A domain model approach to network security

H. Wang, A. Prasad, P. Schoo
DoCoMo Communications Laboratories Europe GmbH
Landsberger Str. 308-312, Munich, 80687, Germany
{wang|prasad|schoo@docomolab-euro.com}

S. Tessier, O. Tirla
T-Systems Nova Innovationsgesellschaft mbH, Berkom
Goslarer Ufer 35. Berlin, 10589, Germany
{serge.tessier|octavian.tirla}@t-systems.com

***Abstract*— As result of combining heterogeneous network technologies, network architectures become increasingly complex. Administrative domains, representing functional or non-functional responsibilities and obligations, and their relationships in terms of reference points are used to find appropriate abstractions and thus managing the complexity. In this paper domain models, as organization of environments of autonomous administrative control and reference points, are suggested and applied as a method to develop a threat analysis and find suitable security mechanisms.**

I. Introduction

The technical approach of IST project MIND (Mobile IP based Network Developments) [1] provides a vision of what shows a path towards 4G. The work is based on results of the IST project BRAIN (Broadband Radio Access for IP based Networks) [2]. The project takes as a starting point the concept of an IP core, accessed by a variety of technologies and searches for extensions of IP-based radio access networks to include ad-hoc and wireless elements both within and attached to the fixed infrastructure. The BRAIN project carried out conceptual work concerning the BRAIN QoS Framework and the Brain ENd Terminal Architecture (BRENTA). The design of selected parts of BRENTA is currently under study within the MIND project. There is a need for an architecture, where system level properties, resources, application level semantics and user preferences can be observed and managed so as to best decide when and how adaptation has to be performed. Figure 1 shows the evolutionary approach taken by BRAIN and MIND projects towards 4G. BRAIN extended the current telecommunication network and the Internet to address micro-mobility and QoS [2]. MIND provides a further evolution to allow mobile networks [3] and Personal Area Networks (PAN) leveraging the public infrastructure to gain access to the Internet, to long distance calls facilities, and to services, but foremost to security support.

In this architecture security needs to be considered. Here security is not only an issue from the user's perspective, where users do expect confidentiality and integrity maintained by the applications and in the communications. Security is also important from the network operators' point of view, as they have to fulfil contracts – contracts signed with their customer or among each other. This adds further security requirements on the operation of such heterogeneous network technologies. In this setting the domain model helps to find essential security and accounting mechanisms that lower vulnerabilities at reference points, on interactions between domains. This is the part of the job enforcing interoperability while leaving domain internal security considerations to the party administering and operating a domain.

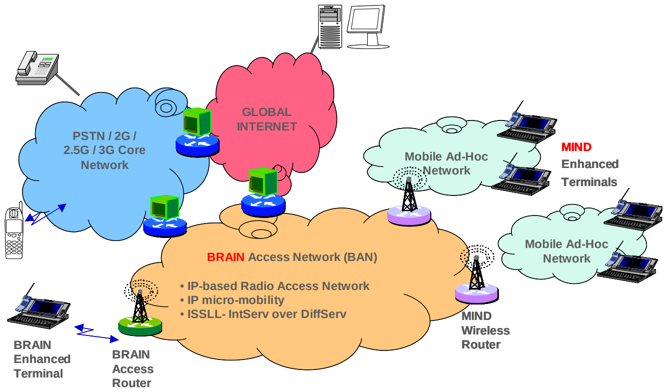


Figure 1: Simplified BRAIN/MIND architecture

This paper is structured as follows: Section II presents the MIND scenario based on which a domain model (Section III) and protocol stacks at reference points (Section IV) are derived. A threat analysis is given in Section V prior to the discussion on security mechanisms (Section VI) and accounting issues (Section VII). The paper is concluded in section VIII.

II. Scenario

MIND project follows a top-down approach by using scenarios to identify requirements on the network and terminal architectures and security mechanism. "Nomadic worker scenario" is one of the three scenarios used in MIND, which takes place simultaneously on a train, in an airport and at a company, with the actors related and connected to each other by wireless communication networks. A part of this scenario is used here and referred to as "Train scenario".

Stephanie Jones is on the train. She will organize an in-train meeting with colleagues from other companies. Her Personal Wireless Assistant (PWA) informs her that the train service provider is running a wireless communication network (e.g. HiperLAN/2), which is also connected to the Internet. Stephanie logs into the train network by entering her secure pre-paid account number and sets up a videoconference to the project leader. Her service provider charges her for all used services. The service provider is obliged to pay specified percentages of the charged fees to the holder of the train network (extended network provider), network provider, application service provider and content provider, respectively. The network provider and the extended network provider have a contract of the network connectivity between them.

