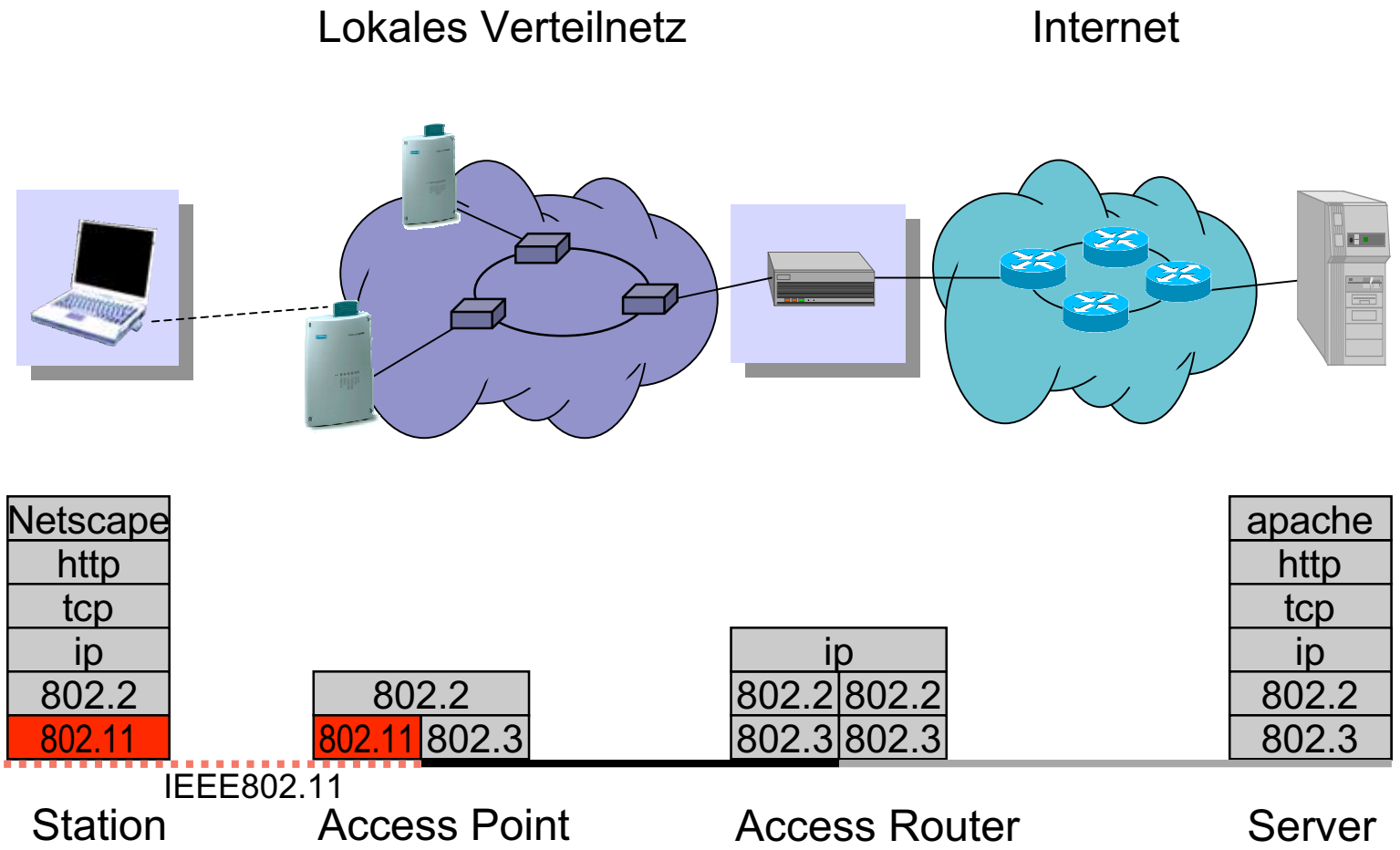
Verbesserte WLAN Sicherheit mit WPA, EAP und 802.11i

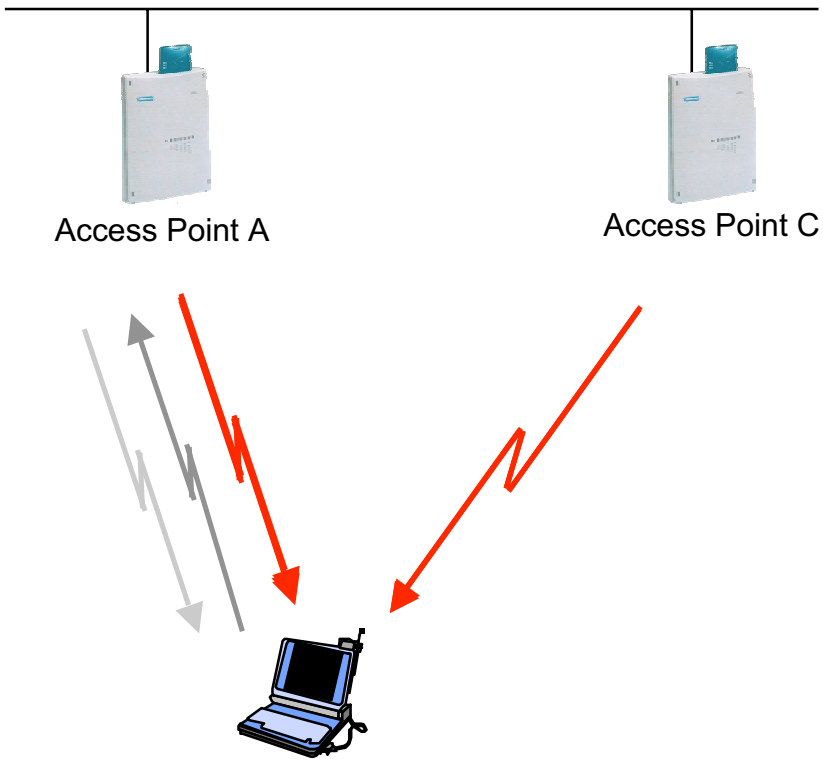
Maximilian Riegel

Wireless LAN IEEE802.11 Architektur



Einbuchen in ein Wireless LAN: z.B. passives Scanning

- Erstmaliger Verbindungsaufbau zu einem Access Point
  - Wiederherstellung der Verbingung erfolgt ähnlich.



Ablauf Association:

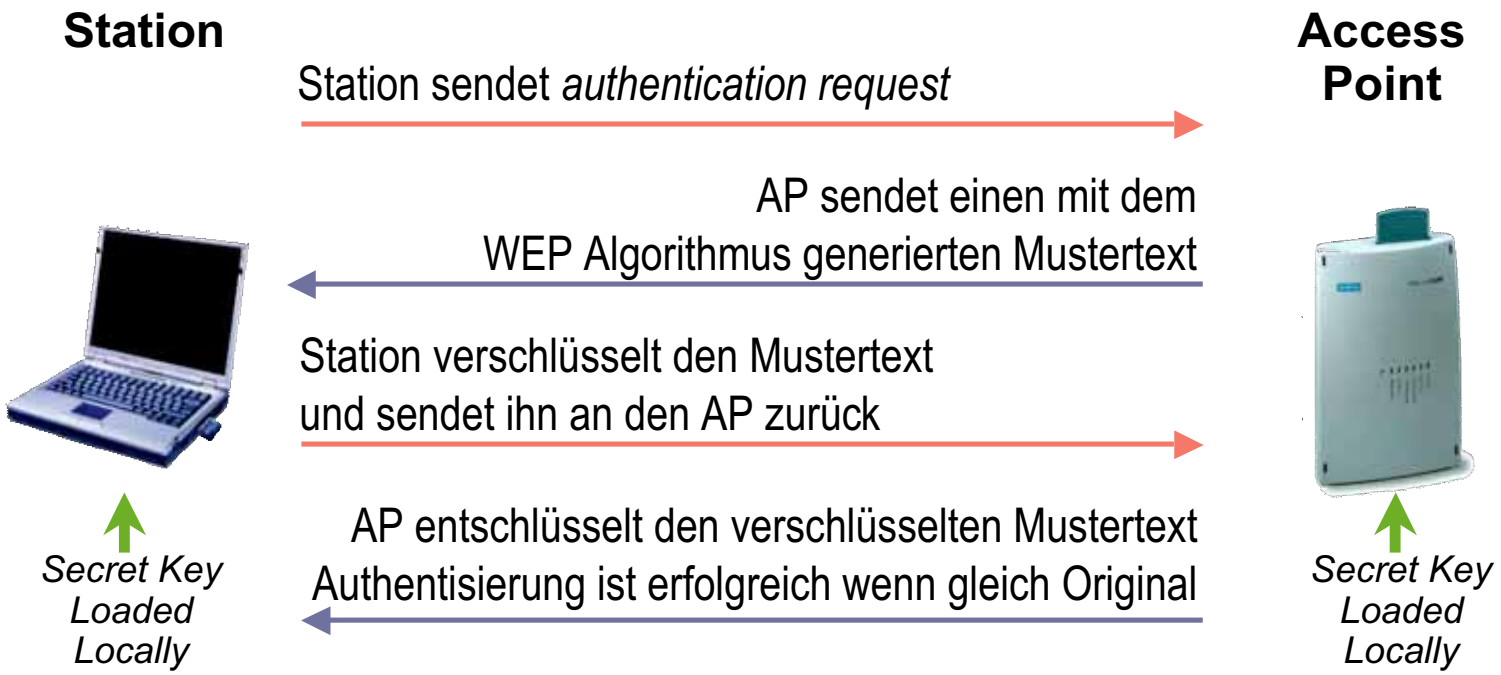
APs senden Beacons.

