الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

# ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

# X.1403

(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن تكنولوجيا السجلات الموزعة

# مبادئ توجيهية أمنية بشأن استخدام تكنولوجيا السجلات الموزعة في إدارة الهوية اللامركزية

التوصية ITU-T X.1403

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

## شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

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

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

**التوصية ITU-T X.1403**

# مبادئ توجيهية أمنية بشأن استخدام تكنولوجيا السجلات الموزعة في إدارة الهوية اللامركزية


## ملخص

تتيح تكنولوجيا السجلات الموزعة (DLT) وحالات التنفيذ الخاصة بها، مثل سلسلة الكتل، فرصة فريدة لاستخدام بنية تحتية موثوقة ومنصة قد تفيدان في تمكين اتحاد موثوق من تبادل نعوت الهويات ومعلوماتها. وتعرض التوصية ITU T X.1403 اعتبارات الخصوصية والأمن الخاصة بالاتصالات من أجل استخدام بيانات تكنولوجيا السجلات الموزعة في إدارة الهوية.



## التسلسل التاريخي

| الطبعة | التوصية | تاريخ الموافقة | لجنة الدراسات | معرف الهوية الفريد* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1403 | 2020-09-03 | 17 | 11.1002/1000/14264 |


## مصطلحات أساسية

تكنولوجيا السجلات الموزعة، إدارة الهوية.

* 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 (ITU) هو 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**

# مبادئ توجيهية أمنية بشأن استخدام تكنولوجيا السجلات الموزعة في إدارة الهوية اللامركزية

## 1 مجال التطبيق

توفر تكنولوجيا السجلات الموزعة (DLT) بنية تحتية موثوقة تفيد في تمكين أنظمة إدارة الهوية اللامركزية من تبادل نعوت الهويات ومعلوماتها.

وتقدم هذه التوصية نظرة عامة عن استخدام تكنولوجيا السجلات الموزعة في إدارة الهوية اللامركزية. ويشمل مجال التطبيق ما يلي:

- نظرة عامة مختصرة عن استخدام السجلات الموزعة في إدارة الهوية وبياناتها،
- مناقشة حول الفوائد الأمنية للهوية اللامركزية،
- مبادئ توجيهية بخصوص الضوابط التي ينبغي استخدامها للحد من التهديدات التي تتعرض بيانات الهوية.

## 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 وقت نشر هذه التوصية. وبما أن جميع التوصيات والمراجع الأخرى تخضع للمراجعة، يُرجى من مستعملي هذه التوصية السعي إلى تقصّي إمكانية تطبيق أحدث طبعة للتوصيات وغيرها من المراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات سارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

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

[ITU-T X.1254] التوصية ITU-T X.1254 (2012)، *إطار ضمان استيقان الكيان*.

[ITU-T X.1277] التوصية ITU-T X.1277 (2018)، *إطار الاستيقان العالمي*.

[ITU-T X.1278] التوصية ITU-T X.1278 (2018)، *البروتوكول من العميل إلى المستيقن/إطار عالمي من عاملين*.

## 3 التعاريف

### 1.3 مصطلحات معرفة في مراجع أخرى

تستخدم هذه التوصية المصطلحات التالية المعرفة في مراجع أخرى:

**1.1.3 ادعاء (Claim)** [ITU-T X.1252]: القول بأن الأمر كذا، دون التمكن من تقديم إثبات.

**2.1.3 إثباتات (Credential)** [ITU-T X.1252]: مجموعة بيانات تقدم كدليل على هوية و/أو استحقاقات مزعومة.

**3.1.3 وثيقة معرف هوية لامركزي (DID document)** [b-W3C-2]: مجموعة من البيانات التي تصف الجهة المعنية بمعرف الهوية اللامركزي (DID)، بما في ذلك الآليات مثل المفاتيح العمومية والقياسات البيومترية المستعارة، التي يمكن للجهة المعنية بالمعرف DID أن تستخدمها لاستيقان نفسها وإثبات ارتباطها بالمعرف DID.

**4.1.3 كيان (Entity)** [ITU-T X.1252]: شيء له وجود قائم بذاته ومميز ويمكن تعريفه في سياق ما.

**5.1.3 اتحاد (Federation)** [ITU-T X.1252]: رابطة بين مستعملين وموردي خدمات وموردي خدمة الهوية.

**6.1.3 مورّد خدمة الهوية (identity service provider) (IdSP)** [b-ITU-T X.1252]: كيان يقوم بالتحقق من معلومات الهوية وتحديثها وإدارتها، ويمكنه استحداث معلومات هوية وتخصيصها لكيانات أخرى.

## 2.3 مصطلحات معرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

**1.2.3 معرف هوية لامركزي (Decentralized identifier) (DID)** [b-W3C-2]: معرف هوية متفرد عالمياً لا يحتاج إلى سلطة تسجيل مركزية لأنه مسجل بتكنولوجيا السجلات الموزعة (DLT) أو بأي شكل آخر من الأنظمة اللامركزية.

**ملاحظة** – بناءً على التعريف الوارد في المرجع [b-W3C-2].

**2.2.3 الجهة المعنية بالمعرف DID (DID Subject)**: الكيان الذي تتناوله وثيقة المعرف DID. وهو الكيان الذي يحدده المعرف DID وتصفه وثيقة المعرف DID.

**ملاحظة** – بناءً على التعريف الوارد في المرجع [b-W3C-2].

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

**4.2.3 نقطة طرفية للخدمة (Service endpoint)**: عنوان سجل موزع تعمل عنده الخدمة نيابة عن جهة معنية بالمعرف DID. ومن أمثلة الخدمات المحددة خدمات الاكتشاف وشبكات التواصل الاجتماعي وخدمات تخزين الملفات وخدمات مستودعات الادعاءات التي يمكن التحقق منها. ويمكن أيضاً توفير النقاط الطرفية للخدمات من خلال بروتوكول معمم لتبادل البيانات مثل تبادل البيانات القابل للتوسيع.

**ملاحظة** – بناءً على التعريف الوارد في المرجع [b-W3C-2].

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

**6.2.3 محفظة (محفظة هويات) ((Wallet (identity wallet))**: تطبيق يمكّن المستعمل في الأساس من الاحتفاظ بمعرفات هوية وإثباتات بتخزين المفاتيح الخاصة المقابلة على جهاز المستعمل.

**7.2.3 إثبات المعرفة دون الإفصاح عن المعلومة (Zero knowledge proof)**: إثبات يستخدم تجفيراً خاصاً وسراً 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 الشخص القائم بالإثبات.

# 4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

DDO وثيقة المعرّف DID *(DID Document)*

DID معرف هوية لامركزي *(Decentralized Identifier)*

DIdAm إدارة الهوية اللامركزية والنفاذ إليها *(Decentralized Identity and Access Management)*

DLT تكنولوجيا السجلات الموزعة *(Distributed Ledger Technology)*

IdAM النفاذ إلى الهوية وإدارتها *(Identity Access and Management)*

IdSP مورد خدمة هوية *(Identity Service Provider)*

IT تكنولوجيا المعلومات *(Information Technology)*

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

PII المعلومات المحدِّدة لهوية الأشخاص *(Personally Identifiable Information)*

RP الطرف المعول *(Relying Party)*

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

SP مقدّم الخدمة *(Service Provider)*

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

SSO تسجيل الدخول بإثباتات وحيدة *(Single Sign On)*

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

## 5 الاصطلاحات

تطبق هذه التوصية الأشكال الشفهية التالية لتعابير النصوص:

أ ) "يجب/صيغة المضارع" تشير إلى معنى اشتراطي،

ب) "ينبغي" تشير إلى التوصية بأمر ما،

ج) "يجوز" تشير إلى السماح لطرف أو جهة بأمر ما،

د ) "بإمكان/يمكن لـ" تشير إلى الإمكانية أو المقدرة على أمر ما.

