الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2720
(2009/01)

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

شبكات الجيل التالي – الأمن

إطار إدارة الهوية في شبكات الجيل التالي

التوصيـــة ITU-T Y.2720

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
جودة الخدمة وأداء الشبكة	Y.1599–Y.1500
التشوير	Y.1699–Y.1600
الإدارة والتشغيل والصيانة	Y.1799–Y.1700
الترسيم	Y.1899–Y.1800
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099–Y.2000
جودة الخدمة والأداء	Y.2199–Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249–Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2299–Y.2250
الترقيم والتسمية والعنونة	Y.2399–Y.2300
إدارة الشبكة	Y.2499–Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599–Y.2500
الأمن	**Y.2799–Y.2700**
التنقلية المعممة	Y.2899–Y.2800

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

التوصيـــة ITU-T Y.2720

إطار إدارة الهوية في شبكات الجيل التالي

ملخص

توفر التوصية ITU-T Y.2720 إطاراً لإدارة الهوية (IdM) في شبكات الجيل التالي. والغرض الأول من هذا الإطار هو وصف نهج مبني لتصميم وتعريف وتنفيذ حلول في إدارة الهوية ولتسهيل قابلية التشغيل البيني في بيئة غير متجانسة.

وليس هنالك من جديد في إدارة معلومات هوية الكيان (من قبيل المعرّفات والإثباتات والنعوت). ولكننا إذ نتجه صوب بيئة شبكات متقاربة حيث تعتمد الخدمات على السياقات والأدوار ويكون النفاذ إليها في كل زمان ومكان، يزداد تعقيد عمليات ضمان معلومات الهوية وأمنها وإدارتها. أضف إلى ذلك إمكانية وجود حلول مختلفة ومستقلة تستدعي الحاجة إلى قابلية التشغيل البيني. لذلك من الضروري توفير مقدرات جديدة معززة أوتوماتية وقابلة للتشغيل فيما بينها، وذلك للأسباب التالية:

- المستعمل النهائي يزيد من استعمال هويات متعددة؛
- قد ترتبط هذه الهويات بسياقات وامتيازات خدمة مختلفة؛
- قد لا تعرّف الهويات المستعمل النهائي إلا جزئياً؛
- قد تستعمل الهويات في أي مكان وفي أي زمان؛
- قد لا تكون الهويات قابلة للتشغيل بين المزودين.

وإدارة الهوية تتناول هذه الأحوال وهي مجموعة من الوظائف والمقدرات (من قبيل عمليات الإدارة والصيانة والكشف وتبادل الاتصال والربط وإنفاذ السياسة والاستيقان والتأكيد) التي تستعمل للأغراض التالية:

- ضمان معلومات الهوية (من قبيل المعرّفات والإثباتات والنعوت)؛
- ضمان هوية كيان ما (من قبيل المستعملين/المشتركين والجماعات وأجهزة المستعمل والمنظمات وموردي الشبكات والخدمات وعناصر الشبكة وأغراضها والأغراض الافتراضية)؛
- تمكين تطبيقات الأعمال التجارية والأمن.

ومن المزمع استعمال هذا الإطار كأساس لوضع وتحديد جوانب معينة من إدارة الهوية كالمتطلبات المفصلة والآليات والإجراءات بحسب الحاجة. كما يعطي صورة عامة واضحة ومتماسكة لمجمل إدارة الهوية في شبكات الجيل التالي.

والإطار المرسوم في هذه التوصية ملائم لشبكات الجيل التالي (أي شبكات الرزم المدارة) كما هي معرّفة في التوصية ITU-T Y.2001، نظرة عامة على شبكات الجيل التالي. ولكن من الممكن تطبيقها حسبما يكون مناسباً في أنماط أخرى من الشبكات (شبكات المؤسسات والشركات مثلاً).

ملاحظة – 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.

المصدر

وافقت لجنة الدراسات 13 (2009-2012) لقطاع تقييس الاتصالات بتاريخ 23 يناير 2009 على التوصية ITU-T Y.2720، بموجب إجراء القرار 1 للجمعية العالمية لتقييس الاتصالات.

تمهيـــد

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

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

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

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

ملاحظـــة

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

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

حقوق الملكية الفكرية

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

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

المحتـــويات

الصفحة

التوصيـــة ITU-T Y.2720

إطار إدارة الهوية في شبكات الجيل التالي

1 مجال التطبيق

توفر هذه التوصية إطاراً لإدارة الهوية في شبكات الجيل التالي. والغرض الأساسي من هذه التوصية هو وصف المفاهيم الأساسية والمكونات والقدرات الوظيفية لهذا الإطار الذي يمكن استعماله في تنظيم وتوجيه حلول بناءة لشبكات الجيل التالي. ويشمل مجال تطبيق هذه التوصية ما يلي:

- وصف المسوغات والمنافع والمزايا التجارية لخدمات إدارة الهوية والقدرات التنوعية المستخدمة في توفير ضمان الهوية مع تعريف مفاهيم إدارة الهوية المطبقة على شبكات الجيل التالي وذلك استناداً إلى المتطلبات الوظيفية لشبكة الجيل التالي ومعماريتها (FRA) على النحو المحدد في التوصية [b-ITU-T Y.2012]، *المتطلبات الوظيفية ومعمارية الإصدار 1 من شبكات الجيل التالي*؛
- تحديد ووصف الكيانات الوظيفية والأدوار والعلاقات والظروف المؤاتية والاتصالات الداعمة لخدمات وقدرات إدارة الهوية لشبكات الجيل التالي؛
- تحديد ووصف العلاقات (داخل الشبكة) الداعمة لخدمات وقدرات إدارة الهوية داخل شبكة من شبكات الجيل التالي؛
- تحديد ووصف العلاقات الداعمة لخدمات وقدرات إدارة الهوية بين موردي شبكات الجيل التالي (داخل اتحاد مثلاً) وبين مجموعة من موردي شبكات الجيل التالي ومجموعة أخرى من نظرائهم (بين الاتحادات مثلاً).

والإطار الوارد في هذه التوصية خاص بشبكات الجيل التالي (أي الشبكات المدارة بالرزم) على النحو المحدد في التوصية [b-ITU-T Y.2001]، *نظرة عامة على شبكات الجيل التالي*. بيد أنه يمكن تطبيق هذا الإطار على أنماط الشبكات الأخرى (مثل شبكات الشركات والمؤسسات الخاصة)، حسبما يتناسب.

ومن المزمع استعمال هذا الإطار كأساس لوضع وتوصيف الجوانب المحددة لإدارة الهوية في شبكات الجيل التالي مثل المتطلبات التفصيلية والآليات والإجراءات المطلوبة. كما يقدم نظرة عامة واضحة ومتماسكة بشأن إدارة الهوية إجمالاً في شبكات الجيل التالي.

ملاحظة – 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.

2 المراجع

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

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

3 تعاريف

1.3 مصطلحات معرفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في وثائق أخرى:

1.1.3 إغفال الهوية [التوصية b-ITU-T X.1121]: القدرة على توفير النفاذ إلى الخدمات بدون هوية وهو ما يحول دون تتبع المعلومات الشخصية للمستعمل وسلوكه، مثل موقعه ووتيرة استعماله للخدمة وما إلى ذلك.

2.1.3 الاستيقان [التوصية b-ITU-T X.811]: توفير التأكيد على صحة الهوية التي يدعيها كيان ما.

3.1.3 الترخيص [التوصية b-ITU-T X.800]: منح الحقوق التي تشمل منح إمكانية النفاذ استناداً إلى حقوق النفاذ.

4.1.3 المدّعي [التوصية b-ITU-T X.811]: كيان أو ممثل كيان رئيسي لأغراض الاستيقان. يحتوي الكيان المدعي على الوظائف اللازمة للدخول في تبادلات استيقان بالنيابة عن الكيان الرئيسي.

5.1.3 التفويض [التوصية b-ITU-T X.911]: الإجراء الخاص بإضفاء سلطة أو مسؤولية أو وظيفة لكيان آخر.

6.1.3 معرف الهوية [التوصية b-ITU-T Y.2091]: هو مجموعة أرقام وسمات ورموز أو أي شكل آخر من أشكال البيانات المُستعملة لتحديد هوية المشترك (المشتركين)، أو المستعمل (المستعملين)، أو عنصر (عناصر) شبكة أو وظيفة (وظائف) أو كيان (كيانات) الشبكة التي توفر الخدمات/التطبيقات، أو سواها من الكيانات (كالكيانات المادية أو المنطقية).

7.1.3 شبكة الجيل التالي [التوصية b-ITU-T Y.2001]: 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.

8.1.3 الكيان الرئيسي [التوصية b-ITU-T X.811]: الكيان الذي يمكن التحقق من هويته.

9.1.3 ميدان أمن [التوصية b-ITU-T X.810]: مجموعة عناصر وسياسة أمن وسلطة أمن ومجموعة أنشطة ذات صلة بالأمن تدار فيها العناصر من أجل الأنشطة المحددة طبقاً لسياسة الأمن وتعمد سلطة الأمن إلى تطبيق سياسة الأمن بالنسبة لميدان الأمن.

10.1.3 المتحقق [التوصية b-ITU-T X.811]: كيان أو ممثل كيان يتطلب هوية مستيقن منها. ويحتوي الكيان المتحقق على الوظائف اللازمة للقيام بتبادلات الاستيقان.

2.3 مصطلحات معرفة في معايير أخرى خلاف معايير الاتحاد الدولي للاتصالات

1.2.3 النعت [المعيار b-ETSI TS 102 042]: معلومات وصفية تقتصر على كيان ما تحدد خاصية من خواصه مثل الظروف أو الجودة أو أي معلومات أخرى مرتبطة بهذا الكيان.

3.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.3.3 الضمان: مقياس الثقة بأن الخواص والمعمارية الأمنية لقدرات إدارة الهوية تتوسط بدقة وتعمل على إنفاذ تفهم السياسات الأمنية بين الطرف المعول ومقدم الهوية.

2.3.3 ضمان الاستيقان: انظر الضمان.

3.3.3 مستوى الضمان: تعبير كمي للضمان المتفق عليه بين طرف معول ومقدم هوية.

4.3.3 الإثبات: أي شيء قابل للتعريف يمكن استعماله للاستيقان مما يدعيه المدعي والترخيص له بحقوق النفاذ.

5.3.3 الاكتشاف: عملية تحديد موضع الوصف القابل للمعالجة آلياً لمورد خاص بالشبكة قد يكون مجهولاً من قبل ويفي بمعايير وظيفية معينة. وتشمل هذه العملية مواءمة مجموعة من المعايير الوظيفية وغيرها من المعايير مع مجموعة أوصاف الموارد. والهدف من هذه العملية هو التوصل إلى مورد مناسب خاص بالخدمة.

6.3.3 الكيان: أي شيء يكون له وجود قائم بذاته ومميز يمكن تعريفه بصورة متفردة. ومن أمثلة الكيان، في سياق إدارة الهوية، المشتركون والمستعملون وعناصر الشبكة والشبكات وتطبيقات البرمجيات والخدمات والأجهزة. ويجوز أن يكون للكيان الواحد عدة معرفات هوية.

7.3.3 الاتحاد: إقامة علاقة بين كيانين أو أكثر أو أي اتحاد يضم أي عدد من موردي الخدمات ومقدمي الهويات.

8.3.3 الهوية الاتحادية: هوية يمكن استعمالها للنفاذ إلى مجموعة من الخدمات أو التطبيقات المحددة بسياسات وشروط اتحاد ما.

9.3.3 الهوية: معلومات عن كيان تكفي لتعريف هذا الكيان في سياق معين.

