الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2702

(2008/09)

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

شبكات الجيل التالي – الأمن

متطلبات الاستيقان والترخيص في الإصدار 1 من شبكات الجيل التالي

التوصيـــة ITU-T Y.2702

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.2702

متطلبات الاستيقان والترخيص في الإصدار 1 من شبكات الجيل التالي

ملخص

تحدد التوصية ITU-T Y.2702 متطلبات الاستيقان والترخيص في شبكات الجيل التالي (NGN).

المصدر

وافقت لجنة الدراسات 13 (2005-2008) لقطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات على التوصية ITU-T Y.2702 بتاريخ 12 سبتمبر 2008 بموجب الإجراء الوارد في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

كلمات رئيسية

نعوت، استيقان، ترخيص، معرفات، إدارة الهوية (IdM)، شبكات الجيل التالي (NGN)، امتيازات، أمن.

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

التوصيـــة ITU-T Y.2702

متطلبات الاستيقان والترخيص في الإصدار 1 من شبكات الجيل التالي

1 مجال التطبيق

تتناول هذه التوصية متطلبات الاستيقان والترخيص في شبكات الجيل التالي (NGN) استناداً إلى [ITU-T Y.2012]. ويشمل ذلك متطلبات الاستيقان والترخيص وحيد الاتجاه والمتبادل عبر سطح التماس بين المستعمل والشبكة (UNI)، وسطح التماس بين شبكتين (NNI) وسطح التماس بين تطبيق وشبكة (ANI) وكذلك أي كيانات داخلية في شبكة ما قد تتطلب الاستيقان والترخيص. ويشمل نطاق تطبيق هذه التوصية ما يلي:

1) استيقان وترخيص المستعمل للنفاذ إلى الشبكة (مثال ذلك استيقان وترخيص جهاز مستعمل نهائي أو بوابة شبكة في منزل أو بوابة مؤسسة من أجل النفاذ إلى الشبكة أو الارتباط بها)

2) استيقان وترخيص المستعمل من جانب مقدم الخدمة للنفاذ إلى الخدمة/التطبيق (مثال ذلك استيقان وترخيص مستعمل أو جهاز أو مجموع مستعمل/جهاز حيث ينطبق الاستيقان والترخيص على النفاذ إلى خدمة/تطبيق في شبكات الجيل التالي)

3) استيقان وترخيص الشبكة من جانب المستعمل (مثال ذلك استيقان المستعمل من هوية شبكة موصولة من شبكات الجيل التالي أو من مقدم الخدمة)

4) الاستيقان والترخيص المتبادل بين المستعملين (مثال ذلك استيقان وترخيص المستعمل المطلوب (أو كيان مطراف)، أو استيقان وترخيص كيان مصدر الاتصال، أو استيقان مصدر البيانات كوظيفة من وظائف الشبكة)

5) الاستيقان والترخيص المتبادل بين الشبكات (مثال ذلك الاستيقان والترخيص عبر سطح التماس بين شبكتين في مستوى النقل أو مستوى الخدمة/التطبيق)

6) استيقان وترخيص مقدم الخدمة/التطبيق

7) استعمال خدمة الاستيقان والترخيص من جانب طرف ثالث

8) استيقان الأشياء (مثال ذلك معرّف عملية تطبيق أو محتوى رسالة أو محتوى بيانات).

تشمل البنود المدرجة أعلاه استيقان تدفقات التشوير وحركة الحامل والإدارة، حسب مقتضى الحال.

وعلاوة على ذلك تقدم هذه التوصية نماذج مرجعية لاستيقان شبكات الجيل التالي.

الملاحظة 1 – يُنظر إلى استيقان وترخيص شبكات الجيل التالي كجزء من الموضوع الأوسع لإدارة الهوية (IdM) في شبكات الجيل التالي (NGN). وعلى وجه التحديد، ينبغي أن تستعمل وظائف ومقدرات الاستيقان والترخيص الموصوفة في هذه التوصية لدعم مقدرات التأكد من الهوية وذلك لإدارة الهوية في شبكات الجيل التالي (NGN IdM).

الملاحظة 2 – استعمال المصطلح "مستعمل" في هذه التوصية لا يعني الاقتصار على شخص ما. فقد يكون المستعمل شخصاً أو مجموعات أو مؤسسات أو كيانات قانونية.

الملاحظة 3 – استيقان كيان ما لا يعني الدلالة على صلاحية شخص.

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. ولا تضفي مجرد الإحالة إلى وثيقة ما ترد في هذه التوصية صفة التوصية على هذه الوثيقة.

[ITU-T X.800] التوصية ITU-T X.800، (1991) *معمارية الأمن للتوصيل بين الأنظمة المفتوحة.*

[ITU-T X.805] التوصية ITU-T X.805 (2003)، *معمارية الأمن لأنظمة توفير الاتصالات من طرف إلى طرف.*

[ITU-T X.810] التوصية ISO/IEC 10181-1:1996 | ITU-T X.810 (1995)، *تكنولوجيا المعلومات – التوصيل بين الأنظمة المفتوحة – إطار الأمن للأنظمة المفتوحة: لمحة عامة.*

[ITU-T X.811] التوصية ISO/IEC 10181-2:1996 | ITU-T X.811 (1995)، *تكنولوجيا المعلومات – التوصيل بين الأنظمة المفتوحة – أطر الأمن لنظام مفتوح: إطار الاستيقان.*

[ITU-T Y.2012] التوصية ITU-T Y.2012 (2006)، *المتطلبات الوظيفية ومعمارية الإصدار 1 من شبكات الجيل التالي.*

[ITU-T Y.2201] التوصية ITU-T Y.2201 (2007)، *متطلبات الإصدار 1 من شبكات الجيل التالي.*

[ITU-T Y.2701] التوصية ITU-T Y.2701 (2007)، *متطلبات الأمن للإصدار 1 من شبكات الجيل التالي.*

3 التعاريف

1.3 تعاريف التوصية [ITU-T X.800]

تستخدم التوصية الحالية المصطلحات التالية المحددة في التوصية [ITU-T X.800]:

1.1.3 معلومات الاستيقان: معلومات تستعمل للتحقق من صلاحية هوية مدّعاة.

2.1.3 الترخيص: منح الحقوق التي تشمل منح إمكانية النفاذ استناداً إلى حقوق النفاذ.

3.1.3 أوراق الاعتماد: بيانات تقدم لتثبيت هوية مزعومة لكيان ما.

4.1.3 استيقان مصدر البيانات: التصديق على أن مصدر البيانات المتلقاة هو المصدر المدّعي.

5.1.3 الاستيقان بين الكيانات: التصديق على أن كياناً آخر في رابطة ما هو الكيان المدّعي.

2.3 تعاريف التوصية [ITU-T X.810]

تستخدم التوصية الحالية المصطلحين التاليين المعرّفين في التوصية [ITU-T X.810]:

1.2.3 الثقة: يقال إن الكيان X يثق بالكيان Y بالنسبة لمجموعة من الأنشطة فقط شريطة أن يعتمد الكيان X على تصرف الكيان Y بشكل محدد فيما يتعلق بالأنشطة.

2.2.3 طرف ثالث موثوق به: سلطة أمن، أو وكيل لها، موثوق بها فيما يتعلق ببعض الأنشطة المتصلة بالأمن (في سياق سياسة أمن).

3.3 تعاريف التوصية [ITU-T X.811]

تستخدم التوصية الحالية المصطلحات التالية المعرفة في التوصية [ITU-T X.811]:

1.3.3 أسلوب الاستيقان اللاتناظري: طريقة في الاستيقان لا يتقاسم فيها الكيانان جميع معلومات الاستيقان.

2.3.3 هوية مستيقن منها: معرف متميز لكيان أساس تم التأكد منه بواسطة الاستيقان.

3.3.3 الاستيقان: توفير التأكيد على صحة الهوية التي يدعيها كيان ما.

4.3.3 شهادة الاستيقان: شهادة أمن تضمنها سلطة استيقان ويمكن استعمالها لتأكيد هوية كيان ما.

5.3.3 تبادل الاستيقان: تتابع لنقل واحد أو أكثر لتبادل معلومات الاستيقان (AI) لأغراض القيام بعملية استيقان.

6.3.3 معلومات الاستيقان (AI): معلومات تستخدم لأغراض الاستيقان.

7.3.3 بادئ الاستيقان: الكيان الذي يبدأ تبادل الاستيقان.

8.3.3 المدّعي: كيان أو ممثل كيان أساس لأغراض الاستيقان. يحتوي الكيان المدعي على الوظائف اللازمة للدخول في تبادلات استيقان بالنيابة عن الكيان الأساس.

9.3.3 معلومات استيقان الادعاء (claim AI): معلومات يستعملها المدعي لتوليد تبادل معلومات استيقان ضرورية لاستيقان كيان أساس.

10.3.3 معلومات تبادل الاستيقان (exchange AI): معلومات متبادلة بين مدعٍ ومتحقق أثناء عملية استيقان كيان أساس.

11.3.3 الأساس: الكيان الذي يمكن التحقق من هويته.

12.3.3 طريقة الاستيقان التناظري: طريقة استيقان يشارك فيها كلا الكيانين معلومات استيقان مشتركة.

13.3.3 معلومات التحقق من الاستيقان (verification AI): معلومات يستعملها متحقق للتحقق من هوية مدّعاة من خلال تبادل معلومات الاستيقان.

14.3.3 المتحقق: كيان أو ممثل كيان يتطلب هوية مستيقن منها. ويحتوي الكيان المحقق على الوظائف اللازمة للقيام بتبادلات الاستيقان.

4.3 تعاريف التوصية [ITU-T Y.2701]

تستخدم التوصية الحالية المصطلحات التالية المعرفة في لتوصية [ITU-T Y.2701]:

1.4.3 عنصر حدود: عنصر شبكة يوفر وظائف توصيل مختلف ميادين الأمن والإدارة.

2.4.3 شبكة مؤسسية: شبكة خاصة تدعم عدة مستعملين وقد تكون في مواقع متعددة (مثال ذلك مباني مؤسسة أو جامعة).

3.4.3 ميدان أمن: مجموعة عناصر وسياسة أمن وسلطة أمن ومجموعة أنشطة ذات صلة بالأمن تدار فيها العناصر طبقاً لسياسة الأمن. وتعمد سلطة الأمن إلى تطبيق سياسة الأمن. وقد يشمل ميدان أمن ما عدة مناطق أمن.

4.4.3 عنصر حدود تجهيزات مطرافية: عنصر حدود يوفر وظائف أمن بين تجهيزات في مكان العميل وشبكة مقدم الخدمة.

5.3 المصطلحات المعرفة في هذه التوصية

تعرف هذه التوصية المصطلح التالي:

1.5.3 اتفاق على مستوى الخدمة (SLA): اتفاق رسمي بين طرفين أو أكثر يبرم بعد عملية تفاوض بهدف تحديد خصائص الخدمة ومسؤوليات كل طرف من الأطراف وأولوياته. وقد يشمل اتفاق على مستوى الخدمة بيانات عن الأمن والأداء وتحديد التعريفات والفوترة وتسليم الخدمة والتعوضيات.

4 مختصرات وتسميات مختصرة

تستخدم التوصية الحالية المختصرات والتسميات المختصرة التالية:

ACL قائمة التحكم في النفاذ (*Access Control List*)

AI معلومات الاستيقان (*Authentication Information*)

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

AS مخدم التطبيقات (*Application Server*)

BE عنصر حدود (*Border Element*)

BSF وظيفة مخدم إنهاض (*Bootstrapping Server Function*)

B-TID معرّف معاملة إنهاض (*Bootstrapping Transaction Identifier*)

CSCF وظيفة تحكم في جلسة نداء (*Call Session Control Function*)

DSL عروة مشترك رقمي (*Digital Subscriber Loop*)

ENI تنفيذ وطني لخدمة اتصالات الطوارئ (*ETS National Implementation*)

ETS خدمة اتصالات الطوارئ (*Emergency Telecommunication Service*)

FE كيانات وظيفية (*Functional Entities*)

GAA معمارية استيقان نوعية (*Generic Authentication Architecture*)

GBA معمارية إنهاض نوعية (*Generic Bootstrap Architecture*)

GUSS إنشاءات أمن مستعمل المعمارية GBA (*GBA User Security Settings*)

HSS نظام مشترك محلي (*Home Subscriber System*)

HTTP بروتوكول نقل النصوص المترابطة (*Hypertext Transfer Protocol*)

HTTPS أمن بروتوكول نقل النصوص المترابطة (*HTTP Security*)

IAD جهاز النفاذ المتكامل (*Integrated Access Device*)

I-CSCF استجواب وظيفة التحكم في جلسة النداء (*Interrogating Call Session Control Function*)

ID-FF إطار تجميع الهويات (*Identity Federation Framework*)

IdM إدارة الهوية (*Identity Management*)

IdP مقدم الهوية (*Identity Provider*)

ID-WSF إطار خدمات الويب للهويات (*Identity Web Services Framework*)

IMS خدمة تعدد وسائط بروتوكول الإنترنت (*IP Multimedia Service*)

IP بروتوكول الإنترنت (*Internet Protocol*)

ISDN شبكة رقمية متكاملة الخدمات (*Integrated Services Digital Network*)

IWF وظيفة التشغيل البيني (*Interworking Function*)

LUAD وكيل مستعمل أو جهاز يقبل بروتوكول Liberty (*Liberty enabled User Agent or Device*)

MAC التحكم في النفاذ إلى الوسائط (*Media Access Control*)

MS مخدم الوسائط (*Media Server*)

NACF وظيفة التحكم في الارتباط بالشبكة (*Network Attachment Control Function*)

NAF وظيفة تطبيق الشبكة (*Network Application Function*)

NAP نقطة النفاذ إلى الشبكة (*Network Access Point*)

NGN شبكة الجيل التالي (*Next Generation Network*)

NNI سطح التماس بين شبكتين (*Network-to-Network Interface*)

OAM&P العمليات والإدارة والصيانة والتموين (*Operations, Administration, Maintenance and Provisioning*)

OSI التوصيل بين الأنظمة المفتوحة (*Open System Interconnection*)

P-CSCF وظيفة التحكم في جلسة نداء بالوكالة (*Proxy Call Session Control Function*)

PES خدمة تطور ISDN/PSTN (*PSTN/ISDN Evolution Service*)

PIN رقم تعرف هوية شخصي (*Personal Identification Number*)

PKI بنية تحتية لمفاتيح عمومية (*Public Key Infrastructure*)

PPII معلومات شخصية معرّفة PII (*Personally Identifiable Information*)

PSK مفاتيح متقاسمة سلفاً (*Pre-shared Keys*)

RACF وظيفة التحكم في الموارد والقبول (*Resource and Admission Control Function*)

RBAC التحكم في النفاذ على أساس الدور (*Role Based Access Control*)

RP طرف معتمد (*Relying Party*)

RPH رأسية أولوية المورد (*Resource-Priority Header*)

RSVP بروتوكول حجز الموارد (*Resource Reservation Protocol*)

SAML لغة ترميز تأكيد الأمن (*Security Assertion Markup Language*)

SASL طبقة بسيطة للاستيقان والأمن (*Simple Authentication and Security Layer*)

SBC مراقب حدود الجلسة (*Session Border Controller*)

S-CSCF وظيفة خدمة التحكم في جلسة النداء (*Serving Call Session Control Function*)

SDP بروتوكول وصف الجلسة (*Session Description Protocol*)

SIM وحدة تعرف هوية المشترك (*Subscriber Identification Module*)

SLA اتفاق على مستوى الخدمة (*Service Level Agreement*)

SLF وظيفة تحديد موقع المشترك (*Subscriber Locator Function*)

SOAP بروتوكول بسيط للنفاذ إلى الأشياء (*Simple Object Access Protocol*)

SP مقدم خدمة (*Service Provider*)

SSOS خدمة استيقان وحيد (*Single-Sign-On Service*)

TDR اتصالات الإغاثة في حالات الكوارث (*Telecommunication for Disaster Relief*)

TE تجهيزات مطرافية (*Terminal Equipment*)

TE-BE عنصر حدود تجهيزات مطرافية (*Terminal Equipment – Border Element*)

TLS أمن طبقة النقل (*Transport Layer Security*)

UAI سطح التماس بين التطبيق والمستعمل (*User Application Interface*)

UE تجهيزات المستعمل (*User Equipment*)

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

URL محدد موقع موارد موحد (*Uniform Resource Locator*)

WS مخدم ويب (*Web Server*)

XML لغة ترميز موسعة (*eXtensible Markup Language*)

5 نماذج مرجعية

1.5 إطار الاستيقان في التوصية ITU-T X.811

تستخدم التوصية الحالية المفاهيم الأساسية للاستيقان الموصوفة في التوصية [ITU-T X.811] كما هو موجز أدناه.

1.1.5 المفاهيم الأساسية للاستيقان

يوفر الاستيقان ضمان صحة الهوية المدّعاة لكيان ما. وليس للاستيقان من مغزى إلا في سياق علاقة بين كيان أساس ومحقق. وثمة حالتان هامتان هما:

- الكيان الأساس يمثله مدّعٍ لديه علاقة اتصالات معينة مع المحقق (استيقان الكيان)؛
- الكيان الأساس مصدر بند بيانات متاح للمحقق (استيقان مصدر البيانات).

يوفر استيقان الكيان التصديق على هوية الكيان الأساس، وذلك في سياق علاقة اتصال. ولا يمكن تأكيد صحة الهوية المستيقن منها للكيان الأساس إلا عندما تكون خدمة الاستيقان ناشطة.

الملاحظة 1 – عند استيقان مصدر البيانات من الضروري أيضاً توفر الضمان الكافي بأن البيانات لم تخضع لأي تعديل. ويمكن تحقيق ذلك باستعمال خدمة سلامة البيانات، وذلك مثلاً:

- باستعمال بيئات لا يمكن فيها تعديل البيانات؛
- بالتحقق من أن البيانات المستلمة تقابل بصمات رقمية للبيانات المرسلة؛
- باستعمال آلية للتوقيع الرقمي؛
- باستعمال خوارزمية تشفيرية تناظرية.

الملاحظة 2 – يمكن تفسير عبارة "علاقة اتصالات" المستعملة في تعريف استيقان الكيان تفسيراً واسعاً ويمكنها أن تشير مثلاً إلى توصيل بين أنظمة مفتوحة (OSI) أو اتصال بين العمليات أو تفاعل بين مستعمل ومطراف.

2.1.5 معرِّفات

الكيان الأساس هو كيان يمكن استيقان هويته. ولكل كيان أساس واحد أو أكثر من المعرِّفات المميِّزة المرتبطة به. فخدمات الاستيقان تُستخدم من جانب كيان ما للتحقق من الهويات المدّعاة لكيانات أساس. وتُدعى هوية الكيان الأساس التي يكون قد تم التحقق منها على هذا النحو هوية مستيقن منها. وعلى غرار ذلك يدعى الكيان الأساس الذي يكون قد تم التحقق من هويته كيان مستيقن منه.

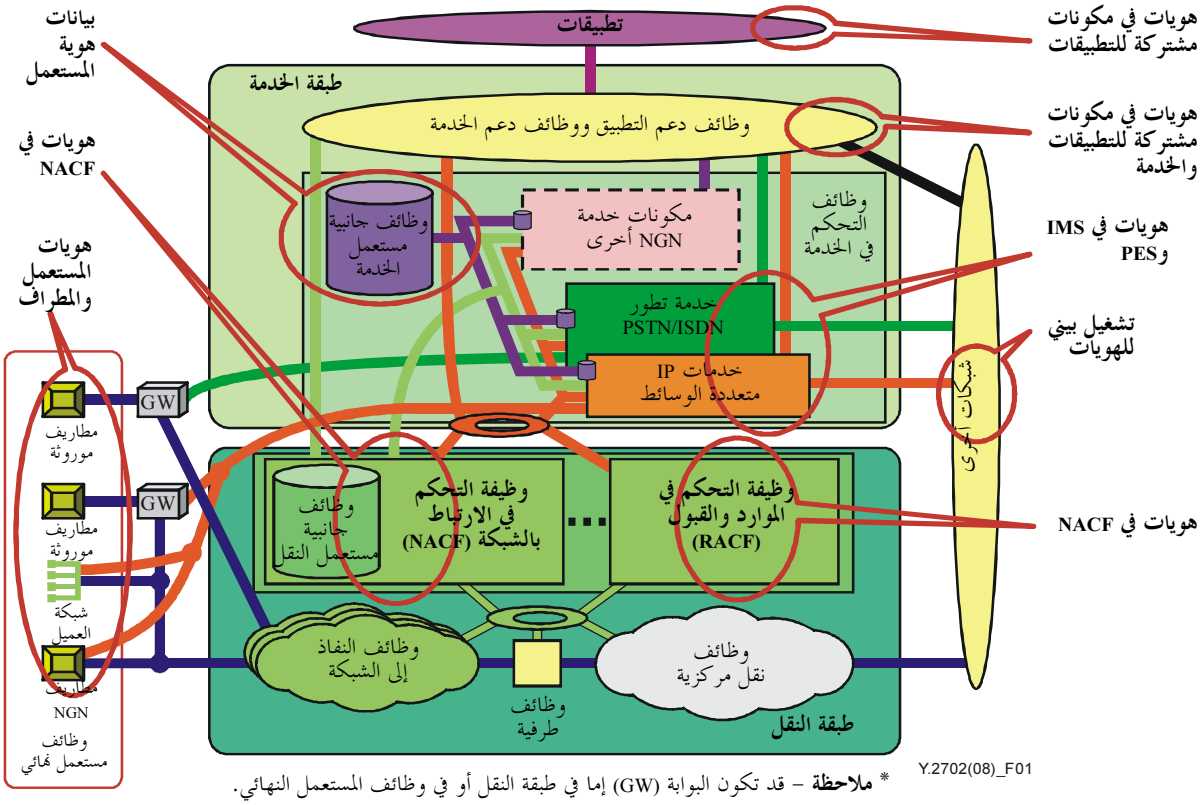
ومن أمثلة الكيانات الأساس التي يمكن تعرف هويتها وبالتالي الاستيقان منها، دون حصر، ما يلي:

- مستعملون؛
- مقدمو شبكات الجيل التالي؛
- عمليات؛
- أنظمة مفتوحة حقيقية؛
- كيانات طبقة التوصيل بين الأنظمة المفتوحة (OSI)؛
- المؤسسات؛
- التدفقات في حركة الحامل والتشوير والإدارة.

تُستخدم معرِّفات التمييز لتأكيد صحة هوية ما ضمن ميدان أمن معين. وتميِّز معرفات التمييز الكيان الأساس من غيره في نفس الميدان، وذلك بأحد أسلوبين:

1) بفضل عضوية في مجموعة من الكيانات تعتبر مكافئة لأغراض الاستيقان (في هذه الحالة تعتبر المجموعة بكاملها كيان أساس واحد ولها معرِّف تمييز واحد)؛
2) بتعرُّف هوية كيان واحد فقط لا غير.

عندما يتم الاستيقان بين ميداني أمن مختلفين قد لا يكون استعمال معرِّف تمييز واحد كافياً لتعرُّف كيان ما دون لبس وذلك لأن سلطات ميدان أمن مختلفة قد تستعمل نفس معرِّفات التمييز. ويتعيَّن في هذه الحالة استعمال معرِّفات التمييز بالترادف مع معرِّف ميدان أمن لكي توفر معرِّف كيان لا لبس فيه.



* **ملاحظة** – قد تكون البوابة (GW) إما في طبقة النقل أو في وظائف المستعمل النهائي.

الشكل 1 – مثال لمعرِّفات شبكات الجيل التالي

ومن الممكن للمكونات والعناصر الوظيفية في مختلف طبقات شبكات الجيل التالي أن تستعمل معرِّفات مستخدمة لتعرّف كيان أساس أو كيان آخر. ويبيِّن الشكل 1 مثال معرِّفات لشبكات الجيل التالي اعتماداً على الشكل 8 (مكونات شبكات الجيل التالي) في [ITU-T Y.2012].

ومن أمثلة معرِّفات التمييز الشائعة ما يلي:

- أسماء الأدلة؛
- عناوين الشبكات؛
- تسميات عملية التطبيق (AP) وكيان التطبيق (AE)؛
- معرِّفات الأشياء؛
- أسماء الأشخاص (دون لبس في سياق الميدان)؛
- خماسيات تحتوي على ما يلي:
  - عنوان مصدر بروتوكول الإنترنت،
  - عنوان مقصد بروتوكول الإنترنت،
  - رقم منفذ المصدر،
  - رقم منفذ المقصد،
  - رقم البروتوكول.

3.1.5 كيانات الاستيقان

يُستخدم مصطلح "مدّعٍ" لوصف الكيان الأساس أو الذي يمثله لأغراض الاستيقان. ويحتوي المدعي على الوظائف اللازمة للدخول في عملية تبادل الاستيقان نيابة عن الكيان الأساس.

ويُستخدم مصطلح "محقق" لوصف الكيان الأساس أو الذي يمثله والذي يتطلب هوية مستيقن منها. ويحتوي المحقق على الوظائف اللازمة للدخول في عملية تبادل الاستيقان لطلب التحقق من هوية مزعوم مدّعاة.

ويضطلع الكيان المشارك في عملية استيقان متبادل بدور كل من المدعي والمحقق على السواء.

يُستخدم تعبير "الطرف الثالث الموثوق به" لوصف سلطة أمن، أو وكيلها، تثق بها كيانات أخرى فيما يتعلق بالأنشطة المتصلة بالأمن. وفي سياق هذه التوصية يكون الطرف الثالث موثوق به من جانب المدعي و/أو المحقق لأغراض الاستيقان.

ملاحظة – يمكن لمدع أو لمحقق أن يشمل مكونات وظيفية متعددة، ربما موجودة في أنظمة مفتوحة مختلفة.

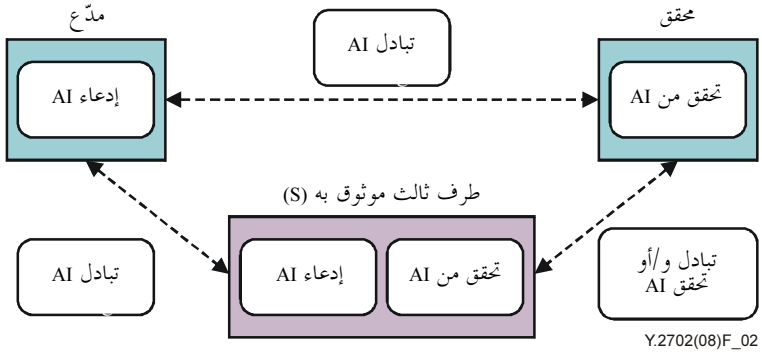
4.1.5 معلومات الاستيقان

فيما يلي أنماط معلومات الاستيقان الموصوفة في هذا المعيار:

- تبادل معلومات الاستيقان (تبادل AI)؛
- إدعاء معلومات الاستيقان (إدعاء AI)؛
- التحقق من معلومات الاستيقان (تحقق AI).

يُستخدم تعبير "تبادل الاستيقان" لوصف تتابع من عملية نقل أو أكثر لتبادل معلومات الاستيقان AI لأغراض أداء عملية الاستيقان.

يوضح الشكل 2 العلاقة بين مدع ومحقق وطرف ثالث موثوق به. كما يوضح أنماط معلومات الاستيقان الثلاثة التي يمكن أن يتألف منها تبادل الاستيقان.



الشكل 2 – العلاقة بين المدعي والمحقق والطرف الثالث الموثوق به

قد يحتاج المدعي، في بعض الحالات، لتوليد تبادل معلومات الاستيقان، إلى التفاعل مع طرف ثالث موثوق به. وكذلك قد يحتاج المحقق، للتحقق من تبادل معلومات الاستيقان، إلى التفاعل مع طرف ثالث موثوق به. وفي هذه الحالات، قد يحتوي الطرف الثالث الموثوق به على معلومات استيقان للتحقق متصلة بكيان أساس.

ومن الممكن أيضاً اللجوء إلى طرف ثالث موثوق به في نقل تبادل معلومات الاستيقان. وتبعاً لطبيعة التبادل، قد يضطلع الطرف الثالث بدور المدعي إزاء المحقق.