## 6 نحو هوية رقمية لامركزية

تؤدي تكنولوجيا السجلات الموزعة دوراً حاسماً في زيادة تطور واكتمال أنظمة الهوية اللامركزية.

وقد زاد انتشار الأجهزة المتنقلة وإنترنت الأشياء من الضغط على الأنظمة التقليدية لإدارة الهوية والنفاذ إليها (IdAM) للتطور نحو منصات تتسم بالمرونة والذكاء وبوسعها دعم الأنظمة المتنقلة والقائمة على الحوسبة السحابية.

وتستند الأنظمة التقليدية لإدارة الهوية إلى السلطات المركزية مثل خدمات الدليل بالشركات أو سلطات إصدار الشهادات أو مكاتب تسجيل أسماء الميادين. وكل سلطة من هذه السلطات المركزية من حيث التنظيم تعمل كميادين موثوقة خاصة بها. وفي أي نظام تقليدي للنفاذ إلى الهوية وإدارتها، يمكن للسلطة المركزية أن تمثل نقطة فشل وحيدة. وقد ظهرت اتحادات الهوية [ITU-T X.1252] كحل مؤقت يمكن أنظمة النفاذ إلى الهوية وإدارتها من العمل عبر أنظمة تتولى منظمات مختلفة التحكم في الميادين الخاصة بها.

وقد أتاح ظهور تكنولوجيا السجلات الموزعة الفرصة لتطوير حلول إدارة الهوية اللامركزية والنفاذ إليها (DIdAm). وتوفر تكنولوجيا السجلات الموزعة وسيلة لإدارة الثقة بدون أي سلطة مركزية مما يؤدي إلى تفادي أي نقطة فشل وحيدة. وعلاوةً على ذلك، تمكن تكنولوجيا السجلات الموزعة أي كيان من استحداث وإدارة معرفات الهوية الخاصة به على أي عدد من السجلات الموزعة.

وقد شهدت نماذج الهوية الرقمية تطوراً مستمراً من أجل تلبية الاحتياجات المتغيرة للأعمال. وهناك ثلاثة نماذج أساسية للهوية كما هو موضح في القسم 6.

### 1.6 نموذج الهوية المركزية

هذا هو نموذج الهوية الرقمية الأقدم والأكثر استعمالاً في الوقت الحالي [ITU-T X.1252]. وفي نموذج الهوية المركزية، تتصرف المنظمات كجهات موردة لخدمة الهوية (IdSP). وفي هذا النموذج، تقيم المنظمة علاقة موثوقة من طرف إلى طرف مع كل مستعمل من مستعمليها. وهذا النموذج تقليدي ومنغلق، حيث تصدر فيه المنظمة إثباتاً للمستعمل يمكنه من النفاذ إلى خدمات هذه المنظمة.

وتتصرف كل منظمة في هذا النموذج كمورد لخدمات الهوية. وتدير المنظمة الهوية الرقمية للمستعمل وتحدد علاقات الثقة المقبولة. وتنشأ الثقة بين المستعمل ومورد خدمة الهوية عادة من خلال استعمال أسرار مشتركة كاستخدام اسم مستعمل وكلمة مرور. وفي بعض الحالات، تتم زيادة الأسرار المشتركة باستيقانات متعددة العوامل مثل الحلول القائمة على العلامات الرمزية للعتاد أو القياسات البيومترية أو الهوية السريعة على الإنترنت (FIDO) [ITU-T X.1277] و[ITU-T X.1278].

وفي النموذج المركزي، يستطيع مورد خدمة الهوية تخزين وجمع بيانات عن المستعملين. ويمكن تحويل البيانات إلى نقد أو تقاسمها أو بيعها لأطراف أخرى طبقاً لنموذج أعمال مورد خدمة الهوية (IdSP). ويجب أن يثق المستعملون في مورد خدمة الهوية من أجل التصرف بالشكل السليم عندما يتعلق الأمر بإدارة بياناتهم. وبالرغم من استفادة المستعملين النهائيين من خدمات المنظمة، فإنهم لا يملكون في معظم الأحوال القدرة على التحكم في إدارة هوياتهم الخاصة بهم أو بياناتهم الشخصية أو نعوت هوياتهم الشخصية. وفي هذا النموذج، يكون مورد خدمة الهوية هو المالك لهويات المستعملين. ولا يتسنى للمستعملين نقل بياناتهم إلى موردين آخرين.

ويلزم نموذج الهوية المركزية المستعمل باستحداث وإدارة إثباتات منفصلة لكل علاقة عمل خاصة به مع كل مورد من موردي خدمات الهوية. ويتعين أن تقوم المنظمة باستحداث هذه الإثباتات قبل أن يسمح لأي مستعمل بالنفاذ إلى مواردها. ويغرق هذا النموذج المستعملين بالكثير من الهويات الإلكترونية. والافتقار إلى الاستيقان المتبادل عند تسجيل الدخول يجعل هذا النموذج عرضة لهجمات الانتحال وسرقة الإثباتات. ويشجع النموذج المستعملين على إعادة استعمال كلمات المرور، وهو ما يؤدي إلى مزيد من المخاطر ومواطن الضعف الأمنية.

ويلقي النموذج المركزي بعبء على موردي خدمات الهوية عندما يتعلق الأمر بإدارة دورة حياة الهوية. ويتطلب النموذج، بوجه خاص، أن يقوم كل مورد خدمة هوية بإجراء تحقق من الهوية [ITU-T X.1254] في إطار مرحلة تسجيل الهوية عند إدارة دورة حياة الهوية. ولا بد من التحقق من الهوية لتحقيق مستوى من الثقة في الهوية المدعاة. ويمكن تكرار هذه العملية طوال فترة حياة أي هوية. وتشكل هذه الخطوة معضلة من وجهة نظر المستعمل لأن النموذج المركزي يلزم المستعمل بإجراء خطوة التحقق من الهوية بشكلٍ منفصل مع كل مورد من موردي الهوية. وإضافةً إلى ذلك، تزيد تهديدات انتهاكات البيانات من مخاطر الاستيلاء على الحسابات نتيجة لاعتماد المنظمات على بيانات مركزية مخزنة تمثل هدفاً للقراصنة على أساس منتظم.

### 2.6 نموذج الهوية الاتحادية

أدركت المنظمات القيود التي يتسم بها نموذج الهوية المركزية والتي نوقشت في القسم 1.6 وعملت على تطوير نموذج الهوية الاتحادية لمواجهة هذه التحديات. ويرمي نموذج الهوية الاتحادية إلى الحد من الأعباء التي يتحملها المستعملون بتمكينهم من استخدام هوياتهم من ميدان لآخر. وتوفر لغة وسم تأكيد الأمن (SAML) [ITU-T X.1242] المزيد من السهولة للأفراد من خلال وظيفة تسجيل الدخول بإثباتات وحيدة (SSO).

ويمكن لأنظمة إدارة الهوية الاتحادية توفير قدرات الاستيقان والتخويل عبر حدود المنظمات والأنظمة. وهي تستوجب إبرام اتفاقات عمل وثقة بحيث تحظى هوية مستعمل لدى أحد الموردين باعتراف الموردين الآخرين (أعضاء الاتحاد). وعموماً، يشمل اتفاق الثقة أيضاً اتفاقاً تعاقدياً بشأن ملكية البيانات واستخدام المعلومات المحددة لهوية الأشخاص (PII) والامتثال [ITU-T X.1242].

