IMPROVING COMMUNICATION TO CITIZENS AND WITHIN PUBLIC ADMINISTRATION BY ATTRIBUTE CERTIFICATES

Michael Sonntag

Institute of Information Processing and Microprocessor Technology (FIM), University of Linz, Austria
sonntag@fim.uni-linz.ac.at

Abstract. *Public administration should serve the citizens. However, electronic communication with it is still in its infancy. To improve response speed on inquiries and allow unattended inspection of records, an unambiguous and secure way of identifying records is needed. Another issue is how citizens locate the person responsible for handling certain requests. If this information is stored in a public directory it can also be used for finding distributed knowledge embodied in persons. Both issues can be solved by using attribute certificates, which are additional signed information pertaining to a persons certificate.*

1. Introduction

First, two issues in public administration will be discussed briefly and then the concept of attribute certificates is explained. They are an often overlooked part of the X.509 standard ([16]), and found entrance into some applications, but are provided for only in few legal rules. The German signature law ([1], [2]) explicitly includes them, while the signature directive [12] of the EU and the Austrian signature law [9] ignore them.

Then it will be discussed how representing record numbers for records by attribute certificates can improve service for citizens when using electronic communication and bring a modest decrease of work for the administration.

Afterwards a possible solution for another issue is presented. The publication of authorizations for signing certain types of notifications can be done by introducing attribute certificates and making them publicly available in a directory. This is an improvement both in a legal way and in service for citizens, but creates additional work for the administration.

How hidden knowledge within administration can be unearthed using current, and the history of, signing authorisations is described in the next part: Doing a reverse lookup on attribute certificates or signed and archived documents. Information embodied in persons, who are working distributed across the coun-

try, is rather hard to find. This is because usually only persons know, who possesses this information (this meta-information is not on record). Using attribute certificates allows making this information explicit and usable.

Before the conclusion a short discussion of the additional work required for implementing these proposed improvements is included and what alternatives could be used.

2. Two issues in public administration

Comparing electronic communication to and from public administration with a call center and telephone calls seems to be a bit out of the way, but nevertheless these can be compared. One similarity is (or should be), that both try to serve their customers (i. e. citizens) in the best and fastest way. To improve response quality and speed, a call center possesses automatic caller identification: If somebody phones, the software identifies the telephone number from which the call originates, finds the data of this person in the database, and presents it immediately on the screen of the person taking the call. This allows personally addressing the caller and providing individualized information to him or her. In the context of public administration phone calls are less important than written and possibly electronically signed and transmitted records. The distribution of incoming external communication to the person responsible for handling it has to be done either manually or according to predefined rules and heuristics (which might err sometimes). However, as the problem is the same (identifying related material) a similar solution might be adopted at least in electronic communication. Uniquely identifying records through their normal number is not an ideal solution, as these are usually hand-typed (and therefore might be wrong or in a different format) or copied somewhere into the text. In both cases, they are rather hard to find. Therefore a solution is required which can be identified regardless of its placement and where mistakes are unlikely and recognizable.

Another more legal issue is the publication of the permission to approve certain types of notifications (“Approbationsbefugnis für Bescheide“). In Austria an administrative notification is then valid, if a person approved/signed it, which is authorized to approve *some* type of notification of the public authority ([5] 168 Z 7 on § 18 AVG; VwGH 19.1.1990, Zl 89/18/0079). If he is not authorized for this particular notification it is nevertheless binding for the authority. There may be internal repercussions (VwGH 27.5.1988, Zl 88/18/0015), but they do not extend to the outside. If, on the other hand, the person signing it has *no* authorization *whatsoever* to approve notifications for *this* authority, it is not even a notification at all (VwGH 20.12.1996, Zl 95/17/0392). For citizens it is therefore very important to know, who is authorized to approve notifications (and in what area). Otherwise it is almost

