Mobile IP WG
INTERNET-DRAFT
Date: 23 February 2001
Expires: 23 August 2001

Franck Le
Stefano M. Faccin
Nokia Research Center

Temporary Shared Key Function for secure delegation of security to the local network

<draft-le-mobileip-sharedsecret-00.txt>

Status of This Memo

Abstract

When roaming to other domains, mobile nodes (clients) need to offer credentials to a local AAA server in order to be granted access to the local network. Security association may need to be set up between the mobile nodes and entities of the visited domain (e.g. between the MN and Home Agent when Home Agent is assigned in the visited network, or between the MN and Mobility Agents when extensions [1], [2] to Mobile IP are used). These security associations have a lifetime that when expired, needs to be refreshed. In addition, network operators need the ability to force a MN to provide authentication information anytime during a session.

The home network and/or the visited network need to have this capability. In the same way, the mobile node may want to challenge the network at any time e.g. to avoid man in the middle attacks. All these procedures require the involvement of the AAA-H since only the MN and the home domain share a long term key. This implies that several message round trips between the visited and home domains are needed to support the above mentioned authentication and key distribution procedures. This document introduces the concept of a MN specific Temporary Shared Key (TSK) between the AAA-L and MN, thus allowing authentication and key distribution control to be securely performed by the visited domain. In this way, the AAA-L can set up security associations to be shared between the MN and entities of the visited domain, and perform network and user entity authentication without having to involve the home network, yet, such procedures are performed securely because the user-specific Temporary Shared Key was created by the MN and the home domain.

1. Introduction

When roaming to other domains, mobile nodes (clients) need to offer credentials to a local AAA server in order to be granted access to the local network. Security association may need to be set up between the mobile nodes and entities of the visited domain (e.g. between the MN and Home agent when Home agent is assigned in the visited network, or between the MN and Mobility agent when extensions [1], [2] to Mobile IP are used). These security associations have lifetime and, when expired, need to be refreshed. The visited network may also want to authenticate the MN at any time and in the same way, the mobile node may want to challenge the network. All these procedures require the AAA-L to invoke the AAA-H in order to perform authentication and key distribution. In fact, only the MN and the home domain share a long term key that can support authentication of the MN or of the network, thus AAA-h needs to be involved. This implies that several message round trips between the visited and home domains are needed to support the above mentioned authentication procedures.

This document introduces the concept of a user-specific Temporary Shared Key (TSK) between the AAA-L and MN, thus allowing authentication and key distribution control to be securely performed by the visited domain. In this way, the AAA-L can set up security associations to be shared between the MN and entities of the visited domain, and perform network and user entity authentication without having to involve the home network of the MN but, at the same time, performing such procedures securely due to the fact that the user-specific TSK was created by the MN and the home domain.

In some cellular systems such as the ones built according to the IS-41 standards, concepts similar to the Temporary Shared Key Function had been defined. Such a function encompasses the processes by which the authentication center in the home network and the serving (visited) system manage the sharing of authentication responsibilities for a visiting MS. Temporary Shared Key (TSK)

sharing gives the visited system significant local control over the authentication of a visiting MS. Specifically, thanks to TSK, the visited system can control the following network functions without having to involve the Home network:

- set up of security keys between the mobile node and entities within the visited domain (key distribution)

- MN Authentication at any time

- Network authentication at any time.

The concept of Temporary Shared Key Function would enable the AAA-L to support user authentication, key distribution and network authentication without having to involve the AAA-H. This would allow for less round trips between the visited and home domains, thus reducing time delay and load over the network.

To allow TSK sharing between the MN and AAA-L, the MN and the AAA-L must have a common algorithm to compute authentication data and session keys. In case multiple algorithms are available, a negotiation needs to take place between MN and AAA-L to select one.

2. TSK sharing option

The TSK is optional and can be shared or not between the home domain and the visited domain depending on network policies and roaming agreements: In order to maximize the security, there may be cases in which the home domain will not be willing to share the TSK with the visited domain. This may happen when, as an example, the mobile node moves to a visited domain that the home domain does not trust sufficiently or with which the home domain does not have a roaming agreement covering the TSK mechanism. Also, there may be cases when the visited domain does not have an authentication and key distribution algorithm in common with the mobile node and thus the TSK cannot be used.

