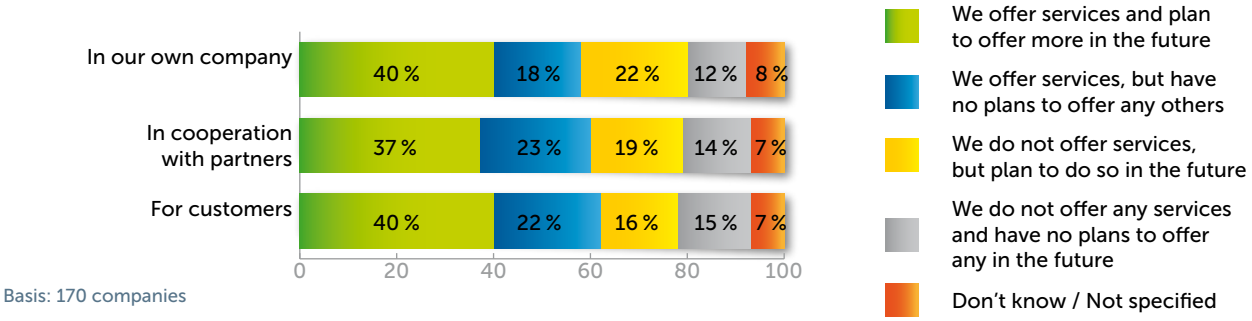
The current levels of use are quite similar across the four different deployment fields. In dealings with customers, 52 per cent of the companies use technologies for unambiguous identification; 54 per cent use these for cooperation with partners; while 59 per cent of the companies use identification technologies for their own staff. Only in the case of the use of public authority services is the proportion less than a half (46 per cent).

In the future, the proportion of companies using technologies for unambiguous electronic identification will grow even further. Across all fields of application, a 20 to 30 per cent increase in the use of technologies can be discerned. From this perspective, it can be determined that at least three quarters of the companies plan to use technologies for electronic identification in the future.

Nonetheless, there is also a sizeable proportion of companies that do not want to use electronic identification. In particular, retail companies and organisations from the health and social sectors tend to be rather sceptical. This is especially the case when it comes to customer identification. For example, 43 per cent of the retail companies and half of the non-profit organisations and companies from the health and social sector report a lack of intention to use electronic identification technologies for communication and cooperation with their customers, either now or in the future.

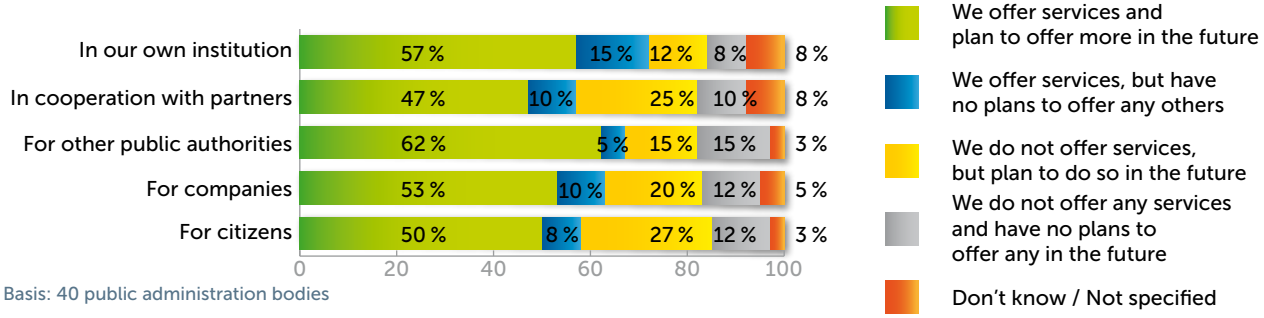
In public administration bodies, electronic identification is used much more often, especially internally. In total, 85 per cent of the municipalities use electronic identification methods for their own staff, and almost two thirds use these methods for cooperation with other public authorities

Offers of services on the basis of secure digital identities – **Companies**



Basis: 170 companies

Offers of services on the basis of secure digital identities – **Public authorities**



Basis: 40 public administration bodies

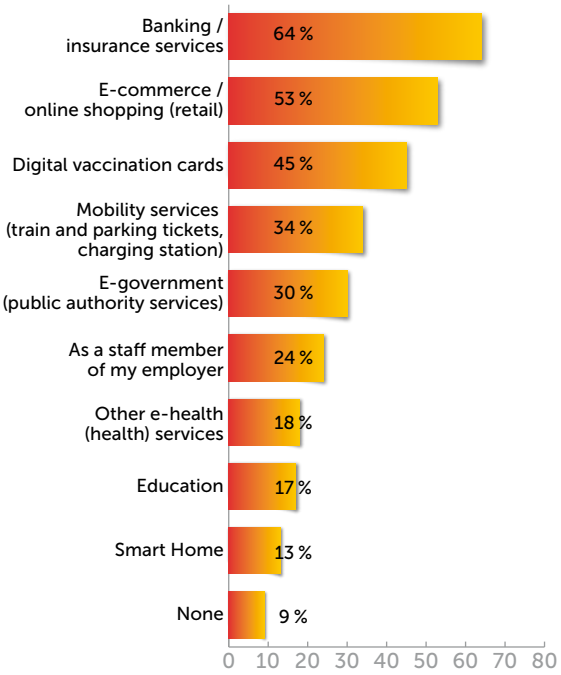
High potential for the offer of identity-based services

Companies and public authorities can use electronic identification technologies for all kinds of services for their customers, partners, their own staff, or for other institutions. Such services based on secure digital identities are offered by 40 per cent of the providers to customers, partners and their own staff, and these are intended to be further rolled out. Just under a fifth currently offer such services but have no plans to offer any further services in the future. Another 20 per cent of the companies do not currently offer any services, but plan to do so in the medium term.

Larger companies, in particular, are already increasingly using identity-based services. For instance, SIM cards can be activated at telecommunication providers via online ID, digital payments can be made via e-commerce, or security accounts can be opened at credit institutions. No single company with more than 2,500 staff reported a lack of service offers to customers or a lack of intention to offer such services in the future. The situation among a number of smaller companies with fewer than 50 staff is different. Of these small companies, 37 per cent neither offer customer-related services now nor plan to do so in the future. The situation is similar with services for partners and their own staff. The smaller the companies, the greater their disinclination to offer services based on digital identities.

Public administration bodies are already quite a bit further ahead than companies when it comes to offering services based on digital identities, such as the eID. Examples of classic application fields in the public authority environment include: digital services for citizens, such as digital administrative services with the online ID card; digitally operable vehicle registrations; or the paperless submission of tax returns (e.g., the German electronic tax declaration ELSTER). More than half of the municipalities have services that can be used by citizens and companies, and others are already in the pipeline. The availability of services will rise sharply in the future. For example, 27 per cent of the municipalities that do not yet offer digital services for citizens are planning the future initial introduction of services. In this context, services that are perceived as particularly suitable are those that are already established in other municipalities, such as the issuance of identity cards and passports or the digital registration or of the place of residence.

Fields where digital identities are used



Basis: 300 citizens (multiple answers)

Citizens open to identity-based services

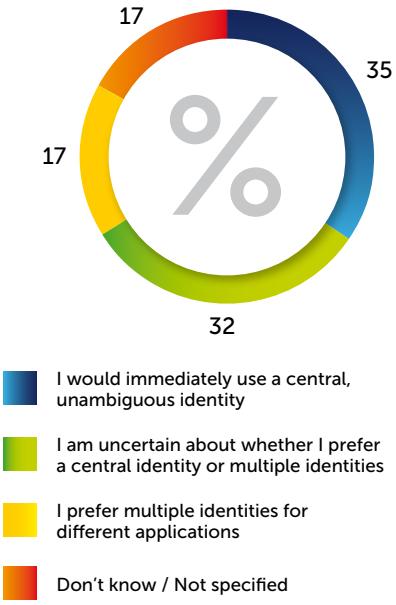
Services based on electronic identities also have great potential, as the results of the citizens' survey show. Almost two thirds of the citizens surveyed have already used digital services from banks and insurance companies. In addition, more than half of the citizens have used services based on a digital identity in the area of online retail. In addition, just under a third have already used mobility services, e.g., for train tickets or charging stations, whereas digital public authority services have so far only been used by just under 30 per cent of citizens.

In principle, citizens would consider using services based on digital identities in many fields in the future, assuming these services were also widely available. For example, 55 per cent of citizens would use e-government services to carry out their administrative procedures digitally instead of on location. A further 55 per cent would use mobility services. For instance, in the areas of car rental, car sharing or the sharing of other vehicles such as e-scooters or e-bikes, identification could be carried out simply and easily via a smartphone.

