Authentication Issues in Multi-Service Residential Access Networks

Judith Rossebø[1], John Ronan[2], and Kristian Walsh[3]

[1] Telenor Research & Development, Telenor Communication II AS,
N-1331 Fornebu, Norway (judith.rossebo@telenor.com)
[2] Telecommunications Software & Systems Group,
Waterford Institute of Technology, Waterford, Ireland (jronan@tssg.org)
[3] Department of Mathematics and Computing,
Cork Institute of Technology, Cork, Ireland (krwalsh@cit.ie)

Abstract. Multi-service residential access networks allow residential customers to choose amongst a variety of service offerings, over a range of Core Networks and subject to user requirements such as QoS, mobility, cost and availability. These issues place requirements on authentication for network access, with a need for mutual authentication of the residential gateway (RG) to the local access point (LAP). The EU-IST project TORRENT is building a testbed providing for multi-service residential access networks in order to demonstrate the benefit of intelligent control, both for the customer and for the network operators and service providers. Adequate security measures are essential in order to secure access to the TORRENT system and services and for QoS provisioning to authorised users. This paper examines the authentication issues for the TORRENT system and presents a public key based authentication protocol for mutually authenticating the RG and the LAP.

Keywords: Authentication, Public Key Infrastructure, Encryption, Residential Gateway

1 Introduction

Multi-service residential access networks are concerned with exploiting the use of shared physical access networks for a range of different services and traffic types optimising bandwidth utilisation in existing access networks while meeting user requirements related to QoS, security, cost and availability. In order to deliver such offerings to the residential customers, an infrastructure is required mapping user requirements to the appropriate networks, services, and applications. The infrastructure typically incorporates a residential gateway in the home and one or more serving local access point(s)(LAP) integrating access technologies with services and core networks. The residential gateway(RG) connects the home network technologies (especially WLAN, Ethernet) to the access network(s), e.g. cable and ISDN, xDSL and ISDN, or even LMDS. Functions of the local access point may include providing customer negotiation facilities

and host accounting and security functionality (e.g., AAA services) of customer access to e.g., metering, security, and monitoring.

This work has evolved from investigations in the TORRENT project of authentication issues in multi-service residential access networks. In future multi-service residential access networks, users may have the opportunity to choose between several network operators and service providers. Authentication requirements of the different network operators and service providers can lead to the situation that a user has to keep track of several different usernames and passwords and different methods of authenticating to the networks and services. There is a need for a single mechanism for authentication, which gives the user access to all services. For this, the mechanism should be suitable for services requiring strong authentication (e.g. signing your loan application electronically). This paper discusses the issues involved and presents our scheme for public-key based authentication for which a smart card is used as certificate and key container and may also be used for authentication to many services.

1.1 TORRENT Overview

TORRENT is an EU-supported Framework V project, aiming at building a test-bed for multi-service residential access networks. This test-bed (Figure 1) will allow the project to demonstrate the benefit of intelligent control, for the customer, for the network operators and service providers. An important goal is to optimise the bandwidth utilisation in existing access and core networks, while at the same time meeting user requirements in an optimal manner. These requirements include Quality of Service (QoS), security, cost, and availability. Security is of major importance, and adequate security measures are essential in order to secure access to the TORRENT system and services, and also for provisioning QoS to authorised users.

IPv6 is integrated in TORRENT as a transport protocol and the IP Security Protocol (IPsec) is used as a service for securing the data between the Residential Gateway (RG) and the Local Access Point (LAP). Investigations of various authentication and key agreement schemes have been carried out in the IPsec performance trials, as documented in [2].

The authentication requirements for the TORRENT system have been determined by a threat analysis. It was determined that the threats of masquerading by LAP or RG can be mitigated by mutually authenticating the LAP and the RG. Authentication is important e.g. to ensure that the authorised customer behind an RG is getting the QoS that was requested, to reduce the likelihood of fraud and also as a baseline for avoiding repudiation of messages e.g. payments. Users and providers of networks and services will thus benefit from this security service. A scheme for providing this will be presented later in the paper.