The TSK is a possible optimization to the security procedures in particularly considering the signaling involved between the Visited and the Home networks, but whether the Temporary Shared Key is provided to the Visited Domain depends on the Home network.

3. Definitions

Data Origin Authentication:

> Data Origin authentication is a type of authentication whereby a party is corroborated as the (original) source of specified data created at some tim in the past. Data origin authentication includes data integrity.

Entity Authentication:

> Entity authentication is the process allowing one party (the verifier) to gain assurances that the identity of another (the

> claimant) is as declared, thereby preventing impersonation.

Perfect forward Secrecy:

> A protocol is said to have perfect forward secrecy if compromise of long-term keys does not compromise past session keys.

4. Computation and Distribution of the TSK

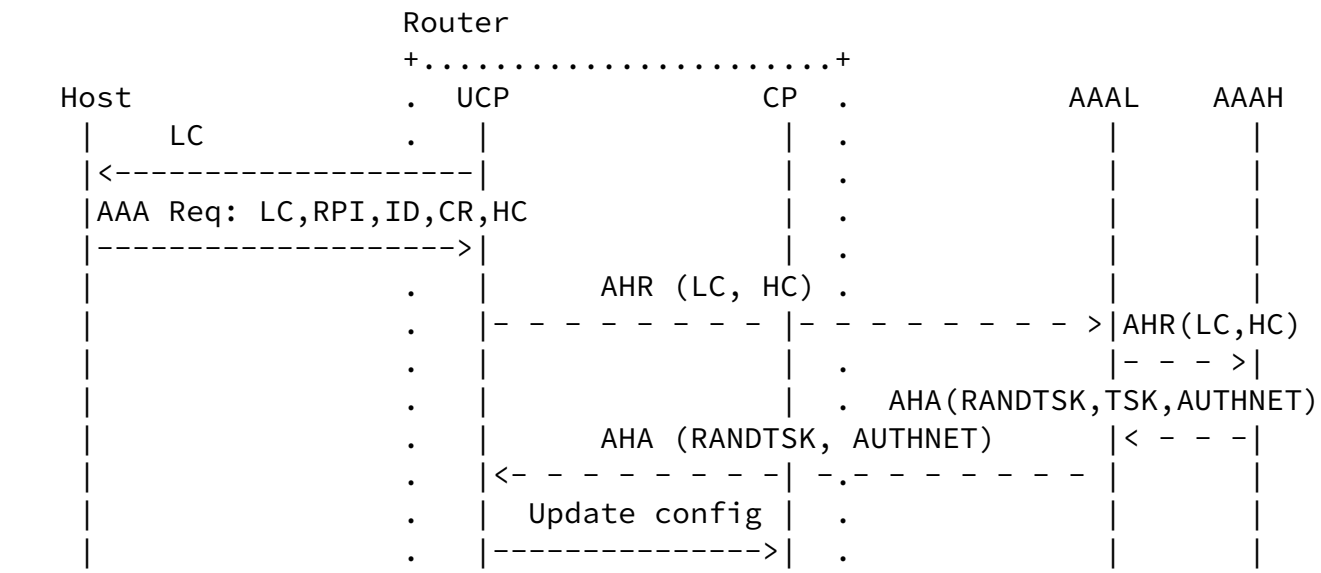
4.1. Initial Authentication and Initiation of Temporary Shared Key Function

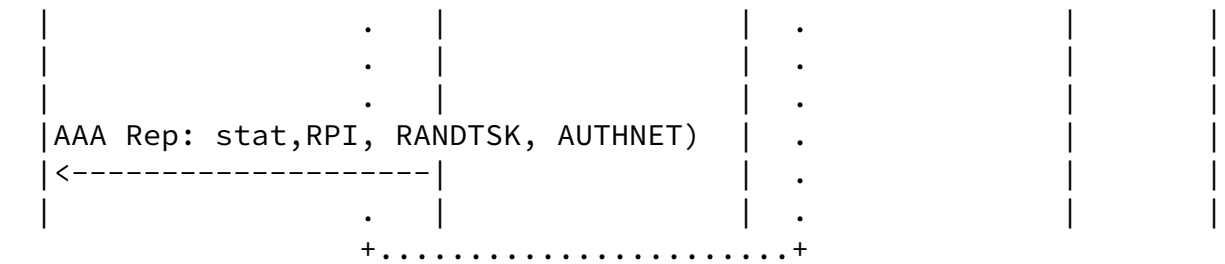
When the MN enters a new visited domain and first registers, its Home AAA server is invoked to verify the validity of the user and if the visited and home domains decide to use the Temporary Shared Key concept, the Temporary Shared Key must be updated and distributed.