كما قد تحتاج الكيانات أيضاً إلى أن تحتوي على معلومات استيقان تُستخدم لدى الاستيقان من الطرف الثالث الموثوق به.

5.1.5 الاستيقان متعدد العوامل

يتناول الاستيقان متعدد العوامل إثبات صحة هوية كيان أساس بالتحقق من عدة معرِّفات ونعوت مرتبطة بهذا الكيان الأساس. ويمكن عموماً تنظيم الاستيقان متعدد العوامل على أساس التجميعات التالية من نعوت الاستيقان:

1) ما تختص به (مثال ذلك خصائص مادية أو سلوكية لمستعمل نهائي أو ميزة أو نعت يختص بها عميل يجري مقارنتها كمنوال الطباعة أو تعرُّف الصوت)؛

2) ما تملكه (مثال ذلك رخصة قيادة أو علامة أمن)؛

3) ما تعرفه (مثال ذلك كلمة سر أو رقم تعرُّف هوية شخصي أو صورة أمن).

وأكثر الأمثلة شيوعاً لمفتاح استيقان مفرد العامل هو كلمة السر (ما تعرفه). وقد لا توفر كلمات السر، في حد ذاتها، وفي بعض الأحيان الدرجة الكافية من الثقة في هوية الكيان، ومن ثم يحتاج الأمر إلى أشكال أقوى من الاستيقان، تتناول مفاتيح استيقان أخرى، لتمكين النفاذ إلى بعض الموارد والتطبيقات والخدمات في شبكات الجيل التالي. ويتوقف ذلك على المخاطر المرتبطة باحتمال نفاذ كيانات غير مرخص لها إلى الموارد والتطبيقات والخدمات في شبكات الجيل التالي.

وينبغي انتقاء عوامل ومفاتيح الاستيقان على أساس المخاطر التي ينبغي التصدي لها. وعلى وجه التحديد لا بد من تقييم آثار نفاذ الكيانات غير المرخَّص لها إلى الموارد والتطبيقات والخدمات في شبكات الجيل التالي لتحديد مدى الاستيقان المطلوب. ومن أمثلة مفاتيح الاستيقان الإلكترونية ما يلي:

- كلمات السر،
- علامات في معدّات الحاسوب،
- علامات في برمجيات الحاسوب،
- علامات إنتاج كلمة سر وحيدة الاستعمال.

إن استعمال كلمات السر من أجل الاستيقان ممارسة واسعة النطاق. وكلمة "السر" كلمة يحفظها في ذاكرته المدعي ويستعملها لاستيقان هويته. وتتألف كلمات السر عموماً من سلسلة سمات أو صور يحفظها المشترك في ذاكرته ويجب عليه أن يميِّزها عندما تُعرض عليه إلى جانب صور مشابهة أخرى. ولكن أنظمة كلمة السر عرضة للعديد من الهجمات. ومن الممكن تعزيز حماية قناة الاتصال بغية حماية كلمة السر، ولكن ذلك لا يمنع حقاً جميع الهجمات.

وعلامات معدات الحاسوب عبارة عن أجهزة متخصصة لحماية الأسرار (مفاتيح تشفير عادة) وهي تقوم بأداء عمليات تشفيرية. وتتحقق عملية الاستيقان بالبرهان على ملكية الجهاز والتحكم في المفتاح. وتمكن العمليات التشفيرية استيقان الطرفين وتُستخدم حماية قناة الاتصال لعملية تبادل الاستيقان.

أما علامات برمجيات الحاسوب فهي أساساً تطبيقات برمجية لعلامات معدات الحاسوب وتتقاسم العديد من مزايا علامات المعدات (مثال ذلك مفتاح تشفير يُختزَن عموماً في قرص أو في شكل آخر من أشكال الوسائط). ويمكن تشفير مفتاح علامة البرمجية في إطار مفتاح مشتق من بعض بيانات التفعيل. وبيانات التفعيل عموماً عبارة عن كلمة السر معلومة فقط لدى المستعمل ويحتاج الأمر بالتالي إلى كلمة سر لتفعيل العلامة. وتتحقق عملية الاستيقان بالبرهان على ملكية المفتاح والتحكم فيه. وكما هو حال علامات معدات الحاسوب فإن علامات البرمجية تمكّن من استيقان الطرفين على السواء وتوفر الحماية لقناة الاتصال المستعملة في تبادل الاستيقان.

أما علامة إنتاج كلمة سر وحيدة الاستعمال فهي جهاز حاسوبي شخصي يولّد كلمات سر "وحيدة الاستعمال" لاستعمالها في الاستيقان. وتعتمد أنظمة كلمات السر وحيدة الاستعمال على سلسلة من كلمات السر تتولّد باستعمال خوارزميات خاصة. وتُدعى كل كلمة سر في السلسلة كلمة سر وحيدة الاستعمال لأنها متميِّزة عن غيرها ولا يمكن استعمالها إلا مرة واحدة. وهنالك طائفة متنوعة واسعة من أنظمة كلمات السر وحيدة الاستعمال توفر درجات متفاوتة من الحماية من الهجمات.

2.5 تهديدات الاستيقان

يمكن مهاجمة عوامل ومفاتيح الاستيقان كما يلي:

1) "ما تختص به" – محاكاة ميزة أو نعت يتسم به العميل وتجري مقارنته (مثال ذلك بصمات الأصابع ومنوال الطباعة وغيرها).

2) "ما تملكه" – الحصول على ما لدى العميل أو على نسخة منه.

3) "ما تعرفه" – اكتشاف ما يعرف العميل.

ويمكن عموماً تقسيم تهديدات الاستيقان إلى تهديدات تنطوي على هجمات ضد بروتوكول الاستيقان وهجمات أخرى قد تكشف إما عن قيم علامة ما أو تعرِّض للكشف معلومات سرية.

ومن شأن استعمال عوامل استيقان متعددة تحسين درجة الأمن لأن الأمر يتطلب تخطي عوائق متعددة. ومن شأن استعمال جهاز في المعدات "ما تملكه" لا يمكن استنساخه بسهولة أن يحد من نطاق الهجوم، إذ من المتوقع أن يلاحظ المالك فقدان ذلك الجهاز. ويمكن ضم مفاتيح استيقان قائمة على أساس علامات برمجيات أو معدات إلى بيانات تفعيل (كلمة سر مثلاً) تنفيذ استيقان ذي عاملين بحيث لا يعتمد الاستيقان على مجرد امتلاك علامة ما.

وقد ينال عميل ما من نظام الاستيقان بأن يكشف عمداً عن مفتاح استيقان وحيد العامل لديه إلى جهة متواطئة وينكر ذلك فيما بعد بهدف إحباط عمليات الاستيقان اللاحقة. ومن شأن استعمال عوامل استيقان متعددة أن يجعل مثل هذا الإنكار أقل مصداقية وأن يدرأ مثل هذه الهجمات.

1.2.5 تهديدات بروتوكول الاستيقان

من أمثلة تهديدات بروتوكول الاستيقان ما يلي:

1) التنصت:
   - يلاحظ المتنصت تبادل رسائل بروتوكول الاستيقان لتحليلها لاحقاً؛
   - يحاول المتنصت عموماً الحصول على علامات للتنكر بصفة مدع.

2) الانتحال:
   - ينتحل المدعي صفة مشترك إزاء المحقق لاختبار علامات مخمنة أو للحصول على معلومات أخرى عن مشترك معين؛
   - ينتحل المدعي صفة المحقق إزاء مشترك مشروع للحصول على علامات يمكن استعمالها بعد ذلك لانتحال شخصية المشترك إزاء محقق مشروع؛
   - ينتحل المدعي صفة الطرف المعتمد إزاء المحقق للحصول على معلومات حساسة عن المستعمل.

3) الاختطاف:
   - كيان يختطف جلسة مستيقن منها ويتنكر في هيئة مشترك إزاء طرف معتمد للحصول على معلومات حساسة أو لإدخال معلومات غير صحيحة؛
   - كيان يختطف جلسة مستيقن منها ويتنكر في هيئة طرف معتمد إزاء المحقق للحصول على معلومات حساسة أو إخراج معلومات غير صحيحة.

ويمكن الحد من هذه الهجمات بالأساليب التالية:

- اشتراط عنصر جديد لكل استيقان لردع هجمات التكرار.
- يمكن درء هجمات التنصت واختطاف الجلسة باستعمال التشفير لحماية قناة التشوير (تشفير القناة) المستعملة لتبادل الاستيقان (أمن طبقة النقل (TLS) في أسلوب مُغْفل مثلاً).

- يمكن مقاومة هجمات الاعتراض وانتحال هوية المحقق، بشكل محدود، باستخدام أساليب حماية مماثلة لأساليب درء هجمات التنصت واختطاف الجلسة. ومن شأن الجمع بين التجفير وأساليب التشفير الإضافية تحسين الحماية من هذه الهجمات (مثال ذلك، استعمال "المصافحة" القائمة على أساس التشفير – مثل TLS في أسلوب مستيقن منه – على أن تكون مفاتيح التشفير في حوزة العميل والمحقق مما يؤدي إلى استيقان متبادل "قوي").
- لا يوفر التجفير إلا مقاومة محدودة لهجمات الاعتراض وانتحال هوية المحقق، إذ من الممكن تعريض أمن التبادل للخطر دون فك التجفير. فمن الممكن مثلاً أن ينخدع العميل بحيث يقبل تبادل الاستيقان على أنه من المحقق عندما لا يكون كذلك. ويمكن استعمال أساليب الاستيقان المتبادل القائمة على أساس التجفير بين العميل والمحقق.

2.2.5 تهديدات علامة الاستيقان

إذا تمكّن مهاجم من التحكم بعلامة ما فإنه يمكن أن يتنكر بوصفه مالك تلك العلامة. ويمكن تصنيف تهديدات العلامات على أنها هجمات على مفاتيح الاستيقان كما يلي:

- يمكن للمهاجم أن يسرق أو يستنسخ "ما يملكه العميل". فقد يعمد المهاجم الذي يتمكّن من النفاذ إلى حاسوب العميل أن يستنسخ علامة برمجية. كما يمكن سرقة علامة معدات أو استنساخها.
- قد يكتشف المهاجم "ما يعرفه العميل". فقد يتمكّن من تخمين كلمة سر أو رقم تعرُّف هوية شخصي (PIN). وعندما تكون العلامة سراً متقاسماً قد يتمكّن المهاجم من النفاذ إلى المحقق والحصول على كلمة السر. فقد يعمد المهاجم إلى تركيب برمجية مؤذية (مسجل لمسات مفاتيح مثلاً) لالتقاط هذه المعلومات. وعلاوة على ذلك، قد يتمكّن المهاجم من معرفة السر من خلال هجمات "خارج الخط" على حركة الشبكة انطلاقاً من محاولة استيقان.
- قد يتمكن المهاجم من استنساخ "ما يختص به العميل". فقد يحصل على نسخة من هوية مالك العلامة ويقوم بصنع نسخة منها.

وهنالك عدة استراتيجيات للحد من هذه التهديدات:

- من شأن تعدد العوامل أن يرفع عتبة التحصين أمام الهجمات. فإذا كان على المهاجم أن يختلس علامة تشفير وأن يخمن كلمة سر فإن عامل الصعوبة مرتفع جداً.
- يمكن استخدام آليات أمن مادية لحماية علامة مسروقة من الاستنساخ. وبإمكان هذه الآليات أن توفر البرهان على التلاعب والكشف عنه والتصدي إليه.
- كلما ازداد تعقيد كلمات السر انخفض احتمال نجاح هجمات التخمين. ومن شأن اشتراط استعمال كلمات سر طويلة لا تظهر في القواميس الشائعة أن يضطر المهاجم إلى تجريب كل كلمات السر الممكنة.
- يمكن استخدام أساليب التحكم في أمن الأنظمة والشبكات لمنع المهاجم من النفاذ إلى نظام ما أو من تركيب برمجية مؤذية فيه.

3.2.5 تهديدات استيقان أخرى

لا تقتصر الهجمات على بروتوكول الاستيقان بالذات. ومن الهجمات الأخرى ما يلي:

- هجمات شفرة مؤذية قد تنال من علامات الاستيقان؛
- هجمات الاقتحام للحصول على شهادات أو علامات بالتغلغل إلى نظام المشترك/المدعي أو سلطة الإشهاد أو نظام التحقق؛
- تهديدات من داخل المؤسسة يمكن أن تنال من علامات الاستيقان؛
- الهجمات خارج الحاسوب التي تحصل على العلامات بأساليب أخرى مثل "الهندسة الاجتماعية" – لاستدراج مشترك للكشف عن كلمة السر للمهاجم – أو اختلاس النظر إلى كلمة السر من فوق كتف المشترك؛

- هجمات تغرر بالمدعين وتحدو بهم إلى استعمال بروتوكول غير آمن، بينما يخيل لهم أنهم يستعملون بروتوكولاً آمناً، أو تستدرجهم إلى تجاوز ضوابط الأمن (مثال ذلك قبول شهادات مخدِّم لا يمكن التحقق من صحتها)؛
- الاستهتار من جانب المشتركين الذين يعرِّضون علاماتهم للخطر عمداً.

وتعتبر أساليب التوعية وإرشاد العملاء من طرائق مكافحة هجمات الشفرة المؤذية والهندسة الاجتماعية. وكثيراً ما تُستعمل أساليب التدقيق والكشف عن أحوال الشذوذ في التصدي لهجمات الخداع والاحتيال الموجهة ضد العميل. ومن شأن استعمال مفاتيح الاستيقان المتعددة أن تحدّ من هذه الهجمات ضد العميل. ويمكن التصدي لهجمات الأفراد داخل المؤسسة من خلال حُسن فرز الموظفين وعمليات التدقيق واللجوء (حيثما كان ملائماً) إلى الفصل من الخدمة واستعمال التحكم المزدوج.

3.5 كفالة الاستيقان

حرصاً على حماية موارد وتطبيقات وخدمات شبكات الجيل التالي، يتعيَّن على مقدِّمي خدمات هذه الشبكات تقرير المستوى المطلوب من الكفالة في مجال الاستيقان من أجل النفاذ إلى الشبكة ومن أجل معاملات التطبيق/الخدمة.

ينبغي لكل من مقدِّمي خدمات شبكات الجيل التالي وضع وتنفيذ عملية لكفالة الاستيقان. وتنطوي عملية كفالة الاستيقان على طريقة لتصنيف الثقة (أي الثقة في معلومات الهوية المقدمة إلكترونياً إلى مقدِّم الخدمة) في آليات الاستيقان والمعلومات المقدمة من أجل الاستيقان.

تعمد عملية كفالة الاستيقان إلى وضع واستعمال سويات نسبية ومنفصلة من الكفالة لتكمية الثقة بعملية الاستيقان. مثال ذلك، يمكن استعمال "n" سوية من سويات كفالة الاستيقان. ويمكن أن تمثل السوية "0" أخفض سوية للكفالة بينما تمثل السوية "n" أعلى سوية. وتُستعمل سويات "n" لتحديد سوية الكفالة من حيث العاقبة المحتملة (أي طبيعة الآثار المحتملة) التي تترتب على خطأ استيقان انطلاقاً من الافتراض بأن جميع المعرِّفات المستعملة في الاستيقان ليست متساوية أو ليس لها بالضرورة نفس قيمة الاستيقان.

وفيما يلي مثال لطريقة كفالة الاستيقان:

مثال لطريقة استيقان

سوية الكفالة	الثقة النسبية
السوية 0	انعدام الثقة في صحة الهوية المدعاة (مثال ذلك استعمال أساليب التحكم بواسطة قائمة النفاذ)
السوية 1	بعض الثقة في صحة الهوية المدعاة
السوية 2	ثقة عالية في صحة الهوية المدعاة
--	--
السوية n	أعلى درجة من الثقة في صحة الهوية المدعاة

يتعيَّن على مقدم خدمات شبكات الجيل التالي أن يتمكّن من النفاذ إلى المخاطر المحتملة المرتبطة بعواقب أخطاء الاستيقان أو أن يحدد السوية الملائمة من الكفالة في صحة هوية كيان ما (المستعمل النهائي مثلاً). وكلما كانت العواقب المحتملة لأخطاء الاستيقان جسيمة يتطلب الأمر سويات أعلى من الكفالة.

ويرتبط الخطر الناجم عن خطأ استيقان بعاملين:

أ) الضرر أو الأثر المحتمل؛

ب) احتمال حدوث هذا الضرر أو الأثر.

يشمل الضرر والأثر الفئات التالية دون أن يقتصر عليها:

- الإزعاج أو الامتعاض أو النيل من المكانة أو السمعة
- خسارة مالية
- مسؤولية مقدم خدمات شبكات الجيل التالي أو العميل
- ضرر ينال البنية التحتية أو الموارد أو التطبيقات أو الخدمات أو المصالح العامة لدى مقدم خدمات شبكات الجيل التالي
- ضرر ينال المصلحة العامة أو مصالح الحكومة (اتصالات حساسة مثل خدمات اتصالات الطوارئ (ETS) أو اتصالات الإغاثة في حالات الكوارث (TDR))
- الكشف غير المرخص به عن معلومات حساسة
- ضرر ينال خدمات الأمن الشخصي
- مخالفات مدنية أو جنائية

4.5 إدارة الترخيص والامتيازات

لا يكفي الاستيقان في حد ذاته لتحديد ما يرخص للكيان المستيقن منه القيام به بعد منحه النفاذ. ويجب أن يقترن الاستيقان بآليات لإدارة الترخيص والامتيازات وبمناهج لتوفير التحكم في النفاذ إلى خدمات وموارد NGN. من ذلك مثلاً، تخصيص الأدوار والامتيازات إلى المستعملين النهائيين/المشتركين للتحكم في النفاذ إلى الخدمات والتطبيقات وإلى السطوح البينية للإدارة بغية إدارة ما لديها من اشتراكات وجانبيات. ومن الأمثلة الأخرى التحكم في النفاذ على أساس الدور (RBAC) من أجل التحكم في النفاذ إلى العمليات والإدارة والصيانة والتموين (OAM&P).

ويمكن اعتبار الترخيص والامتياز بمثابة نعت من نعوت هوية الكيان. وتبعاً لسياسة الأمن يمكن إثبات صحة الترخيص والامتيازات لكيان ما بوساطة الاستيقان.

5.5 نموذج معماري مرجعي من طرف إلى طرف

تصف هذه الفقرة النموذج المرجعي من طرف إلى طرف المستعمل لتنظيم وتجميع متطلبات الاستيقان في هذه التوصية. ويصف النموذج المرجعي ما يلي:

1) استيقان وترخيص المستعمل للنفاذ إلى الشبكة (مثال ذلك استيقان وترخيص جهاز مستعمل نهائي أو بوابة شبكة محلية أو بوابة مؤسسة من أجل النفاذ إلى الشبكة أو الارتباط بها).
2) قيام مقدم الخدمة باستيقان وترخيص المستعمل من أجل النفاذ إلى الخدمة/التطبيق (مثال ذلك استيقان وترخيص مستعمل أو جهاز أو مجموعة مستعمل/جهاز حيث ينطبق الاستيقان والترخيص على النفاذ إلى الخدمة/التطبيق في شبكة الجيل التالي).
3) قيام مقدم الخدمة باستيقان وترخيص المستعمل للنفاذ إلى خدمة/تطبيق معين (مثال ذلك الاستيقان والترخيص المحددين لخدمة اتصالات الطوارئ (ETS) واتصالات الإغاثة في حالات الكوارث (TDR)[1]).
4) قيام المستعمل باستيقان وترخيص الشبكة (مثال ذلك استيقان المستعمل من هوية شبكة مرتبطة بشبكات الجيل التالي أو من مقدم خدمة).
5) استيقان وترخيص بين المستعملين (مثال ذلك استيقان وترخيص المستعمل المطلوب (أو كيان الانتهاء) أو استيقان وترخيص كيان المصدر أو استيقان مصدر البيانات كوظيفة من وظائف الشبكة).
6) استيقان وترخيص الشبكة المتبادل (مثال ذلك الاستيقان والترخيص عبر سطح التماس بين شبكتين (NNI) في مستوى النقل أو مستوى الخدمة/التطبيق).

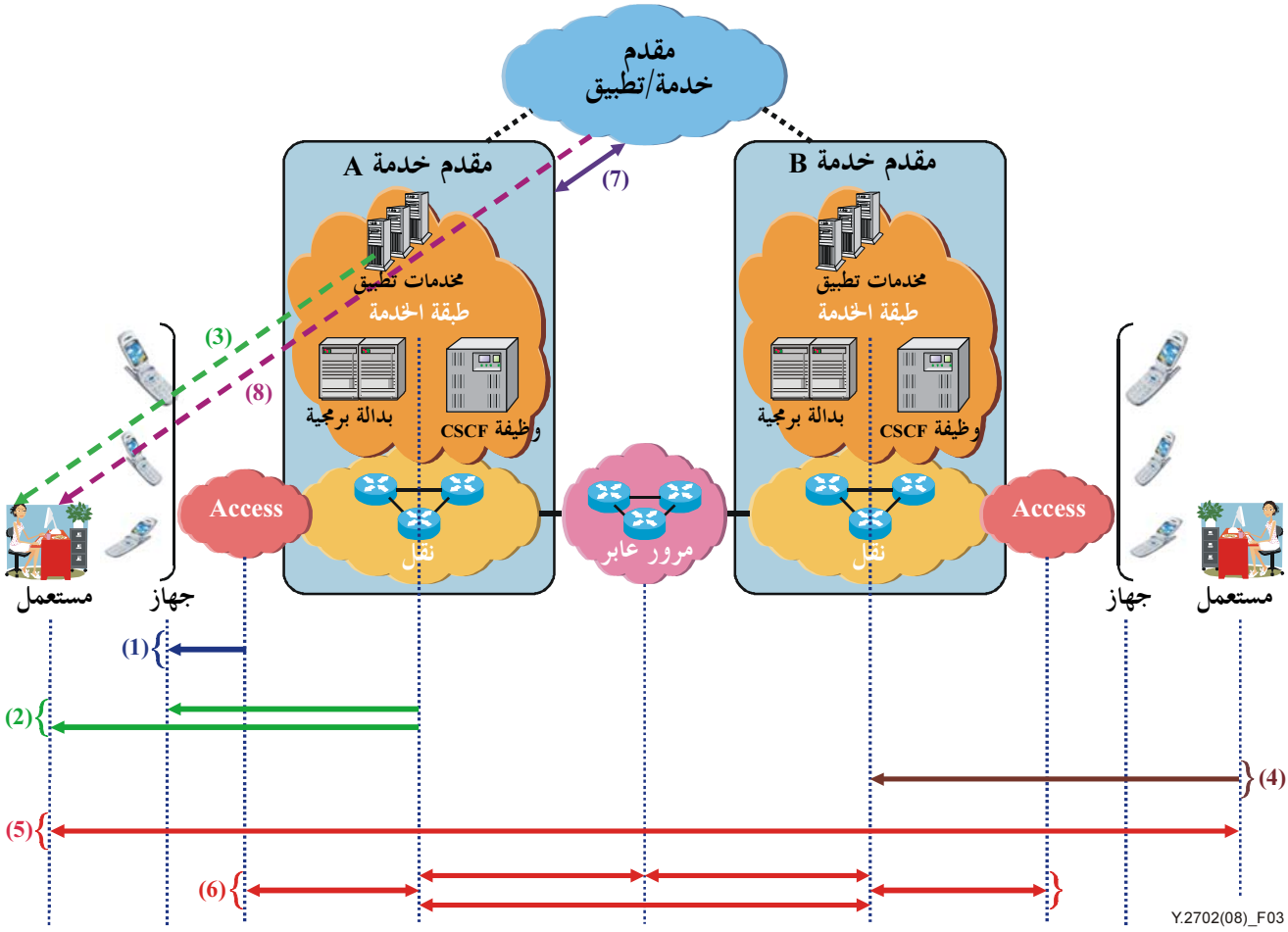
[1] قد يفترض استيقان خدمة اتصالات الطوارئ (ETS) متطلبات إضافية تتجاوز المتطلبات الأساسية.

7) استيقان وترخيص مقدم الخدمة/التطبيق.

8) استعمال خدمة استيقان الطرف الثالث.

يبيِّن الشكل 3 النقاط المرجعية للاستيقان الموجزة أعلاه.

لا يقتصر استعمال المصطلح "مستعمل" في هذه التوصية على شخص، بل قد يكون شخصاً أو مجموعات أو شركات أو كيانات قانونية.



الشكل 3 – نموذج معماري مرجعي من طرف إلى طرف

كما هو مبيَّن في الشكل 3، يحدث كل من الاستيقان والترخيص عند مستوى النقل ومستوى تطبيق الخدمة على السواء. وعلاوة على ذلك، هنالك إمكانية تجميع أو ترزيم الاستيقان. مثال ذلك عندما يقوم مقدم الخدمة بربط/بترزيم استيقان المستعمل وجهاز المستعمل من أجل توفير سوية أعلى من كفالة الاستيقان. ويتحسَّن ذلك إلى درجة أبعد عندما يكون مقدم النفاذ إلى الشبكة ومقدم الخدمة نفس الكيان. وفي غالب الأحوال يتحقق الاستيقان الأفقي على أساس قفزة قفزة. والاستثناء الرئيسي في هذا الشأن هو الاستيقان بين المستعملين الذي يكون من طرف إلى طرف. وباستثناء قيام المستعمل باستيقان وترخيص الشبكة، فإن العلاقات تتطلب الاستيقان المتبادل.

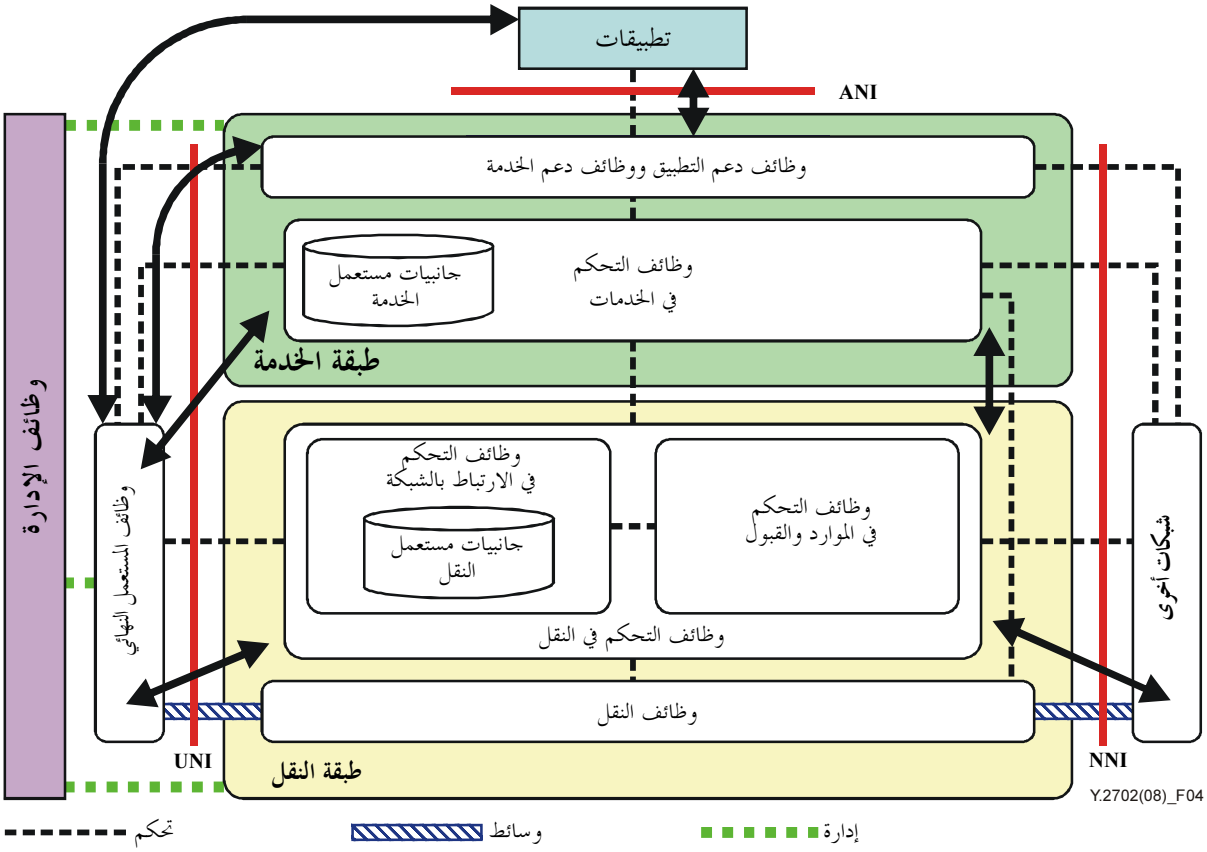
6.5 العلاقة بمعمارية شبكات الجيل التالي المحددة في [ITU-T Y.2012]

تصف هذه الفقرة العلاقة بين النموذج المرجعي الموصوف في التوصية الحالية والنموذج المعماري الوظيفي الموصوف في التوصية [ITU-T Y.2012]. وهي تسلّط الضوء تحديداً على ما يلي:

- علاقة الاستيقان بين الأقران في الشكل 1 من [ITU-T Y.2012] "لمحة عامة عن معمارية شبكات الجيل التالي".
- العناصر الوظيفية في الشكل 1 من [ITU-T Y.2012] الرامية إلى أداء وظائف الاستيقان.

