الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2703

(2009/01)

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

شبكات الجيل التالي – الأمن

تطبيق خدمة الاستيقان والتخويل والمحاسبة (AAA) في شبكات الجيل التالي (NGN)

التوصيـــة ITU-T Y.2703

الاتحاد الدولي للاتصالات

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
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
الأمن	**Y.2799–Y.2700**
التنقلية المعممة	Y.2899–Y.2800

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

التوصيـــة ITU-T Y.2703

تطبيق خدمة الاستيقان والتخويل والمحاسبة (AAA) في شبكات الجيل التالي (NGN)

الملخص

تتناول هذه التوصية تطبيق الاستيقان والتخويل والمحاسبة (AAA) بخصوص الإصدار الأول من شبكات الجيل التالي، (NGN).

المصدر

وافقت لجنة الدراسات 13 (2009-2012) لقطاع تقييس الاتصالات على التوصية ITU-T Y.2703 بتاريخ 23 يناير 2009، بموجب إجراء القرار 1 للجمعية العالمية لتقييس الاتصالات (WTSA).

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/.

المحتـــويات

الصفحة

الصفحة

تطبيق خدمة الاستيقان والتخويل والمحاسبة (AAA) في شبكات الجيل التالي (NGN)

1 مجال التطبيق

تصف هذه التوصية تطبيق الاستيقان والتخويل والمحاسبة (AAA) على شبكات الجيل التالي (NGN) وذلك على أساس التوصية [b-ITU-T Y.2201]: متطلبات الإصدار 1 من شبكات الجيل التالي، والتوصية [b-ITU-T Y.2012]: المتطلبات الوظيفية ومعمارية الإصدار 1 من شبكات الجيل التالي، والتوصية [b-ITU-T Y.2701]: المتطلبات الأمنية للإصدار 1 من شبكات الجيل التالي، والتوصية [b-ITU-T Y.2702]: استيقان شبكات الجيل التالي. وتنطبق هذه التوصية على عملية الاستيقان والتخويل والمحاسبة (AAA) في النفاذ إلى شبكة ما من شبكات الجيل التالي باستخدام عميل الخدمة AAA ومخدم الخدمة AAA. وعلى وجه التحديد، تتناول هذه التوصية وظيفة المحاسبة من زاوية مساهمتها في المحاسبة الأمنية فقط.

ويشمل نطاق هذه التوصية ما يلي:

1) عملية "الاكتتاب" (enrolment).
2) وظائف الاستيقان وإجراءاته.
3) وظائف التخويل وإجراءاته.
4) وظائف المحاسبة الأمنية وإجراءاتها.

2 المراجع

لا يوجد.

3 التعاريف

1.3 المصطلحات المعرفة في مواضع أخرى

تستخدم هذه التوصية التعاريف التالية المعرفة في مواضع أخرى:

1.1.3 الاستيقان [b-ITU-T X.811]: تقديم الضمان لهوية مزعومة لكيان ما.

2.1.3 شهادة الاستيقان [b-ITU-T X.811]: شهادة أمن مضمونة من جانب سلطة استيقان ويمكن استخدامها لتقديم ضمان هوية كيان ما.

3.1.3 معلومات الاستيقان [b-ITU-T X.811]: المعلومات المستعملة لأغراض الاستيقان.

4.1.3 التخويل [b-ITU-T X.800]: منح الحقوق، ويشمل السماح بالنفاذ على أساس حقوق النفاذ.

5.1.3 المُطالِب [b-ITU-T X.811]: كيان أصيل أو وكيل لأصيل لأغراض الاستيقان. ويشمل المُطالِب الوظائف اللازمة للدخول في تبادلات الاستيقان نيابة عن الأصيل.

6.1.3 آثار التدقيق الأمني [b-ITU-T X.800]: البيانات المجمَّعة والتي يُحتمَل استعمالها لتسهيل عملية تدقيق أمني ما.

2.3 المصطلحات المعرفة في هذه التوصية

تعرّف هذه التوصية المصطلح التالي:

1.2.3 المحاسبة الأمنية: الدور الذي يقتفي أثر الإجراءات أو الأحداث المتعلقة بالأمن التي يمكن إدراجها كموارد في وظيفة التدقيق الأمني.

4 المختصرات

تُستخدم في هذه الوثيقة المختصرات التالية:

AAA الاستيقان والتخويل والمحاسبة *(Authentication, Authorization, Accounting)*

AM-FE كيان وظيفي لإدارة النفاذ *(Access management functional entity)*

ANI سطح بيني بين التطبيق والشبكة *(Application-to-Network Interface)*

EAP بروتوكول الاستيقان الموسع *(Extensible Authentication Protocol)*

ID الهوية – بالصيغة التي تحددها الشبكة أو الخدمة أو الكيان موضوع النفاذ *(Identity - as Defined by the Network, Service, or Entity Being Accessed)*

NAS مخدم النفاذ إلى الشبكة *(Network Access Server)*

NGN شبكة الجيل التالي *(Next Generation Network)*

NNI سطح بيني بين شبكة وشبكة *(Network-to-Network Interface)*

NP مورد الشبكة *(Network Provider)*

OAMP العمليات والإدارة والصيانة والتموين *(Operation Administration Maintenance and Provision)*

RACF وظيفة التحكم في النفاذ إلى مورد *(Resource Access Control Function)*

SCTP بروتوكول نقل للتحكم في التدفق *(Stream Control Transport Protocol)*

SR مورد خدمة *(Service Resource)*

TAA-FE كيان وظيفي لاستيقان النقل وتخويله *(Transport Authentication and Authorization Functional Entity)*

TE تجهيزات مطرافية *(Terminal Equipment)*

TUP-FE كيان وظيفي لمواصفات مستعمل النقل *(Transport User Profile Functional Entity)*

UNI سطح بيني بين المستعمل والشبكة *(User-to-Network Interface)*

5 الاصطلاحات

لا توجد.

6 مفاهيم عامة لخدمة الاستيقان والتخويل والمحاسبة (AAA)

تتناول هذه الفقرة المفاهيم الأساسية لخدمة الاستيقان والتخويل والمحاسبة (AAA).

1.6 عرض عام

توفر خدمة الاستيقان والتخويل والمحاسبة الوظائف التي يتم من خلالها التيقن من هوية مستعمِلٍ ما (الاستيقان)، ويُمنَح هذا المستعمِل النفاذ إلى الخدمات (التخويل)، والوسيلة التي يُقاس من خلالها استهلاك الموارد (المحاسبة).

2.6 عملية الاستيقان والتخويل والمحاسبة (AAA)

تجري العمليات المنفردة ضمن إطار خدمة الاستيقان والتخويل والمحاسبة (AAA) كما يلي:

تقوم عملية الاستيقان بإثبات صلاحية هوية المستعمل النهائي قبل السماح له بالنفاذ إلى الشبكة. ويقدم المستعمل النهائي مجموعة من وسائل الاعتماد، من قبيل اقتران اسم المستعمل وكلمة السر أو مفتاح الأمن أو شهادة أو بيانات بيومترية

(بصمات الأصابع مثلاً). ويتم عادةً الاتفاق على وسائل الاعتماد هذه أثناء عملية "الاكتتاب" (enrolment). ويؤدي التحقق من وسائل الاعتماد إلى عملية التخويل.

وتحدد عملية التخويل الامتيازات والخدمات الممنوحة للمستعمل النهائي حالما يتم السماح له بالنفاذ إلى الشبكة. وقد يشمل ذلك منح المستعمل عنوان بروتوكول إنترنت أو استعمال مرشاح لتحديد أي التطبيقات أو البروتوكولات يمكن تفعيلها. ويتم إجراء عمليتي الاستيقان والتخويل معاً في بيئة تحكمها العملية AAA.

وتوفر عملية المحاسبة المنهجية اللازمة لجمع المعلومات بشأن استهلاك المستعمل النهائي للموارد والتي يمكن بعدئذ معالجتها لأغراض الفوترة والتدقيق وتخطيط القدرات. وتفيد بعض بيانات المحاسبة في بناء مسار التدقيق الأمني.

وتندمج هذه العمليات الثلاث في مجموعة من الوظائف تُستخدَم معاً لتوفير التحكم في النفاذ.

3.6 إجراء الاستيقان والتخويل والمحاسبة (AAA)

يتألف نظام الاستيقان والتخويل والمحاسبة (AAA) من مخدم AAA وعميل AAA.

ولدى مخدم AAA إمكانية النفاذ إلى قاعدة بيانات من مواصفات المستعملين وبيانات التشكيل. ويتواصل هذا المخدم مع عملاء AAA في مكونات الشبكة، مثل مخدم النفاذ إلى الشبكة (NAS) والمسيّرات، وذلك من أجل تقديم خدمات AAA الموزّعة.

وتتلخص سيناريوهات AAA في الخطوات التالية:

- يقوم المستعمل النهائي بالاتصال بجهاز نقطة الدخول ويطلب النفاذ إلى الشبكة.
- يحيل عميل AAA هوية/وسائل استيقان المستعمل النهائي إلى مخدم AAA.
- يستيقن مخدم AAA المستعمل على أساس وسائل الاعتماد. فإذا نجح الاستيقان، يحدد المخدم حينئذ أي خدمة أو خدمات مرخص بها ثم يَرُدّ بإرسال إجابة إلى عميل AAA بالقبول أو الرفض إلى جانب بيانات أخرى ذات صلة.
- يُخطِر عميل AAA المستعمل النهائي بأن النفاذ إلى الموارد المحددة مسموح به أو مرفوض.

يُرسِل عميل AAA رسالة محاسبة إلى مخدم AAA أثناء عملية الإعداد للتوصيل وإنهائه بهدف جمع السجلات وتخزينها.

7 نموذج التطبيق للاستيقان والتخويل في شبكات الجيل التالي (NGN)

تستند هذه التوصية إلى المتطلبات الأمنية لشبكات الجيل التالي (NGN) الواردة في التوصية [b-ITU-T Y.2701] وإلى النموذج المرجعي للاستيقان في شبكات الجيل التالي الوارد في التوصية [b-ITU-T Y.2702]. ويصف هذا النموذج المرجعي NGN (الشكل 7-1) ثماني نقاط مرجعية للاستيقان؛ تُراعي/تأخذ منها هذه التوصية ثلاث نقاط بعين الاعتبار.

