مصدر التكنولوجيا

لخدمات النظم والبرمجيات

والتجارة العامة المحدودة

البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI)

هيئة التصديق لتوقيع البرمجيات

بيان ممارسة الشهادات

التحكم بالوثيقة

أُعد/حُدثَ بواسطة	راجعه	وافق عليه	المالك	الإصدار	تاريخ الموافقة
			مصدر التكنولوجيا	1.2	

سجل التغييرات

الرقم التسلسلي	الإصدار	وصف التغييرات	
0.1	18.01.2023	النسخة الأولية	مصطفى طوير
0.2	23/02/2023	مراجعة داخلية وتحديث	أحمد إبراهيم
0.3	02/07/2023	تحديث القسم 4.9.1 ليتماشى مع BR CS 3.3.0	مصطفى طوير
0.4	04/12/2023	إضافة قيم OID ومعلومات الاتصال ورابط المستودع وتطبيق قالب مصدر التكنولوجيا	مصطفى طوير
0.5	28/02/2024	مراجعة وتحديث استناداً إلى ملاحظات المدقق على CP/CPS للهيئة الجذرية و CPلمزود خدمات الثقة	مصطفى طوير وياسر خان
0.6	02/05/2024	تحديث القسم 5.4.1 لتوضيح البيانات التي يجب تسجيلها ضمن متطلبات تسجيل أنشطة الجدار الناري والموجهات	مصطفى طوير
0.7	15/05/2024	مراجعة وتحديث استناداً إلى ملاحظات المدقق علىCPSs	مصطفى طوير وياسر خان
1.0	15/07/2024	تحديثات استناداً إلى توصيات المدقق بعد تدقيق نقطة في الزمن	مصطفى طوير وياسر خان
1.1	16/09/2025	المراجعة السنوية	شركة مصدر التكنولوجيا
1.2	03/06/2026	• تقليص الحد الأقصى لصلاحية شهادات توقيع الكود (Code Signing)ليتوافق مع أحدث المتطلبات الأساسية - (CS BR) (التصويت رقم.(CSCWG-31	شركة مصدر التكنولوجيا

الرقم التسلسلي	الإصدار	وصف التغييرات	
		• تعديل مسمى "اتفاقية المشترك (Subscriber Agreement) " ليصبح "شروط وأحكام استخدام المشترك (Subscriber Terms and Conditions of Use). • التعديل ليشمل إمكانية إعادة استخدام البيانات التي تم التحقق منها مسبقاً بدلاً من إجراء عملية تحقق كاملة عند طلب مفتاح جديد (Re-key). • التعديل لاستبدال عملية التحقق القائمة على الإقرار (Attestation-based) بعملية التأكيد المباشر (Direct confirmation) - القسم 3.2.5. • تصحيح أخطاء مطبعية أخرى.	

الموافقة على الوثيقة

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

الفهرس

1. المقدمة

يُعد هذا المستند بيان ممارسة الشهادات (CPS) الذي يصف ممارسات التصديق المطبقة من قبل هيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا (ويشار إليها لاحقاً بTS) .ويتوافق هذا البيان مع سياسة الشهادات الخاصة بمقدمي خدمات الثقة (TSP) المعتمدة لتقديم خدمات التصديق التي يقدمها مقدمو خدمات الثقة الذين يصدرون شهادات موثوقة علنياً للجهات النهائية وذلك تحت هيئات التصديق الجذرية للبنية التحتية الوطنية للمفاتيح العامة العراقية في جمهورية العراق.

يتناول هذا البيان السياسات الفنية والإجرائية والتنظيمية الخاصة بهيئة التصديق لتوقيع البرمجيات التابعة لTS والتي أُنشئت وتُدار من قبل شركة مصدر التكنولوجيا ضمن التسلسل الهرمي للبنية التحتية الوطنية للمفتاح العام في العراق وذلك فيما يتعلق بكامل دورة حياة الشهادات التي تصدرها هذه الهيئة.

يشمل هذا البيان إصدار الشهادات وإجراءات التحكم المتعلقة بأنواع الشهادات التالية التي تصدرها هيئة التصديق لتوقيع البرمجيات التابعة لـ TS:

- **شهادات توقيع البرمجيات –** تُصدر للأشخاص الاعتباريين لتوقيع المكتبات وملفات exe وملفات msi وما إلى ذلك.
- **شهادة مستجيب OCSP –** تُستخدم لتوقيع استجابات بروتوكول التحقق من حالة الشهادة عبر الإنترنت (OCSP) المتعلقة بالشهادات الصادرة عن هيئة التصديق لتوقيع البرمجيات.

يتوافق هذا البيان مع المتطلبات الرسمية المحددة من قبل فرقة مهام هندسة الإنترنت (IETF) في الوثيقة RFC 3647 من حيث الهيكل والمحتوى. ورغم أن بعض العناوين مدرجة بما يتماشى مع بنيةRFC 3647 إلا أن بعض المواضيع قد لا تكون قابلة للتطبيق في تنفيذ هيئة التصديق لتوقيع البرمجيات الخاصة بـ .TS وتُصنّف هذه الأقسام بأنها "غير قابلة للتطبيق". وتُدرج معلومات إضافية في الفروع الفرعية من البنية القياسية عند الحاجة.

تلتزم هيئة حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا بالحفاظ على هذا البيان متوافقاً مع الإصدارات الحالية للمتطلبات التالية المنشورة على الموقعhttp://www.cabforum.org :

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

وفي حال وجود أي تعارض بين هذا المستند والمتطلبات المشار إليها أعلاه فإن المتطلبات المذكورة أعلاه لها الأسبقية على هذا المستند.

يُعد بيان ممارسة الشهادات هذا وثيقة عامة. وفي الحالات التي يُشار فيها إلى معلومات سرية ضمنه فإن النص يُحيل إلى وثائق مصنفة متاحة فقط للأشخاص المخولين.

يمكن الحصول على مزيد من المعلومات المتعلقة بهذا البيان من مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا باستخدام معلومات الاتصال الواردة في البند 1.5.

1.1.نظرة عامة

تُعد البنية التحتية الوطنية للمفاتيح العامة العراقية في العراق (PKI) منشأة تحت إشراف الشركة العامة للاتصالات والمعلوماتية(ITPC) والتي تشرف على عدة هيئات تصديق جذرية تمثل البرنامج الوطني لهيئات التصديق الجذرية. ومن خلال هذه البنية التحتية الوطنية للمفاتيح العامة العراقية تهدف الحكومة العراقية إلى توفير إطار عمل يُسهم في تسهيل إنشاء مقدمي خدمات الثقة (TSP) لتقديم خدمات التصديق الرقمي والخدمات الموثوقة للجهات الحكومية وغير الحكومية. وتتكون البنية التحتية للمفتاح العام في العراق من مستويين كما هو موضح أدناه:

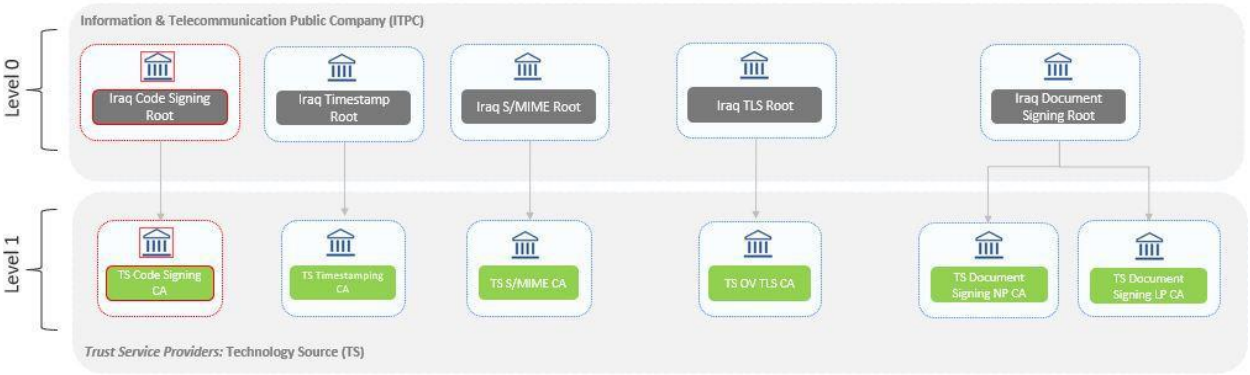
المستوى 0:

أُنشئت خمس (5) هيئات تصديق جذرية لأنواع مختلفة من الشهادات التي تُصدر. وتتحمل الشركة العامة للاتصالات والمعلوماتية (ITPC) المسؤولية عن هذا المستوى من الهيئات الجذرية. وبصفتها الهيئة الوطنية لحوكمة البنية التحتية للمفتاح العام كُلفت الشركة العامة للاتصالات والمعلوماتية بإدارة اللجنة العليا لإدارة التوقيع الإلكتروني (PMA). هيئات التصديق الجذرية التابعة لـ ITPC هي:

- هيئة التصديق الجذرية لتوقيع البرمجيات في العراق: تصدّق/توقّع على هيئات التصديق التابعة لتوقيع البرمجيات.
- هيئة التصديق الجذرية للبريد الإلكتروني الآمن (S/MIME) في العراق: تصدّق/توقّع على هيئات التصديق التابعة لحماية البريد الإلكتروني.
- هيئة التصديق الجذرية لاتصال الأمن TLS في العراق: تصدّق/توقّع على هيئات التصديق التابعة لـTLS
- هيئة التصديق الجذرية لتوقيع المستندات في العراق: تصدّق/توقّع على هيئات التصديق التابعة لتوقيع المستندات للأشخاص الطبيعيين والاعتباريين.
- هيئة التصديق الجذرية لختم الوقتي في العراق: تصدّق/توقّع على هيئات التصديق التابعة للختم الوقتي.

