Consumer-Centric and Privacy-preserving Identity Management for Distributed e-Health Systems

Richard Au
Faculty of Information Technology
Queensland University of Technology, Australia
w.au@qut.edu.au

Peter Croll
Faculty of Information Technology
Queensland University of Technology, Australia
p.croll@qut.edu.au

Abstract

A new framework of privacy-preserving identity management for distributed e-Health systems is proposed. Utilizing a consumer-centric approach, the healthcare consumer maintains a pool of pseudonymous identifiers for use in different healthcare services. Without revealing the identity of consumers, health record data from different medical databases distributed in various clinic/hospitals can be collected and linked together on demand. While pseudo-anonymity preserves user privacy, the architectural design allows the anonymity to be revoked by a trusted authority under well-defined policies with legal-compliance. This framework inherits the advantages in centralized management for distributed medical databases. Security of the interactions among different entities in the architecture is guaranteed by certification and cryptographic technologies.

1 Introduction

Healthcare systems around the world are moving towards the integration of health data sources. The main objectives are to improve the efficiency in healthcare services through data sharing, and to revolutionize clinical research by supporting population-based epidemiologic studies. However, this development has heightened concerns about the right of healthcare consumers to protect their privacy in the e-Health system. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) [10] legislation introduced regulations relating to data security and privacy within the healthcare sector. European Union issued the Recommendation R(75) [14] and Privacy Directive [13].

In the Common Criteria [8], which contributes to the development of an international standard for evaluation of IT security, privacy is described as the right of individuals to be left alone. The privacy class can be decomposed into the following characteristics:

- Anonymity - A consumer may use a resource or service without disclosing the consumer's identity.
- Pseudonymity - a consumer may use a resource or service without disclosing its consumer identity, but can still be accountable for that use.
- Unlinkability - a consumer may make multiple uses of resources or services without others being able to link these uses together.
- Unobservability - a consumer may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

In the health sector, healthcare consumers have good reason to seek more confidential management of their personal health data. They are unwilling to have their personal information distributed other than for purposes of clinical care and they like to be consulted before their information is released [16]. A key component of user privacy is preserving the consumers ability to remain anonymous [5, 7, 12]. However, anonymity affects many security requirements, such as accountability, authenticity and non-repudiation. Full anonymity leads to increased abuse usage by anonymous users and present

1530-1605/08 $25.00 © 2008 IEEE

an unacceptable level of security risk to the system. In pseudonymity systems, anonymity can be revoked in a well-regulated manner, preferably with the involvement of neutral trusted authorities.

On the other hand, controlled linkability of health record data is needed in the health sector. Medical researcher needs to collect and correlate health record data for the purpose of clinical research studies. The availability of this information is crucial for improvements in medical and surgical care, clinical-research and some medical education programs. The linkability of health data also benefits the patients in the healthcare service if the doctor can retrieve all relevant medical records of the patient efficiently and determine the best medical treatment.

The question of interest is how to assure security and privacy while allowing health record data to be accessible by authorized people. In this paper, a secure and privacy-preserving architecture for the e-health system is proposed. Each healthcare consumer can use different identifiers (pseudonyms) in different medical consultations to preserve user privacy. Sensitive medical information can be collected from distributed health record databases in different clinic/hospitals and linked together dynamically without revealing the consumer's real identity. The architectural design also allows the revocation of anonymity under well-defined policies with legal-compliance.

The paper is organized as follows. Section 1 gives an introduction. In Section 2, the proposed anonymous architecture is overviewed with different entities described. In Section 3, the concept of personal identity tree and various certificates for use in the anonymous health services are introduced. In Section 4, security protocols for communications between different entities in the architecture are described with some security analysis. Section 5 describes how health record data can be linked and how the anonymity can be revoked. In Section 6, some prototype systems are briefly described. The paper finishes with a conclusion and some future works in Section 7.

2 Architectural Overview

Referring to Figure 1, there are four main entities in the proposed framework for e-Health systems.

Healthcare consumer/Client

The healthcare consumer initiates communication with the health service provider requesting access to service or resource. After receiving the requirements for granting access, the consumer requests appropriate external referral servers to issue some referral credentials.

