الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1252

(2021/04)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

مصطلحات وتعاريف أساسية تتعلق بإدارة الهوية

التوصية ITU-T X.1252

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	X.1140–X.1149
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	**X.1250–X.1279**
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1360–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1389
أمن تكنولوجيا السجلات الموزعة	X.1400–X.1429
أمن سجل الحسابات الموزع	X.1430–X.1449
البروتوكول الأمني (2)	X.1450–X.1459
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
أمن شبكات الجيل الخامس	X.1800–X.1819

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

مصطلحات وتعاريف أساسية تتعلق بإدارة الهوية

ملخص

تعرِّف التوصية ITU-T X.1252 المصطلحات الأساسية المستعملة في إدارة الهوية (IdM). وهذه المصطلحات مستقاة من مصادر كثيرة ولكنها جميعاً شائعة الاستعمال في أعمال إدارة الهوية. وليس المقصود من التوصية ITU-T X.1252 أن تكون بمثابة خلاصة وافية ضخمة للمصطلحات المتعلقة بإدارة الهوية. بيد أن المصطلحات المعرفة في هذه التوصية تقتصر على التي يعتبر أنها تمثل خط الأساس لأكثر المصطلحات الخاصة بإدارة الهوية من حيث الأهمية وشيوع الاستعمال. وتتضمن التوصية ITU-T X.1252 ملحقاً يوضح الأساس المنطقي لبعض من هذه المصطلحات الأساسية.

ومن بين أهداف التوصية ITU-T X.1252 النهوض بفهم مشترك لهذه المصطلحات بين المجموعات القائمة حالياً (أو التي تخطط) بوضع المعايير المتعلقة بإدارة الهوية. وتم وضع التعاريف بحيث تكون مستقلة، بأقصى قدر ممكن، عن عمليات التنفيذ أو عن أي سياق محدد، وبالتالي تكون مناسبة لكي تمثل التعاريف الأساسية لأي عمل من أعمال إدارة الهوية. ومن المسلم به أنه في بعض الحالات والسياقات، قد يلزم وجود تفصيل أكبر لمصطلح معين، وفي هذه الحالة، يمكن النظر في صياغة التعريف الأساسي.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1252	2010-04-16	17	11.1002/1000/10440
2.0	ITU-T X.1252	2021-04-30	17	11.1002/1000/14642

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة 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 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظة

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 "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" 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 البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1252

مصطلحات وتعاريف أساسية تتعلق بإدارة الهوية

1 مجال التطبيق

تعرِّف هذه التوصية مجموعة أساسية من المصطلحات التي يشيع استعمالها في إدارة الهوية (IdM). وتعاريف المصطلحات هذه هي تعاريف أساسية، أي يراد لها أن تنقل المعنى الأساسي على الرغم من أنه يمكن في حالات استثنائية إضافة ملاحظة عندما تساعد في إيضاح التعريف. ويرد في الملحق A الأساس المنطقي لبعض المصطلحات والتعاريف الأساسية.

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

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.

لا توجد.

3 التعاريف

يرد سرد المصطلحات والتعاريف المجمعة لإدارة الهوية (IdM) في الفقرة 6.

4 المختصَرات والمختزَلات

تستعمل هذه التوصية المختصَرات والمختزَلات التالية:

CID المعرف التجفيري *(Cryptographic Identifier)*

DDO واصف كائن معرِّف الهوية اللامركزي *(DID Object Descriptor)*

DID معرِّف الهوية اللامركزي *(Decentralized Identifier)*

DLT تكنولوجيا سجل الحسابات الموزع *(Distributed Ledger Technology)*

ID المعرِّف *(Identifier)*

IdM إدارة الهوية *(Identity Management)*

IdP مورّد الهوية *(Identity Provider)*

IdSP مورّد خدمة الهوية *(Identity Service Provider)*

IH محور الهوية *(Identity Hub)*

PII المعلومات المحددة لهوية شخص *(Personally Identifiable information)*

PKI البنية التحتية للمفاتيح العمومية *(Public Key Infrastructure)*

RA سلطة التسجيل *(Registration Authority)*

RE الكيان الطالب *(Requesting Entity)*

RP الطرف المعول *(Relying Party)*

SIM وحدة هوية المشترك *(Subscriber Identity Module)*

SSI هوية السيادة الذاتية *(Self-Sovereign Identity)*

URL محدد مواقع الموارد الموحد *(Uniform Resource Locator)*

ZKP إثبات المعرفة دون الإفصاح عن المعلومة *(Zero-Knowledge Proof)*

5 الاصطلاحات

لا توجد.

6 المصطلحات والتعاريف

1.6 التحكم في النفاذ (access control): إجراء يمكن به للمدير تقييد النفاذ إلى موارد أو مرافق أو خدمات أو معلومات استناداً إلى ما هو محدد مسبقاً من قواعد وحقوق معينة أو إلى سلطة يتمتع بها الطرف الطالب.

2.6 العنوان (address): يعرف العنوان نقطة انتهائية محددة للشبكة ويمكن استعماله لأغراض التسيير إلى هذه النقطة الانتهائية المادية والمنطقية داخل شبكة عمومية أو خاصة.

ملاحظة – على أساس التوصية [b-ITU-T E.101].

3.6 وكيل (agent): كيان يتصرف نيابةً عن كيان آخر.

4.6 تحالف (alliance): اتفاق بين اثنين أو أكثر من الكيانات المستقلة يحدد كيفية التعامل فيما بينهم وكيفية القيام بأنشطة معاً.

5.6 اسم مُغْفَل (anonym): معرِّف يستخدم مرة واحدة بالضبط.

6.6 إغفال الهوية (anonymity): حالة تعذر تحديد هوية كيان ضمن مجموعة من الكيانات.

ملاحظة – يمكن أن يحول إغفال الهوية دون تتبع الكيانات وتحديد مصدرها وتحليل خصائصها أو سلوكها، من قبيل موقعها ووتيرة استعمالها للخدمة.

7.6 مزعم (assertion): بيان أدلى به كيان دون إرفاقه بدليل على صحته.

ملاحظة – من المتفق عليه أن مصطلحي مزعم وادعاء يتشابهان كثيراً.

8.6 ضمان (assurance)

ملاحظة – انظر ضمان الاستيقان وضمان الهوية.

9.6 مستوى الضمان (assurance level): مستوى الثقة في الربط بين كيان ومعلومات الهوية المقدمة.

10.6 نعت (attribute): معلومات مرتبطة بكيان تحدد خاصيته.

11.6 نمط النعت (attribute type) [b-ITU-T X.501]: ذلك المكون من النعت الذي يبيّن صنف المعلومات الذي يعطيه النعت.

12.6 قيمة النعت (attribute value) [b-ITU-T X.501]: حالة معيّنة من صنف المعلومات يبيّنها نمط النعت.

13.6 استيقان (authentication) [b-ISO/IEC 24760-1]: عملية تحقق رسمية تؤدي، في حال نجاحها، إلى هوية مستيقَنة لكيان.

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

14.6 ضمان الاستيقان (authentication assurance): إقرار إيجابي في عملية الاستيقان يهدف إلى تقديم الثقة بأن الشريك الذي يجري الاتصال معه هو الكيان الذي يدّعي كونه أو يُتوقع كونه.

ملاحظة – يستند الضمان إلى درجة الثقة في العلاقة بين الكيان المتصل والهوية المقدمة.

15.6 تخويل (authorization): منح الحقوق، وعلى أساس هذه الحقوق، السماح بالنفاذ.

ملاحظة – على أساس التوصية [b-ITU-T X.800].

16.6 إسناد (binding): مصاحبة أو رابطة أو صلة صريحة وثابتة.

17.6 تعرف بيومتري؛ المقاييس البيومترية (biometric recognition; biometrics) [b-ISO/IEC 2382-37]: التعرّف المؤتمت على الأفراد على أساس مراقبة الخصائص السلوكية والبيولوجية.

18.6 شهادة (certificate): مجموعة من البيانات ذات الصلة بالأمن صادرة عن سلطة أمنية أو طرف ثالث موثوق، إلى جانب معلومات أمنية تُستعمل لتوفر للبيانات السلامة وخدمات استيقان مصدر البيانات.

ملاحظة – على أساس تعريف "شهادة الأمن" في التوصية [b-ITU-T X.810].

19.6 ادعاء (claim) [*اسم*]: زعم رقمي بشأن نعوت الهوية التي قدمها كيان عن نفسه أو عن كيان آخر. [*الفعل*] القول بأن الأمر كذا، دون التمكن من تقديم إثبات.

ملاحظة – من المتفق عليه أن مصطلحي مزعم وادعاء يتشابهان كثيراً.

20.6 المدّعي (claimant): كيان أو ممثل كيان أساس لأغراض الاستيقان.

الملاحظة 1 – يتضمن المدعي الوظائف اللازمة للمشاركة في تبادل الاستيقان نيابةً عن الأساس.

الملاحظة 2 – على أساس التوصية [b-ITU-T X.811].

21.6 تعريف الادعاء (claim definition): تعريف تمكن قراءته آلياً للبنية الدلالية للادعاء.

ملاحظة – تسهل تعاريف الادعاء إمكانية التشغيل البيني للادعاءات والإثباتات عبر العديد من الجهات القائمة بالإصدار والمستحوذين والأطراف المعوِّلة.

22.6 سياق (context): البيئة محددة الحدود التي توجد فيها الكيانات وتتفاعل.

23.6 تلازُم (correlation): توليفة من أجزاء مختلفة من المعلومات التي ترتبط بكيان أو تصبح مرتبطة بكيان عند جمعها معاً.

ملاحظة – التلازُم وثيق الصلة بتحديد الهوية. ويمكن أن يسهل التلازُم تحديد الهوية واستدلال معلومات عن كيان لا تقدمها البيانات المعطاة مباشرة.

24.6 بيانات الاعتماد (credential): مجموعة بيانات تقدم كدليل على هوية و/أو استحقاقات مزعومة.

ملاحظة – يرد في المرجع [b-ISO/IEC 29115] نص مشابه لنص التوصية [b-ITU-T X.1254] ويحتوي على نفس تعريف بيانات الاعتماد الذي وضعته الأفرقة المعنية.

25.6 تقليل البيانات إلى الحد الأدنى (data minimization): تقييد جمع وتخزين واستخدام المعرفات والنعوت والبيانات الأخرى المرتبطة بالكيان بما هو ضروري فقط لإجراء الاستيقان وقصر أي تبادل وكشف للبيانات المرتبطة بالكيان، بما في ذلك المعلومات السياقية لطلب، على ما هو ضروري فقط للرد على الطلب وعلى الطرف المعوِّل المرتبط بالطلب فقط.

26.6 معرف هوية لامركزي (Decentralized identifier) (DID): معرف هوية متفرد عالمياً لا يتطلب سلطة تسجيل مركزية لأنه مسجل بتكنولوجيا سجل الحسابات الموزَّع أو بشكل آخر من الأنظمة اللامركزية. ويرتبط معرف الهوية اللامركزي مع واصف واحد لكائنه (DID) بالضبط.

ملاحظة – انظر المرجع [b-W3C-DID].