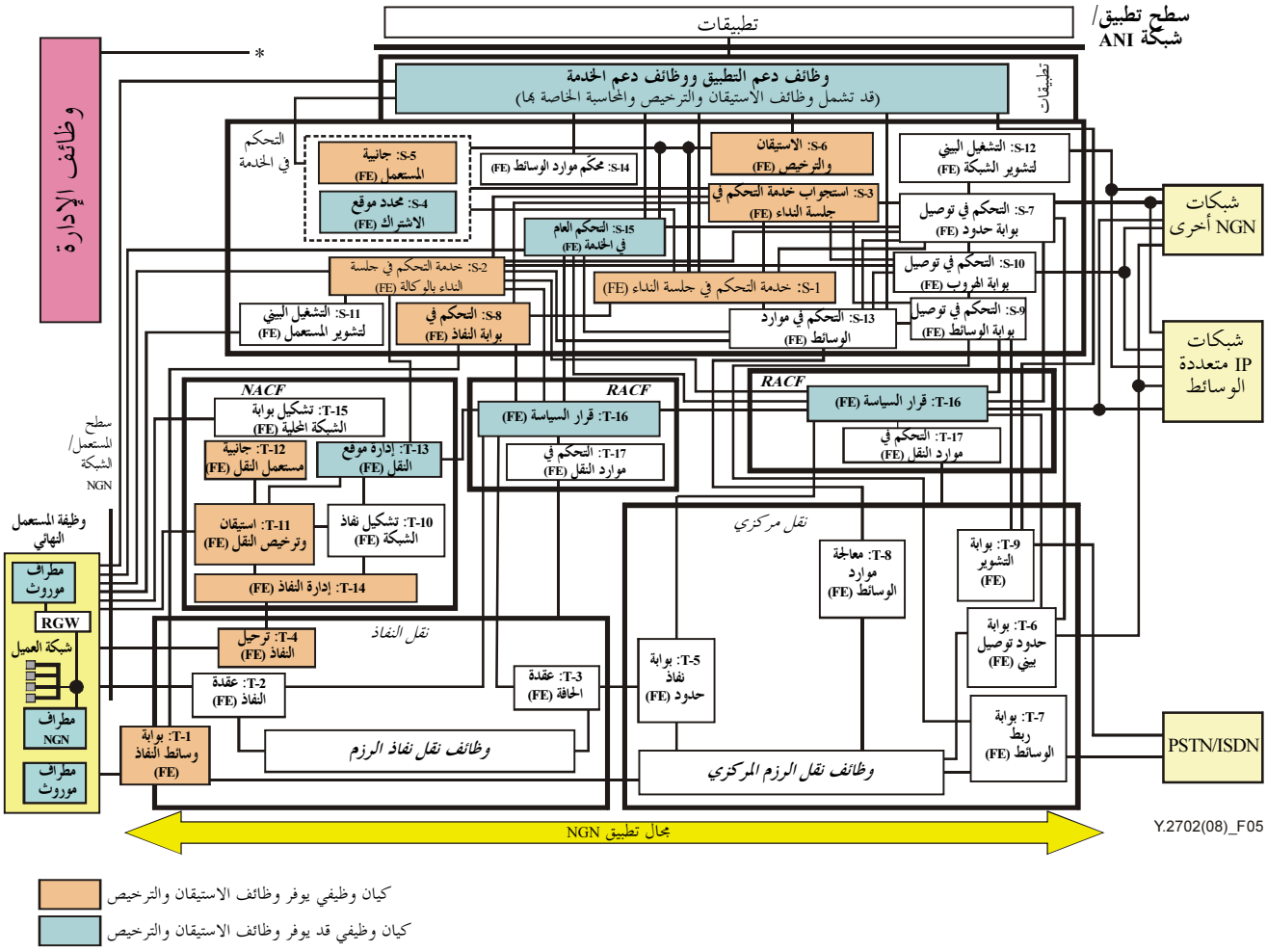
- العناصر الوظيفية في الشكل 1 من [ITU-T Y.2012] الرامية إلى أداء إدارة الهوية وعلاقات الترابط والربط.
- العناصر الوظيفية في الشكل 1 من [ITU-T Y.2012] الرامية إلى تعزيز التحكم في النفاذ اعتماداً على إنكار الاستيقان.

يستعمل الشكل 4 الشكل 1 من [ITU-T Y.2012] لبيان علاقات الاستيقان بين الأقران المحددة في الفقرة 5.5 من التوصية الحالية. وتبيِّن روابط الاستيقان بين الأقران في شكل أسهم مزدوجة الرؤوس. ولا يبدو في الشكل الخطوة (5)، الاستيقان والترخيص بين الأقران من المستعملين. ويلاحظ، حتى عندما يقوم مقدم خدمات شبكات الجيل التالي بتقديم التطبيقات إلى المستعمل (أي بدون سطح التماس بين التطبيق والشبكة (ANI))، أنه ما زالت هنالك علاقة استيقان بين المستعمل النهائي والتطبيق وبين طبقة الخدمة والتطبيق.



الشكل 4 – مراجع الاستيقان بين الأقران

يبرز الشكل 5 الكيانات الوظيفية من النموذج المرجعي في [IYI-T Y.2012] الذي يوفر أو قد يوفر وظائف الاستيقان والترخيص.



الشكل 5 – الكيانات الوظيفية للاستيقان والترخيص في التوصية [ITU-T Y.2012]

6 متطلبات عامة

تتطلب هذه التوصية توفير المتطلبات العامة لتعرف الهوية والاستيقان والترخيص المحددة في [ITU-T Y.2701] و[ITU-T Y.2201] وذلك على النحو التالي:

(R-1) – توفير المتطلبات المحددة في البند 2.3.7 (استيقان) من [ITU-T Y.2701].

(R-2) – توفير المتطلبات المحددة في البند 12.6 (تعرف هوية واستيقان وترخيص) من [ITU-T Y.2201].

7 استيقان وترخيص المستعمل للنفاذ إلى الشبكة

1.7 الوصف

يحتاج الأمر إلى خدمات ومقدرات استيقان وترخيص النفاذ إلى الشبكة وذلك للحد من التهديدات المرتبطة بالنفاذ غير المرخص به. ويحتاج الأمر أيضاً إلى خدمات الاستيقان والترخيص بالنفاذ إلى الشبكة للتحقق من الهويات ولتحديد ما إذا كان ينبغي منح النفاذ إلى تجهيزات المستعمل النهائي (أي التجهيزات المطرافية (TE) وعناصر حدود التجهيزات المطرافية (TE-BE)) التي تطلب التوصيلية إلى شبكات الجيل التالي.

افتراضات عامة:

أ) لا يقتصر المستعمل النهائي على الأشخاص بل قد يكون شخصاً أو مجموعات أو شركات أو كيانات قانونية.

ب) طبقاً للتوصية [ITU-T Y.2012]، لا توضع أي افتراضات بشأن مختلف السطوح البينية للمستعمل النهائي وشبكات المستعمل النهائي التي يمكن توصيلها بشبكة النفاذ إلى شبكات الجيل التالي. ويمكن استيعاب جميع فئات تجهيزات المستعمل النهائي في شبكات الجيل التالي، من موروث الهواتف وحيدة الخط إلى شبكات المؤسسات المعقدة. وقد تكون تجهيزات المستعمل النهائي إما متنقلة أو ثابتة.

ج) لا يقع في نطاق هذه التوصية تقرير عناصر الشبكة التي تنفِّذ خدمات النفاذ والترخيص.

د) يمكن توفير وظائف النفاذ إلى الشبكة والترخيص كجزء من وظيفة التحكم في الارتباط بالشبكة العامة (NACF) المعرَّفة في التوصية [ITU-T Y.2012].

2.7 النموذج المرجعي العام

يبيِّن الشكل 6 النموذج المرجعي للاستيقان والترخيص بالنفاذ/الارتباط بالشبكة والذي يتألف من ميادين الأمن التالية:

1) ميدان العميل – ميدان غير موثوق به يحتوي تجهيزات المستعمل التي يملكها ويشغِّلها العميل، مثال ذلك:)

أ) موروث تجهيزات مطرافية (TE) وعنصر حدود تجهيزات مطرافية (TE-BE):

- يمثل موروث التجهيزات المطرافية (TE) الموروث من أجهزة المستعمل الموصولة عبر نفاذ ضيق النطاق (خطوط تماثلية أو ISDN مثلاً). ويكون نفاذ هذه التجهيزات TE إلى شبكة بروتوكول الإنترنت عبر بوابة مقدم شبكات الجيل التالي (بوابة نفاذ أو بوابة وسائط مثلاً).
- يمثل عنصر حدود التجهيزات المطرافية (TE-BE) تجهيزات المستعمل التي تُستخدم بمثابة تجميع لنقاط انتهاء (مثال ذلك بوابة مؤسسة وبوابة شبكة محلية) موصولة عبر نفاذ بالنطاق الضيق (مثل الخطوط التماثلية وخطوط ISDN). ويكون نفاذ هذه العناصر (TE-BE) إلى شبكة بروتوكول الإنترنت عبر بوابة مقدم NGN (بوابة نفاذ أو بوابة وسائط مثلاً).

ب) موروث التجهيزات TE والعناصر TE-BE المزوَّد بجهاز النفاذ المتكامل (IAD):

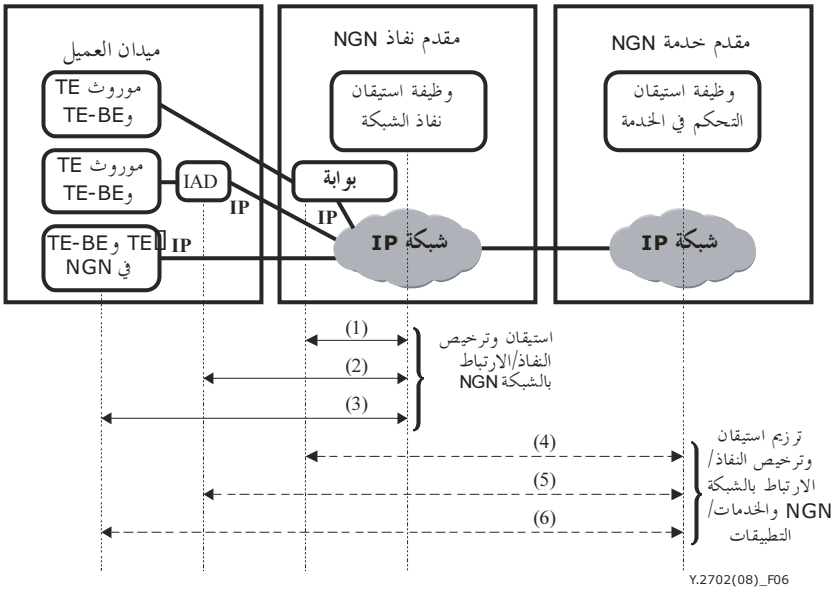
- يمثل الموروث TE المزوَّد بالجهاز IAD موروث أجهزة مستعمل موصولة عبر النفاذ عريض النطاق (مثال ذلك xDSL أو كبل). ويكون نفاذ هذه الأجهزة TE إلى شبكة بروتوكول الإنترنت عبر جهاز النفاذ المتكامل (IAD) في ميدان العميل.
- يمثل موروث العناصر TE-BE تجهيزات المستعمل التي تعمل بمثابة تجميع لنقاط الانتهاء (مثال ذلك بوابة مؤسسة وبوابة شبكة محلية) الموصولة عبر نفاذ النطاق العريض (مثال ذلك xDSL وكبل). ويكون نفاذ معدات المستعمل هذه إلى شبكة بروتوكول الإنترنت عبر الجهاز IAD في ميدان العميل.

ج) التجهيزات TE وعناصر TE-BE في شبكات الجيل التالي:

- تمثل التجهيزات TE في شبكات الجيل التالي تجهيزات المستعمل في ميدان العميل على أساس مقدرات بروتوكول الإنترنت لدعم التوصيلية المباشرة إلى شبكة بروتوكول الإنترنت (مثال ذلك باستعمال xDSL والنفاذ الكبلي عريض النطاق).
- تمثل العناصر TE-BE في شبكات الجيل التالي تجهيزات المستعمل التي تُستخدم بمثابة تجميع لنقاط الانتهاء (مثال ذلك بوابة مؤسسة وبوابة شبكة مركزية) تتسم بمقدرات بروتوكول الإنترنت لدعم التوصيلية مباشرة إلى شبكة بروتوكول الإنترنت.

2) ميدان مقدم النفاذ NGN: شبكة نفاذ يستضيفها مقدم خدمات NGN (مثال ذلك النطاق الضيق وخط xDSL والكبل). وقد يكون أو لا يكون مقدم النفاذ إلى شبكات NGN نفس مقدم خدمة هذه الشبكات. وتحكم علاقات الثقة بين مقدِّمي خدمات NGN اتفاقات مستوى الخدمة (SLA).

3) ميدان مقدم خدمات NGN: يعرض مقدم خدمات NGN خدمات تطبيقات NGN على المشتركين لديه. وتحكم علاقات الثقة بين مقدِّمي خدمات NGN اتفاقات مستوى الخدمة (SLA).



الشكل 6 – نموذج مرجعي لاستيقان وترخيص النفاذ/الارتباط بالشبكة

يبيِّن الشكل 6 علاقات تعريف الهوية والاستيقان والترخيص للنفاذ/الارتباط بالشبكة:

أ) استيقان وترخيص النفاذ/الارتباط بجهاز في شبكة NGN – خدمات ومقدرة لتعرُّف واستيقان وترخيص نفاذ أو ارتباط أجهزة مستعمل من أجل النفاذ إلى شبكة بروتوكول الإنترنت.

1) يمثل تدفق المعلومات هذا خدمات ومقدرات تعرُّف واستيقان وترخيص موروث التجهيزات TE والعناصر TE-BE للنفاذ/الارتباط من أجل النفاذ إلى شبكة بروتوكول الإنترنت. ويكون تدفق المعلومات بين البوابة (المدعي) في ميدان النفاذ NGN الذي ينتهي بالموروث TE وTE-BE في ميدان العميل وبين عنصر الشبكة (مثال ذلك نقطة نفاذ إلى الشبكة) في ميدان النفاذ إلى NGN بتقديم وظائف الاستيقان والترخيص للنفاذ/ الارتباط بشبكات الجيل التالي. وقد تكون وظائف استيقان وترخيص النفاذ/الارتباط بالشبكات NGN (المحقق) جزءاً من الوظيفة العامة للتحكم في الارتباط بالشبكة (NACF) المعرَّفة في التوصية [ITU-T Y.2012]. ولكن مكان تنفيذ هذه الوظيفة يعتمد على التنفيذ.

2) يمثل تدفق المعلومات هذا خدمات ومقدرات تعرُّف واستيقان وترخيص موروث التجهيزات TE والعناصر TE-BE على أساس جهاز النفاذ المتكامل (IAD) في ميدان العميل من أجل النفاذ/الارتباط بشبكة نفاذ بروتوكول الإنترنت. ويكون تدفق المعلومات بين الجهاز IAD (المدعي) في ميدان العميل وبين عنصر شبكة (مثال ذلك نقطة نفاذ إلى الشبكة) في ميدان النفاذ إلى شبكات NGN التي تقدم الاستيقان والترخيص للنفاذ/الارتباط بشبكات الجيل التالي. وقد تكون وظائف استيقان وترخيص النفاذ/الارتباط بشبكات NGN (المحقق) جزءاً من الوظيفة العامة للتحكم NACF العامة المعرَّفة في التوصية [ITU-T Y.2012]. ولكن مكان تنفيذ هذه الوظيفة يعتمد على التنفيذ.

3) يمثل تدفق المعلومات هذا خدمات ومقدرات تعرُّف واستيقان وترخيص التجهيزات TE والعناصر TE-BE في شبكات الجيل التالي التي لها مقدرات بروتوكول الإنترنت في ميدان العميل من أجل النفاذ/الارتباط

بشبكة بروتوكول الإنترنت. ويكون تدفق المعلومات بين التجهيزات TE أو العناصر TE-BE في شبكات NGN (المدعي) في ميدان العميل وبين عنصر شبكة (مثال ذلك نقطة نفاذ إلى الشبكة) في ميدان النفاذ إلى شبكات NGN التي تقدم الاستيقان والترخيص للنفاذ/الارتباط بشبكات NGN. وقد تكون وظائف استيقان وترخيص بالنفاذ/الارتباط بشبكات NGN (المحقق) جزءاً من الوظيفة العامة للتحكم NACF المعرَّفة في [ITU-T Y.2012]. ولكن مكان تنفيذ هذه الوظيفة يعتمد على التنفيذ.

ب) ترزيم أجهزة النفاذ/الارتباط بشبكات NGN واستيقان وترخيص الخدمة/التطبيق – خدمات ومقدرات لترزيم استيقان أجهزة المستعمل في النفاذ إلى مقدم خدمات NGN مع استيقان وترخيص المستعمل لخدمات مقدم NGN:

4) يمثل تدفق المعلومات هذا خدمات ومقدرات تمكن مقدم خدمات NGN ضمناً من تعرُّف وترخيص موروث التجهيزات TE والعناصر TE-BE. ويكون تدفق المعلومات بين بوابة (المدعي) في ميدان النفاذ إلى الشبكة وبين ميدان مقدم خدمات NGN (المحقق).

5) يمثل تدفق المعلومات هذا خدمات ومقدرات تمكّن مقدم خدمات NGN ضمناً من تعرُّف وترخيص موروث التجهيزات TE والعناصر TE-BE على أساس جهاز النفاذ المتكامل (IAD). ويكون تدفق المعلومات بين الجهاز IAD (المدعي) في ميدان العميل وبين ميدان مقدم خدمة NGN (المحقق).

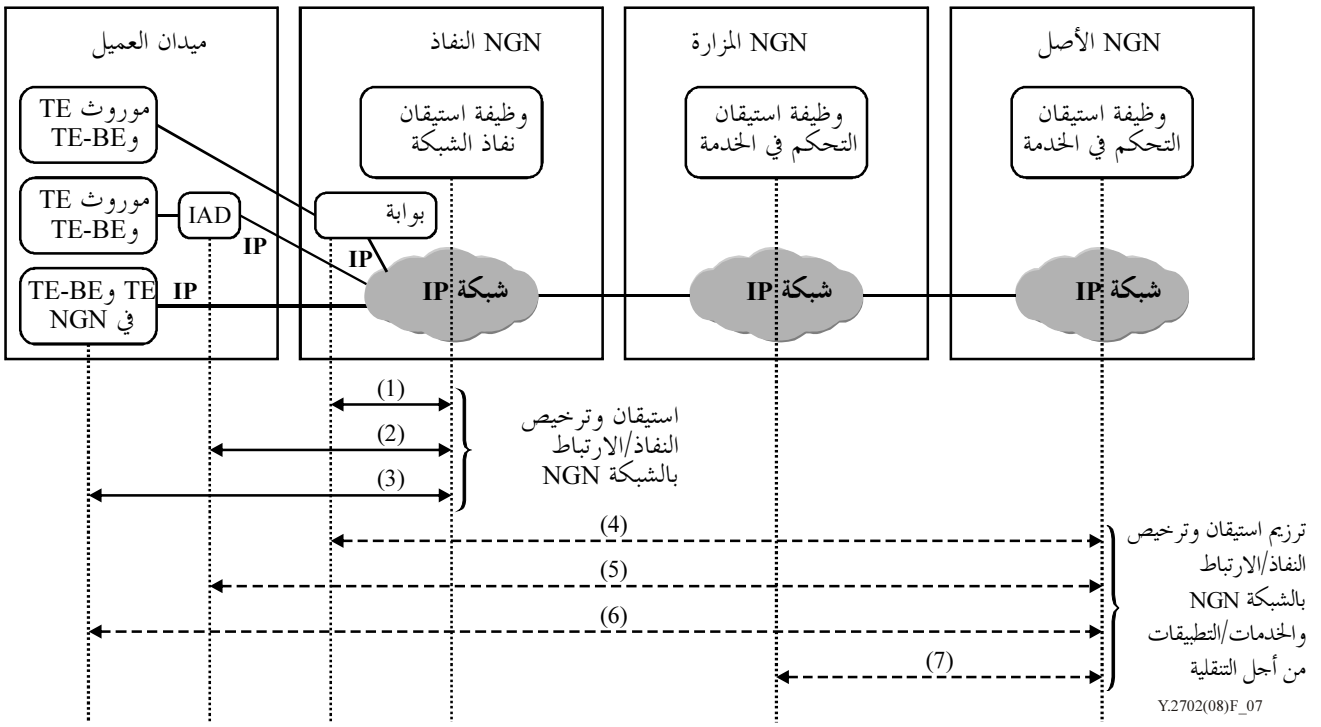
6) يمثل تدفق المعلومات هذا خدمات ومقدرات تمكّن مقدم خدمات NGN ضمناً من تعرُّف واستيقان وترخيص التجهيزات TE والعناصر TE-BE في شبكات الجيل التالي في ميدان العميل. ويكون تدفق المعلومات بين التجهيزات TE والعناصر TE-BE في شبكات NGN (المدعي) في ميدان العميل وبين ميدان مقدم خدمات NGN (المحقق).

نموذج مرجعي من أجل التجوالية

يبيِّن الشكل 7 النموذج المرجعي من أجل التجوالية. وهذا النموذج المرجعي مشابه للنموذج المرجعي العام ما عدا أن هنالك في هذا السيناريو شبكة NGN مزارة وشبكة NGN أصل ينبغي أن تؤخذا في الاعتبار.

1) ميدان NGN المزارة: شبكة NGN يستضيفها مورد خدمات NGN مزارة. يقدم وظائف شبكة مزارة لموردي خدمات NGN آخر (أي مقدم خدمات الشبكة الأصل). وعلاقات الثقة تحكمها اتفاقات مستوى الخدمة. ويمكن أن تقدم الشبكة المزارة خدمات NGN كما يمكن أن يكون لها مشتركوها الخاصون بها.

2) ميدان شبكة NGN الأصل: شبكة NGN يستضيفها مقدم خدمات NGN الأصل. يوفر مقدم خدمات NGN الأصل خدمات NGN إلى مشتركيه. وعلاقات الثقة تحكمها اتفاقات مستوى الخدمة.



الشكل 7 – النموذج المرجعي من أجل التجوالية

يبيِّن النموذج المرجعي تدفق المعلومات بين مختلف الميادين لترزيم استيقان وترخيص جهاز المستعمل واستيقان وترخيص المستعمل من أجل التجوالية. وتمثل تدفقات المعلومات الخدمات والمقدرات اللازمة لترزيم استيقان وترخيص جهاز المستعمل لدى مقدم خدمات NGN المزارة مع استيقان وترخيص المستعمل من أجل التجوالية لدى مقدم خدمات NGN الأصل.

(1) –(6) – تدفقات المعلومات هذه هي نفس التدفقات الموصوفة لسيناريو مقدم الخدمات الوحيد في الشكل 6.

(7) – يمثل تدفق المعلومات هذا الخدمات والمقدرات لدى مقدم خدمات NGN المزارة ومقدم خدمات NGN الأصل لتبادل معلومات التعرُّف والاستيقان والترخيص من أجل التجوالية.

3.7 المتطلبات

1.3.7 متطلبات عامة

فيما يلي المتطلبات العامة من أجل تعرُّف واستيقان وترخيص نفاذ/ارتباط الأجهزة بالشبكات:

(R-3) – من المطلوب أن تتمكن شبكة NGN من أن تتعرَّف بشكل فريد على أجهزة المستعمل النهائي/المشترك (مثال ذلك التجهيزات TE والعناصر TE-BE) اعتماداً على سياسة مقدم خدمات NGN.

(R-4) – من المطلوب أن تتمكن شبكة NGN من تعرُّف واستيقان وترخيص اتصال التجهيزات TE والعناصر TE-BE عند نقاط النفاذ إلى الشبكات (NAP).

(R-5) – من المطلوب ألا يُمنح النفاذ إلى الشبكة سوى إلى الأجهزة TE والعناصر TE-BE المرخَّص لها.

(R-6) – بالنسبة لترتيبات تعدد الشبكات، من المطلوب من كل ميدان إداري (مثال ذلك مقدم خدمات النفاذ إلى شبكة NGN ومقدم خدمات NGN المزارة ومقدم خدمات NGN الأصل) أن يقوم بتنفيذ سياسات (علاقات الثقة مثلاً) من أجل تعرُّف واستيقان وترخيص نفاذ/ارتباط شبكة التجهيزات TE والعناصر TE-BE (باستعمال اتفاقات مستوى الخدمة مثلاً).

(R-7) – من المطلوب أن يكون لدى NGN مقدرات دعم لحماية معلومات الاستيقان والترخيص (مثال ذلك جانبية المستعمل ومعلومات الاشتراك وأنماط الهوية) من النفاذ غير المرخَّص له أو التلاعب أو التخريب.

(R-8) – من المطلوب أن تكون لدى NGN مقدرات دعم لتوفير السرية وسلامة الحماية لتبادلات الرسائل والمعلومات المستعملة لأغراض الاستيقان والترخيص.

(R-9) – من المطلوب أن يكون لدى NGN مقدرات دعم للحماية من الهجمات (مثال ذلك تكرار الرسائل وهجمات إنكار الخدمة) على وظائف ومقدرات الاستيقان والترخيص.

(R-10) – من المطلوب أن تكون شبكات NGN قادرة على تحرّي وتسجيل محاولات النفاذ غير المرخَّص له (مثال ذلك إمكانية تحديد عتبة جهاز قابلة للتشكيل بالنسبة لعدد محاولات النفاذ غير المرخَّص له حيث يتولّد بعد هذه العتبة إنذار ويسجل ويبلّغ إلى نظام الإدارة).

2.3.7 الموروث من تجهيزات TE وعناصر TE-BE

يتعيَّن على نقاط النفاذ إلى الشبكة (NAP) التي تدعم النفاذ إلى شبكات الموروث من تجهيزات TE وعناصر TE-BE أن تكون قادرة على دعم تعرُّف واستيقان وترخيص هذا النفاذ.

(R-11) – من المطلوب أن تكون نقاط النفاذ إلى الشبكة (NAP) التي تدعم الموروث من تجهيزات TE وعناصر TE-BE أن تكون قادرة على تعرُّف فريد للخط الثابت من أجل الارتباط أو التوصيلية بشبكة NGN. ويمكن استعمال عنوان الطبقة 2 لتعرُّف خط ثابت (مثال ذلك عنوان تحكم في النفاذ إلى الوسائط (MAC) أو عنوان طبقة الوصل). ويمكن توفير هذه الوظيفة كجزء من الوظيفة العامة للتحكم في الارتباط بالشبكة (NACF) المعرَّفة في التوصية [ITU-T Y.2012].

(R-12) – من المطلوب من نقاط النفاذ إلى الشبكة (NAP) التي تدعم الموروث من تجهيزات TE وعناصر TE-BE أن تكون قادرة على استيقان وترخيص الخط الثابت للارتباط أو التوصيلية بشبكة NGN. ويمكن استعمال قوائم التحكم في النفاذ (ACL) ومعلومات اشتراك طبقة النقل/جانبية المستعمل لترخيص نفاذ الخط الثابت إلى شبكة NGN. ويمكن توفير هذه الوظائف كجزء من الوظيفة العامة NACF المعرَّفة في التوصية [ITU-T Y.2012].

