# A Flexible Role-based Secure Messaging Service: Exploiting IBE Technology for Privacy in Health Care

Marco Casassa Mont
*Trusted Systems Laboratory*
*HP Laboratories, UK*
*marco.casassa-mont@hp.com*

Pete Bramhall
*Trusted Systems Laboratory*
*HP Laboratories, UK*
*pete.bramhall@hp.com*

Keith Harrison
*Trusted Systems Laboratory*
*HP Laboratories, UK*
*keith.harrison@hp.com*

## Abstract

*The management of private and confidential information is a major problem for dynamic organizations. Secure solutions are needed to exchange confidential documents, protect them against unauthorised accesses and cope with changes of people's roles and permissions. Traditional cryptographic systems and PKI show their limitations, in terms of flexibility and manageability.*

*This paper describes an innovative technical solution in the area of secure messaging that exploits Identifier-based Encryption (IBE) technology. It illustrates the advantages against a similar approach based on traditional cryptography and PKI. It discusses a few open issues. Our main contribution is a practical solutions based on IBE technology. A secure messaging system based on IBE has been fully implemented and it is currently used in a trial with a UK health service organization.*

## 1. Introduction

Modern societies and organisations are more and more complex, dynamic and flexible. People's roles, rights and duties change because of frequent reorganisations and evolution of market and customers' needs. Information is continuously generated and exchanged between all the involved parties, including confidential and private information. This information has to be protected against unauthorised accesses.

In the last decade, there has been an exponential increase of the usage of the e-mail service to exchange any kind of digital document. On one hand the e-mail service allows an easy, almost instantaneously and asynchronous transmission of digital information at a fraction of the costs of traditional mechanisms. On the other hand, providing a secure e-mail service is a non-trivial problem.

Dynamic organisations need secure messaging solutions to store and exchange confidential information and protect its privacy, against unauthorised accesses or disclosures. These solutions need to be flexible enough to cope with changes of people's roles and permissions.

Secure messaging solutions, based on traditional cryptographic systems and PKI show their limitations in dynamic contexts, in terms of flexibility and manageability.

Innovative work has been done in this area by the Trusted Systems Laboratory, HP Labs, UK by leveraging the Identifier-based Encryption (IBE) cryptography and applying it in a solution run in a trial with a UK health service organisation.

## 2. Addressed problem

The key problem addressed by this paper is the enforcement of information confidentiality and privacy in dynamic contexts, where people's roles and permissions are subject to frequent changes. Specifically, confidential information has to be exchanged in a way that only the entities that satisfy predefined constraints and policies, at a specific point in time, are allowed to access it.

We focus on the problem of providing a role-based secure e-mail service to enable secure communication in dynamic organisations, specifically in a health-care environment. We describe a few real-life scenarios in health care, we highlight key requirements and we present a practical solution based on IBE that we believe has advantages, in terms of simplicity, manageability and flexibility, against solutions purely based on traditional PKI/cryptographic systems.

## 3. Scenarios

This section describes a few real-life interactions among workers in a UK health service organization. We partnered with this organisation, for a technology trial. Currently, most of these interactions happen by exchanging traditional paper-based documents. The objective is to automate them by using a flexible and secure e-mail service and improve the overall quality of the service. Documents, such as [1], describe guidelines to

deal with the access of patients' confidential data, based on people's roles.

Figure 1 shows a high-level interaction model involving general practitioners (GPs) and members of a department of the health care organization.

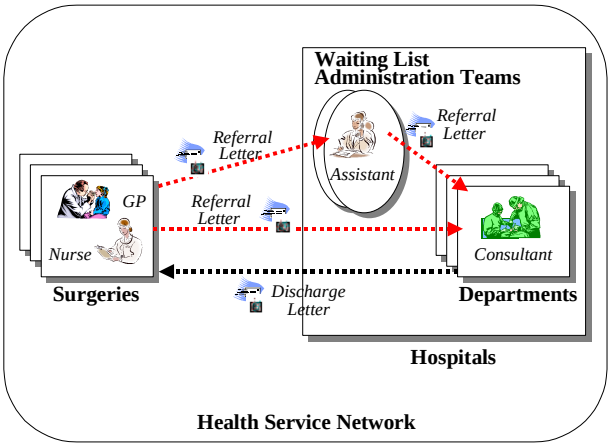


Figure 1. Interaction Diagram

A general practitioner (GP) or his/her assistants might need to send referral letters to hospital consultants, containing patients' confidential information. The GP might have no idea of which specific consultant is on duty or which specific person needs to be contacted. On the other hand, the GP has clear in his mind the role of the person he/she is willing to communicate to.

