Secure Billing for Ubiquitous Service Delivery

Les Green[1], Linas Maknavicius[2]

[1] University of Technology, Sydney, Faculty of IT
P.O. Box 123, Broadway, NSW, 2007, Australia
lesgreen@it.uts.edu.au
[2] Alcatel Research & Innovation
Route de Nozay, 91460 Marcoussis, France
linas.Maknavicius@alcatel.fr

Abstract. This work presents a secure interaction framework for establishing ad-hoc billing paths between untrusted players in a global telecommunications network. User authentication is supported through the introduction of a Billing provider, responsible for identifying users and acting as a proxy financial entity to visited service providers. Authentication, Integrity, Validity and non-repudiation issues are addressed, along with the processes involved.
Keywords: Security, Billing, Ubiquity, Authentication

1 Introduction

The current trend in service delivery is a movement towards wireless networks. This is largely due to two factors.

First, consumers desire the convenience of mobile connectivity. Freedom from the confines of wires is sought and consumers are prepared to pay a reasonable price for that luxury. That price may be a lower quality, higher risk of disconnection or simply higher monetary cost [1]. If these factors can be maintained, a user's Quality of Experience may be vastly improved.

Second, providers seek to minimise the large capital and operational expense in construction and maintenance of a wired local loop. This is especially evident in countries with insufficient existing fixed infrastructure. For example, Latin America is the largest current broadband wireless market in relation to population with significant pre-WiMAX deployment [2].

Recently, there has been increased effort towards ubiquity in wireless services, converging heterogeneous networks in respect to technologies and administration[3][4]. Within ubiquitous service availability, an end user is free to roam within the constraints of any possible network connectivity. Consequently, application services utilised by end users may be delivered via numerous network service domains. The owner of each domain involved in a service delivery at any point in time will want to be reimbursed for the services it has provided. A method of billing for the provision of these ubiquitous services is sought.

Within current generation networks, research has suggested [5] that the cost of providing and maintaining a mobile network billing system may be anything up to 50% of the total infrastructure investment and annual turnover. Seamless, automated

billing which can provide added value to the service delivery chain is therefore a large concern for current and new generation network operators.

1.1 The User Perspective

Users desire simplicity and predictability [6]. In terms of billing, an end user will not want to pay individually each domain which has provided (a fraction of) a network service. This opens the way for billing aggregators and speculators. Billing aggregators package provided services into one bill whilst speculators speculate on future costs and so quote a fee for some future period. Say the next six months. Speculation offers a method to manage risk and gain in an economic system.

A player may be both an aggregator and a speculator, with end users appointing such a player, following referred to as a Billing Provider, to manage billing on their behalf.

With the global increase of wireless connectivity via a multitude of available access technologies, both in the licensed and unlicensed spectrum, it is not feasible for a billing provider to have pre-existing agreements with every possible network access provider around the world into which an end user could roam. Ubiquitous service availability may require user connectivity from a domain with which a user and associated billing provider is unfamiliar. We are left with issue of establishing a secure billing path for services in an ad-hoc capacity amongst untrusted players.

2 A Secure Billing System

A method is proposed whereby an end user, or nominated user agent is responsible for negotiating service contracts autonomously, and is supported by a means to verify its identity as a basis for trust in an unknown network. Services are automatically billed to users via ad-hoc billing paths.

If automated billing is to be adopted, especially involving unknown players, participants should feel secure in their use of the system. This holistic view of security can be decomposed into two components.

- Trust in the system.
- Trust in the other players

2.1 System Security

Trust in the system can be established by ensuring known security concerns have been adequately addressed. There are three widely accepted components to information security. Confidentiality, Integrity and Availability.

Confidentiality has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access”[7]. Essentially, confidentiality is concerned with keeping information *private*, accessible only by correctly *authenticated identities* with appropriate *authorisation*.

ISO17799[7], an internationally recognised generic information security standard describes integrity as “safeguarding the accuracy and completeness of information and processing methods”. Information integrity describes the consistency of data. It

is concerned with ensuring the data has not been altered or corrupted either intentionally or accidentally. A step beyond information integrity is validity. Data which is valid is correct for its intended purpose. This may involve semantic checking or a logical proof of reason.

