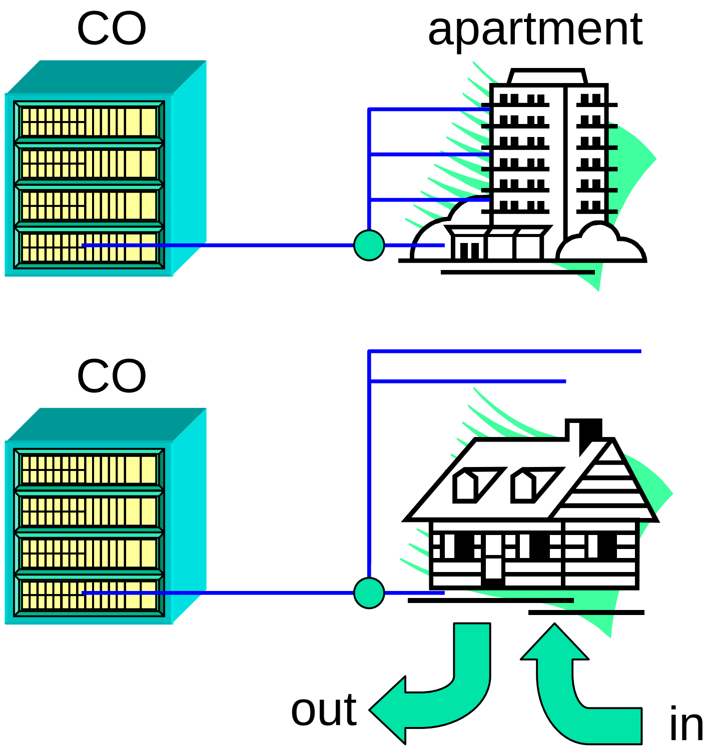
Authentication and Encryption in EPON

Ken Murakami: Mitsubishi Electric

Supporters
Yukio Fujimoto: NTT
Osamu Yoshihara: NTT

Purpose of Authentication

- Users without contract can be connected on PON section by Auto Discovery.
  - Pre establishment of optical fiber in newly-built apartment
  - Leaving of optical fiber at the moving
- Authentication on PON section is necessary!



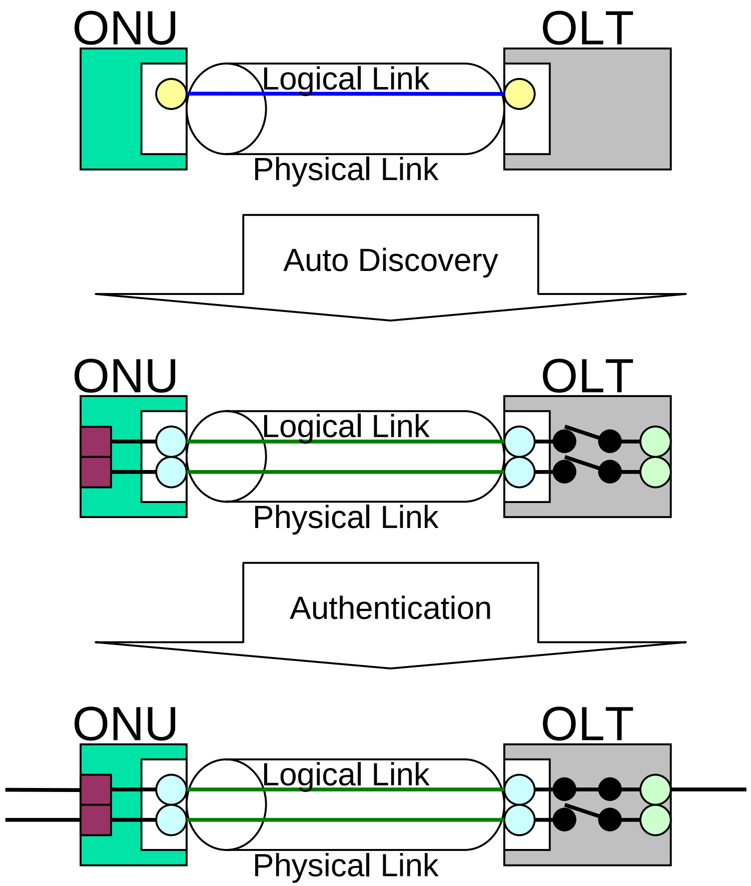
Authentication to whom?

