Patient Privacy Protection Using Anonymous Access Control Techniques

D. Weerasinghe, M. Rajarajan, K. Elmufti, V. Rakocevic
School of Engineering and Mathematical Sciences, City University, London, UK

Summary

Objective: The objective of this study is to develop a solution to preserve security and privacy in a healthcare environment where health-sensitive information will be accessed by many parties and stored in various distributed databases. The solution should maintain anonymous medical records and it should be able to link anonymous medical information in distributed databases into a single patient medical record with the patient identity.

Methods: In this paper we present a protocol that can be used to authenticate and authorize patients to healthcare services without providing the patient identification. Healthcare service can identify the patient using separate temporary identities in each identification session and medical records are linked to these temporary identities. Temporary identities can be used to enable record linkage and reverse track real patient identity in critical medical situations.

Results: The proposed protocol provides main security and privacy services such as user anonymity, message privacy, message confidentiality, user authentication, user authorization and message replay attacks. The medical environment validates the patient at the healthcare service as a real and registered patient for the medical services. Using the proposed protocol, the patient anonymous medical records at different healthcare services can be linked into one single report and it is possible to securely reverse track anonymous patient into the real identity.

Conclusion: The protocol protects the patient privacy with a secure anonymous authentication to healthcare services and medical record registries according to the European and the UK legislations, where the patient real identity is not disclosed with the distributed patient medical records.

Keywords

Anonymous medical service, record linkage, healthcare security, patient privacy

Methods Inf Med 2008; 47: ■–■

doi:10.3414/ME9116

1. Introduction

Electronic or mobile healthcare networks are established by connecting information systems used by general practitioners, hospitals and national/private medical centres. This approach is an attractive solution for the already overstretched and under-budgeted health sector since it reduces the current paper-based work, decreases waiting time, eliminates prior appointment requirements, enhances healthcare services with efficient, faster and more reliable methods, eliminates errors that can happen in the paper records and speeds up administrative procedures [1]. However, the development of such a working model in live medical environment will be subjected to an increase in the amount of sensitive medical information being transferred between different parties, with the data transport taking place over the Internet or the mobile network. The key problem with this is the security and privacy of communication, especially preserving the patient privacy by preserving the integrity of the information about the health condition and medications. Our previous paper [2] proposed the necessary security framework to prevent eavesdropping, spoofing and modifications to the healthcare information over the network. This paper proposes an approach to solve the problem of patient privacy using a novel anonymous access control technique.

Privacy as a social and legal issue has been analysed in detail in the past [3]. Privacy can be understood as the right and desire of a person to control the disclosure of personal information [4]. This control can be passed to a third party in exchange for some services. A function of anonymity is a sub-section of the privacy protection. Anonymity protects user privacy by authenticating the user without identification. For example a patient who has registered with the National Health Service (NHS) should be able to receive healthcare advices from any medical centre in the country without disclosing his identity.

The UK parliamentary POSTnote on data protection and medical research [5] proposed to encrypt personal identifiers in the electronic patient records using a code key before using those patient records for secondary use such as analysis, audit and research. These anonymous medical records consist of information about cancer registration, heart disease, HIV or drug surveillance and there should be a methodology for patients to request a report on their data. The data linkage is a task of matching and combining anonymous medical records that relates to the same patient from one or more organizations and creating a patient medical history. There has been number of activities carried out in data linkage as a major requirement for healthcare data warehousing. Kerkri et al. [6] presented a medical data warehousing approach that aims to use data semantics to regroup and link patient medical data from different health information systems. Christen discussed an overview of current privacy preserving data linkage approaches and their limitations in one of his research publications [7]. Quantin et al. studied the effect of different parameters on the reliable linkage in order to reduce the homonymous and synonymous errors [8].

The demand for user anonymity has increased with the expansion of electronic and mobile healthcare systems. An unauthorized access to a person's health-sensitive data can be subjected to different type of misdemeanours. Some of the misdemeanours are as follows:

- The insurance companies are interested to know the un-disclosed medical conditions of their clients to increase the insurance premium.

- The access to addiction or mental sensitive health information of a patient will affect badly on his potential employment opportunities.
- Banks will be reluctant to approve loans if they notice any serious health conditions of the account holder.

