

Basic information: eID Service

eID Service: The system behind the new German ID card

Since 1 November 2010, the new ID card has been issued in internationally standardised credit-card format. For the first time ever, citizens can use this ID card to clearly identify themselves on the Internet. The so-called eID Service, a complex and highly secure system, allows the data stored on the chip of the ID card to be read out. But to do this, the companies or public agency communicating with the citizen must first furnish proof of their identity. Bundesdruckerei not only produces the new ID card, it is also supplying a high-performance eID Service and authorisation certificates through D-TRUST, its accredited trust center.

What the partners need for online transactions

The central elements of the eID system architecture are the new ID card, a reading device, the AusweisApp software and so-called authorisation certificates. These elements are sensibly linked via an eID server which companies and public agencies can operate themselves according to the rules of the Federal Office for Information Security (BSI). Or, they can use the services of an eID Service provider like D-TRUST which provides such a service on behalf of Bundesdruckerei.

What the ID card holder needs

When requested, citizens can use the online ID function of their documents. The following is required in order to use the function for Internet transactions:

- The new German ID card: The online ID function of the ID document must be active.
- PIN: The card holder must authorise each data transmission using their six-digit PIN. Once citizens have applied for a new ID card, they first receive a PIN letter from Bundesdruckerei. This letter contains the five-digit transport PIN, the unblocking number (PUK) and a disable password. The card holder must immediately replace the transport PIN with a secret number of their own.
- Reader: BSI-approved readers are commercially available. These can be recognised by the circular green/blue logo of the new ID card printed on the device.

- Certificate: In order to use the qualified electronic signature (QES) of the ID card, the citizen will need a certificate. This certificate can be acquired from a Certification Service Provider (CSP).
- Driver software: The AusweisApp software makes it possible for the ID card and the computer to communicate with each other. It can be downloaded at: www.ausweisapp.bund.de.

What companies and public agencies need

In order to use the online ID function of the new ID card, companies and public agencies as service providers must meet with clearly defined requirements pursuant to Section 21 of the German ID Card Law (PAuswG) and furnish proof of this in writing.

- Authorisation: The issuing office for authorisation certificates (VfB), a unit of the Federal Office of Administration, demands that the service provider make a voluntary declaration concerning data protection. The service provider must also demonstrate to what extent the data which is to be read out is required for the service provided. The certificate issued by VfB is valid for a maximum period of three years.
- Authorisation certificates: Once authorisation has been granted, the company can sign an individual service provision agreement with a CSP: D-TRUST, Bundesdruckerei's trust center, is one such a CSP. The authorisation certificates are valid for a few days only and are automatically renewed on a regular basis. If there is any suspicion of data misuse, the certificates are no longer issued.
- eID server or eID Service: Together with the authorisation certificate, this is what makes it possible to read the data stored on the chip of the ID card.

How the eID Service works

The new ID card can make the following information available in digital form: family name, first name, doctoral degree, date and place of birth, address, type of document, service and card-specific ID (pseudonym), the abbreviation "D" for the Federal Republic of Germany, details of whether a certain age has been reached or not, details of whether a place of residence matches the place of residence requested, religious order or artistic name. In order to obtain access to the citizen's data, the service provider must identify himself during each transaction with his authorisation certificate. The citizen determines in each individual authorisation process which data he wishes to transmit to the service provider. The citizen then releases the data using his six-digit PIN or can refuse access completely.

In this context, there are two functions that are particularly interesting to citizens: the age-verification function and the pseudonym function. Age verification confirms whether the ID card holder has reached a certain age. The user's specific date of birth is not revealed. This information is relevant, for instance, when buying computer games over the Internet. The pseudonym function allows the citizen to communicate in social networks using the anonymous card ID of his new ID card and the pseudonym assigned to him.

What makes the eID Service interesting

Accredited certification service providers like D-TRUST, Bundesdruckerei's CSP, have extensive experience in the management of digital identities. They provide a powerful infrastructure for this purpose. The service provider does not have to set up his own eID server in order to enable his customers to use the online ID function or the qualified electronic signature (QES). This saves the service provider from having to invest heavily in the related system architecture. He can make use of Bundesdruckerei's eID Service which checks the latest ID card revocation lists during each transaction. The purpose of this is to prevent fraud using lost or stolen ID cards.