ENABLING EFFICIENT AND OPERATIONAL MOBILITY IN LARGE HETEROGENEOUS IP NETWORKS

NSIS NATFW Security Options

Qin Wu (HUAWEI)
Yuan kui zhao(HUAWEI)

Huawei Technologies Co.,LTD

Information Society Technologies

Scope

- Scenarios
  - One or more Firewalls located in MN's ASP
  - One or more Firewalls located in CN's ASP
  - One or more Firewalls located in MN's MSP
- Problem Statement (Two issues have to be solved)
  - How to secure the FW traversal signaling
  - How to authorize the creation of pinholes on FWs
- Existing security infrastructure Options
  - TLS mechanism
  - EAP mechanism
  - GBA mechanism
  - GSABA mechanism
  - Authorization Token
- Comparison between existing security infrastructures

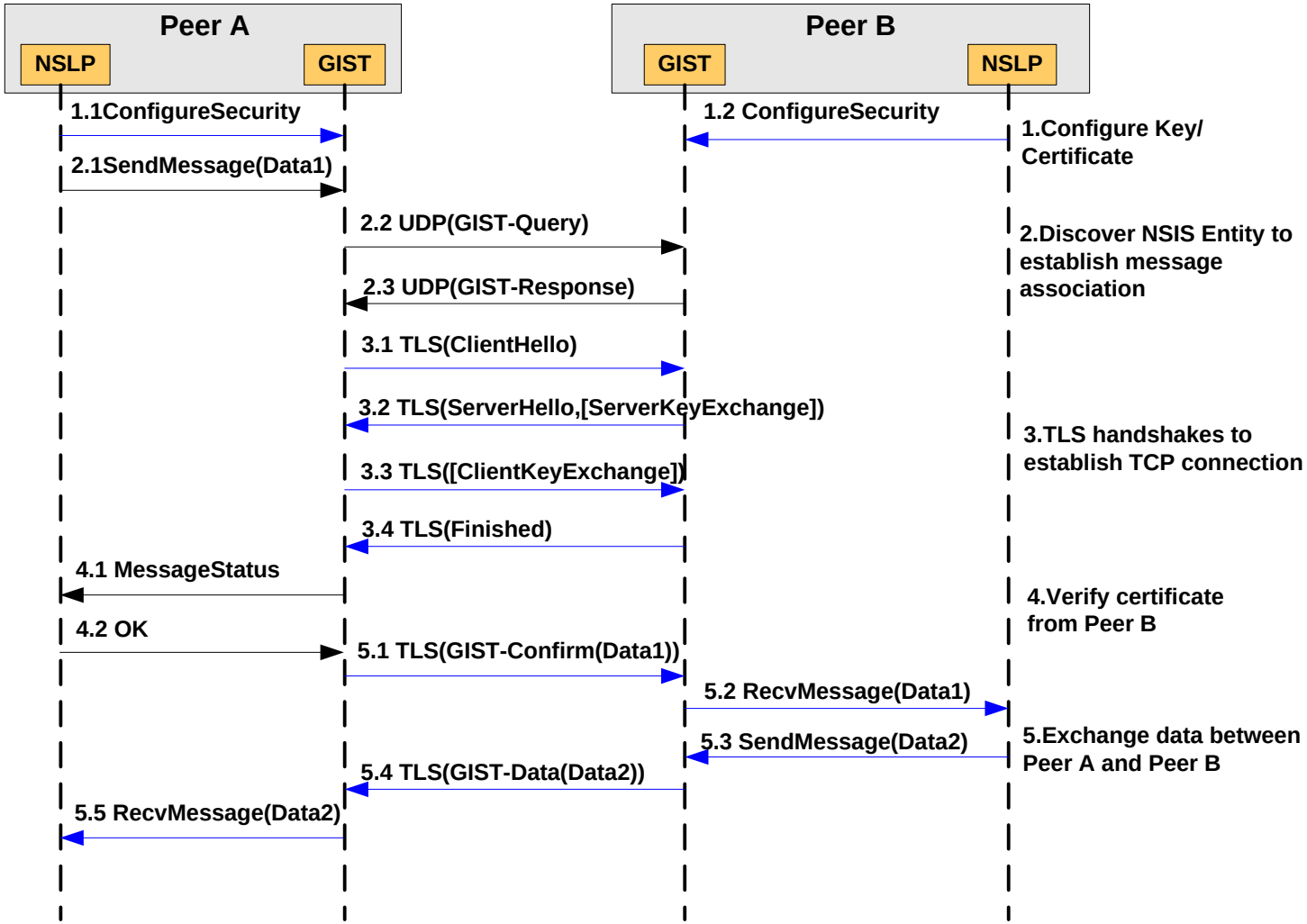
Problem Statement

- For the NSIS case, the transport layer is secured by TLS
- For the NSIS case, authorization is provided at the signaling layer
- Additional security attributes need to be exchanged through the API between the transport and the signaling layer.

TLS with X.509 PKI (1/3)

- security mechanisms for protecting application-layer protocols
- supports authenticating the parties using public-key certificates , pre-shared keys, and Kerberos
- run over TCP or SCTP, but datagram TLS also allows the use of unreliable transports such as UDP.

TLS with X.509 PKI (2/3)



TLS with X.509 PKI(3/3)

Advantage

- allow flexibility in what kind of semantics the certificates have
  - X.509 certificates bind together one or more identifiers and a public key,
  - Have additional authorization semantics