2 Background and objectives

This paper presents the work on authentication done in the TORRENT IST [8] project. It is a requirement of TORRENT to mutually authenticate the RG and

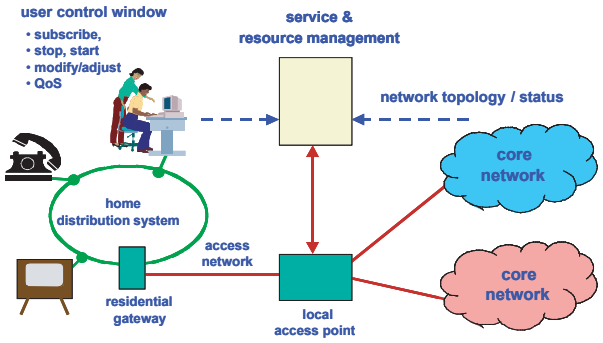

Fig. 1. TORRENT Architecture

the LAP. It is a requirement to provide users with secure access to TORRENT services. It is also a requirement to authenticate users accessing the system e.g. to make changes to the user profile and user preferences (service subscription, QoS, cost, etc.) It was also foreseen that if a hardware (HW) token is used as key holder of the authentication exchange, then this HW token could also be used for user authentication (of the RG user) and eCommerce applications. The same token could be used for authentication and key exchange for the IPsec VPN tunnel service. Certificates and associated private keys for authentication and encryption of agents and agent communication can also be stored on the HW token. In fact, certificates and associated private keys for the services of user authentication, electronic signature, and encryption can be reused by TORRENT's agent based Service to Resource Management system for authentication of the user agents. Therefore, public key techniques were explored early on in the TORRENT project.

2.1 Assumptions

We make the following general assumptions about the TORRENT system:

- The link between the RG and LAP is vulnerable.
- The user access to the user profile interface is vulnerable.
- The link (not shown) between service domains (e.g., LAP to LAP) is vulnerable.

2.2 Security Objectives

Authentication is the verification of claimed identity, and can be either single-sided or mutual. In TORRENT, authentication of the RG to the LAP is important to prevent false or unauthorised RGs from registering and obtaining access

to the TORRENT system. Similarly, authentication of the LAP to the RG is important, to prevent another device from masquerading as a real LAP in order to intercept user traffic and private information. It is feasible that an RG owner can subscribe to services on different LAPs, which increases the risk of such a masquerade attack. Authentication of the user behind the RG to the subscriber interface is also important e.g. to prevent unauthorised changes to the user preferences and possibly fraud. Authentication of agents to each other in the agent system is also required to prevent manipulation of traffic sent between agents. Authentication of agents is addressed in [4].

2.3 Enabling Quality Of Service

Authentication alone will not guarentee that the customer receives the QoS that was requested. However, assuming that QoS mechanisms are in place to maintain and control the quality of service, mutual entity authentication is an important countermeasure to a number of threats to QoS provisioning.

For example, if authentication of the RG to the LAP is insufficient, an attacker may make a distributed attack from many false RGs allocating a substantial number of QoS enabled flows, which binds up the resources and degrades the performance for authorised user flows. An important mitigating measure to counter this attack is mutual authentication of the RG and the LAP. In the case of the TORRENT project, the user may select a level of QoS on a per service basis via a GUI hosted on the LAP. Sufficient authentication of the user for access to the GUI and integrity protection of the communication on the link between the RG and the LAP is required to prevent unauthorised users from registering using an authorised customers ID and masquerading in order to obtain a higher level of QoS without paying for it.

3 Authentication and key agreement based on public key techniques

In this section we will discuss the case for public key authentication techniques for network access.

3.1 Background

Historically, authentication for network access has been done using shared secret techniques and this has proven to be scalable. For ISDN and now ADSL the residential user is issued a terminal per service (NT box for ISDN, ADSL modem for ADSL). ADSL modem authentication is at best, password based and open to dictionary attacks when the password is small or insufficiently random. Requirements have been lax: it is well known that most ADSL modems can be hacked without requiring sophistication [5]. It is well known that 2G and 3G mobile telecommunication systems use secret key techniques for network access.

As the number of access networks increases scalabity issues become more significant. In GSM, for example, scalability is achieved using brokers and roaming agreements. A small operator has an agreement with a roaming broker, which establishes roaming agreements with a lot of other operators. It can be argued that as the number of operators and roaming agreements grows significantly, then these bilateral agreements may be inefficient and costly to maintain. But essentially, scalability issues alone do not provide a strong argument for the case for public key techniques for network access.

Public key techniques were ruled out early on in the 3G design and standardisation process as these were considered too complex and seemed to require too much computational overhead. Since then, however, public key based mechanisms have been successfully implemented in the GSM SIM card for e.g. mCommerce and in smartcards [6], demonstrating that computational overhead is no longer an issue.

The strong arguments for public key techniques are scalability and to some extent mobility (of the user to choose freely between networks and service providers), and the elegance of the reusability of public key techniques for a multitude of services such as authentication, and key exchange, notary public services, eCommerce, mCommerce, and electronic signatures. Use of public key techniques is also motivated in part by stronger requirements for user anonymity — public key authentication offers possibilities for providing strong user identity and location confidentiality as the user id and location information does not need to be transmitted in the clear over the network. For example, the public key of the authorised receiving party can be used to encrypt the identity and other private information belonging to the user.

