# Next Generation Access Network (in)security

## Security proposal for NGN standardization

**4th ETSI Security Workshop**

**Sophia Antipolis, France**

**13 -14 January 2009**

Paolo DE LUTIIS, Roberta D'AMICO, Luciana COSTA

Telecom Italia SpA

Via Reiss Romoli 274, Turin Italy

# Next Generation Access Network (in)security

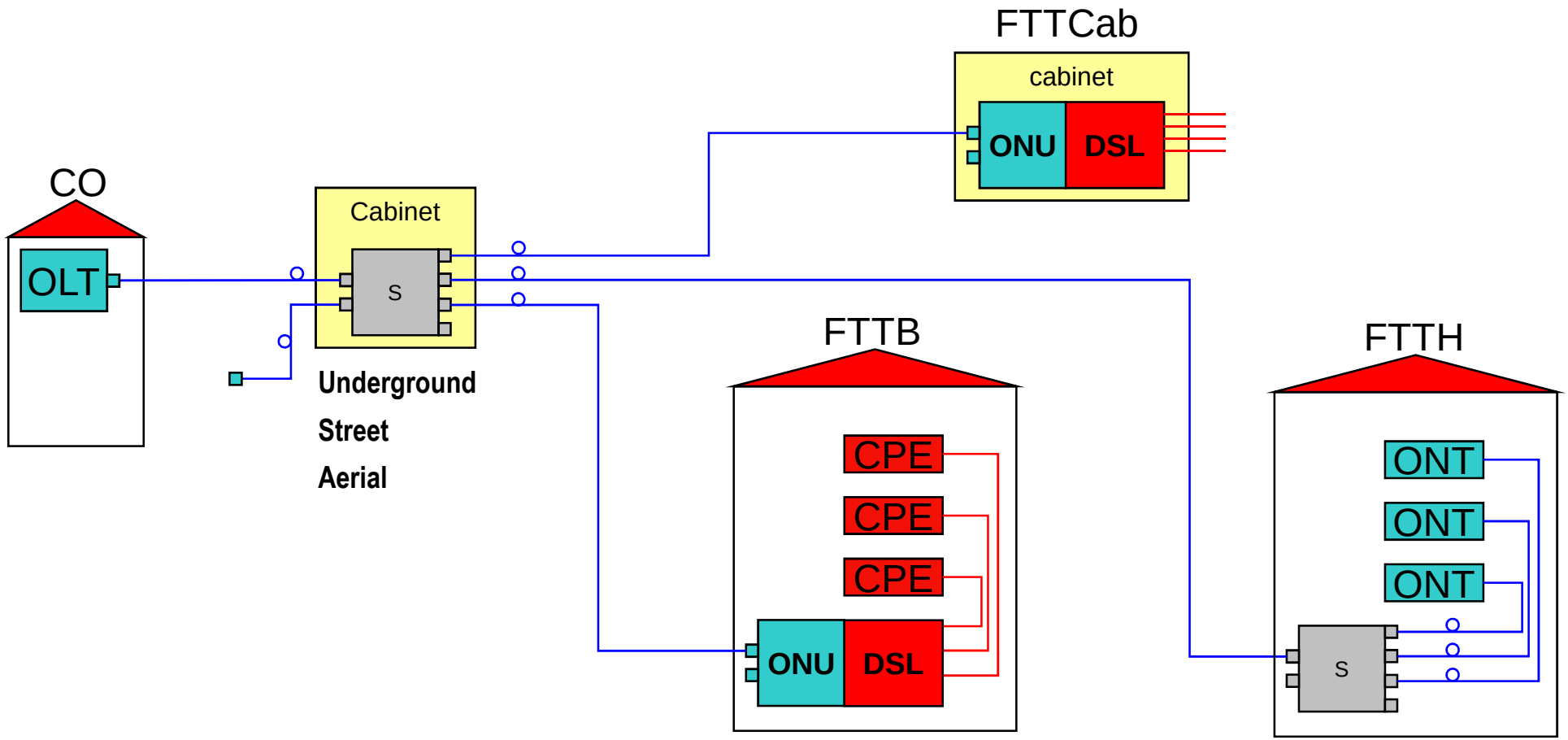
Summary:

- Background: GPON-based NGA Networks (ITU-T G.984.x)
- GPON-based NGA main security threats
- Profiling a complete security mechanism for GPON
- Conclusions

# Background: ITU-T G.984.x Passive Optical Network (PON)

- In order to fully deploy the potentiality of the NGN and related services (e.g. Video-On-Demand, interactive gaming, video conferencing), telco Operators are migrating their broadband access network (copper based) to the ultrabroadband fiber-based access networks.
- Passive Optical Networks (PON) appear to be the best candidate for the Next Generation Access (NGA) network.
- GPON is an International Telecommunication Union (ITU)-backed standard, supported by the Full Service Access Network (FSAN) group, a forum comprising mostly carriers. GPON can support to 2.5 Gbps downstream and 1.25 Gbps upstream data transmissions
- Like all PON standards, GPON uses a point-to-multipoint access architecture downstream (to the user) and a point-to-point architecture upstream.

