

# Austrian eID Strategy and Implementation

## A successful approach

by Prof. Dr. Reinhard Posch

The introduction and implementation of Austria's eID and eGovernment programmes proved a resounding success. An achievement that is not only attributable to the strength of the chosen strategy, but also to the stringent eID data protection requirements adopted by the Austrian authorities. As the modular and carefully designed structure of the eID programme can also be used to assign mandates and powers of attorney, further take-up is guaranteed.

One of the key factors behind Austria's success is the strategic approach adopted in 2001, at which time the country ranked 13th on the eGovernment benchmark conducted by the European Commission. During the ensuing period of two to three years, the authorities collected background as well as strategic information, and defined appropriate processes. A broad overview of the country's eGovernment framework was also drawn up. This outline allowed the main interfaces and standards required for the eGovernment application to be listed.

The implementation of the main eGovernment applications started in 2003. Since then, Austria has consistently moved up the European ranking: from 13th to 11th to 4th to 2nd to 1st (in 2006). A concerted effort was made to arrive at and implement a consolidated ICT strategy, which was given the name ICT 2005+ (figure 1). At the top level of this strategy is the coordination platform DIGITAL:AUSTRIA, which can be used by civil servants of all levels to discuss strategic issues and contribute solutions, which are subsequently embedded in conventions. The platform encourages and creates the homogeneity needed for the successful implementation of the eGovernment programme.

At a federal level, a federal ICT strategy unit was established, which is organised on the basis of three pillars. The first focuses on legal and organisational aspects in combination with international relations (insofar as these affect eGovernment). The second

covers the program and project management function for larger eGovernment projects, while the third deals with the ICT infrastructure within the Federal Chancellery. To sustain early successes, it was important that the platform - and, by association, the federal ICT strategy - be directly associated with the head of government. By implementing the above structure, Austria's consolidated ICT strategy responds to the need for ongoing innovation through the establishment of an eGovernment innovation and knowledge centre. To optimise the dissemination of information and awareness, the authorities also launched a public relations programme.

### Why introduce eID?

One of the key technologies driving eGovernment solutions is electronic identification on the basis of (i) specific data protection rules and (ii) a technological framework that can be used throughout the public sector while facilitating interoperability with European Member States.

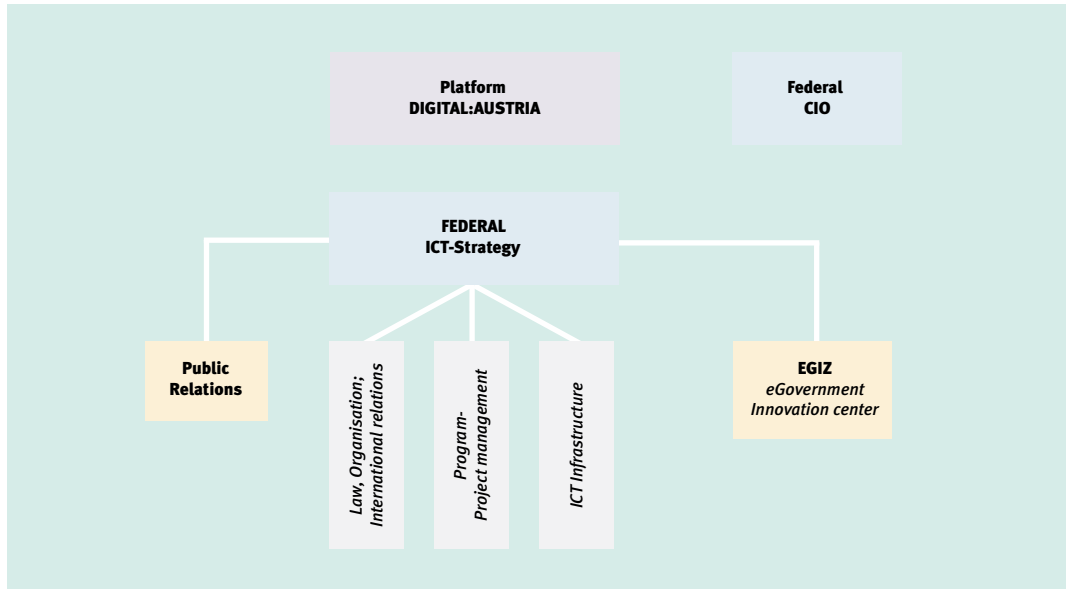
There are several ways to identify users of eGovernment applications. While it is reasonable to assume that a user-ID/password combination is the easiest and most cost effective solution to implement, experience<sup>1</sup> has shown that the initial costs and maintenance expenses are very high compared to other identification solutions. Costs are typically attributable to the enrolment process, which will, at the very least, involve the use of an established system to dispatch passwords. The resultant costs amount to approximately € 10 per person. A further complication is that user IDs and passwords may be forgotten if they are not used regularly. Think, for example, of the password one might use to file an electronic tax return. Although exact numbers are difficult to estimate, up to 80% of those who lose their password may need to be re-enrolled. Reason enough for the Austrian authorities to use electronic signatures based on smartcards or other tokens used by citizens to access a variety of applications and/or obtain a diversity of services.

