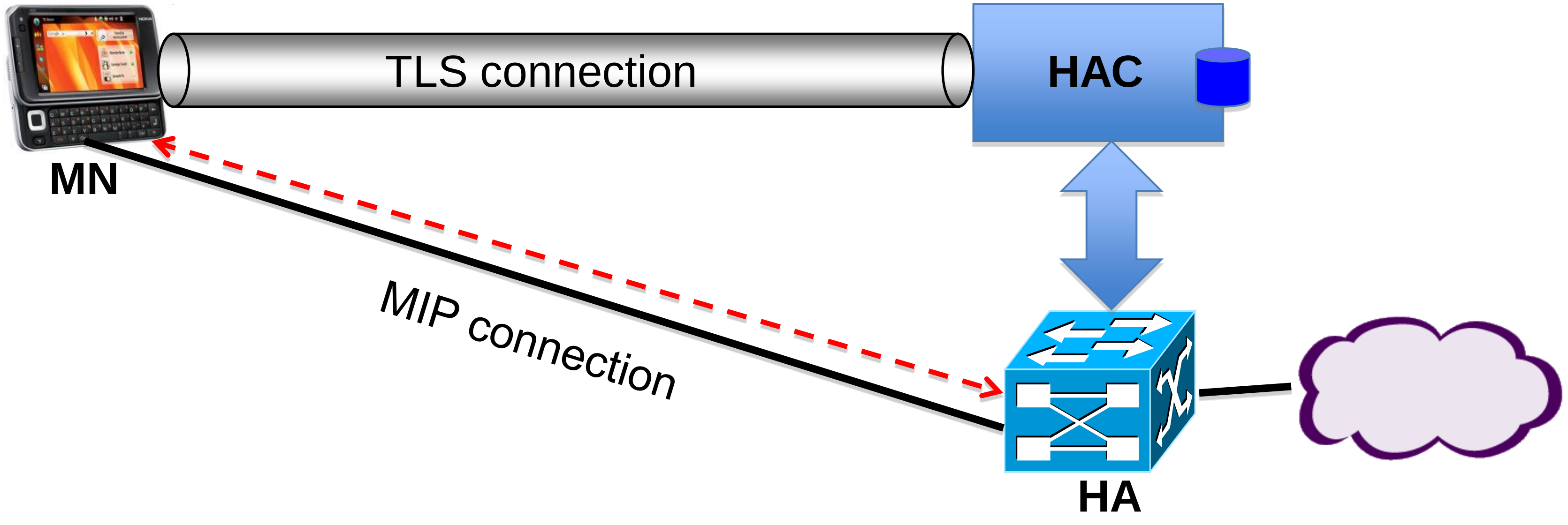
TLS-based Security solution for Mobile IPv6

