الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

F.747.10

(2022/01)

السلسلة F: خدمات الاتصالات غير الهاتفية

خدمات الوسائط المتعددة

متطلبات أنظمة السجلات الموزَّعة من أجل خدمات العوامل البشرية الآمنة

التوصية ITU-T F.747.10

توصيات السلسلة F الصادرة عن قطاع تقييس الاتصالات

خدمات الاتصالات غير الهاتفية

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

التوصية ITU-T F.747.10

متطلبات أنظمة السجلات الموزَّعة من أجل خدمات العوامل البشرية الآمنة

ملخص

تقدم التوصية ITU-T F.747.10 المتطلبات العامة والقدرات الوظيفية لأنظمة السجلات الموزَّعة (DLS) من أجل خدمات العوامل البشرية الآمنة.

وتصف هذه التوصية المتطلبات الخاصة بنموذج خدمة السجلات الموزعة للعوامل البشرية الآمنة، والذي يمكن أن يحل مشكلة الأهداف المتضاربة لحماية الخصوصية واستخدام بيانات العوامل البشرية الشخصية الضخمة. وتشمل هذه التوصية أيضاً القدرات الوظيفية للعقد المشتركة للسجلات الموزعة للعوامل البشرية لتنفيذ تعلم الآلة دون فك تجفير بيانات العوامل البشرية المجفرة. ومع ذلك، قد يكون العبء الحاسوبي لتعلم الآلة بالنسبة للبيانات المجفرة مفرطاً. ولحل هذه المعضلة، يوفر نموذج خدمة السجلات الموزعة للعوامل البشرية هذا إجراءات للسماح باستخدام اثنين أو أكثر من أزواج مفاتيح التجفير والإخطار بنوع المفتاح. بالإضافة إلى ذلك، تتضمن هذه التوصية متطلبات الحفاظ على السلامة لخدمات العوامل البشرية الآمنة للحفاظ على سجلات موزعة آمنة والتحقق منها من البداية لتوزيع معلومات العوامل البشرية الشخصية. لذلك، فإن تطبيق أنظمة السجلات الموزعة في توزيع معلومات العوامل البشرية الشخصية الآمنة يمكن أن يضمن التتبع الشفاف بدءاً من عملية التوزيع وصولاً إلى مسار الاستعمال النهائي.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T F.747.10	2022-01-17	16	11.1002/1000/14644

مصطلحات أساسية

نموذج خدمة السجلات الموزعة؛ توسيع حماية الخصوصية؛ العوامل البشرية الآمنة؛ تتبع الشفافية.

* للنفاذ إلى التوصية، يرجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب، متبوعاً بمعرف التوصية الفريد. مثال 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، كان الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع/حقوق تأليف ونشر البرمجيات 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 قواعد البيانات المناسبة لدى قطاع تقييس الاتصالات المتاحة من خلال الموقع الإلكتروني لقطاع تقييس الاتصالات عبر الرابط: http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T F.747.10

متطلبات أنظمة السجلات الموزَّعة من أجل خدمات العوامل البشرية الآمنة

1 مجال التطبيق

تصف هذه التوصية متطلبات أنظمة السجلات الموزعة (DLS) من أجل خدمات العوامل البشرية الآمنة، وتضم:

- الخلفية؛
- المتطلبات العامة لأنظمة السجلات الموزعة من أجل خدمات العوامل البشرية الآمنة؛
- القدرات الوظيفية لأنظمة السجلات الموزعة من أجل خدمات العوامل البشرية الآمنة.

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 للمراجَعة، يُشجع جميع مستعملي هذه التوصية على بحث إمكانية 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

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الفدرة (block) [b-ISO 22739]: بيانات مهيكلة تضم بيانات الفدرة ورأسية للفدرة.

2.1.3 التوافق (consensus) [b-ISO 22739]: اتفاق بين عقد تكنولوجيا السجلات الموزعة على 1) أنه قد تم التحقق من صحة المعاملة و2) أن السجل الموزع يتضمن مجموعة متسقة من المعاملات التي تم التحقق من صحتها وترتيبها.

3.1.3 التوقيع الرقمي (digital signature) [b-ISO 22739]: بيانات، عندما تُلحق بشيء رقمي، تمكِّن مستعمل هذا الشيء الرقمي من استيقان منشأه وسلامته.

4.1.3 السجل الموزع (distributed ledger) [b-ISO 22739]: سجل يتم التشارك فيه عبر مجموعة من عقد تكنولوجيا السجلات الموزعة وهو متزامن بين عقد تكنولوجيا السجلات الموزعة باستخدام آلية توافق.

5.1.3 تكنولوجيا السجلات الموزعة (distributed ledger technology) [b-ISO 22739]: تكنولوجيا تمكِّن من تشغيل السجلات الموزعة واستخدامها.

6.1.3 التفريع (fork) [b-ITU-T TS FG DLT D1.1]: استحداث نسختين مختلفتين أو أكثر من السجل الموزع.

7.1.3 قيمة الاختزال (hash value) [b-ISO 22739]: سلسلة من البتات هي خرج دالة اختزال تجفيرية.

8.1.3 الصحة (health) [b-WHO]: الصحة هي حالة من اكتمال السلامة البدنية والعقلية والاجتماعية ينعدم فيه المرض والعجز.

9.1.3 السجل (ledger) [b-ISO 22739]: مخزن معلومات يحفظ سجلات المعاملات المزمع أن تكون نهائية وباتة وغير قابلة للتغيير.

