التوصية

# ITU-T X.1410 (03/2023)

السلسلة X شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) – أمن أنظمة النقل الذكية (ITS)

---

# معمارية أمن إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة

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 (1) | X.1140–X.1149 |
| أمن التطبيقات (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.1350–X.1369 |
| أمن أنظمة النقل الذكية (ITS) | X.1370–X.1399 |
| **أمن تكنولوجيا السجلات الموزعة (DLT)** | **X.1400–X.1429** |
| أمن التطبيقات (2) | X.1450–X.1459 |
| أمن الويب (2) | X.1470–X.1489 |
| تبادل معلومات الأمن السيبراني | |
| نظرة عامة على 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 |
| الدفاع السيبراني | X.1590–X.1599 |
| 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 |
| المولد الكمومي للأعداد العشوائية | X.1702–X.1709 |
| إطار أمن شبكات توزيع المفاتيح الكمومية (QKDN) | X.1710–X.1711 |
| التصميم الأمني للشبكات QKDN | X.1712–X.1719 |
| التقنيات الأمنية للشبكات QKDN | X.1720–X.1729 |
| أمن البيانات | |
| أمن البيانات الضخمة | X.1750–X.1759 |
| حماية البيانات | X.1770–X.1789 |
| آمن الاتصالات المتنقلة الدولية –2020 | X.1800–X.1819 |

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

**التوصية ITU-T X.1410**

# معمارية أمن إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة


## ملخص

تحدد التوصية ITU-T X.1410 معمارية الأمن لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة (DLT). وتحدد أيضاً، بناءً على هذه المعمارية، السطوح البينية بين الكيانات الوظيفية وإجراءات إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة. وتحول تكنولوجيات السجلات الموزعة (DLT) الصناعات من خلال حلول مبتكرة وتغير طريقة عمل الحكومات والمؤسسات والشركات. وهي توفر حلاً لتكرار البيانات وتبادلها ومزامنتها بشكل آمن عبر شبكة حاسوبية موزعة، بالنظر إلى سماتها المتمثلة ميزاتها المتمثلة في اللامركزية ومقاومة التلاعب. وأدت النهج الحالية المتعلقة بتبادل بيانات الأعمال وبيانات المعلومات المحدِّدة لهوية الأشخاص (PII) مع الشركات والمنصات الرقمية إلى ظهور مواطن ضعف فيما يتعلق بالخصوصية بسبب عمليات الاختراق أو سوء إدارة البيانات. ويسمح اعتماد تكنولوجيا السجلات الموزعة أو سلسلة الكتل في مجال إدارة تبادل البيانات للأفراد أو الشركات بالحفاظ على مزيد من التحكم المباشر في معلوماتهم السرية. وفي الحل القائم على تكنولوجيا السجلات الموزعة، يتم تخزين البيانات غير المتعلقة بالمعلومات المحدِّدة لهوية الأشخاص فحسب، على سبيل المثال، قيم البيانات المختزلة، في السلسلة. وتُخزن البيانات المتعلقة بالمعلومات المحدِّدة لهوية الأشخاص ذات الصلة بمالك البيانات خارج السلسلة. ويوفر الحل القائم على تكنولوجيا السجلات الموزعة طريقة تعمل على تحسين إمكانية التتبع وإمكانية التحقق وإمكانية تغيير حالة البيانات.



## التسلسل التاريخي

| الطبعة | التوصية | تاريخ الموافقة | لجنة الدراسات | معرف الهوية الفريد* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1410 | 2023-03-03 | 17 | 11.1002/1000/15109 |


* 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**

# معمارية الأمن إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة

## 1 مجال التطبيق

تحدد هذه التوصية معمارية الأمن لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة (DLT). وتشمل هذه التوصية:

- تصميم معمارية الأمن لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة؛
- تحديد الوظائف المنطقية لمعمارية الأمن لتبادل البيانات؛
- تحديد السطوح البينية بين الوظائف المنطقية لمعمارية الأمن؛
- تحديد إجراءات تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة.

## 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.

[ITU-T X.1408] التوصية ITU-T X.1408 (2021)، *التهديدات والمتطلبات الأمنية للنفاذ إلى البيانات وتقاسمها على أساس تكنولوجيا سجل الحسابات الموزَّع.*

## 3 التعاريف

### 1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

**1.1.3 العنوان (address)** [b-ITU-T FG DLT D1.1]: معرف للكيان (الكيانات) الذي يقوم بإجراء معاملات أو إجراءات أخرى في سلسلة كتل أو في شبكة لتكنولوجيا السجلات الموزعة.

**2.1.3 سلسلة الكتل (blockchain)** [b-ITU-T X.1400]: نوع من تكنولوجيا السجلات الموزعة يتكون من بيانات مسجلة رقمياً مرتبة على شكل سلسلة كتل متزايدة على نحو متتالٍ، مع ارتباط كل كتلة تجفيرياً وتحصينها ضد التلاعب والمراجعة.

**3.1.3 سلطة إصدار الشهادات (certification authority) (CA)** [b-ITU-T X.509]: جهة موثوق بها من جانب كيان أو أكثر لاستحداث شهادات المفاتيح العمومية الموقعة رقمياً. ويمكن، خيارياً، لسلطة التصريح أن تستحدث مفاتيح المستعملين.

**4.1.3 مورّد البيانات (data provider)** [b-ISO/IEC/IEEE 15939]: فرد أو منظمة يشكل (تشكل) مصدراً للبيانات.

**5.1.3 الهوية (identity)** [b-ISO/IEC 29100]: مجموعة من النعوت التي تجعل من الممكن تحديد صاحب المعلومات المحدِّدة لهوية الأشخاص.

**6.1.3 خارج السلسلة (off-chain)** [b-ISO 22739]: مرتبط بنظام سلسلة الكتل، ولكن الموقع أو التنفيذ أو التشغيل يكون خارج نظام سلسلة الكتل.

**7.1.3 داخل السلسلة (on-chain)** [b-ISO 22739]: حيث يكون الموقع أو الأداء أو التشغيل داخل نظام سلسلة الكتل.

**8.1.3 المعلومات المحدِّدة لهوية الأشخاص (personally identifiable information) (PII)** [b-ISO/IEC 29100]: أي معلومات ( أ ) يمكن أن تستخدم للتعرّف على هوية الشخص الذي تتعلق به هذه المعلومات، أو (ب) قد تكون مرتبطة بشكل مباشر أو غير مباشر بهوية الشخص المراد التعرف عليه من خلالها.

**ملاحظة** – لتحديد إمكانية التعرف على هوية الشخص صاحب المعلومات PII، ينبغي مراعاة جميع الوسائل التي يمكن لصاحب المصلحة في الخصوصية الذي يحتفظ بالبيانات أو أي طرف آخر أن يستعملوها استعمالاً معقولاً لتحديد هوية هذا الشخص الطبيعي.

**9.1.3 البينة التحتية للمفاتيح العمومية (public-key infrastructure) (PKI)** [b-ITU-T X.509]: البنية التحتية التي بمقدورها دعم إدارة مفاتيح عمومية تستطيع دعم خدمات الاستيقان أو التجفير أو السلامة أو عدم الرفض.

**10.1.3 العقد الذكي (smart contract)** [b-ITU-T X.1400]: برنامج مكتوب على نظام السجلات الموزَّعة يشفر القواعد الخاصة بأنواع معينة من معاملات أنظمة السجلات الموزَّعة بطريقة يمكن التحقق من صحتها، ويستدعى تشغيلها بشروط محددة.

**11.1.3 نظام التجفير المتناظر (symmetric encryption system)** [b-ISO/IEC 18033-1]: تقنية التجفير المستخدمة لحماية سرية البيانات، والتي تتكون من ثلاثة مكونات: خوارزمية تجفير، وخوارزمية فك التجفير، وطريقة لتوليد المفاتيح، إذ تستخدم خوارزميات التجفير وفك التجفير المفاتيح نفسها.

### 2.3 المصطلحات المعرفة في هذه التوصية

تعرف هذه التوصية المصطلح التالي:

**1.2.3 مستهلك البيانات (data consumer)**: المستعمل الذي يقرأ البيانات ثم يعالجها إلى الحد الذي يتم فيه اكتشاف الحدود المعجمية أو التشفيرية.

**ملاحظة** – مقتطف من المعيار [b-ISO/IEC 20944-1].

## 4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية الاختصارات والأسماء المختصرة التالية:

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

CA سلطة إصدار الشهادات *(Certification Authority)*

DLT تكنولوجيا السجلات الموزعة *(Distributed Ledger Technology)*

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

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

## 5 الاصطلاحات

في هذه التوصية:

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

"**يمكن**" و"**طوعاً**" تدلان 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 للمواصفة في نفس الوقت.

يستخدم *النص المائل* في هذه التوصية للإشارة إلى الوظائف.

## 6 معمارية الأمن لتبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة

توفر تكنولوجيا السجلات الموزعة حلاً لتكرار البيانات وتبادلها ومزامنتها بشكل آمن عبر شبكة حاسوبية موزعة، بالنظر إلى سماتها المتمثلة في اللامركزية ومقاومة التلاعب. وأدت النهج الحالية المتعلقة بتبادل بيانات الأعمال وبيانات المعلومات المحدِّدة لهوية الأشخاص (PII) مع الشركات والمنصات الرقمية إلى ظهور مواطن ضعف فيما يتعلق بالخصوصية بسبب عمليات الاختراق أو سوء إدارة البيانات. ويسمح اعتماد تكنولوجيا السجلات الموزعة أو سلسلة الكتل في مجال إدارة تبادل البيانات للأفراد أو الشركات بالحفاظ على مزيد من التحكم المباشر في معلوماتهم السرية. وفيما يتعلق بالحل القائم على تكنولوجيا السجلات الموزعة، يتم تخزين البيانات غير المتعلقة بالمعلومات المحدِّدة لهوية الأشخاص فحسب، على سبيل المثال، قيم البيانات المختزلة، في السلسلة. ويتم تخزين البيانات المتعلقة بالمعلومات المحدِّدة لهوية الأشخاص ذات الصلة بمالك البيانات خارج السلسلة. ويوفر الحل القائم على تكنولوجيا السجلات الموزعة طريقة تعمل على تحسين إمكانية التتبع وإمكانية التحقق وإمكانية تغيير حالة البيانات. وتحدد هذه التوصية معمارية الأمن لإدارة تبادل البيانات استناداً إلى تكنولوجيات السجلات الموزعة. وتستخدم إدارة تبادل البيانات نظام تجفير متناظر، إذ تستخدم خوارزميات التجفير وفك التجفير المفتاح نفسه. ويرد وصف التهديدات الأمنية في التوصية [ITU-T X.1408].

