الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T X.1275

(2010/12)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

مبادئ توجيهية بشأن حماية المعلومات التي يمكن تَعرُّف هوية أصحابها شخصياً (PII) في تطبيقات تكنولوجيا التعرُّف بواسطة التردد الراديوي (RFID)

التوصيـــة ITU-T X.1275

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
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
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

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

التوصيـــة ITU-T X.1275

مبادئ توجيهية بشأن حماية المعلومات التي يمكن تَعرُّف هوية أصحابها شخصياً (PII) في تطبيقات تكنولوجيا التعرُّف بواسطة التردد الراديوي (RFID)

الملخص

تعترف التوصية ITU-T X.1275 بأن تكنولوجيا التعرُّف بواسطة التردد الراديوي (RFID) تجعل المعلومات المتعلقة تحديداً بالبضائع التي يرتديها أو يحملها الأفراد عرضةً لإساءة الاستعمال حتى وإن كانت تؤدي إلى تيسير النفاذ إلى مثل هذه المعلومات وتوزيعها لأغراض نافعة. ويمكن أن تكون إساءة الاستعمال ظاهرة للعيان من قبيل اقتفاء أثر الفرد لمعرفة مكانه أو انتهاك خصوصيته بأي أسلوب غير مشروع. ولذلك، تقدم هذه التوصية مبادئ توجيهية بشأن إجراءات RFID التي يمكن استعمالها من أجل التمتع بفوائد هذه التكنولوجيا مع محاولة حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII) في نفس الوقت.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1275	2010/12/17	17

الكلمات الافتتاحية

حماية المعلومات التي يمكن تعرف هوية أصحابها شخصياً، تطبيقات التعرف بواسطة التردد الراديوي (RFID).

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/.

جـــدول المحتـــويات

الصفحة

الصفحة

التوصيـــة ITU-T X.1275

مبادئ توجيهية بشأن حماية المعلومات التي يمكن تَعَرُّف هوية أصحابها شخصياً (PII) في تطبيقات تكنولوجيا التعرُّف بواسطة التردد الراديوي (RFID)

1 مجال التطبيق

تُقدِّم هذه التوصية الإرشاد لفائدة مستعملي وبائعي تكنولوجيا التعرف بواسطة التردد الراديوي (RFID) (بمن فيهم مقدمي خدمات هذه التكنولوجيا ومُصَنِّعيها) في حماية المعلومات التي يمكن تعرف هوية أصحابها شخصياً (PII) قصد حماية خصوصية الأفراد في إطار تكنولوجيا RFID.

ويمكن تطبيق هذه المبادئ التوجيهية على الحالات التي يمكن أن يُستخدَم فيها نظام RFID لانتهاك خصوصية الفرد، فالمعلومات التي يمكن تعرف هوية أصحابها شخصياً (PII)، على سبيل المثال، تُسجَّل في بطاقة لتكنولوجيا RFID ثم تُجمَّع لاحقًا، أو تُربَط معلومات الشيء (أو الهدف) المجمعة بواسطة تكنولوجيا RFID بمعلومات PII. بيد أن هذه المبادئ لا تنطبق على تلك الحالات التي تُجمَّع فيها معلومات الشيء وتُستخدَم دون أية مخاطر لإفشاء معلومات PII وانتهاك الخصوصية.

وتسعى هذه المبادئ التوجيهية إلى حماية معلومات PII لصالح خصوصية الأفراد الذين يُحتمل أن يتأثروا جراء نظام RFID وتعزيز بيئة آمنة لاستخدام RFID. ويُقصَد من هذه المبادئ التوجيهية توفير القواعد الأساسية لمقدم خدمة RFID وتقديم الإرشاد لفائدة مقدم خدمة RFID ومُصَنِّعي هذه التكنولوجيا ومستعملها فيما يتعلق بالخصوصية في نظام RFID وهي مبادئ تخضع للقوانين المحلية والوطنية.

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.

[ISO/IEC 18000] ISO/IEC 18000-6 (2004), *Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz.*

[ISO/IEC 19762-3] ISO/IEC 19762-3 (2005), *Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part3: Radio frequency identification (RFID).*

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 المعلومات التي يمكن تعرُّف هوية أصحابها شخصياً (PII) [ITU-T X.1171]: المعلومات المتعلقة بأي شخص حي، والتي تجعل التعرف على مثل هذا الفرد ممكناً (بما في ذلك المعلومات القادرة على تحديد هوية شخص عند الجمع بينها وبين معلومات أخرى حتى وإن كانت المعلومات لا تعرف هذا الشخص بوضوح).

2.1.3 نظام التعرّف بواسطة التردد الراديوي (RFID) [ISO/IEC 19762-3]: النظام الأوتوماتي لتحديد الهوية ونظام التقاط البيانات المتضمن قارئة/مستفهمة واحدة أو أكثر لنظام RFID وبطاقة واحدة أو أكثر لهذا النظام حيث يتحقق نقل البيانات بواسطة ترددات حاملة مُشكَّلة بالأسلوب الملائم وتكون إما حثية أو مشعة كهرمغنطيسية.

3.1.3 بطاقة التعرف بواسطة التردد الراديوي (RFID) [ISO/IEC 19762-3]: أي جهاز مرسل-مستجيب مع آلية تخزين المعلومات الملحقة بالشيء.

2.3 مصطلحات معرَّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 الموافقة: تقديم اتفاق لاختيار القبول أو الرفض لقيام مراقب البيانات بجمع أو نقل أو استخدام أو تخزين أو أرشفة أو التصرف (في) معلومات PII محددة، ويعني ذلك اتفاقاً فرديّاً محدوداً.

2.2.3 مراقب البيانات: كيان يربط معلومات الشيء المسجلة في بطاقة تكنولوجيا RFID بمعلومات PII، أو يسجل معلومات PII في بطاقة تكنولوجيا RFID، أو يجمع معلومات PII المسجلة في بطاقة RFID.

3.2.3 موضوع البيانات: شيء يمكن التعرف عليه بواسطة جزء أو أكثر من البيانات المتعلقة بصفاته البدنية والفسيولوجية والعقلية والمالية والثقافية والاجتماعية.

4.2.3 اختيار القبول: موافقة الفرد الصريحة على قيام مراقب البيانات بجمع أو نقل أو استخدام أو تخزين أو أرشفة أو التصرف (في) معلومات PII محددة، لغرض محدد.

5.2.3 اختيار الرفض: ممارسة الفرد لاختيار من خلال طلب عدم حدوث عملية معينة لجمع أو نقل أو استخدام أو تخزين أو أرشفة أو التصرف (في) بيانات معينة.

6.2.3 بيانات شخصية: انظر المعلومات التي يمكن تعرُّف هوية أصحابها شخصياً، حيث إن المصطلحين مترادفان.

7.2.3 مُصَنِّع تكنولوجيا التعرف بواسطة التردد الراديوي (RFID): أي كيان يُصنِّع ويبيع رقاقات/بطاقات تكنولوجيا RFID أو يُصنِّع (ما يشمل المعالجة أو التجميع) ويبيع أشياء تشمل بطاقات مدمجة وملحقة بهذه التكنولوجيا.

8.2.3 مورّد خدمة تكنولوجيا التعرف بواسطة التردد الراديوي (RFID): أي كيان يقدم خدمة تستخدم أشياء تحمل بطاقات تكنولوجيا RFID تكون مدمجة أو ملحقة.

9.2.3 المستعمِل: شخص يقتني شيئاً يشمل بطاقات مدمجة أو ملحقة بتكنولوجيا RFID أو يستفيد من خدمة تستخدم شيئاً يحمل بطاقة مدمجة أو ملحقة بتكنولوجيا RFID.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

- AES: معيار تشفير متقدم *(Advanced Encryption Standard)*
- NFC: اتصالات المجال القريب *(Near Field Communication)*
- PDA: مساعد رقمي شخصي *(Personal Digital Assistant)*
- PIA: تقييم أثر الخصوصية *(Privacy Impact Assessment)*
- PII: المعلومات التي يمكن تعرف هوية أصحابها شخصياً *(Personally identifiable information)*
- RFID: التعرف بواسطة التردد الراديوي (RFID) *(Radio frequency identification)*

5 الاصطلاحات

لا توجد.

6 مبادئ الخصوصية

تستند هذه المبادئ التوجيهية الموصوفة في هذه التوصية إلى مبادئ الخصوصية الواردة في الوثائق التالية: [b-Council Of Europ] و[b-EC1] و[b-EC2] و[b-OECD] و[b-UNHCR] وتشمل هذه المبادئ على وجه التحديد ما يلي:

- قيود الجمع: ينبغي أن تكون هنالك قيود على جمع البيانات الشخصية وينبغي أن يتم الحصول على أية بيانات من هذا النوع بواسطة وسائل قانونية ونزيهة وملائمة، بمعرفة أو بموافقة موضوع البيانات.
- جودة البيانات: ينبغي أن تكون البيانات الشخصية ذات صلة بالمقاصد التي يتعين استخدامها من أجلها وينبغي أن تكون، في الحدود الضرورية لتلك المقاصد، دقيقة وكاملة ومحدَّثة.
- تحديد المقاصد: ينبغي أن تُحَدَّد مقاصد جمع البيانات الشخصية في غضون فترة لا تتجاوز موعد جمع المعلومات وينبغي أن يقتصر الاستخدام اللاحق لها على تحقيق تلك المقاصد، أو على مقاصد أخرى ليست غير متلائمة مع تلك المقاصد ومتوافقة مع الطريقة التي تُحَدد بها عند كل مناسبة لتغير المقاصد.
- قيود الاستخدام: ينبغي ألا يتم إفشاء البيانات الشخصية، أو إتاحتها أو استخدامها لأية مقاصد أخرى غير تلك المحددة طبقاً للمقصد المحدد.
- ضمانات الأمن: ينبغي أن تتم حماية البيانات الشخصية بواسطة ضمانات أمنية ضد مخاطر من قبيل فقدان البيانات أو النفاذ إليها غير المسموح أو إتلافها أو استخدامها أو إفشائها.
- الانفتاح: ينبغي أن تكون هنالك سياسة عامة للانفتاح بشأن هذه المستجدات والممارسات والسياسات فيما يتعلق بالبيانات الشخصية. وينبغي أن تتوفر وسائل سهلة المنال لإثبات وجود بيانات شخصية وطبيعتها والمقصد الرئيسي من استخدامها، وكذلك هوية مراقب البيانات ومحل إقامته العادي.
- المشاركة الفردية: ينبغي أن يكون للفرد (ذكراً كان أم أنثى) الحق فيما يلي:

أ) الحصول من مراقب البيانات، أو التأكد، بأية طريقة أخرى، مما إذا كان مراقب البيانات يحتفظ ببيانات تخصه أم لا؛

ب) والاستجابة لإرسال البيانات التي تخصه إليه في غضون فترة معقولة؛ ومقابل رسوم معينة، إن كانت مطبقة، مع عدم الشطط فيها؛ وبطريقة معقولة؛ وبأسلوب يكون مفهوماً بسهولة بالنسبة إليه؛

ج) وإعطائه أسباب الرفض، إذا ما تقدم بطلب بمقتضى الفقرتين الفرعيتين (أ) و(ب) أعلاه، وإتاحة الفرصة له للاعتراض على هذا الرفض؛

د) والاعتراض على البيانات التي تخصه والاستجابة لمحو البيانات، أو تصحيحها، أو استكمالها، أو تعديلها إذا ما كان الاعتراض ناجحاً.