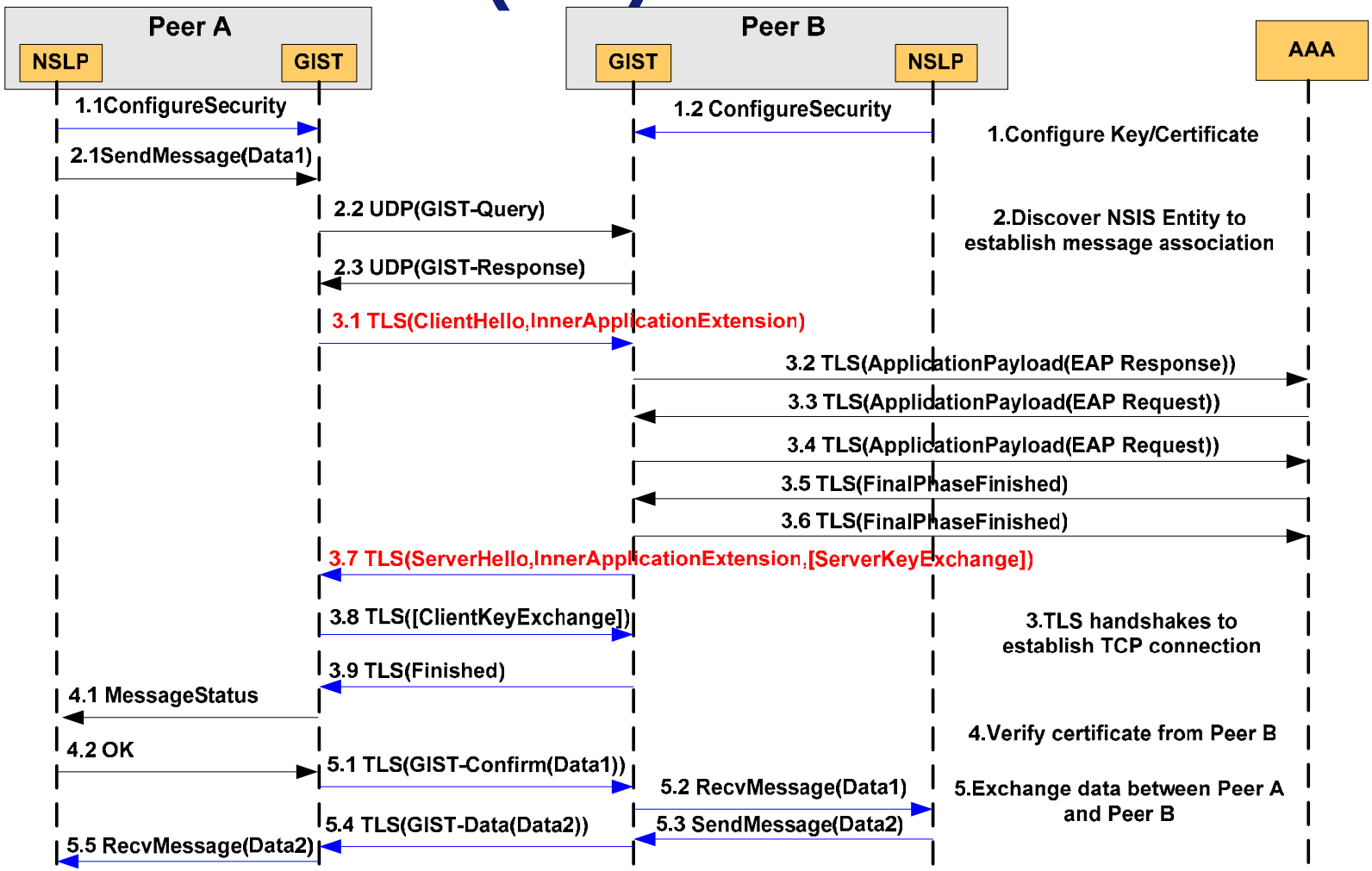
Drawback

- Depend on certificates to derive key materials
  - Suit for scenarios that authentication infrastructure based on X.509 certificates
  - difficult to integrate TLS using X.509 PKI with AAA infrastructure.

TLS/IA with EAP(1/3)

- Flexible support for authentication and key exchange protocols.
- Ability to reuse existing long-term credentials and already deployed authentication and key exchange protocols
- Integration into the existing AAA infrastructure, namely RADIUS and Diameter.
- Ability to execute the authorization decision at the user's home network

TLS/IA with EAP(2/3)



TLS/IA with EAP(3/3)

