الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2721

(2010/09)

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

شبكات الجيل التالي – الأمـــن

متطلبات إدارة الهوية في شبكات الجيل التالي (NGN) وحالات الاستعمال

التوصيـــة ITU-T Y.2721

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
تلفزيون بروتوكول الإنترنت عبر شبكات الجيل التالي	Y.1999-Y.1900
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099-Y.2000
نوعية الخدمة والأداء	Y.2199-Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249-Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2299-Y.2250
الترقيم والتسمية والعنونة	Y.2399-Y.2300
إدارة الشبكة	Y.2499-Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599-Y.2500
الأمـــن	**Y.2799-Y.2700**
التنقلية المعممة	Y.2899-Y.2800
البيئة المفتوحة عالية الجودة	Y.2999-Y.2900
شبكات المستقبل	Y.3099-Y.3000

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

التوصيـــة ITU-T Y.2721

متطلبات إدارة الهوية في شبكات الجيل التالي (NGN) وحالات الاستعمال

ملخص

تقدم التوصية ITU-T Y.2721 أهداف إدارة الهوية (IdM) ومتطلباتها وأمثلة عن حالات استعمالها في شبكات الجيل التالي (NGN) وسطوحها البينية. وتُستعمل وظائف إدارة الهوية وقدراتها لزيادة الثقة في معلومات الهوية؛ ولدعم التطبيقات التجارية والأمنية وتعزيزها، بما في ذلك الخدمات على أساس الهوية.

والقصد من الاحتياجات الواردة في هذه التوصية هو شبكات الجيل التالي (أي الشبكات بالرزم الخاضعة للإدارة) على النحو المحدد في التوصية ITU-T Y.2001.

وتستند الأهداف والمتطلبات الواردة في هذه التوصية إلى إطار إدارة الهوية الوارد في التوصية ITU-T Y.2720 وإلى تحليل أمثلة حالات الاستعمال ذات الصلة بشبكات الجيل التالي. وإذ تُعتبر أمثلة حالات الاستعمال إعلامية، فهي موثقة في تذييلات في هذه التوصية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T Y.2721	2010.09.16	13

المصطلحات الرئيسية

الهوية الاتحادية، إدارة الهوية، شبكات الجيل التالي، الأمن.

تمهيـــد

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

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

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

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

ملاحظـــة

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

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

حقوق الملكية الفكرية

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

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

جدول المحتويات

الصفحة

الصفحة

التوصيـــة ITU-T Y.2721

متطلبات إدارة الهوية في شبكات الجيل التالي (NGN) وحالات الاستعمال

1 مجال التطبيق

ترد في هذه التوصية أهداف إدارة الهوية (IdM) ومتطلباتها ومبادئها التوجيهية وأمثلة عن حالات استعمالها في شبكات الجيل التالي (NGN) وسطوحها البينية. وتُستعمل وظائف إدارة الهوية وقدراتها لزيادة الثقة في معلومات الهوية ولدعم التطبيقات التجارية والأمنية وتعزيزها، بما في ذلك الخدمات على أساس الهوية.

ويشمل مجال تطبيق بهذه التوصية أهدافاً ومتطلبات ومبادئ توجيهية وأمثلة عن حالات الاستعمال تتناول ما يلي:

- زيادة الثقة في معلومات الهوية الخاصة بكيان من كيانات شبكات الجيل التالي (وهي من قبيل: مستعمل ومجموعة ومورد خدمة واتحاد ومؤسسة وجهاز مستعمل وعنصر شبكة وغرض).
- الإدارة الآمنة لدورة حياة معلومات الهوية (مثل التسجيل وإقرار الصلاحية والإلغاء)، بموافقة محددة وصريحة من المستعمل.
- إدارة الهوية بوصفها مفعّلةً لمصالح الأعمال (مثال ذلك، تسجيل دخول واحد إلى خدمات التطبيقات المتعددة وتسجيل خروج واحد منها) ولتطبيقات الأمن (مثل أدوات التحكم في النفاذ) بما في ذلك الخدمات القائمة على أساس الهوية (كالاستيقان والتأكيدات والهوية الاتحادية).
- ما يرتبط بهوية أو هويات كيان في شبكات الجيل التالي من اكتشاف وتبادل للمعلومات على نحو آمن بموافقة محددة وصريحة من المستعمل. ويشمل ذلك المعلومات التي قد تكون موجودة ضمن شبكات الجيل التالي وعبر مختلف الميادين الإدارية أو الاتحادات.
- العمل البيني/إمكانية التشغيل البيني ما بين أنظمة إدارة الهوية وقدراتها ضمن ميدان مورّد شبكة الجيل التالي (أي داخل الشبكة).
- العمل البيني/إمكانية التشغيل البيني لأنظمة إدارة الهوية وقدراتها ما بين مختلف ميادين أو اتحادات المورّدين، بموافقة محددة وصريحة من المستعمل، عندما يتعلق الأمر بمعلومات المستعمل. (مثل مورّدي شبكة الجيل التالي ومقدمي خدمات الويب ومورّدي المحتوى).
- إنفاذ السياسة المرعية (مثل حماية المعلومات التي تعرِّف بأصحابها شخصياً) المرتبطة بهوية كيان أو بمعلومات عنها.
- أمن أنظمة إدارة الهوية ووظائفها وقدراتها وبياناتها واتصالاتها.

والقصد من الأهداف والاحتياجات الواردة في هذه التوصية هو شبكات الجيل التالي (أي الشبكات بالرزم الخاضعة للإدارة) على النحو المحدد في [التوصية ITU-T Y.2001]، *نظرة عامة على شبكات الجيل التالي*.

وتستند الأهداف والمتطلبات الواردة في هذه التوصية إلى إطار إدارة الهوية الوارد في [التوصية ITU-T Y.2720] وإلى تحليل أمثلة حالات الاستعمال الموثقة في التذييلات.

الملاحظـــة 1 – لا يشير استعمال مصطلح "الهوية" فيما يتعلق بإدارة الهوية (IdM) في هذه التوصية إلى معناه المطلق. حيث لا يشكل بشكل خاص أي تحقق إيجابي من شخص ما.

الملاحظـــة 2 – في هذه التوصية، مصطلح "مستعمل" يجوز أن يكون شخصاً أو جماعات أو شركات أو كيانات قانونية، أو أي كيانات أخرى تستفيد من خدمات شبكات الجيل التالي.

الملاحظـــة 3 – في هذه التوصية، يُستعمل مصطلح "شبكة الجيل التالي/مورّد الهوية (NGN/IdSP)" لبيان أن خدمات إدارة الهوية قد يقدمها مورّد شبكة الجيل التالي أو طرف ثالث.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T E.107] التوصية ITU-T E.107 (2007)، *خدمة اتصالات الطوارئ (ETS) وإطار التوصيل البيني من أجل عمليات تنفيذ خدمة اتصالات الطوارئ على الصعيد الوطني*.

[ITU-T X.811] التوصية ITU-T X.811 (1995) | المعيار ISO/IEC 10181-2:1996، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الأطر الأمنية للأنظمة المفتوحة: إطار الاستيقان*.

[ITU-T X.1252] التوصية ITU-T X.1252 (2010)، *مصطلحات وتعاريف أساسية تتعلق بإدارة الهوية*.

[ITU-T Y.2001] التوصية ITU-T Y.2001 (2004)، *نظرة عامة على شبكات الجيل التالي*.

[ITU-T Y.2012] التوصية ITU-T Y.2012 (2010)، *المتطلبات الوظيفية لشبكات الجيل التالي ومعماريتها*.

[ITU-T Y.2201] التوصية ITU-T Y.2201 (2009)، *المتطلبات والمقدرات الخاصة بشبكات الجيل التالي حسب قطاع تقييس الاتصالات بالاتحاد*.

[ITU-T Y.2205] التوصية ITU-T Y.2205 (2008)، *شبكات الجيل التالي – اتصالات الطوارئ – اعتبارات تقنية*.

[ITU-T Y.2702] التوصية ITU-T Y.2702 (2008)، *متطلبات الاستيقان والترخيص في الإصدار 1 من شبكات الجيل التالي*.

[ITU-T Y.2720] التوصية ITU-T Y.2720 (2009)، *إطار إدارة الهوية في شبكات الجيل التالي*.

3 التعاريف

1.3 مصطلحات معرفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في وثائق أخرى:

1.1.3 إغفال الهوية [التوصية ITU-T X.1252]: حالة تعذر تحديد هوية كيان ضمن مجموعة من الكيانات.

ملاحظـــة – يحول إغفال الهوية دون تتبّع الكيانات أو سلوكها، من قبيل موقعها ووتيرة استعمالها للخدمة وما إلى ذلك.

2.1.3 مزعم [التوصية ITU-T X.1252]: بيان أدلى به (كيان) دون إرفاقه بدليل على صحته.

3.1.3 نعت [التوصية ITU-T X.1252]: معلومات مرتبطة بكيان تحدد خاصيته.

4.1.3 استيقان [التوصية ITU-T X.1252]: عملية تستعمل لتحقيق قدر كاف من الثقة في الربط بين الكيان والهوية المقدمة.

ملاحظـــة – يؤخذ استعمال مصطلح استيقان في سياق إدارة الهوية (IdM) على أنه يعني استيقان كيان.

5.1.3 ضمان الاستيقان [التوصية ITU-T Y.1252]: درجة الثقة التي يُتوصل إليها في عملية الاستيقان بأن الشريك الذي يجري الاتصال معه هو الكيان الذي يدّعي كونه أو يُتوقع كونه.

ملاحظـــة – تستند الثقة على درجة الثقة في العلاقة بين الكيان المتصل والهوية المقدمة.

6.1.3 تخويل [التوصية ITU-T X.1252]: منح الحقوق، وعلى أساس هذه الحقوق، السماح بالنفاذ.

7.1.3 إسناد [التوصية ITU-T X.1252]: مصاحبة أو رابطة أو صلة صريحة وثابتة.

8.1.3 ادّعاء [التوصية ITU-T X.1252]: القول بأن الأمر كذا، دون التمكّن من تقديم إثبات.

9.1.3 المدّعي [التوصية ITU-T X.1252]: كيان أو ممثل كيان أساس لأغراض الاستيقان.

ملاحظـــة – يتضمن المدعي الوظائف اللازمة للمشاركة في تبادل الاستيقان نيابة عن الأساس.

10.1.3 سياق [التوصية ITU-T X.1252]: البيئة محددة الحدود التي توجد فيها الكيانات وتتفاعل.

11.1.3 أوراق الاعتماد [التوصية ITU-T X.1252]: مجموعة بيانات تقدم كدليل على هوية و/أو استحقاقات مزعومة.

12.1.3 تفويض [التوصية ITU-T Y.2720]: الإجراء الخاص بإسناد سلطة أو مسؤولية أو وظيفة لكيان آخر.

13.1.3 الاكتشاف [التوصية ITU-T Y.2720]: عملية تحديد موضع الوصف القابل للمعالجة آلياً لمورد خاص بالشبكة قد يكون مجهولاً من قبل ويفي بمعايير وظيفية معينة. وتشمل هذه العملية مجموعة من المعايير الوظيفية وغيرها من المعايير مع مجموعة أوصاف الموارد. والهدف من هذه العملية هو التوصل إلى مورد مناسب خاص بالخدمة.

14.1.3 كيان [التوصية ITU-T Y.1252]: شيء له وجود قائم بذاته ومميّز ويمكن تعريفه في سياق.

ملاحظـــة – يمكن أن يكون الكيان شخصاً طبيعياً أو حيواناً أو شخصاً اعتبارياً أو منظمة، أو شيئاً فاعلاً أو منفعلاً، أو تطبيقاً برمجياً، أو خدمة وما إلى ذلك، أو مجموعة مما تقدم. وفي سياق الاتصالات، تشمل أمثلة الكيانات نقاط نفاذ ومشتركين وعناصر شبكة وشبكات وتطبيقات برمجيات وخدمات وأجهزة وسطوح بينية، وما إلى ذلك.

15.1.3 اتصالات الطوارئ (ET) [التوصية ITU-T Y.2205]: أي خدمة طوارئ تتطلب معالجة خاصة من الشبكة NGN مقارنة بالخدمات الأخرى. وتضم خدمات الطوارئ الحكومية المرخّصة وخدمات السلامة العامة.

16.1.3 خدمة اتصالات الطوارئ (ETS) [التوصية ITU-T E.107]: خدمة وطنية توفر أولوية الاتصالات للمستعملين المخولين باستعمال خدمة اتصالات الطوارئ في أوقات الكوارث وحالات الطوارئ.

17.1.3 اتحاد: [التوصية ITU-T X.1252]: رابطة بين مستعملي وموردي خدمات وموردي خدمة الهوية.

18.1.3 الهوية الاتحادية [التوصية ITU-T Y.2720]: هوية يمكن استعمالها للنفاذ إلى مجموعة من الخدمات أو التطبيقات المحددة بسياسات وشروط اتحاد ما.

19.1.3 معرّف الهوية [التوصية ITU-T X.1252]: نعت واحد أو أكثر يُستعمل لتحديد هوية كيان ضمن سياق.

ملاحظـــة – في سياق شبكات الجيل التالي وكما هو معرّف في التوصية [b-ITU-T Y.2091]، معرف الهوية هو مجموعة أرقام أو سمات ورموز أو أي شكل آخر من أشكال المعطيات المستعملة لتحديد هوية المشترك (المشتركين) أو المستعمل (المستعملين) أو عنصر (عناصر) أو وظيفة (وظائف) أو كيان (كيانات) الشبكة التي توفر الخدمات/التطبيقات أو سواها من الكيانات (كالجهات المادية أو المنطقية).

20.1.3 هوية [التوصية ITU-T X.1252]: تمثيل كيان في شكل واحد أو أكثر من النعوت التي تتيح تمييز الكيان أو الكيانات بالقدر الكافي ضمن سياق. ولأغراض إدارة الهوية (IdM)، يُفهم مصطلح هوية كهوية سياقية (مجموعة فرعية من النعوت)، أي تُحَدّ المجموعة المتنوعة من النعوت بإطار ذي حدود محددة (سياق) يوجد فيه الكيان ويتفاعل.

ملاحظـــة: يمثل كل كيان هوية واحدة شاملة تضم جميع عناصر المعلومات المحتملة التي تميز ذلك الكيان (النعوت) بيد أن هذه الهوية الشاملة هي قضية نظرية عصيّة على أي وصف واستعمال عملي لأن العدد الكلي لجميع النعوت المحتملة لا حصر له.

21.1.3 ضمان الهوية [التوصية ITU-T X.1252]: درجة الثقة في عملية التحقق والتأكد من الهوية التي يُلجأ إليها للتثبّت من هوية الكيان الذي تصدر أوراق الاعتماد له، ودرجة الثقة بأن الكيان الذي يستعمل أوراق الاعتماد هو الكيان الذي أُصدرت أو خُصّصت أوراق الاعتماد له.

22.1.3 إدارة الهوية (IdM) [التوصية ITU-T Y.2720]: مجموعة من الوظائف والقدرات (مثل الإدارة والتسيير الإداري والصيانة والاكتشاف وتبادل الاتصالات والربط والارتباط وإنفاذ السياسات والاستيقان وعمليات التأكد) المستعملة فيما يلي:

- ضمان معلومات الهوية (مثل معرفات الهوية والإثباتات والنعوت)؛
- ضمان هوية كيان ما (المستعملون/المشتركون، المجموعات، أجهزة المستعملين، المنظمات، موردو الشبكات والخدمات، عناصر وأشياء الشبكات، الأشياء الافتراضية)؛
- تمكين تطبيقات الأعمال التجارية والتطبيقات الأمنية.

23.1.3 نمط الهوية [التوصية ITU-T X.1252]: تعبير هيكلي عن نعوت كيان (مثل سلوك الكيان) يمكن استعماله في بعض عمليات تحديد الهوية.

24.1.3 مورّد الهوية (IdP): انظر مورّد خدمة الهوية (IdSP).

ملاحظـــة – يُستعمل مصطلح "مورد الهوية" في التوصية [ITU-T Y.2720] وفي مواصفات لمنظمات أخرى. بيد أنه تفادياً للبس في تفسيره بأنه الكيان الذي يورد الهويات، بدلاً من الكيان الذي يدير الهويات، يستخدم في هذه التوصية مصطلح مورد خدمة الهوية (IdSP).

25.1.3 مورّد خدمة الهوية (IdSP) [التوصية ITU-T Y.2720]: كيان يقوم بالتحقق من معلومات هويات الكيانات الأخرى مع الحفاظ عليها وإدارتها، ويمكن أن يستحدثها ويخصصها.

26.1.3 شبكة الجيل التالي [التوصية ITU-T Y.2720]: شبكة تقوم على الرزم ويمكنها تقديم خدمات الاتصالات ويمكنها الاستفادة من النطاق العريض المتعدد وتكنولوجيات النقل التي تتسم بجودة الخدمة وتكون فيها الوظائف المتصلة بالخدمة مستقلة عن التكنولوجيات الأساسية المتصلة بالنقل. وتتيح هذه الشبكة نفاذ المستعملين دون عوائق إلى الشبكات وموردي الخدمات المتنافسين و/أو الخدمات التي يختارونها. وهي تدعم التنقلية العامة التي تسمح بتقديم الخدمات إلى المستعملين بشكل متسق في كل مكان.

27.1.3 معلومات قابلة للتعرف الشخصي (PII) [التوصية ITU-T X.1252]: أي معلومات أ) تعرف أو يمكن استعمالها في التعرف على الشخص الذي تخصه هذه المعلومات أو الاتصال به أنو تحديد موقعه؛ ب) أو يمكن من خلالها الحصول على معلومات التعرف على شخص أو بيانات اتصاله؛ أو ج) تكون مرتبكة أو يمكن ربطها بشخص طبيعي بطريقة مباشرة أو غير مباشرة.

28.1.3 الوجود [التوصية ITU-T Y.2720]: مجموعة من النعوت تحدد خصائص كيان ما بالنسبة لوضعه الحالي.

29.1.3 الكيان الأساسي [التوصية ITU-T TX.811]: كيان يمكن استيقان هويته.

30.1.3 الخصوصية [التوصية ITU-T X.1252]: حق الأفراد في التحكم أو التأثير في ماهية المعلومات الشخصية المتعلقة بهم التي يمكن أن يجري جمعها وإدارتها والاحتفاظ بها والنفاذ إليها واستعمالها أو توزيعها.

31.1.3 الطرف المعوِّل [التوصية ITU-T X.1252]: كيان يعوِّل على تقديم هوية أو ادعائها من جانب كيان طالب/زاعم ضمن سياق طلب ما.

32.1.3 ميدان الأمن [التوصية ITU-T X.1252]: مجموعة عناصر وسياسة أمن وسلطة أمن ومجموعة أنشطة ذات صلة بالأمن تُدار فيها العناصر وفقاً للسياسة العامة للأمن.

33.1.3 ثقة [التوصية ITU-T X.1252]: الاعتقاد الراسخ بموثوقية المعلومات وصدقها؛ أو بقدرة أو بوضع كيان على حسن التصرّف ضمن سياق محدد.

34.1.3 مستعمِل: أي كيان يستفيد من مورد، مثل نظام أنو معدات أو مطراف أو تطبيق أو شبكة مشاع.

ملاحظـــة – في سياق شبكات الجيل التالي، وطبقاً للتوصية [ITU-T Y.2091-b]، يشمل ذلك المستعمل النهائي أو شخص أو مشترك أو نظام أو معدة أو مطراف (فاكس، حاسوب، مثلاً) أو كيان (وظيفي) أو عملية أو تطبيق أو مورد أو شبكة مؤسسة.

35.1.3 جهة التحقق [التوصية ITU-T X.1252]: كيان يؤكد صحة معلومات الهوية ويتحقق منها.

2.3 مصطلحات معرّفة في هذه التوصية

لا توجد.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات التالية:

3G الجيل الثالث (*3rd Generation*)

AKA اتفاق الاستيقان والمفتاح (*Authentification and Key Agreement*)

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

API السطح البيني لمبرمج التطبيق (*Application Programmer's Interface*)

BSS نظام دعم الأعمال (*Business Support System*)

CSP مقدم خدمة الاتصالات (*Communications Service Provider*)

DDoS حجب الخدمة موزع (*Distributed Denial of Service*)

DeviceID هوية جهاز (*Device Identity*)

DoS حجب الخدمة (*Denial of Service*)

EAG بوابة التطبيق الخارجية (*External Application Gateway*)

EDS خدمة دليل المؤسسة (*Enterprise Directory Service*)

ET اتصالات في حالات الطوارئ (*Emergency Telecommunications*)

ETS خدمة اتصالات في حالات الطوارئ (*Emergency Telecommunications Service*)

EV-DO (معيار) بيانات الارتقاء المثلى (*Evolution Data Optimized*)

FE كيان وظيفي (*Functional Entity*)

FTTX مد الألياف البصرية إلى الموقع X (*Fiber-to-the-X*)

GBA المعمارية العامة للاستيقان بالسر المشترك (*Generic Bootstrapping Architecture*)

HSS مخدم المشترك المنزلي (*Home Subscriber Server*)

IBGC-FE الكيان الوظيفي للتحكم في بوابة حد التوصيل البيني (*Interconnection Border Gateway Control Functional Entity*)

IdM إدارة الهوية (*Identity Management*)

IdMCC-FE الكيان الوظيفي لتنسيق، والتحكم في، إدارة الهوية (*IdM Coordination and Control Functional Entity*)

IdSP مورّد خدمة الهوية (*Identity service Provider*)

IDPS أنظمة كشف الاقتحام ومنعه (*Intrusion Detection and Prevention System*)

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

IMS النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت (*IP Multimedia Subsystem*)

IP بروتوكول الإنترنت (*Internet Protocol*)

IPTV تلفزيون بروتوكول الإنترنت (*IP Television*)

ISC	التحكم في خدمة النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت (*IMS Service Control*)
IT	تكنولوجيا المعلومات (*Information Technology*)
KDC	مركز توزيع المفاتيح (*Key Distribution center*)
LS	مخدم الموقع (*Location Server*)
LTE	الارتقاء الطويل الأمد (*Long Term Evolution*)
MNO	مشغل شبكة الخدمة المتنقلة (*Mobile Network Operator*)
MSISDN	رقم مدير الخدمة المتنقلة المتكاملة لمشترك (*Mobile Subscriber Integrated Service Director Number*)
NACF	وظائف التحكم في مرفقات الشبكة (*Network Attachment Control Function*)
NGN	شبكات الجيل التالي (*Next Generation Networks*)
NNI	السطح البيني من شبكة إلى شبكة (*Network-to-network Interface*)
OAM&P	التشغيل والإدارة والصيانة والتزويد (*Operation, Administration, Maintenance and Provisioning*)
OSS	نظام دعم العمليات التشغيلية (*Operations Support System*)
PC	حاسوب شخصي (*Personal Computer*)
P-CSC-FE	الكيان الوظيفي المفوَّض للتحكم في دورة النداء (*Proxy Call Session Control Functional Entity*)
PDA	المساعد الرقمي الشخصي (*Personal Digital Assistant*)
PII	معلومات تعرِّف صاحبها شخصياً (*Personally Identifiable Information*)
POTS	النظام الهاتفي العادي (*Plain Old Telephone System*)
PS	مخدّم الحضور (*Presence Server*)
PSTN	شبكة هاتفية عمومية تبديلية (*Public Switched Telephone Network*)
QoS	جودة الخدمة (*Quality of Service*)
RACF	وظائف التحكم في الموارد والقبول (*Resource and Admission Control Function*)
RFID	التعرف بواسطة الترددات الراديوية (*Radio-frequency Identification*)
RP	الطرف المعوِّل (*Relying Party*)
SAA-FE	كيان وظيفي للاستيقان من الخدمة والتخويل باستعمالها (*Service Authentification and Autorisation Functional Entity*)
SAML	لغة ترميز تأكيد الأمن (*Security Assertion Markup Language*)
S-CSC-FE	كيان وظيفي للتحكم في دورة النداء المخدمة (*Serving Call Session Control Functional Entity*)
SIM	وحدة هوية المشترك (*Subscriber Identity Module*)
SIP	بروتوكول استهلال الدورة (*Session Initiation Protocol*)
SLA	اتفاق مستوى الخدمة (*Service Level Agreement*)
SN	عقدة الخدمة (*Service Node*)
SNI	السطح البيني من المخدم إلى الشبكة (*Server-to-Network Interface*)
SP	مقدم الخدمة (*Service Provider*)

SUP-FE الكيان الوظيفي للبيانات العامة لمستعمل الخدمة (*Service User Profile Functional Entity*)

TGS مخدم منح البطاقات (*Ticket Granting Server*)

UE معدات المستعمل (*User Equipment*)

UICC بطاقة دارة إلكترونية شاملة (*Universal Integrated Circuit Card*)

UNI سطح بيني من المستعمل إلى الشبكة (*User-to-Network Interface*)

URI معرف مورد منتظم (*Uniform Resource Identifier*)

UserID هوية المستعمل (*UserIidentity*)

VoD فيديو عند الطلب (*Video on Demand*)

VoIP نقل الصوت عبر بروتوكول الإنترنت (*Voice over Internet Protocol*)

WiFi الأمانة اللاسلكية (*Wireless Fidelity*)

WiMAX التشغيل البيني العالمي للنفاذ بالموجات الصغرية (*Worldwide Interoperability for Microwave Access*)

WLAN شبكة محلية لاسلكية (*Wireless Local Area Network*)

WS مخدم الويب (*Web Server*)

WSG بوابة خدمات ويب (*Web Services Gateway*)

xDSL عروة البدالة الهاتفية الرقمية للمشترك (*x Digital Subscriber Loop*)

5 اصطلاحات

يتعين فهم المصطلحات الأساسية التالية في هذه التوصية على النحو التالي:

"**يجب**"، "**يلزم**"، "**مطلوب**" كلمات تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه التوصية.

"**يوصى**" كلمة تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين توفر هذه المتطلب لزعم المطابقة.

"**يجب ألا**"، "**يلزم ألا**"، "**يحظر**" كلمات تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه التوصية.

"**ربما**"، "**يجوز**"، "**من الجائز**"، "**يمكن**": تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا ترمي هذه المصطلحات إلى إلزام التطبيق بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن المصنّع يمكنه إدراج هذا الخيار وزعم مطابقة هذه التوصية في نفس الوقت.

وفي متن هذه التوصية وملحقاتها، تصادَف أحياناً عبارات "*يتعين*" و"*يتعين ألا*" و"*ينبغي*" و"*يمكن*"، وينبغي تأويلها لتفيد بالمعاني الآتية على التوالي: "*مطلوب*" و"*يحظر*" و"*يوصى*" و"*يجوز*". وإذ تظهر مثل هذه العبارات أو المصطلحات الرئيسية في تذييل أو في مادة محددة صراحة على أنها "*إعلامية*"، تفسَّر على أن لا قصد معيارياً منها.

6 نظرة شاملة على إدارة الهوية

1.6 لمحة عامة

توفر التوصية [ITU-T Y.2720] إطاراً لإدارة الهوية. وتُستعمل وظائف إدارة الهوية لزيادة الثقة في معلومات الهوية الخاصة بكيان ما ودعم التطبيقات التجارية والأمنية (مثل التحكم في النفاذ والتخويل) بما في ذلك الخدمات القائمة على أساس الهوية.

والكيان هو شيء ما له وجود قائم بذاته ومميز يمكن تعريفه في سياق ما. ومن أمثلة الكيان، في سياق إدارة الهوية، المشتركون والمستعملون وعناصر الشبكة والشبكات وتطبيقات البرمجيات والخدمات والأجهزة.

وستدعم شبكات الجيل التالي مجموعة واسعة من خدمات التطبيقات للمشتركين لدى المستعمل النهائي وللمؤسسات الحكومية والتجارية. ولتوفير السلامة والحماية الأمنية لخدمات التطبيقات يوصى بأن تدعم شبكات الجيل التالي الوظائف والقدرات اللازمة لضمان الهوية وضمان بياناتها المرتبطة بكيان على أساس سياق محدد. راجع التوصية [ITU-T X.1252] للاطلاع على تعريف إدارة الهوية.

وتؤخذ في الاعتبار أمثلة حالات الاستعمال الموثقة في التذييلات التالية لدى تحديد احتياجات إدارة الهوية:

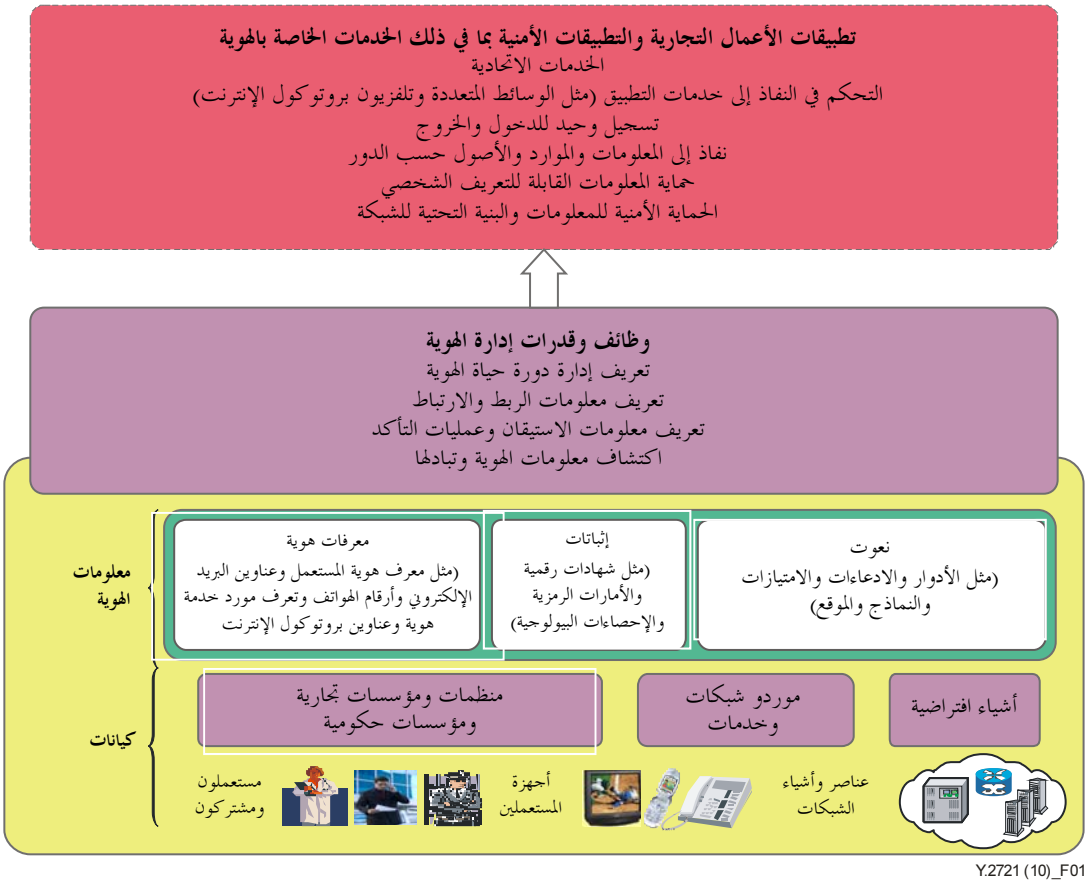
- التذييل I – حالات الاستعمال العامة لإدارة الهوية.
- التذييل II – حالات استعمال إدارة الهوية في تطبيقات شبكات الجيل التالي.
- التذييل III – خدمة الاتصالات في حالات الطوارئ فيما يتعلق بحالات استعمال إدارة الهوية.
- التذييل IV – حالات الاستعمال المتصلة بالخدمة المتنقلة.

وبالإضافة إلى ذلك، فإن العوامل التالية المرتبطة بهوية المستعمل النهائي في بيئة شبكات الجيل التالي تؤخذ في الاعتبار لدى تحديد متطلبات إدارة الهوية:

- الاستعمال المتزايد لهويات متعددة من جانب المستعملين النهائيين.
- إمكانية ارتباط الهوية بسياقات وامتيازات خدمية مختلفة.
- قد لا تُعرِّف الهوية بمستعمل نهائي إلا جزئياً.
- يمكن استعمال الأسماء المستعارة كهويات.
- إمكانية استعمال الهويات في أي مكان وزمان ومن أي جهاز.
- قد يتعذر التشغيل البيني للهويات فيما بين موردي شبكات الجيل التالي.

2.6 علاقات إدارة الهوية

يقدم الشكل 1 نظرة عامة على علاقات إدارة الهوية القائمة على أساس الإطار الوارد في التوصية [ITU-T Y.2720].



الشكل 1 – العلاقات في إدارة الهوية

يمكن أن تتراوح الكيانات بين فرادى المستعملين البشر ومنظمات فضفاضة مثل مصالح الأعمال وأشياء افتراضية كالتطبيقات الإلكترونية. ويمكن لمعلومات الهوية المرتبطة بكل من هذه الكيانات أن تتراوح في حساسيتها ما بين البيانات العامة نسبياً كأرقام الهواتف المدرجة في الدليل العمومي، مثلاً، وبيانات الهوية بالغة الحساسية مثل كلمات المرور والشهادات الرقمية وغيرها من أدوات الاستيقان الخاصة.

ويجوز لكيان أن يحمل هوية واحدة أو أكثر. ويجوز استعمال هذه الهويات لكي تمثل أدواراً متعددة (مثل أدوار المواطن والزوج والوالد والزبون والمريض) وتستعمل في معاملات محددة تتراوح بين أنشطة تجارية واجتماعية، وقد تتعدد الهويات الرقمية المرتبطة بشخص أو فرد حسب اختلاف السياقات، على النحو المبين في الشكل 1. أضف إلى ذلك أن الشخص العامل من خلال الهويات الرقمية قد يكون معروفاً لدى واحدة أو أكثر من الشخصيات المفترضة أو الظاهرة للعيان أو في المجتمع، أو قد يُعرف من خلال الأدوار التي توكلها إليه أو تمنحه إياها سلطة ما (كدور الجهة المستجيبة في حالات الطوارئ).

ويبين الشكل 1 ما يلي:

أ) الكيانات

في بيئة شبكات الجيل التالي حيث ترتكز الخدمات على سياقات وأدوار ويمكن النفاذ إليها من أي مكان وفي أي زمان ومن أي جهاز، تتعدد أشكال المعلومات المتصلة بالهوية التي يمكن أن ترتبط بكيان. وعلاوة على ذلك، يمكن لكيان أن يتخذ هوية واحدة أو أكثر حسب السياق. وتشمل أمثلة الكيانات ما يلي:

- المستعمل والمشتركون
- أجهزة المستعمل، وعناصر الشبكة وأغراضها
- المنظمات والجماعات والمؤسسات التجارية والمؤسسات الحكومية

- موردو الشبكة والخدمة
- الأشياء الافتراضية.

ب) معلومات الهوية

ويمكن تصنيف معلومات الهوية المرتبطة بكيان ما كما يلي:

- معرِّفات هوية (مثل حساب اشتراك، عناوين عناصر شبكية، معرّفات هوية موردي الخدمات)
- نعوت (مثل عناوين البريد الإلكتروني وأرقام الهواتف ومعرف هوية مورد منتظم وعناوين بروتوكول الإنترنت، الأدوار والادعاءات والامتيازات وطريقة الاستيقان والنماذج والموقع)
- الإثباتات (مثل الشهادات الرقمية والشارات)

ج) وظائف وقدرات إدارة الهوية

تستعمل وظائف وقدرات إدارة الهوية في زيادة الثقة في معلومات الهوية الخاصة بكيان ما؛ ودعم أو تعزيز تطبيقات الأعمال التجارية والتطبيقات الأمنية بما في ذلك الخدمات القائمة على الهوية. وفيما يلي أمثلة عن وظائف وقدرات إدارة الهوية:

- إدارة دورة حياة هوية
- تنظيم معلومات الهوية وإقامة الترابط والإسناد فيما بينها
- الاستيقان وضمان الاستيقان والتأكيد
- اكتشاف وتبادل معلومات الهوية
- وظائف وقدرات مد الجسور بين مختلف أنظمة إدارة الهوية تسهيلاً لإمكانية التشغيل البيني.

د) التطبيقات التجارية والأمنية

تقوم وظائف وقدرات إدارة الهوية بدعم وتعزيز التطبيقات التجارية والأمنية بما في ذلك الخدمات القائمة على أساس الهوية.

وتشمل أمثلة التطبيقات التجارية ما يلي:

- الخدمات الاتحادية (مثل النفاذ إلى الخدمات عبر مقدمي خدمات أو موردين لشبكات الجيل التالي على اختلافهم).
- تسجيل دخول وخروج وحيد (مثل النفاذ إلى مختلف التطبيقات والخدمات دون الحاجة إلى إعادة تقديم إثباتات الاستيقان الفردي لكل منصة تطبيق أو خدمة)

وتشمل أمثلة التطبيقات الأمنية ما يلي:

- التحكم في النفاذ
- إدارة التخويل الخاص بامتيازات
- حماية المعلومات التي يمكن أن تعرّف صاحبها شخصياً.

وتشمل أمثلة الخدمات القائمة على أساس الهوية ما يلي:

- الخدمات الخاصة بمعرفات الهوية والإثباتات والنعوت
- خدمات مد الجسور (مثل تقابل وتشبيك معلومات الهوية في بيئة غير متجانسة)
- خدمات معلومات النماذج.

وتشمل إدارة الهوية عمليات إدارة دورة الحياة، بالإضافة إلى وظائف وقدرات اكتشاف مصادر الهوية الموثوقة والحصول عليها بحيث يمكن استعمالها للتحقق والتأكد من صحة هوية فتتيح خدمات وقدرات إدارة الهوية للكيانات التحكم في طريقة استعمال ونشر معلومات الهوية الخاصة بهم. وتزود إدارةُ الهوية الكيانات (ومثالها الأطراف المعولة) بالمعلومات اللازمة لاتخاذ القرارات المتعلقة بالاستيقان والوثوق بما يرتبط بها من تعاملات واتصالات. كما تسمح إدارة الهوية بتقاسم واستعمال معلومات الهوية الاتحادية من جانب أعضاء الاتحاد (مثل مختلف موردي شبكات الجيل التالي أو المؤسسات التجارية

أو المؤسسات الحكومية) لدعم الخدمات الاتحادية. فعلى سبيل المثال، تتيح خدمات الهوية الاتحادية للكيانات المخولة من أعضاء الاتحاد النفاذ إلى موارد على أساس أدوارهم وامتيازاتهم وفقاً لقواعد وسياسات الاتحاد دون الحاجة لتسجيل كل عضو في الاتحاد والاستيقان منه.