(R-13) – من المطلوب أن تكون النقاط NAP التي تدعم الموروث من تجهيزات TE وعناصر TE-BE أن تكون قادرة على وصل وضم هوية خط ثابت إلى عنوان بروتوكول الإنترنت المستعمل من أجل توصيلية النفاذ إلى شبكة NGN. ويمكن توفير هذه الوظيفة كجزء من الوظيفة العامة NACF المعرَّفة في التوصية [ITU-T Y.2012].

3.3.7 الموروث من تجهيزات TE وعناصر TE-BE المزودة بجهاز نفاذ متكامل (IAD)

يتعيَّن أن تكون النقاط NAP التي تدعم نفاذ الشبكة لتجهيزات TE وعناصر TE-BE المزودة بجهاز نفاذ متكامل (IAD) في ميدان العميل أن تكون قادرة على تعرُّف واستيقان وترخيص مثل هذا النفاذ.

(R-14) – من المطلوب من النقاط NAP التي تدعم الموروث من تجهيزات TE وعناصر TE-BE المزودة بجهاز نفاذ متكامل (IAD) في ميدان العميل أن تكون قادرة على تعرّف فريد للخط الثابت وللجهاز IAD من أجل الارتباط أو التوصيلية بشبكة NGN. ويمكن استعمال عنوان الطبقة 2 لتعرّف خط ثابت (مثال ذلك عنوان تحكم MAC أو عنوان طبقة الوصل) وعنوان IP من أجل الجهاز IAD. ويمكن توفير هذه الوظيفة كجزء من الوظيفة العامة NACF المعرّفة في التوصية [ITU-T Y.2012].

(R-15) – من المطلوب من النقاط NAP التي تدعم الموروث من تجهيزات TE وعناصر TE-BE والمزودة بجهاز IAD في ميدان العميل أن تكون قادرة على استيقان وترخيص الجهاز IAD من أجل الارتباط أو التوصيلية بشبكة NGN. ويمكن استعمال القوائم ACL ومعلومات اشتراك طبقة النقل/جانبية المستعمل لترخيص نفاذ الجهاز IAD والخط الثابت إلى شبكة NGN. ويمكن توفير هذه الوظائف كجزء من الوظيفة العامة NACF المعرّفة في التوصية [ITU-T Y.2012].

(R-16) – من المطلوب من النقاط NAP التي تدعم الموروث من تجهيزات TE وعناصر TE-BE والمزودة بجهاز IAD في ميدان العميل أن تكون قادرة على وصل وضم هوية خط ثابت بهوية جهاز IAD. ويمكن توفير هذه الوظيفة كجزء من الوظيفة العامة NACF المعرّفة في [ITU-T Y.2012].

4.3.7 التجهيزات TE والعناصر TE-BE في شبكات الجيل التالي

يتعيَّن أن تكون النقاط NAP التي تدعم نفاذ تجهيزات TE وعناصر TE-BE إلى شبكات NGN قادرة على تعرّف واستيقان وترخيص مثل هذا النفاذ.

(R-17) – من المطلوب من النقاط NAP التي تدعم التجهيزات TE والعناصر TE-BE في شبكات NGN (أي التوصيلية المباشرة ببروتوكول الإنترنت) أن تكون قادرة على دعم تعرُّف فريد لتجهيزات المستعمل ضمن ميدانه من أجل الارتباط والتوصيلية بشبكات NGN. ويمكن التعرُّف بصورة فريدة إلى التجهيزات TE والعناصر TE-BE في شبكات NGN بواسطة هويات الأجهزة وعناوين الشبكات (مثال ذلك هويات التجهيزات وبطاقات وحدة تعرُّف هوية المشترك (SIM) وعلامات الأمن وعناوين بروتوكول الإنترنت، وغير ذلك).

(R-18) – من المطلوب من النقاط NAP التي تدعم التجهيزات TE والعناصر TE-BE في شبكات NGN (أي التوصيلية المباشرة ببروتوكول الإنترنت) أن تكون قادرة على استيقان وترخيص أجهزة المستعمل ضمن ميدانه من أجل الارتباط أو التوصيلية بشبكات NGN. ويمكن أن يعتمد الاستيقان والترخيص على معلومات اشتراك طبقة النقل/جانبية المستعمل. ويقتصر السماح بالارتباط أو التوصيلية بالشبكات NGN على تجهيزات TE وعناصر TE-BE المرخص لها في شبكات NGN. ويمكن توفير هذه الوظائف كجزء من الوظيفة العامة NACF المعرَّفة في [ITU-T Y.2012].

5.3.7 ترزيم استيقان وترخيص المستعمل وأجهزة المستعمل

قد يحتاج الأمر، تبعاً لتقييم المخاطر، إلى تجميع استيقان وترخيص المستعمل وأجهزة المستعمل وذلك لتوفير سوية أعلى من كفالة الهوية. ويمكن لشبكات NGN أن تكون قادرة على ترزيم وظائف الاستيقان من أجل النفاذ/الارتباط بشبكات NGN والنفاذ إلى الخدمات/التطبيقات اعتماداً على معلومات طبقة النقل (مثل معلومات أجهزة المستعمل والنفاذ إلى الشبكة) ومعلومات طبقة الخدمة (مثل جانبية الاشتراك/المستعمل).

(R-19) – من المطلوب توفُّر مقدرات التعرُّف الفريد وترزيم مجموعة المستعملين وأجهزة المستعملين اعتماداً على سياسة مقدم خدمات NGN.

(R-20) – من المطلوب أن تتوفر مقدرات استيقان وترخيص مجموع المستعملين وأجهزة المستعملين اعتماداً على سياسة مقدم خدمات NGN. ويقتصر السماح بالارتباط/النفاذ إلى الشبكة والنفاذ إلى الخدمات/التطبيقات على المستعملين المرخَّص لهم والأجهزة المرخَّص لها.

6.3.7 استيقان وترخيص ترزيم المستعملين وأجهزة المستعملين من أجل التجوالية

من الممكن استيقان وترخيص مجموع المستعملين وأجهزة المستعملين لتوفير سوية أعلى من كفالة الهوية من أجل التجوالية. ومن الممكن توفير المقدرات من أجل تبادل وتقاسم معلومات تعرُّف الهوية والاستيقان والترخيص (معلومات جانبية المستعمل مثلاً) بين مختلف الميادين الإدارية (أي مقدم النفاذ إلى شبكات NGN ومقدم خدمات NGN المزارة ومقدم خدمات NGN الأصل) من أجل إدارة الهوية (انظر الفقرة 2.2.8).

(R-21) – من المطلوب توفُّر مقدرات التعرُّف الفريد على مجموع المستعملين وأجهزة المستعملين من أجل التجوالية وذلك اعتماداً على سياسة مقدم خدمات NGN.

(R-22) – من المطلوب توفُّر مقدرات استيقان وترخيص مجموع المستعملين وأجهزة المستعملين من أجل التجوالية وذلك اعتماداً على سياسة مقدم خدمات NGN. وفي الحالات التي تكون فيها الخدمة مستقلة عن جهاز المستعمل، من الممكن تجميع استيقان معلومات النفاذ، مثل الخط الثابت أو الموقع أو عنوان النفاذ، مع عملية استيقان المستعمل وذلك لتوفير سوية أعلى من الكفالة.

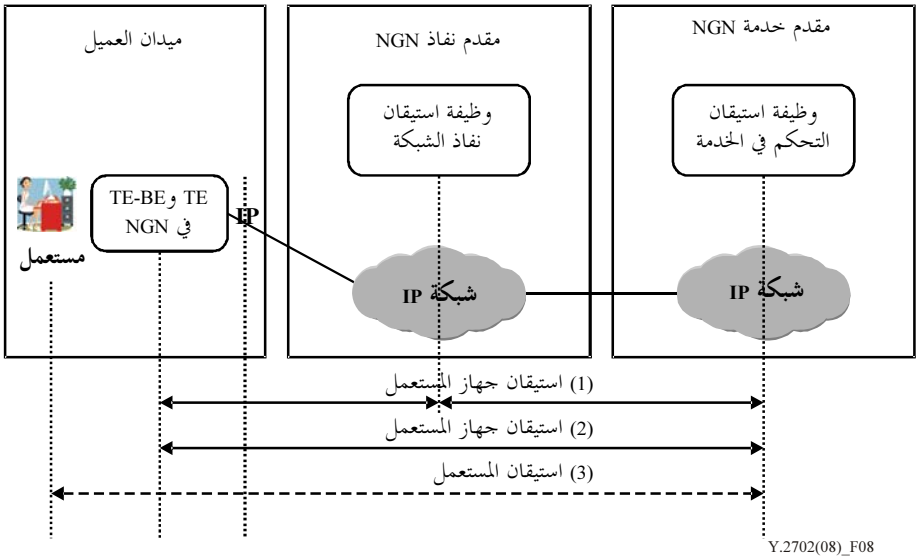
8 استيقان وترخيص المستعمل من جانب مقدم خدمات NGN من أجل النفاذ إلى الخدمة/التطبيق

1.8 الوصف

يحتاج الأمر إلى توفُّر مقدرات للتخفيف من التهديدات المرتبطة بالنفاذ غير المرخَّص به إلى الخدمات والمزايا التي يوفِّرها مقدم خدمات NGN. كما يحتاج الأمر إلى خدمات ومقدرات الاستيقان والترخيص لتقرير ما إذا كان المستعمل مرخَّصاً له بتلقي الخدمة أو مرخَّصاً له بأداء إجراء ما اعتماداً على الامتيازات الممنوحة له. ويعتبر استيقان وترخيص الخدمة/التطبيق بمثابة استيقان مقدم خدمات NGN من المستعمِل والترخيص للمستعمل بتلقي خدمات NGN أو أداء إجراء اعتماداً على الامتيازات الممنوحة له. وقد يتطلب استيقان وترخيص الخدمة/التطبيق التحقق من الهويات والترخيص بالامتيازات للجهات التالية:

- المستعمل
- جهاز المستعمل
- مجموع المستعمل والجهاز

من الممكن، اعتماداً على معمارية NGN المعرَّفة في [ITU-T Y.2012]، توفير وظائف استيقان وترخيص الخدمة/التطبيق في طبقة الخدمة باستعمال معلومات الاشتراك وجانبية المستعمل.



الشكل 8 – نموذج مرجعي لاستيقان وترخيص الخدمة/التطبيق

يبيِّن الشكل 8 مثالاً لعلاقات استيقان وترخيص الخدمة/التطبيق في إطار سيناريو مقدم خدمة شبكات متعددة:

(1) يمثل تدفق المعلومات هذا جانب مقدم خدمة NGN المعتمد على مورد خدمة نفاذ NGN للاستيقان لجهاز مستعمل من خلال روابط ثقة.

(2) يمثل تدفق المعلومات هذا الاستيقان والترخيص من جانب مقدم خدمة NGN لجهاز المستعمل. وتتطلب هذه الحالة أن ينطوي جهاز المستعمل على مقدرات تعرُّف خاصة (مثال ذلك وحدة تعرُّف هوية المشترك (SIM)).

(3) يمثل تدفق المعلومات هذا الاستيقان من جانب مقدم خدمة NGN من المستعمل (مثال ذلك عندما يسجل المستعمل نفسه ويقدم كلمة السر أو رقم تعرف هوية شخصي (PIN)).

2.8 المتطلبات

1.2.8 متطلبات عامة

فيما يلي المتطلبات العامة فيما يتعلق باستيقان وترخيص المستعمل من جانب مقدم خدمة NGN:

(R-23) – من المطلوب أن تتمكن شبكة NGN من تعرُّف هوية المستعمل وجهاز المستعمل ومجموع المستعمل والجهاز اعتماداً على معلومات الاشتراك وجانبية المستعمل.

(R-24) – من المطلوب أن تتمكن شبكة NGN من استيقان وترخيص المستعمل أو جهاز المستعمل أو مجموع المستعمل والجهاز اعتماداً على معلومات الاشتراك وجانبية المستعمل.

(R-25) – من المطلوب أن يقتصر منح خدمات NGN على المستعمل أو الجهاز أو مجموع المستعمل والجهاز المرخَّص له.

(R-26) – من المطلوب أن تكون شبكة NGN قادرة على تحقق وترخيص امتيازات المستعمل (مثال ذلك السماح للمستعمل بأداء بعض الإجراءات فقط في حالة الترخيص له بذلك الدور أو الامتياز).

(R-27) – بالنسبة لترتيبات الشبكات المتعددة، يتعيَّن على كل ميدان إداري (مثال ذلك مقدم نفاذ NGN ومقدم خدمات NGN المزارة ومقدم خدمات NGN الأصل) أن يطبِّق سياسات (مثال ذلك اتفاقات مستوى الخدمة) من أجل تعرّف واستيقان وترخيص مستعمل ما أو جهاز مستعمل أو مجموع المستعمل والجهاز.

(R-28) – من المطلوب أن تكون شبكات NGN قادرة على توفير حماية السرية والسلامة لتبادلات الرسائل والمعلومات المستعملة لاستيقان وترخيص المستعمل أو جهاز المستعمل أو مجموع المستعمل والجهاز.

(R-29) – من المطلوب أن تكون شبكات NGN قادرة على الحماية من النفاذ غير المرخَّص به ومن التلاعب ومن تخريب معلومات خدمة الاستيقان والترخيص (مثال ذلك معلومات الاشتراك وجانبية المستعمل).

(R-30) – من المطلوب أن تكون شبكات NGN قادرة على الحماية من الهجمات (مثل هجمات تكرار الرسائل وإنكار الخدمة) على وظائف ومقدرات الاستيقان والترخيص.

(R-31) – من المطلوب أن تتوفر إمكانات ترزيم الاستيقان المرتبط بتكنولوجيا النفاذ إلى الشبكة لدى جهاز المستعمل مع الاستيقان من المستعمل وذلك على أساس سياسة مقدم خدمات NGN.

(R-32) – من المطلوب أن تكون شبكات NGN قادرة على كشف وتدوين محاولات النفاذ غير المرخَّص به إلى خدمات أو موارد شبكات NGN (مثال ذلك إمكانية تحديد عتبة نظام قابلة للتشكيل من أجل عدد معيَّن من محاولات النفاذ غير المرخَّص به حيث يتولّد بعد هذه النقطة إنذار ويدوَّن ويُبلّغ إلى نظام الإدارة).

(R-33) – من المطلوب أن تكون شبكات NGN قادرة على كشف وتدوين محاولات استغلال الامتيازات غير المرخَّص بها (مثال ذلك إجراءات المستعمل غير المرخَّص بها).

2.2.8 تقاسم نتائج الاستيقان من أجل إدارة الهوية

قد يحتاج مقدم خدمات NGN إلى تبادل نتائج الاستيقان بين مختلف الخدمات و/أو التطبيقات ضمن شبكته أو خارجياً مع مقدِّمي خدمات NGN آخرين وذلك لتنفيذ خدمات إدارة الهوية. وقد يشتمل ذلك على التأكيدات وغير ذلك من المعلومات ذات الصلة بإدارة الهوية ومنها (دون حصر):

أ) سياسة الثقة؛

ب) طريقة الاستيقان والمعلومات المستعملة من أجل الاستيقان (مفاتيح الاستيقان مثلاً)؛

ج) سويات الكفالة؛

د) معلومات إدارة الامتيازات (مثال ذلك الامتيازات المخصصة أو المحققة).

من شأن مقدرات توفير التبادل الآمن لمعلومات نتيجة الاستيقان (كالتأكيدات مثلاً) وما يتصل بذلك من معلومات، كما هو موصوف أعلاه، أن يمكِّن مقدِّمي خدمات NGN من تصميم منصات الخدمة/التطبيق باستخدام ملامح استيقان وترخيص تتسم بالكفاءة وسهولة الاستعمال. إذ يمكن مثلاً تقاسم معلومات نتائج الاستيقان بين الأنظمة (مخدمات التطبيقات مثلاً) التي تدعم مختلف الخدمات و/أو التطبيقات لتمكين مقدم خدمات NGN من توفير مزايا وقدرات "الاستيقان الوحيد" مما يخفف العبء على المستعمل. وتنطبق المتطلبات التالية على تبادل وتقاسم نتائج الاستيقان ضمن شبكة مقدم خدمات NGN:

(R-34) – من المطلوب أن تتمكن شبكات NGN من تمكين الأنظمة وعناصر الشبكات (مخدمات التطبيقات مثلاً) التي تدعم مختلف الخدمات و/أو التطبيقات من تبادل وتقاسم معلومات نتائج الاستيقان (مثال ذلك التأكيدات ومعلومات إدارة الامتيازات وسياسة الثقة وسويات الكفالة) القائمة بشكل آمن على التصميمات وسياسة الأمن الخاصة بمنصة الخدمة/التطبيق لدى مقدم خدمات NGN.

(R-35) – من المطلوب حماية الاتصال بين مختلف الأنظمة أو عناصر الشبكات (مخدمات التطبيق مثلاً) لتبادل أو تقاسم معلومات نتائج الاستيقان وذلك من النفاذ غير المرخَّص به أو المراقبة أو التلاعب أو التخريب (مثال ذلك حماية السرية والسلامة). ويشمل ذلك حماية أي معلومات مخزنة.

وقد يحتاج مقدمو خدمات NGN، في بيئة شبكات متعددة، إلى تبادل وتقاسم نتائج الاستيقان بشكل آمن فيما بينهم على أساس اتفاقات مستوى الخدمة. وتنطبق المتطلبات التالية على تبادل وتقاسم نتائج الاستيقان بين مختلف مقدِّمي خدمات NGN:

(R-36) – من المطلوب توفُّر مقدرات لتمكين مقدِّمي خدمات NGN من تبادل وتقاسم نتائج الاستيقان بشكل آمن (أي عبر سطح التماس بين شبكتين NNI وبين التطبيق والشبكة ANI) اعتماداً على علاقات الثقة والسياسات واتفاقات مستوى الخدمة القائمة بين مقدِّمي خدمات NGN.

(R-37) – من المطلوب حماية الاتصالات بين مقدِّمي شبكات NGN لتبادل وتقاسم معلومات نتائج الاستيقان (أي عبر سطح التماس بين شبكتين NNI وبين التطبيق والشبكة ANI) من النفاذ غير المرخَّص به أو المراقبة أو التلاعب أو التخريب (مثال ذلك حماية السرية والسلامة). ويشمل ذلك حماية أي معلومات مخزنة. وتقوم آليات الأمن المحددة وممارسات الأمن على علاقات الثقة والسياسات واتفاقات مستوى الخدمة القائمة بين مقدِّمي خدمات NGN.

(R-38) – من المطلوب توفُّر القدرات للبرهان على طريقة الاستيقان وتوصيل المعلومات عن الطريقة أو الطرائق التي استُخدمت لاستيقان الكيانات إلى الأطراف المعتمدة مثل:

- طريقة التحقق من هوية المستعمل؛
- طريقة الاستيقان (استعمال الشهادات الرقمية والتواقيع وعلامات الأمن وبيانات القياس الحيوي ووحدة تعرف هوية المشترك (SIM)، وغير ذلك)؛
- سياسة الثقة؛
- سويات كفالة الاستيقان.

يخضع تقاسم معلومات الاستيقان ونتائجه للامتثال للسياسات ذات الصلة مثل القواعد التنظيمية والتشريعات الوطنية والإقليمية من أجل حماية معلومات تحديد الهوية (PII).

(R-39) – يشترط أن يضمن مورد شبكات الجيل التالي الامتثال للسياسات ذات الصلة مثل التنظيمات والتشريعات الوطنية والإقليمية من أجل معلومات تحديد الهوية الشخصية (PII). ويشمل ذلك السياسات القائمة على مبادئ حماية البيانات الأساسية التالية:

- الربط بين البيانات الخاصة بغرض محدد؛
- عدم تقاسم البيانات بين تطبيقات متباينة الأغراض؛

- اقتصار البيانات على الحد الأدنى اللازم لغرض محدد؛
- حق الأشخاص في التحكم في المعلومات PII الخاصة بهم.

3.2.8 استيقان وترخيص المستعمل من جانب مقدم خدمات NGN من أجل النفاذ إلى خدمة/تطبيق معيّن

يتعيَّن على مقدِّمي خدمات NGN إدارة امتيازات المستعمل من أجل النفاذ (بما في ذلك أدوار وامتيازات المستعمل لأداء إجراءات معيَّنة) إلى خدمة/تطبيقات معيَّن مثل:

- خدمات صوت
- خدمات تدفق
- خدمات بيانات ومراسلة
- خدمة اتصالات الطوارئ (ETS) وخدمة اتصالات الإغاثة في حالات الكوارث (TDR)

وقد يكون لكل خدمة متطلب سوية الكفالة الخاصة بها لإثبات صلاحية هوية وامتيازات المستعمل أو جهاز المستعمل أو مجموع المستعمل والجهاز اعتماداً على المخاطر المرتبطة باحتمال تمكُّن كيانات غير مرخَّص لها بالنفاذ إلى مورد الخدمة. وينبغي وضع وتنفيذ سوية الكفالة الضرورية لاستيقان وإثبات صلاحية امتيازات المستعمل أو جهاز المستعمل أو مجموع المستعمل والجهاز لخدمة معيَّنة اعتماداً على سياسة الأمن في الشبكة NGN. ويستدعي ذلك توفُّر واستعمال مختلف طرائق الاستيقان التي تتراوح بين طرائق الاستيقان الأساسية باستعمال كلمات السر وأرقام تعرُّف الهوية الشخصية (PIN) وبين الطرائق الأكثر تشدداً التي تستعمل مفاتيح الاستيقان مثل:

أ) الشهادات الرقمية (مثال ذلك X.509 PKI)

ب) علامات الأمن (علامات المعدات والبرمجيات) والبطاقات الذكية

ج) البيانات الخاصة بالسلوك (مثال ذلك تحليل لمسات المفاتيح)

د) بيانات تعرُّف الهوية بالقياس الحيوي (مثال ذلك تعرُّف الصوت أو بصمات الأصابع أو بؤبؤ العين أو الشبكية)

ملاحظة – لا يفترض استيقان كيان ما الدلالة على تأكيد واضح لشخص ما.

وينبغي أيضاً أن يؤخذ في الحسبان سهولة الاستعمال من جانب المستعمل في مجال الاستيقان والترخيص. وينطبق ذلك بصفة خاصة على بعض أنماط الخدمات مثل خدمة اتصالات الطوارئ (ETS) واتصالات الإغاثة في حالات الكوارث (TDR). ومن المستحسن أن تكون عملية الاستيقان ميسورة الاستعمال من جانب المستعمل. يرجى الرجوع إلى التذييل II للاطلاع على أمثلة الاستيقان والترخيص في سياق خدمة اتصالات الطوارئ (ETS).

وعند النظر في عمليات الاستيقان والترخيص الخاصة بكل خدمة، تنطبق المتطلبات التالية بالإضافة إلى تلك الواردة في الفقرتين 1.2.8 و2.2.8:

(R-40) – من المطلوب توفُّر طرائق استيقان من أجل الشهادات اعتماداً على سياسة مقدم خدمات NGN. ويستدعي الأمر توفر طرائق استيقان متعددة العوامل واستعمالها حسب مقتضى الحال اعتماداً على سياسة مقدم خدمات NGN من أجل كفالة الهوية والامتياز.

(R-41) – من المطلوب، رهناً بسياسة مقدم خدمات NGN، أن يكون من الممكن التعرُّف بصفة فريدة على جميع المستعملين المرتبطين باشتراك في خدمة تطبيق. ويشمل ذلك تعرُّف هوية مجموعة مستعملين نهائيين قد لا تكون هوياتهم كمستعملين متوفرة لدى مقدم خدمات NGN.[2]

[2] يكون لنقطة نهاية تجمّعية تجمُّع مستعملَين أو أكثر مرتبطان بها. وقد تقتصر معرفة هوية هؤلاء المستعملين على نقطة النهاية التجمّعية فقط ولا تكون معروفة لدى مقدم خدمة NGN.

(R-42) – من المطلوب، رهناً بسياسة مقدم خدمات NGN، أن يكون من الممكن ربط عدد من المستعملين الإفراديين بنفس الاشتراك.

(R-43) – من المطلوب أن يكون كل مستعمل/مشترك مرتبط باشتراك خدمة تطبيق قابلاً للاتصال بشكل فريد.

(R-44) – من المطلوب، رهناً بسياسة مقدم خدمات NGN، أن يكون من الممكن للمستعمل النهائي النفاذ إلى خدمة ما عدة مرات في آن واحد و/أو من أجهزة متعددة.

(R-45) – من المطلوب أن يكون من الممكن تناول عدة جانبيات اشتراك لمستعمل نهائي بمفرده. ومن المطلوب توفُّر إمكانية تعرُّف هوية جانبيات الاشتراك المتعددة هذه بشكل فريد.

قد يكون من الضروري، رهناً بسياسة مقدم خدمات NGN، الاستيقان دورياً من مستعمل وذلك تحقيقاً لدرجة عالية من الكفالة والأمن.

(R-46) – من المطلوب، رهناً بسياسة مقدم خدمات NGN، أن يكون من الممكن إعادة استيقان المستعمل دورياً (مثال ذلك مستعمل نهائي أو عنصر شبكة أو شيء) طوال فترة جلسة اتصال أو معاملة قائمة.

9 استيقان وترخيص المستعمل لمقدِّمي خدمات NGN

تتناول هذه الفقرة المتطلبات المتصلة بقيام المستعمل باستيقان وترخيص شبكة ما (مثال ذلك استيقان المستعمل من هوية شبكة NGN الموصولة أو من مقدم الخدمة).

1.9 الوصف

تمكّن معمارية NGN المستعملين النهائيين من الحصول على خدمات من عدة مقدِّمي خدمات NGN. وعلاوة على ذلك، قد يكون مقدم خدمات النقل في شبكة NGN (مثال ذلك مقدم النفاذ إلى شبكة NGN) مختلفاً عن مقدم خدمة NGN. ونتيجة لذلك، قد يحتاج المستعملون النهائيون إلى التحقق من هويات مقدمي خدمات NGN (مثال ذلك مقدِّمو النفاذ والنقل والخدمة). وعلى وجه التحديد، ينبغي توفُّر ما يلي:

- مقدرات لتمكين المستعمل النهائي من تعرُّف واستيقان وترخيص مقدم نفاذ NGN من أجل توصيلية الشبكة (النفاذ إلى الشبكة مثلاً).
- مقدرات تمكين المستعمل النهائي من تعرُّف واستيقان وترخيص مقدم خدمات NGN.

2.9 الأهداف والمتطلبات

1.2.9 استيقان المستعمل من مقدم خدمات NGN من أجل الارتباط بالشبكة

ينبغي أن يتوفر في نقاط النفاذ إلى الشبكة، التي تدعم نفاذ التجهيزات المطرافية (TE) وعناصر حدود التجهيزات المطرافية (TE-BE) في شبكات NGN، مقدرات تمكّن المستعمل من تعرُّف واستيقان وترخيص الارتباط بالشبكة.

(R-47) – يتعين أن يكون لدى نقاط النفاذ إلى الشبكة (NAP)، التي تدعم التجهيزات TE والعناصر TE-BE في شبكات NGN (أي التوصيلية مباشرة ببروتوكول الإنترنت)، مقدرات لتمكين المستعمل النهائي من التعرُّف بشكل فريد على مقدم خدمات NGN لأغراض الارتباط والتوصيلية إذا ما تطلبت سياسة الأمن ذلك.

(R-48) – يتعين أن يكون لدى نقاط النفاذ إلى الشبكة (NAP)، التي تدعم التجهيزات TE والعناصر TE-BE في شبكات NGN (أي التوصيلية المباشرة ببروتوكول الإنترنت)، مقدرات لتمكين المستعمل من استيقان وترخيص مقدم خدمات NGN لأغراض الربط والتوصيلية إذا ما تطلبت سياسة الأمن ذلك. ويمكن توفير هذه الوظائف كجزء من وظيفة التحكم في الارتباط بالشبكة (NACF) المعرَّفة في التوصية [ITU-T Y.2012].

