Cross-Context Delegation through Identity Federation *

Roel Peeters† Koen Simoens Danny De Cock Bart Preneel

Department of Electrical Engineering, ESAT/SCD-COSIC
Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, 3001 Heverlee, Belgium
{firstname.lastname}@esat.kuleuven.be

Abstract: We present in this paper a basic scheme for delegation in a federated setting and two more advanced schemes, transferable and corporated delegation. By transferable delegation delegatees are able to delegate the received privileged actions further to someone else. Corporate delegation is delegation within a business context. Our schemes are generic and user-centric. We elaborate on the different procedures to issue, accept and revoke mandates in these schemes. Different variations are discussed and their impact on the corresponding procedures is evaluated. For the basic scheme of delegation mandates are used, for more advanced schemes, as the complexity increases, use of delegation assertions is proposed.

1 Introduction

Delegation is the process of giving a mandate to an identified entity [HV07]. Basically, this means that this entity receives the right or responsibility to act for the account of the mandate issuer. There are at least three parties involved in the process of delegation: the *delegator*, who gives or shares one or more of his privileged actions to another party; the *delegatee*, who receives one or more privileged actions; and the *service provider*, who provides services to a requester. Apart from these principal parties, there are a number of other parties that might be involved for specific purposes, e.g., a *mandate authority* could register that a given privileged action was delegated and may be queried about the validity status of a mandate.

Let us consider the following example. The general rule for taxation in the European Economic Area is that citizens working abroad for a certain duration pay taxes in the country where they work. A citizen may decide to delegate filing his tax declaration to an accountant in the foreign country. The citizen acts in another context than the accountant and the

*This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government, by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy), and in part by the IDEM (Identity Management for eGovernment) project of the IBBT (Interdisciplinary institute for BroadBand Technology) of the Flemish Government.

†Roel Peeters is funded by a research grant of the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen).

ministry of finance of the foreign country (the service provider). As will be described further in this paper, the service provider has to verify the identity of both the delegator and the delegatee and validate the mandate. The delegatee, who has to authenticate himself towards the service provider, might originate from the same country as the delegator.

We demonstrate, under the assumption that a federated identity management system is in place, that different forms of delegation are possible across contexts. Identity federation includes the ability for a citizen to authenticate himself towards service providers in different contexts, and therefore a foreign service provider. With the European directive on electronic signatures [ESI00] every European citizen is, in theory, able to also authenticate documents or arbitrary data, because these signatures should be accepted in all Member States of the EU. This implies a legal support for cross-context delegation. Note that we focus on a group of entities, acting across different contexts, delegating their privileged actions in one specific domain.

Related work. In literature [WO06, CK06, ZAC03, WK05], delegation has extensively been studied for role based access control (RBAC) systems. The purpose of this paper is to present delegation, independent of the underlying context and open to other systems. It can make use of, but is not limited to RBAC.

Our approach requires that a delegator is able to authenticate data. Without loss of generality, we will assume that digital signatures are used to provide this authenticity. In our schemes, delegation will be represented in the form of a token that shows similarities with attribute certificates, like those introduced by Farrell and Housley [FH02], or SPKI certificates as described by Ellison et al. [EFL$^+$99]. The focus of this work, however, is on the processes of their issuance, acceptance, revocation and invocation, where Francis and Pinkas [FP06] suggested extensions for attribute certificates to include policies.

Gomi et al. [GHHF05] presented similar work. They developed a delegation framework for federated identity management for Web Services based on RBAC in which privileged actions are transferred in a SAML (Security Assertion Markup Language) assertion. Their model requires the presence of a delegation authority and an authentication authority. The scope of our work is more generic and much more user-centric. We present advanced schemes that include acceptance and revocation procedures, which may be required from a legal point of view. One of our schemes applies to business contexts where policies become important.

Organization. First we discuss a basic scheme for delegation in section 2. The more advanced delegation mechanisms are based upon this basic scheme. Transferable delegation is discussed in section 3 and corporate delegation in section 4. Conclusions are drawn in section 5.

2 Basic scheme for delegation

Delegation requires at least two procedures: issuance and invocation. Commonly, a revocation procedure is also needed. Optionally, acceptance of the mandate can be required.

