Diameter IKEv2 PSK:
Pre-Shared Secret-based Support for IKEv2 Server to Diameter Server Interaction

draft-ietf-dime-ikev2-psk-diameter-08

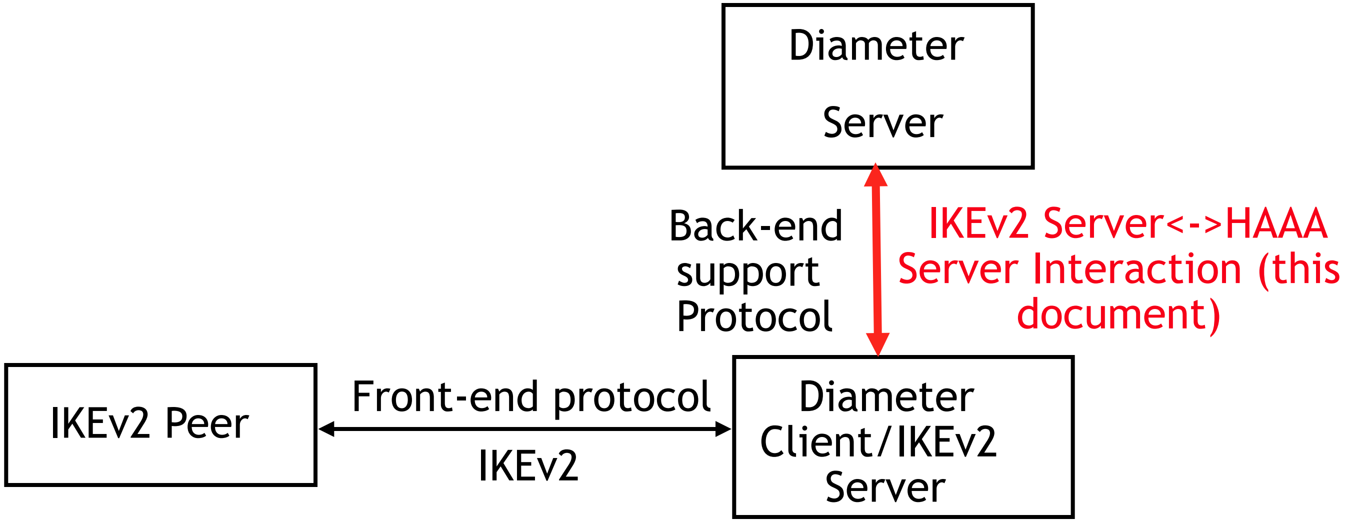
draft-ietf-dime-ikev2-psk-diameter-09 in progress

Violeta Cakulev violeta.cakulev@alcatel-lucent.com
Avi Lior avi@bridgewatersystems.com
Simon Mizikovsky simon.mizikovsky@alcatel-lucent.com

ITEF 81 – Quebec City, Canada

Diameter IKEv2 PSK

Specification of the interaction between the IKEv2 Server (e.g. Home Agent, Access Gateway) and Diameter server for the IKEv2 based on pre-shared secrets


Diameter
Server
Back-end support Protocol
IKEv2 Server<->HAAA Server Interaction (this document)
IKEv2 Peer
Front-end protocol
IKEv2
Diameter Client/IKEv2 Server

Draft is currently under IESG evaluation

Has 4 Open COMMENTS

Has enough positions to pass once DISCUSS is resolved

Resolved Comments in Re.08

1. Clarified that mutually authenticated TLS between Diameter nodes is already expected
2. "Encr" column in earlier version of the Draft is removed.
3. Initial recommendation to use Diameter agents that can be trusted was removed as unenforceable.
4. Auth-Request-Type AVP in the Request MUST be set to ‘Authorize-Only’
5. Key-SPI AVP is included in the request instead of Key AVP
6. Trust model is described in Security Consideration Section
7. Abbreviations section added
8. Editorials

Resolved Comments in Rel.09 (in progress)

1. Added the figure showing general Architecture (Rel.09).
2. Ni and Nr format was changed to OcterString from Unsigned32 because in RFC 5996 they are of variable length.
3. Recommendation to roll this draft into the 3588bis was withdrawn, because it was not clear when will 3588bis be ready.
4. It was clarified that SPI used in this draft (identifying the PSK for IKEv2) is different than SPI defined by IKEv2 for IPSec.

Open Discuss (Comment 1)

1. Procedure for Pre-Shared Key generation

“For interoperability, procedure for PSK generation needs to be specified”

- Response: The PSK could be generated following outside rules established between AAA and IKEv2 Client, or could be provisioned and stale.

- For systems and protocols that leverage this Diameter application but do not specify the key derivation procedure, Rel.09 specifies the default key generation procedure that uses N_i and N_R for freshness, similar to that in RFC 5295 sec.3.1 for USRK generation.

PSK = KDF (Root Key Material,“psk4ikev2@ietf.org”|“\0”|N_i|N_R|ID_i|length)

Open Discuss (Comments 2 & 3)

2. Need for applicability text

“Limit the applicability to MIPv6”

- Response: MIPv6 is described as an <u>example of use</u> in the Draft. Multiple uses are possible. Limiting the applicability in the text can disable any future use.

3. Routing based on NAI

“Routing based on NAI (realm) seems to make it very hard to do with security, unless there is some way to validate the domain component of the NAI. Generic text that could be referenced is requested.”

- Response: Routing based on NAI is a generic issue true for all Diameter deployments, not specific for this draft. Business agreement between IKEv2 Server and AAA Server (associated with the realm in NAI) is expected.

Open Discuss (Comment 4)

4. IDr in IKEv2-PSK-Request

> *"If IDr is included in IKE_AUTH from Initiator to Responder should it be included in IKEv2-PSK-Request for IKEv2 Server binding into the PSK generation."*

- Response:
  - IKEv2 allows the Peer to specify an IDr as optional parameter. But according to RFC 5996, the IKEv2 server can assert a different IDr.
  - The Peer needs the PSK at the time of computing the IKEv2 AUTH for the CREATE_CHILD_SA Request. But the correct IDr only comes from the IKEv2 Server in the CREATE_CHILD_SA Response, or too late.
  - Therefore, IDr is not included in IKEv2 PSK computation.