Secure Cryptographic Workflow in the Standard Model

M. Barbosa[1] and P. Farshim[2]

[1] Departamento de Informática, Universidade do Minho,
Campus de Gualtar, 4710-057 Braga, Portugal
mbb@di.uminho.pt
[2] Department of Computer Science, University of Bristol,
Merchant Venturers Building, Woodland Road,
Bristol BS8 1UB, United Kingdom
farshim@cs.bris.ac.uk

Abstract. Following the work of Al-Riyami *et al.* we define the notion of key encapsulation mechanism supporting cryptographic workflow (WF-KEM) and prove a KEM-DEM composition theorem which extends the notion of hybrid encryption to cryptographic workflow. We then generically construct a WF-KEM from an identity-based encryption (IBE) scheme and a secret sharing scheme. Chosen ciphertext security is achieved using one-time signatures. Adding a public-key encryption scheme we are able to modify the construction to obtain escrow-freeness. We prove all our constructions secure in the standard model.

Keywords: Cryptographic Workflow, Key Encapsulation, Secret Sharing, Identity-Based Encryption.

1 Introduction

The term *workflow* is used to describe a system in which actions must be performed in a particular order. In *cryptographic workflow* [23] this is achieved by making decryption a privileged action which can only be executed by users which possess an appropriate set of *authorisation credentials*, or simply *credentials*. Credentials are issued by a set of *authorisation authorities*, which can ensure that some action has been performed, or that some event has occurred, before granting them to users. Restricting access to encrypted messages in this way, workflow mechanisms can be implemented with cryptographic security guarantees.

An encryption scheme supporting cryptographic workflow should provide the following functionality [1]. Alice specifies the credentials that Bob should have in a *policy* that she decides before encrypting. Alice should be able to perform this encryption without knowing what credentials Bob actually has. A particular authorisation authority will validate that Bob is entitled to a given credential before awarding it. Each credential acts as a (partial) decryption key. Alice may also want to be sure that no colluding set of these authorisation authorities is able to decrypt and recover the message that she intended for Bob. If this is the case, the system should be *escrow-free*.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 379–393, 2006.

In this paper we introduce the notion of KEMs supporting cryptographic workflow (WF-KEM) and their escrow-free counterparts (EFWF-KEM). We adapt the security models proposed in [1] for encryption schemes accordingly. We argue that the KEM-DEM paradigm introduced by Cramer and Shoup [14] for public-key encryption schemes also applies when one moves to encryption schemes supporting cryptographic workflow. In fact, we show that combining a secure WF-KEM (EFWF-KEM) with a secure DEM, one obtains a secure (escrow-free) encryption scheme supporting cryptographic workflow.

We present a generic construction that permits building WF-KEMs out of simpler cryptographic primitives. This is a generalisation of the construction presented in [1] based on the identity-based encryption (IBE) scheme of Boneh and Franklin. We show how one can construct analogous schemes by replacing its building blocks with other components providing the same functionality. More specifically, we prove that our transformation permits constructing a secure WF-KEM using secure IBE and Secret Sharing (SS) schemes. Finally, we extend our generic construction to obtain an EFWF-KEM using a secure public-key encryption scheme. Chosen ciphertext security is achieved via a one-time signature scheme. Our constructions are all secure in the standard model.

The paper is structured as follows. We first review related work in Section 2 and present the cryptographic primitives we use as building blocks in Section 3. Then in Section 4 we define precisely what we mean by secure WF-KEMs and EFWF-KEMs. In Section 5 we propose generic constructions of these primitives and prove them secure. Finally, in Section 6, we analyse the implications and efficiency of our results for cryptographic workflow and related problems.

2 Related Work

Identity-based cryptography was initially proposed by Shamir [26], who also introduced the first identity-based signature scheme. The first practical identity-based encryption (IBE) scheme is that proposed by Boneh and Franklin in [7], whose operation relies on the use of bilinear maps over groups of points on an elliptic curve. Sakai and Kasahara [24] later proposed another IBE scheme, also based on bilinear maps, but adopting a different key construction. The security of this scheme was established by Chen *et al.* in [11]. The latter scheme allows for more efficient encryption operation. Both these schemes are secure in the random oracle model (ROM). Recently, Waters [28], Kiltz [20] and Gentry [17] have proposed practical IBE schemes which are secure in the standard model.

The KEM-DEM construction was formalised by Cramer and Shoup in [14]. It captures the concept of hybrid encryption whereby one constructs a public-key encryption scheme by combining a symmetric Data Encapsulation Mechanism (DEM) with an asymmetric Key Encapsulation Mechanism (KEM). The security of the hybrid construction depends, of course, on the security of the KEM and DEM. In [14] it is shown that if the KEM and DEM constructions are individually secure, the resulting public-key encryption scheme will be also secure. The relations between the security notions for KEMs and the conditions for the security