





### Document Properties:

<b>Document Number:</b>	IST-2002-507134-AN/ WP7/D02
<b>Document Title:</b>	<b>Annex 5 - Non-repudiable billing protocol for subscription based access</b>
<b>Author(s)/editor(s):</b>	Mark Priestley
<b>Dissemination level<sup>1</sup>:</b>	PU
<b>Security Type:<sup>2</sup></b>	Public
<b>Status of the Document:</b>	Final
<b>Version</b>	1.0

### Table of Contents

1	Non-repudiable billing for dynamic roaming agreements.....	2
1.1	Problem description .....	2
1.2	Related State of the Art (SoA) research .....	2
1.2.1	Non-subscription based access.....	2
1.2.2	Non-repudiable billing.....	3
1.2.3	Hash chains.....	3
1.3	Solution.....	4
1.4	Protocol.....	4
1.4.1	Endorsement re-use .....	8
1.5	Evaluation .....	8
2	References.....	8

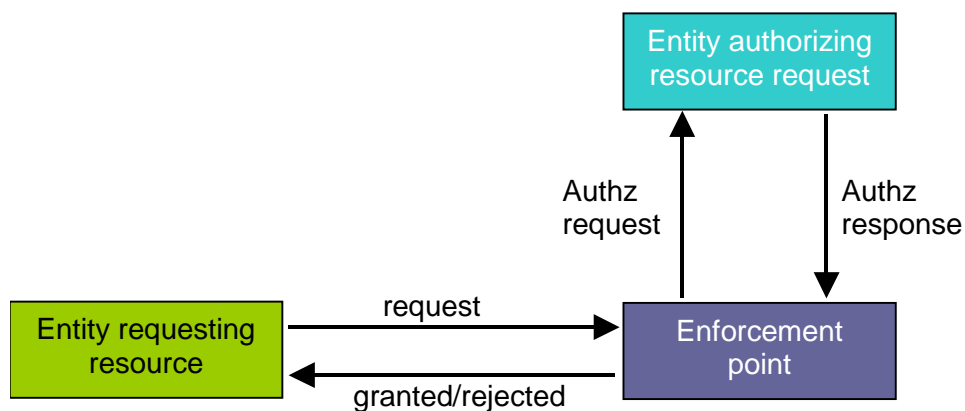
<sup>1</sup> Dissemination level as defined in the EU Contract:  
PU = Public  
PP = Distribution limited to 6<sup>th</sup> FP participants  
RE = Distribution to a group specified by the consortium  
CO = Confidential, only allowed for members of the consortium

<sup>2</sup>Security Type:  
Confidential Internal circulation within project (and Commission project Officer if requested)  
Restricted Restricted circulation defined in the document or dissemination level PP  
Internal With no confidential content but intended for internal use  
Public Public document

# 1 Non-repudiable billing for dynamic roaming agreements

## 1.1 Problem description

When two operators enter into a roaming agreement the Home Operator (the entity authorising resource request) must trust the Access Network Operator (the enforcement point) to provide them with accurate billing records for roaming traffic generated by a particular user (the entity requesting resource). Authentication and authorisation procedures are typically based on symmetric cryptography, due to their performance advantages over asymmetric cryptography in the mobile environment. Figure 1 shows the architecture and the respective entities:



**Figure 1: Three-party approach for subscription based access**

Between GSM networks today this trust is typically based on the belief that the potential disincentives associated with being caught providing incorrect or fraudulent billing records significantly outweigh any possible gains. No form of cryptographic evidence is used.

With the introduction of Dynamic Roaming Agreements [R7.5], which allow roaming agreements to be quickly and cheaply set up between operator ANs, it is not clear that the same disincentives will exist. For example, smaller operators may have less brand value to protect and/or roaming may not be a major part of the operators business.

To address this concern, report R7.5 [R7.5] outlined a protocol for providing non-repudiable cryptographic evidence of a Client's service usage. Section 1.5 provides an update to that proposal that aims to take advantage of the properties of the Network Attachment Protocol [R7.5]. Section 1.2 provides a brief summary of related state of the art research.

