Bundeskanzleramt

Digital identity

How an ecosystem can promote a self-sovereign and user-friendly approach to digital identity

Federal Chancellery
Digital State Division
March 2021

Contents

The lack of digital credentials is one of the most pressing obstacles facing the digital transformation at the present. This document sheds light on the importance of credentials for the digital world and, with this in mind, outlines the objectives and functioning of self-sovereign identity (SSI). It also sets out the vision for a European identity ecosystem. The establishment of this ecosystem is the objective of the European Digital Identity Initiative project, which the German Federal Government has established together with partners from the business community.

This document consists of the following sections:

1. An electronic “filing system” as an objective

Whenever we interact with others, we must disclose parts of our identity, be it our voice or appearance in conversations with friends or, when dealing with strangers, identity documents stating information such as our name, address and date of birth. Often, further proof of identity is important – for example, when applying for state support for studies (e.g. grants from the Federal Government (BAföG)) additional credentials are required to verify whether the applicant is enrolled at a university as well as their personal income or asset situation. It is frequently the case that several pages of credentials have to be attached to a one-page application form.

Requirements to submit credentials are ubiquitous – in both the public and private sectors. A lack of digital credentials is therefore one of the greatest obstacles facing the digital transformation at present. Those submitting applications online are often required to scan in credentials. The cumbersome digitisation of analogue credentials requires considerable effort, not only on the part of the holders of the credentials, but often also on the part of the document recipients due to poor machine readability.

Therefore, what we need is an electronic “filing system” – not just for members of the public, but also for companies, associations, public authorities and other institutions for whom interactions are increasingly taking place digitally. All of the above require credentials, for example regarding liquidity, tax payments and entries in public registers. The concept of an electronic “filing system” can be extended to include the likes of objects and machines, which can also be repositories of credentials, such as certificates.

But how can we create structures that ensure a particularly user-friendly issuance and transmission of digital credentials while simultaneously taking into account all relevant fields, such as technology, regulations, security, data protection and cost effectiveness? This is the challenge that the Federal Government, together with various commercial enterprises, is addressing with its initiative to establish an ecosystem of digital identities.

