McKinsey
& Company

Public and Social Sector Practice

# How governments can deliver on the promise of digital ID

Governments globally are working to roll out digital identity schemes, but few have achieved broad adoption and utilization. To succeed, governments can create a virtuous circle of supply and demand.

*by Axel Domeyer, Michael McCarthy, Simon Pfeiffer, and Gundbert Scherf*

© mapodile/Getty Images

August 2020

**Digital ID provides** reliable authentication and enables delivery of a range of services via web or mobile applications that require proof of identity. It has the potential to generate significant economic and social benefits, including lower costs and increased financial, social, and political inclusion.[1] To date, governments around the world have launched around 165 digital, or partially digital, ID schemes. However, their track record is mixed. Only a few programs have achieved high levels of adoption, and use rates are often low, averaging just once or twice a year per person in some countries.[2]

To unlock the potential of digital ID, governments must work on two fronts—boosting both the supply and demand sides of the equation. On the supply side, this means delivering schemes that are technically and legally enabled for a broad range of applications. From a demand perspective, governments must ensure that schemes are accessible and are linked to the services that people most frequently use. They also need to guarantee a consistently positive user experience and engender a high level of trust.

## The significant potential of digital ID

ID systems collect and validate attributes to establish a person's identity and provide proof of that identity in the form of a credential—typically a physical ID card, passport, or driver's license. This can be used by identity-holders to prove their identity, for example to employers, financial institutions, or government agencies. Digital IDs are thus the digital counterpart to physical identification. A digital ID provides the credentials necessary to show that a person is who he or she claims to be online.[3] A digital ID's ability to simplify interactions between individuals, governments, and businesses can bring significant benefits.

*Individuals and government:* Digital ID is a key enabler for modernizing public services such as those related to healthcare, welfare payments, certifications, and licenses. It boosts convenience for users, eliminates potential travel costs, and minimizes waiting times by allowing remote online authentication. From a government perspective, the technology enhances administrative efficiency—reducing paperwork, speeding up processing, and reducing the risk of identity fraud. Beyond public services, digital ID can support citizen participation, for example through electronic voting.

*Individuals and business:* Digital ID supports consumers and businesses through benefits that include streamlined registration and authentication processes, secure digital payments, and digital

[1] For more, see "Digital identification: A key to inclusive growth," McKinsey Global Institute, April 17, 2019, on McKinsey.com.
[2] Identification for Development (ID4D) Global Dataset, World Bank Group, June 25, 2018, database.worldbank.org.
[3] *ID4D Practitioner's Guide,* World Bank Group working paper, number 137292, October 17, 2019, documents.worldbank.org.

A functional digital ID is a big step toward a digital society, in which individuals and organizations can trust each other online.

high-assurance contracting, for example through digital notary services. The technology is particularly useful for industries that collect significant amounts of customer data, such as financial services. It can also be a key enabler of simplified know-your-customer solutions.

*Government and business:* Digital ID can substantially streamline relations between governments and the private sector in areas including corporate registrations, taxes, economic support, permits, and authorizations. By enabling online interactions, the technology can lead to significant cost savings. Further, it supports regulatory compliance, providing fraud-secure paths for activities such as age and background checks.

A functional digital ID is a big step toward a digital society, in which individuals and organizations can trust each other online. Given the technology's sensitivity, governments should be in the lead on digital ID. Rather than outsourcing it entirely, for example to large tech companies, governments should consider retaining control over the framework on digital ID and involve the private sector within this framework.

