Identity-Based Key Derivation Method for Low Delay Inter-domain Handover Re-authentication Service

Radu Lupu[1], Eugen Borcoci[1], and Tinku Rasheed[2]

[1] University Politehnica of Bucharest, Bucharest, Romania
{rlupu,eugen.borcoci}@elcom.pub.ro
[2] CREATE-NET, Povo, Italy
tinku.rasheed@create-net.org

Abstract. Several statistics on the factors of attacks' proliferation revealed the scarce deployment of entity authentication mechanisms being one of the most important. Particularly, providing seamless mobile re-authentication service for real-time inter-domain handover procedures is still an open issue. This paper is focused on the re-authentication architecture and mechanisms design, aiming to low latency re-authentication services for roaming WLAN or WiMAX terminals. Authentication architecture is specified to integrate the proposed mechanisms and a novel generic key material concept is defined in addition to the current state-of-the-art. An identity-based key material derivation method is developed, relying on the multiplicative group associativity property and the intractable underlying RSA problem. Then, the required cryptographic properties are evaluated. A simple generic key material pre-distribution mechanism is proposed and the related local re-authentication protocol. Eventually, the validation of the security properties of the re-authentication protocol, as well as the functional correctness validation of the re-authentication service is performed.

Keywords: entity authentication, key derivation, inter-domain handover, real-time.

1 Introduction

The pervasive and secure Internet real-time multimedia communications need enhanced design solutions for the mutual authentication mechanisms, capable to offer low latency operations (i.e. tens of milliseconds). This paper proposes a new solution designed[1] for real-time re-authentication service that could be integrated within the handover procedure of the roaming WLAN [1] and WiMAX [3] mobile devices. Even though considerable research work has been performed with notable results in this field of research [4, 5, 6, 7, 8], providing seamless real-time re-authentication service for inter-domain handover procedures is still an open issue. Both, reactive and proactive techniques have been employed in the design of the fast re-authentication solutions, relying on minimum one transaction crossing the Internet, either with the

[1] Within EU funded project Alicante IST 248652-IP.

P. Laud (Ed.): NordSec 2011, LNCS 7161, pp. 162–175, 2012.

previously visited domain, with the home domain, or with a trusted third party. The current reactive solutions have been optimized with respect to the number of transactions per re-authentication phase or per visited domain. In both cases, these solutions expose high latency (hundreds of milliseconds) which directly affects the real-time communications performances. It has been shown empirically [9] that 90% of the re-authentication delay is due to the communication over Internet. On the other side, the proposed proactive solutions have high complexity in terms of communication, processing operations and trust relationships. Moreover, if prediction techniques are employed to guess the mobile next target visiting network, the low latency guarantees are at most only statistic ones and come often with an important overhead. The complexity is mainly inherited from Public Key Infrastructure (PKI) management [10] and the asymmetric cryptographic mechanisms utilization. In addition, due the trust relationships they introduce part of the proactive solutions are sensible to the domino effect [11, 12].

Our solution also belongs to the proactive class due the key material pre-distribution procedure it employs. The key idea (to overcome the current state-of-the-art limitations) consists in re-authentication phase decoupling from key material distribution phase, through the use of a special key material derivation method. Furthermore, the scalable pre-distribution procedure design was possible to be achieved, due the definition of the generic key material concept and the adoption of the identity-based cryptographic techniques. However, the solution proposed in this paper is still compatible with the legacy related protocols (e.g. EAP, Radius, Diameter) and architectures [2].

The paper is organized as follows. In Section I, the motivation of this work is presented. Section II, outlines the main phases of the new re-authentication service; each phase is defined and its role is pointed out. Section III specifies the new local mutual re-authentication protocol offering guarantees for authentication service continuity. In Section IV, it is specified the key hierarchy design needed to implement our cryptographic mechanisms. Section V, introduces the concept of generic key material and defines the methods proposed for derivation of the generic key material, and for the re-authentication key. Also, the main design requirements are specified for our methods. In Section VI we specified the distribution protocol for provisioning of the generic key material to the local re-authentication server. Section VII presents the main activity and the related results, to prove the design correctness. Afterwards, we evaluated the performance of the re-authentication service to prove feasibility of our approach, in Section VIII. The paper ends with Section IX that concludes this work and points out the related directions for further research.

2 The Re-authentication Service Architecture

For the definition of our re-authentication service we focused on satisfaction of the following overall design requirements: compatibility with legacy technologies, mutual authentication, low overall re-authentication delay to the level acceptable by real-time communications, minimization of trust relationships and prevention of the domino

effect, low processing and communication complexity, resilience of the related mechanisms.

