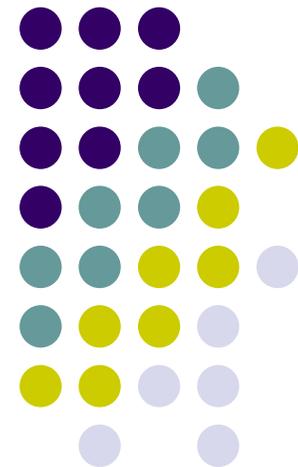


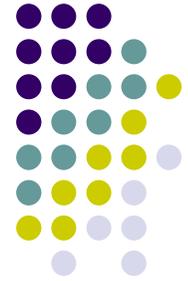
ERP extension for EAP Early-authentication Protocol (EEP)

draft-ietf-hokey-erp-aak-04

Zhen Cao, Hui Deng
Glen Zorn
Qin Wu, Yungui Wang
KOKEY WG @ IETF80
March 29, 2011
Prague, CZ



Status



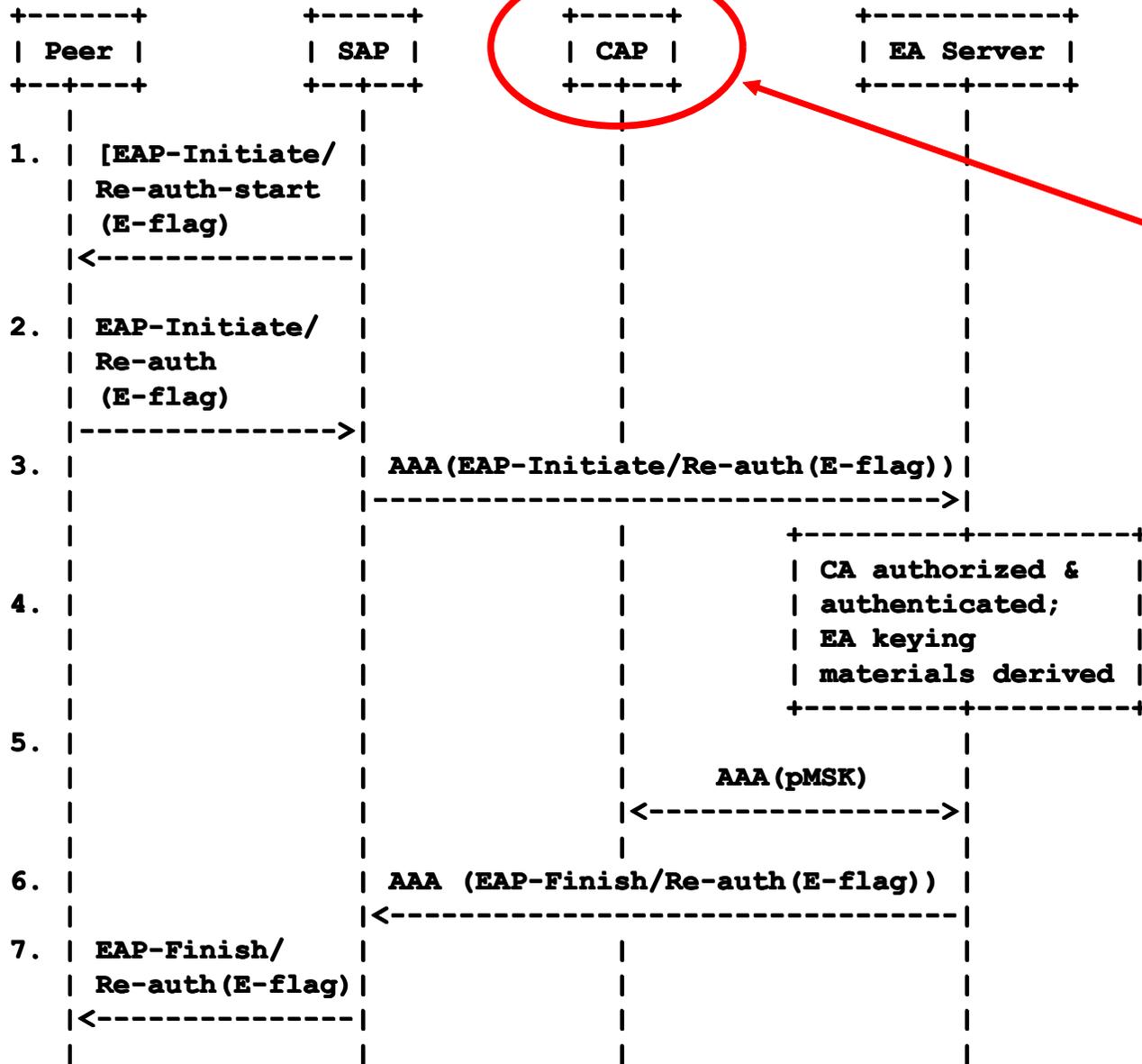
- Adopted as a WG item at IETF 77
- Revised to 02 version WG draft based on feedbacks from the group
 - Present at IETF78
- Revision 03 after IETF78
 - Version number changes only
- Revision 04 after IETF79

Changes #1: Multiple CAs to Single CA



- AAA server lacks capability to distribute the keys for multiple CA
 - Focus on distributing the key for a single CA
 - Leaving the issue of multiple CAPs for extension
- Keep it simple and it works better

ERP-AAK Operation, looking like this now



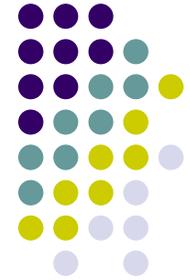
Only ONE CAP

Change #2: Complete security consideration section



- Security Considerations section has been filled
- This section provides an analysis of the protocol in accordance with the AAA key management requirements specified in [RFC4962]

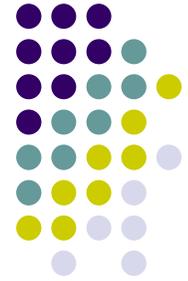
Cryptographic algorithm independence:	√
Strong, fresh session keys	√
Limit key scope	√
Replay detection mechanism	√
Authenticate all parties	√
Peer and authenticator authorization	√
Keying material confidentiality	√
Uniquely named keys	√
Prevent the domino effect	√
Bind key to its context	√
Confidentiality of identity	√
Authorization restriction	√



Change #3: TLV allocation

- "List of crypto suites" & NAS-Identifier TLVs are defined in RFC 5296, Why not reuse them?
- Yes, we reuse them

Moving Forward



- Submit for WGLC
- Encourage more review of the draft and early feedback

Thank you

- Q&A?