(R-49) – بالنسبة لترتيبات تعدد الشبكات، يتطلب من كل ميدان إداري (أي مقدم النفاذ إلى الشبكة ومقدم شبكة NGN المزارة ومقدم شبكة NGN الأصل) تنفيذ سياسات (مثل علاقات الثقة) فيما يتعلق بتعرُّف هوية واستيقان وترخيص الارتباط بالشبكة (مثال ذلك باستعمال اتفاقات مستوى الخدمة).

2.2.9 استيقان المستعمل من مقدم خدمات NGN من أجل الحصول على الخدمة

يمكن توفير مقدرات لتمكين المستعمل النهائي من استيقان وترخيص مقدم خدمات NGN للحصول على هذه الخدمات.

(R-50) – يتعين أن يكون لدى شبكات NGN مقدرات تمكّن المستعمل النهائي من التعرُّف بشكل فريد على مقدم خدمات NGN الذي يقدم خدمة ما أو مجموعة من الخدمات إذا ما تطلبت سياسة الأمن ذلك.

(R-51) – يتعين أن يكون لدى شبكات NGN مقدرات تمكّن المستعمل النهائي من استيقان وترخيص مقدم خدمات NGN الذي يقدم خدمة ما أو مجموعة من الخدمات إذا ما تطلبت سياسة الأمن ذلك.

10 الاستيقان والترخيص بين المستعملين من جانب مقدم خدمات NGN

الغرض من إدراج هذه الفقرة هو استكمال الصورة ومجرد الإعلام.

من المسائل الشفافة من منظور مقدم خدمات NGN حدوث الاتصالات بين المستعملين، إذ إن الحركة تعبر شبكة مقدم خدمات NGN في طبقة النقل فقط. وجدير بالملاحظة أن مقدم خدمات NGN قد يضطلع بالدور بوصفه مقدم هوية (IdP) يقدم خدمات إدارة الهوية (IdM) (مثال ذلك مقدرات للاستيقان بين الأقران) لسيناريوهات الاتصال هذه.

11 الاستيقان والترخيص المتبادلان بين الشبكات

1.11 الوصف

يحتاج الأمر إلى الاستيقان والترخيص المتبادل بين الشبكات للحد من التهديدات الناجمة عن النفاذ غير المرخَّص به. وكما يحتاج الأمر إلى خدمات استيقان وترخيص النفاذ إلى الشبكات للتحقق من الهويات ولتقرير ما إذا كان ينبغي منح النفاذ إلى طبقة النقل في الشبكة و/أو الخدمات والمقدرات. وقد يحدث النفاذ إلى الشبكة إما عند سطح التماس بين شبكتين (NNI) أو عند سطح التماس بين التطبيق والشبكة (ANI).

يبيِّن الشكل 9 النموذج المرجعي للاستيقان والترخيص المتبادلين بين الشبكات الذي يتألف من ميادين الأمن التالية:

1) ميدان شبكة النفاذ: شبكة نفاذ يستضيفها مقدم شبكة نفاذ (مثال ذلك نطاق عريض، xDSL، كبل). وقد يكون مقدم شبكة النفاذ أو لا يكون نفس مقدم شبكة NGN. وعلاقات الثقة بين مقدم شبكة النفاذ ومقدم شبكة NGN تحكمها اتفاقات مستوى الخدمة (SLA).

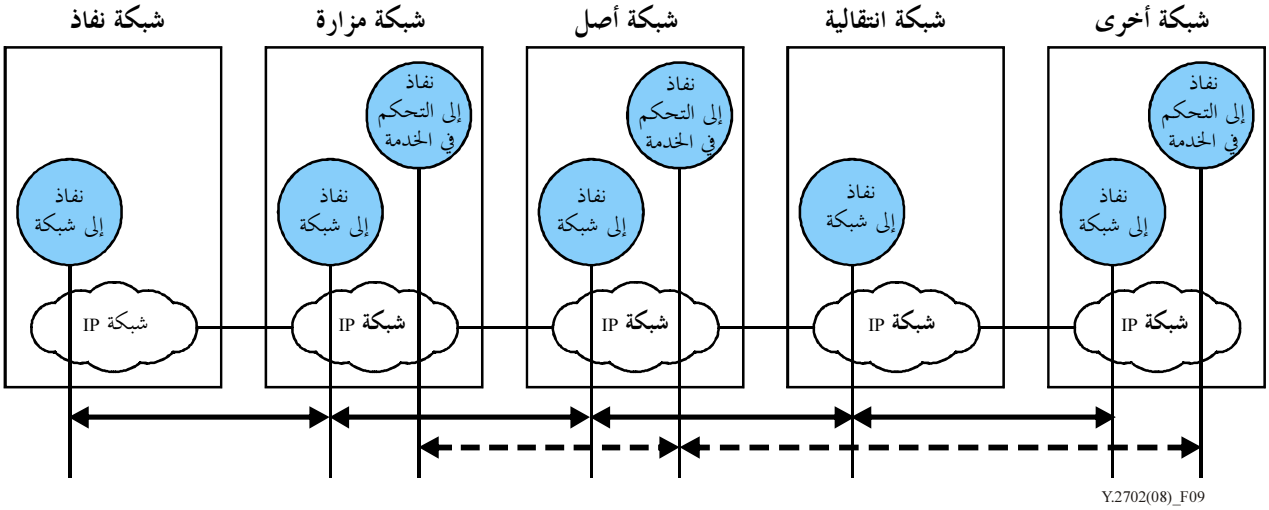
2) ميدان NGN المزارة: NGN يستضيفها مقدم شبكة مزارة. وهو يوفر وظائف شبكة مزارة لمقدم شبكة NGN آخر (أي مقدم خدمات الشبكة الأصل). وعلاقات الثقة تحكمها اتفاقات مستوى الخدمة (SLA). ويمكن للشبكة المزارة أن تقدم خدمات NGN وأن يكون لها مشتركوها الخاصون بها. وعلاوة على ذلك، قد يكون للشبكة المزارة اتفاقات مع مقدم خدمة تطبيق كطرف ثالث. وبالإضافة إلى ذلك، قد تتصل الشبكة المزارة بالشبكة الأصل عبر شبكة انتقالية وعلاقة الثقة تحكمها اتفاقات مستوى الخدمة (SLA).

3) ميدان الشبكة الأصل: شبكة NGN يستضيفها مقدم خدمات الشبكة الأصل. تقدم الشبكة الأصل خدمات NGN إلى المشتركين فيها. وعلاوة على ذلك، قد يكون لدى الشبكة الأصل اتفاقات مع مقدم خدمة تطبيق كطرف ثالث من خلال سطح تماس بين التطبيق والشبكة (ANI). وعلاقات الثقة بين مقدم خدمات الشبكة المزارة ومقدم خدمات الشبكة الأصل، بما فيها أي طرف ثالث مقدم للخدمات، تحكمها اتفاقات مستوى الخدمة (SLA).

وعلاوة على ذلك، قد تتصل الشبكة الأصل بينياً مع شبكة مزارة أو شبكة أخرى عن طريق شبكة انتقالية، حيث تخضع علاقات الثقة لاتفاقات مستوى الخدمة (SLA).

4) ميدان شبكة الانتقال: شبكة NGN لا تقدم سوى النقل. وعلاقات الثقة بين شبكة النقل والشبكات المجاورة، بما فيها أي طرف ثالث مقدم للخدمات، تحكمها اتفاقات مستوى الخدمة (SLA).

5) ميدان شبكة أخرى: إما مقدم خدمات NGN أو غير مقدم خدمات NGN. وعلاقات الثقة تحكمها اتفاقات مستوى الخدمة (SLA).



الشكل 9 – الاستيقان المتبادل بين الشبكات

1.1.11 الاستيقان في مستوى النقل

كما يبدو في الشكل 9، يتم الاستيقان في مستوى النقل على أساس قفزة قفزة، حيث يكون الاستيقان دائماً مع الشبكة المجاورة في مستوى النقل. وهذا يعني أن الشبكة الأصل لا تحتاج بالضرورة إلى أن تكون لديها اتفاقية مستوى خدمة مع الشبكة الأخرى المبيَّنة في الشكل وإنما تقوم علاقة مستوى النقل بين الشبكة الأصل والشبكة الانتقالية ومن ثم بين الشبكة الانتقالية والشبكة الأخرى.

2.1.11 الاستيقان في مستوى الخدمة/التطبيق

كما يبدو في الشكل 9، يتم الاستيقان في مستوى الخدمة/التطبيق مباشرة بين طبقات التحكم في الخدمة في الشبكة المزارة والشبكة الأصل والشبكة الأخرى، وذلك في مستوى الخدمة/التطبيق بين الأقران. وهذه العلاقة بين الأقران علاقة منطقية وليست مادية. فالمسير المادي رأسي من التحكم في الخدمة إلى النفاذ إلى شبكة في شبكة واحدة ثم يُنقل مباشرة أو عبر شبكة انتقالية ومن ثم رأسياً من الشبكة إلى نفاذ التحكم في الخدمة في شبكة الخدمة/التطبيق المقابلة.

2.11 متطلبات الاستيقان المتبادل بين الشبكات

(R-52) – من المطلوب أن تكون شبكة NGN قادرة على التعرُّف بشكل فريد على الشبكات المجاورة في طبقة النقل.

(R-53) – من المطلوب أن تكون شبكة NGN قادرة على استيقان وترخيص النفاذ من الشبكات المجاورة في طبقة النقل.

(R-54) – من المطلوب أن تكون شبكة NGN قادرة على التعرُّف بشكل فريد على الشبكات المجاورة في طبقة الخدمة/التطبيق.

(R-55) – من المطلوب أن تكون شبكة NGN قادرة على استيقان وترخيص النفاذ من الشبكات المجاورة عند طبقة الخدمة/التطبيق.

(R-56) – من المطلوب من كل مقدم خدمة NGN أن يكون قادراً على تنفيذ سياسات التعرُّف والاستيقان والترخيص المتبادل بين الشبكات (باستعمال اتفاقات طبقة الخدمة (SLA) وعلاقات الثقة مثلاً).

(R-57) – بالنسبة للاتصال بين الشبكات، من المطلوب أن يكون من الممكن التعرُّف بشكل فريد على عناصر الشبكة المعنية، وذلك بمقابلة معرِّفات عناصر الشبكة مع المعرِّفات المرتبطة بمقدم الخدمة NGN الموصولة بينياً.

(R-58) – من المطلوب أن تكون شبكة NGN قادرة على الحماية من النفاذ غير المرخَّص به والتلاعب والتخريب في معلومات الاستيقان والترخيص المتبادل بين الشبكات.

(R-59) – من المطلوب أن تكون شبكة NGN قادرة على الحماية من الهجمات (مثل تكرار الرسائل وإنكار الخدمة) على وظائف ومقدرات الاستيقان والترخيص المتبادل بين الشبكات.

(R-60) – من المطلوب أن تكون شبكة NGN قادرة على تحرّي وتدوين محاولات النفاذ غير المرخَّص بها من شبكات أخرى (مثال ذلك إمكانية تحديد عتبة نظام قابلة للتشكيل لعدد محاولات النفاذ غير المرخَّص به والتي يولّد تجاوزها إنذاراً يدوَّن ويُبلّغ إلى نظام إدارة).

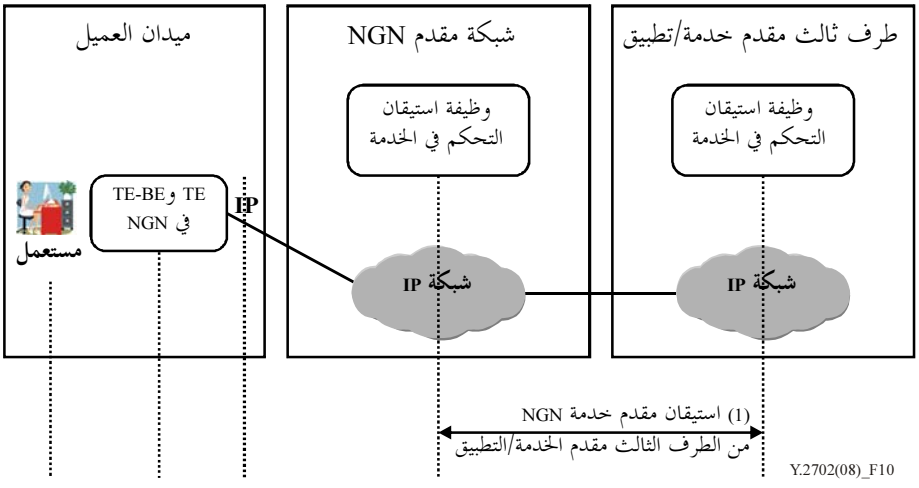
قد يكون من الضروري، رهناً بسياسة مقدم خدمات NGN، القيام باستيقان دوري لمقدم خدمات NGN المجاورة حرصاً على توفير درجة عالية من الكفالة والأمن.

(R-61) – من المطلوب، رهناً بسياسة مقدم خدمات NGN، أن يكون من الممكن دورياً إعادة الاستيقان من مقدم خدمات NGN الموصلة بينياً طوال جلسة أو معاملة الاتصال القائمة.

12 استيقان وترخيص طرف ثالث مقدم للخدمة/التطبيق من قبل مقدم خدمات NGN

1.12 الوصف

قد يكون هنالك بعض السيناريوهات حيث يكون مقدم تطبيق ما أو خدمة ما مختلف عن مقدم خدمات NGN (أي طرف ثالث مقدم خدمة/تطبيق). وفي مثل هذه السيناريوهات، يحتاج مقدم خدمة NGN إلى استيقان وترخيص الطرف الثالث مقدم الخدمة/التطبيق كما هو مبيَّن في الشكل 10.



الشكل 10 – استيقان وترخيص الطرف الثالث مقدم الخدمة/التطبيق

جدير بالملاحظة أن عمليات استيقان المستعملين والشبكات الموصوفة في الفقرات السابقة تحدث ولكنها ليست مبيَّنة في الشكل 10 ولا في النص الوارد أدناه.

2.12 المتطلبات

(R-62) – من المطلوب من طرف ثالث مقدم خدمة/تطبيق أن يكون قادراً على التعريف بنفسه لمقدم خدمة NGN.

(R-63) – من المطلوب من طرف ثالث مقدم خدمة/تطبيق أن يكون قادراً على التعريف بنفسه لدى المستعمل.

(R-64) – من المطلوب أن تكون الشبكة NGN قادرة على التعرُّف بشكل فريد على الأطراف الثالثة من مقدِّمي الخدمات/التطبيقات.

(R-65) – من المطلوب أن تكون شبكة NGN قادرة على استيقان وترخيص أطراف ثالثة من مقدِّمي الخدمات/التطبيقات.

(R-66) – من المطلوب من مقدِّمي خدمات NGN والأطراف الثالثة من مقدِّمي الخدمة/التطبيق تنفيذ السياسات من أجل تعرُّف الهوية والاستيقان والترخيص (مثال ذلك استعمال اتفاقات مستوى الخدمة وعلاقات الثقة).

(R-67) – من المطلوب من مقدِّمي خدمات NGN والأطراف الثالثة من مقدِّمي الخدمة/التطبيق أن يكونوا قادرين على توفير الحماية من النفاذ غير المرخَّص به ومن التلاعب ومن تخريب معلومات الاستيقان والترخيص.

(R-68) – من المطلوب من مقدم خدمة NGN والأطراف الثالثة من مقدِّمي الخدمة/التطبيق أن يكونوا قادرين على توفير الحماية من الهجمات (مثل تكرار الرسائل وإنكار الخدمة) على وظائف ومقدرات الاستيقان والترخيص.

(R-69) – من المطلوب أن تكون شبكة NGN قادرة على تحرّي وتدوين محاولات النفاذ غير المرخَّص به من جانب الأطراف الثالثة من مقدِّمي الخدمة/التطبيق (مثال ذلك نظام عتبة قابل للتشكيل يمكن تحديده بالنسبة لعدد من محاولات النفاذ غير المرخَّص به يتولّد بعده إنذار ويدوَّن ويُبلّغ إلى نظام الإدارة).

قد يكون من الضروري، رهناً بسياسة مقدم خدمة NGN، القيام باستيقان دوري للطرف الثالث مقدم الخدمة/التطبيق وذلك تحقيقاً لدرجة عالية من الكفالة والأمن.

(R-70) – من المطلوب، رهناً بسياسة مقدم الخدمة NGN، أن يكون من الممكن دورياً إعادة استيقان الطرف الثالث مقدم الخدمة/التطبيق طوال فترة جلسة أو معاملة الاتصال القائمة.

13 استخدام طرف ثالث لتوفير خدمة الاستيقان والترخيص

1.13 الوصف

يمكن للأطراف الثالثة من مقدِّمي خدمات الاستيقان والترخيص توفير ما يلي:

- استيقان المستعمل لصالح مقدم خدمة؛
- استيقان مقدم خدمة لصالح مستعمل؛
- استيقان بين مقدِّمي الخدمات؛
- استيقان مقدم خدمة/تطبيق إما من جانب مستعمل أو من جانب مقدم خدمة.

هنالك في هذا الصدد على الأقل ثلاثة كيانات مشاركة عند استخدام طرف ثالث مقدم خدمة استيقان. إذ بالإضافة إلى قيام الطرف الثالث مقدم خدمة الاستيقان بوظيفة أو وظائف خدمة الاستيقان بناء على الطلب، فإن من المطلوب تمكين الاستيقان منه بالذات لدى كل من الطرف الطالب والمطلوب.

2.13 المتطلبات

تنطبق المتطلبات الواردة في الفقرة 2.12 أعلاه.

14 استيقان وترخيص الأشياء

1.14 الوصف

بالإضافة إلى استيقان وترخيص المستعملين وأجهزة المستعملين ومقدِّمي الخدمات، هنالك حاجة إلى استيقان الأشياء عموماً. ويشمل ذلك الأشياء المادية، مثل عناصر أو أنظمة الشبكة وكذلك الأشياء الافتراضية مثل:

- التطبيقات؛
- عملية التطبيق؛
- البرمجيات؛
- رسائل التشوير والإدارة والحامل ومحتوى البيانات.

2.14 المتطلبات

(R-71) – من المطلوب، رهناً بسياسة مقدم خدمات NGN، أن تكون شبكات NGN قادرة على تعرُّف الأشياء بشكل فريد.

(R-72) – من المطلوب، رهناً بسياسة مقدم خدمات NGN، أن تكون شبكات NGN قادرة على استيقان وترخيص الأشياء.

(R-73) – من المطلوب أن تكون شبكة NGN قادرة على تحقق وترخيص امتيازات شيء ما (مثال ذلك تمكين الشيء من أداء إجراء ما أو الضلوع في عملية فقط عندما يكون دوره أو الامتياز الذي يتمتع به يرخِّص له ذلك).

(R-74) – من المطلوب من مقدم خدمات NGN أن يقوم بتنفيذ سياسات تعرُّف الهوية والاستيقان والترخيص للأشياء.

(R-75) – من المطلوب أن تكون شبكة NGN قادرة على توفير حماية السرية والسلامة لتبادلات الرسائل والمعلومات المستخدمة في استيقان وترخيص الأشياء.

(R-76) – من المطلوب من شبكات NGN أن تكون قادرة على توفير الحماية من النفاذ غير المرخَّص به والتلاعب وتخريب معلومات استيقان وترخيص الأشياء.

(R-77) – من المطلوب من شبكات NGN أن تكون قادرة على الحماية من الهجمات (مثل تكرار الرسائل وإنكار الخدمة) على وظائف ومقدرات استيقان وترخيص الأشياء.

(R-78) – من المطلوب أن تكون شبكات NGN قادرة على تحرّي وتدوين محاولات النفاذ غير المرخَّص به من جانب الأشياء (مثال ذلك وضع عتبة نظام قابل للتشكيل لعدد محاولات النفاذ غير المرخَّص به والذي يتولّد بعده إنذار ويدوَّن ويُبلّغ إلى نظام إدارة).

(R-79) – من المطلوب من شبكة NGN أن تكون قادرة على تحرّي وتدوين محاولات الامتياز غير المرخَّص بها (مثال ذلك إجراءات مستعمِل غير مرخَّص بها).

قد يكون من الضروري، رهناً بسياسة مقدم خدمات NGN، القيام دورياً باستيقان مقدم خدمات NGN مجاورة وذلك تحقيقاً لدرجة عالية من الكفالة والأمن.

(R-80) – من المطلوب، رهناً بسياسة مقدم خدمات NGN، أن يكون من الممكن دورياً إعادة استيقان الأشياء المعنية طوال الفترة ذات الصلة لجلسة أو معاملة الاتصال المقامة.

التذييل I

حالة استعمال SAML

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I استخدام [b-ITU-T X.1141]، لغة ترميز تأكيد الأمن (SAML 2.0)

يوفر هذا التذييل مثالاً لحالات استعمال لنقل نتائج الاستيقان والعمل في الوقت ذاته على توفير لغة الترميز SAML من أجل الخصوصية في استيقان الخدمة/التطبيق.

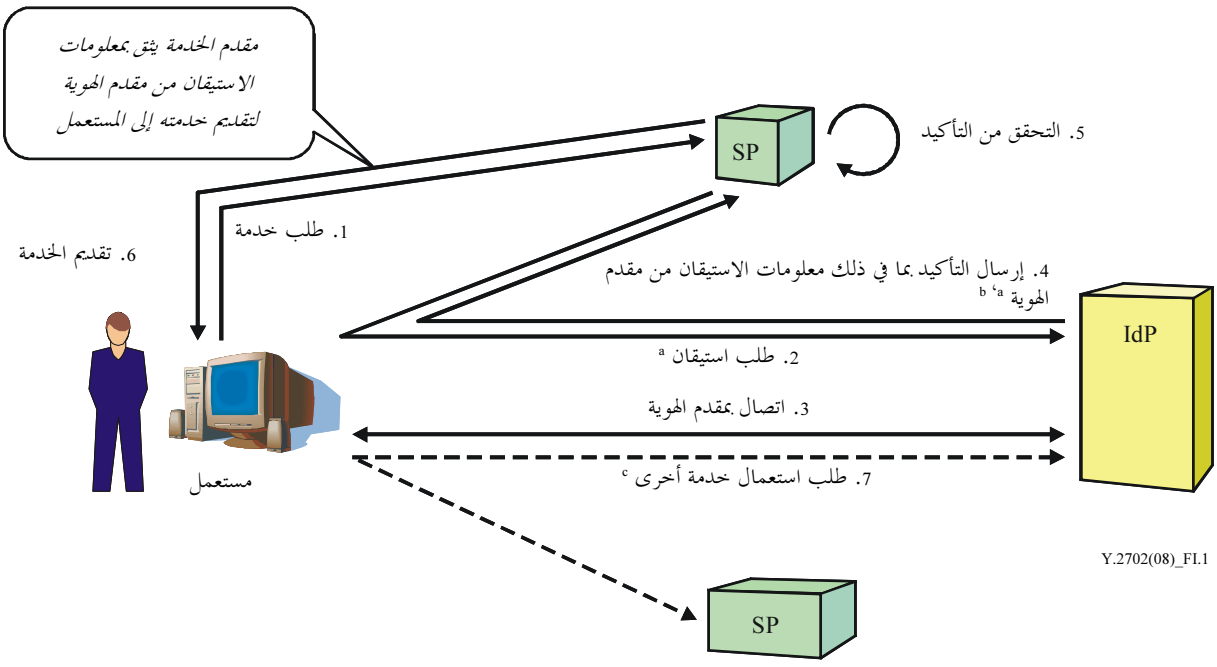
2.I إجراءات استيقان الخدمة/التطبيق

يمكن استعمال لغة ترميز تأكيد الأمن (SAML 2.0) عند استيقان النتائج الواجب تبادلها بين الخدمات الموثوقة و/أو التطبيقات التي قد تكون أطراف ثالثة من مقدِّمي الخدمات. والبرمجية SAML 2.0 عبارة عن مواصفة مفتوحة مقيَّسة من جانب منظمة النهوض بالمعايير القياسية للمعلومات المنظمة هيكلياً (OASIS). ويمكن استعمال اللغة SAML على وجه التحديد في الحالتين التاليتين:

- استيقان وحيد: عندما تسمح مختلف الخدمات والتطبيقات لمستعمليها بعملية استيقان وحيدة تيسيراً على المستعملين دون تبادل جميع معلومات المستعملين فيما بينها.
- جمع الحسابات: عندما تعمد خدمات وتطبيقات مختلفة إلى ربط حساباتها من أجل المستعمل ذاته.

3.I استيقان الخدمة/التطبيق – أمثلة تدفق النداء

يبيِّن الشكل 1.I مثالاً نموذجياً لعملية استيقان وحيدة وتوحيد حسابات باستعمال البرمجية SAML 2.0.



a 2 و4 تمثلان اتصال حاصل (إعادة توجيه HTTP مثلاً) عن طريق وكيل مستعمل (متصفح ويب مثلاً)

b يمكن أن يحتوي التأكيد معلومات نعوت وقرار ترخيص إذا اقتضى الأمر

c التدفق ذاته كما من 1 إلى 6، باستثناء الاتصال بمقدم الهوية. (بعبارة أخرى، يكفي أن يتصل المستعمل بمقدم الهوية مرة واحدة ليكون مستيقناً).

الشكل 1.I – مثال تدفق نداء خدمة استيقان وحيد (SSO) باستعمال البرمجية SAML 2.0

تحدد [b-ITU-T X.1141] البنود الواردة في الشكل 1.I كما يلي:

- مقدم الهوية (IdP)

نوع من مقدِّمي الخدمة يقوم باستحداث معلومات الهوية والحفاظ عليها وإدارتها من أجل الكيانات الأساس ويوفر استيقان الكيان الأساس لمقدِّمي الخدمة الآخرين ضمن اتحاد، مثلما هو الحال في جانبيات متصفح الويب.

- مقدم الخدمة

دور يضطلع به كيان نظام حيث يوفر كيان النظام الخدمات إلى الكيانات الأساس أو إلى كيانات نظام أخرى.

- التأكيد

بيانات تقدمها سلطة البرمجية SAML إما بشأن عمل استيقان تم بشأن موضوع ما أو معلومات نعت بشأن الموضوع أو بيانات ترخيص تنطبق على الموضوع فيما يتعلق بمورد محدد.

4.I أمن إجراءات وآليات استيقان الخدمة/التطبيق

تتسم اللغة SAML 2.0 في حد ذاتها بمزايا، من قبيل الاتحاد المُغْفل والأسماء المستعارة، لحماية الأمن والخصوصية على حد سواء. ويوفر الاتحاد المغفل اسم هوية مؤقت لمقدم الخدمة. وتمكّن الأسماء المستعارة المستعملين من التعريف بأنفسهم لدى مقدم خدمة أثناء الاستيقان الوحيد لدى استعمال أسماء مستعارة في شكل أزواج بحيث تحافظ على الخصوصية وتمكّن في الوقت نفسه من الحفاظ على علاقة مستمرة مع المستعمل. وتمكّن اللغة SAML 2.0 من تجفير بيانات النعوت ومعرِّفات الأسماء أو تأكيدات بأكملها. وتضمن هذه الميزة إمكانية الحفاظ على سرية هذه العناصر من طرف إلى طرف حسبما تدعو الحاجة.

التذييل II

استيقان وترخيص خدمة اتصالات الطوارئ (ETS)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II لمحة عامة

لقد وضعت البلدان، أو هي تسعى إلى وضع، خدمة اتصالات طوارئ (ETS). وتنفيذ هذه الخدمة (ETS) مسألة وطنية حكماً. ولكن حالات الكوارث/الطوارئ قد تتجاوز الحدود الجغرافية، ومن ثم هنالك احتمال أن تدخل البلدان/الإدارات في اتفاقات ثنائية و/أو متعددة الأطراف لربط ما لديها من أنظمة ETS. ويقدم المرجع [b-ITU-T E.107] الإرشادات التي تمكّن من الاتصالات بين تنفيذ خدمة وطنية لاتصالات الطوارئ وخدمة أو خدمات أخرى.