Another benefit of using public key techniques is that the mechanism can also be re-used (e.g. for application security, electronic signature, and electronic payment) this will be described in more detail later in the paper.

4 Authentication in TORRENT

In this section we will propose a scheme for public key authentication for securing network access from the user of the RG to the LAP.

The LAP is fitted with a hardware key container with a (possibly several) server certificate(s) and associated private key(s). A smartcard as certificate and key container is inserted in the RG. The user behind the RG has a relationship with a trusted third party (certificate validator/broker).

At least one X.509 certificate and associated pair of keys are stored on the smartcard for authentication and encryption purposes (actually, the public key is contained in the certificate, while the private key is not). The trusted third party's public key certificate is also stored on the smartcard to enable validation of foreign incoming certificates.

The RG user Smartcard contains a certificate binding the RG user to a public key suitable for both encryption and signature verification (or it contains two separate certificates). The LAP has a certificate binding the LAP operator

to certificate issued by a Certificate Authority (CA). The CVC functions as a trusted third party and has an agreement with the CA that issued the certificate to the LAP allowing it to perform certificate validation services on behalf of the CA, and it also has such an agreement with the CA that issued the certificate(s) to the RG user. The CVC public key is installed on the RG user smartcard a priori. Note, it is feasible that the RG user may have the public keys of several CVCs installed on their smartcard.

The aim is to mutually authenticate the RG and the LAP using public key techniques. The motivation for this is the case that the user of the RG does not have to be bound to a Service Provider or Operator (by a subscription) but is free to shop around for network access and services. In this case, shared secret keying techniques are not appropriate. It should be noted that this algorithm can be applied to both wired and non-wired network access.

Use of public key techniques for network access has been studied in the SHAMAN project [7] and two methods for authentication and key agreement using public key techniques are described. The protocol presented in this paper is different from those presented by SHAMAN. In the method described in SHAMAN the mobile node has a subscription to a home operator, and must establish network access with an access network, which has an agreement with the home operator or a roaming broker. This network access point (e.g. LAP) has a number of pre-installed public key certificates (signed by each trusted third party or home network with which it has an agreement). The access network sends the appropriate one to the node (e.g. RG) and this is used by the node to assure the node that a roaming agreement exists with the home network.

In the TORRENT case, however, the user does not necessarily have a relationship/subscription to a home network, nor does the LAP have to have an agreement with other access network operators. Both must have X.509 certificates that can be validated by a trusted third party, which we call a Certificate Validation Clearinghouse/broker (CVC). It is the Certificate Authority's public key that is pre-installed in the RG key holder (probably a smartcard) and which is used in the validation process. The CVC validates the RG user's certificate on behalf of the Certificate Authority for the LAP, and the LAP's certificate on behalf of the RG.

Public key techniques are used to mutually authenticate the LAP to the RG and the RG to the LAP using a trusted third party called the CVC. The CVC can function as a broker and a clearinghouse. This differs from the method presented in SHAMAN [7]. In the case provided in [7], the Local Access Point has a collection of certificates and must send the appropriate one to the RG. The RG then validates the Local Access Point based on the certificate that it receives. In the TORRENT protocol, it is the CVC that validates the LAP certificate for the RG, and the CVC validates the RG certificate for the LAP. How this validation is performed is outside of the scope of this paper: a thorough explanation can be found in [3].

Once the certificate validation process is completed, the type of payment for services (e.g., bandwidth, QoS, VPN) can be agreed using the preferred payment

method such as credit card, online banking, billing directly based upon some method associated with the smartcard, etc. (again, the exact method used is outside of the scope of this paper).

5 Protocol RRW strong two-way entity authentication

The basic protocol involves A (the RG User Smartcard), B (the LAP), and T (the CVC server). At outset the RG User Smartcard contains at least one public key pair suitable for both encryption and signature verification and in accordance with X.509 standards. The RG user's Smartcard must also acquire (and authenticate) the CVC encryption public key *a priori*. The LAP has its public key pair for signature and encryption. The CVC server has a public key pair for signature and encryption. The CVC has an agreement with the CA that issued the certificate to the LAP, allowing the CVC to validate on behalf of the CA which issued the LAP certificate. The CVC also has an agreement with the CA that issued the card to the user.
SUMMARY: RG User Smartcard interacts with a Trusted CVC server and LAP.
RESULT: mutual entity authentication.