27.6 وثيقة معرف هوية لامركزي (DID object descriptor (DDO)): مجموعة من البيانات التي تصف الجهة المعنية بمعرف الهوية اللامركزي (DID)، بما في ذلك الآليات مثل المفاتيح العمومية التجفيرية، التي يمكن للجهة المعنية بالمعرف DID أو الجهة المنتدَبة من المعرف DID أن تستخدمها لاستيقان نفسها وإثبات ارتباطها بالمعرف DID.

28.6 تفويض (delegation): الإجراء الخاص بإسناد سلطة أو مسؤولية أو وظيفة لكيان آخر.

29.6 هوية رقمية (digital identity): تمثيل رقمي لمعلومات معروفة عن فرد أو مجموعة أو منظمة على وجه التحديد.

30.6 سجل الحسابات الموزَّع (distributed ledger) [b-ITU-T X.1400]: سجل الحسابات الموزَّع هو نوع من السجلات يمكن تناقله واستنساخه ومزامنته بطريقة موزَّعة لامركزية.

31.6 نظام إدارة المفاتيح اللامركزي (decentralized key management system): معيار لإدارة مفاتيح تجفيرية قابلة للتشغيل البيني على أساس معرف الهوية اللامركزي.

32.6 ميدان (domain): بيئة يمكن للكيان فيها استخدام مجموعة من النعوت لتحديد الهوية ولأغراض أخرى.

ملاحظة – الميدان يقدم السياق.

33.6 انتساب (enrolment): عملية تنصيب كيان في سياق. وقد يشمل الانتساب التحقق من هوية الكيان وإنشاء هوية سياقية.

الملاحظة 1 – قد يشمل الانتساب التحقق من هوية الكيان وتحديد هوية سياقية.

الملاحظة 2 – الانتساب أيضاً شرط مسبق للتسجيل. وفي كثير من الحالات، يُستعمل التسجيل لوصف كلتا العمليتين.

34.6 كيان (entity): شيء له وجود قائم بذاته ومميز ويمكن تعريفه في سياق.

الملاحظة 1 – يمكن أن يكون للكيان تجسيد مادي أو منطقي.

الملاحظة 2 – 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.

35.6 استيقان كيان (entity authentication): عملية للتحقق ولتحقيق ثقة كافية في الربط بين الكيان والهوية المقدَمة.

ملاحظة – يؤخذ استعمال مصطلح استيقان في سياق إدارة الهوية على أنه يعني استيقان كيان.

36.6 اتحاد (federation) [b-ITU-T Y.2720]: إقامة علاقة بين كيانين أو أكثر أو رابطة تضم أي عدد من موردي الخدمات وموردي الهوية.

37.6 المستحوِذ (holder): كيان أصدرت له جهة قائمة بالإصدار ادعاءً. وإذا دعم الادعاء إثباتات المعرفة دون الإفصاح عن المعلومة (ZKP)، فإن المستحوِذ هو أيضاً جهة الإثبات.

38.6 تحديد الهوية (identification) [b-ISO/IEC 24760-1]: عملية تبيّن كياناً في ميدان معين متميزاً عن الكيانات الأخرى.

39.6 معرف الهوية (ID) [b-ITU-T E.101]: سلسلة من الأرقام والسمات والرموز المستعملة لكي تعرف بشكل منفرد هوية مشترك أو مستعمل أو عنصر شبكة أو وظيفة أو كيان من كيانات الشبكة أو خدمة أو تطبيق. ويمكن استعمال معرفات الهوية لأغراض التسجيل أو التخويل. وقد تكون هذه المعرفات عامة لجميع الشبكات أو خاصة لشبكة معينة (لا تُكشف معرفات الهوية الخاصة لأطراف ثالثة).

ملاحظة – يمكن أن يكون معرف الهوية نعتاً أنشئ خصيصاً بقيمة مخصصة ليكون فريداً ضمن ميدان.

40.6 هوية (identity): تمثيل كيان في شكل واحد أو أكثر من النعوت التي تتيح تمييز الكيان أو الكيانات بالقدر الكافي ضمن سياق. ولأغراض إدارة الهوية، يُفهم مصطلح هوية كهوية سياقية (مجموعة فرعية من النعوت)، أي تُحَدّ المجموعة المتنوعة من النعوت بإطار ذي حدود محددة (سياق) يوجد فيه الكيان ويتفاعل.

ملاحظة – يُمثَّل كل كيان بهوية واحدة شاملة تضم جميع عناصر المعلومات المحتملة التي تميز ذلك الكيان (النعوت). بيد أن هذه الهوية الشاملة هي قضية نظرية عصية على أي وصف واستعمال عملي لأن العدد الكلي لجميع النعوت المحتملة لا حصر له.

41.6 ضمان الهوية (identity assurance): الثقة المتاحة في عملية التحقق والتأكد من الهوية التي يُلجأ إليها للتثبت من هوية الكيان الذي تصدر أوراق الاعتماد له، ودرجة الثقة بأن الكيان الذي يستعمل أوراق الاعتماد هو الكيان الذي أُصدرت أو خُصصت أوراق الاعتماد له.

42.6 سياسة أمنية قائمة على الهوية (identity-based security policy) [b-ITU-T X.800]: سياسة أمنية قائمة على هويات و/أو نعوت المستعملين أو مجموعة المستعملين أو الكيانات العاملة نيابةً عن المستعملين والموارد/الأغراض الجاري النفاذ إليها.

43.6 إدارة الهوية (identity management) (IdM): مجموعة من الوظائف والمقدرات (مثل عمليات الإدارة والصيانة والكشف وتبادل الاتصالات والربط والإسناد وإنفاذ السياسة والاستيقان والمزاعم) التي تستعمل لأغراض ضمان معلومات الهوية (من قبيل المعرفات وأوراق الاعتماد والنعوت)؛ وضمان هوية كيان ودعم تطبيقات الأعمال التجارية والأمن.

ملاحظة – على أساس التوصية [b-ITU-T Y.2720].

44.6 مالك الهوية (Identity Owner): كيان يمكن تحميله المسؤولية. ويجب أن يكون مالك الهوية إما فرداً أو مؤسسة. وهو على النقيض مع الشيء.

45.6 نمط الهوية (identity pattern): تعبير هيكلي عن نعوت كيان (مثل سلوك الكيان) يمكن استعماله في بعض عمليات تحديد الهوية.

46.6 تدقيق الهوية (identity proofing) [b-ISO/IEC 29115]: عملية تلتقط من خلالها سلطة التسجيل (RA) معلومات كافية لتعريف الكيان بمستوى ضمان موصَّف أو مفهوم وتتحقق منها.

47.6 مورّد الهوية (identity provider (IdP))

ملاحظة – انظر مورّد خدمة الهوية (IdSP).

48.6 مورّد جسر خدمة الهوية (identity service bridge provider): مورّد خدمة هوية (IdSP) يقوم بدور وسيط موثوق بين موردي خدمة هوية آخرين.

49.6 مورّد خدمة الهوية (identity service provider (IdSP)): كيان يقوم بالتحقق من معلومات هويات الكيانات الأخرى مع الحفاظ عليها وإدارتها، ويمكن أن يستحدثها ويخصصها.

50.6 تحقق من الهوية (identity verification): عملية التأكد من صحة هوية مزعومة بمقارنة الادعاءات المقدمة عن الهوية بمعلومات مثْبَتة سابقاً.

51.6 المستقل (independent): الفرد الذي يتحكم مباشرةً فيما يلزم من المفتاح الخاص (المفاتيح الخاصة) والمفتاح السري الرئيسي (المفاتيح السرية الرئيسية) لإدارة هوية لامركزية.

52.6 فرد (individual): صاحب الهوية وهو شخص طبيعي. وهو على النقيض مع المنظمة.

53.6 جهة الإصدار (issuer): الجهة التي تصدر ادعاء.

54.6 مفتاح جهة الإصدار (issuer Key): النوع الخاص من المفتاح التجفيري اللازم للجهة القائمة بالإصدار لإصدار ادعاء يدعم إثباتات المعرفة دون الإفصاح عن المعلومة (ZKP).

55.6 سلسلة المفاتيح (key-chain): مهمة تأمين تخزين المفاتيح أو البيانات الخاصة على وحدة موثوقة من عتاد أي جهاز.

56.6 الهوية القانونية (legal identity): مجموعة من المعلومات الكافية لتحديد مالك الهوية لغرض المساءلة القانونية في ولاية قضائية واحدة على الأقل. ولأغراض الشبكة المؤقتة، يمكن إنشاء الهوية القانونية بالإحالة إلى واحد أو أكثر من موارد الإنترنت المتاحة للعموم مثل المواقع أو المدونات الإلكترونية أو ملفات تعريف الشبكة الاجتماعية أو صفحات الويب الأخرى التي تقدم معلومات كافية لتلبية هذا الاختبار.

57.6 إمكانية إقامة الصلات (Linkability): القدرة على التمييز، ضمن مجموعة من المعلومات، ما إذا كان اثنان أو أكثر من النعوت أو المعرفات أو الهويات أو البيانات الأخرى مرتبطة بدرجة عالية من الاحتمال لتكون مفيدة.

58.6 مظهر (manifestation): تمثيل لكيان ملحوظ أو مكتشف (أي ليس مزعوماً ذاتياً).

ملاحظة – (قارن مع مزعم).

59.6 استيقان متبادل (mutual authentication) [b-ISO/IEC 29115]: استيقان هويتي كيانين يقدم لكلا الكيانين ضماناً لهوية كل منهما.

60.6 الاسم (name): الاسم عبارة عن توليفة من السمات ويستعمل لتعريف الكيانات (مثل المشتركين وعناصر الشبكة) والتي يمكن حلها أو ترجمتها إلى عنوان. وقد تتضمن السمات أرقاماً وحروفاً ورموزاً.

الملاحظة 1 – يستعمل الاسم في سياق ما ولا يمكن ضمان كونه متفرداً أو لا يلفه الغموض ولأغراض التسيير يمكن تحليله أو ترجمته إلى عنوان.

الملاحظة 2 – على أساس التوصية [b-ITU-T E.101].

61.6 عدم التنصل (non-repudiation): القدرة على الحماية من إنكار أحد الكيانات المشاركة في إجراء ما مشاركته في الإجراء كله أو في جزء منه.

62.6 نمط (pattern)

ملاحظة – انظر نمط الهوية.

63.6 ثابت (persistent): أي قائم ويمكن استعماله في خدمات بمعزل عن التحكم المباشر لصاحب التكليف المبادر، وبدون حد زمني مذكور.

64.6 معلومات محددة لهوية شخص (personally identifiable information (PII)): أي معلومات أ) تعرف أو يمكن استعمالها في التعرف على الشخص الذي تخصه هذه المعلومات أو الاتصال به أو تحديد موقعه؛ ب) أو يمكن من خلالها الحصول على معلومات التعرف على شخص أو بيانات اتصاله؛ أو ج) تكون مرتبطة أو يمكن ربطها بشخص طبيعي بطريقة مباشرة أو غير مباشرة.

65.6 أساس (principal): كيان يمكن استيقان هويته.

ملاحظة – يرد هذا القيد في التوصيات [b-ITU-T X.811] و[b-ITU-T Y.2702] و[b-ITU-T Y.2720].

66.6 سياسة الخصوصيات (privacy policy): سياسة ترسي متطلبات حماية النفاذ إلى معلومات محددة لهوية شخص (PII) ونشرها، وحقوق الأفراد فيما يتعلق بكيفية استعمال المعلومات الشخصية الخاصة بهم.

