الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1171

(2009/02)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة والأمن

تطبيقات وخدمات آمنة – أمن معرفات الهوية المتداولة شبكياً

التهديدات ومتطلبات حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في التطبيقات التي تستعمل تعرّف الهوية على أساس العلامة

التوصيـــة ITU-T X.1171

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة والأمن

الشبكات العمومية للبيانات	X.119–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	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

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

التوصيـــة ITU-T X.1171

التهديدات ومتطلبات حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في التطبيقات التي تستعمل تعرّف الهوية على أساس العلامة

ملخص

قد يتسبب اتساع انتشار علامات التعرّف بما فيها علامات التعرف على الترددات الراديوية (RFID) في شواغل تتعلق بتجاوز حدود الخصوصية وذلك بحكم قدرات تكنولوجيا RFID على جمع (ومعالجة) البيانات أوتوماتياً، واحتمال الكشف عن هذه البيانات لعامة الناس (عن قصد أو غير قصد).

وبالنسبة إلى التطبيقات التي تستعمل تعرّف الهوية على أساس العلامة وتعتمد على علامة هوية خاصة بالشخص في تطبيقات إدارة خدمة المبيعات الشخصية والتطبيقات المتصلة بالرعاية الصحية وما إلى ذلك، ما فتئت مسألة الخصوصية تتحول إلى مشكلة خطيرة. وتصف هذه التوصية عدداً من انتهاكات المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII) بالنسبة إلى التطبيقات التي تستعمل تعرّف الهوية على أساس العلامة، كما تصف متطلبات حماية هذه المعلومات. وعلاوة على ذلك، توفر هذه التوصية هيكلاً أساسياً لحماية المعلومات PII يعتمد على مواصفة سياسة المعلومات PII.

المصدر

وافقت لجنة الدراسات 17 (2009-2012) لقطاع تقييس الاتصالات على التوصية ITU-T X.1171 بتاريخ 20 فبراير 2009 بموجب إجراء القرار 1 للجمعية العالمية لتقييس الاتصالات.

تمهيـــد

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، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

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، 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 المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2009

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

المحتـــويات

الصفحة

1 مجال التطبيق..... 1
2 المراجع..... 1
3 تعاريف..... 2
1.3 المصطلحات المعرَّفة في أماكن أخرى: 2
2.3 مصطلحات معرَّفة في هذه التوصية..... 3
4 مختصرات 3
5 اصطلاحات..... 4
6 لمحة عامة 4
7 تطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة 4
8 نموذج مرجعي لتطبيقات B2C باستعمال تعرف الهوية على أساس العلامة 5
9 انتهاك معلومات PII في التطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة 6
1.9 تسرب المعلومات المتصلة بمعرف الهوية 6
2.9 تسرب بيانات السياق التاريخي 7
3.9 العلاقة بين انتهاك المعلومات PII والنموذج المرجعي..... 7
10 متطلبات حماية المعلومات PII لتطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة 8
1.10 مراقبة المعلومات PII من جانب مستعمل علامة تعرف الهوية 8
2.10 الاستيقان من مستعمل علامة تعرف الهوية و/أو مستعمل مطراف تعرف الهوية..... 8
3.10 مراقبة النفاذ إلى معلومات PII الخاصة بمستعمل علامة تعرف الهوية في مخدم التطبيق 9
4.10 سرية البيانات المتعلقة بالمعلومات المرتبطة بعلامة تعرف الهوية 9
5.10 الموافقة على تجميع البيانات التي يحتوي عليها السياق التاريخي لمستعمل مطراف تعرف الهوية..... 9
6.10 العلاقة بين المتطلبات وانتهاكات معلومات PII 9
7.10 العلاقة بين المتطلبات وانتهاكات معلومات PII 9
الملحق A – المبادئ الأساسية للتطبيق الوطني..... 10
الملحق B – المبادئ الأساسية للتطبيق الدولي: التدفق الحر والقيود التشريعية..... 11
التذييل I – تتبع معرف الهوية للموقع في خدمات تعرف الهوية بواسطة التردد الراديوي (RFID) 12
التذييل II – خدمة حماية المعلومات PII (PPS) في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة 13
1.II خدمة حماية المعلومات PII (PPS) في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة... 13
2.II كيانات الخدمة المتعلقة بالخدمة PPS في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة. 13
3.II السيناريو العام للخدمة فيما يتعلق بالخدمة PPS 14
4.II وظائف الخدمة PPS 15
بيبليوغرافيا 18

التوصيـــة ITU-T X.1171[1]

التهديدات ومتطلبات حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في التطبيقات التي تستعمل تعرّف الهوية على أساس العلامة

1 مجال التطبيق

يشمل مجال تطبيق هذه التوصية الأهداف التالية بما في ذلك التهديدات ومتطلبات حماية المعلومات التي يمكن تعرف هوية أصحابها شخصياً (PII) في التطبيقات التي تستعمل تعرّف الهوية على أساس العلامة كما هو موصوف أدناه:

- تهديدات المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في بيئة تقوم على العلاقة بين شركة وعميل (B2C) في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة؛
- متطلبات حماية المعلومات التي يمكن تعرف هوية أصحابها شخصياً في بيئة تقوم على العلاقة بين شركة وعميل في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة؛

ولا يشمل مجال تطبيق هذه التوصية الأهداف التالية:

- تحليل تهديدات الأمن العام ومتطلبات التطبيقات التي تستعمل تعرف الهوية على أساس العلامة؛
- تحليل تهديدات ومتطلبات المعلومات التي يمكن تعرف هوية أصحابها شخصياً بين علامة تعرف الهوية (ID) ومطراف تعرف الهوية؛
- تحليل تهديدات ومتطلبات المعلومات التي يمكن تعرف هوية أصحابها شخصياً اعتماداً على علامة تعرف الهوية الخاصة وطريقة القراءة، مثلاً علامة التعرف بواسطة التردد الراديوي (RFID) ومطراف تعرف الهوية؛
- تحديد ووضع أنساق الرسالة وآليات لحماية المعلومات PII تعتمد على مواصفة سياسة المعلومات PII للمستعمل في تطبيق يستعمل تعرف الهوية على أساس العلامة.

الملاحظة 1 – هناك حاجة إلى مزيد من الدراسة لتعريف هذه الأنساق التي قد لا تقتصر على حماية المعلومات PII المتعلقة باستعمال تعرف الهوية على أساس العلامة فحسب، ولكن ربما على طريقة أكثر شمولاً (خصوصية).

يتمتع مستعمل علامة تعرف الهوية في هذه التوصية بالقدرة على التحكم في العلامة ID ذاتها وبالتالي من المفترض أن يكون مستعمل علامة تعرف الهوية مسؤولاً عن سلوك العلامة ID.

الملاحظة 2 – يكون مستعمل علامة تعرف الهوية في بعض الحالات غير قادر إطلاقاً على التحكم في علامة تعرف الهوية. وعندما يشتري شخص منتجاً موسوماً، يطلب منه المصنع علامة تعرف الهوية لكي يبقى نشيطاً لأغراض الضمان مثلاً. ويمكن أن يكون مستعمل العلامة ID في هذا السيناريو مجرد شخص يحمل منتجاً موسوماً ويستعمله. وبالتالي، لا يمكن تطبيق هذه التوصية لتسوية المشكلة المتعلقة بهذه الحالة. ويقتضي هذا السيناريو إصدار بعض التشريعات وتناول قضايا السياسة العامة [انظر المعايير b-OECD] ويمكن معالجة هذا الموضوع باستعمال توصية أخرى.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications.*

[1] قد لا تكون هذه التوصية مطبقة في ألمانيا نتيجة للتشريعات الألمانية.

3 تعاريف

1.3 المصطلحات المعرَّفة في أماكن أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في أماكن أخرى:

1.1.3 مراقبة النفاذ [b-ITU-T X.800]: منع الاستعمال غير المرخص لمورد ما، بما في ذلك منع استعمال مورد ما بطريقة غير مرخصة.

2.1.3 مخدم التطبيق [ITU-T X.1121]: كيان موصل بشبكة مفتوحة لإرسال البيانات باستعمال مطاريف متنقلة.

3.1.3 مورد خدمة التطبيق (ASP) [ITU-T X.1121]: كيان (شخص أو مجموعة أشخاص) يقدم خدمة (خدمات) التطبيق لمستعملين متنقلين من خلال مخدم التطبيق.

4.1.3 الاستيقان [b-ITU-T X.811]: التأكد من الهوية التي يدّعيها الكيان.

