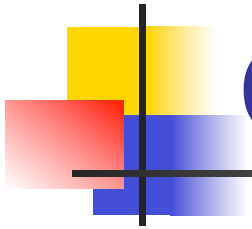
RFC 5539 Update Status

draft-badra-netconf-rfc5539bis-01

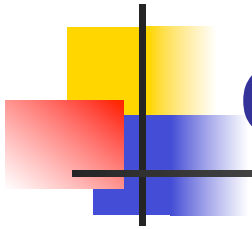
Mohamad Badra

ETF 83, Paris, France



Change log: From -00 to -01

- Shorten the YANG object names
- Extend the YANG module to support configuration of PSK

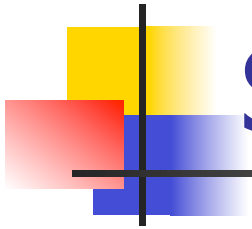


changes to be done

- After the WG call for discussion
  - SubjectAltName extraction and examination
  - Reverse Proxy
  - implementations

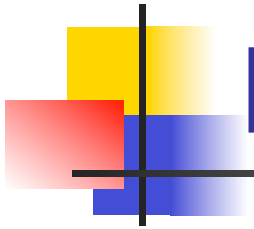
SubjectAltName: revised text

- SubjectAltName may contains more than one ipAddress, dnsName, or rfc822Name
  - If the subjectAltName contains more than one rfc822Name, dnsName, or iPAddress, then only the first rfc822Name, dnsName, or iPAddress is extracted and used. Subsequent rfc822Names, dnsNames, or iPAddresses are ignored.



SubjectAltName Examination

- Examine the subjectAltName's rfc822Name, dnsName, and iPAddress fields in a pre-defined order
  - The user can pick between 1 of 6
  - ISMI case: dnsName, rfc822Name, iPAddress
  - Shall we keep the same as IMSI?



Reverse proxy

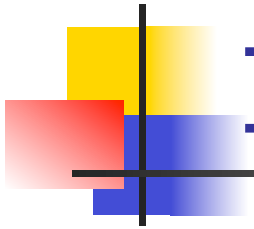
- A TLS connection cannot transparently extend across a reverse proxy
  - The reverse proxy shall always terminate the TLS secure session

Replace:

It MUST connect to the server that passively listens for the incoming TLS connection on the TCP port 6513

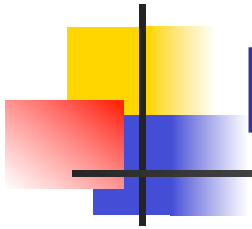
With:

The peer actively opens the TLS connection, and the server passively listens for the incoming TLS connection.



Implementations

- Juergen confirmed that Vlad Perelman (Jacobs Univ. Bremen) is working on a TLS implementation for NETCONF Light that is using PSK authentication.
- SNMPR will most likely implement it



Next Steps

- Make any agreed changes
- WG item?