Waiting list administration teams (at the hospital premises) are in charge of dealing with health care requests for patients and allocate them to the available resources. Members of the team could be asked to act as information "routers". In particular circumstances, they might not be allowed to access or read the content of the requests because of the confidentiality of patients' data. Roles can be dynamically (re)-allocated, depending on timetables, availability or lack of medical personnel.

The consultant that is on duty or in charge of a specific patient can change, over time. Similarly the members of a consultant's team and the members of the waiting list administration team can vary depending on personnel availability and workloads.

In analogous scenarios a consultant, from the hospital, might wants to send patient's confidential information (a discharge letter) back to the surgery that is in charge of the patient.

In the highlighted interactions, the initial sender of the secured e-mail is acknowledged when a legitimate receiver successfully reads it.

## 4. High-level requirements

The previous section stressed the need for a system that, on one hand, ensures the privacy and confidentiality of the content of e-mails exchanged by health service employees and, on the other hand, copes with frequent changes of their roles and access rights.

It is important to notice that there is a neat separation between the concept of "e-mail address" and "role" of the receivers. The e-mail service is purely a communication service. In general, confidential messages can be sent to e-mail addresses or mailing lists that are accessible by different kind of people, with different roles and rights. On the other hand, the roles played by a receiver at a specific point in time are determinant to decide if that person can access a confidential message. Confidential messages might be sent without knowing, *a priori*, who the final receiver is. On the other hand, all the above scenarios describe situations where disclosure policies are well known and specified by the sender.

High-level system requirements follow:

- **Privacy and confidentiality**: messages need to be obfuscated by the system before being transmitted and securely stored at the receiver site, at least till a legitimate user is entitled to de-obfuscate and read them;
- **Policy-based disclosure**: disclosure policies need to be strictly associated to the obfuscated messages. It must be possible to tell if policies have been tampered with.
- **Strong authentication**: people need to be strongly authenticated by the system. The system needs users' identities to decide if they are entitled to access obfuscated messages by retrieving their associated profiles (including their roles) and checking them against disclosure policies;
- **Flexibility**: the system must allow users to flexibly specify policies to constrain the access to confidential information. In particular it must be possible to specify role-based disclosure policies. The system must support late-binding mechanisms for roles;
- **Simplicity**: the overall system must be simple to use, both for end-users (to define disclosure policies and protect messages) and system administrators.

The next section describes relevant technologies currently available on the market, a possible solution of the problem based on them and related problems.

## 5. Solution by using traditional technology

Traditional cryptographic systems [2] (based on public/private key, symmetric keys or any combination of them) and X.509 Public Key Infrastructure (PKI) [3] can be used to address the problem.

Digital certificates along with PKI infrastructures are a suitable technology to underpin authentication, non-repudiation and confidentiality.

In case of secure messaging services, digital certificates and traditional cryptography schema (based on public/private key pairs) offer a viable solution when privacy criteria depends on the "identity" of message receivers: in this case a confidential message can be encrypted by directly using the public key of the receiver.

If privacy criteria do not depend on receivers' identities but on other aspects, such as the satisfaction of predefined disclosure policies (including membership to roles), it is not possible to use digital certificates as specified before. In this case it is not known, *a priori*, which digital certificate (public key) must be used for encryption purposes.

