Universal Identity Management Model Based on Anonymous Credentials

Yang ZHANG
State Key laboratory of Networking and Switching Technology
Beijing University of Posts & Telecommunications
Beijing 100876, China
YangZhang@bupt.edu.cn

Jun-Liang CHEN
State Key laboratory of Networking and Switching Technology
Beijing University of Posts & Telecommunications
Beijing 100876, China
chjl@bupt.edu.cn

Abstract—The relationship-focused and credential-focused identity management are both user-centric notions in Service-oriented architecture (SOA). For composite services, pure user-centric identity management is inefficient because each sub-service may authenticate and authorize users and users need participate in every identity provisioning transaction. If the above two paradigms are unified into the universal identity management model where identity information and privileges are delegatable, user-centricity will be more feasible in SOA. This paper aims to extend WS-Federation to build a universal identity management model based on anonymous credentials, which provides the delegation of anonymous credentials and combines identity metasystem to support easy-to-use, consistent experience and transparent security. In addition, the concept of self-generated pseudonym is introduced to construct efficient anonymous delegation model.

Keywords—Privacy Concerns of Service-Oriented Solutions, Identity Management, Identity Metasystem, Privilege Delegation.

I. INTRODUCTION*

With the advent of identity management technology, users can consume services in Web service environment with privacy-preservation. In the SOA environment, a user often uses identity providers to provide identity information and his identity is represented by a set of attributes [1], [2]. Based on the user-centricity philosophy, identity management systems [3], [4] are classified as the relationship-focused and credential-focused [5]. In the relationship-focused identity management system, identity providers play an important role and are involved in each transaction conveying identity information to a service provider. The user only adopts identity providers to provide identity information and has control over his attributes. Therefore, the user participates in every identity provisioning transaction. On the contrary, the user obtains in the credential-focused approach long-term credentials from identity providers and stores them locally. Then, these credentials will be used to provide identity information without involving the identity provider. But the user is involved in every identity transaction as well.

A universal identity management system incorporates the advantages of both the user-centric system types to address the above issues [5] with delegation support. The credential-focused system is a good starting point for constructing a universal identity management system. However, how to extend WS-Federation [4] to build a universal identity management model based on anonymous credentials is still vague. In addition, it is difficult for our model to directly adopt anonymous credential schemes [6], [7], [8] to support anonymous delegation.

As a public specification, WS-Federation defines a framework to allow different security domains to federate, such that authorized access to web services can be realized in distributed realms. That includes mechanisms for brokering of identity, attribute, authentication and authorization assertions between domains, and privacy of federated claims. Based on WS-Trust [9], WS-Federation supports delegation by using identity providers to issue appropriate security tokens for providers in different security domains. As a relationship-focused framework, it also has the undesirable features of general relationship-focused paradigms. Our model extends this relationship-focused framework with enhanced credentials to achieve universal identity management.

Users are a key component in the SOA environment. Therefore, how to easy-to-use identity management systems and provide consistent experiences and transparent security is very critical in our model. The notion of Identity Metasystem [10], [11] has been introduced to put an abstract identity management layer on the Internet to allow existing identity systems based on various technologies to inter-operate with each other. Identity metasystem introduces the important concept of an "information card" modeled after a business card, license, etc. In general, an information card is a digital representation of user identity to realize easy-to-use and consistent experiences. However, the identity metsystems do not support delegation and composite services. In SOA, a service often consists of sub-services and delegation mechanisms are critical for efficiency. We combine the identity metasytem which is user perspective and WS-Federation framework which is service federation perspective, and extend them to the universal identity management model.

The contribution of this paper is two-fold. Our first contribution is that we extend WS-Federation to build a

* Supported by the National Natural Science Foundation of China under Grant No. 60432010; National Grand Fundamental Research 973 Program of China under Grant No. 2007CB307103; the National Science Foundation for Post-doctoral Scientists of China under No. 20090450335.

978-0-7695-4126-6/10 $26.00 © 2010 IEEE
DOI 10.1109/SCC.2010.46

universal identity management model based on anonymous credentials, which provides the delegation of anonymous credentials and combines identity metasystem to support easy-to-use, consistent experience and transparent security. Our second contribution is that the novel concept of self-generated pseudonym is introduced for anonymous credentials to reduce interaction rounds and complexity of anonymous delegation.

The remainder of the paper is structured as follows. Section 2 gives a description on the identity metasystem model. Section 3 contains our universal identity management model. Section 4 gives a healthcare example to illustrate our model. Section 5 focuses on analysis. Section 6 presents a discussion of related works. Finally, conclusions are drawn in Section 7.