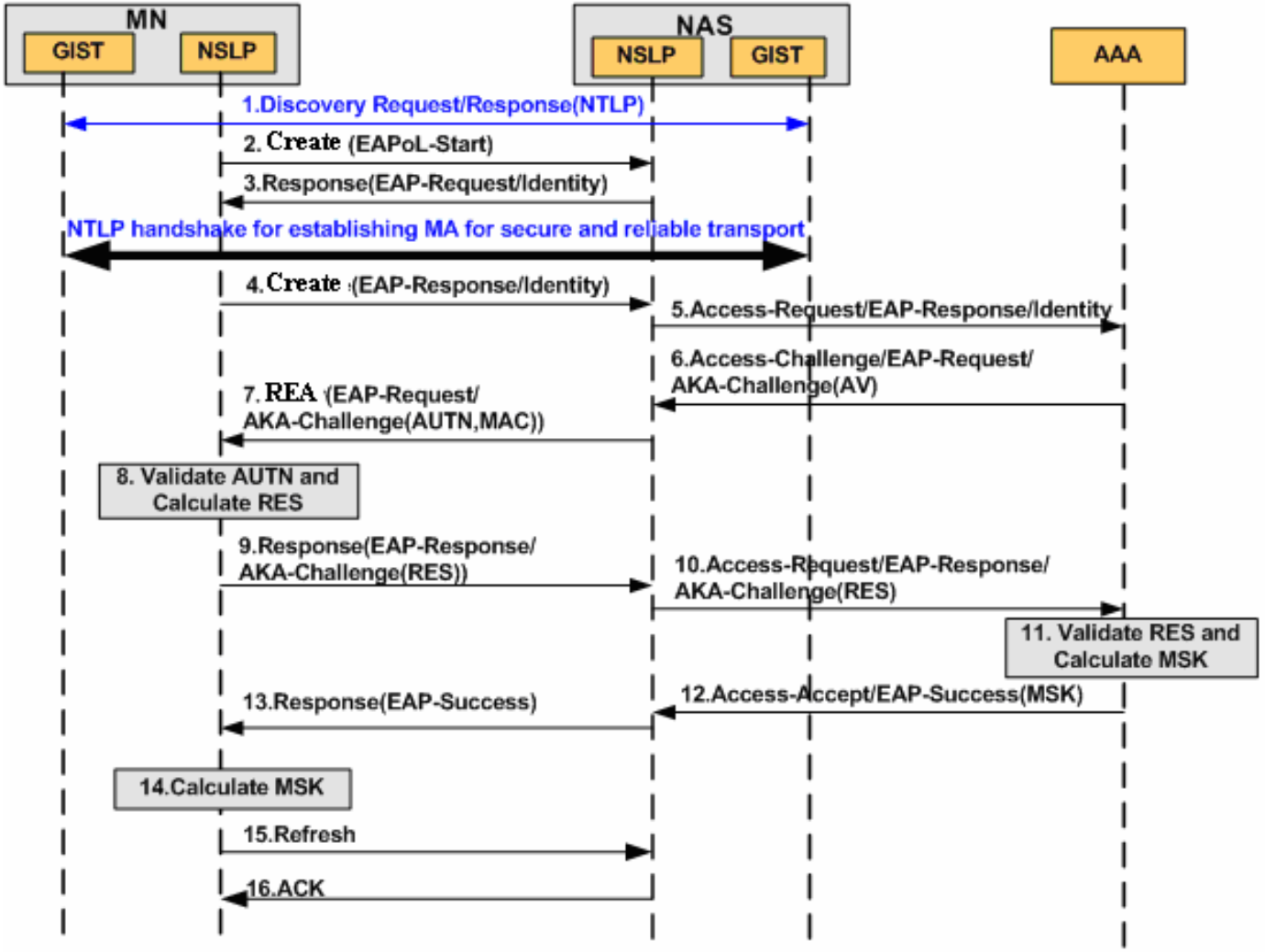
Advantage

- Require no modifications for the NSIS protocol suite
  - EAP exchange is encapsulated within the TLS Handshake exchange.
- The AAA interaction triggered as part of the TLS/IA (and the EAP method processing)

Drawback

- Authorizing the specific NSLP operation need to be provided at the NSLP
  - key establishment and a separate exchange might be required at the NSLP.
  - the specific NSLP payloads need to be processed.

EAP in NSLP(1/2)



EAP in NSLP(2/2)

Advantage

- Allows a seamless inter-working between EAP and NAT/FW NSLP protocol
  - a proper encapsulation of the EAP payloads into NAT/FW NSLP Create/Nofity/Response messages.

