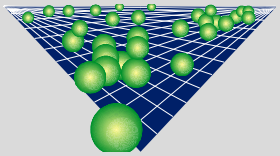
S



SA negotiation protocol for the Z_A interface (S3-z00021)

3GPP SA3 meeting #15bis - S3z000034
08/09 Nov. 2000

© Siemens AG, ZT IK 3
Dirk Kröseberg

S

SA negotiation over Z_A: The Basic Scenario

- Key administration centers negotiate security associations between networks, using the Z_A interface. SAs are provided for IPsec and MAP security.
- Two alternatives for the SA negotiation protocol are under discussion
  - A) IKE (IETF RFC 2409) is directly used for negotiation.
    For IPsec SAs, the IPsec DOI (IETF RFC 2407) is used.
    For MAP security SAs, a new MAPsec DOI is required.
  - B) IKE/IPsec provide a secure channel between two KACs over Z_A.
    A SA negotiation protocol (to be defined by 3GPP) uses the secure channel for SA negotiation.
- S3-z000021

  discusses problems of alternative A

  proposes to use alternative B

© Siemens AG, ZT IK 3

SA negotiation over Z_A: Problems with alternative A

- Functional split between IKE and the IPsec kernel
  - SA negotiation takes place between two KACs
  - The SAs are used between network elements (NE) other than the KACs
  - KAC and NE have different IP addresses

  This functional split is not intended by the IPsec framework

- Negotiation of configuration parameters describing how to use the SA
  - Standard IKE negotiates SAs for the IP addresses of the IKE peers
  - Only a single, additional ID payload is allowed for each IKE peer for the exchange of configuration information (where and how to apply the SAs).

  „Standard“ IKE does not seem to be sufficient for NDS key management.

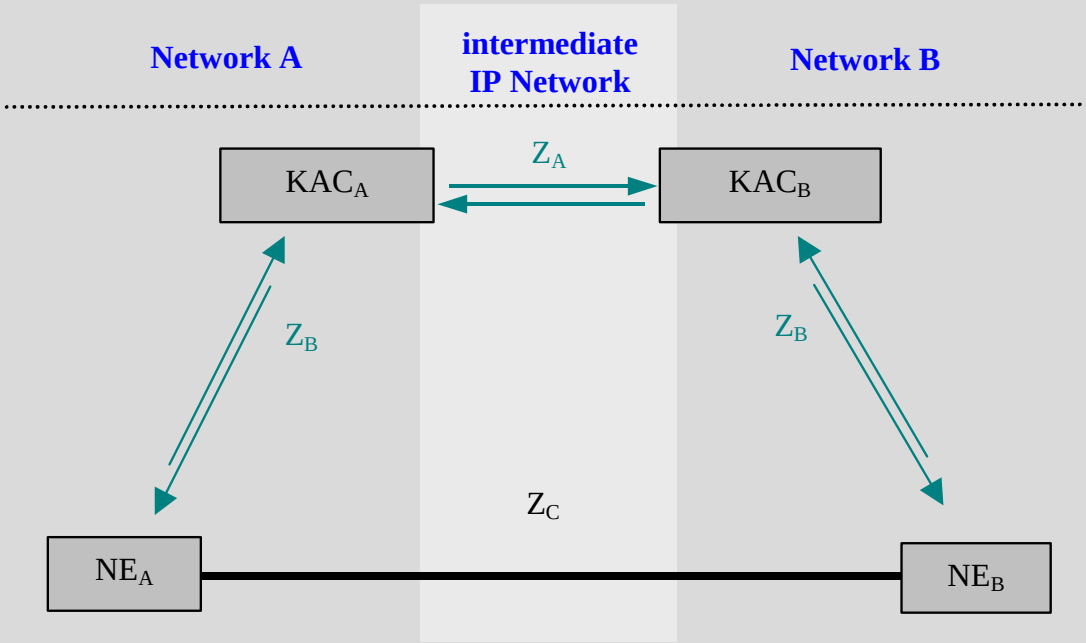
© Siemens AG, ZT IK 3

SA negotiation over Z_A: Example A

- NE_A needs to establish SAs with NE_B through KAC_A
- KAC_A initiates IKE with KAC_B

Problem:

- KAC_B needs to know between which NEs the SAs shall be used
- KAC_A must send at least the IP addresses of NE_A and NE_B to KAC_B