II. Identity Metasystem

The goal of an identity metasystem is to guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies, to provide unambiguous human-machine communication mechanisms with easy-to-use, and to provide its users transparent security. The premise is that no single identity management system will emerge on the Internet. An abstract layer is needed for identity systems to interoperate with each other.

The identity metasystem model has three roles: the **resource**, the **identity provider** (IdP) and the **identity selector system**. A resource is any system capable of authenticating users based on their information cards. The IdP issues information cards to user and provides authentication service. The identity selector system is a core component to handle messages between a resource and an IdP. A user can use the identity selector system to securely manage his information cards. For example, when a user wants to access a resource, the resource first sends the security requirements on user authentication. Then information cards that satisfy the policies are displayed on the user's terminal. The user can choose one of these cards. Once the user selects a card, the identity selector completes the authentication of the user to the identity provider. Finally, the IdP verifies the request and issues a access token to identity selector.

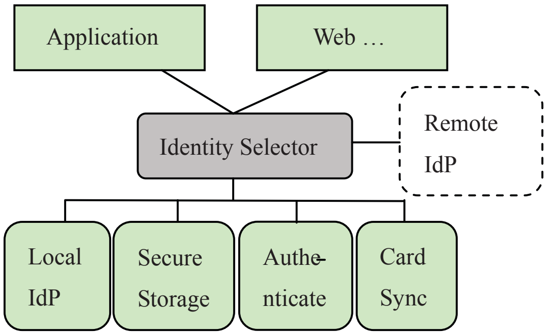

Fig.1. Basic Architecture of Identity Metasystem

Fig. 1 illustrates the basic architecture of identity metasystem. The identity selector system is main part of the metasystem model. The underlying is backup services such as local IdP, Secure Storage, and Card Sync. It supports different human-computer interfaces. Such identity metasystems include Microsoft Cardspace [11], [12] and Novel Bandit project [13].

The above two identity metasystem provide limited support for secure roaming where a user uses the same set of identities and credentials across different terminals. Bandit project is extended to support secure roaming by introducing trusted device and client being structured as a set of distributable components [14]. In our model, roaming identity metasystem is adopted as a basic concept. However, the identity metsystem and its extend do not support delegation and composite services. In SOA, a service often consists of sub-services and delegation mechanisms are critical for efficiency. We combine the identity metasytem which is user perspective and WS-Federation framework which is service federation perspective, and extend them to universal identity management model.

III. Universal Identity Management Model

A. Delegation Model Based on Anonymous Credential

The participants in a delegation model for universal identity management are identity providers (who grant credentials), user u (who obtains credentials), user v (who is delegated by u to access services) and service providers. Our model is different from the model of delegatable anonymous credential systems. As in the delegatable anonymous credential systems, a user first registers a pseudonym with the identity provider, and then the identity provider grants to the user a credential associated with the registered pseudonym. Compared with those schemes, our model allows a user first to get a credential from the identity provider, and then to generate multiple new pseudonyms as needed while the identity provider does not participates. The user can show to service providers without interacting with the identity provider that he possesses a right credential. In addition, the user can grant his credential to other users with prevention of misuse of delegation.

The delegation model is specified by six sub-protocols as follows：

Setup： The identity provider generates system parameter and system public/private key pair.

Credential Issuing： The identity provider grants a secret credential to user u.

Pseudonym Generation： User u generates a new pseudonym in current time slot according to its secret credential and timestamp. Two pseudonyms are unlinkable and only loose time synchronization is required.

Signing-warrant: User u sign under the pseudonym a warrant that contains delegation period, delegate identity, delegated identity, and which services to be accessed, etc.

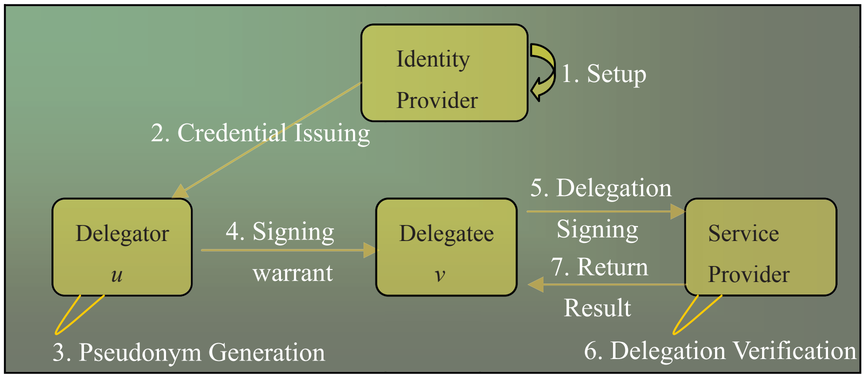

Fig. 2. Relationship in the anonymous delegation model

User v obtains a proxy key according to his private key and the signature of the warrant.

