ENABLING EFFICIENT AND OPERATIONAL MOBILITY IN LARGE HETEROGENEOUS IP NETWORKS

GSABA: A Generic Service Authorization and Bootstrapping Architecture

Florian Kohlmayer
Hannes Tschofenig
Rainer Falk
(Siemens AG)

Rafael Marin
Pedro Segura
Antonio Gomez-Skarmeta
Santiago Zapata
(University of Murcia)

MobiArch 2006

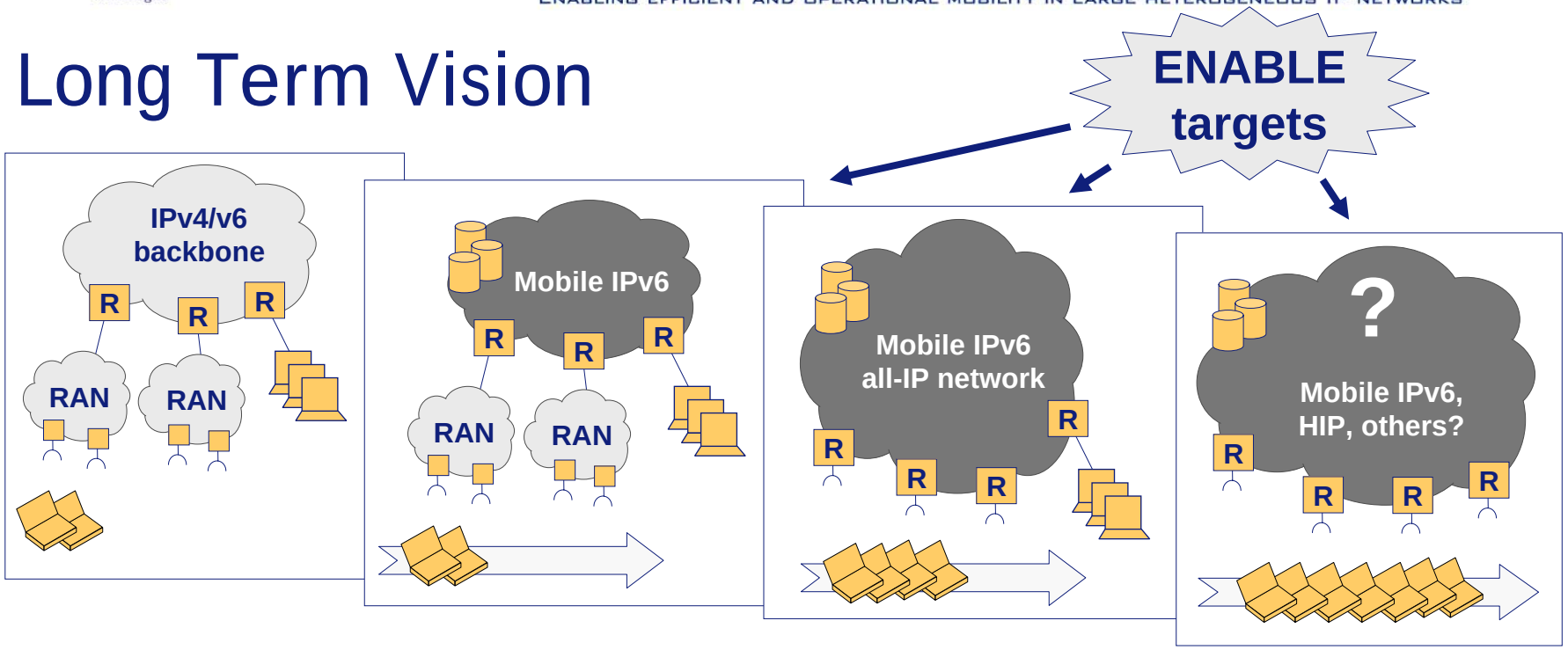
First ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture

Dec 1, 2006 – San Francisco, California, USA

Enabling Efficient and Operational Mobility in Large Heterogeneous IP Networks

- Duration: Jan 2005 – Dec 2007 (2 years)
- Overall volume: 406 p.m.
- Project consortium
  - Telecom Italia (through Telecom Italia Lab, Italy)
  - Consultores Integrales en Telecomunicaciones, S.L. (Spain)
  - Georg-August-University of Goettingen (Germany)
  - Siemens AG (Germany)
  - University of Murcia (Spain)
  - Industrieanlagen-Betriebsgesellschaft mbH (Germany)
  - Waterford Institute of Technology (Ireland)
  - Brunel University (United Kingdom)
  - Shanghai R&D Centre of Huawei Technologies Co. Ltd (China)

Long Term Vision



Today

Dedicated RANs optimized for specific services

- cellular (2.5-3G)
- Wireless LAN
- WMAN (WiMAX)

Step 1

Integration of heterogeneous RANs to offer efficient and cost-effective ubiquitous mobility

- MIPv6 is the key

Step 2

Smooth migration to an all-IP network architecture

- all services over IP
- MIPv6 with fast handover support

Step 3

Fully mobile Internet

- tremendous growth in the number of terminals
- MIPv6 might suffer its age

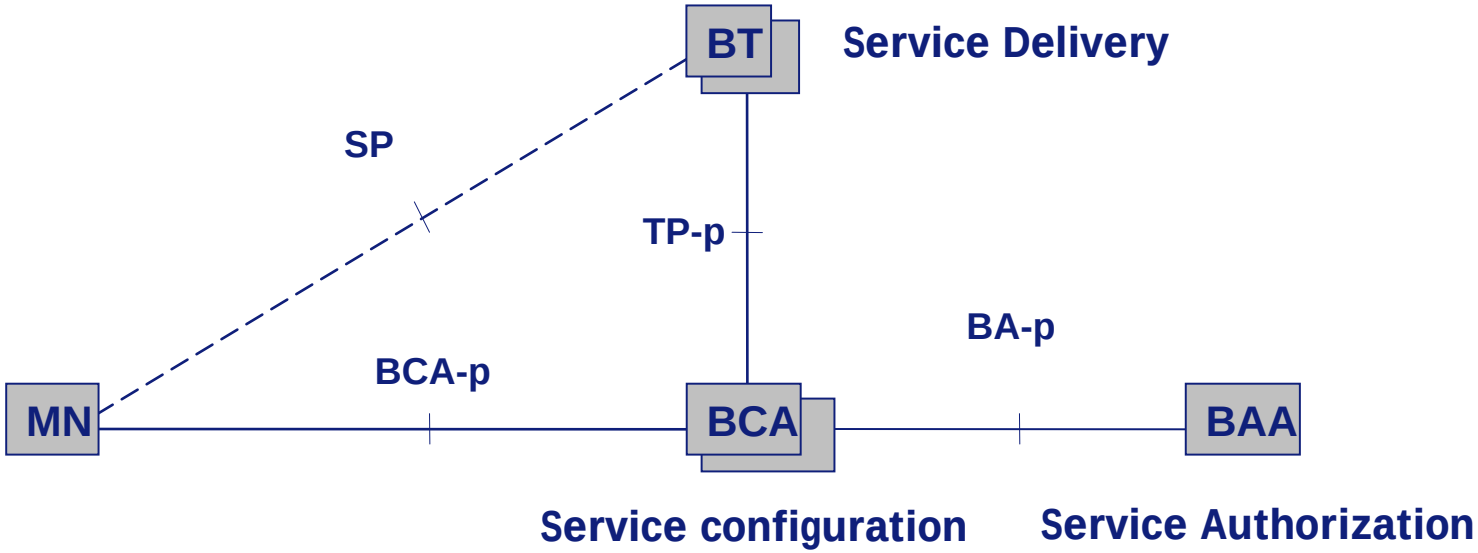
Problem Statement

- Network providers are very interested in introducing additional services in their networks
  - Seamless Mobility
  - Multi-Homing
  - Quality of Service
  - Application Services
- End host wants to use a variety of protocols and needs to secure them.
- In order to establish this security context the mobile terminal must be authenticated and authorized
- Static configuration of services at network entities or end host increases deployment costs => dynamic configuration.