1. Notation

   A denotes the RG User Smartcard.
   B denotes the LAP
   T denotes the CVC server.
   I_T denotes the identification of the CVC so that the authentication request can be sent to the correct CVC.
   $P_X(y)$ denotes the result of applying X's encryption public key to data y.
   $S_X(y)$ denotes the result of applying X's signature private key to data y.
   (t_X, r_X) denote the challenge and response pair generated by X.
   Let r_{TX} denote the response generated by T to the challenge of X.
   $CertX$ is a certificate binding party X to a public key suitable for both encryption and signature verification. Remark: A good practice is to avoid using the same cryptographic key for multiple purposes.
   Let $cert_X ok$ denote the "$Cert_X$ has been validated

2. System Setup

   a) Each party has its public key pair for signature and encryption.
   b) The encryption public key of the CVC is installed on the RG user Smartcard *a priori*.
   c) The CVC server has an agreement with the Certificate Authority (CA) that issued A's public key certificate(s) allowing the CVC to validate A's certificate on behalf of the CA, and similarly with the Certificate Authority that issued B's public key certificate.

3. Protocol messages

$$A \longleftarrow B: \ Cert_B, S_B(t_B) \quad (1)$$
$$A \longrightarrow B: \ Cert_A \quad (2)$$
$$A \longrightarrow B: \ P_T(Cert_A, S_A(t_A), Cert_B, S_B(t_B)), I_T \quad (3)$$
$$B \longrightarrow T: \ P_T(Cert_A, S_A(t_A), Cert_B, S_B(t_B)) \quad (4)$$
$$A \longleftarrow T: \ P_A(cert_B ok, r_{TA}) \quad (5)$$
$$B \longleftarrow T: \ P_B(cert_A ok, r_{TB}) \quad (6)$$

4. Protocol actions
   - **a)** On request from A, B creates challenge and response pair (t_B, r_B), signs the challenge and sends the signed challenge with its public-key certificate to A. (1)
   - **b)** A sends (2), its public-key certificate to B
   - **c)** A creates challenge and response pair (t_A, r_A). A encrypts a message for the CVC server T containing A's public-key certificate ($Cert_A$), A's generated and signed challenge ($S_A(t_A)$), B's public-certificate ($Cert_B$) and B's generated and signed challenge ($S_B(t_B)$). This combined message is sent along with the CVC identification I_T to B (for relaying to T).
   - **d)** B uses the cleartext identifier in message (3) to relays the encrypted data containing A's public-key certificate ($Cert_A$), A's generated and signed challenge $S_A(t_A)$, B's public-certificate ($Cert_B$) and B's generated and signed challenge $S_B(t_B)$ to T.
   - **e)** T decrypts (4) using its private decryption key. T validates $Cert_A$, $Cert_B$, and the signatures of the two challenges. If all checks succeed, Validation yields two messages: "$Cert_A$ has been validated" and "$Cert_B$ has been validated" . T also computes the response r_{TA} to A's challenge t_A, and the response r_{TB} to B's challenge t_B and sends (5) to A and (6) to B.
   - **f)** A decrypts (5) and checks that $r_{TA} = r_A$. If decryption is successfull and all checks succeed, A declares authentication of B successful.
   - **g)** B decrypts (6) and checks that $r_{TB} = r_B$. If decryption is successful and the check succeeds, B declares authentication of A successful.

Note: Upon authentication, A and B may proceed directly with a key-exchange for IPsec. The symmetric VPN session key is not embedded in the above protocol as is the case with the Kerberos protocol as we have determined that the CVC shouldn't know what the session key would be. With Kerberos, two session keys are optionally generated: one by the trusted third party, and a subsession key shared by A and B, but not chosen by T. In both cases the CVC is aware of the session key. As the session key may be used for encryption over weeks, even months, it is unnecessary for the CVC to be aware of this key. Upon authentication, then A and B should proceed directly with a key-exchange for IPsec.

Figure 2 shows the flow of information in the proposed RRW mutual authentication protocol

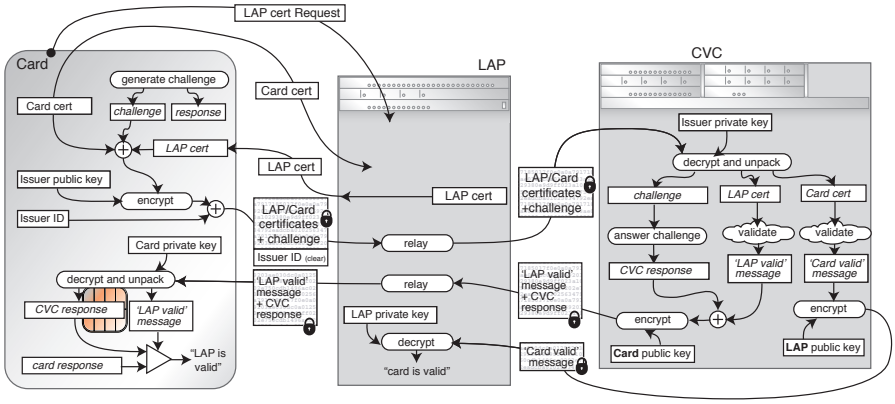

Fig. 2. Authentication Process information flow

5.1 Periodic Validation

To prevent redirection of the communications channel once authentication has been completed, it is necessary to periodically ensure that the authenticated parties are still in control of the communications channel. The method used here is a periodic "challenge-response" from LAP to the Card in the RG.

