WORKSHOP GARR 2026

NET MAKERS

La fine della transizione: WPA3 nelle reti Wi-Fi

Jan Reister

Università degli Studi di Milano

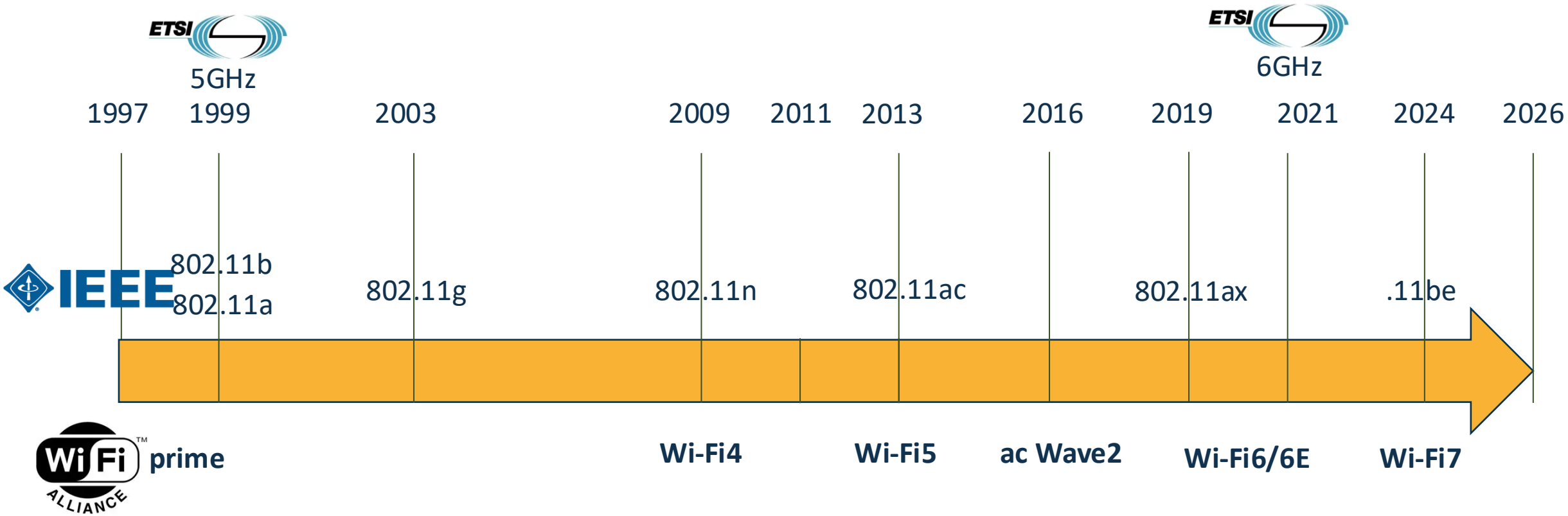
Da dove arriviamo

Cicli ricorrenti nella tecnologia WLAN

WORKSHOP GARR 2026

NET MAKERS

Evoluzione della sicurezza Wi-Fi (802.11)



Cicli tecnologici di 4-5 anni

Wi-Fi: le costanti del successo

Prestazioni: efficienza spettrale, datarate elevati, roaming, multiutenza e affidabilità.

Compatibilità: coesistenza di generazioni differenti, misure di compromesso e penalità crescenti.

Sicurezza: confidenzialità, integrità e disponibilità in scenari complessi

- WEP, TKIP
- WPA2 PSK offline brute force
- KRACK (Key Reinstallation Attack)
- WPA3 Dragonblood (SAE Side-Channel)
- FragAttacks
- SSID Confusion…