In turn, 42 per cent can envisage using digital health services. Especially with regard to the planned further development of the telematics infrastructure, in which all actors in the healthcare system will be integrated in a simple and secure ecosystem, digital health services are set to become much more attractive in the future. For example, authentication will, in future, be able to take place entirely via the eID, without chip cards. With their smartphone, patients would then be able to access services such as the electronic patient file or the electronic prescription.

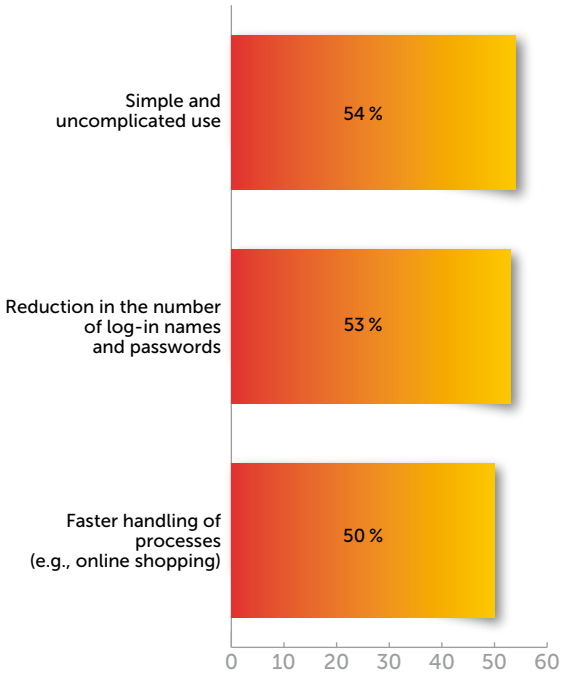
It is evident that citizens are open to using services based on digital identities. However, for this to function, these services must be available in the first instance and must fulfil certain requirements in order to be used.

Deployment of a central and unambiguous identity for the use of all online offers of state or private services



Basis: 300 citizens

Advantages of deploying a central identity



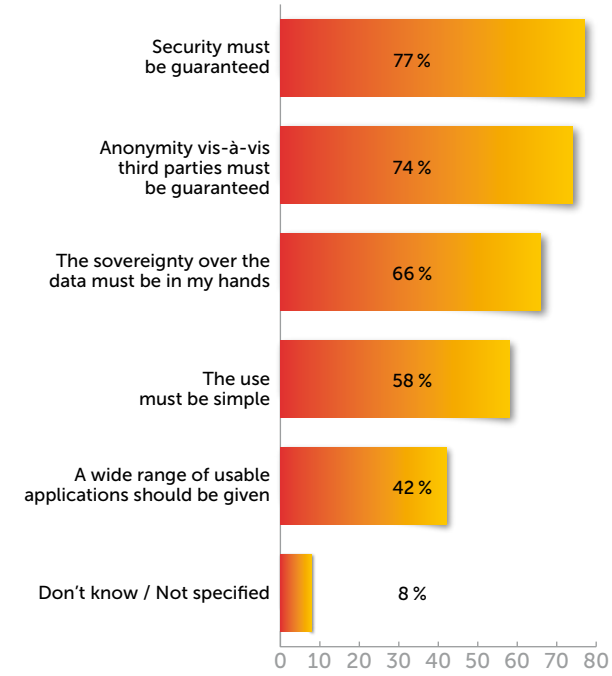
Basis: 300 citizens (multiple answers)

The central digital identity

Today, most people use different identifications for different services. Just how many there are can be seen in the number of different user accounts where citizens have to register for different services. One third of citizens have to manage more than ten different user accounts in order to use Internet services. One in ten even have more than 20 user accounts. To counteract the proliferation of different digital identities, a single secure digital identity is particularly suitable for all public authority services as well as private transactions.

It is, therefore, no surprise to learn that the deployment and use of a secure, central and unambiguous identity is viewed positively by the citizens surveyed. Of these citizens, 35 per cent would use such an identity and a further 32 per cent are, at the very least, interested in the use of such an identity, even if it is a matter of "waiting and seeing". Only 17 per cent of respondents, on the other hand, would continue to want multiple identities for different services. Citizens see the advantages above all in the simple and uncomplicated use (54 per cent) and the reduction in the number of user names and passwords (53 per cent).

Required characteristics of a universal digital identity



Basis: 300 citizens (multiple answers)

Companies and public authorities also get to benefit

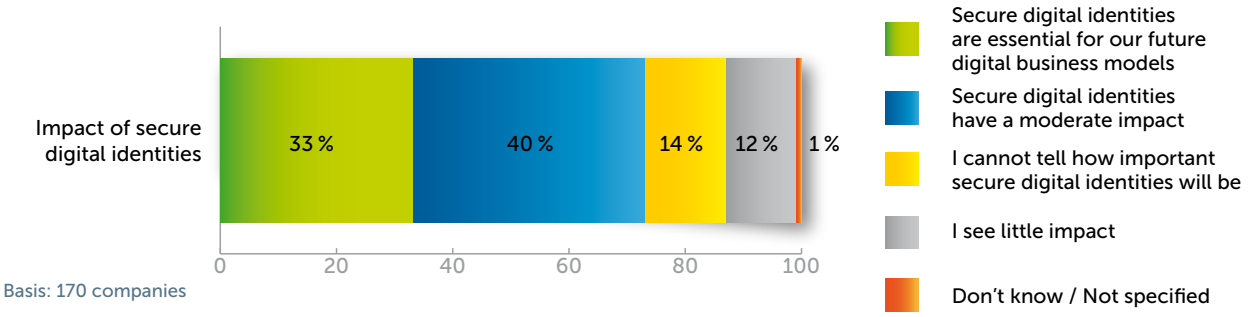
The deployment of a single central digital identity also has a number of advantages for companies and public administration bodies. Of central importance is the unambiguous identification of users and customers. In total, 55 per cent of the companies surveyed and 9 out of 10 public authorities (91 per cent) see unambiguous identification as an advantage of the very highest quality. A digital identity assigns certain unique identity attributes to each person in an unambiguously identifiable data form. Users and/or customers are already unambiguously identified via the digital identity. This also simplifies the digital onboarding process of new users, for example, which can thus become faster and more cost-efficient.

Following on from this, 44 per cent of companies identify the improvement of customer experience as an advantage. For example, it is perceived that companies would be able to offer a personalised and cross-channel user experience by means of a digital customer card to unambiguously identify customers across all channels. Simplified identity management is in the third place. In total, 42 per cent of companies and 73 per cent of public authorities see this as a great advantage of a centralised digital identity.

Security is of paramount importance

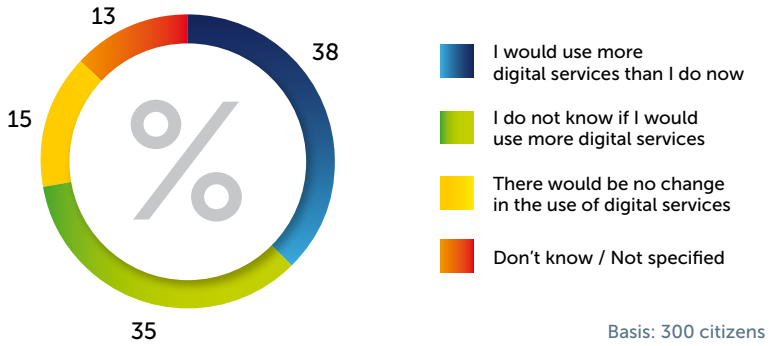
However, in order for citizens to use such a unique universal identity, it must have very specific properties. Citizens will only even consider using such a universal identity when it is absolutely secure. This is also confirmed by more than three quarters of the citizens surveyed. Disclosing highly sensitive personal data is regarded as a major obstacle for everyone. And if, for example, this data falls into the wrong hands or is made public without authorisation due to vulnerabilities, this would lead to massive damage and loss of trust. Furthermore, the majority of the citizens (74 per cent) are of the opinion that the anonymity of personal identity must also be guaranteed vis-à-vis third parties.

