مصدر التكنولوجيا

لخدمات النظم والبرمجيات

والتجارة العامة المحدودة

البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI)

هيئة تصديق ختم الوقت

البيان المعتمد لممارسات الشهادات

التحكم في الوثيقة

أعد بواسطة	راجعه	وافق عليه	المالك	الإصدار	تاريخ الموافقة
			مصدر التكنولوجيا	1.2	

سجل التغييرات

الرقم التسلسلي	الإصدار	وصف التغييرات	
0.1	29/01/2023	النسخة الأولية	مصطفى طوير
0.2	23/02/2023	مراجعة داخلية وتحديث	أحمد إبراهيم
0.3	04/12/2023	إضافة قيمOID معلومات الاتصال وعنوان مستودع الوثائق وتطبيق قالب مصدر التكنولوجيا	مصطفى طوير
0.4	28/02/2024	معالجة ملاحظات المدقق	مصطفى طوير و ياسر خان
0.5	14/03/2024	مراجعة وتحديث بناءً على ملاحظات المدقق بخصوص سياسة الشهادات CP وبيان الممارسة CPS الخاص بالجذر وهيئة تقديم الخدمة الموثوقة TSP	مصطفى طوير و ياسر خان
0.6	02/05/2024	تحديث في القسم 5.4.1 لتوضيح البيانات المطلوب تسجيلها ضمن متطلبات تسجيل أنشطة الجدار الناري والموجه	مصطفى طوير
0.7	15/05/2024	مراجعة وتحديث بناءً على ملاحظات المدقق بخصوص بيانات ممارسة الشهاداتCPSs	مصطفى طوير و ياسر خان
1.0	15/07/2024	تحديثات بناءً على توصيات المدقق بعد تدقيق نقطة في الزمن	مصطفى طوير و ياسر خان
1.1	16/09/2025	المراجعة السنوية	شركة مصدر التكنولوجيا

الرقم التسلسلي	الإصدار	وصف التغييرات	
1.2	03/06/2026	تعديل لتغيير مصطلح "اتفاقية المشترك" إلى "شروط وأحكام استخدام المشترك."	شركة مصدر التكنولوجيا

الموافقة على الوثيقة

رقم الإصدار	الاسم / اللقب المعتمد	التواقيع	
1.2	مدير مجلس حوكمة البنية التحتية للمفتاح العام		
		التاريخ	
		03/06/2026	

Contents

1 المقدمة

يمثل هذا المستند بيان ممارسة الشهادات (CPS) الذي يصف ممارسات التصديق المطبقة من قبل هيئة إصدار الختم الزمني التابعة لشركة مصدر التكنولوجيا) ويُشار إليها لاحقاً بـ .(TS يتوافق هذا البيان مع سياسة شهادات مقدم خدمات الثقة(TSP Certificate Policy) المطبقة على تقديم خدمات التصديق من قبل مقدمي خدمات الثقة الذين يُصدرون شهادات موثوقة علنياً للجهات النهائية ضمن هيكلية هيئات التصديق الجذرية الوطنية للبنية التحتية للمفتاح العام في جمهورية العراق.

يتناول هذا البيان السياسات الفنية والإجرائية والتنظيمية الخاصة بهيئة ختم الوقت التي تنشئها وتديرها TS ضمن تسلسل هيئات التصديق الوطنية العراقية وفيما يتعلق بكامل دورة حياة الشهادات التي تصدرها هذه الهيئة.

يشمل هذا البيان إصدار الشهادات والإجراءات الرقابية المرتبطة بالنوعين التاليين من شهادات هيئة ختم الوقت:

- شهادة CS لهيئة ختم الوقت: شهادة تُستخدم في توقيع البرمجيات.
- شهادة DS لهيئة ختم الوقت: شهادة تُستخدم في توقيع المستندات.

يتوافق هذا البيان مع المتطلبات الشكلية لمجموعة عمل هندسة الإنترنت (IETF) كما وردت في [RFC 3647] من حيث البنية والمحتوى. ورغم إدراج بعض العناوين وفقاً لبنية[RFC 3647] قد لا تنطبق بعض المواضيع على تنفيذ هيئة ختم الوقت. وتُصنّف هذه البنود بعبارة "البند غير قابل للتطبيق".

كما يتوافق البيان مع مبادئ ومتطلبات WebTrust لهيئات التصديق والمنشورة على الموقع : https://www.cpacanada.ca.

يُؤكد مجلس البنية التحتية للمفاتيح العامة في TS التزامه بالحفاظ على هذا البيان متوافقاً مع الإصدارات الحالية من المتطلبات التالية والمنشورة على الموقع http://www.cabforum.org ::

- المتطلبات الأساسية لإصدار وإدارة شهادات توقيع البرمجيات الموثوقة.
- متطلبات أمان الشبكة ونظام الشهادات.

في حال وجود أي تعارض بين هذا المستند والمتطلبات المشار إليها أعلاه تكون الأولوية للمتطلبات العليا.

يُعد هذا البيان متاحاً للعامة وفي حال احتوى المستند على معلومات سرية يُشار إلى وثائق سرية متاحة فقط للأشخاص المخولين بالاطلاع عليها.

للحصول على مزيد من المعلومات بشأن هذا البيان يُرجى التواصل مع مجلس PKI فيTS باستخدام معلومات الاتصال الواردة في البند 1.5.

1.1 نظرة عامة

أُنشئت البنية التحتية الوطنية للمفاتيح العامة العراقية ((PKI تحت إشراف الشركة العامة للاتصالات والمعلوماتية (ITPC)وتضم عدداً من هيئات التصديق الجذرية التي تمثل البرنامج الوطني للبنية التحتية للمفتاح العام ومن خلال هذه البنية تهدف الحكومة العراقية إلى توفير إطار عمل يُسهم في تأسيس مقدمي خدمات موثوقين (TSP) يقدمون خدمات التصديق الرقمي وخدمات الثقة للجهات الحكومية وغير الحكومية.

يتكون التسلسل الهرمي للبنية التحتية الوطنية للمفتاح العام من مستويين كما يلي:

المستوى 0:

تأسيس خمس (5) هيئات تصديق جذرية مختلفة لتغطية أنواع الشهادات المتعددة التي سيتم إصدارها. تتولى الشركة العامة للاتصالات والمعلوماتية (ITPC) مسؤولية إدارة هذا المستوى من هيئات التصديق الجذرية وبصفتها الجهة الوطنية ل البنية التحتية للمفتاح العام و بـ ITPC تشغيل اللجنة العليا لإدارة التوقيع الإلكتروني .(PMA) وتشمل هيئات التصديق الجذرية التابعة لـ ITPC ما يلي:

- الجذر العراقي لتوقيع البرمجيات: يُصادق/يوقّع هيئات التصديق التابعة الخاصة بتوقيع البرمجيات.
- الجذر العراقي للبريد الإلكتروني الآمن :(S/MIME) يُصادق/يوقّع هيئات التصديق التابعة لحماية البريد الإلكتروني.
- الجذر العراقي لـ :TLS يُصادق/يوقّع هيئات التصديق التابعة الخاصة بـTLS .
- الجذر العراقي لتوقيع المستندات: يُصادق/يوقّع هيئات التصديق التابعة الخاصة بتوقيع وثائق الأشخاص الطبيعيين والاعتباريين.
- الجذر العراقي لختم الوقت: يُصادق/يوقّع هيئات التصديق التابعة لخدمات ختم الوقت.

المستوى 1:

تقع هيئات التصديق التابعة التابعة لشركة مصدر التكنولوجيا ضمن هذا المستوى من التسلسل الهرمي للبنية التحتية الوطنية للمفتاح العام وكما هو موضح في الشكل أدناه:

الشكل 1 - التسلسل الهرمي للبنية التحتية الوطنية للمفتاح العام في العراق.

فيما يتعلق بشهادات ختم الوقت تُعد هيئة التصديق الجذرية لختم الوقت العراقية هي الوحيدة ذات الصلة حيث تتولى توقيع شهادة هيئة التصديق التابعة لختم الوقت التابعة لشركة مصدر التكنولوجيا أما هيئات التصديق الجذرية الأخرى التابعة للبنية التحتية الوطنية للمفتاح العام في العراق فهي لا تمت بصلة لإصدار شهادات ختم الوقت وبالتالي لا تُدرج ضمن هيكل ختم الوقت كما هو موضح في الشكل 1.

تشغّل شركة مصدر التكنولوجيا هيئات التصديق التابعة وتقدم من خلالها خدمات الثقة ذات الصلة إلى القطاعات الحكومية وغير الحكومية في العراق وبناءً على ذلك تعمل شركة مصدر التكنولوجيا كمقدم لخدمات الثقة (TSP) من خلال تسلسل هرمي من هيئات التصديق التابعة التي تنجز تحت هيئات التصديق الجذرية التابعة للشركة العامة للاتصالات والمعلوماتية .(ITPC) وقد صادقت هيئات التصديق الجذرية التابعة لـ ITPC على هيئات التصديق التابعة الخاصة بـ TSP التابع لشركة مصدر التكنولوجيا على النحو التالي:

- هيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات لتوقيع مكتبات البرمجيات وملفات jar. و exe.و msi.وغيرها.
- هيئة التصديق للبريد الإلكتروني الآمن (S/MIME) التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات لتوقيع البريد الإلكتروني وتشفيره.
- هيئة التصديق لـ TLS التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات تحقق تنظيمي (OV) لخوادم الويب.
- هيئة التصديق لتوقيع المستندات للأشخاص الطبيعيين (NP) التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات توقيع المستندات للمواطنين والموظفين.
- هيئة التصديق لتوقيع المستندات للأشخاص الاعتباريين (LP) التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات توقيع المستندات للجهات الحكومية وغير الحكومية العراقية.
- هيئة التصديق لختم الوقت التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات هيئة ختم الوقت (TSA) المستخدمة في توقيع المستندات والبرمجيات.

تُعد حالات الاستخدام أعلاه من الركائز الأساسية للتحول الرقمي إذ تمثل حجر الزاوية في تأمين المعاملات الإلكترونية ودعم هذه الاستخدامات ضمن نموذج ثقة موحد بضمان حكومي يُسهّل التبني ويُعزز قابلية التشغيل البيني ويزيد من ثقة المستخدم.

يتواصل مجلس البنية التحتية للمفاتيح العامة في شركة مصدر التكنولوجيا (TS PKI GB) بشكل وثيق مع اللجنة العليا لإدارة التوقيع الإلكتروني التابعة لـ ITPC لضمان توافق هذا البيان (CPS) مع عمليات إصدار وتشغيل هيئة ختم الوقت الخاصة بشركة مصدر التكنولوجيا .

1.1.1 مجلس البنية التحتية للمفاتيح العامة في شركة مصدر التكنولوجيا

يُعرف مجلس الإدارة المسؤول عن حوكمة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا (بما في ذلك هيئة ختم الوقت) باسم مجلس TS PKI GB. يضم هذا المجلس الوظائف الأساسية المطلوبة لتوفير التوجيه الاستراتيجي والإشراف المستمر على عملياتTS PKI بما في ذلك السياسة والأمن والامتثال والشؤون القانونية.

يتحمل مجلس TS PKI GB المسؤوليات التالية بوجه خاص:

- تحديد استراتيجية TS PKI والحفاظ عليها.
- تحديد خدمات TS PKI والموافقة على نموذج تقديمها.
- تحديد سياسات وممارسات TS PKI والمحافظة عليها.
- تنفيذ أنشطة إشراف دورية على فريق عملياتTS PKI .
- الموافقة على ميزانية PKI واتخاذ القرارات التجارية الرئيسية.
- الموافقة على التغييرات الجوهرية في بنية PKI التحتية.
- الموافقة على مراسيم المفاتيح وتعيين المدققين الداخليين والخارجيين حسب الحاجة.
- المشاركة في الحوادث الكبرى واتخاذ القرارات المناسبة عند الضرورة.
- قيادة تسوية النزاعات الناشئة عن أو المتعلقة بأنشطةTS PKI .
- تقييم الحوادث التي لم يلتزم فيها موظفو TS PKI الرئيسيون بالإجراءات الأمنية و التشغيلية بما في ذلك الجوانب الأخلاقية.

1.2 اسم الوثيقة ومعرّفها

عنوان هذه الوثيقة هو "بيان ممارسة الشهادات لهيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا" ويُعرّف بواسطة المعرّف الكائني (OID) التالي 2.16.368.1.2.1.5 : ويُشار إليه في الوثائق ذات الصلة بالاختصار .[TS TSA CA CPS] وقد أقرّ كل من مجلس TS PKI GB واللجنة العليا لإدارة التوقيع الإلكتروني في ITPC هذه الوثيقة للنشر.

تُدرج هيئة ختم الوقت هذا المعرّف الكائني (OID) في امتداد سياسة الشهادة (CP extension) ضمن الشهادات التي تصدرها للإشارة إلى التوافق مع المتطلبات الحالية.

1.3 المشاركون في البنية التحتية للمفتاح العام(PKI)

تشارك عدة جهات خلال إدارة دورة حياة الشهادات الرقمية التي تصدرها هذه الهيئة وتشمل هذه الجهات ما يلي:

- هيئة التصديق لختم الوقت التابعة لشركة مصدر التكنولوجيا.
- هيئات التسجيل التابعة لشركة مصدر التكنولوجيا (TS Registration Authorities - RA) .
- المشتركون.
- الأطراف المعتمدة.

ويُشار إلى هذه الجهات مجتمعة بمسمى "المشاركون في البنية التحتية للمفتاح العام"(PKI Participants) وسيُشرح دور كل منها في الفقرات التالية.

1.3.1 هيئات التصديق

تتولى شركة مصدر التكنولوجيا تشغيل وإدارة هيئة التصديق لختم الوقت ويُشار إليها لاحقاً بـ (CA من خلال مقارها في العراق. وقد جرت المصادقة على هذه الهيئة من قبل الشركة العامة للاتصالات والمعلوماتية ووقّعتها هيئة التصديق الجذرية العراقية لختم الوقت كما هو موضح في الشكل 1 (الفقرة 1.1) .تقدم هذه الهيئة خدمات التصديق التالية:

- خدمة إنشاء الشهادات: تُصدر الشهادات للجهات النهائية بناءً على التحقق الذي تنفذه هيئات التسجيل.
- خدمة النشر :تقوم بنشر شهادات هيئة التصديق واستجابات بروتوكولOCSP وتُتيحها للأطراف المعتمدة. كما تُوفر هذه الخدمة أي معلومات علنية تتعلق بالسياسات والممارسات للمشتركين والأطراف المعتمدة.
- خدمة إدارة الإلغاء :تتولى معالجة طلبات الإلغاء والتقارير ذات الصلة لتحديد الإجراء المناسب. وتُتاح نتائج هذه الخدمة عبر خدمة حالة صلاحية الشهادة.
- خدمة حالة صلاحية الشهادة :تُوفر معلومات حالة صلاحية الشهادات للأطراف المعتمدة استناداً إلى قوائم إلغاء الشهادات (CRL) وخدمة استجابة .OCSP ويجب أن تعكس معلومات الحالة دائماً الحالة الفعلية للشهادات الصادرة من هذه الهيئة.

1.3.2 هيئات التسجيل (RA)

تشغّل شركة مصدر التكنولوجيا وظيفة هيئة التسجيل (RA) التي تخدم هيئة التصديق لختم الوقت وتُعنى أساساً بمعالجة طلبات إصدار الشهادات لخدمات هيئة ختم الوقت .(TSA) تندرج وظيفة RA ضمن هيكل عمليات البنية التحتية للمفتاح العام وتتحمل مسؤولية التحقق من الهوية وإدارة طلبات الشهادات للجهات الحكومية وغير الحكومية.

تشمل مهام هيئة التسجيل في TS دون حصر ما يلي:

- المصادقة على طلبات الشهادات أو الموافقة عليها أو رفضها بما في ذلك طلبات الإلغاء.
- تحديد هوية المشتركين وفقاً لاتفاقيات التسمية المعتمدة في هذا البيان (CPS) بحيث يُعرَّف كل مشترك بطريقة فريدة وواضحة.
- معالجة طلبات إصدار الشهادات وطلبات الإلغاء استناداً إلى الطلبات التي جرت المصادقة عليها والموافقة عليها.
- إنشاء وصيانة سجل تدقيق يوثق جميع الأحداث الهامة المتعلقة بعمليات هيئة التسجيل.
- توفير وصول انتقائي إلى سجلات سجل التدقيق وفقاً لما هو محدد في هذا البيان.
- تنفيذ الضوابط التشغيلية الأخرى كما هو مذكور في هذا البيان ومعالجة وتخزين المعلومات بما يتوافق مع المتطلبات المنصوص عليها في هذا البيان لا سيما في القسم 5.

1.3.3 المشتركون

المشترك في هذه الهيئة هو شركة مصدر التكنولوجيا نفسها والتي تُشغّل خدمة هيئة ختم الوقت .(TS TSA) وبالنسبة لأي شهادة يُوقّع المشترك أو يُصادق على شروط وأحكام استخدام المشترك لتحديد الشروط والأحكام المنصوص عليها من قبل شركة مصدر التكنولوجيا.

1.3.4 الأطراف المعتمدة

يتوجب على الأطراف المعتمدة الرجوع بشكل دائم إلى خدمات التحقق من حالة صلاحية الشهادات الصادرة عن شركة مصدر التكنولوجيا مثل CRL وOCSP وذلك قبل الاعتماد على أية معلومات واردة في الشهادة المعنية.

1.3.5 مشاركون آخرون

تشمل الجهات الأخرى المشاركة ما يلي:

- اللجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية :(ITPC PMA) وهي السلطة الإشرافية المسؤولة عن مراقبة كامل نشاط مقدم خدمات الثقة المرخص له (أي شركة مصدر التكنولوجيا). وترد أدوار وصلاحيات اللجنة العليا لإدارة التوقيع الإلكتروني في سياسة الشهادات وبيان الممارسات لهيئات ITPC الجذرية والمنشورة على الرابط https://pki.itpc.goviq :.
- المدققون المستقلون المؤهلون وفق :WebTrust يتحققون من استيفاء المتطلبات الموضحة في القسم 8.2.

1.4 استخدام الشهادات

1.4.1 استخدامات الشهادات المسموح بها

تشمل الشهادات الصادرة عن هيئة التصديق لختم الوقت التابعة لشركة مصدر التكنولوجيا ما يلي:

1. شهادات خدمة هيئة ختم الوقت (TS TSA) :

شهادات وحدة الختم الزمني:

تُصدر هذه الشهادات من قبل سلطة التصديق التابعة الخاصة بالختم الزمني لغرض إنشاء وتدقيق الأختام الزمنية الإلكترونية. إن شهادات وحدة الختم الزمني الصادرة بموجب سياسة ممارسات التصديق هذه لصالح شركة مصدر

التكنولوجيا حصراً، تُستخدم لتقديم خدمة الختم الزمني وفقاً لسياسة وبيان ممارسات الختم الزمني المتاحة عبر الموقع الإلكتروني للمستودع الرقمي التابع للشركة pki.techsource.iq.

تتولى سلطة التصديق هذه إصدار شهادات وحدة الختم الزمني الآتية: .

- **شهادة الختم الزمني للتوقيع الرقمي:** وهي الشهادات المخصصة لتوقيع الأختام الزمنية المستخدمة في عمليات توقيع المستندات والوثائق.
- **شهادة الختم الزمني لتوقيع الشفرات البرمجية:** وهي الشهادات المخصصة لتوقيع الأختام الزمنية المستخدمة في عمليات توقيع البرمجيات والتطبيقات.

2. شهادة مستجيب OCSP: تُستخدم لتوقيع ردود بروتوكول حالة الشهادة عبر الإنترنت (OCSP) للشهادات الصادرة عن هذه الهيئة.

1.4.2 استخدامات الشهادات المحظورة

يُمنع منعاً باتاً استخدام الشهادات الصادرة من هذه الهيئة لأغراض غير مذكورة في القسم 1.4.1.

1.5 إدارة السياسة

1.5.1 الجهة المسؤولة عن إدارة الوثيقة

تتولى إدارة هذه الوثيقة (CPS) لجنة TS PKI (TS PKI GB) وفقاً لنموذج التشغيل المعتمد لديها وبناءً على التفاعل حسب الحاجة مع اللجنة العليا لإدارة التوقيع الإلكتروني فيITPC .

1.5.2 جهة الاتصال

يُوجّه أي طلب للحصول على معلومات أو استفسار يتعلق بهذه الوثيقة إلى :مجلس البنية التحتية للمفاتيح العامة .

شركة مصدر التكنولوجيا شركة.

مصدر التكنولوجيا.

العنوان: بغداد – الاربع شوارع – بالقرب من إعدادية المأمون.

البريد الإلكترونيinfo@techsource.iq :.

رقم الهاتف1693 136 784 (964+) :.

لا يقبل مجلس TS PKI GB أي تعليقات تتعلق بهذه الوثيقة (CPS) إلا إذا ارسلت إلى جهة الاتصال المذكورة أعلاه.

تقرير مشاكل الشهادات.

تحافظ شركة مصدر التكنولوجيا على قدرة دائمة (7/24) للاستجابة الداخلية لأي طلبات إلغاء ذات أولوية عالية أو بلاغات متعلقة بمشاكل الشهادات. وتوفر الشركة تعليمات مخصصة لإجراءات إلغاء الشهادات والإبلاغ عن المشاكل عبر صفحة مخصصة على موقعها الإلكتروني العام:

https://pki.techsource.iq/repository/Certificate Problem Report.html.

يجوز للمشتركين والأطراف المعتمدة وموردي برامج التطبيقات وأي جهات أخرى من الأطراف الثالثة الإبلاغ عن حالات مشتبه بها مثل اختراق المفتاح الخاص أو إساءة استخدام الشهادة أو أنواع أخرى من الاحتيال أو الاختراق أو السلوك غير الملائم أو أي مسائل أخرى تتعلق بالشهادات وذلك بإرسال بريد إلكتروني إلى:

certificate.problem@techsource.iq.

تتولى شركة مصدر التكنولوجيا التحقق من صحة بلاغ الإلغاء والتحقيق فيه قبل اتخاذ أي إجراء وذلك وفقاً لما ورد في القسم 4.9.

وفي حال رأت شركة مصدر التكنولوجيا أن ذلك مناسب فقد تقوم بإحالة تقارير الإلغاء إلى الجهات المختصة بإنفاذ القانون.

1.5.3 الشخص المسؤول عن تحديد ملاءمة CPS للسياسة

استناداً إلى نتائج وتوصيات تدقيقات الامتثال يتولى مجلس TS PKI GB مسؤولية تحديد مدى ملاءمة وقابلية تطبيق هذا البيان .(CPS) ويجب أن تتم الموافقة على هذا البيان من قبل اللجنة العليا لإدارة التوقيع الإلكتروني (PMA) أيضاً نظراً لضرورة توافقه النهائي مع أحكام سياسة الشهادات(TSP CP) .