Bootstrapping

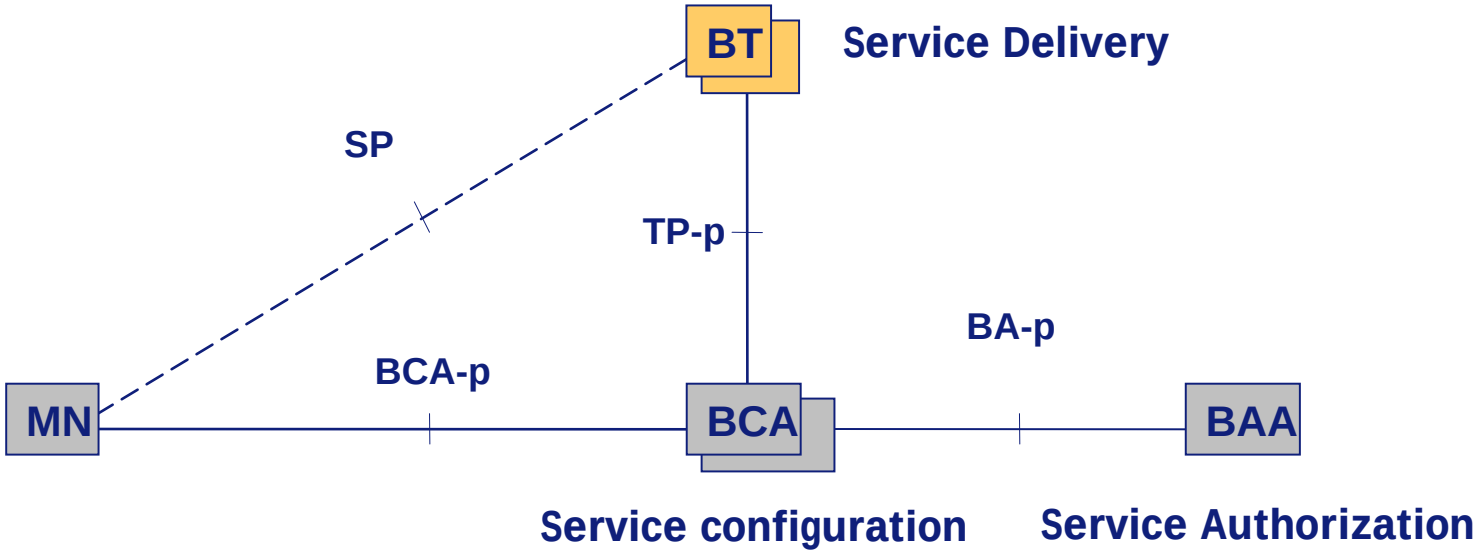
- The goal is to develop a mechanism to dynamically and securely provide the end host with the necessary information for service access based on some long-term credential
- Using this long-term credential it should be possible to for a client to carry out a process that distributes necessary information for service access
- This process creates an state between client and service based on a trust relationship between these two parties and a trusted third party that controls and manages the service
- We call this process **bootstrapping**

GSABA Architecture



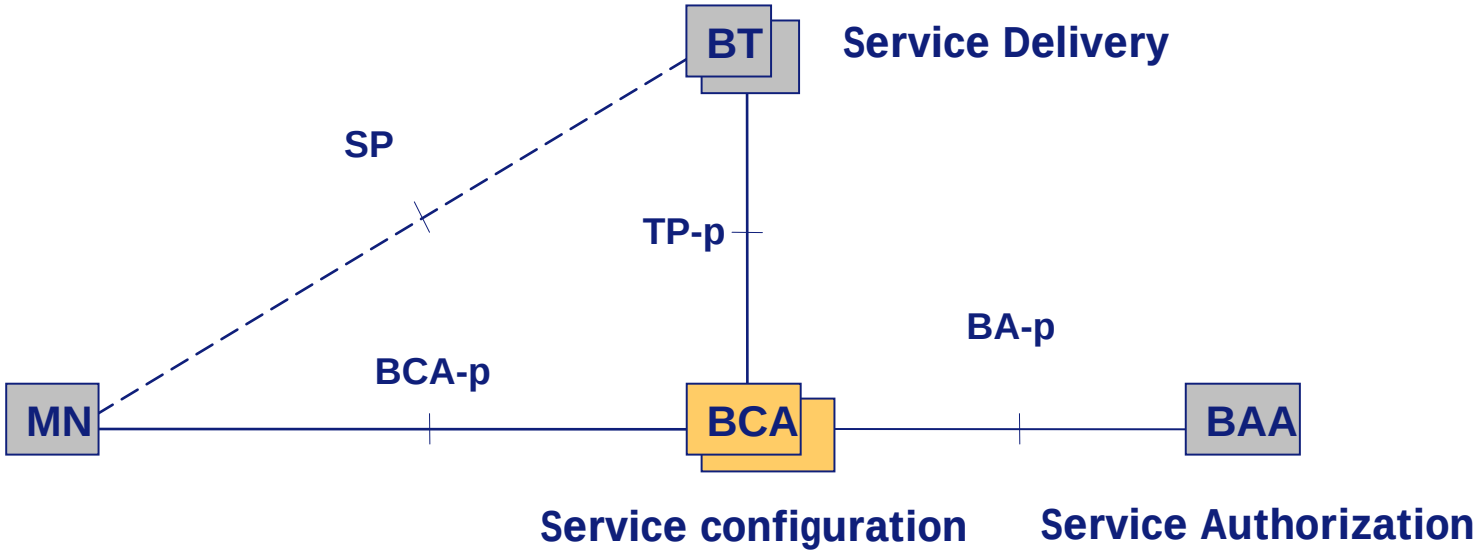
- The proposed architecture consists of a set of basic entities that can be instantiated in a variety of ways, providing a flexible deployment

GSABA Architecture



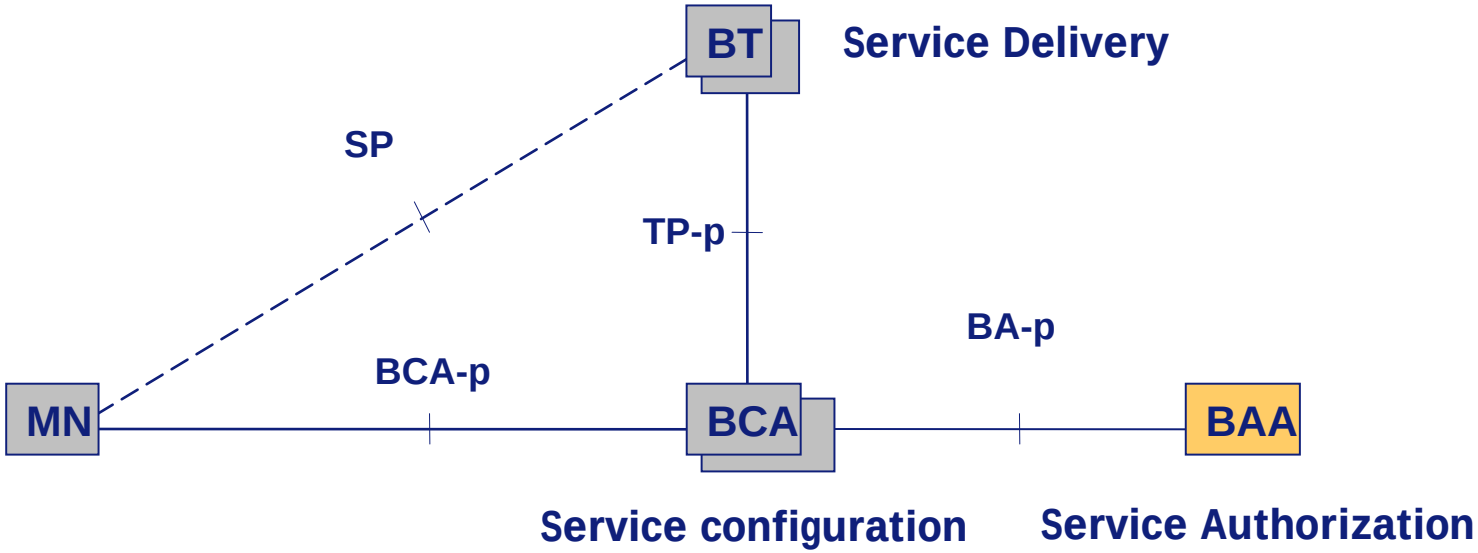
- Bootstrapping Target (BT)
  - It's the entity that offers the requested service (e.g., the Home Agent)
  - The service can be provided by a single BT or by mutiple BTs