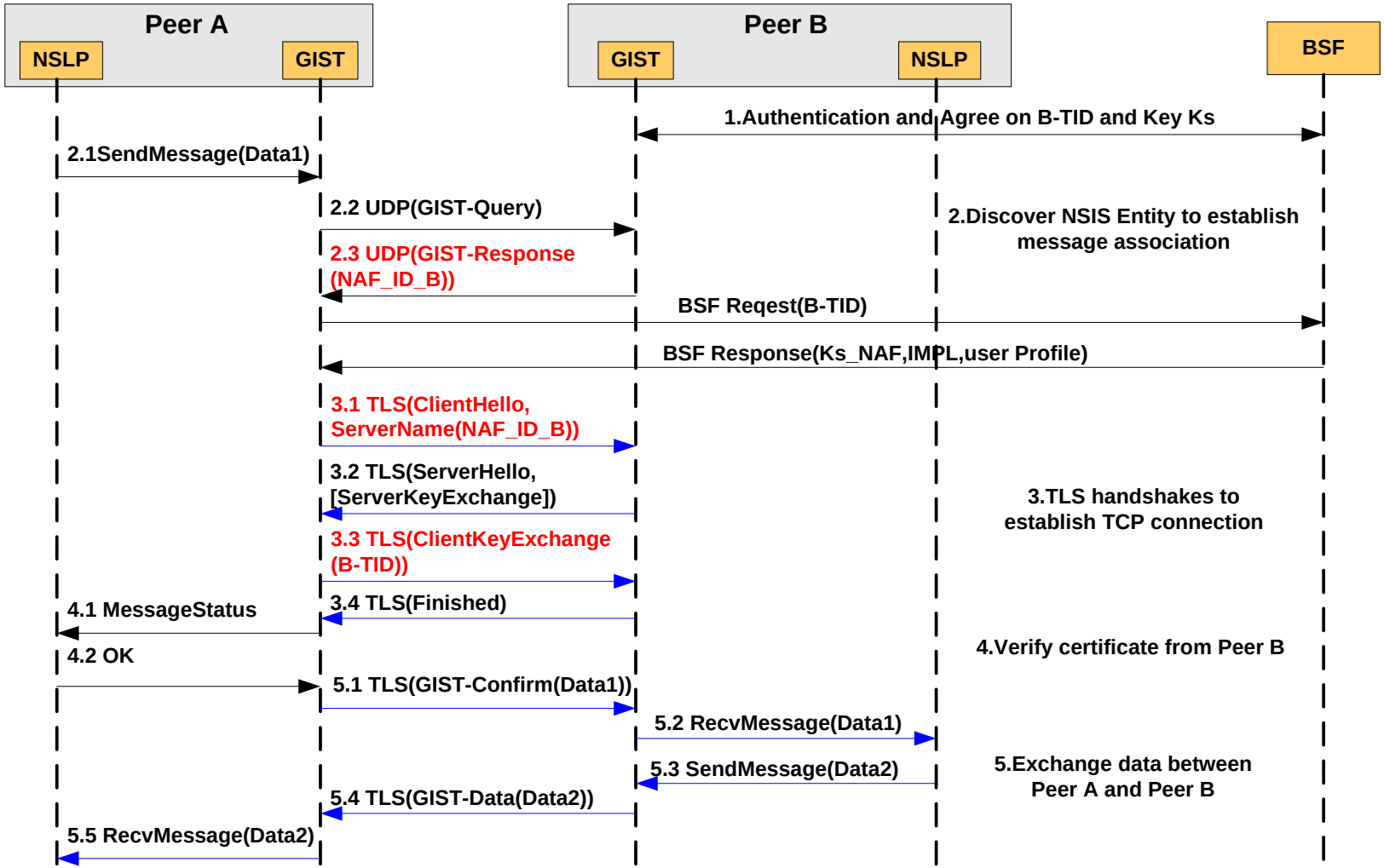
Drawback

- EAP methods should deal with fragmentation, reliability and re-transmission of the EAP data into the NAT/FW NSLP messages.
- integrating EAP into a NSLP application, a new NSLP payload object should be defined to carry the EAP packets.
- a NAT/FW policy aware node should be authenticated and authorized to be one side in an AAA NAT/FW Authorization session
  - the authorization decision is based not only on an authenticated identity, but also on the description of requested NAT/FW parameters

GBA(1/3)

- an authentication system with three parties: a trusted third party (called Bootstrapping Server Function or BSF), a client and server .
- isolate knowledge of long-term secrets and credentials to a single trusted node, the BSF.
- The actual servers (NAFs) do not have access to the clients' long-term credentials,

GBA(2/3)


Peer A
NSLP
GIST
Peer B
GIST
NSLP
BSF
1.Authentication and Agree on B-TID and Key Ks
2.1SendMessage(Data1)
2.2 UDP(GIST-Query)
2.Discover NSIS Entity to establish message association
2.3 UDP(GIST-Response (NAF_ID_B))
BSF Reqest(B-TID)
BSF Response(Ks_NAF,IMPI,user Profile)
3.1 TLS(ClientHello, ServerName(NAF_ID_B))
3.2 TLS(ServerHello, [ServerKeyExchange])
3.TLS handshakes to establish TCP connection
3.3 TLS(ClientKeyExchange (B-TID))
3.4 TLS(Finished)
4.1 MessageStatus
4.2 OK
4.Verify certificate from Peer B
5.1 TLS(GIST-Confirm(Data1))
5.2 RecvMessage(Data1)
5.3 SendMessage(Data2)
5.Exchange data between Peer A and Peer B
5.4 TLS(GIST-Data(Data2))
5.5 RecvMessage(Data2)

