

# MIERA: Method for Inter-Enterprise Role-Based Authorization

Heiko Ludwig<sup>1</sup>, Luke O'Connor<sup>1</sup>, and Simon Kramer<sup>2\*</sup>

<sup>1</sup> IBM Research, Zurich Research Laboratory, 8803 Rüschlikon, Switzerland  
hlu@zurich.ibm.com

<sup>2</sup> École Polytechnique Fédérale de Lausanne, 1015 Lausanne, Switzerland

**Abstract.** This paper addresses the problem of inter-enterprise transaction authorization, as required when an employee of one organization commissions work to another organization. On receiving an order from another organization, a company wants to be sure that the sender is actually entitled to do so within his or her organization. The MIERA scheme can be used for both intra- and inter-enterprise authorization and bases the decisions on roles. We define an authorization tree for a transaction type that determines which combination of roles can authorize such transactions. This tree allows the order-receiving organization to verify whether the order-sending employee was properly authorized.

## 1 Introduction

Traditionally, authorization was considered a security service that controls who may access resources and in what manner. This service is implemented via an access control matrix [1] or a related concept such as access control lists [2] or capabilities [3]. These mechanisms typically assume that fine-grained control over resources is required, such as explicitly specifying which users can read a given file  $F$ , which group can write to  $F$  and so on. This approach is referred to as the subject-object paradigm [1, 4], which specifies access control in terms of  $(s, o, a)$  triples (subject, object, access rights) and is commonly integrated quite closely with the underlying operating system. Whereas this model is appropriate for single or closed systems, the subject-object paradigm is less suited to distributed and general e-commerce applications which require authorization decisions based on non-local information and credentials [5, 6]. Considering an inter-enterprise workflow application, authorization is more likely to be based on a combination of general policies, company affiliation, roles, group privileges, delegated rights, location information and possibly third-party credentials rather than on read/write file permissions, for example [5, 7].

### 1.1 Transaction Authorization between Organizations

A major issue is to determine how credentials (or authorization attributes) issued in one security domain (say company  $A$ ) are to be interpreted in another distinct

\* Simon Kramer stayed with the IBM Zurich Research Laboratory as a summer student for the MIERA project from August to October of 1999.

security domain (say company  $B$ ). Security frameworks such as Kerberos [8, 9], OSF DCE and Sesame [10, 11] permit trust relationships to be specified between domains. Whereas such a solution is potentially feasible in controlled environments such as between departments of one company, the business-to-business e-commerce promotes access to services where no standard authorization attributes exist. For these environments the trend is towards service requestors providing their credentials to service providers who decide whether the request is authorized based on the credentials supplied and a given access policy [12–15]. Much of the emphasis on credentials coincides with the introduction of public key cryptography [16], which permits authorities to issue statements that can be digitally signed and verified at the time of presentation. Attribute certificates [17] are a means of collecting authorization attributes into a format similar to the standard X.509 certificate for representing public keys [18].

The approach to distributed authorization that we take in this paper is to consider the middle ground between all service requestors and providers agreeing on common authorization attributes on the one hand, and service requestors processing arbitrary requestor credentials on the other. For example, consider the scenario in which two companies— $A$  and  $B$ —have a formal agreement for making business transactions. In the context of this paper we use the term transaction for any legally binding action between organizations, such as an offer or an order. We denote the possible set of transaction types between  $A$  and  $B$  by  $T(A, B) = \{T_1, T_2, \dots, T_n\}$ , where for example  $T \in T(A, B)$  may denote  $T \rightarrow$  “purchase  $X$  units of product  $Y$  at price  $P$  per unit”.

We assume that the transaction types denoted by the set  $T(A, B)$  are general, and that when the particular transaction takes places, additional details beyond those given in the transaction descriptions of  $T(A, B)$  must be provided. A typical situation would be for a person  $U_A$  from company  $A$  to receive a transaction of type  $T \in T(A, B)$  from a person  $U_B$ , who purports to be from company  $B$ . As the request originates from a public network, there are several security issues that  $U_A$  may consider:

- Should the details of transaction  $T(A, B)$  be confidential and encoded for integrity?
- How can one verify that the person  $U_B$  requesting the transaction is in fact an employee of company  $B$ ?
- Even if it is known that the person requesting the transaction is  $U_B$  from company  $B$ , how can it be verified that  $U_B$  is authorized to request such a transaction for the given values of  $X$ ,  $Y$  and  $P$ ?

The first two points are addressed by standard security protocols and cryptographic algorithms [16]. In particular, with public key cryptography each user  $U$  can be issued with one or several certificates [18] that can be used to demonstrate their identity (and employer) through the use of digital signatures [16]. In this paper we address the point of *authorization* of the transaction.

From a legal point of view, many countries maintain company registers that (among other things) list the employees who are entitled to act legally on behalf of an organization. If a transaction is signed by a registered employee it is legally enforceable by transaction partners. However, this is usually only a very small