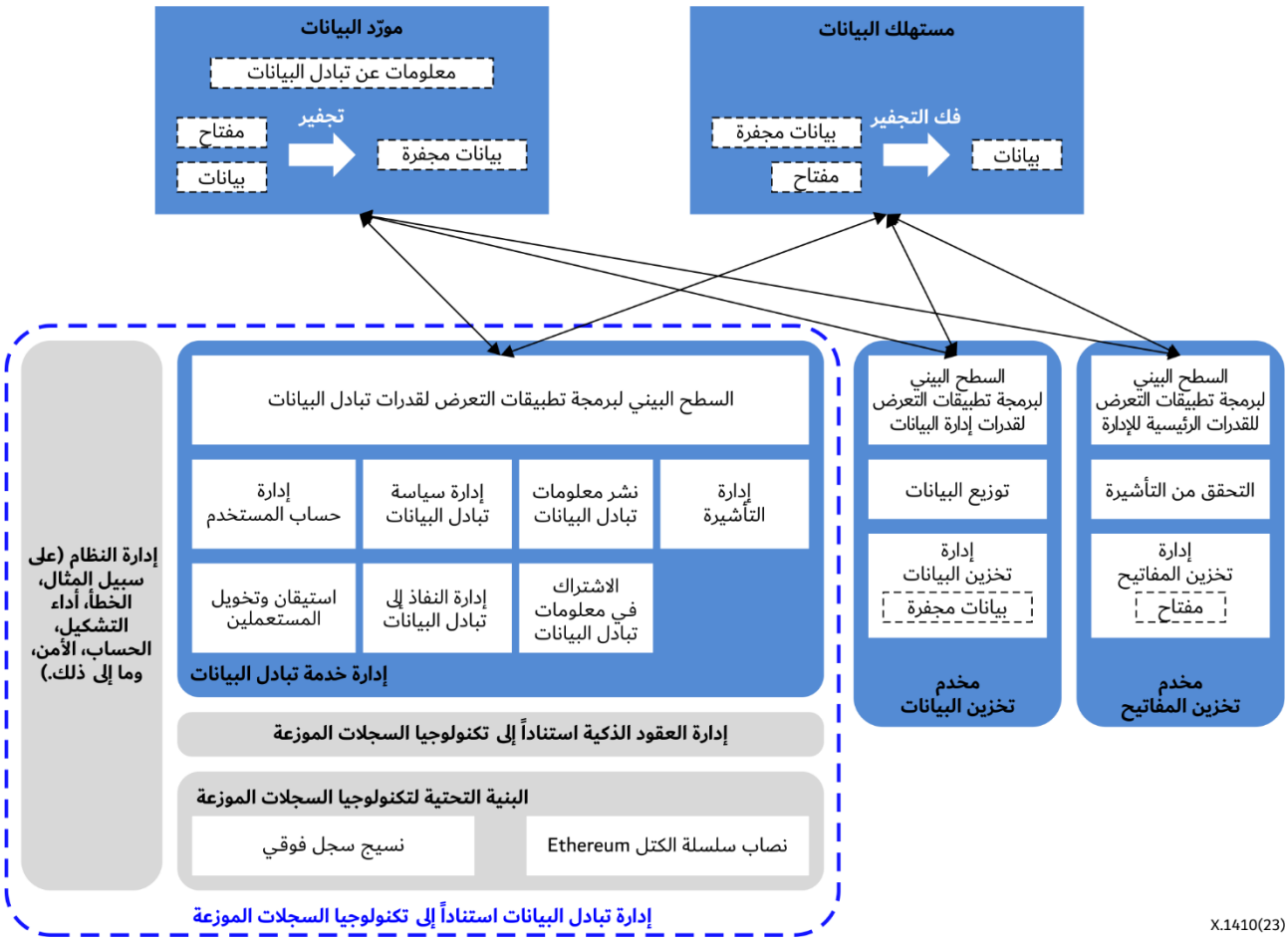
وقد وُضعت هذه التوصية استناداً إلى التوصية [ITU-T X.1408]. وبالرغم من أن التوصية [ITU-T X.1408] صُممت من وجهة نظر مفاهيمية، فقد وُضعت هذه التوصية من وجهة نظر تنفيذية. ويبين الجدول 1 تقابل المصطلحات بين هذه التوصية والتوصية [ITU-T X.1408].

**الجدول 1 – تقابل المصطلحات بين هذه التوصية والتوصية [ITU-T X.140]**

| هذه التوصية | التوصية [ITU-T X.1408] |
|---|---|
| مورّد البيانات | وكيل تبادل البيانات (مالك البيانات) |
| مستهلك البيانات | عميل مستهلك للبيانات (معالج البيانات) |
| مخدم تخزين المفاتيح | مخدم إدارة المفاتيح |
| مخدم تخزين البيانات | مخدم تخزين البيانات (مورّد خدمة تخزين البيانات) |
| إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة | وسيط البيانات |

### 1.6 لمحة عامة عن المعمارية الوظيفية

يوضح الشكل 1 المعمارية الوظيفية لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة من وجهة نظر التنفيذ. ويتفق ذلك مع معمارية النفاذ إلى البيانات استناداً إلى تكنولوجيا السجلات الموزعة وتبادلها المبينة في الشكل 1.B من التوصية [ITU-T X.1408]. والأخير مصمم من وجهة نظر مفاهيمية ويعبر عن معمارية عالية المستوى. وتتكون المعمارية الوظيفية في الشكل 1 من خمسة مكونات وظيفية زرقاء وثلاثة مكونات وظيفية رمادية.




**الشكل 1 – المعمارية الوظيفية لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة**

يتم وصف هذه المكونات على النحو التالي:

- المكونات الوظيفية الزرقاء الخمسة هي *مورّد البيانات* و*مستهلك البيانات* و*إدارة خدمة تبادل البيانات* و*مخدم تخزين المفاتيح* و*مخدم تخزين البيانات*، والتي يرد تعريفها ووصفها بالتفصيل في الفقرة 2.6.
- المكونات الوظيفية الرمادية الثلاثة هي *البنية التحتية لتكنولوجيا السجلات الموزعة* و*إدارة العقود الذكية استناداً إلى تكنولوجيا السجلات الموزعة* و*إدارة النظام (على سبيل المثال، الخطأ والتشكيل والأداء والحساب والأمن)*، والتي تعيد استعمال المنصات القائمة لتكنولوجيا السجلات الموزعة مفتوحة المصدر (على سبيل المثال، نسيج سجل فوقي)، وتقع خارج نطاق هذه التوصية.

ويرد وصف لإجراءات إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة في الملحق ألف.

## 2.6 المكونات الوظيفية

### 1.2.6 مورّد البيانات ومستهلك البيانات

تقدم هذه التوصية نوعين من المستعملين: مورّد البيانات (أي المستعملون الذين يقدمون بياناتهم) ومستهلك البيانات (أي المستعملون الذين يستهلكون البيانات المعروضة والمقدمة من مستعملين آخرين). ويتسم كلا النوعين بنفس القدرات:

1) الحصول على شهادات رقمية (بما في ذلك المفاتيح العمومية) والمفاتيح الخاصة المقابلة من سلطة إصدار الشهادات؛
2) تخزين الشهادات الرقمية التي تم الحصول عليها والمفاتيح الخاصة المقابلة بشكلٍ آمن؛
3) التواصل مع مخدم إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة؛

4) الحصول على شهادات رقمية ومعلمات الشبكة وتشكيلات الشبكة لعقد شبكة تكنولوجيا السجلات الموزعةوتخزينها؛

5) استلام إخطارات من إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة؛

6) الاستفادة من نظام التجفير المتناظر.

ويتمتع مورّد البيانات ومستهلك البيانات بقدرات خاصة بكل منهما على النحو التالي:

- يتمتع *مورّد البيانات* بالقدرات التالية:

1) جمع البيانات غير المعالجة وإزالة حساسيتها (على سبيل المثال، جعل البيانات مجهولة الهوية، وإزالة المعلومات الحساسة مثل الاسم ورقم الهاتف المحمول وبيانات بطاقة الائتمان) دون أن يكون لذلك تأثير سلبي على جودة البيانات المتبادلة؛

2) توليد مفتاح لنظام التجفير المتناظر؛

3) تجفير البيانات بالمفتاح الذي يستخدم نظام التجفير المتناظر؛

4) تخزين نص مجفر ومفتاح التجفير المقابل بشكل آمن على المخدم المحلي أو البعيد؛

5) ضمان الاستيقان المتبادل مع إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة؛

6) تزويد إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة، بمعلومات عن تبادل البيانات والتي تشمل معرّف مورّد البيانات، والمفتاح العمومي لمورّد البيانات، ومعرّف النص المجفر وعنوان التخزين الخاص به، ومعرّف مفتاح التجفير وعنوان التخزين الخاص به، والصناعات التي يتعين السماح لها بالنفاذ، والمستعملين المسموح لهم بالنفاذ ، ونعوت البيانات الأخرى (على سبيل المثال، فئة البيانات، وإدخال البيانات، والاستخدام والسعر)؛

7) الجمع بين معلومات تبادل البيانات والمعلومات الأخرى لصياغة سياسة لتبادل البيانات ثم التوقيع عليها باستخدام المفتاح الخاص؛

8) إرسال سياسة تبادل البيانات مع التوقيع الرقمي المقابل إلى إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة؛

9) تلقي إخطار من إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة، والذي يشير إلى إبرام العقد الذكي لتبادل البيانات؛

10) إدارة سياسة تبادل البيانات، مثل الاستفسار والتحديث.

- يتمتع *مستهلك البيانات* بالقدرات التالية:

1) الاشتراك في رسائل تبادل البيانات المنشورة؛

2) ضمان الاستيقان المتبادل مع إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة؛

3) الحصول على معلومات عن تبادل البيانات؛

4) إرسال معلومات مستهلك البيانات (مثل هوية مستهلك البيانات والمفتاح العمومي لمستهلك البيانات) ومعلومات عن البيانات المتبادلة (مثل هوية مورّد البيانات والمفتاح العمومي لمورّد البيانات ومعرف النص المجفر ومعرف مفتاح التجفير) جنباً إلى جنب مع التوقيع الرقمي (الذي يتم بواسطة المفتاح الخاص لمستهلك البيانات) إلى إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة؛

5) استلام إخطارات من إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة، والتي تتضمن معلومات عن البيانات المتبادلة وعنوان تخزين المفاتيح وعنوان تخزين النص المجفر وتأشيرة النفاذ؛

6) إرسال تأشيرة النفاذ إلى مخدم تخزين المفاتيح من أجل الحصول على مفتاح تجفير البيانات وفقاً لعنوان تخزين المفتاح؛

7) الحصول على النص المجفر وفقاً لعنوان تخزين البيانات؛

8) فك تجفير النص المجفر بالمفتاح الذي تم الحصول عليه من نظام التجفير المتناظر للحصول على البيانات في صورة نص غير مجفر؛

9) إدارة السجلات للوصول إلى البيانات المتبادلة.

### 2.2.6 إدارة خدمة تبادل البيانات

يتم وصف إمكانيات كل مكون من مكونات إدارة خدمة تبادل البيانات على النحو التالي.

- يتمتع مكوّن ***إدارة حساب المستعمل*** بالقدرة على إدارة حسابات المستعملين، مثل الإنشاء والتحديث والاستفسار والحذف.
- يتمتع مكوّن ***استيقان وتخويل المستعملين*** بالقدرات التالية:

1) إجراء استيقان متبادل مع المستعملين (أي مورّد البيانات ومستهلك البيانات)
2) تخويل المستعملين تبادل البيانات والنفاذ إلى البيانات المتبادلة.

- يتمتع مكوّن ***إدارة سياسة تبادل البيانات*** بالقدرات التالية:

1) استلام معلومات تبادل البيانات وسياسة تبادل البيانات جنباً إلى جنب مع التوقيع الرقمي المقابل من مورّد البيانات؛
2) إنشاء معاملة لتكنولوجيا السجلات الموزعة وفقاً للمعلومات الواردة من مورّد البيانات؛
3) إحالة معاملة تكنولوجيا السجلات الموزعة إلى المكونات الأساسية (أي *البنية التحتية لتكنولوجيا السجلات الموزعة* و*إدارة العقود الذكية*) لإنشاء عقد ذكي لتبادل البيانات، يتم توزيعه على عقد شبكة تكنولوجيا السجلات الموزعة؛
4) إخطار *مورّد البيانات* ومكوّن نشر معلومات تبادل البيانات بإنشاء العقد الذكي لتبادل البيانات؛
5) تمكين *مورّدي* البيانات من إدارة بياناتهم المتبادلة.

