

Scalability Issues in PMI Delegation

Scott Knight

Royal Military College of Canada

knight-s@rmc.ca

Chris Grandy

NDHQ/Directorate of National Information Systems (DNIS)

grandy.cc@forces.ca

Abstract

The Canadian Department of National Defence (DND) is shifting its methods for the delegation and exercise of authority from paper-based to electronic-based means. DND has deployed a commercial PKI but there is no general technical solution presently employed by DND for access control or electronic authorization of workflow in distributed processing environments. The aim of this research is to show how an authorization system, or privilege management infrastructure (PMI), can be used to support business processes DND. The results are expected to be applicable to large enterprises in general.

The research demonstrates how ITU-T standard X.509 can be used to support DND authority and delegation models. The investigation involves the analysis of the key authorizations within a specific DND problem domain. The X.509 standard and concepts from role-based access control form the basis of the PMI design. This involves the use of attribute certificates to control the specification and delegation of privileges. A novel interpretation of X.509 attribute certificates is proposed that provides separate hierarchies of responsibility for the management and delegation of roles. The results provide insight into, and quantification of, the complexity of the resulting delegation chains. The use of a roles based model for delegation is seen as being important to the scaling of PMI to service large enterprises with mature, complex authority structures. If the processing complexity can be managed, the flexibility of being able to model the actual privilege delegation paths in an organization is an advantage of a role-based model.

1. Introduction

Public-key infrastructure (PKI) has matured into a commercially supported, deployable technology. With a high degree of assurance current PKI products offer secure, reliable security services to support identification, authentication, confidentiality, and non-repudiation. These are powerful services but the adoption of PKI in enterprise environments has been slow. It is the opinion of the authors that wider proliferation of PKI will come with the ability to provide effective support for authority structures within an enterprise. The authority structures within an enterprise govern business process. Every legitimate task is performed under the approval of some authority that has ultimate responsibility for that part of the business process. In many cases there is a requirement that the entities performing a task must have the appropriate approval, or privilege, to do so. An attribute-certificate based privilege management infrastructure (PMI) is a mechanism that can be used to

support enterprise authority structures. Attribute-certificate based PMI is an aspect of PKI and requires underlying services for the management of public-key certificates (PKCs). To this extent the proliferation of PMI can lead to more wide spread adoption of PKI. Although there are standards that define PMI services [X.509], and some commercial products that provide support, there is little attention in the literature paid to the issues of scalability in an enterprise environment. Also, there do not seem to be examples of attribute-certificate deployment models to support business process. This work examines these issues by proposing a PMI model to support authority structures in the Canadian Department of National Defence (DND).

DND has deployed a commercial PKI to be used to support the Government of Canada policy on Electronic Authorization and Authentication [Gov96]. The PKI is intended to support a variety of new systems and legacy systems, and to provide a unified mechanism for managing task authorization.

An attribute-certificate based PMI model is used to explore the complexity of the certificate chains that need to be verified when exercising privilege. The resulting certificate chains are quite complex and some chain pre-processing strategies are discussed to reduce the real-time privilege verification overhead.

This work is an extension of [Gra01]. Although the model discussed here pertains to DND it is believed that the work is relevant in a broader context and reflects authority structure and business process issues in large organizations in general. The rest of the paper is organized as follows. Section 2 reviews the significance of privilege management in the context of supporting an organization's security policy. An overview of privilege management within DND is presented in Section 3 to provide the context for the development of a role-based authorization model. Complexity issues arising from the model are discussed in Section 4. Finally, Section 5 concludes the paper and discusses further work.

2 Support Mechanisms for a Security Policy

In defining security policy the classic literature defines three security properties: confidentiality, integrity and availability. The security policy defines the access privileges a specified set of subjects have for objects in the system. The objects are the information resources that are protected by the system. In an information system the security policy is realized by implementing security mechanisms such as identification and authentication (I&A), access control, audit. Through the use of public-key certificates a PKI system can provide strong I&A support for a system. This mechanism provides good assurance of the true identity of the subjects. In most business systems there must be a determination of what kinds of access are permitted to the system objects. Currently access control and the format of the authorization database is application specific (stovepipes) and there is no unified way to deal with permission. A standard mechanism for the support of access control decisions can provide more complete support for security policy at the enterprise level. This support can be provided by attribute-certificate based PMI and the development of such mechanisms may lead to greater proliferation of PKI in general.

The authority structures in a specific enterprise environment have evolved over a period of time and represent efficiencies in the command and control of the organization. This is the case with the DND case study being examined. It seems reasonable to expect that the PMI would support the organization's authority

structures and business process, and not expect that the organization would have to make large changes to its authority structures and business process to adapt to the PMI mechanisms.

