الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2740

(2011/01)

السلسلة Y: البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

شبكات الجيل التالي – الأمـــن

متطلبات الأمن بشأن المعاملات المالية المتنقلة عن بُعد في شبكات الجيل التالي (NGN)

التوصيـــة ITU-T Y.2740

الاتحاد الدولي للاتصالات

توصيات السلسلة Y الصادرة عن قطاع تقييس الاتصالات

البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

البنية التحتية العالمية للمعلومات	
اعتبارات عامة	Y.199-Y.100
الخدمات والتطبيقات، والبرمجيات الوسيطة	Y.299-Y.200
الجوانب الخاصة بالشبكات	Y.399-Y.300
السطوح البينية والبروتوكولات	Y.499-Y.400
الترقيم والعنونة والتسمية	Y.599-Y.500
الإدارة والتشغيل والصيانة	Y.699-Y.600
الأمن	Y.799-Y.700
مستويات الأداء	Y.899-Y.800
جوانب متعلقة ببروتوكول الإنترنت	
اعتبارات عامة	Y.1099-Y.1000
الخدمات والتطبيقات	Y.1199-Y.1100
المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد	Y.1299-Y.1200
النقل	Y.1399-Y.1300
التشغيل البيني	Y.1499-Y.1400
نوعية الخدمة وأداء الشبكة	Y.1599-Y.1500
التشوير	Y.1699-Y.1600
الإدارة والتشغيل والصيانة	Y.1799-Y.1700
الترسيم	Y.1899-Y.1800
تلفزيون بروتوكول الإنترنت عبر شبكات الجيل التالي	Y.1999-Y.1900
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099-Y.2000
نوعية الخدمة والأداء	Y.2199-Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249-Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2299-Y.2250
الترقيم والتسمية والعنونة	Y.2399-Y.2300
إدارة الشبكة	Y.2499-Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599-Y.2500
الأمـــن	**Y.2799-Y.2700**
التنقلية المعممة	Y.2899-Y.2800
البيئة المفتوحة عالية الجودة	Y.2999-Y.2900
شبكات المستقبل	Y.3099-Y.3000

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

التوصيـــة ITU-T Y.2740

متطلبات الأمن بشأن المعاملات المالية المتنقلة عن بُعد في شبكات الجيل التالي (NGN)

الملخص

أنشئت في السنوات القليلة الماضية، مجموعة كبيرة ومتنوعة من شبكات الدفع عن بُعد باستخدام الشبكات المتنقلة. وعلى الرغم من تنفيذ النهج المختلفة، فإنها تفتقر إلى الأمن في كثير من الأحيان. وفي الوقت نفسه، تشهد شبكات الاتصالات بما في ذلك الشبكات المتنقلة، تغيرات كبيرة مما يجعلها تتطور إلى شبكات الجيل التالي (NGN).

تحدد التوصية ITU-T Y.2740 نهجاً لتطوير أمن الشبكات من أجل التجارة المتنقلة والخدمات المصرفية المتنقلة في شبكات الجيل التالي (NGN). وتصف متطلبات الأمن للتجارة المتنقلة والأنظمة المصرفية المتنقلة استناداً إلى مستويات الأمن الأربعة المحددة. وتلخص المخاطر المحتملة في التجارة المتنقلة والأنظمة المصرفية المتنقلة وتحدد الوسائل الكفيلة بالحد من المخاطر.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T Y.2740	2011.01.28	13

المصطلحات الرئيسية

الخدمات المصرفية المتنقلة، التجارة المتنقلة، الدفع المتنقل، الدفع عن بُعد، الأمن.

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/.

المحتـــويات

الصفحة

التوصيـــة ITU-T Y.2740

متطلبات الأمن بشأن المعاملات المالية المتنقلة عن بُعد في شبكات الجيل التالي (NGN)

1 مجال التطبيق

تصف هذه التوصية مخاطر الأمن المرتبطة بالمعاملات المالية المتنقلة عن بعد المدعومة بخدمات تطبيقات شبكات الجيل التالي والتخفيف من حدة المخاطر والتدابير المضادة القائمة على مستويات الأمن الأربعة. وتحدد هذه التوصية أيضاً الحد الأدنى من متطلبات الأمن لحماية خصوصية البيانات الشخصية للأفراد فيما يتعلق بالمعاملات المالية المتنقلة عن بُعد.