- Discovered ONU contains one or more logical links.
- User makes a contract with service provider for each logical link.
- Authentication information (identity and password) are assigned to each logical link.

⇩

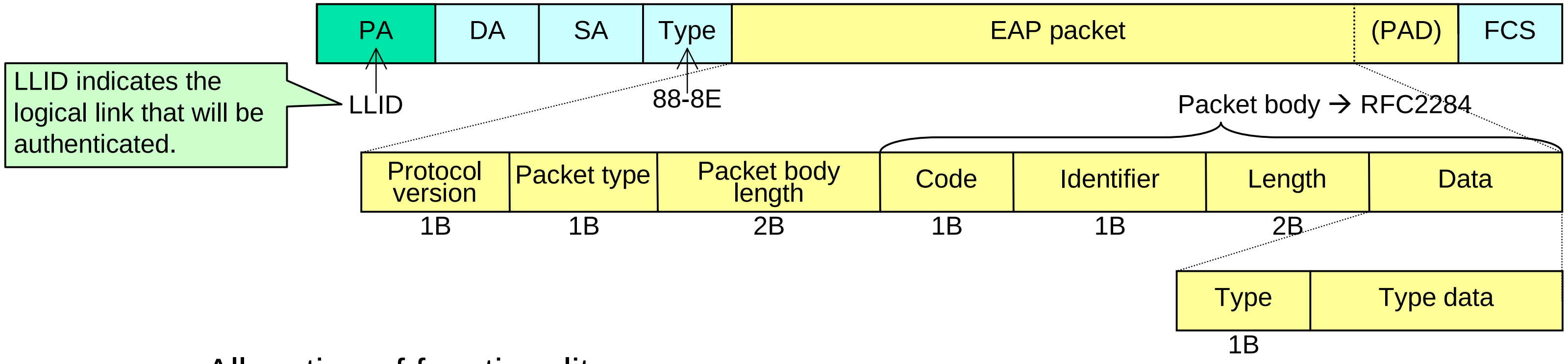
- Logical Link level authentication is suitable. Not for ONU.

- Behaviors
  - Users with contract can be connected toward SNI with the guarantee of bandwidth.
  - Users without contract should be assigned bandwidth for authentication.
  - Users without contract should not be connected to SNI.



Authentication Protocol

- 802.1x
  - EAPOL
    - Extensible Authentication Protocol encapsulation over LANs
    - EAP encapsulation with Ethernet MACs can be applied to EPON easily.



PA	DA	SA	Type	EAP packet	(PAD)	FCS

LLID indicates the logical link that will be authenticated.

LLID

88-8E

Packet body → RFC2284

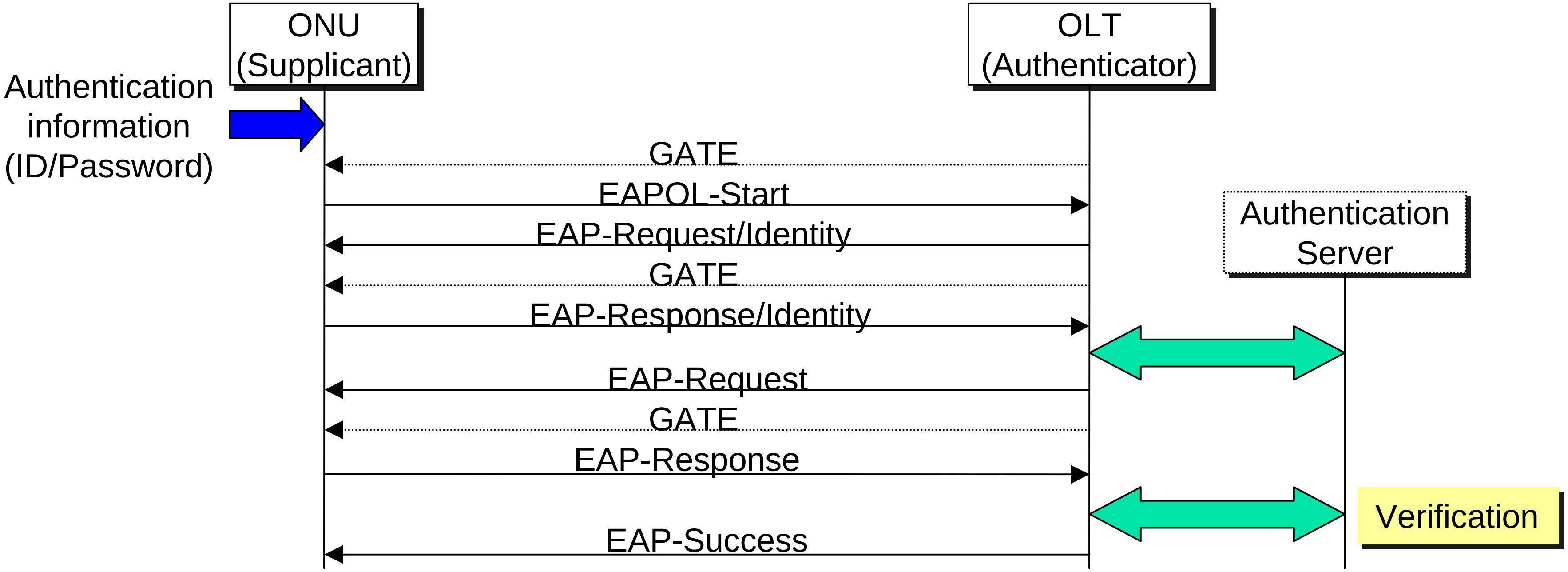
Protocol version	Packet type	Packet body length	Code	Identifier	Length	Data
1B	1B	2B	1B	1B	2B	