المستوى 1:

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



فيما يخص شهادات توقيع البرمجيات فإن هيئة التصديق الجذرية العراقية لتوقيع البرمجيات فقط هي المعنية لأنها توقّع شهادة هيئة التصديق التابعة لتوقيع البرمجيات الخاصة بشركة مصدر التكنولوجيا. أما الهيئات الجذرية الأخرى فهي تابعة للبنية التحتية للمفتاح العام العراقية لكنها ليست ذات صلة بإصدار شهادات توقيع البرمجيات ولا تُدرج ضمن تسلسل توقيع البرمجيات كما هو موضح في الشكل 1.

شركة مصدر التكنولوجيا هي الجهة المسؤولة عن تشغيل هيئات التصديق التابعة وتقديم خدمات الثقة ذات الصلة للمجالات الحكومية وغير الحكومية. وبناءً على ذلك تعمل شركة مصدر التكنولوجيا كمقدم خدمات ثقة (TSP) وتقدم خدماتها من خلال تسلسل هرمي لهيئات التصديق التابعة المنشأة تحت هيئات التصديق الجذرية التابعة للشركة العامة للاتصالات والمعلوماتية .(ITPC) وقد صدّقت هيئات التصديق الجذرية التابعة لـ ITPC على هيئات التصديق التابعة لمقدم خدمات الثقة الخاص بشركة مصدر التكنولوجيا على النحو التالي:

- هيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا: هيئة تابعة تصدر شهادات لتوقيع مكتبات البرمجيات وملفات jar وملفات exe وملفات msi وغيرها.
- هيئة التصديق للبريد الإلكتروني الآمن (S/MIME) التابعة لشركة مصدر التكنولوجيا: هيئة تابعة تصدر شهادات لتوقيع البريد الإلكتروني وتشفيره.
- هيئة التصديق لاتصال TLS التابعة لشركة مصدر التكنولوجيا: هيئة تابعة تصدر شهادات TLS لخوادم الويب بالتحقق التنظيمي.(OV)
- هيئة التصديق لتوقيع المستندات للأشخاص الطبيعيين التابعة لشركة مصدر التكنولوجيا: هيئة تابعة تصدر شهادات توقيع المستندات للأشخاص الطبيعيين مثل المواطنين والموظفين.
- هيئة التصديق لتوقيع المستندات للأشخاص الاعتباريين التابعة لشركة مصدر التكنولوجيا: هيئة تابعة تصدر شهادات توقيع المستندات للأشخاص الاعتباريين من الجهات الحكومية وغير الحكومية.
- هيئة التصديق للختم الوقتي التابعة لشركة مصدر التكنولوجيا: هيئة تابعة تصدر شهادات هيئة ختم الوقتي TSA المخصصة لتوقيع المستندات وتوقيع البرمجيات.

تُعد حالات الاستخدام المذكورة أعلاه من العوامل الأساسية الممكنة للتحول الرقمي لأنها تمثل حجر الأساس في تأمين المعاملات الإلكترونية. ويُسهم دعم هذه الحالات ضمن نموذج ثقة موحد بضمان حكومي في تسهيل الاعتماد وتمكين التوافقية وتعزيز ثقة المستخدم.

يتفاعل مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا (TS PKI GB) بشكل وثيق مع اللجنة العليا لإدارة التوقيع الإلكتروني التابعة للشركة العامة للاتصالات والمعلوماتية (ITPC PMA) لضمان التوافق مع بيان ممارسة الشهادات (CPS) هذا فيما يتعلق بإصدار الشهادات وتشغيل هيئات التصديق التابعة لشركة مصدر التكنولوجيا.

1.1.1.مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا (TS PKI GB)

يُشار إلى مجلس الحوكمة المسؤول عن إدارة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا (بما في ذلك هيئة التصديق لتوقيع البرمجيات) باسم مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا .(TS PKI GB) ويضم هذا المجلس الوظائف الأساسية اللازمة مثل السياسات والأمن والامتثال والشؤون القانونية بهدف تقديم التوجيه الاستراتيجي والإشراف المستمر على عمليات البنية التحتية للمفاتيح العامة الخاصة بشركة مصدر التكنولوجيا.

ويتولى مجلس TS PKI GB بشكل خاص المسؤوليات التالية:

- وضع استراتيجية البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا والمحافظة عليها.
- تحديد خدمات البنية التحتية للمفاتيح العامة والموافقة على نموذج تقديمها.
- وضع سياسات وممارسات البنية التحتية للمفاتيح العامة والمحافظة عليها.
- تنفيذ أنشطة إشراف دورية على فريق عمليات البنية التحتية للمفاتيح العامة.
- الموافقة على ميزانية البنية التحتية للمفاتيح العامة واتخاذ القرارات التجارية الرئيسية.
- الموافقة على التغييرات الرئيسية في بنية البنية التحتية للمفاتيح العامة.
- الموافقة على مراسيم المفاتيح وتعيين المدققين الداخليين أو الخارجيين حسب الحاجة.
- التدخل في الحوادث الكبرى واتخاذ القرارات اللازمة.
- قيادة حل النزاعات الناشئة عن أو المرتبطة بأنشطة البنية التحتية للمفاتيح العامة.
- تقييم الحوادث التي لا يلتزم فيها الموظفون الرئيسيون في البنية التحتية للمفاتيح العامة بالإجراءات الأمنية أو التشغيلية بما في ذلك الجوانب الأخلاقية.

1.2.اسم الوثيقة وتحديدها

يحمل هذا المستند عنوان "بيان ممارسة الشهادات لهيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا" ويُعرَّف بواسطة المعرّف الكائني OID 2.16.368.1.2.1.1 ويُشار إليه في الوثائق ذات الصلة بالرمز[TS CS CA CPS] .

تُدرج هيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا المعرف الكائني المذكور أعلاه في امتداد سياسة الشهادات (CP) ضمن الشهادات التي تُصدرها للدلالة على التزامها بالمتطلبات الحالية.

1.3.المشاركون في البنية التحتية للمفاتيح العامة

1.3.1.هيئات التصديق

تعود ملكية وتشغيل هيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا (ويُشار إليها لاحقاً بـ الهيئة) إلى شركة مصدر التكنولوجيا من خلال مواقعها داخل العراق. وقد تمت الموافقة على هذه الهيئة من قبل الشركة العامة للاتصالات والمعلوماتية (ITPC) وجرى توقيعها من قبل هيئة التصديق الجذرية العراقية لتوقيع البرمجيات كما هو موضح في الشكل 1 (البند 1.1).

تُقدّم هذه الهيئة خدمات التصديق التالية:

- خدمة إصدار الشهادات — تصدر شهادات الكيانات النهائية استناداً إلى التحقق الذي تجريه سلطات التسجيل
- خدمة النشر — تنشر شهادات OCSP وقوائم إلغاء الشهادات وشهادات هيئة التصديق وتجعلها متاحة للأطراف المعتمدة. كما تُتيح هذه الخدمة أي معلومات علنية تتعلق بالسياسات والممارسات للمشتركين والأطراف المعتمدة
- خدمة إدارة الإلغاء — تعالج الطلبات والتقارير المتعلقة بإلغاء الشهادات من أجل تحديد الإجراء المناسب الواجب اتخاذه. وتتوفر نتائج هذه الخدمة من خلال خدمة التحقق من حالة الشهادة

- خدمة التحقق من حالة الشهادة — توفر معلومات حول حالة صلاحية الشهادة للأطراف المعتمدة استناداً إلى قوائم إلغاء الشهادات وخدمة مستجيب OCSP. وتعكس معلومات الحالة دائماً الوضع الحالي للشهادات الصادرة عن هذه الهيئة.

1.3.2.سلطات التسجيل

تُعد سلطة التسجيل (RA) الجهة التي تتولى عملية التعرف والتحقق من هوية طالبي الشهادات للكيانات النهائية وتبدأ أو تُحوّل طلبات الإلغاء كما تُوافق على طلبات إصدار وتجديد الشهادات نيابةً عن هيئة التصديق.

تُشغّل شركة مصدر التكنولوجيا وظيفة سلطة التسجيل الخاصة بها ولا تعتمد على جهات خارجية مفوضة للقيام بوظائف سلطة التسجيل. وتعالج هذه الوظيفة بشكل أساسي طلبات شهادات توقيع البرمجيات التي تُصدر للمنظمات القانونية. تندرج وظيفة سلطة التسجيل ضمن هيكل عمليات البنية التحتية للمفاتيح العامة وتتحمل مسؤولية التحقق من الهوية وإدارة طلبات الشهادات للجهات الحكومية وغير الحكومية.

تشمل مهام سلطة التسجيل لدى شركة مصدر التكنولوجيا على سبيل المثال لا الحصر:

- المصادقة على طلبات الشهادات وطلبات الإلغاء أو رفضها.
- تحديد هوية المشتركين وفقاً لاتفاقيات التسمية المحددة في هذا البيان لضمان أن يُعرَّف كل مشترك بشكل فريد وغير غامض.
- معالجة طلبات إصدار الشهادات وطلبات الإلغاء مع هذه الهيئة استناداً إلى الطلبات المُحققة والمُعتمدة.
- إنشاء وصيانة سجل تدقيق يُوثّق جميع الأحداث المهمة المتعلقة بعمليات سلطة التسجيل.
- توفير وصول انتقائي إلى سجلات سجل التدقيق حسب ما هو محدد في هذا البيان.
- تنفيذ الضوابط التشغيلية الأخرى حسب ما هو منصوص عليه في هذا البيان.
- معالجة المعلومات وتخزينها وفقاً للمتطلبات المحددة في هذا البيان وخصوصاً في القسم 5.