draft-korhonen-mext-mip6-altsec-02

Jouni Korhonen,
Basavaraj Patil,
Hannes Tschofenig,
Dirk Kroeselberg

IETF #76, MEXT WG

Solution Architecture



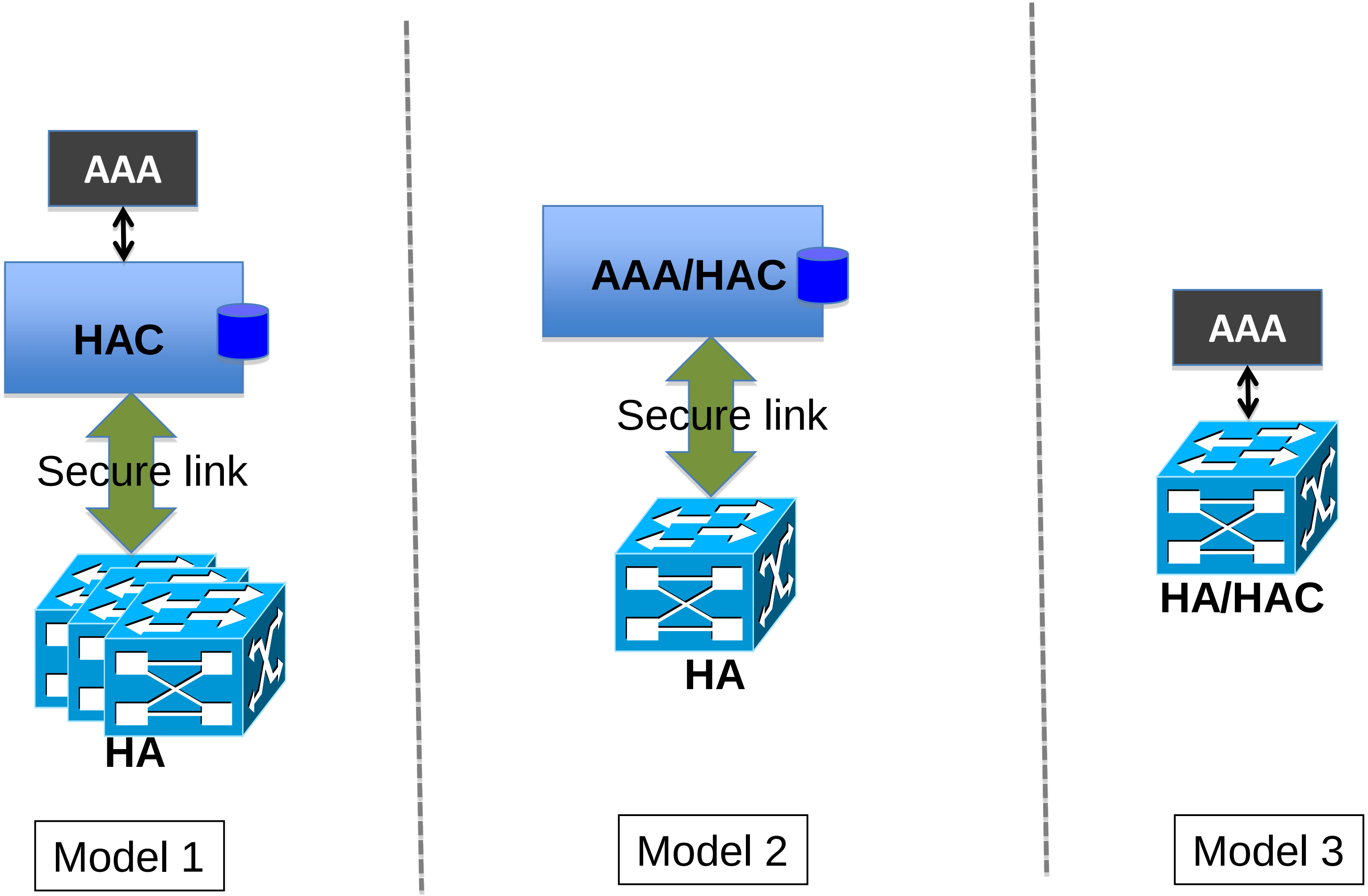
<- - - -> Secured signaling

—— Traffic (optionally secure)

Solution Architecture Cont’d

- The TLS connection is only used between the MN and the HAC during the **MN authentication** & **bootstrapping** phase.
- HAC is a functional entity and can be colocated with the HA, AAA or as a separate element.
- Security for the MN-HA signaling and optionally user traffic is via the SA bootstrapped by the HAC.

HAC and HA Deployment Models



AAA

HAC

Secure link

HA

Model 1

AAA/HAC

Secure link

HA

Model 2

AAA

HA/HAC

Model 3

MN-HAC Communication

- Simple Request-Response lockstep protocol inside the TLS-tunnel.
- The I-D defines one container format that carries “http-like” Type-Value pair headers:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Reserved      | Identifier    | Length                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Content portion..                                             ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Six “pseudo” messages defined:
  - Request/MHAuth-Init, Response/MHAuth-Init
  - Request/MHAuth-Mid, Response/MHAuth-Mid
  - Request/MHAuth-Done, Response/MHAuth-Done

MN-HAC Authentication

- Simple PSK exchange based on (simplified) GPSK.
- Also supports EAP based authentication.
- Protected by the encapsulating TLS tunnel between the MN and the HAC.
- Uses TLS channel binding (‘tls-server-endpoint’ described in [I-D.altman-tls-channel-bindings]).
- Server Certificate required for TLS.