impossible to know, whether the notification he or she received is valid or not (See VwGH 21.10.1992, Zl 92/02/0195, where the complainant was not heard about the information, whether the signer of a notification was authorized or not). However, these signing authorizations are only handled internally by the authorities. They should instead be created in the form of decrees and published, as requested in literature ([7] 17, [14] RZ 107). The Austrian supreme courts have rendered different judgments on this, mostly accepting the current practice of no publication (e. g. none required in VfSlg 10338, but otherwise VwSlgNF 11801 A or OGH 15.10.1986, 9Os7/86, where the effects of authorization are identified as both internal and external of the authority). In my opinion, publication is required, for only then due process of law is guaranteed for citizens as they can then decide, whether the paper they received from an administrative authority is a notification or does not have any legal consequences at all. In the past this practice of non-publication had the reason that the alternative would have been very cumbersome (where to publish?) and require a lot of work, as these authorizations change frequently (e. g. usually with each promotion or transfer). Nowadays, the Internet allows publications with a lot less effort and should therefore be used, increasing the legal protection of citizens.

3. Attribute certificates

An attribute certificate is a separate structure, referring to a base certificate and containing additional attributes like clearances or authorizations. It can also be used to implement signatures by legal persons [13] through encoding the authority of natural persons to sign for them in the attribute certificate. A signature may contain any number of attribute certificates (or references to them) without repetition ([11] 6.1.5). Whether an attribute certificate can be used with different base certificates or not depends on the type: It may refer directly to a certain certificate (only one possible) or to a distinguished name. This name may be used in multiple certificates and so the attribute certificate could be used with all of them ([16]; forbidden in [10] 3.3). Attribute certificates can be issued and revoked independently from their base certificate and also by a different authority (“attribute authority”; AA; [3] 5.3.4; in contrast to the “certificate authority”, CA, issuing the base certificate). They are defined (ASN.1) and encoded (usually DER [15], [6]) in a special format to be portable and platform independent.

3.1. Content of attribute certificates

Attribute certificates contain the following (and other, in this case not relevant) data, but no public key. As a reference to the base certificate(s) it belongs to, the name (or pseudonym) of the person according to the X.509 standard

([16]; restrictions exist in [10]) or the unique serial number of the certificate must be included:

1. Holder: This is either a reference to the base certificate using the issuer and the serial number of the certificate or the distinguished name of the subject. In the latter case it must be exactly identical to the name in the base certificate, else automatic verification is impossible. Care has to be taken as this might not be unique (two persons can possess the same name, but not identical certificate serial numbers).
2. Issuer: To identify the authority, which issued this attribute certificate.
3. Signature: The signature of the certificate authority.
4. Certificate validity period: The period during which the attribute certificate is valid. It is (technically) unrelated to the validity period of the base certificate.
5. Attributes: The actual attributes associated with the subject. Any number of attributes can be included.

3.2. Standard attributes

A number of standard attributes which will be often needed are defined in [10] (for base certificates additional attributes are defined, e. g. serial number of the chip card containing the certificate and private key): Monetary limit, declaration of majority, or date of certificate generation. Important in this context are “Procuration” and “ Admission”, which could serve as examples.

Procuration allows specifying that a person is allowed to represent a different person, which is identified in the attribute certificate either through the name or a referenced certificate, similar to specifying the holder. Optionally, the country and type of substitution can be included to specify it and which law is to be used for interpreting it.

Admission is more complicated but would be better suited as a base for modelling an attribute for the second use proposed. It is intended for representing admissions for certain professions, e. g. medical doctors. It includes two different authorities, an admission authority, which guarantees the admission of the subject of the certificate (the person transferring the authorisation), and a naming authority, which is responsible for providing lists of professions and/or areas of work (centralised maintenance of subtypes used).

