

ETSI-BSM work on Satellite Communication Network Security

*Future Security Workshop: The threats, risks
and opportunities*

*Sophia Antipolis
16-17 January 2006*

Dr. Haitham S Cruickshank

University of Surrey

h.cruickshank@surrey.ac.uk

<http://www.ee.surrey.ac.uk/Personal/H.Cruickshank/>



Presentation overview

- *Introduction to BSM architecture.*
- *Threat analysis in BSM.*
- *Security architecture and various security scenarios.*
- *Some security challenges in BSM network such as PEPs and multicast.*
- *Conclusions and future plans in BSM WG.*

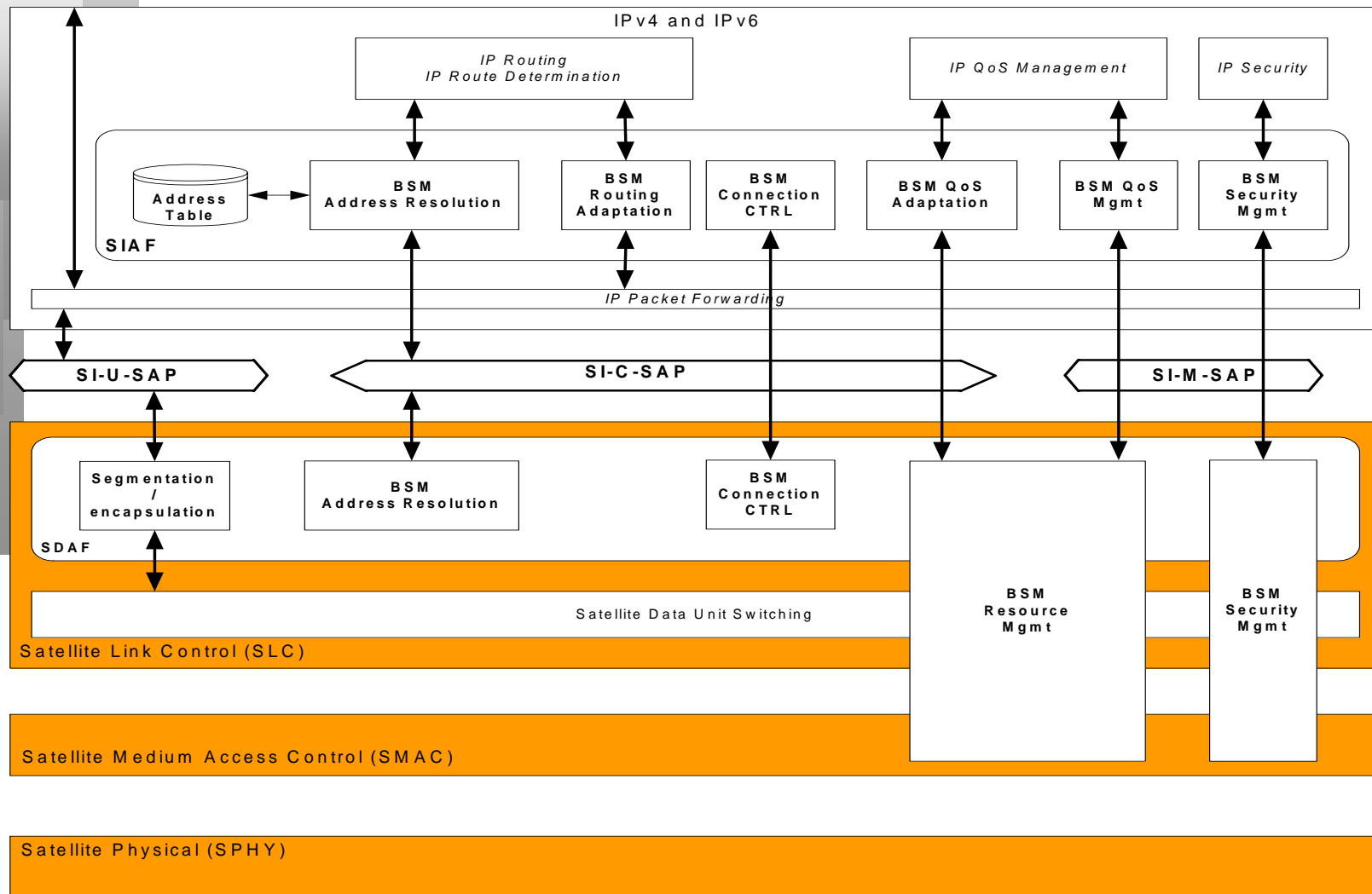
Introduction to BSM STF283 - Security

- *The ETSI Broadband Satellite Multimedia (BSM) working group aims to develop broadband satellite services based on complete interworking with the Internet Protocol (IP).*
- *An important feature of BSM is the Satellite Independent Service Access Point interface or SI-SAP interface:*
 - *This interface provides the BSM with a layer of abstraction for the lower layer functions*
- *Part of BSM STF 283 work focuses on the security architecture for BSM networks (ETSI TS 102 465).*