The accuracy and completeness of processing methods aims at ensuring a system is used correctly. A system with ill defined processes may be vulnerable to compromise through external hacking or improper use from authorised entities. A recent area of concern is the hacking technique of Social Engineering or "scam" attacks. Such attacks are difficult to control as they often occur outside the bounds of the system designed. A billing system should address information and process integrity and may go further to ensure information is valid in its intended context.

Finally, a definition of availability is given as "ensuring that authorized users have access to information and associated assets when required."[7] A system should be built to adequately handle any foreseeable load and be designed as to prevent attacks which may cause denial of service to authorised users. Positively securing availability is difficult in today's massively connected world. Methods such as access frequency limits and distributed load balancing are a step towards securing availability.

A fourth component of security often included is the aspect of accountability. Accountability involves non-repudiable actions and traceability. For an action to be non-repudiable, the performer cannot deny having performed that action. The aspect of traceability is an issue of specific implementations and is not considered a concern of the communication system.

2.2 Trust Between Players

Trust is concerned with the maintenance of expectation. Establishing trust in another player involves verifying their identity and ascertaining their probability of satisfying or exceeding expectation. Correct identification ensures a player with which you believe you are interacting is in fact that player. Given the correct identification of players, an attempt to model their trust can be made.

The probability of a player performing to expectation may be determined largely from their reputation, built from the outcome of one or more past interactions between players. REGRET[8], a reputational model for trust, approaches reputation from three dimensions. Individual, Social and Ontological.

The Individual dimension models the direct interaction between two players. When the same two players have repeat interactions, private trust models may be built about opponents.

In situations where once off interactions between players are common, Social reputation becomes important as players may have no previous private history on an opponent. In this situation, membership to a group may give lead to opponent reputability, or a collaborative reputation model may be consulted, built from the outcomes of multiple individual interactions.

As an alternative to a single reputability score, the Ontological dimension of reputation divides reputability into separate aspects, each applicable to a domain of concern. Multiple aspects of reputation may be combined by a player to form a view of another.

The secure billing model discussed does not attempt to model or handle reputation, but does deal with the identification aspect of trust. Players within the system are securely identified, but no assumptions are made on players regarding their discovery of the reputation of others.

2.3 System Aims

The main aim of the system is to enable ubiquitous, secure, ad-hoc billing for mobile networks. The goal of this paper is to outline the interaction processes involved in the system, and its secure approach. The way in which players implement the functionality is not important here, providing they adhere to the interaction specification.

In order to provide ubiquity and ad-hoc capability, the billing processes are designed to enable autonomous authorisation for resources controlled by each player. I.e. each player has ultimate responsibility for its own resources. For a user, this is its payment funds, for a service provider, it is the services provided, and for a billing provider, it is its reputation and the provided proxy financial responsibility on behalf of a user.

Following from the security concepts discussed above, the security goals for the system are as follows:

- Ensure positive identification of players involved.
- Enable the transmission of sensitive data, ensuring the secrecy of such information is respected when required.
- Ensure the integrity of information during transmission.
- Enable provable checking of message validity when required.
- Ensure messages are non-repudiable.
- Provide complete and well defined processes, considering possible attacks on the system.

Sections V, VI and VII discuss the security features of the billing system, addressing the above aspects of security.

Before specifying the interaction framework, we begin with a discussion of the players and their roles in the system.

3 Players in the System

There are three entities involved in the billing system discussed. Each entity is represented in the system by an electronic agent and is responsible for its own resources

3.1 End User

End users are the end points of the “billed” telecommunications zone. They are represented by User Agents, residing on a network access device. The end user (or user agent) may have access to one or more physical or administrative network domains simultaneously, and may use billable services provided by these networks once an appropriate billing path has been established.

3.2 Network Service Provider

Network Service Providers control access to one or more services delivered over a telecommunications network. Resources supporting the service may or may not be owned by the service provider. They may be a service retailer, reselling services over a network managed by a different entity, or may themselves manage a network and provide services at varying levels of the OSI stack, from raw IP access, to a managed video conference service for example.

