الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2760

(2011/05)

السلسلة Y: البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

شبكات الجيل التالي – الأمن

إطار أمن التنقلية في شبكات الجيل التالي

التوصيـــة ITU-T Y.2760

توصيات السلسلة Y الصادرة عن قطاع تقييس الاتصالات

البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

البنية التحتية العالمية للمعلومات	
اعتبارات عامة	Y.199-Y.100
الخدمات والتطبيقات، والبرمجيات الوسيطة	Y.299-Y.200
الجوانب الخاصة بالشبكات	Y.399-Y.300
السطوح البينية والبروتوكولات	Y.499-Y.400
الترقيم والعنونة والتسمية	Y.599-Y.500
الإدارة والتشغيل والصيانة	Y.699-Y.600
الأمن	Y.799-Y.700
مستويات الأداء	Y.899-Y.800
جوانب متعلقة ببروتوكول الإنترنت	
اعتبارات عامة	Y.1099-Y.1000
الخدمات والتطبيقات	Y.1199-Y.1100
المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد	Y.1299-Y.1200
النقل	Y.1399-Y.1300
التشغيل البيني	Y.1499-Y.1400
نوعية الخدمة وأداء الشبكة	Y.1599-Y.1500
التشوير	Y.1699-Y.1600
الإدارة والتشغيل والصيانة	Y.1799-Y.1700
الترسيم	Y.1899-Y.1800
تلفزيون بروتوكول الإنترنت عبر شبكات الجيل التالي	Y.1999-Y.1900
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099-Y.2000
نوعية الخدمة والأداء	Y.2199-Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249-Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2299-Y.2250
الترقيم والتسمية والعنونة	Y.2399-Y.2300
إدارة الشبكة	Y.2499-Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599-Y.2500
الشبكات الذكية الشمولية	Y.2699-Y.2600
الأمـــن	**Y.2799-Y.2700**
التنقلية المعممة	Y.2899-Y.2800
البيئة المفتوحة عالية الجودة	Y.2999-Y.2900
شبكات المستقبل	Y.3099-Y.3000

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـــة ITU-T Y.2760

إطار أمن التنقلية في شبكات الجيل التالي

ملخص

توصّف هذه التوصية إطار أمن التنقلية في طبقة النقل في شبكات الجيل التالي. وهي تتناول متطلبات الأمن وآلياته وإجراءات إدارة التنقلية والتحكم فيها ضمن شبكات الجيل التالي.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T Y.2760	2011.05.20	13

عبارات رئيسية

أمن التنقلية، شبكات الجيل التالي

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

التوصيـــة ITU-T Y.2760

إطار أمن التنقلية في شبكات الجيل التالي

1 مجال التطبيق

تصف هذه التوصية إطار أمن التنقلية في طبقة النقل في شبكات الجيل التالي (NGN). وهي تنظر في متطلبات الأمن التي وردت في التوصية [ITU-T Y.2018]. وتشمل هذه التوصية الاستيقان وإدارة المفاتيح؛ وإنشاء سياق الأمن؛ وأمن التنقلية في بروتوكول الإنترنت؛ وإدارة أمن التنقلية والتحكم فيها ونقلها في طبقة النقل. وتتناول هذه التوصية سيناريوهات تشمل التنقلية ضمن التكنولوجيا الواحدة وفيما بين التكنولوجيات، والتنقلية ضمن الميدان الواحد وفيما بين الميادين.

2 المراجع

تشتمل التوصيات والمراجع الأخرى التالية لقطاع تقييس الاتصالات على أحكام تشكّل، من خلال الإشارة إليها في هذا النص، أحكاماً في هذه التوصية. وكانت الطبعات المشار إليها صالحة وقت نشر هذه التوصية. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات سارية الصلاحية. والإشارة إلى أي وثيقة داخل هذه التوصية لا يعطي هذه الوثيقة في حد ذاتها وضع التوصية.

[ITU-T Q.1706] التوصية ITU-T Q.1706 /Y.2801 (2006)، *متطلبات إدارة التنقلية في شبكات الجيل التالي*.

[ITU-T X.805] التوصية ITU-T X.805 (2003)، *معمارية أمن الأنظمة التي تكفل الاتصالات من طرف إلى طرف*.

[ITU-T Y.2011] التوصية ITU-T Y. 2011 (2004)، *المبادئ العامة والنموذج المرجعي العام لشبكات الجيل التالي*.

[ITU-T Y.2012] التوصية ITU-T Y.2012 (2010)، *المتطلبات الوظيفية والمعمارية في شبكات الجيل التالي*.

[ITU-T Y.2014] التوصية ITU-T Y.2014 (2010)، *وظائف التحكم في مرفقات الشبكة في شبكات الجيل التالي*.

[ITU-T Y.2018] التوصية ITU-T Y.2018 (2009)، *وظائف إدارة التنقلية والتحكم فيها في شبكات الجيل التالي*.

[ITU-T Y.2701] التوصية ITU-T Y.2701 (2007)، *المتطلبات الأمنية من شبكات الجيل التالي الإصدار 1*.

[ITU-T Y.2704] التوصية ITU-T Y.2704 (2010)، *آليات وإجراءات الأمن لشبكات الجيل التالي*.

[ITU-T Y.-Sup.7] سلسلة التوصيات ITU-Y – الإضافة 7 (2008)، *سلسلة التوصيات ITU-T Y.2000 - إضافة إلى شبكات الجيل التالي، الإصدار 2، مجال التطبيق*.

[ITU-R M.1645] التوصية ITU-R M.1645 (2003)، *الإطار والأهداف العامة للتطور المستقبلي لأنظمة الاتصالات المتنقلة الدولية - 2000 وما بعدها*.

3 التعاريف

1.3 مصطلحات معرَّفة في أماكن أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في أماكن أخرى:

1.1.3 التمرير [2.2.6/ITU-T Q.1706]: هو القدرة على تقديم خدمات لشيء متحرك أثناء الحركة وبعدها مع بعض التأثير على اتفاقات مستوى هذه الخدمات.

2.1.3 **التنقلية الأفقية** [3.2.6/ITU-T Q.1706]: هي التنقلية عبر نفس الطبقة مثلما هو محدد في التوصية [ITU-R M.1645]، ويُشار إليها عموماً على أنها التنقلية ضمن نطاق تكنولوجيا النفاذ ذاتها.

3.1.3 **التنقلية** [2.3/ITU-T Q.1706]: هي قدرة المستعمل أو الكيانات المتنقلة الأخرى على الاتصال والنفاذ إلى الخدمات، بصرف النظر عن التغييرات في الموقع أو البيئة التقنية.

4.1.3 **طبقة النقل في شبكات الجيل التالي** [10.3/ITU-T Y.2011]: هي جزء من شبكة الجيل التالي يوفر وظائف المستخدم لنقل البيانات والوظائف التي تتحكم في موارد النقل وتديرها لنقل هذه البيانات بين الكيانات الانتهائية.

5.1.3 **الثقة** [9.2.3/ITU-T Y.2701]: يقال إن الكيان X يثق في الكيان Y بالنسبة إلى المجموعة من الأنشطة إذا وثق الكيان X في أن الكيان Y سيتصرف بطريقة معينة فيما يتعلق بالأنشطة.

6.1.3 **التنقلية الرأسية** [3.2.6/ITU-T Q.1706]: هي التنقلية بين طبقات مختلفة على غرار ما هو محدد في التوصية [ITU-R M.1645]، ويُشار إليها عموماً على أنها التنقلية بين تكنولوجيات نفاذ مختلفة.

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية.

1.2.3 **التنقلية فيما بين التكنولوجيات**: انظر التنقلية الرأسية في الفقرة 1.3.

2.2.3 **التنقلية ضمن التكنولوجيا الواحدة**: انظر التنقلية الأفقية في الفقرة 1.3.

3.2.3 **سياق الأمن**: مجموعة معلمات أمنية تشمل المعرّف والمادة الرئيسة والخوارزمية الرئيسية، وما إلى ذلك.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

3G الجيل الثالث *(3rd Generation)*

ABG-FE الكيان الوظيفي لبوابة حدود النفاذ *(Access Border Gateway Functional Entity)*

AE توسيع الاستيقان *(Authentication Extension)*

AKA اتفاق الاستيقان والمفاتيح *(Authentication and Key Agreement)*

AM-FE الكيان الوظيفي لإدارة النفاذ *(Access Management Functional Entity)*

AN-FE الكيان الوظيفي لعقدة النفاذ *(Access Node Functional Entity)*

ANI السطح البيني من التطبيق إلى الشبكة *(Application to Network Interface)*

AR-FE الكيان الوظيفي لترحيل النفاذ *(Access Relay Functional Entity)*

DDoS الحرمان من الخدمة الموزع *(Distributed Deny of Service)*

EAP بروتوكول الاستيقان القابل للتوسيع *(Extensible Authentication Protocol)*

EN-FE الكيان الوظيفي لعقدة الحافة *(Edge Node Functional Entity)*

FA وكيل أجنبي *(Foreign Agent)*

HA وكيل محلي *(Home Agent)*

HDC-FE الكيان الوظيفي المعني بقرار التحكم في التمرير *(Handover Decision Control Functional Entity)*

IP بروتوكول الإنترنت *(Internet Protocol)*

L3HEF وظيفة تنفيذ التمرير في الطبقة 3 *(Layer 3 Handover Execution Function)*

MIP بروتوكول الإنترنت للخدمة المتنقلة *(Mobile IP)*

MIPv4 الإصدار الرابع من بروتوكول الإنترنت للخدمة المتنقلة. انظر [b-IETF RFC 3220] *(Mobile IP for IP version 4. See [b-IETF RFC 3220])*

MIPv6 الإصدار السادس من بروتوكول الإنترنت للخدمة المتنقلة. انظر [b-IETF RFC 3775] *(Mobile IP for IP version 6. See [b-IETF RFC 3775])*

MLM-FE الكيان الوظيفي لإدارة الموقع المتنقل *(Mobile Location Management Functional Entity)*

MMCF وظائف التحكم في إدارة التنقلية *(Mobility Management Control Functions)*

MN عقدة متنقلة *(Mobile Node)*

MOBIKE بروتوكول التنقلية والتوجيه المتعدد في الإصدار الثاني من بروتوكول تبادل المفاتيح (IKEv2) انظر [b-IETF RFC 4555] *(IKEv2 Mobility and Multihoming Protocol. See [b-IETF RFC 4555])*

NACF وظائف التحكم في مرفقات الشبكة *(Network Attachment Control Functions)*

NGN شبكة الجيل التالي *(Next Generation Network)*

NID-FE الكيان الوظيفي لتوزيع معلومات الشبكة *(Network Information Distribution Functional Entity)*

NNI سطح بيني من شبكة إلى أخرى *(Network to Network Interface)*

PKI بنية تحتية للمفاتيح العمومية *(Public Key Infrastructure)*

PMIPv6 الإصدار السادس من بروتوكول الإنترنت للخدمة المتنقلة بالوكالة. انظر [b-IETF RFC 5213] *(Proxy Mobile IPv6. See [b-IETF RFC 5213])*

RAN شبكة النفاذ الراديوي *(Radio Access Network)*

RRP رد التسجيل *(Registration Reply)*

RRQ طلب تسجيل *(Registration Request)*

TAA-FE الكيان الوظيفي لاستيقان النقل وتخويله *(Transport Authentication and Authorization Functional Entity)*

TLM-FE الكيان الوظيفي لإدارة موقع النقل *(Transport Location Management Functional Entity)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TTLS أمن طبقة النقل المغلفة *(Tunnelled Transport Layer Security)*

TUP-FE الكيان الوظيفي المعني بالبيانات العامة لمستخدم النقل *(Transport User Profile Functional Entity)*

UE جهاز المستخدم *(User Equipment)*

UNI السطح البيني من المستخدم إلى الشبكة *(User to Network Interface)*

WiMax إمكانية التشغيل البيني للنفاذ بالموجات الصغرية في كل أنحاء العالم *(Worldwide Interoperability for Microwave Access)*

WLAN شبكة محلية لا سلكية *(Wireless LAN)*

5 متطلبات الأمن للتنقلية في شبكات الجيل التالي

تدعم شبكات الجيل التالي تكنولوجيات نفاذ متعددة مثل WLAN وWiMax و3G RAN وغيرها [ITU-T Y.2012]. ودعم التنقلية هو إحدى الميزات الموجودة في شبكات الجيل التالي التي تتضمن التجوال والتمرير. وفي الإصدار الثاني من شبكات الجيل التالي، يشمل التمرير سيناريوهات ما بين شبكات النفاذ ووضمن شبكة النفاذ الواحدة [ITU-T Y - Sup.7].

وتدعم شبكات الجيل التالي الميزات التالية:

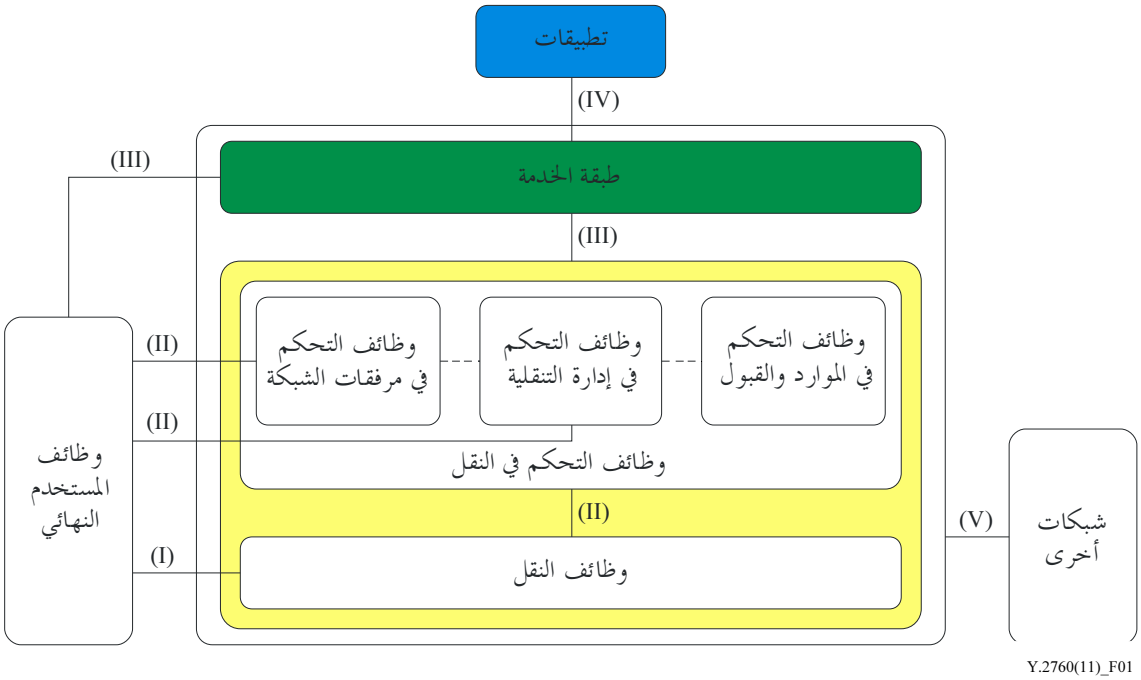
1) نموذج الثقة: يحدد نموذج الثقة الأمني في شبكات الجيل التالي ثلاث مناطق أمنية: موثوقة، وموثوقة ولكن تشوبها نقاط ضعف، وغير موثوقة [ITU-T Y.2701]. وهو يبين وجوب عبور شبكة النفاذ لبوابة أمنية قبل النفاذ إلى الشبكة الأساسية.

2) وتدعم شبكات الجيل التالي تكنولوجيات نفاذ متعددة.

3) وتدعم شبكات الجيل التالي عدة بروتوكولات تنقلية مثل MIPv4 وMIPv6 وDSMIPv6 وPMIPv6 وMOBIKE.

4) وتدعم شبكات الجيل التالي معدات المستخدم المتعددة راديوياً، مثل WLAN وWiMax و3G RAN وغيرها.

5) وتدعم شبكات الجيل التالي استمرارية الخدمة عند التمرير بين أنظمة النفاذ غير المتجانسة.



