World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:1, No:5, 2007

Authenticated Mobile Device Proxy Service

W. Adi[1], Khaled E. A. Negm[1], A. Mabrouk[2], H. Ghraieb [3]

Open Science Index, Electronics and Communication Engineering Vol:1, No:5, 2007 publications.waset.org/6760/pdf

***Abstract*—**In the current study we present a system that is capable to deliver proxy based differentiated service. It will help the carrier service node to sell a prepaid service to clients and limit the use to a particular mobile device or devices for a certain time. The system includes software and hardware architecture for a mobile device with moderate computational power, and a secure protocol for communication between it and its carrier service node. On the carrier service node a proxy runs on a centralized server to be capable of implementing cryptographic algorithms, while the mobile device contains a simple embedded processor capable of executing simple algorithms. One prerequisite is needed for the system to run efficiently that is a presence of Global Trusted Verification Authority (GTVA) which is equivalent to certifying authority in IP networks. This system appears to be of great interest for many commercial transactions, business to business electronic and mobile commerce, and military applications.

***Keywords*—**Mobile Device Security, Identity Authentication, Mobile Commerce Security.

I. Introduction

THE rapid progress in wireless communication systems, personal communication systems, and smart card Technologies has brought new opportunities and challenges to be met by engineers and researchers working on the security aspects of the contemporary communication technologies [1,2].

Having this technology available on the market, made a high demand for many applications and services to get restricted to certain physical devices. However, there are still significant difficulties to overcome when integrating mobile devices with embedded features into a ubiquitous computing environment. These difficulties include designing devices smart enough to collaborate with each other, increasing ease-of-use, and enabling enhanced connectivity between the different devices [3-6].

Public-key cryptography offers robust solutions to many of the existing problems in communication systems, however;

Manuscript received March 19, 2005. (Write the date on which you submitted your paper for review.)
W. Adi and K. E. Negm are with the Etisalat College of Engineering, Sharjah, POB 980, UAE (corresponding author to provide phone: 50-482-1316; fax: 6-522-5937; e-mail: knegm@eim.ae). A. Mabrouk is with [2]Lufthansa Systems, Germany. H. Gharieb is with Lucent Technologies, Germany.

excessive computational demands (on-line memory, code size, and speed) have made the use of public key cryptography limited. The integration of the CPU-intensive public key cryptography techniques in wireless environment is often delayed or completely ruled out due to the difficulty of implementing efficient reliable solutions A common public cryptographic algorithm such as RSA using 1024 bit keys takes 43 ms to sign and 0.6 ms to verify on a 32-bit ARM9-based RISC CPU installed on the recent Nokia 9210i. Even with the recently released Linux based mobile phone E28 E2800+ with 400 MHz processor the previous argument still valid. [7,8]
A common solution for mobile authentication requires that the mobile device provides its unambiguous identity to the network node to prove its legality. Then the network should be able to confirm the correctness of the provided identity [9-11].

A possible scenario for a carrier service node offering a certain service, which is restricted to a certain mobile device, is presented. In the current research we present a scheme for a carrier service node that can sell a prepaid service to clients and limit the use to particular device or devices for a certain time. To acquire such services, an operator-independent service carrier wireless device should be securely identified, independent on the service provider of the wireless link. Using the authentic identity together with a service token, would allow having a device-restricted service with low management overhead, moderate implementation complexity and minimum payload on the traffic on both network and wireless device side. 3GPP/UMTS, GSM and many Wireless LANs systems do not include authentic physical identification [12-14]. In here we present a novel design for system composed of hardware devices together with a secured software computing mechanism to allow authenticating the device identity in a global operation environment. The mechanism is based on distributed security using a global Challenge-Response technique. This enables the integration of reliable secure mobile equipment identification and shared secret key generation between mobile equipment and carrier service node. The propose systems need no increase in size and complexity which makes it ideal for mobile devices where size, security and power consumption are the most important factors.