Impact of the deployment of secure digital identities on the success of future digital business models



Basis: 170 companies

Effects of a single secure digital identity on all private and public authority services



Basis: 300 citizens

Digital Identities: Potential and Challenges

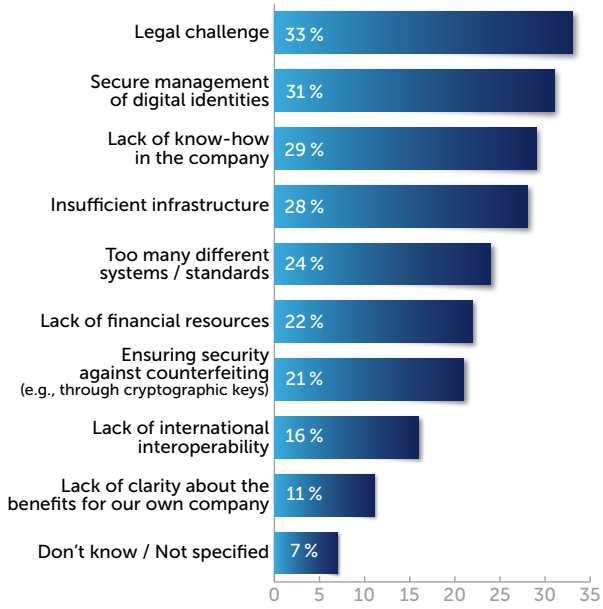
The digital identity as a success factor

To what extent do companies see the use of secure digital identities contributing to the actual success of future digital business models? After all, introducing them is not just for fun, but should bring about positive effects and concrete benefits for the companies. Overall, companies are convinced of the positive impact of secure digital identities. However, the largest number (40 per cent) do not regard the entire situation in a particularly glowing light and are merely of the opinion that secure digital identities will have a moderate impact. Just under a third are much more positive and believe that secure digital identities will have an essential impact on future digital business models.

Citizens would use more services

Above all, citizens' willingness to use more digital services – as long as the conditions are met – indicates that the introduction of a secure digital identity and its corresponding services will have a positive influence on the business models of companies. In this regard, 38 per cent of the citizens surveyed say that they would use more digital services than they currently do if they had a single secure digital identity for all private services. A further 35 per cent are still undecided about whether their use of digital services would increase or remain the same.

Implementation obstacles – **Companies**



Basis: 170 companies (multiple answers)

Implementation obstacles– **Public authorities**

Basis: 40 public administration bodies (multiple answers)

Obstacles to the implementation of central identities

Secure digital identities are an important factor for the services of the future. However, the introduction of associated technologies based on secure digital identities is not free of obstacles, given the fact that companies always have to face many issues when introducing new technology. These issues range from determining a company's own expertise, to the existing infrastructure, right through to questions of legal security.

The biggest obstacle (33 per cent) is seen to lie in the various legal challenges related to digital identities. In the maze of different legal requirements regarding identifiers – not only among different sectors, but also on a national and international level – companies without specialist knowledge can quickly come up against their own barriers.

Depending on the business sector, companies have to comply with different laws and regulations in their planning. Financial service providers in Germany, for example, have to verify the identity of their customers before entering into a business relationship in accordance with the German Anti-Money Laundering Act and the German Fiscal Code. In addition, data protection issues within the framework of the GDPR also pose major challenges for companies.

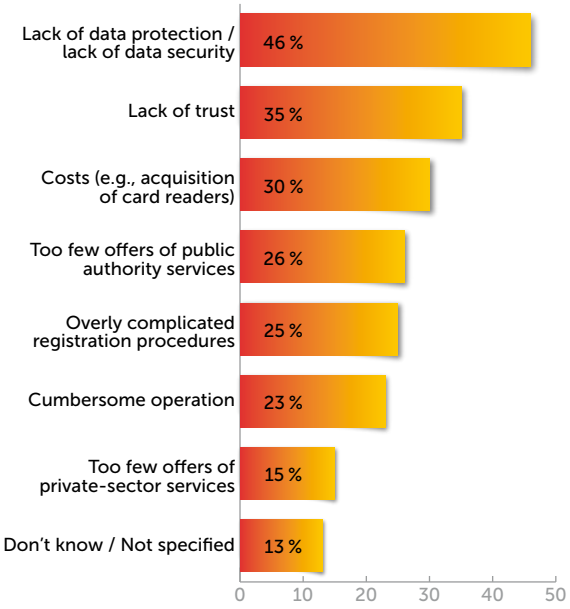
This is closely followed by the secure management of these identities. Only if the digital identities are actually used in a secure environment – i.e., protected against data theft, misuse and the like – can services be offered on the basis of identities.

The third most pressing factor concerns the lack of know-how for correct implementation. Many companies lack the necessary specialists to implement such a complex project. It is not only the expertise on the IT side that is required. The legal issues involved should also not be underestimated by the companies – because, where there is no expertise, no efforts can be made to integrate new technologies into the company.

Public authorities also overstretched by legal issues

As is the case with companies, legal issues are also a major obstacle for public authorities. Of the public authorities surveyed, 53 per cent named this as their top challenge. In second place (38 per cent) comes insufficient interoperability between different public authorities due to completely different technologies and unsuitable interfaces. The ability to interoperate with other national and international systems is a cornerstone of an overarching digital identity ecosystem. Although certain technical standards already exist in the field of digital identities, there are sometimes very different individual approaches within the various institutions, which prevents systems from communicating with each other. A unification of technical standards is essential for the provision of identity-based services.

Obstacles in the use of digital identities such as the online ID function (eID) – **Citizens**



Basis: 300 citizens (multiple answers)

The guarantee of secure management of digital identities (33 per cent) and the lack of internal know-how (33 per cent) are major obstacles that need to be overcome, with this also being the case for companies. Municipalities usually do not have enough trained IT professionals to implement such a complex project in a way that meets all legal and technical requirements.

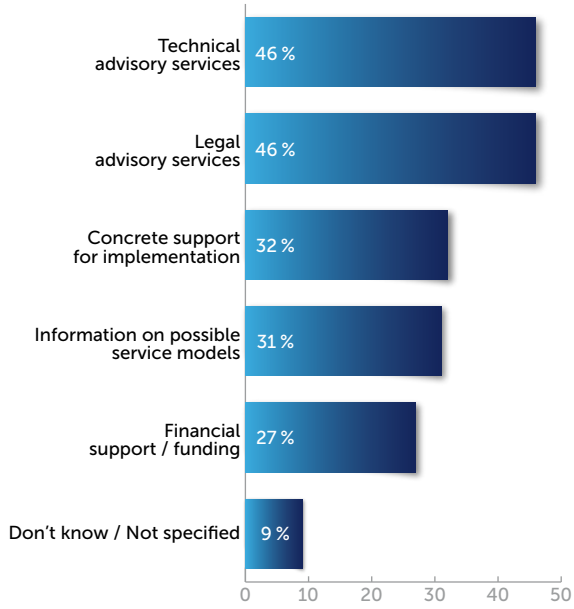
Citizens worry about security

In order for citizens to use digital identities, obstacles must be overcome. Above all, citizens regard a lack of data protection or data security as a bottleneck that prevents the use of digital identities. Of the citizens surveyed, 46 per cent have this as number one on their top three list. This is followed by a lack of trust in the technology and the services behind it (35 per cent). In third place are questions about possible additional costs; for example, for the acquisition of card readers.

Closing skills gaps with providers

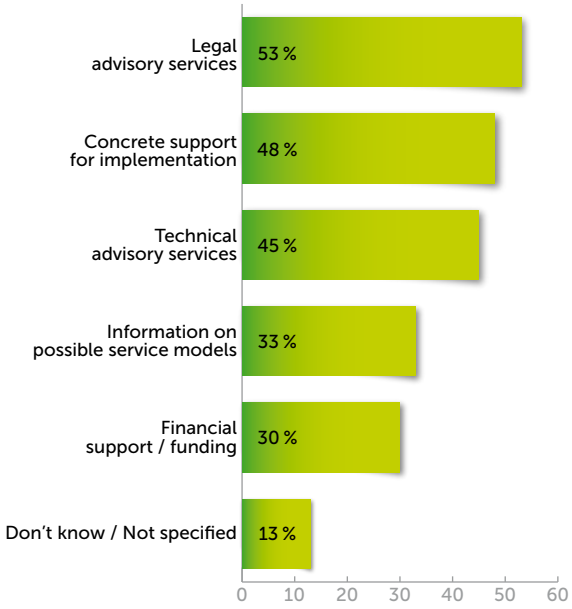
Companies and public authorities should urgently examine the possibility of closing their own qualification gaps with the help of external providers. These providers can not only offer advice and support with the necessary know-how on technology, but also have experts for legal or security-related questions who help to flawlessly implement the technologies in companies. Those companies and public authorities that close their gaps and make digital identities a core aspect of their future business strategy will have the chance to establish themselves on the market as innovative and competent partners.