الشكل 1 – معمارية أمن التنقلية في شبكات الجيل التالي

تعرَّف خمس مجموعات من الميزات الأمنية.

(I) التركيز على الأمن في طبقة النقل مثل أمن النفاذ الذي يمكن حمايته مادياً أو منطقياً بين وظائف المستخدم النهائي ووظائف النقل في كيان شبكة النفاذ. كما تخص الفقرة (I) أمن السطح البيني من المستخدم إلى الشبكة (UNI) بين وظائف المستخدم النهائي ووظائف النقل.

(II) التركيز على الأمن في طبقة التحكم بين وظائف المستخدم النهائي وكيان وظيفة التحكم في النقل. كما تركز الفقرة (II) على الأمن في السطح البيني لرسالة التحكم ما بين كيان وظائف النقل وكيان وظيفة التحكم في النقل. وتخص الفقرة (II) أمن السطح البيني من المستخدم إلى الشبكة (UNI) بين وظائف المستخدم النهائي ووظائف التحكم في النقل.

(III) التركيز على أمن السطح البيني بين وظائف المستخدم النهائي وطبقة الخدمة. كما تركز الفقرة (III) على الأمن في السطح البيني لرسالة التحكم ما بين كيان وظائف التحكم في النقل وطبقة الخدمة. وتخص الفقرة (III) أمن السطح البيني من المستخدم إلى الشبكة (UNI) بين وظائف المستخدم النهائي وطبقة الخدمة.

(IV) التركيز على أمن السطح البيني بين طبقة الخدمة وكيان التطبيق. وتخص الفقرة (IV) أمن السطح البيني من المستعمل إلى الشبكة (ANI) بين وظائف المستخدم النهائي ووظائف النقل.

(V) التركيز على أمن سطح البيني من شبكات الجيل التالي إلى الشبكات الأخرى، ويشمل ذلك طبقة النقل وطبقة التحكم. وتخص الفقرة (V) أمن السطح البيني من شبكة إلى أخرى (NNI) بين شبكات الجيل التالي والشبكات الأخرى.

وتنطبق مبادئ التوصية [ITU-T X.805] على التهديدات الأمنية والمتطلبات الأمنية التي تم تحديدها في هذه التوصية.

1.5 التهديدات الأمنية

حُددت التهديدات الأمنية التالية في التوصية [ITU-T Y.2018]:

T1 يمكن ألاّ تكون معدات المستخدم مخولة للشروع في تشوير التنقلية مع الكيان الوظيفي لإدارة الموقع المتنقل (MLM-FE).

T2 يمكن للدخلاء العبث بتشوير التنقلية.

T3 يمكن انتحال صفة الكيان الوظيفي لإدارة الموقع المتنقل (MLM-FE) لتقديم معلومات كاذبة إلى جهاز المستخدم.

T4 يمكن للدخلاء التنصت على موقع جهاز المستخدم.

T5 يمكن وقوع هجوم يغير اتجاه الحركة.

T6 يمكن لمهاجم أن ينسل وسط مسير اتصالات بين طرفين.

T7 يمكن لهجوم الحرمان من الخدمة الموزع (DDoS) أن يستهلك كمية كبيرة من موارد الشبكة.

T8 يمكن ألاّ تكون معدات المستخدم مخولة للحصول على معلومات من الكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE) أو الكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE).

T9 يمكن انتحال صفة الكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE) أو الكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE) لدس معلومات كاذبة إلى جهاز المستخدم.

T10 يمكن تعديل التشوير بين الكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE) أو الكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE)، أو التنصت على هذا التشوير.

T11 يمكن التنصت على بيانات طبقة المستخدم أو تعديلها.

2.5 متطلبات الأمن

حُددت متطلبات الأمن التالية في التوصية [ITU-T Y.2018]:

R1 يتعين إجراء الاستيقان المتبادل بين جهاز المستخدم والكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE).

R2 تلزم حماية التشوير بين جهاز المستخدم والكيان الوظيفي لإدارة الموقع المتنقل (MLM-FE) من حيث السلامة والسرية.

R3 تلزم حماية التشوير بين جهاز المستخدم والكيان الوظيفي لإدارة الموقع المتنقل (MLM-FE) من هجمات التكرار.

R4 يتعين أن تتوفر خصوصية موقع جهاز المستخدم.

R5 يتعين إجراء الاستيقان المتبادل بين جهاز المستخدم والكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE).

R6 تلزم حماية التشوير بين جهاز المستخدم والكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE) من حيث السلامة والسرية.

R7 تلزم حماية التشوير بين جهاز المستخدم والكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE) من هجمات التكرار.

R8 يلزم توفر الاستيقان منخفض الكمون وحماية التشوير.

R9 يلزم نقل سياق الأمن على الوجه الأمثل.

R10 يلزم أن يكون حل أمن التنقلية مستقلاً عن الوسائط.

R11 يلزم توفر آليات لحماية حركة طبقة المستخدم ما بين جهاز المستخدم والكيان الوظيفي لعقدة الحافة (EN-FE) عندما تنص البيانات العامة للمستخدم على ذلك.

وبالإضافة إلى متطلبات الأمن المحددة في التوصية [ITU-T Y.2018]، فإن متطلب الأمن التالي على صلة بالموضوع.

R12 يلزم دعم أمن التوصيلات المتعددة.

6 قدرات الأمن التي تدعمها كيانات وظيفية ذات صلة

إن الكيانات الوظيفية المتصلة بأمن التنقلية في شبكات الجيل التالي هي التالية:

- الكيان الوظيفي المعني بالبيانات العامة لمستخدم النقل (TUP-FE)
- الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE)
- الكيان الوظيفي لإدارة الموقع المتنقل (MLM-FE)
- الكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE)
- الكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE)
- الكيان الوظيفي لإدارة النفاذ (AM-FE)
- وظيفة تنفيذ التمرير في الطبقة 3 (L3HEF)
- الكيان الوظيفي لعقدة النفاذ (AN-FE)

1.6 الكيان الوظيفي المعني بالبيانات العامة لمستخدم النقل (TUP-FE)

يخزن الكيان الوظيفي المعني بالبيانات العامة لمستخدم النقل (TUP-FE) بيانات الاستيقان من الاشتراك، كمادة المفتاح وأساليب الاستيقان والبيانات العامة لنقل المستخدم. ويرد في التوصية [ITU-T Y.2014] وصف وظيفي مفصل للكيان الوظيفي المعني بالبيانات العامة لمستخدم النقل.

2.6 الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE)

يستخرج الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) بيانات الاستيقان ومعلومات تخويل النفاذ من الكيان الوظيفي المعني بالبيانات العامة لمستخدم النقل (TUP-FE). ويمكن أيضاً للكيان الوظيفي TAA-FE أن يعمل بمثابة وكيل.

ويرد في التوصية [ITU-T Y.2014] وصف وظيفي مفصل لهذا الكيان الوظيفي.

3.6 الكيان الوظيفي لإدارة الموقع المتنقل (MLM-FE)

يحصل الكيان الوظيفي لإدارة الموقع المتنقل (MLM-FE) على معلومات الاستيقان والتخويل والمحاسبة من وظائف التحكم في مرفقات الشبكة (NACF)، ويقوم بالاستيقان المتبادل مع جهاز المستخدم ويقيم رابطة أمنية معه. ويرد في التوصية [ITU-T Y.2018] وصف وظيفي مفصل لهذا الكيان الوظيفي.

4.6 الكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE)

يتعين على الكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE) أن يقيم رابطة أمنية مع جهاز المستخدم، وهو يحصل على مفتاح الأمن المستخدم للرابطة الأمنية من الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) عبر الكيان الوظيفي TLM-FE. ويرد في التوصية [ITU-T Y.2018] وصف وظيفي مفصل للكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE).

5.6 الكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE)

يتعين على الكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE) أن يقيم رابطة أمنية مع جهاز المستخدم لحماية معلومات مثل معلومات انتقاء الشبكة. ويمكن لهذا الكيان أن يحصل على معلومات الأمن من الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) عبر الكيان الوظيفي TLM-FE. ويرد في التوصية [ITU-T Y.2018] وصف وظيفي مفصل للكيان الوظيفي لتوزيع معلومات الشبكة.

6.6 الكيان الوظيفي لإدارة النفاذ (AM-FE)

يسيّر الكيان الوظيفي لإدارة النفاذ (AM-FE) طلبات النفاذ إلى الشبكة إلى الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) للاستيقان من المستخدم أو تخويله بالنفاذ إلى الشبكة أو منعه من ذلك، ويستخرج معلمات تشكيلة النفاذ الخاصة بالمستخدم. ويمكن للكيان الوظيفي لإدارة النفاذ أن يعيد استخدام بيانات تسجيل/تشكيلة الشبكة كي تستعاد الخدمة بسرعة دون تكرار كل إجراءات التسجيل/الاستيقان/التشكيلة. ويرد في التوصية [ITU-T Y.2014] وصف وظيفي مفصل للكيان الوظيفي لإدارة النفاذ.

7.6 وظيفة تنفيذ التمرير في الطبقة 3 (L3HEF)

يتعين على وظيفة تنفيذ التمرير في الطبقة 3 (L3HEF) أن تقيم رابطة أمنية مع جهاز المستخدم لحماية الحركة بينهما. ويرد في التوصية [ITU-T Y.2018] وصف وظيفي مفصل لهذه الوظيفة.

ملاحظة – يتناول أمن وظيفة تنفيذ التمرير في الطبقة 3 (L3HEF) المتطلبات الأمنية لحماية الحركة في طبقة المستخدم بين جهاز المستخدم والكيان EN-FE.

8.6 الكيان الوظيفي لعقدة النفاذ (AN-FE)

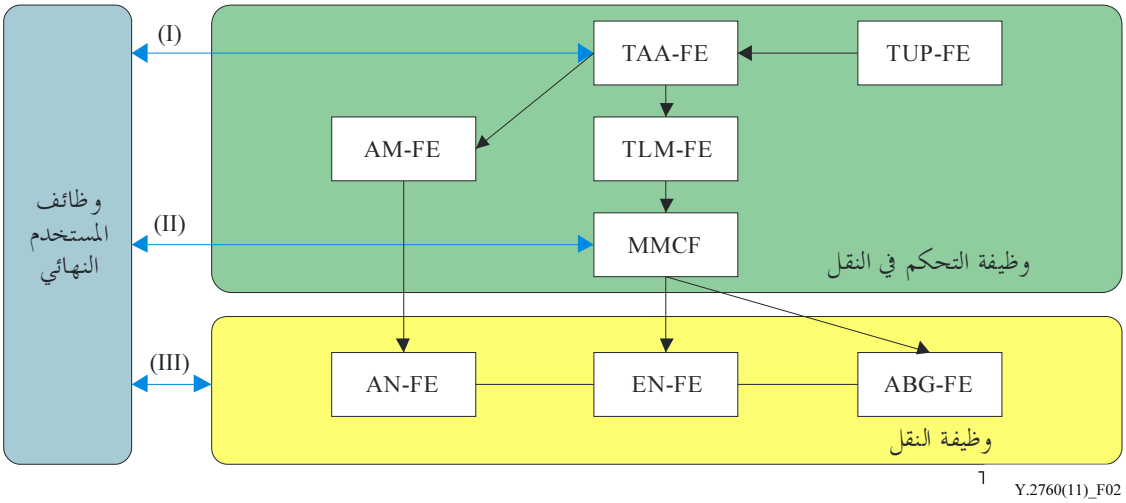
يتعين على الكيان الوظيفي لعقدة النفاذ (AN-FE) أن يقيم رابطة أمنية مع جهاز المستخدم، وهو يحصل على مادة المفتاح من الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) عبر الكيان الوظيفي لإدارة النفاذ (AM-FE). ويرد في التوصية [ITU-T Y.2018] وصف وظيفي مفصل للكيان الوظيفي لعقدة النفاذ.

7 إدارة المفتاح والاستيقان منه

1.7 إطار إدارة المفتاح

تُستخدم آلية اشتقاق المفتاح التراتبي لأمن التنقلية في شبكات الجيل التالي. وهناك عدة أنواع من مواد المفتاح في شبكات الجيل التالي، مثل مفتاح الجذر ومفتاح الدورة وما إلى ذلك. ومفتاح الجذر هو أحد أنواع الإثباتات الطويلة الأمد المخزنة بأمان (مثلاً، مفتاح سري أو كلمة مرور مشتركة). أما مفتاح الدورة فهو أحد أنواع مادة المفتاح القصيرة الأمد ويتولد على أساس مفتاح الجذر. وفي شبكات الجيل التالي، يُختزن مفتاح الجذر في جهاز المستخدم وفي كيان الاستيقان (مثل TAA-FE/TUP-FE) على السواء.

وعادة ما تُستولد مادة مفتاح الدورة على أساس مفتاح الجذر ومعلمات توليد المفتاح الأخرى مثل معلومات التفاوض أثناء إجراء الاستيقان. وتُستخدم مادة مفتاح الدورة لحماية حركة التشوير وحركة المستخدم. ويمكن مواصلة اشتقاق مفتاح الدورة. وتعتمد آلية اشتقاق المفتاح على خصوصية الخوارزمية التجفيرية أو البروتوكول.



الشكل 2 – الإطار العام للمفاتيح لأمن التنقلية في شبكات الجيل التالي

يوصَف الإطار العام للمفاتيح لأمن التنقلية في شبكات الجيل التالي على النحو التالي:

(I) يقوم جهاز المستخدم بإجراء الاستيقان المتبادل مع الكيانات الوظيفية في شبكات الجيل التالي. وفي إجراء الاستيقان، يولد كيان TUP-FE متّجهات الاستيقان على أساس مادة مفتاح الجذر ويرسل هذه المتّجهات إلى كيان TAA-FE. وبعد الانتهاء من إجراء الاستيقان المتبادل بنجاح، يولّد كيان TAA-FE وجهاز المستخدم كلاهما مادة مفتاح الدورة. ويمكن استخدام مادة مفتاح الدورة لتوليد مادة مفتاح الدورة الفرعية. وتُنقل مادة مفتاح الدورة إلى الكيانات الوظيفية مثل AM-FE وMMCF اللذين يمكن أن يولدا كلاهما مواد مفتاح دورة على أساس مادة مفتاح الدورة المتلقاة.

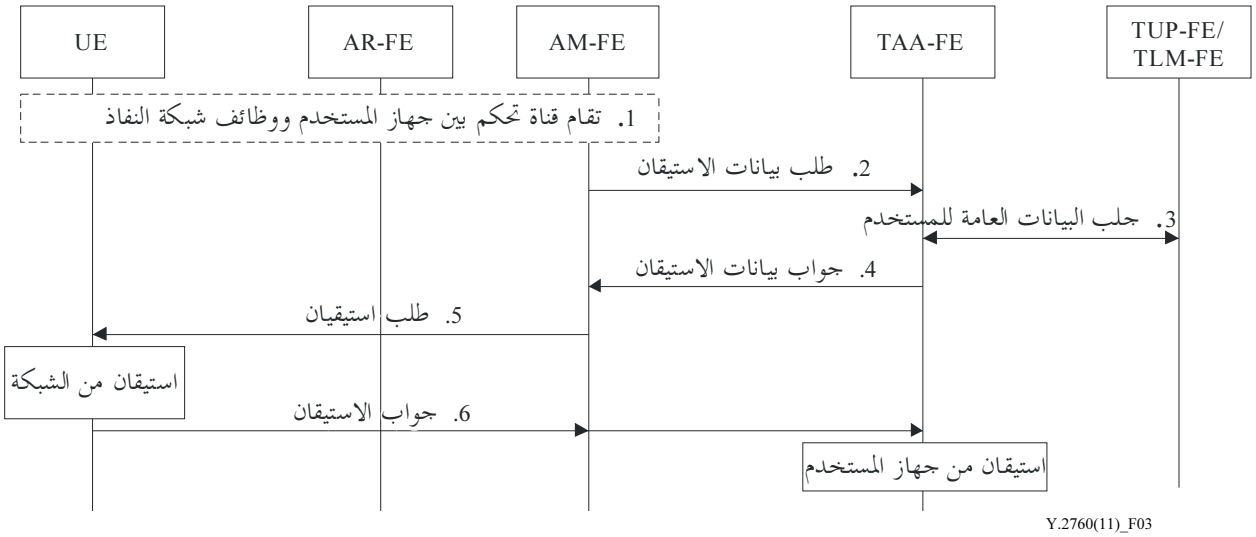
(II) وتقوم رابطات الأمن للنقاط المرجعية بين معدات المستخدم ووظائف التحكم في إدارة التنقلية (MMCF) على مادة مفتاح الدورة من الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) عبر الكيان الوظيفي TLM-FE. وتولّد مادة مفتاح الدورة المستخدَمة في هذه الفقرة أو تُشتق وفقاً لمادة مفتاح الدورة في الكيان الوظيفي لاستيقان النقل وتخويله.