- المساءلة: ينبغي أن يكون مراقب البيانات قابلاً للمساءلة بشأن الامتثال للتدابير التي تنفذ المبادئ المبينة أعلاه.

7 تهديدات وانتهاكات معلومات PII في تكنولوجيا RFID

يمكن أن تُنسَب تهديدات وانتهاكات معلومات PII في RFID إلى خصائص تكنولوجيا RFID بدون احتكاك، ومواطن ضعف الاتصالات اللاسلكية، واحتمال جمع طرف ثالث للمعلومات بواسطة قارئة RFID. ويصف التذييل الثاني خصائص تكنولوجيا RFID بالتفصيل.

وبالإضافة إلى ذلك، هنالك احتمال متزايد بانتهاك معلومات PII بسبب استحداث تكنولوجيا RFID، ما دامت المعلومات التي يحصل عليها مراقب البيانات انطلاقاً من بطاقة RFID يمكن استعمالها في جميع أنحاء الشبكة بكاملها، عوضاً عن استعمالها طبقاً لقوانين وأطر تنظيمية وسياسات وطنية وإقليمية، ويمكن كذلك تعديل هذه المعلومات من أجل استنتاج معلومات PII. وتصف الفقرة التالية التهديدات والانتهاكات الرئيسية لمعلومات PII التي تشكلها تكنولوجيا RFID.

ومع ذلك، تجدر الملاحظة إلى أن إدراج بعض آليات الأمن داخل البطاقة الحالية لتكنولوجيا RFID قد يكون صعباً بسبب الموارد التي يمكن أن تستهلكها البطاقة – مثل الطاقة الإلكترونية ووقت المعالجة ومساحة التخزين، وما إليها. ويصف التذييلان الأول والثاني قيود تكنولوجيا RFID والتدابير التقنية للحماية في نظام RFID.

1.7 جمع المعلومات يتم في الخفاء

يمكن أن يحدث جمع المعلومات دون معرفة موضوع البيانات، بسبب الخصائص المحددة لتكنولوجيا RFID. ويمكن أن تُقرَأ البيانات الموجودة في بطاقة تكنولوجيا RFID دون وجود أي خط بصر مباشر لأن الموجات الراديوية تخترق العوائق، مثل الحقائب أو الملابس، ولأن أي شخص يحمل قارئة يمكنه قراءة البيانات الموجودة في بطاقة تكنولوجيا RFID. وفضلاً عن ذلك، فإن حجم كل من بطاقة RFID وقارئة RFID يمكن أن يكون لهما حجماً صغيراً جدًّا، كما يمكن ألا توجد أية دلائل على تشغيلها. ويمكن أن تكون هذه الخاصية إحدى أسباب انتهاك معلومات PII لتكنولوجيا RFID.

2.7 رسم المظاهر الجانبية

يمكن أن يكشف النفاذ إلى معلومات بطاقة RFID موجودة في شيء يمتلكه أو يحمله موضوع البيانات جوانب خاصة من التفضيلات (أو الاختيارات المفضلة) لهذا الموضوع. فالمظاهر الجانبية والاستنتاجات التي قد تُستنبَط، على وجه الخصوص، انطلاقاً من زمرة من البطاقات التي يحملها موضوع بيانات يمكن أن تكشف عن معلومات حساسة. وفضلاً عن ذلك، فقد يتم الكشف عن معلومات حساسة، من قبيل الجنسية ومعلومات الاستدلال الأحيائي أو السجلات الطبية، في تطبيقات تكنولوجيا RFID من قبيل جواز السفر الإلكتروني والرعاية الصحية باستخدام تكنولوجيا RFID، ويمكن أن تُستعمَل مباشرة لرسم المظاهر الجانبية واستنباط استنتاجات معينة بشأن موضوع البيانات.

3.7 التتبُّع

يمكن تتبُّع مواضيع البيانات الذين يحملون بطاقة تكنولوجيا RFID، بسبب تخصيص معرف الهوية الوحيد لبطاقة تكنولوجيا RFID.

ويتم تنشيط التتبع بواسطة جمع أو معالجة بيانات عن المكان أو الوقت ويمكن تنفيذه إما في وقت لاحق – أي بعد تخزين البيانات بالفعل في قاعدة بيانات، أو في الوقت الفعلي.

8 تطبيقات RFID

تُستَعمَل تكنولوجيا RFID على نطاق واسع لمجموعة متنوعة من التطبيقات، من قبيل الرعاية الصحية والنقل واللوجستيات والحكومة الإلكترونية وخدمات المعلومات دعماً لسلسلة البيع بالتجزئة والإمدادات. ويبين الجدول 1 التهديدات الممكنة لمعلومات PII الموجودة في التطبيقات النمطية التي تستخدم تكنولوجيا RFID.

الجدول 1 – التطبيقات النمطية لتكنولوجيا RFID والتهديدات الممكنة لمعلومات PII

المجال	التطبيقات النمطية	المعلومات الموجودة في بطاقة تكنولوجيا RFID	التهديدات الممكنة للخصوصية
سلسلة الإمدادات	إدارة الجرد	منتج	التتبُّع، رسم المظاهر الجانبية للأشخاص، إجراء عملية جرد
	البيع بالتجزئة (مثل الأسواق المركزية)	منتج	التتبُّع، رسم المظاهر الجانبية (بعد شراء السلع)
النقل واللوجستيات	تذاكر النقل العام	هوية المستعمِل، فرض الرسوم، إلخ.	التتبع، رسم المظاهر الجانبية
	رسوم الطرق السريعة	هوية المستعمِل، فرض الرسوم، إلخ.	التتبع، رسم المظاهر الجانبية
	تتبع المركبات	منتج	التتبع، رسم المظاهر الجانبية
	إدارة أسطول/حاويات	منتج	التتبُّع، رسم المظاهر الجانبية للأشخاص، تداول الحاويات
الرعاية الصحية	تتبع المرضى	هوية المريض، السجلات الطبية، إلخ.	التتبع، رسم المظاهر الجانبية، العمل في الخفاء (مثل رقاقة VeriChip)
	الوقاية من أخطاء الأدوية	هوية المريض، السجلات الطبية، الوصفات الطبية، إلخ.	التتبع، رسم المظاهر الجانبية
	تتبع الدم أو الأدوية لمكافحة التزوير	منتج	×
الحكومة الإلكترونية	جواز السفر الإلكتروني	هويات الأشخاص، الجنسية، بيانات الاستدلال الأحيائي	التتبع، رسم المظاهر الجانبية، تزوير معلومات PII
خدمات المعلومات	الملصقات الذكية	منتج	×

مثلما جاء بيانه في الجدول 1، لا تثير كل تطبيقات تكنولوجيا RFID شواغل انتهاك معلومات PII (كما أنها لا تؤدي إلى مشاكل محتملة). وإذا كان تطبيق تكنولوجيا RFID لا يُدرج المستعمل في سلسلة إمدادات ما، على سبيل المثال، فليس من المرجح أن تُثار شواغل بشأن انتهاكات معلومات PII.

ومع ذلك، إذا كان العاملون يقومون على سبيل المثال بمناولة الحاويات في حالات أخرى من تطبيقات سلسلة الإمداد، فإنه يمكن مراقبة نشاط هؤلاء العاملين باستعمال بطاقات RFID.

وتقدم الفقرات الفرعية التالية بعض الأمثلة عن تطبيقات مع تقديم سيناريوهات للخدمات التي يمكن أن يثير فيها انتهاك معلومات PII بعض الشواغل.

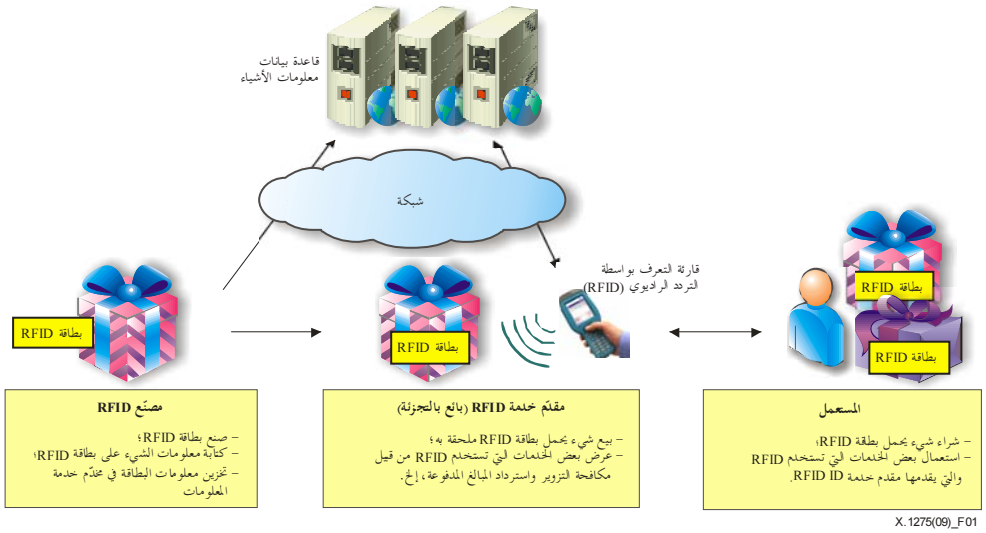
وينشط الجمع بين قارئات تكنولوجيا RFID وغيرها من التطبيقات (مثل تطبيقات الأجهزة المتنقلة) مجموعة متنوعة من علاقات الاتصالات التي يمكن أن تؤدي إلى قدرات معززة للتتبع ورسم المظاهر الجانبية.

1.8 إدارة سلسلة الإمدادات

لقد استُعمِلت تكنولوجيا RFID على نطاق واسع لإدارة سلسلة الإمدادات منذ أمد طويل. وتشمل التطبيقات الرئيسية للأعمال التجارية في مجال إدارة سلسلة الإمدادات والتي تستخدم تكنولوجيا RFID وإدارة الجرد/الموجودات، وتطبيقات البيع بالتجزئة، وما إليها. ويتيح البيع بالتجزئة خدمة تطبيق RFID الأكثر تمثيلية. ويقدم الشكل 1 مثالاً عن استخدام تكنولوجيا RFID في تطبيق للبيع بالتجزئة، كما يمثل كيفية توزيع بطاقة تكنولوجيا RFID.