One of the most common forms of delegation is agency, whereby the delegatee has the obligation to perform legal acts in name of the delegator. This implies the acceptance of the mandate. In practice, the required acceptance of the mandate will be evaluated on a case-by-case basis. The possible steps for acceptance are mentioned below, but as an option that can be omitted if formal acceptance of the mandate is not required.

2.1 Issuance

The delegator gives or shares one or more of his privileged actions, under a set of restrictions, to or with a delegatee, who can invoke the privileged action in the name of the delegator. These restrictions may impose limits on the time frame in which the delegatee can invoke the privileged action (validity period) or determine from which specific service providers (SP) a service may be requested. Mandate issuance includes three steps as shown in Figure 1: privileged action selection, mandate construction and forwarding to the delegatee.

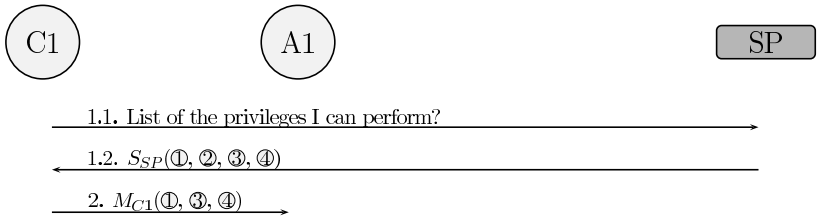


Figure 1: Delegator C1 issues a mandate to delegatee A1 for use with service provider SP

Privileged action selection. Consider the following example. The delegator goes to the tax declaration service provider and asks for a list of his privileged actions. The delegator needs to authenticate himself to obtain this list. The service providers sends the following authenticated list: (1) submit the taxation form, (2) view previously submitted forms, (3) calculate the amount to pay and (4) receive notifications. The delegator selects, for instance, privileged actions (1), (3) and (4). This prevents the delegator to delegate privileged actions he is not entitled to execute.

More in general, if privileged actions are specific to a particular service provider, the service provider has to be referenced for each privileged action in the mandate. If privileged actions are domain specific, a reference to a list of domain specific privileged actions needs to be included in the mandate. It is possible to specify in the constraints the set of service providers to which the use of the mandate is limited.

Mandate construction. A mandate is a token containing information about forwarded privileged actions, the identities of both the delegator and the delegatee, the validity period, the optional constraints and optionally a reference to a mandate authority (for revocation purposes). It is implicitly assumed that the mandate is authenticated by the delegator, e.g., by means of a digital signature created with the delegator's eID card.

The start date of the validity period is the creation date of this mandate or somewhere in the future. The mandate becomes automatically invalid after its expiration date. The delegator can define further constraints, but the mandate is only valid if all constraints are met. The constraints need to be understandable by the service provider and by the delegatee.

Mandate forwarding. The delegator sends the constructed mandate to the delegatee.

2.2 Acceptance

Depending on the context in which the mandate will be used and the context-specific legal requirements, a delegatee needs to accept the given mandate before it is formally valid. This procedure is depicted in Figure 2 and consists of two steps, namely, notification of acceptance and proof of acceptance. A system constraint could be that a given mandate can be accepted only once. Furthermore, it can be required that the mandate should be accepted within a certain timeframe after issuing the mandate, e.g., two weeks, otherwise the mandate would automatically become invalid.

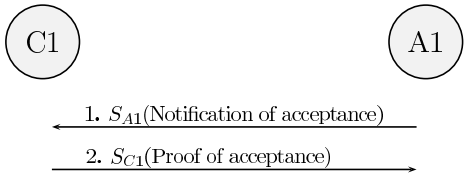


Figure 2: Delegatee A1 accepts the mandate given by delegator C1

Notification of acceptance. The delegatee expresses the acceptance of a mandate by means of a notification of acceptance. Before accepting a mandate, the delegatee validates the mandate. The notification of acceptance needs to be authenticated by the delegatee.

Proof of acceptance. After receiving a notification of acceptance and validating its authenticity, the delegator issues a proof of acceptance to the delegatee. It is also the responsibility of the delegator to make sure that the mandate has been accepted within the specified timeframe after issuing the mandate, if any. The proof of acceptance contains a reference to the mandate and is authenticated by the delegator. The delegatee can present this proof of acceptance to the service provider to prove that he has accepted the mandate and that the delegator was notified.