- يتمتع مكوّن ***إدارة النفاذ إلى تبادل البيانات*** بالقدرات التالية:

1) استلام طلب النفاذ إلى البيانات (بما في ذلك معلومات مستهلك البيانات ومعلومات البيانات المتبادلة والتوقيع الرقمي المقابل) من مستهلك البيانات والتحقق مما إذا كان يُسمح له بالنفاذ إلى البيانات وفقاً لسياسة تبادل البيانات (على سبيل المثال، يمكن لمستهلك البيانات من صناعة ما أو بلد محدد لا غير، النفاذ إلى البيانات المتبادلة)؛
2) إنشاء معاملة تكنولوجيا السجلات الموزعة وفقاً للمعلومات الواردة من مستهلك البيانات؛
3) تقديم معاملة تكنولوجيا السجلات الموزعة إلى المكونات الأساسية (أي *البنية التحتية لتكنولوجيا السجلات الموزعة*) لتسجيل النفاذ إلى البيانات، تُوزع على عقد شبكة تكنولوجيا السجلات الموزعة؛
4) إخطار *إدارة التأشيرة* بأنه تم إنشاء معاملة النفاذ إلى البيانات وإنشاء تأشيرة للنفاذ؛
5) استلام تأشيرة النفاذ من *إدارة التأشيرة*؛
6) إرسال معلومات النفاذ إلى تبادل البيانات (على سبيل المثال، تأشيرة النفاذ وعنوان تخزين المفاتيح وعنوان تخزين البيانات) إلى مستهلك البيانات؛
7) تمكين مستهلكي البيانات من إدارة سجلات النفاذ إلى البيانات المتبادلة الخاصة بهم.

- يتمتع مكوّن ***نشر معلومات تبادل البيانات*** بالقدرات التالية:

1) استلام إخطارات من *إدارة سياسة تبادل البيانات*، تتضمن معلومات تبادل البيانات الجديدة؛
2) نشر معلومات تبادل البيانات الجديدة؛
3) إخطار مكوّن *الاشتراك في معلومات تبادل البيانات* بنشر معلومات تبادل البيانات الجديدة.

- يتمتع ***الاشتراك في معلومات تبادل البيانات*** بالقدرات التالية:

1) استلام إخطارات من *إدارة معلومات تبادل البيانات*، تتضمن معلومات تبادل البيانات الجديدة؛
2) إرسال معلومات تبادل البيانات الجديدة إلى المشتركين.

- يتمتع مكوّن ***إدارة التأشيرة*** بالقدرات التالية:

1) استلام إخطارات من *إدارة النفاذ إلى تبادل البيانات* لإنشاء التأشيرة؛

2) إنشاء تأشيرة النفاذ؛

3) إرسال تأشيرة النفاذ التي تم إنشاؤها إلى *إدارة النفاذ إلى تبادل البيانات*.

- يُمكّن ***السطح البيني لبرمجة تطبيقات التعرض لقدرات تبادل البيانات (API)*** المستعملين من إدارة خدمات تبادل البيانات والنفاذ إليها على النحو الوارد أعلاه.

### 3.2.6 مخدم تخزين المفاتيح

يتم وصف قدرات كل مكون في مخدم تخزين المفاتيح على النحو التالي:

- يتمتع مكوّن ***إدارة تخزين المفاتيح*** بالقدرات التالية:

1) استلام طلبات من *مورّد البيانات* لتخزين المفتاح؛

2) استيقان *مورّد البيانات*؛

3) تخزين المفتاح بشكل آمن، على سبيل المثال، تخزين المفتاح في نص مشفر و/أو في مكان تخزين معزول؛

4) إخطار *مورّد البيانات* بأن المفتاح قد تم تخزينه؛

5) استلام إخطارات من *التحقق من التأشيرة*، تشير إلى نتيجة التحقق من تأشيرة النفاذ؛

6) إرسال المفتاح إلى *مستهلك البيانات*.

- يتمتع مكوّن ***التحقق من التأشيرة*** بالقدرات التالية:

1) استلام تأشيرة النفاذ من مستهلك البيانات؛

2) التحقق من تأشيرة النفاذ المستلمة؛

3) إرسال نتيجة التحقق إلى *إدارة تخزين المفاتيح*.

- يُمكّن ***السطح البيني لبرمجة تطبيقات التعرض لقدرات إدارة المفاتيح*** المستعملين من إدارة مفتاح تجفير البيانات والنفاذ إليه.

### 4.2.6 مخدم تخزين البيانات

يتم وصف قدرات كل مكون من المكونات الموجودة في مخدم تخزين البيانات على النحو التالي:

- يتمتع مكوّن ***إدارة تخزين البيانات*** بالقدرات التالية:

1) استلام الطلب من *مورّد البيانات* بتخزين النص المجفر؛

2) استيقان *مورّد البيانات*؛

3) تخزين النص المجفر؛

4) إخطار *مورّد البيانات* بأن النص المجفر قد تم تخزينه؛

- يتمتع مكوّن ***توزيع البيانات*** بالقدرات التالية:

1) استلام الطلب من *مستهلك البيانات*؛

2) استيقان *مستهلك البيانات*؛

3) إرسال النص المجفر إلى *مستهلك البيانات*.

- يتيح السطح البيني لبرمجة تطبيقات ***التعرض لقدرات إدارة البيانات (API)*** للمستعملين إدارة البيانات المتبادلة والنفاذ إليها.

## 7 معمارية الأمن لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة

وفقاً للمعمارية الوظيفية الواردة في الشكل 1، يطلب مستهلكو البيانات مفتاح تجفير البيانات ويستلمونه، ثم يستخدمونه في فك تجفير البيانات المذكورة في النص المجفر والحصول في نهاية الأمر على البيانات المتبادلة في شكل نص عادي. وبعد ذلك، لا يمكن لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعةالتحكم في البيانات المتبادلة في النص العادي. ويمكن لمستهلكي البيانات إعادة توجيه البيانات المتبادلة في النص العادي إلى مستعملين آخرين ليس لديهم إذن بالنفاذ إليها.

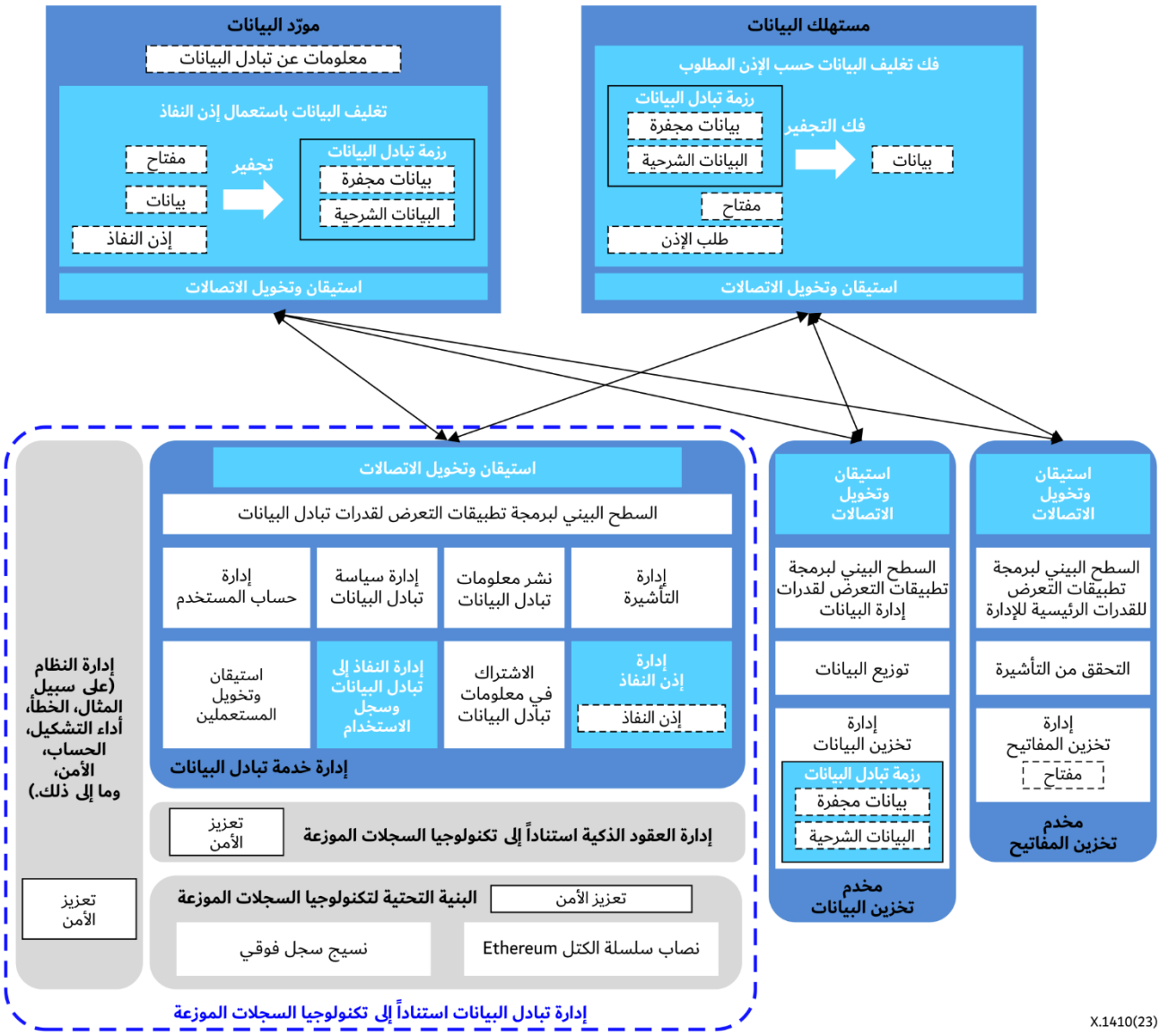
ودعماً لمورّدي البيانات الذين يتبادلون البيانات مع الأشخاص الآخرين بشكل آمن، ومنعاً لإعادة توجيه مستهلكي البيانات للبيانات المتبادلة في النص العادي إلى مستعملين آخرين، تتطلب المعمارية الوظيفية الواردة في الشكل 1 ميزات أمن محسنة ترد في الشكل 2.

### 1.7 لمحة عامة على معمارية الأمن

يصف الشكل 2 معمارية الأمن لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة، والتي تضمن ما يلي:

- اتصالات مؤمنة بين المكونات الوظيفية في الشكل 1؛
- يقوم مورّدو البيانات بتجفير البيانات ووضع إذن النفاذ إليها قبل تبادلها مع الآخرين؛
- يقوم مستهلكو البيانات بفك تجفير البيانات المتبادلة في النص المجفر وفقاً لإذن النفاذ قبل النفاذ إليها؛
- يقوم مستهلكو البيانات بتجفير البيانات المتبادلة بالطريقة نفسها التي يقوم بها مورّدو البيانات بعد الانتهاء من النفاذ إلى البيانات، وبهذه الطريقة يتم تخزين البيانات المتبادلة في النص المجفر من جانب مستهلكي البيانات؛
- يقوم مستهلكو البيانات بإعادة توجيه البيانات المتبادلة في إلى الأشخاص الآخرين في صورة نص مجفر فقط.