4. Using attribute certificates for record numbers

Issuing an attribute certificate for each person related to a certain record could solve the first of the issues mentioned. If a communication including a signature with this attribute certificate is received, it can automatically and without possibility for error be allocated to the person in charge of this specific pro-

ceeding, where it is presented with all the accompanying data (including the record, previous communications, etc.). The base certificate alone is not sufficient, as a person might be involved in numerous proceedings. With support by the software this could also be extended to e. g. videoconferencing systems, where the need to reliably identify the other partner is the same as in written communication. Here the issue is even more pressing, as the record needs to be retrieved in a very short time. Using attribute certificates this can be done automatically during opening the connection. This improves service for the citizens and yet may reduce the work by the administration slightly, as the record is retrieved without human intervention.

Using this system another benefit for both the administration and citizens is possible. If the record is uniquely identified by an attribute certificate issued by the administrative authority to a certain person and accompanies a signature by this person, inquiries for examination of records could be fulfilled automatically. The approval of an official would then only be needed in special cases. As attribute certificates are always used in combination with normal certificates, automatic logging is also possible, ensuring that it is stored who viewed which part or parts of the record at which time. However, this benefit does not come without a price: If parts of the record are to be kept secret, they have to be specially marked for each person, who should receive (or not receive) access to it. In any case this system is only then useful, if most or all of the parts of a record are available in electronic form.

Advantages of using attribute certificates for record numbers are:

? Automatic retrieval of records without error. This need not replace previous methods of assigning communication elements to procedures, but can be added, so the less reliable methods are only used if the identification was not possible in this way.

? Status and content of the procedure is available to the parties without need for supervision. Citizens can request and receive information on the current status of their application at any time and without the need for an official to approve or reject it.

? Full logging of inspection by parties and not only of officials. Currently, inspection by parties, which is done through officials, has to be marked explicitly by the official, otherwise this information is lost. In the case of electronic inquiry this access can be logged with all relevant details (time, duration, parts retrieved, etc.), securing evidence without the possibility for later repudiation of access.

Disadvantages or problems for the usefulness of this method are:

? Initial issuing of an attribute certificate for each party of each procedure is required, implying that the personal certificates of the parties need to be available. This might be a problem if the application is filed on paper but later electronic communication is desired. In this case the initial electronic contact would require an official to verify the information and the status as a party to the procedure. The attribute certificate itself, however, can then be issued automatically.

? Requires standard values for visibility to parties and their verification for marking exceptions. Every piece of the record has to be marked according to its visibility: To all parties, only certain parties or internally. Default values might be used for certain types of procedures or documents, but even then a revision is needed on creation or when applying additions/changes.

? Depends on the use of certificates by citizens. For its usefulness and reduction in work a precondition is the widespread use of certificates by citizens and the availability of communication programs employing them (common for E-Mail, but not for other modes of communication like IP-phones or video-conferencing).

5. Publishing signing authorizations through attribute certificates

A remedy for the second issue of publishing the authority to sign certain types of notifications could be the introduction of attribute certificates, issued when these authorizations are transferred. They should contain the general area of authorization (should be standardized; see below) and, if necessary, a detailed textual description of the exact scope. Accompanying certificates allow citizens (perhaps with advice from a lawyer to interpret the textual description if it is longer or more complicated) to verify whether authorization for signing this particular notification was present at the time of signing or not. The general issue, whether even a very small signing authorisation for this authority was granted or not, could be decided by the citizen itself.

Issuing attribute certificates does not immediately solve the problem, as this is only an internal technical solution, but it allows publication of the data in a very easy way. For verification purposes certificates (except the lowest in the certification path) need to be published. Otherwise the whole certificate chain would have to be included in every signature, including up to the root certificate of the certificate authority. Similarly, no longer valid certificates (except those, whose timespan of validity elapsed), need to be published (Certificate Revoca-

