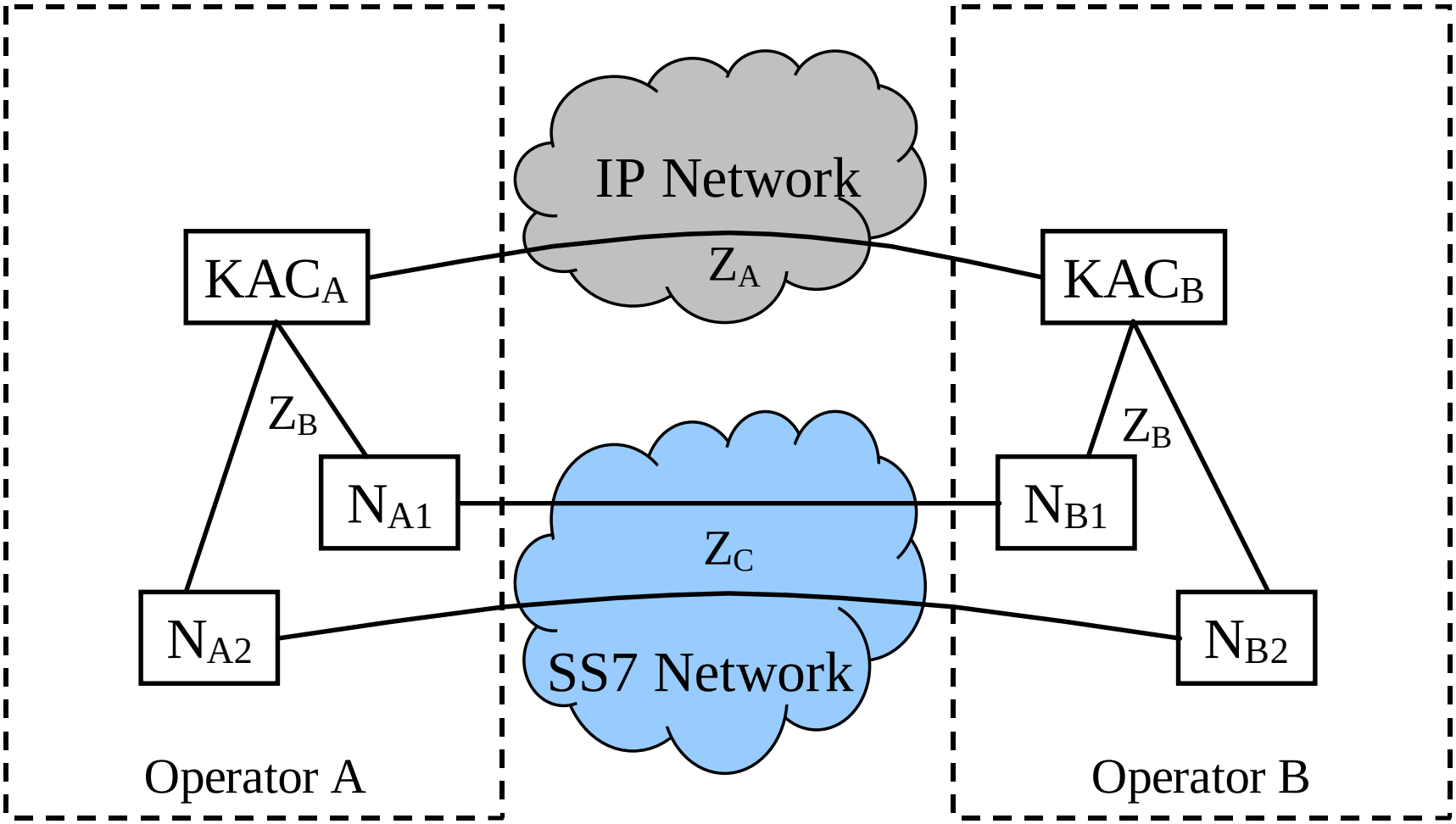
Key Management for MAP Security

ERICSSON