External Referee

In the real world, a consumer has many relationships with commercial or governmental entities. For example, a person has a credit account in a credit card company, a driving license from the transport department and a variety of memberships in various health insurers or clubs. Different business relationships exist among these organizations and a trust infrastructure has been formed. These external entities can act as referee servers and provide referrals to their clients upon requests. User identification/authentication may be required before issuing referrals to the client.

Health Service Providers

The health service provider determines whether to grant the service or not based on the assessment of the referral credentials submitted by the client. Clearly, it is assumed that the service provider has some trust relationships with different referee servers involved and accepts those certified attributes they supply. A health service provider can also act as a referee server to provide referrals to its consumer so that he can access a healthcare service provided by another health service provider.

Trustee Infrastructure

The trustee is a trusted authority providing a centralized identity management service to different entities in the e-Health system. It is independent of any other entities (health service providers or referees) and has three important functions:

- To generate identifiers and certificates for requesting clients;
- To ensure the integrity and uniqueness of the identifiers;
- To provide identity escrow service and manage the revocation of anonymity.

A trustee server is used to serve local clients in its administrative domain. As some trustee services involve entities in foreign administrative domains, an infrastructure of domain-based trustee servers is needed so that the trustees can work collaboratively in a federation. Taking an example in the identity escrow service, a health service provider can lodge the application of anonymity revocation to a local trustee. Upon approval, the request is forwarded to the designated trustee (may be in a foreign administrative domain) to provide the necessary revocation. The revoked identity information can be delivered to the service provider directly or through the local trustee in a secure channel.