Delegation-Signing: User v generates proxy signatures on behalf of user u .

Delegation-Verification: Services providers verify proxy signatures from v and the u 's delegation together.

The relationship among the six sub-protocols is illustrated in Fig. 2. If the service provider trusts the identity provider (IdP) and a secret credential is issued to the delegator u by the IdP, u can grant delegate the delegatee v the access privilege to the service when v does not have the privilege. u uses the pseudonym generation protocol to protect its privacy and the signing-warrant protocol to grant privilege.

We adopt the concept from WS-Federation to describe how to use the delegation model in federated domains. Uesr u is also referred to a requestor who is an end user or an application. A resource means a web service or service provider. We will illustrate the delegation model by some typical scenarios in Fig. 3. Each arrow represents a possible communication path between the participants. Each dashed arrow represents that the possible communication can be executed offline between the participants. Each participant has its own policies which combine to determine the security tokens and associated claims required to communicate along a particular path. In Fig. 3a, a secret credential is issued to the requestor by the IdP in the requestor's trust realm (Domain A) if the requestor has not stored the credential to access resource C (1). The requestor self-generates identity security tokens (pseudonyms) based on its credential, and delegates its privilege with respect to the pseudonyms (i.e., sends a delegation token) to the resource/service in domain B (2). The delegation signing tokens are then proved to the IdP in domain C and an access security tokens are returned from C (3). Resource B uses the access token to access resource C. In Fig. 3b, a secret credential is issued to the requestor from the IdP in domain C if the requestor has not stored the credential to access resource C (1). The requestor self-generates pseudonyms based on its credential, and sends a delegation token to the resource/service in domain B (2). Resource B uses the delegation signing token access resource C. Unlike with the classic delegation process in WS-Federation, no IdP is involved when new identity and delegation tokens are needed if the requestor has stored the credentials, and the privacy of the requestor is protected using unlinkable pseudonyms. In the both cases, whether IdP B and IdP C trust each other does not matter.

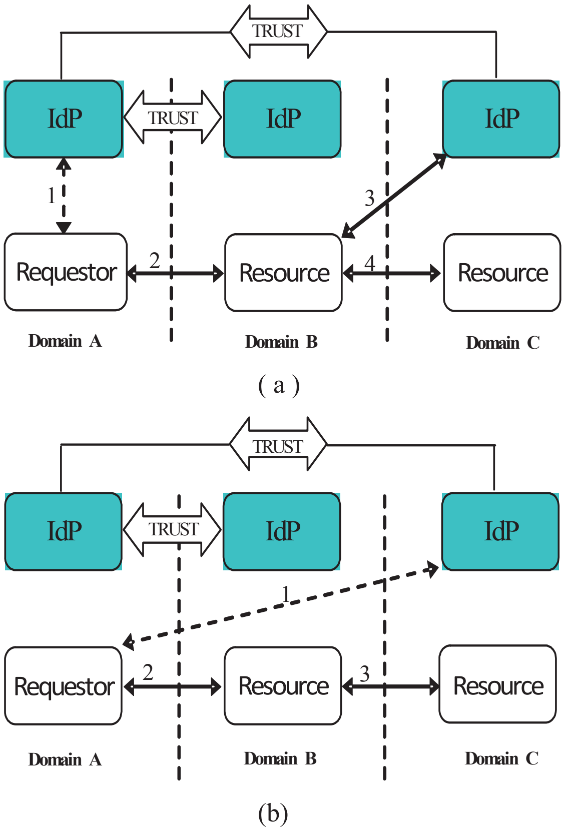

Fig. 3. Delegation scenarios: (a) the requestor IdP issues credentials; (b) target service IdP issues credentials.

B. *Personal Identity Metasystem in Working Place*

A personal identity metasystem often runs on his/her trusted device such as a mobile phone or USB device. The device can now operate as a self-issued identity provider.

The self-issued IdP component running on the trusted device is responsible for issuing security tokens when self-issued information cards are used. The identity selector can run on an untrusted terminal when a person uses a computer such as in an airport. The data transmitted between the terminal and the trusted device is not sensitive such that it is considered to be secure. The personal identity metasystem has to collaborate closely with other identity systems when a person logs in his working system in his company. The terminal computer in working place cannot be completely trusted by the personal identity metasystem because it could be attacked.