1.5.4 إجراءات اعتماد CPS

يُقرّ مجلسTS PKI GB بالتعاون مع اللجنة العليا لإدارة التوقيع الإلكتروني (PMA) رسمياً أي إصدار جديد من هذا البيان .(CPS)

يقوم موظفون متخصصون في سياسات البنية التحتية للمفتاح العام (PKI) من مجلس TS PKI GB بمراجعة هذا البيان سواء في نسخته الأولية أو عند إدخال أية تعديلات لاحقة وذلك لضمان التوافق مع أفضل الممارسات المطبقة ومع سياسة الشهادات (TSP CP)قبل اعتمادها من قبل مجلس TS PKI GB.

قد تكون التعديلات على هذا البيان على شكل نسخة معدلة من الوثيقة بالكامل أو إشعار بالتحديث. ويتم تتبع جميع التغييرات في جدول المراجعات.

يُحال الإصدار الجديد من البيان بعد ذلك إلى اللجنة العليا لإدارة التوقيع الإلكتروني (PMA) للموافقة النهائية وذلك لضمان التوافق الكامل مع أحكام سياسة الشهادات الخاصة بمقدم خدمات الثقة(TSP CP) .

1.5.5 تحديثات CPS ودورية المراجعة

لضمان المصداقية وتعزيز الثقة في هذا البيان(CPS) وبما يتماشى مع متطلبات الاعتماد والمتطلبات القانونية يُجري مجلس TS PKI GBمراجعة دورية لهذا البيان مرة واحدة على الأقل سنوياً. ويجوز للمجلس إدخال تعديلات أو تحديثات على السياسات متى ما رأى ذلك مناسباً أو عند وجود ظروف أخرى تستدعي ذلك.

وقبل أن تُصبح النسخة المعدلة سارية المفعول عنها في مستودع الوثائق المنشور على الرابط التالي:
https://pki.techsource.iq.

وبعد نشرها تُعد النسخة المحدّثة ملزمة لجميع المشتركين بما في ذلك المشتركين والأطراف المعتمدة على الشهادات الصادرة بموجب نسخة سابقة من هذا البيان.

1.6 التعاريف والاختصارات

1.6.1 التعاريف

المتقدم بالطلب: الكيان الذي يتحكم أو يُشغّل الجهاز المسمى في الشهادة حتى وإن كان الجهاز هو الذي يرسل طلب الشهادة فعلياً. في سياق هذا البيان يُشير مصطلح "المتقدم بالطلب" إلى شركة مصدر التكنولوجيا المشغّلة لخدمة ختم الوقت.

ممثل المتقدم بالطلب: شخص طبيعي أو مفوض يتصرف بصفة المتقدم بالطلب أو موظف لديه أو وكيل مفوَّض قانونياً للقيام بالمهام التالية نيابةً عنه:

1. توقيع وتقديم أو الموافقة على طلب الشهادة.
2. توقيع وتقديم شروط وأحكام استخدام المشترك.
3. الموافقة على شروط الاستخدام نيابةً عن المتقدم بالطلب في حال كان المتقدم بالطلب هو جهة تابعة لهيئة التصديق أو الهيئة نفسها.

في سياق هذا البيان يتولى ممثل المتقدم بالطلب مسؤولية تقديم طلبات إصدار الشهادات وطلبات الإلغاء نيابةً عن المتقدم بالطلب. وتُستخدم عبارتا "ممثل المتقدم بالطلب" و"مقدم الطلب" بالتبادل.

مورد برامج التطبيقات : مزود برمجيات مستعرض الإنترنت أو أي برنامج طرف معتمد يستخدم أو يعرض الشهادات ويُضمّن شهادات الجذر ضمن بيئته البرمجية.

خطاب إثبات : خطاب يُثبت صحة معلومات الموضوع يُعدّه عادةً محاسب أو محامٍ أو مسؤول حكومي أو طرف ثالث موثوق يُعتمد عليه في مثل هذه الحالات. في سياق هذا البيان وقعت خطابات الإثبات من قبل فرق الموارد البشرية في الجهات الحكومية.

فترة التدقيق : في التدقيق المعتمد على فترة زمنية وتشير إلى الفترة الممتدة بين اليوم الأول (البداية) واليوم الأخير (النهاية) من العمليات التي يغطيها المدققون في مهمة التدقيق. (ولا تعني بالضرورة الفترة الزمنية التي يوجد فيها المدققون فعلياً في موقع هيئة التصديق).

تقرير التدقيق : تقرير صادر عن مدقق مؤهل يتضمن رأيه بشأن مدى امتثال عمليات وضوابط الكيان المعني للأحكام الإلزامية المنصوص عليها في هذه المتطلبات.

زوج مفاتيح هيئة التصديق : زوج مفاتيح تُدرج فيه المفتاح العام كمعلومة مفتاح عام موضوع الشهادة ضمن شهادة هيئة تصديق جذرية أو شهادة هيئة تصديق فرعية واحدة أو أكثر.

الشهادة : وثيقة إلكترونية تستخدم التوقيع الرقمي لربط مفتاح عام بهوية معينة.

بيانات الشهادة : تشمل طلبات الشهادات وأية بيانات ذات صلة (سواء جُمعت من المتقدم بالطلب أو من مصادر أخرى) وتكون في حيازة هيئة التصديق أو تحت سيطرتها أو ضمن نطاق وصولها.

عملية إدارة الشهادات : مجموعة العمليات والممارسات والإجراءات المرتبطة باستخدام المفاتيح والبرمجيات والأجهزة والتي من خلالها تقوم هيئة التصديق بالتحقق من بيانات الشهادة إصدار الشهادات إدارة المستودع وإلغاء الشهادات.

سياسة الشهادات : مجموعة من القواعد التي تُحدد مدى ملاءمة الشهادة المسماة لمجتمع معين اوتنفيذ معين للبنية التحتية للمفتاح العام يتمتع بمتطلبات أمنية مشتركة.

تقرير مشكلة الشهادة : شكوى تتعلق باشتباه في اختراق المفتاح أو إساءة استخدام الشهادة أو أنواع أخرى من الاحتيال أو السلوك غير المناسب المرتبط بالشهادات.

قائمة إلغاء الشهادات : قائمة موقّتة يتم تحديثها بانتظام تحتوي على الشهادات الملغاة وتُنشأ وتوقّع رقمياً من قبل هيئة التصديق التي أصدرت تلك الشهادات.

هيئة التصديق : كيان مسؤول عن إنشاء وإصدار وإلغاء وإدارة الشهادات. وينطبق المصطلح على كل من هيئات التصديق الجذرية والفرعية.

بيان ممارسة الشهادات : أحد الوثائق التي تُشكّل الإطار الحوكمي الذي يتم ضمنه إنشاء الشهادات وإصدارها وإدارتها واستخدامها.

ملف تعريف الشهادة : مجموعة من الوثائق أو الملفات التي تُحدد متطلبات محتوى الشهادة وامتداداتها بما يتوافق مع القسم 7 من المتطلبات الأساسية. على سبيل المثال: قسم في بيان ممارسة الشهادات الخاص بهيئة التصديق أو ملف قالب شهادة يُستخدم من قبل برمجيات هيئة التصديق.

التحكم : يُقصد بها وكذلك المشتقات ذات الصلة مثل "تحت السيطرة" أو "يخضع للسيطرة المشتركة" امتلاك بشكل مباشر أو غير مباشر القدرة على:

1. توجيه إدارة أو موظفي أو شؤون الكيان المالية أو التخطيطية .
2. التحكم في انتخاب أغلبية أعضاء مجلس الإدارة .
3. التصويت بالنسبة المطلوبة من الأسهم المقررة للسيطرة وفقاً لقوانين جهة التأسيس أو التسجيل الخاصة بالكيان بشرط ألا تقل في جميع الأحوال عن 10%.

الدولة : إما دولة عضو في الأمم المتحدة أو إقليم جغرافي معترف به كدولة ذات سيادة من قبل دولتين عضوين على الأقل في الأمم المتحدة.

جهاز التوثيق الثنائي : جهاز تشفير عبر منفذ USB حاصل على شهادة توافق مع المعيار FIPS 140 المستوى 2 أو ما يعادله.

مولد أرقام عشوائية آمن :(CSPRNG) مولد أرقام عشوائية مصمم للاستخدام ضمن أنظمة التشفير.

طرف ثالث مفوض : شخص طبيعي أو كيان اعتباري ليس من ضمن هيئة التصديق ولا تندرج أنشطته ضمن نطاق تدقيقات هيئة التصديق المعتمدة ولكنه مفوَّض من قبل الهيئة للمساعدة في عمليات إدارة الشهادات من خلال تنفيذ أو استيفاء أحد أو أكثر من متطلبات الهيئة المحددة في هذا البيان.

تاريخ الانتهاء : التاريخ المحدد في حقل تاريخ الانتهاء في الشهادة والذي يُحدد نهاية فترة صلاحية الشهادة.

جهة حكومية : كيان اعتباري تديره الحكومة مثل وكالة أو دائرة أو وزارة أو فرع أو ما شابه ضمن حكومة دولة ما أو إحدى تقسيماتها السياسية (مثل ولاية محافظة مدينة قضاء...إلخ).

طلب شهادة عالي الخطورة : طلب تحدده هيئة التصديق يتطلب تدقيقاً إضافياً استناداً إلى معايير داخلية وقواعد بيانات وقد يشمل ذلك الأسماء المعرّضة للاحتيال أو التصيّد أو تلك التي ظهرت في طلبات مرفوضة سابقاً أو شهادات ملغاة أو الأسماء المدرجة في قوائم التصيّد مثل Miller Smiles أو قائمة Google للتصفح الآمن أو أي أسماء تُحددها الهيئة استناداً إلى معاييرها الخاصة لتخفيف المخاطر.

هيئة التصديق المُصدِرة : الهيئة التي أصدرت الشهادة المعنية وقد تكون هيئة تصديق جذرية أو فرعية.

اختراق المفتاح : يُعتبر المفتاح الخاص مخترقاً إذا كشف عن قيمته لشخص غير مخوّل أو إذا حصل شخص غير مخوّل على إمكانية الوصول إليه.

نص إنشاء المفاتيح : خطة موثقة تتضمن الإجراءات الخاصة بإنشاء زوج مفاتيح هيئة التصديق.

زوج مفاتيح : المفتاح الخاص والمفتاح العام المرتبط به.

الكيان الاعتباري : جمعية أو شركة أو شراكة أو مؤسسة فردية أو مؤسسة ائتمانية أو جهة حكومية أو أي كيان آخر يتمتع بصفة قانونية وفقاً لنظام قانوني في دولة معينة.

معرّف الكائن : معرّف أبجدي رقمي أو رقمي فريد مُسجل بموجب المعيار المعتمد لدى المنظمة الدولية للمعايير(ISO) يُستخدم لتحديد كائن معين أو صنف كائنات.

مستجيب :OCSP خادم إلكتروني يعمل تحت سلطة هيئة التصديق ومرتبط بمستودعها لمعالجة طلبات التحقق من حالة الشهادات. يُراجع أيضاً بروتوكول حالة الشهادة عبر الإنترنت.

بروتوكول حالة الشهادة عبر الإنترنت : بروتوكول إلكتروني يُستخدم للتحقق من حالة الشهادة ويُتيح لبرامج التطبيقات التابعة للأطراف المعتمدة تحديد صلاحية شهادة معينة يُراجع أيضاً مستجيبOCSP .

المفتاح الخاص : هو المفتاح ضمن زوج مفاتيح ويُحتفظ به بسرية من قبل مالكه ويُستخدم لإنشاء التواقيع الرقمية أو لفك تشفير السجلات أو الملفات التي شفرت باستخدام المفتاح العام المقابل.

المفتاح العام : هو المفتاح ضمن زوج مفاتيح ويجوز لصاحبه نشره علناً ويُستخدم من قبل الطرف المعتمد للتحقق من التواقيع الرقمية المُوقعة بالمفتاح الخاص المقابل أو لتشفير رسائل لا يمكن فك تشفيرها إلا باستخدام المفتاح الخاص المقابل.

البنية التحتية للمفتاح العام : مجموعة من الأجهزة والبرمجيات والأشخاص والإجراءات والقواعد والسياسات والالتزامات تُستخدم لتسهيل إنشاء وإصدار وإدارة واستخدام الشهادات والمفاتيح بطريقة موثوقة استناداً إلى التشفير بالمفتاح العام.

شهادة موثوقة علناً : شهادة تُعد موثوقة نظراً لأن شهادة الجذر المقابلة لها موزّعة كنقطة ثقة ضمن برمجيات التطبيقات المتاحة على نطاق واسع.

مدقق مؤهل : شخص طبيعي أو كيان اعتباري يستوفي المتطلبات الواردة في القسم 8.2.

قيمة عشوائية : قيمة تُحددها هيئة التصديق للمتقدم بالطلب ويجب أن تتضمن ما لا يقل عن 112 بت من الإنتروبيا.

اسم نطاق مسجل : اسم نطاق جرى تسجيله لدى جهة تسجيل نطاقات الإنترنت .

هيئة التسجيل : كيان اعتباري مسؤول عن تحديد هوية والتحقق من المشتركين في الشهادات ولا تُعد هيئة تصديق ولذلك فهي لا تُصدر الشهادات ولا توقّعها. قد تُساعد هيئة التسجيل في عملية تقديم طلبات الشهادات أو طلبات الإلغاء أو كليهما. عند استخدام"RA" كصفة تصف دوراً أو وظيفة لا يُشير ذلك بالضرورة إلى جهة مستقلة بل يمكن أن تكون جزءاً من هيئة التصديق نفسها.

مصدر بيانات موثوق : وثيقة تعريف أو مصدر بيانات يُستخدم للتحقق من معلومات هوية الموضوع ويُعترف به بشكل عام بين المؤسسات التجارية والحكومات كمصدر موثوق. ويكون قد أُنشئ من قبل طرف ثالث لغرض غير متعلق بالحصول على شهادة من قبل المتقدم بالطلب.

طريقة اتصال موثوقة: وسيلة اتصال مثل عنوان بريد أو شركة توصيل أو رقم هاتف أو بريد إلكتروني حقق منها باستخدام مصدر يختلف عن ممثل المتقدم بالطلب.

الطرف المعتمد: أي شخص طبيعي أو كيان اعتباري يعتمد على شهادة صالحة. ولا يُعد مورد برامج التطبيقات طرفاً معتمداً عندما تقتصر برامجه على عرض معلومات تتعلق بالشهادة دون الاعتماد عليها فعلياً.

المستودع: قاعدة بيانات إلكترونية تتضمن وثائق ال الخاصة بالبنية التحتية للمفتاح العام المنشورة للعامة مثل سياسات الشهادات وبيانات ممارسات الشهادات ومعلومات حالة الشهادات سواء على شكل قائمة إلغاء (CRL) أو ردOCSP .

رمز الطلب: قيمة يتم توليدها باستخدام طريقة تحددها هيئة التصديق وترتبط بعملية إثبات السيطرة ضمن طلب الشهادة. تشمل الأمثلة على رموز الطلب: تجزئة المفتاح العام أو تجزئة معلومات المفتاح العام للموضوع[X.509] أو تجزئة ملف طلب شهادةPKCS#10 .

هيئة التصديق الجذرية: هيئة التصديق العليا التي يتم توزيع شهادتها الجذرية من قبل موردي برمجيات التطبيقات وهي الجهة التي تصدر شهادات هيئات التصديق التابعة.

الشهادة الجذرية: شهادة موقعة ذاتياً تصدرها هيئة التصديق الجذرية لتعريف نفسها وتُستخدم لتسهيل التحقق من الشهادات الصادرة لهيئات التصديق التابعة التابعة لها.

الموضوع: خدمة ختم الوقت التي تُشغّلها وتديرها شركة مصدر التكنولوجيا أي المشترك.

معلومات هوية الموضوع: المعلومات التي تُحدد هوية الموضوع في الشهادة. لا تشمل معلومات هوية الموضوع أسماء النطاقات المدرجة ضمن امتداد جميع الاسماء أو في حقل الاسم الاعتيادي.

هيئة التصديق التابعة: هيئة تصديق تُوقّع شهادتها من قبل هيئة التصديق الجذرية أو من قبل هيئة تصديق فرعية أخرى.

المشترك: كيان اعتباري تُصدر له شهادة ويرتبط قانونياً باتفاقية مشترك أو بشروط الاستخدام.

شروط وأحكام استخدام المشترك: اتفاق يُبرم بين هيئة التصديق والمتقدم بالطلب أو المشترك ويُحدد الحقوق والمسؤوليات الخاصة بكل طرف.

شهادة هيئة تصديق فرعية مقيّدة تقنياً: شهادة تُصدر لهيئة تصديق فرعية ويتم فيها استخدام إعدادات موسعة لاستخدام المفتاح وقيود اسمية لتقييد النطاق الذي يُسمح للهيئة الفرعية ضمنه بإصدار شهادات للمشتركين أو هيئات تصديق فرعية إضافية.

شروط الاستخدام: أحكام تتعلق بحفظ الشهادة واستخداماتها المسموح بها تُطبق عندما يكون المتقدم بالطلب أو المشترك جهة تابعة لهيئة التصديق أو الهيئة نفسها وذلك وفقاً للمتطلبات الأساسية.

وحدة ختم الوقت :(TSU) مجموعة من الأجهزة والبرمجيات تُدار كوحدة واحدة وتحتوي على مفتاح توقيع زمني واحد نشط في كل مرة. في سياق هذا البيان تُشغّل شركة مصدر التكنولوجيا وحدتين (02) لختم الوقت: واحدة لتوقيع المستندات وأخرى لتوقيع البرمجيات.

الشهادة الصالحة: شهادة تجتاز إجراءات التحقق المنصوص عليها في المعيارRFC 5280 .

أخصائي التحقق: الشخص الذي يؤدي مهام التحقق من المعلومات كما هو موضح في هذه المتطلبات.

فترة الصلاحية: الفترة الزمنية الممتدة من تاريخ إصدار الشهادة وحتى تاريخ انتهائها.

.

1.6.2 الاختصارات

AICPA	المعهد الأمريكي للمحاسبين القانونيين المعتمدين.
CA	هيئة التصديق.
CCTV	كاميرات المراقبة.
CICA	المعهد الكندي للمحاسبين القانونيين المعتمدين.
CP	سياسة الشهادات.
CPS	بيان ممارسة الشهادات.
CRL	قائمة إلغاء الشهادات.
CSR	طلب توقيع الشهادة.
CV	السيرة الذاتية.
DBA	الاسم التجاري.
DN	الاسم المميز.
DNS	نظام أسماء النطاقات.
FIPS	معايير المعالجة الفيدرالية للمعلومات.
EID	بطاقة الهوية الإلكترونية.
EIDAS	خدمات التعريف والمصادقة والثقة الإلكترونية.
ETSI	المعهد الأوروبي لمعايير الاتصالات.
HSM	جهاز توليد المفاتيح الشفرية.
HTTP	بروتوكول نقل النص التشعبي.
IANA	هيئة تخصيص أرقام الإنترنت.
ICANN	المؤسسة الدولية للأسماء والأرقام المخصصة.
IETF	فرقة عمل هندسة الإنترنت.
IPSEC	أمن بروتوكول الإنترنت.

ISO	المنظمة الدولية للمعايير.
ITPC	الشركة العامة للاتصالات والمعلوماتية.
IT	تكنولوجيا المعلومات.
OCSP	بروتوكول حالة الشهادة عبر الإنترنت.
OID	معرف الكائن.
PIN	الرقم السري.
PKCS#1	معايير التشفير بالمفتاح العام – الإصدار 1.
PKCS#7	صيغة رسائل التشفير.
PKCS#10	صيغة طلب الشهادة.
PKI	البنية التحتية للمفتاح العام.
PMA	اللجنة العليا لإدارة التوقيع الإلكتروني.
RA	هيئة التسجيل.
RSA	ريفست-شامير-أدلمان.
RTO	هدف زمن الاستعادة.
SSL	الاتصال الامن.
TLD	نطاق المستوى الأعلى.
TS	شركة مصدر التكنولوجيا.
TSA	هيئة ختم الوقت.
TLS	الاتصال الامن.
TSP	مقدم خدمات الثقة.
UPS	مزود الطاقة غير المنقطعة.
URI	معرف المورد العالمي.
URL	موقع المورد العالمي.

1.6.3 المراجع

تستند هذه الوثيقة إلى المعايير واللوائح الفنية الدولية المدرجة أدناه:

1. **المعيار الدولي :(X.509)** المعيار الصادر عن قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات والمختص بهيكلية الشهادات الرقمية.
2. **وثيقة المعايير :(RFC3647)** الإطار العام لسياسات شهادات البنية التحتية للمفاتيح العامة وبيان ممارسات التصديق.
3. **وثيقة المعايير :(RFC5280)** المواصفات الفنية لشهادات البنية التحتية للمفاتيح العامة وقوائم الشهادات الملغاة.
4. **وثيقة المعايير :(RFC3161)** البروتوكول الخاص بخدمات الختم الزمني ضمن البنية التحتية للمفاتيح العامة.
5. **معايير (ويب-ترست) لتوقيع الشفرات البرمجية :**المبادئ الصادرة عن المعاهد المهنية للمحاسبين في أمريكا وكندا والمتعلقة بالمتطلبات الأساسية لسلطات التصديق.
6. **معايير (ويب-ترست) العامة :**المبادئ والمعايير الخاصة بضوابط عمل سلطات التصديق الرقمي.
7. **معايير (ويب-ترست) لأمن الشبكات :**المتطلبات الفنية لتأمين شبكات سلطات التصديق.
8. **متطلبات أمن أنظمة الشهادات والشبكات :**المعايير الأمنية الصادرة عن منتدى سلطات التصديق ومتصفحات الشبكة العالمية.
9. **المتطلبات الأساسية لشهادات توقيع الشفرات الموثوقة :**الضوابط الصادرة عن منتدى سلطات التصديق والمتصفحات بخصوص إصدار وإدارة الشهادات.
10. **معيار المعهد الأوروبي لمعايير الاتصالات :(319421)** المتطلبات السيادية والأمنية لمزودي خدمات الثقة عند إصدار الأختام الزمنية.
11. **معيار المعهد الأوروبي لمعايير الاتصالات :(319422)** المواصفات الفنية لبروتوكولات الختم الزمني ورموز التوثيق الزمني.

2 المسؤوليات المتعلقة بالنشر والمستودعات

2.1 المستودعات

تُدير شركة مصدر التكنولوجيا مستودعاً إلكترونياً متاحاً على مدار الساعة وطيلة أيام الأسبوع ويمكن الوصول إليه عبر الرابط التالي:
https://pki.techsource.iq.