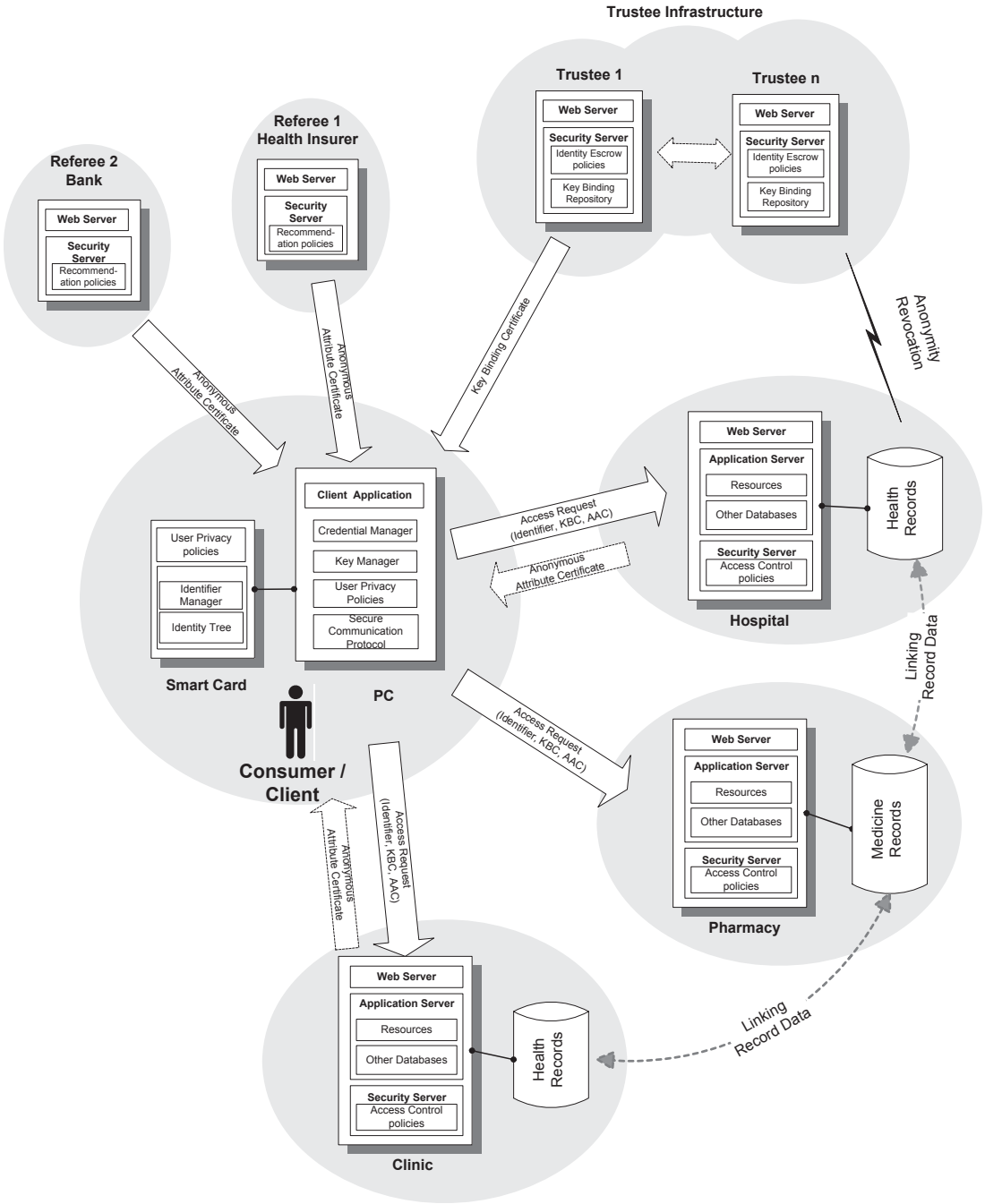

Figure 1. Consumer-Centric Anonymous Authorization for e-Health System

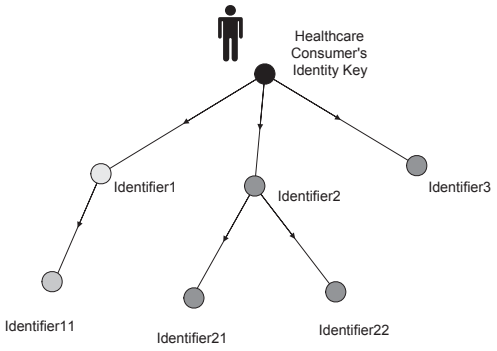

Figure 2. Personal Identity Tree

3 Consumer-centric Identity Management

Every consumer/client has a unique identity and holds a pool of identifiers in his personal secure device. Each identifier can be used independently or two identifiers can be correlated in a chain using a Key Binding Certificate (KBC). Thus, the identifiers for the same client can be organized in a hierarchical or other structure as illustrated in Figure 2.

3.1 Cryptographic Key as Pseudonymous Identifier

In our proposal, the trustee generates a cryptographic key pair and issues to the consumer. The public key is used as an identifier in a medical consultation or other activities. The private key is stored securely in a personal secure device and can be used for authentication and digital signing purposes. The design has the following advantages:

- *Anonymity Support and Enhanced Privacy*: Pseudonymous Identifiers are used directly in health records without reference to the unique identity of the consumer. The consumers can remain anonymous without taking any special measures. It becomes difficult to correlate different activities of a single consumer over time because the public keys used as the explicit identifiers in the activities, are randomly scattered. Using different identifiers when communicating with different entities, or when performing different unrelated tasks, prevents the easy combination of gathered information for the many roles of a single entity.
- *Higher Security*: While identities/names of consumers are not explicitly advertised, attackers must systematically collect intelligence data about the system and analyze it in order to identify individual entities and their activities. As the explicit identifier is different for each service, the risk of certain security threats, e.g. eavesdropping and replay, can be reduced. Even if an attacker manages to compromise a key used in one service, only information for one activity is disclosed. Since other activities are independent, the scope of damage to the system may be confined and reduced.

3.2 Key Binding Certificate (KBC)

A Key Binding Certificates (KBC) issued by the trustee is used to certify the binding of an identifier to the identity key or another identifier. Its access is restricted in order to preserve the anonymity of the consumer. Following the format of an X.509 certificate [11], the contents of a KBC is showed in Figure 3. Note that the two independent cryptographic keys in a KBC can be of different ciphers and key lengths to suit different security requirements in different systems.

3.3 Anonymous Attribute Certificate (AAC)

When the client make a request to a health service provider for a service, he can submit his identity certificate and complete the authentication process in standard way. Alternately, the proposed architecture allows the client to request access anonymously using one of his identifiers and some Anonymous Attribute Certificates (AACs). AACs are the referral credentials issued by various external referee servers or other health service providers to a registered consumer. In such option, the service provider does not need to reveal the real identity of the client but can grant the service based on the assessment on the AACs submitted by the client. Taking as an example, a patient, who has joining a drug abuse recovery program, does not want to disclose his real identity in his daily treatment in the clinic. While the client is identified by the identifier in the AAC, the revocability of anonymity is guaranteed by the trustee, who generates a *trustee signature* by signing the identifier with the trustee's private signing key in the AACs.