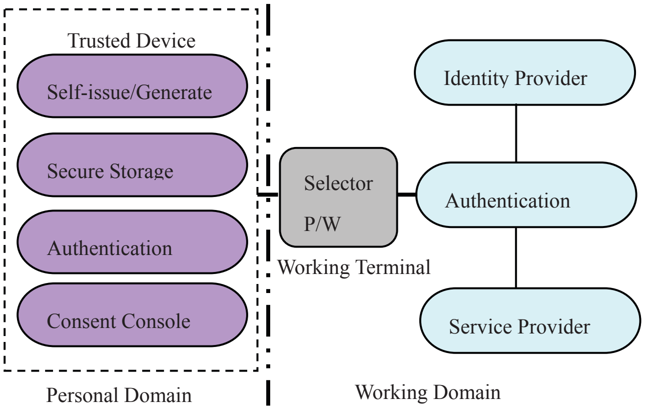

Fig. 4. Personal Identity Metasystem in Working Place

Fig.4 illustrates the close cooperation between the personal identity metasystem and local identity systems in local place. We can regard they belongs to different security domain and the two domain have a trust relationship after logging. However, they share a common identity selector, and the personal identity metasystem temporally integrates authentication services in working system. We can consider this close cooperation system as a new identity metasystem. The user uses working terminal in his local security domain and personal identity metasystem can delegate some privilege based on some secret credentials to the identity system in working place. For a user-centricity philosophy, any personal identity select from the working system should be confirmed by the person in his consent console.

C. *Universal Identity Management Model*

Our model takes credential-focused identity approach as a start point, which may be trivially set to short-term credentials. With delegation enhanced, users can re-issue security tokens based on long-term credentials stored in their personal identity metasystem. The underlying credential-focused approach can provide strong data minimization and anonymity.

In this model, it is assumed that different security domains are federated, and there exists a personal identity metasystem to aid a user to manage his identities. Fig. 5 illustrates a conceptual model focusing on a relationship among a requestor, a delegatee, a resource and a personal identity metasystem. The requestor uses his personal identity metasystem to log in his local security domain. The local security domain and delegatee security domain trust each other such that the requestor can uses short-term credential to access the delegatee based on the trust relationship of identity providers in two domains. When it wants to access the resource in the resource domain, the delegatee can be appointed to represent the requestor anonymously with certain attributes if the requestor has privilege to access the resource and the delegatee hasn't.

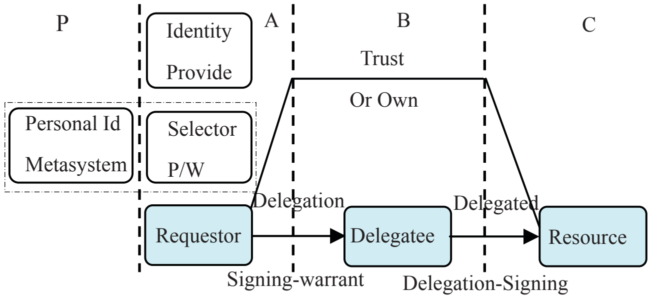

Fig. 5. Universal Identity Management Model

In SOA, a service is often composite and a delegatee may be a composite service provider. When the requestor accesses this service, the delegatee may ask him to grant the privilege to access sub-service, the resource. Fig. 6 illustrates typical runs in web services environment where the delegator accesses data from another resource on behalf of the requestor.

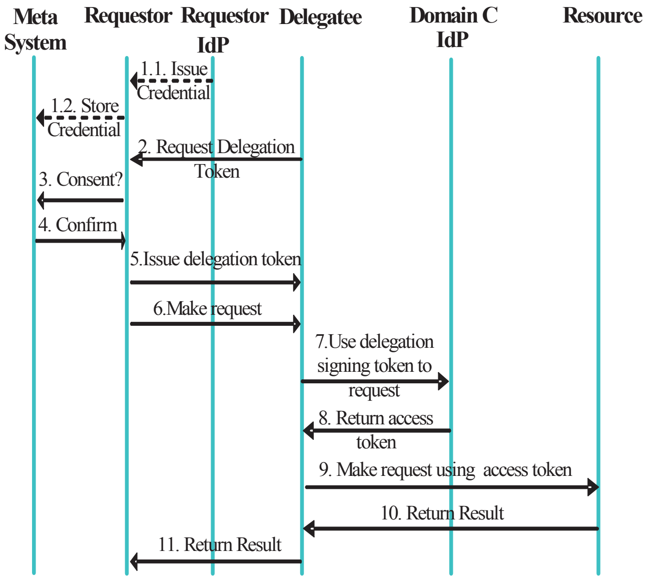

Fig. 6. Typical Run in Universal Identity Management Model

The entities in WS-Federation are enhanced as follows.

IdP – An Identity Provider is an entity that acts as an authentication service to end-requestors and as a data origin authentication service to service providers. IdPs are trusted third parties to maintain the requestor's some identity information. The original IdP is enhanced to issue secret credentials by adding ***Credential Issuing*** interface.

Requestor – An end user, an application, an agent--is typically represented by a digital identity and may have multiplevalid digital identities. The original requestor is enhanced to self-generate pseudonyms and delegate privileges by adding the issued party interface of ***Credential Issuing*** and a ***Signing-warrant*** interface.

