IPsec application requirements

draft-mglt-btns-ipsec-api-requirements-00 – IETF74 San Fransisco

Daniel Migault, Orange Labs

Background & Goals

- BTNS screws out network security and IPsec deployment with unauthenticated connection.
- Applications can hardly benefit from IPsec functionnalities. IPsec seems to much network centric and complex to use.

We want applications benefit from IPsec security features.

draft-mglt-btns-ipsec-api-requirements-00

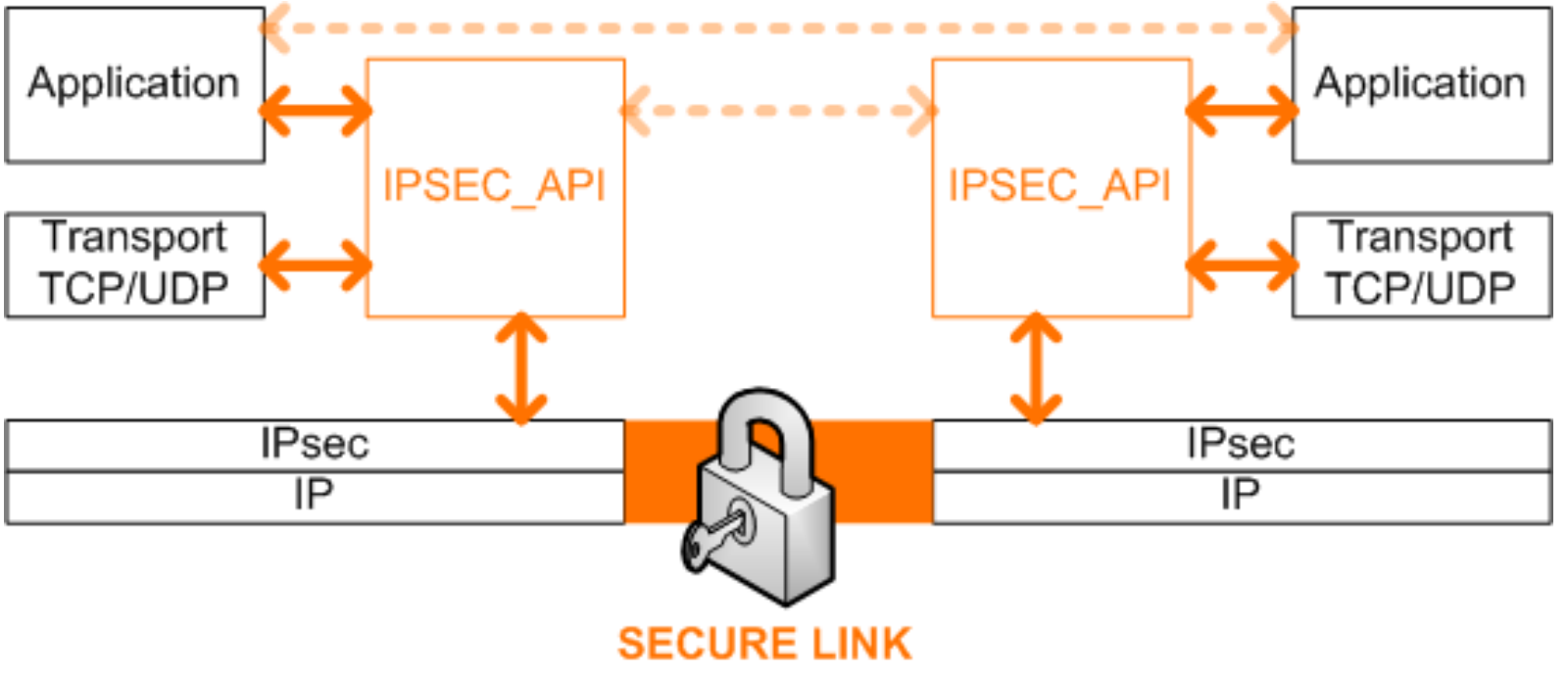
What we think applications want

- Rely on IPsec to :
  - AUTHENTICATE a peer.
  - SECURE a channel.
- Provide its requirements :
  - In an EASY-way : application developpers should not be security experts.
  - With different GRANULARITY matching different applications security requirements
  - Platform independent