يتم تمكين تطبيقات البيع بالتجزئة لتكنولوجيا RFID من قبل مُصَنِّع يصنع بطاقة RFID ويكتب معلومات الشيء على بطاقة RFID ويلحق البطاقة بهذا الشيء. وفي هذا المثال، يبيع بائع التجزئة المعني، وهو مقدم خدمة RFID، لمستعملٍ ما شيئاً يحمل بطاقة

RFID مضافة إليه. وقد استُعمِلت البطاقات المنفعلة بصورة عامة لنظام RFID في إدارة سلسلة الإمدادات مع استعمال كلمة سر لإعدام البطاقة، وما إلى ذلك، من أجل حماية معلومات PII الخاصة بموضوع البيانات. وفي بعض الحالات، من قبيل تطبيقات سلع منفردة، غالباً ما تتطلب إدارة سلسلة إمدادات بطاقات منفعلة ذات مدى طويل للاتصالات حتى بالنسبة إلى السلع المنفردة.



الشكل 1 – مثال عن استخدام تكنولوجيا RFID في تطبيقات البيع بالتجزئة

وتُثار الشواغل حول انتهاك معلومات PII فيما يتعلق بتطبيقات البيع بالتجزئة بصورة رئيسية بعد شراء مستعمِل لشيء يحمل بطاقة RFID ملحقة به، ما دامت مشاركة المستعمِل تحدث عند نقطة البيع فقط خلال هذه العملية. وعندما يقتني مستعمِل شيئاً يحمل بطاقة RFID مضافة إليه يمكن للبائع بالتجزئة أن يتعرف على تفضيلات المستعمِل بربط معلومات الشيء المخزنة في بطاقة RFID بمعلومات التسديد الخاصة بالمستعمِل، أو بطاقة ائتمانه، وبالقيام باستمرار بمراقبة وتحليل السلوك الشرائي للمستعمِل. وفي هذه الحالة، يصبح مقدم خدمة RFID هو مراقب البيانات، ويصبح المستعمِل هو موضوع البيانات. وهكذا يمكن لأي شخص يحمل قارئة أن يقرأ بطاقة RFID، ما لم يتم إزالة البطاقة أو إتلافها.

2.8 النقل واللوجستيات

تُعَد أنظمة RFID مناسبة جدّاً لبعض التطبيقات في مجال النقل واللوجستيات. فإذا ما توفر التوزيع الملائم لقارئات RFID، يمكن تتبع المركبات المجهزة ببطاقة في منطقة صغيرة مثل مستودع أو مصنع. أما أنظمة تذاكر النقل العام وجمع رسوم الطرق السريعة، من قبيل تلك الأنظمة الموصوفة في المرجع [b-E-Zpass]، فهي تطبيقات يمكن أن تثير شواغل بشأن الخصوصية في قطاعي النقل واللوجستيات.

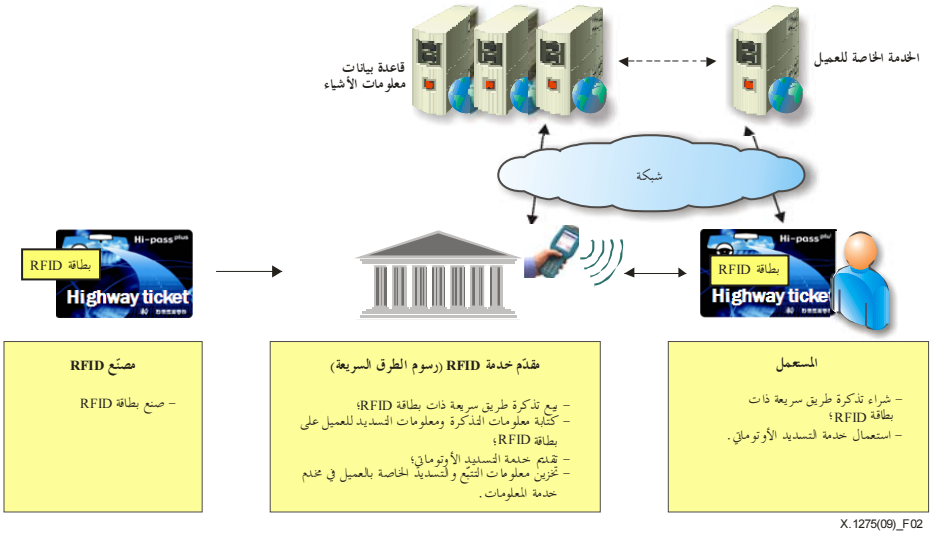
وهنالك عدة تطبيقات لتكنولوجيا RFID في النقل واللوجستيات. وعلى وجه الخصوص، هنالك أنظمة عديدة لتذاكر النقل العام ورسوم الطرق السريعة تستند بالفعل إلى تكنولوجيا RFID. ويُقَدِّم الشكل 2 مثالاً عن تطبيق للنقل، مع توضيح كيفية استعمال بطاقة RFID من أجل التعرف على مركبة وتتبعها في نظام للطرق السريعة.

يقوم مُصَنِّع تكنولوجيا RFID في تطبيق لرسوم الطرق السريعة ببساطة بصنع بطاقة RFID ويبيعها لمقدم خدمة RFID. ويمكن لمقدم خدمة RFID الذي يقدم ويدير خدمة رسوم الطرق السريعة أن يكتب معلومات التسديد الخاصة بالمستعمِل على بطاقة RFID في بعض الحالات المحددة. وتُعَد معلومات التسديد الخاصة بالمستعمِل والمخزنة في بطاقة RFID نوعاً من أنواع المعلومات PII التي يمكن أن تُستعمَل للتعرف على المستعمِل بسهولة.

ومع ذلك، إذا كانت معلومات التسديد الخاصة بالمستعمِل مصاحبة لمعلومات تتبع الحركة الخاصة بالمستعمِل حسبما هي مسجلة في نظام رسوم الطرق السريعة، يمكن لمثل هذه المعلومات أن تُشكِّل تهديداً خطيراً لخصوصية المستعمِل. وفي هذه

الحالة، يُصبح مقدم خدمة RFID – أي نظام رسوم الطرق السريعة – هو مراقب البيانات، ويصبح المستعمِل هو موضوع البيانات.

وقد استُعمِلت البطاقات المنفعلة لنظام RFID، بصورة عامة، في مجال النقل واللوجستيات. ويستعمل في النقل عادة مخططات تشفير بسيطة (تقوم على مخطط تشفير تناظري) لأغراض الاستيقان بين البطاقة والقارئ ولتأمين إرسال البيانات لاحقاً.



الشكل 2 – مثال عن استخدام تكنولوجيا RFID في النقل واللوجستيات

أما بالنسبة إلى تذاكر النقل، فغالباً ما تُستَعمَل بطاقة ذكية بدون احتكاك مُصنَّعَة برقاقة RFID تعمل بتردد 13,56 MHz وبمدى اتصالات قصير. وفي حالة بطاقة ذات مدى قصير للقراءة كمثل هذه الحالة، فإنه يمكن على الأقل تقنياً استعمال مخططات التشفير المؤمّنة التقليدية (حتى وإن كانت تناظرية) – حيث يمكن أن تخفف، جزئيّاً، من خطر تسريب المعلومات PII الخاصة بموضوع البيانات. ويلاحظ، مع ذلك، أن البروتوكولات المستعمَلة في أيامنا هذه يمكن أن تمنع فقط نسخ بطاقة ما (ومن ثم تمنع سلب المستعمِل). ويظل معرّف هوية البطاقة مكشوفاً بنص واضح في بداية المعاملة بين البطاقة والقارئ. وبذلك، يمكن لأي شخص أن يقرأ بطاقة عنصر الهوية، مع ما يلازم ذلك من شواغل انتهاك المعلومات PII. وعلى كل الأحوال، فإن البيانات المجمّعة في قاعدة البيانات عند تعامل المستعمِل مع النظام، ينبغي إخفاءها بأسرع وقت ممكن للحدّ من التهديدات على خصوصية المستعمِل.

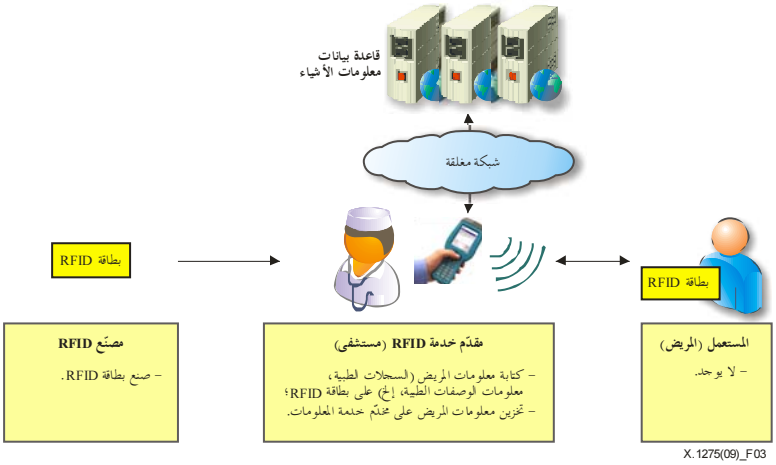
3.8 الرعاية الصحية والتطبيقات الطبية

هنالك عدة تطبيقات لتكنولوجيا RFID في مجال الرعاية الصحية. وبالرغم من ذلك، فإن استعمال تكنولوجيا RFID في تطبيقات الرعاية الصحية يمكن أن تثير شواغل انتهاك معلومات PII بسبب الطبيعة الحساسة لخصوصية بيانات الرعاية الصحية. وتشمل التطبيقات المختلفة لتكنولوجيا RFID في مجال الرعاية الصحية تتبع المرضى لأسباب الأمن والسلامة، وتتبع الأدوية لتدابير مكافحة التزوير، ومطابقة وصفة المريض، وتتبع الدم. وتُستعمَل أنظمة RFID بالفعل في صناعة المستحضرات الصيدلية من أجل تيسير تتبع الأدوية ومنع التزوير والخسارة الناجمة عن السرقة أثناء النقل. ويُقدم الشكل 3 مثالاً عن استعمال RFID في تطبيقات الرعاية الصحية يوضح كيفية استعمال بطاقة RFID.

يقوم مُصنِّع تكنولوجيا RFID في مطابقة وصفة المريض ببساطة بصنع بطاقة RFID وبيعها. ويمكن أن يصبح مقدمو خدمة RFID، أي الأطباء والممرضين/الممرضات في المستشفى، مراقبي بيانات يكتبون ويديرون المعلومات الطبية للمريض.

