WLAN im öffentlichen Raum

Was Hotspot 2.0 bringt.

Max Riegel

2011-11-20

Ankündigung

WLAN im öffentlichen Raum

Was Hotspot 2.0 bringt.

- **Während der Einsatz von 'Wireless Protected Access (WPA2)" inzwischen Standard beim WLAN im Heim- und Firmennetz ist, wird im öffentlichen Raum WLAN immer noch ungesichert betrieben und der Zugang mittels Portalseiten im umgeleiteten Web-Browser geregelt.**
- **Der Vortrag stellt vor, wie die Initiative 'Hotspot 2.0' der Wi-Fi Alliance den gesicherten WLAN Zugang auch im öffentlichen Raum einführen und die Zugangskontrolle über umgeleitete Webseiten ablösen wird.**

Inhaltsübersicht

- **Einführung**
  - Segmentierung der WLAN Zugänge
  - Stand der Technik im Heim- und Unternehmensnetz
- **Aktuelle Technik beim öffentlichen WLAN Zugang**
  - Offener Zugang und Umlenkung von Web-Browserzugriffen
  - Betriebliche Schwächen der aktuellen Technik
  - Sicherheitsprobleme
- **Die ‘Hotspot 2.0’ Initiative der Wi-Fi Alliance**
  - Anwendungsszenarien
- **Die IEEE802.11u Erweiterung des WLAN Standards**
- **Technische Komponenten der Hotspot 2.0 Lösung**
  - Erkennung und Auswahl des gewünschten WLAN Netzes
  - Der gesicherte Zugang mit WPA2-Enterprise
  - Automatische Konfiguration von WLAN Parametern in Terminals
  - Einrichtung eines neuen WLAN Accounts über WLAN
- **Zusammenfassung und Ausblick**

Hinweis

- **Die Unterlagen zu Hotspot 2.0 sind bisher nicht frei zugänglich sondern unterliegen der Vertraulichkeits-verpflichtung der Wi-Fi Alliance.**
- **Der Vortrag basiert auf frei verfügbaren Informationen im Web und insbesondere auf den Vortragsfolien, die von der Wi-Fi Alliance für öffentliche Schulungs-veranstaltungen in Paris und Tokyo verwendet wurde.**
- **Nachdem die Spezifikation von Hotspot 2.0 noch nicht abgeschlossen ist, sollten die vorgestellten technischen Details als vorläufig betrachtet werden.**

  - *BTW: Dieser Vortrag verwendet 'WLAN' anstelle von 'Wi-Fi' für die Bezeichnung der IEEE802.11 Technik, da der Begriff 'WLAN' in Deutschland üblicher ist.*

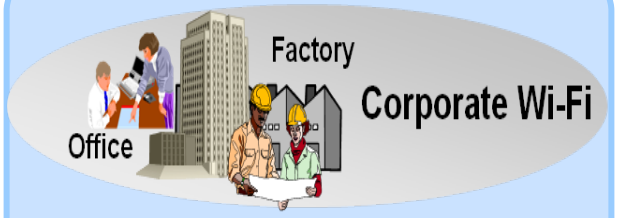
EINFÜHRUNG

WLAN Einsatzfelder

WLAN im Heimnetz

~ 90% der Access Points*

- Aufgebaut und konfiguriert durch ‘Hobby Administratoren’
- Großes Sicherheitsbewußtsein verstärkt durch Gerichtsurteile
- Heute überall verschlüsselte Luftschnittstelle



WLAN im Unternehmensnetz

< 10% der Access Points*

- Aufgebaut und konfiguriert durch die IT Abteilung
- Großes Sicherheitsbewußtsein aus wirtschaftlichen Gründen (Spionage, Sabotage)
- Heute überall verschlüsselte Luftschnittstelle

WLAN im Public Hotspot

< 1% of Access Points*

- Aufgebaut und betrieben von Telekommunikationsbetreiber
- Sicherheit ist Kundensache, Beteiber kümmert sich nur um seine Betriebssicherheit
- Heute grundsätzlich offene Luftschnittstelle

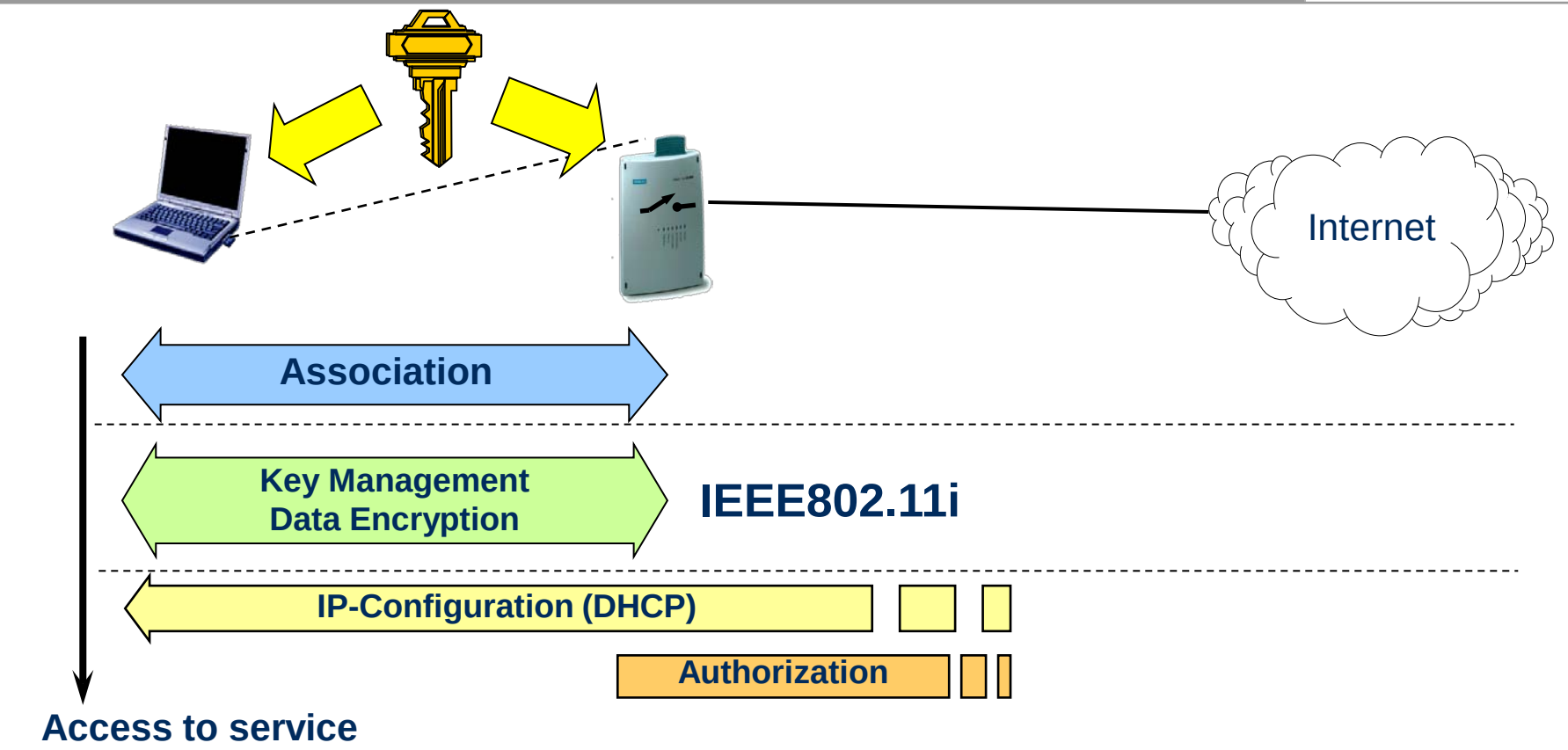
*Die Zahlen sind für den Deutschen WLAN Markt. Ähnliche Verhältnisse gelten in den anderen Ländern (z.B.: USA, Korea)