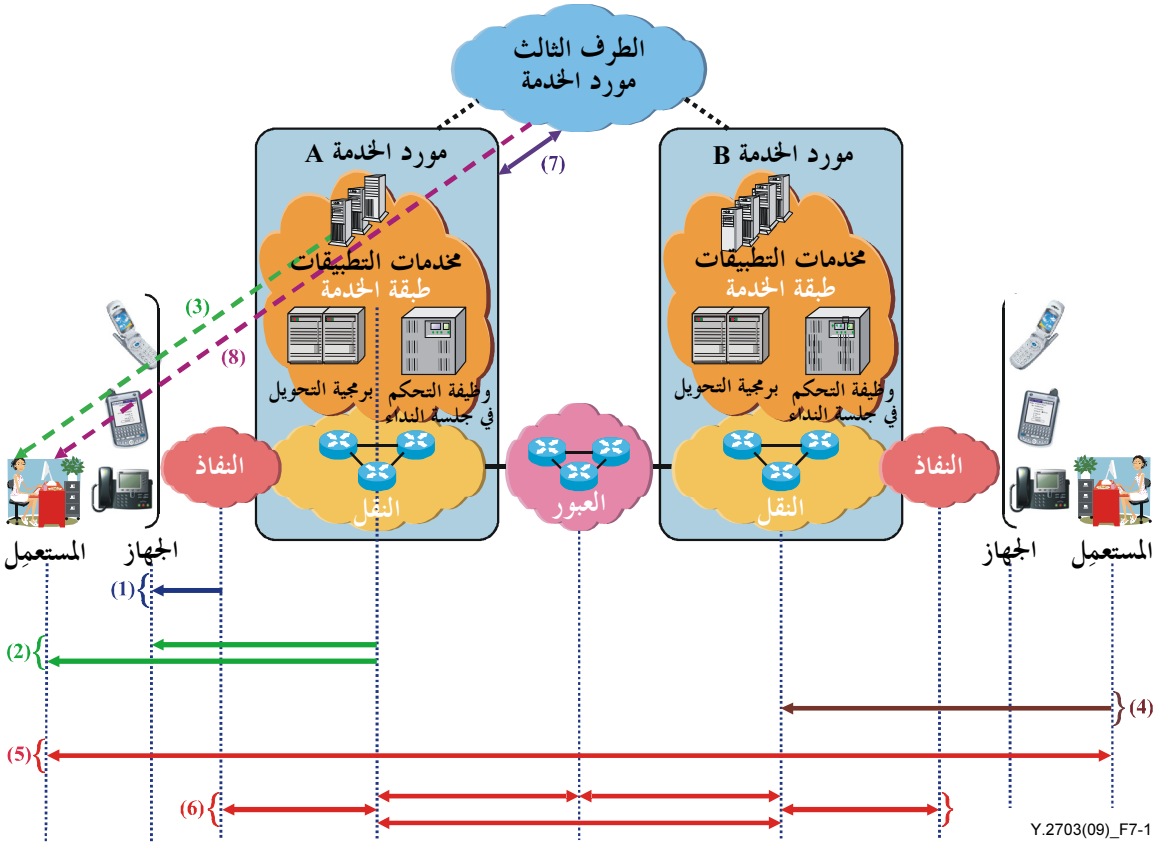
وهذه النقاط هي:

(1) نفاذ المستعمل إلى الشبكة؛

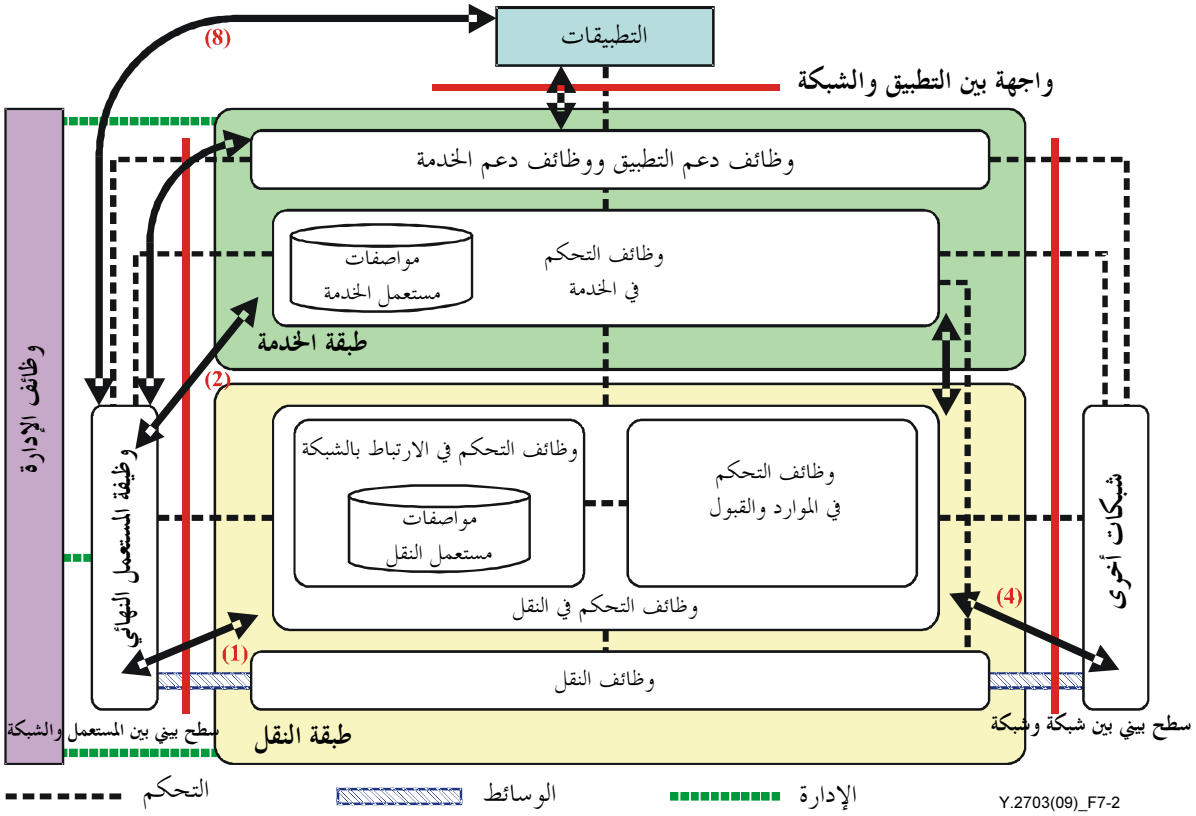
(2) نفاذ المستعمل إلى الخدمة التي تقدمها الشبكة؛

(4) نفاذ مورد الخدمة إلى المستعمل المتلقي لها.

وتُشير النقطتان المرجعيتان (1) و(4) إلى نقل حركة المستعملين ويمكن النظر إليهما على أنهما تتوقفان على التحكم في النفاذ "الأفقي" على مستوى التحكم في النقل، بينما يمكن النظر إلى النقطتين (2) و(8) على أنهما تتوقفان على بيانات التحكم بين طبقتي التحكم في النقل والخدمة، وبالتالي على أنهما "رأسيتان". وهذه العلاقة معروضة في الشكل 7-2.



الشكل 7-1 – معمارية النموذج المرجعي من طرف إلى طرف (التوصية Y.2702: الاستيقان في شبكات الجيل التالي)

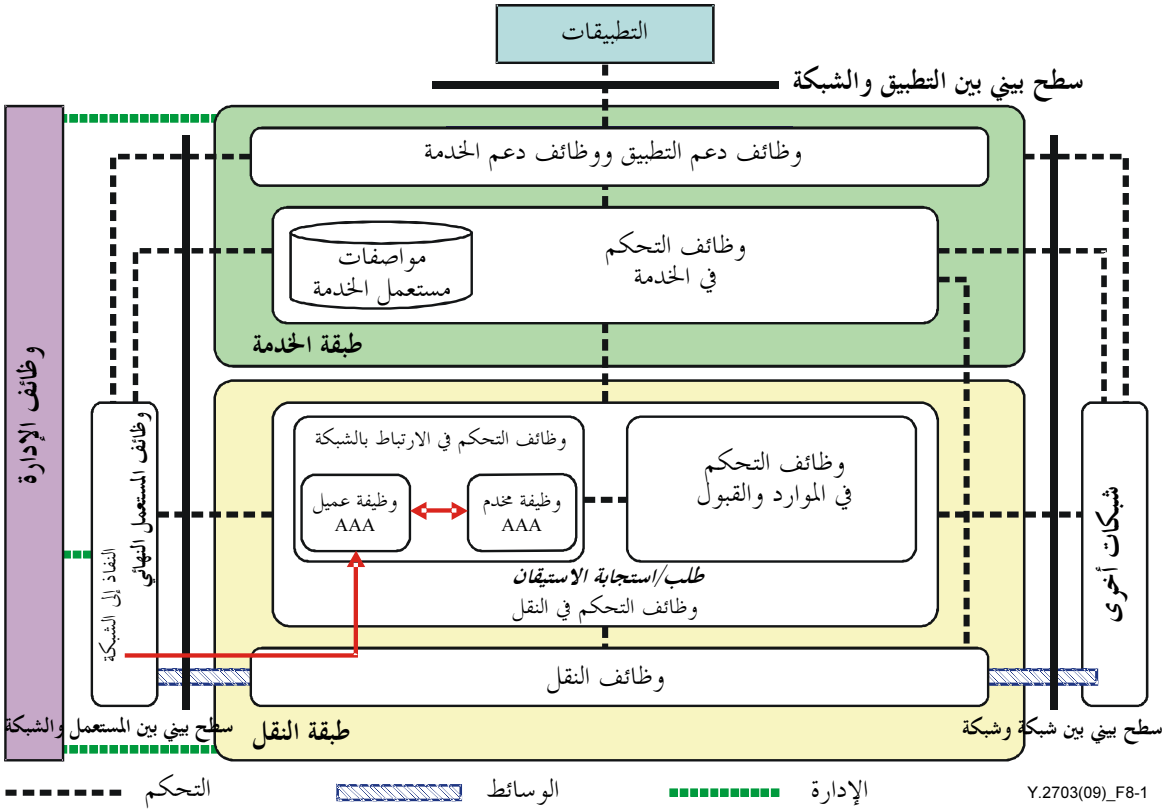


الشكل 7-2 – معمارية شبكات الجيل التالي والمجالات المتعلقة بخدمة AAA
(التوصية Y.2702: الاستيقان في شبكات الجيل التالي)

8 معمارية الاستيقان والتخويل والمحاسبة (AAA) في شبكات الجيل التالي

يصف هذا البند العلاقة بين النموذج المرجعي لخدمة AAA والنموذج المعماري الوظيفي الموصوف في التوصية [b-ITU-T Y-2012].

1.8 نفاذ المستعمِل إلى الشبكة

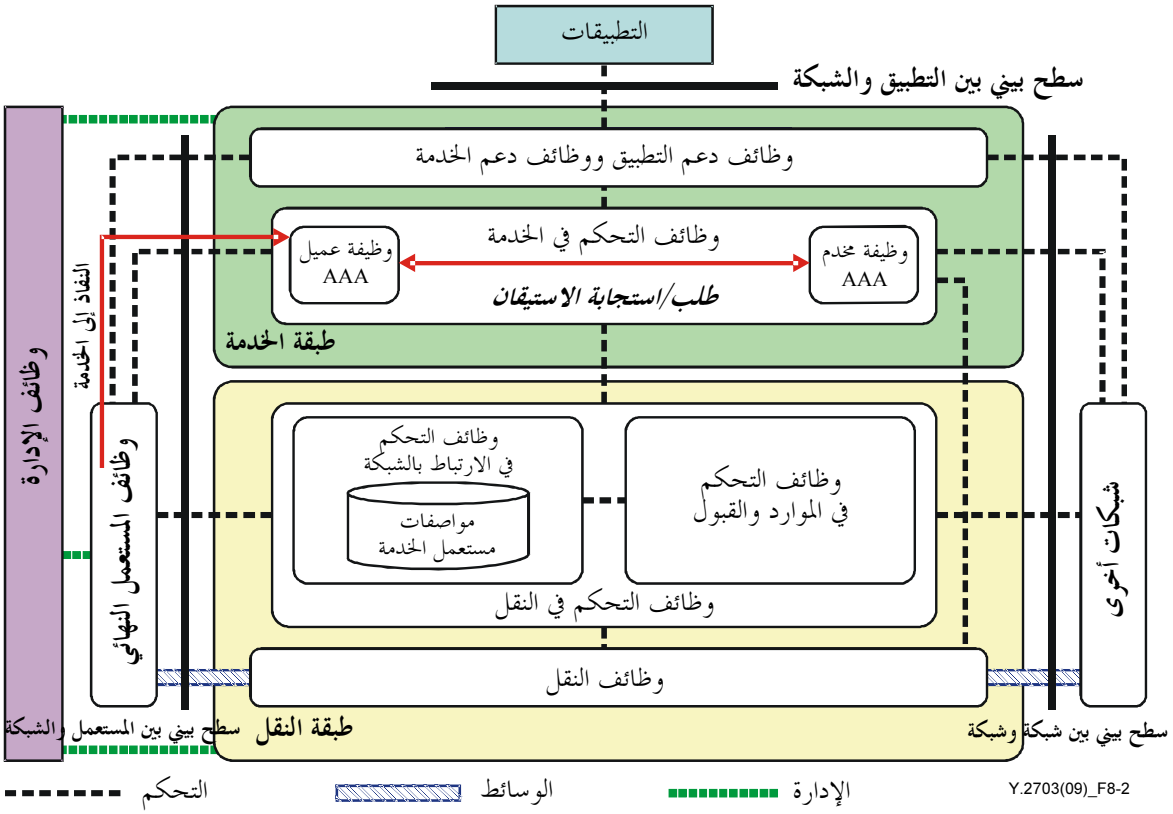


الشكل 8-1 – الاستيقان من مستعمِل ما والتخويل له بالنفاذ إلى الشبكة

يصف الشكل 8-1 تطبيق خدمة الاستيقان والتخويل والمحاسبة (AAA) في عملية نفاذ المستعمِل إلى الشبكة (أي تطبيق من النمط 1 في الشكل 7-1 أعلاه).