3.3 Billing Provider

Every customer has an associated Billing Provider whose status as a trusted and reliable player is generally known. The billing provider acts as a financial proxy for its customers to visited service providers.

In a global roaming environment, involving varying laws and regulations applicable to users and providers, a Billing Provider is a common ground through which a standard billing relationship can be established. Given a larger buying power than a single end user, the billing provider may negotiate for bulk rates from service providers. A billing provider may be a user's home network service provider or a third party billing provider.

The Billing Provider is responsible for authenticating the user agent to foreign networks as required. It provides the billing service through which network service users and providers can quickly, dynamically and securely establish a billing path. The following activities are the responsibility of the Billing Provider in the delivery of the billing service:

- Bill Aggregation and Speculation – Combine charges accumulated by users for services delivered by visited providers and package them into one bill for a customer.
- User Authentication – Provide a trusted, secure identification mechanism to support roaming users.
- Provider Remuneration – Establish financial paths for remuneration of providers for services delivered to the billing provider's customers. This includes negotiation of customer pricing as required.

4 Processes Involved

Borrowing from Internet Single Sign On (SSO) technologies[9][10], the following security model is proposed, based on asymmetric encryption[11][12] and the Public Key Infrastructure[13].

It is well known that security is only as strong as the weakest link. The Public Key Infrastructure has risks associated [14], however a widely accepted aim of security is to make the effort involved in breaking the security larger than the reward. All risk can not be eliminated and PKI is the current leading approach to many aspects of security.

4.1 User Authorisation and Authentication

User Authorisation is the process that occurs between a user agent and the service provider to allow the user to request services from the provider. A natural requirement a provider may have on authorising a user is that the user agent is first authenticated. I.e. Its identity is verified by a trusted party. Refer to Figure 1 for a numbered diagram corresponding to the below points.

1. The user generates a public and private key pair and registers the public key with the Billing Provider. This step happens once and may be performed manually by the user via a web interface on the billing provider's website or by another offline means. The Billing Provider must be sure that the public key it has registered for a user belongs to the appropriate customer.
   The system relies on the user's private key remaining known only to the user. If this secrecy is breached, the user must generate a new key pair and register the new public key with the billing provider, revoking the previous public key. User public keys remain valid throughout a specific time period. All entities in the negotiation environment should therefore have synchronised clocks within a broad tolerance to ensure correct authentication. This requirement is easily satisfiable using the existing and widely used network time protocol [15].
2. When a user agent wants authorisation to request services from a provider, it creates a User Authorisation Request (Figure 2) comprised of its billing provider details and customer identifier and sends it to the service provider.
3. At this point, the Authorisation request may be rejected by the service provider for any reason, such as a banned billing provider or maybe because the service provider is simply too busy.
4. The service provider then builds a User Authentication Request (Figure 3) from the original signed User Authorisation Request, including a request for the Billing Provider's Identity Credentials (Digital Certificate) if the identity of the billing provider is not known in advance. The Authentication Request is then sent to the billing provider.
5. The billing provider checks the User Authentication Request by validating the signature on the enclosed User Authorisation Message against the stored public key on the customer record.