2.1 Attribute-certificates

X.509 public-key certificates have some support for privilege management through the use of subject attributes. However in the following cases it is recommended that attribute-certificates are the more suitable mechanism [X509]:

- a) a different entity is responsible for assigning particular privilege to a holder than for issuing PKCs;
- b) there are a number of privilege attributes to be assigned to a holder, from a variety of authorities;
- c) the lifetime of a privilege differs from that of the holder's PKC validity;
- d) the privilege is valid only during certain intervals of time which are asynchronous with that user's PKC validity or validity of other privileges; or
- e) delegation of authority is permitted, and for any specific delegation there may be differences in the kind of privilege that the delegating authority passes down to the delegated authority.

All these conditions are true in the case of the DND example. In complex inter and intra-organizational relationships, it makes more sense to manage authentication separately. It is reasonable to expect that PKC authorities will not have jurisdiction over privileges that are solely the domain of the process owner. One would expect this will become the rule rather than the exception as the market encourages the emergence of commercial CA services and PKI outsourcing providers [WH99].

It is also the case that the authority structures of the example environment have evolved to be heavily role-based. For example, a member of the Canadian Armed Forces normally has a career spanning decades. Personal identification information is static for long periods during this time. The member may serve in a number of different roles (concurrently and overlapping). The privileges associated with the roles may be defined and modified by different agencies than

those assigning the member to the role. It is expected that this is not unique to the example, and that there are a large number of enterprise environments where these conditions hold. The X.509 standard provides a mechanism for managing roles. This seems to be a natural mechanism to be used to model the required authority structures. The standard warns that the “use of roles within an authorization framework can increase the complexity of path processing.” There is no indication in the standard of how complex the path processing can become, how the model will scale to larger organizations, or how the role delegation paths will effect the performance of privilege verifiers.

There are several factors that make X.509 attribute certificates (ACs) an attractive option for managing privileges. An X.509 AC can be managed in the same way as the X.509 PKC. ACs can also be digitally signed like PKCs. This authenticates the attributes and provides integrity protection so that the certificates cannot be modified. ACs are generalizations of identity certificates, PKCs (an identifier through the use of a public-key is just one of many possible attributes), and have naturally evolved from them [Bra00]. ACs are digital certificates that serve primarily to enable verifiers to establish attributes other than the identity of the key holder (such as access rights, authorities, adherence to standards, legal requirements, privileges, permissions, capabilities, preferences, assets, demographic information, and policy specifications). An authorization service, PMI, can be designed using attribute certificates which each point to a PKC. More comprehensively, a PMI includes people, policies, hardware and software interacting together to bind privileges to a user by issuing him attribute certificates

[Ada99].

Because a PMI depends on the authentication provided by a PKI, a PKI must be available before a PMI can be implemented. Since ACs do not provide authentication, one cannot assign privileges to a user using attribute certificates if that user does not have at least one associated PKC.

The standard specifies that a privilege holder must present an attribute-certificate (AC) containing the appropriate attributes/privileges to a privilege verifier before access is granted to an information object (i.e. the privilege holder asserts a privilege). The privilege verifier acts as a reference monitor and controls access to the object. The decision to allow access is based on the security policy being enforced by the verifier and any applicable environment variables (e.g. time of day).

2.2 Delegation

Delegation is the conveyance of privilege, from one entity that holds such privilege to another entity. The model consists of four components: the source of authority (SOA), the attribute authority (AA), the privilege holder and the privilege verifier.

The SOA occupies the highest position in the authority hierarchy. Within a PMI, the source of authority (SOA) is analogous to the root CA in hierarchical PKIs. It is different in that there may be many sources of authority (one for each privilege or set of privileges) whereas there is only one root CA in a strictly hierarchical PKI. The SOA is the issuer of certificates that assign privileges to privilege holders and is present even in

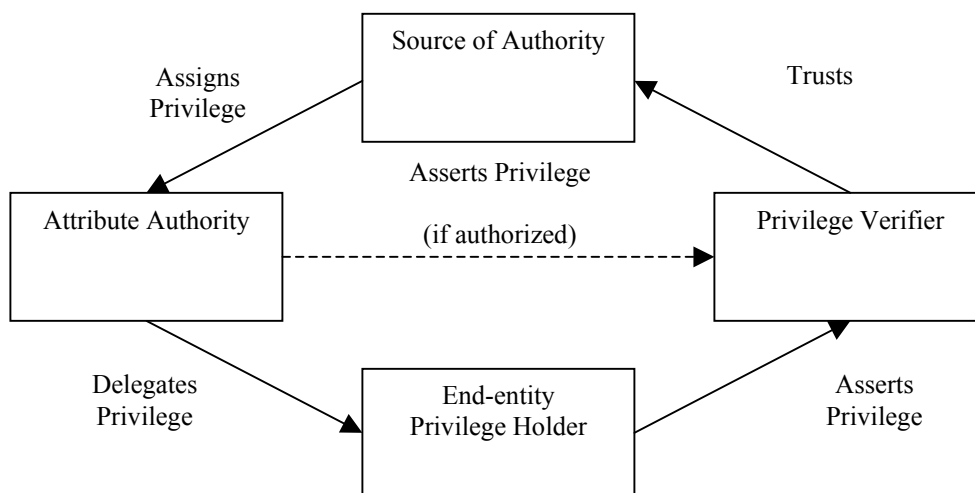


Figure 1 - The Delegation Model [Int00]

environments where delegation does not occur.