3.6 الدوافع والحوافز

لا بد من أن تتمكن حلول إدارة الهوية من الاستجابة في الوقت الفعلي لتفاعلات تزداد تعقيداً فيما قد يتنقل المستعملون ما بين الأجهزة وتكنولوجيات النفاذ وطرائق الدفع وحتى الهويات، لأن العديد من خدمات شبكات الجيل التالي وقدراتها تنطوي على خدمة تقوم على أساس هوية المشترك والنواحي المفضلة لديه وعلى أساس النفاذ من أي جهاز وفي أي مكان وزمان. زد على ذلك أن المستعملين النهائيين يطالبون أيضاً بقدرات يسهل استعمالها. والأهم من ذلك أن المستعملين النهائيين يطالبون بقدرات تتيح لهم التحكم في الخصوصية وبالمعلومات التي تعرّف بهم شخصياً.

وتنبع دوافع إدارة الهوية وحوافزها من المستعملين النهائيين (مثل المشتركين في التطبيقات والخدمات) ومن موردي شبكات الجيل التالي والمؤسسات التجارية والحكومية الذين يرغبون جميعاً بأن تلبى مصالحهم واحتياجاتهم بعمليات تنفيذ إدارة الهوية. وتؤخذ العوامل التالية بعين الاعتبار في تحديد متطلبات إدارة الهوية لشبكات الجيل التالي:

- حاجة المستعملين النهائيين/المشتركين للتحكم في المعلومات الخاصة بهوياتهم وحمايتها، والرغبة بطرائق مرنة ومنتظمة للنفاذ إلى الموارد، وضرورة تحقيق التوازن بين مزايا الشبكات الاجتماعية وانكشاف المعلومات الشخصية.
- حاجة موردي شبكات الجيل التالي (موردي الشبكة والخدمة) إلى حماية موارد البنية التحتية لشبكتهم وخدماتها وتطبيقاتها، وإلى تمكين الخدمات الاتحادية وتعزيز الخدمات المتاحة على نطاق واسع على أساس الاشتراك، وتلبية احتياجات المستعملين النهائيين للخصوصية وحماية المعلومات التي تعرّف بهم شخصياً.
- حاجة المؤسسات التجارية والمستعملين إلى حماية مصالحهم التجارية والثقة بقدرات الاستيقان في التعاملات وحماية بيانات هويات الشركاء التجاريين.
- حماية البنية التحتية للشبكة من أي هجوم سيبراني وحماية البيانات الخاصة
- دعم المؤسسات الحكومية للخدمات الحكومية الإلكترونية وخدمات السلامة العامة وخدمات الإنذار المبكر وخدمة الاتصالات في حالات الطوارئ وغير ذلك من خدمات على الصعيد الوطني.

4.6 تعدد مقدمي الخدمات والبيئة الاتحادية

تُستعمل خدمات إدارة الهوية وقدراتها في بيئة اتحادية يتعدد فيها مقدمو الخدمات لاكتشاف المعلومات ونقلها بغية إرساء الثقة في هوية (هويات) كيان ما. فعلى سبيل المثال، يمكن لمورّد خدمة الهوية أن يتحقق من المعرفات والإثباتات والنعوت المرتبطة بهوية ما والتي يعتبرها الطرف المعوّل موثوقة وأن يوافي الطرف المعول (مستعمل، مورد خدمة، مثلاً) بالنتيجة من خلال تأكيدات، وذلك لدعم الاستيقان الذي قد يكون ضرورياً للتحكم في النفاذ وللقرارات التجارية ولإنفاذ السياسة المرعية (مثلاً، بشأن الخصوصية وحماية المعلومات التي تعرّف أصحابها شخصياً).

وبالإضافة إلى ذلك، قد تختلف الحلول المستقلة لإدارة الهوية مما يقتضي إمكانية التشغيل البيني بين مقدمي الخدمة.

5.6 مورّد خدمة الهوية

لا تفرض هذه التوصية أي قيود على من يوفر خدمات مورد خدمة الهوية (IdSP).

ومورّد خدمة الهوية عبارة عن كيان يقوم برعاية وإدارة وربما استحداث معلومات هويات لكيانات أخرى (مثل المستعملين/المشتركين والمنظمات والأجهزة) ويقدم خدمات خاصة بالهوية تقوم على الثقة والأعمال التجارية والأشكال الأخرى من العلاقات.

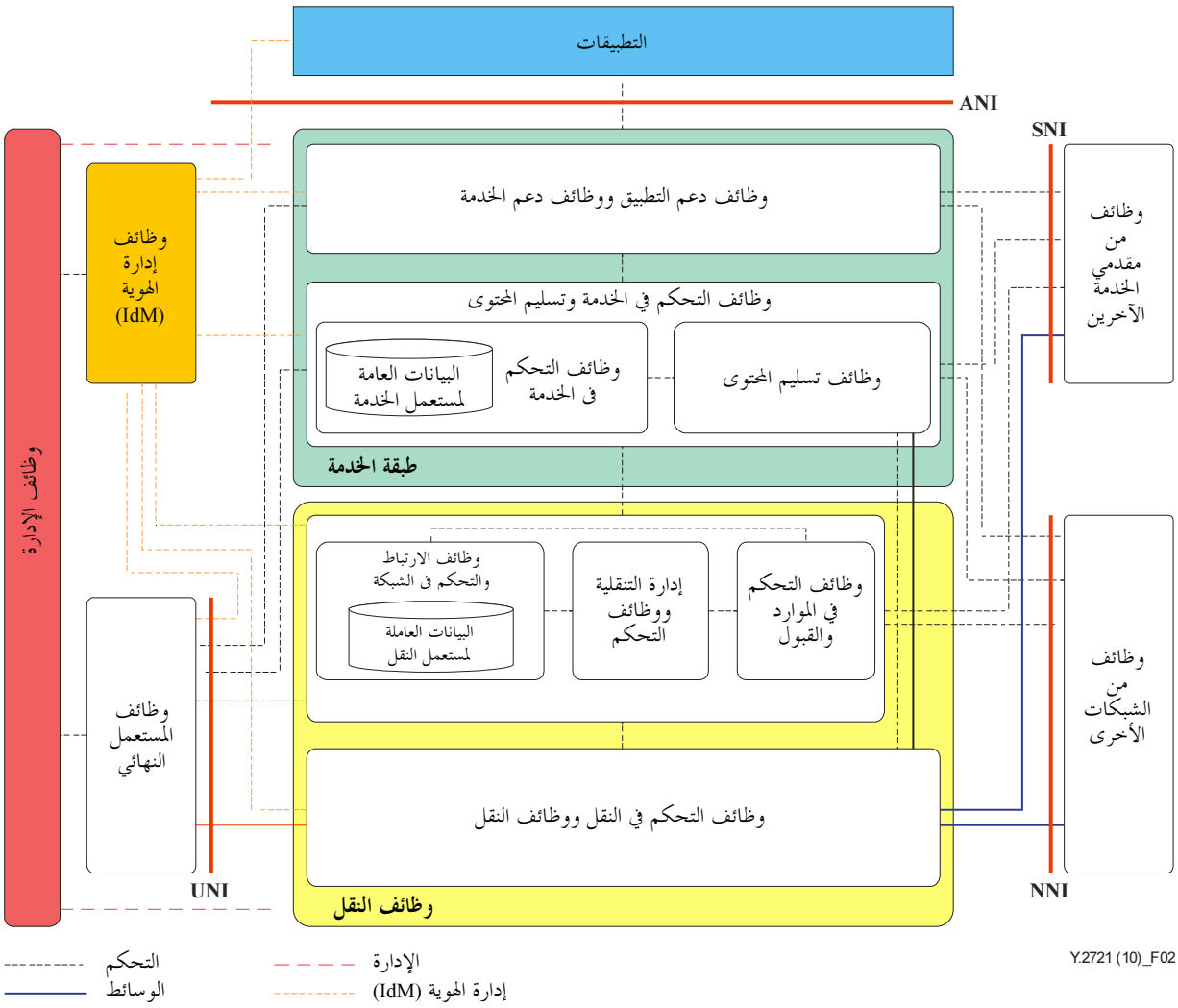
وفي بيئة تضم العديد من موردي الخدمات، قد يكون مورّد شبكات الجيل التالي مورد خدمة الهوية أيضاً، بحيث يوفر خدمات إدارة الهوية (مثل الخدمات القائمة على الهوية) لموردين آخرين.

ويُستعمل في هذه التوصية مصطلح "مورّد شبكات الجيل التالي/مورّد خدمة الهوية (NGN/IdSP)" للدلالة على أن خدمات إدارة الهوية يقدمها مورّد شبكات الجيل التالي أو طرف ثالث.

6.6 إدارة الهوية في سياق معماريات شبكة الجيل التالي ونماذجها المرجعية

1.6.6 العلاقة مع المعمارية الوظيفية لشبكة الجيل التالي

في سياق نموذج المعمارية المرجعية لشبكة الجيل التالي المعرّفة في التوصية [ITU-T Y.2012]، يمكن للوظائف المتصلة بإدارة الهوية أن تقع في مستويات مختلفة (مثل مستويات المستعمِل والتحكم والإدارة) وفي طبقات مختلفة من المعمارية الموزعة (مثل طبقة الخدمة وطبقة النقل). ومن منظور الإنجاز أو التنفيذ، قد ينطوي الدعم لخدمات إدارة الهوية ولقدراتها على استعمال العناصر الموجودة في الشبكة أو عناصر إضافية في الشبكة (من قبيل مخدمات التطبيقات المتخصصة) في شبكة الجيل التالي.



الشكل 2 – نظرة عامة على معمارية شبكة الجيل التالي

يقوم الشكل 2 على الشكل 7-1 [من التوصية ITU-T Y.2012] وهو يعرض قدرة وظيفية تمثل وظائف إدارة الهوية في المعمارية الوظيفية لشبكة الجيل التالي. ويبين الشكل 7-1 [من التوصية ITU-T Y.2012] المفاهيم العامة التي تفيد بأن الدعم لخدمات إدارة الهوية ولقدراتها يمكن أن يتضمن التفاعل مع كيانات وظيفية (FE) محددة لتفعيل خدمات معينة

ودعمها، منها خدمات الهوية. وتبعاً للخدمة المحددة في إدارة الهوية أو للقدرة الجاري دعمها ولتصميم التنفيذ، قد يشمل ذلك التفاعلات مع كيانات وظيفية ضمن الفدر الوظيفية التالية:

- التطبيقات؛
- طبقة الخدمة: وظائف دعم التطبيق ووظائف دعم الخدمة ووظائف التحكم في الخدمة ووظائف تسليم المحتوى؛
- طبقة النقل: وظائف التحكم في النقل ووظائف النقل؛
- وظائف المستعمل النهائي؛
- وظائف الإدارة.

في المعمارية الوظيفية لشبكة الجيل التالي، يمكن أن تقع وظائف إدارة الهوية في مستويات مختلفة (مثل مستويات المستعمِل والتحكم والإدارة) وفي طبقات مختلفة من المعمارية الموزعة (مثل طبقة الخدمة وطبقة النقل). ورغم ظهور وظائف إدارة الهوية في مجموعة من الوظائف قائمة بذاتها، فليس القصد من ذلك فرض أي تصميم لإدارة الهوية ولا وضع قيود عليها في التنفيذ. ويخضع تنفيذ وظائف إدارة الهوية للامتثال للسياسات ذات الصلة، مثل اللوائح والتشريعات الوطنية والإقليمية الخاصة بحماية بيانات الهوية (مثل البيانات PII). ويجب أن يكفل في تنفيذ واستعمال وظائف إدارة الهوية الامتثال تحديداً للسياسات ذات الصلة المتعلقة بالمبادئ الأساسية لحماية البيانات:

- ربط البيانات بغرض محدد؛
- عدم تبادل المعلومات بين التطبيقات لأغراض مختلفة؛
- الحد من البيانات للقدر الأدنى المطلوب لغرض محدد؛
- حق الأشخاص في التحكم في بياناتهم PII.

ملاحظـــة – بالنسبة لبعض اللوائح الوطنية المحددة، قد يستلزم ذلك تنفيذ وظائف منفصلة لإدارة الهوية في الطبقات المختلفة لشبكات الجيل التالي.

2.6.6 السطوح البينية الخارجية واتصالات إدارة الهوية

تُستعمل السطوح البينية المعيارية المعرّفة في [التوصية ITU-T Y.2012] لتبادل بيانات الهوية بين مختلف الميادين والاتحادات الإدارية. وقد يشمل ذلك السطوح البينية التالية حسب الاقتضاء:

- السطح البيني من المستعمل إلى الشبكة (UNI)؛
- السطح البيني من الشبكة إلى الشبكة (NNI)؛
- السطح البيني من التطبيق إلى الشبكة (ANI)؛
- السطح البيني من المخدّم إلى الشبكة (SNI).

وتعتمد حلول السطح البيني على عوامل مثل التطبيق المحدد واحتياجات الخدمات (من قبيل تلبيتها في الوقت الفعلي مقابل في قرابة الوقت الفعلي) والحل البروتوكولي (من قبيل بروتوكولات لغة ترميز تأكيد الأمن (SAML)، والقطر (Diameter) ونصف القطر (RADIUS) وبروتوكول استهلال الدورة (SIP)) وآليات ونُهُج.

راجع التذييل IV للاطلاع على مثال عن سيناريو تحقيق إدارة الهوية يوضح كيف يمكن أن تكون السطوح البينية الخارجية لشبكات الجيل التالي قابلة للتطبيق.

3.6.6 نماذج المعاملات

ترد في التوصية [b-ITU-T X.1250] أوصاف لأمثلة نماذج معاملات تشارك فيها أطراف متعددة (كالمستعملين وموردي خدمات الهوية والأطراف المعولة). راجع التذييل V للاطلاع على موجز لنماذج المعاملات التي يرد وصفها في التوصية.

7 أهداف إدارة الهوية

ترد فيما يلي الأهداف العامة لإدارة الهوية:

1) تسهيل اتخاذ القرارات بشأن الثقة بين الكيانات.

2) دعم حلول لإدارة الهوية تُقلل التأثيرات على المستعملين/المشتركين إلى أدنى حد.

3) أن تقدم الحلول ذات القدرات الجديدة حلا انتقالياً مناسباً.

4) أن تُدعم حلول إدارة الهوية القابلة للتشغيل البيني ضمن ميدان مورّد شبكات الجيل التالي. ومثال ذلك، قابلية التشغيل البيني ما بين مختلف منتجات الباعة الداعمة لخدمات تطبيقات متعددة (على سبيل المثال، نقل الصوت عبر بروتوكول الإنترنت وتلفزيون بروتوكول الانترنت والفيديو والبيانات).

5) أن تُدعم حلول إدارة الهوية القابلة للتشغيل البيني لمختلف ميادين واتحادات موردي شبكات الجيل التالي ومقدمي الخدمة استناداً إلى الترتيبات والعلاقات التجارية المرعية، وفي إطار تطبيق اللوائح والسياسات الخاصة بحماية المعلومات PII.

6) أن يُدعم مد الجسور ما بين أنظمة إدارة الهوية واتحاداتها غير المتجانسة. ومثال ذلك، القدرة على مد الجسور ما بين أنظمة إدارة الهوية لمورّد شبكات الجيل التالي وغيرها من أنماط أنظمة إدارة الهوية (مثل خدمات الويب والمحتوى وأنظمة إدارة الهوية لطرف ثالث مورّد) استناداً إلى الترتيبات والعلاقات التجارية المرعية وفي إطار تطبيق اللوائح والسياسات الخاصة بحماية المعلومات PII.

7) أن يتمكن المستعملون النهائيون/المشتركون من التفاعل مع خدمات التطبيقات واستعمالها بطريقة سهلة وبديهية مع الحفاظ على السيطرة على بياناتهم الشخصية طوال دورة حياتها. ويشمل ذلك كيفية استعمال هذه المعلومات ومتى تُستعمل ومن يستعملها.

8) أن يتمكن المستعملون النهائيون/المشتركون من عدم الإفصاح عن المعلومات إلا بالحد الأدنى الضروري منها لإرساء الثقة المتبادلة وإجراء المعاملات استناداً إلى السياسات المرعية.

9) أن يتمكن المستعملون النهائيون/المشتركون من التحقق من صحة الكيان الطالب لبيانات الهوية والمعلومات التي تعرِّف صاحبها شخصياً (PII). والهدف هو أن يتمكن مستعمل نهائي/مشترك من استعمال معرفات هوية متعددة استناداً إلى السياق.

10) أن يتمكن مستعمل نهائي/مشترك من العمل على نحو مغفل أو باسم مستعار أو معروف عمداً استناداً إلى سياق التطبيق والسياسات المرعية.

8 متطلبات إدارة الهوية

تصف هذه الفقرة متطلبات إدارة الهوية المطبقة على شبكات الجيل التالي، بما يتماشى مع المتطلبات العليا لشبكات الجيل التالي التي يرد وصفها في التوصية [ITU-T Y.2201].

1.8 المتطلبات العامة

ترد فيما يلي المتطلبات العامة لإدارة الهوية:

المتطلب 1 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وظائف وقدرات إدارة الهوية لأنواع مختلفة من الكيانات التي تدعمها شبكات الجيل التالي، ومنها:

أ) المستعملون/المجموعات.

ب) المنظمات/الاتحادات/المؤسسات/مقدمو الخدمات.

ج) الأجهزة/عناصر الشبكة/الأنظمة.

د) أشياء (مثل عملية التطبيق والمحتوى والبيانات).

المتطلب 2 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم ما يلي:

أ) الإدارة الآمنة لدورة حياة هويات كيان (أي من الإصدار حتى الإلغاء).

ب) اكتشاف وتبادل معلومات الهوية على نحو آمن. ويشمل ذلك اكتشاف وتبادل معلومات الهوية التي قد تكون موجودة ضمن شبكات الجيل التالي وعبر الميادين الإدارية المختلفة.

المتطلب 3 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم إنفاذ السياسات المرعية المرتبطة بهوية كيان أو بمعلومات الهوية.

المتطلب 4 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وظائف إدارة الهوية وقدراتها في تطبيقات الوقت الفعلي (مثل نقل الصوت عبر بروتوكول الإنترنت وتلفزيون بروتوكول الانترنت) وتطبيقات الوقت الذي يكاد يكون فعلياً (مثل معاملات البيانات القائمة على شبكة الإنترنت).

المتطلب 5 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وظائف إدارة الهوية وقدراتها للسماح بالتأكيد المغفل لمعلومات الهوية (مثل الهوية والنعوت)، رهناً بالسياسة المرعية.

المتطلب 6 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم العمل البيني الآمن لإدارة الهوية بين عناصر الشبكة ضمن ميدان مورّد شبكات الجيل التالي (أي داخل الشبكة) وبين ميادين الموردين المختلفين (مثل مورّد غير شبكات الجيل التالي ومقدمي خدمات الإنترنت).

المتطلب 7 يترتب على شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم خدمات تيسير الاستعمال على المستعملين النهائيين وميزات من قبيل:

أ) تسجيل واحد للدخول/الخروج إلى/من خدمات التطبيق المتعددة.

ب) الخدمات المتقاربة (مثل تقارب الخدمتين الثابتة والمتنقلة).

ج) التحكم في معلومات تعرِّف صاحبها شخصياً (PII) وحمايتها.

المتطلب 8 يترتب على مورد شبكة الجيل التالي/مورد خدمة الهوية (NGN/IdSP) دعم تسجيل الدخول لمرة واحدة إلى التطبيقات التي تستعمل أوراق اعتماد ترتبط بجهاز مشترك (مثل أوراق اعتماد UICC) أو أوراق اعتماد ترتبط بمستعمل/مشترك (مثل أوراق اعتماد تنظيم بروتوكول استهلال الدورة)، حسب الحالة، استناداً إلى المتطلبات الأمنية للتطبيقات، وتحديداً:

- يجب أن تتوفر إمكانية استعمال أوراق اعتماد المشترك (مثل أوراق اعتماد تنظيم بروتوكول استهلال الدورة) لدعم تسجيل الدخول لمرة واحدة إلى التطبيقات التي يتم النفاذ إليها عبر أجهزة متنقلة.
- يجب أن تتوفر إمكانية استعمال أوراق اعتماد المشترك (مثل أوراق اعتماد تنظيم بروتوكول استهلال الدورة) لدعم تسجيل الدخول لمرة واحدة إلى التطبيقات التي يتم النفاذ إليها عبر أجهزة ثابتة.

2.8 متطلبات إدارة دورة حياة الهوية

تنطوي إدارة دورة حياة هوية على العملية والإجراءات المرتبطة بانتساب معلومات هوية وإصدارها (مثل معرفات الهوية والمستندات والنعوت).

المتطلب 9 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) وضع وتنفيذ سياسات تطبَق لإدارة دورة حياة هوية. ويشمل ذلك العمليات والإجراءات والسياسات الرامية إلى تدقيق بيانات هوية ما وتنسيبها وإصدارها وإلغائها.

1.2.8 الانتساب والإصدار

يبدأ تنسيب هوية لكيان (مثل مشترك أو جهاز أو منظمة أو مورّد شبكة الجيل التالي أو شيء) في سياق ما بتدقيق الهوية أو المستندات وتنسيبها. والتنسيب هي العملية اللازمة لتدشين هوية في سياق ما وتتضمن تسجيل هوية الكيان وربما تخصيص

نعوت محددة (مثل معرفات الهوية) أو مستندات أو أدوار. وفي حال كون المشتركين من المستعملين النهائيين، فهذه هي العملية التي يتقدم صاحب الطلب فيها بطلبه ليصبح مشتركاً لدى مورد خدمة الهوية أو مورّد شبكة الجيل التالي.

ويتضمن التدقيق التحقق والتأكد من صلاحية النعوت، وربما المستندات ذات الصلة.

المتطلب 10 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) التحقق والتأكد من صلاحية هوية الكيان أثناء التنسيب، طبقاً لمتطلبات السياق. ويخضع تسجيل هوية الكيان وتخصيص المعرفات والمستندات والنعوت لسياق محدد لعملية تحقق ناجحة من معايير وسياسات التدقيق المطبقة.

حيث يتعين أن تستند عملية التدقيق وسياساته إلى قيمة الموارد (ومثال ذلك، الخدمات والمعاملات والمعلومات والامتيازات) التي تسمح بها الهوية والمخاطر المرتبطة بحصول كيان غير مخول له على الهوية واستخدامه لها. وعلى وجه التحديد، يتعين اتخاذ تدابير لضمان ما يلي:

- وجود كيان (كشخص أو منظمة أو كيان قانوني) بالنعوت المزعومة، وملاءمة هذه النعوت لتمييز الكيان بشكل كاف طبقاً لاحتياجات السياق.
- أن صاحب الطلب الذي تسجل هويته هو فعلاً الكيان المربوط عليه الهوية.
- أن يصعب على كيان يكون قد استعمل الهوية والمستندات المسجلة أن يتنصل لاحقاً من التسجيل/الانتساب وأن يطعن في استيقان.

يتوّج نجاح اكتمال عملية الانتساب والتدقيق بتسجيل الهوية التي قد تتضمن النعوت و/أو المستندات المخصصة، حيث يمكن الاستيقان من الكيان بموجبها مستقبلاً.

المتطلب 11 يتعين عدم إصدار معلومات الهوية (مثل المعرفات والمستندات والنعوت) المرتبطة بهوية ما إلا بعد نجاح تدقيق بيانات هوية الكيان.

وفي بعض السيناريوهات، قد ينطوي ذلك على تسجيل وإصدار مستندات إلكترونية وإسناد شارات إلى هوية أو التقدم بادعاء (أي نعت) بشأن هوية. وتبعاً لنمط الشارة المستعملة، إما أن تُستحدث شارة جديدة من قبل مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) وتورَّد إلى المشترك، أو أن يُطلب إلى المشترك أن يسجل الشارة التي يملكها صاحب الطلب بالفعل أو التي استحدثها مؤخراً.

المتطلب 12 في كلتا الحالتين، يتعين تأمين آلية لنقل الشارة من منطلقها إلى الطرف الآخر لضمان الحفاظ على سرية وسلامة الشارة حديثة النشأة.

2.2.8 الصيانة والتحديثات

بعد تسجيل وإصدار هوية (أو هويات) بما في ذلك أي معلومات عنها (معرفات الهوية والمستندات والنعوت)، تقع على عاتق مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) والمشترك كليهما مسؤوليات أثناء مرحلة التشغيل والاستعمال للحفاظ على أمن الهوية.

المتطلب 13 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) القيام، على نحو آمن، بإدارة وصيانة البيانات وصفة البيانات (مثل معرفات الهوية والمستندات والنعوت) المرتبطة بهوية.

المتطلب 14 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) القيام، على نحو آمن، بإدارة وتدوين أي تحديثات أو تعديلات تُدخل على هوية (أو هويات).

المتطلب 15 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) القيام، بصفة دورية، بالتحقق من صحة صفة الهوية.

المتطلب 16 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم إجراءات تقديم البلاغات بشأن التحديثات أو التعديلات على هوية (أو هويات) أو على البيانات المرتبطة بها إلى الأنظمة وعناصر الشبكة التي تحتاج لأن تكون على علم بالتحديثات أو التغييرات.

المتطلب 17 يترتب على مورد شبكة الجيل التالي/مورد خدمة الهوية (NGN/IdSP) توفير وظائف لإبلاغ المستعمل ببيانات هوية أو بتغييرها أو بحذفها.

كما يتولى المشترك مسؤولية أمن المستندات المخصصة على أساس الاتفاقات التجارية والسياساتية مع مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP). فمن مسؤوليات المشترك مثلاً أن يدير مستنداته الإلكترونية (ومثالها الشارات) وأن يبقيها آمنة.

المتطلب 18 يترتب على مورد شبكة الجيل التالي/مورد خدمة الهوية أن يتخذ تدابير على أساس الاتفاقات التجارية والتعاقدية لضمان قيام أي كيان (أي مشترك) أو مورد شبكة NGN/مورد خدمة هوية آخر بإدارة واستعمال المستندات الصادرة له (كالشهادات الرقمية أو الشارات) المرتبطة بهوية بشكل آمن طبقاً للسياسات واللوائح.

3.2.8 الإلغاء

إلغاء الهوية هو عملية إبطال الهوية والمستندات المرتبطة بها. ومن مسؤولية الطرف أو النظام الذي (مثل مورد شبكة NGN/مورد خدمة الهوية) الذي يدير الهوية أو المستندات أن ينهيها أو يوقف العمل بها. ويلزم الإلغاء لمنع الاستخدام المستمر للهوية أو المستندات التي لم تعد صالحة أو التي اختُرقت أمنياً.

المتطلب 19 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) وضع وتنفيذ سياسات تُطبّق لإلغاء هوية (أو هويات). وعلى وجه التحديد، يتعين دعم قدرات إنهاء أو إتلاف المستندات (كالشهادات الرقمية أو الشارات) عندما تنتهي صلاحية هذه المستندات أو تُخترق أمنياً.

المتطلب 20 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم إجراءات التبليغ عن إلغاء أو إنهاء هوية (أو هويات) أو أي من البيانات المرتبطة بها إلى الكيان والأنظمة وعناصر الشبكة التي تحتاج لأن تكون على علم بالأمر (أي يجب تبليغ جميع الأنظمة والعمليات التي يمكن للهوية استخدامها للنفاذ بانتهاء صلاحية الهوية).

3.8 وظائف التشغيل والإدارة والصيانة والتزويد في إدارة الهوية

1.3.8 نموذج البيانات ومخططها

يمكن لكل مورّد شبكات الجيل التالي أو اتحاد أو مؤسسة أن يكون لهم ما يخصهم من أنساق أو تعاريف أو مخططات يمثلون بها البيانات والمعلومات المتعلقة بالهوية ويطلعون الآخرين عليها. وتوضح الفقرة 1.2.8 من التوصية [ITU-T Y.2720] الحاجة إلى إمكانية التشغيل البيني ما بين أنظمة إدارة الهوية غير المتجانسة باستعمال نماذج وهياكل ومخططات مختلفة للبيانات.

المتطلب 21 يترتب على مورّد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وظائف وقدرات تتيح إمكانية التشغيل البيني ما بين أنظمة إدارة الهوية غير المتجانسة التي تستعمل نماذج وهياكل ومخططات مختلفة للبيانات حسب الحاجة.

2.3.8 إدارة بيانات الهوية

توضح الفقرة 2.8 من التوصية [ITU-T Y.2720] الحاجة إلى إدارة بيانات الهوية (كإدارة معرفات الهوية والمستندات والنعوت). أما المتطلبات التفصيلية لإدارة بيانات الهوية فهي خارج نطاق هذه التوصية.

وفي شبكات الجيل التالي، يمكن لبيانات الهوية المختلفة (مثل المعرفات كعنوان البريد الإلكتروني وأرقام الهاتف ومعرفات الموارد الموحدة (URI) وعناوين بروتوكول الإنترنت) أن تدار بأنظمة إدارة وعمليات تشغيلات مختلفة (ومثالها نظام دعم التشغيلات (OSS)/نظام دعم الأعمال (BSS)). وتوفّر المتطلبات العامة التالية في سياق توفير نهج مهيكل ومنسق للتفاعل بين مختلف أنظمة الإدارة أنظمة العناية بالزبائن دعماً لخدمات إدارة الهوية وقدراتها.

المتطلب 22 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم سطح بيني معياري (مثل بوابة الزبون) للسماح للمستعملين النهائيين/المشتركين بالتفاعل مع الأنظمة والعمليات المطبقة لإدارة شبكات الجيل التالي دعماً لمعاملات إدارة بيانات الهوية (مثل التغييرات والتحديثات)، طبقاً للوائح والسياسات المطبقة لحماية البيانات.

المتطلب 23 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم ما يلزم من السطوح البينية والوظائف والقدرات لتسهيل اتساق المعاملات ومجريات العمل بين مختلف أنظمة وعمليات الإدارة المتصلة بإدارة بيانات الهوية (مثل التغييرات والتحديثات التي تمر عبر مختلف أنظمة دعم التشغيلات/دعم الأعمال وأنظمة العناية بالزبائن ومنصات خدمات التطبيق) حسب مقتضى الحال، طبقاً للوائح والسياسات المطبقة لحماية البيانات.

المتطلب 24 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وظائف وقدرات تدوين وتخزين (على غرار البيانات الرديفة) سجلات المعاملات ذات الصلة بإدارة بيانات الهوية، طبقاً للوائح والسياسات المطبقة لحماية البيانات.

المتطلب 25 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وظائف وقدرات مزامنة تغييرات وتحديثات بيانات الهوية ما بين مختلف أنظمة وعمليات الإدارة حسب الاقتضاء، طبقاً للوائح والسياسات المطبقة لحماية البيانات.

المتطلب 26 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وظائف وقدرات التحقق من الروابط بين بيانات الهوية المرتبطة بكيان (مثل المشترك) والخدمات المتعاقد عليها (مثل النفاذ والصوت والبيانات والفيديو)، طبقاً للوائح والسياسات المطبقة لحماية البيانات.

4.8 وظائف التشوير والتحكم

1.4.8 اكتشاف معلومات الهوية

في بيئة شبكات الجيل التالي الموزعة، قد توجد معلومات الهوية في مختلف عناصر الشبكة (ومثالها، مخدّم الاشتراك ومخدّم الموقع ومخدّم الحضور ومخدّم الاشتراك المنزلي، وما إلى ذلك). فكي يستفيد التطبيق من معلومات الهوية، فإنه يحتاج إلى معرفة أنها موجودة وأين يجدها.

المتطلب 27 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وظائف وقدرات اكتشاف مصادر معلومات الهوية ضمن ميدان مورد شبكة الجيل التالي/مورد خدمة الهوية. ومثال ذلك، وظائف مخدّم إدارة الهوية وقدراته في اكتشاف وجود معلومات الهوية في العناصر الأخرى للشبكة مثل مخدّمات الموقع أو الحضور أو الاشتراك؛ أو وظائف وقدرات تطبيق/خدمة في اكتشاف إدارة الهوية أو المخدّمات الأخرى الحاضنة لبيانات الهوية.

المتطلب 28 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وظائف وقدرات استعمال السطوح البينية والبروتوكولات المعيارية لاكتشاف مصادر معلومات الهوية عبر الميادين المختلفة لمورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP). ومثال ذلك، استعمال السطوح البينية والبروتوكولات المعيارية لاكتشاف مصادر معلومات الهوية في ميدان آخر لمورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) على أساس الاتفاقات المرعية بين الشبكات.

المتطلب 29 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم قدرات حماية مقدرات وآليات الاكتشاف.

2.4.8 التحكم في النفاذ إلى معلومات الهوية

ينبغي أن تكون بيانات الهوية متاحة فقط للكيانات المخوّل لها بالنفاذ إلى تلك المعلومات.

المتطلب 30 يتعين ألا تتاح معلومات الهوية إلا للكيانات المخوّل لها، رهناً باللواح والسياسات المرعية. وعلى وجه التحديد:

- يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) الاستيقان من الكيان (مثل الطرف المعول) الطالب لبيانات الهوية أو تنفيذ استيقان متبادل.
- يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) استيقان كيان (مثل الطرف المعول أو الطرف الطالب) يطلب بيانات الهوية والتحقق من تخويله والتأكد من صلاحيته، قبل إتاحة النفاذ إلى المعلومات أو تبادل بيانات الهوية مع الطرف الطالب.

3.4.8 اتصالات إدارة الهوية

تحتاج أنظمة الشبكة وعناصرها لإقامة دورات لتبادل معلومات الهوية (مثل معرفات الهوية والمستندات والنعوت) الواقعة في أنظمة شبكية مختلفة (مثل مخدّم إدارة الهوية ومخدّم الاشتراك ومخدّم الموقع ومخدّم الحضور، وما إلى ذلك) بحيث يمكن الربط بينها والتحقق منها (بواسطة مخدّم تطبيقات إدارة الهوية الذي يوفر وظائف الاستيقان والارتباط) لتقديم قدرات ضمان الهوية.

ويمكن لمورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdP) موافاة الأطراف المعولة بتأكيدات الهوية والنعوت المرتبطة بها (مثل الادعاءات والامتيازات) كي تتخذ هذه الأطراف، على سبيل المثال، قرارات التحكم في النفاذ. ويتيح ذلك لمختلف خدمات التطبيق (أي المقدمة من منصات باعة مختلفين) استعمال خدمة مشتركة متاحة لإدارة الهوية على النقيض من حلول مستقلة وقائمة بذاتها. وتشمل علاقات الاتصالات التي يتعين النظر فيها ما يلي:

- داخل الشبكة: اتصالات مع ميدان مورّد شبكات الجيل التالي (بين عناصر الشبكة مثلاً).
- بين الشبكات: الاتصالات بين مورّدين مختلفين لشبكات الجيل التالي.
- الاتحاد: اتصالات بين أعضاء الاتحاد.

1.3.4.8 الاتصالات في الوقت الفعلي وفي الوقت القريب من الوقت الفعلي

إن الحل الذي يُلجأ إليه لاكتشاف وتبادل معلومات الهوية يجب أن يأخذ في الاعتبار ما إذا كانت الاتصالات المطلوبة تجري في الوقت الفعلي أم في الوقت القريب من الوقت الفعلي. ومن شأن ذلك أن يعتمد على التطبيقات المحددة الجاري دعمها. فقد تحتاج بعض التطبيقات (مثل نقل الصوت عبر بروتوكول الإنترنت وتلفزيون بروتوكول الإنترنت) إلى التحقق من صحة هوية المستعمل/المشترك الطالب وإلى تخويل خدمة التطبيق. ومن التطبيقات الأخرى (مثل خدمات البيانات والمراسلة) ما لا يحتاج إلا لدورات اتصالات في الوقت القريب من الوقت الفعلي للتحقق من صحة هوية المستعمل/المشترك الطالب وتخويل خدمة التطبيق.

المتطلب 31 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم قدرات لإقامة دورات الاتصالات وفقاً لمتطلبات خدمة تطبيق معينة لتبادل معلومات الهوية في الوقت الفعلي وفي الوقت القريب من الوقت الفعلي. ويشمل ذلك دورات الاتصالات لتبادل معلومات الهوية ضمن ميدان مورّد شبكات الجيل التالي، وبين مورّدين مختلفين لهذه الشبكات، وبين أعضاء اتحاد.

ويمكن أن تتناول معلومات النعت، على سبيل الذكر لا الحصر، صفة العضوية والوظائف التابعة (الفوترة والعمليات) والنعوت التي تستخدمها خدمات أخرى (مثل خدمة الدليل أو خدمة الشهادة). ويتيح ذلك للطرف المعول أن يقدم معلومات ومحتويات حسب الطلب إلى المستعملين استناداً إلى نعوتهم.

المتطلب 32 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) والطرف المعول أن يتبادلا التأكيدات المرتبطة بهوية كيان. ويشمل ذلك تأكيد النعوت.

4.4.8 الارتباط والإسناد

يمكن أن تترابط معلومات الهوية (مثل معرفات الهوية والمستندات والنعوت) لإقامة إسناد يضمن هوية كيان. فعلى سبيل المثال، يمكن أن تتلازم معلومات الهوية، المرتبطة بمشترك (مثل هوية المستعمل (UserID)) وبجهاز المشترك (مثل هوية الجهاز (DeviceID)) وبالمعلومات الأخرى ذات الصلة مثل الموقع وبيانات النموذج، لإسناد درجة أعلى من الضمان لهوية المشترك (أي الثقة في صحة الهوية).

المتطلب 33 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم القدرات اللازمة لربط أجزاء متعددة من البيانات المتصلة بالهوية (مثل الموقع والنموذج) ودعم إقامة الإسناد المناسب لهوية الكيان طبقاً للوائح والسياسات المطبقة لحماية البيانات. ويستلزم استعمال هذه القدرات الحصول على موافقة محددة وصريحة من المستعمل.

ملاحظـــة – ربما تُقيّد بعض اللوائح والسياسات الوطنية لحماية البيانات دعم هذا المتطلّب.

5.4.8 متطلّبات الاستيقان

الاستيقان هو عملية إرساء الثقة في الارتباط بين هوية ما والكيان. وتتمثل إحدى طرائق تحقيق ضمان الاستيقان في إيضاح الأهداف والمبادئ التوجيهية اللازمة للتحديد الكمي للمخاطر التي ينطوي عليها كون كيان ما، من أو ما يدعي كونه. ويشمل ذلك تبيان أي من معرّفات الكيان أهم من غيرها في عملية تحديد الهوية، ودواعي عدم إيلاء القيمة الاستيقانية نفسها لمعرفات معينة تُستعمل في الاستيقان.

راجع التوصية [ITU-T Y.2702] للاطلاع على متطلبات الاستيقان من شبكات الجيل التالي.

وفيما يلي المتطلبات الأمنية للجوانب الاستيقانية في إدارة الهوية:

المتطلب 34 يجب أن يتسنّى الاستيقان المتبادل بين الكيانات (مثل مستعملي، موردو شبكة NGN/مورد خدمة الهوية، طرف معول).

المتطلب 35 يتعين أن يتمكن طرف معول من إرسال طلبات إلى مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) للاستيقان من كيان (كالمستعمل/المشترك).

المتطلب 36 يتعين أن يكون بمقدور مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم الاستيقان من كيان (كالمستعمل/المشترك) وموافاة الطرف المعول بالضمانات.