تتحمل شركة مصدر التكنولوجيا مسؤولية إتاحة المعلومات التالية للنشر في مستودعها:

- النسخ الحالية والسابقة من بيانات ممارسة الشهادات (CPS) الخاصة بشركة مصدر التكنولوجيا.
- النسخة الحالية من سياسة الشهادات وبيان ممارسة الشهادات لهيئة التصديق الجذرية التابعة للشركة العامة للاتصالات والمعلوماتية بالإضافة إلى سياسة الشهادات الخاصة بمزود خدمات الثقة.
- اتفاقيات المشترك وهيئة التسجيل المحلية والطرف المعتمد وبيان إفصاح البنية التحتية للمفتاح العامة وبيان ممارسة هيئة ختم الوقت وبيان إفصاح هيئة ختم الوقت.
- شهادات الهيئة الجذرية الذاتية التوقيع الصالحة بالإضافة إلى شهادات هيئات التصديق التابعة لشركة مصدر التكنولوجيا وشهاداتOCSP وقوائم إلغاء الشهادات (CRLs) الصادرة عن الهيئات الفرعية.
- شهادات وحدات ختم الوقت (TSU).
- تقارير التدقيق.

2.2 نشر معلومات الشهادات

تعد شركة مصدر التكنولوجيا الكيان المسؤول عن توفير المعلومات الخاصة بالنشر كما ورد في القسم 2.1 من هذا المستند.

تنشر شركة مصدر التكنولوجيا معلومات حالة صلاحية الشهادات على فترات متكررة كما هو موضح في بيان ممارسة الشهادات(CPS) .

تُقدَّم خدمة معلومات حالة صلاحية الشهادات على مدار الساعة وطيلة أيام الأسبوع على النحو التالي:

- نشر قوائم إلغاء الشهادات (CRLs) التي تتضمن أي تغييرات منذ نشر قائمة CRL السابقة وذلك على فترات منتظمة. وتُضيف هيئة تصديق ختم الوقت الخاصة بشركة مصدر التكنولوجيا رابطاً (URL) إلى قائمة CRL ذات الصلة في شهادات المشتركين كجزء من امتداد نقطة توزيع الشهادة (CDP) متى ما توفر هذا الامتداد .
- موفر خدمة OCSP متوافق مع المواصفة .RFC 6960 يُشار إلى رابط خدمة OCSP ضمن امتداد معلومات الوصول إلى الهيئة (AIA) في شهادات المشتركين الصادرة عن هيئة تصديق ختم الوقت الخاصة بشركة مصدر التكنولوجيا.

2.3 توقيت أو تكرار النشر

تُراجع لجنة البنية التحتية للمفتاح العام لشركة مصدر التكنولوجيا (TS PKI GB) بيان ممارسة الشهادات (CPS) هذا مرة واحدة على الأقل سنوياً وتجري التعديلات المناسبة لضمان استمرار توافق عمليات هيئات التصديق المُصدرة مع المتطلبات المحددة في القسم 1 من هذا البيان. في الحالات التي لا تتطلب إجراء أي تعديلات، يتم تحديث رقم إصدار بيان ممارسة الشهادات، مع إدراج قيد في سجل التغييرات مؤرخاً لتوثيق عملية المراجعة.

تُنشر النسخ المعدلة من بيان ممارسة الشهادات (CPS) والاتفاقيات (شروط وأحكام استخدام المشترك والطرف المعتمد) خلال مدة لا تتجاوز خمسة (5) أيام من تاريخ موافقة لجنةTS PKI GB.

2.3.1 شهادة هيئة التصديق

تُنشر شهادات هيئات التصديق التابعة وشهادات OCSP في المستودع العام فور إصدارها وتبقى متاحة إلى حين انتهاء صلاحيتها أو إعادة إصدارها بمفاتيح جديدة.

2.3.2 قوائم إلغاء الشهادات (CRLs)

تقوم هيئة التصديق بالحفاظ على قوائم إلغاء الشهادات ونشرها وفقاً لما يلي:

- تُنشأ قائمة CRL جديدة كل 24 ساعة حتى في حال عدم حدوث أي تغييرات منذ إصدار قائمة CRL السابقة.
- مدة صلاحية قائمة CRL تُحدد بـ 26 ساعة.

2.4 ضوابط الوصول إلى المستودعات

تكون المعلومات المنشورة في المستودع العام الخاص بشركة مصدر التكنولوجيا متاحة للجمهور مع ضمان الوصول غير المقيد للقراءة.

تُنفذ شركة مصدر التكنولوجيا تدابير أمنية منطقية ومادية لمنع الأشخاص غير المصرح لهم من إضافة أو حذف أو تعديل أي مدخلات ضمن المستودع.

3 التعريف والمصادقة

3.1 التسمية

3.1.1 أنواع الأسماء

تتبع هيئة التصديق هذه (CA) معيار الأسماء المميزةX.500 والتي يجب أن تكون فريدة وذات معنى.
تتوافق أسماء الموضوع في شهادة هيئة التصديق مع معايير الأسماء المميزة .X.500 يتم التحقق من اسم الموضوع المستخدم واعتماده من خلال وظيفة هيئة التسجيل (RA) التابعة للجنة إدارة السياسات(PMA) ويجب أن يكون ذا دلالة ولا يجوز إعادة تخصيصه لأي جهة أخرى.

تُعرَّف هيئة التصديق هذه في حقل اسم المُصدِر في شهادات المشتركين على النحو التالي:

CN الاسم العام	TS TSA CA G1
O المنظمة	مصدر التكنلوجيا
C الدولة	العراق(IQ)

تتضمّن الشهادات الصادرة عن هيئة التصديق هذه (CA) أسماء مميزة وفق معيار (DN) X.500 على النحو الآتي:

شهادة خدمة هيئة ختم الوقت لتوقيع المستندات:

السمة	القيمة
CN الاسم العام	توقيع ختم الوقت للوثائق
الرقم التعريفي للمنظمة	تعريف للمنظمة يختلف عن اسم المنظمة
O المنظمة	مصدر التكنولوجيا
C الدولة	العراق(IQ)

شهادة خدمة هيئة ختم الوقت لتوقيع الخوارزميات:

السمة	القيمة
CN الاسم العام	توقيع ختم الوقت للخوارزميات
الرقم التعريفي للمنظمة	تعريف للمنظمة يختلف عن اسم المنظمة
O المنظمة	مصدر التكنولوجيا
C الدولة	العراق(IQ)

شهادة استجابة OCSP لهيئة ختم الوقت:

السمة	القيمة
CN الاسم العام	TS TSA CA G1 OCSP
Oالمنظمة	مصدر التكنولوجيا
Cالدولة	العراق(IQ)

3.1.2 الحاجة إلى أن تكون الأسماء ذات دلالة

تفرض هيئة التصديق الخاصة بختم الوقت (TSA CA) استخدام أسماء ذات دلالة على النحو الآتي:

- بالنسبة للشهادات الصادرة لخدمات هيئة ختم الوقت (TSA) تُستخدم الأسماء المميزة (DN) لتعريف الخدمة بطريقة ذات معنى.
- بالنسبة لشهادة مستجيب :OCSP يكون الاسم ذا دلالة لأنه يوضح اسم شهادة مستجيب OCSP الخاص بهيئة التصديق التابعة.

3.1.3 عدم السماح باستخدام الأسماء المجهولة أو المستعارة للمشتركين

لا يُسمح بوجود مشتركين مجهولي الهوية أو يستخدمون أسماء مستعارة.

3.1.4 قواعد تفسير صيغ الأسماء المختلفة

يعتمد نظام التسمية المستخدم من قبل هيئة التصديق هذه على معيار ISO/IEC 9595 (X.500) للأسماء المميزة(DN) .

3.1.5 فرادة الأسماء

وفقاً للقسم 3.1.1 من بيان ممارسات الشهادات(CPS) تفرض هيئة التصديق هذه فرادة الأسماء من خلال أسماء عامة فريدة على مستوى النظام بما يضمن فرادة الأسماء المميزة(DN) .

ولا يُعد إصدار عدة شهادات لنفس الكيان انتهاكاً لمبدأ فرادة الأسماء.

3.1.6 التعرف على العلامات التجارية والمصادقة عليها ودورها

من خلال تقديم طلب شهادة إلى هيئة التصديق هذه يوافق المتقدم على أن طلبه لا يحتوي على بيانات تنتهك بأي شكل من الأشكال حقوق أي طرف ثالث ضمن أي ولاية قضائية فيما يتعلق بالعلامات التجارية أو علامات الخدمة أو الأسماء التجارية أو أسماء الشركات أو أسماء "العمل تحت اسم(DBA) " أو أي حقوق ملكية فكرية أخرى وأنه لا يقدّم تلك البيانات لأي غرض غير قانوني.
وتحتفظ هيئة التصديق هذه بالحق في إلغاء الشهادة عند تلقي أمر موثَّق رسمياً من مجلس البنية التحتية للمفاتيح العامة لمصدر التكنولوجيا (TS PKI GB) أو من محكمة ذات اختصاص تطلب إلغاء شهادة أو شهادات تحتوي على اسم موضوع محل نزاع.

3.2 التحقق الأولي من الهوية

لا تصدر هيئة التصديق لختم الوقت شهادات لأي شخص اعتباري سوى شركة مصدر التكنولوجيا.
يشرف كلٌّ من هيئة التسجيل التابعة لشركة مصدر التكنولوجيا (TS RA) ومسؤول إدارة البنية التحتية للمفاتيح العامة (TS PKI Administrator)على عملية إصدار شهادات هيئة ختم الوقت(TS TSA) .

تُصدِر هيئة التصديق لختم الوقت شهادات الخدمة وكذلك شهادة مستجيب OCSP كجزء من الطقوس التشغيلية الداخلية المعتمدة وتحت إشراف مجلس البنية التحتية للمفاتيح العامة لمصدر التكنولوجيا(TS PKI GB) .

3.2.1 طريقة إثبات حيازة المفتاح الخاص

غير قابل للتطبيق.

3.2.2 التحقق من هوية المنظمة

غير قابل للتطبيق.

3.2.2.1 التحقق من الدولة

غير قابل للتطبيق.

3.2.3 التحقق من هوية الفرد

غير قابل للتطبيق.

3.2.4 معلومات المشترك غير المُتحقَّق منها

غير قابل للتطبيق.

3.2.5 التحقق من الصلاحية

غير قابل للتطبيق.

3.2.6 معايير التشغيل البيني

لا يوجد نص محدد.

3.3 التعريف والمصادقة لطلبات إعادة إصدار المفتاح

3.3.1 التعريف والمصادقة لإعادة إصدار المفتاح بشكل روتيني

يُجرى التعريف والمصادقة لإعادة إصدار المفتاح بنفس طريقة التسجيل الأولي (انظر القسم 3.2).

3.3.2 التعريف والمصادقة لإعادة إصدار المفتاح بعد الإلغاء

يُجرى التعريف والمصادقة لإعادة إصدار المفتاح بعد الإلغاء بنفس طريقة التسجيل الأولي (انظر القسم 3.2).

3.4 التعريف والمصادقة لطلبات الإلغاء

يُجرى التعريف والمصادقة لطلب الإلغاء بنفس طريقة التسجيل الأولي (انظر القسم 3.2).

4 متطلبات تشغيل دورة حياة الشهادة

4.1 طلب الشهادة

لا تصدر هيئة التصديق لختم الوقت شهادات لأي شخص اعتباري سوى شركة مصدر التكنولوجيا.
يشرف كلٌّ من هيئة التسجيل (TS RA) ومسؤول إدارة البنية التحتية للمفاتيح العامة (TS PKI Administrator) على إصدار شهادات خدمة هيئة ختم الوقت (TS TSA) وكذلك شهادة مستجيبOCSP وذلك ضمن الطقوس التشغيلية الداخلية المعتمدة وتحت إشراف مجلس البنية التحتية للمفاتيح العامة(TS PKI GB) .

4.1.1 من يمكنه تقديم طلب شهادة

غير قابل للتطبيق.

4.1.2 عملية التسجيل والمسؤوليات

غير قابل للتطبيق.

4.2 معالجة طلب الشهادة

لا تصدر هيئة التصديق لختم الوقت شهادات لأي شخص اعتباري سوى شركة مصدر التكنولوجيا .يشرف كلٌّ من هيئة التسجيل (TS RA)ومسؤول إدارة البنية التحتية للمفاتيح العامة على إصدار شهادات خدمة هيئة ختم الوقت (TS TSA) وكذلك شهادة مستجيبOCSP وذلك ضمن الطقوس التشغيلية الداخلية المعتمدة وتحت إشراف مجلس البنية التحتية للمفاتيح العامة(TS PKI GB) .

4.2.1 تنفيذ وظائف التعريف والمصادقة

غير قابل للتطبيق.

4.2.2 الموافقة أو رفض طلبات الشهادات

غير قابل للتطبيق.

4.2.3 المدة الزمنية لمعالجة طلبات الشهادات

لا يوجد نص محدد.

4.3 إصدار الشهادة

لا تصدر هيئة التصديق لختم الوقت شهادات لأي شخص اعتباري سوى شركة مصدر التكنولوجيا .يشرف كلٌّ من هيئة التسجيل (TS RA) ومسؤول إدارة البنية التحتية للمفاتيح العامة على إصدار شهادات خدمة هيئة ختم الوقت (TS TSA) وكذلك شهادة مستجيبOCSP وذلك ضمن الطقوس التشغيلية الداخلية المعتمدة وتحت إشراف مجلس البنية التحتية للمفاتيح العامة(TS PKI GB) .

4.3.1 إجراءات هيئة التصديق أثناء إصدار الشهادة

غير قابل للتطبيق.

4.3.2 إشعار المشترك بإصدار الشهادة من قبل هيئة التصديق

غير قابل للتطبيق.

4.4 قبول الشهادة

لا تصدر هيئة التصديق لختم الوقت شهادات لأي شخص اعتباري سوى شركة مصدر التكنولوجيا.
يشرف كلٌّ من هيئة التسجيل (TS RA) ومسؤول إدارة البنية التحتية للمفاتيح العامة على إصدار شهادات خدمة هيئة ختم الوقت (TS TSA) وكذلك شهادة مستجيبOCSP وذلك ضمن الطقوس التشغيلية الداخلية المعتمدة وتحت إشراف مجلس البنية التحتية للمفاتيح العامة(TS PKI GB) .

4.4.1 التصرفات التي تُعد قبولاً للشهادة

غير قابل للتطبيق.

4.4.2 نشر الشهادة من قبل هيئة التصديق

تُنشَر كل من شهادات وحدة ختم الوقت (TSU) وشهادة مستجيب OCSP على المستودع العام لمصدر التكنولوجيا.

4.4.3 إشعار الكيانات الأخرى بإصدار الشهادة من قبل هيئة التصديق

غير قابل للتطبيق.

4.5 استخدام زوج المفاتيح والشهادة

4.5.1 استخدام المفتاح الخاص وشهادة خدمة هيئة ختم الوقت

تتعهد خدمة هيئة ختم الوقت (TS TSA) باستخدام الشهادة وفقاً لما يلي:

- استخدام الشهادات فقط لأغراض قانونية ومصرح بها وفقاً للمتطلبات العامة المشتركة المنطبقة على سياسة الشهادات (TSP CP) وبيان ممارسات الشهادات (CPS) هذا .
- حماية المفتاح الخاص (وجميع الأسرار المرتبطة به) من الاختراق أو الفقدان أو الكشف أو أي استخدام غير مصرح به .
- عدم استخدام الشهادة خارج فترة صلاحيتها أو بعد إلغائها .
- تجنب استخدام المفتاح الخاص قبل إصدار الشهادة من قبل هيئة التصديق .
- التوقف عن استخدام المفتاح الخاص بعد انتهاء فترة صلاحية الشهادة أو عند إلغائها.

4.5.2 استخدام المفتاح العام والشهادة من قبل الطرف المعتمد

يتعيّن على أي طرف يعتمد على شهادة صادرة عن هيئة التصديق لختم الوقت أن:

- يستخدم برنامجاً متوافقاً مع معيار X.509 ومعايير IETF PKIX المعمول بها للتحقق من صحة توقيع الشهادة وفترة صلاحيتها .
- يتحقق من صلاحية الشهادة باستخدام لائحة إلغاء الشهادات (CRL) أو خدمة حالة الصلاحية عبر بروتوكول OCSP وفقاً لإجراءات التحقق من مسار الشهادة.
- الثقة بالشهادة فقط إذا لم تُلغَ وكانت ضمن فترة صلاحيتها.
- الثقة بالشهادة فقط لتوقيع رموز ختم الوقت المتوافقة مع المواصفة3161 RFC .

4.6 تجديد الشهادة

غير قابل للتطبيق.

4.6.1 الظروف التي تستدعي تجديد الشهادة

غير قابل للتطبيق.

4.6.2 من يمكنه طلب التجديد

غير قابل للتطبيق.

4.6.3 معالجة طلبات تجديد الشهادة

غير قابل للتطبيق.

4.6.4 إشعار المشترك بإصدار شهادة جديدة

غير قابل للتطبيق.

4.6.5 التصرفات التي تُعد قبولاً لشهادة مجدَّدة

غير قابل للتطبيق.

4.6.6 نشر الشهادة المجددة من قبل هيئة التصديق

غير قابل للتطبيق.

4.6.7 إشعار الكيانات الأخرى بإصدار الشهادة من قبل هيئة التصديق

غير قابل للتطبيق.

4.7 إعادة إصدار الشهادة (Re-Key)

تُعد عملية إعادة إصدار الشهادة (Re-Key) عملية إصدار شهادة جديدة للمشترك باستخدام مفتاح عام جديد وفترة صلاحية جديدة بينما قد تبقى بقية المعلومات في الشهادة دون تغيير .تدعم هيئة التصديق لختم الوقت إعادة إصدار شهادات خدمة ختم الوقت .(TS TSA) وتتشابه عملية إعادة الإصدار مع عملية طلب الشهادة الأولية.

4.7.1 الظروف التي تستدعي إعادة إصدار الشهادة

قد تحدث إعادة إصدار الشهادة بينما تكون الشهادة لا تزال فعالة أو بعد انتهاء صلاحيتها أو بعد إلغائها .وقد تؤدي عملية إعادة الإصدار إلى إبطال أي شهادات TS TSA نشطة حالياً.

4.7.2 من يمكنه طلب اعتماد مفتاح عام جديد

وفقاً لإجراءات إصدار الشهادة الأولية.

4.7.3 معالجة طلبات إعادة إصدار الشهادة

وفقاً لإجراءات إصدار الشهادة الأولية.

4.7.4 إشعار المشترك بإصدار شهادة جديدة
وفقاً لإجراءات إصدار الشهادة الأولية.

4.7.5 التصرفات التي تُعد قبولاً لشهادة معاد إصدارها
وفقاً لإجراءات إصدار الشهادة الأولية.

4.7.6 نشر الشهادة المعاد إصدارها من قبل هيئة التصديق
وفقاً لإجراءات إصدار الشهادة الأولية.

4.7.7 إشعار الكيانات الأخرى بإصدار الشهادة من قبل هيئة التصديق
وفقاً لإجراءات إصدار الشهادة الأولية.

4.8 تعديل الشهادة

4.8.1 الظروف التي تستدعي تعديل الشهادة
غير قابل للتطبيق.

4.8.2 من يمكنه طلب تعديل الشهادة
غير قابل للتطبيق.

4.8.3 معالجة طلبات تعديل الشهادة
غير قابل للتطبيق.

4.8.4 إشعار المشترك بإصدار شهادة جديدة
غير قابل للتطبيق.

4.8.5 التصرفات التي تُعد قبولاً لشهادة معدّلة
غير قابل للتطبيق.

4.8.6 نشر الشهادة المعدّلة من قبل هيئة التصديق
غير قابل للتطبيق.

4.8.7 إشعار الكيانات الأخرى بإصدار الشهادة من قبل هيئة التصديق
غير قابل للتطبيق.

4.9 إلغاء وتعليق الشهادة

لا تسمح هيئة التصديق لختم الوقت بتعليق الشهادة. ويسمح فقط بإلغاء الشهادة بشكل دائم.

لا تصدر هيئة التصديق لختم الوقت شهادات لأي شخص اعتباري سوى شركة مصدر التكنولوجيا .وقد يؤدي اختراق المفتاح الخاص المرتبط بشهادات TS TSA أو شهادة مستجيبOCSP أو الاشتباه في اختراقه إلى تفعيل إجراء الإلغاء ويُعد ذلك بمثابة كارثة وتُعالَج وفقاً لخطة استمرارية الأعمال والتعافي من الكوارث الخاصة بشركة مصدر التكنولوجيا.

4.9.1 الظروف التي تستدعي الإلغاء

4.9.1.1 الظروف المتعلقة بإلغاء شهادات المشتركين

غير قابل للتطبيق.

4.9.1.2 الظروف المتعلقة بإلغاء شهادات هيئة التصديق التابعة

تُلغى شهادة هيئة التصديق لختم الوقت خلال سبعة (7) أيام في حال تحقق أحد أو أكثر من الحالات التالية:

1. تقديم طلب الإلغاء كتابياً .
2. قامت شركة مصدر التكنولوجيا بإخطار هيئة التصديق المُصدِرة (أي الهيئة الجذرية) بأن طلب الشهادة الأصلي لم يكن مفوضاً ولم تُمنَح صلاحية بأثر رجعي .
3. حصلت شركة مصدر التكنولوجيا على دليل يُثبت أن المفتاح الخاص المقابل للمفتاح العام في الشهادة قد تم اختراقه أو أنه لم يعد يفي بمتطلبات البندين 6.1.5 و6.1.6 .
4. حصلت هيئة التصديق المُصدِرة (الهيئة الجذرية) على دليل يُثبت إساءة استخدام شهادة هيئة التصديق لختم الوقت .
5. علمت الهيئة الجذرية بأن الشهادة لم تُصدر وفقاً لهذا المستند أو أن هيئة التصديق لختم الوقت لم تلتزم به .
6. قررت الهيئة الجذرية أن أي من المعلومات الواردة في شهادة هيئة التصديق لختم الوقت غير دقيقة أو مضللة .
7. توقفت هيئة التصديق لختم الوقت عن العمل لأي سبب ولم ترتب بدائل لتوفير خدمات دعم الإلغاء للشهادة .
8. انتهى حق هيئة التصديق لختم الوقت في إصدار الشهادات وفقاً لهذه المتطلبات أو الغيت أو إنهاؤه ما لم تكن الهيئة الجذرية قد رتبت لاستمرار إدارة مستودعCRL/OCSP .
9. طُلب الإلغاء بموجب سياسة الشهادات أو بيان ممارسة الشهادات الخاصة بالهيئة الجذرية.