والمطلوب من مقدِّمي خدمات NGN تمكين النفاذ لمستعملي الخدمة ETS المرخَّص لهم بذلك فقط. وينبغي منع النفاذ غير المرخَّص به للمقتحمين مثلاً الذين يتنكرون في هيئة مستعملين مرخَّص لهم. ولذلك من المهم لأمن الخدمة ETS توفر الآليات والمقدرات لاستيقان وترخيص النفاذ من جانب مستعمل الخدمة ETS أو من جانب جهاز أو من مجموع المستعمل والجهاز حسب مقتضى الحال اعتماداً على السياسة[3] ومستوى الكفالة للخدمة المعيَّنة (مثال ذلك الصوت والبيانات والفيديو).

وفي مجال التوصيلات بين المشاريع التنفيذية لخدمة ETS، يتعيَّن على مقدِّمي خدمات NGN الاعتماد بعضهم على الآخر لاستيقان وترخيص مستعملي الخدمة ETS من خلال اتفاقات مستوى الخدمة. وهنالك مناهج متعددة لعمليات استيقان وترخيص خدمة ETS. ويوفر هذا التذييل معلومات عن أمثلة مناهج لاستيقان وترخيص خدمة ETS بما فيها بعض أمثلة تدفق النداء.

2.II استيقان وترخيص مستعمل الخدمة ETS

إن كيفية استيقان وترخيص مستعملي خدمة الطوارئ ETS مسألة وطنية. إذ يعمد مقدم خدمات NGN عموماً إلى استيقان وترخيص طلب نداء/جلسة من مستعمل خدمة ETS اعتماداً على طريقة التسجيل وعلى كيفية تفعيل الخدمة. وقد يكون الاستيقان على أساس نداء/جلسة أو على أساس استيقان وحيد المرة (محدود زمنياً) ينطبق على النفاذ الجاري لمستعمل النظام ETS أو على أساس اشتراك. وينبغي لمقدِّمي خدمات NGN المسارعة إلى استيقان وترخيص مستعملي خدمات الطوارئ في وقت مبكر من عملية إقامة النداء/الجلسة. ويجب استخدام آليات وطرائق محددة لعملية الاستيقان والترخيص اعتماداً على السياسة المعمول بها (مثال ذلك استعمال رقم تعرُّف هوية شخصي (PIN) وجانبيات المستعمل والاشتراك). وحالما يتم استيقان وترخيص المستعمل، أو جهاز المستعمل أو مجموع المستعمل والجهاز اعتماداً على السياسة المعمول بها، يجري ترميز النداء/الجلسة ETS وتبلّغ الشبكات اللاحقة بذلك، ويمكن أيضاً بيان درجة أولوية مستعمل الخدمة ETS. وعلاوة على ذلك، وحالما تتم عملية الاستيقان والترخيص، تعطى الأولوية إلى جميع جوانب النداء/الجلسة ETS وعملية التشوير/التحكم والحركة الحاملة وأي عملية إدارة معمول بها.

ومن أمثلة استيقان وترخيص خدمة اتصالات الطوارئ ETS ما يلي:

أ) استعمال رقم تعرُّف الهوية الشخصي (PIN): يستخدم هذا النهج الرقم PIN لاستيقان وترخيص المستعمل. ونتعرف في هذا النهج هوية المستعمل وليس جهاز المستعمل. ولذلك فهو يُستعمل عادة في الحالات التي يمكن فيها للمستعمل تفعيل الخدمة ETS من أي جهاز.

[3] **ملاحظة:** تشمل كلمة السياسة في هذا السياق جميع السياسات السارية مثل قواعد وأنظمة مقدِّمي شبكات NGN وقواعد وأنظمة الهيئات التنظيمية والحكومات.

ب) استعمال جانبية الاشتراك/الخدمة: تُستخدم في هذا النهج جانبية خدمة مطراف المستعمل للدلالة على الاشتراك في الخدمة ETS. ويجري استيقان مطراف المستعمل والتعرُّف إلى جانبية خدمة المستعمل كجزء من إجراءات التسجيل المعتادة لدى مقدم خدمة NGN (أي مقدم خدمة ETS). وعندما يبادر المستعمل بطلب، فإن التحقق من جانبية خدمة المستعمل يحدد ما إذا كان المستعمل مرخَّص له باستعمال الخدمة ETS أم لا. وبالتالي يلبَّى طلب الخدمة ETS إذا تأكدت صحة اشتراك الخدمة ETS من جانب مطراف المستعمل.

ج) استعمال مجموع الرقم PIN وجانبية الخدمة: يمكن أيضاً استخدام نهج الجمع بين الرقم PIN وجانبية الخدمة لاستيقان كل من المستعمل وجهاز المستعمل بغية توفير قدر أعلى من الكفالة.

د) استعمال علامات أمن خاصة وقياسات حيوية: إضافة إلى النُهج الموصوفة أعلاه، يمكن استعمال نُهج أكثر تطوراً باستعمال علامات الأمن الخاصة بمقدرات القياس الحيوي لاستيقان وترخيص مستعملي الخدمة ETS وذلك بغية توفير مستوى أعلى من كفالة تحقق الهوية.

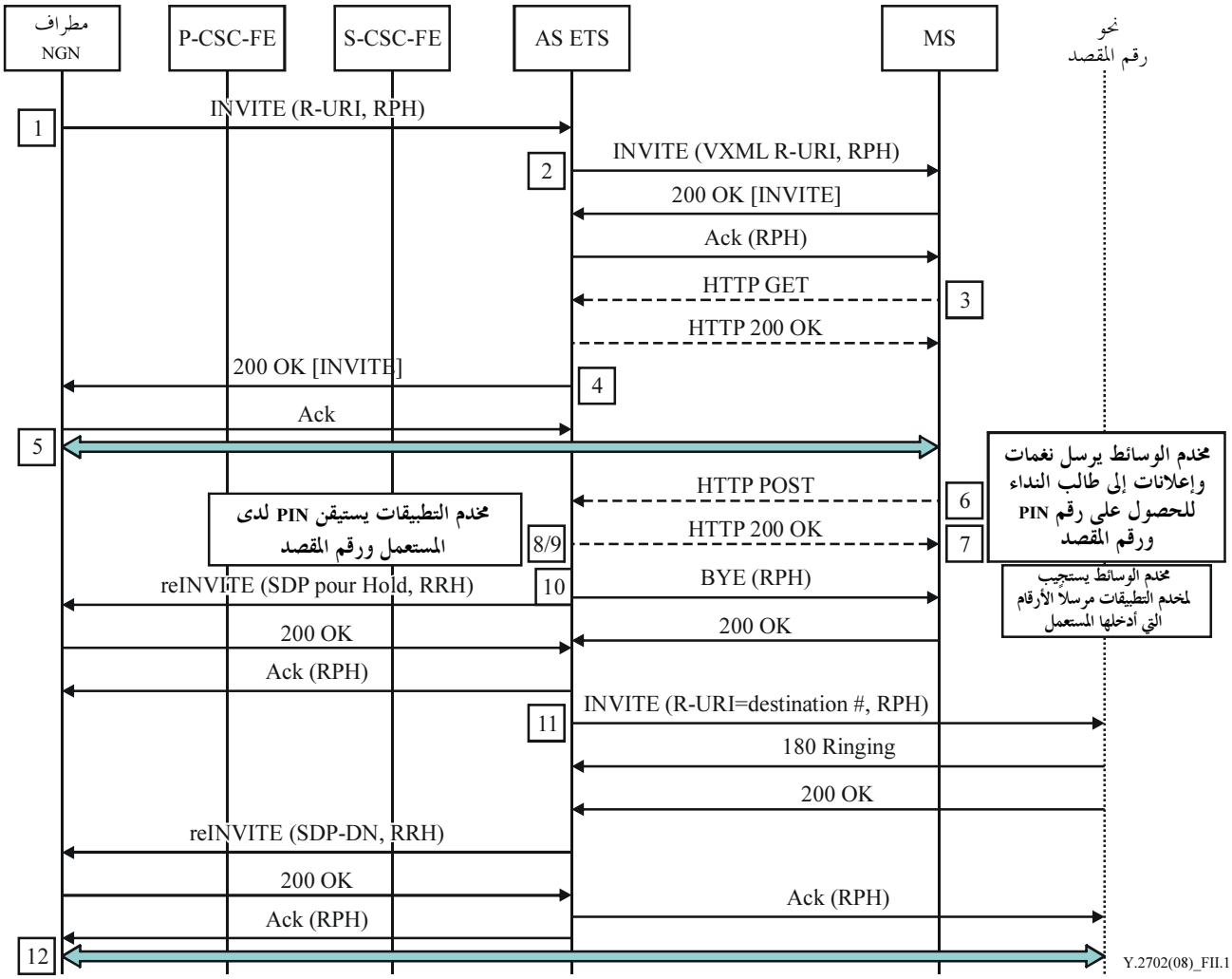
3.II استيقان وترخيص مقدم خدمة NGN من أجل خدمة اتصالات الطوارئ (ETS)

يتعيَّن أيضاً مراعاة الاستيقان والترخيص عند تسليم واستلام حركة ETS بين مقدِّمي خدمة NGN، على أن يؤخذ في الحسبان بيئة تعدد المقدمين والفصل بين التحكم في الخدمة والنقل. ومن الضروري أيضاً بالنسبة إلى أمن ETS إجراء عملية استيقان وترخيص مقدِّمي خدمة NGN لتسليم واستلام نداءات/جلسات ETS والحركة اعتماداً على اتفاقات مستوى الخدمة والسياسة المعمول بها.

4.II أمثلة لحالات استيقان وترخيص الخدمة ETS

1.4.II مثال حالة استيقان وترخيص أساسية تعتمد رقم تعرف الهوية الشخصي (PIN)

يبيِّن الشكل 1.II مثالاً أساسياً لاستيقان وترخيص الخدمة ETS يتناول استعمال رقم تعرُّف الهوية الشخصي (PIN).



الشكل II.1 – الاستيقان والترخيص على أساس PIN

يفترض هذا المثال أن مستعمل الخدمة ETS يطلب مباشرة نداء/جلسة ETS بالتقدم بطلب نداء/جلسة إلى رقم ETS. وعلاوة على ذلك، فإن جميع بروتوكولات استهلال الجلسة (SIP) تتضمن رأسية لأولوية المورد (RPH) [RFC 4412] للدلالة على طلب معاملة ذات أولوية.

1) يُسيَّر النداء/الجلسة إلى مخدم التطبيقات (AS) ETS حيث تُستهل عملية استيقان المستعمل.

2) يُرسل مخدم التطبيقات رسالة INVITE إلى مخدم الوسائط (MS) المختار مشفوعة بعرض لبروتوكول وصف الجلسة (SDP) مرتبط بجهة النداء. وتحتوي رسالة INVITE على محدد موقع الموارد الموحد (URL) لمكتوب VoiceXML مخزَّن في مخدم التطبيقات. ويصف المكتوب كيف ينبغي لمخدم الوسائط (MS) أن يتفاعل مع جهة النداء (ما هو الإعلان الواجب إرساله وكيف يكون جمع الأرقام وكم عددها وما هي المؤقتات بين الأرقام وغير ذلك).

3) عند استلام رسالة INVITE يقوم المخدم MS بما يلي:

- قد يرسل 100 Trying إلى المخدم AS؛
- يستقي المكتوب VoiceXML مباشرة من المخدم AS باستعمال HTTP وURL في رسالة INVITE. (يرسل المخدم MS رسالة HTTP GET إلى المخدم AS ويعاد مكتوب VoiceXML من المخدم AS في شكل HTTP 200 OK)؛
- تؤكَّد صلاحية المكتوب؛

- تصاغ وتُرسل رسالة 200 OK تحتوي البروتوكول SDP الخاص بها إلى المخدم AS.

4) يرسل المخدم AS رسالة 200 OK إلى الجهة طالبة النداء (مطراف NGN) تتضمن معلومات الجلسة التي تلقّاها من المخدم MS.

5) عند هذه النقطة يتاح توصيل الوسائط بين المخدم MS والجهة طالبة النداء.

6) لدى استلام رسالة ACK ومكتوب VXML في شكل HTTP 200 OK، يُنفِّذ المخدم MS المكتوب VoiceXML. ويرسل نغمة ويجمع أرقام PIN التي أدخلتها الجهة طالبة النداء.

7) يرسل المخدم MS الأرقام المجموعة مباشرة إلى المخدم AS باستعمال رسالة HTTP POST.

8) لدى استلام الأرقام المجمعة، يتحقق المخدم AS مما إذا كانت الأرقام PIN المستلمة صحيحة.

- إذا كانت الأرقام المتلقاة غير صحيحة (عدد الأرقام المتلقاة أو الرقم خاطئ)، يقرر المخدم AS أن المزيد من التفاعل مع صاحب النداء مطلوب. يعيد المخدم AS الرسالة HTTP 200 OK إلى المخدم MS مع مكتوب VoiceXML جديد.
- يقرر المخدم AS المعاملة النهائية. إذا كانت الأرقام المتلقاة صحيحة يأمر المخدم AS المخدم MS بإرسال النداء لجمع الأرقام (رقم المقصد).

9) يقرر المخدم AS أن صاحب النداء أدخل أرقام المقصد الصحيحة.

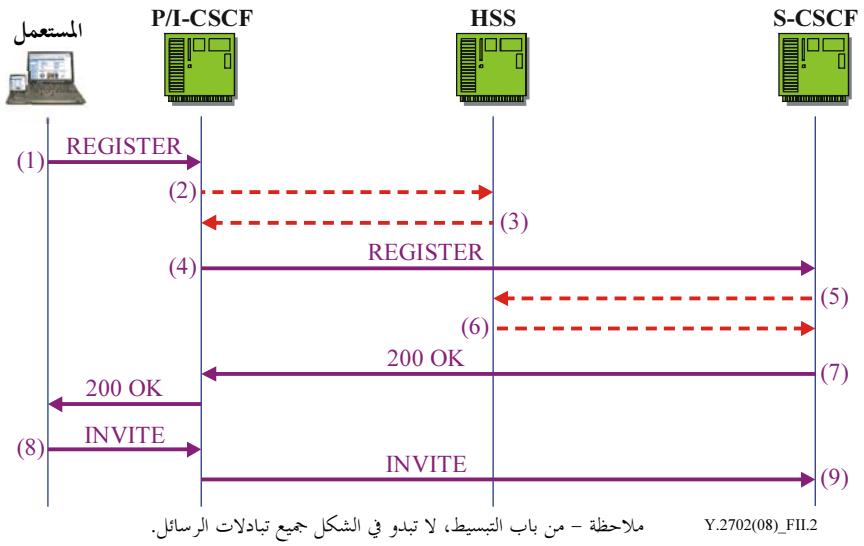
10) يحرِّر المخدم AS المخدم MS من النداء/الجلسة برسالة SIP BYE، ويرسل رسالة reINVITE إلى صاحب النداء مع بروتوكول SDP لوضع الوسائط في حالة تأهب.

11) يرسل المخدم AS رسالة INVITE إلى الطرف المقصود. ولدى تلقي رسالة 200 OK (رد)، يرسل المخدم AS رسالة reINVITE مع بروتوكول SDP مرتبط بالمقصد إلى الطرف صاحب النداء.

12) يقام مسير الوسائط بين الطرف صاحب النداء والرقم المقصود مشفوعاً باستيقان المخدم AS في مسير التحكم في النداء.

2.4.II مثال لاستعمال استيقان وترخيص جانبية الاشتراك/الخدمة

يبيِّن الشكل 2.II مثال حالة حيث تُستعمل جانبية الاشتراك/الخدمة لاستيقان وترخيص الخدمة ETS.



الشكل 2.II – مثال يقوم على أساس الاشتراك

يعتمد هذا المثال على جانبية الاشتراك/الخدمة المرتبطة بجهاز المستعمل. وتضطلع الشبكة بعملية التسجيل والاستيقان المعتادة لجهاز المستعمل. وعندما يطلب المستعمل نداء/جلسة ETS، يجري التحقق من جانبية الخدمة/الاشتراك لمعرفة ما إذا كان جهاز المستعمل مرخَّص له باستعمال نداء/جلسة ETS أم لا. ويكون تدفق النداء على النحو التالي:

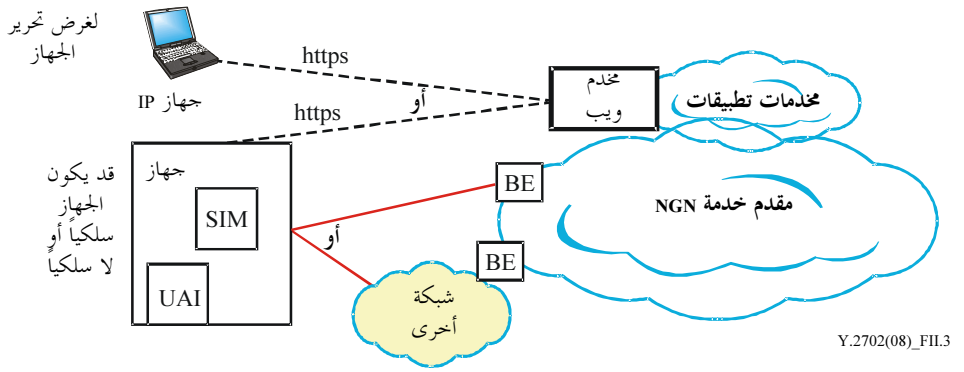
1) استهلال التسجيل
2) وظيفة التحكم P/I-CSCF تستفسر من نظام المشترك المحلي HSS
3) يتحقق النظام HSS من اشتراك المستعمل ويقدم هوية للوظيفة S/CSCF
4) ترسل الوظيفة P/I-CSCF رسالة تسجيل إلى الوظيفة S-CSCF
5) تستفسر الوظيفة S-CSCF من النظام HSS
6) يقدم النظام HSS معلومات جانبية خدمة المستعمل (قد يتناول التفاعل مع مخدم التطبيقات AS)
7) ترسل الوظيفة S-CSCF رسالة OK 200
8) يستهل المستعمل جلسة الخدمة ETS
9) تتحقق الوظيفة S-CSCF من جانبية الخدمة لتقرير ما إذا كانت جلسة ETS مرخَّصاً بها أم لا.

3.4.II مثال استيقان وترخيص مجموع المستعمل والجهاز

يبيِّن الشكل 3.II مثالاً يتناول جهاز مستعمل مزوَّد ببطاقة SIM ترتبط بالشبكة باستعمال معمارية إنهاض نوعية (GBA) 3GPP المعيارية.

وفي هذا المثال، يكون الجهاز مزوَّداً بسطح بيني لتطبيق المستعمل (UAI) يمكّن المستعمل من توفير معلومات الاستيقان عبر الجهاز إلى طبقة التطبيق لشبكة مقدم الخدمة. وقد يكون السطح البيني UAI ببساطة استعمال لوحة مفاتيح أو بتعقيد عملية قياسات حيوية.

ويُفترض وجود اتصالات آمنة من أجل التشوير والوسائط.



SIM وحدة تعرف هوية المشترك
UAI سطح تماس استيقان المستعمل

الشكل 3.II – استيقان وترخيص مستعمل الخدمة ETS

تدفق النداء/الدورة:

1) يدار جهاز المستعمل.
2) يربط الجهاز بشكل آمن بالشبكة باستعمال المعمارية 3GPP GBA.

3) يستهل مستعمل الخدمة ETS الاستيقان المحلي بوحدة SIM على الجهاز باستعمال السطح البيني UAI. وقد يكون هذا السطح لوحة مفاتيح حيث يُدخل الرقم PIN أو نوعاً ما من أنواع القياس الحيوي.

أ) تستيقن الوحدة SIM مستعمل الخدمة ETS وتشير إلى نجاح العملية. تُعلِم وحدة SIM مخدم التطبيق AS باستيقان مستعمل الخدمة ETS.

ب) ويمكن خلاف ذلك ترحيل المعلومات بشكل آمن إلى طبقة التطبيق في شبكة مقدم الخدمة.

4) في هذا الوقت يتم استيقان المستعمل "العادي" والجهاز لدى الشبكة. ويقوم المخدم AS باستيقان المستعمل في دوره كمستعمل ETS.

إذا فشل استيقان المستعمل محلياً بعد x محاولة، ينبغي عندئذٍ إقفال الجهاز إزاءه. وثمة مثال لنهج يؤدي إلى تحرير الجهاز وهو أن ينفذ المستعمل إلى سطح بيني GUI عبر سطح بيني AS/WS، ويُدخل رقم PIN لإثبات الصلاحية. وإذا صح التحقق من هوية المستعمل، يُرسل المخدم AS/WS رسالة إلى الجهاز يطلب فيها تحرير الجهاز من الإقفال.

4.4.II مثال حالة استعمال موقع المؤسسة

قد تصدر نداءات ETS عن مواقع مؤسسات حكومية أو تنتهي عندها. وتكون الحالة عموماً كما يلي:

- وجود مرافق مكرّسة بين موقع المؤسسة ومقدم الخدمة.
- يتسجل المستعمل لدى موقع المؤسسة وليس لدى مقدم الخدمة.
- يتسجل موقع المؤسسة باستعمال بطاقة عمومية أو باستعمال وظيفة تشغيل بيني IWF (مثال ذلك مراقب حدود الجلسة (SBC)) عند طرف شبكة مقدم الخدمة ويقوم بتسجيل بديل نيابة عن المؤسسة.

وهكذا إذا كان المطلوب استيقان يتعدى الاستيقان القائم على أساس الرقم PIN، عندئذٍ يحتاج الأمر إلى القيام بوظائف إضافية. وقد تشمل هذه الوظائف مثلاً ما يلي:

- تُعلِم المؤسسة مقدم الخدمة بوجود المستعمل. وتضيف هذه البيانات إلى كفالة الاستيقان.
- تحيل المؤسسة علامة آمنة إلى مقدم الخدمة لتحديد هذه العلامة بمثابة نداء/جلسة ETS محتملة عند الطبقة 2/3 (مثال ذلك توسيع العلامة الآمنة في بروتوكول حجز الموارد RSVP).

تكون كفالة الاستيقان مع بيانات من موارد متعددة مطلوبة تبعاً للمستعمل.

التذييل III

معمارية إنهاض نوعية (GBA) من معيار 3GPP

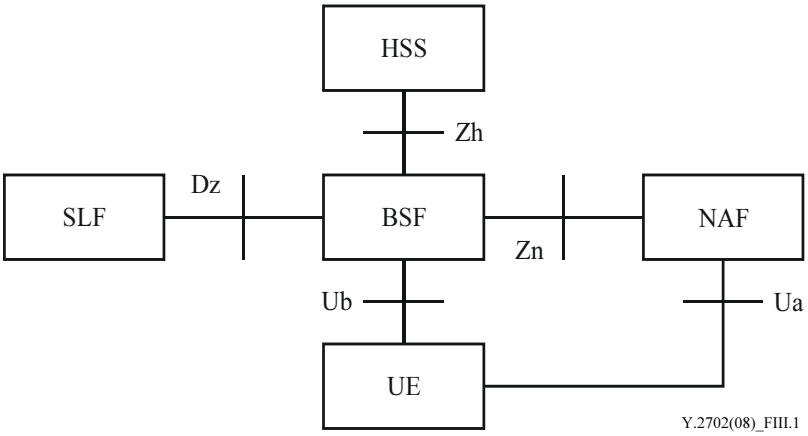
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

تحدد معمارية الإنهاض النوعية (GBA) إجراءات الإنهاض المستقلة عن النفاذ. وهي توفر إطاراً للاستيقان المتبادل للمستعملين النهائيين ولوظيفة تطبيق الشبكة (NAF).

والمعمارية GBA عبارة عن نظام استيقان يضم ثلاثة أطراف:

- مستعمل نهائي يسعى إلى الحصول على خدمات شبكة باستعمال تجهيزات مستعمل (UE)
- مخدم تطبيق (يدعى وظيفة تطبيق الشبكة NAF)
- كيان موثوق به (يدعى وظيفة مخدم إنهاض BSF) يشارك في عملية الاستيقان وتبادل المفاتيح بين الكيانين الآخرين.

ويبيِّن النموذج المرجعي أساسيات عملية الاستيقان بواسطة المعمارية GBA الموصوفة أدناه.



الشكل III.1 – نموذج شبكة بسيط لعملية الإنهاض مقتطف من المعيار [b-ETSI TS 133 220]

وفيما يلي الخطوات الأساسية في إجراءات المعمارية GBA:

1) تطلب الوظيفة NAF الاستيقان وتفاوض استعمال المعمارية GBA عبر النقطة المرجعية Ua.

2) يستهل عميل الوظيفة BSF الذي يجري على تجهيزات المستعمل (UE) إجراءات الإنهاض عبر النقطة المرجعية Ub. وتستجلب الوظيفة BSF معلومات الاستيقان ومعلَمات أمن مستعمل المعمارية GBA من النظام HSS عبر النقطة Zh. وتجري عملية الاستيقان المتبادل بين UE وBSF باستعمال مجموعة AKA في بروتوكول HTTP. وينتهي الإجراء بأن تتلقى التجهيزات UE معرِّف معاملة الإنهاض (B-TID) من الوظيفة BSF وبأن يوضع مفتاح متقاسم (Ks) بين التجهيزات UE والوظيفة BSF.

3) تستقي التجهيزات UE المفتاح المتقاسم Ks_NAF من المفتاح Ks وترسل المعرِّف B-TID (إلى جانب البيانات الخاصة بالتطبيق) إلى الوظيفة NAF.

4) ترسل الوظيفة NAF المعرِّف B-TID إلى الوظيفة BSF عبر النقطة المرجعية Zn.

5) تحدد الوظيفة BSF القائمة على أساس المعرِّف B-TID المفتاح Ks الذي ينبغي استعماله وتستقي منه المفتاح Ks_NAF وترسله إلى الوظيفة NAF.

6) وأخيراً يمكن لكل من التجهيزات UE والوظيفة NAF استيقان الكيان الآخر باستعمال المفتاح المتقاسم Ks_NAF. ويتوقف الإجراء الدقيق للاستيقان على البروتوكول القائم بين التجهيزات UE والوظيفة NAF.

فالمعمارية GBA تحدد مثلاً أن بإمكان التطبيقات القائمة على أساس بروتوكول HTTP إما أن تستعمل استيقان مجموعة HTTP [المعيار b-IETF RFC 2617] أو طواقم شفرات مفاتيح أمن طبقة النقل المتقاسمة سلفاً [المعيار b-IETF RFC 4279].

ملاحظة – تستفسر الوظيفة BSF الوظيفة SLF عبر النقطة المرجعية Dz للحصول على اسم النظام HSS الذي يحتوي البيانات الخاصة بالمشترك. ولا حاجة إلى الوظيفة SLF عندما تكون الوظيفة BSF مشكَّلة لاستعمال نظام HSS محدد سلفاً.

ومقابلة كيانات المعمارية GBA مع كيانات الشبكات NGN محددة في التوصية [ITU-T Y.2012].

- الوظيفة NAF تقابل كيان *التطبيقات* في الشكل 3 في التوصية [ITU-T Y.2012].
- الوظيفة BSF يمكن إدراجها في الكيانات الوظيفية T-11 للاستيقان والترخيص. أي من الممكن زيادة T-11 وتمكينها بمقدرات مخدم الوظيفة BSF.
- النظام HSS يقابل الكيانات الوظيفية في جانبية مستعمل الخدمة S-5.
- الوظيفة SLF تقابل الكيانات الوظيفية لمحدد موقع الاشتراك S-4.
- التجهيزات UE تقابل وظيفة المستعمل النهائي.

التذييل IV

أمثلة تدفق نداء إدارة الهوية (IdM)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.IV لمحة عامة

أمثلة التدفق في هذا التذييل مستقاة من المرجع [b-TR 33.980].

وتوفر هذه التدفقات تفاصيل طرائق تشغيل بيني ممكنة بين الصيغة 2.0 من لغة ترميز تأكيد الأمن SAML v2.0 (أو بديلاً من ذلك إطار اتحاد الهويات Liberty Alliance، ID-FF) وإطار هويات خدمات الويب (ID-WSF) ولغة ترميز تأكيد الأمن (SAML) ومكون معمارية الإنهاض النوعية (GBA). وهذا التذييل من قبيل الإعلام ولا ينطبق إلا إذا استُعمِل الإطار ID-WSF والمعمارية GBA أو البرمجية SAML v2.0 والمعمارية GBA مجتمعين.

2.IV أمثلة تدفق النداء

لا تنطبق هذه التدفقات إلا باستعمال إطار Liberty Alliance والمعمارية GBA أو البرمجية SAML v2.0 والمعمارية GBA مجتمعين.