المتطلب 37 يتعين أن يتمكن طرف معول من طلب إعادة الاستيقان من كيان مع توصيف الطريقة الحالية أو البديلة لإعادة الاستيقان المطلوبة.

6.4.8 ضمان الاستيقان

ضمان الاستيقان هو درجة الثقة في عملية الاستيقان التي يكون فيها شريك الاتصال هو الكيان الذي يدعيه أو يتوقع أن يكونه. وتقوم الثقة على درجة من الثقة في الارتباط بين الكيان المتصل والهوية المقدمة. وتختلف احتياجات الكيانات (مثل، المستعملين وخدمات التطبيق وغيرها) من حيث ضمان الاستيقان حسب السياق. فهناك حالات تتطلب مقادير مختلفة من قوة الاستيقان للنفاذ إلى موارد مختلفة تبعاً لحساسية وقيمة معلومات المعاملات المتوقعة. وفي مثل هذه الحالات، تدعو الحاجة الأطراف المعولة (مثل المستعملين ومورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) إلى تفاصيل (من قبيل طرائق الاستيقان وعدد عوامله وسياقاته، وغير ذلك) أكثر من المعتاد لضمان الوفاء بالاستيقان المتوقع. وينطوي ذلك على تقييم المخاطر المحتملة المرتبطة بعواقب أخطاء الاستيقان، أو لتحديد المستوى المناسب للضمان في هوية كيان. أما أخطاء الاستيقان التي يمكن أن تستتبع عواقب أسوأ فهي تتطلب مستويات أعلى من الضمان.

المتطلب 38 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم طريقة (أو طرائق) الاستيقان المناسبة حسب ما يلزم من مستوى (أو مستويات) الضمان.

المتطلب 39 يتعين أن يتمكن طرف معول من أن يبين لمورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) مستوى الضمان اللازم للاستيقان من كيان.

المتطلب 40 يتعين أن تتاح إمكانية التفاوض على مستوى الضمان بين مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) والطرف المعول والكيان الذي يجري الاستيقان منه.

1.6.4.8 ضمان هوية وسلامة جهاز المستعمل

ستدعم شبكات الجيل التالي مجموعة متنوعة من أجهزة المستعمل (ومثالها، الهواتف الثابتة والمهتفات اللاسلكية والحواسيب الشخصية والمساعد الشخصي الرقمي والوحدات الطرفية للمشتركين في تلفزيون بروتوكول الإنترنت). وتتراوح مكونات العتاد والبرمجيات في الأجهزة المرفقة بشبكات الجيل التالي من البسيط إلى المعقد. وإذا ما سُرقت واختُرقت، يمكن استعمالها لتنسيق مجموعة متنوعة من الهجمات. ومن المعروف أن شبكات الجيل التالي سيكون عليها أيضاً دعم أجهزة (على غرار المطاريف البكماء أو أجهزة الخدمة POTS) والتي لن يكون بمقدورها توفير درجة الحماية اللازمة.

المتطلب 41 يتعين أن يكون بمقدور مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم أجهزة المستعمل النهائي ذات القدرات الأمنية والتي تكون بيانات إدارة الهوية الخاصة بها مجفرة (ومثالها، كلمات المرور والمفاتيح الرقمية والشهادات) في مكونات العتاد المقاومة للعبث.

المتطلب 42 يتعين أن يكون بمقدور مورد شبكة الجيل التالي/مورّد الهوية (NGN/IdSP) الاتصال مع القدرات الأمنية في مكونات العتاد المقاومة للعبث في جهاز المستعمل النهائي عبر سطوح بينية مقيّسة لدعم خدمات التطبيق الأمني التي تعتمد على مكون العتاد المقاوم للعبث والمحدد كمرتكز ثقة لتعرف وضمان هوية جهاز المستعمل النهائي بصورة متفرّدة.

أما التطبيقات التي تنفذ على أجهزة المشتركين للسماح لهم بالتفاعل مع الخدمات والمميزات المحلية للجهاز، فيمكنها أن تؤثر بصورة سلبية على سلامة الجهاز. ويمكن لتطبيقات الإنترنت الشائعة مثل متصفحات الويب والبريد الإلكتروني أن تُدخل نقاط ضعف تنال من سلامة أجهزة المشترك. ومن شأن تحميل البرمجيات والملفات، لا سيما من مصدر غير موثوق، أن يعرّض أجهزة المشترك لخطر الشفرات الخبيثة والديدان والفيروسات وأحصنة طروادة. ويمكن أن يصمَم مكون العتاد المتخصص المقاوم للعبث وينفَذ في جهاز المستعمل النهائي ليوفر التحقق من سلامة الجهاز. فعلى سبيل المثال، قد يحوي مكون العتاد المتخصص المقاوم للعبث خوارزميات ووظائف خاصة بالبائع للتفتيش عن الخروق التي تنال من السلامة. فقد يتضمن هذا المكون نموذجاً مرجعياً بمجموعة من مقاييس السلامة المعروفة جيداً التي تتعرف على الشفرة الصحيحة تحديداً وتوفر قيماً مرجعية للجهاز. فتُستعمل هذه المقاييس لمقارنة القيم الفعلية مع التشكيلة للوقوف على ما إذا كانت الوحدة ضمن حدود الالتزام.

المتطلب 43 يتعين أن يكون بمقدور مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم أجهزة المستعمل النهائي المزودة بمكون العتاد المتخصص المقاوم للعبث كي توفر للتطبيقات والخدمات مرجعيات السلامة وتأكيداً بامتثال الأجهزة لمعايير السلامة.

المتطلب 44 يتعين أن يكون بمقدور مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) الاتصال مع القدرات الأمنية في مكون العتاد المقاوم للعبث في جهاز المستعمل النهائي عبر سطوح بينية مقيّسة لدعم خدمات التطبيق الأمني التي تعتمد على مرجعيات السلامة وعلى التأكيد بامتثال الجهاز لمعايير السلامة.

وإذ يمكن لفقدان أو سرقة جهاز يحوي معلومات تعرِّف صاحبها شخصياً وبيانات حساسة أخرى أن يجر عواقب وخيمة على الأفراد وقطاع الأعمال والمؤسسات الحكومية، فإن مكون العتاد المتخصص المقاوم للعبث والمصمم لتحديد هوية الأجهزة الموثوقة على نحو تنفرد به عن سواها يمكنه أيضاً دعم قدرات محتملة لتجفير وحماية معلومات تعرِّف صاحبها شخصياً وبيانات حساسة أخرى في أجهزة المستعمل النهائي.

المتطلب 45 يتعين أن يكون بمقدور مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم أجهزة المستعمل النهائي المزودة بمكون العتاد المتخصص المقاوم للعبث كي تجفّر وتحمي معلومات تعرِّف صاحبها شخصياً وبيانات حساسة أخرى في أجهزة المستعمل النهائي.

7.4.8 دعم خدمات تتطلب أولوية في المعاملة

يتعين على أنظمة إدارة الهوية وقدرات شبكات الجيل التالي أن تدعم خدمات التطبيق ودورات الاتصالات التي تتطلب أولوية في المعاملة بالنسبة إلى الخدمات الأخرى. وتصف التوصية [ITU-T Y.2205] الاتصالات في حالات الطوارئ (ET) التي تستدعي معالجة خاصة من شبكات الجيل التالي. ويرد في التوصية [ITU-T E.107] مثال محدد عن خدمة الاتصالات في حالات الطوارئ (ETS). إذ تستفيد هذه الخدمة من قدرات إدارة الهوية المستعملة لخدمات عادية (ومثالها، ضمان الهوية واكتشاف الهويات الموثوقة). ولذلك، لا بد لأنظمة إدارة الهوية من أن تدعم الوظائف والقدرات اللازمة للاعتراف بالأولوية في المعاملة وتقديمها عند إقامة ومواصلة نداء/دورة في الاتصالات في حالات الطوارئ على أساس القواعد والسياسات المرعية على الصعيد الوطني. راجع التوصيتين [ITU-T E.107] و[ITU-T Y.2205] للاطلاع على معلومات بشأن الخدمات والقدرات التي تتطلب أولوية في المعاملة.

المتطلب 46 يترتب على أنظمة إدارة الهوية لدى مورد شبكة الجيل التالي/مورد خدمة الهوية (NGN/IdSP IdM) أن تدعم الوظائف والقدرات اللازمة للاعتراف بالأولوية في المعاملة وتقديمها عند إقامة ومواصلة نداء/دورة في الاتصالات في حالات الطوارئ على أساس القواعد والسياسات المرعية على الصعيد الوطني.

المتطلب 47 يتعين على عناصر شبكة إدارة الهوية وقواعد البيانات المستخدمة لدعم نداءات/دورات الاتصالات في حالات الطوارئ أن تولي أولوية في المعاملة على أساس القواعد والسياسات المرعية على الصعيد الوطني. ويشمل ذلك الاتصالات التالية، دون أن يقتصر عليها:

- اتصالات إدارة الهوية ضمن الشبكة (مثل التفاعلات ضمن نظام إدارة الهوية المورّد لشبكات الجيل التالي).
- اتصالات إدارة الهوية ضمن الشبكة (مثل التفاعلات بين نظامي توريد لشبكات الجيل التالي استناداً إلى الاتفاقات والسياسات الثنائية).
- اتصالات إدارة الهوية الاتحادية (مثل التفاعلات بين أعضاء الاتحادات على أساس القواعد والسياسات المرعية بشأن الهوية الاتحادية).

راجع التذييل III للاطلاع على أمثلة عن حالات استعمال تتصل بالاتصالات في حالات الطوارئ.

5.8 وظائف الهوية الاتحادية في إدارة الهوية

ينطوي الاتحاد على إقامة علاقة بين كيانين أو أكثر أو إنشاء رابطة تضم أي عدد من مقدمي الخدمات وموردي الهويات. ويتمثل المفهوم العام للاتحاد في السماح لكل عضو فيه بالبقاء مستقلاً مع تيسير تبادل معلومات محددة بشأن الهوية لإتاحة خدمات اتحادية. فعلى سبيل المثال، يمكن لمعلومات معينة عن هوية مستعمل/مشترك (كمجموعة فرعية من البيانات العامة لمشترك مثلاً) أن تتخذ صفة اتحادية (أي أن تتاح لأعضاء الاتحاد) على أن تتقيد بسياسات وشروط الاتحاد ولوائحه وسياساته الخاصة بحماية البيانات. وتتيح الهوية الاتحادية إمكانية حمل ونقل معلومات الهوية عبر ميادين أمنية مستقلة بذاتها في شؤونها الأخرى ولكنها تتقيد بسياسات وشروط الاتحاد، وتخضع للقواعد واللوائح والسياسات المرعية. وتمكّن الهوية الاتحادية المستعملين في ميدان ما من النفاذ الآمن إلى بيانات أو أنظمة ميدان آخر مستغنين عن إدارة المستعملين الفائضة تماماً عن الحاجة.

المتطلب 48 يتعين أن يكون بالإمكان اكتشاف وتبادل معلومات الهوية الاتحادية بين أعضاء الاتحاد، مع مراعاة القواعد واللوائح والسياسات المرعية.

المتطلب 49 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم قدرات تمكّن مشترك من تقديم التخويل اللازم لإعطاء الصفة الاتحادية لهوياته.

المتطلب 50 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم قدرات تتيح لمشترك خيار إنهاء مشاركته في جميع خدمات وتطبيقات الهوية الاتحادية، أو في فئات محددة منها، وتتيح للاتحاد إنهاء هوياته.

المتطلب 51 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم قدرات تمكّن مشترك من تحديد المسموح والممنوع فيما يتعلق بمعلومات هويته الاتحادية. ويتعين أن يتمكن المشتركون من التحكم في مسألة أي من البيانات الشخصية تعطى ولمن تعطى ولأي أغراض تعطى.

ملاحظـــة – إن متطلبات حماية المعلومات التي تعرّف صاحبها شخصياً الواردة في الفقرة 6.8) تطبَق أيضاً على الهوية الاتحادية.

ويمكن عموماً أن يكون لكل مورّد لشبكات الجيل التالي أو مؤسسة أو عضو اتحاد ما يخصهم من أنساق أو مخططات أو تعاريف أو دلالات لتمثيل البيانات والمعلومات المتعلقة بالهوية ولتبادلها مع الجهات الأخرى. فيمكن لنظامين مختلفين مثلاً أن يمثلا المعلومة نفسها مثل تاريخ ميلاد بطريقتين مختلفتين. كما يمكن أن تختلف الدلالات والمخططات والتكنولوجيات والآليات المستخدمة لتمثيل المعلومات ذات الصلة بالهوية وطلبها وتبادلها، مما يؤدي إلى مشاكل في التشغيل البيني. ولذلك، تقتضي الضرورة قدرات مناسبة تسمح بمد جسور بين الاتحادات الموثوقة وبعملها البيني.

المتطلب 52 يتعين أن يكون بالإمكان تحقيق مد الجسور والتشغيل البيني ما بين اتحادات موثوقة تستعمل أنظمة مختلفة لإدارة الهوية وللدلالات والمخططات والآليات والتكنولوجيات. فيتعين مثلاً أن يتاح العمل البيني والتشغيل البيني لأطراف معولة في ميادين مختلفة (مثل ميدان شبكات الجيل التالي وخدمات الويب/الإنترنت) تستعمل قدرات وتكنولوجيات مختلفة لإدارة الهوية. ويتعين، على وجه الخصوص، ضمان الإرسال الآمن لمعلومات الهوية الاتحادية.

6.8 وظائف المستعمل/المشترك وحماية المعلومات التي تعرّف بأصحابها شخصياً

يتعين تزويد المستعملين/المشتركين بسطوح بينية وقدرات متعارف عليها ليتحكموا في المعلومات التي تعرّف بهم شخصياً ويتخذوا قرارات مستنيرة ويوافقوا فيما يتعلق ببياناتهم الشخصية. وينبغي أن يتمكن المستعملون/المشتركون من التعبير عن سياسات الخصوصية الخاصة بهم والنواحي المفضلة لديهم، والتفاوض على شروط الكشف عن البيانات مع مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP).

وينبغي ألا يُكشف عن البيانات الشخصية إلا للكيانات المخول لها بذلك استناداً إلى السياسات المرعية (من قبيل موافقة المستعمل/المشترك، والقواعد التنظيمية الحكومية). وبالإضافة إلى ذلك، ينبغي الإقلال إلى أدنى حد من جمع المعلومات التي تعرّف بأصحابها شخصياً ومن تخزينها واستخدامها، وينبغي الالتزام بالسياسات المرعية.

المتطلب 53 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) توفير خدمات إدارة الهوية وحماية سرية المعلومات التي تعرّف بأصحابها شخصياً طبقاً للوائح والسياسات والقواعد المرعية.

المتطلب 54 يتعين أن يتمكن المستعملون/المشتركون من إعلام مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) بما يفضلونه فيما يتعلق ببياناتهم الشخصية (بمجموعة من أفضليات الخصوصية مثلاً) وفقاً للوائح والسياسات المرعية (ومثال ذلك، موافقة الأفراد المعلنة أو سياسات الموردين أو القواعد التنظيمية).

المتطلب 55 يتعين أن يتمكن المستعمل/المشترك من التحقق من أصالة الكيان الطالب للمعلومات التي تعرّف بأصحابها شخصياً قبل تقديم المعلومات المطلوبة.

المتطلب 56 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) حذف المعلومات التي تعرّف بأصحابها شخصياً عند الوفاء بالأغراض المحددة من جمع البيانات والاحتفاظ بها على أساس اللوائح والسياسات والقواعد المرعية.

المتطلب 57 يتعين أن يتمكن المستعمل النهائي/المشترك من التشغيل بهوية مغفلة أو مستعارة تبعاً لسياق التطبيق واللوائح والسياسات والقواعد المرعية.

7.8 الأمن

لَئِن كانت معلومات وبيانات الهوية بالغة الحساسية، فهي مستهدفة من الدخلاء. وبما أن خدمات وقدرات إدارة الهوية ستُستعمل للتحكم في النفاذ إلى التطبيقات التجارية والحكومية وإلى تطبيقات الشبكات الاجتماعية، فإن الهجمات

والاقتحامات الأمنية ستستهدف عناصر وأنظمة الشبكة (مثل عناصر الشبكة وقواعد البيانات الداعمة لوظائف إدارة الهوية وقدراتها). ولذلك، يجب تنفيذ التدابير الأمنية المناسبة لتأمين وحماية عناصر الشبكة والأنظمة التي توفر وظائف إدارة الهوية وخدماتها وقدراتها.

1.7.8 التحكم في النفاذ إلى النظام والبيانات

ينطوي التحكم في النفاذ إلى النظام على إجراءات أمنية لمنع النفاذ غير المخوّل به إلى عناصر الشبكة والأنظمة ونقاط النفاذ المرتبطة بها. وثمة تهديدات ترتبط بالنفاذ غير المخوّل به إلى عناصر الشبكة والأنظمة الداعمة لوظائف إدارة الهوية وقدراتها وبياناتها. ومن ثم، لا بد من وضع وإنفاذ الإجراءات المناسبة للتحكم في النفاذ للحؤول دون النفاذ غير المخوّل به.

المتطلب 58 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم إجراءات التحكم في النفاذ إلى النظام وإنفاذها لمنع النفاذ غير المخوّل به إلى عناصر الشبكة والأنظمة الداعمة لوظائف إدارة الهوية وقدراتها. ويتعين على مورد شبكة الجيل التالي/مورّد خدمة الهوية عدم السماح لكيان بالنفاذ إلى عناصر الشبكة وقواعد البيانات الداعمة لوظائف إدارة الهوية وقدراتها ما لم تُحدد هوية الكيان ويُتأكد من صحتها ويخوَّل لها بالنفاذ. وينطبق ذلك على جميع الكيانات (أي الأشخاص والعمليات والأنظمة البعيدة).

وينطوي التحكم في النفاذ إلى البيانات على إجراءات أمنية لمنع النفاذ غير المخوّل به إلى البيانات المخزنة أو المزودة وإلى البيانات العابرة. وثمة تهديدات ترتبط بالنفاذ غير المخوّل به إلى البيانات المخزنة ذات الصلة بإدارة الهوية. ومن ثم، لا بد من وضع وإنفاذ الإجراءات المناسبة للتحكم في النفاذ للحؤول دون النفاذ غير المخوّل به.

المتطلب 59 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم إجراءات التحكم في النفاذ وإنفاذها لمنع النفاذ غير المخوّل به إلى بيانات إدارة الهوية. ويتضمن ذلك أي بيانات مخزنة أو مزودة في قواعد بيانات إدارة الهوية أو مخدمات التطبيق أو مخدم المشترك المنزلي (HSS) أو في أي عنصر من عناصر الشبكة الأخرى. ويتعين على مورد شبكة الجيل التالي/مورّد خدمة الهوية عدم السماح لكيان بالنفاذ إلى بيانات إدارة الهوية ما لم تُحدد هوية الكيان ويُتأكد من صحتها ويخوَّل لها بالنفاذ. وينطبق ذلك على جميع الكيانات (أي الأشخاص والعمليات والأنظمة البعيدة).

2.7.8 سلامة النظام والبيانات

يجب أن تحمى سلامة عناصر الشبكة والأنظمة والوظائف الداعمة لخدمات إدارة الهوية وقدراتها. ويشمل ذلك قواعد بيانات ومخدمات تطبيق إدارة الهوية.

المتطلب 60 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) حماية سلامة جميع عناصر الشبكة والأنظمة والوظائف الداعمة لخدمات إدارة الهوية وقدراتها.

ويجب أن تحمى سلامة معلومات الهوية وبياناتها لمنع أي إفساد للبيانات أو تلاعب بها على نحو يؤثر في سلامتها.

المتطلب 61 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) حماية سلامة البيانات المزودة لإدارة الهوية.

المتطلب 62 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) حماية سلامة أي توزيع أو اتصالات أو تحديثات أو تغييرات للبيانات، وأي بيانات مفصولة عن الخط ترتبط بإدارة الهوية.

3.7.8 سرية البيانات

المتطلب 63 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وإنفاذ إجراءات لحماية البيانات المزودة لإدارة الهوية من رصد الكيانات غير المخول لها (مثل الجهات في الداخل غير المخول لها).

المتطلب 64 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم وإنفاذ إجراءات لحماية توزيع أو اتصالات أو تحديثات أو تغييرات البيانات وأي بيانات مفصولة عن الخط ترتبط بإدارة الهوية، من رصد الكيانات غير المخول لها (مثل الجهات في الداخل غير المخول لها).

4.7.8 الحماية الأمنية لاتصالات إدارة الهوية

يجب حماية اتصالات إدارة الهوية (التشوير والوسائط) من النفاذ غير المخوّل والفساد والتلاعب والاعتراض (ومثاله التنصت).

المتطلب 65 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) حماية سلامة وسرية اتصالات إدارة الهوية ضمن الشبكة وبين الشبكات. ويتعين حماية سلامة كل ما يتعلق بإدارة الهوية من عبور التشوير وحركة وسائط للسطح البيني من شبكة إلى شبكة (NNI) أو السطح البيني من تطبيق إلى شبكة (ANI) أو السطح البيني من مخدم إلى شبكة (SNI) ما بين ميادين الشبكة.

5.7.8 أمن الإدارة

يجب تأمين نفاذ الإدارة إلى عناصر شبكة الجيل التالي والبيانات المشكّلة وحمايته من النفاذ غير المخوّل والضوابط.

المتطلب 66 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) منع النفاذ غير المخول إلى السطوح البينية للإدارة وإلى ضوابط عناصر الشبكة والكيانات الوظيفية الداعمة لإدارة الهوية.

ويجب تأمين حركة الإدارة وحمايتها من الفساد والتلاعب والرصد غير المخوّل به.

المتطلب 67 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) حماية سلامة وسرية حركة الإدارة المرتبطة بدعم إدارة الهوية.

6.7.8 سجل الأمن والتدقيق

تدعو الحاجة لسجل الأمن والتدقيق لغرض تسجيل أحداث يمكن أن تدعم استقصاء أنشطة معينة بعد الانتهاء منها.

المتطلب 68 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) إعداد سجلات أمنية لغرض تسجيل أحداث متصلة بدعم إدارة الهوية يمكن أن تدعم استقصاء أنشطة معينة بعد الانتهاء منها (مثل تسجيلات الدخول، وتعديل موارد وبيانات النظام الحرجة، ونفاذ الإدارة إلى معلمات وموارد شبكة الجيل التالي).

7.7.8 الحماية من هجمات تؤدي إلى حجب الخدمة (DoS) وحجب الخدمة الموزع (DDoS)

يجب أن تكون خدمات وقدرات إدارة الهوية متيسرة بدرجة عالية، وبالتالي لا بد من حمايتها من تهديدات حجب الخدمة وحجب الخدمة الموزع التي يمكن أن تؤثر في تيسر الخدمة.

المتطلب 69 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) توفير الحماية من حجب الخدمة وحجب الخدمة الموزع وغيرها من أنواع الهجمات التي تؤثر على تيسر خدمات وقدرات إدارة الهوية. ويشمل ذلك دعم واستخدام قدرات وأدوات حسب الاقتضاء لكشف حجب الخدمة الموزع وغيره من أنواع الهجمات ولعزل هذه الهجمات والتخفيف منها.

8.7.8 المراقبة وكشف الاقتحام

المتطلب 70 يترتب على مورد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) دعم واستخدام أدوات المراقبة الأمنية وكشف الاقتحام حسب الاقتضاء لكشف الاحتيال وإساءة الاستعمال واقتحام عناصر الشبكة وأنظمتها.

التذييل I

الحالات العامة لاستعمال إدارة الهوية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I مقدمة

يعرض هذا التذييل الحالات العامة لاستعمال إدارة الهوية المنظمة ضمن فئات الحكومات ومؤسسات الأعمال والمستعملين النهائيين/المشتركين.

2.I الحكومات

يمكن للحكومات أن تستخدم قدرات إدارة الهوية لتعزيز ودعم التطبيقات والمعاملات بين المؤسسات الحكومية والمواطنين، وبين المؤسسات الحكومية المختلفة (الخدمات الحكومية الاتحادية) والوكالات، وبين الحكومات المختلفة (الخدمات الاتحادية بين الحكومات). وتشمل الأمثلة عن حالات الاستعمال الحكومية ما يلي:

- ضمان تحديد هوية المواطن: يمكن للحكومات أن تستعمل إدارة الهوية للتحقق من صحة هوية المواطنين لدى حصولهم على خدمات الحكومة الالكترونية، مع تحسين حماية المعلومات التي تعرّف بأصحابها شخصياً. فإذا أُخذت الرعاية الصحية مثلاً، فإن حساسية المعلومات ذات الصلة بالصحة تسلط الضوء على أهمية التقليل من البيانات، وبصورة أعم، على الحاجة إلى مزيد من الأمن والخصوصية لمعلومات الهوية.
- ضمان تحديد هوية الموظف الحكومي في الخدمات الحكومية الاتحادية: يمكن للمؤسسات الحكومية أن تستخدم قدرات إدارة الهوية لوضع حلول مشتركة لأشكال آمنة وموثوقة لتحديد هوية موظفي الحكومة على نحو يعزز الأمن والكفاءة ويقلل الاحتيال في الهوية ويحمي الخصوصية الشخصية.
- تعزيز ودعم الخدمات الاتحادية بين الحكومات المختلفة: يمكن استخدام إدارة الهوية لتعزيز ودعم الخدمات الاتحادية بين الحكومات المختلفة. فعلى سبيل المثال، يمكن للحكومات أن تتعاون لوضع حلول تعزز إدارة الهوية للمواطنين المسافرين بين بلدان مختلفة وتتناول قضايا الأمن والخصوصية وتجارب المستعملين.

3.I مؤسسات

يمكن استخدام إدارة الهوية لمساعدة منظمات الأعمال على تعزيز ودعم مصالح الأعمال الجديدة والقائمة مع تحسين الأمن والخصوصية وحماية المعلومات التي تعرّف بأصحابها شخصياً. وتشمل الأمثلة عن حالات الاستعمال في مؤسسة الأعمال ما يلي:

- خدمات الهوية الاتحادية: يمكن استعمال إدارة الهوية لدعم خدمات التسجيل الواحد للدخول والخروج بين شركاء تجاريين متعددين (بما فيهم موردو شبكات الجيل التالي وخدمات الويب والمحتوى والطرف الثالث).
- خدمات الاتصالات: يمكن لموردي شبكات الجيل التالي أن يستعملوا إدارة الهوية ليتمكنوا من تقديم خدمات التطبيق إلى المستعملين النهائيين/المشتركين عبر منصات مختلفة (مثل شبكات بروتوكول الإنترنت الخاضعة للإدارة، وشبكة الإنترنت، والمنصات المتنقلة)، والسماح للمستعملين بالنفاذ إلى التطبيقات التي يختارونها على منصات متعددة بسبل تتناسب مع ما يفضلونه.
- المعاملات والتطبيقات المالية الإلكترونية: يمكن استعمال إدارة الهوية لتعزيز ودعم المدفوعات الالكترونية في المعاملات التجارة الإلكترونية.

4.I المستعملون النهائيون/المشتركون

يمكن للمستعملين النهائيين/المشتركين أن يستفيدوا من إدارة الهوية لتعزيز الخبرات والتحكم في المعلومات التي تعرّف بأصحابها شخصياً. وتشمل الأمثلة عن حالات الاستعمال لدى المستعمل النهائي/المشترك ما يلي:

- تحكم المستعمل المعلومات التي تعرّف بأصحابها شخصياً: يمكن استعمال إدارة الهوية لتعزيز خبرات المستعمل والسماح له بالتحكم في المعلومات التي تعرّف به شخصياً. ويمكن للأفراد استخدام أسماء مستعارة متعددة للمشاركة في أنشطة مختلفة مثل الاطلاع على قنوات الأخبار ونشر مدونات على شبكة الإنترنت وإدارة الشبكات الاجتماعية وتبادل الصور أو الموسيقى. ويمكن لإدارة الهوية أن تساعد في إتاحة المزيد من الخيارات للأفراد بشأن كيفية مشاركتهم في مختلف المجتمعات، والدرجة التي يريدون بها إقامة الصلة بين جوانب شخصياتهم المختلفة (أي التحكم في المعلومات التي تعرّف بهم شخصياً).
- الشبكات الاجتماعية: يمكن استعمال إدارة الهوية لتعزيز ودعم تطبيقات الشبكات الاجتماعية من خلال توفير الأدوات اللازمة للتحكم الفعال من جانب المستعمل في المعلومات التي تعرّف به شخصياً وللمساءلة.

التذييل II

حالات استعمال إدارة الهوية في تطبيقات شبكات الجيل التالي

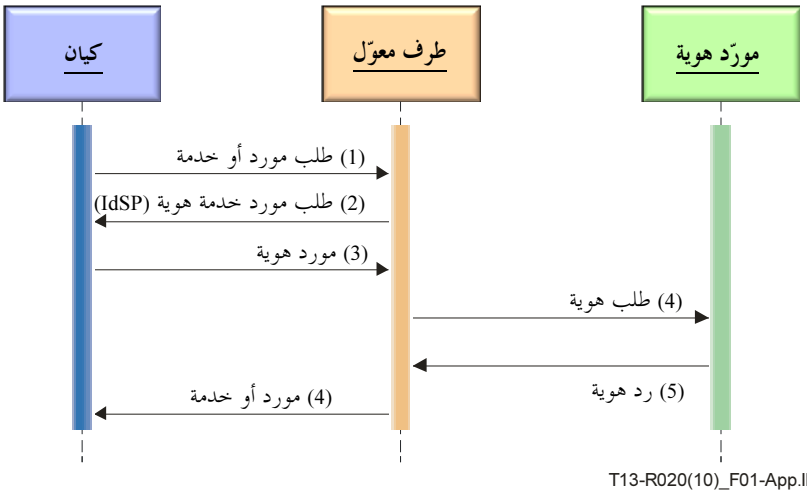
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II مقدمة

يعرض هذا التذييل أمثلة عن حالات استعمال إدارة الهوية في تطبيقات شبكات الجيل التالي. ومن شأن هذه الأمثلة أن تُستعمل كأساس لوضع متطلبات إدارة الهوية في تطبيقات شبكات الجيل التالي.

2.II مثال عن حالة الاستعمال الأساسي

يُظهر الشكل 1.II مثالاً عن حالة الاستعمال الأساسي ينطوي على ثلاثة عناصر أساسية. وتوجد سيناريوهات أخرى محتملة خلاف هذا المثال الأساسي. راجع التذييل V للاطلاع على شرح السيناريوهات الأخرى المحتملة (مثل السيناريوهات المتمحورة حول المستعمل).



الشكل 1.II – مثال عن حالة الاستعمال الأساسي

تتألف العناصر الثلاثة من كيان (كالطرف المؤكد أو الكيان الرئيسي) يسعى بطلب خدمات من طرف معوّل (يمكن أن يكون الطرف المعول شبكة أو تطبيقاً) فيحصل على تأكيد هوية مرتبط بطلبه، بما في ذلك التأكيدات المغفلة أو بأسماء مستعارة، من مورد خدمة الهوية (IdSP) على أساس الثقة والسياسة الأمنية.

وفي الشكل 1.II، يظهر الانسياب التالي لمعلومات إدارة الهوية في المستوى العالي.

1) يقدم الكيان هوية يدعيها إلى الطرف المعوِّل (مقدم المورد أو الخدمة) طالباً مورداً أو خدمة منه.

2) يحتاج الطرف المعوِّل (شبكة أو تطبيق) للاستيقان من استيقان الكيان قبل يقدم له ما طلبه من مورد أو خدمة. وللاستيقان، يحتاج الطرف المعول لمعلومات من مورد خدمة الهوية المناسب الذي يجب تحديده والاتصال به. فيجيب الطرفُ المعول الكيانَ برسالة "طلب معلومات من موّرد خدمة الهوية" ("Request for IdSP info") طالباً إلى الكيان أن يوافيه باسم مورد خدمة الهوية المناسب.

3) فيرد الكيان على رسالة "طلب معلومات من موّرد خدمة الهوية" بتحديد هوية مورد خدمة الهوية المناسب للطرف المعوِّل. وقد يحدد الكيان عدداً من موردي خدمة الهوية.

4) ويستعلم الطرف المعوِّل بدوره من موّرد (أو موردي) خدمة الهوية المناسب (المناسبين) للتحقق من صحة الهوية التي يدعيها الكيان بمستوى كاف من الثقة (مستوى الضمان)، على النحو المطلوب.

5) يؤكد مورد خدمة الهوية الهويةَ التي يدعيها الكيان. وقد تشمل وظائف مورد خدمة الهوية التفويض (أي أن مورد خدمة الهوية يمكنه أن يفوض موردي خدمة هوية آخرين ببعض جوانب عملية الاستيقان بنقل زعم الهوية إليهم). وقد ترد طلبات أخرى من الطرف المعول إلى موّرد (أو موردي) خدمة الهوية، إذا ما دعت الحاجة لمستوىً أعلى من الاستيقان، أو لقدرات أخرى خاصة بتطبيق معين.

6) يقدم الطرف المعوِّل ما طلب منه من مورد أو خدمة بعد تلقي التحقق من الهوية التي يدعيها الكيان من موّرد (أو موردي) خدمة الهوية.

ويمكن الجمع بين هذه العناصر الثلاثة (الكيان والطرف المعوِّل وموّرد خدمة الهوية). أما الوسائط الضمنية المشاركة فلا صلة لها بالأمر. والشرط الوحيد هو أن تكون آليات الاتصالات هذه "مهيكلة جيداً" مع قواعد التركيب والبيانات العامة المعروفة أو التي يمكن للأطراف المعنية الحصول عليها إذا كانت تملك الأذونات الضرورية لاستخدام الآليات. وحسب الاقتضاء، ينبغي استعمال آليات معيارية للتشغيل البيني الموثوق عالمياً.

وبالإضافة إلى ذلك، يمكن أن تكون هناك انسيابات أخرى لمعلومات إدارة الهوية في المستوى العالي، ومنها مثلاً:

1) يمكن للطرف المعول أن يطلب مستندات الاستيقان من كيان مباشرةً.

2) يمكن للكيان أن يقدم مستندات الاستيقان إلى مورد خدمة هوية موثوق.

3) يمكن لموّرد خدمة الهوية أن يتحقق من صحة المستندات المقدمة من الكيان، وأن يصدر مستندات جديدة للكيان لتلبية طلب الاستيقان الوارد من الطرف المعوِّل.

4) يمكن لكيان (أو لمن يفوضه) أن يحصل من مورد خدمة الهوية على المستندات الصادرة وأن يعطيها إلى الطرف المعوِّل.

5) يمكن للمستندات الصادرة التي يرسلها الكيان إلى الطرف المعوِّل أن تحوي إما 1) نسخة عن ادعاءات الهوية الصادرة عن موّرد خدمة الهوية، أو 2) إحالة إليها.

أضف إلى ذلك أن الكيان قد يقرر ألا يعطي الطرف المعوِّل مستندات الاستيقان الصادرة عن موّرد خدمة الهوية.

ومن الممكن أيضاً وجود تسلسل هرمي من موردي خدمة الهوية أو تسلسل هرمي من أطراف معولة. كما يمكن أن يكون لكيان أكثر من مندوب مفوض واحد.

3.II استعمال نظام إدارة هوية مشترك لدعم خدمات تطبيق متعددة (مثل الصوت والبيانات وتلفزيون بروتوكول الإنترنت) ضمن شبكة مقدم الخدمة

1.3.II نظرة عامة

من شأن موردي الشبكة/الخدمة (كموردي شبكات الجيل التالي) أن يدعموا العديد من التطبيقات والخدمات ويستضيفوها. وتتيح الطبيعة الموزعة لبيئة شبكات الجيل التالي إمكانية استضافة خدمات تطبيق مختلفة في عناصر الشبكة المختلفة وعلى منصات باعة محددين (كمنصات نقل الصوت عبر بروتوكول الإنترنت، والبيانات وتلفزيون بروتوكول الإنترنت). وقد يكون لكل خدمة وسائلها للتحكم في النفاذ التي ينفرد بها كل بائع أو كل تكنولوجيا فيها. وقد لا تتوافق هذه الوسائل مع بعضها البعض، فيتعين تهيئتها وإدارتها واستعمالها على نحو منفصل.

من شأن نهج يستثمر البنية التحتية المشتركة لإدارة الهوية ويفعّل العديد من التطبيقات/الخدمات، أن يوفر الفوائد من حيث التكاليف والكفاءة التجارية. ومن شأن ذلك أيضاً أن يوفر نهجاً معيارياً يتيح لمعدي التطبيق أن يستخدموا المفعّلات المشتركة في إدارة الهوية بدلاً من أن يوكل لكل تطبيق أو خدمة دعم وظائف محددة في إدارة الهوية (مثل قدرات وآليات التحكم في النفاذ التي ينفرد بها كل بائع)، وأن يتيح قيام عملية تتميز بالكفاءة في تصميم خدمات التطبيق وتنفيذها وعرضها. وبالإضافة إلى ذلك، يمكن لنهج مشترك أن يساعد في إدارة المخاطر الأمنية لكل خدمة تطبيق ولمجمل البنية التحتية للشبكة ككل.

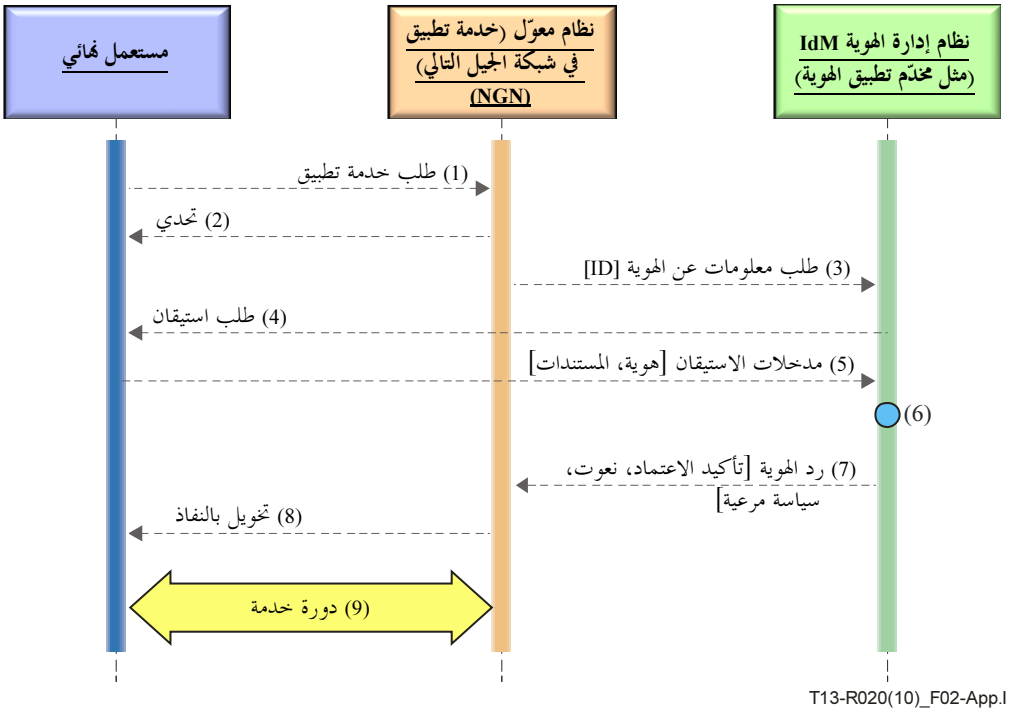
ويشمل نهج إدارة الهوية في شبكة الجيل التالي حلولاً ضمن الشبكة (أي حلول ضمن ميدان مورد شبكات الجيل التالي) وحلولاً بين الشبكات (أي حلول بين مختلف موردي شبكات الجيل التالي بما في ذلك الموردين عن طريق طرف ثالث) على السواء. وفي سيناريو ضمن الشبكة، قد ينطوي ذلك على نُهُج للسماح بتفاعلات بين مختلف عناصر الشبكة أو مكونات لإدارة الهوية ضمن ميدان مورّد شبكات الجيل التالي (مثل المدعين والأنظمة المعولة وأنظمة الهوية). أما في سيناريوهات ما بين الشبكات، فقد يشمل ذلك تحديد نُهُج للسماح بالتفاعل بين كيانات عناصر الشبكة عبر مختلف ميادين إدارة الهوية في شبكات الجيل التالي (مثل المدعين والأطراف المعوّلة وموردي خدمة الهوية).