67.6 المفتاح الخاص (private key) [b-ITU-T X.509]: (في نظام تجفير مفتاح عمومي)، هو المفتاح الذي لا يعرفه إلا الكيان فقط من زوج المفاتيح المخصص للكيان.

68.6 امتياز (privilege): حق في حال منحه يسمح لكيان القيام بعمل ما.

69.6 إثبات (proof): تحقق تجفيري من ادعاء. والتوقيع الرقمي هو شكل بسيط من أشكال الإثبات. والاختزال التجفيري هو أيضاً شكل من أشكال الإثبات. وللإثباتات نوعان: شفاف أو دون الإفصاح عن المعلومة. وتكشف الإثباتات الشفافة جميع المعلومات الواردة في الادعاء. بينما يتيح إثبات ZKP الكشف الانتقائي للمعلومات الواردة في الادعاء.

70.6 جهة الإثبات (prover): الكيان الذي يصدر إثباتاً من الادعاء. وجهة الإثبات هي أيضاً المستحوذ على الادعاء.

71.6 اسم مستعار (pseudonym) [b-ISO/IEC 24760-1]: معرّف هوية يحتوي على الحد الأدنى من معلومات الهوية بما يكفي للسماح للمتحقق بتثبيته كصلة وصل بهوية معروفة.

الملاحظة 1 – يمكن أن يكون الاسم المستعار معرّف هوية بقيمة يختارها الشخص أو تخصَص عشوائياً.

الملاحظة 2 – يمكن استعمال الاسم المستعار لتفادي أو التقليل من المخاطر المتعلقة بالخصوصية المرتبطة باستعمال إسنادات معرف الهوية التي يمكن أن تكشف عن هوية الكيان.

72.6 بيانات عمومية (public data) [b-ITU-T L.1410]: البيانات المتاحة للعموم دون تقييد النفاذ بمتطلبات العضوية أو اتفاقات عدم الإفصاح أو قيود مماثلة.

73.6 مفتاح عمومي (public key) [b-ITU-T X.509]: هذا المفتاح من زوج مفاتيح الكيان المعروف للعموم.

74.6 ملف تعريف عمومي (public profile): المعلومات التي تصف مورِّد خدمة، بما في ذلك هويته القانونية أو شعاره (شعاراته) أو علاماته التجارية الأخرى وموقعه (مواقعه) ومعلوماته التسويقية وروابط الويب الخاصة به وأي معلومات أخرى يتطلبها إطار الثقة لضمان الشفافية الكاملة بشان الهوية القانونية للمورِّد ومؤهلاته.

75.6 تسجيل (registration): عملية يطلب فيها كيان امتيازات لاستعمال خدمة أو مورد، ويُخصَص بها.

ملاحظة – الانتساب شرط مسبق للتسجيل. ويمكن دمج وظيفتي الانتساب والتسجيل أو الفصل بينهما.

76.6 الطرف المعوِّل (relying party (RP)): كيان يعوِّل على تقديم هوية أو ادعائها من جانب كيان طالب/زاعم ضمن سياق طلب ما.

ملاحظة – على أساس التوصية [b-ITU-T Y.2720].

77.6 تنصل (repudiation): إنكار أحد الكيانات المشاركة في إجراء ما مشاركته في الإجراء كله أو في جزء منه.

78.6 كيان طالب (requesting entity (RE)): كيان يقوم بتقديم هوية أو ادعائها لطرف معوّل ضمن سياق طلب ما.

79.6 إلغاء (revocation): قيام شخص مخول بإلغاء شيء تم القيام به سابقاً.

80.6 دور (role): مجموعة خصائص أو نعوت تصف المقدرات أو الوظائف التي يمكن لكيان القيام بها.

ملاحظة – يمكن لكل كيان تولي أدوار عديدة أو القيام بها. والقدرات قد تكون متأصلة أو مخصصة.

81.6 تدقيق أمني (security audit) [b-ITU-T X.800]: استعراض مستقل وفحص لسجلات النظام وأنشطته بغية اختبار مدى كفاية ضوابط النظام، ولضمان الامتثال للسياسات والإجراءات التشغيلية المعمول بها، ولكشف الخروقات الأمنية، وللتوصية بأي تغييرات ضرورية في الضوابط والسياسات والإجراءات.

82.6 ميدان الأمن (security domain): مجموعة عناصر وسياسة أمن وسلطة أمن ومجموعة أنشطة ذات صلة بالأمن تدار فيها العناصر وفقاً للسياسة العامة للأمن.

ملاحظة – على أساس التوصية [b-ITU-T X.810]. وترد تعاريف مشابهة في التوصيتين [b-ITU-T Y.2701] و[b-ITU-T Y.2720].

83.6 منطقة أمن (security zone): منطقة محمية تتسم بالتحكم التشغيلي والموقع والتوصيلية بعناصر الأجهزة أو الشبكات الأخرى.

ملاحظة – على أساس التوصية [b-ITU-T Y.2701].

84.6 سلطة ميدان الأمن (security domain authority) [b-ITU-T X.810]: سلطة أمن تتولى مسؤولية تنفيذ سياسة أمنية لميدان الأمن.

85.6 هوية مزعومة ذاتياً (self-asserted identity): هوية يعلن الكيان أنها تخصه.

86.6 الشيء (thing): كيان لا تمكن محاسبته قانوناً. وقد يكون الشيء حيواناً (من قبيل حيوان أليف، أو ماشية)، أو كائناً طبيعياً (من قبيل منزل، سيارة، هاتف)، أو كائناً رقمياً (من قبيل برنامج برمجيات، خدمة شبكة، هيكل بيانات). وهو على النقيض مع صاحب الهوية.

87.6 الثقة (trust): وثوق طرف أو كيان بأن طرفاً أو كياناً آخر سيتصرف بطريقة محددة جيداً لا تنتهك القواعد أو السياسات أو البنود القانونية المتفق عليها لنظام إدارة الهوية.

88.6 مصدر الثقة (trust Anchor): مالك الهوية الذي قد يكون بمثابة نقطة انطلاق في شبكة الثقة اللامركزية. ويتمتع مصدر الثقة بامتيازين فريدين:

- إضافة مالكي هوية جدد إلى الشبكة،
- إصدار دعوات مصدر الثقة.

ويجب أن يستوفي مصدر الثقة مؤهلات مصدر الثقة ويوافق على التزامات مصدر الثقة المحددة في إطار الثقة. وجميع أمناء الثقة والمضيفين هم تلقائياً مصادر ثقة.

89.6 إطار ثقة (Trust Framework): مجموعة من المواصفات والقواعد والاتفاقات القابلة للإنفاذ قانوناً تحكم نظام من أنظمة الهوية.

ملاحظة – على أساس المرجع [b-OIX-TFIS].

90.6 طرف ثالث موثوق (trusted third party): في سياق سياسة أمنية ما، هو سلطة أمن، أو وكيل لها، موثوق بها فيما يتعلق ببعض الأنشطة المتصلة بالأمن.

الملاحظة 1 – على أساس التوصيتين [b-ITU-T X.810] و[b-ITU-T Y.2702].

الملاحظة 2 – انظر التوصية [b-ITU-T X.800].

91.6 مستوى الثقة (trust level): مقياس متسق، يوفر قياساً كمياً، لمدى ما يعتد به من خصال أو قدرة أو قوة أو صدق لدى شخص أو أمر ما.

92.6 مستعمِل (user): أي كيان يستفيد من مورد، مثل نظام أو معدات أو مطراف أو تطبيق أو شبكة مشاع.

93.6 نظام متمحور حول المستعمل (user-centric): نظام إدارة هوية يوفر للمستعمل القدرة على التحكم في، وإنفاذ، مختلف السياسات الناظمة لبيانات المستعمل، بما فيها المعلومات المحددة لهوية شخص.

94.6 عقدة التحقق من الصحة (validator node): عقدة تتحقق من صحة المعاملات الجديدة لسجلات الهوية وتنشط بكتابة المعاملات الصالحة إلى سجل الحسابات باستخدام بروتوكول توافق سجل الحسابات.

95.6 ادعاء يمكن التحقق منه (verifiable claim): ادعاء يتضمن إثباتاً من جهة الإصدار. وعادةً ما يكون هذا الإثبات في شكل توقيع رقمي. ويمكن التحقق من ادعاء يتسنى التحقق منه بواسطة مفتاح عمومي مرتبط بمعرِّف هوية لامركزي (DID) يعود لجهة الإصدار.

ملاحظة – على أساس المرجع [b-W3C-VC].

96.6 تحقق (verification) [b-ISO/IEC 24760-1]: عملية التثبت من أن معلومات الهوية المرتبطة بكيان معين صحيحة.

الملاحظة 1 – تطبق عملية تعرُّف الهوية التحقق على النعوت المدعاة أو المرصودة.

الملاحظة 2 – قد تشمل عملية التحقق من معلومات الهوية التحري عن صلاحية هذه المعلومات ومصدرها الصحيح وأنها المعلومات الأصلية (لم يتم تغييرها) ومدى صحتها وإسنادها إلى الكيان وما إلى ذلك.

الملاحظة 3 – المعلومات صحيحة في وقت التحقق.

97.6 جهة التحقق (verifier) [b-ISO/IEC 24760-1]: كيان يقوم بالتحقق.

98.6 محفظة (محفظة هويات) (identity wallet) (wallet)): تطبيق يمكن المستعمل في الأساس من الاحتفاظ بمعرفات هوية وبيانات الاعتماد بتخزين المفاتيح الخاصة المقابلة على جهاز المستعمل.

99.6 إثبات المعرفة دون الإفصاح عن المعلومة (Zero knowledge proof (ZKP)): إثبات يستخدم تجفيراً خاصاً أو مفتاحاً سرياً رئيسياً للسماح بكشف انتقائي عن المعلومات في مجموعة من الادعاءات. وهذا الإثبات يثبت أن بعض البيانات أو كل البيانات المتضمنة في مجموعة ادعاءات حقيقية دون الكشف عن أي معلومات إضافية، بما في ذلك هوية جهة الإثبات.

الملاحظة 1 – مفهوم "الكشف الانتقائي" يعني مجموعة واسعة من خيارات الكشف. فعلى سبيل المثال، يمكن استخدام إثباتات ZKP لإثبات العديد من الادعاءات بشأن البيانات المكتومة مثل: (1) سن الرشد، دون الكشف عن تاريخ الميلاد؛ (2) الملاءة المالية (عدم الإفلاس)، دون إظهار تكوين المحفظة؛ (3) ملكية الأصل دون الكشف أو الارتباط بمعاملات سابقة.

الملاحظة 2 – على أساس التوصية [b-ITU-T X.1403].

الملحق A

النقاط الرئيسية والأساس المنطقي للمصطلحات الأساسية لإدارة الهوية

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية.)

معلومات أساسية

بيّنت المناقشات الدائرة حول إدارة الهوية اختلافات في فهم الناس لمقاصد إدارة الهوية وللإجراءات الأساسية المتبعة، وتعاريف المصطلحات. وأدت هذه الاختلافات إلى سوء فهم ومناقشات مطولة خلال عملية تقييس إدارة الهوية.

