الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

# ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

# X.1258

(2016/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

---

# تعزيز الاستيقان من الكيانات على أساس تجميع النعوت

التوصية ITU-T X.1258

الاتحاد الدولي للاتصالات

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 | |
| 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 | 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 | |
| اتصالات الطوارئ | X.1309-X.1300 |
| أمن شبكات المحاسيس واسعة الانتشار | X.1339–X.1310 |
| التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية | X.1349–X.1340 |
| 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 |

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

**التوصية ITU-T X.1258**

# تعزيز الاستيقان من الكيانات على أساس تجميع النعوت


## ملخص

قد يلزم تجميع النعوت من سلطات نعوت متعددة من أجل تمكين أي طرف معول من تعزيز ثقته في هوية طرف ما. ويمكن النظر إلى التجميع على أنه تعامل مع مجموعة من معرفات الهوية المتفردة عالمياً والمشتركة بين جميع سلطات النعوت. ومن الناحية العملية، لا تملك الكيانات معرف هوية عالمياً ولكنها تملك معرفات هوية ونعوت مختلفة للكيان مخصصة من قبل موردي خدمات الهوية المختلفين (IdSP).

ولمعالجة مشكلة تجميع النعوت في هذا السيناريو، يستعمل مفهوم اتحاد الهوية. فعلى سبيل المثال، إذا كان هناك متجر للكتب الإلكترونية يخطط لعمل تخفيض للكبار، فإنه يتعين عليه الحصول على مجموعة مجمعة من النعوت (بطاقة الائتمان والشريحة العمومية) من اثنين من موردي خدمات الهوية، ولكن بدون أن يعرف الواحد منهما مشاركة الآخر. وفي الإدارة العادية للهويات الاتحادية، لا يمكن لأي كيان أن يقدم نعوتاً إلا من هوية واحدة، غير أن هذه المعاملة تحتاج إلى نعوت من اثنتين. وهناك طرائق متعددة لاتحادات الهويات مثل لغة وسم التأكيد الأمني (SAML) وشيبوليث [b-Shibboleth] والهوية المفتوحة (OpenID) والاستيقان المفتوح (OAuth) وغيرها.

وتطرح التوصية ITU-T X.1258 (X.eaaa) مفهوم تجميع النعوت لتمكين أي كيان من تجميع النعوت من موردي خدمات هوية متعددين. وتجميع النعوت آلية لجمع النعوت الخاصة بأي كيان والتي يتم استرجاعها من موردي خدمات هوية متعددين. ويلزم تجميع النعوت من أجل تجميع النعوت دينامياً عند الطلب. ويمكن لمورد خدمات الهوية أن يدرك وجود طلب بالتجميع عندما يحتاج أي من الكيانات الحصول على خدمة. وإلى جانب ذلك، يمكن أيضاً تطبيق آلية تجميع نعوت متمحورة حول الكيان على الاستيقان من أجل التخفيف من فقدان الخصوصية.


## التسلسل التاريخي

| الصيغة | التوصية | تاريخ الموافقة | لجنة الدراسات | معرف الهوية الفريد* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1258 | 2016-09-07 | 17 | 11.1002/1000/12850 |

## مصطلحات أساسية

تجميع النعوت، إدارة اتحادية للهوية.

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بمعرّف الهوية الفريد للتوصية. ومثال على ذلك http://handle.itu.int/11.1002/1000/11830-en.

## تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة 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 رقم 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 "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

## حقوق الملكية الفكرية

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

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

© ITU 2017

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

# جدول المحتويات

**الصفحة**


1 مجال التطبيق ..... 1

2 المراجع ..... 1

3 التعاريف ..... 1

1.3 المصطلحات المعرَّفة في وثائق أخرى ..... 1

2.3 تعاريف معرّفة في هذه التوصية ..... 1

4 الاختصارات والأسماء المختصرة ..... 2

5 الاصطلاحات ..... 2

6 لمحة عامة ..... 2

7 المعماريات والتدفقات لطرائق تجميع النعوت ..... 3

1.7 الطرائق المدارة من قبل مورد خدمة الهوية ..... 4

2.7 مورد الخدمة (SP) – الطرائق الوسيطة ..... 9

3.7 طريقة الكيان الوسيط ..... 13

8 مقارنة بين طرائق تجميع الاستيقانات ..... 14

بيبليوغرافيا ..... 16

**التوصية ITU-T X.1258**

# تعزيز الاستيقان من الكيانات على أساس تجميع النعوت

## 1 مجال التطبيق

توفر هذه التوصية الاستيقان المعزز على أساس تجميع نعوت الهوية عبر الميادين. وتتناول هذه التوصية الموضوعين التاليين:

- طرائق تجميع نعوت موردي خدمات هوية (IdSP) متعددين؛
- تعزيز الاستيقان على أساس تجميع النعوت.

## 2 المراجع

لا توجد.

## 3 التعاريف

### 1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

**1.1.3 نعت** [b-ITU-T X.1252]: معلومات مرتبطة بكيان تحدد إحدى خصائصه.

**2.1.3 الاستيقان من (كيان)** [b-ITU-T X.1252]: عملية تستعمل لتحقيق قدر كاف من الثقة في الربط بين الكيان والهوية المقدّمة.

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

**3.1.3 دائرة الثقة** [b-ITU-T X.1251]: مجموعة من المعايير الموضوعية لربط المنظمات ضمن اتحاد لأغراض النفاذ الموثوق إلى موارد بعضها البعض. يلاحظ أن دائرة الثقة هي النتيجة النهائية لانضمام منظمات إلى اتحاد ما.

**4.1.3 اتحاد** [b-ITU-T X.1252]: رابطة بين مستعملين وموردي خدمات وموردي خدمة الهوية.

**5.1.3 الهوية** [b-ITU-T X.1252]: تمثيل كيان في شكل واحد أو أكثر من النعوت التي تتيح تمييز الكيان أو الكيانات بالقدر الكافي ضمن سياق. ولأغراض إدارة الهوية (IdM)، يُفهم المصطلح هوية كهوية سياقية (مجموعة فرعية من النعوت)، أي تتحدّد المجموعة المتنوعة من النعوت بإطار ذي ظروف حدّية محددة (السياق) يوجد فيه الكيان ويتفاعل.

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

**6.1.3 مورد خدمة الهوية (IdSP)** [b-ITU-T X.1252]: كيان يقوم بالتحقق من معلومات هويات الكيانات الأخرى مع الحفاظ عليها وإدارتها ويمكن أن يستحدثها ويخصصها.

### 2.3 تعاريف معرّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

**1.2.3 تجميع النعوت:** آلية لجمع النعوت من موردي خدمات هوية متعددين (IdSP).

**ملاحظة** – بمجرد جمع النعوت يتعين تجميعها والتأكد منها من أجل الاستيقان والتخويل.

**2.2.3 ميدان:** تغطية الإدارة لمورد خدمات هوية وحيد (IdSP).

**3.2.3 مورد خدمة (SP):** كيان يوفر الخدمات للعملاء أو لموردي خدمات آخرين.

## 4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

CoT دائرة الثقة *(Circle of Trust)*

DB قاعدة بيانات *(Database)*

ID هوية *(Identity)*

IdM إدارة الهوية *(Identity Management)*

IdSP مورد خدمة الهوية *(Identity Service Provider)*

LS خدمة الربط *(Linking Service)*

OAuth الاستيقان المفتوح *(Open Authentication)*

OpenID هوية مفتوحة *(Open Identity)*

PKI بنية تحتية للمفتاح العمومي *(Public Key Infrastructure)*

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

SP مورد خدمة *(Service Provider)*

SSO تسجيل دخول وحيد *(Single Sign-On)*

VC تعاون افتراضي *(Virtual Collaboration)*

## 5 الاصطلاحات

لا توجد.

## 6 لمحة عامة

تتناول إدارة الهوية (IdM) الإلكترونية، بوجهٍ عام، إدارة أي شكل من أشكال الهوية الرقمية. ويمكن لعملية تطوير الأدلة، كتلك التي تدعمها التوصية [b-ITU-T X.500]، أن تكون المنشأ لإدارة الهوية. وتحدد التوصية [b-ITU-T X.509] الشهادات التي تحتوي على نعوت الهوية. وتعمل شهادات التوصية [b-ITU-T X.509] وأنظمة البنية التحتية للمفتاح العمومي (PKI) لإثبات "هوية" موضوع ما على الخط. لذا، يمكن اعتبار إدارة الهوية كإدارة للمعلومات.

