

Università di Napoli Federico II – Scuola Politecnica e delle Scienze di Base
Corso di Laurea in Ingegneria Informatica



Corso di Protocolli per Reti Mobili

**Lo standard IEEE 802.11:
Sicurezza**



- L'utilizzo del mezzo wireless consente a chiunque (in un determinato raggio) di ascoltare i dati trasmessi
- L'individuazione dei soggetti appartenenti "lecitamente" alla rete wireless avviene mediante una procedura di **autenticazione**
- Occorre inoltre garantire:
 - La **confidenzialità** dei dati (soggetti non autorizzati non devono poter avere accesso ai dati)
 - L'**integrità** dei dati (i dati inviati non devono poter arrivare modificati al destinatario – a causa di errori del canale o di attacchi)

- Il meccanismo di sicurezza definito nella prima versione dello standard IEEE 802.11 è WEP (Wired Equivalent Privacy)
 - Fornisce confidenzialità ed integrità dei dati
- Dopo che sono state dimostrate diverse falle nella sicurezza offerta da WEP, lo standard 802.11-2007 ha deprecato l'uso di WEP
- WEP è basato su RC4
 - Algoritmo di crittografia (*stream cipher*) a chiave simmetrica
 - Non è open, ma proprietà intellettuale di RSA Security, Inc.

Symmetric stream cipher

- A partire da una chiave (key), uno stream cipher determina una *keystream* usata per ottenere la sequenza cifrata mediante una XOR con la sequenza originale
- Il ricevitore, conoscendo la key, determina la keystream e la sequenza originale mediante una operazione XOR

dati	keystream	seq. cifrata	keystream	dati
0	1	1	1	0
1	1	0	1	1
0	1	1	1	0
1	0	1	0	1
1	0	1	0	1
0	1	1	1	0
0	0	0	0	0
0	1	1	1	0
1	0	1	0	1

Symmetric stream cipher

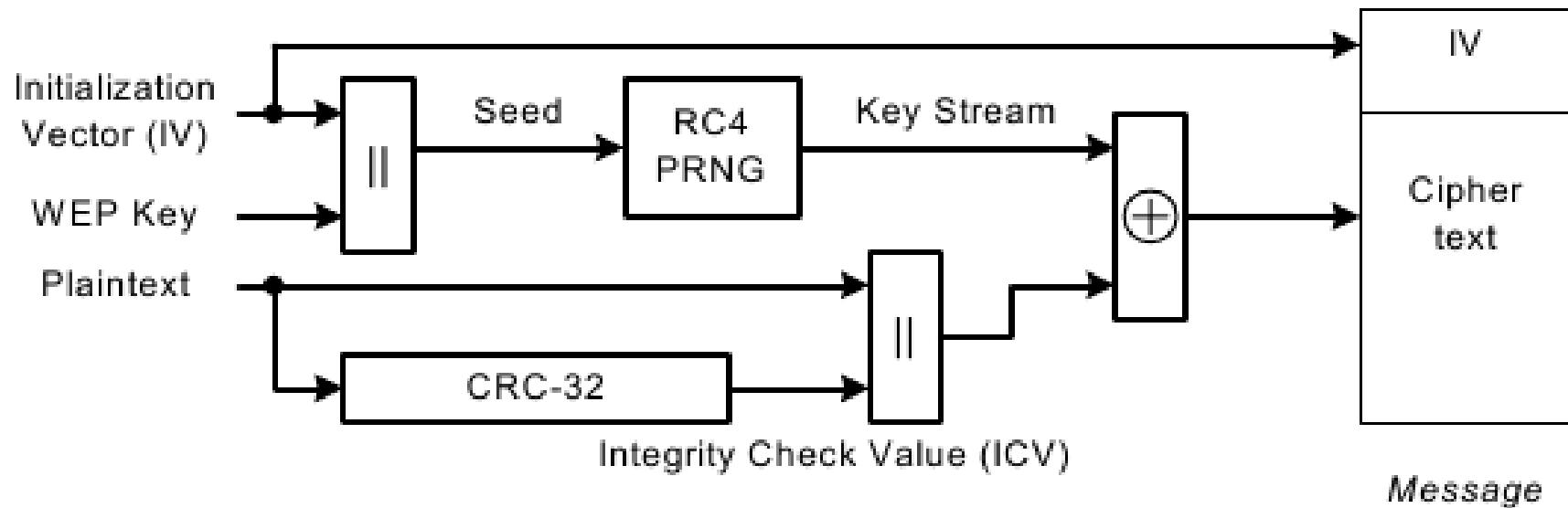
- Quanto è difficile per un attaccante decifrare la sequenza cifrata?
- **Ruovo chiave svolto dalla keystream**
- L'unico schema di crittografia che è stato matematicamente provato di essere in grado di proteggere contro certi tipi di attacchi è una keystream *totalmente* casuale
- Difficoltà di realizzazione pratica inducono ad usare generatori di numeri pseudo-casuali (PRNG) per espandere la key in una keystream
- **I valori pseudo-casuali si ripetono con periodicità**
- La sicurezza di uno stream cipher dipende dalla aleatorietà della keystream generata dal PRNG

- L'integrità dei dati è verificata aggiungendo un ICV (Integrity Check Value), calcolato usando CRC-32 sul campo *dati* della MPDU
- La keystream usata per cifrare dati + ICV è calcolata usando il PRNG di RC4 su un seme formato dalla chiave WEP (40 o 104 bit) + IV (Initialization Vector, 24 bit)
 - Un nuovo IV per ogni MPDU (per evitare il riuso della stessa keystream)
 - L'algoritmo per determinare l'IV non è specificato
 - L'IV deve essere comunicato al ricevente

Wired Equivalent Privacy (WEP)



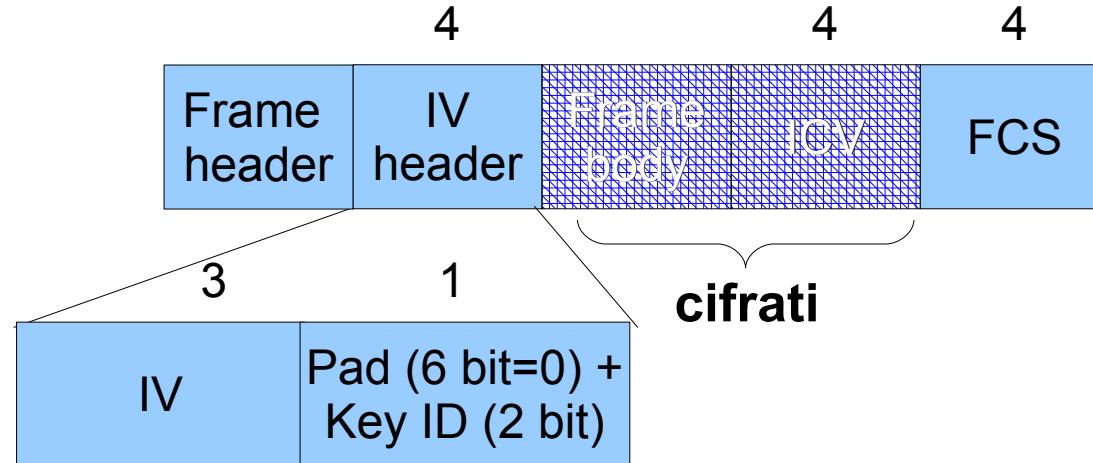
- Incapsulamento



Wired Equivalent Privacy (WEP)