ويمكن للأطباء والممرضين/الممرضات في المستشفى، في التطبيق المبين في الشكل 3، أن يتحققوا من سجل العلاج والوصفات للمريض من خلال قراءة المعلومات المسجلة في بطاقة RFID التي يحملها المريض، وأن يقوموا لاحقاً باتخاذ الإجراءات الملائمة على أساس مثل هذه المعلومات. وعلى العكس من ذلك، ففي تطبيق تتبع الأدوية، يمكن بسهولة إفشاء معلومات البطاقة

الخاصة بالشخص الذي يحمل الأدوية الحاملة للبطاقة خارج المستشفى أو مخزن الصيدلية؛ ويمكن كذلك استنتاج اسم مرض المريض بصورة مباشرة من معلومات بطاقة RFID. ومن ثم، فإن خطر إفشاء المعلومات الشخصية لموضوع البيانات يمكن أن يكون أعلى من الخطر الكامن في التطبيق الموصوف في الشكل 2. وبناء على ذلك، إذا لم تكن المعلومات الطبية للمريض، حسبما هي مخزنة في بطاقة RFID أو قاعدة بيانات خلفية (أو خفية عن المستعمِل) موضوع إدارة وحماية سليمتين، يمكن لذلك أن يشكل خطراً مباشراً على معلومات PII الخاصة بموضوع البيانات.



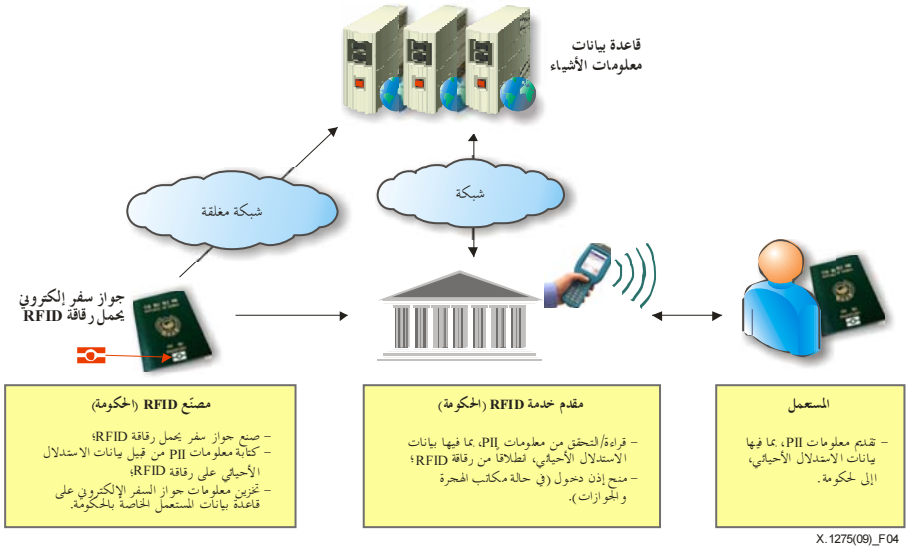
الشكل 3 – مثال عن استخدام تكنولوجيا RFID في الرعاية الصحية والتطبيقات الطبية

و لم تُستعمَل البطاقات النشيطة ذات مدى الاتصالات الطويل بصفة عامة لنظام RFID في التطبيقات الطبية للرعاية الصحية. ومع ذلك، هنالك بعض الحالات التي قد تُفضَّل فيها البطاقة النشيطة ذات مدى الاتصالات الطويل، من قبيل الرعاية المنـــزلية لرصد الحالة الصحية لمريض مُقعد.

4.8 الحكومة الإلكترونية

إن جواز السفر الإلكتروني هو التطبيق الأكثر نمطية في الحكومة الإلكترونية. وعادة ما تحمل رقاقة RFID المدمجة في جواز السفر الإلكتروني الكثير من معلومات PII الخاصة بموضوع البيانات، من قبيل رقم جواز السفر والاسم والجنسية ومعلومات الاستدلال الأحيائي، وما إلى ذلك؛ مما يُحتمل أن يثير شواغل كبرى حيال انتهاك معلومات PII.

ومن الضروري أن تتضمن البطاقة RFID تدابير أمنية مناسبة لتخفيف مخاطر التقاط البيانات أو استنساخها في جواز السفر الإلكتروني، بما أن البيانات الموجودة في هذا الجواز هي الأكثر أهمية وحرجاً من بين كل معلومات PII. ويقدم الشكل 4 مثالاً عن استعمال تكنولوجيا RFID في نظام جواز السفر الإلكتروني، مع توضيح كيفية استعمال رقاقة RFID.



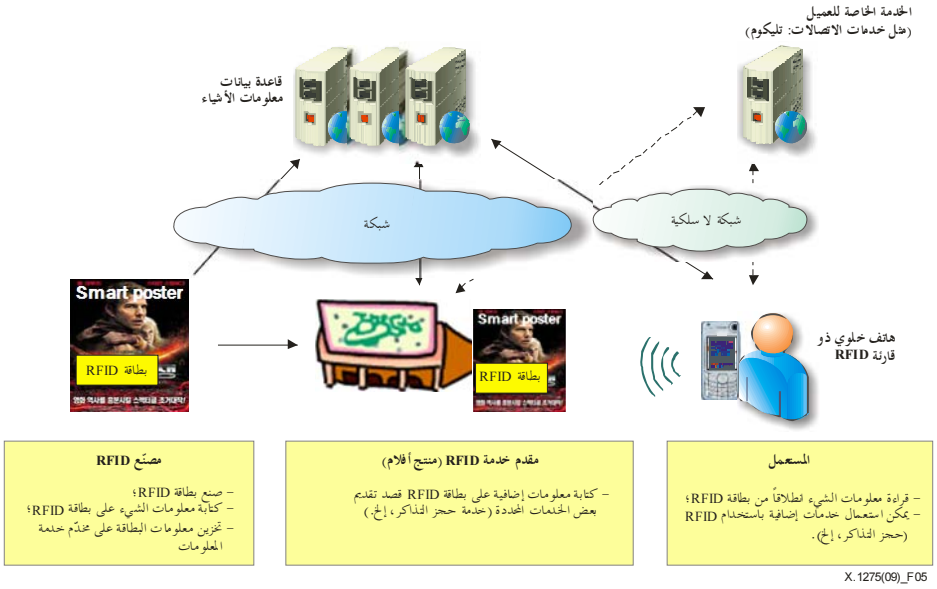
الشكل 4 – مثال عن استخدام تكنولوجيا RFID في تطبيقات جواز السفر الإلكتروني

يُقدِّم أي مستعمِل يرغب في الحصول على جواز سفر بيومتري معلومات PII تشمل بيانات الاستدلال الأحيائي إلى الوزارات الحكومية، التي يمكن أن تكون هي مُصنِّع تكنولوجيا RFID في تطبيقات جواز السفر الإلكتروني. وتصنع هذه الوزارات جواز السفر الإلكتروني مع رقاقة RFID وتكتب عليها معلومات PII الخاصة بالمستعمِل على رقاقة RFID. ويقرأ مقدم خدمة RFID، مثل مكتب الهجرة والجوازات، معلومات RFID من رقاقة RFID ويتحقق منها. وتُعد بيانات الاستدلال الأحيائي المخزنة في رقاقة جواز السفر الإلكتروني من معلومات PII الأكثر حساسية؛ إذ يمكن استعمالها للاستيقان أو للتعرّف على المستعمِل. وإذا تم إفشاء مثل هذه البيانات للاستدلال الأحيائي أو تعديلها، فسوف تشكل تهديداً خطيراً لخصوصية المستعمِل. وفي هذا التطبيق، يمكن أن يكون كل من مُصنِّع RFID ومقدم خدمة RFID مراقب البيانات؛ ويكون المستعمِل هو موضوع البيانات. وقد استُعمِلت البطاقات المنفعلة ذات المدى القصير للاتصالات، بصورة عامة، في هذا التطبيق. ويجب أن يدعم جواز السفر الإلكتروني خاصية التشفير.

بيد أن بروتوكولات الأمن الموصوفة في معايير من قبيل تلك الخاصة بمنظمة الطيران المدني الدولي (الإيكاو) في المرجع [b-ICAO] تُعَد أحياناً اختيارية أو أنها تُستعمَل استعمالاً سيئاً. ومن ثم، فما زالت هنالك شواغل كبرى قائمة إزاء الخصوصية في تطبيقات جواز السفر الإلكتروني.

5.8 خدمة المعلومات

تُعَدّ الملصقات الذكية إحدى التطبيقات النمطية لخدمة المعلومات. وفي حالة الملصقات الذكية، عادة ما تكون قارئة RFID مزودة في جهاز متنقل وتُوجد بطاقة RFID مركبة في موقع ثابت. ويقدم الشكل 5 مثالاً عن استعمال تكنولوجيا RFID في تطبيقات الملصقات الذكية، مع توضيح كيفية استعمال بطاقة وقارئة RFID.



الشكل 5 – تمثيل انسيابي لاستخدام تكنولوجيا RFID في تطبيقات الملصقات الذكية

يقوم مُصَنِّع ملصق ذكي بتكنولوجيا RFID ببساطة بصنع رقاقة RFID ويبيعها لمقدم خدمة RFID. ويكون منتج الأفلام أو قاعة السينما مقدم خدمة RFID الذي يكتب المعلومات بشأن الفيلم على بطاقة RFID المدمجة في الملصق الذكي. وتشكل إرشادات الطرق، في أمثلة أخرى لخدمات المعلومات، خدمة تقدم المعلومات إلى المستعمِل بشأن كيف يجد طريقه بسهولة. ولا تثير مثل هذه التطبيقات أية شواغل بشأن الخصوصية لأنها لا تستعمل أية معلومات خاصة أو حساسة. لاحظ، مع ذلك، أن التنقلية ومدى القراءة لقارئة RFID المدمجة في الجهاز المتنقل يمكن أن تكون عاملاً يهدد خصوصية المستعمِلين.

9 مبادئ توجيهية بشأن حماية معلومات PII

ما دامت التكنولوجيات الخاصة بالخصوصية والأمن المتعلقين بتكنولوجيا RFID ما زالت في مرحلة مبكرة، حتى وإن كانت ما زالت قيد التطوير، ولا يوجد أي حل "ملائم لكل المواقف" بما أن سياق الاستعمال والخصائص التقنية لبطاقات RFID تختلف اختلافاً شاسعاً من تطبيق إلى آخر، فإن تطبيق هذه التكنولوجيات على خدمة RFID برمتها سوف يمثل خطوة سابقة لأوانها. ومن ثم، تركز هذه المبادئ التوجيهية بصورة رئيسية على التدابير الإدارية العامة لحماية معلومات PII الخاصة بموضوع البيانات عوضاً عن التركيز على التدابير التقنية. وبالرغم من ذلك، لا ينبغي تجاهل التدابير التقنية: أثناء تصور تطبيق قائم على تكنولوجيا RFID يُشجَّع المصممون على دراسة اعتماد أحدث الحلول التقنية التي يمكن أن تحسن حماية الخصوصية.

1.9 السياسات والإجراءات

ينبغي أن يقوم مراقبو البيانات في خدمة RFID بصياغة السياسات والإجراءات التي تحكم نظام RFID، لا سيما بشأن الاستعمال الملائم لمعلومات PII، ونشرها على نحو مسبق. وينبغي أن تُحَدد الأدوار والمسؤوليات المتعلقة بإدارة واستعمال معلومات PII في مثل هذه السياسات والإجراءات. وفضلاً عن ذلك، ينبغي أن يكلف شخصاً معيناً يقوم بإدارة واستعمال معلومات PII بالمزيد من المسؤوليات المباشرة بعكس الآخرين.