Type	Type data
1B	

- Allocation of functionality
  - Authenticator →OLT
  - Supplicant →ONU
  - Authentication Server →Implementation matter
    - External equipment
    - Inside OLT
- Two types of message flow
  - Supplicant initiated
  - Authenticator initiated

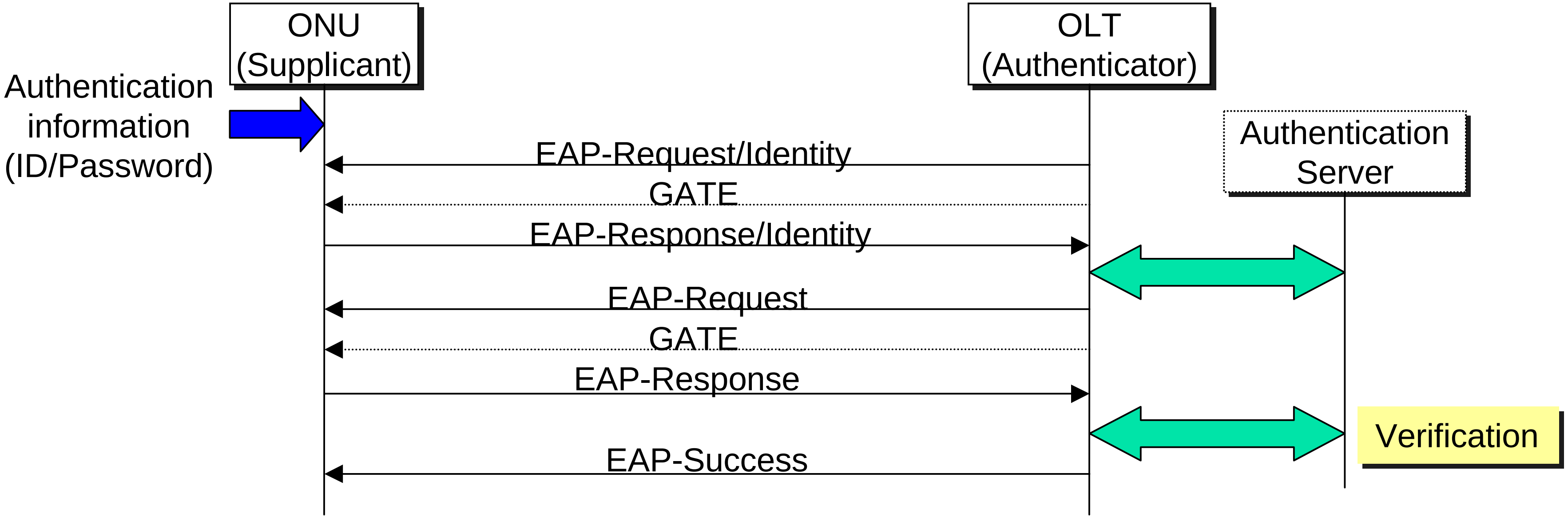
Message flow (1)

- Supplicant initiated
  - Only GATE for authentication same as normal GATE should be periodically sent.



