الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1365

(2020/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن إنترنت الأشياء (IoT)

منهجية أمنية من أجل استخدام التجفير القائم على الهوية لدعم خدمات إنترنت الأشياء (IoT) على شبكات الاتصالات

التوصية ITU-T X.1365

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
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 (1)	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 (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	**X.1369–X.1360**
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن سجل الحسابات الموزع	X.1449–X.1430
البروتوكول الأمني (2)	X.1459–X.1450
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	X.1729–X.1700

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

التوصية ITU-T X.1365

منهجية أمنية من أجل استخدام التجفير القائم على الهوية لدعم خدمات إنترنت الأشياء (IoT) على شبكات الاتصالات

ملخص

توفر التوصية ITU-T X.1365 منهجية أمنية من أجل استخدام تكنولوجيا المفاتيح العمومية للتجفير القائم على الهوية (IBC) لدعم خدمات إنترنت الأشياء (IoT) على شبكات الاتصالات بما في ذلك آليات إدارة الهوية، ومعمارية إدارة المفاتيح، وعمليات إدارة المفاتيح، والاستيقان.

وتشمل المنهجية الأمنية التقليدية القائمة على الشهادات عمليات ثقيلة العبء لإدارة المفاتيح، بما في ذلك إصدار الشهادات والاستعلام عنها وإبطالها. وتواجه هذه الأنظمة صعوبة كبيرة في مواكبة الأعداد المتزايدة من الأجهزة الموصولة بإنترنت الأشياء مع الحفاظ على الأداء اللائق.

وتُعد تكنولوجيا التجفير القائم على الهوية منهجية أمنية أخرى تستخدم الهوية الخاصة بالكيان المعني كمفتاح عمومي. ومن الخصائص الضرورية لإنترنت الأشياء أن يكون لكل شيء معرِّف هوية (ID) فريد. وباستخدام معرِّفات الهوية هذه كمفاتيح عمومية، لن تكون هناك حاجة للشهادات. ونتيجة لذلك، يستخدم الحل الأمني الذي يعتمد التجفير القائم على الهوية إدارة المفاتيح بشكل أبسط ويُمكّن السلطات الموزعة من التحكم بأجهزتها ومقاييسها على نحو جيد لكل من النقاط الطرفية والأجهزة المتنوعة ذات الأعداد الكبيرة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1365	2020-03-26	17	11.1002/1000/14089

مصطلحات أساسية

إنترنت الأشياء، IBC، التجفير القائم على الهوية، منهجية أمنية، أمن بيانات المستعمل.

* للنفاذ إلى التوصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة 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 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

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

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

جدول المحتويات

الصفحة

الصفحة

منهجية أمنية من أجل استخدام التجفير القائم على الهوية لدعم خدمات إنترنت الأشياء (IoT) على شبكات الاتصالات

1 مجال التطبيق

تحدد هذه التوصية منهجية أمنية من أجل استخدام تكنولوجيا التجفير القائم على الهوية (IBC) لدعم خدمات إنترنت الأشياء (IoT) على شبكات الاتصالات. وتشتمل هذه المنهجية الأمنية على آليات لتحديد الأجهزة، وإصدار المفاتيح الخاصة، والبحث عن المعلمات العمومية، وبروتوكولات الاستيقان.

ملاحظة – لا تقتصر هذه المنهجية على خدمة إنترنت الأشياء، بل يمكن أن تستخدمها أيضاً خدمات 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 للمراجَعة، يُشجع جميع مستعملي هذه التوصية على بحث إمكانية تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[IETF RFC 4764] IETF RFC 4764 (2007), *The EAP-PSK protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method*.

[IETF RFC 5091] IETF RFC 5091 (2007), *Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems*.

[IETF RFC 5216] IETF RFC 5216 (2008), *The EAP-TLS Authentication Protocol*.

[IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[IETF RFC 5408] IETF RFC 5408 (2009), *Identity-Based Encryption Architecture and Supporting Data Structures*.

[IETF RFC 5480] IETF RFC 5480 (2009), *Elliptic Curve Cryptography Subject Public Key Information*.

[IETF RFC 5958] IETF RFC 5958(2010), *Asymmetric Key Packages*.

[IETF RFC 6507] IETF RFC 6507 (2012), *Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)*.

[IETF RFC 6508] IETF RFC 6508 (2012), *Sakai–Kasahara Key Encryption (SAKKE)*.

[IETF RFC 6960] IETF RFC 6960 (2013), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

[IETF RFC 7250] IETF RFC 7250 (2014), *Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*.

[IETF RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3*.

[ISO/IEC 11770-3] ISO/IEC 11770-3:2015, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*.

[ISO/IEC 14888-3] ISO/IEC 14888-3:2018, *IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*.

[ISO/IEC 18033-5] ISO/IEC 18033-5:2015, *Information technology – Security techniques – Encryption algorithms – Part 5: Identity-based ciphers*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 مورد الهوية (identity provider) [b-ITU-T Y.2720]: كيان يقوم باستحداث معلومات هوية موثوقة للكيانات الأخرى مع الحفاظ عليها وإدارتها (وتضم هذه الكيانات الأخرى المستعملين/المشتركين والمنظمات والأجهزة) ويقدم خدمات خاصة بالهوية تقوم على الثقة والأعمال التجارية والأشكال الأخرى من العلاقات.

2.1.3 معرِّف الهوية (identifier) (ID) [b-ITU-T E.101]: سلسلة من الأرقام والسمات والرموز المستعملة لكي تعرف بشكل منفرد هوية مشترك أو مستعمل أو عنصر شبكة أو وظيفة أو كيان من كيانات الشبكة أو خدمة أو تطبيق. ويمكن استعمال معرِّفات الهوية لأغراض التسجيل أو التخويل. وقد تكون هذه المعرّفات عامة لجميع الشبكات أو خاصة لشبكة معينة (لا تُكشف معرِّفات الهوية الخاصة لأطراف ثالثة).

3.1.3 المفتاح العمومي الرئيسي (master public key) (MPK) [ISO/IEC 18033-5]: القيمة العمومية التي يحددها بشكل فريد مفتاح السر الرئيسي المقابل.

4.1.3 مفتاح السر الرئيسي (master secret key) (MSK) [ISO/IEC 18033-5]: القيمة السرية التي يستخدمها مولّد المفاتيح الخاصة لحساب المفاتيح الخاصة لأي خوارزمية تجفير قائم على الهوية.

5.1.3 مولّد المفاتيح الخاصة (private key generator) (PKG) [ISO/IEC 18033-5]: كيان أو وظيفة تولّد مجموعة من المفاتيح الخاصة.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرّف هذه التوصية المصطلح التالي:

1.2.3 ميدان الهوية (identity domain): مجموعة من الكيانات التي تتقاسم مجموعة المعلمات العمومية وقواعد تسمية الهوية نفسها.

2.2.3 معلمة عمومية (public parameter): معلمة من المعلمات المتعلقة بحساب التجفير، بما في ذلك اختيار مخطط تجفير أو وظيفة تجفير معينة من عائلة من مخططات أو وظائف التجفير، أو من عائلة من المساحات الرياضية والمفتاح العمومي الرئيسي.

3.2.3 مخدم معلمات عمومية (public parameter server): كيان يوفر معلمات عمومية عند الطلب.

4.2.3 وحدة أمنية نمطية (security module) (SecM): جزء من برمجيات أو عتاد أو تركيبة من البرمجيات والعتاد تنفذ بشكل آليات التجفير وتوفر الخدمات الأمنية بصورة مؤمنة.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

4G الجيل الرابع *(fourth Generation)*

5G الجيل الخامس *(fifth Generation)*

AuC مركز الاستيقان *(Authentication Centre)*

AGW بوابة التجميع *(Aggregate Gateway)*

AK مفتاح الاستيقان *(Authentication Key)*

AKA اتفاق المفاتيح المستيقنة *(Authenticated Key Agreement)*

AN عقدة النفاذ *(Access Node)*

AS نظام النفاذ *(Access System)*

ASN.1 ترميز قواعد التركيب المجردة رقم 1 *(Abstract Syntax Notation one)*

AU وحدة الاستيقان *(Authentication Unit)*

BN باريتو–نيهريغ *(Barreto-Naehrig)*

BLS-12 تضمين باريتو لين سكوت درجة 12 *(Barreto-Lynn-Scott embedding degree 12)*

BLS-24 تضمين باريتو لين سكوت درجة 24 *(Barreto-Lynn-Scott embedding degree 24)*

CRL قائمة إبطال الشهادات *(Certificate Revocation List)*

DER قواعد التشفير المميزة *(Distinguished Encoding Rules)*

EAP بروتوكول الاستيقان القابل للتوسع *(Extensible Authentication Protocol)*

ECCSI التوقيعات المعتمدة القائمة على منحنيات إهليلجية بدون شهادات من أجل التشفير القائم على الهوية *(Elliptic Curve-based Certificateless Signatures for Identity-based encryption)*

EID معرِّف الهوية استناداً إلى بطاقة الدارة المتكاملة الشاملة المدمجة *(eUICC-ID)*

EIS مجموعة المعلومات المدمجة في بطاقة الدارة المتكاملة الشاملة *(eUICC Information Set)*

eUICC بطاقة الدارة المتكاملة الشاملة المدمجة *(Embedded Universal Integrated Circuit Card)*

EUM الشركة المصنعة لبطاقة الدارة المتكاملة الشاملة المدمجة *(eUICC Manufacturer)*

GW بوابة *(Gateway)*

HSM وحدة نمطية لأمن العتاد *(Hardware Security Module)*

HTTP بروتوكول نقل النصوص الترابطية *(Hypertext Transfer Protocol)*

IBAKA اتفاق المفاتيح المستيقنة القائم على الهوية *(Identity-Based Authenticated Key Agreement)*

IBC التجفير القائم على الهوية *(Identity-Based Cryptography)*

IBE التشفير القائم على الهوية *(Identity-Based Encryption)*

IBS التوقيع القائم على الهوية *(Identity-Based Signature)*

ID معرِّف الهوية *(Identifier)*

IdP مورد الهوية *(Identity Provider)*

IMSI هوية الاشتراكات المتنقلة الدولية *(International Mobile Subscription Identity)*

IoT إنترنت الأشياء *(Internet of Things)*

ISP منصة خدمة إنترنت الأشياء *(IoT Service Platform)*

IRL قائمة إبطال الهوية *(Identity Revocation List)*

ISD	الميدان الأمني لجهة الإصدار *(Issuer Security Domain)*
KDF	وظيفة اشتقاق المفاتيح *(Key Derivation Function)*
KDK	مفتاح اشتقاق المفاتيح *(Key Derivation Key)*
KEK	مفتاح تشفير المفاتيح *(Key Encryption Key)*
KEM	آلية تغليف المفاتيح *(Key Encapsulation Mechanism)*
KMIP	بروتوكول قابلية التشغيل البيني لإدارة المفاتيح *(Key Management Interoperability Protocol)*
KMS	خدمة إدارة المفاتيح *(Key Management Service)*
KPAK	مفتاح الاستيقان العمومي لخدمة إدارة المفاتيح *(KMS Public Authentication Key)*
KSS-16	تضمين كاشيزا شيفر سكوت درجة 16 *(Kachisa-Schaefer-Scott embedding degree 16)*
KSS-18	تضمين كاشيزا شيفر سكوت درجة 18 *(Kachisa-Schaefer-Scott embedding degree 18)*
LTE	التطور الطويل الأجل *(Long-Term Evolution)*
LTE-M	التطور الطويل الأجل، الفئة M1 *(Long-Term Evolution, category M1)*
MAC	التحكم في النفاذ إلى الوسائط *(Media Access Control)*
MNO	مشغل الشبكة المتنقلة *(Mobile Network Operator)*
MSK	مفتاح السر الرئيسي *(Master Secret Key)*
NB-IoT	إنترنت الأشياء الضيقة النطاق *(Narrowband Internet of Things)*
OCSP	بروتوكول تحديد حالة الشهادة الإلكترونية *(Online Certificate Status Protocol)*
OID	معرِّف هوية الغرض *(Object Identifier)*
OISP	بروتوكول تحديد حالة الهوية الإلكترونية *(Online Identity Status Protocol)*
PKG	مولّد المفاتيح الخاصة *(Private Key Generator)*
PKI	البنية التحتية للمفاتيح العمومية *(Public Key Infrastructure)*
PPS	مخدم المعلمات العمومية *(Public Parameter Server)*
PVT	رمز التحقق العمومي *(Public Verification Token)*
RSF	وظيفة مخدم الإبطال *(Revocation Server Function)*
SecM	وحدة نمطية أمنية *(Security Module)*
SK	ساكاي كاساهارا *(Sakai-Kasahara)*
SM-DP	إعداد بيانات مدير الاشتراكات *(Subscription Manager Data Preparation)*
SM-SR	التسيير المؤمن لمدير الاشتراكات *(Subscription Manager Secure Routing)*
SOK	ساكاي أوجيشي كاساهارا *(Sakai-Ohgishi-Kasahara)*
SSK	مفتاح التوقيع السري *(Secret Signing Key)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TLV الوسم والطول والمتجه *(Tag, Length and Vector)*

TVP معلمة متغيرة زمنياً *(Time-Variant Parameter)*

UE معدات المستعملين *(User Equipment)*

UICC بطاقة الدارة المتكاملة الشاملة *(Universal Integrated Circuit Card)*

5 الاصطلاحات

لا توجد.

6 لمحة عامة

يمكن اعتبار إنترنت الأشياء كبنية تحتية عالمية لمجتمع المعلومات تتيح تقديم خدمات متقدمة عن طريق التوصيل البيني لأشياء (مادية وافتراضية) تقوم على تكنولوجيات معلومات واتصالات (ICT)، وذلك وفقاً للفقرة 1.6 من التوصية [b-ITU-T Y.4000]. ويُعد أمن إنترنت الأشياء من أهم الشواغل نظراً إلى الطبيعة الواسعة الانتشار للأجهزة المقترنة بحساسية بيانات المستعمل المتزايدة. ويرد في التوصية [b-ITU-T Y.4100] وصفاً للمتطلبات الأمنية الشائعة رفيعة المستوى لإنترنت الأشياء، بما في ذلك أمن الاتصالات، وأمن إدارة البيانات، وأمن توفير الخدمات، فضلاً عن الاستيقان والتخويل المتبادلين. ويرد في التوصية [b-ITU-T X.1361] مزيداً من التحليل للتهديدات والتحديات الأمنية في بيئة إنترنت الأشياء ووصفاً للقدرات التي يمكن أن تتعامل مع هذه التهديدات والتحديات وتحد منها. ومن بين القدرات الأمنية اللازمة المعرفة في التوصية [b-ITU-T X.1361] ما يلي:

- قدرة اتصالات آمنة لدعم الاتصالات الآمنة والموثوقة والمحمية الخصوصية؛
- قدرة آمنة لإدارة المفاتيح لدعم الاتصالات الآمنة؛
- قدرة إدارة آمنة للبيانات لتوفير إدارة بيانات آمنة وموثوق بها ومحمية الخصوصية للبيانات؛
- قدرة استيقان من أجل الاستيقان من الأجهزة؛
- قدرة تخويل (مراقبة النفاذ) لتخويل الأجهزة؛
- قدرة لتنفيذ البروتوكولات الآمنة استناداً إلى خوارزميات تجفير بسيطة.

وتتميز أجهزة إنترنت الأشياء بتقييد الموارد، مثل قدرات الحوسبة والاتصال. وتجلب طبيعة أجهزة إنترنت الأشياء تحديات جديدة لتلبية المتطلبات الأمنية في نظام إنترنت الأشياء. ويُعد النشر السهل للغاية، والعمليات الإدارية الخفيفة، والسلطات الموزعة من بين العوامل الرئيسية عند النظر في الحلول الأمنية فيما يتعلق بإنترنت الأشياء.

وعلى النحو الموصوف في التوصية [b-ITU-T X.1361]، يُعد الاستيقان، والتحكم في النفاذ، وكذلك سلامة البيانات وسريتها من بين الخدمات الأساسية اللازمة لتأمين إنترنت الأشياء. ويمكن الاستفادة من آليات تجفير المفاتيح المتناظرة والمفاتيح العمومية على السواء لتوفير مثل هذه الخدمات.

ويُعد الحل الأمني القائم على المفاتيح المتناظرة بسيطاً نسبياً. ومع ذلك، فإنه لا يلائم سيناريوهات الاتصالات بين الأنداد مثل التطبيقات من الآلة إلى الآلة في إنترنت الأشياء دون خدمة على الخط تعمل بوصفها وسيط ثقة أو دون تقاسم مسبق لسر مزدوج بين الأجهزة. وتُعد الاتصالات الآمنة عبر النظام معقدة أيضاً دون الكشف عن سر المستعمل للأطراف النظيرة.

وينطوي الحل التقليدي المتمثل في تجفير المفاتيح العمومي القائم على الشهادات على العمليات المرهقة لإدارة المفاتيح، بما في ذلك إصدار الشهادات والاستعلام عنها وتوزيعها والتحقق منها وإبطالها. وتواجه هذه الأنظمة تحديات كبيرة في مواكبة وتيرة تزايد أعداد الأجهزة ووظائفها في إنترنت الأشياء مع الحفاظ على الأداء اللائق. وتتسبب أيضاً البيانات الزائدة الناجمة عن تبادل الشهادات

في بروتوكولات الأمن في حدوث مشكلات، لا سيما في شبكات إنترنت الأشياء الضيقة النطاق (NB-IoT) التي تحتوي على وحدة بيانات رزمة صغيرة.

ويُعد التجفير القائم على الهوية نوعاً آخر من أنواع التكنولوجيا، وهو يستخدم هوية الكيان كمفتاح عمومي. وكميزة أساسية من ميزات إنترنت الأشياء، يتمتع كل شيء بمعرِّف هوية فريد. وباستخدام هذه المعرِّفات بوصفها مفاتيح عمومية، لا توجد حاجة إلى شهادات. ونتيجة لذلك، يستخدم الحل الأمني للتجفير القائم على الهوية ما يلي: إدارة المفاتيح بشكل أبسط؛ وتمكين السلطات الموزعة من السيطرة على أجهزتها الخاصة؛ والارتقاء إلى عدد كبير من النقاط الطرفية مع تنوع الأجهزة. ونظراً لعدم إرسال أي شهادات، يمكن تنفيذ بروتوكولات الأمن على نحو أكثر كفاءة.

وفي نظام التجفير القائم على الهوية، يكون طرف موثوق يشار إليه بعبارة خدمة إدارة المفاتيح مسؤولاً عن توليد المفتاح الخاص بكل كيان. وقبل توفير خدمة توليد المفاتيح، تبدأ خدمة إدارة المفاتيح عملية تدميث النظام من خلال استخدام الوظيفة **IBSetup** التي توفر معلمة أمنية تحدد مجموعة من معلمات النظام وتولد مفتاح سر رئيسياً ومفتاحاً عمومياً رئيسياً. ويلاحظ أن خدمة إدارة المفاتيح لديها نفس وظيفة مولد المفاتيح الخاصة. ومن ثم، ومن أجل سهولة التعبير، تستخدم هذه التوصية مصطلحي "خدمة إدارة المفاتيح" و"مولد المفاتيح الخاصة" على نحو قابل للتبادل، ويشار إلى الجمع بين معلمات النظام والمفتاح العمومي الرئيسي بالمعلمات العمومية. وتحافظ خدمة إدارة المفاتيح على السرية الصارمة لمفتاح السر الرئيسي وتجعل المعلمات العمومية متاحة للعامة. ويمكن عند الضرورة نشر المعلمات العمومية بواسطة مخدم معلمات عمومية مخصص.

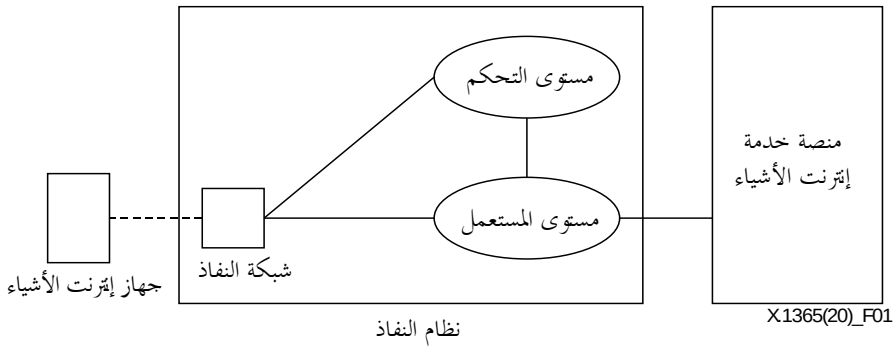
ويمكن أن يستخدم نظام الأمن النمطي للتجفير القائم على الهوية مجموعة من آليات التجفير القائم على الهوية، بما في ذلك التشفير القائم على الهوية، والتوقيع القائم على الهوية، واتفاق المفاتيح المستيقنة القائم على الهوية لتوفير مختلف الخدمات الأمنية، بما فيها سرية البيانات، واستيقان الكيانات، وإنشاء قناة آمنة. ويمكن اعتبار كل هذه الخوارزميات الخاصة بالتجفير القائم على الهوية بمثابة تشكيل لمجموعتين من الوظائف. تتكون المجموعة الأولى من وظائف توليد المفاتيح، التي تولد أزواجاً من المفاتيح العمومية والخاصة القائمة على الهوية. وتولّد وظيفة توليد المفاتيح الخاصة **(IBExtract)** مفتاحاً خاصاً من معرِّف الهوية، ومفتاح سر رئيسي، ومعلمات عمومية. وتقوم وظيفة اشتقاق المفاتيح العمومية للهوية **(IBDerivate)** بحساب مفتاح عمومي من معرِّف الهوية والمعلمات العمومية. وتستخدم المجموعة الأخرى من الوظائف، مثل التشفير أو فك التشفير **(IBEnc/IBDec)**، والتوقيع أو التحقق **(IBSign/IBVerify)**، وبروتوكول إنشاء مفتاح الدورة المستيقنة، أزواج المفاتيح المولّدة لاستكمال عمليات التجفير المقابلة.

وجرى تقييس تكنولوجيا التجفير القائم على الهوية من جانب مختلف منظمات وضع المعايير، بما فيها المنظمة الدولية للتوحيد القياسي (ISO)، واللجنة الكهرتقنية الدولية (IEC)، وفريق مهام هندسة الإنترنت (IETF)، ومعهد مهندسي الكهرباء والإلكترونيات (IEEE)، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، وإدارة المعايير في الصين (SAC). وترد في البيبليوغرافيا قائمة ببعض المعايير ذات الصلة التي وضعتها هذه المنظمات. وينظر النظام OneM2M أيضاً في استخدام تكنولوجيات التجفير القائم على الهوية فيما يتعلق بشبكات إنترنت الأشياء في الإصدار 4، ويمكن الاطلاع على التحليل الأمني الخاص به في التوصية [b-ETSI TR 118 508].

ويرد في هذه التوصية وصفاً لإطار أمني فيما يتعلق باستخدام تكنولوجيا التجفير القائم على الهوية لتوفير القدارت الأمنية لخدمات إنترنت الأشياء على شبكات الاتصالات. ويغطي هذا الإطار جوانب إدارة الهوية، ومعمارية إدارة المفاتيح، وعمليات إدارة المفاتيح، والاستيقان، وكذلك بروتوكولات اتفاقات المفاتيح الخاصة باستخدام التجفير القائم على الهوية.

7 المعمارية المرجعية للنظام فيما يتعلق بخدمات إنترنت الأشياء على شبكات الاتصالات

يقدم هذا البند معمارية مرجعية للنظام العام فيما يتعلق بخدمات إنترنت الأشياء على شبكات الاتصالات. ويوضح الشكل 1 معمارية مرجعية مفاهيمية للنظام فيما يتعلق بخدمات إنترنت الأشياء. ويتكوَّن النظام من ثلاثة ميادين هي: جهاز إنترنت الأشياء، ونظام النفاذ (AS)، ومنصة خدمة إنترنت الأشياء (ISP).



الشكل 1 – معمارية مفاهيمية للنظام فيما يتعلق بخدمات إنترنت الأشياء

تضطلع أجهزة إنترنت الأشياء بمسؤولية جمع البيانات أو تنفيذ الإجراءات. ويمكن لمعظم أجهزة إنترنت الأشياء إقامة توصيل مع نظام من أنظمة الاتصالات، والاتصال بمنصة خدمة إنترنت الأشياء. وفي أيامنا هذه، تتصل غالبية أجهزة إنترنت الأشياء بمنصة خدمة إنترنت الأشياء عبر وصلة لاسلكية تقام مع شبكة اتصالات. ويشير نظام النفاذ، في هذه التوصية، إلى شبكات الاتصالات. ويتكون هذا النظام عادة من جزأين هما: شبكة النفاذ والشبكة الأساسية. ويمكن تقسيم الشبكة الأساسية بدورها إلى قسمين: مستوي التحكم ومستوي المستعمل، المسؤولان عن تشوير التحكم ونقل البيانات، على التوالي.

إن شبكة الاتصالات، بوصفها توصيلية لاسلكية تقليدية، استخدمت بالفعل لعدة أجيال. ومن الناحية التاريخية، تصمم شبكات الاتصالات لدعم الاتصالات المتنقلة للإنسان مع سمات التجوال السلس. وفي السنوات الماضية، جرى النظر أيضاً في دعم أجهزة إنترنت الأشياء في مجال التصميم بدءاً من الجيل الرابع من شبكات التطور طويل الأجل. فعلى سبيل المثال، وفي الجيل الرابع من التطور طويل الأجل (4G-LTE)، تم تطوير الفئة M1 (LTE-M) والتكنولوجيات NB-IoT لدعم أجهزة إنترنت الأشياء.

وتتكون غالبية أنظمة الاتصالات الحالية من ثلاثة مكونات هي: المطاريف أو معدات المستعملين (UE)، وشبكة نفاذ (AN)، والشبكات الأساسية ويفترض هنا أن كل من شبكة النفاذ والشبكات الأساسية تنتمي إلى نظام النفاذ كما هو موضح في الشكل 1. وعادةً ما تكون خدمات إنترنت الأشياء خارج شبكات الاتصالات مع بعض السطوح البينية لنقل البيانات وإدارة الخدمات. ولتوفير دعم أفضل لخدمات إنترنت الأشياء، تُضمّن شبكات الاتصالات مزيداً من التصاميم المحددة حصراً لإنترنت الأشياء في مواصفات النظام الخاص بها. وأصبح التكامل بين شبكات الاتصالات وخدمات إنترنت الأشياء أوثق في السنوات الماضية.

ومع وضع مواصفات النظام لشبكات الجيل الخامس (5G)، تُدعم تكنولوجيات المفاتيح العمومية من أجل خدمات إنترنت الأشياء، بما في ذلك استيقان النفاذ إلى الشبكة. وعلى النحو المشار إليه في الفقرة 6، ومقارنة مع تكنولوجيات المفاتيح العمومية الأخرى، يُعد التجفير القائم على الهوية أبسط في الإدارة وأكثر فعالية على صعيد النقل. ولذلك، يتطلب استخدام التجفير القائم على الهوية فيما يتعلق بخدمات إنترنت الأشياء على شبكات الاتصالات مواصفات معينة بوصفها مكملاً قياسياً للمواصفات القائمة.