وبهذه الطريقة، حتى وإن استلم المستعملون البيانات المتبادلة التي أُعيد توجيهها من أشخاص آخرين، فعليهم طلب إذن النفاذ إليها من إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة.




**الشكل 2 – المعمارية الأمنية لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة**

يتضمن الشكل 2، خلافاً للشكل 1، مكونات وظيفية بخلفية زرقاء فاتحة وهي وظائف أمن منطقية، يرد وصفها بالتفصيل في الفقرة 2.7.

ولا تصف هذه التوصية التعزيز الأمني للمكونات الوظيفية الثلاثة الرمادية اللون الواردة في الشكل 2؛ انظر التوصية [b-ITU-T X.1402].

## 2.7 المكونات الوظيفية للأمن

### 1.2.7 تغليف البيانات باستعمال إذن النفاذ

دعماً للمستعملين الذين يضعون إذن النفاذ إلى البيانات المراد تبادلها، يحتاج *مورّد البيانات* في الشكل 1 إلى التعزيز من خلال إدخال وظيفة أمن منطقية جديدة، *وتغليف البيانات باستعمال إذن النفاذ*، والتي تتمتع بالقدرات التالية:

- توليد مفتاح لنظام تجفير متناظر يُستخدم لتجفير البيانات المراد تبادلها؛
- الاتصال *بمخدم تخزين المفاتيح* للتسجيل لأغراض الحصول على معرّف المفتاح وعنوان الحصول عليه؛
- الاتصال *بمخدم تخزين البيانات* للتسجيل لأغراض الحصول على معرّف رزمة تبادل البيانات وعنوان الحصول عليه؛

- وضع إذن النفاذ إلى البيانات التي سيتم تبادلها، والذي يتضمن أوقات النفاذ، ووقت انتهاء الصلاحية، والتحديد لأغراض القراءة فقط، ومعرّف المفتاح وعنوان تخزينه، ومعرّف رزمة تبادل البيانات وعنوان تخزينها؛
- توليد البيانات الشرحية التي تشمل معرّف رزمة تبادل البيانات ومعرّف مورّد البيانات والمفتاح العمومي لمورّد البيانات وتوقيع المعلومات السابقة؛
- توليد رزمة تبادل البيانات، والتي تشمل البيانات المجفرة والبيانات الشرحية؛
- تحميل المفتاح على *مخدم تخزين المفاتيح* من خلال قناة إرسال مؤمنة؛
- تحميل رزمة تبادل البيانات على *مخدم تخزين البيانات* من خلال قناة إرسال مؤمنة؛
- تحميل إذن النفاذ على مكوّن *إدارة خدمة تبادل البيانات* من خلال قناة إرسال مؤمنة.

### 2.2.7 فك تغليف البيانات حسب الإذن المطلوب

دعماً لنفاذ المستعملين إلى البيانات المتبادلة وفقاً للإذن المطلوب، يحتاج *مستهلك البيانات* في الشكل 1 إلى التعزيز من خلال إدخال وظيفة أمن منطقية جديدة، *وفك تغليف البيانات وفقاً للإذن المطلوب* الذي يتمتع بالقدرات التالية:

- الحصول على عنوان لتنفيذ العقد الذكي المتعلق بتبادل البيانات؛
- الاتصال *بإدارة خدمة تبادل البيانات*، وتنفيذ العقد الذكي المتعلق بتبادل البيانات والحصول على الإذن المطلوب الذي يتضمن أوقات النفاذ، ووقت انتهاء الصلاحية، والتحديد لأغراض القراءة فقط، ومعرّف المفتاح وعنوان تخزينه، ومعرّف رزمة تبادل البيانات وعنوان تخزينها؛
- الاتصال *بمخدم تخزين المفاتيح* للحصول على مفتاح التجفير؛
- الاتصال *بمخدم تخزين البيانات* للحصول على رزمة تبادل البيانات التي تتضمن بيانات مجفرة وبيانات شرحية؛
- التحقق من صحة رزمة تبادل البيانات المستلمة بناءً على التوقيع في البيانات الشرحية؛
- فك تجفير البيانات المجفرة بناءً على مفتاح التجفير؛
- تقديم البيانات المتبادلة بنص عادي للمستعملين حسب الإذن المطلوب؛
- تجفير البيانات المتبادلة بالطريقة نفسها التي يقوم بها مورّدو البيانات بعد الانتهاء من النفاذ إلى البيانات.

### 3.2.7 إدارة إذن النفاذ

دعماً للمستعملين في وضع إذن النفاذ إلى البيانات المتبادلة أو لدعم المستعملين في النفاذ إلى البيانات المتبادلة وفقاً للإذن المطلوب، تحتاج *إدارة خدمة تبادل البيانات* في الشكل 1 إلى التعزيز من خلال تقديم وظيفة أمن منطقية جديدة، أي *إدارة إذن النفاذ*، والتي تتمتع بالقدرات التالية:

- دعم المستعملين في وضع إذن النفاذ إلى البيانات المراد تبادلها:
  - استلام إذن النفاذ الذي وضعه مورّد البيانات من *إدارة سياسة تبادل البيانات*؛
  - تخزين إذن النفاذ؛
  - إرسال الرد إلى إدارة *سياسة تبادل البيانات*؛
- دعم نفاذ المستعملين إلى البيانات المتبادلة حسب الإذن المطلوب:
  - استلام الإذن الذي طلبه *مستهلك البيانات من إدارة النفاذ إلى البيانات وسجل الاستخدام*؛
  - توليد الإذن المطلوب؛
  - إرسال الإذن المطلوب إلى إدارة *النفاذ إلى البيانات وسجل الاستخدام*.

### 4.2.7 إدارة النفاذ إلى البيانات وسجل الاستخدام

دعماً للمستعملين في تتبع استخدام بياناتهم المتبادلة، يتعيّن تحسين *إدارة النفاذ إلى تبادل البيانات وسجل الاستخدام* في الشكل 2 من خلال القدرات التالية:

- الاتصال *بإدارة إذن النفاذ* من أجل الحصول على الإذن المطلوب؛
- تسجيل استخدام البيانات المتبادلة بناءً على الإذن المطلوب.

### 5.2.7 استيقان وتخويل الاتصالات

تحقيقاً لاتصالات مؤمنة، يتعين تعزيز المكونات الوظيفية الخمسة الواردة في الشكل 1 (أي *مورّد البيانات*، و*مستهلك البيانات*، و*إدارة خدمة تبادل البيانات*، و*مخدم تخزين المفاتيح*، و*مخدم تخزين البيانات*) من خلال إدخال وظيفة أمن منطقية جديدة، وهي استيقان وتخويل الاتصالات.

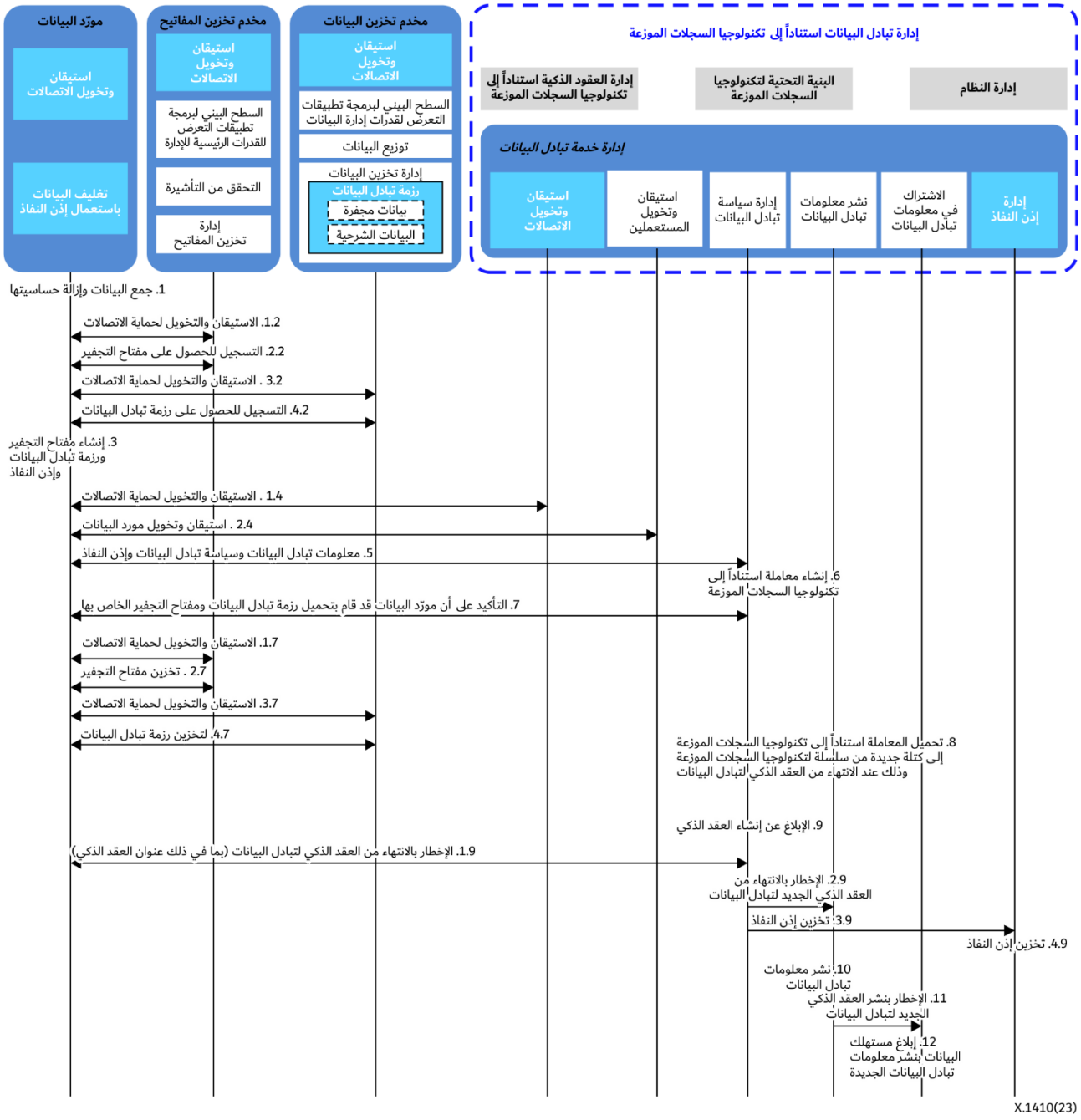
وعندما يرسل *مورّد البيانات* أو *مستهلك البيانات* رسالة الطلب إلى *إدارة خدمة تبادل البيانات*، أو *مخدم تخزين المفاتيح* أو *مخدم تخزين البيانات*، يمكن *لاستيقان وتخويل الاتصالات* دعم:

- *إدارة خدمة تبادل البيانات/مخدم تخزين المفاتيح/مخدم تخزين البيانات* التي تقوم باستيقان *مورّد البيانات/مستهلك البيانات* بناءً على الشهادة [b-IETF RFC 4306] [b-IETF RFC 5246] أو المفتاح المشترك مسبقاً [b-IETF RFC 4279] [b-IETF RFC 4306]؛
- مورّد البيانات/مستهلك البيانات الذي يقوم باستيقان إدارة خدمة تبادل البيانات/مخدم تخزين المفاتيح/مخدم تخزين البيانات على أساس الشهادة [b-IETF RFC 4306] [b-IETF RFC 5246]؛
- *إدارة خدمة تبادل البيانات/مخدم تخزين المفاتيح/مخدم تخزين البيانات* الذي يقوم بتخويل *مورّد البيانات/مستهلك البيانات* على أساس القائمة البيضاء/القائمة السوداء [b-IETF RFC 5782] [b-IETF RFC 5851] أو قائمة التحكم في النفاذ [b-IETF RFC 4314] [b-IETF RFC 4949]؛
- توليد مفتاح الدورة الذي سيُستخدم لحماية الاتصالات بين مورّد البيانات/مستهلك البيانات وإدارة خدمة تبادل البيانات/مخدم تخزين المفاتيح/مخدم تخزين البيانات.