2 المراجع

تشتمل التوصيات والمراجع الأخرى التالية لقطاع تقييس الاتصالات على أحكام تشكّل، من خلال الإشارة إليها في هذا النص، أحكاماً في هذه التوصية. وكانت الطبعات المشار إليها صالحة وقت نشر هذه التوصية. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات سارية الصلاحية. والإشارة إلى أي وثيقة داخل هذه التوصية لا يعطي هذه الوثيقة في حد ذاتها وضع التوصية.

[ITU-T X.800] التوصية ITU-X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة لتطبيقات اللجنة الاستشارية الدولية للبرق والهاتف.*

[ITU-T X.805] التوصية ITU-T X.805 (2003)، *معمارية الأمن المتعلقة بالأنظمة التي توفر الاتصالات من طرف-إلى-طرف.*

[ITU-T Y.2720] التوصية ITU-T Y.2720 (2009)، *إطار إدارة الهوية في شبكات الجيل التالي.*

[ITU-T Y.2741] التوصية ITU-T Y.2741 (2011)، *معمارية المعاملات المالية المتنقلة الآمنة في شبكات الجيل التالي.*

3 التعاريف

1.3 مصطلحات معرَّفة في أماكن أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في أماكن أخرى:

1.1.3 مراقبة النفاذ (access control) [ITU-T X.800]: منع الاستعمال غير المصرح لمورد ما، بما في ذلك منع استعمال مورد بطريقة غير مصرح بها.

2.1.3 التطبيق (application) [ITU-T Y.2741]: تطبيق خاص لخدمة مصرفية متنقلة أو تجارة متنقلة يتم تحميلها على الأجهزة المحمولة للمستعمل.

3.1.3 الاستيقان (authentication) [ITU-T X.800]: انظر الاستيقان من مصدر البيانات والاستيقان من الكيان الند.

ملاحظة – لا يستخدم مصطلح "استيقان" في هذه التوصية فيما يتعلق بسلامة البيانات، ويستخدم المصطلح "سلامة البيانات" بدلاً من ذلك.

4.1.3 التيسر (availability) [ITU-T X.800]: خاصية إمكانية النفاذ وإمكانية الاستعمال بناءً على طلب من كيان مخول.

5.1.3 الزبون (client) [ITU-T Y.2741]: فرد أو شخصية اعتبارية وقعت على اتفاق تعاقدي بشأن استعمال خدمات الاتصالات ونظام التجارة المتنقلة.

6.1.3 السرية (confidentiality) [ITU-T X.800]: خاصية تفيد عدم إتاحة المعلومات أو الإفصاح عنها لأفراد أو كيانات أو عمليات غير مخولة.

7.1.3 سلامة البيانات (data integrity) [ITU-T X.800]: خاصية تفيد أن البيانات لم تُغير أو تتعرض للإتلاف بطريقة غير مصرح بها.

8.1.3 الاستيقان من مصدر البيانات (data origin authentication) [ITU-T X.800]: التأكد من أن يكون مصدر البيانات المستلمة كما أُعلن عنه.

9.1.3 نظام الدفع المتنقل (mobile payment system) [ITU-T Y.2741]: نظام الخدمات المصرفية المتنقلة و/أو التجارة المتنقلة.

10.1.3 شبكة الجيل التالي (next generation network) [ITU-T Y.2001]: شبكة تقوم على أساس الرزمة ويمكنها تقديم خدمات الاتصالات ويمكنها الاستفادة من النطاق العريض المتعدد وتكنولوجيات النقل التي تتسم بنوعية الخدمة وتكون فيها الوظائف المتصلة بالخدمة مستقلة عن التكنولوجيات الأساسية المتصلة بالنقل. وتتيح هذه الشبكة نفاذ المستعملين دون عوائق إلى الشبكات ومقدمي الخدمات المتنافسين و/أو الخدمات التي يختارونها. وهي تدعم التنقلية العامة التي تسمح بتقديم الخدمات إلى المستعملين بشكل متسق في كل مكان.

11.1.3 الخصوصية (privacy) [ITU-T X.800]: حق الأفراد في التحكم أو التصرف في المعلومات التي يمكن تجميعها وتخزينها والأشخاص الذين يمكنهم كشف هذه المعلومات أو يمكن أن تكشف لهم.