8 إطار استعمال التجفير القائم على الهوية (IBC) من أجل خدمات إنترنت الأشياء عبر شبكات الاتصالات

يقدم في هذه الفقرة إطار استعمال تكنولوجيات المفاتيح العمومية للتجفير القائم على الهوية من أجل خدمات إنترنت الأشياء في شبكات الاتصالات. ويحتوي هذا الإطار على معمارية للنظام بإدراج مكونات الشبكة المطلوبة عند استعمال تكنولوجيات التجفير القائم على الهوية. وعلاوةً على ذلك، يُحدد في هذه الفقرة إطار لإدارة المفاتيح من أجل التجفير القائم على الهوية باعتباره ضروري لأي نظام يستخدم تكنولوجيا التجفير القائم على الهوية. ويتناول هذا الإطار أيضاً مسائل حساسة أخرى، مثل إدارة المفاتيح، وتسمية الهوية وبروتوكولات الاستيقان.

1.8 معمارية نظام لإنترنت الأشياء بالتجفير القائم على الهوية

بالنسبة لخدمات إنترنت الأشياء المشغلة على شبكات الاتصالات، يمكن استعمال التجفير القائم على الهوية سواء من أجل استيقان النفاذ إلى الشبكة أو استيقان النفاذ إلى الخدمة أو كلاهما. ويتناول استيقان النفاذ إلى الشبكة ما إذا كان الجهاز مسموحاً له بالنفاذ إلى هذه الشبكة من عدمه، في حين يتناول استيقان النفاذ إلى الخدمة ما إذا كان الجهاز مسموحاً له بالنفاذ إلى منصة خدمات إنترنت الأشياء من عدمه.

ويمكن لأجهزة إنترنت الأشياء النفاذ إلى شبكة الاتصالات بشكل مباشر أو غير مباشر. وبالتالي، هناك نموذجان للنفاذ:

- نموذج الاتصال المباشر: توصل أجهزة إنترنت الأشياء بنظام النفاذ مباشرة؛
- نموذج الاتصال غير المباشر: توصل أجهزة إنترنت الأشياء بنظام النفاذ عبر بوابة التجميع (AGW).

ويبين الشكل 2 البنية المرجعية لنظام إنترنت الأشياء حيث يُستعمل التجفير القائم على الهوية لحماية أمن نظام النفاذ ومنصة خدمات إنترنت الأشياء. ومن وجهة نظر أمنية، قد يكون لكل من نظام النفاذ ومنصة خدمات إنترنت الأشياء متطلبات الأمن الخاصة بكل منهما عندما يتعلق الأمر بخدمات إنترنت الأشياء. وبالنظر إلى الإثباتات الأمنية التي يمكن أن يوفرها نظام النفاذ أو منصة خدمات إنترنت الأشياء للإثباتات الأمنية، هناك ثلاثة سيناريوهات يُستعمل فيها تكنولوجيات التجفير القائم على الهوية في شبكات إنترنت الأشياء، وهي على النحو التالي:

- استعمال تكنولوجيات التجفير القائم على الهوية في سيناريو حماية أمن باستعمال نظام النفاذ:

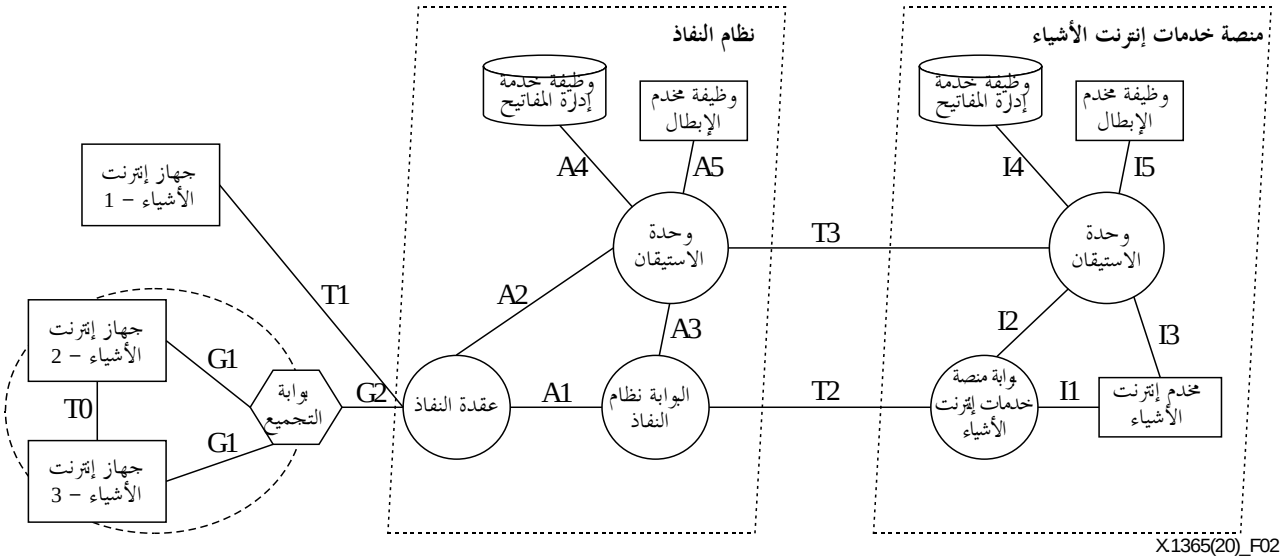
  في هذا السيناريو، يوفر نظام النفاذ ويدير الإثباتات الأمنية المخزنة في أجهزة إنترنت الأشياء والتي تتيح النفاذ إلى الشبكة. فنظام النفاذ هذا يقوم باستيقان أجهزة إنترنت الأشياء عند توصيلها به. فمثلاً، يقوم جهاز من أجهزة إنترنت الأشياء بحساب التوقيع القائم على الهوية استناداً إلى المفتاح الخاص الذي يوفره نظام النفاذ ثم يرسل هذا التوقيع إلى نظام النفاذ نفسه. ووفقاً لذلك، يمكن أن يستيقن نظام النفاذ جهاز إنترنت الأشياء استناداً إلى التوقيع القائم على الهوية المقدم في رسائل الاستيقان. وإذا نجحت عملية التحقق، يرسل نظام النفاذ البيانات من جهاز إنترنت الأشياء إلى مخدم إنترنت الأشياء؛

- استعمال التجفير القائم على الهوية لحماية أمن منصة خدمات إنترنت الأشياء:

  في هذا السيناريو، توفر منصة خدمات إنترنت الأشياء وتدير الإثباتات الأمنية للتجفير القائم على الهوية المخزنة في أجهزة إنترنت الأشياء والتي تتيح النفاذ إلى الخدمة. وتستيقن منصة خدمات إنترنت الأشياء من أجهزة إنترنت الأشياء استناداً إلى التوقيع المتولد من إثباتات التجفير القائم على الهوية؛

- سيناريو استعمال التجفير القائم على الهوية لحماية أمن كل من نظام النفاذ ومنصة خدمات إنترنت الأشياء:

  في هذا السيناريو، توفر منصة خدمات إنترنت الأشياء أو نظام النفاذ ويديران الإثباتات الأمنية للتجفير القائم على الهوية المخزنة في أجهزة إنترنت الأشياء. ويستيقن نظام النفاذ ومنصة خدمات إنترنت الأشياء أجهزة إنترنت الأشياء استناداً إلى مجموعة الإثباتات نفسها.



الشكل 2 – معمارية نظام إنترنت الأشياء استناداً إلى تكنولوجيات التجفير القائم على الهوية في كل من سيناريو حماية أمن نظام النفاذ وسيناريو حماية أمن منصة خدمات إنترنت الأشياء

تصف السيناريوهات الثلاثة الواردة أعلاه معظم حالات استعمال التجفير القائم على الهوية من أجل النفاذ إلى الشبكة والخدمة. ومع ذلك، قد تكون هناك سيناريوهات أخرى لا يشملها نطاق هذه التوصية.

وتتكون معمارية نظام إنترنت الأشياء المستندة إلى التجفير القائم على الهوية من الوظائف الشبكية والأجهزة التالية:

- نظام النفاذ (AS): يُقصد به نظام النفاذ إلى أجهزة إنترنت الأشياء أو إلى بوابة التجميع، بما في ذلك عقدة النفاذ (AS.AN)، ووظيفة خدمة إدارة المفاتيح (AS.KMS)، ووحدة الاستيقان (AS.AU)، ووظيفة مخدم الإبطال (AS.RSF) والبوابة (AS.GW)؛
- منصة خدمات إنترنت الأشياء (ISP): هي منصة لإدارة خدمات إنترنت الأشياء، بما في ذلك خدمة إدارة المفاتيح (ISP.KMS)، ووحدة الاستيقان (isp.au)، ووظيفة مخدم الإبطال (ISP.RSF)، والبوابة (ISP.GW)، ومخدم إنترنت الأشياء. ويجب أن تدعم هذه المنصة إدارة المفاتيح، والتوزيع، واستيقان الهوية، والتجفير أو فك التجفير، والتوقيع أو التحقق منه، وما إلى ذلك؛
- بوابة التجميع (AGW): يُقصد بها عقدة تجميع، مسؤولة عن توصيل جهاز إنترنت الأشياء، وتجميع وإرسال جميع بيانات هذا الجهاز إلى نظام النفاذ. وتقوم بوابة التجميع بدور وكيل نقل البيانات بين أجهزة إنترنت الأشياء وعقدة النفاذ؛
- عقدة النفاذ (AN): ويُقصد بها عقدة النفاذ إلى أجهزة إنترنت الأشياء أو إلى بوابة التجميع، ويمكن أن تكون على شكل نفاذ لاسلكية أو ثابتة إلى الشبكة؛
- وظيفة خدمة إدارة المفاتيح (KMS): هو نظام للإدارة، مسؤول عن توليد المفاتيح وتوزيعها وتحديث مفاتيح ومعلمات التجفير القائم على الهوية لأجهزة إنترنت الأشياء ووظائف الشبكة؛
- وحدة الاستيقان (AU): تقوم هذه الوحدة باستيقان جهاز إنترنت الأشياء استناداً إلى نظام التجفير القائم على الهوية؛
- وظيفة مخدم الإبطال (RSF): هو مخدم يحتفظ بقائمة إبطال للهويات (IRL). وتُستبعد المفاتيح العمومية أو الهويات الواردة في قائمة الإبطال من الاستعمال؛

ملاحظة – قد يكون لكل من نظام النفاذ ومنصة خدمات إنترنت الأشياء النظام KMS والوحدة AU والوظيفة RSF الخاصة بكل منهما.

- بوابة نظام النفاذ (AS.GW): هي عنصر شبكة موصول ببوابة إنترنت الأشياء، مسؤول عن نقل بيانات مستعمل إنترنت الأشياء؛
- بوابة إنترنت الأشياء (IoT GW): بوابة مسؤولة عن إعادة تسيير أو تجميع البيانات وإرسالها إلى مخدم إنترنت الأشياء، أو إعادة تسيير البيانات/التشوير من مخدم إنترنت الأشياء إلى أجهزة إنترنت الأشياء؛

- مخدم إنترنت الأشياء: هو مخدم موجود على جانب مورد خدمة إنترنت الأشياء، يقوم بجمع بيانات إنترنت الأشياء من بوابة إنترنت الأشياء؛
- جهاز إنترنت الأشياء: هو الجهاز الطرفي الذي يُستعمل لجمع البيانات وإنشاء توصيل مع عقدة النفاذ ومخدم إنترنت الأشياء، ويوفر الحماية للبيانات، بما في ذلك التفاوض بشأن المفاتيح والتجفير أو فك التجفير والتوقيع أو التحقق منه؛

ويرد أدناه توضيح وظائف النقاط المرجعية المبنية في الشكل 2:

- G1: هي نقطة مرجعية بين جهاز إنترنت الأشياء وبوابة التجميع، تُستعمل للاستيقان واتصالات الأمن؛
- G2: هي نقطة مرجعية بين بوابة التجميع وعقدة النفاذ، تُستعمل للتشوير ونقل البيانات بين بوابة التجميع وعقدة النفاذ؛
- T0: هي نقطة مرجعية بين أجهزة إنترنت الأشياء وعقدة النفاذ، تُستعمل لتشوير وتبادل البيانات؛
- T1: هي نقطة مرجعية بين أجهزة إنترنت الأشياء وعقدة النفاذ، تُستعمل للاستيقان واتصالات الأمن؛
- T2: هي نقطة مرجعية بين بوابة نظام النفاذ وبوابة منصة خدمات إنترنت الأشياء، توفر مساراً حاملاً لبيانات مستوى المستعمل بين البوابة AS.GW والمنصة ISP؛
- T3: هي نقطة مرجعية بين وحدتي الاستيقان AS.AU وISP.AU، لتبادل التشوير، بما في ذلك تبادل الهوية أو توفير المفاتيح؛
- A1: هي نقطة مرجعية بين عقدة النفاذ والبوابة AS.GW، توفر مساراً حاملاً لبيانات مستوى المستعمل؛
- A2: هي نقطة مرجعية بين وحدة الاستيقان AS.AU وعقدة النفاذ، لتشوير مستوى التحكم؛
- A3: هي نقطة مرجعية بين وحدة الاستيقان AS.AU والبوابة AS.GW، من أجل تخصيص البوابات وبروتوكول الإدارة في نظام النفاذ؛
- A4: هي نقطة مرجعية بين وحدة الاستيقان AS.AU ووظيفة خدمة إدارة المفاتيح، من أجل بروتوكول توفير المفاتيح في نظام النفاذ؛
- A5: هي نقطة مرجعية بين وحدة الاستيقان AS.AU ووظيفة مخدم الإبطال AS.RSF، من أجل بروتوكول الهوية أو بروتوكول إبطال المفاتيح في نظام النفاذ؛
- I1: هي نقطة مرجعية بين مخدم إنترنت الأشياء والبوابة ISP.GW، توفر مساراً حاملاً لبيانات مستوى المستعمل؛
- I2: هي نقطة مرجعية بين وحدة الاستيقان ISP.AU والبوابة ISP.GW، من أجل تخصيص البوابات وبروتوكول الإدارة في منصة خدمات إنترنت الأشياء؛
- I3: هي نقطة مرجعية بين وحدة الاستيقان ISP.AU ومخدم إنترنت الأشياء، لتبادل المعلومات، مثل معلومات الاشتراك المتعلقة بالخدمة والتي تُنقل من مخدم إنترنت الأشياء إلى وحدة الاستيقان ISP.AU، ورسالة الإشعار بالاستيقان من وحدة الاستيقان ISP.AU إلى مخدم إنترنت الأشياء؛
- I4: هي نقطة مرجعية بين وحدة الاستيقان ISP.AU وخدمة إدارة المفاتيح AS.KMS، من أجل بروتوكول توفير المفاتيح في منصة خدمات إنترنت الأشياء؛
- I5: هي نقطة مرجعية بين وحدة الاستيقان ISP.AU ووظيفة مخدم الإبطال AS.RSF، من أجل الهوية أو بروتوكول إبطال المفاتيح في منصة خدمات إنترنت الأشياء.

2.8 معمارية إدارة المفاتيح

تصف هذه الفقرة المعمارية الوظيفية اللازمة لدعم إدارة المفاتيح عند استعمال آليات التجفير القائم على الهوية في إنترنت الأشياء. وبناءً على ما إذا كان جهاز إنترنت الأشياء مزودا بمكون يحتوي على بطاقة دارة متكاملة شاملة مدمجة (eUICC) حسب المعيار [b-GSMA SGP.02]، يؤخذ في الحسبان نوعان من معماريات إدارة المفاتيح باستعمال: (1) التجفير القائم على الهوية

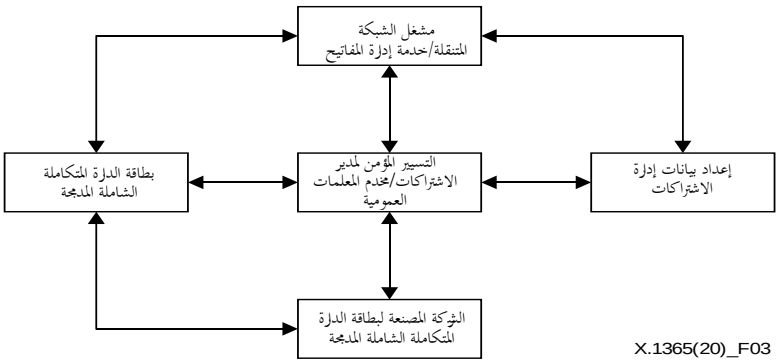
في أجهزة إنترنت الأشياء المزودة ببطاقة دارة متكاملة شاملة مدمجة؛ (2) التجفير القائم على الهوية في أجهزة إنترنت الأشياء غير المزودة ببطاقة دارة متكاملة شاملة مدمجة.

وفي حالة استعمال أجهزة إنترنت الأشياء المزودة ببطاقة دارة متكاملة شاملة مدمجة، تتبع المعمارية نفس المعمارية الخاصة بتوفير الدارة المتكاملة الشاملة المدمجة عن بُعد على النحو الموصوف في المعيار [b-GSMA SGP.02] عن طريق إضافة كيانين وظيفيين جديدين، وهما خدمة إدارة المفاتيح ومخدم المعلمات العمومية (PPS). وحسب موقع خدمة إدارة المفاتيح، تُقسم هذه الحالة بدورها إلى الحالتين الفرعيتين التاليتين:

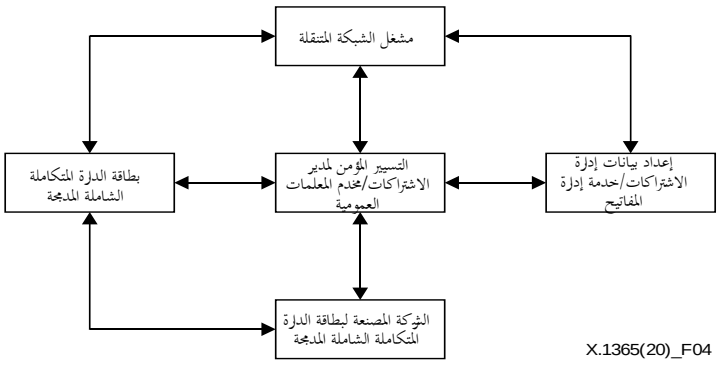
1) يقوم نفس الكيان المسؤول عن مشغل الشبكة المتنقلة (MNO) بإدارة خدمة إدارة المفاتيح – انظر الشكل 3؛

2) يقوم الكيان المسؤول عن إعداد بيانات مدير الاشتراكات (SM-DP) بإدارة خدمة إدارة المفاتيح – انظر الشكل 4.

وفي كلتا الحالتين الفرعيتين، تتولد المفاتيح بما في ذلك المفاتيح الخاصة والمعلمات العمومية عندما يقدم مشغل الشبكة المتنقلة طلباً لإنشاء مواصفة. وبعد ذلك تُتاح المفاتيح عن بُعد للأجهزة المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة حيث يتم تثبيت هذه المفاتيح وفقاً لمواصفة توفير المفاتيح عن بُعد المعمول بها حالياً في المعيار [b-GSMA SGP.02]. ويمكن الاطلاع على تفاصيل الأدوار والوظائف ذات الصلة والسطوح البينية لتوفير المفاتيح عن بُعد للأجهزة المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة في المعيار [b-GSMA SGP.02]. وتندرج عملية تحديد المواصفات ونسق التخزين واستعمال هذه المفاتيح في بطاقة الدارة المتكاملة الشاملة المدمجة خارج نطاق هذه التوصية.



الشكل 3 – المعمارية A لإدارة مفاتيح التجفير القائم على الهوية في أجهزة إنترنت الأشياء المزودة ببطاقة دارة متكاملة شاملة مدمجة

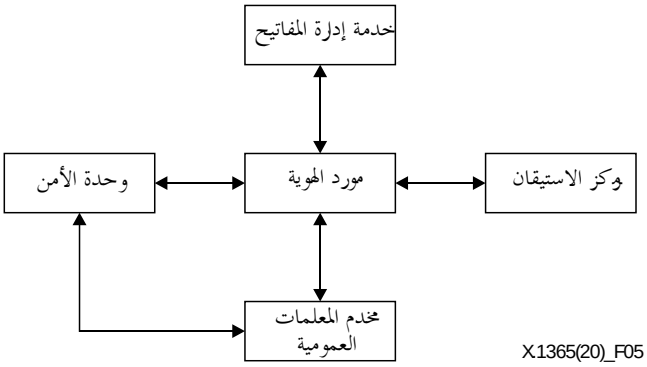


الشكل 4 – المعمارية B لإدارة مفاتيح التجفير القائم على الهوية في أجهزة إنترنت الأشياء المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة

وتبين في الشكل 5 معمارية عامة في حالة استعمال التجفير القائم على الهوية في أجهزة إنترنت الأشياء غير المزودة ببطاقة دارة متكاملة شاملة مدمجة. وتشمل اللبنات الأساسية المكونة لها ما يلي:

- وحدة الأمن (SecM): تعتبر وحدة الأمن عنصراً يمكنه تخزين المفاتيح بشكل مؤمن وتنفيذ آليات الأمن باستعمال المفاتيح المخزنة لإكمال العمليات الأمنية. وينبغي لكل جهاز من أجهزة إنترنت الأشياء أن يحتوي على وحدة أمن.
- مورد الهوية (IdP): مورد الهوية هو كيان يولد معلومات الهوية ويحافظ عليها ويديرها.
- مركز الاستيقان (AuC): يوفر مركز الاستيقان استيقان الكيان كخدمة.

يعتمد مورد الهوية على خدمة الاستيقان التي يوفرها مركز الاستيقان في استيقان أجهزة إنترنت الأشياء. فبعد عملية الاستيقان الأولى، يزود مورد الهوية وحدة الأمن بخدمة توريد الهوية بما في ذلك إنشاء الهوية وتخصيصها واستبدالها وإبطالها. وبعد إنشاء هوية جديدة وتخصيصها لجهاز إنترنت الأشياء، يلتمس مورد الهوية من خدمة توليد المفاتيح الخاصة التي توفرها خدمة إدارة المفاتيح توليد المفتاح الخاص المقابل للهوية المخصصة حديثاً ويوزع المفاتيح بشكل مؤمن على وحدة الأمن. كما يقوم مورد الهوية أيضاً باستخراج المعلمات العمومية من خدمة إدارة المفاتيح وإدخالها في مخدم المعلمات العمومية الذي يقوم بدوره بنشرها على الكيانات الخارجية. وقد يزود مورد الهوية أيضاً الكيانات الأخرى بخدمة الاستيقان بأن ينفذ هو ووحدة الأمن بروتوكولات الاستيقان الخاصة بما في ذلك تلك المحددة في هذه التوصية.



الشكل 5 – معمارية إدارة مفاتيح التجفير القائم على الهوية في أجهزة إنترنت الأشياء غير المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة

3.8 تسمية الهوية

عند استعمال تكنولوجيا التجفير القائم على الهوية في خدمات إنترنت الأشياء عبر شبكة اتصالات، يمكن أن توفر تسمية الهوية معلومات مفيدة لمساعدة المشغلين على إدارة الشبكات. ويمكن تضمين أشكال متنوعة من المعلومات، مثل نوع الخدمة، والموقع، ومعرِّف هوية الجهاز، ووقت الصلاحية في الهوية. وجزء من هذه المعلومات ضروري عند استعمال تكنولوجيا التجفير القائم على الهوية، مثل، وقت الصلاحية. وباستعمال معلومات الهوية، يمكن للمشغل استمثال إدارة الشبكة، على سبيل المثال عن طريق توزيع التوصيل على شرائح شبكية محددة، بناءً على نوع الخدمة التي يقدمها. ومن السهل أيضاً تحديد موقع الجهاز استناداً إلى معلومات الموقع الخاصة به. ويرد مثال توضيحي لتعريف الهوية في التذييل I.

4.8 إدارة المفاتيح

بصرف النظر عن قيمة الهوية، يتضمن نظام التجفير القائم على الهوية ثلاثة أنواع من قيم مفاتيح التجفير: مفتاح السر الرئيسي، والمعلمات العمومية، والمفتاح الخاص. ويرد في الملحق B تعريف ترميز قواعد التركيب المجردة رقم 1 (ASN.1) للبنى الخاصة بهذه المفاتيح.

ولإدارة هذه المفاتيح، يستعمل نظام التجفير القائم على الهوية خمس عمليات لإدارة المفاتيح:

1) عملية تدميث النظام؛
2) تدميث الجهاز؛
3) البحث في المعلمة العامة؛
4) توفير الهوية والمفاتيح؛
5) إلغاء الهوية والمفاتيح.

يمكن استعمال بروتوكول قابلية التشغيل البيني لإدارة المفاتيح (KMIP) على النحو الموصوف في التوصية [b-OASIS KMIP] لتبادل الرسائل بين كيان الإدارة وخدمة إدارة المفاتيح. ومع ذلك، لا بد من توسيع نطاق بروتوكول قابلية التشغيل البيني لإدارة المفاتيح ليلبي المتطلبات الجديدة لوظيفتي **IBSetup** و**IBExtract**. وبالنسبة إلى لأجهزة إنترنت الأشياء المزودة ببطاقة دارة متكاملة شاملة مدمجة، تُستخدم الإجراءات القياسية لتوفير المفاتيح عن بُعد الواردة في المعيار [b-GSMA SGP.02]. وبالنسبة لأجهزة إنترنت الأشياء غير المزودة ببطاقة دارة متكاملة شاملة مدمجة، تُحدد بروتوكولات التفاعل بين وحدات الأمن وكيانات الإدارة على أساس بروتوكول نقل النصوص الترابطية (HTTP). وتُحدد مواصفات هذه العمليات في الملحق C.

وتقوم عملية تدميث النظام بتدميث نظام التجفير القائم على الهوية عن طريق توليد مفتاح السر الرئيسي والمعلمات العمومية. ويُفترض أن يتولى كيان إداري، مثل مورد الهوية أو وظيفة إعداد بيانات مدير الاشتراكات أو مشغل الشبكة المتنقلة، مسؤولية تدميث نظام التجفير القائم على الهوية. ويقوم هذا الكيان بإنشاء قناة مؤمنة مع كيان خدمة إدارة المفاتيح تنفذ الوظيفة **IBSetup**. ويقوم الطرفان بتنفيذ بروتوكول قابلية التشغيل البيني لإدارة المفاتيح من خلال عملية توليد زوج المفاتيح. ويوفر كيان الإدارة المعلومات اللازمة لخدمة إدارة المفاتيح لاستدعاء الوظيفة **IBCSetup** وتوليد مفتاح السر الرئيسي والمعلمات العمومية. ويُوسع نطاق بروتوكول قابلية التشغيل البيني لإدارة المفاتيح ليدعم وظائف الإعداد بما في ذلك وظائف خوارزميات التجفير القائم على الهوية القياسية المختلفة. وترد تفاصيل هذه العملية في الفقرة 1.C.