Required support services to offer more identity-based online services in the future – **Companies**



Basis: 170 companies (multiple answers)

Required support services to offer more identity-based online services in the future – **Public authorities**



Basis: 40 public administration bodies (multiple answers)

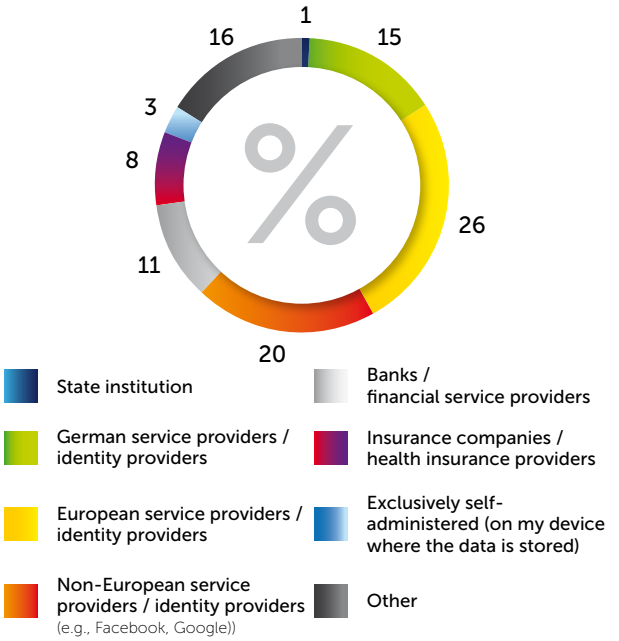
A call for technical and legal advisory support

As already noted, companies and public administration bodies generally cannot implement identity-based online services on their own and need targeted assistance. In line with the obstacles mentioned on behalf of the companies and public authorities, what would be particularly welcomed is assistance with legal matters. In total, 46 per cent of the companies and 53 per cent of the public administration bodies would like legal advice on how to introduce identity-based services in a legally compliant manner. Among other factors, there are different regulations and standards in different jurisdictions, and there are also different sector-specific requirements. In order to be able to harness the potential of digital identities, legal standards must be harmonised.

Technical advisory services are also high up on the wish list. On the part of both companies (46 per cent) and public administration bodies (45 per cent), almost half of the respondents need support on questions such as how to integrate the services into the existing IT infrastructure.

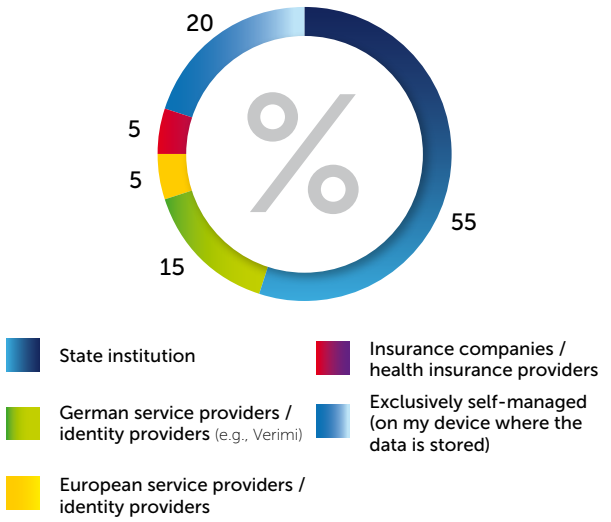
Public administration bodies also have a greater need for support in implementing the introduction of identity-based online services in practice. Almost half of the public administration bodies would like assistance in this regard. In comparison, companies are much more confident in their implementation. Just under a third of the companies state that they rely on additional support.

Trust in providers for the management of central (universal) digital identities – **Companies**



Basis: 170 companies

Trust in providers for the management of central (universal) digital identities – **Public authorities**



Basis: 40 public administration bodies

Management of the digital identities

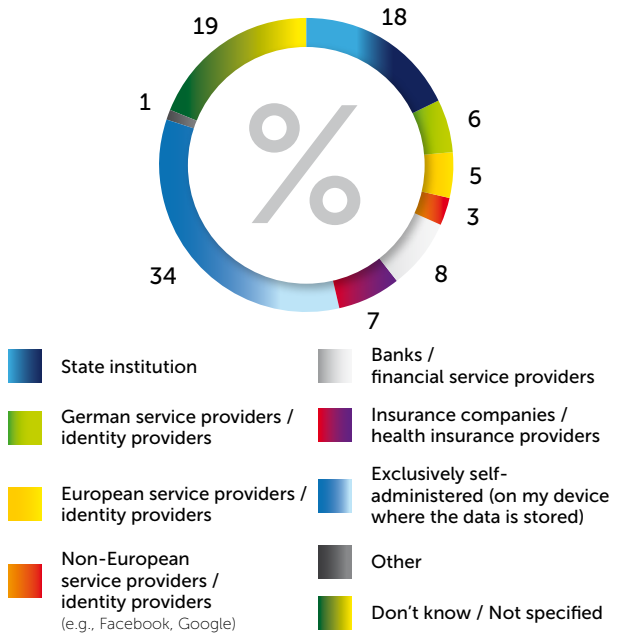
The central identities must also be administered by a central body in order to ensure that various services can be logged into with only one single account. In this context, "Made in Germany" enjoys the greatest trust from German companies. Of these companies, 25 per cent would entrust the management of identities exclusively to German identity providers. Just under a fifth of the companies would entrust the management to European identity providers. Overall, larger companies are much more open to European service providers than smaller companies. Nearly one-fifth of companies with 50 or more staff would choose a European service provider, but only four per cent of companies with fewer than 50 staff would do so. The ratio is similar for non-European providers. The larger the company, the more likely it is to consider a non-European service provider. For example, while 17 per cent of the large companies surveyed with 2,500 or more staff would opt for such a provider, no single company with fewer than 50 staff would be willing to do so.

Public authorities favour the state, citizens prefer self-administration

It is not particularly surprising to learn that public authorities prefer a state institution as the administrator of central digital identities. A total of 55 per cent of the authorities would delegate the management to a state institution, while 15 per cent favour German providers, and only five per cent would rely on European service providers.

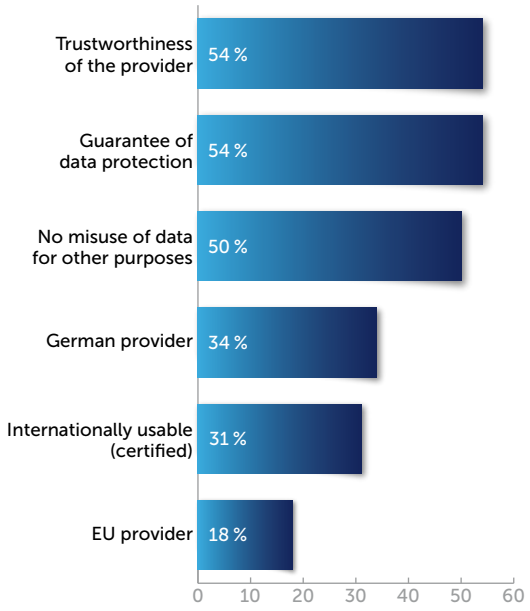
Citizens, on the other hand, prefer a self-administered solution. Just under a third of the citizens surveyed would prefer not to have the management of the central identity taken out of their own hands. Such a management would take place, for example, on the individual's own smartphone with the help of an app, such as the digital wallet. State institutions also enjoy a high level of trust. A full 18 per cent of the citizens surveyed would entrust the management of their identity to the state. In contrast, private service providers have a harder hurdle to overcome. Only six per cent would use a German service provider, five per cent a European service provider and three per cent a non-European service provider.

Trust in providers for the management of central (universal) digital identities – Citizens



Basis: 300 citizens

Grounds for selecting a provider to manage your central (universal) identity



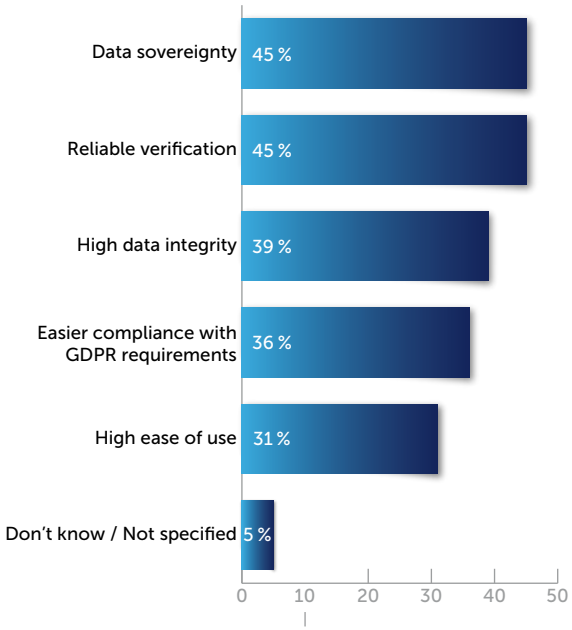
Basis: 170 companies (multiple answers)

Unanimity on the grounds for selecting service providers

The decisive aspects for the selection of the respective service providers are the trustworthiness of the providers (54 per cent), as well as the guarantee of data protection (54 per cent). With German and European providers, this is particularly the case due to strict data protection regulations. Another key factor is the certainty that the data will not be misused for other purposes (50 per cent).