Resource – A web service, service provider, or any valuable things. Sometimes, it can act as another requestor. The original resource is enhanced to sign messages and verify signatures by adding ***Delegation-Signing*** and ***Delegation-Verification*** interfaces. When it acts as a requestor, it delegates privileges to other resources by adding a ***Signing-warrant*** interface.

Delegatee – A resource in domain B.

The detail runs in Fig. 6 are as follows.

Step 1.1: A secret credential is issued to the requestor by the IdP in the domain A if the requestor has not stored the credential to access resource C. That is to say, the ***Credential Issuing*** sub-protocol in the solution is executed between the IdP and the requestor.

Step 1.2: The secret credential is stored the new composite identity metasystem.

Step 2: In some transaction, the delegatee may ask the requestor to grant privilege to access the resource in domain c. Therefore, the delegate requests the requestor the delegation token.

Step 3: The requestor sends the delegation request to the metasystem and asks for consent from the user.

Step 4: If the user confirms the request, the metasystem self-generates pseudonyms based on its stored credential using the ***Pseudonym Generation*** sub-protocol.

Step 5: Then, the metasystem uses the ***Signing-warrant*** sub-protocol to issue delegation token with respect to the self-generated pseudonym.

Step 6: The requestor makes a composite service request to service B.

Step 7: The delegation uses the ***Delegation-Signing*** sub-protocol to sign an access-token request to the IdP in the domain C.

Step 8: The IdP in the domain C uses the ***Delegation-Verification*** sub-protocol to verify the request. If the verification is successful, it returns an access token to the requestor.

Step 8: The delegatee makes a service request to the resource using the access token.

Step 9, 10: The resource returns the service response to the delegatee, and the delegatee returns a composite service response to the requestor.

A delegation chain means that multiple delegations occur recursively. Compared with credential chain discovery in [15], our model focuses on delegation composition for this privacy-preserving delegation chain to improve the efficiency of identity system. For a delegation chain $x_1 \to x_2 \to x_3 \to \cdots \to x_n$ where the requestor is denoted by x_1, resource A is denoted by x_2, and so on, the delegation model works as above by iterating delegation token issuance. So, we describe in detail the delegation token in the chain as follows:

$$\{\alpha, KSet\}$$

where $\alpha = \alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_n$ is the signature and $\alpha_1 \to \alpha_2 \to \alpha_3 \to \cdots \to \alpha_n$ is the signature chain for the warrant m_w which are respectively produced by $x_1 \to x_2 \to x_3 \to \cdots \to x_n$; $KSet$ is a list of pseudonyms, i.e., $KSet =$ $\{PKey_{x_1}, PKey_{x_{n-1}}, PKey = PKey_{x_1} + PKey_{x_3} + PKey_{x_4} + \cdots + PKey_{x_{n-1}}\}$, where middle pseudonyms can be hidden.

IV. A HEALTHCARE EXAMPLE

This healthcare example is from the work of [16]. Assume there is a Medical Authority that can legally certify doctors, hospitals and other public healthcare facilities. All of them do not know each other in advance for there are many participants in this ecosystem. It is useful to dynamically recognize other valid participants when sharing some resources is vital for treatment.

In this scenario, when a doctor arrives at work, his personal identity metasystem composes local identity services, provides a consistent human-computer interface, and will be called identity metasystem. The doctor has been issued a secret credential by the Medical Authority (as an identity provider) which shows the doctor is a licensed physician. Based on this credential, a new pseudonym PSD is self-generated which does not disclose other personal information other than licensed physician. The doctor is also provided an identity ID associated with a token by the Hospital's IdP. The PSD delegates his licensed physician to ID.

When the doctor is on duty, an unconscious patient, Carol, is sent to the Hospital. The doctor has some available options to do treatment after checking the status of Carol. However, Carol has some allergies threatening life, which shows some ones of the options are dangerous for Carol. There should be quick way to get this information.

A student ID card on Carol is found which indicates a link to the affiliated University Hospital's Health Record Service. The Hospital's system sends a WS-MetadataExchange request to the University Hospital's Health Record Service URL. Two available endpoints for requesting medical records are displayed, one for normal access and the other for emergency access. The doctor selects the emergency access path. Fig.7 illustrates the message sequence in this scenario.