1.3.3.المشتركون

يتمثل المشتركون في هيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا في الكيانات القانونية العراقية بما في ذلك الجهات الحكومية وغير الحكومية في العراق وحتى شركة مصدر التكنولوجيا نفسهاوجميعهم خاضعون للولاية القضائية العراقية. ولكل شهادة تُصدر يُوقّع المشترك أو يصدّق على شروط واحكام استخدام المشترك لإقرار الشروط والأحكام المحددة من قبل شركة مصدر التكنولوجيا.

1.3.4. الأطراف المعتمدة

يجب على الأطراف المعتمدة الرجوع دائماً إلى خدمات التحقق من صلاحية الشهادات الصادرة عن شركة مصدر التكنولوجيا (أي قوائم إلغاء الشهادات وخدمة مستجيب OCSP) قبل الاعتماد على المعلومات الواردة في الشهادة المعنية.

1.3.5.المشاركون الآخرون

تشمل الجهات الأخرى المشاركة ما يلي:

- اللجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية (ITPC PMA) وهي الجهة الرقابية المسؤولة عن الإشراف على كامل نشاط مقدم خدمات الثقة المرخص (أي شركة مصدر التكنولوجيا). وقد وُضحت الأدوار والمسؤوليات الخاصة بـ PMA في سياسة الشهادات وبيان ممارسة الشهادات لهيئات التصديق الجذرية لـ ITPC والمنشورة على الموقع: https://pki.itpc.gov.iq
- مدققو WebTrust المستقلون المؤهلون الذين يتحققون من المتطلبات المحددة في البند 8.2.

1.4.استخدام الشهادات

1.4.1.الاستخدامات المناسبة للشهادات

يمكن استخدام الشهادات الصادرة عن هذه الهيئة في الحالات التالية:

1. شهادات للأشخاص الاعتباريين (الجهات الحكومية وغير الحكومية العراقية):
   أ) شهادات توقيع البرمجيات: تُستخدم لتوقيع مكتبات البرمجيات وملفات exe وملفات msi وغيرها
2. شهادة مستجيب — OCSP تُستخدم لتوقيع استجابات بروتوكول التحقق من حالة الشهادات عبر الإنترنت (OCSP)المتعلقة بالشهادات الصادرة عن هيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا

1.4.2.الاستخدامات المحظورة للشهادات

يُصرح للمشتركين باستخدام شهاداتهم للأغراض المحددة في البند 1.4.1 من هذا البيان فقط. ويُحظر تماماً استخدام الشهادات لأي أغراض أخرى.

1.5.إدارة السياسات

1.5.1.الجهة المسؤولة عن إدارة الوثيقة

يُدار هذا البيان من قبل مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا (TS PKI GB) وفقاً لنموذج التشغيل الخاص به واستناداً إلى تفاعل مع اللجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية (ITPC PMA) حسب الحاجة.

1.5.2.جهة الاتصال

يُوجّه تقديم أي طلب معلومات أو استفسار متعلق بهذا البيان إلى:

مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا

شركة مصدر التكنولوجيا

بغداد — شارع الأربع شوارع — بالقرب من إعدادية المامون

البريد الإلكتروني: info@techsource.iq

رقم الهاتف: 784 136 1693 (964+)

يقبل مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا التعليقات المتعلقة بهذا البيان فقط عند توجيهها إلى جهة الاتصال أعلاه.

تقرير مشكلة الشهادة

تُوفر شركة مصدر التكنولوجيا قدرة داخلية دائمة على مدار الساعة طوال أيام الأسبوع للاستجابة لأي طلبات إلغاء ذات أولوية عالية أو تقارير عن مشاكل في الشهادات. وتتوفر تعليمات إلغاء الشهادات والإبلاغ عن مشاكل الشهادات في صفحة مخصصة ضمن المستودع العام على الرابط التالي:

https://pki.techsource.iq/repository/Certificate_Problem_Report.html

يجوز للمشتركين والأطراف المعتمدة وموردي برمجيات التطبيقات وأي جهات أخرى الإبلاغ عن حالات الاشتباه باختراق المفتاح الخاص أو سوء استخدام الشهادة أو أنواع أخرى من الاحتيال أو سوء الاستخدام أو السلوك غير الملائم أو أي مسألة أخرى تتعلق بالشهادات عبر البريد الإلكتروني التالي: certificate.problem@techsource.iq.

ستقوم شركة مصدر التكنولوجيا بالتحقق من صحة طلب الإلغاء والتحقيق فيه قبل اتخاذ أي إجراء وفقاً للبند 4.9

إذا رأت شركة مصدر التكنولوجيا أن الأمر يستدعي ذلك فقد تُحوّل تقارير الإلغاء إلى الجهات الأمنية المختصة.

1.5.3.الشخص المسؤول عن تحديد مدى ملاءمة هذا البيان للسياسة

استناداً إلى نتائج تدقيقات الامتثال وتوصياتها يُحدد مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا مدى ملاءمة هذا البيان وقابليته للتطبيق. وقد أُعتمد هذا البيان من قبل مجلس TS PKI GB وكذلك من قبل اللجنة العليا لإدارة التوقيع الإلكتروني PMA لأنه يجب أن يمتثل في نهاية المطاف لأحكام سياسة الشهادات الخاصة بمقدم خدمات الثقة (TSP CP).

1.5.4. إجراءات اعتماد بيان ممارسة الشهادات

يعتمد مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا بالتعاون مع اللجنة العليا لإدارة التوقيع الإلكترونيPMA رسمياً أي إصدار جديد من بيان ممارسة الشهادات.

يتولى موظفون متخصصون في سياسات البنية التحتية للمفاتيح العامة من مجلس TS PKI GB مراجعة هذا البيان منذ مسودته الأولى وأي تعديلات لاحقة لضمان التوافق مع أفضل الممارسات المطبقة ومع سياسة الشهادات الخاصة بمقدم خدمات الثقةTSP CP وذلك قبل اعتماده من قبل مجلس TS PKI GB. وقد تتخذ التعديلات شكل مستند يحتوي على نسخة معدلة من البيان أو إشعار تحديث. وتُوثق أي تغييرات تُجرى على هذا البيان ضمن جدول المراجعات.

يُقدَّم الإصدار الجديد من هذا البيان بعد ذلك إلى اللجنة العليا لإدارة التوقيع الإلكتروني PMA لاعتماده النهائي لأنه يجب أن يتوافق مع أحكام سياسة الشهادات الخاصة بمقدم خدمات الثقة TSP CP.

ولضمان المصداقية وتعزيز الثقة في هذا البيان وتحقيق التوافق مع متطلبات الاعتماد والمتطلبات القانونية يقوم مجلس TS PKI GBبمراجعة هذا البيان مرة واحدة على الأقل سنوياً وقد يجري التعديلات أو التحديثات على السياسات حسب ما يراه مناسباً أو كما تفرضه الظروف الأخرى.

وقبل أن يدخل الإصدار المحدث من البيان حيز التنفيذ يُعلن عنه في المستودع العام على الرابط التالي: https://pki.techsource.iq

وبمجرد نشره يُصبح الإصدار المحدث ملزماً لجميع المشتركين بما في ذلك المشتركين والأطراف المعتمدة على الشهادات التي صدرت وفقاً لإصدار سابق من هذا البيان.

1.6.التعاريف والاختصارات والمراجع

1.6.1.التعاريف

المتقدم: الشخص الطبيعي أو الكيان القانوني الذي يتقدّم بطلب إصدار شهادة أو تجديدها. وعند إصدار الشهادة يُشار إلى هذا الكيان باسم "المشترك". وفي سياق هذا البيان تصدر هيئة التصديق هذه الشهادات فقط للكيانات القانونية.

ممثل المتقدم: شخص طبيعي أو ممثل بشري يكون إما هو المتقدم نفسه أو موظفاً لدى المتقدم أو وكيلاً مفوضاً صراحةً لتمثيله ويقوم بما يلي: (1) يوقّع ويقدّم أو يوافق على طلب الشهادة نيابةً عن المتقدم أو (2) يوقّع ويقدّم شروط واحكام استخدام المشترك نيابةً عن المتقدم (3)يقر بشروط الاستخدام نيابةً عن المتقدم عندما يكون المتقدم تابعاً لهيئة التصديق أو هو هيئة التصديق نفسها. وفي سياق هذا البيان يكون ممثل المتقدم مسؤولاً عن تقديم طلبات الشهادات وطلبات إلغاء الشهادات نيابةً عن المتقدم. ويُستخدم مصطلحا "ممثل المتقدم" و"مقدّم الطلب" بالتبادل.

منظمة مكافحة البرمجيات الخبيثة: كيان يحتفظ بمعلومات عن البرمجيات المشتبه بها أو يطوّر برامج تستخدم للكشف عن البرمجيات الخبيثة أو منعها أو إزالتها.

مزود برامج التطبيقات البرمجية: مزوّد برمجيات أو تطبيقات أخرى تعتمد على الشهادات وتعرض أو تستخدم شهادات توقيع البرمجيات وتُدرج شهادات الجذر وتتبع هذه المتطلبات كلياً أو جزئياً ضمن شروطها للمشاركة في برنامج تخزين الشهادات الجذرية.

فترة التدقيق: في حالة تدقيق يغطي فترة زمنية محددة تُعرّف فترة التدقيق بأنها الفترة الممتدة من اليوم الأول (البداية) حتى اليوم الأخير (النهاية) من العمليات التي يغطيها المدققون ضمن نطاق عملهم. (ولا تعني هذه الفترة مدة تواجد المدققين في مقر هيئة التصديق)

تقرير التدقيق: تقرير صادر عن مدقق مؤهل يبيّن فيه رأيه بشأن مدى التزام العمليات والضوابط لدى الكيان المعني بالأحكام الإلزامية لهذه المتطلبات.

