Hierarchical Mobile IPv6 (HMIPv6) is a protocol that enhances Mobile IPv6 (MIPv6) with faster handovers. Neither HMIPv6 nor MIPv6 provides ways to authenticate roaming mobile nodes, although visited networks will need to check if mobile nodes can be authorized access. A solution is required before MIPv6 can be commonly deployed.

Mechanisms to integrate Mobile IPv4 and the Diameter protocol for authentication, authorization and accounting (AAA) have proved to be a useful solution for IPv4. However, a similar mechanism does not yet exist for IPv6. We therefore propose a modification to HMIPv6 to allow for authenticated access for IPv6 supported mobility. HMIPv6, as well as Diameter protocols, supports transportation of AAA information and extends MIPv6 with mobility anchor points.

Our proposed solution shows how different mechanisms for secure roaming can be united in an efficient, secure and scalable manner. Furthermore, since HMIPv6 is a protocol designed to reduce the delay and signaling overhead of MIPv6, our proposal represents a way to integrate fast handovers with authenticated and authorized access.
Contents

1 Introduction ............................................................................................................. 2

2 Background ............................................................................................................ 3
2.1 MIPv6 ............................................................................................................... 3
2.2 Hierarchical Mobile IPv6 (HMIPv6) ............................................................... 4
2.3 Mobility and AAA interactions ..................................................................... 5

3 Problem definition ............................................................................................... 7

4 Authenticated access for IPv6 mobility .............................................................. 8
4.1 Anchor points provided by HMIPv6 ............................................................. 8
4.2 HMIPv6 for AAA between MN and MAP ............................................... 8
4.3 Diameter for AAA between MAP and home domain .......................... 9
4.4 One RTT signaling delay by sequential registration ............................. 9
4.5 Challenge Response extension to MIPv6 ................................................. 10
4.6 Message extensions ..................................................................................... 11

5 Discussion .............................................................................................................. 13
5.1 Functionality with a hierarchy of MAPs .................................................. 13
5.2 Security Considerations ............................................................................. 13

6 Further Work ....................................................................................................... 15

7 Concluding Remarks .......................................................................................... 16

Significance for Telenor ......................................................................................... 17

References .............................................................................................................. 18
2 Background

2.1 MIPv6

A MIPv6 mobile node (MN) has a home address (Haddr) and a Home Agent (HA) on its home subnet [3]. While away, the MN obtains a care-of-address (CoA) on the visited network. It then registers the CoA with its HA by transmitting a Binding Update (BU), and the HA replies with a Binding Acknowledgement (BA). If the registration is successful, the HA will snoop packets destined for MN’s Haddr on its home subnet, and tunnel the packets to MN’s CoA.

MN decapsulates the tunneled packets and sends a BU to the source of the incoming packet flow. The source is hereafter referred to as a Correspondent Node (CN). The CN will reply with a BA and start source routing subsequent packets to MN’s Haddr via MN’s CoA. As a result of this route optimization, the packets are sent directly to MN, without taking the detour via MN’s HA.

However, before MN can send the BU to CN, CN must perform a return routability test on MN’s locations, i.e. to test if MN is reachable both via its HA on its home network and on the visited network. This is to eliminate a large number of security threats associated with route optimization. The MN initiates the test.

It should be noted that unlike for MIPv4, the MIPv6 architecture requires no Foreign Agent or other routers with MIPv6 capabilities in the visited network [4]. The lack of an anchor point for mobility management makes access control for mobile devices more difficult.
2.2 Hierarchical Mobile IPv6 (HMIPv6)

It is anticipated that a few protocols will be widely deployed to enhance MIPv6 with mechanisms for faster handovers [7] [8]. HMIPv6 is one of these proposals. The core of HMIPv6 is to introduce Mobility Anchor Points (MAPs) in networks that MIPv6-enabled nodes are visiting. A MAP mainly improves the handover speed but also helps reduce the amount of signaling related to mobility.