In the current research we propose a lightweight system that provides a solution to one of the main authentication problems in wireless data network systems.

Open Science Index, Electronics and Communication Engineering Vol:1, No:5, 2007 publications.waset.org/6760/pdf

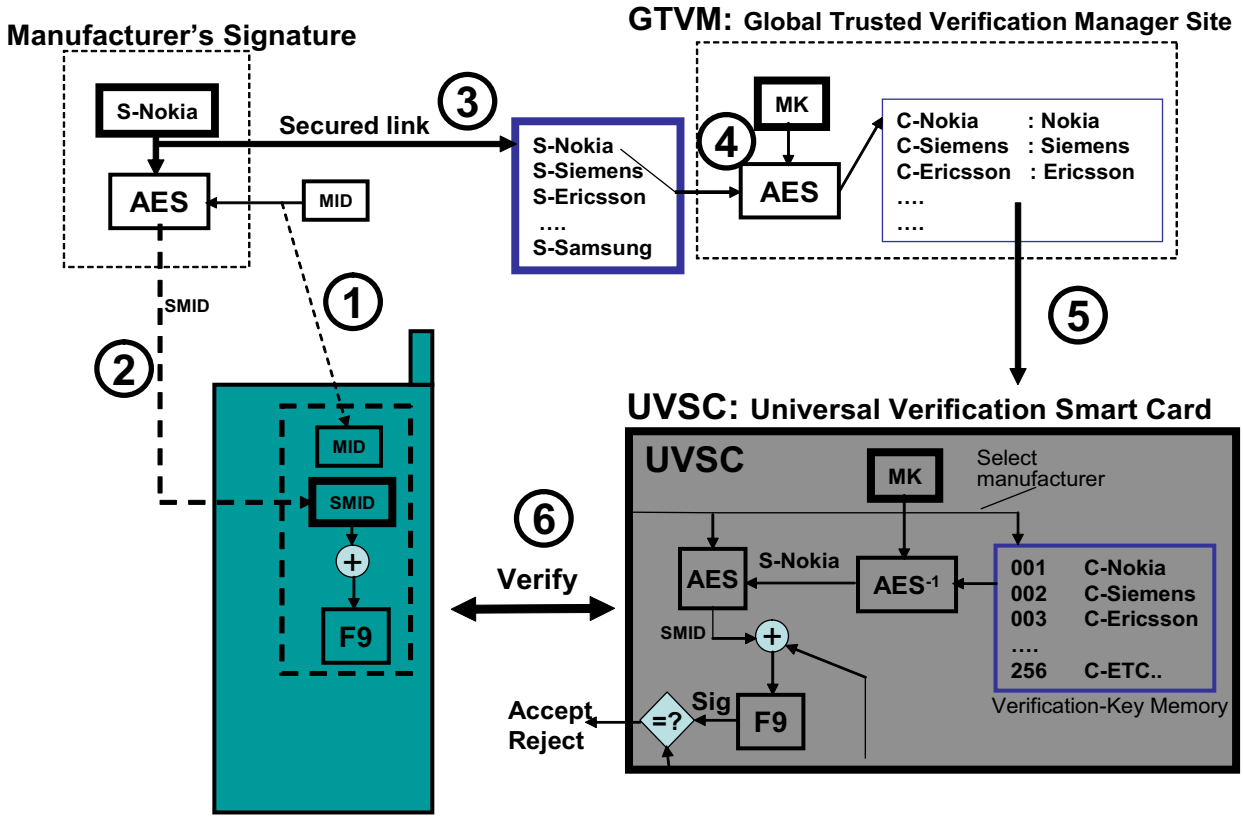


Figure a. Manufacturer Certification Process

To have the system performs good stands; it is obvious that we need the following:

- Public key or public-key equivalent cryptographic system with higher strength per key bit.
- Efficient platform specific and optimized implementations for a given restricted environment.
- Fast transparent secure system that is user friendly.
- Self secured system that do not allow for known hacking techniques to gain an access to the client session or attack service data over the wireless IP service points.