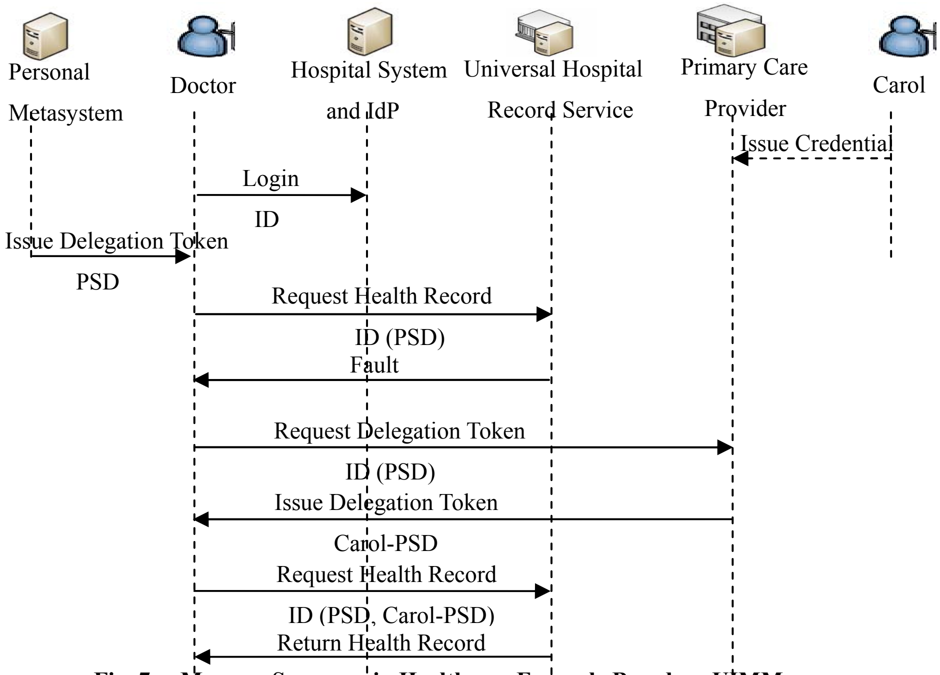

Fig. 7. Message Sequence in Healthcare Example Based-on UIMM

A token of a licensed physician is required to access the University Hospital's emergency Health Record Service endpoint. The secret credential issued by the Medical Authority and the corresponding pseudonym PSD are stored in his personal identity metasystem. In this scenario, the personal identity metasystem uses ***Signing-warrant*** to issue delegation token to ID in the hospital system based on PSD. Unfortunately, a fault is returned for the request. This fault specifies that a third token is required to release Carol's records. The specific metadata in the fault contains a reference to the Carol's Primary Care Provider (PCP).

The PCP is authorized to release her health records when Carol enrolled in the University. She authorized her PCP by issuing a secret credential to her PCP, and the release condition is that the request is sent by a licensed physician and certified by a hospital as an emergency. If it verifies that the request satisfies the condition, the PCP will self-generate a new pseudonym Carol-PSD and delegate the privilege to doctor by using ***Signing-warrant***. This allows the University Hospital's emergency Health Record Service to accept the doctor's request and release the patient records.

V. ANALYSIS

How to realize the delegation model based on anonymous credential is critical for an identity system based-on the UIMM. We can adopt two signature schemes to implement those sub-protocols in the delegation model based on anonymous credential. The first one is pseudonym-based signature scheme which provides anonymous proof of possession of credentials to protect user's privacy. Service providers verify the signature to decide whether the signer has the rights to access the services. The second one is a warrant proxy signature scheme where the original signer u delegates his signing capability to the proxy signer v without leaking his private key, and then the proxy signer creates a valid signature on behalf of the original signer. The pseudonym-based signature scheme mainly implements Credential Issuing, Pseudonym Generation and Signing-warrant, and the warrant proxy signature scheme mainly implements Delegation-Signing and Delegation-Verification.

In our prior wok [17], we proposed a pseudonym-based signature. In [18], we proposed a delegation solution to realize the delegation model based on anonymous credential. These works show that our UIMM model can be realized efficiently. Except adopting pseudonym-based signature, we can adopt pseudonym systems to realize the model [18]. Compared with exiting pseudonym systems, pseudonym-based signature scheme is more efficient to realize the model.

The identity unlinkability is accounted for by the use of the special pseudonym-based signature schemes. In addition, pseudonym-based signature schemes also allow that the user selectively releases information of the attributes in a transaction by using knowledge signature in the scheme. Conditional release is rather hard to achieve in the anonymous setting without involving the identity provider in the transaction. But in our model, it is inevitable for users to conditionally release personal information. The mechanism of verifiable encryption [19] makes it possible. Other security attributes such as confidentiality and integrity can be straightforward realized. The scheme for revocation of identity information should be considered during the design of detail systems. Our pseudonym-based signature scheme in [17] had the capacity to revoke a pseudonym.