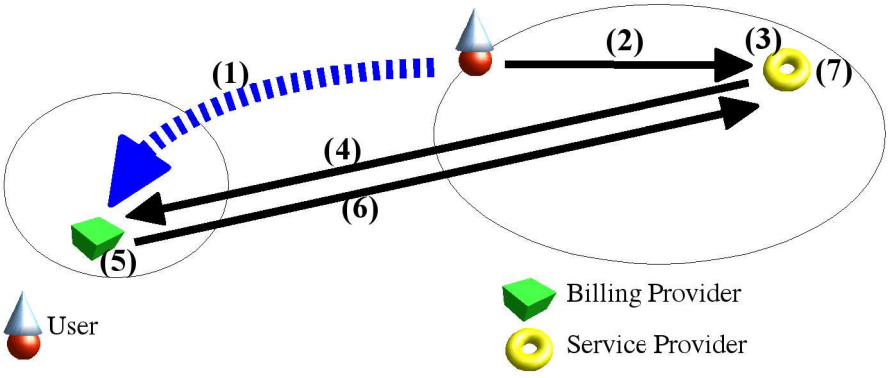

Figure 1: User Authentication

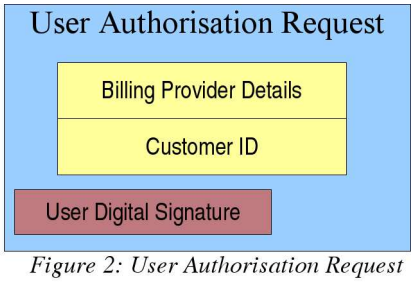

Figure 2: User Authorisation Request

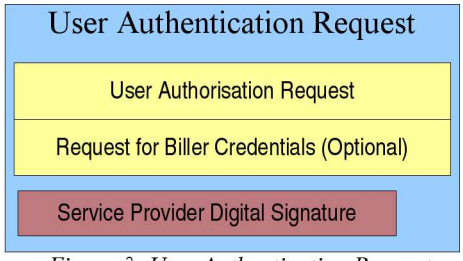

Figure 3: User Authentication Request

6. If user authentication is successful, the Billing Provider returns a Success Message (Figure 4) bundled with the user's public key and a Service Provider Billing Authorisation which authorises the Service Provider to issue bills for the supplied public key. This billing authorisation may include constraints on the provision of services or accumulation of costs by the user, or it may be an open authorisation to bill as required. The Billing Provider's credentials are also supplied if initially requested, to certify the billing provider's identity.
   The billing provider must, for each customer, maintain a list of Service Providers which have been authorised as billers for the particular customer's public key. This is to ensure that if for some reason the customer's purchasing rights are revoked, or the secrecy of the private key associated with the public key has been breached, the Billing Provider can contact each Service Provider to revoke the public key.
   The Billing Provider must receive proof from each Service Provider it has registered as an authorised biller that it has acknowledged the revocation of the public key. One appropriate means of non-repudiation is through the use of digitally signed messages in concert with valid Digital Certificates. A Billing Provider cannot claim it did not have a particular service provider registered as a recipient of a key because the User Authorisation Success Message provides a digitally signed proof that a service provider was given authorisation to send the billing provider bills signed by a particular public key.
7. Upon receiving a success message, the service provider validates the billing provider's credentials. The returned user's public key is then used to validate the signature from the initial User Authorisation Request received from the User Agent. On successfully passing authorisation, a trusted path for future services is established, and the user can proceed to request services from the provider.
   Users' public keys are stored by service providers for use in validating future Service Level Agreement (SLA) requests. In this way, the service provider need not validate with the billing provider for each SLA provisioned.

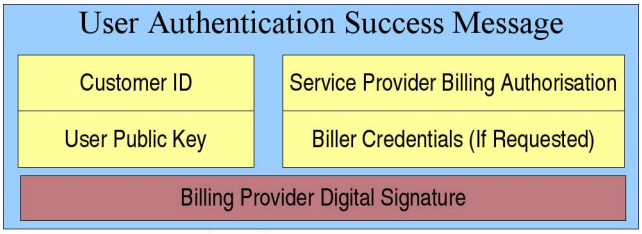

Figure 4: Authentication Success Message

4.2 Billing Path Establishment

Creation of secure, ad hoc billing paths from End Users to Service Providers involves establishing two billing relationships. A billing relationship must be forged between an end user and their billing provider. Such relationships are common in today's telecommunication environment between Internet subscribers and their ISPs. This customer facing relationship is tied in heavily with marketing strategies and individual business models chosen by the billing provider and is not explored further in this work. It is assumed a method of billing exists between end users and billing providers. However, the way in which a billing provider is charged from service providers for services used by an end user is the interesting research point and is addressed here.

The Service Provider to Billing Provider relationship process allows Network Service Providers, visited by a roaming user to form ad-hoc billing relationships with unknown Billing Providers associated with those roaming users. To establish a solid financial relationship, billing providers and service providers should be certain of each others identity and must agree on other billing details such as invoicing frequency and payment method employed. Discounting specifics and other pricing related details may also be included in a billing method.