Costs are not the only consideration, however. As it turned out, the need to protect data is the most significant and potentially the most restrictive factor. As a consequence, the Austrian authorities opted for an unambiguous solution that prioritises data protection and identifies users on the basis of data maintained in the Central Register of Residents (CRR). Throughout the



**Prof. Dr. Reinhard Posch** has been Chief Information Officer (CIO) for the Austrian Government since 2001. He is responsible for the strategic coordination in the field of information and communications technology and heads the Austrian eGovernment platform "DIGITAL:AUSTRIA". Reinhard is also head of the Institute for Applied Information Processing and Communications at the Graz University of Technology, where he holds a professorship. Reinhard has been scientific director of the Austrian Security Information Technology Centre (A-SIT) since 1999.

**Figure 1**  
Overview of ICT strategy  
'ICT 2005+'.



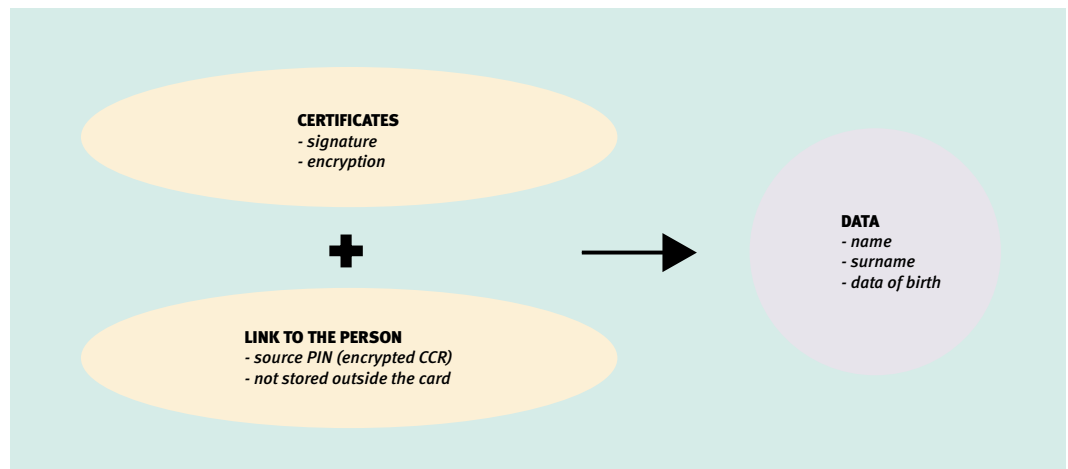
identification process, strong cryptographic algorithms are used. In addition, use is made of identifiers that are derived from a person's main identifier (source PIN). This approach also enables private sector entities to be involved in the process. As far as the use of electronic signatures is concerned, the Austrian approach relies on private sector certification authorities as well as tokens issued by, for example, banks and healthcare providers. To safeguard data protection, the key identifier is not stored in the certificate. Instead, it is stored in a signed record, and linked to the signature of the issuing authority and the serial number and/or public key of the certificate in question. This approach implies that a user can have several eID tokens.