ملاحظة – استعمل تعبير "هوية" على أن يُفهم في سياق الاتصالات على أنه معرف أو مجموعة معرفات موثوقة، أي يعتبر أنه يمكن التعويل عليه لأغراض حالة خاصة لتمثيل عنصر شبكة أو جهاز مطرافي للشبكة أو مستعمل بعد استكمال عملية التحقق. ولا يمكن أن يستخلص من هذا التعبير على النحو المستخدم هنا، أن المعرفات الموثوق منها تعني أنه تم التحقق من هوية شخص ما على نحو إيجابي.

5.1.3 معرف الهوية [b-ITU-T F.771]: مجموعة من الأرقام والسمات والرموز أو أي شكل من أشكال البيانات المستعملة لتعرف هوية كيان العالم الحقيقي. ويستعمل لتمثيل العلاقة القائمة بين كيان العالم الحقيقي ومعلوماته/صفاته في الحواسيب. وتمكّن هذه العلاقة المستعملين من النفاذ إلى معلومات/صفات الكيان المخزنة في الحواسيب عبر مطاريف تعرف هوية المستعمل.

6.1.3 علامة تعرف الهوية [b-ITU-T F.771]: شيء مادي صغير جداً يخزن كمية صغيرة من المعلومات، ويعتبر معرف الهوية أو يتضمن معرف الهوية مع بيانات تطبيق إضافية كالاسم واللقب والسعر والعنوان.

7.1.3 مطراف تعرف الهوية [b-ITU-T F.771]: جهاز يتمتع بالقدرة على التقاط البيانات من علامات تعرف الهوية، وبقدرات أخرى كالقدرة على الاتصال والقدرة على عرض تقديم المعلومات متعددة الوسائط. وقد تشمل القدرة على التقاط البيانات وظيفة تسمح بالحصول على معرف الهوية من علامات ID حتى في حالة عدم وجود قدرة الاتصال كشفرة القضبان وشفرة القضبان ثنائية الأبعاد (2D). ومن أمثلة تقنيات التقاط البيانات، آلة التصوير الرقمية وجهاز المسح البصري والمرسل المستجيب RF وIrDA والخطوط السلكية الغلفانية وما إلى ذلك.

8.1.3 شبكة متنقلة [ITU-T X.1121]: شبكة توفر نقاط نفاذ الشبكة اللاسلكية إلى المطاريف المتنقلة.

9.1.3 مطراف متنقل [ITU-T X.1121]: كيان يقوم بوظيفة النفاذ إلى شبكة لاسلكية ويوصل شبكة متنقلة لإرسال البيانات بمخدمات التطبيق أو مطاريف متنقلة أخرى.

10.1.3 مستعمل متنقل [ITU-T X.1121]: كيان (شخص) يستعمل المطراف المتنقل ويُشَغِله لاستقبال خدمات مختلفة من موردي خدمات التطبيق.

11.1.3 المعلومات التي يمكن التعرف على هوية أصحابها شخصياً (PII) [b-ITU-T Y.2720]: معلومات تخص أي شخص من الأحياء تجعل بالإمكان التعرف عليه (بما في ذلك المعلومات التي بمقدورها تعريف شخص عند دمجها مع معلومات أخرى حتى وإن كانت هذه المعلومات لا تعرف الشخص صراحة).

2.3 مصطلحات معرَّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 تطبيقات تستخدم تعرف الهوية على أساس العلامة: تطبيقات تشمل العناصر التالية على الأقل: معرف الهوية ومطراف تعرف الهوية وعلامة ID وشبكة (شبكات). ويخزَّن معرف الهوية، في هذا التطبيق، في علامة ID وتوفر جميع المعلومات المرتبطة بمعرف الهوية على جانب الشبكة.

ملاحظة – يخزن معرف الهوية في علامة ID (أو في علامة ID حسب نوع العلامة ID) ويقرأ مطراف ID معرف الهوية من/إلى علامة ID عبر جهاز المسح البصري (للقراءة فقط)، وآلة التصوير (للقراءة فقط)، وIrDA (قراءة/كتابة)، وتقنية RF (قراءة/كتابة) أو غيرها من الطرائق الشبيهة.

2.2.3 علاقة الشركة بالعميل (B2C): علاقة تجارية بين الشركات والمستهلكين حيث يوفر موردو الخدمات خدمات قيمة ومفيدة للمستهلك الذي يستعملها.

3.2.3 مواصفة سياسة المعلومات PII بالتغيب: مجموعة منسقة من قواعد حماية المعلومات PII وسياساتها في تطبيق يستعمل تعرف الهوية على أساس العلامة.

4.2.3 تعرف الهوية (ID): إجراء تعريف هوية شيء بالتحديد من بين أصناف واسعة من الأشياء من خلال قراءة معرفات هوية علامات ID.

5.2.3 مستعمل علامة ID: شخص يشتري شيئاً موسوماً بعلامة ID ويحمله أو يستعمله.

6.2.3 مستعمل مطراف تعرف الهوية ID: شخص يستعمل مطرافاً لتعرف الهوية ويُشَغله. ويمكن أن يكون مستعمل متنقل بمطراف تعرف الهوية مثالاً نموذجياً لمستعمل مطراف تعرف الهوية.

7.2.3 علامة تعرف هوية شخصية: علامة تعرف هوية تتضمن معرف هوية يتيح إمكانية تعرف هوية شخص بدلاً من شيء مجهول المصدر.

8.2.3 خدمة حماية المعلومات PII (PPS): خدمة الأمن التي توفر حماية المعلومات PII المتعلقة بمستعمل علامة ID و/أو مستعمل مطراف ID في تطبيق يستعمل تعرف الهوية على أساس العلامة. وتدير الخدمة PPS (أي تنشئ/تحدّث/تحذف/تطبق) (علامة ID و/أو مطراف ID) مواصفة سياسة المعلومات PII للمستعمل على الشبكة التي يجري فيها تشغيل تطبيق يستعمل تعرف الهوية على أساس العلامة.

9.2.3 مواصفة سياسة المعلومات PII: مجموعة منسقة من قواعد حماية المعلومات PII وسياساتها.

10.2.3 مواصفة سياسة المعلومات PII المحددة للمستعمل: مجموعة منسقة من قواعد حماية المعلومات PII وسياساتها كما يحددها المستعمل (علامة ID و/أو مطراف ID).

4 مختصرات

تستعمل هذه التوصية المختصرات والرموز المختصرة التالية:

ASP مورد خدمة التطبيقات (*Application Service Provider*)

B2C العلاقة بين الشركة والعميل (*Business-to-Customer*)

ID تعرف الهوية (*Identification*)

IrDA ربط البيانات بالأشعة تحت الحمراء (*Infrared Data Association*)

OECD منظمة التعاون والتنمية في الميدان الاقتصادي (*Organization for Economic Cooperation and Development*)

PII معلومات يمكن تحديدها شخصياً (*Personally Identifiable Information*)

PPS خدمة حماية المعلومات PII (*PII Protection Service*)

RF تردد راديوي (*Radio Frequency*)

RFID التعرف بواسطة التردد الراديوي (*Radio Frequency Identification*)

SCM إدارة سلسلة التزويد (*Supply Chain Management*)

5 اصطلاحات

لا توجد.

6 لمحة عامة

قد يتسبب اتساع انتشار علامات التعرّف (بما فيها علامات RFID) في شواغل تتعلق بتجاوز حدود الخصوصية وذلك بحكم قدرات تكنولوجيا RFID على جمع (ومعالجة) البيانات أوتوماتياً، واحتمال الكشف عن هذه البيانات لعامة الناس (عن عمد أو مصادفة).

وبالنسبة إلى التطبيقات التي تستعمل تعرّف الهوية على أساس العلامة وتعتمد على علامة تعرف الهوية الشخصية في خدمات الإدارة بعد البيع الشخصية والخدمات المتصلة بالرعاية الصحية وما إلى ذلك، ما فتئت مسألة الخصوصية تتحول إلى مشكلة خطيرة.

وفي الأوساط الأكاديمية والصناعية، تركز معظم الجهود المبذولة إزاء آلية حماية المعلومات PII على بروتوكولات الاستيقان بين علامة تعرف الهوية ومطراف تعرف الهوية. ومع ذلك يلاحظ أن هذه الجهود لا يمكن تطبيقها على البيئة الحالية خاصة على التطبيقات التي تستعمل تعرف الهوية على أساس العلامة، والبيئة التي توجد فيها معلومات مفيدة عن معرف الهوية على المخدم في ميدان الشبكة. ولذا، فإن استعمال آلية حماية المعلومات PII الملائمة في بيئة التطبيقات التي تستعمل تعرف الهوية على أساس العلامة يعتبر ضرورياً. ويمكن أن تكون آلية حماية المعلومات PII على أساس المواصفة أحد الحلول الممكنة لمثل هذه البيئة.