10.1.3 شجرة ماركل (Merkle tree) [b-NIST]: هيكل بيانات تُختزل فيه البيانات وتُجمع حتى يتم الحصول على دالة اختزال جذرية مفردة تمثل هيكل البيانات بأكمله.

11.1.3 استخلاص البيانات (mining) [b-ITU-T F.751.0]: نشاط البحث عن ضالة في بعض آليات التوافق.

12.1.3 العقدة (node) [b-ISO 22739]: المكون الأولي الذي يتم من خلاله بناء هيكل البيانات.

13.1.3 نظام السجلات الموزعة العمومي (public distributed ledger system) [b-ITU-T F.751.0]: نظام لتكنولوجيا السجلات الموزعة يمكن للعامة النفاذ إليه لاستخدامه.

14.1.3 المعاملة (transaction) [b-ISO 22739]: أصغر وحدة في عملية أي عمل، وهي عبارة عن تتابع واحد أو أكثر من الأعمال المطلوبة لتحقيق نتيجة تتوافق مع القواعد الحاكمة.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 عمق الفدرة (block depth): مستوى الكتلة الملحقة بسلسلة نظام السجلات الموزعة من الفدرة الأولية.

2.2.3 سجلات العوامل البشرية الكهربائية (electronic human factor records): الجمع المنهجي لمعلومات العوامل البشرية المخزنة إلكترونياً للأشخاص والسكان بنسق رقمي.

3.2.3 العوامل البشرية (human factor): مبادئ تصميم الظروف المثلى لنمط الحياة فيما يتعلق برفاهية الإنسان وسلامته وصحته، بما في ذلك تطوير التكنولوجيات الحالية وحيازة تكنولوجيات جديدة.

ملاحظة – بتصرف من [b-ISO 6385] و[b-Wickens].

4.2.3 معلومات العوامل البشرية الشخصية (personal human factor information): المعلومات التي يتم جمعها عن طريق القياس المباشر لجسم الإنسان وبيئاته والتي يتم إرسالها إلى أجهزة العوامل البشرية الشخصية أو غيرها من الأجهزة من خلال شبكة اتصالات لاستخدامها في سجلات العوامل البشرية الإلكترونية.

5.2.3 جهاز العوامل البشرية الشخصية (personal human factor device): نوع من الأجهزة يقيس جسم الإنسان وبيئاته، ويتبادل المعلومات التي يتم جمعها مع أجهزة العوامل البشرية الأخرى.

6.2.3 عوامل بشرية آمنة (secure human factor): العوامل البشرية في أمن المعلومات.

4 المختصَرات والمختزَلات

تستعمل هذه التوصية المختصَرات والمختزَلات التالية:

CPU وحدة المعالجة المركزية *(Central Processing Unit)*

DLS أنظمة السجلات الموزعة *(Distributed Ledger Systems)*

DLT تكنولوجيا السجلات الموزعة *(Distributed Ledger Technology)*

IP بروتوكول الإنترنت *(Internet Protocol)*

PDLS أنظمة السجلات الموزعة العمومية *(Public Distributed Ledger Systems)*

UUID معرّف هوية فريد عالمياً *(Universally Unique Identifier)*

VRF دالة عشوائية يمكن التحقق منها *(Verifiable Random Function)*

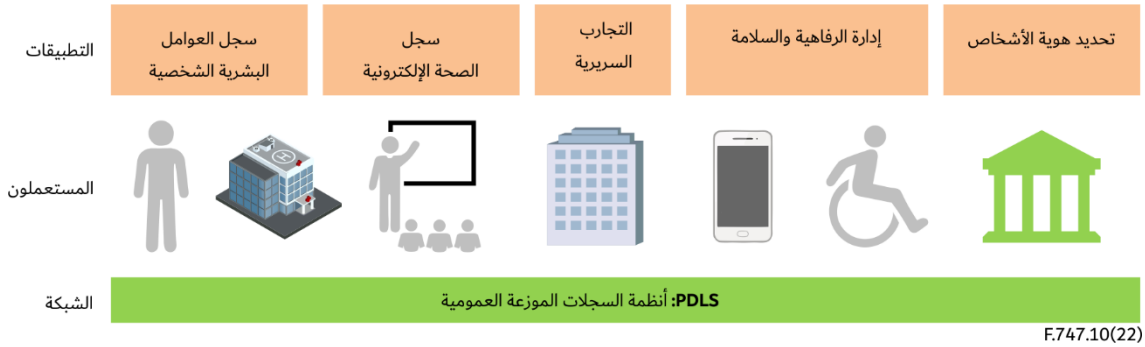
5 الاصطلاحات

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

- "يجب" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.
- "يوصى" كلمة تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.
- "من الجائز" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه التوصية في نفس الوقت.

6 خلفية

في السنوات الأخيرة، زادت معلومات العوامل البشرية الشخصية بشكل كبير بسبب تطوير أجهزة جمع معلومات الصحة الشخصية بالإضافة إلى بيانات السجلات الطبية الشخصية في المستشفيات. ويعد نموذج خدمة السجلات الموزعة أحد أفضل النماذج لإدارة وتبادل بيانات العوامل البشرية الشخصية. وتوفر خصائص أنظمة السجلات الموزعة الموثوقية باستخدام قاعدة بيانات موزعة مع وجود عدة عقد، وتضمن شفافية استرجاع البيانات باستخدام التوقيعات الرقمية وقيم دوال الاختزال. ومع ذلك، يمكن أن تكون بيانات العوامل البشرية حساسة للغاية من حيث حماية المعلومات. لذلك، يلزم نموذج خدمة السجلات الموزعة العمومية متطلبات حماية معلومات العوامل البشرية الشخصية (انظر الشكل 1).