Station wählt besten AP aus.

Station sendet Association Request zum gewählten AP.

AP sendet Association Response zurück.

Shared key Authentisierung



- Shared key Authentisierung benötigt den WEP Algorithmus
- Schlüsselmanagement ist in IEEE802.11 nicht spezifiziert
- Die Authentisierung erfolgt nur einseitig

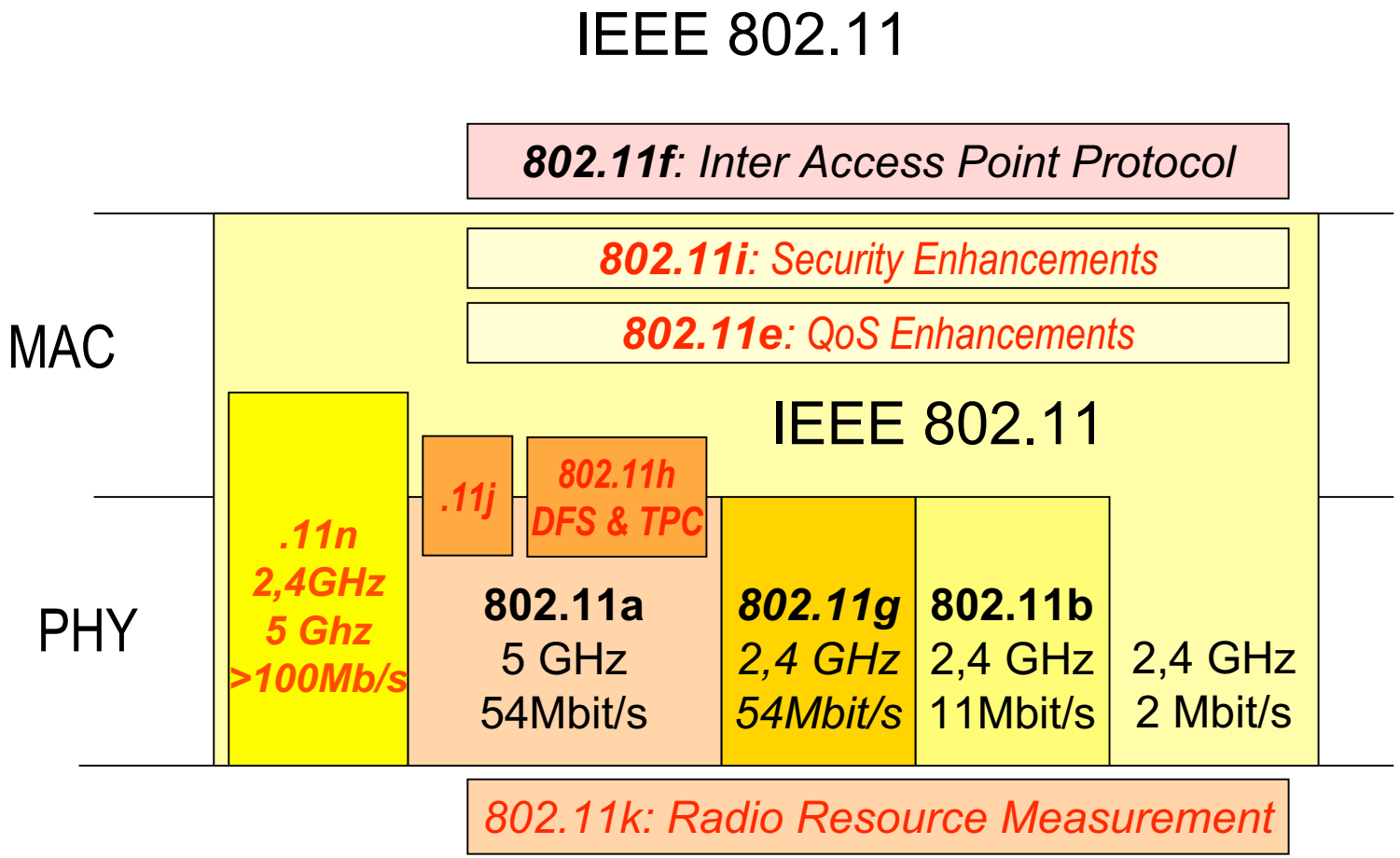
IEEE802.11 Verschlüsselung und Zugangskontrolle

- Ziel von 802.11 war eine "Wired Equivalent Privacy" (WEP)
  - Weltweit verwendbar
- 802.11 bietet einen Authentisierungsmechanismus
  - zur Unterstützung der Zugangskontrolle.
  - sieht "OPEN", "Shared Key" und proprietäre Verfahren vor
- Shared key Athentisierung basiert auf WEP
  - Beschränkt sich auf Station-zu-Station, nicht Ende-zu-Ende.
  - Benützt den RC4 Algorithmus mit:
    - *40 bit secret key*
    - *und einen 24 bit IV der mit den Daten mitgeschickt wird.*
    - *beinhaltet einen ICV für die Integritätsprüfung.*

Nachteile der einfachen WEP Sicherheit

- WEP ist bei jeder Schlüssellänge unsicher
  - IV zu klein, Schutz vor IV Wiederverwendung fehlt
  - Angriffsmöglichkeit bei bekanntem Klartext
- Keine Benutzerauthentisierung
  - Nur das Netzwerkinterface wird authentisiert
- Keine gegenseitige Authentisierung
  - Nur die Stations authentisieren sich gegenüber dem AP
- Fehlende Schlüsselverwaltung
  - Kein Standard zum Austausch der Schlüssel während des Betriebs
  - Schlüsselverwaltung für einen grosseren Nutzerkreis schwierig
- WEP ist auf keinen Fall eine Einrichtung für absolute Sicherheit,
  - … aber kann in manchen Gelegenheiten nützlich sein.
- IEEE P802.11 hat vor 4 Jahren eine Arbeitsgruppe zur Verbesserung der Sicherheit von WLAN eingerichtet.
  - Die Task Group 802.11i hat ihre Arbeit nun abgeschlossen.

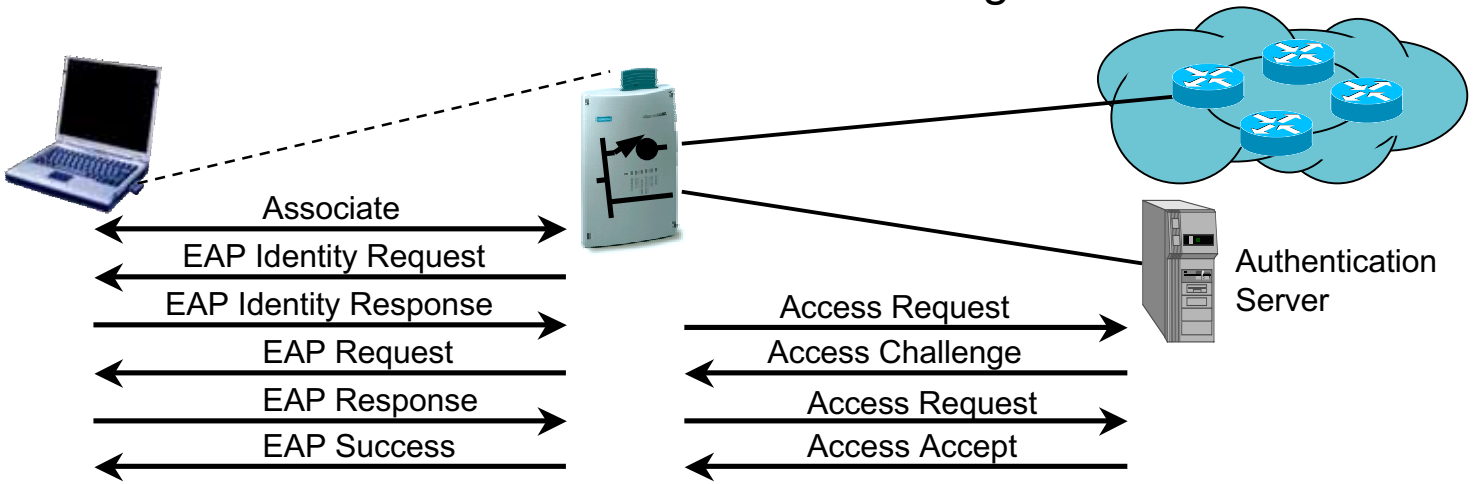
Wireless LAN Standardisierung



IEEE802.11i: Robust Security Network (RSN)