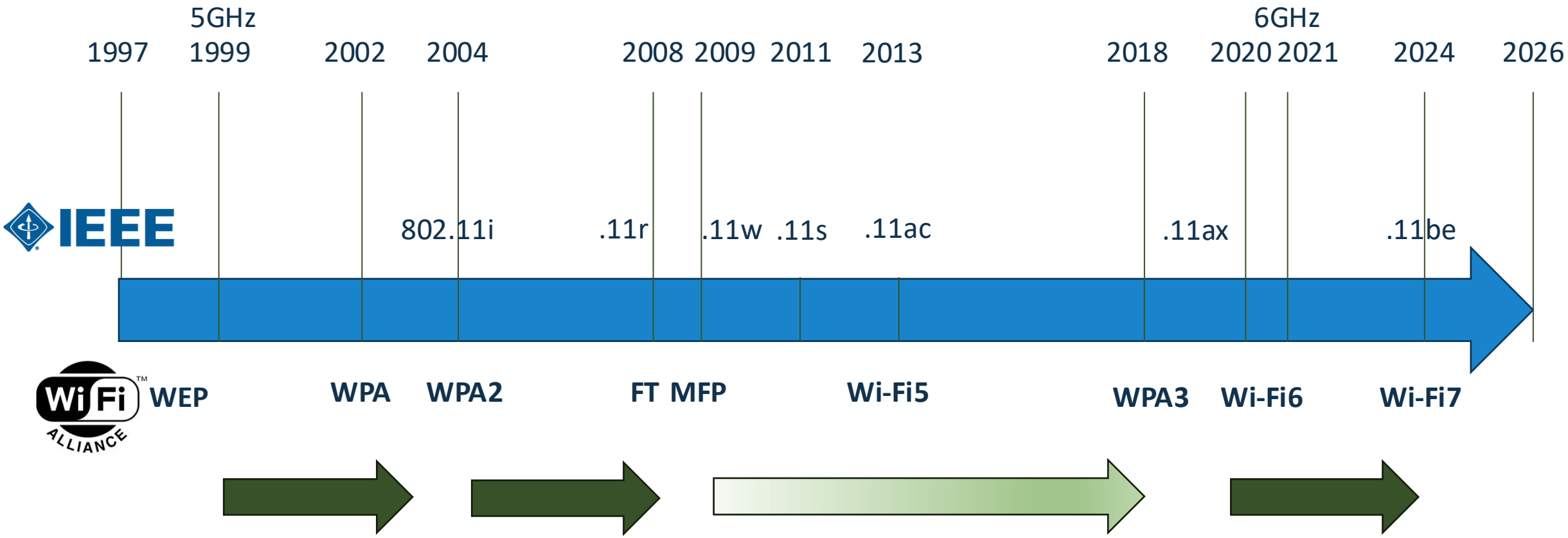
Strange bedfellows

- Autorità normativa
- IEEE
- Wi-Fi Alliance
- Chipmakers
- Device makers
- Consumatori finali

priorità e tempi divergenti



Evoluzione della sicurezza Wi-Fi (802.11)



1 - Il paradosso della compatibilità

TKIP e il provvisorio definitivo

WPA/WPA2 (2002-2004)

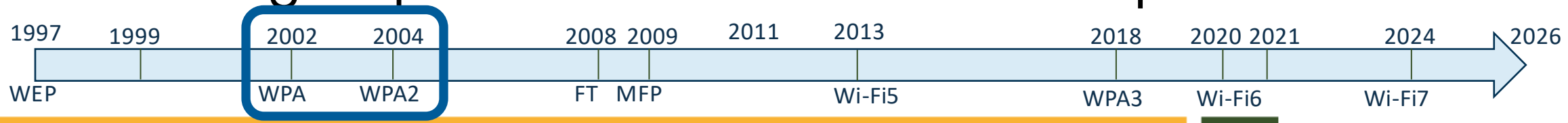
WPA 2002: TKIP, firmware upgrade post-WEP, chiavi globali

WPA2 2004: RSN, nuovo hardware, pairwise keys individuali

WPA/WPA2: compatibiltà opzionale con TKIP

Compatibilità: come funziona?