DIE
TI.
UNI
NA

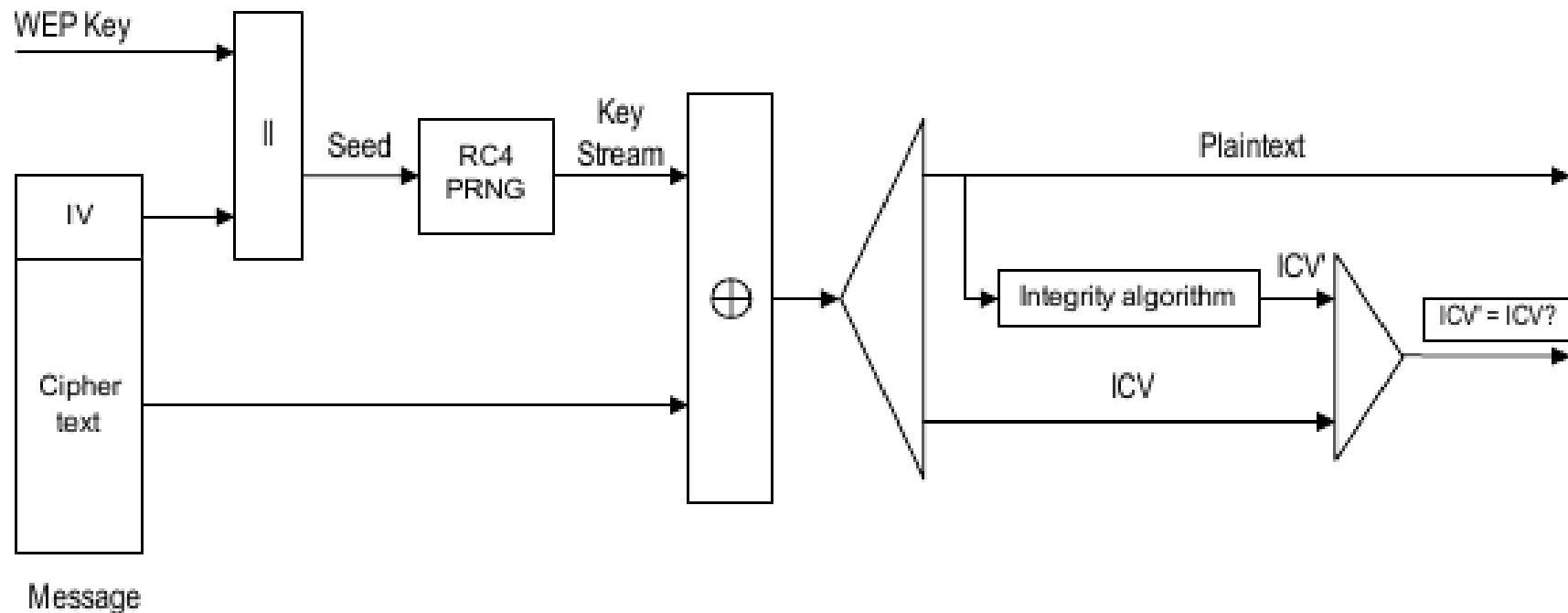


- Due tipi di chiavi
 - Key-mapping key
 - Specifica per una coppia <TA,RA>
 - Se definita, va usata (Key ID = 0)
 - Default keys
 - Memorizzate nella MIB di ogni stazione
 - Max 4, l'indice (0..3) di quella usata va in Key ID

Wired Equivalent Privacy (WEP)



- De-incapsulamento



Problemi con WEP



DIE
TI.
UNI
NA

- La gestione manuale della chiave WEP è una miniera di problemi
 - Se non cambiata di frequente, diventa di dominio pubblico!
 - Implementazioni non accurate
 - Un vendor di AP esponeva le chiavi WEP di default attraverso SNMP!
 - Valori di IV non generati casualmente
 - CRC non è crittograficamente sicuro
 - Chi è in possesso della chiave WEP, può decifrare e alterare le frame inviate da tutte le altre stazioni!

Problemi con WEP



- ICV protegge solo il payload ma non l'header di una frame
 - Redirezione di frame (modificando DA o RA)
 - Impersonation attack (modificando SA o TA)
- Nessuna protezione contro i replay attack
 - un attaccante può ascoltare la frame (cifrata) di un utente valido (es. ARP request) e ritrasmetterla più volte
 - l'attaccante ascolterà tutte le risposte dell'AP, cifrate con IV diversi
 - più risposte riceve, più è facile decifrare la chiave WEP

- Nel 2001, Fluhrer, Mantin e Shamir hanno pubblicato un lavoro (“Weaknesses in the Key Scheduling Algorithm of RC4”) che descrive teoricamente un modo per attaccare WEP per ricavare la chiave
- Questo lavoro è stato seguito da una serie di dimostrazioni “pratiche” che ne implementano l’idea
 - [AirSnort](#), [WEPCrack](#), [Aircrack-ng](#), ...

Autenticazione

- In un ESS, una STA e l'AP devono completare la fase di autenticazione prima di effettuare l'associazione
- L'autenticazione è opzionale in un IBSS
- Le frame di autenticazione sono unicast
- Due tipi di autenticazione:
 - Open System
 - Non c'è algoritmo di autenticazione
 - Tipicamente l'AP ha una lista di MAC address
 - Bastano 2 messaggi (richiesta e risposta)
 - Shared Key

Shared Key Authentication



- Mira a determinare se una stazione conosce la chiave WEP condivisa
 - Usata solo in combinazione con cifratura WEP
 - Deprecata in IEEE 802.11-2007
- Consiste nello scambio di 4 frame:
 - STA → AP: richiesta di autenticazione Shared Key
 - AP → STA: invio di un testo di “prova” (128 byte generati dal WEP PRNG)
 - STA → AP: frame encapsulata usando WEP e la chiave condivisa, contenente il testo di prova
 - AP → STA: conferma il successo dell'autenticazione se, dopo aver deincapsulato la terza frame, ICV è corretto e il testo coincide con quello di prova

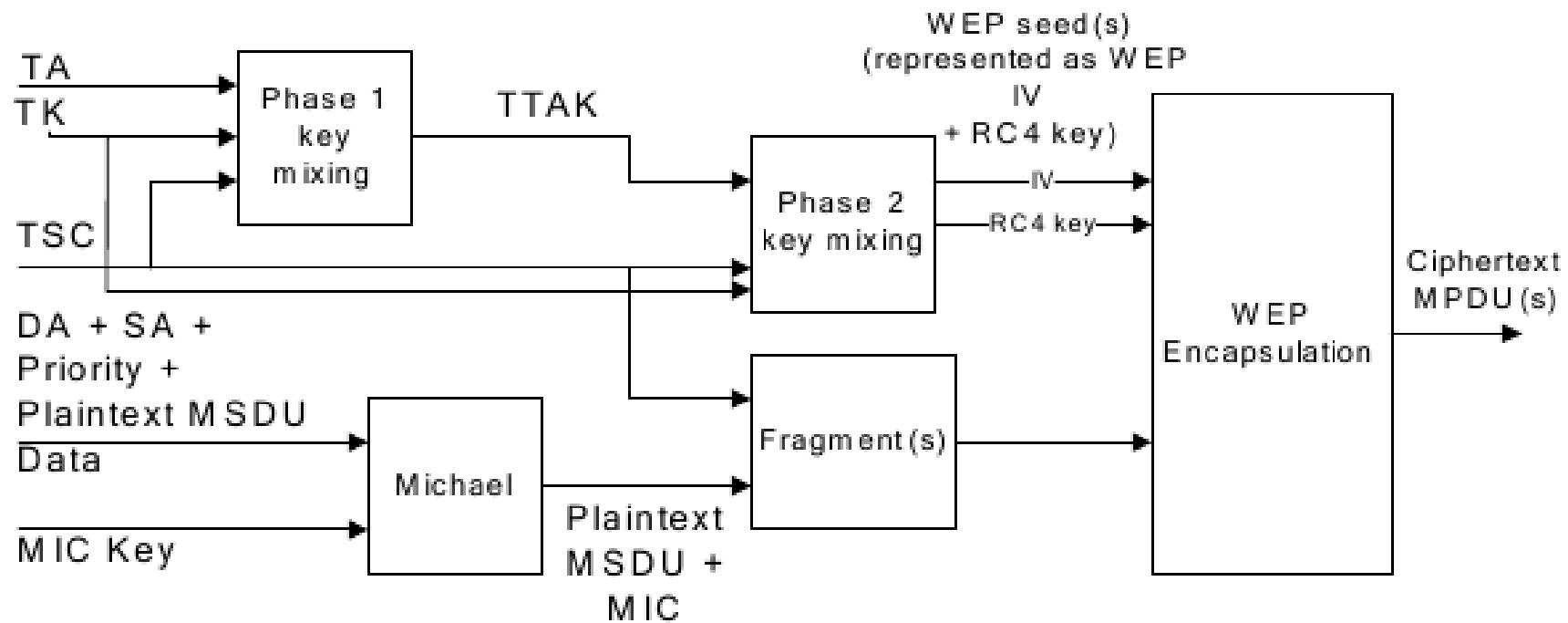
- Nel 2004, lo standard IEEE 802.11i ha introdotto due nuovi algoritmi per la confidenzialità e l'integrità dei dati:
 - CCMP (Counter mode with Cipher-block chaining MAC Protocol)
 - Obbligatorio
 - TKIP (Temporal Key Integrity Protocol)
 - Opzionale
 - Meno robusto di CCMP
 - Ideato per essere installato su hardware che supporta solo WEP tramite un upgrade del firmware