حالما يكتشف كيان ما في وظائف التحكم في النقل طلب التوصيل من مطراف مستعمِل ما (كيان وظيفي لإدارة النفاذ T-14 عادة) يشرع في التصرف كعميل خدمة AAA. فيطلب من الكيانات في وظائف التحكم في النقل والتي تضطلع بدور مخدم AAA (مثال ذلك كيان وظيفي لاستيقان النقل وتخويله T-11 أو كيان وظيفي لمواصفات مستعمل النقل T-12) الاستيقان من المستعمِل والتخويل له باستخدام موارد شبكات الجيل التالي. ويمكن استخدام بروتوكولات، مثل بروتوكول خدمة المستعمِل بواسطة المراقمة الداخلية للاستيقان عن بعد (RADIUS) أو بروتوكول ديامتر (Diameter)، للتعامل مع إجراء الطلب والاستجابة هذا. وعلى أساس الطلب الوارد من عميل AAA، يقوم مخدم AAA بالاستيقان من المستعمِل بواسطة إجراءات صريحة (مثل بروتوكول الاستيقان الموسع) أو ضمنية (مثل استيقان خط النفاذ). وبعد نجاح التخويل لمستعمِل ما، وهو ما يتوقف على مواصفات المستعمل (التي يديرها عادة كيان وظيفي لمواصفات مستعمل النقل)، يطلب مخدم AAA من وظيفة التحكم في النفاذ إلى الموارد حجز موارد في شبكات الجيل التالي لصالح ذلك المستعمل. وعندما يُمنح التخويل يقوم مخدم AAA بإخطار عميل AAA بالإذن له بتوصيل تجهيزات ذلك المستعمِل.

2.8 ارتباط المستعمِل بخدمة الشبكة



الشكل 8-2 – الاستيقان من مستعمِل ما والتخويل له بالنفاذ إلى الخدمة

يبين الشكل 8-2 تطبيق خدمة AAA في عملية نفاذ المستعمِل إلى الخدمة (أي تطبيق من النمط 2 في الشكل 7-1 أعلاه).

وعلى غرار الحالة السابقة الموضحة في الشكل 8-1، يكتشف عميل AAA في وظائف التحكم في الخدمة (كيان وظيفي من نوع S-CES S-1 عادة) طلب التوصيل من مطراف مستعمِلٍ ما. فيطلب من مخدم AAA (مثال ذلك كيان وظيفي لمواصفات مستعمل الخدمة S-5، أو كيان وظيفي لاستيقان الخدمة وتخويلها S-6) استيقان الخدمة المطلوبة وتخويلها. ويتوقف تقديم الخدمة المطلوبة أو رفضها على نتيجة الاستيقان والتخويل.

ومتى تم توصيل المستعمِل بالشبكة أو بالخدمة، يقوم كل عميل AAA بإخطار مخدم AAA بالمعلومات المتعلقة بموارد شبكات الجيل التالي المستهلَكة من جانب المستعمل قصد مساعدة مخدم AAA على جمع معلومات المحاسبة المرتبطة بهذا المستعمل.

3.8 الاستيقان من المستعمِل والتخويل له من أجل النفاذ إلى خدمة طرف ثالث

لا يتناول الإصدار الأول من شبكات الجيل التالي خدمات الأطراف الثالثة التي يمكن النفاذ إليها من خلال الواجهة بين التطبيق والشبكة. ولذلك فإن موضوع الاستيقان من المستعمِل والتخويل له من أجل النفاذ إلى خدمات الطرف الثالث يقع خارج نطاق هذه الوثيقة. ولا تصف هذه التوصية النموذج المرجعي لخدمات الطرف الثالث. ومع ذلك، يتناول التذييل الثالث حالة استعمال توضح خدمة الاستيقان والتخويل لدى طرف ثالث.

9 "الاكتتاب"

من الشروط المسبقة لخدمة AAA تحديد هوية الكيان المطلوب الاستيقان منه، مثل المستعمِل أو الجهاز. وتستحدث وسائل الاعتماد التي تحدد هوية الكيان من خلال عملية "الاكتتاب" (enrolment) التي تحدد الهوية الفريدة لمستعملٍ أو جهازٍ ما. وتُستخدم وسائل الاعتماد في عملية الاستيقان كلما طُلِب النفاذ إلى خدمة أو خدمات. وقد تشمل عملية الاكتتاب قبول القيود والشروط وكذا الترتيبات المالية. ومع أن التحقق الأولي من الهوية ووسائل الاعتماد يشار إليه بمصطلح "الاكتتاب" (enrolment)، فإن النفاذ اللاحق إلى الخدمات وعمليات التأكد من وسائل الاعتماد يُعرف بمصطلح "التسجيل" (registration). وتتوقف الترتيبات الدقيقة للاكتتاب على سياسات مورد الخدمة وطبيعة الخدمات، وغير ذلك.

10 الاستيقان

تستخدم هذه التوصية المفاهيم الأساسية للاستيقان الموصوفة في التوصية [b-ITU-T X.811]. وهناك حاجة لخدمات وقدرات الاستيقان من النفاذ إلى الشبكات والخدمات من أجل درء المخاطر المصاحبة لمحاولات النفاذ غير المرخص به. وثمة معلومات إضافية بشأن الشهادات الرقمية متاحة في التذييل الثاني.

1.10 كيانات الاستيقان

يُستعمَل مصطلح "المُطالِب" لوصف كيان يطلب الاستيقان. ويشمل المُطالِب الوظائف الضرورية للدخول في تبادلات الاستيقان.

ويقدم عميل AAA وظيفة متخصصة تمثل جزءاً من مسار النفاذ بين المُطالِب والكيان المحقِّق في كل طلب من طلبات النفاذ كما يعمل على إنفاذ القرار الذي يتوصل إليه المحقِّق.

وفي البيئة التي تديرها خدمة AAA، يكون مخدم AAA هو الكيان المحقِّق ويصدر شهادة استيقان لصالح المُطالِب عند نجاح الاستيقان.

2.10 إجراء الاستيقان

في البيئة التي تديرها خدمة AAA، يوفر مخدم AAA الاستيقان للمستعمل. ويقوم هذا المخدم بتحديد هوية الكيان طالب النفاذ لدرجة تسمح بتحديد أي الخدمات يمكن تخويل النفاذ إليها وفرض الرسوم عليها. ويمكن لمخدم AAA أن يصدر شهادة استيقان.

1.2.10 عمليات الاستيقان الناجحة

تقدم الخطوات التالية والشكل 10-1 مثالاً عن المخطط الانسيابي للرسائل اللازمة لعملية استيقان ناجحة.

الخطوة 1: يطلب كيان ما النفاذ من عميل AAA.

الخطوة 2: يطلب عميل AAA من مخدم AAA الاستيقان من الكيان.

الخطوة 3: يطلب مخدم AAA من عميل AAA وسائل اعتماد الكيان قصد الشروع في الاستيقان.

الخطوة 4: يطلب عميل AAA من الكيان وسيلة/وسائل الاعتماد اللازمة للاستيقان.

الخطوة 5: يُرسل الكيان، الذي أصبح الآن مطالباً، وسيلة/وسائل الاعتماد إلى عميل AAA.

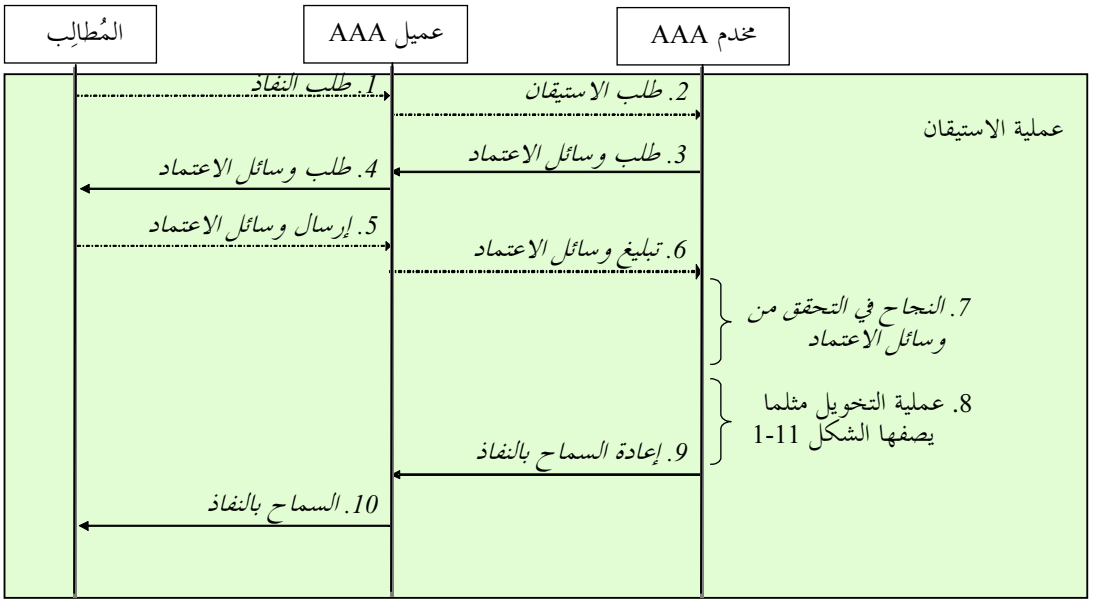
الخطوة 6: يقوم عميل AAA بإحالة وسيلة/وسائل الاعتماد إلى مخدم AAA بهدف الاستيقان.

الخطوة 7: يتحقق مخدم AAA من وسائل الاعتماد الواردة بمقارنتها بمواصفات اعتماد المستعمل لدى المُطالِب.

الخطوة 8: إذا أمكن التحقق من وسائل الاعتماد، يمضي مخدم AAA في عملية التخويل دون إخطار عميل AAA أو المُطالِب.

الخطوة 9: بعد عملية التخويل، يبعث مخدم AAA إلى عميل AAA برسالة السماح بالنفاذ.

الخطوة 10: يبعث عميل AAA إلى المُطالِب برسالة السماح بالنفاذ.



الشكل 10-1 – الخطوات الانسيابية للرسائل والضرورية لعملية استيقان ناجحة

2.2.10 عمليات الاستيقان غير الناجحة

تقدم الخطوات التالية والشكل 10-2 مثالاً عن مخطط لانسياب الرسائل في عملية استيقان غير ناجحة.

الخطوة 1: يطلب كيان ما النفاذ من عميل AAA.

الخطوة 2: يطلب عميل AAA من مخدم AAA الاستيقان من الكيان.

الخطوة 3: يطلب مخدم AAA من عميل AAA وسائل اعتماد الكيان قصد الشروع في الاستيقان.

الخطوة 4: يطلب عميل AAA من الكيان وسيلة/وسائل الاعتماد اللازمة للاستيقان.

