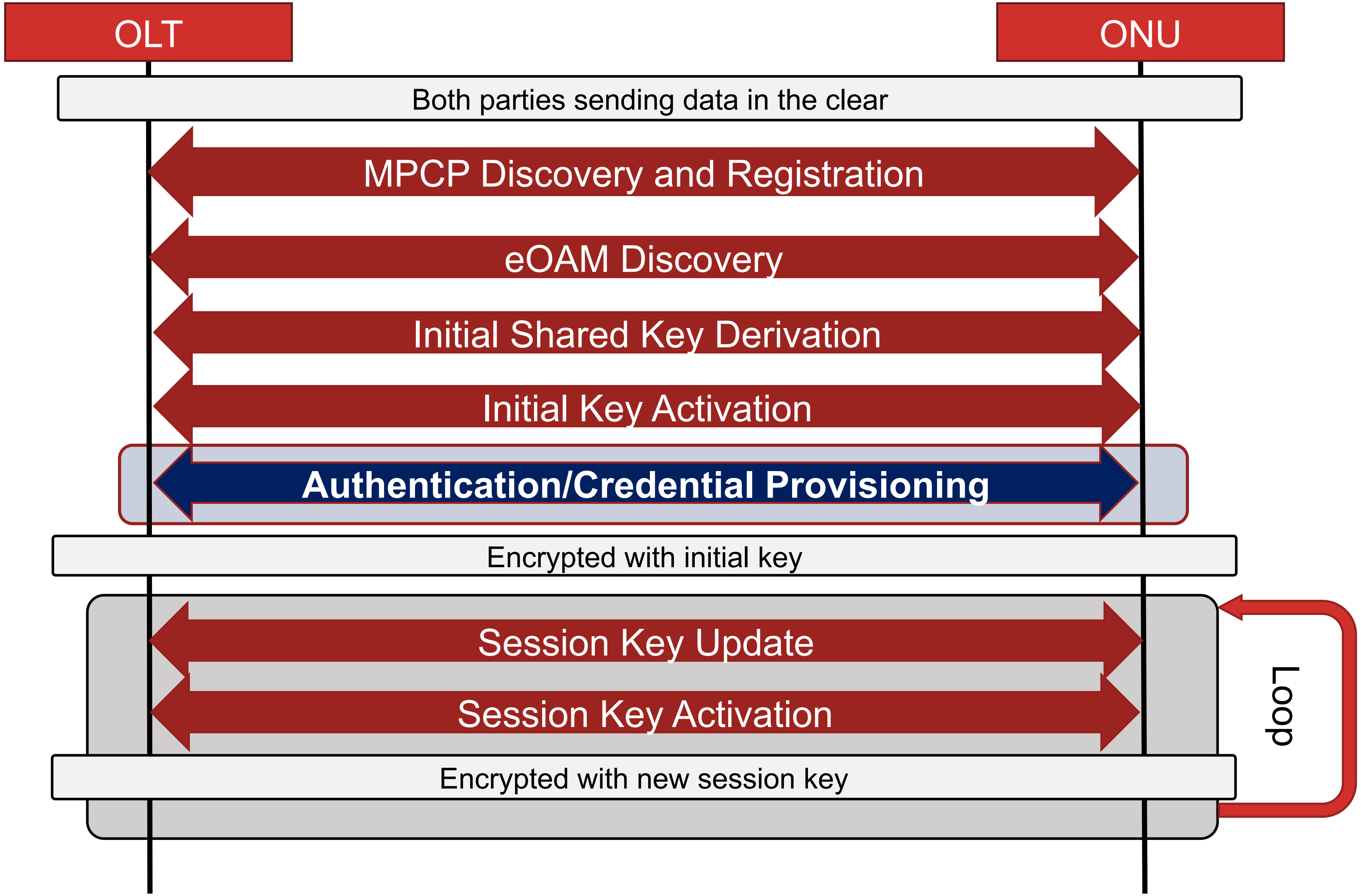
SIEPON.4 Authentication Proposal
v0.3 – 2023-10-31

