Empowerment through Electronic Mandates – Best Practice Austria

Thomas Rössler

Secure Information Technology Center Austria (A-SIT)
thomas.roessler@a-sit.at

Abstract. For dealing with electronic identities—especially in the area of e-Government—several approaches have been developed and successfully deployed already. However, most of them lack of an adequate vehicle to express exhaustively all kinds of representation and authorization types with which we are faced in every day's life. This is even more unsatisfying as, for instance, the European Union undertakes tremendous efforts to enforce the support of e-services for businesses and service providers, e.g. through the EU Service Directive. Especially businesses and service providers have an urgent need for being able to express all the various kinds of representations by electronic means. This paper firstly addresses the issue of representation from a general perspective in order to analyze the requirements. Finally, it introduces a concrete approach to solution—the concept of electronic mandates—which is successfully used by the Austrian e-Government initiative. This concept provides an exhaustive and all-embracing vehicle for building any kind of representation by electronic means.

1 Introduction

Empowering a person to act for another person or to conduct a certain transaction are important legal elements in everyday business. Empowering is almost always implicitly accepted in various situation, e.g. if a parent acts for her minor child or if a businessman acts on behalf of his company. Both scenarios are examples of authorisation because a person becomes authorised to act under delegated power. In the former example, the law empowers parents to represent their child in business. If a parent wants to act for her child in a conventional business, it is almost always sufficient to claim to be the parent. In the "worst" case, the adult would have to prove her identity and if the surname of both the adult and the child are the same, then parenthood is usually deemed to be proved. In the latter example, when "claiming" that a businessman acts in the name of some company it is often sufficient just to present a business card. Often no further proof is required, depending of course on the intended action.

Both examples demonstrate that authorisation and representation are elements of daily life that are taken for granted implicitly. In everyday life, proof of authorisation is not usually required, but when working with electronic transactions, authorisation has to be expressed explicitly. This creates a need for having an electronic form of empowerment and representation.

Throughout Europe, several Member States of the European Union are using various concepts in order to realize empowerment by electronic means. For instance,

C. Godart et al. (Eds.): I3E 2009, IFIP AICT 305, pp. 148–160, 2009.

Spain issues special digital certificates to companies with which total empowerment is simply expressed (i.e. the holder of the certificate has absolute power to represent the company by all means). However, introducing special types of certificates or to just add identifiers to digital certificates that express a certain type of representation provides a basis for building only simple scenarios and does not provide flexibility.

Also in literature (e.g. [1][2][3]) representation and empowerment has been discussed from various perspectives whereas most of the existing work focus on role based access control. On the other hand, [4] and [5] proposes using attribute certificate profiles and policies for expressing empowerment and delegation. Although this approach would somehow fit to the targeted scenario—i.e. the introduction of a mechanism for electronic empowerment in the electronic identity (e-ID) system of Austrian e-Government—a solution based on attribute certificates would be of limited flexibility. Thus, this paper introduces XML based electronic mandates as a vehicle for achieving empowerment and representation by electronic means within the Austrian e-ID system.

Electronic mandates were introduced into the Austrian identification schema for two main reasons. On the one hand, electronic mandates are the electronic equivalent of conventional mandates for empowering a person, in which a proxy acts for another person, referred to as the mandatory under certain circumstances. On the other hand, electronic mandates serve to close the gap between private persons and legal entities with respect to the Austrian electronic identity management system. Austrian Citizen Cards, i.e. the vehicle to electronically identify a person in front of Austrian e-Government applications, are issued to natural persons only. So without electronic mandates legal entities cannot actively participate in Austrian e-Government as they do not possess a Citizen Card to do so.

The rest of this paper is organized as follows. The following section shortly introduces the Austrian e-ID system and the Citizen Card concept in particular. Section 3 analysis scenarios where representation may occur and identifies the basic types of representations. In the course of this, the scenario of chained mandates will be discussed. Section 4 describes the Austrian approach to solution, i.e. the Austrian electronic mandates, in detail. After giving a report on the Austrian practical implementation, section 6 shortly touches a specialty of representation, namely how to deal with so called professional representatives. Finally conclusions are drawn.

