Communications and Network, **2009, 1, 74-81**
doi:10.4236/cn.2009.12012 Published Online November 2009 (http://www.scirp.org/journal/cn).

Scientific Research

A Privacy Enabled Fast Dynamic Authentication and Authorization for B3G/4G Mobility

Zhikui CHEN, Song YANG
School of Software Technology, Dalian University of Technology, Dalian, China
E-mail: *zkchen@dlut.edu.cn*
Received July 13, 2009; *accepted July* 29, 2009

Abstract

Mobile technologies make their headway by offering more flexibility to end-users and improve the productivities. Within the application of ubiquitous access and pervasive communication, security (or privacy) and QoS (Quality of Service) are two critical factors during global mobility, so how to get a smooth and fast handover based on a user privacy protected infrastructure is our focus. Based on a user-centric virtual identity defined by EU IST project Daidalos, this paper firstly proposes an effective infrastructure which protects the context-driven access policies for online services in order to avoid attacks by malicious eavesdroppers. In the proposed infrastructure, SMAL and Diameter are used to securely protect and deliver authenticated and authorized entities and XACML is used to authorize the user-level privacy policy. On the basis of it, a dynamic fast authentication and authorization handover mechanism is proposed which can save one trip communication time consummation between administrative domains.

Keywords: Privacy, Policy, Security, VID, Authentication, Authorization

1. Introduction

The Internet is today's most used tool for work and leisure. In recent years, the need for a digital identity has risen as a strong driving force behind network architecture design, service provisioning and content handling, billing and charging. Digital Identity is expected to be a powerful tool for users to access unlimited digital resources via a limited number of trusted relationships and for providers to offer these resources across different layers of communication systems, administrative domains and even legal boundaries. However, the lack of a common view on Digital Identity across these different layers has so far resulted in independently developed and thus often inconsistent identity management frameworks as well as incompatible applications. Therefore, identity is no longer a matter of who you are but also of the use you are making of a service or even a network connection. As a result, the ill-prepared architectures of today need to support users at the service level and usually tend to create situations where the privacy of the user is in danger.

However, for pervasive computing, privacy is a server problem. Servers may very well convey sensitive personal data, such as patient health care, employee records, credit card details, etc. It is critical that users have control over their identity and profile information; from what it is to how it is being protected and to who has access. E.g., e-Government heavily relies on the reuse and exchange of personal data and protecting the privacy of health information is an important issue that has gained tremendous significance with the advance of electronic health-care records. Identity management (IDM) is thereby a crucial component, e.g., to make sure that only authorized users have access to protected data resources.

Protecting the privacy of users in user-centric identity management systems is a challenging problem for service access, which can only be achieved if it gives users complete control over their identity data. However, none of the existing solutions offers this possibility. Key challenges towards the development of a more consistent approach are to tackle the conflicting requirements of privacy, identification and security for the open and distributed pervasive services [1,2].

Authentication and Authorization define the process of verifying an object's permission to perform a particular action or not. Two different classes of mechanisms exist for this: 1) Authentication-based schemes require, as a precondition, an authentication of the object, which is utilized by checking access control lists, whether this identified object is allowed to perform the requested ac-

tion. 2) Credential-based schemes apply credentials, which provide trustworthy information being held by the algorithm performing the authorization process. Authorization depends on service specific attributes e.g., service class for QoS and user-specific attributes e.g., name, age, etc [3].

Handover occurs when a mobile terminal (MT) is roaming from one domain to another domain. During the procedure of the handover, there exists a time that MT loses its connection with both the previous access router (PAR) and new access router (NAR) and data which is sent to it at this time will be lost. So it firstly needs handover fast enough to reduce the lost of the data. Secondly, handover should be secure without disclosing privacy and breaking integrity of user's data. Besides, QoS will be another factor that affects handover, as shown in Figure 1.