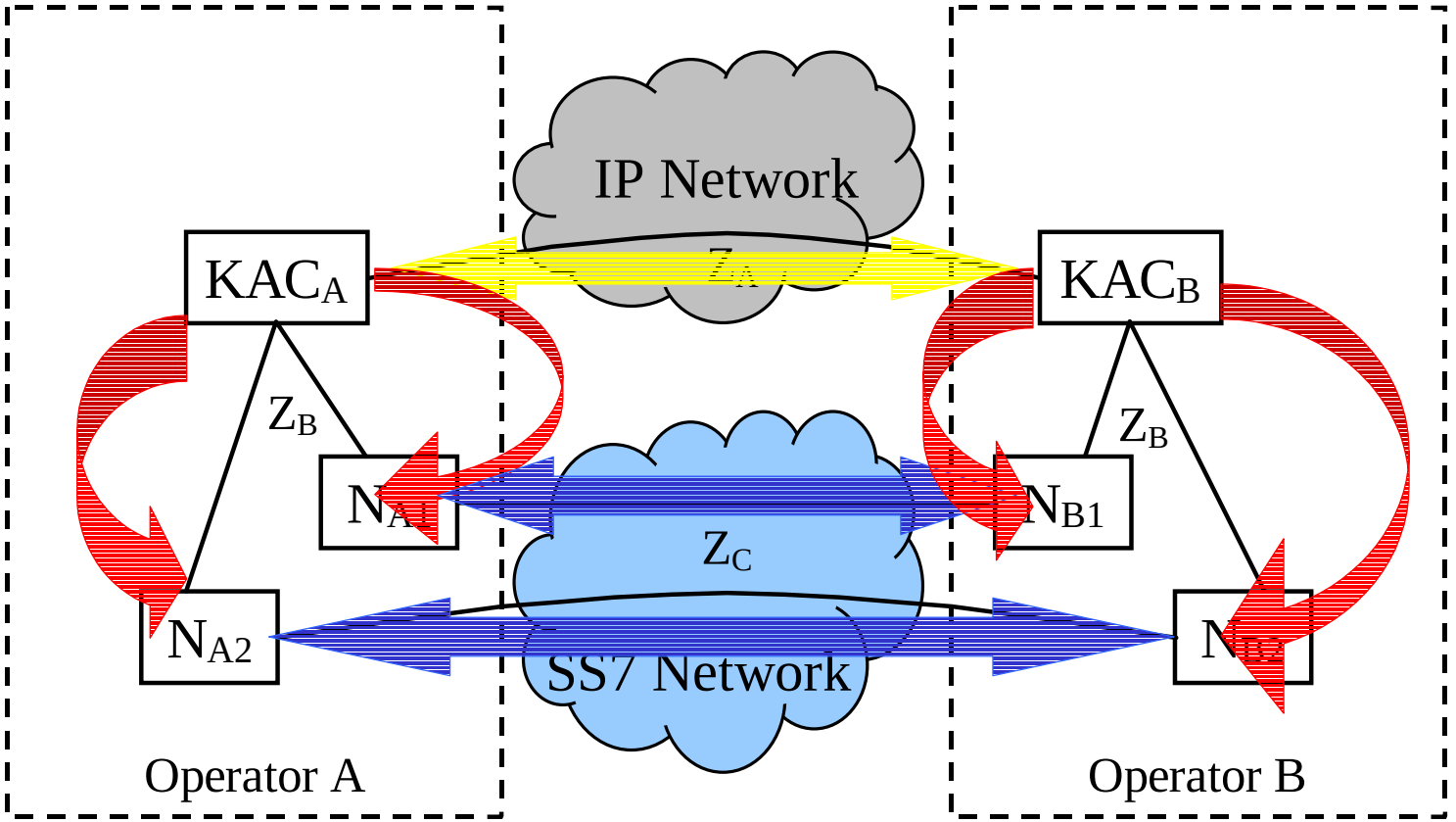
Overview

S3-000476



Key Management for