ويفيد نموذج الاتحاد المستعملين من حيث إن مورد خدمة الهوية عادة ما يوفر للمستعمل تجربة تسجيل الدخول بإثباتات وحيدة. وهو يقلل عدد الإثباتات المنفصلة التي يتعين على المستعمل رعايتها وحيازتها. وفي هذا النموذج، تعتمد الأطراف المعولة المشاركة في الاتحاد، بما في ذلك مستعملوهم، على تيسر الخدمات الخاصة بمورد معين من موردي خدمات الهوية ورغبته في الاستمرار في الاتحاد.

وكما هو الحال في نموذج الهوية المركزية، فإن الاستيقان في نموذج الاتحاد غير متبادل ويعاني من نفس القيود.

### 3.6 نموذج الهوية اللامركزية

يمكن تنفيذ الهوية اللامركزية باستخدام تكنولوجيا السجلات الموزعة أو أي تكنولوجيات أخرى ناشئة قائمة على المعايير مثل الادعاءات التي يمكن التحقق منها [b-W3C-1] ومعرفات الهوية اللامركزية (DID) [b-Sovrin] و[b-W3C-1] و[b-W3C-2]. ويمكن أن يستند نموذج الهوية اللامركزية إلى تكنولوجيا السجلات الموزعة وعلاقة بين مستعمل ومنظمة [b-Sovrin] و[b-W3C-17]. وفي هذا النموذج، يكون المستعمل والمنظمة نظيرين.

وتسمح الهوية اللامركزية للمستعملين بالسيطرة على هوياتهم وملكيتها. ويمكن لمستوى الملكية أن يختلف باختلاف النموذج اللامركزي. ففي نموذج هوية السيادة الذاتية (SSI)، على وجه الخصوص، يفترض أن الكيانات ستكون قادرة على التحكم في هوياتها الرقمية.

وتتسم معظم حلول الهوية الحالية بالدعم المحدود فيما يتعلق بالتحكم في الهوية والشفافية والقدرة على التنقل، حيث إن موردي خدمات الهوية ذوي الأنظمة مسجلة الملكية يسهلون هذه الحلول. وقد يتم في المستقبل القريب التوصل إلى نظام هوية ممتثل تماماً لنموذج هوية السيادة الذاتية، بيد أن ذلك لا يستبعد الحاجة إلى تحديد مبادئه الأساسية، على النحو المناقش في القسمين 1.3.6 و2.3.6. ويناقش استخدام تكنولوجيا السجلات الموزعة في إدارة الهوية اللامركزية مجدداً في القسم 7.

#### 1.3.6 معرفات الهوية اللامركزية

معرفات الهوية اللامركزية [b-W3C-2] هي نوع من أنواع المعرفات من أجل أنظمة الهوية التي يمكن التحقق منها واللامركزية. ويسمح نسق هذه المعرفات بأن تكون 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)، تسند الجهة المعنية بالمعرف DID إلى وسائل من أجل تفاعلات موثوقة مع هذه الجهة. وتشمل العناصر القياسية لوثيقة المعرف DID (DDO) [b-W3C-2]:

1) معرف DID (من أجل الوصف الذاتي)
2) مجموعة المفاتيح العمومية (من أجل التحقق)
3) مجموعة بروتوكولات الاستيقان (من أجل الاستيقان)
4) مجموعة النقاط الطرفية للخدمة (من أجل التفاعل)
5) خاتم التوقيت (من أجل مراجعة التسلسل التاريخي)
6) التوقيع (من أجل السلامة).

وينتج عن حل أي معرف DID [b-W3C-2] وثيقة DDO، وهي وثيقة بسيطة تشرح كيفية استخدام هذا المعرف DID المحدد. وتتضمن كل وثيقة DDO ثلاثة عناصر على الأقل: مواد تجفيرية، ومجموعات استيقان، ونقاط طرفية للخدمة. وتتحد المواد التجفيرية مع مجموعات الاستيقان لتوفير مجموعة من الآليات لاستيقان الجهة المعنية بالمعرف DID (وهو المستعمل المرتبط بالوثيقة DDO). ومن أمثلة خيارات الاستيقان المفاتيح العمومية وبروتوكولات القياسات البيومترية المستعارة. وتسمح النقاط الطرفية للخدمة بالاتصالات الموثوقة مع الجهة المعنية بالمعرف DID.

ولاستخدام معرف DID [b-W3C-2] مع سجل موزع خاص، لا بد من تحديد طريقة للمعرف DID. ويمكن لمواصفة طريقة المعرف DID أن تستند إلى المعيار [b-RFC 8141]. وتوصف طريقة المعرف DID مجموعة القواعد التي تحدد كيفية تسجيل المعرف DID وحله وتحديثه وإبطاله على إحدى تكنولوجيات السجلات الموزعة المحددة. وتوصف جميع المعرفات DID وتحل على سجل موزع.

ويقلل استعمال المعرف DID القائم على تكنولوجيا السجلات الموزعة [b-W3C-2] من الاعتماد على السجلات المركزية بالنسبة لمعرفات الهوية فضلاً عن سلطات إصدار الشهادات المركزية فيما يتعلق بإدارة المفاتيح. وبما أن المعرفات DID تقع على قمة سجل موزع، فإن كل كيان يمكن أن يعمل كميدان الثقة الخاص به مما يفضي إلى بنية تحتية للثقة لامركزية. وينشأ عن ذلك جسر لقابلية التشغيل البيني بين عوالم معرفات الهوية المركزية والاتحادية واللامركزية.

وللمعرف DID زوج من مفاتيح التجفير، عمومي وخاص [b-W3C-2]. ويتم إثبات ملكية أي معرف DID عن طريق خوارزميات تجفير تعتمد على مفتاح خاص، لا ينبغي أن يستحوذ عليه إلا مالك المعرف DID. وبالتالي، يمكن نشر أو تغيير أو الاستفسار عن أو إلغاء المعرفات DID. وبما أن لكل تكنولوجيا من تكنولوجيات السجلات الموزعة عملية التنفيذ الخاصة بها لطريقة المعرف DID، فإنه يوجد عملياً عمليات تنفيذ مختلفة من أجل عمليات "استحداث وقراءة وتحديث وإلغاء (CRUD)" المعرف DID.

### 2.3.6 الإثباتات التي يمكن التحقق منها

تحل الإثباتات التي يمكن التحقق منها [b-W3C-1] مشكلة تبادل الإثباتات مثل رخصة القيادة وشهادات الميلاد والمؤهل العلمي وبيانات الرعاية الصحية، عبر شبكة اتصالات بطريقة يمكن التحقق منها وتحمي في نفس الوقت المعلومات PII الخاصة بالأفراد. وفي هذا النهج، تتألف الإثباتات من بيانات تسمى ادعاءات يمكن التحقق منها. والادعاءات التي يمكن التحقق منها [b-W3C-1] تكون 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 للإثباتات التي يمكن التحقق منها من أربعة أدوار رئيسية:

1) الجهة القائمة بالإصدار، التي تصدر الإثباتات التي يمكن التحقق منها لكيان محدد،
2) المستحوذ على الإثباتات، الذي يخزن الإثباتات نيابة عن أي كيان، والمستحوذون هم عادة الكيانات المعنية بالإثباتات أيضاً،
3) المتحقق، الذي يطلب مواصفة الكيان. وتتضمن المواصفة مجموعة محددة من الإثباتات. ويتأكد المتحقق من أن الإثباتات المقدمة في المواصفة تفي بالغرض،
4) سجل معرفات الهوية، عبارة عن آلية تستخدم لإصدار معرفات هوية للكيانات.

وأي ادعاء [b-W3C-1] هو عبارة بيان عن كيان ما يعبر عنه بعلاقة كيان–ملكية–قيمة. ويمكن دمج الادعاءات معاً لإعداد رسم بياني لمعلومات عن كيان بعينه.