ملاحظـــة – يمكن لمورّد شبكات الجيل التالي أن يكون مورّداً لخدمة الهوية أيضاً.

2.3.II وصف حالة الاستعمال

يوضح مثال حالة الاستعمال هذا كيف تستعمل خدمات التطبيق المتعددة (مثل نقل الصوت عبر بروتوكول الإنترنت، والبيانات وتلفزيون بروتوكول الإنترنت) بنية تحتية مشتركة لإدارة الهوية من التحكم في النفاذ والحماية الأمنية لخدمة التطبيق. وتنطوي حالة الاستعمال على تفاعلات بين الكيانات التالية:

- المستعملون النهائيون (أي المستعمل النهائي و/أو جهاز المستعمل النهائي)
- النظام المعول (أي خدمة التطبيق أو نظام الشبكة)
- نظام إدارة الهوية (أي نظام الشبكة الذي يقدم خدمات إدارة الهوية مثل التسجيل والاستيقان والتخويل ومعلومات بيانات الاشتراك).



الشكل 2.II – مثال عن حالة الاستعمال الأساسي

يوضح الشكل 2.II مثالاً أساسياً حيث تستعمل خدمة التطبيق خدمات نظام إدارة هوية خارجي أو مستقل عن خدمة التطبيق للتحكم في النفاذ وإدارة امتياز. أما انسيابات مثال النداء فهي كالتالي:

1) طلب خدمة تطبيق. يمثل انسياب المعلومات هذا طلب المستعمل النهائي لاستدعاء خدمة التطبيق.

2) التحدي. ترسل خدمة التطبيق رداً يتحدى نفاذ المستعمل.

3) طلب معلومات الهوية [هوية المستعمل]. ترسل خدمة التطبيق طلباً إلى نظام إدارة الهوية لتأكيد هوية المستعمل وتقديم نعوت مرتبطة بهوية المستعمل. وقد يتضمن ذلك معلومات مثل البيانات العامة للخدمة، والامتياز والأفضليات ومعلومات عن السياسة العامة. ومثال ذلك، أي سياسة أو قيود مرتبطة بالهوية.

4) طلب استيقان. ترسل أنظمة إدارة الهوية إلى المستعمل طلب استيقان.

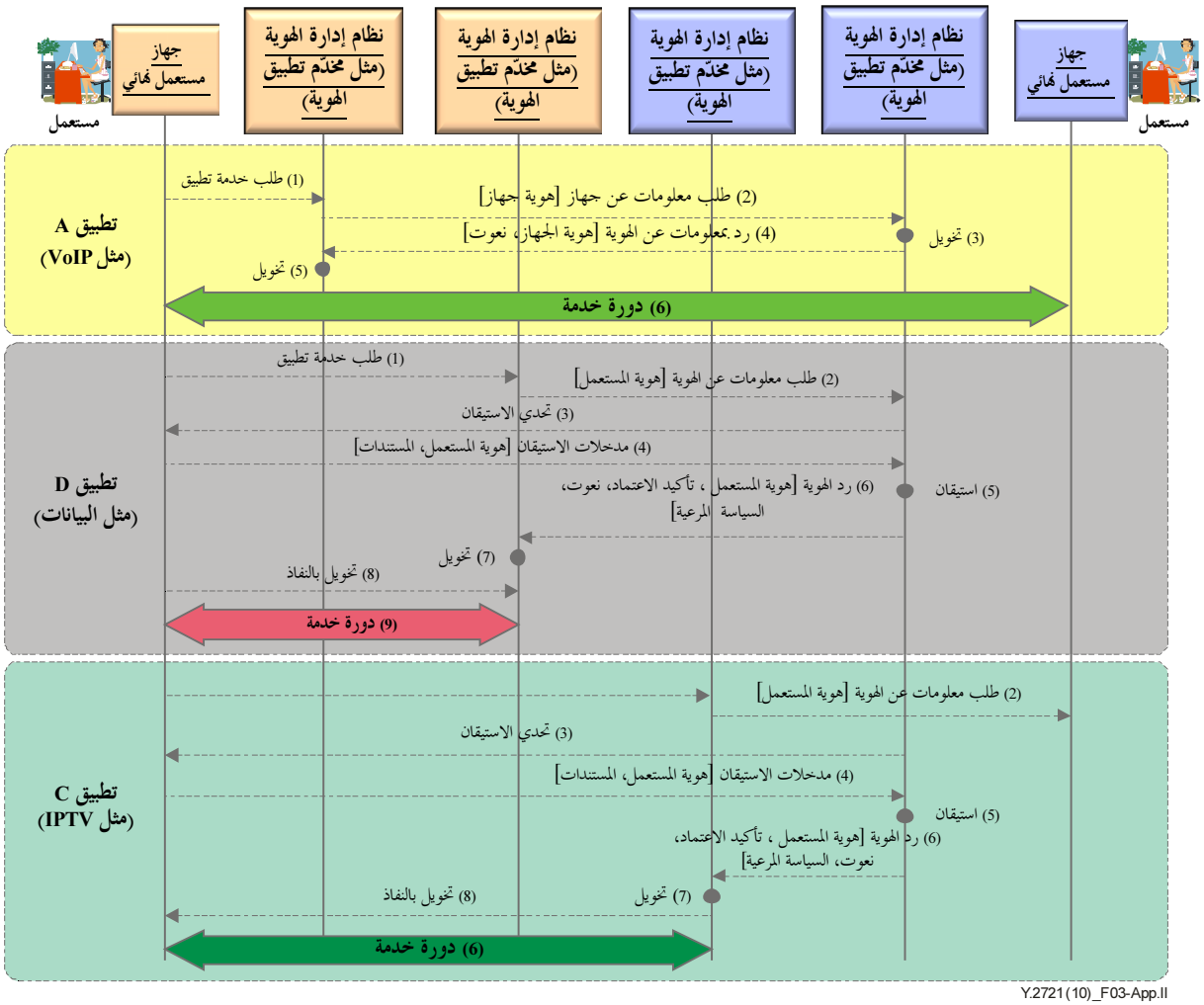
5) مدخلات الاستيقان [المستندات]. يقدم المستعمل معلومات للاستيقان منه (مثل اسم المستعمل وكلمة المرور أو رقم التعريف الشخصي).

6) الاستيقان. يقوم نظام إدارة الهوية بالاستيقان ويحصل على المعلومات الضرورية الأخرى. وقد يشمل ذلك الحصول على المعلومات من أنظمة الشبكة الأخرى (مثل مخدم المشترك المنزلي (HSS)).

7) الرد بمعلومات الهوية [تأكيدات المستند، النعوت، السياسة العامة]. يقدم نظام إدارة الهوية معلومات تؤكد المستندات. والمعلومات الأخرى التي يمكن إيرادها هي النعوت المرتبطة بهوية المستعمل (مثل الامتيازات والأفضليات) والسياسة ذات الصلة بمعلومات الهوية (كأي قيود فيما يتعلق باستخدام الهوية وعرضها ونشرها).

8) تخويل بالنفاذ. تشير خدمة التطبيق للمستعمل بمنحه إمكانية النفاذ إلى الخدمة.

9) دورة خدمة التطبيق. يبين انسياب المعلومات هذا نجاح دورة المستعمل لدى خدمة التطبيق.



الشكل 3.II – استعمال خدمات التطبيق المتعددة للبنية التحتية المشتركة لإدارة الهوية

يوضح الشكل 3.II مثالاً عن حالة استعمال حيث تستعمل خدمات التطبيق المتعددة (مثل الصوت عبر بروتوكول الإنترنت، والبيانات وتلفزيون بروتوكول الإنترنت) نظاماً مشتركاً لإدارة الهوية خارجياً ومستقلاً عن خدمات التطبيق. ويفترض هذا المثال أن جهاز المستعمل النهائي مسجل ويلتحق بمقدم الخدمة باستخدام الإجراءات العادية.

وفيما يلي انسيابات المثال للتطبيق A (الصوت عبر بروتوكول الإنترنت (VoIP)):

1) طلب خدمة تطبيق: يمثل انسياب المعلومات هذا بدء نداء من جانب المستعمل النهائي.

2) طلب معلومات عن الهوية [هوية الجهاز]: ترسل خدمة التطبيق طلباً إلى نظام إدارة الهوية للتحقق مما إذا كان جهاز المستعمل النهائي مخوّلاً بالاستفادة من خدمة الصوت عبر بروتوكول الإنترنت. ويفترض هذا المثال أن خدمة الصوت عبر بروتوكول الإنترنت تستند إلى البيانات العامة لاشتراك جهاز المستعمل أو الخط (مثل اشتراك عروة البدالة الهاتفية الرقمية للمشترك (xDSL)).

3) التخويل: يحدد نظام إدارة الهوية ما إذا كان المستعمل النهائي مخولاً بالاستفادة من خدمة الصوت عبر بروتوكول الإنترنت.

الملاحظـــة 1 – يُفترض أن ذلك ينطوي على استخراج البيانات العامة لاشتراك جهاز المستعمل أو الخط (مثل اشتراك عروة البدالة الهاتفية الرقمية للمشترك (xDSL). ويُفترض أيضاً أن لا حاجة لاستيقان خدمة الصوت عبر بروتوكول الإنترنت من المستعمل النهائي.

4) الرد بمعلومات الهوية [هوية جهاز، نعوت]. يقدم نظام إدارة الهوية نعوتاً مرتبطة بهوية الجهاز (أي ما إذا كان الجهاز مخوّلاً بالاستفادة من خدمة الصوت عبر بروتوكول الإنترنت). ويشمل ذلك المعلومات ذات الصلة المستخرجة من البيانات العامة للاشتراك (مثل الامتيازات والأفضليات).

5) التخويل بالنفاذ. تشير خدمة التطبيق للمستعمل بمنحه إمكانية النفاذ إلى الخدمة.

6) دورة خدمة التطبيق. يبين انسياب المعلومات هذا نجاح المستعمل في دورة النداء.

وفيما يلي انسيابات النداء في المثال للتطبيق B (بيانات):

1) طلب خدمة تطبيق. يمثل انسياب المعلومات هذا طلب المستعمل النهائي لاستدعاء خدمة التطبيق.

2) طلب معلومات عن الهوية [هوية مستعمل]. ترسل خدمة التطبيق طلباً إلى نظام إدارة الهوية ليؤكد هوية المستعمل ويقدم نعوتاً مرتبطة بهوية المستعمل. وقد يشمل ذلك معلومات مثل البيانات العامة للخدمة ومعلومات عن الامتياز والأفضليات والسياسة العامة. ومثال ذلك، أي سياسة أو قيود مرتبطة بالهوية.

3) تحدي الاستيقان: ترسل أنظمة إدارة الهوية إلى المستعمل طلب استيقان.

4) مدخلات الاستيقان [المستندات]. يقدم المستعمل معلومات للاستيقان منه (مثل هوية المستعمل وكلمة المرور أو رقم التعريف الشخصي).

5) الاستيقان. يقوم نظام إدارة الهوية بالاستيقان ويحصل على المعلومات الضرورية الأخرى. وقد يشمل ذلك الحصول على المعلومات من أنظمة الشبكة الأخرى (مثل مخدم المشترك المنزلي (HSS) أو قاعدة بيانات اشتراك أخرى).

6) الرد بمعلومات الهوية [تأكيدات المستند، النعوت، السياسة العامة]. يقدم نظام إدارة الهوية معلومات تؤكد المستندات. والمعلومات الأخرى التي يمكن إيرادها هي النعوت المرتبطة بهوية المستعمل (مثل الامتيازات والأفضليات) والسياسة ذات الصلة بمعلومات الهوية (كأي قيود فيما يتعلق باستخدام الهوية وعرضها ونشرها).

7) التخويل. تقوم خدمة التطبيق بمعالجة المعلومات، وتحدد ما إذا كان المستعمل النهائي مخولاً بالاستفادة من الخدمة.

8) التخويل بالنفاذ. تشير خدمة التطبيق للمستعمل بمنحه إمكانية النفاذ إلى الخدمة.

9) دورة خدمة التطبيق. يبين انسياب المعلومات هذا نجاح دورة المستعمل لدى خدمة التطبيق.

وفيما يلي انسيابات النداء في المثال للتطبيق C (تلفزيون بروتوكول الإنترنت (IPTV)):

1) طلب خدمة تطبيق. يمثل انسياب المعلومات هذا طلب المستعمل النهائي لاستدعاء خدمة التطبيق.

2) طلب معلومات عن الهوية [هوية مستعمل]. ترسل خدمة التطبيق طلباً إلى نظام إدارة الهوية ليؤكد هوية المستعمل ويقدم نعوتاً مرتبطة بهوية المستعمل. وقد يشمل ذلك معلومات مثل البيانات العامة للخدمة ومعلومات عن الامتياز والأفضليات والسياسة العامة. ومثال ذلك، أي سياسة أو قيود مرتبطة بالهوية.

3) تحدي الاستيقان: ترسل أنظمة إدارة الهوية إلى المستعمل طلب استيقان.

4) مدخلات الاستيقان [المستندات]. يقدم المستعمل معلومات للاستيقان منه (مثل هوية المستعمل وكلمة المرور أو رقم التعريف الشخصي).

5) الاستيقان. يقوم نظام إدارة الهوية بالاستيقان ويحصل على المعلومات الضرورية الأخرى. وقد يشمل ذلك الحصول على المعلومات من أنظمة الشبكة الأخرى (مثل مخدم المشترك المنزلي (HSS) أو قاعدة بيانات اشتراك أخرى).

6) الرد بمعلومات الهوية [تأكيدات المستند، النعوت، السياسة العامة]. يقدم نظام إدارة الهوية معلومات تؤكد المستندات. والمعلومات الأخرى التي يمكن إيرادها هي النعوت المرتبطة بهوية المستعمل (مثل الامتيازات والأفضليات) والسياسة ذات الصلة بمعلومات الهوية (كأي قيود فيما يتعلق باستخدام الهوية وعرضها ونشرها).

7) التخويل. تقوم خدمة التطبيق بمعالجة المعلومات، وتحدد ما إذا كان المستعمل النهائي مخولاً بالاستفادة من الخدمة.

8) التخويل بالنفاذ. تشير خدمة التطبيق للمستعمل بمنحه إمكانية النفاذ إلى الخدمة.

9) دورة خدمة التطبيق. يبين انسياب المعلومات هذا نجاح دورة المستعمل لدى خدمة التطبيق.

الملاحظـــة 2 – للاستيقان المتبادل (أي استيقان مورد التطبيق أو الخدمة)، ستكون هناك حاجة إلى وظائف وانسيابات أخرى. بيد أن هذا الأمر بلا يظهر في الشكل 3.II.

3.3.II المتطلبات الضمنية

ترد المتطلبات الضمنية التالية في مثال حالة الاستعمال هذا:

- قد يكون لشبكات الجيل التالي حل مشترك لإدارة الهوية كي تستعمله تطبيقات وخدمات متعددة أياً ما كانت منصة التطبيق أو حلول الباعة.
- يجب عدم استعمال وظائف إدارة الهوية المشتركة، إذا كانت تتعارض مع مبادئ تقييد عملية جمع البيانات وتقليل البيانات إلى الحد الأدنى وفصل البيانات وتحديد الغرض وقيود الاستعمال.
- يتعين أن تدعم شبكات الجيل التالي نهجاً معيارياً ومهيكلاً للسماح لخدمات التطبيق باكتشاف نظام (أو أنظمة) إدارة الهوية وبتبادل بيانات الهوية على بأمان.

4.II التسجيل الواحد للدخول إلى/التسجيل الواحد للخروج من خدمات التطبيق المتعددة (مثل الصوت والبيانات وتلفزيون بروتوكول الإنترنت) ضمن شبكة مقدم الخدمة

1.4.II نظرة عامة

على المستعملين عادةً أن يسجلوا دخولهم إلى أنظمة متعددة تستضيف خدمات التطبيقات (مثل الصوت عبر بروتوكول الإنترنت، والبيانات وتلفزيون بروتوكول الإنترنت)، مما يستلزم عدداً مساوياً من حوارات الدخول، قد ينطوي كل منها على أسماء مستعملين ومعلومات استيقان مختلفة. ويواجه مديرو النظام مهمة إدارة حسابات المستعمل ضمن كل من الأنظمة المتعددة التي يراد النفاذ إليها على نحو منسق من أجل الحفاظ على سلامة إنفاذ السياسة الأمنية.

ويطالب المستعملون النهائيون المشتركون بميزات تسهل الاستعمال مثل "التسجيل الواحد للدخول/التسجيل الواحد للخروج". وينطلق مفهوم "التسجيل الواحد للدخول" من أن المستعمل النهائي أو الجهاز أو المستعمل النهائي والجهاز معاً

يمكنهم تسجيل الدخول لمرة واحدة (أي بتقديم مدخلات المستند للاستيقان والتخويل) إلى خدمة في شبكة الجيل التالي، ونتيجة لذلك يُستيقن منهم لدى خدمة أو المزيد من الخدمات الإضافية في شبكة الجيل التالي نفسها (أي لا يتحمل المستعمل النهائي عبء الاستيقان في كل خدمة). وتؤدي عبارة "تسجيل الدخول" نفس معنى "التسجيل لدى"، حيث يتسجل المستعمل النهائي/الجهاز لدى الخدمة.

وعلى غرار ما تقدم، فإن "التسجيل الواحد للخروج" يزود المستعمل بميزة تجنبه الاضطرار إلى "تسجيل الخروج" من كل خدمة تطبيق في دورة معينة.

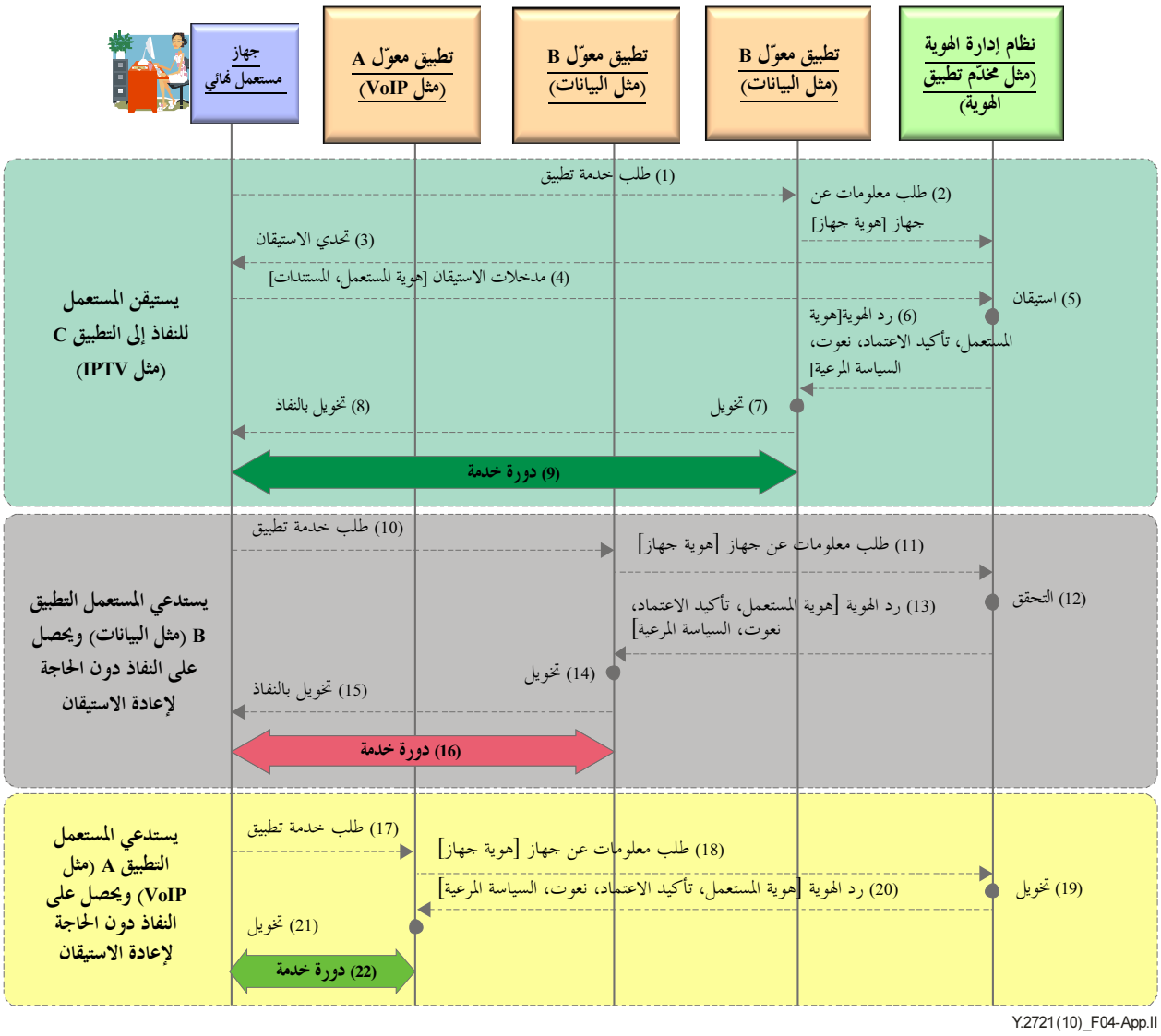
وتشمل الفوائد التي توفرها خدمات التسجيل الواحد للدخول/التسجيل الواحد للخروج ما يلي:

- اختصار الوقت الذي يستغرقه المستعملون في عمليات تسجيل الدخول إلى الميادين الفردية، بما في ذلك الحد من إمكانية فشل عمليات تسجيل الدخول هذه.
- تحسين الأمن من خلال الحد من حاجة المستعمل للتعامل مع مجموعات متعددة من معلومات الاستيقان وتذكرها.
- اختصار الوقت الذي يستغرقه مديرو النظام وتحسين استجابتهم بإضافة مستعملين إلى النظام وحذفهم منه أو تعديل حقوقهم في النفاذ.
- تحسين الأمن من خلال تعزيز قدرة مديري النظام على الحفاظ على سلامة تشكيلة حساب المستعمل بما في ذلك القدرة على منع أو إلغاء نفاذ مستعمل معين إلى جميع موارد النظام بطريقة منسقة ومتسقة.

2.4.II وصف حالة الاستعمال

يوضح مثال حالة الاستعمال هذا استعمال نظام إدارة الهوية لدعم "التسجيل الواحد للدخول إلى/التسجيل الواحد للخروج من" خدمات التطبيق المتعددة (مثل نقل الصوت عبر بروتوكول الإنترنت، والبيانات وتلفزيون بروتوكول الإنترنت) ضمن ميدان مورّد شبكات الجيل التالي. وتنطوي حالة الاستعمال على تفاعلات بين الكيانات التالية:

- المستعملون النهائيون (أي المستعمل النهائي و/أو جهاز المستعمل النهائي)
- النظام المعول (أي خدمة التطبيق أو نظام الشبكة)
- نظام إدارة الهوية (أي نظام الشبكة الذي يقدم خدمات إدارة الهوية مثل التسجيل والاستيقان والتخويل ومعلومات بيانات الاشتراك).



الشكل 4.II – التسجيل الواحد للدخول

يبين الشكل 4-II استعمال مستعمل نهائي مشترِك لخدمة التسجيل الواحد للدخول للنفاذ إلى خدمات التطبيق المتعددة (مثل الصوت عبر بروتوكول الإنترنت، والبيانات وتلفزيون بروتوكول الإنترنت). ويفترض هذا المثال أن جهاز المستعمل النهائي مسجل ويلتحق بمقدم الخدمة باستخدام الإجراءات العادية.

وفيما يلي انسيابات النداء في المثال:

1) طلب خدمة تطبيق. يمثل انسياب المعلومات هذا طلب المستعمل النهائي لاستدعاء خدمة التطبيق C (تلفزيون بروتوكول الإنترنت).

2) طلب معلومات عن الهوية [هوية مستعمل]: ترسل خدمة التطبيق C (تلفزيون بروتوكول الإنترنت) طلباً إلى نظام إدارة الهوية ليؤكد هوية المستعمل ويقدم نعوتاً مرتبطة بهوية المستعمل. وقد يشمل ذلك معلومات مثل البيانات العامة للخدمة ومعلومات عن الامتياز والأفضليات والسياسة العامة. ومثال ذلك، أي سياسة أو قيود مرتبطة بالهوية.

3) تحدي الاستيقان: يتحدى نظام إدارة الهوية المستعمل ليستيقن منه.

4) مدخلات الاستيقان [المستندات]. يقدم المستعمل معلومات للاستيقان منه (مثل هوية المستعمل وكلمة المرور أو رقم التعريف الشخصي).

5) الاستيقان. يقوم نظام إدارة الهوية بالاستيقان ويحصل على المعلومات الضرورية الأخرى. وقد يشمل ذلك الحصول على المعلومات من أنظمة الشبكة الأخرى (مثل مخدم المشترك المنزلي (HSS) أو قاعدة بيانات اشتراك أخرى).

6) الرد بمعلومات الهوية [تأكيدات المستند، النعوت، السياسة العامة]. يقدم نظام إدارة الهوية معلومات تؤكد المستندات. والمعلومات الأخرى التي يمكن إيرادها هي النعوت المرتبطة بهوية المستعمل (مثل الامتيازات والأفضليات) والسياسة ذات الصلة بمعلومات الهوية (كأي قيود فيما يتعلق باستخدام الهوية وعرضها ونشرها).

7) التخويل. تقوم خدمة التطبيق C (تلفزيون بروتوكول الإنترنت) بمعالجة المعلومات، وتحدد ما إذا كان المستعمل النهائي مخولاً بالاستفادة من الخدمة.

8) التخويل بالنفاذ. تشير خدمة التطبيق C (تلفزيون بروتوكول الإنترنت) للمستعمل بمنحه إمكانية النفاذ إلى الخدمة.

9) دورة خدمة التطبيق. يبين انسياب المعلومات هذا نجاح دورة المستعمل لدى خدمة التطبيق C (تلفزيون بروتوكول الإنترنت).

10) طلب خدمة تطبيق. يمثل انسياب المعلومات هذا طلب المستعمل النهائي لاستدعاء خدمة التطبيق B (بيانات).

11) طلب معلومات عن الهوية [هوية مستعمل]: ترسل خدمة التطبيق B (بيانات) طلباً إلى نظام إدارة الهوية ليؤكد هوية المستعمل ويقدم نعوتاً مرتبطة بهوية المستعمل. وقد يشمل ذلك معلومات مثل البيانات العامة للخدمة ومعلومات عن الامتياز والأفضليات والسياسة العامة. ومثال ذلك، أي سياسة أو قيود مرتبطة بالهوية.

12) التحقق. يقوم نظام إدارة الهوية بمعالجة الطلب ليحدد ما إذا كان التسجيل الواحد للدخول قابلاً للتطبيق وليتحقق من أن الاستيقان من المستعمل لا يزال ساري المفعول.

13) الرد بمعلومات الهوية [تأكيدات المستند، النعوت، السياسة العامة]. يقدم نظام إدارة الهوية معلومات تؤكد المستندات. والمعلومات الأخرى التي يمكن إيرادها هي النعوت المرتبطة بهوية المستعمل (مثل الامتيازات والأفضليات) والسياسة ذات الصلة بمعلومات الهوية (كأي قيود فيما يتعلق باستخدام الهوية وعرضها ونشرها).

14) التخويل. تقوم خدمة التطبيق B (بيانات) بمعالجة المعلومات، وتحدد ما إذا كان المستعمل النهائي مخولاً بالاستفادة من الخدمة.

15) التخويل بالنفاذ. تشير خدمة التطبيق B (بيانات) للمستعمل بمنحه إمكانية النفاذ إلى الخدمة.

16) دورة خدمة التطبيق. يبين انسياب المعلومات هذا نجاح دورة المستعمل لدى خدمة التطبيق B (بيانات).

17) طلب خدمة تطبيق. يمثل انسياب المعلومات هذا طلب المستعمل النهائي لاستدعاء خدمة التطبيق A (الصوت عبر بروتوكول الإنترنت).

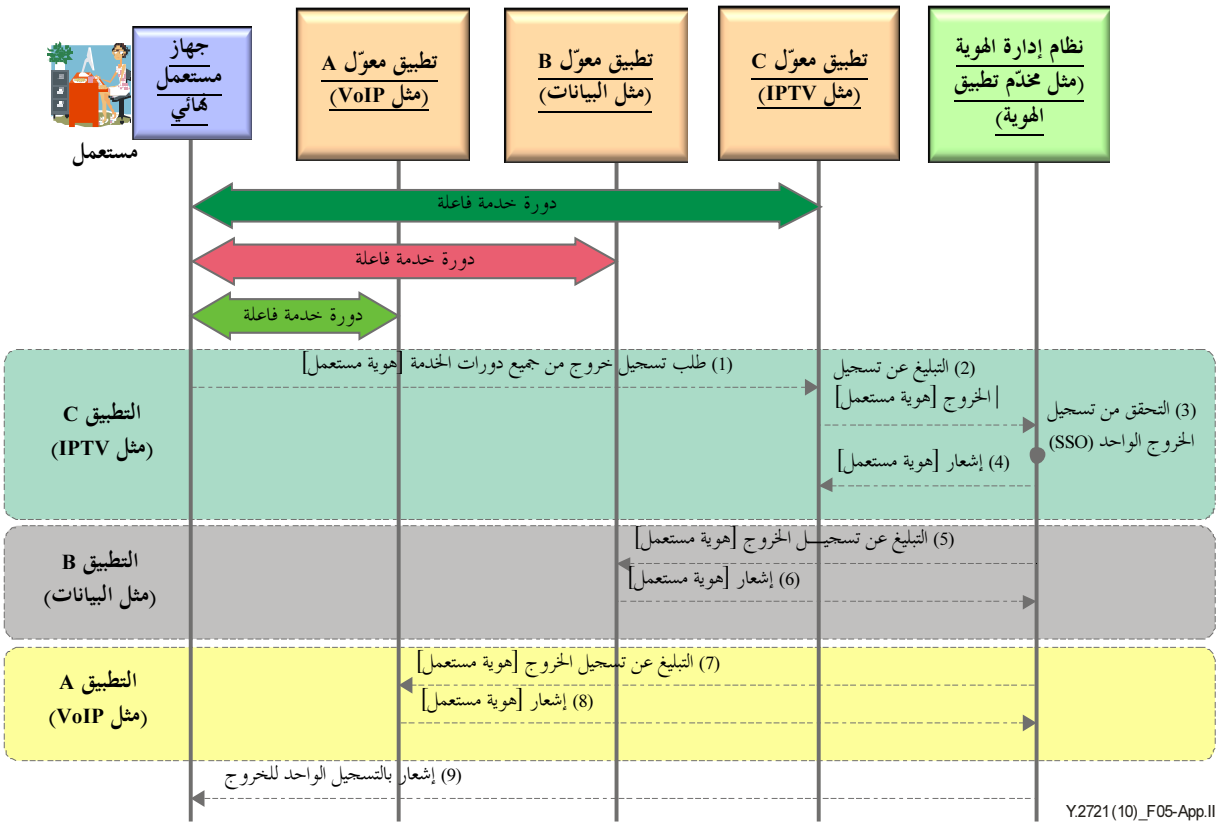
18) طلب معلومات عن الهوية [هوية جهاز]: ترسل خدمة التطبيق A (الصوت عبر بروتوكول الإنترنت) طلباً إلى نظام إدارة الهوية ليؤكد هوية المستعمل ويقدم نعوتاً مرتبطة بهوية الجهاز.

19) التحقق. يقوم نظام إدارة الهوية بمعالجة الطلب ليحدد ما إذا كان التسجيل الواحد للدخول قابلاً للتطبيق وليتحقق من أن الاستيقان من المستعمل لا يزال ساري المفعول.

20) الرد بمعلومات الهوية [تأكيدات المستند، النعوت، السياسة العامة]. يقدم نظام إدارة الهوية معلومات تؤكد المستندات. والمعلومات الأخرى التي يمكن إيرادها هي النعوت المرتبطة بهوية الجهاز (مثل الامتيازات والأفضليات) والسياسة ذات الصلة بمعلومات الهوية (كأي قيود فيما يتعلق باستخدام الهوية وعرضها ونشرها).

21) التخويل. تقوم خدمة التطبيق A (الصوت عبر بروتوكول الإنترنت) بمعالجة المعلومات، وتحدد ما إذا كان المستعمل النهائي مخولاً بالاستفادة من الخدمة.

22) دورة خدمة التطبيق. يبين انسياب المعلومات هذا نجاح دورة المستعمل لدى خدمة التطبيق A (الصوت عبر بروتوكول الإنترنت).



الشكل 5.II – التسجيل الواحد للخروج

يبين الشكل II-5 سماح خدمة "التسجيل الواحد للخروج" للمستعمل بتسجيل الخروج تلقائياً من خدمات التطبيقات المتعددة (الصوت عبر بروتوكول الإنترنت والبيانات وتلفزيون بروتوكول الإنترنت) دون الحاجة إلى تسجيل الخروج من كل خدمة تطبيق في الدورة. وتفترض حالة الاستعمال هذه وجود المستعمل في دورة خدمة ذات خدمات التطبيق الفاعلة: A (الصوت عبر بروتوكول الإنترنت) وB (بيانات) وC (تلفزيون بروتوكول الإنترنت).

وفيما يلي انسيابات النداء:

1) تسجيل الخروج من الخدمة [هوية المستعمل]. يمثل انسياب النداء هذا طلب المستعمل بإنهاء جميع دورات الخدمة.

2) التبليغ عن تسجيل الخروج [هوية المستعمل]. تبلّغ خدمة التطبيق C (تلفزيون بروتوكول الإنترنت) نظام إدارة الهوية بأن المستعمل يطلب تسجيل خروجه.

3) التحقق من التسجيل الواحد للخروج (SSO): يحدد نظام إدارة الهوية ما إذا كان التسجيل الواحد للخروج قابلاً للتطبيق ويتحقق من خدمات التطبيق الفاعلة.

4) إشعار [هوية المستعمل]. يرسل نظام إدارة الهوية إلى خدمة التطبيق C (تلفزيون بروتوكول الإنترنت) إشعار باستلام طلب بشأن إنهاء دورة الخدمة.

5) التبليغ عن تسجيل الخروج [هوية المستعمل]. يبلّغ نظامُ إدارة الهوية خدمةَ التطبيق B (بيانات) تسجيل الخروج.

6) إشعار [هوية المستعمل]. تقر خدمةَ التطبيق B (بيانات) بتسجيل الخروج.

7) التبليغ عن تسجيل الخروج [هوية الجهاز]. يبلّغ نظامُ إدارة الهوية خدمةَ التطبيق A (الصوت عبر بروتوكول الإنترنت) تسجيل الخروج.

8) إشعار [هوية الجهاز]. تقر خدمةُ التطبيق A (الصوت عبر بروتوكول الإنترنت) بتسجيل الخروج.

9) إشعار بالتسجيل الواحد للخروج [هوية المستعمل]. ترسل أنظمة إدارة الهوية إشعاراً إلى المستعمل تؤكد فيه تسجيل الخروج من جميع خدمات التطبيق الفاعلة في الدورة.

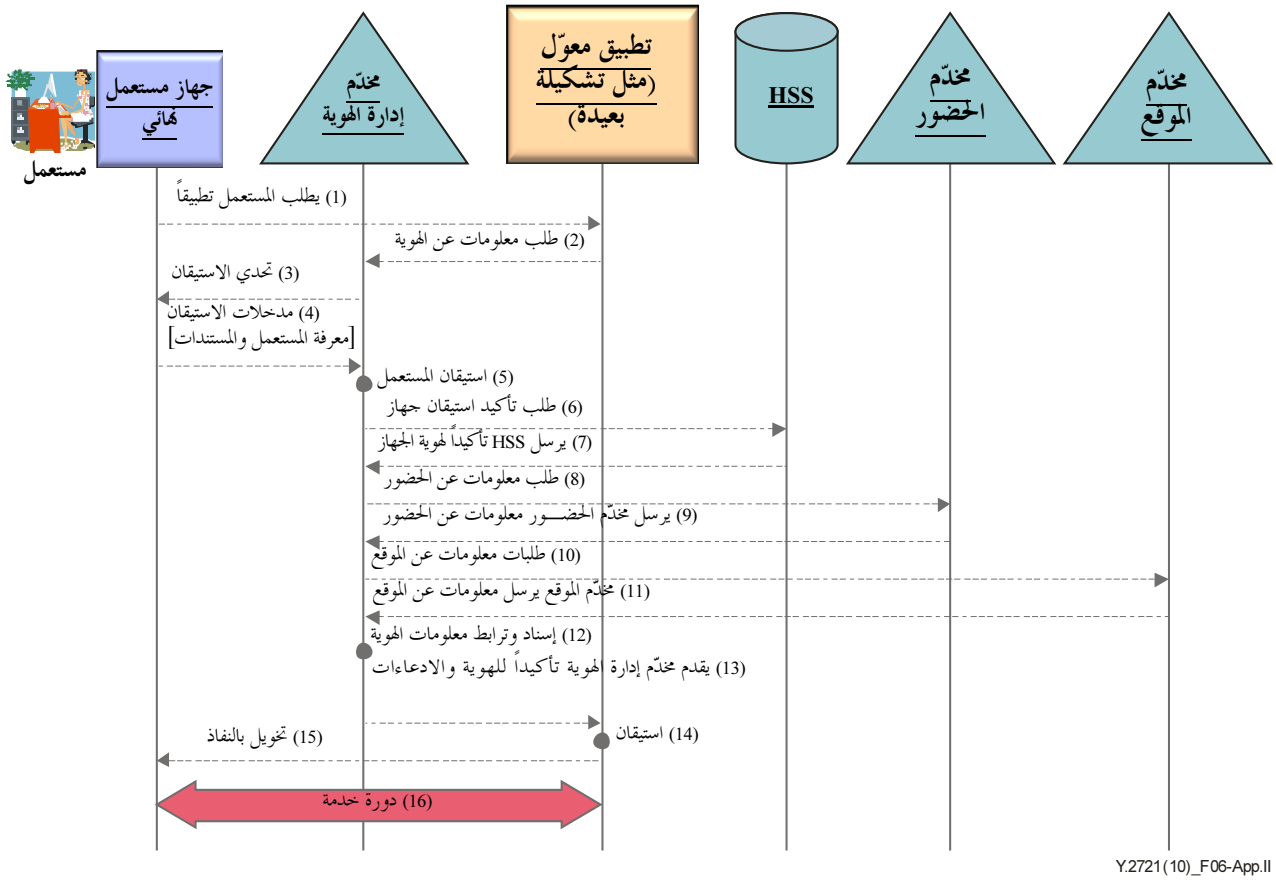
5.II ترابط معلومات الهوية الموزعة في ضمان الاستيقان متعدد العوامل

1.5.II نظرة عامة

تبين حالة الاستعمال هذه استخدام إدارة الهوية لإقامة الترابط والإسناد بين أجزاء متعددة من معلومات الهوية (ومثالها، معرفات الهوية والمستندات والنعوت) لضمان هوية مستعمل نهائي/مشترك. فعلى سبيل المثال، يمكن الربط بين معلومات الهوية المرتبطة بمشترك (مثل هوية مستعمل (UserID)) وجهاز المشترك (DeviceID مثلاً) ومعلومات الموقع لتوفير ضمان أعلى بشأن المشترك.