MIPv6 MNs discover MAPs as part of MIPv6 Neighbor Discovery, i.e. by means of MAP-options appended to ICMPv6 Router Advertisements (RAs) [7].

![Diagram](image)

*Figure 1* Example illustrating HMIPv6 architecture with MAPs. In this example the visited network has two MAPs; one is co-located with an access router (AR), while the other is not. The regional Care-of-Address (RCoA) is MN's address associated with its MAP, while the On-Link Care-of-address (LCoA) is MN's CoA on the access link.

MN may then register its CoA on the access link (LCoA) with a selected MAP by sending it a MIPv6 BU (Figure 1). In place of the Haddr in the BU, MN uses instead a Regional Care of Address (RCoA) that it has auto-configured from a prefix in the MAP-option. The MAP responds to the registration attempt by returning a MIPv6 BA. If the registration was accepted, the MAP will in large function like a regular MIPv6 HA and forward packets destined for MN's RCoA to MN's LCoA.

After successful MAP registration the MN sends a BU to its Home Agent (and possibly to other CNs), demanding to get packets forwarded to its RCoA (Figure 1). The MAP operations are completely transparent for CNs and the HA.

When MN moves locally to other subnets within the visited network, it may register a new LCoA by sending a new BU to the MAP. CNs and the HA, on the other hand, will not be affected by this local movement. Hence, handover time is reduced, because the MN does not have to signal all the way back to its HA and CNs when changing its local CoA.

It should be noted that HMIPv6 uses a parallel registration procedure: MN first sends a BU to the anchor point (i.e. the MAP), and after having received a successful BA, sends another BU directly to its HA (Figure 2). MIPv4, on the contrary, is based on sequential registration: The MN sends the registration request to the anchor point (i.e. the FA), which processes it and in turn forwards it further to the MIPv4 HA (Figure 3). Hence, MIPv4 uses only one common registration request to register with both the anchor point (FA) and the HA.
2.3 Mobility and AAA Interactions

AAA is a framework for delivering authentication authorization and accounting services across administrative domains [9] [10]. AAA is a key technology for commercial operations where subscribers are authenticated, authorized and accounted for the usage of the network service.

The Diameter protocol is expected to become the de-facto baseline protocol for conveying AAA related information between network elements requiring AAA services [11]. Specific applications use this protocol for delivering specific AAA services.

The “Mobile IPv4 Diameter Application” is one such application [12]. Its purpose is among others to authenticate mobile nodes and to distribute security associations (SAs) between mobile nodes and mobility nodes across administrative domains. This allows for a scalable secure framework for delivering mobile IP services across administrative domains.

As illustrated in figure 4, the MIPv4 Foreign Agent (FA) is the Diameter client that requests an authentication service from the AAA infrastructure (i.e. message 2). The MIPv4 registration is integrated with the authentication so that they are both realized in one step and by only one round-trip-time (RTT) of signaling between the visited and the home
networks (i.e. messages 3 and 6). This is possible since MIPv6 uses a sequential registration procedure (Figure 3). This procedure allows the FA to realize both mobility and AAA functions.

Although the MN is roaming, it only needs to maintain a Security Association (SA) with its home domain (i.e. SA1 of Figure 5). By ‘home domain’ we refer to the administrative domain of MN’s home network. If a visited domain (i.e. the administrative domain of the network the roaming MN is visiting) is a roaming partner to the home domain, the two domains share an SA (i.e. SA3 of Figure 5). By combining these two SAs, the visited domain and MN may establish a trust relationship that allows the MN to be granted access to the visited network.

![Diagram](image)

**Figure 5** Established security associations of the Diameter architecture. The SA1 and SA3 can be used to establish trust between MN and the visited domain.

The SAs between a AAA server (i.e. AAAf or AAAh) and other nodes in the supported network (i.e. SA2 and SA4 of Figure 5) are targeted at the specific Diameter application. Hence, only one SA (i.e. SA3 of Figure 5) needs to be realized between the two domains, and this SA can be reused for a number of other Diameter applications. As such, Diameter provides a framework that scales well to a large number of applications that require inter-domain security associations.