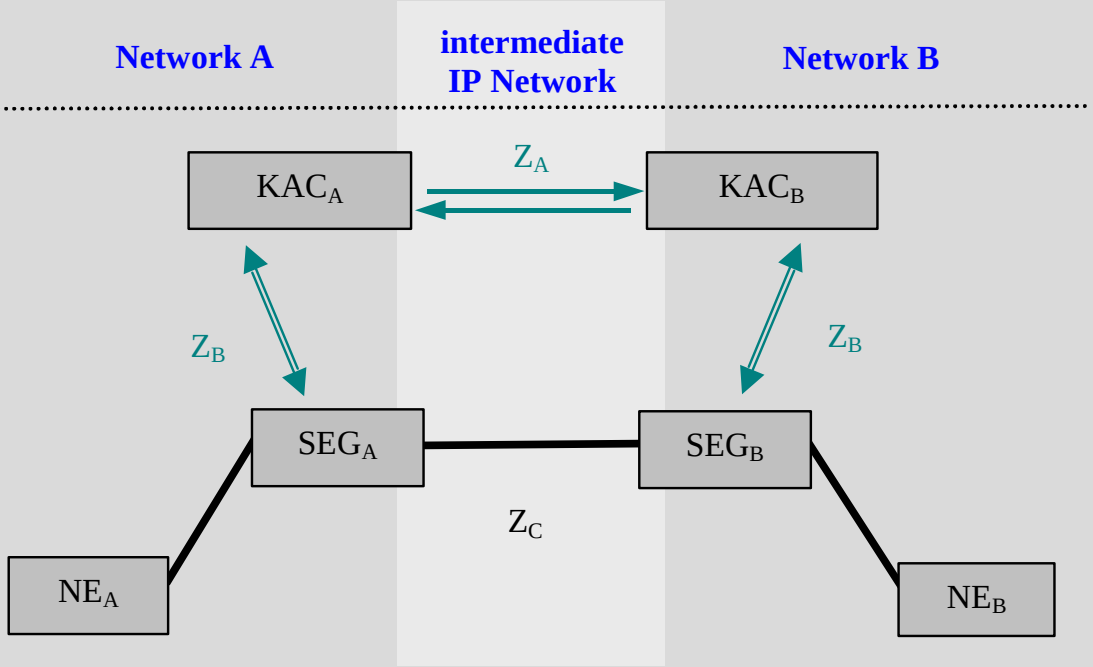
© Siemens AG, ZT IK 3

SA negotiation over Z_A: Example B

- SEG_A needs to establish SAs with SEG_B through KAC_A to establish a secure tunnel, for communication only between NE_A and NE_B
- KAC_A initiates IKE with KAC_B

Problem:

- KAC_A must send at least the IP addresses of NE_A and NE_B to KAC_B
- KAC_A must send the IP addresses of NE_A and NE_B as well



© Siemens AG, ZT IK 3

SA negotiation over Z_A: What does IKE support?

- In an IKE quick mode exchange (used for IPsec SA negotiation), two additional identification payloads IDci and IDcr are allowed (this is called „client mode“).
- These allow each IKE peer to add a single ID payload, which can carry
  - an IP address with port and protocol
  - a subnet mask
  - other selectors, defined by the IPsec DOI
- Problem: Not sufficient for network domain key management (without changes to either the IKE or the IPsec DOI specification)

© Siemens AG, ZT IK 3

SA negotiation over Z_A: What could be a solution?

- Carry a pointer to a specific configuration profile in the ID payload. Then
  - all configuration profiles have to be exchanged off-line
  - a change in one network‘s configuration affects all related profiles in other networks
  - this could conflict with the IPsec DOI
- Use certificates in IKE and add a profile pointer to the certificate
  - Certificates are used for authenticating IKE phase 1, IPsec SAs are subsequently negotiated during quick mode (phase 2)
  - This would require a new, expensive IKE phase 1 exchange each time that SAs for a new configuration profile are required
- Both solutions seem to be (at least) problematic

© Siemens AG, ZT IK 3

S

SA negotiation over Z_A: Our proposal

- We propose to use alternative B for the Z_A interface:
  - Use IKE over Z_A to negotiate SAs for the KACs
  - Use these SAs to establish an IPsec secured channel between the KACs
  - Define a new protocol to negotiate SAs for IPsec and MAPsec over Z_C

- Note: Since for both IPsec and MAP security over Z_C the same SA negotiation mechanism should be used, this alternative does not require the definition of a MAPsec DOI for IKE.

© Siemens AG, ZT IK 3
Dirk Kröselberg