User attributes are bound to an identifier in a *Anonymous Attribute Certificate* while the identifier is bound to the identity key in a *Key Binding Certificate*, as illustrated in Figure 3.

4 Interactions and Protocol Overview

With the introduction of pseudonymity in the system, the security in the communications between different entities using these identifiers is the first concern. In the context of an e-Health environment, some security protocols are proposed as below and they are shown to be able to prevent

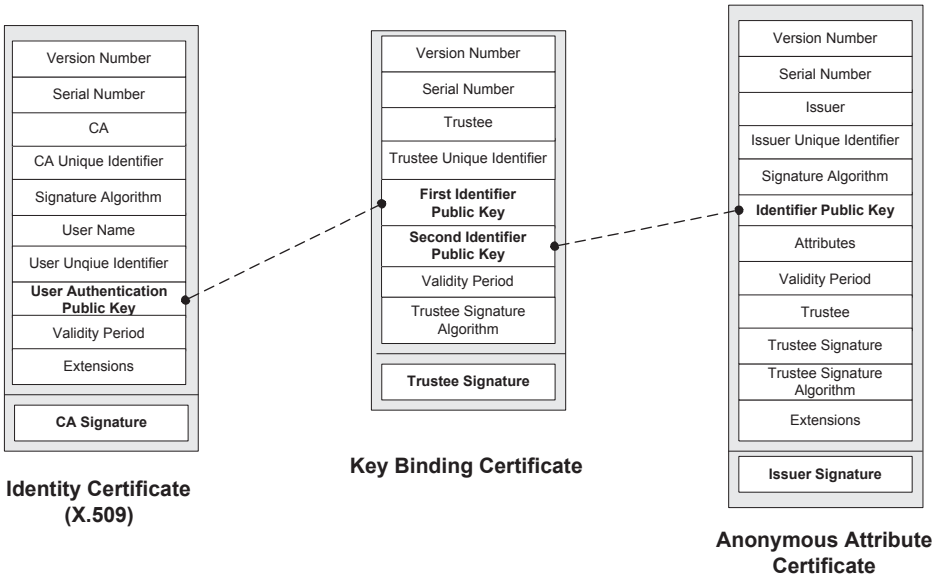

Figure 3. Binding Various Certificates

some main attacks related to pseudonyms, such as colluding user attack, replay attack and impersonation attack [4].

4.1 Security Protocols

In this proposed architecture, we assume that an existing Public Key Infrastructure (PKI) is in place and each registered entity is issued a unique public/private identity key pair and a public key (identity) certificate. The notations introduced in Table 1 are used.

Abbreviation	*Description*
U	Consumer/client
ERS	External Referee Server
HSP	Health Service Provider
TS	Trustee Server
AA	Authorization agent
SN	Serial Register Number
Q_{ACC}	Access request
Q_{REF}	Referral request
Q_{IDK}	New IDK pair request
K_A, K_A^{-1}	Public/private identity key pair of A
AAC_n	n*th* Anonymous Attribute Certificate
IDC_U	Identity Certificate of U
KBC_U	Key Binding Certificate of U
IDK_U, IDK_U^{-1}	Public/private identifier key pair of U
$\{m\}_{K_U}$	Encryption of message m with public key of U
$[m]_{K_U^{-1}}$	MAC digest/Signature of message m using private key of signer U
AT_n	n*th* Authorization Token

Table 1. Notations

Phase 1. Acquiring a New Identifier from Trustee

The protocol begins when a healthcare consumer U requests for a new identifier in the form of a public/private key pair from the designated trustee server TS. U sends the "new identifier request" Q_{IDK} to TS, together with U's identity certificate IDC_U (which contains U's public identity key K_U) and a randomly chosen nonce N_U, encrypted using TS's public key. The use of nonce N_U ensures that an old message cannot be replayed.

TS proceeds to generate a new public/private identifier key pair $\{IDK_U, IDK_U^{-1}\}$ that has yet to been assigned, using a secure random key generator algorithm. Then TS creates a key binding certificate KBC_U to associate K_U with IDK_U, which will be the new identifier for the consumer. TS computes the ciphertext α, which is the encryption of KBC_U, IDK_U^{-1} and the nonce N_U originated from U, using the requesting client's public key K_U. Then TS signs on α, P_1 and IDC_U using K_{TS}^{-1}. TS will then send the ciphertext α and the signature to U. Upon receiving the message, U decrypts α with K_U^{-1} to retrieve the new IDK_U^{-1} and KBC_U, which contains IDK_U. Using TS's public key, U can verify the signature. If the verification returns true, then U will terminate the protocol run and accept $\{IDK_U, IDK_U^{-1}\}$.