وتتمثل عملية تدميث الجهاز في إعداد جهاز إنترنت الأشياء من أجل توفير الهوية والمفاتيح. وهناك حالتان: تدميث أجهزة إنترنت الأشياء المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة وتدميث أجهزة إنترنت الأشياء غير المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة. ومن الضروري أن تستكمل البطاقة eUICC في الأجهزة المزودة بها التسجيل في التسيير المؤمن لمدير الاشتراكات (SM-SR) وبذلك تكون جاهزة لتنزيل المواصفة على النحو الوارد في المعيار [b-GSMA SGP.02]. ولا توجد هناك عملية إضافية مطلوبة من الأجهزة القياسية المزودة بالبطاقة eUICC. وبالنسبة لأجهزة إنترنت الأشياء غير المزودة بالبطاقة eUICC، يجب على وحدة الأمن أولاً التسجيل لدى مركز الاستيقان للحصول على هوية عملية التوفير (PROV.ID) وإثباتاتها (PROV.CRED). ويُستخدم هذا الزوج، PROV.ID/PROV.CRED، لاستيقان الكيان في عملية توفير الهوية/المفاتيح. وإذا تعذر على أجهزة إنترنت الأشياء إنشاء قناة مؤمنة مع مورد الهوية باستخدام أمن طبقة النقل (TLS)، فمن الضروري أيضاً تثبيت هوية المورد لهوية المفتاح والمفتاح العمومي للمورد لمعرِّف هوية المفتاح العمومي اللذين ينتميان إلى مورد الهوية أو المعلمة العمومية في وحدة الأمن أثناء عملية تدميث الجهاز. وترد تفاصيل هذه العملية في الفقرة 2.C.

وتتمثل وظيفة عملية البحث عن المعلمات العمومية في استرداد المعلمات العمومية للتجفير القائم على الهوية. ويجب أن يستخدم جهاز إنترنت الأشياء الهوية وإجراءات توفير المفاتيح للحصول على المعلمات العمومية لنظام التجفير القائم على الهوية التي ينتمي إليها. وقد تتبع هذه العملية المواصفة الواردة في الفقرة 4 من التوصية [IETF RFC 5408] لاسترداد المعلمات العمومية لنظام آخر من أنظمة التجفير القائم على الهوية من مخدم المعلمات العمومية المعروف. وترد تفاصيل هذه العملية في الفقرة 3.C.

وتتضمن عملية توفير الهوية والمفاتيح تخصيص الهوية، واستخراج المفتاح الخاص، وإجراءات توزيع المفاتيح. وتحصل أجهزة إنترنت الأشياء بعد عملية التدميث على هوية مؤقتة فقط. ويجب على مورد الهوية أو وظيفة إعداد بيانات مدير الاشتراكات أو مشغل الشبكة المتنقلة تحديد الهوية التي سيتم تخصيصها للجهاز المتقدم بالطلب، ثم الاتصال بخدمة إدارة المفاتيح لإنشاء المفتاح الخاص

المقابل وفي نهاية المطاف توزيع الهوية، والمفتاح الخاص، والمعلمات العمومية على الجهاز بشكل مؤمن. وترد تفاصيل هذه العملية في الفقرة 4.C.

وتُستخدم عملية إبطال الهوية والمفاتيح عندما تتطلب سياسة الأمن الصارمة إبطال هوية ما في الوقت المناسب. وإذا ما أُبطلت الهوية، فإنها تُضبط على وضع الإبطال. وإذا استفسر بيان ما عن حالة هوية مبطلة، يقوم مورد الهوية أو وظيفة إعداد بيانات مدير الاشتراكات أو مشغل الشبكة المتنقلة بإعادة القيمة الصحيحة كما هو محدد في بروتوكول وضع الهوية على الخط (OISP). وللتحقق من أوضاع مجموعة من الهويات بشكل أكثر كفاءة، يمكن لأي كيان استرداد قائمة إبطال الهوية من مورد الهوية أو وظيفة إعداد بيانات مدير الاشتراكات أو مشغل الشبكة المتنقلة بانتظام وتخزينها محلياً، ويمكن للكيان التحقق من قائمة إبطال الهوية الجديدة لتحديد ما إذا كان قد تم إبطال هوية ما دون الاستفسار عن وضع كل هوية من على الخط. وترد تفاصيل هذه العملية في الملحق 5.C.

5.8 الاستيقان

الاستيقان هو عملية تحديد ما إذا كان لأي كيان (جهاز أو مستعمل) الحق في النفاذ إلى موارد معينة. وفي شبكات الاتصالات، هناك نوعان من الاستيقان يتعلقان بأجهزة إنترنت الأشياء: استيقان النفاذ إلى الشبكة واستيقان الخدمة. ويتناول استيقان النفاذ إلى الشبكة ما إذا كان يُسمح لجهاز ما بالنفاذ إلى الشبكة، بينما يتناول استيقان الخدمة ما إذا كان بإمكان الجهاز النفاذ إلى منصة خدمات إنترنت الأشياء (ISP) أم لا.

وتعد بروتوكولات الاستيقان المستندة إلى تكنولوجيات التجفير القائم على الهوية مناسبة لاستيقان إنترنت الأشياء في شبكات الاتصالات. ويرجع ذلك إلى حقيقة مفادها أن التجفير القائم على الهوية يمكن أن يحد إلى حد كبير من العبء الواقع على إدارة الهوية والمفاتيح لعدد ضخم من أجهزة إنترنت الأشياء. وهناك ميزة أخرى للتجفير القائم على الهوية هي أنه يتيح الاستيقان الموزع، الذي لا يحد فقط من زمن الاستيقان بشكل كبير، ولكنه يمكّن أيضاً من تنفيذ سيناريوهات التطبيقات الجديدة، مثل، الاستيقان من جهاز إلى جهاز، والاستيقان من مركبة إلى مركبة. وبالنسبة لشبكات الاتصالات الحالية، مثل شبكات التطور طويل الأجل من الجيل الرابع، يمكن استخدام التجفير القائم على الهوية في الاستيقان بين أجهزة إنترنت الأشياء ومنصة خدمات إنترنت الأشياء. وبالنسبة للشبكات الخلوية من الجيل الخامس، يمكن استخدام التجفير القائم على الهوية لكل من استيقان النفاذ إلى الشبكة واستيقان النفاذ إلى الخدمة. وتحدد المواصفة الحالية لأمن تكنولوجيا الجيل الخامس، التوصية [b-ETSI TS 133.501]، إطار استيقان موحد يدعم أساليب بروتوكول الاستيقان القابل للتوسع (EAP). ويوصف ملحق التوصية [b-ETSI TS 133.501] بشكل أكبر كيفية استخدام أمن طبقة النقل لبروتوكول الاستيقان القابل للتوسع في تكنولوجيا الجيل الخامس من أجل شبكات إنترنت الأشياء.

ويُعد إطار بروتوكول الاستيقان القابل للتوسع مفتوحاً ويدعم العديد من بروتوكولات الاستيقان، بما في ذلك أمن طبقة النقل لبروتوكول الاستيقان القابل للتوسع. وتدعم أساليب استيقان بروتوكول الاستيقان القابل للتوسع كلاً من المفاتيح التناظرية واللاتناظرية.

وباعتبارها تكنولوجيا من تكنولوجيات المفاتيح العمومية الجديدة نسبيا، لا تدعم بروتوكولات الاستيقان الحالية التجفير القائم على الهوية. لذلك، أُدخلت تعديلات، على النحو الوارد في الملحق D، على أربعة بروتوكولات حالية لدعم التجفير القائم على الهوية في عملية الاستيقان:

1) الفقرة 1.D: بروتوكول النقل بكلمة سر تُستخدم لمرة واحدة، التوصية [ISO/IEC 11770-3]؛
2) الفقرة 2.D: أمن طبقة النقل من خلال مفتاح عمومي غير معالج، التوصية [IETF RFC 8446]؛
3) الفقرة 3.D: أمن طبقة النقل لبروتوكول الاستيقان القابل للتوسع، التوصية [IETF RFC 5216]؛
4) الفقرة 4.D: البروتوكول EAP-PSK، التوصية [IETF RFC 4764IETF RFC 4764].

9 المتطلبات الأمنية

لا تركز هذه التوصية إلا على المتطلبات الأمنية لاستخدام التجفير القائم على الهوية في إنترنت الأشياء. ويرد في التوصية [b-ITU-T X.1361] توصيف التهديدات والمتطلبات الأمنية العامة من أجل إنترنت الأشياء. وباعتباره نظام تجفير، تكمن الشواغل الأمنية الكبرى في سلامة والمفاتيح العمومية المستخدمة واستيقانها وسرية المفاتيح السرية المستخدمة طويلة الأجل والمؤقتة. ويتضمن نظام التجفير القائم على الهوية المكونات التالية: مفتاح السر الرئيسي، والمعلمات العمومية، ومعرِّفات الهوية، والمفاتيح الخاصة، والأسرار المؤقتة المستخدمة في العمليات التجفيرية.

1.9 المتطلبات الأمنية بشأن مفتاح السر الرئيسي

تتولد كل المفاتيح الخاصة من مفتاح السر الرئيسي. وعلى وجه الخصوص، إذا تعرض مفتاح السر الرئيسي للخطر، فإن الخصم تكون لديه القدرة على إعادة إنشاء المفتاح الخاص لأي كيان، ومن ثم يمكنه فك تجفير جميع الرسائل المحمية بالمفتاح العمومي المقابل أو انتحال شخصية أي كيان. ومن شأن أي نفاذ غير قانوني إلى مفتاح السر الرئيسي أن يعرض أمن نظام التجفير القائم على الهوية للخطر. وعليه، يجب تخزين مفتاح السر الرئيسي في بيئة محصنة مثل وحدة أمن العتاد (HSM). وأي نفاذ إلى المفتاح يجب أن يستيقن عبر آليات أمنية قوية.

2.9 المتطلبات الأمنية بشأن المعلمات العمومية

يُحسَب المفتاح العمومي من المعلمات العمومية ومن هوية عن طريق العملية **IBDerivate**. وبالتالي، فإن من شأن استعمال مجموعة زائفة من المعلمات العمومية التي يولدها خصم من أجل تجفير رسالة ما أو التحقق من توقيع ما سيؤدي إلى تعريض سرية الرسالة المجفرة للخطر أو التوصل إلى استنتاج خاطئ عن مُصدِر التوقيع. ومن ثم، يجب نقل المعلمات العمومية من خلال قناة مؤمنة أو بتوقيع صالح. ويجب أن يتحقق الكيان من الكيان النظير التي تتبعه القناة المؤمنة أو من صلاحية التوقيع فيما يتعلق بأي مفتاح عمومي موثوق قبل قبول المعلمات العمومية.

3.9 المتطلبات الأمنية بشأن معرِّف الهوية

كل كيان يمتلك معرِّف هوية في إنترنت الأشياء. وإذا وُزع نفس معرِّف الهوية على أكثر من كيان وزُوِّد كل كيان من هذه الكيانات بالمفتاح الخاص المقابل، فإنه قد يؤدي ذلك إلى تسريب معلومات حساسة أو وقوع هجمات انتحال الهوية. ولذا، يجب أن يُوزَّع لكل جهاز معرِّف هوية فريد.

4.9 المتطلبات الأمنية بشأن المفتاح الخاص

يمكن أن يسرَّب المفتاح الخاص إذا تعرضت البيئة الأمنية لجهاز إنترنت الأشياء للخطر. ولذلك، يجب أن يُوزَّع المفتاح الخاص عبر قناة مؤمنة ويخزن في بيئة مؤمنة.

5.9 المتطلبات الأمنية بشأن الأسرار المؤقتة

يمكن تسرب الأسرار المؤقتة، مثل السر العشوائي المستخدم في عمليات التجفير أو التوقيع، إذا تعرضت البيئة الأمنية لجهاز إنترنت الأشياء للخطر. ولذلك، يجب ضمان عشوائية هذه الأسرار المؤقتة.

الملحق A

الصياغة العامة للتجفير القائم على الهوية وخوارزمياته

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية.)

يعطي هذا الملحق صياغة عامة للتجفير القائم على الهوية ويوفر قائمة بخوارزميات التجفير القائم على الهوية المدعومة في هذه التوصية. أما الخوارزميات التي تتبع هذه الصياغة العامة، ولكنها غير المدرجة أدناه، فيمكن إدراجها أيضاً في المستقبل بسهولة كامتدادات لهذا الإطار. كما توجه الصياغة العامة المحددة هنا أوصاف بنى بيانات المفاتيح وعمليات إدارة المفاتيح ذات الصلة، فضلاً عن بروتوكولات الاستيقان وإنشاء المفاتيح المعرَّفة في الملحقات A حتى D.

ويتضمن نظام التجفير الخاص بالتجفير القائم على الهوية الأنواع التالية من بيانات المفاتيح، حيث يتبع تصنيف هذه المفاتيح المعيار [ISO/IEC 18033-5]:

- *ib.msk*: مفتاح السر الرئيسي هو القيمة السرية التي تستخدمها خدمة إدارة المفاتيح لحساب مفتاح خاص على أساس الهوية. ويتولد المفتاح *ib.msk* خلال عملية تدميث النظام وهو غير معلوم إلا لخدمة إدارة المفاتيح؛
- *ib.mpk*: هو المفتاح العمومي الرئيسي الذي يحدد بشكل فريد بواسطة مفتاح السر الرئيسي المقابل. وتحسب خدمة إدارة المفاتيح المفتاح *ib.mpk* خلال عملية تدميث النظام؛
- *ib.sysparam*: معلمات النظام من أجل حساب التجفير بما في ذلك اختيار مخطط تجفير بعينه أو وظيفة تجفير معينة من عائلة مخططات أو وظائف التجفير، أو من عائلة من الفضاءات الرياضية. وتختار خدمة إدارة المفاتيح المعلمات *ib.sysparam* خلال عملية تدميث النظام؛
- *ib.pubparam*: المعلمات العمومية هي مزيج من معلمات النظام *ib.sysparam* مع المفتاح العمومي الرئيسي *ib.mpk*. ويعرف هذا النوع من المفاتيح لتقديم رؤية موحدة فيما بين المعايير الدولية مثل المعيار [ISO/IEC 18033-5] وطلبات تقديم التعليقات المتعلقة بالتجفير القائم على الهوية مثل [IETF RFC 5091]؛
- *ib.prk*: المفتاح الخاص القائم على الهوية، والذي تولده خدمة إدارة المفاتيح باستخدام المفتاح *ib.msk* والمعلمات العمومية *ib.pubparam* المقابلين لمعرِّف الهوية؛
- *ib.pub*: المفتاح العمومي القائم على الهوية، والذي يُحسب من معرِّف الهوية والمعلمات العمومية *ib.pubparam* من خلال وظيفة يحددها مخطط تجفير قائم على الهوية.

وقد يتضمن نظام التجفير الخاص بالتجفير القائم على الوظائف التالية التي توصف بمدخلات ومخرجات:

الوظيفة IBSetup

الدخل: معلمة أمنية

الخرج: *ib.pubparam*، *ib.msk*

الوظيفة IBExtract

الدخل: *ib.pubparam*، *ib.msk*، *معرِّف الهوية (ID)*

الخرج: *ib.prk*

الوظيفة IBDerivate

الدخل: *ib.pubparam*، *معرِّف الهوية (ID)*

الخرج: *ib.puk*

الوظيفة IBEnc

الدخل: *ib.pubparam*، *معرِّف الهوية (ID)*، الرسالة *M*

الخرج: النص التجفيري *C*

الوظيفة IBDec

الدخل: *ib.pubparam*، *معرِّف الهوية (ID)*، *ib.prk*، النص التجفيري *C*

الخرج: نص بسيط *M* أو خطأ

الوظيفة IBSign

الدخل: *ib.pubparam*، *معرِّف الهوية (ID)*، *ib.prk*، الرسالة *M*

الخرج: التوقيع *S*

الوظيفة IBVerify

الدخل: *ib.pubparam*، *معرِّف الهوية (ID)*، الرسالة *M*، التوقيع *S*

الخرج: صالح أو غير صالح

يجب أن تدعم هذه التوصية استخدام الخوارزميات التالية القائمة على الهوية بما فيها:

- BB1-KEM [IETF RFC 5091] (آلية تغليف المفاتيح (KEM))؛
- BF-IBE [IETF RFC 5091]؛
- SK-KEM [IETF RFC 6508]؛
- SM9-IBE [b-GM/T 0044.2]؛
- Cha-Cheon-IBS (IBS2) [ISO/IEC 14888-3]؛
- ECCSI (التوقيعات المعتمدة القائمة على منحنيات إهليلجية بدون شهادات من أجل التشفير القائم على الهوية) [IETF RFC 6507]؛
- Hess-IBS (IBS1) [ISO/IEC 14888-3]؛
- SM9-IBS (Chinese IBS) [ISO/IEC 14888-3]؛
- Fujioka-Suzuki-Ustaoglu-AKA (اتفاق المفاتيح المستيقنة (AKA)) [ISO/IEC 11770-3]؛
- Smart-Chen-Cheng-AKA [ISO/IEC 11770-3]؛
- SM9-AKA [b-GM/T 0044.2]؛
- Wang-AKA [b-IEEE P1363.3].

وتستند كل هذه الخوارزميات إلى افتراض اللوغاريتم المنفصل ويتم تنفيذها عادةً على مجموعة النقاط على منحنى إهليلجي. ويواصل الكثير من هذه الخوارزميات أيضاً الاستفادة من المزاوجة التجفيرية على منحنى إهليلجي [b-Galbraith]. والمزاوجة التجفيرية e هي خريطة ثنائية الخطية e قابلة للحساب بكفاءة: $G1 \times G2 \rightarrow G3$، محققة المعادلة:

$$e([a]P1, [b]P2) = e(P1, P2)^{a*b}$$

حيث P1 وP2 هما مولدي المجموعتين الدوريتين $G1$ و$G2$، على التوالي. وتشير [a]P1 إلى العدد a من عمليات المجموعات باستخدام المولد P1، وعلى نفس المنوال [b]P2 هي العدد b من عمليات المجموعات باستخدام المولد P2.

ويمكن إنشاء أي مزاوجة تجفيرية عن طريق المزاوجة Weil، والمزاوجة Tate، والمزاوجة Ate المثلى، إلخ.، على منحنيات إهليلجية تسهل مزاوجتها [b-Freeman]. وتتضمن المنحنيات الإهليلجية الشائعة التي تسهل مزاوجتها المنحنيات الإهليلجية فائقة التفرد، ومنحنيات باريتو–نهريغ (BN)، ومنحنيات تضمين باريتو–لين–سكوت درجة 12 (BLS-12)، ومنحنيات تضمين كاتشيزا–شيفر–سكوت درجة 16 (KSS-16)، ومنحنيات تضمين كاتشيزا–لين–سكوت درجة 18 (KSS-18)، ومنحنيات تضمين باريتو–لين–سكوت درجة 24 (BLS-24) [b-Freeman]. وتستند كل هذه المنحنيات E إلى حقل رئيسي، وحقل منته من الرموز الرئيسية p، F_p، حيث p هو عدد صحيح أولي. و$G1$ هي المجموعة الفرعية للنقاط على المنحنى E. و$G2$ هي إما $G1$ نفسها إذا كانت المنحنيات فائقة التفرد هي المستخدمة أو مجموعة فرعية من النقاط على المنحنى المتعرج E. ويُبنى المنحنى المتعرج E من أحد حقول التمديد الخاصة بالحقل الأساسي F_p. و$G3$ هو تمديد الحقل F_p^k الخاص بالحقل الأساسي F_p، حيث k هي درجة التضمين.

وتُبنى خوارزميات التجفير القائم على الهوية بآليات رياضية أخرى مثل الشبيكات؛ على سبيل المثال [b-Ducas]. ويتسم هذا النوع من الخوارزميات بالكفاءة فيما يتعلق بالحوسبة، مع تمتعه بحجم أكبر للمفاتيح والخرج مقارنةً بتلك المستندة إلى اللوغاريتم المنفصل على المنحنيات الإهليلجية. ويُعتقد عموماً أن الخوارزميات مقاومة للهجمات التي تعمل على حواسيب كمومية. إلا أن الخوارزميات التي تندرج تحت هذه الفئة لا تزال قيد التطوير. وعليه، يبدو من المبكر النظر فيها من أجل التقييس، ولكن يجوز النظر في خوارزميات التجفير القائم على الهوية القائمة على الشبيكات هذه من أجل إدراجها مستقبلاً.

الملحق B

تحديد بيانات المفاتيح في التجفير القائم على الهوية

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

باستخدام طريقة معيار ترميز قواعد التركيب المجردة رقم 1، عرف الطلب [IETF RFC5408] بنية عامة لمعلمات النظام، بما في ذلك المعلمات *ib.pubparam* ومعلومات أخرى مساعدة، وعرف الطلب [IETF RFC 5091] مجموعتين من بنى بيانات المفاتيح بما فيها المفتاحان *ib.msk* و*ib.prk* من أجل خوارزميتين للتشفير القائم على الهوية، أي BF-IBE وBB1-IBE. ومع الحفاظ على التوافق مع التعاريف القائمة، توسع هذه التوصية من تعريف معلمة النظام وتعرف بنى بيانات جديدة لدعم المزيد من الخوارزميات وعمليات التنفيذ المتنوعة ذات الكفاءة باستخدام منحنيات ومزاوجات مختلفة.

وفيما يلي تعريف بنية معلمة النظام العامة.

```
IBSysParams ::= SEQUENCE {
        version                 INTEGER { v3(3) },
        domainName              IA5String,
        domainSerial            INTEGER,
        validity                ValidityPeriod,
        ibPublicParameters      IBPublicParameters,
        ibIdentityType          OBJECT IDENTIFIER,
        ibParamExtensions       [0] IMPLICIT IBParamExtensions OPTIONAL,
        signatureAlgorithm      [1] IMPLICIT AlgorithmIdentifier OPTIONAL,
        signature               [2] IMPLICIT BIT STRING OPTIONAL
}
```

ويقابل IBSysParams تعريف IBESysParams في الطلب [IETF RFC 5408]، مع تغيير الإصدار إلى v3 (3) وإضافة حقلين إضافيين. وتم تغيير اسم districtName وdistrictSerial ليصبحا domainName وdomainSerial، على التوالي. وقد تم تعديل تعريف IBPublicParameter من النمط OCTET STRING إلى النمط المعرف حديثاً IBParameterData، والذي هي اختيار (CHOICE) محدد بقيمة الخوارزمية pkgAlgorithm. ويزيل هذا التعريف أي تجفير مزدوج غير ضروري يتسبب فيه التعريف السابق، وتحديداً، تجفير البيانات publicParameterData باعتبارها **تتابعاً** (SEQUENCE) مثل BFPublicParameters، مثل، ومواصلة تجفير النتيجة باعتبارها سلسلة OCTET STRING. وباستثناء الحقلين الجديدين، يظل معنى الحقول الأخرى دون تغيير كما في الطلب [IETF RFC 5408]. وفيما يلي معنى الحقلين الجديدين:

- تحدد الخوارزمية Signature Algorithm خوارزمية التوقيع المستخدمة لإنشاء قيمة التوقيع. وهذا الحقل اختياري، لأن حقل التوقيع ليس إجبارياً.
- يحتوي حقل التوقيع على التوقيع الرقمي المحوسب بناءً على نتائج قواعد التجفير المميزة (DER) في إطار الترميز ASN.1 من نسخة الحقل إلى التمديدات *ibParamExtensions*. ويجفر هذا الحقل باعتباره سلسلة BIT STRING وهو اختياري.

وإذا تواجد حقل التوقيع، فإنه يُستعمل لمساعدة أي كيان على فحص استيقان المعلمات العمومية للنظام دون اللجوء لأي أساليب أخرى. فعلى سبيل المثال، إذا لم تكن لجهاز إنترنت الأشياء القدرة على إنشاء قناة مؤمنة قائمة على أمن طبقة النقل حسبما يقتضيه الطلب [IETF RFC 5408] لاسترجاع المعلمات العمومية لنظام آخر للتجفير القائم على الهوية، فقد يستفسر عن اختيار البروتوكول والمعلمات (PPS) الخاص به عن طريق بروتوكول نقل النصوص الترابطية (HTTP). وفي هذه الحالة، يجب أن يوقع كيان

اختيار البروتوكول والمعلمات PPS المعلمات العمومية المطلوبة بمفتاحه الخاص بالتوقيع. ويمكن لجهاز إنترنت الأشياء التحقق من التوقيع للتحقق من استيقان الرد. وإذا كان اختيار البروتوكول والمعلمات ينشر المعلمات العمومية الخاصة بنظام آخر للتجفير القائم على الهوية على كياناته العاملة، يوصى بمعاملة رسالة التوقيع كهوية وأن تستخدم الخوارزمية **IBExtract** كخوارزمية توقيع لتوليد المفتاح الخاص باعتباره قيمة مقابلة للتوقيع. وبذلك، تتحقق أجهزة إنترنت الأشياء مما إذا كانت قيمة التوقيع هي مفتاح خاص صالح مقابل لنتيجة قواعد التجفير المميزة في إطار الترميز ASN.1 من نسخة الحقل إلى التمديدات *ibParamExtensions* وأنها لا تحتاج إلى مفتاح عمومي للتحقق الإضافي من أجل التحقق من التوقيع.

```
ValidityPeriod ::= SEQUENCE {
        notBefore       GeneralizedTime,
        notAfter        GeneralizedTime
}
IBPublicParameters ::= SEQUENCE SIZE (1..MAX) OF IBPublicParameter
IBPublicParameter ::= SEQUENCE {
        pkgAlgorithm                OBJECT IDENTIFIER,
        publicParameterData         IBParameterData
}
```

وتتحدد قيمة publicParameterData عن طريق pkgAlgorithm. ويمكن أن تكون أحد الخيارات التالية.

```
IBParameterData ::= CHOICE {
        bb1ParameterData        [0] IMPLICIT BB1PublicParameters,
        bfParameterData         [1] IMPLICIT BFPublicParameters,
        eccsiParameterData      [2] IMPLICIT ECCSIPublicParameters,
        skParameterData         [3] IMPLICIT SKPublicParameters,
        sm9ParameterData        [4] IMPLICIT SM9PublicParameters
}
IBParamExtensions ::= SEQUENCE OF IBParamExtension
IBParamExtension ::= SEQUENCE {
        ibParamExtensionOID OBJECT IDENTIFIER,
        ibParamExtensionValue           OCTET STRING
}
AlgorithmIdentifier ::= SEQUENCE {
        algorithm           OBJECT IDENTIFIER,
        parameters          ANY DEFINED BY algorithm OPTIONAL
}
```

ويتضمن الطلب [IETF RFC 5091] مجموعتين من مفاتيح السر الرئيسية، والمعلمات العمومية، ومجموعة مفاتيح خاصة، أي:

- BB1MasterSecret وBB1PublicParameters وBB1PrivateKeyBlock؛
- BFMasterSecret وBFPublicParameters وBFPrivateKeyBlock من أجل وظيفة إنشاء مفتاح BF وBB1.