It is opinion of the authors that the AAA-H SHOULD perform a Temporary Shared Key update process at least every time the MN is entering a new visited domain. Otherwise the pevious visited domain

has the value of the Temporary Shared Key and can act of behalf of the MN and perform undesirable things.

The Temporary Shared Key computation and distribution can be integrated to the entity authentication at the first registration as follow:





LC = Local AAA Challenge
HC = Host Challenge generated by the MN to authenticate the network
RPI = Replay Protection Indicator used between host and AAAH
CR = AAA Credential
ID = Client Identifier
AUTHNET = Authentication data computed by the network
UCP = Uncontrolled part
CP = Controlled part
AHR = AAA Host Request (using an AAA protocol)
AHA = AAA Host Answer (using an AAA protocol)

As described in [1] and [7], the MN uses the Local Challenge to compute some authentication data [1] and can derive some temporary ciphering and integrity protection keys from that Local Challenge and the long term key shared between the MN and its Home AAA server [7]. The MN also generates a Host challenge to require network authentication. Then the MN encrypts and integrity protects the message using the temporary security keys and leaving its Identity (e.g. the NAI) in cleartext.

The AAA-V forwards the message to the AAA-H including the Local Challenge. From the Local Challenge and the user specific shared

long-term key retrieved thanks to the user's NAI, the AAA-H derives the ciphering and integrity protection keys and decrypts the message.

It verifies the validity of the user, computes some network authentication data from the Host Challenge, and eventually generates some keying material. At that point, if the AAA-H and AAA-V decide to use the Temporary Ciphering Key, the AAA-H generates a new random number called the the RandomVariableTSK (RANDTSK) and executes the

algorithm shared with the MN using the long term shared key to compute the new "pending" TSK. The AAA-H sends the RANDTSK to the MN and sends the corresponding Temporary Shared Key to the AAA-V. The AAA-H can use the temporal keys to protect the response to the MN and uses inter AAA servers security to protect the message to the AAA-V.

The MN receiving the response, decrypts it using the Temporal Ciphering and Integrity protection keys, and verifies the authenticity of the network thanks to the network authentication data computed from the Host Challenge. If RANDTSK is provided to the MN, the MN derives, from the long term key and the common algorithm shared with its AAA-H server, the corresponding TSK to use for subsequent entity authentication and key distribution procedures.

The MN receives the RANDTSK in the message carrying the network authentication data and can therefore be sure that the information is coming from its Home network. In addition, RANDTSK is protected using the Temporal ciphering and integrity protection keys thus increasing the level of security.

The TSK is thus updated every time the MN is entering a new Domain but in addition, the Home network MUST be able to update the TSK at any time when the MN is in a visited domain and the TSK is shared: As an example, the TSK may get corrupted and the Home network MUST be able to revocate the TSK by performing a new TSK update.

In the following section the description of the procedures relevant for the TSK update while the MN is in a session is provided.

4.2. Temporary Shared Key Update

The Temporary Shared Key (TSK) Update function encompasses the processes by which the TSK in a MN is changed to a new value under the direction of the AAA-H. Only the AAA-H may initiate this operation when the TSK is shared with the serving system.

On the network side, a user authentication process could be executed immediately after the TSK Update to confirm that the target MN has successfully changed its TSK: the network sends a challenge to the MN

and based on the expected received authentication data that MUST be

from the TSK, the network cam make sure the TSK update had been successful and the MN is having the new TSK value. This would ensure that the MN will be able to authenticate itself and the network in the future.

On the MN side, the MN initiates a network authentication procedure when the MN is directed by the network to change its TSK. This authentication procedure allows the MN to authenticate the network issuing the TSK Update, thus preventing a fraudulent network from disrupting the normal network operation by forcing the MN's TSK out of alignment with the legitimate network TSK.

The TSK update includes AAA-H TSK update process and the serving system TSK update process.