Based on the above mentioned scenarios and the XACML standard, this paper proposes a service authorization mechanism based on user-level privacy policies, which, at the enforcement level, defines exactly what resources are 'personal data' and exactly who is an 'authorized person'. The user-level privacy-policy management is implemented by using a user-centric IDM, based on a key concept defined in the European IST (Information Society Technology) project Daidalos [4], in terms of a virtual identity (VID) that operates across all network layers and/or federated intra or inter-domains. Besides, in order to get a fast and smooth handover, a fast and securely scenario of authentication and authorization for mobile terminal mobility among different domains is also proposed.

The rest of this paper is structured as follows. Section 2 firstly introduces two key components of a user-centric identity management system proposed in Daidalos, and then describes the proposed infrastructure in detail. A dynamic authentication and authorization handover mechanism will be proposed in Section 3. Section 4 summarizes the paper.

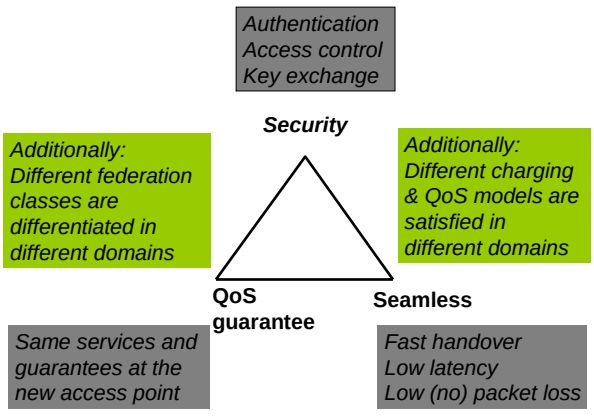

Figure 1. Handover requirement in pervasive environment.

2. Privacy-Enabled Authentication and Authorization Mechanism

2.1. Two Key Terms—VID and EPP

Before description the proposed infrastructure, two concepts firstly introduced, namely VID and EPP.

• **VID**

A concept of virtual identities and extensive investigation into their management and efficiency is made central to our approach. By efficiency of virtual identities, it is meant that a virtual identity does not disclose too much or too little information for the purposes required (e.g. service usage), that the virtual identity makes it difficult for the general public to link it to other virtual identities of the same person and that it preserves an optimum balance between its (contradictive) primary functions: pseudonymity and protecting true identity, whilst still enabling service provisioning, non-repudiation, and authentication on a reasonable scale. Virtual identities are complemented with a management cycle to support their efficiency, which should support privacy policy negotiation, access control, reputation and trust and context obfuscation.

A VID is a collection of references (e.g. URIs) to actual Entity Part Profiles (EPPs-see next subsection) stored at different places. A VID may include a variable number of references and, as such, it fulfils the Entity Profile View (EPV) function. Whilst defining a VID, the Identity Manager also declares access control policies and thus consequently defines a filtered EPV (FEPV) according to the user's request for the service, which will use the VID. A VID is equipped with a pseudonymous identifier for which it is not possible to resolve the true identity of the VID holder. The pseudonymous identifier is not a human-like name (although such a pseudonym could be included in the VID as an EPP) but is a machine identifier (a number) used as a primary key for records on the VID data in A4C (Authentication, Authorization, Accounting, Auditing and Charging) administrative domain. The pseudonym is commonly referred to as the VID Identifier (or VIDID). A VID serves several functions: authentication, authorization, accounting (e.g. non-repudiation), pseudonymization, and data minimization (according to the data minimization principle or proportionality principle). This way, all the entities in the construction of an administrative domain serves the same VID of one legal entity, which is liable for this administrative domain. Further details are described in the literature [1,2,5].