In this paper we show how this model can be extended to HMIPv6.
3 Problem definition

In a MIPv6 enabled environment protected by AAA mechanisms, users might be authorized access to visited networks if there is a roaming agreement in place between the home and the visited domain. Policy and key information will normally be centralized in the home domain, because distributing such information would not scale well to a large number of visited domains.

This requires that there are dedicated nodes in the two domains assigned to the task of handling the authentication and authorization messaging between the visited domain and home domain. In IPv4, it can be handled by the MIPv4 FA as anchor point in the visited domain, and the home agent or a AAA server in the home domain. Such a solution is not possible for MIPv6, since MIPv6 does not have a corresponding anchor point.

![Diagram](image)

*Figure 6  AAA requires an anchor point for the authentication process in the visited domain.*

Furthermore, given that there exists a natural anchor point for the authentication process in the visited domain, some protocols are required to carry authentication messages between the MN and the anchor-point (1 - (Figure 6)). A protocol is also needed to carry AAA messages between the anchor point and the home domain (2, 3 - (Figure 6)).

Authentication also adds to the total signaling delay. Before the MN can register with its home agent, the visited domain needs to check with the home domain to find out whether the MN can be granted access to the visited network (4, 5 - (Figure 6)). As a result, it takes at least two Round-Trip-Times worth of signaling between the visited and the home domains before MN can start receiving packets: One RTT is required to check MN’s credentials with the home domain, and a second RTT is needed for registration with the HA. To speed up this time-critical process, Mobility and AAA should instead be integrated to achieve only one RTT worth of signaling between the visited and home networks.

An additional drawback of not integrating AAA and mobility is that MN needs to maintain two SAs. One SA is required for authentication with the authentication server in the home domain. Another SA is required for mobility management, i.e. to protect BUs sent to the HA.

In summary, mobility and AAA should be integrated to achieve better registration latency as well as higher scalability of the security architecture. This integration requires an anchor point in the visited domain, as well as protocols to carry AAA messages between MN and the anchor point, and between the anchor point and the home domain.
4 Authenticated access for IPv6 mobility

4.1 Anchor points provided by HMIPv6

It is here proposed to use HMIPv6 as a tool to integrate MIPv6 with AAA. HMIPv6 extends MIPv6 by introducing MAPs as anchor points in the visited network. With HMIPv6 as a basis for integration of IPv6 mobility and AAA, it would be natural to let MN's attempt to register with a MAP to trigger the authentication and authorization messaging (Figure 7).

![Figure 7 Using an HMIPv6 MAP as an authentication anchor point in the visited domain.]

4.2 HMIPv6 for AAA between MN and MAP

Furthermore, it is also proposed to use HMIPv6 as the protocol to carry authentication information between the MN and the anchor point. Hence, message 1 and 4 of (Figure 7) can be integrated into one common message, as illustrated for message 1 of (Figure 8). This requires extensions to HMIPv6 messages to be realized.

![Figure 8 Using an HMIPv6 to carry authentication messages between the MN and the MAP, and using Diameter to carry AAA messages between visited and home domains.]
4.3 Diameter for AAA between MAP and home domain

The next step will be to transfer the necessary authentication information from the anchor point to the home domain. HMIPv6 does not provide a protocol that can carry AAA messaging between the anchor point (MAP) and the home domain (HA), as HMIPv6 is based on parallel registration (Figure 2).

The main reason for the parallel registration procedure of HMIPv6 is that the signaling between MN and HA follows the MIPv6 specification. Hence, the home agent does not need to be aware that MN uses HMIPv6, and the MIPv6 specification—which has taken years to develop—does not need to be changed to accommodate HMIPv6.