- Nel Robust Security Network Element viene aggiunto un sottocampo
- In questo caso, una seconda Pairwise Cipher Suite (TKIP)
- Il client sceglie quale usare in Association Request



WPA2 (2004) - *Sicurezza*

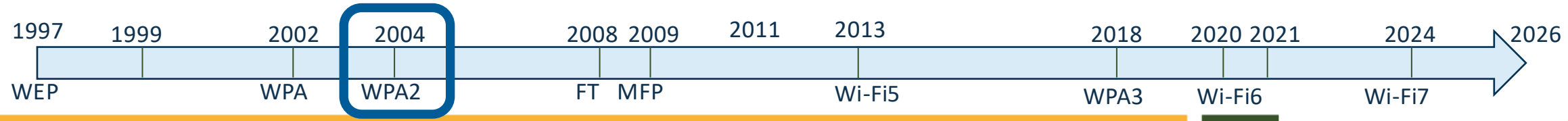
	AKM	PCS	Sicurezza	MITM
WPA2 PSK	PSK (2)	CCMP-128 (4)	Offline Brute Force	MITM, DoS
WPA2 802.1X	802.1X (1)	CCMP-128 (4)	V	MITM, DoS

WPA2 PSK

```
Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 20
  RSN Version: 1
  Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: AES (CCM) (4)
  Pairwise Cipher Suite Count: 1
  Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 1
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: PSK (2)
  RSN Capabilities: 0x0028
```

WPA2 802.1X

```
Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 20
  RSN Version: 1
  Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: AES (CCM) (4)
  Pairwise Cipher Suite Count: 1
  Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 1
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: WPA (1)
  RSN Capabilities: 0x0000
```

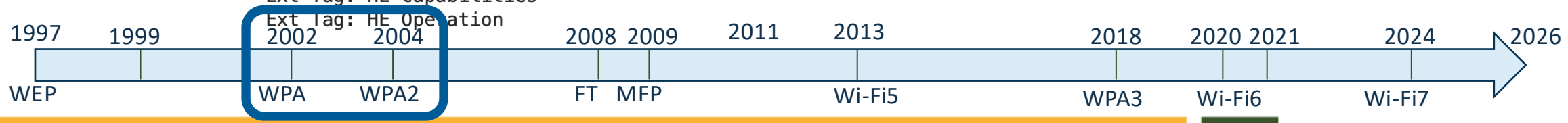


WPA/WPA2 (TKIP) - *Compatibilità*

```
> Tag: Country Information: Country Code IT, Environment Global operating classes
> Tag: Power Constraint: 0
> Tag: TPC Report Transmit Power: 17 dBm
v Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 24
    RSN Version: 1
  v Group Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
      Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Cipher Suite type: TKIP (2)
    Pairwise Cipher Suite Count: 2
  v Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) 00:0f:ac (Ieee 802.11) TKIP
    > Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    > Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
    Auth Key Management (AKM) Suite Count: 1
  v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA
    v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: WPA (1)
    > RSN Capabilities: 0x0000
> Tag: QBSS Load Element 802.11e CCA Version
> Tag: RM Enabled Capabilities (5 octets)
> Tag: HT Capabilities
> Tag: HT Operation
> Tag: Extended Capabilities (10 octets)
> Tag: VHT Capabilities
> Tag: VHT Operation
> Tag: Tx Power Envelope
> Ext Tag: HE Capabilities
> Ext Tag: HE Operation
```

originale

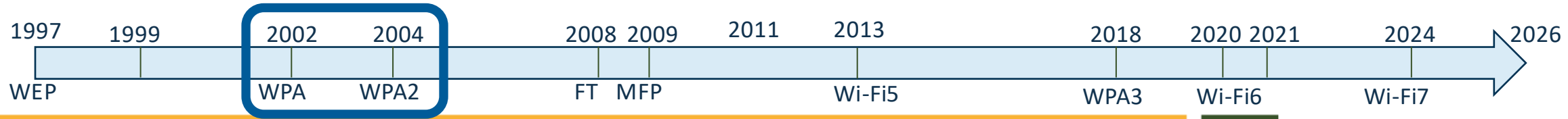
aggiuntivo



WPA/WPA2 (2002-2004)

Compatibilità TKIP:

- Riguarda dispositivi 1997-2004
- Dopo 2007 (iPhone) sempre meno rilevante
- Dal 2009 (Wi-Fi4) penalità: niente datarate elevati
- Dal 2020 (Wi-Fi6) deprecato
- Nel 2026 il 6% delle reti configura ancora TKIP!
  - 1198 reti su di 19154, campione raccolto a Milano il 24/10/2026
  - Configurazioni di default
  - Rarissimi casi reali (industria, trasporti)