2.9 تقييد تسجيل معلومات PII

ينبغي لمراقبي البيانات الامتثال لمبدأ تقييد عملية الجمع. وبالتالي، لا يقوم المراقب إلاّ بمعالجة البيانات المرتبطة بالغرض المصمّم من أجله النظام، ويمكن تلافي تخزين المعلومات PII لفترة أطول من اللازم.

ويجب، بوجه خاص، ألا يقوم مراقبو البيانات في خدمة PII في الأحوال العادية بتسجيل معلومات PII على بطاقة RFID، باستثناء الحالات التي يشترط فيها القانون تسجيل معلومات PII أو الحالات التي توجد فيها موافقة كتابية صريحة صادرة عن موضوع البيانات.

ويتعيّن أن تكون جميع معلومات PII المسجلة على بطاقات RFID مشفَّرة، إذا كان على مراقبي البيانات تسجيل معلومات PII على بطاقة RFID. وعندما يحتاج مراقبو البيانات موافقة موضوع البيانات، ينبغي حينها تفضيل اختيار القبول. ويجب أن يُخطر هؤلاء المراقبون موضوع البيانات على نحو مسبق بالغرض من هذا التسجيل والاستعمال المحتمل لمعلومات PII.

ويحتاج مراقبو البيانات في خدمة RFID إلى الحصول على موافقة فردية محددة لكل بند مسجل من معلومات PII وينبغي لهم إخطار مواضيع البيانات عن الغرض من تسجيل أو استعمال معلومات PII.

3.9 المعلومات والموافقة وحق النفاذ والتنقيح وحق الاعتراض

ينبغي لمراقبي البيانات الامتثال لمبدأ المشاركة الفردية. وبالتالي، يتعيّن عليهم اتخاذ التدابير المناسبة لإمداد المستعمِل بمعلومات عن المعلومات PII المسجلة والموافقة وحق النفاذ والتنقيح وحق الاعتراض بالنسبة لمعلومات PII الخاصة بموضوع البيانات دون تحميل المستعمِل أي تكاليف. وينطبق ذلك على المعلومات PII المشفّرة على بطاقات RFID وكذلك على معلومات PII المرتبطة بمعلومات مخزّنة في البطاقات RFID.

1.3.9 المعلومات

ينبغي لمراقبي البيانات إخطار موضوع البيانات ببيان عن البطاقة RFID المُرفقة وبتركيب القارئ RFID وعن الأطراف الثالثة التي تم إخبارها ببيانات عن أي تنقيح أو حذف الحجب، إلا إذا كان هذا الأمر مستحيلاً أو ينطوي على جهود غير مناسبة.

1.1.3.9 ذكر البطاقة RFID المُلحقة

يجب على مراقبي البيانات في خدمة RFID، بالنسبة لبطاقة تكنولوجيا RFID المدمجة أو الملحقة، حتى بعد أن يقتني المستعمِل أو يستلم الشيء، توضيح الأمور التالية للمستعمِل على نحو مسبق قبل شرائه للشيء أو ذكر هذه المعلومات على الشيء أو استعمال وسائل تسهل ملاحظتها:

- حقيقة إلحاق بطاقة RFID وموقعها على الجهاز.
- طبيعة ووظيفة بطاقة RFID.
- نوع المعلومات المسجلة على بطاقة RFID.
- غرض أو استعمال المعلومات المسجلة في بطاقة RFID.
- معلومات الاتصال لموظف حماية البيانات طبقاً للفقرة 9.9.

ويُلاحظ أنه إذا لم يُقصد استعمال موضوع البيانات للبطاقة بمجرد شرائه للشيء، فينبغي حينها إخماد البطاقة من جانب خدمة RFID أو مراقبي البيانات لخطة شراء المستعمِل للشيء الموسوم ما لم يقرر المستعمِل إبقاء البطاقة منشّطة.

2.1.3.9 ذكر تركيب قارئة RFID

يجب على أي شخص يركّب قارئة قادرة على قراءة المعلومات على شيء يحمل بطاقة RFID مدمجة أو ملحقة (أو معلومات PII مسجلة في بطاقة RFID ومسلمة لمواضيع البيانات) ذكر مكان وسبب تركيب قارئة وذلك في مكان مثل مكان الدفع بحيث يمكن لفت نظر مواضيع البيانات لذلك بسهولة. وينبغي لهذا البيان أن يتضمّن على أقل تقدير هوية المشغل وجهة اتصال لكي يتمكّن الأفراد من الحصول على سياسات الخدمة المتعلقة بالمعلومات.

وإذا كانت قارئة RFID مدمجة في مساعد رقمي شخصي (PDA) أو هاتف خلوي، لا بد من تقييد مدى القراءة/للقارئة قصد الحد من حيازة معلومات PII عن طريق بطاقة RFID.

2.3.9 الموافقة

يتعيّن على مراقبي البيانات الحصول على موافقة موضوع البيانات مقدّماً. وفي حالات التجزئة واللوجيستيات، عندما يُخمد المبدأ بالتغيّب، يمكن لمراقبي البيانات الحصول على هذه الموافقة من خلال تلقّي موافقة محددة مكتوبة أو استمارة تسجيل المستعمل أو رسالة عبر البريد الإلكتروني وما إلى ذلك. وفي حالات أخرى على غرار التطبيقات البيومترية لجواز السفر الإلكتروني، لا يتعيّن وجود موافقة من المستعمِل لأن هناك التزاماً قانونياً بجمع معلومات PII وتخزينها في البطاقة.

3.3.9 حقوق النفاذ والتنقيح وحق الاعتراض

ينبغي أن يكون موضوع البيانات قادراً على الحصول على ما يلي من مراقب البيانات دون أي قيود وخلال فترات زمنية معقولة لا تنطوي على أي تأخيرات أو نفقات كبيرة:

- تأكيد بما إذا كانت البيانات المتعلقة بموضوع البيانات تجري معالجتها أم لا، ومعلومات على الأقل عن الأغراض من وراء هذه المعالجة وفئات البيانات المعنية ومتلقّي المعلومات أو فئاتهم الذين سيتمّ إفشاء هذه البيانات لهم،
- رسالة إلى موضوع البيانات في نسق واضح بالبيانات الجاري معالجتها وبأي معلومات متاحة عن مصدرها،
- معلومات عن المنطق المتّبع في أي معالجة آلية لبيانات تتعلق بموضوع البيانات وذلك في حالة القرارات المؤقتة على أقل تقدير.

وعلاوة على ذلك، يتعين وجود وسائل تحكم في الخدمة RFID لاتخاذ التدابير المناسبة لتزويد المستعمل بطريقة لتصحيح وتعديل وتدمير المعلومات PII الخاصة بموضوع البيانات دون تحميل المستعمل أي تكاليف وينطبق هذا الأمر على المعلومات PII المشفرة في بطاقات RFID إضافة إلى المعلومات PII المرتبطة بمعلومات مخزنة على هذه البطاقات.

ويتعيّن، على نحو خاص، على مراقبي البيانات، في حال توقف موضوع البيانات للبطاقة (في قطاع التجزئة، مثلاً، عندما يشتري المستعمل عنصراً موسوماً ببطاقة)، إخماد أو إلغاء أو تدمير البطاقة كما هو مبين في الفقرة 5.9، ما لم يطلب موضوع البيانات استمرار سريان هذه البطاقة.

4.9 القيود على جمع المعلومات PII وربطها

ينبغي لمراقبي البيانات في الخدمة RFID أن يقوموا بإخطار موضوع البيانات ذي الصلة عند جمعهم لمعلومات PII مسجلة في البطاقة أو مخزنة في قاعدة بيانات من خلال ربطها مع معلومات عن الشيء في البطاقة. وإذا احتاج موردو الخدمة RFID إلى استعمال معلومات PII لأغراض خلاف الأغراض الأصلية أو تقديمها إلى طرف ثالث، فإنه يتعيّن عليهم الحصول مقدماً على موافقة مكتوبة محددة وصريحة من موضوع البيانات.

1.4.9 المعلومات PII المسجلة في البطاقة RFID

يتعيّن على مراقبي البيانات في الخدمة RFID إخطار موضوع البيانات ذي الصلة حسب الحالة أو بيان ذلك بصورة يسهل ملاحظتها بأنه بإمكانهم جمع بيانات PII المسجلة في البطاقة RFID والحصول على موافقة محددة وصريحة من المستعمِل مقدماً.

وعند قيام مراقبي البيانات بجمع معلومات PII، يجب عليهم اتخاذ بعض التدابير الخاصة بالتوثيق لكل من القارئ والبطاقة RFID، مثل بروتوكول الاستيقان بين البطاقة والقارئ RFID. وبين القارئ وقاعدة بيانات الطرف النهائي. وتشير "تدابير التوثيق" هنا إلى مخطط تشفير لقاعدة بيانات الطرف النهائي التي تقوم بتخزين معرف هوية البطاقة RFID والمعلومات PII المستعملة في تعريف واستيقان القارئ RFID ومراقب البيانات.

ومن منظور حماية المعلومات PII، تجدر الإشارة مع ذلك إلى أن بروتوكولات الاستيقان الموجودة حالياً بين البطاقة والقارئ تعتبر فعالة فقط إذا كانت البطاقة تخزن معلومات أكثر من معرّف هوية البطاقة، كما هو الحال مع بروتوكولات إرسال RFID الموجودة حالياً، حيث إن معرفة هوية البطاقة نفسه غير محمي.

2.4.9 ربط المعلومات PII بمعلومات الشيء في البطاقة RFID

إذا رغب مراقبو البيانات في ربط معلومات الشيء المسجلة في البطاقة RFID بالمعلومات PII، سيكون عليهم عادة قبل تقديم البطاقة إخطار موضوع البيانات المعني بذلك مقدماً وبيان ذلك بشكل يسهل ملاحظته والحصول على الموافقة المحددة والصريحة. وعند ربط مراقبي البيانات لمعلومات الشيء بالمعلومات PII في البطاقة RFID، ينبغي عليهم اتخاذ بعض تدابير التوثيق للقارئ RFID مثل كلمة السر أو بروتوكول الاستيقان بين القارئ والبطاقة RFID.

وإذا لم يفترض ربط المعلومات PII بمعلومات الشيء وقت جمعها ولكن استدعى الأمر ربطهما فيما بعد، ينبغي لمراقبي البيانات عندها إخطار المستعمِل بالغرض من ذلك والحصول على موافقة أخرى محددة وصريحة امتثالاً للمتطلبات القانونية.