Craig Pratt | Lead Software Engineer

c.pratt@cablelabs.com

ONU Encryption Initialization

CableLabs



OLT

ONU

Both parties sending data in the clear

MPCP Discovery and Registration

eOAM Discovery

Initial Shared Key Derivation

Initial Key Activation

Authentication/Credential Provisioning

Encrypted with initial key

Session Key Update

Session Key Activation

Encrypted with new session key

Loop

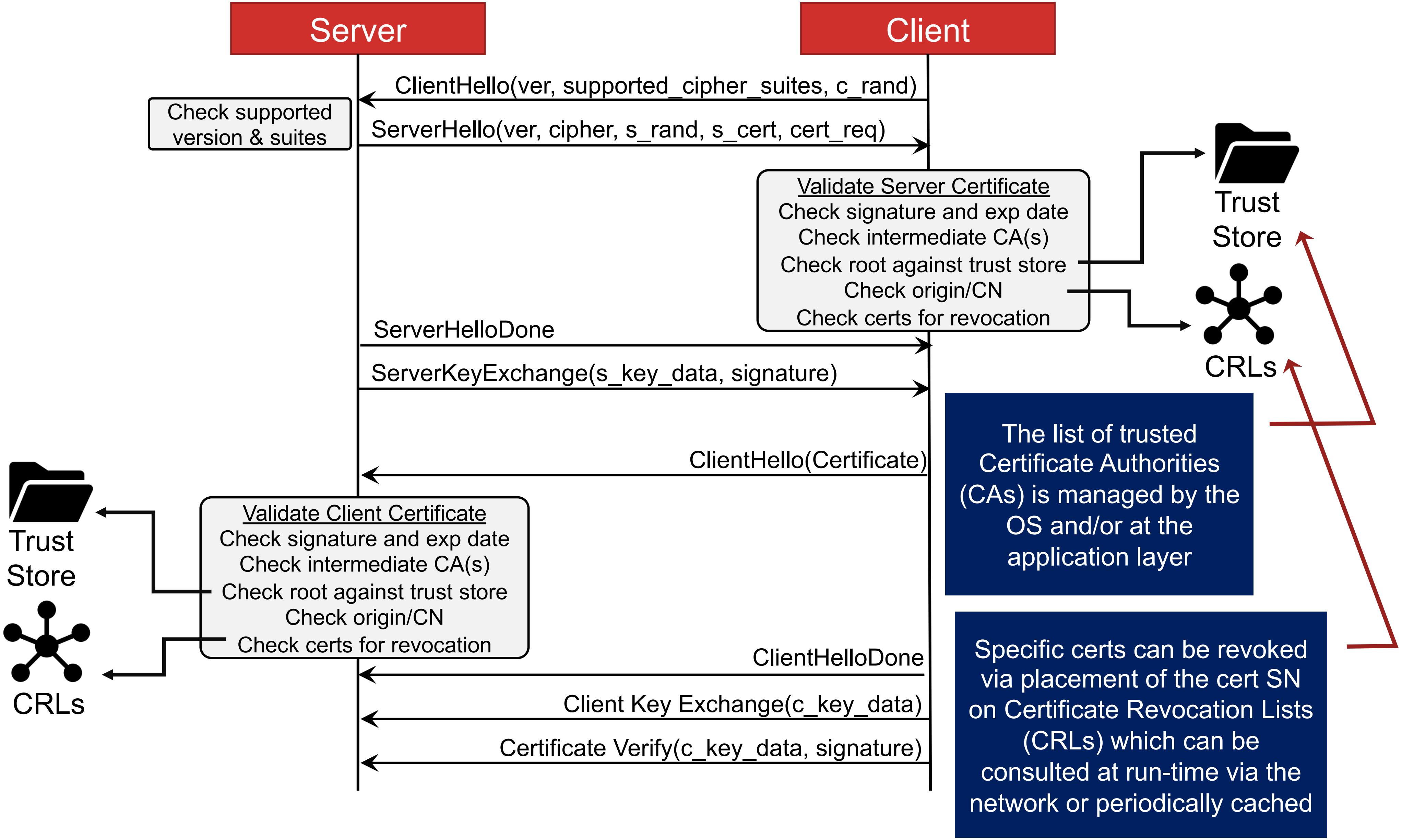
Mutual Authentication

- In SIEPON terms, MA means the OLT authenticates the ONU and the ONU authenticates the OLT.
- Goals/Requirements:
  - Provide a mechanism that can ensure that the identity of the ONU connecting to the OLT is authentic and authorized (registered)
  - Provide a mechanism that can ensure the ONU is communicating with an operator-authorized OLT
  - Provide a mechanism to allow the trust store and access lists that an ONU uses to validate the OLT to be updated by the OLT
  - Enable the operator to configure these features conditionally per device

Mutual Authentication - Terminology

- Identity – a context-unique way to know who were talking to
  - Security identity – is an identity that can be independently attested as belonging to the entity is is assigned (e.g., a PKI certificate and an associated private key)
- Credentials – which the other party supplies to help communicate and prove their ID (among other things)
  - e.g. An x.509 certificate
- Authentication – secure means of verifying the Credential(s)