المتطلبات الأساسية: وهي المتطلبات الأساسية لإصدار وإدارة شهادات توقيع الشفرات البرمجية الموثوقة عاماً، والمحررة من قبل منتدى سلطات التصديق ومتصفحات الشبكة العالمية.

زوج مفاتيح هيئة التصديق: زوج مفاتيح يتضمن مفتاحاً عاماً يظهر كمعلومة المفتاح العام للموضوع في شهادة جذرية واحدة أو أكثر و/أو شهادة هيئة تصديق تابعة.

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

بيانات الشهادة: البيانات المتعلقة بطلبات الشهادات سواء حَصِلَ عليها من المتقدم أو بوسائل أخرى والتي تكون بحوزة هيئة التصديق أو ضمن نطاق سيطرتها أو يمكنها الوصول إليها

عملية إدارة الشهادات: العمليات والممارسات والإجراءات المرتبطة باستخدام المفاتيح والبرمجيات والمعدات والتي من خلالها تتحقق هيئة التصديق من بيانات الشهادة وتُصدر الشهادات وتحافظ على المستودع وتلغي الشهادات

سياسة الشهادة: مجموعة من القواعد التي تُحدد مدى قابلية تطبيق شهادة مُسمّاة على مجتمع معين أو ضمن تنفيذ للبنية التحتية للمفاتيح العامة يتمتع بمتطلبات أمنية مشتركة.

معرّف سياسة الشهادة: كما هو موضح في القسم (7.1.6) من المتطلبات الأساسية.

تقرير مشكلة الشهادة: شكوى تتعلق باختراق محتمل للمفتاح أو إساءة استخدام الشهادة أو أنواع أخرى من الاحتيال أو سوء الاستخدام أو السلوك غير المناسب المرتبط بالشهادات.

قائمة إلغاء الشهادات: قائمة محدثة زمنياً تحتوي على الشهادات الملغاة تُنشئ وتوقيعها رقمياً من قبل هيئة التصديق التي أصدرت الشهادات.

هيئة التصديق: منظمة خاضعة لهذه المتطلبات مسؤولة عن شهادة توقيع البرمجيات وتشرف على إنشاء الشهادات وإصدارها وإلغائها وإدارتها وإذا كانت هيئة التصديق هي نفسها الجذرية فإن الإشارة إليها تعني أيضاً الهيئة الجذرية.

مستفيدو الشهادات: جميع مزودي برامج التطبيقات الذين دخلوا في عقد مع هيئة التصديق أو هيئتها الجذرية لتوزيع شهادة الجذر ضمن البرمجيات الموزعة وجميع الأطراف المعتمدة الذين يعتمدون بشكل منطقي على تلك الشهادة طالما أن توقيع الشيفرة المرتبط بها لا يزال صالحاً.

بيان ممارسة الشهادات: أحد الوثائق التي تُشكل إطار الحوكمة الذي تُنشأ وتُصدر وتُدار وتُستخدم فيه الشهادات.

ملف مواصفات الشهادة: مجموعة من الوثائق أو الملفات التي تُحدد متطلبات محتوى الشهادة وامتداداتها وفقاً للبند 7 من المتطلبات الأساسية مثلما ورد في القسم 7 من هذا البيان.

البرمجيات: مجموعة متصلة من البتات وُقِعَ عليها أو يمكن توقيعها رقمياً باستخدام مفتاح خاص مرتبط بشهادة توقيع البرمجيات.

توقيع البرمجيات: توقيع يرتبط منطقياً ببرامج موقعة.

شهادة توقيع البرمجيات: شهادة رقمية تصدرها هيئة التصديق وتحتوي على امتداد توقيع البرمجيات.

إقرار الهوية: وثيقة خطية تتضمن ما يلي هوية الشخص الذي يجري التحقق وتوقيع المتقدم ورقم تعريفي فريد من وثيقة تعريف تخص المتقدم وتاريخ التحقق وتوقيع الشخص الذي أجرى التحقق.

التحكم: امتلاك الصلاحية بشكل مباشر أو غير مباشر لـ: توجيه إدارة الكيان أو موظفيه أو موارده المالية أو خططه أو التحكم في انتخاب أغلبية أعضاء مجلس الإدارة أو التصويت بنسبة الأسهم المطلوبة لتحقيق مفهوم التحكم وفقاً لقوانين الولاية القضائية للكيان ولكن لا تقل هذه النسبة في جميع الأحوال عن 10 بالمئة.

الدولة: إما عضو في الأمم المتحدة أو منطقة جغرافية معترف بها كدولة ذات سيادة من قبل دولتين على الأقل من الدول الأعضاء في الأمم المتحدة.

الرمز التشفير المحمول: جهاز تشفيري من نوع USB حاصل على شهادة مطابقة لمعيار FIPS 140 المستوى الثاني أو ما يعادله.

مولد الأرقام العشوائية للأغراض التشفيرية: مولد أرقام عشوائية معد للاستخدام ضمن نظام تشفيري.

طرف ثالث مفوض: شخص طبيعي أو كيان قانوني ليس هيئة التصديق ولا تندرج أنشطته ضمن نطاق تدقيقات هيئة التصديق المعنية ولكنه مفوض من قبلها للمساعدة في عملية إدارة الشهادات من خلال تنفيذ أو استيفاء واحد أو أكثر من المتطلبات الواردة في هذا البيان.

تاريخ الانتهاء: التاريخ المشار إليه في الشهادة بعبارة "ليس بعد" والذي يُحدد نهاية فترة صلاحية الشهادة.

كيان حكومي: كيان قانوني تديره الحكومة أو وكالة أو إدارة أو وزارة أو فرع أو جهة مشابهة تابعة لحكومة دولة أو تقسيم سياسي ضمن تلك الدولة مثل ولاية أو محافظة أو مدينة أو مقاطعة.

طلب شهادة عالي المخاطر: طلب تقوم هيئة التصديق بوضع علامة عليه لمزيد من التدقيق استناداً إلى معايير داخلية وقواعد بيانات تحتفظ بها الهيئة وقد يشمل ذلك أسماء معرّضة لخطر التصيد الاحتيالي أو الاستخدام الاحتيالي أو أسماء وردت في طلبات شهادات مرفوضة أو شهادات مُلغاة سابقاً أو أسماء مدرجة ضمن قوائم التصيد الاحتيالي مثل Miller Smilesأو قائمة Google Safe Browsing أو أسماء تحددها هيئة التصديق بناءً على معاييرها الخاصة لتخفيف المخاطر.

وحدة حماية الأجهزة الأمنية: وهي جهاز مصمم لتقديم وظائف تشفيرية مخصصة لغرض الحفظ الآمن للمفاتيح الخاصة.

هيئة التصديق المصدِرة: الهيئة التي أصدرت الشهادة المعنية وقد تكون هذه الهيئة إما هيئة تصديق جذرية أو هيئة تصديق تابعة.

اختراق المفتاح: يُعد المفتاح الخاص مخترقاً إذا كُشفَ عن قيمته لشخص غير مصرح له أو إذا تمكن شخص غير مصرح له من الوصول إليه.

برنامج إنشاء المفتاح: خطة موثقة للإجراءات المعتمدة في إنشاء زوج مفاتيح هيئة التصديق.

زوج المفاتيح: المفتاح الخاص والمفتاح العام المرتبط به.

الكيان القانوني: جمعية أو شركة أو شراكة أو ملكية فردية أو صندوق استئماني أو جهة حكومية أو أي كيان آخر يتمتع بصفة قانونية ضمن النظام القانوني لدولة ما.

معرف الكائن: معرف أبجدي رقمي أو رقمي فريد مسجّل وفقاً للمعيار المعتمد من قبل المنظمة الدولية للمعايير لعنصر أو فئة معينة من العناصر.

الوجود القانوني: تتمتع المنظمة الخاصة أو الجهة الحكومية أو الكيان التجاري بوجود قانوني إذا كان قد تم تأسيسه بشكل أصولي ولم يتم إنهاؤه أو حله أو التخلي عنه بأي شكل من الأشكال.

شهادة توقيع البرمجيات (غير معززة التحقق): مصطلح يُستخدم للإشارة إلى المتطلبات التي تنطبق على شهادات توقيع البرمجيات التي لا يشترط فيها استيفاء معايير التحقق المعزز.

مُستجيب بروتوكول الحالة: خادم متصل عبر الإنترنت يعمل تحت سلطة هيئة التصديق ومرتبط بمستودعها لمعالجة طلبات حالة الشهادات انظر أيضاً بروتوكول حالة الشهادات عبر الإنترنت.

بروتوكول حالة الشهادات عبر الإنترنت: بروتوكول تحقق من الشهادات عبر الإنترنت يتيح لتطبيقات الأطراف المعتمدة تحديد حالة شهادة معينة انظر أيضاً مُستجيب بروتوكول الحالة.

المفتاح الخاص: المفتاح ضمن زوج المفاتيح الذي يحتفظ به صاحب الزوج بشكل سري ويُستخدم لإنشاء التواقيع الرقمية أو لفك تشفير السجلات أو الملفات الإلكترونية التي شَفرت باستخدام المفتاح العام المقابل.

المفتاح العام: المفتاح ضمن زوج المفاتيح الذي يمكن لصاحب المفتاح الخاص المقابل نشره علناً ويُستخدم من قبل الطرف المعتمد للتحقق من التواقيع الرقمية التي أُنشئَ باستخدام المفتاح الخاص المقابل أو لتشفير الرسائل بحيث لا يمكن فك تشفيرها إلا باستخدام المفتاح الخاص المقابل.