وتصف هذه التوصية انتهاكات معلومات PII في بيئة التطبيقات التي تستعمل تعرف الهوية على أساس العلامة، ومتطلبات حماية المعلومات PII والهيكل الأساسي لحماية المعلومات PII على أساس مواصفة سياسة المعلومات PII المحددة للمستعمل.

7 تطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة

يعرف التطبيق الذي يستعمل تعرف الهوية على أساس العلامة على أنه تطبيق موسع وأكثر شمولاً لتعرف الهوية يستعمل للتواصل مع مجموعة من الشبكات وفيما بين الشبكات وأنظمة التطبيق الموزعة عالمياً. وبعبارة أخرى، يعتبر تطبيق يستعمل تعرف الهوية على أساس العلامة تطبيقاً قائماً على شبكة عالمية تطلقه علامة تعرف الهوية (بما فيها علامة التعرف بواسطة التردد الراديوي).

وقد تم بالفعل اعتماد التطبيقات التي تستعمل تعرف الهوية على أساس العلامة بشكل واسع في صناعات مثل إدارة سلسلة العرض (SCM) وإدارة المخازن وفي تدابير مكافحة التزييف في سلسلة التزويد بالأدوية. وقد تم توسيع الآن تطبيق تعرف الهوية على أساس العلامة ليشمل منطقة تطبيق المستعمل النهائي (أي تسليم محتوى المعلومات المتعلقة بالمنتجات التي تطلقها علامة تعرف الهوية، وإدارة الخدمة بعد البيع للأشياء المادية، وسجلات المرضى ومراقبة سداد رسوم العبور إلخ.) والتطبيقات الصناعية.

ويمكن تصنيف التطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة إلى ثلاثة أنواع:

أ) مستعمل المطراف ID بصفته عميلاً: في خدمة تسليم محتوى المعلومات مثلاً، يسترجع العميل المعلومات باستعمال المطراف ID الخاص به. وفي هذا النوع من الخدمة، يمكن أن يفترض معظم موردي خدمة التطبيق أن المطراف ID يتمتع بالقدرة على توفير اتصالات متنقلة والقدرة على تقديم المعلومات متعددة الوسائط. ويبين الشكل 1 نموذجاً أساسياً لهذا النوع من التطبيقات. وهو يشمل عمليتين أساسيتين للشبكة: استبانة ID واسترجاع المحتوى.

واستبانة ID هي إجراء نقل أو تحويل معرف هوية إلى عنوان [b-ITU-T Y.2213]. يقوم المطراف المتنقل المجهز بمطراف ID أولاً بتحويل معرف الهوية كما استُلم من علامة ID عبر خدمة الدليل ثم يقوم باسترجاع المحتوى.

الشكل 1 – نموذج أساسي للتطبيق B2C باستعمال تعرف الهوية على أساس العلامة

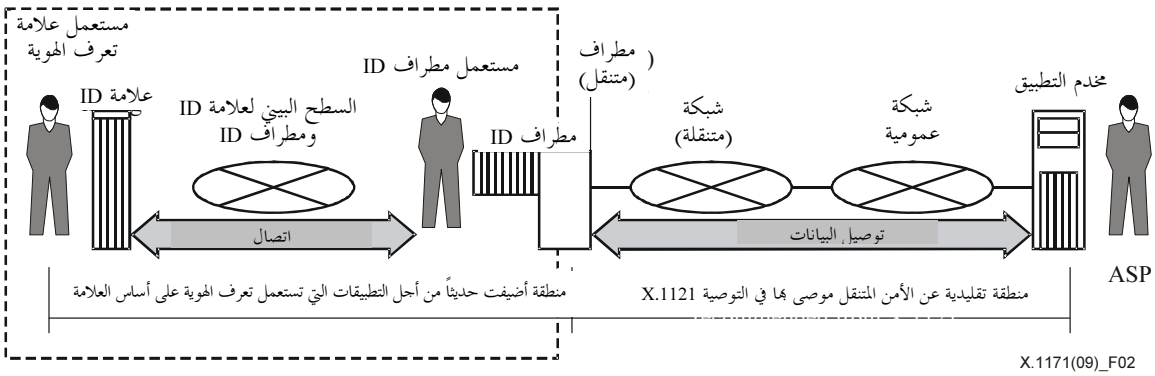
ب) مستعمل العلامة ID بصفته عميلاً: مثال نموذجي عن التطبيق B2C باستعمال تعرف الهوية على أساس العلامة يتعلق بمراقبة النفاذ و/أو الاستيقان، مثلاً المراقبة عند الدخول ومراقبة جوازات السفر، والترخيص، وخدمة الإدارة بعد البيع، وما إلى ذلك. وتكون المطاريف ID في هذا النوع من نموذج التطبيق من نوع المطراف الثابت و/أو المطراف المتنقل، وقد لا يحتاج العميل إلى مطرافه الخاص.

ج) العميل بصفته مستعمل علامة ID أو مستعمل مطراف ID: في خدمة استرجاع المعلومات المتعلقة بالمنتج (نوع أساسي في التطبيق B2C باستعمال تعرف الهوية على أساس العلامة)، يصبح المستعمل أيضاً مستعمل العلامة إثر شرائه المنتج الموسوم بعد استعراض محتوى المعلومات المتعلقة بالمنتج بواسطة مطرافه المتنقل. وفي مثال آخر، يمكن ذكر الخدمة المتعلقة بالرعاية الصحية التي تطلقها بطاقة مريض موسومة بعلامة ID. ويشمل هذا التطبيق عدة فئات من العملاء، من بينهم المريض والطبيب والممرضة إلخ، بوصفهم من مستعملي علامة ID. ويستطيع مستعمل علامة ID أن يتصفح السجلات الخاصة بالمريض بواسطة المطراف المتنقل المجهز بمطراف ID من خلال قراءة بطاقة المريض الموسومة بعلامة ID.

ونظراً لاتساع انتشار التطبيقات التي تستعمل تعرف الهوية على أساس العلامة لتشمل تطبيقات B2C، فإن المستهلكين في غاية الانشغال نتيجة لتسرب المعلومات PII من علامات تعرف الهوية. وينصب التركيز أساساً في هذه التوصية على نموذج التطبيق B2C باستعمال تعرف الهوية على أساس العلامة.

8 نموذج مرجعي لتطبيقات B2C باستعمال تعرف الهوية على أساس العلامة

يبين الشكل 2 نموذجاً مرجعياً لتطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة.



الشكل 2 – نموذج مرجعي لتطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة

يعتبر هذا النموذج المرجعي نموذجاً معززاً لتوصيل البيانات المتنقلة من طرف إلى طرف في التوصية [ITU-T X.1121]. وتشمل الكيانات التي أضيفت حديثاً، علامة تعرف الهوية، ومستعمل علامة تعرف الهوية، والسطح البيني لعلامة ID ومطراف ID. وفي هذا النموذج، يمكن أن يكون المطراف (المتنقل) عبارة عن مطراف سلكي مستقر ومطراف متنقل لا سلكي أيضاً ويمكن اعتباره مطرافاً لتعرف الهوية.

9 انتهاك معلومات PII في التطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة

تحدث أهم الانتهاكات لمعلومات PII في بيئة التطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة، في الحالات التي يتم فيها نقل ملكية منتج معين أو وثيقة موسومة بعلامة تعرف الهوية إلى شخص خاص.