We chose to design the security architecture for our re-authentication service upon the HOKEY security model [13]. Thus, we will further assume the same type of principals with their roles and the related terminology, as specified by the standard. However, we will define new procedures of interaction between the principals and their related mechanisms. Figure 1, depicts the main phases of the re-authentication service we designed that are run according to HOKEY standard model. As it can be seen, our solution is made up of four distinct phases.

The "*Home Authentication*" relies on complete legacy Extensible Authentication Protocol (EAP) [14] with Master Session Key (MSK) and Extended MSK (EMSK) material establishment support, achieved according to IEEE 802.1x, in between mobile node MN (EAP supplicant role) and home AAA (H-AAA) (EAP authentication server role) via access point (AP) (EAP Authenticator role). In this case, foreign AAA (F-AAA) plays the AAA proxy role. Particularly, for our solution EMSK is assigned Mobile Specific – Root Key (MS-RK) alias and computed by the generic key material derivation function we designed with special properties which is defined in a separate section of the paper. In addition, H-AAA server assigns an index to the current MS-RK and conveys it to MN entity concatenated with MS-RK. In our solution, this phase is initiated by MN entity when it enters the access network for the first time (e.g. after reboot), as well as, whenever MN needs to refresh MS-RK.

For "*Local Re-authentication*" phase we designed a new mutual authentication protocol with support for session key establishment and augmented with mechanisms for checking MS-RK synchronization. It was dedicated a separate section in this paper for detailed specification of this protocol (see Section III). The related messages are exchanged according to HOKEY model in between MN (EAP supplicant), AP (EAP authenticator) and F-AAA (EAP re-authentication server). It is invoked periodically by MN to get its communication sessions reauthorized, whenever the local AAA server notifies support for it.

"*Local Authentication*" phase relies on legacy "4-way Handshake" protocol to achieve the goals as specified in [1]. It is initiated by AP (EAP Authenticator) subsequently to successful authentication of MN and H-AAA by "Home Authentication" or "Local Re-authentication" phase, respectively.

"*DS-RK (Domain Specific – Root Key) distribution*" is carried out through periodic secured transfer of the generic key material (DS-RK), from the home domain H-AAA (in key distribution center role) to each access network F-AAA it wants to enable for running "Local Authentication" phase with its mobile subscribers. The DS-RK derivation procedure with special properties and the related pre-distribution protocol we designed are defined in separate sections of the paper. Analogous to MS-RK, H-AAA server, also assigns an index to each DS-RK and conveys them concatenated to F-AAA entity.

The design of the procedures we propose is based on the underlying hybrid cryptographic techniques to facilitate performances and cost trade-off. In this regard, we involved in the design process the asymmetric techniques for less frequent operations, such as generic key material generation (i.e. MS-RK, DS-RK), and symmetric

techniques for more frequent operations, such as MN re-authentication, respectively. Due the new generic key material generation procedure with support for scalable pre-distribution, we enabled the overall re-authentication procedure latency for inter-domain handover scenario to be reduced to the values corresponding to the local legacy intra-domain authentication procedures. Moreover, for the certification of the DS-RK generic key material, that is transferred from H-AAA server to each F-AAA server, our solution relies on the pre-established trust relationships and the related SAs defined for the legacy AAA overlay [15]. This way, our solution completely avoids the costs entailed by the PKI management procedures, as well as, maintains the number of the trust relationships required at the same level as for the underlying AAA overlay.