In Figure 1, the SOA authorizes an entity to act as an AA by assigning it a privilege and the authority to delegate that privilege. The AA further delegates that privilege to other AA's or end entities through the issuance of certificates that contain the same privilege (or a subset thereof). The AA is analogous to subordinate CAs within a PKI, but a CA issues public-key certificates whereas an AA issues attribute certificates. All entities that issue and obtain attribute certificates need to be authenticated; therefore, they will each require their own PKC. This means AAs will also require PKCs. Each of the intermediary AAs may, in certificates that it issues to further privilege holders, authorize further delegation by those holders also acting as AAs. The SOA may impose constraints on the re-delegation of a privilege. A delegator can also further restrict the ability of downstream AAs to delegate [Int00]. A universal restriction on delegation, known as the domination rule, is that no AA can delegate more privilege than it holds [Int00].

The privilege verifier trusts the SOA as the authority for a given set of privileges for the resource. Also, when delegation is used, the privilege verifier trusts the SOA to delegate some or all of those privileges to other holders. If the privilege asserter's certificate is not issued by the SOA, then the privilege verifier must locate a delegation path of certificates from that privilege asserter to the SOA. The validation of that delegation path must include checking that each AA had sufficient privileges and was duly authorized to delegate those privileges.

Processing an attribute certificate path in PMI is analogous to processing other certificate paths within a PKI. Validation is conducted with respect to attribute authorities rather than certification authorities, and the information pertains to privileges rather than identity. However, with privilege path processing, the processing engine will need to consider elements of both the PMI and the PKI in the course of determining the ultimate validity of a privilege asserter's attribute certificate. With respect to PKI, the privilege verifier must verify the identity of every entity in the path using the certification path processing procedure identified in the X.509 standard [Int00]. For example, a referenced public-key must be checked for its validity before the digital signature on an attribute certificate can be verified.

Privilege path processing relies on the elements of PMI to establish a valid delegation path. The central requirement is to ensure that each entity in the path has the authority to delegate privileges to the entity below.

The delegation path is distinct from the certificate validation path used to validate the public-key certificates of the entities involved in the delegation process. The attribute certificates within the path must still be digitally signed by the corresponding authority. The delegation path represents a chain of trust between the privilege asserter and the SOA.

Figure 2 provides a general illustration of the privilege processing checks used to establish a chain of trust back to the SOA. The privilege verifier is presented with an AC, EE-AC, belonging to an end-entity, EE. EE-AC might pertain to access to some resource. In order to verify that EE has legitimate possession of EE-AC the verifier must verify the signature on the certificate to ensure it actually was created by the issuer named on the certificate. In this case the issuer is AA1. To ensure that AA1 legitimately holds the relevant privilege the verifier must retrieve the AC that is owned by AA1. AA1-AC is the certificate that allocates privilege to AA1; it is issued by AA2. AA1-AC must also have its signature verified. AA2 may or may not be directly trusted by the privilege verifier for the required attributes. If not, the privilege verifier may have to retrieve another AC (e.g. AA2-AC) until it finds one issued by a directly trusted AC issuer (SOA) for that privilege.

Once a valid chain has been confirmed, the privileges contained in that attribute certificate may be used to make an access control decision. The attributes are compared with the relevant privilege policy and other information associated with the context in which the certificate is being used. It must be determined if the privilege holder actually intended to assert the contained privileges for use with that context. The fact that a chain of certificates to a trusted SOA exists is not enough. The willingness of the privilege holder to use that certificate has to be clearly indicated and verified. The standard does not specify this application-dependent mechanism.

The issue of certificate revocation complicates this process. For the purposes of this paper we will consider certificates to be short lived and the use of certificate revocation lists will not be required. A more complete treatment of this issue and the formats for the attribute certificates can be found in [Gra01].

