An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange

draft-cakulev-emu-eap-ibake-00

Violeta Cakulev
Violeta.Cakulev@alcatel-lucent.com

Ioannis Broustis
Ioannis.Broustis @alcatel-lucent.com

ITEF 80 – Prague

EAP-IBAKE

EAP method that leverages IBAKE

IBAKE - Identity Based Authenticated Key Exchange

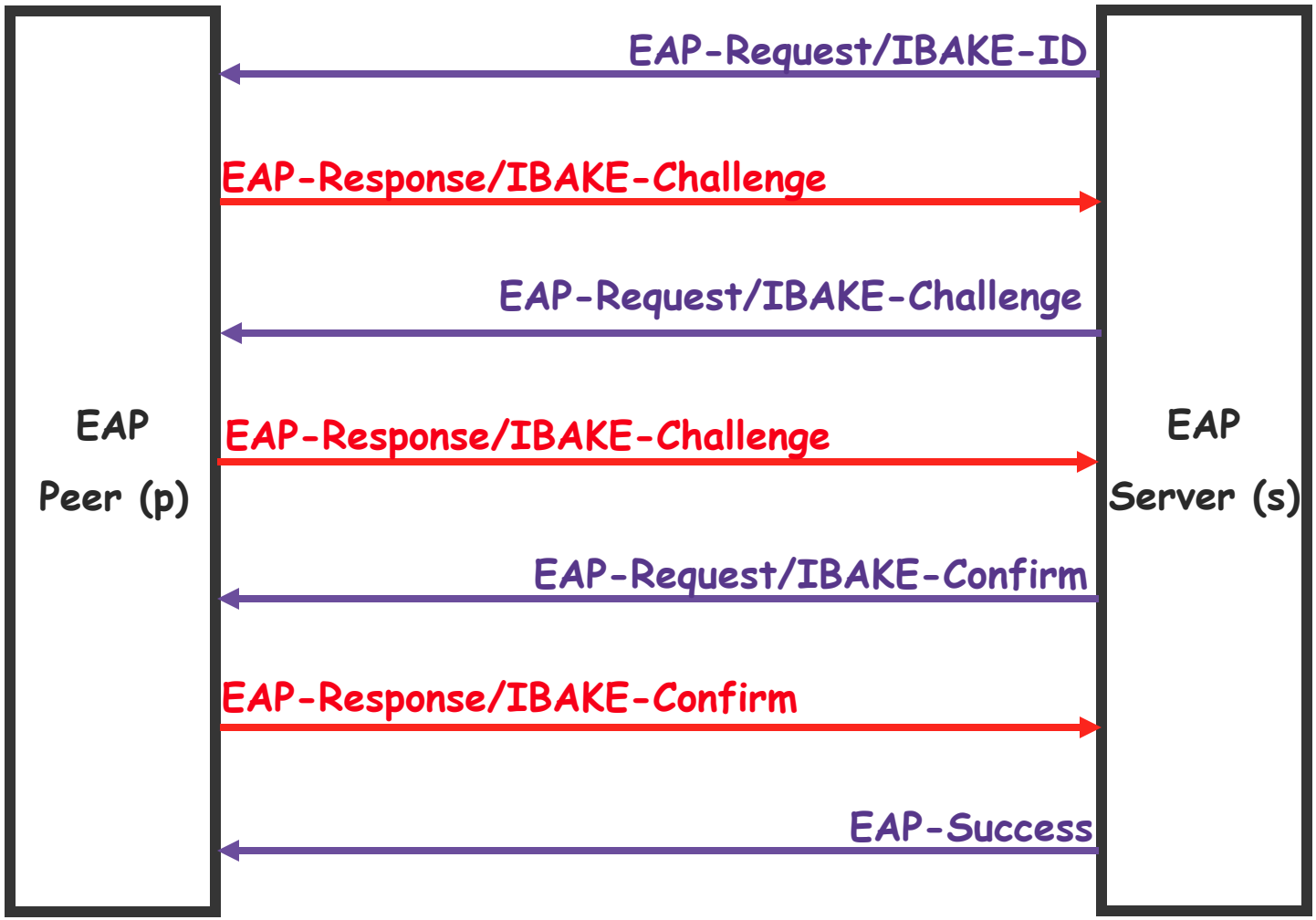
- Mutual authentication through the use of identity-based encryption
- Derivation of exportable keying material
- Perfect forward and backward secrecy
- Escrow-free key agreement
- Security formally proven

IBAKE Framework

Based on an Identity Based asymmetric cryptographic framework

- Every participant has a public and a private key
- Public key is identity based
- Private key corresponding to Public key is issued by a trusted Key Generation Function (KGF)
- Participants obtain private keys from KGF offline
  - Security association between KGF and participant is pre-provisioned
- Encryption and Decryption of messages during EAP exchange based on Identity Based Encryption (IBE)
  - Reference: Boneh et al., RFC 5091, RFC 5408, RFC 5409

EAP-IBAKE Exchange



EAP-IBAKE Messages

SERVER PEER

IDs, Crypto Proposals →

← Encr(K_PUBs,IDp), Encr(K_PUBs, Crypto Selection)

Encr(K_PUBp, IDs, IDp, [Rs]P) →

← Encr(K_PUBp, IDs, IDp, [Rs]P, [Rp]P)

Encr(K_PUBp, IDs, IDp, [Rp]P), Auth_S →

← Auth_P

K_PUBp and K_PUBs - peer's and server's public keys

Rp and Rs - random integers, chosen by Peer and Server

Auth_S, Auth_P - signature fields to protect the integrity of the negotiated parameters

P is a point on an elliptic curve

- Negotiated during IBAKE-ID exchange

EAP-IBAKE Features

- Identity Protection
- Ciphersuite negotiation
- Mutual authentication
- Reply protection
- Integrity protection
- Confidentiality
- Secure Key generation
- Session independence
- Fragmentation

Targeted Application

European Telecommunications Standards Institute (ETSI)

- ETSI adopted IBAKE as a bootstrapping protocol (ETSI TS 102 690)
- ETSI is currently discussing what protocol to use to carry IBAKE messages
  - EAP is one of the proposals

Next Step

Does this fit current working group charter?