10.3.3 مقدم الهوية (IdP): كيان يقوم باستحداث معلومات هوية موثوقة للكيانات الأخرى مع الحفاظ عليها وإدارتها (وتضم هذه الكيانات الأخرى المستعملين/المشتركين والمنظمات والأجهزة) ويقدم خدمات خاصة بالهوية تقوم على الثقة والأعمال التجارية والأشكال الأخرى من العلاقات.

11.3.3 إدارة الهوية (IdM): 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.

12.3.3 النموذج: تعبير هيكلي مشتق من سلوك كيان معين ويقوم بتعريفه أو المساهمة في تعريفه؛ وقد يشمل ذلك سمعة الكيان. ويمكن للنماذج أن ترتبط بشكل متفرد بكيان أو بصنف يرتبط به الكيان.

13.3.3 معلومات قابلة للتعريف الشخصي: المعلومات الخاصة بأي شخص [حي] والتي تجعل من الممكن التعرف على هذا الفرد (بما في ذلك المعلومات التي تسمح بالتعرف على الشخص عندما تدمج مع معلومات أخرى حتى وإن كانت هذه المعلومات لا تعرِّف الشخص بوضوح).

14.3.3 الوجود: مجموعة من النعوت تحدد خصائص كيان ما بالنسبة لوضعه الحالي.

15.3.3 الخصوصية: حماية المعلومات القابلة للتعريف الشخصي.

16.3.3 الطرف المعوِّل: كيان يعوِّل على تمثيل أو ادعاء هوية من جانب كيان طالب/مؤكِد.

15.3.3 الثقة: مقياس الاعتماد على سمة أو قدرة أو قوة أو الوثوق بشخص أو شيء ما.

4 المختصرات

تستعمل هذه التوصية المختصرات التالية:

API السطح البيني لبرمجة التطبيق *(Application Programming Interface)*

BSS نظام دعم العمليات التجارية *(Business Support System)*

CSCF وظيفة التحكم في دورة النداء *(Call Session Control Function)*

FRA المتطلبات والمعمارية الوظيفية *(Functional Requirements and Architecture)*

GBA معمارية تغذية مرتدة عامة *(Generic Bootstrapping Architecture)*

IdM إدارة الهوية *(Identity Management)*

IdP مقدم هوية *(Identity Provider)*

NGN شبكة الجيل التالي *(Next Generation Network)*

OAM&P التشغيل والإدارة والصيانة والتزويد *(Operation, Administration, Maintenance and Provisioning)*

OSS نظام دعم العمليات التشغيلية *(Operations Support System)*

PII معلومات قابلة للتعريف الشخصي *(Personally Identifiable information)*

PSTN شبكة هاتفية عمومية تبديلية *(Public Switched Telephone Network)*

QoE جودة الخبرة *(Quality of Experience)*

QoS جودة الخدمة *(Quality of Service)*

RP طرف معوِّل *(Relying Party)*

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

SBC مراقب حدود الدورة *(Session Border Controller)*

SIP بروتوكول استهلال الدورة *(Session Initiation Protocol)*

SP مورد خدمة *(Service Provider)*

SS7 نظام التشوير رقم 7 *(Signaling System No. 7)*

URI معرف هوية مورد منتظم *(Uniform Resource Identifier)*

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

5 مقدمة

1.5 نظرة عامة على إدارة الهوية

إن إدارة معلومات هوية كيان (مثل معرفات الهوية والإثباتات والنعوت) ليست بالأمر الجديد. ولكننا إذ نتجه صوب بيئة شبكات متقاربة حيث تعتمد الخدمات على السياقات والأدوار ويكون النفاذ إليها في كل زمان ومكان يزداد تعقيد عمليات ضمان معلومات الهوية وأمنها وإدارتها. أضف إلى ذلك إمكانية وجود حلول مختلفة ومستقلة تستدعي الحاجة إلى قابلية التشغيل البيني. لذلك من الضروري توفير قدرات جديدة معززة أوتوماتية وقابلة للتشغيل فيما بينها. والغرض الأساسي من هذا الإطار هو وصف نهج بناء لتصميم وتعريف وتنفيذ حلول من شأنها أن تسهيل قابلية التشغيل البيني في بيئة غير متجانسة.

وتتناول إدارة الهوية هذا الأمر، وهي 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؛
- ضمان هوية كيان ما؛
- تمكين تطبيقات الأعمال التجارية والتطبيقات الأمنية.

ويقدم الشكل 1 نظرة عامة على إدارة الهوية.

الشكل 1 – نظرة عامة على إدارة الهوية

ويمكن تصنيف معلومات الهوية المرتبطة بكيان ما كما يلي:

- معرفات الهوية (مثل معرف هوية المستعمل وعناوين البريد الإلكتروني وأرقام الهواتف ومعرف هوية مورد منتظم وعناوين بروتوكول الإنترنت)؛
- الإثباتات (مثل الشهادات الرقمية والأمارات الرمزية والسمات البيومترية)؛
- النعوت (مثل الأدوار والادعاءات والامتيازات والنماذج والموقع).

وتستعمل وظائف وقدرات إدارة الهوية في ضمان معلومات الهوية؛ وضمان هوية كيان ما؛ ودعم تطبيقات الأعمال التجارية والتطبيقات الأمنية بما في ذلك الخدمات القائمة على الهوية.

وعلاوة على ذلك، تتيح خدمات وقدرات إدارة الهوية لكيانات المستعملين/المشتركين التحكم في طريقة استعمال ونشر معلومات الهوية الخاصة بهم. كما تسمح إدارة الهوية بتقاسم واستعمال معلومات الهوية الاتحادية من جانب أعضاء الاتحاد (مثل الشركاء التجاريين) لدعم الخدمات الاتحادية.

وتمكن إدارة الهوية من تطوير الكثير من التطبيقات المتنوعة. والتطبيقات التالية بعد على سبيل المثال لا الحصر:

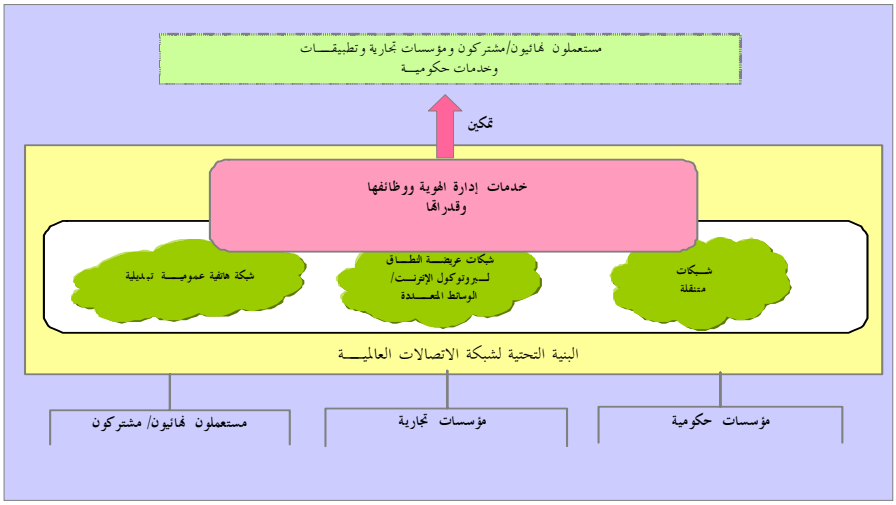
- *تطبيقات الأعمال التجارية*
  - تسجيل دخول وخروج وحيد (مثل النفاذ إلى التطبيقات والخدمات دون الحاجة إلى الاستيقان الفردي لكل منصة تطبيق أو خدمة)
  - الخدمات الاتحادية (مثل النفاذ إلى الخدمات عبر موردي خدمات مختلفين أو موردين لشبكات الجيل التالي).

- *الخدمات القائمة على الهوية*
  - الخدمات الخاصة بمعرفات الهوية والإثباتات والنعوت
  - خدمات التجسير (مثل تقابل وتشبيك معلومات الهوية في بيئة غير متجانسة)
  - خدمات معلومات النماذج
- *التطبيقات الأمنية*
  - التحكم في النفاذ بالنسبة لخدمات الشبكات والتطبيقات (مثل نقل الصوت عبر بروتوكول الإنترنت والتلفزيون القائم على بروتوكول الإنترنت والبيانات)
  - التحكم في النفاذ القائم على الدور المؤدى إلى المعلومات والموارد والأصول
  - إدارة الترخيص والامتيازات
  - خدمات الحماية الأمنية (مثل الخواص الأمنية لحماية موارد البنية التحتية للشبكة ومعلومات الهوية الخاصة بالمستعملين/المشتركين والأصول)
  - حماية المعلومات القابلة للتعريف الشخصي (PII).

وفي بيئة تضم موردي خدمات متعددين واتحادات، تستعمل خدمات وقدرات إدارة الهوية في اكتشاف وتوصيل معلومات من شأنها بناء الثقة في هوية (هويات) كيان ما بين كيانات شبكية مختلفة مثل المشتركين/المدعين والأطراف المعولة (مثل المستعملين وموردي الخدمات والشبكات) وموردي خدمات الهوية (مثل موردي الإثباتات وموردي وسائل التحقق) عبر ميادين الشبكات والميادين الأمنية. فمثلاً، يمكن التحقق من معرفات الهوية والإثباتات والنعوت الخاصة بهوية ما عن طريق مقدم هوية منتقى (مثل مورد الاستيقان/المتحقق) وتوصيلها من خلال عمليات التأكد إلى طرف معول (كمورد خدمة مثلاً) لتسهيل التحكم في النفاذ والقرارات التجارية وإنفاذ السياسات المطبقة (مثل الخصوصية وحماية المعلومات القابلة للتعريف الشخصي).

2.5 العوامل المؤثرة على الأعمال التجارية ودوافعها

فضلاً عن كونها أداة تمكينية لأمن شبكات الجيل التالي، تمكن إدارة الهوية وتسهل من تطبيقات وخدمات الأعمال التجارية الجديدة والبازغة لشبكات الجيل التالي (مثل التطبيقات الثابتة والمتنقلة المتقاربة والتطبيقات القائمة على شبكة الويب). وتحديداً، تدعم خدمات إدارة الهوية وقدراتها ووظائفها نطاق عريض من المستعملين النهائيين/المشتركين ومؤسسات الأعمال التجارية (مثل موردي الشبكات والخدمات والشركات) وتطبيقات وخدمات المؤسسات الحكومية على النحو المبين في الشكل 2.



الشكل 2 – استعمال خدمات إدارة الهوية

وتعتبر إدارة الهوية أحد المكونات الحاسمة في إدارة أمن شبكات الجيل التالي وتمكين النفاذ المتجول وحسب الطلب إلى خدمات وتطبيقات شبكات الجيل التالي التي تحدد خصائص توقعات المستعملين النهائيين في عصر المعلومات. فإلى جانب الآليات الدفاعية الأخرى (مثل حوائط الحماية وأنظمة كشف عمليات التطفل والاقتحام والحماية من الفيروسات الحاسوبية)، تلعب إدارة الهوية دوراً هاماً في حماية البنية التحتية لشبكات الجيل التالي وخدماتها وتطبيقاتها من الجرائم السيبرانية مثل الاحتيال وسرقة الهوية. كما أنه نتيجة لثقة المستعملين بأن معاملات شبكات الجيل التالي ستكون آمنة وموثوقة، فستؤدي إدارة الهوية إلى إتاحة الفرصة أمام عروض لخدمات جديدة قائمة على الهوية. ومن ثم سيعزز استعمال إدارة الهوية إلى حد كبير الخدمات والقدرات الحالية للشبكات. ويقدم الجدول 1 ملخصاً للعوامل المؤثرة في إدارة الهوية ودوافعها.