Instead, we propose to use Diameter as a protocol to carry AAA information between the anchor point and the authentication server in the home domain (Figure 8). An advantage of this proposal is that MN only needs to maintain one SA with the home domain. The same SA can also be used by other applications that require inter-domain SAs between the visited and the home domain.

Only some extensions to Diameter messages are required to make Diameter applicable to HMIPv6. Hence, authentication messages are carried over a AAA infrastructure, rather than being carried directly between different MAPs and the authentication server in the home domain (Figure 8).

4.4 One RTT signalling delay by sequential registration

Despite parallel registration of HMIPv6, MN is not permitted to send BUs to the MAP and HA simultaneously to speed up the registration process. This is to avoid that HA starts forwarding MN’s packets erroneously to the MAP if the BUha results in a successful registration by the HA, while the BUmap registration fails at the MAP (Figure 2). Instead, HMIPv6 mandates that an MN wait for a successful response from the MAP (BAmapping) before starting the registration with the HA (BUha), leading to two RTTs worth of signaling delay.

Authenticating and registering simultaneously would be even more difficult with AAA in place. The MAP will need to get acceptance from the home domain before the visited domain will grant MN access through external networks. Hence, the MN must complete the authentication procedure before it can register with its home agent (4, 5—Figure 6).

To solve the problem of two RTT’s worth of signaling delay, it is here proposed a sequential registration procedure for HMIPv6, in which the MN node piggybacks its BUha onto the registration message sent to the MAP. Since BUha now is under the control of the MAP, it can safely forward the BUha to MN’s home domain without granting the MN general access to external networks.

![Figure 9](image)

*Figure 9* A fully integrated solution for mobility and AAA. It results in a delay of only one round-trip-time between visited and home domain.
The MAP sends the BU_{ha} over Diameter to AAAh in the home domain together with other authentication information (2-3, (Figure 9)). Since AAAh manages security associations between MN and the home domain, it integrity checks and decrypts BU_{ha} after having successfully authenticated the MN.

Since AAAh also has a security association with HA, it now performs the registration procedure with HA on behalf of the MN (4, (Figure 9)). AAAh constructs a BU_{ha} that will result in the same registration by MN’s HA, as the BU_{ha} would give. Hence, MN’s RCoA must be included in the Alternate-Care-of-Address option of BU_{ha} to tell HA that MN’s new care-of-address is different from the source address of the BU_{ha}. BU_{ha} is securely protected by IPSec and the security association between AAAh and HA.

HA processes the BU_{ha} according to the MIPv6 specification, and returns an appropriate BA_{ha} to the source address of the BU_{ha} (5, Figure 9). When AAAh receives the BA_{ha}, it reconstructs a BU_{ha} as a response to the BU_{ha} sent by the MN, and forwards this together with the authentication result back towards the MN along the AAA infrastructure (6-8, (Figure 9)).

Note that the sequential registration builds upon the concept of Mobile IPv4 Diameter application where the Foreign Agent acts as an access control point as well as a mobility manager.

4.5 Challenge Response extension to MIPv6

The most common authentication mechanism for MIPv4 is Challenge/response [5]. The same mechanism might be used for the HMIPv6 Diameter application proposed in this paper. Hence, the anchor point (i.e. the FA in case of MIPv4 or the MAP in case of HMIPv6) provides MN with a challenge on behalf of the home agent through an extension to a Router Advertisement (RA). The MN hashes the challenge with a secret key shared with the home domain, and sends the challenge together with the hashed result over to the home domain via the anchor point. If the anchor point can verify that the challenge is of a value that it recently has issued, it allows the challenge to pass, and awaits the result from the home domain.

To realize this, HMIPv6 BUUs must allow a challenge/response extension to be added to carry the challenge together with the MN’s response to the MAP, and HA’s authentication and authorization result back to the MAP. This is illustrated in message 2 and 9 of (Figure 10).

