دليل عمليات ونشر OmniTWAG

أنشأه Omnitouch

هذا الدليل مخصص لمشغلي الشبكات، ومديري الأنظمة، والعملاء الذين يقومون بنشر OmniTWAG.

جدول المحتويات

مقدمة

OmniTWAG (بوابة الوصول الموثوقة لشبكة WiFi) 3 هو تنفيذ متوافق مع المعايير لـ 3GPP TWAG ا��ذي يمكّن مشغلي الشبكات المحمولة من تحميل حركة مرور المشتركين من الشبكات الخلوية إلى نقاط الوصول لشبكة WiFi على المصادقة الآمنة المعتمدة على SIM.

يقوم TWAG بمصادقة مشتركي WiFi باستخدام بيانات اعتماد SIM عبر EAP-AKA الخاصة بهم، وهو نفس آلية المصادقة (بروتوكول المصادقة القابل للتوسيع - المصادقة واتفاقية المفتاح) المستخدمة في الشبكات الخلوية. وهذا يوفر وصولاً سلسًا وآمنًا لشبكة WiFi منفصلة للمشتركين المتنقلين دون الحاجة إلى كلمات مرور.

الفوائد الرئيسية

للمستخدمين النهائيين:

- **عدم وجود تكوين**: يعمل مباشرة مع متوافق SIM
- **تجربة سلسة**: اتصال تلقائي مثل الشبكات الخلوية
- **آمن**: يستخدم دائمًا WiFi مشفر (WPA2)
- **لا كلمات مرور**: مصادقة تعتمد على SIM

لمشغلي الشبكات المحمولة:

- **تخفيف سعة الشبكة**: يقلل الحمل على محطات القاعدة الخلوية
- **تحم��ل متحكم فيه**: يمكن فقط للمشتركين المصرح لهم الاتصال
- **تحسين تجربة المستخدم**: توفر عادةً عرض نطاق ترددي أعلى WiFi
- **كفاءة التكلفة**: بنية التحتية أقل تكلفة من الخلوية WiFi
- **هوية متسقة**: نفس والخلوية WiFi المستخدمة لـ IMSI
- **تكامل الفوترة**: إذا رغبت WiFi يمكن شحن استخدام

للمواقع/الشركات:

- **أمان على مستوى المشغل**: لا خطر من مشاركة كلمات المرور
- **قابلية التوسع**: دعم لآلاف المستخدمين دون توفير يدوي
- **إدارة مبسطة**: لا حاجة لتوزيع كلمات مرور WiFi

ما هو تحميل WiFi؟

يسمح تحميل WiFi لمشغلي الشبكات المحمولة بإعادة توجيه حركة بيانات المشتركين من الشبكات الخلوية المزدحمة إلى شبكات WiFi.

التحميل TWAG كيف يمكّن

يعمل TWAG كبوابة المصادقة بين:

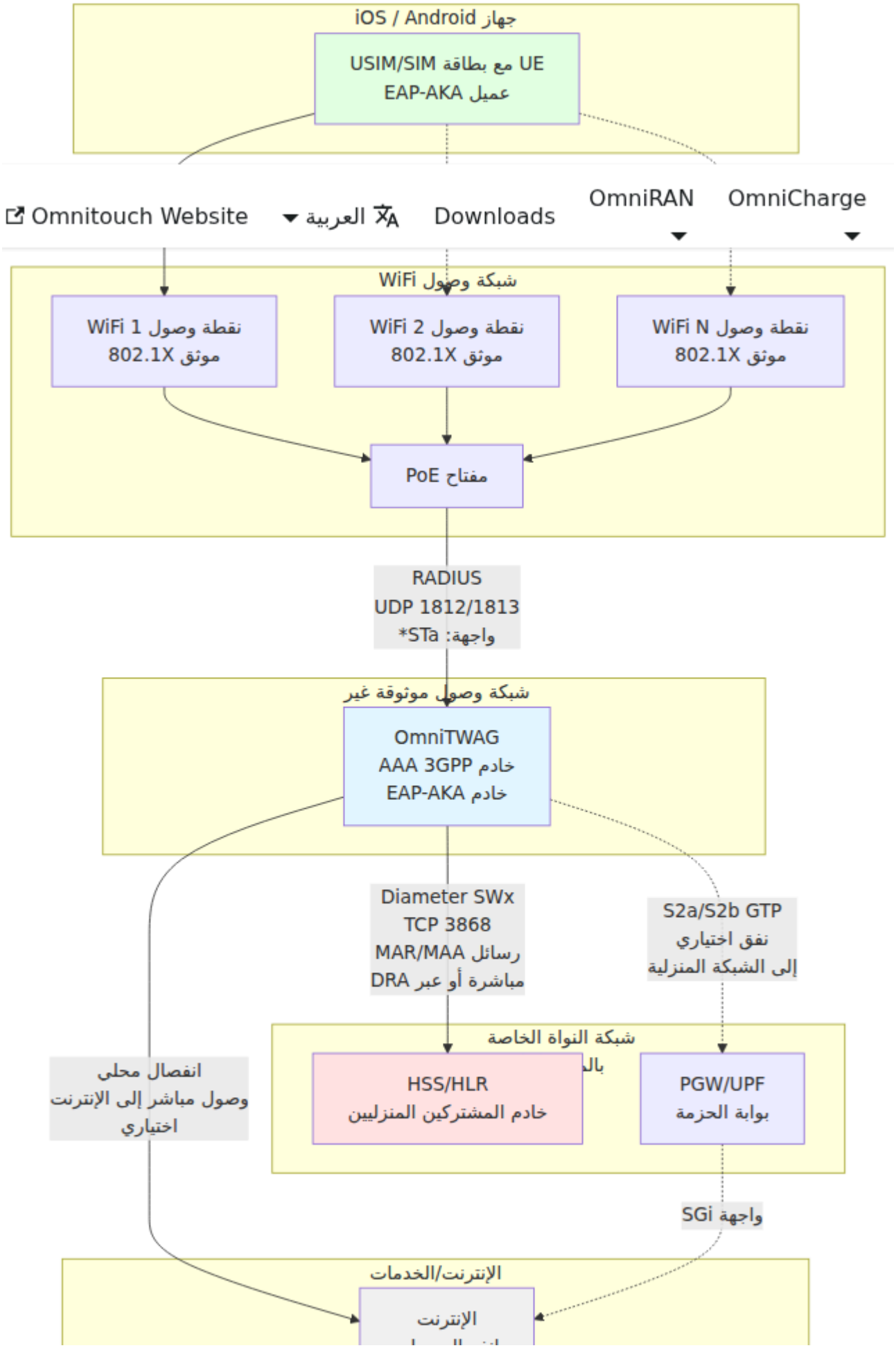
- **نقاط وصول WiFi** (عبر بروتوكول RADIUS)
- **شبكة النواة المحمولة** HSS/HLR (عبر واجهة Diameter SWx)

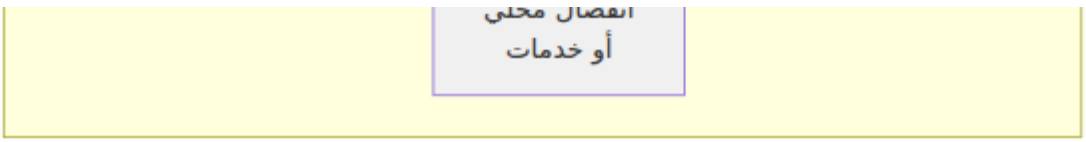
تم تكوينها للتحميل WiFi عندما يتصل جهاز المشترك بنقطة وصول:

1. يتعرف الجهاز على نفسه باستخدام IMSI الخاص به (من بطاقة SIM)
2. تقوم نقطة وصول WiFi بإرسال طلبات المصادقة إلى TWAG عبر RADIUS
3. يتواصل TWAG مع HSS الخاص بالمشغل لاسترجاع متجهات المصادقة
4. تحدث مصادقة التحدي-الاستجابة EAP-AKA بين الجهاز وTWAG
5. عند المصادقة الناجحة، يُمنح الجهاز وصول WiFi
6. اختياريًا، يمكن أن يتم توجيه الحركة مرة أخرى إلى النواة المحمولة أو الانفصال محليًا

معمارية النشر

طوبولوجيا الشبكة


جهاز iOS / Android
UE مع بطاقة USIM/SIM
عميل EAP-AKA
Omnitouch Website
العربية
Downloads
OmniRAN
OmniCharge
شبكة وصول WiFi
نقطة وصول WiFi 1
موثق 802.1X
نقطة وصول WiFi 2
موثق 802.1X
نقطة وصول WiFi N
موثق 802.1X
مفتاح PoE
RADIUS
UDP 1812/1813
واجهة: STa*
شبكة وصول موثوقة غير
OmniTWAG
خادم AAA 3GPP
خادم EAP-AKA
Diameter SWx
TCP 3868
رسائل MAR/MAA
مباشرة أو عبر DRA
S2a/S2b GTP
نفق اختياري
إلى الشبكة المنزلية
شبكة النواة الخاصة
HSS/HLR
خادم المشتركين المنزليين
PGW/UPF
بوابة الحزمة
انفصال محلي
وصول مباشر إلى الإنترنت
اختياري
واجهة SGi
الإنترنت/الخدمات
الإنترنت

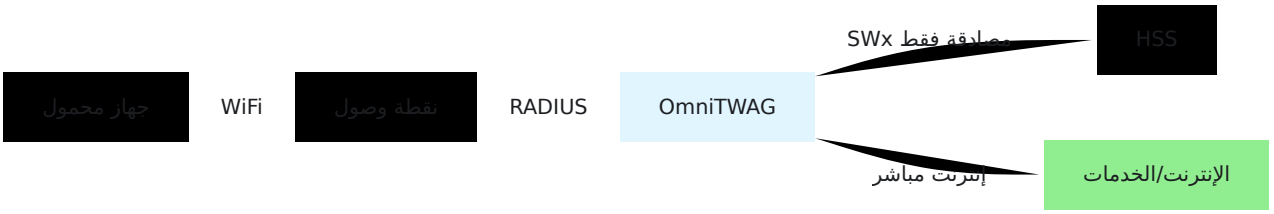


أسطورة الواجهة:

- **STa***: واجهة RADIUS/Diameter بين نقطة وصول WiFi وTWAG (3 إلى غيرGPP AAA)
- **SWx**: واجهة Diameter بين TWAG (خادم AAA 3GPP) وHSS
- **S2a/S2b**: واجهة نفق GTP (اختياري) للعودة إلى الشبكة المنزلية
- **SGi**: واجهة إلى الشبكات الخارجية لنقل البيانات (الإنترنت)
- **802.11**: واجهة راديو WiFi
- **EAPOL**: EAP عبر LAN (802.1 مصادقةX)

سيناريوهات النشر

السيناريو 1: الانفصال المحلي (موصى به للأداء)

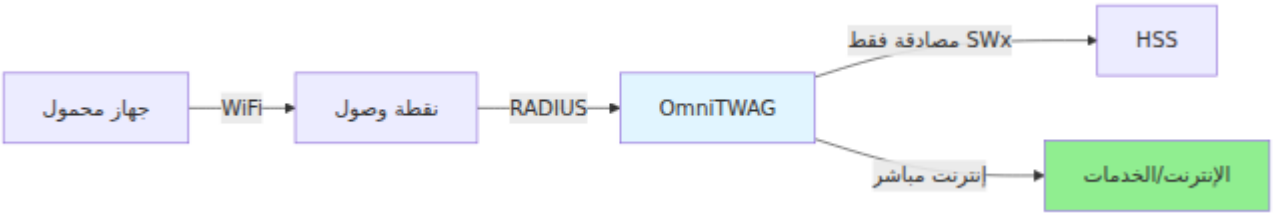


الفوائد:

- زمن انتقال أقل (لا إعادة توجيه إلى النواة)

- تقليل الحمل على الشبكة الأساسية
- تجربة أفضل للمستخدمين في التطبيقات عالية النطاق
- توفير في سعة النقل

السيناريو 2: توجيه الشبكة المنزلية (نفق GTP)



الفوائد:

- تنفيذ سياسة متسقة
- فوترة/محاسبة مركزية
- تطبيق سياسات VPN/الأمان الخاصة بالشركات
- تنقل سلس بين WiFi والخلوية

خيارات اتصال SWx

الخيار 1: اتصال مباشر بـ HSS

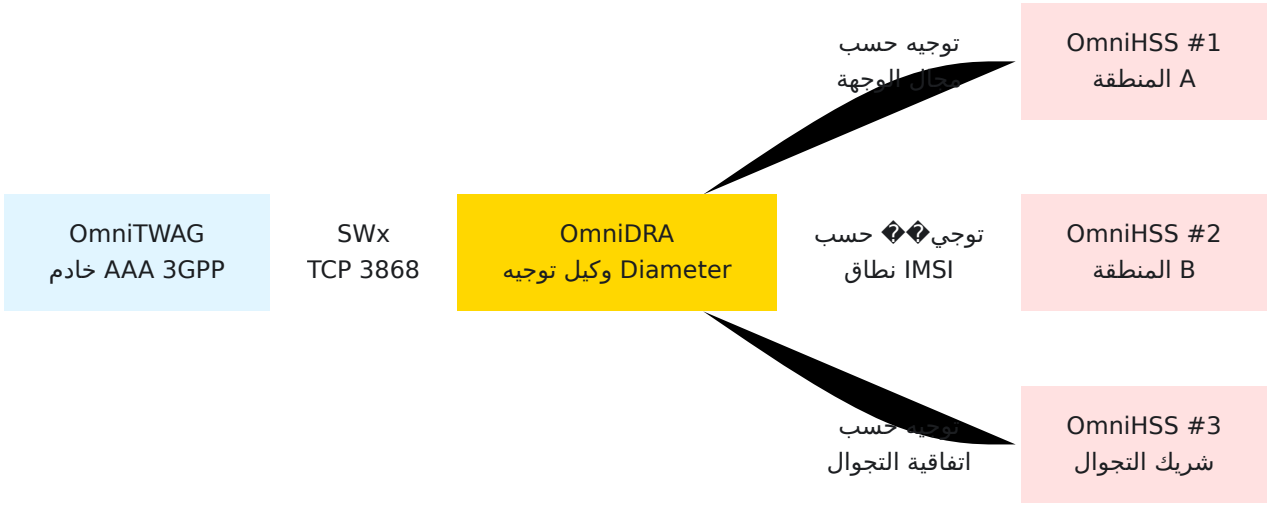
OmniTWAG خادم AAA 3GPP	SWx مباشر TCP 3868 MAR/MAA	OmniHSS قاعدة بيانات المشتركين

حالة الاستخدام: نشرات بسيطة، بيئات مختبرية، واحد HSS

الفوائد:

- زمن انتقال أقل (لا قفز عبر DRA)
- تكوين مبسط
- سهولة استكشاف الأخطاء

الخيار 2: عبر DRA (وكيل توجيه Diameter)



سيناريوهات التجوال، الشبكات الكبيرة، HSS **حالة الاستخدام**: نشرات متعددة

الفوائد:

- منطق توجيه مركزي
- توازن الحمل عبر HSS متعددة
- دعم التجوال (توجيه إلى HSS المنزلية)
- تكرار وفشل
- الالتصاق بالجلسة

تدفق الشحن

يمكن تكامل TWAG عبر Diameter `Gy` إلى نظام الشحن بالكامل لإرسال طلبات الشحن عبر الإنترنت (OCS).