وهوية أي كيان قد تتألف من نعوت تحدد خصائص هذا الكيان في سياقات مختلفة وقد يحتاج الأمر إلى هويات مختلفة حسب السياق والوضع. ويوفر نظام إدارة الهوية أدوات لإدارة هذه الهويات في عالم رقمي. وإدارة الهوية عبارة عن مجموعة من الوظائف والقدرات مثل استحداث/إلغاء الهوية واكتشافها وتبادل معلوماتها. وفي العالم الواقعي، يختار الناس المعلومات التي يمكن كشفها للآخرين مع مراعاة سياق المعلومات وحساسيتها. وفي العالم الرقمي، يجري هذا العمل بدوره بواسطة نظام إدارة الهوية.

واستناداً إلى التكنولوجيات والمعايير المتعلقة بإدارة الهوية، تصنف طرائق أنظمة إدارة الهوية إلى تقليدية ومركزية واتحادية. وتتمثل خصائص الطريقة التقليدية في أن مورد الخدمة (SP) هو من يتولى أمر الهويات ويتواجد في نفس موقع مورد خدمة الهوية (IdSP). ويقوم أي كيان باستحداث هويته الرقمية (ID) لكل مورد خدمة يرغب في الحصول منه على خدمات. وعادةً، لا يتم تبادل الهويات الرقمية للكيانات بين موردي الخدمات المختلفين وينزع هذا النهج إلى تكلفته الأكبر بالنسبة للكيان وموردي الخدمات، على السواء. وقد يحتاج كل مورد خدمة بصورة متكررة إلى مجموعته الخاصة من النعوت لتشكيل الهوية الرقمية للكيان.

وقد استنبطت الطريقة المركزية كحل لعدم المرونة في الطريقة التقليدية ولتبادل الهويات فيما بين موردي الخدمات وهي تقوم على مفهوم الاستيقان الوحيد، تسجيل الدخول لمرة واحدة (SSO). وتحاول الطريقة تفادي أوجه عدم الاتساق والتكرار الموجودة في الطريقة التقليدية بتزويد الكيانات بالقدرة على التفاعل مع موردي خدمات مختلفين دون الحاجة إلى إجراء الاستيقان بصورة متكررة.

وكل مورد خدمة لديه علاقات ثقة مع مورد خدمة الهوية سيعتمد بشكل كامل على استيقانات الكيانات المقدمة من مورد خدمة الهوية هذا. ومود خدمة الهوية هو المسؤول عن استيقان أي كيان وتزويد موردي الخدمات بمعلومات النعوت الخاصة بالكيان ضمن ميدان يمكن أن يمثل شركة أو جامعة، وما إلى ذلك، ويضم كيانات وموردي خدمات متعددين ومورد خدمة هوية واحد. والاستيقان الوحيد (SSO) يريح الكيانات بشكل كبير حيث لن تحتاج إلى إجراء عملية الاستيقان إلا مرة واحدة فقط. وبعدها، يمكن للكيانات استعمال الإثباتات المتحصل عليها مع جميع موردي الخدمات التي ترغب في النفاذ إليهم. بيد أن نقطة ضعف الطريقة المركزية تتمثل في أن مورد الهوية يملك التحكم المطلق في المعلومات الخاصة بكياناته وربما يستخدم هذه المعلومات بأي طريقة كانت. وهذا هو السبب الرئيسي لعدم اعتماد الطريقة المركزية على نطاق واسع.

ولحل المشكلات الناتجة عن الطريقة المركزية، طرحت طريقة الهوية الاتحادية التي تقوم على توزيع مهمة الاستيقان على موردي خدمات هوية متعددين، ينتمون إلى ميادين مختلفة. ويعتمد مفهوم الهوية الاتحادية على علاقات الثقة المقامة بين موردي خدمات هوية متعددين والميادين المقابلة. ولتوصيل معلومات الهوية الموزعة بين مورد خدمة هوية (IdSP) ومورد خدمة، يلزم وجود علاقة ثقة بين الطرفين. ويطلق على علاقة الثقة هذه اسم دائرة الثقة (CoT) والتي يمكنها أن تضم مورد خدمة هوية واحدة أو أكثر وموردي خدمات. وفي أي دائرة ثقة، إذا جرى استيقان المستعمل في مورد خدمة هوية، فإن النفاذ إلى موردي خدمات داخل دائرة الثقة يسمح به دون الحاجة إلى استيقان آخر ونتيجةً لذلك، يحتاج أي مستعمل إلى الاستيقان مرة واحدة فقط داخل أي دائرة ثقة [b-ITU-T X.1251].

وإدارة الهوية الاتحادية نهج لمعالجة مخاطر وجود مورد خدمة هوية واحد وللحد من عمليات تبادل المعلومات مع مورد خدمة الهوية أثناء الاستيقان. وهذه الاتفاقات بين موردي خدمات الهوية تضمن أن الهويات التي تصدر في ميدان ما يعترف بها موردو الخدمات في الميادين الأخرى وأن مفهوم تسجيل الدخول لمرة واحدة سيتاح حتى مع وجود ميادين مختلفة.

وتتمثل الفائدة التي تعود على موردي الخدمات من الهويات الاتحادية في أنه يمكنهم تداول عدد أقل من معلومات الكيانات. وتتبع مبادرة Kantara [b-Kantara] وShibboleth [b-Shibboleth] وHiggins [b-Higgins] طريقة إدارة الهوية الاتحادية. وفي طرائق الهويات الاتحادية، توزع الهويات على مورّدي خدمات هوية مختلفين ويمكن لمعلومات الكيانات أن تتاح لأي أطراف ثالثة أخرى (موردو خدمات هوية (IdSP)) في الاتحاد.

## 7 المعماريات والتدفقات لطرائق تجميع النعوت

يفترض العمل المبكر بشأن دمج النعوت المجمعة من سلطات متعددة لتوفير النعوت أن للهوية معرف هوية فريد على المستوى العالمي يكون مشتركاً بين جميع سلطات النعوت. وفي الواقع، لا تملك الكيانات معرفات هوية عالمية بل معرفات هوية مختلفة للكيانات ونعوتاً يخصصها لها موردو خدمات الهوية المختلفين.

وتحالف Liberty [b-Liberty] الذي خلفته المبادرة Kantara [b-Kantara]، كان المجموعة الأولى التي تصدت لمشكلة تجميع النعوت، من خلال مفهومه المتمثل في اتحاد الهوية [b-Chadwick]. ومع ذلك، هناك مشكلة لم تُحل تتمثل في الافتقار إلى نهج قياسي لتجميع نعوت الكيانات المؤكدة من سلطات متعددة، كي يستعملها مورد الخدمة في صنع قرارات التحكم في النفاذ.

وهناك حالتا استعمال قد تكونا مفيدتين في النظر في أسباب الحاجة إلى تجميع النعوت:

- إذا كان هناك متجر للكتب الإلكترونية يخطط لعمل تخفيض للكبار، فإنه يتعين عليه الحصول على مجموعة مجمعة من النعوت (تفاصيل بطاقة الائتمان وإثبات المقام الرفيع) من موردي خدمات هوية متعددين. وفي هذا المثال، يتعين على أي كيان تقديم النعوت من هويتين.
- وبافتراض أن هناك باحثاً يود شراء حاسوب باستخدام حساب مصرفي اتحادي من متجر إلكتروني يقدم تخفيضات للقطاع التعليمي، فإنه يجب على الباحث تقديم إثبات بأنه عضو في منظمة تعليمية وأن لديه حساباً محدداً في المصرف الخاص به. والنعوت المخزنة في هويات مختلفة متعددة يتعين تجميعها على أن يرسل ناتج هذا الاتحاد إلى أحدٍ من موردي الخدمات، في عملية يطلق عليها تجميع النعوت [b-Klingenstein].