![Figure 10 Using challenge/response as an authentication method, and HMIPv6 and Diameter to carry authentication.](image)

Furthermore, HMIPv6 must be extended to allow a challenge extension to be included for each MAP address in IPv6 RAs, as illustrated by message 1 of (Figure 10). HMIPv6 already mandates that ARs include MAP options in neighbor discovery messages in order...
to advertise information about MAPs to roaming nodes on the visited link. Hence, HMPv6 requires that MAPs and ARs are coordinated, and there are several different ways to achieve this [7]. As part of this coordination, MAPs should also have a means to convey challenges to ARs. As challenges are updated frequently, a challenge/response authentication scheme for HMPv6 might require more frequent synchronization between ARs and MAPs.

4.6 Message extensions

Sequential registration means that MN must include all BUs and authentication information into one message that it sends to the selected MAP (Figure 9). Since HMPv6 is chosen as a carrier for this message, the message should be sent like an HMPv6 BU_{map} with additional information appended in appropriated message options. The authentication information would naturally be added in a separate option, while the BU_{ba} intended to register with the HA could be added in another. This message construct is described in (1).

\[ \text{BU}_{map} \text{ [Auth.]^{option} [BU_{ba}]^{option}} \]  

(1)

The MAP receives and processes the BU_{map}. If it cannot accept the RCoA that the MN has auto-configured, it returns a negative BA_{map} that terminates the registration process. Otherwise, the visited domain must contact the home domain to authenticate the MN and to verify that it is authorized access to the visited network before the MAP can return a successful BA_{map} to the MN. Hence, the MAP wraps the authentication information and the BU_{ba} into appropriate attribute-value-pairs (AVP) defined for the Diameter HMPv6 application. Hence, the Diameter AVPs will be as described in (2).

\[ \text{[Auth.]^{AVP} [BU_{ba}]^{AVP}} \]  

(2)

After AAAa has successfully authenticated the MN, the HMPv6 module of AAAa processes the BU_{ba}, and sends a corresponding BU_{bi} to HA. Based on the BA_{ba} it gets in return, it constructs a corresponding BA_{ba}, which is returned through the AAA infrastructure together with the authentication and authorization result. The Diameter AVPs that are returned back towards the visited network will be as described in (3).

\[ \text{[Auth.Resp.]^{AVP} [BA_{ba}]^{AVP}} \]  

(3)

Finally, the MAP nests the BA_{ba} into its own BA_{map} and returns this message to the MN. It will not respond with a successful BA_{map} unless the MN managed to authenticate correctly and the BA_{ba} implies a successful registration with the HA. The message returned to MN is described in (4).

\[ \text{BA}_{map} \text{ [BA}_{ba}]^{^{option}} \]  

(4)

If the aforementioned challenge/response method is chosen as authentication mechanism of our proposed scheme, the content of the authentication information sent will mainly consist
of challenges and responses as illustrated in Figure 10. In this case, however, a challenge for each MAP needs to be conveyed to MNs through MAP-options of Router Advertisements (i.e. ICMP neighbor discovery messages). This message should be as described in (Figure 5).

\[ \text{RA[MAP}_1, \text{Chall}_{1}]^{\text{MAP-option}} \text{[MAP}_2, \text{Chall}_{2}]^{\text{MAP-option}} \]  \tag{5} 

Diameter provides a large number of AVPs that could be reused for the scheme presented in this paper. For example, if the challenge/response method is chosen as authentication mechanism, the AVPs used for the MIPv4 Diameter application could also be used for the proposed scheme here. A new specification for HMIPv6 Diameter application would still be required. This is beyond the scope of this paper.
5 Discussion

5.1 Functionality with a hierarchy of MAPs

Although the HMIPv6 draft does not recommend a hierarchy of MAPs, it is definitely possible. The proposed scheme would still be valid and would work as illustrated in (Figure 11).

