

PCP Authentication Requirements

draft-reddy-pcp-auth-req-04

T.Reddy, P.Patil, D.Wing, R.Penno

IETF-87

Presenter: Prashanth Patil

REQ-4

The server MUST be able to ~~optionally~~ trigger re-authentication with the client. An unsolicited message for authentication trigger MUST be integrity protected if there is a valid unexpired SA.

~~The server can continue to use the same SA to protect messages even if SA has expired.~~

REQ-9

A PCP proxy that modifies PCP messages SHOULD have the ability to independently authenticate with the PCP client and PCP server. The presence of a PCP proxy hence requires two separately authenticates SAs.

The PCP proxy MUST also permit authentication on only one side of the proxy. For example, a customer premises host may not authenticate with the PCP proxy but the PCP proxy may authenticate with the PCP server.

REQ-14

There SHOULD be support for Server-Side only authentication.

Eg: A client visiting foreign networks such as hotel, hot-spot etc. where the client may gain access to a network but does not have the credentials to authenticate with the PCP server.

Other discussions

- Should exchanges that carry cipher suite selection or other authentication parameters be protected?
- Secure integrity of authentication response packets.
- Should the document go into details of cryptographic strength and user identity model?

Next Steps?