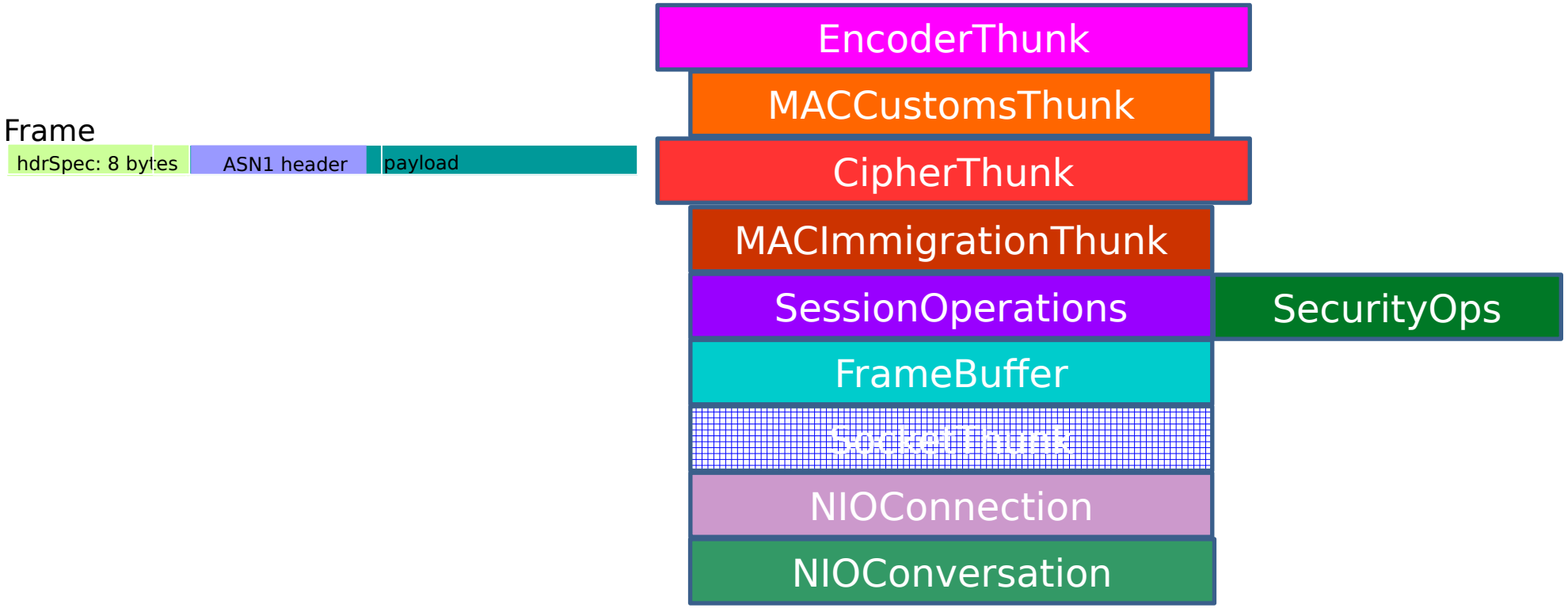
ParrotTalk Frame Design

Version 3.7

Homeless Council
Callisto House Limited
Callisto Enterprises

https://github.com/CallistoHouseLtd/ParrotTalk



ParrotTalk Frame Design

- Frames are used in message pipeline, consisting of
  - an 8 byte message specification,
  - a msgType ASN1Choice Encoded header
  - a possible data payload.
- Frames are exchanged between layers, up & down the stack.
- Each protocol frame transforms session state through the SessionOperations layer.
- Each data layer transforms each frame by established session protocol.
- As payload is transformed, header is transformed and re-encoded ASN1Der.
- MsgSpec knows header & frame encoding specification.
- Natural nested wrapping of data msgs, where an inner frame's payload is an encoded frame, enveloped.
- Protocol stack is established during session rendezvous with these data wrapping specifications:
  - Encoded – Primary payload
  - Encrypted – AES-256/CBC/PKCS7Padding with 128-bitblockSize & IV and a 256-bit key
  - MAC – 160-bit hmac hash

ParrotTalk Protocol

- 5-way message rendezvous handshake protocol with Protocol pre-exchange
- Protocol exchange (ProtocolOffered/ProtocolAccepted), determines v3.7 viz v3.6
- Protocol exchange (ProtocolOffered/ProtocolAccepted), determines v3.7 viz v3.6
- 2 different protocols negotiated with the prior messages
  - ProtocolOffered
  - ProtocolAccepted
- With version 3.7 Session Operations installed, the v3.7 state machine is active.
- 3 message exchange
  - Hello_v3_7
  - Response_v3_7
    - Signature_v3_7
- CryptoProtocol negotiation
- DataEncoder negotiation
- 2048-bit prime/secret Diffie-Hellman parameter exchange
- 2048-bit RSA Signature authentication
- QuadScopeInfrastrucure 4,5,6, , ,9:
  - 4: Goose – routing
  - 5: Parrot – session
  - 6: Raven – presentation
  - 7: Pidgeon - App DSL
  - 8: Vulture - Container DSL
  - 9: Eagle - meta