To solve the problem, a further level of indirection is required. An additional system component can to be introduced to deal with policy management interpretation and authorization. This component must be a trusted element of the system. A digital certificate (well known by the system users) can be associated to this trusted component. Encrypted message bundles can be used to represent, transmit and store secured messages (along with the associated disclosure policies). Enveloping techniques, such as PKCS#7 [4] or signed XML [5] document, can be used for this purpose.

Role-based access control (RBAC) [6] mechanisms (along with a role based authorization engine) can be coupled to the above component to deal with role-based disclosure policies.

To build the above solution, traditional secure e-mail services based on S/MIME and users digital certificates are of little help. Additional mechanisms need to be implemented to deal with the authoring of disclosure policies, the management of encrypted bundles and late binding of roles. A trusted component has to be built from scratch. Although it is possible to solve the secure messaging problem by building hybrid solutions that use traditional cryptography and PKI (coupled with RBAC) this is not the most natural way of using the PKI model and digital certificates.

The work described in this paper is a research and development effort to provide an alternative solution to the secure messaging problem that is simpler and more flexible.

## 6. Proposed solution

The technical solution proposed in this paper leverages the Identifier-based Encryption (IBE) schema, a new emerging cryptographic schema [7, 8, 12]. The next sections describe the key IBE principles along with the details of our lightweight and flexible *role-based encryption system.*

### 6.1. IBE cryptography schema

The IBE cryptography schema [7,8] has three core properties:

- **1st Property**: any kind of string can be used as an IBE encryption key (public key). This "string" consists of any sequence of characters or bytes such as **a role** description, a text, a name, an e-mail address, a picture, a list of terms and conditions, etc. Information is encrypted by using this string along with a "public detail", uniquely associated to a specific trusted third party, referred in this paper as *trust authority (TA)*. This trust authority is the only entity that can generate the correspondent IBE decryption key. It only relies on a local *secret* that is a critical resource and needs to be properly protected;
- **2nd Property**: the generation of an IBE decryption key (associated to an IBE encryption key, i.e. a string) can be postponed in time. In other words an IBE decryption key can be generated (by a trust authority) a long time after the correspondent IBE encryption key was created.
- **3rd Property**: Reliance on at least one trusted third party (i.e. Trust Authority) for the generation of IBE decryption keys.

Figure 2 shows the IBE interaction model:

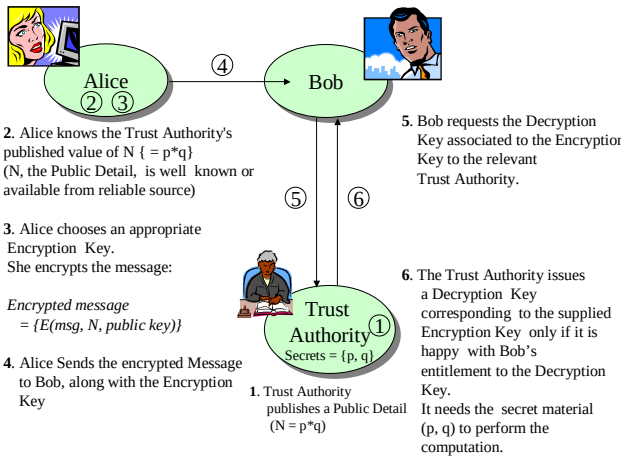


Figure 2. High-level IBE Interaction Model

Three players are involved in the above interaction model: a sender of an encrypted message (Alice), the receiver of the encrypted message (Bob) and a trust authority in charge of issuing decryption keys.

Alice sends an encrypted message to Bob, by using a chosen IBE encryption key. Alice and Bob trust a third party, the trust authority (TA). Bob has to interact with the

trust authority and provide the requested credentials in order obtain the correspondent IBE decryption key.

The IBE model fits very well to address the role-based secure messaging problem. First of all, it is possible to use the "role" of the intended e-mail receiver as an IBE encryption key and directly encrypt a confidential e-mail. Secondly, the TA can generate the correspondent IBE decryption key on the fly (when needed) if the receiver is currently playing the requested role. There is no need to share or store any secret between the sender and the receiver.