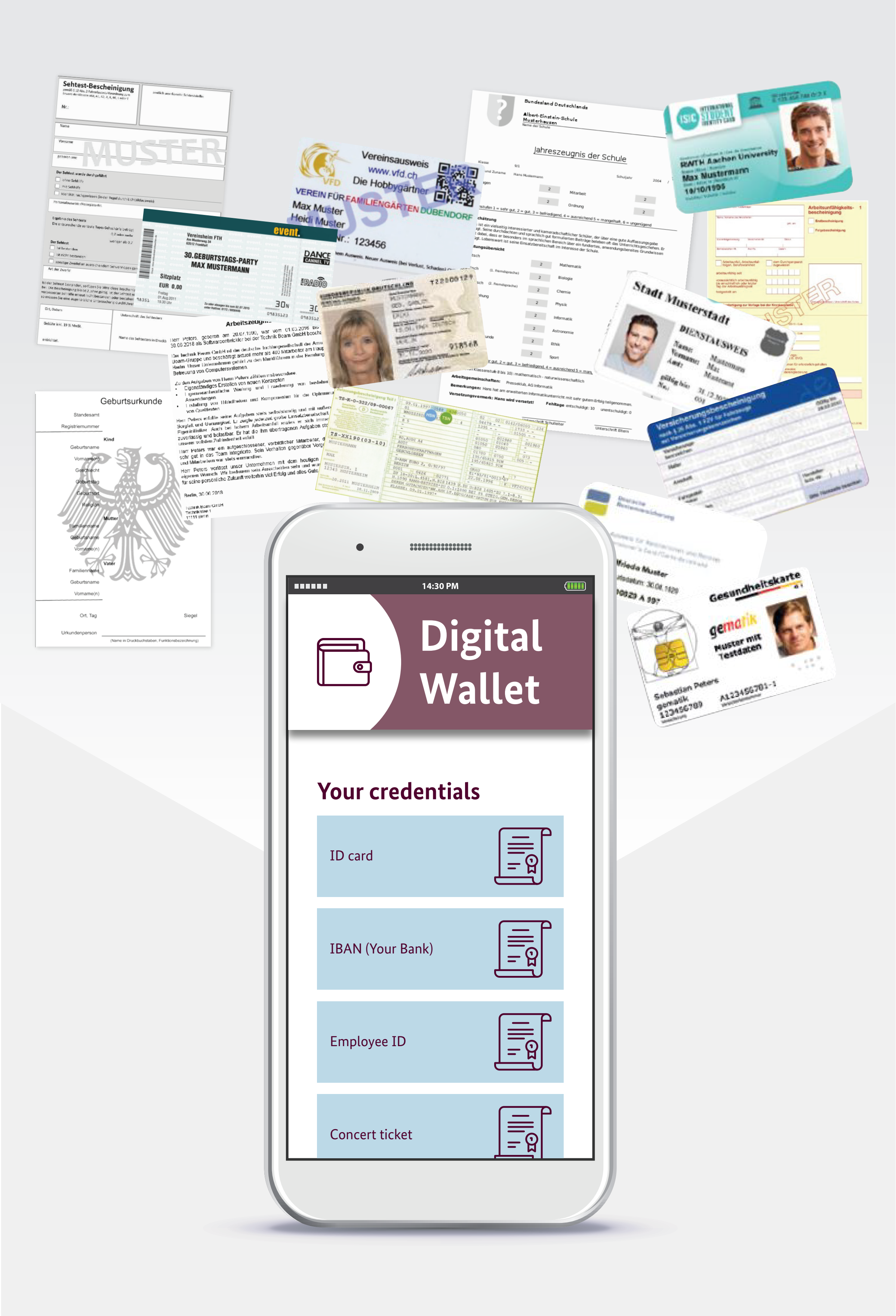
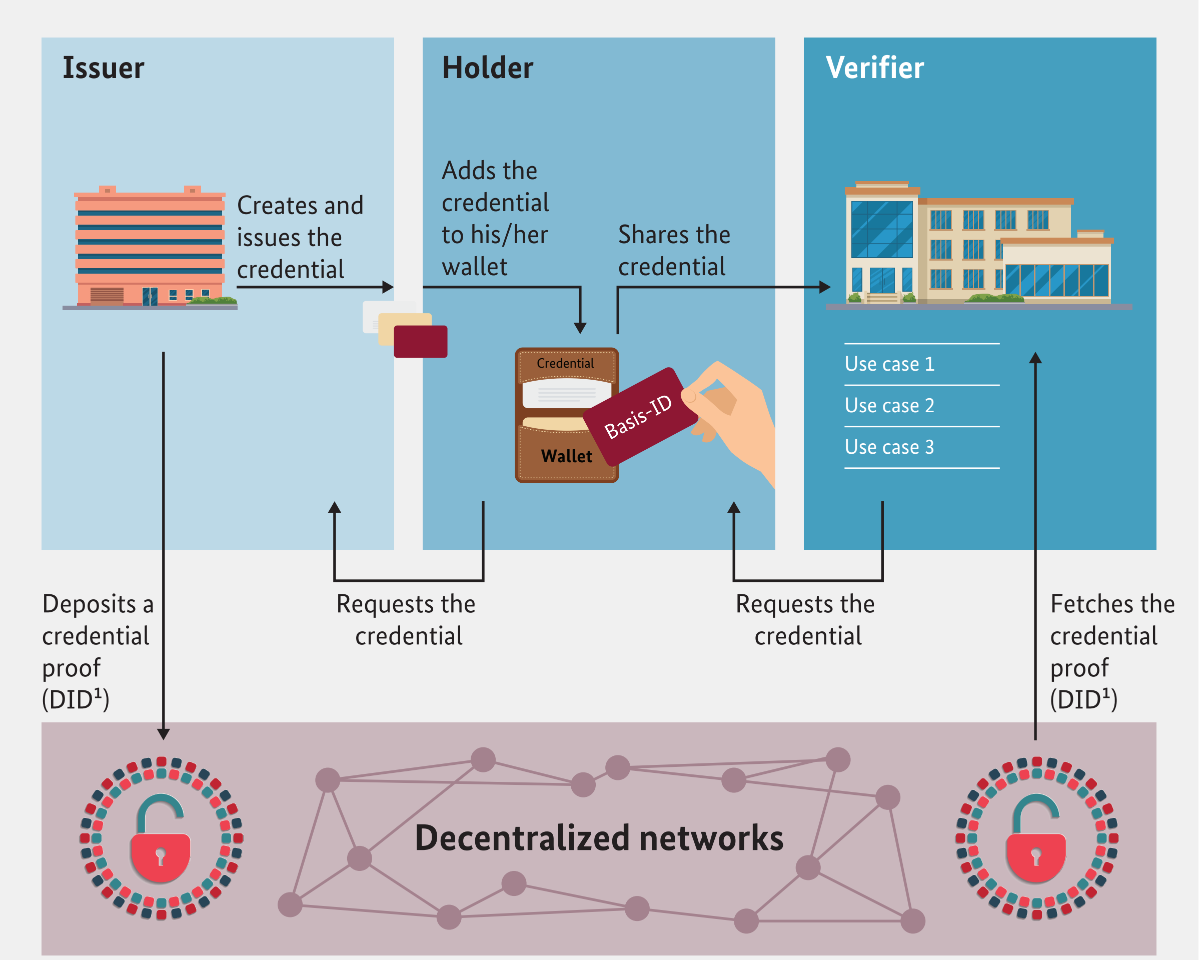


Figure 1

Digitising credentials

2. Self-sovereign administration and sharing credentials throughout Europe

A digital identity ecosystem should be based on the idea that people can manage all their credentials independently and share them in a self-sovereign manner depending on the context.