II. Related Work and Self-Certification Key (SCK)

The concept of self-certified key (SCK), introduced in [15], is a sophisticated combination of certificate-based and identity-based models. Using RSA cryptosystem a user assigns his secret key, computes public key, and submits it to the certifying authority. Then the authority computes a certification parameter for the client, which satisfies a computational unforgeable relationship with the public key and the identity [16]. A verifier can compute the public key from the identity and the certification parameter. Petersen and Horster extended the previous work to DLP-based cryptosystem in which, self-certified key is issued securely using weak blind Schnorr signature protocol [17].

A problem of SCK schemes is that it provides only implicit authentication, i.e., the validity of a SCK is verified only after a successful communication. Lee and Kim improved Petrson and Horster efforts such that explicit authentication of SCK is provided by using the concept of self-certificate [18].

III. Proxy-Firewall Authentication and Accounting System

In the normal operation of the wireless networks the wireless proxy router will be the client's gateway. The handshaking steps that are required prior to service delivery are established over a wireless media, which makes it susceptible to most of the well-known attacks.

In the present system our system we add a security box that enforces security features of the communication establishment and of the service delivered to the client. This is to insure, (after fulfilling the required verification and authentication procedure) that no one can break or steal the session establishment and/or interpret the communicated data.

IV. Device Authentication Mechanism Setup

The mobile device identity MID is a physical unique serial number securely assigned by the device manufacturer. As soon as the authenticity of the MID is proven, the service provider can be sure that the device requesting a service is type approved and fulfils certain quality standards and specifications as assigned by the manufacturer (as embedded

Open Science Index, Electronics and Communication Engineering Vol:1, No:5, 2007 publications.waset.org/6760/pdf