2.3 Revocation

A mandate authority is a trusted third party that provides genuine information about mandates. The mandate authority keeps track of all revoked mandates and publishes the corresponding list on a daily basis. This list is called a mandate revocation list (MRL). This list may also contain additional information such as acceptance of mandates (cf. supra). If a service provider needs more up to date information on the status of a specific mandate or if constraints require it, the service provider can use an online mandate status protocol (OMSP, which would be a trivial extension of the OCSP [MAM+99]) to query the status of a particular mandate, if this service is available at the mandate authority.

The MRL is signed by the mandate authority and contains a list of references to all revoked mandates. References to revoked mandates that are no longer valid due to the expiration of their validity period, are removed from the list. Instead of downloading the whole list, it should be possible to only get references to revoked mandates since a given published MRL. This list is called the delta-MRL (ΔMRL). Both MRL and ΔMRL are trivial extensions of CRL and ΔCRL [HFPS99].

If no revocation mechanism is available, a mandate can become invalid, e.g., if it does not satisfies certain constraints, without its proof of acceptance, or if the validity period expires shortly. An MRL should not be used if the validity period of a mandate is of the same order of frequency as that by which the mandate authority publishes the MRL, e.g., once a day.

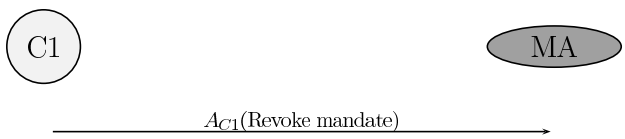


Figure 3: Delegator C1 revokes his mandate given to delegatee A1 at the mandate authority MA

Revocation is depicted in Figure 3. The delegator should be able to revoke a given mandate at any time. The mandate authority must be able to check the authenticity of the request to revoke the mandate. This can be done either by setting up an authentic connection between the two, e.g., by verifying the delegator's digital signature on the request. An authentic connection implies mutual authentication of the sender and receiver of information.

2.4 Invocation

After having received a mandate, the delegatee can use the mandate to invoke a service in the name of the delegator. This procedure includes three steps, shown in Figure 4: service request, verification and service provisioning.

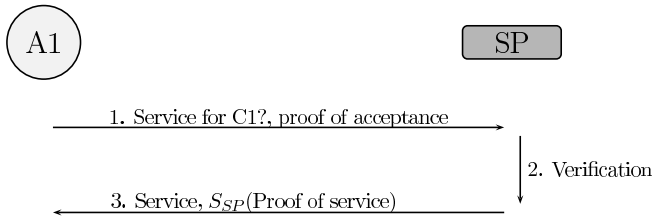


Figure 4: Delegatee A1 invokes a privileged action of delegator C1 at service provider SP

Service request. The delegatee requests a service in the name of the delegator at the service provider. The delegatee sets up an authentic connection with the service provider. Together with the request for service in the name of the delegator, the delegatee provides the given mandate and the proof of acceptance.

Verification. The service provider checks if the mandate is valid for the requested service by verifying that (in the following order):

1. The mandate is presented within the mandate's validity period;
2. The service requester is the delegatee specified in the mandate;
3. The mandate has not been revoked;
4. The digital signature on the mandate is correct and the delegator's public-key certificate has not been revoked, for instance, this might be the case when a delegator gets a new eID card;
5. The delegator is authorized to invoke the delegate privileged actions;
6. The delegatee is authorized to receive the mandate, which depends on the context;
7. The mandate has been accepted, where relevant, the signature on the proof of acceptance is correct;
8. The optional constraints are met.

Service provisioning. If the mandate is a valid mandate for the requested service, the service is provided and the service provider logs this event. The delegatee receives a proof of service, signed by the service provider. This proof can be used by the delegatee to defend himself in case of a dispute. The proof should be checked by the delegatee at the moment he receives it. At any time, a delegator may wish to query the service provider about the delegatees and the services rendered to them using a particular mandate issued by this delegator.

2.5 Alternatives

We now present some variations of the basic scheme in which some of the steps are slightly modified, extended or replaced with alternatives.

Anonymous delegation. An identity provider can be used where anonymous delegation is desired. An identity provider creates, maintains, and manages identity information for entities and may provide entity authentication services to service providers. The identity provider creates opaque handles for each delegator-delegatee relation (see also [GHHF05]). The service provider uses an opaque handle instead of the identity of the delegatee and trusts the identity provider. The service provider needs to know on whose behalf the delegatee is invoking a privileged action, hence the identity of the delegator must be known.