ParrotTalk Protocol Headers

- Layer 4: Goose – routing
  - <1> ProtocolOffered {‘ParrotTalk-3.7’}

<3> ProtocolAccepted {‘ParrotTalk-3.7’}

- Layer 5: Parrot – session
  - <16> Hello_v3_7
    - VatId
    - Domain
    - Public key
    - CryptoProtocols
    - DataEncoders
    - DiffieHellmanParamenter
  - <17> Response_v3_7
    - VatId
    - Domain
    - Public key
    - SelectedCryptoProtocol
    - SelectedDataEncoder
    - DiffieHellmanParamenter
    - Signature
  - <18> Signature_v3_7
    - Signature
  - <14> DuplicateConnection
  - <15> NotMe

Generic Structure

8-byte MessageSpecification

- messageSpecification: 8 byte frame header, bit encoded
  - 1st word, 4 bytes
    - 4 bits : tags
    - 10 bits : multicast
    - 10 bits : hash
    - 1 bits : frameVersion = 1
    - 2 bits : priority
    - 5 bits : headerType {headerTypes unspecified: 0, 2, 4, 21-31}
  - 2nd word, 4 bytes
    - 32 bits : messageSize <payload bytes = (messageSize - headerSize – 8 bytes)>
- messageHeader: headerType::size byte ASN1.Der encoded
- payload: (Z bytes)

ProtocolOffered Message

- messageSpecification: 8 bytes frame header, bit encoded
  - headerType = <1>
- ProtocolOffered Header: ASN1.Der encoded explicitTag: 1
  - offered – ASN1UTF8StringType = ‘ParrotTalk-v3.7, ParrotTalk-v3.6’
  - preferred – ASN1UTF8StringType = ‘ParrotTalk-v3.7’
- payload – zero bytes

ProtocolAccepted Message

- messageSpecification: 8 bytes frame header, bit encoded
  - headerType = <3>
- ProtocolAccepted Header: ASN1.Der encoded explicitTag: 3
  - accepted – ASN1UTF8StringType = ‘ParrotTalk-v3.7’
- payload – zero bytes

Encoded Message

- messageSpecification: 8 bytes frame header, bit encoded
  - HeaderType = <5>
- Encoded Header: ASN1.Der encoded explicitTag: 5
- payload – data bytes

Encrypted Message

- messageSpecification: 8 bytes frame header, bit encoded
  - headerType = <6>
- Encrypted Header: ASN1.Der encoded explicitTag: 6
  - ivSequence - ASN1ByteArrayType
- payload – data bytes

MAC Message

- messageSpecification: 8 bytes frame header, bit encoded
  - headerType = <7>
- MAC Header: ASN1.Der encoded explicitTag: 7
  - MAC: ASN1ByteArrayType
- payload: Data bytes

Hello_v3_7 Message

- messageSpecification: 8 bytes frame header, bit encoded
  - HeaderType = <16>
- Hello_v3_7 Header: ASN1.Der encoded explicitTag: 16
  - vatID – ASN1UTF8StringType
  - domain – ASN1UTF8StringType
  - publicKey – RSAPublicKey
  - CryptoProtocols – ASN1SequenceOfType(ASN1UTF8StringType)
  - DataEncoders – ASN1SequenceOfType(ASN1UTF8StringType)
  - diffieHellmanParam – ASN1ByteArrayType
- payload – zero bytes

Response_v3_7 Message

- messageSpecification: 8 bytes frame header, bit encoded
  - HeaderType = <17>
- Response_v3_7 Header: ASN1.Der encoded explicitTag: 17
  - vatID – ASN1UTF8StringType
  - domain – ASN1UTF8StringType
  - publicKey – RSAPublicKey
  - cryptoProtocol – ASN1UTF8StringType
  - dataEncoder – ASN1UTF8StringType
  - diffieHellmanParam – ASN1ByteArrayType
  - signature - ASN1ByteArrayType
- payload – zero bytes

Signature_v3_7 Message

- messageSpecification: 8 bytes frame header, bit encoded
  - HeaderType = <18>
- Signature_v3_7 Header: ASN1.Der encoded explicitTag: 18
  - signature – ASN1ByteArrayType
- payload – zero bytes

DuplicateConn Message

- messageSpecification: 8 bytes frame header, bit encoded
  - headerType = <14>
- DuplicateConn Header: ASN1.Der encoded explicitTag: 14
- payload – zero bytes

NotMe Message

- messageSpecification: 8 bytes frame header, bit encoded
  - headerType = <15>
- NotMe Header: ASN1.Der encoded explicitTag: 15
- payload – zero bytes