This challenge is encrypted using the Card's public key (as obtained by the LAP during authentication), and can be as simple as a series of numbers from which the card must calculate a result. The card will then encrypt this result using the LAP's public key (as received from the LAP during authentication).

If the LAP does not receive the correct result from the card within a reasonable amount of time, the LAP will cease routing traffic to or from the RG containing the non-responsive card. Conversely, if the Card does not receive a challenge from the LAP within a reasonable time, it will disable the RG interfaces on the assumption that the LAP has either failed or has been compromised.

6 Feasibility

The greatest barrier to implementation of this system is the ability of the smart card processor to perform the necessary encryption and decryption operations.

The protocol, as presented, requires the smart card to perform one encryption and one decryption. These operations must be performed on-card, as the RG in which the card sits is a non-trusted system.

6.1 Encryption Algorithm

Because of the limited computational power of the smart card processor, a computationally-light, but still secure encryption scheme is required. Elliptic

Curve Cryptography (ECC)[13] offers strength at least equal to the more widely-deployed RSA. However, ECC requires shorter key lengths and lower computational load [**?**] [**ref to report to back this up**], and as such would be an ideal candidate for use in the system described here.

6.2 Smart Card Performance

The encryption and decryption operations performed by the card are not time-critical: because authentication is not performed regularly, a time of up to three seconds from card insertion (a similar performance to most pay TV systems) is acceptable and easily achievable.

Current microprocessor smart cards can already be used for key generation and encryption using ECC techniques, and so are well able to perform the encrypt/decrypt operations required by the protocol presented here.[15][16].

6.3 Threat analysis

The primary weakness in this system, as in all trusted-party systems, is the integrity of the CVC server. However, assuming that the operator of the CVC Server takes adequate measures to protect it from subversion, destruction or replacement, a potential attacker is left with only three other targets: the smart card, the RG, and the LAP. Each of these is examined in turn.

Smart Card The Smart card is a closed computer system (with CPU, RAM, ROM), whose only means of communication with the RG —and via the RG, the network — is via a simple serial data link [**?**]. The firmware running on the smart-card card CPU controls what information is sent along this serial link to the RG.

The smart card private key and public key are written into on-card read-only memory during manufacture. The software on the smart card will never cause the private key to be sent out of the card, and there is no other way to access the on-card memory without resorting to industrial disassembly of the card chip.

Messages from the smart card to the LAP and CVC are encrypted on the card before being passed to the RG for transmission. The exception to this is the initial exchange of certificates between smart card and LAP, when the smart card sends its X.509 certificate in "clear text". However, the only information of consequence in this certificate is the card's public key, disclosure of which does not compromise the safety of the card's private key.[11]

To defeat counterfeit cards, the smart card signs its challenge to the CVC using the card's own private key — a counterfeit card will not have this key, and so cannot generate a correctly-signed challenge message.

RG The Residential Gateway is probably the most physically insecure part of the system. The RG is envisioned as a mass-produced, dedicated computer system, based on open-standards. As such, the RG is susceptible to substitution:

a malicious user can create their own fraudulent RG using a general purpose PC and a smart-card interface. It is precisely for this reason that the protocol as presented here assumes that the RG is a hostile party in the system.

No critical messages are passed to the RG without first being encrypted. The RG can choose not to forward these messages, but this will result in a denial of service, as the LAP will not enable the RG to LAP link until authentication is complete.

Authentication messages arriving into the RG are encrypted, with the exception of the LAP's certificate received during initial certificate exchange. However, the LAP appendeds a signed (by the LAP) challenge message to its certificate in order to prevent tampering with this message by the RG (or the smart card).

It is conceivable that a tampered RG could be re-programmed to perform authentication once with a legitimate card inserted, and then remain on-line indefinitely, regardless of the presence of the smart card. The periodic validation scheme (§5.1) is designed to defeat this attack: without a legitimate card in the RG to answer the challenge of the LAP, the RG will quickly be disconnected from the network.

LAP The LAP is a dedicated computer system owned and maintained by the network operator, and located on their property. As such, the LAP is a less attractive target for direct attack than the RG or smart card. However, where a shared-medium network (e.g., CATV cable) serves the LAP and RGs, the risk of LAP substitution arises.