ملاحظة – نظراً لأن هذا المصطلح يتعلق بحق من حقوق الأفراد، لا يمكن أن يكون على درجة عالية من الدقة وينبغي استعماله لأغراض الأمن فقط.

12.1.3 الرفض (repudiation) [ITU-T X.800]: إنكار أحد الكيانات المشاركة في الاتصال أنه قد شارك في الاتصال بالكامل أو في جزء منه.

13.1.3 الأبعاد الأمنية (security dimension) [ITU-T X.805]: مجموعة تدابير أمنية مكرسة لمعالجة جانب خاص من أمن الشبكة.

14.1.3 طبقة الأمن (security layer) [ITU-T X.805]: تراتب أجهزة الشبكة ومجموعات المرافق.

15.1.3 سويات الأمن (security planes) [ITU-T X.805]: أحد أنماط نشاط الشبكة المحمي بأبعاد الأمن.

2.3 مصطلحات معرفة في هذه التوصية

تستعمل هذه التوصية المصطلح التالي:

1.2.3 مستوى الأمن (security level): مواصفات أمن النظام التي تحدد فعالية الحماية من المخاطر.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

GSM النظام العالمي للاتصالات المتنقلة *(Global System for Mobile Communications)*

MPS نظام الدفع المتنقل *(Mobile Payment System)*

MSISDN رقم ISDN الدولي للمحطة المتنقلة *(Mobile Station International ISDN Number)*

NGN شبكات الجيل التالي *(Next Generation Network)*

PA-DSS معيار أمن بيانات تطبيق الدفع *(Payment Application Data Security Standard)*

PCI DSS معيار أمن بيانات قطاع بطاقات الدفع *(Payment Card Industry Data Security Standard)*

5 الاصطلاحات

لا يوجد.

6 اعتبارات الأمن المتعلقة بالأنظمة المصرفية المتنقلة والتجارة المتنقلة في شبكات الجيل التالي

يقوم أمن نظام الدفع المتنقل في شبكات الجيل التالي على معمارية النظام MPS وأدوار المشاركين في هذا النظام المحددة في [ITU-T Y.2741]، "*معمارية المعاملات المالية المتنقلة الآمنة في شبكات الجيل التالي*" وتحليل المخاطر التي يتعرض لها المشاركون في النظام MPS الوارد وصفه أدناه.

1.6 المخاطر الأساسية في المعاملات المصرفية المتنقلة عن بعد

لا تتناول هذه الفقرة العوامل التي تتأثر بها المخاطر الصناعية الجديدة التي يتعرض لها المشاركون على الصعيد العالمي عند تنفيذ نظام الدفع المتنقل – مخاطر النظام والمخاطر الاستراتيجية، والقطرية والمخاطر المتعلقة بالسيادة، والسوق والفوائد والسيولة والمخاطر القانونية والمخاطر المتعلقة بالسمعة، إلخ. بل تتناول هذه الفقرة المخاطر المتعلقة بالمعلومات التي قد تنشأ مباشرة أثناء الدفع المتنقل عن بُعد والتي تقتضي اتخاذ قرارات بشأن قضايا الأمن للتقليل من هذه المخاطر:

- خطر فقدان السرية مما يعني النفاذ غير المخول إلى معلومات سرية؛
- خطر انتهاك سلامة البيانات المتمثل في تشويه المعلومات عند نقل البيانات أو معالجتها؛
- خطر تزوير الوثائق الإلكترونية (خطر الاستيقان) والذي ينشأ عند إصدار وثائق إلكترونية من جانب مشاركين غير مخولين؛
- خطر الرفض المتمثل في التملص من مسؤولية إصدار وثيقة إلكترونية معينة؛
- خطر إتلاف المعلومات سواء عن قصد أو عن طريق الإهمال؛
- خطر المعاملات المتمثل في فشل إنهاء أو استكمال معاملة (بسبب سوء جودة الإرسال مثلاً).