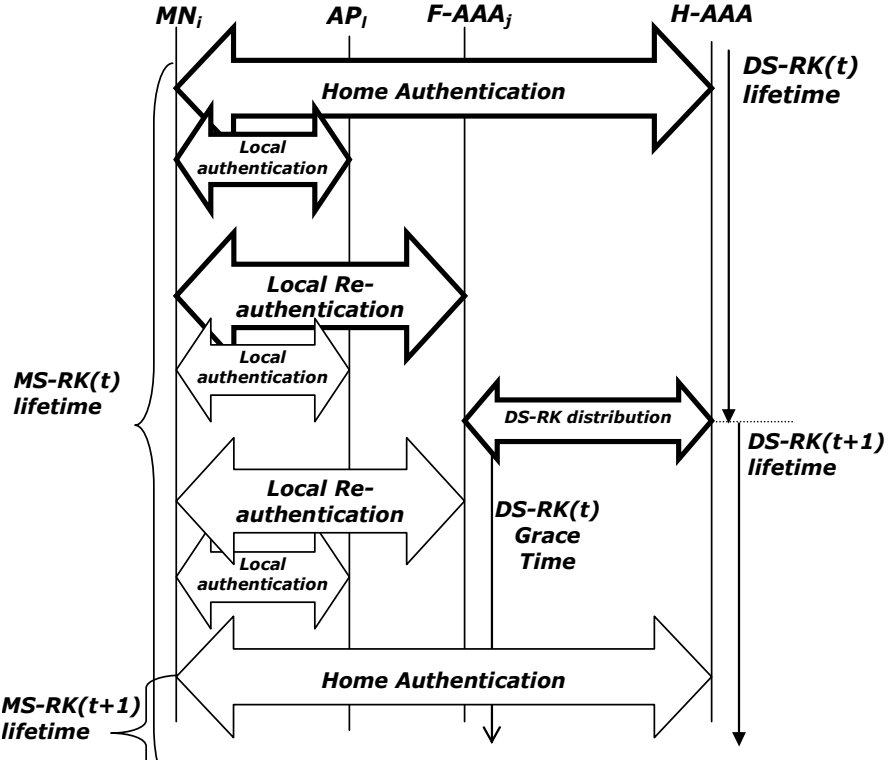

Fig. 1. The Re-authentication Service Workflow Design

The re-authentication key material generation method relies on the identity-based mechanism in order to enable scalable pre-distribution procedure and key usage control function. Moreover, it prevents the domino effect and allows the minimization of communication complexity in terms of the number of the messages exchanged. The robustness of our re-authentication service against interruptions experienced over the communication path with the home domain is enabled through the distribution of the

generic key material required prior to the re-authentication moment in conjunction with the delegation (according to HOKEY architecture) of the re-authentication server role from home to the homologous server from the potential visiting domains. Therefore, we expect our approach to be appropriate for networks with dynamic topologies where the multi-hop connectivity issues are mundane.

In the following sections we will focus on the specification of the mechanisms we designed for re-authentication service.

3 Enhanced Two-Key Re-authentication Protocol

In this section, we will specify a new entity re-authentication protocol for the low delay "Local Re-authentication" phase, which works in conjunction with the generic key material pre-distribution procedure we designed. This protocol aims to provide the following functionalities: mutual authentication of the principals, re-authentication key material synchronism verification and notification and session key establishment.

It is designed to run in between the mobile node (MN) and the local re-authentication server (F-AAA) on behalf of the visited access network. The specification of the protocol is achieved in the MSC diagram in Figure 2. It can be seen, that this protocol belongs to the class of "challenge-response" protocols with the nonces of type random number. The principals independently generate a nonce and exchange their values with the following goals: to prove the re-authentication messages are fresh, to contribute to the new session key generation in order to avoid session key control by the corresponding principal. Alternatively, a Diffie-Hellman technique could be used to achieve perfect forward secrecy property for the session keys. The yielded session key will be denoted further root MSK (rMSK) to highlight on its usage by the "Local Authentication" phase to produce traffic protection keys (i.e. PTK, GTK [1]). Optionally, the protocol messages should offer support to convey the principal's identifier (i.e. ID_{DS}, ID_{MS}) to the peer to enable the re-authentication key (rAK) derivation. Alternatively, there must be an independent reciprocal mechanism for the identification of the principals.

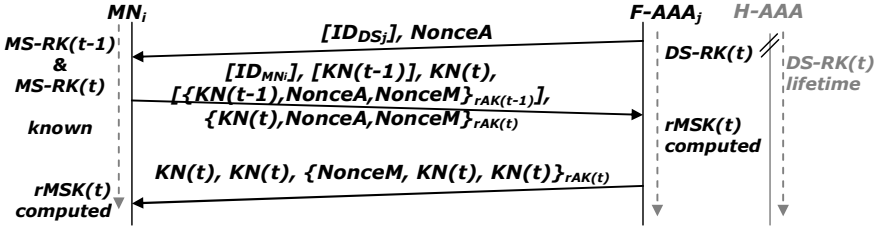

Fig. 2. The Two-Key Re-authentication Protocol with Key Sync Mechanism

To avoid the re-authentication service interruptions due the related system state inconsistence during the generic key material update, we designed the protocol to work simultaneously with two consecutive re-authentication keys, rAK(t-1) and rAK(t),