Hence patients are reluctant to use online healthcare services due to the possibility of the misuse of the health-sensitive personal data by third parties. In the past there have been incidents where the patient medical information was disclosed to external parties from various institutions such as healthcare providers, blood banks, pharmacies and adoption agencies [9, 10]. Some patients are too embarrassed to meet a doctor or a general practitioner face-to-face to discuss private and sensitive healthcare issues. They prefer to use a remote access system in which their identity will not be disclosed [11]. On the other hand, one of the problems with this approach is the reluctance of the doctors or physicians to give medications without knowing that they are communicating with a real patient. Eysenbach et al. [12] discussed the level of frustration of doctors or physicians responding to unidentified and unauthorized e-mails seeking medical advices. Therefore in an anonymous medical situation, patients should have some validation tokens to prove their legitimacy to the healthcare service but it should not be linked with their identity.

Therefore the anonymous access to medical services is one of the key requirements in electronic and mobile healthcare environments. This paper proposes communication architecture for the medical environment which enables access to medical services without revealing the patient identity to the medical services or the third party service providers. However, medical environment validates the patient to the healthcare service as a real and registered patient for medical services. The patient may get medications anonymously from different medical services in the proposed environment and all the anonymous medical history can be linked as a single medical report for the patient. Doctor or physician has the capability to reverse track the patient for further communication on anonymous medical records without compromising the real identity.

2. Related Work and Technology Requirements

The research on anonymous authentication has been carried out by a number of research groups worldwide. A group of researchers from Tokai University, Japan, have proposed an approach [13] to access services based on user's authority but without identifying the patient at the service provider. This approach is based on attribute certificate issued by the Attribute Authority. Leszczyna has presented two un-traceability protocols for mobile agent environment as a solution for anonymous access of IT services and its applications to an e-health counselling scenario [14]. Un-traceability is a subset of anonymity since the identity cannot be inferred by tracing the message. Gritzalis et al. [3] discussed about the importance of privacy and confidentiality in electronic healthcare to the human psyche. They used a real scenario implemented through a well-established distributed electronic environment in Greece that has been used for treating one beta-thalassemia patient for more than five years.

Splitting the personal identification from the medical details and encrypting each part separately is a methodology proposed to protect privacy and confidentiality in disease registers. Kelman et al. [15] proposed a secure protocol to link health data from unparalleled resources for the monitoring and evaluation. There is a proposed anonymous record linkage procedure using a one-way hash coding based on a standard hash algorithm [16]. As an extension to this procedure the same authors have introduced two large random files of keys, called pads, to avoid dictionary attacks on identification data [17]. A number of methods for record linkage have been presented and evaluated [7, 18-20]. Quantin et al. have done a comparison on statistical methods to provide data anonymity against preserving data confidentiality using encryption methods in epidemiological environment [21]. A group of researchers from Aalborg University, Denmark, have proposed a solution to protect user-sensitive data with context-aware privacy protection mechanism by filtering the data before any disclosure in a medical environment [22].

One of our previous papers [23] addresses authentication and privacy concern in electronic healthcare environment and ways to prevent it using the technologies such as Web services, Generic Authentication Architecture from 3GPP and Universal Mobile Telecommunications System (UMTS). The system proposed in this paper is based on the Single-Sign-On (SSO) and XML security technologies. The SSO technology lets user authenticate to a single authentication authority once and allows accessing all the authentication-protected resources and services without re-authentication [24]. The protocol developed in this study follows the SSO model based on Liberty Alliance standards and guidelines [25].

3. Proposed Architecture

A patient with a web browser/mobile device connects to the healthcare service unit (HSU) over the Internet/mobile network in the proposed anonymously accessible medical environment. This HSU and medical environment is owned by a publicly trusted organisation for medical services. The healthcare service providers (HSP) such as private medical centres and general practitioners provide healthcare services to patients. These services have to be registered using an offline methodology with the HSU before providing any services. The HSU authenticates and authorises patient for accessing service providers. The patient registers with healthcare service providers before accessing any services and registration process is performed through the HSU as shown in Figure 1. Once the registration process is completed the patient can access services with a hidden identity to the healthcare service provider. However the patient identity is disclosed to HSU for the patient authentication into the environment. Based on the identity and credentials the patient is authenticated and authorized to access healthcare service providers through HSU.

However patient identification is not disclosed to the healthcare service providers. The HSU acts as an anonymous identity provider, user authenticator and service access storage.