WLAN Sicherheit

Security Feature	Manual WEP (pre-RSN)	Dynamic WEP (pre-RSN)	*aka* WPA TKIP (RSN)	*aka* WPA2 CCMP (RSN)
Core cryptographic algorithm	RC4	RC4	RC4	AES
Key sizes	40-bit or 104-bit (encryption)	40-bit or 104-bit (encryption)	128-bit (encryption), 64-bit (integrity protection)	128-bit (encryption and integrity protection)
Per-packet key	Created through concatenation of WEP key and the 24-bit IV	Derived from EAP authentication	Created through TKIP mixing function	Not needed; temporal key is sufficiently secure
Integrity mechanism	Enciphered CRC-32	Enciphered CRC-32	Michael message integrity check (MIC) with countermeasures	CCM
Header protection	None	None	Source and destination addresses protected by Michael MIC	Source and destination addresses protected by CCM
Replay detection	None	None	Enforce IV sequencing	Enforce IV sequencing
Authentication	Open system or shared key	EAP method with IEEE 802.1X	EAP method with IEEE 802.1X or PSK	EAP method with IEEE 802.1X or PSK
Key distribution	Manual	IEEE 802.1X	IEEE 802.1X or manual	IEEE 802.1X or manual

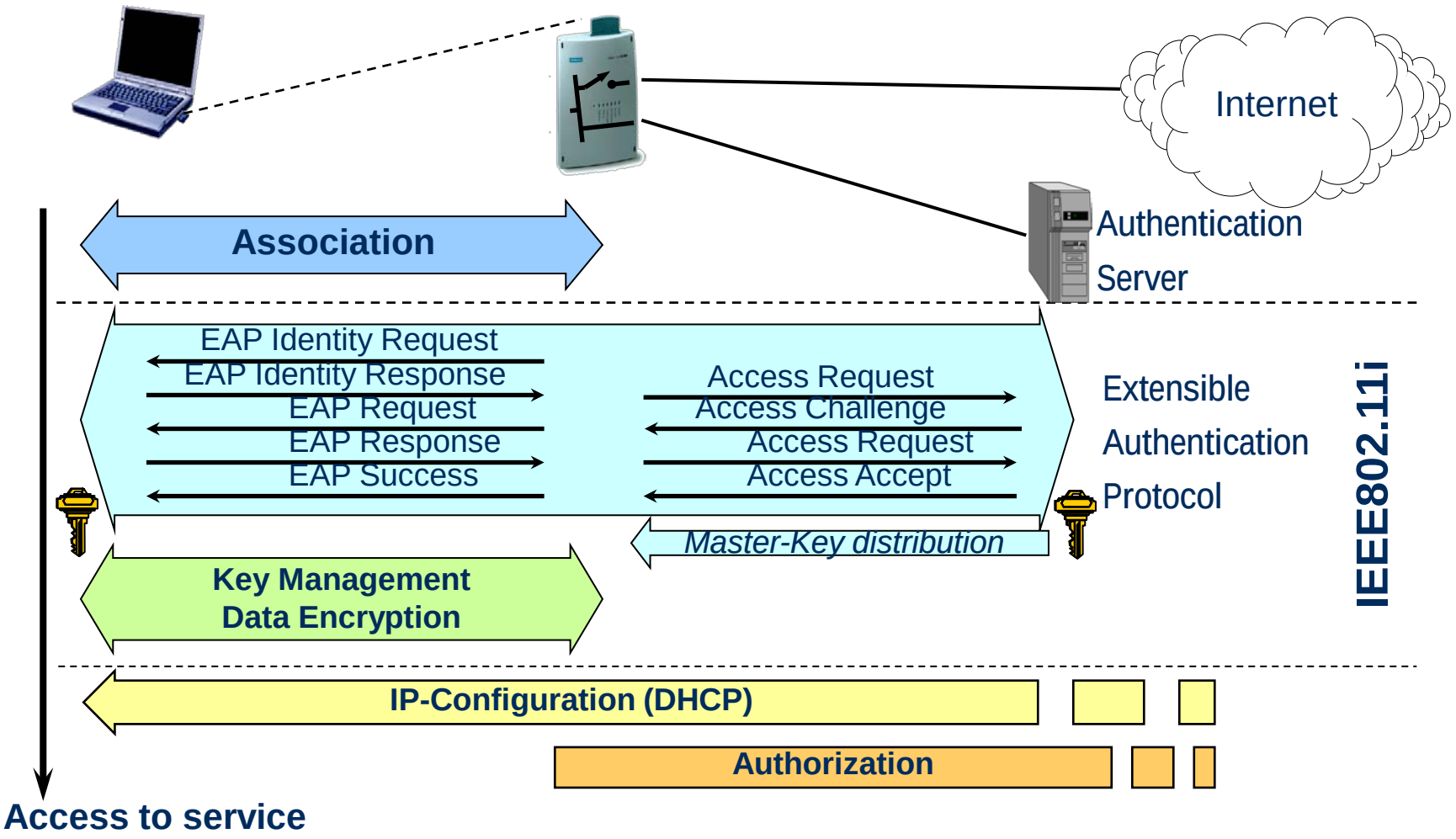
Zwei Modi: **WPA2-PSK und WPA2-Enterprise**

WPA2-PSK (Pre-Shared Key)



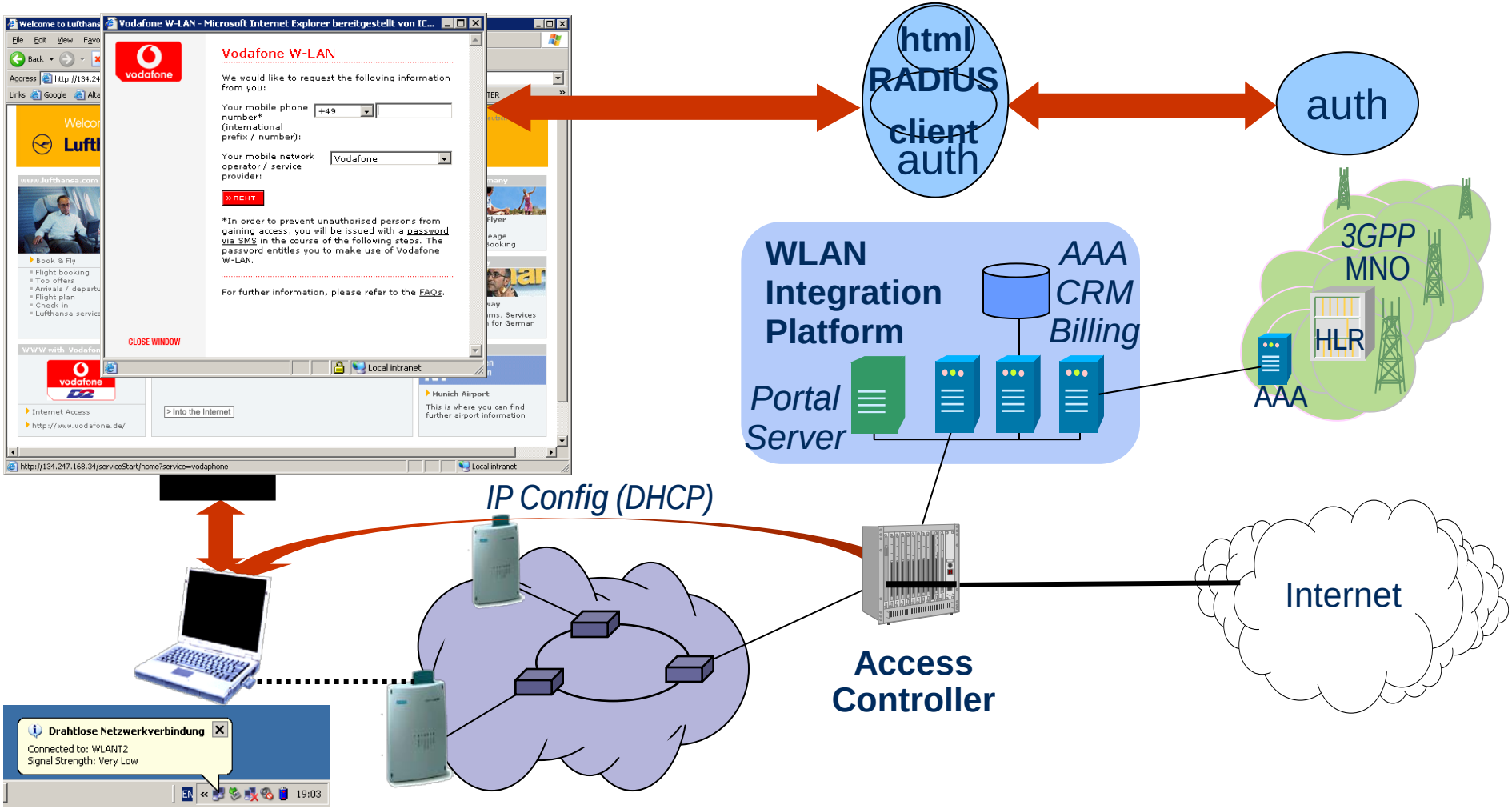
- **Password-to-Key Mapping**
  - Benutzt PKCS #5 um einen 256-bit PSK aus einem ASCII Passwort zu generieren
  - Hintergrund: Menschen geben Passwörter ein, aber 256 bit lange kryptographische Schlüssel sind etwas für Maschinen