Message flow (2)

- Authenticator initiated
  - In addition to GATE, EAP-Request/Identity should be periodically sent.

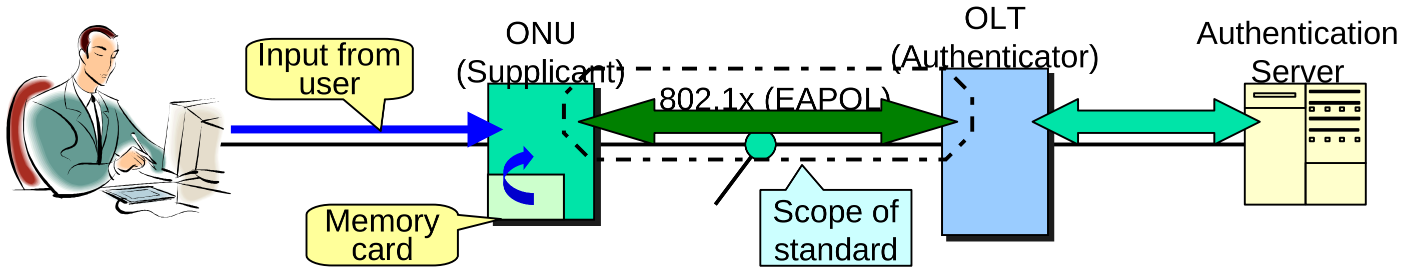


Authentication mechanism

- Password based authentication
  - EPON is wired and closed network. → no “man in the middle attack”
  - Authentication information is transferred in the upstream. → difficult to eavesdrop
  - Same intensity of authentication as P2P or dial-up is enough!
  - Long length of password such as WLAN is not necessary.
- Exchange of initial master key
  - 802.1x can exchange initial master key for encryption using EAP-TLS (RFC2716) as an example.

ID and Password

- Authentication information (Identity, Password)
  - Pre-registered in Authentication Server
  - How to give authentication information to ONU is implementation matter.
    - Memory card on ONU
    - Input from user .etc
  - Authentication Protocol on PON section is independent of the location of authentication server and the method how to give authentication information to ONU.



Purpose of Encryption

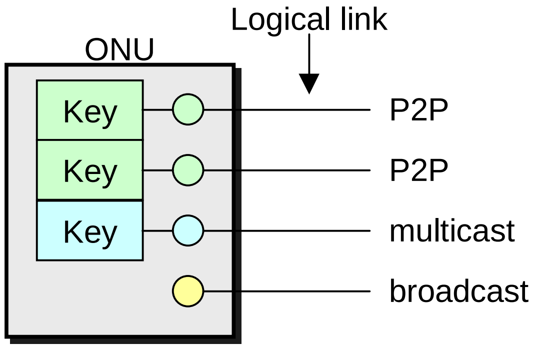
- Downstream encryption
  - Prevent eavesdropping of OAM traffic, MPCP messages and user frames
    - User frames are encrypted by Higher layer protocol. But it is not enough.
    - Eavesdropping of GATE enables users to analyze the traffic of other users.

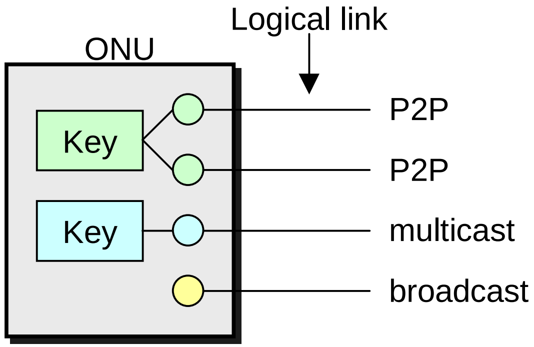
⇩

  - Encryption on PON section is necessary!

Encryption to whom?

- Two candidates
  - Encryption to each logical link
    - Common algorithm
    - Individual keys for each logical link (P2P)
    - Individual keys for each group (multicast)
    - No encryption for broadcast
    - Encryption for authenticated logical link
  - Encryption to each ONU
    - Common algorithm
    - Individual key for each ONU (P2P).
    - Individual keys for each group (multicast)
    - No encryption for broadcast
    - Maintenance of relationship between LLIDs and physical ONUs
    - Encryption for discovered ONU
- Our recommendation = Encryption to each logical link
  - MPCP is performed per logical link.
    - Grant assignment → GATE is issued to a certain LLID.
    - Bridge → Logical link corresponds to bridging port.
  - MPCP does not care physical ONU at all.