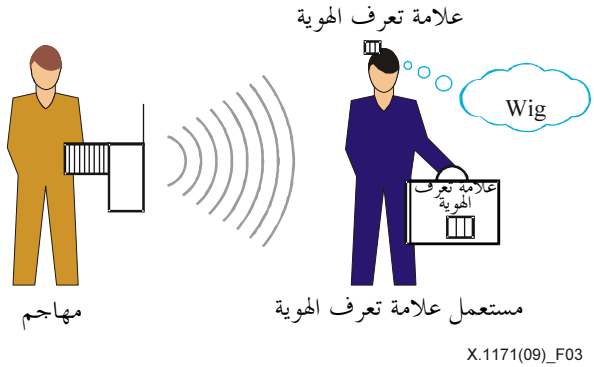
وتوجد في بيئة التطبيقات التي تستعمل تعرف الهوية على أساس العلامة، عدة طرائق تخزين/قراءة لمعرف الهوية كشفرة القضبان (ثنائية الأبعاد) وجهاز المسح البصري (أو آلة التصوير) وقارئ علامة التعرف بواسطة التردد الراديوي المنفعل في المجال القريب وقارئ علامة التعرف بواسطة التردد الراديوي المنفعل في المجال البعيد. ويقتصر هذا البند على وصف التسرب التنوعي لمعلومات PII في بيئة قائمة على أساس العلاقة بين الشركة والعميل في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة. وبصورة أدق، لا يشمل نطاق هذه التوصية التهديدات التالية:

- تهديدات الأمن العام في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة: يقتصر التركيز في هذا البند على التهديدات المتصلة بالمعلومات PII في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة.
- التهديدات الخاصة بطريقة تخزين/قراءة معرف الهوية: مثلاً، في حالة علامة التعرف بواسطة التردد الراديوي، يمكن لمهاجم أن يتتبع موقع مستعمل علامة تعرف الهوية الخاص بمنتج موسوم بعلامة التعرف بواسطة التردد الراديوي من خلال معرف هوية علامة التعرف بواسطة التردد الراديوي. ويقدم التذييل I تفسيراً مفصلاً عن تتبع الموقع في بيئة التعرف بواسطة التردد الراديوي.
- تهديد بين علامة تعرف الهوية ومطراف تعرف الهوية: يقتصر التركيز في هذا البند على تهديدات المعلومات PII على جانب الشبكة.

1.9 تسرب المعلومات المتصلة بمعرف الهوية

يمكن للمهاجم أن يقرأ المعلومات من خلال علامة تعرف الهوية دون أن يكون مستعمل علامة تعرف الهوية للمنتج الموسوم بعلامة تعرف الهوية على دراية بذلك. يقوم المهاجم أولاً بقراءة معرف هوية من خلال علامة ID التي يحملها المستعمل، ثم يحول معرف الهوية ويستفسر عن موقع المعلومات في خدمة الدليل. وأخيراً، يطلب المهاجم المعلومات المتصلة بعلامة تعرف الهوية. وعلاوة على ذلك، إذا كانت هذه المعلومات تتعلق بالمعلومات PII مثل معلومات بطاقة الائتمان أو التاريخ الطبي، وغيره، ففي هذه الحالة قد يعني ذلك انتهاكاً أكثر خطورة لمعلومات PII الخاصة بمستعمل علامة تعرف الهوية. ويصف الشكل 3 انتهاك لمعلومات PII من خلال تسرب المعلومات. وفي هذه الحالة، يمكن للمهاجم أن يجمّع بعض المعلومات المتغيرة (ساعة ومكان شراء المنتج الموسوم، وتتبع معلومات المنتج إلخ.) والمعلومات الثابتة كاسم المنتج ومواصفاته.

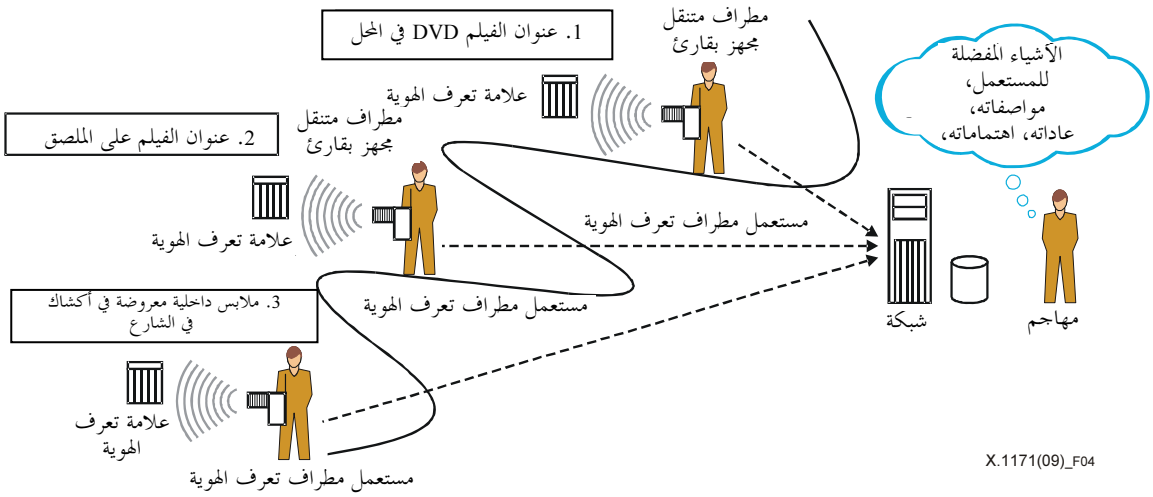
ويمكن منع هذا النوع من الانتهاك لمعلومات PII عن طريق إزالة علامة تعرف الهوية أو تعطيلها. ومع ذلك، يعتبر الاحتفاظ بعلامة تعرف الهوية ووظيفته ضرورياً في العديد من التطبيقات التي تستعمل تعرف الهوية على أساس العلامة كخدمة الإدارة بعد البيع الشخصية، والخدمة المتصلة بالرعاية الصحية وغيرها.



الشكل 3 – انتهاك المعلومات PII من خلال تسرب المعلومات

2.9 تسرب بيانات السياق التاريخي

يستطيع المهاجم أن يستخرج البيانات المفيدة الخاصة بالمستعمل كالأشياء المفضلة له وعاداته ومجالات اهتمامه وما إلى ذلك من بيانات السياق التاريخي المرتبط بعلامة تعرف الهوية. وبالإضافة إلى ذلك، يجوز أن يستعمل المهاجم هذه البيانات لأغراض غير مشروعة أو تجارية دون موافقة المستعمل. وفي حالة الانتهاك هذه، يلجأ المستعمل إلى مستعمل مطراف تعرف الهوية. يقوم مستعمل مطراف تعرف الهوية بقراءة معرف الهوية من خلال منتجات أو وثائق موسومة عن طريق استعمال مطراف تعرف الهوية الخاص به ويحصل على معلومات مفيدة من مخدم التطبيق في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة. وعندئذ، يمكن تجميع مختلف البيانات التي يحتوي عليها السياق التاريخي (تاريخ إعادة فيلم DVD وتاريخ ومكان شراء المنتج، مكان قراءة ملصق الفيلم إلخ.) بواسطة شبكة التطبيقات التي تستعمل تعرف الهوية على أساس العلامة، ويمكن ربط هذه البيانات بالمستعمل (انظر الشكل 4).



الشكل 4 – انتهاك معلومات PII من خلال تجميع بيانات السياق التاريخي

3.9 العلاقة بين انتهاك المعلومات PII والنموذج المرجعي

يلخص الجدول 1 العلاقة بين انتهاكات المعلومات PII والنموذج المرجعي الموضح في الشكل 2. وتعني الخلايا التي تحمل علامة "X" في الجدول أن انتهاك معلومات PII الوارد في الصف مرتبط بكيان أو أن هناك علاقة بين الكيانات الواردة في العمود.

الجدول 1 – العلاقة بين انتهاك المعلومات PII والنموذج المرجعي

الكيانات والعلاقة بين الكيانات	الانتهاكات	
	تسرب المعلومات المتاحة بواسطة التطبيق (التطبيقات) باستعمال تعرف الهوية على أساس العلامة	تسرب بيانات السياق التاريخي المخزنة في مخدم (مخدمات) التطبيق
العلاقة بين علامة تعرف الهوية ومستعمل مطراف تعرف الهوية		X
العلاقة بين المطراف (المتنقل) ومخدم التطبيق	X	X
العلاقة بين مستعمل علامة تعرف الهوية ومخدم التطبيق	X	
العلاقة بين علامة تعرف الهوية ومخدم التطبيق	X	
مخدم التطبيق	X	X

10 متطلبات حماية المعلومات PII لتطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة

ينصب التركيز في هذا البند أساساً على المتطلبات التقنية للتصدي لحالتي انتهاك معلومات PII تم تحليلهما في البند 9. وتتناول توصيات أخرى مبادئ توجيهية أكثر شمولاً لمستعملي وبائعي خدمة تعرف الهوية بواسطة التردد الراديوي فيما يتعلق بحماية المعلومات PII في سياق تكنولوجيا تعرف الهوية بواسطة التردد الراديوي. وتستند هذه المتطلبات في جانب منها إلى المبادئ المستمدة من المبادئ التوجيهية المتعلقة بالخصوصية والصادرة عن منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) [b-OECD]. ويشرح الملحق A أسس هذه المبادئ التوجيهية والتي تمت مراعاتها في هذا البند، فيما يشرح الملحق B أسس أخرى لهذه المبادئ. والمتطلبات التالية مستمدة من انتهاك معلومات PII في تطبيقات B2C التي تستعمل تعرف الهوية على أساس العلامة:

- مراقبة المعلومات PII من جانب مستعمل علامة تعرف الهوية و/أو مستعمل مطراف تعرف الهوية؛
- الاستيقان من مستعمل علامة تعرف الهوية و/أو مستعمل مطراف تعرف الهوية؛
- مراقبة النفاذ إلى معلومات PII الخاصة بمستعمل علامة تعرف الهوية في مخدم التطبيق؛
- سرية البيانات المتعلقة بالمعلومات المرتبطة بعلامة تعرف الهوية؛
- الموافقة على تجميع المعلومات PII؛
- وسائل حماية تقنية لمخدمات التطبيقات.