2 The Austrian E-ID System at a Glance

The Austrian e-ID system is technically realized through the Austrian Citizen Card which serves two purposes: electronic identification and qualified electronic signatures. This section highlights the most important issues of both elements (for further readings refer to [6] and [7]) as electronic mandates extend the existing Austrian e-ID system.

For identification purposes, the Austrian e-ID system provides unique identification on the one hand, but aims to provide a maximum of privacy on the other hand. Every Austrian citizen—i.e. natural person—residing in Austria has to be registered with the so called Central Register of Residents (CRR). As a result, each Austrian citizen got assigned a unique identifier derived from her very unique CRR number.

As the so created unique identifier serves the basis for electronic identification in Austrian e-Government, it is denoted as Source Personal Identification Number (sourcePIN). The concrete derivation algorithm is depicted in figure 1.

SourcePINs are created during the Citizen Card issuing process only. This process and all required secrets, i.e. the secret key used during the creation process, are under the control of the so called Source-PIN Register Authority which is governed by the Austrian Data Protection Commissioner. Due to privacy reasons, it is forbidden by law to use this sourcePIN within e-Government applications directly. Instead, Austrian e-Government applications have been divided into a number of application sectors and for each application sector a different Sector-Specific Personal Identification Number (ssPIN) has to be created (the derivation algorithm is given in figure 1). As a result, an ssPIN of one sector, e.g. sector "SA", cannot be used in another sector, e.g. "GH", to identify the affected citizen and vice-versa.

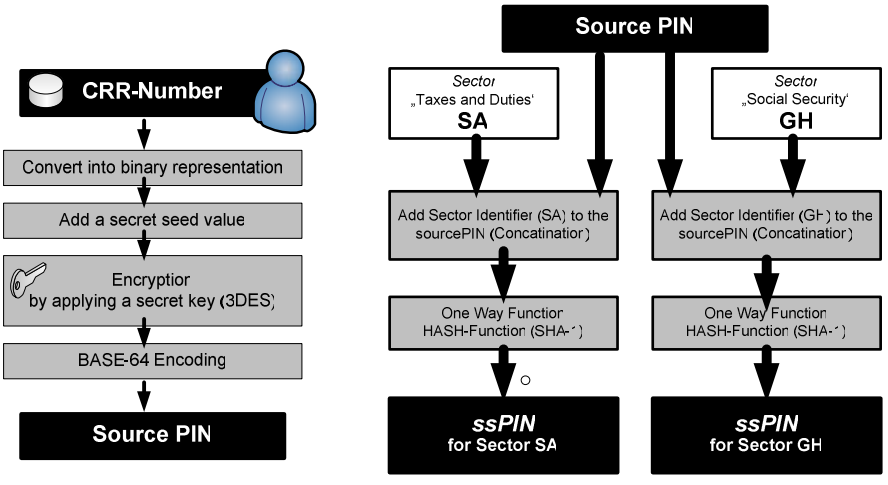

Fig. 1. Left: Creation of sourcePIN; Right: Creation of two ssPINs of different sectors

For authentication purposes the Austrian e-ID system fully relies on qualified electronic signatures according to the Austrian Signature Law [8] and the EU Signature Directive [9]. In other words, the Austrian Citizen Card is a secure signature creation device in terms of the laws mentioned before.

In order to realize person authentication, i.e. proving that a person is really the person she claims to be, the Citizen Card introduces the so called Identity-Link which is an XML structure combining a person's unique identification number—her sourcePIN—and her qualified signature. Very similar to an electronic signature certificate the Identity-Link combines a person's sourcePIN with her public keys required to verify her qualified signatures. The Identity-Link structure itself is electronically signed by the issuing Source PIN Register Authority which is in charge of issuing the identity credentials of the Austrian Citizen Card. In contrast to ordinary public-key certificates, the Identity-Link is solely stored in the person's Citizen Card. Furthermore, the Identity-Link is the only place where a person's sourcePIN is allowed to be

stored (note, although the issuing authority is called Source-PIN Register Authority it does not maintain a register of sourcePINs; this authority is only allowed to create sourcePINs on demand during the Citizen Card issuing process by taking a person's base identification number from the CRR and applying the derivation mechanism described above).