Zusätzliche Verbesserungen zu bestehenden Funktionen:

- Datenverschlüsselung:
  - TKIP (Temporal Key Integrity Protocol) um mit RC4-basierter Hardware höhere Sicherheitsanforderungen zu erfüllen, und
  - WRAP (Wireless Robust Authenticated Protocol) basierend auf AES (Advanced Encryption Standard) und CCMP
- Management der gesicherten Verbindung:
  - RSN Verhandlungen zur Errichtung des Sicherheits-Kontexts
  - IEEE802.1X basierte Authentisierung und Schlüsselverwaltung



Sicherheitsanforderungen an den Datentransport

- Kein Transport ungesicherter Datenpakete
- Authentisierung der Nachrichtenquelle
  - Vermeidung von Betrug
- Serialisierung der Pakete
  - Detektierung von Wiederholungen
- Vermeidung der Schlüsselwiederverwendung
  - 48 bit Sequenznummer
- Schutz der Quell- und Zieladresse
- Einsatz von starker Verschlüsselungstechnik
  - für den Schutz von Vertraulichkeit und Integrität

TKIP: Temporal Key Integrity Protocol

- Zur Maskierung der Schwächen von WEP auf existierender AP Hardware
- Ist als Hülle für den WEP-Algorithmus konstruiert
  - Kann vollständig in Software implementiert werden
  - Macht Gebrauch von existierender WEP Hardware
  - Betreibt WEP als Komponente
- *Die Lösung erfüllt die Ansprüche an einen guten Standard!*
  - *niemand ist damit wirklich voll zufrieden*
- TKIP verwendet zwei Arten von Schlüssel
  - 1x 128 bit für die Verschlüsselung der Daten; AP und STA verwenden den selben Schlüssel
  - 2x 64-bit für den Schutz der Integrität: AP und STA verwenden unterschiedliche Schlüssel

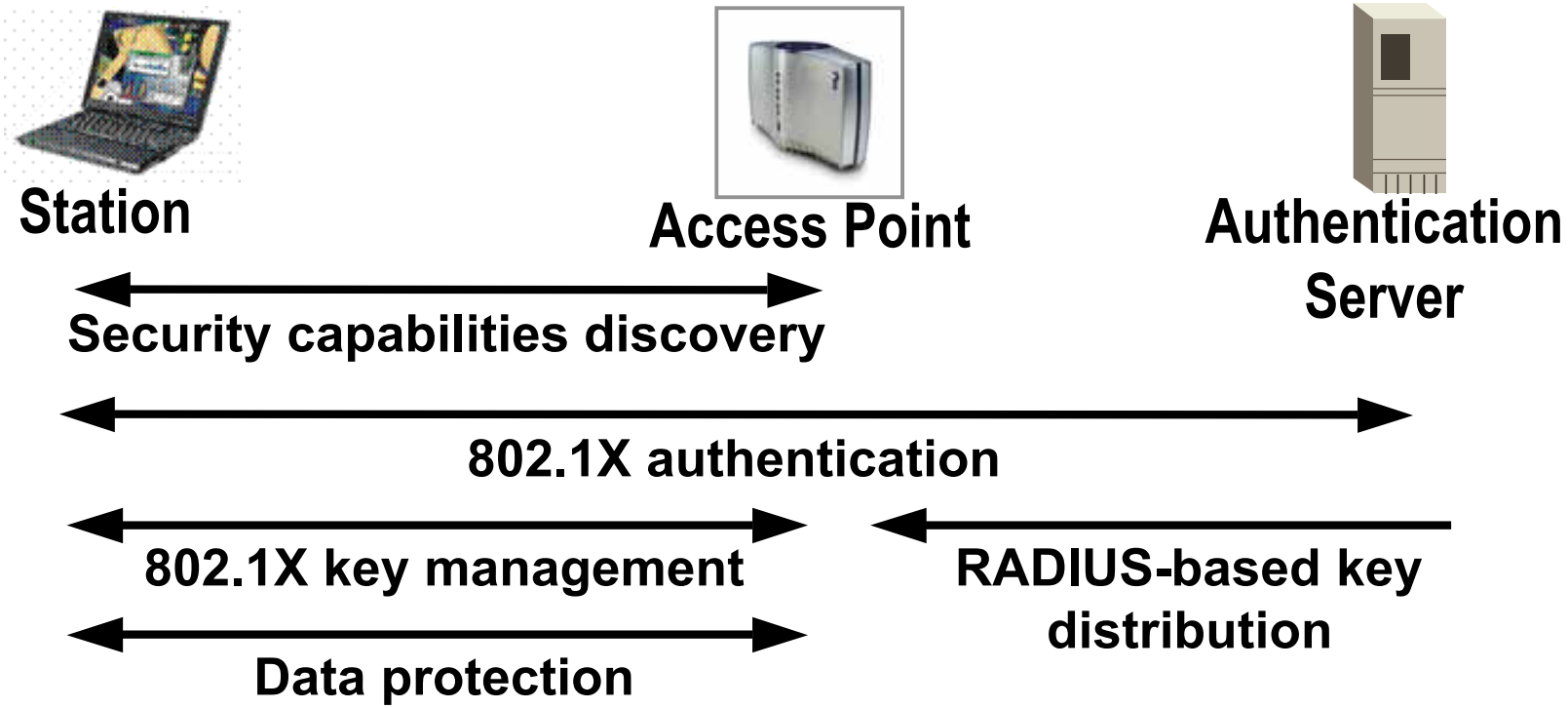
CCMP

- Die verbindliche Verschlüsselungslösung für 802.11 auf Dauer
- Ein vollständig neues Protokoll ohne Verwandschaft zu WEP
- Speziell für IEEE 802.11i entworfen
- Benötigt einen einzelnen 128-bit Schlüssel
  - Der selbe 128-bit Arbeitsschlüssel wird auf AP und STA eingesetzt.
- Schlüsselkonfiguration durch 802.1X
- CCMP verwendet CCM um
  - Datenpakete zu verschlüsseln
  - ausgewählte Header-Felder vor Verfälschung zu sichern
- CCM = Counter Mode Encryption mit CBC-MAC Data Origin Authenticity mit einem einzigen Schlüssel
  - Verlangt einen 128 bit block cipher – IEEE 802.11i verwendet AES
  - Die Anforderungen von AES verlangen neue AP Hardware
  - Die Anforderungen von AES können neue Hardware bei Handheld-Geräten bedingen, aber nicht bei PCs

Zusammenfassung: Datentransport

	WEP	**TKIP**	**CCMP**
Cipher	RC4	RC4	AES
Key Size	40/104 bits	128 bits Encr. 64 bit auth	128 bits
Key Life	24-bit IV, wrap	48-bit IV	48-bit IV
Packet Key	Concat.	Mixing Fnct.	Not Needed
Integrity			
Data	CRC-32	Michael	CCM
Header	None	Michael	CCM
Replay	None	Use IV	Use IV
Key Mgmt.	None	EAP-based	EAP-based