A user-centric privacy-preserving delegation protocol was proposed by Wohlgemuth and Müller [WM06]. It is based on anonymous credentials and used within the context of business processes where a proxy mediates between users and service providers.

Acceptance by mandate authority. The mandate authority now also needs to keep track of mandates that have not yet been accepted. References to mandates that have not yet been accepted are also put on the MRL, which now includes an additional field indicating the status of the mandate. Before handing out the mandate to the delegatee, the delegator registers the mandate at the mandate authority. The mandate authority sets the status of this mandate to ”acceptance pending.” The delegatee accepts the mandate by sending a notification of acceptance to the mandate authority. The mandate authority changes the status of this mandate to ”accepted.” In this case, there is no need to any longer issue a proof of acceptance.

Acceptance by mandate authority requires less effort from all participating parties. The delegator does not need to confirm the acceptance, the delegatee does not need to send the proof of acceptance when requesting a service and the service provider can check the status of the mandate (”revoked,” ”accepted,” ”acceptance pending”) in one step.

Acceptance revocation. If acceptance of a mandate implies the obligation to perform legal acts, it should also be possible for the delegatee to revoke acceptance of a mandate. This can only be done when a mandate authority registers the acceptance of the mandate.

Mandate issued by mandate authority. Instead of the delegator issuing a mandate, all mandate information can be given to the mandate authority. The mandate authority will issue the mandate and registers acceptance. All information is checked prior to the mandate’s issuance to prevent circulation of invalid mandates. The delegator does not need to have a private key to sign the mandate. Electronic mandates issued by a mandate authority have been implemented in Austrian eGovernment [RH05].

Delegation assertion. Instead of a mandate, delegation assertions can be used. All information about the mandate is kept central at the mandate authority, making the mandate more flexible. The mandate can be updated dynamically, without having to revoke the mandate and issue a new one with updated constraints. Upon request of the delegatee, the mandate authority hands out a delegation assertion, which must be used in a short time frame, e.g., an hour. If the request is valid, the delegatee receives a delegation assertion that can be used to invoke a particular privileged action. This drastically reduces the complexity of checking a mandate for the service provider.

When using delegation assertions, a procedure for mandate acceptance might not be necessary. A request by the delegatee for a delegation assertion can be viewed as implicit mandate acceptance. In certain cases it might still be necessary for the delegatee to formally accept the mandate.

3 Transferable delegation

Transferable delegation extends the basic scheme for delegation with the possibility for delegatees to delegate the received privileged actions further to someone else.

3.1 Issuance

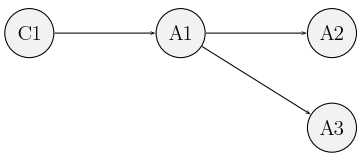


Figure 5: Subdelegator A1 delegates to delegatee A2, the mandate he received from original delegator C1. Optionally, A1 delegates the same mandate to another delegatee A3

A sub-delegator wants to delegate another delegatee (a subset of) the privileged actions in the mandate given by the original delegator (see Figure 5). The original delegator specifies in his mandate the maximum allowed delegation depth. This limit puts an upper bound on the length of the delegation path. The default value is zero, meaning that further delegation is not allowed. When delegating further the value of the maximum allowed delegation depth has to be decreased. If delegation depths are relevant, it is the responsibility of the service provider to check their consistency. Alternatively, the maximum allowed delegation depth can be replaced by a boolean value indicating whether or not further delegation is allowed without specifying an actual maximum depth. In addition, the original delegator can specify extra conditions.

Because a sub-delegator can delegate the same mandate to multiple delegatees, the original delegator might specify a cardinality to introduce an upper bound on the total number

of delegatees. The original delegator can, for instance, specify that only three people are allowed to possess a set of privileged actions, contained within his mandate. The cardinality can only be enforced by a mandate authority that hands out mandates or delegation assertions.