2.5.II مثال عن حالة استعمال

يبين الشكل II-6 مثالاً عن حالة استعمال تسند هوية المستعمل إلى هوية الجهاز وتربطهما مع معلومات الحضور والموقع لتوفر مستوى أعلى من الضمان بشأن الهوية والادعاءات المرتبطة بها.



الشكل II-6 – ترابط معلومات الهوية

في هذا المثال، يسعى المستعمل النهائي/المشترك للنفاذ إلى تطبيق يتطلب مستوى عالياً من الضمان بشأن هوية المستعمل والامتيازات المرتبطة بالهوية بسبب المخاطر الأمنية التي ينطوي عليها السماح غير المخوّل بالنفاذ إلى التطبيق أو المورد، والتي يمكن أن تكون مكلفة.

وفيما يلي انسيابات النداء في المثال:

1) يطلب المستعمل النفاذ إلى التطبيق.

2) يرسل التطبيق طلباً إلى مخدّم إدارة الهوية بشأن تأكيدات هوية المستعمل والادعاءات المرتبطة بالهوية.

3) يرسل مخدّم إدارة الهوية تحدياً إلى المستعمل.

4) يقدم المستعمل إلى مخدّم إدارة الهوية مدخلات للاستيقان (مثل هوية المستعمل والمستندات).

5) يستيقن مخدّم إدارة الهوية من المستعمل.

6) يرسل مخدّم إدارة الهوية طلباً إلى مخدم المشترك المنزلي (HSS) لتأكيد هوية جهاز المستعمل (يُلاحظ أنه يُفترض أن جهاز المستعمل النهائي يتسجل ويُستيقن منه لدى الشبكة باستخدام الإجراءات العادية).

7) يرسل مخدم المشترك المنزلي تأكيداً بشأن هوية جهاز المستعمل.

8) يرسل مخدّم إدارة الهوية طلباً إلى مخدم الحضور للحصول على معلومات عن الحضور.

9) يقدم مخدم الحضور إلى مخدّم إدارة الهوية معلومات عن الحضور.

10) يرسل مخدّم إدارة الهوية طلباً إلى مخدم الموقع للحصول على معلومات عن الموقع.

11) يقدم مخدم الموقع إلى مخدّم إدارة الهوية معلومات عن الموقع.

12) يُسند مخدّم إدارة الهويةِ معلومات هوية المستعمل إلى معلومات هوية الجهاز. وتُربط الهوية المدمجة مع معلومات الحضور والموقع للتحقق من الادعاءات (الامتيازات مثلاً) المرتبطة بالهوية.

13) يزود مخدّمُ إدارة الهويةِ التطبيق بتأكيدات هوية المستعمل والادعاءات المرتبطة بالهوية.

14) يحدد التطبيق ما إذا كان المستعمل مخولاً بالنفاذ.

15) يُمنح المستعمل حق النفاذ إلى التطبيق.

16) تقام دورة الخدمة.

6.II إنفاذ تحكم المستعمل في المعلومات التي تعرف به شخصياً (مثل الأفضليات) عبر ميادين شبكة الند/مقدم الخدمة

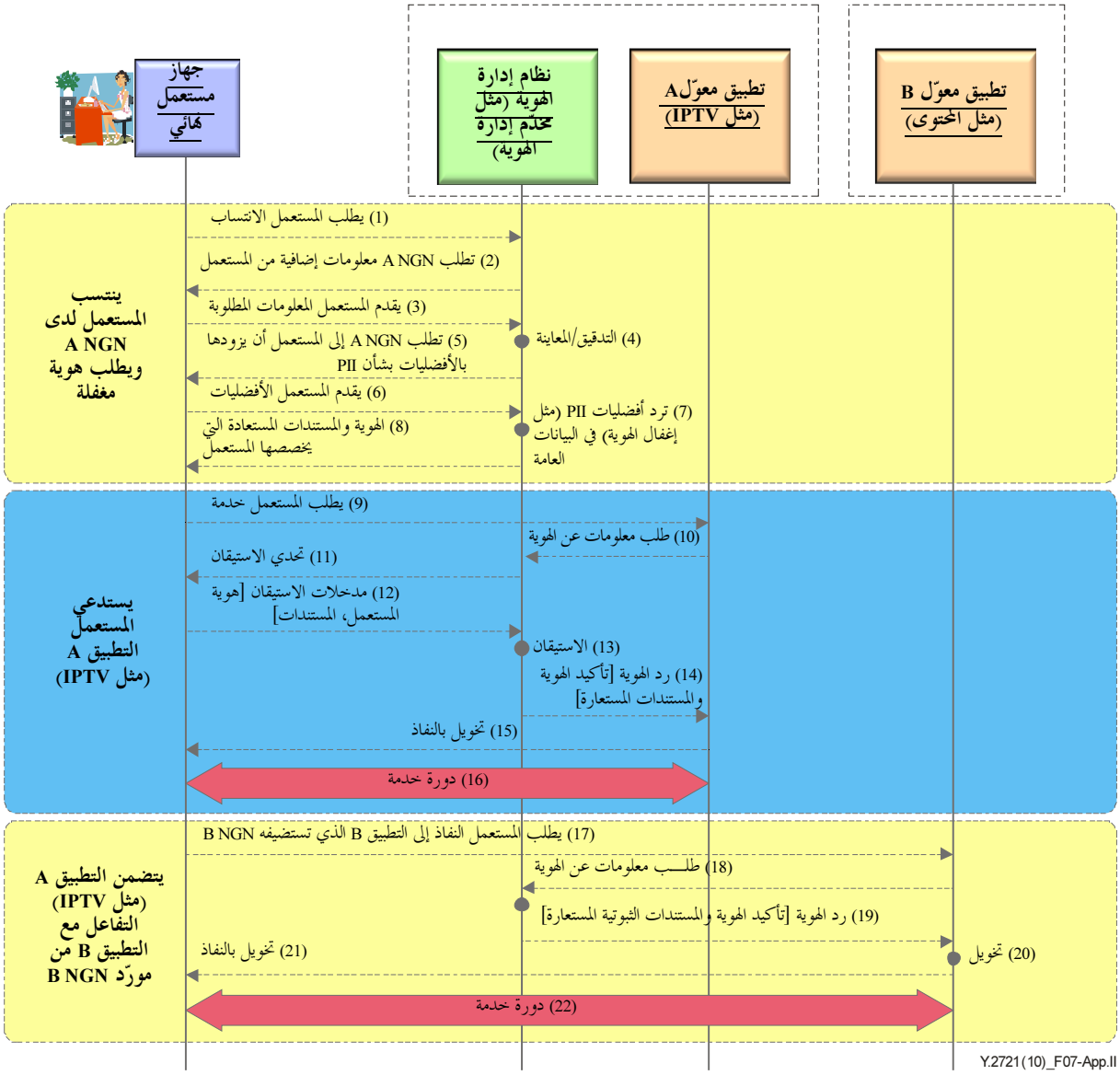
1.6.II نظرة عامة

تُعدّ حماية المعلومات التي تعرّف بأصحابها شخصياً أمراً بالغ الأهمية للمستعملين النهائيين/المشتركين. ومن الميزات الهامة لإدارة الهوية تمكينها للمستعملين النهائيين/المشتركين من موافاة مقدمي الخدمة وموردي الهوية بمعلومات عن الشروط والقيود والموافقات والتخويلات بشأن استحداث وجمع واستعمال ونشر معلومات الهوية الخاصة بهم.

2.6.II وصف حالة الاستعمال

ترتبط حالة الاستعمال هذه بإنفاذ السياسات المرعية كالسياسات المتعلقة بمعلومات الهوية المغفلة أو الواردة باسم مستعار.

يبين الشكل 7.II حالة استعمال يطلب فيها المستعمل عدم الكشف عن هويته.



الشكل 7.II – هوية المستعمل المغفلة

ملاحظـــة – يُستعمل مصطلح نظام إدارة الهوية كمصطلح عام للدلالة على أي عنصر من عناصر الشبكة التي يمكن أن توفر وظائف إدارة الهوية وتتيح إمكانيات مختلفة لتحقيقها أو تنفيذها.

يعرض مثال حالة الاستعمال قيام مورد شبكة الجيل التالي (مورد شبكات الجيل التالي A) بتخصيص أسماء مستعارة بناء على طلب مستعمل نهائي/مشترك بعدم الكشف عن هويته. وتُستعمل الهوية المغفلة للتفاعلات مع مورد شبكات الجيل التالي B لحماية المعلومات التي تعرّف شخصياً بالمستعمل النهائي المشترك.

وفيما يلي انسيابات النداء في المثال:

1) يطلب المستعملُ الانتساب لدى مورد شبكات الجيل التالي A.
2) يطلب مورد شبكات الجيل التالي A معلومات إضافية من المستعمل.
3) يقدم المستعملُ المعلومات المطلوبة إلى مورد شبكات الجيل التالي A.
4) يدقق مورد شبكات الجيل التالي A المعلومات ويتفحصها.
5) يطلب مورد شبكات الجيل التالي A إلى المستعمل أن يزوده بمعلومات عما يفضله بشأن المعلومات التي تعرّف بالمستعمل شخصياً.

6) يبين المستعمل أنه يفضل عدم الكشف عن هويته.

7) يدرج مورد شبكات الجيل التالي A تفضيل إغفال الهوية ضمن معلومات البيانات العامة للمستعمل.

8) يخصَّص المستعمل بهوية مستعارة وبمستند يُسنَد إليها.

9) يستدعي المستعملُ التطبيق A (تلفزيون بروتوكول الإنترنت (IPTV) مثلاً) الذي يستضيفه مورد شبكات الجيل التالي A.

10) يطلب التطبيقُ المعول A معلومات عن هوية المستعمل من نظام إدارة الهوية (مخدّم إدارة الهوية مثلاً).

11) يرسل نظام إدارة الهوية تحدي استيقان إلى المستعمل.

12) يقدم المستعمل إلى نظام إدارة الهوية مدخلات للاستيقان (مثل هوية المستعمل والمستندات).

13) يستيقن نظام إدارة الهوية من المستعمل.

14) يرسل نظام إدارة الهوية إلى التطبيق المعول A تأكيدات بشأن هوية المستعمل ومستنداته.

ملاحظـــة – لا تقدَّم إلا معلومات الهوية المستعارة لإنفاذ الإغفال.

15) يخوَّل المستعمل بالنفاذ إلى التطبيق A.

16) دورة الخدمة.

17) يطلب المستعمل النفاذ إلى التطبيق B الذي تستضيفه شبكة الجيل التالي B.

18) يرسل التطبيق B طلبات إلى نظام إدارة الهوية بشأن معلومات تؤكد هوية المستعمل والادعاءات المرتبطة بها.

19) يقدم نظام إدارة الهوية تأكيداً بشأن هوية المستعمل والادعاءات المرتبطة بها. ولا تُرسل إلا معلومات الهوية المستعارة لإنفاذ سياسة الإغفال.

20) يتحقق التطبيق B من المعلومات من أجل التخويل.

21) يخوَّل المستعمل بالنفاذ.

22) تقام دورة الخدمة.

7.II مد الجسور/التقابل بين أنظمة إدارة الهوية غير المتجانسة

1.7.II نظرة عامة

تدعو الحاجة لوجود آليات لمد الجسور ما بين مختلف أنظمة إدارة الهوية في شبكات الجيل التالي لتمكين المستعمل من الحصول على خدمات متعددة تقدمها مختلف مكونات هذه الشبكات. وتتضح هذه الحاجة في حالة الاستعمال الموصوفة في الفقرة التالية.

2.7.II وصف حالة الاستعمال

يصف هذا السيناريو نفاذ مشترك في شبكات الجيل التالي إلى مورد (مثل مخدّم الدليل) يقع في شبكة مؤسسة بواسطة مهتفته. وبما أن شبكات الجيل التالي وشبكات المؤسسات تستخدم آليات مختلفة لإدارة الهوية، تقتضي الحاجة مد جسور بين أنظمة إدارة الهوية في هذه الشبكات.

وتشترك الكيانات التالية في المثال الذي يوضح هذا السيناريو:

- نظام إدارة الهوية في شبكة الجيل التالي. يعدَّل هذا النظام بحيث يستطيع دعم الاستيقان المتبادل لمهتفة المستعمل على أساس اتفاق الاستيقان والمفتاح (AKA)، وأيضاً، تزويدها بالمستندات ليستيقن منها نظام إدارة الهوية في شبكة المؤسسة.
- إدارة الهوية في شبكة المؤسسة (مثل مركز توزيع المفاتيح)
- مخدّم دليل المؤسسة (EDS) الموجود في شبكة المؤسسة
- مهتفة المستعمل

تقوم هذه الكيانات بالتفاعلات التالية:

- تستيقن مهتفة المستعمل وشبكة الخدمة المتنقلة من بعضهما الآخر باستعمال طريقة اتفاق الاستيقان والمفتاح.
- يرسل المستعمل الذي يستخدم مهتفة طلباً إلى مخدّم دليل المؤسسة (EDS) الموجود في شبكة المؤسسة.
- يرد مخدّم دليل المؤسسة بطلب استيقان.
- يحصل المستعمل من نظام إدارة الهوية في شبكة الجيل التالي على مستندات الاستيقان (مثل بطاقة كربيروس (Kerberos)) القائمة على نتائج استيقان اتفاق الاستيقان والمفتاح، والصالحة للاستيقان لدى نظام إدارة الهوية في المؤسسة.

فعلى سبيل المثال، تحصل مهتفة المستعمل على بطاقة لمركز توزيع المفاتيح (KDC) في شبكة المؤسسة. وعلى وجه التحديد، فإن البطاقة تتيح الاستيقان من المستعمل لمخدم منح البطاقات (TGS) الذي يشكل جزءاً من مركز توزيع المفاتيح:

- يطلب المستعمل من مخدم منح البطاقات (TGS) بطاقة للاستيقان لدى مخدّم دليل المؤسسة (EDS).
- يتحقق مخدم منح البطاقات من صحة المستندات المقدمة ويرد على المستعمل ببطاقة لمخدّم دليل المؤسسة.
- يرد المستعمل النهائي على طلب الاستيقان الوارد من مخدّم دليل المؤسسة بالبطاقة التي وردته من مخدم منح البطاقات.
- يستيقن مخدّم دليل المؤسسة من المستعمل ويرد عليه بمستندات المخدم للاستيقان وبتأكيد للخدمة المطلوبة. وبعد التحقق من صحة مستندات المخدم، يستطيع المستعمل النفاذ إلى خدمة دليل المؤسسة.

3.7.II المتطلبات الضمنية

- على نظام إدارة الهوية في شبكة الجيل التالي أن يدعم آلية استيقان اتفاق الاستيقان والمفتاح (AKA) وآلية الاستيقان (مثل كربيروس (Kerberos)) التي تستعملها شبكة المؤسسة.
- يجب أن يتمكن نظام إدارة الهوية في شبكة الجيل التالي من إصدار مستندات الاستيقان (مثل بطاقة كربيروس (Kerberos)) إلى جهاز المستعمل النهائي كي يُستيقن المستعمل لدى نظام إدارة الهوية في المؤسسة.
- يجب أن يدير نظام إدارة الهوية في شبكة الجيل التالي هوية المستعمل ومستنداته.
- يجب أن يدير نظام إدارة الهوية في المؤسسة هوية المخدّم ومستنداته.

ملاحظـــة – (أ) لا تُطلب قدرة جديدة من شبكات الجيل الثالث (3G) (لذلك يمكن أن تكون مثالاً)؛ (ب) تطبَّق المتطلبات الواردة هنا لدعم حالة الاستعمال أعلاه على وجه التحديد.

8.II دعم الخدمات المتقاربة (كالنفاذ من الخدمة الثابتة والمتنقلة) ضمن شبكة مقدم الخدمة

1.8.II نظرة عامة

تعِد شبكات الجيل التالي بدعم عدد لا يحصى من الخدمات المتقاربة عبر شبكات النفاذ في الخدمة الثابتة والمتنقلة. وبذلك من شأن المستعمل أن يحظى بمرونة استدعاء خدمة ما باستعمال ما يلائمه من أجهزة النفاذ والشبكات في لحظة معينة. (وفي المقابل، من شأن مقدم الخدمة أن يوسع قاعدة زبائنه ويزيد عائداته). ونظراً للاختلاف النمطي بين آليات الأمن المناسبة التي ترتكز إليها البيئات الثابتة والمتنقلة، سيكون النظام المتقارب لإدارة الهوية الذي يمكنه معالجة هذه الاختلافات مفعّلاً مهماً. إذ أن الإدارة المتقاربة للهوية ستدير هويات ومستندات المستعملين النهائيين ومخدمات الشبكة بغض النظر عن تكنولوجيا النفاذ.

2.8.II وصف حالة الاستعمال

يصف هذا السيناريو نفاذ المشترك في شبكة الجيل الثالث (3G) بواسطة مهتفته إلى مورد (مثل مخدّم الفيديو عند الطلب) الموجود في شبكة الخدمة الثابتة. وفي هذا السيناريو، تُدعم آليات مختلفة في شبكة الجيل الثالث (3G) والشبكة الثابتة فيما يتعلق بإدارة الهوية. وتشترك الكيانات التالية في المثال الذي يوضح هذا السيناريو:

- نظام إدارة الهوية في شبكة الجيل الثالث (3G). يعدَّل هذا النظام بحيث يستطيع دعم الاستيقان المتبادل لمهتفة المستعمل على أساس اتفاق الاستيقان والمفتاح (AKA)، وأيضاً، تزويدها بالمستندات ليستيقن منها مخدم الفيديو عند الطلب (VoD).
- مخدم الفيديو عند الطلب الموجود في شبكة الخدمة الثابتة.
- مهتفة المستعمل من الجيل الثالث (3G).

تقوم هذه الكيانات بالتفاعلات التالية:

- تستيقن مهتفة المستعمل وشبكة الخدمة المتنقلة من بعضهما الآخر باستعمال طريقة اتفاق الاستيقان والمفتاح (AKA).
- يرسل المستعمل الذي يستخدم مهتفة طلباً إلى مخدّم الفيديو عند الطلب (VoD).
- يرد مخدّم الفيديو عند الطلب على المستعمل بطلب استيقان.
- يحصل المستعمل من نظام إدارة الهوية في شبكة الجيل الثالث على مستندات الاستيقان (مثل بطاقة كربيروس (Kerberos)) التي يصدرها النظام على أساس نتائج استيقان اتفاق الاستيقان والمفتاح.
- يرد المستعمل على مخدّم الفيديو عند الطلب بمستند الاستيقان (ببطاقة).
- يستيقن مخدّم الفيديو عند الطلب من المستعمل ويرد عليه بتأكيد للخدمة المطلوبة.

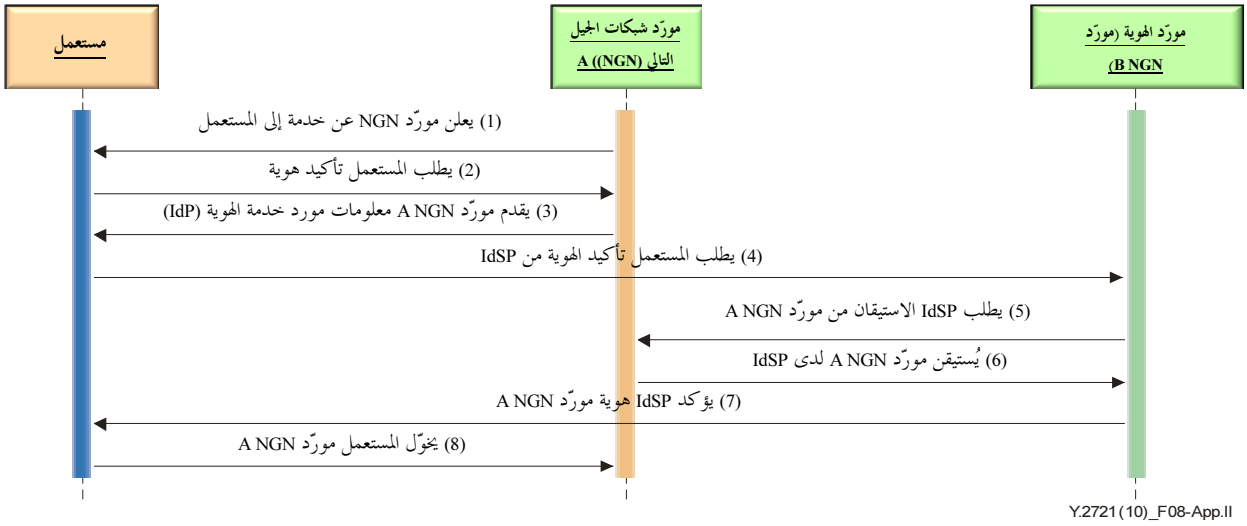
3.8.II المتطلبات الضمنية

- على نظام إدارة الهوية في شبكة الجيل التالي أن يدعم آلية استيقان اتفاق الاستيقان والمفتاح (AKA) وآلية الاستيقان (مثل كربيروس (Kerberos)) التي يستعملها مخدّم الفيديو عند الطلب (VoD).
- يجب أن يتمكن نظام إدارة الهوية من إصدار مستندات الاستيقان (مثل بطاقة) إلى جهاز المستعمل كي يُستيقن المستعمل لدى مخدّم الفيديو عند الطلب.
- يجب أن يدير نظام إدارة الهوية في شبكة الجيل الثالث هوية المستعمل ومستنداته.
- يجب أن يدير نظام إدارة الهوية في شبكة الجيل الثالث هوية ومستندات مخدّم الفيديو عند الطلب.

ملاحظـــة – تطبَّق المتطلبات الواردة هنا لدعم حالة الاستعمال المعروضة على وجه التحديد.

9.II مثال حالة استعمال – استيقان المستعمل من مورّد شبكات الجيل التالي وتخويله للمورّد (الاستيقان والتخويل المتبادل)

يبين الشكل 8.II مثال عن حالة استعمال تنطوي على استيقان المستعمل من مورّد شبكات الجيل التالي. ويفترض هذا المثال بيئة مفتوحة حيث يتمكن موردو شبكات الجيل التالي من الإعلان عن خدمات إلى المستعمل. ويوضح هذا المثال عن حالة الاستعمال ثغرات أو نواقص في قدرة المستعمل على الاستيقان من مورّد شبكات الجيل التالي وتخويله للمورّد (أو الاستيقان والتخويل المتبادل) في بيئة خدمة مفتوحة يتعدد فيها الموردون.



الشكل 8.II – مثال حالة استعمال: استيقان المستعمل من مورّد شبكات الجيل التالي وتخويله للمورّد

تلخَّص انسيابات النداء في المثال على النحو التالي:

1) يعلن مورّد شبكات الجيل التالي A عن خدمات إلى المستعمل.

2) يطلب المستعمل تأكيداً لهوية مورّد شبكات الجيل التالي A.

3) يقوم مورّد شبكات الجيل التالي A بتزويد المستعمل بعنوان مورد خدمة هوية.

4) يرسل المستعمل طلباً إلى مورد خدمة الهوية بشأن تأكيد هوية مورّد شبكات الجيل التالي A.

5) يرسل مورد خدمة الهوية طلبات إلى مورّد شبكات الجيل التالي A ليستيقن منه.

6) يقدم مورّد شبكات الجيل التالي A معلومات الاستيقان.

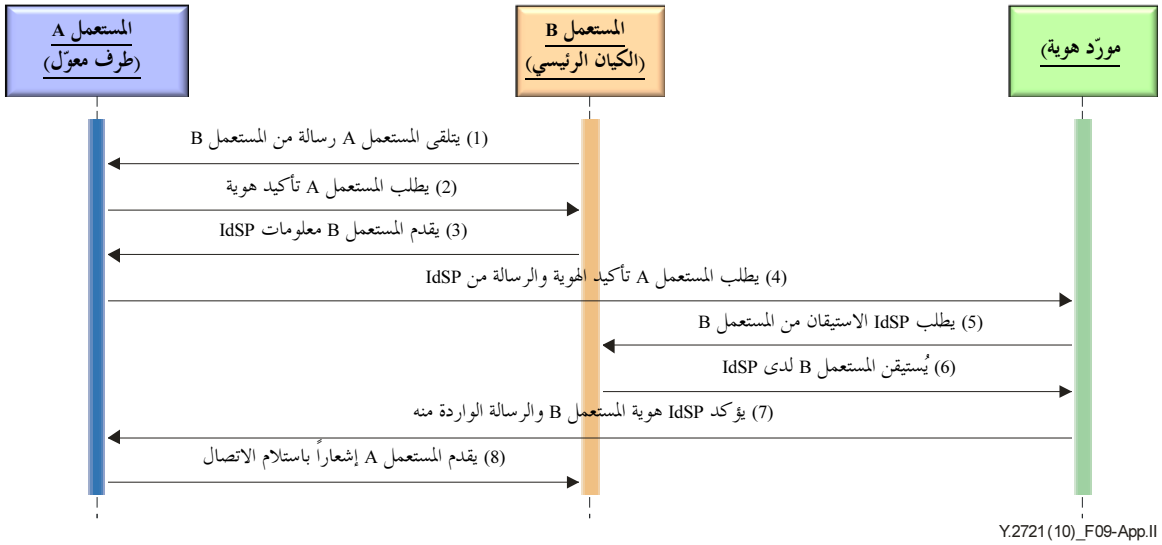
7) يرسل مورد خدمة الهوية معلومات إلى المستعمل مؤكداً هوية مورّد شبكات الجيل التالي A.

8) يخوّل المستعملُ مورّد شبكات الجيل التالي A بتقديم الخدمات.

ملاحظـــة – لا يظهر هذا المثال الانسيابات المتعلقة باستيقان مورّد شبكات الجيل التالي من المستعمل وتخويله للمستعمل.

10.II مثال حالة استعمال – تأكيد مستعمل ندي (المعاملات غير النقدية)

هناك حالياً نقص في قدرات إدارة الهوية في شبكات الجيل التالي للسماح للمستعملين بالاستيقان من منشأ الاتصال أو مصادر البيانات. وبصفة عامة، تركز نُهُج إدارة الهوية الجاري توصيفها أساساً على إدارة الهوية في المعاملات النقدية والتجارة الإلكترونية. ومن شأن شبكات الجيل التالي أن تحتاج إلى دعم قدرات إدارة الهوية لطائفة واسعة من المعاملات والاتصالات. وهذا أمر مهم خاصة لخدمات طوارئ معينة يتعين دعمها في شبكات الجيل التالي. ويظهر الشكل II-9 مثال عن حالة استعمال توضح الحاجة إلى قدرات إدارة الهوية في شبكات الجيل التالي للسماح للمستعملين بتأكيد هوية كل منهما الآخر في الاتصالات بين الأنداد والمعاملات غير النقدية. فعلى سبيل المثال، قد يحتاج المستعمل للاستيقان من مصدر رسالة وردته (مثل بريد إلكتروني أو رسالة فورية)، أو مصدر طلب اتصال (مثل اتصالات الصوت أو الفيديو أو البيانات) أو بيانات وردته. وهناك حالياً نقص في توصيف شبكات الجيل التالي لدعم قدرات إدارة هوية من هذا القبيل.



الشكل 9.II – مثال حالة استعمال – تأكيد مستعمل ندي (المعاملات غير النقدية)

يفترض مثال حالة الاستعمال المبين في الشكل 9-II أن المستعمل A يتلقى رسالة أو طلب للاتصال من المستعمل B، وأنه يرغب بتأكيد هوية المستعمل B والبيانات الواردة. وتلخَّص انسيابات النداء في المثال على النحو التالي:

1) يتلقى المستعمل A رسالة أو طلب للاتصال من المستعمل B.
2) يطلب المستعمل A تأكيداً لهوية المستعمل B ولمعلومات الاستيقان الواردة من المستعمل B.
3) يقوم المستعمل B بتزويد المستعمل A بعنوان مورّد خدمة الهوية.
4) يرسل المستعمل A طلبات إلى مورد خدمة الهوية بشأن تأكيد هوية المستعمل B والاستيقان من المعلومات الواردة.
5) يرسل مورد خدمة الهوية طلب إلى المستعمل B للاستيقان.
6) يرد المستعمل B ويُستيقن لدى مورّد خدمة الهوية.
7) يرسل مورد خدمة الهوية رداً إلى المستعمل A مؤكداً هوية المستعمل B والمعلومات الواردة.
8) يُشعر المستعملُ A المستعملَ B باستلام الاتصال.

11.II حالة استعمال إدارة الهوية – ضمان هوية وسلامة جهاز المستعمل النهائي

ستدعم شبكات الجيل التالي مجموعة متنوعة من أجهزة المستعمل (ومثالها، الهواتف الثابتة والمهتفات اللاسلكية والحواسيب الشخصية والمساعد الشخصي الرقمي والوحدات الطرفية للمشتركين في تلفزيون بروتوكول الإنترنت). وتتراوح مكونات العتاد والبرمجيات في الأجهزة المرفقة بشبكات الجيل التالي من البسيط إلى المعقد. وإذا ما سُرقت واختُرقت، يمكن استعمالها لتنسيق مجموعة متنوعة من الهجمات.

ويمكن تصميم قدرات أمنية خاصة وتنفيذها كجزء من مكونات العتاد المقاومة للعبث في أجهزة المستعمل النهائي لحفظ بيانات إدارة الهوية في شكل مجفّر ولدعم القدرات الأمنية المتخصصة للتحقق من هوية أجهزة المستعمل النهائي وضمان سلامتها. وتصف هذه الفقرة أمثلة عن حالات استعمال، حيث يمكن تصميم مكون عتاد أمني متخصص وتنفيذه كجزء من أجهزة المستخدم النهائي واستعماله لدعم خدمات إدارة الهوية الساعية لتحقيق ما يلي:

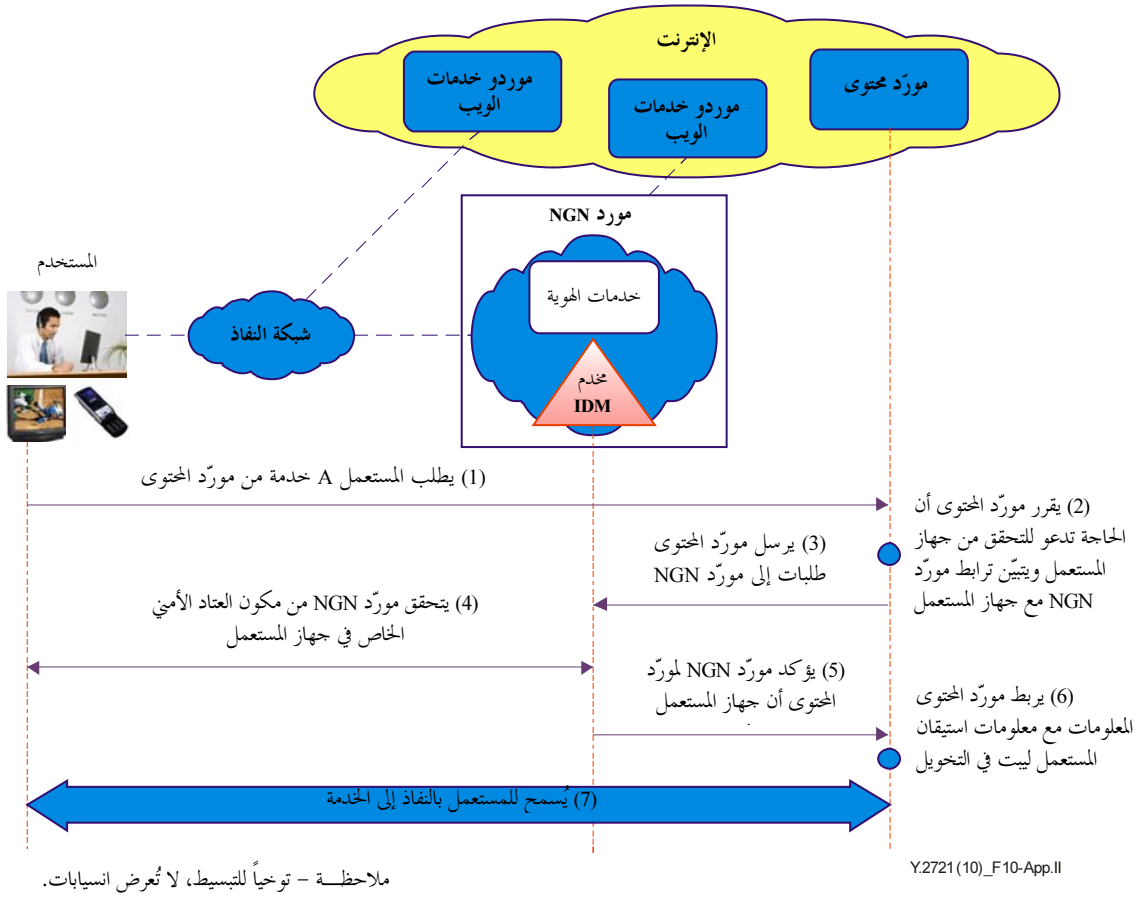
1) ضمان هوية جهاز المستعمل النهائي.
2) ضمان سلامة جهاز المستعمل النهائي (أي التحقق من عدم اختراق تشكيلة البرمجيات والعتاد).
3) السماح للمستعملين بتجفير وحماية البيانات التي تعرِّف صاحبها شخصياً وغيرها من البيانات الحساسة في أجهزة المستعمل النهائي.

1.11.II مثال حالة استعمال – ضمان المستعمل والاستيقان من الجهاز

تنطوي حالة الاستعمال هذه على دعم مكون عتاد أمني متخصص مقاوم للعبث في أجهزة المستعمل النهائي لتحديد هوية الجهاز على نحو ينفرد به عن سواه. ومثال ذلك، كلمات المرور والمفاتيح الرقمية والشهادات التي يمكن حفظها في مكون العتاد الأمني المتخصص المقاوم للعبث في الجهاز لتحديد هويته على نحو ينفرد به عن سواه. ويمكن لمكون العتاد الأمني المتخصص أن يدعم سطوح بينية مقيّسة لبرمجة التطبيق (API) للسماح بدعم خدمات التطبيق الأمني التي تعتمد على مكون العتاد المتخصص كمرتكز ثقة لهوية جهاز المستعمل النهائي.

ويمكن إقامة ترابط لما يوفره مكون العتاد الأمني المتخصص المقاوم للعبث من تحديد للهوية واستيقان فريدين مع تحديد هوية المستعمل والاستيقان منه لتقديم درجة أعلى من الضمان للتحكم في النفاذ ضمن بيئة يتعدد فيها مقدمو الخدمة.

يبين الشكل II-10 مثالاً عن حالة استعمال حيث يُصمم مكون عتاد أمني متخصص مقاوم للعبث وينفَّذ في أجهزة المستعمل النهائي لتحديد هوية الجهاز على نحو ينفرد به عن سواه. وفي هذا المثال، يُفترض أن مورّد شبكات الجيل التالي يتحكم في مكون العتاد الأمني المتخصص المقاوم للعبث من خلال اتفاق تعاقدي مع المشترك. ويمكن لمورّد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) أن يقدم بعد موافقة مؤكدة من المستعمل خدمات الهوية لغيره من موردين (مثل موردي المحتوى وموردي خدمات الويب وأطراف ثالثة مورّدة) وشركاء يضمنون هوية جهاز المستعمل النهائي ويستيقنون منه. ومن شأن ذلك أن يجعل مقدمي الخدمة يثقون في هوية جهاز المستعمل النهائي وفي الاستيقان منه. ويمكن ربط المعلومات بشأن هوية جهاز المستعمل النهائي والاستيقان منه مع استيقان المستعمل للحصول على درجة أعلى من الضمان والثقة.



الشكل II.10 – ترابط الاستيقان من المستعمل ومن الجهاز من أجل الضمان

تلخَّص انسيابات النداء على النحو التالي:

1) يطلب المستعمل خدمة من مورّد محتوى.

2) يقرر مورّد المحتوى أن الحاجة تدعو للتحقق من جهاز المستعمل للسماح بالنفاذ إلى الخدمة ويتبين ترابط مورد شبكات الجيل التالي مع جهاز المستعمل.

3) يرسل مورّد المحتوى طلبات إلى مورّد شبكات الجيل التالي لتأكيد هوية واستيقان جهاز المستعمل.

4) يحدد مورّد شبكات الجيل التالي هوية مكون العتاد الأمني الخاص في جهاز المستعمل ويستيقن منه (مثلاً، من خلال التحقق من الشهادات المخزنة في مكون العتاد الأمني المقاوم للعبث في الجهاز).

5) يرسل مورّد شبكات الجيل التالي رداً إلى مورّد المحتوى مؤيداً صحة هوية واستيقان جهاز المستعمل.

6) يربط مورّد المحتوى المعلومات الواردة من مورّد شبكات الجيل التالي مع معلومات استيقان المستعمل ويبت في التخويل بالخدمة.