## 3.7 إجراءات تبادل البيانات بشكل مؤمن

### 1.3.7 الإجراء الخاص بمورّدي البيانات لتبادل البيانات بوضع إذن النفاذ

يوضح الشكل 3 الإجراء الخاص بمورّدي البيانات لتبادل البيانات بوضع إذن النفاذ.




**الشكل 3 – الإجراء الخاص بمورّدي البيانات لتبادل البيانات بوضع إذن النفاذ**

كما هو مبين في الشكل 3، يتم وصف الإجراء على النحو التالي:

1) يقوم *مورّد البيانات* بجمع البيانات الأصلية ويزيل حساسيتها دون أن يكون لذلك تأثير سلبي على جودة البيانات التي سيتم تبادلها.

2) يسجل *مورّد البيانات* رزمة تبادل البيانات ومفتاحها على مخدم تخزين المفاتيح المحلي أو البعيد ومخدم تخزين البيانات على النحو التالي:

1.2) يقوم *مورّد البيانات* ومكوّن *استيقان وتخويل اتصالات مخدم تخزين المفاتيح* بإجراء استيقان متبادل والحصول على مفتاح دورة يستخدم لحماية الاتصالات اللاحقة بينهما؛

2.2) يتصل *مورّد البيانات* *بمخدم تخزين المفاتيح* ويسجل معرف المفتاح والعنوان الذي يمكن من خلاله الحصول عليه؛

3.2) يقوم *مورّد البيانات* ومكوّن *استيقان وتخويل اتصالات مخدم تخزين البيانات* بإجراء استيقان متبادل والحصول على مفتاح دورة يستخدم لحماية الاتصالات اللاحقة بينهما؛

4.2) يتصل *مورّد البيانات* *بمخدم تخزين البيانات* ويسجل معرف رزمة تبادل البيانات وعنوان الحصول عليها.

3) يقوم *مورّد البيانات* باستحداث معلومات تبادل البيانات التي تشمل معرف مورّد البيانات، والمفتاح العمومي لمورّد البيانات، ومعرف رزمة تبادل البيانات وعنوان تخزينها، ومعرف المفتاح وعنوان التخزين الخاص به، والصناعات التي يُسمح لها بالنفاذ، والمستعملين الذين يُسمح لهم بالنفاذ وخصائص البيانات الأخرى (على سبيل المثال، فئة البيانات ومقدمة البيانات والاستخدام والسعر).

يقوم *مورّد البيانات* بإنشاء مفتاح يتم استخدامه لتجفير البيانات التي سيتم تبادلها.

يضع *مورّد البيانات* إذن النفاذ إلى البيانات الذي يتضمن أوقات النفاذ، ووقت انتهاء الصلاحية، والتحديد للقراءة فقط، ومعرف المفتاح وعنوان التخزين الخاص به، ومعرف رزمة تبادل البيانات وعنوان تخزينها الذي سيتم تبادله؛

يضع *مورّد البيانات* البيانات الشرحية التي تتضمن معرف رزمة تبادل البيانات ومعرف مورّد البيانات والمفتاح العمومي لمورّد البيانات وتوقيع المعلومات السابقة؛

يقوم *مورّد البيانات* بإنشاء رزمة تبادل البيانات، والتي تتضمن البيانات المجفرة والبيانات الشرحية.

4) قبل نشر البيانات المراد تبادلها، من الضروري أن:

1.4) يقوم *مورّد البيانات* ومكوّن *استيقان وتخويل اتصالات إدارة خدمة تبادل البيانات* بإجراء الاستيقان المتبادل والحصول على مفتاح دورة يستخدم لحماية الاتصالات اللاحقة بينهما.

2.4) يقوم *مورّد البيانات* ومكوّن *استيقان وتخويل مستعملي إدارة خدمة تبادل البيانات* بإجراء الاستيقان المتبادل. وبعد نجاح الاستيقان المتبادل، يتحقق مكوّن *استيقان وتخويل المستعملين* مما إذا كان *لمورّد البيانات* الحق في نشر البيانات التي يتعين تبادلها.

5) يوفر *مورّد البيانات* معلومات تبادل البيانات وفقاً لمتطلبات *إدارة سياسة تبادل البيانات* التابعة *لإدارة خدمة تبادل البيانات*. ويضع *مورّد البيانات* سياسة لتبادل البيانات مع معلومات تبادل البيانات والمعلومات الأخرى. ويرسل معلومات تبادل البيانات وسياسة تبادل البيانات وإذن النفاذ والتوقيع الرقمي إلى *إدارة سياسة تبادل البيانات*.

6) وبعد استلام معلومات تبادل البيانات وسياسة تبادل البيانات وإذن النفاذ والتوقيع الرقمي المقابل من *مورّد البيانات*، تتحقق *إدارة سياسة تبادل البيانات* من التوقيع الرقمي ثم تنشئ المعاملة الخاصة بتكنولوجيا السجلات الموزعة.

7) وتؤكد *إدارة سياسة تبادل البيانات* مع *مورّد البيانات* أنه تم تخزين المفتاح ورزمة تبادل البيانات على *مخدم تخزين المفاتيح* و*مخدم تخزين البيانات*، على التوالي. وإذا لم يكن الأمر كذلك، فيتعين اتخاذ الخطوات التالية:

1.7) يقوم *مورّد البيانات* ومكوّن *استيقان وتخويل اتصالات مخدم تخزين المفاتيح* بإجراء استيقان متبادل والحصول على مفتاح دورة يستخدم لحماية الاتصالات اللاحقة بينهما؛

2.7) يتصل مورّد البيانات بمخدم تخزين المفاتيح ويخزن المفتاح عليه؛

3.7) يقوم *مورّد البيانات* ومكوّن *استيقان وتخويل اتصالات مخدم تخزين البيانات* بإجراء استيقان متبادل والحصول على مفتاح دورة يستخدم لحماية الاتصالات اللاحقة بينهما؛

4.7) يتصل *مورّد البيانات* *بمخدم تخزين البيانات* ويخزن رزمة تبادل البيانات عليه.

8) ترسل *إدارة سياسة تبادل البيانات* معاملةً أو أكثر من المعاملات القائمة على تكنولوجيا السجلات الموزعة جنباً إلى جنب مع توقيعاتها الرقمية إلى المكونات الأساسية *للبنية التحتية لتكنولوجيا السجلات الموزعة* و*إدارة العقود الذكية القائمة على تكنولوجيا السجلات الموزعة* لتشكيل كتلة جديدة تنطوي على عقد ذكي واحد أو أكثر لتبادل البيانات. وتُوزع الكتلة التي تم إنشاؤها حديثًا على عقد تكنولوجيا السجلات الموزعة ذات الصلة. ويعتمد تحميل معاملات تكنولوجيا السجلات

الموزعة على سلسلة التكنولوجيا، على تكنولوجيا التنفيذ المحددة الأساسية (على سبيل المثال، نسيج السجل الفوقي ونصاب Ethereum)، والتي تقع خارج نطاق هذه التوصية.

9) وتُبلّغ *إدارة سياسة تبادل البيانات* المكونات ذات الصلة بإنشاء العقد الذكي لتبادل.

1.9) تُخطر *إدارة سياسة تبادل البيانات موزّد البيانات* باكتمال العقد الذكي لتبادل البيانات. ويتضمن الإخطار عنوان تنفيذ العقد الذكي.

2.9) تُخطر *إدارة سياسة تبادل البيانات مكوّن نشر المعلومات عن تبادل البيانات باكتمال* العقد الذكي لتبادل البيانات. ويتضمن الإخطار عنوان تنفيذ العقد الذكي ومعلومات تبادل البيانات.

3.9) تُخطر *إدارة سياسة تبادل البيانات إدارة أذونات النفاذ باكتمال* العقد الذكي لتبادل البيانات. ويتضمن الإخطار عنوان تنفيذ العقد الذكي وإذن النفاذ.

4.9) تقوم *إدارة إذن النفاذ* بتخزين إذن النفاذ.

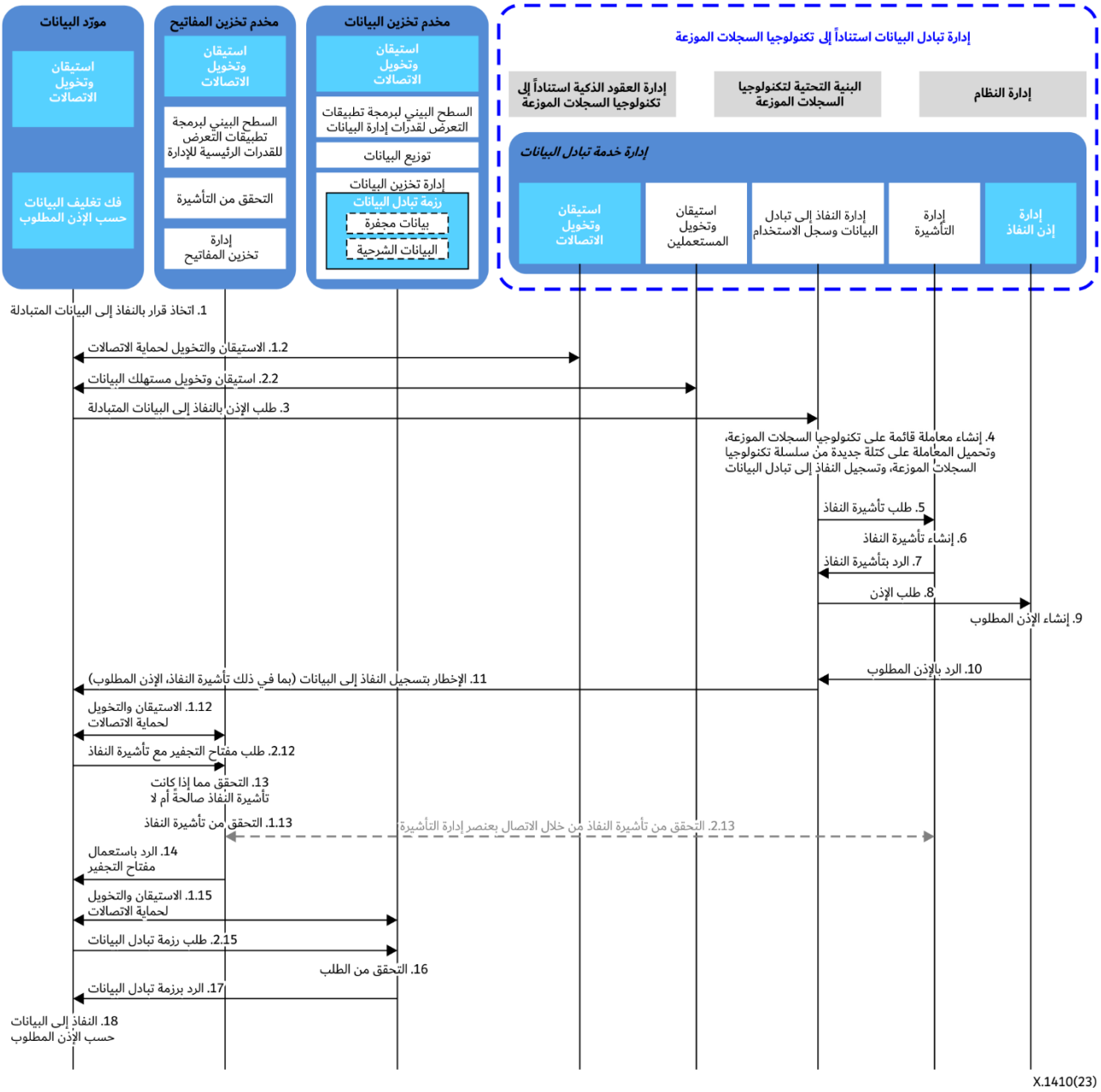
10 وبعد استلام الإخطار من *إدارة سياسة تبادل البيانات*، يقوم *مكوّن نشر معلومات تبادل البيانات* بنشر المعلومات الجديدة المستلمة.