WPA2-Enterprise
(auch bekannt unter WPA2-EAP)



AKTUELLE TECHNIK BEIM ÖFFENTLICHEN WLAN ZUGANG

Immer noch Stand der Technik: Web-Portalseiten als Zugangskontrolle

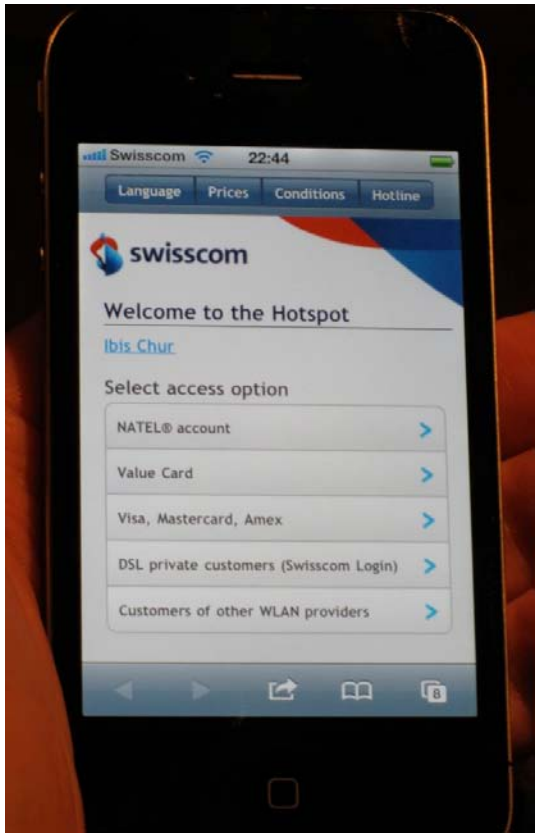


Betriebliche Schwächen beim öffentlichen WLAN Zugang

- **Login-Prozess zum Aufbau der Internet-Verbindung**
  - Zuerst Start des Web-Browsers und Aufruf einer Seite notwendig, bevor irgend ein anderes Programm mit Internet-Zugriff gestartet werden kann
    - Problematisch insbesondere bei Smartphones mit vielen ‘Apps’
- **Umleitung des Aufrufs einer Web-Seite**
  - Viele, wirklich viele Fehlermöglichkeiten…
- **Keine Rückmeldung zu Verbindungsfehlern**
  - Keine direkte Unterscheidung zwischen Verbindungsfehlern und dem Ablauf eines Zeit-Budgets
    - WLAN und Autokonfiguration o.k. obwohl Verbindung fehlgeschlagen
- **Auswahl des WLANs bei mehreren Hotspots am Ort**
  - Kein Hinweis, was sich hinter einem WLAN Namen (SSID) befindet, und welche SSID wirklich zu einem öffentlich zugänglichen WLAN Zugang führt.
- **Unterstützung von Roaming Szenarien**
  - Fehlender Hinweis auf die mögliche Unterstützung eines existierenden Benutzer-Accounts

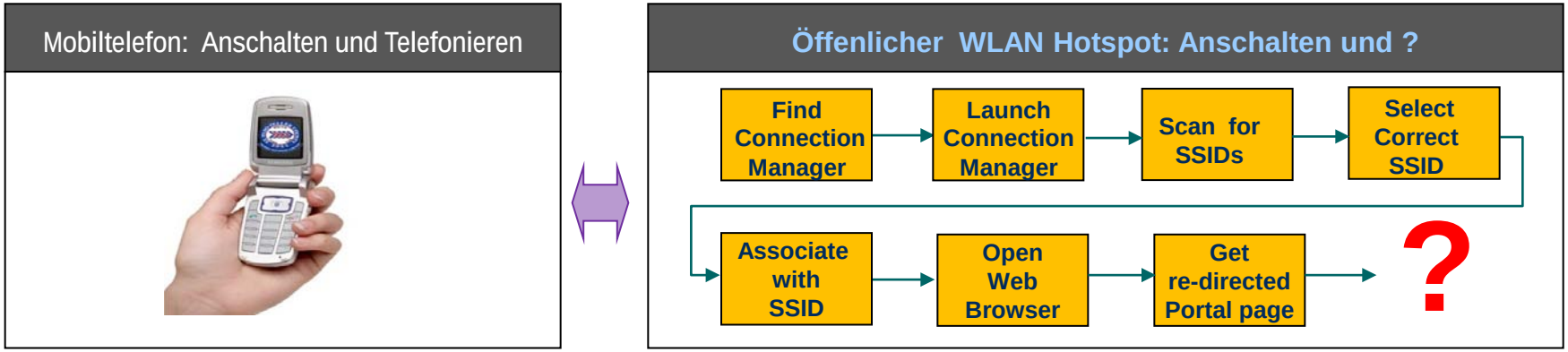
Sicherheitsprobleme beim öffentlichen WLAN Zugang

- **Evil twin attack (Betrug)**
  - Ein Angreifer verwendet die gleiche SSID um einen Access Point zu fälschen und so an geheime Informationen (Account-Daten, Bezahlinformationen) zu kommen.
- **Denial-of-service attack (Sabotage)**
  - Ein Angreifer wirft einen angemeldeten WLAN Teilnehmer aus dem Hotspot indem er eine gefälschte 'Disassociate' Message schickt,
- **Session hi-jacking (Diebstahl)**
  - Ein Angreifer übernimmt eine laufende WLAN Verbindung indem er die MAC Adresse des Teilnehmer fälscht und gleichzeitig den Teilnehmer vorspielt, dass er vom WLAN abgemeldet ist.
- **Eavesdropping (Spionage)**
  - Ein Angreifer lauscht die unverschlüsselte Kommunikation eines angemeldeten WLAN Hotspot Teilnehmers mit und bringt vertrauliche Daten in Erfahrung.



DIE HOTSPOT 2.0 INITIATIVE DER WI-FI ALLIANCE

Die Verbesserung des öffentlichen WLAN Zugangs ist gar nicht so schwer.



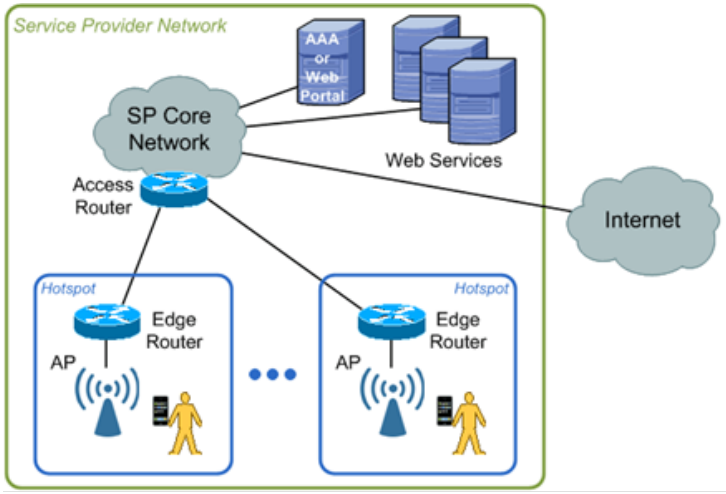
- **Was bereits existiert:**
  - die passende Sicherheitstechnik auf der Luftschnittstelle: WPA2-Enterprise
    - durch die Anwendung in Unternehmensnetzen seit Jahren weit verbreitet
  - Unterstützung von passenden EAP Methoden in Terminals
    - EAP-SIM/EAP-TLS/EAP-TTLS werden nahezu auf jedem System unterstützt
  - Automatischer WLAN-Verbindungsaufbau zu bekannten WLAN Netzen
    - Jedes Betriebssystem kennt eine priorisierte WLAN Auswahlliste
  - Standard für eine bessere WLAN Netzsignalisierung und Auswahl: IEEE802.11u
- **Was fehlt:**
  - Systemspezifikation für den öffentlichen WLAN Zugang mit WPA2-Enterprise
  - IEEE802.11u Unterstützung in den WLAN Treibern (Wi-Fi Certification Program)