• **EPP**

We are inclined to think of private identification data as being highly distributed; there are some practical reasons

and arguments for this: the data have always been held internally by data controllers (operators, small and large providers, state departments and other authorities have always been collecting and storing data on people) as well as privately by the very data subject. Moreover, it is unclear who takes ownership of this identification data: the usual state of affairs is that the data subject is not generally the owner of the data as the data subject (a legal or natural person) can never for example sell a particular piece of personal data held by a data controller; even more so, the regulations about this are not very distinct. According to this, we first model a notion of smallest (semantically) consistent part of personal data for a (legal) entity called the Entity Profile Part (EPP). A particular EPP is a subset of all the personal data specifying a certain fact about the (legal) entity such that this fact is still entirely (semantically) captured or described inside this subset but it is the smallest such subset for this fact. E.g., a first name and a surname of a person are together the smallest consistent part of data capturing the full name of the person If we take only the first name or the surname, it is no longer clear which person this is. Thus, the first name plus surname is an example of an EPP. An abstract union of all the EPPs is called an Entity Profile (EP). An EPV should be defined and controlled by the data subject and in this way the *principle of user consent* is enforced. Then, for any EPV, the actual access to the data is potentially subject to access control mechanisms for access to EPPs so that the actual perception an observer gets on the EPV is filtered by the access control on EPPs and this is then called a Filtered EPV (FEPV). A notification principle and a principle of right to object processing of personal data are followed by the data subject having the power to define the access control on EPPs-to define FEPVs.

2.2. Architecture Components

Figure 2 illustrates the components of the proposed authentication and authorization system, in which the Key Deployment Centre (KDC) is responsible for issuing keys and the PANA Client (PaC), is used to bootstrap the VID and EPPs which will be explained in the following. The Policy Manager manages various context-driven policies including adding, modifying and deleting a policy to a specific EPP. The Context Manager controls various contexts of an EPP with a specific VID including adding, timely updating and deleting. The EPP Manager manages all EPPs including querying, adding, deleting and modifying data in a specific VID. The ID Manager manages VIDs including creating, deleting and retrieving from the VID wallet [5]. All of these functionalities interact with the ID Broker. The ID Broker is a key component in the proposed scheme. In fact, the ID Broker controls the user's VID and services including the privacy policy. Next, we will explain the concepts about the VID and EPP.

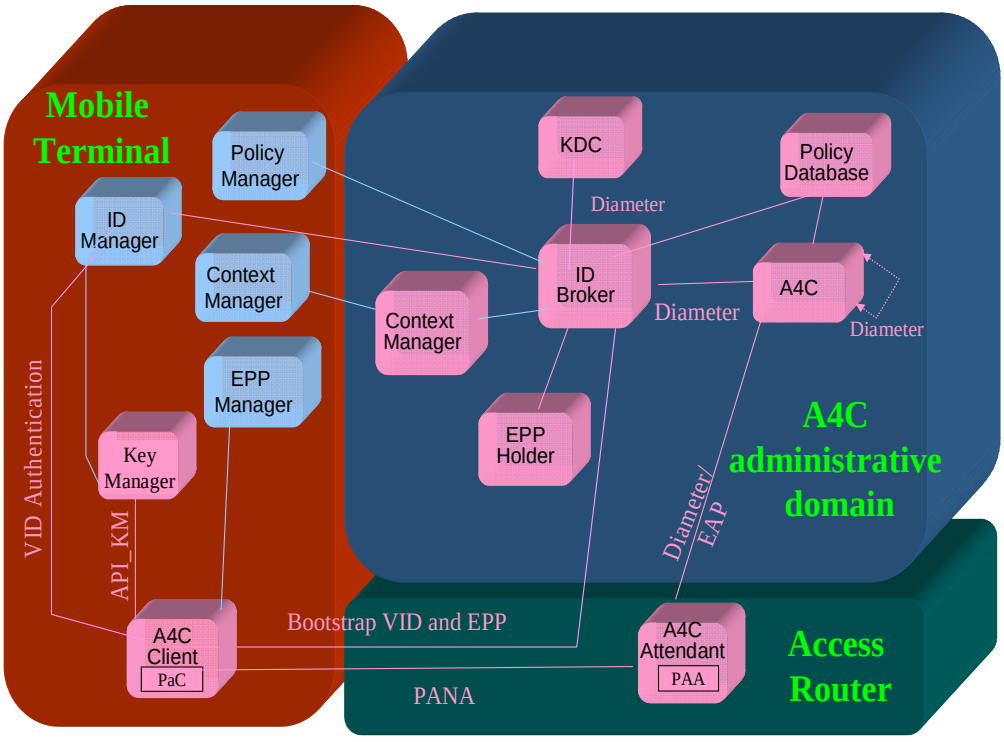

Figure 2. Authentication and authorization system policy.