  - e.g. Cryptographic signatures – hashes that are cryptographically verifiable (such as using asymmetric keys)
  - e.g. Challenge request – peer who asserts ownership of public key proves ownership by encrypting a challenge using their private key – which the challenger can verify using the public key
- Trust Stores – information that enables verification of the other party's credential when one Credential is used to help verify another ("chain of trust")
  - e.g. A list of trusted X.509 Certificate Authority (CA) certificates, which can be used to verify X.509 certificates provided by other parties
- Access Control Lists – to establish what a verified identity is allowed/not allowed to perform or access

Example: Mutual TLS Authentication



Server

Client

ClientHello(ver, supported_cipher_suites, c_rand)

Check supported version & suites

ServerHello(ver, cipher, s_rand, s_cert, cert_req)

Validate Server Certificate
Check signature and exp date
Check intermediate CA(s)
Check root against trust store
Check origin/CN
Check certs for revocation

Trust Store

CRLs

ServerHelloDone

ServerKeyExchange(s_key_data, signature)

ClientHello(Certificate)

Validate Client Certificate
Check signature and exp date
Check intermediate CA(s)
Check root against trust store
Check origin/CN
Check certs for revocation

Trust Store

CRLs

ClientHelloDone

Client Key Exchange(c_key_data)

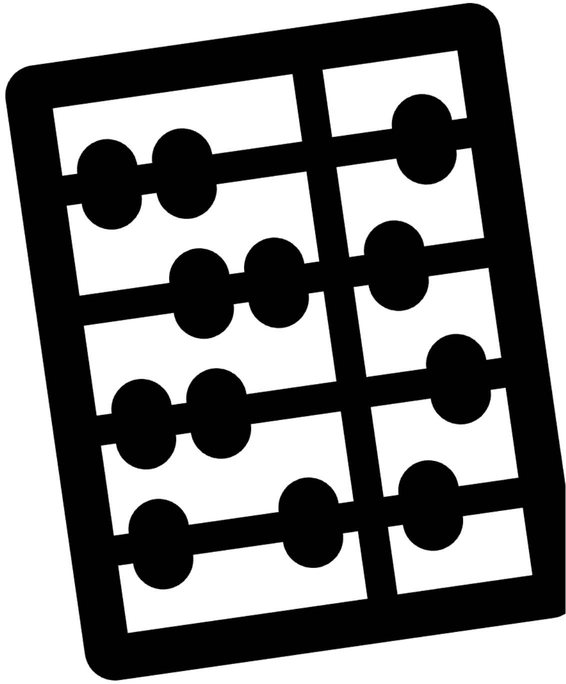
Certificate Verify(c_key_data, signature)

The list of trusted Certificate Authorities (CAs) is managed by the OS and/or at the application layer