وللمساعدة على تجنب سوء التفاهم هذا مستقبلاً، يسجل هذا الملحق بعض الاتفاقات التي تم التوصل إليها أثناء مناقشات قطاع تقييس الاتصالات بشأن هذه المفاهيم والمصطلحات الأساسية، ويساعد على تفسير الأفكار التي أفضت إلى وضع المصطلحات الواردة في هذه التوصية (أو إلى اعتمادها في بعض الحالات). ويرجى الانتباه إلى أن هذا الملحق لا يصف أو يشرح منظوراً شمولياً لإدارة الهوية.

مقدمة

الهوية هي المصطلح الذي تدور حوله سائر المصطلحات الأخرى الخاصة بإدارة الهوية. ففي العالم الفعلي مثلاً، على غير العالم الرقمي، تُقبل هوية شخص طبيعي بلا عناء على أساس مجموعة واسعة من الخصائص أو النعوت. فبعضها ملامح جسدية من قبيل الطول ولون الشعر والمظهر العام والسمات المميزة والسلوك. كما يمكن استعمال بعضها الآخر كتاريخ ومكان الميلاد وعنوان المنزل ورقم الهاتف. وفي عملية اتصالات، يتطلب كلا الطرفان عادة ما يكفي من الثقة في أنهما يتواصلان مع الشريك الصحيح. وكثيراً ما تنطوي عملية السعي لنيل الثقة على اثنين أو أكثر من الأفراد أو "الكيانات". فالكيان الذي يتعين تأكيد هويته هو الكيان الطالب (RE)، بينما الكيان الذي يعول على هوية مؤكدة هو الطرف المعوِّل. وقد يشارك كيان ثالث ليدير الهويات، وهو مورِّد خدمة الهوية.

وفي العالم الرقمي أو العالم "على الخط"، تتكون "الهوية" من نعوت أيضاً، شأنها شأن العالم الفعلي تماماً. بيد أنها في الحالة يمكن أن تقتصر على سمة واحدة أو أن تتسم بسمات عديدة؛ تبعاً للسياق الذي ترد فيه. وهذا ينطبق على الجماد وكذلك على الأشخاص الطبيعيين. لذا، كثيراً ما تُخلع على المستعملين صفة كيان.

وعموماً، تميّز معرفات الهوية (ID) أو النعوت ما ينفرد به كيان دون غيره في سياق معين. لذلك، يمكن أن يكون لكيان عدد من الهويات المختلفة يشكل بعضها مجموعة فرعية من هويات أخرى.

1.A الاستيقان والثقة

تشكل عملية الاستيقان جزءاً رئيسياً من إدارة الهوية. وتساعد هذه الفقرة على شرح عملية الاستيقان وصلتها بالثقة.

علماً بأنه عند ترجمة هذا النموذج إلى إجراءات وتطبيقات حقيقية، يُتطلب الوضوح بشأن الشركاء المعنيين بالاتصالات وبشأن سلاسل الثقة الواجبة التطبيق.

ويمكن وصف عملية الاستيقان على النحو التالي.

تتطلب معظم عمليات الاتصالات أن يكون لدى الشركاء على جانبي الاتصالات قدر كاف من الثقة أو الائتمان بأنهم يتواصلون حقاً مع الشريك المقصود. ومن ثم، يسعى الشركاء، في مستهل اتصال، للوصول إلى مستوى كافٍ من الثقة على أساس المعلومات المتاحة عن هوية الشريك، أي الثقة في الربط القائم بين الكيان والهوية المقدمة.

وتتسم عملية إرساء الثقة بأهمية خاصة عندما تباعد المسافات بين شركاء يتواصلون عبر وصلة اتصالات لا غير. فتُنفَّذ عملية الاستيقان للتثبت بدرجة كافية من الثقة من أن الهوية التي يقدمها شريك الاتصال هي هويته حقاً.

وتنطوي الاتصالات دوماً على اثنين أو أكثر من شركاء متمايزين يتبادلون معلومات. ونظراً لاتساع المجموعة المتنوعة من الشركاء المحتملين (مثل البشر والأشياء)، تدعو الحاجة لوضع مصطلح عام. فوقع الاختيار على مصطلح *كيان* الذي يُعرَّف على أنه: شيء ما له وجود قائم بذاته ومميز ويمكن تعريفه في سياق.

الملاحظة 1 – يمكن أن يكون للكيان تجسيد مادي أو منطقي.

الملاحظة 2 – 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.

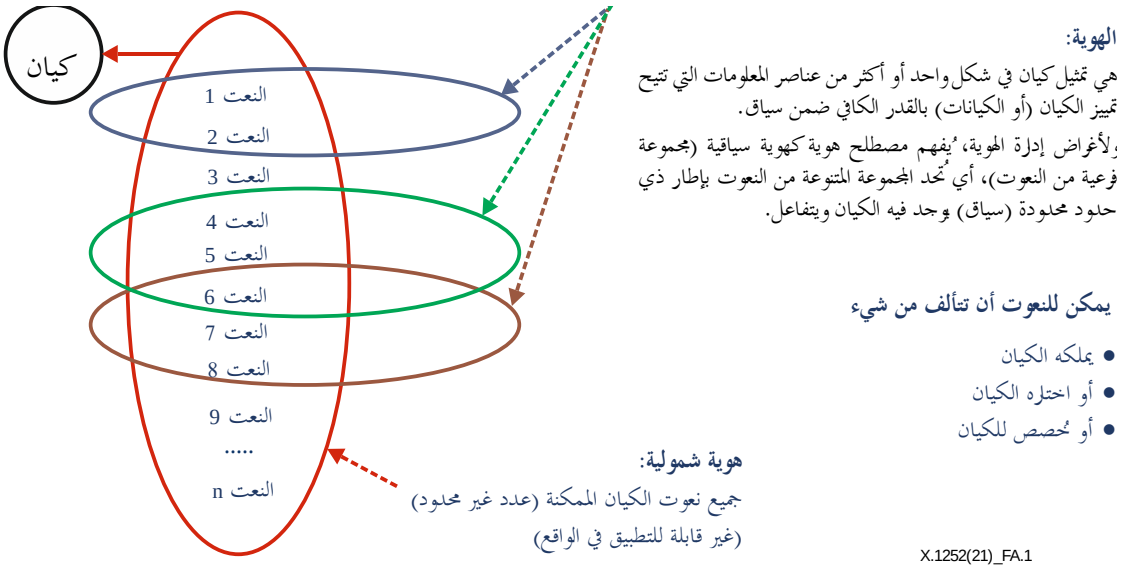
ويمكن استعمال المعلومات لتحديد هوية كيان استناداً إلى نعوت الكيان. ويُعرَّف النعت على النحو التالي: هو معلومات مرتبطة بكيان تحدد خاصيته. ومن الناحية العملية، يقوم تحديد هوية كيان عادةً على مجموعة فرعية من نعوته، باعتبار أن تحديد الهوية محدود بما يدعى السياق الذي يوجد فيه الكيان ويتفاعل. فكلما ضاق السياق واتضحت الظروف الحدية السائدة، قلّ عدد النعوت اللازمة لتحديد الهوية. ويعرَّف السياق على أنه: البيئة محددة الحدود التي توجد فيها الكيانات وتتفاعل.

ولأن تعريف كيان يقوم على أساس القدرة على تحديد هويته، فمن الضروري أن يكون هناك تعريف مناسب لتحديد الهوية: فهو عملية التعرف على كيان في ميدان معين دوناً عن الكيانات الأخرى.

وللتمييز بين الكيانات، يكفي استعمال مجموعة فرعية من النعوت المناسبة للسياق. ويشار إلى ذلك *بالهوية* التي تعرّف بأنها: تمثيل كيان في شكل واحد أو أكثر من النعوت التي تتيح تمييز الكيان أو الكيانات بالقدر الكافي ضمن سياق. ولأغراض إدارة الهوية، يُفهم مصطلح هوية كهوية سياقية (مجموعة فرعية من النعوت)، أي تُحَدّ المجموعة المتنوعة من النعوت بإطار ذي حدود محددة (السياق) يوجد فيه الكيان ويتفاعل.

ويمكن أن تكون الهوية مجموعة فرعية من هوية أخرى. وقد تكون هناك تقاطعات في الهويات أيضاً. ولكن، ولأسباب متنوعة (كالمخاوف بشأن انتهاك الخصوصية)، فإن تقاطعات الهويات المستعمَلة لأغراض مختلفة أو في سياقات مختلفة، ربما تُعدّ غير مرغوبة صراحةً، أو حتى تُستبعد.

ويُظهر الشكل 1.A العلاقات بين الكيان والهويات والنعوت.



الشكل 1.A – العلاقات بين الكيان والهويات والنعوت

وكما ذُكر سابقاً، فإن للاستيقان صلة بإدارة الهوية. فهو العملية اللازمة لتحقيق قدر كاف من الثقة في أن الاتصال جارٍ مع الشريك المقصود. وسيعتمد المستوى الفعلي للثقة اللازمة على مدى حساسية التطبيق أو مخاطر الضرر اللاحق جراء الانخراط في اتصال مع الشريك الخطأ.

ويمكن تخصيص الحقوق والامتيازات لأغراض شتى، ومن بينها:

- تقاسم أو إيصال معلومات لا يراد لها أن تكون متاحة للجميع؛
- إتاحة النفاذ إلى:
  - معلومات،
  - غرف أو مناطق أو ميادين،
  - خدمات،
  - استعمال الموارد؛
- إبرام عقود.

ويتطلب اكتساب مثل هذه الثقة إمكانية التمييز الواضح لشريك الاتصالات عن غيره من شركاء الاتصالات المحتملين، وإمكانية إعادة تقييم هذا التمييز دورياً، عند اللزوم.

وبصفة عامة، تجرى عملية تحقيق الثقة هذه، أي عملية الاستيقان، بصورة متبادلة. وهذا يعني أن عملية الاستيقان، على النحو المبين في الشكل 2.A، تُنجَز مرتين بحيث يؤدي كلُّ كيان كلَّ دور، أي:

استيقان Y: يتصرف الكيان Y ككيان طالب (RE)، فيما يتصرف الكيان X كطرف معوِّل (RP).

استيقان X: يتصرف الكيان X ككيان طالب، فيما يتصرف الكيان Y كطرف معوِّل.

وتبسيطاً للموضوع وتسهيلاً للفهم، توصف عملية الاستيقان المبيّنة في الشكل 2.A في اتجاه واحد فقط. ومع ذلك، تتشابك انسيابات هاتين العمليتين.

فالتنفيذ المتشابك يتيح للطرفين التحقق من الشروط المسبقة قبل تقديم نعوت قد يراد التكتم عليها. ويمكن لمثل هذه الشروط أن تكون كالآتي:

- معرفة كيفية مخاطبة الطرف المعول،
- ثقة كافية في أن الطرف المعول هو الطرف الصحيح (على سبيل المثال: ينبغي أن يكون لدى المستعملين بعض الثقة في أنهم على صفحة الويب الصحيحة قبل أن يُدخلوا معلومات الهوية كاسم المستعمل وكلمة المرور).