When it comes to selecting a service provider, these three main grounds are also the three most important arguments on behalf of public authorities as well as citizens.

Grounds for selecting a provider to manage your central (universal) identity



Basis: 96 companies (multiple answers)

Self-sovereign identity management

A reasonably high proportion of respondents from companies (16 per cent), public administration bodies (20 per cent) and citizens (34 per cent) favour self-sovereign identity management.

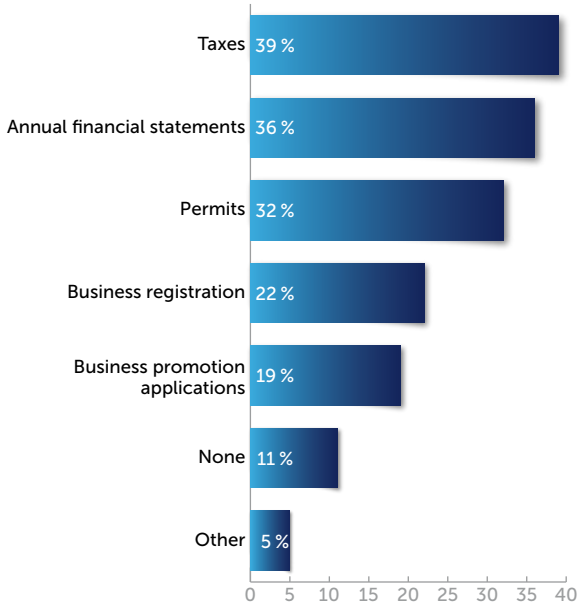
Self-sovereignty means that users can decide for themselves which applications receive their digital identity data, and when. Such a form of identity data management is called self-sovereign identity (SSI). This self-sovereign identity can be seen as much more user-friendly than the classic identity services administered by service providers or state institutions. The basic principle behind the SSI ecosystem is a triangle of trust. The stakeholders are as follows: the issuers of digital credentials – for example, companies or organisations that are in a position to issue such digital credentials; the verifiers of the digital credentials – for example, the application that uniquely verifies the digital credentials cryptographically; and the holders, who usually have the digital credentials securely stored on their mobile device with a corresponding SSI wallet – i.e., a kind of digital wallet.

More than half of the companies reported that they knew the term SSI and what it meant. On the part of the citizens, however, only just under one fifth said they had heard of a digital wallet. And only seven per cent of citizens have even used an ID wallet app. Considering the general wish for self-administered identities, it is surprising that so few people know which technologies make this possible. There is still a lot of potential here to increase awareness of this technology, given that citizens in particular have only rarely come into contact with the topic of SSI.

Independent management offers advantages not only for citizens, but companies also benefit from an SSI concept. For example, 45 per cent of companies name the retention of data sovereignty and the reliable verification of users as primary advantages of such an approach.

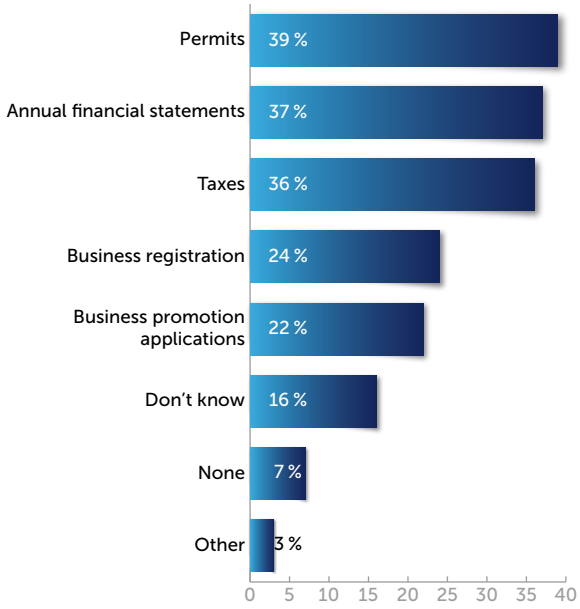
Independent management offers advantages not only for citizens, but companies also get to benefit from an SSI concept. For example, 45 per cent of companies name the retention of data sovereignty and the reliable verification of users as primary advantages of such an approach.

Use of e-government offers – **Companies**



Basis: 170 companies (multiple answers)

Desired e-government offers – **Companies**



Basis: 170 companies (multiple answers)

Classic Deployment Scenario: E-government

Multiple public authorities already offering digital services

A classic deployment scenario for identity-based services is the electronic processing of public authority services (e-government). These online services are available to both citizens and companies in various forms.

Large companies reticent

The services most frequently used by companies are those for submitting tax assessment notices (39 per cent) and for annual financial statements (36 per cent). In third place comes the digital request for permits (32 per cent). It is striking to note that those tending to use e-government services less frequently are, in particular, the large companies with more than 2,500 employees, as well as the very small companies with fewer than 50 employees. For example, only 17 per cent of large companies report that they conduct their annual financial statements electronically. In addition, one-fifth of the smallest companies say they have never used an e-government service, while for the largest companies, the figure is just 14 per cent. Approximately one out of ten of all companies have never used any e-government services.

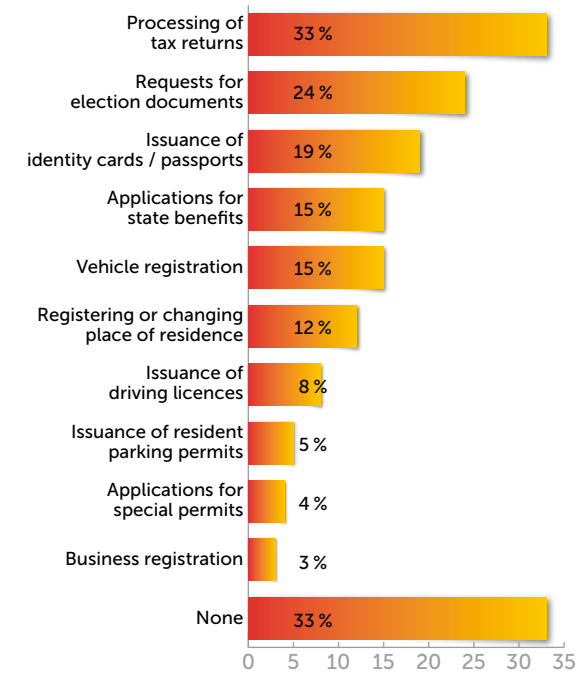
Looking at the statements on the question of which e-government services companies would like to use, it quickly becomes apparent that those services that are currently used most frequently are also at the top of the wish list. Above all, however, the possibility of electronic approval processes shows great potential. Four out of ten companies would like to see such a service in their municipality. What follows directly after that are the electronic processing of annual financial statements (36 per cent) and taxes (36 per cent). This also applies to the large companies that have not yet availed much of e-government services. Just under a third of the largest companies would like to have electronic services for handling their annual financial statements.

One third of citizens have never used e-government

Citizens are also the ones who most frequently use the existing electronic services of public authorities. At the top of the list is the digital processing of tax returns, with one third of the citizens surveyed already having used ELSTER (the German electronic tax declaration) to submit their income tax returns to the tax office.

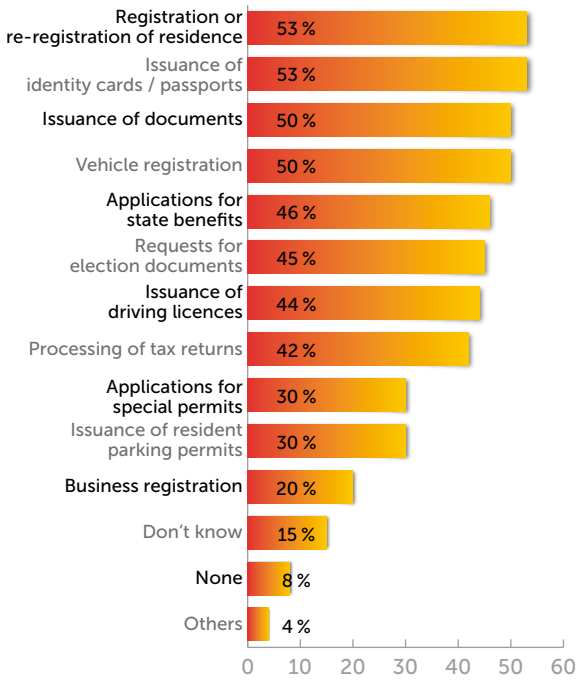
Already today, almost a quarter of citizens are postal voters and request their election documents digitally via the portal of their municipality. Rounding out the top three is the issuance of identity cards and passports (19 per cent). Nonetheless, one third of citizens state that they have not used any e-government services.