11 ويُخطر *مكوّن نشر معلومات تبادل البيانات مكوّن الاشتراك في معلومات تبادل البيانات* باكتمال العقد الذكي لتبادل البيانات. ويتضمن الإخطار عنوان تنفيذ العقد الذكي ومعلومات عن تبادل البيانات الجديدة.

12 وبعد استلام الإخطار من *مكوّن نشر معلومات تبادل البيانات*، يُرسل *مكوّن الاشتراك في معلومات تبادل البيانات* عنوان تنفيذ العقد الذكي ومعلومات تبادل البيانات الجديدة إلى المشتركين.

### 2.3.7 الإجراء الخاص بمستهلكي البيانات للنفاذ إلى البيانات المتبادلة وفقاً للإذن المطلوب

يوضح الشكل 4 الإجراء الخاص بمستهلكي البيانات للنفاذ إلى البيانات المتبادلة وفقاً للإذن المطلوب.




**الشكل 4 – الإجراء الخاص بمستهلكي البيانات للنفاذ إلى البيانات المتبادلة وفقاً للإذن المطلوب**

كما هو مبين في الشكل 4، يتم وصف الإجراء الخاص بمستهلكي البيانات للنفاذ إلى البيانات المتبادلة وفقاً للإذن المطلوب على النحو التالي:

1) يحصل *مستهلك البيانات* على معلومات تبادل البيانات من خلال البحث في مكوّن *نشر المعلومات عن تبادل البيانات*، أو الاشتراك في المعلومات المنشورة أو التي أُعيد توجيهها من أشخاص آخرين. ويقرر *مستهلك البيانات* النفاذ إلى البيانات المتبادلة، وينفذ العقد الذكي لتبادل البيانات.

2) وقبل تنفيذ العقد الذكي لتبادل البيانات من أجل النفاذ إلى البيانات المتبادلة، يتم تنفيذ العمليات التالية.

1.2) يجري *مستهلك البيانات* ومكون *استيقان وتخويل اتصالات إدارة خدمة تبادل البيانات* الاستيقان المتبادل ويحصل على مفتاح دورة يُستخدم لحماية الاتصالات اللاحقة بينهما.

2.2) يضمن *مستهلك البيانات* الاستيقان المتبادل مع مكوّن *استيقان وتخويل مستعملي إدارة خدمة تبادل البيانات*. وبعد نجاح الاستيقان المتبادل، يتحقق مكوّن *استيقان وتخويل المستعملين* مما إذا كان مستهلك البيانات لديه الحق في النفاذ إلى البيانات المتبادلة.

3) ويرسل *مستهلك البيانات* معلومات هويته (مثل المعرف والمفتاح العمومي) ومعلومات تبادل البيانات جنباً إلى جنب مع توقيعه الرقمي إلى *إدارة النفاذ إلى تبادل البيانات وسجل الاستخدام*.

4) وبعد استلام معلومات هوية *مستهلك البيانات* ومعلومات تبادل البيانات وتوقيعه الرقمي، تتحقق *إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام* من التوقيع الرقمي ثم يتحققان مما إذا كان يُسمح لمستهلك البيانات بالنفاذ إلى البيانات وفقاً لسياسة تبادل البيانات (على سبيل المثال، يمكن فقط لمستهلك البيانات من صناعة ما أو بلد محدد النفاذ إلى البيانات المتبادلة). وإذا تم استيفاء جميع متطلبات النفاذ إلى البيانات المتبادلة، فإن *إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام* يقومان بإنشاء معاملة قائمة على تكنولوجيا السجلات الموزعة وفقًا للمعلومات المستلمة من مستهلك البيانات. وترسل *إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام* معاملةً واحدة أو أكثر من المعاملات القائمة على تكنولوجيا السجلات الموزعة جنباً إلى جنب مع توقيعه الرقمي إلى المكونات الأساسية *للبنية التحتية لتكنولوجيا السجلات الموزعة* و*إدارة العقود الذكية القائمة على تكنولوجيا السجلات الموزعة* لتشكيل كتلة جديدة تحتوي على سجل أو أكثر من سجلات النفاذ إلى البيانات. وتُوزع الكتلة التي تم إنشاؤها حديثاً على عقد شبكة تكنولوجيا السجلات الموزعة ذات الصلة. ويعتمد تحميل معاملات تكنولوجيا السجلات الموزعة على سلسلة تكنولوجيا السجلات الموزعة على تكنولوجيا التنفيذ المحددة الأساسية (على سبيل المثال، نسيج السجل الفوقي، نصاب Ethereum)، والتي تقع خارج نطاق هذه التوصية.

5) وتُخطر إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام إدارة التأشيرة بإنشاء تأشيرة النفاذ.

6) وبعد استلام الإخطار من إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام، تنشئ إدارة التأشيرة، تأشيرة النفاذ.

7) وترسل إدارة التأشيرة، تأشيرة النفاذ التي تم إنشاؤها إلى إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام.

8) وتُخطر *إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام* إدارة أذونات النفاذ لإنشاء الإذن المطلوب.

9) وبعد استلام الإخطار من إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام، تنشئ إدارة أذونات النفاذ الإذن المطلوب.

10) وترسل إدارة أذونات النفاذ الإذن المطلوب إلى إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام.

11) وبعد استلام تأشيرة النفاذ والإذن المطلوب، تسجل *إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام* استعمال البيانات المتبادلة وترسل تأشيرة النفاذ، والإذن المطلوب، ومعلومات المفاتيح (على سبيل المثال، المعرف وعنوان التخزين الخاص به)، ومعلومات عن رزمة تبادل البيانات (على سبيل المثال، المعرف وعنوان التخزين الخاص به)، ومعلومات أخرى (مثل الشهادات الرقمية *لمخدم تخزين المفاتيح* و*مخدم تخزين البيانات*) *لمستهلك البيانات*.

12) وبعد استلام تأشيرة النفاذ والإذن المطلوب ومعلومات المفاتيح ومعلومات رزمة تبادل البيانات من *إدارة النفاذ إلى البيانات المتبادلة وسجل الاستخدام*، يقوم *مستهلك البيانات* بالعمليات التالية:

1.12) يجري *مستهلك البيانات* ومكون *استيقان وتخويل اتصالات مخدم تخزين المفاتيح* الاستيقان المتبادل ويحصل على مفتاح دورة يُستخدم لحماية الاتصالات اللاحقة بينهما؛

2.12) يرسل *مستهلك البيانات* تأشيرة النفاذ إلى مكوّن *التحقق من التأشيرة* التابع *لمخدم تخزين المفاتيح* وفقاً لعنوان تخزين المفاتيح للحصول على مفتاح التجفير.

13) ويتحقق مكوّن *التحقق من التأشيرة* التابع *لمخدم تخزين المفاتيح* مما إذا كانت تأشيرة النفاذ صالحةً.

1.13) يستقبل مكوّن *التحقق من التأشيرة* التابع *لمخدم تخزين المفاتيح*، تأشيرة النفاذ من *مستهلك البيانات* ثم يتحقق منها.

2.13) قد يتعين على مكوّن التحقق من التأشيرة، اختيارياً، الاتصال بإدارة التأشيرة لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة عند التحقق من تأشيرة النفاذ.

14) ويرسل مكوّن التحقق من التأشيرة نتيجة التحقق إلى إدارة تخزين المفاتيح لمخدم تخزين المفاتيح. وبعد استلام نتيجة التحقق المقدمة من عنصر التحقق من التأشيرة، ترسل إدارة تخزين المفاتيح لمخدم تخزين المفاتيح المفتاح إلى مستهلك البيانات.

15) وبعد استلام المفتاح من إدارة تخزين المفاتيح لمخدم تخزين المفاتيح، يقوم مستهلك البيانات بالعمليات التالية.

1.15) يجري *مستهلك البيانات* ومكوّن *استيقان وتخويل اتصالات مخدم تخزين البيانات* الاستيقان المتبادل ويحصل على مفتاح دورة يُستخدم لحماية الاتصالات اللاحقة بينهما؛

2.15) يرسل *مستهلك البيانات* الطلب إلى *مخدم تخزين البيانات* للحصول على رزمة تبادل البيانات.

16) وبعد استلام الطلب من مستهلك البيانات، يقوم مكوّن توزيع البيانات التابع لمخدم تخزين البيانات باستيقان مستهلك البيانات.

17) ويرسل مكوّن توزيع البيانات التابع لمخدم تخزين البيانات رزمة تبادل البيانات إلى مستهلك البيانات.

18) ويقوم *مستهلك البيانات* بالنفاذ إلى البيانات حسب الإذن المطلوب. ويقوم بتجفير البيانات المتبادلة بالطريقة نفسها التي يقوم بها *موزّد البيانات* بعد الانتهاء من النفاذ إلى البيانات.