Specific certs can be revoked via placement of the cert SN on Certificate Revocation Lists (CRLs) which can be consulted at run-time via the network or periodically cached

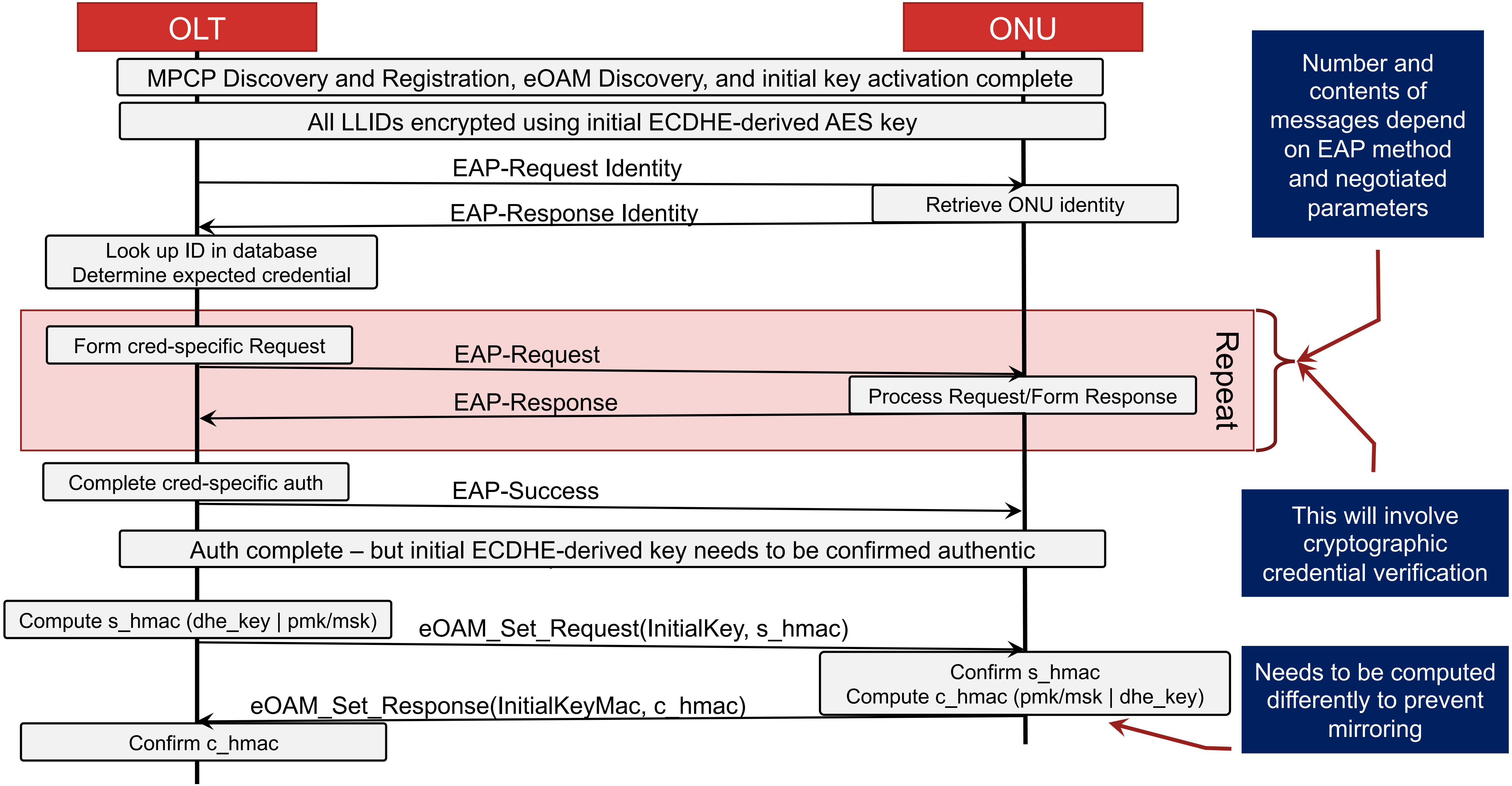
SIEPON MA - Approaches/assumptions:

1. SIEPON should *enable* authentication methods, while allowing the *policy* to be dictated/described by the operator
2. Credentials must be attested/verified
   - e.g. via challenge/response and hash/signatures
3. Trust store/lists must be operator-configurable (on OLT and ONU) and initialization/updates to the ONU trust store should be securely updatable by the operator via the OLT.
4. Initial AES key must ephemeral and mutually verified
   - To provide forward secrecy and prevent Machine in the Middle (MITM) attacks



Authorization Flow

CableLabs



OLT

ONU

MPCP Discovery and Registration, eOAM Discovery, and initial key activation complete

All LLIDs encrypted using initial ECDHE-derived AES key

EAP-Request Identity

Retrieve ONU identity

EAP-Response Identity

Look up ID in database
Determine expected credential

Form cred-specific Request

EAP-Request

Process Request/Form Response

EAP-Response

Repeat

Complete cred-specific auth

EAP-Success

Auth complete – but initial ECDHE-derived key needs to be confirmed authentic

Compute s_hmac (dhe_key | pmk/msk)

eOAM_Set_Request(InitialKey, s_hmac)

Confirm s_hmac
Compute c_hmac (pmk/msk | dhe_key)

eOAM_Set_Response(InitialKeyMac, c_hmac)

Confirm c_hmac

Number and contents of messages depend on EAP method and negotiated parameters

This will involve cryptographic credential verification

Needs to be computed differently to prevent mirroring

Some challenges (and opportunities…)

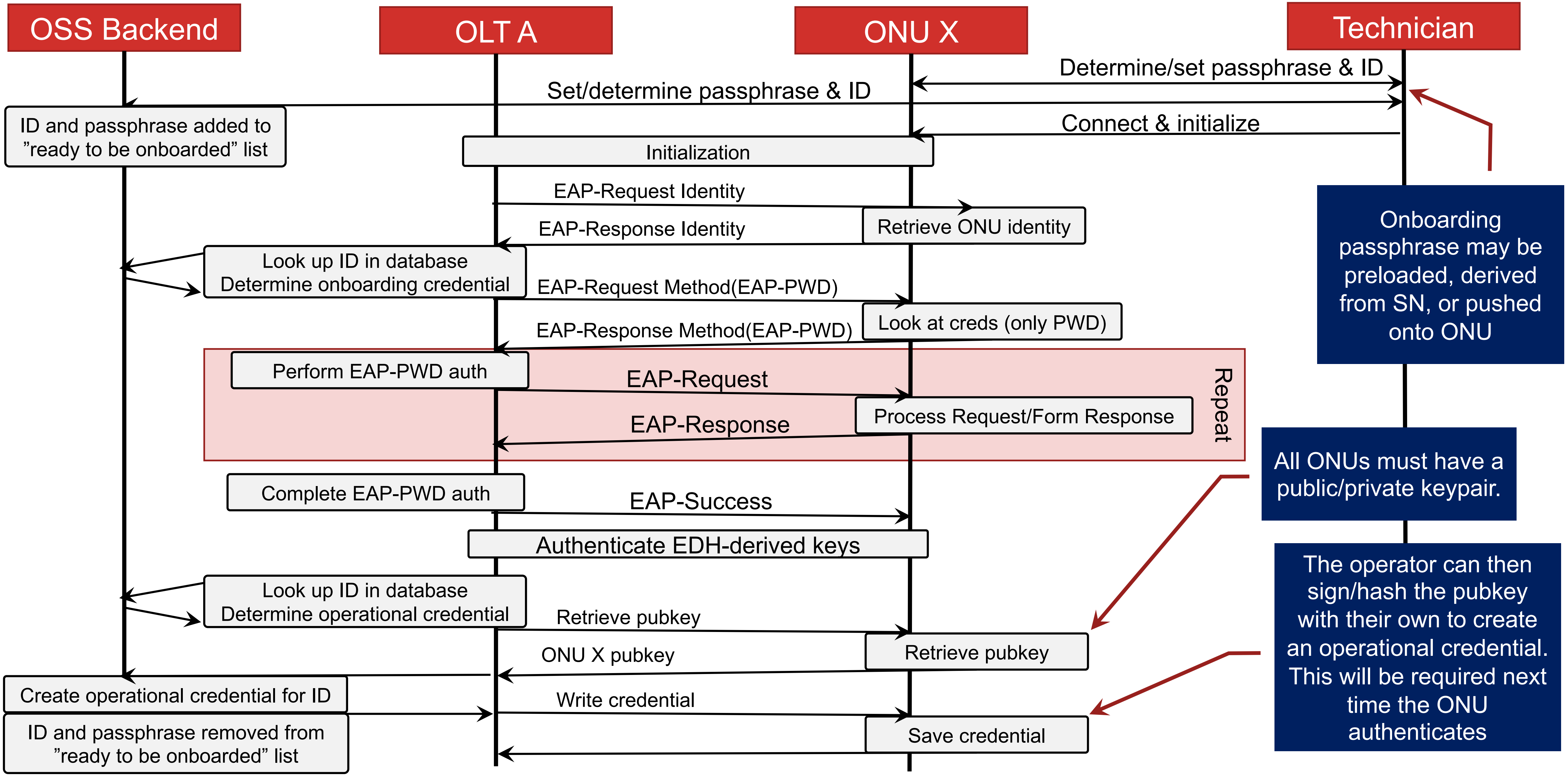
- Operators will want to deploy ONUs in different ways:
  - Sideloaded pub/private keypair or passphrase + ID
  - Sideloaded with certificate identifying the ONU and CA
  - Credential provided at time of deployment using a token/passphrase
- Authentication of the OLT by the ONU
  - ONU's basis of trust needs to be established/updated
- ONU credential update/revocation
  - Credentials may expire and need to be updated or revoked
- Trust store updates on ONU:
  - If/when infrastructure updates are performed, an ONU may need to restrict/expand/change the OLT(s) credentials it should trust
- Operators may want to enable auth in certain places/products
  - And they may want to roll out authentication/encryption on different dates