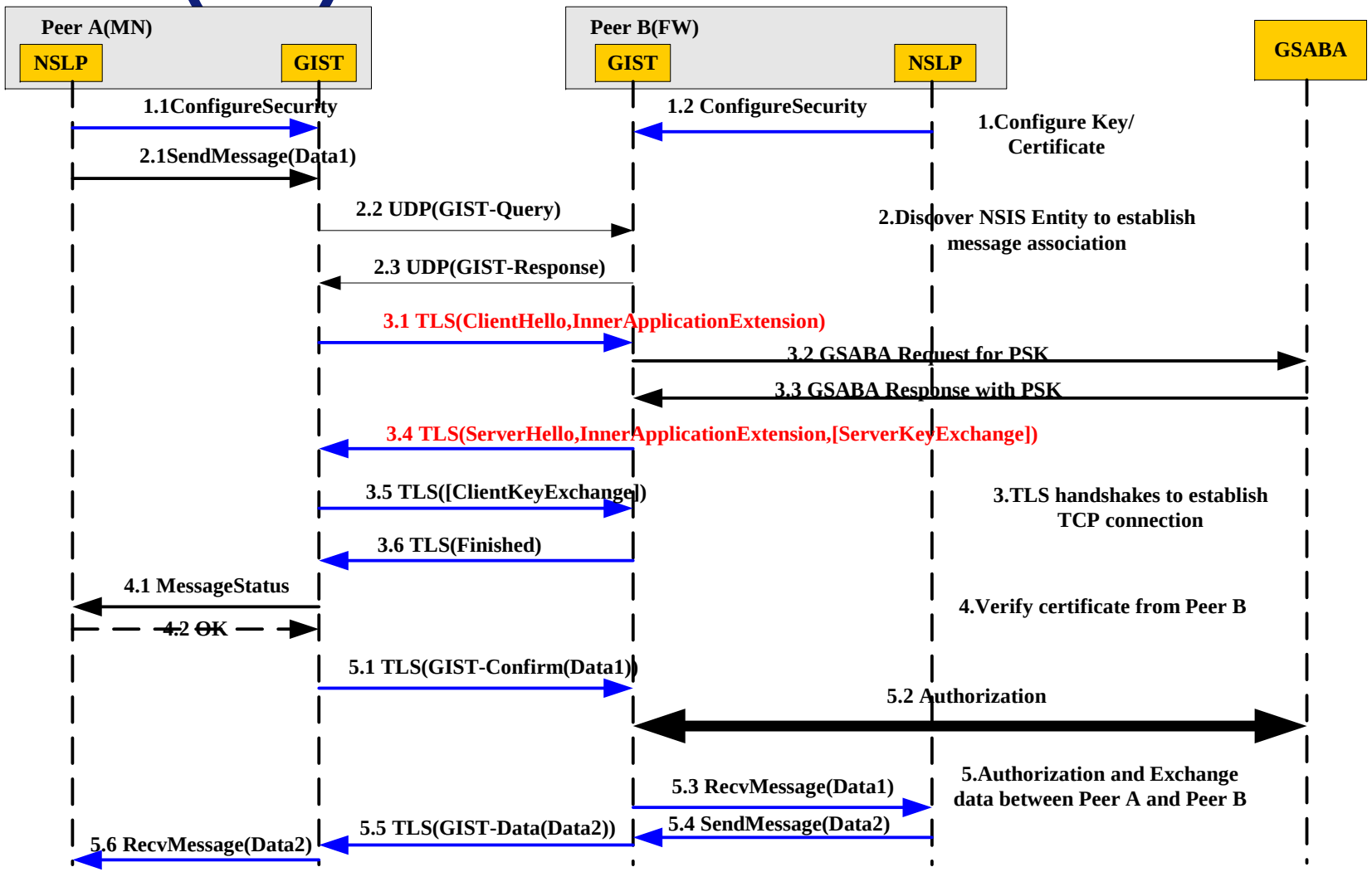
GBA(3/3)