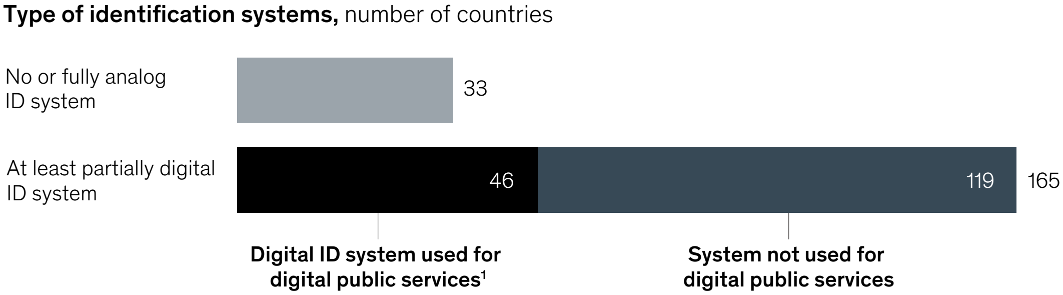
## Missing the mark

Many governments around the world have introduced ID systems that incorporate digital technology. However, only a few countries have managed to roll out the technology at scale, and only a minority of schemes have attracted a high number of compelling digital use cases.[4] Just 46 offer authentication for digital public services (Exhibit 1).

Governments have had mixed success getting citizens on board. While some countries, including Estonia, Denmark, and Sweden, have achieved almost universal adoption, others have signed up relatively few users (Exhibit 2). Take-up dynamics tend to be binary—schemes either achieve high levels of acceptance or get stuck in first gear. Levels of adoption are independent of the absolute number of eligible citizens; both New Zealand and Japan have struggled to achieve sign-ups at scale.

Exhibit 1

### Although the number of partially or fully digital ID systems is rising, few enable digital public services.



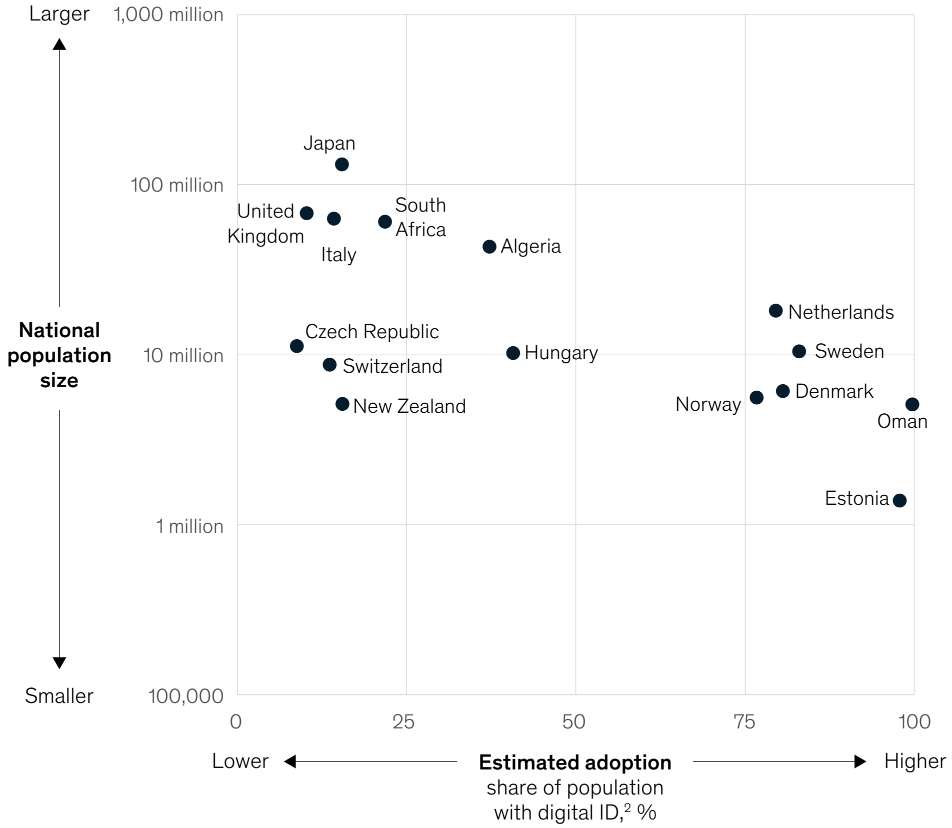
[1] Data as of April 2020.
Source: Identification for Development (ID4D) Global Dataset 2018; press research; McKinsey analysis

[4] "Digital identification," McKinsey Global Institute.