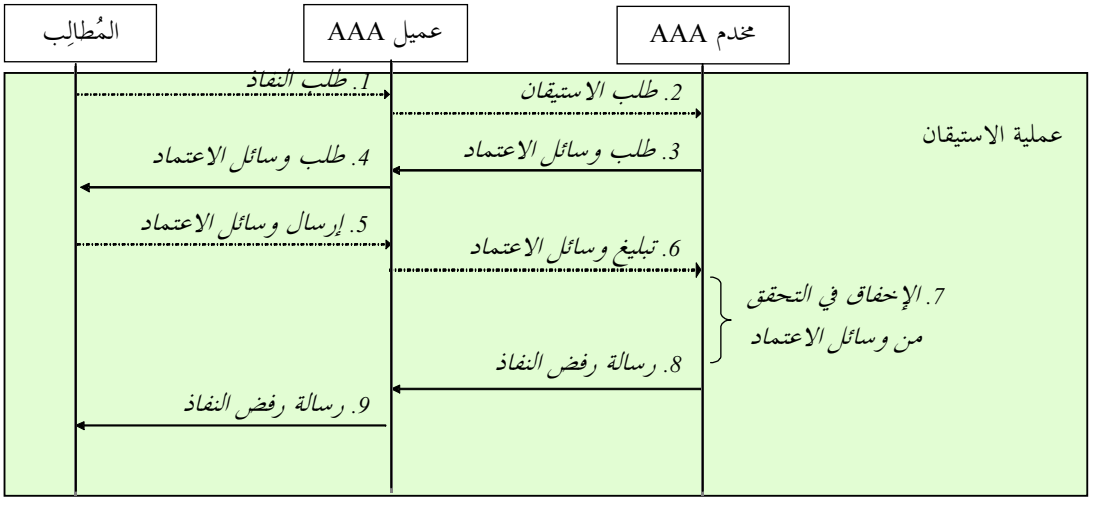
الخطوة 5: يُرسل الكيان، الذي أصبح الآن مطالباً، وسيلة/وسائل الاعتماد إلى عميل AAA.

الخطوة 6: يقوم عميل AAA بإحالة وسيلة/وسائل الاعتماد إلى مخدم AAA بهدف الاستيقان.

الخطوة 7: يتحقق مخدم AAA من وسائل الاعتماد الواردة بمقارنتها بمواصفات اعتماد المستعمل لدى المُطالِب.

الخطوة 8: إذا لم يتسنَّ التحقق من وسائل الاعتماد، يُرسِل مخدم AAA رسالة رفض النفاذ إلى عميل AAA.

الخطوة 9: يقوم عميل AAA بإحالة رسالة رفض النفاذ إلى المُطالِب.



الشكل 10-2 – الخطوات الانسيابية لعملية استيقان غير ناجحة

11 التخويل

تُعرَّف عملية التخويل على أنها عمل لتحديد ما إذا كان بالإمكان منح امتياز محدَّد إلى مورد وسيلة اعتماد محدَّدة. وقد يكون الامتياز حق النفاذ إلى مورد خدمة وقد يشمل حق القراءة أو الكتابة أو التعديل للموارد حسب السياسة المنطبقة. وتتبع عملية التخويل عملية الاستيقان كما توافق على النفاذ إلى خدمة شبكات الجيل التالي أو ترفضه تبعاً لنتائج خطوات الاستيقان السابقة وسياسته.

1.11 جوانب التخويل لشبكات الجيل التالي

الغرض من التخويل هو إتاحة النفاذ والتحكم فيه بالنسبة للخدمات المرخص بها والمستعمِل المُستَيْقَن منه. وفي شبكات الجيل التالي، يتواصل مخدم AAA مع عناصر الشبكة التي تتضمن امتيازات النفاذ للكيانات "المكتتبة".

وتعامل هذه التوصية عمليتي الاستيقان والتخويل على أنهما عمليتان مترابطتان، حيث يتم إجراؤهما عادة الواحدة تلو الأخرى من أجل الكيانات المكتتبة كلما طُلب النفاذ. ومع ذلك، فإن سياسة مورد خدمة ما قد تسمح لكيانٍ ما بطلب النفاذ/حقوق الاستخدام بشكل فوري دون معاودة الاستيقان أو الاكتتاب. وهذه الحالة ليست موضع بحث في هذه الوثيقة.

ويتم التخويل لمستعمِلٍ ما باستعمال خدمة ما من قبل مخدم AAA يقوم بإرسال واستقبال معلومات التخويل من العناصر الملائمة في الشبكة. وبعد استكمال عملية التخويل من جانب مخدم AAA، تحال معلومات الإقرار إلى المستعمل طالب الخدمة.

ويُشكل استلام معلومات الإقرار نجاح استكمال عمليات الاستيقان والتخويل معاً، وبالتالي يُعتبر الكيان طالب النفاذ موصولاً بالشبكة أو بمورد الخدمة المرخص به.

2.11 كيانات التخويل

تتم عملية التخويل بشكل أوتوماتي من قبل مخدم AAA إثر عملية الاستيقان دون مشاركة من الكيان طالب النفاذ. ويضطلع مخدم AAA بوظيفة تخصصية تتخذ قرارات التخويل بتطبيق قواعد سياسة التحكم في النفاذ.

3.11 إجراء التخويل

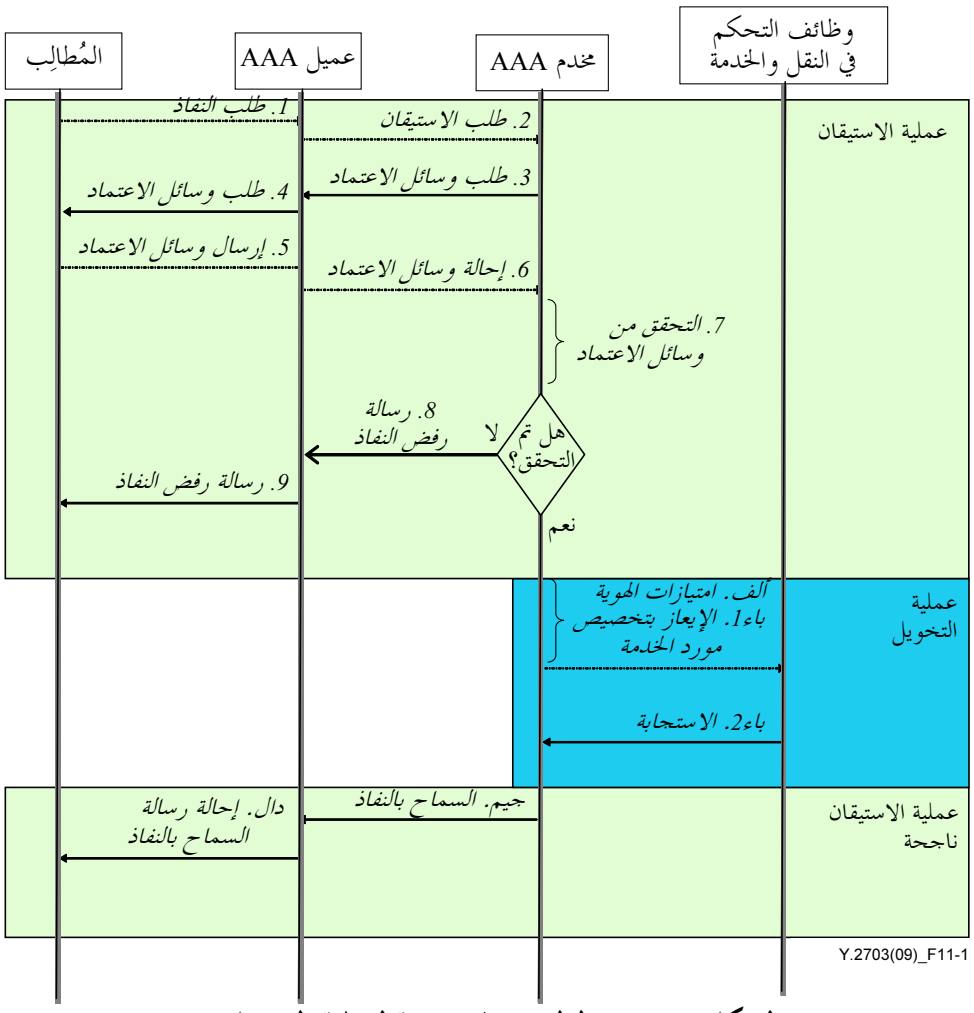
إجراء عملية التخويل موصوف في الشكل 11-1:

الخطوة ألف: بعد نجاح استيقان الكيان، يحدد مخدم AAA الخدمات والموارد المتاحة للمُطالِب والمفتوحة لنفاذه إليها.

الخطوة باء: بعد استكمال الخطوة ألف، يطلب مخدم AAA من وظائف التحكم في النقل والخدمات بتخصيص/تعيين الخدمات والموارد المرخصة لاستعمال المُطالِب.

الخطوة جيم: يُرسِل مخدم AAA رسالة سماح بالنفاذ إلى عميل AAA.

الخطوة دال: يحيل عميل AAA رسالة السماح بالنفاذ إلى المُطالِب.



الشكل 11-1 – الخطوات الانسيابية لعملية التخويل

12 المحاسبة

يرمز الحرف "A" الأخير من الحروف "AAA" إلى "المحاسبة". وفي سياق خدمة AAA تشمل المحاسبة عنصر أمن يمكن استعماله بالموازاة مع بيانات أحداث أمنية أخرى لتوفير وظيفةٍ محاسبة.

1.12 المحاسبة الأمنية

تستعمل محاسبة الأحداث الأمنية تلك المجموعة الفرعية من وظيفة المحاسبة التي توفر البيانات المحاسبية والتي تُستعمل بعدئذ في رسم مسارٍ للتدقيق الأمني قصد استعماله في وظيفة التدقيق الأمني. ويتوقف مدى مسار التدقيق الأمني على احتياجات التدقيق الأمنيٍ وسياسته التي يحددها مورد خدمة شبكات الجيل التالي لذلك السياق المحدد، من قبيل مواعيد البداية والنهاية للنفاذ الناجح وغير الناجح إلى الشبكة أو الخدمة، والخدمة التي يتم النفاذ إليها، ومعلومات الهوية الخاصة بالكيان طالب النفاذ (بالنسبة لعمليات الاستيقان الناجحة). وتقع وظيفة التدقيق الفعلية خارج نطاق هذه التوصية. وإجراء المحاسبة الأمنية مبيَّن في الشكل 12-1.

2.12 وظائف المحاسبة الأمنية

المحاسبة الأمنية مجال خدمة تضطلع بوظائف من قبيل:

1) الالتقاط: وهو مسؤول عن تجميع البيانات القابلة للاكتشاف من حدث ما وتوفير المعلومات ذات الصلة بالسياق الأمني. وقد تشمل البيانات التي يتعين التقاطها ما يلي:
   - نتائج الاستيقان؛

- المعلومات المتعلقة بإلغاء الاستيقان و/أو الشهادة؛
- المعلومات الخاصة بضمان الاستيقان؛
- غير ذلك من المعلومات المتعلقة بعملية الاستيقان.