VI. Related works

In distributed federated identity environment, there exists some leading specification such as SAML (Security Assertion Markup Language) [20], Liberty ID-FF (Identity Federation Framework) [21] and WS-Federation [4]. These specifications support privacy-preservation and have capabilities to prevent identity tracking and collusion through issuance of an opaque handle for each user. The work of [22] extended the existing framework for federated identity management to support delegation. However, these specifications do not address the issue of anonymous delegation. In this relationship-focused model, identity provider almost involves each identity provision transaction, systems are difficult to use in a long-term credential setting, and the token is often issued with a limited audience set which in turn pre-determines the use of the token.

Trust management systems often have the delegation function. For example, PolicyMaker [23], Key-Note [24] and RT [15] had explored extensively the delegation issue for public-key infrastructures (PKI). In these systems, the user can delegate some of his authority to a delegatee. If a delegation chain from the source to the requestor is found, the requestor can access the source. Therefore, a core problem in trust management is to determine whether such a chain exists, which is called credential chain discovery problem [15]. The work of [25] proposed a delegation framework for grid security, which exchanged proxy certificates based on PKI [25]. However, the privacy issue was not thoroughly addressed in the above system.

Our model is inspired by the work of [5]. That work discussed the issue of user centricity for identity management, and gave the possible mechanism to realize universal identity system. Following this direction, we give a detail model based on anonymous credentials, which can be efficiently realized. For user-centricity, our model includes the philosophy of identity metasystem to provide consistent user experience and easy-to-use.

Anonymous credentials are the key component in our model. However, there is no straightforward transformation of anonymous credential schemes without delegation into delegatable schemes. Classic anonymous credential systems were introduced by Chaum [6] in 1985, as a way of allowing the user to work effectively, but anonymously, with multiple organizations. The works of [26], [27], [28], [29] developed the model and implementation of anonymous credential systems. Camenisch and Lysyanskaya [30], [31], [32] proposed anonymous credential systems, which are more efficient than the earlier ones, by constructing a signature scheme with efficient protocols. All the above systems use interactive zero-knowledge protocols to prove the possession of credentials without optimizing the rounds of interaction. Belenkiy [33] introduced non-interactive anonymous credentials in 2007 to solve this problem. However, the scheme could not be directly transformed into a delegatable anonymous credential scheme.

Delegatable anonymous credential schemes were proposed in [7], [8] where users can obtain credentials from identity providers and delegate their credentials to other users. If an identity provider issues user A a credential for his given pseudonym Nym_A, user A can prove to user B that Nym_A has a credential from the identity provider. Credentials received directly from the identity provider are level 1 credentials, those that have been delegated once are level 2 credentials, and so on. User A can also delegate his credential to user B, and user B can then prove that he has a level 2 credential from the identity provider where user B proves to others his possession of credential without involving any identity information of A. However, the size of the possession proof increases with increase in delegation level, and cannot be bounded to a constant number by aggregating proofs. Furthermore, in those schemes, identity providers are involved in issuing credentials when a new pseudonym is generated, and those schemes are not efficient either as far as network resources are concerned. In our model, the concept of self-generated pseudonym is introduced to make efficient anonymous delegation possible.

VII. Conclusions

In this paper, an efficient delegation model based on anonymous credential is proposed where a user can prove the possession of valid credentials without interacting with identity providers, and grant delegatee to perform actions on his behalf. Beyond user-centricity, a universal identity management model is presented based on the delegation model to unify the relationship-focused and credential-ocused paradigms. For user's perspective, a roaming identity metasystem is also adopted and combined in our model to support easy-to-use, consistent experience and transparent security. Our model focuses on the privacy-preservation of users through the unlinkability of pseudonyms, data minimization and selective release of personal information. In order to easily implement, our model extends WS-Federation with enhanced credentials supporting efficient service composition. In addition, we give a healthcare example and detail analysis to show that our model can realize user-centricity beyond the old concept. Therefore, the model will provide strong building blocks for the design and implementation of user-centric identity management systems.

REFERENCE

[1] K. Cameron, Laws of identity. http://www.identityblog.com, 5/12/2005

[2] PRIME CONSORTIUM. Privacy and Identity Management for Europe (PRIME). http://www.prime-project.eu.

[3] Identity-management. Liberty alliance project. http://www.projectliberty.org.

[4] C. Kaler and A. Nadalin. WS-federation: Passive requestor profile, 2003. Available from: ftp://www6.software.ibm.com/ software/developer/library/ws-fedpass.pdf.

[5] A. Bhargav-Spantzel, J. Camenisch. User Centricity: A Taxonomy and Open Issues. In The Second ACM Workshop on Digital Identity Management - DIM 2006, pages 493-527, 2007.

[6] D. Chaum. Security without identification: transaction systems to make big brother obsolete. Communications of the ACM, 28(10), pages 1030-1044, 1985.