GSABA Architecture



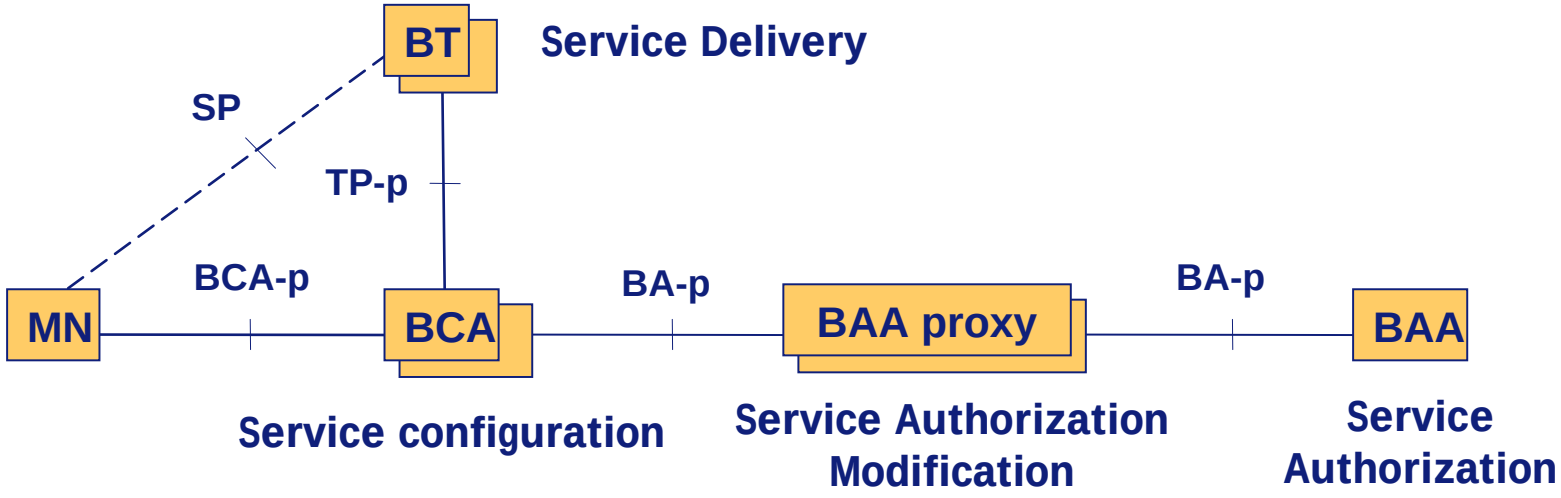
- Bootstrapping Configuration Agent (BCA)
  - Provides necessary bootstrapping information to the Mobile Node (MN)
  - Must be able to authenticate the MN and the BT

GSABA Architecture



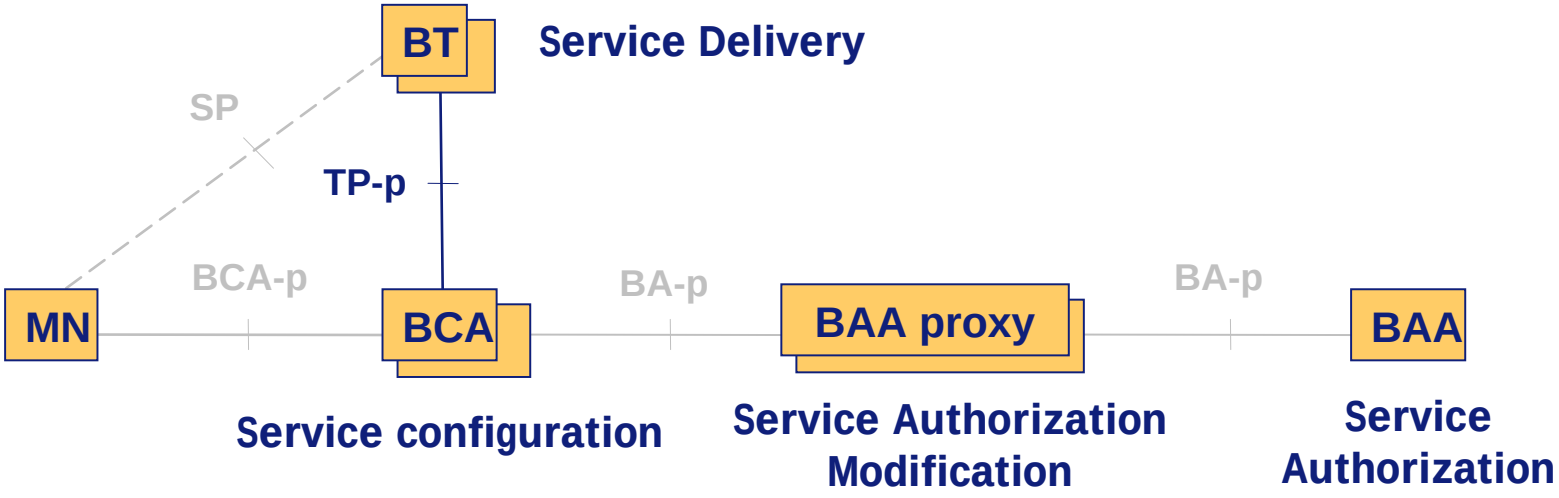
- The Bootstrapping Authorization Agent (BAA)
  - Asserts authorization statements based on the MN's profile
  - These statements and related parameters must be conveyed to the MN

Roaming GSABA Architecture



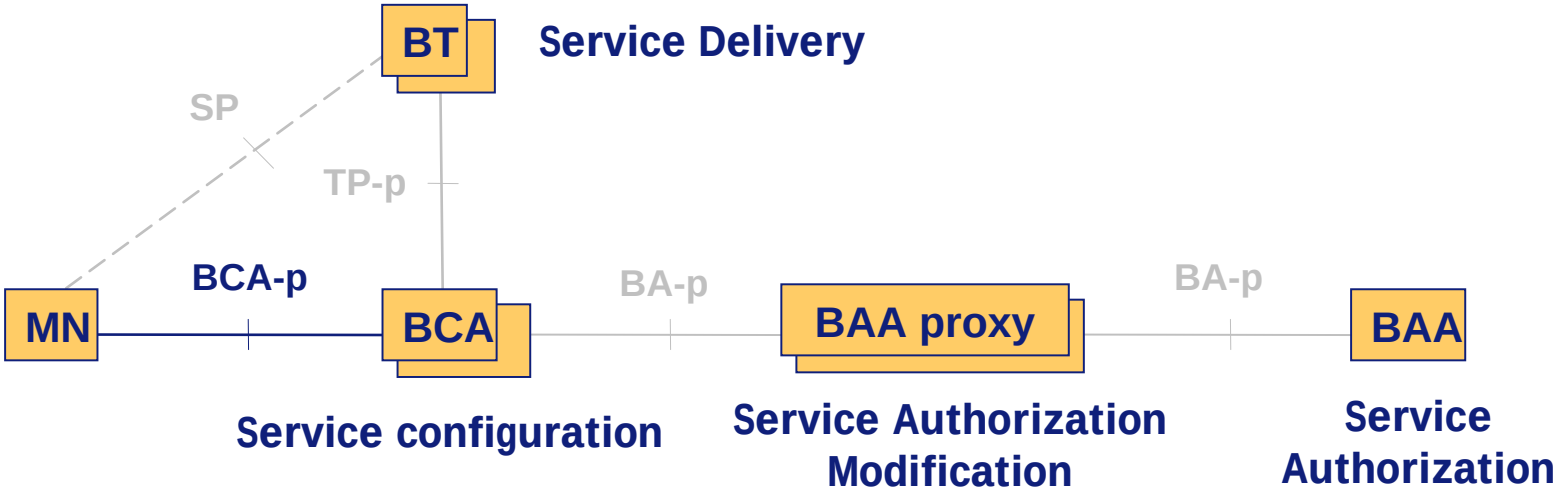
- The roaming architecture introduces a new architectural entity: the BAA proxy
- This entity is responsible for:
  - Forwarding the policies asserted from the BAA
  - Modifying these policies

Main Interfaces (I)