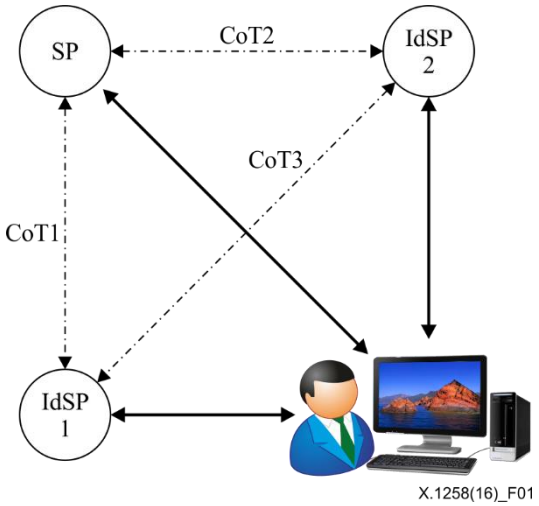
تبادل الموارد وتنسيق استعمالها ضمن مجتمعات دينامية متعددة المؤسسات أمر ضروري من أجل مدى متزايد من تطبيقات الحاسوب التي تتراوح من هيئات التعاون العلمية إلى الرعاية الصحية. وهذا التبادل يتعين بالضرورة التحكم فيه بشدة. ويتعين على موفري الموارد والمستهلكين أن يحددوا بوضوح وبعناية ما الذي يتعين تبادله بدقة ومن هم المسموح لهم بالتبادل وما هي الشروط التي يتم طبقاً لها هذا التبادل. ويتحدد من خلال قواعد التبادل هذه مجموعة من الأفراد أو المؤسسات من ما يعرف بهيئة التعاون الافتراضية (VC). وتوفير الإدارة الذاتية الهيئات VC لكي يتسنى لها استحداث الأعضاء وإدارتهم بسهولة والأدوار المتعلقة بمجموعاتهم الخاصة وضوابط النفاذ لمواردهم الخاصة، أمر صعب، خاصةً عندما تتم استضافة هذه الموارد المتبادلة في مؤسسات متعددة. وفي سيناريو الهيئة VC، لا يتسنى لمورد خدمة الهوية الاتحادية (IdSP) دائماً تقديم جميع النعوت ذات الصلة بموردي الخدمات المشاركين (SP) في الهيئة VC. وهذه النعوت المتعلقة بالهيئة VC، هي واسم الهيئة VC وحالة العضوية والقائمة البريدية للأعضاء وما إلى ذلك، يتعين تجميعها من مصادر أخرى. ويتعين مشاركة العديد من سلطات النعوت المختلفة في إدارة نعوت المستعملين [b-Hulsebosch].

وهناك العديد من طرائق اتحادات الهوية: لغة وسم التأكيد الأمني (SAML) وShibboleth [b-Shibboleth]، واتحاد خدمات الويب، [b-WS-Federation]، ومبادرة Kantara [b-Kantara]، والهوية المفتوحة [b-OpenID]، والاستيقان المفتوح [b-OAuth]، وCardSpace [b-CardSpace]، ومشروع Higgins [b Higgins]، وغيرها. واستناداً إلى الجهة القائمة بإدارة العملية بأكملها، يمكن تصنيف طرائق تجميع النعوت إلى ثلاث فئات: طرائق الإدارة من قبل مورد خدمة الهوية وطرائق الإدارة من قبل مورد الخدمة وطرائق الإدارة من قبل الكيان.

## 1.7 الطرائق المدارة من قبل مورد خدمة الهوية

### 1.1.7 ربط الهويات

هناك طريقة طرحها إطار التحالف Liberty، تعد من أولى الطرائق لمعالجة مشكلة تجميع النعوت من خلال مفهوم التحالف الخاص باتحاد الهوية، انظر الشكل 1 [b-Liberty]. ففي الشكل 1، يسمح موردو خدمات الهوية للكيان باستحداث رابط مزدوج (دائرة الثقة 3 (CoT3)) بين اثنين من موردي خدمات الهوية. وعندما يتحرك كيان ما حول الخدمات، فإن مورد خدمة الهوية الأول (IdSP1 في الشكل 1) يسأل الكيان ما إذا كان يود عمل اتحاد بين مورد خدمة الهوية هذا (IdSP1) ومورد خدمة الهوية الآخر (IdSP2). وعند هذه النقطة، سيتعامل موردا خدمة الهوية مع بعضهما لاستحداث مؤشر رابط. وأثناء النفاذ إلى الخدمات من مورد خدمة، يقدم أحد موردي خدمة الهوية مؤشر الرابط هذا إلى مورد الخدمة إلى جانب التأكيد الذي يضم النعوت. ويمكن لمورد الخدمة استخدام مؤشر الرابط لاستخلاص تأكيد آخر يضم نعوتاً من مورد خدمة الهوية الثاني. وبتجميع النعوت المستخلصة من موردي خدمة الهوية الاثنين، يمكن لمورد الخدمة تحديد ما إذا كان باستطاعة الكيان النفاذ إلى خدمة ما.




**الشكل 1 – معمارية طريقة ربط الهويات**

ويبين الشكل 2 تدفق تحكم مفاهيمياً لعملية تجميع النعوت باستخدام طريقة ربط الهويات.

(1) يرسل كيان ما طلب خدمة لأحد موردي الخدمات.

(2) عندما يحتاج مورد الخدمة تصريح الخدمة الخاص بالكيان، يرسل طلباً للاستيقان وتأكيد الاستيقان.

(3) يعاد توجيه الكيان إلى مورد خدمة الهوية رقم 1 للاستيقان.

(4) يستقين مورد خدمة الهوية رقم 1 الكيان ويطلب المزيد من النعوت.

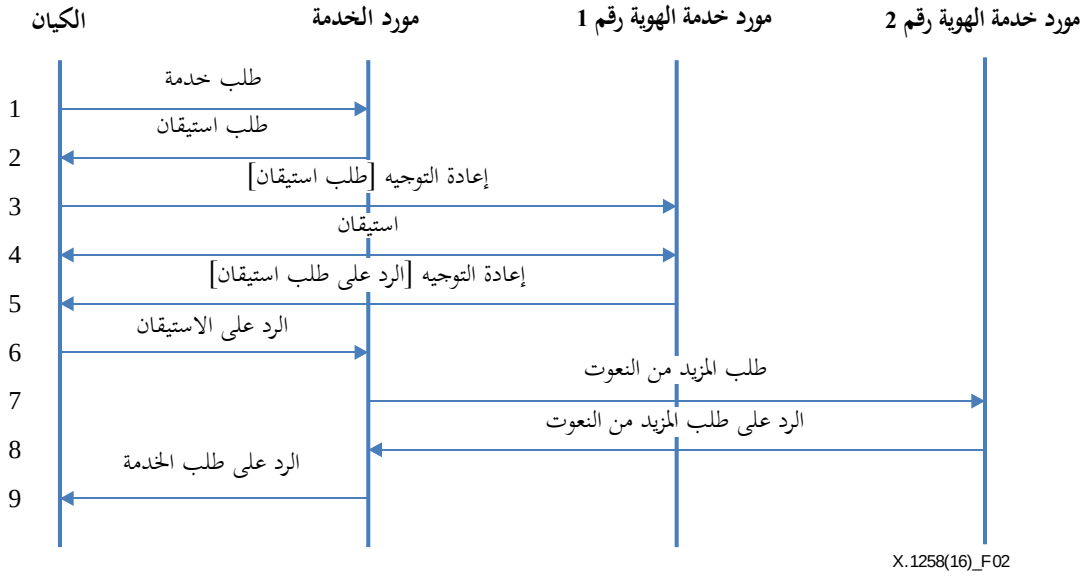
(5) يعيد مورد خدمة الهوية رقم 1 تأكيد الاستيقان.

(6) يقدم الكيان تأكيد استيقان إلى مورد الخدمة.

(7) يطلب مورد الخدمة المزيد من النعوت بخصوص الكيان من مورد خدمة الهوية رقم 2.

(8) يقدم مورد خدمة الهوية رقم 2 نعوتاً إضافية.

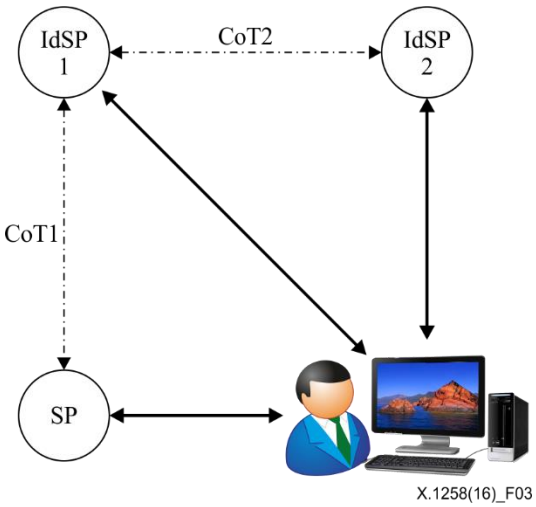
(9) يتحقق مورد الخدمة من التأكيدات ويسمح للكيان بالنفاذ إلى الخدمة.