4. Protocol

The protocol presented in this paper provides an anonymous authentication for patients to access healthcare service providers. Patients receive medications over the Internet or mobile network without revealing their true identity. The following conditions must be satisfied prior to the use of the protocol.

- Many healthcare service providers are registered with the HSU.
- The HSU and healthcare service providers maintain an asymmetric key secure communication channel between them.
- Each HSP has more than one registered patient through HSU for anonymous access.

4.1 Patient Registration with the HSP

The patient registers with the HSP using the authentication at HSU. The sequences of exchanged messages (Fig. 1) are as follows:

- **Patient to HSU;** the patient makes a request to register for an anonymous service access with healthcare service provider.
- **HSU to patient;** HSU generates and sends the registration token and a temporary session key (tsK). The temporary session key is used for the secure communication between the patient and the healthcare service provider.
- **HSU to HSP;** the HSU sends the registration request token to HSP.
- **Patient to HSP;** the patient sends the registration token with HSP offline/-online service access information to HSP. The service access information is an option field in the message and it is encrypted using the tsK.
- **HSP to HSU;** HSP sends the registration confirmation message to the HSU if the registration request token is validated successfully with the patient registration token. With the successful confirmation HSU records the identity of the patient with the healthcare service provider's identification.

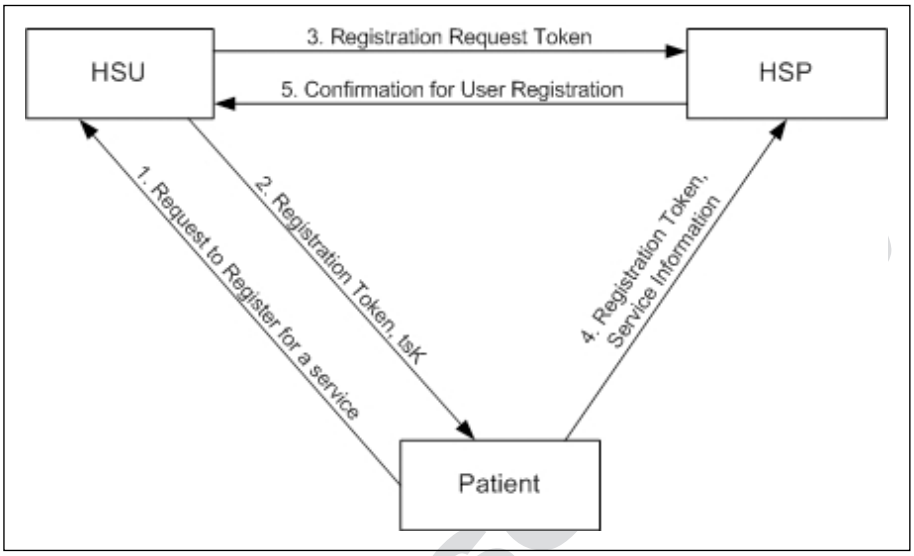

Fig. 1 Patient registration with HSP

4.2 Patient Authorization and Anonymous Service Access

The patient authorises to access services from HSP using the authorization provided by HSU. The sequences of exchanged messages (Fig. 2) are as follows:

- **Patient to HSU;** the patient requests to access a healthcare service provider anonymously by sending the healthcare service provider's identity.
- **HSU to patient;** the HSU generates a temporary user identity for the patient and it is a random number for each service request. The temporary session key (tsK) is generated by the HSU to establish a secure communication channel between the patient and the healthcare ser-