When the other colleagues gradually join Stephanie in the train, they attach their mobile terminals to hers to setup a secure wireless ad-hoc network using the temporary session key sent by her earlier. Some colleagues connect their terminals to her terminal in order to access the train network and the Internet because they do only feature short range radio technology (e.g. Bluetooth). In this case, Stephanie is charged for the usage of the Internet access she is offering for her partners. By the time they arrive at their destination they suspend the meeting.

This scenario demands innovative technologies. The involved network domains for nomadic worker scenario are displayed in Figure 2.

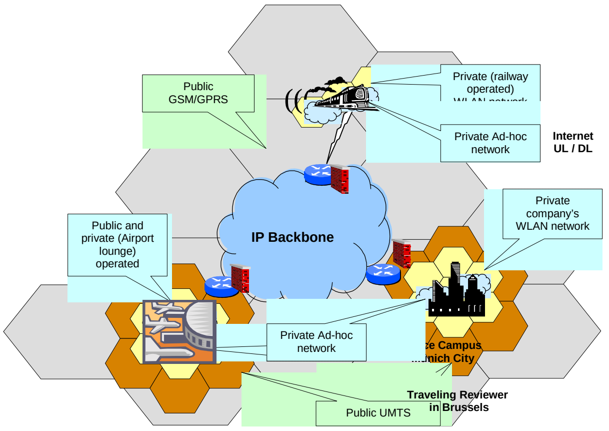

Public GSM/GPRS
Private (railway operated) WLAN network
Private Ad-hoc network
Internet UL / DL
IP Backbone
Private company's WLAN network
Public and private (Airport lounge) operated
Private Ad-hoc network
ce Campus nich City
Traveling Reviewer in Brussels
Public UMTS

Figure 2: Involved Network Domains in the Nomadic Worker Scenario

III. Domain model for the "Train scenario"

A domain model identifies different administrative domains and their respective responsibilities, the reference points, which describe trust, relationships and interaction interfaces between them. Technical realizations of domains encompassing functionalities and restrictions on network components are also described in domain model. Therefore, domain model is very important when analyzing security threats and to prove proposed security and accounting mechanisms. Administrative domains, representing functional or non-functional responsibilities and obligations, and their relationships in terms of reference points have been used to define domain models. To present network architecture on a high level, they abstract from technical realizations, restrictions on network components and even domain internal details. Such abstractions allow

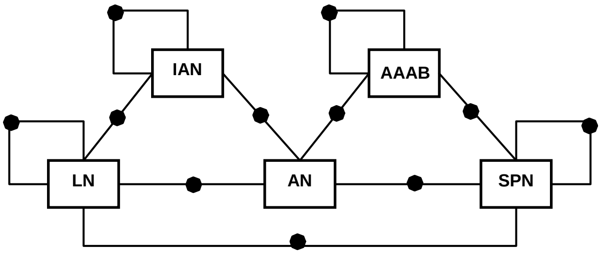
- to describe various network configurations of routers as they can be formed, without listing example configurations;
- to identify the administrative autonomy of domain owners and their obligation towards the environment they are interacting with (including off-line aspects like, for example, subscriptions)
- to identify the trust that needs to be achieved in flexible network configurations amongst administrative domains, which is crucial when proposing security and accounting mechanisms;

Now roles of participants involved in the scenario are identified and mapped onto the administrative domains. Users can consume various services. Subscribers have contract with and pay bills to their Service Provider. The latter sells prepaid account to or has contract with Subscriber and facilitates corresponding Users to connect to the wireless access network. Auxiliary Network Provider offer mobile terminal featuring routing functionality and providing access to other Users. Extended Network Providers operate hot-spot wireless networks. Network Providers (NPs) operate cellular/backbone networks to connect hot-spot networks to the Internet. Value Added Service Providers (VASPs) may be Application Service Providers or Content Service Providers.