2.3 Roles

Roles provide a means to indirectly assign privileges to entities. Providing access control based on the entity's functional role as opposed to its personal identity is a powerful concept known as Role-based Access Control

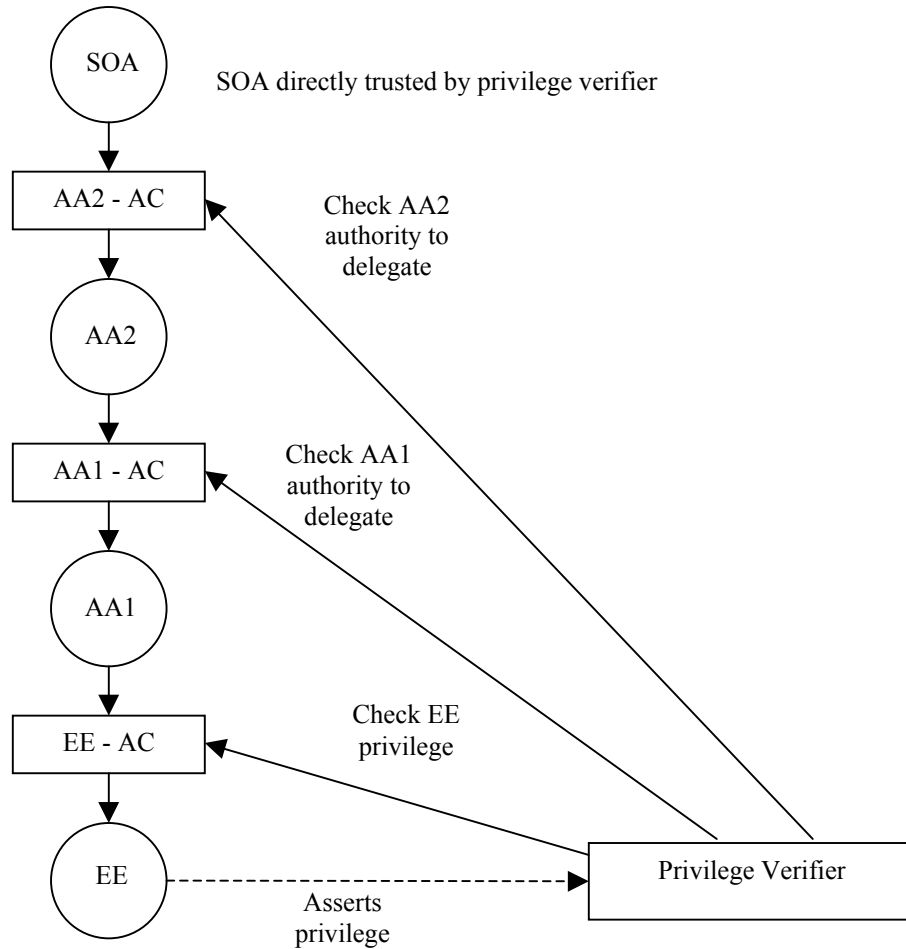


Figure 2 - Chaining attribute certificates

(RBAC). RBAC is a useful approach because it can reflect the authority structures within an enterprise. The basic role model described in the X.509 standard consists of two types of ACs. Specific privileges associated with a particular role are specified within Role Specification Certificates (RSCs). Entities are assigned to the role (specified by the RSC) via another attribute certificate called a Role Assignment Certificate (RAC). The de-coupling of privilege assignment to roles, from the role assignment to individuals allows privileges to be updated without affecting the assignment of the roles.

3 Authorizations in the Problem Domain

3.1 A Procurement Example

Consider a familiar business transaction. Suppose a customer on a Canadian Forces Base needs to procure a

personal computer. This computer may be required because of an operational requirement and it will be connected to the Defence Wide Area Network (DWAN). This particular example is chosen for a number of reasons. Many readers will relate to this example. More importantly, the procurement requires the delegation of authority and the cooperation of several different roles.

Specific authorities and responsibilities for the control and spending of funds appropriated by Parliament for DND are conferred on the Minister of National Defence (MND) by the Financial Administration Act (FAA) and the National Defence Act (NDA). Since the MND cannot carry out these responsibilities personally, it is necessary for him to authorize officials to exercise these authorities on his behalf.

The MND is required to ensure that separate organizations or individuals are invested with spending authority and the complimentary, but completely

distinct, payment authority. This is a standard business practice for fraud protection. This requires at least two distinct delegation paths to ensure the proper separation-of-duty. Additionally the computer is required to be connected to the DWAN. This requires the approval of a network technical authority that derives its privilege from a completely separate delegation path.

As an example of delegation, the Responsibility Centre (RC) Manager plays a central role exercising spending authority. An RC Manager is anyone (military or civilian) who manages a distinct unit or organization, prepares and controls a budget, and has spending authority for his/her budget [Dep99].

It is possible to summarize a process model for this procurement process.¹ The customer, acting in the role of RC Manager, will normally recognize the need for the purchase. In this case, the requirement is for a computer. The Base Telecommunications and Information Services Officer (BTISO) role will take responsibility for specifying and describing the technical aspects of this need. The next five steps are usually performed by the section belonging to the Integrated Logistics Officer (ILogO role) based on the input from the customer and the BTISO: determining sourcing options; establishing price and terms; preparing and placing a purchase order; and following up on the order. The vendor receives the order and ships the computer along with an invoice. The customer, in his role as the RC Manager, receives the computer and confirms it matches the requirement. He then approves the invoice and submits the transaction for review to another role, the Financial Officer, who authorizes the release of funds to the vendor.