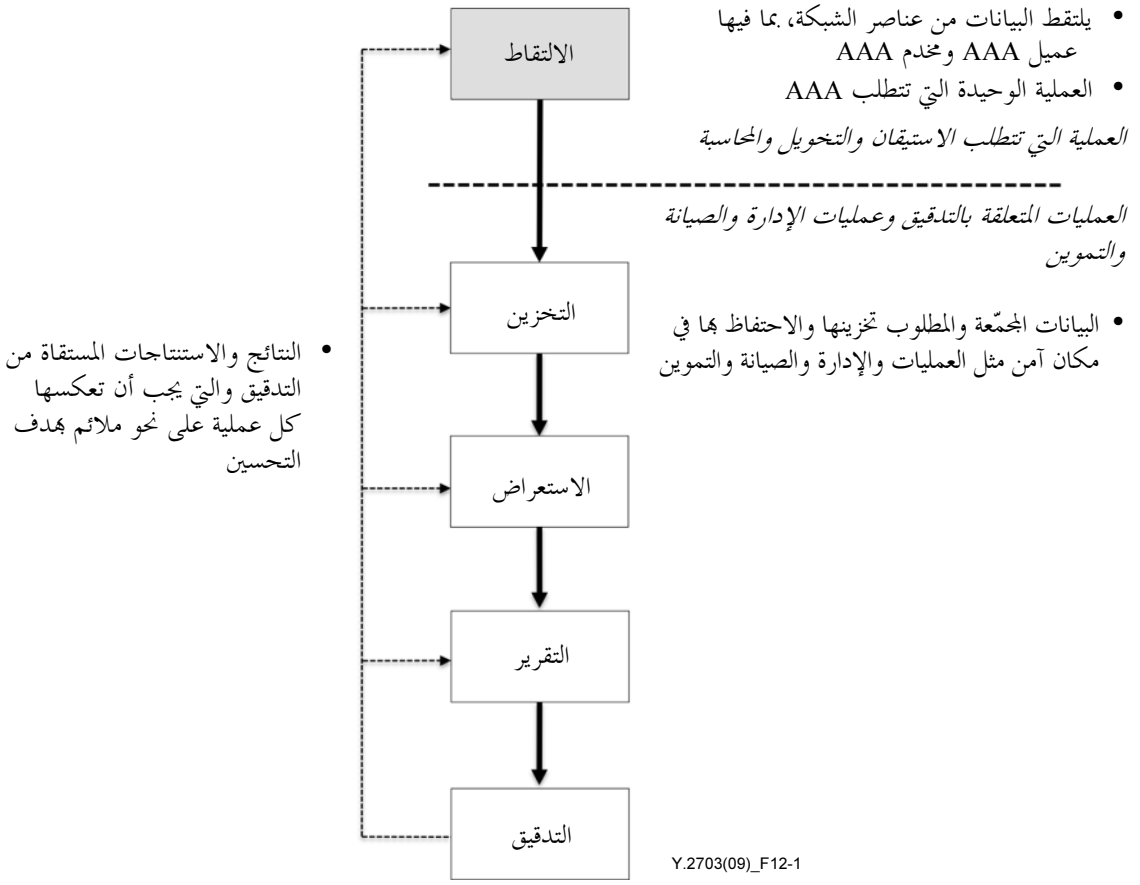
2) التخزين: يحتفظ بالبيانات التمثيلية التي تنتجها وظيفة الالتقاط.

3) الاستعراض: ويسعى لوصف الحدث وصفاً دقيقاً من خلال: التحقق من دقة ما تم التقاطه، وتمييز الحقائق من خلال فحص ما تم التقاطه.

4) التقرير: يجلب المعلومات من وظيفة الاستعراض ويقدمها لوظيفة التدقيق.

5) التدقيق: يتحقق من صحة تقرير ما للمحاسبة الأمنية أو من مطابقة سياسة الاستخدام والمبادئ التوجيهية الأمنية. وقد تتطلب وظيفة التدقيق القدرة على إطلاق الإنذار فوراً.

وجدير بالملاحظة أن "الالتقاط" فقط هو وظيفة من وظائف AAA أما التخزين والاستعراض والتقرير والتدقيق فهي وظائف إدارة. وهي وظائف تقع خارج نطاق هذه التوصية.



الشكل 12-1 – مثال عن عملية المحاسبة الأمنية

التذييل I

بروتوكول الاستيقان لخدمة AAA في شبكات الجيل التالي

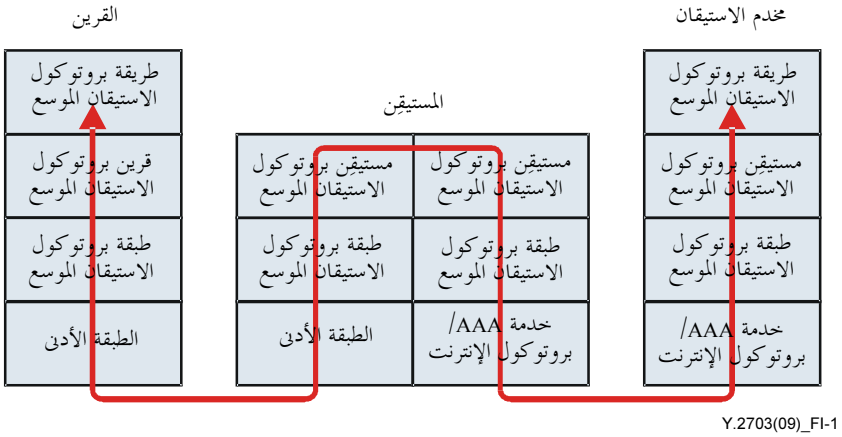
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يتناول هذا التذييل بروتوكول الاستيقان الموسع (EAP) الذي يتم نقله على طبقات وصلات البيانات، وبروتوكولات AAA التي توفر إطار خدمة AAA في شتى التطبيقات.

1.I بروتوكول الاستيقان الموسع (EAP) لخدمة AAA في شبكات الجيل التالي

يحدد بروتوكول الاستيقان الموسع إطاراً للاستيقان للاضطلاع بمختلف طرائق الاستيقان. ويتم تشغيل هذا البروتوكول على مخدم القرين والاستيقان عبر المستيقِن. ويتم نقل هذا البروتوكول مباشرة على طبقات وصلات البيانات، مثل بروتوكول IEEE 802 لمعهد مهندسي الكهرباء والإلكترونيات والبروتوكول من نقطة إلى نقطة (PPP).

ومع ذلك، وبسبب تبعية الوصلات، يتطلب بروتوكول الاستيقان الموسع الطبقة الأدنى، مثل بروتوكول الاستيقان الموسع على شبكة منطقة محلية (EAPoL)، ومعيار IEEE 802.1X، ومعيار IEEE 802.11i. ويصف الشكل 1.I نموذج الإرسال المتعدد لبروتوكول الاستيقان الموسع. وتشمل طبقة طريقة هذا البروتوكول خوارزمية الاستيقان. ولكل من قرين ومستيقِن هذا البروتوكول وظيفته الخاصة بصفته عميل استيقان ومستيقِن، على التوالي. وتتولى طبقة البروتوكول EAP تسليم رسائله. وتقوم الطبقة الأدنى بإرسال أو استلام أرتال هذا البروتوكول بين القرين والمستيقِن. ولما كانت طبقة الوصلات تتألف من مختلف بروتوكولات الوصلات، فإن بروتوكول الاستيقان الموسع يتطلب طبقات أدنى مختلفة لكل بروتوكول من بروتوكولات الوصلات.



الشكل 1.I – نموذج الإحالة لبروتوكول الاستيقان الموسع

ويتطلب بروتوكول الاستيقان الموسع الطبقة الأدنى من أجل التسليم الموثوق للرسائل واكتشاف الأخطاء وترتيب الرسائل كما يلي:

- لما كان بروتوكول الاستيقان الموسع لا يدرك أن القرين يستلم الرسالة من المستيقِن، فإن هذا البروتوكول يتطلب قناة موثوقة بين القرين والمستيقِن.
- لا يقوم بروتوكول الاستيقان الموسع بتأمين وصول رسائل هذا البروتوكول إلى مقصدها دون خطأ. وبالتالي يحتاج هذا البروتوكول إلى وظيفة لاكتشاف الأخطاء من الطبقة الأدنى.

- قد يتم تغيير الرسائل إما من حيث ترتيبها أو من حيث تكرارها لأي سبب من الأسباب. وهكذا، فإن بروتوكول الاستيقان الموسع يتطلب اكتشاف التكرار والترتيب بما يضمن صحة العمليات.
- لا تُدرك الطبقة الأدنى ما إذا كانت الطبقة الأعلى تشمل بروتوكولاً للاستيقان أم لا. ويتطلب بروتوكول الاستيقان الموسع إشارة من بروتوكول الاستيقان.

2.I بروتوكولات خدمة AAA

لقد تم في بادئ الأمر نشر بروتوكولات خدمة AAA، مثل بروتوكول خدمة المستعمل بواسطة المراقمة الداخلية للاستيقان عن بعد (RADIUS)، قصد إتاحة النفاذ بواسطة المراقمة الخارجية إلى البروتوكول من نقطة إلى نقطة وإلى المخدم المطرافي. ويُجري الجدول 1.I مقارنة بين بروتوكولين من بروتوكولات خدمة AAA.

الجدول 1.I – مقارنة بين بروتوكولي الخدمة AAA

	بروتوكول المستعمل بواسطة المراقمة الداخلية للاستيقان عن بعد (RADIUS)	**بروتوكول ديامتر (DIAMETER)**
حجم الشبكة	صغير	كبير
النقل	بروتوكول وحدات بيانات المستعمل	بروتوكول نقل التحكم في التدفق/ بروتوكول التحكم في النقل
التجفير	كلمة السر فقط	الرزمة بكاملها
الاستيقان/التخويل	مزيج	مزيج
المعيار	الفريق العامل المعني بهندسة الإنترنت	الفريق العامل المعني بهندسة الإنترنت
معمارية البروتوكول	عميل/مخدم	من نقطة إلى نقطة
قابلية التوسع	منخفضة	عالية

وفي حالة بروتوكول المستعمل بواسطة المراقمة الداخلية للاستيقان عن بعد (RADIUS) قد تستدعي إدارة مجموعات من الخطوط التسلسلية وأجهزة المودم المتناثرة لأعداد كبيرة من المستعملين قدراً لا بأس به من الدعم الإداري. ولما كانت تجمعات أجهزة المودم، بحكم تعريفها، وصلة إلى العالم الخارجي، فهي تتطلب عناية خاصة بالأمن والتخويل والمحاسبة. وأفضل سبيل لتحقيق ذلك هو إدارة "قاعدة بيانات" واحدة للمستعملين، تسمح بالاستيقان (التحقق من اسم المستعمل وكلمة السر) وكذا معلومات التشكيل التي تحدد تفاصيل نوع الخدمة الواجب تقديمها للمستعمِل.

ويمكن استعمال بروتوكول ديامتر (Diameter) الأساس بمفرده لتطبيقات المحاسبة، أما لأغراض الاستيقان والتخويل فإن هذا البروتوكول يتم توسيعه دوماً لأغراض تطبيقٍ معين.