We will use TKIP as a temporary solution until…

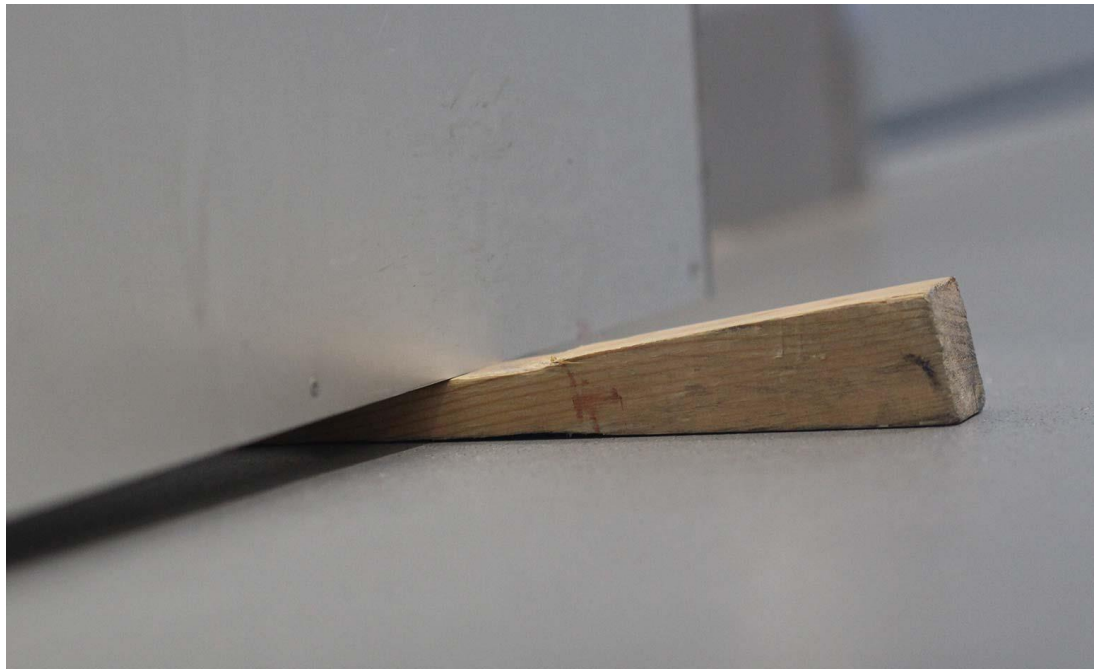
00:1A:DD:D9:6A:41	DaadGuest	Peplink	d/e/i	WPA/WPA2 (PSK)
D8:76:AE:55:5F:50	JKGUESTS	Huawei	d/e/i/k/v	WPA/WPA2 (PSK)
74:1A:E0:E0:B2:D6	Ek_2.4G		e/i	WPA/WPA2 (PSK)
E2:55:A8:B2:56:23	wefy_user	Cisco Meraki	d/e/h/i/k/v	WPA/WPA2 (PSK)
D6:31:27:5C:8B:FC	*Hidden Network*	Ruijie Networks	d/e/h/i/k/v	WPA/WPA2 (PSK)
AC:84:C6:3D:D0:7F	zspw	TP-Link	e/v	WPA (PSK)
B8:50:01:CD:39:F1	*Hidden Network*	Extreme Networks	d/e/h/i/k/v	WPA/WPA2 (PSK)
CC:2D:21:A5:6C:F1	passarella	Tenda	e/i	WPA/WPA2 (PSK)
B4:B0:24:DE:2C:BC	GETPALM	TP-Link	e/i	WPA/WPA2 (PSK)
80:AF:CA:B0:58:06	Cudy-56B6	Cudy	e/i	WPA/WPA2 (PSK)
04:F0:21:1B:6C:5E	SPINTEC2	Compex Systems	d/e/i	WPA/WPA2 (PSK)
88:5A:92:D8:EA:50	DECAS	Cisco Systems	d/e/i	WPA/WPA2 (PSK)
18:D6:C7:86:E3:EE	Flybox_E3EE	TP-Link	e/i	WPA/WPA2 (PSK)
EA:55:B8:93:29:32	Herno Mon...leone Test	Cisco Meraki	d/e/h/i/k/v/w	WPA/WPA2 (PSK)
E2:55:A8:B2:56:80	wefy_user	Cisco Meraki	d/e/h/i/k/v	WPA/WPA2 (PSK)
02:18:5A:58:92:D5	PrPT	Cisco Meraki	d/e/h/i/k/v	WPA/WPA2 (PSK)