## 1.2 Related State of the Art (SoA) research

### 1.2.1 Non-subscription based access

The mechanisms that have been proposed for non-subscription based access, e.g. the ability to make direct non-repudiable payments<sup>3</sup> to a service provider, are not only of general interest to the Ambient Network project but also provide a good introduction to the issues relating to non-repudiable billing. An introduction to this work is provided in [R7.2].

<sup>3</sup> The payment might be in the form of a virtual currency that has to be cashed by the receiver



### 1.2.2 Non-repudiable billing

The mechanisms proposed to provide non-repudiable billing are closely related to the ideas of non subscription access. Both schemes typically use hash chains to provide non-repudiable evidence to service provider after an initial authentication and authorization phase with a trusted third party.

For example, in [ZHO98] a mechanism is proposed to provide a mechanism for undeniable billing when a user roams onto a visited network. The mechanism relies on digital signatures and hash chains. To ensure user anonymity, the user's home network generates a pair of temporary signature and verification keys, which are to be used as user's temporary identity, and issues to both the visited network and the user. The home network is responsible for mapping the user's permanent and temporary identities. The user then generates a hash chain and sends the hash chain anchor, signed with its temporary identity, and sends to the visited network as part of a service request. If the visited network can verify the signature on the service request, it acknowledges the request from the user. The user can release, at pre-defined intervals, the pre-images of the hash chain anchor to the visited network in order to receive services. The mechanism is extended to allow an undeniable meter to be set up, in which a single service request can be used for multiple instances of a service usage within a limited time period.

The ideas of proposal form the basis of the proposal described in section 1.3, however, there are a number of notable differences:

- The user's temporary identities are generated by the user device, reducing the amount of trust a user must place in their Home Operator<sup>4</sup>.
- No attempt is made to link the hash values to any monetary value to the user<sup>5</sup>. This allows non-linear relationships between the pricing schemes of the Inter-Operator tariffs and the user's subscription.
- The frequency at which the tokens must be presented by the user to the visited network is not determined by the user, but is instead communicated by the visited network (certified by the Home Network), allowing a simpler payment protocol between the visited and home networks.
- Mechanisms are proposed to re-use pre-endorsed tokens over multiple attachments.

### 1.2.3 Hash chains

For the readers convenience this section provides a brief outline of one-way hash chains. A one way hash chain is created by recursively applying a one-way hash function to an initial random seed value, e.g.  $H^i(x) = H(H^{i-1}(x))$ , where  $x$  is the initial random seed value,  $H(x)$  is a one way hash function of  $x$  and  $i = 1, 2, 3, \dots, n$  (where  $n$  is the length of the hash chain). Typically, the user then provides the service provider with whom they wish to use the hash chain with the hash chain anchor,  $H^n(x)$ , signed with their private key. If the signature can be verified by the service provider (or a trusted third party) and the service request is acknowledged, and the user can "pay" for a service by releasing pre-images of the hash chain anchor, at pre-defined intervals.

---

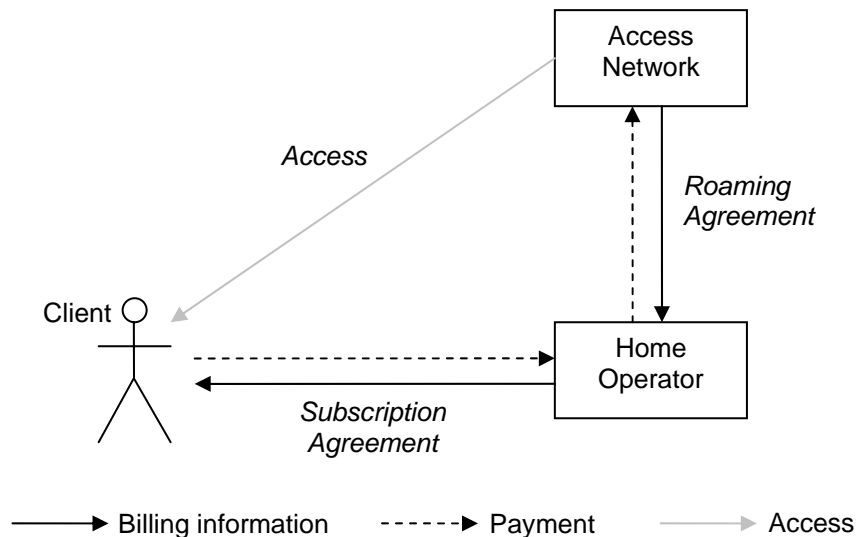
<sup>4</sup> Zhou describes a mechanism in which the user generates a permanent public private key pair to reduce the trust required in the home operator at the cost of untraceability to the visited network