4.9.2 من يمكنه طلب الإلغاء

غير قابل للتطبيق.

4.9.3 إجراءات طلب الإلغاء

غير قابل للتطبيق.

4.9.4 فترة السماح لتقديم طلب الإلغاء

غير قابل للتطبيق.

4.9.5 المدة الزمنية التي يجب على هيئة التصديق خلالها معالجة طلب الإلغاء

غير قابل للتطبيق.

4.9.6 متطلبات التحقق من الإلغاء للطرف المعتمد

يقع على عاتق الأطراف المعتمدة وحدها تنفيذ التحقق من حالة الإلغاء لجميع الشهادات ضمن سلسلة الثقة قبل اتخاذ قرار بالاعتماد على المعلومات الواردة في الشهادة .توفر هيئة التصديق لختم الوقت حالة الإلغاء عبر آليات مضمّنة داخل شهادات خدمة ختم الوقت(TS TSA) أي عبر لائحة الإلغاء (CRL) وخدمة حالة الشهادة عبر بروتوكولOCSP .

4.9.7 تكرارية إصدار لائحة الإلغاء (CRL) إن وُجد

يُجرى إصدار قوائم الإلغاء وفقاً لما ورد في القسم 2.3 من بيان ممارسة الشهادات (CPS) هذا.

4.9.8 الحد الأقصى للتأخير في إصدار لائحة الإلغاء) (CRL) إن وُجد

تصدر هيئة التصديق لختم الوقت قوائم الإلغاء بشكل فوري وفقاً لتكرار الإصدار المحدد في القسم 4.9.7 من بيان ممارسة الشهادات.

4.9.9 توفر التحقق من الإلغاء/الحالة عبر الإنترنت

توفّر هيئة التصديق لختم الوقت خدمة مستجيب OCSP متوافقة مع المواصفة.RFC 6960
يُتيَح المستجيب المعلومات فوراً لتطبيقات الأطراف المعتمدة بناءً على إجراءات هيئة التصديق بشأن الشهادات الصادرة.
تتضمن شهادة OCSP امتداداً من النوع id-pkix-ocsp-nocheck وامتداد ocspSigning EKUوفقاً لـRFC 6960 .

ويتم الإشارة إلى عنوان URL الخاص بخدمة OCSP في الشهادات الصادرة عن هيئة التصديق لختم الوقت.

4.9.10 متطلبات التحقق من الإلغاء عبر الإنترنت

يدعم مستجيب OCSP طريقتي HTTP GET وHTTP POST.

بالنسبة لحالة شهادات المشتركين:

- تتمتع استجابات OCSP بفترة صلاحية لا تقل عن ثماني ساعات .
- ولا تتجاوز فترة الصلاحية عشر أيام.

عندما تقل صلاحية ردود OCSP عن ست عشرة ساعة تقوم هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا بتحديث المعلومات المقدمة عبر بروتوكول حالة الشهادة عبر الإنترنت (OCSP) قبل مرور نصف مدة الصلاحية وقبل وقت .

.عندما تكون صلاحية ردود OCSP تساوي أو تتجاوز ست عشرة ساعة تقوم هيئة ختم الوقت بتحديث المعلومات المقدمة عبر بروتوكول حالة الشهادة عبر الإنترنت (OCSP) قبل ما لا يقل عن ثماني ساعات من وقت ولا يتجاوز ذلك أربعة أيام من وقت .

عندما يتلقى مستجيب OCSP طلباً للتحقق من حالة رقم تسلسلي لشهادة غير مستخدمة (أي غير مُصدرة من قبل هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا) يرد مستجيب OCSP بحالة "مُلغاة" كما هو معرّف في المواصفة RFC 6960القسم 4.4.8 تعريف الإلغاء الموسّع.

تراقب هيئة ختم الوقت مستجيب OCSP لرصد الطلبات التي تتعلق بأرقام تسلسلية غير مستخدمة كجزء من إجراءات المراقبة الأمنية وتؤدي أي حالة من هذا النوع إلى فتح تحقيق إضافي من قبل الفرق المختصة ضمن فريق عمليات شركة مصدر التكنولوجيا.

4.9.11 أشكال أخرى لإعلانات الإلغاء المتاحة

تعتمد هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا فقط على بروتوكول OCSP وقوائم الإلغاء (CRL) كطرق لنشر معلومات إلغاء الشهادات.

4.9.12 متطلبات خاصة تتعلق باختراق المفتاح

إذا اكتشفت شركة مصدر التكنولوجيا أو كان لديها سبب للاعتقاد بحدوث اختراق لمفاتيحها الخاصة سواء لمفاتيح هيئة ختم الوقت أو شهادات TSA أو شهادة مستجيبOCSP فإنها تعلن فوراً عن حالة كارثية وتفعّل خطة استمرارية الأعمال الخاصة بها. كما تقوم:

- تحديد نطاق الشهادات التي يتوجب إلغاؤها .
- إلغاء الشهادات المتأثرة خلال 24 ساعة ونشر قوائم الإلغاء (CRL) على الإنترنت خلال 30 دقيقة من إنشائها.
- بذل جهد معقول لإخطار الجهات الحكومية والمشتركين والأطراف المعتمدة المحتملة بوقوع اختراق للمفتاح.
- إنشاء زوج مفاتيح جديد لهيئة التصديق وفقاً للسياسات والإجراءات التشغيلية المعتمدة لدى شركة مصدر التكنولوجيا.

4.9.13 الظروف المؤدية إلى التعليق

غير قابل للتطبيق.

4.9.14 الجهة التي يمكنها طلب التعليق

غير قابل للتطبيق.

4.9.15 إجراءات طلب التعليق

غير قابل للتطبيق.

4.9.16 حدود فترة التعليق

غير قابل للتطبيق.

4.10 خدمات حالة الشهادة

يُرجى الرجوع إلى القسم 4.9.6 من بيان ممارسة الشهادات هذا (CPS) بالإضافة إلى ذلك تم اتخاذ الأحكام التالية:

4.10.1 الخصائص التشغيلية

تنشر هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا قوائم الإلغاء (CRLs) في المستودع العام المتاح للأطراف المعتمدة.

يوفر مستجيب OCSP التابع لهيئة ختم الوقت واجهة HTTP تكون متاحة أيضاً للأطراف المعتمدة.

لا تُزال قيود الإلغاء من قوائم الإلغاء (CRL) أو من ردود OCSP بعد تاريخ انتهاء صلاحية الشهادات المُلغاة. تتضمن قائمة الإلغاء الامتداد وفقاً لتعريف المواصفة / ISO / IEC 9594-8 التوصية ITU-T X.509 .

4.10.2 توفر الخدمة

يكون المستودع العام الذي تُنشر فيه معلومات الشهادات وقوائم الإلغاء متاحاً على مدار 24 ساعة يومياً وسبعة أيام في الأسبوع مع ضمان توفر الخدمة بنسبة لا تقل عن 99.6% خلال فترة سنة واحدة.

تشغّل هيئة ختم الوقت TSA وتُحافظ على قدرات قوائم الإلغاء (CRL) ومستجيب OCSP باستخدام موارد كافية لضمان وقت استجابة لا يتجاوز عشر ثوانٍ في ظل الظروف التشغيلية العادية.

تحافظ هيئة ختم الوقت TSA على قدرة تشغيلية على مدار الساعة طوال الأسبوع (24×7) للرد داخلياً على تقارير مشكلات الشهادات ذات الأولوية العالية كما هو موضح في القسم 4.9.3 من هذا البيان وعند الضرورة تُحوِّل هذه الشكاوى إلى الجهات القانونية المختصة او تُبطل الشهادة التي تتعلق بها الشكوى.

4.10.3 الميزات الاختيارية

لا يوجد تنظيم محدد.

4.11 نهاية الاشتراك

غير قابل للتطبيق.

4.12 الإيداع والاسترداد الرئيسي

4.12.1 سياسة وممارسات تغليف واسترداد مفتاح الجلسة

غير قابل للتطبيق.

4.12.2 سياسة وممارسات إيداع واسترداد المفتاح

غير قابل للتطبيق.

5 الضوابط الخاصة بالمرافق والإدارة والتشغيل

يحدد هذا القسم الضوابط الأمنية الفيزيائية والإجرائية التي تطبقها شركة مصدر التكنولوجيا ضمن عملياتها.

يتوافق برنامج إدارة أمن البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا (TS PKI GB) مع متطلبات أمن الشبكة ونظام الشهادات الصادرة عن منتدىCA/Browser بما في ذلك:

- الضوابط الأمنية الفيزيائية والبيئية .
- ضوابط سلامة النظام بما يشمل إدارة التهيئة والتغيير إدارة التحديثات إدارة الثغرات واكتشاف منع البرمجيات الخبيثة والفيروسات .
- الحفاظ على سجل بجميع الأصول وإدارتها وفقاً لتصنيفها .
- أمن الشبكات وإدارة الجدران النارية بما في ذلك تقييد المنافذ وتصفية عناوينIP .
- إدارة المستخدمين توزيع المهام على أدوار موثوقة بشكل منفصل التثقيف رفع الوعي والتدريب .
- ضوابط الوصول المنطقي تسجيل ومراقبة الأنشطة ومراجعة دورية لصلاحيات المستخدمين لضمان المساءلة الفردية.

يتضمن البرنامج الأمني لشركة مصدر التكنولوجيا إجراء تقييم سنوي للمخاطر يهدف إلى ما يأتي:

1. تحديد التهديدات الداخلية والخارجية المتوقعة التي قد تؤدي إلى الوصول غير المخول، أو الإفصاح، أو إساءة الاستخدام، أو التعديل، أو الإتلاف لأي من بيانات الشهادات الرقمية أو عمليات إدارتها.
2. تقييم احتمالية حدوث هذه التهديدات وحجم الأضرار المحتملة الناجمة عنها، مع مراعاة درجة حساسية بيانات الشهادات وعمليات الإدارة المتعلقة بها.
3. تقييم مدى كفاية السياسات والإجراءات وأنظمة المعلومات والتقنيات والترتيبات الأخرى التي تعتمدها الشركة لمواجهة تلك التهديدات.

وبناءً على نتائج تقييم المخاطر، تعمل الشركة على إعداد وتنفيذ وصيانة خطة أمنية تتألف من إجراءات وتدابير ومنتجات أمنية مصممة لتحقيق الأهداف المذكورة أعلاه، ولإدارة السيطرة على المخاطر التي تم تحديدها بما يتناسب مع حساسية البيانات وعمليات الإدارة.

تشمل هذه الخطة الأمنية ضمانات إدارية وتنظيمية وفنية ومادية ملائمة لحساسية البيانات والعمليات، كما تراعي الخطة التقنيات المتاحة وكلفة تنفيذ التدابير المحددة، مع تطبيق مستوى أمني معقول يتناسب مع الضرر المتوقع حدوثه في حال حصول أي خرق أمني، وبما ينسجم مع طبيعة البيانات المراد حمايتها.

5.1 الضوابط الأمنية الفيزيائية

تضمن شركة مصدر التكنولوجيا (TS PKI GB) تنفيذ الضوابط الفيزيائية المناسبة في منشآت استضافة البنية التحتية للمفاتيح العامة. وقد جرى توثيق هذه الضوابط ضمن السياسات الداخلية للشركة ويتم فرضها والتحقق من فعاليتها بانتظام من خلال تدقيقات داخلية يجريها فريق TS PKI GB على فريق عملياتTS PKI .

5.1.1 موقع البناء والإنشاء

تُستضاف جميع المكونات الحيوية لحل البنية التحتية للمفاتيح العامة داخل منشأة عالية الأمان تديرها شركة مصدر التكنولوجيا. تُفرض ضوابط أمنية فيزيائية لمنع وصول الأشخاص غير المصرح لهم من خلال أربع طبقات من الأمن

الفيزيائي. وعند دمج هذه المستويات المتعددة من التحكم في الوصول مع آليات الحماية الفيزيائية مثل الحراس وأجهزة استشعار التسلل وكاميرات المراقبة(CCTV) يتم توفير حماية قوية ضد الوصول غير المصرح به إلى أنظمةTS PKI .

تقع مرافق الحوسبة التي تستضيف خدمات هيئات التصديق التابعة لشركة مصدر التكنولوجيا في مدينة بغداد العراق.

5.1.2 الوصول الفيزيائي

تحظى أنظمة هيئات التصديق التابعة لشركة مصدر التكنولوجيا بحماية من خلال ضوابط أمنية فيزيائية متعددة الطبقات (أربع طبقات) حيث لا يمكن الوصول إلى الطبقات الأدنى إلا بعد اجتياز الطبقات الأعلى. وتُنفذ الأنشطة التشغيلية الحساسة لهيئات التصديق المرتبطة بدورة حياة الشهادة ضمن هذه الضوابط الصارمة.

تُنفّذ الأنشطة الإدارية ضمن طبقات فيزيائية شديدة التقييد. ويسجّل نظام التحكم في الوصول مرور الأشخاص عبر كل منطقة (أي طبقة).

تشمل الضوابط الأمنية الفيزيائية: دخول المبنى تحت مراقبة حراس الأمن التحقق البيومتري والمراقبة عبر كاميرات الدائرة التلفزيونية المغلقة(CCTV) وتعمل هذه الضوابط على حماية أنظمة هيئة التصديق من الوصول غير المصرح به حيث تتم مراقبتها على مدار الساعة وطوال أيام السنة ما يشكل طبقات متعددة من الحماية للأشخاص الداخلين والخارجين من المنشأة.

يُمنح الدخول إلى المنشأة عند تقديم بطاقة هوية المواطن الوطنية والتي يقوم حارس الأمن بالتحقق منها ويشمل ذلك تسجيل معلومات ذات صلة مثل هوية الشخص ووقت الوصول والمغادرة وتقديم شارة زائر. ولا يُسمح بالدخول إلا للأشخاص المخولين بذلك من قبل أحد أعضاء مجلس إدارة البنية التحتية للمفاتيح العامة (PKI Board) ويجب أن يرافقهم أحد الموظفين الموثوقين من شركة مصدر التكنولوجيا.

بالإضافة إلى ذلك لا يُسمح بالدخول إلى منطقة الحماية التي تستضيف أنظمة هيئة التصديق إلا إذا حضر موظفان موثوقان لفتح باب المنطقة.

5.1.3 الطاقة وتكييف الهواء

يتضمن تصميم منشأة استضافة البنية التحتية للمفاتيح العامة الخاصة بشركة مصدر التكنولوجيا وحدات تزويد طاقة غير منقطعة(UPS) ومولدات احتياطية قادرة على دعم تشغيل الأنظمة أثناء حالات انقطاع التيار الكهربائي. تتوفر وحدات UPSوالمولدات الاحتياطية لتغطية كامل المنشأة.

وقد تم تركيب نظام تكييف هواء مزدوج التهيئة بالكامل في المناطق التي تستضيف أنظمة البنية التحتية للمفاتيح العامة لضمان عمل المعدات ضمن نطاقات درجات الحرارة والرطوبة المحددة من قبل الشركات المصنعة.

5.1.4 التعرض للمياه

اتخذ فريق TS PKI GB احتياطات معقولة لتقليل تأثير التعرض للمياه على منشأة الاستضافة. وتشمل هذه الاحتياطات تركيب المعدات على أرضيات مضادة للكهرباء الساكنة ومزودة بكواشف للرطوبة.

5.1.5 الوقاية من الحرائق والحماية منها

تتبع منشأة استضافة البنية التحتية للمفاتيح العامة أفضل الممارسات واللوائح الأمنية المعمول بها في العراق وتخضع للمراقبة على مدار الساعة وطوال أيام السنة. كما جهزت بمعدات الكشف عن الحرائق والحرارة.

تتوفر أنظمة إخماد الحرائق في المناطق المخصصة وتعمل تلقائياً في حال حدوث حريق كما يمكن تفعيلها يدوياً عند الحاجة.

5.1.6 تخزين الوسائط

تخضع وسائط التخزين الإلكترونية والبصرية وغيرها من الوسائط إلى نفس الضوابط الأمنية الفيزيائية متعددة الطبقات وتتم حمايتها من التلف العرضي (كالماء أو الحريق أو التداخل الكهرومغناطيسي).

يتم تخزين وسائط التدقيق والنسخ الاحتياطي داخل خزنة آمنة مقاومة للحريق كما تُنسخ هذه الوسائط وتُخزّن في موقع الاستعادة من الكوارث.

5.1.7 التخلص من النفايات

يجب إتلاف جميع الأوراق ووسائط التخزين التي انشئت داخل المنشأة الآمنة قبل التخلص منها. تُفرم الوسائط الورقية باستخدام آلة تمزيق من نوع التقاطع وتُطبّق الإجراءات التالية على وسائط الحوسبة القابلة للإزالة:

- يجب الحصول على تفويض مسبق لإتلاف أي وسائط حوسبة قابلة للإزالة.
- تُمحى الوسائط أولاً ثم تُدمّر فعلياً إذا لم تعد مطلوبة.
- يُحتفظ بسجل لإتلاف هذه الوسائط.
- يمكن التخلص من الوسائط بعد تنفيذ الخطوات أعلاه.

تُدمَّرالأجهزة التشفيرية مادياً أو تُصفّر وفقاً لتعليمات الشركة المصنعة قبل التخلص منها.

5.1.8 النسخ الاحتياطي خارج الموقع

تُنفّذ نسخ احتياطية كاملة وتزايدية بشكل روتيني لأنظمة هيئة ختم الوقت لضمان توفر بيانات كافية لاستعادتها عند الحاجة. يتم أخذ نسخة احتياطية كاملة واحدة على الأقل وعدة نسخ تزايدية يومياً من الأنظمة الإلكترونية التابعة لهيئة ختم الوقت وفقاً لسياسات وإجراءات النسخ الاحتياطي الموثقة التي يلتزم بها فريق عمليات البنية التحتية للمفاتيح العامة.

يتم أخذ نسخ احتياطية من المعلومات الأكثر أهمية (مثل: المفاتيح الخاصة) في نهاية كل مراسيم توليد المفاتيح وفقاً لنص معتمد لمراسيم المفاتيح.

توفر منشآت النسخ الاحتياطي الكافية ضماناً بأن نُسخ النسخ الاحتياطي تُنقل إلى موقع الاستعادة من الكوارث حيث تُخزَّن هناك تحت نفس الضوابط الفيزيائية والتقنية والإجرائية المطبقة على المنشأة الأساسية.

5.2 الضوابط الإجرائية

5.2.1 الأدوار الموثوقة

يُعد جميع أعضاء الفريق الذين يُديرون عمليات إدارة المفاتيح والمسؤولين الإداريين وضباط الأمن أو أي فرد يشارك في عمليات تؤثر مادياً على هذه الأنشطة ضمن مناصب موثوقة (أفراد موثوقين).

يُجرى تحقق من الخلفية لجميع الموظفين الذين يُعينون في مناصب موثوقة قبل السماح لهم بتولي مسؤولياتهم. كما يتم الاحتفاظ بسجلات هذا التحقق ومراجعتها سنوياً.

تشمل الأدوار الموثوقة لهيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا ما يلي:

- مدير البنية التحتية للمفاتيح العامة :يمتلك بيانات اعتماد برمجيات هيئة التصديق. يتحمل مسؤولية تهيئة الهيئة وصيانتها.
- مشغّل البنية التحتية للمفاتيح العامة : مخوّل بتنفيذ دورة التشغيل الخاصة بهيئة التصديق ويشارك في العمليات الحيوية مثل عمليات إصدار شهادات المشتركين.
- ضابط الأمن : يمتلك بيانات اعتماد تخوّله تهيئة جهاز توليد المفاتيح الشفرية (HSMs) وسياسات البنية التحتية للمفاتيح العامة على الأنظمة المعنية بتوليد المفاتيح خلال مراسيم المفاتيح ذات الصلة.
- مسؤول هيئة التسجيل : مسؤول عن التحقق من المعلومات اللازمة لإصدار الشهادات والموافقة على طلبات الشهادات.
- أمناء :M-of-N يمتلكون بيانات تفعيل جهاز توليد المفاتيح الشفرية HSM ويتولون مسؤولية خزائن هيئات التصديق التابعة.
- مالك نطاق هيئة التصديق : يمتلك بيانات اعتماد تتيح تنفيذ عمليات النسخ الاحتياطي والاستعادة لأجهزة HSM الخاصة بهيئات التصديق التابعة.
- مدقق وحدة أمان المعدات : يمتلك بيانات اعتماد تخوّله استرجاع سجلات التدقيق الخاصة بوحداتHSM .
- أمناء مركز البيانات : يمتلكون بيانات اعتماد لفتح مركز بيانات البنية التحتية للمفاتيح العامة أثناء تنفيذ عمليات هيئة التصديق.
- مسؤول النظام : مخوّل بتثبيت وتهيئة واستكشاف وصيانة نظام التشغيل وقاعدة البيانات الداعمة.
- مسؤول الشبكة : مخوّل بتثبيت وتهيئة واستكشاف وصيانة معدات الشبكة الداعمة.

5.2.2 عدد الأشخاص المطلوبين لكل مهمة

يتبع فريق عمليات TS PKI إجراءات رقابة صارمة لضمان فصل المهام بناءً على المسؤوليات الوظيفية ولمنع قيام موظف موثوق واحد فقط بأداء العمليات الحساسة.

تتطلب المهام الأكثر حساسية وجود شخصين أو أكثر وتشمل ما يلي:

- الوصول الفيزيائي إلى المنطقة الآمنة التي تستضيف أنظمة هيئة ختم الوقت .
- الوصول إلى جهاز توليد المفاتيح الشفرية (HSM) الخاصة بهيئة التصديق وإدارتها .
- التحقق من صحة طلبات الشهادات والموافقة على إصدارها.

تُسجّل جميع الأنشطة التشغيلية التي ينفذها الأفراد في الأدوار الموثوقة ضمن سجل تدقيق موثوق وآمن ويمكن التحقق منه.

5.2.3 التحقق من الهوية والمصادقة لكل دور

قبل أداء مسؤوليات الدور الموثوق:

- يُؤكد فريق إدارة أمن البنية التحتية للمفاتيح العامة (TS PKI GB) هوية الموظف وتاريخه من خلال إجراء فحوصات خلفية وأمنية.

- عند الطلب عبر الإجراءات الداخلية لشركة مصدر التكنولوجيا يُصدر فريق تشغيل المنشأة بطاقة وصول لكل موظف يحتاج إلى الوصول الفيزيائي للمعدات الموجودة داخل المنطقة الآمنة.
- يُصدر موظفو البنية التحتية للمفاتيح العامة في شركة مصدر التكنولوجيا (TS PKI) المخصصون مثل مسؤولي الأنظمة بيانات اعتماد نظم تكنولوجيا المعلومات والاتصالات اللازمة لموظفي هيئة ختم الوقت.
- لتنفيذ مهامهم حسب أدوارهم.