البنية التحتية للمفتايح العامة: مجموعة من العتاد والبرمجيات والأشخاص والإجراءات والقواعد والسياسات والالتزامات المستخدمة لتيسير إنشاء الشهادات وإصدارها وإدارتها واستخدامها بطريقة موثوقة بالاعتماد على التشفير باستخدام المفاتيح العامة.

الشهادة المعتمدة علنًا: شهادة تُعتبر موثوقة لكون شهادة الجذر المقابلة لها موزعة كنقطة ثقة ضمن برمجيات التطبيقات المتاحة على نطاق واسع.

المدقق المؤهل: شخص طبيعي أو كيان قانوني يستوفي المتطلبات المنصوص عليها في القسم 8.2.

القيمة العشوائية: قيمة تُحددها هيئة التصديق للمتقدم تحتوي على ما لا يقل عن 112 بت من العشوائية.

اسم النطاق المسجّل: اسم نطاق سُجِل لدى مسجّل أسماء النطاقات.

هيئة التسجيل: أي كيان قانوني مسؤول عن التحقق من هوية الأشخاص الخاضعين للشهادة ولكن ليس هيئة تصديق وبالتالي لا يقوم بالتوقيع أو إصدار الشهادات وقد تساهم هيئة التسجيل في عملية طلب الشهادة أو عملية الإلغاء أو كلتيهما وعندما يُستخدم مصطلح هيئة التسجيل لوصف دور أو وظيفة فإنه لا يشير بالضرورة إلى كيان منفصل بل يمكن أن يكون جزءاً من هيئة التصديق وفي سياق هذا البيان فإن وظيفة هيئة التسجيل تُدار من قبل شركة مصدر التكنولوجيا.

مُعرّف التسجيل: وهو الرمز الفريد المخصص لمقدم الطلب من قبل جهة التأسيس أو التسجيل ضمن الولاية القضائية التي تم فيها تسجيل أو تأسيس الكيان.

مصدر بيانات موثوق: مستند تعريف أو مصدر بيانات يُستخدم للتحقق من معلومات هوية الشخص الخاضع للشهادة ويُعترف به بشكل عام بين المؤسسات التجارية والحكومات كمصدر موثوق وقد أُنشئ من قبل طرف ثالث لغرض غير إصدار الشهادة لصالح المتقدم وفي سياق هذا البيان فإن الجهة العراقية المعنية بتسجيل الشركات تُعد المصدر الموثوق للكيانات غير الحكومية في العراق أما الجريدة الرسمية العراقية فهي المصدر الموثوق للكيانات الحكومية

وسيلة اتصال موثوقة: وسيلة اتصال مثل عنوان بريد أو رقم هاتف أو بريد إلكتروني تم التحقق منه باستخدام مصدر غير ممثل المتقدم

الطرف المعتمد: أي شخص طبيعي أو كيان قانوني يعتمد على شهادة صالحة ولا يُعتبر مزود برامج التطبيقات طرفاً معتمداً عندما تكتفي برمجياته بعرض معلومات تتعلق بالشهادة

المستودع: قاعدة بيانات إلكترونية تحتوي على وثائق حوكمة البنية التحتية للمفاتيح العامة المُعلنة للعامة مثل سياسات الشهادات وبيانات ممارسة الشهادات إضافة إلى معلومات حالة الشهادات إما على شكل قائمة إلغاء الشهادات أو استجابة بروتوكول الحالة

رمز الطلب: قيمة تُوَلد وفق طريقة تحددها هيئة التصديق وتربط بين إثبات التحكم وطلب الشهادة وتشمل الأمثلة على رموز الطلب على سبيل المثال لا الحصر تجزئة المفتاح العام أو تجزئة معلومات المفتاح العام لموضوع الشهادة أو تجزئة طلب الشهادة بصيغةPKCS#10

هيئة التصديق الجذرية: هيئة التصديق في المستوى الأعلى التي تُوزع شهادتها الجذرية من قبل مزودي برامج التطبيقات والتي تُصدر شهادات لهيئات التصديق التابعة

الشهادة الجذرية: شهادة ذاتية التوقيع تُصدرها هيئة التصديق الجذرية للتعريف بنفسها وتيسير التحقق من الشهادات المُصدرة لهيئات التصديق التابعة لها.

التوقيع: ملف بيانات إلكترونية مشفرة يتم إرفاقه ببيانات إلكترونية أخرى أو يرتبط بها منطقياً، ويقوم بـ: (1) تحديد هوية الموقع على البيانات الإلكترونية والارتباط به بشكل فريد، (2) يتم إنشاؤه باستخدام وسائل تقع تحت سيطرة الموقع وحده، (3) يرتبط بالبيانات بطريقة تسمح بكشف أي تغييرات لاحقة تُجرى عليها.

الموضوع: الكيان أو المؤسسة المعرفة ضمن حقل "الموضوع" في الشهادة

معلومات هوية الموضوع: المعلومات التي تُعرّف الشخص أو الكيان المُشار إليه في الشهادة ولا تشمل معلومات هوية الموضوع أسماء النطاق المدرجة ضمن امتداد subjectAltName أو الحقل commonName للموضوع

هيئة التصديق التابعة: هيئة تصديق يُوقيع شهادتها من قبل هيئة التصديق الجذرية أو من قبل هيئة تصديق تابعة أخرى

المشترك: كيان قانوني تصدر له الشهادة ويكون ملزماً قانونياً بموجب شروط واحكام استخدام المشترك أو شروط الاستخدام.

البرمجيات المشبوهة: هي البرمجيات التي تحتوي على وظائف خبيثة أو ثغرات أمنية جسيمة، بما في ذلك برامج التجسس والبرمجيات الضارة وغيرها من البرمجيات التي تُثبّت دون موافقة المستخدم أو تقاوم عملية إزالتها، أو البرمجيات التي تؤدي إلى اختراق أمن المستخدم أو البرمجيات التي يمكن استغلالها بطرق غير مقصودة من قبل مصمميها لزعزعة موثوقية منصات العمل التي تعمل عليها.

هجوم الاستحواذ: هو هجوم يتم من خلاله اختراق المفتاح الخاص المرتبط بشهادة توقيع البرمجيات عن طريق الاحتيال، أو السرقة، أو فعل خبيث متعمد من قبل وكيل الجهة المخولة، أو أي سلوك غير قانوني آخر.

شروط واحكام استخدام المشترك: اتفاق يُبرم بين هيئة التصديق والمتقدم أو المشترك يحدد حقوق ومسؤوليات الطرفين.

شهادة هيئة التصديق التابعة ذات القيود التقنية: شهادة تابعة تستخدم مزيجاً من إعدادات استخدام المفتاح الممتد وإعدادات قيود الاسم لتحديد نطاق إصدار الشهادات التي يمكن أن تُصدرها هيئة التصديق التابعة سواء كانت شهادات للمشتركين أو لشهادات تابعة إضافية.

شروط الاستخدام: أحكام تتعلق بحفظ الشهادة واستخدامها بشكل مقبول وفقاً للمتطلبات الأساسية وذلك عندما يكون المتقدم أو المشترك جهة تابعة لهيئة التصديق أو هو نفسه هيئة التصديق.

الشهادة الصالحة: شهادة تجتاز إجراء التحقق المحدد في المعيار RFC 5280 .

المتخصصون في التحقق: أشخاص يؤدون مهام التحقق من المعلومات كما هو محدد في هذه المتطلبات.

فترة الصلاحية: الفترة الزمنية المحتسبة 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
CP	سياسة الشهادات
CPS	بيان ممارسة الشهادات
CRL	قائمة إلغاء الشهادات
CSR	طلب توقيع الشهادة
CV	السيرة الذاتية
DBA	ممارسة الأعمال تحت اسم تجاري
DN	الاسم المميز
DNS	نظام أسم المجال
EID	بطاقة الهوية الإلكترونية
EIDAS	خدمات التعريف والمصادقة والثقة الإلكترونية
ETSI	المعهد الأوروبي لمعايير الاتصالات
FIPS	معايير المعالجة الفدرالية للمعلومات
HTTP	بروتوكول نقل النص الفائق
HSM	جهاز توليد المفاتيح الشفرية
ICANN	المؤسسة المسؤولة عن تخصيص أسماء الإنترنت والأرقام

IETF	فرقة عمل هندسة الإنترنت
IPSEC	أمن بروتوكول الإنترنت
ISO	المنظمة الدولية للمعايير
IT	تكنولوجيا المعلومات
ITPC	الشركة العامة للاتصالات والمعلوماتية
OCSP	بروتوكول حالة الشهادة عبر الإنترنت
OID	معرف الكائن
PIN	الرقم السري الشخصي
PKCS#1	معايير التشفير بالمفتاح العام – رقم 1
PKCS#7	صيغة الرسائل المشفرة
PKCS#10	مواصفة طلب الشهادة
PKI	البنية التحتية للمفتايح العامة
PMA	اللجنة العليا لإدارة التوقيع الإلكتروني
RA	سلطة التسجيل
RSA	ريفست–شمير–أدلمن (مخترعو خوارزميةRS)
RTO	مدة استعادة الخدمة
SSL	طبقة المنافذ الآمنة
TLD	نطاق المستوى الأعلى
TSA	هيئة ختم الوقتي
TS	شركة مصدر التكنولوجيا
TLS	أمن طبقة النقل

TSP	مزود خدمات الثقة
UPS	مزود طاقة غير منقطع
URI	معرف الموارد الموحد
URL	محدد الموارد الموحد

1.6.3.المراجع

- المعيار :X.509 معيار الاتحاد الدولي للاتصالات (ITU-T) الخاص بالشهادات الرقمية.
- المعيار :RFC3647 إطار سياسات الشهادات وممارسات التصديق للبنية التحتية للمفاتيح العامة (X.509) عبر شبكة الإنترنت.
- المعيار :RFC5280 مواصفات شهادات البنية التحتية للمفاتيح العامة (X.509) وقوائم إلغاء الشهادات (CRL) عبر شبكة الإنترنت.
- مبادئ ومعايير (ويب-ترست) الصادرة عن المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) والمعهد الكندي للمحاسبين المعتمدين (CPA Canada) لسلطات التصديق – المتطلبات الأساسية لتوقيع البرمجيات.
- مبادئ ومعايير (ويب-ترست) الصادرة عن (AICPA/CPA Canada) لسلطات التصديق.
- مبادئ ومعايير (ويب-ترست) الصادرة عن (AICPA/CPA Canada) لسلطات التصديق – أمن الشبكات.
- متطلبات أمن الشبكات وأنظمة الشهادات الصادرة عن منتدى سلطات التصديق ومتصفحات الشبكة العالمية.
- المتطلبات الأساسية لإصدار وإدارة شهادات توقيع البرمجيات الموثوقة عاماً الصادرة عن منتدى سلطات التصديق ومتصفحات الشبكة العالمية.