5.9 إخماد البطاقة RFID بمجرد انتفاء الغرض

يجب إزالة البطاقات RFID المدمجة أو الملحقة أو تدميرها أو إخمادها بشكل دائم من جانب مورد الخدمة RFID أو مراقبي البيانات وقت شراء المستعمِل أو استلامه لشيء موسوم ببطاقة (من مركز البيع)، إلا إذا قرر المستعمل الإبقاء على البطاقة نشطة أو إذا كان يفرض ذلك قانون/ولوائح. حتى إذا قرر المستعمِل الإبقاء على البطاقة نشطة، ينبغي لمراقبي البيانات توفير تدابير لإلغاء البطاقات أو تدميرها أو إخمادها بشكل دائم في مرحلة تالية حسب طلب موضوع البيانات. وينبغي إخطار المستعمِل بتبعات عملية الإخماد.

ويتعيّن اعتبار أن الإخماد هو الوضع الطبيعي، وإن كان لا يمثل حلاً مناسباً لجميع التطبيقات. فمثلاً، إذا تم إخماد بطاقة مستخدمة في النفاذ إلى التاريخ العلاجي لمريض ومعلومات عن الأدوية المستعملة في تطبيق للرعاية الصحية، فإن استمرار علاج المريض قد يكون أصعب. ويمكن جعل الإخماد إجبارياً في تطبيقات تندرج ضمن إدارة سلسلة الإمداد، في حين يترك للمستعمِل الخيار في تطبيقات كتلك المتعلقة بالنقل واللوجيستيات. وفي حالة تطبيقات الرعاية الصحية، والحكومة الإلكترونية، لا يطبق الإخماد، سواء بالنسبة للصحة العامة أو بموجب القانون. ويمكن لمصنع RFID أو مراقب البيانات في الخدمة RFID استعمال تدابير تقنية لإخماد البطاقة RFID، مثل استعمال كلمة السر Kill أو إعطابها بجهاز التدمير الكهرباء وما إلى ذلك. وإذا ما أدى إخماد البطاقة RFID إلى تشويش ذهن المستعمِل أو الجمهور، ينبغي عندها لمراقبي البيانات شرح الأسباب للمستعمل أو بيان ذلك على الشيء أو استعمال وسائل يسهل ملاحظتها.

6.9 معلومات عن مورّدي الخدمات ومراقبي البيانات

ينبغي لمورّدي الخدمات ومراقبي البيانات وضع ونشر سياسات المعلومات بشكل محدد ودقيق ويسهل فهمه بشأن كل تطبيق من تطبيقاتهم. وينبغي أن تتضمن هذه السياسات على الأقل ما يلي:

- هوية وعناوين المراقبين،
- الغرض من النظام RFID،
- ما هي البيانات التي سيعالجها النظام، خاصة، إذا كان سيجري معالجة بيانات شخصيته وما إذا كان موقع البطاقات سيتم مراقبته،
- ملخص عن الخصوصية وتقييم لآثار حماية البيانات،
- مخاطر الخصوصية المرجّحة، إن وُجدت، والمتعلقة باستعمال البطاقات في التطبيق والتدابير التي يمكن للأفراد اللجوء إليها للتخفيف من هذه المخاطر.

7.9 تدابير تنظيمية وتقنية لحماية معلومات PII

- عندما يستعمل مراقبو البيانات في خدمة RFID نظام RFID لتسجيل وجمع معلومات PII أو ربط معلومات الشيء المسجلة في بطاقة RFID بمعلومات PII، ينبغي أن يتخذوا التدابير التنظيمية والتقنية الأمنية من أجل حماية معلومات

PII لنظام RFID خِشية فقدان معلومات PII ذات الصلة، أو سرقتها أو تسربها أو تبديلها أو إتلافها. تشمل التدابير التنظيمية والتشغيلية لحماية معلومات PII التدابير التالية:

- خطة إدارة الأمن الداخلي
- تحليل المخاطر، وتحليل تهديدات الخصوصية، وتقييم أثر الخصوصية
- التوعية بالخصوصية في خدمة RFID، إلخ.

– تشمل التدابير التقنية لحماية معلومات PII التدابير التالية:

- مراقبة وتدقيق النفاذ لقاعدة البيانات الخلفية:
- مراقبة النفاذ للحيلولة دون نفاذ أي قارئ للمعلومات المخزّنة في البطاقة
- تشفير المعلومات المخزنة في البطاقة وفي قاعدة البيانات الخلفية
- استعمال أي بروتوكول قابل للتشغيل بين القارئة والبطاقة من أجل حماية إرسال معلومات PII، من قبيل بروتوكولات التشفير أو أية تقنيات يمكن أن تكون ذات صلة
- استعمال البطاقات التي تسمح بتطبيق معرّفات هوية عشوائية للبطاقات، للحدّ من مخاطر التتبُّع
- تصديق قارئة RFID صالحة للاستعمال
- إخماد بطاقة RFID، من قَبيل RFID وكلمة السر kill، وجهاز التحكم عن بُعد لتدمير بطاقة RFID، وما إلى ذلك
- تقييد قدرة القارئة والبطاقة، من قبيل التشويش المقصود النشيط، وكشف محاسيس RFID، والبطاقة المقطعة، وبطاقة الصد، وما إلى ذلك (انظر المرجع [b-Juels])
- تدابير أمنية لتخفيف مخاطر الخصوصية الناشئة عن تقييم أثر الخصوصية.

ويُلاحظ أن التدابير التنظيمية والتقنية المُدرجة أعلاه تشكل جزءاً من كل التدابير المتعلقة بحماية المعلومات PII. وقد تظهر تدابير جديدة في المستقبل نتيجة للتقدم الذي تشهده البحوث في هذا المجال.

8.9 تقييم أثر نظام RFID على الخصوصية

عندما يستعمل مقدمو خدمة RFID ومراقبو بيانات RFID نظاماً RFID من أجل تسجيل وجمع معلومات PII، أو ربط معلومات الشيء المسجلة في بطاقة RFID بمعلومات PII، ينبغي أن يبذلوا الجهود من أجل ضمان عدم انتهاك معلومات PII من خلال تحليل وتقييم أي احتمال لتسرب معلومات PII أو تهديدات لهذه المعلومات المصاحبة لاستعمال نظام RFID، وذلك، عند مرحلة مثالية، قبل إدخال نظام RFID، أي في مرحلة التصميم.

وبسبب التنوع الواسع لسيناريوهات التشكيلات التقنية وسيناريوهات الاستعمال التقني، لا يُوجد أي حل يلائم كل تطبيقات RFID المختلفة. ومن ثم يمكن لتقييم أثر الخصوصية أن يساعد على تحديد التبعات للخصوصية (وفقا لوجهات نظر مختلفة مثل المنظور القانوني والجوانب التقنية) وعلى إيجاد أفضل الاستراتيجيات للتخفيف من هذه التبعات. وتصف الخطوات التالية عملية محتملة لتقييم أثر الخصوصية (PIA) (وينبغي لتقييم PIA أن يغطي النظام RFID بأكمله):

– الخطوة 1: إطلاق المشروع

تحدد هذه الخطوة نطاق الأعمال التجارية، وتنظم عملية PIA القائمة بالتنفيذ فريق تنفيذ PIA، وتطبق أدوات PIA وفقاً لنطاق التطبيق المحدد.

– الخطوة 2: تحليل انسياب البيانات

يتمثل الغرض من هذه الخطوة في السعي لرسم شكل أو مخطط انسيابي للمعلومات التي يمكن تعرف هوية أصحابها شخصياً حتى يمكن التحقق من هدف تحليل المخاطر عن طريق تحديد هذه المعلومات التي تعالجها الخدمة الهدف لتقييم الأثر وموجودات المعلومات التي تتضمن مثل هذه المعلومات.

وتحدد هذه الخطوة، على وجه التحديد، معلومات PII التي تُجمَع أو تُستعمَل أو تُخزَّن أو يتم التصرف فيها أو تُقدَّم إلى طرف ثالث بواسطة استعمال طريقة "ماذا" في شكل أو مخطط انسيابي. وبالإضافة إلى ذلك، تصف هذه الخطوة دور ومسؤولية الشخص المكلف بكل خطوة (جمع، واستعمال، وتخزين، وتصرف) من خطوات معالجة معلومات PII.

- الخطوة 3: تحليل عوامل ومخاطر انتهاك المعلومات التي يمكن تعرف هوية أصحابها شخصياً

تحدد هذه الخطوة التهديدات ونقاط الضعف التي تهدد موجودات هذه المعلومات وتنفذ تحليل المخاطر عليها.

- الخطوة 4: خطة التحسين والتخطيط إدارة المخاطر

تحدد هذه الخطوة مستوى المخاطر الذي يتطلب إدارة المخاطر المختلفة التي تم التعرف عليها أثناء تحليل المخاطر فيما يتعلق بالمعلومات التي يمكن تعرف هوية أصحابها شخصياً وتحضر طرائق مختلفة للمراقبة بالنسبة لكل خطر يتعين التخفيف منه وإدارته.

- الخطوة 5: التبليغ عن نتائج تحليل أثر الخصوصية (PIA)

تستلزم هذه الخطوة، بصفتها أكثر الخطوات حرجاً في عملية PIA، صياغة وتقديم تقارير بشأن عملية PIA ونتيجتها.

وينبغي أن تتضمن PIA تقارير نتيجة المحتويات التي جرت مناقشتها في جميع عمليات PIA، ابتداء من نتيجة PIA ووصولاً إلى طريقة المراقبة وإدارة المخاطر بالنسبة للخطر المحدد فيما يتعلق بالمعلومات التي يمكن تعرف هوية أصحابها شخصياً.

ويلاحظ أن عملية التقييم PIA الموصوفة أعلاه لأغراض التوضيح فقط ويمكن مواءمة عملية التقييم PIA طبقاً للاحتياجات المحددة أو استناداً إلى عمليات تقييم PIA خارجية أخرى موجودة.

9.9 تعيين موظف حماية البيانات

ينبغي أن يقوم مراقبو البيانات بتعيين موظف حماية البيانات يكون مسؤولاً على نحو خاص عن الاحتفاظ بسجل يضم المعلومات التفصيلية عن عمليات المعالجة التي يقوم بها مراقب البيانات، بما في ذلك المعلومات المتعلقة بتقييمات أثر الخصوصية والتدابير الأمنية لتطبيقات RFID، ويكون مسؤولاً كذلك عن المعالجة السريعة لشكاوى المستعملين أو طلباتهم المتعلقة بممارسة حقوقهم.

التذييل I

خصائص وقيود بطاقة RFID

(هذا التذييل لا يشكل جزءاً أساسيّاً من هذه التوصية)

1.I تصنيف وخصائص بطاقات تكنولوجيا RFID

توضح هذه الفقرة خصائص تصنيف بطاقات RFID، وكذلك الأسباب التي تجعل تقنيات الأمن غير قابلة للتطبيق بسهولة على البطاقات المنفعلة. وعادة ما يمكن تصنيف بطاقات RFID إلى صنفين، بطاقات منفعلة وبطاقات نشيطة. ويبين الجدول 1.I تصنيف هذه البطاقات.