2.6 أهداف الأمن

تحسين أمن الدفع المتنقل والحد من المخاطر التي يتعرض لها المشاركون، يجب أن يضمن الحل تحقيق الأهداف التالية:

- الحد من إمكانية اعتراض المعلومات الشخصية أو المالية أثناء المعاملة؛
- الحد من إمكانية استرجاع معلومات شخصية أو مالية من قواعد البيانات؛
- الحد من إمكانية استبدال أو تشويه معلومات شخصية أو مالية أثناء المعاملة؛
- الحد من إمكانية استعمال هذا الحل من جانب أشخاص غير مخولين وأشخاص يحاولون التنكر من خلال تنفيذ استيقان وحيد؛
- الحد من إمكانية استعمال معلومات "مختلسة" في الحل؛
- توفير الظروف اللازمة ليستحيل لبادئ معاملة أو لمشارك إنكار أعماله بعد القيام بها؛
- ضمان الامتثال للحقوق والواجبات القانونية لجميع المشاركين في المعاملة؛
- ضمان إنهاء المعاملة.

3.6 مستويات الأمن والوسائل اللازمة لدعمها

تصف هذه التوصية أربعة مستويات للأمن فيما يخص نظام الدفع المتنقل بناءً على تحليل المخاطر التي يتعرض لها المشاركون في هذا النظام.

ويُحدد مستوى أمن النظام بمجموعة عمليات تنفيذ الأبعاد الأمنية (انظر الجدول 1). ومن ثم ينبغي أن يكون للمستوى الرابع (أعلى مستوى) لنظام الأمن أعلى درجة تنفيذ للأبعاد الأمنية. ومع ذلك، تُوحد متطلبات عدد من الأبعاد الأمنية بالنسبة إلى جميع مستويات الأمن.

وينبغي للأطراف التي تستخدم نظام الدفع المتنقل أن تكون على علم بمستوى أمن النظام وبالمخاطر التي ينطوي عليها النظام.

ويحدد الطرف الذي يتعرض للمخاطر مستوى الأمن المقبول لخطر معين أو لمكون معين للنظام.

ويمكن للأطراف أيضاً أن تقلل من مخاطر استعمال نظام الدفع المتنقل باستعمال تدابير تشغيلية يمكن أن تتمثل في الحد من عدد المعاملات أو قيمتها المالية، وتوفير الخدمة للمستعملين مع مستوى عالٍ من الثقة، وما إلى ذلك.

يعرّف العميل للنظام عن طريق استعمال معرف الهوية العمومي للشبكة NGN (الرقم MSISDN من أجل شبكات النظام العالمي للاتصالات المتنقلة، مثلاً).

1.3.6 تنفيذ الأبعاد الأمنية فيما يتعلق بجميع مستويات الأمن

يكون كل مشارك في النظام مسؤولاً عن ضمان أمن النظام ويتحقق ذلك بواسطة الوسائل المادية والإدارية لضمان الأمن عند نقل البيانات ومعالجتها وتخزينها. ويجب على المشاركين ضمان تطبيق معايير القطاع المتصلة بضمان أمن المعلومات (مثلاً، [b-PCI DSS] و[b-PA-DSS] وما إلى ذلك).

وترد أدناه ثمانية أبعاد أمنية [ITU-T X.805] تحدد مستويات الأمن لنظام الدفع المتنقل. وجميع المشاركين في النظام ملزمون بتنفيذ الأبعاد الأمنية المتعلقة بالمعلومات المتضمنة في تبادل البيانات.

1) مراقبة النفاذ: يجب ألا يُمنح النفاذ إلى كل عنصر في نظام الدفع المتنقل إلا لمن يحدده موظفو الأمن أو مستوى النفاذ للمستعمل النهائي. ويُطبق هذا الشرط على جميع مستويات الأمن.

2) الاستيقان: يجب ضمان استيقان الهوية المدّعاة للكيانات المشاركة. ويمثل ذلك أحد العوامل الرئيسية للتقليل من مخاطر التملص من مسؤولية التأليف. ونظراً لإمكانيات التنفيذ التنظيمية والتقنية الواسعة، يحدد كل مستوى من مستويات الأمن حداً أدنى من المتطلبات اللازمة لآلية الاستيقان.

وهناك ثلاثة عوامل للاستيقان من العميل (المستعمل):

- يستعمل العميل بعض المعلومات التي لا يمكن لأحد غيره معرفتها مثل كلمة السر اللازمة للنفاذ (شيء تعرفه)؛
- يملك العميل شيئاً يكون متاحاً له فقط ويقوم ببعض الإجراءات بصورة فريدة مثلاً إصدار توقيع إلكتروني أو شفرة الاستيقان من الرسالة (شيء تملكه)؛
- يستعمل العميل بياناته البيومترية (شيء تمثله).