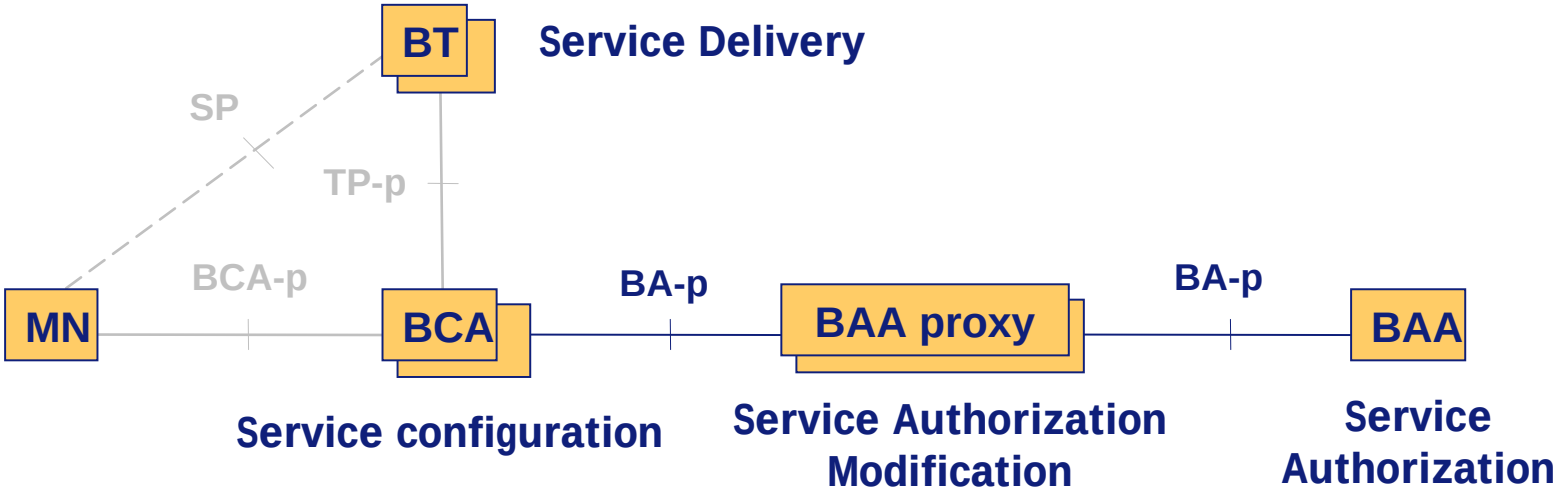
- Bootstrapping Target Protocol (TP-p)
  - Exchanges service related information
  - Authorizes the BT to provide service to the MN
  - Example protocols: RADIUS, Diameter

Main Interfaces (II)



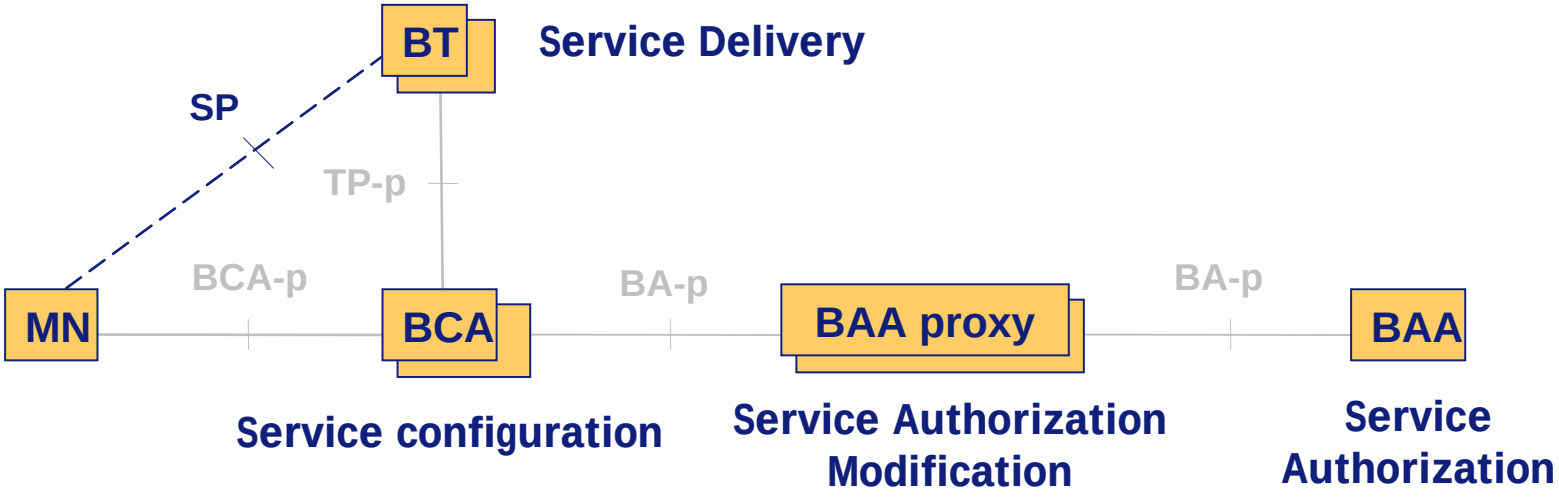
- Bootstrapping Protocol (BCA-p)
  - Conveys bootstrapping information to the MN
  - Informs the MN of the authorization decision taken by the BAA and the BAA proxy
  - Some candidate protocols:
    - EAP/PANA, IKEv2 (without IPsec), HTTP, SOAP, EAP+DHCP, etc.

Main Interfaces (III)



- Bootstrapping Agent Protocol (BA-p)
  - Allows information exchange needed for the BAA entities to base the decision on
  - Delivers these decisions to the BCA.
  - Protocols: RADIUS, Diameter

Main Interfaces (IV)

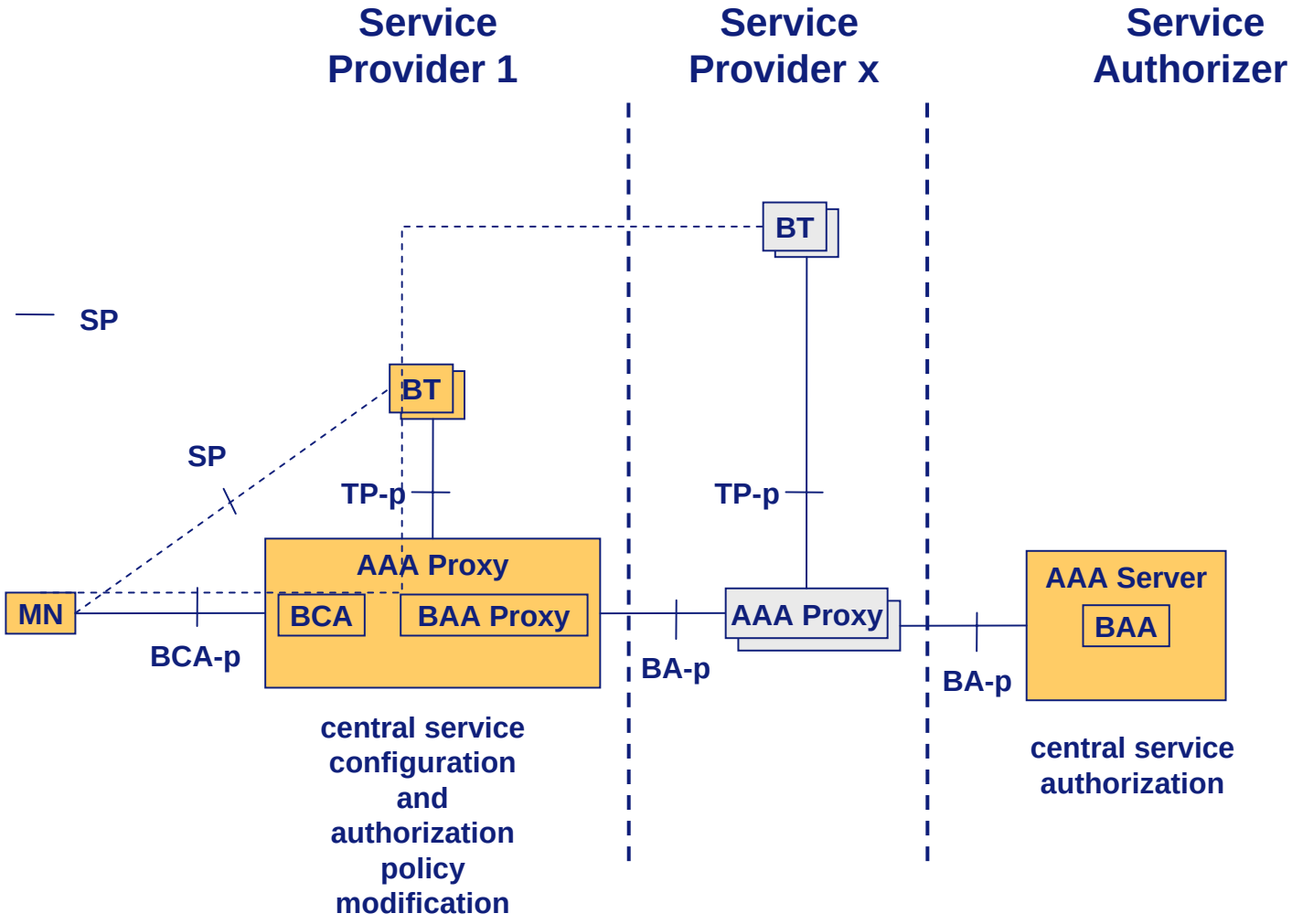


- Service Related Protocol (SP)
  - Protocol ideally left unmodified

Integration in AAA Infrastructure (I)