D	Length	Information Element	Details
45	26 bytes	HT Capabilities	*20/40 MHz, Short GI for 20 MHz, Short GI for 40 MHz, 2 Spati*
61	22 bytes	HT Operation	*Primary Channel: 36 (Any Width Supported), Secondary Chanr*
74	14 bytes	Overlapping BSS Scan Parameters	
127	8 bytes	Extended Capabilities	*20/40 BSS Coexistence Management Support, Extended Chan*
48	**24 bytes**	**RSNE**	***Group Cipher: TKIP; Pairwise Cipher(s): TKIP, CCMP-128; AKM***
51	5 bytes	AP Channel Report	
51	4 bytes	AP Channel Report	
32	1 bytes	Power Constraint	*0 dB*
35	2 bytes	TPC Report	*Transmit Power: 20 dBm*
70	5 bytes	RM Enabled Capabilities	*Link Measurement, Neighbor Report, Beacon Passive Measure*
173	15 bytes	Symbol Proprietary: Zebra	
221	24 bytes	Vendor Specific: Microsoft	*Wi-Fi Protected Access (WPA): Multicast Cipher: TKIP: Unicast*

Filter dot11.rsn

Networks Found: 19154, **Displayed: 1198, Selected: 1**

1198 reti TKIP (6%) su di 19154, campione raccolto a Milano il 24/10/2026



Avon Fire & Rescue Service warns about dangers of wedging open fire doors
Tuesday 24th September, 2019
Avon Fire & Rescue Service is asking businesses and residents across the local area to pledge to lose the wedge this Fire Door Safety week, taking place between 23rd – 29th September.

https://www.bathecho.co.uk/news/community/avon-fire-rescue-warns-dangers-wedging-fire-doors-86414/

2 – L’innovazione può attendere

Due storie di prestazioni e sicurezza

WORKSHOP GARR 2026

NET MAKERS

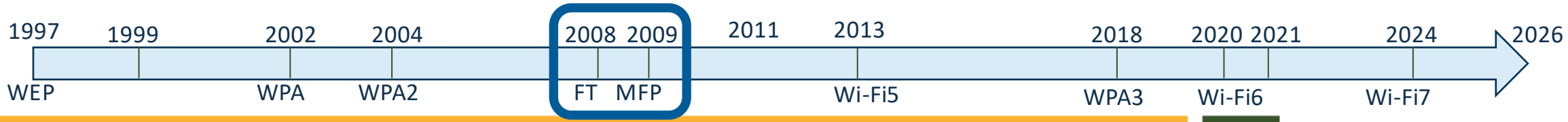
FT, MFP (2008-2009) – *Sicurezza , Compatibilità*

Fast Transition (FT 802.11r)

- fast roaming < 150ms
- Standard per mobilità sicura (RSN)
- WFA certification:
  - Mandatory - Voice Enterprise (2012)
  - Mandatory – Agile Multiband (2017)
- Adozione iniziale lenta

Management Frame Protection (MFP 802.11w)

- Anti-spoofing, DoS, MITM
- WFA certification:
  - Mandatory – (2014 2018 2019 2020)
  - Laptop, tablet, smartphones: 99%+ compatibile
  - IoT, legacy Wi-Fi5: driver difettosi



FT e MFP frame capture - *Sicurezza*

FT

```
Auth Key Management (AKM) Suite Count: 2
   Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA 00:0f:ac (Ieee 8
   Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
      Auth agement (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key gement (AKM) type: WPA (1)
   Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key gement (AKM) type: FT over IEEE 802.1X (3)
```