Can enable these with EAP, a couple Get/SetConfig attributes, and file read/write messages

Operational vs Onboarding Credentials

Operational Credential	Onboarding Credential
For ongoing authentication of the ONU	Just for onboarding the ONU
Certificate containing the ONU ID, public key, and anything else the operator wants	Passphrase or Certificate containing the ONU ID, public key, and onboarding token
Signed by operator or third-party	Unsigned or manufacturer-signed
Provided by operator to provide robust, ongoing trust	Provided by manufacturer to provide initial trust
Robust and attestable	Not robust on its own – depends on multi-factor authentication

Credential provisioning via passphrase



OSS Backend

OLT A

ONU X

Technician

Determine/set passphrase & ID

Set/determine passphrase & ID

ID and passphrase added to "ready to be onboarded" list

Connect & initialize

Initialization

EAP-Request Identity

EAP-Response Identity

Retrieve ONU identity

Look up ID in database
Determine onboarding credential

EAP-Request Method(EAP-PWD)

EAP-Response Method(EAP-PWD)

Look at creds (only PWD)

Perform EAP-PWD auth

EAP-Request

EAP-Response

Process Request/Form Response

Repeat

Complete EAP-PWD auth

EAP-Success

Authenticate EDH-derived keys

Look up ID in database
Determine operational credential

Retrieve pubkey

ONU X pubkey

Retrieve pubkey

Create operational credential for ID

Write credential

ID and passphrase removed from "ready to be onboarded" list

Save credential

Onboarding passphrase may be preloaded, derived from SN, or pushed onto ONU

All ONUs must have a public/private keypair.