(III) وتقام رابطات الأمن بين جهاز المستخدم وطبقة وظيفة النقل في شبكات الجيل التالي على أساس مادة مفتاح مشتركة تولّد من مادة مفتاح الدورة السابقة في TAA-FE أو AM-FE أو MMCF. ويتلقى الكيان الوظيفي لعقدة النفاذ (AN-FE) مادة مفتاح الدورة من الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) عبر الكيان الوظيفي لإدارة النفاذ (AM-FE). فإذا كان الكيان الوظيفي لإدارة النفاذ قادراً على اشتقاق مادة مفتاح الدورة، أمكن للكيان الوظيفي لعقدة النفاذ (AN-FE) الحصول على مادة مفتاح الدورة من الكيان الوظيفي لإدارة النفاذ مباشرةً. ويتلقى كيانا EN-FE وABG-FE مادة المفتاح المولّدة من الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) عبر الكيان الوظيفي لإدارة موقع النقل (TLM-FE) ووظيفة التحكم في إدارة التنقلية (MMCF) كليهما. وإذا كانت وظيفة التحكم في إدارة التنقلية (MMCF) قادرة على اشتقاق مادة مفتاح الدورة، أمكن للكيانين EN-FE وABG-FE كليهما الحصول على مادة المفتاح من هذه الوظيفة.

ويستند إجراء الاستيقان إلى بروتوكول التحدي والردّ، مثل اتفاق الاستيقان والمفاتيح (AKA) [b-3GPP TS 33.102].

2.7 الاستيقان

1.2.7 إجراء الاستيقان العام



الشكل 3 – إجراء الاستيقان العام

1) تقام قناة تحكم بين جهاز المستخدم ووظائف شبكة النفاذ (يقع هذا الإجراء خارج نطاق هذه التوصية).

2) يرسل الكيان AM-FE معلومات جهاز المستعمل إلى الكيان TAA-FE طلباً لبيانات الاستيقان.

3) يحصل الكيان TAA-FE من طلب الاستيقان على معلومات الاستيقان التي تتضمن معلومات هوية المستخدم المشترِك وشبكة النفاذ، ويتفاعل مع الكيانين TUP-FE/TLM-FE للحصول على البيانات العامة للمستخدم وعلى متجهات الاستيقان التي تتضمن أمارة (علامة) الاستيقان ومادة مفتاح الدورة.

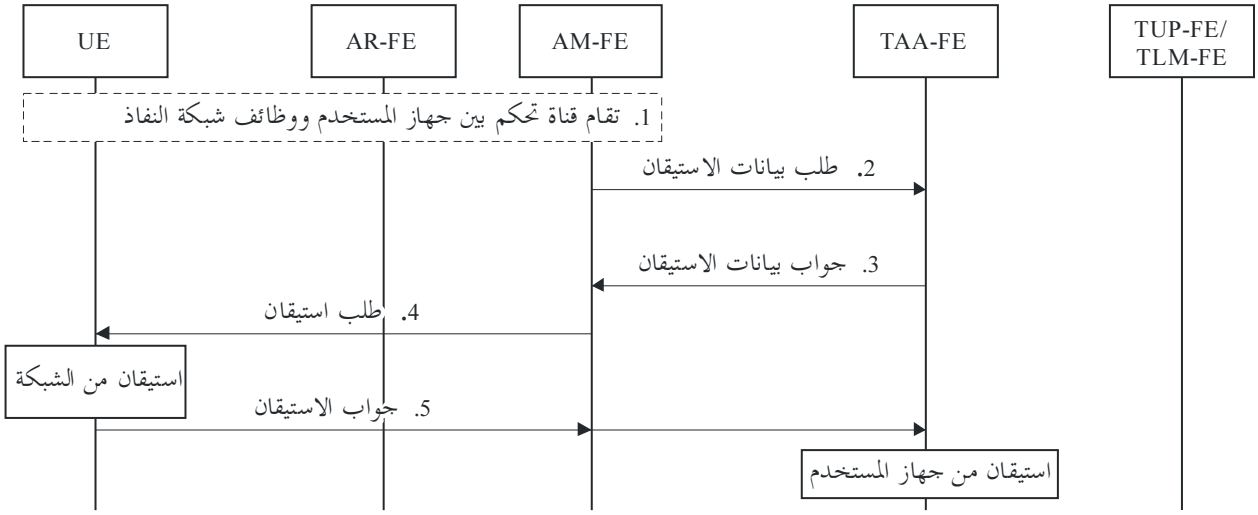
4) يرسل الكيان TAA-FE إلى الكيان AM-FE رداً ببيانات الاستيقان يتضمن أمارة الاستيقان.

5) يرسل الكيان AM-FE طلب استيقان إلى جهاز المستخدم الذي يجلب أمارة الاستيقان من طلب الاستيقان ويولد متجهات استيقان محلية تتضمن مادة مفتاح الدورة القائمة على أمارة الاستيقان ومفتاح الجذر. ويستيقن جهاز المستخدم من الشبكة بالتحقق من أمارة الاستيقان الواردة.

6) يرسل جهاز المستخدم جواب استيقان إلى الكيان AM-FE يتضمن أمارة الاستيقان التي يولدها جهاز المستخدم. ويسيّر الكيان AM-FE المعلومات إلى الكيان TAA-FE الذي يجلب أمارة الاستيقان ويراجع التحقق من أمارة الاستيقان الواردة للاستيقان من جهاز المستخدم.

2.2.7 إجراء معاودة الاستيقان السريعة العامة

تُستخدم معاودة الاستيقان السريعة لخفض كمون التمرير. ولا شأن للكيانين TUP-FE/TLM-FE في إجراء معاودة الاستيقان السريعة الذي يسرّع الاستيقان ويخفف العبء على الكيانين TUP-FE/TLM-FE. وفي شبكات الجيل التالي، يوصى بأن تدعم تجهيزات المستخدم وكيانات الاستيقان على السواء معاودة الاستيقان السريعة العامة.



Y.2760(11)_F04

الشكل 4 – إجراء معاودة الاستيقان السريعة العامة

تنفَّذ الخطوات التالية على افتراض أن جهاز المستخدم والكيان TAA-FE قادران على معاودة الاستيقان السريعة:

1) تقام قناة تحكم بين جهاز المستخدم ووظائف شبكة النفاذ (يقع هذا الإجراء خارج نطاق هذه التوصية).

2) يرسل الكيان AM-FE معلومات جهاز المستخدم إلى الكيان TAA-FE طلباً لبيانات الاستيقان.

3) يرسل الكيان TAA-FE إلى الكيان AM-FE رداً ببيانات الاستيقان يتضمن أمارة الاستيقان.

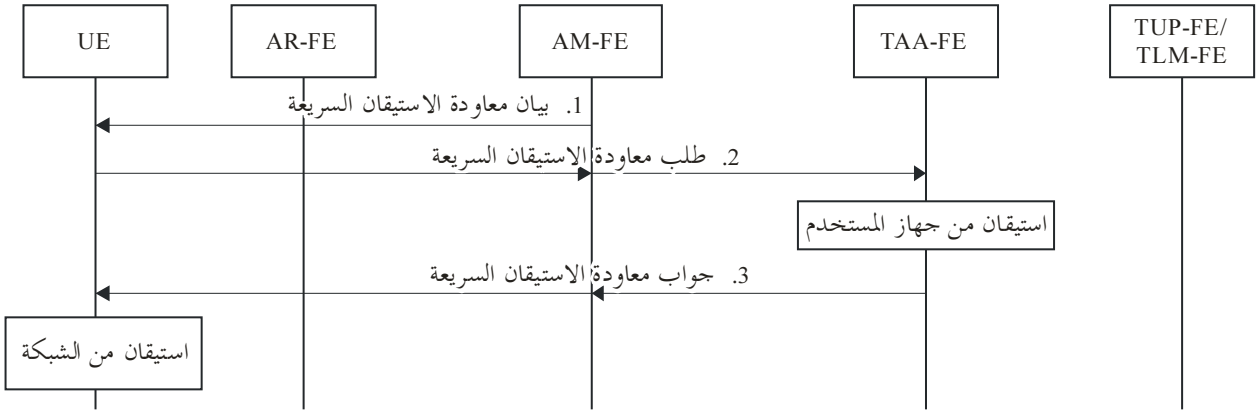
4) يرسل الكيان AM-FE طلب استيقان إلى جهاز المستخدم الذي يجلب أمارة الاستيقان من طلب الاستيقان ويولد متجهات استيقان محلية تتضمن مادة مفتاح الدورة القائمة على أمارة الاستيقان ومفتاح الجذر. ويستيقن جهاز المستخدم من الشبكة بالتحقق من أمارة الاستيقان الواردة.

5) يرسل جهاز المستخدم رد استيقان إلى الكيان AM-FE يتضمن أمارة الاستيقان التي يولدها جهاز المستخدم. ويسيّر الكيان AM-FE المعلومات إلى الكيان TAA-FE الذي يجلب أمارة الاستيقان ويراجع التحقق من أمارة الاستيقان الواردة للاستيقان من جهاز المستخدم.

وعندما يقوم جهاز المستخدم بإعادة استعمال مادة مفتاح الدورة، لا تُستخدم معلومات معاودة الاستيقان السريعة إلا للاستيقان المتبادل. أما عندما لا يقوم جهاز المستخدم بإعادة استعمال مادة مفتاح الدورة، فإن جهاز المستخدم وكيان الاستيقان (مثل TAA-FE/TUP-FE) كليهما يولدان مفتاح دورة جديد على أساس معلومات مادة مفتاح الدورة ومعاودة الاستيقان السريعة.

1.2.2.7 معاودة الاستيقان السريعة المثلى

في معاودة الاستيقان السريعة المثلى، يولّد جهاز المستخدم معلومات الاستيقان بعد أن تكون شبكة الجيل التالي قد استيقنت منه أولاً. ويختلف ذلك عن معاودة الاستيقان العامة في أن جهاز المستخدم هو الذي يستيقن أولاً من شبكة الجيل التالي التي تولد بعد ذلك أمارة الاستيقان.



Y.2760(11)_F05

الشكل 5 – إجراء معاودة الاستيقان السريعة المثلى

1) تقام قناة تحكم بين جهاز المستخدم ووظائف شبكة النفاذ (يقع هذا الإجراء خارج نطاق هذه التوصية). ويرسل كيان AM-FE بيان معاودة الاستيقان المثلى إلى جهاز المستخدم مما يشير إلى أن كيان TAA-FE يدعم معاودة الاستيقان السريعة المثلى.

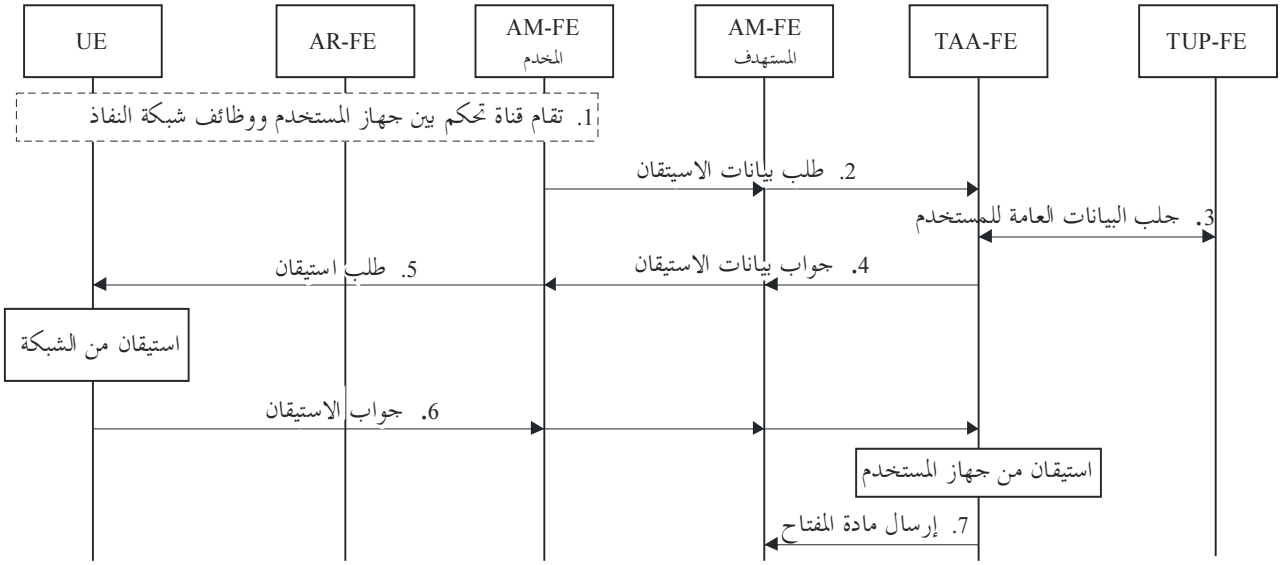
2) يولد جهاز المستخدم متّجه استيقان ويرسل طلباً لمعاودة الاستيقان المثلى إلى الكيان TAA-FE عبر الكيان AM-FE. ويشمل هذا الطلب أمارة الاستيقان ومعلومات معاودة الاستيقان. ويولد الكيان TAA-FE متجه استيقان محلي ومادة مفتاح دورة جديدة على أساس معلومات معاودة الاستيقان ومادة مفتاح الدورة. ويستيقن الكيان TAA-FE من جهاز المستخدم بالتحقق من أمارة الاستيقان الواردة.

3) يرسل الكيان TAA-FE إلى جهاز المستخدم عبر الكيان AM-FE رداً بمعاودة الاستيقان يتضمن أمارة الاستيقان. ويستيقن جهاز المستخدم من الشبكة بواسطة متجه الاستيقان الخاص بها. وبعد الانتهاء من إجراء الاستيقان بنجاح، يمكن لجهاز المستخدم أن يولد مادة مفتاح الدورة الفرعية.

3.2.7 الاستيقان ضمن الميدان

1.3.2.7 الاستيقان في توصيل بشبكة واحدة

يفيد التوصيل بشبكة واحدة أن جهاز المستخدم يمكنه أن يكشف شبكات مختلفة، ولكن لا يمكنه النفاذ إلا إلى شبكة واحدة في المرة الواحدة. ويفيد الاستيقان المسبق أن جهاز المستخدم يقوم بالاستيقان المتبادل مع الشبكة المستهدفة عبر الشبكة المخدّمة قبل أن يقوم جهاز المستخدم بالتمرير إلى الشبكة المستهدفة. وعندما يكون جهاز المستخدم قائماً على توصيل بشبكة واحدة، فإنه يلجأ إلى الاستيقان المسبق للحفاظ على استمرارية الخدمة وتخفيض الكمون. ويشابه إجراء الاستيقان المسبق إجراء الاستيقان العام. ويمكن أن يشارك كيان AM-FE المخدّم وكيان AM-FE المستهدَف في إجراء الاستيقان المسبق إذا لزم الأمر.



Y.2760(11)_F06

الشكل 6 – إجراء الاستيقان المسبق القائم على توصيل بشبكة واحدة

1) تقام قناة تحكم بين جهاز المستخدم ووظائف شبكة النفاذ (يقع هذا الإجراء خارج نطاق هذه التوصية).

2) يرسل الكيان AM-FE إلى الكيان TAA-FE طلب بيانات الاستيقان الذي يتضمن معلومات المشترك. ويسيّر كيان AM-FE المخدّم وكيان AM-FE المستهدَف طلب بيانات الاستيقان هذا.