Am Horizont: ‘Wi-Fi CERTIFIED Passpoint’

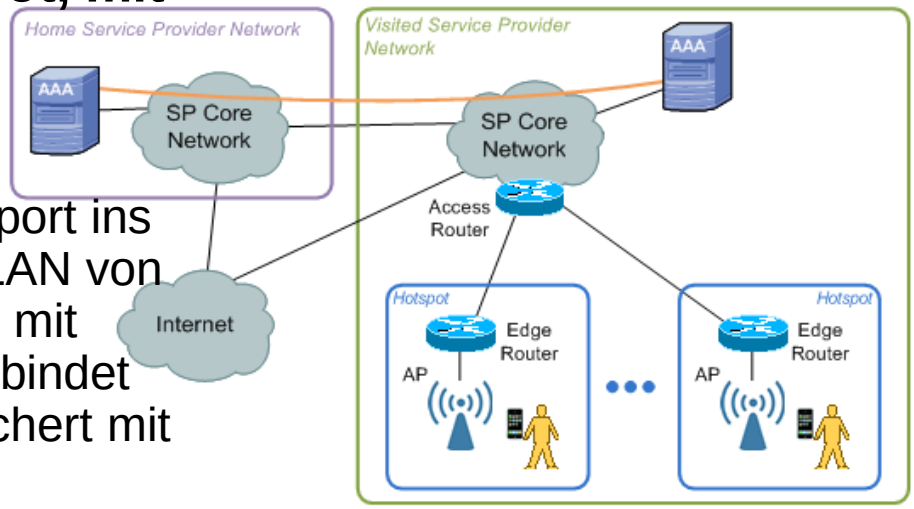
- **Die Wi-Fi Alliance arbeitet an der Systemspezifikation für den automatischen und gesicherten öffentlichen WLAN Zugang**
  - Hotspot 2.0
- **Es ist geplant, bis zum 3. Quartal 2012 das ‘Wi-Fi CERTIFIED Passpoint’ Zertifizierungsprogramm zur Verbreitung des Hotspot 2.0 Zugangsverfahren einzuführen.**
- **Kernkomponenten des Hotspot 2.0 Verfahrens:**
  - Verbesserte WLAN Netzauswahlverfahren mit Anzeige der potentiellern Roaming-Partner eines WLAN Zugangs
  - Gesicherter WLAN Zugang mit WPA2-Enterprise
  - Standard für die gesicherte Einrichtung eines neuen Accounts direkt am WLAN Hotspot (Online Signup Procedure)
    - Ersatz für die derzeitigen Portalseiten
  - Standardisierte Verfahren für die automatische Konfiguration von Betriebs- und Zugangsparametern für öffentliche WLAN Zugänge.

Nutzungs-Szenarien von Hotspot 2.0

- **Automatischer Zugang zu den WLAN Hotspots des lokalen Breitbandbetreibers, mit dem man einen Servicevertrag hat.**
  - Hans, ein Kunde von Wondertels DSL Service ist am Bahnhof. Er möchte mit seinem Notebook im Internet surfen. Das Notebook findet automatisch Wondertel's Hotspot und verbindet sich gesichert mit dem WLAN.

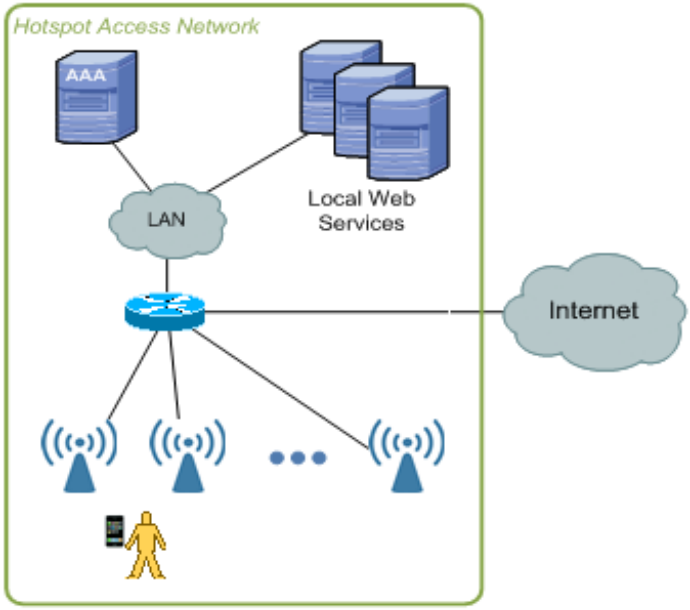


- **Gesicherter Zugang zu einem Hotspot, mit dem der lokale Breitbandbetreiber ein Roaming- Abkommen hat.**
  - Karl, der einen Vertrag mit Wondertel in Nürnberg hat, möchte am Londoner Airport ins Internet. Das Smartphone findet das WLAN von Fantastitel, die ein Roaming Abkommen mit Wondertel haben. Nach Bestätigung verbindet sich das Smartphone automatisch gesichert mit dem WLAN Hotspot in London.



Hotspot 2.0 Nutzungs-Szenarien, Forts.

- **Offload von Mobilfunk-Traffic im Heimbereich**
  - Kurt möchte das Fußballspiel seines Heimatvereins in Ruhe auf seinem Smartphone zu Ende sehen können, da seine Kinder den heimischen Fernseher beanspruchen. Gerade wenn Fußballspiele stattfinden ist häufig das Mobilfunknetz überlastet. Von der Wohnung ist ein WLAN Zugang erreichbar, der vom Mobilfunkbetreiber oder in Absprache von einem anderen Dienstleister betrieben wird, und der die Mobilfunkdaten über WLAN ableitet.
- **Nutzung eines Hotspots nach Annahme der Bedingungen**
  - Brigitte wartet am Flughafen auf den Aufruf ihres Flugs und möchte vorher nochmal kurz ihre email abrufen. Ihr Notebook findet einen kostenlosen WLAN Zugang, der aber vor der Benutzung die Zustimmung zu den Benutzungsrichtlinien verlangt. Das Notebook stellt die Benutzungsrichtlinien dar und verbindet sich nach Annahme gesichert mit dem WLAN Zugang. Beim nächsten Mal erkennt der WLAN Hotspot automatisch, dass Brigitte die Nutzungsrichtlinien bereits akzeptiert hat und erlaubt ihr den gesicherten Zugang ohne weitere Zustimmung.

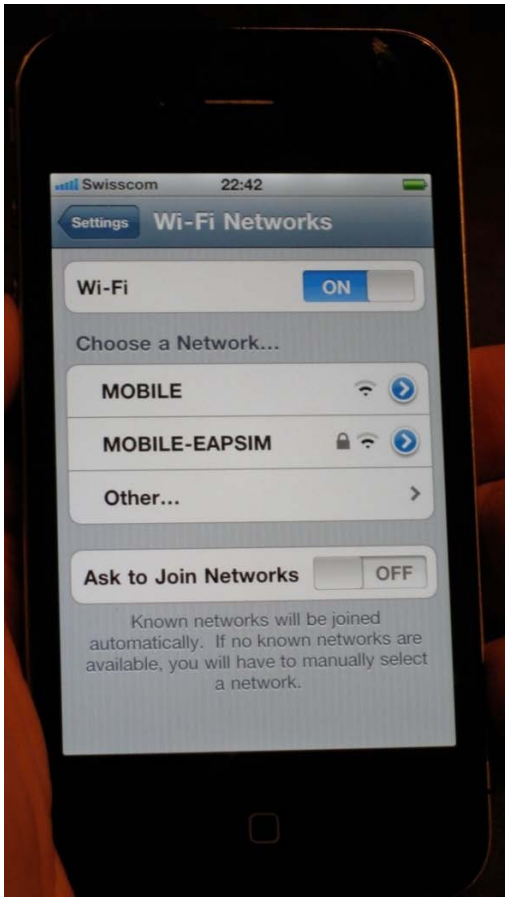


Hotspot 2.0 Nutzungs-Szenarien, Forts.