**الشكل 2 – تدفق تجميع النعوت باستخدام طريقة ربط النعوت**

### 2.1.7 التوكيل بتفويض الهويات

هناك مورد خدمة هوية وكيل ويوجد توصيل بين مورد الخدمة ومورد خدمة الهوية الوكيل هذا يثق فيه تماماً؛ وموردو خدمات الهوية الآخرون غير معروفين لمورد الخدمة وتوجد لديهم علاقات ثقة مع مورد خدمة الهوية الوكيل (IdSP1) فقط، انظر الشكل 3 [b-Klingenstein]. فإذا ما رغب الكيان في تجميع النعوت من موردي خدمات هوية متعددين، يعاد توجيه الكيان بداية لمورد خدمة الهوية الوكيل (IdSP1 في الشكل 3)، ويقوم مورد خدمة الهوية الوكيل بعد ذلك بإعادة توجيه الكيان إلى موردي خدمات الهوية المتعددين الآخرين. وبعد أن تم استيقان الكيان بشكل منفرد عند كل مورد خدمة هوية، يعيد الكيان تأكيداً إلى مورد خدمة الهوية الوكيل. وبعد ذلك، يتحقق مورد خدمة الهوية الوكيل من كل تأكيد ويستخلص النعوت من موردي خدمات الهوية ثم يقوم بتجميع هذه النعوت كافة. ويمكن لمورد خدمة الهوية الوكيل ملء المجموعة المتجمعة من نعوت كياناته الخاصة به ويعيد تأكيد التأكيدات. ويقوم مورد خدمة الهوية الوكيل بعد ذلك بإرسال جميع تأكيدات النعوت المعاد تأكيدها إلى مورد الخدمة. ويحدد مورد الخدمة بعد ذلك ما إذا كان بإمكان الكيان النفاذ إلى الخدمة استناداً إلى النعوت المجمعة. وحيث إن مورد الخدمة لا يتسلم بموردي خدمات الهوية الآخرين ولكن لديه علاقة فقط مع مورد خدمة الهوية الوكيل، فإنه يفترض أن جميع النعوت قد صدرت عن مورد خدمة الهوية الوكيل.




**الشكل 3 – معمارية التوكيل بتفويض الهويات**

ويبين الشكل 4 تدفق تحكم مفاهيمياً لتجميع الهويات باستخدام طريقة التوكيل بتفويض الهويات.

(1) يرسل الكيان طلب خدمة إلى مورد الخدمة.

(2) عندما يحتاج مورد الخدمة تصريح الخدمة الخاص بالكيان، يرسل طلباً للاستيقان وتأكيد الاستيقان.

(3) يعاد توجيه الكيان إلى مورد خدمة الهوية رقم 1 (كوكيل) للاستيقان.

(4) يقوم مورد خدمة الهوية رقم 1 بإعادة توجيه الكيان إلى مورد خدمة الهوية رقم 2.

(5) يستلم مورد خدمة الهوية رقم 2 طلب استيقان ونعوت.

(6) يستيقن مورد خدمة الهوية رقم 2 الكيان.

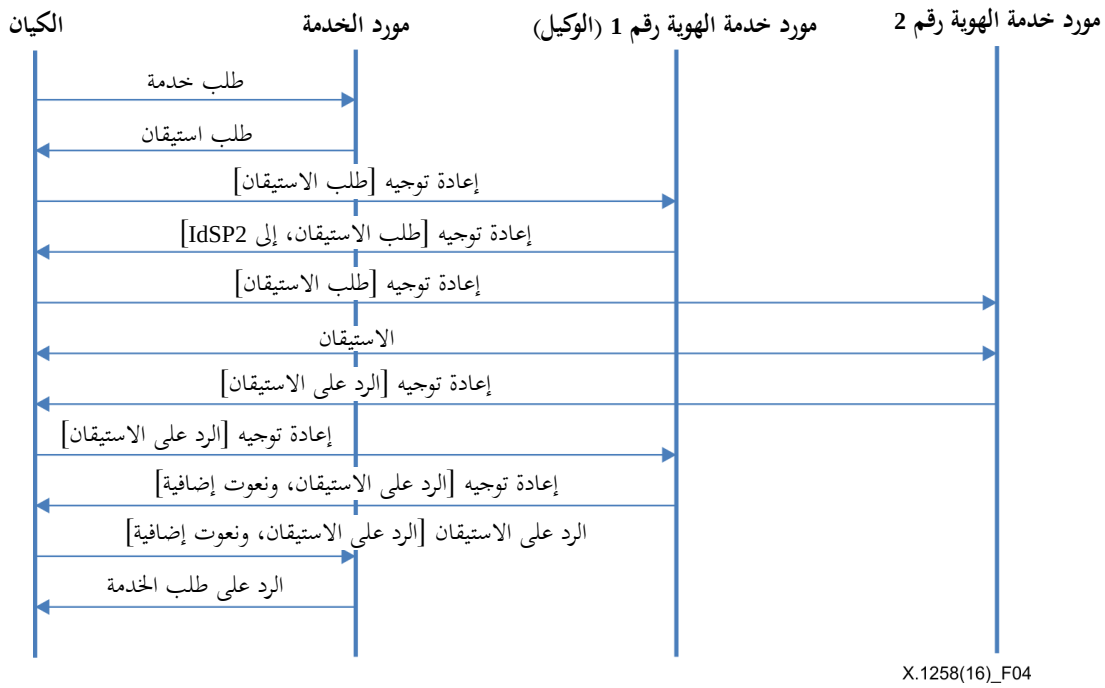
(7) يعيد مورد خدمة الهوية رقم 2 نتائج الاستيقان وتأكيدات النعوت.

(8) يحيل الكيان نتائج الاستيقان وتأكيدات النعوت إلى مورد خدمة الهوية رقم 1.

(9) يضيف مورد خدمة الهوية رقم 1 نعوتاً إضافية ويوقع التأكيدات ويعيدها إلى الكيان.

(10) يقدم الكيان التأكيدات إلى مورد الخدمة.

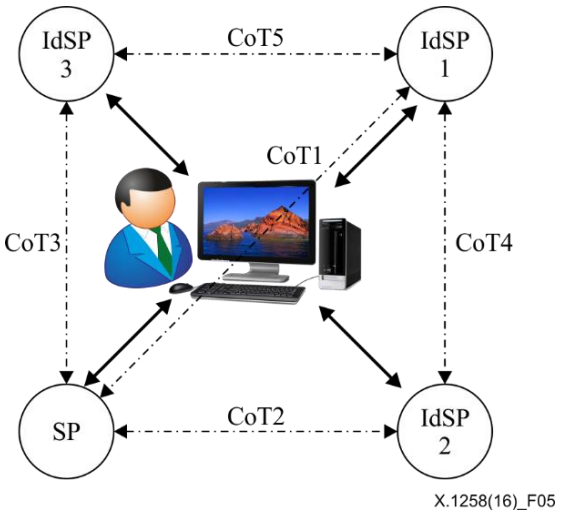
(11) يتحقق مورد الخدمة من التأكيدات ويسمح للكيان بالنفاذ إلى الخدمة.




**الشكل 4 – تدفق تجميع النعوت باستخدام طريقة التوكيل بتفويض الهويات**

### 3.1.7 ترحيل الهويات

طريقة ترحيل الهويات تشبه طريقة التوكيل بتفويض الهويات دون الحاجة إلى ثقة قوية بين مورد الخدمة ومورد خدمة الهوية الوكيل. ومع ذلك، تلزم طريقة التوكيل بتفويض الهوية مورد الخدمة بأن يثق ثقة تامة في مورد خدمة الهوية الموثوق فيه. وفي الواقع، قد يكون مستحيلاً وجود ثقة مطلقة بين مورد خدمة الهوية الوكيل ومورد الخدمة. وفي طريقة ترحيل الهويات، يمكن لمورد خدمة هوية وسيط (أو مورد خدمة هوية للترحيل؛ مورد خدمة الهوية رقم 1 في الشكل 5) أن يعمل كمورد خدمة هوية وكيل. ويتشابه التدفق بعد ذلك مع طريقة التوكيل بتفويض الهوية، حيث يعاد توجيه الكيان إلى مورد خدمة الهوية المرحل بدايةً وبعد ذلك يقوم مورد خدمة الهوية المرحل بإعادة توجيه الكيان إلى موردي خدمات الهوية المتعددين الآخرين. وبعد استيقان الكيان بشكل منفرد عند كل مورد من موردي خدمات الهوية، يعيد الكيان تأكيداً إلى مورد خدمة الهوية المرحل. وبعد ذلك يقوم مورد خدمة الهوية المرحل بتجميع جميع التأكيدات في تأكيد واحد وإحالته إلى مورد الخدمة. والفارق بين النموذجين يكمن في توقيع تأكيدات النعوت. ولا يوقع مورد خدمة الهوية المرحل تأكيدات النعوت، بل يقوم فقط بترحيل التأكيدات الموقعة من مورد خدمة الهوية الأصلي. وبعد ذلك، يستقبل مورد الخدمة تأكيدات النعوت المجمعة من موردي خدمات الهوية ومن مورد خدمة الهوية المرحل، ويقرر ما إذا كان باستطاعة الكيان النفاذ إلى الخدمة استناداً إلى النعوت المجمعة. وتحتاج هذه الطريقة إلى علاقة ثقة بين موردي خدمات الهوية ومورد الخدمة.