ولا تناسب هذه التسميات سوى تنفيذ الوظائف ذات المزاوجات المتناظرة على منحنيات إهليلجية فائقة التفرد معرفة على حقول أولية. وتوصف هذه التوصية بنى جديدة مع تغيير الإصدار إلى v3 لدعم عمليات تنفيذ هذه الخوارزميات بمزاوجات غير متناظرة. وبالنسبة للمزاوجات المتناظرة على منحنيات إهليلجية فائقة التفرد، يظل الحقل المقابل في بنى بيانات

المفاتيح BB1 وBF دون تغيير كما في الطلب [IETF RFC 5091]. وفيما يلي ثلاثة مجموعات أخرى من بنى بيانات المفاتيح معرفة من أجل التوقيعات المعتمدة القائمة على منحنيات إهليلجية بدون شهادات من أجل التشفير القائم على الهوية وSM9 وSK-KEM، على التوالي؛

```
BB1MasterSecret ::= SEQUENCE {
        version         INTEGER { v3(3) },
        alpha           INTEGER,
        beta        INTEGER,
        gamma           INTEGER
}
```

- ولعمليات التنفيذ ذات المزاوجات غير المتناظرة، يجب ضبط alpha على s1، وbeta على s2، وgamma على s3 في الفقرة 3.9 من المعيار [ISO IEC 18033-5]؛

```
BB1PublicParameters ::= SEQUENCE {
        version         INTEGER { v3(3) },
        curve           OBJECT IDENTIFIER,
        hashfcn         OBJECT IDENTIFIER,
        pairing         PAIRING OPTIONAL,
        p               INTEGER OPTIONAL,
        q               [0] IMPLICIT INTEGER OPTIONAL,
        pointP          FpPoint,
        pointQ          [1] EXPLICIT FpxPoint OPTIONAL
        pointP1         FpPoint,
        pointP2         [2] EXPLICIT FpxPoint OPTIONAL,
        pointP3         FpPoint,
        v               FpxElement
}
```

- توصف المزاوجة أي نوع من الخرائط ثنائية الخطية يجب أن يُستخدم مع المعلمات المتولدة. ويتم دعم ثلاثة أنواع من المزاوجات: مزاوجة Weil، ومزاوجة Tate، ومزاوجة Ate المثلى.
- تصبح القيمتان p وq اختياريتين. وبالنسبة لبعض أنواع المنحنيات، مثل BN وBLS-12، إلخ، يتم تحديد القيمتين p وq مسبقاً عن طريق معرِّفات هوية غرض (OID) المنحنى، ومن ثم، من غير الضروري تحديدهما مجدداً.
- يجب أن تكون النقطتان pointP وpointQ، لأغراض التنفيذ مع المزاوجات غير المتناظرة، Q1 في $G1$ وQ2 في $G2$ في الفقرة 3.9 من المعيار [ISO IEC 18033-5]. وبالنسبة للمزاوجات المتناظرة، تتساوى النقطتان pointP مع pointQ، وبالتالي تصبح النقطة pointQ اختيارية.
- يجب أن تكون النقطتان PointP1 وPointP3، لأغراض التنفيذ مع المزاوجات غير المتناظرة، R وT في الفقرة 3.9 من المعيار [ISO/IEC 18033-5].
- تتخذ النقطة pointP2، لأغراض التنفيذ مع المزاوجات غير المتناظرة مثل مزاوجة Ate المثلى على منحنيات BN، قيمة من حقل تمديد الحقل الأساسي F_p. وتصبح النقطة pointP2 اختيارية لأنه إذا كانت القيمة v معطاة، تصبح النقطة pointP2 غير لازمة لتنفيذ لخوارزمية BB1-KEM.

- القيمة v هي نتيجة المزاوجة، وهي أحد عناصر حقل تمديد الحقل الرئيسي F_p. ولأغراض التنفيذ مع المزاوجات غير المتناظرة، مثل مزاوجة Ate المثلى على منحنيات BN، يكون حقل التمديد F_p^k، حيث k هي درجة التضمين. وفي هذه الحالة، يجب أن تكون v هي J في الفقرة 3.9 من المعيار [ISO/IEC 18033-5].
- يظل معنى الحقول الأخرى دون تغيير كما في الطلب [IETF RFC 5091].

```
PAIRING ::= ENUMERATED {
        weil        (1),    --Weil pairing
        tate        (2),    --Tate pairing
        optimalAte  (3)     --Optimal Ate pairing
}
FpPoint ::= SEQUENCE {
        x   INTEGER,
        y   INTEGER
}
```

تعرف النقطة FpPoint نقطة على منحنى إهليلجي على حقل أولي. وللنقطة إحداثيان، هما الإحداث x والإحداث y. وللإحداثيين قيم لأعداد صحيحة كبيرة.

```
FpxPoint ::= CHOICE {
        fpPoint   [1] EXPLICIT FpPoint,
        fp2Point      [2] EXPLICIT Fp2Point,
        fp3Point      [3] EXPLICIT Fp3Point,
        fp4Point      [4] EXPLICIT Fp4Point
}
```

- تعرف النقطة Fp2Point نقطة على منحنى إهليلجي على الحقل F_p^2. وكل إحداث لنقطة ما يتخذ قيمة من أحد عناصر الحقل F_p^2.
- تعرف النقطة Fp3Point نقطة على منحنى إهليلجي على الحقل F_p^3. وكل إحداث لنقطة ما يتخذ قيمة من أحد عناصر الحقل F_p^3.
- تعرف النقطة Fp4Point نقطة على منحنى إهليلجي على الحقل F_p^4. وكل إحداث لنقطة ما يتخذ قيمة من أحد عناصر الحقل F_p^4.

```
Fp2Point ::= SEQUENCE {
        x   Fp2Element,
        y   Fp2Element
}
```

- تعرف النقطة Fp2Point نقطة على منحنى إهليلجي على الحقل F_p^2. وللنقطة إحداثيان، هما الإحداث x والإحداث y. وللإحداثيين قيم من الحقل F_p^2.

```
Fp3Point ::= SEQUENCE {
        x   Fp3Element,
        y   Fp3Element
}
```

- تعرف النقطة Fp3Point نقطة على منحنى إهليلجي على الحقل F_p^3. وللنقطة إحداثيان، هما الإحداث x والإحداث y. وللإحداثيين قيم من الحقل F_p^3.

```
Fp4Point ::= SEQUENCE {
        x    Fp4Element,
        y    Fp4Element
}
```

- تعرف النقطة Fp4Point نقطة على منحنى إهليلجي على الحقل F_p^4. وللنقطة إحداثيان، هما الإحداث x والإحداث y. وللإحداثيين قيم من الحقل F_p^4.

```
Fp2Element ::= SEQUENCE {
        a    INTEGER,
        b    INTEGER
}
```

- يعرف العنصر Fp2Element أحد عناصر الحقل F_p^2، الممثلة بالمعادلة a+bα حيث α هي جذر غير تربيعي في الحقل F_p.

```
Fp3Element ::= SEQUENCE {
        a    INTEGER,
        b    INTEGER,
        c    INTEGER
}
```

- يعرف العنصر Fp3Element أحد عناصر الحقل F_p^3، الممثلة بالمعادلة a+bβ+cβ^2 حيث β هي جذر غير تكعيبي في الحقل F_p.

```
Fp4Element ::= SEQUENCE {
        a    Fp2Element,
        b    Fp2Element
}
```

- يعرف العنصر Fp4Element أحد عناصر الحقل F_p^4، والممثلة كبرج من عنصرين من الحقل F_p^2.

```
FpxElement ::= CHOICE {
        fp2Elemt     [1] EXPLICIT Fp2Element,
                     --for super singular elliptic curve implementation
        fp12Elemt    [2] EXPLICIT Fp12Element,
                     --using F_p->F_p^2->F_p^6->F_p^12 tower representation
        fp16Elemt    [3] EXPLICIT Fp16Element,
                     --using F_p->F_p^2->F_p^4->F_p^8->F_p^16 tower representation
        fp18Elemt    [4] EXPLICIT Fp18Element,
                     --using F_p->F_p^3->F_p^6->F_p^18 tower representation
        fp24Elemt    [5] EXPLICIT Fp24Element
                     --using F_p->F_p^2->F_p^6->F_p^12->F_p^24 tower representation
}
```

- يعرف العنصر FpxElement التمثيل البرجي لأحد العناصر في $G3$. وتقابل المزاوجة e مدخلين من $G1$ و$G2$، على التوالي مع أحد العناصر في $G3$. ولأغراض المنحنيات شائعة الاستخدام والتي تسهل مزاوجتها، تمثَّل العناصر في $G3$ عادة بأسلوب برجي. وبالنسبة لدرجات التضمين المختلفة، قد توجد تمثيلات برجية مختلفة. وتعرف هذه التوصية تمثيلاً برجياً شائع الاستخدام لعناصر في حقل مع درجات تضمين 12 و16 و18 و24.

```
Fp12Element ::= SEQUENCE {
        a    Fp6Element,
        b    Fp6Element
}
```

- يعرف العنصر Fp12Element أحد عناصر الحقل F_p^12 بتمثيل برجي بالنسق 2x3x2 ويجب استخدامه في التنفيذ بمنحنيات BN أو منحنيات BLS-12 أو منحنيات BLS-24.

```
Fp6Element ::= SEQUENCE {
        a    Fp2Element,
        b    Fp2Element,
        c    Fp2Element
}
```

- يعرف العنصر Fp6Element أحد عناصر الحقل F_p^6 بتمثيل برجي بالنسق 3x2 ويجب استخدامه في التنفيذ بمنحنيات BN أو منحنيات BLS-12 أو منحنيات BLS-24.

```
Fp16Element ::= SEQUENCE {
        a    Fp8Element,
        b    Fp8Element
}
```

- يعرف العنصر Fp16Element أحد عناصر الحقل F_p^16 بتمثيل برجي بالنسق 2x2x2x2 ويجب استخدامه في التنفيذ بمنحنيات KSS-16.

```
Fp8Element ::= SEQUENCE {
        a    Fp4Element,
        b    Fp4Element
}
```

- يعرف العنصر Fp8Element أحد عناصر الحقل F_p^8 بتمثيل برجي بالنسق 2x2x2 ويجب استخدامه في التنفيذ بمنحنيات KSS-16.

```
Fp18Element ::= SEQUENCE {
        a    Fp6bElement,
        b    Fp6bElement,
        c    Fp6bElement
}
```

- يعرف العنصر Fp18Element أحد عناصر الحقل F_p^18 بتمثيل برجي بالنسق 3x2x3 ويجب استخدامه في التنفيذ بمنحنيات KSS-18.

```
Fp6bElement ::= SEQUENCE {
        a    Fp3Element,
```

```
        b    Fp3Element
}
```

- يعرف العنصر Fp6bElement أحد عناصر الحقل F_p^6 بتمثيل برجي بالنسق 2x3 ويجب استخدامه في التنفيذ بمنحنيات KSS-18.

```
Fp24Element ::= SEQUENCE {
        a    Fp12Element,
        b    Fp12Element
}
```

- يعرف العنصر Fp24Element أحد عناصر الحقل F_p^24 بتمثيل برجي بالنسق 2x2x3x2 ويجب استخدامه في التنفيذ بمنحنيات BLS-24.

```
BB1PrivateKeyBlock ::= SEQUENCE {
        version        INTEGER { v3(3) },
        pointD0 FpxPoint,
        pointD1 FpxPoint
}
```

- يظل معنى النقطتين pointD0 وpointD1 دون تغيير كما في الطلب [IETF RFC 5091]، ولكن يتم أخذه من G2 إذا تم تنفيذ BB1-KEM بمزاوجات غير متناظرة. وفي هذه الحالة يجب أن تكون النقطتان pointD0 وpointD1، dID0 وdID1 على التوالي في الفقرة 3.9 من المعيار [ISO/IEC 18033-5].

```
BFMasterSecret ::= SEQUENCE {
        version            INTEGER {v3(3) },
        masterSecret INTEGER
}
```

- يظل معنى كل حقل دون تغيير كما في الطلب [IETF RFC 5091].

```
BFPublicParameters ::= SEQUENCE {
        version        INTEGER { v3(3) },
        curve          OBJECT IDENTIFIER,
        hashfcn        OBJECT IDENTIFIER,
        pairing        PAIRING OPTIONAL,
        p              INTEGER OPTIONAL,
        q              [0] IMPLICIT INTEGER OPTIONAL,
        pointP         FpxPoint,
        pointPpub      FpxPoint
}
```

- يظل معنى كل حقل دون تغيير كما في الطلب [IETF RFC 5091]، ولكن تؤخذ النقطتان pointP وpointPpub من *G*2 إذا تم تنفيذ BF-IBE بمزاوجات غير متناظرة. وفي هذه الحالة، يجب أن تكون النقطتان pointP وpointPpub، Q وR على التوالي في الفقرة 2.8 من المعيار [ISO/IEC 18033-5].

```
BFPrivateKeyBlock ::= SEQUENCE {
        version         INTEGER { v3(3) },
        privateKey      FpPoint
}
```

- يظل معنى كل حقل دون تغيير كما في الطلب [IETF RFC 5091]. ولأغراض عمليات التنفيذ بمزاوجات متناظرة، يجب أن يكون المفتاح privateKey هو skid في الفقرة 2.8 من المعيار [ISO/IEC 18033-5].

```
ECCSIMasterSecret ::= SEQUENCE {
        version         INTEGER {v3(3) },
        masterSecret    INTEGER
}
```

- يجب أن يكون السر masterSecret هو KSAK في الطلب [IETF RFC 6507].

```
ECCSIPublicParameters ::= SEQUENCE {
        version         INTEGER { v2(2) },
        curve           OBJECT IDENTIFIER,
        hashfcn         OBJECT IDENTIFIER,
        pointP          FpPoint,
        pointPpub       FpPoint
}
```

- يجب أن تكون النقطة pointP هي G في الطلب [IETF RFC 6507].
- يجب أن تكون النقطة pointPpub هي مفتاح الاستيقان العمومي لخدمة إدارة المفاتيح (KPAK) في الطلب [IETF RFC 6507].

```
ECCSIPrivateKeyBlock ::= SEQUENCE {
        version         INTEGER { v2(2) },
        ssk             INTEGER ,
        pvt             OCTET STRING
}
```

- يجب أن يكون ssk وpvt مفتاح توقيع سري (SSK) ورمز التحقق العمومي (PVT) في الطلب [IETF RFC 6507]، على التوالي.

```
SKMasterSecret ::= SEQUENCE {
        version         INTEGER {v3(3) },
        masterSecret INTEGER
}
```

- يجب أن يكون masterSecret هو z_T في الطلب [IETF RFC 6508] وs في الفقرة 2.9 من المعيار [ISO/IEC 18033-5].

```
SKPublicParameters ::= SEQUENCE {
        version         INTEGER { v3(3) },
        curve           OBJECT IDENTIFIER,
        hashfcn         OBJECT IDENTIFIER,
        pairing         PAIRING OPTIONAL,
```

```
    p               INTEGER OPTIONAL,
    q               [0] IMPLICIT INTEGER OPTIONAL,
    pointP1         FpPoint,
    pointP1pub      [1] EXPLICIT FpPoint OPTIONAL,
    pointP2         [2] EXPLICIT FpxPoint OPTIONAL,
    pointP2pub      [3] EXPLICIT FpxPoint OPTIONAL,
    v               [4] EXPLICIT FpxElement
}
```

- لأغراض عمليات التنفيذ ذات المزاوجات المتناظرة على منحنيات فائقة التفرد، يرد تعريف p وq في الطلب [IETF RFC 5091]. ولأغراض عمليات التنفيذ ذات المزاوجات غير المتناظرة، يتم تحديد p وq مسبقاً عن طريق المنحنى المستخدم وتصبحان اختياريين.
- يجب أن تكون النقطة pointP1 هي P في الطلب [IETF RFC 6508] وQ1 في G1 في الفقرة 2.9 من المعيار [ISO/IEC 18033-5].
- يجب أن تكون النقطة pointP1pub هي Z_T في الطلب [IETF RFC 6508] وR في الفقرة 2.9 من المعيار [ISO/IEC 18033-5]. وقد تصبح النقطة pointP1pub غير ضرورية بالنسبة لخوارزميات أخرى، مثل خوارزميات التوقيع، بناءً على وظيفة توليد المفتاح ساكاي–كاساهارا (SK)، وبالتالي فهي اختيارية.
- يجب أن تكون النقطة pointP2 هي Q2 في G2 في الفقرة 2.9 من المعيار [ISO/IEC 18033-5] إذا تم تنفيذ SK-KEM باستخدام مزاوجات غير متناظرة. والنقطة pointP2 ليست ضرورية لتنفيذ SK-KEM، ومن ثم فهي اختيارية.
- يجب أن تكون النقطة pointP2pub هي Q2[*ib.msk*]، وهي غير ضرورية لتنفيذ SK-KEM ، ولكنها قد تكون ضرورية لخوارزميات أخرى، مثل خوارزميات التوقيع، بناءً على وظيفة توليد المفتاح SK، وبالتالي فهي اختيارية.

```
SKPrivateKeyBlock ::= SEQUENCE {
    version         INTEGER { v3(3) },
    privateKey      FpxPoint
}
```

- يجب أن يكون المفتاح privateKey هو RSK في الطلب [IETF RFC 6508] وskID في الفقرة 2.9 من المعيار [ISO/IEC 18033-5].

```
SM9MasterSecret ::= SEQUENCE {
    version         INTEGER {v3(3) },
    masterSecret    INTEGER
}
```

- يجب أن يكون السر masterSecret هو *ib.msk* والذي هو الرمز U المعرف في الفقرة 4.7 من المعيار [b-ISO/IEC 14888-3a].

```
SM9PublicParameters ::= SEQUENCE {
    version         INTEGER { v3(3) },
    curve           OBJECT IDENTIFIER,
    hashfcn         OBJECT IDENTIFIER,
    pairing         PAIRING OPTIONAL,
    p               INTEGER OPTIONAL,
```

```
        q               [0] IMPLICIT INTEGER OPTIONAL,
        pointP1         FpPoint,
        pointP1pub      [1] EXPLICIT FpPoint OPTIONAL,
        pointP2         [2] EXPLICIT FpxPoint OPTIONAL,
        pointP2pub      [3] EXPLICIT FpxPoint OPTIONAL,
        v               [4] EXPLICIT FpxElement
}
```

- لأغراض عمليات التنفيذ ذات المزاوجات المتناظرة على منحنيات فائقة التفرد، يرد تعريف p وq في الطلب [IETF RFC 5091]. ولأغراض عمليات التنفيذ ذات المزاوجات غير المتناظرة، يتم تحديد p وq مسبقاً عن طريق المنحنى المستخدم.
- يجب أن تكون النقطة pointP1 هي P في الفقرة 4.7 من المعيار [ISO/IEC 14888-3].
- النقطة pointP1pub غير ضرورية بالنسبة إلى SM9-IBS، ولكنها ضرورية بالنسبة إلى **SM9-IBE** وفي هذه الحالة، يجب أن تكون النقطة pointP2pub هي P[*ib.msk*].
- يجب أن تكون النقطة pointP2 هي Q في الفقرة 4.7 من الطلب [ISO/IEC 14888-3]. والنقطة pointP2 ليست ضرورية لتنفيذ **SM9-IBE**، وبالتالي فهي اختيارية.
- يجب أن تكون النقطة pointP2pub هي V في الفقرة 4.7 من المعيار [ISO/IEC 14888-3a]. والنقطة pointP2pub ليست ضرورية لتنفيذ **SM9-IBE**، وبالتالي فهي اختيارية.

```
SM9PrivateKeyBlock ::= SEQUENCE {
        version         INTEGER { v3(3) },
        privateKey      FpxPoint
}
```

- يجب أن يكون المفتاح privateKey هو X ف الفقرة 4.7 من المعيار [ISO/IEC 14888-3a] من أجل التوقيع، ويجب أن يكون *ib.prvk* في *G1* من أجل SM9-IBE وSM9-AKA.

ويجب استخدام تعريف BFMasterSecret وBFPublicParameters وBFPrivateKeyBlock من أجل الخوارزميات التي تستخدم وظيفة توليد المفاتيح ساكاي–أوهاغيشي–كاساهارا (SOK) مثل BF-IBE وCha-Cheon-IBS وHess-IBS وFujioka-Suzuki-Ustaoglu-AKA وSmart-Chen-Cheng-AKA وWang-AKA. ويجب استخدام تعريف BB1MasterSecret وBB1PublicParameters وBB1PrivateKeyBlock من أجل الخوارزميات التي تستخدم وظيفة توليد المفاتيح BB1 مثل BB1-KEM. ويجب استخدام SKMasterSecret وSKPublicParameters وSKPrivateKeyBlock من أجل SK-KEM وربما من أجل خوارزميات أخرى بناءً على وظيفة توليد المفاتيح ساكاي–كاساهارا (SK). ويجب استخدام SM9MasterSecret وSM9PublicParameters وSM9PrivateKeyBlock من أجل خوارزميات SM9 بما فيها SM9-IBE وSM9-IBS وSM9-AKA. ويجب استخدام ECCSIMasterSecret وECCSIPublicParameters وECCSIPrivateKeyBlock من أجل التوقيعات المعتمدة القائمة على منحنيات إهليلجية من أجل التشفير القائم على الهوية.

وإذا كان المفتاح الخاص بحاجة إلى حماية، يجب استخدام البنية EncryptedPrivateKeyInfo كما هي معرفة في الطلب [IETF RFC 5958].

```
EncryptedPrivateKeyInfo ::= SEQUENCE {
        encryptionAlgorithm     EncryptionAlgorithmIdentifier,
        encryptedData           EncryptedData
}
EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
```

```
EncryptedData ::= OCTET STRING
AlgorithmIdentifier ::= SEQUENCE {
        algorithm       OBJECT IDENTIFIER,
        parameters      ANY DEFINED BY algorithm OPTIONAL
}
```

الملحق C

عمليات إدارة المفاتيح

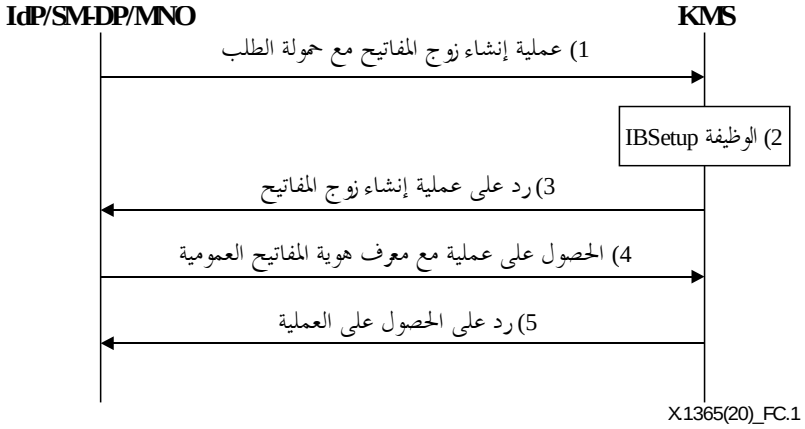
(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية.)

تشمل عمليات إدارة المفاتيح في أي نظام تجفير قائم على الهوية، تدميث النظام وتوفير الهوية أو المفتاح الخاص أو إبطال الهوية أو المفتاح الخاص ونشر معلمات النظام. وتشمل عملية تدميث النظام خطوة لاستدعاء الوظيفة **IBSetup**، وتشمل عملية توفير المفتاح الخاص خطوة لاستدعاء الوظيفة **IBExtract**. وتتطلب هذه العمليات التفاعل بين كيان الإدارة وخدمة إدارة المفاتيح. وتستخدم هذه التوصية بروتوكول قابلية التشغيل البيني لإدارة المفاتيح من أجل تبادل الرسائل بين هذين الطرفين. ويُحدد التمديد اللازم للوفاء بالمتطلبات الجديدة للخوارزميتين **IBSetup** و**IBExtract** المدعومتين ويمكن الاطلاع عليه في التذييل II. وتُعرّف بروتوكولات التفاعل بين وحدات إدارة الأمن وكيانات الإدارة استناداً إلى بروتوكول نقل النصوص الترابطية فيما يتعلق بأجهزة إنترنت الأشياء غير المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة. وبالنسبة للأجهزة المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة، تُستخدم المعايير [b-GSMA SGP.02] ويتم تمديدها عند اللزوم.

1.C تدميث النظام

في كل نظام تجفير قائم على الهوية، ينبغي استكمال عملية تدميث النظام قبل توفير خدمات إدارة المفاتيح لمستعمليها. وفي هذه العملية، تنفذ خدمة إدارة المفاتيح وظيفة أو أكثر من الوظائف **IBSetup** لتوليد مجموعة أو أكثر من أزواج المفاتيح *ib.msk* و*ib.pubparam*. وكممارسة جيدة، يجب توليد المفتاح *ib.msk* وتخزينه في وحدة أمن العتاد. وإن أمكن، يمكن نشر مخطط توليد المفاتيح الموزع الذي يطبق نظام تقاسم الأسرار لتقسيم المفتاح *ib.msk* ونشر أجزاء الأسرار ووظيفة توليد المفاتيح الخاصة عبر العديد من خدمات إدارة المفاتيح. وفي هذه الحالة، لا يمكن توليد مفتاح خاص مقابل لمعرّف هوية توليداً صحيحاً إلا إذا كان هناك أكثر من عدد محدد من خدمات إدارة المفاتيح يعمل بشكل مناسب.

انظر الشكل 1.C.



الشكل 1.C – تدميث النظام باستعمال بروتوكول قابلية التشغيل البيني لإدارة المفاتيح

شروط البداية:

يُفترض أن الكيان IdP/SM-DP/MNO يؤدي دور وحدة تدميث النظام ويتولى مسؤولية عملية تدميث النظام. وقبل أن يتمكن الكيان IdP/SM-DP/MNO من استدعاء الوظيفة **IBSetup** في خدمة إدارة المفاتيح، ينبغي استيفاء الشروط التالية.

أ) وجود قناة مؤمنة قائمة بين الكيان IdP/SM-DP/MNO وخدمة إدارة المفاتيح.

ب) استكمال الكيان IdP/SM-DP/MNO لعملية استيقان مع الخدمة KMS، ويُخول للكيان IdP/SM-DP/MNO المستقين منه تقديم طلب الوظيفة **IBSetup**.

الإجراء:

1) يقوم الكيان IdP/SM-DP/MNO بإعداد حمولة الطلب واستدعاء عملية إنشاء زوج المفاتيح لإرسال رسالة الطلب المشفرة إلى الخدمة KMS؛

2) تتحقق الخدمة KMS من صلاحية الطلب ويُخول للكيان IdP/SM-DP/MNO استدعاء هذه العملية. وإذا لم يُستوف أحد هذين الشرطين، عندئذ تعيد الخدمة KMS رداً يشير إلى فشل. وخلاف ذلك، تنفذ الخدمة الوظيفة **IBSetup** باستعمال معلمات محددة ضمن الطلب؛

3) تعيد الخدمة KMS إلى الكيان IdP/SM-DP/MNO رد التنفيذ. وإذا تكللت العملية بالنجاح، عندئذ، تقوم الخدمة KMS على أقل تقدير بإعادة معرِّف هوية فريد لمفتاح خاص إلى المفتاح *ib.msk* ومعرِّف هوية فريد لمفتاح عمومي إلى المعلمات *ib.pubparam*، على التوالي؛

4) اختيارياً، إذا نجحت عملية إنشاء زوج المفاتيح، قد يستدعي الكيان IdP/SM-DP/MNO عملية الاستحواذ من خلال معرِّف الهوية الفريد للمفتاح العمومي الذي يتم الحصول عليه من الرد الأخير لاستعادة المعلمات العمومية *ib.pubparam*؛

5) تعيد خدمة إدارة المفاتيح قيمة مفتاح المعلمات العمومية المولدة حديثاً.