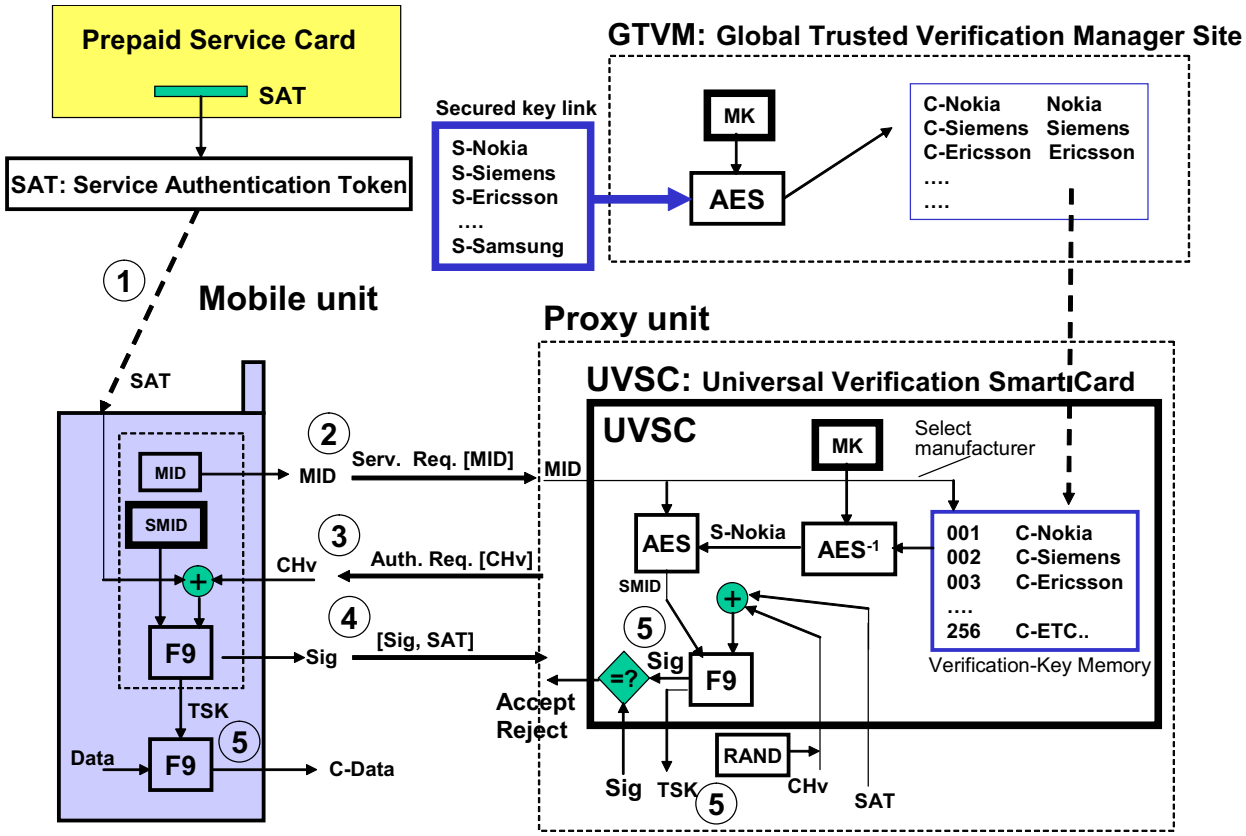


Figure b. Authentication and service flow between a wireless device and a service proxy

in the that MID.) The MID is assumed to be unique such as the IMEI in GSM system or MAC in the internet system. The manufacturer certifies the MID by using the setup shown in Figure a.

To personalize a mobile device, for example by the manufacturer Nokia, the following steps are performed as also numbered in Figure b:

2. A mobile identity number MID is assigned to the device and stored in a permanent memory cell in the mobile device. MID can also printed on the device as a unique serial number.
3. MID is ciphered by using for example AES algorithm with a secret key S-Nokia generated by the manufacturer Nokia. The result is a ciphered S-MID, stored in a write only memory in a physically and electrically tamperproof area within the mobile device itself.
4. The manufacturer submits its secret key S-Nokia to a Global Trusted Verification Manager GTVM who should globally manage the verification keys for all manufacturers (assuming that this communication should be authenticated and secured by some known usual techniques.)
   The GTVM encrypts S-Nokia to C-Nokia by using his secret encryption key (Manager Key) MK and publishes the ciphered Nokia verification key C-Nokia in a public Internet site.

At this stage the certification and authentication mechanism is established. Any Service Provider that is interested to verify the authenticity of a mobile identity MID can purchase a verification smart card from a public source without a need of connection to GTVM and performs following procedure: (the two steps 5 and 6)

5. Pick up the verification key from the home site of the GTVM.
6. Execute an authentication challenge for the mobile device and verify the signature of the mobile manufacturer.

A detailed description of the authentication process is presented in the subsequent sections.

V. Device Restricted Authentication Proxy Service Protocol Analysis

The proxy service can be offered by subscription (e.g., prepaid service) by the service clients through a one time Service Authentication Token SAT. The STA is randomly generated and managed by the service provider. A usual secured technique for providing business finances and management for such value tokens can be integrated. Figure 2 shows the general flow of the whole process with the corresponding hardware, software and network based units.

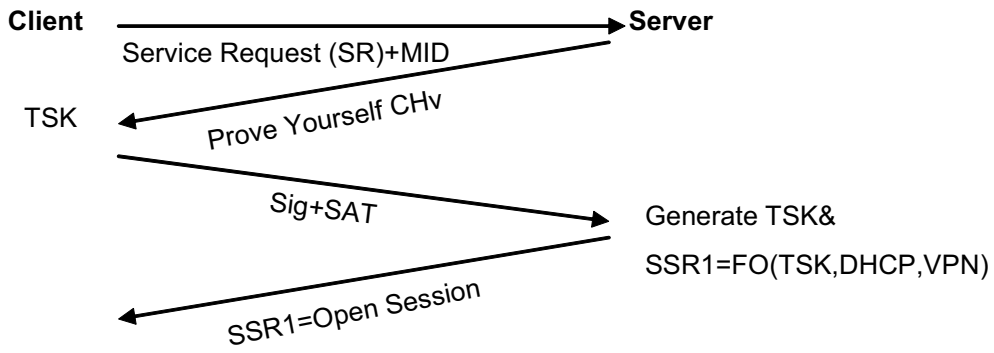


Figure c. Subsequent Sessions' Authentication Mechanism

Open Science Index, Electronics and Communication Engineering Vol:1, No:5, 2007 publications.waset.org/6760/pdf

