Identification in E-Government

Herbert Leitold
A-SIT, Secure Information Technology Center, Austria

Reinhard Posch
Federal Chief Information Officer, Austria

INTRODUCTION

Official procedures usually require that the citizen is unmistakably identified. This may be needed to ensure that the person approaching the authority is the one that has filed an application such as tracking the status of a request, for exercising certain rights such as representing a company or being a party in a proceeding, or for ensuring that the person is eligible to receive certain information such as her penal record. We define identification as the process necessary to validate or recognize identity.

In addition to identification, authenticity of a declaration of intent or act is needed in order to establish assurance of the purported identity. In conventional paper-based processes with personal appearance identification is usually carried out using identity cards, deeds, or witnesses. Authentication is provided by handwritten signatures.

When in e-government official processes are carried out electronically, both identification and authentication remain important aspects and need to be supported electronically. This may be provided by introducing electronic substitutes of paper-based official documents and handwritten signatures. At first glance, electronic signatures, digital certificates, and public key infrastructure (PKI) are such means. The legal basis for electronic signatures exists, for example, at the E.U. level (Signature Directive, 1999) or by national signature laws such as (Signature Law, 2000).

However, some issues need to be considered when introducing identification models for e-government on the regional or national level. These issues include scalability, durability, sustainability, and last but not least data protection and privacy. In this article we discuss these issues on identification in e-government. Therefore, the requirements on identification are sketched in section "Requirements of an Identification Model." Section "Identification vs. Electronic Signatures" continues by highlighting what shortcomings an identification model solely relying on electronic signatures and PKI faces. Section "Approaches to Electronic Identification" gives an overview of what solutions have been proposed and section "Fragmented Identifiers to Preserve Privacy" deepens one approach by introducing the model that has been followed by Austria (E-Government Act, 2004).

REQUIREMENTS OF AN IDENTIFICATION MODEL

When introducing an identification model for e-government usually a number of considerations are being made. Irrespective of whether the identification model is being introduced on a national, regional or municipality level, unique identities shall be supported as this is needed by many official processes. The model also should support permanent, preferably lifelong identifiers that resist changes of names and so forth. This ensures that a citizen can be identified within a certain process irrespective when the identification is needed. Land registers are an obvious example where identification may be needed for quite a while.

In particular on the large scale, establishing the identity based on features such as name and date of birth is not sufficient, as widespread names may lead to digital twins. Thus, scalability is a further issue. Related to scalability, an aspect that shall not be underestimated is that systems that work well with early adopters that usually are technology-educated may turn out to not scale when the technology is taken up generally. An example—aside from security considerations—are usernames and passwords that tend to become costly on the large scale, as forgotten passwords and helpdesk costs become an issue. This particularly holds for e-government, as most citizens have official business rarely—in many cases once a year or less.

When obtaining an electronic identity linking to a physical person might require personal appearance to proof the identity by conventional means, such as identity cards. It however is hard to argue that a registration needs to be done with every authority that aims for introducing e-government. A single registration requiring personal appearance should suffice. Moreover, an identification system should be interoperable between

Table 1. Overview of identification requirements

• Unique identification: Citizens shall be unmistakably distinguished from others • Durability: Permanent identifiers should be supported • Scalability: Digital twins shall be avoided even in large scale environments • Maintainability: The system shall, for example avoid forgotten identifiers if rarely used • Single registration: A single show-up to obtain an electronic identity suffices • Interoperability: Identification shall work in various administrative domains • Privacy: Data protection shall be maintained

administrations, preferably taking cross-border processes into account, so that the citizen can use his electronic identity with different authorities.

Interoperability and cross-administrative usage of electronic identification comes with a connotation putting privacy at stake, as unrelated cases might be linked. This raises data protection concerns, in particular with nation-wide identifiers.

Table 1 summarizes the requirements that have been identified above.

IDENTIFICATION vs. ELECTRONIC SIGNATURES

For unique identification an identifier of the person is needed. This unique identifier needs to be linked to the electronic signature to allow the relying party—usually the public authority in case of e-government processes—to verify that an electronic signature has been created by the claimed identity. If considering electronic signatures as the sole means of identification, the link between the physical person and the electronic signature is provided by the digital certificate.

However, data that is usually included in digital certificates—if using qualified certificates following the E.U. Signature Directive (Signature Directive, 1999) at least the name or a pseudonym—are not sufficient for uniquely identifying a person, as there might be digital twins, that is, two persons holding the same name. Even when amending the name by the date of birth and the place of birth, the digital twin problem isn't necessarily avoided. Even in a relatively small country such as Austria with a population of about 8 million several hundred citizens having the same name and date of birth exist. Moreover, the name may change over time such as due to marriage, thus processes started under the former name no longer can be identified solely relying on a certificate. Further problems that arise are that the spelling of names may not be consistent which affects the data quality that can be gained.

An option alleged useful might be to use the serial number of the certificate which per definition should be unique. Still several problems exist: First, a citizen might have several certificates each having different serial numbers that need to be linked to one person. Secondly, the certificate might expire or be revoked and thus no permanent identifier is given.

APPROACHES TO ELECTRONIC IDENTIFICATION

Unique personal identification numbers (PIN) are a tool of choice to avoid the digital twin problem. However, data protection is a concern, as, for example, the E.U. (Data Protection Directive, 1995) explicitly refers to national PINs when asking the Member States to determine "the conditions under which a national identification number or any other identifier of general application may be processed." The solutions followed by Member States vary significantly—also depending on culture and historically grown approaches: Using the national PINs within E-Government processes is accepted in some countries. Similarly the tax numbers or social security numbers may be used in others. For data protection reasons, such an approach is however considered unacceptable in several countries.

When linking unique identifiers to the electronic signature for authentication purposes, several options exist: From a theoretical perspective, this can either be done explicitly by holding the PIN with the data needed to create the electronic signature—the digital certificate or the signed document—or implicitly by defining a separate record that establishes the link.

Summarizing, the following approaches are worth investigating when introducing unique identification, have been proposed or even been implemented by countries, respectively:

- Introducing a permanent identifier into the certificate has been investigated by the IETF PKIX group