NegoEx

Larry Zhu

IETF72

Microsoft

Summary

- **draft-zhu-negoex-01** published
- Informational document
- Deficiencies in SPNEGO being dealt
- No changes to SPNEGO messages in RFC 4178
- negoEx is a pseudo mechanism under SPNEGO
- Logically extends SPNEGO
- Seek working group feedback

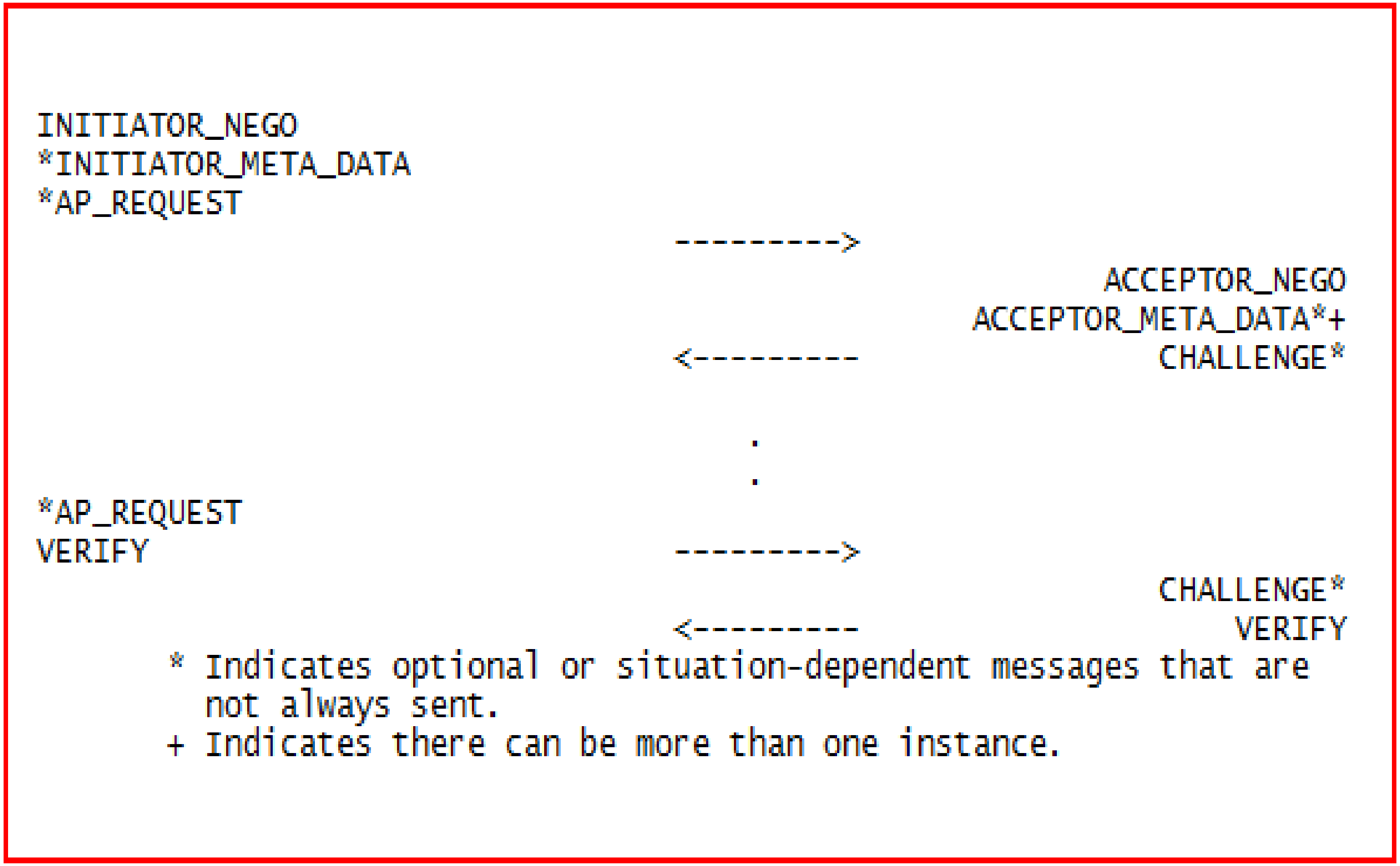
Problem Statments

- SPNEGO only allows exchanging OIDs and lacks of auxiliary data in the negotiation phrase in any other form
- SPNEGO is one shot protocol

NegoEx One Pager

- Added Meta-Data tokens
- Added protection of negotiation based on RFC3961
- Simple C style encoding, no ASN.1
- Added supporting new GSS-API extensions
- No extra roundtrip required comparing with SPNEGO

Protocol Message Sumary



```
INITIATOR_NEGO
*INITIATOR_META_DATA
*AP_REQUEST
                                  --------->
                                                         ACCEPTOR_NEGO
                                                  ACCEPTOR_META_DATA*+
                                  <---------                CHALLENGE*

                                      .
                                      .
*AP_REQUEST
VERIFY                            --------->
                                                            CHALLENGE*
                                  <---------                    VERIFY
       * Indicates optional or situation-dependent messages that are
         not always sent.
       + Indicates there can be more than one instance.
```

Supporting GSS-API Extensions

- GSS_Query_meta_data
- GSS_Exchange_meta_data
- GSS_Query_mechanism_info
- GSS_Query_context_attr

Questons?