Exhibit 2

## Adoption rates vary widely across national boundaries.

**Population size of selected countries and estimated coverage of digital ID solutions,** by country[1]



[1] Selection of countries based on data availability.
[2] Estimation based on latest publicly available data.
Source: Identification for Development (ID4D) Global Dataset 2018; World Development Indicators; press research; McKinsey analysis

Data regarding utilization of digital ID schemes for public- and private-sector transactions is scarce, and a lack of consistent metrics prevents a comprehensive and exact like-for-like comparison. However, the data that is available indicates that ID schemes that fail to attract widespread adoption are used significantly less often on a per-user measure. Around the world, annual utilization rates range from less than one transaction per year to weekly or even daily transactions per user. Again, there seems to be little middle ground (Exhibit 3).

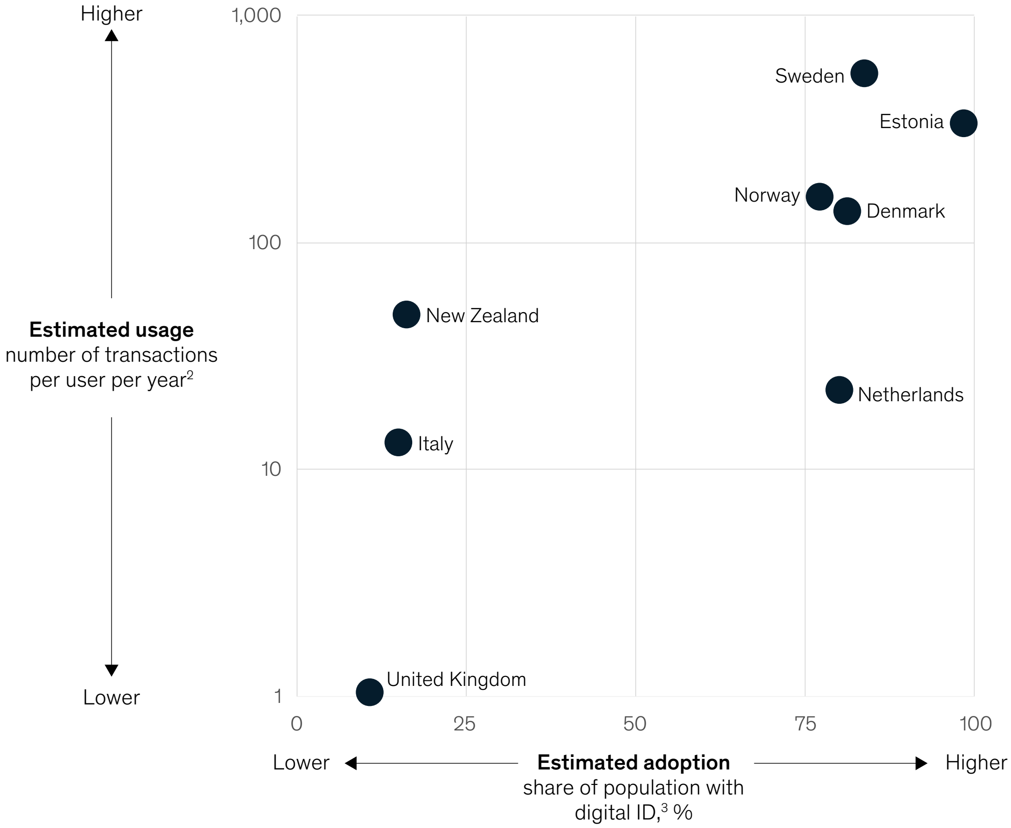
## Creating a virtuous cycle

The make-or-break characteristics of digital ID schemes are driven by an underlying circular dynamic. Successful schemes incentivize private and public service providers to integrate the

Exhibit 3

## Broad coverage is a precondition of high transaction rates.

**Estimated adoption rate and usage of selected digital ID solutions,** by country[1]



[1] Selection of countries based on data availability.
[2] Measured as number of transactions or service accesses divided by total user base; selection of countries based on data availability.
[3] Estimation based on latest publicly available data.
Source: Identification for Development (ID4D) Global Dataset 2018; World Development Indicators; press research; McKinsey analysis

technology, attracting users and, in turn, pulling in more service providers. Unsuccessful programs see the opposite dynamic. This binary state of affairs creates an imperative for governments to ensure systems are designed for success and are supported by adequate resources and incentives.