802.11 Betriebsablauf für die Einrichtung einer gesicherten Verbindung



Ablaufphasen

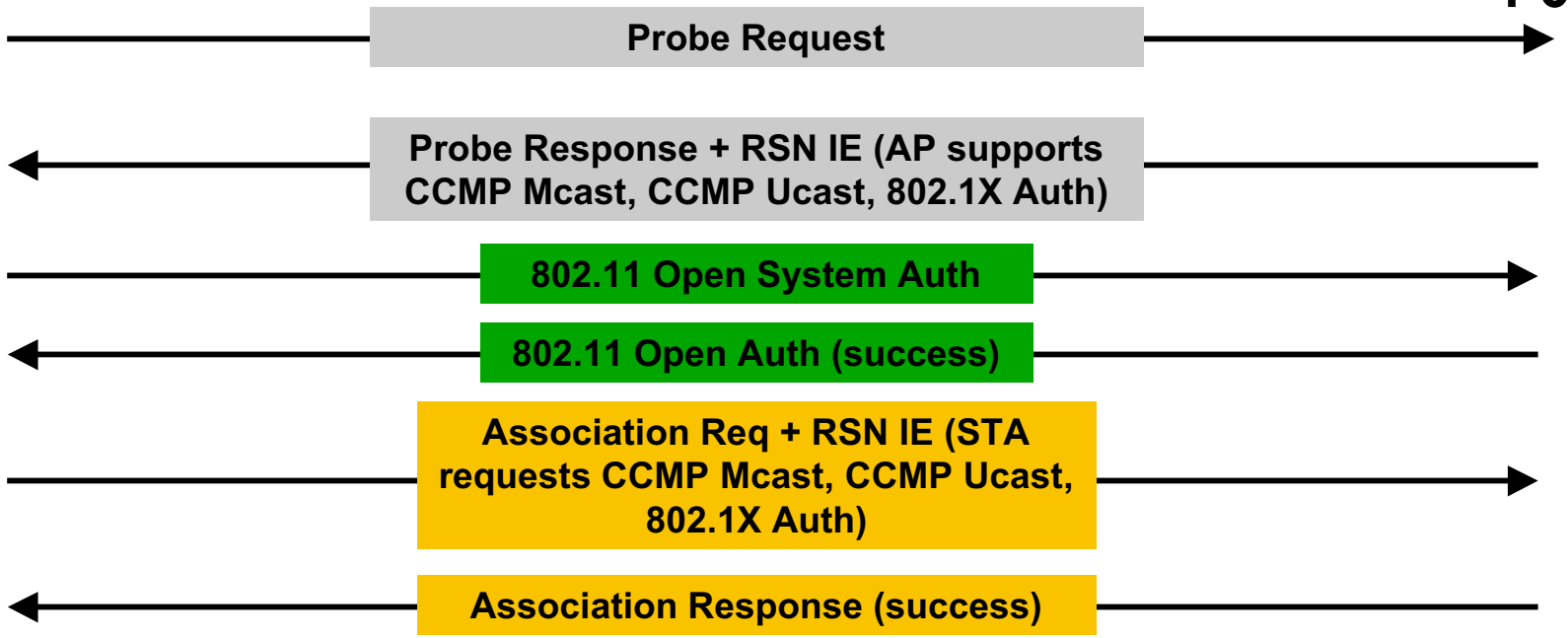
- *Discovery*
- *Authentication*
- *Key Management*

Zweck der einzelnen Phasen

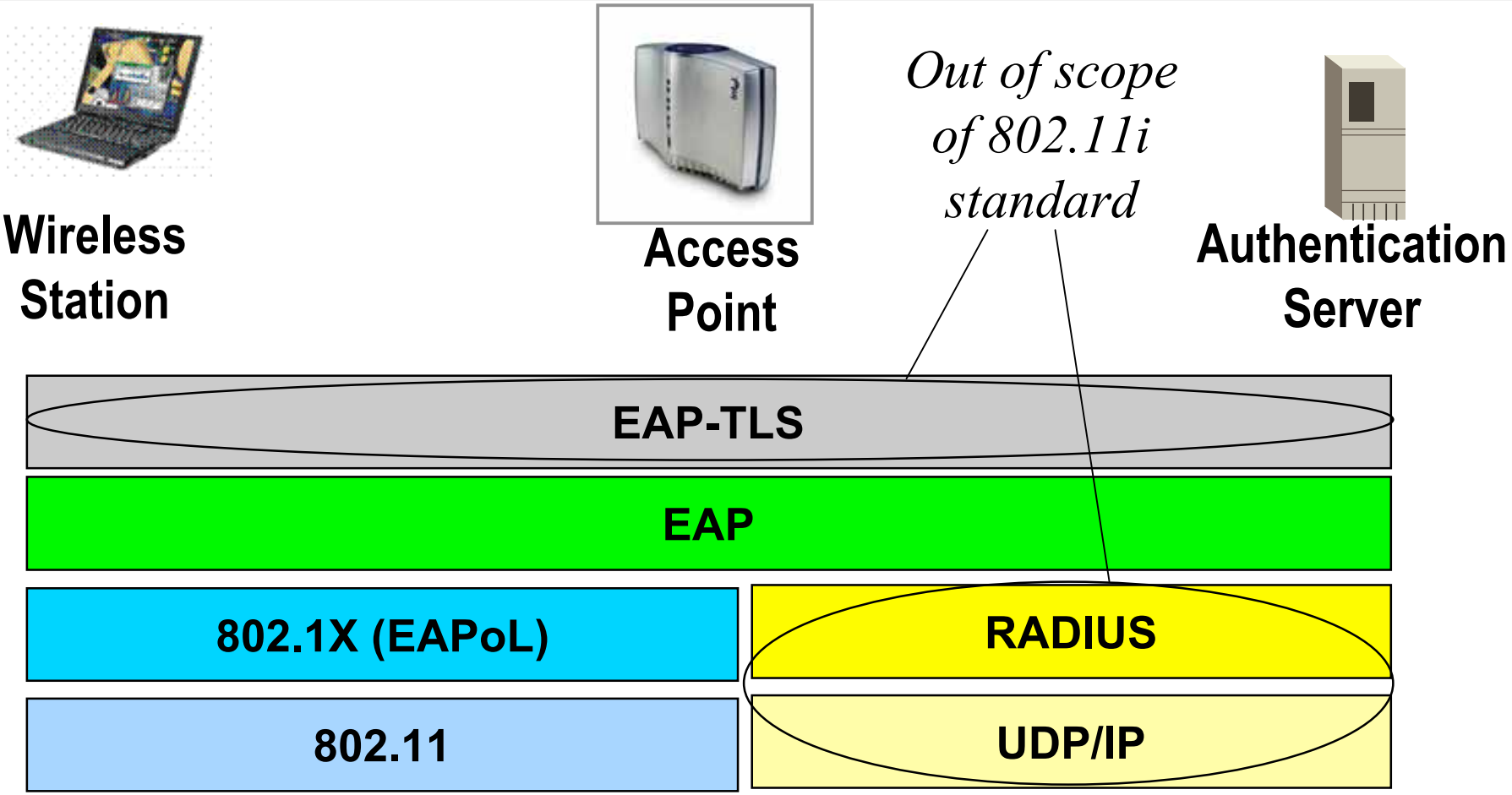
- Discovery
  - Bestimmung von potentiellen Kommunikationspartnern
  - Der AP informiert die STAs über die Sicherheitsfeatures
- Authentication basierend auf 802.1X
  - Zentrale Verwaltung der Zugangskontrolle im AS
  - Endgültige Entscheidung der STA über den Verbindungsaufbau
  - Gegenseitige Authentisierung zwischen STA und AS
  - Erzeugung des *Master Key* als Abfallprodukt der Authentisierung
  - Erzeugung des *Authorization token* aus dem *Master Key*
- RADIUS-basierende Schlüsselübergabe
  - AS übergibt den Session-Key (PMK) zu dem dazugehörigen AP
- Key management mittels 802.1X
  - Bindung des PMK zur STA und zum AP
  - Bestätigung dass beide, der AP und die STA den PMK besitzen
  - Die Erzeugung von frischen Arbeitsschlüsseln (PTK)
  - Überwachung der Arbeitsfähigkeit der Kommunikationspartner