- **Nutzung eines öffentlichen Hotspots ohne existierenden Vertrag**
  - Yvonne kommt abends in ihrem Hotel an und möchte ihre email abrufen. Ihr Notebook zeigt ihr nach dem Start automatisch an, dass es in dem Hotel einen kostenpflichtigen WLAN Zugang gibt. Sie wählt das WLAN aus und ihr wird automatisch eine Seite angezeigt, auf der sie die Dauer des Zugangs und die Bezahlungsmodalitäten eingeben kann. Nach der Eingabe der Daten verbindet sich ihr Notebook automatisch gesichert mit dem Hotel WLAN.
- **Benutzer-Information über ein bevorstehendes Ende der Session**
  - Yvonne benutzt den öffentlichen WLAN Zugang in einem Hotel um eine Präsentation fertigzustellen, zu der sie Zugang zum Internet benötigt. Sie hat sich dafür einen Zugang für eine Stunde gekauft. 5 Minuten vor Ablauf der Nutzungszeit öffnet sich auf ihrem Bildschirm ein Informationsfenster, auf dem das nahe Ende der Session angezeigt und die Möglichkeit zur Verlängerung angeboten wird.
- **Information über die Verfügbarkeit eines Hotspot 2.0 WLAN Zugangs**
  - Josef ist viel unterwegs und legt Wert auf den Komfort und die Sicherheit von Hotspot 2.0 WLAN Zugängen. Immer wenn er im Einzugsbereich eines Hotspot 2.0 WLAN Zugangs sein Notebook öffnet, wird ihm die Existenz des Hotspot 2.0 Zugangs angezeigt.

Nicht jedes der Nutzungs-Szenarien benötigt volle Hotspot 2.0 Funktionalität

- **Heute bereits möglich mit existierenden Accounts**
  - Automatischer Zugang zu den WLAN Hotspots des lokalen Breitbandbetreibers, mit dem man einen Servicevertrag hat.
  - Offload von Mobilfunk-Traffic im Heimbereich
- **Benötigt zumindest IEEE802.11u Unterstützung**
  - Information über die Verfügbarkeit eines Hotspot 2.0 WLAN Zugangs
  - Benutzer-Information über ein bevorstehendes Ende der Session
  - Gesicherter Zugang zu einem Hotspot, mit dem der lokale Breitbandbetreiber ein Roaming- Abkommen hat.
- **Benötigt zusätzlich die Online Signup Prozeduren**
  - Nutzung eines Hotspots nach Annahme der Bedingungen
  - Nutzung eines öffentlichen Hotspots ohne existierenden Vertrag



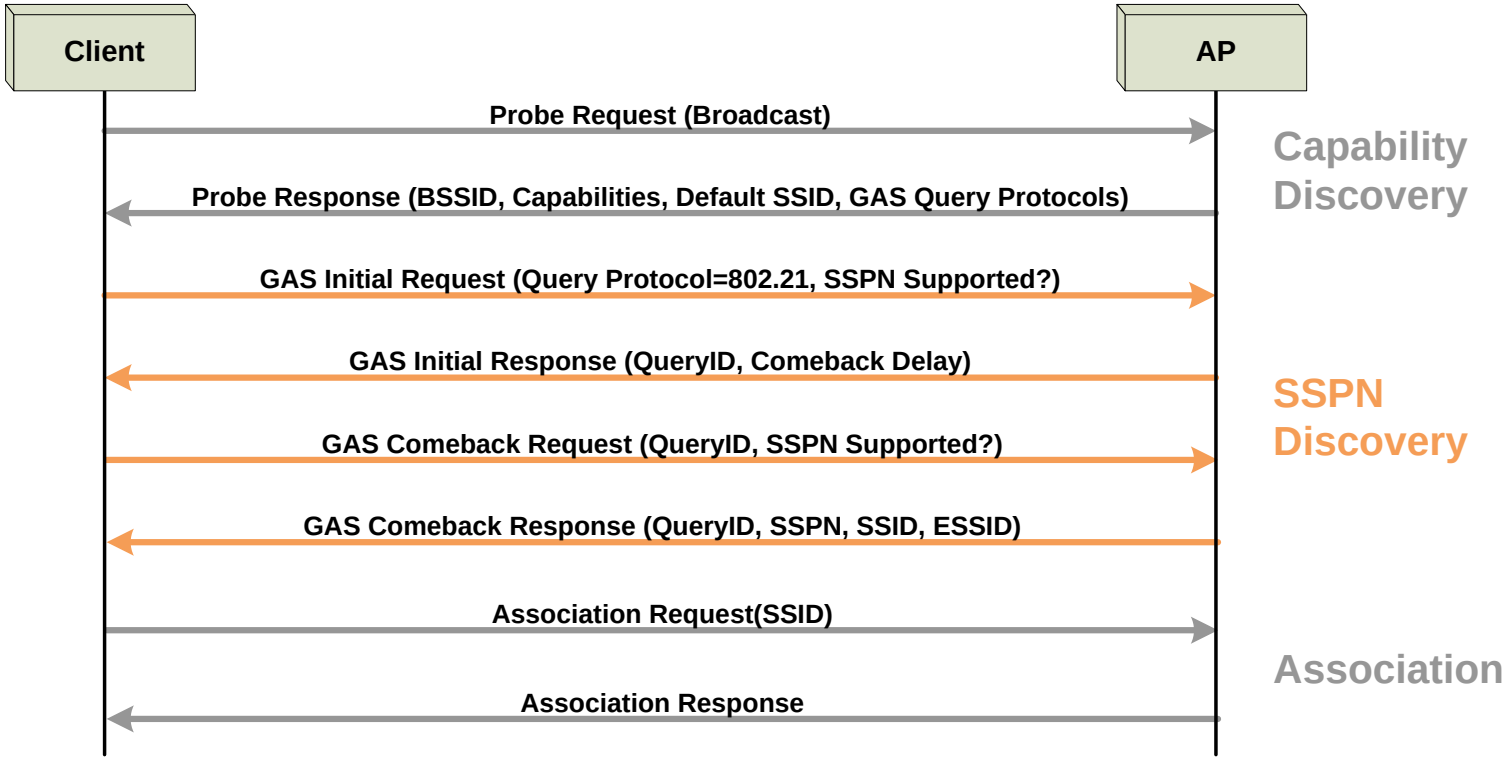
DIE IEEE802.11U ERWEITERUNG DES WLAN STANDARDS

Die IEEE802.11u Erweiterung

- **Die '*IEEE P802.11u-2011, Amendment 9: Interworking with External Networks*' Spezifikation erweitert den IEEE802.11 WLAN Standard mit einer Anzahl von neuen Funktionen, die speziell im öffentlichen Umfeld wichtig sind:**
  - Externes Netzwerk Interface ("SSPN") für die erweiterte Konfiguration
  - Erweiterte QoS Signalisierung
  - Generic Advertising Service (GAS)
  - Empfehlungen für den Notruf über WLAN (bei Voice over WLAN)
- **Hotspot 2.0 nutzt nur einen (kleinen) Teil der IEEE802.11u Möglichkeiten für**
  - Unterstützung bei der Netzauswahl
  - Signalisierung der Funktionalität vor dem Verbindungsaufbau
- **Die Wi-Fi Alliance definiert in der Hotspot 2.0 Spezifikation die Benutzung und Erweiterung von IEEE802.11u Informationselementen**

Generic Advertising Services (GAS)