5.2.4 الأدوار التي تتطلب فصل المهام

تحدد الأدوار الموثوقة المذكورة في القسم 5.2.1 مع تطبيق فصل مناسب للمهام.

5.3 الضوابط الخاصة بالموظفين

5.3.1 المؤهلات والخبرة والمتطلبات الأمنية

قبل توظيف أي فرد ضمن فريق TS PKI سواء كموظف أو وكيل أو متعاقد مستقل يضمن فريق إدارة أمن البنية التحتية للمفاتيح العامة (TS PKI GB) إجراء فحوصات تهدف إلى التحقق من الخلفية والمؤهلات والخبرة المطلوبة لأداء المهام ضمن السياق المهني للوظيفة المحددة. وتشمل هذه الفحوصات:

- التحقق من هوية الشخص :ويجب أن يُنفّذ التحقق من الهوية من خلال:
  - الحضور الشخصي (الفيزيائي) للفرد أمام أشخاص موثوقين مسؤولين عن وظائف الموارد البشرية أو الأمن.
  - التحقق من وثائق تعريف حكومية معترف بها وتحمل صورة فوتوغرافية.
- التحقق من موثوقية الشخص :ويشمل ذلك الفحص الخلفي والذي يغطي على الأقل ما يلي أو ما يعادله:
  - إدانات جنائية بجرائم خطيرة .
  - تقديم معلومات مضللة من قبل المرشح .
  - ملاءمة المراجع المقدمة .
- وأي تصاريح أمنية تراها الإدارة مناسبة.

5.3.2 إجراءات الفحص الخلفي

يُختار جميع الموظفين المكلفين بأدوار موثوقة بناءً على النزاهة والتحقيق في الخلفية والتصريح الأمني. ويضمن فريق .

TS PKI GB إجراء هذه الفحوصات مرة واحدة سنوياً لجميع الأفراد الذين يشغلون أدواراً موثوقة.

5.3.3 متطلبات التدريب

يوفر فريق TS PKI GB تدريباً فنياً أساسياً لموظفيه لتمكينهم من أداء مهامهم بفعالية. ويُحدّث هذا التدريب ويُنفّذ سنوياً لفريق هيئة ختم الوقت.

ويشمل برنامج التدريب مجموعة واسعة من المواضيع ويُقدّم من خلال مزيج من موظفي هيئة ختم الوقت ذوي الخبرة وخبراء خارجيين متخصصين في مجال الأمن والبنية التحتية للمفاتيح العامة. وقد صمم البرنامج بعناية ليلبّي المتطلبات الخاصة بكل دور موثوق مشارك في إدارة وتقديم خدمات هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا.

- نظرية البنية التحتية للمفاتيح العامة ومبادئها.

- ضوابط البيئة الأمنية وسياسات الحماية الخاصة بالبنية التحتية للمفاتيح العامة.
- عمليات هيئة التسجيل (RA) في البنية التحتية للمفاتيح العامة بما يشمل إجراءات التدقيق والتحقق.
- العمليات التشغيلية للبنية التحتية للمفاتيح العامة.
- تدريب عملي على منتجات البنية التحتية للمفاتيح العامة.
- إدارة الأدوار الموثوقة في البنية التحتية للمفاتيح العامة.
- إجراءات التعافي من الكوارث واستمرارية الأعمال لهيئة إصدار الشهادات TSA .

يحتفظ فريق إدارة أمن البنية التحتية للمفاتيح العامة (TS PKI GB) بتوثيق شامل لجميع الموظفين الذين خضعوا للتدريب ويقيّم بشكل دوري مدى رضا المشاركين والمدرّبين. وفي نهاية كل دورة تدريبية تُنظّم اختبارات وتُمنح شهادات للموظفين الذين يجتازونها. ويُشترط على جميع الأفراد الذين يشغلون أدواراً موثوقة بمن فيهم متخصصو التحقق اجتياز هذه الاختبارات قبل السماح لهم بممارسة مهامهم في الأدوار الموثوقة.

5.3.4 تكرار ومتطلبات إعادة التدريب

يُقدَّم منهج التدريب لجميع أعضاء فريق TS PKI وتُراجع المواد التدريبية وتُعدَّل سنوياً لتعكس أحدث الممارسات الرائدة وأية تغييرات على إعدادات أنظمة هيئات التصديق.

5.3.5 تكرار وتتابع دوران الوظائف

يضمن فريق TS PKI GB أن أي تغيير أو تدوير في الموظفين لا يؤثر على الكفاءة التشغيلية أو استمرارية وسلامة خدمات هيئة إصدار الشهاداتTSA .

5.3.6 العقوبات على الأفعال غير المصرح بها

لضمان المساءلة يفرض فريق TS PKI GB عقوبات على الموظفين نتيجة الأفعال غير المصرح بها أو إساءة استخدام الصلاحيات أو استخدام الأنظمة بدون تفويض وذلك وفقاً لسياسات وإجراءات الموارد البشرية المعتمدة والقانون العراقي الساري.

5.3.7 متطلبات المتعاقدين المستقلين

يخضع المتعاقدون المستقلون وموظفوهم لنفس فحوصات الخلفية التي يخضع لها موظفو .TS PKI وتشمل فحوصات الخلفية ما يلي:

- الإدانات الجنائية المتعلقة بجرائم جسيمة .
- تقديم معلومات مضللة من قبل المرشح .
- ملاءمة المراجع المقدمة .
- أية تصاريح أمنية تراها الإدارة ضرورية .
- حماية الخصوصية .
- شروط السرية.

5.3.8 الوثائق المزوّدة للموظفين

يوثّق فريق إدارة أمن البنية التحتية للمفاتيح العامة (TS PKI GB) جميع المواد التدريبية ويجعلها متاحة لموظفي .TS PKI كما يضمن الفريق توفير الوثائق التشغيلية الأساسية لأعضاء الفريق المعنيين وتشمل هذه الوثائق كحد أدنى بيان ممارسة الشهادات(CPS) وسياسات الأمان وأدلة التشغيل والوثائق الفنية ذات الصلة بكل دور موثوق.

5.4 إجراءات تسجيل التدقيق

تشمل إجراءات تسجيل التدقيق تسجيل الأحداث وتدقيق الأنظمة وتُنفذ لغرض الحفاظ على بيئة آمنة. وتشمل هذه الأنشطة إدارة دورة حياة المفاتيح بما في ذلك توليد المفاتيح النسخ الاحتياطي التخزين الاستعادة الإتلاف وإدارة الأجهزة التشفيرية بالإضافة إلى هيئة التصديق (CA) ومستجيب OCSP .

يتم توليد ملفات سجل التدقيق الأمني لجميع الأحداث المتعلقة بأمن هيئة التصديق وهيئة التسجيل (RA) ومستجيبي OCSP ويتم الاحتفاظ بها. وتُراجع هذه السجلات من قبل فريق ضباط أمن TS كما تخضع أيضاً للمراجعة كجزء من عمليات التدقيق الداخلي المنتظمة التي تنفذها وحدة الالتزام في TS على عمليات هيئة ختم الوقت.

5.4.1 أنواع الأحداث المسجلة

5.4.1.1 أنواع الأحداث المسجلة لهيئات التصديق (CAs)

تقوم شركة (مصدر التكنولوجيا) بتوثيق كافة الأحداث المتعلقة بالإجراءات المتخذة لمعالجة طلبات الشهادات الرقمية وإصدارها، بما في ذلك جميع المعلومات والوثائق المستلمة ذات الصلة بطلب الشهادة، مع تحديد التاريخ والوقت بدقة، وبيان الكوادر المعنية بالتنفيذ. وتلتزم (مصدر التكنولوجيا) بإتاحة هذه السجلات للمدقق المعتمد لغرض إثبات امتثال سلطة التصديق للمتطلبات والمعايير المحددة. كما تُولّد سجلات تدقيق لجميع الأحداث المتعلقة بأمن وخدمات أنظمة هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا. ويحتوي كل سجل تدقيق كحد أدنى على ما يلي:

- التاريخ والوقت الذي وقع فيه الحدث .
- مؤشر نجاح أو فشل الحدث (مثل: حدث توقيع من قبل هيئة التصديق حدث إلغاء حدث تحقق من الشهادة) .
- هوية الكيان اوالمشغّل الذي تسبب في الحدث .
- وصف الحدث.

عند الإمكان تُولَّد سجلات التدقيق تلقائياً وعند عدم توفر ذلك تُستخدم دفاتر أو نماذج ورقية. ويتم الاحتفاظ بكل من السجلات الإلكترونية وغير الإلكترونية من قبل فريق عمليات البنية التحتية للمفاتيح العامة وقد تُتاح للمراجعة خلال عمليات التدقيق على الالتزام.

تشمل الأحداث المسجلة في سياق عمليات هيئة ختم الوقت ما يلي:

1. أحداث إدارة دورة حياة مفاتيح هيئة ختم الوقت وتشمل:
   - توليد المفاتيح النسخ الاحتياطي التخزين الاستعادة الأرشفة والإتلاف.
   - أحداث إدارة دورة حياة الأجهزة التشفيرية.
   - طلبات الشهادات التجديد طلبات إعادة المفتاح والإلغاء.
   - الموافقة أو رفض طلبات الشهادات.

- توليد قوائم الإلغاء(CRLs) .
- توقيع ردودOCSP .
- إدخال ملفات تعريف شهادات جديدة وإيقاف ملفات تعريف الشهادات الحالية.

2. أحداث إدارة دورة حياة شهادات هيئة ختم الوقت وشهادات المشتركين:
   - طلبات الشهادات طلبات إعادة المفتاح والإلغاء .
   - جميع الشهادات المُصدرة بما في ذلك الشهادات الملغاة والمنتهية الصلاحية .
   - أدلة أنشطة التحقق مثل: التاريخ الوقت المكالمات الأشخاص الذين تواصل معهم .
   - قبول ورفض طلبات الشهادات .
   - إصدار الشهادات .
   - تحديثات قوائم الإلغاء بما في ذلك تحديثات إدخالات OCSP عند الاقتضاء .
   - توقيع ردود OCSP .
3. أحداث أمنية وتشمل:
   - محاولات الوصول الناجحة وغير الناجحة إلى أنظمة البنية التحتية للمفاتيح العامة .
   - الإجراءات المُنفّذة على أنظمة البنية التحتية للمفاتيح العامة وأنظمة الأمان .
   - أنشطة أجهزة التوجيه والجدران النارية ذات الصلة (كما هو موضح في القسم 5.4.1.3) .
   - تغييرات ملفات التعريف الأمنية .
   - مشكلات منصة النظام (مثل الأعطال) وأعطال الأجهزة والظواهر غير الاعتيادية الأخرى .
   - تثبيت وتحديث وإزالة البرمجيات على نظام الشهادات .
   - الدخول إلى مرفق هيئة التصديق والخروج منه.

كما يضمن فريق إدارة أمن البنية التحتية للمفاتيح العامة (TS PKI GB) الاحتفاظ بالمعلومات التالية التي لا تُنتجها هيئة ختم الوقت مباشرة سواء إلكترونياً أو يدوياً من قبل فريق عمليات TS :

- موظفو هيئة التصديق وتناوب/تغيير ملفاتهم الأمنية .
- جميع إصدارات هذا البيان(CPS) .
- محاضر الاجتماعات .
- تقارير التدقيق الداخلي على الالتزام .
- الإصدارات الحالية والسابقة من إعدادات هيئة ختم الوقت وأدلة التشغيل الخاصة بها.

5.4.1.2 أنواع الأحداث المسجلة لهيئات ختم الوقت

بالإضافة إلى ما سبق يتعين على هيئة ختم الوقت تسجيل المعلومات التالية وإتاحتها للمدقق المعتمد كدليل على التزام هيئة ختم الوقت بهذه المتطلبات:

1. الوصول الفيزيائي أو عن بُعد إلى خادم الختم الزمني بما في ذلك وقت الوصول وهوية الفرد الذي قام بالوصول .
2. سجل تاريخ إعدادات خادم الختم الزمني .
3. أي محاولة لحذف أو تعديل سجلات الختم الزمني .
4. الأحداث الأمنية وتشمل:
   - محاولات الوصول الناجحة وغير الناجحة إلى هيئة ختم الوقت .

- الإجراءات المنفذة من قبل هيئة ختم الوقت .
- تغييرات ملفات التعريف الأمنية .
- أعطال النظام أعطال الأجهزة وأي ظواهر غير طبيعية أخرى .
- أنشطة أجهزة التوجيه والجدران النارية ذات الصلة (كما هو موضح في القسم 5.4.1.3) .

5. إلغاء شهادة ختم زمني .
6. التغييرات الجوهرية على وقت خادم الختم الزمني .
7. تشغيل النظام وإيقافه.

5.4.1.3 سجلات أنشطة أجهزة التوجيه والجدران النارية تشمل:

1. محاولات تسجيل الدخول الناجحة وغير الناجحة إلى أجهزة التوجيه والجدران النارية .
2. تسجيل جميع الإجراءات الإدارية المنفذة على أجهزة التوجيه والجدران النارية بما في ذلك تغييرات الإعدادات تحديثات البرمجيات الثابتة وتعديلات التحكم بالوصول .
3. تسجيل جميع التعديلات التي أُجريت على قواعد الجدار الناري بما في ذلك الإضافات والتعديلات والحذف .
4. تسجيل جميع أحداث النظام والأخطاء بما يشمل أعطال الأجهزة تعطل البرمجيات وإعادة تشغيل النظام.

5.4.2 وتيرة معالجة السجلات

يضمن فريق إدارة أمن البنية التحتية للمفاتيح العامة (TS PKI GB) قيام الموظفين المعيّنين بمراجعة ملفات السجلات على فترات منتظمة للتحقق من سلامتها والتعرف في الوقت المناسب على الأحداث غير الاعتيادية .وكحد أدنى يعتمد فريق TS PKI GB دورة المراجعة التالية لسجلات التدقيق:

- تتم مراجعة سجلات التدقيق والأمان لتطبيقات هيئة التصديق من قبل فريق المراقبة والامتثال بشكل شهري.
- تفرض سياسات التحكم في الوصول المطبقة على أنظمة TS PKI أن يُمنح الوصول للقراءة فقط للموظفين الذين تشمل مهامهم التشغيلية الاطلاع على سجلات التدقيق.
- لا يمكن الوصول إلى الأنظمة التي تُخزن فيها سجلات التدقيق إلا من قبل الأدوار المخولة بذلك ويمكن تتبّع أي محاولة للتلاعب بسجلات التدقيق إلى الموظف المعني في هيئة ختم الوقت.
- يقوم قسم التدقيق والامتثال التابع لوحدة إدارة البنية التحتية للمفاتيح العامة (TS PKI GB) بإجراء تدقيق داخلي سنوي على عمليات هيئة تصديق الختم الزمني (TS Timestamping CA). ويطلب هذا التدقيق الداخلي عينات من تقارير مراجعة السجلات وسجلات التدقيق المجمعة منذ دورة التدقيق السابقة.
- يتم جمع وتوثيق أدلة مراجعات سجلات التدقيق، ونتائج عملية المراجعة، والإجراءات التصحيحية المنفذة.

5.4.3 إجراءات النسخ الاحتياطي لسجلات التدقيق

تُجرى نسخ احتياطية تزايدية وكاملة بشكل دوري. بالإضافة إلى ذلك تُطبّق القواعد التالية على نسخ سجلات التدقيق الخاصة بهيئة ختم الوقت:

- تُخزّن وسائط النسخ الاحتياطي محلياً في الموقع الرئيسي لهيئة ختم الوقت في موقع آمن .
- تُخزّن نسخة ثانية من بيانات وسجلات التدقيق في موقع الاستعادة من الكوارث الذي يوفر مستوى مماثلاً من الحماية الفيزيائية والبيئية كما في الموقع الرئيسي.

5.4.4 نظام جمع سجلات التدقيق (داخلي مقابل خارجي)

تبدأ عمليات التدقيق التلقائي عند بدء تشغيل النظام وتنتهي عند إيقافه. وفي حال فشل نظام التدقيق التلقائي وتهددت سلامة النظام أو سرية المعلومات المحمية يقرر فريق TS PKI GB ما إذا كان يجب تعليق عمليات هيئة التصديق المعنية حتى يتم حل المشكلة.

5.4.5 الإخطار للطرف المسبب للحدث

عند تسجيل حدث ما بواسطة نظام جمع سجلات التدقيق لا يُطلب تقديم إشعار للفرد أو المؤسسة أو الجهاز أو التطبيق الذي تسبب في الحدث.

5.4.6 تقييمات الثغرات

يجري فريق عمليات TS PKI تقييماً سنوياً للمخاطر يتضمن:

1. تحديد التهديدات المحتملة الداخلية والخارجية التي قد تؤدي إلى وصول غير مصرح به أو إفشاء أو إساءة استخدام أو تعديل أو إتلاف لأي بيانات شهادات أو عمليات إدارة الشهادات .
2. تقييم احتمال وتأثير هذه التهديدات مع الأخذ بعين الاعتبار حساسية بيانات الشهادات وعمليات إدارتها .
3. تقييم كفاية السياسات والإجراءات والأنظمة المعلوماتية والتقنيات والترتيبات الأخرى المعتمدة لدى TS لمواجهة تلك التهديدات.

كما تخضع أنظمة وبنية TS PKI التحتية لتقييمات أمنية دورية وفقاً لما يلي:

- خلال أسبوع واحد من استلام طلب من منتدىCA/Browser .
- بعد أي تغييرات جوهرية على النظام أو الشبكة حسب تقييم هيئة التصديق .
- مرة واحدة على الأقل كل ثلاثة (3) أشهر على عناوين الإنترنت العامة والخاصة التي حددت لأنظمة هيئة ختم الوقت الأساسية والمساندة في البنية التحتية للمفاتيح العامة. ويُنفّذ هذا التقييم الذاتي المنتظم من قبل أفراد الأمن ضمن فريق عملياتTS PKI .
- سنوياً وبعد أي ترقية أو تعديل في البنية التحتية أو التطبيقات تُعدّها إدارة TS PKI GB تغييرات جوهرية تقوم الإدارة بالتنسيق لتنفيذ تقييم مستقل للثغرات الأمنية واختبار اختراق من قبل طرف ثالث.

تُتاح نتائج هذه التقييمات المنتظمة وما يتم تحديده من مشكلات لفريق إدارة TS PKI GB والإدارة التشغيلية للبنية التحتية حيث يتحمل هؤلاء المسؤولية عن تنظيم وتنفيذ معالجات تلك المشكلات من قبل الفرق المختصة.

تُجمع الأدلة الخاصة بتنفيذ أنشطة تقييم الثغرات واختبار الاختراق وتُؤرشف من قبل الموظفين المعنيين في هيئة ختم الوقت.

5.5 أرشفة السجلات

5.5.1 أنواع السجلات المؤرشفة

تُؤرشف هيئة ختم الوقت جميع سجلات التدقيق (كما هو موضح في القسم 5.4.1) بالإضافة إلى ما يلي:

1. الوثائق المتعلقة بأمن أنظمة هيئة التصديق وأنظمة إدارة الشهادات.
2. الوثائق المتعلقة بالتحقق من الطلبات إصدار الشهادات وإلغائها.

5.5.2 مدة الاحتفاظ بالأرشيف

تحتفظ هيئة ختم الوقت بجميع الوثائق المتعلقة بطلبات الشهادات والتحقق منها وكافة الشهادات وإلغائها بالإضافة إلى الوثائق المتعلقة بأمن نظام هيئة التصديق لمدة سبع (7) سنوات بعد إصدار أي شهادة بناءً على هذه الوثائق وتاريخ انتهاء صلاحيتها.

5.5.3 حماية الأرشيف

تُؤرشف السجلات بطريقة تمنع حذفها أو إتلافها. وتُطبق ضوابط لضمان إمكانية إدارة الأرشيف فقط من قبل الموظفين المخولين دون المساس بسلامة أو مصداقية أو سرية السجلات المخزنة.

5.5.4 إجراءات النسخ الاحتياطي للأرشيف

تُحتفظ نسخة واحدة فقط من كل أرشيف رقمي في منشأة هيئة التصديق الرئيسية وموقع الاستعادة من الكوارث.
ويستخدم فريق عمليات TS PKI إجراءات موثقة للنسخ الاحتياطي والاستعادة والأرشفة تحدد كيفية إنشاء معلومات الأرشيف ونقلها وتخزينها.

5.5.5 متطلبات الختم الزمني للسجلات

تتضمن جميع الأحداث المسجلة والمؤرشفة تاريخ ووقت حدوث الحدث. ويُزامَن وقت الأنظمة الإلكترونية لهيئة ختم الوقت مع مصدر وقت مستمد من ساعة .GPS وتحقق إعدادات خدمات الختم الزمني دقة زمنية تبلغ ±1 ثانية أو أفضل بالنسبة للتوقيت العالمي المنسق(UTC) .

بالإضافة إلى ذلك يفرض فريق عمليات البنية التحتية للمفاتيح العامة (PKI) إجراءً يتحقق من انحراف الساعة ويقوم بتصحيحه.

5.5.6 نظام جمع الأرشيف (داخلي أو خارجي)

يُعد نظام جمع الأرشيف الخاص بهيئة ختم الوقت نظاماً داخلياً.

5.5.7 إجراءات الحصول على معلومات الأرشيف والتحقق منها

لا يُسمح بالوصول إلى المواد المؤرشفة إلا للموظفين المخولين والمصادق عليهم. يستخدم فريق عمليات TS PKI إجراءات النسخ الاحتياطي والاستعادة والأرشفة الخاصة بهيئة ختم الوقت والتي توثّق كيفية إنشاء معلومات الأرشيف ونقلها وتخزينها. كما توفّر هذه الإجراءات معلومات عن نظام جمع الأرشيف.

5.6 تبديل المفاتيح

لتقليل أثر اختراق المفاتيح يجب تغيير مفتاح هيئة ختم الوقت بتواتر يضمن أن تظل فترة صلاحية هيئة ختم الوقت أطول من العمر الأقصى لشهادات المشتركين بعد إصدار أحدث شهادة.

راجع القسم 6.3.2 من هذا البيان (CPS) لتفاصيل تواتر تبديل المفاتيح.

لدعم إدارة الإلغاء للشهادات المُصدرة يتم الاحتفاظ بالمفاتيح الخاصة للهيئة السابقة حتى انتهاء صلاحية جميع الشهادات التي وُقّعت باستخدامها.