[7] M. Chase and A. Lysyanskaya. On signatures of knowledge. In Cynthia Dwork, editor, CRYPTO 2006, volume 4117 of LNCS, pages 78–96, 2006.

[8] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham. Delegatable Anonymous Credentials. http://eprint.iacr.org/2008/428.

[9] IBM, Microsoft, Actional, BEA, Computer Associates, Layer 7, Oblix, Open Network, Ping Identity, Reactivity, and Verisign. Web Services Trust Language (WS-Trust). February 2005.

[10] Microsoft organization. Microsoft's Vision for an Identity Metasystem. Microsoft Whitepaper, May 2005. http://msdn2.microsoft.com/en-us/library/ms996422.aspx http://zoo.cs.yale.edu/classes/cs457/tsui_digital_identity_management.doc

[11] D. Chappell. Introducing Windows CardSpace. Windows Vista Technical Articles, April 2006 http://msdn2.microsoft.com/ en-us/library/aa480189.aspx

[12] CodeIdol.com. InfoCard Architecture and Security http://codeidol.com/csharp/indigo/InfoCard/ InfoCard-Architecture-and-Security/

[13] Novell corp. Bandit project http://www.bandit-project.org/index.php/Welcome_to_Bandit

[14] L.N. Hoang, P. Laitinen, N. Asokan. Secure roaming with identity metasystem. Proceedings of the Symposium on Identity and Trust on the Internet, pp.36-47, March 2008.

[15] N.H. Li, W.H. Winsborough, J.C. Mitchell. Distributed credential chain discovery in trust management: extended abstract. In ACM Conference on Computer and Communications Security (2001), pp. 156–165, 2001.

[16] Marc Goodner, Maryann Hondo, Anthony Nadalin, Michael McIntosh, and Don Schmidt. Understanding WS-Federation. Microsoft and IBM, 2007 May.

[17] Y. Zhang. An Efficient Anonymous Authentication Protocol with Pseudonym Revocability. 2009 Fifth International Joint Conference on INC, IMS and IDC, pp. 1929-1934, 2009.

[18] Y. Zhang, J.L. Chen. A Delegation Solution for Universal Identity Management in SOA. IEEE Transaction on Services Computing, 3, 2010, 10.1109/TSC.2010.9 .

[19] J. Camenisch, V. Shoup. Practical verifiable encryption and decryption of discrete logarithms. In Advances in Cryptology-RYPTO, pp. 126-144, 2003

[20] OASIS. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005.

[21] Liberty Alliance Project. Liberty ID-FF Protocols and Schema Specification. Version 1.2, November 2003. http://www.projectliberty.org/specs.

[22] Hidehito Gomi,Makoto Hatakeyama,Shigeru Hosono,Satoru Fujita. A Delegation Framework for Federated Identity Management. Proceedings of the 2005 workshop on Digital identity management, pp. 94-103, 2005.

[23] M. Blaze, J. Feigenbaum, J. Lacy. Decentralized trust management. Tech. Rep. 96-17, 28, 1996.

[24] M. Blaze, J. Feigenbaum, A.D. Keromytis. KeyNote: Trust management for public-key infrastructures (position paper). Lecture Notes in Computer Science 1550 (1999), pp. 59–63, 1999.

[25] M. Ahsant, J. Basney, O. Mulmo. Grid Delegation Protocol. Proceedings of the Workshop on Grid Security Practice and Experience, July 2004.

[26] D. Chaum and J.H. Evertse. A secure and privacy-protecting protocol for transmitting personal information between organizations. In Advances in Cryptology-CRYPTO'86, pp. 118-167, 1986.

[27] I.B. Damgard. Payment systems and credential mechanisms with provable security against abuse by individuals. Advances in Cryptology-CRYPTO'88, pp. 328-335, 1988.

[28] L,D, Chen. Access with pseudonyms. Lecture Notes in Computer Science, 1029: pages 232-243, 1995.

[29] A. Lysyanskaya, R. Rivest, and A. Sahai. Pseudonym systems. In Selected Areas in Cryptography, 6th Annual International Workshop, SAC'99, pp. 184-199, 1999.

[30] J. Camenisch and A. Lysyanskaya. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In Birgit Pfitzmann, editor, EUROCRYPT 2001, volume 2045 of LNCS, pp. 93-118. Springer Verlag, 2001.

[31] J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. In SCN 2002, volume 2576 of LNCS, pp. 268-289, 2002.

[32] J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In CRYPTO 2004, volume 3152 of LNCS, pp. 56-72, 2004.

[33] M. Belenkiy, M. Chase, M. Kohlweiss. Non-Interactive Anonymous Credentials. Theoretical Cryptography Conference (TCC) 2008. http:// eprint.iacr.org/2007/384.