ERICSSON

IPsec, IKE, MAPSEC DOI Profiles for the 3GPP

Contribution #91 and #101

Jari Arkko

Ericsson

Jari.Arkko@ericsson.com

ERICSSON

Contents

- Reasons for profiling
- Current profile
- MAP DOI IKE profile
- IPsec Profile
- IKE Profile
- Open Issues

ERICSSON

Reasons for Profiling

- Limit cost
- Limit complexity
- Improve interoperability through a common agreement of the minimum acceptable functionality

- Does not limit vendors in providing additional functionality
- Does not limit 3GPP in requiring additional functionality in the future

ERICSSON

Current Profiles from 33.200

- No IP compression protocol
- No AH, only ESP
- NULL encryption not allowed
- Only tunnel mode is mandatory
- AES instead of DES

Can we say more regarding IPsec?

Should we say something about IKE?

Differences in the profiles wrt KAC-KAC, SEG-SEG, etc?

ERICSSON

MAP DOI IKE Profile

- Only Phase 1 of IKE is used, the rest is MAP DOI
- Only IPv6 is mandatory
- Perfect Forward Secrecy (PFS) optional: Limits CPU requirements
- Aggressive mode to be mandatory, main mode optional: Limits complexity,loses some security against DoS
- Only FQDN identities to be mandatory: Limits complexity

ERICSSON

MAP DOI IKE Profile Cont'd

- AES, SHA1 used for protection of IKE: No AES-based hash yet in the IETF
- SA lifetime notifications will not be allowed: Limits complexity, ensures simultaneous timeout
- SA deletion will not be allowed: Allows pull-based mode to work
- Also note that IKE mandates preshared secrets, public-key based mechanisms are optional

ERICSSON

Additional IPsec Profiling

- Only IPv6 is mandatory
- Only HMAC_SHA1 is mandatory
- Make support of bundles (nested SAs) optional
- Do not require all policy and selector mechanisms. Only addresses, ports, and transport protocol are mandatory. Only single values, address masks, and wildcards are the required values for these.

ERICSSON

IKE Profiling

- Phase 1
  - Only IPv6 is mandatory
  - Aggressive mode to be mandatory, main mode optional: Limits complexity,loses some security against DoS
  - Only FQDN identities to be mandatory: Limits complexity
  - Also note that IKE mandates preshared secrets, public-key based mechanisms are optional: Enables building SEG/NE nodes without public key support and PKI interfaces
  - Only AES and SHA1 (or AES-MAC) are mandatory

ERICSSON

IKE Profiling Cont'd

- Phase 2
  - Perfect Forward Secrecy (PFS) optional: Limits CPU requirements
  - Only IP address or subnet identity types are mandatory (IPv6)
  - Notifications are mandatory.

ERICSSON

Open Issues

- It is clear to us that IPv6 should be used on all inter-operator interfaces. What about intra? Tentative answer: IPv6 in there as well.
- Are there interfaces on which 3GPP could make IPsec mandatory but IKE optional?
- Which integrity protection algorithm should be employed by IPsec and IKE? Tentative answer: SHA1 now for interfaces that are defined for Relese 4, later releases can use newer IETF work.