1 Decentralized identifier

Figure 2
The self-sovereign identity approach

To make this possible, issuers of credentials must first digitally transmit them to the people to whom they are issued, known as the holders. Holders, in turn, must be able to forward their credentials on a selective basis, depending on the context, to all parties who need them for a specific purpose, who are known as verifiers. An issuer should not know when and for what purpose a credential is used for by its holder. Why, for example, should a university know who graduates share their diplomas with? Since the verifier should not contact the issuer regarding the authenticity of a document, an additional component is required to ensure reliability. This component is usually conceived as a decentralised network and contains key information about the issuer. It is not necessary to store personal or retrievable data in the network.

This approach is being taken by various initiatives around the world and is known as self-sovereign identity (SSI). SSI has not only been outlined theoretically but is also quite advanced technically – a considerable spectrum of open-source components and commercial solutions are already available today.

In order for a digital identity ecosystem, based on the principles described above, to become particularly beneficial, it should be designed for broad-based, transnational use. Whether the services are used in the south or the north of the European Union should be just as irrelevant as the question which country we are in at the time of using the credentials. This creates considerable potential for members of the public as well as for Europe as a business location.

A study by the McKinsey Global Institute concludes that even developed economies with well-functioning identity solutions can increase their GDP by 3 to 4 percent[1]. We can therefore assume that Germany would also benefit from such potential. For the United States, this translates to an economic potential of almost USD 1,000 billion, and almost USD 100 billion for the United Kingdom.

In addition, a digital identity ecosystem provides the technical basis for the user-friendly implementation of European values, particularly with regard to data protection. For example, holders of credentials retain control over the documents issued to them at all times. This ecosystem can also support the Bologna Process by simplifying the submission of foreign study certificates to home universities. In many respects Europe's diverse nature is being complemented by a layer of technical interoperability that will promote the further convergence of Europe as a single market.

[1] McKinsey Global Institute, "Digital identification: A key to inclusive growth", 2019

3. The European Digital Identity Initiative

The Federal Government's objective is to establish an infrastructure that facilitates the secure exchange of identity information, is suitable for use throughout Europe and functions equally well for people, institutions and things.

The public sector and private companies need to work together to achieve this goal. On the one hand, the public sector issues important credentials, such as sovereign ID documents, while, on the other, businesses can draw on use cases that are particularly important in everyday life, such as logging in to customer accounts and digital vehicle access.

With this in mind, in 2021 the Federal Government, together with renowned partners from the business community, will implement up to ten use cases that are particularly important to citizens' everyday lives. To this end, in December 2020 the Federal Government launched a process together with 18 commercial enterprises to select use cases that are particularly beneficial and at the same time easy to implement. For the purpose of design and implementation, the initial group of 18 companies will be gradually expanded to ensure a consistent open-door policy for further domestic and foreign companies.

During the implementation, the Federal Government will make an implementation partner available for each use case from the second quarter of 2021 to create central infrastructure components. It is also committed to the gradual removal of regulatory barriers to ensure the legally sound use of the ecosystem, even in regulated areas. The commercial enterprises will, in turn, integrate the new solution into their business processes and ensure widespread use.

4. Use case 1: hotel check-in

In the first use case, the Federal Government will work with three hotel chains and four other companies to simplify check-in procedures for corporate travellers. The companies will provide their employees with a digital credential confirming their company's billing address. At the same time, the Bundesdruckerei will issue these employees with credentials based on their ID cards. With this identity information, the pilot participants can check in to hotels on business trips, simultaneously providing their private and their company's billing address for hotel bills.

Preparations for the implementation of the first use case began at the end of 2020 and actual development commenced in January 2021. The go-live for the minimum viable product (MVP) is scheduled for May 2021. By summer 2021, around 120 hotel locations in Germany should already be connected to this system.

In the hotel check in example, both proof of sovereign origin (attributes of the ID card) and proof of private origin (company address) are already required in the first use case. At the same time, a legal amendment to the Federal Act on Registration was initiated, which aims to enable the hotel registration form to be completed digitally based on the use case as part of an experimental clause.