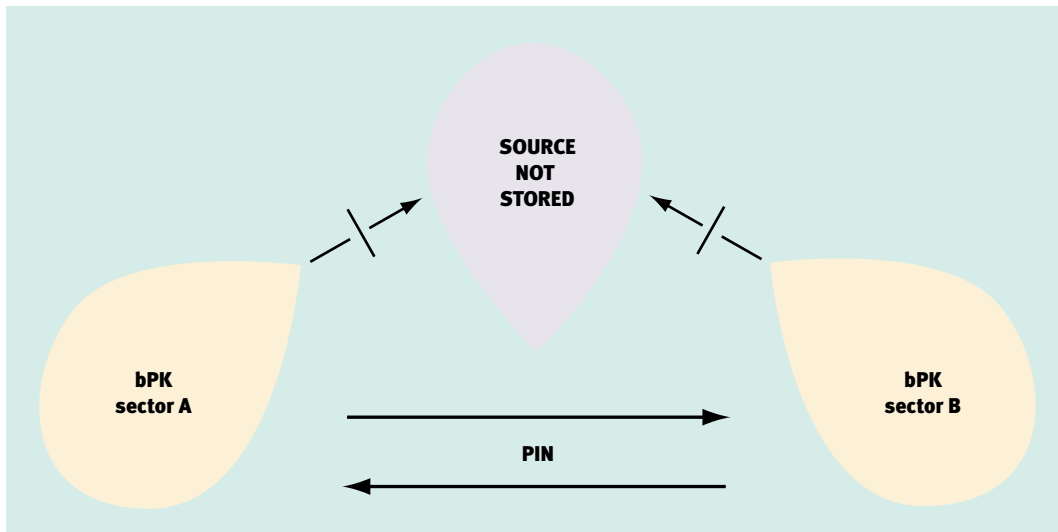
**How is the protection of Austria's citizens managed?**

The data on the eID token is uncomplicated and consists only of a name, a surname and a date of birth. All data is stored in a form, allowing it to be

used for the purposes of automated form population. Electronic signatures are stored in different certificates, including the certificate assigned to a person as well as certificates for encryption (used to transmit sensitive data, for example). A well defined XML record containing the data from the eID token is combined with the source PIN (the encrypted CRR number). The resultant record is signed by the competent authority, which, in combination with the signature of the person whose identity is transmitted, provides for a strong means of authentication (figure 2). To make sure that data is well protected, the authorities have adopted the following security principle: "do not add unnecessary risk to eID and automation". This protection principle allows the source PIN to be transformed to a sector specific PIN through the use of a one-way hash function. In other words, social security applications have a very different local identifier than, for example, tax applications. It is mathematically impossible to derive one identifier from the other. The only way to

**Figure 2**  
Citizen protection management.





**Figure 3**  
Only intersectoral communication is possible via the 'sector PIN' (bPK).

obtain the derived PIN is via the source PIN, which is not stored in or by any application (and therefore unavailable).

As indicated, the highly encrypted source PIN is derived from a citizen's CRR number. This approach circumvents the need to establish a separate register. The entire registration process may be based on data in the CRR. As the eID is inextricably linked to the electronic signature, data relating to directories and revocations need not be kept at eID level. The directories do not reveal any eID data, even if they are freely accessible. Instead, they only contain data relating to the signature certificate. They cannot, therefore, be linked to a person.

As far as citizen cards<sup>2</sup> are concerned, the following are required:

- an appropriate signature, based on a qualified certificate from any recognised country;
- the source PIN, which is generated via the CRR on behalf of the Source Pin Authority;
- the signature and source PIN are combined in an XML structure, which is signed by eGovernment authority in charge of eID-management.

### The use of eID in Austria

Austrians using the eID are identified by means of signature verification and authentication. It is also encryption for example in the case of delivery of electronic documents. As the only data on the card relates to the holder's name and date of birth, the scope for data misuse is about the same as it is for a bank card.

The Austrian eID is as secure as the signature it contains. Secure authentication means the bearer is able to sign a record presented by any government online service. The latter could, for example, present an

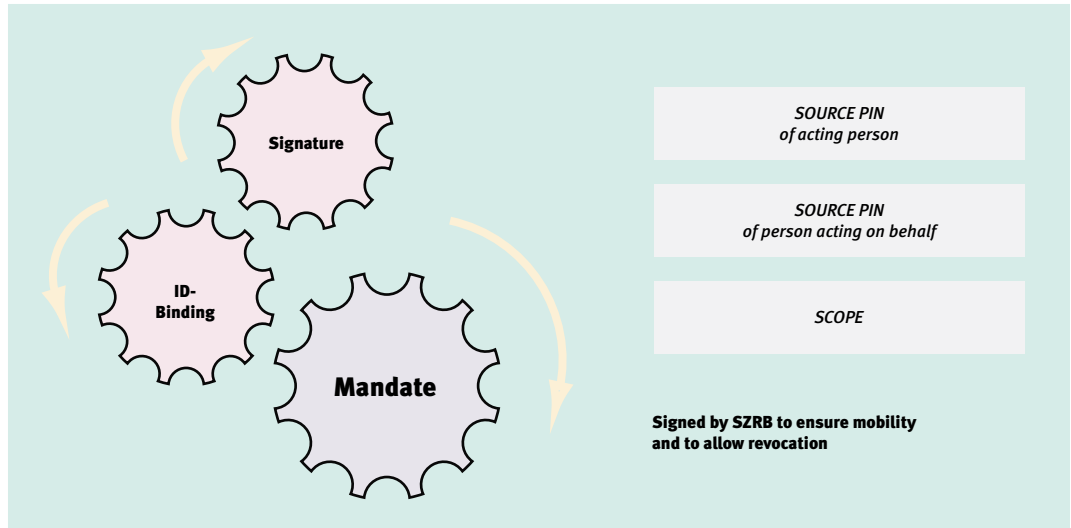
eID record containing the following information: today is January 13, 2007; I am John Smith and I would like to access application XYZ. John Smith would subsequently sign the record, proving his identity and authenticating the 'transaction'.