الشكل 1 – نموذج خدمة السجلات الموزعة للعوامل البشرية

وتصف هذه التوصية المتطلبات الأمنية لنموذج خدمة السجلات الموزعة للعوامل البشرية، والذي يمكن أن يحقق أهداف حماية الخصوصية واستخدام البيانات الضخمة للصحة الشخصية. وتقدم التوصية أيضاً المتطلبات الوظيفية للعقد المشتركة للسجلات الموزعة لتنفيذ تعلم الآلة دون فك تجفير البيانات المجفرة. وتصف متطلبات الحوافز في نموذج خدمة السجلات الموزعة لتحسين جودة الحياة عن طريق أتمتة توزيع المنتجات الصحية مباشرة إلى المستهلكين والمنتجين. ويبدأ تطبيق تكنولوجيا السجلات الموزعة بالقدرة على تتبع وإدارة إنتاج المعلومات الصحية وتوزيعها. بمعنى آخر، يمكن أن يضمن تطبيق تكنولوجيا السجلات الموزعة في توزيع معلومات العوامل البشرية الشخصية تتبعاً شفافاً بدءاً من عملية التوزيع وصولاً إلى مسار الاستعمال النهائي. ولهذا السبب، يمكن للأفراد الذين تمثلهم العقد الفردية المشاركة في نظام السجلات الموزعة الوثوق بالمعلومات الموزعة واستخدامها. بالإضافة إلى ذلك، من الممكن توفير طريقة لمنع التوزيع غير القانوني لمعلومات العوامل البشرية الشخصية من الأساس.

7 المتطلبات العامة لأنظمة السجلات الموزعة من أجل خدمات العوامل البشرية الآمنة

تصف هذه الفقرة متطلبات إجراء إدارة حركة السجلات الموزعة الآمنة الذي يمكن أن يحقق الأهداف المتضاربة لحماية المعلومات الشخصية واستخدام البيانات الضخمة لمعلومات العوامل البشرية الشخصية. وتقدم المتطلبات الوظيفية لأي عقدة مشتركة في السجلات الموزعة لتعلم الآلة دون فك تجفير البيانات المجفرة. فعلى سبيل المثال، يعد التجفير المتماثل أحد تقنيات التجفير التي يمكنها إجراء جميع العمليات الحاسوبية التي يقوم بها أي حاسوب دون فك التجفير حتى في وجود حالة مجفرة. وحتى عند تحليل البيانات الذي يشمل معلومات شخصية تلزم حمايتها، يمكن تنفيذ تعلم الآلة اختيارياً دون تسرب المعلومات الشخصية أو فقدان البيانات.

1.7 المتطلبات الوظيفية للعقد المشتركة في السجلات الموزعة العمومية

فيما يلي المتطلبات الوظيفية للعقد المشتركة في السجلات الموزعة العمومية:

- لا بد للعقد من تخزين بيانات سلسلة السجلات الموزعة المتراكمة من الفدرة الأولى.
- يجب تسليم حالة الانتهاء من العملية إلى العقد الأخرى، حيث تقوم العقدة بتنفيذ خوارزمية تأكيد موزعة، عند التحقق من صحة المعاملة.
- من أجل التحقق من صحة السجل الموزع الذي يتم إنشاؤه في كل جولة، لا بد أن تقوم العقدة بالتحقق من صلاحية الفدرة التي تم إنشاؤها من خلال مقارنتها بقيمة دالة الاختزال المستهدفة.
- لا بد أن تقوم كل عقدة بتحديث وصيانة البيانات المشتركة مثل قائمة المفاتيح العمومية لجميع العقد الأخرى والسجل الموزع.
- يجب أن تقوم العقدة بنشر المعاملة إلى العقد الأخرى حتى مرحلة الاتفاق (على سبيل المثال، الانتهاء من تأكيد المعاملة) في عملية التحقق من المعاملة.
- يجب أن تقوم العقدة بتجفير بيانات المعاملة التي تتطلب الأمن باستخدام مفاتيح التجفير (على سبيل المثال، شهادة المفتاح العمومي [b-ITU-T X.509]، التجفير المتماثل [b-ISO 18033-6]، الدالة العشوائية التي يمكن التحقق منها (VRF) [b-IETF draft-irtf-cfrg-vrf-08]) والإبلاغ عن نوع مفتاح التجفير.
- يلزم أن تقوم العقدة بتحديد ما إذا كان فك التجفير ضرورياً. فإذا كانت هناك حاجة إلى فك التجفير، تقوم العقدة بفك تجفير البيانات وإرسالها إلى العقدة الطالبة. وإذا لم تكن هناك حاجة إلى فك التجفير، تقوم العقدة بتجفير البيانات بالمفتاح العمومي للعقدة الطالبة، وإرسالها.

2.7 متطلبات الاستيقان لعقدة جديدة مشاركة

يوصى بأن توفر العقد القائمة الوظائف المبينة في الفقرات من 1.2.7 إلى 3.2.7، لاستيقان العقد المشاركة الجديدة في أي نظام مشترك للسجلات الموزعة.

1.2.7 متطلبات طلب استيقان عقدة جديدة

- يوصى بأن تحتوي العقدة الجديدة على زوجين على الأقل من مفاتيح التجفير لاستخدامهما (على سبيل المثال، شهادة المفتاح العمومي [b-ITU-T X.509]، مفاتيح التجفير المتجانسة [b-ISO 18033-6]) قبل تقديم الطلب.
- يوصى بأن تقوم العقدة الجديدة بتجفير رسالة الطلب بمفتاحها الخاص وإرسال البيانات المجفرة ومفتاحها العمومي معاً إلى العقدة.
- يوصى بأن تقوم كل عقدة بتحديث قائمة المفاتيح العمومية التي تم التحقق منها للعقد الجديدة والقائمة وتخزين قائمة المفاتيح العمومية لنظام السجلات الموزعة المشترك للمشاركة، عندما تتحقق العقدة من المعلومات المستيقن منها وترسلها.