يمكن الاطلاع على تمديد بروتوكول قابلية التشغيل البيني لإدارة المفاتيح لدعم هذه العملية في التذييل II.

شرط النهاية: يتم تدميث خدمة إدارة المفاتيح بنجاح ويكون للكيان IdP/SM-DP/MNO معرِّف الهوية الفريد للمفتاح الخاص ومعرِّف الهوية الفريد للمفتاح العمومي من أجل النفاذ إلى المفتاح المولد MSK *ib.msk* وإلى المعلمات العمومية *ib.pubparam* المولدة، على التوالي. ويستخدم الكيان IdP/SM-DP/MNO معرِّف الهوية الفريد للمفتاح الخاص لاستدعاء عملية التوقيع من أجل توليد المفاتيح الخاصة للهوية ويستخدم معرِّف الهوية الفريد للمفتاح العمومي لاستدعاء عملية الحصول من أجل استعادة المعلمات العمومية.

2.C تدميث الجهاز

تتمثل عملية تدميث الجهاز في إعداد الجهاز من أجل توفير الهوية والمفاتيح. وفيما يخص أجهزة إنترنت الأشياء المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة وأجهزة إنترنت الأشياء الأخرى غير المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة، يتم اتباع إجراءات مختلفة لتدميث الجهاز.

1.2.C الحالة 1: التدميث من أجل الأجهزة المزودة بالبطاقة eUICC

بالنسبة للأجهزة المزودة بالبطاقة eUICC، يتم تنزيل الهوية والمفتاح الخاص key *ib.prk* المقابلين والمعلمات العمومية *ib.sysparam* المقابلة في مواصفة الميدان الأمني لجهة الإصدار (ISD). وبالتالي، فإنه بعد عملية تدميث الجهاز، ينبغي أن تكون البطاقة eUICC جاهزة لإنشاء مواصفة الميدان الأمني للمُصدر. ووفقاً للمعيار [b-GSMA SGP.02]، يجب استكمال عملية التسجيل. وما يلي تكرار للفقرة 1.5.3 من المعيار [b-GSMA SGP.02].

- تسجيل البطاقة eUICC لدى الكيان SM-SR

شرط البداية:

أ) يتم إنتاج البطاقات eUICC وتحميل مواصفة التوفير وتفعيله في شبكة المشغل الخاصة بالتوفير. ويتم اختبار هذه البطاقات وتصبح جاهزة للشحن. ولكل بطاقة eUICC مجموعة معلومات مقابلة مدمجة في البطاقة eUICC (EIS).

الإجراء:

1) يرسل مصنّع البطاقة eUICC (EUM) إلى الكيان SM-SR المختار طلب تسجيل للبطاقة eUICC يتضمن المعلومات المدمجة في البطاقة؛

2) يخزّن الكيان SM-SR المعلومات EIS في قاعدة البيانات الخاصة به، مع اعتبار معرِّف الهوية eUICC-ID (EID) المعلمة الرئيسية؛

3) يؤكد الكيان SM-SR نجاح التسجيل للمصنّع EUM. وتشمل رسالة التأكيد المعرّف EID.

شرط النهاية: تُسجل البطاقة eUICC لدى الكيان SM-SR وتصبح جاهزة لتحميل المواصفة. ويمكن الآن شحنها إلى مصنّع جهاز الاتصالات من آلة إلى آلة.

2.2.C الحالة 2: تدميث أجهزة إنترنت الأشياء غير المزودة ببطاقات الدارة المتكاملة الشاملة المدمجة

بالنسبة إلى أجهزة إنترنت الأشياء غير المزودة ببطاقات الدارة المتكاملة الشاملة المدمجة، يجب استكمال عملية التسجيل التالية.

- تسجيل الوحدة SecM في المركز AuC

شرط البداية:

أ) يتم إنتاج وحدة الأمن ويجب أن يكون جهاز إنترنت الأشياء قادراً على التواصل مع مورد الهوية في شبكة المشغل.

الإجراء:

1) ترسل وحدة الأمن طلب حيازة بيانات لتوفير الوحدة SecM إلى مركز الاستيقان؛

2) يولد مركز الاستيقان معرِّف هوية التوفير PROV.ID وإثبات الاستيقان ذي الصلة (PROV.CRED) من أجل وحدة الأمن مقدمة الطلب؛

3) يرسل مركز الاستيقان معرِّف هوية التوفير PROV.ID والإثبات PROV.CRED إلى وحدة الأمن. ويرسل أيضاً في نفس الرسالة، معرِّف هوية مورد الهوية والقائم بتوريد هوية المفاتيح مفتاحاً عمومياً ذا صلة IdP.PUK أو المعلمة *ib.sysparam* إلى وحدة الأمن إذا كانت هذه الأخيرة غير قادرة على تنفيذ بروتوكول أمن طبقة النقل؛

4) تُخزن وحدة الأمن الإثباتين PROV.ID وPROV.CRED بصورة مؤمنة، وتخزن IdP.ID وIdP.PUK أو *ib.sysparam* في حالة توفيرها. وتؤمن وحدة الأمن الحماية للمعرِّف IdP.ID والمفتاح IdP.PUK أو المعلمة *ib.sysparam* من التغيير المصرح به.

شرط النهاية: تُسجل وحدة الأمن لدى مركز الاستيقان وتصبح جاهزة لتوفير الهوية والمفاتيح.

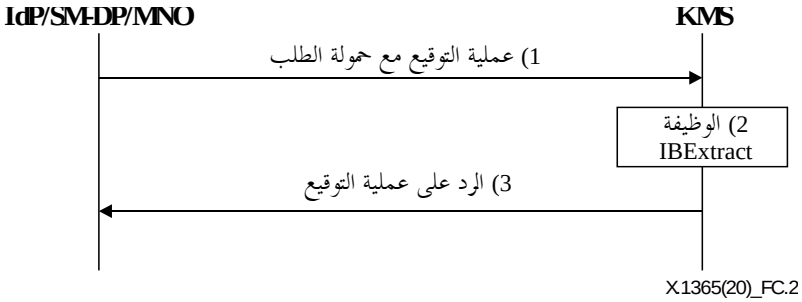
3.C البحث عن المعلمات العمومية

يجب أن يستعمل الكيان إجراء توفير الهوية أو المفاتيح للحصول على المعلمات العمومية من أجل نظام التجفير القائم على الهوية الذي سُجل الكيان من خلاله. ويجب على الكيان الذي يمكن أن يكون جهازاً لإنترنت الأشياء أو كيان إدارة لنظام تجفير قائم على الهوية، أن يتبع المواصفة المحددة في الفقرة 4 من الطلب [IETF RFC 5408] لاسترجاع المعلمات العمومية لنظام IBC آخر من مخدم معلمات عمومية معروف. ويجب الاستعاضة عن المعلمات IBESysParams في الاستجابة الرد الوارد في الطلب [IETF RFC 5408] بالمعلمة IBSysParams المعرّفة في هذه التوصية. ويفترض الطلب [IETF RFC 5408] أن جهاز إنترنت الأشياء المستفسِر بإمكانه إنشاء قناة مؤمنة قائمة على أمن طبقة النقل من خلال مخدم المعلمات العمومية المطلوب. وإذا تعذرت تلبية هذا المطلب، يجب أن تكون الخوارزمية signatureAlgorithm وحقل التوقيع في المعلمات IBSysParams موجودين وصالحين. وبمجرد استرجاع المعلمات IBSysParams، تُتبع عملية سليمة للتحقق من التوقيع، ولا يمكن قبول المعلمات العمومية المسترجعة إلا إذا كان التوقيع الوارد في المعلمات IBSysParams صالحاً والتوقيع الذي يتيح التحقق من المفتاح العمومي مستقيناً منه وصحيحاً.

4.C توفير الهوية والمفاتيح

يشمل توفير الهوية والمفاتيح تخصيص الهوية واستخراج المفتاح الخاص وإجراء وتوزيع المفاتيح. وتُمنح الأجهزة هوية مؤقتة فقط بعد عملية التدميث. ويجب على مورد الهوية أو وظيفة إعداد بيانات مدير الاشتراكات أو مشغل الشبكة المتنقلة تحديد الهوية التي ستُخصص للجهاز الطالب ثم التواصل مع خدمة إدارة المفاتيح لتوليد المفتاح الخاص المقابل وفي نهاية المطاف توزيع الهوية، والمفتاح الخاص، والمعلمات العمومية على الجهاز بصورة مؤمنة.

انظر الشكل 2.C.



الشكل 2.C – توليد المفاتيح الخاصة باستعمال بروتوكول قابلية التشغيل البيني لإدارة المفاتيح

- **توليد المفاتيح العمومية باستعمال بروتوكول قابلية التشغيل البيني لإدارة المفاتيح**

شروط البداية:

يُفترض أن الكيان IdP/SM-DP/MNO يقوم بدور توليد المفتاح الخاص key *ib.prk*. وقبل أن يتمكن الكيان IdP/SM-DP/MNO من استدعاء الوظيفة IBExtract في خدمة إدارة المفاتيح، يجب استيفاء الشرطين التاليين.

أ) وجود قناة مؤمنة بين الكيان IdP/SM-DP/MNO وخدمة إدارة المفاتيح.

ب) استكمال الكيان IdP/SM-DP/MNO لعملية استيقان لخدمة إدارة المفاتيح، ويُخول للكيان IdP/SM-DP/MNO المستقين منه تقديم أداء طلب الوظيفة IBExtract.

الإجراء:

1) يقوم الكيان IdP/SM-DP/MNO بإعداد حمولة الطلب ويستدعي عملية التوقيع لإرسال رسالة الطلب المشفرة إلى خدمة إدارة المفاتيح.

2) تتحقق خدمة إدارة المفاتيح من صلاحية الطلب ومن أن الكيان IdP/SM-DP/MNO مخول لاستدعاء هذه العملية. وإذا لم يُستوف أحد هذين الشرطين، عندئذ تعيد خدمة إدارة المفاتيح رداً يشير إلى فشل. وخلاف ذلك، تقوم خدمة إدارة المفاتيح بتنفيذ الوظيفة **IBExtract** باستعمال المعلمتين *ib.msk* و*ib.pubparam* والمعلمات المحددة في الطلب.

3) تقوم خدمة إدارة المفاتيح بإعادة رد التنفيذ إلى الكيان IdP/SM-DP/MNO. وإذا تكللت العملية بالنجاح، عندئذ، تعيد خدمة إدارة المفاتيح المفتاح الخاص المولَّد *ib.prk* في شكل IBPrivateKeyBlock وهو **خيار** (CHOICE) معرّف بالترميز ASN.1 على النحو التالي:

```
IBPrivateKeyBlock ::= CHOICE {
    bb1PrivateKeyBlock BB1PrivateKeyBlock,
    bfPrivateKeyBlock       BFPrivateKeyBlock,
    eccsiPrivateKeyBlock    ECCSIPrivateKeyBlock,
    skPrivateKeyBlock       SKPrivateKeyBlock,
    sm9PrivateKeyBlock      SM9PrivateKeyBlock
}
```

ويمكن الاطلاع على تمديد بروتوكول قابلية التشغيل البيني لإدارة المفاتيح من أجل دعم هذه العملية في التذييل II.

شرط النهاية: يستعيد الكيان IdP/SM-DP/MNO المفتاح الخاص المقابل لهوية الطلب.

- **توفير الهوية/المفاتيح لبطاقة الدارة المتكاملة الشاملة المدمجة**

شروط البداية:

أ) تُسجل البطاقة eUICC لدى الكيان SM-SR وتصبح جاهزة لتحميل المواصفة.

ب) يكون الكيان SM-DP قد قام بإنشاء مواصفة غير شخصية بالاستناد إلى وصف المواصفة المقدم من مشغل الشبكة المتنقلة.

ج) لدى مشغل الشبكة المتنقلة الآن طلب للحصول على قدر من مواصفات البطاقة eUICC.

د) يتم التحقق من المواصفة غير الشخصية على نمط البطاقة eUICC المستهدفة باستعمال إجراء التحقق من المواصفة غير الشخصية.

الإجراء:

1) يقدم مشغل الشبكة المتنقلة طلب المواصفة للكيان SM-DP المختار. وتوضح الفقرة 3.5.3 من المعيار [b-GSMA SGP.02] عملية طلب المواصفة؛

2) يُنشئ الكيان SM-DP مواصفة شخصية باستعمال البيانات الواردة من مشغل الشبكة المتنقلة. وعلى وجه الخصوص، يستعمل الكيان SM-DP هوية الاشتراك المتنقل الدولية (IMSI) كهوية لإكمال عملية التوقيع مع خدمة إدارة المفاتيح على النحو المحدد في عملية توليد المفتاح الخاص باستعمال بروتوكول قابلية التشغيل البيني لإدارة المفاتيح من أجل توليد مفتاح خاص لهوية الاشتراك المتنقل الدولية المختارة. ويُدرج المفتاح الخاص المولّد والمعلمات ibPublicParameters الواردة في المعلمات IBSysParams باعتبارهما مفتاحيْن في المواصفة؛

3) توفر المواصفة المستهدفة على البطاقة eUICC من مشغل الشبكة المتنقلة. ويمكن الاطلاع على تفاصيل المواصفة وعملية التحميل والتثبيت في الفقرة 4.5.3 من المعيار [b-GSMA SGP.02]؛

4) تفعل المواصفة المستهدفة للبطاقة eUICC عبر الكيان SM-SR أو الكيان SM-DP والكيان SM-SR. وفيما يخص الخطوات المحددة لتفعيل المواصفة، انظر الفقرة 6.5.3 أو الفقرة 7.5.3 من المعيار [b-GSMA SGP.02].

شرط النهاية: تُفعل المواصفة المستهدفة على البطاقة eUICC. ويتم تعطيل المواصفة المفعلة سابقاً. وتكون مجموعة المعلومات المدمجة في البطاقة محدثة.

- **توفير هوية/مفتاح من أجل أجهزة إنترنت الأشياء غير المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة**

الحالة 1: لدى وحدة الأمن القدرة على إنشاء دورة أمن طبقة النقل من خلال مورد الهوية.

شروط البداية:

أ) وحدة الأمن مسجلة لدى مركز الاستيقان.

الإجراء:

1) تنشئ وحدة الأمن دورة أمن طبقة النقل مع مورد الهوية وتتحقق بنجاح من صلاحية الشهادة IdP TLS؛

2) تنفذ وحدة الأمن إجراء استيقان الويب مع مورد الهوية باستخدام معرِّف هوية التوفير PROV.ID وإثبات التوفير PROV.CRED؛

3) يختار مورد الهوية هوية مخصصة للجهاز الطالب ويستكمل عملية التوقيع مع خدمة إدارة المفاتيح على النحو المحدد في عملية توليد المفاتيح الخاصة باستعمال بروتوكول قابلية التشغيل البيني لإدارة المفاتيح من أجل توليد مفتاح خاص للهوية المختارة؛

4) يرسل مورد الهوية المخصصة والمفتاح الخاص المولّد والمعلمات العمومية إلى وحدة الأمن من خلال دورة أمن طبقة النقل؛

5) تُخزن وحدة الأمن المفتاح الخاص بصورة مؤمنة وتوفر الحماية للمعلمات العمومية من التغيير غير المصرح به.

شرط النهاية: يُوفر المفتاح المستهدف في وحدة الأمن.

تتبع وحدة الأمن ومورد الهوية البروتوكول المعرّف في الفقرة 5 وفي الطلب [IETF RFC 5408] لاستكمال إجراء توفير الهوية والمفاتيح. ويُستعاض في الرد عن البنية IBEPrivateKeyReply المعرّفة في الطلب [IETF RFC 5408] بالبنية IBPrivateKeyReply.

```
IBPrivateKeyReply ::= SEQUENCE SIZE (1..MAX) OF IBPrivateKey
IBPrivateKey ::= SEQUENCE {
        pkgIdentity         IBIdentityInfo OPTIONAL,
        pkgAlgorithm        OBJECT IDENTIFIER,
        pkgKeyData IBPrivateKeyBlock,       --defined by pkgAlgorithm
        pkgOptions          SEQUENCE SIZE (1..MAX) OF PKGOption,
        ibSysParams IBSysParams OPTIONAL
}
PKGOption ::=  SEQUENCE {
        optionID        OBJECT IDENTIFIER,
        optionValue     OCTET STRING
}
```

الحالة 2: وحدة الأمن ليس لديها تنفيذ لأمن طبقة النقل

شروط البداية:

أ) وحدة الأمن مسجلة لدى مركز الاستيقان.

الإجراء:

1) تولد وحدة الأمن مفتاح تشفير المفاتيح (KEK) وتُشفر طلب توفير المفتاح (IBKeyProvRequest). ويشمل الطلب مفتاح تشفير المفاتيح ومعرِّف هوية التوفير (PROV.ID) وإثباتات التوفير (PROV.CRED) التي يتم تشفيرها باستخدام المفتاح العمومي لمورد الهوية الذي تحدده الهوية IdP.ID. وتُشفر نتيجة التشفير بوصفها رسالة EncryptedMsg. ويرسل الطلب المشفر كنص للطلب HTTP POST إلى مورد الهوية؛

2) يفك مورد الهوية تجفير النص المشفر باستخدام المفتاح الخاص الذي تحدده الهوية IdP.ID في الطلب، ويتحقق من حداثة خاتم التوقيت أو من صحة العداد أو كليهما. وفي حال عدم اجتياز الطلب عمليات التحقق هذه، يعيد مورد الهوية رداً يشير إلى فشل. ويواصل مورد الهوية التحقق من صحة المعرِّف PROV.ID والإثباتات PROV.CRED مع مركز الاستيقان. وإذا فشل هذا التحقق، يعيد مورد الهوية رداً يشير إلى فشل. ويختار مورد الهوية هوية تخصص للجهاز الطالب ويستكمل عملية التوقيع مع خدمة إدارة المفاتيح على النحو المحدد في عملية توليد المفاتيح الخاصة باستعمال بروتوكول قابلية التشغيل البيني لإدارة المفاتيح من أجل توليد مفتاح خاص للهوية المختارة؛

3) يُشفر مورد الهوية المفتاح الخاص المولد وإذا لزم الأمر، الهوية والمعلمات العمومية المشفرة بوصفها IBKeyProvisionData، بمفتاح تشفير المفاتيح باستعمال الخوارزمية المحددة (keyProtAlg) المرسلة في الطلب. ويشفر النص المشفر كرسالة EncryptedMsg. ويرسل مورد الهوية إلى وحدة الأمن الرد المشفر كنص رد بالبروتوكول HTTP؛

4) تفك وحدة الأمن تجفير الرد وتحصل على الهوية المخصصة والمفتاح الخاص والمعلمات العمومية. وتُخزن المفتاح الخاص بصورة مؤمنة وتوفر الحماية للمعلمات العمومية من التغيير غير المرخص به.

شرط النهاية: يُوفر المفتاح المستهدف في وحدة الأمن.

```
IBKeyProvisionRequest ::= SEQUENCE {
        version         INTEGER { v1(1) },
        timer           Time OPTIONAL,
        counter         INTEGER         OPTIONAL,
        identity        OCTET STRING,
        credential      OCTET STRING,
        keyProtAlg      OBJECT IDENTIFIER,
        kek             OCTET STRING
}
Time ::= CHOICE {
    utcTime      UTCTime,
    generalTime GeneralizedTime
}
IBKeyProvisionResponse ::= SEQUENCE SIZE(1..MAX) OF IBKeyProvisionData
IBKeyProvisionData ::= SEQUENCE {
        identity            OCTET STRING OPTIONAL,
        ibSysParams         IBSysParams OPTIONAL,
        ibPrivateKey        IBPrivateKeyBlock
}
EncryptedMsg ::= SEQUENCE {
        encryptionAlgorithm    EncryptionAlgorithmIdentifier,
        encryptedData          EncryptedData
}
EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
EncryptedData ::= OCTET STRING
```

5.C إبطال الهوية والمفاتيح

إذا كان يجب منع هوية في نظام التجفير القائم على الهوية لأسباب مختلفة منها مثلاً أن مالك الهوية ألغى الاشتراك في الخدمة أو أن المفتاح الخاص المقابل تعرض للخطر، فإنه ينبغي إبطال الهوية وقد يلزم تدمير المفتاح الخاص المقابل لها لأسباب أمنية. وإذا تم إبطال هوية، فإنها تُضبط على وضع الإبطال. وإذا استفسر بيان ما عن حالة هوية تم إبطالها، يعيد الكيان IdP/SM-DP/MNO القيمة الصحيحة المحددة في بروتوكول حالة الهوية الإلكترونية. وللتحقق من تحديد حالة الهوية بكفاءة أكبر، يمكن لأي كيان استرجاع قائمة إبطال الهوية (IRL) من الكيان IdP/SM-DP/MNO بانتظام وتخزينها محلياً، ويمكن للكيان أن يتحقق من خلال القائمة IRL الحديثة لتحديد ما إذا كانت هوية ما قد أبطلت دون الاستفسار من على الخط عن وضع كل هوية. وبالنسبة إلى البطاقة eUICC، تكون عملية تدمير المفتاح الخاص ممكنة عن طريق تعطيل المواصفة أولاً ثم حذفها من البطاقة.

- إبطال الهوية والمفاتيح بالنسبة لبطاقة الدارة المتكاملة الشاملة المدمجة

شروط البداية:

أ) تفعل المواصفة المستهدفة على بطاقة الدارة المتكاملة الشاملة المدمجة.

الإجراء:

1) يستهل مشغل الشبكة المتنقلة تعطيل المواصفة بواسطة عملية إعداد بيانات مدير الاشتراكات (SM-DP). وترد تفاصيل عملية تعطيل المواصفة في الفقرة 8.5.3 من المعيار [b-GSMA SGP.02]. ويضبط الكيان SM-DP الهوية على وضع الإبطال.

2) يستهل مشغل الشبكة المتنقلة عملية حذف المواصفة. وفيما يتعلق بالخطوات المحددة في حذف مواصفة الميدان الأمني للمُصدر (SD-P)، انظر الفقرة 10.5.3 من المعيار [b-GSMA SGP.02]. ويقوم الكيان SM-DP بضبط الهوية على وضع الإبطال، وإذا تكللت عملية حذف مواصفة الميدان الأمني للمُصدر بنجاح، تُضبط الهوية أيضاً على وضع الحذف. وعندما يستفسر الكيان عن وضع الهوية، يرد الكيان SM-DP بالشكل المناسب وفقاً لسجل الحالة. وينشر الكيان SM-DP دورياً قائمة بحالة الهويات التي أبطلت خلال هذه الفترة.

شرط النهاية: يتم تعطيل المواصفة المستهدفة وحذفها من البطاقة eUICC.

- **إبطال الهوية والمفاتيح بالنسبة لأجهزة إنترنت الأشياء غير المزودة ببطاقة الدارة المتكاملة الشاملة المدمجة (non-eUICC IoT)**

إذا أبطلت هوية ما، يضبط المورد IdP على وضع الإبطال. وعندما يستفسر الكيان عن وضع الهوية، يستجيب مورد الهوية بشكل مناسب وفقاً لسجل الحالة. وينشر مورد الهوية دورياً قائمة بحالة الهويات التي أبطلت خلال هذه الفترة.

وتقع عملية إطلاق الإبطال وتحديث وضع الهوية خارج نطاق هذه التوصية.

- **بروتوكول وضع الهوية الإلكترونية**

نظراً إلى وجود عدد كبير من أجهزة إنترنت الأشياء الموصولة بمشغل الاتصالات، قد يكون من الضروري أن يحصل الكيان SM-DP أو مورد الهوية أو جهاز إنترنت الأشياء في الوقت المناسب على المعلومات المتعلقة بحالة إبطال هوية جهاز إنترنت الأشياء. وفي هذه التوصية، يوصف بروتوكول وضع الهوية الإلكترونية لتمكين الكيان SM-DP أو مورد الهوية أو جهاز إنترنت الأشياء من تحديد الوضع الحالي للهوية من خلال عمليات الاستفسار من على الخط. ويصدر عميل بروتوكول وضع الهوية الإلكترونية طلب الحالة لمستجيب بروتوكول وضع الهوية الإلكترونية ويعلّق قبول الهوية المعنية حتى يرد المستجيب. وإن البروتوكول OISP مماثل لبروتوكول وضع الشهادة الإلكترونية (OCSP) [IETF RFC 6960].

يتضمن طلب بروتوكول وضع الهوية الإلكترونية البيانات التالية:

```
OISPRequest ::= SEQUENCE {
        version                 INTEGER { v1(1) },
        identity        IBIdentityInfoSet
}
```

- يشير الإصدار إلى إصدار البروتوكول، وهو v1(1) بالنسبة إلى هذه الوثيقة.
- الهوية هي طلب بروتوكول وضع الهوية الإلكترونية.

```
IBIdentityInfoSet ::= SEQUENCE SIZE(1..MAX) OF IBIdentityInfo
IBIdentityInfo ::= SEQUENCE {
        domainName              IA5String OPTIONAL,
        domainSerial            INTEGER OPTIONAL,
        identityType            OBJECT IDENTIFIER OPTIONAL,
        identityData            OCTET STRING
}
```

- الميدان domainName **اختياري** وتمثل السلسلة IA5String المعرّف [b-URI] URI أو [b-IRI] IRI.
- الميدان domainSerial **اختياري** ويشمل **عدداً صحيحاً** يعرّف مجموعة فريدة من المعلمات العمومية للتجفير القائم على الهوية في حال استعمال ميدان وحيد لأكثر من مجموعة واحدة من المعلمات.
- الميدان identityType **اختياري** ويشمل **معرِّف هوية الشيء** الذي يعرّف النسق الذي تم به تشفير الحقل identityData. وإذا كان هذا الحقل غير متاح، يُستخدم نوع الهوية الافتراضي.
- البيانات identityData هي بيانات الهوية المستهدفة.

بمجرد استلام الطلب، يتحقق مستجيب البروتوكول OISP مما إذا كانت الرسالة مُعدّة بشكل جيد ومما إذا كان الطلب يحتوي على المعلومات التي يطلبها المستجيب. وإذا فشلت عملية التحقق هذه، ينتج مستجيب البروتوكول OISP رسالة خطأ؛ وإلا فإنه يعيد رداً محدداً وفقاً لحالة الهويات التي جرى الاستعلام عنها في الطلب.

```
OISPResponse ::= SEQUENCE {
        responseStatus          OISPResponseStatus,
        responseData            OISPResponseData OPTIONAL
}
```

- تشير الحالة responseStatus إلى حالة معالجة الطلب السابق.
- الحقل responseData **اختياري** ويشمل بيانات الرد للطلب. وإذا كانت قيمة الحقل responseStatus من بين شروط الخطأ، لا يضبط الحقل responseData.

```
OISPResponseStatus ::= ENUMERATED {
      successful  (0),   -- Response has valid confirmations
      malformedRequest     (1),   -- Illegal confirmation request
      internalError        (2),   -- Internal error in issuer
      tryLater             (3),   -- Try again later
                           --(4) is not used
      unauthorized         (5)   -- Request unauthorized
}
OISPResponseData ::= SEQUENCE {
    version                 INTEGER { v1(1) },
    producedAt              GeneralizedTime,
    hashAlgorithm           AlgorithmIdentifier OPTIONAL,
    tbsIdStatus             SEQUENCE OF SingleIdStatus,
    signatureAlgorithm      AlgorithmIdentifier OPTIONAL,
    signature               BIT STRING OPTIONAL,
    certs                   [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL
}
```

- **يجب** أن يكون الإصدار v1(1) من أجل هذا الإصدار لقواعد تركيب الرد الأساسية.
- الحقل producedAt هو الوقت الذي وقّع فيه مستجيب البروتوكول OISP هذا الرد.