- obtain FQDN through GIST exchange message
- use authentication entity identifier to request key material from AAA Infrastructure and establish trust relationship with authenticated entity.

GSABA(1/2)

- A generic service authorization and bootstrapping framework that leverages the use of the AAA infrastructure
- 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.

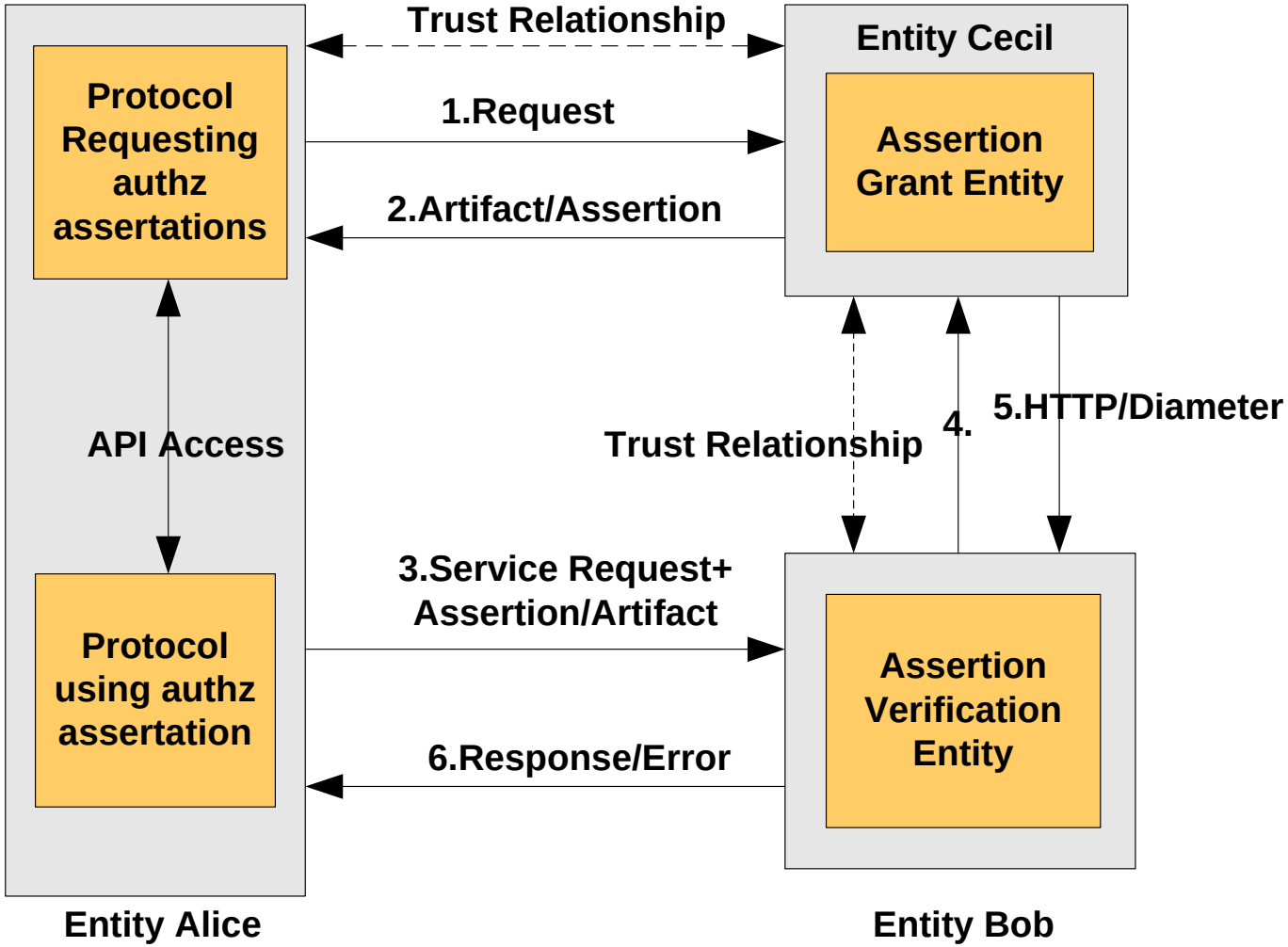
GSABA(2/2)