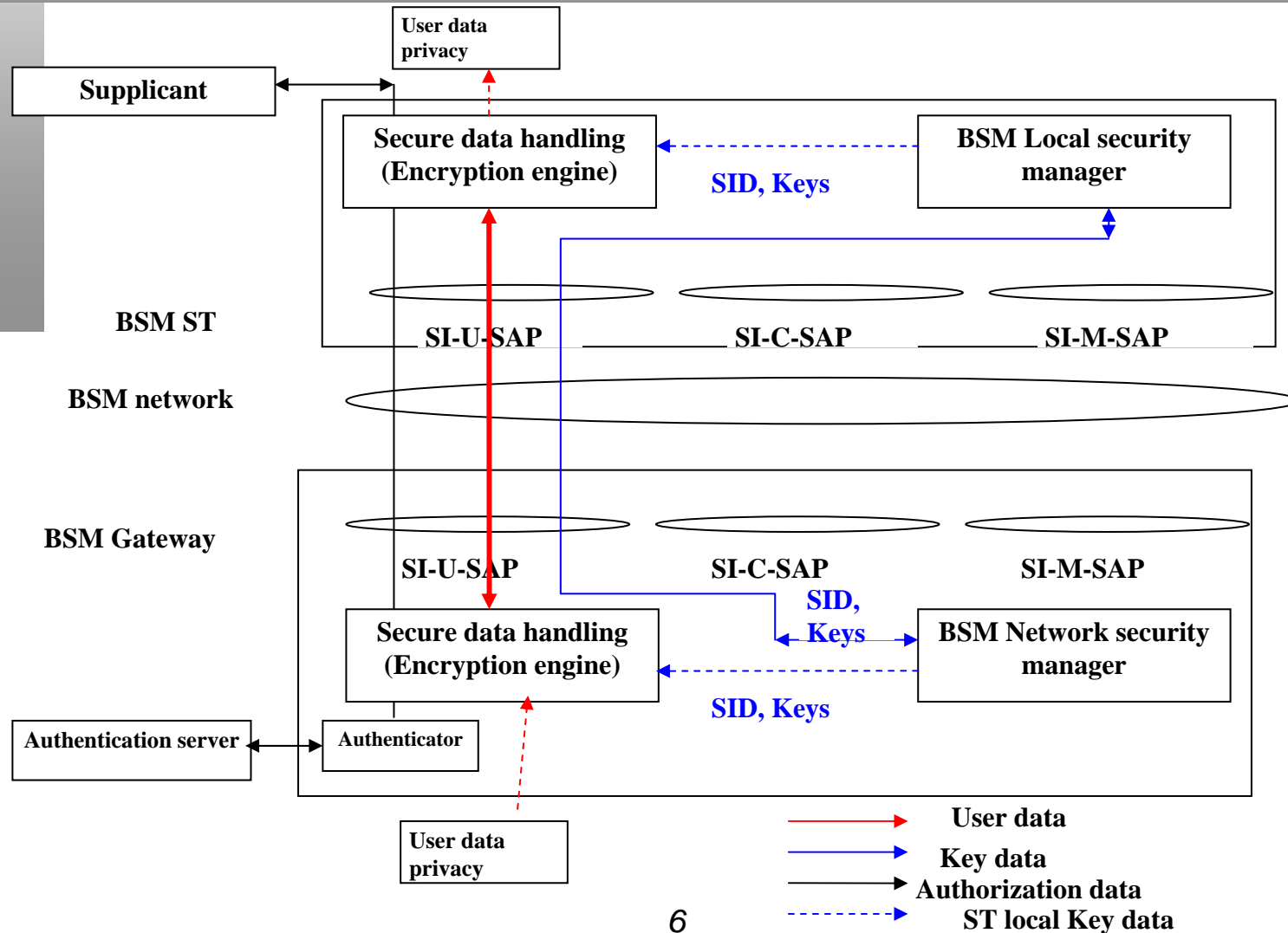
Threats and security requirement in BSM networks

- **Network threats:** Including passive and active threats:
 - *In satellite broadcast networks (such as BSM), passive attacks need particular attention, such as eavesdropping or monitoring of transmissions.*
- **Software threats:** Many systems fail because of mistakes in software implementation.
- **Hardware threats:** All hardware systems including hosts (e.g. client stations), satellite terminals and network equipment (e.g. routers and firewalls) can provide a way of attack if not properly configured.
- **Human threats:** Insider and outsider attacks.
- **BSM security deals with the above threats with the focus on networking issues.**