2.2.7 المتطلبات الوظيفية للاستيقان بالنسبة للعقدة

- يوصى بأن تقوم العقدة بالتحقق من الصلاحية عن طريق فك تجفير البيانات المجفرة المرسلة من العقدة المرغوبة المشاركة الجديدة المستلمة مع المفتاح العمومي، لتجفير المعلومات التي تم التحقق منها وقائمة المفاتيح العمومية بالمفتاح العمومي للعقدة الجديدة وإرسال المعلومات المجفرة.
- يوصى بأن تكون للعقدة قائمة بالمفاتيح العمومية لجميع العقد المشاركة في نظام السجلات الموزعة المشترك وتحديث قائمة المفاتيح العمومية المقابلة لها في كل مرة تتعامل فيها مع استيقان للعقدة الجديدة.
- في كل مرة يوصى فيها بأن تقوم العقدة بتحديث قائمة مفاتيحها العمومية، يلزم تجفير قائمة المفاتيح العمومية بمفتاحها الخاص وإرسالها إلى جميع العقد المشاركة في نظام السجلات الموزعة المشترك.
- يوصى بأن تقوم العقدة بتخزين المعلومات التي تم التحقق منها عن العقد المشاركة بشكل دائم في نظام السجلات الموزعة المشترك مع وقت التحقق وعنوان العقدة المشاركة.

3.2.7 متطلبات التحقق من استيقان العقدة الجديدة للعقد القائمة

- يوصى بأن تقوم العقد القائمة بالتحقق من التوقيع الرقمي لقائمة المفاتيح العمومية المرسلة من العقدة وتحديثها بقائمة المفاتيح العمومية الجديدة.
- يوصى بأن تقوم العقد القائمة بالتحقق من مشاركة العقدة الجديدة المستيقن منها عن طريق التحقق من قائمة المفاتيح العمومية الجديدة.

3.7 المتطلبات الأمنية لأنظمة السجلات الموزعة

يوصى بأن تتبع العقد القائمة الأحكام الواردة في هذه الفقرة.

- يجب التحقق من محاولات التلاعب بالمعلومات الموجودة في أي سجل موزع مشترك قائم باستخدام توقيع إلكتروني ورفضها في السجل الموزع.
- من بين السلاسل الرئيسية المستخدمة في أنظمة السجلات الموزعة، يجب رفض السلاسل ذات المحتويات المختلفة من أطول سلسلة قبل عمق اعتباطي للفدرة b عند إنشاء فدرة جديدة، في السجل الموزع. وb هنا عدد أكبر من أو يساوي 1.
- يجب رفض البيانات في عملية إنشاء السجل الموزع، عند إضافة البيانات ذات العناوين المكررة (على سبيل المثال، العناوين IP، المعرفات UUID) إلى نظام السجل الموزع.
- من الضروري أن يكون المصدر العشوائي المشترك (على سبيل المثال، قيمة تجفير ظرفية [b-NIST]) هو نفسه بالنسبة للفدرات من أي عمق d للفدرة. والفدرات بعد تلك ذات العمق d مطلوبة لتحديث المصدر العشوائي المشترك بعمق g للفدرة. وعند التحديث، يوصى باستخدام دالة الاختزال للفدرة المضافة حديثاً كمصدر عشوائي.

  ملاحظة – يُعنى هنا بالفدرات ذات العمق d وg، أي فدرات بعمق أكبر من 1.
- يجب رفض السلاسل التي تحتوي على فدرات ذات قيم اختزال مختلفة للفدرات السابقة وقيم جذر شجرة ماركل (Merkle) في السجل الموزع.
- في حالة حدوث عقدة خطأ بين العقد المكونة لنظام السجل الموزع، يوصى بالحفاظ على العقد الخالية من الأخطاء إذا كانت أعلى من مستوى التوافق المحدد سلفاً لنظام السجلات الموزعة.

4.7 متطلبات الحفاظ على سلامة أنظمة السجلات الموزَّعة

يوصى بأن تتبع العقد القائمة الأحكام الواردة في هذه الفقرة.

- يوصى بأن تقوم كل عقدة بالتخلص من أي محاولة للتلاعب بالمعلومات الموجودة في السجل الموزع المشترك القائم. وفي حالة اكتشاف هجوم كهذا، يوصى بتجميع عدد العقد للحصول على معدل قوة الاختزال. ويوصى بمقارنة العدد الحالي لأشجار الفدرات مع قيمة العتبة لحساب السلامة وإرسال (بث) المعلومات ذات الصلة وعناوين العقد إلى جميع العقد.
- يوصى بأن تزيل كل عقدة أطول السلاسل المستخدمة بشكل شائع في نظام السجل الموزع والسلاسل ذات المحتويات المختلفة من نظام السجل الموزع.
- يوصى بأن تزيل كل عقدة السلسلة التي تحتوي على فدرات ذات قيم اختزال مختلفة أو قيم جذر شجرة ماركل (Merkle) للفدرات السابقة في السجل الموزع وحساب العدد المتراكم من العقد التي تعرضت لهجمات لتحديد ما إذا كان السجل الموزع آمناً أم لا، وإرسال (بث) المعلومات ذات الصلة وعنوان العقدة.
- عند حدوث خطأ أو عقدة مزيفة بين مكونات نظام السجل الموزع، يوصى بأن تقوم كل عقدة بإزالة وتجميع عدد العقد التي حاولت تنفيذ خطأ ما أو هجوم للحصول على نسبة من قدرة الاختزال. ويوصى، في السجل الموزع، بالحفاظ على عدد العقد الآمنة لتكون أكبر من قيمة العتبة ويوصى بإرسال (بث) المعلومات ذات الصلة وعناوين العقد.
- يوصى بأن ترفض كل عقدة البيانات في عملية إنشاء السجل الموزع عند إضافة بيانات جديدة مع عناوين مكررة إلى بيانات نظام السجل الموزع.