Payment methods adopted may be be a bank routing and account number, credit card number or any other of the numerous payment systems available. Payments are not addressed further in this work. It is sufficient to say that at Biller/Service Provider negotiation time, the payment method to be used should be defined. ISO 20022[1], IFX[2] and Rosettanet[3] all offer tools to mark up payment information.

To remain a generic, open and extensible system, specifics of the final billing method between service provider and billing provider should not be limited to a single implementation. Ultimately the billing method should be based on individual provider requirements. A common process for establishing or "bootstrapping" the billing process must be defined so a suitable billing method for use can be agreed on ad-hoc.

The Bootstrap Mechanism. The mechanism used to establish a billing method between the service provider and billing provider is based on the fulfillment of individual requirements. Both players in a potential billing relationship may have different requirements of the final billing method specification. The following process ensures all requirements are fulfilled so an appropriate billing method can be found.

Based on ontological knowledge representation, the mechanism occurs in three stages:

1. Initially, each party informs the other of a list of OWL[16] ontologies which it can understand, and in which the billing method may be specified.
2. In the second stage, the service provider informs the billing provider of the information it requires to bill for services. These requirements are expressed using ontological concepts exchanged in the previous step.
   Using these requirements, the billing provider then constructs a billing method template including components satisfying the informational requirements of the service provider, and components satisfying its own requirements of a

1 http://www.iso20022.org/
2 http://www.ifxforum.org/
3 http://www.rosettanet.org/payment

billing method. The billing method template may only be composed of ontological elements common to both sets of ontologies specified in step 1.

3. The third stage in establishing a billing method is forming an agreement on the concrete values to be used in the billing method. Such values may include pricing specifics or bill frequency, etc. This stage follows an offer / counter offer / final offer argumentation strategy at which point either the negotiation succeeds and the outcome is a concrete billing method instance, or the negotiation fails and the service provider may not provide services to the billing provider's customers. A Service Negotiation Protocol (SrNP)[17] has been proposed by the TEQUILA[18] and MESCAL[19] projects and is well suited to this argumentation component.

A billing provider may also be a network service provider – and hence at some point may act as a Service Provider to the foreign Service Provider's home customers. Both parties have something to gain by establishing an optimal billing agreement.

At initial Biller/Service Provider relationship establishment, for instance when a customer of a Billing Provider wanders into a unknown Service Provider's zone and wishes to use its services, the Service Provider and Billing Provider have a requirement to establish ***some sort*** of agreement ***before*** the user can use the services. This may be relatively urgent. The Service Provider may have a "base" pricing scheme which is used when it has accumulated little or no information on the Billing Provider or User and therefore has no indicator of trustworthiness of the player. The Billing Provider is left in a take-it-or-leave-it situation with the service provider until a stronger relationship can be formed.

In contrast, *adjustments* to the billing method formed between a service provider and billing provider are infrequent, may have no strict time requirements for convergence, and presumably happen over high speed network links. A more complex and optimal negotiation strategy can therefore be employed.

5 Secure Communication

Security has been discussed in terms of Authenticated Identification, Reputation, Authorisation, and secure, non-repudiable processes. Billing for ubiquitous services involves communication between concerned players. To address all aspects of security, this communication between players should also be secure. Issues such as message integrity, privacy and accountability should be addressed.

5.1 Communication Mechanism

Secure billing is part of a greater project exploring service ubiquity through electronic negotiation, titled "Managing Quality of experience Delivery In New generation telecommunication networks with E-negotiation" (QDINE). A primary goal of the project is the development of a secure, comprehensive, open service negotiation framework built on intelligent agents. The agents use economic principals to enable ubiquitous, mobile service provisioning. Services are described within Service Level Agreements (SLA).

There are three agents involved in the billing system. The User Agent, Network Service Provider Agent and Billing Provider Agent. Agents communicate using FIPA Agent Communication Language (FIPA-ACL)[20]. ACL messages may be sent via numerous methods. These message transports may be standardised or implementation specific. Some existing message transports are RPC and IIOP.