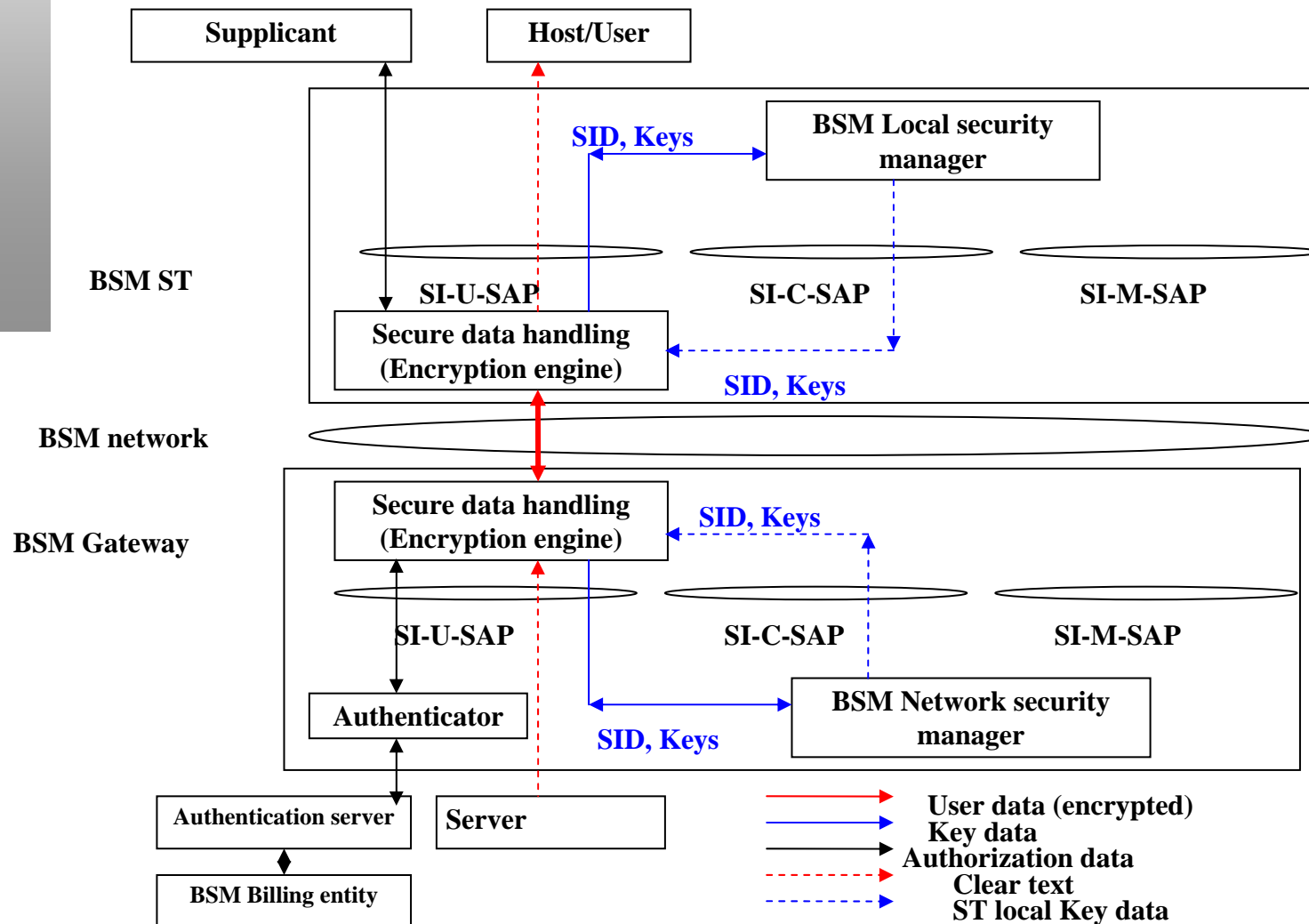
BSM general architecture



Architecture case 1: IPsec and security entities in BSM



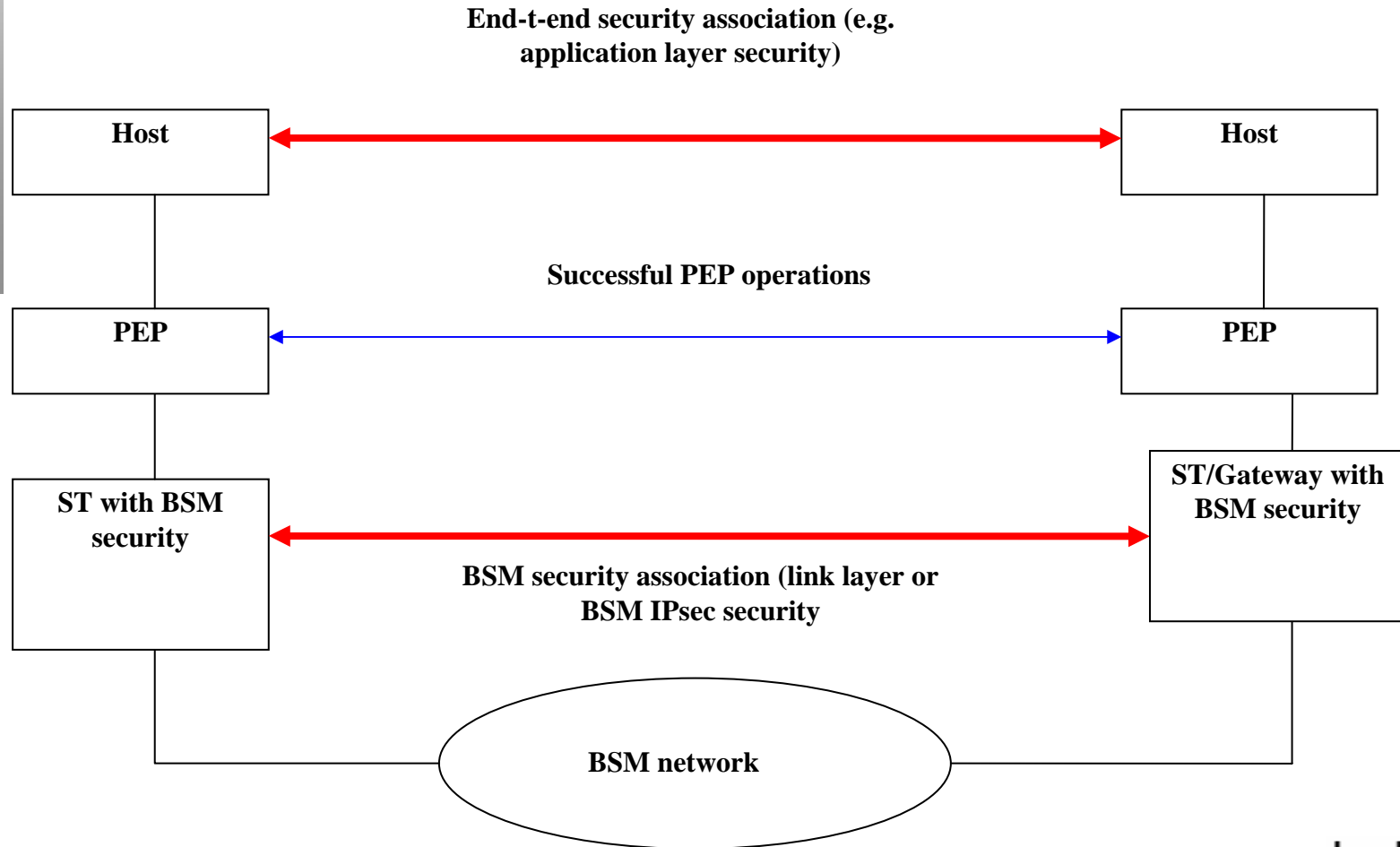
Architecture case 2: Mixed link layer security entities