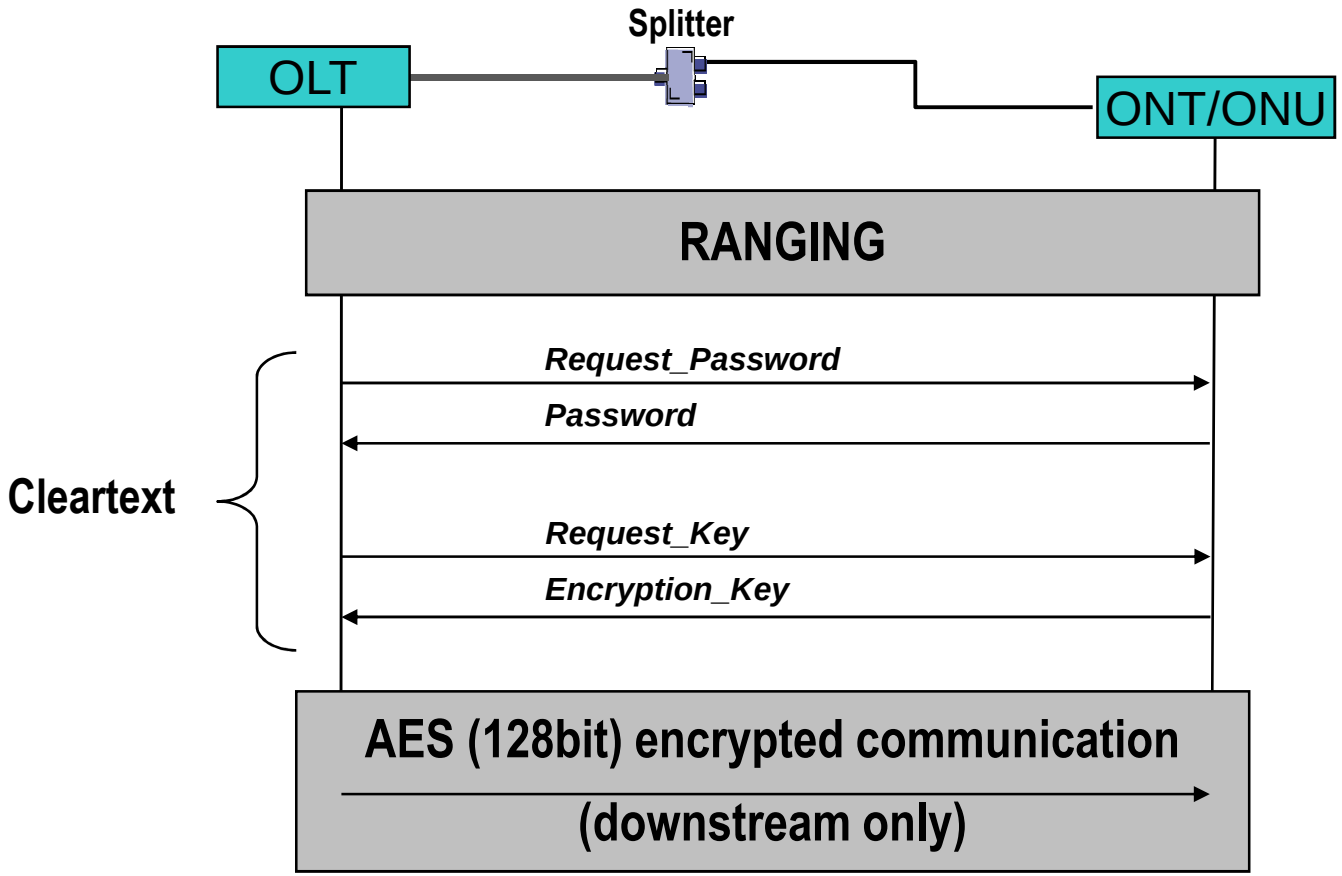
# Background: (G)PON deployment scenarios