1.2.IV سيناريو الاستيقان الوحيد SSO: ID-FF مع تحويل <lib:AuthnResponse>

1.1.2.IV بروتوكول HTTPS مع أمن طبقة النقل TLS التقليدي

في هذا السيناريو لا تدرك تجهيزات المستعمل UE البروتوكول LAP. وجميع عناصر البروتوكول مأخوذة من إطار اتحاد الهويات [b-ID-FF] ومستكمَلة بتفاصيل محددة بمعمارية GAA مأخوذة من [b-TS 33.222]. تحدَّد أولاً الخطوات اللازمة عند استعمال بروتوكول HTTPS ونشر أمن طبقة النقل TLS [b-IETF RFC 2246] التقليدي تبعاً للمعيار [b-TS 33.222]، الفقرة 3.5:

1) تتصل التجهيزات UE بمقدم الخدمة SP للنفاذ إلى خدمة يوفرها SP بإرسال طلب HTTP. ويحتوي هذا الطلب إشارة دعم استيقان قائمة على أساس GBA (قارن مع الخطوة 3) حيث ذلك مطلوب لإعادة توجيه الطلب تبعاً للخطوة 3.

2) لدى استلام طلب HTTP من التجهيزات UE يحصل SP على عنوان مقدم الهوية ويرسل إلى التجهيزات UE استجابة HTTP محوّلة مع <lib:AuthnRequest>. ويعتمد أسلوب الحصول على عنوان مقدم الهوية على التنفيذ وهو من شأن مقدم الخدمة.

3) تتصل التجهيزات UE بدورها بمقدم الهوية IdP بموجب URL الوارد في ميدان رأسية الموقع ويتعيَّن على UE النفاذ إلى NAF/IdP URL مع طلب HTTP ومعلومات <lib:AuthnRequest> [b-ID-FF bindings].

تبيِّن التجهيزات UE للوظيفة NAF/IdP أن الاستيقان القائم على أساس GBA مدعوم بإضافة متوالية ثابتة إلى رأسية HTTP لدى "User-Agent" كعلامة منتج كما هو محدد في المعيار [b-IETF RFC 2616]. وتحدَّد هذه المتوالية الثابتة تبعاً للخطوة 2 في الفقرة 3.5 من المواصفة [b-TS 33.222].

إذا كان هنالك ترابط أمن إنهاض بين التجهيزات UE ومقدم الهوية IdP عندئذٍ تتقاسم التجهيزات UE والوظيفة IdP/NAF المفاتيح لحماية النقطة المرجعية Ua ويكون لدى UE جميع البيانات اللازمة لأداء استيقان موجز HTTP من الرسائل السابقة. وفي هذه الحالة تُجمع الخطوة 3 مع الطلب في الخطوة 5 وتُحذف الخطوة 4.

4) بما أن مقدم الهوية IdP يشارك مكان الوظيفة NAF، فإن استيقان موجز HTTP يجري وفقاً للبروتوكول [b- TS 33.222] واستجابة HTTP بوضع غير مرخَّص به ويرسَل ميدان رأسية WWW-Authenticate إلى التجهيزات UE. وطريقة هذا الاستيقان وتفاصيله معرَّفة في المواصفة [b-TS 33.222] وليس في [b-ID-FF].

إذا لم تكن UE تحتوي على جلسة إنهاض صالحة أو لم تكن حداثة مواد المفتاح كافية لمقدم الهوية IdP، عندئذٍ تقوم UE بإجراءات إنهاض جديدة مع الوظيفة BSF. وهذا الإجراء شفاف إزاء مقدم الخدمة SP.

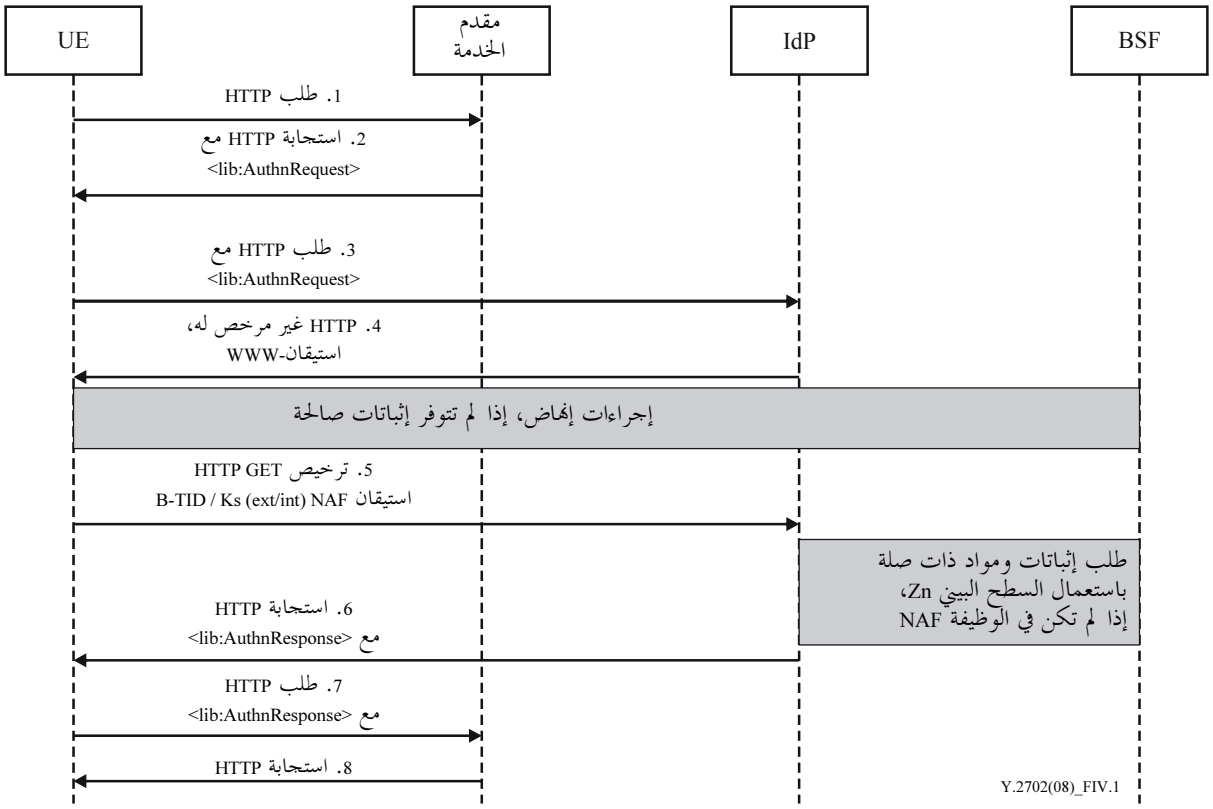
5) تعيد UE بيانات الاستيقان مستعمِلة B-TID كاسم مستعمِل وKs_(ext/int)_NAF ككلمة سر لمقدم الهوية IdP. وقد تشتمل UE على المزيد من بيانات المستعمل المتصلة بالبروتوكول LAP.

إذا كان IdP يشارك المكان مع NAF، عندئذٍ يحدث ذلك كما هو مبيَّن في [b-TS 33.222]. وقد تحتوي USS معلومات خاصة بمؤسسة Liberty.

6) يُعالَج الطلب <lib:AuthnRequest>. ويستجيب IdP برد <lib:AuthnResponse> في الاستجابة HTTP المحوّلة إلى URL [b-ID-FF bindings]. وقد يحتوي IdP على مزيد من البيانات المتصلة بالبروتوكول LAP.

7) تتصل UE بمقدم الخدمة SP ثانية باستعمال هذا المحدد URL وطلب HTTP مع <lib:AuthnResponse>.

8) يردّ مقدم الخدمة باستجابة HTTP.



الشكل IV.1 – تدفق الرسائل من أجل استيقان وحيد SSO مع <lib:AuthnResponse> وأمن طبقة النقل TLS التقليدي مع معمارية GBA

الملاحظة 1 – بما أن IdP يشارك المكان مع NAF، أي أن Ua مختارة للاستيقان كما هو وارد في المواصفة [b-TS 33.222]، فإن كل طلب عبر Ua يجري استيقانه في حد ذاته، إذ إن كل طلب يحمل رأسية الاستيقان كاملة. ولا فرق هنالك بين الطلب الأول وطلبات المتابعة.

الملاحظة 2 – تحدد المواصفة LAP ID-FF [b-ID-FF] أيضاً اتصالاً على أساس POST بين التجهيزات UE ومقدم الهوية IdP إلى جانب طلب قائم على GET مع متوالية استفسار. وهذا متوافق مع المواصفة [b- TS 33.222]، حيث إن طلب HTTP محدد دون بيان أي طريقة صريحة.

الملاحظة 3 – قد يستعمل مقدم الخدمة SP إشارة دعم الاستيقان على أساس المعمارية GBA المتلقاة في الخطوة 1 لاختيار عنوان مقدم هوية ملائم.

2.1.2.IV البروتوكول HTTPS والمفاتيح المتقاسمة سلفاً (PSK) في أمن طبقة النقل (TLS)

عندما يُستخدم البروتوكول HTTPS مع المفاتيح المتقاسمة سلفاً (PSK) في أمن طبقة النقل (TLS) وفقاً للمواصفة [b- TS 33.222]، الفقرة 4.5، تكون عندئذٍ الخطوات على النحو التالي:

1) تتصل التجهيزات UE بمقدم الخدمة SP للنفاذ إلى خدمة يقدمها الأخير بإرسال طلب HTTP. ويحتوي هذا الطلب على إشارة دعم استيقان على أساس المعمارية GBA (قارن مع الخطوة 3 في الفقرة 1.1.2.IV)، إذ قد تضطر تجهيزات المستعمل UE بتأثير IdP/NAF إلى استعمال TLS التقليدية حتى لو كانت UE تعرض استعمال المفاتيح PSK TLS.

2) عند استلام طلب HTTP من UE، يحصل SP على عنوان مقدم الهوية ويرسل استجابة HTTP محوّلة مع <lib:AuthnRequest> في المحدد URL إلى UE. ويعتمد أسلوب الحصول على عنوان مقدم الهوية على التنفيذ وهو من شأن مقدم الخدمة.

3) تبدأ تجهيزات UE بإقامة نفق PSK TLS إلى IdP/NAF كما هو محدد في الفقرة 4.5 في المواصفة [b-TS 33.222]. ويكون ذلك استعداداً لإرسال الطلب المحوّل إلى IdP/NAF (قارن مع الخطوة 4). وتشير UE، أثناء إقامة النفق TLS، إلى إمكانية استعمال PSK TLS، وبإمكان IdP/NAF أن تختار استعمال PSK TLS مع معمارية GBA.

وتدرك UE، من طاقم شفرة TLS الذي اختاره IdP/NAF، ما إذا كان هذا الأخير سوف يستعمل PSK TLS.

وإذا كان هنالك ترابط أمن إنهاض بين UE والوظيفة IdP/NAF، عندئذٍ يتقاسم هذان الكيانان المفاتيح لحماية النقطة المرجعية Ua. وهكذا فإن UE لديها جميع البيانات اللازمة لإقامة نفق PSK TLS وفقاً للمواصفة [b-TS 33.222] ويمكن الانتقال إلى الخطوة التالية فوراً دون تنفيذ إجراءات الإنهاض.

وإذا لم يكن هنالك من ترابط أمن إنهاض بين UE والوظيفة IdP/NAF، ولكن UE تحتوي على مفتاح إنهاض صالح Ks، عندئذٍ تقيم UE نفق PSK TLS مع IdP/NAF على أساس المفتاح Ks_(ext)_NAF المعني.

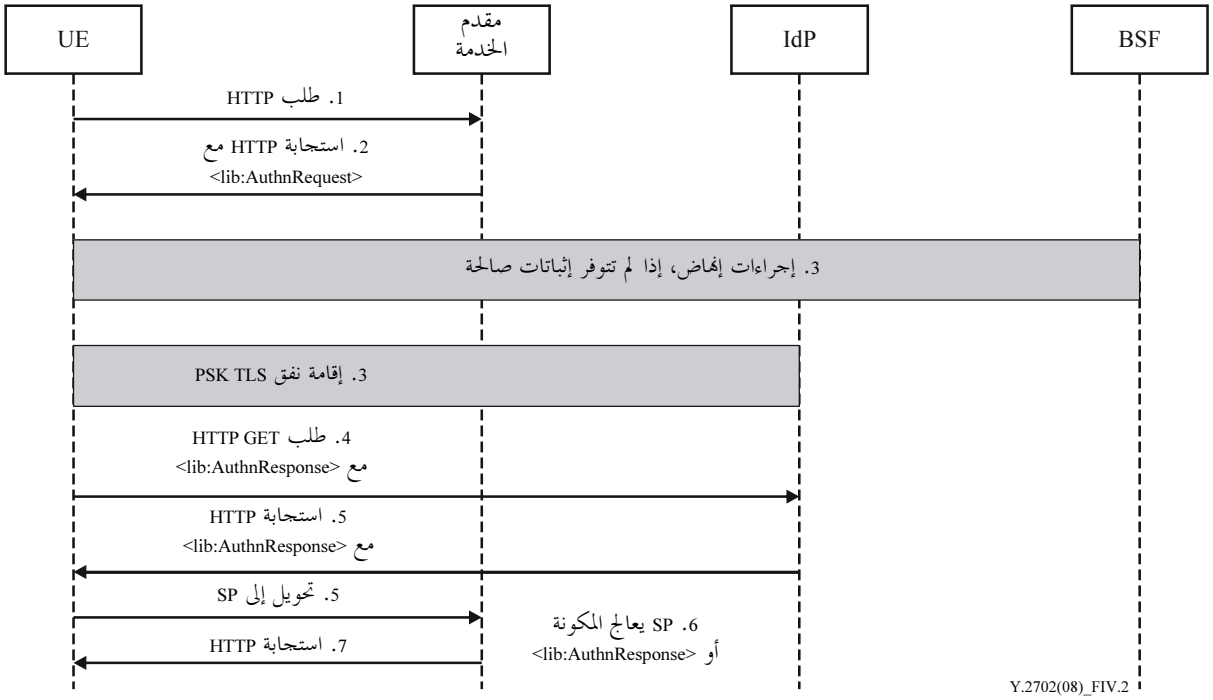
وإذا لم تكن UE تحتوي على جلسة إنهاض صالحة، أو لم تكن حداثة مواد المفتاح كافية بالنسبة إلى IdP/NAF، عندئذٍ تقوم UE بتنفيذ إجراءات إنهاض جديدة مع الوظيفة BSF. وهذه العملية شفافة إزاء SP.

4) تحقق UE النفاذ إلى IdP/NAF URL بطلب HTTP GET مع معلومات <lib:AuthnRequest> [b-ID-FF bindings] ضمن نفق PSK TLS المقام.

5) يستخلص مقدم الهوية IdP الطلب <lib:AuthnRequest>، ويقوم بمعالجته ويستعمل استيقان UE الذي جرى أثناء إقامة نفق PSK TLS، ويرسل استجابة HTTP المحوّلة إلى UE التي تحوّلها ثانية إلى SP. وقد يحتوي المحدد URL على مكونة من SAML أو <lib:AuthnResponse>.

6) يستخلص SP مكونة SAML أو <lib:AuthnResponse> ويعالجها ويرد باستجابة HTTP.

7) يرد SP باستجابة HTTP.



الشكل 2.IV – تدفق الرسائل من أجل استيقان وحيد مع <lib:AuthnResponse> واستعمال PSK TLS مع معمارية GBA

ملاحظة – الملاحظات الواردة في الفقرة 1.1.2.IV سارية أيضاً لاستعمال PSK TLS كما هو محدد في هذه الفقرة الفرعية.

2.2.IV سيناريو الاستيقان الوحيد SSO: إطار تجميع الهويات ID-FF مع تحويل مكونة

هذا السيناريو مشابه للسيناريو الوارد في الفقرة 1.2.IV، بالإضافة إلى أن مقدم الخدمة بإمكانه الاتصال بمقدم الهوية IdP مباشرة.

ملاحظة – بما أن تدفق الرسائل الأساسي هو ذاته بالنسبة لاستعمال المكونة وبالنسبة إلى <lib:AuthnResponse>، فإن نفس الفوارق بين استعمال TSL التقليدية واستعمال PSK TLS كما في الفقرة 1.2.IV تنطبق على هذه الفقرة أيضاً. وتدفقات الرسائل الواردة في هذه الفقرة تشير إلى TLS التقليدية، والاستعمال التماثلي للمفاتيح PSK TLS ممكن أيضاً.

يجب على مقدم الهوية IdP أن يدعم سطحاً بينياً إضافياً لمقدم الخدمة SP لتمكنيه من استقاء تأكيد الاستيقان. وهذا السطح البيني غير منفصل كلياً عن معمارية GBA، إذ إن معلومات الاستيقان هذه قد تشمل معلومات معمارية GBA متصلة بذلك، منها مثلاً هوية المستعمل والاسم المستعار والمزيد من المعلومات من GUSS والتقييدات القائمة على معمارية GBA وغير ذلك.

1) تتصل UE بمقدم الخدمة SP للنفاذ إلى خدمة يوفرها الأخير بإرسال طلب HTTP. ويحتوي هذا الطلب على إشارة دعم استيقان تقوم على أساس معمارية GBA (قارن مع الخطوة 3)، وهذا مطلوب من أجل تحويل الطلب وفقاً للخطوة 3.

2) عند استلام طلب HTTP من UE، يحصل SP على مقدم الهوية ويرسل استجابة HTTP محوّلة مع <lib:AuthnRequest> إلى UE. ويعتمد أسلوب الحصول على عنوان مقدم الهوية على التنفيذ وهو شأن مقدم الخدمة.

3) تتصل UE بدورها بمقدم الهوية IdP بموجب المحدد URL الوارد في ميدان رأسية الموقع ويتعيَّن على UE النفاذ إلى NAF/IdP URL مع طلب HTTP ومعلومات <lib:AuthnRequest> [b-ID-FF bindings].

تبيِّن UE للوظيفة NAF/IdP أن الاستيقان القائم على معمارية GBA مدعوم بإضافة متوالية ثابتة إلى رأسية HTTP لدى "User-Agent" كعلامة منتج كما هو محدد في المعيار [b-IETF RFC 2616]. وتُحدَّد هذه المتوالية الثابتة وفقاً للخطوة 2 في الفقرة 3.5 في المواصفة [b-TS 33.222].

إذا كان هنالك ترابط أمن إنهاض بين UE وIdP/NAF، عندئذٍ يتقاسم هذان الكيانان المفاتيح لحماية النقطة المرجعية Ua ويكون لدى UE جميع البيانات اللازمة لأداء استيقان موجز HTTP من الرسائل السابقة. وفي هذه الحالة تُجمَع الخطوة 3 مع الطلب في الخطوة 5 وتُحذَف الخطوة 4.

4) إذا لم تكن UE مستيقنة بعد مع IdP، عندئذٍ يتعيَّن أن يتم الاستيقان هنا، كما هو محدد في المواصفة [b-TS 33.222]. وطريقة هذا الاستيقان وتفاصيله غير محددة من قِبل Liberty Alliance في [b-ID-FF]. ويرسل IdP استجابة HTTP مع بيان وضع غير مرخَّص به إلى UE كما هو محدد في المواصفة [b-TS 33.222].

إذا لم يكن هنالك من مواد مفاتيح محددة بالوظيفة NAF صالحة، أو إذا لم تكن حداثة مواد المفاتيح مرضية لأي من NAF أو IdP، عندئذٍ يتعيَّن أداء إجراءات الإنهاض المحددة في المواصفة [b-TS 33.220]. وهذه العملية شفافة إزاء SP.

5) تردّ UE بطلب HTTP GET مع ميدان رأسية استيقان تحتوي كاسم مستعمل B-TID وككلمة سر Ks_(ext/int)_NAF. ويمكن أن تحتوي UE على المزيد من بيانات المستعمل المتصلة بالبروتوكول LAP.

بإمكان IdP/NAF أن يطلب شهادات ومواد متصلة بذلك إذا لم تكن مخزونة لديه أصلاً. وقد تحتوي المواد USS المستلَمة على المزيد من المعلومات الخاصة بمؤسسة Liberty.

6) يستجيب IdP بمكونة SAML في الاستجابة HTTP المحوّلة والموقع URL [b-ID-FF bindings]. وقد يحتوي IdP على المزيد من البيانات المتصلة بالبروتوكول LAP.

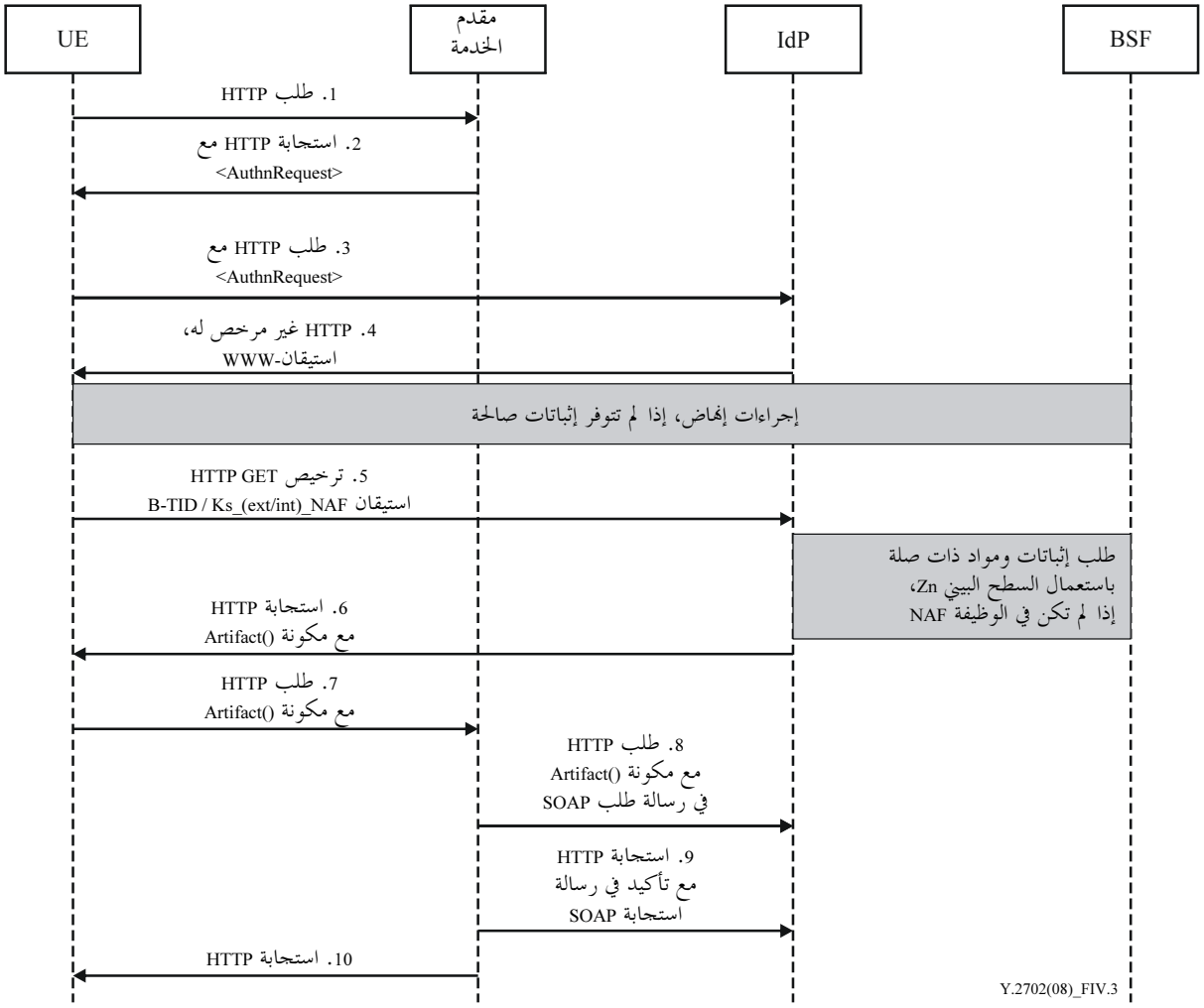
7) تتصل UE ثانية بمقدم الخدمة SP باستعمال هذا المحدد URL والطلب HTTP مع المكونة SAML.

8) يرسل SP الطلب HTTP مع المكونة SAML إلى IdP. ويحتوي الطلب على رسالة الطلب SOAP <samlp:Request> إلى نهائية بروتوكول النفاذ بسيط الغرض SOAP لدى مقدم الهوية، ويطلب التأكيد بتقديم مكونة تأكيد SAML في عنصر <samlp:AssertionArtefact> كما هو محدد في [b-ID-FF bindings].

9) وبإمكان IdP الآن بناء أو إيجاد التأكيد المطلوب والرد برسالة استجابة SOAP <samlp:Response> مع <saml:Assertion> المطلوب أو شفرة وضع كما هو محدد في [b-OASIS]. ويرسل IdP تأكيد الاستيقان الذي يقابل المكونة.

10) يقوم SP بمعالجة رسالة SOAP مع <saml:Assertion> معاد في <samlp:Response>، ويتحقق من التوقيع في <saml:Assertion> ويعالج الرسالة كما هو محدد في [b-ID-FF bindings] ثم يرد باستجابة HTTP.

ينبغي أن يكون عمر تأكيد الاستيقان SAML مساوياً أو أقل من معرِّف معاملة الإنهاض B-TID.



الشكل 3.IV – تدفق الرسائل من أجل استيقان وحيد (SSO) مع تحويل مكونة واستعمال معمارية GBA

3.2.IV سيناريو استيقان وحيد: خدمة استيقان وظيفة ID-WSF

تكون التجهيزات UE في هذا السيناريو متمكنة من بروتوكول LAP، أي وكيل مستعمل أو جهاز في بروتوكول Liberty (LUAD) (كما هو محدد في جانبيات Liberty ID-WSF لهذه المواصفة [b-ID-WSF profiles]). وعناصر البروتوكول المستعملة مأخوذة من خدمة استيقان [b-id-wsf service]، ويشتمل التفاعل بين UE وIdP على دورتي بروتوكول متعاقبتين. ويتصل عميل LUAD النشيط بمقدم هوية NAF/IdP أولاً قبل النفاذ إلى الخدمة التي يقدمها SP.

1) تستيقن UE لدى خدمة الاستيقان من مقدم الهوية IdP وتستخرج علامة أمن تخولها من تفعيل بعض الخدمات.

2) تلجأ التجهيزات UE إلى خدمة الاستيقان الوحيد (SSOS) لدى مقدم الهوية IdP باستعمال علامة الأمن. وفي هذه الخطوة تتلقى التجهيزات UE تأكيد الاستيقان (معلومات الاستيقان والترخيص) الواجب استعمالها لدى SP.

3) تقدم UE تأكيد الاستيقان إلى SP الذي يتصرف كمقدم خدمة ويب (WSP) من أجل النفاذ إلى خدمة الويب.

وعندما يكون تقديم خدمة الويب إلى المستعمل جزءاً من ميدان مشغِّل مقدم الهوية، فإن بإمكان عميل LUAD أيضاً الاتصال بمقدم خدمة الويب WSP مباشرة بواسطة علامة أمن. وفي هذه الحالة يمكن الاستغناء عن الاتصال بخدمة الاستيقان الوحيد (SSOS).