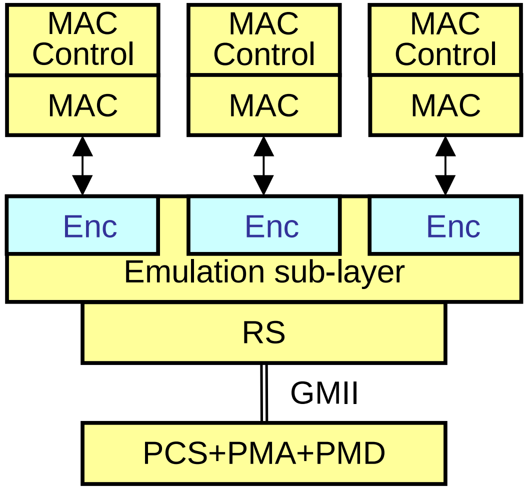


Encryption algorithm

- Encryption algorithm
  - TBD
  - Packet length should be maintained.
    - No overhead due to encryption

Encryption layering

- Emulation layer has optional encrypt and decrypt function for each logical link separately.
  - Key update indication (e.g., encryption flag, key index) is included in preamble.
  - Encryption range
    - MAC frame (DA – FCS)
    - Preamble including LLID and key update indication should not be encrypted.
    - All of frames including MPCP messages and OAM frames on authenticated logical link are encrypted.



Creation of Encryption key (initialization)

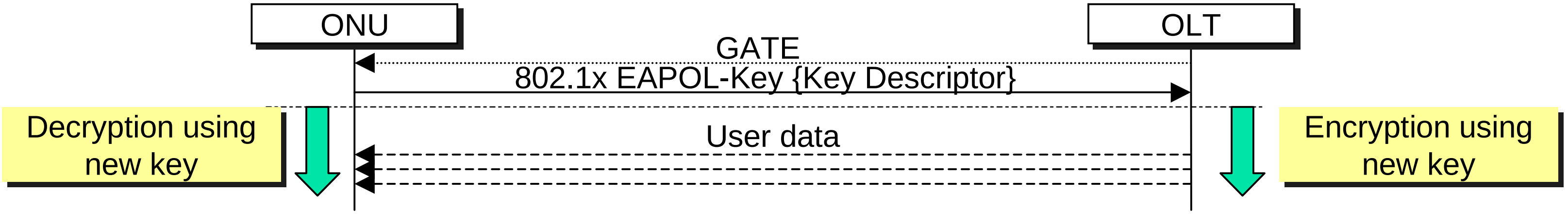
- Process
  - Initial master key is exchanged in the authentication.
  - Master session key is derived from master key. (802.11i Annex J)
  - Transient session key is derived from master session key. (802.11i Annex I)
  - Encryption key is truncated from transient session key.

Encryption key update procedure (Re-keying)

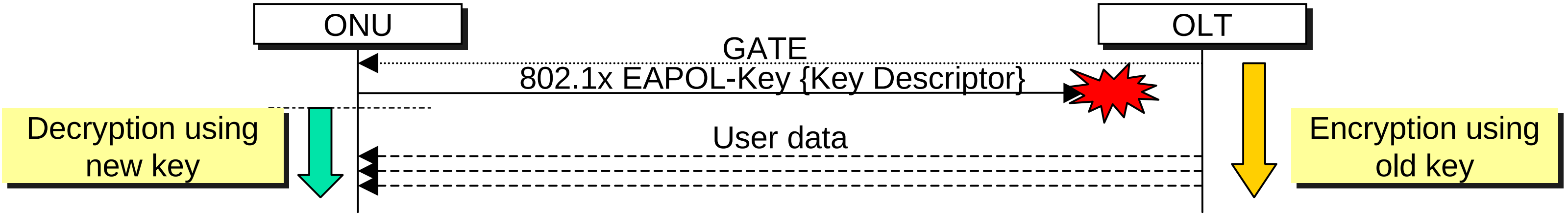
- Encryption key can be updated periodically. The interval of update depends on algorithm.
- 802.1x based procedure
  - EAPOL-Key frame
  - Key Descriptor for the selected encryption algorithm should be specified in 802.1x.
  - MAC Control layer is responsible for the procedure.
- Key creation process
  - Master session key is derived from the current transient key and from the nonce contained in EAPOL-Key frame.
  - Transient session key and encryption key are derived using the same process as in the initialization.