tion Lists; CRL [8]) to allow verifying the validity of a signature at different times (invalid after the publication of the revocation, but older signatures remain in force). In exactly the same way currently valid certificates can be published and would therefore be publicly available. In contrast to CRLs, which are time-stamped and signed by the certificate authority at the time of the revocation to prevent later modifications and insertion of fake ones, the currently valid authorizations would have to be time-stamped and signed on each access. This guarantees for the person inquiring that this certificate is currently valid (and it could be later used as a proof of this). Alternatively (the previous approach is quite a burden for the directory server containing the certificates) the certificate itself and the (signed) revocation list could be used instead: If the certificate is not in the list, it is valid. This is equal to the first approach with no errors possible if revocation entries are not dated back in time and immediately published upon creation (which is both legally required for a CA). Through this public directory citizens can access the list of authorized persons without the need for complicated programs. Additionally, upon receiving an electronically signed notification, the verification of the validity according to its content can be done partially without intervention. Mathematical validity and existence of the certificate in the directory can be verified automatically, while the actual authorization has to be inspected by the citizen (unless the notification itself is marked as belonging to a certain type; but this information is guaranteed only by the signature itself…).

This method results in an advantage for citizens, but, in comparison to the current situation, a bit more work for the administration. If internal electronic communication and electronic handling of files is used, similar authorizations are required in any case, although they need not be in the form of a public key infrastructure (e. g. using passwords and write-once storage).

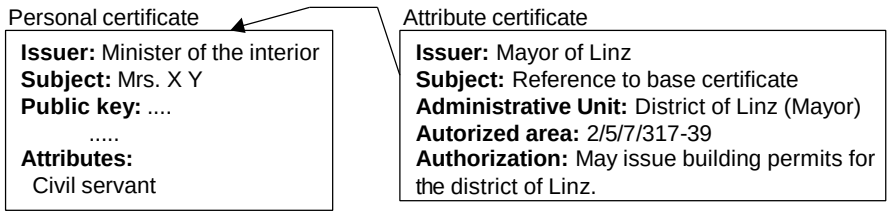

Figure 1: Example of a base and an attribute certificate (It is assumed here that the minister of the interior would issue all base certificates, regardless of the actual employer of the civil servant)

6. Unearthing hidden knowledge in administration using signing authorizations

In public administration the intended way of resolving non-standard (and both common and uncommon) or more complicated issues works like this: A citizen sends a petition, the administration works on it, and later an administrative notification is issued, either positive or negative. In case of a negative response the citizen then changes his request and starts over again. However, the usual and more sensible way is something different: The citizen tries to locate the person responsible for this issue, discusses the planned petition and the requirements for a positive conclusion and only then the petition is finalised and sent to the administrative office. This requires identifying the appropriate person, which can be a tedious and complicated task. Similarly, an administrative officer might stumble upon a difficult problem and try to find a colleague from a different geographical area responsible for the same topic, who might know a possible solution or the way of solving the problem.

Finding the persons who may decide some issues and discovering those with knowledge in a certain area is therefore often a necessity. Using attribute certificates issued for signing authorisations as explained above, a “reverse lookup” is possible: Searching the list of certificates reveals those persons, who are authorised to sign in certain areas. As signing authority usually goes hand in hand with continuous practice in this area, the persons with knowledge on a certain topic can be found. As the attribute certificates are included in a standardised public list, searching through it entails no special problems and could be done with only minor modifications to existing software.

If documents are stored and classified, those could also be used for a search: Who signs many documents of a certain type involving a special sub-area will have the applicable regulations (and how to interpret them) at hand. This produces more detailed results, as also conclusions from the content of the documents are integrated. Allowing searches like this requires more work in advance, as all the documents need to be classified, though most will only rarely be needed again. The alternative, using a full text search or automatic classification requires no work time, but reduces the quality of the results.

Collecting the attribute certificates of a single person is a first approximation for this persons knowledge (or the knowledge the person has access to through staff members). It is surely not complete, but it can serve as an initial start. Certificates are only issued for a certain period of time; similarly information deteriorates over longer spans of time. So if somebody had the authorisation to sign documents with a certain content some years ago but moved on to other tasks, he probably still knows the basics of the area, but might have forgotten details

(and the legal framework could also have changed in the meantime). So not only current, but also past knowledge can be found using this system as attribute certificates expire, but are not destroyed for a long time (to allow verification of signatures at a later point in time). This might be useful in certain cases, e. g. if an overview on rare or special cases is needed.