As is evident, the first use case already promotes successful interaction between the state and the business community and also starts reducing regulatory barriers. In addition, the project will provide essential infrastructure components for further use cases and the development of the ecosystem.

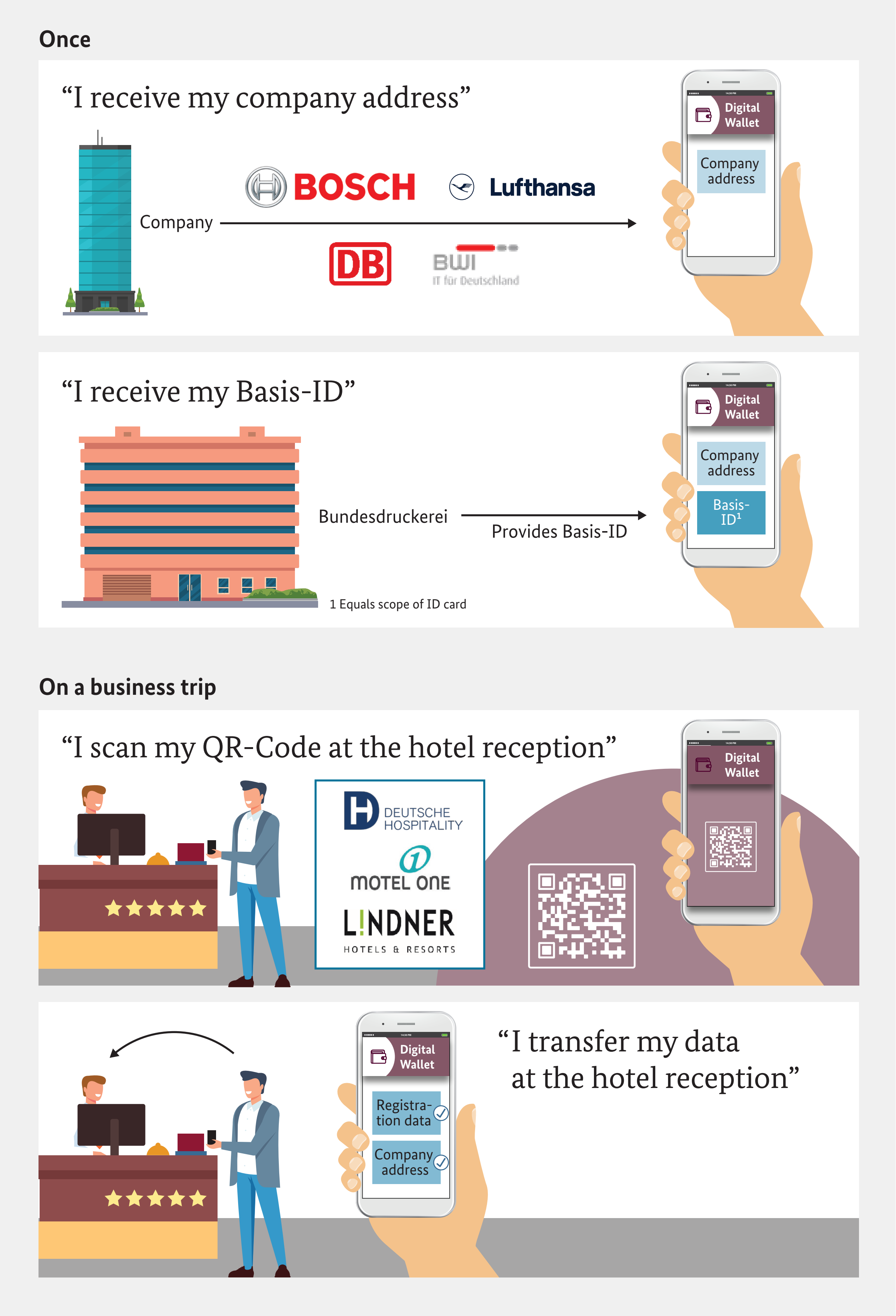


Figure 3
Hotel check-in use case

Use case at a glance:

Contracting authority:
the Federal Government

Participating hotels:
Deutsche Hospitality, Motel One GmbH, Lindner Hotels AG

Participating pilot companies:
BWI GmbH, Deutsche Bahn AG, Lufthansa AG, Robert Bosch GmbH

Commencement of preparations:
December 2020; Go-live: May 2021

Legislative amendment:
the Federal Act on Registration (“experimentation clause”)

Point of contact for the European Digital Identity Initiative project:

Federal Chancellery
Digital State Division
Willy-Brandt-Straße 1
10557 Berlin
Email: eid@bka.bund.de