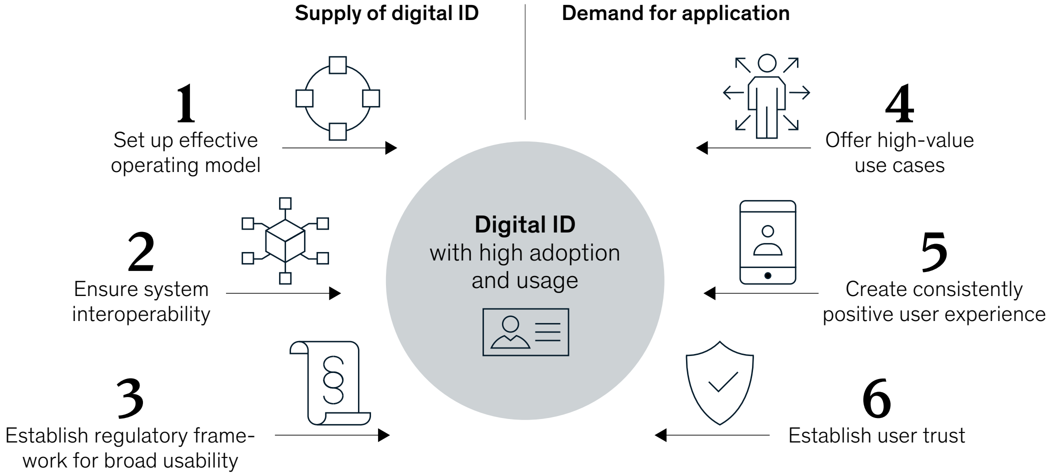
Two important preconditions for creating successful digital ID schemes are guaranteeing availability and fostering demand. Beneath these umbrella concepts are six critical steps (Exhibit 4).

### 1. Set up an effective operating model

Digital ID operations should be carefully managed from end to end, including user enrollment, authentication, and integration of service providers. An important early decision is whether to “make or buy.” The former sets up the scheme

Exhibit 4

## Six critical steps help guarantee supply and boost demand.


Supply of digital ID
Demand for application
1
Set up effective operating model
2
Ensure system interoperability
3
Establish regulatory framework for broad usability
Digital ID
with high adoption and usage
4
Offer high-value use cases
5
Create consistently positive user experience
6
Establish user trust

to be operated under a centralized model while the latter precipitates a federated structure.

In the centralized model, the government is accountable for collecting attributes, issuing digital credentials, and authenticating users. This requires the necessary technical and organizational capabilities for implementation and operation. In Estonia, which has successfully implemented a centralized model, the government has remained the sole provider since system launch in 2002, and it has achieved coverage of 99 percent of the population.[5]

In federated models, multiple accredited identity providers collect, store, and manage attributes and credentials and authenticate users. This approach is especially beneficial if there is a broad network of providers with substantial capabilities in identity proofing. Several successful implementations of this model harness the banking system: Denmark, Finland, Norway, and Sweden all run successful digital ID schemes in collaboration with banks.[6]

Federated schemes require prudent capacity management. Three of five commercial identity providers of British digital ID system GOV.UK Verify decided they would no longer issue new identities from March 2020.[7] When digital demand for benefits surged during the COVID-19 pandemic, the system's capacity was pushed to its limits, with virtual lines exceeding 150,000 users during peak periods. Thanks to the swift reaction of the Government Digital Service, which scaled up capacity and balanced traffic between the two remaining providers, queues disappeared after seven days.[8]

Factors influencing operating model choice could include existing digital ID infrastructure and its technical reliability and efficiency and citizens'