The details of (Figure 11) are as follows: The MN first sends a combined BU to the preferred MAP, MAP1. This MAP requires authentication and forwards the BU to the local AAA server, AAA1. The AAA1 server forwards the BU to the next AAA server (AAA2) in the chain, which in turns forwards the message to a preferred MAP in this domain (MAP2). This operation continues until the home domain is reached. After successful authentication the home agent is updated with the BU. The authentication and authorization result as well as the BA are then propagated through the chain created upstream. Each MAP can then create a binding as a result of a successful BA coming from the upstream MAP, and nest the previous BAs into an extension of a BA it sends towards the MN. The MN finally receives a BA from MAP1, containing BAs from the HA and all other upstream MAPs.

![Hierarchical Diameter architecture, using a hierarchy of MAPs](image)

5.2 Security Considerations

To our knowledge the proposed solution does not introduce any degradation of the security compared with HMIPv6.

We would like to emphasize that the challenge/response method that is suggested as a possible authentication mechanism for the proposed scheme, allows the visited network to authenticate an MN. However, it does not allow the MN to authenticate nodes (e.g. ARs or MAPs) on the visited network. An additional authentication mechanism would be required for the purpose of network authentication. The MN could for example send a challenge to the MAP. AAAf could then respond to the challenge, and use AAAH to verify for the MN that AAAf's response was correct. Mutual authentication would then still be possible in only one RTT between the visited and the home networks. This mechanism could easily be added to the proposed scheme presented in this paper. Alternatively, an authentication scheme that provides mutual authentication could be employed.

It should also be noted that our proposal is not affected by the required return routability test of MIPv6. MN must initiate the return routability test with CNs to achieve route optimization after having successfully registered with the HA. The proposed scheme, on the other hand, is only active as part of MN's initial registration with the HA.

During MN’s initial registration with the HA, it is a critical point of security to secure the BUa. MIPv6 uses IPSec, but this proposal may use any mechanism to get BUa securely protected on the way from MN to AAAH since this part is transparent to the MIPv6 specification. It is beyond the scope of this paper to detail how this should be done. It is
more important that AAAH uses IPSec when sending BA_{ah} and registering on behalf of HA. In this way, HA can be transparent to whether MN uses the proposed variation of HMIPv6 or not.
6 Further Work

The proposed interactions between mobility protocol and AAA procedures need to be
evolved to a more generic solution in order to coexist with non-mobile nodes in a cost
effective manner. This means that authentication processes supported by a AAA
infrastructure for non-mobile nodes should be maintained in the consideration for a
generically applicable architecture. A generic solution should also consider the possibilities
to exploit the accounting and authorisation capabilities within the AAA infrastructure.
Further work should also consider the possibilities to create a local security association in
order to minimize the signaling based on the SA between the MN and HA. This will also
provide a fundament for distributing the policy control from the HA.

In the future careful thoughts should be made on the possibilities of supporting mobile
networks in the generic solution.
7 Concluding Remarks

HMIPv6 is a protocol that enhances MIPv6 with faster handovers. Neither HMIPv6 nor MIPv6 provide ways to authenticate roaming mobile nodes, though this would be required for inter-domain roaming. MIPv4, on the contrary, provides a way to authenticate roaming mobile nodes. This solution is based on FAs working as anchor points for both mobility and authentication in visited networks.

It is here proposed a similar solution to MIPv6. HMIPv6 provides MIPv6 with MAPs that can handle both authentication and mobility management in visited networks. Furthermore, Diameter is proposed as AAA infrastructure. Among a number of possible authentication mechanisms, it is also showed how the proposed solution would work with challenge/response as an authentication method.

Further considerations need to be put on how the AAA infrastructure could be used to establish temporary security associations between mobile nodes and the networks they are visiting. Thus, applications that require subsequent authentication may not require signaling between the visited and the home domain.
Significance for Telenor

Internet generated traffic data over Mobile Networks will increase significantly in a near future. It is thus important to understand how IP technology can cope with mobility so as to provide a more effective platform. Use of IP technology can also ensure that all platforms, fixed and Mobile, can use a common technology, this would further reduce operational costs.
References