**الشكل 5 – معمارية طريقة ترحيل الهويات**

ويعرض الشكل 6 تدفق تحكم مفاهيمياً لتجميع النعوت باستخدام طريقة ترحيل الهويات.

(1) يرسل الكيان طلب خدمة إلى مورد الخدمة.

(2) عندما يحتاج مورد الخدمة تصريح الخدمة الخاص بالكيان، يرسل طلباً للاستيقان وتأكيد الاستيقان.

(3) يعاد توجيه الكيان إلى مورد خدمة الهوية رقم 1 (كمرحل) للاستيقان.

(4) يعيد مورد خدمة الهوية رقم 1 توجيه الكيان إلى مورد خدمة الهوية رقم 2.

(5) يستلم مورد خدمة الهوية رقم 2 طلب استيقان ونعوت.

(6) يستقين مورد خدمة الهوية رقم 2 الكيان.

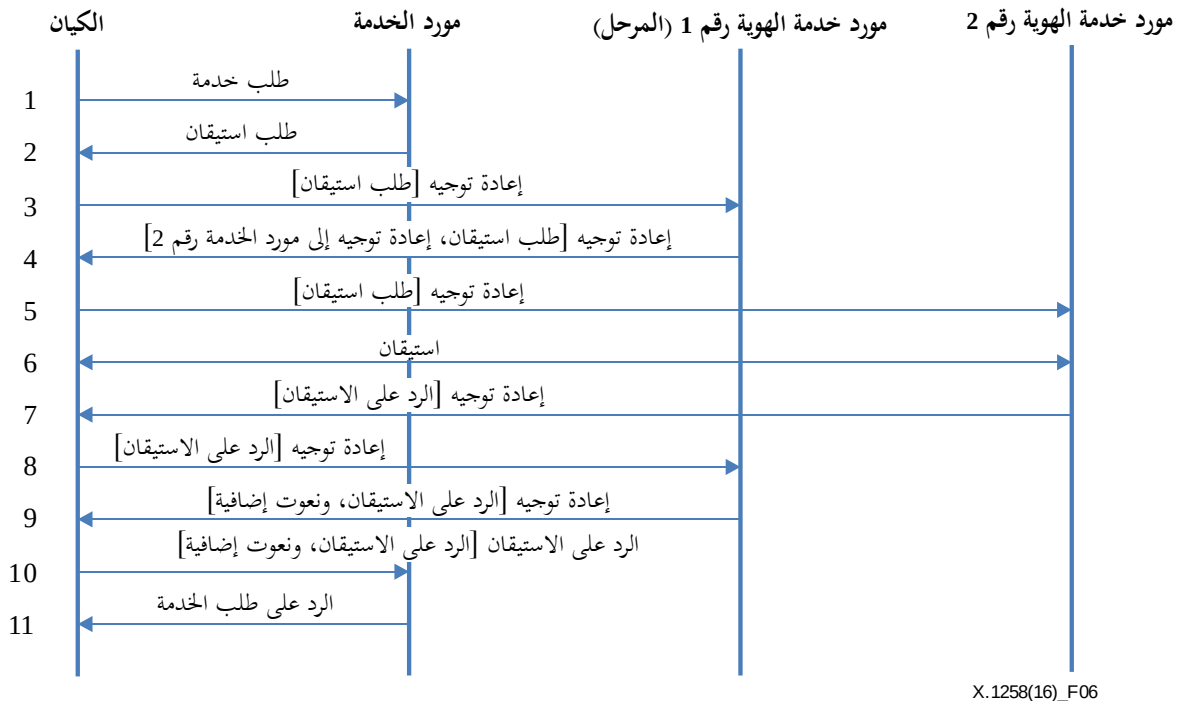
(7) يعيد مورد خدمة الهوية رقم 2 نتائج الاستيقان وتأكيدات النعوت.

(8) يحيل الكيان نتائج الاستيقان وتأكيدات النعوت إلى مورد خدمة الهوية رقم 1.

(9) يضيف مورد خدمة الهوية رقم 1 نعوتاً إضافية ويوقع التأكيدات ويعيدها إلى الكيان.

(10) يقدم الكيان التأكيدات إلى مورد الخدمة.

(11) يتحقق مورد الخدمة من التأكيدات ويسمح للكيان بالنفاذ إلى الخدمة.

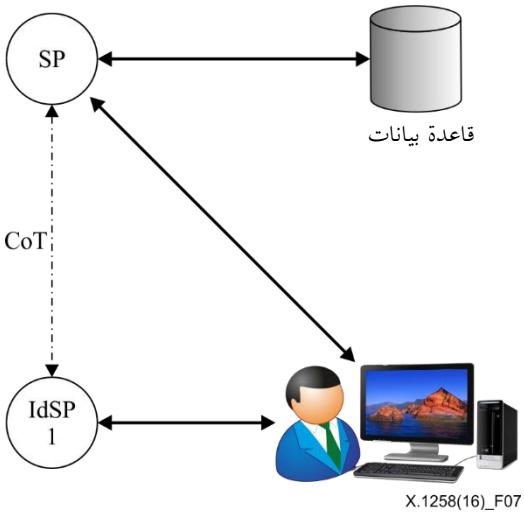



**الشكل 6 – تدفق تجميع النعوت باستخدام طريقة ترحيل الهويات**

## 2.7 مورد الخدمة (SP) – الطرائق الوسيطة

### 1.2.7 قاعدة بيانات التطبيق

تعد طريقة قاعدة بيانات التطبيق (DB) الطريقة أبسط طرائق تجميع النعوت، انظر الشكل 7 [b-Hulsebosch]. ويحتفظ مورد الخدمة بنعوت إضافية للكيانات وباللقب وتفضيلات الكيان بالنسبة لخدمة معينة وعضوية المجموعة وما إلى ذلك، إلى جانب النعوت التي يوفرها مورد خدمة الهوية. ويدير مورد الخدمة النعوت المضافة للتطبيقات. كما أن نعوت قاعدة بياناته هذه يمكن استخراجها فيما بعد لكي يحدد مورد الخدمة ما إذا كان بإمكان الكيان النفاذ إلى خدمة معينة.




**الشكل 7 – معمارية طريقة قاعدة بيانات التطبيق**

ويعرض الشكل 8 تدفق تحكم مفاهيمياً لتجميع النعوت باستخدام قاعدة بيانات التطبيق.

(1) يرسل الكيان طلب خدمة إلى مورد الخدمة.

(2) عندما يحتاج مورد الخدمة تصريح الخدمة الخاص بالكيان، يرسل طلباً للاستيقان وتأكيد الاستيقان.

(3) يعاد توجيه الكيان إلى مورد خدمة الهوية رقم 1 للاستيقان.

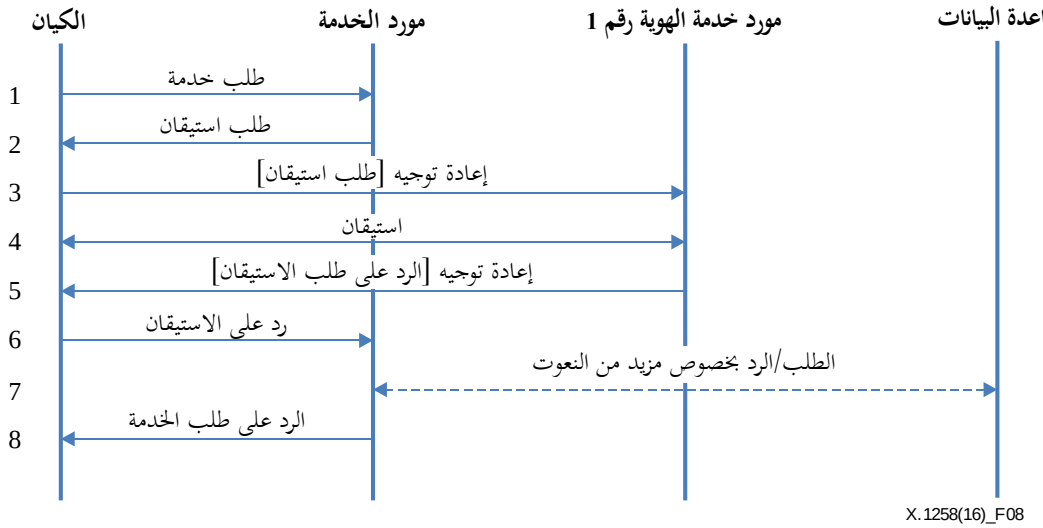
(4) مورد خدمة الهوية رقم 1 يستيقن الكيان.

