

Secure Multicast in Broadband Satellite Multimedia (BSM) Networks

**IST Summit 2007 Workshop –
IP networking over satellites”**

Budapest, Hungary

Dr. Haitham Cruickshank

5/07/2007



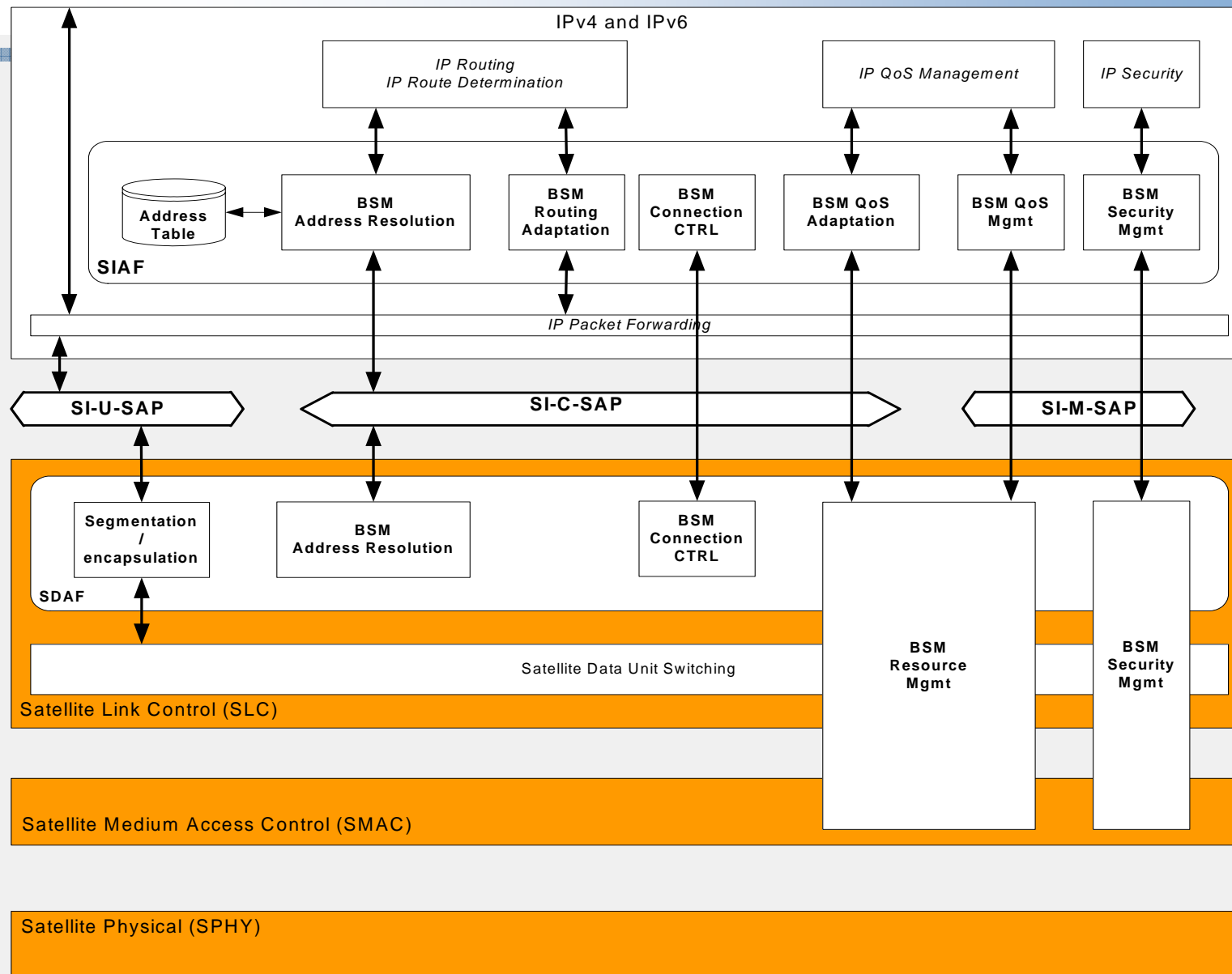
Contents

- Security requirements in satellite networks
- Introduction to ETSI Broadband Satellite Multimedia (BSM) security architecture
- Four security architectural cases
- Conclusions