8 القدرات الوظيفية لأنظمة السجلات الموزعة من أجل خدمات العوامل البشرية الآمنة

يلزم كحافز تحسين جودة الحياة في نموذج خدمة السجل الموزع عن طريق أتمتة التوزيع المباشر لمعلومات العوامل البشرية الشخصية. يبدأ تطبيق تقنية سجل الحسابات الموزع بالقدرة على تتبع وإدارة إنتاج معلومات العامل البشري وتوزيعها. ويبدأ تطبيق تكنولوجيا السجلات الموزعة بالقدرة على تتبع وإدارة إنتاج معلومات العوامل البشرية وتوزيعها. بمعنى آخر، يمكن أن يضمن تطبيق تكنولوجيا السجلات الموزعة في توزيع معلومات العوامل البشرية الشخصية تتبعاً شفافاً بدءاً من عملية التوزيع وصولاً إلى مسار الاستعمال النهائي. ولهذا السبب، يمكن للأفراد الذين تمثلهم العقد الفردية المشاركة في نظام السجلات الموزعة الوثوق بالمعلومات الموزعة واستخدامها. بالإضافة إلى ذلك، من الممكن توفير طريقة لمنع التوزيع غير القانوني لمعلومات العوامل البشرية الشخصية من الأساس.

1.8 هيكل السجل الموزع عند توزيع معلومات العوامل البشرية الشخصية

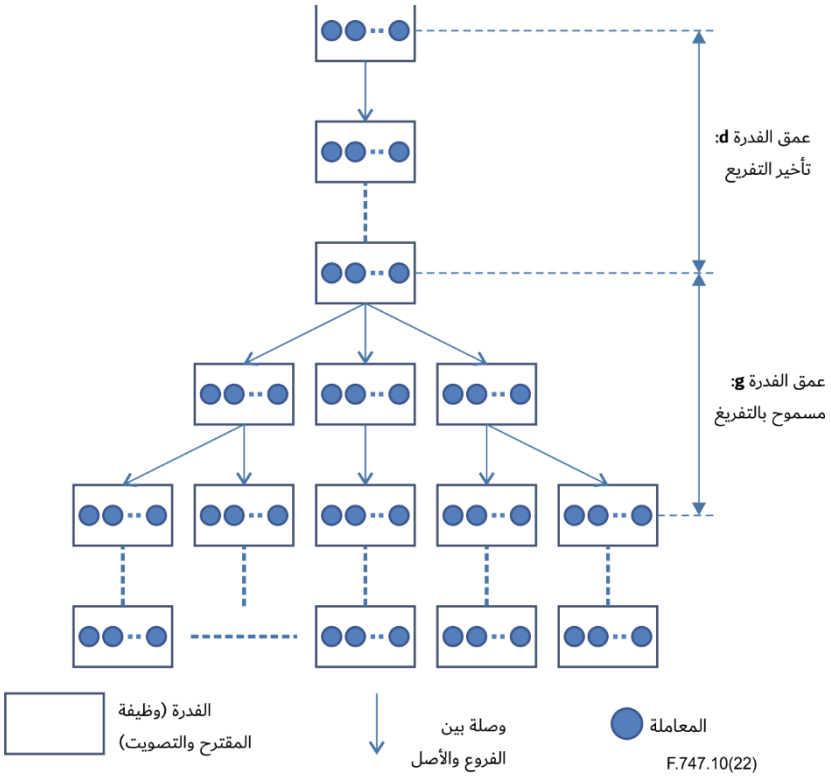
وفقًا للاتفاقية، فإن المعاملة الأولى في السجل هي معاملة خاصة تبدأ حافزاً جديداً (على سبيل المثال، العملات الافتراضية [b-ITU-T F.751.0]) التي سيتم صرفها إلى منشئ السجل. ويُمنح هذا الحافز للعقد للحفاظ على السجل الموزع وتوزيعه من البداية لتوزيع معلومات العوامل البشرية الشخصية. ويوصى بالاتفاق المسبق على تقنيات توفير هذه الحوافز وتوزيعها لأنها تعمل كنظم موزعة. والسبب وراء إضافة عدد معين من الحوافز الجديدة باستمرار هو تعويض العقد (التي تقوم باستخلاص البيانات) التي تستهلك الموارد لتشغيل نظام السجلات الموزعة. وتستهلك هذه العقد القدرات الحاسوبية والذاكرة والعملات الخاصة بوحدة المعالجة المركزية (CPU).

2.8 وظيفتان في هيكل السجل الموزع عند توزيع معلومات العوامل البشرية الشخصية

كطريقة لتقليل وقت الانتظار مع زيادة سرعة استخلاص البيانات، يمكن، بشكل اختياري، استخدام تقنية تفكك هيكل السجل الموزع الأساسي إلى ثلاث وظائف. ويمكن اعتبار ذلك على أنه اختيار للسلسلة الرئيسية في بروتوكول السجل الموزع (على سبيل المثال، تقنية اختيار أطول سلسلة)، مما يؤدي إلى اختيار السجل الآمن من بين جميع السجلات عند كل عمق من شجرة السجل. وهنا، يتم تعريف عمق السجل على أنه المسافة من السجل الأصلي (عدد الفدرات الموصولة في السجل).