In this paper, we mainly focus on context-aware service authorization. VID authentication and authorization are described in [1,5]. In the proposed service authorization scheme, XACML is used to control access and authorize services, which are built around the logical separation of application-specific PEP from a PDP—see next subsection. A service is a group of filtered EPPs, e.g., a video conversation service may include the following EPPs: user preference EPP, context EPP, credit card EPP, video EPP and audio EPP including their QoS levels etc. Those EPPs have different policies, even one EPP has different policies for different users or different callers/callees, e.g., my family could locate me to within 1m, my employer only to within 10km, and Playboy knows that I am over 18 rather than my date of birth. Depending on the type of authorisation, different credentials are submitted by the terminal client. In order to verify these authorisations, the service provider is going to contact the A4C server to implement an XACML decision. In its request, it provides the VID and an artifact of the client and his Service ID (SID) or EPP identifier. In the same request, it may also ask for a number of user credentials which are then checked by the A4C server. After receiving the response from the A4C authority, the Service Provider (SP) may decide to store each received authorisation assertion associated with the revealed VID in order to avoid re-sending an authorisation request at the next session. Of course, this behaviour is only useful in the case of credentials which are not subject to frequent changes (e.g. legal age verifications).

Figure 3 demonstrates the general service authorization process between a mobile terminal, a user home domain, a service provider and an XACML decision when a user wants to use a service. Furthermore, authorization for network access as well as for 3rd party services is just special cases of the general service authorization. These interactions are detailed in the following subsections.

Access-control in an open, distributed independent environment must enable a customer's secure service consumption across federated domains. The proposed ID-token approach in [5] builds on SAML, which greatly facilitates the secure access, by providing independence from specific authentication mechanisms and the seamless usage of services without being actively confronted with an authentication mechanism, enabling a smooth, practical and enjoyable inter-domain consumption of services.

The process flow is described as follows: the ID-token is included within the service request from the Mobile Terminal (MT) to the SP, where it can be extracted. The SP sends this token to the responsible A4C. The A4C decrypts the token, verifies the signatures and maps the ID-token to the corresponding authentication assertion, which has been created during initial authentication. This assertion is used for checking user's authentication session status. Then, a profile-specific attribute and authorization assertion, which is related to the VID, is created and sent to the SP. When the user is not accessing an SP in its home domain, the same procedure applies from the MT's point of view. However, the foreign A4C cannot access the ID-token, and thus is unable to verify it. It must then request the A4C from the user's home domain for the verification of the ID-token and the generation of the VID-specific authorization assertion.