Based on the Identity-Link, identification and authentication of a person in front of an e-Government application is easy to achieve by the following steps:

1. The application asks the citizen to provide her Citizen Card. The citizen will usually make use of a middleware that provides communication between the Citizen Card and the e-Government application.
2. Through the middleware, the application reads the person's Identity-Link from her Citizen Card. Next, the e-Government application has to verify the electronic signature on the Identity-Link in order to prove its authenticity. If verification attains success, the application takes the person's sourcePIN in order to create her according ssPIN immediately.
3. In order to authenticate the person, the application asks the citizen to create a qualified electronic signature. Therefore, the middleware presents a given text to be signed (the text is given by the application and usually relates to the application's context or purpose) and asks the citizen to sign it by entering her secret code (the code is used to trigger the signature creation process on the Citizen Card).
4. The application finally verifies the created signature. Furthermore, after signature verification the application tries to match the public-keys given in the Identity-Link with the electronic signature just provided by the citizen. If the match is successful, the application is ensured that the claimed identity (i.e. represented through the sourcePIN/ssPIN provided in step 1) is the one who has created the electronic signature provided (in step 3).

From a technical perspective, the Citizen Card is an open concept which means it is bound neither to a concrete technology nor to a concrete implementation. There just exists a detailed specification defining the interfaces of and the requirements for an Austrian Citizen Card, however, every technical device which provides qualified electronic signatures and fulfills the technical Citizen Card specification can be immediately used as a Citizen Card in Austria. This means that the Citizen Card is not limited to smartcards only.

3 Scenarios and Types of Representations

From a use-case perspective, electronic mandates should serve to describe any kind of representations. Thus it should enable, for example:

a) a natural person to represent a legal person/entity
b) a natural person to represent another natural person
c) a legal person/entity to represent another legal person/entity
d) a legal person/entity to represent a natural person.

By combining multiple mandates of different types, even more complex situations can be created (by chaining multiple mandates).

These four examples roughly sketch the set of possible empowerment scenarios. Instead of discussing empowerment scenarios based on examples, the following sections will introduce generic types of representations from an abstract point of view. Finally, the special scenario of "chained mandates" will be discussed.

3.1 Types of Representations

The basic form of all types of representations is a simple *bilateral representation* where a person empowers another person to act in her name. More generally speaking and as representations are not just focused on natural persons only, a bilateral representation can be established between two entities.

However, the analysis of possible scenarios for representations bears three basic types of representations:

A) Bilateral Type
B) Substitution Type
C) Delegation Type

All three types are depicted in figure 1; this illustration requires three roles:

- Proxy
- Mandator
- Intermediary

The **Proxy** is the entity who becomes empowered to represent the **Mandator**. An **Intermediary** is an entity who may act between the Proxy and the Mandator in the event of indirect representations. As figure 1 deals with entities in general, natural persons and legal persons are used synonymously. According to this terminology, types of representations can be defined as follows (as it is not relevant for this general discussion, the following characterisation does not make assumptions about the scope of empowerment):

Bilateral Type. A bilateral representation is the basic type as mentioned above. In this case an entity—the Mandator—empowers another entity—the Proxy—to act in her name. This type is also denoted as direct representation.

Substitution Type. In contrast to the bilateral type a substitution is a pure indirect representation requiring two relations. Firstly, the Mandator has to empower an Intermediary. Considering this first relation solely, it turns out being a simple bilateral representation. Additionally, the Mandator has to allow the Intermediary to empower a substitute for representing the Mandator. This first relation in addition with the allowance for substitution is the precondition for this type of representation. Secondly, the Intermediary chooses a substitute—the real Proxy—to act in her name. As the Intermediary is empowered to represent the Mandator and as the Mandator gave the allowance that the Intermediary may choose a substitute, the substitute is empowered to represent the Mandator as well. Thus the substitute becomes a Proxy of the Mandator.