A. First Session Establishment Authentication Analysis

After scratching the token and inserting it into the mobile or wireless device, the service client can start requesting the service. The several authentication processes are executed as being a part of the underlining authentication protocol (see Figure b). Authentication scheme comes into two parts. The first session is from the client side and the second one is on the proxy (server) side. In the following we will summarize the authentication steps for each.

Session A: Verification of the MID

This part establishes the authentication dialogue between the client and the server, and it constitutes the following steps:

1. A client purchases a service authentication token SAT and inserts it into his mobile device.
2. The mobile device sends-in clear-a service request to the proxy server together with its device identity MID.
   The proxy requests the device to authenticate its MID and challenges the device with a fresh random number CHv. CHv is fresh generated random of say 128 bits by the random generator RAND on the proxy side [19].
3. The Device responds with a fresh electronic signature Sig proving that the given MID is authentic. The signature Sig and the temporary session key TSK are computed as
   TSK|Sig = F0 [S-MID, SAT+CHv],
   where F0 is a highly nonlinear function as a cipher like AES or 3GPP standard Cipher KASUMI [20],

S-MID is the manufacturer unreadable secret signature, which resides in the tamperproof area together with F0 in the mobile similarly as described in [21]. SAT is the purchased service authentication token. The addition is the XOR function.

4. The generated temporary session key TSK is used to encipher any other communication data from Data to C-Data between the proxy and the mobile device using the same function F0. The vector Sig|SAT is then exported to the proxy as the authentication proof for the delivered mobile device identity MID.

Session B: Proxy Proof for the Authentic MID

After the client started his part to authenticate and/or register itself with the service node, the node will perform global verifications for the previous session. One it gets successful, the communication becomes a full fledged and authentic.

5. After receiving the proof vector Sig|SAT, the proxy generates Sig as follows: The mobile device clear identity MID is used to allocate the manufacturer ciphered verification key from the verification memory key, in this case C-Nokia. C-Nokia is then deciphered through AES´ using the protected key MK to yield Nokia signature key S-Nokia. S-Nokia is used to generate the secret mobile device identity S-MID which is combined together with the XORed CHv and SAT to yield the signature Sig' and the temporary session key TSK through the function F0. The output in this case should be equal to the sent Sig. If Sig'=Sig then the identity is assumed to be correct.
6. If the mobile device identity is authentic, then the same TSK that generated on the mobile device side will be generated on the proxy end through the smart card VSC [22]. The generated TSK is used to communicate securely with the mobile device for any further data communications.

Note that the computation power of the smart card should not be high as both encryption functions use either AES or F0 (for example KASUMI) are chosen as block ciphers. The total performance of the system is equivalent to a public key system but it uses only fast secret key mappings.

B. Subsequent Sessions' Authentication Mechanism

For any new session, different authentication mechanism will take place. In this case the mobile device will make use of the TSK that is previously issued from the last session and will perform the following steps:

1. After being authenticated together with the mobile device, the client sends a service request packet (SR) to the server as shown in Figure 3.
2. Then the server replies by requesting verification in form of a challenge.
3. The client replies back by the temporary service key TSK that was assigned for it at the end of the previous session.

4. The server encrypts the incoming TSK along with allocated virtual channel numbers assigned to the current session in addition to dynamical IP (if required) for the type of service requested by the client. The proposed type of encryption function is AES.