1.10 مراقبة المعلومات PII من جانب مستعمل علامة تعرف الهوية و/أو مستعمل مطراف تعرف الهوية

يجب أن يكون مستعمل علامة تعرف الهوية و/أو مستعمل مطراف تعرف الهوية قادرين على إدارة أو تحديث معلومات PII المرتبطة بعلامة تعرف الهوية و/أو مطراف تعرف الهوية الخاص به/بها على الشبكة. وهكذا يمكن المستعمل من أن يحدد معلومات PII التي يجب حذفها أو إبقاؤها في التطبيق الذي يستعمل تعرف الهوية على أساس العلامة. كما يمكن للمستعمل تحديد حد زمني لمعلوماته/معلوماته PII في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة.

2.10 الاستيقان من مستعمل علامة تعرف الهوية و/أو مستعمل مطراف تعرف الهوية

يكون مخدم التطبيق مطلوباً في تطبيق يستعمل تعرف الهوية على أساس العلامة لتأمين إجراء الاستيقان لمستعمل علامة تعرف الهوية، ويمكن لمخدم التطبيق أن يؤمن إجراء الاستيقان لمستعمل مطراف تعرف الهوية إذا كان يلزم ذلك (لا تكون بعض التطبيقات التي تستعمل تعرف الهوية على أساس العلامة مطالبة بالاستيقان من المستعمل).

3.10 مراقبة النفاذ إلى معلومات PII الخاصة بمستعمل علامة تعرف الهوية في مخدم التطبيق

النفاذ إلى معلومات PII الخاصة بمستعمل علامات ID من جانب أي مخدم تطبيق ينبغي أن يكون مأموناً وقاصراً على طالبي المعلومات المخولين وعلى المعلومات ذات الصلة التي يطلبها كل منهم.

4.10 سرية البيانات المتعلقة بالمعلومات المرتبطة بعلامة تعرف الهوية

يكون مخدم التطبيق مطلوباً في تطبيق يستعمل تعرف الهوية على أساس العلامة لتوفير سرية البيانات من أجل ضمان عدم تمكن مستعملين غير مرخص لهم من قراءة المعلومات المرتبطة بعلامة تعرف الهوية.

5.10 الموافقة على تجميع معلومات PII

يتعين على مخدم التطبيق في تطبيق يستعمل تعرف الهوية على أساس العلامة، أن يوفر إجراء الموافقة على جمع معلومات PII بما في ذلك بيانات السجل التاريخي لمستعمل مطراف تعرف الهوية. ويوفر التطبيق الذي يستعمل تعرف الهوية على أساس العلاقة حلاً تقنياً للحفاظ على المعلومات PII بالقدر الذي يلزم لها من دقة وحداثة من أجل الغرض المحدد ويقصرها على المعلومات المطلوبة ذات الصلة. وفي عملية الموافقة، ينبغي للتطبيق أن يصرح بالغرض من تجميع المعلومات PII. ويلزم الحصول على موافقة أخرى من المستعمل إذا كانت المعلومات PII التي يتم تجميعها ستستخدم في استخدامات أخرى غير مدرجة في الغرض المحدد سابقاً.

6.10 وسائل حماية تقنية لمخدمات التطبيقات

المورد ASP القائم بتوريد تطبيق يستعمل تعرف الهوية على أساس العلامة مسؤول عن معالجة المعلومات PII، يتعين عليه تبني تدابير أمنية تقنية لمخدمات التطبيق، بما في ذلك المعلومات PII.

7.10 العلاقة بين المتطلبات وانتهاكات معلومات PII

يلخص الجدول 2 العلاقة بين متطلبات الحماية PII وانتهاكات معلومات PII. وتعني الخلايا التي تحمل علامة "X" في الجدول على أن انتهاك المعلومات PII الواردة في العمود متصلة بمتطلبات الحماية للمعلومات PII الواردة في الصف.

الجدول 2 – العلاقة بين المتطلبات وانتهاكات معلومات PII

المتطلبات	الانتهاكات	
	تسرب المعلومات المرتبطة بمعرف الهوية	تسرب بيانات السياق التاريخي
مراقبة المعلومات PII من جانب مستعمل علامة تعرف الهوية و/أو مستعمل مطراف تعرف الهوية	X	
الاستيقان من مستعمل علامة تعرف الهوية و/أو مستعمل مطراف تعرف الهوية	X	X
مراقبة النفاذ إلى المعلومات PII الخاصة بمستعمل علامة تعرف الهوية في مخدم التطبيق	X	
سرية البيانات المتعلقة بالمعلومات المرتبطة بعلامة تعرف الهوية	X	X
الموافقة على تجميع المعلومات PII		X
وسائل حماية تقنية لمخدمات التطبيقات	X	X

الملحق A

المبادئ الأساسية للتطبيق الوطني[2]

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

- قيود التجميع: ينبغي أن تكون هناك قيود على تجميع البيانات الشخصية وأن يتم الحصول على أي بيانات من هذا النوع عبر الوسائل القانونية والنـــزيهة وأن يتم ذلك بعلم أو موافقة صاحب البيانات، إن أمكن.
- جودة البيانات: ينبغي أن تكون البيانات الشخصية ذات صلة بالأغراض التي ستعمل فيها وضمن الحدود اللازمة لهذه الأغراض، على أن تكون دقيقة وكاملة ومحدثة دائماً.
- تحديد الغرض: ينبغي تحديد الغرض من تجميع البيانات قبل البدء في تجميعها وأن يقتصر الاستعمال اللاحق لهذه البيانات على الغرض المحدد أو على أغراض أخرى لا تتفق مع هذا الغرض، تحدد في كل مرة يتم فيها إدخال تعديل على الغرض.
- قيود الاستعمال: لا ينبغي الكشف عن البيانات الشخصية أو إتاحتها أو استعمالها في أغراض غير الأغراض المحددة في الغرض المحدد.
- وسائل الحماية الأمنية: ينبغي حماية البيانات الشخصية باستعمال وسائل حماية أمنية مناسبة من أخطار على غرار فقدانها أو النفاذ غير المخول إليها أو تدميرها أو استعمالها أو تعديلها أو الكشف عنها.
- الانفتاح: ينبغي أن تكون هناك سياسة عامة بشأن التطورات والممارسات والسياسات المتعلقة بالبيانات الشخصية. وينبغي أن تكون الوسائل الخاصة بترسيخ وجود وطبيعة البيانات الشخصية متاحة بسهولة وكذلك الأغراض الرئيسية من استعمالها فضلاً عن هوية المتحكم في هذه البيانات ومقره المعتاد.
- مشاركة الأفراد: ينبغي أن يكون لأي فرد الحق في:

أ) الحصول على المتحكم في البيانات، أو من أي جهة أخرى، على تأكيد بشأن ما إذا كان المتحكم في البيانات لديه بيانات تخصه من عدمه؛

ب) أن ترسل إليه البيانات التي تخصه

- في غضون مدة زمنية معقولة؛
- مقابل رسوم غير مجحفة، إن وجدت؛
- بأسلوب مناسب؛
- بصورة يسهل عليه فهمها؛

ج) أن توضح له أسباب رفض أي طلب مقدم منه طبقاً للنقطتين أ) وب) وأن يكون بمقدوره الاعتراض على هذا الرفض؛

د) أن يختبر المعلومات التي تخصه، إذا كان الاختبار سيؤدي إلى حذف البيانات أو التصديق عليها أو استكمالها أو تعديلها.

- المسؤولية: يكون المتحكم في البيانات مسؤولاً عن الالتزام بالتدابير التي من شأنها تطبيق المبادئ المذكورة أعلاه.

---

[2] هذه المبادئ مستخرجة من الجزء II من "مبادئ توجيهية بشأن حماية البيانات الشخصية وتدفقها عبر الحدود"، منظمة OECD، 1980.