- يعرف الحقل hashAlgorithm خوارزمية اختزال لتوليد idHash في الحالة tbsIdStatus، في حالة وجود هذا الحقل. وهذا الحقل اختياري والقيمة الافتراضية هي **معرِّف هوية الشيء** (OBJECT IDENTIFIER) من أجل خوارزمية الاختزال المؤمنة SHA256 دون معلمات.
- يشير الحقل tbsldStatus إلى الردود المتعلقة بكل هوية في الطلب.
- الحقل signatureAlgorithm **اختياري** ويشمل الخوارزمية التي استُعملت لتوقيع الرد.
- يتم احتساب التوقيع بناء على نتيجة التشفير ASN.1 DER من الحقل producedAt إلى tbsIdStatus باستعمال خوارزمية التوقيع المحددة. وهذا الحقل **اختياري** وقد لا يضبط إذا كان لعميل البروتوكول OISP أساليب أخرى لضمان صحة الرد. فعلى سبيل المثال، يُرسل الرد من خلال قناة مؤمنة TSL بين العميل والمستجيب.
- الحقل certs **اختياري** ويشير إلى الشهادة التي تساعد عميل البروتوكول OISP على التحقق من توقيع المستجيبين. وتُعرّف بنية الشهادة في الطلب [IETF RFC 5280].

```
SingleIdStatus ::= SEQUENCE {
    idHash          OCTET STRING OPTIONAL,
    identityID      IBIdentityInfo OPTIONAL,
    identityStatus  IdentityStatus,
}
```

- الحقل idHash **اختياري** ويشمل اختزال طلب الهوية. وإذا كان معرِّف الهوية طويلاً جداً، يمكن استعمال الخوارزمية idHash لتمثيل الهوية التي جرى الاستعلام عنها. والحقل identityID **اختياري** ويتضمن الحقل IBIdentityInfo الخاص بالهوية المستهدفة في الطلب.
- يشير الحقل identityStatus إلى حالة الهوية في الطلب السابق.

```
IdentityStatus ::= CHOICE {
    good                [0]  IMPLICIT NULL,
    revoked     [1]  IMPLICIT RevokedInfo,
    unknown             [2]  IMPLICIT UnknownInfo,
    updated     [3]  IMPLICIT IBIdentityInfo,
    revokedAndDeleted   [4]  IMPLICIT RevokedInfo
}
UnknownInfo ::= NULL
```

- تشير حالة "good" إلى رد إيجابي على الاستعلام عن الحالة.
- تشير حالة "revoked" إلى أن الهوية أبطلت، إما بصفة مؤقتة أو دائمة وأن القيمة هي معلومات الإبطال.
- تشير حالة "unknown" إلى أن المستجيب لا يعرف أن الشهادة مطلوبة.
- تشير حالة "updated" إلى أن الهوية قد حُدثت وأن القيمة هي هوية مخصصة حديثاً للهوية التي جرى الاستعلام عنها.
- تشير حالة "revokedAndDeleted" إلى أن الهوية أبطلت وأن المفتاح الخاص قد تم تدميره من الجهاز عن بُعد.

```
RevokedInfo ::= SEQUENCE {
  revocationTime     GeneralizedTime,
  revocationReason   [0] EXPLICIT IRLReason OPTIONAL
}
IRLReason ::= ENUMERATED {
```

```
    unspecified             (0),
    keyCompromise           (1),
    pkgCompromise           (2),
    affiliationChanged      (3),
    superseded              (4),
    cessationOfOperation    (5),
    identityHold            (6),
                            -- value 7 is not used
    removeFromIRL           (8),
    privilegeWithdrawn      (9)
}
```

- **قائمة إبطال الهوية**

إلى جانب استخدام البروتوكول OSIP للرد على الاستعلامات عن حالة الهوية، يمكن لأحد الكيانات مثل IdP أو SM-DP أن ينشر قائمة كاملة بالهويات التي أبطلت على فترات منتظمة، أي قائمة إبطال الهوية. ولتسريع عملية التحقق من حالة الهوية، يمكن لكيان التحقق من الحالة تكون لديه سعة تخزين استعلام القائمة IRL وتخزينها محلياً. ويمكن للكيان المعني بالتحقق أن يحدد ما إذا كانت هوية ما مقبولة لعمليات معيّنة أم لا، مثل الترخيص بالنفاذ إلى الشبكة استناداً إلى القائمة IRL. وإذا كانت هذه الهوية غير موجودة في القائمة IRL، عندئذ، يُفترض أن الهوية صالحة. ولتحسين كفاءة النظام، قد يكتفي الكيان IdP/SM-DP/MNO بنشر الهويات الملغاة حديثاً منذ وقت محدد. وهذا ما يُعرف باسم القائمة "delta IRL". وتتضمن القائمة delta IRL معلومات الهويات التي أبطلت منذ أي نشر كامل للقائمة IRL. ويمكن باستعمال القائمة delta IRL الحد من بيانات الاتصالات الزائدة إلى حد كبير ووقت معالجة قوائم إبطال الهوية. وتتشابه قائمة إبطال الهوية مع قائمة إبطال الشهادة (CRL) [IETF RFC 5280].

تُعرّف قائمة إبطال الهوية على النحو التالي:

```
IdentityRevocationList ::= SEQUENCE {
    tbsIdentityList         TBSIdentityRevocationList,
    signatureAlgorithm      AlgorithmIdentifier OPTIONAL,
    signatureValue          BIT STRING OPTIONAL
}
```

- يشير الحقل tbsIdentityList إلى قائمة الهويات التي أبطلت مع معلومات إضافية مثل وقت الإبطال.
- يعرّف الحقل signatureAlgorithm خوارزمية مُصدر قائمة إبطال الهوية المستعملة للتوقيع على القائمة. وهذا الحقل اختياري ولا يكون موجوداً إذا كانت القيمة signatureValue غير موجودة.
- تعرف القيمة signatureValue قيمة التوقيع الذي ولده المصدّر على القائمة tbsIdentityList. وهذا الحقل اختياري ولا يكون موجوداً إذا كان لدى عميل الطلب وسائل أخرى لضمان استيقان القائمة المسترجعة.

```
TBSIdentityRevocationList ::= SEQUENCE {
    version             INTEGER { v1(1) },
    issuer              Name,
    irlNumber           INTEGER OPTIONAL,
    deltaList           BOOLEAN OPTIONAL,
    thisUpdate    Time,
    nextUpdate          Time OPTIONAL,
    domainName          IA5String OPTIONAL,
    domainSerial        INTEGER OPTIONAL,
    revokedIdentities   SEQUENCE OF SEQUENCE  {
        identity        IBIdentityInfo,
        revocationDate          Time,
        irlEntryExtensions      Extensions OPTIONAL
    } OPTIONAL,
    irlExtensions               [0] EXPLICIT Extensions OPTIONAL
}
Name ::= CHOICE {--imported from [IETF RFC 5280]
    rdnSequence  RDNSequence
}
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
RelativeDistinguishedName ::= SET SIZE (1..MAX) OF AttributeTypeAndValue
AttributeTypeAndValue ::= SEQUENCE {
    type      AttributeType,
    value     AttributeValue
}
AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY -- DEFINED BY AttributeType
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
Extension ::=  SEQUENCE  {--imported from [IETF RFC 5280]
   extnID      OBJECT IDENTIFIER,
   critical    BOOLEAN DEFAULT FALSE,
   extnValue   OCTET STRING
           -- contains the DER encoding of an ASN.1 value
           -- corresponding to the extension type identified
           -- by extnID
}
```

- يشير الإصدار إلى إصدار بنية قائمة إبطال الهوية.
- المُصدر هو اسم الكيان الذي يقوم بإصدار قائمة إبطال الهوية.

- irlNumber هو رقم مُصدر القائمة الحالية لإبطال الهوية. ويبدأ من 0. وبالنسبة لكل نشر كامل للقائمة IRL، يزداد العدد بمقدار 1. وهذا الحقل اختياري.
- يبين الحقل deltaList ما إذا كانت القائمة IRL الحالية قائمة delta IRL أم لا. ولا تحتوي القائمة إلا على معلومات الهويات التي تم إبطالها منذ النشر الكامل للقائمة IRL المبين بواسطة الحقل irlNumber.
- يحدد الحقل thisUpdate وقت توليد القائمة IRL الحالية.
- يعرّف الحقل nextUpdate وقت توليد القائمة IRL التالية. وهو اختياري.
- يعرّف الحقل domainName ميدان هوية التجفير القائم على الهوية.
- يشير الحقل revokedIdentities إلى مجموعة الهويات التي تم إبطالها.
  - الهوية هي بيانات الهوية التي تم إبطالها.
  - يشير الحقل revocationDate إلى الوقت الذي تم فيه إبطال الهوية.
  - يعرّف الحقل irlEntryExtensions التمديدات المحتملة للحقل revokedIdentity. ولا يُعرّف حالياً أي تمديد.
- يعرّف الحقل irlExtensions التمديدات المحتملة للقائمة IRL. ولا يُعرّف حالياً أي تمديد.

الملحق D

الاستيقان

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية.)

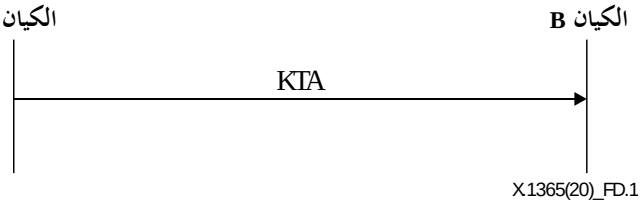
يقدم هذا الملحق بروتوكولات الاستيقان الأربعة القائمة لدعم تقنية التجفير القائم على الهوية.

1.D بروتوكول نقل السر بالمرور الواحد

يقابل هذا البروتوكول الآلية 2 لنقل المفتاح السري الواردة في المعيار 11770-3 المشترك بين المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية [ISO/IEC 11770-3]. إذ تنقل هذه الآلية مفتاحاً سرياً أصدره الكيان A وجفّره ووقع عليه منه إلى الكيان B، مع الاستيقان الصريح من المفتاح من الكيان A إلى الكيان B والاستيقان الضمني من المفتاح من الكيان B إلى الكيان A. ويتحقق الاستيقان الصريح من المفتاح من الكيان A إلى الكيان B بتوقيع الكيان A على السر المجفَّر مع استخدام مَعلمة متغيرة زمنياً (TVP)، بينما يتحقق الاستيقان الضمني من المفتاح من الكيان B إلى الكيان A بتجفير السر بمعرِّف هوية الكيان B، وهو ما يترتب عليه استئثار الكيان B وحده بإمكانية استعادة السر. انظر الشكل 1.D.

ولتنفيذ البروتوكول يتم الوفاء بالمتطلبات التالية:

- أن يكون للكيان A مفتاح خاص للتوقيع، *A.ib.prk*، يقابل معرِّف هويته، والمعلمات العمومية ذات الصلة *A.ib.pubparam*؛
- أن يكون للكيان B مفتاح خاص لفك التجفير، *B.ib.prk*، يقابل معرِّف هويته، والمعلمات العمومية ذات الصلة *B.ib.pubparam*؛
- إمكانية حصول الكيان A على نسخة مستيْقَنة من مَعلمة التجفير العمومية للكيان B *B.ib.pubparam* ومعرِّف هوية الكيان B؛
- إمكانية حصول الكيان B على نسخة مستيْقَنة من مَعلمة التوقيع العمومية للكيان A للتوقيع *A.ib.pubparam* ومعرِّف هوية الكيان A؛
- أن تكون المعلمة الاختيارية المتغيرة زمنياً إما خاتم توقيت أو رقماً تسلسلياً. وإذا استُخدمت أختام التوقيت، يلزم عندئذ أن يحتفظ الكيانان A وB بميقاتيتين متزامنتين أو يستخدما خاتم توقيت لطرف ثالث موثوق؛
- يجوز للكيانين A وB تقاسم نفس المعلمات العمومية، أي أن *B.ib.pubparam = A.ib.pubparam*.



الشكل 1.D – بروتوكول نقل السر بالمرور الواحد

1) يولد الكيان A السر العشوائي *K* بالطول اللازم؛

2) يولد الكيان A *BE*=**IBEnc**(*B.ib.pubparam, ID_B,* [*ID_A*]||*K*||*Text1*). ويمكن أن يكون النص Text1 خاوياً. ومعرِّف هوية الكيان A (*ID_A*) اختياري إذا كان للكيان B أساليب أخرى للحصول على معرِّف هوية الكيان A؛

3) يولد الكيان A *S*=**IBSign**(*A.ib.pubparam, ID_A, A.ib.prk,* [*ID_B*]||TVP||BE||*Text2*). ويمكن أن يكون النص Text2 خاوياً. ومعرِّف هوية الكيان B (*ID_B*) اختياري إذا كان الكيان B على علم بمعرِّف الهوية المستخدم، *ID_B*، *للتحضير*؛

4) يولد الكيان A الرمز KTA=[*ID_B*]||TVP||BE|| *Text2*|| S||*Text3*؛

5) إذا كانت المعلمة المتغيرة زمنياً (TVP) خاتم توقيت، يتحقق الكيان B مما إذا كانت المعلمة في حدود اختلاف التوقيت المسموح به، وإلا يرفض الكيان B الرمز؛

6) إذا تسنى للكيان B الحصول على معرِّف هوية الكيان A (*ID_A*) بوسيلة أخرى وكانت المعلمة TVP رقماً تسلسلياً، يتحقق الكيان B أولاً مما إذا كان الرقم التسلسلي أكبر من الرقم المحتفظ به للكيان B، وإلا يرفض الكيان B الرمز؛

7) إذا تسنى للكيان B الحصول على معرِّف هوية الكيان A (*ID_A*) بوسيلة أخرى، يتحقق الكيان B من التوقيع *S* في الرمز KTA باستخدام الوظيفة **IBVerify**(*A.ib.pubparam, ID_A,* [*ID_B*]||TVP||BE||*Text2,* S)؛

8) يفك الكيان B تجفير *BE* باستخدام **IBDec**(*B.ib.pubparam, ID_B, B.ib.prk,* BE)=*[ID_A]||K||Text1*؛

9) إذا لم يتسن للكيان B الحصول على المعرِّف *ID_A* إلا بعد تنفيذ الخطوة 8، فإنه يتحقق من مدى حداثة المعلمة TVP، إذا كانت رقماً تسلسلياً. وإذا لم تكن المعلمة TVP حديثة، يرفض الكيان B الرمز. ويتحقق الكيان B كذلك من التوقيع *S*. وإذا كان التوقيع غير سليم، يرفض الكيان B الرمز؛

10) وإذا اجتيزت جميع عمليات الفحص والتحقق، يستخدم الكيانان A وB المفتاح *K* لحماية الرسائل التالية. ويمكن لكلا الكيانين استخدام وظيفة اشتقاق المفاتيح (KDF) [b-IEEE 1363] لتوليد مفاتيح للتجفير والاستيقان من الرسائل.

الملاحظة 1 – يمكن تحويل هذا البروتوكول إلى بروتوكول استيقان أُحادي الكيان بإزالة BE من الرسالة الموقّعة من جانب الكيان A والرمز KTA. وبالتالي، يصبح هذا التعديل نظام الاستيقان من الكيانات بالمرور الواحد، المحدد في المعيار [b-ISO/IEC 9798-3].

الملاحظة 2 – يمكن تحويل هذا البروتوكول إلى بروتوكول استيقان ثنائي الكيان بإلزام الكيان B بإعادة المفتاح *K* إلى الكيان A. ويستيقن الكيان A من الكيان B بإبداء قدرة الكيان A على استعادة المفتاح *K*، وهو ما يتطلب منه امتلاكه المفتاح الخاص *B.ib.prk*.

الملاحظة 3 – لتحسين الكفاءة يمكن استخدام خوارزميات التوقيع المشفَّر القائمة على الهوية من قبيل خوارزميتي التوقيع المشفَّر BLMQ [b-Barreto] وChen-Malone-Lee [b-Chen].

2.D بروتوكول أمن طبقة النقل بالتوقيع القائم على الهوية (TLS-IBS)

يوصف هذا القسم بروتوكولاً آخر للاستيقان يُدعى بروتوكول أمن طبقة النقل بالتوقيع القائم على الهوية (TLS-IBS). إذ يُفترض أن كلا من جانبي المخدِّم وجهاز إنترنت الأشياء كليهما مزودان بإثباتات قائمة على الهوية، تشمل هوية ما ومفتاح خاص للتوقيع ومعلمات عمومية لخدمة إدارة المفاتيح (مثل المفتاح KPAK المعرَّف في المعيار [IETF RFC 6507] كمعلمة حاسوبية). ويمكن الاطلاع في الملحق B على تعاريف بنى المعلمات العمومية للخدمة KMS فيما يتعلق بالخوارزميات المدعومة.

وطور البروتوكول TLS-IBS استناداً إلى المعيار [IETF RFC 7250]. إذ يتبادل عميل ومخدِّم أمن طبقة النقل، تقليدياً، مفاتيح عامة معتمدة بشهادات البنية التحتية للمفاتيح العمومية (PKI). وتعتبر عملية التبادل هذه عملية معقدة وقد تتسبب في وجود مواطن ضعف أمنية جراء استخدام شهادات PKI. ولتبسيط تبادل الشهادات، توصف في المعيار [IETF RFC 7250] إمكانية استخدام مفتاح عمومي غير معالج في أمن طبقة النقل، أي أنه بدلاً من إرسال شهادة كاملة في رسائل أمن طبقة النقل، لا يتبادل العميل والمخدِّم سوى المفاتيح العمومية. إلا أنه يُفترض استخدام آلية خارج النطاق للربط بين المفاتيح العمومية والهويات. ففي شبكات إنترنت الأشياء، يُعد استخدام أمن طبقة النقل مع مفتاح عمومي غير معالج خياراً جذاباً جداً، لكنّ ربط الهويات بمفاتيح عمومية قد يكون صعباً. فحفظ جدول كبير للتقابل بين الهويات والمفاتيح العمومية على جانب المخدِّم تترتب عليه تكاليف حفظ إضافية؛ فيجب، مثلاً، تسجيل الأجهزة مسبقاً لدى المخدِّم. ولتحسين تبسيط عملية الربط بين المفتاح العمومي والكيان الذي يقدمه، يمكن، كطريقة أفضل، استخدام أسلوب التجفير القائم على الهوية لأغراض الاستيقان، كالمفتاح العمومي ECCSI الموصف في المعيار [IETF RFC 6507]. فخلافاً لشهادات التوصية ITU-T X.509 والمفاتيح العمومية غير المعالجة بأخذ المفتاح العمومي في التجفير IBC شكل هوية الكيان، وهو ما يساعد على الاستغناء عن الربط بين المفتاح العمومي والكيان الذي يقدمه.

وعند استخدام التوقيع القائم على الهوية كمفتاح عمومي غير معالج في أمن طبقة النقل، يجري خلال الاتفاق التفاوض على خوارزميات التوقيع والاختزال. ويتّبع الاتفاق القائم بين العميل والمخدِّم في أمن طبقة النقل الإجراءات المحددة في المعيار [IETF RFC 7250] وTLS 1.3 [IETF RFC 8446]، ولكن مع دعم من خوارزميات التوقيع القائم على الهوية باعتبارها مخططات التوقيع.

وفيما يلي توصيف بروتوكول TLS-IBS المطور استناداً إلى المعيار [IETF RFC 7250] وTLS 1.3 بالمفاتيح ECCSI [IETF RFC 6507] وIBS1 (Hess-IBS) وIBS1 (Cha-Cheon-IBS) و[ISO/IEC 14888-3] SM9-IBS كخوارزميات التوقيع:

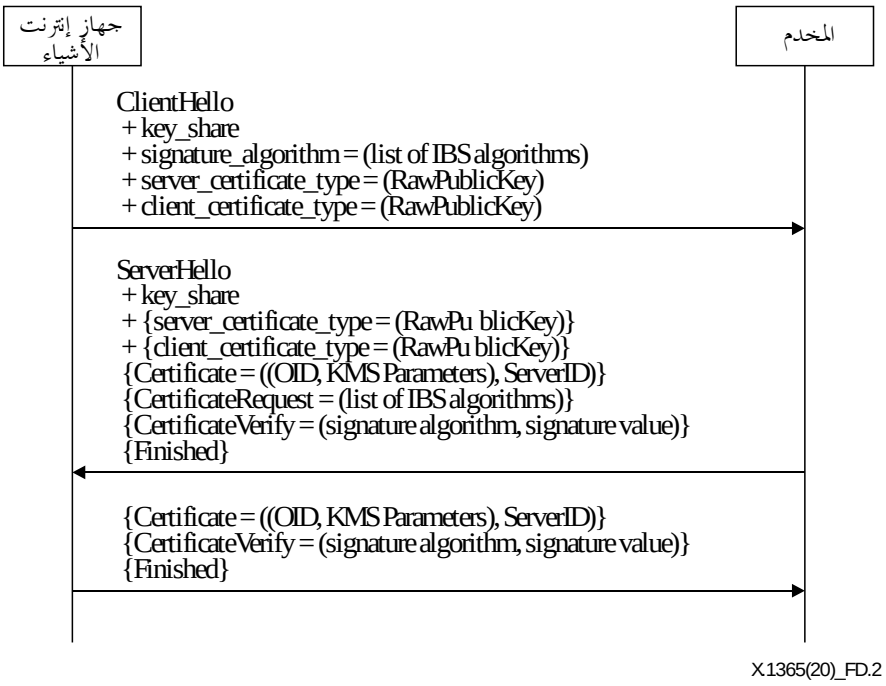
1) يرسل جهاز إنترنت الأشياء إلى المخدِّم رسالة ClientHello وتشمل تقاسم_المفتاح_الموسّع، وخوارزميات_التوقيع، ونمط_شهادة_ المخدِّم، ونمط_شهادة_العميل، مبيناً أنه يدعم المفتاح العمومي غير المعالج وخوارزميات IBS؛

2) يرسل المخدِّم إلى جهاز إنترنت الأشياء رسالة ServerHello، تشمل تقاسم المفتاح الموسّع (key_share)، ونمط شهادة المخدِّم (server_certificate_type)، ونمط شهادة العميل (client_certificate_type)، والشهادة (Certificate)، وطلب الشهادة (CertificateRequest)، والتحقق من صحة الشهادة (CertificateVerify)، وانتهاء التبادل (Finished)، مبيناً دعم المفتاح العمومي غير المعالج، ويدرج المخدِّم هويته (ServerID) ومعلمات KMS (معلمات OID وKMS) في الجزء المتعلق بالشهادة. وتعرف في الفقرة 3.2.D من هذه التوصية بنى بيانات المعلمات KMS. وتشمل رسالة التحقق من صحة الشهادة (CertificateVerify) توقيعاً يولده المفتاح الخاص المملوك للمخدِّم؛

3) بعد التحقق من هوية المخدِّم وتوقيعه، يرسل جهاز إنترنت الأشياء مفتاحه العمومي غير المعالج كشهادة ورسالة التحقق من صحة الشهادة ورسالة انتهاء إلى المخدم. ويدرج جهاز إنترنت الأشياء هويته (ClientID) والمعلمات KMS (معلمات OID وKMS) في الجزء المتعلق بالشهادة، وهو المفتاح العمومي غير المعالج للعميل. وتعرف في الفقرة 3.2.D من هذه التوصية بنى بيانات المعلمات KMS. ويدرج توقيع يولده المفتاح الخاص للعميل؛

4) أما سائر الخطوات فهي نفس خطوات المعيار TLS 1.3 في الطلب [IETF RFC 8446].

انظر الشكل 2.D.



الشكل 2.D – بروتوكول أمن طبقة النقل بالتوقيع القائم على الهوية (TLS-IBS)

1.2.D الرسالة ClientHello

إن نسق الرسالة ClientHello هو النسق ذاته الموصف في المواصفة في TLS 1.3 [IETF RFC 8446]، ولكن يلزم تمديد خوارزمية التوقيع لتشمل التوقيع القائم على الهوية (IBS).

وتُفيد الرسالة ClientHello المخدِّم بأنماط الشهادات أو المفتاح العمومي غير المعالج المدعومَيْن من العميل، فضلاً عن أنماط الشهادات التي يتوقع العميل تلقيها من المخدِّم. وتشمل الرسالة ClientHello خوارزميات IBS المرغوب فيها بناءً على ترتيب

أفضليات العميل. وفي المواصفة TLS 1.3، يحدَّد لخوارزميات التوقيع بنية بيانات تُسمى SignatureScheme. ولدعم الخوارزمية IBS لا بد من تمديدها على النحو التالي:

```
enum {
    ...
  /* IBS signature algorithm */
    eccsi_sha256 (0x0704),
    ibs1_sha256(0x0705)
    ibs2_sha256(0x0706)
    sm9_ibs_sm3(0x0707)
  /* Reserved Code Points */
  private_use (0xFE00..0xFFFF),
  (0xFFFF)
} SignatureScheme;
```

ويمكن الاطلاع على تفاصيل نقاط الشفرة لخوارزميات التوقيع الموسعة في سجل المواصفة TLS [b-IANA TLS REG].

2.2.D الرسالة ServerHello

إن نسق الرسالة ServerHello هو النسق ذاته المحدد في TLS 1.3 [IETF RFC 8446]. ويُمدّد نظام التوقيع بنفس طريقة تمديده في الرسالة Client_Hello.

3.2.D شهادة المخدِّم

فيما يتعلق بشهادة المخدِّم، يحدد المعيار [b-IEF RFC 7250] بنية للشهادة كمفتاح RawPublicKey. وكما هو الحال في [IETF RFC 7250]، تُستخدم بنية للبيانات تُسمى subjectPublicKeyInfo لتوصيف المفتاح العمومي غير المعالج وخوارزمية تجفيره. ويعرف بنية المعلومات subjectPublicKeyInfo حقلان، أحدهما للخوارزمية والآخر للمعلمات. ويوصف حقل الخوارزمية خوارزمية التجفير المستخدمة بمفتاح عمومي غير معالج يمثل بمعرِّفات OID، بينما يوفر حقل المعلمات المعلمات اللازمة المرتبطة بالخوارزمية. وينبغي أن تكون هوية المخدِّم في الجزء subjectPublicKey.