1. U $\longrightarrow$ TS : $\{IDC_U, Q_{IDK}, N_U\}_{K_{TS}}$
   $[\{IDC_U, Q_{IDK}, N_U\}_{K_{TS}}]_{K_U^{-1}}$
2. TS $\longrightarrow$ U : $\{KBC_U, IDK_U^{-1}, N_U\}_{K_U}$,
   $[IDC_U, \{KBC_U, IDK_U^{-1}, N_U\}_{K_U}]_{K_{TS}^{-1}}$

Phase 2. Requesting Service from Service Provider

The consumer U encrypts the public IDK_U, the access request Q_{ACC} and a randomly chosen nonce N_U, using the public key of HSP, with whom U desires to communicate, to form a ciphertext α_U. U signs on α_U and IDK_U^{-1} and then sends α_U together with the signature to HSP.

Upon receiving the message, HSP decrypts the ciphertext received with HSP's private key to obtain IDK_U (which is U's unique identifier) and Q_{ACC}. HSP can then verify the signature to determine if the message received originates from U. Once the verification is satisfied, HSP assigns an authorization agent AA and a unique serial register number SN to U.

1. U $\longrightarrow$ HSP : $\{IDK_U, Q_{ACC}, N_U\}_{K_{HSP}}$, $[\{IDK_U, Q_{ACC}, N_U\}_{K_{HSP}}]_{IDK_U^{-1}}$
2. HSP $\longrightarrow$ U : $\{AA, SN, N_U\}_{IDK_U}$, $[\{AA, SN, N_U\}_{IDK_U}]_{K_{HSP}^{-1}}$

Phase 3. Requesting Referrals from Referees

Upon receiving the message from HSP, the client U can execute the authorization agent on the client platform to reveal all the requirements and conditions for the access of the service. Then U may need to request for referral credentials from one or more external referee servers or other health service providers. If U need to request for referral credentials from n external referee servers, the protocol shown below is executed n times.

1. U $\longrightarrow$ ERS : $\{IDC_U, KBC_U, Q_{REF}, N_U\}_{K_{ERS}}$, $[\{IDC_U, KBC_U, Q_{REF}, N_U\}_{K_{ERS}}]_{IDK_U^{-1}}$
2. ERS $\longrightarrow$ U : $\{AAC, N_U\}_{IDK_U}$, $[U, \{AAC, N_U\}_{IDK_U}]_{K_{ERS}^{-1}}$

Phase 4. Accessing Service on Service Provider

Once U has collected the required referral credentials in the form of Anonymous Attribute Certificates (AACs), U will send these AACs to HSP. Based on the submitted referral credentials $\{AAC_1, \ldots, AAC_n\}_{K_{HSP}}$, the service provider will reach a decision on whether to grant the authorization token AT_1, which is used as a credential for the consumer to access the healthcare service later on.

1. U $\longrightarrow$ HSP : $\{IDK_U, AAC_1, \ldots, AAC_n, SN, N_U\}_{K_{HSP}}$, $[\{IDK_U, AAC_1, \ldots, AAC_n, SN, N_U\}_{K_{HSP}}]_{IDK_U^{-1}}$
2. HSP $\longrightarrow$ U : $\{AT_1\}_{IDK_U}$, $[SN, N_U, \{AT_1\}_{IDK_U}]_{K_{HSP}^{-1}}$

4.2 Security Analysis

The primitives used in the proposed protocol are the relatively standard notions of a secure encryption scheme and a secure message authentication scheme. The protocol is secure if the underlying message authentication scheme is secure in the sense of existential unforgeability and the underlying encryption scheme is indistinguishable under various cryptanalysis attacks.