MAP Security

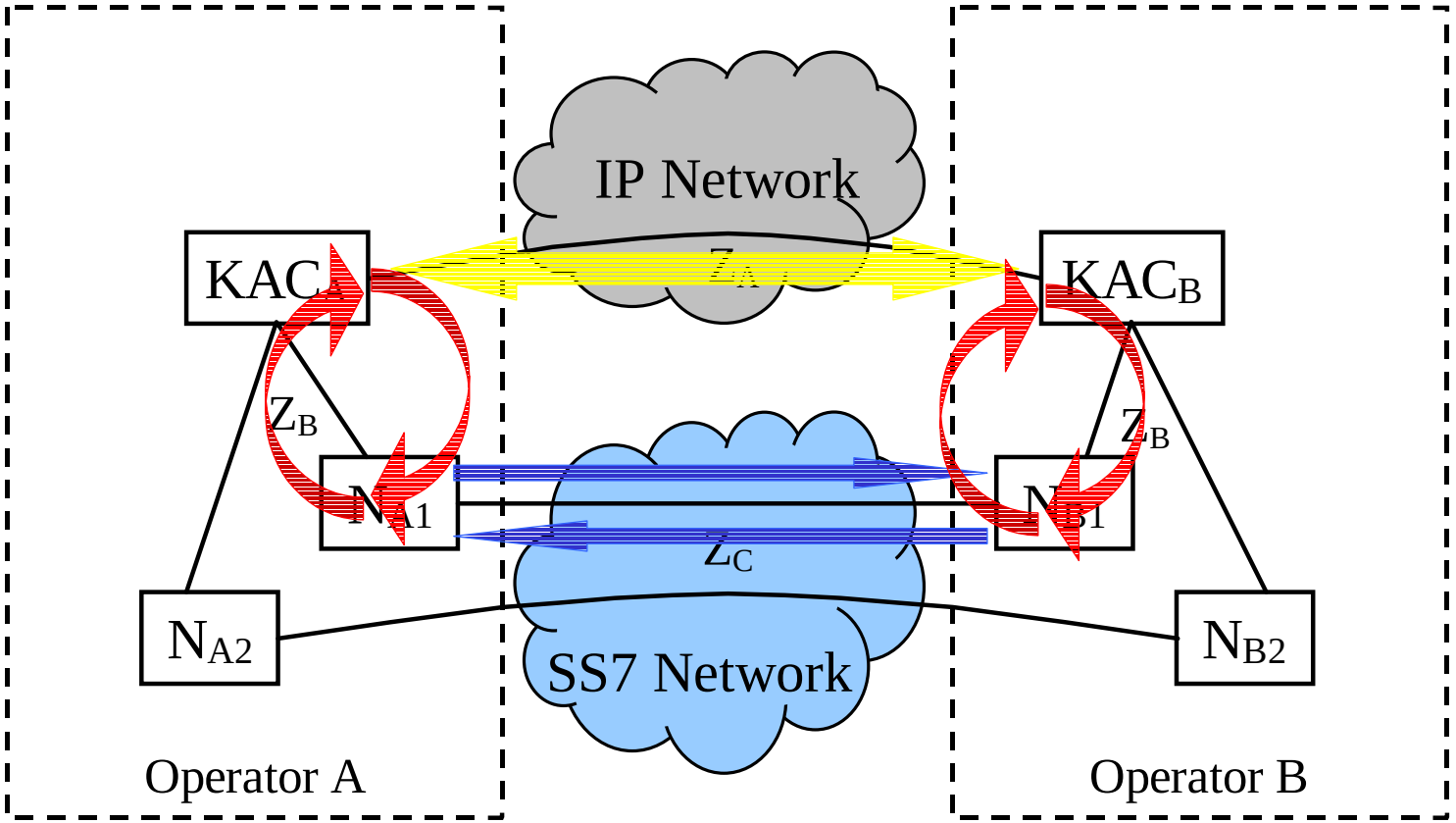
ERICSSON



KAC PUSH ...