يسمح ذلك بمحاسبة جميع البيانات المستهلكة على WiFi، ويتم تسليمها عبر مقابل رصيد العميل، وإعادة توجيهها إلى TWAG بواسطة `Gy` وتحويلها إلى RADIUS على AP وإعادة توجيهها إلى DRA/OCS.

في جميع الأوضاع، يتم تتبع الاستخدام بواسطة مقاييس TWAG.

أوضاع الشحن

يدعم TWAG ثلاثة أوضاع شحن عبر الإنترنت:

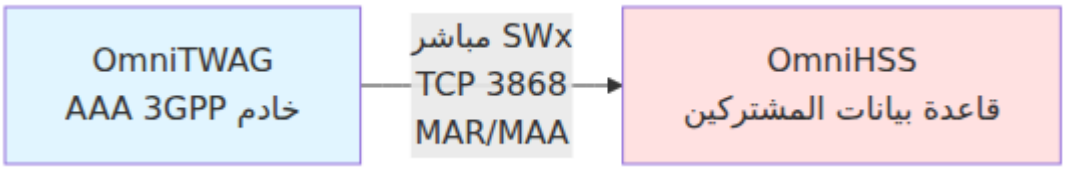
1. الشحن معطل

لا يتم إرسال طلبات التحكم في الائتمان. لا يتم إجراء تفويض للرصيد.

حالات الاستخدام:

- شبكات WiFi مفتوحة/مجانية
- بيئات مختبرية/اختبارية
- الشبكات التي تستخدم الشحن غير المتصل فقط (محاسبة RADIUS إلى الفوترة)

التدفق:



2. تفويض فقط

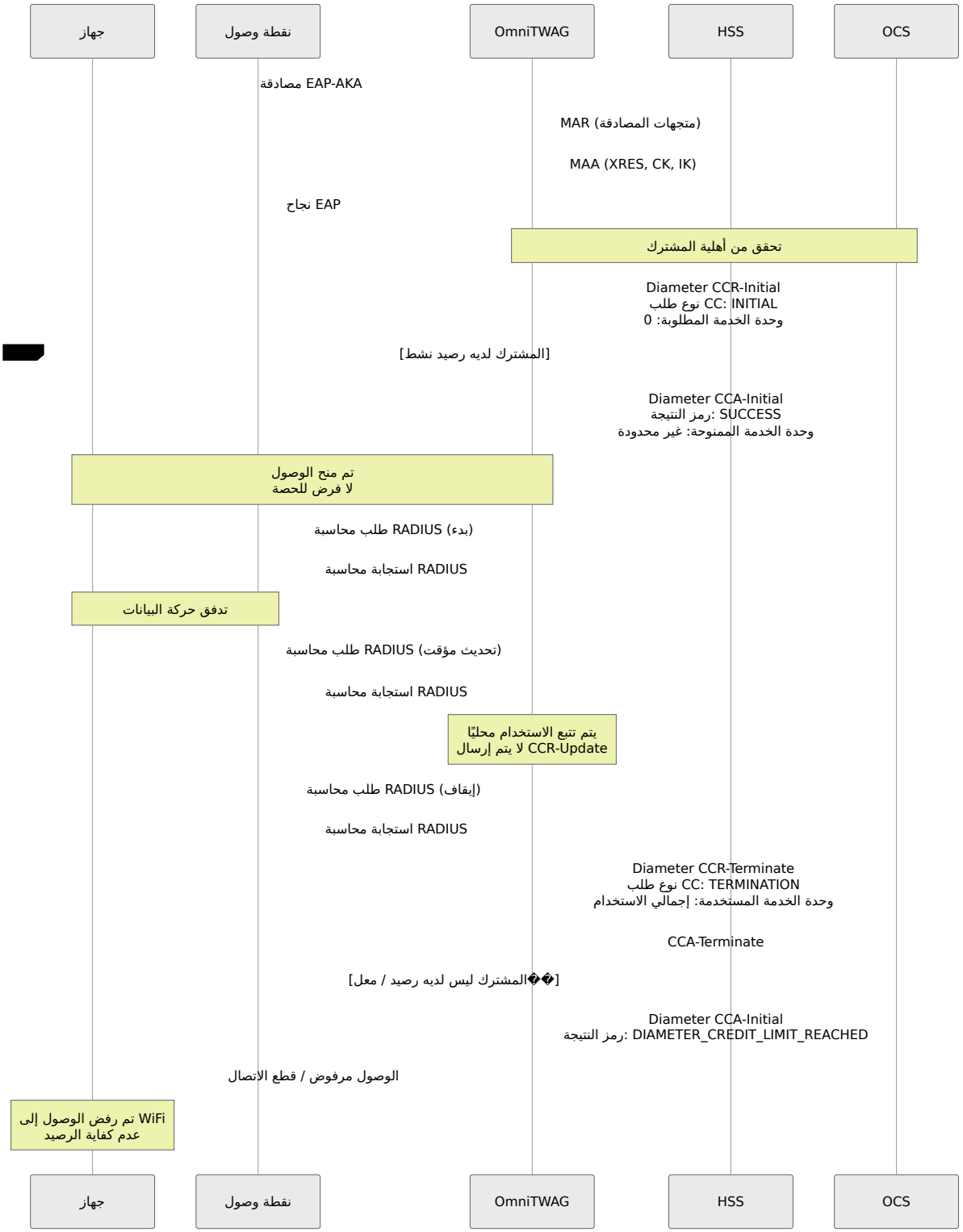
يتم إرسال CCR-Initial (طلب التحكم في الائتمان) إلى OCS في بداية جلسة WiFi للتحقق من أن المشترك لديه رصيد، ولكن لا يتم سحب الرصيد خلال الجلسة.

حالات الاستخدام:

- التحقق من أن المشترك لديه حساب/رصيد نشط

- للحسابات المعلقة WiFi منع الوصول إلى
- التحقق من أهلية الخدمة دون تتبع الحصة
- كخدمة مكافأة/غير محدودة للعملاء الذين يدفعون WiFi السماح لـ

التدفق:



التكوين:

- يتم استعلام OCS عند بدء الجلسة (CCR-I) وعند الانتهاء (CCR-T)
- لا يتم إرسال رسائل CCR-Update خلال الجلسة
- يتم تفويض المشترك بناءً على حالة الحساب، وليس الحصة
- يتم الإبلاغ عن الاستخدام في نهاية الجلسة لأغراض إعلامية فقط

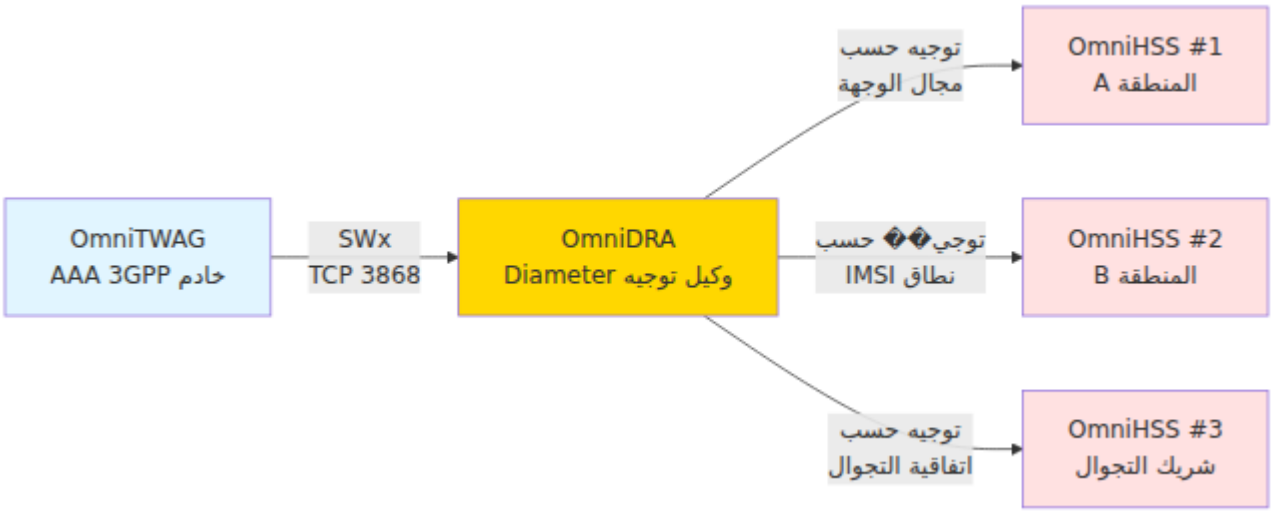
3. شحن Gy (تنفيذ كامل) عبر الإنترنت بالكامل

يتم تمرير جميع الاستخدامات على WiFi إلى 3GPP. يتم اتباع تدفق الشحن عبر الإنترنت القياسي للشحن، ويتم قطع المشترك بمجرد تجاوزهم حصتهم OCS.