(5) بعد نجاح الاستيقان، يعيد مورد خدمة الهوية رقم 1 نتائج الاستيقان والتأكيد.

(6) يقدم الكيان تأكيد الاستيقان إلى مورد الخدمة.

(7) يستخرج مورد الخدمة نعوت إضافية للكيان من قاعدة بياناته، إذا استدعى الأمر.

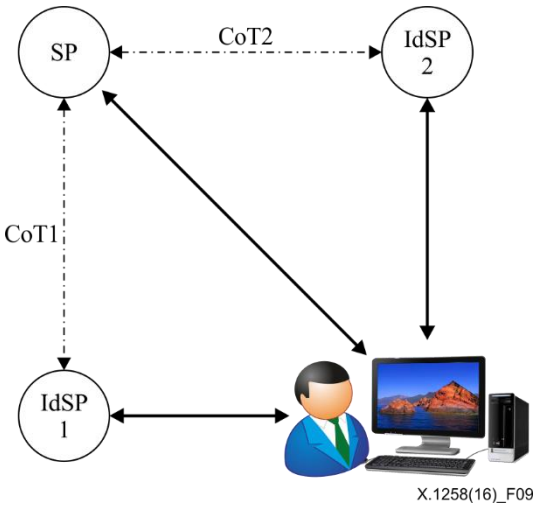
(8) يتحقق مورد الخدمة من التأكيد (التأكيدات) ويسمح للكيان بالنفاذ إلى الخدمة.




**الشكل 8 – تدفق تجميع النعوت باستخدام طريقة قاعدة بيانات التطبيق**

### 2.2.7 مورد الخدمة

تسمح طريقة مورد الخدمة للكيان بتجميع النعوت من موردي خدمات هوية متعددين في دورة واحدة، انظر الشكل 9 [b-Hulsebosch]. ويعاد توجيه الكيان إلى موردي خدمات هوية مختلفين الواحد تلو الآخر حيث يستيقن الكيان بشكل منفصل ويعيد تأكيداً للنعوت إلى مورد الخدمة. يقوم مورد الخدمة بتجميع تأكيدات النعوت من موردي خدمات الهوية ويحدد ما إذا كان بإمكان الكيان النفاذ إلى خدمة معينة.




**الشكل 9 – معمارية طريقة مورد الخدمة**

ويعرض الشكل 10 تدفق تحكم مفاهيمياً لتجميع النعوت باستخدام طريقة مورد الخدمة.

(1) يرسل الكيان طلب خدمة إلى مورد الخدمة.

(2) عندما يحتاج مورد الخدمة تصريح الخدمة الخاص بالكيان، يرسل طلباً للاستيقان وتأكيد الاستيقان.

(3) يعاد توجيه الكيان إلى مورد خدمة الهوية رقم 1 للاستيقان.

(4) يستيقن مورد خدمة الهوية رقم 1 للكيان.

(5) يعيد مورد خدمة الهوية رقم 1 نتائج الاستيقان والتأكيد.

(6) يقدم الكيان تأكيد الاستيقان إلى مورد الخدمة.

(7) يطلب مورد الخدمة من الكيان المزيد من النعوت الخاصة به.

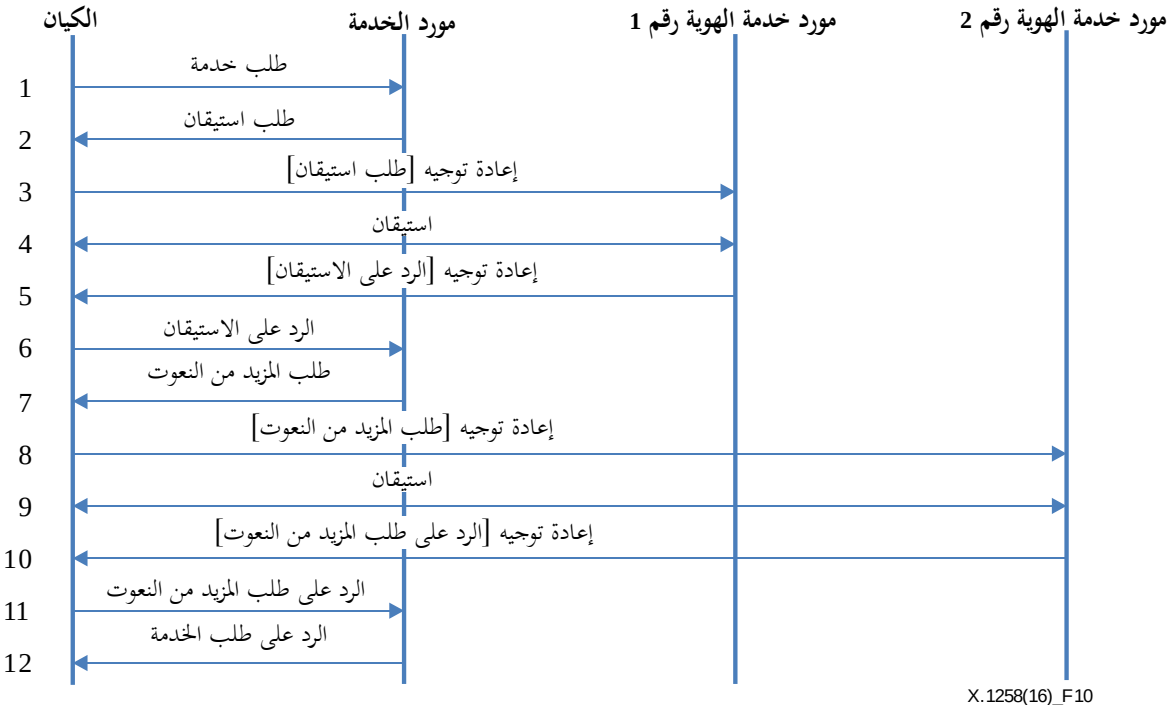
(8) يرسل الكيان طلبات بالمزيد من النعوت إلى مورد خدمة الهوية رقم 2.

(9) يستيقن مورد خدمة الهوية رقم 2 الكيان.

(10) يقدم مورد خدمة الهوية رقم 2 النعوت الإضافية.

(11) يقدم الكيان تأكيدات الاستيقان إلى مورد الخدمة.

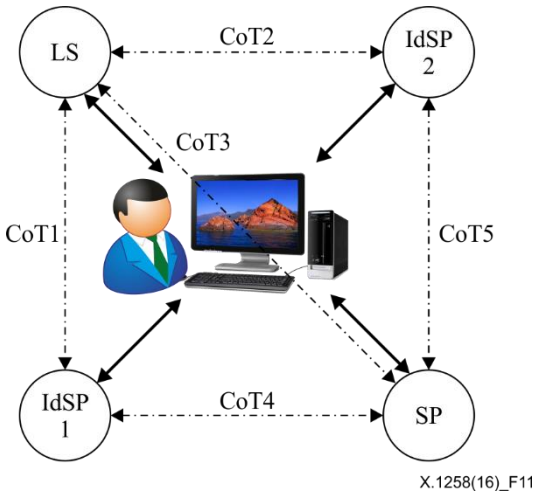
(12) يتحقق مورد الخدمة من التأكيد (التأكيدات) ويسمح للكيان بالنفاذ إلى الخدمة.




**الشكل 10 – تدفق تجميع النعوت باستخدام طريقة مورد الخدمة**

### 3.2.7 خدمة الربط

طريقة خدمة الربط (LS) عبارة عن توليفة لطريقتي الربط وترحيل الهويات، وهي نوع خاص من طريقة مورد الخدمة، انظر الشكل 11، حيث تستخدمها الكيانات التي تستعمل معرفات هوية موردة من خدمتي الربط [b-Chadwick] و[b-Hulsebosch]. ويستعمل معرف الهوية المورد من الخدمة LS لربط مختلف موردي خدمات الهوية الذين يستعملون معرفات هوية ثابتة محددة للخدمة LS وموردة من موردي خدمات الهوية ترد في جدول يطلق عليه جدول الربط. وعندما يرغب كيان ما في النفاذ إلى خدمة ما، يزور مورد الخدمة ويعاد توجيهه إلى مورد خدمة الهوية الأول (مورد خدمة الهوية رقم 1 في الشكل 11). ويستيقن الكيان عند مورد خدمة الهوية رقم 1، ثم يعاد تأكيد يضم نعوت الكيان ومعرف هوية للخدمة LS إلى مورد الخدمة عن طريق الكيان. ويحيل مورد الخدمة معرف الهوية إلى الخدمة LS للحصول على المزيد من النعوت. وعند هذه النقطة، يتاح خياران: إما يتسنى للخدمة LS استخراج قائمة بموردي خدمات الهوية المرتبطين بالنسبة لمعرف الهوية الثابت هذا باستخدام جدول الربط واستخراج نعوت من كل واحد منهم بحيث يتم تجميعها فيما بعد عند الخدمة LS وتعاد إلى مورد الخدمة، أو يتسنى للخدمة LS إرسال القائمة الخاصة بموردي خدمات الهوية المرتبطين ثانية إلى مورد الخدمة. ويقوم مورد الخدمة بعد ذلك باستخراج نعوت من كل واحد من موردي خدمات الهوية. وفي النهاية يحدد مورد الخدمة ما إذا كان بإمكان الكيان النفاذ إلى الخدمة على أساس النعوت المجمعة.