Peer A(MN)
NSLP
GIST
Peer B(FW)
GIST
NSLP
GSABA
1.1ConfigureSecurity
1.2 ConfigureSecurity
1.Configure Key/ Certificate
2.1SendMessage(Data1)
2.2 UDP(GIST-Query)
2.Discover NSIS Entity to establish message association
2.3 UDP(GIST-Response)
3.1 TLS(ClientHello,InnerApplicationExtension)
3.2 GSABA Request for PSK
3.3 GSABA Response with PSK
3.4 TLS(ServerHello,InnerApplicationExtension,[ServerKeyExchange])
3.5 TLS([ClientKeyExchange])
3.TLS handshakes to establish TCP connection
3.6 TLS(Finished)
4.1 MessageStatus
4.Verify certificate from Peer B
4.2 OK
5.1 TLS(GIST-Confirm(Data1))
5.2 Authorization
5.3 RecvMessage(Data1)
5.Authorization and Exchange data between Peer A and Peer B
5.5 TLS(GIST-Data(Data2))
5.4 SendMessage(Data2)
5.6 RecvMessage(Data2)

Authorization Token(1/5)

- computing authorization decisions might require a lot of time and also requires multiple messages between the entity enforcing the decisions and the entity computing the authorization decision.
- in a mobile environment these entities are physically separated - or not even in the same administrative domain.
- authorization token is one kind of authorization assertions, and trait-based authorization
  - existing authentication identifier that is used to be authenticated and be authorized through one protocol can be reused in another unrelated protocol exchanges.
  - usually used to complete authentication and authorization with the other security infrastructures mentioned above

Authorization Token(2/5)



Authorization Token(3/5)

- 1.Client requests authorization token from the third grant entity
- 2.The third grant entity reply to client with the corresponding token
- 3.Client sends authorization request to assertion verification entity with client's token
- 4.Assertion verification entity exchange message with the third grant entity to validate token
- 5.In case validating token, assertion verification entity responds to client with authorization result.

Authorization Token(4/5)

A	B	r	r	Type	r	r	r	r	Length
AUTH_ENT_ID									
SOURCE_ADDR									
DEST_ADDR									
START_TIME									
END_TIME									
AUTHENTICATION_DATA									

Authorization Token(5/5)

- Authorization token mainly consist of authorization identifier, source address, destination address, session start time, end time and authentication data. and policy element of session is included in authentication data.
- In symmetric share key environment, token can be used with AAA infrastructure, AUTH_ENT_ID is usually IPv4 address, IPv6 address or FQDN,NAI.
- In public key environment, token can be used with digital certificates, AUTH_ENT_ID is usually X509_V3_CERT or PGP_CERT.

Comparison among existing security infrastructures

	TLS+X.509	EAP	GBA	GSA BA
source for Key Materials	X.509	AAA	AAA	AAA
Authorization Token	Not necessary	Not necessary	Not necessary	Need
Layer to establish trust relationship	GIST Layer	GIST Layer or NSLP layer	GIST Layer	GIST Layer and NSLP layer
Integration with AAA	Hard	Easy	Easy	Easy
Authentication signaling overhead	small	large	small	small

Thank you!