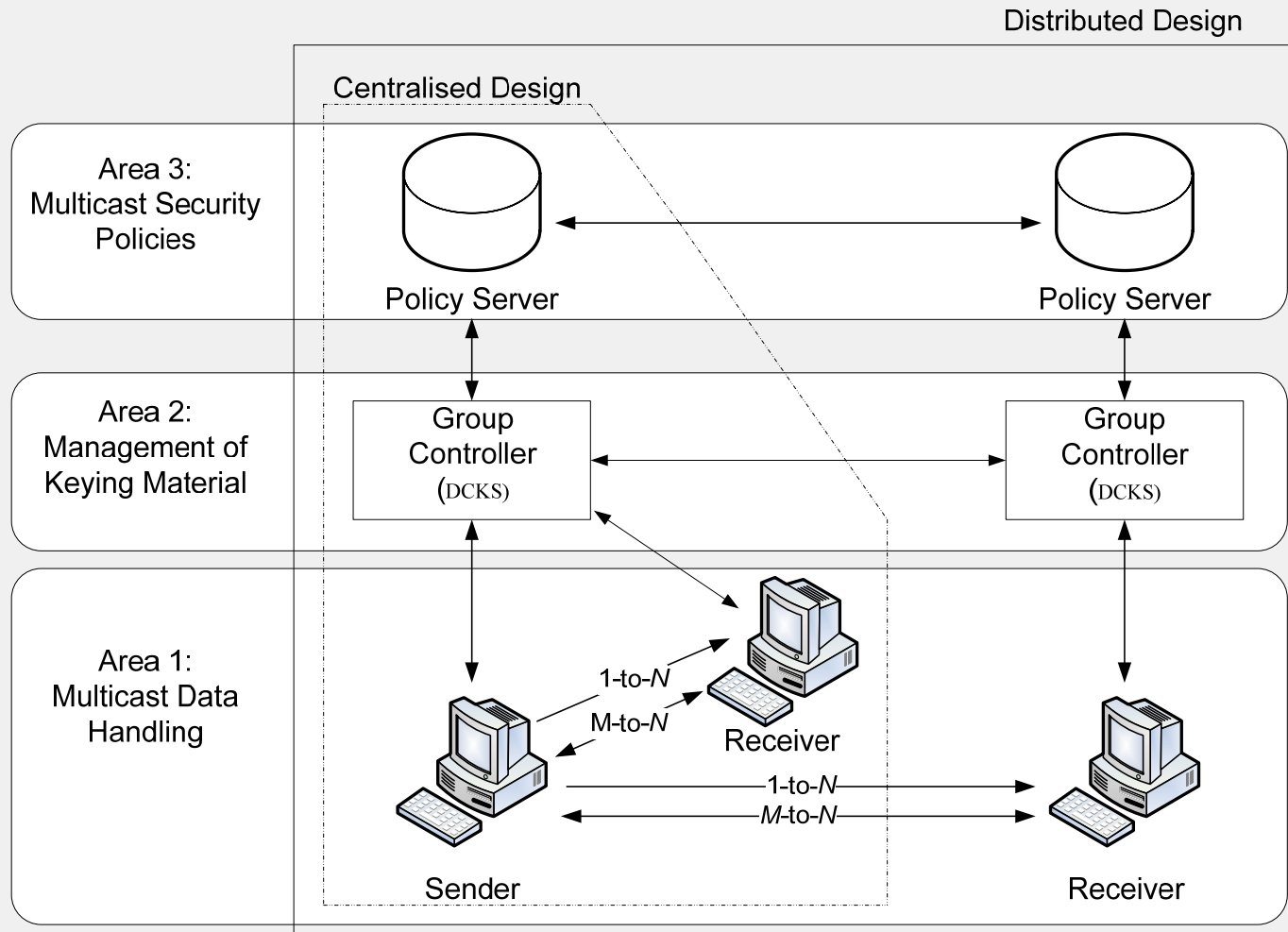
Satellite security service requirements

- **Data confidentiality** is the major requirement against passive threats (using encryption).
- **BSM terminal authentication** (link layer). It is performed during the initial key exchange and authentication phase.
- **For active threats:** Source authentication and data integrity are required, using techniques such as message authentication code and digital signatures.
- **End-to-end security** (such as IPsec) and **link layer** security should work in parallel without obstructing each other.
- **Decoupling of key management** functions from satellite data encryption. This will allow the independent definition of these systems such as the re-use of existing security management systems (IETF or DVB-RCS).