assigned to the time intervals (t-1) and (t), respectively. Note, the F-AAA server shall be able to work with the most recent two key materials DS-RK(t-1) and DS-RK(t) it has received from H-AAA. KN(.) denotes the generic key material index which is associated to rAK(.) for some time interval, to be used for generic key material synchronization in between MN and F-AAA server, as well as to point out which rAK(.) to be used for validation of the authentication token by the peer principal. If either of the authentication tokens in the second message {KN(t), NonceA, NonceM}rAK(t) or {KN(t-1), NonceA, NonceM}rAK(t-1) is valid, then F-AAA declares MN genuine. Where, the authentication tokens are computed through some MAC transform with the keys rAK(t) and rAK(t-1), respectively. On the other side, MN entity relies on the third message validity and the trust relationship shared by H-AAA and F-AAA to declare F-AAA is genuine. Regarding the structure of the last message, the first index KN(.) sent in clear points to the rAK(t) to be used by MN to check the authenticity of the message. The second index KN(.) notifies MN what is the most recent key material known by F-AAA (e.g. in Figure 2, the last message shows the key materials are synchronized. Therefore, the MN's generic key material is up to date). Whenever, MN finds out this way a new key material has been distributed, it enters "Home Authentication" phase in order to refresh its key material (i.e. MS-RK). Also, if none of the two key materials is valid, the re-authentication protocol fails and MN shall enter "Home Authentication" phase. The transmission of the last message in this case is optional, since its integrity cannot be verified, in order to prevent DoS attacks on the protocol.

4 The Key Hierarchy

Figure 3 depicts the key hierarchy we designed to allow the cryptographic-based re-authentication security service with required properties.

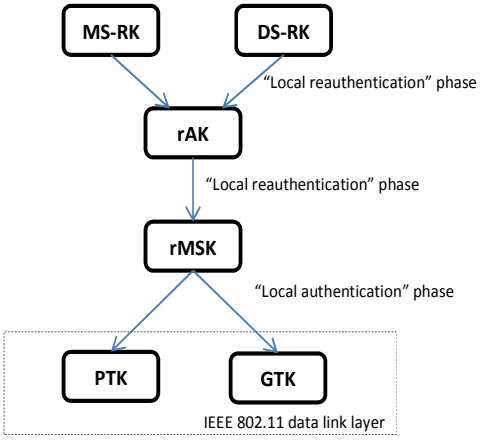

Fig. 3. The Design of the Key Hierarchy

We remark the whole hierarchy is derived starting from the two generic key materials MS-RK and DS-RK. For a given 3-tuple (MNi, F-AAAj, t), each principal shall be able to independently compute the same re-authentication symmetric key rAK(t) based on the key derivation mechanism we designed (specified within a separate section of this paper). Whenever, successful re-authentication of the principals is achieved, the master session key rMSK(t) is derived independently by principals according to the following formula:

$$rMSK(t) = hash(NonceA, NonceM, rAK(t)) .$$

Nevertheless, the properties of the hash function guarantee the potential correlations-based attacks mounted on several re-authentication keys are avoided. Thereafter, rMSK(t) is securely transported from F-AAA to authenticator (typically an access point) to enable "Local Authentication" phase. The derivation of the traffic encryption keys from rMSK(t) is out of the scope of our solution. For instance, in the case the MN's communications are run on top of the IEEE 802.11 link layer, the derivation of the (PTK, GTK) keys shall be accomplished according to the standard [1].

5 The Generic Key Material and Re-authentication Key Derivation

In this section we present the method we designed for the computation of the re-authentication symmetric key (rAK) with cryptographic guarantees, which enables scalable rAK pre-distribution procedures from H-AAA to each potential visiting F-AAA. Note, rAK shall be unique for each instance of the pair of principals which share this key (MN, F-AAA).

The key idea was to enable each principal to locally derive rAK "on-the-fly", at the visiting access network, from two components the generic key material uniquely assigned to the principal and the peer principal's identity. While the generic key material provides the authenticity for rAK and supplies the necessary entropy, the peer identity binds rAK to the current instance of the pair of principals. The generic key material is cryptographically bound to the corresponding principal through its construction, as well as totally decoupled from any of its potential peers. Due the last property the scalable generic key material pre-distribution it is feasible, before any tentative of re-authentication of the related principals.