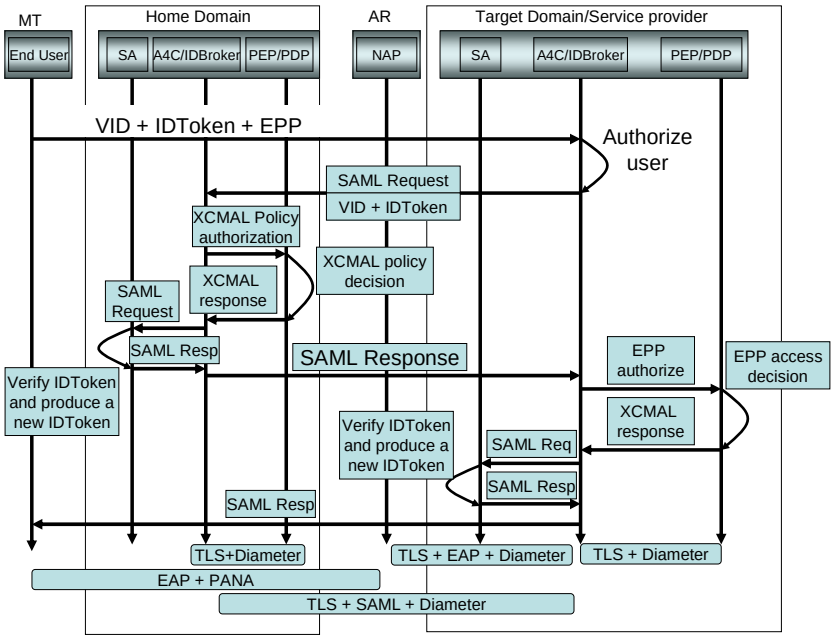

Figure 3. General authorization process.

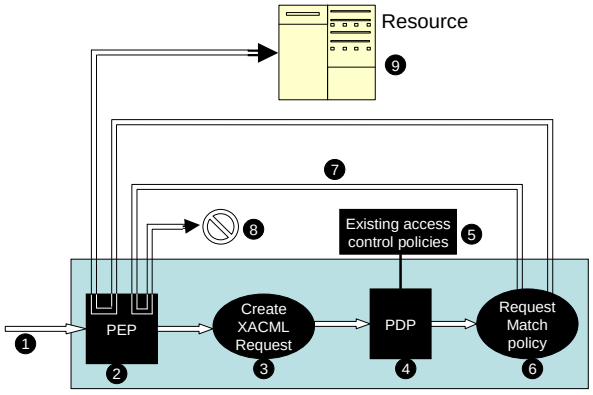

Figure 4. XACML authorization.

The ID-token has information on which A4C to contact through normal AAA routing. Federation will be based on A4C's interconnection and trust establishment.

2.3. General Service Authorization Using XACML

Figure 4 demonstrates the process using XACML to authorize a service based on a privacy policy, which consists of the following steps: 1) a user attempts to access a specific network resource (e.g. a file system, database or web service). 2) The query is passed to the entity protecting the resource-the PEP. The PEP is defined as a system entity that performs access control by making decision requests and enforcing authorization decisions. PEPs come in many forms. E.g., PEP may be part of a remote access gateway, part of a Web server or part of an email user agent. 3) The PEP uses the XACML request language to create a request based on the user, the action and the resource. 4) The PEP sends this request to a PDP. A PDP is an entity that accepts XACML access requests and evaluates them against one or more policies to produce an access decision. 5) The PDP retrieves applicable policies from a policy store. A policy store is also called a Policy Administration Point (PAP). A PAP is the system entity that creates a policy or policy set (a collection of policies). 6) The PDP compares the request against policies retrieved in step 5, and determines whether access should be granted or denied. 7) The answer (i.e. decision) is sent back to the PEP. The Decision is usually either 'Permit' or 'Deny'. 8) If the answer is 'Deny', the PEP is denying the user access to the resource. 9) If the answer is 'Permit', the user is granted access to the resource.

For authorizing a specific user to a requested value-added service, the Policy Enforcement Point of the service can request authorization decisions from the Authority. The Asserting Authority issues the authorization decision based on the policies and profiles it holds connected to the binding of the VID and the Service Identifier.

If a service has to be personalized for the user, it may require some attributes and profiles. The authority can collect the required attributes from the profile associated with the VID and issue them via an attribute assertion.

2.4. SAML-Based Security Issues

The SAML authority in conjunction with the identity management system plays an important role for maintaining users' privacy. The RegID (registered user identity) is always kept within the identity manager and the SAML authority and is never revealed to unauthorized entities. The SAML authority generates, after successful VID authentication at the authentication service, an authentication assertion, which is mapped to the relevant RegID. This guarantees that the authentication assertion is mapped to all VIDs related to the RegID. The artefact is sent back to the MT. The MT can request its valid VIDs directly from the SAML authority, which are then included in an attribute assertion. If a certain application needs specific parameters, they can be obtained from the SAML authority.