3) عدم الرفض: توفير الوسائل اللازمة لمنع فرد أو كيان من إنكار قيامه بإجراء معين (مثلاً إرسال رسالة أو تحويلها أو استلامها). ولذلك، تخضع جميع الإجراءات التي يقوم بها الموظفون أو المستعمل النهائي للنظام للتسجيل الإلزامي. ويجب أن تكون سجلات الأحداث قائمة على مواكبة التغيرات وأن تتضمن جميع الإجراءات التي يقوم بها جميع المستعملين. ويتحقق الامتثال للمتطلبات بواسطة وسائل وآليات الاستيقان المقبولة المنصوص عليها قانوناً والتي يتم الالتزام بها. ويسري هذا الشرط على جميع مستويات الأمن.

4) سرية البيانات: حماية البيانات المستخدمة في النظام من الكشف لغير المخولين ومن التغيير. وتتحدد متطلبات السرية حسب درجة أهمية بيانات النظام. ويحدد كل مستوى من مستويات الأمن بعض الوسائل لضمان السرية ويفرض قيوداً حسب مستوى أهمية بيانات النظام.

5) سلامة الاتصالات: يشمل التسليم المضمون لتتابع الرسائل في كلا الاتجاهين (من وإلى المرسل إليه) إنهاء المعاملة (باستعمال البروتوكولات التي تضمن إنهاء المعاملة) وحماية المعلومات من الكشف لغير المخولين أثناء نقل البيانات عبر قنوات الاتصال. وينطبق هذا الشرط على جميع مستويات الأمن.

6) سلامة البيانات: ضمان صحة البيانات ودقتها وسلامتها عن طريق حمايتها من التعديل والحذف والاستحداث والاستنساخ من قبل غير المخولين فضلاً عن الكشف عن هذه الأنشطة غير المخولة. ويكون إنهاء المعاملة المنطقي مضموناً عند استيفاء بعض الشروط، التي يتم تنفيذها على مستوى التطبيق. ويحدد كل مستوى من مستويات الأمن بعض الآليات الخاصة بضمان سلامة البيانات. ويمكن تحقيق ضمان سلامة البيانات بواسطة سرية البيانات ومراقبة النفاذ.

7) التيسر: يضمن حفظ النفاذ المخول إلى بيانات نظام الدفع المتنقل وخدماته. وينطبق هذا الشرط على جميع مستويات الأمن، ويجب على موردي الخدمة بذل قصارى الجهود للوفاء به بأفضل طريقة.

8) الخصوصية: تضمن الخصوصية أمن المعلومات المتضمنة في عمليات تبادل البيانات من قبل المشاركين في النظام والمخزنة فيه. ويجب أن يُستعمل في الحل أدنى عدد ممكن من البيانات اللازمة لتشغيل النظام. ويجب أن يمنع المشاركون في النظام حيازة بيانات ونقلها لغير المخولين. ويجب أن يكفل النظام الامتثال لمعايير القطاع المالي.

الأبعاد الأمنية التي تنفذ بالتساوي على جميع مستويات الأمن هي كالآتي:

- مراقبة النفاذ؛
- عدم الرفض؛
- أمن الاتصالات؛
- التيسر.

أبعاد الأمن التالية التي تُطبق بدرجات متفاوتة على مستويات الأمن المختلفة:

- الاستيقان؛
- سرية البيانات؛
- سلامة البيانات؛
- الخصوصية.

2.3.6 المستوى 1 للأمن

يمكن أن يعتمد نظام الدفع المتنقل على الاستيقان من العميل الذي يوفره مشغل شبكة الجيل التالي.

وتُكفل سرية البيانات وسلامتها من خلال بيئة نقل البيانات (أمن الاتصالات)، وعند تخزينها ومعالجتها من خلال آلية تخزين البيانات إضافة إلى وسائل التحكم في النفاذ إلى النظام.

وتُكفل الخصوصية من خلال عدم إدراج بيانات حساسة في الرسالة التي يجري نقلها وكذلك من خلال تنفيذ الآليات المطلوبة لتخزين البيانات ووسائل التحكم في النفاذ إلى النظام. ويجب ألا تحتوي مكونات النظام على أي إمكانات كامنة لحيازة البيانات ونقلها لغير المخولين.