The rAK derivation method was designed to satisfy the following overall cryptographic requirements:

(Req.1) the re-authentication key derived shall have high level of entropy;
(Req.2) the derivation method must have one-way property;
(Req.3) to guarantee both principals shall independently compute the same re-authentication key;
(Req.4) the key material owned by one principal can be used to compute neither the key material of any other principal nor the re-authentication key corresponding to another pair of principals

Besides, the generic key material shall be transported over a secure channel (with confidentiality and authenticity guarantees) from H-AAA principal to each potential F-AAA principal and MN principal.

The problem: For a given pair of principals, MN and F-AAA (on behalf of the visiting domain) we further denote the generic key material assigned with MS-RK and DS-RK, respectively. Also, we will denote with ID_{MN} the MN's identifier and with ID_{DS} the visiting domain identifier. Assuming the parameters RAND (i.e. a random number), ID_{MN}, ID_{DS} defined over Z_n, we had to research two functions f(.) and g(.), such that *(Req.3)* property holds on their composition, as follows:

$$f, g : Z_n \times Z_n \rightarrow Z_n .$$

$$f(g(RAND, ID_{DS}), ID_{MN}) = f(g(RAND, ID_{MN}), ID_{DS}) .$$

Furthermore, assigning to g(.) the generic key material computation role, and to f(.) the re-authentication key derivation role, we claim the following definitions:

$$MS\text{-}RK = g(RAND, ID_{MN}) \text{ and } DS\text{-}RK = g(RAND, ID_{DS})$$

$$rAK = f(MS\text{-}RK, ID_{DS}) = f(DS\text{-}RK, ID_{MN}) .$$

Within our work we considered two associative one-way functions f(.) and g(.) with the following definition:

$$g(x, y) = f(x, y) = x^{h(y) + A} \bmod n, \forall x \in Z_n \setminus \{0, 1\}, \forall y \in Z_n . \quad (1)$$

Where, n – it is a composite number hard to factor, defined in the same way as for RSA algorithm ($n = p*q$ with p, q – two big prime numbers, $p \neq q$).
The expression of the exponent has been figured out such that (R*eq.1*) and (*Req.4*) holds. In this regard, the constant value $A = 2^w$ has the role to shift the interval of values of the exponent, such that there are not factors of $\Phi(n)$ within its interval of values. Also, shall be assured that A is greater than the order of the set of y values that will be leveraged by this crypto scheme. On the other part, h(.) is the hash function with values within interval [0, a], where $a \leq A-1$ and greater than the order of the set of y values. It may be remarked that it is not necessary to have h(.) with one-way property.

Proof: It can be easily verified that property *(Req.3)* holds on (1):

$$f(g(x, y), z)=(x^{h(y)+A} \bmod n)^{h(z)+A} \bmod n=(x^{h(z)+A})^{h(y)+A} \bmod n=f(g(x, z), y) .$$

The deployment of this crypto scheme for re-authentication service introduced in Section II, requires the following initiation operations from the part of each H-AAA entity in the network. Independently, each H-AAA server has to establish the value of n, which will openly be shared with its mobile subscriber and F-AAA servers. H-AAA chose the value of a to be at least the number of mobile subscribers registered. Greater values of a are recommended to avoid too frequency updates. Afterward, H-AAA entity figures out the appropriate value of w. Eventually, the RAND

value is established randomly, then DS-RKs are computed and transferred together with n and A toward each F-AAA entity.

Security analysis of the re-authentication key

The security of the re-authentication key is guaranteed by the cryptographic properties stated previously as *(Req.1) … (Req.4)* and fulfilled through design of f(.) and g(.).

The entropy of the re-authentication keys is assured by the entropy of RAND value and the calculus of the powers of f(.) and g(.). The size of n shall be selected according to the security level required by the authentication service. It is expected at least a value of 1024 bits for n to be used.

The confidentiality is guaranteed by the security channel during the generic key material transfer between H-AAA and F-AAA. Moreover, the small subgroup attack on the confidentiality mounted by internal/external attacker is avoided through the condition on the powers of f(.) and g(.) to be prime with $\Phi(n)$. Also, the condition on the values of h(.) guarantees protection against internal attack in which one principal tries to compute another one keys through exponentiation of his keys. To note, that neither the size of hash value nor w does influence the confidentiality property. The one-way property guarantees the confidentiality of RAND, therefore precludes principals key computation and impersonation attacks launched by internal attackers.

The authenticity guarantee is provided by including of the identity information directly into the calculus of the generic key material and the re-authentication key.