Other layers of delegation are possible. For example, the BTISO would likely delegate this authority to review and approve technical requirements to a subordinate such as the Network Maintenance Officer (NMO).

The processing of this procurement will require that the individuals filling the various roles have access to the necessary functions of the procurement system software (a legacy system). Their access must be authorized. Their decisions must enable the respective business process function and can not be repudiable. An interesting observation is that the entire transaction can

be viewed as series of authentications and authorizations.

3.2 Mapping the Requirement to Attribute Certificates

The interaction of users in the various roles in the previous section suggests that role-based access control can have tremendous relevance in establishing electronic authorization for business process. RBAC takes the approach that authorizations are distributed according to role rather than identity. The process model clearly revealed that roles can be effectively used to conduct a local procurement transaction.

The style of RBAC proposed by the X.509 roles model, and summarized in section 2.3, can be applied to this procurement example. Individuals could be assigned a role assignment certificate matching one of the procurement roles e.g. BTISO, ILogO, NMO. These role assignment certificates could point to a corresponding role specification certificate containing the key authorizations, or privileges.

A complete design in support of this procurement example will not be described here. The intent here is to demonstrate the application of the X.509 standard to this problem, and not to stipulate all the details of a specific design. The portions of the design described in this work are sufficient to support the modeling scheme. Addressing every role in the process is not only time-consuming, but also unnecessarily repetitious. As much insight can be gained about the specification, assignment and delegation of privileges by investigating one role as by examining them all. Therefore, only the BTISO role will be explored in detail. The technique is completely analogous for the other roles, such as the ILogO and the Finance Officer.

3.2.1 Extending the X.509 Roles Model

The BTISO typically requires more privileges than just those needed to participate in a local procurement transaction. He would also likely be the COMSEC Custodian for the Base Crypto Account, the local configuration authority for connections to the DWAN, and, like many other managers (such as the customer in this procurement example), an RC Manager responsible for his own budget. While the details of these privileges are unimportant here, it is likely that the privileges associated with these other duties originate from different sources of authority. Unfortunately, the X.509 standard offers no direct guidance for dealing with complex roles

¹ A complete process model for the procurement was completed and is available at [Gra01].

The design in this paper employs a novel interpretation of the roles model described within the X.509 standard. The standard suggests using the role attribute within a role assignment certificate to point to a single role specification certificate where all the privileges are held. The new interpretation builds upon this idea by proposing that the role specification certificate can itself contain role attributes, each pointing to another role specification certificate.

Convenience was considered important in this design. Otherwise, the attraction of using a certificate-based PMI would fade for those wishing to apply it to complex organizations and roles. The BTISO role in the procurement example is quite common in DND; many of the privileges and responsibilities associated with the role are not unique to a particular Base. The same is true for the other positions. It would be convenient if the same role design could be reused wherever a BTISO position exists. DND is an dynamic organization that demands managers to adapt to unfamiliar work environments in short periods of time. It may be asking too much to expect an infantry Colonel, newly appointed as a Base Commander, to understand PMI and all the privileges required of his BTISO. Sending him on a “shopping trip” for privileges at the various SOAs, besides wasting time, will likely yield incomplete and unsatisfactory results. Convenience, therefore, also suggests that a Base Commander should be able to appoint someone to a position, such as a BTISO, by simply issuing him a single role assignment certificate.

Think of the BTISO role as a super-role encompassing the privileges held by a BTISO. Smaller, more specific roles, such as COMSEC Custodian, DWAN Configuration Control Officer and RC Manager, can be thought of as sub-roles comprising the super-role.

Viewing complex roles in this way offers several advantages. The most obvious convenience is that it allows complex roles, or super-roles, to be quickly and easily constructed by simply combining more elementary roles. Designers of the role specification certificate for the super-role can quickly gather many of the necessary privileges by inserting pointers to role specification certificates for the sub-roles.

Reuse is another observable benefit. The number of attributes that have to be developed exclusively for the role of BTISO can be minimized since many of the necessary attributes already exist within the recognized sub-roles. Of course, this can be a double-edged sword. Each role will have to be carefully inspected to ensure that a super-role does not inherit privileges that are part of the sub-role, such that the super-role acquires

privileges it is not entitled to. Nonetheless, a single role specification certificate can be reused by several super-roles. The BTISO needs spending authority, but so does the ILogO, the customer and many others across DND. Somewhere in the hierarchies below these roles the same generic set of spending privileges (identified by the sub-role of RC Manager) could be referenced.