3) يجلب كيان TAA-FE البيانات العامة للمستخدم بالتفاعل مع الكيان TUP-FE.

4) يرسل الكيان TAA-FE إلى الكيان AM-FE المستهدَف والكيان AM-FE المخدّم رداً ببيانات الاستيقان يتضمن أمارة الاستيقان.

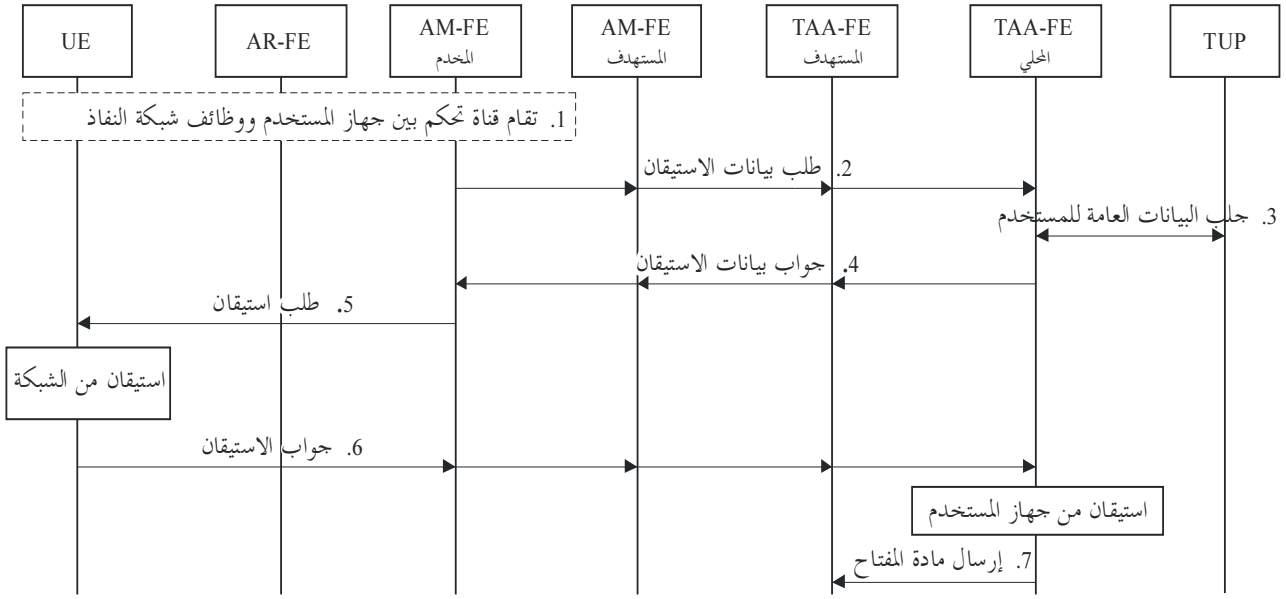
5) يرسل الكيان AM-FE المخدّم طلب استيقان إلى جهاز المستخدم الذي يجلب أمارة الاستيقان ويستيقن من الشبكة بواسطة معلومات الاستيقان لديه. وبعد الانتهاء من الاستيقان بنجاح، يولد جهاز المستخدم مادة مفتاح الدورة.

6) يرسل جهاز المستخدم رد استيقان إلى الكيان AM-FE المخدّم. ويسيّر الكيان AM-FE المخدّم المعلومات إلى الكيان AM-FE المستهدَف وإلى الكيان TAA-FE التي تتضمن أمارة الاستيقان. ويستخرج الكيان TAA-FE أمارة الاستيقان ويستيقن من جهاز المستخدم. وبعد الانتهاء من الاستيقان بنجاح، يولد الكيان TAA-FE مادة مفتاح الدورة التي يمكن أن تشتق مادة مفتاح الدورة الفرعية إذا لزم الأمر.

7) يرسل الكيان TAA-FE إلى الكيان AM-FE المستهدَف مادة المفتاح التي ستُستخدم بعد أن ينفذ جهاز المستخدم التمرير إلى الشبكة المستهدَفة من أجل حماية الاتصالات بين جهاز المستخدم والشبكة المستهدفة.

4.2.7 الاستيقان بين الميادين

إن اختلاف الميادين الإدارية يعني اختلاف موّردي شبكات الجيل التالي. ويرد أدناه وصف لإجراء الاستيقان من أجل تمرير جهاز المستخدم ما بين ميادين إدارية مختلفة.



Y.2760(11)_F07

الشكل 7 – إجراء الاستيقان بين الميادين المختلفة

1) تقام قناة تحكم بين جهاز المستخدم ووظائف شبكة النفاذ (يقع هذا الإجراء خارج نطاق هذه التوصية).

2) يرسل الكيان AM-FE إلى الكيان TAA-FE المحلي طلب بيانات الاستيقان الذي يتضمن معلومات المشترك. ويسيّر كيان AM-FE المستهدَف وكيان TAA-FE المستهدَف طلب بيانات الاستيقان هذا. ويجلب كيان TAA-FE المحلي البيانات العامة للمستخدم بالتفاعل مع الكيان TUP-FE.

3) يجلب كيان TAA-FE البيانات العامة للمستخدم بالتفاعل مع الكيان TUP-FE.

4) يرسل الكيان TAA-FE المحلي إلى الكيان AM-FE المخدّم رداً ببيانات الاستيقان يتضمن أمارة الاستيقان. ويقوم كيانا TAA-FE وAM-FE المستهدفان بتسيير طلب بيانات الاستيقان.

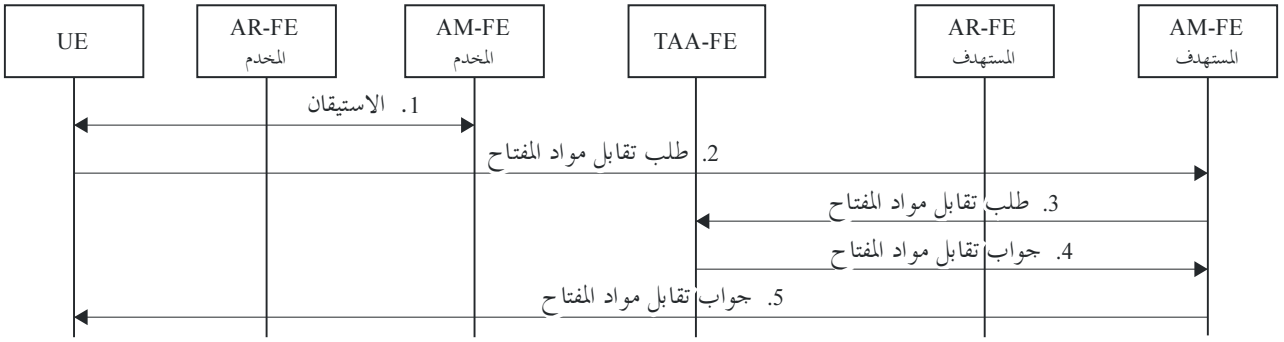
5) يرسل الكيان AM-FE المخدّم طلب استيقان إلى جهاز المستخدم الذي يجلب أمارة الاستيقان ويستيقن من الشبكة بواسطة معلومات الاستيقان لديه. وبعد الانتهاء من الاستيقان بنجاح، يولد جهاز المستخدم مادة مفتاح الدورة.

6) يرسل جهاز المستخدم إلى الكيان TAA-FE المحلي رد استيقان يتضمن أمارة الاستيقان. ويستخرج الكيان TAA-FE المحلي أمارة الاستيقان ويستيقن من جهاز المستخدم. وبعد الانتهاء من الاستيقان بنجاح، يولد الكيان TAA-FE المحلي مادة مفتاح الدورة التي يمكن استخدامها لاشتقاق مادة مفتاح الدورة الفرعية إذا لزم الأمر.

7) بعد الانتهاء من الاستيقان بنجاح، يرسل الكيان TAA-FE المحلي إلى الكيان AM-FE المستهدَف مادة المفتاح التي ستُستخدم بعد أن ينفذ جهاز المستخدم التمرير من الشبكة المخدمة إلى الشبكة المستهدَفة من أجل حماية الاتصالات بين جهاز المستخدم والشبكة المستهدفة.

5.2.7 آلية تقابل مادة المفتاح في الاستيقان

عندما ينتقل جهاز المستخدم من شبكة مخدمة إلى شبكة مستهدَفة، ينفّذ الاستيقان المتبادل وتولد مادة مفتاح الدورة. وإذ تدعم شبكات الجيل التالي آليات مختلفة لاشتقاق المفتاح، يُستخدم تقابل مادة المفتاح لهذه الآليات المختلفة.



Y.2760(11)_F08

الشكل 8 – إجراء تقابل مادة المفتاح

1) يقام التوصيل بين جهاز المستخدم وكيان TAA-FE، وينتهي إجراء الاستيقان، وتولَّد مادة مفتاح الدورة.

2) يكتشف جهاز المستخدم الشبكة المستهدَفة ويحضّر للتمرير إلى الشبكة المستهدَفة. ويرسل جهاز المستخدم طلب تقابل مادة المفتاح إلى كيان AM-FE المستهدَف. ويتضمن هذا الطلب معلومات تقابُل مثل آلية اشتقاق المفتاح الحالي وآلية اشتقاق المفاتيح المدعومة.

3) يرسل الكيان AM-FE المستهدف إلى الكيان TAA-FE طلب تقابل مادة المفتاح.

4) يتلقى الكيان TAA-FE طلب تقابل مادة المفتاح، ويقيم التقابل بين مادة المفتاح في الشبكة المخدمة وبين مادة المفتاح في الشبكة المستهدَفة، ويرسل رداً بتقابل مادة المفتاح إلى الكيان AM-FE المستهدَف.

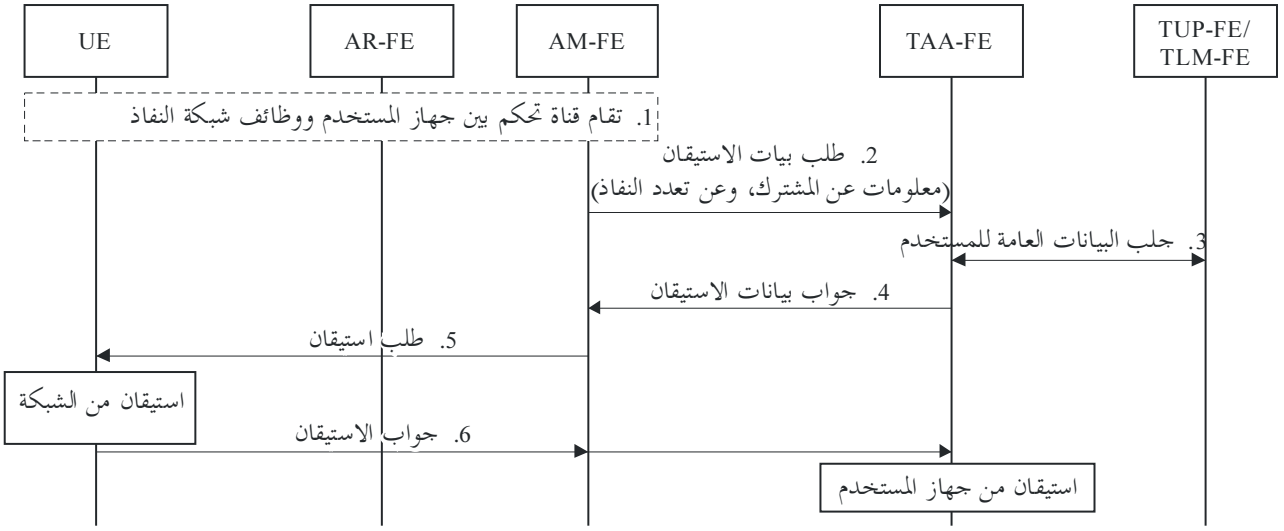
5) يرسل الكيان AM-FE المستهدَف رد التقابل إلى جهاز المستخدم الذي يقيم التقابل بين مادة المفتاح في الشبكة المخدّمة وبين مادة المفتاح في الشبكة المستهدَفة. ويشترك جهاز المستخدم مع الكيان TAA-FE في مادة المفتاح في الشبكة المستهدَفة، التي تستخدم لحماية الحركة بين جهاز المستخدم والشبكة المستهدَفة.

6.2.7 تعدد النفاذ إلى الشبكة على أساس الاستيقان

يُقصد بتعدد النفاذ إلى الشبكة على أساس الاستيقان قدرة جهاز المستخدم على الاتصال مع شبكات نفاذ متعددة في وقت واحد. وعندما يكون لجهاز المستخدم قدرة على النفاذ إلى عدة شبكات يوصل جهاز المستخدم بالشبكة المستهدفة وينفذ إجراء الاستيقان المتبادل قبل فصل الشبكة المخدّمة. والاستيقان المتبادل هو استيقان عام على النحو المبين في الشكل 3. وبعد الانتهاء من الاستيقان المتبادل بنجاح، يولد جهاز المستخدم والكيان TAA-FE كلاهما مادة مفتاح دورة مشتركة، ويرسل الكيان TAA-FE مادة مفتاح الدورة إلى الكيان AM-FE المستهدَف. وعندما ينتقل جهاز المستخدم إلى الشبكة المستهدَفة، تكون الحركة بين جهاز المستخدم والشبكة المستهدَفة محمية بمادة مفتاح الدورة أو بمادة مفتاح الدورة الفرعية.

7.2.7 الاستيقان القائم على تعدد التوصيل

يقصد بتعدد التوصيل احتفاظ جهاز المستخدم بأكثر من توصيل واحد بالشبكة في وقت واحد. ويتيح اختلاف أنماط التوصيلات بالشبكة حالات تعاطٍ مختلفة للمستخدم، مثل عرض النطاق العريض وانخفاض التأخير الزمني وإجراءات الأمن المشددة. أما حالة تعدد التوصيلات بميادين إدارية مختلفة، فهي تقع خارج نطاق هذه التوصية.



Y.2760(11)_F09

الشكل 9 – الاستيقان القائم على تعدد التوصيل

1) تقام قناة تحكم بين جهاز المستخدم ووظائف شبكة النفاذ (يقع هذا الإجراء خارج نطاق هذه التوصية). ويحصل جهاز المستخدم على المعلومات من شبكة النفاذ مع بيان بدعم استيقان النفاذ المتعدد.

2) يرسل الكيان AM-FE إلى الكيان TAA-FE طلب بيانات الاستيقان الذي يتضمن معلومات جهاز المستخدم مثل معلومات المشترك (كهوية المستخدم المشترك)؛ ومعلومات تعدد النفاذ (كمؤشر تعدد النفاذ وهوية السطح البيني لتعدد النفاذ).

3) يحصل الكيان TAA-FE على معلومات الاستيقان، ويتفاعل مع الكيانين TUP-FE/TLM-FE للحصول على البيانات العامة للمستخدم وعلى متجه الاستيقان الذي يولَّد في الكيانين TUP-FE/TLM-FE ويتضمن أمارة الاستيقان.

4) يرسل الكيان TAA-FE إلى الكيان AM-FE رداً ببيانات الاستيقان يتضمن أمارة الاستيقان.

5) يرسل الكيان AM-FE طلب استيقان إلى جهاز المستخدم الذي يولد أمارات الاستيقان المحلية على أساس معلومات الاستيقان في رسالة طلب الاستيقان. ويستيقن جهاز المستخدم من الشبكة بالتدقيق في صلاحية أمارة الاستيقان الواردة وفقاً لأمارات الاستيقان المحلية. وبعد الانتهاء من الاستيقان بنجاح، يولد جهاز المستخدم مادة مفتاح الدورة على أساس معلومات الاستيقان. فإذا ضُبط مؤشر تعدد النفاذ، يولد جهاز المستخدم مواد متعددة لمفتاح الدورة على أساس معلومات تعدد النفاذ.