The ID information is cryptographically bounded to the key based on the one-way property of the f(.) and g(.). This warranty together with the high-level of the entropy assures the yielded re-authentication key pair-wise uniqueness. To note, that the size of w does not influence the authenticity property. On the other part, the space of the hash values must be greater than the potential number of entities (mobile subscribers and AAA servers) in order to avoid yielded keys collision.

The strength of the one-way property of f(.) and g(.) is guaranteed by the complexity of solving the RSA underlying problem [16].

6 The DS-RK Generic Key Material Distribution Protocol

The main goal of this protocol is to proactively transport DS-RK together with the assigned index from H-AAA to each potential re-authentication server F-AAA. The operation of this protocol is illustrated in Figure 4. H-AAA is the only entity responsible with DS-RK update. A secured AAA protocol (e.g. secured RADIUS) may be used to push DS-RK encapsulated as AVP (Attribute Value Pair) digital object toward all F-AAAs with confidentiality and integrity guarantees. Note, DS-RK is specific for each F-AAA and is critical for real-time re-authentication of all MNs principals that administratively belongs to the same H-AAA. Besides, it is important to have DS-RK updated periodically. The exact period of time for DS-RK update could be a subject of further research. With respect to the security level needed by some application we

foresee the update period and the multiplicative group order tradeoff is achievable. We highlight here the time period to be at least the delay required for updating all F-AAAs (denoted with Δ in Figure 4). Moreover, to ensure re-authentication service continuity the DS-RK lifetime must be twice the update period.

In Figure 4, the moment (A) corresponds to the MN entry in the network, for instance after a reboot. It is now that MN applies "Home Authentication" phase and get MS-RK(t-1) from H-AAA. Afterward, MN is periodically re-authenticated through "Local Re-authentication" phase, based on the MS-RK(.) it knows. See the moment (B) related to such an event run in between MN and L-AAAj. At the moment (B), the MN is locally re-authenticated with MS-RK(t-1) and notified that a new generic key material was released (based on KN(t) index). Thereafter, MN initialize "Home Authentication" phase to get the new MS-RK(t), without interrupting MN's data transfer. Later, MN hands-off to another access network within jurisdiction of $L\text{-}AAA_l$. When MN tries to re-authenticate again at the moment (C), it will succeeds to do it locally based on the MS-RK(t). Then MN finds out that a new generic key material was released and proceeds further to get MS-RK(t+1), as previously mentioned without interrupting MN's data transfer.

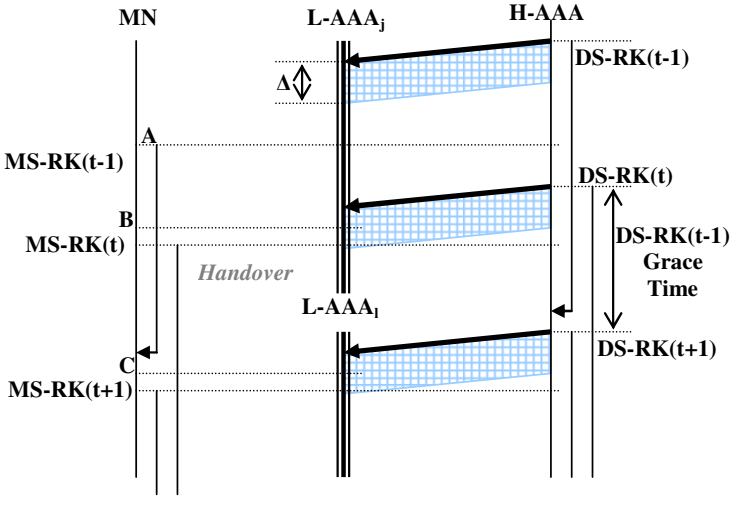

Fig. 4. DS-RK Material Distribution Protocol

We claim this method of update is scalable with communication complexity in O(N), where N represents the number of potential visited domains (i.e. F-AAAs) to update.