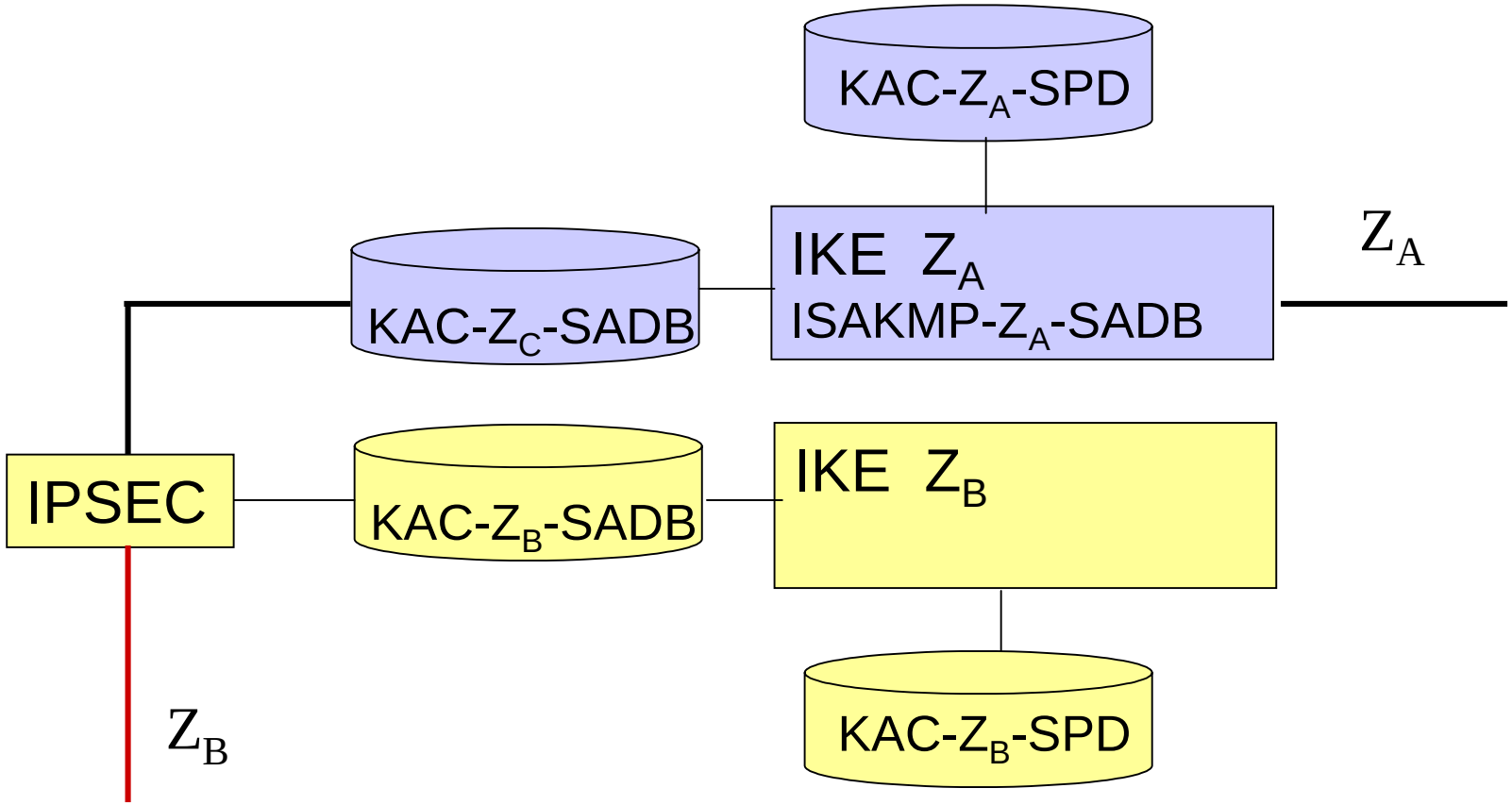
Key Management for MAP Security

ERICSSON



… or NE PULL ?