AKM base

FT

```
Tag: Mobility Domain
   Tag Number: Mobility Domain (54)
   Tag length: 3
   Mobility Domain Identifier: 0xe803
   FT Capabi and Policy: 0x01
      .... ...1 = Fast BSS Transition over DS: 0x1
      .... ..0. = Resource Request Protocol Capability: 0x0
      0000 00.. = Reserved: 0x00
```

FT

MFP required

```
RSN Capabilities: 0x00cc
   .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not
   .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can s
   .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay
   .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay
   .... .... .1.. .... = Management Frame Protection Required: Required
   .... .... 1... .... = Management Frame Protection Capable: Capable
```

MFP optional

```
RSN Capabilities: 0x0080
   .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not su
   .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can supp
   .... .... .... 00.. = RSN PTKSA Replay Counter capabilities: 1 replay co
   .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay co
   .... .... .0.. .... = Management Frame Protection Required: Not required
   .... .... 1... .... = Management Frame Protection Capable: Capable
```

	AKM	PCS	Sicurezza	MFP Optional	MFP Required
WPA2 PSK	PSK (2), FT-PSK (4)	CCMP-128 (4)	Brute Force	MITM, DoS	V
WPA2 802.1X	802.1X (1), FT 802.1X (3)	CCMP-128 (4)	V	MITM, DoS	V



Quando possono scegliere, talvolta i client sbagliano

Fast Transition affianca sempre una AKM di base.

Il client che non supporta FT, può legalmente escludere FT nella Association Request

Eppure capita che il client tenti di associarsi con:

- Non-FT AKM e
- Mobility Domain ID

```
Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 26
  RSN Version: 1
> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 1
v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA (SHA256)
  v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA256)
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
    v Auth Key Management (AKM) type: WPA (SHA256) (5)
      > [Expert Info (Error/Protocol): Non-FT AKM suite is prohibited for FT association request]
> RSN Capabilities: 0x00bc
  PMKID Count: 0
  PMKID List
> Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
v Tag: Mobility Domain
  Tag Number: Mobility Domain (54)
  Tag length: 3
  Mobility Domain Identifier: 0x4d3b
```



Ancora Client che sbagliano (quasi sempre)

Association Request a rete WPA3 Transition

Source	Type/Subtype	Management Frame Protection	Management Frame Protectior
86:b4:d0:9d:a8:18	Association Request	Required	Capable
e2:43:4f:50:dd:db	Association Request	Not required	Capable
a6:9d:94:4e:b4:f0	Association Request	Not required	Capable
ee:be:57:42:14:3c	Association Request	Not required	Capable
da:5c:52:92:49:05	Association Request	Not required	Capable
aa:4e:78:c0:f2:be	Association Request	Not required	Capable
e2:ee:99:9f:d9:5a	Association Request	Not required	Capable
62:0a:99:68:23:f9	Association Request	Not required	Capable
Apple_74:4f:da	Association Request	Not required	Capable
ae:57:fd:19:38:aa	Association Request	Not required	Capable
d2:52:32:fa:7e:bd	Association Request	Not required	Capable
aa:4e:78:c0:f2:be	Association Request	Not required	Capable
e2:07:3b:bd:4e:87	Association Request	Not required	Capable
e2:07:3b:bd:4e:87	Association Request	Not required	Capable



Management Frame Protection:

- Il client sceglie la via più semplice

MFP optional:

- Capable, Not Required



3 - WPA3, finalmente

Sicurezza, privacy e affidabilità - dopo 14 anni

WPA3 Personal (2018) - *Compatibilità*

Enorme sicurezza vs. WPA2

- PTK non derivabile dalla passphrase

AKM8, MFP Required

2 modalità di transizione

- Transition
- Compatibility (2024)

Strategie SSID di migrazione

- (In-place + fallback)
- Origine > Destinazione

```
Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 20
    RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
    v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: SAE (SHA256) (8)
  v RSN Capabilities: 0x00cc
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can s
      .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 repla
      .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay
      .... .... .1.. .... = Management Frame Protection Required: Required
      .... .... 1... .... = Management Frame Protection Capable: Capable
```