802.1x based procedure

- Message
  - EAPOL-Key frame (ONU→OLT)



- Problem
  - Loss of frame
    - Disagreement of key between OLT and ONU

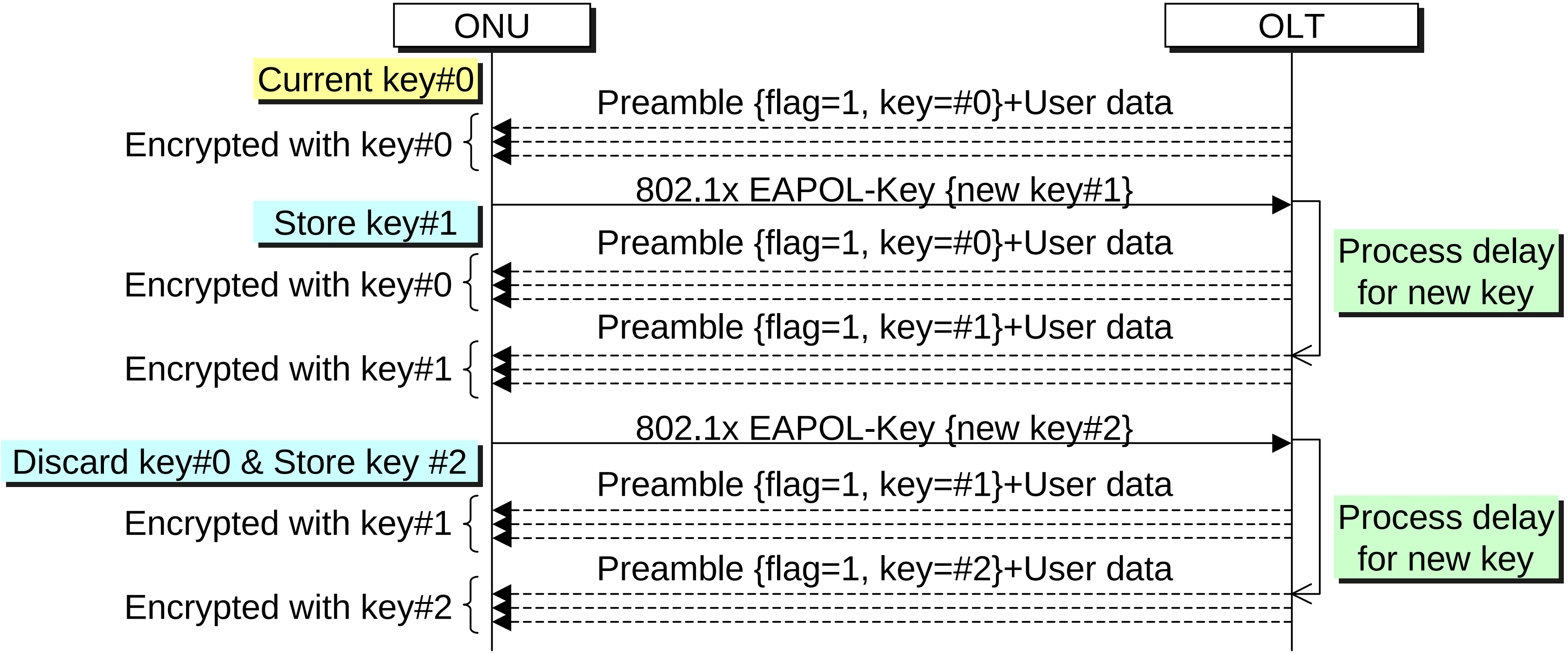


Frame by frame indication of encryption

- Indication of encryption is necessary frame by frame.
  - Encryption flag
    - Encrypted or not encrypted
  - Key index
    - Current used key
    - Significant when encryption flag is set to 1
  - Others
- Use of preamble

Usage of flag and key index

- Encryption function stores 2 keys for smooth transition.
- Current used key is reported in preamble.