# الملحق A

## إجراءات إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

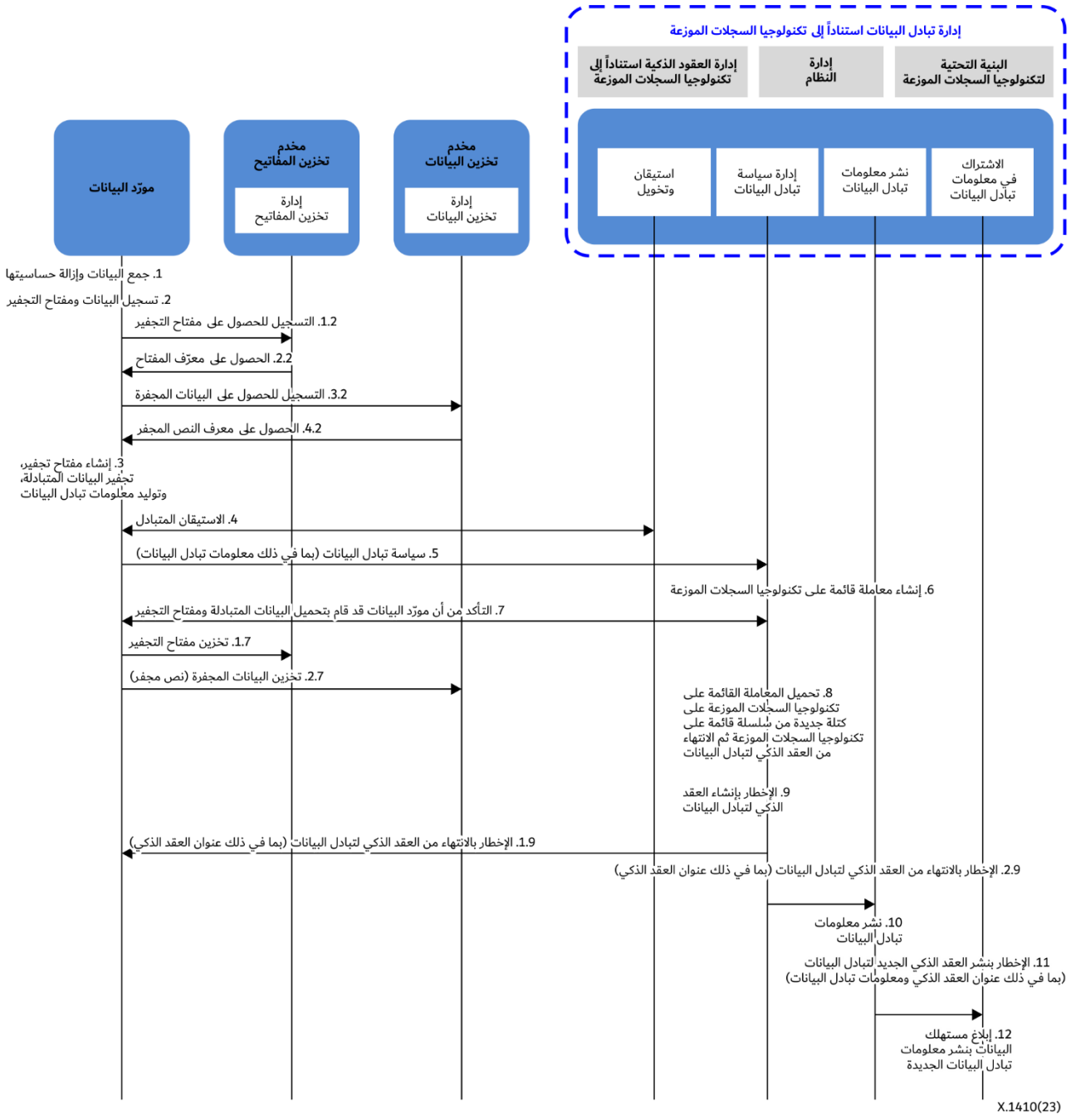
يصف هذا الملحق إجراءين رئيسيين: 1) إجراء لمورّد البيانات من أجل نشر البيانات التي سيتم تبادلها استناداً إلى تكنولوجيا السجلات الموزعة؛ 2) وإجراء لمستهلك البيانات من أجل النفاذ إلى البيانات المتبادلة استناداً إلى تكنولوجيا السجلات الموزعة.

وقبل وصف إجراءات إدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة، من المفترض تحقيق الشروط التالية:

- حصول كل مستعمل (على سبيل المثال، *مورّد البيانات*، و*مستهلك البيانات*) على شهادة رقمية ومفتاحها الخاص المقابل، ذاتي المنشأ أو من سلطة إصدار الشهادات؛
- إجراء كل مستعمل للتشكيلات الصحيحة المقابلة (مثل الشهادة الرقمية لعقدة تكنولوجيا السجلات الموزعة، ومعلمات توصيل شبكة تكنولوجيا السجلات الموزعة، وتوفير الشبكة)؛
- إتاحة أنظمة التجفير المتناظر للمستعملين (على سبيل المثال، *مورّد البيانات*، و*مستهلك البيانات*). وهي توفر قوة تجفير كافية لضمان سرية البيانات.
- تعمل البنية التحتية لتكنولوجيا السجلات الموزعة وإدارة العقود الذكية استناداً إلى تكنولوجيا السجلات الموزعة بشكل صحيح؛
- تعمل شبكة تكنولوجيا السجلات الموزعة بشكل صحيح؛
- يعمل مخدم تخزين المفاتيح ومخدم تخزين البيانات بشكل صحيح.

### 1.A الإجراء الخاص بمورّد البيانات من أجل نشر البيانات التي سيتم تبادلها والقائمة على تكنولوجيا السجلات الموزعة

يوضح الشكل 1.A الإجراء الخاص بمورّد البيانات من أجل نشر البيانات التي سيتم تبادلها استناداً إلى تكنولوجيا السجلات الموزعة.




**الشكل 1.A – الإجراء الخاص بمورّد البيانات من أجل نشر البيانات التي سيتم تبادلها استناداً إلى تكنولوجيا السجلات الموزعة**

كما هو مبين في الشكل 1.A، يتم وصف الإجراء على النحو التالي:

1) يقوم *مورّد البيانات* بجمع البيانات الأصلية ويزيل حساسيتها دون أن يؤثر بالسلب على جودة البيانات التي سيتم تبادلها.

2) ويقوم *مورّد البيانات* بتسجيل البيانات المراد تبادلها ومفتاح نظام التجفير المتناظر على مخدم تخزين المفاتيح المحلي أو البعيد ومخدم تخزين البيانات على النحو التالي:

1.2) إنشاء مفتاح تجفير البيانات المستخدم لنظام التجفير المتناظر.

2.2) يحصل *مورّد البيانات* على معرف المفتاح وعنوان التخزين الخاص به من *مخدم تخزين المفاتيح*؛

3.2) تجفير البيانات بمفتاح يستخدم نظام التجفير المتناظر، وتسجيل البيانات المجفرة، أي النص المجفر؛

4.2) يحصل *مورّد البيانات* على معرف النص المجفر وعنوان التخزين الخاص به من *مخدم تخزين البيانات*.

3) ويقوم *مورّد البيانات* بإنشاء مفتاح تجفير البيانات، ويُجفر البيانات المقرر تبادلها بمفتاح التشفير الذي تم إنشاؤه. إن البيانات المجفرة هي نص مجفر. ويقوم أيضاً بإنشاء معلومات تبادل البيانات التي تشمل معرف مورّد البيانات، والمفتاح العمومي لمورّد البيانات، ومعرف رزمة تبادل البيانات وعنوان تخزينها، ومعرف المفتاح وعنوان التخزين الخاص به، والصناعات التي يُسمح لها بالنفاذ، والمستعملين الذين يُسمح لهم بالنفاذ ونعوت البيانات الأخرى (على سبيل المثال، فئة البيانات ومقدمة البيانات والاستخدام والسعر).

4) قبل نشر البيانات المقرر تبادلها، من الضروري أن يضمن *مورّد البيانات* الاستيقان المتبادل مع مكوّن *استيقان وتخويل المستعملين* التابع *لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة*. ويمكن استخدام شهادة اعتماد رقمية في الاستيقان المتبادل. وبعد نجاح الاستيقان المتبادل، يتحقق مكوّن *استيقان وتخويل المستعملين* مما إذا كان لمورّد البيانات الحق في نشر البيانات المقرر تبادلها.

5) وبعد نجاح الاستيقان والتخويل، يوفر *مورّد البيانات* معلومات تبادل البيانات وفقاً لمتطلبات *إدارة سياسة تبادل البيانات* التابعة *لإدارة تبادل البيانات استناداً إلى تكنولوجيا السجلات الموزعة*. ويضع *مورّد البيانات* سياسة تبادل البيانات باستخدام معلومات تبادل البيانات ومعلومات أخرى. ويرسل سياسة تبادل البيانات والتوقيع الرقمي إلى *إدارة سياسة تبادل البيانات*.

6) وبعد استلام سياسة تبادل البيانات والتوقيع الرقمي المقابل من *مورّد البيانات*، تتحقق *إدارة سياسة تبادل البيانات* من التوقيع الرقمي ثم تنشئ معاملة قائمة على تكنولوجيا السجلات الموزعة.

7) وتتأكد *إدارة سياسة تبادل البيانات* مع *مورّد البيانات* أنه تم تخزين المفتاح والنص المجفر على *مخدم تخزين المفاتيح* و*مخدم تخزين البيانات*، على التوالي. وإذا لم يكن الأمر كذلك، فيجب اتخاذ الخطوات التالية:

1.7) يقوم مورّد البيانات بتخزين المفتاح على مخدم تخزين المفاتيح؛

2.7) يقوم *مورّد البيانات* بتخزين النص المجفر على *مخدم تخزين البيانات*.

8) وترسل *إدارة سياسة تبادل البيانات* معاملةً أو أكثر من المعاملات القائمة على تكنولوجيا السجلات الموزعة جنباً إلى جنب مع توقيعها الرقمي إلى المكونات الأساسية *للبنية التحتية لتكنولوجيا السجلات الموزعة* و*إدارة العقود الذكية القائمة على تكنولوجيا السجلات الموزعة* لإنشاء كتلة جديدة تنطوي على عقد ذكي واحد أو أكثر لتبادل البيانات. وتُوزع الكتلة التي تم إنشاؤها حديثاً على عقد تكنولوجيا السجلات الموزعة ذات الصلة. ويعتمد تحميل معاملات تكنولوجيا السجلات الموزعة على سلسلة تكنولوجيا السجلات الموزعة، على تكنولوجيا التنفيذ المحددة الأساسية (على سبيل المثال، نسيج السجل الفوقي، ونصاب Ethereum)، والتي تقع خارج نطاق هذه التوصية.

9) وتُخطر *إدارة سياسة تبادل البيانات* المكونات ذات الصلة بإنشاء العقد الذكي لتبادل البيانات.

1.9) تُخطر *إدارة سياسة تبادل البيانات* *مورّد البيانات* باكتمال العقد الذكي لتبادل البيانات. ويتضمن الإخطار عنوان تنفيذ العقد الذكي.

2.9) تُخطر *إدارة سياسة تبادل البيانات* مكوّن *نشر معلومات تبادل البيانات* باكتمال العقد الذكي لتبادل البيانات. ويتضمن الإخطار عنوان تنفيذ العقد الذكي ومعلومات تبادل البيانات.