Use of e-government services – **Citizens**



Basis: 300 citizens (multiple answers)

Desired e-government services – **Citizens**



Basis: 300 citizens (multiple answers)

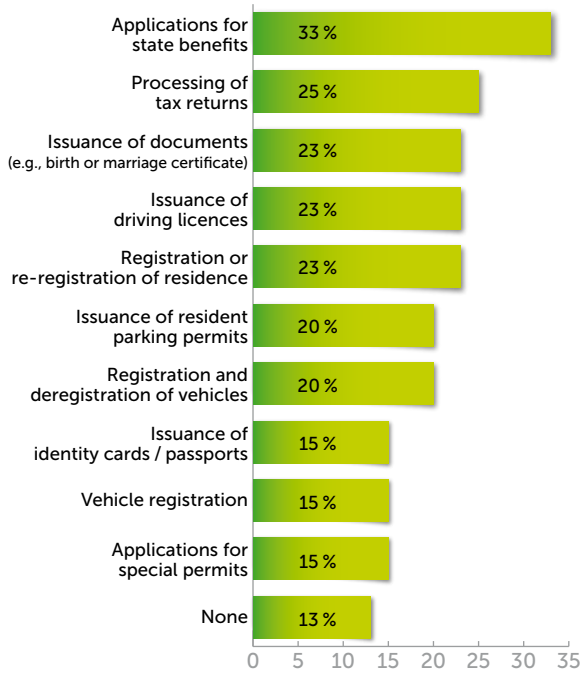
As is the case with companies, citizens also see great potential in services. The services with the highest values and thus at the top of the citizens' wish list are the issuance of identity cards and passports (53 per cent), the registration or re-registration of residence (53 per cent), as well as the services for issuance of general documents such as birth certificates (50 per cent) and vehicle registration (50 per cent). But almost all other possible services would also be highly accepted in principle.

Requested services for state benefits

The primary public administration services sought by companies and citizens are applications for state benefits (33 per cent). The next most popular services are tax returns (25 per cent), the electronic issuance of driving licences (23 per cent), registration or re-registration of residence (23 per cent), requests for election documents (23 per cent) and the issuance of general documents (23 per cent). Applications for state benefits offer the greatest potential, with 30 per cent of the public authorities keen to offer such services in the future. The Covid-19 pandemic in particular has highlighted the need to ensure the provision of state benefits, even in times of crisis. In order to be able to issue benefit applications for citizens and companies quickly, easily and without an on-location appointment, digital processes are therefore essential.

The potential for special permits is also high on the priority list. A quarter of the authorities would like to provide electronic services in this field.

E-government services in **public authorities**



Basis: 40 public administration bodies (multiple answers)

How do citizens and companies rate e-government?

Given all the potential that e-government services are seen to offer, the question arises as to why a considerable proportion (33 per cent) of citizens have not yet used any e-government services, while companies are far less likely (11 per cent) to have never used e-government services.

To answer this question, companies and citizens were asked to rate the e-government services in terms of the number of services available and their operability – because, ultimately, the range on offer must cover a broad spectrum of online services, and this range must be easy to use and clearly operable in order to quickly finalise processes without any major obstacles.

As it appears, the public authorities' online services which are available for companies are deemed to be appealing. Almost three quarters of the companies are satisfied with both the offer and the operability of the services and rate these as good to very good.

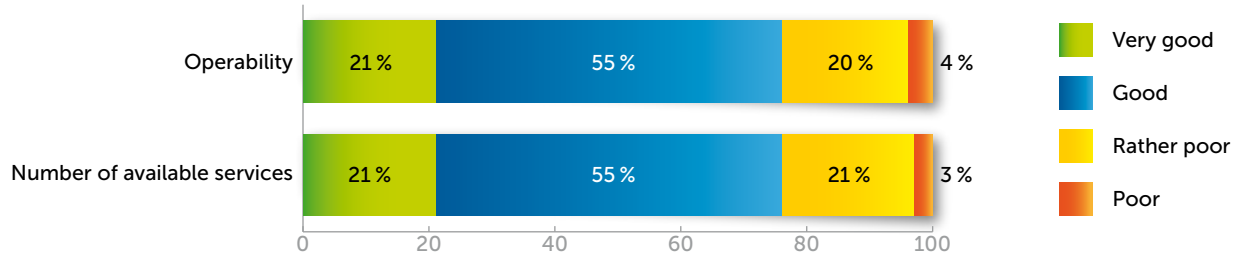
A slightly more critical view is taken by very small companies with less than 50 employees and by the very large companies with more than 2,500 employees. In each of these sectors, just over half of the companies surveyed are satisfied with the services available. This means that public authorities must augment their offer with services that can satisfy the special needs of companies of these sizes. Depending on the size of the company, special services or facilities are needed. Micro companies, for example, do not need the same services as large companies. With this in mind, in order to be able to offer suitable services to every company, collaborative work should be undertaken with the companies or business associations for services specifically tailored to the target groups.

Citizens give e-government a poor rating

Citizens are much more stringent than companies when it comes to rating the e-government services of their municipalities. Nearly 60 per cent of the citizens surveyed are not satisfied with the number of services available. One fifth of the citizens even consider the number of available services to be poor.

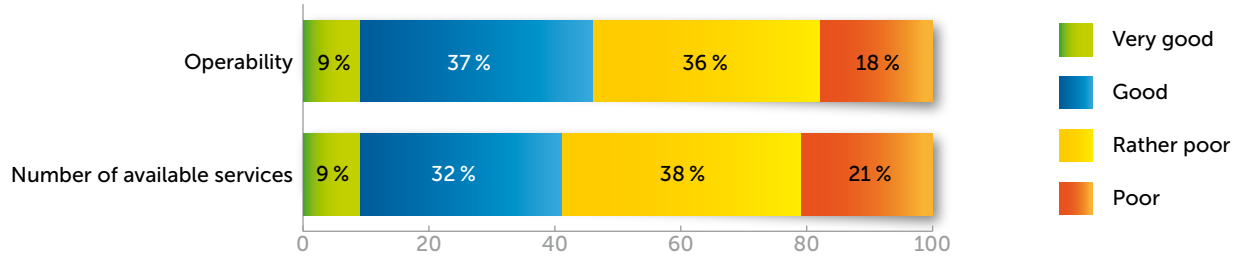
In addition, slightly more than half (54 per cent) of the citizens are not satisfied with the operability of the available services. In total, 18 per cent of respondents are even completely dissatisfied and regard the current operability of the offered e-government services as a major impediment.

Rating of e-government offers in terms of the number of available services and operability – **Companies**



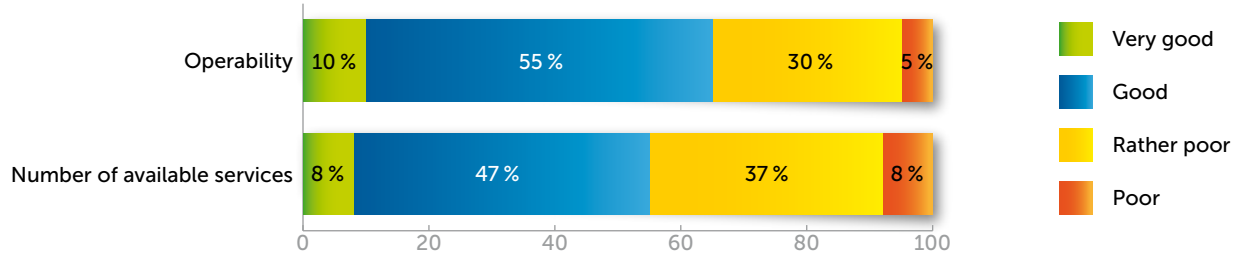
Basis: 170 companies

Rating of e-government offers in terms of the number of available services and operability – **Citizens**



Basis: 300 citizens

Rating of their own e-government offers in terms of the number of available services and operability by the **public authorities**



Basis: 40 public authorities

Public authorities see themselves as well positioned

Public authorities were also able to provide a self-assessment of the services they offer and the operability of these services. Overall, the public authorities see their own offers as good. In total, 55 per cent believe that the number of available services available are good or very good, while two thirds of public authorities are satisfied with the operability of these services. In comparing the authorities' satisfaction ratings with those of the citizens, it quickly becomes clear that there is a certain discrepancy between the authorities' assessment and how things really are. Citizens have much higher demands for operability than perceived by the public authorities. To merely be of the view that the services are "functioning" is not sufficient. For citizens, it is essential that public authority services also have the same level of convenience and simplicity that citizens are accustomed to in their daily private applications. This does not just apply to the desktop variant; in addition, simple operation via the smartphone, either as a native web application or as a separate app, must not be overlooked.