## Background: currently defined ITU.T G.984.3 security mechanisms

- Currently G.984.3 defines two identification/activation mechanisms
  - Method A: pre-provision of ONU/ONT serial number to an OLT
  - Method B: the serial number is not known in advance and the OLT activates the ONT/ONU on the fly
- There are currently 2 security mechanisms, both specified as optional:
  - Authentication of the ONU/ONT by means of (PLOAM) password;
  - Encryption of the downstream traffic only (from the CO to the customer side) by means of AES (128 bit)
    - **The upstream traffic is not considered at risk because the high directionality of the PON components (it is assumed that the traffic sent from one ONT to the OLT cannot be sniffed by other ONTs).**

# Background: currently defined ITU.T G.984.3 security mechanisms (optional)

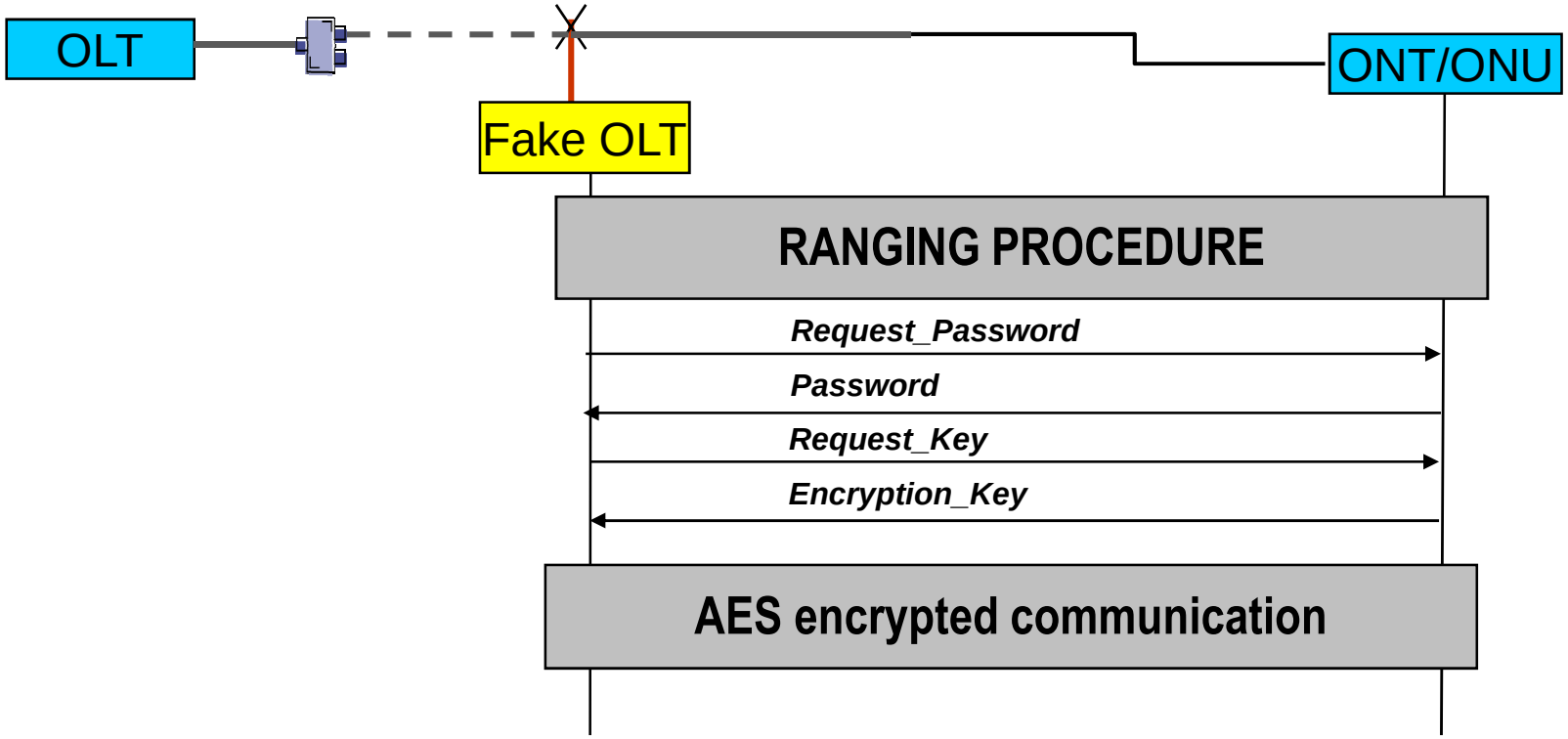


## GPON main security threats

- The security mechanisms already defined are based on the assumption that all the GPON elements will be strongly physically protected. GPON communication are vulnerable to severe security issues, such as:
  - **Fake/Forged OLT: currently no OLT identification and authentication mechanisms have been specified**
  - **Man In The Middle (MITM) attacks**
    - Passive attacks: password and keys sent as cleartext
    - Active attack: sensitive PLOAM messages are not authenticated (e.g. PASSWORD, encryption KEY)
  - **Several kind of DOS (Denial of Service) at GPON level e.g. during the activation phases.**