الملحق B[3]

المبادئ الأساسية للتطبيق الدولي: التدفق الحر والقيود التشريعية

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

- ينبغي للدول الأعضاء أن تراعي تداعيات قيام الدول الأعضاء الأخرى بمعالجة البيانات الشخصية محلياً وإعادة تصديرها.
- ينبغي للدول الأعضاء اتخاذ جميع الخطوات المعقولة والمناسبة لضمان أن يكون تدفق اليانات الشخصية عبر الحدود، بما في ذلك العبور خلال دولة عضو، سلساً ومؤمناً.
- ينبغي للدول الأعضاء الإحجام عن تقييد تدفق البيانات الشخصية عبر الحدود فيما بينها إلا إذ اكانت الدولة المنقول إليها البيانات لا تلتزم بهذه البيانات إلتزاماً كاملاً أو إذا كانت إعادة تصدير هذه البيانات تنتهك تشريعاتها المحلية المتعلقة بالخصوصية. كما يمكن لأي دولة عضو فرض قيود بالنسبة لفئات معينة من البيانات الشخصية التي تتضمن تشريعاتها المحلية المتعلقة بالخصوصية لوائح محددة بشأنها من حيث طبيعة هذه البيانات والتي لا توفر الدول الأعضاء الأخرى نفس القدر من الحماية لفئات البيانات هذه.
- ينبغي للدول الأعضاء تحاشي وضع قوانين وسياسات وممارسات بحجة حماية الخصوصية وحرية الأفراد من شأنها وضع العراقيل أمام تدفق البيانات الشخصية عبر الحدود بما يتجاوز المتطلبات الخاصة بهذه الحماية.

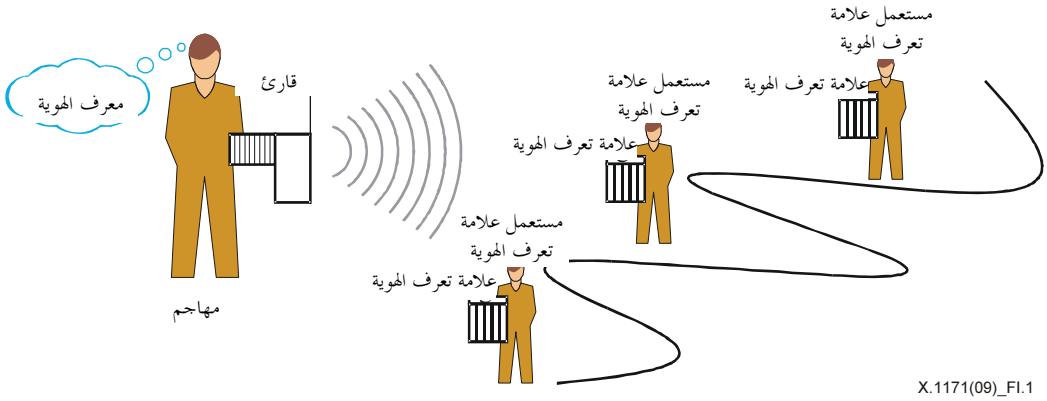
[3] هذه المبادئ مستخرجة من الجزء III من "مبادئ توجيهية بشأن حماية البيانات الشخصية وتدفقها عبر الحدود"، منظمة OECD، 1980.

التذييل I

تتبع معرف الهوية للموقع في خدمات تعرف الهوية بواسطة التردد الراديوي (RFID)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يمكن لمهاجم أن يتتبع مكان مستعمل علامة تعرف الهوية لمنتج موسوم من خلال معرف هوية علامة RFID. ويتيح هذا النوع من انتهاك الأمن إمكانية تتبع معرف هوية علامة خاصة أو رصده باستعمال قارئ RFID محتال غير مرئي. ونظراً لأنه يمكن للمهاجم استعمال معرف هوية العلامة كمعرف شخصي، يمكنه تتبع مكان المستعمل بسهولة كما هو موضح في الشكل I.1.



الشكل I.1 – تهديد الأمن من خلال تتبع مكان شخص

ويمكن استعمال طريقة استيقان بين علامة RFID والقارئ من أجل حماية إمكانية تتبع معرف الهوية. ولا تمنح علامة RFID للقارئ معرف الهوية الخاص به إلا بعد الاستيقان من القارئ بواسطة علامة RFID. وبعبارة أخرى، لا يمكن للمهاجم أن يحصل على معرف هوية العلامة دون إجراء الاستيقان. بيد أنه إذا كانت علامة RFID لا تتمتع بالقدرة الكافية لإجراء عمليات مكثفة من الناحية الحسابية كحسابات التجفير، لا يمكن اعتبار طريقة الاستيقان هذه حلاً واقعياً.

ويمكن أن يتمثل حل آخر في تقنية إعادة تشفير معرف الهوية. ويشمل إعادة تشفير معرف الهوية، إعادة تشفير معرف علامة RFID بشكل دوري بواسطة شبه معرف (أو معرف شرحي)؛ مما يخفض التوصيلية بين معرف علامة RFID ومستعمل علامة تعرف الهوية. ومع ذلك تجدر ملاحظة أن هذه الطريقة لإعادة تشفير المعرف غير قابلة للتطبيق إذا كانت علامة RFID لا تتمتع بوظيفة إعادة القراءة أو إذا كانت علامة تعرف الهوية تستخدم نسقاً معيناً لمعرف الهوية (مثل الشفرة EPC [b-EPCglobal]). علاوة على ذلك، تقتصر فائدة هذه التقنية على الخدمات التي تتطلب قراءة علامة RFID بشكل متكرر، ويجوز أن تؤدي إلى تعقيد كبير على مستوى المخدم.

التذييل II

خدمة حماية المعلومات PII (PPS) في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II خدمة حماية المعلومات PII (PPS) في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة

تشكل الخدمة PPS مثالاً على خدمة لحماية المعلومات PII تقوم على مواصفة سياسة المعلومات PII المتعلقة بالمستعمل.

يبين البند 3.II سيناريو عام للخدمة PPS فيما يتعلق بتطبيق يستعمل تعرف الهوية على أساس العلامة. وبالنسبة إلى الخدمة PPS، تضع علامة تعرف الهوية أو مستعمل مطراف تعرف الهوية المستخدم في تطبيق خاص باستعمال تعرف الهوية على أساس العلامة، سياسات الحماية PII الخاص به/فيما يتعلق بهذا التطبيق ويرسله إلى نظام طرف ثالث موثوق (النظام PPS). ثم يستحدث هذا النظام مواصفة سياسة المعلومات PII الخاصة بالمستعمل ويرسلها إلى مخدمات التطبيق (أنظمة جانب الخدمة). حينئذ، يمكن لمخدمات التطبيق مراقبة النفاذ إلى المعلومات PII المرتبطة بعلامة تعرف الهوية و/أو بمستعمل مطراف تعرف الهوية.

2.II كيانات الخدمة المتعلقة بالخدمة PPS في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة

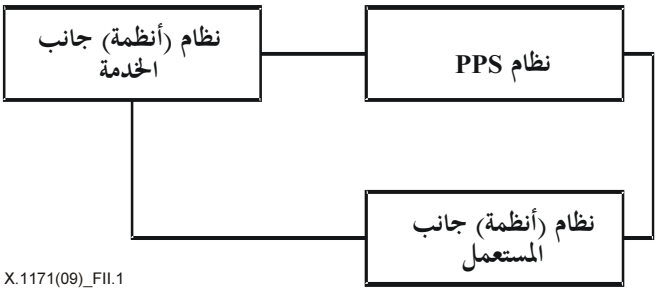
تتمتع الخدمة PPS بثلاثة كيانات كما يلي (انظر الشكل 1.II):

- نظام PPS: يحدد هذا الكيان، بصفته الكيان الذي يقوم بوظيفة إدارة سياسة المعلومات PII الخاصة بالمستعمل، مواصفة سياسة المعلومات PII المعرِّفة للمستعمل فيما يتعلق بسياسة المعلومات PII الخاصة بالمستعمل، ويوفر مواصفة سياسة المعلومات PII لنظام (أنظمة) جانب الخدمة.

  ملاحظة – ينبغي، في حالة نظام PPS مركزي مسؤول عن عدة تطبيقات تستعمل تعرف الهوية على أساس العلامة، اتخاذ تدابير مضادة ملائمة ضد نقطة عطل وحيدة. غير أنه يجوز أن يكون نظام PPS واحد فقط متوفراً في تطبيق يستعمل تعرف الهوية على أساس العلامة، حسب حالة الاستعمال.