**الشكل 11 – معمارية طريقة خدمة الربط**

ويعرض الشكل 12 تدفق تحكم مفاهيمياً لتجميع النعوت باستخدام طريقة خدمة الربط.

(1) يرسل الكيان طلب خدمة إلى مورد الخدمة.

(2) عندما يحتاج مورد الخدمة تصريح الخدمة الخاص بالكيان، يرسل طلباً للاستيقان وتأكيد الاستيقان.

(3) يعاد توجيه الكيان إلى مورد خدمة الهوية رقم 1.

(4) يستيقن مورد خدمة الهوية رقم 1 الكيان.

(5) يعيد مورد خدمة الهوية رقم 1 تأكيد الاستيقان ومعرف هوية للخدمة LS.

(6) يقدم الكيان التأكيد ومعرف هوية الخدمة LS إلى مورد الخدمة.

(7) يرسل مورد الخدمة طلبات لمزيد من النعوت إلى الكيان.

(8) يعاد توجيه الكيان إلى خدمة الربط.

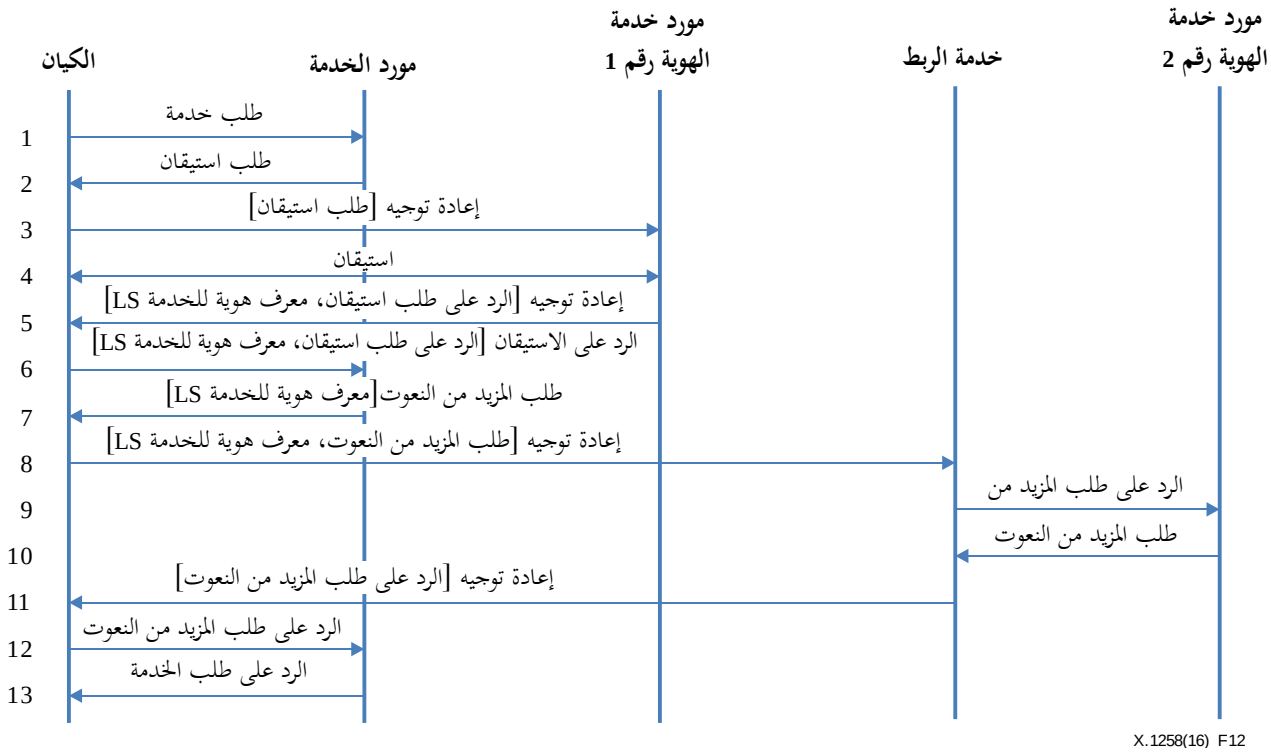
(9) تطلب خدمة الربط من مورد خدمة الهوية رقم 2 نعوتاً.

(10) يقدم مورد خدمة الهوية رقم 2 النعوت.

(11) تعاد النعوت إلى الكيان.

(12) يقدم الكيان تأكيد (تأكيدات) الاستيقان إلى مورد الخدمة.

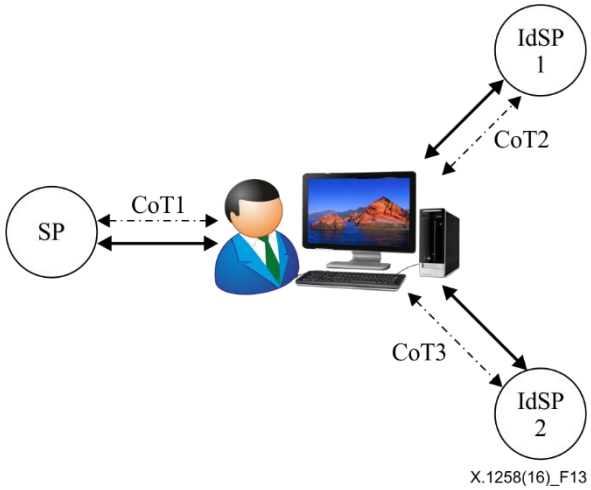
(13) يتحقق مورد الخدمة من التأكيد (التأكيدات) ويسمح للكيان بالنفاذ إلى الخدمة.




**الشكل 12 – تدفق تجميع النعوت باستخدام طريقة خدمة الربط**

### 3.7 طريقة الكيان الوسيط

تستخدم طريقة الكيان الوسيط عميلاً (وكيل الكيان أو التطبيق) يملك القدرة على تجميع النعوت من مختلف موردي خدمات الهوية، انظر الشكل 13 [b-Klingenstein]، و[b-Hulsebosch]. ويعلم مورد الخدمة العميل بقائمة موردي خدمات الهوية الموثوقين. ويعيد العميل توجيه الكيان إلى كل واحد من موردي خدمات الهوية هؤلاء. وبعد الاستيقان المنفصل لكل مورد خدمة هوية، يستقبل العميل التأكيدات من جميع موردي خدمات الهوية ويعرض المجموعة الموحدة من التأكيدات على مورد الخدمة. يتحقق مورد الخدمة من كل تأكيد ويستخرج جميع النعوت، ثم يحدد ما إذا كان بإمكان الكيان النفاذ إلى الخدمة.




**الشكل 13 – معمارية طريقة العميل**

ويعرض الشكل 14 تدفق تحكم مفاهيمياً لتجميع النعوت باستخدام طريقة العميل.

(1) يرسل الكيان طلب خدمة إلى مورد الخدمة.

(2) عندما يحتاج مورد الخدمة تصريح الخدمة الخاص بالكيان، يرسل طلباً للاستيقان وتأكيد الاستيقان.

(3) يستيقن مورد خدمة الهوية رقم 1 الكيان.

(4) يعيد مورد خدمة الهوية رقم 1 تأكيد الاستيقان.