التذييل II

الشهادات الرقمية X.509 بصفتها وسائل اعتماد

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

ثمة طريقة شائعة لتوفير ضمان الاستيقان وهي استعمال الشهادات الرقمية الموصوفة في التوصيتين [b-ITU-T X.509] و[b-ITU-T X.811]. وتتضمن الشهادة التي حددتها التوصية [b-ITU-T X.509] والتي تُستعمل على نطاق واسع، الأنواع التالية من البيانات:

- ***الصيغة (version)*** وهي صيغة الشهادة المشفّرة. وإذا كانت مكوّنة التوسعات (extensions) موجودة في الشهادة، تكون صيغة الشهادة v3. أما إذا كانت المكوّنة issuerUniqueIdentifier أو subjectUniqueIdentifier موجودة في الشهادة، فتكون الصيغة v2 أو v3.
- ***رقم التسلسل (serialNumber)*** عدد صحيح تخصصه سلطة إصدار الشهادات إلى كل شهادة. وعليه تكون قيمة رقم التسلسل فريدة لكل شهادة صادرة عن سلطة معنية لإصدار الشهادات. (أي أن اسم المُصدِر ورقم التسلسل يعرِّفان هوية شهادة فريدة).
- ***التوقيع (signature)*** تحتوي على معرف هوية الخوارزمية للخوارزمية وعلى دالّة الفرم اللتين تستعملهما سلطة إصدار الشهادات لتوقيع الشهادة (مثل md5WithRSAEncryption وsha-1WithRSAEncryption وid-dsa-with-sha1 وغيرها).
- ***المُصْدِر (issuer)*** تدل على الكيان الذي وقّع الشهادة وأصدرها.
- ***الصلاحية (validity)*** الفاصل الزمني الذي تضمن فيه سلطة إصدار الشهادات أنها ستحتفظ بالمعلومات الخاصة بوضع الشهادة.
- ***الغرض (subject)*** يدل على الكيان المرتبط بالمفتاح العمومي الموجود في حقل "المفتاح العمومي للغرض".
- ***معلومات المفتاح العمومي للغرض (subjectPublicKeyInfo)*** تُستعمل لنقل المفتاح العمومي الجاري تصديقه وللتعريف بالخوارزمية التي يشكل هذا المفتاح العمومي تعبيراً لها (مثل rsaEncryption وdhpublicnumber وid-dsa وغيرها).
- ***معرف الهوية الوحيد للمُصْدِر (issuerUniqueIdentifier)*** تُستعمل للتعريف دون لبس بمُصدِر، في حالة إعادة استخدام اسم.
- ***معرف الهوية الوحيد للغرض (subjectUniqueIdentifier)*** تُستعمل للتعريف دون لبس بغرض، في حالة إعادة استخدام اسم.
- ***حقل التوسّعات (extensions field)*** يتيح إضافة حقول جديدة إلى البنية.

التذييل III

حالة استعمال الاستيقان والتخويل

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

تستند حالة الاستعمال الخاصة بخدمة AAA في هذا التذييل إلى النموذج المرجعي المورد في التوصية [b-ITU-T Y.2702].

1.III الاستيقان والتخويل لنفاذ المستعمِل إلى الشبكة

ثمة حاجة إلى خدمات الاستيقان من النفاذ إلى الشبكة والتخويل بهذا النفاذ وذلك بهدف التحقق من الهويات وتحديد ما إذا كان ينبغي السماح بالنفاذ لتجهيزات المستعمل النهائي.

1.1.III الاستيقان والتخويل لنفاذ الأجهزة إلى شبكات الجيل التالي أو ارتباطها بها

في هذه الحالة، ثمة 3 أنواع من خدمات وقدرات الاستيقان والتخويل لنفاذ الأجهزة إلى شبكات الجيل التالي أو ارتباطها بها. وهي تهدف إلى تحديد الهوية والاستيقان والتخويل لنفاذ أجهزة المستعمل إلى شبكة النفاذ القائمة على بروتوكول الإنترنت أو ارتباطها بها:

- تحديد الهوية والاستيقان والتخويل للتجهيزات المطرافية التقليدية وعناصر حدود التجهيزات المطرافية من أجل النفاذ إلى شبكة النفاذ القائمة على بروتوكول الإنترنت أو الارتباط بها ((1) من الشكل 1.III)؛
- تحديد الهوية والاستيقان والتخويل للتجهيزات المطرافية التقليدية وعناصر حدود التجهيزات المطرافية المجهزة بتجهيزات النفاذ المتكامل ضمن مجال العميل من أجل النفاذ إلى شبكة النفاذ القائمة على بروتوكول الإنترنت أو الارتباط بها ((2) من الشكل 1.III)؛
- تحديد الهوية والاستيقان والتخويل للتجهيزات المطرافية وعناصر حدود التجهيزات المطرافية المجهزة بقدرات بروتوكول الإنترنت ضمن مجال العميل من أجل النفاذ إلى شبكة النفاذ القائمة على بروتوكول الإنترنت أو الارتباط بها ((3) من الشكل 1.III).

يقدم عميل AAA خدمة الاستيقان لمورد الجهاز والشبكة: فهو يسمح أوتوماتياً للجهاز بالنفاذ إلى مورد الشبكة حسبما يقتضيه الحال.

ويكون إجراء تحديد الهوية الموصوف في (1) من الشكل 1.III كما يلي:

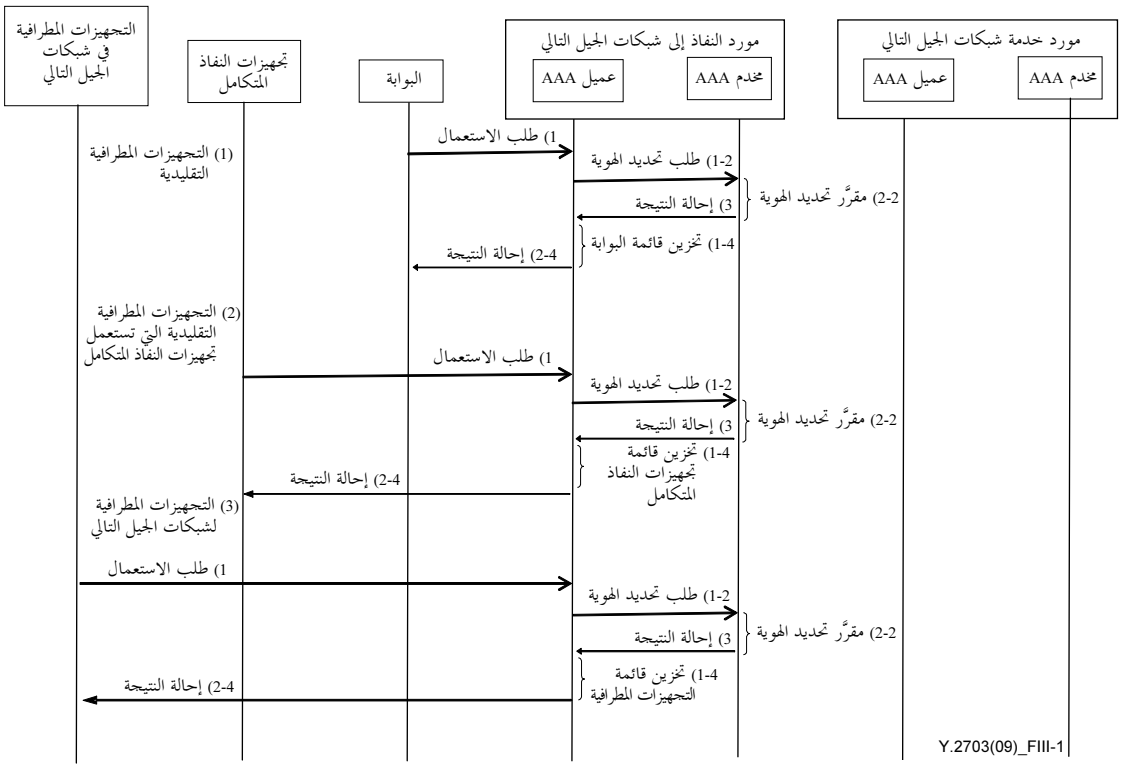
الخطوة 1: تطلب البوابة (المُطالِب) النفاذ إلى/الارتباط من عميل AAA.

الخطوة 2: يطلب عميل AAA تحديد هوية البوابة من مخدم AAA (المحقِّق) الذي يحدد هوية البوابة.

الخطوة 3: يُرسل مخدم AAA نتائج تحديد الهوية إلى عميل AAA.

الخطوة 4: يحيل عميل AAA النتائج إلى البوابة، حيث يُخزن عميل AAA قائمة نفاذ البوابة.

في الحالتين (2) و(3)، تضطلع تجهيزات النفاذ المتكامل والتجهيزات المطرافية لشبكات الجيل التالي بدور المُطالِب على التوالي. وتكون بقية العملية مطابقة لإجراء (1).



الشكل 1.III – إجراء تحديد الهوية لنفاذ الأجهزة إلى شبكات الجيل التالي

2.1.III نفاذ الأجهزة المجمَّعة إلى شبكات الجيل التالي/ارتباطها بها واستيقان وتخويل الخدمة/التطبيق

في هذه الحالة، ثمة 3 أنواع من خدمات وقدرات الاستيقان والتخويل لنفاذ الأجهزة إلى شبكات الجيل التالي أو ارتباطها بها وهي تهدف إلى ضم استيقان جهاز المستعمل عن طريق مورد النفاذ المجهز بشبكات الجيل التالي إلى استيقان وتخويل الاستعمال عن طريق مورد الخدمة المجهز بشبكات الجيل التالي:

- خدمات وقدرات مورد خدمة شبكات الجيل التالي على القيام ضمنياً بتحديد هوية وتخويل الأجهزة المطرافية التقليدية وعناصر حدود التجهيزات المطرافية ((1) من الشكل 2.III)؛
- خدمات وقدرات مورد خدمة شبكات الجيل التالي على القيام ضمنيّاً بتحديد هوية وتخويل الأجهزة المطرافية التقليدية وعناصر حدود التجهيزات المطرافية المجهزة بتجهيزات النفاذ المتكامل ((2) من الشكل 2.III)؛
- خدمات وقدرات مورد خدمة شبكات الجيل التالي على القيام مباشرةً بتحديد هوية وتخويل الأجهزة المطرافية لشبكات الجيل التالي وعناصر حدود التجهيزات المطرافية في مجال العميل ((3) من الشكل 2.III).

يقدم عميل AAA خدمة الاستيقان لمورد الجهاز والخدمة/التطبيق: فهو يسمح أوتوماتياً للجهاز بالنفاذ إلى مورد الخدمة/التطبيق حسبما يقتضيه الحال.

ويكون إجراء تحديد الهوية الموصوف في (1) من الشكل 2.III كما يلي:

الخطوة 1: تطلب البوابة (المُطالِب) استعمال الخدمة/التطبيق من عميل AAA.

الخطوة 2: يطلب عميل AAA تحديد هوية البوابة من مخدم AAA (المحقِّق) ضمن نطاق شبكة النفاذ، حيث يقوم مخدم AAA بتحديد هوية البوابة.

الخطوة 3: يُرسل مخدم AAA نتائج تحديد الهوية إلى عميل AAA وإلى مخدم AAA ضمن نطاق مورد الخدمة المجهز بشبكات الجيل التالي على نحو متزامن.

الخطوة 4: يحيل عميل AAA النتائج إلى البوابة، حيث يُخزن عميل AAA قائمة نفاذ البوابة.