## 6.2. Technical solution

### 6.2.1. Model

The model used for our solution derives from the IBE model. Confidential e-mails are directly encrypted by means of textual strings, representing IBE encryption keys. These strings explicitly describe the disclosure policies (terms and conditions) under which the content of an e-mail can be disclosed, specifically a list of roles. For example if a GP wants to send an e-mail that can be accessed by any member of the waiting list administration team, he/she can use the "*Member of the Waiting List Administration team"* string to encrypt the e-mail.

We do make use of a trust authority. The receiver of a confidential e-mail has to authenticate and interact with this trust authority to retrieve the appropriate decryption key. The trust authority retrieves up-to-date lists of roles associated to users and checks them against the relevant disclosure policies. The trust authority will generate and issue a decryption key only if the requestor has the required role(s). If the disclosure policies are tampered with, the generation of the correct decryption key is impossible.

### 6.2.2. Additional technical constraints

Our role-based secure messaging solution has been constrained by additional technical requirement expressed by the UK health care organisation we are running a technology trial with:

- Microsoft (MS) Outlook 2000 is used as e-mail browser and Microsoft Exchange as e-mail servers;
- People are authenticated by using the *MS Windows* authentication mechanisms [9] via a unique *MS Windows* logon and Windows trust domain;
- Multiple *MS Windows* trust domains are tactically used to reflect the structure of the health care organisation. Specifically, GPs and their assistants belong to a *GPDomain* trust domain; consultants, their collaborators and waiting list administration teams are part of the *HospitalDomain* trust domain.
- All the PCs used to exchange confidential information are part of a protected and secured organisation's Intranet.

The above constraints along with the high-level requirements influenced the design and implementation of our solution.

### 6.2.3. Technical details

Figure 3 shows the high-level architecture of our solution:

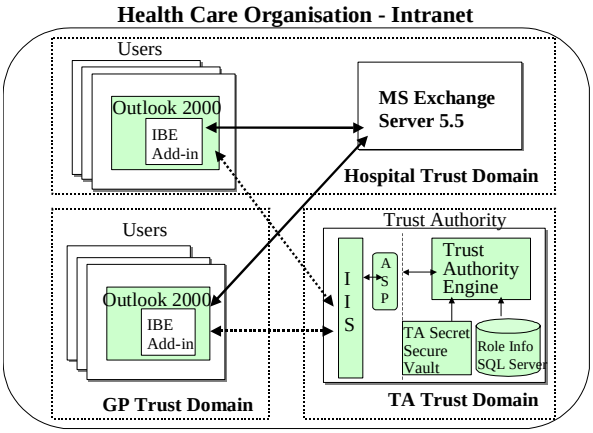


Figure 3. High-level System Architecture

The core architectural components are:

- ***A Microsoft Outlook 2000 Add-In***: it is a standard add-in implementing the Microsoft Office *IDTExtensibility2* interface [10]. It is deployed on users' Outlook 2000 e-mail browsers. It includes a module providing the IBE cryptographic algorithms used to encrypt and decrypt e-mails; a graphical UI to author role-based encryption policies; a communication module to remotely interact, via https protocol, with the trust authority.
- ***A Trust Authority Service***: it is a web service, hosted by a secure and protected server, and accessible via a Microsoft IIS web server. Only secure (https) connections are accepted from authenticated users. The web service includes: (1) a front-end wrapper (.asp scripts), to deal with remote invocation; (2) a back-end persistent trust authority engine. This engine makes authorization decisions and relies on IBE cryptographic algorithms to generate the IBE decryption keys; (3) a cryptographically secure vault used to store the trust authority secret. Trusted administrators run the server and the trust authority service.
- **A Microsoft SQL Server database**, associated to the trust authority. It containing up-to-date lists of roles and up-to-date associations of people's

identities to their current roles. Trusted administrators run and update the database.

In terms of *privacy and confidentiality* the Outlook add-in uses IBE cryptography to encrypt confidential messages. User's disclosure policies (list of roles) are used as IBE encryption key. The decryption key is not known *a priori*.