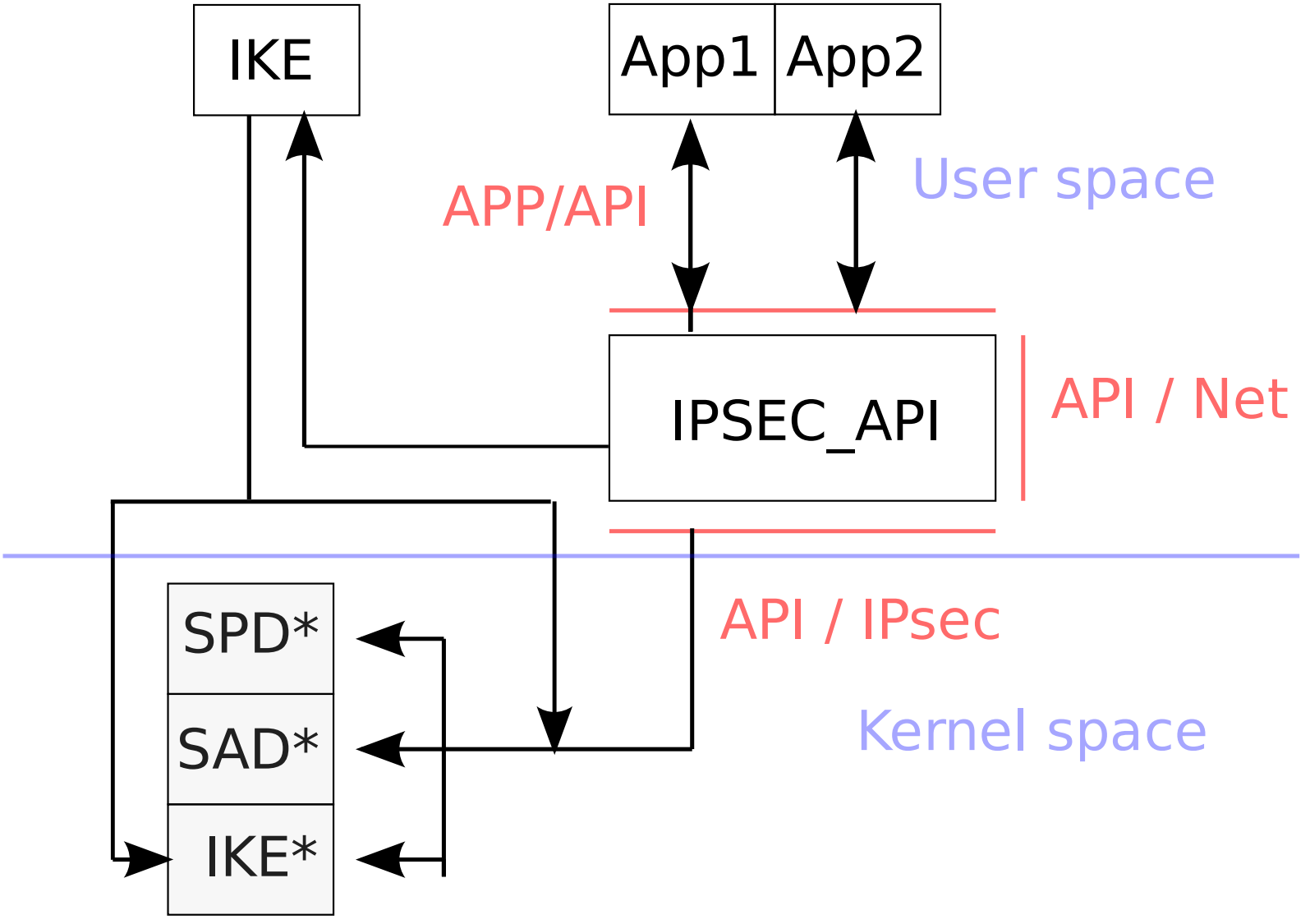
IPSEC_API caracteristics

- FLEXIBLE :
  - Provides different interfaces for the applications– socket, sockoptions, IPC, network.
- SECURE :
  - It should not weaken the system by providing an open interface to all applications.
- APPLICATION-centric :
  - NOT another XFRM / PF_KEY

IPSEC_API architecture (1/2)



IPSEC_API architecture (2/2)



IPSEC_API & authentication

Applications MUST be able to :

- READ : Check WHO it is sending packets to.
- READ : Request how the authentication was performed.
- CONFIGURE : Request how the authentication need to be performed.
- CONFIGURE : Decide the authentication part IPsec plays.
- INTERACT : Decide to accept / reject an peer.
- INTERACT : Require an authentication.