ويكون إجراء تحديد الهوية الموصوف في (2) من الشكل 2.III كما يلي:

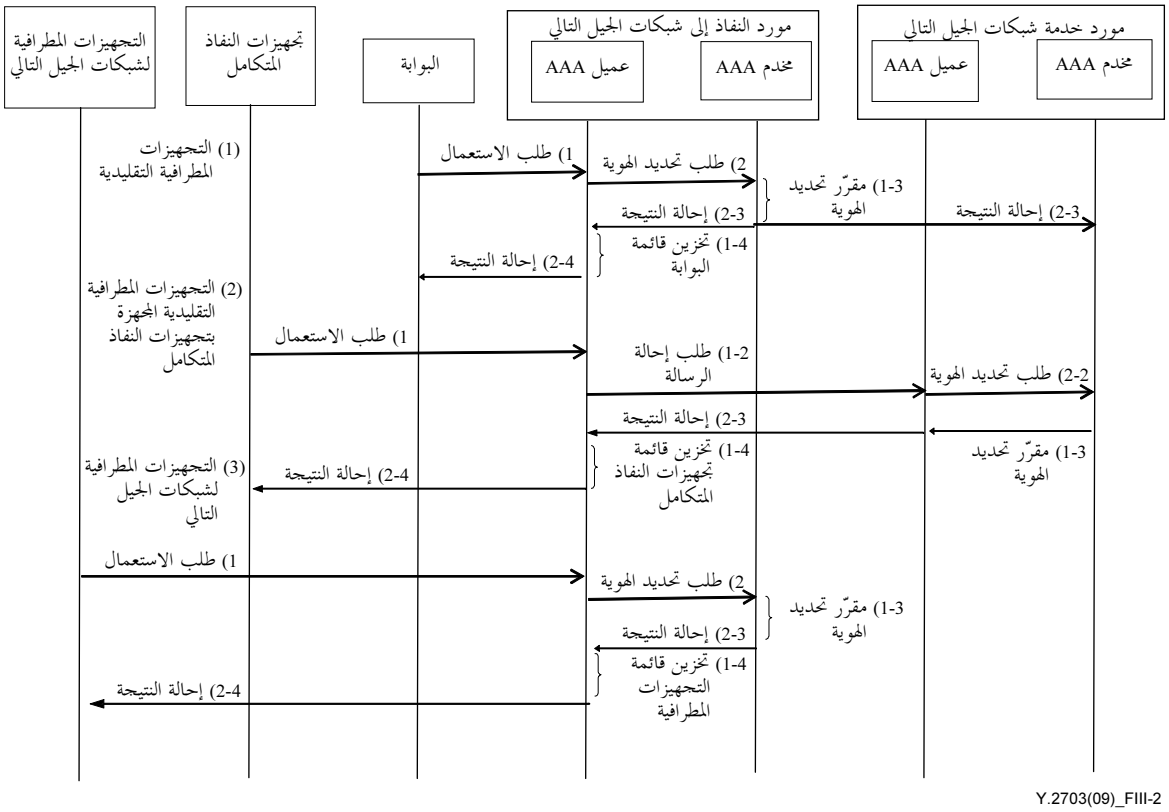
الخطوة 1: يطلب جهاز النفاذ المتكامل (المُطالِب) استعمال الخدمة/التطبيق من عميل AAA.

الخطوة 2: يطلب عميل AAA تحديد هوية تجهيزات النفاذ المتكامل من عميل AAA ضمن نطاق مورد الخدمة المجهز بشبكات الجيل التالي، حيث يقوم مخدم AAA (المحقِّق) ضمن مجال مورد الخدمة المجهز بشبكات الجيل التالي بتحديد هوية تجهيزات النفاذ المتكامل.

الخطوة 3: يُرسل مخدم AAA نتائج تحديد الهوية إلى عميل AAA.

الخطوة 4: يحيل عميل AAA النتائج إلى جهاز النفاذ المتكامل، حيث يُخزن عميل AAA قائمة نفاذ تجهيزات النفاذ المتكامل.

في الحالة (3)، يكون الجهاز المطرافي لشبكات الجيل التالي هو المُطالِب. وتكون بقية العملية مطابقة للإجراء (2).



الشكل 2.III – إجراء تحديد الهوية لتمكين جهاز من استعمال الخدمة/التطبيق لدى موردِيها

2.III استيقان وتخويل مورد خدمة شبكات الجيل التالي لنفاذ المستعمِل إلى الخدمة/التطبيق

في هذه الحالة، ثمة 3 أنواع من خدمات وقدرات استيقان وتخويل الخدمة/التطبيق لدى مورد شبكات متعددة:

- استيقان مورد الخدمة المجهز بشبكات الجيل التالي بشكل غير مباشر من جهاز المستعمل من خلال علاقات الثقة مع مورد النفاذ المجهز بشبكات الجيل التالي ((1) من الشكل 3.III)؛
- استيقان وتخويل مورد الخدمة المجهز بشبكات الجيل التالي بشكل مباشر لجهاز المستعمل ((2) من الشكل 3.III)؛
- استيقان مورد الخدمة المجهز بشبكات الجيل التالي بشكل مباشر من المستعمل ((3) من الشكل 3.III).

يقدم عميل AAA خدمة الاستيقان للمستعمِل ولمورد الخدمة/التطبيق: فهو يسمح أوتوماتياً للمستعمِل بالنفاذ إلى مورد الخدمة/التطبيق حسبما يقتضيه الحال.

ويكون إجراء تحديد الهوية الموصوف في (1) من الشكل 3.III كما يلي:

الخطوة 1: يطلب الجهاز المطرافي (المُطالِب) استعمال الخدمة/التطبيق من عميل AAA.

الخطوة 2: يطلب عميل AAA تحديد هوية الجهاز من مخدم AAA (المحقِّق) ضمن مجال شبكة النفاذ، حيث يقوم مخدم AAA بتحديد هوية الجهاز.

الخطوة 3: يُرسل مخدم AAA نتائج تحديد الهوية إلى عميل AAA وإلى مخدم AAA ضمن مجال مورد الخدمة المجهز بشبكات الجيل التالي على نحو متزامن.

الخطوة 4: يحيل عميل AAA النتائج إلى البوابة، حيث يُخزن عميل AAA قائمة نفاذ الجهاز.

ويكون إجراء تحديد الهوية الموصوف في (2) من الشكل 3.III فيما يلي:

الخطوة 1: يطلب الجهاز المطرافي (المُطالِب) استعمال الخدمة/التطبيق من عميل AAA ضمن مجال مورد الخدمة المجهز بشبكات الجيل التالي.

الخطوة 2: يطلب عميل AAA تحديد هوية الجهاز من مخدم AAA (المحقِّق) ضمن مجال مورد الخدمة المجهز بشبكات الجيل التالي، حيث يقوم مخدم AAA بتحديد هوية الجهاز.

الخطوة 3: يُرسل مخدم AAA نتائج تحديد الهوية إلى عميل AAA.

الخطوة 4: يحيل عميل AAA النتائج إلى الجهاز، حيث يُخزن عميل AAA قائمة نفاذ الجهاز.

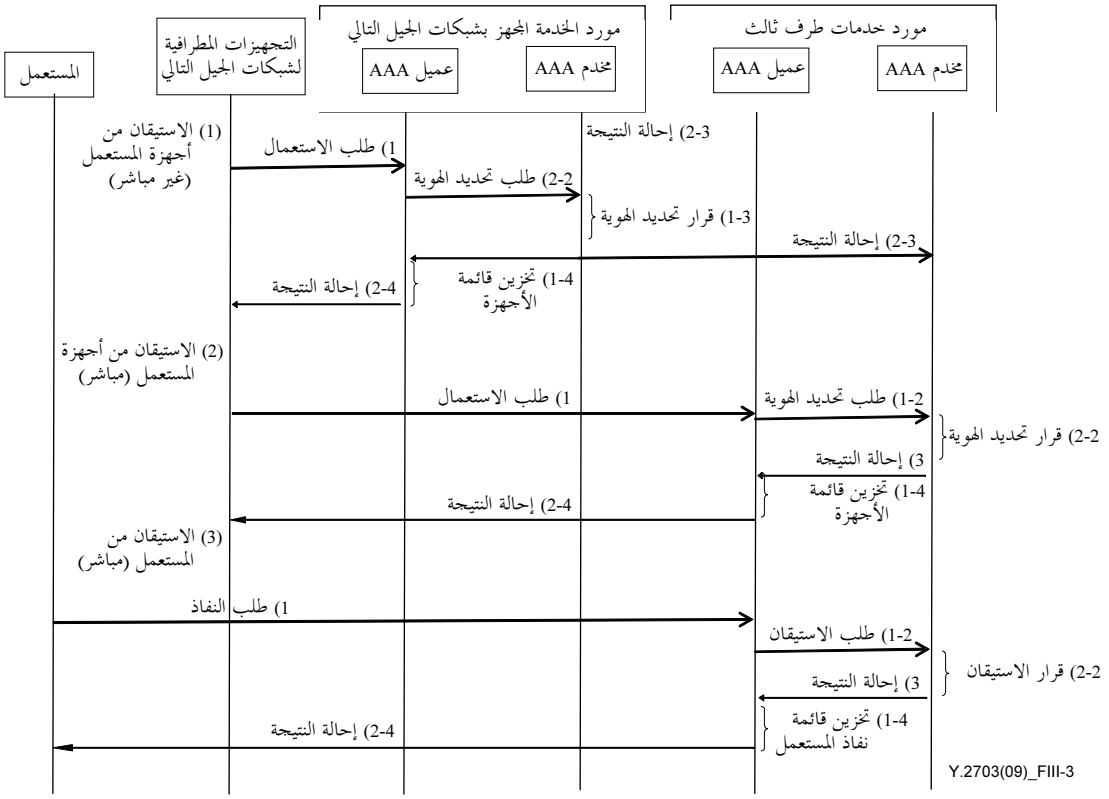
ويكون إجراء الاستيقان الموصوف في (3) من الشكل 3.III كما يلي:

الخطوة 1: يطلب المستعمل (المُطالِب) استعمال الخدمة/التطبيق من عميل AAA ضمن مجال مورد الخدمة المجهز بشبكات الجيل التالي.

الخطوة 2: يطلب عميل AAA الاستيقان المستعمل من مخدم AAA (المحقِّق) ضمن مجال مورد الخدمة المجهز بشبكات الجيل التالي، حيث يقوم مخدم AAA بالاستيقان من المستعمل.

الخطوة 3: يُرسل مخدم AAA نتائج الاستيقان إلى عميل AAA.

الخطوة 4: يحيل عميل AAA النتائج إلى المستعمل، حيث يُخزن عميل AAA قائمة نفاذ المستعمل.



الشكل 3.III – إجراء الاستيقان من المستعمل والتخويل له من قبل مورد الخدمة المجهز بشبكات الجيل التالي

3.III استيقان وتخويل المستعمِل لموردي خدمة شبكات الجيل التالي

في هذه الحالة، ثمة نوعان من عمليات الاستيقان من المستعمل والتخويل للشبكة:

- استيقان المستعمل من ارتباط مورد شبكات الجيل التالي بالشبكة ((1) من الشكل 4.III)؛
- استيقان المستعمل من حصول مورد شبكات الجيل التالي على الخدمة ((2) من الشكل 4.III).

يقدم عميل AAA خدمة استيقان المستعمل والتخويل للشبكة: فهو يسمح أوتوماتياً للمستعمل بالنفاذ إلى مورد خدمة/الشبكة حسبما يقتضيه الحال.

ويكون إجراء تحديد الهوية الموصوف في (1) من الشكل 4.III كما يلي:

الخطوة 1: يطلب المستعمل (المُطالِب) الاستيقان من نقاط النفاذ إلى الشبكة من الطرف الثالث المحقِّق.

الخطوة 2: يحيل الطرف الثالث المحقِّق معلومات الاستيقان إلى نقاط النفاذ إلى الشبكة.

الخطوة 3: يتم تبادل معلومات الاستيقان بين الطرف الثالث المحقِّق ونقاط النفاذ إلى الشبكة.

الخطوة 4: يحيل الطرف الثالث المحقِّق النتائج إلى المستعمل، حيث يتحقق منها هذا المحقِّق.