Challenges for using security with Performance Enhancing Proxies (PEPs)

- *A Performance Enhancing Proxy (PEP, RFC 3135) is used to improve the performance of the Internet protocols on network paths where native TCP performance suffers due to characteristics of a link such as satellites.*
- *The most detrimental negative implication of PEPs is breaking the end-to-end semantics of a connection:*
 - *Therefore it disables end-to-end use of IPsec*
- *In BSM networks, PEPs should be used in the following configurations:*
 - *With Link layer security (such as DVB-RCS security)*
 - *With IPsec being performed closer to BSM ST/Gateway than the PEP*

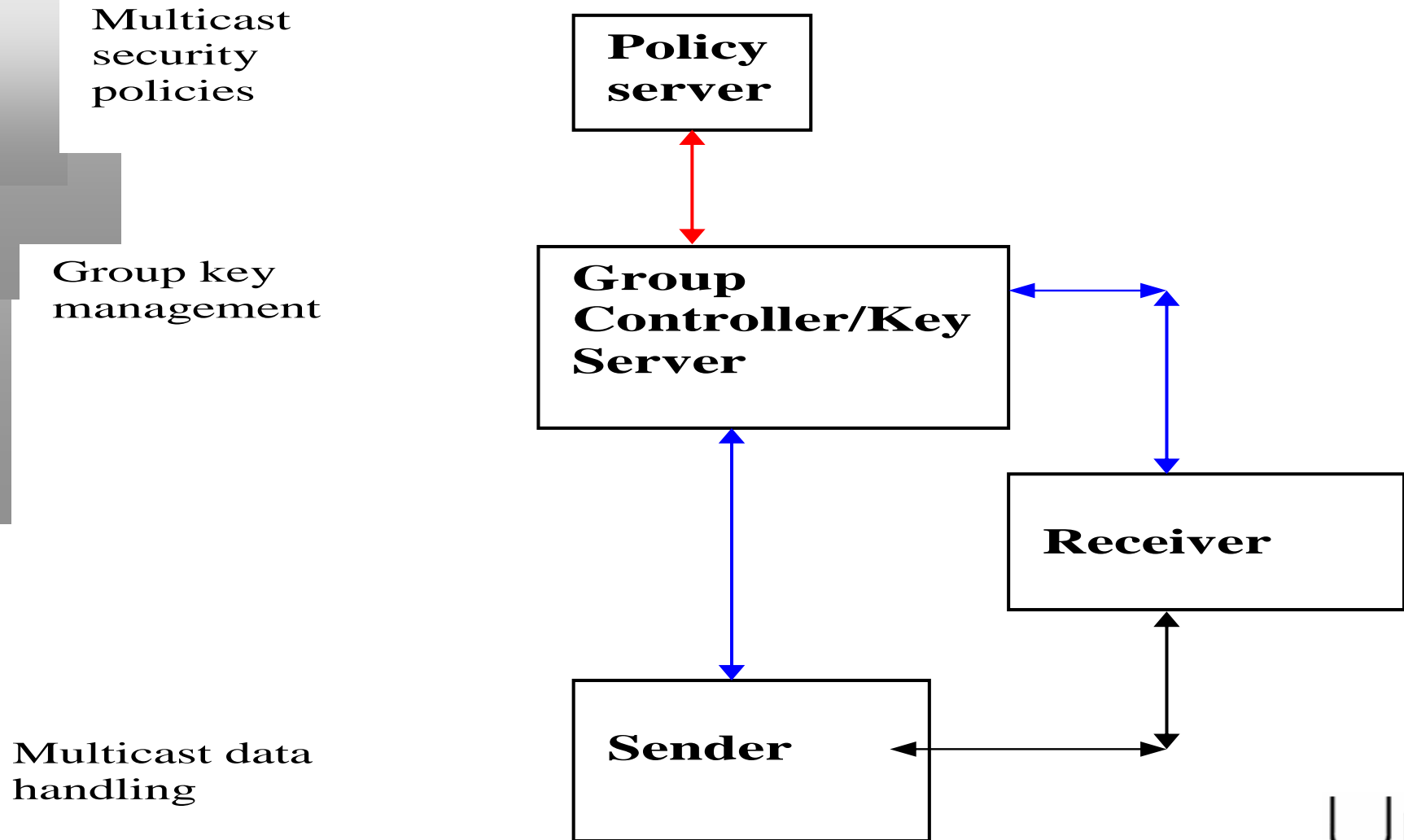
Suitable security associations for interworking with PEPs