6) يرسل جهاز المستخدم رسالة جواب الاستيقان إلى الكيان AM-FE. ويسيّر الكيان AM-FE إلى الكيان TAA-FE المعلومات التي تتضمن أمارة الاستيقان التي يولدها جهاز المستخدم. ويجلب الكيان TAA-FE أمارة الاستيقان في رسالة جواب الاستيقان ويستيقن من جهاز المستخدم على أساس متجه الاستيقان في الكيان TAA-FE. وبعد الانتهاء من الاستيقان بنجاح، يولد الكيان TAA-FE مادة مفتاح الدورة على أساس أمارة الاستيقان. فإذا ضُبط مؤشر تعدد النفاذ، يولد الكيان TAA-FE مواد متعددة لمفتاح الدورة على أساس معلومات تعدد النفاذ.

8 إنشاء سياق الأمن

1.8 نقل سياق الأمن بين كيان AM-FE المخدّم وكيان AM-FE المستهدَف

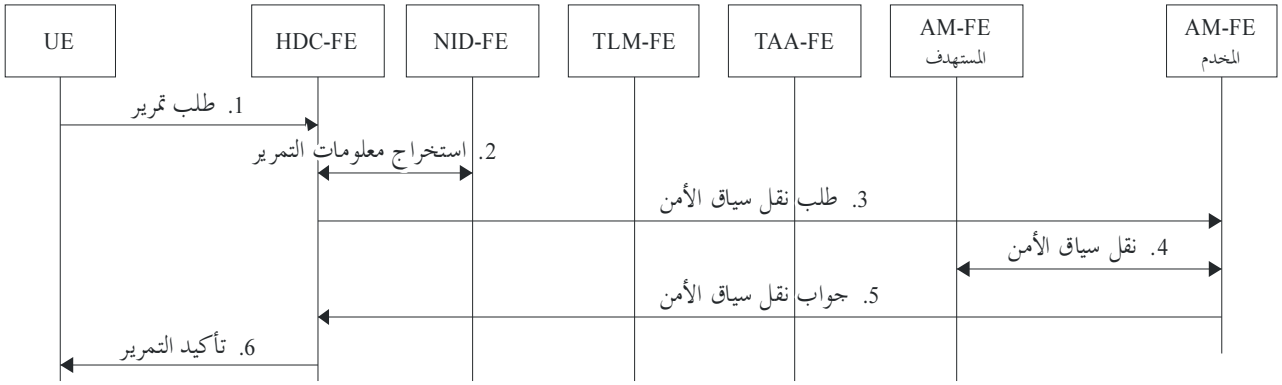
ينبغي حماية حركة نقل سياق الأمن بين كيان AM-FE المخدّم وكيان AM-FE المستهدَف. ويتحقق الأمن بينهما من خلال إنشاء رابطة أمنية يمكن الاستغناء عنها إذا كانا في المنطقة نفسها. أما إذا كانا في منطقتين مختلفتين كميداني تشغيل مختلفين، فتُنشأ الرابطة الأمنية عن طريق آلية الأمن وسياسة أو اتفاق المشغّل.

2.8 نقل سياق الأمن بين كيان AR-FE المخدّم وكيان AR-FE المستهدَف

يتعين حماية حركة نقل سياق الأمن بين كيان AR-FE المخدّم وكيان AR-FE المستهدَف، عندما يقوم جهاز المستخدم بالتمرير بينهما. ويتحقق أمن نقل سياق الأمن بينهما من خلال إنشاء رابطة أمنية.

3.8 نقل سياق الأمن بين جهاز المستخدم والكيان HDC-FE

1.3.8 نقل سياق الأمن بمبادرة من المضيف



الشكل 10 – إجراء نقل سياق الأمن بمبادرة من المضيف

عندما يقرر جهاز المستخدم إنجاز تمرير من الشبكة المخدّمة إلى الشبكة المستهدَفة، يقوم بإرسال طلب تمرير إلى الكيان HDC-FE مما يطلق نقلاً لسياق الأمن. وبعد الانتهاء من نقل سياق الأمن، يستخدم الكيان AM-FE المستهدَف سياق الأمن لحماية الحركة بين جهاز المستخدم والشبكة المستهدَفة، وفق الخطوات التالية:

1) يرسل جهاز المستخدم طلب تمرير إلى الكيان HDC-FE.

2) يتلقى الكيان HDC-FE طلب التمرير، ويتفاعل مع الكيان NID-FE للحصول على المعلومات ذات الصلة بالتمرير.

3) يسيّر الكيان HDC-FE طلب التمرير بما فيه المعلومات ذات الصلة بالتمرير إلى الكيان AM-FE المخدّم.

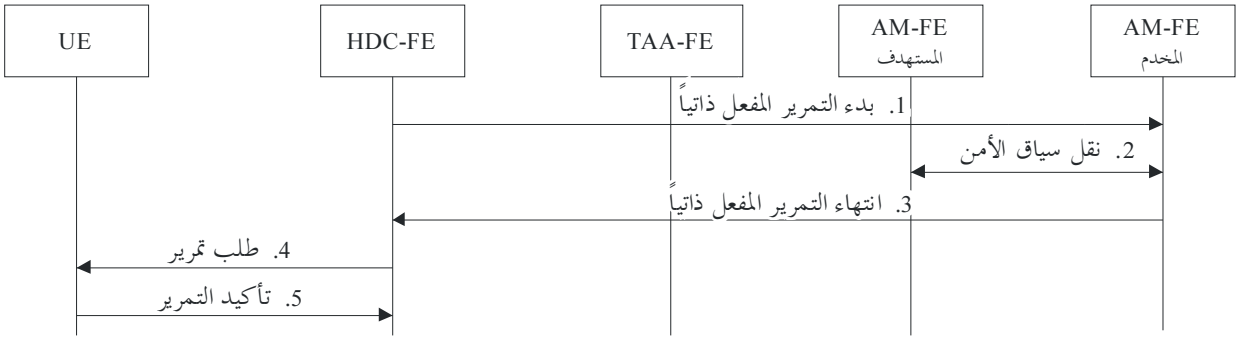
4) يتفاعل الكيان AM-FE المخدّم مع الكيان AM-FE المستهدَف لنقل سياق الأمن.

5) عند الانتهاء من نقل سياق الأمن، يرسل الكيان AM-FE المخدّم رداً بنقل سياق الأمن إلى الكيان HDC-FE.

6) يتلقى الكيان HDC-FE الردّ بنقل سياق الأمن. وبعد الانتهاء من نقل سياق الأمن بنجاح، يرسل الكيان HDC-FE رسالة تأكيد التمرير إلى جهاز المستخدم.

2.3.8 نقل سياق الأمن بمبادرة من الشبكة

عندما يقرر الكيان HDC-FE أن يوعز لجهاز المستخدم بإنجاز تمرير من الشبكة المخدّمة إلى الشبكة المستهدَفة، يرسل هذا الكيان رسالة تمرير مفعّلة ذاتياً لإطلاق نقل سياق الأمن. وبعد الانتهاء من نقل سياق الأمن، يستخدم الكيان AM-FE المستهدَف سياق الأمن لحماية الحركة بين جهاز المستخدم والشبكة المستهدَفة.



الشكل 11 – إجراء نقل سياق الأمن بمبادرة من الشبكة

1) يتأهب الكيان HDC-FE لإجراء التمرير ويرسل رسالة البدء بتمرير مفعّل ذاتياً إلى الكيان AM-FE المخدّم لإطلاق نقل لسياق الأمن.

2) يتفاعل الكيان AM-FE المخدّم مع الكيان AM-FE المستهدَف لنقل سياق الأمن.

3) عند الانتهاء من نقل سياق الأمن، يرسل الكيان AM-FE المخدّم إلى الكيان HDC-FE رسالة انتهاء التمرير المفعّل ذاتياً.

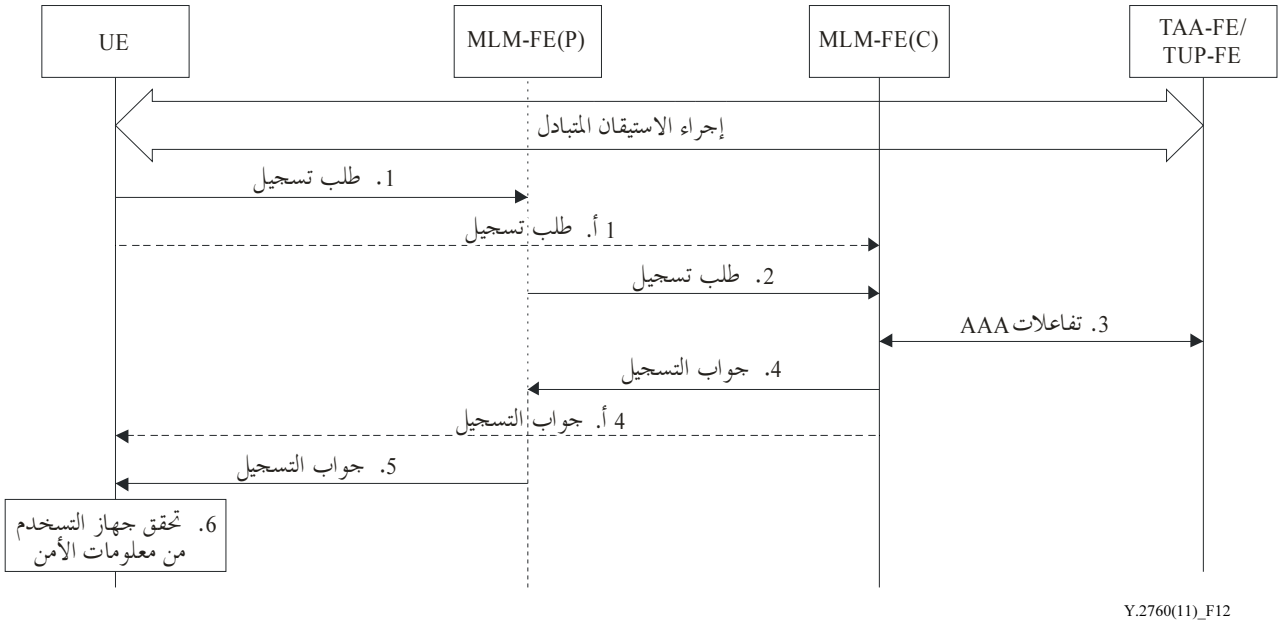
4) عندما يتلقى الكيان HDC-FE رسالة انتهاء التمرير المفعّل ذاتياً، يباشر بإجراء التمرير مرسلاً طلب التمرير إلى جهاز المستخدم.

5) يرسل جهاز المستخدم رسالة تأكيد التمرير عند انتهاء التمرير.

9 أمن التنقلية في بروتوكول الإنترنت

1.9 أمن التنقلية المستندة إلى المضيف

يتعين حماية حركة التحكم في التنقلية المستندة إلى المضيف بين جهاز المستخدم والكيان الوظيفي لإدارة الموقع المتنقل مركزياً (MLM-FE (C)). ويتعين إنشاء رابطة أمنية (SA) بينهما. أما الرابطة الأمنية بين جهاز المستخدم والكيان الوظيفي لإدارة الموقع المتنقل بالوكالة (MLM-FE (P)) فهي اختيارية.



الشكل 12 – إجراء التنقلية المستندة إلى المضيف

تنفَّذ الخطوات التالية على افتراض أن جهاز المستخدم والكيان TAA-FE قد أنهيا إجراء الاستيقان العام:

1) يرسل جهاز المستخدم إلى الكيان MLM-FE(P) طلب تسجيل يتضمن معلومات الأمن بين جهاز المستخدم والكيان MLM-FE(C) ومعلومات الأمن بين جهاز المستخدم والكيان MLM-FE(P).

- 1أ – إن لم يكن الكيان MLM-FE(P) موجوداً، يرسل جهاز المستخدم طلب التسجيل إلى الكيان MLM-FE(C) مباشرةً.

2) يتحقق الكيان MLM-FE(P) من معلومات الأمن بين جهاز المستخدم والكيان MLM-FE(P) ويسيّر طلب التسجيل إلى الكيان MLM-FE(C). ويمكن للكيان MLM-FE(P) أن يضيف إلى رسالة جواب التسجيل قبل تسييرها معلومات بشأن الأمن بين الكيانين MLM-FE(P) وMLM-FE(C).

3) يتفاعل الكيان MLM-FE(C) مع الكيانين TAA-FE/TUP-FE للحصول على معلومات الاستيقان ومعلومات التخويل.

4) يتحقق الكيان MLM-FE(C) من معلومات الأمن بين جهاز المستخدم والكيان MLM-FE(C) في طلب التسجيل. ويرسل الكيان MLM-FE(C) إلى الكيان MLM-FE(P) جواب التسجيل ومعلومات الأمن. وقد يتضمن جواب التسجيل معلومات الأمن بين جهاز المستخدم والكيان MLM-FE(C) ومعلومات الأمن بين الكيانين MLM-FE(P) وMLM-FE(C).

- 4أ – إن لم يكن الكيان MLM-FE(P) موجوداً، يرسل الكيان MLM-FE(C) جواب التسجيل إلى جهاز المستخدم مباشرةً. وقد يتضمن جواب التسجيل معلومات الأمن بين جهاز المستخدم والكيان MLM-FE(C).

5) يتحقق الكيان MLM-FE(P) من معلومات الأمن بين الكيانين MLM-FE(P) وMLM-FE(C) ويرسل جواب التسجيل إلى جهاز المستخدم. ويمكن للكيان MLM-FE(P) أن يضيف إلى رسالة جواب التسجيل قبل تسييرها معلومات بشأن الأمن بين جهاز المستخدم والكيان MLM-FE(P).

6) يتحقق الكيان MLM-FE(C) من معلومات الأمن بين جهاز المستخدم والكيان MLM-FE(C) ويقيم رابطة أمنية بين جهاز المستخدم والكيان MLM-FE(C). فإذا كان الكيان MLM-FE(P) موجوداً، يتحقق جهاز المستخدم من معلومات الأمن بين جهاز المستخدم والكيان MLM-FE(P) ويقيم رابطة أمنية بينهما.

2.9 أمن التنقلية القائم على الشبكة

إن حماية حركة التحكم في التنقلية القائمة على الشبكة بين كياني شبكة في منطقة موثوقة، أو موثوقة ولكن تشوبها نقاط ضعف، تُعتبر أمراً اختيارياً يستند إلى سياسة المشغل. وآليات أمن حركة التحكم في التنقلية القائمة على الشبكة تقوم على آليات الأمن الواردة في التوصية [ITU-T Y.2704].

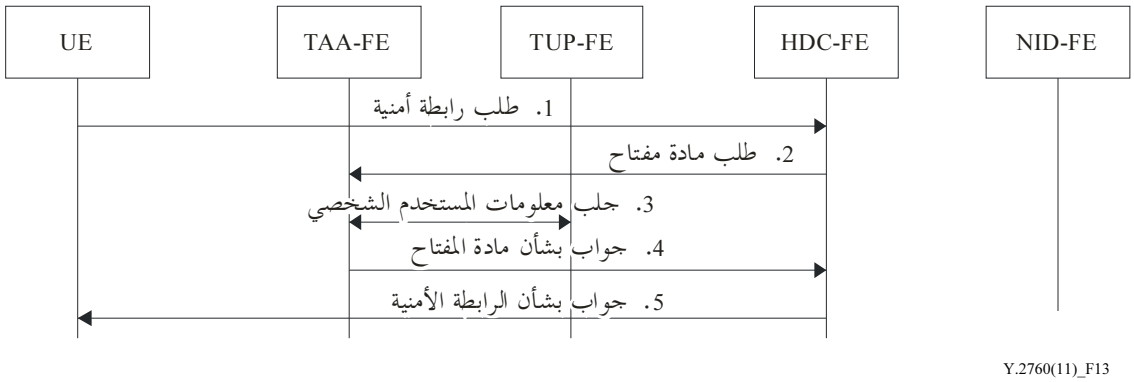
10 الأمن بين جهاز المستخدم (UE) والكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE)

يُستخدم تدفق المعلومات بين جهاز المستخدم (UE) والكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE) لحمل المعلومات اللازمة لاتخاذ قرار التمرير. وينبغي لجهاز المستخدم والكيان HDC-FE إقامة رابطة أمنية لحماية تدفق المعلومات بينهما.