<sup>5</sup> Zhou implies this in the proposal

Lamport first proposed the use of one-way hash chains for one-time password authentication [LAM81]. Subsequently, one-way hash chains have been used as a basic building block for source authentication in multicast groups, payment protocols and in many other security protocols.

### 1.3 Solution

The goal of the non-repudiable billing protocol is to provide an Access Network with cryptographic evidence that a particular client used a certain amount of service at a particular time. The Access Network can then present this evidence to the Client's Home operator when billing them for the Client's service usage.



**Figure 4: Roaming interactions related to compensation**

No attempt is made to link the service usage evidence to a monetary value relevant to the Client; instead the evidence is linked (implicitly) to the Inter-Operator Tariff (IOT) values that form part of the roaming agreement between the Operators. It is assumed that control of user credit and advice of charge are handled by separate mechanisms. The decision to de-couple the evidence of a Client's usage from the charge for that usage is based on the observation that the pricing structure in the subscription agreement between the Client and the Home Operator may be different to the IOTs in the Roaming Agreement between the Access Network Operator and the Home Operator. Without a linear relationship between these pricing strategies, designing a multi-purpose protocol introduces additional requirements that invariably result in inefficiencies.

### 1.4 Protocol

This section provides a sketch of a protocol proposed to allow non-repudiable billing between a Client AN, an Access AN (Access Network Operator) and a Home AN (Home Operator). The protocol builds on the Network Attachment Protocol (NAP) [R7.5]. As such, the reader should be aware of the following properties of the NAP:

- The Client AN generates an ephemeral cryptographic identifier ( $ID_C$ ) by applying a hash function to a self-generated public key. It uses  $ID_C$  in all communications with the



Access AN. The Access AN also uses a cryptographic identifier ( $ID_A$ ), which the Client AN can authenticate, e.g. it's certified by the Client AN's Home AN.

- A session identifier  $S$  is established between the Client AN and Access AN
- The Client AN and Access AN establish a secret key,  $g^{xy}$ , using Diffie Hellman key agreement protocol.
- In the roaming case, the Client AN is authorized to use the services of the Access AN through interaction with their Home AN. During this process the Home AN obtains the information necessary to link the temporary identity of the Client AN ( $ID_C$ ) to the Client's permanent identity. This is required to enable billing.

The following notation is used for the remainder of this document:

$e\{K, X\}$  =  $X$  encrypted with key  $K$

$m\{K, X\}$  = MAC function over content  $X$  using key  $K$

$v\{A, X\}$  = Signature of  $A$  over  $X$

One modification is made to the Network Attachment Protocol, the list of roaming services ( $R_A$ ) presented by the Access AN to the Client AN is extended to contain a time or volume based token release frequency ( $FR$ ) for each service ( $SV$ ). A service may have multiple token release frequencies, e.g. for different time periods or QoS, in order to allow support flexible pricing models, without requiring an explicit value to be attributed to a token endorsement. The roaming service list should also contain an indication of the allowable lifetime for an endorsement, the expiry value ( $E$ ). This value can also be used by the Client AN to estimate the length of the hash chain to use in the token endorsement request. The signature of the Access AN covers the entire message.