- Calcola un *message integrity code* (MIC) per proteggere l'integrità di
 - Destination Address (DA)
 - Source Address (SA)
 - Priority
 - L'intero payload della **MSDU**
- Per la codifica vengono usate chiavi diverse a seconda della direzione
- La funzione di codifica (“Michael”) è dettagliata nello standard
- Il MIC (64 bit) viene appeso alla MSDU prima della eventuale frammentazione in MPDU

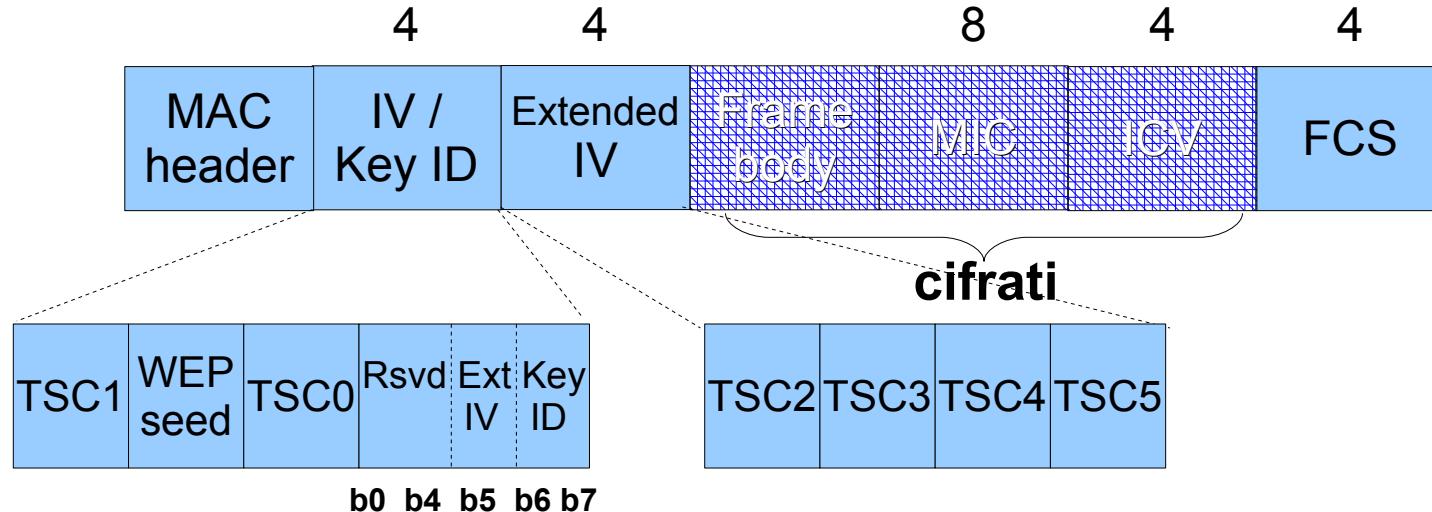
- A differenza di WEP, anche alcuni campi dell'header della frame vengono protetti
- Un controllo sul MIC fallito può indicare che sono stati alterati i campi dell'header protetti
- Se in 60 secondi si verificano due controlli MIC falliti la stazione scarta tutte le frame ricevute per 60s
- Gli MPDU vengono poi incapsulati usando WEP

- Come protezione contro i replay attack, ogni MPDU contiene un numero di sequenza (TSC – *TKIP sequence counter*) di 48 bit
- Una stazione scarta gli MPDU ricevuti fuori ordine
- Il TSC, insieme al Transmitter Address (TA) e ad una *temporal key* (TK) di 128 bit, viene usato per generare la chiave WEP (128 bit) usata per cifrare l'MPDU
 - La chiave WEP non è unica ma varia dinamicamente
 - Tutti gli MPDU di una MSDU devono essere cifrati usando la stessa temporal key
- Come si settano TK e MIC keys?
- Io vedremo più avanti...