حالات الاستخدام:

- خدمات البيانات المدفوعة مسبقًا
- حسب الاستخدام WiFi
- خطط قائمة على الحصة (بدل شهري GBمثل، 10)
- شحن في الوقت الحقيقي وقطع الاتصال

التدفق:



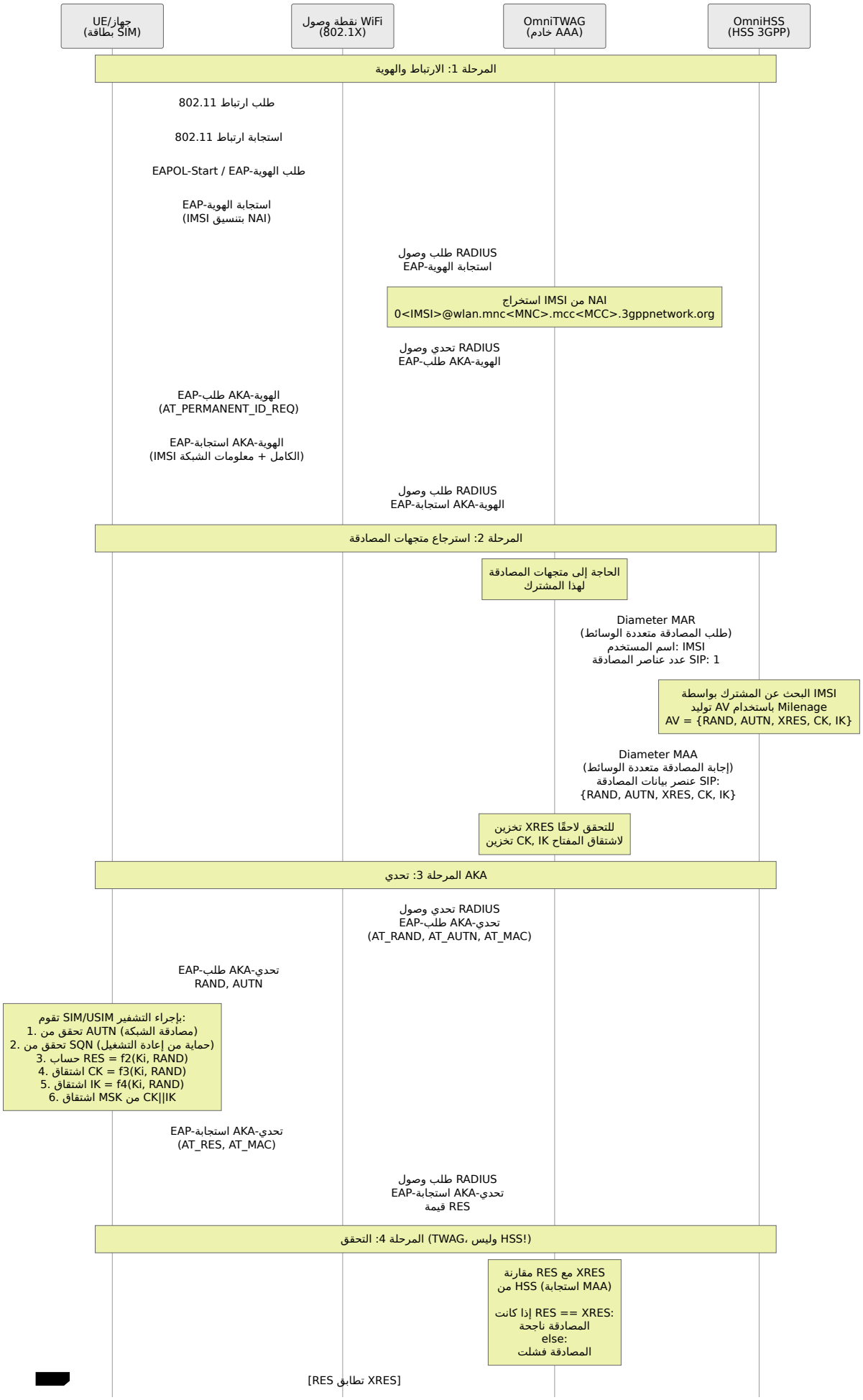
التكوين:

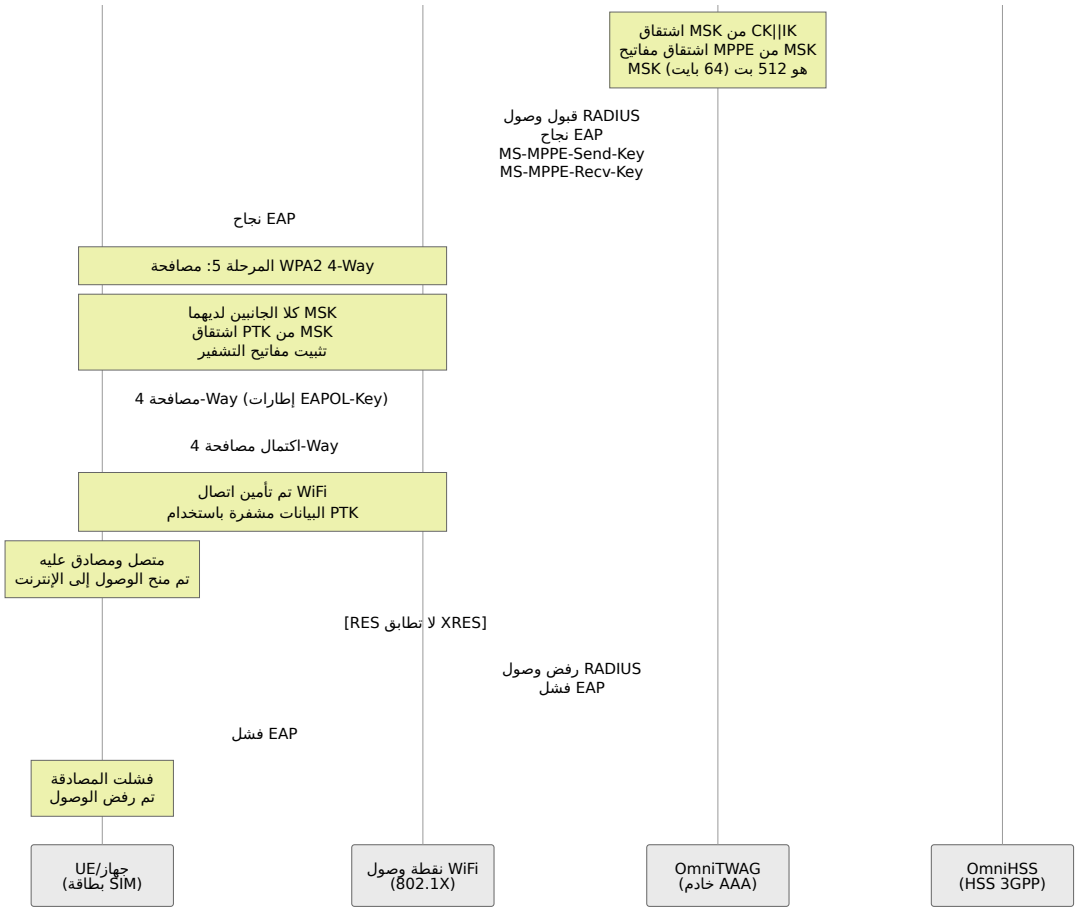
- يتم استعلام OCS عند بدء الجلسة (CCR-I)، خلال الجلسة (CCR-U)، وعند الانتهاء (CCR-T)
- يتم طلب الحصة في قطع قابلة للتكوين (10 مثل، 100MB، 50MB)
- يتم تفعيل CCR-Update عند عتبة قابلة للتكوين (مثل، 80% من الحصة الممنوحة)
- يقوم مؤقت الصلاحية بتفعيل إعادة التفويض إذا لم يتم استنفاد الحصة
- قطع الاتصال القسري عند استنفاد الحصة