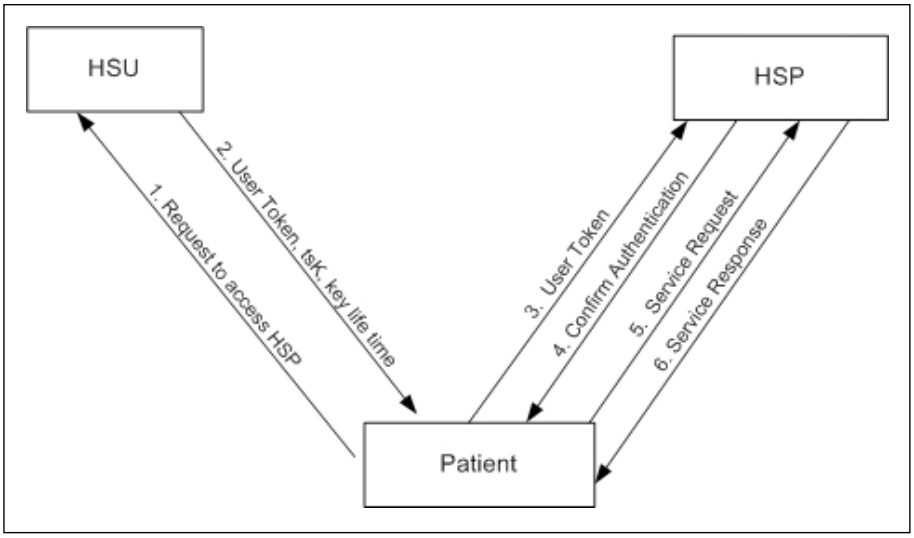

Fig. 2 Patient authorization and anonymous service access

vice provider. The HSU sends the tsK, key life time and user token to the patient. HSU records the user identity, temporary user identity, service provider identity and timestamp in its database.

- **Patient to HSP;** the patient sends the user token as the login request to healthcare service provider. The patient will be an anonymous user to the HSP since the user token doesn't have any parameters to identify the true identity of the patient but it confirms that patient is a registered user at the HSP and he/she is authorized to access services.
- **HSP to patient;** the healthcare service provider validates user token and sends the confirm authentication message to the patient.
- **Patient to HSP;** patient sends the service request message to healthcare service provider and it is secured using the tsK.
- **HSP to patient;** the healthcare service provider responses to the message with encrypting the response using the tsK.

The patient can send many service requests to the same healthcare service providers until the temporary session key is expired. If it is expired or the patient wants to change the healthcare service provider then patient has to do a new service access request to the HSU. Then the HSU will generate a new temporary session key and temporary identification for the patient.

5. Security Tokens

The following are tokens deployed in the proposed schema and authors have reduced sizes and complexity of tokens as much as possible due to the processing power constrains of the mobile device and bandwidth constrains in the mobile networks.

- RegistrationToken
  (RT = eHSP (sHSU [UID|TS])); used by the healthcare service provider to identify and authenticate legitimate patient registration requests that are validated from the HSU. It consists with the user identification created by the HSU and the timestamp. The registration token is signed by the secret key of HSU and it is encrypted using the service provider's public key.
- RegistrationRequestToken
  (RRT = eHSP (sHSU [UID|TS|tsK|KeyLifeTime])); used by the healthcare service provider to identify legitimate patient registration requests from HSU. It consists with the user identification of patient, temporary session key, key life time and the timestamp. The RegistrationRequestToken is signed by the HSU secret key and encrypted using the service provider's public key.
- UserToken
  (UT = eHSP (sHSU [TUID|TS|tsK|KeyLifeTime])); used by the healthcare service provider to authorize anonymous service access requests from patients. It consists with temporary user identity, timestamp and temporary session key and key life time. The UserToken token is signed by the HSU secrete key and encrypted using the service provider's public key.

Following are the implementation of tokens as XML objects. However these snapshots are taken before the XML encryption and XML signature are applied.

- RegistrationToken

```
<RegistrationToken>
   <UID>String</UID>
   <TimeStamp>Time
     stamp</Time Stamp>
</RegistrationToken>
```

- RegistrationRequestToken

```
<RegistrationRequestToken>
   <UID>String</UID>
   <TimeStamp>Timestamp</
    TimeStamp>
   <TempSessionKey>Key</
    TempSessionKey>
</RegistrationRequestToken>
```

- UserToken

```
<UserToken>
   <TempUID>String</TempUID>
   <TimeStamp>Timestamp</
    TimeStamp>
   <TempSessionKey>Key</
    TempSessionKey>
   <KeyLifeTime>Time</
    KeyLifeTime>
</UserToken>
```

6. Risk Analysis

The above healthcare environment is proposed as a solution to the privacy and security threats in the electronic and mobile healthcare environments. This section will discuss the possible threats that exist in the distributed healthcare environment and show how the proposed protocol can protect some of the possible security and privacy issues.

6.1 User Anonymity

The patient identity is only known by the healthcare service unit which is a trusted organisation by all the users and healthcare service providers. The healthcare service unit authenticates and authorizes patients at the healthcare service provider with a temporary identification. The patient obtains distinct temporary identification for each service access request to the same healthcare service provider. The temporary identification is a random number and it doesn't have any relationship with the true identification of the patient. There are no relationships between temporary identifications that belong to the same patient or those generated for the same healthcare service provider access. Therefore healthcare service providers are unable to trace back the temporary identity to the real identification of the patient. So the patient identification is not disclosed to healthcare service providers and third parties who are interested to gather health-sensitive information.