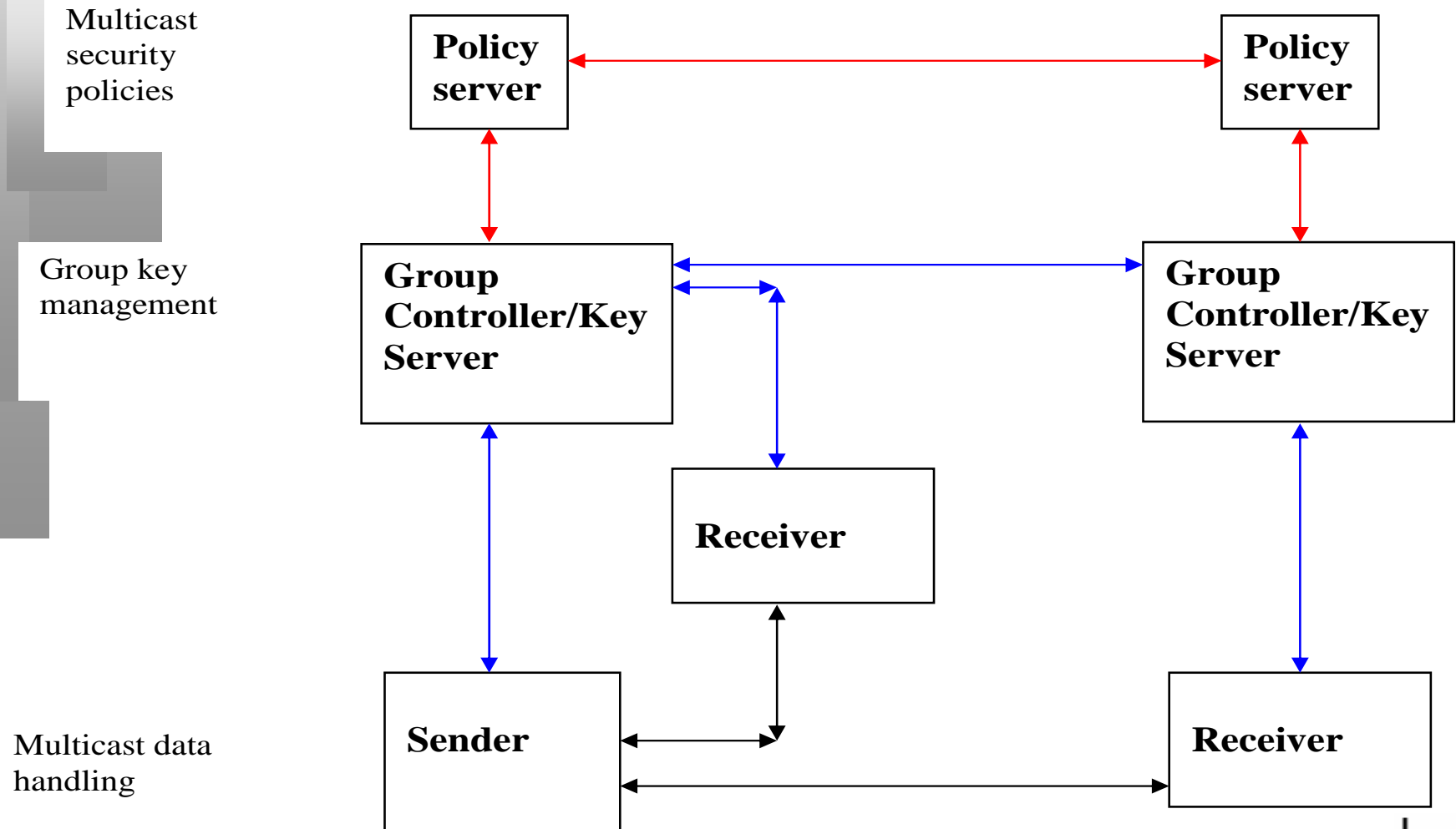
Challenges in Secure multicast over satellites

- *Secure multicast is a difficult problem. There are many open issues:*
 - *IPsec with multicast between BSM security gateways*
 - *Key management architecture for large groups*
 - *Security policies creation and enforcement*
 - *Centralised versus distributed architectures*
- *BSM multicast security architecture will aim to provide a balanced solution between existing link layer (such as DVB-RCS) and network layer (such as IPsec) solutions:*
 - *Interactions through the SI-SAP interface have to be carefully thought.*

Secure Multicast architecture - Centralised



Secure Multicast architecture - Distributed



Liaison with EU IST projects

- *The work in ETSI BSM on security will not be complete without full liaison with relevant IST projects:*
 - *The aim is to achieve co-ordination of work between BSM and these projects*
- *One example of such collaboration is the EU NoE called SATNEX project (Satellite Communications Network of Excellence).*
- *Other examples of EU projects are SATLIFE and SATSIX.*