Client AN  $\leftarrow$  Access AN

$v\{ID_A, (ID_C, ID_A, S, e\{g^{xy}, R_A\})\}$

where  $R_A = ((SV_0(FR_0, FR_1, \dots, FR_n)), (SV_1(FR_0, FR_1, \dots, FR_n)) \dots (SV_n(FR_0, FR_1, \dots, FR_n)), E)$

This has the advantages of allowing the Client AN to create general use tokens, e.g. a token does not have to be linked to a particular service, time or QoS at the time of endorsement. It is noted that it is possible that all of this information could be pre-provisioned by the Home AN of Client AN.

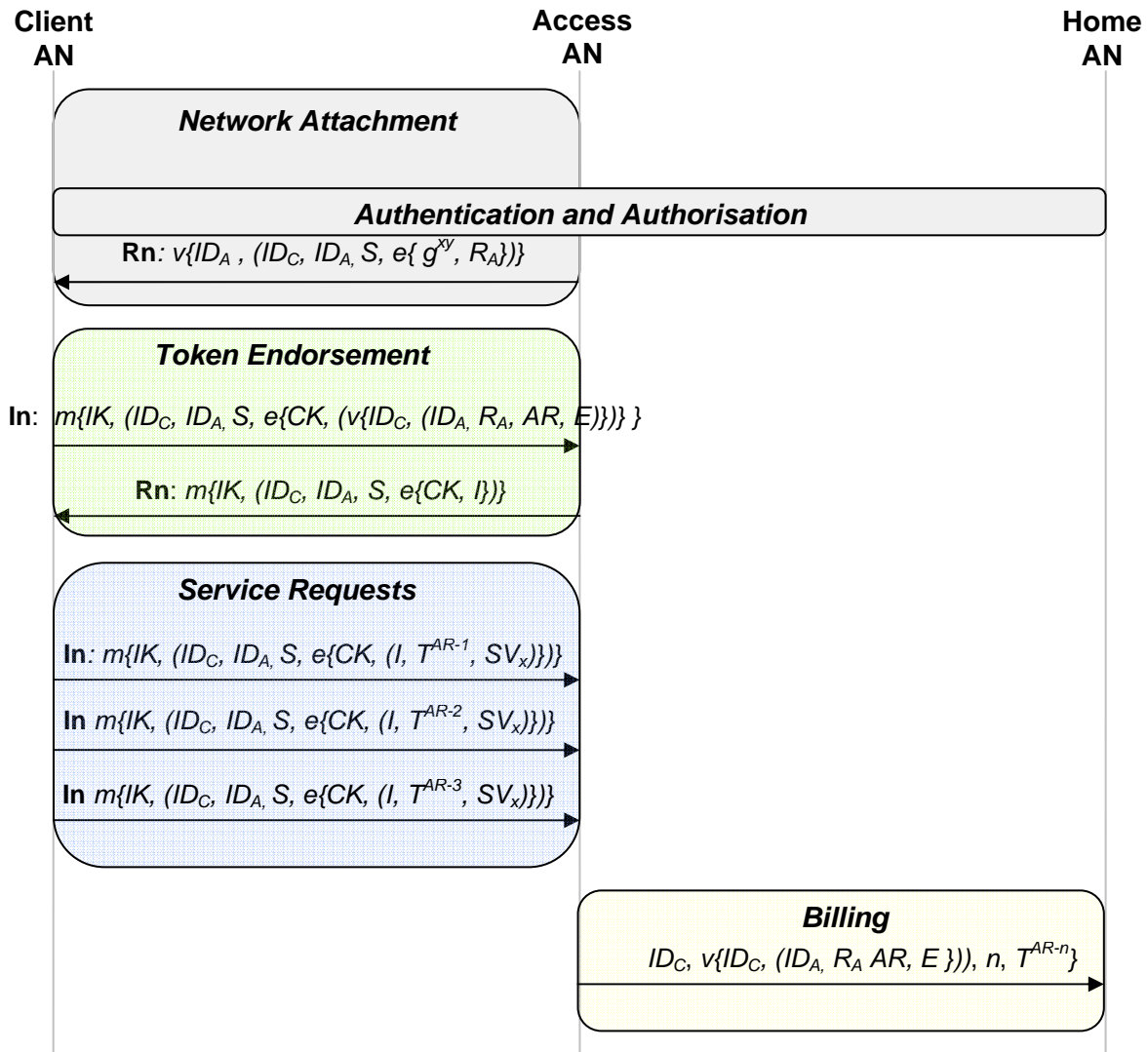
A Key Derivation function ( $KDF$ ) is used to derive a Cipher Key ( $CK$ ) and Integrity Key ( $IK$ ) from the secret key  $g^{xy}$ , established during the NAP, to be used between the Client AN and Access AN for the non-repudiation of billing protocol:

$KDF(g^{xy}) = (CK, IK)$

The creation of the  $IK$  also enables the use of a MAC function to protect the integrity of the messages between the Client AN and the Access AN, without requiring digital signatures. This is computationally cheaper and provides key separation. The derived keys ( $CK, IK$ ) are used throughout the protocol.

The reader should also note that there also needs to be a cryptographic binding between the keys used to encrypt the non-repudiation protocol and the key(s) used to protect the services

being accessed. Without such a binding, replay attacks are possible. This could be as simple as using  $CK$  for all services (including the non-repudiation protocol) or might require separate key derivations for each service. This is for further analysis.



**Figure 5: Protocol for non-repudiable billing**

*NB. Only the final message of the NAP is depicted. For the full protocol see [R7.5]. Messages between the Access AN and Home AN are secured using a previously established security association.*

Once the Client AN has received the roaming service list ( $R_A$ ) from the Access AN during the NAP, it generates a token endorsement request. This message contains; the cryptographic identifiers of the Client AN and Access AN ( $ID_C$  and  $ID_A$  respectively), the session identifier ( $S$ ), the list of services and token presentation frequencies presented by the Access AN ( $R_A$ ), the hash chain anchor ( $AR$ ) of a pre-generated hash chain (encrypted with the symmetric key  $CK$ ) and expiry time ( $E$ ). The MAC function ( $m\{\}$ ) covers the entire message to provide integrity protection.



Client AN → Access AN

**In:**  $m\{IK, (ID_C, ID_A, S, e\{CK, (v\{ID_C, (ID_A, R_A, AR, E)\})\})\}$

$R_A$  is included in this message to ensure that the Access AN has not changed the presentation frequencies agreed between itself and the Home AN in the message it presented to the Client AN<sup>6</sup>.  $ID_A$  is included in the payload of the message to stop the endorsement being “cashed” by any other Access AN to that which issued it. The lifetime of a token endorsement request indicated by the expiry value ( $E$ ) should be set to match the value provided by the Access AN in  $R_A$ .

On receiving the token endorsement request, the Access AN verifies its source and if satisfied replies to the Client AN with an acceptance message, which includes; the cryptographic identifiers of the Client AN and Access AN ( $ID_C$  and  $ID_A$  respectively), the session identifier ( $S$ ) and an identifier for the endorsement ( $I$ ) (encrypted with the symmetric key  $CK$ ). The MAC function ( $m\{\}$ ) covers the entire message to provide integrity protection.

Client AN ← Access AN

**Rn:**  $m\{IK, (ID_C, ID_A, S, e\{CK, I\})\}$

The identifier for the endorsement should be constructed such that it is unique to both the Client AN and the Access AN, e.g. it could be the result of a hash function over the concatenation of  $AR$  and  $ID_C$ .

When the Client AN wishes to use a service it sends a service request message to the Access AN. This message contains; the cryptographic identifiers of the Client AN and Access AN ( $ID_C$  and  $ID_A$  respectively), the session identifier ( $S$ ), the service ID ( $SV_x$ ) of the requested service, the endorsement identifier ( $I$ ) and the next token available in the endorsed hash chain ( $T^{AR-1}$  to  $T^{AR-L}$ , where  $L$  is the length of the hash chain). Symmetric key  $CK$  is used to encrypt the message payload. The MAC function ( $m\{\}$ ) covers the entire message to provide integrity protection.