The Outlook add-in intercepts a confidential e-mail, before it is sent to the receiver(s) and replaces it with a new e-mail containing protected information within an attached "data bundle". This "data bundle" contains the original e-mail's subject line, body and attachments, in an encrypted format. The relevant disclosure policies are also part of the bundle. For convenience and flexibility, we used XML [11] to represent the data bundle. The subject of the new e-mail is by default a generic string (such as "Encrypted e-mail"). The user can modify it, for example to contain useful "routing" information for the e-mail.

A user can virtually author any kind of *disclosure policies* and use them as an IBE encryption key to protect a confidential e-mail. For the purpose of the trial, we limited these policies to a list of the roles that the intended receiver needs to play. A simple and intuitive authoring tool has been built and integrated in Outlook.

At the receiver side, the Outlook add-in manages all the interactions (via https) with the trust authority service, in order to retrieve an IBE decryption key. The user triggers this interaction by pushing a "Decrypt" button, within the e-mail window.

The trust authority shares the semantics of the disclosure policies with the Outlook add-in. After authenticating a user, it checks if the user has the required role(s) by looking at tables in an associated SQL database. Only in case of success, it generates (on-the-fly) the decryption key. The trust authority never accesses the content of confidential messages, as only the disclosure policies are sent to it.

In case of dynamic changes of people's roles the system administrator has to update the content of the database tables accordingly. Note that no wider publication of these is required.

The trust authority service is run in a very secured and protected PC. The trust authority **secret** is physically stored in a pass phrase protected vault, on the PC hard disks. Copies of this secure vault are made on CD-ROM and other persistent storages, and stored in safes, as a precaution for disaster recovery.

In terms of *authentication*, because of constraints dictated by the trial, we make use of *Microsoft Windows* authentication to authenticate users. Every user has a unique *MS Windows* logon. Users authenticate to the trust authority by using the *MS Windows* authentication mechanism, via the IIS web server. This process is mediated by the Outlook add-in and it is transparent to users.

In order to make this authentication process more scalable, an ad-hoc trust domain has been explicitly associated to the trust authority. This trust domain trusts (by means of trust relationships) the *GPDomain* and the *HospitalDomain* trust domains.

In terms of *simplicity* of usage, users can encrypt and decrypt confidential e-mails by using intuitive functionalities that are completely integrated in the Microsoft Outlook browser. System administrators only need to start the trust authority engine and provide to the system the pass phrase to access the trust authority secret.

## 7. Discussion

We believe that our main contribution is a practical application of the IBE cryptography, in a real-life trial. We currently have a fully working implementation of the messaging solution, deployed in a UK health-care environment.

IBE cryptographic libraries (based on [8]) have been fully implemented by HP Labs and optimised to achieve cryptographical performances comparable to traditional RSA algorithms.

Based on the experience and evidence we accumulated so far, we believe that the proposed solution has advantages in terms of *simplicity* and *flexibility* if compared to a similar solution build with traditional cryptography schemas and PKI infrastructure.

In terms of flexibility, our solution allows the encryption of confidential e-mails without having to depend on the identity of the receiver. Disclosure policies are directly used as IBE encryption keys. Because of the IBE properties, it has been straightforward to implement a mechanism that supports "late-bindings" of roles. The semantic of disclosure policies can be extended in a simple way, independently by the underlying encryption algorithms. In this case, only the trust authority engine needs to be extended. This has no impact on the underlying IBE cryptography system.

We believe that our solution is *simple to manage*. No public key/digital certificates need to be issued, managed and revoked, *at least* for encryption purposes, at the users' sites. In the current solution, no secret need to be stored at users' PCs or exchanged among them. The Outlook add-in (installed at the users' sites) only needs to know what the trust authority's public detail is (necessary for encryption purposes). This can be locally stored (at the installation time of the Outlook add-in) or downloaded from the trust authority web site.

The solution deployed in the trial relies on Microsoft Windows authentication mechanisms to authenticate users. This is a quite specific approach to authentication and it simplified the way we solved the problem.

At the current state of our research we are exploring IBE-based challenge/response schemas for authentication purposes but we do not yet have evidence that they are better than traditional PKI-based authentication or they simplify users' experiences and the overall management.