Discovery

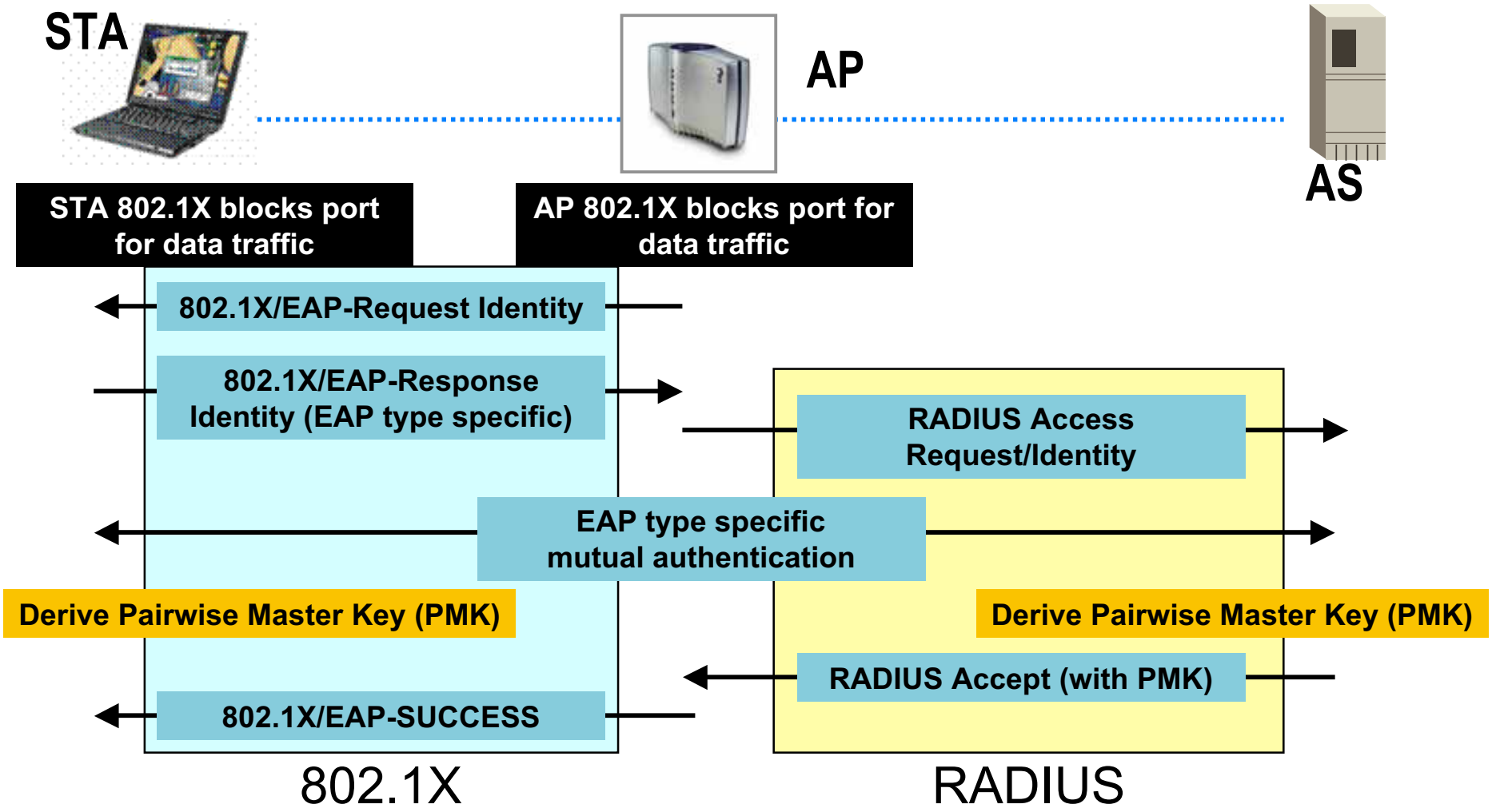
Station **Access Point**



Authentication and Key Management Architektur



Authentication



802.1X und EAP

802.1X

- Einfacher Transport von EAP Nachrichten über IEEE802 LANs
- Einrichtung und Verweigerung der Öffnung für Ports
- Adaptiert EAP Architektur
  Authentication server/AP ("Authenticator")/STA ("Supplicant")

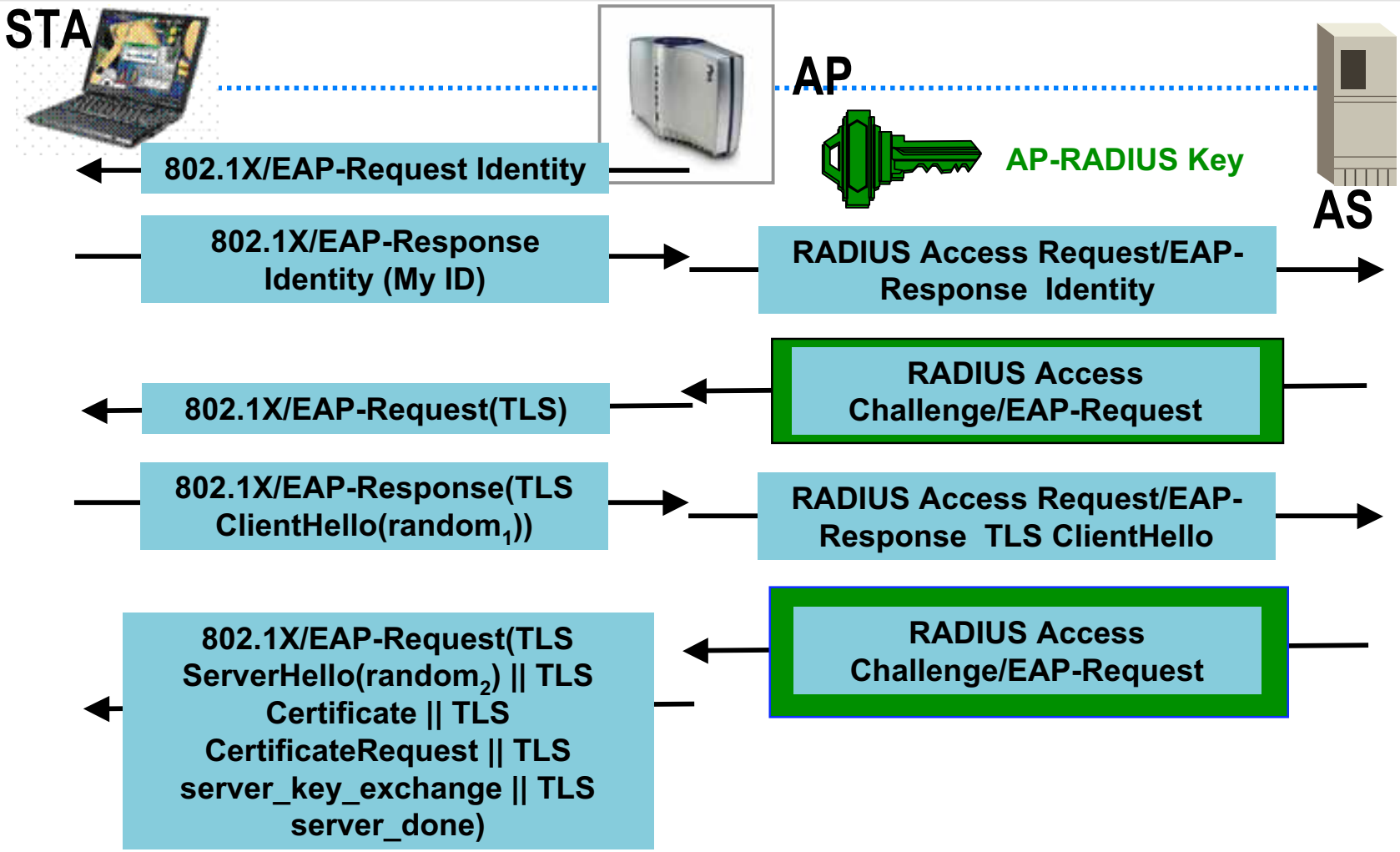
EAP (Extensible Authentication Protocol)

- Transportprotokoll für Authentisierungsinformation, nicht die Authentisierungsmethode an sich
  - kein kryptographischer Schutz der Nachrichten
  - kein Schutz gegen gefälschte EAP-Success-Nachrichten
  - vertraut auf die Fähigkeiten der konkreten Authentisierungsmethoden
- Effiziente Anwendung in IEEE802.11:
  - Minimiert AP Kosten durch Verlagerung der Authentisierung in den AS
  - Ein AP kann ganz unterschiedliche Authentisierungsmethoden bedienen