On top of the conditions for a mandate to be valid, as described for a basic scheme of delegation in section 2.4, following conditions need to be satisfied:

9. The new mandate must refer to the original mandate(s);
10. The conditions for further delegation on all the original mandates must be met, e.g., the new mandate is invalid if these conditions specify that two or more privileged actions from the original mandates, referenced by the new mandate, can not be combined;

The original delegator should be informed about the transfer of his mandate. Without a mandate authority controlling the creation of new mandates, it is impossible to enforce notification to the original delegator.

3.2 Revocation

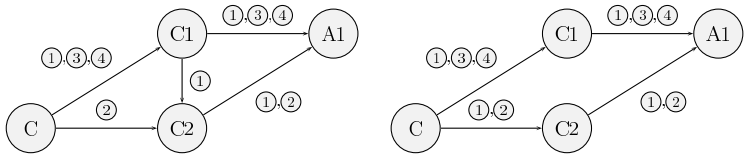
The original delegator wants to revoke the mandate given by a sub-delegator to a particular delegatee, without revoking any other mandates handed by the sub-delegator. Delegation assertions allow direct revocation of a particular mandate by simply informing the mandate authority. When mandates are used, the original delegator can not directly revoke a particular mandate from the sub-delegator. He can revoke his mandate to the sub-delegator, automatically making all further delegation based on this mandate invalid. Afterwards the original delegator issues a new mandate to the sub-delegator with additional restrictions to exclude particular delegatees.

3.3 Invocation

Upon invocation of a privileged action supported by a mandate, all mandates in the delegation path need to be validated. Delegation assertions allow further delegation without increasing the effort required from the service provider to validate the request.

3.4 Overlapping delegation

We present a special case that can result as a consequence of transferable delegation: overlapping delegation. It is possible to receive the same privileged action(s) from two different sub-delegators (see Figure 6). Recall that a privileged action is the right to perform a **certain** action for a **certain** entity.



(a) C1 and C2 are grant-connected (b) C1 and C2 are not grant-connected

Figure 6: Overlapping delegation

Conflict resolution [RV03] may become necessary, as both positive and negative authorizations are allowed. The positive authorizations are in the form of mandates, the negative are in the form of the revocation or invalidation.

If the sub-delegators are not grant-connected for a particular privileged action to each other, i.e., the sub-delegators did not receive the right to perform the privileged actions from one another, negative authorizations do not prevent invocation of a privileged action as long as one positive authorization is available.

When the sub-delegators are grant-connected, a conflict may occur. Revocation of a mandate directly given to a delegatee does not imply invalidation of indirect mandates containing the same privileged actions. To solve this conflict, a negative authorization needs to be propagated in all mandates that potentially create a positive authorization by further delegation. This is trivial when delegation assertions are used.

4 Corporate delegation

Corporate delegation (see Figure 7) builds on a basic scheme for delegation and incorporates transferable delegation where necessary. The legal entity of a company and its policies are manifested by the board of directors. The daily management of the company is done by an executive management team. The executive management team is appointed by the board of directors. The board of directors gives mandates to the executives to handle certain tasks on behalf of the company and to delegate some of their privileged actions further to employees in their division. Under certain conditions and approval of some of the board members the executive can be allowed to delegate some of his privileged actions to someone outside his division or company.

The rules for corporate delegation are defined through a company's delegation policy, which is defined by the board of directors. For example, the chief financial officer is able to deal with the tax administration on behalf of the company. The company's delegation policy might dictate that if he wants to delegate these privileged actions to an external accountant, he must get at least two members of the board to approve this delegation.

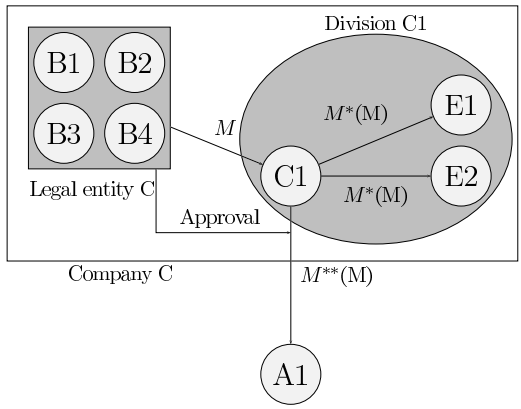
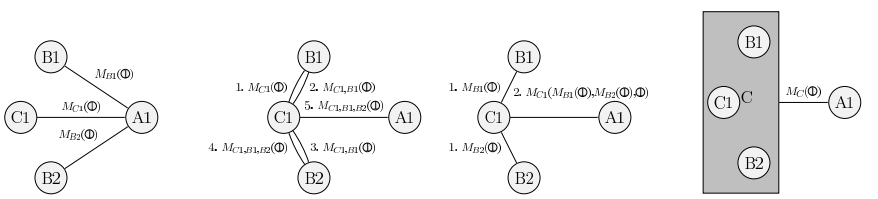


Figure 7: Corporate delegation. Board members B1 till B4 mandate executive C1, who further delegates to employees E1 and E2 of his division, or to an employee A1 of an external firm.