عندما تقوم إحدى الجهات المصدرة بإرسال بيانات لمستحوذ ما، تقوم بتجميع مجموعة من الادعاءات في بنية بيانات تسمى إثبات وتوقع رقمياً على بنية البيانات [b-W3C-1]. وعندما يطلب المتحقق بيانات من المستحوذ، يقوم المستحوذ عادة بتجميع مجموعة من الإثباتات في بنية بيانات تسمى مواصفة ويوقع رقمياً على بنية البيانات [b-W3C-1].

## 7 الهوية اللامركزية باستخدام تكنولوجيا السجلات الموزعة

يمكن تصور الهوية اللامركزية على أنها هوية تدعمها تكنولوجيا من تكنولوجيات السجلات الموزعة. وفي هذا النهج، يمكن لإثبات المعرفة دون الإفصاح عن المعلومة [b-W3C-1] أن يربط الهويات بطريقة تجعلها قابلة للاكتشاف عالمياً. وتمكن الهوية اللامركزية المستعمل من إثبات هويته مرة واحدة لطرف ثالث موثوق وتخزين إثباتات معرفات الهوية في واحدة من تكنولوجيات السجلات الموزعة (DLT). وتتصرف التكنولوجيا DLT كخزانة موثوقة للهوية. وتوفر هذه التكنولوجيا خدمات البنية التحتية الخاصة بالهوية دعماً للاتصالات بين النظراء وخدمات البنية التحتية للمفاتيح العمومية (PKI) القائمة على تكنولوجيا DLT وبروتوكولات تبادل الادعاءات التي يمكن التحقق منها، وذلك ضمن أمور أخرى.

وتمكن الهوية اللامركزية المستعمل من النفاذ إلى الخدمات من خلال عملية مباشرة. فمثلاً، يتفاعل مستعمل ما مع أحد موردي خدمات الهوية الذي يستخدم بدوره تكنولوجيا DLT لاستحداث معرف هوية DID للمستعمل يشير إلى موقع منصة التكنولوجيا DLT التي يمكن للمستعمل استخدامها. وهذه الخطوة واضحة تماماً للمستعمل النهائي. وتعادل هذه الخطوة استحداث زوج من المفاتيح، خاص وعمومي للمستعمل. ويخزن المفتاح الخاص مع المستعمل في شكل ما من أشكال المحفظة الرقمية. ويخزن المفتاح العمومي المقابل في منصة التكنولوجيا DLT. ويعمل المفتاح العمومي كمعرف هوية للمحفظة (هوية مستعمل باتفاق قائم على الاستيقان والمفتاح في منصة التكنولوجيا DLT) وتختزل وتخزن بصورة آمنة في السجل. وفي إطار الخدمات المقدمة من المنصة DLT، يمكن إصدار الادعاءات وتوقيعها بشأن مستعمل معين من جانب جهات الإصدار في المنصة DLT وتزويد المستعمل بها. ويمكن تخزين هذه الادعاءات في محفظة المستعمل.

وفي هذا النموذج، يمكن للمستعمل النفاذ إلى أي خدمة بتقديم معرف الهوية الخاص به إلى مورد الخدمة في صورة علامة رمزية. ويتحقق مورد الخدمة من الهوية بمقارنة القيم المختزلة لمعرفات الهوية مع السجلات المختزلة المقابلة المخزنة في المنصة DLT. ويمنح مورد الخدمة النفاذ أو يرفضه طبقاً لنتيجة عملية التحقق.

### 1.7 إطلاق المحفظة

يوفر العمل في [b-Sovrin] و[W3C-1] مثالاً للتفاعلات الداعمة لخدمة قائمة على الهوية. نفترض أن أحد المستعملين قرر التفاعل باستخدام خدمات هوية لامركزية لنظام ثقة للهوية قائم على التكنولوجيا DLT. وفي هذا السياق، توفر المنصة DLT خدمات لتمكين المستعمل النهائي من إنشاء معرف DID وعلاقة مع السجل. وتنتهي مهمة إنشاء معرف DID للمستعمل بحفظ عنوان سجل لهذا المستعمل واستحداث زوج مفاتيح عام وخاص للتفاعل مع المستعمل. ويمكن للسجل أن يوفر أيضاً خدمات يمكن استخدامها في إنشاء وثيقة المعرف DID وروابط الوثيقة 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.

وتفضي عملية استحداث معرف DID في السجل إلى استحداث محفظة كي يستخدمها المستعمل لتقديم الادعاءات المتحقق منها إلى الطرف المعول (RP). وتحتفظ المحفظة بالمفاتيح الخاصة والمفاتيح العمومية والمواصفات الأخرى للهوية للمستعمل كما حددتها طريقة المعرف DID. ويضمن استخدام تقنيات إثبات المعرفة دون الإفصاح عن المعلومة [b-Sovrin] إمكانية التحقق من الادعاءات بصورة تحفظ المعلومات PII وتتماشى مع الاستعمال الحالي للإثباتات والوثائق التقليدية القائمة على الورق. فمثلاً، يمكن لأي مستعمل إثبات كم يبلغ عمره برخصة القيادة في أي مكان دون مشاركة الجهة المصدرة لرخصة القيادة في المعاملة. 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 المشاركة المباشرة من جانب المستعمل.

وتتعلق الخطوات التالية بهذه العملية:

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 المرتبط بمحفظة الهوية. وينشأ عنوان ويخزن في المنصة DLT في إطار عملية التسجيل.

2) استهلال الهوية: بالنسبة لأي منصة DLT من المقرر استخدامها في أنظمة هوية لامركزية، يفترض وجود 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 المستعملين. بداية، يمكن للمستعملين البدء بالادعاءات المؤكدة ذاتياً. ويمكن للمستعملين بعد ذلك الاستناد إلى ادعاءاتهم الأولية بمحافظهم لجمع المزيد من الادعاءات من موردين متعددين لإضافتها إلى محافظهم ولتعزيز صحة هوياتهم داخل النظام. وتتم 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، يطلب الطرف المعول (المتحقق) من المستعمل منحه النفاذ إلى الادعاءات المتاحة في محفظته. ويلجأ المتحقق بعد ذلك إلى المنصة DLT من أجل التحقق من صحة الادعاءات الموقعة باستخدام المفاتيح العمومية المقابلة للمعرف DID المنصوص عليها في المعاملة. ويفترض النظام 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 للمنصة DLT وتقنيات اختزال التحقق.

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

### 2.7 حل المعرفات DID واستيقانها

يمكن لمفهوم المعرفات DID [b-W3C-2] أن يسهل استحداث أداة عالمية للحل [b-DIF] لأي معرف DID. ويمكن لأداة الحل العالمية المشاركة في طبقة استيقان للمعرفات DID القابلة للتشغيل البيني. ويمكّن استيقان المعرفات DID مالك الهوية من التحكم في المعرف DID أثناء تفاعله مع أي طرف معول. ويتطلب ذلك تنفيذ الطرف المعول للخطوات التالية:

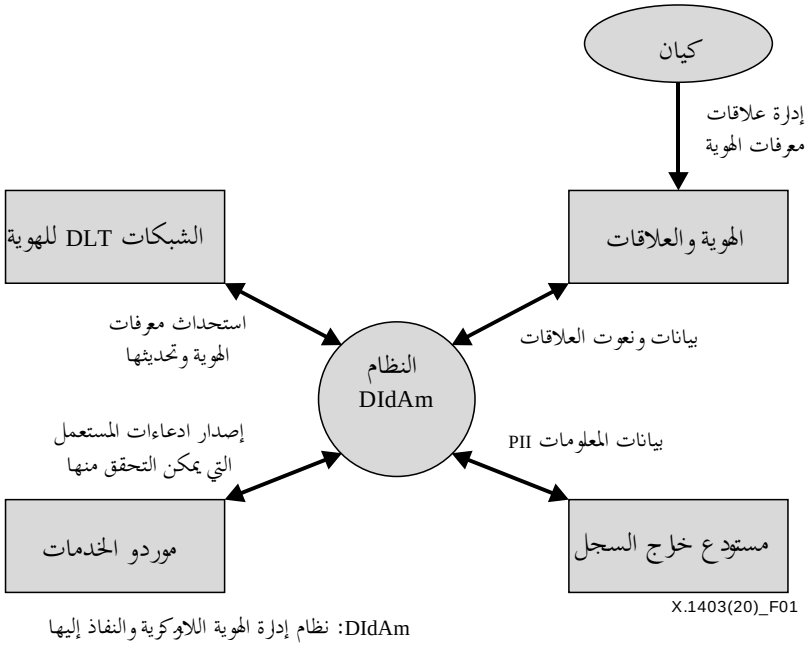
1) يحل الطرف المعول المعرف DID الخاص بمالك الهوية إلى وثيقة معرف DID على منصة DLT،

2) يحاول الطرف المعول استيقان مالك الهوية باستخدام غرض (أغراض) الاستيقان الموجود (الموجودة) في وثيقة المعرف DID على المنصة DLT،

3) يمكن لغرض (أغراض) الاستيقان أن يتضمن (تتضمن) غرضاً لمفتاح عمومي أو يحيل (تحيل) إليه، في الحالات التي ينشأ فيها إثبات مالك الهوية في صورة توقيع مجفر.

### 3.7 فوائد استخدام التكنولوجيا DLT في أنظمة إدارة الهوية اللامركزية والنفاذ إليها (DIdAm)

يمهد استخدام التكنولوجيا DLT كإطار ثقة لأنظمة الهوية اللامركزية الطريق أمام الموردين لتصميم أطر تمكنهم من التصرف كطبقة تجريد لبرمجيات وسيطة بين المستعمل وسجلات مختلفة. وتحتاج هذه التفاعلات إلى أنظمة تقليدية لإدارة الهوية والنفاذ إليها لإنشاء الإطار المناسب لدعم الأنظمة اللامركزية. وفي الأساس، يمكن الإشارة إلى عملية الدمج بين الأنظمة المركزية واللامركزية على أنها نظام لإدارة الهوية اللامركزية (DIdAm) [b-Angelov et al.]. وفي هذا الصدد، فإن النظام DIdAm [b-Angelov et al.] هو نظام مكون من أنظمة يمكنها التفاعل مع العديد من المنصات DLT التي تدعم نماذج الهوية اللامركزية القائمة على المعرفات DID. ويصور ذلك في الشكل 1.




**الشكل 1 – إطار النظام DIdAm**

وفيما يلي مكونات النظام DIdAm الذي يستخدم التكنولوجيا DLT:

1) مالك الهوية اللامركزية: هو كيان يدير هوياته اللامركزية باستعمال خدمات يقدمها النظام DIdAm عبر سجلات متعددة.

2) موردو الخدمات (SP): جهات الإصدار التي توفر الخدمات لمالكي الهويات (استحداث الهويات). مثلاً، الوكالات الحكومية مثل إدارة المركبات الآلية أو الشركات الخاصة مثل المؤسسات المالية.

3) مستودع هويات خارج السجل: هي قاعدة بيانات تخزن فيها نعوت هوية المستعمل وادعاءاته ومعلوماته العامة. ويتحكم المستعمل في مكان تخزين البيانات. وعادة ما تكون هذه البيانات بيانات PII حساسة ينبغي تخزينها خارج السجل. وينبغي للمستودع أن يوفر القدرة على قراءة وكتابة البيانات وفقاً لتقدير المستعمل.

4) يمكن اعتبار أنظمة الهوية القائمة على التكنولوجيا DLT أنظمة هوية منفصلة بحدود ثقة ومفاتيح تجفير مختلفة. وبالتالي، يجب أن يسهل النظام DIdAm التفاعلات بين السجلات نيابة عن المستعمل.

ويمكن تنفيذ خدمات النظام DIdAm داخلياً بواسطة الشركة أو ربما يقوم طرف ثالث ما بدور هؤلاء الموردين.

### 1.3.7 دعم الهوية اللامركزية عبر سجلات DLT متعددة

هناك الكثير من متطلبات السطوح البينية [b-Angelov et al.] اللازمة لدعم الهوية اللامركزية باستخدام المعرفات DID عبر سجلات DLT متعددة. وتنشأ الصعوبة من المتطلبات المتغيرة من إطار الثقة مثل نوع السجل DLT، وما إذا كان عاماً أو خاصاً. وينبغي أن يكون النظام DIdAm قادراً على دعم المستعمل أياً كانت تفضيلاته فيما يتعلق بنوع شبكة النفاذ إلى الاتصالات التي يستخدمها. ويبين الشكل 1 النظام DIdAm في صورة سطح بيني موحد تجاه مالك الهوية بمقدوره العمل على سجلات متعددة.

ويتصرف النظام DIdAm [b-Angelov et al.] كطبقة تجريد للمستعمل النهائي. فهو يمكن المستعمل من التفاعل مع العديد من السجلات DLT مع استخدام سطح بيني افتراضي وحيد. وسيتصرف النظام DIdAm أيضاً كطبقة تجريد للشركة حيث يمكن لأنظمة إدارة الهوية التقليدية التفاعل معه دعماً للوظائف الداخلية لإدارة الهوية المركزية. وتتمثل فائدة هذا التجريد في قدرة المستعمل على إدارة الهويات على أي عدد من السجلات. وسيمكن ذلك المستعمل من إنشاء علاقات مع الموردين مع القدرة على التحكم بصورة أفضل في هويته.

### 2.3.7 دعم خدمات الهوية

في الأنظمة DIdAm التقليدية، يستطيع مورد خدمة الهوية أن يشهد لدى الطرف المعول على هوية المستعمل. وينبغي للنظام DIdAm [b-Angelov et al.] أن يكون قادراً على دعم هذا الدور بوجه خاص لكي يكون متوافقاً عكسياً مع الأنظمة التقليدية. ويمكن للإجراءات التالية أن تدعم متطلبات الشهادة:

1) ينبغي للنظام DIdAm التصرف كشريك موثوق. وينبغي أن يضمن استحواذ مالك الهوية على إثباتات دقيقة وسليمة عبر إجراءات صحيحة لجهات الإصدار فيما يتعلق بالإثباتات التي يمكن التحقق منها.

2) الحد من خلافات تدقيق الهوية بالنسبة للمستعملين. فسيحتاج المستعمل عادة إلى عبور مرحلة تدقيق الهوية مع كل جهة إصدار. ويمكن لنظام DIdAm مصمم بشكل سليم أن يساعد المستعمل على التغلب على هذا القيد بأن يكون مشاركاً موثوقاً نشطاً في التفاعل.

3) التحقق من صحة البيانات في الوقت الفعلي: تعد البيانات غير الدقيقة مشكلة في الأنظمة التقليدية. ويمكن علاج هذه المشكلة بواسطة النظام DIdAm من خلال توفير خدمات تساعد الأطراف المعولة على القول بأن نعوت المستعمل ليست متقادمة.

4) إدارة الموافقات: الموافقة جزء لا يتجزأ من الامتثال. ويمكن للنظام DIdAm توفير خدمات للمستعملين وللطراف المعولة لضمان مراعاة الامتثال للموافقات.