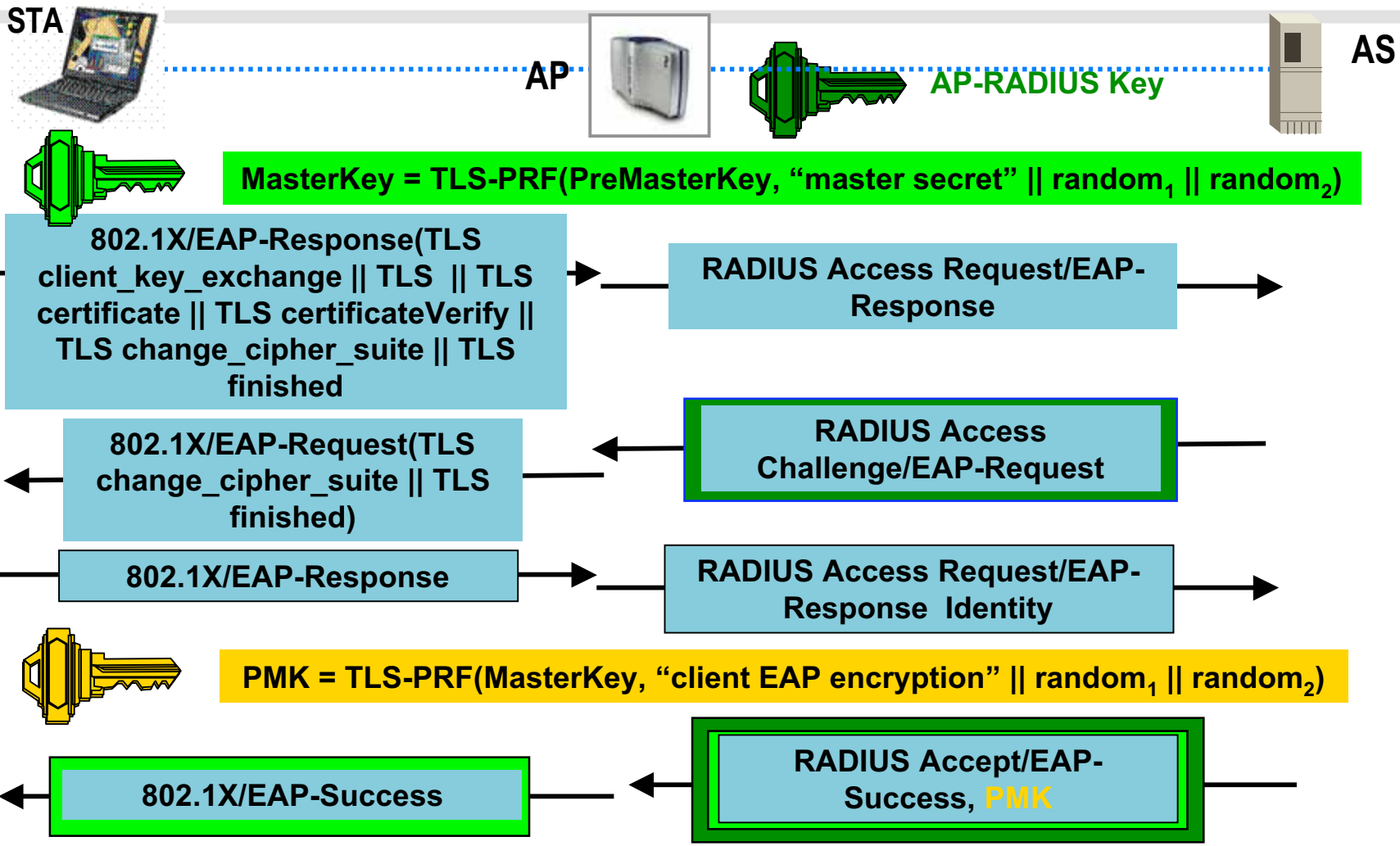
EAP-TLS

- EAP-TLS ist nicht Teil von 802.11i
  - genausowenig wie jede andere spezifische Authentisierungsmethode
- Aber EAP-TLS ist die de-facto 802.11i Authentisierungsmethode
  - Im Gegensatz zu anderen verbreiteten EAP-Methoden erfüllt sie alle 802.11i Anforderungen
- EAP-TLS = TLS Handshake über EAP
  - EAP-TLS ist bereits standardisiert (RFC 2716)
  - Verwendet den selben Verbindungsaufbau wie TLS/SSL
- Verlangt, dass grundsätzlich immer das AS Zertifikat auf der STA installiert wird
- Beidseitige Authentisierung verlangt die Bereitstellung eines STA Zertifikats im AS.

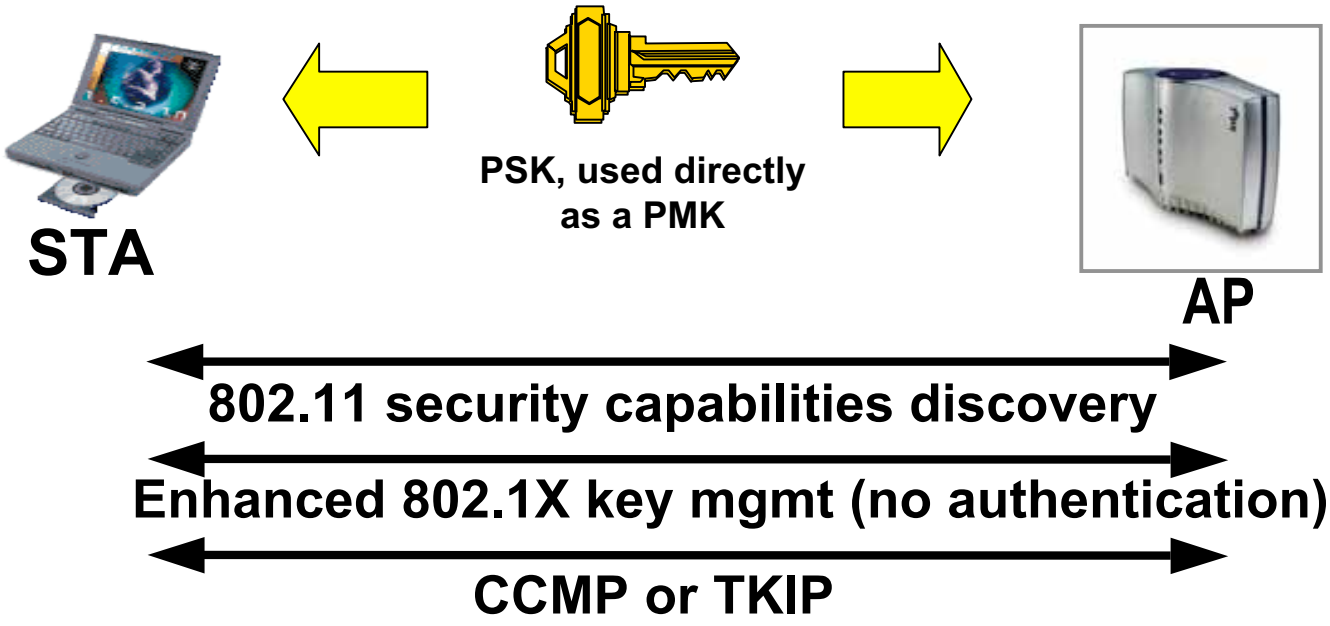
Authentication basierend auf EAP-TLS (1)



Authentication based on EAP-TLS (2)



Sicherheit ohne Authentication Server
Pre-shared Key



Schlüsselgenerierung aus einem Passwort

- Verwendet PKCS #5 v2.0 PBKDF2 um einen 256-bit PSK aus einem ASCII Passwort zu generieren
- Motiv:
  Heimanwender konfigurieren vielleicht Passwörter, aber niemals Schlüssel

Key Management

- Original 802.1X Schlüsselmanagement hoffnungslos fehlerbehaftet
- Neues Modell in IEEE 802.11i:
  - Ableitung eines Pairwise Master Key (PMK)
  - AP und STA verwenden den PMK um den Pairwise Transient Key (PTK) zu erzeugen
  - Der PTK wird zum Schutz der Verbindung eingesetzt
- *4-Way Handshake*
  - Etabliert einen frischen, dedizierten Schlüssel für die STA und den AP für diese Session
  - Überprüft die Betriebsfähigkeit der Peers
  - Zeigt an, dass es keinen man-in-the-middle zwischen Inhabern eines PTK gibt, wenn es keinen man-in-the-middle für den PMK gab.
  - Synchronisiert den Gebrauch der paarweisen Schlüssel
- *Group Key Handshake* versorgt alle STAs mit dem Group Key