BSM Protocol Stack - Security

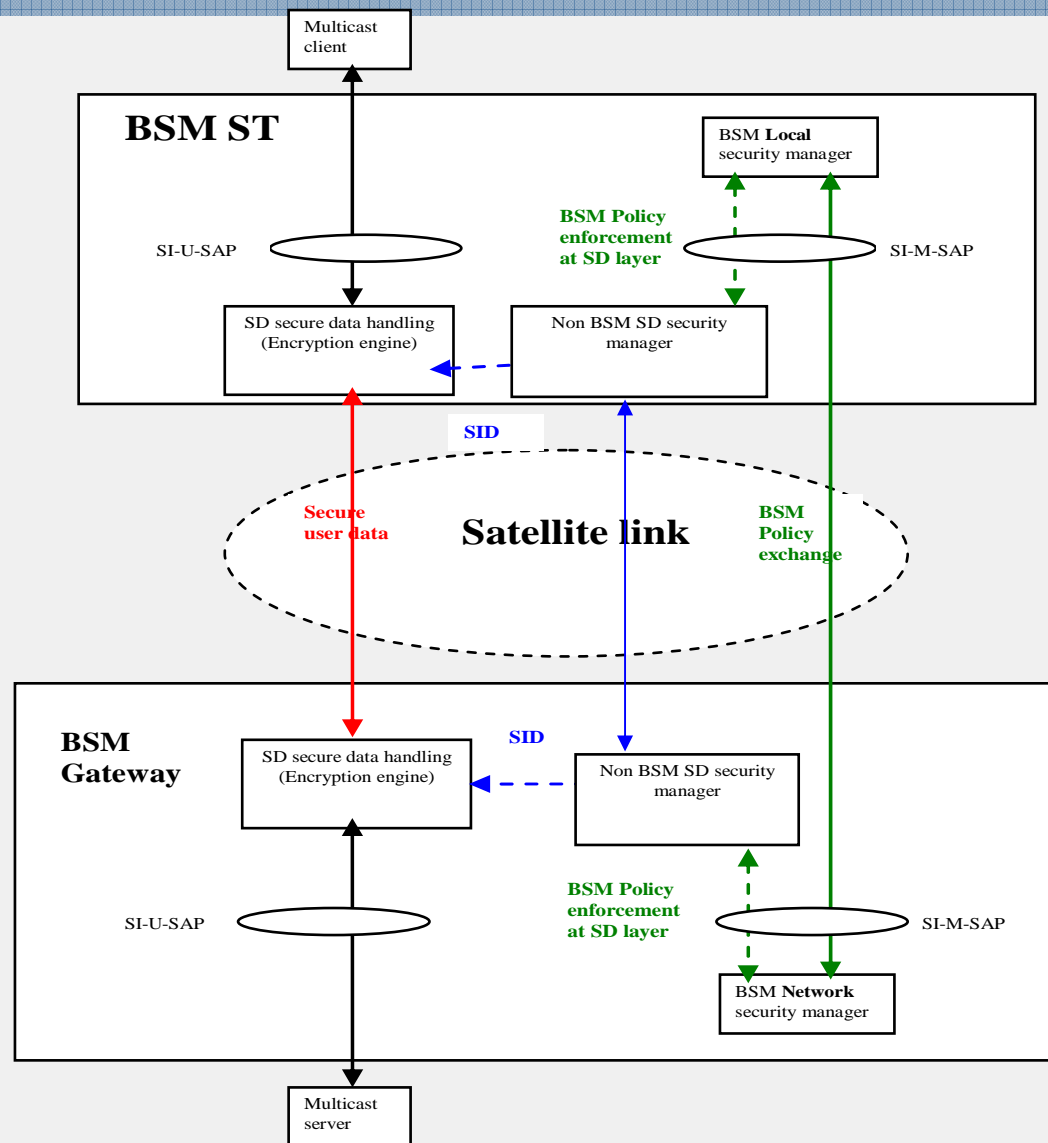


General secure multicast problem areas

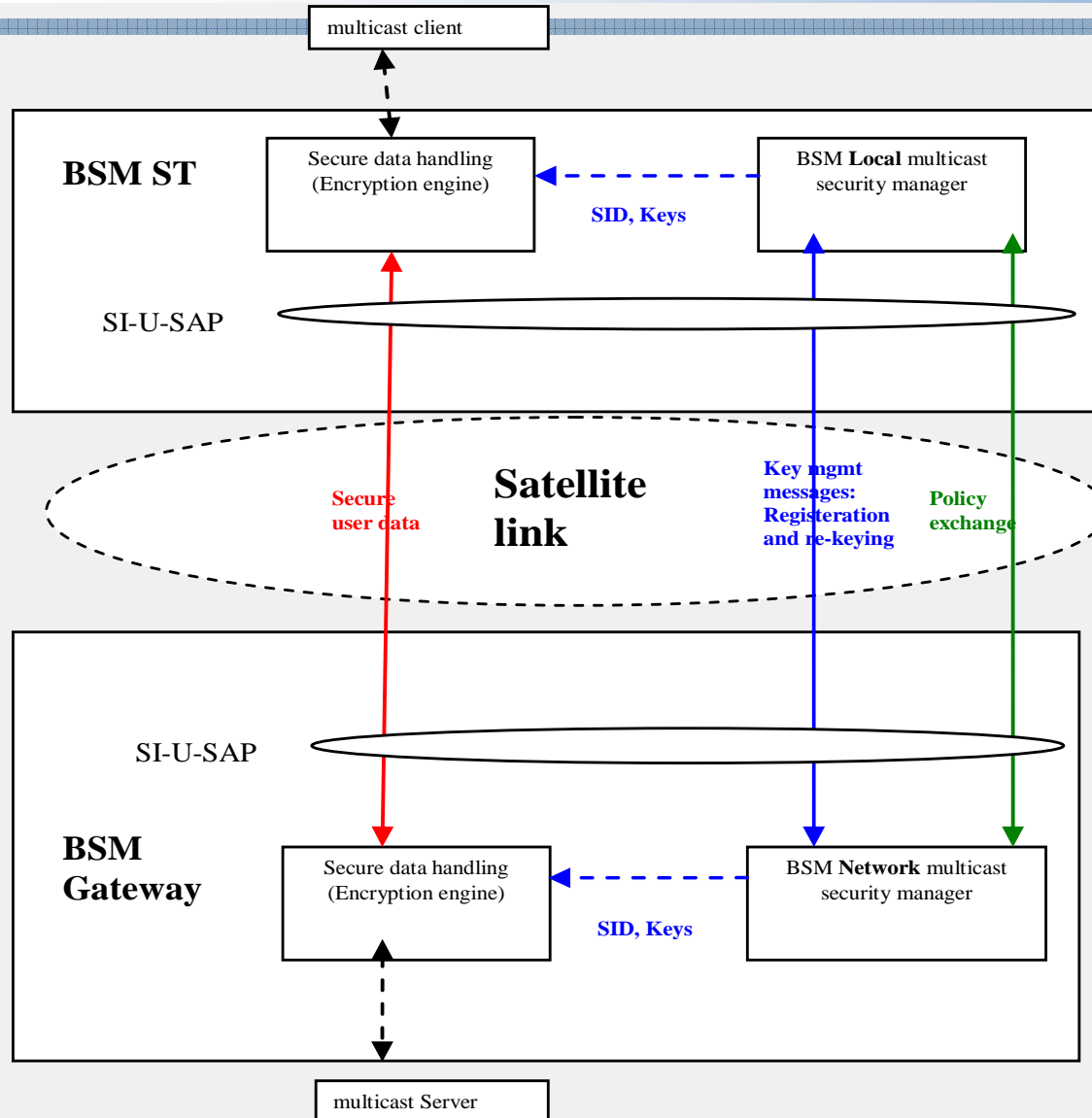


1-to-N : Only a single sender is allowed to transmit data to the group
M-to-N : Many group members can transmit data to the group