[5] "electronic ID," e-estonia, e-estonia.com; other successful implementations of the centralized model include India's Aadhaar program and DigiD in the Netherlands.
[6] Kim Catherin Kasch et al., *Federated e-IDs as a value driver in the banking sector based on experience from Nordic markets,* Signicat, April 4, 2019, resources.signicat.com.
[7] Sam Trendall, "What next for GOV.UK Verify?," Public Technology, May 15, 2020, publictechnology.net.
[8] Government Digital Service, "Scaling up GOV.UK Verify to help during coronavirus," blog entry by GDS digital identity team, May 11, 2020, gds.blog.gov.uk.

likely attitudes to private-sector involvement. Most importantly, governments should consider choosing a model that is likely to encourage rapid enrollment and that is built on infrastructure that will be sufficiently robust to handle rising user numbers and authentications. In either case, a firm political commitment is a precondition of success.

### 2. Ensure system interoperability

A digital identity is only as useful as the context in which it can be used. A key determinant is its level of interoperability—the ability of the ID system to exchange data with other systems, databases, devices, and applications. A priority for governments can be to ensure interoperability across private and public service providers domestically, as well as ID systems in other jurisdictions. The risk of not ensuring interoperability is that digital ID schemes lose momentum, leading to fragmentation as service providers build authentication tools compatible with their own needs.

Interoperability on the level of service provision is necessary to promote seamless integration with the systems and processes of service providers. In this way, users can, for example, both buy a personalized ticket for public transport and register a business with a local authority. Externally, some jurisdictions require interoperability by law. The most notable example is the EU's eIDAS Regulation, under which all organizations delivering public digital services within an EU member state must recognize electronic identification from other EU member states.[9] Compliance with these kinds of standards extends the range of applications in the context of activities such as travel, tourism, and immigration.

There are two critical steps to achieving a high level of interoperability. The first is committing to standards in accordance with international best practice. These can help ensure interoperability in respect of technology (for example, biometrics, cards, digital signatures) and data, meaning the structure of information collected and used by the system.[10] The second is implementing technologies enabling data transfer to and from other systems, including technical interoperability layers, web services, and application programming interfaces.

### 3. Establish a regulatory framework for broad usability

The challenge for legislators is creating a regulatory framework that permits a broad range of use cases across the public and private sectors, which is a precondition of widespread adoption by individuals and service providers. Governments, therefore, should consider putting in place the necessary rules to support use cases. Regulatory frameworks for the most advanced digital ID schemes, for example, in Estonia, make electronic authentication and signatures legally equivalent to face-to-face identification and handwritten signatures.[11] A priority in drafting legislation should be to avoid subverting these basic equivalencies. Often, laws governing delivery of specific services can have the effect of inhibiting utilization. Common examples include explicit in-person requirements, or the need to provide original documents that cannot be shared digitally, such as a visa or university diploma.

Governments must also address barriers that may arise from unintended effects of the requirements of the ID system and supranational regulation. In the UK's digital ID system, a duty on banks under the EU's Fourth Anti-Money Laundering Directive to keep a record of how they verified customers proved difficult to map over to the scheme and prevented take-up of the solution for financial services.[12] The issue was resolved in the EU's Fifth Anti-Money Laundering Directive.[13]

[9] "Trust services and electronic identification," European Commission, July 24, 2020, ec.europa.eu.

[10] Anita Mittal, *Catalog of digital standards for digital identification systems (English),* World Bank Group working paper, number 129743, September 1, 2018, documents.worldbank.org.

[11] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?,* first edition, Washington, DC: Center for Global Development, 2018.

[12] *Digital Identity in the UK: The cost of doing nothing,* Open Identity Exchange, April 19, 2018, oixuk.org.

[13] *Financial crime in focus,* "5th EU money laundering directive: Electronic identification using a trust scheme (eIDAS)," blog post, January 17, 2020, blogs.lexisnexis.com.

## A priority for governments can be to ensure interoperability across private and public service providers domestically, as well as ID systems in other jurisdictions.

The bottom line? Governments must act both to establish general equivalence and to amend legislation that may prevent or inhibit use cases in the private and public sectors.