4.2.1. AAA-H TSK update process

The AAA-H may initiate the TSK update process at any moment when the MN is in a visited domain and is sharing TSK. The decision on when the TSK is updated is based on home domain policies. TSK should not be changed too often, otherwise the benefits of TSK disappear. At the same time, TSK must have a lifetime to ensure that the same TSK is not used for too long. The first step in the TSK update process is for the AAA-H to execute the algorithm shared with the MN using the long term shared key and a random number, called the RandomVariableTSK (RANDTSK). The result is the new "pending" TSK.

The AAA-H then sends the RANDTSK and the new TSK to the AAA-L. The AAA-H then waits for a report from the AAA-L.

With the RANDTSK and the new TSK, the AAA-L can:

- update the TSK in the MN
- respond to the network authentication request from the MN
- verify the update by issuing a user specific authentication procedure to the MN

4.2.2. Serving system Temporary Shared Key update process

The serving system begins the TSKupdate process when it receives the RANDTSK parameter from the AAA-H. The message also contains either the new TSK Key.

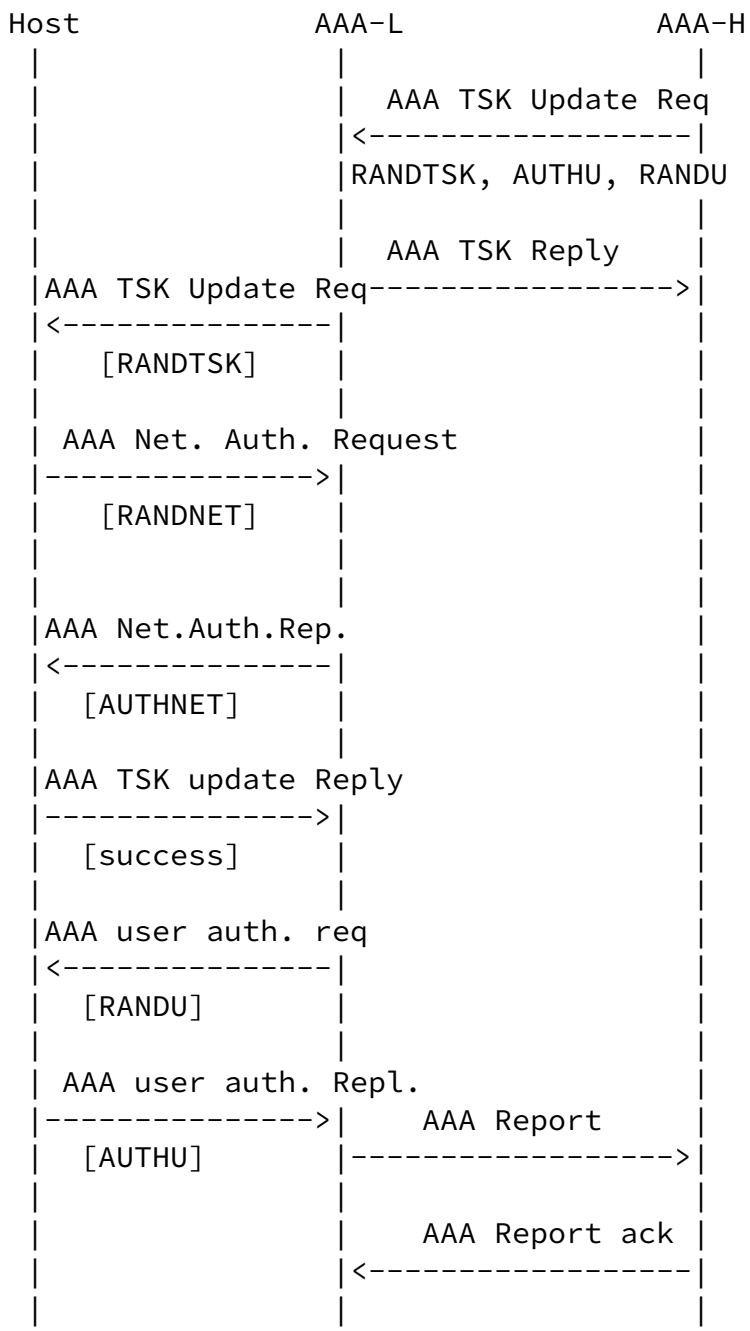
- The AAA-L directs the serving router to send a TSK Key update order, including RANDTSK, to the MN.