4.1 Issuance

The issued mandates need to comply with the company's delegation policy. The delegation policy can be enforced implicitly by internal procedures that ensure that only mandates, with the proper restrictions, in accordance with the delegation policy of the company, are handed out. Mandates that have already been issued are unaffected by changes in the delegation policy. Explicit enforcement requires publication of the delegation policy in a publicly known location or in a location referenced by the mandate. Changes in the policy also affect the already issued mandates. Infringements on the company's delegation policy are made impossible as opposed to being detected afterwards, as is the case with implicit policy enforcement. To ensure interoperability, a universal policy format needs to be established. Otherwise a service provider (or mandate authority) is unable to parse the content and check the constraints.

Figure 8 shows different possibilities for issuing a mandate without a mandate authority. The last three options result in a single mandate. These possibilities are now discussed in more detail. Following notation is used in the figure: $M_A(1)$, a mandate created and signed by A for privileged action 1; $M_A(M_B)$, a mandate from A containing a mandate from B.



(a) No changes (b) Multiple signatures (c) Embedded mandates (d) Corporate certificates

Figure 8: Mandate issuance for corporate delegation without mandate authority

(a) No changes. The chief financial officer hands out a mandate to the delegatee. The board members approve this delegation by issuing mandates directly to the delegatee. For implicit policy enforcement, each mandate should at least specify in the constraints that in order for the mandate to be used, the delegatee should also have a mandate from two other members of the board.

(b) Multiple signatures. The chief financial officer hands out a single mandate to the delegatee after he got the approval from some of the board members. The board members approve this mandate by signing it.

(c) Embedded mandates. The mandate format is changed in order to embed mandates from some of the board members. The advantage of collecting multiple mandates over multiple signatures, is that the mandates can be created in parallel.

This case is quite different from transferable delegation with privileged actions from different mandates combined in a new mandate. Each included mandate allows a set of privileged actions. In corporate delegation only the collection of all included mandates allows certain privileged actions.

(d) Corporate certificates. The existing public-key infrastructure for natural persons can be extended to give corporate bodies a way of digitally manifesting their identity as a company. A certification authority issues a corporate certificate to the company, which is responsible for managing the private key that corresponds to the public key in the certificate. It is a good practice to divide the key among the board members and to use a threshold signature scheme to sign mandates or the company's delegation policy. In a (t, n)-threshold signature scheme, there are n participants that receive a share of the private key and at least t of them need to cooperate to create a signature. This threshold signature scheme can be part of an (implicit) implementation of the company's delegation policy. Corporate certificates make validity checking easier, instead of multiple signatures from the board members only one signature needs to verified, and they allow explicit policy enforcement. They prevent reissuance of mandates when the members of the board vary. Shares are stored on tamperproof tokens and leaving members hand in their token.

Mandate authority and delegation assertions. As an alternative to the above settings, each board member passes the information about his mandate to a mandate authority, who combines this information and issues a single mandate. A company could set up its own mandate authority. A service provider may then require external certification of that authority before trusting it.

Instead of issuing a mandate, the mandate authority may inform the delegatee about the possibility to request a delegation assertion. The mandate authority will enforce the company's delegation policy when the assertion is requested and the policy no longer needs to be published.

4.2 Revocation

In corporate delegation, a minimum of t board members has to give their consent to allow an executive to further delegate some of his tasks and privileged actions. As long as the required minimum number of board members supports a mandate it remains valid. In theory, a mandate only becomes invalid if less than t board members give up their support for the mandate. Unfortunately, this can only be enforced explicitly when a mandate authority issues delegation assertions or when board member mandates are embedded. In all other cases, the mandate needs to be revoked directly, either by the executive who issued it or by a certain number of board members if the policy allows it. As soon as less than t board members support the mandate, the mandate is irreversibly revoked. When t or more board members again agree on supporting the mandate, a new mandate is issued, because allowing a revoked mandate to become valid again, would create legal uncertainty. For example, if the delegatee would use the mandate during the grace period, i.e., between the moment of revoking and the time of actual revocation, the implications of privileged actions that have been performed during and after this grace period may be contested.