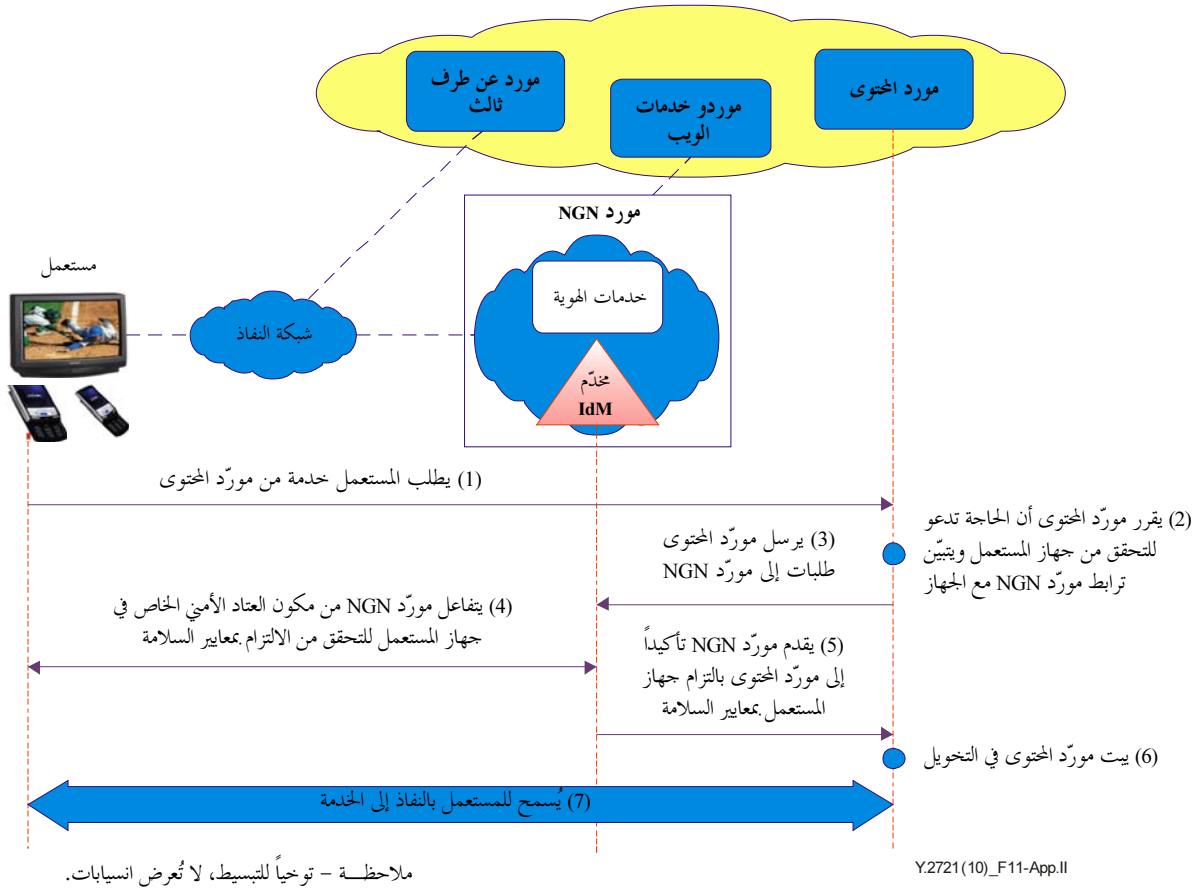
7) يُسمح للمستعمل بالنفاذ إلى خدمة (مثل المحتوى).

2.11.II مثال حالة استعمال – ضمان سلامة جهاز المستعمل

في البيئة الأمنية اليوم، يرتبط المشتركون بالشبكة باستخدام أجهزة مختلفة (ومثالها، الهواتف الثابتة والمهتفات اللاسلكية والحواسيب الشخصية والمساعد الشخصي الرقمي والوحدات الطرفية للمشتركين في تلفزيون بروتوكول الإنترنت). وقد تُخترق سلامة أجهزة المستعمل النهائي (مثل تشكيلة البرمجيات والعتاد) بسهولة على غفلة من المستعمل/المشترك. فتطبيقات الإنترنت الرائجة مثل متصفحات الويب والبريد الإلكتروني وغيرها من التطبيقات التي تنفّذ على أجهزة المشتركين للسماح للمشتركين بالتفاعل مع الخدمات ومع مميزات الجهاز المحلي، يحتمل أن تهدد سلامة الجهاز باستحداث نقاط ضعف فيه. فعلى سبيل المثال، قد تكمن في هذه التطبيقات عيوب أمنية خافية، أو قد تتيح ميزات يمكن استغلالها مثل تحميل الملفات، وبرمجيات، وملحقات برمجية للمتصفح، ووصلات برمجية مبيّتة. فتحميل البرمجيات والملفات، وبخاصة من مصدر غير موثوق، يعرّض أجهزة المشترك للشفرات الخبيثة والديدان والفيروسات وأحصنة طروادة. فمسجلات المفاتيح (التي تسجل جميع المدخلات عبر لوحة المفاتيح، بما في ذلك أسماء المستعملين وكلمات المرور، ثم تنقل هذه المعلومات إلى مهاجم يستطيع أن يستعملها للنفاذ غير المخول به) هي من الأنماط الشائعة من الشفرات الخبيثة. وتشمل الأنماط الأخرى من الشيفرات الخبيثة برمجيات التجسس (البرامج التي تتبع نشاط المشترك) وبرمجيات الإعلانات المتسللة (التي تزج بإعلانات غير مرغوب فيها، غالباً ما تستند إلى معلومات جُمعت من خلال مراقبة المشترك). فبعض هذه البرامج يختطف، بكل معنى الكلمة، أجهزة المشترك، ويعتم على وجوده بالاختباء في عمق ثنايا نظام التشغيل.

وتنطوي حالة الاستعمال هذه على دعم مكون عتاد أمني متخصص مقاوم للعبث في أجهزة المستعمل النهائي لمعاينة سلامتها وتأكيد هذه السلامة للتطبيقات والخدمات. فعلى سبيل المثال، قد يحوي مكون العتاد المتخصص المقاوم للعبث خوارزميات خاصة بالبائع تؤدي وظيفة التفتيش عن الخروق التي تنال من السلامة. فقد يتضمن هذا المكون نموذجاً مرجعياً بمجموعة من مقاييس السلامة المعروفة جيداً التي تتعرف على الشفرة الصحيحة تحديداً وتوفر قيماً مرجعية للجهاز. فتُستعمل هذه المقاييس لمقارنة القيم الفعلية مع التشكيلة للوقوف على ما إذا كانت الوحدة ضمن حدود الالتزام.

ويبين الشكل 11.II مثالاً عن حالة استعمال حيث يُصمم مكون عتاد أمني متخصص مقاوم للعبث وينفَّذ في جهاز المستعمل النهائي للتحقق من سلامة الجهاز. وفي هذا المثال، يُفترض أن مورّد شبكات الجيل التالي يتحكم في مكون العتاد الأمني المتخصص المقاوم للعبث من خلال اتفاق تعاقدي مع المشترك. ويمكن لمورّد شبكة الجيل التالي/مورّد خدمة الهوية (NGN/IdSP) أن يقدم بعد موافقة مؤكدة من المستعمل خدمات الهوية لغيره من موردين (مثل موردي المحتوى وموردي خدمات الويب وأطراف ثالثة مورّدة) وشركاء يتحققون من سلامة والتزام جهاز المستعمل النهائي.



الشكل 11.II – ضمان سلامة الجهاز

تلخَّص انسيابات النداء في المثال على النحو التالي:

1) يطلب المستعمل خدمة من مورّد محتوى.

2) يقرر مورّد المحتوى أن الحاجة تدعو للتحقق من سلامة جهاز المستعمل ويتبين ترابط مورّد شبكات الجيل التالي مع جهاز المستعمل.

3) يرسل مورّد المحتوى طلبات إلى مورّد شبكات الجيل التالي لتأكيد سلامة جهاز المستعمل.

4) يتفاعل مورّد شبكات الجيل التالي مع مكون العتاد الأمني المقاوم للعبث في جهاز المستعمل للتحقق من الالتزام بمعايير السلامة.

5) يقدّم مورّد شبكات الجيل التالي تأكيداً إلى مورّد المحتوى بسلامة جهاز المستعمل.

6) يبت مورّد المحتوى في التخويل.

7) يُسمح للمستعمل بالنفاذ إلى خدمة (مثل المحتوى).

3.11.II مثال حالة استعمال – تجفير المعلومات التي تعرِّف صاحبها شخصياً والملفات/البيانات الحساسة

يمكن لفقدان أو سرقة جهاز يحوي معلومات تعرِّف صاحبها شخصياً وبيانات حساسة أخرى أن يجر عواقب وخيمة على الأفراد وقطاع الأعمال والمؤسسات الحكومية. ومن ثم، فإن مكون العتاد المتخصص المقاوم للعبث والمصمم لتحديد هوية الأجهزة الموثوقة على نحو تنفرد به عن سواها يمكنه أيضاً دعم قدرات محتملة لتجفير وحماية معلومات تعرِّف صاحبها شخصياً وبيانات حساسة أخرى في أجهزة المستعمل النهائي. وبتجفير البيانات السرية، يتعذر على الأطراف غير المخول لها النفاذ إلى البيانات الموجودة على الحواسيب أو الهواتف الخلوية أو أجهزة التخزين، مما يغني عن اتخاذ إجراءات تصحيحية واسعة النطاق، ناهيك عن تحمل التكاليف.

التذييل III

حالات استعمال إدارة الهوية المتعلقة بخدمة اتصالات الطوارئ (ETS)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.III المقدمة

يقدم هذا التذييل أمثلة لحالات استعمال إدارة الهوية المتعلقة بخدمة اتصالات الطوارئ. وخدمة اتصالات الطوارئ عبارة عن خدمة تحتاج إلى أولوية في معالجتها. انظر الفقرة 7.4.8.

2.III ضمان الاستيقان باستعمال الجهاز والمستعمل معاً

من الضروري استيقان المستعملين المخوّلين لخدمة اتصالات الطوارئ لحماية تيسّر هذه الاتصالات والشبكات المرتبطة بها وسلامتها. وهناك طريقتان أساسيتان للاستيقان تستعملان في الوقت الحالي من التطبيقات التقليدية لخدمة اتصالات الطوارئ وهما:

1 طريقة تعتمد على رقم تعرّف الهوية الشخصي (PIN)؛

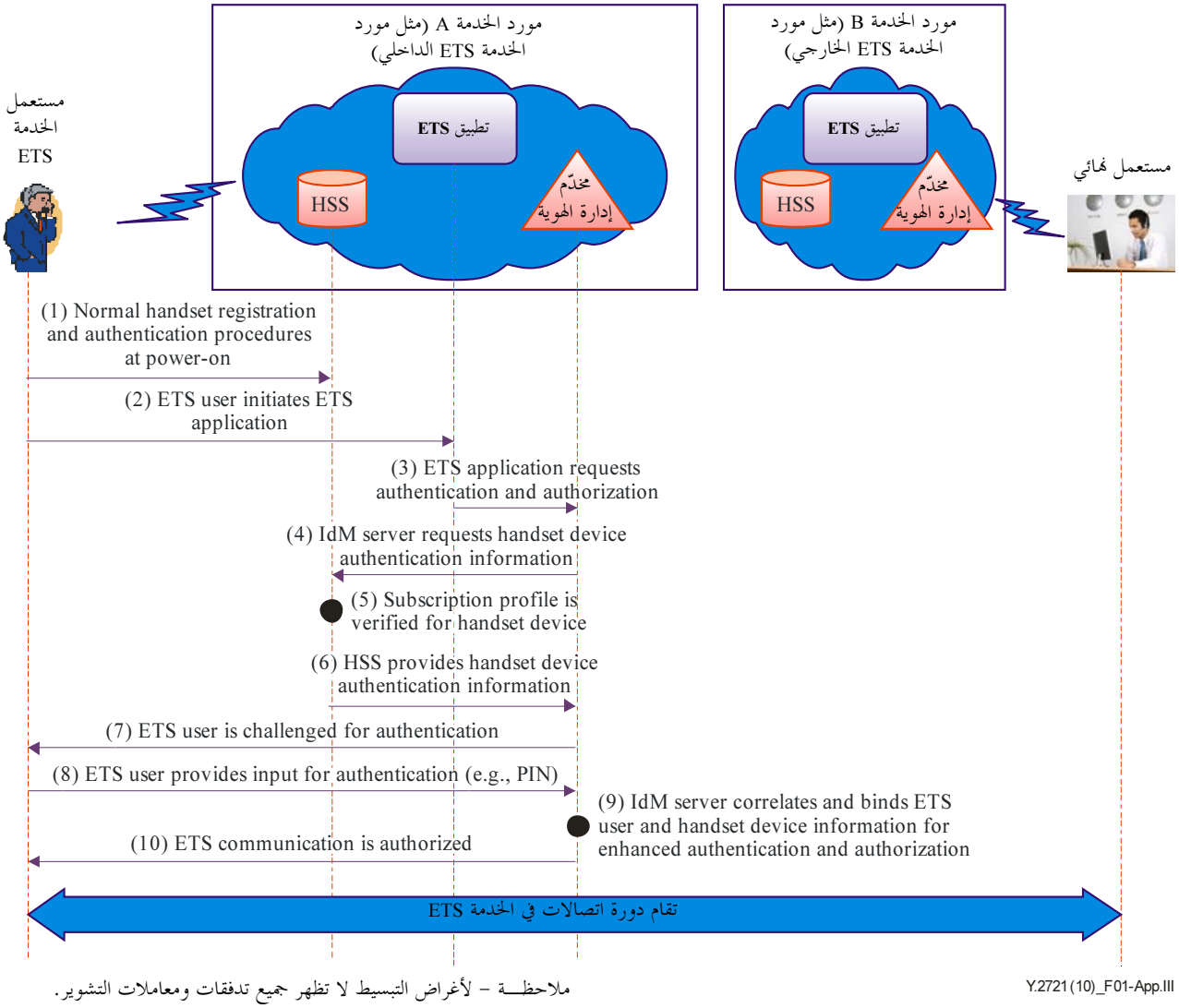
2 طريقة تعتمد على الاشتراك.

وتشمل الطريقة الأولى استعمال أرقام تعرّف الهوية الشخصية للاستيقان والتحويل. ويؤدي التحقق من الرقم PIN إلى استيقان المستعمل ومن ثم تخويله استعمال خدمة اتصالات الطوارئ. ويتعرّف هذا النهج على المستعمل وليس جهاز المستعمل. وبالتالي، فإن هذه الطريقة تستعمل عادة في الحالات التي يسمح فيها للمستعمل بالنفاذ إلى خدمة اتصالات الطوارئ من أي جهاز.

وتشمل الطريقة الثانية الاستيقان والتخويل استناداً إلى معلومات المظهر الجانبي للاشتراك المرتبطة بجهاز مطرافي معيّن أو جهاز معين لمستعمل نهائي. ويجري استيقان هوية جهاز المستعمل أو الجهاز المطرافي كجزء من التسجيل والاستيقان المعتادين لمورد شبكة الجيل التالي (أي مورد خدمة اتصالات الطوارئ) وتخوّل النداءات/الدورات الإفرادية لخدمة اتصالات الطوارئ بالتحقق من المظهر الجانبي للاشتراك (أي التحقق مما إذا كان الاشتراك في الخدمة يجيز تبادل نداءات/دورات خدمة اتصالات الطوارئ من هذا الجهاز أم لا).

ويستيقن هذا النهج جهاز المستعمل (أي جهاز اليد اللاسلكي) وليس المستعمل. واستعمال الطريقتين البسيطتين التي تعتمد على رقم تعرف الهوية الشخصي والتي تعتمد على الاشتراك يعتبر كافياً للتطبيقات التقليدية لخدمة اتصالات الطوارئ. بَيد أن هاتين الطريقتين البسيطتين لا تكفيان لجميع أنماط تطبيقات خدمة اتصالات الطوارئ في بيئة شبكات الجيل التالي. وتحديداً، فإن تطبيقات مثل خدمات الأولوية متعددة الوسائط (مثل خدمات البيانات والفيديو) تحتاج إلى درجة أكبر من الضمان أو الثقة في هوية مستعمل خدمة اتصالات الطوارئ ومن مستوى التخويل بالنفاذ إلى تطبيقات خدمة اتصالات الطوارئ والموارد المرتبطة بها. وبالتالي، فإنه إضافة إلى دعم طريقتي الاستيقان الحاليتين المشار إليهما آنفاً، فإن شبكات الجيل التالي تحتاج كذلك إلى أن تدعم آليات معزّزة لاستيقان وتخويل مستعملي خدمة اتصالات الطوارئ وأجهزتها.

وهناك نهج يستحق الدراسة في مجال انتقال خدمة اتصالات الطوارئ (أي خدمات صوتية ذات أولوية) إلى بيئة شبكات الجيل التالي يتمثل في استعمال إدارة الهوية لربط وتلازم استيقان المستعمِل وتعرف هوية جهاز المستعمل واستيقانه. وسيوفر ذلك ضماناً محسناً (أي ثقة) في هوية وتخويل المستعمل للنفاذ إلى خدمة اتصالات الطوارئ. والمفهوم المقصود يرد توضيحه في المثال التالي لحالة استعمال عام.



الشكل 1.III – استيقان مشترك للمستعمل والجهاز

ويبين الشكل 1.III مثالاً لحالة استعمال تستعمل فيه وظائف إدارة الهوية في الاستيقان المشترك للمستعمل والجهاز من أجل ضمان معزز لاستيقان مستعمل خدمة اتصالات الطوارئ.

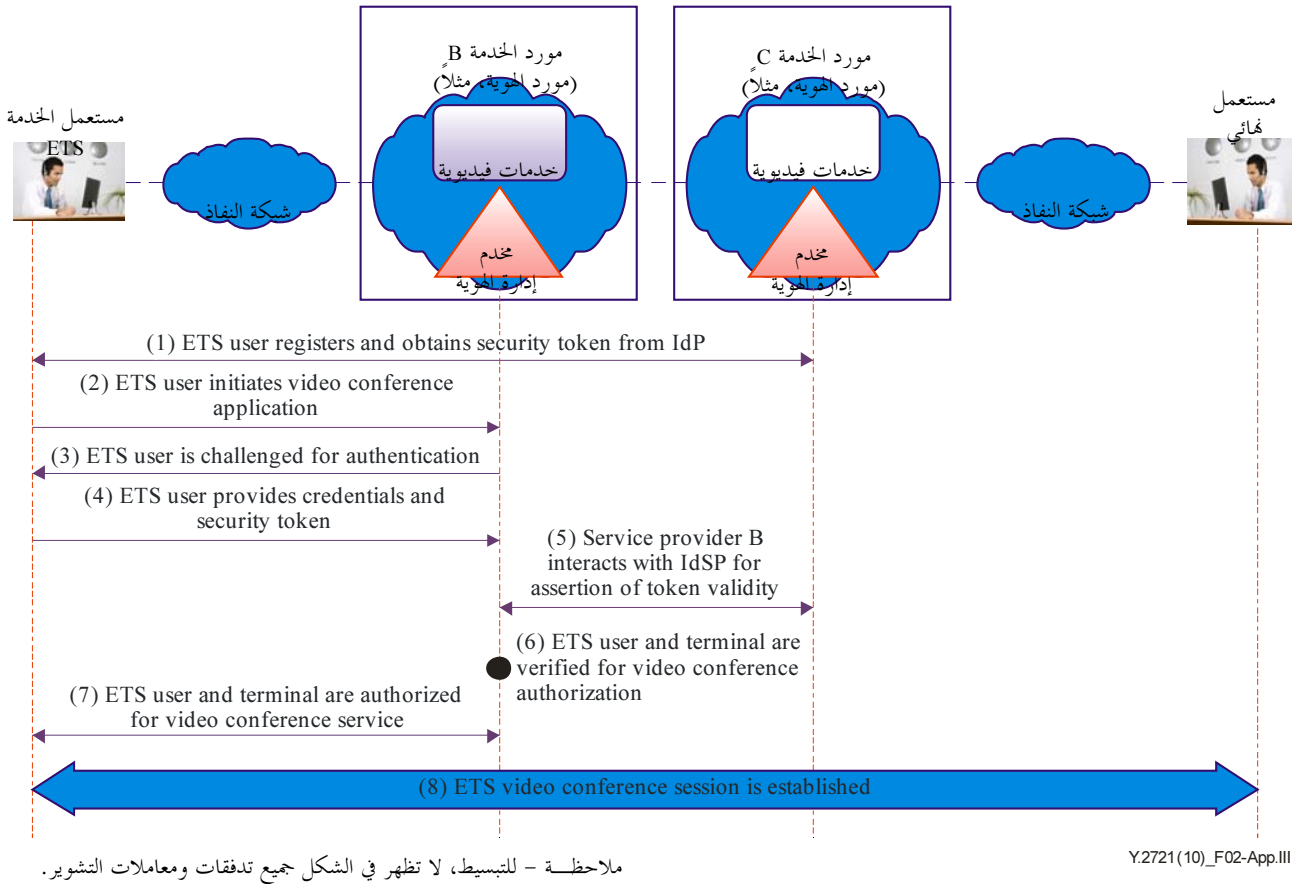
ويمكن تلخيص تدفقات النداء في المثال التالي:

1) يتم تسجيل جهاز اليد للمستعمل واستيقانه باستعمال الإجراءات الاعتيادية بعد تشغيل الجهاز.
2) يقوم مستعمل الخدمة ETS باستهلال تطبيق للخدمة ETS.
3) يطلب تطبيق الخدمة ETS الاستيقان والتخويل من مخدّم إدارة الهوية.
4) يطلب مخدّم إدارة الهوية معلومات استيقان جهاز اليد من مخدّم المشترك المنزلي (HSS).
5) يتحقق مخدّم المشترك المنزلي من المظهر الجانبي لاشتراك جهاز اليد.
6) يزوّد مخدّم المشترك المنزلي مخدّم إدارة الهوية بمعلومات استيقان جهاز اليد.
7) يُطلب من مستعمل الخدمة ETS تعريف هويته من أجل الاستيقان.
8) يقدم مستعمل الخدمة ETS مدخلاته من أجل الاستيقان (مثل رقم تعرف الهوية الشخصي).
9) يقوم مخدّم إدارة الهوية بربط وملازمة معلومات مستعمل الخدمة ETS وجهاز اليد من أجل استيقان وتخويل معزّزين.
10) يتم تخويل إجراء دورة اتصالات في الخدمة ETS.

وينتُج عن مثال التدفقات هذا ضمان معزز لهوية مستعمل الخدمة ETS وتخويله باستعمال الخدمة. وضم استيقان الجهاز من المستعمل يحتاج إلى معاملات إضافية مع مستعمل الخدمة ETS من أجل الاستيقان وربما ينظر إليها باعتبارها أعباءً ثقيلة. ومع ذلك، قد لا تحتاج جميع دورات الخدمة ETS لذلك. ويمكن النظر في ذلك بالنسبة لدورات الخدمة ETS التي تحتاج إلى مستويات أعلى من الضمان.

3.III الاستيقان المعزز لمستعملي الخدمة ETS من أجل خدمات الأولوية في شبكات الجيل التالي (خدمات الأولوية متعددة الوسائط)

مع انتقال بيئة الاتصالات إلى بيئة شبكات الجيل التالي (NGN)/النظام الفرعي متعدد الوسائط القائم على بروتوكول الإنترنت (IMS)، سيتعيّن على مستعملي الخدمة ETS مواكبة التغيّرات التكنولوجية والاتجاهات الجديدة في مجال الاتصالات. فعلى سبيل المثال، سيزيد اعتماد مستعملي الخدمة ETS على الاتصالات التي تتجاوز الاتصالات الصوتية، مثل المراسلة اللحظية والمراسلة النصية والرسائل الإلكترونية لتنفيذ مهامهم. وبوجه عام، هناك مبادرات في مرحلتي التخطيط والتطوير بحيث يمكن لمستعملي الخدمة ETS الحصول على أولوية النفاذ إلى خدمات الوسائط المتعددة مثل خدمات الصوت والبيانات والفيديو. وبالتالي، فإن آليات الاستيقان القائمة على رقم تعرف الهوية الشخصي والاشتراك المستعملة من أجل الخدمة ETS في بيئة شبكة المهاتفة العمومية التبديلية (PSTN) لن تكون كافية لخدمات الوسائط المتعددة في بيئة شبكات الجيل التالي/النظام الفرعي متعدد الوسائط القائم على بروتوكول الإنترنت. وتحديداً، فإن تطبيقات مثل خدمات الأولوية متعددة الوسائط (مثل خدمات البيانات والفيديو) ستحتاج إلى درجة أعلى من الضمان أو الثقة في هوية مستعمل الخدمة ETS وفي مستوى التخويل بالنفاذ إلى تطبيقات الخدمة ETS والموارد المرتبطة بها وذلك للمستوى الأعلى من المخاطر والتهديدات الأمنية التي تتعرض لها بيئة شبكات الجيل التالي بوجه عام. كذلك، وخلافاً للخدمة ETS المدعومة من الشبكة PSTN، يتوقع ألا يتم تخويل خدمات الأولوية متعددة الوسائط من الجيل التالي إلا لعدد مختار من مستعملي الخدمة ETS. كما أنه نظراً للهدف العام لمستعملي الخدمة ETS والمتمثل في الحصول على نفاذ سهل لا ينطوي على أي تعقيدات في الاستعمال من أي مكان وفي أي وقت من أي جهاز، فإن من المهم النظر في آليات أكثر تقدماً لإدارة الهوية مع تحسينها حسبما يتناسب. وسيكون الضمان العالي لهوية المستعمل من الأمور الحاسمة لحماية سلامة وتيسّر خدمات الوسائط المتعددة في الخدمة ETS ومواردها والبيئة التحتية لشبكات الجيل التالي/النظام الفرعي متعدد الوسائط القائم على بروتوكول الإنترنت ككل خلال الكوارث وحالات الطوارئ. وتعتبر تطبيقات البيانات والفيديو متعددة الوسائط (مثل عمليات تحميل معلومات الويب أو مقاطع الفيديو) من التطبيقات التي تستهلك عرض النطاق والموارد بكثافة مقارنة بالتطبيقات الصوتية. وبدون ضوابط كافية، فإن النفاذ غير المخوّل إلى تطبيقات البيانات والفيديو للخدمة ETS قد يؤدي بآثار سلبية على تطبيقات الخدمة ETS نفسها وعلى بنية الاتصالات بالكامل بوجه عام. فعلى سبيل المثال، يمكن استعمال النفاذ غير المخوّل إلى تطبيق في الخدمة ETS كثيف في استهلاك الموارد في التسبّب في ازدحام الشبكة أو تنفيذ هجمات تعطيل الخدمة. وبالتالي، ينبغي النظر في نهج أكثر تعقيداً لاستيقان وتخويل مستعملي و/أو مطاريف الخدمة ETS وذلك باستعمال أمارات رمزية أمينة خاصة أو شهادات رقمية أو التمييز الصوتي أو الإمكانات البيومترية.



ملاحظـــة – للتبسيط، لا تظهر في الشكل جميع تدفقات ومعاملات التشوير.

الشكل 2.III – استيقان معزز من أجل خدمات الأولوية من الجيل التالي

يوضح الشكل 2.III مثالاً لحالة استعمال تضم استيقاناً معززاً لمستعملين مخولين لخدمات الأولوية متعددة الوسائط من الجيل التالي (مثل المؤتمرات الفيديوية). وتفترض حالة الاستعمال هذه أن إثباتات الهوية (أي الأمارات الرمزية الأمنية أو الشهادات الرقمية) تقدم من قِبل مورد خدمة هوية (IdSP) يختلف عن مورّد خدمة الوسائط المتعددة (على الرغم من أنه يمكن أن يكون مورّد الخدمة ومورد خدمة الهوية مورّداً واحداً). وفي حال اختلاف مورد الخدمة عن مورد خدمة الهوية، يتطلب ذلك إبراماً مسبقاً للاتفاقات الضرورية المتعلقة بالأعمال التجارية والضمان. ويستلزم ذلك إجراء استيقان متبادل بين مورد خدمة الهوية ومورد الخدمة.

وفيما يلي ملخص لتدفقات النداء:

1) يقوم مستعمل الخدمة ETS بالتسجيل أو الحصول على إثبات (أي إشارة رمزية أمنية أو شهادة رقمية) تعرف مستعمل الخدمة ETS وتحدد امتيازاته بالنسبة للخدمات متعددة الوسائط.

2) يقوم مستعمل الخدمة ETS باستهلاك تطبيق خاص بمؤتمر فيديو.

3) يطلب من مستعمل الخدمة ETS تعريف هويته من أجل الاستيقان.

4) يقدم مستعمل الخدمة ETS إثباتاته من أجل الاستيقان (مثل الإشارة الرمزية الأمنية أو الشهادة الرقمية).

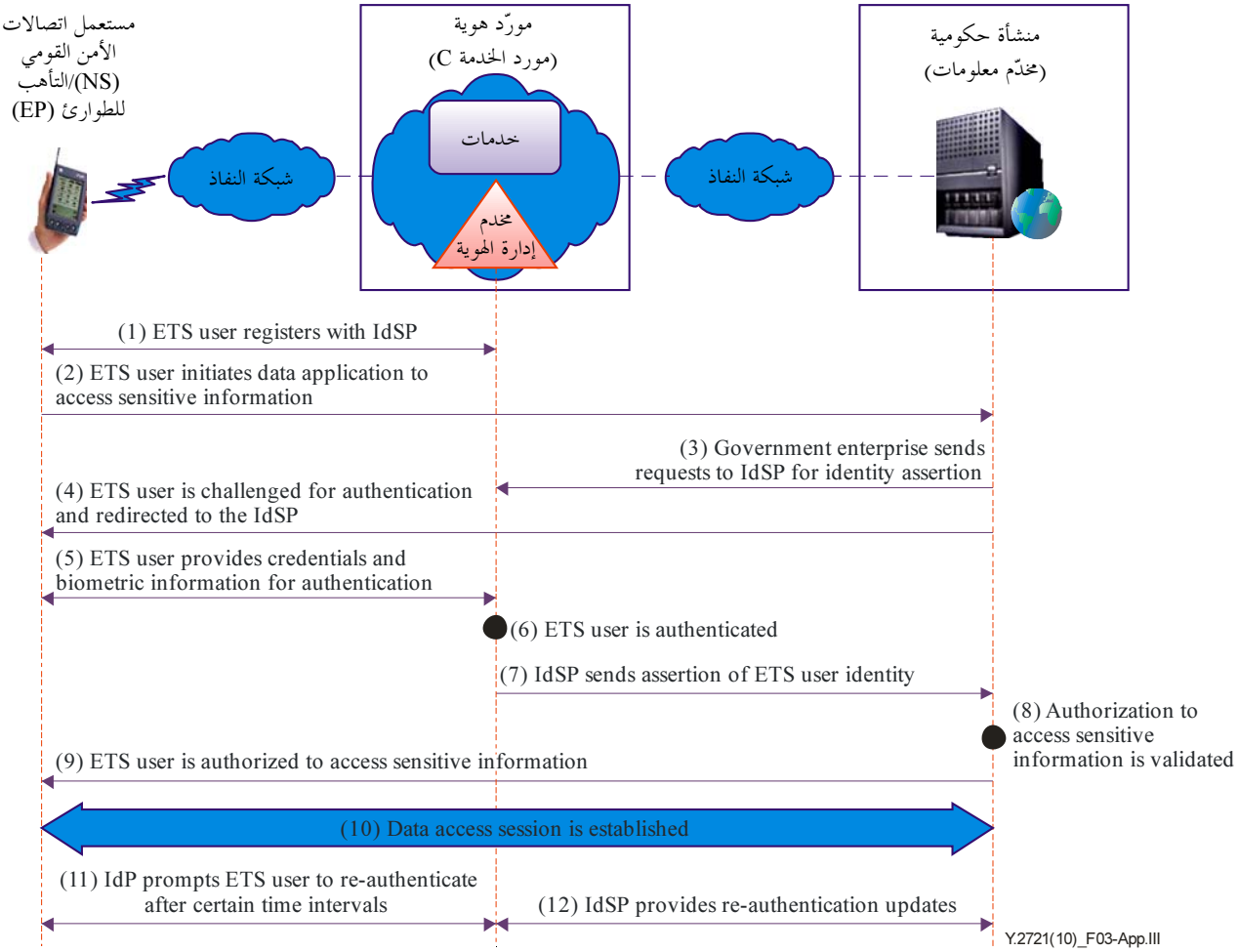
5) يتعامل مورد الخدمة B مع مورد خدمة الهوية (IdSP) طالباً منه التحقق من الإثباتات (مثل الإشارة الرمزية الأمنية أو الشهادة الرقمية).

6) يعالج مورد الخدمة B المعلومات ويتحقق منها لتحديد ما إذا كان مستعمل الخدمة ETS ومطرافه مخوّلين لخدمات الأولوية متعددة الوسائط.

7) يُخوّل مستعمل الخدمة ETS باستهلال خدمة أولوية متعددة الوسائط (مؤتمر فيديوي، مثلاً) بعد الاستيقان الناجح.

8) تقام وتحقق دورة متعددة الوسائط.

وقد تحتاج بعض اتصالات الوسائط المتعددة من الجيل التالي إلى استعمال معلومات بيومترية لاستيقان مستعملي الخدمة ETS المخوّلين. فمثلاً، قد تحتاج الطبيعة الحساسة لبعض المعلومات إلى تبادلها بين مجموعة فرعية من مستعملي الخدمة ETS المخوّلين فقط. وفي سيناريو كهذا، من المهم توفر درجة عالية من الثقة في التحقق من هوية مستعمل الخدمة ETS. وفي هذه الحالات، يمكن النظر في آليات بيومترية كتكنولوجيات يمكن استعمالها في التحقق.



ملاحظـــة – لأغراض التبسيط، لا تظهر في الشكل جميع تدفقات ومعاملات التشوير.

الشكل 3.III – مثال لحالة استعمال للوسائل البيومترية

يعرض الشكل 3.III مثالاً لحالة استعمال تضم وسائل بيومترية. ويُفترض في هذا المثال أن جهاز اليد الخاص بالمستعمل مجهز بالإمكانية المناسبة لقراءة المعلومات البيومترية. كما يُفترض أن مستعمل الخدمة ETS يقوم بالتسجيل المسبق مع مورّد خدمة الهوية، وأنه يتم الحصول على المعلومات البيومترية وتخزينها. ويلاحظ أيضاً أنه يمكن للمنشأة الحكومية استضافة خدمات الهوية وتقديمها (مثل تسجيل هوية مستعمل الخدمة ETS ومعلوماته البيومترية وحفظها) بدلاً من استعمال خدمات طرف ثالث مورد للخدمة. وفيما يلي ملخص لتدفق النداء:

1) يقوم مستعمل الخدمة ETS بالتسجيل مع مورد خدمة الهوية لتنشيط خدمة استيقان الوسائل البيومترية. ويفترض أن العمليات اللازمة لجمع المعلومات البيومترية ومعلومات الهوية الأخرى والتثبّت منها قد تمت بالفعل (مثل التسجيل الشخصي).

2) يقوم مستعمل الخدمة ETS باستهلال اتصال من أجل النفاذ عن بُعد إلى قاعدة بيانات المنشأة الحكومية التي تستضيف معلومات حساسة.

3) تشير السياسات الأمنية للمنشأة الحكومية إلى أنه يلزم مستوى عال من الضمان للسماح بالنفاذ، وتبدأ في إجراء عكسي مع مورّد خدمة الهوية.

4) يُطلب من مستعمل الخدمة ETS الاستيقان ويُعادُ توجيهه إلى مورد خدمة الهوية.

5) يقوم مستعمل الخدمة ETS بتقديم مدخلات الاستيقان. ومثال ذلك مسح بصمة الإبهام على ماسح بيومتري خاص مدمج في جهاز يد لاسلكي.

6) يستعمل مورد خدمة الهوية المعلومات المدخلة للاستيقان من مستعمل الخدمة ETS.

7) يرسل مورد خدمة الهوية معلومات إلى المنشأة الحكومية تؤكد هوية مستعمل الخدمة ETS.

8) تتحقق المنشأة الحكومية مما إذا كانت هوية مستعمل الخدمة ETS تخوّل له النفاذ إلى مخدم المعلومات الذي يستضيف البيانات الحساسة.

9) يخوّل لمستعمل الخدمة ETS النفاذ.

10) تقام دورة نفاذ إلى البيانات.

11) يحض مورد خدمة الهوية مستعمل الخدمة ETS لإعادة الاستيقان بعد فترة زمنية محددة نتيجة للسياسات الأمنية الخاصة بالنفاذ إلى مخدّم معلومات المنشأة الحكومية.

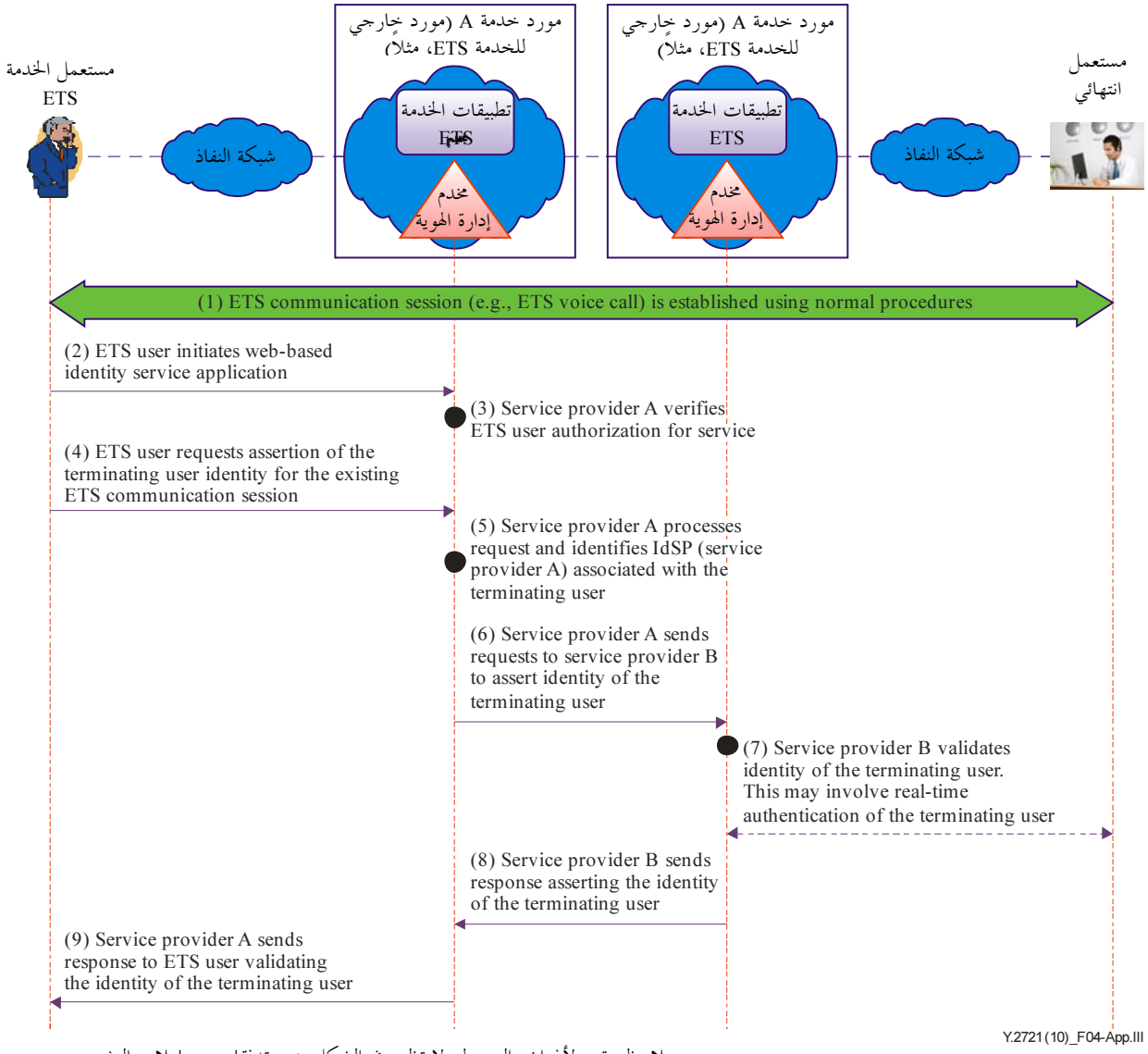
12) يقدم مورد خدمة الهوية معلومات عن إعادة استيقان مستعمل الخدمة ETS إلى المنشأة الحكومية.