IPSEC_API & secure channel

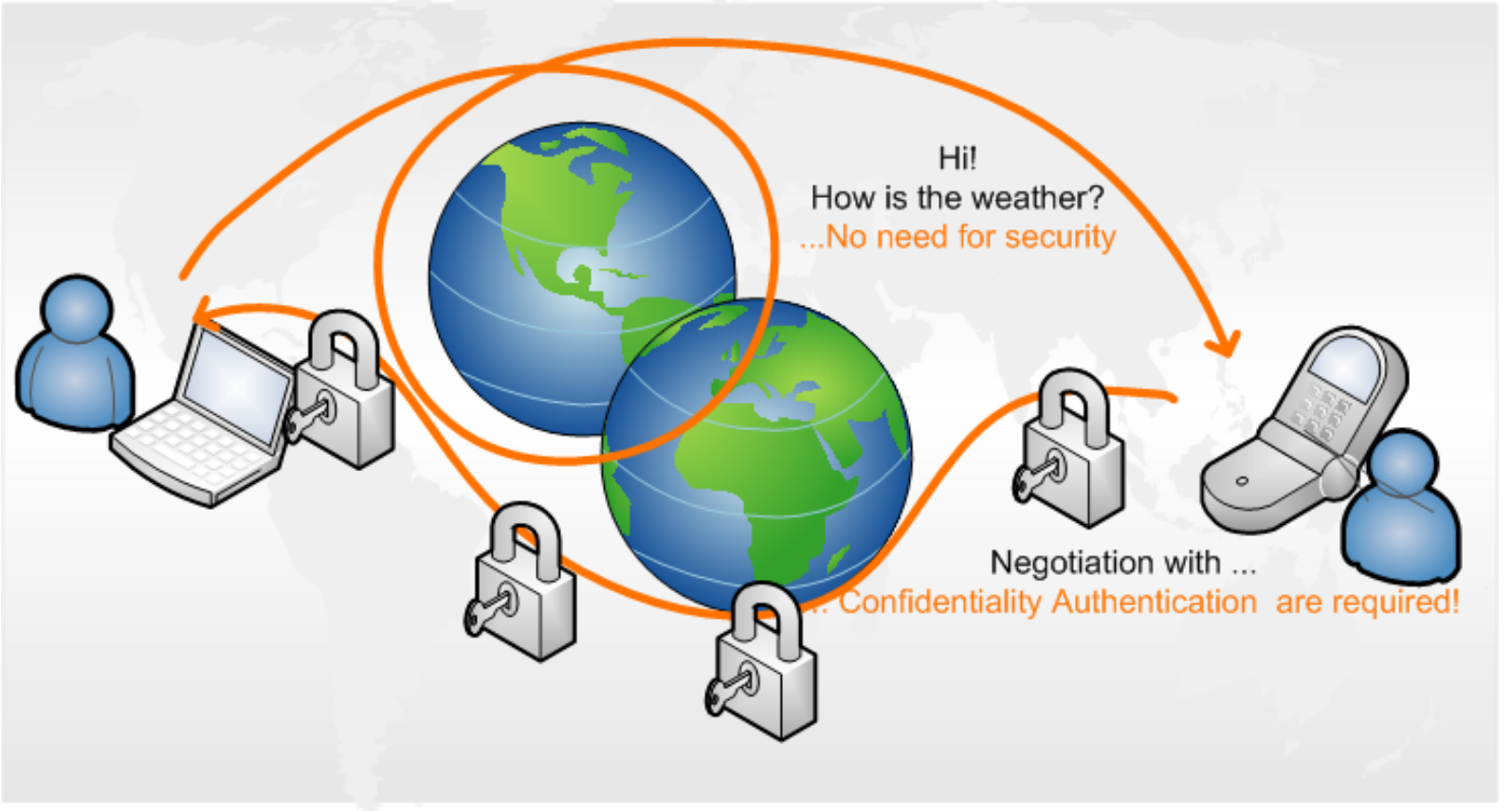
Applications MUST be able to :

- READ IPsec parameters of an ESTABLISHED connection.
- CONFIGURE : how the channel should be secured.
- INTERACT : trigger IKE negotiation, delete an SA.

Current works

- Version 00 of the draft.
  - Next version will focus more on application needs. – clarification, more explicite.
- We are working on :
  - Designing the architecture of IPSEC_API : draft is expected very soon, – before IETF75.
  - Secure channel scenario and message exchanges : drafts are expected very soon, – before IETF75.
  - Mobility and Multihoming scenario and message exchanges : drafts are expected very soon.
  - We hope a demo will be available for IETF75.

IPSEC_API secure channel scenario



Future works

- Provide feed backs to the draft
- Provide applications you know would benefit from IPSEC_API and their explicite requirements with IPsec security.