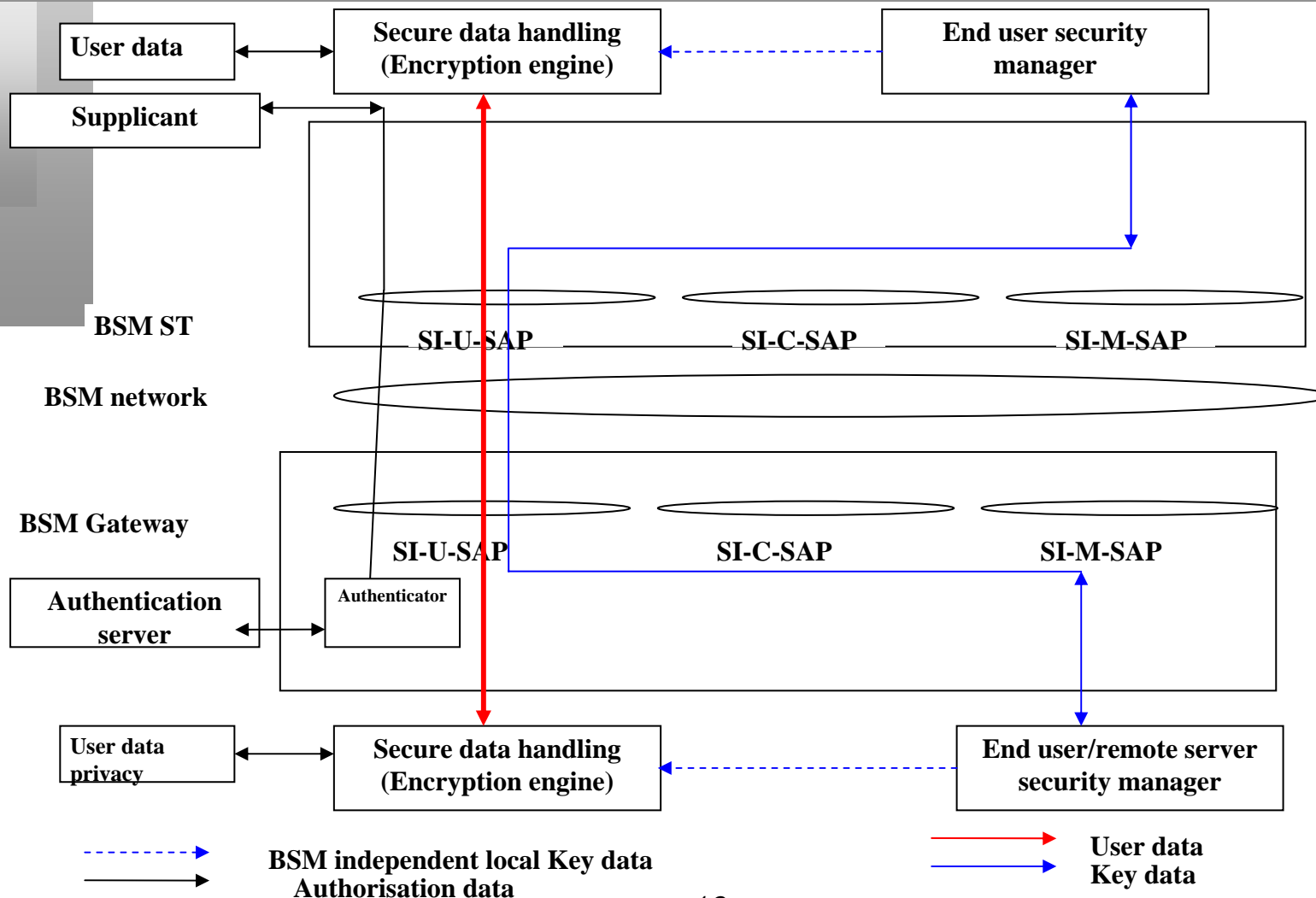
Conclusion

- *Interworking with the IPsec and link layer security is critical for the success of BSM specifications.*
- *Security interactions through the BSM SI-SAP interface has been defined.*
- *There are future challenges in secure multicast over satellites:*
 - *Next phase in BSM security work will focus on multicast issues (New ETSI TS 102 466)*

