# OWE Pentest

Pass the Salt 2026 - Rumps

Ajabep - @ajabep@infosec.exchange

KPN REDteam

# Just a FYI

- Some enterprise Wi-Fi systems are particularly aggressive when you try to mess with them
  - (and even when you don’t try!)

- Please, don’t annoy the event nor the venue 💗

# Context

- Pass the Salt is hosted by Université Catholique de Lille
- The Wi-Fi name (SSID) is `ICL_INVITE`.

Compte WiFi - WiFi Account

**WiFi-Université Catholique de Lille** <[redacted]>
to

Bonjour [redacted]

Vous recevez ce mail suite à une demande de création de compte d'accès au réseau WiFi invité de l'Institut Catholique de Lille.
Cette demande a été faite le 29/06/2026 par [redacted]

Les informations concernant ce comptes sont les suivantes :
[redacted]

Validité du 29/06/2026 au 02/07/2026 inclus.

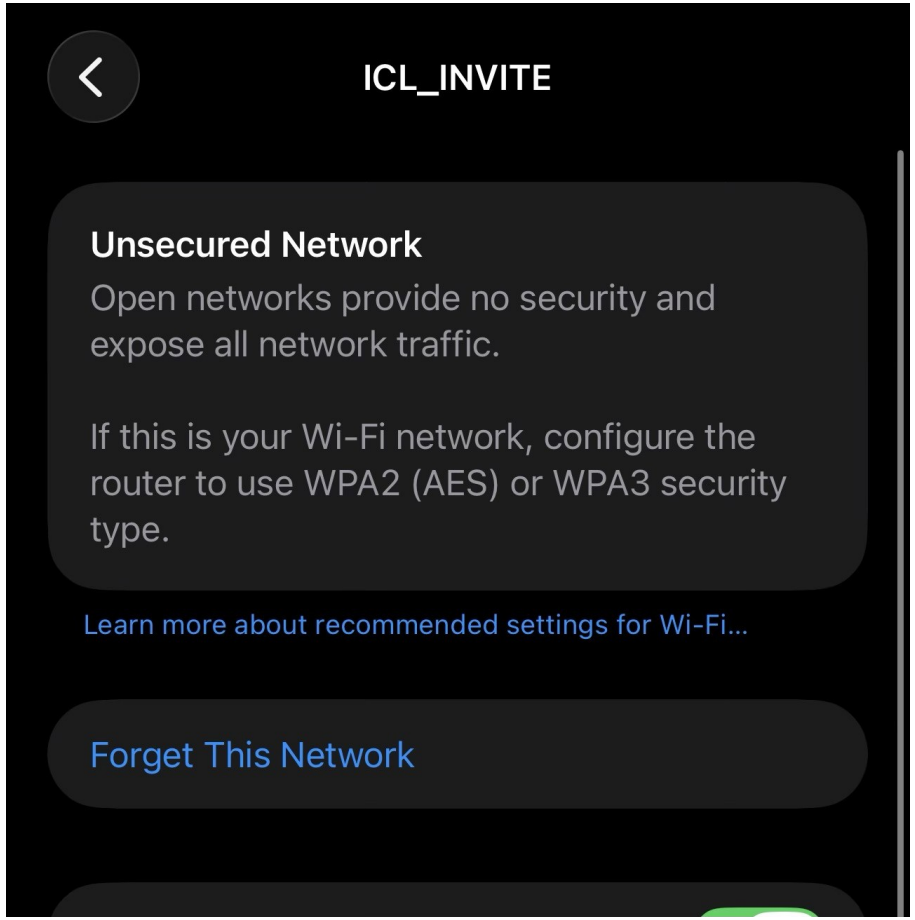
Les informations techniques d'accès au réseau WiFi invité sont :

**SSID : ICL_INVITE**
**Identifiant :** [redacted]
**Mot de passe :** [redacted]

# ICL_INVITE

- Just an open Wi-Fi
- With a captive portal
  - Probably based on MAC addresses
- Traffic is in cleartext over the air

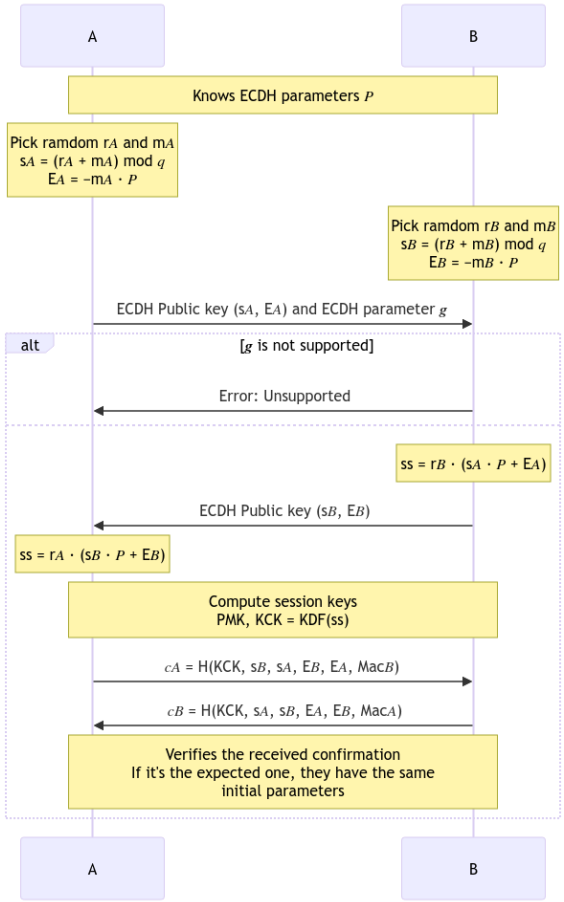
Should we recommend the University to migrate on an Encrypted Open Wi-Fi?



# OWE?

- WPA-3 equivalent of Open Wi-Fi (thus without password)
  - Sometimes named “WPA3-Open”
- Defined in the IEEE 802.11 standard
  - Enforced by “Enhanced Open™” certification, defined by the Wi-Fi Alliance “Opportunistic Wireless Encryption Specification”
- Has a “transition” mode
- Uses internal security requirements of WPA3
  - Requires Management Frame Protection, PMK caching, etc.
  - Uses the *SAE Handshake*

# SAE variant for Open Wi-Fi




- SAE stands for “Simultaneous Authentication of Equals”
- ECDH exchange before the Wi-Fi 4 way-handshake
  - Based on Dragonfly protocol (RFC 7664), based on SPEKE
- Derives a PMK from the ECDH exchange

# Encrypted Open Network, end of the game?

(spoiler: nope!)

- In transition mode, some previous clients are using only the unencrypted network
- No AP Authentication (“Evil-Twin”/“Rogue AP”).
  - AP transition based on the RSSI & technology (and other variables).
- “Think out of the box”™
  - Wi-Fi configurations
    - Using different bands, channels and bandwidth
    - Configuration inconsistencies between BSS
  - Network Pentest Edition
    - Multicast & broadcast traffic, Isolation between clients
    - MAC address filtering
    - Attacks on routers and on clients, network interceptions via ARP or ICMP type 5
    - Social Engineering

# What should you use at Pass-The-Salt?

- Eduroam. Always. But you need credentials. From any university in EU.
  - No, the absence of certificate is not really a vulnerability in Enterprise Wi-Fi
    - Speak to me to know more
- Your 5G
- Or a VPN and cross fingers