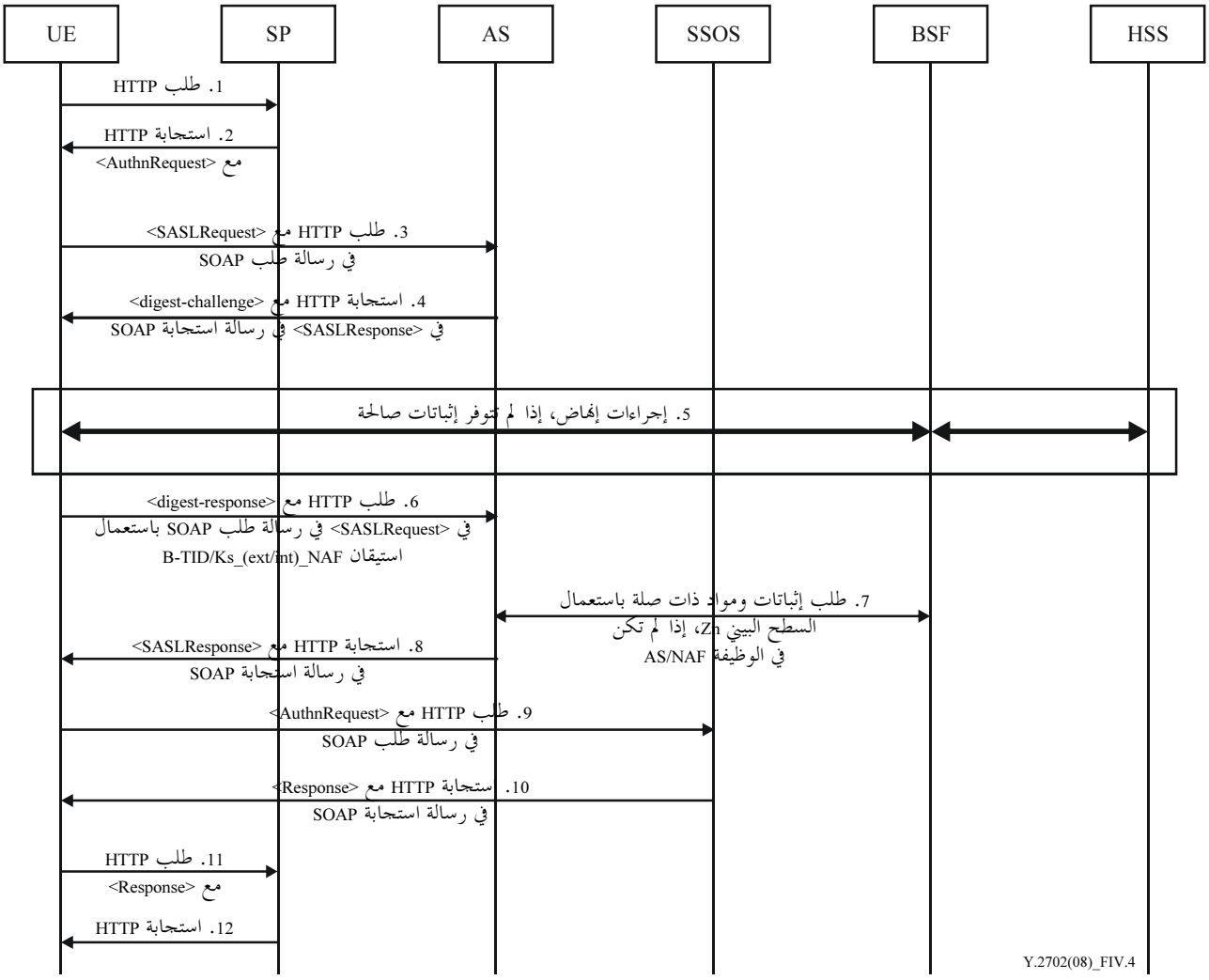
وتجري مقابلة الخطوات الثلاث مع معمارية GBA على النحو التالي:

– تُقابَل الخطوة الأولى مع الاتصال بين المستعمل (LUAD) وخدمة الاستيقان كما هو محدد ضمن البروتوكول LAP [b-ID-WSF service]. وبروتوكول الاستيقان مبطّن في بروتوكول طبقة الاستيقان البسيط والأمن

(SASL). وينبغي تنفيذ دورة Ub من جانب UE إذا دعت الضرورة. وهذا لا يقوم على أساس بروتوكولات LAP [b-ID-WSF service] أو [b-ID-FF] أو [b-ID-WSF service]، وإنما على أساس بروتوكولات معمارية GBA فقط [b-TS 33.220].

– والخطوتان الثانية والثالثة تماماً كما هو محدد في البروتوكول LAP (لا علاقة بمعمارية GBA). وعلاقة التبعية الوحيدة بمعمارية GBA هي في محتوى تأكيد استيقان لغة ترميز تأكيد الأمن (SAML) والتي تعتمد جزئياً على نتائج GBA (معلمات البروتوكولات، مثل وقت التنفيذ، والمعلمات الخاصة بالمستعمل، مثل تلك المأخوذة من USS).

فيما يلي تدفق الرسائل في سيناريو الاستيقان الوحيد SSO وخدمة الاستيقان ID-WSF مع تحويل الاستجابة. ويمكن أن ينطبق ذلك أيضاً عندما تقدم الخدمة SSOS أيضاً خدمة استيقان ID-WSF، وفي هذه الحالة تشارك الخدمة SSOS موقع خدمة الاستيقان.



الشكل 4.IV – تدفق الرسائل من أجل خدمة الاستيقان ID-WSF والاستيقان الوحيد (SSO) مع تحويل الاستجابة واستعمال معمارية GBA

1) تتصل التجهيزات UE بمقدم الخدمة SP للنفاذ إلى خدمة يقدمها الأخير وذلك بإرسال طلب HTTP.

2) عند استلام طلب HTTP من UE، يحصل SP على عنوان خدمة الاستيقان ويرسل استجابة HTTP محوّلة إلى UE. وقد تحتوي الاستجابة HTTP أو لا تحتوي على رأسية <lib:AuthnRequest> طبقاً لنموذج التطبيق أو النشر. ويعتمد أسلوب الحصول على عنوان خدمة الاستيقان على التنفيذ.

3) ترسل التجهيزات UE (LUAD-WSC) طلب HTTP إلى خدمة الاستيقان. ويحتوي الطلب رأسية <SASLRequest> مرتبطة بالبروتوكول SOAP، حيث تُملأ معلمة "آلية" قائمة من اسم أو أكثر من أسماء آلية SASL المدعومة لدى العميل.

تبيِّن التجهيزات UE إلى NAF/AS أن الاستيقان القائم على أساس معمارية GBA مدعوم بإضافة متوالية ثابتة إلى رأسية HTTP لدى "User-Agent" كعلامة منتج كما هو محدد في المعيار [b-IETF RFC 2616]. وتحدَّد هذه المتوالية الثابتة تبعاً للخطوة 2 في الفقرة 3.5 في المواصفة [b-TS 33.222].

إذا كان هنالك ترابط أمن إنهاض بين UE وNAF/AS، عندئذٍ يتقاسم هذان الكيانان المفاتيح لحماية النقطة المرجعية Ua ويمكن للتجهيزات UE أداء إجراءات الاستيقان اللاحقة إذا كانت جانبية طبقة الاستيقان البسيطة والأمن (SASL) تسمح بذلك. وفي هذه الحالة تُجمَع الخطوة 3 مع الطلب في الخطوة 6، وتُحذَف الخطوتان 4 و5.

4) ترسل خدمة الاستيقان AS استجابة HTTP إلى UE. وتحتوي الاستجابة على رأسية <SASLResponse> مرتبطة بالبروتوكول SOAP، حيث تُملأ معلمة "ServerMechanism" باسم آلية مختارة SASL (أي استيقان DIGEST) من قائمة آليات SASL مدعومة لدى العميل، وفي هذه الحالة تحتوي الرأسية <SASLResponse> أيضاً معلمة <digest-challenge>. وتمتثل طريقة هذه المعلمة وتفاصيلها للمواصفة [b-IETF RFC2831].

5) وإذا لم تكن تجهيزات UE تحتوي على جلسة إنهاض صالحة أو لم تكن حداثة مواد المفاتيح كافية لأغراض خدمة الاستيقان، عندئذٍ تقوم التجهيزات UE بتنفيذ إجراءات إنهاض جديدة مع الوظيفة BSF وتحصل على مفتاح مشترك Ks_(ext/int)_NAF. وهذه العملية شفافة لدى SP.

6) وتعيد التجهيزات UE إرسال طلب HTTP إلى خدمة الاستيقان. ويحتوي الطلب على رأسية <SASLRequest> مرتبطة بالبروتوكول SOAP، حيث تُملأ معلمة "mechanism" بآلية SASL المعادة في الخطوة 4، وفي هذه الحالة تحتوي الرأسية <SASLRequest> أيضاً على معلمة <digest-response>، حيث تحسب بيانات الاستيقان باستعمال المعرِّف B-TID كاسم مستعمل وKs_(ext/int)_NAF ككلمة سر. وتمتثل طريقة وتفاصيل هذه المعلمة للمواصفة [b-IETF RFC2831]. ويمكن للتجهيزات UE إدراج المزيد من بيانات المستعمل المتعلقة بالبروتوكول LAP.

7) وبما أن خدمة الاستيقان تشارك موقع NAF، فإنها تطلب Ks_(ext/int)_NAF وغير ذلك من المواد من الوظيفة BSF باستعمال السطح البيني Zn إذا لم تكن متاحة بعد.

8) تعالج خدمة الاستيقان معلمة <digest-response> في رأسية <SASLRequest>. ثم تستجيب خدمة الاستيقان برأسية <SASLResponse> مرتبطة بالبروتوكول SOAP في الاستجابة HTTP. وتحتوي رأسية <SASLResponse> على معلمة EPR (مرجع نقطة نهائية) في الوظيفة ID-WSF تشير إلى خدمة الاستيقان الوحيد SSOS ويوضع نمط خدمة URI طبقاً للمواصفة [b-ID-WSF service] وذلك لتعرُّف ID-WSF SSOS. وتحتوي الرأسية <SASLResponse> أيضاً على بعض الإثباتات الضرورية لكي تتمكن التجهيزات UE من تفعيل الخدمة SSOS. وقد تشمل خدمة الاستيقان المزيد من البيانات المتصلة ببروتوكول LAP.

9) ترسل التجهيزات UE طلب HTTP إلى الخدمة SSOS. ويحتوي الطلب على رأسية <samlp2:AuthnRequest> مرتبطة بالبروتوكول SOAP، حيث يوضع نعت ProtocolBinding تبعاً للمواصفة [b-ID-WSF service] لتعرُّف رابطة بروتوكول SAML الواجب استعمالها. كما يحتوي الطلب على رأسية <wsse:security> التي تشمل الإثباتات المعادة في الخطوة 8. وقد تحتاج التجهيزات UE إلى بناء رأسية <samlp2:AuthnRequest> في حد ذاتها إذا لم تتلق مثل هذه الرأسية في الخطوة 2 طبقاً لنموذج التطبيق أو النشر.

10) يُعالَج تعبير <samlp2:AuthnRequest>. وتستجيب الخدمة SSOS برأسية <samlp2: Response> في المحدد URL المحوّل في استجابة HTTP [b-ID-FF bindings]. وتحتوي رأسية <samlp2: Response> على معلمة <saml2:Assertion>. وقد تحتوي الخدمة SSOS على مزيد من البيانات المتصلة ببروتوكول LAP.

11) تتصل التجهيزات UE مرة ثانية بمقدم الخدمة SP باستعمال هذا المحدد URL والطلب HTTP مع <samlp2: Response>.

12) يردّ مقدم الخدمة SP باستجابة HTTP.

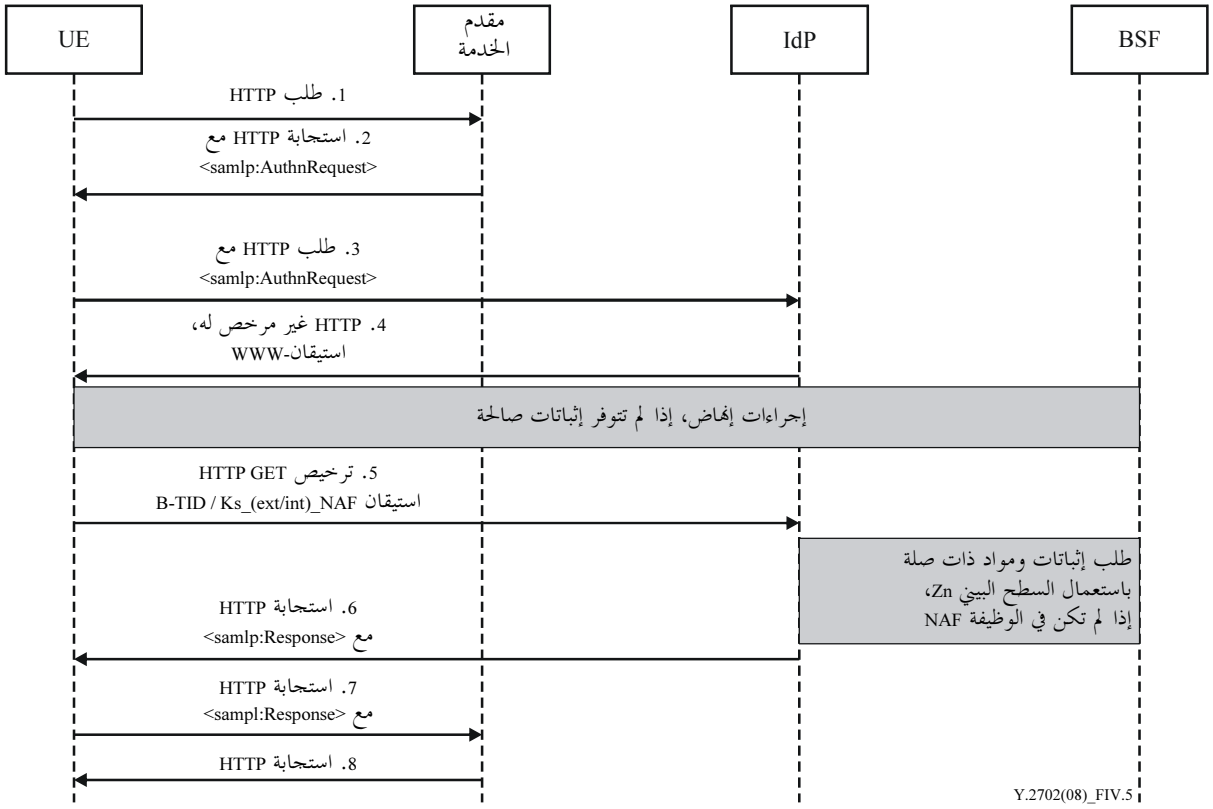
ملاحظة – إذا كان مقدم الهوية IdP يشارك في موقع الوظيفة BSF، عندئذٍ يمكن مقابلة الخطوة الأولى مع النقطة المرجعية Ub في معمارية GBA [b-TS 24.109]. ويمكن مقابلة الخطوة الثانية مع السطح البيني Ua في معمارية GBA.

على الرغم من هذا التماثل الشكلي في تنفيذ دورتين متعاقبتين من دورات البروتوكول المطلوبتين في كل من البروتوكولين، يبدو أن ليس من الممكن القيام بعملية مقابلة بسيطة. ويختلف تركيب ومعاني عناصر المعلومات المحالة بين بروتوكول GBA وبروتوكول LAP اختلافاً كبيراً.

4.2.IV سيناريو الاستيقان الوحيد (SSO): لغة ترميز تأكيد الأمن SAML v2.0 مع نقل <samlp:Response>

1.4.2.IV بروتوكول HTTPS وأمن طبقة النقل (TLS)

هذا السيناريو صيغة مماثلة للسيناريو في الفقرة 1.1.2.IV مع الفرق بأن جميع عناصر البروتوكول مأخوذة من ضمن البرمجية [b SAML v2.0] بتنفيذ جانبية الاستيقان الوحيد SSO لمتصفح الويب من المواصفة [b-OASIS]. وبالتالي فإن جميع الخطوات الموصوفة هناك تنطبق هنا أيضاً، بعد الاستعاضة عن العلاقة <lib:AuthnRequest> بالعلاقة <samlp:AuthnRequest> والاستعاضة عن العلاقة <lib:AuthnResponse> بالعلاقة <samlp:Response>. ولذلك لا تكرَّر الخطوات هنا، وإنما هنالك صيغة معدلة من الشكل 1.IV فيما يلي أدناه.

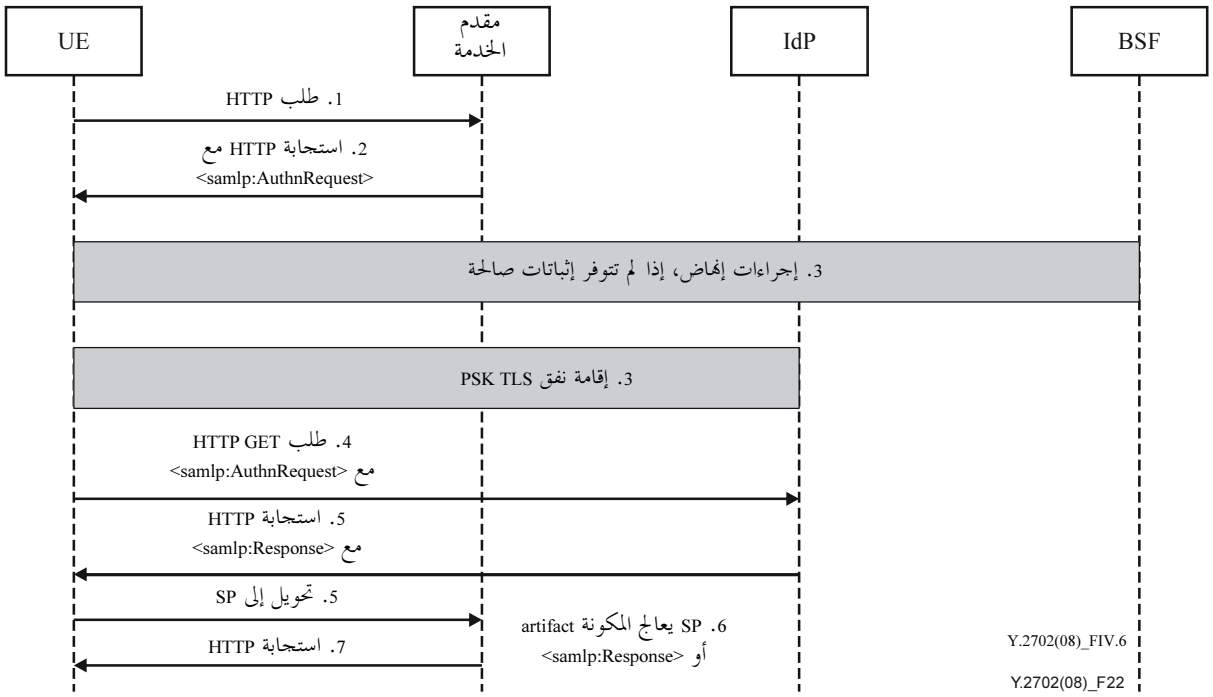


الشكل 5.IV – تدفق الرسائل من أجل استيقان وحيد (SSO) مع <samlp:Response> وأمن طبقة النقل (TLS) ومعمارية GBA

2.4.2.IV البروتوكول HTTPS والمفاتيح PSK في أمن طبقة النقل (TLS)

هذا السيناريو صيغة مشابهة للسيناريو الوارد في الفقرة 2.1.2.IV مع الاختلاف بأن جميع عناصر البروتوكول مأخوذة من ضمن البرمجية [b-SAML v.2.0] بتنفيذ جانبية SSO لمتصفح الويب [b-OASIS]. وبالتالي فإن جميع الخطوات الموصوفة هناك

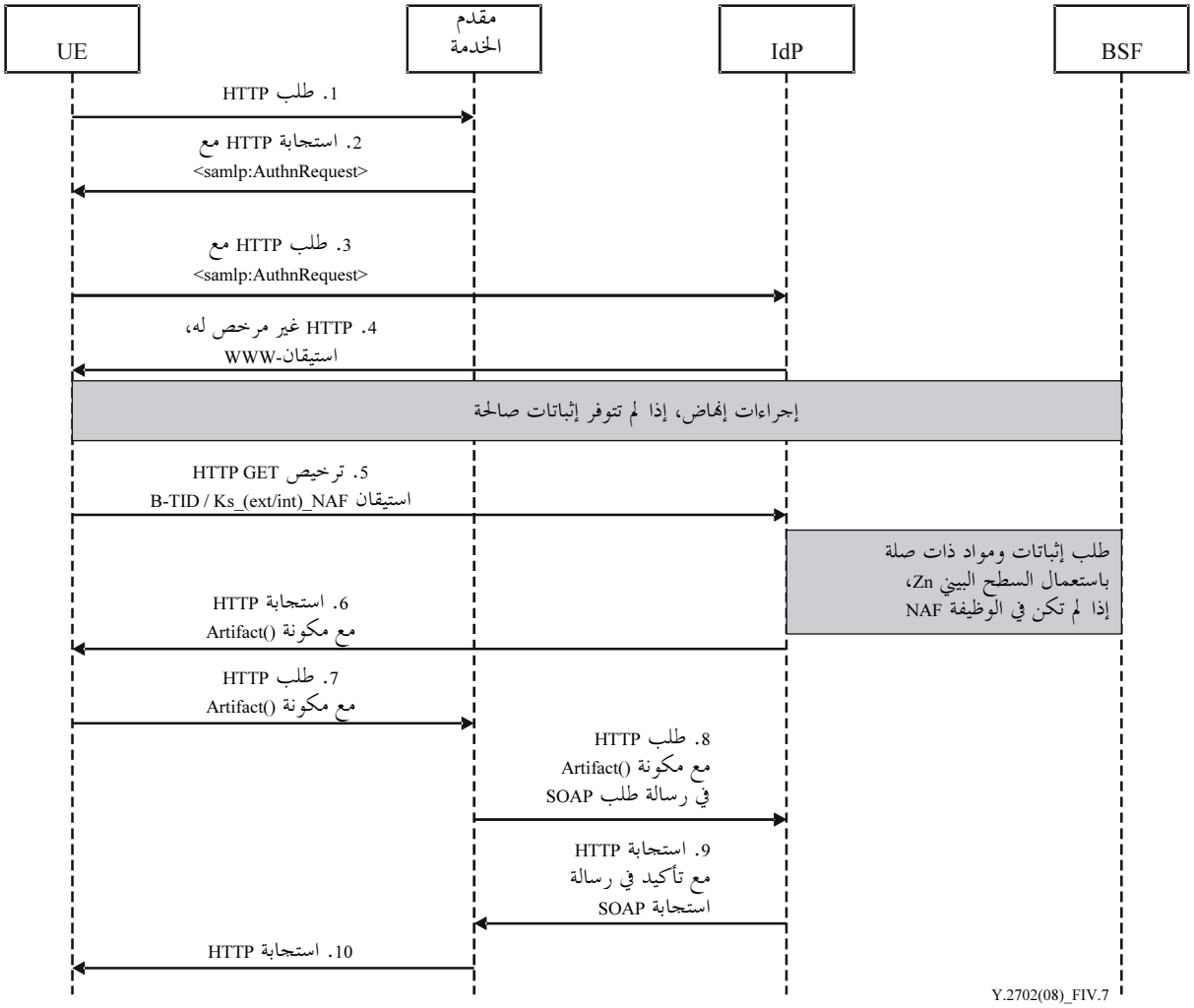
تنطبق هنا كذلك بعد الاستعاضة عن العلاقة <lib:AuthnRequest> بالعلاقة <samlp:AuthnRequest> والاستعاضة عن العلاقة <lib:AuthnResponse> بالعلاقة <samlp:Response>. ولا تكرر الخطوات هنا، وإنما تدرج صيغة معدلة من الشكل 2.IV فيما يلي أدناه.



الشكل 6.IV – تدفق الرسائل من أجل الاستيقان الوحيد SSO مع <samlp:Response> واستعمال المفاتيح PSK في أمن طبقة النقل (TLS) مع معمارية GBA

5.2.IV سيناريو استيقان وحيد (SSO): البرمجية SAML v2.0 مع نقل مكونة (استبانة)

هذا السيناريو صيغة مشابهة للسيناريو الوارد في الفقرة 2.2.IV مع الاختلاف بأن جميع عناصر البروتوكول مأخوذة من ضمن البرمجية [b-SAML v2.0] لتنفيذ جانبية SSO لمتصفح الويب من المواصفة [b-OASIS]. وبالتالي فإن جميع الخطوات الموصوفة هناك تنطبق هنا كذلك بعد الاستعاضة عن العلاقة <lib:AuthnRequest> بالعلاقة <samlp:AuthnRequest>. ولا تُكرَّر الخطوات هنا، وإنما يدرج فيما يلي صيغة معدلة من الشكل 3.IV.



الشكل IV.7 – تدفق الرسائل من أجل استيقان وحيد (SSO) مع استبانة المكونة (SAML v2.0) واستعمال معمارية GBA

البيبليوغرافيا

[b-ITU-T E.107] Recommendation ITU-T E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS*.

[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.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[b-Alliance] Liberty Alliance Project, ID-SIS: *Liberty Alliance ID-SIS 1.0 Specifications*.
<http://www.projectliberty.org/liberty/specifications__1>

[b-ID-FF] Liberty Alliance Project, ID-FF v1.2: *Liberty ID-FF Architecture Overview*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-FF bindings] Liberty Alliance Project, *ID-FF v1.2: Liberty ID-FF Bindings and Profiles Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-FF protocols] Liberty Alliance Project, ID-FF v1.2: *Liberty ID-FF Protocols and Schema Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-WSF binding] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF SOAP Binding Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID WSF discovery] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Discovery Service Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF profiles] Liberty Alliance Project, ID-WSF: *Profiles for Liberty enabled User Agents and Devices*.
<http://projectliberty.org/liberty/content/download/3447/22967/file/liberty-idwsf-client-profiles-v2.0-original.pdf>

[b-ID-WSF security] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Security Mechanisms*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF service] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Authentication Service Specification and Single Sign-On Service*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF v1.2] Liberty Alliance Project, ID-WSF v1.2: *Security Mechanisms*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_1_1_specifications>

[b-LAP] Liberty Alliance Project Support Documents: *Authentication Context Specification v2.0*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_specifications_support_documents_and_utility_schema_files>

[b-M-04-04] M-04-04: *E-Authentication Guidance for Federal Agencies*. <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf >

[b-NIST 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*. <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf >

[b-OASIS] OASIS, *Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>

[b-OASIS auth] OASIS, *Authentication Contexts for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>

[b-Reverse] Liberty Alliance Project Support Documents: *Liberty Reverse HTTP Binding for SOAP Specification v1.1*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_specifications_support_documents_and_utility_schema_files>

[b-SAML assertions] OASIS, SAML v2 Core, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

[b-SAML v2.0] OASIS, SAML v2 Core, *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf>

[b-TR 21.905] 3GPP TR 21.905 (in force), *Vocabulary for 3GPP Specifications*. <http://www.3gpp.org/ftp/Specs/html-info/21905.htm>

[b-TR 33.980] 3GPP TR 33.980 (in force), *Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA) (Release 7)*. <http://www.3gpp.org/ftp/Specs/html-info/33980.htm>

[b-TS 24.109] 3GPP TS 24.109 (in force), *Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details*. <http://www.3gpp.org/ftp/Specs/html-info/24109.htm>

[b-TS 29.109] 3GPP TS 29.109 (in force), *Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*. <http://www.3gpp.org/ftp/Specs/html-info/29109.htm>

[b-TS 33.220] 3GPP TS 33.220 (in force), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*. <http://www.3gpp.org/ftp/Specs/html-info/33220.htm>

[b-TS 33.221] 3GPP TS 33.221 (in force), *Generic Authentication Architecture (GAA); Support for subscriber certificates*. <http://www.3gpp.org/ftp/Specs/html-info/33221.htm>

[b-TS 33.222] 3GPP TS 33.222 (in force), *Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)*. <http://www.3gpp.org/ftp/Specs/html-info/33222.htm>

[b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL)*. <http://www.ietf.org/rfc/rfc2222.txt?number=2222>

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*. <http://www.ietf.org/rfc/rfc2246.txt?number=2246>

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol-HTTP/1.1*. <http://www.ietf.org/rfc/rfc2616.txt?number=2616>

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*. <http://www.ietf.org/rfc/rfc2617.txt?number=2617>

[b-IETF RFC 2831] IETF RFC 2831 (2000), *Using Digest Authentication as a SASL Mechanism*. <http://www.ietf.org/rfc/rfc2831.txt?number=2831>

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*. <http://www.ietf.org/rfc/rfc3546.txt?number=3546>

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*. <http://www.ietf.org/rfc/rfc4279.txt?number=4279>

[b-IETF RFC 4412] IETF RFC 4412 (2006), *Communication Resource Priority for the Session Initiation Protocol*. <http://www.ietf.org/rfc/rfc4412.txt?number=4412>

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، 2009