The proposed architecture addresses the five general requirements on anonymous credential systems using pseudonyms introduced by Camenisch et al. [6]:

- Security - The identifiers used by different clients should be unique and unforgeable.
- Non-Transferability - A consumer cannot share an identifier with another person.
- Separation of Duties - Different entities, i.e. trustee, health service provider, referee, consumer, in the architecture have different duties. More than one entities are involved in creating a health record or reveal all the medical records related to a patient.
- Unlinkability - Different health records cannot be linked to a particular consumer unless the consumer or the trustee disclose the identity tree.
- Revocable anonymity - The mechanism for revealing the identity of consumer is achieved by the introduction of the trustee and Key Binding Certificate in the architecture.

Below is some security analysis of the protocol considering some common attacks related to the proposed anonymous e-Health system.

Replay and Substitution Attacks Since a randomly chosen (fresh) nonce N_U is included in every message (either in the encryption or signature) that is sent by the client U, old messages cannot be replayed. If a malicious adversary $\mathcal{A}$ substitutes the message with an old message, U will detect this attack in the reply message it receives as the nonce from U is included in the reply message. Alternatively, time-stamps can be also used (instead of a nonce). Hence, the improved protocol is secure against replay and substitution attacks.

Impersonation and Man-in-the-Middle Attacks Messages originated from the client U is always encrypted with the public key of the designated recipient. Although a malicious adversary $\mathcal{A}$ can intercept and/or replace the intercepted message with other message of her choice, $\mathcal{A}$ is not able to decrypt the intercepted message without

knowledge of the corresponding private key. Messages sent to U consist of an encryption of some messages under U's IDK_U, and a signature consisting of the earlier encryption with some other messages under the sender's private key. Again, $\mathcal{A}$ is not able to decrypt the intercepted message without knowledge of the corresponding IDK_U^{-1}.

Colluding Service Provider Attacks If different service providers collude, they can link the AACs using the same IDK. However, the identity of the client is preserved (i.e., not revealed or leaked) since neither the key binding certificate nor the identity key certificate are sent in the messages by an individual client to the service providers. Hence, the improved protocol is secure and provides client privacy even if service providers collude. Since the trustee is tasked with issuing unique IDK pairs for every individual task (requested by the registered client), the IDK pair is unlinkable with previous activities.

5 Management of e-Health Data

The proposed approach assumes a level of cooperation can be reached between healthcare organisations. It is recognized that this is not always possible particularly when support and funding is required from organisations that span both private and public sectors or different authorities, either from a regional or healthcare provision viewpoint, e.g. primary or hospital. Some countries have an advantage here, in particular the UK, Canada and New Zealand for example, which inherently have a national approach to healthcare provision. Australia is typical of a country where a patient's episodes can transverse a mix of public and private provision spanning different levels of service. While the disparate healthcare providers recognize the mutual advantages in a more unified approach they are not necessarily in a position to fund solutions that provide for continuity of care. Significant funding has been provided by the Australian government to both promote and standardizse electronic health. This was initially through the HealthConnect scheme and more recently through the National E-Health Transition Authority [1]. NEHTA's work to date has focussed on the shared electronic health record and national solutions to address this with unique identifiers for patients and clinicians plus standardisation on terminology, e.g. SNOMED CT. Some Australian states are closely monitoring developments at the national level while making their own moves towards their own patient-centric approach with healthcare provision, see [2]. It is envisaged that through such initiatives this research on consumer-centric identity management will be able to gain acceptance.

5.1 Linking Health Records

In a particular healthcare service or clinical research, it may be necessary to link together the health records of the same consumer who has used different identifiers. This should be authorized by the consumer according to his preset privacy policies. The consumer or the trustee with the consent of the consumer, can disclose the related Key Binding Certificates to link those identifiers together. Then the health service provider can link the related health records of the consumer together as shown in Figure 4. Alternately, the consumer can create signatures using his corresponding private keys to prove that he owns the identifiers. Note that this linkability of health records involves two parties, i.e. both the health service providers and either the trustee or the consumer. In this well-regulated environment, no single entity (neither the trustee nor health service providers) can exploit the system to compromise the consumer's privacy in his medical records.

In the process of linking health records in different medical database systems for research and analysis, other mechanisms, such as de-identification or k-anonymization can be used in parallel to further protect consumer's anonymity [3].