For service authorization, the ID-token is sent to the 3rd party service provider (3PSP). The 3PSP can request service authorization from the SAML authority providing the Identity Token for requesting an assertion based on the profile of the current VID. For verifying the authentication status, the Identity Token is mapped to the authentication assertion related to the RegID. Then, the SAML authority can dynamically generate a new authentication, attribute and authorization decision assertion based on the current valid policies and attributes and the current VID presented within the token. Thus, the authorization is very dynamic, representing current policies and attributes. The RegID authentication assertion is never revealed, because a new assertion based on the VID is dynamically generated.

2.5. Privacy-Enabled Policy

In a context-aware pervasive communications environment, privacy plays a central role. A common approach is to allow users to act under multiple virtual identities. Thus, it is possible to reveal only the amount of information to a service, which is really necessary for a specific service provision. However, the user can use many services, without leaving a too detailed data trace when linking all the information that is known at those services.

The policy management concepts are generally in line with the terms and definitions defined in [6].

Role—A role represents a functional characteristic or capability of a service to which policies are applied.

Policy—A policy is essentially a rule, which consists of a name, a condition that is dependent on one or more events and zero or more actions.

Policy Decision Point (PDP)-Is the component responsible for deciding on actions to take given one or more events from the event management. It must decide which policy receives priority, when multiple policies match the input events and inform the Policy Enforcement Point of the actions to take.

Policy Enforcement Point (PEP)—This component enforces the actions prescribed by the policies in the PDP.

Configuration policies [7] —Are policies which can be used to specify the configuration and installation of applications and services.

Obligation policies [8] —Are policies that are used to ensure requirements are met and expected conditions are not violated. These are also called action policies [9].

Management policies [7] —Are policies which can be used to manage the policies or the policy management system itself. E. g., such policies could specify prioritization rules for choosing between applicable policies.

From a policy framework viewpoint, the configuration and policy management block implements the PEP and provides a partial implementation of a PDP. As such, at key points in service execution, events are generated towards the PDP via event management. The PDP evaluates the available policies and informs the enforcement point of the actions to take. These enforcement actions are part of the policy description.

The policy management aspects are implemented using XACML in the back-end core networks (in the A4C server, as described in the next section) and include the provisioning of policies, static conflict detection and resolution. These functions are however provided by other components in the service provisioning platform.

We distinguish between two strategies for protecting privacy: restrictive privacy protection, where most of the EPPs about the data subject are not known publicly, or weaker protection performed by approaches of anonymity and pseudonymity while generally allowing disclosure of EPPs. The former is clearly not possible if it is in the interest of the data subject to make use of services: some EPPs should be disclosed for this purpose. We have also seen in the previous paragraph that the majority of the personal data is already publically known. The privacy protection that we can enforce is to make it difficult for an outsider observer to identify which (legal) entity is performing the actions with the EPPs involved in (electronic) transactions: this can be accomplished by careful selection of EPPs which will be used in particular (electronic) transactions so that as little inference about the real identity of the (legal) entity performing the transactions is possible. To capture this idea inside the data model we introduce another notion: if we take a subset of EPPs from the whole EP, then we get a view on the EP and we call this the Entity Profile View-see above section.

VIDs will be selected according to these instructions, access control rights and credentials will be put in place to satisfy or empower particular statements of privacy policy and complement the selected VID to obtain an FEPV and context filtering will source the relevant information, using a privacy policy, in order to achieve adequate obfuscation.

In other words, context-driven user-level privacy policy is bound to a concrete EPP with a specific VID.

3. A Dynamic Fast Authentication and Authorization Handover Mechanism

In the Daidalos project, device mobility is impacted by the Virtual Identity concept, as mentioned above. Following the VID framework specifications, mobility should be regarded not anymore as a pure device mobility issue, rather as a mean of providing mobility to identities for a network access session. In this sense VID-specific network access sessions become mobile. This would be called the traditional host mobility when it is related to changing network access on one interface. Using the VID concept, the proposed fast handover scheme at access router is based on RFC4068, which proposed fast handover for Mobile IPv6 [10]. RFC describes the protocol operations for a mobile node by which to maintain connectivity to the Internet, during its handover from one access router to another. These operations involve movement detection, IP address configuration, and location update, as shown in Figure 4.