- خصم الرصيد في الوقت الحقيقي

تدفق المصادقة

تسلسل المصادقة الكامل EAP-AKA


UE/جهاز
(بطاقة SIM)
WiFi نقطة وصول
(802.1X)
OmniTWAG
(خادم AAA)
OmniHSS
(HSS 3GPP)
المرحلة 1: الارتباط والهوية
طلب ارتباط 802.11
استجابة ارتباط 802.11
طلب الهوية-EAP / EAPOL-Start
استجابة الهوية-EAP
(بتنسيق NAI IMSI)
طلب وصول RADIUS
استجابة الهوية-EAP
استخراج IMSI من NAI
0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org
تحدي وصول RADIUS
طلب الهوية-EAP AKA
طلب الهوية-EAP AKA
(AT_PERMANENT_ID_REQ)
استجابة الهوية-EAP AKA
(الكامل + معلومات الشبكة IMSI)
طلب وصول RADIUS
استجابة الهوية-EAP AKA
المرحلة 2: استرجاع متجهات المصادقة
الحاجة إلى متجهات المصادقة
لهذا المشترك
Diameter MAR
(طلب المصادقة متعددة الوسائط)
اسم المستخدم: IMSI
عدد عناصر المصادقة SIP: 1
البحث عن المشترك بواسطة IMSI
توليد AV باستخدام Milenage
AV = {RAND, AUTN, XRES, CK, IK}
Diameter MAA
(إجابة المصادقة متعددة الوسائط)
عنصر بيانات المصادقة SIP:
{RAND, AUTN, XRES, CK, IK}
تخزين XRES للتحقق لاحقًا
تخزين CK, IK لاشتقاق المفتاح
المرحلة 3: تحدي AKA
تحدي وصول RADIUS
تحدي-طلب EAP-AKA
(AT_RAND, AT_AUTN, AT_MAC)
تحدي-طلب EAP-AKA
RAND, AUTN
تقوم SIM/USIM بإجراء التشفير:
1. تحقق من AUTN (مصادقة الشبكة)
2. تحقق من SQN (حماية من إعادة التشغيل)
3. حساب RES = f2(Ki, RAND)
4. اشتقاق CK = f3(Ki, RAND)
5. اشتقاق IK = f4(Ki, RAND)
6. اشتقاق MSK من CK||IK
تحدي-استجابة EAP-AKA
(AT_RES, AT_MAC)
طلب وصول RADIUS
تحدي-استجابة EAP-AKA
قيمة RES
المرحلة 4: التحقق (TWAG، وليس HSS!)
مقارنة XRES مع RES
من HSS (استجابة MAA)
إذا كانت RES == XRES:
المصادقة ناجحة
else:
المصادقة فشلت
[XRES تطابق RES]



النقاط الرئيسية في تدفق المصادقة

1. **MAR/MAA هو نهاية الاتصال مع HSS**: بعد استلام MAA (إجابة المصادقة متعددة الوسائط) مع XRES، يتولى TWAG جميع عمليات التحقق اللاحقة محليًا.

2. **يقوم TWAG بإجراء التحقق من RES**: يوفر HSS الاستجابة المتوقعة (XRES)، لكن TWAG يقارنها مع RES الفعلي من UE. لا يشارك HSS في هذه المقارنة.

3. **تحدث المصادقة في TWAG**: هذا يختلف عن بعض المخططات التي تظهر HSS يقوم خادم AAA (TWAG) بإجراء المقارنة - في الهيكلية الفعلية لـ 3GPP، تقوم بالتحقق.

تنسيق الهوية

يستجيب الجهاز بهويته الدائمة (IMSI) بتنسيق NAI:

```
505570000000000001@wlan.mnc057.mcc505.3gppnetwork.org
```

`0` التنسيق: `<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

هو الهوية، وعادة ما يكون 0 ولكن قد يكون رقمًا آخر من رقم IMSI ملاحظة - الرقم الأول، قبل الهواتف متعددة SIM / واحد لبطاقات IMSI.

مفتاح الجلسة الرئيسي (MSK)

هو مفتاح تشفير بطول 512 بت (64 بايت) يتم اشتقاقه أثناء (MSK) مفتاح الجلسة الرئيسي مصادقة EAP-AKA. يعمل كمادة المفتاح الأساسية لتأمين اتصال WiFi.

اشتقاق MSK:

1. يقوم كل من UE و TWAG بشكل مستقل باشتقاق نفس MSK
2. UE يشتق من CK/IK المحسوبة بواسطة SIM
3. TWAG يشتق من CK/IK المستلمة من HSS
4. MSK = PRF'(CK || IK, "Full Authentication", IMSI, ...)

استخدام MSK:

1. **اشتقاق PMK**: PMK = من (32 بايت) أول 256 بت MSK
2. **مصافحة WPA2 4-Way**: يستخدم كل من UE و AP PMK لاشتقاق PTK
3. **تشفير البيانات**: يتم تشفير جميع إطارات بيانات WiFi باستخدام المفتاح الزمني (TK) من PTK

لماذا MSK حاسم:

- **السرية**: بدون MSK، ستكون حركة مرور WiFi غير مشفرة
- **السلامة**: يمنع التلاعب بإطارات WiFi
- **ربط المصادقة**: يربط مصادقة EAP بتشفير WiFi
- **حماية من إعادة التشغيل**: يمنع هجمات إعادة التشغيل MSK الجديد
- **سرية مثالية للأمام**: لا يؤثر اختراق MSK واحد على الآخرين

استعادة التزامن

إذا اكتشف الجهاز عدم تطابق في رقم التسلسل (SQN خارج التزامن)، فإنه يبدأ عملية الاستعادة:

1. يحسب الجهاز AUTS (رمز المصادقة - التزامن)
2. يرسل EAP-AKA Synchronization-Failure مع AT-AUTS
3. يقوم TWAG بإعادة توجيه AUTS إلى HSS

4. يقوم HSS بإعادة تزامن رقم التسلسل وتوليد متجهات جديدة
5. تتم محاولة المصادقة مرة أ��رى باستخدام متجهات جديدة

هذا يكون شفافًا للمستخدم النهائي ولا يتطلب تدخل المشغل.

دليل التكوين

يتم تكوين TWAG عبر ملفات تكوين Elixir في دليل `config/`. التكوين الرئيسي في وقت التشغيل موجود في `config/runtime.exs`.

بالنسبة لنشر الإنتاج، يتم إدارة التكوين مركزيًا. أدناه هو مرجع فقط، أي قيم تم تغييرها على عقدة الإنتاج ستفقد في المرة القادمة التي يتم فيها تشغيل التشغيل الآلي.