- Incapsulamento

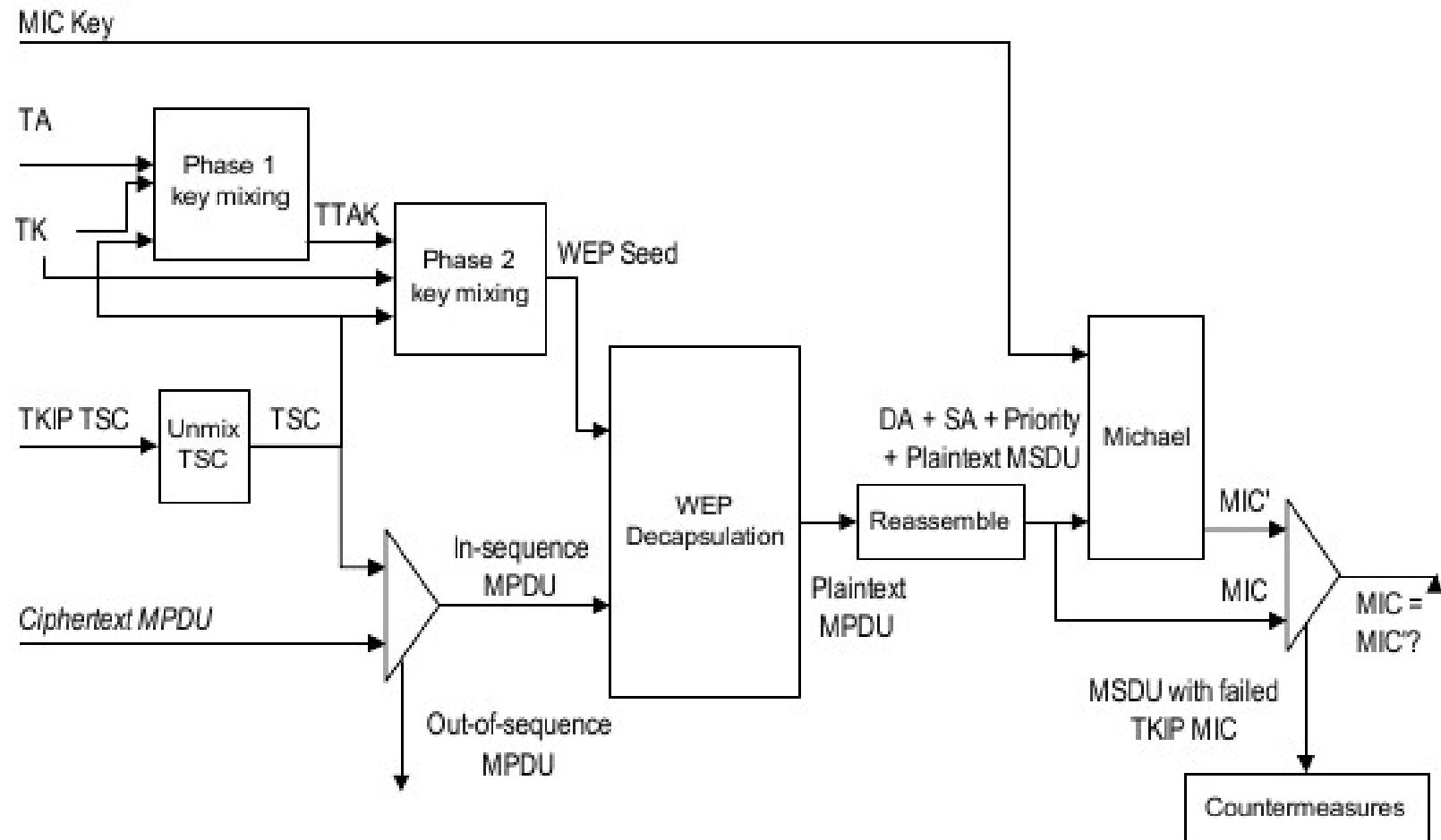


TKIP



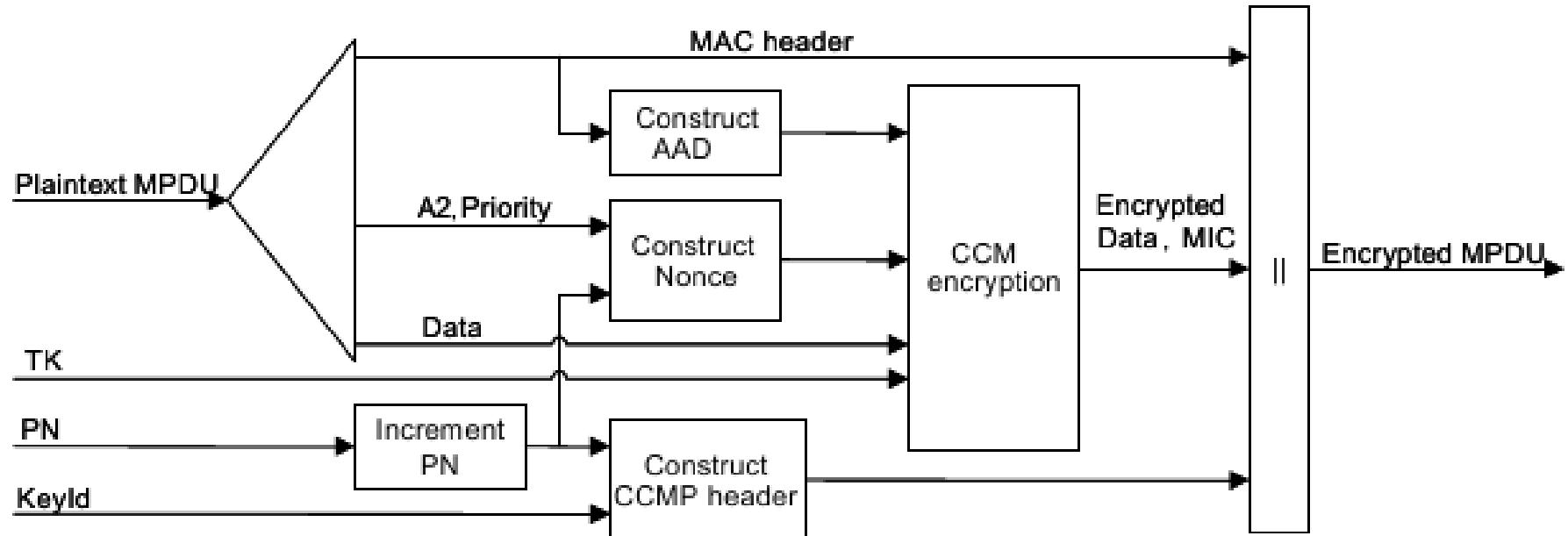
- TKIP riusa il formato degli MPDU WEP aggiungendo un campo *extended IV* per trasportare (in chiaro) il TSC
- Ext IV = 1 → presenza del campo extended IV (MPDU TKIP)
- TSC5 è il MSB di TSC
- TSC1+WEPSseed+TSC0 sono i primi 3 byte della stringa restituita dalle funzioni di key mixing

- De-incapsulamento

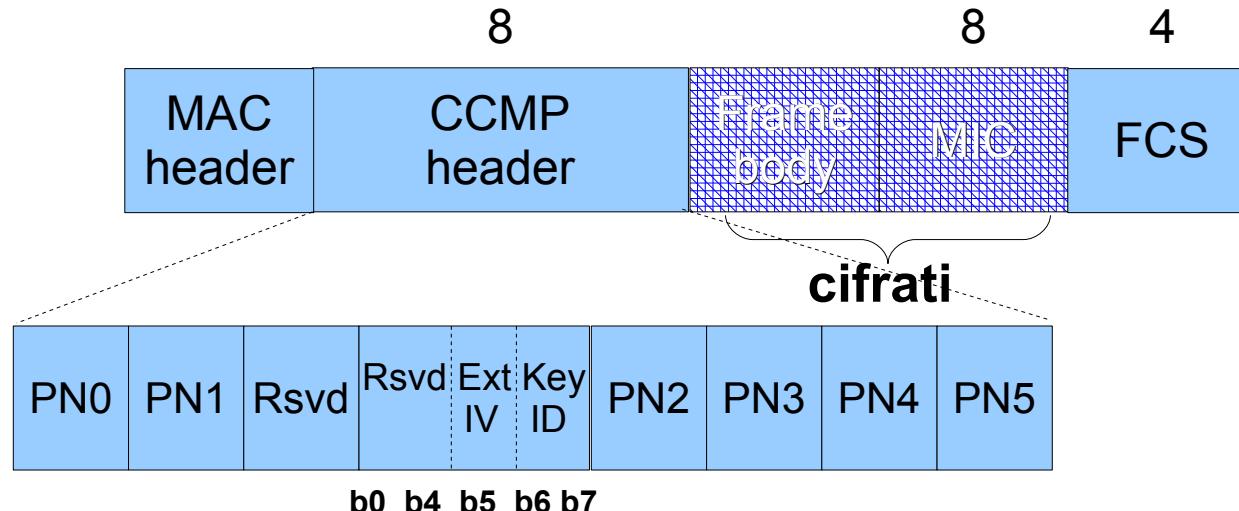


- CCMP è basato su CCM (Counter with CBC-MAC), un *generic authenticated encryption block cipher mode*
- Definito in IETF (Internet Engineering Task Force) RFC (Request For Comment) 3610
- CCM è definito per essere usato con *block cipher* a 128 bit, come AES (Advanced Encryption Standard)
- Definito in NIST (National Institute of Standards and Technology) FIPS PUB (Federal Information Processing Standards Publication) 197-2001

- Offre autenticità e integrità del frame body e di (parte dell') header
- Offre confidenzialità del frame body
- Offre protezione contro i replay attack
 - Usa un packet number (PN) di 48 bit
 - Usa un temporal key (TK) per sessione
 - No due PN uguali all'interno di una sessione
- Non è hardware-compatibile con WEP
 - Usa un metodo di cifratura (AES) più robusto di quello usato da WEP (RC4)
- A differenza di TKIP, opera sui singoli MPDU