2. المسؤوليات المتعلقة بالنشر والمستودعات

2.1.المستودعات

تحتفظ شركة مصدر التكنولوجيا بمستودع إلكتروني متاح على مدار الساعة (24 × 7) ويمكن الوصول إليه من خلال الرابط: https://pki.techsource.iq

وتتحمل 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 المعتمدوبيان إفصاح البنية التحتية للمفتاح العامة وسياسة وبيان ممارسة هيئة الختم الوقتي وبيان إفصاح هيئة الختم الوقتي.
- شهادات الهيئة الجذرية الذاتية التوقيع الصالحة بالإضافة إلى شهادات هيئات التصديق التابعة التابعة لشركة مصدر التكنولوجيا وشهاداتOCSP وقوائم إلغاء الشهادات (CRLs) الصادرة عن الهيئات الفرعية.
- شهادات وحدات ختم الزمني (TSU).
- تقارير التدقيق.

2.2.نشر معلومات الشهادات

تُعد شركة مصدر التكنولوجيا الجهة المسؤولة عن توفير المعلومات اللازمة للنشر كما هو موضح في القسم 2.1 من هذا المستند.

تنشر شركة مصدر التكنولوجيا معلومات حالة صلاحية الشهادات على فترات متكررةوفقاً لما هو محدد في بيان ممارسة الشهادات هذا(CPS) .

تُوفَّر خدمة معلومات حالة صلاحية الشهادات على مدار الساعة من خلال ما يلي:

- نشر قوائم إلغاء الشهادات (CRLs) التي تتضمن أي تغييرات طرأت منذ نشر قائمة الإلغاء السابقة على فترات منتظمة. وتُضيف هيئة التصديق لشهادات توقيع البرمجيات (TS Code Signing CA) رابطاً (URL) إلى قائمة الإلغاء ذات الصلة في شهادات المشتركين كجزء من امتداد نقطة توزيع الشهادة (CDP) متى ما كان هذا الامتداد موجوداً.
- مستجيب OCSP متوافق مع المواصفة .RFC 6960 ويُضَمن عنوان URL الخاص بخدمة OCSP في امتداد معلومات الوصول للسلطة (AIA) لشهادات المشتركين التي تصدرها هذه الهيئة.

2.3.توقيت أو تكرار النشر

يُجري مجلس حوكمة البنية التحتية للمفتاح العامة لشركة مصدر التكنولوجيا (TS PKI GB) مراجعة لبيان ممارسة الشهادات (CPS) هذا مرة واحدة على الأقل سنوياً ويُجري التعديلات المناسبة لضمان أن تبقى عمليات هيئات التصديق التابعة متوافقة تماماً مع المتطلبات المذكورة في القسم 1 من هذا البيان.

تُنشر النسخ المعدّلة من بيان ممارسة الشهادات والاتفاقيات (اتفاقيات المشترك والطرف المعتمد) خلال مدة لا تتجاوز خمسة أيام من موافقة مجلس الحوكمة.

2.3.1.شهادات هيئات التصديق

تُنشر شهادات هيئة التصديق لتوقيع البرمجيات وشهادات OCSP في المستودع العام فور إصدارها وتبقى منشورة حتى انتهاء صلاحيتها أو استبدالها بشهادات جديدة.

2.3.2.قوائم إلغاء الشهادات(CRLs)

تقوم هيئة التصديق لتوقيع البرمجيات في مصدر التكنولوجيا بإنشاء ونشر قوائم إلغاء الشهادات على النحو التالي:

- تُوَلد قائمة إلغاء جديدة كل 24 ساعة حتى في حال عدم حدوث أي تغييرات منذ إصدار القائمة السابقة؛
- تُحدد صلاحية كل قائمة إلغاء بـ 26 ساعة.

2.4.ضوابط الوصول إلى المستودعات

تُتاح المعلومات المنشورة في المستودع العام لشركة مصدر التكنولوجيا للاطلاع العام ويُضمن الوصول المفتوح وغير المقيّد لقراءتها.

وتطبق 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

تتوافق أسماء الموضوعات في شهادة هيئة التصديق لتوقيع البرمجيات مع معايير الأسماء المميزة .X.500 يتحقق مشغل وظيفة هيئة التسجيل التابعة لاللجنة العليا لإدارة التوقيع الإلكتروني من اسم الموضوع المستخدم في شهادة هيئة التصديق ويصدّقه ويجب أن يكون ذا معنى ولا يجوز إعادة تعيينه لأي جهة أخرى.

تُعرَّف هذه الهيئة في حقل "الجهة المُصدِرة" في شهادات المشتركين كما يلي:

شهادة TS CS CA

CN	TS CS CA G1
O	شركة مصدر التكنولوجيا
الدولة (C)	العراق

تستخدم الشهادات الصادرة عن هذه الهيئة أسماء مميزة (DN) كما ورد في توصية .ITU-T X.500 توضح الجداول التالية بنية DN المتبعة لكل نوع من أنواع الشهادات المدعومة.

شهادات توقيع البرمجيات الصادرة للمشتركين:

CN	الاسم الكامل المسجَّل للمنظمة
O	الاسم القانوني للمنظمة
الدولة (C)	IQ
L (اختياري في حال وجد S والزامي بخلاف ذلك)	اسم المنطقة التي تقع فيها المنظمة
S (اختياري في حال وجد L والزامي بخلاف ذلك)	اسم المحافظة التي تقع فيها المنظمة

شهادة مستجيب OCSP لهيئة TS Code Signing CA:

CN	TS CS CA G1 OCSP
O	شركة مصدر التكنولوجيا
الدولة (C)	العراق

3.1.2.الحاجة إلى أن تكون الأسماء ذات معنى

تُطبق هيئة التصديق لتوقيع البرمجيات سياسة استخدام الأسماء ذات المعنى لتحديد هوية المنظمة في حقل "الموضوع" ضمن الشهادات.

بالنسبة لشهادات توقيع البرمجيات الصادرة للكيانات القانونية: تُعد الأسماء ذات معنى نظراً لأن حقل CN يتضمن تمثيلاً لاسم المنظمة أو الكيان.

بالنسبة لشهادة مستجيب OCSP يُعد الاسم ذا معنى لأنه يشير إلى اسم مستجيب OCSP الخاص بهيئة التصديق التابعة.

3.1.3.إخفاء الهوية أو استخدام أسماء مستعارة للمشتركين

يُحظر تماماً إخفاء الهوية أو استخدام أسماء مستعارة للمشتركين.

3.1.4.قواعد تفسير أشكال الأسماء المختلفة

تستند سياسة التسمية المعتمدة من قبل هذه الهيئة إلى معيار الاسم المميز (DN) وفقاً للمواصفة ISO/IEC 9595 (X.500).

3.1.5.تفرّد الأسماء

بالنسبة لشهادات توقيع البرمجيات الصادرة للكيانات القانونية: كما ورد في القسم 3.1.1 من هذا البيان تفرض هذه الهيئة التفرّد من خلال استخدام اسم فريد للمنظمة يحتوي على تمثيل لاسم الكيان القانوني.

بالنسبة لشهادة مستجيب OCSP يُدرج الاسم الفريد لمستجيب OCSP في حقل "الموضوع" ضمن اسم DN في شهادة OCSP الصادرة.

3.1.6.التعرف والمصادقة ودور العلامات التجارية

يُقرّ المتقدمون بطلبات الشهادات لدى هذه الهيئة من خلال تقديمهم الطلب بأن بيانات طلبهم لا تتضمن بأي شكل من الأشكال ما يُخل بحقوق أي طرف ثالث في أي اختصاص قضائي فيما يتعلق بالعلامات التجارية أو علامات الخدمة أو الأسماء التجارية أو أسماء الشركات أو الأسماء المستخدمة في الأعمال (DBA) أو أي حق آخر من حقوق الملكية الفكرية كما يُقرّون بعدم استخدام هذه البيانات لأي غرض غير قانوني.

تحتفظ هذه الهيئة بحق إلغاء الشهادة عند استلام أمر مصادق عليه رسمياً من مجلس حوكمة البنية التحتية للمفتاح العامة لمصدر التكنولوجيا (TS PKI GB) أو من محكمة مختصة يقتضي إلغاء شهادة أو شهادات تحتوي على اسم موضوع محل نزاع.

3.2.التحقق الأولي من الهوية

تُستخدم الأساليب الموضحة في هذا القسم للتحقق من هوية المشترك.

تتولى هيئة التسجيل التابعة لشركة مصدر التكنولوجيا (TS RA) التحقق من هوية المتقدم بالطلب والمصادقة على صفاته الأخرى قبل إدراجها ضمن الشهادة. ويجوز لهيئة التسجيل وفقاً لتقديرها المطلق رفض إصدار الشهادة إذا لم تنجح عملية التحقق من الهوية.