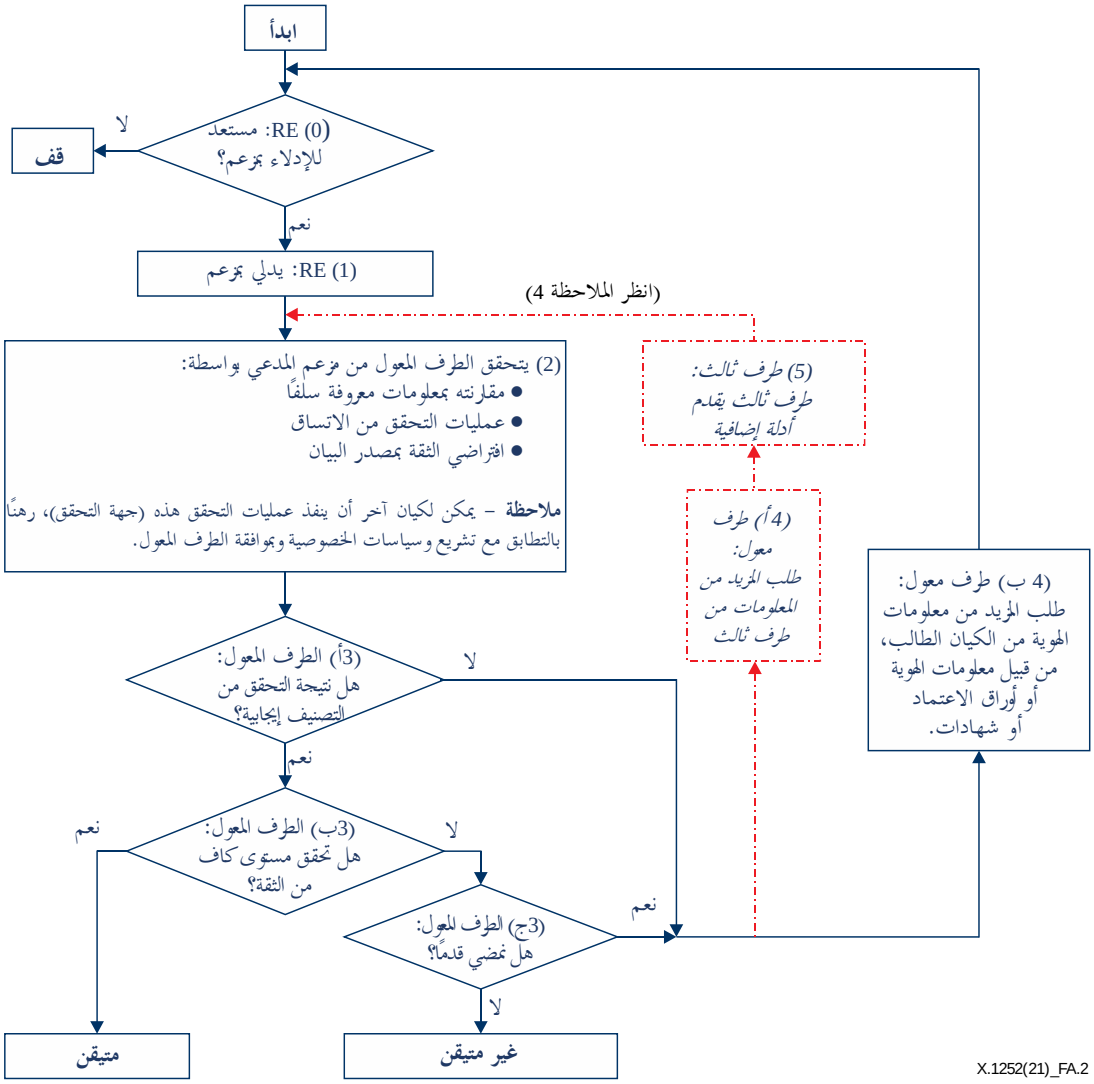
في بعض الحالات (ولكن ليس في الأنظمة المتمحورة حول المستعمل)، يمكن إشراك طرف ثالث مباشرةً ليقدم المزيد من المعلومات كأدلة للطرف المعول بغية تعزيز الثقة في نعوت الكيان الطالب.

وتتألف الهويات من نعوت يمكن أن تكون شيئاً:

- يملكه الكيان (مثل بطاقة شفرة)؛
- أو يعرفه الكيان (مثل كلمة مرور)؛
- أو من صفات الكيان (مثل لونه أو مقاسه)؛
- أو يمكن للكيان القيام به (مثل تجفير معين)؛
- أو يقع فيه الكيان؛
- أو مجموعة من تلك الأشياء.

ويمكن التحقق من الهويات بواسطة:

- اتساق المعلومات نفسها؛
- والاتساق مع غيرها من المعلومات الداعمة؛
- ومقارنتها بمعلومات معروفة سلفاً.



الملاحظة 1 – يبين هذا الشكل عملية استيقان أساسية أحادية الاتجاه.
وتنفذ هذه العملية عمومًا بصورة متبادلة على التوازي و/أو التشابك.
الملاحظة 2 – يمكن الاستغناء عن الخطوة 2 إذا لم يُطلب مستوى ثقة.
الملاحظة 3 – يمكن تنفيذ هذا المخطط الانسيابي مرات عديدة، كما يمكن فصل هذه التكرارات في الزمان و/أو المكان.
الملاحظة 4 – تخضع مشاركة طرف ثالث لتشريع وسياسات الخصوصية وموافقة الكيان الطالب. (- - - - - - -).

الشكل 2.A – عملية الاستيقان أحادية الاتجاه

كما يمكن تحديد النعوت بدلالة نمط الهوية وهو تعبير هيكلي عن نعوت كيان (مثل سلوك الكيان) يمكن استعماله في بعض عمليات تحديد الهوية.

ولاحظ بصورة خاصة ما يبينه مثال المخطط الانسيابي في الشكل 2.A من أن قرار قبول الكيان الطالب من عدمه يعود دوماً إلى الطرف المعول استناداً إلى عملية الاستيقان. وما من جهة أخرى يمكنها اتخاذ هذا القرار.

وعلى وجه العموم، ينبغي أن يكون بوسع كل شريك في اتصال أن يحدد مستوى الثقة اللازم للسماح بتنفيذ الامتيازات. سوى أن هذا الحق يمكن أن يكون محدوداً، وفي بعض الحالات، يجب أن يحدَد تشريعياً.

وحيث يكون هناك تفاوت كبير بين شريكي الاتصال، ثمة خطر محدد في أن يستغل الشريك الأقوى هذا الوضع ويتطلب مستوىً من الثقة غير عالٍ بما يكفي أو يرفض استيقان هويته. من الضروري إذن أن تقوم التطبيقات التقنية لآليات الاستيقان على آليات متناظرة منعاً لهيمنة طرف واحد، ودرءاً لاستعمال وضع مهيمن على غير وجه حق في حالات غير متكافئة.

وعند تطبيق إدارة الهوية، بصفة عامة، من الضروري أن نكون واضحين جداً حول الكيانات المعنية والغرض منها حتى يتسنى حصر السياق والهويات (مجموعة النعوت) في غرض معين.

وبالنسبة لمستوى الثقة فيما يتعلق بأغراض الاتصالات الصرفة، يكفي عادةً أن يكون العميل على ثقة مناسبة بكونه موصولاً مع مورّد النقل أو الخدمة المقصود، وأن يكون الموردون على ثقة من أن استعمال الخدمات مسموح وأنه يمكن إرسال فواتير لقاء هذه الخدمات وينبغي سدادها. ويمكن تحقيق الشطر الأخير باستيقان نقطة نفاذ أو حساب مشترك مثلاً، مما لا يحتاج لأن يتطابق مع المستعمل الفعلي للخدمة أو يحيل إليه. وفي بعض الحالات، كما في بطاقات الهاتف أو بطاقات وحدة هوية المشترك (SIM) المدفوعة مسبقاً، لا ضرورة للاستيقان.

ويمكن تقديم أوراق اعتماد في عملية الاستيقان كدليل على بعض أو كل نعوت الهوية السياقية المقدمة. وتعرَّف أوراق الاعتماد على أنها: مجموعة بيانات تقدم كدليل على هوية و/أو استحقاقات مزعومة. ولكن من الضروري التمييز بوضوح بين نمطين من أوراق الاعتماد:

1) مجموعة من البيانات المقدمة كدليل على هوية مزعومة، وهي مهمة لأغراض الاستيقان (جواز سفر مثلاً). ويُستعمل هذا النمط من أوراق الاعتماد لتعزيز الثقة في النعوت عبر تأكيد من الطرف الذي أصدر أوراق الاعتماد.

2) مجموعة من البيانات المقدمة كدليل على استحقاقات وهي مهمة لأغراض التخويل فحسب (ومثالها، تذكرة لحضور حفل موسيقي أو مباراة كرة قدم). وهي تسمح بممارسة امتياز (من قبيل التمكن من حضور حدث ما على أساس حيازة تذكرة) دون الكشف، بالضرورة، عن هوية الكيان الذي يقدم أوراق الاعتماد.

وقد تشمل بعض أوراق الاعتماد كلتا الوظيفتين، ويمكن أن تخضع أوراق الاعتماد بنمطيها على السواء لعملية استيقان منفصلة.

2.A ادعاء أو مزعم

من المتفق عليه عموماً أن مصطلحي ادعاء ومزعم يتشابهان في المعنى بعض الشيء مع اختلاف طفيف في مدلولاتهما. ففي بعض الحالات، يُعتبر المزعم "أقوى" في دلالته من الادعاء. فعلى سبيل المثال، يمكن تعريف الادعاء على النحو التالي:

أ) هو القول بأن الأمر كذا، دون التمكن من تقديم إثبات؛

ب) بيان بأن حال الشيء كذا،

ويعرّف المزعم بأنه: بيان "واثق" و"قوي اللهجة". إلا أن صفتي "واثق" و"قوي اللهجة" لا مغزى حقيقياً لهما في سياق رقمي.

وفي الشبكات المفتوحة، العلاقة بين الطرف الذي يدلي ببيان (أي يقدم معلومات الهوية) والطرف الذي يعول على ذلك البيان ستكون أكثر تعقيداً والتباساً. وعليه، يُفترض أن يكون أي بيان موضع شك، ومن ثم، خاضعاً للتحقق أو لطلب مزيد من الأدلة. ولا يمكن افتراض أن الادعاءات أو المزاعم جديرة بالقبول بأي حال، بل إن قرار قبولها أو عدمه سيعود دوماً إلى الطرف المعول على أساس التحقق الذي يجريه (أو تجريه جهة التحقق بناءً على طلب الطرف المعول).

3.A الانتساب والتسجيل

الانتساب والتسجيل هما عمليتان ترتبطان ارتباطاً وثيقاً وتتداخلان فيما بينهما. ويُستخدم المصطلحان أحياناً للدلالة على نفس المعنى. ورغم إمكانية جمعهما في خطوة واحدة، فهما في الواقع عمليتان متمايزتان.

فالانتساب هو: عملية تنصيب كيان في سياق. وقد يشمل الانتساب التحقق من هوية الكيان وإنشاء هوية سياقية. أما التسجيل فهو: عملية يطلب فيها كيان امتيازات لاستعمال خدمة أو مورد، ويُخصَص بها. والانتساب هو شرط مسبق للتسجيل.

وفي العالم الفعلي مثلاً، يمكن لمستعمل في مرحلة معينة أن ينتسب للاستفادة من خدمات مصرفية، لا على التعيين، ثم يسجل في وقت لاحق ليستفيد من خدمات مصرفية على الخط. وبدلاً من ذلك، يمكن للمستعمل، عند فتح حساب جديد، أن يفي بمتطلبات تحديد الهوية والشكليات (المتصلة به) (أي ينتسب) ويسجل ليستفيد من خدمات مصرفية على الخط في الوقت نفسه.

