Identity Based Delegation Network

Sherman S.M. Chow*, Richard W.C. Lui, Lucas C.K. Hui, and S.M. Yiu

Department of Computer Science,
The University of Hong Kong,
Pokfulam, Hong Kong
{smchow, wclui, hui, smyiu}@cs.hku.hk

Abstract. Delegation of authorities is a common practice in various organizations. The way delegation is performed can be quite complicated. To capture possible delegation structures, the concept of *delegation network* is proposed, so that anyone can be convinced of who obtained delegation from whom in order to produce the final proxy signature. In this paper, we consider the delegation network for identity-based (ID-based) scenario. Since the public key is just a string denoting the user's identity, certificate management is simplified. Proxy signature schemes have been devised to delegate signing authorities. We show that a trivial attempt of extending an existing ID-based proxy signature may result in an insecure scheme. After that we propose a building block of our ID-based delegation network, which is an ID-based proxy signature supporting batch verifications. Our proposed ID-based delegation network is flexible in the sense that the whole delegation network does not need to be known in advance. Our proposal is provably secure under the random oracle model.

Keywords: Delegation network, identity-based cryptography, proxy signature, batch verification, bilinear pairings

1 Introduction

Delegation. Delegation is a process where a user (the delegator) grants some of his/her rights (power), e.g. the signing right, to another user (the delegate), to work on his/her behalf. It is a very common practice for users in an office to delegate their power to subordinates when they are on leave or need assistance. For a delegate to digitally sign on behalf of the delegator so that the receiver of the document be convinced that the signer has the signing right from the delegator, a straight-forward approach is to pass the delegator's signing key to the delegate. Obviously, this do not work well since the delegator has to change the key frequently. It also violates the non-repudiation requirement since it is difficult to prove who actually signed the document.

Proxy Signature. To tackle this problem, the notion of proxy signature was proposed in [21] to deal with the delegation of signing. In a proxy signature,

* Corresponding Author

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 99–115, 2005.

the original signer creates a proxy key pair, denoted as (psk, ppk), using his/her own signing key (and possibly the delegate's public key). The delegate (called the proxy signer) signs a document using psk. The verifier has to use ppk as well as the public key of the original signer (again, and possibly the delegate's public key) to check the validity of the signature. Since the public key of the original signer is involved in the checking, the delegation relationship can be confirmed. Such schemes are very important technologies in various application domains, examples include but not limited to grid computing [9], distributed systems [22], distributed shared object systems [18] and a bunch of electronic commerce applications such as offline e-cash [23], privacy preserving signature in mobile communications [26], global distribution networks [2], and last but not least, mobile agents for electronic commerce.

Delegation Network. Hierarchical structure, which is common in organizations nowadays, complicates the way delegation is performed. Firstly, there can be chained delegation, in which the delegation occurs across more than two levels. For example, A may delegate her job to her subordinate B and B can further delegate the job to his subordinate C. Secondly, it is common that a signature is constructed by a group of members. In other words, the delegator can be a group of members instead of one single user. In this case, delegation can be passed from one group of users to another group of users. For example, A and B are required to sign together on a check. Now they both are on leave and so they may delegate the signing right to C and D.

To capture possible delegation structures, the concept of *delegation network* was proposed in [1]. The delegation structure of the signing group is modeled in a directed graph so that anyone can be convinced of who obtained delegation from whom in order to produce the final signature. An application of delegation network can be found in the use of mobile agents in electronic commerce application. Suppose mobile agents are ordered by a customer to search for a proper bid presented by a server and then digitally sign the server's bid together with the customer's requirement with both server's key and customer's key [16]. Consider a scenario that a mobile agent E is ordered to search for a travel package of lowest price (which includes both air ticket and hotel accommodation) offered by a travel agency on behalf of a research student. On the other hand, a mobile agent F is ordered by a travel agency to search for the prices of flight ticket and hotel accommodation. Then, agent E will delegate the signing authority to agent F, in which F will further delegate this signing authority to the airline company and the hotel, who sign their corresponding bid using the delegation received together with their respectively private key.

Identity-Based Cryptography. Most of the proxy signature schemes are based on a public key infrastructure (PKI). As an alternative to PKI, Shamir introduced the concept of identity-based (ID-based) signature schemes [27] and the design of ID-based schemes have attracted a lot of attention recently [3,5, 6,13,19,25,31,32,33]. For traditional PKI, the public key is a "random-looking" string that is unrelated to the user's identity, so a trusted-by-all party