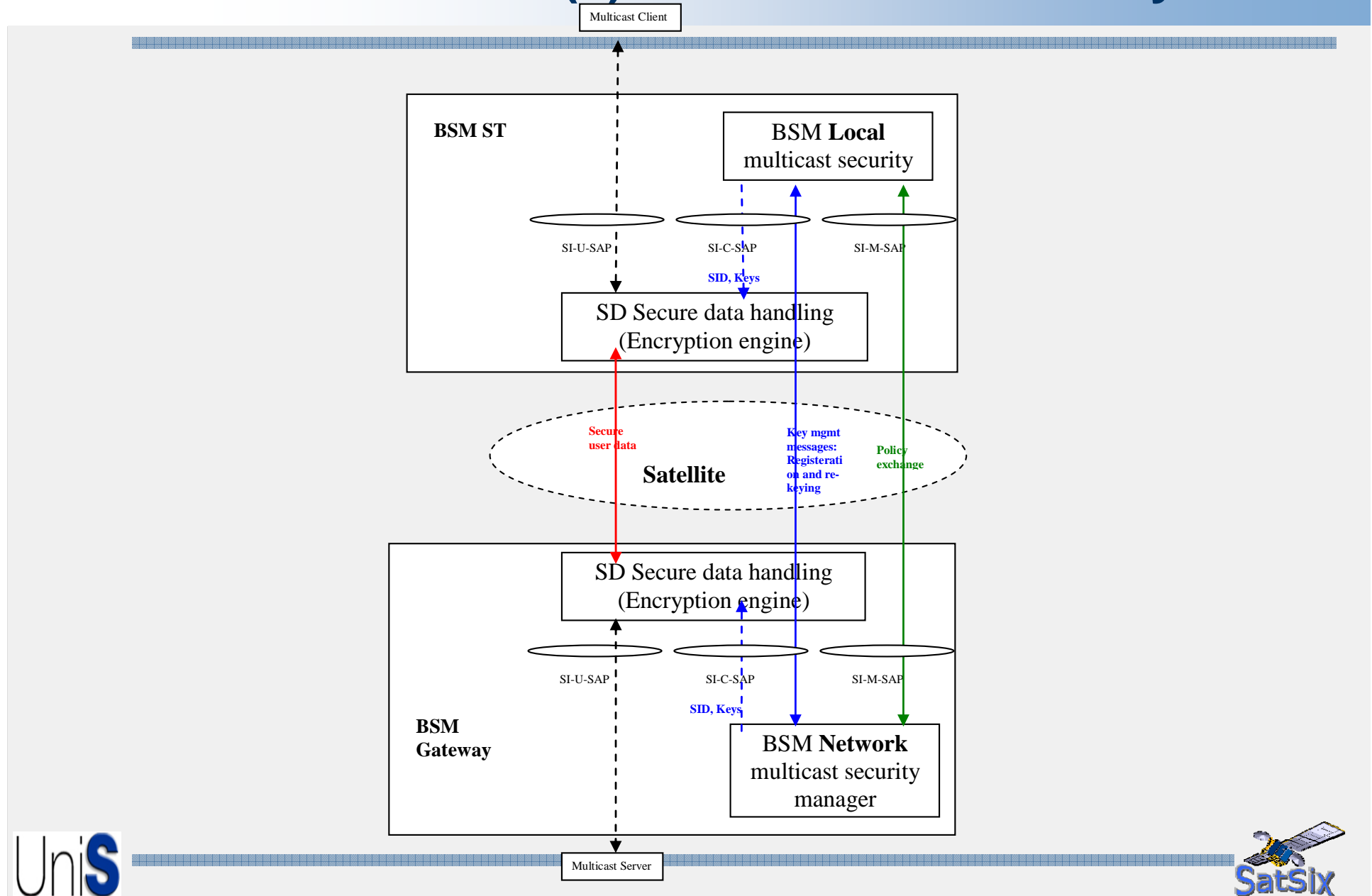
Architecture case (1): Secure satellite link layer (SD layer)