الجدول 1 – العوامل المؤثرة في إدارة الهوية ودوافعها

الفئة المنظورة	العوامل المؤثرة في إدارة الهوية ودوافعها
مستعملون نهائيون/مشتركون	• تحكم المستعمل في المعلومات الشخصية وحماية المعلومات القابلة للتعريف الشخصي [PPII] – يوفر القدرة على التحكم فيمن يُسمح له بالنفاذ (أي منح الموافقة) إلى المعلومات الشخصية وكيفية استعمالها) • تسجيل وحيد للدخول والخروج – يوفر نفاذ منتظم إلى التطبيقات/الخدمات المتعددة وعبر موردي خدمات متعددين/اتحادات متعددة. • تحكم مرن في النفاذ بالنسبة لخدمات الشبكات وتطبيقاتها (مثل نقل الصوت عبر بروتوكول الإنترنت والتلفزيون القائم على بروتوكول الإنترنت والبيانات) • التشبيك المجتمعي – يوفر قدرات دينامية ومرنة للهوية من أجل النفاذ إلى الخدمات الشبكية الاجتماعية بثقة. • الأمن – يوفر الثقة في التعاملات، من خلال إدخال وسيلة للحماية من سرقة الهوية (ID)
مؤسسات تجارية (مثل موردي شبكات الجيل التالي)	• تمكن من النفاذ إلى الخدمات القائمة على الاشتراك من أي مكان وفي أي وقت ومن أي جهاز. • توفر وظائف وقدرات ضمان الهوية لدعم تطبيقات وخدمات متعددة • تمكن من التوصيلية الدينامية/الأوتوماتية بين شركاء متعددين (مثل المستعملين النهائيين والشبكات المزارة والأصلية) مقارنة بالترتيبات القائمة على الأزواج وذلك لوضع ترتيبات الخدمة وتبادل معلومات الهوية وإنفاذ السياسات • تسمح بتطبيقات وخدمات جديدة (مثل التقارب بين الخدمة الثابتة والمتنقلة) بما في ذلك الخدمات القائمة على الهوية مثل خدمات معرفات الهوية والإثباتات والنعوت للمشتركين وموردي الخدمات الآخرين • تسمح بمخطط قياسي للسطح بيني لبرمجة التطبيق والبيانات لتصميم التطبيق عبر بائعين متعددين ومنصات تزويد بالخدمة متعددة • تتيح الهوية والخدمات الاتحادية • توفر الحماية لخدمات التطبيقات والبنية التحتية للشبكات والموارد • تسهل من الامتثال للمتطلبات التنظيمية
مؤسسات حكومية	• تسمح بخدمات وقدرات ضمان الهوية وتزيد من مستوى الثقة والموثوقية في الهويات لدعم: – خدمات الحكومة الإلكترونية (مثل المعاملات القائمة على شبكة الويب) – خدمات السلامة العامة (خدمات الطوارئ للرقم 911) – خدمات إنفاذ القانون (مثل عمليات التنصت القانونية) – خدمة اتصالات الطوارئ (ETS) – خدمات الإنذار المبكر – خدمات الأمن الوطني • تسمح بالخدمات الحكومية الاتحادية • توفر الحماية للبنى التحتية للاتصالات (أي حمايتها من تهديدات الأمن السيبرانية)

3.5 مقدم الهوية (IdP)

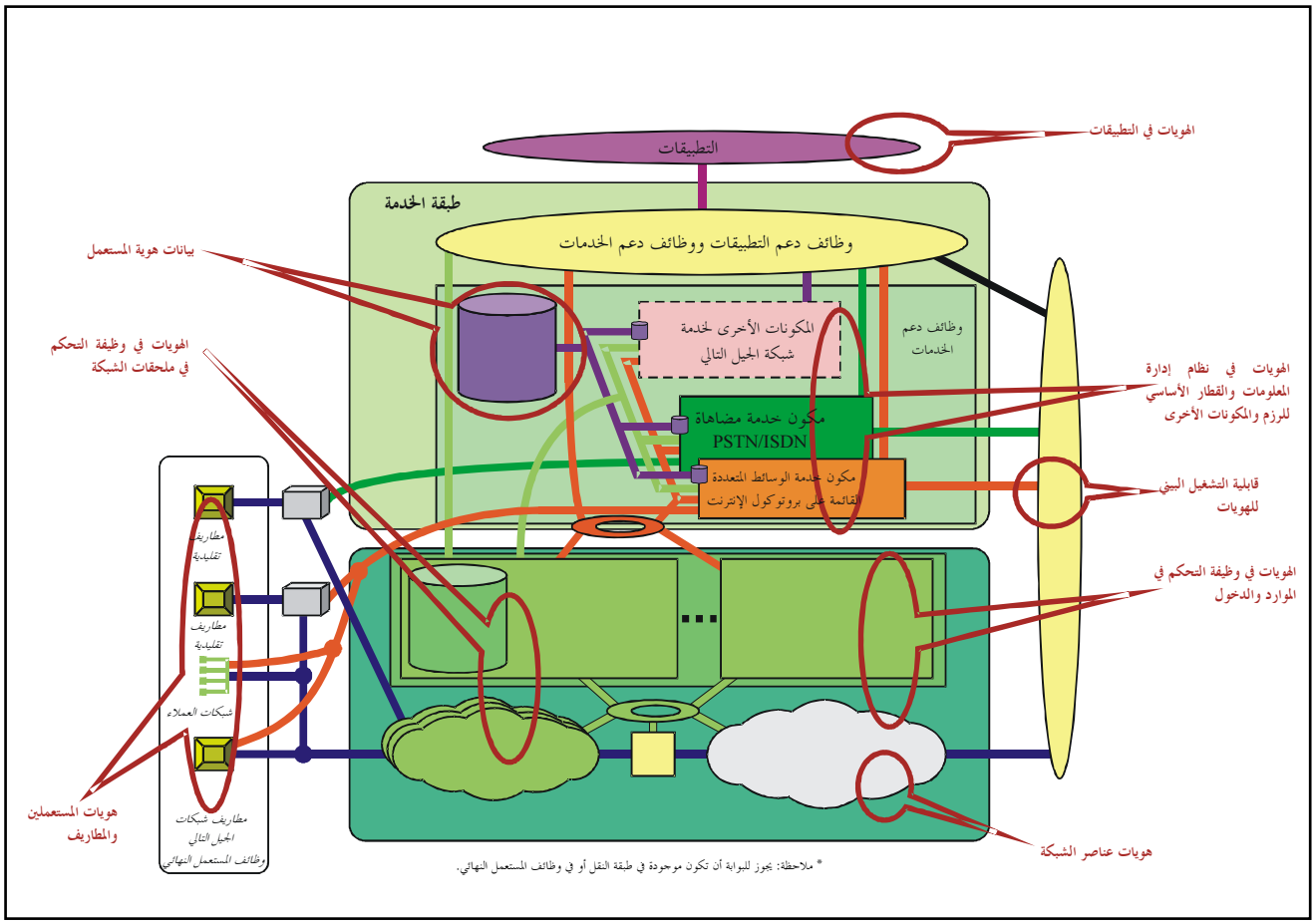
لا تفرض هذه التوصية أي قيود على من يوفر خدمات مقدم الهوية (IdP).

ومقدم الهوية عبارة عن كيان يقوم باستحداث معلومات هويات موثوقة لكيانات أخرى (مثل المستعملين/المشتركين والمنظمات والأجهزة) ويحافظ عليها ويقوم بإدارتها ويقدم خدمات خاصة بالهوية تقوم على الثقة والأعمال التجارية والأشكال الأخرى من العلاقات.

وفي بيئة تضم العديد من موردي الخدمات، قد يكون مورد شبكات الجيل التالي هو نفسه مقدم الهوية. ويمكن لمورد شبكات الجيل التالي أن يوفر أيضاً خدمات مقدم الهوية (مثل الخدمات القائمة على الهوية) لموردين آخرين. وعلاوة على ذلك، يمكن استعمال خدمات مقدم الهوية الخاصة بطرف ثالث.

4.5 المعمارية الوظيفية لشبكة الجيل التالي واستعمال معرفات الهوية

على نحو ما ورد شرحه في التوصية [b-ITU-T Y.2012]، *المتطلبات الوظيفية ومعمارية الإصدار 1 من شبكات الجيل التالي*، تتكون شبكة الجيل التالي من عناصر وظيفية متعددة تستعمل معرفات الهوية الخاصة بالكيانات للقيام بوظائفها من أجل دعم وتسهيل الخدمات والتطبيقات. ويبين الشكل 3 أمثلة لهويات تم مقابلتها بمخطط وظيفي لشبكة من شبكات الجيل التالي، أي معمارية شبكة الجيل التالي المبينة في التوصية [b-ITU-T Y.2012].



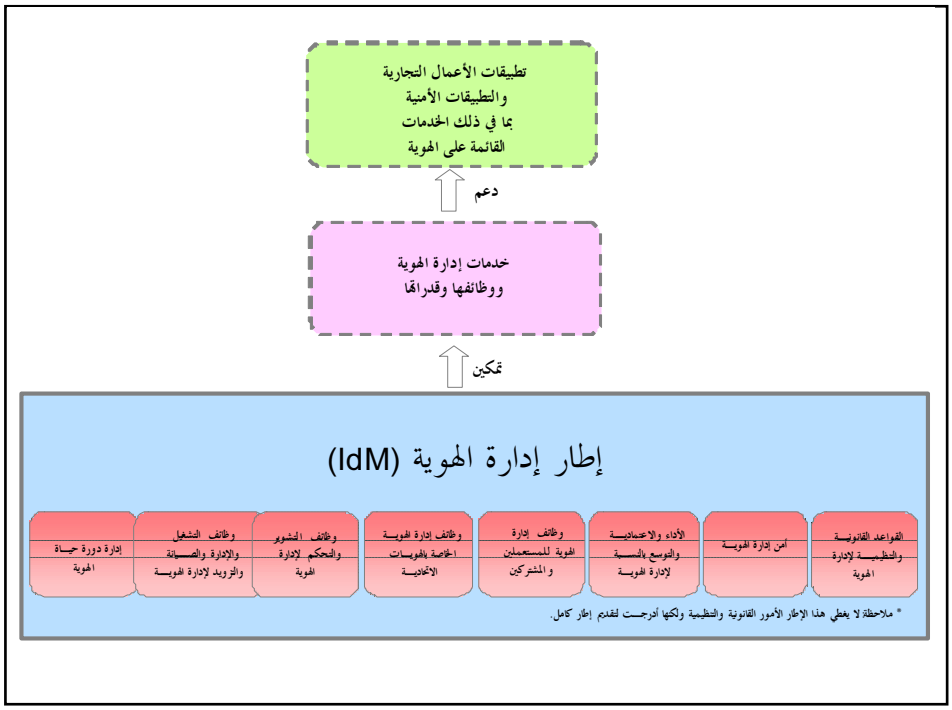
الشكل 3 – أمثلة على هويات شبكات الجيل التالي

وحيث إن جميع عمليات شبكات الجيل التالي تستعمل هذه الهويات المتنوعة، فإن من المهم الحفاظ على سلامة هوياتها. وتوفر إدارة الهوية خدمات الضمان وقدراته ووظائفه فيما يتعلق بسلامة هويات شبكات الجيل التالي واستعمالها.