4.III استيقان الطرف المنادى عليه ومصادر اتصالات البيانات

لا توجد حالياً آليات محددة كجزء من تطبيقات الخدمة ETS ذاتها لاستيقان الطرف المنادى عليه في دورة الاتصالات (أي جانب انتهائية نداء الخدمة ETS). وفي البيئة المغلقة للشبكات PSTN، لم يكن ذلك بالأمر الهام. بَيد أنه مع الانتقال إلى بيئة IMS/NGN مع النقل القائم على بروتوكول الإنترنت، فإن ذلك يسمح بإمكانية تزييف رقم الطرف المنادى عليه والمعلومات الخاصة بالتسيير مما يؤدي إلى تهديدات متعلقة بالتزوير.

وفي المستقبل، يمكن تعزيز خدمات إدارة الهوية التي يقدمها موردو خدمات الاتصالات (CSP) والأطراف الثالثة من مورّدي الخدمات لاستيقان الطرف المنادى عليه أو جانب إنهاء دورات اتصالات الخدمة ETS. ويمكن لمورّد الخدمة ETS تحديداً أن يدعم قدرات إدارة الهوية لتقديم خدمات الهوية من أجل استيقان المستعملين وضمان هوياتهم. ومن أمثلة معلومات الهوية عوامل التحقق ببساطة من الخط واسم الطرف الطالب أو استعمال آليات استيقان أقوى مثل الأمارات الرمزية الأمنية أو البطاقات الذكية أو الشهادات الرقمية للتأكد من هوية المستعمل.

ويوضح الشكل 4.III مثالاً لحالة استعمال تضم التأكد من مستعمل الانتهائية في دورة اتصالات للخدمة ETS (مثل نداء صوتي في الخدمة ETS). تفترض حالة الاستعمال هذه تحديداً أن مستعمل الخدمة ETS يقوم بالتسجيل المسبق مع مورّد خدمة ETS من أجل خدمات هوية قائمة على الويب. وبعد إقامة اتصال ETS (نداء صوتي في الخدمة ETS، مثلاً) لمستعمل في شبكة عمومية، يقوم مستعمل الخدمة ETS باستهلال خدمة هوية عبر بوابة ويب للتحقق من هوية مستعمل الانتهائية عند الطرف الآخر من الاتصالات ETS. وفي حالة الاستعمال هذه، لا تعتمد إقامة دورة اتصال ETS على خدمة الهوية المستعملة في التأكد من هوية مستعمل الانتهائية.



ملاحظـــة – لأغراض التبسيط، لا تظهر في الشكل جميع تدفقات ومعاملات التشوير.

الشكل 4.III – التأكد من هوية مستعمل الانتهائية

وفيما يلي ملخص لتدفق ومعاملات النداء:

1) يقوم مستعمل الخدمة ETS باستهلال دورة اتصالات ETS (مثل نداء صوتي في الخدمة ETS). تقام دورة الاتصالات ETS باتباع الإجراءات الاعتيادية.

2) يقوم مستعمل الخدمة ETS باستهلال خدمة هوية قائمة على الويب (عن طريق بوابة الويب لمورّد الخدمة A، مورد الخدمة ETS الداخلي، مثلاً) للتحقق من المستعمل الموجود في طرف انتهائية دورة الاتصالات ETS المقامة.

3) يتحقق مورد الخدمة A من تخويل المستعمل للخدمة.

4) يطلب مستعمل الخدمة ETS التحقق من هوية المستعمل الموجود على طرف انتهائية دورة الاتصالات المقامة.

5) يقوم مورّد الخدمة A بمعالجة الطلب وتحديد مورد خدمة الهوية المرتبط بمستعمل الانتهائية (أي مورّد الخدمة ETS الخارجي).

6) يرسل مورّد الخدمة A طلباً إلى مورد الخدمة B للتأكد من هوية مستعمل الانتهائية.

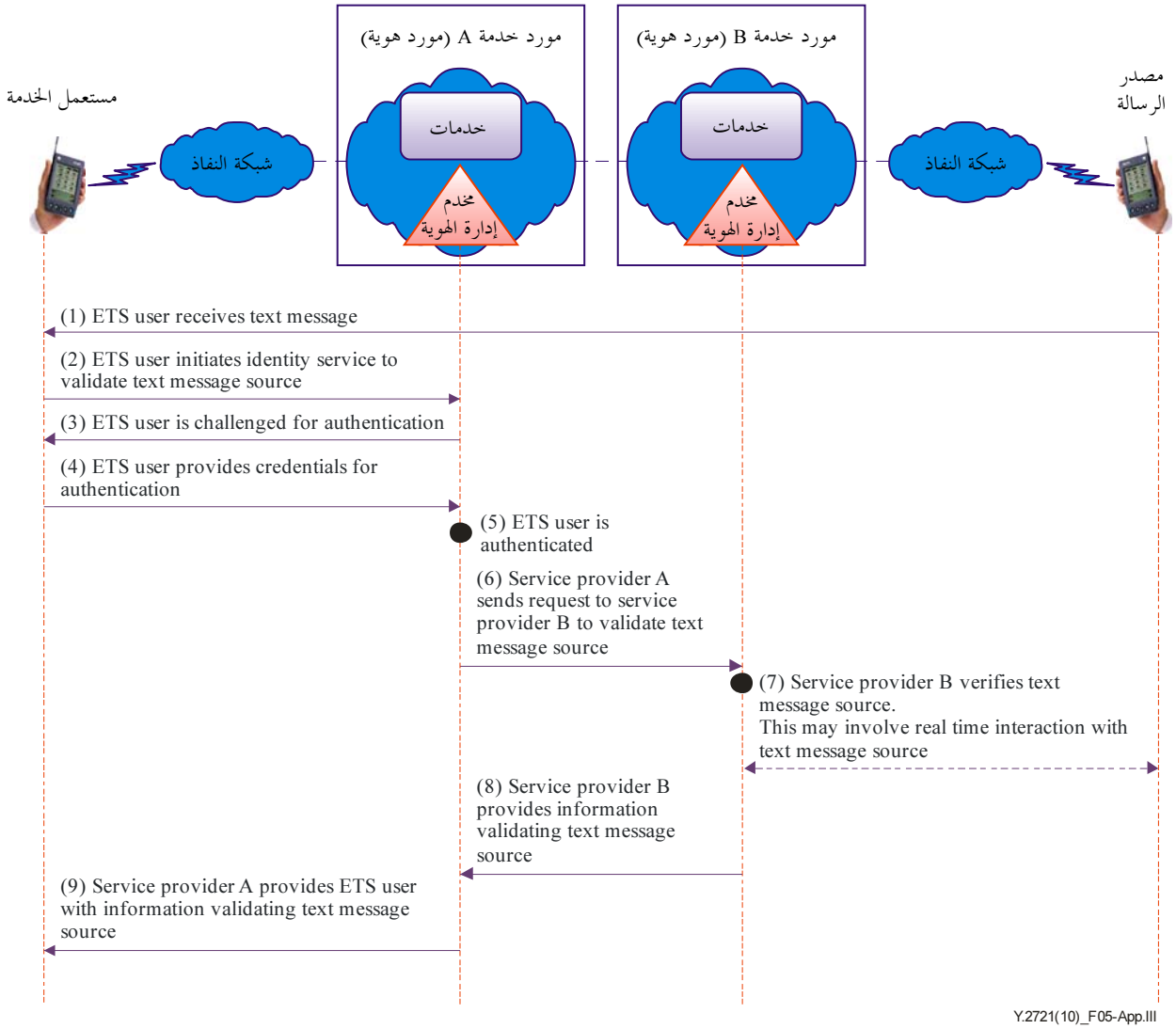
7) يتحقق مورد الخدمة B من هوية مستعمل الانتهائية. قد يشمل ذلك استيقان مستعمل الانتهائية في الوقت الفعلي.

8) يرسل مورد الخدمة B رداً يؤكد فيه هوية مستعمل الانتهائية.

9) يرسل مورد الخدمة A رداً إلى مستعمل الخدمة ETS (مثل شاشة ويب مرئية) يؤكد فيه هوية مستعمل الانتهائية في دورة الاتصالات ETS يؤكد فيه هوية مستعمل الانتهائية في دورة الاتصالات ETS.

ويعتمد مستعملو الخدمة ETS أيضاً وبشكل متزايد على استعمال خدمات البيانات مثل رسائل البريد الإلكتروني والمراسلة اللحظية والمراسلة النصية. وفي بعض الحالات، قد يتعيّن استيقان أو التحقق من مصادر خدمات البيانات هذه. ونظراً لغزارة الرسائل الإلكترونية التافهة والاقتحامية، فإن القدرة على تمييز الرسائل المستيقنة والتحقق منها أثناء بعض الحوادث المتعلقة بالكوارث يكون أمراً بالغ الأهمية بالنسبة لخدمة اتصالات الطوارئ.

ويوضح الشكل 5.III مثالاً لحالة استعمال يجري فيها التأكد من مصدر رسالة نصية. ويُفترض في هذا المثال أن مستعمل الخدمة ETS يتلقى رسالة نصية منشؤها مصدر قد يكون أو لا يكون مستعملاً ثانياً للخدمة ETS. وللحصول على ضمان بشأن مصدر الرسالة النصية، تستعمل خدمات الهوية الخاصة بمورد الخدمة. وقد تكون خدمة الهوية المستعملة في التأكد من مصدر الرسالة النصية أو لا تكون جزءاً من خدمة الرسائل النصية ذاتها.



ملاحظـــة – لأغراض التبسيط، لا تظهر في الشكل جميع تدفقات ومعاملات التشوير.

الشكل 5.III – التأكد من مصدر رسالة نصية

وفيما يلي ملخص للمعاملات:

1) يستقبل مستعمل الخدمة ETS رسالة نصية.

2) يرغب مستعمل الخدمة ETS في التحقق من استيقان مصدر الرسالة النصية ويبدأ في خدمات الهوية من مورّد الخدمة A.

3) يطلب من مستعمل الخدمة ETS معلومات من أجل الاستيقان.

4) يقدم مستعمل الخدمة ETS إثباتات من أجل الاستيقان.

5) يستيقن مورّد الخدمة A من مستعمل الخدمة ETS ويتحقق من تخويله لخدمة الهوية.

6) يرسل مورّد الخدمة A طلباً إلى مورّد الخدمة B للتأكد من مصدر الرسالة النصية.

7) يقوم مورّد الخدمة B بمعالجة الطلبات والتحقق من مصدر الرسالة النصية. قد يتضمن ذلك إجراء معاملة مع مصدر الرسالة النصية.

8) يرسل مورّد الخدمة B رداً إلى مورد الخدمة A يؤكد فيه هوية مصدر الرسالة النصية.

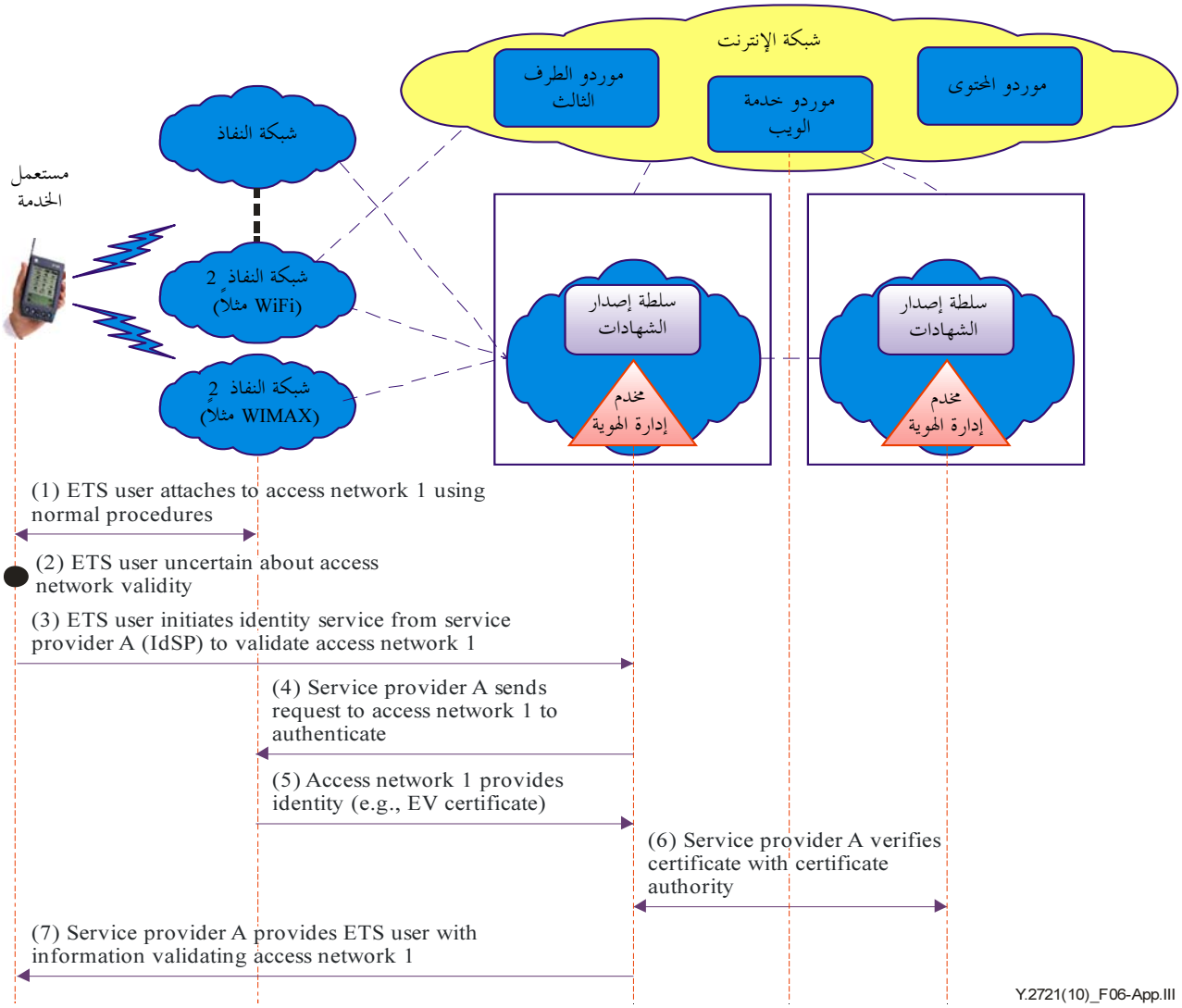
9) يرسل مورّد الخدمة A إلى مستعمل الخدمة ETS معلومات التحقق من مصدر الرسالة النصية.

5.III التعريف والاستيقان الموثوقان لمورّدي الخدمات في بيئة يتعدد فيها المورّدون

تطوّرت بنية الاتصالات حالياً إلى بيئة تضم مورّدين متعددين لنفاذ ثابت ومتنقل باستخدام تكنولوجيات مختلفة (مثل xDSL والكبلات FTTX وWiFi وFTTX وWiMAX وEV-Do وLTE) ومورّدي خدمات اتصالات باستعمال "الشبكات الأساسية المُدارة القائمة على بروتوكول الإنترنت" وموردي خدمات الويب ومورّدي المحتوى وموردي الطرف الثالث. وفي بيئة المورّدين المتعددين هذه، لا يمكن الوثوق المُطلق في هوية مورّد الخدمة كما هو الحال في بيئة الشبكات PSTN المغلقة.

ففي بيئة المورّدين المتعددين المفتوحة، يوجد نقص في إمكانات توفير تعرّف موثوق للهوية واستيقان وتخويل لمورّدي الخدمات وهو ما قد يؤدي إلى إمكانية تنكر كيانات غير شرعية أو التزييف أو التمثيل الكاذب لمورّدين شرعيين. وبالتالي، فإن إمكانات إدارة الهوية الخاصة بتعريف مورّدي الخدمات والتحقق من هوياتهم تُعد من العوامل الهامة لحماية البنية التحتية. وعندما يدعم مورّدو الخدمات خدمات ETS، فإن هذه الإمكانات تعتبر على قدر كبير من الأهمية للأمن القومي.

ويعرض الشكل 6.III مثالاً لحالة استعمال للخدمة ETS يحاول فيها مستعمل الخدمة ETS الحصول على نفاذ شبكي في بيئة مورّدين متعدّدين. ويقوم مستعمل الخدمة ETS تحديداً بالتداول وبإمكان جهاز اليد المتنقل التوصيل بمجموعة من مورّدي شبكات النفاذ الذين يقدمون الخدمات في هذا المجال (قد لا يكون جميع مورّدي الخدمات مورّدين مخوّلين للخدمة ETS). وفي هذا المثال، يُفترض أن مستعمل الخدمة ETS منضم إلى شبكة النفاذ رقم 1 كاختيار أول. وبعد الانضمام إلى شبكة النفاذ 1، سيرغب مستعمل الخدمة ETS في التحقق من الشبكة قبل إجراء أي اتصالات ETS حساسة. وهناك خيارات وتغيرات متعددة للتحقق من مورّد شبكة النفاذ، منها الاستيقان المباشر من جانب مستعمل الخدمة ETS. ويفترض هذا المثال أن مستعمل الخدمة ETS يستعمل خدمات الهوية الخاصة بمورّد الخدمة A للخدمة ETS للتحقق من شبكة النفاذ. وفي هذا المثال، يثق مستعمل الخدمة ETS في مورّد الخدمة A وسيقبل بمعلومات التحقق المرسلة من مورّد الخدمة A بشأن شبكة النفاذ 1.



ملاحظـــة – لأغراض التبسيط، لا تظهر في الشكل جميع تدفقات ومعاملات التشوير.

الشكل 6.III – التحقق من مورّد خدمة النفاذ

وفيما يلي ملخص للمعاملات:

1) يقوم مستعمل الخدمة ETS بالتجوال بواسطة جهاز يد متنقل بإمكانه الانضمام إلى أنماط متعددة من شبكات النفاذ (مثل WiFi أو WiMAX أو LTE أو EV-DO). ويوصل جهاز اليد المتنقل لمستعمل الخدمة ETS بالشبكة 1 (أي، الاختيار الأول استناداً إلى عوامل مثل مورّد معروف للخدمة ETS وقوّة الإشارة).

2) سيرغب مستعمل الخدمة ETS في التحقق من الشبكة 1 قبل التخويل بالخدمات.

3) يقوم مستعمل الخدمة ETS باستهلال خدمات الهوية من مورّد الخدمة A للخدمة ETS للتحقق من شبكة النفاذ 1.

4) يرسل مورد الخدمة A طلبات استيقان إلى شبكة النفاذ 1.

5) تقدم شبكة النفاذ 1 معلومات الهوية من أجل الاستيقان (مثل شهادة التحقق الممتد حسب التوصية ITU-T X.509).

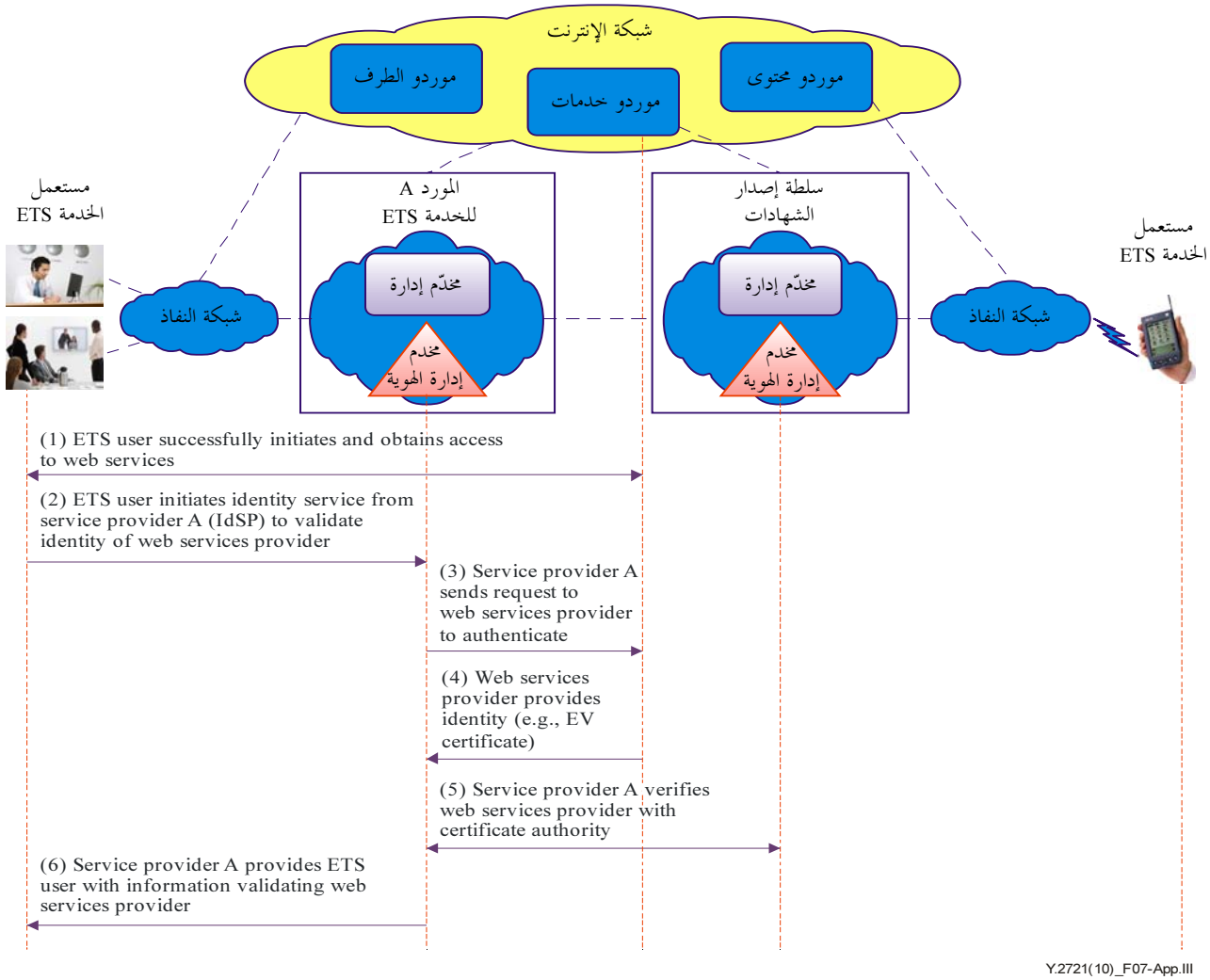
6) يتحقق مورّد الخدمة A من شهادة الشبكة 1 من سلطة إصدار الشهادات.

7) يزوّد مورّد الخدمة A مستعمل الخدمة ETS بمعلومات التحقق من شبكة النفاذ 1.

ويتيح ذلك لمستعمل الخدمة ETS بالاستمرار مع الثقة بأن جهاز اليد المتنقل الخاص به موصّل بشبكة نفاذ مخوّلة.

وبعد الحصول على النفاذ الشبكي، يمكن لمستعمل الخدمة ETS استعمال خدمات العديد من مورّدي الخدمات في بنية تحتية تضم مورّدين متعددين. فمثلاً قد يحتاج مستعمل الخدمة ETS إلى استعمال خدمات مورّدي خدمات الويب (مثل مورّدي معلومات الأرض وغيرها من الخرائط/البيانات) أو خدمات مورّدي المحتوى (مثل موردي الخدمات الذين يقدمون البث المتقاطر في الوقت الفعلي لكاميرا للمراقبة أو تقارير الطقس أو الفيديو). ويمكن لمستعمل الخدمة ETS النفاذ إلى خدمات مورّدي خدمات الويب ومورّدي المحتوى مباشرة عبر النفاذ من خلال شبكة الإنترنت أو بطريقة غير مباشرة من خلال خدمات مورّدي شبكات الجيل التالي. وفي هذه الحالات، قد يتعيّن على مستعمل الخدمة ETS التحقق من مورّد خدمة محددة.

ويوضح الشكل 7.III مثالاً لحالة استعمال يتعيّن فيها على مستعمل الخدمة ETS التحقق من هوية مورّد خدمات ويب. وعلى غرار حالة الاستعمال أعلاه، هناك خيارات وتغايرات كثيرة للتحقق من مورّد خدمات الويب، منها الاستيقان المباشر من جانب مستعمل الخدمة ETS. ويفترض هذا المثال أن مستعمل الخدمة ETS يستعمل خدمات الهوية الخاصة بمورّد الخدمة A للخدمة ETS للتحقق من مورد خدمات الويب. وعلى غرار المثال أعلاه، يثق مستعمل الخدمة ETS في مورّد الخدمة A ويستقبل بمعلومات التحقق المرسلة منه بشأن مورّد خدمات الويب.



ملاحظـــة – لأغراض التبسيط، لا تظهر في الشكل جميع تدفقات ومعاملات التشوير.

الشكل 7.III – التحقق من مورّد خدمات ويب أو مورد محتوى

وفيما يلي ملخص للمعاملات:

1) ينجح مستعمل الخدمة ETS في استهلال والنفاذ إلى خدمات الويب. بَيد أن مستعمل الخدمة ETS يرغب في التحقق من مورّد الخدمة للوثوق في البيانات.

2) يقوم مستعمل الخدمة ETS باستهلال خدمة هوية خاصة بالمورّد A للخدمة ETS للتحقق من مورّد خدمة الويب.

3) يرسل مورّد A للخدمة ETS طلبات إلى مورّد خدمات الويب للاستيقان.

4) يقدم مورّد خدمات الويب معلومات من أجل الاستيقان (مثل الشهادة EV[1]).

5) يتحقق المورّد A للخدمة ETS من المعلومات من سلطة إصدار الشهادات.

6) يزوّد المورد A للخدمة ETS مستعمل الخدمة ETS بمعلومات التحقق من هوية مورّد خدمات الويب.

ومن شأن التحقق من مورّد خدمات الويب أن يوفر لمستعمل الخدمة ETS الثقة في هوية خدمات الويب، وهو ما يقوي من ثقته في المعلومات المتحصّل عليها من خدمات الويب.

6.III تسجيل دخول وخروج وحيد

يتعيّن على المستعملين عادة التسجيل للدخول إلى أنظمة متعددة تحوي خدمات تطبيقات (مثل تبادل الصوت عبر بروتوكول الإنترنت والبيانات والفيديو) يستوجب وجود رقم مكافئ لحوارات تسجيل الدخول يتضمن كل حوار منها أسماء مختلف المستعملين ومعلومات الاستيقان الخاصة بهم. ويُواجه مديرو الأنظمة بحسابات إدارة المستعملين داخل كل نظام من هذه الأنظمة المتعددة بشكل منسق من أجل إنفاذ السياسات الأمنية.

وقد يتعيّن على مستعملي الخدمة ETS تحسين بعض إمكانات إدارة الهوية مثل "تسجيل دخول/خروج وحيد". ويتمثل الأساس المنطقي لتسجيل الدخول الوحيد في أنه يمكن لأي مستعمل نهائي أو جهاز أو توليفة من مستعمل نهائي وجهاز التسجيل للدخول مرة واحدة (أي، تقديم إثباتات للاستيقان والتخويل) إلى خدمة ما ومن ثم يتم استيقانه لخدمة إضافية أخرى أو أكثر في نفس ميدان شبكة الجيل التالي، أو في حالة الخدمات الاتحادية، عبر ميادين شبكات NGN متعددة. وتعود قيمة تسجيل الدخول الوحيد إلى أن المستعمل النهائي لا يتم تحميله بأعباء الاستيقان بالنسبة لكل خدمة. ومصطلح "تسجيل الدخول" كما هو مستخدم هنا يعني نفس المعنى لمصطلح "التسجيل مع" أو "الدخول" أو "التسجيل" حيث يقوم المستعمل النهائي أو الجهاز بالتسجيل مع أو "الدخول" أو "التسجيل" في الخدمة. وينطبق الأمر نفسه على "تسجيل الخروج الوحيد" الذي يوفر "خروج" شامل من خدمات تطبيقات متعددة في دورة معينة.

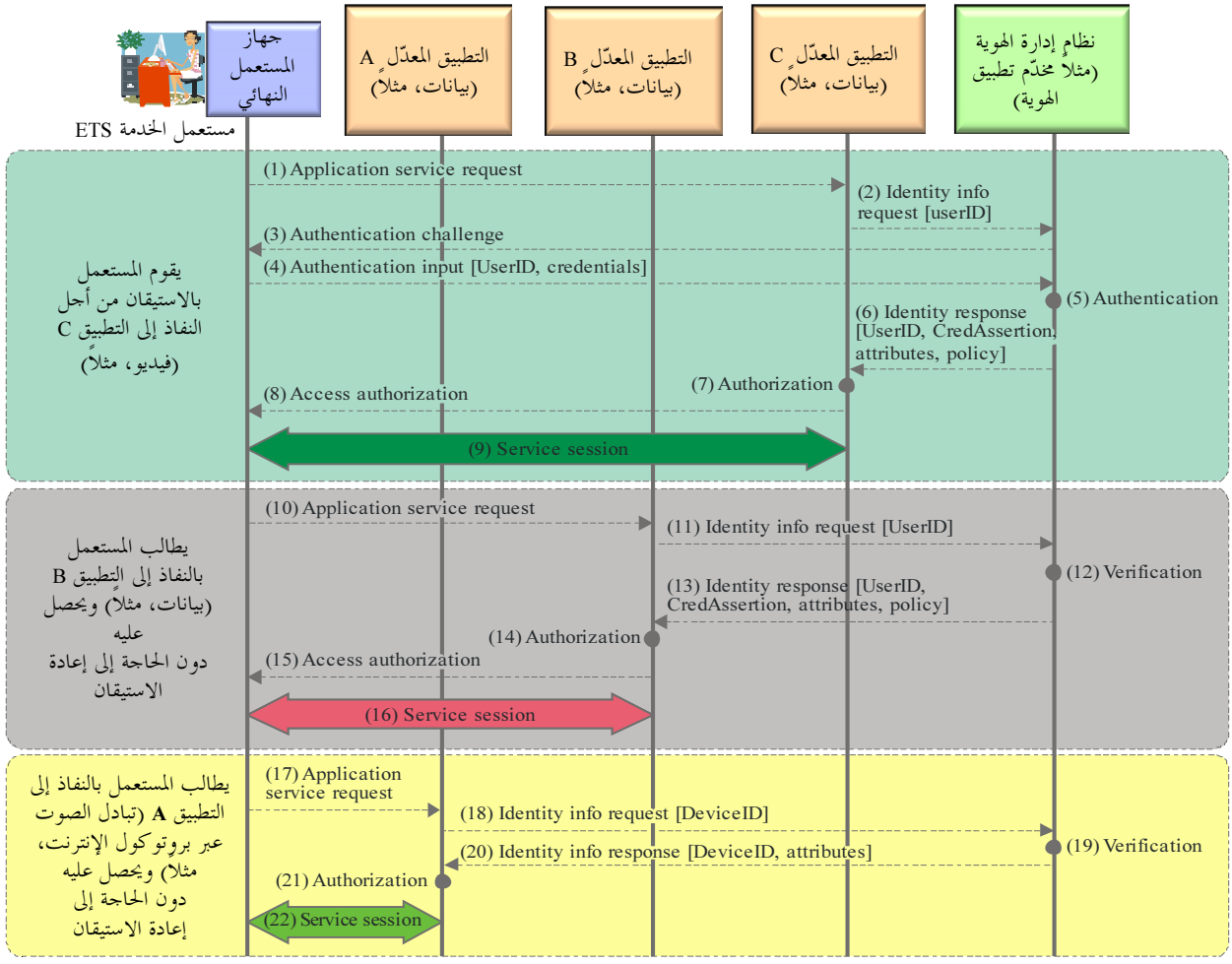
ومن بين الفوائد المحتملة لإمكانات تسجيل الدخول/الخروج الوحيد:

- تقليل الزمن الذي يستغرقه المستعملون في عمليات التسجيل لدخول ميادين إفرادية، بما في ذلك تقليل عدد حالات فشل التسجيل. كما يطرأ تحسّن على الأمن من خلال تقلّص الحاجة إلى أن يقوم المستعمل بتداول وتذكر مجموعات متعددة من معلومات الاستيقان.
- تقليل الزمن الذي يستغرقه مديرو الأنظمة في إضافة وحذف مستعملين إلى النظام أو تعديد حقوق النفاذ الخاصة بهم.
- تحسين الأمن من خلال قدرة أكبر لمديري الأنظمة على الحفاظ على سلامة تشكيلات حسابات المستعملين، بما في ذلك القدرة على منع أو حذف نفاذ مستعمل فردي إلى جميع موارد النظام بشكل منسّق ومتّسق.

[1] شهادة التحقق الممتدة هي نمط خاص من شهادة التوصية X.509 تحتاج إلى تحرّي الكيان الطالب بدقة من جانب سلطة إصدار الشهادات قبل إصدارها.

ويوضح الشكل III.8 مثالاً لحالة استعمال تشمل استعمال نظام إدارة هوية لدعم "تسجيل دخول/خروج وحيد" لخدمات تطبيقات متعددة (مثل تبادل الصوت القائم على بروتوكول الإنترنت والبيانات والفيديو) داخل ميدان مورد شبكات NGN. وتشمل حالة الاستعمال معاملات بين الكيانات التالية:

- مستعملون نهائيون (أي مستعملون نهائيون و/أو أجهزة مستعملين نهائيين).
- نظام معول (أي خدمة تطبيق أو نظام شبكي).
- نظام إدارة الهوية (أي نظام شبكي يقدم خدمات إدارة الهوية مثل التسجيل والاستيقان والتخويل ومعلومات المظهر الجانبي للاشتراك).



ملاحظـــة – لأغراض التبسيط، لا تظهر في الشكل جميع تدفقات ومعاملات التشوير.

الشكل III.8 – تسجيل دخول وحيد

يفترض هذا المثال أن جهاز المستعمل النهائي يسجل في الشبكة NGN وينضم إليها باتباع الإجراءات الاعتيادية.

وفيما يلي تدفقات النداء:

1) طلب خدمة تطبيق. تدفق هذه المعلومة يمثل طلب المستعمل النهائي للخدمة ETS الحصول على خدمة التطبيق C (فيديو).

2) طلب معلومات هوية [معرّف هوية المستعمل]. ترسل خدمة التطبيق C (الفيديو) طلباً إلى نظام إدارة الهوية للتأكد من هوية المستعمل وتقدم نعوتاً مرتبطة بمعرّف هوية المستعمل. وقد يشمل ذلك معلومات مثل المظهر الجانبي للخدمة، والامتيازات والأفضليات ومعلومات خاصة بالسياسة العامة. فعلى سبيل المثال، قد يشمل ذلك أيّ سياسات أو قيود مرتبطة بالهوية.

3) طلب الاستيقان. يطلب نظام إدارة الهوية معلومات من المستعمل من أجل الاستيقان.

4) مدخلات الاستيقان [إثباتات]. يقدم المستعمل معلومات من أجل الاستيقان (مثل معرّف هوية المستعمل وكلمة السر أو رقم التعريف الشخصي).

5) الاستيقان. يقوم نظام إدارة الهوية بالاستيقان والحصول على المعلومات الأخرى المطلوبة. قد تتضمن هذه المعلومات تلمّس معلومات من أنظمة شبكية أخرى (مثل مخدّم المشتري المنزلي (HSS) أو قاعدة بيانات أخرى للاشتراك).

6) الرد بشأن الهوية [ضمانات الإثباتات والنعوت والسياسات]. يقدم نظام إدارة الهوية معلومات تؤكد صحة الإثباتات. ومن بين المعلومات الأخرى المتضمّنة النعوت المرتبطة بمعرّف هوية المستعمل (مثل الامتيازات والأفضليات) والسياسات المرتبطة بمعلومات الهوية (مثل أي قيود تتعلق بالاستعمال والعرض والنشر).

7) التخويل. تقوم خدمة التطبيق C (الفيديو) بمعالجة المعلومات وتحدد أن المستعمل مخوّل للخدمة.

8) تخويل النفاذ. تقدم الخدمة الخاصة بالتطبيق C (الفيديو) إلى المستعمل ما يفيد منحه النفاذ إلى الخدمة.

9) دورة الخدمة. تقام دورة ناجحة للمستعمل مع خدمة التطبيق C (الفيديو).

10) طلب خدمة تطبيق. يطلب المستعمل الحصول على خدمة التطبيق B (بيانات).

11) طلب معلومات هوية [معرّف هوية المستعمل]. ترسل خدمة التطبيق B (بيانات) طلباً إلى نظام إدارة الهوية للتأكد من هوية المستعمل وتقدم نعوتاً مرتبطة بمعرّف هوية المستعمل. وقد يشمل ذلك معلومات مثل المظهر الجانبي للخدمة، والامتيازات والأفضليات ومعلومات خاصة بالسياسة العامة. فعلى سبيل المثال، قد يشمل ذلك أيّ سياسات أو قيود مرتبطة بالهوية.

12) التحقق. يقوم نظام إدارة الهوية بمعالجة الطلب ويحدد أن تسجيل الدخول الوحيد سار، ويتحقق كذلك من أن استيقان المستعمِل لا يزال سارياً.

13) الرد بشأن الهوية [ضمانات الإثباتات والنعوت والسياسات]. يقدم نظام إدارة الهوية معلومات تؤكد صحة الإثباتات. ومن بين المعلومات الأخرى المتضمّنة النعوت المرتبطة بمعرّف هوية المستعمل (مثل الامتيازات والأفضليات) والسياسات المرتبطة بمعلومات الهوية (مثل أي قيود تتعلق بالاستعمال والعرض والنشر).

14) التخويل. تقوم خدمة التطبيق B (البيانات) بمعالجة المعلومات وتحدد أن المستعمل مخوّل للخدمة.