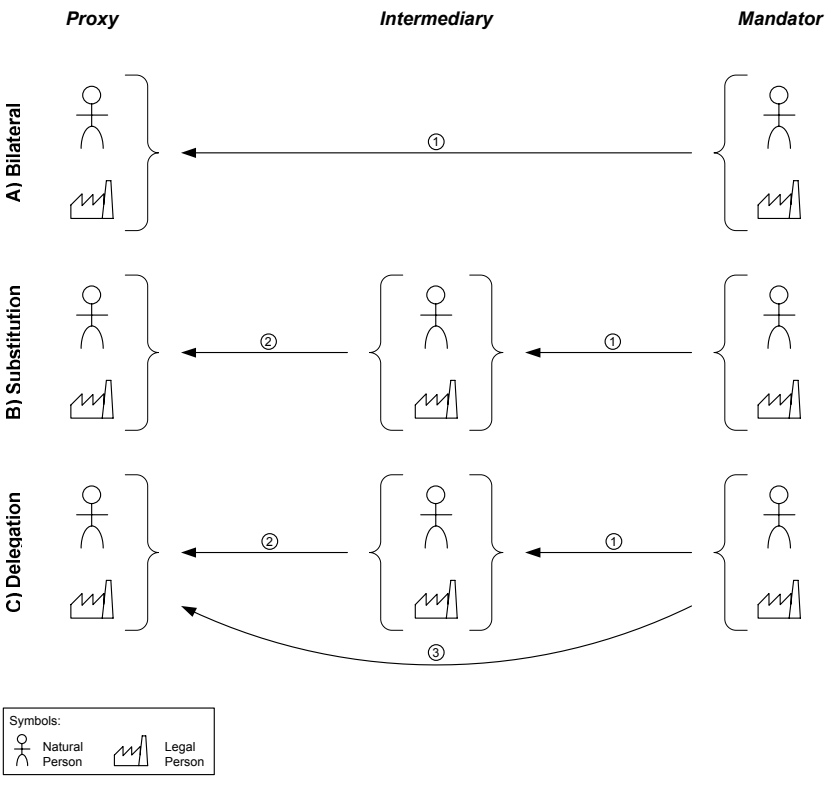

Fig. 2. Types of Representations

Delegation Type. The delegation type is an indirect representation at first sight. In contrast to the Substitution Type, the Delegation Type requires three relations. Firstly, the Mandator empowers an Intermediary to act in her/its name. Secondly, the Intermediary acts in the name of the Mandator and empowers another entity—the Proxy—to act in the name of the Mandator. Of course, the original Mandator has to allow this kind of delegation during the establishment of the relation between Intermediary and Mandator. As a result, the Proxy becomes empowered to act in the name of the original Mandator. In this third relation the Intermediary disappears as this relation exists between the Mandator and the Proxy only. So this third relation is finally a pure bilateral one as it exists between Mandator and Proxy directly. However, the important difference is that not the Mandator but an Intermediary establishes this relation.

Most of the existing empowerment scenarios are either of bilateral or delegation type. From the point of view of verification—i.e. the process of verifying if a given electronic mandate is authentic and establishes the empowerment required by a given application—these two types are rather simple to handle as just one electronic mandate has to be proven. In contrast to this, the substitution type may require to verify not only one but several mandates as it may cause to build a so called chain of mandates. The next subsection discusses the situation of chained mandates briefly.

However, the aforementioned basic types of representation have to be seen as primitives. By combining them arbitrarily nearby any relationship between mandator, proxy and intermediary can be created. Also from the verification perspective, a complex scenario can be easily handled by stepwisely separating the complex scenario into these primitives.

3.2 Chained Mandates

In contrast to the other types of representations, a substitution scenario usually causes chains of mandates. To give a very simple example, consider:

- company A empowers company B to represent company A in a certain context (depending on the scope of empowerment)
- company B empowers, for instance, its sales man to represent it by using an additional bilateral mandate

In this simple scenario, when the sales man aims to represent not only his own company B but also company A (according to the established relationship between company A and company B) he is required to provide two mandates which finally establish a chain as depicted in figure 2.