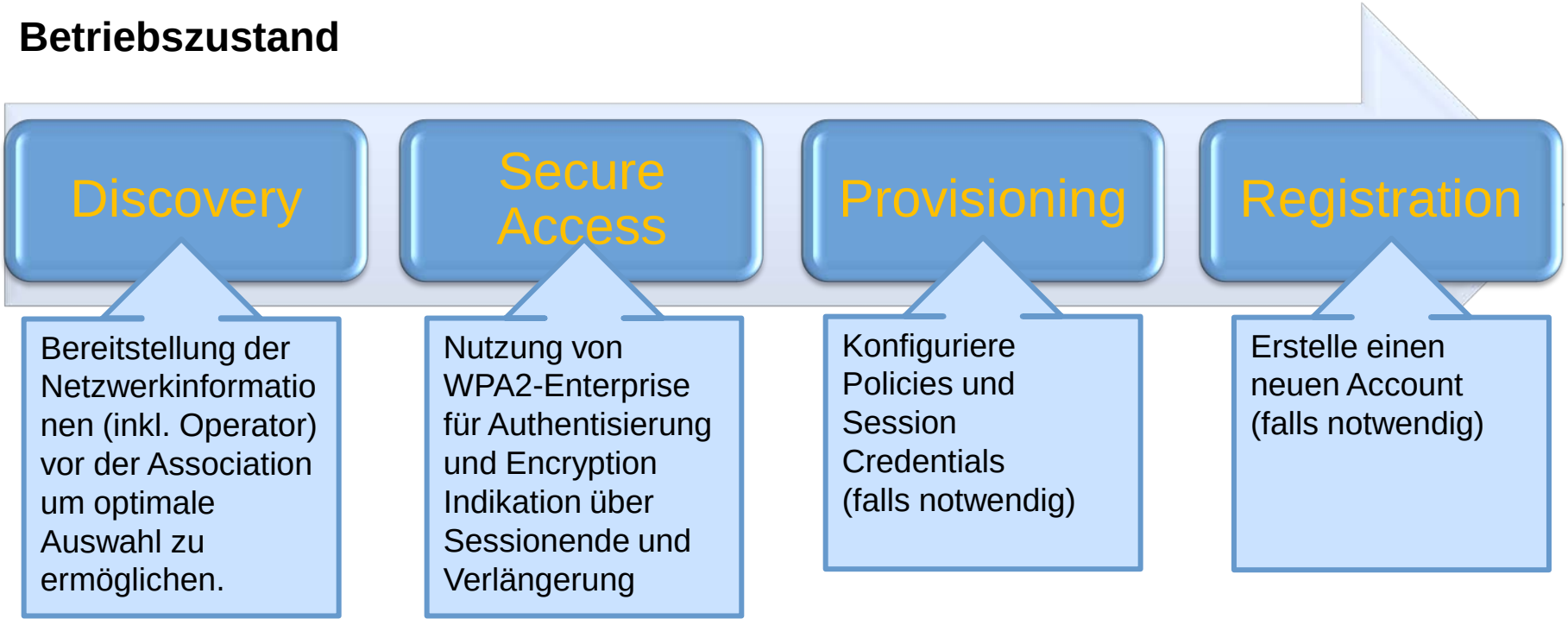
- **Natives Abfrage Protokol:**
  - Wird für die Bereitstellung von Layer 2+ Informationen an das Terminal verwendet
  - Informationen nur auf Verlangen, daher kein Aufblähen des Beacons
  - Multicast oder Unicast Verteilung
  - Wird vom Access Point realisiert (nicht durch einen zusätzlichen Server)



TECHNISCHE KOMPONENTEN DER HOTSPOT 2.0 LÖSUNG

Der Umfang von Hotspot 2.0

Betriebszustand



Technische Elemente Zertifizierung

802.11u Elements WPA2 Enterprise

Operator Policy

Online Signup

Discovery

Hotspot 2.0 capable AP Beacons and Probe Response frame include:

- RSN IE(WPA2)
- Interworking Element (includes HESSID and Venue Information)
- Advertisement Protocol Element (Indicates ANQP)
- Roaming Consortium Element(A list of roaming consortium identifier)
- The Hotspot 2.0 Indication element

Hotspot 2.0 capable STAs scan for networks and discover an AP advertising Hotspot 2.0 capability.

Hotspot 2.0 capable STA uses ANQP to the AP to determine properties of the Hotspot 2.0 Access Network. The Hotspot capable STA selects the ANQP query elements it requires to query the Hotspot 2.0 network for Interworking Service information.

GAS Initial Request Frame(Advertisement Protocol = ANQP;
ANQP Query = {Venue Name, Network Auth, Roaming Consortium, IP Address Type, NAI Realm, 3GPP Cellular information, Domain Name; Operator Friendly Name, WAN Metrics, Connection Capability})

→

GAS Initial Response Frame(Advertisement Protocol = ANQP;
Venue Name; Network Auth; Roaming Consortium; IP Address Type; NAI Realm; 3GPP Cellular information; Domain Name; Operator Friendly Name,; WAN Metrics; Connection Capability)

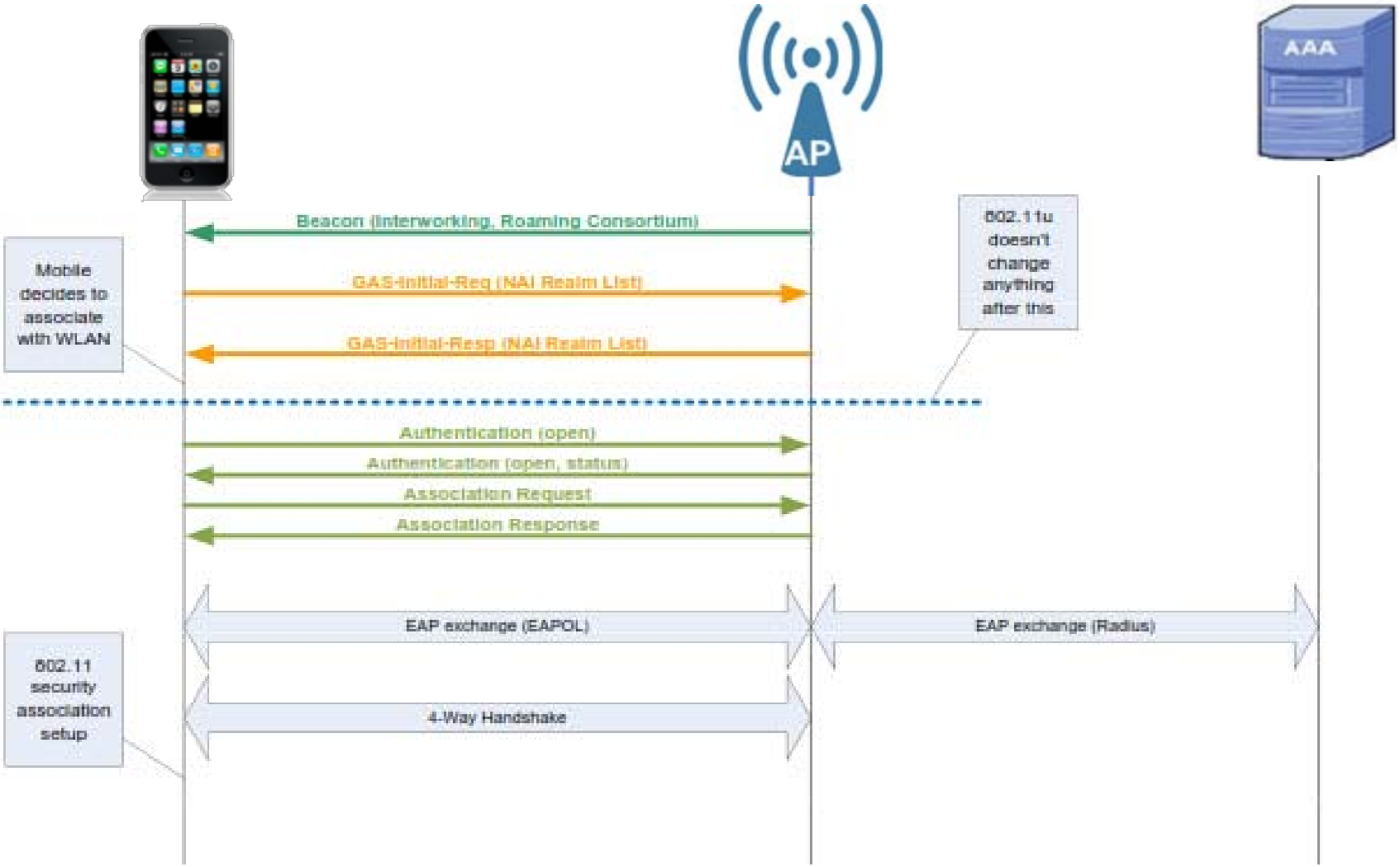
←

Hotspot 2.0 capable STA evaluates the response based on its Hotspot 2.0 subscription information and associated policy and choose to associate to the AP.
NOTE SSID is not necessary to make the network selection.