3.2.1.طريقة إثبات امتلاك المفتاح الخاص

يقدّم المتقدم بالطلب طلب توقيع شهادة (CSR) موقّعاً رقمياً بصيغة PKCS#10 لإثبات حيازته للمفتاح الخاص المقابل للمفتاح العام المطلوب إدراجه في الشهادة. تفرض أنظمة هيئة التسجيل التابعة لشركة مصدر التكنولوجيا التحقق من إثبات امتلاك المفتاح الخاص كجزء من معالجة طلب الشهادة. ويُقدَّم هذا الإثبات إلى هيئة التسجيل من خلال طلبات CSR بصيغة PKCS#10.

3.2.2.التحقق من هوية الكيان

يُجرى التحقق من هوية الكيان وفقاً للتشريعات العراقية النافذة باستخدام إجراءات تحقق مبيّنة أدناه تقوم بموجبها هيئة التسجيل بتسجيل الكيان وتنفيذ التحقق الأولي من هويته ومن هوية ممثليه.

3.2.2.1.الهوية

تتحقق هوية الكيان المُتقدّم بالطلب بالاعتماد على مصادر موثوقة للبيانات الرسمية والتي يُتوقّع منها تقديم معلومات تفصيلية عن الكيان بما في ذلك الاسم القانوني والعنوان ومعلومات الممثل المفوّض.

تعتمد شركة مصدر التكنولوجيا على "الوقائع العراقية" أو وسائل الاتصال المباشر مع الكيان أو مع الجهة القضائية المختصة التي تُنظّم إنشاء الكيان أو الاعتراف به للتحقق من معلومات الكيانات الحكومية وتعتمد على المراسلات الرسمية المعتمدة مع "دائرة تسجيل الشركات" للتحقق من الكيانات غير الحكومية.

يجوز لشركة مصدر التكنولوجيا مطالبة المتقدم بالطلب بتقديم وثائق رسمية لإثبات هوية الكيان مثل النظام الأساسي للشركة أو وثائق ضريبية صادرة عن جهة حكومية أو خطاب مهني (صادر عن محاسب أو رأي قانوني) أو مستندات أخرى ذات صلة كما يجوز لها تنفيذ زيارة ميدانية إلى مقر الكيان للتحقق من عنوانه.

تتحقق هيئة التسجيل من ارتباط المعلومات الواردة في نموذج الطلب بموضوع الشهادة من خلال التأكد من التطابق التام بين المعلومات المقدمة وتلك التي ستُدرج في الشهادة.

يجوز لسلطة التسجيل التابعة لشركة مصدر التكنولوجيا إعادة استخدام معلومات الهوية التي تم التحقق منها مسبقاً من خلال أنشطة التحقق الموضحة في هذا القسم، شريطة أن تظل تلك المعلومات دقيقة وموثوقة. ويُحظر تماماً إعادة استخدام هذه المعلومات إذا تم التحقق منها قبل أكثر من (365) يوماً من تاريخ إصدار الشهادة.

سلطة المتقدم بالطلب

تتحقق هيئة التسجيل التابعة لشركة مصدر التكنولوجيا من سلطة الممثل المفوّض ومقدّم طلب الشهادة وفقاً لما ورد في القسم 3.2.5.

3.2.2.2.الاسم التجاري / الاسم المستخدم في الأعمال(DBA)

لا تدعم هذه الهيئة استخدام الأسماء التجارية أو الأسماء المستخدمة في الأعمال (DBA) ضمن معلومات هوية الموضوع في الشهادة.

3.2.2.3.التحقق من الدولة

تصدر هيئة التصديق لتوقيع البرمجيات الشهادات فقط للمنظمات المؤسسة داخل العراق. تتحقق هيئة التسجيل من أن قيمة حقل "الدولة" في معلومات هوية الموضوع مُعيّنة إلى."IQ"

3.2.3.التحقق من هوية الأفراد

لا تصدر هيئة التصديق لتوقيع البرمجيات شهادات للأشخاص الطبيعيين بل تصدر الشهادات فقط للكيانات القانونية.

3.2.4.معلومات المشترك غير المؤكدة

تتحقق هيئة التسجيل من جميع معلومات المشترك الواردة ضمن الشهادة بشكل كامل.

3.2.5.التحقق من السلطة

يُعيّن الممثل المفوض للكيان شخصاً من داخل المنظمة كمقدّم لطلبات الشهاداتويكون مسؤولاً عن تقديم طلبات إدارة الشهادات إلى هيئة التسجيل التابعة لشركة مصدر التكنولوجيا. تتولى سلطة التسجيل التابعة لشركة مصدر التكنولوجيا عملية التحقق من هوية مقدم الطلب، وارتباطه بالكيان، وصلاحية تفويضه، وذلك من خلال تطبيق الخطوات الآتية كحد أدنى:

- تُجري هيئة التسجيل عملية تحقق من الهوية من خلال المقارنة المباشرة مع هوية حكومية أصلية (وليس نسخة منها) يُبرزها مقدّم الطلب بشكل شخصي.
- تستخدم هيئة التسجيل خطاب إثبات العمل (خطاب إثبات) المُقدّم ضمن طلب الشهادة للتحقق من ارتباط مقدّم الطلب بالكيان.
- تتحقق هيئة التسجيل من صحة طلب الشهادة وصحة خطاب الإثبات بشكل مباشر مع الممثل المفوض للكيان باستخدام وسيلة تواصل موثوقة تشمل استخدام البريد الإلكتروني الرسمي للمنظمة وعند الحاجة تُنظّم الهيئة اجتماعاً حضورياً مع الممثل.
- تتولى سلطة التسجيل التابعة لشركة مصدر التكنولوجيا التحقق من الارتباط بين مقدم الطلب والكيان، وتأكيد صحة طلب الشهادة من خلال التواصل المباشر مع الممثل المخول للكيان. ويتم استخدام وسيلة اتصال موثوقة تتضمن عناوين البريد الإلكتروني الخاصة بالمؤسسة، كما يمكن تنظيم اجتماع حضوري عند اقتضاء الضرورة وبحسب ما تراه سلطة التسجيل مناسباً.
- ويُجرى التحقق من تفويض مقدّم الطلب لتقديم طلبات الشهادات نيابة عن الكيان استناداً إلى نموذج طلب الشهادة الموقّع من قبل كل من مقدّم الطلب والممثل المفوضوالذي يثبت صلاحية مقدّم الطلب.

3.2.6.معايير التوافق التشغيلي

لا يوجد تنظيم محدد.

3.3.التعريف والمصادقة لطلبات إعادة إصدار المفاتيح

3.3.1.التعريف والمصادقة لإعادة الإصدار الروتينية

يُنفّذ التحقق من الهوية والمصادقة عند إعادة إصدار المفاتيح كما هو الحال في التسجيل الأولي بالإضافة إلى ما يلي:

- تتحقق هيئة التسجيل من وجود الشهادة المطلوب إعادة إصدارها وصلاحيتها ومن استمرار صلاحية المعلومات المُستخدمة للتحقق من هوية وخصائص الموضوع.
- في حال طرأ أي تغيير على الشروط والأحكام الخاصة بشركة مصدر التكنولوجيا تُبلّغ هيئة التسجيل المشترك بذلك.

3.3.2.التعريف والمصادقة لإعادة الإصدار بعد الإلغاء

يُنفّذ التحقق من الهوية والمصادقة عند إعادة الإصدار بعد الإلغاء كما هو الحال في التسجيل الأولي.

3.4.التعريف والمصادقة لطلبات الإلغاء

تتضمن إجراءات التحقق من الهوية والمصادقة في طلبات الإلغاء تقديم طلب رسمي من ممثل الكيان الذي صدرت له الشهادة. وتُطبق هيئة التسجيل إجراء الإلغاء الذي يشمل ما يلي:

- توقيع نموذج طلب الإلغاء من قبل الممثل المفوض.
- التحقق من هوية مقدّمي الطلب من خلال مطابقة المعلومات المتوفرة لدى هيئة التسجيل والمقدمة أثناء تسجيل المشترك.
- التواصل مع الكيان لتوفير تأكيدات معقولة تفيد بأن ممثله الرسمي قد فوّض عملية الإلغاء. ويشمل هذا التواصل حسب الظروف واحداً أو أكثر من الوسائل التالية: الاتصال الهاتفي أو البريد الإلكتروني أو خدمة البريد السريع.

بعد نجاح التحقق من طلب الإلغاء تُبطل هيئة التسجيل الشهادة محل الطلب من خلال نظام هيئة التسجيل المعني.

بالنسبة لشهادات مستجيبي OCSP لا يتضمن هذا البيان أحكاماً تفصيلية لإلغاء هذا النوع من الشهادات. وقد يُستند إلى الإلغاء في حال اختراق المفتاح الخاص المرتبط أو الاشتباه باختراقه وتُعدّ هذه الحالة كارثة وتُعالج وفقاً لخطة استمرارية الأعمال والتعافي من الكوارث المعتمدة لدى شركة مصدر التكنولوجيا.

4. متطلبات التشغيل لدورة حياة الشهادة

4.1.طلب الشهادة

4.1.1.من يمكنه تقديم طلب الشهادة

يجب أن يلتزم المتقدمون بطلبات الشهادات بالأحكام المنصوص عليها ضمن عمليات التسجيل وهذا البيان (CP/CPS) وشروط واحكام استخدام المشترك.

يتحمل ممثل المتقدم بالطلب مسؤولية صحة جميع البيانات المقدَّمة ضمن طلبات الشهادات. ويضمن الموافقة على الطلب من خلال توقيع وختم نموذج طلب الشهادة وشروط واحكام استخدام المشترك المُرفقة.