From a general perspective, the situation of having chained mandates is not necessarily relevant for the mandate issuing process but has to be considered during the verification process.

Examining the example depicted in figure 2 once again, two independent empowerments using two separate mandates can be identified. In a first step, entity A empowers entity B to represent entity A. In a second step, entity B empowers entity C to represent entity B.

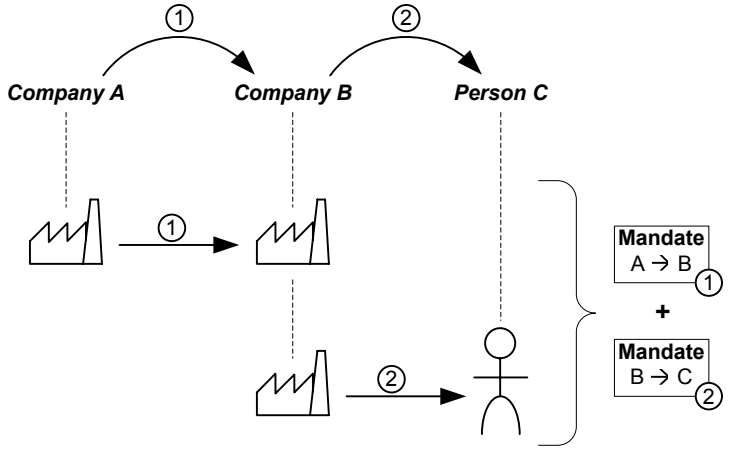

Fig. 3. A simple example of chained mandates

It is important to note that both relations are totally independent from each other. For example, the second empowerment may be established even before the first one. Furthermore, the second one does not necessarily contain any explicit provision or statement relating to the first empowerment and vice versa. However, depending on the national law it may be necessary that at least the first mandate contains the explicit allowance for this kind of substitution. From the point of view of an e-Government application, it will simply ask Person C—e.g. the sales man—to provide both mandates (mandate 1 and 2). In the course of the mandate verification process, the application must prove not only both mandates separately but also whether the mandator given in mandate 2 (i.e. Company B) corresponds to the proxy given in mandate 1.

4 The Concept of Electronic Mandates in Austria

Electronic mandates aim to provide end to end security as the proxy is holding a token (i.e. an electronic mandate) asserting that she is empowered to act in the name of another entity and can prove it in front of any application. So it is not an issue for applications to know about a person's authorisation to represent other entities/persons. Applications just have to verify electronic mandates. This makes it finally easy to manage authorizations from applications' perspective.

Similar to conventional mandates, an electronic mandate should hold:

- identity of the mandator
- identity of the proxy
- date and place of issuing
- content and concern of the mandate
- optional restrictions

The electronic mandate must hold the electronic identity of the mandator (i.e. the person who empowers another person to act in her name). In the event the mandator is a natural person, the identity of the mandator is denoted not only by her first and last name, date of birth, etc. but also by her unique electronic identifier, i.e. her sourcePIN as introduced before. The mandator's unique identifier is important as it is required to uniquely identify the mandator within applications. The identity of the proxy has to be similarly formulated by her full name, date of birth and her unique identifier which is her sourcePIN in the event the proxy is a natural person. In the event of having legal entities, analogous identity attributes are to be used, e.g. the full name of a company and its unique identifier taken from the commercial register.

The main concern of a mandate—i.e. the scope of empowerment—should be formulated in a textual description, more precisely, in arbitrarily combinable textual description blocks. It is expected that standard text blocks will come up for all types of standard mandates, e.g. mandates representing a procuration. In addition to the textual description of a mandate's concern, optional restrictions may be applied.

In order to assert the authenticity of a mandate, it has to be electronically signed, either by the mandator or by an issuing authority.