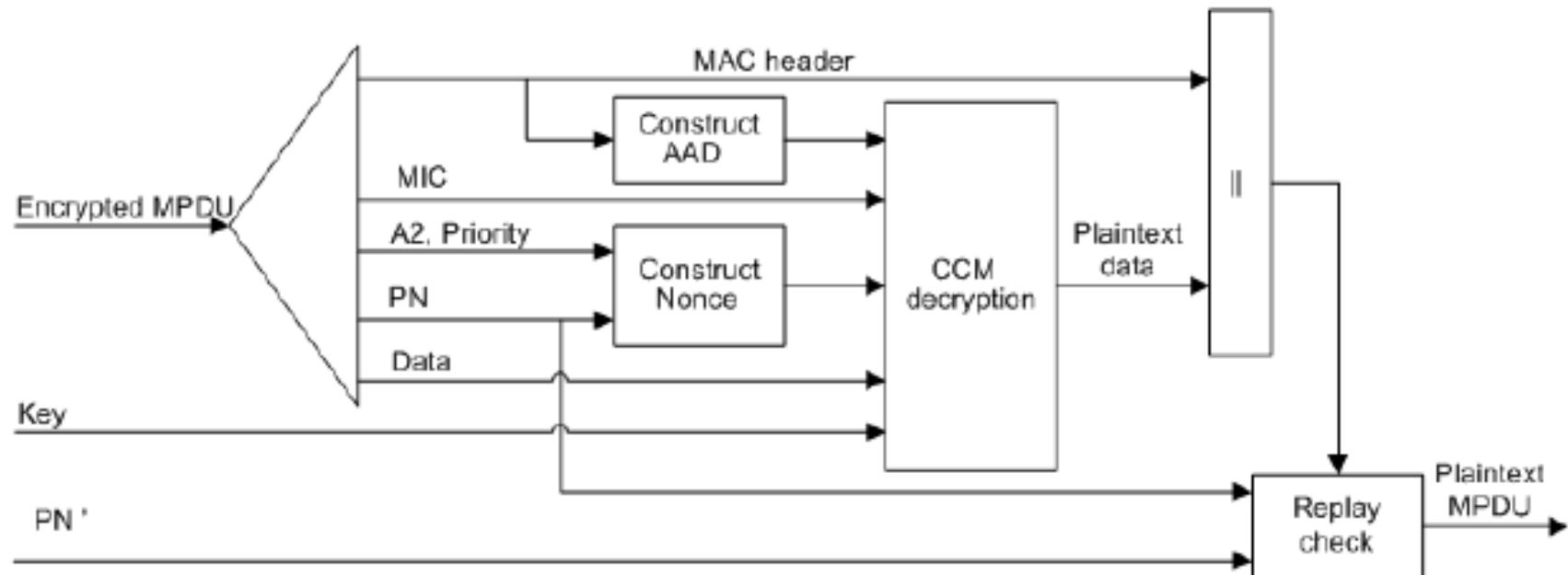


- AAD (Additional Authentication Data) è l'header privato dei campi che possono cambiare a seguito di ritrasmissione (es. Duration)
- Nonce è dato da priority (4 bit) + reserved (4 bit) + Address 2 (A2, 6 byte) + PN (6 byte)
- CCMP header (vedi formato MPDU)
- Oltre a cifrare i dati, CCM fornisce un MIC (cifrato)



- Il PN è inviato in chiaro
- Con cifratura CCMP, non c'è l'ICV WEP
- L'Ext IV bit è sempre settato ad 1 con CCMP