ملاحظة – ينبغي أن تتّبع الهوية النسق المعرف في التذييل 1.

```
subjectPublicKeyInfo ::= SEQUENCE {
        algorithm                AlgorithmIdentifier,
        subjectPublicKey                BIT STRING
}
AlgorithmIdentifier ::= SEQUENCE {
        algorithm           OBJECT IDENTIFIER,
        parameters          ANY DEFINED BY algorithm OPTIONAL
}
```

وعند استخدام خوارزمية التوقيع القائم على الهوية (IBS)، تُستخدم هوية كمفتاح عمومي غير معالج يمكن تحويله إلى سلسلة OCTET. لذا، يمكن إعادة استخدام الشهادة وبنية المفتاح subjectPublicKey دون إدخال أي تغييرات عليهما.

ويمثل حقل الخوارزمية في بنية المعرِّف AlgorithmIdentifier معرِّف هوية الشيء للخوارزمية IBS المستخدمة. وإلى جانب ذلك، من الضروري إفادة الطرف النظير بمجموعة المعلمات العمومية التي يستخدمها الكيان الموقِّع. ويمكن أن تُحمَل هذه المعلومات في الحمولة النافعة لحقل المعلمات في المعرِّف AlgorithmIdentifier.

وفيما يخص الخوارزميات أعلاه، فإن بنى المعلمات العمومية هي المعلمات ECCSIPublicParameters وBFPublicParameters وBFPublicParameters وSM9PublicParameters، على التوالي، على النحو المعرف في الملحق B.

ولدعم خوارزميات التوقيع القائم على الهوية عبر بروتوكول أمن طبقة النقل من أجل توليد الرسالة CeritificateVerify، يلزم تعريف بنية بيانات لقيمة التوقيع.

- تعرف بنية البيانات للمعلمات ECCSI (استناداً إلى المعيار [IETF RFC 6507]) على النحو التالي:

```
ECCSI-Sig-Value ::= SEQUENCE {
  r INTEGER,
  s INTEGER,
  pvt  OCTET STRING
}
```

حيث يشفر رمز التحقق العمومي (كما هو معرف في المعيار [IETF RFC 6507]) كالتالي:
0x04 || x-coordinate of [v]G || y-coordinate of [v]G.

- تعرف بنية البيانات للمعلمات IBS1 على النحو التالي:

```
IBS1-Sig-Value ::= SEQUENCE {
  r INTEGER,
  s ECPoint
}
ECPoint ::= OCTET STRING as defined in [IETF RFC 5480]
```

- تعرف بنية البيانات للمعلمات IBS2 على النحو التالي:

```
IBS2-Sig-Value ::= SEQUENCE {
  r ECPoint,
  s ECPoint
}
```

- تعرف بنية البيانات للمعلمات SM9-IBS على النحو التالي:

```
SM9-Sig-Value ::= SEQUENCE {
  r INTEGER,
  s ECPoint
}
```

ولاستعمال خوارزمية توقيع مع البروتوكول TLS، لا بد من توفير معرِّف هوية الكائن لخوارزمية التوقيع. ويبين الجدول 1.D المعلومات الأساسية اللازمة عن خوارزميات التوقيع القائم على الهوية الواجب استعمالها في بروتوكول أمن طبقة النقل.

الجدول 1.D – خوارزميات التوقيع القائم على الهوية

نوع المفتاح	الوثيقة	معرِّفات الكائن
ISO/IEC 14888-3 ibs-1	ISO/IEC 14888-3: IBS-1 mechanism	1.0.14888.3.0.7
ISO/IEC 14888-3 ibs-2	ISO/IEC 14888-3: IBS-2 mechanism	1.0.14888.3.0.8
SM9-IBS	الآلية الصينية للتوقيع القائم على الهوية: ISO/IEC 14888-3	1.2.156.10197.1.302.1
التوقيعات المعتمدة القائمة على منحنيات إهليلجية بدون شهادات من أجل التشفير القائم على الهوية (ECCSI)	الفقرة 2.5 للمعيار [IETF RFC 6507]	1.3.6.1.5.5.7.6.29

4.2.D شهادة العميل

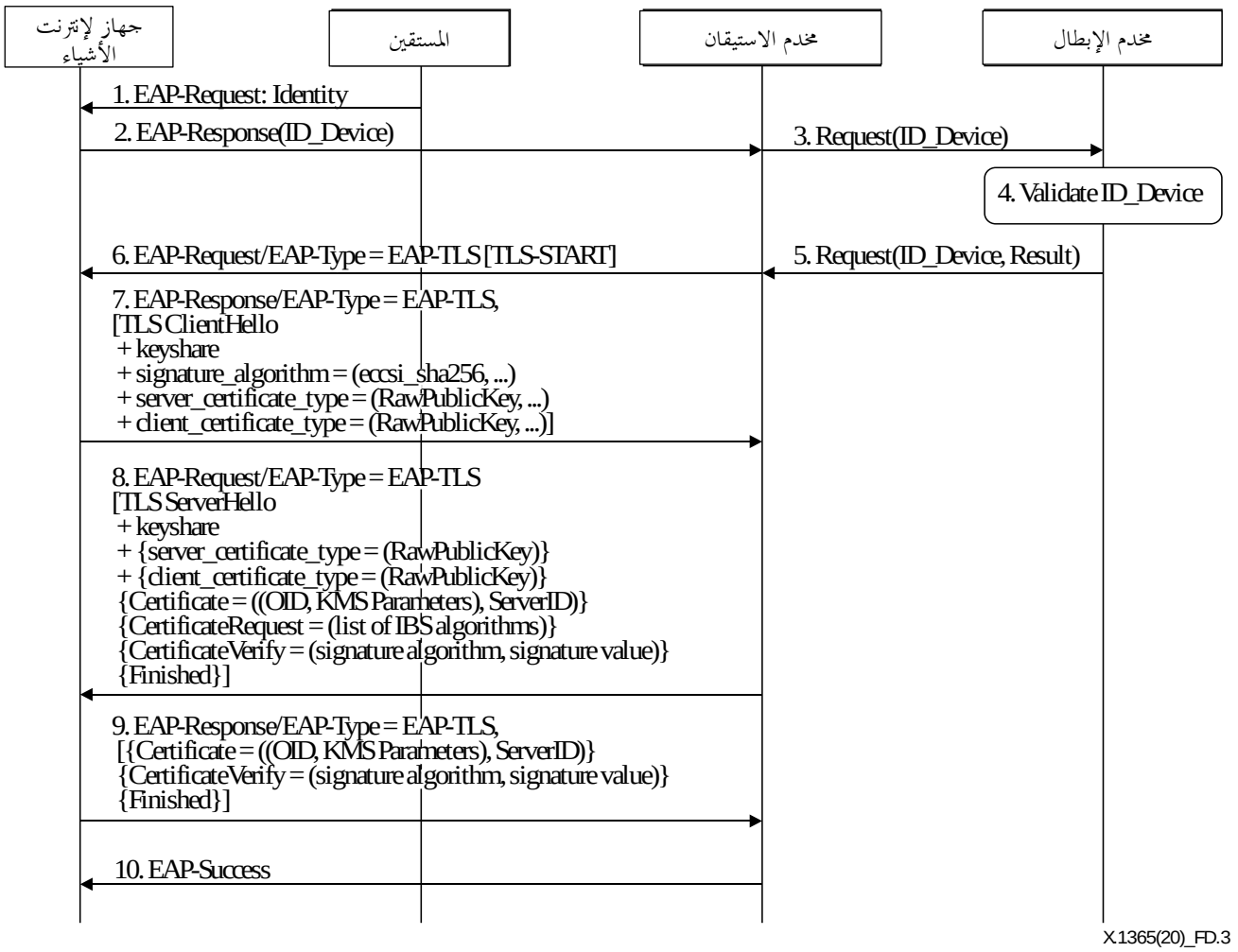
بغية دعم التوقيع القائم على الهوية، تُمدد شهادة العميل بالطريقة ذاتها التي تُمدد بها شهادة المخدّم.

3.D التوقيع EAP-TLS-IBS

في هذه الفقرة، يمدد البرتوكول EAP-TLS من أجل دعم التوقيع القائم على الهوية. ويُزود جانب الشبكة وجانب معدات المستعمل بإثباتات قائمة على الهوية، تتضمن هوية، عبارة عن مفتاح خاص للتوقيع ومعلمات عمومية لخدمة إدارة المفاتيح (على سبيل المثال، المفتاح KPAK على نحو ما هو معرف في المعيار [IETF RFC 6507]). انظر الشكل 3.D.

ويُعدل البروتوكول EAP-TLS على النحو التالي:

1) طريقة التعديل ذاتها للبروتوكول EAP-TLS؛
2) بعد استلام رد بالهوية وفق بروتوكول الاستيقان القابل للتوسيع مع هوية معدات المستعمل، ID_UE؛
3) ترسل وحدة الاستيقان معرِّف الهوية ID_UE إلى وظيفة مخدم الإبطال (RSF) من أجل التحقق؛
4) تتحقق الوظيفة RSF من معرِّف الهوية ID_UE استناداً إلى قائمة الإبطال المخزنة؛
5) ترسل الوظيفة RSF نتيجة التحقق إلى وحدة الاستيقان؛
6) إذا كان معرِّف الهوية ID_UE صالحاً ترسل وحدة الاستيقان رسالة البدء المتعلقة بالبروتوكول EAP-TLS إلى معدات المستعمل؛
7-9) الخطوات ذاتها الموصوفة في البروتوكول TLS-IBS الآنف الذكر؛
10) نجاح بروتوكول الاستيقان القابل للتوسيع.



الشكل 3.D – التوقيع EAP-TLS-IBS

1.3.D الرسالة EAP-Request

نسق الرسالة EAP-Request هو نفسه النسق الموصف في المعيار [IETF RFC 5216].

2.3.D الرد على الرسالة EAP-Response

نسق الرد EAP-Response هو نفسه النسق الموصف في المعيار [IETF RFC 5216].

3.3.D الرسالة ClientHello

نسق رسالة ClientHello هو نفسه النسق الوارد في الفقرة 2.2.D.

4.3.D الرسالة ServerHello

نسق الرسالة ServerHello هو نفسه النسق الوارد في الفقرة 2.2.D.

5.3.D شهادة المخدّم

نسق شهادة المخدم هو نفسه النسق الوارد في الفقرة 3.2.D.

6.3.D شهادة العميل

نسق شهادة العميل هو نفسه النسق الوارد في الفقرة 4.2.D.

4.D التوقيعات EAP-PSK-ECCSI

في هذه الفقرة، يُمدد البروتوكول EAP-PSK من أجل دعم إحدى خوارزميات التوقيع القائم على الهوية، ECCSI، لأغراض الاستيقان. وتُزود معدات المستعمل ووحدة الاستيقان بإثباتات قائمة على الهوية تتضمن هوية، ومفتاح توقيع سري ورمز تحقق عمومي ومفتاح KPAK، وذلك على النحو المعرف في المعيار [IETF RFC 6507] كمعلمة حاسوبية.

وبتوفير هذه الإثباتات، يمكن لمعدات المستعمل ووحدة الاستيقان أن تشتق المفاتيح المتناظرة استناداً إلى بيانات ديفي–هيلمان السكونية عن طريق تبادل معلومات الهوية ورمز التحقق العمومي، ويتبع ذلك استعمال مفتاح التوقيع السري الذي يملكه كل كيان. فعلى سبيل المثال، يمكن لمعدات المستعمل أن تشتق مفتاحاً بعد استلامها هوية وحدة الاستيقان ورمز التحقق العمومي الخاص بها، واللذين يرمز لهما بالرمزين ID_AU وPVT_AU، على التوالي، كما يلي:

K_UE = [SSK_UE](KPAK+[hash(G || KPAK || ID_AU || PVT_AU)]PVT_AU))

حيث G هي نقطة التوليد على المنحنى الإهليلجي المستخدمة من قبل خدمة إدارة المفاتيح من أجل توليد المفاتيح لمعدات المستعمل والشبكات. وتوفرها خدمة إدارة المفاتيح لمعدات المستعمل ووحدة الاستيقان إلى جانب المفتاح SSK والرمز PVT والمفتاح KPAK وما إلى ذلك. ويمكن استعمال دالة الاختزال تبعاً للملحق A بالمعيار [IETF RFC 6507].

وعلى نحو مماثل، يمكن لوحدة الاستيقان أن تشتق المفتاح K_AU بعد استلامها للهوية والرمز PVT من معدات المستعمل على النحو التالي:

K_AU = [SSK_AU](KPAK+[hash(G || KPAK || ID_UE || PVT_UE)]PVT_UE))

ويمكن إثبات أن المفتاح K_UE يساوي في الواقع K_AU.

ومع الخصائص المذكورة أعلاه، يمكن استعمال البروتوكول EAP-PSK من أجل الاستيقان المتبادل على النحو التالي:

1) ترسل معدات المستعمل طلب إرفاق إلى وحدة الاستيقان وتشير إلى أن البروتوكول EAP-PSK يجب أن يُستعمل من أجل الاستيقان المتبادل؛

2) تتحقق وحدة الاستيقان من نوع الاستيقان وتحدد أسلوب الاستيقان؛

3) ترسل وحدة الاستيقان الرسالة الأولى بخصوص البرتوكول EAP-PSK إلى معدات المستعمل مع حقل هوية يتضمن المعرِّف ID_AU والرمز PVT_AU وكذلك رقم عشوائي RAND_S على النحو المطلوب في البروتوكول EAP-PSK؛

4) تشتق وحدة الاستيقان مفتاحاً متناظراً كالآتي: K = [SSK_UE](KPAK+[hash(G || KPAK || ID_AU || PVT_AU)]PVT_AU)). وتولد معدات المستعمل رقماً عشوائياً RAND_P وتشتق أيضاً مفتاحاً كالآتي: K' = KDF(K, RAND_P, RAND_S). وتشتق معدات المستعمل مفتاح استيقان (AK) ومفتاح اشتقاق المفاتيح (KDK) استناداً إلى المعيار [b-IETF RFC4764] من أجل البروتوكول EAP-PSK؛

5) ترسل معدات المستعمل الرسالة الثانية بشأن البرتوكول EAP-PSK إلى وحدة الاستيقان، وتتضمن هذه ما يلي، RAND_S وRAND_P وMAC_P (MAC_P=CMAC-AES-128(AK, ID_P||ID_S||RAND_S||RAND_P)) لأغراض الاستيقان، وحقل هوية يتضمن معرِّف الهوية ID_UE والرمز PVT_UE؛

6) ترسل وحدة الاستيقان معرِّف الهوية ID_UE إلى الوظيفة RSF من أجل التحقق؛

7) تتحقق الوظيفة RSF من معرِّف الهوية ID_UE وفقاً لقائمة الإبطال؛

8) ترسل الوظيفة RSF نتائج التحقق إلى وحدة الاستيقان؛

9) إذا كان معرِّف الهوية صالحاً، تشتق وحدة الاستيقان المفتاح المتناظر كالآتي: K = [SSK_AU](KPAK+[hash(G || ID_UE || PVT_UE)]PVT_UE)). وتشتق وحدة الاستيقان كذلك مفتاحاً كالتالي: K = [SSK_AU](KPAK+[hash(G || KPAK || ID_UE || PVT_UE)]PVT_UE)). وتشتق وحدة الاستيقان مفتاحين AK وKDK استناداً إلى المعيار [IETF RFC 4764] من أجل البروتوكول EAP-PSK. وتستيقن وحدة

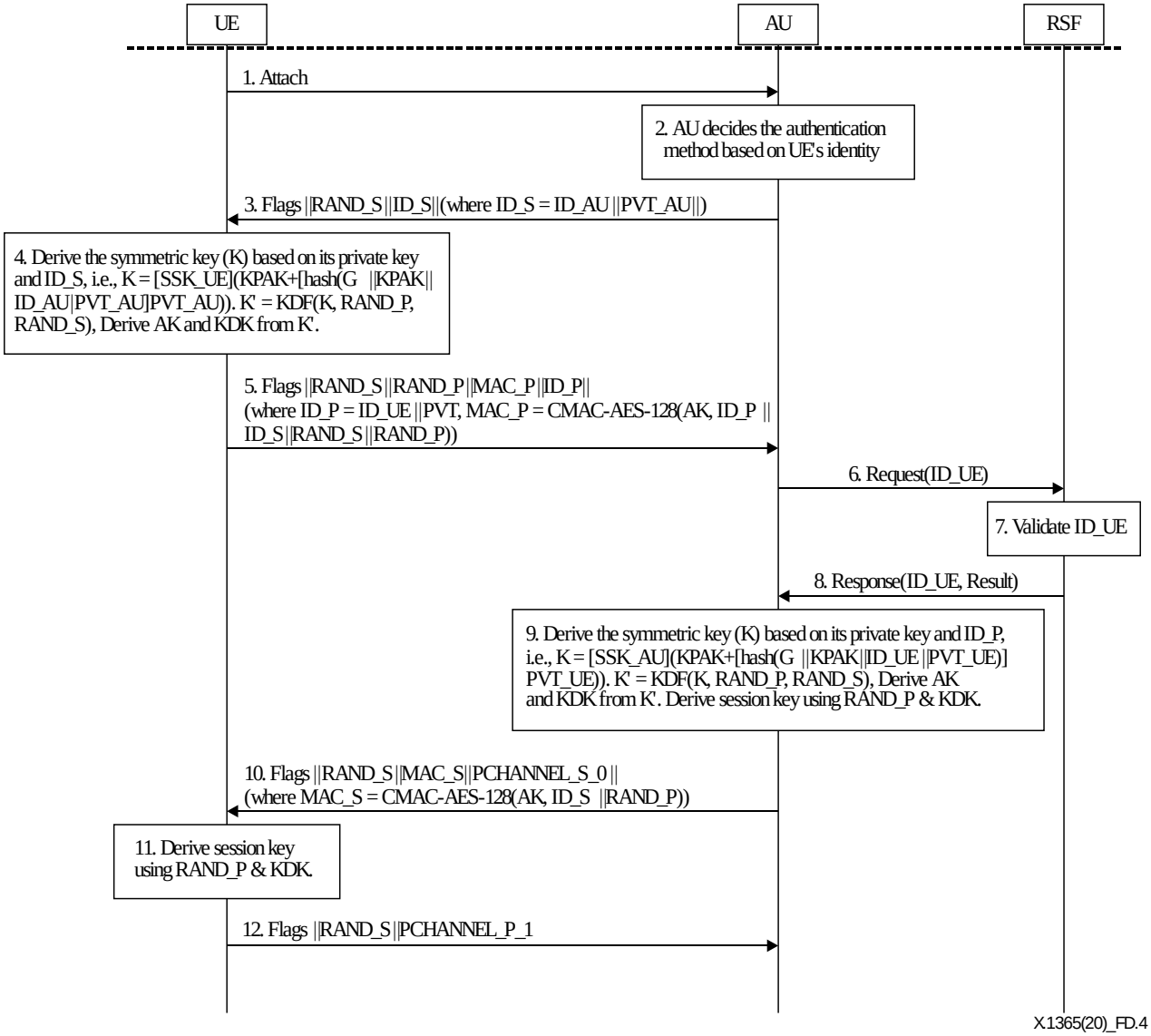
الاستيقان من معدات المستعمل استناداً إلى الرقم MAC_P الوارد من الرسالة. وتشتق أيضاً وحدة الاستيقان مفتاح الدورة استناداً إلى الرقم RAND-P ومفتاح اشتقاق المفاتيح؛

10) ترسل وحدة الاستيقان الرسالة الثالثة بشأن البروتوكول EAP-PSK إلى وحدة الاستيقان مع رقم MAC_S (MAC_S=CMAC-AES-128(AK, ID_S||RAND_P)) لأغراض الاستيقان مع الحقول الأخرى المطلوبة بموجب البروتوكول EAP-PSK؛

11) تستيقن معدات المستعمل من وحدة الاستيقان بالرقم MAC_S الوارد وتشتق مفتاح الدورة باستعمال الرقم RAND_P ومفتاح اشتقاق المفاتيح الذي تم اشتقاقه مسبقاً؛

12) ترسل معدات المستعمل الرسالة الأخيرة بشأن البروتوكول EAP-PSK إلى وحدة الاستيقان من أجل إنهاء عملية الاستيقان الخاصة بالبروتوكول EAP-PSK.

انظر الشكل 4.D.



الشكل 4.D – التوقيعات EAP-PSK--ECCSI

1.4.D الإرفاق

تشبه هذه الرسالة إجراء الاستيقان.

2.4.D الرسالة الأولى بشأن التوقيعات EAP-PSK--ECCSI (الرسالة 3 في الشكل 4.D)

يرسل المخدم إلى الطرف النظير الرسالة الأولى بشأن EAP-PSK--ECCSI. والنسق كتالي.

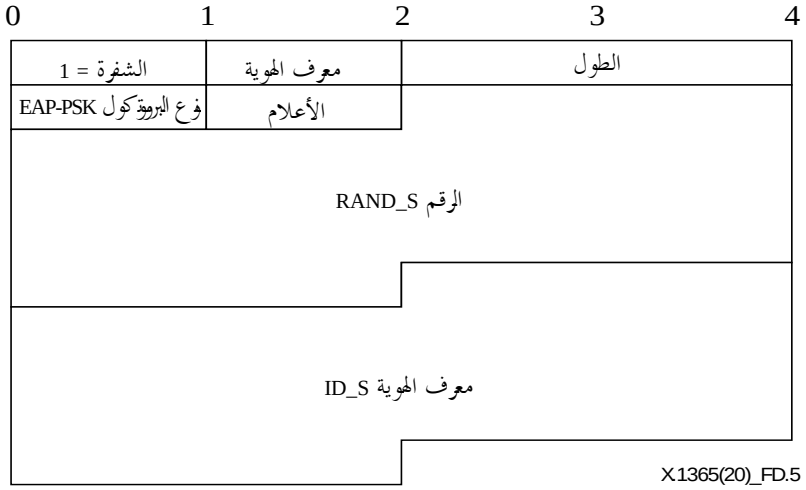
الرسالة الأولى بشأن EAP-PSK--ECCSI تتألف من:

حقل أعلام من بايتة واحدة

رقم عشوائي من 16 بايتة: RAND_S

حقل طول متغير ينقل معرِّف النفاذ إلى الشبكة الخاص بالمخدِّمات: ID_S. ويستنتج طول هذا الحقل من حقل طول بروتوكول الاستيقان القابل للتوسيع. ويجب ألا يتجاوز معرِّف النفاذ إلى الشبكة هذا 966 بايتة. ويهدف هذا التقييد إلى تجنب مشاكل التشرذم.

ويعرض الشكل 5.D مثالاً على نسق الرسالة الأولى بشأن البروتوكول EAP-PSK.



الشكل 5.D – نسق البروتوكول EAP-PSK

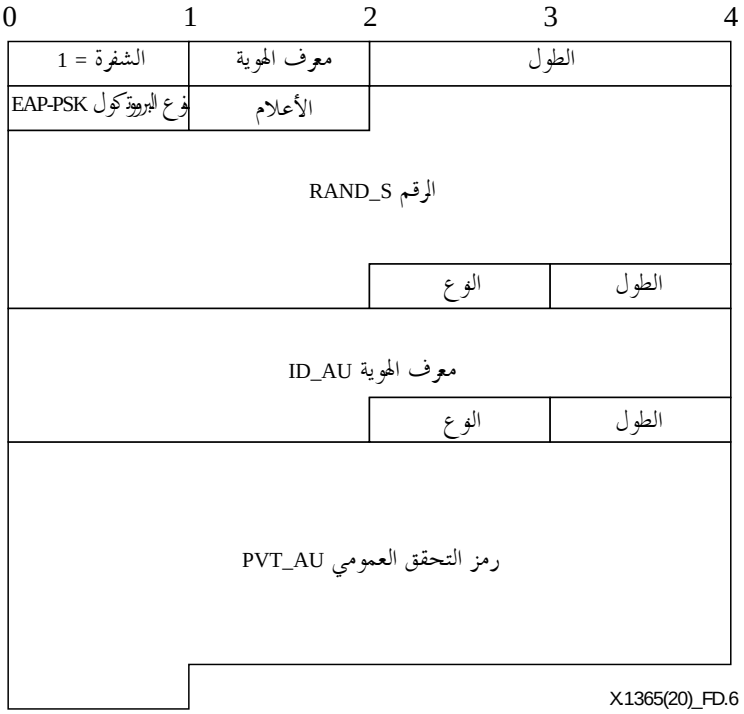
ولدعم استيقان البروتوكول EAP-PSK الذي يستند إلى التوقيع القائم على الهوية، يُستعمل معرِّف الهوية ID_S من أجل البروتوكول EAP-PSK لنقل معرِّف الهوية ID_AU والرمز PVT_AU. ويتم نقل معرِّف الهوية ID_S والرمز PVT_AU بنية البيانات "الوسم، الطول، المتجه (TLV)"، حيث ينقل الأثمون الأول مؤشر الوسم، وينقل الثاني حقل الطول، مبيناً طول الحقل التالي. وينقل حقل المتجه القيمة.

ويعرف الجدول 2.D البنية "الوسم، الطول، المتجه (TLV)" من أجل معرِّف الهوية ورمز التحقق العمومي المستعملين في البروتوكول EAP-PSK.

الجدول 2.D – تعريف البنية "الوسم، الطول، المتجه (TLV)" من أجل الهوية ورمز التحقق العمومي

	الوسم	الطول	القيمة
الهوية	1	متغير (≤255)	يحددها مورد الخدمة
رمز التحقق العمومي	2	65	عدد ست عشري

ويعرض الشكل 6.D نسق الرسالة EAP-PSK—ECCSI message التي تحمل الهوية ورمز التحقق العمومي ضمن حقل معرِّف الهوية ID_S.