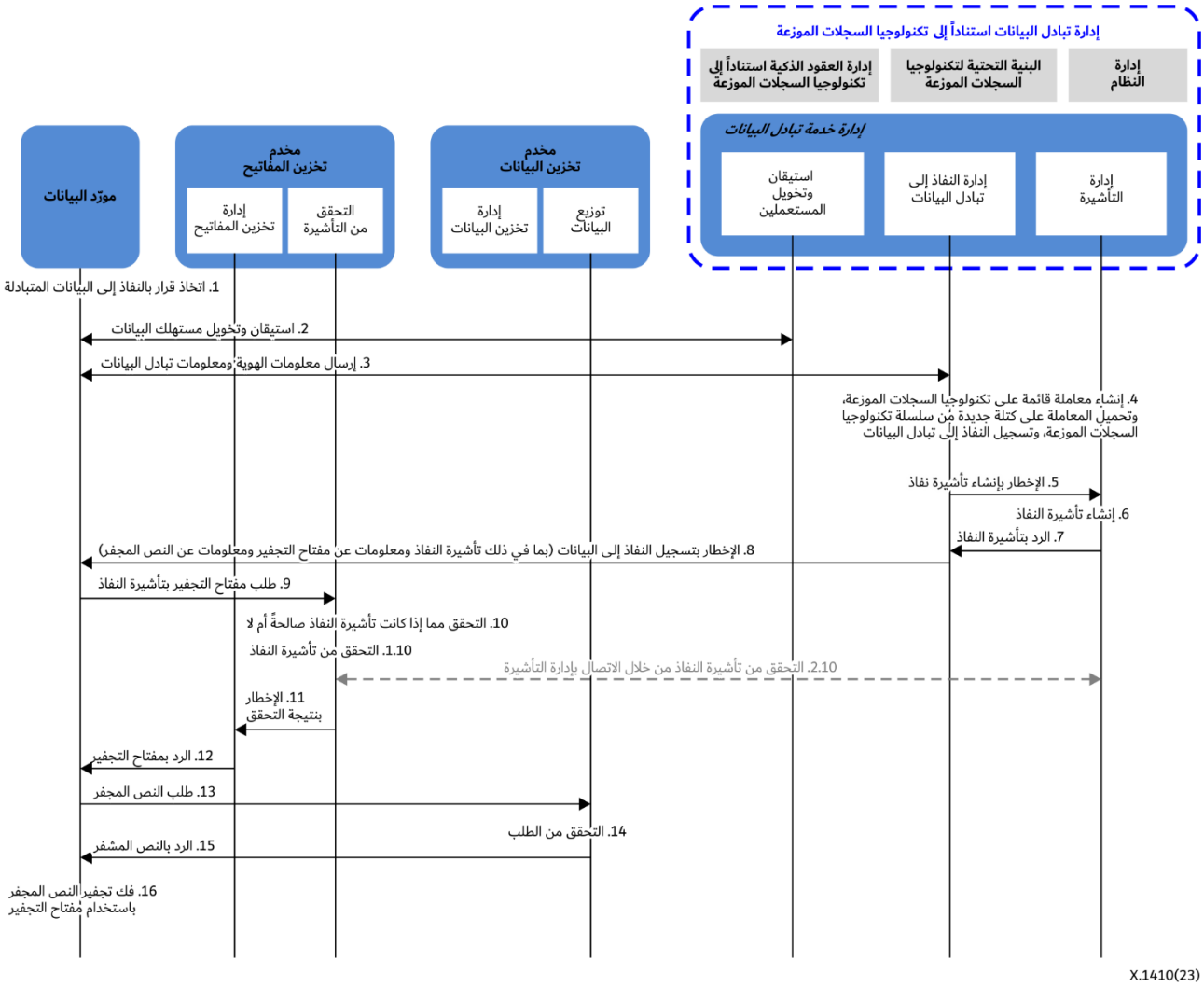
10) وبعد استلام الإخطار من *إدارة سياسة تبادل البيانات*، يقوم مكوّن *نشر معلومات تبادل البيانات* بنشر المعلومات الجديدة المستلمة.

11) ويُخطر مكوّن *نشر معلومات تبادل البيانات* مكوّن *الاشتراك في معلومات تبادل البيانات* باكتمال العقد الذكي لتبادل البيانات. ويتضمن الإخطار عنوان تنفيذ العقد الذكي ومعلومات تبادل البيانات الجديدة.

12) وبعد استلام الإخطار من مكوّن *نشر معلومات تبادل البيانات*، يُرسل مكوّن *الاشتراك في معلومات تبادل البيانات* عنوان تنفيذ العقد الذكي ومعلومات تبادل البيانات الجديدة إلى المشترك.

## 2.A الإجراء الخاص بمستهلك البيانات من أجل النفاذ إلى البيانات استناداً إلى تكنولوجيا الحسابات الموزعة

يوضح الشكل 2.A الإجراء الخاص بمستهلك البيانات من أجل النفاذ إلى البيانات استناداً إلى تكنولوجيا الحسابات الموزعة




**الشكل 2.A – الإجراء الخاص بمستهلك البيانات**
**من أجل النفاذ إلى البيانات استناداً إلى تكنولوجيا الحسابات الموزعة**

كما هو مبين في الشكل 2.A، يتم وصف الإجراء على النحو التالي:

1) يحصل *مستهلك البيانات* على معلومات تبادل البيانات من خلال البحث في مكوّن *نشر معلومات تبادل البيانات*، والاشتراك في المعلومات المنشورة أو التي أُعيد توجيهها من أشخاص آخرين. ويقرر *مستهلك البيانات* النفاذ إلى البيانات المتبادلة وينفذ العقد الذكي لتبادل البيانات.

2) وقبل تنفيذ العقد الذكي لتبادل البيانات من أجل النفاذ إلى البيانات المتبادلة، يضمن *مستهلك البيانات* الاستيقان المتبادل مع مكوّن *استيقان وتخويل مستعملي إدارة تبادل البيانات استناداً إلى تكنولوجيا الحسابات الموزعة*. ويوصى باستخدام شهادة اعتماد رقمية في الاستيقان المتبادل. وبعد نجاح الاستيقان المتبادل، يتحقق مكوّن *استيقان وتخويل المستعملين* مما إذا كان مستهلك البيانات لديه الحق في النفاذ إلى البيانات المتبادلة.

3) وبعد نجاح الاستيقان والتخويل، يرسل *مستهلك البيانات* معلومات هويته (مثل المعرف والمفتاح العمومي) ومعلومات تبادل البيانات جنباً إلى جنب مع توقيعه الرقمي إلى *إدارة النفاذ إلى تبادل البيانات*.

4) وبعد استلام معلومات هوية مستهلك البيانات ومعلومات تبادل البيانات وتوقيعه الرقمي، تتحقق *إدارة النفاذ إلى البيانات* من التوقيع الرقمي ثم تتحقق مما إذا كان يُسمح لمستهلك البيانات بالنفاذ إلى البيانات وفقاً لسياسة تبادل البيانات (على سبيل المثال، يمكن فقط لمستهلك البيانات من صناعة ما أو بلد محدد النفاذ إلى البيانات المتبادلة). وإذا تم استيفاء جميع متطلبات النفاذ إلى البيانات المتبادلة، تُنشئ *إدارة النفاذ إلى البيانات المتبادلة* معاملة قائمة على تكنولوجيا السجلات الموزعة وفقاً للمعلومات المستلمة من مستهلك البيانات. وترسل *إدارة النفاذ إلى البيانات المتبادلة* معاملةً واحدة أو أكثر من المعاملات القائمة على تكنولوجيا السجلات الموزعة جنباً إلى جنب مع توقيعاتها الرقمية إلى المكونات الأساسية *للبنية التحتية لتكنولوجيا السجلات الموزعة* و*إدارة العقود الذكية القائمة على تكنولوجيا السجلات الموزعة* لإنشاء كتلة جديدة تحتوي على سجل أو أكثر من سجلات النفاذ إلى البيانات. وتُوزع الكتلة التي تم إنشاؤها حديثاً على عقد شبكة تكنولوجيا السجلات الموزعة ذات الصلة. ويعتمد تحميل معاملات تكنولوجيا السجلات الموزعة على تكنولوجيا السجلات الموزعة على تكنولوجيا التنفيذ المحددة الأساسية (على سبيل المثال، نسيج السجل الفوقي، نصاب Ethereum)، والتي تقع خارج نطاق هذه التوصية.

5) وتُخطر إدارة النفاذ إلى البيانات المتبادلة إدارة التأشيرة بإنشاء تأشيرة النفاذ.

6) وبعد استلام الإخطار من إدارة النفاذ إلى البيانات المتبادلة، تنشئ إدارة التأشيرة، تأشيرة النفاذ.

7) وترسل إدارة التأشيرة، تأشيرة النفاذ التي تم إنشاؤها إلى إدارة النفاذ إلى البيانات المتبادلة.

8) وبعد استلام تأشيرة النفاذ، ترسل *إدارة النفاذ إلى البيانات المتبادلة* التأشيرة، ومعلومات المفتاح (على سبيل المثال، المعرف وعنوان التخزين الخاص به)، ومعلومات عن النص المجفر (على سبيل المثال، المعرف وعنوان التخزين الخاص به)، ومعلومات أخرى (مثل الشهادات الرقمية *لمخدم تخزين المفاتيح* و*مخدم تخزين البيانات*) إلى *مستهلك البيانات*.

9) وبعد استلام تأشيرة النفاذ ومعلومات المفتاح ومعلومات النص المجفر من *إدارة النفاذ إلى البيانات المتبادلة*، يرسل *مستهلك البيانات* تأشيرة النفاذ إلى *مكوّن التحقق* منها *التابع لمخدم تخزين المفاتيح* وفقاً لعنوان تخزين المفاتيح من أجل الحصول على مفتاح التجفير الذي يتم استخدامه لفك تجفير النص المجفر.

10) ويتحقق مكوّن *التحقق من التأشيرة* مما إذا كانت تأشيرة النفاذ صالحةً.

1.10) يستقبل مكوّن التحقق من التأشيرة التابع لمخدم تخزين المفاتيح، تأشيرة النفاذ من مستهلك البيانات ثم يتحقق منها.

2.10) قد يتعين على عنصر التحقق من التأشيرة، اختيارياً، الاتصال بإدارة التأشيرة التابعة لإدارة تبادل البيانات استناداً إلى تكنولوجيا الحسابات الموزعة عند التحقق من تأشيرة النفاذ.

11) ويرسل مكوّن التحقق من التأشيرة نتيجة التحقق إلى إدارة تخزين المفاتيح.

12) وبعد تلقي نتيجة التحقق من *عنصر التحقق من التأشيرة*، ترسل *إدارة تخزين المفاتيح* مفتاح التجفير إلى *مستهلك البيانات*.

13) وبعد استلام مفتاح التجفير من *إدارة تخزين المفاتيح*، يرسل *مستهلك البيانات* طلباً إلى *مخدم تخزين البيانات* للحصول على النص المجفر.

14) وبعد استلام الطلب من مستهلك البيانات، يقوم مكوّن توزيع البيانات التابع لمخدم تخزين البيانات باستيقان مستهلك البيانات.

15) ويرسل مكوّن توزيع البيانات التابع لمخدم تخزين البيانات النص المجفر إلى مستهلك البيانات.

16) ويقوم *مستهلك البيانات* بفك تجفير النص المجفر باستخدام مفتاح التجفير ثم يقوم بالنفاذ إلى البيانات المتبادلة التي تكون في شكل نص عادي.

# بيبليوغرافيا


[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

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

[b-ITU-T X.1402] Recommendation ITU-T X.1402 (2020), *Security framework for distributed ledger technology*.

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

[b-ISO/IEC 18033-1] ISO/IEC 18033-1:2021, *Information security – Encryption algorithms – Part 1: General*.

[b-ISO/IEC 20944-1] ISO/IEC 20944-1:2013, *Information technology – Metadata registries interoperability and bindings (MDR-IB) – Part 1: Framework, common vocabulary, and common provisions for conformance*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework.*

[b-ISO/IEC/IEEE 15939] ISO/IEC/IEEE 15939:2017, Syst*ems and software engineering – Measurement process.*

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-shared key ciphersuites for transport layer security (TLS)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet key exchange (IKEv2) protocol*.

[b-IETF RFC 4314] IETF RFC 4314 (2005), *IMAP4 access control list (ACL) extension*.

[b-IETF RFC 4949] IETF RFC 4949 (2007), *Internet security glossary, version 2*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol: Version 1.2.*

[b-IETF RFC 5782] IETF RFC 5782 (2010), *DNS blacklists and whitelists*.

[b-IETF RFC 5851] IETF RFC 5851 (2010), *Framework and requirements for an access node control mechanism in broadband multi-service networks*.

## 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، 2023