Client AN → Access AN

**In:**  $m\{IK, (ID_C, ID_A, S, e\{CK, (I, T^{AR-1}, SV_x)\})\}$

When the Access AN wants to periodically receive payment for the roaming services that it has provided to the Client AN from the Home AN, it must submit the necessary evidence within the billing message. The billing message will therefore include; the Client identity ( $ID_C$ ), the token endorsement request provided by the Client AN ( $v\{ID_C, (ID_A, R_A, AR, E)\}$ ), the number of tokens used by the Client AN ( $n$ ), and the last token issued by the Client AN ( $T^{AR-n}$ ). This message should be protected using a pre-establish security association between the Access AN and the Home AN (not shown in notation).

---

<sup>6</sup> This information will be presented to the Home AN when the Access AN “cashes” the endorsement. If there is any discrepancy the Home AN can refuse payment.



Access AN → Home AN

**Billing:**  $ID_C, v\{ID_C, (ID_A, R_A, AR, E)\}, n, T^{AR-n}$

To verify the billing information the Home AN must:

- i.) Verify the signature of the Client AN over the token endorsement request.
- ii.) Check whether the billing information has been provided within the allowable period. This period should be set to be a certain period, e.g. 7 days, after the expiry value of the token endorsement request. This is required to mitigate against the possibility that the Access AN could generate the pre-images of the hash chain anchor provided by the Client AN and thereby create false billing records<sup>7</sup>.
- iii.) Verify the validity of the hash chain from the hash chain anchor included in the token endorsement request to the final token presented by the Client. The number of hash operations required to get from the hash chain anchor to the final token should equal the number of tokens claimed by the Access AN.

If all of these checks are satisfied the Home AN can be confident that the Client AN used a specific amount of service with a particular Access AN.

#### 1.4.1 Endorsement re-use

For efficiency a Client should be able to continue to use a previously endorsed set of tokens when re-attaching to an Access AN. If we assume a new run the NAP at re-attachment, where the Client uses a new alias ( $ID_{C2}$ ), in order to provide traceability protection against eavesdroppers, and where the new encryption and integrity keys ( $CK_2$  and  $IK_2$  respectively) are generated, the Client could prove ownership of the endorsed tokens to the Access AN by including the endorsement identifier ( $I$ ) signed using the private key of the identity that the endorsement was granted to ( $ID_{C1}$ ). The Access AN could then be confident that the Client is the owner of the endorsement (assuming that the Client AN is not able to distribute private keys). The reader should be aware that the benefits provided by the re-use of an endorsement come at the cost of losing the Client's untraceability towards the Access AN, as the Client now provides a link between their old and new identities.

Client AN → Access AN

**In:**  $m\{IK_2, ID_{C2}, ID_A, S, e\{CK_2, (v\{ID_{C1}, I\})\}\}$

## 1.5 Evaluation

The protocol described in this section provides a simple, lightweight and modular approach to providing non-repudiable evidence of service usage. The protocol is significantly more efficient than the protocol described in [R7.5] due to the decreased number of messages and public key encryptions required.

Further work is required to analyse the overheads generated by the protocol in comparison with other non-repudiation schemes.

## 2 References

---

<sup>7</sup> It is felt to be highly unlikely that this type of activity could be profitable for an Access AN if the value per token is relatively low.



**Document:** IST-2002-507134-AN/WP7/D02

**Date:** 2005-12-29

**Security:** Public

**Status:** Final

**Version:** 1.0

---

- [LAM81] "Password authentication with insecure communication", Leslie Lamport, Communications of the ACM, vol. 24, no. 11, November 1981.
- [R7.5] "Security Requirements, Concepts and Solutions for Secure Access and Mobility Procedures"; Georgiades, M. (Ed.); Ambient Networks WP7 report 5; September 2005; IST-2002-507134-AN/WP7/R005; (Annex 2 of D7.2).
- [TEW03] "Multiparty Micropayments for Ad Hoc Networks", Hitesh Tewari and Donal O'Mahony, Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '03) March 2003
- [ZHO98] Jianying Zhou and Kwok-Yan Lam. "Undeniable Billing in Mobile Communication" Proceedings of 4th ACM/IEEE International Conference on Mobile Computing and Networking, pages 284--290, Dallas, USA, October 1998, ACM Press.