الجدول 1.I – تصنيف وخصائص بطاقات تكنولوجيا RFID

الخصائص	البطاقات المنفعلة	البطاقات النشيطة
مصدر الطاقة	الطاقة المنقولة من القارئة	البطاريات الداخلية
مدى الاتصالات	3 أمتار أو أقل	100 متر أو أكثر
عمر نافع	غير محدود	(عمر) مقيد بعمر البطاريات
تخزين البيانات	التخزين الصغير لبيانات القراءة/الكتابة (بالبايتات)	التخزين الكبير لبيانات القراءة/الكتابة (بالكيلو بايتات)
التطبيقات النمطية	إدارة الجرد، البيع بالتجزئة مراقبة الأمتعة/المنصات النقالة، بطاقات الأمن، إلخ.	التطبيقات المعقدة مع وجود شخص متتبع، إلخ. (الرعاية الصحية أو مراقبة منطقة، رسوم الطرق السريعة، إلخ.)

ليس للبطاقات المنفعلة مصدر داخلي للطاقة؛ فهي تستعمِل الطاقة المنقولة من قارئة RFID بغية إرسال الإشارة إلى القارئة. ويبلغ مدى الاتصالات للبطاقات المنفعلة حوالي 3 أمتار أو أقل. وفي حالة التردد 13,56 MHz، يكون مدى الاتصالات 4~10 سنتيمترات ولكن هذا المدى يمكن تمديده بواسطة هوائي واسع النطاق. أما البطاقة ذات الموجات الديسيمترية فلها مدى اتصالات أطول إذ يبلغ حوالي 3 أمتار إلى 7 أمتار.

وبعكس البطاقات المنفعلة، تمتلك البطاقات النشيطة مصدرها الخاص للطاقة الذي يمكنها من إرسال إشارة ما إلى القارئة بنفسها. ويبلغ مدى اتصالات البطاقات النشيطة حوالي 100 متر أو أكثر، ولكن عمرها النافع مقيد بعمر بطارياتها. وعلاوة على ذلك، فإن البطاقات المنفعلة أكبر حجماً وأعلى ثمناً من البطاقات المنفعلة.

وعادة ما يكون نظاماً يعمل في نطاق تردد منخفض (135/125 kHz) أو نطاق تردد عال (13,56 MHz) نظاماً منفعلاً. ويمكن أن تكون الأنظمة العاملة في نطاق الموجات الديسيمترية (900/433 MHz، 2,45 GHz) ونطاق الموجات الصغرية إما أنظمة منفعلة وإمَّا أنظمة نشيطة.

وغالباً ما تُستعمَل البطاقة ذات الترددات المنخفضة لأغراض الأمن وإدارة الموجودات والتحقق من ضمان الاستيقان لمنتج معين بسبب مدى المسح القصير للبطاقة؛ بينما تُستعمَل البطاقة ذات الترددات العالية لخدمات السكك الحديدية واللوجستيات والتوزيع بسبب مدى المسح الخاص بها والبالغ 30 متراً أو أكثر. ويُعَد التردد 13,56 MHz، على وجه الخصوص، تردداً مدمجاً ومستعمَلاً في بطاقات الائتمان أو بطاقات تسديد رسوم النقل. ويُعَد جواز السفر الإلكتروني وكذلك الاتصالات في المجال القريب (NFC) مثالين آخرين عن التطبيقات التي تستعمِل التردد 13,56 MHz.

2.I قيود البطاقات المنفعلة

يسترعي العديد من الخبراء العاملين في قطاع RFID الانتباه إلى أن ثمن بطاقة RFID ينبغي أن يكون أقل من 5 سنتات بغية ترويج سوق RFID. ويقيد هذا الشرط الخاص بسعر البطاقة الموارد التي يمكن أن تستعملها هذه البطاقة، من قبيل الطاقة الكهربائية، ووقت المعالجة، ومساحة التخزين، وعدد البوابات.

ومن أجل تسعير بطاقة بأقل من 5 سنتات، يمكن لبطاقات RFID أن تخزن فقط مئات من البتات وأن يكون لها عدد 5-10 K من البوابات المنطقية، ومدى أقصى للاتصالات يبلغ بضعة أمتار. وضمن هذا العدد من البوابات، يمكن تخصيص عدد يتراوح بين 250 و3 000 بوابة فقط للوظائف الأمنية. أضف إلى ذلك أن قيود الطاقة ينبغي أن تؤخذ في الحسبان، ما دامت أغلب بطاقات RFID المستعملة حاليّاً بطاقات منفعلة.

وغالباً ما تقيد التشريعات القدرة المشعة للقارئات ومن ثم فإن تغذية البطاقة بالطاقة مقيدة بدورها. ويُعَد استعمال التشفير المعياري الآمن في البطاقات المنفعلة، في إطار التكنولوجيا المتوفرة في يومنا هذا، حتى بدون قيود التكلفة، مقتصراً على البطاقات ذات المدى القصير. أما في البطاقات التي لها مدى يبلغ عدة أمتار، فإن القدرة التي تشعها القارئة غير كافية لتغذية البوابات العديدة بالطاقة اللازمة لتنفيذ وظائف التشفير الآمن.

وطبقاً للمرجع [b-CRYPTREC]، تتطلب البطاقة عدداً يساوي 6~13 K من البوابات من أجل تنفيذ خوارزمية تشفير لا تناظري، وتتطلب كذلك عدداً مماثلاً من البوابات لتنفيذ دالة فرم. وعلى سبيل المثال، تتطلب البطاقة عدداً يساوي 20~30 K من البوابات للتنفيذ المعياري لمعيار التشفير المتطور (AES). ويجري حالياً تطوير خوارزمية تشفير خفيف لتطبيقها على بطاقة RFID. ومع ذلك، فإن تنفيذ خوارزمية تشفير داخل بطاقة ما لم يجد التمكين الكامل بسبب هذه القيود على الموارد.

التذييل II

تدابير تقنية لحماية معلومات PII في نظام RFID

(لا يشكل هذا التذييل جزءاً أساسيّاً من هذه التوصية)

يجري تطوير تكنولوجيات مختلفة لحماية معلومات PII من أجل تقليل الانتهاكات التي تهدد الخصوصية في خدمات تطبيق RFID إلى الحد الأدنى. ويجري، على وجه الخصوص، تطوير التكنولوجيات الجديدة الموصوفة أدناه، ما دامت التكنولوجيا القائمة للتشفير والاستيقان والمصممة لحماية الخصوصية غير قابلة للتطبيق بسبب تقييد الموارد داخل بطاقات RFID.

1.II إعدام البطاقة باستخدام كلمة سر

تستغل هذه التقنية، بصفتها الطريقة الأكثر شيوعاً لحماية خصوصية المستعمِل، الحقيقة المتمثلة في أن بطاقة RFID يمكن أن يكون لها مرحلة "إعدام" أو مرحلة "نشيطة". وترسل القارئة، عند اللزوم، أمر "إعدام" يتضمن كلمة سر (من 32 بتة) من أجل إخماد وظيفة البطاقة. وبالرغم من ذلك، فإن إعدام البطاقة يمكن استعماله فقط في بعض التطبيقات، ما دامت وظيفة التعرف الآلي التي تمثل مكمن القوة لتكنولوجيا RFID، لا يمكن استعمالها بعد تنفيذ أمر الإعدام. وعلى سبيل المثال، إذا كانت وظيفة المنتج الحامل لبطاقة RFID ملحقة به معطلة عند الشراء، فإن إرجاعه أو استعادة ثمنه قد يكون مستحيلاً ما دامت سجلات المنتج المعني غير قابلة للاسترداد. وفضلاً عن ذلك، ليست البطاقة القابلة للإعدام آمنة إلى حد كاف لحماية معلومات PII لأنها تحمل فقط كلمة سر بحجم 32 بتة وقد تكون المقدرة الوظيفية للإعدام ضعيفة أمام هجوم رفض الخدمة التي يعدم فيها المهاجم كل البطاقات المحيطة به.

2.II حماية الخصوصية باستخدام التكنولوجيا المادية

1.2.II قفص فارادي

قفص فاراداي هو تكنولوجيا تمنع قارئة RFID غير القانونية من مسح المعلومات المسجلة على البطاقة بالتشويش على إرسال إشارة لا سلكية، وذلك باستخدام محفظة مصنوعة من مادة خاصة تصد الإرسالات الراديوية. ويُستعمَل ملف معدني لصد الإشارة اللاسلكية. ومع ذلك، فإن استعمال قفص فاراداي، وإن كان له تطبيقات مفيدة في بعض المجالات، محدود نسبيًّا، ما دامت وظيفة حماية الخصوصية تُفقَد عند إخراج المنتج من المحفظة.

X.1275(10)_FII.1

الشكل 1.II – محفظة جواز سفر بقفص فارادأي

2.2.II بطاقة الصّد

بطاقة الصد هي تكنولوجيا طورتها شركة RSA عام 2003. وتمنع هذه البطاقة الخاصة تسرب معلومات البطاقة الذي تتسبب فيه محاولة قارئة غير قانونية للتشويش على اتصالات البطاقات المحيطة وذلك بواسطة توليد إشارات لا معنى لها. وعلى سبيل المثال، تتضمن بطاقة RFID بتة خاصة مخصصة بصفتها "عمومية" أو "خاصة". وتُوضَع هذه البتة الخاصة، بالنسبة إلى منتج الإمدادات الطبية الملحق بهذه البطاقة، في الوضع "العمومي" قبل بيع البطاقة ولكن يتم تغييرها إلى الوضع "الخاص" في محل البيع عند الشراء. وعند إدراج منتج الإمدادات الطبية الملحق ببطاقة موضوعة في الوضع "الخاص" داخل محفظة تستخدم بطاقة صد، لا يمكن للآخرين قراءة معلومات البطاقة الموضوعة في الوضع "الخاص" بواسطة بطاقة صد؛ وبذلك تتم حماية خصوصية مشتري المنتج.

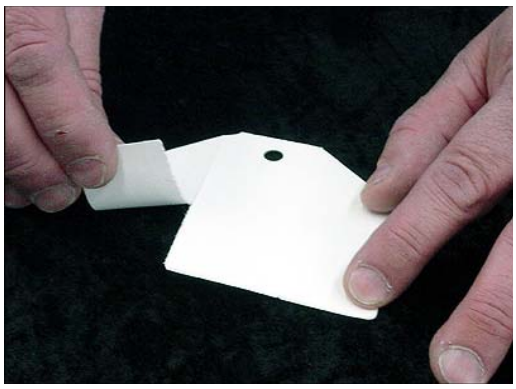
3.2.II التشويش النشيط

يؤثر التشويش النشيط بالسلب على تشغيل كل قارئات RFID الموجودة قريباً من الجهاز، وذلك باستخدام جهاز يبث موجة شديدة للتشويش المقصود. وبهذه الطريقة تمنع هذه التكنولوجيا تسرب المعلومات الشخصية بالصد عن معلومات بطاقة RFID.

ويلاحظ أن بطاقة الصد والتشويش النشط تكنولوجيتان بسيطتان يمكن استعمالهما بسهولة لرفض هجمات الخدمة. كما أنهما حلان محتملان فقط على مستوى المستعمل ولا يمكن دمجهما ضمن الخدمة RFID.