VI. Security Concerns

Only one sort of attack on the system appears to be possible but with very great difficulty. Another mobile can highjack the service if it catches the mobile MID as in a man in the middle attack and forwards its own MID, then wait until the original mobile device send its SAT and use it instead of the original mobile. This requires however very careful and strict synchronization. This risk scenario can however be ruled out with minor changes in the protocol if necessary [23-24].

VII. Summary And Conclusion

Secured mobile device restricted proxy service is presented. The system authenticates securely the mobile device identity in a global fashion. The system exhibits public key behavior without using highly complex public key techniques. Such mechanisms could be very useful and very low cost effective to implement in the future wireless widespread global application.

It is clear that the resulting system is a set of low complexity secret key mechanisms, which is well established in mobile technology authentication [15, 17]. The main advantages are, no online secret key transmission is required to check mobile device identity and no prior secret agreement is required, while no secured large databases are required during system operation as in PKI infrastructure. In addition to no large data bases are required although million of mobile identities are authenticated.

VIII. Future Work

Currently we are studying an implementation to secure the system against man in the middle attack. Two proposed scenarios are undergoing. The *first* scenario, by using the current available technology of 802.1x and WPA encryption based on the fact that most of the current mobile systems are IP enabled and having it presence in some countries like Germany as afforded by the T-online nation wide [25]. The *second*, scenario is via using secure mobile agents and/or other secure mobile computing mechanism [26-28].

References

[1] Malan, D., Crypto for Tiny Objects, Harvard University Computer Science Report, TR-04-04, 2004.

[2] Handschuh, H. and Paillier, P., Smart card crypto-coprocessors for public-key cryptography, In J.-J. Quisquater and B. Schneier, editors, LNCS, 1820, pp. 386-394. Springer-Verlag, 2000.

[3] M. Dertouzos. The future of computing. Scientific American, August 1999.

[4] G. Banavar, J. Beck, E. Gluzberg, J. Munson, J. Sussman, and D. Zukowski. Challenges: An application model for pervasive computing. In Proc. ACM MOBICOM, 2000.

[5] Patriciu, V., Marin Bica, M. and Ion Bica, I., Implementation Issues of PKI ssTechnology, International Carpathian Control Conference ICCC' 2002, pp. 513-518.

[6] Housley R. and Polk T., Planning for PKI, John Wiley, 2001.

[7] http://linuxdevices.com/

[8] http://www.linuxmobilealliance.org

[9] Koutsopoulou, M., at al., Charging, Accounting and Billing Management Schemes in Mobile Telecommunication Networks and the internet, IEEE Communication Surveys, 6, 2004, pp. 50-58.

[10] Kim, H. and Afifi, H., Improving Mobile Authentication with New AAA Protocols, in IEEE International Conference on Communications 2003 (ICC'03), Anchorage, USA, 2003.

[11] Mitton, D., et al., "Authentication, Authorization, and Accounting: Protocol Evaluation," RFC 3127, 2001.

[12] 3GPP. 3G security: Security Architecture, Technical Specification Group Service and System Aspects, 3GPP TS 33.102 V. 3.6.0, 2000.

[13] Glass, S. et al., Mobile IP Authentication, Authorization, and Accounting Requirements, Internet RFC2977, 2000.

[14] G.Schaefer, G., Karl, H., and Festag, "Current Approaches to Authentication in Wireless and Mobile Communications Networks", Technical Report TKN-01-002, Telecommunication Networks Group, Technische Universität Berlin, 2001.

[15] M. Girault, Self-certified public keys", Advances in Cryptology: Eurocrypt'91, LNCS 547, Springer-Verlag, 1991, pp. 490-497.

[16] Blaze, M, Feigenbaum, J, and Lacy,J., Decentralized Trust Management, IEEE Symposium on Security and Privacy, 1996, pp. 164-174.

[17] Petersen, H. and Horster, P., Self-certified keys "Concepts and Applications", In Proc. Communications and Multimedia Security'97, pp. 102-116, Chapman & Hall, 1997.