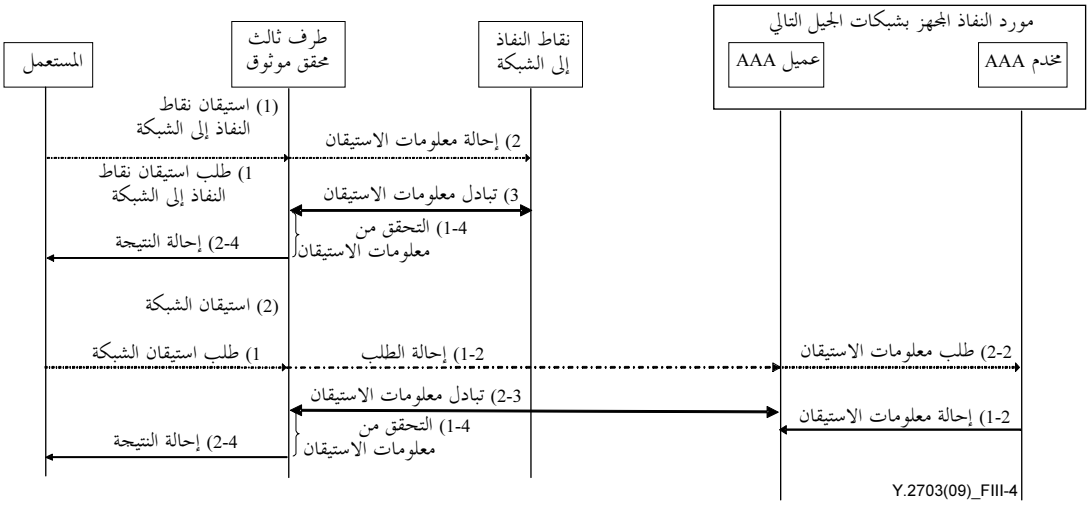
ويكون إجراء تحديد الهوية الموصوف في (2) من الشكل 4.III كما يلي:

الخطوة 1: يطلب المستعمِل (المُطالِب) استيقان الشبكة من الطرف الثالث المحقِّق.

الخطوة 2: يحيل الطرف الثالث المحقِّق طلب المستعمل إلى عميل AAA، حيث يطلب عميل AAA معلومات الاستيقان من مخدم AAA.

الخطوة 3: يُرسل مخدم AAA معلومات الاستيقان إلى عميل AAA ويتم تبادل معلومات الاستيقان بين الطرف الثالث المحقِّق وعميل AAA.

الخطوة 4: يحيل الطرف الثالث المحقِّق النتائج إلى المستعمل، حيث يتحقق منها هذا المحقِّق.



الشكل 4.III – إجراء الاستيقان والتخويل لموردي خدمة شبكات الجيل التالي من قبل المستعمل

4.III استيقان وتخويل مورد شبكات الجيل التالي للطرف الثالث مورد الخدمة/التطبيق

قد يكون هنالك سيناريو يختلف فيه مورد التطبيق أو الخدمة عن مورد شبكات الجيل التالي (أي طرف ثالث مورد الخدمة/التطبيق). وفي هذه الحالة، يتعين على مورد شبكات الجيل التالي الاستيقان من الطرف الثالث مورد الخدمة/التطبيق والتخويل له.

يقدم عميل AAA خدمة الاستيقان لمورد شبكات الجيل التالي الذي يضطلع بالاستيقان من الطرف الثالث مورد الخدمة/التطبيق والتخويل له.

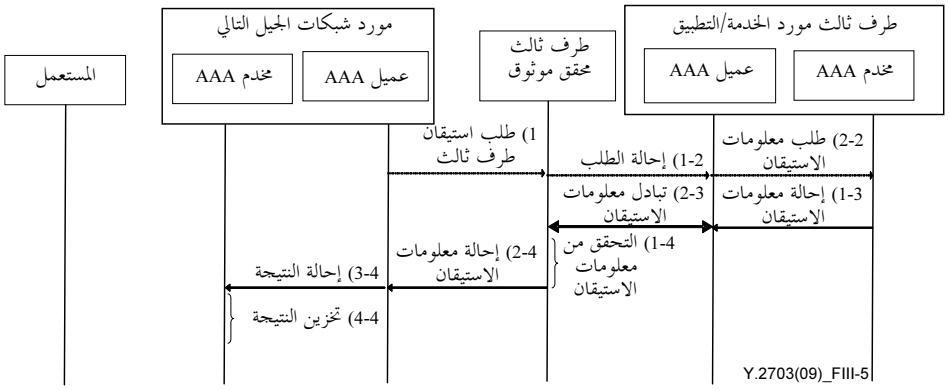
ويكون إجراء تحديد الهوية الموصوف في الشكل 5.III كما يلي:

الخطوة 1: يطلب عميل AAA (المُطالِب) لدى مورد شبكات الجيل التالي الاستيقان من الطرف الثالث مورد الخدمة/التطبيق من الطرف الثالث المحقِّق.

الخطوة 2: يحيل الطرف الثالث المحقِّق طلب المستعمل إلى عميل AAA لدى الطرف الثالث مورد الخدمة/التطبيق ويطلب عميل AAA معلومات الاستيقان من مخدم AAA.

الخطوة 3: يحيل مخدم AAA معلومات الاستيقان إلى عميل AAA ويتم تبادل معلومات الاستيقان بين الطرف الثالث المحقِّق وعميل AAA.

الخطوة 4: يحيل الطرف الثالث المحقِّق النتائج إلى عميل AAA لدى مورد شبكات الجيل التالي، حيث يقوم الطرف الثالث المحقِّق بالتحقق ويقوم مخدم AAA بتخزين النتيجة.



الشكل 5.III – إجراء الاستيقان والتخويل للطرف الثالث مورد الخدمة/التطبيق من قبل مورد شبكات الجيل التالي

5.III استعمال خدمة الاستيقان والتخويل الموردة من طرف ثالث

يستطيع موردو الخدمات توفير الاستيقان والتخويل كطرف ثالث. وفي هذه الحالة، ثمة نوعان من استعمال خدمة الاستيقان والتخويل من جانب طرف ثالث:

- الاستيقان من المستعمل لصالح مورد خدمات ((1) في الشكل 6.III)؛
- الاستيقان من مورد خدمات لصالح المستعمل ((2) في الشكل 6.III).

1.5.III الاستيقان من المستعمل لصالح مورد خدمات

يوفر عميل AAA خدمة الاستيقان لمستعمل الاستيقان والتخويل لصالح مورد خدمات: فهو يسمح أوتوماتياً للمستعمل بالنفاذ إلى الطرف الثالث مورد الخدمة/التطبيق حسبما يقتضيه الحال.

ويكون إجراء تحديد الهوية الموصوف في الشكل 6.III كما يلي:

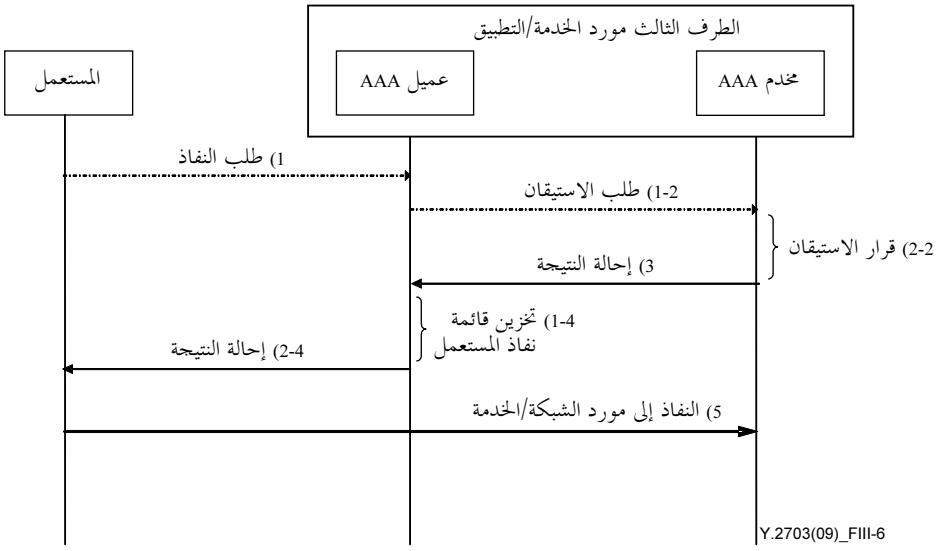
الخطوة 1: يطلب المستعمل (المُطالِب) من عميل AAA النفاذ إلى الشبكة.

الخطوة 2: يطلب عميل AAA مؤهلات من المستعمل لدى مخدم AAA عند الطرف الثالث مورد الخدمة/التطبيق، حيث يقوم مخدم AAA (المحقِّق) بالاستيقان من المستعمل.

الخطوة 3: يُرسل مخدم AAA نتائج الاستيقان إلى عميل AAA.

الخطوة 4: يحيل عميل AAA النتائج إلى المستعمل، حيث يُخزن عميل AAA قائمة نفاذ المستعمل.

الخطوة 5: في حال تخويله، يُمكن للمستعمل النفاذ إلى المورد المحدد في الشبكة.



الشكل 6.III – إجراء استعمال خدمة الطرف الثالث للاستيقان والتخويل

2.5.III الاستيقان من مورد خدمات لصالح المستعمل

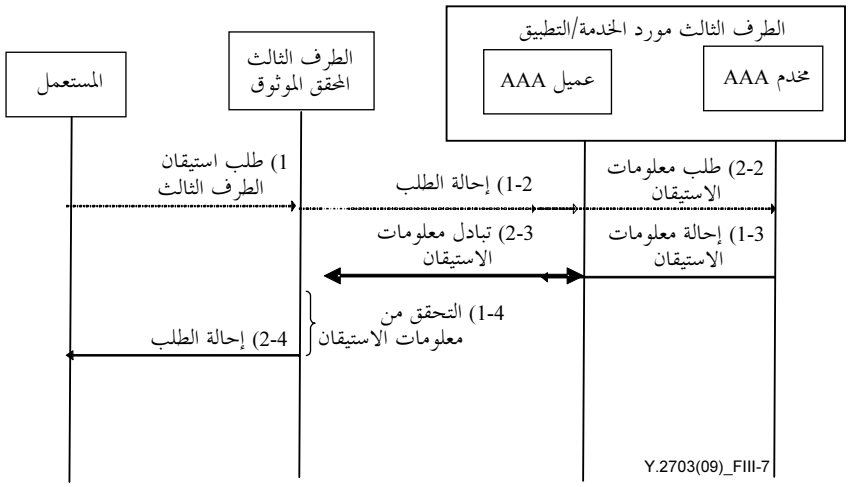
يوفر عميل AAA خدمة الاستيقان من مورد خدمة لصالح المستعمل. وإجراء تحديد الهوية الموصوف في الشكل 7.III كما يلي:

الخطوة 1: يطلب المستعمِل (المُطالِب) في مجال العميل من الطرف الثالث المحقِّق الاستيقان من الطرف الثالث مورد الخدمة/التطبيق.

الخطوة 2: يحيل الطرف الثالث المحقِّق طلب المستعمل إلى عميل AAA لدى الطرف الثالث مورد الخدمة/التطبيق ويطلب عميل AAA معلومات الاستيقان من مخدم AAA.

الخطوة 3: يحيل مخدم AAA معلومات الاستيقان إلى عميل AAA ويتم تبادل معلومات الاستيقان بين الطرف الثالث المحقِّق وعميل AAA.

الخطوة 4: يحيل الطرف الثالث المحقِّق النتائج إلى عميل AAA لدى مورد شبكات الجيل التالي، حيث يتحقق الطرف الثالث المحقِّق من النتيجة ويخزنها.



الشكل 7.III – إجراء استعمال خدمة الطرف الثالث للاستيقان والتخويل

ثبت المراجع

[b-ITU-T M.3410] Recommendation ITU-T M.3410 (2008), *Guidelines and requirements for security management systems to support telecommunications management*.

[b-ITU-T Q.3201] Recommendation ITU-T Q.3201 (2007), *EAP-based security signalling protocol architecture for network attachment*.

[b-ITU-T Q.3202.1] Recommendation ITU-T Q.3202.1 (2008), *Authentication protocols based on EAP-AKA for interworking among 3GPP, WiMax, and WLAN in NGN*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[b-ITU-T X.812] Recommendation ITU-T X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

[b-ITU-T X.816] Recommendation ITU-T X.816 (1995) | ISO/IEC 10181-7:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for next generation networks*.

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.

[b-ITU-T Y.2233] Recommendation ITU-T Y.2233 (2008), *Requirements and framework allowing accounting and charging capabilities in NGN*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

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، 2010