### 3.3.7 إدارة سلسلة المفاتيح

يشير مصطلح سلسلة المفاتيح إلى مهمة تأمين تخزين المفاتيح الخاصة المرتبطة بمحفظة معينة على جهاز المستعمل. وهناك علاقة مباشرة من طرف إلى طرف بين المعرف DID والإثباتات التي يمكن التحقق منه ومورد الخدمة. وقد يكون الجهاز جهازاً متنقلاً أو جهاز قائم على متصفح. ولما كان النفاذ إلى المفاتيح الخاصة يستخدم في هذا النموذج للتحقق من صحة هوية المستعمل، فإن مهمة حماية أزواج المفاتيح تعد حاسمة لمنع الهجمات الاحتيالية على الهوية. وعند التعامل مع معرفات DID متعددة عبر العديد من السجلات DLT، يواجه المستعملون بمهمة حماية مجموعة من المفاتيح الخاصة التي تستخدم لإطلاق هوياتهم عبر فضاء الهويات بأكمله.

وسلسلة المفاتيح هي الهيكل الذي تخزن فيه المفاتيح الخاصة المقابلة للمعرفات DID الخاصة بالمستعملين بصورة مؤمنة. وهو هيكل يمتلكه مالك الهوية ويخضع لتحكم المفاتيح الخاصة التي تترجم إلى امتلاك معرفات DID. وينبغي لأي نظام DIdAm أن يكون قادراً على إدارة سلسلة المفاتيح نيابة عن المستعمل، لا سيما:

1) ينبغي أن يكون المستعمل قادراً على استخدام وظائف سلسلة المفاتيح وتخزينها خلال وجوده داخل ميدان النظام DIdAm.

2) ينبغي أن تخضع إدارة المفاتيح لسيطرة المستعمل.

3) ينبغي إدارة ومراجعة النفاذ إلى سلسلة المفاتيح.

4) يمكن للنظام DIdAm توفير الخدمات التي تمكن المستعمل من حفظ المحفظة واستعادتها.

## 8 مبادئ توجيهية أمنية بشأن استخدام التكنولوجيا DLT في النظام DIdAm

تحل الهوية اللامركزية بعض المشكلات الرئيسية المرتبطة بنماذج الهويات التقليدية والاتحادية. وتعد تكنولوجيا السجلات الموزعة عرضة لمخاطر الأمن السيبراني. وتشمل المخاطر الأمنية تلك المخاطر الناتجة عن الأخطاء البشرية مثل أخطاء تشفير البرمجيات.

وعموماً، ينبغي ألا ينشر (تنشر) المعرف (المعرفات) DID الخاص (الخاصة) بالمستعمل في سجل لا يستوجب الترخيص حتى وإن تطلب الأمر في بعض الحالات توفير معرف هوية فريد لكل مستعمليه. ومع ذلك، فإن البيانات التي تساعد المستعملين على الثقة في السجل، مثل المفاتيح العمومية لموردي خدمات الهوية وقوائم الإبطال والبيانات التي تعزز قابلية التشغيل البيني مثل مخططات الإثباتات المتغيرة، يمكن أن تكون معلومات للعامة على السجلات.

ويتناول هذا القسم الفوائد والتحديات والمخاطر الأمنية لنماذج الهوية اللامركزية.

### 1.8 الاعتبارات الأمنية للسجلات الموزعة

هناك نوعان واسعان من السجلات الموزعة، يصنفان كسجلات لا تستوجب الترخيص وسجلات تستوجب الترخيص. فالسجلات التي لا تستوجب الترخيص تسمح لأي كيان بالنفاذ إلى البيانات الموجودة على السجل ومشاهدتها واقتراح بيانات جديدة أو التحقق من صحة البيانات الموجودة طالما يتبع البرتوكولات المحددة للسجل. ويضمن السجل سرية البيانات وسلامتها وتيسرها واتساقها مع بروتوكولات الموافقة اللازمة لتوليد الثقة بين المشاركين الذين قد لا يثقون في بعضهم البعض. وتعمل السجلات التي لا تستوجب الترخيص، عموماً، بدون أي سلطة مركزية.

والسجل الذي يستوجب الترخيص هو نظام يتألف من أطراف موثوقة تمنح حقوق الاستعمال حسب دور كل منها في إطار الثقة. وفي هذا النموذج، يمكن لمشاركين منتقين تغيير بيانات السجل. ووفقاً لاتفاقات الثقة، يجوز لبعض السجلات السماح بالنفاذ المفتوح إلى السجل لقراءته.

ويضمن السجل الذي لا يستوجب الترخيص الثقة عبر بروتوكولات الموافقة التي هي عبارة عن نفقات حسابية ولها تأثير مباشر على صبيب وأداء نظام الهوية العامل على السجل. ومن جهة أخرى، تعتمد السجلات التي تستوجب الترخيص على الثقة بين مستحدثي السجلات للتأكد من أن أمن بيانات السجل يشمل بيانات الهوية. وبوجه عام، تعد السجلات التي تستوجب الترخيص أسرع وأكثر اقتصاداً من السجلات التي لا يستوجب الترخيص.

### 2.8 فوائد استخدام المعرفات DID في التكنولوجيا DLT

تحقق الهوية اللامركزية الفوائد التالية:

1) تنقلية الهوية: تضمن المعرفات DID اللامركزية تحكم الأفراد في هوياتهم الرقمية. وهي تنهي الاعتماد على موردي خدمات الهوية المركزيين. ونظرياً، يمكن للأفراد امتلاك معرفات هوياتهم وعلاقاتهم الخاصة بهم والتحكم فيها وإدارتها.

2) تشجع خدمات الهوية القائمة على العلاقات: تمكن المعرفات DID الكيانات من استحداث معرفات هوية رقمية لكل العلاقات تقريباً. وتحافظ المعرفات DID المكونة من أزواج مستعارة على البيانات PII.

3) تقلل إلى أدنى حد من المخاطر الأمنية: تلزم الهويات DID مالكي معرفات الهوية بإثبات الملكية بإثبات معرفتهم بالمفاتيح الخاصة المرتبطة بالمفاتيح العمومية المقابلة. ويتم التحقق من صحة الإثباتات دينامياً على السجل DLT في الوقت الفعلي. ويمكن إجراء التحقق دون الحاجة إلى مخدمات مركزية، مما يقلل من فضاء الهجمات.

4) توزيع التكلفة: التحقق من صحة الهوية على سجل DLT يمكن أن يستفيد من القدرة على استخدام المعرف DID في إعادة استعمال إثبات الهوية عبر المشاركين في السجل DLT. ويقلل هذا الأمر من التكلفة ويعزز الأمن.

5) المعلومات PII حسب التصميم: خدمات المعرفات DID ذات السيادة اللامركزية توزع المخاطر الناجمة عن استعمال مخازن البيانات المركزية في تخزين معلومات المستعمل ومن ثم تزيد من الصعوبات التي يواجهها المهاجمون.

6) التبادل الموافق عليه والمتتبع للبيانات الشخصية: توفر المعرفات DID القدرة على تبادل البيانات بين المستعملين والموردين استناداً إلى سياسات متفق عليها، مما يحسن قدرة المستعملين على حماية بياناتهم.

7) الاتحاد الدينامي والمحسن: استعمال المعرفات DID داخل سجل DLT يوسع نطاق الثقة ليشمل جميع المنظمات المشاركة في النظام الإيكولوجي. ويمكن للمشاركين التركيز على تقديم الخدمات مع عدم التركيز على تفاصيل الاتحاد وكيفية تأسيسه.

8) تحمل الأعطال: الطابع اللامركزي للسجل DLT يوفر درجة من تحمل الأعطال وقدرة على الصمود للبنى التحتية.