15) تخويل النفاذ. تقدم خدمة التطبيق B (البيانات) إلى المستعمل ما يفيد منحه النفاذ إلى الخدمة.

16) دورة الخدمة. تُستهل بنجاح دورة للمستعمل مع خدمة التطبيق B (البيانات).

17) طلب خدمة تطبيق. يطلب المستعمل الحصول على خدمة التطبيق A (تبادل الصوت عبر بروتوكول الإنترنت).

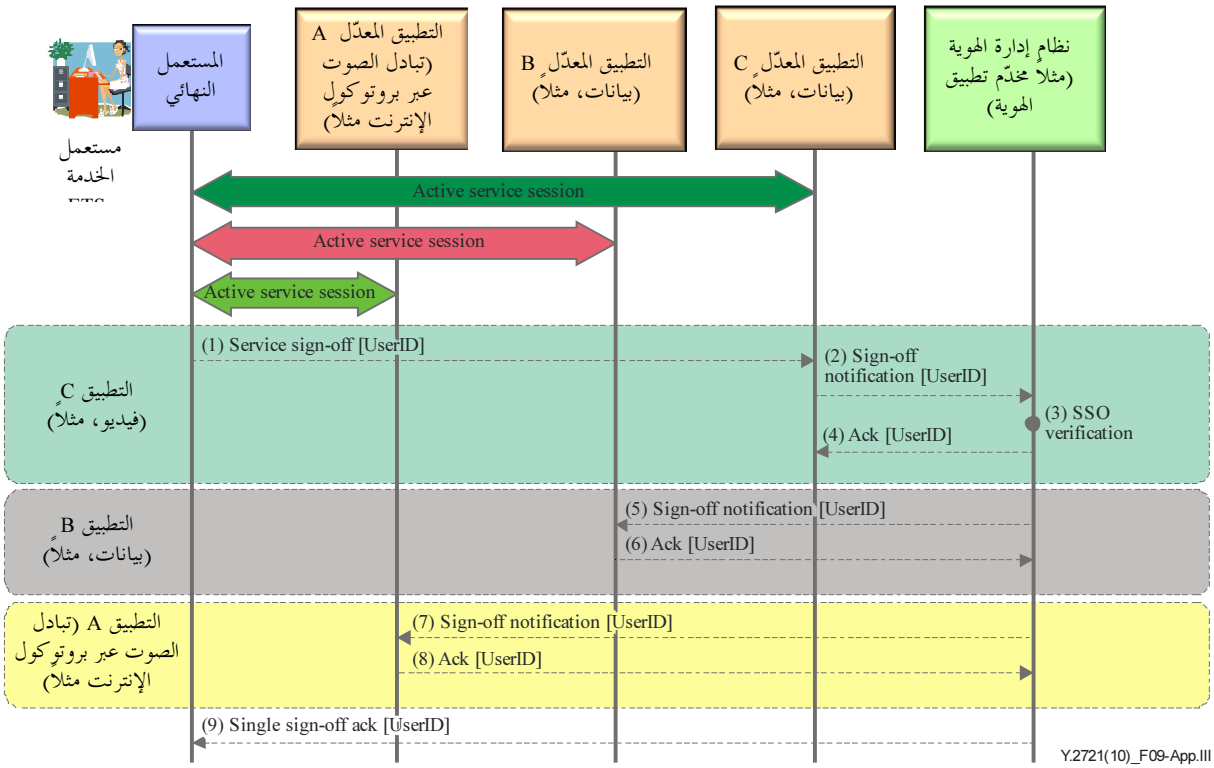
18) طلب معلومات الهوية [معرّف هوية الجهاز]. ترسل خدمة التطبيق A (تبادل الصوت عبر بروتوكول الإنترنت) طلباً إلى نظام إدارة الهوية للتأكد من هوية المستعمل وتقدم نعوتاً مرتبطة بمعرّف هوية الجهاز.

19) التحقق. يقوم نظام إدارة الهوية بمعالجة الطلب ويحدد أن تسجيل الدخول الوحيد سار ويتحقق كذلك من أن استيقان المستعمل لا يزال سارياً.

20) الرد بشأن الهوية [ضمانات الإثباتات والنعوت والسياسات]. يقدم نظام إدارة الهوية معلومات تؤكد صحة الإثباتات. ومن بين المعلومات الأخرى المتضمّنة النعوت المرتبطة بمعرّف هوية المستعمل (مثل الامتيازات والأفضليات) والسياسات المرتبطة بمعلومات الهوية (مثل أي قيود تتعلق بالاستعمال والعرض والنشر).

21) التخويل. تقوم خدمة التطبيق A (تبادل الصوت عبر بروتوكول الإنترنت) بمعالجة المعلومات وتحدد أن المستعمل مخوّل للخدمة.

22) دورة خدمة التطبيق. يقيم المستعمل دورة مع خدمة التطبيق A (تبادل الصوت عبر بروتوكول الإنترنت).



ملاحظـــة – لأغراض التبسيط، لا تظهر في الشكل جميع تدفقات ومعاملات التشوير.

الشكل 9.III – تسجيل خروج وحيد

يوضح الشكل 9.III خدمة "تسجيل خروج وحيد" تتيح للمستعمِل الخروج أوتوماتياً من خدمات تطبيقات متعددة (نقل الصوت عبر بروتوكول الإنترنت وبيانات وفيديو) دون الحاجة إلى تسجيل الخروج من كل خدمة تطبيق في الدورة. وتفترض حالة الاستعمال هذه أن المستعمل ضالع في دورة خدمة بخدمات التطبيقات النشطة A (نقل الصوت عبر بروتوكول الإنترنت) وB (بيانات) وC (فيديو).

وفيما يلي تدفقات النداء:

1) تسجيل الخروج من الخدمة [معرّف هوية المستعمِل]. يرسل مستعمل الخدمة ETS طلباً لإنهاء دورة الخدمة.

2) تبليغ تسجيل الخروج [معرّف هوية المستعمِل]. تقوم خدمة التطبيق C (الفيديو) بتبليغ نظام إدارة الهوية بطلب المستعمِل التسجيل للخروج.

3) التحقق من تسجيل الخروج الوحيد. يحدد نظام إدارة الهوية أن تسجيل الخروج الوحيد سار، ويتحقق من خدمات التطبيقات النشطة.

4) الإشعار [معرّف هوية المستعمِل]. يرسل نظام إدارة الهوية إشعاراً إلى خدمة التطبيق C (الفيديو) بإنهاء دورة الخدمة.

5) تبليغ تسجيل الخروج [معرّف هوية المستعمِل}. يقوم نظام إدارة الهوية بتبليغ خدمة التطبيق B (البيانات) بتسجيل الخروج.

6) الإشعار [معرّف هوية المستعمِل]. ترسل خدمة التطبيق B (البيانات) إشعاراً باستلام تسجيل الخروج.

7) تبليغ تسجيل الخروج [معرّف هوية المستعمل]. يقوم نظام إدارة الهوية بتبليغ خدمة التطبيق A (تبادل الصوت عبر بروتوكول الإنترنت) بتسجيل الخروج.

8) الإشعار [معرّف هوية المستعمل]. تقوم خدمة التطبيق A (تبادل الصوت عبر بروتوكول الإنترنت) بإرسال إشعار باستلام تسجيل الخروج.

9) الإشعار بتسجيل خروج وحيد [معرّف هوية المستعمِل]. يرسل نظام إدارة الهوية إشعارا إلى المستعمل يؤكد فيه الخروج من جميع خدمات التطبيقات النشطة في الدورة.

التذييل IV

حالات الاستعمال ذات الصلة بالخدمة المتنقلة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.IV مقدمة

يقدم هذا التذييل أمثلة عن حالات استعمال إدارة الهوية ذات الصلة بالخدمة المتنقلة. وتستند هذه الأمثلة إلى حالات الاستعمال التي يرد وصفها في الورقة البيضاء لتجمع الجيل الثالث في الأمريكتين، بعنوان: *إدارة الهوية: نظرة عامة على المعايير والتكنولوجيات للإنترنت المتنقل والثابت* [b-3G Americas White Paper].

2.IV أمثلة حالات الاستعمال

1.2.IV ينفُذ مستعمل الخدمة المتنقلة بجهاز من الجيل الثالث مفعّل ببطاقة دارة إلكترونية شاملة (UICC) إلى بوابة مشغّل شبكة الخدمة المتنقلة (مخزن الويب) لشراء نغمة رنين.

الجهات الفاعلة:

- مستعمل الخدمة المتنقلة.
- مشغّل شبكة الخدمة المتنقلة (MNO).
- مقدم الخدمة (SP) هو مشغّل شبكة الخدمة المتنقلة.

الفوائد للمستعمل:

- الاستفادة من التسجيل الواحد للدخول مع النفاذ إلى مختلف خدمات مشغّل شبكة الخدمة المتنقلة.

القيود الرئيسية:

- يقع مقدم الخدمة ومشغّل شبكة الخدمة المتنقلة في دائرة الثقة نفسها (وفقاً لأحكام تحالف الحرية (Liberty Alliance)).

2.2.IV ينفُذ مستعمل الخدمة المتنقلة بجهاز من الجيل الثالث مفعّل ببطاقة دارة إلكترونية شاملة (UICC) إلى مخزن الويب في بوابة مشغّل شبكة الخدمة المتنقلة؛ ويتصفح كتالوج البضائع الرقمية في البوابة، ويرى مادة ترويجية خاصة (مثل لعبة فيديو تنحصر حقوق توزيعها في مشغّل الشبكة) ويبادر إلى الشراء، ثم يتفق على إدراج الثمن في فاتورة هاتفه المتنقل؛ فيستطيع المستعمل تحميل لعبة الفيديو من وصلة آمنة يعاد توجيهها من مشغّل شبكة الخدمة المتنقلة على مورّد المحتوى.

الجهات الفاعلة:

- مستعمل الخدمة المتنقلة.
- مشغّل شبكة الخدمة المتنقلة (MNO).
- مقدم الخدمة a (SP-a) هو مشغّل شبكة الخدمة المتنقلة؛ ومقدم الخدمة b (SP-b) هو مورّد محتوى خارجي (مثل لعبة فيديو).

الفوائد للمستعمل:

- الاستفادة من التسجيل الواحد للدخول إلى بوابة مشغّل شبكة الخدمة المتنقلة والبائع الخارجي.
- القدرة على استعمال مستنداته من مشغّل شبكة الخدمة المتنقلة الخاص به لإتمام الصفقة مع مورّد المحتوى الخارجي.

القيود الرئيسية:

- يقع مقدم الخدمة a (SP-a) لدى مشغّل شبكة الخدمة المتنقلة ومقدم الخدمة b (SP-b) لدى مورّد المحتوى في دائرة الثقة نفسها.

3.2.IV يستخدم مستعمل الخدمة المتنقلة هاتفاً ذكياً من الجيل الثالث مفعّلاً ببطاقة دارة إلكترونية شاملة (UICC) ويتجول في بلد آخر؛ وأثناء تصفحه لشبكة الإنترنت، يوقّع اشتراكاً مقابل بدل نقدي في مجلة سيارات أجنبية ويحمّل ثمن الاشتراك على بطاقته الائتمانية (فيُفصَح انتقائياً عن نعوت من بياناته العامة كمستعمل المحفوظة لدى مشغّل شبكة الخدمة المتنقلة (MNO) لاستكمال عملية طلب الاشتراك في المجلة)؛ فتخوّل شركة بطاقة الائتمان الدفع إلى بوابة مجلة السيارات نيابةً عن مستعمل الخدمة المتنقلة.

الجهات الفاعلة:

- مستعمل الخدمة المتنقلة.
- مشغّل شبكة الخدمة المتنقلة (MNO).
- مقدم الخدمة a (SP-a) هو مورّد المحتوى (مجلة السيارات)؛ ومقدم الخدمة b (SP-b) هو شركة بطاقة الائتمان.

الفوائد للمستعمل:

- الاستفادة من التسجيل الواحد للدخول لدى مشغّل شبكة الخدمة المتنقلة الخاص به وشركة بطاقة الائتمان.
- القدرة على استعمال مستنداته من مشغّل شبكة الخدمة المتنقلة الخاص به للتخويل بالدفع من شركة بطاقة الائتمان الخاصة به لإتمام الصفقة مع مورّد المحتوى الخارجي.
- القدرة على إعادة استخدام نعوته الشخصية من بياناته العامة كمشترك لدى مشغّل شبكة الخدمة المتنقلة لإتمام الاشتراك في خدمة خارجية مما يقلل إلى أدنى حد إعادة إدخال الكثير من هذه التفاصيل.

القيود الرئيسية:

- يقع مشغّل شبكة الخدمة المتنقلة ومقدم الخدمة b (SP-b)، وهو شركة بطاقة الائتمان، في دائرة الثقة نفسها.
- لا يقع مقدم الخدمة a (SP-a) وهو مورّد مجلة السيارات، في دائرة الثقة.

4.2.IV يستخدم مستعمل الخدمة المتنقلة حاسوباً محمولاً من الجيل الثالث مفعّلاً ببطاقة دارة إلكترونية شاملة (UICC) ويتجول في بلد آخر وينتظر في مطار؛ فيوقّع مسجلاً للحصول على خدمة الأمانة اللاسلكية (WiFi) لبضع ساعات؛ وبما أن مشغّل الشبكة المحلية اللاسلكية (WLAN) يقيم تحالفاً مع مشغّل شبكة الخدمة المتنقلة (MNO)، فيمكنه قبول إدراج رسوم استخدام المستعمل لخدمة WiFi في فاتورة الهاتف المتنقل للمستعمل؛ وكذلك فإن مستعمل الخدمة المتنقلة الذي يستخدم خدمة WiFi ينفُذ إلى العديد من بوابات الويب التي يتفاعل معها مراراً، ومنها بوابة مصرف ووكالة سفر وشركة استثمارات مالية؛ ويود المستعمل من أن يتمكن من استعمال الخدمات التي يقدمها تجار الويب هؤلاء دون إعادة تسجيل الدخول، وأن يتمكن كذلك من تبادل المعلومات الشخصية الخاصة بشكل آمن.

الجهات الفاعلة:

- مستعمل الخدمة المتنقلة.

مشغّل الشبكة المحلية اللاسلكية (WLAN)

- مشغّل شبكة الخدمة المتنقلة (MNO).
- مقدم الخدمة a (SP-a) هو مشغّل شبكة الخدمة المتنقلة؛ ومقدم الخدمة b (SP-b) هو المصرف، ومقدم الخدمة c (SP-c) هو وكالة السفر، ومقدم الخدمة d (SP-d) هو شركة الاستثمارات المالية.

الفوائد للمستعمل:

- الاستفادة من التسجيل الواحد للدخول لدى مشغّل شبكة الخدمة المتنقلة الخاص به ومشغّل خدمة WiFi.
- القدرة على استعمال مستنداته من مشغّل شبكة الخدمة المتنقلة الخاص به للتخويل بدفع رسوم خدمة WiFi.
- القدرة على النفاذ إلى العديد من مقدمي الخدمات القائمة على الويب غير المنتسبين لدى مشغّل شبكة الخدمة المتنقلة بإجراءات تسجيل دخول مبسطة وبنقل مأمون للمعلومات الخاصة.

القيود الرئيسية:

- يقع مشغّل شبكة الخدمة المتنقلة ومشغّل الشبكة المحلية اللاسلكية في دائرة الثقة نفسها.
- ولا تضم دائرة الثقة نفسها مقدم الخدمة a (SP-a) المصرف ومقدم الخدمة b (SP-b) وكالة السفر ومقدم الخدمة c (SP-c) شركة الاستثمارات المالية.

5.2.IV يستخدم مستعمل الخدمة المتنقلة حاسوباً محمولاً من الجيل الثالث مفعّلاً ببطاقة دارة إلكترونية شاملة (UICC) أثناء وجوده في منزله ويتصفح الشبكة بواسطة خدمة الخط الرقمي للمشترك (DSL) المنزلية عريضة النطاق والتي يستطيع من خلالها النفاذ إلى بوابة مشغّل شبكة الخدمة المتنقلة الخاص به؛ ويسدد فاتورة حسابه في الخدمة المتنقلة (باستعمال بطاقته الائتمانية، حيث التخويل المسبق في الملف) ويضيف ميزة جديدة إلى اشتراكه في الخدمة المتنقلة؛ وبعدئذ ينفُذ إلى موقع استئجار الأفلام ويحمّل فيلماً يدفع أجرته ببطاقته الائتمانية غير المخوّلة مسبقاً).

الجهات الفاعلة:

- مستعمل الخدمة المتنقلة.
- شركة شبكة الخطوط الرقمية للمشتركين (DSL) في الخدمة الثابتة.
- مشغّل شبكة الخدمة المتنقلة (MNO).
- مقدم الخدمة a (SP-a) هو مشغّل شبكة الخدمة المتنقلة؛ ومقدم الخدمة b (SP-b) هو بوابة تأجير الأفلام، ومقدم الخدمة c (SP-c) هو شركة بطاقة الائتمان.

الفوائد للمستعمل:

- الاستفادة من التسجيل الواحد للدخول لدى مشغّل شبكة الخدمة الثابتة ومشغّل شبكة الخدمة المتنقلة الخاصين به.
- القدرة على استعمال مستنداته من مشغّل شبكة الخدمة الثابتة الخاص به للاستيقان لدى حسابه في الخدمة المتنقلة ولطلب خدمات إضافية من مشغّل شبكة الخدمة المتنقلة (MNO).
- القدرة على تخويل تحميل أثمان شراء المحتوى من مقدم خدمة خارجي (مثل خدمة تأجير أفلام) على حساب بطاقته الائتمانية.

القيود الرئيسية:

- تضم دائرة الثقة نفسها مشغّل شبكة الخدمة المتنقلة وشركة شبكة الخدمة الثابتة ومقدم الخدمة b (SP-b) أي شركة بطاقة الائتمان.
- ولا يقع مقدم الخدمة b (SP-b) أي مورّد تأجير الأفلام في دائرة الثقة نفسها.

6.2.IV مستعمل خدمة متنقلة مزود بجهاز من الجيل الثالث مفعّل ببطاقة دارة إلكترونية شاملة (UICC) يريد النفاذ إلى موارد (مثل خدمة دليل المؤسسة) موجودة في شبكة المؤسسة.

الجهات الفاعلة:

- مستعمل الخدمة المتنقلة.
- مشغّل شبكة الخدمة المتنقلة (MNO).

- نظام إدارة الهوية في المؤسسة.
- مخدّم خدمات دليل المؤسسة (مخدّم EDS).

ويرد أدناه وصف للتفاعلات الرفيعة المستوى بين هذه الجهات الفاعلة.

- يطلب مستعمل الخدمة المتنقلة خدمة من مخدّم خدمات دليل المؤسسة.
- يحصل المستعمل، الذي يستيقن نظامُ مشغّل شبكة الخدمة المتنقلة (MNO) منه، على مستندات الاستيقان من النظام من أجل الاستيقان لدى نظام إدارة الهوية في المؤسسة.
- يقدم المستعمل المستندات إلى نظام إدارة الهوية في المؤسسة، وبعد نجاح الاستيقان، يحصل من النظام على مستندات من أجل الاستيقان لدى مخدّم خدمات دليل المؤسسة (EDS).
- يرد المستعمل على مخدّم خدمات دليل المؤسسة بالمستندات الواردة من نظام إدارة الهوية في المؤسسة.
- يحصل المستعمل المستيقَن منه على الخدمة المطلوبة من مخدّم خدمات دليل المؤسسة.

الفوائد للمستعمل:

- يمكن لمستعمل الخدمة المتنقلة النفاذ إلى المورد المتوفر في شبكة مؤسسته (مثل خدمة دليل المؤسسة) بطريقة فعالة من حيث التكلفة مع الوفاء بالمتطلبات الأمنية الصارمة التي تمليها عادةً بيئات تكنولوجيا المعلومات في المؤسسات.

القيود الرئيسية:

- يمكن لنظام إدارة الهوية في المؤسسة أن يتطلب استيقاناً قائماً على عاملين (مثل هوية المستعمل/كلمة المرور/رقم التعريف الشخصي (PIN)) علاوة على مستندات المستعمل الواردة من مشغّل شبكة الخدمة المتنقلة (MNO).
- يقع نظاما إدارة هوية لدى مشغّل شبكة الخدمة المتنقلة ولدى المؤسسة في دائرة الثقة نفسها.

التذييل V

أمثلة عن نماذج معاملات إدارة الهوية

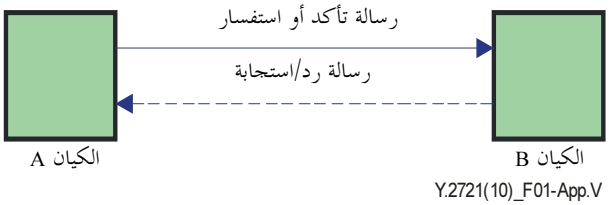
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.V مقدمة

يعرض هذا التذييل أمثلة عن نماذج معاملات إدارة الهوية. وتصف التوصية [b-ITU-T X.1250] النماذج الواردة في هذا التذييل. وهناك نماذج أخرى ممكنة أيضاً غير تلك المدرجة في هذا الملحق.

2.V أمثلة من النماذج الممكنة لمعاملات إدارة الهوية

تتمثل إحدى المعاملات الأولية لإدارة الهوية في عملية الاستفسار–الرد الأساسية الشائعة في معظم تبادل المعلومات المهيكل الموضح في الشكل 1.V. وينطوي أبسط أشكال تبادل الرسائل على طرفين يتفقان على استعمال بروتوكول ونموذج للمعلومات.

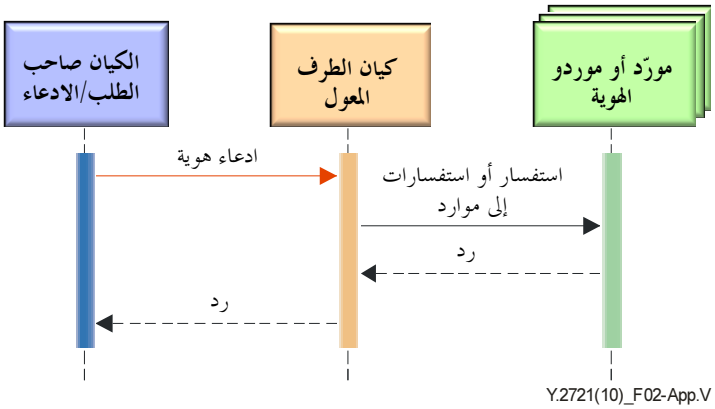


الشكل 1.V – العملية الأساسية لتبادل معلومات الاستفسار/الرد

يمكن للأطراف التي تشارك في هذه العملية أن تكون أي نوع من الكيانات. ويمكن أن يكون الكيان شخصاً طبيعياً أو حيواناً أو شخصاً اعتبارياً أو منظمة، أو شيئاً فاعلاً أو منفعلاً، أو تطبيقاً برمجياً، أو خدمة وما إلى ذلك، أو مجموعة مما تقدم. وفي سياق الاتصالات، تشمل أمثلة الكيانات نقاط نفاذ ومشتركين وعناصر شبكة وشبكات وتطبيقات برمجيات وخدمات وأجهزة وسطوح بينية، وما إلى ذلك. فيمكن أن تكون الكيانات أي غرض مادي أو افتراضي مثل معدات الشبكات والبرمجيات والأجهزة الطرفية وأجهزة الاستشعار والأغراض المادية ذات الوسم الفاعل (مثل التعرف بواسطة الترددات الراديوية (RFID) أو الشفرات البصرية)، أو أغراض ذات وسم منفعل. فتعالج أجهزة الشبكة، على سبيل المثال، على أنها كيانات خاضعة لمتطلبات إدارة هوية خاصة لحساب المستعملين النهائيين والمورّدين والسلطات الحكومية. وفي سياق إدارة الحقوق الرقمية، قد يكون الكيان مادة تحميها حقوق الملكية الفكرية أو حقوق المؤلف كمحتويات الوسائط المتعددة أو تلفزيون بروتوكول الإنترنت (IPTV) مثلاً. وهناك نمط خاص من الكيانات هو الزمرة. وهوية الزمرة هي ملتقى هويات أعضائها (النعوت المشتركة بينهم).

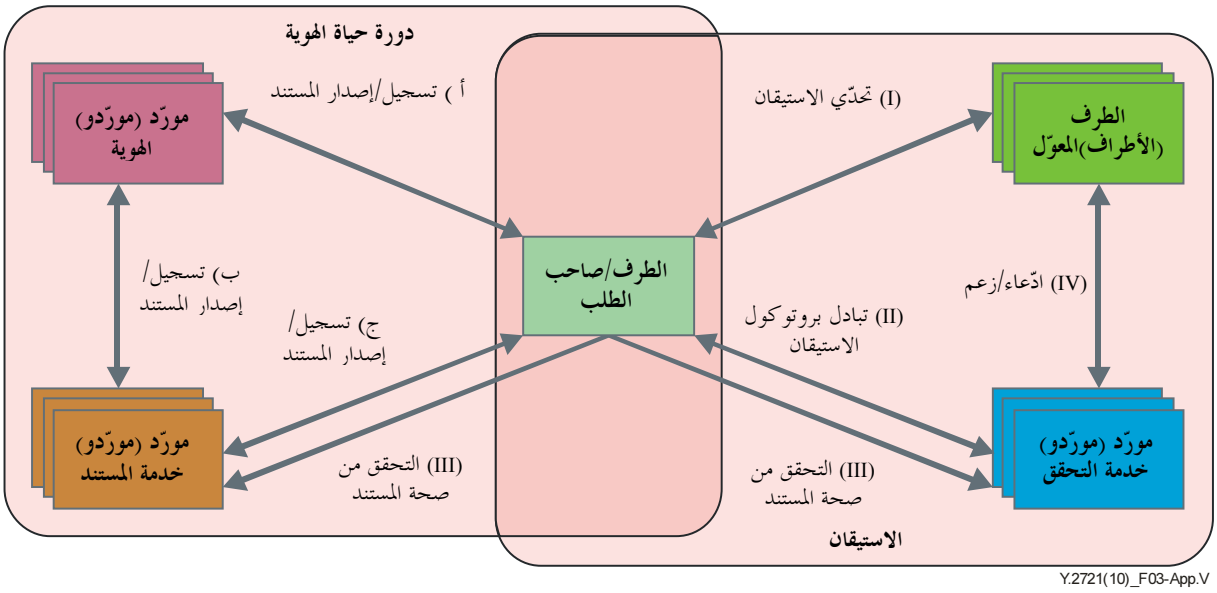
وتستخدم معظم حالات استعمال إدارة الهوية نماذج معقدة. ومثال ذلك، حيث لا يكون الطرف المعوّل الذي يتلقى الادعاء أولاً مورّد الهوية، وكما هو مبين في الشكلين 2.V و3.V، فإن وظيفة مورد خدمة الهوية منفصلة ومستقلة عن الطرف المعوّل؛ إذ يقيّم الطرف المعوّل الردود الواردة من مورّد (أو موردي) خدمة الهوية ويقرر ما إذا كان هناك مستوىً كاف من ضمان الاستيقان من الكيان. فالوظيفة الرئيسية لمورّد خدمة هوية هي إدارة معلومات الهوية استحداثها وتحديثها والتحقق منها وتعليقها وحذفها.

وهناك العديد من النماذج لتبادل معلومات الهوية. وأحدها هو نموذج إدارة الهوية ثلاثي الأطراف الشائع الاستعمال والمبين في الشكل 2.V. وتستند بعض البروتوكولات الجديدة المفتوحة لإدارة الهوية إلى هذا النموذج.



الشكل 2.V – مثال عن نموذج إدارة الهوية ثلاثي الأطراف

ويظهر في الشكل 2.V نموذج آخر لإدارة الهوية يوفر للطرف صاحب الطلب المزيد من التحكم في علاقات الهوية.



الشكل 3.V – مثال عن نموذج لإدارة الهوية خماسي الأطراف متحور حول المستعمل

إن النماذج "المتمحورة حول المستعمل" (أي التي تتطلب تفعيل التحكم الكامل للطرف صاحب الطلب في استعمال هوياته) تحظى باهتمام كبير، وقد تنص عليها أيضاً الولايات القضائية الوطنية والإقليمية. ويعرض الشكل 3.V مثالاً يقدم فيه موردو خدمة مختلفون إدارة الهوية. وتوجَّه جميع الاستفسارات/الردود عبر الطرف صاحب الطلب. ولأغراض هذا النوع من النماذج، تعرَّف الكيانات على النحو التالي:

- مورّد الهوية: كيان يقوم بالحفاظ على معلومات هوية موثوقة للكيانات الأخرى وبإدارتها (وتضم هذه الكيانات الأخرى المستعملين النهائيين والمنظمات والأجهزة). ويمكن لمورّد أن يستحدث تلك المعلومات، وهو يقدم خدمات خاصة بالهوية. ويتولى هذا الكيان مسؤولية تخصيص النعوت وإصدارها (أي تلك التي تتضمن الهوية في سياق معين (كتوريد هوية مشترك إلى مورّد مستندات – وهو ما يوصف بالانتساب)). ويتولى أيضاً مسؤولية إدارة دورة حياة الهوية التي تشمل تدقيق الهوية وتسجيلها والحفاظ عليها، بما في ذلك الإلغاء.
- مورّد خدمة المستند: كيان يوفر قدرات تتصل بإصدار مستندات وشارات (كالمستندات التي تُسند الشارات إلى معرّفات ونعوت يمكن التحقق منها).

- مورّد خدمة التحقق: كيان يوفر قدرات تقييم معلومات الهوية (مثل الادعاءات والمستندات) وتصنيف مدى صحتها.
- الطرف المعوِّل [التوصية ITU-T Y.2720]: كيان يعوِّل على تمثيل أو ادعاء هوية من جانب كيان طالب/مؤكِّد في سياق طلب ما.

التذييل VI

مثال عن سيناريو نشر توضيحي لإدارة الهوية في شبكات الجيل التالي

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.VI مقدمة

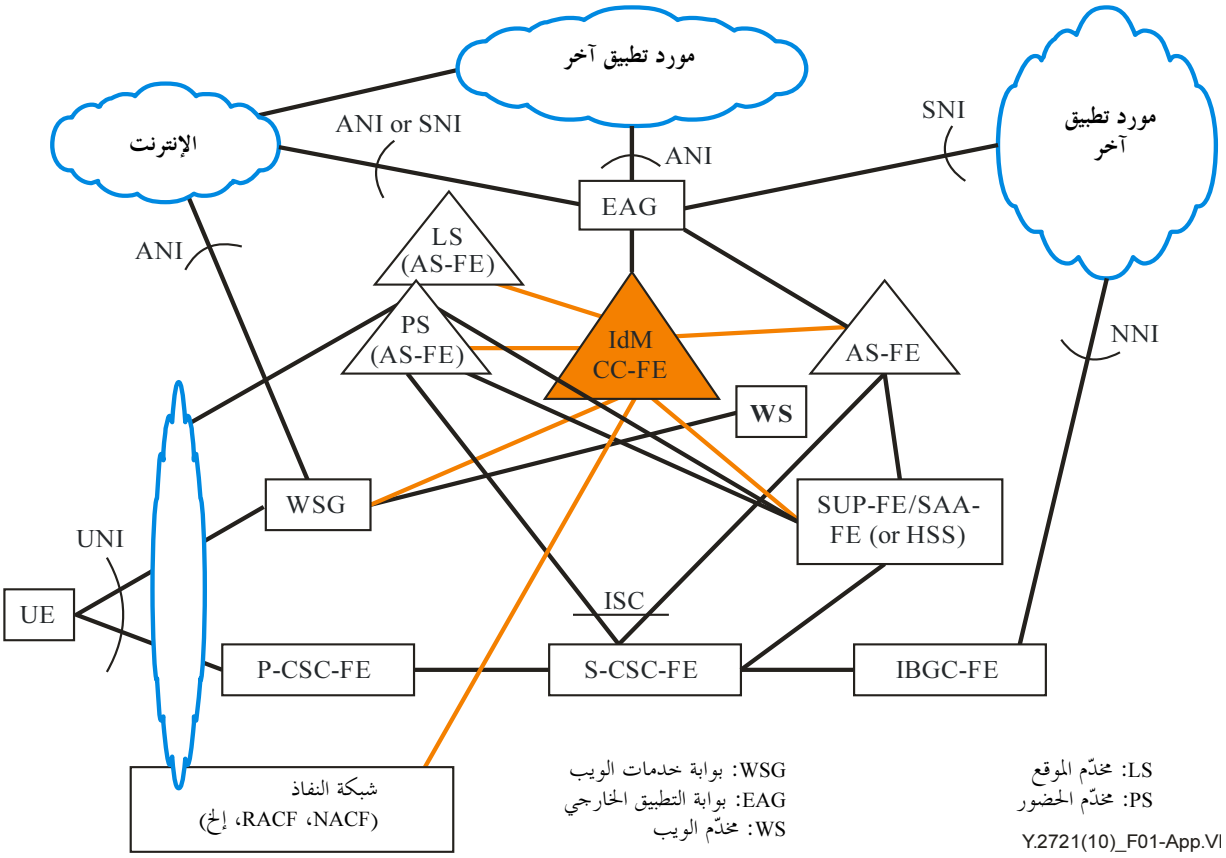
يعرض هذا التذييل مثالاً عن سيناريو نشر لإدارة الهوية في شبكات الجيل التالي.

2.VI نشر معمارية إدارة الهوية

يمكن لشبكات الجيل التالي أن تنشر لمستخدميها البنية التحتية لإدارة الهوية ذات القدرات الداعمة للخدمات القائمة على الهوية بالاستفادة من قدرات ومواصفات خدمات الويب المحددة بمشروع تحالف الحرية (Liberty Alliance Project) وبمعيار الهوية المفتوحة (OpenID). ومثال ذلك، قدرات إدارة الهوية التي تتيح لمستعمليها النفاذ إلى خدمات ما بين ما يقدمه موردون مختلفون للخدمات والتطبيقات، بما في ذلك خدمات التطبيق الاتحادية. كما يمكن لشبكات الجيل التالي أن تدعم قدرات إدارة الهوية لتقدم خدمات مورد خدمة الهوية إلى غيرها من التطبيقات ومقدمي الخدمات (مثل تأكيد هوية جهاز المستعمل والاستيقان منه، وموقعه وغيرها من المعلومات المتعلقة بالهوية).

وستلزم وظائف مد الجسور والعمل البيني لتسهيل إمكانية العمل البيني ولدعم قدرات إدارة الهوية كي تقدم خدمات مورد خدمة الهوية أو تتشارك مع غيرها من التطبيقات ومقدمي الخدمات التي تستخدم أنواعاً مختلفة من أنظمة إدارة الهوية تبعاً لاختلاف الدلالات والمخططات والآليات والتكنولوجيات. فعلى سبيل المثال، يقتضي دعم خدمة إدارة الهوية وقدراتها لدى غيرها من التطبيقات ومقدمي الخدمات (مثل خدمات الويب ومورّدي المحتوى) أن تدعم شبكات الجيل التالي قدرات لما يلي:

- العمل البيني لمعمارية الاعتماد على الذات العامة لمشروع شراكة الجيل الثالث (3GPP GBA) مع إطار تحالف الحرية (Liberty Alliance Framework).
- العمل البيني لمعمارية الاعتماد على الذات العامة لمشروع شراكة الجيل الثالث (3GPP GBA) مع معيار الهوية المفتوحة (OpenID).
- آليات أخرى للعمل البيني مع معيار الهوية المفتوحة (OpenID) وإطار تحالف الحرية (Liberty Alliance Framework).



الشكل 1.VI – مثال نشر إدارة الهوية في شبكات الجيل التالي

يبين الشكل 1.VI مثالاً عن نشر إدارة الهوية في شبكات الجيل التالي. ويُظهر هذا المثال استخدام مخدّم إدارة الهوية الذي قد يكون صندوقاً مستقلاً أو مجموعة من الوظائف الموزعة و/أو الموجودة في مخدّم المشترك المنزلي (HSS). فيقيم مخدّم إدارة الهوية سطحاً بينياً مع عناصر الشبكة ويتفاعل معها ليدعم الكيانات الوظيفية المحددة لشبكات الجيل التالي. فعلى سبيل المثال، يمكن لمخدّم إدارة الهوية أن يقيم سطحاً بينياً مع ما يلي:

ملاحظـــة – بالنسبة لبعض اللوائح الوطنية المحددة قد يستلزم ذلك تنفيذ وظائف منفصلة لإدارة الهوية في الطبقات المختلفة لشبكات الجيل التالي.

- خدمة تمكّن مخدّمات التطبيق (AS)، مثل مخدّم الموقع (LS) أو مخدّم الحضور (PS) أو تطبيقات أخرى ليوفر مستوى أعلى من ضمان الاستيقان وليدعم خدمات التطبيق القائمة على الهوية.
- السياسة المرعية ومرفقات الشبكة ومخدّمات التحكم لضمان الاستيقان وإدارة السياسة المرعية.

وستحتاج شبكات الجيل التالي لدعم قدرات محددة للتحكم في النفاذ وفي العمليات المتبادلة بين إدارة الهوية وغيرها من التطبيقات ومقدمي الخدمات (مثل خدمات الويب ومورّدي المحتوى) كي تدعم خدمات معينة في إدارة الهوية للمستعملين/المشتركين ولكي تقدم خدمات مورد خدمة الهوية أو تتشارك مع غيرها من التطبيقات ومقدمي الخدمات. ويبين هذا المثال التوضيحي استخدام بوابة خدمات الويب (WSG) وبوابة التطبيق الخارجي (EAG) لدعم خدمات معينة في إدارة الهوية بالاستفادة من، أو الشراكة مع، غيرها من التطبيقات ومقدمي الخدمات. وعلى وجه التحديد، يبين الشكل 1.V1 مخدّم إدارة الهوية وهو يقيم سطحاً بينياً مع المستعمل عبر بوابة خدمات الويب (WSG) التي تستيقن من المستعمل وتقدم له سطحاً بينياً لإدارة البيانات العامة لهويته. ويدعم أيضاً الاستيقان المتبادل بين المستعمل ومورد الخدمة، حسب الحاجة. كما يقيم مخدّم إدارة الهوية سطحاً بينياً مع بوابة التطبيق الخارجي (EAG) التي تتيح للمستعمل النفاذ إلى الخدمات القائمة على الويب في شبكات الجيل التالي أو من خلال غيرها من التطبيقات أو مقدمي الخدمات.

بيبليوغرافيا

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

[b-ITU-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2009), *A framework for user control of digital identity*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.

[b-NIST SP 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*.

[b-NIST SP 800-94] NIST Special Publication 800-94 (2007), *Guide to Intrusion Detection and Prevention Systems (IDPS)*.

[b-CA/Browser Forum] CA/Browser Forum, *Guidelines For The Issuance And Management Of Extended Validation Certificates*.

[b-3G Americas White Paper] 3G Americas White Paper (2009), *Identity Management, Overview of Standards and Technologies for Mobile and Fixed Internet*.

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	**البُنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي**
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2012