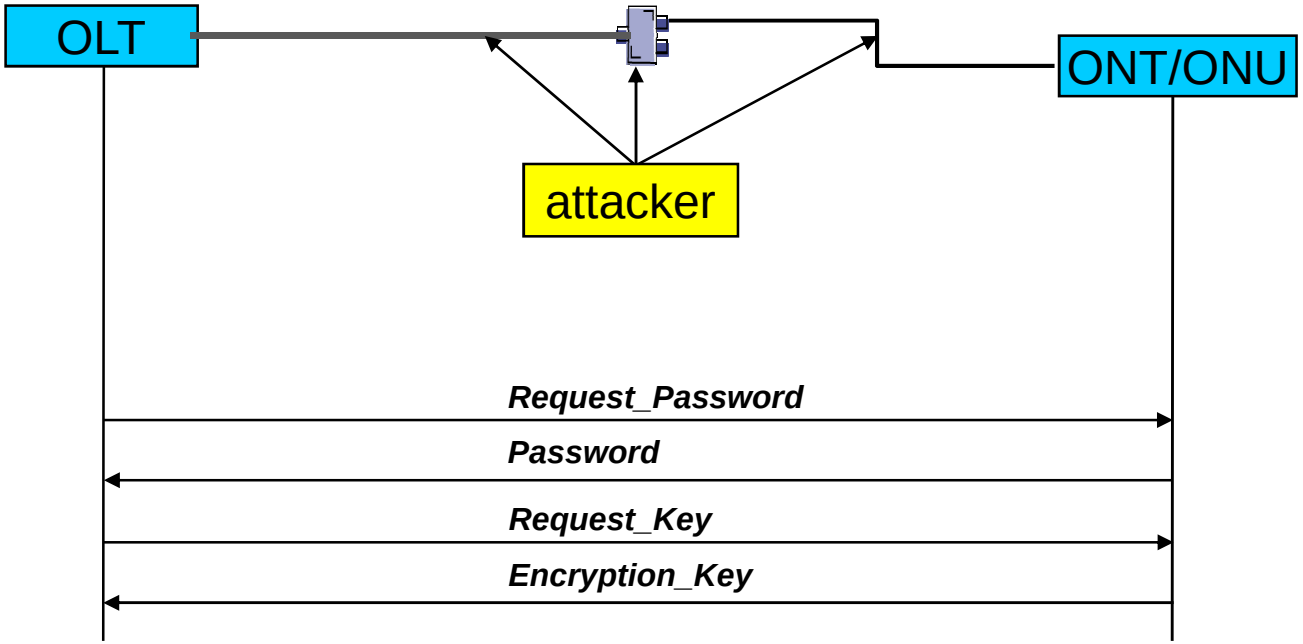
# Main Security Threats: Fake OLT scenario (1/3)