### 3.8 التهديدات ومواطن الضعف

للسجلات الموزعة قدرات متوارثة تحد من مخاطر الأمن السيبراني على نظام تكنولوجيا المعلومات والاتصالات. وفيما يلي بعض أمثلة السمات الأمنية المحسنة:

1) زيادة قدرة النظام على الصمود: المعمارية الموزعة لأي سجل DLT، والتي تمنعه من التحول إلى نقطة فشل وحيدة.

2) تحسين المتانة: تحسن آليات الموافقة من السلامة العامة للسجلات الموزعة، لأن موافقة المشاركين ضرورية قبل قبول أي بيانات جديدة في السجل.

3) زيادة الشفافية: يصعب بشكل أكبر على البرمجيات الخبيثة العمل داخل السجل DLT لأن للنظام العديد من الطبقات المنفصلة من الأمن على مستوى البنية التحتية للسجل.

وأنظمة الهوية اللامركزية التي تبنى باستخدام التكنولوجيا DLT سترث المخاطر الأمنية من هذه التكنولوجيات. وإلى جانب ذلك، هناك مخاطر أمنية تتعلق باستخدام التكنولوجيا DLT في إدارة الهوية.

#### 1.3.8 إدارة بيانات الهوية

ترمز CRUD إلى استحداث–قراءة–تحديث–حذف. وهذه هي العمليات الأساسية لقاعدة بيانات التخزين التقليدية. وفي السجل DLT، خاصة مع سلسلة الكتل المرخصة، لا تستطيع كيانات التنفيذ حذف معاملات مكتوبة على واحدة من سلاسل الكتل. حتى تحديث المعاملات الموجودة لا يمكن إجراؤه لأنها غير قابلة للتحوير. وبالتالي لا يمكن اعتبار العمليات "CRUD" عمليات اعتيادية للتعامل مع بيانات المستعمل.

وبدلاً من ذلك يمكن وصف العمليات على سلسلة الكتل بالرمز CRAB: استحداث واستعادة وتعليق وحرق. والتعليق الذي يحل محل تحديث، يعني أن المنفذين يمكنهم فقط تعليق المعاملات الجديدة في تكنولوجيا سلسلة الكتل، ومن ثم تغيير "حالة العالم" (مجموع جميع الأحداث/المعاملات السابقة حتى الآن). تعني عملية الحرق في الرمز CRAB أنك تلقي بمفاتيح التجفير بعيداً، ومن ثم لا يمكنك تعليق معاملات جديدة أو إجراء أي تغييرات أخرى على حالة السجل الخاص بالأصل المعني.

وبالتالي، من المهم إيلاء عناية كافية لكتابة البيانات الشخصية على سجل DLT أو إحدى سلاسل الكتل مادامت البيانات غير قابلة للسحب أو النسيان في المستقبل. وفي هذا الصدد، من الأفضل كتابة البيانات خارج السلسلة مع إدراج مؤشرات في السجل DLT إلى البيانات الموجودة خارج السلسلة. ولذلك توجد أيضاً عيوب لتخزين البيانات خارج السجل. وهي على وجه الخصوص:

- تقل فائدة الشفافية لأن المستعملين لن يكونوا على علم بأنه غير مخول لهم النفاذ إلى البيانات خارج السجل.
- تقل فائدة ملكية البيانات مع سلسلة الكتل مادامت البيانات، بمجرد وجودها خارج السجل، يمكن لأي كيان يستطيع النفاذ إليها تملكها.

#### 2.3.8 القدرة على ربط مفاتيح المعرفات DID

هناك إمكانية لحقيق ارتباط بين المعرفات DID. ويمكن تحقيق ذلك إذا استخدم المعرف DID نفسه بين أكثر من علاقة. ويمكن للسجلات DLT أن تخفف من حدة هذا الخطر باستخدام معرفات DID مكونة من أزواج للعلاقات. ويعني ذلك أن كل زوج من المعرفات DID المستعملة مختلف بالنسبة لكل علاقة. وفي هذا السيناريو، يتصرف كل معرف DID كمعرف مستعار [b-W3C-2]. ويحتاج المعرف DID المستعار إلى أن يتقاسم فقط مع أكثر من طرف عندما ترخص الجهة المعنية بالمعرف DID صراحة بالارتباط بين هذه الأطراف.

وكنقطة نظام، يمكن حتى للمعرفات DID المستعارة الارتباط [b-W3C-2] إذا كان يمكن تحقيق الارتباط للبيانات الموجودة بوثائق المعرفات DID المقابلة. فمثلاً، يمكن اللجوء إلى استخدام أسماء نقاط طرفية مشتركة للخدمات في وثائق متعددة للمعرفات DID لربط المعلومات المتعلقة بالمعرف DID نفسه. ومن ثم، تحتاج وثائق المعرفات DID المتعلقة بمعرفات DID مستعارة هي الأخرى إلى استخدام مفاتيح عمومية فريدة مكونة من أزواج.

### 3.3.8 حماية مفاتيح المعرفات DID

إدارة المفاتيح الخاصة أمر هام. فإذا تم تخزين مفتاح رئيسي في موقع غير مأمون حتى ولو على جهاز وحيد، فإن من المرجح حدوث سرقة للهوية. وينبغي أن يكون من بين المتطلبات استخدام وسائل تخزين مأمونة على الأجهزة.

### 4.3.8 تقنيات حفظ المعلومات PII

يوصى بعدم تخزين معلومات حساسة في السجل. وسيؤدي ظهور الحوسبة الكمومية إلى التأكد من أن كل تقنية تجفير ثنائية الاتجاه يمكن أن تتعرض للتصدع بمرور الوقت، وبالتالي فإن الهدف يتمثل في عدم تخزين أي معلومات حساسة في السجل.

وبالرغم من أن عمليات الاختزال عمليات وحيدة الاتجاه، فإنها يمكن أن تكون حساسة نظراً إلى أن القراصنة لديهم وقت غير محدود لمحاولة الهجوم الكاسح على المعلومات المختزلة. لذا، ينبغي عدم تخزين معلومات مختزلة في السجل.

وبدلاً من تخزين بيانات غير معالجة مثل تاريخ الميلاد في السجل، يمكن تخزين أجوبة على أسئلة تنص مثلاً على أن شخصاً ما أكبر من 21 سنة داخل عقد ذكي في السجل. ويمكن اعتبار ذلك كادعاء يمتثل لمتطلب ما.

ويوصى بألا تخزن إلا المعلومات المختزلة لبيانات خاصة أو حساسة في السجل DLT. ولا ينبغي تخزين المعلومات PII في السجل، حتى وإن كانت مجفرة. وينبغي تخزين البيانات الحساسة خارج السجل وينبغي تبادلها بين الكيانات المعتمدة التي تحتاج إلى استهلاك البيانات. ويحد هذا النهج من مخاطر أن يؤدي انتهاك للسجل DLT إلى فقدان بيانات حساسة. وينبغي استخدام تكنولوجيا بين النظراء مأمونة في عمليات تبادل البيانات الداعمة للنفاذ إلى البيانات خارج السجل. وينبغي استخدام تقنيات مناسبة لتخزين البيانات خارج السجل، بما في ذلك خطط لأرشفة البيانات واستعادتها. فمثلاً، إذا ادعى مالك هوية أنه مورد مرخص للخدمات التأمينية، فإنه يمكن التحقق من الادعاء بواسطة كيان يقوم بدور المورد الموثوق في نظام هوية لامركزية ويخزن الإثبات في السجل DLT في صورة مختزلة. ويمكن للإثبات أن يكون الاختزال للادعاء الموقع رقمياً من المدعي. وينبغي ضمان أمن المستودع خارج السجل.

### 5.3.8 تقييدات البائعين

يمكن تقييس السجلات، ومع ذلك فإن مكونات البرمجيات محددة لحل بعينه وقد تكون مسجلة الملكية وغير قابلة للتشغيل البيني.