5.2 Anonymity Revocation Service

The revocation of anonymity should be authorized by a neutral trusted authority, preferable a law enforcement entity, e.g. the court, which should be external to the trustee infrastructure. Since the trustee act as an identity escrow agent to implement anonymity revocation, the trustee should hold a repository of identification information with the following fields in a record, namely: an individual consumer's public IDK, identity certificate (identity key) or another public IDK, and the expiry details. When situations require a service provider to trace the identity of the holder of an IDK in the AACs submitted by a consumer, the service provider can send a tracing request to the trustee whose identity appears in the AACs. However, this tracing request needs to be accompanied by some pre-agreed documentation issued by some court or law enforcement entities. Upon satisfying all requirements in the pre-defined policy, the trustee can then reveal the binding of the IDK and the consumer's identity key/certificate under supervisions of an external legal authority.

In the proposed architecture, the referee servers are prohibited from disclosing the association between a consumer's identity and the AACs issued. In a real world implementation, some legal binding agreements or legislation are required to reinforce this regulation. If referee servers collude with service providers, the consumer's identity in an activity can be revealed. However,

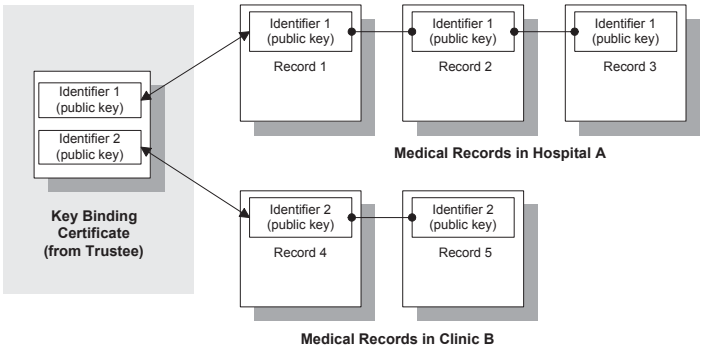

Figure 4. Linking Health Records

referee servers such as commercial banks, healthcare centres and governmental organizations are unlikely to violate these regulations, considering the legal and financial implications. Furthermore, individual consumers have the liberty of choosing referee servers with good reputations for issuance of AACs. Hence, this anonymous architecture provides a reasonable safe environment for real world e-health systems.

6 Prototype Systems

Research at Queensland University of Technologys Information Security Institute has developed a trusted computing platform for securing electronic health information. Based on Security Enhanced (SE) Linux the demonstrator platform has provided a framework for trailing policy-based security access control paradigms. Ongoing concerns have been raised over the effectiveness of information technology products and systems in maintaining privacy protection for sensitive data. The aim is to ensure that sensitive health information can be adequately protected yet still be accessible only to those that need-to-know. To achieve this and ensure sustainability over the longer term, it is advocated that an alternative, stable and secure system architecture is required. The adoption of a model targeted at health information that provides much higher degrees of protection. The long term aim is to provide a viable solution by utilizing contemporary, commercially supported operating system and allied software. This complementary research [17] outlines the advantages and limitations in its application with a medical database and considers the future needs in terms of research, software development and changes in organizational policy for healthcare providers. The architecture to support this utilises a three-tier architecture to implement a pragmatic roll-base access control (RBAC) proxy, see [9].

6.1 Use of Programmable Smart Card

In the proposed consumer-centric framework, the most innovative component is the use of a personal secure device to handle and manage different identifier for different healthcare services. While this personal secure device can be developed on an enhanced Personal Digital Assistant (PDA) or mobile phone with computing power and secure storage, a programmable smart card is chosen as the first prototype. The advantages of smart card include low-cost, high-security, portability, easy-of-use and acceptance by consumers. As the consumer's personal secure device, the smart card stores and manipulates his personal identity tree data. It can also provide a secure platform for hosting and execution of different software agents from different parties. The identifier manager, the software developed and installed on the smart card, can handle new identifiers downloaded from the trustee server and retrieve appropriate identifiers according to the privacy policies preset by the consumer. In our trial implementation, we use a Java card from Schumberger [15] with programming power to facilitate the following functions:

- Authenticating the consumer;
- Storing data of the personal identity tree securely;
- Storing sensitive data, such as private keys and certificates;
- Establishing session keys for secure communications;
- Providing an execution platform for the identifier manager.

The identifier manager is developed in the form of a Java cardlet installed onto the Java card. The smart card can communicates with the application program on the client workstation using APDU (Application Protocol Data Unit) commands. The client application can communicate with various servers via local network and/or the Internet.