في أي سجل موزع، يخدم السجل ثلاثة أغراض. حيث يعمل على انتخاب القبطان، وإضافة المعاملات إلى السلسلة الرئيسية، والتصويت للسجل الأساسي من خلال علاقات الوصلات الرئيسية. وعند التعبير عن السجل كعمل مفاهيمي، يتم تقسيمه إلى وظيفتين (انظر الشكل 2). تجمع وظيفة المقترح المعاملات بنفس العمق في شجرة السجل الأصلي. وتحدد وظيفة التصويت جزء السجل عن طريق التصويت لنفس عمق المعاملات في شجرة السجل. ويأخذ السجل المحدد السجلات الجزئية للمعاملات ويكون السجل النهائي. وتعمل وظيفة التصويت هذه على نفس عمق شجرة السجل وتقوم بإنشاء توصيل بين الفروع والأصل. لذلك، فإن للوصلة بين الفروع والأصل لشجرة السجل الأصلي وظيفتين يتم الفصل بينهما بشكل صريح: 1) توفير ترتيب معين للسجلات في جزء المعاملة بنفس العمق، 2) وظيفة التصويت التي تساعد على التصويت لبعضهم البعض لفرز السجل. ويوضح الشكل 2 الهيكل العام للسجل الموزع لتوزيع معلومات العوامل البشرية الشخصية المشروح أدناه.

ونظراً للطبيعة الموزعة لأنظمة السجلات الموزعة، فإنها تواجه مشكلات فيما يتعلق بالاستقرار. ففي أنظمة السجلات الموزعة، يمكن لكل عقدة تسجيل معاملة، ولكن في النهاية، فإن العقدة التي يتم اختيارها تكون نتيجة خوارزمية التوافق [b-ITU-T F.751.0]. ويجب أن يؤخذ تصميم النظام DLS في الاعتبار كواحد من العديد من العوامل التي تؤثر على الاستقرار، ويوصى بأن يقوم السجل الموزع باستعادة الخدمة المستقرة من خلال المعالجة التكيفية للنظام. ومن أجل حل مشكلة استقرار النظام DLS، يتم الاحتفاظ بالمصدر العشوائي المشترك (على سبيل المثال، قيمة تجفير ظرفية [b-NIST]) كما هو بالنسبة للأعماق d للفدرات، وينبغي أن تقوم الفدرات بعد القيم d للعمق بتحديث المصدر العشوائي المشترك بقيم g لأعماق الفدرات. وعند التحديث، يتم استخدام دالة اختزال الفدرة المضافة حديثاً كمصدر عشوائي. إذا كانت $d = 1$، تتم استعادتها إلى قاعدة التحديث الأساسية التي تتفرع عن كل حقبة، وهي الأكثر عرضة لهجمات التلوث (المتوازنة). ومن أجل زيادة عتبة الأمن بشكل طبيعي، يمكن زيادتها قيمة d. وعندما تكون $d = \infty$، تستخدم جميع الفدرات القيمة الظرفية للفدرة الأصلية كمصدر عشوائي مشترك. وهذا هو بروتوكول أطول سلسلة، حيث لا يسمح بالتفريع، مما يسمح بالتنبؤ الخاص بالسلسلة من قبل المالك الملوث للمفتاح السري.



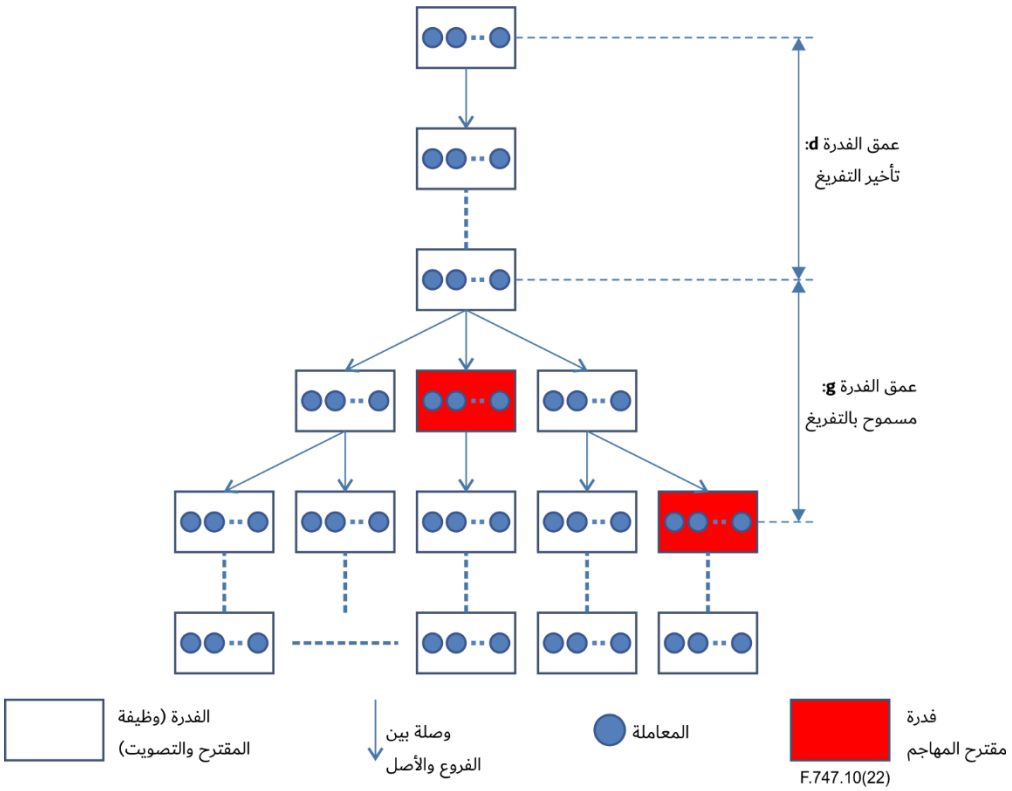
الشكل 2 – هيكل نموذج خدمة السجلات الموزعة