### 6.3.8 الهجمات القائمة على الهوية

السجل الموزع عرضة للهجمات القائمة على الهوية كتلك التي تستهدف البنية التحتية التقليدية لتكنولوجيا المعلومات، مثل هجمات التحايل واستخدام هويات مزورة. والأطراف من ذوي النوايا الخبيثة يمكنهم استخدام هذه الهجمات للسيطرة على معظم عقد السجل. ويمكن للمهاجم، إذا نجح، أن يقوض عملية التحقق من صحة الموافقات ووسائل حماية المعمارية الموزعة. ويمكن تخفيف حدة هذه المخاطر باستعمال حلول استيقان قوية من أجل خدمات الدليل القائمة على الحوسبة السحابية.

### 7.3.8 تأثيرات شبكات الاتصالات

الهيكل الموزع للتكنولوجيا DLT يمكن أن يفرز مشكلات تشغيلية عند التعامل مع الحالة التي يشارك فيها الكثير من الأطراف الفاعلة كل بالحلول الخاصة به لحماية البنية التحتية للاتصالات. ويفرض هذا الهيكل تحديات فيما يتعلق بإدارة الهويات والتحكم في النفاذ والتشكيلات الأمنية وتخزين مفاتيح البنية التحتية للمفاتيح العمومية وإدارتها.

وتحتاج عمليات السجلات DLT إلى تشغيل عقد تستخدم طوبولوجيا مختلفة لشبكات الاتصالات وشفرات برمجيات وبروتوكولات مختلفة قد تكون عرضة لتهديدات أمنية. ويختلف أثر هذه التهديدات باختلاف طابع السجل DLT (خاص أم عمومي). ومن هنا، فإن أنظمة إدارة الهوية وبيانات الهوية تكون عرضة لهجمات على مستوى شبكة الاتصالات تستهدف السجلات DLT. وينبغي لمصممي أنظمة إدارة الهوية مراعاة المسائل على مستوى شبكة الاتصالات والتي تشمل:

1) الأثر على بيانات الهوية في حالة فشل خوارزمية الموافقات بالسجل DLT.
2) كيف يتم التعامل مع المصادمات بين السجلات DLT أو سلاسل الكتل؟

3) ماهي خطة الاستعادة في حالات الكوارث بالنسبة لبيانات الهوية؟

4) ما هي التهديدات التي تواجهها بيانات الهوية في حالة تحكم مجموعة صغيرة من المشاركين في آليات الموافقة للسجل DLT؟

### 8.3.8 تجفير بيانات الهوية

تعتبر بيانات الهوية المخزنة خارج السجل سرية وخاصة بالنسبة لمالك الهوية. وينبغي أن يكون بمقدور المستعمل الحصول على المساعدة من السجل فيما يتعلق بتجفير البيانات سواء كان جملة واحدة أو أثناء الإرسال خاصة عند تقاسم البيانات بين موردين مختلفين.

### 9.3.8 الرديف

هناك مخاطر على المستعمل فيما يتعلق بحماية جهازه ومكوناته من حيث الادعاءات التي يمكن التحقق منها أو المفاتيح الخاصة أو البيانات الشخصية.

وهناك حاجة إلى آلية جيدة لاسترجاع البيانات واستعادتها بالنسبة لمحفظة المستعمل.

وإضافة إلى ذلك، سيحتاج المستعمل إلى ضمان بأن بياناته محمية ولها نسخ احتياطية في السجل. وينبغي توفير التقنيات التي تضمن عدم تعرض البيانات للإتلاف أو الفقد كخدمات للمستعمل النهائي.

### 10.3.8 العقود الذكية

قد يلزم استخدام العقود الذكية عند تنفيذ أنظمة الهوية اللامركزية. ويتولى المطورون تحرير العقود الذكية باستخدام لغات البرمجة الحاسوبية. وهذه البرامج عرضة للتطوير وأخطاء البرمجة خاصة مع تزايد تعقد العقود الذكية. وحالات عدم اليقين فيما يتعلق بدقة هذه العقود تحتاج إلى تطوير إطار حاكم يضمن تمتع أنظمة الهوية اللامركزية بالعمليات والإجراءات المثلى لمواجهة أي قيود تنتج عن العقود الذكية غير الدقيقة سواء كانت عن قصد أو عن غير قصد.

### 11.3.8 إدارة شهادات السجلات DLT

تتضمن أنظمة إدارة الهوية مهمة إدارة دورة حياة الهوية والتي تشمل مهام تدقيق الهوية. وتشمل المهام المتعلقة بإدارة الهوية استحداث الإثباتات وإصدارها وتخزينها وإبطالها واستبدالها والكشف عن الاحتيال.

ويفرض استخدام الشهادات في السجلات بعض التحديات المتفردة على الممارسين الأمنيين. ففي أنظمة الهوية اللامركزية، هناك سعر أعلى يجب دفعه في حالة فقدان المفاتيح الخاصة أو عدم وجودها في مكانها الصحيح مقارنة بأنظمة النفاذ التقليدية. فمثلاً، في حالة فقدان المفاتيح الخاصة لمحفظة مستعمل، فإن نفاذ المستعمل إلى السجل DLT الخاص به يتعرض للعجز الدائم. وسيحدث ضرر أكبر في حالة سرقة المفاتيح، لأن إظهار الشغف بالمفاتيح الخاصة يعادل سرقة الهوية. وصعوبة آليات الاستعادة هي أيضاً من دلائل طبيعة السجلات DLT. ومن الأسهل التعامل مع هذه المسائل في السجلات الخاصة على عكس السجلات التي لا تستوجب الترخيص وتحتاج إلى موافقات بشأن المعاملات.

وينبغي إدراج هذه المسائل عند تصميم الأنظمة الحاكمة للسجلات DLT طالما لا توجد سلطة مركزية للتعامل مع الاحتيال أو لتذليل المصاعب التقنية. ويتطلب ذلك أطر حاكمة للثقة للتأكد من أن جميع حالات دورة حياة الهوية مغطاة من البداية وأن هناك إجراءات جيدة متفق عليها بين جميع المشاركين في السجل DLT لدعم خدمات استعادة الهوية مثل: إدارة دورة حياة المفاتيح، وما هي الأجزاء المجفرة من الحمولة النافعة، وكيفية إبطال المفاتيح، وكيفية حماية المفاتيح الخاصة واستعادتها، وما الذي يتم عمله في حالة الكشف عن نشاط احتيالي.

# بيبليوغرافيا


[b-RFC 8141] RFC 8141, *Uniform Resource Names (URNs)*, April 2017.

[b-Angelov et al.] Angel Angelov, Mihail Milkov, Markus Sørensen, *Decentralized Identity Management System for Self-Sovereign Identity*, https://projekter.aau.dk/projekter/files/281068659/Master_Thesis_ICTE4SER4.2.pdf.

[b-Baars] Djuri Baars, *Towards Self-Sovereign Identity using Blockchain Technology*, https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf.

[b-Blog] Blockchain platforms, https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b.

[b-DIF] Decentralized Identity Foundation (DIF), https://identity.foundation/#wgs.

[b-Gartner] Gartner, Blockchain, *Evolving Decentralized Identity Design*, Published 1 December 2017 – ID G00324208, By Analysts Homan Farahmand.

[b-Sovrin] Sovrin Foundation, https://sovrin.org/.

[b-W3C-1] W3C, *Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web*, https://www.w3.org/TR/2019/CR-vc-data-model-20190725/.

[b-W3C-2] W3C, *Decentralized Identifiers (DIDs) v0.13 Data Model and Syntaxes*, August 2019, https://w3c-ccg.github.io/did-spec/.

## 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