The ONT/ONU have no means to detect the fake OLT



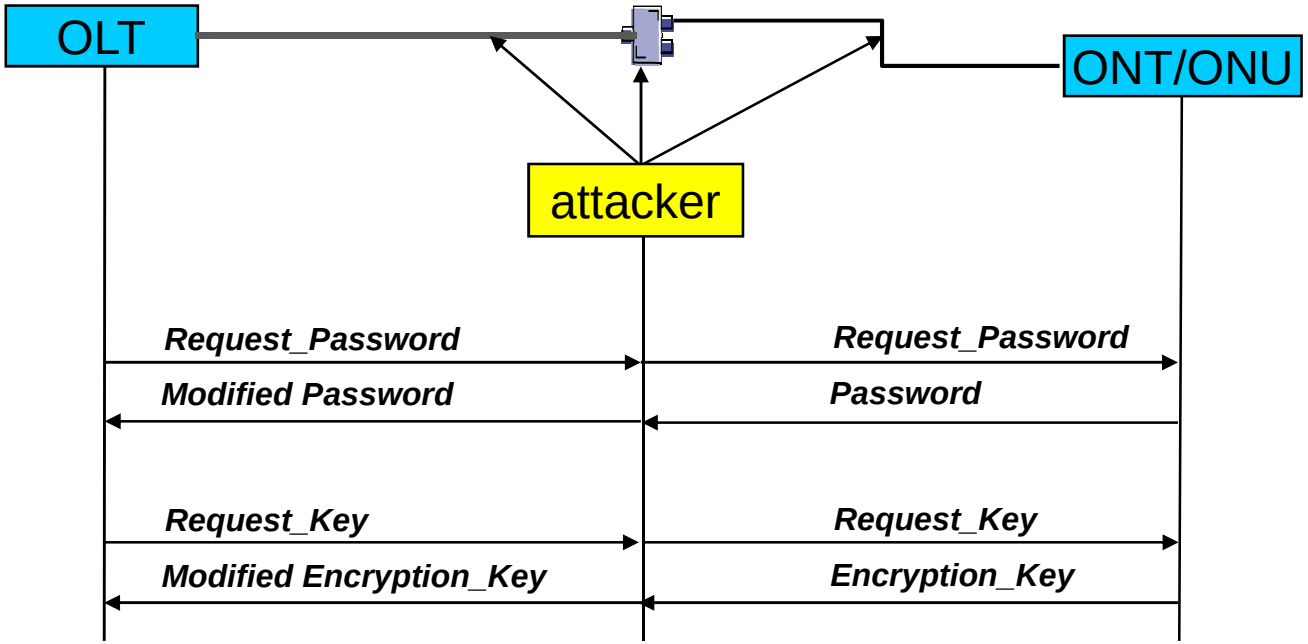
# Main Security Threats: Passive MITM (2/3)

The attacker can intercept data traffic and sensitive (unencrypted) information: authentication passwords and encryption keys (to be used later for e.g. unlawful interception)



# Main Security Threats: Active MITM (3/3)

The attacker can modify sensitive (unencrypted) information: authentication passwords and encryption keys (in order to cause e.g. denial of service)



## Main Security Threats: A robust security mechanism is missing

- Although some of these security threats could be addressed with security mechanisms implemented at the physical layer or at higher layer (e.g. IPSec), the GPON-based NGA remains vulnerable to several security attacks.
- It is important that the GPON infrastructure provides the missing security mechanisms in order to follow the “layered security” principle and to minimize OPEX and CAPEX of the Operators
- All the currently defined mechanisms cannot provide an adequate security level to the Operator needs.
- Moreover the described security gap in the standard could cause the definition of proprietary solutions.

## Profiling a complete security mechanism for GPON

In order to face the listed security threats it is needed to add a new, complete, security mechanism. Such a mechanism should provide the following features:

- Strong authentication: the password used for the authentication should not be sent as cleartext (to avoid a passive MITM attacks)
- Mutual authentication: also the OLT should be authenticated by the ONT/ONU (to prevent fake OLT)
- Message authentication: the most sensitive messages should be authenticated (to prevent packet injection during active MITM attacks).
- Key management: the keys used for the encryption of the downstream traffic should be generated and exchanged in a secure way (to avoid privacy violations).

## How to enhance the current security mechanism: a proposal

The enhanced security mechanism could be based on the following:

- The mutual authentication could be based on a challenge and response mechanisms (e.g. RFC2617) and a pre-shared secret provisioned on both, the OLT and the ONT, never sent as clear text.
  - **For example the current GPON Request_Password and Password messages can be used to convey the "challenge and response" values instead of the actual password**
- The AES encryption keys could be generated independently by the OLT and the ONT/ONU.
  - **For example the current Request_key and Encryption_key messages can be used to convey parameters to be used in conjunction with the shared secret for the generation of the encryption keys, without the need to send any sensitive information as clear text.**
  - **The preshared secret permits also the authentication of the exchanged messages in order to protect them from security attacks (messages forging).**

## Conclusions

- The current specification cannot address properly several severe security issues:
  - **Fake/Forged OLT, passive and active MITM, DOS during GPON activation procedures**
- At present, in order to cope with these security threats, the operator should adopt additional security mechanisms (e.g. at physical layer) and then increase its OPEX and CAPEX
- There is a need to increase the security of the current GPON systems, by means of a new security mechanism. Such a mechanism should fill in the security gap by adding the following features:
  - **Mutual and strong authentication between the OLT and ONT/ONU**
  - **Secure key management for the generation and exchange of the (AES) encryption keys**
  - **Low impact on the current GPON technology and Standards**