- نظام جانب الخدمة: عبارة عن كيان يوفر المعلومات المتصلة بمعرف هوية علامة تعرف الهوية أي يمكن اعتباره بمثابة مخدم تطبيق في تطبيق يستخدم تعرف الهوية على أساس العلامة. وبالتالي، يمكن توفر عدة أنظمة جانب الخدمة لتطبيق واحد يستعمل تعرف الهوية على أساس العلامة. ويؤمن هذا الكيان وظيفة مراقبة النفاذ باستعمال مواصفة سياسة المعلومات PII المعرِّفة للمستعمل أو مواصفة سياسة المعلومات PII بالتغيب.

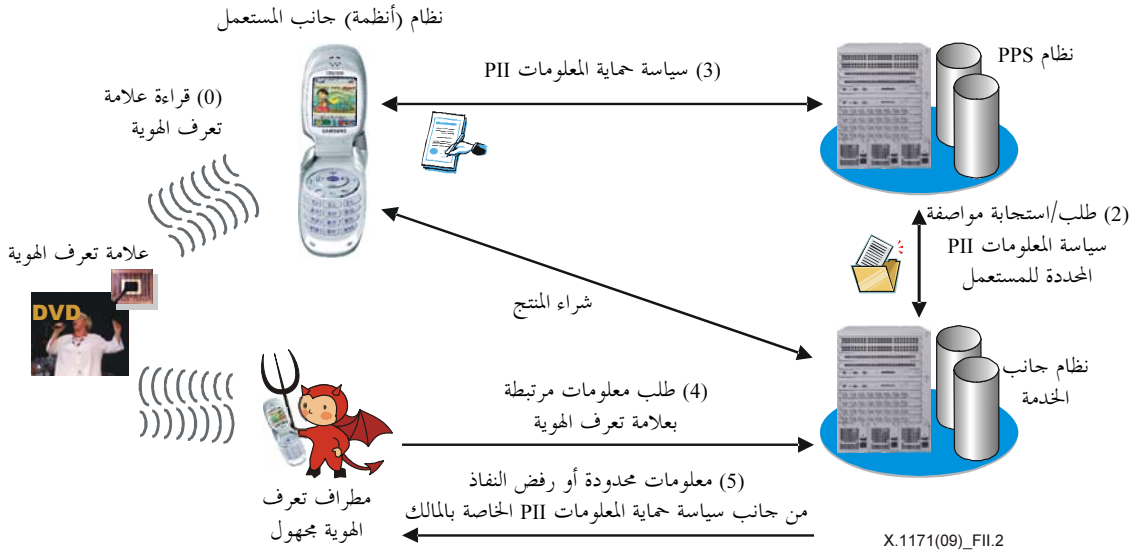
- نظام جانب المستعمل: عبارة عن كيان يؤدي وظيفة النفاذ إلى الشبكة السلكية (أو اللاسلكية) ووظيفة التقاط معرف الهوية عند اللزوم، ويمكن أن يكون هذا الكيان مطرافاً متنقلاً مجهزاً بمطراف تعرف الهوية. ويمكن لمستعمل علامة تعرف الهوية و/أو مطراف تعرف الهوية أن ينفذ إلى نظام جانب الخدمة ونظام PPS عبر نظام جانب المستعمل. وباستعمال نظام جانب المستعمل، يراقب المستعمل سياسة حماية المعلومات PII الخاصة به بها فيما يتعلق بتطبيق خاص يستعمل تعرف الهوية على أساس العلامة.



الشكل 1.II – كيانات الخدمة المتعلقة بالخدمة PPS في تطبيق يستعمل تعرف الهوية على أساس العلامة

3.II السيناريو العام للخدمة فيما يتعلق بالخدمة PPS

ينشأ السيناريو العام للخدمة PPS بصورة عامة عن إجراء علامة شخصي كشراء منتج موسوم. ويوضح الشكل 2.II التدفق العام للخدمة PPS في تطبيق يستعمل تعرف الهوية على أساس العلامة.



الشكل 2.II – التدفق العام للخدمة PPS

0) يقرأ المستهلك معرف الهوية الموجود على المنتج الموسوم باستعمال مطرافه المتنقل المجهز بمطراف تعرف الهوية.

1) يتصفح المستهلك المعلومات المتصلة بالمنتج من خلال شبكة خدمة التطبيق ثم يشتري المنتج باستعمال إحدى طرائق الدفع المختلفة. وعندئذ، يصبح المستهلك مستعمل علامة تعرف الهوية.

2) ثم يطلب التطبيق الذي يستعمل تعرف الهوية على أساس العلامة، مواصفة سياسة المعلومات PII المعرِّفة للمستعمل من النظام PPS، الذي يستجيب فيما بعد للتطبيق باستعمال مواصفة المعلومات PII المعرِّفة للمستعمل.

3) يستقبل النظام PPS سياسة حماية المعلومات PII المتعلقة بالمستعمل بالنسبة إلى هذا التطبيق.

4) يمكن لأي شخص أن يطلب المعلومات المرتبطة بعلامة تعرف الهوية من نظام جانب الخدمة.

5) يمكن لصاحب الطلب أن يتصفح جميع المعلومات التي يقدمها نظام جانب الخدمة إذا كان صاحب الطلب هو مستعمل علامة تعرف الهوية. وخلاف ذلك، يحصل صاحب الطلب على معلومات محدودة أو لا يتمكن من النفاذ إلى المعلومات.

ملاحظة – ثمة حاجة إلى إجراء مزيد من الدراسات بشأن سيناريوهات مختلفة لحالة استعمال الخدمة PPS في التطبيق الذي يستعمل تعرف الهوية على أساس العلامة لوصف مزايا هذه الخدمة.

4.II وظائف الخدمة PPS

تؤدي الخدمة PPS الوظائف التالية لتلبية متطلبات حماية المعلومات PII في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة:

- إدارة مواصفة سياسة المعلومات PII؛
- مراقبة النفاذ؛
- التسجيل؛
- إرسال مواصفة سياسة المعلومات PII؛
- تحديث مواصفة سياسة المعلومات PII.

1.4.II إدارة مواصفة سياسة المعلومات PII

تعتبر إدارة مواصفة سياسة المعلومات PII وظيفة أساسية من وظائف الخدمة PPS. حيث يدير نظام PPS نوعين من أنواع مواصفات سياسة المعلومات PII على النحو التالي:

- مواصفة سياسة المعلومات PII بالتغيب: تشير إلى مجموعة منسقة من قواعد حماية المعلومات PII وسياساتها في تطبيق يستعمل تعرف الهوية على أساس العلامة. ويمكن أن تستند هذه القواعد إلى ممارسات المعلومات المنصفة كتلك الموصوفة في المبادئ التوجيهية الصادرة عن منظمة التعاون والتنمية في الميدان الاقتصادي بشأن حماية السرية وتدفق البيانات الشخصية عبر الحدود [b-OECD].
- مواصفة سياسة المعلومات PII المعرِّفة للمستعمل: يتعلق ذلك بمجموعة منسقة من قواعد حماية المعلومات PII وسياساتها كما يعرفها مستعمل علامة تعرف الهوية و/أو مطراف تعرف الهوية.

يقوم نظام PPS بوضع مواصفة سياسة المعلومات PII المعرِّفة للمستعمل (أو بالتغيب) وإدارتها. وبالتحديد، يجب على النظام PPS أن يضع مواصفة سياسة المعلومات PII بالتغيب ويديرها في تطبيق يستعمل تعرف الهوية على أساس العلامة، ومواصفة المعلومات PII من خلال سياسة حماية المعلومات PII الخاصة بالمستعمل كما هو منصوص عليه في إجراء التسجيل. وهكذا يمكن إرسال مواصفة السياسة PII هذه إلى نظام (أنظمة) جانب الخدمة. ويمكن أن تتضمن ثلاثة عناصر أساساً:

- سياسة الكشف المتعلقة بموارد المعلومات (بما في ذلك المعلومات التي يمكن تعريف هوية أصحابها شخصياً (PII))
- سياسة انقضاء الصلاحية المتعلقة بموارد المعلومات
- سياسة تجميع المعلومات المتعلقة بالسياق التاريخي للأحداث

ويراقب نظام جانب المستعمل فيما بعد النفاذ إلى موارد المعلومات باستعمال مواصفة السياسة PII بالنسبة إلى كل جهة تطلب المعلومات.

2.4.II مراقبة النفاذ

تستعمل وظيفة مراقبة النفاذ في النظام PPS للاستيقان من هوية المستعمل أو مورد خدمة التطبيق وترخيص النفاذ إلى موارد معلومات المستعمل التي تشكل أساساً سياسات حماية المعلومات PII الخاصة بالمالك.