وفي بيئة شبكة الجيل التالي، يجوز وجود عدة نعوت للهوية الواحدة. ويمكن استعمال نعوت الهوية هذه من جانب عناصر مختلفة للشبكة (مثلاً، في ميادين مختلفة لمورد شبكات الجيل التالي أو في طبقات مختلفة لشبكة الجيل التالي (أي طبقة الخدمة أو طبقة النقل)) وبمقدور كيانات مختلفة في مواقع مختلفة استعمال نعوت الهوية هذه أيضاً. ولهذا من الضروري أن توفر إدارة الهوية قدرات تسمح بالتبادل الآمن للمعلومات بين الكيانات (و/أو المواقع) مثل الأطراف المعولة (مثل التطبيقات أو الخدمات أو مورديها) ومقدمي الهويات (IdP). وتجدر الإشارة إلى أن مورد شبكات الجيل التالي يمكن أن يكون هو نفسه مقدم الهوية في نفس الوقت. ويقوم تبادل معلومات إدارة الهوية على سياسات محددة وعلى الثقة القائمة بين هذه الكيانات في بيئة تضم العديد من موردي الخدمات. وتقوم هذه الثقة على التأكد والتحقق من هويات الكيانات عبر شبكات الجيل التالي الموزعة. كما توفر إدارة الهوية قدرات لحماية خصوصية معلومات الكيانات (مثل نعوت الهوية المحددة) ولضمان نشر المعلومات المعتمدة فقط عبر شبكات الجيل التالي.

6 نظرة عامة على إطار إدارة الهوية

يبين الشكل 4 تنظيم هذا الإطار.



الشكل 4 – نظرة عامة على إطار إدارة الهوية

ويتكون الإطار من وظائف وقدرات إدارة الهوية التالية:

1) إدارة دورة حياة الهوية

يشمل ذلك عمليات ووظائف إدارة دورة حياة الهويات ومعلومات الهويات (مثل معرفات الهوية والإثباتات والنعوت). وتضم إدارة دورة حياة الهوية العمليات والإجراءات المرتبطة بتسجيل وإصدار هوية أو البيانات والمعلومات المرتبطة بهوية كيان ما.

2) وظائف التشغيل والإدارة والصيانة والتزويد (OAM&P) لإدارة الهوية (IdM)

يشمل ذلك الوظائف والقدرات الإدارية الخاصة بالتشغيل والإدارة والصيانة والتزويد (OAM&P) المتعلقة تحديداً بدعم إدارة الهوية. ووظائف (OAM&P) عبارة عن مجموعة من الوظائف الإدارية التي توفر مؤشرات الأعطاب ومراقبة الأداء والإدارة الأمنية ووظائف التشخيص والتشكيل وتزويد المستعملين بالنسبة للنظام أو الشبكة. وهي تضم على وجه التحديد الوظائف والقدرات التي تدعمها أنظمة إدارة الشبكات والتي تسمى نمطياً أنظمة دعم عمليات التشغيل (OSS) وأنظمة دعم العمليات التجارية (BSS).

3) وظائف التشوير والتحكم لإدارة الهوية

يشمل ذلك وظائف وقدرات التشوير والتحكم المستعملة في دعم خدمات إدارة الهوية وقدراتها ووظائفها. وتضم التشوير والتحكم بالنسبة لكل من اتصالات الوقت الفعلي والاتصالات القريبة من الوقت الفعلي.

4) وظائف إدارة الهوية للهويات الاتحادية

يشمل ذلك وظائف وقدرات توحيد الهوية ودعم الخدمات الاتحادية.

5) وظائف إدارة الهوية (IdM) للمستعملين والمشتركين

يشمل ذلك الوظائف والعمليات المتعلقة بتحكم المستعملين النهائيين والمشتركين في معلوماتهم الخاصة بالهوية (مثل المعلومات القابلة للتعريف الشخصي ومؤشرات الأداء الشخصية والموقع). وتضم هذه الوظائف والعمليات الوظائف الخاصة بالتحكم والتفويض والتخويل بالنسبة إلى استعمال ونشر المعلومات المتعلقة بالهوية.

6) الأداء والاعتمادية والقابلية للتوسع بالنسبة لإدارة الهوية

يشمل ذلك الوظائف والإجراءات التي تتناول الأداء والاعتمادية والقابلية للتوسع بالنسبة لأنظمة إدارة الهوية وحلولها.

7) أمن إدارة الهوية (IdM)

يشمل ذلك الوظائف والإجراءات التي تتناول توفير الحماية الأمنية لأنظمة إدارة الهوية وخدماتها وقدراتها.

8) القواعد القانونية والتنظيمية لإدارة الهوية (IdM)

لا تدخل اللوائح القانونية والتنظيمية ضمن نطاق هذه التوصية.

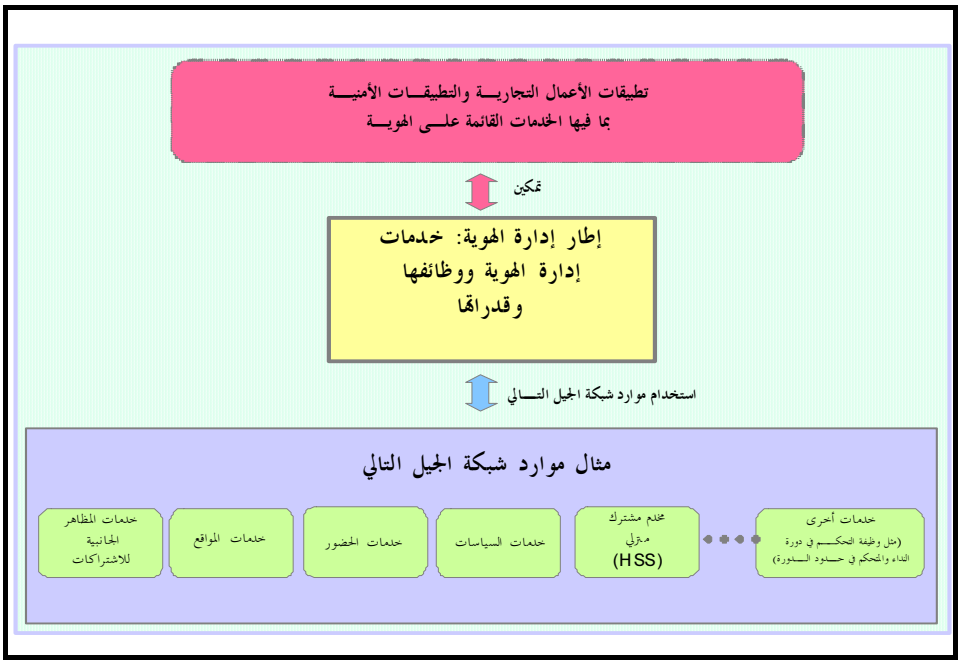
ملاحظة – هذا البند مدرج هنا لأغراض الاستكمال.

ويرد الوصف التفصيلي لكل بند من هذه البنود في القسم 8.

7 إدارة الهوية في سياق معماريات شبكات الجيل التالي ونماذجها المرجعية

1.7 العلاقة العامة بمعماريات شبكات الجيل التالي وخدماتها

يوضح الشكل 5 علاقة إطار إدارة الهوية في السياق الأوسع لشبكات الجيل التالي.

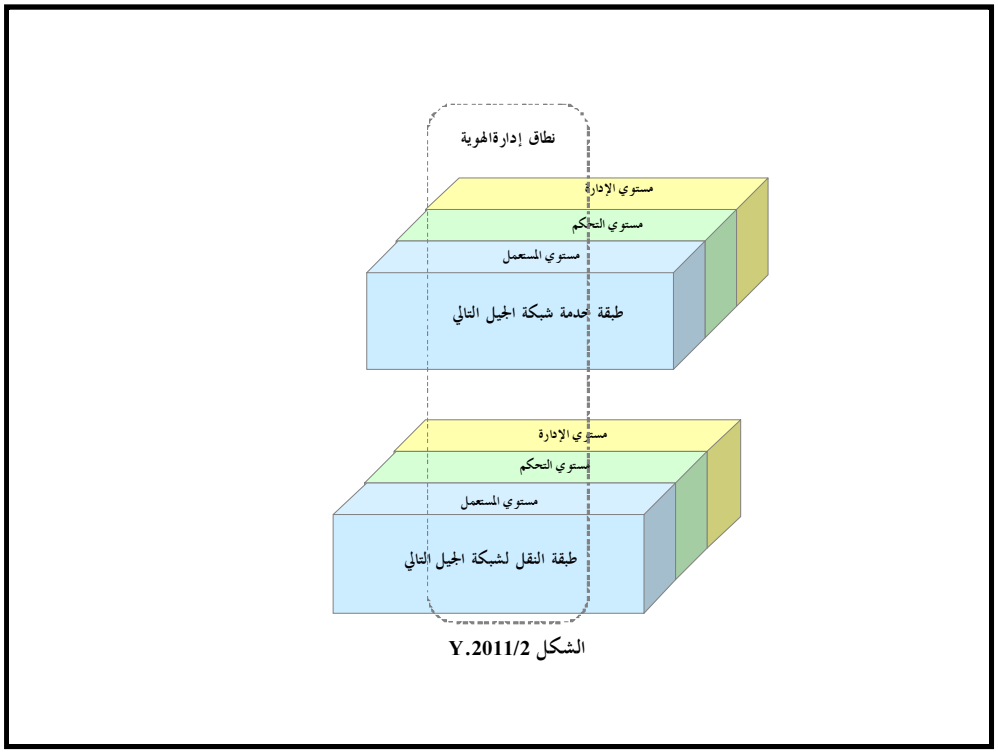


الشكل 5 – العلاقة بمعماريات شبكات الجيل التالي وخدماتها

كما يبين المخطط، يستخدم الإطار موارد شبكة الجيل التالي (مثل المعلومات الخاصة بالاشتراك والموقع والسياسات والحضور ومخدمات المشتركين المنزليين وعناصر الشبكة الأخرى مثل وظيفة التحكم في دورة النداء (CSCF) والمتحكم في حدود الدورة (SBC). وتستعمل خدمات إدارة الهوية ووظائفها وقدراتها التي يوفرها هذا الإطار في دعم وتعزيز تطبيقات الأعمال التجارية والتطبيقات الأمنية بما في ذلك الخدمات القائمة على الهوية.

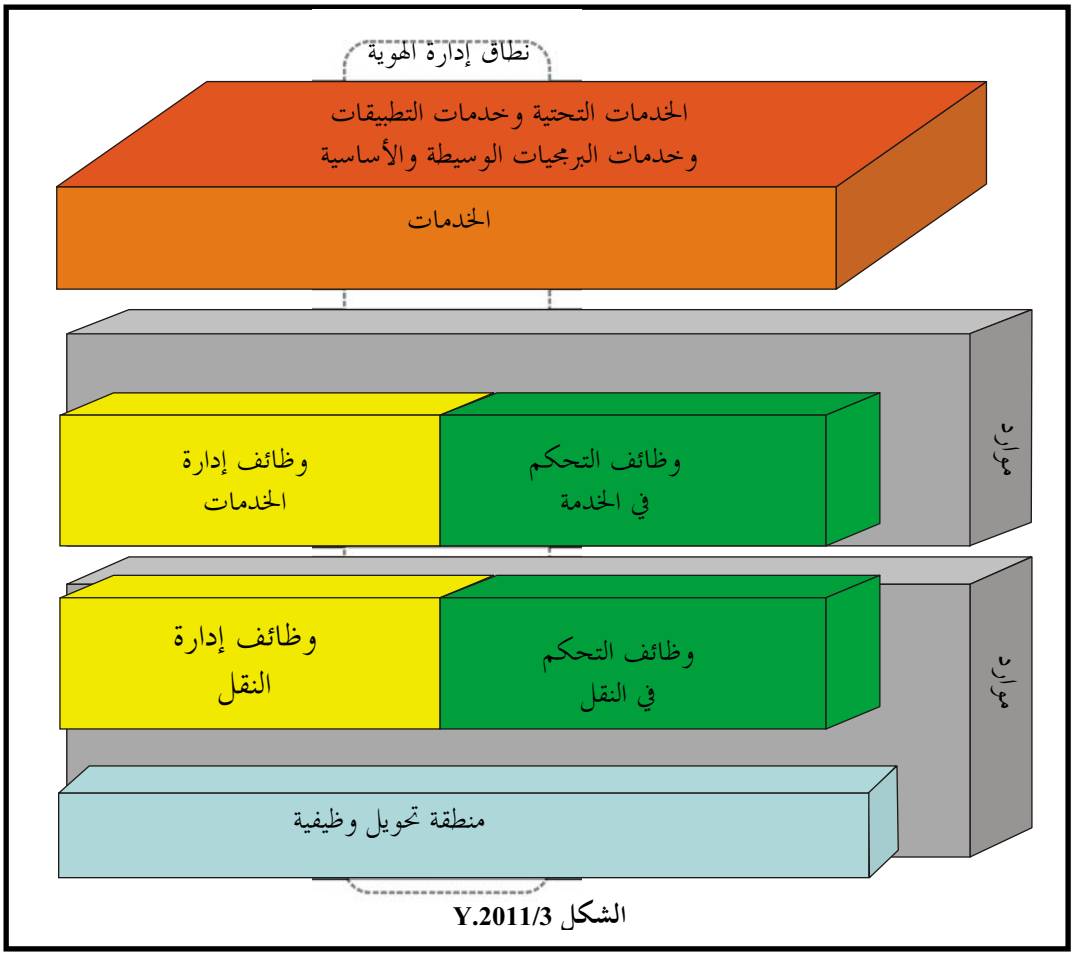
2.7 النماذج المرجعية للتوصية ITU-T Y.2011 (المبادئ العامة والنموذج المرجعي العام لشبكة الجيل التالي)

تصف هذه الفقرة خدمات إدارة الهوية ووظائفها وقدراتها في سياق النماذج المعمارية والمراجع الخاصة بشبكة الجيل التالي المحددة في التوصية [ITU-T Y.2011]، *المبادئ العامة والنموذج المرجعي العام لشبكات الجيل التالي*.