The concept for electronic mandates should introduce an electronic mechanism for revoking a mandate. The introduction of this technical revocation mechanism would be a great improvement in comparison to conventional mandates and it is especially

necessary for electronic mandates. On the one hand, it is sufficient from a legal perspective to revoke a mandate by publicly announcing a revocation. Consider conventional paper-based mandates: if the proxy is still in the possession of a paper that pretends to act as a valid mandate, the proxy would still be able to act illegally in the name of the mandator. Thus, the only effective way to avoid this problem is to request that the proxy destroy the paper mandate, which would prove hard to verify. With electronic mandates, this situation is much more difficult since the proxy could create an arbitrary number of copies of the electronic mandate and the mandator could never be sure whether any illegal copies still exist. An electronic revocation mechanism is therefore very desirable for electronic mandates.

Therefore, the introduction of an electronic revocation mechanism is strongly recommended. To make an electronic mandate electronically defeasible, the mandate needs to be registered with a certain revocation service. As a result, electronic mandates may hold an Internet address that provides revocation information on request. When attempting to verify an electronic mandate, the named revocation service has to be asked about the current revocation status by using the serial number of the electronic mandate. A similar revocation mechanism for digital certificates is already widely used and well-established. Thus, the concept of mandate revocation can be made similar to the revocation mechanism of digital certificates.

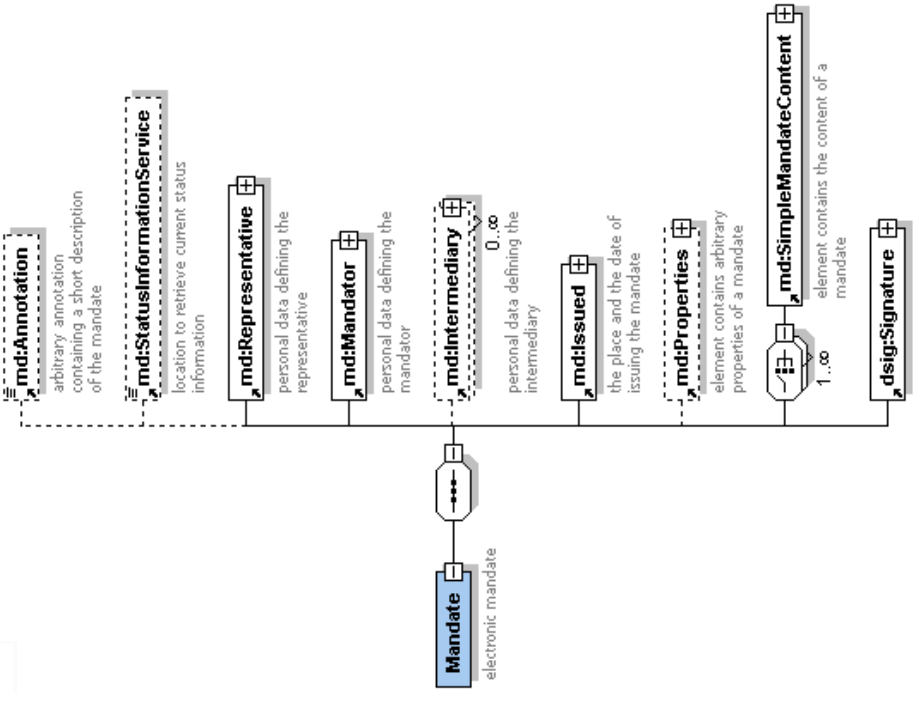

Fig. 4. Basic layout of electronic mandates (XML schema)

Electronic mandates that follow the characteristics described above have been introduced into the Austrian electronic identification schema in 2006. On a technical level, an electronic mandate in Austria is a specific XML structure (figure 4 illustrates the XML-structure of an electronic mandate in Austria) which must be electronically signed by an issuing authority, i.e. the Source-PIN Register Authority. The issuing authority just asserts that the electronic representation bases on an existing and already established authorisation.

The concept of electronic mandates requires that electronic mandates are held by the proxies. Every time a proxy makes use of a mandate, she has firstly to use her e-ID (i.e. Citizen Card) to prove her own identity. Additionally, she has to declare to the e-Government application that she is rightfully acting in the name of the mandator by presenting the electronic mandate.