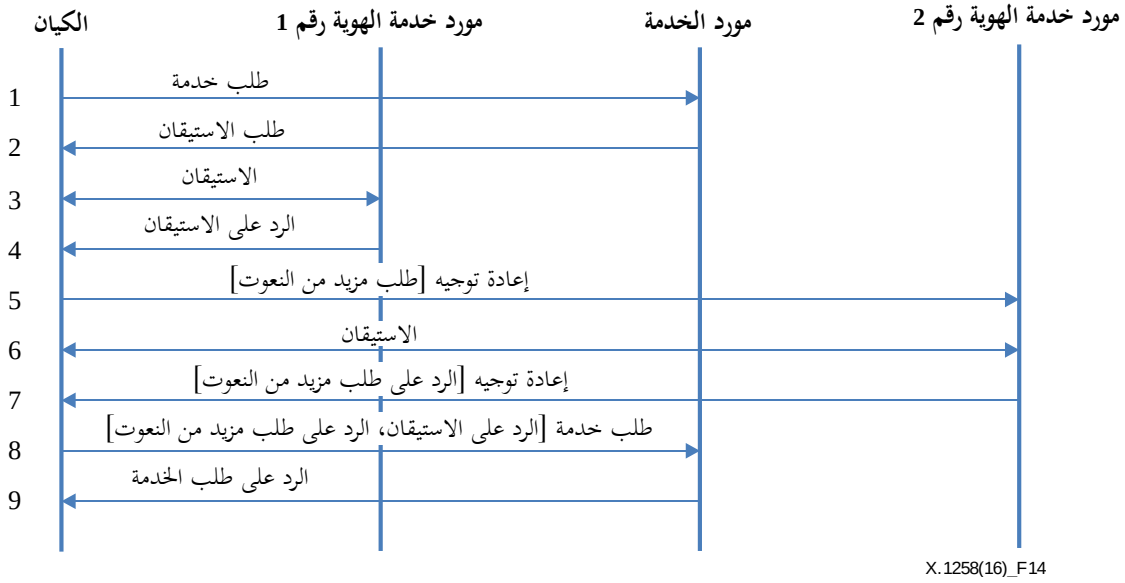
(5) يعاد توجيه الكيان إلى مورد خدمة الهوية رقم 2 من أجل التأكيد (التأكيدات) بشأن المزيد من النعوت.

(6) يستيقن مورد خدمة الهوية رقم 2 الكيان.

(7) يعيد مورد خدمة الهوية رقم 2 تأكيد (تأكيدات) النعوت.

(8) يقدم الكيان تأكيد (تأكيدات) الاستيقان إلى مورد الخدمة.

(9) يتحقق مورد الخدمة من التأكيد (التأكيدات) ويسمح للكيان بالنفاذ إلى الخدمة.




**الشكل 14 – تدفق تجميع النعوت باستخدام طريقة العميل**

## 8 مقارنة بين طرائق تجميع الاستيقانات

الطرائق السبع للفقرة 7 نهج جديدة من الأنظمة التقليدية لإدارة الهوية الاتحادية. ولكل طريقة منها كيانات وتفاعلات إضافية. واستناداً إلى هذه التعديلات، يمكن تحليل الطرائق السبع والمقارنة بينها عن طريق عوامل خاصة لاختيار طريقة التجميع الملائمة. وينبغي أن يراعي المصمم والمطور مسائل مثل: من الذي يقوم بدور الوسيط/من الذي يقوم بالتجميع/من الذي يقوم بالتحقق، بالنسبة للنعوت، أو مصاعب التنفيذ أو إضافة عناصر جديدة.

وتعرض الفقرة 7 العديد من الطرائق استناداً إلى اللغة SAML لتجميع النعوت. ويمكن تشغيل هذه الطرائق بينياً استناداً إلى الكيفية التي يعبر بها عنها بلغة SAML.

ويجري تحليل طرائق التجميع فيما يتعلق بالتوسيط في التجميع وإنفاذ التجميع وإضافة عناصر أخرى. وتعرض في الجدول 1 مقارنة بين طرائق التجميع.

وفي الجدول 1، تشير علامة الصح "✓" الواردة في خلية إلى أن طريقة التجميع المذكورة في الصف لديها القدرة الواردة في العمود. وبدقة أكبر، ينبغي للقدرة المشار إليها أن تدعم من خلال تنفيذ الطريقة المشار إليها.

**الجدول 1 – مقارنة بين طرائق التجميع**

| طريقة التجميع | القدرة | | | | | | |
|---|---|---|---|---|---|---|---|
| | وسيط لمورد خدمة الهوية | وسيط لمورد الخدمة | وسيط للعميل | تجميع مورد خدمات الهوية | تجميع مورد الخدمة | تجميع العميل | عناصر إضافية |
| ربط الهويات | ✓ | | | | ✓ | | |
| التوكيل بتفويض الهويات | ✓ | | | ✓ | | | |
| ترحيل الهويات | ✓ | | | ✓ | | | |
| قاعدة بيانات التطبيق | | ✓ | | | ✓ | | قاعدة بيانات |
| مورد الخدمة | | ✓ | | | ✓ | | |
| خدمة الربط | | ✓ | | | ✓ | | الخدمة LS |
| العميل | | | ✓ | | | ✓ | العميل |

وفيما يتعلق بطريقة ربط الهويات، يتم التوسيط في التجميع بواسطة مورد خدمة الهوية والإنفاذ عند مورد الخدمة. ويعني ذلك أن بروتوكول تجميع النعوت ينبغي تنفيذه عند كل من مورد خدمة الهوية ومورد الخدمة. بيد أن، في حالات أخرى، يمكن توسيط التجميع وإنفاذه عند نفس المورد. وقد يكون من الأسهل على المورد تشغيل طريقة تجميع النعوت أكثر من طريقة ربط الهويات. وفيما يتعلق بالعناصر الإضافية لتجميع النعوت، تحتاج طريقة قاعدة بيانات التطبيق إلى قاعدة بيانات خاصة بها؛ وخدمة الربط (LS) في هذه الخدمة كنوع خاص من تنفيذ مورد الخدمة؛ وتحتاج طريقةُ توسيط الكيان، العميل كوسيط. واستناداً إلى هذه المعايير، فإن طريقتَي التوكيل بتفويض الهويات وترحيل الهويات يوصى بهما في طرائق توسيط موردي خدمات الهوية، ويوصى بطريقة مورد الخدمة في طرائق توسيط موردي الخدمات.

# بيبليوغرافيا


[b-ITU-T X.500] Recommendation ITU-T X.500 (2016) | ISO/IEC 9594-1:2017, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8:2017, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2009), *A framework for user control of digital identity.*

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

[b-CardSpace] *Introducing windows cardspace*. MSDN technical articles, Microsoft Corporation.
Available (viewed 2016-12-19) at: http://msdn.microsoft.com/en-us/library/aa480189.aspx.

[b-Chadwick] Chadwick, D.W., Inman, G. (2009). Attribute aggregation in federated identity management. *IEEE Computer*, **42**(5), pp. 33–40.
<http://doi.ieeecomputersociety.org/10.1109/MC.2009.143>

[b-Higgins] Higgins, *Project.*
Available (viewed 2016-12-05) at: <http://www.eclipse.org/higgins/>

[b-Hulsebosch] Hulsebosch, B., Wegdam, M., Zoetekouw, B., van Dijk, N,, Poortinga-van Wijnen, R. (2012), Virtual collaboration attribute management. 41 pp. Available (viewed 2016-12-05) at:
<https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/EDS+11-06+Attribute+Management+v1.0.pdf >

[b-Kantara] Kantara, *Initiative*
Available (viewed 2016-12-19) at: https://kantarainitiative.org/reports-recommendations/

[b-Klingenstein] Klingenstein, N. (2007). Attribute aggregation and federated identity. In: *Proceedings of the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*, p. 26–29.

[b-Liberty] Liberty Alliance, *ID-FF 1.2 Specifications*, Available (viewed 2016-12-05) at:
<http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications

[b-OAuth] OAuth.
Available (viewed 2016-12-19) at: http://oauth.net/documentation/getting-started/

[b-OpenID] OpenID authentication 2.0.
Available (viewed 2016-12-19) at: http://openid.net/specs/openid-authentication-2_0.html

[b-Shibboleth] Shibboleth Consortium, *Open Source Project*.
Available (viewed 2016-12-05) at: <https://shibboleth.net/>

[b-WS-Federation] Web Services Federation Language (WS-Federation) Version 1.2.
Available (viewed 2016-12-19) at: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

## سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

| | |
|---|---|
| السلسلة A | تنظيم العمل في قطاع تقييس الاتصالات |
| السلسلة D | المبادئ العامة للتعريفة |
| السلسلة E | التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية |
| السلسلة F | خدمات الاتصالات غير الهاتفية |
| السلسلة G | أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية |
| السلسلة H | الأنظمة السمعية المرئية والأنظمة متعددة الوسائط |
| السلسلة I | الشبكة الرقمية متكاملة الخدمات |
| السلسلة J | الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط |
| السلسلة K | الحماية من التداخلات |
| السلسلة L | 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، 2017