1.10 إقامة رابطة أمنية بمبادرة من المضيف بين جهاز المستخدم (UE) والكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE)

ينطوي إجراء إقامة رابطة أمنية بمبادرة من المضيف على أن يفعّل جهاز المستخدم الإجراء لإنشاء رابطة أمنية بين جهاز المستخدم والكيان HDC-FE على النحو المبين في الشكل 13. وهناك شرطان مسبقان لإقامة رابطة أمنية بمبادرة من المضيف بين جهاز المستخدم والكيان HDC-FE. أولهما، التشارك المسبق لجهاز المستخدم والكيان TAA-FE في مادة المفتاح، الأمر الذي يمكن تحقيقه بعد إجراء الاستيقان المتبادل. وثانيهما، معرفة جهاز المستخدم بمعلومات عن الكيان HDC-FE كالعنوان الذي يمكن لجهاز المستخدم أن يرسل إلى الكيان HDC-FE بموجبه طلب الرابطة الأمنية. أما كيفية حصول جهاز المستخدم

على معلومات عن الكيان HDC-FE فهي خارج نطاق هذه التوصية. وتُستخدم إدارة موقع النقل (TLM-FE) لترحيل معلومات مادة المفتاح من وإلى الكيان TAA-FE، وهي محذوفة في الأشكال التالية.



الشكل 13 – إجراء إقامة رابطة أمنية بمبادرة من المضيف

1) يولد جهاز المستخدم مادة المفتاح المشتركة لإنشاء رابطة مع الكيان HDC-FE وفقاً لمعلومات الاستيقان. ويرسل جهاز المستخدم إلى الكيان HDC-FE طلب رابطة أمنية يتضمن معلومات الاستيقان ومعلومات عن جهاز المستخدم.

2) يرسل الكيان HDC-FE إلى الكيان TAA-FE طلب مادة مفتاح يتضمن معلومات عن الكيان HDC-FE ومعلومات الاستيقان ومعلومات عن جهاز المستخدم.

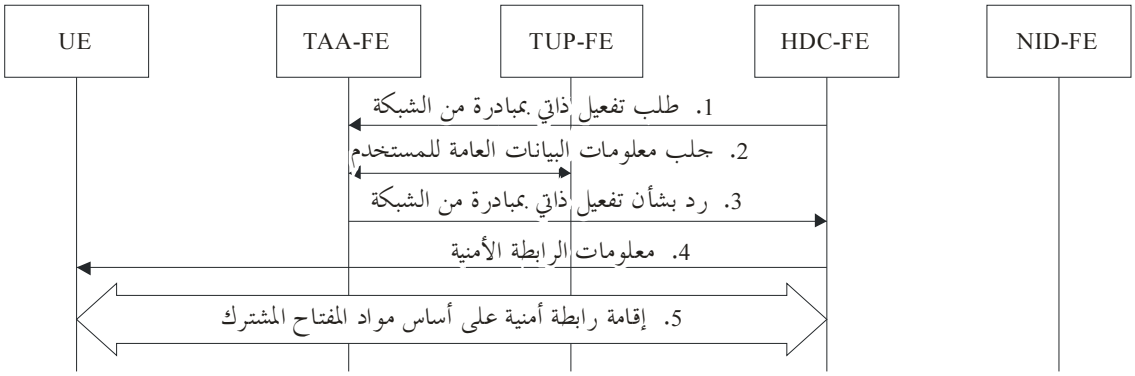
3) يجلب الكيان TAA-FE معلومات البيانات العامة للمستخدم بالتفاعل مع الكيان TUP-FE ويتحقق من أن الكيان HDC-FE مخول بإنشاء رابطة أمنية مع جهاز المستخدم.

4) يولد الكيان TAA-FE مادة المفتاح للكيان HDC-FE وفقاً لمعلومات الاستيقان ومعلومات عن الكيان HDC-FE وعن جهاز المستخدم، وذلك عندما يكون الكيان HDC-FE مخولاً بإنشاء رابطة أمنية مع جهاز المستخدم. ويرسل الكيان TAA-FE إلى الكيان HDC-FE رداً بمادة المفتاح يتضمن معلومات كمادة المفتاح للكيان HDC-FE وعمر هذا المفتاح.

5) يرسل الكيان HDC-FE رداً بالرابطة الأمنية إيذاناً بإقامتها بين جهاز المستخدم والكيان HDC-FE.

2.10 إقامة رابطة أمنية بمبادرة من الشبكة بين جهاز المستخدم (UE) والكيان الوظيفي المعني بقرار التحكم في التمرير (HDC-FE)

يُقصد بإجراء إقامة رابطة أمنية بمبادرة من الشبكة أن يفعّل جانب الشبكة الإجراء لإنشاء رابطة أمنية بين جهاز المستخدم والكيان HDC-FE على النحو المبين في الشكل 14. وهناك شرطان مسبقان لإقامة رابطة أمنية بمبادرة من الشبكة بين جهاز المستخدم والكيان HDC-FE. أولهما، تشارك جهاز المستخدم والكيان TAA-FE في مادة المفتاح، الأمر الذي يمكن تحقيقه بعد إجراء الاستيقان المتبادل. وثانيهما، معرفة الكيان HDC-FE بمعلومات عن جهاز المستخدم، كمعلومات عن المشترك أو عن الموقع التي يمكن أن يرسل الكيان HDC-FE بموجبها طلب الرابطة الأمنية إلى جهاز المستخدم. أما كيفية حصول الكيان HDC-FE على معلومات عن جهاز المستخدم، فهي خارج نطاق هذه التوصية.



Y.2760(11)_F14

الشكل 14 – إجراء إقامة رابطة أمنية بمبادرة من الشبكة

1) يرسل الكيان HDC-FE إلى الكيان TAA-FE طلب تفعيل ذاتي بمبادرة من الشبكة يتضمن معلومات عن الكيان HDC-FE وعن جهاز المستخدم.

2) يجلب الكيان TAA-FE البيانات العامة للمستخدم بالتفاعل مع الكيان TUP-FE ويتحقق من أن الكيان HDC-FE مخول بمباشرة إنشاء رابطة أمنية مع جهاز المستخدم.

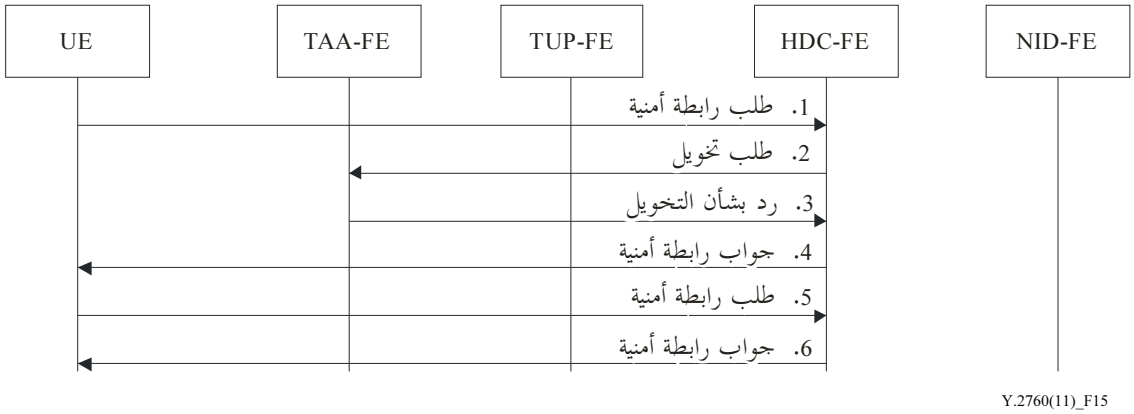
3) يولّد الكيان TAA-FE مادة المفتاح للكيان HDC-FE وفقاً لمعلومات عن الكيان HDC-FE وعن جهاز المستخدم، وذلك عندما يكون الكيان HDC-FE مخولاً بمباشرة إنشاء رابطة أمنية مع جهاز المستخدم. ويرسل الكيان TAA-FE إلى الكيان HDC-FE رداً بشأن تفعيل ذاتي بمبادرة من الشبكة يتضمن معلومات كمادة المفتاح للكيان HDC-FE وعمر هذا المفتاح.

4) يرسل الكيان HDC-FE إلى جهاز المستخدم معلومات عن الرابطة الأمنية تتضمن معلومات الاستيقان، وذلك من أجل إنشاء رابطة أمنية.

5) يولد جهاز المستخدم مادة المفتاح للكيان HDC-FE وفقاً لمعلومات الاستيقان الواردة في معلومات الرابطة الأمنية، ويتحقق من معلومات الرابطة الأمنية. وتقام الرابطة الأمنية بين الكيان HDC-FE وجهاز المستخدم.

3.10 إقامة الرابطة الأمنية مسبقاً بين جهاز المستخدم والكيان HDC-FE على أساس البنية التحتية للمفاتيح العمومية (PKI)

يبيَّن في الشكل 15 إجراء إقامة الرابطة الأمنية بين جهاز المستخدم والكيان HDC-FE على أساس البنية التحتية للمفاتيح العمومية (PKI). والشرط المسبق لإجراء إقامة الرابطة الأمنية هو معرفة جهاز المستخدم بمعلومات عن الكيان HDC-FE، كالعنوان الذي يمكن لجهاز المستخدم أن يرسل إلى الكيان HDC-FE بموجبه طلب الرابطة الأمنية. أما كيفية حصول جهاز المستخدم على معلومات عن الكيان HDC-FE فهي خارج نطاق هذه التوصية.



الشكل 15 – إجراء إقامة الرابطة الأمنية على أساس البنية التحتية للمفاتيح العمومية (PKI)

1) يرسل جهاز المستخدم إلى الكيان HDC-FE طلب رابطة أمنية يتضمن شهادة جهاز المستخدم ومعلومات عن هذا الجهاز.

2) يتحقق الكيان HDC-FE من شهادة جهاز المستخدم ويرسل إلى الكيان TAA-FE طلب تخويل يتضمن معلومات عن جهاز المستخدم وعن الكيان HDC-FE.

3) يتحقق الكيان TAA-FE من التخويل على أساس معلومات عن جهاز المستخدم وعن الكيان HDC-FE. فإذا كان الجهاز مخولاً باستخدام الكيان HDC-FE، يرسل الكيان TAA-FE إلى الكيان HDC-FE رداً بالتخويل يتضمن معلومات التخويل وشهادة المخدّم.

4) يتلقى الكيان HDC-FE معلومات التخويل ويرسل إلى جهاز المستخدم رداً بشأن الرابطة الأمنية يتضمن شهادة المخدّم.

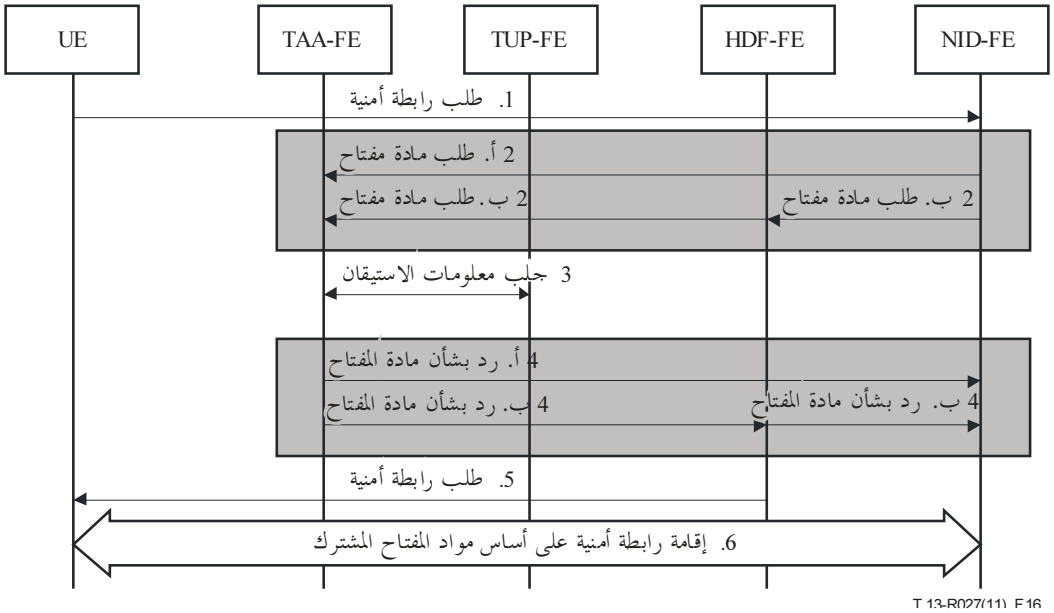
5) إذا دعت الحاجة للتشارك في مادة المفتاح بين جهاز المستخدم والكيان TAA-FE، يرسل هذا الكيان إلى الجهاز معلومات توليد المفتاح المذكورة في الخطوة 4. ويولد جهاز المستخدم مادة المفتاح المشترك على أساس ما يرد من معلومات بشأن توليد المفتاح وتوليد المفتاح المحلي. ويرسل جهاز المستخدم معلومات بشان توليد المفتاح المحلي إلى الكيان HDC-FE.

6) يولد الكيان HDC-FE مادة المفتاح على أساس ما يرد من معلومات بشأن توليد المفتاح وتوليد المفتاح المحلي. ويرسل الكيان HDC-FE إلى جهاز المستخدم رداً بإقامة الرابطة الأمنية بين جهاز المستخدم والكيان HDC-FE.

11 الأمن بين جهاز المستخدم والكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE)

1.11 إقامة رابطة أمنية بمبادرة من المضيف بين جهاز المستخدم والكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE)

يبيَّن إجراء إقامة رابطة أمنية بمبادرة من المضيف بين جهاز المستخدم والكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE) في الشكل 16. وهناك شرطان مسبقان لإقامة هذه الرابطة الأمنية: 1) التشارك المسبق لجهاز المستخدم والكيان TAA-FE في مادة المفتاح، الأمر الذي يمكن تحقيقه بعد إجراء الاستيقان المتبادل. 2) معرفة جهاز المستخدم بمعلومات عن الكيان NID-FE، كالعنوان الذي يمكن لجهاز المستخدم أن يرسل إلى الكيان NID-FE بموجبه طلب الرابطة الأمنية. أما كيفية حصول جهاز المستخدم على معلومات عن الكيان NID-FE فهي خارج نطاق هذه التوصية.



Y.2760(11)_F16

الشكل 16 – إقامة رابطة أمنية بمبادرة من المضيف

1) يرسل جهاز المستخدم إلى الكيان NID-FE طلب رابطة أمنية.

2) يرسل الكيان NID-FE إلى الكيان TAA-FE طلب مادة مفتاح يتضمن معلومات عن الكيان NID-FE ومعلومات عن جهاز المستخدم. وعندما لا يدعم الكيان NID-FE إرسال طلب استيقان إلى الكيان TAA-FE مباشرةً، يرسل الكيان NID-FE طلب استيقان إلى الكيان TAA-FE عبر الكيان HDC-FE.

3) يتفاعل الكيان TAA-FE مع الكيان TUP-FE ويولد مادة المفتاح للكيان NID-FE.