MN Authentication using PSK

- Simple two roundtrip PSK authentication defined in the I-D.

```
MN                                                       HAC
 |                                                        |
 | Request/MHAuth-Init (...)                              |
 |------------------------------------------------------->|
 |                                                        |
 |                            Response/MHAuth-Init (...)  |
 |<-------------------------------------------------------|
 |                                                        |
 | Request/MHAuth-Done (...)                              |
 |------------------------------------------------------->|
 |                                                        |
 |                            Response/MHAuth-Done (...)  |
 |<-------------------------------------------------------|
 |                                                        |
```

MN Authentication Using any EAP Method

```
MN                                                       HAC
 |                                                        |
 | Request/MHAuth-Init (...)                              |
 |------------------------------------------------------->|
 |                                                        |
 |                            Response/MHAuth-Init (...,  |
 |                     eap-payload=EAP-Request/Identity)  |
 |<-------------------------------------------------------|
 |                                                        |
 | Request/MHAuth-Mid (eap-payload=                       |
 |              EAP-Response/Identity)                    |
 |------------------------------------------------------->|
 |                                                        |
 |     Response/MHAuth-Mid (eap-payload=EAP-Request/...)  |
 |<-------------------------------------------------------|
 |                                                        |
 :                                                        :
 :        ..EAP-method specific exchanges..               :
 :                                                        :
 |                                                        |
 | Request/MHAuth-Done (eap-payload=EAP-Response/...,     |
 |                      ..., auth)                        |
 |------------------------------------------------------->|
 |                                                        |
 |        Response/MHAuth-Done (eap-payload=EAP-Success,  |
 |                               ..., auth)               |
 |<-------------------------------------------------------|
 |                                                        |
```

Bootstrapping

- Bootstrapping implies:
  1. Bootstrapping of an SA between the MN and the assigned HA.
  2. Bootstrapping of Mobile IPv6 specific parameters.
- Negotiation is minimal. A HAC “pushes” the configuration to the MN and the HA.
- Bootstrapping messsages between the MN and HAC are protected by the TLS tunnel.

MN-HA Communication

- All communication between the MN and the HA is UDP encapsulated and uses a HAC provisioned port number.
- Control traffic is always protected.
- User traffic may be optionally protected.
- Common encapsulation header format, which allows easy multiplexing of different payload types using a single SA.
- The encapsulation/ciphering is similar to ESP/UDP but is decoupled from and **not** using IKE/IPsec.
  - Everything can be done in user space.

Common MN-HA UDP Encapsulation Header Format – Protected

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:         IPv4 or IPv6 header (src-addr=Xa, dst-addr=Ya)        :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:            UDP header (src-port=Xp,dst-port=Yp)               :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ------
| PType |                    SPI                                | ^Int.
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|                      Sequence Number                          | |ered
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | ----
|                    Payload Data* (variable)                   | |   ^
:                                                               : |   |
|                                                               | |Conf.
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|               |   Optional Padding (0-255 bytes)                | |ered*
+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |   |
|                               |  Pad Length   | Next Header   | v   v
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ------
|    Optional Integrity Check Value-ICV   (variable)            |
:                                                               :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Common MN-HA UDP Encapsulation Header Format – Plain Text

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:         IPv4 or IPv6 header (src-addr=Xa, dst-addr=Ya)        :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:            UDP header (src-port=Xp,dst-port=Yp)               :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|PType=0|                        0                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                0                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:           Payload Data (plain IPv4 or IPv6 Packet)            :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Implementation Progress

- Implementation of this security solution is being done for DSMIP6.
- Our implementation is making progress!
  - MN-HAC part completed.
  - MN-HA part integration to mipd in progress.
- Will be made available by the end of year.

Next steps

- Request the adoption of this I-D as a WG document in MEXT.

Questions and Discussion