7 Validation of the Re-authentication Service Mechanisms

To prove the correctness of the re-authentication service our aim was twofold: to verify the security properties of the re-authentication protocol and to check the completeness and soundness of the whole re-authentication system with respect to the most representative scenarios. In this regard, we chose a simulation-based approach and settled intra/inter-domain handover conditions for several scenarios. To accomplish the first objective, we built-up the formal model of the re-authentication protocol using High-Level Protocol Specification Language (HLPSL) and used the AVISPA tool [17] for automated security properties verification against the generic Dolev-Yao attacker offensive [18]. We formalized the security requirements in terms of HLPSL authentication and confidentiality goals. The following HLPSL code shows the goals we specified within HLPSL mobile node module, identified here by M. The first two goals specify the requirement that rMSK_old and rMSK_new, corresponding to (t-1) and (t) key intervals respectively, are established with guarantees of confidentiality for the two principals. The following two goals specify the requirement that rAK_old and rAK_new, corresponding to the two successive key intervals remain secret after re-authentication protocol execution. The fifth goal, *witness(.)* together with the correspondent *request(.)* goal specified within the peer HLPSL module denoted here by A, claim the principal A shall be authenticated by the peer principal M, by means of NonceM. Analogously, the last goal together with the related *witness(.)* goal from the peer principal A are provided to assure the principals are mutually authenticated.

```
/\ secret (rMSK_old, ma_rmsk_old, {M, A})
/\ secret (rMSK_new, ma_rmsk_new, {M, A})
/\ secret (rAK_old, m_rak_old, {M})
/\ secret (rAK_new, m_rak_new, {M})
/\ witness (M, A, ma_nm, NonceM')
/\ request (M, A, ma_na, NonceA)
```

Thereafter, we achieved four optimized model-checking analyses by means of the following AVISPA's back-ends: On-the-fly model checker (OFMC), Constrain-Logic-based Attack Searcher (CL-AtSe), SAT-based Model Checker (SATMC) and Tree Automata-based analyzer for Security Protocols (TA4SP). All the analyzers' outcome was "SAFE", proving our re-authentication protocol fulfills the required security goals. More specifically, our protocol guarantees the secrecy of the session key and resilience against replay attacks.

On the other hand, we implemented the formal model of the re-authentication service mechanisms using Specification and Description Language (SDL) and specified the required liveness properties for the whole system. We stated initially the properties using Linear Temporal Logic (LTL) formulas, thereafter we had automatically translated them into a distinct Büchi automata [19, 20], each of which we eventually built-up the corresponding SDL model. For instance, a liveness property we verified was "all events of type new generic key material notification shall be pursued by 'Home authentication' phase", which we formally expressed upon the following LTL (negated) formula:

$$F((p->X(G\ (!q))) \&\&\ p)\ .$$

Where p, q denote here, the two boolean propositions in the sentence above. The verification of the re-authentication model against liveness properties was achieved on several scenarios (as previously mentioned) through the model-checking method implemented by IFx tool [21]. The model-checking process have been run over a three days interval on a computer configured with Debian, CPU Intel Pentium D, 3GHz, 2G RAM and 1.5G swap. At the end of the interval this process had been analyzed over 10 million of transitions and 4 millions of states, without error state being reached by Büchi automata. Based on the model-checking process outcome, we claim the re-authentication system satisfy the critical liveness properties we specified for the most representative scenarios.

8 Performance Evaluation

According to our architecture, the generic key material derivation transformation shall be run periodically by H-AAA server, while the re-authentication key derivation transformation is run by MN and F-AAA entities at the moment of first re-authentication that means when MN enters the new visiting network domain. Both derivation transformations have the same complexity in $O(|n|^2)$ multiplications, where $|n|$ represents the length of the modulus. We remark it has the same complexity as RSA encryption transformation, lesser than the RSA digital signing transformation in $O(|n|^3)$. Furthermore, to assure the derivation of the identity-based distinct key material for all subscribers, as fast as possible, a maximal length of 30 bits for the h(.) we estimate to be sufficient in the real world. To note, that our transformation is applied once per each generic key material or re-authentication key derived.

We remark the frequency the derivation transformation is run by the three architectural entities, follows the heuristic of asymmetry of the computational power distribution between network entities. Since it is expected the MN entity rarely roams the computational resources required by our solution are lesser than for the case of the traditional asymmetric mechanisms, such as the digital signatures based re-authentication protocols.

In order to evaluate how much our derivation transformation overloads the H-AAA and F-AAA servers, we measured its computation elapsed time to be roughly 190μs using sage toolkit [22] on the PC 32 bit architecture with CPU Pentium 4, 2.8 GHz, 1GB RAM.

We can observe that H-AAA server is overloaded periodically at the moment of the generic key material derivation for all the potential visiting domains. It yields that over a one hour period more than 18 billions generic key materials may be derived, which is far more than it is required in the real-world scenarios.

The F-AAA re-authentication server computational capacity is the most critical for the whole performance of our solution. In other words it determines the number of the roaming MN entities that could be handled with better performances than traditional solutions. For performance comparisons we assumed a 100ms time interval as reference, which roughly corresponds to one transaction delay over the Internet. Thus, we

figured out that roughly 500 roaming terminals per second could be re-authenticated at the performance claimed by our solution, which is more than required by real-world scenarios.