ONU
OLT
Current key#0
Preamble {flag=1, key=#0}+User data
Encrypted with key#0
802.1x EAPOL-Key {new key#1}
Store key#1
Preamble {flag=1, key=#0}+User data
Process delay for new key
Encrypted with key#0
Preamble {flag=1, key=#1}+User data
Encrypted with key#1
802.1x EAPOL-Key {new key#2}
Discard key#0 & Store key #2
Preamble {flag=1, key=#1}+User data
Encrypted with key#1
Process delay for new key
Preamble {flag=1, key=#2}+User data
Encrypted with key#2

Conclusion

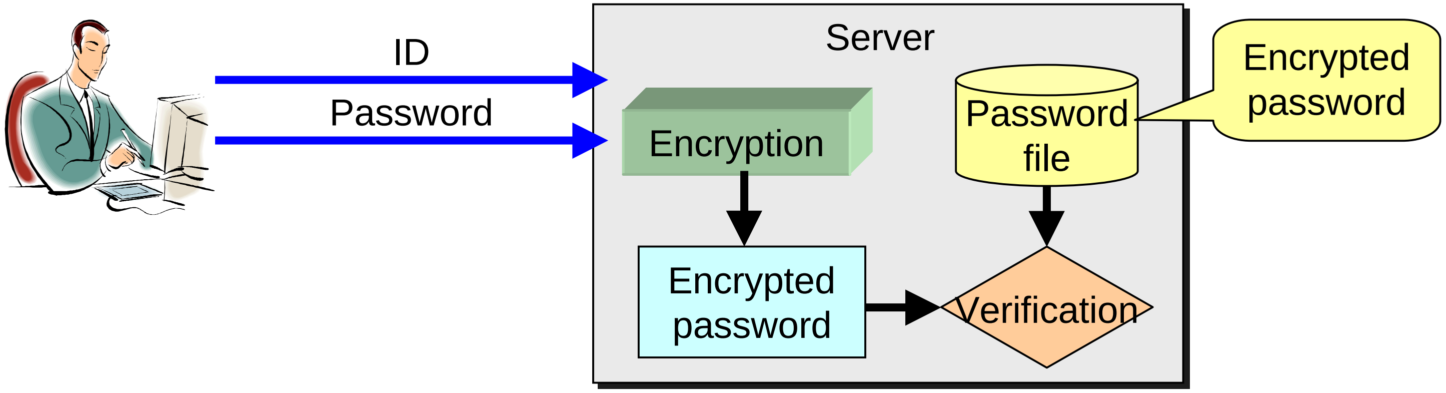
- Authentication
  - 802.1x based authentication protocol is applied on EPON.
  - Logical link level authentication is supported.
  - Initial master key for encryption is exchanged in the authentication.
- Encryption
  - All of frames including OAM frames and MPCP messages are encrypted in the downstream.
  - Logical link level encryption is applied.
  - Encryption is performed on the authenticated logical link.
  - Emulation layer has encryption and decryption function.
  - Entire MAC frame (DA~FCS) is encrypted.
  - MAC control layer is responsible for encryption key update procedure.
  - Creation of encryption key and re-keying based on 802.1x and 802.11i
  - Encryption flag and key index are indicated in preamble frame by frame.

Issues

- Authentication
  - Exchange of initial master key for encryption
    - EAP-TLS
    - EAP-SIM
    - …
- Encryption
  - Message authentication (upstream encryption)
  - Encryption algorithm
  - Key exchanging for multicast