4.A مورّد الهوية ومورّد خدمة الهوية

تشير دراسة الممارسة المتبعة حالياً إلى شيوع استعمال مصطلحي مورّد الهوية (IdP) ومورّد خدمة الهوية (IdSP) على حد سواء. ورغم أن مصطلح مورّد هوية يُستعمل في بعض توصيات قطاع تقييس الاتصالات، فهو مصطلح يمكن تأويله بمعنى كيان يورّد هويات بدلاً من كيان يدير الهويات. وفوق ذلك، فإن هذا المصطلح مضلل لأن لا سبيل لتوريد هويات. فهي موجودة أو إنها تتبلور عندما تُخصص بنعوت. أضف إلى ذلك أن مصطلح مورّد خدمة يُستعمل على نطاق واسع جداً في مصطلحات مثل مورّد خدمة تحقق ومورّد خدمة أوراق اعتماد ومورّد خدمات مالية.

لذا يُنظر إلى مصطلح مورّد خدمة الهوية (IdSP) على أنه أدل على المعنى من مورّد الهوية (IdP)، وينبغي أن يكون المصطلح المفضل. وأمكن استيعاب هذا التغيير بتأثير طفيف فقط على الوثائق القائمة وذلك باستعمال التعريف الحالي لمورّد الهوية مقابل مورّد خدمة الهوية، وبالاحتفاظ بمصطلح *مورّد الهوية* بمجرد الإحالة إلى *مورّد خدمة الهوية*، بدلاً من تعريفه. وينبغي أن تكون العبارة المختصرة هي IdSP.

5.A نمط الهوية

يُنظر إلى الأنماط بوجه عام على أنها المعلومات التي يتم ملاحظتها أو تمييزها ويمكن اكتشاف بنية بخصوصها أو تتطابق مع بنية معروفة بالفعل. لذا يمكن اعتبار نمط الهوية معلومات تحدد خصائص كيان تتم ملاحظتها أو تمييزها ويمكن اكتشاف بنية بخصوصها أو تتطابق مع بنية معروفة بالفعل.

فعلى سبيل المثال، هناك تعريفان لمصطلح نمط وهما: "شكل أو نظام أو ترتيب عادي أو متكرر"، و"عينة موثوقة من السمات أو الأفعال أو الميول أو الخصائص الأخرى التي يمكن ملاحظتها لفرد أو مجموعة أو مؤسسة".

والمفهوم العام إضافة إلى التعريفين أعلاه للنمط تدل ضمناً على أن هناك أكثر من عنصر للنمط ولكن تكرار نعت واحد مع الزمن يشكل هو الآخر نمطاً. ولا يشكل ظهور وحيد لنعت وحيد نمطاً ولكن طريقة ظهور نعت واحد أو أكثر يمكن أن تشكل نمطاً. كذلك، يمكن لنمط الهوية أن يستند إلى أكثر من نشاط ما أو سلوك ما ولا يقتصر على المعلومات التي يتم ملاحظتها أو تمييزها. حيث يمكن لنمط الهوية أن يستند إلى أي نعت (نعوت). فمثلاً، المظهر الجانبي للإطار له بنية واضحة يمكن اكتشافها ومن ثم يعتبر النعت نفسه هنا (المظهر الجانبي) نمط هوية. كما لا يستلزم بالضرورة أن تكون ملاحظة النمط لأكثر من مرة حالة مفيدة. فمثلاً، شخصان يتحدثان عن سيارة في معرض وكيل سيارات، فإنه يمكنهم تعريفها أو الإشارة إليها كالتالي: "السيارة الموجودة في الركن الأيسر الخلفي".

ويمكن إعادة استعمال الأنماط ولكن يمكن أيضاً تخيل حالات يُستعمل فيها النمط مرة واحدة فقط، مثل شفرات المرة الواحدة.

وعلى الرغم من أنه يمكن الدفع بأن جميع النعوت لها شكل ما من البنية، فإن الفارق الواضح بين النعوت وأنماط الهوية تتمثل في أن البنية يمكن اكتشافها واستنتاجها بواسطة الملاحظة ولكن ليس بالضرورة أن تكون البنية معروفة لدى الكيانات الأخرى، حتى الكيانات المرصودة.

ويمكن استعمال أنماط الهوية ليس فقط لأغراض تعرف الهوية ولكن أيضاً في بعض الحالات لأغراض الاستيقان أو ببساطة تحديد فئات أو تصنيف الكيانات. ومثال على الاستعمال الأخير عندما يتم مسح سلوك المستهلكين لمعرفة أنواع المنتجات التي يشترونها ومدى تكرار شرائهم لهذه المنتجات. وفي سياق "تسويقي" كهذا تستعمل الأنماط لتصنيف الكيانات طبقاً لمجموعات معينة من الكيانات ولكن يمكن بدمج بعض هذه الأنماط معاً التوصل إلى تعرف هوية الكيانات كل على حدة.

والعناصر المستعملة لتعرف هوية كيان ما يجب أن تسمح بتمييز الكيان بشكل كاف في إطار السياق. فإذا كان هناك نمط هوية من المزمع استعماله من أجل التعرف على أفراد (على النقيض من مجموعة) أو استيقانهم، فإنه يتعين أن يكون نمط الهوية متفرداً أو لا لبس فيه. ومع ذلك، هناك بعض الحالات التي قد لا تستوجب أن يكون نمط الهوية متفرداً أو لا لبس فيه، مثل الحالات التي يستعمل فيها لأغراض التخويل. ومثال ذلك قد يكون الحالة التي يتعين فيها تقييد مستعملي خدمة معينة، مثل المشاركة في المنافسات الرياضية. حيث قد يلزم في هذه الحالة فرض قيود، تستند على سبيل المثال إلى سلوك ينطوي على استهلاك عقاقير معينة.

الملحق B

النقاط الرئيسية والأساس المنطقي للمصطلحات الأساسية لإدارة الهوية اللامركزية

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

1.B الهوية اللامركزية

تتمحور نماذج الهوية على النحو المعروض في الملحق A حول مورِّد الهوية. ويفترض النموذج أن المستخدمين يعتمدون على مورِّدي الهوية لتأسيس الهويات والحفاظ عليها وتوريدها لاستخدامها في تفاعلاتهم عبر الإنترنت. ويتطلب هذا النهج المتمحور حول مورِّد الهوية أن يأتمن المستخدمون مورِّدي الهوية على هوياتهم. ويقدِّم مورِّدو الهوية خدمات الاتحاد في النهج المتمحور حول المورِّد لإعادة استخدام الهوية. ويقيد أعضاء الاتحاد القدرة على إعادة استخدام هوية المستخدم. ويضع اتحاد الهوية المورِّدين في مركز الثقة بتركيزهم على حماية نموذج أعمالهم بدلاً من تمكين نظام صدى هوية لامركزي حقيقي يسمح للمستخدمين أن يكونوا مسؤولين عن هويتهم وعلاقاتهم. ويتطلب نموذج الهوية المتمحور حول المورِّد ثقة ضمنية في مورِّدي الهوية المركزيين. وعلى هذا النحو، فإن النموذج ليس مرناً وليس دينامياً.

ومن ناحية أخرى، في نموذج الهوية اللامركزية، يمكّن النظام المستخدمين من التحكم في هويتهم. وفي النهج اللامركزي، يركز مورِّدو الخدمات على تأكيد الادعاءات بشأن هويات محددة. وتُدعم نماذج الهوية اللامركزية بالتطور الحالي لتكنولوجيات سجل الحسابات الموزع (DLT).

ولتمكين الخدمات عبر الميادين المشاركة، تركز نماذج الهوية المركزية على تقديم خدمات الاستيقان في ميدان واحد لتمكين النفاذ عبر جسور اتحاد الهوية إلى ميدان آخر. وفي التفاعلات عبر الإنترنت، يقع الضغط على الأنظمة القائمة على الهوية لتأكيد الهوية المزعومة لكيان بدلاً من تقديم التحكم في النفاذ. وعلى هذا النحو، فإن الوظيفة الرئيسية لأنظمة الهوية اللامركزية هي تقديم نموذج لتمكين إيصال مزاعم بشأن هوية المستخدم التي يمكن استخدامها بسهولة عبر مورِّدي الخدمات.

ويتكون نموذج الهوية المتمحور حول المستخدم من تحكم فردي أو إداري عبر ميادين هوية متعددة دون الحاجة إلى اتحاد يعمل كدائرة ثقة. وتهدف الهوية المتمحورة حول المستخدم إلى إنشاء هوية ثابتة عبر الإنترنت لكيان يركز على إنشاء تجربة أفضل عبر الإنترنت مع تقديم تحكم أفضل للمستخدمين في هوياتهم من خلال استخدام نماذج الثقة اللامركزية. ولكن نظراً لافتقار إلى البساطة ونقص تكنولوجيات مثل تكنولوجيات سجل الحسابات الموزَّع، لم ينجح النموذج المتمركز حول المستخدم.

ومفهوم الهوية المتمحورة حول المستخدم آخذ في اكتساب الزخم منذ ظهور تكنولوجيات سجل الحسابات الموزع (DLT). ويجري إعداد كدسة بروتوكولات تستند إلى DLT لتمكين بنية تحتية لامركزية حقيقية للهوية. يمكن تشغيل هذه الأنظمة بواسطة تكنولوجيات DLT العمومية أو الخاصة أو غير المأذونة أو المأذونة لتمكين إدارة الهويات الرقمية. ويتمثل الهدف في إعادة انتقال التحكم في مزاعم الهوية إلى المستخدمين مع الحفاظ على أمن النظام وسلامته وخصوصياته.

2.B نموذج الهوية اللامركزية

الهوية اللامركزية هي نموذج يعزز التحكم الفردي (مع القدرة على تفويض التحكم) عبر أي عدد من السلطات (بما في ذلك مورِّدو الهوية). ويُطلق على أحد النماذج المحددة للهوية اللامركزية اسم الهوية الذاتية السيادية (SSI) التي تنطوي على الافتراضات المدرجة في الجدول 1.B.

الجدول 1.B – افتراضات هوية السيادة الذاتية

الوجود	يجب أن يمتلك المستخدمون وجوداً مستقلاً
التحكم	يجب على المستخدمين التحكم في هوياتهم
النفاذ	يجب أن يمتلك المستخدمون النفاذ إلى بياناتهم
الشفافية	يجب أن تكون الأنظمة والخوارزميات شفافة
الثبات	يجب أن تكون الهويات طويلة الأمد
قابلية النقل	يجب أن تكون المعلومات والخدمات المتعلقة بالهوية قابلة للنقل
قابلية التشغيل البيني	ينبغي أن تكون الهويات قابلة للاستخدام على أوسع نطاق واسع قدر الإمكان
الموافقة	يجب أن يوافق المستخدمون على استخدام هويتهم
التقليل إلى أدنى حد	يجب التقليل إلى أدنى حد من الإفصاح عن الادعاءات
الحماية	تجب حماية حقوق المستخدمين

وتتوافق الجوانب المرغوبة إلى حد كبير مع ما يمكن أن تقدمه تكنولوجيا سجل الحسابات الموزَّع (DLT). وعادة ما تستند عمليات تنفيذ الهوية اللامركزية إلى الادعاءات والشهادات التي يمكن لجهات فاعلة في كثير من الأحيان القيام بأدوار مختلفة فيها.