In general, we believe IBE can be used as a complementary technology to traditional PKI, especially when exploiting its encryption features.

An issue of the current solution is the maintenance of the content of the SQL database tables (containing roles, and role associations). Keeping the access control information up-to-date is a well-understood RBAC problem (and more in general an access control problem). Further automation can be introduced in case this information is available from other sources, such as directory services containing up-to-date organisation data. However role definitions change less frequently than membership of groups of users that perform roles.

At the end, the trial will give us valuable evidence about the validity and scalability of our solution.

## 8. Current and future work

Our secure messaging solution is currently used in a trial with a UK health service organisation. We are monitoring its usage, problems or issues encountered by users.

In parallel, we are exploring how our solution can be extended or re-engineered in order to be used in other dynamic contexts (including government, financial and military environments) that require secure messaging services and lightweighted, policy driven encryption mechanisms. In particular we are investigating how to extend the disclosure policies to include time-based constraints, terms and condition constraints, obligation policies, etc.

We are also exploring how to extend our solution to include multiple trust authorities, run by independent authorities, in order to avoid the reliance on only one third party and at the same time, avoid the complexity of PKI Certification Authorities' hierarchies.

## 9. Conclusion

Privacy management is a major problem for modern dynamic organisations, especially when people frequently change roles, rights and permissions. We focused on the problem of providing a role-based secure messaging service in a health care context, where people's functions are subject to changes and it is imperative to deal with "late-bindings" of roles.

Current technologies, such as traditional cryptography schemas and PKI, can be used to solve the problem but they suffer of flexibility and management problems. Additionally, their underlying models do not naturally fit.

We described an alternative approach to the problem that makes use of the IBE cryptography schema. IBE encryption keys are used to directly represent disclosure policies associated to confidential e-mails, including the list of the required roles. An IBE trust authority generates (on the fly) IBE decryption keys. This component, coupled with a RBAC system, satisfies, in a very simple way, the requirement for "late-binding of roles".

We believe that our approach is more flexible and simpler than an equivalent approach based on traditional cryptography and PKI technology. A few issues still need to be explored in a broader context, especially regarding the authentication of users with trust authorities.

A working secure messaging solution has been implemented and it is used in a technology trial with a UK health care organisation.

## 10. References


[1] The Caldicott Committee, Report on the review of patient-identifiable information. UK- http://www.doh.gov.uk/confiden/crep.htm , 1997

[2] W. Diffie, M.E. Hellman, New Directions in Cryptography, 1976

[3] R. Housley, W. Ford, W. Polk, D. Solo, RFC2459: Internet X.509 Public Key Infrastructure Certificate and CRL profile, IETF, 1999

[4] RSA Laboratories, PKCS#7: Cryptographic Message Syntax Standard. Version 1.5, 1993

[5] D. Eastlake, J. Reagle, D. Solo, XML-Signature Syntax and Processing, draft-ietf-xmldsig-core-08, IETF, 2000

[6] D. Ferraiolo, R. Kuhn, Role-based Access Control. NIST, 1992

[7] C. Cocks, An Identity Based Encryption Scheme based on Quadratic Residues. Communications-Electronics Security Group (CESG), UK. http://www.cesg.gov.uk/technology/id-pkc/media/ciren.pdf , 2001

[8] D. Boneh, M. Franklin, Identity-based Encryption from the Weil Pairing. Crypto 2001, 2001

[9] R. E. Smith, Authentication: From Passwords to Public keys. Chapters 10, 11. Addison Wesley, 2002

[10] D. Gifford, K. Slovak, C. Burnham, Professional Outlook 2000 Programming. Wrox, 2000

[11] W3C, Extensible Mark-up Language (XML) - http://www.w3.org/XML/ , 2003

[12] L. Chen, K. Harrison, A. Moss, D. Soldera, N.P. Smart, "Certification of Public Keys within an Identity Based System", Proc. 5th International Information Security Conference (ISC), 2002. LNCS 2433, Springer-Verlag, 2002