WPA3 Enterprise (2018) - *Compatibilità*

AKM 5

MFP Required

Modalità di transizione

- Facilmente supportata

Strategie SSID di migrazione

- In-place + fallback
- (Origine > Destinazione)

```
Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
  Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: AES (CCM) (4)
  Pairwise Cipher Suite Count: 1
  Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: AES (CCM) (4)
  Auth Key Management (AKM) Suite Count: 2
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 8
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: FT over IEEE 802.1X (3)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA256)
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: WPA (SHA256) (5)
  RSN Capabilities: 0x00cd
    .... .... .... ...1 = RSN Pre-Auth capabilities: Transmitter supports
    .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can su
    .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay
    .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay
    .... .... .1.. .... = Management Frame Protection Required: Required
    .... .... 1... .... = Management Frame Protection Capable: Capable
```



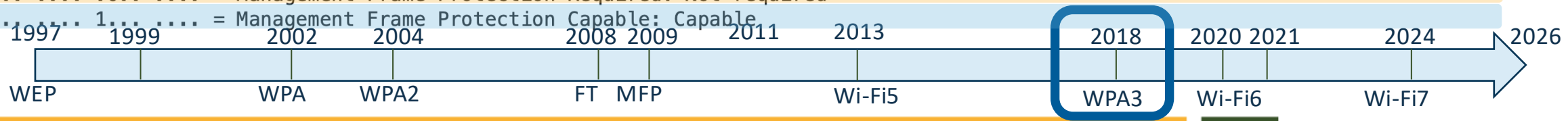
WPA3 Enterprise Transition - *Compatibilità*

```
Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 34
  RSN Version: 1
> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 3
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X 00:0f:ac (Ieee 802.11) WPA (SHA256)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: WPA (1)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: FT over IEEE 802.1X (3)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA256)
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: WPA (SHA256) (5)
  RSN Capabilities: 0x008c
    .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
    .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
    .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
    .... .... .0.. .... = Management Frame Protection Required: Not required
    .... .... 1... .... = Management Frame Protection Capable: Capable
```

compatibilità

base

compatibilità



Enhanced Open - OWE(2018) - *Sicurezza*

AKM 18

Semplice da implementare

MFP Required

Modalità di transizione

- Facilmente supportata

Strategie SSID di migrazione

- In-place con transizione

```
Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 20
  RSN Version: 1
  Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: AES (CCM) (4)
  Pairwise Cipher Suite Count: 1
  Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: AES (CCM) (4)
  Auth Key Management (AKM) Suite Count: 1
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wirele
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) Opportunistic Wi
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: Opportunistic Wireless Encryption (18)
  RSN Capabilities: 0x00cc
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not su
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can supp
      .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay c
      .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay cou
      .... .... .1.. .... = Management Frame Protection Required: Required
      .... .... 1... .... = Management Frame Protection Capable: Capable
```



WPA3 (2018) – *Sicurezza*

* Tabella semplificata, si omettono AKM 12,13,22-25

WPA3	AKM*	PCS	Sicurezza	MFP Optional	MFP Required
WPA3 Personal	SAE (8), FT SAE (9)	GCMP-256 (9)	V	-	V
WPA3 Enterprise	802.1X SHA-256 (5), FT 802.1X (3)	CCMP-128 (4)	V	-	V
Enhanced Open (OWE)	OWE (18)	CCMP-128 (4)	V	-	V
WPA3 Transition					
WPA3 Personal Transition	PSK (2), SAE (8)	CCMP-128 (4), GCMP-256 (9)	X/V	X	V
WPA3 Personal Compatibility (RSN Override)	PSK (2), SAE (8)	CCMP-128 (4), GCMP-256 (9)	X/V	X	V
WPA3 Enterprise Transition	802.1X (1), 802.1X (5)		X/V	X	V
OWE Transition (dual SSID)	-/OWE (18)	-/CCMP-128 (4)	X/V	X	V



Wi-Fi6E (6GHz)

La banda 6GHz è essenziale per:

- Alta densità e alta capacità
- Nuovi casi d'uso: didattica integrata, collaborazione, esami Wi-Fi