الشكل 6 – نطاق إدارة الهوية في سياق الشكل 2 للتوصية ITU-T Y.2011

يبين الشكل 6 نطاق إدارة الهوية في سياق النموذج المعماري المرجعي لشبكة الجيل التالي المحدد في الشكل 2 من التوصية [ITU-T Y.2011]. ويتبين من الشكل أن الوظائف المتعلقة بإدارة الهوية يمكن وجودها في مستويات المستعمل والتحكم والإدارة.



الشكل 7 – إدارة الهوية في سياق الشكل 3 للتوصية ITU-T Y.2011

يبين الشكل 7 نطاق إدارة الهوية في سياق النموذج المعماري المرجعي لشبكة الجيل التالي المحدد في الشكل 3 من التوصية [ITU-T Y.2011]. ويتبين من الشكل أن الوظائف المتعلقة بإدارة الهوية يمكن وجودها في جميع الطبقات الرأسية لمعمارية شبكة الجيل التالي.

8 إطار إدارة الهوية

يقدم هذا القسم الوصف التفصيلي للمجموعات الوظيفية المذكورة في الفقرة 6 أعلاه.

1.8 إدارة دورة حياة الهوية

1.1.8 الإثبات والتسجيل

تبدأ الخطوة الأولى في عملية استحداث هوية لكيان ما (مثل المشترك أو الجهاز أو المنظمة أو مورد شبكات الجيل التالي أو أحد أشياء الشبكة) بعملية إثبات وتسجيل الهوية أو الإثبات. وهي العملية الخاصة بإقرار هوية أو إثبات مرتبطين بكيان معين قد يستندا إلى سياق معين (كالأدوار مثلاً).

وفي حالة مشتركي المستعملين النهائيين، تكون هذه العملية هي العملية التي يتقدم فيها المدعي بطلب لكي يصبح مشتركاً لدى أحد مقدمي الهويات أو أحد موردي شبكات الجيل التالي.

وفي هذه الحالة، يجوز أن يكون اسم المشترك اسما متحققاً منه أيضاً. ويرتبط الاسم المتحقق منه بهوية كيان ما. وقبل أن يتلقى مقدم الطلب الإثباتات أو يُمنح أمارات رمزية مصاحبة لاسم متحقق منه، يتعين عليه إثبات أن الهوية هوية حقيقية وأن مقدم الطلب هو الكيان المخول له استعمال الهوية. وتسمى هذه العملية بإثبات الهوية. وبمجرد التحقق من الاسم، يمكن أن يصاحبه اسم مستعار لإضفاء سمة الهوية المبهمة.

ويشمل الإثبات التحقق من النعوت والادعاءات المرتبطة بالهوية. وتضم العمليات والإجراءات الخاصة بالتحقق من المعلومات والتأكد من صلاحيتها عند تسجيل كيان ما في نظام هوية.

وتعتمد الفعالية الكلية لإدارة الهوية على عملية الإثبات والتسجيل. ويتعين وجود شروط ضمان محددة جيداً وسياسات مناسبة وإجراءات إدارية للتأكد من أن عملية التسجيل بأكملها مصممة ومطبقة بشكل جيد.

وتضم المبادئ التوجيهية التي يتعين مراعاتها:

- تدريب الأفراد المشاركين في عملية التسجيل
- جودة الوثائق والأدلة الأخرى الداعمة لتسجيل كيان ما
- عمليات لتفادي التخفي عند التسجيل
- عمليات لتفادي تعدد أو ازدواج التسجيل للكيان نفسه.

2.1.8 الإصدار والإلغاء

ينتج عن استكمال عملية التسجيل بنجاح منح وسيلة (إثبات مثلاً) يمكن استيقان الكيان بها مستقبلاً. فمثلاً يكون إصدار مقدم هوية (أو مورد شبكات الجيل التالي) لإثبات (إثباتات) مقيداً بالهوية أو النعوت ذات الصلة (مثل الامتيازات والادعاءات) الخاصة بالهوية المرتبطة بكيان ما.

وإلغاء الهوية هي العملية الخاصة بإلغاء هوية والإثباتات المصاحبة لها. والطرف أو النظام (مقدم هوية أو مورد شبكات الجيل التالي مثلاً) الذي يصدر هوية أو إثبات يكون مسؤولاً عن الحفاظ على المعلومات المرتبطة بالهوية وحمايتها. والإلغاء ضروري لمنع الاستعمال المستمر لهوية أو إثبات انتهت صلاحيتهما أو خالفا القانون.

ومن بين المبادئ التوجيهية التي يتعين مراعاتها:

- وضع معايير للإصدار والإلغاء
- وضع معايير لإدخال التحديثات والتعديلات
- تزامن معلومات الهوية
- تحديد عمليات وإجراءات للإصدار والإلغاء
- تدقيق ومراجعة عمليات الإصدار والإلغاء
- إجراءات وعمليات للتبليغ عن عمليات إصدار وتحديث وإلغاء الهويات أو الإثباتات (بمعنى أنه يتعين أن يكون بمقدور جميع الأنظمة والعمليات التي تم وضع الهوية معها أن تحدد أن الهوية أو الإثباتات قد صدرت وحُدثت وأُلغيت).
- إجراءات وعمليات محددة جيداً لإصدار وإلغاء الهويات أو الإثباتات مع السياسات الملائمة. ويلزم أيضاً وجود إجراءات إدارية للتأكد من أن العملية بأكملها مصممة ومطبقة بشكل جيد.
- آليات لحماية عمليات وإجراءات الإلغاء من التهديدات الأمنية.

2.8 وظائف التشغيل والإدارة والصيانة والتزويد لإدارة الهوية

1.2.8 نماذج البيانات ومخططاتها

يجوز أن يكون لكل مورد من موردي شبكات الجيل التالي أو اتحاد أو مؤسسة ما يخصه من أنساق أو مخططات أو تعاريف أو دلالات لغوية لتمثيل البيانات والمعلومات المتعلقة بالهوية وتبادلها. فمثلاً، يمكن لمعلومة واحدة كتاريخ الميلاد مثلاً أن تُمثل بشكل مختلف من جانب نظامين مختلفين (شهر/يوم/سنة أو يوم/شهر/سنة). كما أن الدلالات اللغوية والمخططات والبروتوكولات المستعملة لطلب المعلومات المتعلقة بالهوية وتبادلها يمكن أن تختلف مما يؤدي إلى ظهور مشكلات خاصة بالتشغيل البيني. فعلى سبيل المثال، فإن معلومات الهوية في الشبكة الهاتفية العمومية التبديلية (PSTN) مثل رقم الطرف طالب

النداء وهوية طالب النداء تُمثل باستعمال دلالات محددة ويتم استرجاعها باستعمال بروتوكولات محددة (مثل نظام التشوير SS7) وتختلف عن أنظمة نقل الصوت عبر بروتوكول الإنترنت القائمة على بروتوكول استهلال الدورة.

وإنه لمن المهم وجود حلول تسمح بالتشغيل البيني بين أنظمة إدارة الهوية غير المتجانسة التي تستعمل نماذج وهياكل ومخططات مختلفة للبيانات.

ومن بين المبادئ التوجيهية التي يتعين مراعاتها:

- وجود نماذج ومخططات للبيانات من شأنها أن تسهل التشغيل البيني بين أنظمة إدارة الهوية غير المتجانسة (مثل مصادر بيانات الهوية) ضمن نطاق ميدان مورد شبكات الجيل التالي (أي منتجات موردين مختلفين)؛
- وجود نماذج ومخططات للبيانات من شأنها أن تسهل التشغيل البيني بين موردين مختلفين لشبكات الجيل التالي (بين الشبكات)؛
- وجود نماذج ومخططات للبيانات من شأنها أن تسهل التشغيل البيني بين اتحادات مختلفة (مثل مورد شبكات الجيل التالي ومورد خدمات الويب).

2.2.8 إدارة معرفات الهوية

يجوز أن يكون لهوية (هويات) كيان ما (مثل مستعمل/مشترك، منظمة، اتحاد، مؤسسة، مورد خدمة، جهاز، أشياء للشبكة) معرف هوية واحد أو أكثر مصاحب للهوية يتعين إدارته والحفاظ عليه.

ومعرف الهوية عبارة عن أي تسمي تُستعمل لتمثيل هوية كيان ما مثل معرف هوية المستعمل ومعرف هوية الشبكة وعنوان البريد الإلكتروني والاسم المستعار وأي مجموعة من الأسماء وما إلى ذلك. فمثلاً يمكن لمعرفات الهوية الواردة أدناه أن تصاحب الهوية الخاصة بمستعمل/مشترك:

- معرف هوية المستعمل
- عنوان البريد الإلكتروني
- رقم الهاتف
- معرف هوية مورد منتظم
- عناوين بروتوكول الإنترنت.

وتعتمد الفعالية الكلية لإدارة الهوية على ضمان معرفات الهوية الإفرادية التي يمكن ربطها وارتباطها لضمان الهوية بشأن كيان ما. وبالتالي، يتعين وجود شروط وإجراءات محددة جيداً لإدارة معرفات الهوية.

ومن بين المبادئ التوجيهية التي يتعين مراعاتها في عمليات تصميم وتنفيذ إدارة الهوية:

- وجود أنماط مختلفة لمعرفات الهوية تتسم بخصائص متباينة يتعين إدارتها. فمثلاً، قد تكون بعض معرفات الهوية عالمية (أي فريدة في جميع الاتحادات) أو أسماء مستعارة لها دلالتها داخل نظام ما أو معرف هوية للاستعمال مرة واحدة يكون له فترة صلاحية مؤقتة.
- قد يكون لمعرفات الهوية خصائص مختلفة تضفي بآثارها على الخصوصية فيما يتعلق بالحماية ضد الارتباط غير الملائم لأعمال المستعمل.

3.2.8 إدارة النعوت

نعوت الهوية عبارة عن واصفات للكيان، مثل نوع الكيان وعنوان بروتوكول الإنترنت المفضل والميدان ومعلومات العنوان ورقم الهاتف. وقد تحتوي النعوت كذلك على ادعاءات وحقوق وامتيازات وقوائم التفويض وبعض القيود الخاصة. وتضم الأنماط الأخرى من النعوت المعلومات الجاري تتبعها للكشف عن عمليات الاقتحام، مثل المحاولات الفاشلة للتأكد من الهوية وعدادات إعادة الإبراق وما إلى ذلك.