Message exchanges are grouped into interaction protocols, with agents adopting only the protocols necessary for their personal tasks. Content within the ACL messages is expressed in the Web Ontology Language (OWL)[16].

OWL ontologies have been created for use in specifying Service Level Agreements, describing interaction protocols between agents and formalising the content of ACL messages.

5.2 Message Privacy

Messages passed between agents in the system may travel through untrusted networks. Payment details or other sensitive information may require privacy within participating agents. Public Key Encryption is used to secure sensitive messages from unintended recipients.

Encryption may occur at the socket layer via SSL or TLS. Additionally, the content of ACL messages may be encrypted. Encryption at the network layer through IPSec, although possible, is not likely as the interactions between agents are brief and asynchronous.

A security add-on for ACL called X-security has been developed [21] allowing encryption of ACL message content. Additionally, as the content language used in the QDINE project is based on XML, the standard XML encryption [22] methods may be used.

5.3 Accountability

Service Level Agreements are an electronic contract for a service. To ensure these contracts and the associated bills are not disputable, the automated interactions should be traceable and positively identify the sender.

As part of the QDINE framework, Billing Providers and Service Providers should have a commonly accepted form of identification. Valid digital certificates from trusted certification authorities are widely used for this purpose. Additionally, as outlined above in *User Authentication and Authorisation* section, the billing provider is responsible for guaranteeing a user's identity.

All agents in the framework have a private and public encryption key. Messages sent between agents in the framework must be signed with the sender's private key. In this way, every message sent can be provably attributed to a particular private key and hence, one entity.

5.4 Integrity

Ensuring the integrity of a message involves proving the message has not been tampered with after being sent. A common method of achieving this is by building a secure digest of a message and signing it with the sender's private key. In doing so,

the above requirement of Accountability is also addressed.

A secure digest is unique to the message used to build the digest. If the message is altered in any way, a different digest will be built on application of the digest algorithm. To generate a secure digest, WHIRLPOOL[23][24], or one of the SHA-2[25][24] family of algorithms may be used. To date, these algorithms remain uncompromised and are recommended for standardised secure signing of data.

The X-Security add-on for ACL may be used to attach signature and digest information to an ACL message, alternatively, or additionally, content of the messages may employ the XML digital signature framework [26].

6 Conclusion and Future Work

This work has explored the need for a secure, comprehensive and open billing solution for ubiquitous service delivery over mobile networks. Aspects of security are explored and the aims of the billing framework are presented in respect to these security aspects. The billing framework is introduced with a discussion of the players involved, along with their roles.

The framework is described in terms of the the interaction processes involved, presenting a method to establish secure, ad-hoc billing paths from provider to end user. Within the system, players maintain autonomous responsibility for their own resources.

Identification, transmission privacy and data integrity, along with non-repudiation issues are addressed through the use of different components of the public key infrastructure. The use of OWL messages enables automated validity checking. Additionally, the system is highly available due its distributed nature. I.e. All players are responsible for their own resources and the authentication management is distributed amongst unlimited billing providers.

The introduction of a Billing Provider and associated processes to promote security, handle ad-hoc relationship management and encapsulate speculation within the financial system is an innovative component with respect to current state of the art.

An interesting component of the work is the inclusion of an ontological approach to secure communication and the properties of such an approach.

To date, a framework has been designed for SLA negotiations[27]. Future work will see the implementation of this secure, ubiquitous billing work as an integration into the SLA negotiation framework. The billing component will be analysed for security weaknesses in a formal process.

Acknowledgments

This research is performed as part of an Australian Research Council Linkage Grant, LP0560935 between Alcatel and the University of Technology, Sydney. It extends work already performed on the Negotiation of Service Level Agreements for New Generation Networks, performed as part of the Alcatel Research Partnership Program (ARPP).