Figure 3 depicts the resulting domain model of MIND in which:

- Leaf Network (LN), is the domain administrated by User
- Intermediary Access Network (IAN), is the Auxiliary Network Provider domain, which may be administrated by User
- Access Network (AN), is the Extended Network Provider domain
- Service Provider Network (SPN), is the Service Provider domain
- Authentication Authorization and Accounting Broker (AAAB), is introduced from security and accounting points of view, which acts as an enabler of AAA functionality between AN and SPN

Not being involved in the trust relationship that is specific to the mobile wireless network, other roles, like NP and VASP, are excluded for simplicity. A reference point (RP) between two domains is the interface to interact with each other. It includes the activities and relationships (e.g. service providing, cash flow) from business model point of view, which may be described in a contract. A RP includes possible protocol interfaces.



AN: Access Network
SPN: Service Provider Network
IAN: Intermediary Access Network

LN: Leaf Network
AAAB: AAA Broker

Figure 3: Domain model for the "Train scenario"

A. LN

A LN is an autonomous constellation of Mobile Nodes (MNs) which are supposed to communicate together under given circumstances related to the nature of the formation and perpetuation of the LN via layer two forwarding protocols, layer three (Internet or special MANET) routing protocols or a combination of both. A LN may be a PAN, in which all mobile equipments belong to one user. It also can be a closed ad-hoc network which comprises mobile terminals belonging to different users. However, the essential idea of LN is: at any time there's only one MN of LN being connected to AN and only one subscription contract being used by the MN for the connection. In the simplest case, a LN contains a single MN and only one subscription contract is used. The case of several users sharing one subscription is covered, however – the relationships between the users are handled within the LN and are not visible externally.

B. IAN

Intermediary Access Network (IAN) domain is actually a 'subscriber owned equipment' providing routing and access service to the MNs (LNs), which can't directly access to AN for whatever reasons, or other IANs. IAN provides routing and access services after going through the authentication and authorization process performed by its SPN and AN, especially it should be permitted by AN to provide the services to others. A strong trust relationship between IAN and AN is required. In case that the routing functionality provided by an IAN is part of a MN owned by a user, who also uses the MN to make use of the service provided by AN (or other IANs) for her/his own benefits (acting as a LN), the MN (including its owner) is then regarded as a combination of two domains: a LN and an IAN domain.

C. AN

The Access Network domain consists of access points, access routers (ARs), gateway routers to other networks ("the Internet"), and local AAA servers (AAALs), as well as a routing infrastructure to link them all together and network management infrastructure to manage it.

D. SPN

The Service Provider Network domain is the location of user subscription information, which is used in authentication, authorization and further processing of accounting information related to individual users. Logically, it consists of home AAA servers (AAAHs) and associated customer care equipment and not much else.

E. AAAB

AAA Broker (AAAB) is an intermediary agent, trusted by a group of AAA servers which belong to ANs or SPNs. It can obtain and provide security services from those AAA servers. It's an enabler of AAA functionality between AN and SPN.

F. LN to AN Reference Point

A LN attaches to an AN by going through an authentication procedure which sets up the relationship between the AN and the LN with help of SPN. One LN could attach to more than one AN ('multihoming'), but these relationships are independent. On the other hand side, an AN can simultaneously support relations to zero, one or more LNs who have been authenticated and authorized. Accounting information of the access service usage of LNs are generated by AN and sent to SPNs. An AN relies on the authorization allowance of the SPN in its decision to open for a requesting LN.

G. LN to SPN Reference Point

A LN has a subscription relationship with a single SPN and pays as agreed in the subscription contract its SPN for service, based on accounting information generated by the AN to which it is attached.

H. LN to IAN and IAN to IAN Reference Point

IAN provides access and routing services to LNs and other IANs. LNs and IANs may use the routing service provided by other IANs that are permitted by the same AN in case that they can't connect to AN directly. On the other hand, they (LNs and IANs) don't use the services provided by untrusted IANs and IANs don't provide routing services to untrusted LNs or IANs. The trust relationships amongst IANs and between LN and IAN are rather elaborate in their settings in comparison with those between IAN/LN and AN. One LN can connect to one or many IANs. One IAN can connect to one or many IANs and LNs. The routing algorithm decides how the packets can be transmitted in the ad-hoc networks. The AAA architectural components presence (e.g. attendant) here is still an open issue

IV. PROTOCOL TABLE

In this section the MIND network layer protocol stacks at each RP are briefly discussed. The idea is to perform threat analysis to find the weaknesses of the protocol and give security mechanisms to counter the threats. The protocol stacks can be divided in two categories (Figure 4): control plane (CP) protocols and user plane (UP) protocols. The former are those used for signalling, session management etc. while the latter are used for actual data transmission.