وتعتمد فعالية إدارة الهوية على ضمان النعوت التي يمكن ربطها وارتباطها لضمان هوية كيان ما. ويشمل ذلك تخزين النعوت وتوفيرها. ومن ثم يتعين وجود شروط وإجراءات معرفة جيداً لإدارة النعوت.

والنموذج عبارة عن نمط خاص من النعوت يمثل أي خاصية مصاحبة لسلوك كيان ما. ويمكن لأنظمة إدارة الهوية تخصيص معلومات النموذج استناداً إلى السمعة والمعاملات السابقة، وليس استناداً إلى ما يحدده الكيان ذاته. ومن أمثلة معلومات النموذج التي يمكن استعمالها لتقييم ضمان الهوية عناوين بروتوكول الإنترنت ونقطة النفاذ ومعلومات الموقع ووقت الاستعمال والأنظمة التي يتم النفاذ إليها. ويمكن للخواص الذكية أن تأخذ في اعتبارها كذلك الأحداث الحالية للتنبؤ بنماذج الاستعمال المستقبلية.

ومن بين المبادئ التوجيهية التي يتعين مراعاتها:

- يمكن اعتبار معلومات النموذج معلومات قابلة للتعريف الشخصي.
- شروط وإجراءات صارمة لإدارة معلومات النموذج.
- استعمال معلومات النموذج لتدنية سرقة الهويات.
- الامتثال لسياسات المعلومات القابلة للتعريف الشخصي.

4.2.8 إدارة الإثباتات

تستعمل الإثباتات لاستيقان هوية مدعاة. وتضم الإثباتات:

- اسم المستعمل/كلمات السر؛
- الشهادات الرقمية؛
- الأمارات الرمزية والبطاقات الذكية؛
- تلميحات أمنية؛
- معلومات تتعلق بالبنية التحتية للمفاتيح العمومية (PKI)، مثل المفاتيح والشهادات وسلطة توقيع الشهادات ومعلومات التجفير وما إلى ذلك؛
- السمات البيومترية.

وتشمل إدارة إثباتات الهوية الأنشطة التشغيلية الخاصة باستحداث وإصدار وإدارة معلومات تستعمل في استيقان ادعاءات الهوية. وتعتمد فعالية إدارة الهوية على عمليات إدارة الإثباتات وإجراءاتها وقدراتها. ومن ثم، يتعين وجود شروط وإجراءات محددة جيداً لإدارة الإثباتات.

وتشمل المبادئ التوجيهية الخاصة بإدارة الإثباتات:

- وضع سياسات خاصة بالإثباتات والحفاظ عليها؛
- عمليات وإجراءات لإدارة دورة حياة الإثباتات (تمت مناقشة مجموعة فرعية من إدارة دورة حياة الهوية في الفقرة 1.8)؛
- سياسات واتفاقات خدمة في بيئات تضم العديد من موردي الخدمات/الشبكات (التفاوض بشأن السياسات الخاصة بالإثباتات والامتثال لشروط الاتحاد ونشر المعلومات الخاصة بالإثباتات، مثل المفاتيح العمومية).

5.2.8 التدوين والتدقيق

تعتبر وظائف وقدرات التدوين والتدقيق مهمة لفعالية حلول إدارة الهوية. وتتضمن الأمثلة على التدابير الخاصة بالتدقيق والامتثال الحفاظ على سجلات أمنية تحقيقاً لشروط المسؤولية وحماية المعلومات الشخصية واستعمالها بشكل مناسب وموافاة الأنظمة والكيانات الملائمة (مثل مالكي الهويات) بالتبليغات.

ومن بين المبادئ التوجيهية الخاصة بالتدوين والتدقيق ما يلي:

- تدوين وتدقيق الأحداث المتعلقة بإدارة الهوية (مثل النفاذ إلى معلومات الهوية ومحاولات النفاذ غير المرخص والتحديثات على أختام التوقيتات وما إلى ذلك) لأغراض التحليلات القضائية؛
- آليات وإجراءات للتمكين من تتبع المنشأ؛
- الكشف عن عدم الامتثال للسياسات المطبقة؛
- ضمان المتطلبات التنظيمية الوطنية.

3.8 وظائف التشوير والتحكم لإدارة الهوية

1.3.8 مقدمة

تستعمل وظائف التشوير والتحكم لاكتشاف وتبادل معلومات الهوية الموثوقة (مثل معرفات الهوية والنعوت والادعاءات) المصاحبة لكيان (مثل مستعمل/مشترك، مجموعة، منظمة، عنصر شبكة، مورد خدمات) لدعم خدمات إدارة الهوية ووظائفها وقدراتها.

وتشرح هذه الفقرة وظائف التشوير والتحكم المتعلقة بإدارة الهوية.

2.3.8 اكتشاف معلومات الهوية

في بيئة متشعبة مثل بيئة شبكة الجيل التالي، قد توجد معلومات الهوية في عناصر مختلفة للشبكة (مثل مخدم الاشتراكات ومخدم الموقع ومخدم الحضور ومخدم الاشتراكات المترلية وما إلى ذلك). وتعد الوسائل البناءة لاكتشاف مصادر معلومات الهوية جزءاً لا يتجزأ من إدارة الهوية. وفي تطبيق للاستفادة من معلومات الهوية، يتعين الجزم بوجودها. وفي بيئة شبكة الجيل التالي الدينامية والمتطورة، يتوقع أن تتسم معلومات الهوية ومصادر هذه المعلومات بالدينامية أيضاً. وبالتالي، تحتاج الأطراف والكيانات المعولة إلى وسائل بناءة لمعرفة وجود معلومات الهوية واكتشافها. ويشمل ذلك أيضاً اكتشاف خدمات وظائف إدارة الهوية وقدراتها.

ومن بين المبادئ التوجيهية التي يتعين مراعاتها عند تحديد وتطبيق قدرات الاكتشاف:

- الاكتشاف داخل ميدان مورد شبكة الجيل التالي (داخل الشبكة الواحدة)؛
- الاكتشاف بين ميادين موردين مختلفين لشبكات الجيل التالي (فيما بين الشبكات)؛
- الاكتشاف بين أعضاء اتحاد. راجع الفقرة 2.4.8 (اكتشاف الاتحاد).

كما يشمل الاكتشاف القدرات الخاصة بالتوصل إلى مقدمي الهويات وتحديد مواقعهم. ويعد الاكتشاف ضرورياً في إطار إدارة الهوية الخاص بشبكات الجيل التالي نظراً لوجود العديد من مقدمي الهويات. وفي الحالات التي لا يوجد فيها إلا مقدم واحد للهوية (مؤسسة مثلاً)، لا توجد ضرورة لعملية الاكتشاف حيث سيكون معروفاً المكان الذي يتحصل منه على نعوت الهوية. وإضافة إلى ذلك، يمكن وجود أنظمة متعددة لتوفير مختلف وظائف إدارة الهوية ووظائف الاكتشاف المناسبة داخل شبكة مورد وحيد لشبكات الجيل التالي.

والاكتشاف عملية مشابهة للبحث في شبكة الويب بالنسبة لهوية ما. وتكون المدخلات لمحرك البحث عبارة عن خواص الهوية والخرج عبارة عن قائمة بمعرفات الهوية ومقدمي الهويات المطابقة للشروط. ويحتاج سيناريو الاستفهام والرد هذا نمطياً إلى أن يقوم مقدمو الهويات بتسجيل أنفسهم كموردين لخدمة هوية معينة لمستعمل/جهاز معين.

والأساليب المتاحة المستعملة في دعم الاحتياجات ذات الصلة بالنسبة للاكتشاف والنفاذ المرخصين تندرج مجازاً ضمن فئتين: 1) نُهُج جذر الجذور و/أو 2) الاكتشاف الاستنتاجي. ويعتمد الأول على قيام كيان ما بدور المسجل الأساسي لفراغات الأسماء عن طريق مخدم داعم فيما يعتمد النهج الثاني على قواعد واضحة يمكن بواسطتها الحصول باستمرار على عنوان أي مخدم داعم. ويمكن أيضاً استعمال خليط من النهجين.

3.3.8 اتصالات إدارة الهوية

يشمل ذلك القدرات والوظائف الخاصة باكتشاف وتبادل معلومات الهوية (مثل معرفات الهوية والإثباتات والنعوت المصاحبة لهوية كيان ما يقع ضمن أنظمة شبكية مختلفة (مثل تلك الموجودة في مخدم الاشتراكات ومخدم الموقع ومخدم الحضور وما إلى ذلك) ضمن شبكة مورد من موردي شبكات الجيل التالي بحيث يمكن ربط هذه المعلومات والتحقق منها (أي عن طريق مخدم تطبيق IdM يوفر وظائف الاستيقان والربط) لتوفير قدرات ضمان الهوية. ويمكن إرسال التأكيدات الخاصة بالهوية والنعوت المصاحبة (مثل الادعاءات والامتيازات) إلى الأنظمة المعولة (خدمات التطبيق مثلاً) لاتخاذ قرارات التحكم في النفاذ. ويسمح ذلك لخدمات تطبيقات مختلفة (أي منصات بائعين مختلفين) بالاستفادة من استعمال بنية تحتية مشتركة لإدارة الهوية خلافاً للحلول المنفصلة والمستقلة. ومن بين علاقات الاتصالات التي يتعين مراعاتها:

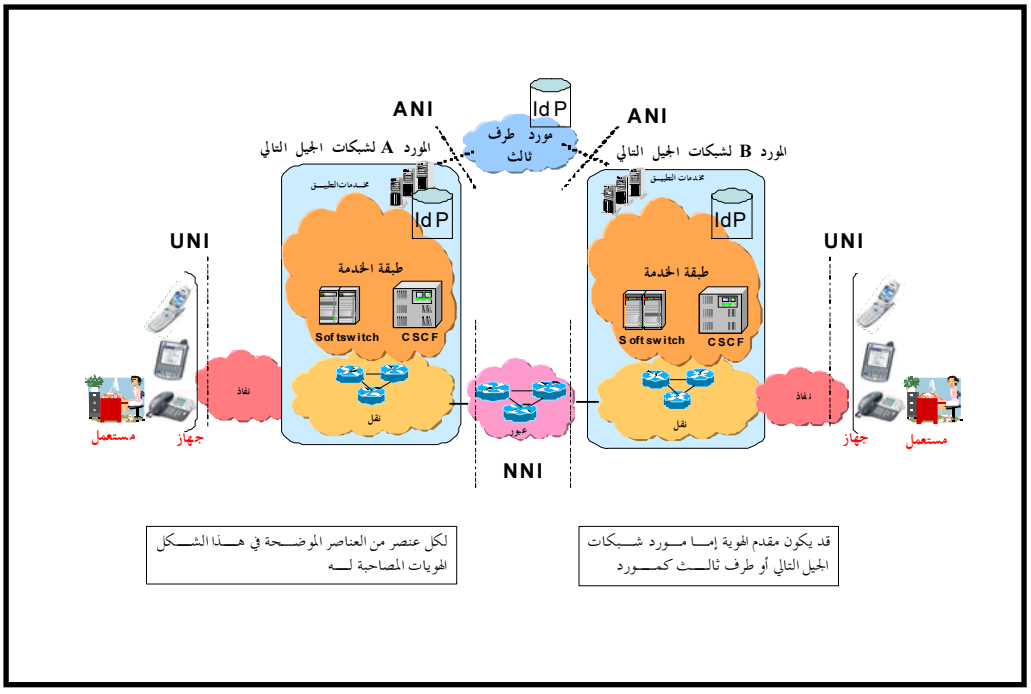
- داخل الشبكة الواحدة: اتصالات مع ميدان مورد شبكات الجيل التالي (بين عناصر الشبكة مثلاً)؛
- فيما بين الشبكات: اتصالات بين موردين مختلفين اثنين من موردي شبكات الجيل التالي؛
- اتحاد: اتصالات بين أعضاء اتحاد ما.