Key Management Overview

STA 

AP

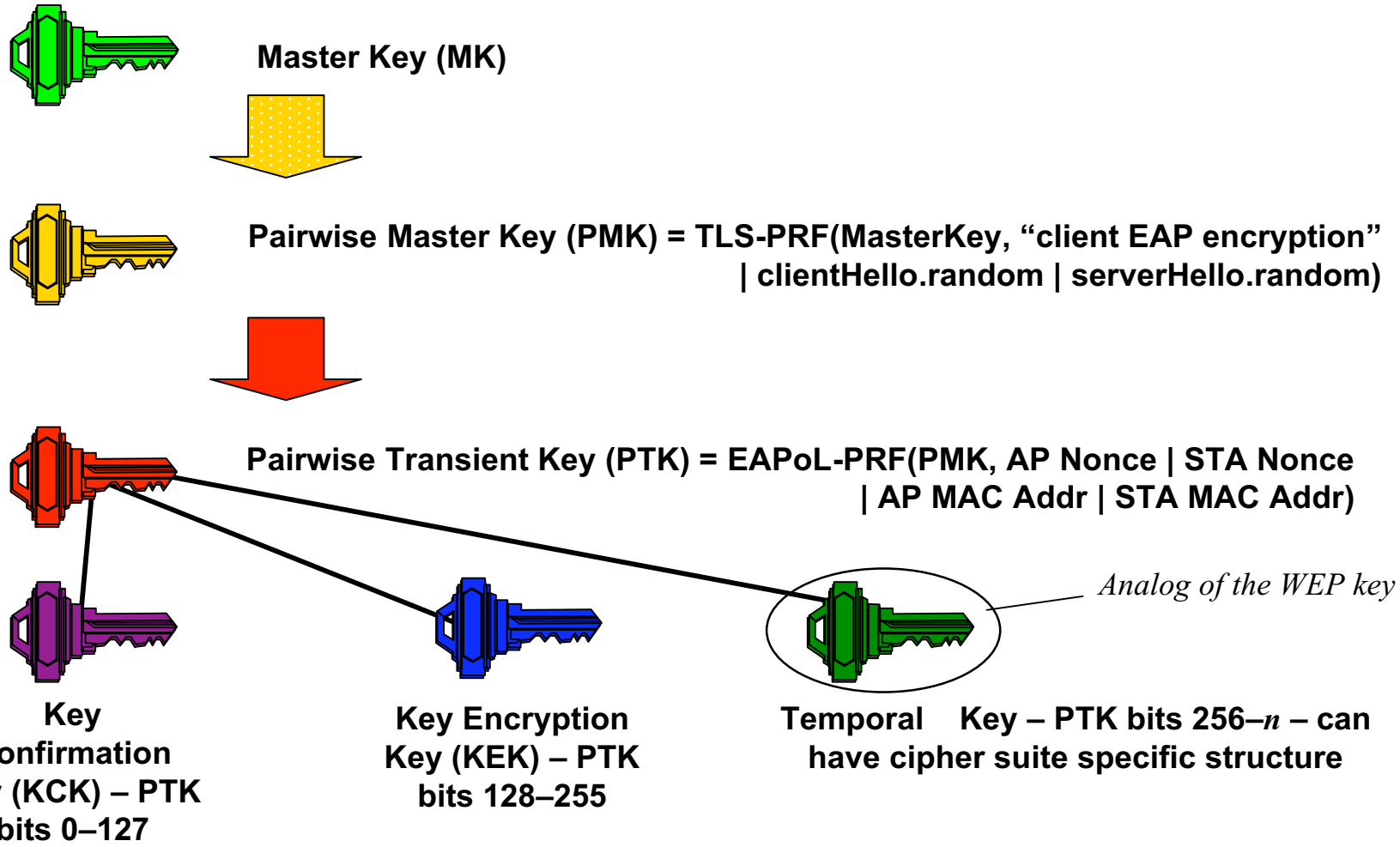
AS 

Step 0: Use RADIUS to push PMK from AS to AP

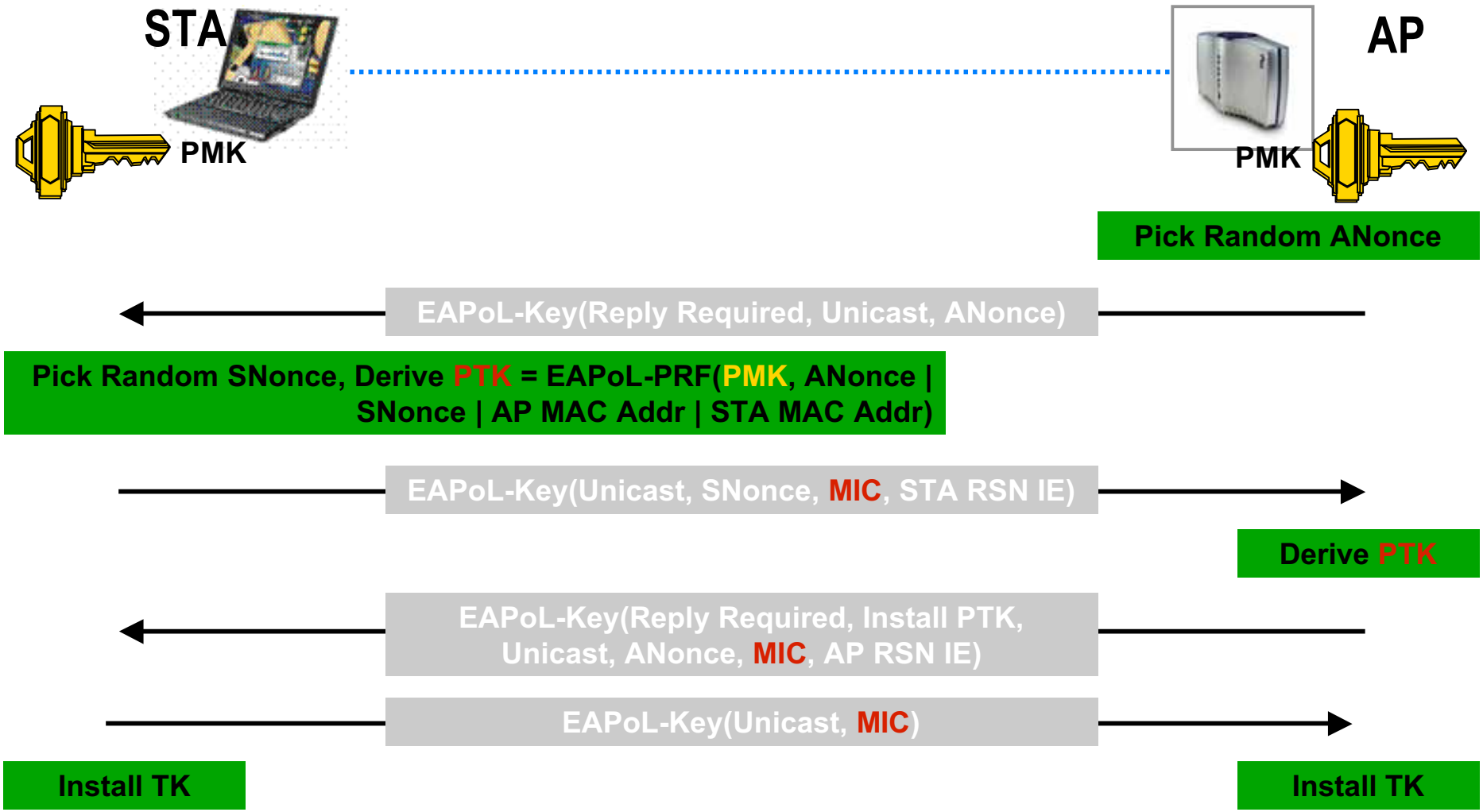
Step 1: Use PMK and 4-Way Handshake to derive, bind, and verify PTK