Associate and WPA2 EAP Authentication ↔

Secure WPA2 Data Connectivity ↔

Association



Secure Access

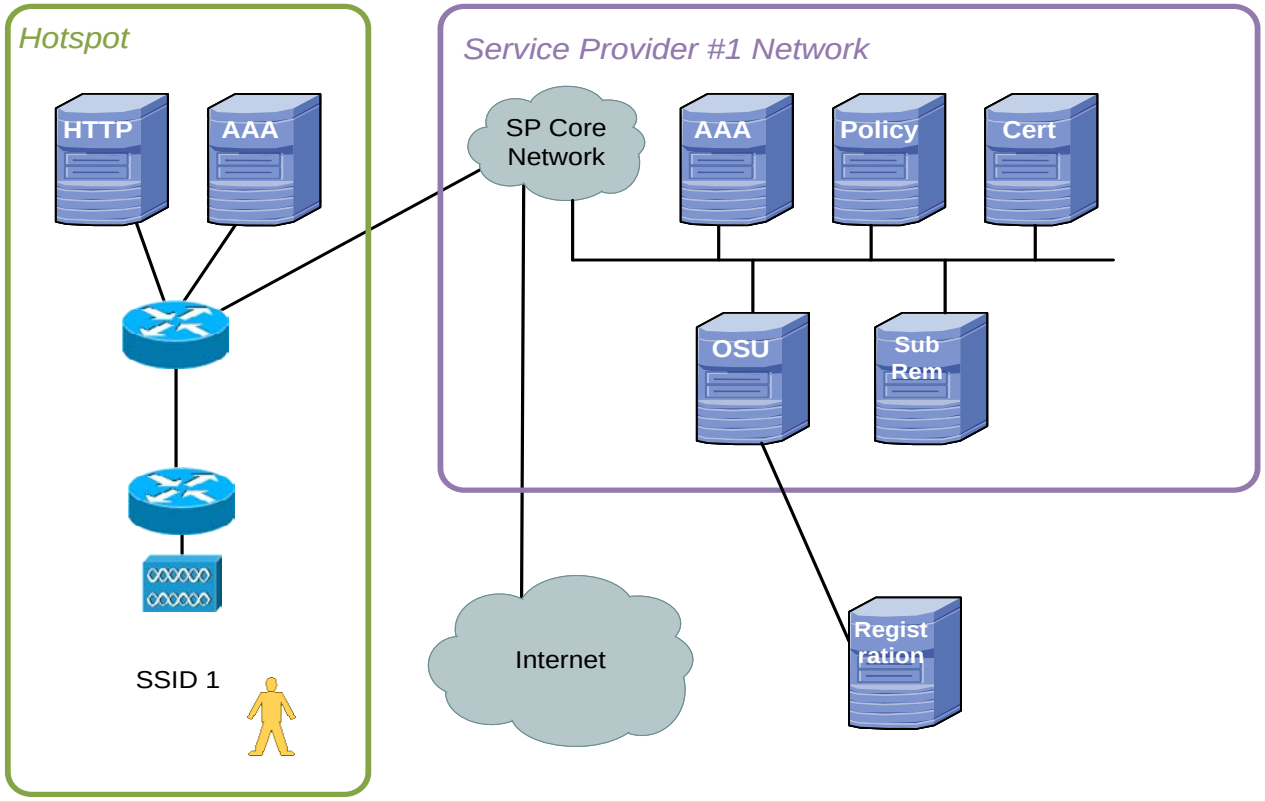
- **Hotspot 2.0 ist gesichert durch WPA2-Enterprise**
  - Folgende Authentisierungsmethoden werden unterstützt:

Credential Type	EAP Method
Certificate	EAP-TLS
SIM/USIM	EAP-SIM , EAP-AKA
Username/Password	EAP-TTLS mit MSCHAPv2

    - Ein Hotspot-Betreiber ohne SIM Infrastruktur soll zumindest Certificate oder Username/Passwort unterstützen
    - Ein Hotspot-Betreiber mit SIM Infrastruktur soll zumindest auch Certificate oder Username/Passwort unterstützen
    - Alle Hotspot-Betreiber sollen die aufgeführten EAP Methoden als ausreichend für den Zugang zum WLAN akzeptieren.
- **Layer 2 Traffic Inspektion und Filterung**
  - Hotspot 2.0 überwacht und filtert den Traffic, der an die Terminals ausgeliefert wird. Die Traffic-Überwachung soll einen gewissen Schutz vor Angriffen bieten.
    - Keine ungeprüfte Auslieferung von Daten innerhalb eines Access Points
    - Keine ungeprüfte Auslieferung von Daten über benachbarte Access Points
    - Wenn der Access Point selber keine Überwachungsfunktionen hat, soll der gesamte Traffic über die Ethernet-Schnittstelle in das Netzwerk weitergegeben werden

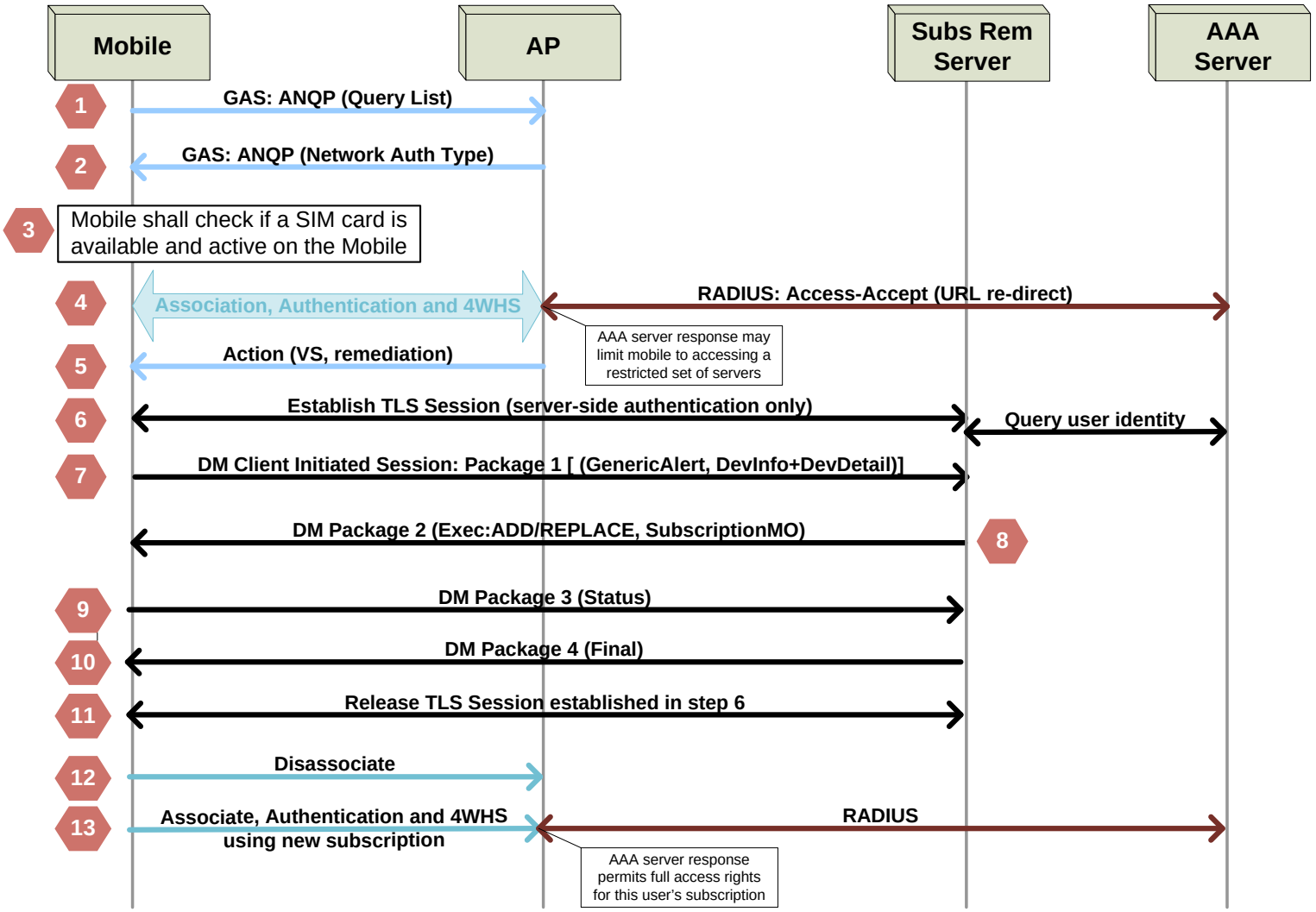
Provisioning

- **Die Provisionierung einer Subscription umfasst Credentials und dazugehörige Metainformation, Policies und Information über den Home Service Provider**
- **Provisioning benötigt umfangreiche Einrichtungen im Netz eines Service Provider :**