Finally, in keeping with the intent of the X.509 standard, many of the updates to complex super-roles would be made automatically. Every change to a role specification certificate will percolate upwards to modify the capabilities of any role specification certificate above it in the hierarchy. This effect will be most pronounced whenever there are changes at the bottom of the hierarchy. For example, any change in the privileges associated with the role specification certificate for RC Manager will automatically update the capability of any super-role which references it, e.g. the BTISO, the ILogO etc. Although designers of role specification certificates higher in the hierarchy will have to monitor the effects of these changes on the super-roles, the outcome should be to generally increase their currency and relevance since the changes are being effected by the source of authority for a particular privilege.

The bottom of the hierarchy would consist completely of privileges that could not be decomposed any further. These privileges would be contained within atomic role specification certificates, such as RC Manager. These atomic certificates contain privileges that naturally go together; it would make no sense to split them any further. It is likely that a large number of these atomic role specification certificates will be re-used as sub-roles within many other super-roles. These atomic role specification certificates are a natural development since, in all probability, a single source of authority will be responsible for various privileges that are closely related. For instance, all spending privileges, including those associated with the role of RC Manager, are controlled by the same source of authority, the MND. These spending authorities (described earlier) are designed to complement each other. Rather than assign them individually, it would be practical to group these complementary privileges together in role specification certificates, such as for the role of RC Manager.

3.2.2 Delegation Chains for the Validation of Role Specification

The specification and maintenance of these roles, used across DND, would be a centralized function of the National Defence Headquarters (NDHQ). In this way role specifications are produced and maintained by

people and organizations that understand the PMI and the interaction of privilege. The SOA, in this case the MND, would set up the required atomic certificates and delegate the responsibility for the creation and maintenance of complex roles for various parts of the business process to staff officers. They can be thought of as role managers. They produce ready-to-use role specifications (probably complex roles) that can be used by field officers to assign people to roles in their organizations. The ability to access a step of the business process must include verifying the delegation chain from the required attribute/permission on an atomic certificate, through more complex role specification certificates, to the author of the RSCs (an AA that must have the right to delegate the privilege), and through any superior role-specification AAs back to the SOA. The validation of this chain ensures that the privilege is being exercised through an authorized role, and that the creators of that role had the right to delegate the privilege to the role.

3.2.3 Delegation Chains for the Validation of Role Assignment

The delegation of authority to individuals has a separate delegation chain tracing back to the SOA (in this case the MND). The delegation of authority to individuals is made by issuing role assignment certificates.

The MND delegates authority for the Canadian Armed Forces to the Chief of the Defence Staff. The Chief of the Defence Staff delegates authority for large formations of the military to superior commanders who in turn delegate authority for smaller units to commanding officers. These delegations are made by using the ready-to-use roles, which are prepared by the centralized RSC managers in NDHQ. The commanders do not have to, and do not want to, understand the specification and maintenance of the ready-to-use RSCs.

The ability to access a step of the business process must include verifying the delegation chain from the required attribute/permission on an atomic certificate, through more complex role specification certificates, to the commander assigning the role to an individual (an AA that must have the right to delegate the privilege), and through any superior commander AAs back to the SOA. The validation of this chain ensures that the privilege is being exercised through an authorized role, and that the chain of commanders assigning that role to the user both possess the privilege and had the right to delegate the privilege to individuals down the chain of command.

Figure 3 provides a graphical representation of these dual delegation chains. It is assumed in the figure that the AAs have the necessary privileges to delegate; the diagram has been simplified and certificates associated with this are not shown. The role specification validation chain extends from the BTISO RSC back through the manager for the BISTO role to the SOA. The role assignment validation chain extends from the BTISO RSC back through the Base Commander to the SOA.

4 Delegation Path Complexity

When an end entity tries to access a controlled object the privilege verifier protecting that object must ensure the end entity is in valid possession of the privilege/security attribute required by the security policy to allow access. This will require the privilege verifier to walk the certificate chains to ensure the chain of trust is not broken between the SOA and the user of the attribute. For each certificate, the verifier will have to ensure the certificate is properly signed (a public-key operation), and that some required attribute(s) exist in the certificate. The public-key certificate operations dominate the complexity, and attribute checks can be ignored.

The diagram in Figure 3 has been simplified. In the general case there may be a number of RSCs in a chain that describes the role hierarchy from the complex role the end user is using, to less complex roles, and finally to atomic roles. Each of the RSC certificates in the hierarchy would have a role specification validation chain rooted at the SOA (section 3.2.2). Each specification validation chain might include more than one role manager (i.e. the role management might be delegated down the chain). Each chain must be validated.

A superior commander assigns the role to the end entity by issuing a RAC. The role assignment validation chain extending back through commanders to the SOA must also be validated. But at each step back through this chain the commanders' own privileges were assigned to them through their own role RACs. So the certificate chains of each commander's role must also be walked.