WPA3 Mandatory in 6GHz spinge l'adozione di WPA3

- 6GHz = nuovo hardware = nuovi client
- WPA3 Transition è un mezzo per aggiungere subito 6GHz alle nostre reti



4 - Wi-Fi7 e oltre

WPA3, 2.4/5/6GHz, Multi-Link Operation

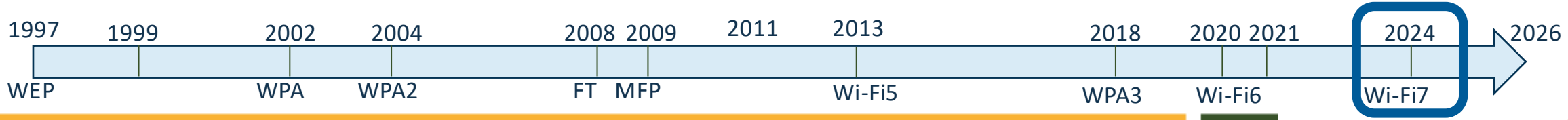
Wi-Fi7 802.11be (2024)

Introduce Multi-Link Operation (MLO)

- Uso di più bande contemporanee
- Seamless intra-AP roaming
- Multi-AP Coordination
- Base per Seamless Mobility Domain (Wi-Fi8)

E inoltre efficienza spettrale e prestazioni:

- 320MHz channels
- 4096 QAM
- Multi-RU
- Preamble Puncturing



Wi-Fi7 (2024) - *Compatibilità*

Un AP Wi-Fi7 2.4/5/6 GHz

- Deve usare WPA3
- WPA3 Transition è possibile, ma con penalità

The AP's BSS Configuration shall not allow any PSK AKM or 802.1X SHA-1 AKM to be used in an association that negotiates use of EHT or MLO (WPA3 Specification v3.5)



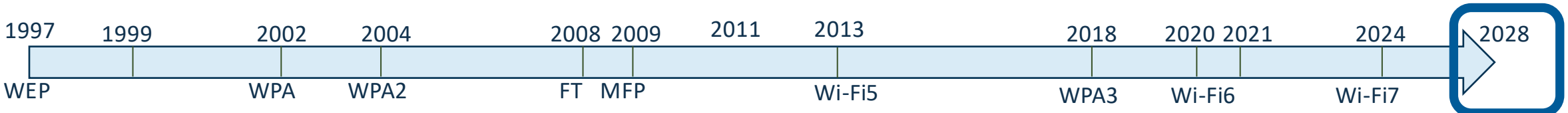
Wi-Fi8 802.11bn (2028?)

Stato:

- Working Group Draft 2.0 (completato, 2026)
- WG Draft 3.0 (2027?)
- Sponsor Ballot (2027?)
- Wi-Fi Certified 7 (2027)
- Approvazione finale e ratifica (2028?)

L'elemento più interessante:

- Multi-AP Coordination e Seamless Mobility, basati su MLO



Conclusioni

Servono obiettivi, strategie, e packet capture

Conosci i tuoi dispositivi client

Analizza i tuoi beacon con Iswifi:

- `lswifi -export my.pcapng` (https://github.com/joshschmelzle/lswifi)

Cattura trame Wi-Fi L2

- Airodump-ng (Linux)
- Hamina, Ekahau, Sidos, Metageek (proprietari)
- Sull'AP (dipende dall'infrastruttura)

Analizza le Association Request con Wireshark:

- `wlan.fc.type_subtype == 2  || wlan.fc.type_subtype == 0`

(Il wireless controller mente)

WPA3 Transition

Sono necessari:

- Obiettivi
- Tempi
- Strategia
  - Gestione delle eccezioni
  - Segmentazione SSID
  - Livelli minimi

Altrimenti è

- Debito Tecnologico



Söderskär, Finland, Miika Silfverberg CC by-sa 2.0 https://www.flickr.com/photos/miikas/87803093



Grazie.
Domande?

www.partici.fi codice 83995288

Contatti: jan.reister@unimi.it

WORKSHOP GARR 2026

NET MAKERS