In order to defeat a user who sets up a fraudulent LAP and replays the genuine LAP's contributions to the authentication protocol, the genuine LAP appends a challenge message to the certificate it passes to the smart card during the initial LAP/Card certificate exchange. This challenge is signed using the LAP's private key, which allows the CVC to determine its veracity (the LAP's public key forms part of the LAP certificate).

The operator of a fraudulent LAP cannot send the genuine LAP's certificate without an accompanying challenge; and they cannot send the challenge unless it is signed with the LAP's private key, which they do not have access to.

If a LAP's private key is somehow disclosed, the compromised LAP can be issued with a new key pair, and the CVC server can reject any messages signed with the old, compromised, private key. No change is necessary to the smart cards, as they do not store LAP information.

7 State and Sequence Diagrams

Figure **??** shows the authentication progression. The two alternative sections show possible deviations in authentication progression, depending on validity of LAP or Card.

The UML state diagram in Figure 7 shows how the CVC validates the RG certificate and LAP certificates contained in the encrypted message, which is requesting certificate validation of RG for LAP, and LAP for RG.

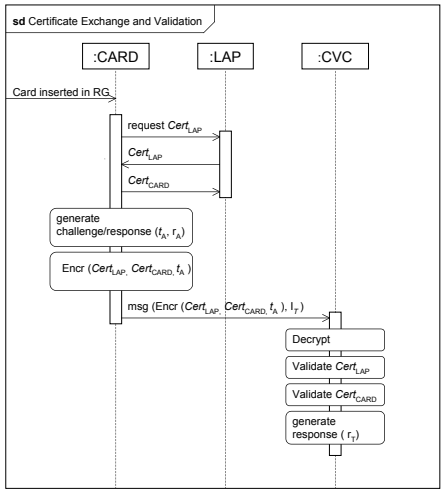

Fig. 3. Sequence for initial LAP/Card certificate exchange

8 Comparison with existing schemes

The proposal is similar to Kerberos[10] in that it involves a party A interacting with a trusted server T and a party B. The encryption algorithm of Kerberos is symmetric, and public key techniques are not involved. A ticket is generated which allows A to re-use the ticket for multiple authentications to B without involving T.

In our approach, multiple authentications are not necessary. The heartbeat function allows the RG and LAP to communicate over long periods of time without requiring re-authentication. Once authentication is finished, the Card still keeps listening on a socket for an occasional "heartbeat" request from the LAP/Authentication server. So even if the card is whipped out without being able to send the "Disable Services" message to the RG (or if the RG has been

tampered with to ignore this message), the LAP will quickly realise the card is no longer in the RG, and thus will stop routing the RG's traffic.

9 Re-usability of the certificates and keys

In this section we give a few examples of how the certificates and keys can be reused for securing other functions of the TORRENT system, for user authentication, application security, eCommerce, etc.

As explained above, the customer behind the RG has a smartcard inserted in the RG. The smartcard contains at least one X.509 certificate and associated asymmetric keys. The certificate belongs to the customer and is linked to the

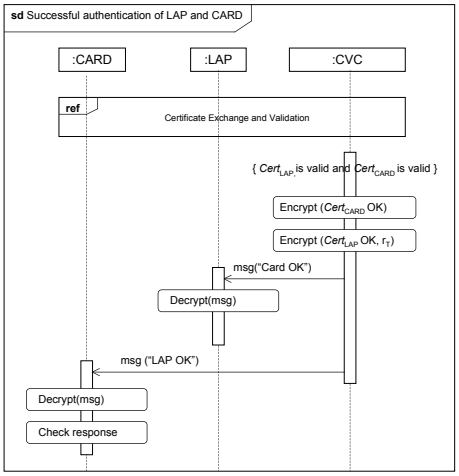

Fig. 4. Sequence for authentication process — normal operation

customer profile database. Depending on the certificate policy, the customer may have to present themselves in person to the CVC to register and receive the certificate and keys. The card and accompanying certificate(s) and keys may be used for authenticating the RG to the LAP, and for key exchange for setting up the IPsec VPN as a confidentiality service for securing the access link between the RG and the LAP [2]. Using Qualified Certificates the smartcard may even be fit for the purpose of creating electronic signatures [12] [17].

In the TORRENT system, a user interface can be used to select services and mark preferences. In its simplest form the user profile interface will contain a list of accessible services with options for the user to select preferred services and maximum tariffs. For some services different quality levels may be distinguished. The X.509 certificate may also be used for customer authentication at login time (through digital signature) e.g. so that the user can securely access their profile and make changes. If the changes made need to be signed, the user can also sign them electronically at this point, provided that the card contains a certificate that can be used for electronic signature. It can also be foreseen that pay-per-use services can be provided on this interface and that the user can provide an electronic signature for payment purposes. In current solutions, payment is bundled with PKI in a way that money may be transferred to a service provider (SP) without revealing the users bank or credit card account information to the SP.