The introduced fast dynamic authentication and authorization scenario is implemented after the handover decision is made. When the handover decision is made by mobile terminal (namely terminal initiated handover) or access network (namely network initiated handover) according to the received signal strength, for example, the mobile terminal or old access router provides some

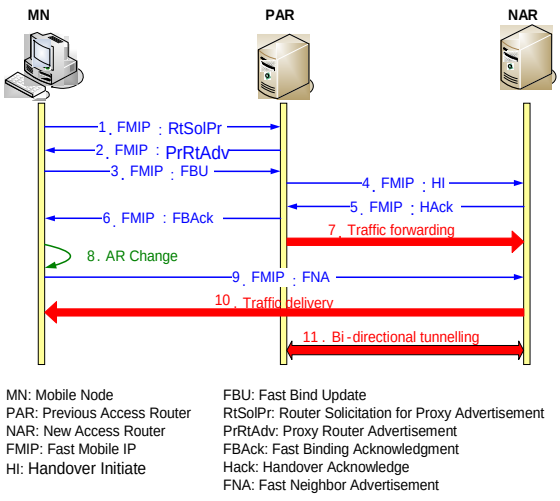

Figure 5. Fast handover for mobile IPv6.

credentials, which will be transferred to the new inter-domain access router using handover context transfer protocol-RFC4067 [11]. The new AR delivers them to the new inter-domain A4C server, which forwards them to the home A4C server using Diameter protocol-RFC3588 [12]. The home A4C checks them, and sends the result back to the new inter-domain A4C and then to the attendant (mobile terminal or access router). Based on single sign on (SSO) and SAML protocol, if all credentials are successfully verified, the service will continue; otherwise the service will be denied and re-authentication and re-authorization are needed. But this process may cause some latency due to signaling communication between different inter-domains. This single thread handoff process will consume much time. Figure 5 shows this authentication and authorization process.

To reduce the signaling transport latency, we propose a multiple-threads approach to signaling transport scenario, using SSO and SAML technology. During a conversation, a mobile node or the user's authenticated and authorized data is stored in the user's home domain, such as QoS agreement and VID credential. During handover this scenario uses the federation concept [12], in which handover between two foreign domains are federated. When a handoff decision is made, one thread transfers context information from the old access router to the new access router. Another thread is in current foreign domain which asks VID credential (ID Token) from user's home domain to the new foreign domain. Finally, the third thread contacts the QoS broker to verify the QoS level under federation class. The process is illustrated in Figure 6, where QoS signaling is not described in the figure. The details of this approach are described below.

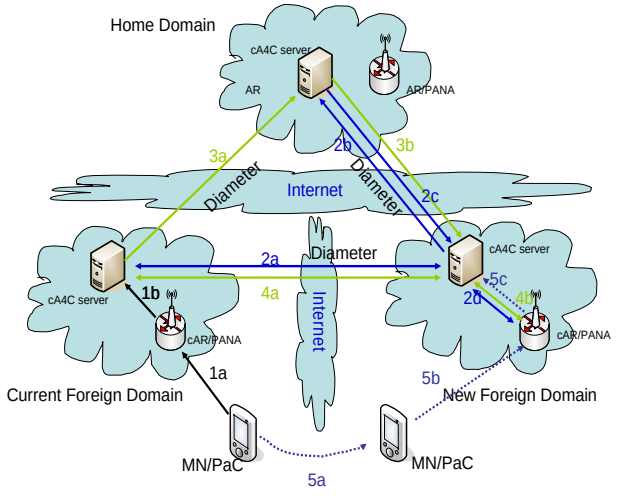

Figure 6. A dynamic authentication and authorization handover mechanism.