5.7 التعامل مع الحوادث والتعافي من الكوارث

5.7.1 إجراءات التعامل مع الحوادث والاختراقات

عند اكتشاف محاولة اختراق محتملة أو أي شكل من أشكال الاختراق لهيئة ختم الوقت من قبل فريق إدارة أمنTS PKI GB يُجرى تحقيق لتحديد طبيعة ومدى الضرر على النحو التالي:

- إذا كان هناك اشتباه في اختراق المفتاح الخاص لهيئة التصديق تُتّبع الإجراءات المنصوص عليها في خطة استمرارية الأعمال والتعافي من الكوارث الخاصة بشركة مصدر التكنولوجيا.
- في الحالات الأخرى يُقيّم نطاق الضرر المحتمل لتحديد ما إذا كانت هناك حاجة إلى إعادة بناء هيئة التصديق أو إلغاء بعض الشهادات فقط أو الإعلان عن أن مفتاح الهيئة قد اختراقه.

كما يُحدّد فريق TS PKI GB آلية الإبلاغ عن الحوادث المتعلقة بالاختراق والإجراءات الاتصالية ذات الصلة كجزء من خطة استمرارية الأعمال والتعافي من الكوارث.

باستثناء حالات اختراق المفاتيح تُحدد شركة مصدر التكنولوجيا (TS) الإجراءات الخاصة بالتعافي عند تلف موارد الحوسبة أو البرمجيات أو البيانات أو عند الاشتباه بتلفها.

5.7.2 تلف موارد الحوسبة أو البرمجيات أو البيانات

تلتزم شركة مصدر التكنولوجيا بتنفيذ التدابير اللازمة لضمان الاستعادة الكاملة لخدمات هيئة ختم الوقت في حال وقوع كارثة أو تلف في الخوادم أو البرمجيات أو البيانات وذلك بعد حصولها على تفويض من فريق إدارة أمن البنية التحتية للمفاتيح العامة (TS PKI GB) لتفعيل إجراءات الاستجابة للحوادث.

تُحدّد وثيقة التعافي من الكوارث واستمرارية الأعمال الخاصة بهيئة ختم الوقت الظروف التي تستوجب تفعيل هذه الإجراءات والتي قد تشمل الاستعانة بموقع التعافي من الكوارث إذا لزم الأمر.

تُختبر خطة التعافي من الكوارث واستمرارية الأعمال الخاصة بهيئة ختم الوقت مرة واحدة على الأقل سنوياً بما في ذلك سيناريوهات التحويل التلقائي إلى موقع التعافي من الكوارث.

5.7.3 إجراءات التعامل مع اختراق المفتاح الخاص للجهة

فيما يخص اختراق مفاتيح المشتركين يُرجى الرجوع إلى القسم 4.9.

أما في حال اختراق المفتاح الخاص لهيئة ختم الوقت أو بيانات التفعيل المرتبطة به أو شهادة مستجيبOCSP فيُعتبر ذلك حادثاً بالغ الخطورة يتطلب تفعيل إجراءات محددة وثقت ضمن خطة التعافي من الكوارث واستمرارية الأعمال الخاصة بشركة مصدر التكنولوجيا.

وبالنظر إلى حساسية هذا النوع من الحوادث وتأثيره على البنية التحتية الوطنية للمفاتيح العامة في العراق يعقد فريق .

TS PKI GB اجتماعاً طارئاً لاتخاذ القرارات المناسبة وتنفيذ الاتصالات اللازمة وذلك ضمن خطة التعامل مع اختراق المفاتيح وإنهاء مهام هيئة التصديق. يُرجى الرجوع إلى القسمين 4.9.1 و4.9.3 لمزيد من التفاصيل.

5.7.4 قدرات استمرارية الأعمال بعد الكوارث

في حال وقوع كارثة أو تلف في الخوادم أو البرمجيات أو البيانات تُفعّل خطة التعافي من الكوارث واستمرارية الأعمال الخاصة بشركة مصدر التكنولوجيا لاستعادة الحد الأدنى من القدرات التشغيلية المطلوبة لهيئة ختم الوقت في الوقت المناسب.

وتركز الخطة تحديداً على استعادة الخدمات التالية سواءً في الموقع الرئيسي أو في موقع التعافي من الكوارث:

- خدمات إصدار وإلغاء الشهادات .
- المستودع العام حيث تُنشر شهادات هيئة التصديق وقوائم الإلغاء .
- خدمات مستجيب OCSP .

تُتيح سيناريوهات التحويل التلقائي إلى موقع التعافي من الكوارث إمكانية استعادة خدمات هيئة ختم الوقت الأساسية وذلك بفضل نظام النسخ الاحتياطي التابع لها الذي يضمن النسخ المتماثل المستمر للبيانات الحرجة من الموقع الرئيسي إلى موقع التعافي. ويتيح هذا النظام استعادة الخدمات الحيوية خلال فترة لا تتجاوز اثنتي عشرة (12) ساعة كحد أقصى لRTO .

تُعرّف خطة استمرارية الأعمال الخاصة بشركة مصدر التكنولوجيا ما يلي:

- الشروط الخاصة بتفعيل الخطة .
- الإجراءات الطارئة .
- إجراءات العودة .
- إجراءات الاستئناف .
- جدول صيانة دوري للخطة .
- متطلبات التوعية والتعليم .
- مسؤوليات الأفراد .
- هدف زمن الاستعادة(RTO) .
- الاختبارات الدورية لخطط الطوارئ .
- خطة للحفاظ على أو استعادة العمليات التشغيلية لهيئة ختم الوقت في الوقت المناسب بعد أي انقطاع أو فشل في العمليات الحيوية .
- شرط تخزين المواد التشفيرية الحساسة (مثل الأجهزة التشفيرية الآمنة ومواد التفعيل) في موقع بديل .
- تعريف ما يُعتبر انقطاعاً مقبولاً للنظام وزمن استعادته .
- مدى تكرار أخذ نسخ احتياطية من المعلومات والبرمجيات الحيوية .
- المسافة بين مرافق الاستعادة وموقع العمل الرئيسي .
- الإجراءات الخاصة بتأمين المنشأة بأقصى قدر ممكن خلال الفترة الممتدة بين وقوع الكارثة واستعادة بيئة آمنة سواء في الموقع الأصلي أو في موقع بديل.

لا تفصح شركة مصدر التكنولوجيا عن خطط استمرارية الأعمال للمشتركين أو الأطراف المعتمدة أو مزودي البرمجيات التطبيقية، إلا أنها تلتزم بتقديم خطة استمرارية الأعمال والخطط الأمنية إلى الجهات التدقيقية بناءً على طلبها.

5.8 إنهاء مهام هيئة التصديق أو هيئة التسجيل

تُنهى خدمات هيئة ختم الوقت في الحالات التالية:

أ) بموجب قرار من الإدارة التنفيذية لشركة مصدر التكنولوجيا .
ب) بقرار مبرر صادر عن الجهة الرقابية الشركة العامة للاتصالات والمعلوماتية ITPC .
ت) بقرار قضائي نهائي ولا رجعة فيه .
ث) عند تصفية أو إنهاء عمليات هيئة ختم الوقت.

إذا قرر فريق TS PKI GB و/أو لجنة إدارة التوقيع الإلكتروني التابعة لـ (ITPC PMA) ITPC أن إنهاء خدمات هيئة ختم الوقت ضروري يقوم فريق TS PKI GB بتنفيذ خطة إنهاء تم الاتفاق عليها مسبقاً مع . ITPC PMA وتتضمن خطة إنهاء TS كحد أدنى ما يلي:

- تقديم إشعار خطي إلى ITPC PMA بنيّة الشركة في إنهاء أنشطتها كهيئة تصديق مع نسخة من خطة الإنهاء وذلك قبل تسعين (90) يوماً على الأقل من:
  - التاريخ الذي ستتوقف فيه عن أداء أنشطة هيئة التصديق .
- انتهاء صلاحية تفويض TS لتقديم خدمات هيئة التصديق عند انطباق ذلك دون نية من TS لتجديد التفويض .
- ترتيبات TS للاحتفاظ بسجلات الأرشيف (كما هو موضح في القسم 5.5) .
- ترتيبات مقدم خدمة الثقة (TSP) للحفاظ على روابط خدمات حالة التحقق من الشهادات المذكورة في الشهادات التي ستظل سارية للفترة المعنية بعد الإنهاء .
- الإعلان عن نية TS بإنهاء أنشطة هيئة ختم الوقت خلال مدة لا تقل عن ستين (60) يوماً قبل الإنهاء الفعلي أو انتهاء التفويض أيّهما يحدث أولاً وذلك في الصحف اليومية أو عبر وسائل أخرى وبالطريقة التي تحددها لجنة إدارة التوقيع الإلكتروني لدى الشركة العامة للاتصالات والمعلوماتية(ITPC PMA) .
- التواصل مع الأطراف ذات العلاقة وترتيبات نقل سجلات هيئة ختم الوقت المؤرشفة إلى جهة حفظ مناسبة.
- خطة لتقديم المساعدة قدر الإمكان للمشتركين الحاليين في الانتقال إلى مقدم خدمة ثقة آخر .
- إلغاء جميع الشهادات الصادرة من هذه الهيئة والتي لم تُلغ بعد أو لم تنتهِ صلاحيتها في نهاية فترة الإشعار سواء طلب المشتركون إلغاءها أم لا .
- اتخاذ التدابير اللازمة لضمان عدم تسبب التوقف عن تقديم الخدمات باضطراب للمشتركين أو لأطراف التحقق المعتمدين .
- ترتيبات تضمن صيانة أنظمة الهيئة وإجراءاتها الأمنية المتعلقة بالبيانات الحساسة والدقيقة بشكل مناسب بعد الإنهاء.

6 الضوابط الأمنية الفنية

6.1 إنشاء أزواج المفاتيح وتركيبها

6.1.1 إنشاء أزواج المفاتيح

6.1.1.1 إنشاء زوج مفاتيح هيئة التصديق (CA)

يُنشأ زوج المفاتيح الخاص بهيئة ختم الوقت داخل ذاكرة وحدة الأجهزة الأمنية (HSM) المعتمدة والمقيمة وفقاً للمعيار FIPS 140-2المستوى 3.

تُسجّل مراسيم إنشاء المفاتيح الخاصة بهيئة ختم الوقت بالفيديو وتُخزن بشكل آمن لأغراض التدقيق.

تُنفذ مراسيم إنشاء مفاتيح هيئة ختم الوقت بحضور مدقق داخلي أو خارجي بهدف إصدار تقرير يتضمن الرأي الفني بشأن التزام شركة مصدر التكنولوجيا بما يلي:

1. توثيق إجراءات إنشاء المفاتيح وحمايتها لهيئة التصديق بما يتوافق مع بيان ممارسات هيئة التصديق (CPS) وسياسة مقدم خدمة الثقة (TSP CP).
2. تضمين التفاصيل المناسبة في نص مراسيم إنشاء مفاتيح هيئة التصديق.
3. تنفيذ المراسيم بحضور نصاب قانوني من الموظفين المخولين بمن فيهم ممثلون من فريق TS PKI GB.
4. الحفاظ على ضوابط فعالة تضمن بدرجة معقولة أن زوج مفاتيح هيئة التصديق قد تم إنشاؤه وحمايته وفقاً للإجراءات المنصوص عليها في هذا البيان والمستندات المعنية الأخرى.
5. تنفيذ جميع الإجراءات المطلوبة بموجب نص مراسيم إنشاء المفاتيح خلال عملية الإنشاء.

6.1.1.2 المشتركين

غير قابل للتطبيق.

6.1.2 تسليم المفتاح الخاص إلى المشترك

لا تتولى سلطة التصديق عملية إنشاء المفاتيح الخاصة بالمشتركين، كما أنها لا تقوم بإيداع تلك المفاتيح أو استردادها أو الاحتفاظ بنسخ احتياطية منها.

وفي حال كشفت سلطة التصديق أو اشتبهت في تسريب المفتاح الخاص بالمشترك إلى شخص غير مخول أو جهة غير تابعة للمشترك، فإن السلطة تقوم بإلغاء كافة الشهادات التي تتضمن المفتاح المعلن المقابل للمفتاح الخاص المُسرّب.

6.1.3 تسليم المفتاح العام إلى جهة إصدار الشهادات

يُرسل المفتاح العام المطلوب تصديقه إلى هيئة التصديق في شكل طلب توقيع شهادة(CSR) وذلك لضمان سلامة مصدر هذا المفتاح.

6.1.4 تسليم المفتاح العام لهيئة التصديق إلى أطراف التحقق المعتمدة

تُنشر شهادات المفتاح العام لهيئة التصديق في المستودع العام الخاص بشركة مصدر التكنولوجيا.

6.1.5 نوع الخوارزمية وأحجام المفاتيح

6.1.5.1 هيئة ختم الوقت

تستخدم هيئة ختم الوقت خوارزمية ECDSA بحجم 348-بت.

6.1.5.2 المشتركين

تُستخدم مفاتيح RSA بحجم 3072-بت أو 4096-بت (موصى به) للمشتركين.

6.1.6 إنشاء معلمات المفتاح العام وفحص جودتها

6.1.6.1 هيئة ختم الوقت

تُنشأ مفاتيح هيئة التصديق العامة والخاصة باستخدام أحدث أساليب توليد المعلمات. تفي وحدة HSM والبرمجيات المرتبطة بها بمتطلبات FIPS 186-2 المتعلقة بالتوليد العشوائي والتحقق من أولية الأعداد. ويستند فريق عمليات TS PKI إلى القسم 6.1.6 من المتطلبات الأساسية الخاصة بفحص الجودة.

6.1.6.2 المشتركين

غير قابل للتطبيق.

6.1.7 أغراض استخدام المفاتيح وفقاً لحقل المفاتيح في شهادة X.509 v3

تتضمن الشهادات الصادرة عن هذه الهيئة سلسلة بتات لأغراض استخدام المفاتيح بما يتوافق مع .[RFC 5280] يُرجى الرجوع إلى القسمين 7.1 و7.3 من هذا البيان.

6.2 حماية المفتاح الخاص وضوابط هندسة وحدات التشفير

6.2.1 معايير وضوابط وحدة التشفير

في عملية إنشاء وتخزين المفاتيح الخاصة بهيئة ختم الوقت تُستخدم وحدات أجهزة أمنية (HSM) معتمدة ومتوافقة مع المعيار FIPS 140-2 المستوى 3. وتُخزن هذه الوحدات ضمن المنطقة الداخلية والأكثر أماناً في منشأة استضافةTS PKI .

6.2.2 التحكم الجماعي n من m بالمفتاح الخاص

تخضع المفاتيح الخاصة لهيئة ختم الوقت دائماً لسيطرة متعددة من قبل أشخاص مخولين يشغلون أدواراً موثوقة في إدارة مفاتيح الهيئة وأسرارها ذات الصلة وتم توثيق هذه الأدوار ضمن إجراءات إنشاء المفاتيح (KGC) وسائر الوثائق الداخلية.

يُعيَّن موظفو هيئة ختم الوقت في الأدوار الموثوقة من قبل فريق TS PKI GB مع ضمان الفصل الوظيفي وتطبيق مبادئ السيطرة الجماعية والمعرفة المجزأة. ويتم تحقيق السيطرة الجماعية على المفاتيح الخاصة باستخدام آلية المعرفة المجزأة بنظام"m--n" حيث يشترط حضور عدد معين من الأشخاص 'm' (على الأقل اثنان) من أصل "n".

يجب أن يحضر ثلاثة (3) أشخاص وهو العدد الكلي لحماة المفاتيح في الوقت ذاته مع مديري جهاز توليد المفاتيح الشفرية (HSMs)لتفعيل المفتاح الخاص لهيئة التصديق أو إعادة تفعيله.

يحتفظ مجلس البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا (TS PKI GB) بسجلات مكتوبة وقابلة للتدقيق تتعلق بتوزيع الرموز وكلمات المرور ذات الصلة على العاملين الموثوقين وحماة المفاتيح. في حال استبدال أحد العاملين الموثوقين أو حماة المفاتيح يحتفظ المجلس بسجلات توزيع الرموز و/أو كلمات المرور الجديدة.

6.2.3 حفظ المفتاح الخاص لدى طرف ثالث
لا يتم حفظ المفاتيح الخاصة لهيئة ختم الوقت التابعة لمصدر التكنولوجيا لدى أي طرف ثالث.

6.2.4 النسخ الاحتياطي للمفتاح الخاص
تُنسخ المفاتيح الخاصة لهيئة ختم الوقت التابعة لمصدر التكنولوجيا وتُخزَّن بأمان داخل خزائن مخصصة في المناطق الأمنية الداخلية الأكثر تحصيناً في مرفق استضافة الهيئة.

تُنفذ عمليات النسخ الاحتياطي كجزء من مراسيم توليد المفاتيح الخاصة بالهيئة. وتخضع مفاتيح النسخ الاحتياطي لنفس مبدأ التحكم المشترك وتجزئة المعرفة المفروضة على المفاتيح الأصلية. وتُطبَّق المبادئ ذاتها في حالة استرجاع المفاتيح من النسخ الاحتياطية.

يُنقل المفتاح الخاص لهيئة ختم الوقت التابعة لمصدر التكنولوجيا فعلياً من الموقع الرئيسي إلى موقع الاستعادة باستخدام إجراء مخصص لمعالجة أجهزة HSM والمفاتيح وذلك ضمن مراسيم توليد مفاتيح الهيئة. يشارك موظفون موثوقون في العملية ويصاحبهم حراس أمن. يُرجى الرجوع إلى القسم 6.2.2 لمزيد من التفاصيل.

6.2.5 أرشفة المفتاح الخاص
لا يحتفظ مجلس البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا بأرشيف للمفاتيح الخاصة لهيئات التصديق.

6.2.6 نقل المفتاح الخاص من/إلى وحدة التشفير
يُسمح فقط بنقل أزواج مفاتيح هيئة ختم الوقت التابعة لمصدر التكنولوجيا إلى وحدة تشفير أخرى من نفس النوع وذلك باستخدام مسار موثوق ونسخ مباشر من وحدة إلى أخرى وتحت إشراف مشترك لعدة أشخاص.

6.2.7 تخزين المفتاح الخاص على وحدة التشفير
لا توجد متطلبات إضافية بخلاف ما ورد في الفقرات 6.2.1 و6.2.2 و6.2.4 و6.2.6.

6.2.8 طريقة تفعيل المفتاح الخاص
تتم عملية تفعيل المفاتيح الخاصة بسلطة التصديق ووحدة الختم الزمني وفقاً لمبادئ الرقابة الثنائية وتجزئة المعرفة. ويجب أن تُنفذ إجراءات التفعيل حصراً باستخدام جهاز إدخال رمز التعريف الشخصي المرتبط بوحدة حماية الأجهزة الأمنية.

6.2.9 طريقة إلغاء تفعيل المفتاح الخاص
يتم إيقاف تفعيل المفاتيح الخاصة بسلطة التصديق ووحدة الختم الزمني وفقاً للتعليمات والوثائق الفنية الصادرة عن الجهة المصنعة لوحدة حماية الأجهزة الأمنية.

6.2.10 طريقة تدمير المفتاح الخاص
يتطلب إتلاف المفتاح الخاص لسلطة التصديق، في غير حالات انتهاء العمر الافتراضي المخطط له، استحصال موافقة رسمية من قبل أعضاء متعددين في مجلس إدارة البنية التحتية للمفاتيح العامة التابع لشركة مصدر التكنولوجيا.

تخضع عملية الإتلاف لإجراءات موثقة ويجب أن تشارك فيها كوادر معينة ضمن الأدوار الموثوقة، بحد أدنى ثلاثة موظفين من الكادر الموثوق وبحضور ممثل واحد على الأقل من مجلس إدارة البنية التحتية للمفاتيح العامة، كما يجب أن تتم عملية الإتلاف بشهادة مدقق مؤهل.

أما فيما يتعلق بالمفاتيح الخاصة بوحدة الختم الزمني، فيتم حذف المفاتيح المقابلة من وحدة حماية الأجهزة الأمنية خلال ثمانية عشر شهراً من تاريخ إصدار الشهادة. وتنفذ عملية الحذف عبر مراسم إتلاف للمفاتيح تجريها الشركة ويشرف عليها ويوقع على محضرها عضوان على الأقل من أصحاب الأدوار الموثوقة.

يجوز لشركة مصدر التكنولوجيا أيضاً إجراء مراسم إتلاف شامل للمفاتيح، لضمان تدمير كافة النسخ الخاصة بالمفتاح -بما في ذلك النسخ الاحتياطية- تدميراً نهائياً وآمناً، بما يجعل عملية استردادها مستحيلة، وهو ما يلبي متطلبات الإزالة الكلية للمفاتيح الخاصة.

6.2.11 مستوى تقييم وحدة التشفير

تمت المصادقة على وحدات التشفير التابعة لهيئة ختم الوقت لمصدر التكنولوجيا وفقاً لمعيار [FIPS 140-2] المستوى الثالث.

6.3 جوانب أخرى لإدارة أزواج المفاتيح

6.3.1 أرشفة المفتاح العام

راجع الفقرة 5.5 للاطلاع على شروط الأرشفة.

6.3.2 فترات صلاحية الشهادات وفترات استخدام أزواج المفاتيح

تكون شهادات هيئة ختم الوقت التابعة لمصدر التكنولوجيا صالحة لمدة ست (6) سنوات بينما تكون فترة استخدام المفتاح ثلاث (3) سنوات.

لا يُستخدم المفتاح الخاص لهيئة التصديق التابعة بعد انتهاء فترة صلاحية شهادة المفتاح العام المرتبطة به. بالإضافة إلى ذلك لا يُستخدم المفتاح الخاص لتوقيع شهادات الكيانات النهائية بعد انتهاء فترة استخدامه باستثناء لوائح إلغاء الشهادات (CRLs) وشهادات مستجيبي OCSP لخدمة حالة صلاحية الشهادات.

تحتوي كل وحدة TSU على مفتاح توقيع ختم زمني نشط واحد في كل مرة، ويتم إنشاؤه كل 12 شهرًا.

6.4 بيانات التفعيل

6.4.1 إنشاء بيانات التفعيل وتثبيتها

6.4.1.1 هيئة إصدار الطوابع الزمنية (TS)

يتم إنشاء المفاتيح الخاصة لهيئة إصدار الطوابع وبيانات تفعيل أجهزة توليد المفاتيح الشفرية (HSM) خلال مراسم إنشاء المفاتيح الخاصة. راجع القسمين 6.1.1 و6.2.8 من هذه الوثيقة لمزيد من التفاصيل.

6.4.1.2 المشتركون

غير مطبق.