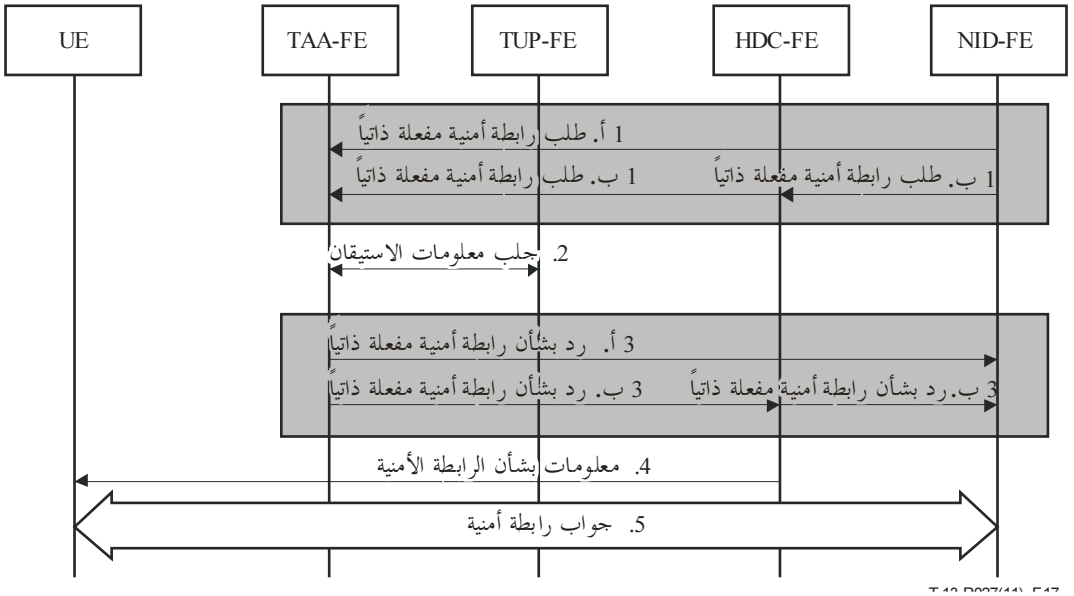
4) يرسل الكيان TAA-FE إلى الكيان HDC-FE رداً بمادة المفتاح يتضمن معلومات الاستيقان التي تشمل مادة المفتاح المشترك وعمر هذا المفتاح. وعندما لا يدعم استيقان النقل وتخويله (TAA-FE) إرسال طلب استيقان إلى الكيان NID-FE مباشرة، يرسل الكيان TAA-FE طلب استيقان إلى الكيان NID-FE عبر الكيان HDC-FE.

5) يرسل الكيان NID-FE إلى جهاز المستخدم رداً بشأن الرابطة الأمنية يتضمن معلومات الاستيقان. ويكون الرد محمياً بمادة المفتاح المشترك.

6) يولد جهاز المستخدم مادة المفتاح المشترك ويتحقق من جواب الرابطة الأمنية. وتقام الرابطة الأمنية من جانب الكيان NID-FE وجهاز المستخدم على أساس مادة المفتاح المشترك.

2.11 إقامة رابطة أمنية بمبادرة من الشبكة بين جهاز المستخدم والكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE)

يبيَّن إجراء إقامة رابطة أمنية بمبادرة من الشبكة بين جهاز المستخدم والكيان الوظيفي لتوزيع معلومات الشبكة (NID-FE) في الشكل 17. وهناك شرطان مسبقان للإجراء المتعلق بإقامة هذه الرابطة الأمنية: 1) التشارك المسبق لجهاز المستخدم والكيان TAA-FE في مادة المفتاح، الأمر الذي يمكن تحقيقه بعد إجراء الاستيقان المتبادل. 2) معرفة جهاز المستخدم بمعلومات عن الكيان NID-FE، كالعنوان الذي يمكن لجهاز المستخدم أن يرسل إلى الكيان NID-FE بموجبه طلب الرابطة الأمنية. أما كيفية حصول جهاز المستخدم على معلومات عن الكيان NID-FE فهي خارج نطاق هذه التوصية.



Y.2760(11)_F17

الشكل 17 – إقامة رابطة أمنية بمبادرة من الشبكة

1) يرسل الكيان NID-FE إلى الكيان TAA-FE طلب رابطة أمنية مفعلة ذاتياً يتضمن معلومات عن الكيان NID-FE. وعندما لا يدعم الكيان NID-FE إرسال طلب رابطة أمنية مفعلة ذاتياً إلى الكيان TAA-FE مباشرةً، يرسل الكيان NID-FE طلب رابطة أمنية مفعلة ذاتياً إلى الكيان TAA-FE عبر الكيان HDC-FE.

2) يتفاعل الكيان TAA-FE مع الكيان TUP-FE ويولد مادة المفتاح للكيان NID-FE.

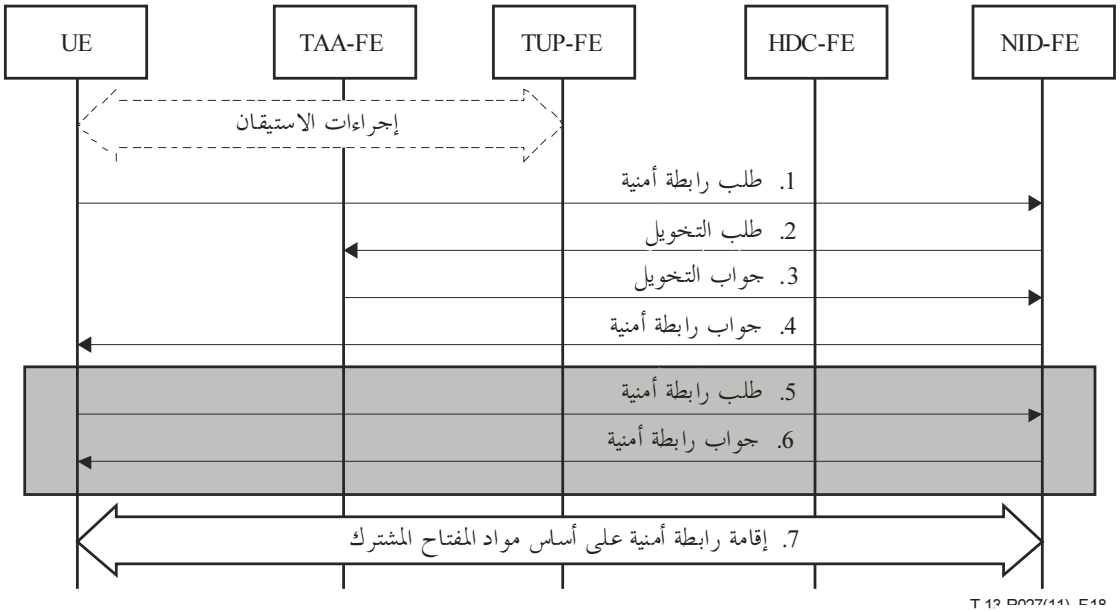
3) يرسل الكيان TAA-FE إلى الكيان NID-FE رداً بشأن رابطة أمنية مفعلة ذاتياً يتضمن معلومات الاستيقان التي تشمل مادة المفتاح المشترك وعمر هذا المفتاح. وعندما لا يدعم الكيان TAA-FE إرسال رد بشأن رابطة أمنية مفعلة ذاتياً إلى الكيان NID-FE مباشرةً، يرسل الكيان TAA-FE رداً بشأن رابطة أمنية مفعلة ذاتياً إلى الكيان NID-FE عبر الكيان HDC-FE.

4) يرسل الكيان NID-FE إلى جهاز المستخدم معلومات بشأن الرابطة الأمنية تشمل معلومات الاستيقان. وتكون المعلومات محمية بمادة المفتاح المشترك.

5) يولد جهاز المستخدم مادة المفتاح المشترك ويتحقق من معلومات الرابطة الأمنية. وتقام الرابطة الأمنية من جانب الكيان NID-FE وجهاز المستخدم على أساس مادة المفتاح المشترك.

3.11 إقامة الرابطة الأمنية بين جهاز المستخدم والكيان NID-FE على أساس البنية التحتية للمفاتيح العمومية (PKI)

يبيَّن في الشكل 18 إجراء إقامة الرابطة الأمنية بين جهاز المستخدم والكيان NID-FE على أساس البنية التحتية للمفاتيح العمومية (PKI). والشرط المسبق لهذا الإجراء هو معرفة جهاز المستخدم بمعلومات عن الكيان NID-FE، كالعنوان الذي يمكن لجهاز المستخدم أن يرسل إلى الكيان NID-FE بموجبه طلب الرابطة الأمنية. أما كيفية حصول جهاز المستخدم على معلومات عن الكيان NID-FE فهي خارج نطاق هذه التوصية.



الشكل 18 – إجراء إقامة الرابطة الأمنية على أساس البنية التحتية للمفاتيح العمومية (PKI)

بعد استكمال إجراء الاستيقان بين الكيان TUP-FE والكيان TAA-FE، تنفَّذ الخطوات التالية:

1) يرسل جهاز المستخدم إلى الكيان NID-FE طلب رابطة أمنية يتضمن شهادة جهاز المستخدم ومعلومات عن هذا الجهاز.

2) يتحقق الكيان NID-FE من شهادة جهاز المستخدم ويرسل إلى الكيان TAA-FE طلب تخويل يتضمن معلومات عن جهاز المستخدم وعن الكيان NID-FE.

3) يتحقق الكيان TAA-FE من التخويل على أساس معلومات عن جهاز المستخدم وعن الكيان NID-FE. فإذا كان الجهاز مخولاً باستخدام الكيان NID-FE، يرسل الكيان TAA-FE إلى الكيان NID-FE رداً بالتخويل يتضمن معلومات التخويل وشهادة المخدّم.

4) يتلقى الكيان NID-FE معلومات التخويل ويرسل إلى جهاز المستخدم رداً بشأن الرابطة الأمنية يتضمن شهادة المخدّم.

5) إذا دعت الحاجة للتشارك في مادة المفتاح بين جهاز المستخدم والكيان TAA-FE، يرسل هذا الكيان إلى جهاز المستخدم معلومات توليد المفتاح المذكورة في الخطوة 4. ويولد جهاز المستخدم مادة المفتاح المشترك على أساس ما يرد من معلومات بشأن توليد المفتاح وتوليد المفتاح المحلي. ويرسل جهاز المستخدم معلومات توليد المفتاح المحلي إلى الكيان NID-FE كجزء من طلب الرابطة الأمنية.

6) يولد الكيان NID-FE مادة المفتاح على أساس ما يرد من معلومات بشأن توليد المفتاح وتوليد المفتاح المحلي. ويرسل الكيان NID-FE إلى جهاز المستخدم رداً بشأن الرابطة الأمنية.

7) تقام الرابطة الأمنية بين جهاز المستخدم والكيان NID-FE.

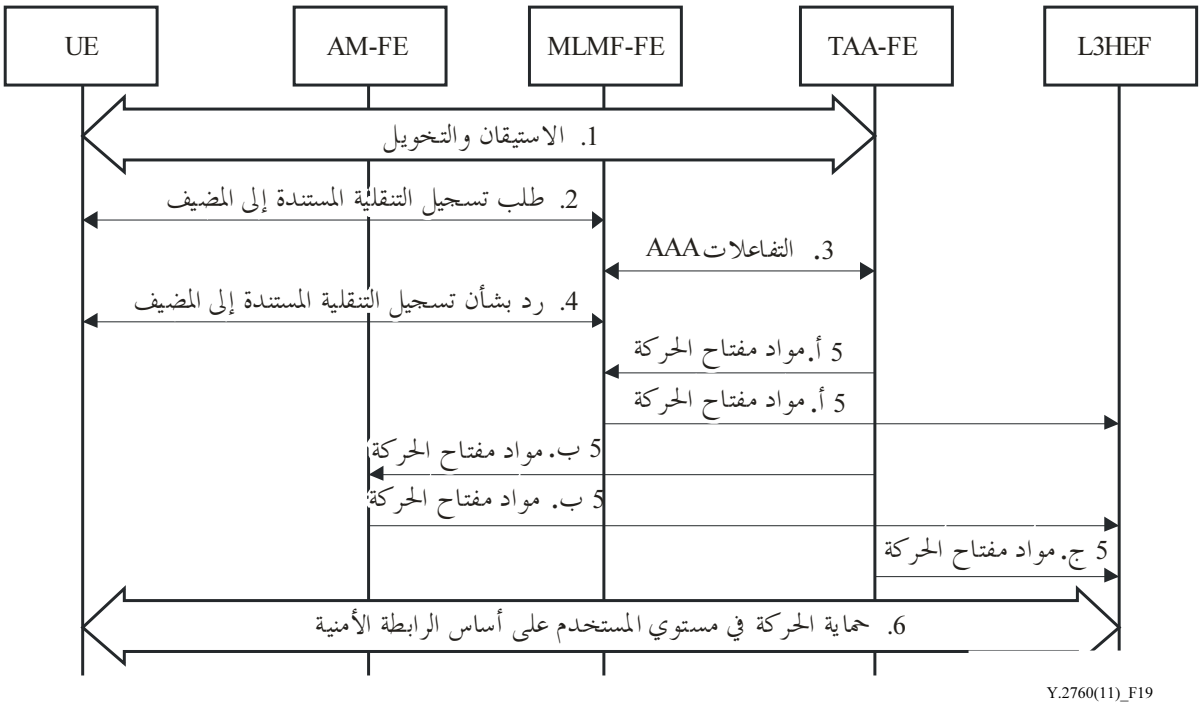
12 أمن وظائف النقل

1.12 الأمن بين جهاز المستخدم والكيان الوظيفي لعقدة النفاذ

ينبغي حماية الحركة بين جهاز المستخدم والكيان الوظيفي لعقدة النفاذ (AN-FE). وتستند الرابطة الأمنية بينهما إلى مادة المفتاح المشترك. وبعد الانتهاء من إجراء الاستيقان المتبادل بنجاح، يولد كيان TAA-FE وجهاز المستخدم كلاهما مادة مفتاح الدورة، مثل مفتاح الدورة لحماية الحركة بينهما. ويرسل الكيان TAA-FE مادة المفتاح إلى الكيان AN-FE عبر الكيانين AM-FE وAR-FE.

2.12 الأمن بين جهاز المستخدم ووظيفة تنفيذ التمرير في الطبقة 3 (L3HEF)

ينبغي حماية الحركة بين جهاز المستخدم ووظيفة تنفيذ التمرير في الطبقة 3 (L3HEF). وتستند الرابطة الأمنية بينهما إلى مادة المفتاح المشترك مسبقاً. وبعد الانتهاء من إجراء الاستيقان المتبادل بنجاح، يولد كيان TAA-FE وجهاز المستخدم كلاهما مادة مفتاح الدورة لحماية الحركة بين جهاز المستخدم ووظيفة تنفيذ التمرير في الطبقة 3 (L3HEF). وتحصل وظيفة L3HEF على مادة المفتاح من الكيان TAA-FE مباشرةً، كما تحصل عليها من الكيان TAA-FE عبر الكيان AM-FE أو الكيان HDC-FE.



Y.2760(11)_F19

الشكل 19 – إجراء أمن الحركة في طبقة المستخدم
بين جهاز المستخدم ووظيفة تنفيذ التمرير في الطبقة 3 (L3HEF)

1) يقام التوصيل بين جهاز المستخدم والكيان TAA-FE. وبعد الانتهاء من الاستيقان المتبادل، يحصل كيان TAA-FE وجهاز المستخدم كلاهما على مادة مفتاح مشترك مثل مادة مفتاح عابر أو مادة مفتاح الدورة.

2) يرسل جهاز المستخدم إلى الكيان MLM-FE طلب تسجيل التنقلية المستندة إلى المضيف لإنشاء رابطة أمنية لتنقلية المضيف.

3) يحصل الكيان MLM-FE على مادة المفتاح بالتفاعل مع الكيان TAA-FE. ويستيقن الكيان MLM-FE من جهاز المستخدم على أساس مادة المفتاح. وبعد الانتهاء من الاستيقان بنجاح، ينشئ الكيان MLM-FE رابطة أمنية مع جهاز المستخدم على أساس مادة المفتاح.

4) يرسل الكيان MLM-FE إلى جهاز المستخدم رداً بشأن تسجيل التنقلية المستندة إلى المضيف، ويتحقق الجهاز من هذا الرد وينشئ رابطة أمنية مع الكيان MLM-FE.

5) بعد إنشاء رابطة أمنية بين جهاز المستخدم والكيان MLM-FE، ستصادَف ثلاث حالات.

5أ – يولد استيقان النقل وتخويله (TAA-FE) مادة مفتاح الحركة ويرسلها إلى وظيفة L3HEF عبر الكيان MLM-FE.

5ب – يولد استيقان النقل وتخويله (TAA-FE) مادة مفتاح الحركة ويرسلها إلى وظيفة L3HEF عبر الكيان MLM-FE والكيان AM-FE.