**4. Offer high-value use cases**
Digital ID schemes must manifestly deliver value to their users. This is not necessarily straightforward, because many citizens have a low average number of touchpoints with the government—for example, only around five per year in Germany.[14]

The antidote is for governments to work to integrate as many public-sector use cases as possible and to focus on adding attractive private-sector use cases early on. A good place to start is the most frequent or cumbersome transactions from a user's perspective, such as transport ticketing and immigration protocols at airports and train stations. More complex use cases may require additional functionality such as electronic signatures or digital vaults for personal digital documents.

Governments should also consider offering incentives for uptake by private-sector service providers. Financial services entities are especially attractive given that people use them frequently. Many of the most successful schemes, particularly in Scandinavia, are delivered by banks. Around 91 percent of use cases of the Swedish BankID stem from the private sector.[15] There are numerous possibilities, including age verification, digital versions of licenses, and digital signing of business contracts.

**5. Create a consistently positive user experience**
People will only use products and services that meet their expectations in terms of experience, while providers will only integrate digital ID if it enhances the customer journey they wish to offer. Governments therefore can focus on creating a compelling user experience.

This process starts with enrollment, which should be intuitive, straightforward, convenient, affordable, and fast (see sidebar, "Improving the user experience for Germany's electronic ID card"). If these conditions are met, progress can be remarkable. By setting up approximately 50,000 enrollment points and offering flexible documentation requirements for registration, India successfully onboarded more than one billion people to its Aadhaar digital ID program. The government offered incentives for efficient enrollment by paying public- and private-sector entities for each successful registration.[16]

[14] "eGovernment MONITOR 2014 study: Use and acceptance of digital administration in an international comparison" ("Studie eGovernment MONITOR 2014: Nutzung und Akzeptanz von digitaler Verwaltung im internationalen Vergleich"), Kantar, September 24, 2014, kantartns.de.
[15] *Federated e-IDs as a value driver,* Signicat.
[16] *Identification revolution,* Center for Global Development.

In the authentication process, governments can work to ensure an intuitive interaction. This includes making low-security services accessible through pragmatic authentication methods. New Zealand's RealMe ID scheme requires just a username and password for many applications, such as interactions with city, district, and regional councils. For other needs, such as replacing a driver's license, it requires a more secure identity check, comprising an existing identity document such as a passport and a photo taken in a RealMe-accredited store.[17] Citizens holding a New Zealand passport issued after 2004 can access full remote identity verification. Australia also has a similar, tiered model, with degree of access depending on the number of identity documents provided by the user.[18] This approach of calibrating the authentication method to different levels of assurance can significantly boost the user experience and increase usage.

Several countries have taken steps to make the authentication process easier. Japan's digital ID scheme previously required users to acquire an additional card reader to use its smartcards. The government recently introduced an app that harnessed near-field communication technology. This enabled ID holders to use their smartphones in combination with their smartcards, rendering additional card readers unnecessary.[19]

Further simplification might comprise abandoning external smartcards and moving to an entirely mobile ID. These solutions can store a virtual token in the smartphone's SIM card, as used in Estonia's

[17] "Where to use RealMe," New Zealand Government, realme.govt.nz.
[18] "What can I use it for?," Australian Government, mygovid.gov.au.
[19] Mikey Campbell, "Japanese iPhone users will be able to access 'My Number Cards' via NFC this fall," Apple Insider, June 11, 2019, appleinsider.com.

## Improving the user experience for Germany's electronic ID card

**Germany introduced** an electronic ID card in 2010. Every new ID is shipped with a chip that stores a digital copy of personal information as well as biometric data.