But also some limitations exist for this approach:

? Authorisation for signing does not always go hand in hand with detailed information. The higher the position the more power a person has, but also probably the less information about details. So additional decisions are necessary: If specific details are needed, the lowest (longest chain of attribute certificates) person with the appropriate authority should be searched for. If a broader view is required, the best solution might be not searching for the highest ranking person, but some person in the middle of the certificate chain.

? To be useful, a detailed system of areas of authorisations is required. While it should not be too difficult to create such systems, agreeing on a single version might take a long time. Additionally this system must be rather static to be workable, so the organisation of the administration can not be used as a model as it often changes. The problem of creating this scheme is mitigated however by the possibility to add a textual description. Finding the correct balance between the description and the general system of predefined areas is an important issue for success, as too much text will result in poor answers. At the same time a too detailed system forces to make difficult decisions, where to place a persons authorisations (and which authorizations to search for; especially for searches by citizens).

? The authority to sign documents embodies not all information. Staff members might have personal interests, which are professionally related but not (currently) used in their tasks. Also, persons not authorised to sign any notifications do not have no knowledge at all. Partly theirs is included in their superiors' authorisations, but this may not be a complete assessment. This could be remedied by including their information through attribute certificates of a different class, containing not the authorisation for signing, but only identifying special abilities in an area. The drawback of this extension is, that it violates the concept of attribute certificates: These persons have no "special attribute" concerning their *signatures*. (Although they can use it for signing internal documents.)

Using attribute certificates in this way the administration can be made more transparent to the citizens and provide better services to them. At the same time, the existing internal knowledge can be utilised to a larger degree, resulting in an increase in quality and perhaps shorter response times.

7. Estimation of additional work required

If electronic media are to be used for legal communication of citizens with public administration, electronic signatures are a fundamental prerequisite, otherwise a (physically) secure network would be required. Should notifications be sent by the administration through electronic communication, also an externally visible public key infrastructure (PKI) is required. This major effort is therefore necessary anyway and the addition of attribute certificates is only a minor technical problem with small costs. Additional costs are however involved in issuing the certificates.

In the case of record numbers the certificates of the parties involved need to be collected and assigned to the proceeding. Actual issuing of the attribute certificate and sending it to the party can be automated. Additional work is required for marking the documents visibility's to parties: This results in a decrease of work if numerous requests are to be expected (only once required), but increases the workload if few requests for inquiries take place. An alternative is using the conventional record number for identifying the procedure involved with a communication received. But those numbers might easily be misspelled (manual typing) and their position in a document is not fixed, requiring a full-text-search. Also, automatic identification is not possible in non-textual forms of communication, e. g. videoconferences, or shared workspace sessions. In contrast to this, attribute certificates are a part of establishing the connection (e. g. when using SSL) and could therefore be used with any means of communication.

Using attribute certificates for signing authorisations requires additional work. They have to be created beside the written document. If however the document is also already created in digital form and electronically signed, only adding the attribute certificate prior to signing is needed. For the content of the attribute certificate, the area the person is authorised to sign for needs to be specifically encoded. Support for this through software is possible, as the division is rather static and predefined. The additional textual description could be copied from the normal authorisation. Only very little additional work is required if electronic issuing is used. In case of completely manual authorisations, a separate and rather complicated (collecting and transferring the data to a separate signer, verification of the data against the written authorisation, etc.) step is necessary. An alternative solution does not seem to be sensible, as publishing the authorisations on paper would be complicated to arrange and cumbersome to verify for citizens, so that only a very small increase in quality and legal security would result. Publishing them in textual form (e. g. as a PDF-file as the Ministry of Justice [4]) has also drawbacks, especially for locating this information (the Ministry of Justice "hides" it in one of its leaflet); automatic verification is also impossible.