- Today, most Telecommunication Operators and ISPs make use of the AAA infrastructure and roaming agreements for their services
- GSABA leverage the existing AAA infrastructure in order to reduce the deployment costs

Integration in AAA Infrastructure (II)

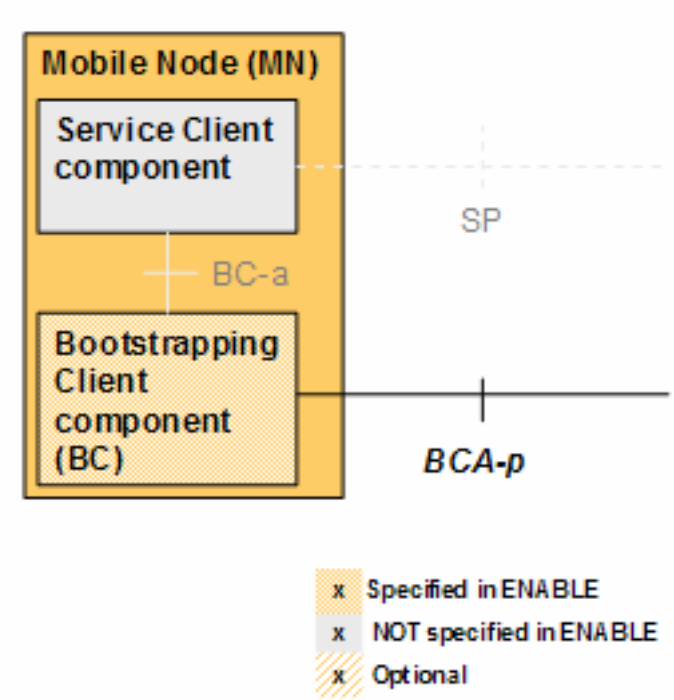


Integration in AAA Infrastructure (III)

- Assumptions:
  - BT and the GSABA AAA proxy are co-located in the same administrative domain
  - Service authorization decisions are taken by the SA AAA server and can be modified along the AAA path to the SP by AAA proxies
  - The SA is the “home domain”
  - The MN interacts only with a single GSABA AAA proxy
  - Solution not tied to network access authentication.
  - Enable end host to learn more about authorization decisions made by the network.

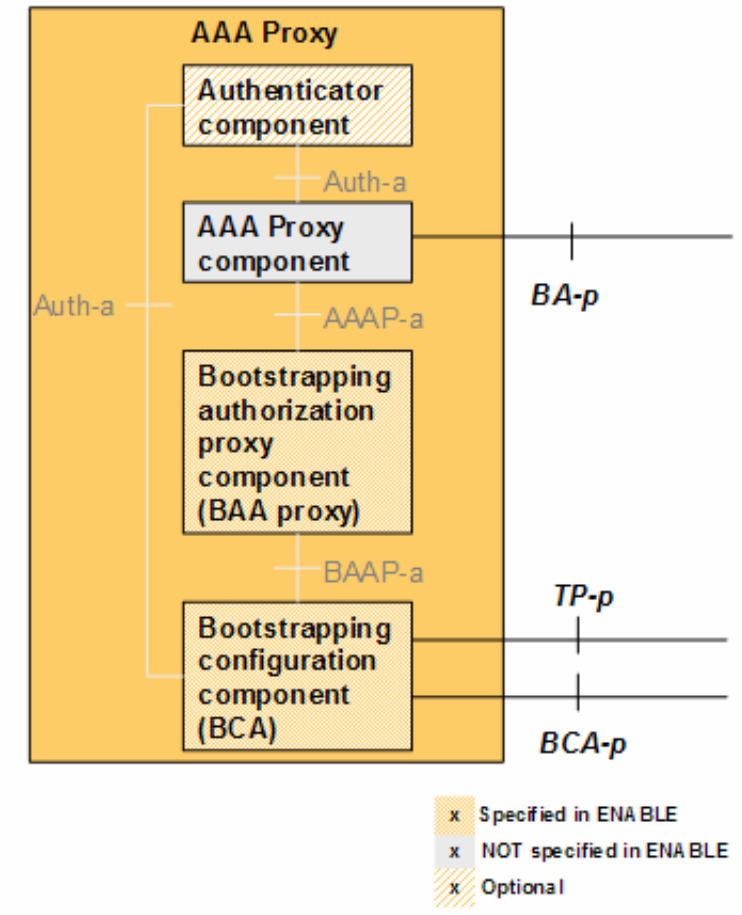
Integration in AAA Infrastructure. Entities (I)

- Mobile Node
  - Obtains the configuration parameter and authorization statements for the services from the GSABA AAA proxy, and uses this information for consuming the services
  - Consists of:
    - Service client component
    - Bootstrapping client component



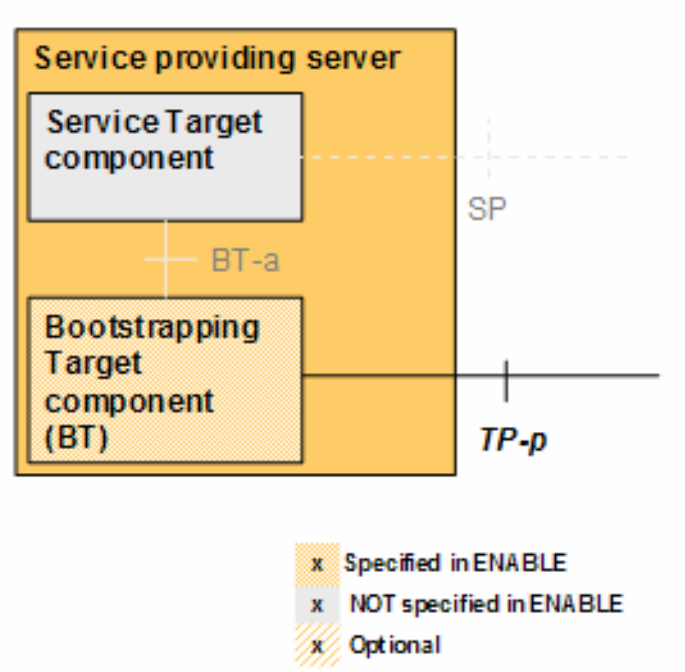
Integration in AAA Infrastructure. Entities (II)

- GSABA AAA proxy
  - Obtains the authorization statements for specific services from the home AAA server where the BAA is co-located and processes (modifies) them
  - Finally, it delivers these statements together with the needed parameters to the MN and the BTs
  - Consists of:
    - Authenticator
    - AAA proxy
    - BAA proxy
    - BCA



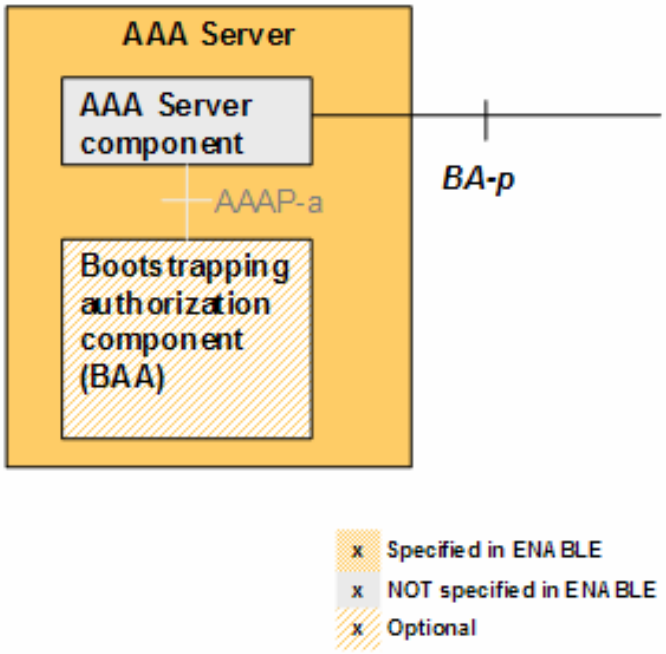
Integration in AAA Infrastructure. Entities (III)