- The MN responds with a network authentication request including the challenge selected by the MN, RANDNET

- the AAA-L executes the shared algorithm using as inputs the MN's challenge RANDNET, and the new TSK. The result of the calculation is AUTHNET which is sent to the MN.

- Depending if AUTHNET equals to the expected corresponding result the MN indicates a successful or an unsuccessful TSKupdate in a message to the AAA-L

- If successful, the serving system executes the user specific authentication procedure; otherwise AAA-L reports the failure to the AAA-H.



5. Entity authentication and key distribution using the TSK

This section describes how the TSK sharing enables the Visited domain to perform entity authentication and key distribution without involving the home network thus reducing the time delay and the signaling between the two domains.

5.1. User authentication using TSK

Currently, as described in section 3.4 [3], the AAA credential is created by the client and is verified by AAA-H. The creation and verification is based on a long-term security association shared between the client and AAA-H. The credential SHOULD securely bind the following pieces of information:

- client identifier,
- local AAA challenge, if one was provided by the attendant, and
- depending on the style of replay protection being used between the host and AAAH, either a timestamp or a pair of challenges.

In specific instantiations, additional data may be included in the computation of the AAA Credential.

The exact algorithm used to compute the AAA Credential depends on the security association between the client and AAAH.

The authentication data is thus computed using a long-term key shared between the MN and the AAA-H, some other information and an algorithm.

When the TSK mechanism is used, the MN takes the same inputs but instead of using the long term key it shares with its AAA-H, the MN uses the TSK it shares with the AAA-L and the shared algorithm. The visited system having the TSK and the shared algorithm can then authenticate the MN without invoking its home network.

5.2. Network authentication using TSK

The MN may want to authenticate the network and thus use the Host Challenge to challenge the network. In such case, the MN expects a network authentication data computed by the AAA-H using the Host Challenge and currently, the long term shared key. The exact algorithm used to compute the AAA Credential depends on the security association between the client and AAAH.

If the TSK mechanism is used, the MN sends the Host Challenge to authenticate the network and the AAA-L applies the common algorithm to the Host Challenge and the TSK to compute the authentication data, i.e. the network authentication data.

Network authentication is thus provided without involving the AAA-H.

5.3. Key distribution using TSK

The key distribution (e.g. between the MN and HA when HA is assigned in the visited network, or between the MN and Mobility agent when extensions [1], [2] to Mobile IP are used) is usually based on the long-term security association between the MN and its AAA-H. This security association is used to create derivative security associations between the mobile node and other entities in the visited domain.

When TSK is shared, the MN receives the indication that TSK is to be used, and therefore the MN uses the TSK to compute the keys instead of the long-term key. In this way, since the AAA-L uses the temporary shared key as well, the keys will be available to MN and AAA-L and AAA-L does not need to involve the Home network in the procedures.

6. Comparison with existing earlier solutions

Previous Request For Comments and Internet Drafts documents specify extensions and suggest mechanisms to distribute the session keys to be shared between the mobile node and mobility agents. Those security associations are to provide data origin authentication of the Binding update and binding acknowledgement messages as required by Mobile IPv6.

But when the lifetime of these session keys expires, a new key distribution procedure (e.g. as defined in [4]) needs to be executed involving the home network. The message round trips between the serving and home domain imply time delays, and increase the load over the network. To avoid these issues, one possible solution seems to give longer lifetime to the session keys. But long lifetime session keys have higher risks to get compromised and thus, a key revocation procedure needs to be defined to solve this induced problem. Refreshing short-time keys is preferrable (same concepts are adopted in Kerberos [5] and in cellular networks) and the Temporary Shared Key mechanism enables to refresh short-time session keys without having to involve the Home network.

The Temporary Shared Key sharing is therefore an enhancement and optimization of the existing schemes.

In addition, the keys defined in current proposals are used to provide data origin authentication, but the home and the visited domain should be able to perform entity authentication for the mobile node based on challenge response based mechanism [6].

The Temporary Shared Key enables to perform that user entity authentication, and network entity authentication without involving the Home network.

7. Pros and Cons of the Temporary Shared Key sharing

The Temporary Shared Key sharing is a function enabling the serving system to securely perform entity authentication and key distribution functions with the MN on behalf of the home network but without having to involve the home network, thus saving round trips between the visited and home networks and reducing time delay and network load.

This mechanism enables to provide strong network authentication such as challenge response based mechanism without having to involve the AAA-H.