8. Conclusion

The use of attribute certificates can bring benefits to both citizens and the public administration: Better legal protection, a slight reduction in work and the possibility to find knowledge on certain topics, which would otherwise be practically impossible. Human resources are a very important part of today's business and this is especially true for public administration, which does not produce goods but services. The knowledge of these persons is naturally distributed. But it is only then useful, if the appropriate item can be found when needed. Using attribute certificates to model signing authorisations allows this, while additionally improving the information for citizens (which administrative officer to contact for a certain case) and improving legal protection, as verifying whether a notification is correctly signed or not is then possible. The additional work required for this is considerable if no PKI already exists. As such is bound to be implemented in the near future anyway, the additional effort for using attribute certificates and the presented two sample applications is very moderate and should therefore be considered right from the start.

9. References

[1] German Law on Digital Signatures (IuKDG Art. 3): http://www.iid.de/rahmen/iukdg.html#a3 (12.2.2001)

[2] Draft for new German Law on Digital Signatures (according to the council resolution of 16. August 2000) http://www.iid.de/iukdg/eval/RefE-DLR.pdf (12.2.2001)

[3] European Telecommunication Standards Institute (ETSI): Electronic Signature Formats (ETSI ES 201 733 V1.2.2 (12/2000)) http://www.etsi.org/SEC/ts_101733v010202p.pdf (12.2.2001)

[4] Geschäftsordnung des Bundesministeriums für Justiz, Stand Februar 2001 http://www.bmj.gv.at/broschueren/download/gesch0201.pdf (26.3.2001), 49 ff

[5] Wolfgang Hauer, Otto Leukauf: Handbuch des österreichischen Verwaltungsverfahrens[3]. Eisenstadt: Prugg 1987

[6] Burton S. Kaliski Jr.: A Layman's Guide to a subset of ASN.1, BER, and DER. ftp://ftp.rsasecurity.com/pub/pkcs/ascii/layman.asc (15.2.2001)

[7] Wolfgang Pichler: Die Approbationsbefugnis als Problem der Verwaltungsreform. ZfV 1978/11

[8] Internet X.509 Public Key Infrastructure Certificate and CRL Profile http://andrew2.andrew.cmu.edu/rfc/rfc2459.html (14.2.2001)

[9] Austrian Federal Electronic Signature Law: Bundesegesetz über elektronische Signaturen (Signaturgesetz- SigG), BGBl I 190/1999 (including proposed amendments according to the cabinet 10/2000) http://www.a-sit.at/TEXTE/Signatur_legislative/SigG%20incl%20Novelle2000.pdf (12.2.2001)

[10] BSI: Schnittstellenspezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV. Signatur-Interoperabilitätsspezifikation SigI. Abschnitt A1: Zertifikate. http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/main/spezi.htm (12.2.2001)

[11] BSI: Schnittstellenspezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV. Signatur-Interoperabilitätsspezifikation SigI. Abschnitt A2: Signatur. http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/main/spezi.htm (12.2.2001)

[12] Signature directive of the EU: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, ABl. 19.1.2000 L 13/12 http://www.a-sit.at/TEXTE/EU_RL_engl.pdf (12.2.2001)

[13] Michael Sonntag: Electronic Signatures for Legal Persons. In: Hofer Susanne, Beneder Manfred (Ed.): IDIMT'00. 8th Interdisciplinary Information Management Talks. Linz: Universitätsverlag Rudolf Trauner 2000, 233-256 (Also as SYSPRO report 72/00, August 2000)

[14] Robert Walter, Heinz Mayer: Grundriß des österreichischen Verwaltungsverfahrensrechts[4]. Wien: Manz 1987

[15] ITU-T Rec. X.680, "Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation", 1994

[16] X.509: ITU-T X.509: Information Technology - Open Systems Interconnection – The Directory: Authentication framework, 1997 (Clause 13: Obtaining Certified Attributes)