3.8 منهجيات صيانة أنظمة السجلات الموزعة

هذا التمثيل للفصل الوظيفي لأي سجل موزع أكثر تعقيداً بكثير من تمثيل السجل الموزع التقليدي، ولكن يمكنه تحسين أداء السجل الموزع من خلال اشتقاق توافق أسرع. يمكن أن تؤدي وظيفة اشتقاق التوافق السريع هذه إلى زيادة عدد السجلات في جزء المعاملة دون المساس بأمن السجل الموزع في الوظيفة المقترحة. لذلك، سيكون عدد السجلات محدوداً فقط بقدرة شبكة الاتصالات الأساسية. ويمكن تأكيد التوافق بشكلٍ اختياري مع كمون منخفض وموثوقية عالية حيث سيتم التصويت من قبل وظيفة التصويت على معاملات متعددة بالتوازي مع السجل الخاص بالمقترح للتأكيد السريع. ومن السهل إدارة نظام السجلات الموزعة لمعلومات العوامل البشرية الشخصية لأن المعدل العام لإنشاء السجلات زاد بشكل كبير، ويمكن أن يكون عدد السجلات الجزئية للوظيفة المقترحة لكل عمق صغيراً.

يمكن لنظام السجلات الموزعة هذا أن يضر بالشفافية من خلال تركيز قدرة الاختزال في الوظيفة المقترحة لمعاملة معينة في عملية اختيار السجل. وكما هو موضح في الشكل 3، إذا كانت قدرة اختزال المهاجم قوية في سجل محدد للوظيفة المقترحة، فقد تكون نقطة ضعف من المنظور الأمني. ويوضح الشكل 3 مثالاً لسلسلة من السجلات يتم تدميرها أو تلويثها بتركيز قدرة الاختزال الخاصة بالمهاجم. فإذا كان المهاجم قادراً على جمع كم من القدرات الحاسوبية والذاكرة والعملات الخاصة بوحدة المعالجة المركزية في مكان واحد أكبر من جميع العقد الآمنة، فسيكون على المهاجم أن يقرر ما إذا كان سيستخدمها لسرقة حوافز العقد الصادقة أو استخدامها للتعاون. وسيكون من الضروري توفير سياسة تحفيزية بحيث يكون من المفيد للمهاجم اتباع القواعد بدلاً من تقويض شفافية نظام السجلات الموزعة لمعلومات العوامل البشرية الشخصية. ويجب تعديل هذا الحافز بحيث يتم توزيعه على العقد المشاركة. ويمكن للمهاجم توفير مثل هذه القاعدة التي سيكون من الأكثر ربحية ربطها مع جميع العقد الأخرى. ويوصى بأن تعمل هذه القاعدة على الحفاظ على عدد العقد الصادقة أعلى من قيمة العتبة (على سبيل المثال، $CD\ (1 + \alpha)/(\alpha\text{-}1)/\log(\alpha)$) وفقاً لنسبة قدرة الاختزال الخاصة بالمهاجم (α) . وترمز C و D هنا إلى سعة وتأخير شبكات الاتصال.

ما يمكن فهمه من هذه المعادلة هو أنه إذا كانت α قريبة من 0، تكون قدرة اختزال المهاجم ضعيفة، ويمكن القول إنه لا توجد مشكلة في أمن أنظمة السجلات الموزعة حتى لو كان عدد شجرة فدرات المصوتين صغيراً. ومع ذلك، إذا كانت α قريبة من 1، أي إذا كانت قدرة اختزال المهاجم قوية، فيجب زيادة عدد شجرة فدرات المصوتين بشكل كبير. وفي هذه المرحلة، يمكن ملاحظة أن الأنظمة تكون ضعيفة جداً من منظور الأمن.