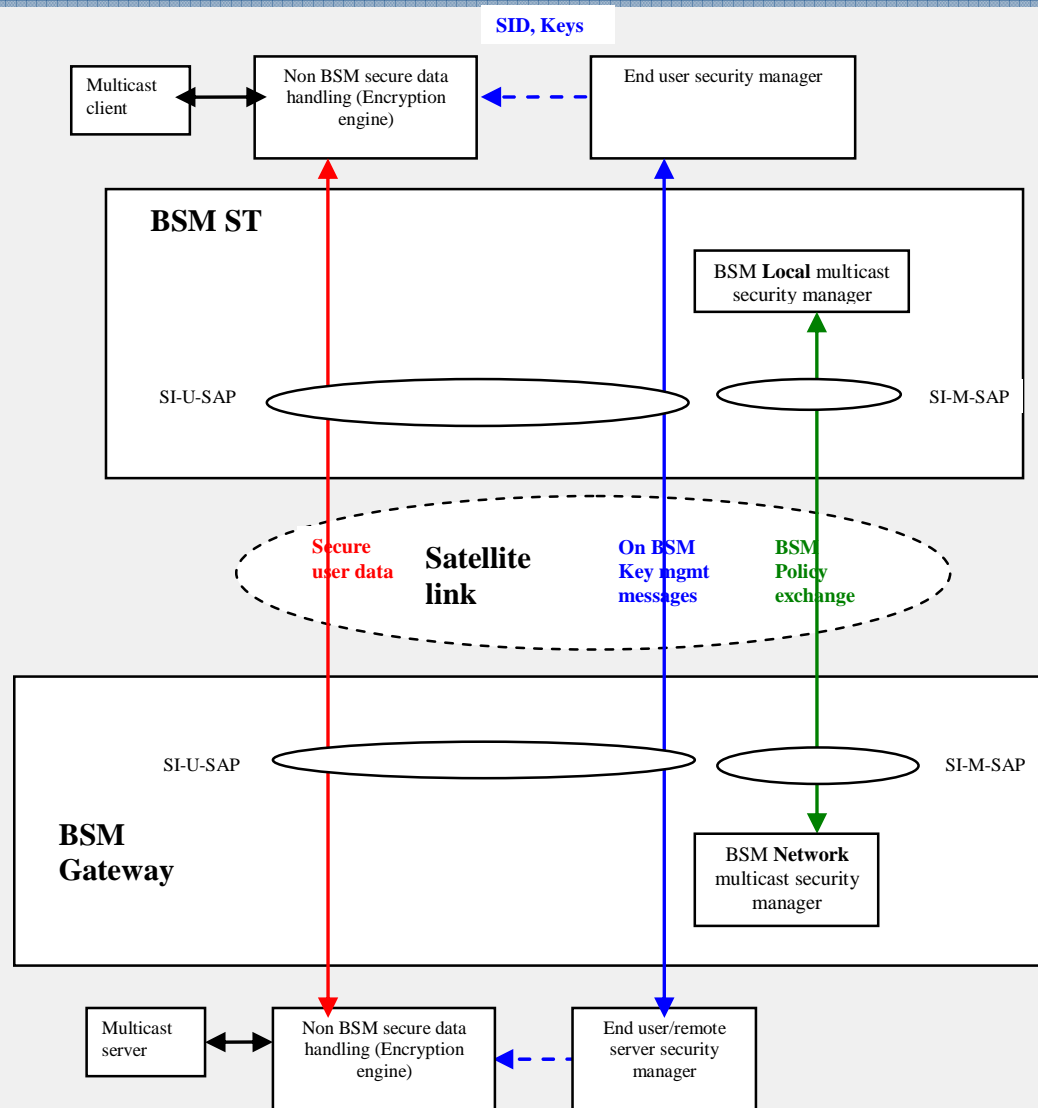
Architecture case (2): IPsec in satellite networks (SI layer)



Architecture case (3): Mixed SI/SD security



Architecture case (4): End-to-end security



Conclusions

- BSM security architecture demonstrates a close integration of satellite networks with the Internet.
- Satellite specific security system such as DVB-RCS and ULE security can also be integrated into the BSM architecture.