To summarize and according to the be basic requirements of electronic mandates introduced before, an electronic mandate according to the Austrian specification [10] contains the following mandatory and optional elements (referring to figure 4):

- **Identity of the Proxy (Representative)**:
  - natural person: first name, last-name, date of birth
  - legal person: full name
  - the person's unique identifier (i.e. the sourcePIN in the event of natural persons)
- **Identity of the Mandator**:
  - natural person: first name, last-name, date of birth
  - legal person: full name
  - the person's unique identifier (i.e. the sourcePIN in the event of natural persons)
- **Identity of the Intermediary [optional]**:
  - natural person: first name, last-name, date of birth
  - legal person: full name
  - the person's unique identifier (i.e. the sourcePIN in the event of natural persons)
- **Scope of Empowerment**:
  - One or several text blocks are used to describe the scope of empowerment. Although arbitrary text blocks are possible, typical electronic mandates are built by using standardized text blocks. This eases mandate verification. However, in order to be able to create any kind of mandate, arbitrary text is allowed.
- **Constraints [optional]**:
  - Additional to the scope of empowerment, arbitrary restrictions can be formulated (optionally). Currently, the specification defines three concrete types of restrictions by using specialized XML elements: time constraint (i.e. a mandate is effective within a given time frame only), collective constraint (i.e. a proxy cannot act alone; further proxies are

required) and financial constraint (i.e. actions taken based on the given mandate are limited with a financial transaction limit).

- **Serial Number**
  - Each electronic mandate gets assigned a unique serial number. This is required for revocation purposes.
- **Link to a Revocation Service [optional]**:
  - If a link to an electronic mandate revocation service is given, the verifier of a mandate is requested to contact this service in order to verify the revocation status of the mandate. For requesting the revocation status a HTTP-based protocol has been developed [10]. Currently, the Source PIN Register Authority runs a mandate revocation service; currently all existing electronic mandates are registered with this registration service per default.
- **Electronic Signature of the issuing Authority**:
  - Due to Austrian law, every electronic mandate has to be signed by the issuing Source PIN Register Authority. This also applies to bilateral mandates.

Electronic mandates are issued by the Source PIN Register Authority only. Therefore, this authority provides a web-application with which citizens can apply for electronic mandates based on an existing authorization (empowerment). This means, that the empowerment must be already established, e.g. based on paper mandates or entries in official registers (e.g. the register of commerce). In order to foster the take up of electronic mandates in the field of e-Government applications, the Austrian e-Government initiative provides open-source software modules for providers and developers of e-Government services, which automatically verify electronic mandates—including chain verification—and provide e-Government applications the unique electronic identity of the mandator and the proxy.

To give an example of how electronic mandates influence the process of identification and authentication, the following scenario illustrates a typically identification and authentication process using the Austrian Citizen Card and electronic mandates. In this example a person aims to access an e-Government application in the name of a company. In addition to the four basic steps already introduced in section 2, the following additional steps are required due to the use of electronic mandates:

1. to 4. See workflow given in section 2. As a result, the application has authenticated the person and thus holds her sourcePIN.
2. The e-Government application has to read the person's mandate(s). As her mandate(s) are stored in her Citizen Card, the application requests to read this/these mandate(s) through the Citizen Card middleware.
3. For each mandate provided, the application has to verify the electronic signature.
4. If the mandate is authentic, the application has to verify whether the person defined as proxy by the mandate is the person who accessed the application by using her Citizen Card. This match is easily verifiable thanks to the sourcePINs

given in the electronic mandate and in the person's Identity-Link. If sourcePINs are equal, the person using the service is an empowered proxy.

5. The application has to verify whether the given mandate—or more precisely its scope of empowerment—is sufficient for this particular e-Government application. This could be verified by comparing the textual description given within the electronic mandate against profiles configured in the application. If the given text block can be recognized and is considered being sufficient, the application can succeed.
6. The application finally takes the identity data of the mandator given by the electronic mandate. As the mandator's unique identifier is given as well, the application can use the mandator's e-identity in the same way as the mandator would access the application personally (in the event of natural persons, the mandator's sourcePIN is provided by the mandate; thus, the application is able to create the mandator's ssPIN immediately).