6.2 Message Privacy

The patient health-sensitive information and the patient identification are not linked to any parties in the proposed environment. For example the patient identity is disclosed to the healthcare service unit but it doesn't receive any patient health-sensitive information. Meanwhile the healthcare service providers have access to patient health-sensitive information but they are unable to trace the patient identity. Therefore the patient privacy is protected in the proposed healthcare environment.

6.3 Message Confidentiality

A secured confidential communication channel is established between the healthcare service unit and the patient web browser/mobile device based on the asymmetric/symmetric encryption and the patient uses the secure channel for the authentication with the healthcare service unit. Therefore the patient authentication requests and tokens are protected from eavesdroppers. The communication between the patient and healthcare service providers is protected using the symmetric key encryption technology. Therefore the patient-sensitive health records are protected from eavesdroppers and the patient privacy is protected.

6.4 User Authentication and Authorization

Patient authenticates to the healthcare service unit by providing his/her identification details and password or relevant credentials. Once the authentication process is successful patient can request authorization to healthcare service providers from the healthcare service unit. The user token is generated by healthcare service unit and with the validity of the user token the healthcare service provider authorizes the patient for healthcare services.

6.5 Replay Attacks

Tokens generated during the authentication and authorization process consist of timestamps to prevent replay attacks. An eavesdropper could capture login request message of a previous protocol between a patient and a healthcare service provider. The attacker might later replay that message trying to impersonate the patient to the healthcare service provider. This attack will not succeed if the healthcare service provider validates the timestamp of the requested message. These tokens are integrity-protected and attackers are unable to alter the timestamps before the attack.

6.6 Reverse Identity Track and Record Linkage

The proposed system provides medication without identifying the user due to the anonymous identification by the healthcare service unit. However healthcare service provider maintains a temporary identity for each patient request. This identification can be used to uniquely identify the patient between the service provider and healthcare service unit. The healthcare service unit maintains mapping between the patient true identity and the temporary identity but this information is not revealed to external bodies. The healthcare service providers may want to contact patients after the medication due to some critical medical situations such as wrong diagnosis or uncovered health risk by research. In these circumstances the proposed system has the capability of tracking the true identification of the patient through healthcare service unit. However healthcare service unit has the complete privilege to make the reverse track identification. If needed in the future, they can request patient to re-access the healthcare service provider with the same temporary identity rather than disclosing the patient identity to the healthcare service provider. The same identity mapping functionality at the healthcare service unit will be used to link all anonymous medical histories of a patient to a single medical report for future medications.

7. Conclusion

This paper described a medical environment that a patient can access without disclosing his identity. There are several situations in which the patient is very reluctant to approach the doctor or a medical expert for advice due to the sensitivity of the medical condition. Also medical records consist of highly sensitive data and it is vital to protect the patient privacy against misdemeanours activities. The anonymous access control protocol defined in this paper will provide the way forward for secure future online/mobile healthcare systems including the functionalities such as reliable record linking and securely reverse tracking anonymous patients to the real identity.