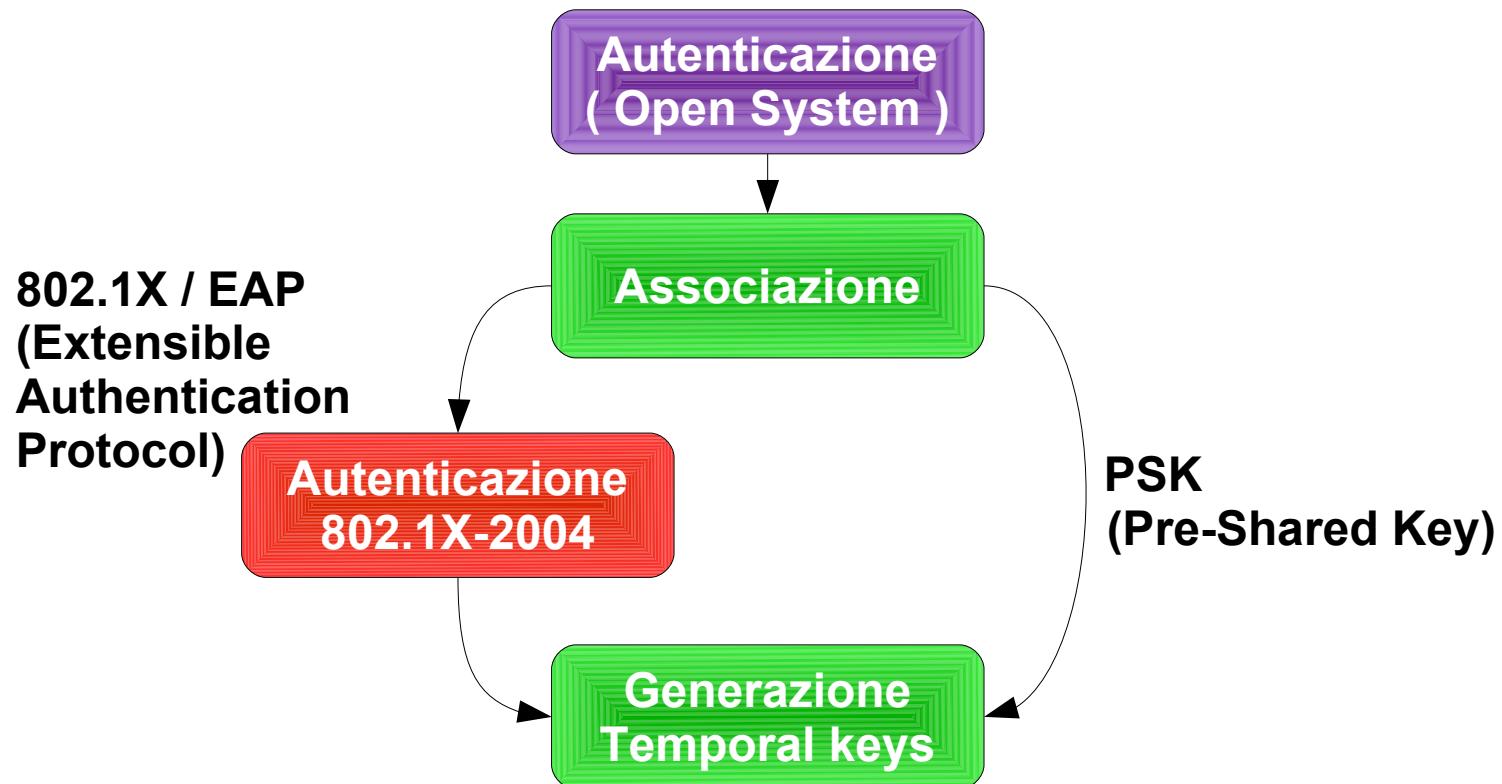
- De-incapsulamento



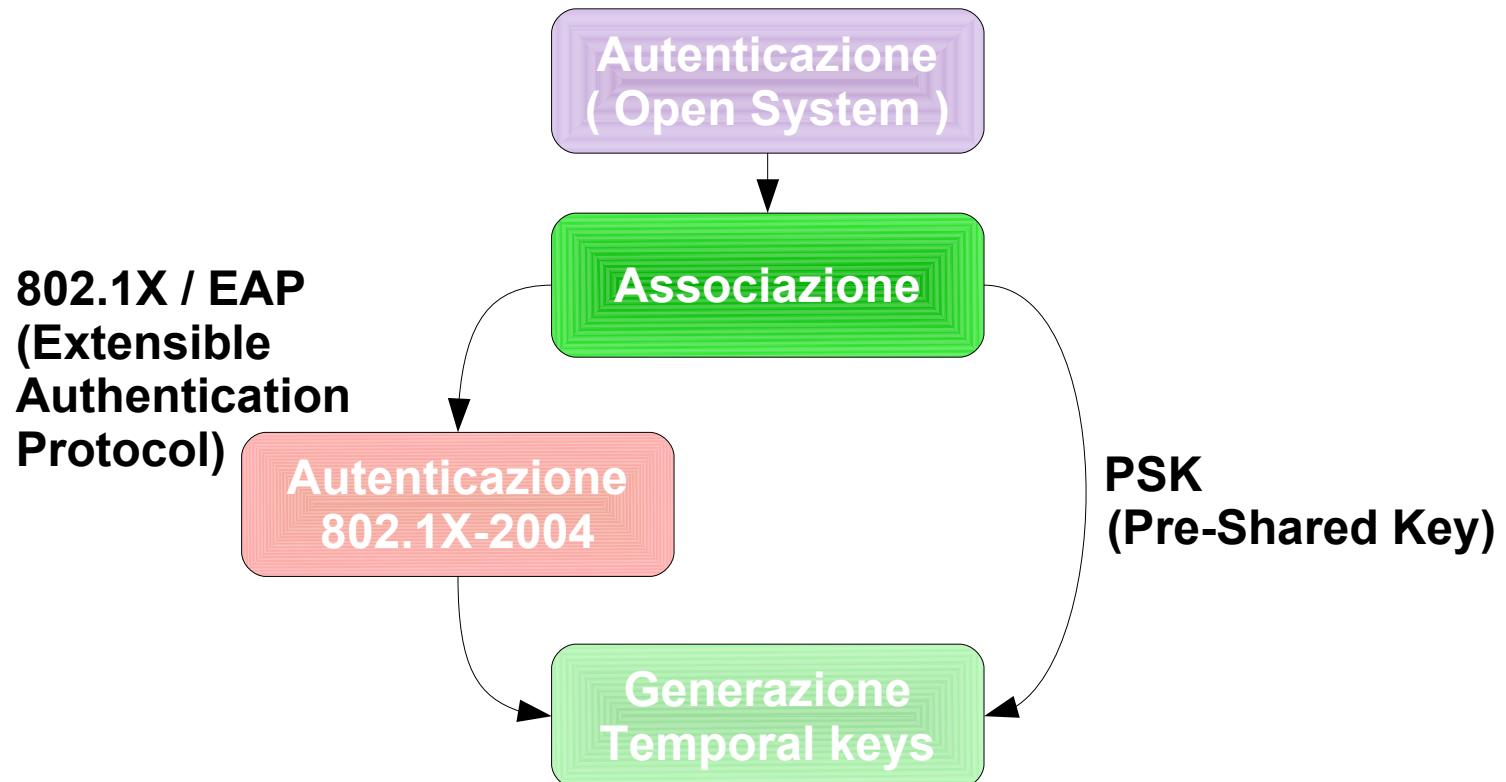
Autenticazione



- TKIP e CCMP sono metodi di cifratura che forniscono integrità e confidenzialità dei dati
- Come avviene l'autenticazione delle stazioni?

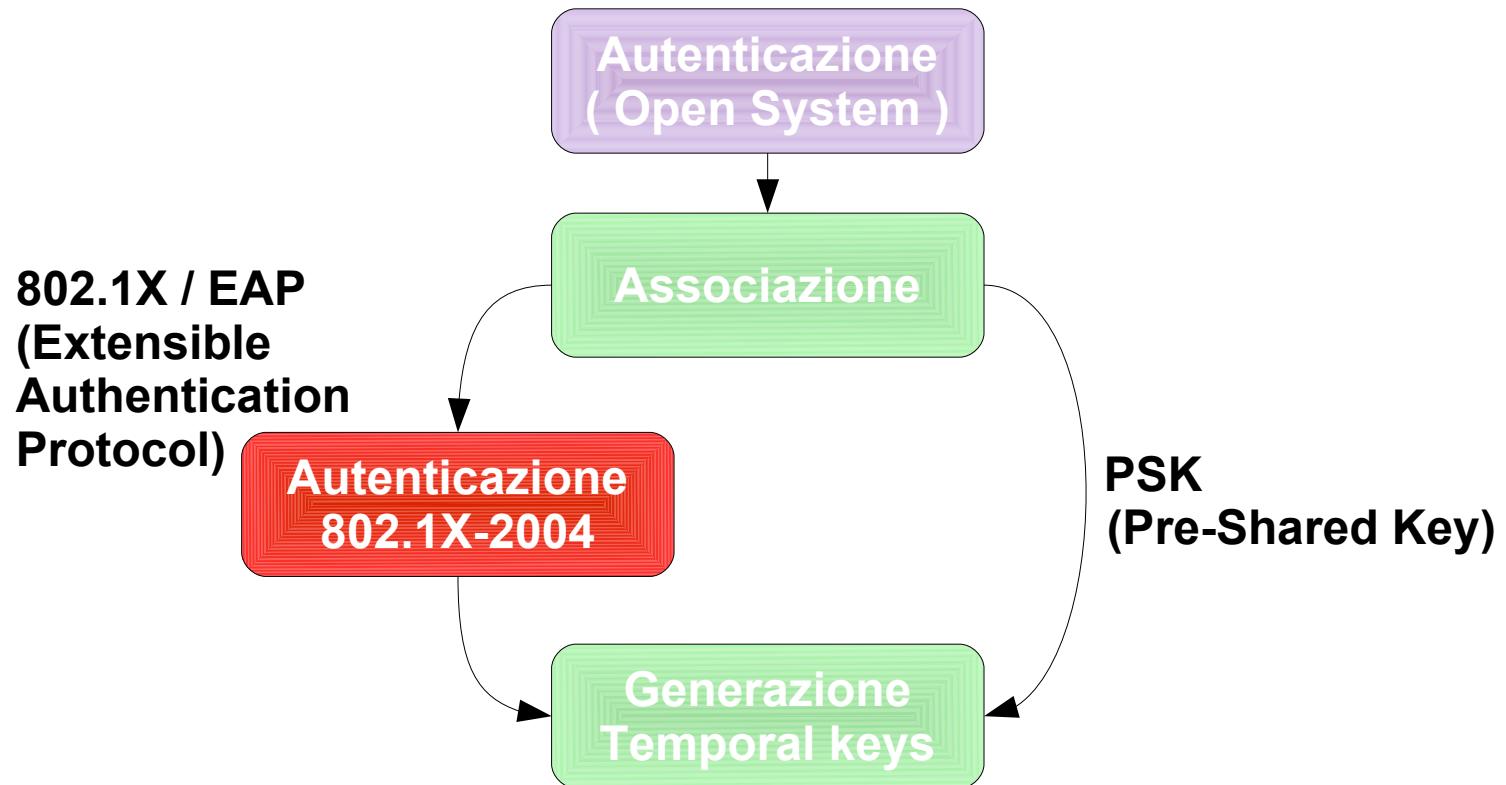


Autenticazione



- Nelle frame Beacon e Probe Response, l'AP specifica tutti i metodi di cifratura e di autenticazione che supporta
- Dopo l'autenticazione Open System, la STA include nel messaggio di richiesta di associazione il metodo di cifratura e quello di autenticazione selezionati
- L'AP rifiuta l'associazione se i metodi selezionati dalla STA non sono tra quelli supportati
- Nella fase di associazione vengono dunque negoziati i parametri di sicurezza

Autenticazione



Autenticazione 802.1X



- Se la STA ha selezionato il metodo di autenticazione 802.1X, inizia la procedura di autenticazione definita dallo standard 802.1X-2010
- Lo standard 802.1X prevede 3 componenti:



- **Suplicant:** l'utente che cerca accesso alla rete
- **Authenticator:** controlla l'accesso alla rete
- **Authentication server:** gestisce le richieste di autenticazione

Autenticazione 802.1X

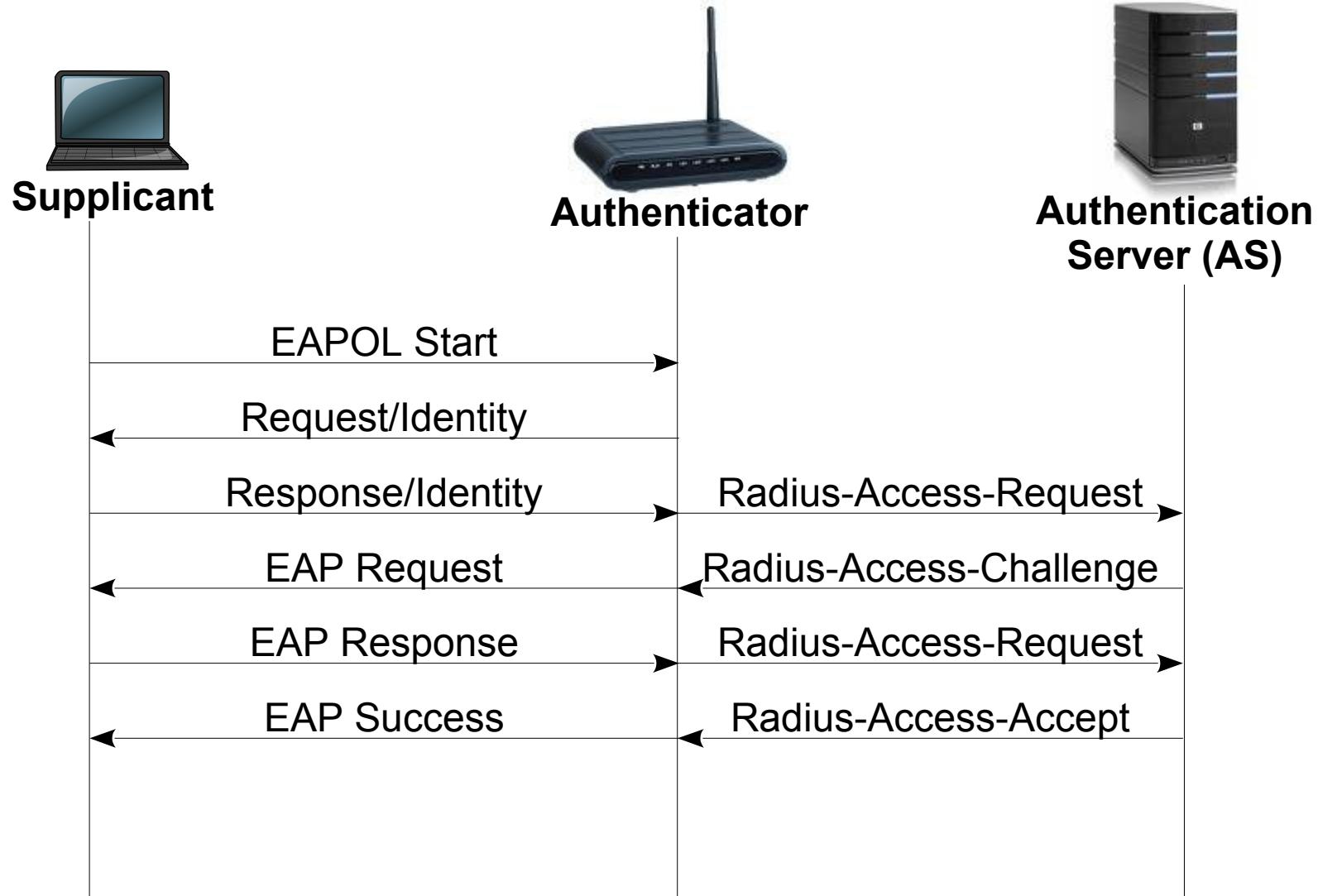
- Lo scambio di messaggi di autenticazione è logicamente condotto tra supplicant e AS
- L'authenticator svolge la sola funzione di bridge
- La comunicazione tra authenticator ed AS è gestita dal protocollo RADIUS
 - Definito in IETF RFC 2865
 - Le credenziali possono essere memorizzate in sorgenti esterne come SQL, LDAP, Active Directory
- La comunicazione tra supplicant ed authenticator è gestita dal protocollo EAPOL (EAP Over LAN)

Autenticazione 802.1X



- EAP è un “framework” di autenticazione che supporta diversi metodi di autenticazione
 - MD-5 challenge
 - One-Time Password
 - Generic Token Card
 - TLS
 - MSCHAPv2
- È basato sullo scambio di messaggi di richiesta e risposta
- È definito in IETF RFC 3748

Autenticazione 802.1X



Autenticazione 802.1X



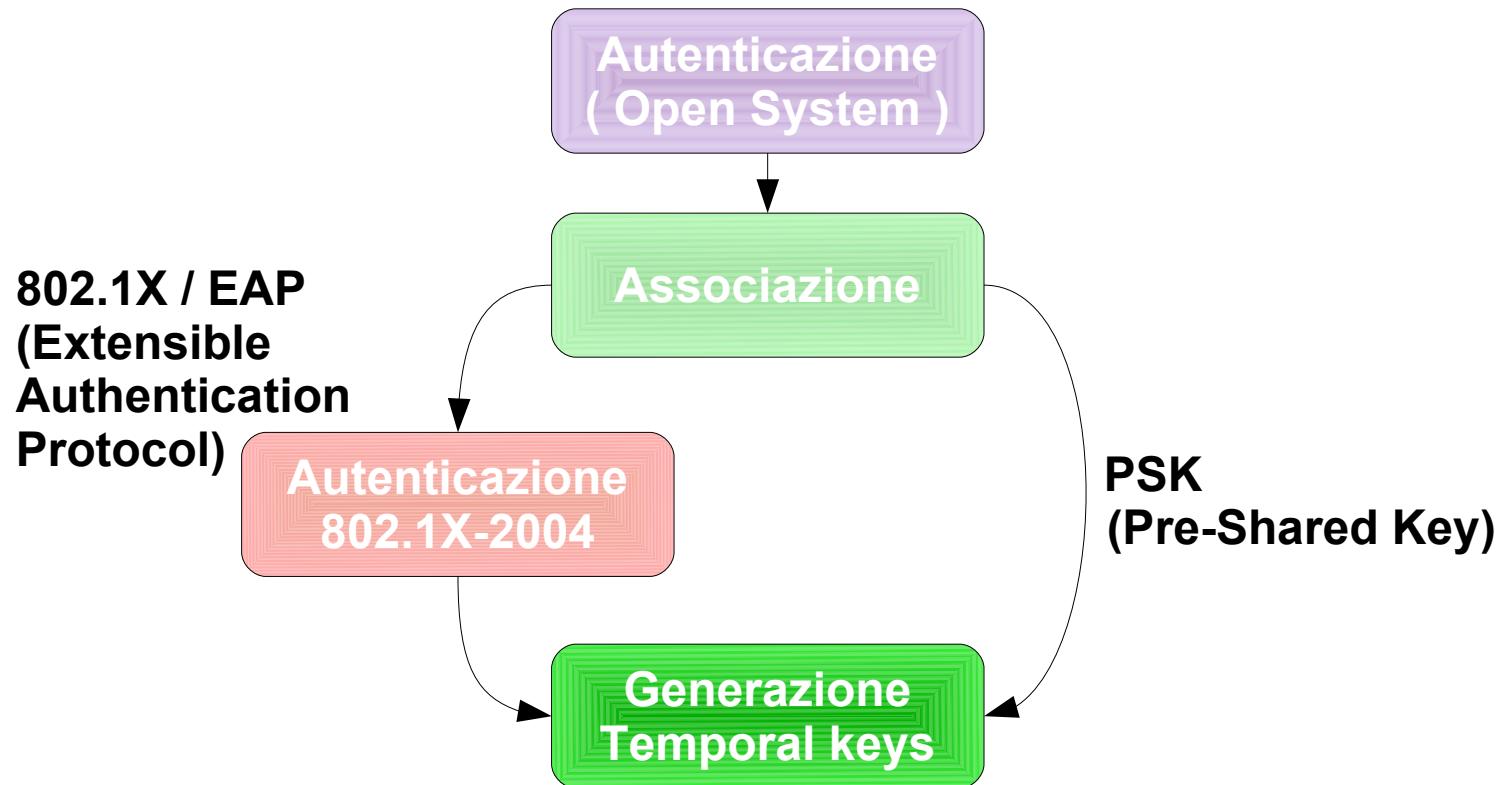
- Quando l'autenticazione 802.1X si conclude con successo, il supplicant e l'AS condividono un “segreto” denominato **PMK** (Pairwise Master Key)
 - Pairwise fa riferimento al fatto che è relativo alla particolare coppia (supplicant, authenticator)
- L'AS trasferisce la PMK all'AP
 - La modalità non è definita nello standard
- La PMK è usata per generare le chiavi usate da TKIP e CCMP