4.2.II البطاقة المقطَّعة

البطاقة المقطعة هي بطاقة طورتها شركة IBM من أجل سد عيوب أمر إعدام البطاقة، بتقصير مسافة اتصالات البطاقة بقطع جزء من خط توصيل الهوائي الموجود داخل البطاقة. ويمكن لهذه التكنولوجيا أن تقلل إلى حد أدنى احتمال انتهاك الخصوصية عن طريق تتبع الموقع عن بعد، وذلك بتقليص مسافة المعلومات إلى حد كبير مع المحافظة على وظيفة تخزين المعلومات دون تغيير.



X.1275(10)_FII.2

الشكل 2.II – بطاقة مقطَّعة

5.2.II الجهاز Zapper المتعلق بالتدمير في التكنولوجيا RFID

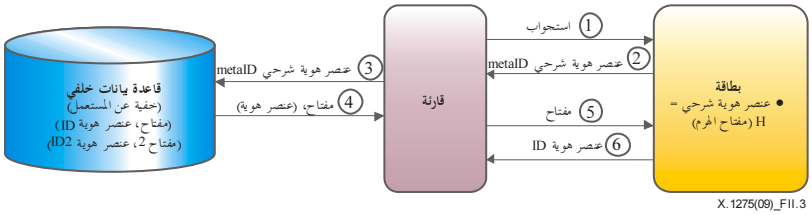
عرض الجهاز Zapper الخاص بالتدمير في التكنولوجيا RFID في مؤتمر شاوس للاتصالات في عام 2005. وهو عبارة عن جهاز كهربائي يمكنه إخماد البطاقات RFID المنفعلة بشكل دائم. وهذا الجهاز مصمم بحيث يتفادى إلحاق الضرر بأي جهاز مُلحق به بطاقة RFID وذلك على النقيض من الطرائق الأخرى مثل التشويش النشط والبطاقة المقطعة.

3.II حماية الخصوصية باستخدام تكنولوجيا التشفير

فيما يلي حلول تستعمل بروتوكولات تشفير بسيطة لتقديم حماية أفضل للأمن والخصوصية على مستوى البطاقة. ولم تصل الحلول المقترحة إلى مرحلة النضج بحيث تستعمل بكفاءة في تطبيقات فعلية، بيد أن هناك الكثير من الأبحاث الأكاديمية الجارية في هذا المجال. حتى وإن كانت غير مطبّقة حالياً، فإن هذه الحلول توفر رؤية جيدة بشأن ماهية الحل المكتمل النضج في المستقبل. ويلاحظ أن هناك فرصة جيدة لأن تلزم هذه البروتوكولات إدخال تغييرات على البروتوكولين الراديويين المقيسين حالياً المعيار [b-ISO/IEC 14443] أو المعيار [b-ISO/IEC 18000]، أو الدراسات الجارية مع EPC Global.

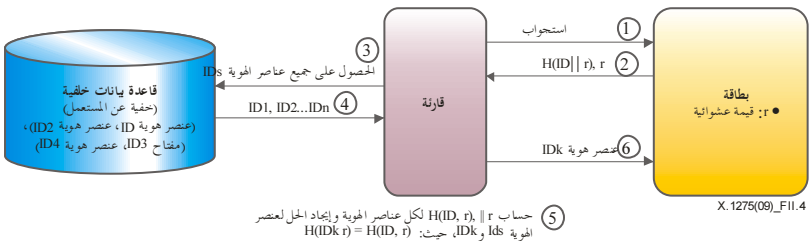
1.3.II قفل الفرم

يُرسِل قفل الفرم، بصفته إحدى الطرق الممثلة لاستخدام تكنولوجيا التشفير، معلومات البطاقة إلى القارئة المرخصة وقاعدة البيانات الخلفية (الخفي عن المستعمِل) فقط على أساس صعوبة حساب دالة معكوسة لدالةٍ فرم باتجاه واحد. ومثلما جاء وصف ذلك بالتفصيل في الشكل 3.II، يُقدَّم فقط عنصر الهوية الشرحي (metaID) استجابةً لطلب قارئة البطاقة، الذي يتم إرساله إلى قارئة بعد التحقق من معلومات الاستيقان التي أحرزتها القارئة قانونيّاً من قاعدة البيانات الخلفية. ومع ذلك، فإن هذه الطريقة تستتبع مشكلة، أي أنه لا يمكن تتبع المستعمِل، ما دام عنصر هوية شرحي ذو قيمة سكونية يمكن استعماله كمعرّف بطاقة.



الشكل 3.II – "قفل" الفرم

وتُعَد تقنية قفل الفرم العشوائي إحدى الطرائق المقترحة لحل مشكلة القدرة على تتبع المستعمِل في التقنية القائمة لقفل الفرم. ومثلما جاء وصف ذلك بالتفصيل في الشكل 4.II، يمكن لهذه التقنية منع التتبُّع بجعل البطاقة تولِّد قيمة مختلفة كلما تم النفاذ إلى معلومات البطاقة، باستخدام مولد أرقام عشوائية بواسطة دالة فرم. وقد اقتُرِحت تقنيات مختلفة أخرى تستند إلى دالة فرم – مثل سلسلة الفرم – بيد أنه حُكِم عليها بأنها غير عملية (انظر المرجع [b-Weis]).

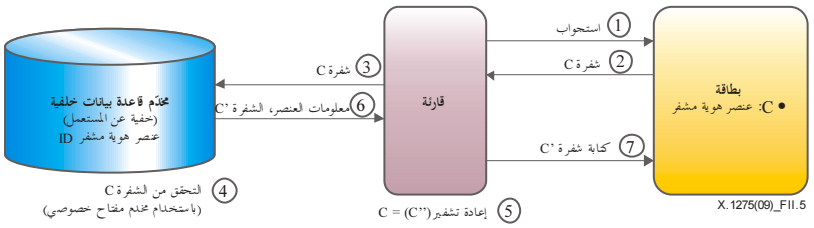


الشكل 4.II – "قفل" فرم يستخدم العشوائية

2.3.II إعادة التشفير

تسمح طريقة إعادة التشفير فقط لقاعدة البيانات الخلفية أو للقارئة التي لها مفتاح عمومي لقاعدة البيانات الخلفية بجمع معلومات البطاقة، ما دامت قاعدة البيانات الخلفية أو القارئة القانونية تشفّر معرّف هوية البطاقة بصورة دورية باستخدام المفتاح العمومي وتحفظ المعلومات المولدة في بطاقة. ويقوم بروتوكول إعادة التشفير على EGamal ويتكون من خطوتين وتولد قاعدة البيانات الخلفية بداية شفرة C باستعمال مفتاحها العمومي مع رقم عشوائي وتخزن الشفرة في بطاقة ويرد وصف للخطوة الثانية بالتفصيل في الشكل 5.II.

ويمكن تطبيق هذه الطريقة على ورقة نقدية ذات قيمة عالية. وما إن تُستعمَل هذه الطريقة حتى يمنع التشفير الدوري تتبع معلومات بطاقة RFID. وبالرغم من ذلك، فإن خطر تسرب المعلومات عن طريق التنصت أثناء إرسال مفتاح عمومي خطر قائم، بما أن هذه العملية تستعمل طريقة تشفير مفتاح عمومي. وبالإضافة إلى ذلك، فإن الطرائق القائمة على تشفير مفتاح عمومي، من قبيل إعادة التشفير، لا يمكن تطبيقها على بطاقة منفعلة زهيدة الثمن باستخدام التكنولوجيا المتاحة حالياً.



الشكل 5.II – إعادة التشفير

ثُبت المراجع

[b-Council of Europe] Council of Europe, "*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*", 1981. http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

[b-CRYPTREC] Telecommunications Advancement Organization of Japan, "*CRYPTREC Report 2002*", March 2003, Information-technology Promotion Agency, Japan.

[b-DSTI/ICCP] "*RFID, OECD Policy Guidance, A Focus on Information Security and Privacy, Applications, Impacts and Country Initiatives*", OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17-18 June 2008.

[b-EC1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 1995. http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[b-EC2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[b-EPIC] Electronic Privacy Information Center, "*Guidelines on Commercial Use of RFID Technology*", July 2004.

[b-E-Zpass] http://www.ezpass.com/static/info/howit.shtml

[b-ICAO] ICAO, Doc 9303, *Machine Readable Travel Documents*, Part 1, Volume 2, 6th edition, 2006.

[b-IPC] Information and Privacy Commissioner/Ontario, "*Privacy Guidelines for RFID information Systems (RFID Privacy Guidelines)* ", June 2006.

[b-Isamu Y] Isamu, Y., Shinichi, S., Akira, I. and Satoshi, I., "*Secure Active RFID Tag System"*, 7th International Conference on Ubiquitous Computing, September 2005.

[b-ISO 22307] ISO 22307:2008, "*Financial services – Privacy impact assessment*", August 2008.

[b-ISO/IEC 14443] ISO/IEC 14443:2008, Identification cards – Contactless integrated circuit cards – Proximity cards.

[b-Japan] MIC (Ministry of Internal Affairs and Communications), METI (Ministry of Economy, Trade and Industry) Government of Japan, "*Guidelines for Privacy Protection with Regard to RFID Tags*", July 2004.

[b-Juels] Juels, A., Rivest, R.L., and Szydlo, M., "*The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*", ACM Conference on Computer and Communications Security, 2003.

[b-Junichiro] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai, "*Enhancing privacy of Universal Re-encryption scheme for RFID tags*", Embedded and Ubiquitous Computing 2004.

[b-Korea] MIC (Ministry of Information and Communication) of Korea, "*RFID Privacy Protection Guideline*", July 2005.

[b-NIST] NIST SP 800-98, "*Guidance for Securing Radio Frequency Identification (RFID) Systems*", September 2007.

[b-OECD] OECD, "*Guideline on the Protection of Privacy and Transborder Flows of Personal Data*", 1980.

[b-Peris-Lopez] Pedro Peris-Lopez *et al*, "*M^2 AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags*", 3rd International Conference on Ubiquitous Intelligence and Computing, September 2006.

[b-PIA Canada] Treasury Board of Canada Secretariat, "*Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*", 2002.
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp

[b-PIA Korea] MIC (Ministry of Information and Communication) of Korea, "*Privacy Impact Assessment Guideline for Private Sector*", December 2005.

[b-Simon L1] Simson, L., Garfinkel, Ari Juels, and Ravi Pappu, "*RFID Privacy: An Overview of Problems and Proposed Solutions*", IEEE Security and Privacy, 2005.

[b-Simon L2] Simson, L., Garfinkel and Beth Rosenberg, "*RFID: Applications, Security, and Privacy*", Addison-Wesley Professional, July 2005.

[b-UNHCR] UN General Assembly, "*Guidelines for the Regulation of Computerized Personal Data Files*", 1990.
http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08, PDF/G9010708-pdf

[b-Weis] Weis S., *et al.*, "*Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*", Security and Pervasive Computing 2003.

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، 2011