References

1. Wang J, Du H. Setting up a wireless local area network (WLAN) for a healthcare system. International Journal of Electronic Healthcare 2005; 1 (3); 335-348.
2. Weerasinghe D, Elmufti K, Rajarajan M, Rakocevic V. Xml security based access control for healthcare information in mobile environment. Proceedings of the Pervasive Health Conference and Workshops, 2006; 2006 Nov 29; Innsbruck, Austria. IEEE Explore; 2006. pp 1-6.
3. Gritzalis S, Lambrinoudakis C, Lekkas D, Defterereos S. Technical guidelines for enhancing privacy and data protection in modern electronic medical environments. IEEE Transactions on Information Technology in Biomedicine 2005; 9 (3): 413-423.
4. Rindfleisch TC. Privacy, information technology, and healthcare. Commun. ACM 1997; 40 (8); 92-100.
5. Data Protection & Medical Research, Parliamentary POSTnote, Parliamentary Office of Science and technology, January 2005 (cited 2007 Nov 10); 235. Available from: www.parliament.uk/documents/upload/POSTpn235.pdf.
6. Kerkri EM, Quantin C, Allaert FA, Cottin Y, et al. An approach for integrating heterogeneous information sources in a medical data warehouse. Journal of Medical Systems 2001; 25 (3): 167-176.
7. Christen P. Privacy-preserving data linkage and geocoding: Current approaches and research directions. Proceedings of the Sixth IEEE International Conference on Data Mining. Hong Kong, 2006.
8. Quantin C, Binquet C, Allaert FA, Gouyon B, Pattisina R, Le Teuff G, Ferdynus C, Gouyon JB. Decision analysis for the assessment of a record linkage procedure. Methods Inf Med 2005; 44; 72-79.
9. Geller LN, Alper JS, Billings PR, Barash CI, Beckwith J, Natowicz MR. Individual, family, and societal dimensions of genetic discrimination: A case study analysis. Science and Engineering Ethics 1996; 2 (1); 71-88.
10. Alan WM. Buying prescription drugs on the internet: Promises and pitfalls. Clevel Clin j med 2006; 73 (3); 282-288.
11. Eysenbach G, Diepgen TL. Patients looking for information on the Internet and seeking teleadvice: motivation, expectations, and misconceptions as expressed in e-mails sent to physicians. Arch Dermatol 1999; 135: 151-156.
12. Eysenbach G, Diepgen T. Responses to unsolicited patient email requests for medical advice on the World Wide Web. JAMA 1998; 280 (15); 1333-1335.
13. Kakizaki Y, Yamamoto H, Tsuji H. A method of an anonymous authentication for flat-rate service. Journal of Computers 2006; 1 (8); 36-42.

14. Leszczyna R. The solution for anonymous access of IT services and its application to e-health counselling. Proceedings of the 1st IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS '05), September 2005.
15. Kelman CW, Bass AJ, Holman CD. Research use of linked health data – a best practice protocol. Aust N Z J Public Health 2002; 26: 251-255.
16. Quantin C, Bouzelat H, Allaert FA, Benhamiche AM, Faivre J, Dusserre L: How to ensure data security of an epidemiological followup: quality assessment of an anonymous record linkage procedure. Int J Med Inf 1998; 49(1); 117-122.
17. Quantin C, Bouzelat H, Allaert FA, Benhamiche AM, Faivre J, Dusserre L. Automatic record hash coding and linkage for epidemiological follow-up data confidentiality. Methods Inf Med 1998; 37: 271-277.
18. Oberaigner W. Errors in Survival Rates Caused by Routinely Used Deterministic Record Linkage Methods. Methods Inf Med 2007; 46 (4): 420-424.
19. Churches T. A proposed architecture and method of operation for improving the protection of privacy and confidentiality in disease registers. BMC Medical Research Methodology 2003; 3 (1): 1-13.
20. Galanti MR, Siliquini R, Cuomo L, Melero JC, Panella M, Faggiano F. Testing anonymous link procedures for follow-up of adolescents in a school-based trial: The EU-DAP pilot study. Prev Med 2007; 44 (2): 174-177.
21. Quantin C, Allaert FA, Dussere L. Anonymous statistical methods versus cryptographic methods in epidemiology. Int J Med Inf 2000; 60: 177-183.
22. Mitseva A, Imine M, Prasad NR. Contextaware privacy protection with profile management. Proceedings of the 4th international workshop on Wireless mobile applications and services on WLAN hotspots, New York, NY, USA. ACM Press; 2006. pp 53-62.
23. Elmufti K, Weerasinghe D, Rajarajan M, Rakocevic V, Khan S. Privacy in mobile web services ehealth. Proceedings of the Pervasive Health Conference and Workshops, 2006; 2006 Nov 29; Innsbruck, Austria. IEEE Explore; 2006. pp 1-6.
24. Hillenbrand M, Gotze J, Muller J, Mullar P. A Single Sign-On Framework for Web-Services-based Distributed Applications. Proceedings of the 8th International Conference on Telecommunications ConTEL; 2005 June 15-17; Zagreb, Croatia. IEEE Explore; 2005. pp 273-279.
25. Liberty id-ff architecture overview. Technical report. Liberty Alliance, April 2003.

Correspondence to:
M. Rajarajan
School of Engineering and Mathematical Sciences
City University
Northampton Square
London, EC1V 0HB
UK
E-mail: R.Muttukrishnan@city.ac.uk