تكوين Diameter

موجود في `config :diameter_ex`:

```
config :diameter_ex,
  diameter: %{
    # اسم الخدمة لكتلة Diameter
    service_name: :omnitouch_twag,

    # عنوان IP المحلي لربط خدمة Diameter
    listen_ip: "10.5.198.200",

    # المنفذ المحلي لاتصالات Diameter (القياسي هو 3868)
    listen_port: 3868,

    # مضيف الأصل Diameter
    host: "omnitwag",

    # مجال الأصل Diameter (يتطابق مع مجال شبكتك)
    realm: "epc.mnc057.mcc505.3gppnetwork.org",

    # أقران Diameter (HSS، DRA، خوادم AAA)
    peers: [
      %{
        # مضيف الأصل Diameter للقرين
        host: "omni-hss01.epc.mnc057.mcc505.3gppnetwork.org",

        # مجال الأصل Diameter للقرين
        realm: "epc.mnc057.mcc505.3gppnetwork.org",

        # عنوان IP للقرين (يمكن أن يكون HSS أو DRA مباشرة)
        ip: "10.179.2.140",

        # المنفذ للقرين (القياسي هو 3868)
        port: 3868,

        # استخدام TLS لأمان النقل
        tls: false,

        # بروتوكول النقل (:diameter_tcp أو :diameter_sctp)
        transport: :diameter_tcp,

        # بدء الاتصال بالقرين (true) أو الانتظار حتى يتصل القرين
(false)
        initiate_connection: true
      }
```

```
    ]
  }
```

3 يتبع **تنسيق المجال**GPP TS 23.003:

```
epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

حيث:

- MNC = رمز الشبكة المحمولة (مثل، 057)
- MCC = رمز الدولة المحمولة (مثل، 505 لأستراليا)

ملاحظة حول استخدام DRA: لاستخدام OmniDRA، قم بتكوين عنوان IP للقرين للإشارة إلى DRA بدلاً من الإشارة م��اشرة إلى HSS. سيقوم DRA بعد ذلك بتوجيه الرسائل إلى HSS المناسب بناءً على قواعد التوجيه (مجال الوجهة، نطاق IMSI، إلخ).

تكوين RADIUS

موجود في `config :omnitwag`:

```
config :omnitwag,
  radius_config: %{
    # قائمة الشبكات الفرعية المسموح بها لمصادر عملاء RADIUS
    # قائمة فارغة = السماح للجميع (غير موصى به للإنتاج)
    allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"],

    # السر المشترك لعملاء RADIUS
    # يجب أن تستخدم جميع نقاط الوصول هذا السر
    secret: "YOUR_STRONG_SECRET_HERE"
  }
```

أفضل ممارسات الأمان:

- استخدم أسرار RADIUS مشتركة قوية (20+ حرف)
- قم بتكوين `allowed_source_subnets` لتقييد وصول AP
- استخدم قواعد جدار الحماية لتقييد الوصول إلى المنافذ 1812/1813

مثال على تكوين الشبكة الفرعية:

```
allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"]
```

إذا كانت فارغة، يُسمح بجميع المصادر (مناسب فقط للمختبر/الاختبار).

تكوين مراقبة Prometheus

موجود في `config :omnitwag`:

```
config :omnitwag,
  prometheus: %{
    # المنفذ لنقطة نهاية مقاييس Prometheus
    port: 9568
  }
```

الوصول إلى المقاييس على: `http://<twag-ip>:9568/metrics`

ملخص المنافذ

المنفذ	البروتوكول	الغرض
1812	UDP	مصادقة RADIUS
1813	UDP	محاسبة RADIUS
3868	TCP	Diameter (SWx إلى HSS/DRA)
443	TCP	لوحة معلومات HTTPS
8444	TCP	واجهة برمجة التطبيقات REST HTTPS
9568	TCP	مقاييس Prometheus

إعداد نقطة الوصول

نقاط الوصول المدعومة

تدعم WiFi مع أي نقطة وصول OmniTWAG يعمل:

- **WPA2-Enterprise** (802.1 مصادقةX)
- **وظيفة عميل RADIUS**
- **طريقة المصادقة EAP-AKA**

المنصات المختبرة: Cisco Aironet، Aruba، Ubiquiti UniFi، Ruckus، نقاط الوصول المعتمدة على hostapd

متطلبات تكوين AP العامة

1. وضع الأمان **WPA2-Enterprise (802.1X)**
2. **خادم RADIUS** يشير إلى عنوان IP لـ TWAG
3. **منفذ مصادقة RADIUS**: 1812
4. **منفذ محاسبة RADIUS**: 1813 (اختياري ولكن موصى به)
5. **السر المشترك لـ RADIUS**: يجب أن يتطابق مع تكوين TWAG
6. **طريقة EAP**: EAP-AKA (الكل "أو")

مثال على تكوين Cisco من AP

تكوين CLI:

```
! تكوين خادم RADIUS
radius-server host 10.5.198.200 auth-port 1812 acct-port 1813 key
YOUR_SHARED_SECRET

! تكوين SSID 802.1 معX
dot11 ssid OPERATOR-WIFI
   vlan 10
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa version 2

! ربط SSID بواجهة الراديو
interface Dot11Radio0
   encryption mode ciphers aes-ccm
   ssid OPERATOR-WIFI
```

واجهة الويب:

1. **الأمان** انتقل إلى ← **AAA** ← **خادم RADIUS**
2. أضف خادم RADIUS: `10.5.198.200:1812` مع السر المشترك
3. انتقل إلى تكوين **WLAN**
4. اضبط الأمان على **WPA2-Enterprise**
5. اضبط طريقة EAP على **EAP-AKA الكل** أو
6. قم بتعيين مجموعة خادم RADIUS

مثال على تكوين hostapd

للنقاط الوصول المعتمدة على Linux (OpenWrt، الأنظمة المدمجة):

```
# /etc/hostapd/hostapd.conf

interface=wlan0
driver=nl80211
ssid=OPERATOR-WIFI

# WPA2-Enterprise
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP
ieee8021x=1

# تكوين RADIUS
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET

# تكوين EAP
eap_server=0

# Hotspot 2.0 (اختياري - للتحميل التلقائي)
interworking=1
internet=1
anqp_3gpp_cell_net=505,057
domain_name=wlan.mnc057.mcc505.3gppnetwork.org
nai_realm=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
roaming_consortium=505057
hs20=1
```

أفضل ممارسات بنية الشبكة

مهم: ضع APs و TWAG في مقاطع شبكة موثوقة. استخدم قواعد جدار الحماية لـ TWAG:

- السماح فقط لـ APs بالوصول إلى منافذ TWAG 1812/1813
- السماح لـ TWAG بالوصول إلى منفذ HSS 3868
- تقييد الوصول الإداري إلى لوحة معلومات TWAG (المنفذ 443)

تكامل Hotspot 2.0

نظرة عامة على Hotspot 2.0 (Passpoint)

Hotspot 2.0 (المعروف أيضًا باسم Passpoint 802.11u) هو معيار من تحالف WiFi يمكّن اكتشاف الشبكات اللاسلكية الآمنة والتوصيل التلقائي دون تدخل المستخدم. إنها التقنية الرئيسية لتحميل WiFi السلس.

الميزات الرئيسية:

- **اكتشاف الشبكة التلقائي**: يجد الجهاز الشبكات المتوافقة بناءً على المعايير
- **المصادقة التلقائية**: يستخدم بيانات اعتماد SIM (EAP-AKA) دون إدخال المستخدم

- **الارتباط الأولي المشفر**: OSEN (المصادقة فقط من خادم OSU) للتزويد الآمن
- **اتفاقيات التجوال**: تدعم الشبكات التي تمت زيارتها (مثل التجوال الخلوي)
- **الأولوية**: يفضل الجهاز الشبكات المملوكة للمشغل

تكوين AP لـ Hotspot 2.0

متطلبات AP:

1. **802.11 دعمu**: قدرة استعلام/استجابة ANQP
2. **WPA2-Enterprise**: 802.1 مصادقةX
3. **دعم EAP-AKA**: يجب أن يدعم طريقة EAP-AKA
4. **تكوين ANQP**: الإعلان عن معلومات المشغل الصحيحة

مثال على التكوين (AP المعتمد على hostapd):