7 Conclusions and Future Work

We have proposed a new privacy-preserving identity management framework for distributed e-health systems. In the consumer-centric approach, the anonymous scheme assures that the consumer can access various health services with privacy being well-protected. The anonymous attribute certificate is designed to provide dynamic authorization suitable for applications in open environments. Two components of the new architecture, namely: trustee and key binding certificate, facilitate a higher level of assurance to various service providers by providing the services of anonymity revocation and linking health record data.

Further directions for this work include formally implementation of the architecture in a controlled environment of an e-health system, and extending the infrastructure of the trustee for a more practical deployment in today's e-health settings.

As further work, several new challenges are particularly worth research efforts:

- *Standardization of anonymous attribute certificate* - While multiple parties across different domains are involved, the design of the attributes and other fields in the anonymous attribute certificates should provide effective and flexible translation of policies and management of trust between these related communities.
- *Security architecture and protocols* - The development of efficient and secure protocols in authentication and authorization services is crucial for e-health systems.
- *Extension of Trustee Infrastructure* - The infrastructure of the trustee needs to be extended to support the integration of healthcare systems across different domains or even countries.

References

[1] NEHTA 2006. *2005-2006 Annual Report for the National E-Health Transition Authority Limited (NEHTA)*. NEHTA, available at http://www.nehta.gov.au, 23 pages, accessed Sept 2007.

[2] QH 2006. *Queensland Health, e-Health Strategy, 12 Sept 2006*. Deloitte, available at http://www.health.qld.gov.au/ehealth/eh-strat-public.pdf, 79 pages, accessed Sept 2007.

[3] R. Agrawal, T. Grandison, C. Johnson, and J. Kiernan. Enabling the 21st century health care information technology revolution . In *Communications of the ACM*, volume 50, pages 35–42, 2007.

[4] R. Au, K. Choo, and M. Looi. A Secure Anonymous Authorisation Architecture for E-commerce. In *Proceedings of IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE' 05)*, 2005.

[5] V. Benjumea, J. Lopez, J. Montenegro, and J. Troya. A First Approach to Provide Anonymity in Attribute Certificates. In *Proceedings of PKC 2004, LNCS 2947*, pages 402–415, 2004.

[6] J. Camenisch and A. Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Advances in Cryptology - EUROCRYPT 2001: Second Symposium, PADO 2001*, pages 93–118. Springer-Verlag, 2001. Volume 2045 of Lecture Notes in Computer Science.

[7] R. Clarke. Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice. In *Proceedings of User Identification & Privacy Protection Conference*, 1999.

[8] Common Criteria. *Common Criteria for Information Technology Security Evaluation* . URL: http://www.commoncriteriaportal.org/public/files/CCPART2V3.1R1.pdf, 1995.

[9] M. Henricksen, W. Caelli, and P.R. Croll. Securing Grid Data Using Mandatory Access Controls. In *Proceedings of the fifth Australasian symposium on ACSW, ACM Intnl Conf*, volume 68, pages 25–32, 2007.

[10] HIPAA. *National Standards to Protect the Privacy of Personal Health Information*. Office for Civil Rights, URL: http://www.hhs.gov/ocr/hipaa/, 2001.

[11] International Telecommunication Union - Telecommunication Standardization Sector. X.509v3. In *URL: http://www.mcg.org.br/mirrors/97x509final.doc*.

[12] M. Koch and W. Worndl. Community Support and Identity Management. In *Proceedings of European Conference on Computer Supported Cooperative Work*, 2001.

[13] Council of Europe. *The Eurpean Union Privacy Directive*. Report 95/46/EC, 1995.

[14] Council of Europe. *On the Protection of Medical Data*. Recommendation R(75), 1997.

[15] Schlumberger. Cyberflex Access Programmer's Guide. In *http://www.cyberflex.com/Support/CyberflexPG.pdf*.

[16] R. Whiddett, I. Hunter, J. Engelbrecht, and J. Handy. Patients' attitudes towards sharing their health information. In *International Journal of Medical Informatics*, volume 75, pages 530–541, 2006.

[17] R. Whiddett, I. Hunter, J. Engelbrecht, and J. Handy. Utilizing SELinux to Mandate Ultra-secure Access Control of Medical Records. In *Proc. 12th World Congress on Health (Medical) Informatics, Building Sustainable Health Systems, Part 1, Medinfo 2007*, pages 498–503, 2007.