With implicit delegation policy enforcement, there is no way for the service provider to know whether or not the mandate is compliant with the company's delegation policy. When changes are made to the policy it may be necessary to revoke certain mandates and issue new ones.

If the corporate certificate is revoked, the mandates that have not yet been verified and were signed with the private key of the corporate certificate become automatically invalid. If the private key is only used to sign the company's delegation policy, the mandate remains valid if it is signed with the new private key and published in the same location as before.

4.3 Invocation

Invocation of privileged actions in the corporate delegation scheme is basically the same as in the previous schemes. For explicit mandate policy enforcement, the service provider needs to check if the delegation policy is available and consistent with the mandate.

5 Conclusion

We have presented a basic scheme for delegation and schemes for transferable and corporate delegation. Different settings are possible depending on the presence of a mandate authority and the form in which delegation manifests itself, i.e., a mandate or an assertion.

Individual mandate issuance is the simplest form of the delegation. The presence of a mandate authority makes revocation possible and facilitates mandate acceptance. Assertions come at a higher cost and demand a higher level of trust in the mandate authority.

The complexity of mandates in transferable delegation, rapidly increases. The flexibility

of the delegation assertion and the guaranteed correctness are two important arguments to choose for delegation assertions in this context. Corporate delegation is even more complex and again delegation assertions reduce the complexity. To achieve explicit policy enforcement and to allow dynamic updates of the delegation policy, assertions are required.

References

[CK06] J. Crampton and H. Khambhammettu. Delegation in Role-Based Access Control. In *ESORICS*, pages 174–191, 2006.

[EFL+99] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen. SPKI Certificate Theory. RFC 2693, 1999.

[ESI00] 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.

[FH02] S. Farrell and R Housley. An Internet Attribute Certificate Profile for Authorization. RFC 3281, 2002.

[FP06] C. Francis and D. Pinkas. Attribute Certificate (AC) Policies Extension. RFC 4476, 2006.

[GHHF05] H. Gomi, M. Hatakeyama, S. Hosono, and S. Fujita. A Delegation Framework for Federated Identity Management. In *DIM '05: Proceedings of the 2005 workshop on Digital identity management*, pages 94–103, New York, NY, USA, 2005. ACM Press.

[HFPS99] R. Housley, W. Ford, W. Polk, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459, 1999.

[HV07] X. Huysmans and B. Van Alsenoy, editors. *Glossary of terms, v1.07*. IDEM project, 2007. https://projects.ibbt.be/idem/index.php?id=161.

[MAM+99] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560, 1999.

[RH05] T. Rössler and A. Hollosi. Elektronische Vollmachten. In *Proceedings of the eGOV Days 2005, Vienna, Austria*, pages 27–34, 2005.

[RV03] C. Ruan and V. Varadharajan. A formal graph based framework for supporting authorization delegations and conflict resolutions. *Int. J. Inf. Sec.*, 1(4):211–222, 2003.

[WK05] J. Wainer and A. Kumar. A fine-grained, controllable, user-to-user delegation method in RBAC. In *SACMAT '05: Proceedings of the 10th ACM symposium on Access control models and technologies*, pages 59–66, New York, NY, USA, 2005. ACM Press.

[WM06] S. Wohlgemuth and G. Müller. Privacy with Delegation of Rights by Identity Management. In Günter Müller, editor, *ETRICS*, volume 3995 of *Lecture Notes in Computer Science*, pages 175–190. Springer, 2006.

[WO06] H. Wang and S.L. Osborn. Delegation in the role graph model. In *SACMAT '06: Proceedings of the 11th ACM symposium on Access control models and technologies*, pages 91–100, New York, NY, USA, 2006. ACM Press.

[ZAC03] L. Zhang, G.-J. Ahn, and B.-T. Chu. A rule-based framework for role-based delegation and revocation. *ACM Trans. Inf. Syst. Secur.*, 6(3):404–441, 2003.