3.3.6 المستوى 2 للأمن

يمكن تنفيذ الاستيقان عند استعمال خدمات النظام باستخدام عامل استيقان واحد فقط ومن ثم يمكن تنفيذه بدون تطبيق بروتوكولات التجفير.

وتستعمل كلمة السر ذات الاستعمال لمرة واحدة من أجل الاستيقان. وتولد هذه الكلمة بواسطة أذنات مختلفة (جهاز إنتاج كلمة سر ذات الاستعمال لمرة واحدة بعامل وحيد، جهاز تجفير بعامل وحيد، وغير ذلك).

وتُكفل سرية البيانات وسلامتها وخصوصيتها بطريقة مماثلة للمستوى 1.

4.3.6 المستوى 3 للأمن

يجب استعمال استيقان متعدد العوامل للعميل من أجل النفاذ إلى خدمات النظام.

ويجب أن يستعمل النظام أكثر من عامل واحد من عوامل الاستيقان من العميل.

ويجب ضمان سرية البيانات وسلامتها وخصوصيتها عند نقل الرسائل باستعمال تجفير إضافي للرسالة إلى جانب بروتوكولات نقل البيانات التي تضمن أمن البيانات التي ينقلها المشاركون في المعاملة (بما في ذلك التحقق من سلامة البيانات)؛ وتُكفل سرية البيانات وسلامتها وخصوصيتها عند تخزينها ومعالجتها بواسطة الآليات الإضافية للتجفير والتقنيع إلى جانب توزيع النفاذ بشكل واضح وفقاً للامتيازات والتصاريح.

وللوفاء بمتطلبات الأمن في هذا المستوى، يجب أن يستعمل النظام تطبيقات برمجية خاصة يتم تحميلها على الأجهزة المتنقلة للعميل. وتسمح هذه التطبيقات بتنفيذ استيقان ذي عاملين مع ضمان تجفير البيانات وفك تجفيرها.

ويجب على كل عملية استيقان أن تلزم بإدخال كلمة سر أو بيانات تفعيل أخرى لتنشيط مفتاح الاستيقان ويجب أن تُمحى النسخة غير المجفرة لمفتاح الاستيقان بعد كل عملية استيقان. (علامة تجفير برمجية متعددة العوامل).

ويجب على كل المشاركين في معاملة MPS استعمال الوسائل الأمنية التي تؤمن النظام ضد الاقتحام. وفي حلول المستوى 3، يجب ضمان أمن البيانات المنقولة عبر قنوات الاتصالات عن طريق أسلوب تجفير قوي. وتعتمد قوة أسلوب التجفير على مفتاح التجفير المستخدم. وينبغي أن يفي حجم المفتاح الفعّال بالحد الأدنى لحجم المفتاح الذي يضمن قوته النسبية.

5.3.6 المستوى 4 للأمن

يمثل هذا المستوى أعلى مستوى لأمن النظام. وللوفاء بمتطلبات الأمن على هذا المستوى، يستعمل النظام وحدات أمن برمجية مركبة في الأجهزة المتنقلة للعميل. وتنفذ هذه الوحدات استيقاناً ثنائي العامل وتضمن تجفير البيانات المنقولة وفك تجفيرها. ويجب على كل عملية استيقان أن تلزم بإدخال كلمة سر أو بيانات تفعيل أخرى لتنشيط مفتاح الاستيقان وتُمحى النسخة غير المجفرة لمفتاح الاستيقان بعد كل عملية استيقان. (علامة تجفير في صورة عتاد متعددة العوامل). وتطبق خوارزميات التجفير التناظرية واللاتناظرية على تجفير الرسائل.

وينبغي أن يقابل تنفيذ الأبعاد الأمنية الأخرى المستوى 3 على نحو تام.