ملاحظة – يستعمل التعبير "هوية" على أن يُفهم منه، في سياق الاتصالات، أنه يدل على معرف الهوية أو مجموعة من معرفات الهوية الموثوقة، بمعنى أنه يمكن الاعتماد عليها لأغراض حالة خاصة لتمثيل عنصر شبكة، أو جهاز مطراف الشبكة، أو مستعمل بعد استكمال عملية إقرار الصلاحية. ولا يمكن أن يستخلص، من هذا التعبير على النحو المستعمل هنا، أن المعرفات الموثوقة تعني أنه تم التحقق من هوية شخص ما على نحو إيجابي.

ومن جهة أخرى، تعد وظيفة مراقبة النفاذ في نظام جانب الخدمة مكوناً أساسياً في النظام PPS، نظراً لأنه يجب على نظام جانب الخدمة مراقبة النفاذ إلى جميع موارد المعلومات وتوفير المعلومات PII بناءً على مواصفة سياسة المعلومات PII المحددة للمستعمل (أو مواصفة السياسة PII بالتغيب في حالة عدم وجود مواصفة السياسة PII المحددة للمستعمل). ويجب أن يكون نظام جانب الخدمة قادراً على استخلاص ما إذا كان الطالب يتمتع بالنفاذ أم لا إلى بعض المعلومات PII المتعلقة بالمستعمل بناءً على مواصفة سياسة المعلومات PII المحددة للمالك.

3.4.II التسجيل

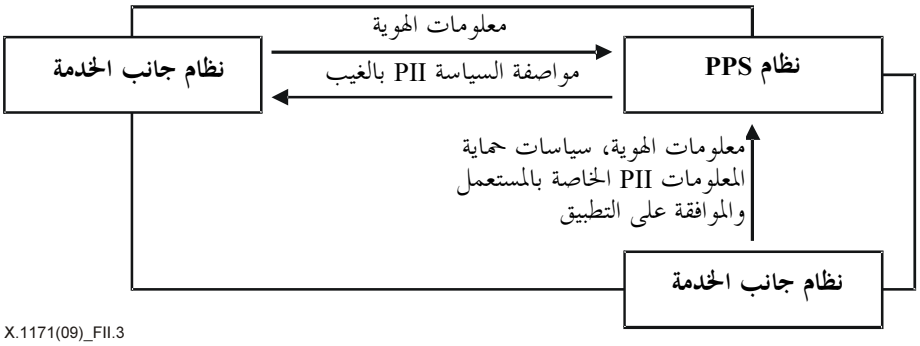
يتميز نظام جانب الخدمة ونظام جانب المستعمل بإجراء للتسجيل مع النظام PPS. وتكون معلومات التسجيل التي يقدمها النظامان في هذا الإجراء كالآتي:

- نظام جانب الخدمة: معلومات الهوية (بما في ذلك معلومات الاستيقان ككلمة السر) ونوع المعلومات (أي معلومات عن السعر، طريقة الشراء، إلخ.) التي يوفرها مخدم التطبيق الذي يستعمل تعرف الهوية على أساس العلامة إلى نظام جانب الخدمة.

– نظام جانب المستعمل: معلومات الهوية (بما في ذلك معلومات الاستيقان ككلمة السر) وسياسات الحماية PII الخاصة بالمستعمل والموافقة على التطبيق الذي يستعمل تعرف الهوية على أساس العلامة.

يجب على النظام PPS أن يضع مواصفة السياسة PII بالتغيب من أجل نظام جانب الخدمة وأن يوفر مواصفة السياسة PII بالتغيب لنظام جانب الخدمة (انظر الشكل 3.II). ويمكن وضع مواصفة السياسة PII بالتغيب من خلال وظيفة إدارة المواصفة PII.

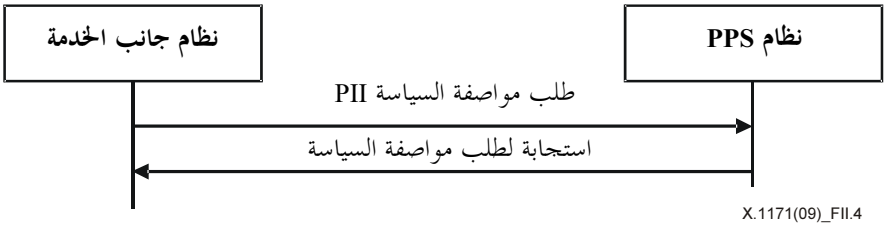
ومن جهة أخرى، يجب على النظام PPS أن يضع مواصفة السياسة PII المحددة للمستعمل بناءً على سياسات حماية المعلومات PII الخاصة بالمستعمل. ويبين الشكل 3.II إجراء التسجيل للنظام PPS.



الشكل 3.II – إجراء التسجيل

4.4.II إرسال مواصفة السياسة PII

يطلق نظام جانب الخدمة إجراء إرسال مواصفة السياسة PII. ويبين الشكل 4.II إجراء إرسال المواصفة PII.



الشكل 4.II – إجراء إرسال مواصفة السياسة PII

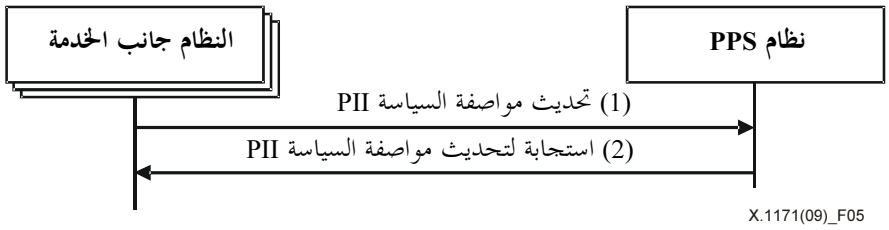
1) طلب مواصفة السياسة PII: يطلب نظام جانب الخدمة مواصفة السياسة PII المحددة للمستعمل مع معرف هوية المستعمل.

2) استجابة لطلب مواصفة السياسة PII: يتحقق النظام PPS من مواصفة السياسة PII المحددة للمستعمل فيما يتعلق بهذا المستعمل ثم يرسل مواصفة السياسة PII المعرِّفة للمستعمل.

ملاحظة – يستعمل التعبير "هوية" على أن يُفهم منه، في سياق الاتصالات، أنه يدل على معرف الهوية أو مجموعة من معرفات الهوية الموثوقة، بمعنى أنه يمكن الاعتماد عليها لأغراض حالة خاصة لتمثيل عنصر شبكة، أو جهاز مطراف الشبكة، أو مستعمل بعد استكمال عملية إقرار الصلاحية. ولا يمكن أن يستخلص، من هذا التعبير على النحو المستعمل هنا، أن المعرفات الموثوقة تعني أنه تم التحقق من هوية شخص ما على نحو إيجابي.

5.4.II تحديث مواصفة السياسة PII

يطلق نظام PPS إجراء تحديث مواصفة السياسة PII. عندما يغير المستعمل سياسات حماية PII الخاصة به، يعيد النظام PPS توليد مواصفة السياسة PII المحددة للمستعمل. ثم يرسل النظام PPS رسالة تحديث مواصفة السياسة PII إلى جميع أنظمة جانب الخدمة المسجلة في النظام PPS. وبعد ذلك، يقوم كل نظام جانب الخدمة بتحديث مواصفة السياسة PII المحددة للمستعمل ثم يرسل رسالة استجابة لتحديث مواصفة السياسة PII. ويبين الشكل 5.II إجراء تحديث مواصفة السياسة PII.



الشكل 5.II – إجراء تحديث مواصفة السياسة PII

1) تحديث مواصفة السياسة PII: يرسل النظام PPS المواصفة PII المحددة للمستعمل المحدّثة إلى كل نظام لجانب الخدمة.

2) استجابة تحديث مواصفة السياسة PII: يرسل كل نظام رسالة استجابة للتحديث إلى النظام PPS.

بيبليوغرافيا

[b-ITU-T F.771] Recommendation ITU-T F.771 (2008), *Service description and requirements for multimedia information access triggered by tag-based identification*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.

[b-ITU-T Y.2213] Recommendation ITU-T Y.2213 (2008), *NGN service requirements and capabilities for network aspects of applications and services using tag-based identification*.

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

[b-EPCglobal] EPCglobal standard (2008), EPCglobal Tag Data Standards Version 1.4. <http://www.epcglobalinc.org/standards/tds/tds_1_4-standard-20080611.pdf>

[b-OECD] OECD (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. <http://www.oecdbookshop.org/oecd/display.asp?CID=&LANG=EN&SF1=DI&ST1=5LMQCR2K94S8>

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	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2009