Linking security to the open use of electronic signatures allows new mechanisms, new electronic signatures and new technologies to be used. Apart from submitting electronic tax returns (the example given above), eID can be used to (i) access electronic files and administrative systems maintained by federal ministries and (ii) 'spot' citizens with a criminal record. One of the most significant applications for eID is electronic delivery, however. As of March 2007, electronic delivery is not only available to natural persons, but also to companies and other entities.

### Communication among back-offices

As long as different applications fall within the same sector, such as taxation or social security, direct communication can occur via the 'sector PIN' (bPK) - see figure 3. Communication between sectors can only take place via the Source Pin Authority (with the help of the CRR), which can provide the PIN of a different sector. This way, communication between sectors is well documented, minimising the likelihood of misuse. All data that is communicated is strongly encrypted, and therefore of no use to anyone who intercepts it. Moreover, the encryption of sector specific PINs is never the same, even if the sector and the person are. As communication between sectors requires the cooperation of the CRR, applications that do store name-related data cannot communicate with other sectors (the CRR requires a name and a birth date). This could be resolved by establishing a separate database. Think, for example, of a register for disease management - any new data in the register can be automatically aligned with the database. However,

**Figure 4**  
The chain of binding record, electronic signature and authorized mandate.



no data can be retrieved from the register unless the individual - and therefore the 'sector PIN' - is available.

### Mandates

For non-natural persons, the management of mandates is crucial. These mandates include all sorts of eID and electronic signatures in the course of an electronic government service. As is the case in the paper world, non-natural persons cannot per se act before any authority. Instead, you need someone to act on behalf of a non-natural person like a company or an association. The Austrian eID programme was primarily designed to be simple. The use of electronic signatures (available to the private sector) in combination with a simple record containing the eID of the person acting and the person acting on behalf as well as the purpose, signed by the authority makes it very easy to mandate another party (both among natural persons and between a non-natural and a natural person)- see figure 4..

The above adds another element to the chain of binding records and electronic signatures in the form of a binding record between person A (the identifier of person A) and the identifier of person B, acting on behalf of person A.

### The European dimension

Under the i2010 program, all European Member States are asked to implement electronic identification and eID management. Clearly, interoperability among different eID programmes is essential. Although several bodies are working on a standard for European citizen cards, the day when Member States use a system that can profit from a standard that permits interoperability among existing and upcoming technologies is still a long way off. The shift from contact to non-contact tokens might complicate matters further. The Austrian system offers two advantages that should facilitate

interoperability with other systems. First, the Austrian system is capable of interfacing with any signature-based eID system. To use eIDs from other Member States, the Austrian authorities only require the record linking the register to the signature. This requires the register to be extended, allowing non-residents to be entered also. The requisite framework will have to be studied in collaboration with other Member States. Second, the Austrian eID system is based on high data protection standards. By treating another Member State as a separate sector, the data submitted by the Member State is subjected to the same, high level of (data) protection prevailing within Austria.

### To sum up

The Austrian eID programme includes all elements needed to identify (and manage the identity of) individuals as well as companies. In addition, it facilitates the issuance of mandates amongst natural and between natural and non-natural persons. At a European level, interoperability will require further large-scale testing. Its present system allows the Austrian authorities to meet the interoperability demands of other Member States while simultaneously enabling it to receive and process the eID data submitted by these Member States.

*1 Think of online banking applications.*

*2 Such a card could consist of a mobile phone, for example.*