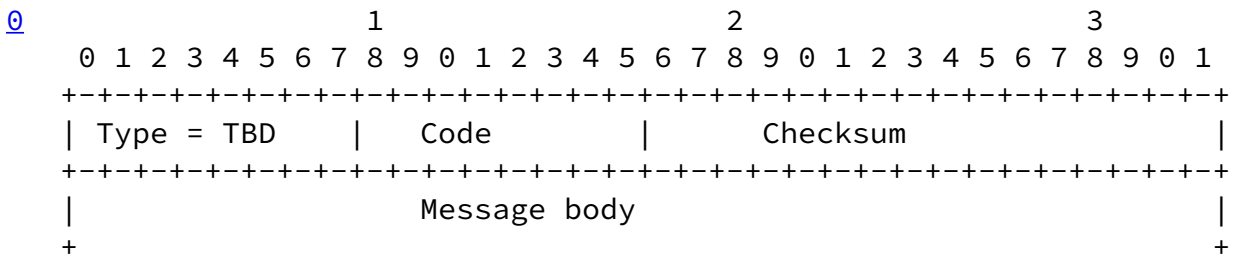
It is a possible optimization and the home and visited system can decide to use it or not based on policies and common agreements.

The only requirement of this Temporary Shared Key is to have a common algorithm between the MN and the AAA-L to perform authentication and key distribution.

8. Messages format

AAA Protocol messages

The Temporary Shared Key sharing requires new messages; they have the following general structure.



Type The following new types are defined:
AAA TSK Update Request: TBD
AAA TSK Update Reply: TBD
AAA Network Auth. Request: TBD
AAA Network auth. Reply: TBD
AAA User auth. Request: TBD
AAA User auth. Reply: TBD
AAA Report

Code The Code field depends on the message type.
- AAA TSK Update Reply

SUCCESS: 0
FAILURE: 1
- For AAA Report
SUCCESS: 0
FAILURE: 1

These messages could be defined either as new ICMPv6 messages or as Destination Option to Mobile IPv6 between the MN and AAA-L and as DIAMETER messages between AAA-L and AAA-H.

9. Security Considerations

This document introduces the concept of securely delegating part of the security functions to the Visited domain to avoid delays in authentication and key distribution procedures and reduce signaling load between the visited and home Domains. The Temporary Shared Key mechanism is an optimization that AAA-L and AAA-H may decide to use or not based on policies and roaming agreements.

10. Intellectual Property Considerations

Nokia Corporation and/or its affiliates hereby declare that they are in conformity with Section 10 of RFC 2026. Nokia's contributions may contain one or more patents or patent applications. To the extent Nokia's contribution is adopted to the specification, Nokia undertakes to license patents technically necessary to implement the specification on fair, reasonable and nondiscriminatory terms based on reciprocity.

11. References

[1] Jari T. Malinen and Charles E. Perkins. Mobile IPv6 Regional Registrations. Internet Draft, Internet

Engineering Task Force, December 2000.

[2] Hesham Soliman, Claude Castelluccia, Karim El-Malki, and Ludovic Bellier. Hierarchical MIPv6 mobility management. Internet Draft, Internet Engineering Task Force, September, 2000.

[3] N. Asokan, Patrik Flykt, Charles E. Perkins and Thomas Eklund AAA for IPv6 Network Access. Internet Draft, Internet Engineering Task Force, January 2000.

[4] Charles E. Perkins and Pat R. Calhoun. AAA Registration Keys for Mobile IP. Internet Draft, Internet Engineering Task Force, January 2001.

[5] Clifford Neuman, John Kohl and Theodore Ts'o. The Kerberos Network Authentication Service (V5). Internet Draft, Internet Engineering Task Force, November 2000.

[6] Franck Le, Raj Patil and Stefano M. Faccin. Challenge-Response Authentication Request. Internet Draft, Internet Engineering Task Force, February 2001.

[7] Franck Le and Stefano M. FaccinKey distribution for Mobile IPv6. Internet Draft, Internet Engineering Task Force, February 2001.

12. Authors' Addresses

Franck Le
Nokia Research Center
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 374-1256
E-mail: franck.le@nokia.com

Stefano M. Faccin
Nokia Research Center
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 894-4994
E-mail: stefano.faccin@nokia.com

Table of Contents