6.4.2 حماية بيانات التفعيل

6.4.2.1 هيئة إصدار الطوابع الزمنية (TS)

تضمن سياسة إدارة المفاتيح وإجراءات المراسم الخاصة بهيئة إصدار الطوابع تطبيق مبادئ التحكم متعدد الأشخاص وتقسيم المعرفة بشكل دائم لحماية مفاتيح هيئة إصدار الطوابع وبيانات تفعيل أجهزة توليد المفاتيح الشفرية. خلال مراسم إنشاء المفاتيح، تكون بيانات التفعيل تحت حراسة موظفي هيئة إصدار الطوابع المعينين بشكل دائم. راجع القسمين 6.1 و6.2 لمزيد من التفاصيل.

6.4.2.2 المشتركون

غير مطبق.

6.4.3 جوانب أخرى لبيانات التفعيل

لا يوجد شرط.

6.5 ضوابط أمن الحاسوب

6.5.1 المتطلبات الفنية الخاصة بأمن الحاسوب

تضمن شركة مصدر التكنولوجيا تطبيق ضوابط أمن الحاسوب بما يتوافق مع المعايير الفنية وإرشادات تعزيز أمن الموردين كحد أدنى. وتُوثَّق ضوابط أمن الحاسوب المُطبَّقة كجزء من وثائق السياسة الداخلية لمركز التحكم في ختم الوقت (TS Timestamping CA).

وتخضع أنظمة مركز التحكم وعملياته، على وجه الخصوص، لضوابط الأمان التالية:

1. فصل المهام وتطبيق ضوابط مزدوجة لعمليات مركز التحكم.
2. تطبيق ضوابط الوصول المادية والمنطقية.
3. تدقيق أحداث التطبيقات والأحداث المتعلقة بالأمان.
4. المراقبة المستمرة لأنظمة مركز التحكم في ختم الوقت (TS Timestamping CA) وحماية نقاط النهاية.
5. آليات النسخ الاحتياطي والاستعادة لعمليات مركز التحكم في ختم الوقت (TS Timestamping CA).
6. تعزيز نظام تشغيل خوادم مركز التحكم في ختم الوقت (TS Timestamping CA) وفقًا لأفضل الممارسات وتوصيات الموردين.
7. بنية أمنية متعمقة للشبكة تشمل جدران الحماية الخارجية والداخلية، وجدران حماية تطبيقات الويب، بما في ذلك أنظمة كشف التسلل.
8. إدارة التحديثات الاستباقية كجزء من العمليات التشغيلية لهيئة إصدار الشهادات بتقنية ختم الوقت (TS Timestamping CA).
9. تُفعّل أنظمة هيئة إصدار الشهادات بتقنية ختم الوقت (TS Timestamping CA) المصادقة متعددة العوامل لجميع الحسابات التي يمكنها إصدار الشهادات بشكل مباشر.

6.5.2 تقييم أمن الحاسوب

تخضع الجوانب التقنية لأمن الحاسوب لعمليات تدقيق دورية.

6.6 ضوابط تقنية لدورة الحياة

6.6.1 ضوابط تطوير النظام

يجب شحن الأجهزة أو البرمجيات المشتراة في حاويات مختومة مقاومة للعبث وتُركّب بواسطة موظفين مؤهلين. تُشترى التحديثات البرمجية أو العتادية بنفس طريقة شراء المعدات الأصلية. ويشارك موظفون موثوقون ومخصصون في تنفيذ إعدادات هيئة ختم الوقت التابعة لمصدر التكنولوجيا وفقاً لإجراءات تشغيلية موثقة.

تُختبر التطبيقات وتُطوّر وتُنفّذ وفقاً لأفضل ممارسات الصناعة في تطوير البرمجيات وإدارة التغيير. ولا يُنشر أي برنامج (أو تحديث) أو عتاد في الأنظمة الحية قبل اجتيازه عمليات إدارة التغيير والتهيئة التي يفرضها فريق عمليات البنية التحتية للمفاتيح العامة(TS PKI) .

يُجرى تقوية جميع المنصات العتادية والبرمجية لهيئة ختم الوقت التابعة لمصدر التكنولوجيا باستخدام أفضل الممارسات المعتمدة وتوصيات الموردين.

6.6.2 ضوابط إدارة الأمن

يُخصص العتاد والبرمجيات المستخدمة في إعداد هيئة التصديق لتنفيذ المهام المتعلقة بالهيئة فقط. ولا يُسمح بوجود أي تطبيقات أو أجهزة أو اتصالات شبكية أو برمجيات غير تابعة للبنية التحتية للمفاتيح العامة لمصدر التكنولوجيا (TS PKI) على عتاد هيئة التصديق أو متصلة به. .

تُطبق عملية إدارة التهيئة لضمان توثيق جميع إعدادات أنظمة هيئة التصديق وتعديلات التكوين والتحديثات والسيطرة عليها من قبل إدارة عمليات.TS PKI تخضع إعدادات أنظمة شركة مصدر التكنولوجيا لعمليات تدقيق دورية ومنتظمة، على ألا تتجاوز المدة الفاصلة بين تدقيق وآخر أسبوعاً واحداً كحد أقصى.

تُطبق عملية لإدارة الثغرات لضمان فحص أجهزة هيئة التصديق من البرمجيات الخبيثة عند الاستخدام الأول وبشكل دوري بعد ذلك. وتدعم هذه العملية معالجة الثغرات الأمنية الحرجة التي لم يتم تداركها سابقاً من قبل فريق عملياتTS PKI وذلك خلال 96 ساعة من اكتشافها.

6.6.3 ضوابط أمن دورة الحياة

يُرجى الرجوع إلى الفقرة 6.5.1.

6.7 ضوابط أمن الشبكة

طبّقت شركة مصدر التكنولوجيا بنية أمن شبكي قوية تتضمن جدران حماية مُدارة وأنظمة كشف التسلل. جرى تقسيم الشبكة إلى عدة مناطق بناءً على العلاقات الوظيفية والمنطقية والفيزيائية.

تُطبق حدود الشبكة بهدف تقييد الاتصالات بين الأنظمة (ضمن المنطقة الواحدة) وبين المناطق المختلفة وذلك باستخدام قواعد تدعم فقط الخدمات والبروتوكولات والمنافذ والاتصالات التي تحددها هيئة التصديق بوصفها ضرورية لعملياتها مع تعطيل جميع الحسابات والتطبيقات والخدمات والبروتوكولات والمنافذ غير المستخدمة في عمليات الهيئة.

تُحاط أنظمة الإصدار وأنظمة إدارة الشهادات وأنظمة الدعم الأمني ضمن منطقة شبكة عالية الأمان.

تُجرى عمليات فحص الثغرات الأمنية للشبكات بشكل دوري كل ثلاثة أشهر على الأقل، كما تُنفذ اختبارات الاختراق مرة واحدة سنوياً كحد أدنى. وتُحدد الفترات الزمنية لمعالجة الثغرات بناءً على مستوى خطورتها؛ حيث تتم معالجة الثغرات "الحرجة" خلال (24) ساعة، والثغرات "عالية الخطورة" خلال (48) ساعة، في حين يتم إصلاح الثغرات ذات الخطورة "المنخفضة والمتوسطة" خلال (96) ساعة. ويتم توثيق أي استثناءات وإخضاعها لتقييم المخاطر وتسجيلها رسمياً.

6.8 ختم الوقت

تُزامن مكونات هيئة ختم الوقت التابعة لمصدر التكنولوجيا بانتظام باستخدام خدمة وقت موثوقة. وتبلغ دقة إعدادات خدمات ختم الوقت +/- ثانية واحدة أو أفضل بالنسبة إلى التوقيت العالمي المنسق(UTC) .

تُشغّل شركة مصدر التكنولوجيا خدمة هيئة ختم الوقت (TSA) لدعم توقيع المستندات وتوقيع البرمجيات.

تحدد سياسة ختم الوقت وبيان الممارسات الخاص بشركة مصدر التكنولوجيا المتطلبات المتعلقة بتشغيل هيئة ختم الوقت التابعة لها. ويجب قراءة هذه السياسة بالاقتران مع بيان ممارسات الشهادات .(CPS) يمكن تحميل كلا الوثيقتين من الموقع التالي:
https://pki.techsource.iq.

7 ملفات تعريف الشهادات و CRL وOCSP

7.1 ملف تعريف الشهادة

7.1.1 رقم الإصدار

تصدر هيئة ختم الوقت التابعة لمصدر التكنولوجيا شهادات X.509 الإصدار 3 كما هو معرّف في المعيارRFC 5280 .

7.1.2 امتدادات الشهادة

تصدر هيئة ختم الوقت شهادات تحتوي على امتدادات X.509 الإصدار 3 كما هو معرّف فيRFC 5280 بالإضافة إلى الامتدادات التي يقرها منتدى CA/Browser .

تتضمن شهادات هيئة التصديق التابعة ووحدات ختم الوقت (TSU) امتداد سياسة الشهادة . ويجوز لشركة مصدر التكنولوجيا استخدام سياسة هيئة التصديق الخاصة بها و/أو عدد من معرفات السياسات المناسبة ضمن النطاق التالي:

- ETSI EN 319 421 البنى التحتية للتوقيع الإلكتروني متطلبات السياسات والأمن لمقدمي خدمات الثقة لإصدار الختم الزمني.
- المتطلبات الأساسية لإصدار وإدارة شهادات توقيع البرمجيات الموثوقة علنياً.

تتضمن شهادات وحدات ختم الوقت (TSU) امتداد الاستخدام الموسّع للمفتاح مع تعيينه كامتداد حرج وتحتوي على المعرفid-kp-timeStamping كمُعرّف لغرض المفتاح.

7.1.3 معرفات كائن الخوارزميات

تُصدر الشهادات باستخدام خوارزميات يحددها معرفات الكائن (OIDs) التالية:

الخوارزمية	معرّف الكائن
ecdsa-with-SHA384	معرّف الكائن } =:: المنظمة الدولية (1) هيئة الأعضاء (2) الولايات المتحدة ansi-X9-62 (840) (10045)التواقيع{ 3 (3) ecdsa-with-SHA2 (4)

7.1.4 أشكال الأسماء

7.1.4.1 ترميز الاسم

تصدر شركة مصدر التكنولوجيا شهادات وحدات ختم الوقت (TSU) بأشكال أسماء تتوافق مع المعيار ETSI EN 319 422بالنسبة للشهادات المخصصة لتوقيع المستندات.

وتصدر شركة مصدر التكنولوجيا شهادات TSU بأشكال أسماء تتوافق مع المتطلبات الأساسية لإصدار وإدارة شهادات توقيع البرمجيات الموثوقة علنياً بالنسبة للشهادات المخصصة لتوقيع البرمجيات.

7.1.4.2 معلومات الطرف - شهادات المشترك

تُحدَّد معلومات الطرف ذات الصلة بشهادات وحدات ختم الوقت (TSU) في الجدول أدناه.
تصدر شركة مصدر التكنولوجيا شهادات إلى وحدات TSU بحيث تتوافق محتويات حقول اسم الطرف مع المتطلبات المقابلة المنصوص عليها في القسم 6 من المعيار.ETSI EN 319 422

نوع الشهادة	اسم الطرف
شهادة توقيع المستندات لوحدة TSU (DS TSU Certificate)	الاسم المشترك
	اسم المنظمة
	معرف المنظمة
	اسم الدولة
شهادة توقيع البرمجيات لوحدةTSU	الاسم المشترك
	اسم المنظمة
	معرف المنظمة
	اسم الدولة

7.1.5 معلومات الموضوع - شهادات الجذر وشهادات هيئة التصديق التابعة

تتضمن شهادات هيئة التصديق الجذرية وشهادات هيئات التصديق التابعة سمات الاسم الشائع واسم المؤسسة واسم الدولة ويشكّل الجمع بين هذه المحتويات معرفاً يميز هيئة التصديق بشكل فريد عن غيرها من الهيئات.

7.1.6 قيود الأسماء

لا يوجد نص.

7.1.7 معرف كائن سياسة الشهادة (OID)

تعتمد شركة مصدر التكنولوجيا مخطط معرف كائن (OID) محدد لسياسة البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI). يُرجى الرجوع إلى قالب الشهادة التالي لمزيد من التفاصيل.

يُستخدم أيضاً معرف الكائن التالي في شهادات ختم الوقت الصادرة لتوقيع البرمجيات:

سياسات شهادة الكيان النهائي	
معرف محجوز وفق BR CS هيئة ختم الوقت TSA	2.23.140.1.4.2

7.1.8 استخدام امتداد قيود السياسات

لا يوجد نص.

7.1.9 بناء وتركيبة مؤهلات السياسات ودلالاتها

تتضمّن شهادات مصدر التكنولوجيا (TS) المُصدَرة إلى وحدات ختم الوقت (TSUs) مؤهل سياسة يشير إلى بيان ممارسة الشهادات (CPS) المعمول به.

7.1.10 الدلالات التنفيذية لامتداد سياسات الشهادات المُعلّمة

لا يوجد نص .

7.1.11 مواصفات شهادة هيئة التصديق لختم الوقت

CE = Critical Extension O/M: O = Optional M = Mandatory CO = Content: S = Static, D = Dynamic M/P: M = Mandatory P = Prohibited

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Root CA Signature	Root CA's signature value
TBSCertificate					
Version	False	M	S		
Version		M	S	2	Version 3
SerialNumber	False	M	D		

	CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature		False	M	S		
	AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer		False	M	S	<Root CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName			M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName			M	S	Informatics & Telecommunications Public Company	UTF8 encoded
CommonName			M	S	ITPC TSA Root CA G1	UTF8 encoded
Validity		False	M	D		Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	

	NotAfter		M	D	Certificate generation process date/time + **[72]** Months	Suggested validity for the subordinate certificate is up to 0val
Subject		False				
CountryName			M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString , size 2 (rfc5280)
OrganizationName			M	S	Technology Source	UTF8 encoded
CommonName			M	S	TS TSA CA G1	UTF8 encoded
SubjectPublicKeyInfo		False	M	D		
	AlgorithmIdentifier		M	D	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	
	SubjectPublicKey		M	D	Value of the key	
Extensions						
Authority Properties						
AuthorityKeyIdentifier		False	M	D		Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported as a minimum

AuthorityInfoAccess	False	M	S		
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.itpc.gov.iq	OCSP responder URL
AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	http://pki.itpc.gov.iq /repository/cert/tsa_root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M	S		
DistributionPoint		M	S	http://pki.itpc.gov.iq /repository/crls/tsa_root_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M	S		
keyCertSign, cRLSign		M	S	True	
ExtendedKeyUsage	False	M			
id-kp-timeStamping		M	S	True	
Policy Properties					

certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.4.2	CA/B BR Reserved Certificate Policy for Timestamping
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.16.368.1.1.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.itpc.gov.iq/repository/cps	
Basic Constraints Properties					
basicConstraints	True	M	S		
cA		M	S	True	
pathLenConstraint		M	S	0	

7.1.12 شهادات الكيانات النهائية

7.1.12.1 ملف تعريف شهادة TS DS TSU

CE = Critical Extension O/M: O = Optional M = Mandatory CO = Content: S = Static, D = Dynamic M/P: M = Mandatory P = Prohibited

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Subordinate CA Signature.	Subordinate CA's signature value
TBSCertificate					

Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M		<Subordinate Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS TSA CA G1	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[36]** Months	Suggested validity for the end user certificate is up to 3 years

Subject	False				
CountryName		M	S	IQ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Technology Source	UTF8 encoded
OrganizationIdentifier		M	D	An identification of the organization different from the organization name	UTF8 encoded
CommonName		M	D	A name commonly used by the subject to represent itself. It must uniquely identifies the TSU	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA	
SubjectPublicKey		M	D	Public Key Key length: 3072 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the subordinate issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			

	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.techsource.iq	OCSP responder URL
	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://pki.techsource.iq/repository/certs/tsa_ca.p7b	Subordinate Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/tsa_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties						
keyUsage		True	M			
	nonrepudiation		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.5	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	

	policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.6	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/tsaps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.6.1	timestamps issued in support of document signing signature.
Extended Key Usage Properties						
extendedKeyUsage		True	M			
	timeStamping		M	S	True	
Private Key Usage Period		False	M			
	GeneralizedTime		M	D	notBefore notAfter	This extension indicates the period of use of the private key corresponding to the certified public key. A new Key pair will be generated each 12 months

7.1.12.2 ملف تعريف شهادةTS CS TSU

CE = Critical Extension O/M: O = Optional M = Mandatory CO = Content: S = Static, D = Dynamic M/P: M = Mandatory P = Prohibited

Field	CE	O/M	CO	Value	Comment
Certificate		M			

TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Subordinate CA Signature.	Subordinate CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M		<Subordinate Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS TSA CA G1	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	

NotAfter		M	D	Certificate generation process date/time + **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False				
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Technology Source	UTF8 encoded
OrganizationIdentifier		M	D	An identification of the organization different from the organization name	UTF8 encoded
CommonName		M	D	A name commonly used by the subject to represent itself. It must uniquely identifies the TSU	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA	
SubjectPublicKey		M	D	Public Key Key length: 3072 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the subordinate issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.techsource.iq	OCSP responder URL

AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	http://pki.techsource.iq/repository/certs/tsa_ca.p7b	Subordinate Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/tsa_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M			
Digital signature		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.2.1.5	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.2.1.6	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/tsaps	

certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.6.2	timestamps issued in support of code signing signature.
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.23.140.1.4.2	BR CS Reserved OID (TSA)
Extended Key Usage Properties						
extendedKeyUsage		True	M			
	timeStamping		M	S	True	
Private Key Usage Period		False	M			
	GeneralizedTime		M	D	notBefore	This extension indicates the period of use of the private key corresponding to the certified public key. A new Key pair will be generated each 12 months
					notAfter	

7.2 ملف تعريف قائمة إبطال الشهادات (CRL)

CE = Critical Extension O/M: O = Optional M = Mandatory CO = Content: S = Static, D = Dynamic M/P: M = Mandatory P = Prohibited

Field	CE	O/M	CO	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	The signature of the CA issuing the CRL.	The signature of the authority issuing the CRL.

TbSCertList					
Version	False	M			
Version			S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M			
CountryName		M	S	IQ	
OrganizationName		M	S	Technology Source	
CommonName		M	S	TS TSA CA G1	
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		M	D	<creation time>	
NextUpdate		M	D	<Creation time> + [1] day + 2 hours	
RevokedCertificates	False	M			
CertificateSerialNumber		M	D	Serial of the revoked certificates	
revocationDate		M	D	Date when revocation was processed by the CA	UTC time of revocation
crlEntryExtension	False	M			
reasonCode		M	D	As per BR 7.2.2	Identifies the reason for the certificate revocation

CRLExtensions		False	M			
	AuthorityKeyIdentifier	False	M	D	160-bit SHA-1 hash of the public key of the CA issuing the CRL	
	CRL Number	False	M	D		Sequential CRL Number
	expiredCertsOnCRL	False	M	D		< contains the date on which the CRL starts to keep revocation status information for expired certificates>

7.2.1 رقم النسخة

تدعم هيئة التصديق لختم الوقت قوائم إلغاء الشهادات (CRLs) وفقاً للنسخة 2 من معيار X.509 راجع القسم 7.2 أعلاه.

7.2.2 امتدادات قائمة الإبطال ومدخلات القائمة

يُقدَّم ملف تعريف قائمة الإبطال في القسم 7.2 أعلاه.

7.3 ملف تعريف بروتوكول حالة الشهادة عبر الإنترنت (OCSP)

يتوافق ملف تعريف OCSP مع متطلبات المعيار RFC 6960 .

CE = Critical Extension O/M: O = Optional M = Mandatory CO = Content: S = Static, D = Dynamic M/P: M = Mandatory P = Prohibited

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	CA's Signature.	CA's Signature.

TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M		<Subject of the CA issuing the OCSP Certificate>	The issuer field is defined as the X.501 type "Name"
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS TSA CA G1	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + [12] months	**Validity period** is 12 months for OCSP Certificates

Subject	False	M			
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS TSA CA G1 OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Authority Properties					
AuthorityKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of the public key of the CA issuing the OCSP Certificate	
Policy Properties					
keyUsage	True	M			
digitalSignature		M	S	True	

extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			

هيكلية استجابة بروتوكول الاستعلام الآني عن حالة الشهادة.

يوضح الملف أدناه هيكلية استجابة بروتوكول الاستعلام الآني عن حالة الشهادة وفقاً للمعيار الدولي(RFC 6960) :

Field	Value	Comment
responseStatus	"0" Response has valid confirmations	Result of the query. If the value of responseStatus is other than "0", the responseBytes field is not set.
responseBytes		
responseType	id-pkix-ocsp-basic	
BasicOCSPResponse		
tbsResponseData		
version	1	Version of the response format
responderID	C = IQ O = <The full registered name of the subject> CN = <A name commonly used by the subject to represent itself>	Distinguished name of the OCSP responder. The information MUST correspond to the certificate that was used to sign the response.
producedAt		The time at which the OCSP responder signed this response.
responses		
certID		In accordance with RFC 6960
hashAlgorithm	Depending on the hash algorithm used in request	hashAlgorithm is the hash algorithm used to generate the issuerNameHash and issuerKeyHash values. Supported hash algorithms are SHA-1, SHA-256, SHA-384 and SHA-512.
issuerNameHash		Hash of issuer's DN
issuerKeyHash		Hash of issuer's public key
SerialNumber		CertificateSerialNumber
certStatus		Status of the certificate: • Good – certificate issued and has not been revoked. • Revoked – certificate is revoked. • Unknown – the certificate is unrecognized by this OCSP responder.
thisUpdate		The most recent time at which the status being indicated is known by the responder to have been correct.

nextUpdate	• ThisUpdate + 8 hours	The time at or before which newer information will be available about the status of the certificate
ArchiveCutoff[1]	• the CA's certificate "notBefore" time and date value	According to RFC 6960 clause 4.4.4. "archive cutoff" date set to the CA's certificate "notBefore" time and date value According to ETSI EN 319 411-2 / CSS-6.3.10-10.
extended-revoked definition	Null	the responder supports the extended definition of the "revoked" status to also include non-issued certificates
signatureAlgorithm	Sha384withRSAEncryption	Signing algorithm
signature		signature value
certs		Certificate corresponding to the private key used to sign the response. Only OCSP responder certificate is included in the OCSP response.

7.3.1 رقم النسخة

وفقاً لملف تعريف شهادةOCSP القسم 7.3.

7.3.2 امتدادات OCSP

وفقاً لملف تعريف شهادةOCSP القسم 7.3.

depicted in Figure 1.
mentation of the OCSP, the ''ArchiveCutoff'' extension is included in OCSP responces only for certificates that have expired

8 التدقيق على الامتثال والتقييمات الأخرى

تستهدف الإجراءات الموضحة في سياسة ممارسات التصديق هذه إلى المواءمة مع المتطلبات المحددة في القسم الأول، كما أنها تغطي كافة العناصر المعمول بها في معايير البنية التحتية للمفاتيح العامة الحالية ذات الصلة بالقطاعات التي تعمل فيها شركة مصدر التكنولوجيا.