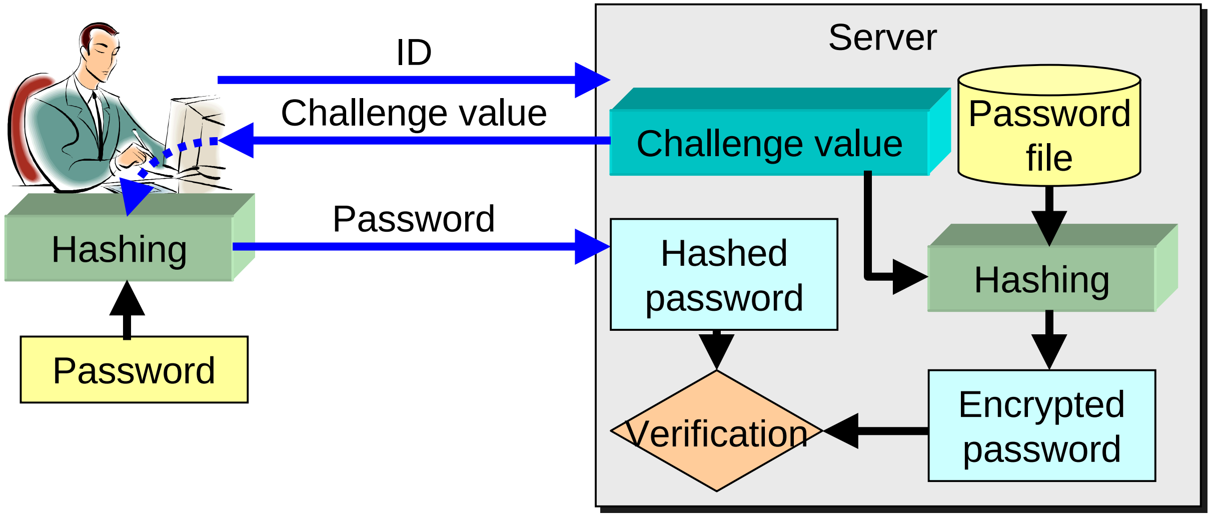
Appendix 1
– Authentication mechanism

- PAP (Password Authentication Protocol: RFC1334)
  - Server maintains encrypted password in the password file.
  - Password from user is not encrypted.
  - Server encrypts password from user and verifies it with encrypted password maintained in the password file.



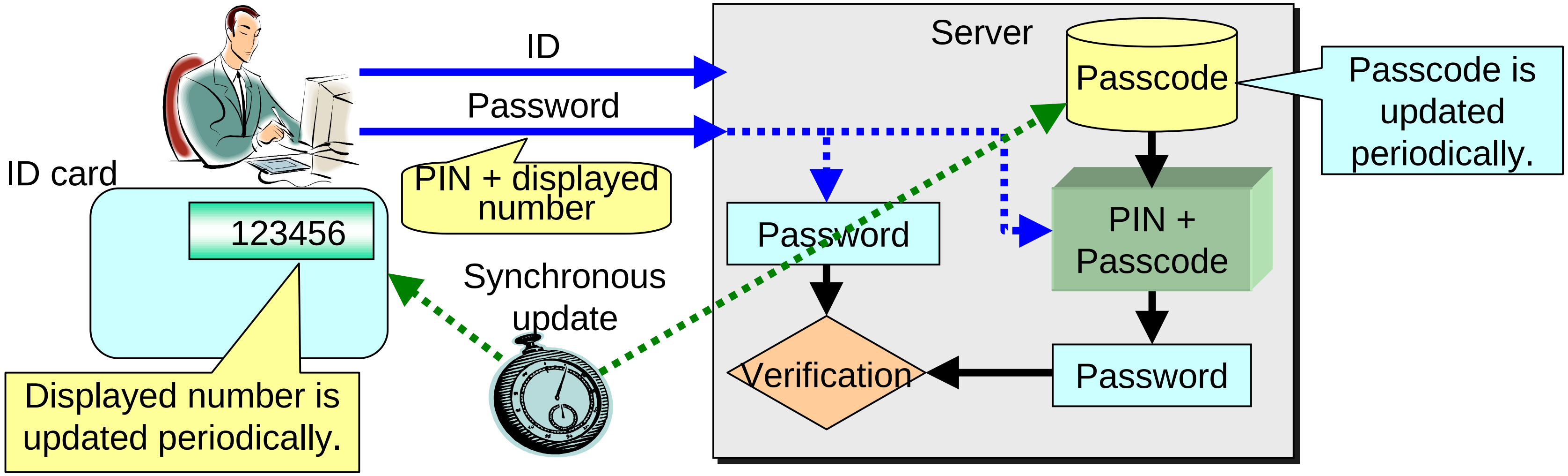
Appendix 1 – Authentication mechanism

- CHAP (Challenge Handshake Authentication Protocol)
  - Server maintains password in the password file.
  - Server creates challenge value and gives it to user.
  - Password from user is hashed with the challenge value given from server.
  - Server hashes password in the password file with the challenge value sent to user and verifies it with hashed password from user.



Appendix 1
– Authentication mechanism

- OTP (One Time Password) – Time synchronous
  - Dedicated hardware (ID card) is necessary.
  - Displayed number on the ID card is periodically updated at a fixed interval.
  - Passcode on the server is also periodically updated at a fixed interval.
  - The timing of password update and that of passcode update are synchronous.
  - Password from user consists of PIN code and displayed number.
  - Server creates password from PIN code and passcode at the receipt of password from user, and verifies it with password from user.


ID
Password
PIN + displayed number
ID card
123456
Displayed number is updated periodically.
Synchronous update
Server
Passcode
Passcode is updated periodically.
Password
PIN + Passcode
Verification
Password