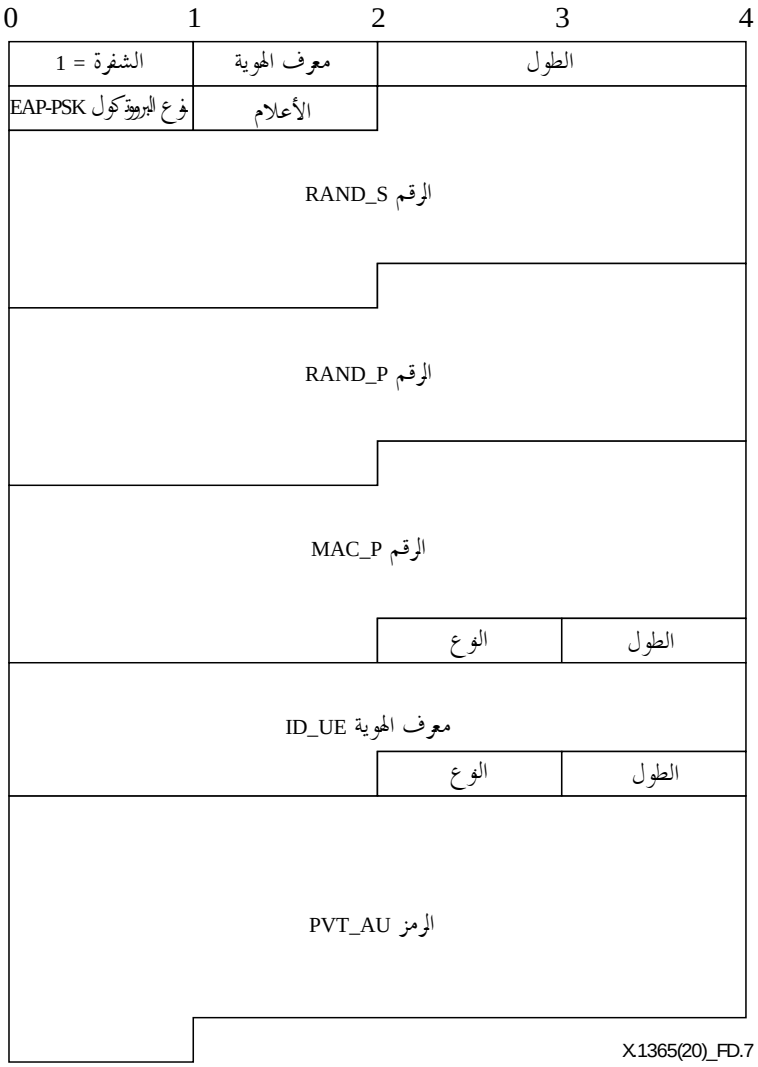
الشكل 6.D – نسق رسالة من أجل EAP-PSK--ECCSI

3.4.D الرسالة الثانية EAP-PSK--ECCSI (الرسالة 5 في الشكل 4.D)

يرسل الطرف النظير الرسالة الثانية EAP-PSK-ECCSI إلى المخدّم. ويتكون نسق صيغة الرسالة مما يلي:

- حقل أعلام من بايتة واحدة؛
- رقم عشوائي 16 بايتة مرسل من المخدِّم في الرسالة الأولى EAP-PSK—ECCSI message (RAND_S) حيث يعمل كمعرِّف هوية للدورة؛
- رقم عشوائي من 16 بايتة: RAND_P؛
- رقم تحكم في النفاذ إلى الوسائط مكون من 16 بايتة (MAC): MAC-P؛
- حقل بطول متغير ينقل معرِّف النفاذ إلى الشبكة الخاص بالأطراف النظيرة: ID_P. ويستنتج طول هذا الحقل من حقل طول بروتوكول الاستيقان القابل للتوسيع. ويجب ألا يتجاوز طول معرِّف النفاذ إلى الشبكة هذا 966 بايتة.

وعلى نحو مماثل، يُستعمل حقل معرِّف الهوية ID_S للبروتوكول EAP-PSK من أجل حمل معرِّف الهوية ID_UE وحقل الرمز PVT_UE. ويظهر الشكل 7.D نسق الرسالة الثانية للبروتوكول EAP-PSK.



الشكل 7.D – نسق رسالة من أجل الرسالة الثانية بشأن التوقيعات EAP-PSK--ECCSI

4.4.D الرسالة الثالثة EAP-PSK--ECCSI (الرسالة 10 في الشكل 4.D)

يرسل المخدم الرسالة الثالثة EAP-PSK--ECCSI إلى الطرف النظير. والنسق هو نفسه الوارد في المعيار [IETF RFC 4764].

5.4.D الرسالة الرابعة EAP-PSK--ECCSI (الرسالة 12 في الشكل 1-4.D)

يرسل الطرف النظير الرسالة الرابعة EAP-PSK--ECCSI إلى المخدِّم. والنسق هو نفسه الوارد في المعيار [IETF RFC 4764].

التذييل I

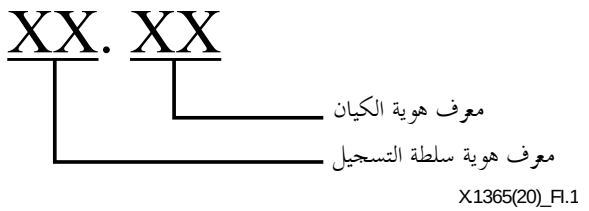
تسمية الهوية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

يمكن أن يكون معرِّف الهوية في أحد تطبيقات إنترنت الأشياء هو معرِّف الهوية لجهاز طرفي أو معرِّف الهوية لمنصة إنترنت الأشياء. ومعرِّف الهوية هو اسم يخدم الغرض من تحديد الهوية. وهو تمثيل للغرض سهل التناول يتيح، على سبيل المثال، الإحالة إلى الغرض أو استهدافه في قاعدة بيانات معينة أو في بروتوكولات الاتصالات. وسعياً إلى تحقيق هذا الغرض، يجب أن تكون معرِّفات الهوية فريدة، أو يكون معرِّف الهوية فريداً في نظام مستقل. فعلى سبيل المثال، يُعد الرمز البريدي فريداً في بلد ما، ويأخذ معرِّف الهوية طابع التفرد في نطاق معين. وبالإضافة إلى ذلك، لا يقتصر معرِّف الهوية على غرض واحد، بل يخص مجموعة من الأغراض أيضاً، مما يُمكّن من إدارة هذه المجموعة وتشغيلها بشكل منتظم.

واشتركت المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية مع قطاع تقييس الاتصالات بالاتحاد (ITU-T) في وضع توصيتين لمعرِّفات هوية الأغراض [b-ITU-T X.660] و[b-ITU-T X-Sup.31]، ولهذه المعرِّفات العديد من الخصائص. ويتمتع معرِّف هوية الغرض ببنية شجرية هرمية يمكن تمديد طبقاتها وطول معرِّفات الهوية فيها بمرونة. ويقابل معرِّف هوية الغرض عقدة في هذه الشجرة، تكون قادرة على تحديد أي شيء (مادي أو افتراضي، جهاز أو غير جهاز)، وقادرة على توصيلها بالبنى التحتية العالمية للمعلومات والاتصالات. ويحتوي جذر الشجرة على الأقواس الثلاثة التالية: 0 (قطاع تقييس الاتصالات)، و1 (المنظمة الدولية للتوحيد القياسي)، و2 (المنظمة الدولية للتوحيد القياسي بالاشتراك مع قطاع تقييس الاتصالات). وتُمثَّل كل عقدة في هذه الشجرة بسلسلة من الأعداد الصحيحة المفصولة بفترات، والمقابلة للمسار انطلاقاً من الجذر وصولاً إلى العقدة مروراً بسلسلة من العقد الأساسية. وينبغي أن تقوم سلطة التسجيل ذات المستوى الأعلى بتوزيع كل مستوى من مستويات معرِّفات هوية سلطة التسجيل. فعلى سبيل المثال، يُوزَّع معرِّف هوية الغرض الذي يرمز إلى المركز الوطني في الصين لتسجيل البطاقات IC، 1.2.156.20005، بواسطة 1.2.156 (ISO.member.china)، لمعرِّف هوية الغرض الخاص بالمركز الوطني في الصين لتسجيل معرِّفات هوية الأغراض.

ويتمثل معرِّف هوية الغرض الكامل في مزيج من معرِّف هوية سلطة التسجيل ومعرِّف هوية الكيان، ويتم الفصل بين هذين المكونين بفترة، على النحو المبيَّن في الشكل 1.I. وإذا سجلت الشركة معرِّف هوية لغرض ما من قبل سلطة التسجيل ذات المستوى الأعلى، فلا يتطلب الأمر إلا تصميم معرِّف هوية الكيان.



الشكل 1.I – بنية معرِّف هوية الغرض الكامل فيما يتعلق بالأغراض

على سبيل المثال، لمعرِّف هوية الكيان البنية الواردة في الجدول 1.I.

الجدول 1.I – معلومات مفصلة عن معرِّف هوية الكيان

البايتة	المكون	التفسير
1	الإصدار ومحجوز	4 بتات لإصدار معرِّف هوية الكيان، و4 بتات للأرقام المحجوزة للمستقبل
2	الأعمال	نوع الأعمال
11~3	وقت انتهاء الصلاحية	وقت انتهاء صلاحية الهوية، 5 بايتات لوقت الإصدار بالنظام Unix، و4 بايتات لفترة الصلاحية بالثواني
12	النمط	القيمة صفر لرقم لا معنى له، والقيمة 1 للتحكم في النفاذ إلى الوسائط، والقيمة 2 لهوية الاشتراكات المتنقلة الدولية
13	الطول (القيمة *l*)	حجم الجزء الخاص بالقيمة (بالبايتات)، القيمة 6 للتحكم في النفاذ إلى الوسائط، والقيمة 8 لهوية الاشتراكات المتنقلة الدولية
l+13~14	القيمة	رقم تعرف هوية فردي

يبلغ طول معرِّف هوية الكيان 19 بايتة عند استخدام التحكم في النفاذ إلى الوسائط كرقم تعرف هوية فردي و21 بايتة عند استخدام هوية الاشتراكات المتنقلة الدولية. وعادة ما يتم تقديم هوية الاشتراكات المتنقلة الدولية كعدد مكوَّن من 15 رقماً أو أقل، بحيث لا يكون الرقم الأول صفراً باستثناء شبكة الاختبار [b-ITU-T E.212]. وإضافة أصفار قبل هوية الاشتراكات المتنقلة الدولية إلى الأرقام البالغ عددها 16 رقماً واستخدام 4 بتات للرقم الواحد، فإن 8 بايتات تكفي لهوية الاشتراكات المتنقلة الدولية.

وتحتفظ منصة إنترنت الأشياء بقائمة للعناوين. وعندما يسجل جهاز طرفي لأول مرة، تضيف المنصة صفاً يحتوي على كل من معرِّف هوية الجهاز وعنوان بروتوكول الإنترنت (IP) الخاص به. ومن خلال البحث عن معرِّف هوية جهاز معين في القائمة، يمكن الحصول على عنوان بروتوكول الإنترنت المقابل للجهاز. انظر الجدول 2.I.

الجدول 2.I – مثال يتعلق بقائمة العناوين

معرِّف الهوية	عنوان بروتوكول الإنترنت
1.2.9c.4e25.10.1.5b3e408003c26700.1.6.38B1DBC3156F	192.168.0.1

التذييل II

تمديدات بروتوكول قابلية التشغيل البيني لإدارة المفاتيح من أجل دعم التجفير القائم على الهوية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

يمكن تمديد بروتوكول قابلية التشغيل البيني لإدارة المفاتيح على النحو التالي لدعم عمليات التجفير القائم على الهوية المطلوبة مع خدمة إدارة المفاتيح، ولا سيما تدميث النظام ببروتوكول قابلية التشغيل البيني لإدارة المفاتيح وتوليد المفاتيح الخاصة مع عمليات بروتوكول قابلية التشغيل البيني لإدارة المفاتيح على النحو المعرف في الفقرتين 1.C و4.C على التوالي.

تتكون الحمولة النافعة للطلب فيما يتعلق بإنشاء زوج المفاتيح على النحو الوارد في الجدول 1.II.

الجدول 1.II – الحمولة النافعة للطلب

الغرض	مطلوب	الوصف
نعت نموذج المفاتيح الخاصة	نعم	يحدد النعوت عند توليد الوظيفة IBSetup للمفتاح *ib.msk* والمعلمات *ib.pubparam*.

يشمل نعت نموذج المفاتيح الخاصة النعوت المدرجة في الجدول 2.II.

الجدول 2.II – النموذج السمة للمفاتيح الخاصة

الغرض	مطلوب	التشفير	الوصف
خوارزمية التجفير	نعم	التعداد، انظر الجدول 3.II	تحدد الوظيفة IBSetup.
طول التجفير	لا	عدد صحيح	يحدد طول خصائص الحقل الأساسي الذي يستند إليه المنحنى الإهليلجي، بالبتات.
قناع استخدام التجفير	نعم	عدد صحيح	يحدد استخدام المفتاح *ib.msk* الذي يكون إشارة لتوليد المفاتيح. الوظيفة IBExtract في الأساس عملية توقيع.
معلمات ميدان التجفير	نعم	الغرض	تحدد المزيد من المعلمات من أجل اختيار معلمات النظام، مثل المنحنى الإهليلجي المستخدم.
معلمات التجفير	نعم	الغرض	تحدد وظائف أخرى، مثل وظيفة الاختزال، التي تُستخدم مع الوظائف IBExtract.

خوارزمية التجفير هي واحدة من القيم المدرجة في الجدول 3.II.

الجدول 3.II – خوارزمية التجفير (توليد المفاتيح)

الاسم	القيمة
IBC-KGA-BB1	00000030
IBC-KGA-BF	00000031
IBC-KGA-ECCSI	00000032
IBC-KGA-SK	00000033
IBC-KGA-SM9	00000034

طول التجفير هو قيمة تساوي 110 أو تزيد عنها.

يضبط استخدام التجفير كالتالي 00000001 (إشارة).

تشمل معلمات ميدان التجفير النعوت المدرجة في الجدول 4.II.

الجدول 4.II – معلمات مجال التجفير

الغرض	مطلوب	التشفير	الوصف
الطول Q	لا	عدد صحيح	يحدد طول ترتيب المجموعة التي يتم اختيار المفتاح *ib.msk* منها، بالبتات.
منحنى موصى به	نعم	التعداد، انظر الجدول 5.II	يحدد المنحنى المستخدم.
نوع المزاوجة	لا	التعداد، انظر الجدول 6.II	إذا استُخدم، يحدد المزاوجة في خوارزمية قائمة على الهوية.
اسم الميدان	لا	سلسلة نصية	يحدد اسماً فريداً لمعلمات النظام المولَّدة *ib.pubparam*.
الرقم التسلسلي للميدان	لا	عدد صحيح	يحدد رقم الإصدار لمعلمات النظام المولَّدة *ib.pubparam*.

المنحنى الموصى به هو إحدى القيم المدرجة في الجدول 5.II.

الجدول 5.II – المنحنى الموصى به

الاسم	القيمة
IBC-CURVE-SS1	00000070
IBC-CURVE-SS2	00000071
IBC-CURVE-BN-254-1	00000072
IBC-CURVE-BN-256-1	00000073
IBC-CURVE-BN-256-2	00000074
IBC-CURVE-BN-382-1	00000077
IBC-CURVE-BLS-12-381-1	0000007A
IBC-CURVE-BLS-12-442-1	0000007B
IBC-CURVE-BLS-12-455-1	0000007C
IBC-CURVE-BLS-12-461-1	0000007D
IBC-CURVE-KSS-16-340-1	0000007E
IBC-CURVE-KSS-18-348-1	0000007F

نوع المزاوجة هو إحدى القيم المدرجة في الجدول 6.II.

الجدول 6.II – نوع المزاوجة

الاسم	القيمة
Weil-Pairing	00000001
Tate-Pairing	00000002
Optimal-Ate-Pairing	00000003

تشمل معلمات التجفير النعوت المدرجة في الجدول 7.II.

الجدول 7.II – معلمات التجفير

الغرض	مطلوب	التشفير	الوصف
خوارزمية الاختزال	نعم	التعداد، انظر الجدول 8.II	تحدد وظيفة الاختزال التي يجب أن تُستخدم مع وظيفة توليد المفاتيح.
مجموعة المفاتيح الخاصة	لا	التعداد، انظر الجدول 9.II	تحدد في أي مجموعة تُولَّد المفاتيح الخاصة في حالة استخدام المزاوجة.

خوارزمية الاختزال هي إحدى القيم المدرجة في الجدول II.8.

الجدول II.8 – خوارزمية التجفير (الاختزال)

الاسم	القيمة
SHA224	00000040
SHA256	00000041
SHA384	00000042
SHA512	00000043
SHA3-224	00000044
SHA3-256	00000045
SHA3-384	00000046
SHA3-512	00000047
SM3	00000048

مجموعة المفاتيح الخاصة هي إحدى القيم المدرجة في الجدول II.9.

الجدول II.9 – مجموعة المفاتيح الخاصة

الاسم	القيمة
IBC-PRK-GROUP1	00000001
IBC-PRK-GROUP2	00000002
IBC-PRK-TWOGROUPS	00000003

تتكون الحمولة النافعة لردود أزواج المفاتيح المنشأة على النحو الوارد في الجدول II.10.

الجدول II.10 – حمولة الردود

الغرض	مطلوب	الوصف
معرِّف الهوية الفريد للمفاتيح الخاصة	نعم	معرِّف الهوية الفريد لغرض المفاتيح الخاصة المنشأة حديثاً والذي يمكن استخدامه للنفاذ إلى المفتاح *ib.msk*. يتم تشفير معرِّف الهوية بوصفه سلسلة نصية.
معرِّف الهوية الفريد للمفاتيح العمومية	نعم	معرِّف الهوية الفريد لغرض المفاتيح العمومية المنشأة حديثاً والذي يمكن استخدامه للنفاذ إلى المعلمات *ib.pubparam*. يتم تشفير معرِّف الهوية بوصفه سلسلة نصية.

تتكون الحمولة النافعة لطلب عملية الحصول على النحو الوارد في الجدول II.11.

الجدول II.11 – الحمولة النافعة للطلب

الغرض	مطلوب	الوصف
معرِّف الهوية الفريد للمفاتيح العمومية	نعم	معرِّف الهوية الفريد لغرض المفاتيح العمومية الذي يمكن استخدامه للنفاذ إلى المعلمات *ib.pubparam*. يتم تشفير معرِّف الهوية بوصفه سلسلة نصية.

تتكون الحمولة النافعة للرد على النحو الوارد في الجدول II.12.

الجدول II.12 – الحمولة النافعة للرد

الغرض	مطلوب	الوصف
نوع الغرض	نعم	نوع الغرض
معرِّف الهوية الفريد	نعم	معرِّف الهوية الفريد للغرض
المفتاح العمومي	نعم	تشمل بنية المفاتيح العمومية بيانات المعلمات العمومية للتجفير القائم على الهوية *ib.pubparam*

معرِّف الهوية الفريد هو نفسه معرِّف الهوية الفريد للمفتاح العمومي الذي أُرسل في الحمولة النافعة لطلب الحصول.

نوع الغرض هو 00000003 (مفتاح عمومي).

تتكون مجموعة المفاتيح في حقل المفاتيح العمومية على النحو الوارد في الجدول II.13.

الجدول II.13 – مجموعة المفاتيح في حقل المفاتيح العمومية

الغرض	مطلوب	التشفير	الوصف
نوع نسق المفاتيح	نعم	التعداد، انظر الجدول II.14.	يحدد نسق قيمة المفاتيح.
انضغاط المفاتيح	لا	التعداد.	يحدد ما إذا كان ينبغي ضغط قيمة المفاتيح.
قيمة المفاتيح	نعم	بنية مفاتيح شفافة للمعلمات العمومية للتجفير القائم على الهوية.	بنية مفاتيح شفافة تعرف حديثاً فيما يتعلق بالمفاتيح العمومية للتجفير القائم على الهوية.
خوارزمية التجفير	نعم	التعداد، انظر الجدول II.15.	على غرار الحمولة النافعة لطلب زوج المفاتيح المنشأة.

نوع نسق المفاتيح هو القيمة في الجدول II.14.

الجدول II.14 – نوع نسق المفاتيح

الاسم	القيمة
المعلمات العمومية للتجفير الشفاف القائم على الهوية	00000016

ضغط المفتاح إما أن يكون 00000001 (غير مضغوط) أو 00000002 (مضغوط أساساً).

لقيمة المفتاح النعوت المدرجة في الجدول II.15:

الجدول II.15 – قيمة المفتاح

الغرض	مطلوب	التشفير	الوصف
P	لا	عدد صحيح كبير	فيما يتعلق بالمنحنيات القائمة على حقل أولي، P هو الخاصية (p) للحقل الأولي.
Q	لا	عدد صحيح كبير	Q هو ترتيب المجموعة الفرعية للنقطة *G*1 التي تُحسب فيها عمليات التجفير.
J	لا	عدد صحيح كبير	J هو العامل المشارك على غرار J*Q = X-1، حيث X هو ترتيب مجموعة النقاط للمنحنى المحدد.
السلسلة P1	نعم	سلسلة بايتات	فيما يتعلق بالخوارزميات القائمة على المزاوجة، P1 هو مولد مجموعة المزاوجة *G*1. وفيما يتعلق بالخوارزميات غير القائمة على المزاوجة، P1 هو مولد المجموعة الفرعية للنقطة العاملة.
السلسلة P2	لا	سلسلة بايتات	فيما يتعلق بالخوارزميات القائمة على المزاوجة، P2 هو مولد المجموعة *G*2 للمزاوجة.
السلسلة sP1	لا	سلسلة بايتات	sP1 هي النتيجة المتدرجة للنقطة P1[*ib.msk*] أو النتيجة المتدرجة لمكوّن عدد صحيح للمفتاح *ib.msk* باستخدام النقطة P1
السلسلة sP2	لا	سلسلة بايتات	فيما يتعلق بالخوارزميات القائمة على المزاوجة، sP2 هي النتيجة المتدرجة للنقطة P2[*ib.msk*] أو النتيجة المتدرجة لمكوّن عدد صحيح للمفتاح *ib.msk* باستخدام النقطة P2.
السلسلة sP3	لا	سلسلة بايتات	انطلاقاً من بعض الخوارزميات القائمة على المزاوجة (خاصةً الخوارزميات التي تستخدم وظيفة توليد المفاتيح BB1)، sP3 هي النتيجة المتدرجة لمكوّن عدد صحيح آخر للمفتاح *ib.msk* باستخدام النقطة P1.
سلسلة المزاوجة العمومية	لا	سلسلة بايتات	فيما يتعلق ببعض الخوارزميات القائمة على المزاوجة، فإن المزاوجة العمومية هي نتيجة مزاوجة (P1، P2[s]) أو مزاوجة (P1[s]، P2) أو مزاوجة (P1، P2)، حيث s هي المفتاح *ib.msk*، فيما يتعلق بالخوارزميات مثل SM9 أو SK-KEM أو SK-KEM أو (P1[s1]، P2[s2]) من أجل الآلية BB1-KEM، حيث s1 وs2 هما مكونان صحيحان للمفتاح *ib.msk*.

تُدرَج تعاريف الوسوم الجديدة في الجدول II.16.

الجدول II.16 – تعاريف الوسوم

الغرض	القيمة
نوع المزاوجة	420100
مجموعة المفاتيح الخاصة	420101
اسم الميدان	420102
الرقم التسلسلي للميدان	420103
السلسلة P1	420104
السلسلة sP1	420105
السلسلة P2	420106
السلسلة sP2	420107
السلسلة sP3	420108
سلسلة المزاوجة العمومية	420109

تتكوّن الحمولة النافعة للطلب فيما يتعلق بالتأشير على النحو الوارد في الجدول II.17.

الجدول II.17 – حمولة الطلب فيما يتعلق بالتأشير

الغرض	مطلوب	الوصف
معرِّف الهوية الفريد	لا	معرِّف الهوية الفريد للغرض المدار الخاضع للتجفير هو مفتاح *ib.msk* يُستخدم في عملية الاستخلاص **IBExtract**. وإذا تم إغفاله، تُستخدم بالتالي القيمة المستحوذة على المكان الخاص بمعرِّف الهوية عن طريق المخدّم كمعرِّف هوية فريد.
معلمات التجفير	لا	يمكن لمعلمات التجفير أن تحدد المجموعة التي يستخلص منها المفتاح الخاص.
البيانات	نعم	تحدد البيانات قيمة الهوية التي يستخلص منها المفتاح الخاص.

تشمل معلمات التجفير النعوت المدرجة في الجدول II.18.

الجدول II.18 – معلمات التجفير

الغرض	مطلوب	التشفير	الوصف
مجموعة المفاتيح الخاصة	لا	التعداد، انظر الجدول II.19.	تحدد المجموعة (*G*1 أو *G*2) التي يتولد منها المفتاح الخاص.

بيبليوغرافيا

[b-ITU-T E.101] Recommendation ITU-T E.101 (2009), *Definitions of terms used for identifiers (names, numbers, addresses and other identifiers) for public telecommunication services and networks in the E-series Recommendations*.

[b-ITU-T E.212] Recommendation ITU-T E.212 (2016), *The international identification plan for public networks and subscriptions*.

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

[b-ITU-T X.660] Recommendation ITU-T X.660 (2011), *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*.

[b-ITU-T X.1361] Recommendation ITU-T X.1361 (2018), *Security framework for the Internet of things based on the gateway model*.

[b-ITU-T X-Sup.31] ITU-T X-series Recommendations – Supplement 31 (2017), *ITU-T X.660 – Supplement on guidelines for using object identifiers for the Internet of things*.

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

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

[b-ISO/IEC 9798-3] ISO/IEC 9798-3:2019. *IT Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*.

[b-ETSI TR 118 508] ETSI TR 118 508 V1.0.0 (2014), *Analysis of Security Solutions for the oneM2M System*.
<https://www.etsi.org/deliver/etsi_tr/118500_118599/118508/01.00.00_60/tr_118508v010000p.pdf>

[b-ETSI TS 133.501] ETSI TS 133 501 V15.2.0 (2018), *5G; Security architecture and procedures for 5G system (3GPP TS 33.501 version 15.1.0 Release 15)*.
<https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.01.00_60/ts_133501v150100p.pdf>

[b-GM/T 0044.2] GM/T 0044.2-2016, *Identity-based cryptographic algorithms SM9 – Part 2: Digital signature algorithm*.

[b-GSMA SGP.02] GSMA Official Document SGP.02 Version 3.1 (2016), *Remote Provisioning Architecture for Embedded UICC – Technical Specification*.

[b-IANA TLS REG] Internet Assigned Numbers Authority (IANA), *Transport Layer Security (TLS) Parameters*. Website available, last viewed 2019-07-12.
<https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml>

[b-IEEE 1363] IEEE 1363-2000, *IEEE Standard Specifications for Public-Key Cryptography*.

[b-IEEE P1363.3] IEEE P1363.3/D9 (May 2013), *IEEE Standard for Identity-Based Cryptographic Techniques using Pairings*.

[b-IETF RFC 3748] IETF RFC 3748 (2004). *Extensible Authentication Protocol (EAP)*.

[b-OASIS KMIP] OASIS (2016), *Key Management Interoperability Protocol Specification Version 1.3*.
<http://docs.oasis-open.org/kmip/spec/v1.3/os/kmip-spec-v1.3-os.pdf>

[b-Barreto] Barreto, P. S. L. M., Libert, B., McCullagh, N., Quisquater, J.-J. (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In: Roy B. (ed.). *Advances in Cryptology – ASIACRYPT 2005, pp. 515-532. Lecture Notes in Computer Science*, vol. 3788. Berlin: Springer

[b-Chen] Chen, L., Malone-Lee, J. (2005). Improved identity-based signcryption. In: Vaudenay S. (ed). *Public Key Cryptography – PKC 2005, pp. 362-379. Lecture Notes in Computer Science*, vol. 3386. Berlin: Springer.

[b-Ducas] Ducas, L., Lyubashevsky, V., Prest, T. (2014). Efficient identity-based encryption over NTRU lattices. In: Sarkar P., Iwata T. (eds). *Advances in Cryptology – ASIACRYPT 2014, pp. 22-41. Lecture Notes in Computer Science*, vol. 8874. Berlin: Springer.

[b-Freeman] Freeman, D., Scott, M., Teske, E. (2010). A taxonomy of pairing-friendly elliptic curves. *J. Cryptol*. **23**, pp. 224–280.

[b-Galbraith] Galbraith, S.D., Paterson, K.G., Smart, N.P. (2008). Pairings for cryptographers. *Discrete Appl. Math*., **156**, pp. 3113-3121.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2020