Pre-Shared Key (PSK)



- Nel caso di autenticazione PSK (Pre-Shared Key), la *passphrase* nota a stazione e AP viene usata come PMK

Autenticazione



Gestione delle chiavi



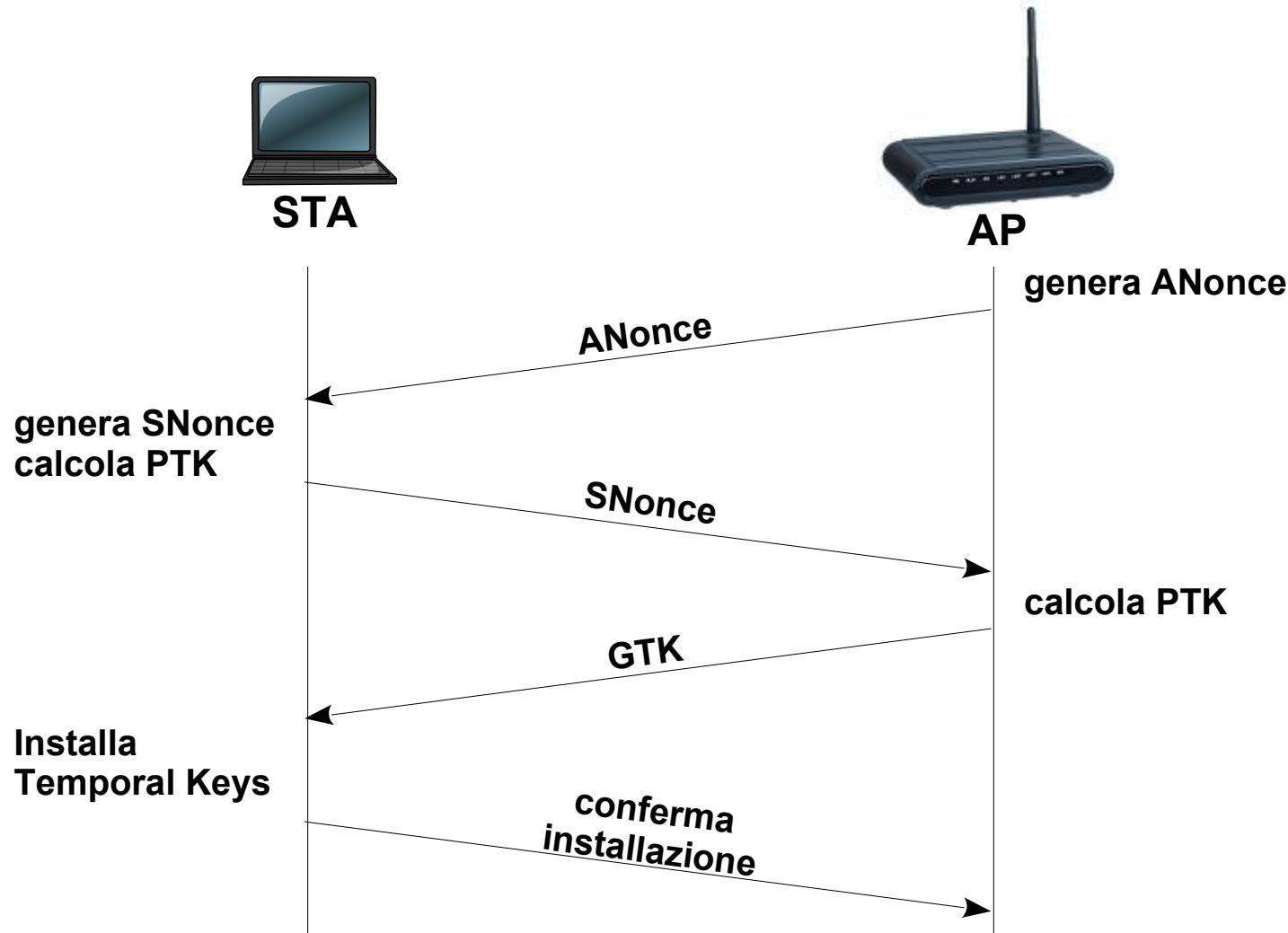
DIE
TI.
UNI
NA

- Due chiavi usate da una stazione:
 - *pairwise*: per cifrare le frame unicast (dirette all'AP)
 - *group*: per cifrare le frame multicast e broadcast
- Vengono determinate a valle di una procedura nota come *4-Way Handshake* che ha l'obiettivo di:
 - Confermare l'esistenza della PMK presso le stazioni
 - Confermare il metodo di cifratura da usare
 - Sincronizzare l'installazione delle Temporal Key
 - Trasferire la chiave di gruppo da AP a STA
- Il 4-Way Handshake può essere ripetuto in seguito per generare nuove chiavi

4-Way Handshake



DIE
TI.
UNI
NA



$$\text{PTK} = f(\text{PMK}, \text{STA_address}, \text{AP_address}, \text{ANonce}, \text{SNonce})$$

$$\text{GTK} = f(\text{GMK}, \text{AP_address}, \text{GNonce})$$

4-Way Handshake

- A valle del 4-Way Handshake, AP e STA hanno calcolato la PTK (Pairwise Temporal Key)
 - Nel caso di TKIP, la PTK fornisce:
 - TK da usare per le funzioni di key mixing
 - MIC key da usare da STA → AP
 - MIC key da usare da AP → STA
 - Nel caso di CCMP, la PTK fornisce la TK da usare
 - L'AP ha inviato a STA la GTK (Group Temporal Key) usata da:
 - STA per decifrare le frame broadcast inviate da AP
 - AP per cifrare le frame da inviare in broadcast

Group Key Handshake



- L'AP può decidere di utilizzare una nuova GTK
- Per inviarle a tutte le stazioni associate, inizia una procedura nota come Group Key Handshake con ciascuna stazione
- Consiste di 2 messaggi:
 - L'AP invia a STA la nuova GTK
 - La STA riscontra la ricezione del primo messaggio

WPA? WPA2?

- WPA (Wi-Fi Protected Access) indica una certificazione della Wi-Fi Alliance prodotta *prima* della pubblicazione dello standard 802.11i
 - grosso modo certifica la cifratura TKIP
- WPA2 certifica invece la piena conformità allo standard 802.11i

Riferimenti

- IEEE Std 802.11-2007
 - Cap. 8
- 802.11 Wireless Networks: The Definitive Guide
 - Capp. 5, 6