ويمكن استخدام أنظمة الهوية اللامركزية لتسهيل المعاملات الموثوقة عبر الإنترنت. وتمكّن أنظمة الهوية اللامركزية المستخدمين من إثبات نعوت عن أنفسهم لمورِّد خدمات (والعكس صحيح) من خلال استخدام ادعاءات (شهادات) يمكن التحقق منها. ويمكن إجراء العملية برمتها بطريقة قابلة للتشغيل البيني وموثوق بها من خلال استخدام مكدس تكنولوجي يتيح نشر الادعاءات الموثوقة دون الحاجة إلى علاقات مباشرة بين المشاركين في المعاملة.

وفي نظام الهوية اللامركزي، يعمل مورِّد الخدمة كطرف معوِّل، بينما تقدِّم الادعاءات جهةُ إصدار شهادة التي تصدر الشهادات الغائبة المطلوبة. والشهادة هي مجموعة من البيانات عن صحة مجموعة أخرى من التصريحات. ويمكن أيضاً تسمية المجموعة الأصلية من التصريحات باسم ادعاء. وينبغي أن يتمكن متلقي الشهادة من التحقق من التزام صاحب الشهادة بالادعاءات. وبالتالي ينبغي أن يتخذ الالتزام شكل توقيع رقمي أو مؤشر للبيانات في سجل الحسابات الموزع.

وتتحدَد هوية العقد في الشبكة عن طريق المعرفات اللامركزية. والمعرف اللامركزي (DID) ضروري للمشاركة في الشبكة وإجراء المعاملات. وهو الرقم/الاسم/السلسلة التي تتحدَد من خلالها هوية شخص ما. والمعرف التجفيري (CID) هو معرِّف هوية لامركزي (DID) موصول تجفيرياً بمفتاح خاص معين.

وتتسم معظم الحلول الحالية القائمة على الهوية بالدعم المحدود فيما يتعلق بالتحكم في الهوية والشفافية وقابلية التنقل، حيث تسهِّل الأطراف الثالثة الموردة ذات الأنظمة مسجلة الملكية هذه الحلول. وقد لا يوجد في المستقبل القريب نظام هوية ملتزم تماماً، بيد أن ذلك لا يغني عن الحاجة لإرساء المبادئ الأساسية للسيادة.

ولتمكين الهوية الذاتية السيادية (SSI)، يجري تقييس موجة جديدة من بروتوكولات وحلول إدارة الهوية اللامركزية كما يرد بحثه في الفقرات 1.2.B حتى 5.2.B.

1.2.B معرفات الهوية اللامركزية

معرفات الهوية اللامركزية (DID) هي معرفات يمكن التحقق منها لأنظمة الهوية اللامركزية بما في ذلك الهوية الرقمية ذات السيادة الذاتية. وبوجه عام، تعتبر المعرفات اللامركزية من إنشاء المستخدم ومملوكة ذاتياً. ويمتلك معرف الهوية اللامركزي خصائص فريدة تعزز ضمان الثبات ومقاومة العبث. وتقع معرفات الهوية اللامركزية تحت سيطرة الجهة المعنية بها، مما يجعلها مستقلة عن أي سجل مركزي، أو مورد هوية مركزي أو سلطة إصدار شهادات مركزية. والمعرفات DID عبارة عن محددات مواقع موارد موحدة (URL)، وتسند الجهة المعنية بالمعرف DID إلى وسائل من أجل تفاعلات موثوقة مع هذه الجهة.

وبشكل عام، تنقسم المعرفات اللامركزية إلى صنفين: معرف الهوية اللامركزي العمومي ومعرف الهوية اللامركزي المزدوج (يمكن اعتبارهما شبه خاصين).

1) معرفات الهوية اللامركزية العمومية هي معرفات يستخدمها المستخدمون الذين يختارون ربط أنفسهم ببيانات مخصصة للتداول مع العموم. وتشمل الأمثلة على ذلك، الملف الشخصي العمومي على وسائل التواصل الاجتماعي أو التحقق من مهنة مثل طبيب. ويتيح معرف الهوية اللامركزي العمومي للمستخدمين دعم الأنشطة التي يستحسنون تداولها مع الآخرين ويمكن للآخرين التحقق منها. فعلى سبيل المثال، يمكنني التحقق من أن طبيبي الشخصي يمتلك معرف الهوية اللامركزي. إذ يمكن اقتفاء أثر معرف الهوية اللامركزي وربطه عبر الإنترنت.

2) وتتولد معرفات الهوية اللامركزية المزدوجة كجزء من علاقة أو مجموعة من التفاعلات يرغب فيها المستخدمون بالانخراط في معاملات متبادلة. ويقوم معرِّف الهوية اللامركزي (DID) المزدوج بعزل المستخدمين ومنع التلازم. وبالنسبة لغالبية المستخدمين، ستكون المعرفات اللامركزية المزدوجة هي الآلية الأساسية لإجراء التفاعلات القائمة على الهوية.

وينتج عن حل معرفات DID وثائق DID بسيطة تشرح كيفية استخدام هذا المعرف DID المحدد. وتتضمن كل وثيقة DID ثلاثة أشياء على الأقل: مواد تجفيرية، ومجموعات استيقان، ونقاط طرفية للخدمة. وتتحد المواد التجفيرية مع مجموعات الاستيقان لتوفير مجموعة من الآليات لاستيقان الجهة المعنية بالمعرف DID (من قبيل المفاتيح العمومية وبروتوكولات القياسات البيومترية المستعارة. وتمكِّن النقاط الطرفية للخدمة التفاعلات الموثوقة مع الجهة المعنية بالمعرف DID.

ولاستخدام معرف DID مع سجل حسابات موزع معيَّن أو شبكة معيَّنة، لا بد من تحديد طريقة للمعرف DID في توصيف منفصل لهذه الطريقة [2]. وتوصف طريقة المعرف DID مجموعة القواعد التي تحدد كيفية تسجيل المعرف DID وحله وتحديثه وإبطاله على سجل الحسابات الموزَّع المعيَّن أو الشبكة المعيَّنة.

ويلغي هذا التصميم الاعتماد على السجلات المركزية بالنسبة لمعرفات الهوية فضلاً عن سلطات إصدار الشهادات المركزية فيما يتعلق بإدارة المفاتيح – وهو النمط المعياري في تراتبية البنية التحتية للمفاتيح العمومية (PKI). وبما أن المعرفات DID تقع على قمة سجل حسابات موزع، فإن كل كيان يمكن أن يعمل كميدان الثقة الخاص به.

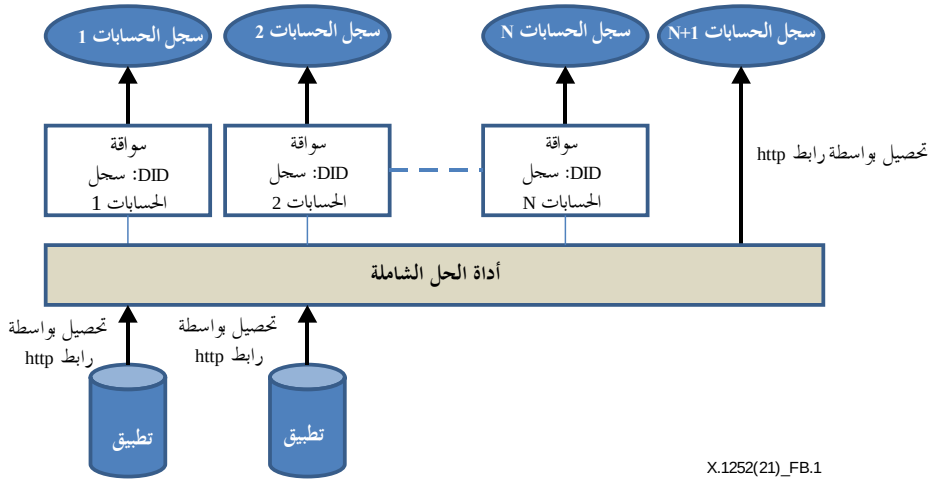
ويجدر بالذكر أن طرق معرِّف الهوية اللامركزي (DID) يمكن إعدادها أيضاً لمعرفات المسجلة في أنظمة إدارة الهوية الاتحادية أو المركزية. ومن جانبها، قد تضيف جميع أنواع أنظمة المعرفات دعماً لمعرفات الهوية اللامركزية. وينشأ عن ذلك جسر لقابلية التشغيل البيني بين عوالم معرفات الهوية المركزية والاتحادية واللامركزية.

2.2.B محاور الهوية

محاور الهوية (IH) هي المكونات المسؤولة عن تخزين مزاعم الهوية بشأن الجهات المعنية. وتستند محاور الهوية إلى نموذج لامركزي لتخزين التمثيلات الدلالية لأي كائن وعرضها بعدئذ كعناوين URL محددة. ويمكن أن تجمع معمارية محور الهوية بين الهويات المخزنة لدي موزِّدين مختلفين بدءاً من سجلات سحابية وصولاً إلى الأجهزة.

3.2.B أداة الحل الشاملة لمعرِّف الهوية اللامركزي (DID)

تعمل أداة الحل الشاملة لمعرِّف الهوية اللامركزي (DID) كنظام موزع يمكنه حل معرف الهوية اللامركزي على تكنولوجيات DLT أو سلاسل كتل متعددة. ولأداة الحل الشاملة لمعرِّف الهوية اللامركزي غرض مماثل لآلية الإسناد في نظام أسماء الميادين (DNS). فبدلاً من العمل مع أسماء الميادين، تركز أدوات الحل الشاملة لمعرِّف الهوية اللامركزي على التعامل مع الهوية الذاتية السيادية (SSI) التي يمكن للكيانات التي تحيل إليها إنشاؤها وتسجيلها مباشرة. ويرد تصوير هذا المفهوم في الشكل 1.B.



الشكل 1.B – أداة الحل الشاملة لمعرِّف الهوية اللامركزي (DID)

4.2.B بيانات الاعتماد التي يمكن التحقق منها

تكون الادعاءات التي يمكن التحقق منها مفيدة عندما يحتاج كيان ما إلى إثبات أنه:

- أكبر من سن معين؛
- قادر على قيادة مركبة آلية معينة؛
- يحتاج إلى دواء معين؛
- مدرب ومعتمد كفني كهرباء؛
- مرخص له مهنياً بممارسة الطب؛
- مسموح له بالسفر الدولي.

ويتألف النظام الإيكولوجي للادعاءات التي يمكن التحقق منها من أربعة أدوار رئيسية:

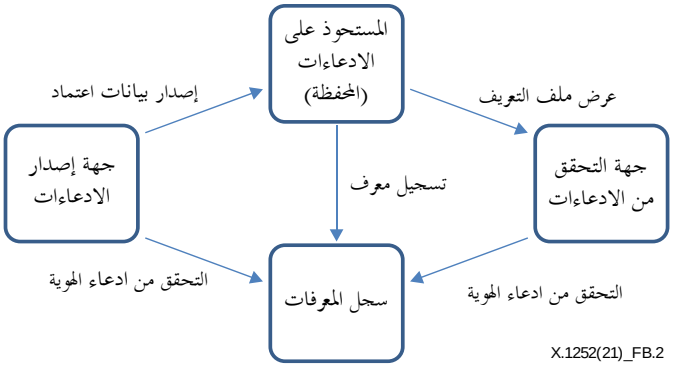
1) جهة الإصدار، التي تصدر بيانات الاعتماد التي يمكن التحقق منها لكيان محدد.