References

1. Jafarkhani, H., 2005, *Space-Time Coding: Theory and Practice*, Cambridge Uni. Press
2. Gabriel, C., 2005, *A Global View of Pre-WiMAX Deployment*, from: Wimax Trends: The Net's Leading Resource for WiMAX Technology & Solutions, *source:* http://www.wimaxtrends.com/articles/excerpt/e101005a.htm, *accessed:* 03-03-2006
3. The FON project: WiFi Everywhere, *Source:* http://en.fon.com/, *Accessed: 03-03-2006*
4. Computer Business Review Online, 2006, *T-Mobile first to bridge 3G, EDGE, GPRS, and WiFi*, March 13, *source: http://www.cbronline.com/article_news.asp?guid=C0AB6620-5C75-49A9-95B9-0F30F14C3884, accessed: 04-04-2006*
5. Cushnie, J., Hutchinson, D., Oliver, H., 2000, *Evolution of Charging and Billing Models for GSM and Future Mobile Internet Services*, QofIS '00: Proceedings of the First COST 263 International Workshop on Quality of Future Internet Services, London, UK
6. Nielsen, J., 2000, *Designing Web Usability: The Practice of Simplicity*, New Riders Publishing, Indianapolis
7. *ISO/IEC 17799:2005, Code of practice for information security management*
8. Sabater, J.,Sierra, C., 2001, *REGRET : a reputation model for gregarious societies*, Fourth Workshop on Deception, Fraud and Trust in Agent Societies, New York
9. Josephson, W. K., Sirer, E. G., Schneider, F. B., 2004, *Peer-to-Peer Authentication With a Distributed Single Sign-On Service*, Third Intl. Workshop IPTPS, San Diego, CA
10. The Java Open Single Sign-On Project, *Source:* http://www.josso.org, *Accsed:* 03-03-06
11. Hellman, M. E., 2002, *An overview of public key cryptography*, IEEE Communications Magazine, *vol.* 40, *num.* 5, *pp.* 42 – 49
12. Kaliski, B., 1993, *A Survey of Encryption Standards*, IEEE Micro, *vol.* 13, *num.* 6, *pp.* 74-81
13. The Public-Key Infrastructure Charter, *Source:* http://www.ietf.org/html.charters/pkix-charter.html, *Accessed:* 03-03-2006
14. Ellison, C., Schneier, B., 2000, *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure*, Computer Security Journal, *vol.* 16, *num.* 1, *pp.* 1-7
15. Mills, D. L., 1992, RFC 1305 - Network Time Protocol (Version 3)
16. OWL Web Ontology Language, *Source:* http://www.w3.org/TR/2004/REC-owl-guide-20040210/, *Accessed:* 26 Nov 2004
17. *MESCAL Deliverable 1.2, Source: http://www.mescal.org/deliverables/MESCAL-D12-public-final.pdf*
18. *TEQUILA - Traffic Engineering for Quality of Service in the Internet, at Large Scale, Source:* http://www.ist-tequila.org, *Accessed:* 02-02-2006
19. *MESCAL - Management of End-to-end Quality of Service Across the Internet at Large, Source:* http://www.mescal.org, *Accessed:* 02-02-2006
20. FIPA ACL Message Structure Specification, *Source:* http://www.fipa.org/specs/fi-pa00061/, *Accessed:* 02-02-2006
21. X-Security - Communication Security in Multi-Agent Systems, *Source:* http://agents.felk.cvut.cz/security, *Accessed:* 02-03-2006
22. XML Encryption, *Source:* http://www.w3.org/TR/xmlenc-core/, *Accessed:* 02-03-2006
23. Barreto, P. S. L. M., Rijmen, V., 2000, *The WHIRLPOOL Hashing Function*, First open NESSIE Workshop, Leuven
24. ISO/IEC 10118-3:2004, *Part 3: Dedicated hash-functions*
25. C S R C - Cryptographic Toolkit: Secure Hashing, *Source:* http://csrc.nist.gov/Crypto-Toolkit/tkhash.html, *Accessed: 03-03-2006*
26. XML Digital Signatures, *Source:* http://www.w3.org/TR/xmldsig-core/, *Accessed:* 02-03-2006
27. Green, L., 2004, *Auto Negotiation of Service Levels for NGNs - T2D2 - System Architecture*, University of Technology, Sydney