1.3.3.8 الاتصالات في الوقت الفعلي وقريباً من الوقت الفعلي

يتعين أن يراعى في الحل المستعمل في اكتشاف معلومات الهوية وتبادلها ما إذا كان المطلوب اتصالات في الوقت الفعلي أم قريباً من الوقت الفعلي. ويعتمد ذلك على التطبيقات المحددة التي يتم دعمها.

2.3.3.8 البروتوكولات والسطوح البينية للتشوير والتحكم

يبين الشكل 8 السطوح البينية الخارجية المطبقة لدعم اتصالات إدارة الهوية. على سبيل المثال، السطوح البينية المستعملة في تبادل معلومات الهوية أو التحكم في خدمات إدارة الهوية ووظائفها وقدراتها.



الشكل 8 – السطوح البينية الخارجية

وتشمل السطوح البينية الخارجية:

- السطح البيني من المستعمل إلى الشبكة (UNI)؛
- السطح البيني من التطبيق إلى الشبكة (ANI)؛
- السطح البيني من شبكة لأخرى (NNI).

وتعتمد المتطلبات والبروتوكولات المحددة التي يتعين استعمالها على السطح البيني المحدد والمعلومات التي يتعين تبادلها أو وظائف التحكم التي يجب القيام بها. وينبغي تحديد ووصف الخيارات والمظاهر الجانبية للمتطلبات والبروتوكولات التي يتعين استعمالها لتسهيل التشغيل البيني. وتعتمد الحلول الخاصة بالسطوح البينية على عوامل على غرار الحاجات المحددة للتطبيق والخدمات (مثل الوقت الفعلي إزاء شبه الوقت الفعلي) وحلول البروتوكولات (مثل بروتوكولات SAML وDiameter وRADIUS) والآليات والنُهُج (مثل التوصية [b-ITU-T X.509]، ومعمارية التغذية المرتدة العامة (GBA)).

وإضافة إلى السطوح البينية الخارجية، تعد السطوح البينية الداخلية مهمة أيضاً بالنسبة للحلول الشاملة. فداخل شبكة من شبكات الجيل التالي، يمكن وضع معلومات الهوية داخل عناصر وخدمات تطبيق مختلفة للشبكة (مثل مخدمات الاشتراكات والموقع والحضور وعناصر الشبكة الأخرى مثل وظيفة التحكم في دورة النداء ومراقب حدود الدورة). وتعتبر السطوح البينية الداخلية التي يتعين استعمالها في اكتشاف معلومات الهوية وتبادلها من الاعتبارات الهامة بالنسبة للتشغيل البيني بين بائعين متعددين.

3.3.3.8 الآليات والإجراءات

ينبغي تحديد وتوصيف الآليات والإجراءات المستعملة في تنفيذ وظيفة أو قدرة محددة من وظائف وقدرات إدارة الهوية. فمثلاً، ينبغي تحديد ووصف الآليات أو البروتوكولات المحددة ومكان وكيفية استعمالها. ومن أمثلة الآليات والبروتوكولات:

- لغة ترميز تأكيد الأمن (SAML)
- X.509
- معمارية التغذية المرتدة العامة (GBA)
- E.115

4.3.8 الربط والارتباط

يمكن ربط معلومات الهوية (مثل معرفات الهوية والإثباتات والنعوت) معاً لتكوين رباط لضمان هوية كيان ما. فعلى سبيل المثال، يمكن ربط معلومات الهوية المصاحبة لمشترك (مثل معرف هوية المستعمل) وجهاز مستعمل (مثل معرف هوية الجهاز) ومعلومات الموقع معاً لتكوين رباط لتوفير ضمان أكبر بالنسبة للمشترك.

ومن بين المبادئ التوجيهية التي يتعين مراعاتها عند تحديد وتنفيذ الربط والارتباط:

- إنفاذ السياسات المطبقة (مثل سياسات إغفال الهوية والخصوصية).

5.3.8 الاستيقان

الاستيقان هو عملية إضفاء الثقة على هوية كيان ما. ومن وسائل تحقيق ضمان الاستيقان وصف الأهداف والمبادئ التوجيهية اللازمة للتقدير الكمي للمخاطر المترتبة على ما يدعيه كيان ما بشأن من هو وماهيته. ويشمل ذلك تحديد أي من معرفات هوية الكيان هي الأكثر أهمية من الأخرى بالنسبة لعملية التعرف على الهوية ولماذا ينبغي ألا يكون لبعض معرفات الهوية المستعملة في الاستيقان نفس قيمة الاستيقان.

وتتحقق الثقة نمطياً من خلال إصدار أزواج معرفات الهوية للمستعمل وكلمات السر بالنسبة للأنظمة الإفرادية. ومع ذلك، لا يُحبذ هذا النهج في شبكات الجيل التالي، حيث إنه غير فعال تشغيلياً ويمكن أن يؤدي إلى ممارسات غير مأمونة. ومن بين المبادئ التوجيهية التي يتعين مراعاتها عند تحديد وتنفيذ الاستيقان:

- سرية وسلامة آليات الاستيقان؛
- وجود إثباتات قوية بما يكفي للوثوق بها عبر الأنظمة جميعها.

6.3.8 ضمان الاستيقان

ضمان الاستيقان هو عملية إضفاء الثقة في الهويات والادعاءات المقدمة لنظام معلومات. وينبغي ألا تعامل جميع المعلومات المستعملة لأغراض الاستيقان نفس المعاملة ولا ينبغي بالضرورة أن يكون لها نفس قيمة الضمان. فمثلاً، تختلف الثقة في الاستيقان باستخدام السمات البيومترية كثيراً عن الاستيقان باستخدام معرف هوية المستعمل/كلمات السر. ويلزم تخصيص قيمة نسبية لكل معرف هوية استناداً إلى مبادئ أساسية من أجل التقدير الكمي للثقة بأن الكيان المستيقن هو الكيان الصالح.

والهدف من ضمان الاستيقان هو التقدير الكمي للأخطار المترتبة على ما يدعيه كيان ما بشأن من هو وماهيته. ولا تعامل جميع معرفات الهوية المستعملة في عملية تقرير الاستيقان نفس المعاملة ولا يتعين أن يكون لها بالضرورة نفس قيمة الاستيقان. وبالإضافة إلى ذلك، ونتيجة لأن يصبح خطأ الاستيقان أكثر خطورة، ينبغي زيادة مستوى الاستيقان المطلوب طبقاً لآثار المخاطر (مثل الطبيعة الحرجة للأثر) الناجمة عن خطأ الاستيقان.

وتتيح آلية التقدير الكمي لضمان الاستيقان وإرساله للأطراف المعولة اتخاذ قرارات فيما يتعلق بثقتها في عملية الاستيقان المستعملة للتحقق من صلاحية هوية أو إدعاءات خاصة بكيان ما.

وتشمل الفوائد الأولية لضمان الاستيقان القدرة على تحديد مستوى الثقة بأن كيان ما هو ما يدعيه خلال دورة حياة الهوية بالكامل. والمعايير القياسية لتخصيص وتبادل قيم الضمان النسبية لعمليات الاستيقان وآلياته وبياناته (مثل كلمات السر والإثباتات والسمات البيومترية) عبر اتحادات مختلفة من الأمور الحاسمة لدعم الخدمات الاتحادية وحماية الأمن السيبراني.

وينبغي لعمليات ضمان الاستيقان أن تأخذ في الاعتبار الآتي بعد:

- آلية الاستيقان: تعد كلمات السر الاستاتيكية أضعف من كلمات السر الخاصة بالاستخدام لمرة واحدة والأمارات الرمزية العتادية ذات أرقام الهوية الشخصية (PIN) أفضل بوجه عام من البرمجية منها.
- بروتوكول الاستيقان: بروتوكول معروف أنه مؤمن ضد الهجمات التي يقوم بها دخلاء خلال الاتصالات، أو بروتوكول يقوم على عمليات تجفير تعتبر قوية بوجه عام.
- خصائص الجهاز المستعمل في الاستيقان: تعتمد ثقة الاستيقان جزئياً على خصائص الجهاز الذي يستعمله المستعمل، هل هو جهاز حاسوب من الأجهزة المتداولة تجارياً تمتلكه وتتحكم فيه المنظمة، أم جهاز مخصص مقاوم للعبث به وهو ما يعد أفضل من جهاز تجاري متيسر النفاذ إليه من الجميع.
- موقع الكيان الجاري الاستيقان منه: ينبغي مراعاة موقع المستعمل، هل هو داخل منطقة منظمة ما مثلاً أم في كشك في مكان عام، أحد مقاهي الإنترنت أو ما شابه. وتكون ثقة الاستيقان أعلى إذا كان من الصعب بالنسبة لجهاز مطراف عمومي موجود في كشك إقناع مخدم الاستيقان بأنه موجود ضمن الحدود المادية لمنظمة ما.
- مسار الاتصالات: يضم الاستيقان عادة مسار اتصالات (شبكات لاسلكية، خطوط تجارية مؤجرة وما إلى ذلك) بين الكيان الجاري الاستيقان منه والمخدم الذي يوفر الاستيقان و/أو قرارات النفاذ. ومن الضروري إرسال المعلومات المستعملة في الاستيقان إلى مخدم الاستيقان بشكل موثوق وألا تكون عرضة للعبث من قبل المهاجمين.
- السهولة النسبية في إجراء الاستيقان عن طريق سلوك خادع: من المهم تقييم المخطر المرتبطة بانتهاك مفاتيح التجفير.

7.3.8 التفويض

يشمل التفويض الإجراءات والعمليات الخاصة بنقل امتيازات القيام بعمل معين نيابة عن كيان رئيسي من كيان يملك هذه الامتيازات عبر كيان آخر لا يملكها.

فعلى سبيل المثال، تبدأ سلطة التفويض بالقدرة على تحديد أي الحسابات يمكنها إجراء بعض الأعمال الإدارية (مثل إنشاء حسابات جديدة) أو يمكنها إدارة وظائف محددة (مثل تغيير كلمة السر الخاصة بحساب ما). ولذا، فإنه بالنسبة للقدرة على التفويض بأعمال أو جهود الإدارة، يتمثل الهدف بعد ذلك في توفير بيئة يتم فيها إجراء هذا العمل بصورة مؤمنة ومسؤولة.

8.3.8 إنفاذ السياسات

ينبغي أن يراعى في تصميم وتنفيذ حلول إدارة الهوية أن السياسات المطبقة يتم إنفاذها. فمثلاً، يرتبط إنفاذ السياسات عادة بالجوانب التالية:

- إغفال الهوية والخصوصية؛
- توليد معلومات الهوية وجمعها؛
- استعمال معلومات الهوية ونشرها.

9.3.8 دعم الخدمات التي تحتاج إلى أولوية في المعاملة

ينبغي أن يراعى في تصميم وتنفيذ حلول إدارة الهوية دعم خدمات التطبيق ودورات الاتصالات التي تحتاج إلى أولوية في المعاملة مثل خدمة اتصالات الطوارئ (ETS). فعلى سبيل المثال، ينبغي لأي معاملات مع أنظمة إدارة الهوية لتحديد دورات اتصالات خدمة اتصالات الطوارئ والحفاظ عليها، أن تعامل بأولوية. راجع التوصيتين [b-ITU-T E.107] و[b-ITU-T Y.2205] للحصول على معلومات عن الخدمات والقدرات التي تتطلب أولوية في المعاملة.