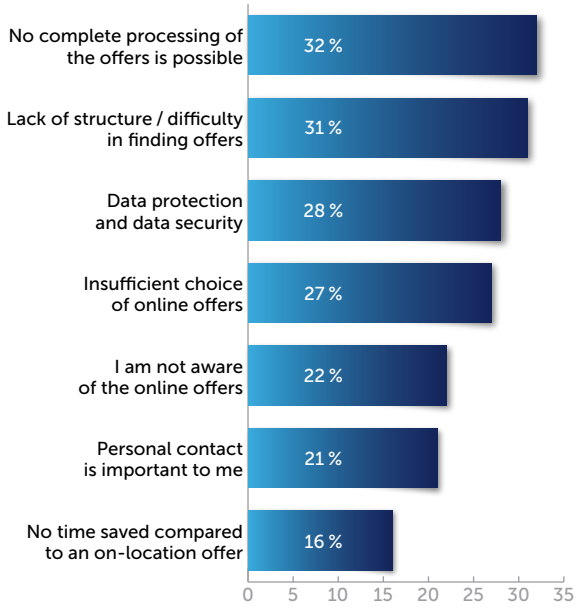
Obstacles to the use of public authority services

Companies and citizens were also asked to indicate which obstacles impede the use of public authorities' online services. In turn, the public authorities were also asked to assess why companies and citizens are either sometimes reticent in using their services or why they rarely use them.

For companies, the fact that processing via online offers is often inconsistent plays a major role (32 per cent) in impeding e-government services. This occurs, for example, when related subsections cannot be processed on a completely electronical basis and when subtasks must continue to be processed in paper form. To a similar degree, a lack of structure and the difficulty to find what is being offered are also aspects which hinder a greater use of these services. If a service is not easy to find and is hidden in complex submenus, this only creates frustration and stops the search for e-government services. The third factor is that of unresolved issues about data protection and data security (28 per cent) – because a service can only be used with no concern if there is a 100 per cent guarantee that the highly sensitive data transferred electronically is also secure and will not fall into the wrong hands.

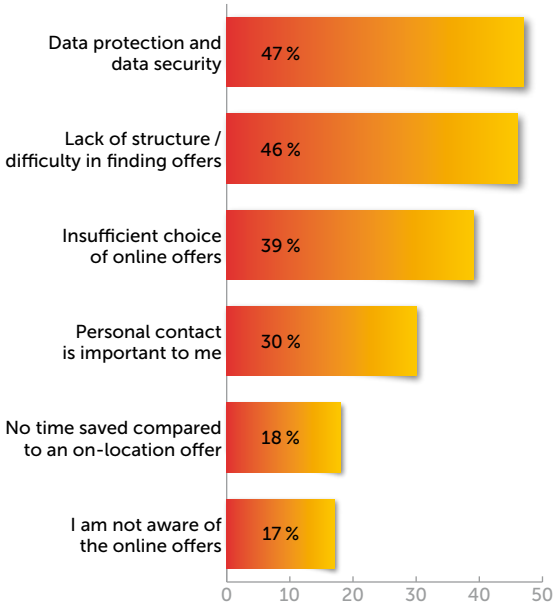
For citizens, unresolved issues relating to data protection and data security (47 per cent) play a major role in their lack of use of e-government services. Older citizens in particular tend to have a far higher degree of concern than younger citizens. As is the case with companies, a lack of structure and the difficulty to find what is being offered also stand in the way of citizens' use of public authorities' online services. Rounding off the top three obstacles in the use of e-government services is the insufficient choice for relevant services. Nearly 40 per cent of the citizens state that the choice of online services offered is not sufficient. This is also in line with citizens' general rating of e-government services.

Obstacles that hinder the use of public authorities' online services – **Companies**



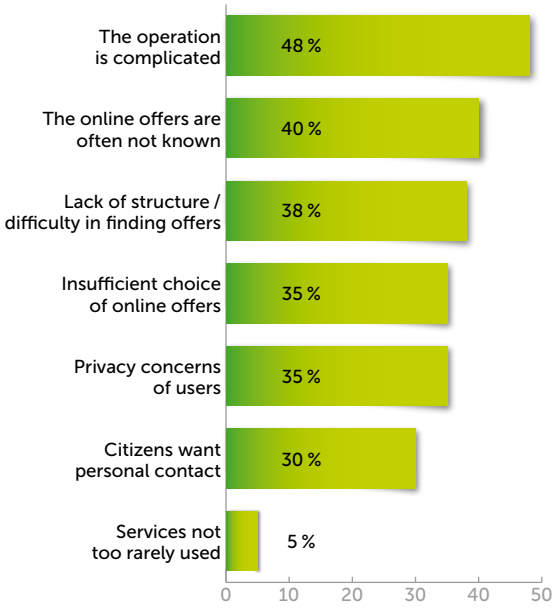
Basis: 170 companies (multiple responses)

Obstacles that hinder the use of public authorities' online services – **Citizens**



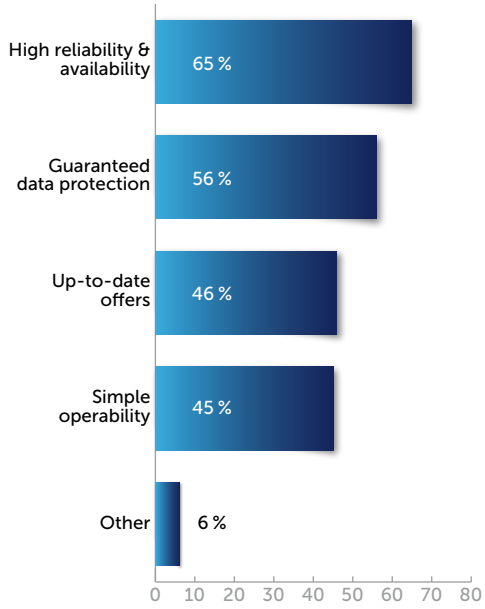
Basis: 300 citizens (multiple answers)

Reasons why e-government offers are used too rarely – from the perspective of the **public authorities**



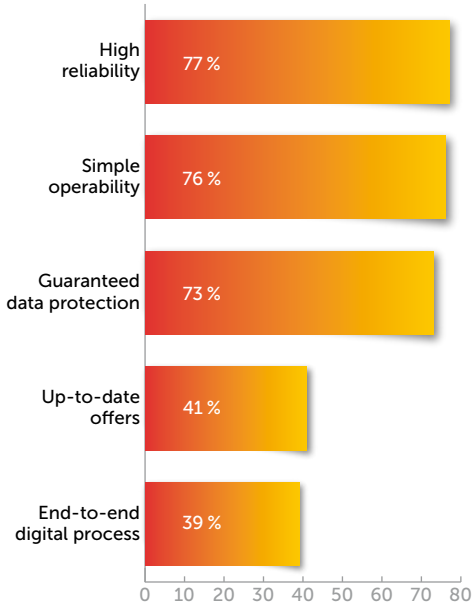
Basis: 40 public administration bodies (multiple answers)

Requirements for e-government offers –
Companies



Basis: 170 companies (multiple responses)

Requirements for e-government offers –
Citizens



Basis: 300 citizens (multiple answers)

The public authorities themselves, on the other hand, believe that their online services are mainly not availed of because their operability is deemed to be too complicated (48 per cent). This is somewhat at odds with the public authorities' own assessment that their services are generally easy to operate. In addition, 40 per cent of public authorities assume that there is a frequent lack of awareness of online offers. However, just under one-fifth of companies and citizens state that they are not aware of the online offers. In third place comes the difficulty in finding offers (38 per cent). The public authorities are thus aware that their services are often neither easy to find nor use. This is an area where work is urgently needed to improve the experience of both citizens and companies with e-services. Ultimately, it is clear that, in the current situation where services are not being used due to a lack of awareness, to their only being found in complicated and convoluted menus, or to their being difficult to use, any effort to provide these services has been practically ineffective.