Step 2: Use Group Key Handshake to send GTK from AP to STA

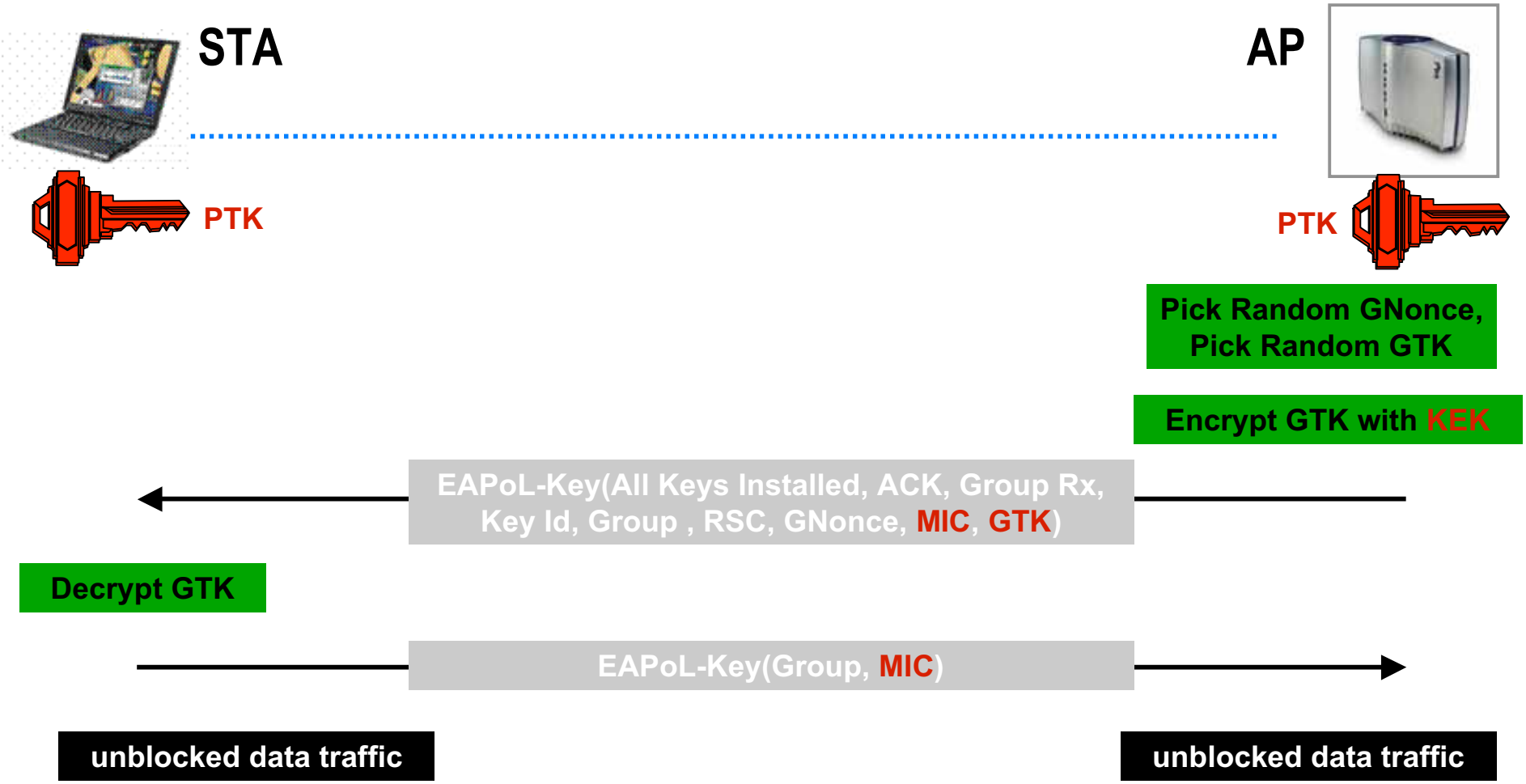
Pairwise Key Hierarchy



Schritt 1: 4-Way Handshake



Schritt 2: Group Key Handshake



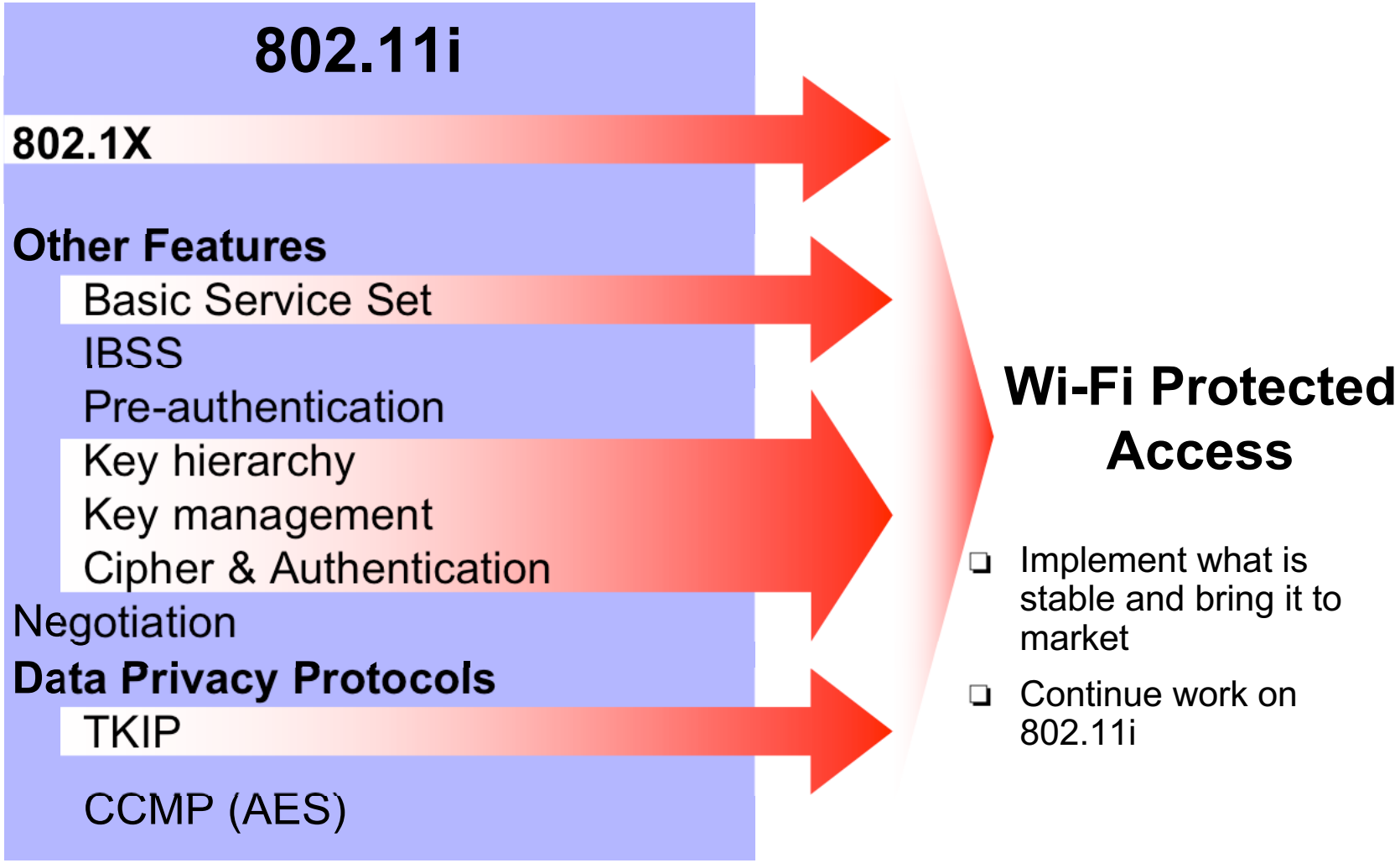
Wi-Fi Alliance (http://www.wi-fi.org)

- Zielsetzung:
  - Zertifizierung der Interoperabilität von IEEE802.11 Produkten
    - *Vergabe des Wi-Fi Zeichens*
  - Verbreitung des Wi-Fi Zeichens als marktübergreifendes Merkmal aller IEEE802.11 konformen Lösungen
- Derzeitige Aktivitäten:
  - Bekanntmachung und Umsetzung der Gütesiegel-Strategie
    - *einheitliches Wi-Fi Logo für alle IEEE 802.11 Zertifizierungen*
    - *produktspezifisch ergänzt durch die Kennzeichnung der getesteten Funktionalitäten*
  - Beginn der 802.11a/b/g Wi-Fi Zertifikation inklusive Dual-Mode/Dual-Band Funktion
  - Bekanntmachung der Wi-Fi Protected Access (WPA) Initiative, verpflichtend für alle neuen Produkte
  - Weitere Vorbereitung des Wi-Fi Zone Programms

Logo

Gütesiegel

WPA and 802.11i



ENDE

- **Danke für Ihre Aufmerksamkeit.**
- **Fragen und Antworten?**

Maximilian Riegel (riegel@max.franken.de)

Literature:

- 802.11 Wireless Networks – The Definitive Guide
  Matthew S. Gast; O‘ Reilly, ISBN 0-596-00183-5
- Real 802.11 Security: Wi-Fi Protected Access and 802.11i
  Jon Edney ,William A. Arbaugh; Addison Wesley 2003
  ISBN : 0-321-13620-9