8.1 تواتر أو ظروف التقييم

تنظم شركة مصدر التكنولوجيا تدقيقاً خارجياً وفق معيار WebTrust لضمان التزامها بالمتطلبات والمعايير والإجراءات ومستويات الخدمة المعمول بها وذلك مرة واحدة على الأقل سنوياً.

تقر شركة مصدر التكنولوجيا بهذا التدقيق لممارساتها وإجراءاتها وتنشر تقرير التدقيق علناً خلال مدة لا تتجاوز ثلاثة أشهر من نهاية فترة التدقيق.

يقوم كل من مجلس البنية التحتية للمفاتيح العامة (TS PKI GB) ولجنة إدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية (ITPC PMA) بتقييم نتائج هذه التدقيقات قبل تنفيذ أي إجراءات إضافية.

إضافة إلى ذلك تُنفذ تدقيقات داخلية استناداً إلى خطة تدقيق توافق عليها لجنة إدارة التوقيع الإلكتروني .(PMA) وتحت ظروف استثنائية (مثل حدوث خرق أمني) يمكن تنفيذ تدقيقات وتقييمات غير مخططة بناءً على طلب لجنة إدارة التوقيع الإلكتروني.

8.2 هوية/مؤهلات المُقيِّم

يُنفذ التدقيق الخارجي من قبل مدققين مؤهلين تنطبق عليهم المتطلبات التالية:

- الاستقلالية التامة عن الجهة الخاضعة للتدقيق .
- القدرة على إجراء تدقيق يغطي المعايير المحددة في معيارWebTrust .
- توظيف أفراد ذوي كفاءة في فحص تقنيات البنية التحتية للمفاتيح العامة وأدوات وتقنيات أمن المعلومات وتدقيق أمن تكنولوجيا المعلومات ووظائف التصديق من طرف ثالث .
- الحصول على ترخيص من WebTrust .
- الالتزام بالقوانين أو اللوائح الحكومية أو المدونات الأخلاقية المهنية .
- باستثناء جهات التدقيق الحكومية الداخلية الاحتفاظ بتأمين ضد المسؤولية المهنية أو الأخطاء والإغفالات بحد أدنى تغطية تأمينية قدرها مليون دولار أمريكي.

8.3 علاقة المُقيِّم بالجهة الخاضعة للتقييم

بالنسبة للتدقيقات الداخلية يمتلك مجلس البنية التحتية للمفاتيح العامة في شركة مصدر التكنولوجيا (TS PKI GB) وظيفة تدقيق مستقلة عن فريق عمليات البنية التحتية للمفاتيح العامة .(TS PKI Operations) أما المدققون الخارجيون فهم جهات مستقلة معتمدة منWebTrust .

8.4 المواضيع التي تغطيها عملية التقييم

تخضع هيئة التصديق هذه للتدقيق للتأكد من التوافق مع المعايير التالية:

- المبادئ والمعايير الخاصة بهيئات التصديق وفق WebTrust.
- المبادئ والمعايير الخاصة بهيئات التصديق – أمن الشبكات وفق WebTrust.
- المبادئ والمعايير الخاصة بهيئات التصديق – متطلبات القواعد الأساسية لتوقيع البرمجيات وفق WebTrust.

يُرجى الرجوع إلى القسم 8.1 للاطلاع على دورية عمليات التدقيق وإلى القسم 8.2 للاطلاع على مؤهلات المقيم.

8.5 الإجراءات المتخذة نتيجة أوجه القصور

تُبلَّغ نتائج التقييم والملاحظات الناتجة عنه إلى مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا (TS PKI GB).

فيما يتعلق بعمليات التدقيق الخاصة بهيئة ختم الوقت فإن أي استثناءات أو نواقص كبيرة تُكتشف خلال عملية التدقيق تدفع مجلس البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا إلى اتخاذ قرار بالإجراء اللازم. يُتخذ هذا القرار بناءً على مشورة المقيم. وفي حال وجود استثناءات أو نواقص يتولى مجلس TS PKI GB مسؤولية وضع وتنفيذ خطة عمل تصحيحية. وبعد تنفيذ الخطة يباشر المجلس إجراء تدقيق إضافي للتأكد من معالجة النواقص المُحددة.

8.6 إيصال نتائج التدقيق

تعكس النتائج الإجمالية لعمليات التدقيق من قبل مجلس TS PKI GB في المستودع العام لشركة مصدر التكنولوجيا.

تُتاح تقارير تدقيق (WebTrust) السنوية للجمهور في موعد لا يتجاوز ثلاثة (3) أشهر من تاريخ انتهاء فترة التدقيق. وفي حال حدوث تأخير يتجاوز المدة المذكورة، تلتزم شركة مصدر التكنولوجيا بتقديم خطاب توضيحي موقع من قبل المدقق المؤهل. يمكن الاطلاع على تقارير تدقيق (WebTrust) الخاصة بشركة مصدر التكنولوجيا عبر الرابط الآتي:

https://pki.techsource.iq/repository/ar/index.html.

9 مسائل قانونية وتجارية أخرى

9.1 الرسوم

9.1.1 رسوم إصدار أو تجديد الشهادات

غير قابلة للتطبيق.

9.1.2 رسوم الوصول إلى الشهادات

غير قابلة للتطبيق.

9.1.3 رسوم الوصول إلى حالة الشهادة أو إلغائها

غير قابلة للتطبيق.

9.1.4 رسوم الخدمات الأخرى

غير قابلة للتطبيق.

9.1.5 سياسة الاسترداد
غير قابلة للتطبيق.

9.2 المسؤولية المالية

9.2.1 التغطية التأمينية
تُؤكّد شركة مصدر التكنولوجيا أن هيئة ختم الوقت مشمولة ضمن الترتيبات التأمينية القائمة.

9.2.2 الأصول الأخرى
لا توجد اشتراطات.

9.2.3 التغطية التأمينية أو الضمان للمستخدمين النهائيين
يُرجى الرجوع إلى القسم 9.6.1.

9.3 سرية المعلومات التجارية

9.3.1 نطاق المعلومات السرية
تعتبر شركة مصدر التكنولوجيا المعلومات التالية معلومات سرية:

- الاتفاقيات التعاقدية بين شركة مصدر التكنولوجيا وموردیها.
- الوثائق الداخلية لشركة مصدر التكنولوجيا (عمليات الأعمال العمليات التشغيلية...).
- معلومات الموظفين السرية.

9.3.2 المعلومات الخارجة عن نطاق المعلومات السرية
تُعدّ أي معلومات لا تُصنِّفها شركة مصدر التكنولوجيا على أنها معلومات سرية معلومات عامة ويشمل ذلك المعلومات المنشورة في المستودع العام لشركة مصدر التكنولوجيا.

9.3.3 المسؤولية في حماية المعلومات السرية
تحمي شركة مصدر التكنولوجيا المعلومات السرية من خلال تدريب الموظفين وتطبيق السياسات على موظفيها ومقاوليها وموردیها.

9.4 خصوصية المعلومات الشخصية

9.4.1 خطة الخصوصية
تلتزم شركة مصدر التكنولوجيا بقواعد خصوصية البيانات الشخصية وقواعد السرية كما هو مبيَّن في بيان ممارسة الشهادات الحالي .(CPS) وتُنفذ شركة مصدر التكنولوجيا هذه الأحكام من خلال هيئة التسجيل التابعة لها(TS RA) .

يُرجى الرجوع إلى القسم 9.4.2 لتحديد نطاق المعلومات الخاصة وإلى القسم 9.4.3 لتحديد العناصر التي لا تُعدّ معلومات خاصة.

قد تخضع كل من المعلومات الخاصة وغير الخاصة لقواعد حماية البيانات إذا كانت تتضمن بيانات شخصية.

يُسمح فقط لعدد محدود من الأفراد الموثوق بهم بالوصول إلى المعلومات الخاصة المتعلقة بالمشترك وذلك لغرض إدارة دورة حياة الشهادة.

تحترم شركة مصدر التكنولوجيا جميع القوانين والأنظمة السارية المتعلقة بالخصوصية والمعلومات الخاصة وأسرار التجارة عند الاقتضاء بالإضافة إلى سياسة الخصوصية المنشورة وذلك عند جمع المعلومات غير العامة أو استخدامها أو الاحتفاظ بها أو الكشف عنها.

لن تُفصح شركة مصدر التكنولوجيا عن أي معلومات خاصة دون موافقة مالك البيانات الشرعي أو أمر قضائي صريح. وعند إفشاء المعلومات الخاصة تتخذ شركة مصدر التكنولوجيا تدابير معقولة لضمان عدم استخدامها إلا للأغراض التي طُلبت من أجلها.

وتلتزم الأطراف المصرَّح لها بالوصول إلى هذه المعلومات بحمايتها من أي اختراق والامتناع عن استخدامها أو إفشائها إلى أطراف ثالثة. كما يجب على هذه الأطراف الالتزام بقواعد حماية البيانات الشخصية وفقاً للقوانين المعمول بها في جمهورية العراق.

تضمن جميع قنوات الاتصال مع شركة مصدر التكنولوجيا الحفاظ على خصوصية وسرية المعلومات الخاصة المتبادلة. ويجب استخدام التشفير عند استخدام قنوات الاتصال الإلكترونية مع أنظمة هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا .

9.4.2 المعلومات المُعاملة كمعلومات خاصة

تُعدّ جميع المعلومات الشخصية التي لا تُنشر علناً ضمن محتوى الشهادة أو لائحة إلغاء الشهادات (CRL) معلومات خاصة.

9.4.3 المعلومات التي لا تُعدّ معلومات خاصة

لا تُعتبر المعلومات المُتضمَّنة ضمن الشهادة أو لائحة إلغاء الشهادات (CRL) معلومات خاصة.

9.4.4 المسؤولية في حماية المعلومات الخاصة

يتعامل موظفو البنية التحتية للمفاتيح العامة (TS PKI) والموردون والمقاولون مع المعلومات الشخصية بسرية تامة بموجب التزامات تعاقدية تفرضها شركة مصدر التكنولوجيا وتوفر على الأقل نفس مستوى الحماية المحدد في القسم 9.4.1.

9.4.5 الإشعار والموافقة على استخدام المعلومات الخاصة

تضمن شركة مصدر التكنولوجيا استخدام المعلومات الشخصية التي جُمعت فقط لغرض إدارة دورة حياة الشهادات وبما يتوافق مع موافقة المشتركين.

9.4.6 الإفصاح بموجب إجراء قضائي أو إداري

لن تُفصح شركة مصدر التكنولوجيا عن أي معلومات خاصة دون موافقة مالك البيانات الشرعي أو تفويض صريح بموجب أمر قضائي. يُرجى الرجوع إلى القسم 9.4.1 لمزيد من التفاصيل.

9.4.7 حالات أخرى للإفصاح عن المعلومات

لا يوجد اشتراط.

9.5 حقوق الملكية الفكرية

تحتفظ شركة مصدر التكنولوجيا بكافة حقوق الملكية الفكرية المتعلقة بقواعد بياناتها ومواقعها الإلكترونية وشهادات هيئات التصديق الصادرة عنها وأي منشور آخر يصدر عن البنية التحتية للمفاتيح العامة(PKI) بما في ذلك هذا البيان.

عند استخدام شركة مصدر التكنولوجيا برامج من موردين خارجيين تبقى هذه البرامج ملكاً فكرياً لموردي المنتجات ويخضع استخدامها من قبل هيئات التصديق التابعة لشركة مصدر التكنولوجيا لاتفاقيات الترخيص المبرمة بين الطرفين.

9.6 الإقرارات والضمانات

9.6.1 إقرارات وضمانات هيئة التصديق

عند إصدار شهادة تُقدّم هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا الضمانات المدرجة في هذا المستند إلى الأطراف المعتمدة التي تعتمد بشكل معقول على شهادة صالحة.

تُقر شركة مصدر التكنولوجيا وتُقدّم الضمانات لمستفيدي الشهادات بأنه خلال فترة صلاحية الشهادة التزمت هيئة ختم الوقت التابعة لها بمتطلبات القواعد الأساسية وبيان ممارسة الشهادات (CPS) عند إصدار الشهادة وإدارتها.

- دقة المعلومات : تؤكد شركة مصدر التكنولوجيا أنها طبّقت عند إصدار الشهادة إجراءات للتحقق من دقة جميع المعلومات الواردة فيها وفقاً لهذا البيان ومتطلبات القواعد الأساسية.
- الحالة :تؤكد الشركة أنها تحتفظ بمستودع عام متاح على مدار الساعة (7/24) يحتوي على معلومات محدثة بشأن حالة جميع الشهادات غير المنتهية (صالحة أو ملغاة).
- الإلغاء :تلتزم الشركة بإلغاء الشهادة لأي من الأسباب المحددة في هذه المتطلبات.
- الامتثال :التزمت هيئة ختم الوقت بمتطلبات القواعد الأساسية لتوقيع الخوارزميات وسياسة الشهادات وبيان ممارسة الشهادات المعتمد في إصدار كل شهادة من شهادات هيئة ختم الوقت وتشغيل البنية التحتية للمفاتيح العامة التابعة لها.

9.6.2 إقرارات وضمانات هيئة التسجيل

غير قابلة للتطبيق.

9.6.3 إقرارات وضمانات المشترك

غير قابلة للتطبيق.

9.6.4 إقرارات وضمانات الطرف المعتمد

يتعيّن على الأطراف المعتمدة التي تعتمد على الشهادات الصادرة عن شركة مصدر التكنولوجيا ما يلي:

- استخدام الشهادة فقط للغرض الذي أُصدرت من أجله كما هو موضح في بيانات الشهادة (مثل: امتداد استخدام المفتاح).
- التحقق من صلاحية الشهادة من خلال التأكد من أنها لم تنتهِ بعد.
- تأسيس الثقة في هيئة التصديق التي أصدرت الشهادة عن طريق التحقق من سلسلة الشهادة وفقاً للإرشادات المحددة في تعديل الإصدار الثالث من معيارX.509 .

- التأكد من أن الشهادة لم تُلغَ من خلال الوصول إلى معلومات حالة الإلغاء المحددة في موقع الشهادة المعتمدة.
- التأكد من أن الشهادة توفر مستوى كافياً من الضمانات للغرض المقصود منها.

9.6.5 إقرارات وضمانات المشاركين الآخرين

لا يوجد اشتراط.

9.7 إخلاء المسؤولية من الضمانات

في حدود ما يسمح به القانون العراقي وباستثناء حالات الاحتيال أو سوء الاستخدام المتعمد لا تتحمل شركة مصدر التكنولوجيا أية مسؤولية عن:

- دقة أي معلومات واردة في الشهادات باستثناء ما يضمنه المشترك الذي يتحمل المسؤولية النهائية عن صحة ودقة جميع البيانات التي يقدمها إلى شركة مصدر التكنولوجيا بهدف تضمينها في شهادة تصديق.
- الأضرار غير المباشرة الناتجة عن أو المرتبطة باستخدام الشهادات أو تقديمها أو إصدارها أو عدم إصدارها أو التواقيع الرقمية.
- السلوك المتعمد لأي طرف ثالث ينتهك القوانين المعمول بها في العراق بما في ذلك على سبيل المثال لا الحصر القوانين المتعلقة بحماية الملكية الفكرية أو البرمجيات الخبيثة أو الوصول غير المشروع إلى الأنظمة الحاسوبية.
- أي أضرار مباشرة أو غير مباشرة ناجمة عن انقطاع غير قابل للسيطرة في خدمات هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا.
- أي شكل من أشكال تحريف المعلومات من قبل المشتركين أو الأطراف المعتمدة فيما يتعلق بالمعلومات الواردة في هذا البيان أو أي وثائق أخرى نُشرت من قبل مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا والمتعلقة بخدمات هيئة ختم الوقت.

9.8 حدود المسؤولية

- لا تتحمل شركة مصدر التكنولوجيا أي مسؤولية فيما يتعلق باستخدام الشهادات أو أزواج المفاتيح العامة/الخاصة الصادرة بموجب هذا البيان لأي استخدام لا يتوافق مع ما ورد في هذا المستند.
- لا تتحمل الشركة مسؤولية تجاه أي طرف عن أي أضرار سواء كانت مباشرة أو غير مباشرة ناجمة عن انقطاع غير قابل للسيطرة في خدماتها.
- يتحمل الطرف المعتمد تبعات فشله في تنفيذ التزاماته كما هو مذكور في هذا البيان.
- تُنكر شركة مصدر التكنولوجيا أي مسؤولية مالية أو من أي نوع آخرعن الأضرار أو الأعطال الناتجة عن عمليات هيئة ختم الوقت التابعة لها.

9.9 التعويضات

غير قابلة للتطبيق.

9.10 مدة النفاذ وإنهاؤها

9.10.1 المدة

أُقرّ هذا البيان من قبل مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا (TS PKI GB) ويظل ساري المفعول إلى حين نشر تعديلات جديدة عليه في المستودع العام لشركة مصدر التكنولوجيا.

9.10.2 الإنهاء

تُطبّق التعديلات على هذا المستند وتُعتمد من قبل مجلس TS PKI GB ويُشار إلى ذلك بإصدار جديد للوثيقة وتُصبح النسخة الأحدث سارية المفعول بمجرد نشرها في المستودع العام لشركة مصدر التكنولوجيا. وتُحفَظ الإصدارات السابقة من هذا المستند في المستودع العام أيضاً.

9.10.3 أثر الإنهاء وبقاء الأحكام

يقوم مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا (TS PKI GB) بإبلاغ شروط وأثر إنهاء هذا البيان عبر الآليات المناسبة.

9.11 الإشعارات والتواصل مع الأفراد المشاركين

يمكن توجيه الإشعارات المتعلقة بهذا البيان إلى عنوان التواصل مع مجلس TS PKI GB كما هو مذكور في القسم 1.5.

9.12 التعديلات

عندما تقتضي الحاجة إدخال تعديلات على هذا البيان يتولى مجلس TS PKI GB دمج تلك التعديلات في إصدار جديد من الوثيقة ويُنشر الإصدار الجديد بعد اعتماده. ويتضمن الإصدار الجديد رقماً جديداً للإصدار.

9.12.1 إجراء التعديل

يُرجى الرجوع إلى القسم 9.12.

9.12.2 آلية الإشعار والفترة الزمنية

يُصبح الإصدار الأحدث من هذا البيان ساري المفعول عند نشره في المستودع العام لشركة مصدر التكنولوجيا. وتُحفَظ الإصدارات السابقة من هذا المستند في المستودع العام .يتولى مجلس TS PKI GB تنسيق التواصل المتعلق بتعديلات هذا البيان وتأثيراتها ذات الصلة.يحتفظ مجلس TS PKI GB بحق تعديل هذا البيان دون إشعار مسبق في حال كانت التعديلات غير جوهرية بما في ذلك على سبيل المثال لا الحصر تصحيح الأخطاء المطبعية أو التحسينات الطفيفة.

9.12.3 الحالات التي يجب فيها تغيير معرف الكائن(OID)

تحتفظ شركة مصدر التكنولوجيا بحق تعديل محتوى أي بيان ممارسة شهادات منشور ولا يؤدي أي تغيير جوهري في هذا البيان إلى تعديل معرف الكائن (OID) الخاص به والمنشور في المستودع العام لشركة مصدرالتكنولوجيا ويُعبّر معرف الكائن (OID)عن النسخة الحالية السارية والمعتمدة من البيان.

9.13 أحكام تسوية النزاعات

تُحال جميع النزاعات المرتبطة بأحكام هذا البيان وخدمات هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا في المقام الأول إلى القسم القانوني لمجلس .TS PKI GB وإذا لم تُفضِ الوساطة التي يجريها القسم القانوني إلى نتيجة تُحال النزاعات إلى المحاكم المختصة في جمهورية العراق للفصل فيها.

9.14 القانون الحاكم

تُطبَّق قوانين جمهورية العراق على قابلية تنفيذ هذا البيان وتفسيره وتأويله وصحته.

9.15 الامتثال للقوانين المعمول بها

يتوافق هذا البيان وخدمات هيئة ختم الوقت التابعة لشركة مصدر التكنولوجيا مع القوانين ذات الصلة والمعمول بها في جمهورية العراق.

9.16 أحكام متنوعة

9.16.1 الاتفاقية الكاملة

لا يوجد اشتراط.

9.16.2 التنازل

ما لم يُنص على خلاف ذلك في عقود أخرى لا يجوز لأي طرف التنازل عن حقوقه أو تفويض واجباته المنصوص عليها في هذا البيان دون موافقة خطية مسبقة من شركة مصدر التكنولوجيا.

9.16.3 قابلية الفصل

إذا تبيَّن أن أي حكم من أحكام هذا البيان غير صالح أو غير قابل للتنفيذ تبقى باقي الأحكام سارية المفعول إلى حين تحديث هذا البيان.

في حال وجود تعارض بين متطلبات القواعد الأساسية وأي تنظيم ساري في العراق يجوز لشركة مصدر التكنولوجيا تعديل أي متطلب متعارض إلى الحد الأدنى اللازم لجعل المتطلب صالحاً وقانونياً في العراق .ينطبق هذا فقط على العمليات أو إصدار الشهادات التي تخضع لذلك القانون. في هذه الحالة تُدرَج في هذا القسم مرجعية تفصيلية للقانون الذي يتطلب التعديل وكذلك التعديل المحدد الذي تم تنفيذه على متطلبات القواعد الأساسية.

كما ستقوم شركة مصدر التكنولوجيا قبل إصدار أي شهادة بموجب المتطلب المعدَّل بإخطار منتدى CA/Browser بالمعلومات ذات الصلة التي تمت إضافتها حديثاً إلى هذا البيان .يُنهى أي تعديل في الممارسة تم بموجب هذا القسم إذا لم يعُد القانون سارياً أو إذا جرى تعديل متطلبات القواعد الأساسية بشكل يُتيح الامتثال لكل منهما في الوقت ذاته. ويُنفذ التعديل المناسب في الممارسة وتُعدَّل الوثيقة ويُرسل إشعار إلى منتدى CA/Browser خلال مدة لا تتجاوز 90 يوماً.

9.16.4 التنفيذ (أتعاب المحاماة والتنازل عن الحقوق)

لا يوجد اشتراط.

9.16.5 القوة القاهرة

لا تتحمّل شركة مصدر التكنولوجيا أية مسؤولية عن أي فشل أو تأخير في أداء التزاماتها بموجب أحكام هذا البيان إذا كان ذلك بسبب أسباب خارجة عن نطاق سيطرتها المعقولة بما في ذلك على سبيل المثال لا الحصر انقطاع أو تأخر خدمات الاتصالات.

9.17 أحكام أخرى

غير قابلة للتطبيق.