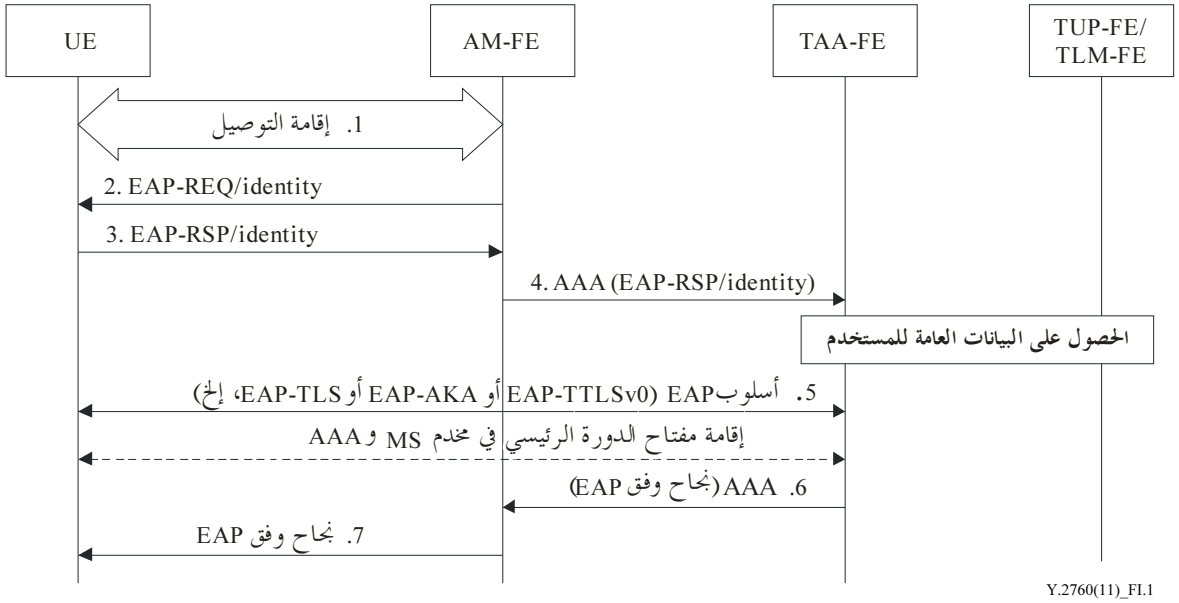
5ج – يرسل الكيان TAA-FE مادة مفتاح الحركة ويرسلها إلى وظيفة L3HEF مباشرةً.

6) تستخدم وظيفة L3HEF مادة مفتاح الحركة لحماية الحركة في طبقة المستخدم بين جهاز المستخدم ووظيفة L3HEF.

التذييل I

(يعتبر هذا التذييل جزءاً لا يتجزأ من التوصية)

1.I مثال على إجراء استيقان كامل



الشكل 1.I – إجراء استيقان كامل

ملاحظة – تشير الهوية في الخطوات 2-4 إلى هوية جهاز المستخدم.

يظهر في الشكل 1.I بيان للتفعيل الذاتي للاستيقان:

1) يقام التوصيل بين جهاز المستخدم والكيان AM-FE.

2) يرسل الكيان AM-FE إلى جهاز المستخدم طلب هوية وفق بروتوكول الاستيقان القابل للتوسيع ((EAP-REQ)/Identity) [b-IETF RFC 3748].

3) يرسل جهاز المستخدم رسالة جوابية بشأن الهوية وفق بروتوكول الاستيقان القابل للتوسيع ((EAP-RSP)/Identity).

4) يسيّر الكيان AM-FE الرسالة الجوابية بشأن الهوية نحو الكيان TAA-FE الذي يتبادل فيما بعد المعلومات مع الكيانين TUP-FE /TLM-FE، اللذين يرسلان إلى الكيان TAA-FE معلومات عن المستخدم تتضمن بياناته العامة.

5) تنفَّذ عملية اشتقاق المفتاح وتوزيعه في الكيان TAA-FE وفي جهاز المستخدم. ويمكن النظر في أساليب عدة، مثل أمن طبقة النقل المغلفة في بروتوكول الاستيقان القابل للتوسيع (EAP-TTLS) واتفاق الاستيقان والمفاتيح في بروتوكول الاستيقان القابل للتوسيع (EAP-AKA) وأمن طبقة النقل في بروتوكول الاستيقان القابل للتوسيع (EAP-TLS) وما إلى ذلك.

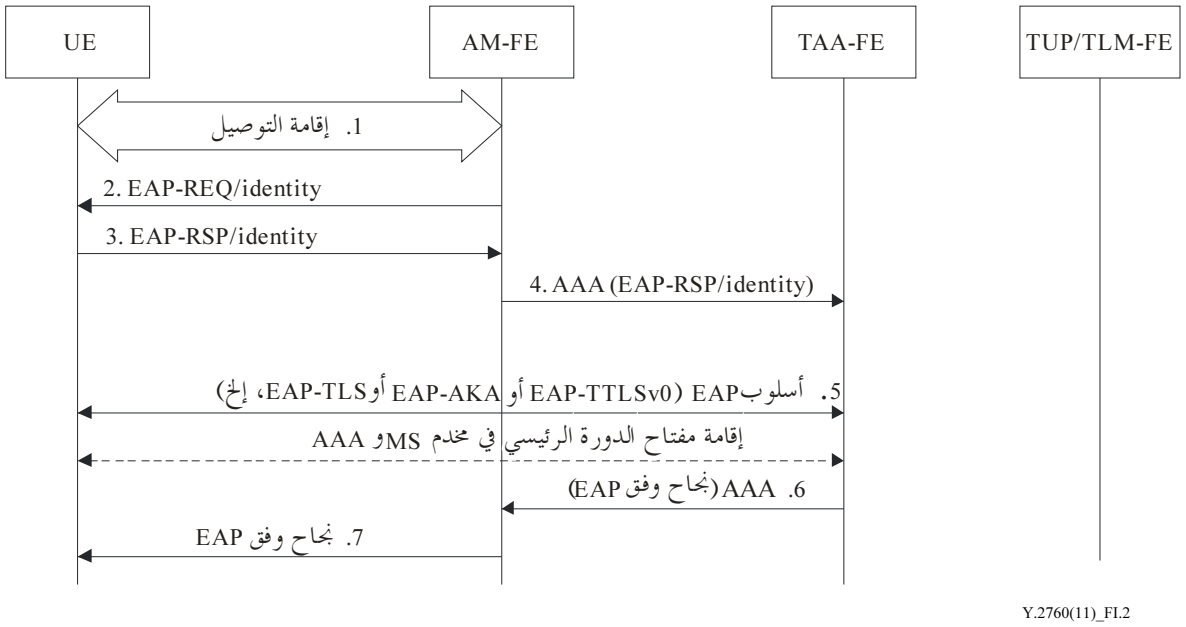
6) يرسل الكيان TAA-FE إلى الكيان AM-FE رسالة نجاح وفق بروتوكول الاستيقان القابل للتوسيع (EAP).

7) يُعلم الكيان AM-FE جهاز المستخدم بنجاح الاستيقان بواسطة رسالة النجاح وفق بروتوكول الاستيقان القابل للتوسيع (EAP). وبعد الإتمام الناجح لعملية تبادل المفاتيح على أساس هذا البروتوكول، يتشارك جهاز المستخدم والكيان AM-FE في المادة المفتاحية المشتقة خلال ذلك التبادل.

2.I مثال على إجراء معاودة الاستيقان السريعة

عند التمرير، يمكن لمعاودة الاستيقان أن تحافظ على استمرارية الخدمة في كمون منخفض. وتحتاج معاودة الاستيقان السريعة لاستخدام هوية إعادة استيقان سريعة، ولا حاجة لها لتبادل معلومات الاستيقان بين الكيان TAA-FE والكيانين TUP-FE/TLM-FE.

ويبيّن فيما يلي إجراء معاودة الاستيقان السريعة.



الشكل 2.I – إجراء معاودة الاستيقان السريعة

1) يقام التوصيل بين جهاز المستخدم والكيان AM-FE.

2) يرسل الكيان AM-FE إلى جهاز المستخدم طلب هوية وفق بروتوكول الاستيقان القابل للتوسيع ((EAP-REQ)/Identity)، ويتضمن الطلب هوية معاودة الاستيقان.

3) يرسل جهاز المستخدم رسالة جوابية بشأن الهوية وفق بروتوكول الاستيقان القابل للتوسيع ((EAP-RSP)/Identity).

4) يسيّر الكيان AM-FE الرسالة الجوابية بشأن الهوية نحو الكيان TAA-FE.

5) تنفَّذ عملية اشتقاق المفتاح وتوزيعه. ويمكن النظر في أساليب عدة، مثل اتفاق الاستيقان والمفاتيح في بروتوكول الاستيقان القابل للتوسيع (EAP-AKA) وأمن طبقة النقل في بروتوكول الاستيقان القابل للتوسيع (EAP-TLS) وما إلى ذلك.

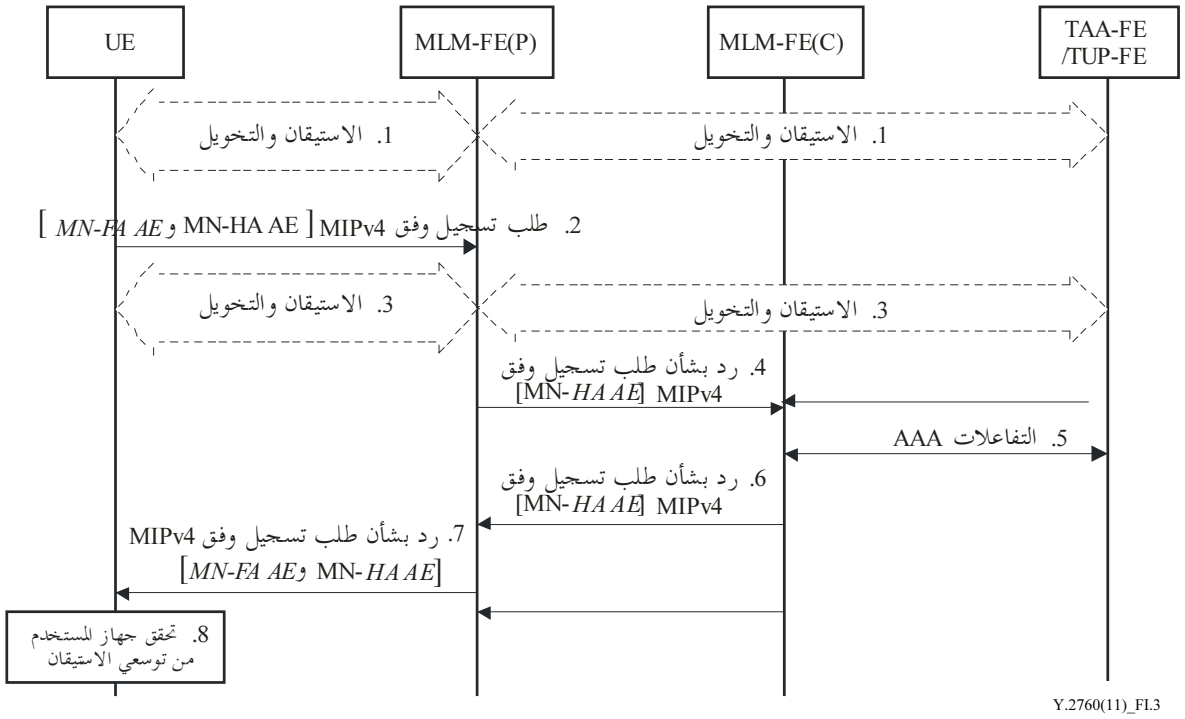
6) يرسل الكيان TAA-FE إلى الكيان AM-FE رسالة نجاح وفق بروتوكول الاستيقان القابل للتوسيع (EAP).

7) يُعلم الكيان AM-FE جهاز المستخدم بنجاح الاستيقان بواسطة رسالة النجاح وفق بروتوكول الاستيقان القابل للتوسيع (EAP). وبعد الإتمام الناجح لعملية تبادل المفاتيح على أساس هذا البروتوكول، يتشارك جهاز المستخدم والكيان AM-FE في المادة المفتاحية المشتقة خلال ذلك التبادل.

3.I مثال على التنقلية المستندة إلى المضيف

في الإصدار الرابع من بروتوكول الإنترنت للخدمة المتنقلة (MIPv4)، يستند أمن تنقلية بروتوكول الإنترنت إلى توسعات الاستيقان في بروتوكول الإنترنت للخدمة المتنقلة (MIP) على النحو المحدد في طلب التعليقات [b-IETF RFC 3344]. ويتعين حماية رسائل تشوير تنقلية بروتوكول الإنترنت بين جهاز المستخدم والعقدة القائمة بمقام وكيل محلي (HA)

(أي الكيان MLM-FE)، وربما أيضاً بين جهاز المستخدم والعقدة القائمة بمقام وكيل أجنبي (FA) (أي الكيان MLM-FE)، وذلك باستخدام توسعات الاستيقان في بروتوكول الإنترنت للخدمة المتنقلة (MIP)



الشكل 3.I – إجراء التفعيل الذاتي وفق الإصدار الرابع من بروتوكول الإنترنت للخدمة المتنقلة (MIPv4)

إن إجراء التفعيل الذاتي وفق الإصدار الرابع من بروتوكول الإنترنت للخدمة المتنقلة (MIPv4) المبين في الشكل 3.I يتم على النحو التالي:

1) يُنشأ الاستيقان والتخويل بين جهاز المستخدم والكيان MLM-FE بمساعدة الكيانين TAA-FE/TUP-FE.

2) يرسل جهاز المستخدم رسالة طلب تسجيل (RRQ) إلى الوكيل الأجنبي (MLM-FE)، ويضمّنها توسع الاستيقان الشامل لوكيل محلي لعقدة متنقلة (MN-HA)، ويضمّنها أيضاً على نحو اختياري توسع الاستيقان الشامل لوكيل أجنبي لعقدة متنقلة (MN-FA)، على النحو الموصّف في طلب التعليقات [b-IETF RFC 3344].

3) تطلق رسالة طلب التسجيل (RRQ) إجراء الاستيقان من النفاذ.

4) يعالج الوكيل الأجنبي الرسالة طبقاً لطلب التعليقات [b-IETF RFC 3344]، ويتحقق من توسع الاستيقان الشامل لوكيل أجنبي لعقدة متنقلة (MN-FA) في حال وجوده. ثم يسيّر الوكيل الأجنبي رسالة طلب التسجيل (RRQ) إلى الوكيل المحلي (MLM-FE).

5) يحصل الكيان MLM-FE المختار على معلومات الاستيقان والتخويل من الكيانين TAA-FE/TUP-FE.

6) يتحقق الكيان MLM-FE من توسع الاستيقان الشامل لوكيل محلي لعقدة متنقلة (MN-HA).وبعد التحقق الناجح من توسع الاستيقان، يرسل الكيان MLM-FE جواب التسجيل (RRP) إلى جهاز المستخدم عبر الوكيل الأجنبي.

7) يعالج الوكيل الأجنبي جواب التسجيل طبقاً لطلب التعليقات [b-IETF RFC 3344]. ثم يسيّر رسالة جواب التسجيل إلى جهاز المستخدم، ويضمّنها توسع الاستيقان الشامل لوكيل أجنبي لعقدة متنقلة (MN-FA) في حال تلقيه لهذا التوسع ضمن الرسالة.

8) يتحقق جهاز المستخدم من توسع الاستيقان الشامل لوكيل محلي لعقدة متنقلة (MN-HA) وتوسع الاستيقان الشامل لوكيل أجنبي لعقدة متنقلة (MN-FA)، في حال وجودهما.

بيبليوغرافيا

[b-IETF RFC 3220] IETF RFC 3220 (2002), *IP Mobility Support for IPv4.*

[b-IETF RFC 3344] IETF RFC 3344 (2002), *IP Mobility Support for IPv4.*

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*.

[b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*

[b-IETF RFC 4555] IETF RFC 4555 (2006), *IKEv2 Mobility and Multihoming Protocol (MOBIKE).*

[b-IETF RFC 5213] IETF RFC 5213 (2008), *Proxy Mobile IPv6*.

[b-3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2007), *3G Security: Security Architecture*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن
السلسلة Y	**البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي**
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2012