2) المستحوذ على بيانات الاعتماد، الذي يخزن بيانات الاعتماد نيابة عن أي كيان، والمستحوذون هم عادة الكيانات المعنية ببيانات الاعتماد أيضاً.

3) المتحقق، الذي يطلب مواصفة الكيان. وتتضمن المواصفة مجموعة محددة من بيانات الاعتماد. ويتحقق المتحقق من أن بيانات الاعتماد المقدمة في المواصفة تفي بالغرض.

4) سجل معرفات الهوية، عبارة عن آلية تستخدم لإصدار معرفات هوية للكيانات.

والشكل 2.B هو تصوير مرئي للنظام البيئي



الشكل 2.B – النظام البيئي

5.2.B المحفظة اللامركزية

وفي هذا النموذج، يمكن للمستعمل النفاذ إلى أي خدمة بتقديم معرف الهوية الخاص به إلى مورد الخدمة (الطرف المعوِّل (RP)) في صورة تأشيرة. ويتحقق الطرف المعوِّل من الهوية بمقارنة القيم المختزلة لمعرفات الهوية مع السجلات المختزلة المقابلة في المنصة DLT. ويمنح الطرف المعوِّل النفاذ أو يرفضه طبقاً لنتيجة عملية التحقق. وفي السيناريوهات الأكثر تقدماً، يمكن للمستخدم اشتقاق أزواج مفاتيح منفصلة من مفتاح خاص رئيسي لإنشاء معرفات منفصلة لعلاقات مختلفة بغية تمكين التفاعلات المراعية للخصوصيات.

يوضح الشكل B.3 مجمل تفاعلات الهوية الداعمة لخدمة قائمة على الهوية. ويوضح الشكل الخطوات التالية في معاملات الهوية اللامركزية:

- نفترض أن أحد المستعملين قرر التفاعل باستخدام خدمات هوية لامركزية لنسيج ثقة للهوية. وعلى النحو الموضح في مربع سجل الحسابات اللامركزي في الشكل 3.B، توفر المنصة DLT خدمات لتمكين المستعمل النهائي من إنشاء معرف DID وعلاقة مع السجل. وتؤدي مهمة إنشاء معرف DID للمستعمل إلى حفظ عنوان سجل لهذا المستعمل واستحداث زوج مفاتيح عام وخاص للتفاعلات مع المستعمل. ويحتفظ سجل الحسابات أيضاً بوثيقة المعرف DID وروابط البيانات المرتبطة بترميز الكائنات بلغة JavaScript (JSON-LD) المطلوبة المحددة من قبل المستعمل. ويوفر السجل خدمات الهوية الأساسية التي تمكن الخدمات من اكتشاف طريقة التفاعل مع محفظة المستعمل من أجل تقديم استفسارات عن الادعاءات المتاحة الخاضعة لتحكم المستعمل.
- ويفضي استحداث معرف DID في السجل إلى استحداث محفظة كي يستخدمها المستعمل لتقديم الادعاءات المتحقق منها إلى الطرف المعول. وتحتفظ المحفظة بالمفاتيح الخاصة والمفاتيح العمومية والمواصفات الأخرى للهوية للمستعملين وفق ما يحتاجه المعرف DID. ويضمن استخدام تقنيات إثبات المعرفة دون الإفصاح عن المعلومة إمكانية التحقق من الادعاءات بصورة تحفظ الخصوصيات وتتماشى مع الاستعمال الحالي للإثباتات والوثائق التقليدية القائمة على الورق. فمثلاً، يمكن لأي مستعمل إثبات كم يبلغ عمره برخصة القيادة في مطعم دون الحاجة لمشاركة الجهة المصدرة لرخصة القيادة في المعاملة. وترد الخطوات المطلوبة في الفقرات التالية. وقد تكون المحفظة افتراضية بحيث يوضع جزء منها على الجهاز المتنقل للمستعمل وجزء آخر في الخدمات السحابية. وتمكن هذه التشكيلة من استحداث وكلاء للتصرف نيابة عن المستعمل وتنفيذ الخدمات دون الحاجة إلى مشاركة المستعمل المباشرة.

1) سجل المعرفات DID: يقوم المستعمل بتنزيل المحفظة المرتبطة بمورد الخدمة DLT ويسجل المعرفات DID الخاصة به في السجل. وتولد المنصة DLT زوج المفاتيح الخاص والعمومي بمحفظة الهوية. وبالإضافة إلى ذلك، ينشأ موقع أو عنوان ويخزن في المنصة DLT في إطار عملية التسجيل.

2) استهلال الهوية: بالنسبة لأي منصة DLT من المقرر استخدامها في أنظمة هوية لامركزية، يفترض إطار ثقة يحدد قائمة بخدمات الهوية المتاحة للمشاركين. وفي هذا السياق، يمكن للمستعمل الاعتماد على تيسر جهة إصدار (طرف موثوق) يمكنه التحقق من صحة هويات الخدمات. ويمكن للمستعملين الاستناد إلى ادعاءاتهم الأولية لجمع الادعاءات من موردين متعددين لإضافتها إلى محافظهم ولتعزيز صحة هوياتهم داخل النظام. ومن الشكل 3.B، تتم حماية كل علاقة من خلال المعرفات DID المتبادلة بين جهة الإصدار والجهة المستحوذة (المستعمل) والمتحقق.

3) التحقق: إذا رغبت الجهة المستحوذة (المستعمل) في النفاذ إلى خدمة ما من طرف معول، يستفسر الطرف المعول (RP) (المتحقق) من المستعمل عن الادعاءات المتاحة. ويلجأ المتحقق بعد ذلك إلى المنصة DLT من أجل التحقق من صحة الادعاءات الموقعة باستخدام المفاتيح العمومية المقابلة للمعرف DID والمتصلة بالمعاملة. وتتضمن هذه الخطوة طبقات أخرى من الاستيقان وعلى وجه الخصوص طريقة عمل النظام وتفترض أن المحفظة مصدر ثقة فيما يتعلق بمعرفة المفاتيح الخاصة للمستحوذ. ويفترض النظام أنه قد أجري الاستيقان المناسب للتأكد من أن المالك الشرعي للمحفظة هو الكيان القائم بالمعاملة.

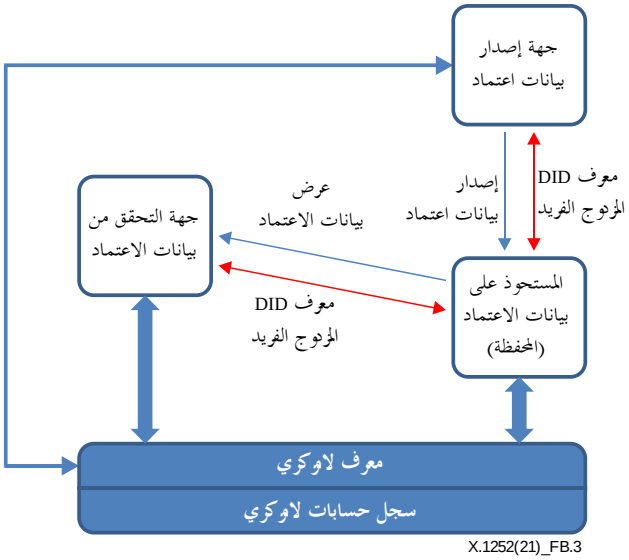
4) التحقق من صحة الادعاءات: يستخدم الطرف المعول الادعاءات المقدمة من المحفظة للتحقق من هوية ونعوت المستعمل باستخدام التوقيع القائم على البنية التحتية للمفاتيح العمومية فضلاً عن تقنيات اختزال التحقق.

5) التخويل: يحدد الطرف المعول الخدمات التي يمكن النفاذ إليها استناداً إلى نتائج التحقق من الهوية.

- ويستدعي تصميم معرف DID قدرة أداة الحل الشاملة على التعامل مع أي معرف DID. ولا تزال تلبية هذا المتطلب قيد الإنجاز لدى مجتمع DLT. وفي نماذج الهوية اللامركزية، تدعو الحاجة لإنشاء طبقة استيقان للمعرفات DID القابلة للتشغيل البيني. ولا يزال ذلك قيد التنفيذ.
- ويمكن استيقان المعرفات DID مالك الهوية من التحكم في المعرف DID أثناء تفاعله مع أي طرف معول (RP). ويتطلب ذلك تنفيذ الطرف المعول للخطوات التالية:

1) يحل الطرف المعول المعرف DID الخاص بمالك الهوية إلى وثيقة معرف DID؛
2) يحاول الطرف المعول استيقان مالك الهوية باستخدام غرض (أغراض) الاستيقان الموجود (الموجودة) في وثيقة المعرف DID؛
3) يمكن لأغراض الاستيقان أن تتضمن أو تحيل إلى غرض لمفتاح عمومي، في الحالات التي ينشا فيها إثبات مالك الهوية في صورة توقيع مجفر.

- ويجب فهم استيقان معرِّف الهوية اللامركزي (DID) على أنه قابل للتوسيع فيما يتعلق بكيف يمكن لمالك الهوية إثبات التحكم في معرف الهوية اللامركزي.



الشكل 3.B – محفظة الهوية اللامركزية مع ادعاءات يمكن التحقق منها

بيبليوغرافيا

[b-ITU-T E.101] Recommendation ITU-T E.101 (2009), *Definitions of terms used for identifiers (names, numbers, addresses and other identifiers) for public telecommunication services and networks in the E-series Recommendations*.

[b-ITU-T L.1410] Recommendation ITU-T L.1410 (2014), *Methodology for environmental life cycle assessments of information and communication technology goods, networks and services*.

[b-ITU-T X.501] Recommendation ITU-T X.501 (2019) | ISO/IEC 9594-2:2020, *Information technology – Open Systems Interconnection – The Directory: Models*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *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 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems – Authentication framework*.

[b-ITU-T X.1254] ITU-T X.1254 (2020), *Entity authentication assurance framework*.

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T X.1403] Recommendation ITU-T X.1403 (2020), *Security guidelines for using distributed ledger technology for decentralized identity management*.

[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-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[b-ISO/IEC 2382-37] ISO/IEC 2382-37:2017, *Information technology — Vocabulary — Part 37: Biometrics*.

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2019, *IT Security and Privacy – A frame work for identity management – Part 1: Terminology and concepts*.

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Information Technology – Security techniques – Entity authentication assurance framework*.

[b-OIX-TFIS] Makaay, E., Smedinghoff, T., Thibeau, D. (2017). *Trust frameworks for identity systems*, White paper, Trust framework series. London: Open Identity Exchange. 18 pp. Available [viewed 2021-05-17] at: https://connectis.com/wp-content/uploads/2018/05/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf

[b-W3C-DIDs] W3C (Internet), [Untitled], Decentralized identifiers (DIDs) … Cambridge, MA: World Wide Web Consortium. Available [viewed 2021-05-15] at: https://w3c.github.io/did-core/

[b-W3C-VC] W3C Working Group Note (2019), *Verifiable credentials use cases*. Cambridge, MA: World Wide Web Consortium. Available [viewed 2021-05-17] at: http://www.w3.org/TR/vc-use-cases/

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
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	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات 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، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
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، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2021