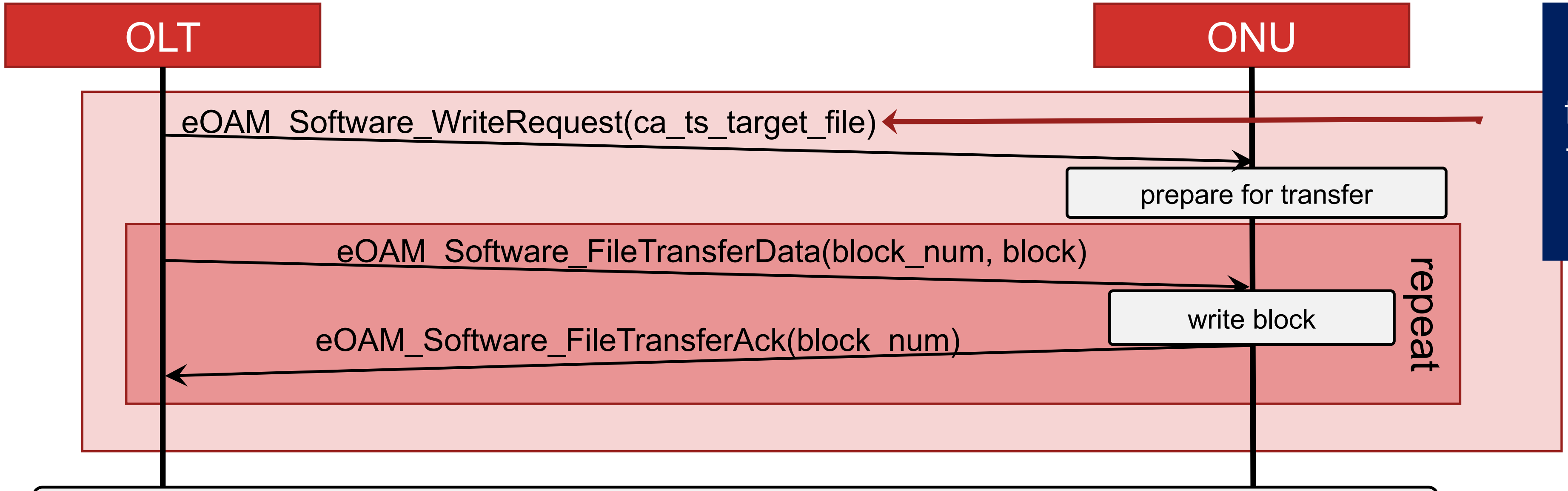
The operator can then sign/hash the pubkey with their own to create an operational credential. This will be required next time the ONU authenticates

Authentication of the OLT by the ONU

- To prevent an ONU from connecting to an unauthorized OLT, the ONU can be given knowledge about what constitutes a legitimate OLT – for instance:
  - ✓ OLT cert is signed by a trusted CA
  - ✓ OLT cert serial number is on an approved list
  - ✓ OLT cert serial number is not on a denied/revoked list
- The ONU's initial Trust Store and approve/deny access lists can be provided by the OLT right after initial provisioning
- OLT can update Trust Store and access lists at operator discretion

ONU Trust Store Updates

- To support mutual authentication, the ONU needs a basis of trust for validating the OLT credential(s)
  - Solution: Allow for initialization and updating of trust store by the OLT post-authentication using the eOAM_Software PDUs



OLT
ONU
eOAM_Software_WriteRequest(ca_ts_target_file)
prepare for transfer
eOAM_Software_FileTransferData(block_num, block)
write block
eOAM_Software_FileTransferAck(block_num)
repeat

Will define abstract filenames to indicate target trust store, for portability

ONU now has a credential (e.g. a X.509 certificate) that will authenticate outside of the context of provisioning and can enable the updating of credentials using the same mechanism

BACKUP MATERIAL

TODO

- Determine how sized
- 13.5

Attack/Defense Scenarios

1. Rogue/MITM OLT attempts
2. Rogue/MITM OLT never initiates authentication (after provisioning)
   - ONU will not enter operation since it can’t authenticate the OLT against the previously provided trust store