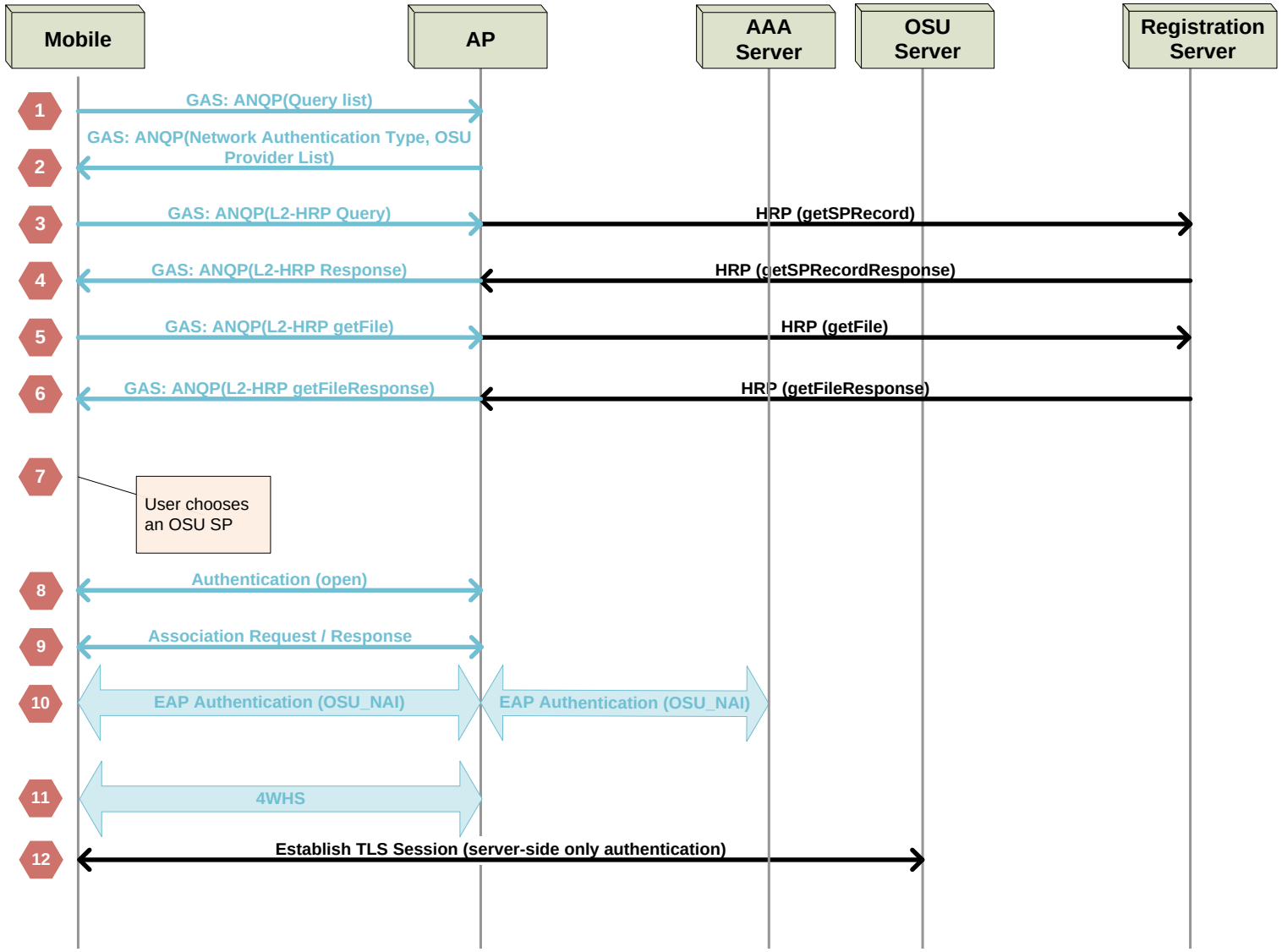
Die 4 nicht mit "AAA" markierten Server werden als "Subscription Server" bezeichnet

Provisioning mit OMA DM (mit SIM Card)



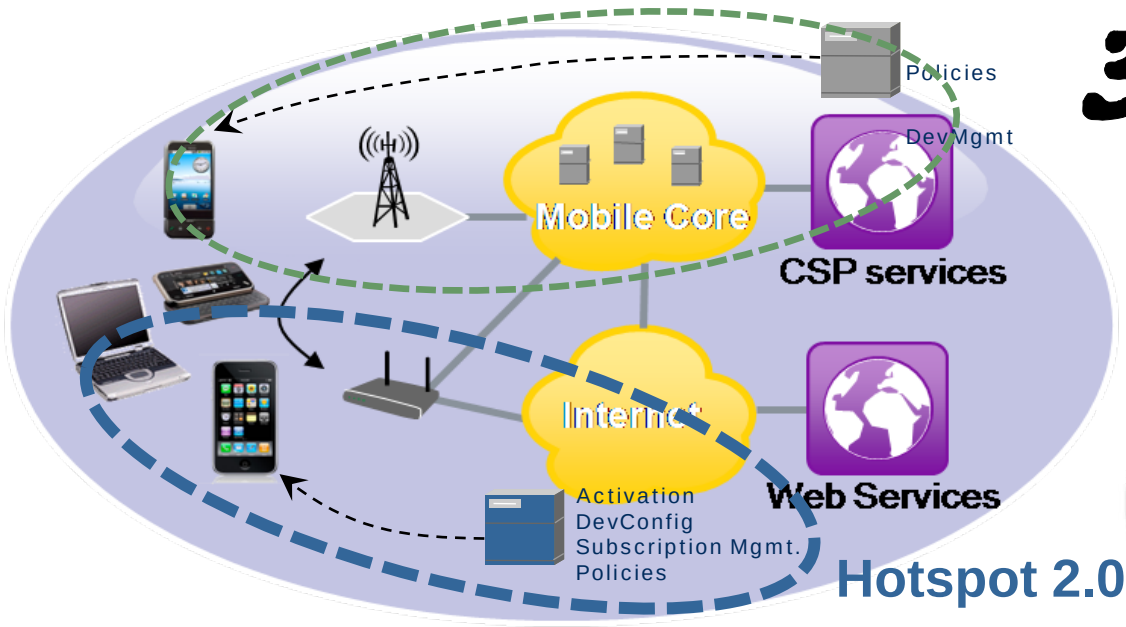
Registration

Online Sign-Up Process (over the air)



ZUSAMMENFASSUNG UND AUSBLICK

Hotspot 2.0 bildet die Basis für den gesicherten öffentlichen WLAN Zugang



- **Verbesserte WLAN Hotspot Erkennung und Auswahl mit IEEE802.11u**
  - Generic Advertisement Service (GAS) für den Layer 2 Transport von Information zwischen AP und Mobile Device vor der Authentisierung
  - Access Network Query Protocol zum Austausch von Informationen über die Funktion udn Art des WLAN Zugangs vor dem Aufbau der Verbindung
- **Online Sign-Up Prozeduren für den Fall dass die passenden Credential fehlen**
  - Erstellung einer neuen Subscription direkt im WLAN Hotspot
  - Annahme der Benutzerbedingungen für einen WLAN Hotspot
- **... auf der Basis von RSN (Robust Security Network) aka WPA2-Enterprise**

BTW: IEEE802.11 (Wi-Fi) Radio Standards

Std	Release	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range (m)	Approximate outdoor range (m)
	Jun 1997	2.4	20	1, 2	1	DSSS	30	120
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	30	120
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	40	140
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM (DSSS)	40	140
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2[X]	4	OFDM	70	250
			40	15, 30, 45, 60, 90, 120, 135, 150[X]			70	250
y	Nov 2008	3.7	5/10/20	Up to 13.5/27/54	1	OFDM		5 000
ac	~ 2013	5	20/40/ 80/160	tbd (up to 867)*	8*	OFDM	40*	140*
ad	~ 2012	60	~ 2000*	tbd (up to 6 700)*	1		Single room	-
af	~ 2013	TV WS	5/10/20	tbd (up to 75)*	tbd	OFDM	200*	1000*
ah	~ 2014	< 1	2.5/5/10/20	tbd (up to 100)*	tbd	OFDM	200*	1000*

[X]Assumes short guard interval (SGI) enabled, otherwise reduce each data rate by 10%.
* Preliminary information; specifications still in early phases of development.
IEEE 802.11y-2008 is only licensed in the United States by the FCC; licensed spectrum allows for higher TX power