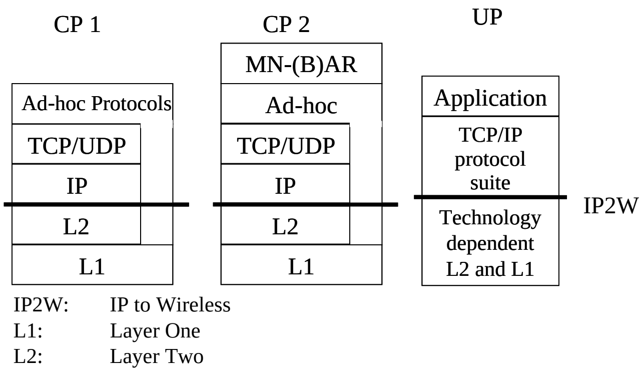


Figure 4 Control plane and user plane protocol stacks

Control plane protocol stacks can either be ad hoc protocols, which can lie at any point in protocol stack from above Layer-1 onwards or MN-(B)AR (Mobile Node – BRAIN Access Router) which lies over ad hoc protocols. User plane protocol stack is considered to be same for all RPs. By TCP/IP protocol suite in user plane we mean any protocol defined by IETF (Internet Engineering Task Force) that can be used for data transmission. In Figure 5 the protocol stack at different reference points are given.

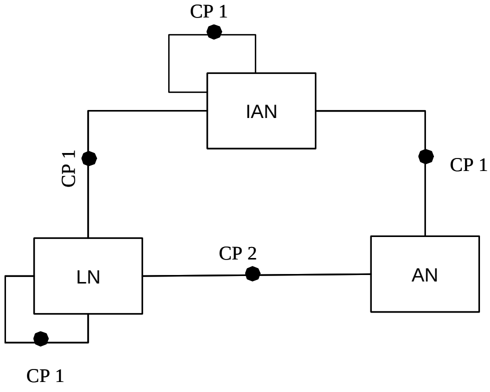


Figure 5 Control plane protocol stacks at various reference points

V. Threat analysis

Based on the domain model covering a MIND usage scenario threats are identified, which are understood as (potential) danger to one of the assets of a scenario participant - *who* threats *what* by *which means*. A new role is introduced: Intruder (I), who performs attacks without having any of the former identified roles. Assets can be categorized as data/information, cost, usage of service, infrastructure resource and reputation. General threats include: denial of service, eavesdropping, masquerading, replay, modification of information, reroute, network flooding, repudiation, unauthorized access, theft of service, disclosure of information, time falsification, sabotage (stolen resources e.g. PWA) and traffic analysis. With this background, Table 1 demonstrates a part of the threat analysis for LN and lists corresponding generic counter measuring security services.

VI. Security mechanisms

After the description of mobile networking environment situation and the potential menace, we propose here some counter measures realisation as mentioned in Table 1. Due to consistence need, we provide the reader only with referenced security guidelines. Note that, for the same reason, these security guidelines are snapshots extracted from the whole MIND security pictures.

As the Internet moves towards a picture where mobility is predominant, we can identify two opposite approaches adopted by engineers and protocol developers: either they choose to adopt (or re-shape) existing standard Internet Protocol, more or less trying to save the original end-to-end paradigm, or they create an entirely set of standards applicable only to the wireless world (and, more generally, only to a specific architecture). In-between solutions are seldom. We use this taxonomy through the three following sections and conclude about pertinence regarding applicability to MIND.

A. *The Internet Approach*

The so-called Internet approach is best represented by the IETF. But also within this forum, various approaches (merely incarnated by working groups) could be selected for the purpose of securing all or only some segments of the mobile computing framework, according either to threats or reference points. Here we present a non-exhaustive listing of existing solutions with highly variable maturity:

- Mobile IP and IPSec (RFC3220) (RFC1825), [4], [5], [6]
- Mobile Router Support with Mobile IP [8]
- Global Connectivity for IPv4 Mobile Ad hoc Networks [9]
- Extensible Authentication Protocol over IP (EAPoIP) [7]
- SSL (RFC2246) [10]

Those standards are widely adopted and are justified by the success of IP. Though, they are not well suited for such a heterogeneous world where the end-to-end paradigm is barely applicable (even if the MIND playground restricts as much as possible the introduction of so-called “walled-garden”). Somehow, we believe that the highly unpredictable nature of the MIND environment as well as the atomisation of trust distribution induced by the rich MIND domain model (not to mention the inherent limitation of the mobile computing environment like e.g. battery life) make those protocol inappropriate.