9 Conclusion and Future Work

This paper proposed several mechanisms designed to support development of the real-time re-authentication service for intra/inter-domain mobile WiFi and/or WiMAX terminals. Even though our solution was designed with the aim to be part of the access control service at the data-link OSI layer, the authors considers it could be easily adopted at the others OSI layers (e.g. network or application layer). Furthermore, our mechanisms are compatible with legacy (re-)authentication mechanisms (e.g. EAP, AAA, HOKEY). Although, several modifications of the EAP state machine work flow are necessary, e.g. to include the logic required to process the events associated to generic key material distribution and synchronization.

Upon the functional validation results we obtained so far, we claim that proposed identity-based key derivation methods, represents the promised paradigm enabling local re-authentication service operation with continuity guarantees even for roaming terminals. The performance evaluation we accomplished on the identity-based key derivation mechanisms shows they will succeeds on real world scenarios. Furthermore, our approach proved to be operational with better performances than other similar solutions, due the elimination of the transaction over the Internet whenever the mobile entity is re-authenticated. The scalable generic key material pre-distribution procedure design relies on the hybrid push-pull model with resilience to DoS attacks. Moreover, the generic key material and re-authentication key derivation transformations prove they fulfill the commonly required cryptographic properties.

Future work will be devoted by authors for implementation of the re-authentication service presented in this paper for further evaluation on the real-life testbed.

Acknowledgments. This work has been supported by the IST Program, Alicante project FP7 IST No. 248652-IP.

References

1. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11 (2007)
2. IEEE-SA Standards Board, Port-based Network Access Control, IEEE Std. 802.1x-2001 (2001) ISBN 0-7381-2626-7
3. IEEE-SA Standards Board, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems. Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE Std. 802.16e (2006)

4. Chen, J.J., Tseng, Y.C., Lee, H.W.: A Seamless Handoff Mechanism for IEEE 802.11 WLANs Supporting IEEE 802.11i Security Enhancements, http://www.cs.nctu.edu.tw/~yctseng/papers.pub/mobile79-handover-tunnel-apwcs2007.pdf
5. Lin, X., Ling, X., Zhu, H., Ho, P.H., Shen, X.: A novel localized authentication scheme in IEEE 802.11 based wireless mesh network. Intl. Journal Security and Networks 3(2) (2008)
6. Hong, Z., Rui, H., Man, Y.: A novel fast authentication method for mobile network access (2003), http://www.cnnic.net.cn/download/2003/11/27/142157.pdf
7. Calhoun, P., Montemurro, M., Stanley, D.: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification, IETF, RFC 5415 (2009)
8. Clancy, T.: Secure Handover in Enterprise WLANs: CAPWAP, HOKEY and 802.11r. IEEE Wireless Communications Journal 15(5) (2008)
9. Mishra, A., Shin, M., Arbaugh, W.: An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process. ACM SIGCOMM Computer Communication 3(2) (2003)
10. Long, M., Wu, C.-H., David Irwin, J.: Localized Authentication for Wireless LAN Internetwork Roaming. IEEE Communications 151(5) (2004)
11. Komarova, M.: Fast authentication and trust based access control in heterogeneous wireless networks, Ph.D. Thesis, Telecom-ParisTech (2008)
12. Huang, P.J., Tseng, Y.C.: A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks. In: Proc. of Vehicular Technology Conference, VTC 2006-Spring (2006)
13. The HOKEY working group documents homepage, http://datatraker.ietf.org/wg/hokey/
14. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP), IETF, RFC 3748 (2004), http://www.ietf.org/rfc/rfc3748.txt
15. Housley, R., Aboba, B.: Guidance for Authentication, Authorization and Accounting (AAA) Key Management, IETF, RFC 4962 (2007)
16. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of applied cryptography. CRC Press (1996)
17. AVISPA project website, http://www.avispa-project.org
18. Dolev, D., Yao, A.: On the security of Public-Key Protocols. IEEE Transactions on Information Theory 2(29) (1983)
19. Vardi, M.: An automata theoretic approach to LTL, http://www.cs.rice.edu/~vardi/papers/banff94rj.ps.gz
20. LTL2BA translator website, http://www.lsv.ens-cachan.fr/~gastin/lt2ba/index.php
21. IFx tool website, http://www-if.imag.fr
22. Sage Math, tool website http://www.sagemath.org