The chip was implemented on every new ID, but users were required to opt in to unlock stored data and enable use of features such as digital authentication and e-signature. Opt in after initial issuance came with an additional fee, and the ID card had to be unlocked with a six-digit code, which was mailed separately. Similarly, the authentication process was complex. The few available digital public services could only be accessed with an additional card reader that cost at least €35. A certified reader required for the use of e-signatures was priced at up to €150.[1]

These barriers prevented adoption at scale. As of May 2019, nine years after the introduction of the eID, 63 million new cards had been issued, but just 40 percent were estimated to be unlocked for digital ID features.[2] In a 2019 survey, only 6 percent of participants said they had used the digital features at least once.[3]

Updates have encouraged more use cases and broader adoption. Since 2017, when a person receives a new ID card, digital features are always enabled. In addition, the chip can now be read via an app on most smartphones, obviating the need to purchase additional card readers. The government has also announced an initiative to implement a new technology that would allow users to store their digital IDs on mobile devices. This would eliminate the need to scan the physical ID card.[4]

[1] Anika Kreller, "Germany gets the Grünlich Card" ("Deutschland kriegt die Grünlich-Card"), *Der Spiegel,* October 27, 2010, spiegel.de.
[2] *Smart solutions for user-friendly digital administration (Smarte Lösungen für eine nutzerfreundliche digitale Verwaltung),* German Federal Ministry of the Interior, for Building and Home Affairs, Number 19-10540 (May 28, 2019).
[3] *eGovernment MONITOR 2019: Use and acceptance of digital administration offers - Germany, Austria and Switzerland in comparison (eGovernment MONITOR 2019: Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich),* Initiative 21 and Kantar, October 2019, initiatived21.de.
[4] *9-point plan for a digital Germany: Priorities of federal CIO Dr. Markus Richter (9-Punkte-Plan für ein digitales Deutschland: Schwerpunkte des Bundes-CIO Dr. Markus Richter),* German Federal Commission for Information Technology, July 2020, onlinezugangsgesetz.de.

Mobile-ID solution.[20] The German technology OPTIMOS, which is in development, aims to store a virtual token on smartphone hardware, making a change of SIM cards unnecessary.[21]

Finally, governments should consider ensuring a coherent look and feel in the authentication process across different service providers. This will help users become familiar with the process and encourage reuse.

### 6. Establish user trust

Users will not embrace digital ID schemes they do not trust. Growing public concern over data privacy and security, if unaddressed, presents a major barrier to adoption.  Even highly sophisticated schemes can fall victim to cybercrime or exposure of private data. For example, in Estonia in 2017, a security flaw in the chips of smartcard chips put 800,000 IDs at risk.[22] That experience helps illustrate that widespread adoption is likely to be contingent on governments winning user trust regarding security and transparency.

Governments can help do so by adopting a "privacy-by-design" approach, which establishes fundamental protections of privacy and data security. This approach could include carefully planning data collection, creating high standards for data storage to guard against intrusions, and mandating user consent for all personal data use. Further, storage can be distributed to avoid concentration of high-value information, with clear standards for all parties involved.[23] Legislation such as the EU's General Data Protection Regulation and the ISO/IEC 27701 guideline on security techniques provide essential guidance.

Finally, digital ID solutions can be designed to ensure transparency of information that is gathered and shared. One successful manifestation is Estonia's data-tracker tool, through which citizens can check data use across four major government registers.[24] They can review the identities of observers as well as the timing of—and the reason for—the access, with the exception of queries related to criminal behavior and national security.[25]

If governments can reliably supply digital ID and generate base demand among users and service providers, they can create a virtuous circle of adoption and participation. Given the numerous benefits of the technology, governments can get ahead of the curve by taking action now to deliver on the promise of digital ID.

[20] "e-identity," e-estonia, e-estonia.com.
[21] Matthias Punz, "A mobile e-ID for Germany" ("Eine mobile E-Identität für Deutschland)," *Tagesspiegel Background,* June 16, 2020, background.tagesspiegel.de.
[22] "What we learned from the e-card security risk?," e-estonia, May 2018, e-estonia.com.
[23] "Digital identification," McKinsey Global Institute.
[24] Federico Plantera, "Data tracker – tool that builds trust in institutions," e-estonia, September 2019, e-estonia.com.
[25] *Identification revolution,* Center for Global Development.

**Axel Domeyer** is an associate partner in McKinsey's Hamburg office, **Michael McCarthy** is an associate partner in the London office, and **Simon Pfeiffer** is a consultant in the Berlin office, where **Gundbert Scherf** is a partner.