Consider the following simplifying assumptions.

- a) There is a simple CA; the verifier has access to a trust root certificate for the CA that it can use to verify any PKC. Therefore certificate validation requires two public-key operations: signature verification of the attribute certificate

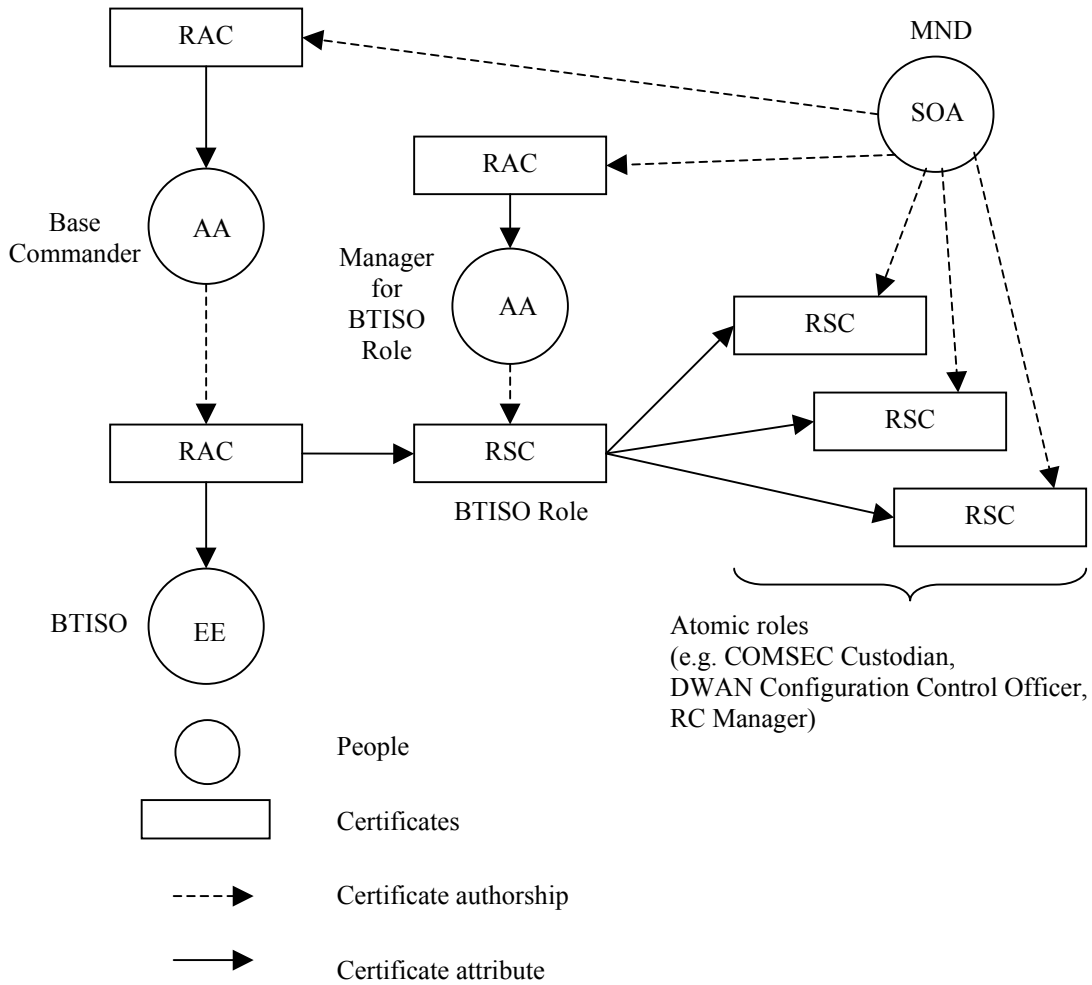


Figure 3 – Delegation Chains

using the issuer’s PKC, and PKC verification using the certificate for the CA.

- b) The SOA directly issues all atomic RSCs.
- c) The RACs issued to the role managers directly reference atomic RSCs and do not reference complex roles.
- d) Delegation in the role specification validation chains is uniform. I.e. there are always the same number of role managers in the management delegation hierarchy for each complex RSC.
- e) The RSC role hierarchy is uniform. I.e. there is always the same number of

complex RSCs in the chain from the end entity’s role RSC to the atomic RSCs.

Now, let num_{roles} be the number of complex roles in the RSC hierarchy from the end entity’s RSC to the atomic RSCs (including the end entity’s role). Let num_{mgr} be the number of role managers in the management delegation hierarchy. Let num_{cdr} be the number of entities in the role assignment validation chain extending back through commanders to the SOA (including the end entity but not including the SOA).