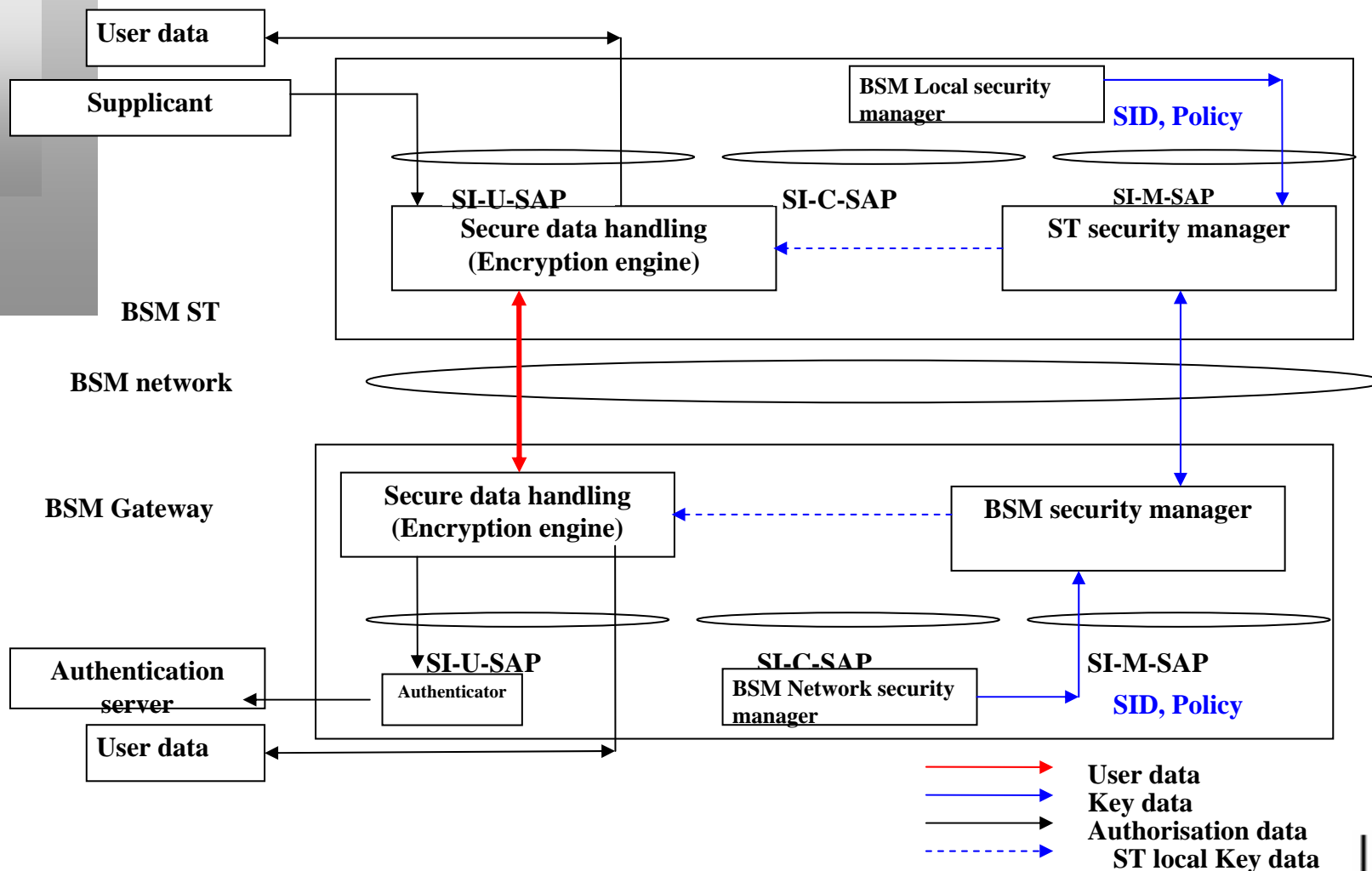


Extra slides

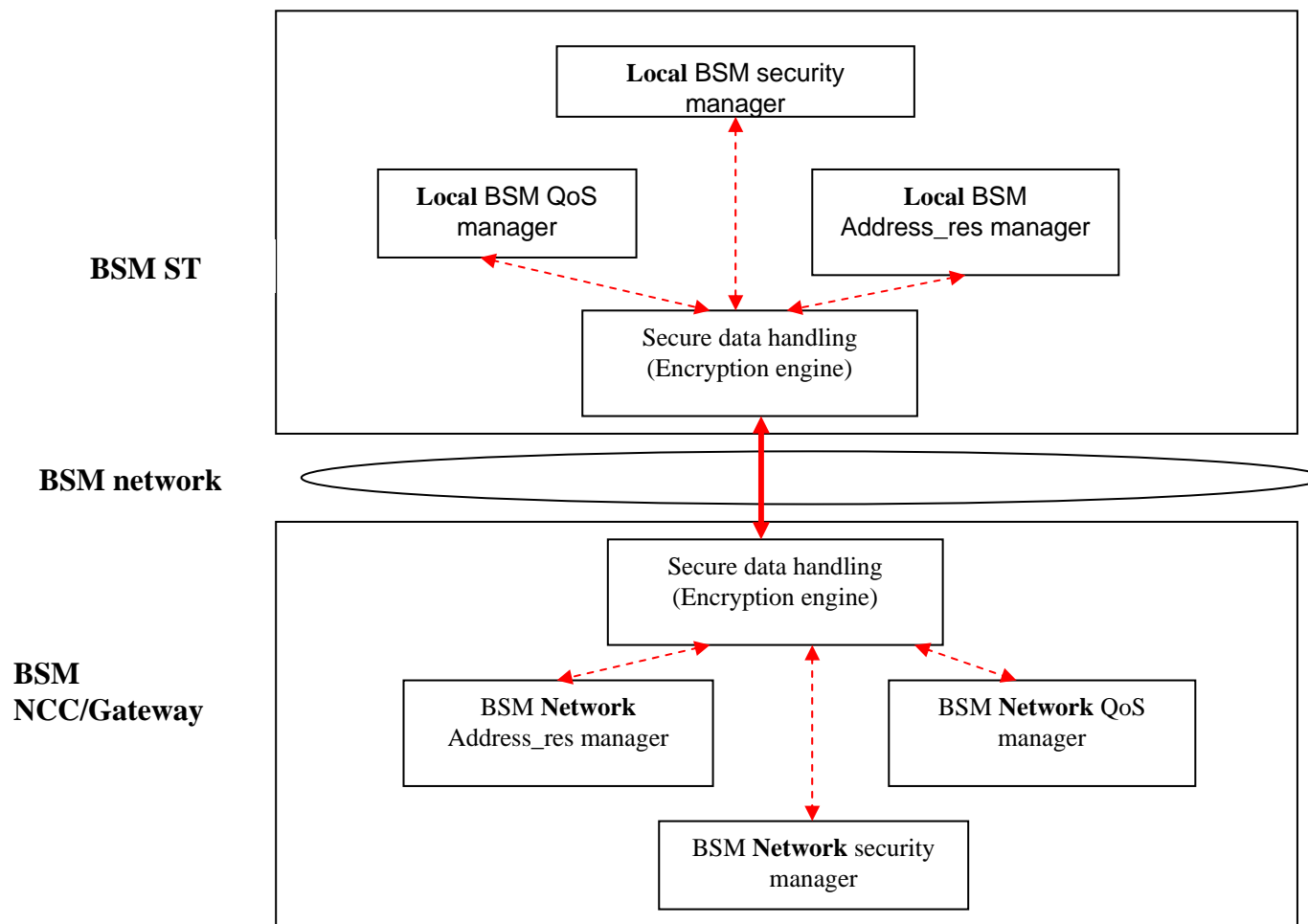
Architecture case 3: End-to-end security, transparent to BSM