The electronic delivery service was one of the very first e-Government applications in Austria which accepted electronic mandates. Mandates are especially important for the Austrian electronic delivery service since legal entities are only able to register for electronic delivery with the use of electronic mandates (this means that a private person has to act in the name of a legal entity).

5 Specialtiy: Professional Representatives

Mandates as described in this paper are just used for so called explicit and bilateral empowerments. In contrast to this, the so called professional representatives, e.g. lawyers, tax advisors, etc., are not required to provide an explicit mandate if they want to act in the name of their clients. For them it is sufficient to prove that they are professional representatives.

Thus, their Citizen Cards, or to be more precisely their qualified certificates, hold a special object identifier (OID, according to ISO/IEC 9834-1) identifying them being a professional representative. As a result, professional representatives are not required to present explicit electronic mandates; instead e-Government applications just verify whether the digital certificate of the representative contains the OID defined for Austrian professional representatives. This situation is similar to the situation we have in the paper world. In order to "mark" professional representatives using standardized methods, the Austrian Federal Chancellery has reserved an OID-sub tree that defines these OIDs on an international level [11].

6 Conclusions

As mandates are an important element of our everyday's life, mandates—or more generally speaking empowerments or representations—have to be introduced in electronic identification systems as well. Not only the existing e-Government applications raise the need for it but especially the upcoming EU Service Directive that explicitly

focuses on processes and applications for service providers, i.e. companies, etc., boosts the demand for a vehicle to express empowerment and representation by electronic means.

Therefore, this paper analyses various types of representations from a general and abstract perspective and identifies three primitive types of representations. By combining these primitives all possible scenarios can be built. Furthermore, this paper introduces a concrete approach for electronic empowerment by introducing the concept of electronic mandates as it is used in Austria. This concept of electronic mandates is used in the Austrian e-Government framework not only to establish empowerment by electronic means but also to close the gap between natural and legal persons.

References

1. Crampton, J., Khambhammettu, H.: Delegation in Role-Based Access Control. In: Gollmann, D., Meier, J., Sabelfeld, A. (eds.) ESORICS 2006. LNCS, vol. 4189, pp. 174–191. Springer, Heidelberg (2006)
2. Zhang, L., Ahn, G.-J., Chu, B.-T.: A rule-based framework for role-based delegation and revocation. ACM Trans. Inf. Syst. Secur. 6(3), 404–441 (2003)
3. Peeters, R., Simoens, K., DeCock, D., Preneel, B.: Cross-Context Delegation through Identity Federation. In: Brömme, A., Busch, C., Hühnlein, D. (eds.) Proceedings of the Special Interest Group on Biometrics and Electronic Signatures. Lecture Notes in Informatics (LNI) P-137, pp. 79–92. Bonner Köllen Verlag (2008)
4. Farrell, S., Housley, R.: An Internet Attribute Certificate Profile for Authorization. RFC 3281 (2002)
5. Francis, C., Pinkas, D.: Attribute Certificate (AC) Policies Extension. RFC 4476 (2006)
6. Leitold, H., Hollosi, A., Posch, R.: Security Architecture of the Austrian Citizen Card Concept. In: Proceedings of ACSAC 2002, pp. 391–400 (2002) ISBN 0-7695-1828-1
7. Rössler, T.: Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government. Computer law and security report the bi-monthly report on computer security and the law governing information technology and computer use 24 (2008)
8. Austrian Federal Law: Federal Act on Electronic Signatures 2001 (Signature law), Austrian Federal Law Gazette, part I, Nr. 190/1999, 137/2000, 32/2001 (2001)
9. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. EC Official Journal, L 013, 12–20 (2000)
10. Rössler, T., Hollosi, A.: Elektronische Vollmachten - Spezifikation 1.0.0 (May 2006)
11. Digital-Austria: OID der öff. Verwaltung, OID-T1 1.0.0. (February 2009)