الجدول 1 – العلاقة بين مستويات الأمن وتنفيذ الأبعاد الأمنية

<table>
<tr><th rowspan="2">الأبعاد الأمنية</th><th colspan="4">مستوى الأمن</th></tr>
<tr><th>المستوى 1</th><th>المستوى 2</th><th>المستوى 3</th><th>المستوى 4</th></tr>
<tr><td>مراقبة النفاذ</td><td colspan="4">يُمنح النفاذ إلى كل عنصر في النظام لموظفي النظام المخولين فقط. وينبغي السماح بتنشيط التطبيقات الخاصة التي يتم تحميلها على الأجهزة المتنقلة للعملاء المخولين فقط.</td></tr>
<tr><td>الاستيقان</td><td>يُكفل الاستيقان في النظام بواسطة بيئة نقل بيانات شبكة الجيل التالي</td><td>استيقان أحادي العامل عند استعمال خدمات النظام</td><td>استيقان متعدد العوامل عند استعمال خدمات النظام</td><td>اشتراك مادي في الخدمات حيث تستعمل البيانات الشخصية مع تعرف الهوية الإجباري.
استيقان متعدد العوامل عند استعمال خدمات النظام. استعمال إجباري لوحدة تجفير في صورة عتاد.</td></tr>
<tr><td>عدم الرفض</td><td colspan="4">تضمن وسائل وآليات الاستيقان المقبولة المنصوص عليها قانوناً أو المدرجة في عقود قانونية صريحة وضمنية متبادلة استحالة أن يُنكر مشارك أو مبادر الأعمال التي قام بها. ويلزم تسجيل جميع أعمال الموظفين والمستعملين النهائيين للنظام. ويجب أن تكون سجلات الأحداث مواكبة للتغيرات وأن تتضمن جميع الإجراءات التي يقوم بها المستعملون.</td></tr>
<tr><td>سرية البيانات</td><td colspan="2" rowspan="2">تُكفل سرية البيانات أثناء نقلها بواسطة بيئة نقل البيانات (أمن الاتصالات) وآلية تخزين البيانات بالإضافة إلى وسائل التحكم في النفاذ إلى النظام – عند نقل البيانات ومعالجتها.</td><td rowspan="3">أثناء نقل البيانات، تُكفل سرية البيانات بالتجفير الإضافي للرسالة إلى جانب بروتوكولات نقل البيانات التي تضمن أمن البيانات التي ينقلها المشاركون في المعاملة (بما في ذلك التحقق من سلامة البيانات). وأثناء تخزين البيانات ومعالجتها، تُكفل سرية البيانات وسلامتها وخصوصيتها بواسطة الآليات الإضافية للتجفير والتقنيع وتوزيع النفاذ بشكل جيد وفقاً للامتيازات والتصاريح.</td><td rowspan="3">تنفيذ متطلبات المستوى 3 مع الاستعمال الإجباري للتجفير باستخدام وحدة عتاد ووسائل أمن البيانات في جانب العميل (وحدة التجفير المادية)</td></tr>
<tr><td>سلامة البيانات</td></tr>
<tr><td>الخصوصية</td><td colspan="2">تكون الخصوصية مضمونة بانعدام بيانات حساسة في الرسالة التي يجري نقلها وكذلك من خلال تنفيذ الآليات المطلوبة لتخزين البيانات ومرافق مراقبة النفاذ للنظام.
وينبغي ألا تتيح مكونات النظام إمكانية مستترة لحيازة بيانات غير مصرح بها ونقلها.</td></tr>
<tr><td>أمن الاتصالات</td><td colspan="4">يجب ضمان تسليم الرسالة إلى المرسل إليه بالإضافة إلى التأمين ضد كشف البيانات لغير المخولين أثناء نقل البيانات عبر قنوات الاتصال. ويضمن ذلك موردو الشبكة NGN.</td></tr>
<tr><td>التيسر</td><td colspan="4">يضمن عدم رفض النفاذ للمخولين إلى بيانات وخدمات النظام. ويكفل هذا التيسر موردو الشبكة NGN وموردو خدمات نظام الدفع المتنقل.</td></tr>
</table>

بيبليوغرافيـــا

[b-ITU-T Y.2001] التوصية ITU-Y.2001 (2004)، *نظرة عامة على شبكات الجيل التالي*.

[b-PA-DSS] Payment Card Industry (PCI)، *معيار أمن بيانات تطبيق الدفع. شروط وإجراءات تقييم الأمن*، النسخة 2.0، أكتوبر 2010.

[b-PCI DSS] Payment Card Industry (PCI)، *معيار أمن البيانات، شروط وإجراءات تقييم الأمن*، النسخة 2.0، أكتوبر 2010.

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