```
# تكوين Hotspot 2.0 / Passpoint
interworking=1
internet=1
asra=0
esr=0
uesa=0

# تكوين ANQP
anqp_3gpp_cell_net=505,057
domain_name=omnitouchns.com,wlan.mnc057.mcc505.3gppnetwork.org

# تكوين مجال NAI
nai_realm=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
# طريقة<,<المجال<,<الترميز> :التنسيق-eap>[-معرف-المصادقة:قيمة
ادقة]الم
# 21 = EAP-AKA
# 2:1 = نوع الاعتماد: SIM
# 5:7 = طريقة EAP لا شيء: الموجهة (EAP-AKA مباشر)

# اتحاد التجوال
roaming_consortium=505057
# MCC=505 (الولايات المتحدة)، MNC=057 (محدد للمشغل)

# معلومات المكان (اختياري)
venue_group=1
venue_type=8
venue_name=eng:شبكة WiFi العامة للمشغل

# تكوين WPA2-Enterprise
wpa=2
wpa_key_mgmt=WPA-EAP
rsn_pairwise=CCMP
ieee8021x=1

# تكوين RADIUS (يشير إلى OmniTWAG)
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET
```

```
# تكوين SSID
ssid=OperatorWiFi
utf8_ssid=1

# إشارة Hotspot 2.0
hs20=1
hs20_oper_friendly_name=eng:شبكة WiFi للمشغل
```

سلوك التحميل التلقائي

كيف يعمل التحميل التلقائي:

1. يقوم الجهاز الذي يحتوي على ملف تعريف Passpoint بإجراء مسح WiFi دوري
2. يرسل استعلام ANQP إلى نقاط الوصول المكتشفة
3. إذا كان استجابة ANQP تتطابق مع الملف الشخصي (MCC/MNC، اتحاد التجوال):
   - تكون الأولوية عالية (لشبكة المنزلية) أو متوسطة (شريك التجوال)
4. إذا كانت الأولوية ≤ العتبة والإشارة > الحد الأدنى:
   - مصادقة EAP-AKA تلقائية
5. إذا كانت المصادقة ناجحة والأولوية > الاتصال الحالي:
   - قطع بيانات الخلوية، التحويل إلى WiFi
6. مراقبة جودة الإشارة والحفاظ على الاتصال

عوامل الأولوية:

1. **الشبكة المنزلية مقابل التجوال** (مطابقة MCC/MNC): تفضل الشبكة المنزلية على التجوال
2. **قوة الإشارة**: تفضل الإشارة الأقوى
3. **الأمان**: تفضل WPA2-Enterprise على الشبكة المفتوحة/WPA2-PSK
4. **السياسة**: يمكن للمشغل تكوين الشبكات المفضلة
5. **تجاوز المستخدم**: يمكن للمستخدم تعطيل WiFi يدويًا أو تفضيل الخلوية

المراقبة والإدارة

لوحة المعلومات على الويب

الوصول إلى لوحة المراقبة في الوقت الحقيقي على: `https://<twag-ip>/`

الميزات:

- **عرض عملاء RADIUS**: المشتركين النشطين، حالة المصادقة، تفاصيل الجلسة
- **عرض نقاط الوصول**: نقاط الوصول المتصلة، عدد العملاء، معلومات SSID
- **عرض استخدام العميل**: بيانات المحاسبة، وقت الجلسة، استخدام البيانات
- **عرض أقران Diameter**: حالة الاتصال بـ HSS/DRA

تكامل Prometheus

قم بتكوين Prometheus لالتقاط مقاييس TWAG:

```
# prometheus.yml
scrape_configs:
  - job_name: 'omnitwag'
    static_configs:
      - targets: ['10.5.198.200:9568']
    metrics_path: '/metrics'
    scrape_interval: 15s
```

المقاييس المتاحة:

مقاييس خادم RADIUS:

- `radius_access_request_count` - إجمالي حزم طلب وصول RADIUS المستلمة
- `radius_access_accept_count` - إجمالي حزم قبول الوصول المرسلة
- `radius_access_reject_count` - إجمالي حزم رفض الوصول المرسلة
- `radius_access_challenge_count` - إجمالي حزم التحدي المرسلة
- `radius_accounting_request_count{status_type}` - إجمالي حزم طلب المحاسبة (موسومة حسب الحالة: بدء، إيقاف، تحديث مؤقت، محاسبة قيد التشغيل، محاسبة متوقفة)

- `radius_active_clients_count` - العملاء المصادق عليهم حاليًا (يتم الاستطلاع كل 5 ثوانٍ)
- `radius_access_points_count` - نقاط الوصول المسجلة (يتم الاستطلاع كل 5 ثوانٍ)

مقاييس مصادقة EAP-AKA:

- `eap_aka_identity_count` - تبادلات هوية EAP-AKA
- `eap_aka_challenge_count` - تبادلات تحدي EAP-AKA
- `eap_aka_sync_failure_count` - حالات فشل التزامن (أحداث إعادة تزامن SQN)
- `eap_aka_auth_success_count` - المصادقات الناجحة
- `eap_aka_auth_reject_count` - المصادقات المرفوضة

مقاييس بروتوكول Diameter:

- `diameter_message_count{application, command, direction}` - إجمالي رسائل Diameter (موسومة حسب التطبيق، نوع الأمر، والاتجاه)

مقاييس ذاكرة VM Erlang:

- `vm_memory_total` - إجمالي كمية الذاكرة المخصصة (بايت)
- `vm_memory_processes` - الذاكرة المستخدمة بواسطة عمليات Erlang (بايت)
- `vm_memory_processes_used` - الذاكرة المستخدمة بواسطة عمليات Erlang باستثناء الذاكرة المخصصة غير المستخدمة (بايت)
- `vm_memory_system` - الذاكرة المستخدمة بواسطة نظام تشغيل Erlang (بايت)
- `vm_memory_atom` - الذاكرة المستخدمة بواسطة الذرات (بايت)
- `vm_memory_atom_used` - الذاكرة المستخدمة بواسطة الذرات باستثناء الذاكرة المخصصة غير المستخدمة (بايت)
- `vm_memory_binary` - الذاكرة المستخدمة بواسطة الثنائيات (بايت)
- `vm_memory_code` - الذاكرة المستخدمة بواسطة الكود المحمل (بايت)
- `vm_memory_ets` - الذاكرة المستخدمة بواسطة جداول ETS (بايت)

مقاييس نظام VM Erlang:

- `vm_system_info_process_count` - العدد الحالي لعمليات Erlang
- `vm_system_info_port_count` - العدد الحالي للمنافذ

- `vm_system_info_atom_count` - العدد الحالي للذرات
- `vm_system_info_schedulers` - عدد خيوط المجدول
- `vm_system_info_schedulers_online` - عدد المجدولين المتصلين حاليًا

مقاييس مجدول VM Erlang:

- `vm_statistics_run_queue` - الطول الإجمالي لجميع قوائم التشغيل
- `vm_total_run_queue_lengths_total` - الطول الإجمالي لجميع قوائم التشغيل (المجدولين الإجماليين)
- `vm_total_run_queue_lengths_cpu` - الطول الإجمالي لقوائم تشغيل المجدول CPU
- `vm_total_run_queue_lengths_io` - الطول الإجمالي لقوائم تشغيل المجدول IO

جمع المقاييس:

- يتم إصدار مقاييس EAP-AKA و RADIUS في الوقت الحقيقي عند حدوث الأحداث
- يتم استطلاع عدد العملاء ونقاط الوصول النشطة كل 5 ثوانٍ
- يتم استطلاع مقاييس VM Erlang كل 5 ثوانٍ من وقت تشغيل
- يتم عرض جميع المقاييس بتنسيق Prometheus على `http://<twag-ip>:9568/metrics`

السجلات

يستخدم TWAG مسجل Elixir المنظم للتسجيل.

عرض السجلات (systemd):