4.8 وظائف إدارة الهوية لهوية اتحادية

1.4.8 الهوية الاتحادية

المفهوم العام للاتحاد هو أن يُتاح لكل عضو في الاتحاد فرصة البقاء مستقلاً مع تسهيل التشارك في معلومات هوية محددة للسماح بالخدمات الاتحادية. فمثلاً، يمكن لبعض معلومات الهوية الخاصة بمستعمل/مشترك (مثل مجموعة فرعية من المظهر الجانبي لمشترك) أن تتسم بالاتحادية (أي تكون متاحة لأعضاء الاتحاد).

2.4.8 اكتشاف الاتحاد

يشمل اكتشاف الاتحاد الوظائف والآليات الخاصة باكتشاف وتبادل معلومات الهوية الاتحادية. فمثلاً، يمكن لبعض معلومات الهوية المتعلقة بمستعمل/مشترك أن تأخذ صفة الاتحادية مثل مجموعة فرعية من المظهر الجانبي للمشترك.

ويتمثل الجانب الرئيسي في اكتشاف الاتحاد في تحديد أو اكتشاف مقدم هوية صالح أو مقدم هوية يكون هو المصدر المخول بالنسبة لمعلومات هوية معينة مصاحبة لكيان ما (مثل معلومات الموقع).

وعملية الاكتشاف ضرورية في أي معمارية يوجد فيها مقدمي هويات متعددين أو يكون موقع مقدمي الهويات بالنسبة إليها دينامياً. وفي الحالات التي يوجد فيها مقدم هوية واحد فقط (مؤسسة، مثلاً)، لا توجد حاجة إلى عملية الاكتشاف، وذلك لأن أي طرف معول/مورد خدمة يمكنه أن يحدد بوضوح من أين يحصل على معلومات هوية الكيان.

3.4.8 التجسير والتشغيل البيني

يمكن، بوجه عام، أن يكون لكل مورد من موردي شبكات الجيل التالي، أو مؤسسة أو عضو في اتحاد الأنساق أو المخططات أو التعاريف أو الدلالات الخاصة به لتمثيل وتبادل البيانات والمعلومات المتعلقة بالهوية. فعلى سبيل المثال، يمكن تمثيل المعلومة الواحدة، مثل تاريخ الميلاد، بشكل مختلف من جانب نظامين مختلفين. كما أن الدلالات والمخططات والآليات المستعملة في طلب المعلومات المتعلقة بالهوية وتبادلها يمكن أن تختلف أيضاً، مما يؤدي إلى ظهور مشكلات بالنسبة للتشغيل البيني. وبالتالي، من الضروري وجود قدرات ملائمة تسمح بالتجسير والتشغيل البيني بين الاتحادات المختلفة.

5.8 وظائف إدارة الهوية الخاصة بالمستعمل والمشترك

من أجل حلول فعالة بالنسبة لإدارة الهوية، يتعين وجود وظائف تسمح للمستعمل النهائي/المشترك بتقديم معلومات فيما يتعلق بالتحكم في معلومات الهوية الخاصة به. وتشمل هذه الوظائف وظائف وقدرات من شأنها تمكين كيان ما كمستعمل

نهائي/مشترك من موافاة موردي الخدمات ومقدمي الهويات بمعلومات عن الشروط والقيود والموافقات والتراخيص بالنسبة لتوليد معلومات الهوية الخاصة به وجمعها واستعمالها ونشرها.

وتتعلق هذه الوظائف بإنفاذ السياسات المطبقة، مثل السياسات المتعلقة بحماية المعلومات القابلة للتعريف الشخصي وإغفال الهوية ومعلومات الهوية المستعارة.

ومن المبادئ التوجيهية التي يتعين مراعاتها:

- وسائل للمستعملين النهائيين/المشتركين لنقل المعلومات إلى مورد شبكات الجيل التالي عن التحكم في معلومات الهوية الخاصة بهم؛
- الامتثال للسياسات المطبقة فيما يتعلق بحماية المعلومات القابلة للتعريف الشخصي؛
- سهولة الاستعمال بالنسبة للمستعمل النهائي/المشترك.

6.8 الأداء والاعتمادية

1.6.8 الأداء

تستعمل قدرات إدارة الهوية ووظائفها في دعم وتعزيز نطاق واسع من تطبيقات الأعمال التجارية والتطبيقات الأمنية. فعلى سبيل المثال، يمكن استعمال وظائف إدارة الهوية لضمان هوية كيانات الاتصالات قبل السماح ببدء دورة اتصالات (مثل دورات نقل الصوت عبر بروتوكول الإنترنت أو التلفزيون القائم على بروتوكول الإنترنت أو البيانات). وبالتالي، فإن تداعيات الأداء لإدارة الهوية على خدمات التطبيقات ذات المستوى الأرفع (مثل دورات نقل الصوت عبر بروتوكول الإنترنت أو التلفزيون القائم على بروتوكول الإنترنت أو البيانات) التي يجري دعمها لها أهميتها بالنسبة للفعالية الكلية للحل. فمثلاً، ينبغي ألا تؤثر إدارة الهوية بالسلب على تطبيقات الخدمات ذات المستوى الأرفع التي يجري دعمها بما يؤثر على مجمل جودة الخدمة (QoS) وجودة الخبرة (QoE) للمستعملين النهائيين/المشتركين.

واعتبارات إدارة الأداء مهمة عند تصميم حلول إدارة الهوية. وتشمل إدارة الأداء جمع البيانات الإحصائية وتحليلها لأغراض مراقبة الأداء. ومراقبة الأداء عبارة عن تقييم نظامي لقدرة نظام الشبكة على تنفيذ الوظيفة المخصصة له، وذلك عن طريق الاستمرار في جمع بيانات الأداء الملائمة وتحليلها. وإجراءات مراقبة الأداء مصممة بحيث تقوم بالتقاط ظروف الأخطاء المتقطعة وأوجه الخلل الناتجة عن التلف التدريجي في معدات الشبكة. وتمكن تقنيات الصيانة الاستباقية التي على شاكلة مراقبة الأداء من الكشف المبكر عن أوجه الخلل قبل أن تتفاقم خطورتها.

2.6.8 دقة أختام التوقيت

تعتبر دقة أختام التوقيت أحد عوامل إدارة الهوية. ويصف التدقيق وقوع الأحداث ضمن الجداول الزمنية هذه. و تعد أختام التوقيت ضرورية لأغراض التدقيق؛ وتتحدد جودة إن لم يكن استعمال بيانات التدقيق من عدمه طبقاً لدقة أختام التوقيت.

وتتحدد دقة أختام التوقيت عن طريق ثلاثة عوامل – الدقة التي تُقرأ بها الميقاتية المحلية لخاتم التوقيت ومدى قابلية تتبع الميقاتية المحلية وصولاً إلى ميقاتية مرجعية وعدم اليقين الرياضي في الميقاتية المحلية مقاساً بدلالة مرجع.

3.6.8 الاعتمادية والتيسر

من الجوانب المهمة في تصميم وتنفيذ حلول إدارة الهوية اعتمادية ومرونة عناصر وأنظمة الشبكة التي توفر وظائف إدارة الهوية وقدراتها، وذلك لأن إدارة الهوية ستستعمل في دعم وتعزيز نطاق واسع من تطبيقات الأعمال التجارية والتطبيقات الأمنية التي قد يكون لها شروط محددة بشأن التيسر. ومن ثم، يتعين مراعاة شروط ومبادئ توجيهية بالنسبة لعوامل الاعتمادية كالواردة أدناه:

- تصميمات الأنظمة (مثل الإطناب) من أجل المتانة والمرونة في التكيف؛
- التنوع (مثل التنوع الجغرافي) من أجل التيسر.

وينبغي، إضافة إلى ذلك، أيضاً أن يراعى في تصميم وتنفيذ حلول إدارة الهوية وجود تدابير ضد الأعطال. فعلى سبيل المثال، يمكن للتطبيق المعول أن يسمح ببعض الامتيازات المحدودة إذا ما كان نظام إدارة الهوية بأكمله عاطلاً أو أصبح غير متيسر.

7.8 أمن إدارة الهوية

1.7.8 الحماية الأمنية لعناصر الشبكة التي توفر إدارة الهوية

نظراً إلى أن معلومات الهوية ومواردها تعد قيمة وحساسة وتستعمل في دعم تطبيقات وخدمات الأعمال التجارية، فإن عناصر الشبكة التي توفر خدمات إدارة الهوية ووظائفها وقدراتها تكون هدفاً للهجمات الأمنية ومن ثم تحتاج إلى حماية أمنية.

ومن الضروري وجود شروط وتدابير لتأمين وحماية عناصر وأنظمة الشبكة التي توفر وظائف إدارة الهوية وخدماتها وقدراتها. ومن أمثلة هذه الاعتبارات الأمنية:

- حماية أمنية لخدمات إدارة الهوية ووظائفها وقدراتها؛
- حماية أمنية للسطوح البينية للتشوير والاتصالات؛
- حماية أمنية للسطوح البينية لإدارة أنظمة إدارة الهوية (أي السطوح البينية المستعملة في تشكيل وإدارة معلومات الهوية).

2.7.8 حماية المعلومات القابلة للتعريف الشخصي (PII)

تعد حماية المعلومات القابلة للتعريف الشخصي من الجوانب شديدة الأهمية بالنسبة لإدارة الهوية. وينبغي تحديد وتنفيذ قدرات محددة لحماية المعلومات القابلة للتعريف الشخصي. ويتعلق ذلك بإنفاذ السياسات المطبقة على حماية المعلومات القابلة للتعريف الشخصي، وذلك رهناً باللوائح الوطنية والإقليمية. ومن بين الوظائف والقدرات التي يتعين مراعاتها:

- قدرات للمستعملين/المشتركين لتوصيل ما يفضلونه بالنسبة للمعلومات القابلة للتعريف الشخصي؛
- قدرات لتوفير الشفافية (أي قدرات للتأكد من أن الكيانات المخولة فقط هي التي يمكنها النفاذ إلى المعلومات القابلة للتعريف الشخصي والاطلاع عليها)؛
- قدرات لتوفير إرشادات تتعلق بنشر واستعمال معلومات الهوية.

بيبليوغرافيا

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

[b-ITU-T E.115] Recommendation ITU-T E.115 (2008), *Computerized directory assistance*.

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

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

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

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 1081-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

[b-ITU-T X.911] Recommendation ITU-T X.911 (2005) | ISO/IEC 15414:2006, *Information technology – Open distributed processing – Reference model – Enterprise language.*

[b-ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

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

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

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

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

[b-ITU-T Y.2205] Recommendation ITU-T Y.2205 (2008), *Next Generation Networks – Emergency telecommunications – Technical considerations*.

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

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

[b-ETSI EG 202 072] ETSI EG 202 072, V1.1.1 (2002), *Universal Communications identifier (UCI); Placing UCI in context; Review and analysis of existing identification schemes*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=14108>

[b-ETSI EG 202 236] ETSI EG 202 236, V1.1.1 (2003), *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON)*; *Design guide; Use of non-numeric names*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=17732>

[b-ETSI EG 284 004] ETSI EG 284 004, V1.1.2 (2007), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Incorporating Universal Communications Identifier (UCI) support into the specification of Next Generation Networks*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=21139>

[b-ETSI TS 102 042] ETSI TS 102 042, V1.3.4 (2007), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=27736>

[b-RFC 3650] IETF RFC 3650 (2003), *Handle System Overview*.
<http://www.ietf.org/rfc/rfc3650.txt?number=3650>

[b-NIST] NIST SP800-63, v6.3.3, *Electronic Authentication Guidelines.*
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

[b-OGIM] The Open Group, *Identity Management White Paper* (03/2004).
<http://www.opengroup.org/bookstore/catalog/w041.htm>

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

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

طُبعت في سويسرا
جنيف، 2009