E-government requirements

In order for e-government services to be widely used by companies and citizens, it is not only the obstacles to their use that must be overcome.

There are also other requirements to be met. For companies, the desire for high reliability and availability (65 per cent) of the services is at the top of the list. A service that repeatedly malfunctions or spits out error messages, for example, causes frustration among companies, deters them from following the online route, and reinstates the preference for a classic paper-based process.

In the second place, 56 per cent of companies highlight guaranteed data protection. As already seen in the previous section, questions of data protection and data security are obstacles to the use of e-government. For companies, it is of the utmost importance that the data exchanged via the online portal is also absolutely secure. A loss of data on the part of public authorities due to vulnerabilities can lead to absolutely sensitive and confidential data falling into the hands of criminals. For companies and public authorities, such a situation would be immensely damaging. Companies would also no longer place their trust in public authorities' online services.

For citizens, on the other hand, the situation is a little different. Like companies, more than three quarters of citizens consider the high reliability of services to be essential. Compared to companies, however, the operability of the services is also much more in focus. For example, 76 per cent of the citizens surveyed say that simple operability is a must in order to use e-government services. Having taken the citizens' criticism of the operability of online services into account, it is unsurprising to note the desire for simple operability. The user-first approach, which users are often already familiar with from e-commerce, is the de facto standard when it comes to rating the operability of an online service from the users' perspective. Complicated processes cost users a lot of time and patience and will result in the future continuation of paper-based work. Especially for older citizens, operability is an

important requirement. Whereas, for example, in the age group up to 49 years, slightly more than two-thirds consider operability to be an important factor, the figure among older citizens stands at approximately 90 per cent.

Conclusion

Companies, public authorities and citizens are all on the same page: Electronic services based on a secure single digital identity will be part of the future. Companies recognise the value of these digital identities for their future business success. The vast majority assume that services based on such identities will, at the very least, have a moderate impact on the future success of digital business models. And citizens also confirm this theory. Many citizens would use significantly more online services if this were possible with a single central digital identity. Currently, for different private and public authorities' services, citizens have to use many different digital identities that are based primarily on user names and passwords. In addition, depending on the field of deployment, processes such as Post-Ident, Video-Ident or the identity card with an online function are also required.

However, in order to be able to successfully use and offer services based on secure digital identities and thus strengthen their own competitiveness, both companies and public authorities must first recognise and take into account the concerns of users and address the many challenges that still exist. The willingness to use online services based on a secure digital identity will only increase if all obstacles are overcome. In particular, legal issues or a lack of know-how in the organisation for the implementation of a truly secure solution pose major challenges for companies and public authorities.

In order to counter the lack of skills, companies and public authorities need assistance on legal and technical topics and on the concrete implementation of identity-based online services. Moreover, it is not only the obstacles that have to be overcome; the high demands on structure, operability and reliability also have to be met. Ultimately, online services of a low standard will not end up being used.

Further Information

About techconsult GmbH

techconsult GmbH, founded in 1992, has a high ranking among the analyst firms in Central Europe. The strategy consultancy firm focuses primarily on the information and communication industry (ICT). Based on many years of both standard and individual analyses, techconsult has acquired a unique wealth of information in the German-speaking world, both in terms of continuity and depth of information. As such, it is an important consultancy partner for CXOs and for the IT industry in the spheres of product innovation, marketing strategies and sales development.

Contact for more information

Raphael Napieralski
Analyst
techconsult GmbH
Baunsbergstrasse 37
34131 Kassel, Germany
Email: raphael.napieralski@techconsult.de
Phone: +49-561-8109-181

Imprint

techconsult GmbH
Baunsbergstrasse 37
34131 Kassel, Germany
Email: info@techconsult.de
Phone: +49-561-8109-0
Fax: +49-561-8109-101
Web: www.techconsult.de

About eco – Association of the Internet Industry

With over 1,000 member companies, eco is the largest Association of the Internet industry in Europe. Since 1995, eco has been instrumental in shaping the Internet, promoting new technologies, creating framework conditions and representing the interests of its members vis-à-vis politicians and in international bodies. The reliability and strengthening of the digital infrastructure, IT security and trust as well as ethically oriented digitalisation are focal points of the association's work. eco is committed to a free, technology-neutral and high-performance Internet.

Contact persons

Markus Schaffrin
Head of Member Services
Email: markus.schaffrin@eco.de

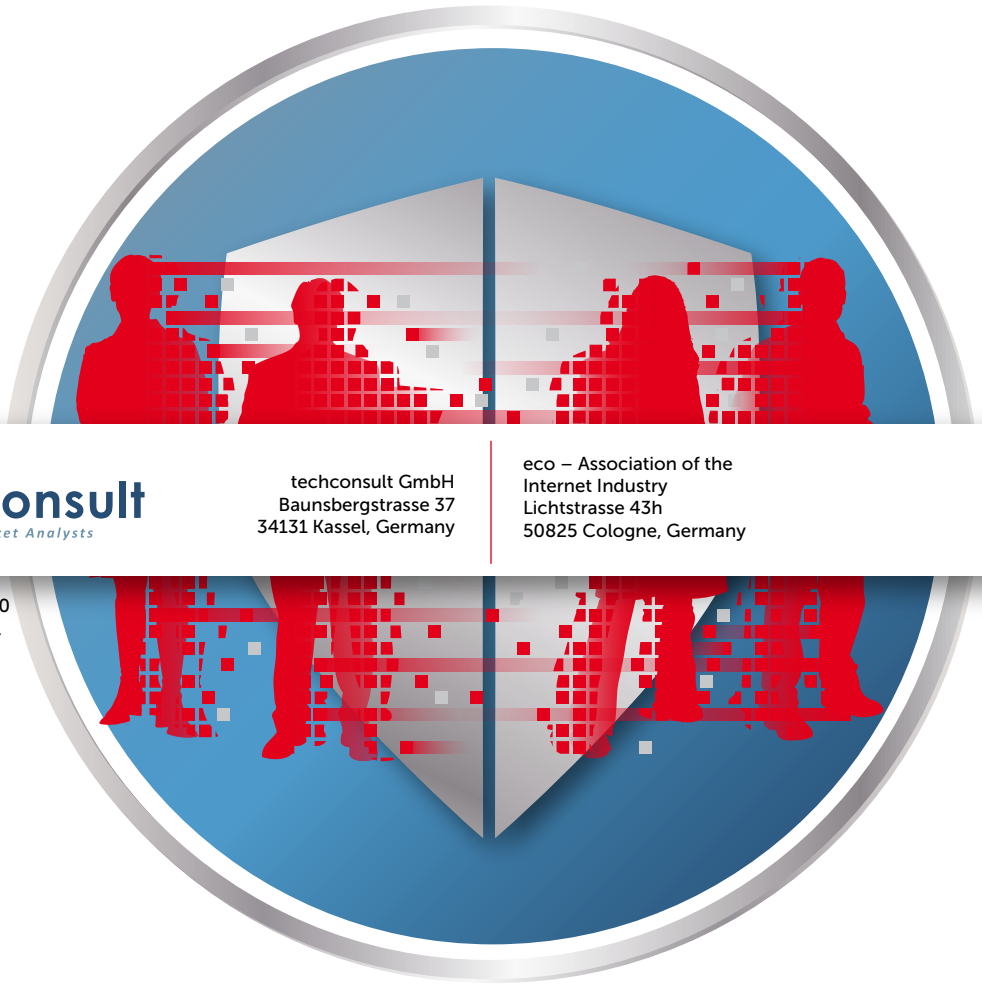
Tatjana Hein
Consultant / Project Manager Internet of Things and Mobility
Email: tatjana.hein@eco.de

Imprint

eco – Association of the Internet Industry
Lichtstrasse 43h
50825 Cologne, Germany
Phone: +49-221 – 7000 48 – 0
Fax: +49-221 – 7000 48 – 111
Email: info@eco.de
Web: https://international.eco.de

Harald A. Summa
Chief Executive Officer
Email: harald.summa@eco.de

Alexander Rabe
Managing Director
Email: alexander.rabe@eco.de



techconsult
The IT Market Analysts

techconsult GmbH
Baunsbergstrasse 37
34131 Kassel, Germany

Phone: +49-5 61 81 09-0
Fax: +49-5 61 81 09-101

info@techconsult.de
www.techconsult.de

eco – Association of the
Internet Industry
Lichtstrasse 43h
50825 Cologne, Germany

Phone: +49-221-70 00 48-0
Fax: +49-221-70 00 48-111

info@eco.de
international.eco.de

eco
ASSOCIATION OF THE INTERNET INDUSTRY