```
# ذيل السجل في الوقت الحقيقي
journalctl -u twag -f

# آخر 100 سطر
journalctl -u twag -n 100

# السجلات منذ آخر تشغيل
journalctl -u twag -b

# السجلات لفترة زمنية محددة
journalctl -u twag --since "2025-10-12 10:00:00" --until "2025-10-12 11:00:00"
```

رسائل السجل الرئيسية:

- `يستمع على المنفذ 1812` - بدء تشغيل الخادم `خادم RADIUS`
- AP من RADIUS `تم استلام طلب الوصول` - طلب `من {IP}:`
- EAP `المرحلة 1: استجابة الهوية` - الهوية الأولية
- `المرحلة 2: تحدي AKA` - التحدي المرسل إلى الجهاز
- `المصادقة مقبولة` - المصادقة الناجحة
- `المصادقة مرفوضة` - فشلت المصادقة
- `مسجلة AP: {IP}` - تم اكتشاف AP جديدة

استكشاف الأخطاء وإصلاحها

فشل المصادقة

العرض: لا يمكن للعميل الاتصال بشبكة WiFi

خطوات التشخيص:

1. تحقق من سجلات TWAG: `journalctl -u twag -f`
2. تحقق من أن السر المشترك لـ RADIUS يتطابق بين AP و TWAG
3. تأكد من وصول حزم RADIUS إلى TWAG: `tcpdump -i eth0 port 1812`
4. تحقق من توفير المشترك في HSS/التكوين

الأسباب الشائعة:

- السر المشترك لـ RADIUS غير صحيح
- جدار الحماية يمنع UDP 1812/1813
- عدم تطابق RES/XRES (Ki خاطئ أو تكوين HSS خاطئ)
- رقم التسلسل (SQN) خارج التزامن (يجب أن يتعافى تلقائيًا عبر إعادة التزامن)
- مشاكل الاتصال الشبكي بين TWAG و AP

مشاكل اتصال Diameter

العرض: عدم اتصال القرين HSS/DRA بـ Diameter

خطوات التشخيص:

1. تحقق من الاتصال الشبكي: `telnet <hss-ip> 3868`
2. تحقق من تكوين Diameter (القرين IP، مضيف الأصل، مجال الأصل)
3. راجع سجلات HSS/DRA لمحاولات الاتصال
4. تحقق من أن جدار الحماية يسمح TCP 3868

الأسباب الشائعة:

- المنفذ غير صحيح للقرين في التكوين/IP
- جدار الحماية يمنع TCP 3868
- عدم تطابق مضيف الأصل/المجال
- TWAG لا تقبل الاتصال من HSS/DRA

مشاكل الأداء

العرض: مصادقة بطيئة (>5 ثوانٍ)

خطوات التشخيص:

1. تحقق من وقت استجابة HSS
2. قياس زمن الانتقال الشبكي: `ping <hss-ip>`, `mtr <hss-ip>`
3. مراقبة استخدام موارد TWAG: `top`, `htop`
4. مراجعة إعدادات مهلة طلب Diameter

الأسباب الشائعة:

- أو استجابة بطيئة HSS مهلة استعلام
- زمن انتقال شبكي مرتفع
- استنفاد موارد TWAG (CPU/ذاكرة)
- عدد كبير جدًا من المصادقات المتزامنة

أدوات التصحيح

التقاط الحزم

```
# التقاط حركة مرور RADIUS
tcpdump -i eth0 -n port 1812 or port 1813 -w radius.pcap

# التقاط حركة مرور Diameter
tcpdump -i eth0 -n port 3868 -w diameter.pcap

# الالتقاط من AP محدد
tcpdump -i eth0 -n host 10.7.15.72 and port 1812 -w radius-
ap1.pcap
```

تحليل باستخدام Wireshark (يدعم محللات RADIUS و Diameter).

وحدة التحكم التفاعلية

الارتباط بـ TWAG الجاري للتصحيح المباشر:

```
# قشرة عن بُعد إلى TWAG الجاري
iex --sname debug --remsh twag@hostname --cookie <cookie>
```

من وحدة التحكم IEx:

```
# قائمة بجميع العملاء المصادق عليهم
CryptoState.keys()

# الحصول على حالة عميل محدد
CryptoState.get("050533805790000 1867@wlan.mnc057.mcc505.3gppnetwork.o

# قائمة بجميع APs
APState.list()

# قائمة بجلسات المحاسبة
ClientUsage.list()
```

رسائل الخطأ الشائعة

رسالة الخطأ	المعنى	الحل
`فشل التحقق من مصادق الرسالة`	عدم تطابق السر المشترك	تحقق من أن السر المشترك يتطابق على RADIUS لـ AP و TWAG
`متوقع RES: فشل التحقق من حصلت على ، <XRES> <RES>`	استجابة المصادقة غير صحيحة	تحقق من Ki لـ SIM، تحقق من توفير HSS
`مهلة اتصال القرين Diameter`	لا يمكن الوصول إلى HSS	تحقق من الشبكة، جدار الحماية، تكوين HSS
`فشل في فك تشفير رسالة EAP`	حزمة EAP مشوهة	تحقق من البرنامج الثابت لـ AP، قد تحتاج إلى تحديث AP
`نوع EAP-AKA غير معروف`	رسالة EAP-AKA غير مدعومة	يستخدم الجهاز إصدار غير قياسي من EAP-AKA
`يتطلب إعادة تزامن رقم التسلسل`	SQN خارج التزامن	طبيعي، سيقوم الجهاز بإعادة التزامن تلقائيًا

الا��تثال للمعايير

يطبق OmniTWAG 3 المواصفات التالية من 3GPP و IETF:

- **3GPP TS 23.402**: تحسينات المعمارية للوصول غير 3GPP
- **3GPP TS 24.302**: الوصول إلى EPC 3 عبر الشبكات غير 3GPP
- **3GPP TS 29.273**: واجهات SWx/SWm المعتمدة على Diameter
- **3GPP TS 33.402**: جوانب الأمان للوصول غير 3GPP
- **3GPP TS 35.206**: مواصفة خوارزمية Milenage
- **RFC 2865**: مصادقة RADIUS
- **RFC 2866**: محاسبة RADIUS
- **RFC 3579**: دعم RADIUS لـ EAP
- **RFC 4187**: بروتوكول المصادقة EAP-AKA
- **RFC 5448**: EAP-AKA' (الإصدار المحسن)

الملخص

يوفر OmniTWAG، الذي أنشأته Omnitouch، حلاً كاملاً متوافقًا مع المعايير لتحميل 3GPP WiFi:

1. **نشر مرن**: يدعم الانفصال المحلي أو حركة المرور الموجهة إلى المنزل
2. **معتمد على المعايير**: ينفذ بروتوكولات 3GPP SWx و EAP-AKA و RADIUS
3. **مصادقة آمنة**: مصادقة متبادلة تعتمد على SIM مع إعادة تزامن تلقائية
4. **تشفير قوي**: مفاتيح مشتقة من MSK توفر تشفير WPA2
5. **جاهز لـ Hotspot 2.0**: يمكّن التحميل التلقائي بالكامل بدون لمس
6. **تحكم المشغل**: يحافظ على الهوية، والسياسة، وخيار الفوترة
7. **اتصال مرن**: اتصال مباشر بـ HSS أو عبر OmniDRA للتوجيه/توازن الحمل