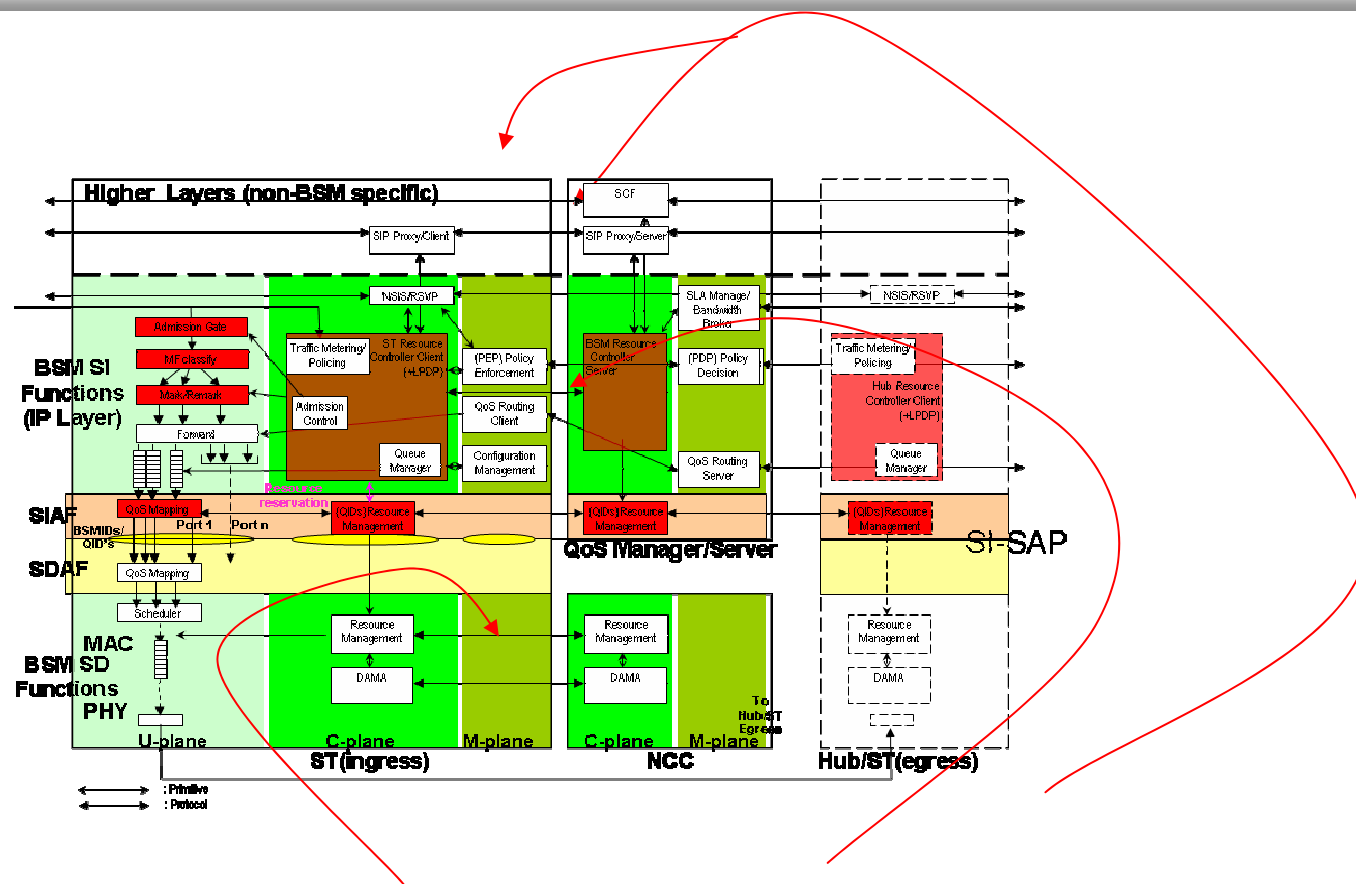
Architecture case 4: link layer security, transparent to BSM



Interactions between security and QoS entities in BSM - 1



Interactions between security and QoS entities in BSM - 2



Interactions between security and Address management entities in BSM