Now, consider the number of certificates that need to be validated in the delegation chains. The atomic RSC containing the required privilege must be validated. Also, each complex RSC in the role hierarchy must be validated. This requires validation of the complex RSC itself and validation of each of the manager’s RACs up

the chain to the SOA. Therefore, for a role used by an end entity or a superior commander $1 + \text{num}_{\text{roles}}(1 + \text{num}_{\text{mgr}})$ operations are required to validate its management chain delegation.

The role used by an end entity or a superior commander is assigned using a RAC, which must be verified. The validity of each superior commander's role must also be verified, which means validating its complete management delegation chain too. The complete set of attribute-certificates is then $\text{num}_{\text{cdr}}(1 + (1 + \text{num}_{\text{roles}}(1 + \text{num}_{\text{mgr}})))$.

The number of operations required to validate an access will be twice the number of certificates in the relevant validation chains (from assumption a.). Therefore the overall complexity of making an access control decision for an end entity is:

$$2\text{num}_{\text{cdr}}(2 + \text{num}_{\text{roles}}(1 + \text{num}_{\text{mgr}})) \quad (1)$$

If a very simple authorization structure is used, where $\text{num}_{\text{roles}}=1$, $\text{num}_{\text{mgr}}=1$ and $\text{num}_{\text{cdr}}=2$, as depicted in Figure 3, then 16 operations are needed to make an access control decision. However, within DND five levels of command delegation would not be unreasonable. E.g. delegation might proceed from the MND, to Chief of the Defence Staff, to the Commander of the Army, to the Base Commander, to the BTISO. Now as a more typical example, consider the case where $\text{num}_{\text{roles}}=3$, $\text{num}_{\text{mgr}}=2$ and $\text{num}_{\text{cdr}}=5$. Complexity for an access control operation is now 110.

Public-key operations are expensive and the complexity of implementing this model seems high. This bears out the complexity warnings in [x509], and in [FH00] where Farrell and Housely do not recommend the use of delegation chains. This complexity results from attempting to mirror the distribution of privilege within a real organization. If the processing complexity can be managed, the flexibility of being able to model the actual privilege delegation paths in an organization is an advantage of this role-based model.

The complexity due to processing paths and retrieving certificates may be mitigated through the use of a cache within the verifier components. This possibility stems from the observation that most of the authorization structure is stable for significant periods of time. The roles assigned to individuals are often stable of a period of months. The privileges associated with roles would also have a similar period of stability. Significant segments of the certificate chains can be pre-validated and cached. Many different end entities require the validation of common chain segments. For example a

superior commanders role validation is used in validating access requests for all subordinates. Only chain segments that have changed recently need to be revalidated. The investigation of efficient caching schemes to improve the efficacy of implementation is future work.

5 Conclusion

This work demonstrates how the X.509 standard can be used to support Canadian Department of National Defence authority structure models. It is expected that the results are applicable to large enterprise environments in general.

The roles model in the X.509 standard is compatible with the hierarchy of roles concept within role-based access control (RBAC). An interpretation of the X.509 standard is proposed that allows the construction of complex super-roles from more basic sub-roles. This structure leads to a separation of attribute authorities responsible for the specification of roles, from attribute authorities responsible for the assignment of roles. The combined effect is to produce a PMI model that meets the DND criteria for control over the granting of authority.

The results provide insight into, and quantification of, the complexity of the delegation chains. The use of a roles based model for delegation is seen as being important to the scaling of PMI to service large enterprises with mature, complex authority structures. Using role assignment and role specification certificates in conjunction with delegation paths will be a challenge for designers in complex business transactions. The large number of certificates required in delegation models will complicate implementation. This concern may be mitigated if the verifier can cache certificates and recently calculated delegation paths.

References

- [Bra00] S. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, Cambridge, Mass, 2000.
- [Dep99] Department of National Defence. *Delegation of Authorities for Financial Administration for DND and the CF A-FN-100-002/AG-006*, Government of Canada, May 1999.
- [FH00] S. Farrell and R. Housley. *An Internet Attribute Certificate Profile for*

Authorizations. Draft – PKIX Working Group. August 2000. (work in progress).
<http://www.ietf.org/internet-drafts/draft-ietf-pkix-ac509prof-00.txt>

- [Gov96] Government of Canada. *The Business Case For Electronic Authorization and Authentication (EAA) in The Government of Canada*. January 1996.
- [Gra01] Grandy, Chris, *Using A Privilege Management Infrastructure To Support Business Processes Within The Department Of National Defence And The Canadian Forces*, Master's Thesis Royal Military College of Canada, April 2001.
- [Int00] International Telecommunications Union. *ITU-T Recommendation X.509|ISO/IEC 9594-8: Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks*. ITU-T, 2000.
- [WH99] P. Wing, B. O'Higgins. Using Public-Key Infrastructures for Security and Risk Management. In *IEEE Magazine*, pages 71-73, September 1999.