[18] Lee, B. and Kim, K., Self-Certificate: PKI using Self-Certified Key", Proc. of Conference on Information Security and Cryptology 2000, Vol. 10, 2000, pp. 65-73.

[19] Cryptographic Module Security Policy, Federal Information Processing Standards Publications, FIPS 140-1, November 2004.

[20] Technical Specification 3G Security, Security Architecture 3G TS 33.102 V. 3.2.0 from 10.1999.

[21] W. Adi, "Secured Mobile Device Identification with Multi-Verifier", International Conference on Telecommunications (ICT2001), 2001, pp. 289 – 292.

[22] 3GPP. Technical Specification Group Services and System Aspects, 3GPP TR 21.905 V5.5.0, 2002.

[23] Kostiainen, K., Intuitive Security Initiation using location-limited channels, Master's Thesis, HELSINKI UNIVERSITY OF TECHNOLOGY, 2004.

[24] Gehrmann, C. Mitchell, C., and Nyberg, K., Manual authentication for wireless devices, CryptoBytes, Vol. 7, 2004, pp. 30-40.

[25] http://www.t-online.com/

[26] Adi, W., Al-Qayedi, A., Negm, K., Mabrouk, A., Musa, S., Secured Mobile Device Software Update over IP Networks, IEEE SoutheastCon 2004, 2004, pp 271-274.

[27] Mabrouk, A., Adi, W., Gharieb, H., and Negm, K., Proxy Based Signature with Secured Mobile Computations, Proceedings of International Symposium of Telecommunications-IST2003, 2003, pp. 544-546.

[28] Negm, K., Adi, W., and Abd-ElWahab, F., Secure Mobile Code Computing Framework, WSEAS Transactions on Information Science and Applications, Vol. 1, 2004, pp. 1411-1416.

Open Science Index, Electronics and Communication Engineering Vol:1, No:5, 2007 publications.waset.org/6760/pdf

K. Negm, Ph.D., SMIEEE, CISSP, CISA, Associate Professor in Etisalat College of Engineering and Senior Security Specialist Dr. Negm is a member of the Information Systems Security Association (ISSA)-USA and Information Systems Audit and Control Association (ISACA)-USA. He is the Associate Chairman for the Security Standards Committee and Secretary for the Scientific Committee of the ISSA for the Middle East and Asia. Also he is a member of the Technical Committee of Security Standards of the IEEE and the USENIX group. He is a member of many IEEE committees as: Technical Committee on Computer Communication, Technical Committee on Security and Privacy, Task Force on Information Assurance.

Currently he is an Associate Professor in Etisalat College of Engineering, UAE. He have various International collaborations, TRIUMF-Canada, ICTP-Italy, and ECT*-Italy, NATO -Italy. For the last 18 years he have been involved in carrying out responsibilities for the Network Security Architecture, including the design, implementation, and administration of firewalls, Web servers, proxy servers, SecureID and other network security components for several Governmental Departments, Security Agencies, Banks and Educational Institutes. He provided training and consulting in the areas of security solutions and security audits. This involved writing the corporate security policy, designing and implementing the corporate firewall solution, and providing secure access for remote systems. Dr.

Dr. Negm has authored over 60 papers in refereed technical journals and international conferences. He is a Senior Member of the IEEE and Member of the Applied Computational Society. He is a regular reviewer for Modeling and Simulation Journal, IEEE Security and Privacy and Computer Security Journal.

Dr. Negm is an author of well knows published three IDS based on neural networks algorithms. Currently he is interested in IPSEC, Wireless Security, IT Forensics and the AAA Wireless Problems. Dr. Negm is listed in Who's Who in Information Technology and Networks Systems Security and Nominated to be the Professional of the Year 2004 (of IT Security) by the International Association of Networking Professionals-USA.

Open Science Index, Electronics and Communication Engineering Vol:1, No:5, 2007 publications.waset.org/6760/pdf