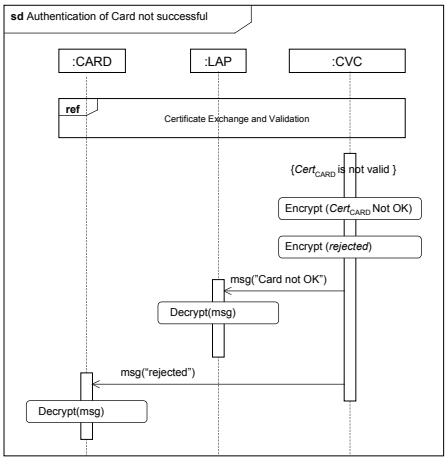

Fig. 5. Sequence for authentication process — invalid card

10 Conclusion

10.1 Discussion

In this research we focus on mutual authentication procedure between the customer's residential gateway and the Local Access Point using a proposed authentication protocol that combines techniques that are already proven to be reliable (X.509 certificates, smartcards, public key cryptography). The motivation comes from a requirement of the TORRENT IST project for a method of mutually authenticating a residential gateway (in the home) and a local access point (in the operator's premises). Bearing in mind that with future multi-service residential access networks, users may have — or demand — the facility to choose between several network operators and service providers.

The authentication requirements of the different operators and providers can lead to a situation where the user has to keep track of several combinations of usernames and passwords which becomes much more difficult to manage as time progresses. The process described in this paper proposes a scheme in an attempt to solve these issues for the TORRENT project and other deployments of LAP/RG types of systems. The process can also be applied to authenthicate to, and access mobile access networks, e.g. for use in 3G and future networks where the smart card may be used for authentication to many services.

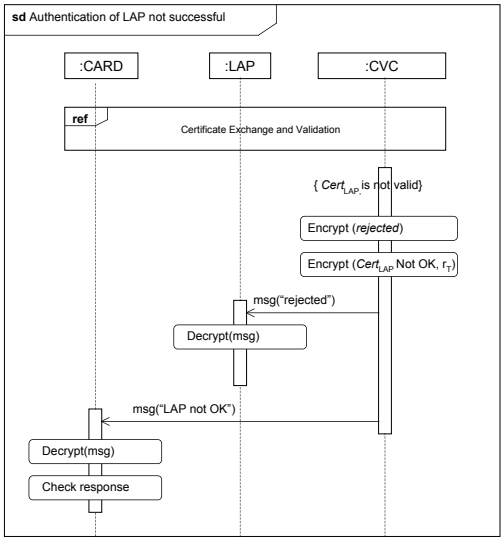

Fig. 6. Sequence for authentication process — invalid LAP

10.2 Related Work

Use of public key authentication and key exchange for network access has been studied in the IST-SHAMAN project [7] and two methods for achieving this are described. The protocol presented in this paper is different from those presented by SHAMAN. In the first method described in SHAMAN the mobile node has a subscription to a home operator, and must establish network access with an access network, which has an agreement with the home operator or a roaming broker. This network access point (e.g. LAP) has a number of pre-installed public key certificates (signed by each trusted third party or home network with which it has an agreement). The access network sends the appropriate one to the node (e.g. RG) and this is used by the node to assure the node that a roaming agreement exists with the home network. Our method does not require such an agreement, and pre-installation of home network operator certificates on the LAP is also not required. As the LAP operates in a multi-provider environment, this scheme could quickly lead to a situation for which the LAP is overloaded by certificate processing.

The second method described in SHAMAN differs also from our work in that it does not require client authentication. This method is concerned with providing anonymous access to the network based on immediate payment for services and therefore does not require authentication of the client. This method is purely concerned with authenticating the network.

The WLAN Smartcard Consortium, which was established in February 2003, is working towards defining specifications for world-wide access to WLAN net-

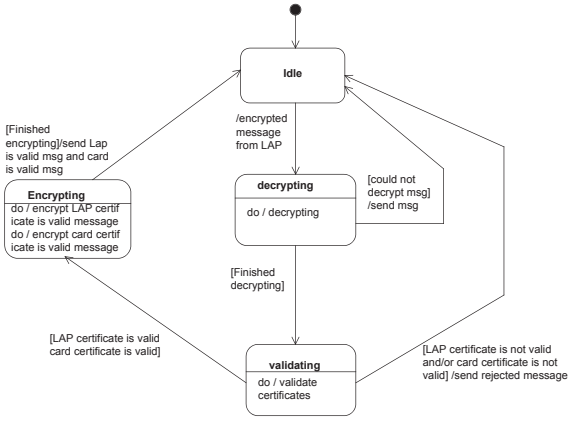

Fig. 7. CVC Authentication state graph

works using smartcard security in order to provide privacy, roaming and related capabilities. As this group is recently established, the specifications are not publicly available at this time. It is projected by the Consortium that they will be available by the end of the 2003.