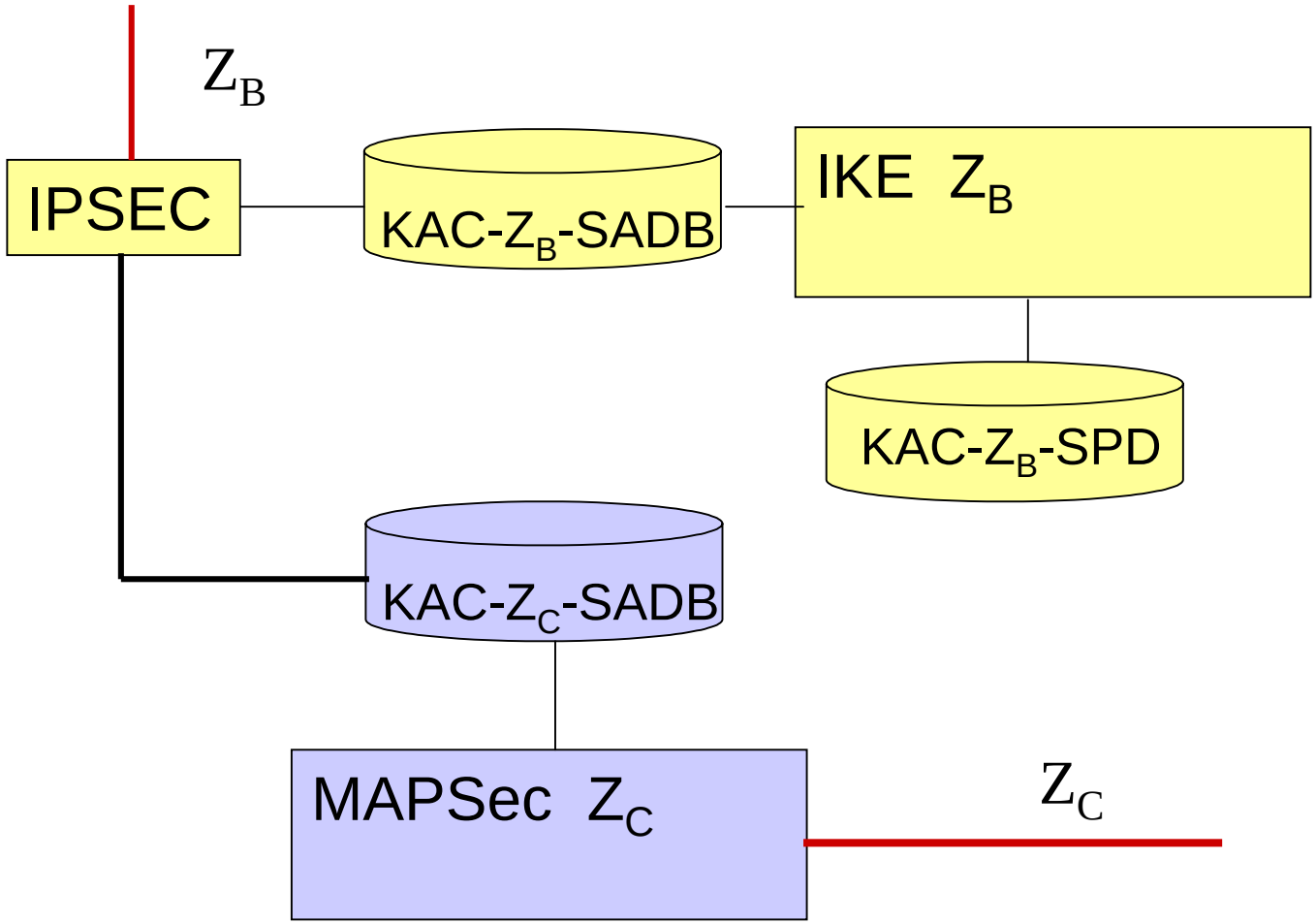
Key Administration Center



Key Management for MAP Security

ERICSSON

Network Element



Tentative MAP-SA and Header Content

SA Info

- Confidentiality Key.
- Encryption Algorithm
- Integrity Key.
- Mac Algorithm
- MAP Protection Profile
- SA Lifetime

Header Info

- Source PLMN_ID
- SPI (Security Parameters Index)
- Time Stamp
- IV (If needed)

Deployment Issues

- A simple-to-introduce mechanism for trust distribution between operators is needed.
- Not all operators will introduce MAPSec at the same time
- Not all nodes within one operator's network will support MAPSec at the same time.
- A mixed environment of IPv4 and IPv6 may exist.
- Interoperability

Work Items / Issues I

- Write stage 2 description of MAPSec key management to be included in 33.102.
- Select algorithms to be supported by MAPSec.
- Write MAPSec Domain Of Interpretation for ISAKMP. Find out if it has to be an RFC.
- Agree on use of PUSH (or PULL) principle for KAC to NE distribution and on the protocol to use.
- Agree on (optional?) protection mechanism for Z_B

Work Items / Issues II

- Define database formats for MAP-SPD and MAP-SADB.
- Agree on standard profiles of MAP-PP
- Agree on use of SPI in and format of MAP security component headers.
- Update 29.002 to conform to use of MAP-SPD and MAP-SA info.
- Agree on standardisation strategy for trust distribution for IKE. This includes the time schedule and the mechanism to use.

Summary I

- The necessary functionality can be built on established protocols and software, which will enable a speedy implementation and deployment.
- Key management procedures common between MAPSec and IPSec.
- IKE includes mechanisms for key refreshing, protection from Denial of Service attacks by using cookies, perfect forward secrecy, possibilities to use standard Diffie Hellman groups or define new ones, digital signatures to name a few.

Summary II

- Facilitates stepwise deployment.
- Introduction of the PULL principle will minimise storage and communication requirements in the NE's.
- The introduction of SA's will lessen the overhead in MAPsec traffic.