- Bootstrapping Target
  - Is the entity responsible for providing the service to the MN
  - Is connected to the GSABA AAA proxy, and obtains via this interface the configuration and authorization information related to a specific MN
  - Consists of:
    - Service Target component
    - Bootstrapping Target



Integration in AAA Infrastructure. Entities (IV)

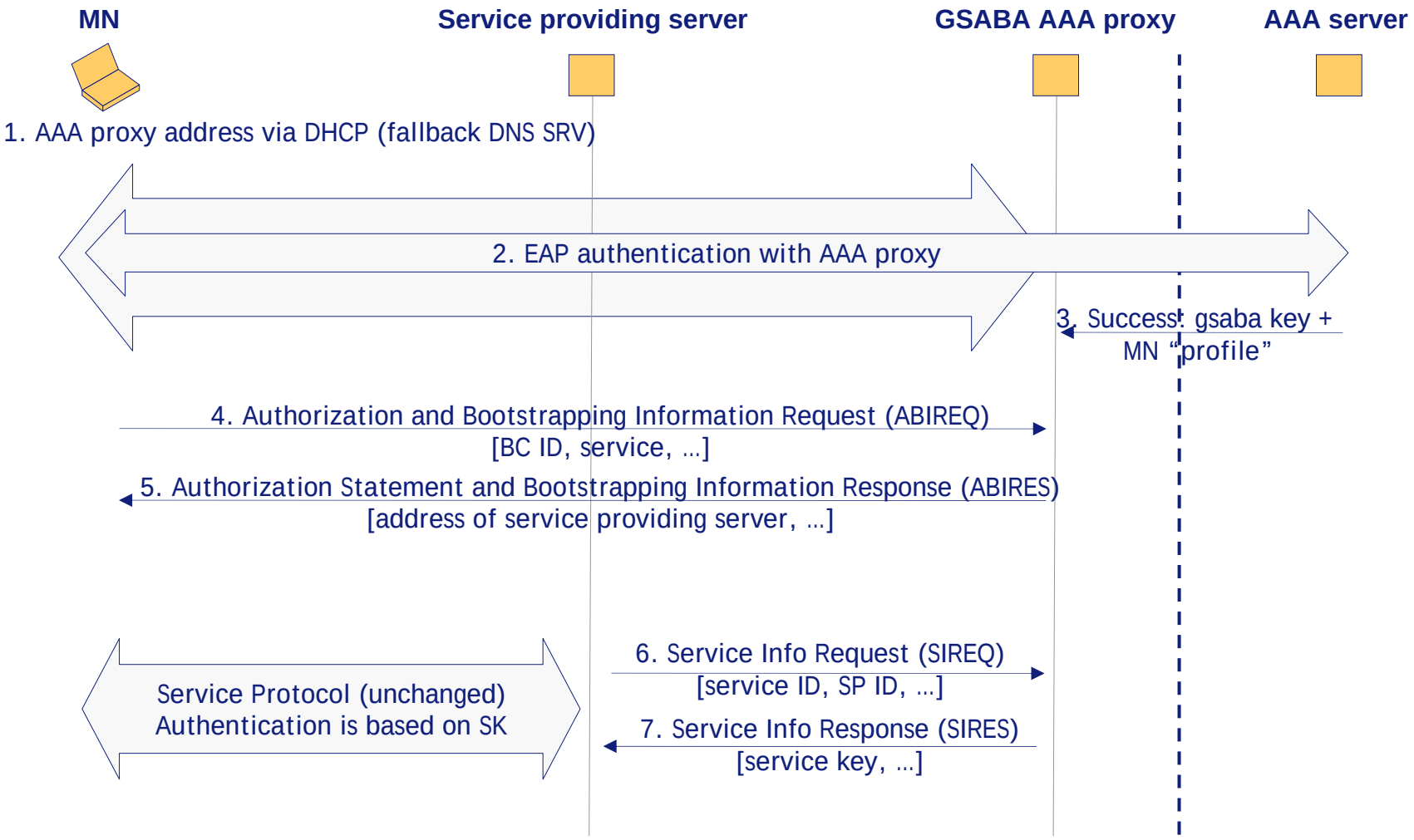
- AAA server
  - Responsible for making authorization decisions and authenticating the MN
  - Needs to be aware of the services is needs to authorize



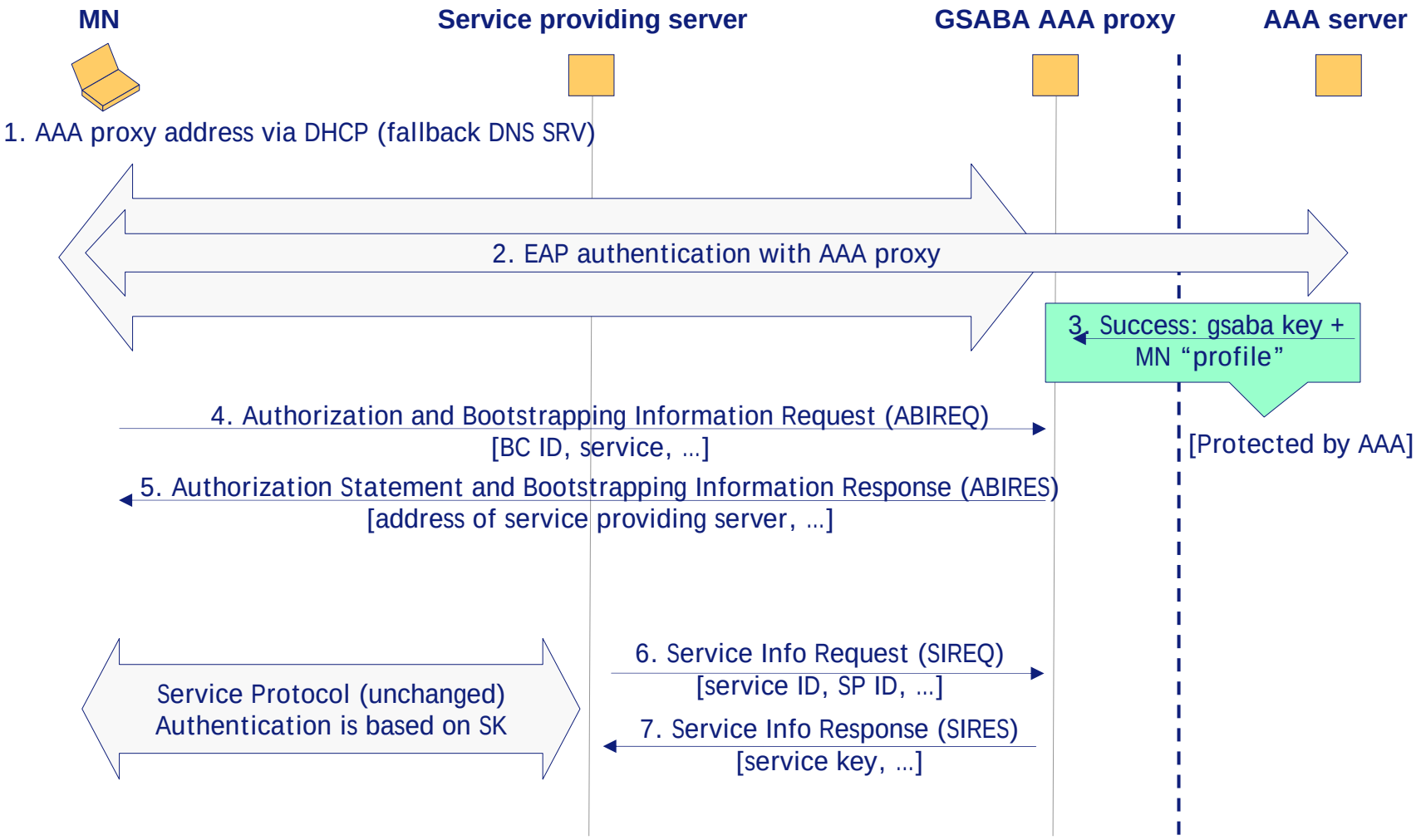
Comparison with Related Work

- **Kerberos**
  - Does not utilize AAA infrastructure
  - Inter-domain communication problematic
  - Not well suited for network access authentication.
  - Authorization content not standardized.
  - Supports only Push semantic
- **3GPP GBA**
  - Does not support generic credentials (e.g., EAP)
  - Usage of HTTP for **BCA-p** interface make it suitable only for higher layer applications
- **Liberty Alliance**
  - Does not distribute keying material
  - Heavyweight due to XML usage; Can be limited with
  - Does not interwork nicely with AAA infrastructure
  - Content of SAML assertions largely non-standardized
  - Some SAML profiles involve end host more and allow end host to learn more about authorization.
  - Provides varying security level