Table 1: Threat analysis from LN’s point of view (part)

Asset	Attacking domain/ role	Threat	Possible security service
data/information	IAN	eavesdrop LN’s data when it passes through	confidentiality
		tamper LN’s data when it passes through	integrity
		collect general information of LN to help further attacks	privacy, management
	I	eavesdrop LN’s data from the air	confidentiality
		collect general information of LN to help further attacks	privacy, management
		masquerade as NIP to eavesdrop/temper LN’s data, e.g., install a roguish access point in public area	authentication
costs	AN	fraudulently charge LN, either too high for a service it has used or for services it has not used at all	non-repudiation
	VASP	make LN to use its service without permission of LN, e.g. to install a roguish agent on LN	access control, (firewall)

B. *Wireless and architecture-specific approaches*

Far before the Internet activity around security and mobility, the wireless world, in particular GSM, standardized solutions relying on the security module (or Subscriber Identity

Module) for authentication to the network. These solutions are based on a long-term subscriber authentication key before allowing a user to use any service from that network. The security module is required to encrypt the voice call with the symmetric key generated in the Subscriber Identity Module (SIM). The SIM is therefore an integral part of the GSM architecture, providing security data storage and cryptographic processing.

Besides cellular solutions, the so-called Wi-Fi sector also provides proprietary solutions addressing the threats described above. So we kindly point the reader to the following references:

- GSM and UMTS [11]
- CHOICE service platform [12]
- 802.1x [13]

Because the limited length of this paper imposes conciseness, we can, without describing these proposals, conclude only on their relevance regarding the MIND project, saying that they suffer from what was considered as profitable from the Internet point of view: They are too proprietary and do not encompass a global pictures like ours. Therefore, as we stated in the previous section, we cannot adopt these solutions.

C. Merging the two worlds

This section proposes some solutions developed to bridge specific architecture to the whole Internet picture frame, in a similar movement to the one perceived in the mobile telecommunication place with the recent 3GPP's 'All-IP' initiative.

Of course, reading the critics previously addressed to the Internet as well as the wireless world, the need of such bridging initiative was evident and it is not so pertinent to conclude by saying that the truth is 'somewhere in the middle between the two worlds'. But the facts are quiet 'stubborn' and here they show, as the existence of proposals and products listed below proves it, that indeed combining in an intelligent way benefits from the two sides (Internet and wireless) is the solution for the secured MIND framework.

- GSM SIM key generation for Mobile IP [14]
- Windows for SMART Cards [15]
- IEEE 802.1X RADIUS Usage Guidelines [16]

The first listed document from Haverinen [14] specifies a mechanism for Mobile IP network access authentication and key distribution using the GSM SIM. The mechanism uses new subtypes of the generalized key distribution extensions for Mobile IP Registration Request and Registration Reply. After the registration keys have been generated, the default Mobile IP authentication with these keys can be used (MD5 in prefix + suffix mode). The keys can be used for several subsequent registrations. However, there are lifetimes for the keys and before the lifetimes expire, new keys can be generated with the same procedure.

So the SIM feature is only use for key generation (the credential of the SIM card are not use for authenticating Mobile IP registration messages). By using the SIM key exchange, no other pre-configured security association besides the SIM card is required on the mobile node.

All these proposals, broadly speaking, have in common the fact that they force heterogeneous building components to talk with each others. This of course requires mapping functions and protocols, meaning in turn Inter Working Function, Gateway and common interfaces.

The wise conclusion sounds therefore: If you are an actor of the MIND domain model, in order to open yourself to a secured mobile communicating scenario you should be ready to accept the necessary compromising with other entities you are not usually used to communicate with.

VII. Security problems in accounting

Inter-domain accounting differs from intra-domain accounting in several important ways. Intra-domain accounting involves the collection of information on resource consumption within an administrative domain, for use within that domain. In intra-domain accounting, accounting packets and session records typically do not cross administrative boundaries. As a result, intra-domain accounting applications typically experience low packet loss and involve transfer of data between trusted entities.

In contrast, inter-domain accounting involves the collection of information on resource consumption within an administrative domain, for use within another administrative domain. In inter-domain accounting, accounting packets and session records will typically cross administrative boundaries. As a result, inter-domain accounting applications may experience substantial packet loss. In addition, the entities involved in the transfers cannot be assumed to trust each other.