الشكل 3 – مثال على منع التلوث في نموذج خدمة السجلات الموزعة

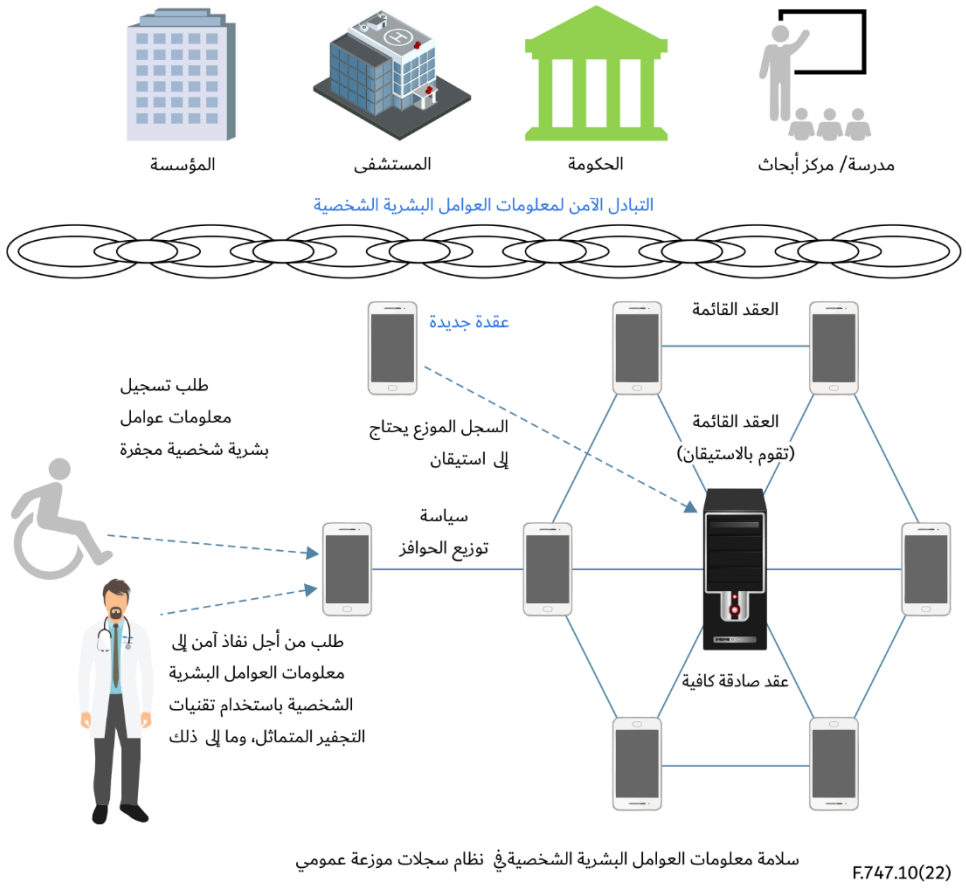
في عملية اختيار فدرة المقترح، يوصى بتحديد وظيفة الفدرة عن طريق ضبط قدرة الاختزال والعملات. وفي هذا الوقت، يمكن ملاحظة أنه إذا كانت قدرة الاختزال والعملات الخاصة بالمهاجم قوية، فإن الأمن يكون ضعيفاً للغاية. فإذا تمكن المهاجم من جمع كم من القدرات الحاسوبية والعملات أكبر من جميع العقد الصادقة، فسيلزم اتخاذ قرار بشأن استخدامها في سرقة فوائد عقدة صادقة، أو استخدامها للتعاون. ويوصى بتوفير سياسات تحفيزية بحيث يكون من المفيد للمهاجمين أكثر الالتزام بالقواعد من تقويض النظام وشرعية ثرواتهم. وباستخدام سياسة تمنع تركيز الأرباح على فدرة مؤيدة محددة، يوصى بهذا لإدراج مثل هذه القاعدة التي سيستفيد المهاجمون باتباعها أكثر من التخصيص مع جميع العقد الأخرى.

الملحق A

تطبيق لنموذج خدمة السجلات الموزعة لمعلومات العوامل البشرية الآمنة

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

يمكن لسيناريو السجل الموزع الموضح في الشكل 1.A أن يدير بأمان وشفافية ليس فقط بيانات العوامل البشرية الشخصية الموجودة في المستشفيات، ولكن أيضاً بيانات العوامل البشرية المتمحورة حول الأشخاص مثل أجهزة جمع بيانات الصحة الشخصية. وفي مثال استخدام تبادل المعلومات الصحية للأشخاص في الشكل 1.A، يمكن توفير الموثوقية باستخدام سجل موزع تشارك فيه عقد متعددة، ويمكن استخدام التوقيعات الرقمية وقيم الاختزال لضمان الشفافية في بيانات البحث. ومع ذلك، يمكن أن تكون بيانات العوامل البشرية الشخصية حساسة للغاية فيما يتعلق بحماية البيانات. وتُسجل هذه البيانات الحساسة في حالة مجفرة باستخدام تقنية تجفير قادرة على معالجة البيانات الضخمة. ويتبع إجراء التنقلية لمعلومات العوامل البشرية الشخصية الحساسة متطلبات وإجراءات نظام السجل الموزع المشترك المشروح في الفقرة 2.7 باستخدام خوارزمية تجفير (انظر الشكل 1.A). بالإضافة إلى ذلك، يلزم تشغيل نظام السجلات الموزعة من أجل معلومات العوامل البشرية الشخصية لتلبية متطلبات وظيفة التحفيز المشروحة في الفقرة 3.8 للتنشيط والصيانة.



الشكل 1.A – سيناريوهات نموذج خدمة السجلات الموزعة الآمن

بيبليوغرافيا

[b-ITU-T F.751.0] Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger systems*.

[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 TS FG DLT D1.1] Technical Specification ITU-T FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions*.

[b-IETF draft-irtf-cfrg-vrf-08] IETF draft-irtf-cfrg-vrf-08 (2020), *Verifiable Random Functions (VRFs)*. https://tools.ietf.org/html/draft-irtf-cfrg-vrf-08

[b-ISO 6385] ISO 6385:2016, *Ergonomics principles in the design of work systems*.

[b-ISO 18033-6] ISO 18033-6:2019, *IT Security techniques – Encryption algorithms – Part 6: Homomorphic encryption*.

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.

[b-NIST] NISTIR 8202 (2018). *Blockchain Technology Overview*.

[b-WHO] World Health Organization (2006), *Constitution of the World Health Organization – Basic Documents*, Forty-fifth edition, Supplement.

[b-Wickens] Wickens, D., Gordon, S., Liu, Y. (1997), *An Introduction to Human Factors Engineering*. pp.2-7. New York, NY: Longman.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

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

طُبعت في سويسرا
جنيف، 2022