Similarly, the ETSI AT NGNHome has announced plans for work on a deliverable entitled "Access and Terminals (AT); Home Area Networks and the support of Next Generation Services; Part 6: Security and Copyright issues" [9]. The intention is to outline the security and copyright (including Digital Rights Management and Privacy) issues related to the support and delivery of Next Generation Services and applications both to and within a Home Area Network.

10.3 Future Work

Future work will include schemes for using the Smartcard to gain secure access to a service at a chosen QoS class. Methods for protection of personal privacy will also be investigated. In the age of full IPv6 deployment, it is envisioned that protection of personal privacy can be made much easier. Today, with unlisted numbers, as soon as the number becomes known, it has to be changed. With IPv6, and certificates, IP addresses can be public, but the certificate, coupled with public key techniques, can be used to govern what traffic is allowed in, and what traffic should be prohibited. Only users with approved certificates can reach (and communicate with the user at) the destination IP address.

References

1. Menezes, A. J, P. C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Florida, 1997
2. Ronan J, Malone P, Ó Foghlú M, *Overhead Issues for Local Access Points in IPsec enabled VPNs*, IPS Workshop, Salzburg, February 2003. Retreived: 3. April, 2003 from `http://www.ist-intermon.org/workshop/papers/09_01_vpn-overhead.pdf`
3. Ølnes J, *Trusted Certificate Validation Services – Breaking the PKI Deadlock*, jon.olnes@validsign.com , `http://www.validsign.com`, 10. October 2002
4. Houmb, Siv Hilde. *Security Issues in FIPA Agents*, paper in progress.
5. Cert Advisory CA-2001-08, *Multiple Vulnerabilities in Alcatel ADSL Modems*, April 12 2001. Retreived: 3. April, 2003 from `http://www.cert.org/advisories/CA-2001-08.html`
6. Schlumberger, *Schlumberger Smart cards Cryptoflex Home Page*, Retreived: April 3, 2003 from `http://www.cryptoflex.com/index.html`
7. IST-SHAMAN Deliverable D09: *Detailed Technical Specification of Security for Heterogeneous Access*, June 2002
8. TORRENT (Technology for a Realistic End User Access Network Test-bed), IST-2000-25187. `http://www.torrent-innovations.org`
9. bleh `http://portal.etsi.org/Portal_Common/home.asp`
10. Neuman B C and Ts'o T, "Kerberos: An Authentication Service for Computer Networks", *IEEE Communications* **32**(9),*pp 33–38*. September 1994
11. Diffie W and Hellman M E, "New directions in cryptography", *IEEE Transactions on Information Theory* **22**(1976), *pp 644–654*
12. EU Directive 1999/93 on Electronic Signatures *ETSI TS 111 456 for Qualified Certificates*
13. Satoh T, Araki K, Miura S. "Overview of elliptic curve cryptography", *Proc. PKC'98*, LNCS **1431**,*pp. 29-49*, Springer-Verlag, 1998.
14. Gupta V, Gupta S and Chang S *Performance Analysis of Elliptic Curve Cryptography for SSL* ACM Workshop on Wireless Security (WiSe), Mobicom 2002, Atlanta, Georgia, USA September. 2002. Retrieved 10. June 2003 from `http://research.sun.com/projects/crypto/performance.pdf`
15. Aydos M, Yanık T, and Koç Ç, *An High-Speed ECC-based Wireless Authentication Protocol on an ARM Microprocessor*, Annual Computer Security Applications Conference, New Orleans, 2000. Retreived: 10. June, 2003 from `http://acsac.org/2000/papers/24.pdf`
16. Woodbury A, *Efficient Algorithms for Elliptic Curve Cryptosystems on Embedded Systems*, Worcester Polytechnic Institue, Massachusetts. Retrieved 10 June, 2003 from `http://www.wpi.edu/Pubs/ETD/Available/etd-1001101-195321/unrestricted/woodbury.pdf`.
17. Santesson S et al, *RFC 3039: Internet X.509 Public Key Infrastructure Qualified Certificates Profile*, January 2001. Retreived: April 3, 2003 from `http://www.ietf.org/rfc/rfc3039.txt`