Since inter-domain accounting applications involve transfers of accounting data between domains, additional security measures may be desirable. In addition to authentication, replay and integrity protection, it may be desirable to deploy security services such as confidentiality and data object integrity. For example, when information is being collected and analyzed within the same administrative domain, integrity protection and authentication may be used in order to guard against collection of invalid data. In inter-domain applications confidentiality may be desirable to guard against snooping by third parties.

VIII. Conclusion

This paper proposes a domain model approach for tackling security concerns in mobile networking environment. The tool of domain model is deployed to conduct security analysis based on identified protocol stacks at various reference points within the domain model of MIND networks. The security analysis helps to identify potential threats and proposes the security mechanisms. Inter-domain accounting is considered in MIND since its business models allow for many different solutions.

We hope this paper will help to better understand and weight the newly pervasive mobile computing environment and its critical security (and consequently accounting) imponderables.

Acknowledgement

This work has been performed in the framework of the IST project IST-2000-28584 MIND, which is partly funded by the European Union. The authors would like to acknowledge the contributions of their colleagues from Siemens AG, British Telecommunications PLC, Agora Systems S.A., Ericsson AB, France Télécom S.A., King's College London, Nokia Corporation, NTT DoCoMo Inc, Sony International (Europe) GmbH, T-Systems Nova GmbH, University of Madrid, and Infineon Technologies AG.

Reference

[1] IST project MIND, www.ist-mind.org

[2] IST project BRAIN, www.ist-brain.org

[3] IETF MONET-WG, http://www.nal.motlabs.com/monet/

[4] Tessier, S., *Guidelines for Mobile IP and IPSec VPN Usage*, draft-tessier-mobileip-ipsec-00.txt, Internet Draft, work in progress, June 2002

[5] Adrangi, F., Leung, K., Kulkarni, M., Patel, A., Zhang, Q., Lau., J., *Problem Statement and Requirements for Mobile IPv4 Traversal Across VPN Gateways*, draft-ietf-mobileip-vpn-problem-statement-00.txt, Internet Draft, work in progress, March 2002

[6] Adrangi, F., Iyer, P., Leung, K., Kulkarni, M., Patel, A., Zhang, Q., Lau, J., *Mobile IPv4 Traversal Across IPsec-based VPN Gateways*, draft-adrangi-mobileip-vpn-traversal-02.txt, Internet Draft, work in progress, June 2002.

[7] Engelstad, P., *Extensible Authentication Protocol over IP (EAPoIP)*, draft-engelstad-pana-eap-over-ip-00.txt, Internet Draft, expired, January 2002

[8] T.J. Kniveton et al., *Mobile Router Support with Mobile IP*, draft-kniveton-mobrtr-02.txt (work in progress), Internet Draft, work in progress, July 2002

[9] Belding-Royer, E. et al., *Global Connectivity for IPv4 Mobile Ad hoc Networks*, draft-royer-manet-globalv4-00.txt, Internet Draft, expired, November 2001

[10] *Mobile Information Device Profile (MIDP)*, http://java.sun.com/products/midp

[11] *Digital cellular telecommunication system (Phase 2); Security related network functions*, GSM Technical Specification GSM 03.20 (ETS 300 534), European Telecommunications Standards Institute, August 1997

[12] Bahl, P., *PAWNs: Satisfying the need for ubiquitous secure connectivity and location services*, IEEE Communication Magazine, February 2002

[13] *IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control*, IEEE Std 802.1X-2001, June 2001.

[14] H. Haverinen, *GSM SIM Authentication and Key Generation for Mobile IP*, draft-haverinen-mobileip-gsmsim-02.txt, Internet Draft, expired, April 2001

[15] *Windows for smart cards*, www.microsoft.com/windowsce/smartcard/start/intro.asp

[16] Congdon, P., Aboba, B. et al., *IEEE 802.1X RADIUS Usage Guidelines*, draft-congdon-radius-8021x-20.txt, Internet Draft, work in progress, June 2002

[17] Glass, et al, *Mobile IP AAA Requirements*, RFC 2977, October 2000

[18] Aboba, B. and J. Vollbrecht, *Proxy Chaining and Policy Implementation in Roaming*, RFC 2607, June 1999

[19] B. Aboba, J. Arkko, D. Harrington, *Introduction to accounting management*, RFC 2975, October 2000

[20] Ròbert Párhonyi, *Status of the provider based architecture (PBA arch)*, January 2002