The basic idea is as follows: when L2 triggers handover and new foreign domain is found, the old AR will send a message to Home domain via current foreign A4C domain in order to request the VID information with a timestamp. This information will be sent to the new foreign domain (this process depends on federation classes). Then the VID credential will be verified locally in order to reduce the handover latency. When handover failed within a given time, which is specified in timestamp, the VID credential will be automatically destroyed. If handover is successful, the VID credential will be destroyed immediately. The terminal VID information will be transferred to the new domain using CXTP. For example, you are a subscriber of DT (Deutsch TeleKom), such a handover between different domains could be faster than that using the current method when you are in USA or Asia. The transferred VID information of MN (Mobile Node) will be delivered from the new foreign domain to Home domain for verification. During this process, such a long distance routing may consume many milliseconds.

It is obvious in Figure 6 that a handover has four communications among different domains. Using the traditional method, the path should be 2a-2b-2c-2a (here we only consider the communications among A4C servers). The proposed scheme, however, has only three communications among different domains, because communication 3a and first 4a are parallel. This can save one trip communication time.

The proposed mobility scheme considers the splitting of the architecture in local and global domains - each one associated to administrative domains. Global domains are typically identified with the home operator domain, retaining most of the information related to users' profiles. Implementations of such global domains should provide global reach ability by means of protocols such as Mobile IPv6 or HIP (Host Identity Protocol). Obviously, the proposed multiple-threads method is much suitable for global mobility.

4. Conclusions

As users of mobile networks have increased in number, the management of mobility and QoS are the two key factors that affect mobility. In order to protect the privacy of the users, by using the VID framework, in which a user or RegID has several avatars, the proposed infrastructure permits a user to control which information is linked to which avatar and can thus create distinct virtual identities to access the network and its services. Handover is a key factor of Qos of the mobility, to achieve a fast and smooth handover, the paper proposes a dynamic fast authentication handover mechanism which can save one trip round time compared with the traditional handover mechanism. The simulation of it on NS2 is our future work.

5. Acknowledgements

The work presented in this paper was partially funded by the EU project IST-2004-026943 'Daidalos II' [1]. Partial contents of the paper based on Daidalos research results.

6. References

[1] R. L. Aguiar, J. Jaehnert, A. F. Gomez Skarmeta, and C. Hauser, "Identity management in federated telecommunications systems," Proceedings of the Workshop on Standards for Privacy in User-Centric Identity Management, Zurich, 2006.

[2] B. Weyl, P. Brandao, A. F. Gomez Skarmeta, R. M. Lopez, P. Mishra, C. Hauser, and H. Ziemek, "Protecting privacy of identities in federated operator environments," IST-14th Wireless Mobile Summit, 2005.

[3] Z. Chen, "Federated dynamic authentication and authorization in Daidalos," Proceedings of IEEE NTMS, May 2007.

[4] European FP6 IST project Daidalos, http://www.ist-daidalos.org.

[5] Z. Chen, "A scenario for identity management in Daidalos," Proceedings of IEEE CNSR, May 2007.

[6] Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, and S. Waldbusser, "Terminology for policy-based management," RFC 3198.

[7] R. M. Bahat, M. A. Bauer, E. M. Vieira, and O. K. Baek, "Using policies to drive autonomic management," In Proceedings of the 2006 international Symposium on World of Wireless, Mobile and Multimedia Networks, International Workshop on Wireless Mobile Multimedia. IEEE Computer Society, Washington D.C., pp. 475–479, June 2006.

[8] E. Lupu, M. Sloman, N. Dulay, and N. Damianou, "Ponder: Realising enterprise viewpoint concepts," Fourth International Enterprise Distributed Object Computing Conference (EDOC'00), 2000.

[9] J. O. Kephart and W. E. Walsh, "An artificial intelligence perspective on autonomic computing policies," Fifth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'04), 2004.

[10] R. Koodli, Ed., Fast Handovers for Mobile IPv6, July 2005.

[11] J. Loughney, Ed., Context Transfer Protocol (CXTP), RFC4067, July 2005.

[12] P. Calhoun, etc., Diameter Base Protocol, RFC3588, September 2003.