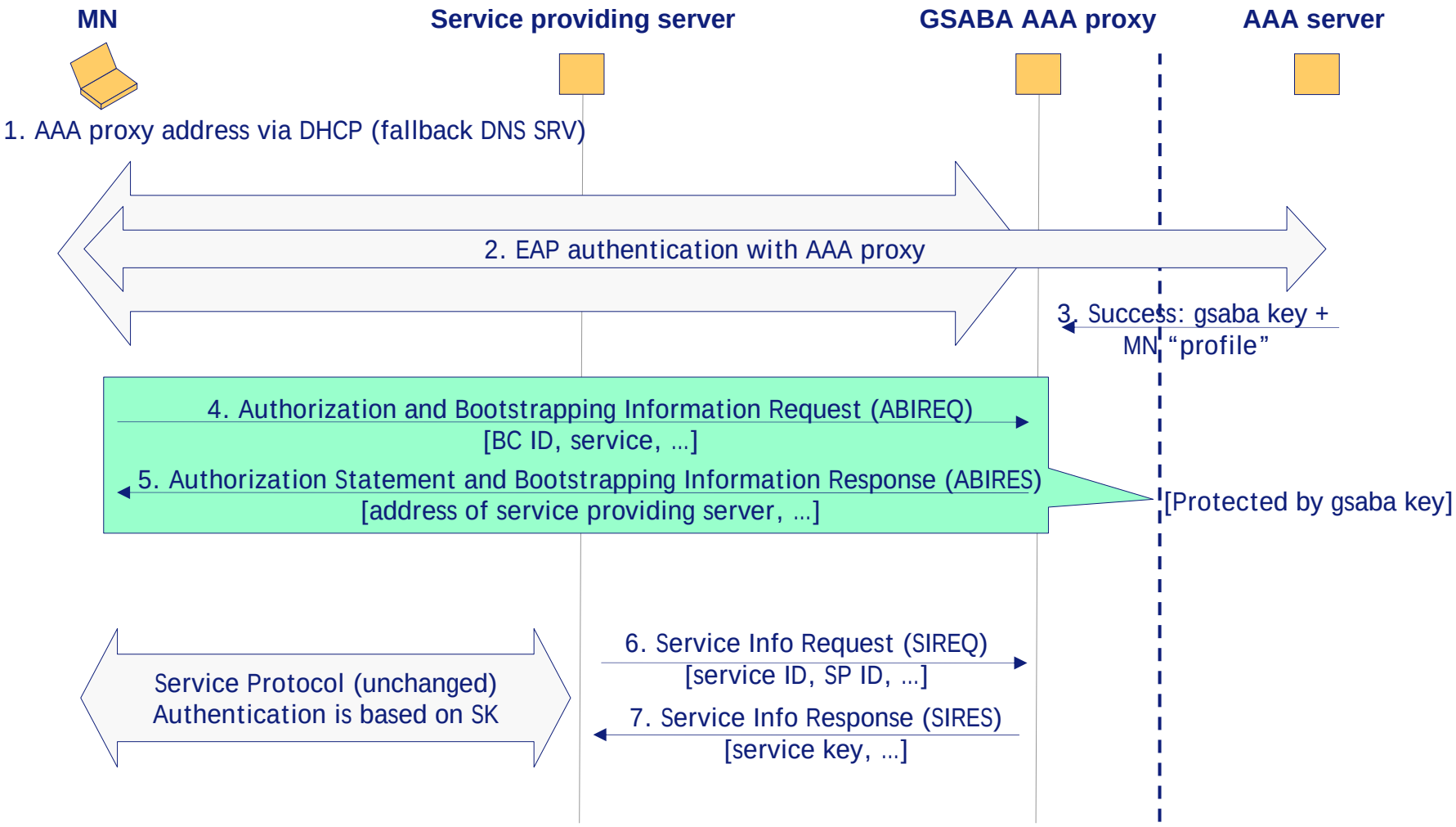
Example Message Flow



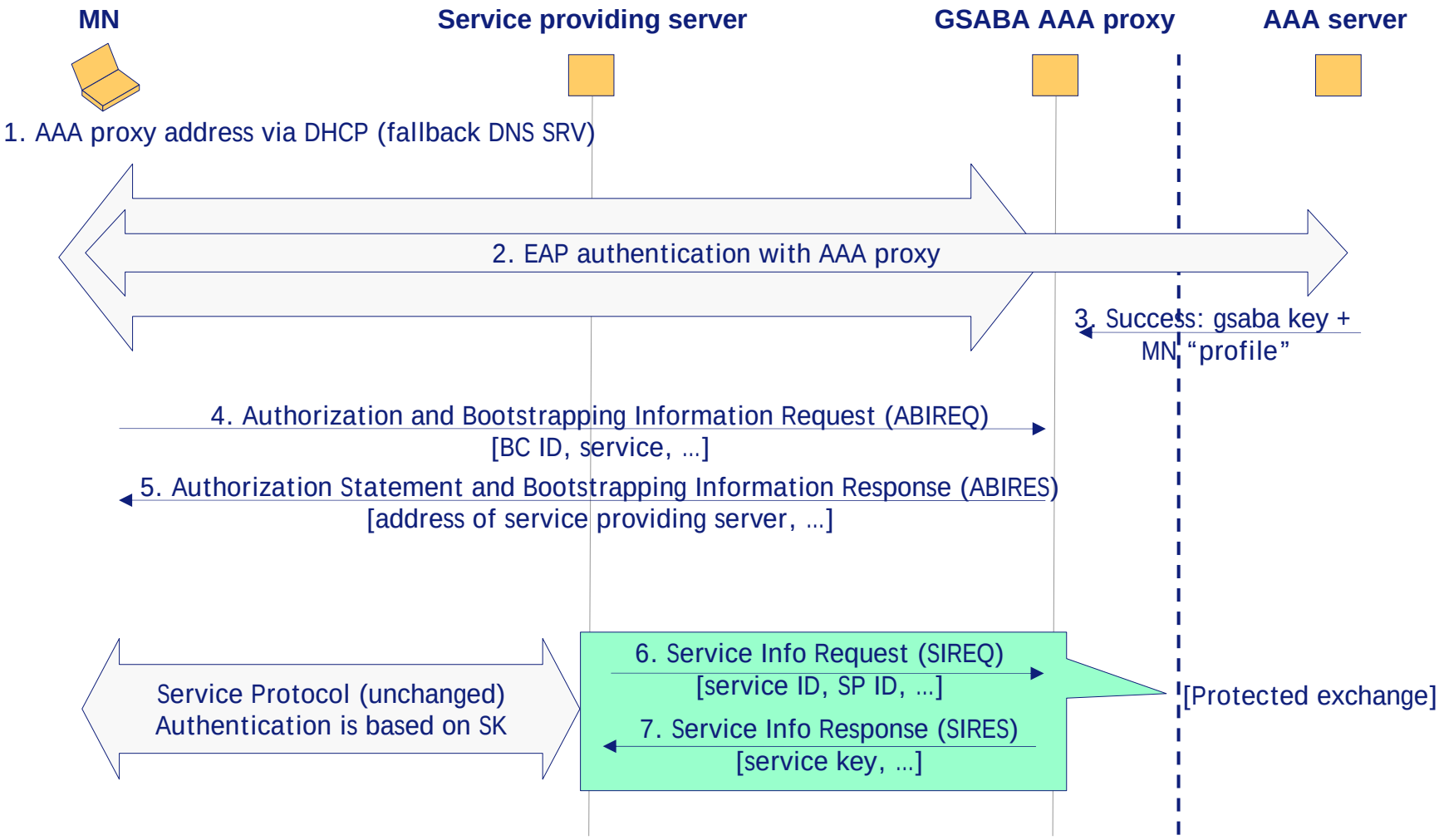
Example Message Flow



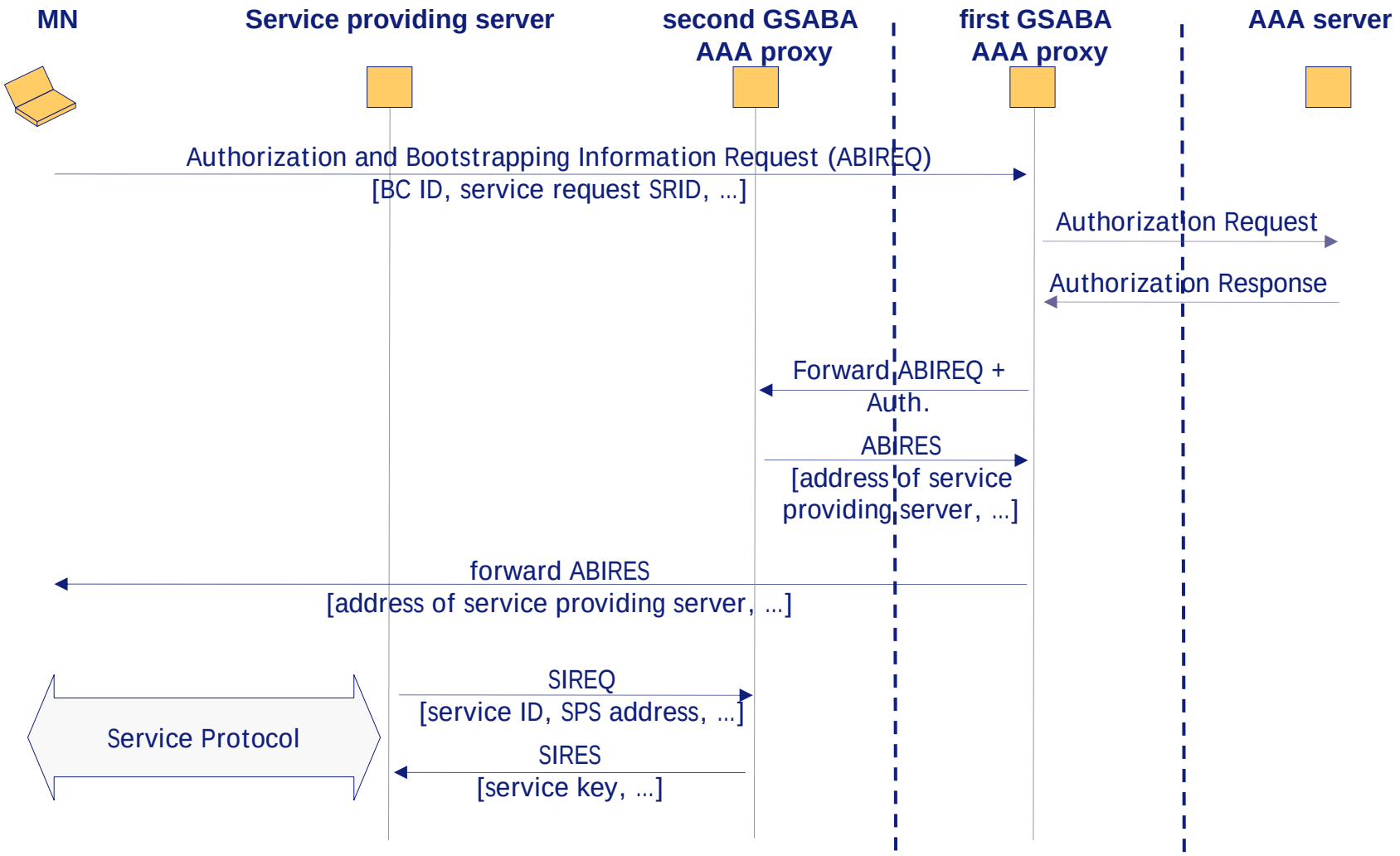
Example Message Flow



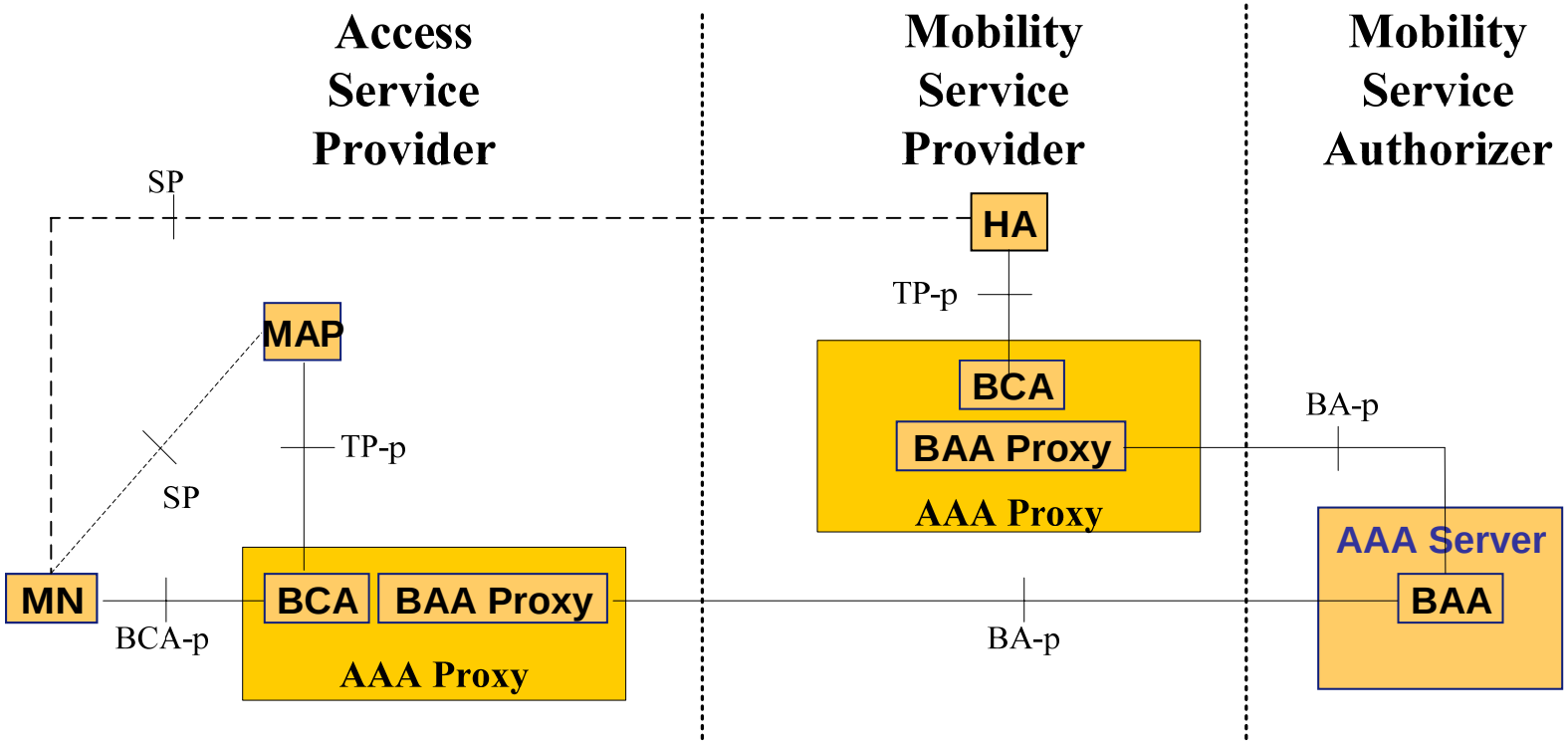
Example Message Flow



GSABA – Interworking AAA Proxies



Applicability Example: Mapping to HMIPv6



Conclusion

- GSABA provides a generic service authorization and bootstrapping framework that leverages the use of the AAA infrastructure, extending it but without requiring additional credentials
- This approach is attractive due to the large deployment base offered by the AAA architecture
- GSABA is able to bootstrap mobility, network and application layer services independently of network access authentication.
- Challenges remain with regard to security and privacy, authorization complexity and performance.