لا تُصدر شركة مصدر التكنولوجيا شهادات للكيانات المُدرجة في القائمة السوداء الداخلية التي تتضمن أسماء المنظمات غير المقبولة. وتُراجع هذه القائمة من قبل فريق هيئة التسجيل في الشركة العامة للاتصالات والمعلوماتية عند تلقي أي طلب شهادة.

بالنسبة لشهادة مستجيب OCSP تُشرف هيئة التسجيل ومشرف موثوق من إدارة البنية التحتية للمفتاح العامة (PKI) على تنفيذ مراسيم تشغيل داخلية مُعتمدة تُصدر بموجبها شهادات OCSP الخاصة بهيئة التصديق لتوقيع البرمجيات.

4.1.2.عملية التسجيل والمسؤوليات

تطلب هيئات التصديق من كل متقدم تقديم طلب شهادة ومعلومات الطلب قبل إصدار الشهادة. وتتحقق هيئة التسجيل من جميع الاتصالات الواردة من المتقدم وتضمن تعبئة نموذج الطلب وتوقيعه كما هو متوقع.

- يقوم ممثل الكيان المتقدّم بالطلب بتحميل نموذج طلب الشهادة وشروط واحكام استخدام المشترك من المستودع العام.
- يُعبّأ نموذج الطلب ويوقّع من قبل الممثل الرسمي للكيان كما يجب أن تُصدَّق شروط واحكام استخدام المشترك.
- يُنشئ الفريق الفني المعني في الكيان زوج مفاتيح باستخدام وحدة تشفير مادية تتوافق على الأقل مع المستوى FIPS 140-2المستوى 2 أو معايير Common Criteria EAL 4+ أو ما يعادلها ثم يُنشئ طلب توقيع شهادة (CSR)باستخدام حقول الشهادة المعتمدة في نموذج الطلب (مثل سماتDN حجم المفتاح نوع المفتاح وغيرها) ويُسلَّم هذا الطلب إلى ممثل المتقدم بالطلب.
- يُجري ممثل المتقدم بالطلب عملية المصادقة على بوابة هيئة التسجيل عبر الويب (Web RA) باستخدام بيانات اعتماد المصادقة متعددة العوامل التي أُعدت كجزء من عملية التسجيل المبينة في وثيقة داخلية خاصة بهيئة التسجيل ثم يقدّم طلب الشهادة متضمناً ما يلي على سبيل المثال لا الحصر:
  - نسخة ممسوحة ضوئياً من نموذج الطلب المعبأ والموقّع.
  - المعلومات والمستندات المطلوبة لإثبات الهوية والتفويض.
  - ملف طلب توقيع الشهادة.(CSR)

يتطلب إصدار شهادة توقيع البرمجيات وجود عضوين من فريق هيئة التسجيل:

- يُراجع فريق هيئة التسجيل ويُصادق على سلامة وصحة جميع المستندات المقدمة ويتحقق من هوية المتقدم بالطلب كما هو موضح في القسم 3.2.2.
- يُراجع فريق هيئة التسجيل القائمة السوداء للمنظمات التي لا تُقبل منها الطلبات. وتُستعلم هذه القائمة عند استلام أي طلب شهادة.
- يُنفّذ فريق هيئة التسجيل إجراءات معالجة طلب الشهادة كما هو موضح في القسم 4.2.

بالنسبة لشهادة مستجيب OCSP تُشرف هيئة التسجيل ومشرف موثوق من إدارة PKI على تنفيذ مراسيم التشغيل التي تُصدر بموجبها هذه الشهادات. ويُوافق مجلس حوكمة البنية التحتية للمفتاح العامة (TS PKI GB) على وثائق المراسيم التشغيلية ويتحقق من تطابق قالب الشهادة المُضمّن واتفاقية التسمية مع أحكام هذا البيان. ويقوم مجلس الحوكمة بعد ذلك بالموافقة على المراسيم وتأكيد قائمة الأفراد ذوي الأدوار الموثوقة المشاركين فيها.

4.2.معالجة طلب الشهادة

4.2.1. تنفيذ وظائف التعريف والمصادقة

يرجى الرجوع إلى القسمين 3.2.2 و4.1 بالإضافة إلى المهام التالية التي تنفذها هيئة التسجيل التابعة لشركة مصدر التكنولوجيا:

أ. يُخصَّص معرّف فريد لكل سجل طلب شهادة.
ب. تُسجّل هيئة التسجيل جميع الأنشطة المرتبطة بطلب الشهادة (مثل الاتصالات عبر البريد الإلكتروني والمكالمات الهاتفية وتدقيق الأدلة) وتُرفقها بسجل الطلب.

ج. يُدرج أي طلب شهادة أو إلغاء خبيثا وأي طلب فشل عدة مرات (أكثر من ثلاث مرات) في القائمة السوداء التي تحتوي على تفاصيل ضرورية لتجنّب أي غموض عند تحديد الطلبات الخبيثة مستقبلاً.

د. تُجري هيئة التسجيل مراجعة للقائمة السوداء الخاصة بها. وفي حال وُجد المتقدم في القائمة يُرفض طلب الشهادة.

1) يملأ مقدّم الطلب نموذج تسجيل الكيان كما يلي:

أ. معلومات الكيان:

1. الاسم القانوني للمنظمة.
2. العنوان الرسمي.
3. رقم الهاتف الرئيسي.

ب. معلومات الممثلين المفوّضين:

بيانات ممثل المتقدّم بالطلب مثل رقم الهاتف البريد الإلكتروني الرسمي المنصب.

ج. معلومات مقدّم الطلب:

الاسم ومعلومات الاتصال الخاصة بمقدّم الطلب المفوّض لتقديم طلبات إدارة الشهادات نيابة عن الكيان.

2) يُوقّع ممثل المتقدّم بالطلب ويصدّق شروط واحكام استخدام المشترك المخصصة.

3) يُرسل مقدّم الطلب نموذج التسجيل الموقّع وخطاب الإثبات والمستندات التحقق الأخرى إلى هيئة التسجيل عبر البريد الإلكتروني.

4) تُنفّذ هيئة التسجيل التحقق التالي لكل طلب شهادة دون الاعتماد على تحقق تم مسبقاً:

- التحقق من هوية المنظمة كما ورد في القسم 3.2.2.
- التحقق من الممثل المفوض للكيان كما ورد في القسم 3.2.2.
- التحقق من تفويض مقدّم الطلب كما ورد في القسم 3.2.5.
- التحقق من رقم هاتف المنظمة عبر إجراء مكالمة عشوائية.

إذا اجتاز الطلب جميع عمليات التحقق أعلاه تُطلق هيئة التسجيل عملية تسجيل الكيان ومقدّم الطلب على بوابة التسجيل الإلكترونية (Web RA Portal) بناءً على المعلومات المجمعة. وبذلك يُمكن لمقدّم الطلب تسجيل الدخول إلى البوابة وتقديم طلبات الشهادات نيابة عن الكيان.

بالإضافة إلى الخطوات أعلاه تضمن هيئة التسجيل ما يلي:

1) لا يُسمح لأي فرد بتنفيذ التحقق والموافقة على طلب إصدار شهادة توقيع البرمجيات بشكل منفرد.
2) يُتحقق من كل طلب شهادة دون الاعتماد على تحقق سابق.

تحتفظ هيئة التسجيل بإجراء داخلي مفصل يتحقق من نشاط طلبات شهادات توقيع البرمجيات لضمان إجراء التحقق بالشكل الصحيح.

بالنسبة لشهادة مستجيب OCSP تُشرف هيئة التسجيل ومشرف موثوق من إدارة البنية التحتية للمفتايح العامة (PKI) على تنفيذ مراسيم التشغيل التي تُصدر بموجبها هذه الشهادات. ويُوافق مجلس حوكمة البنية التحتية للمفتايح العامة (TS PKI GB) على وثائق المراسيم التشغيلية ويتحقق من تطابق قالب الشهادة المُضمّن واتفاقية التسمية مع أحكام هذا البيان. ثم يُصدّق المجلس على المراسيم ويؤكد قائمة الموظفين ذوي الأدوار الموثوقة المشاركين.

4.2.2.الموافقة على طلبات الشهادات أو رفضها

تُوافق هيئة التسجيل على طلب الشهادة فقط إذا استوفت المعايير التالية:

- النجاح في التحقق من الهوية والمصادقة لجميع معلومات المشترك المطلوبة وفقاً لما ورد في القسم 3.2.

ترفض هيئة التسجيل التابعة لشركة مصدر التكنولوجيا طلب الحصول على الشهادة في الحالات التالية:

- عدم إمكانية إتمام عملية تحديد الهوية والتحقق من صحة كافة معلومات المشترك المطلوبة وفقاً للقسم.(3.2)
- فشل المشترك في تقديم الوثائق الثبوتية الداعمة عند طلبها.

يجوز لسلطة التصديق التابعة لشركة مصدر التكنولوجيا إصدار شهادات توقيع شفرات برمجية جديدة أو بديلة للكيان الذي وقع ضحية لهجوم استحواذ موثق، مما أدى إلى فقدان السيطرة على المفتاح الخاص المرتبط بشهادة توقيع البرمجيات الخاصة به.

ومع ذلك، لا تصدر سلطة التصديق التابعة لشركة مصدر التكنولوجيا شهادات توقيع شفرات برمجية جديدة أو بديلة للكيانات التي يثبت قيامها بتوقيع برمجيات مشبوهة بشكل متعمد. ويتم الاحتفاظ بـ "سبب إلغاء شهادة توقيع البرمجيات" كدليل على أن الشهادة قد أُلغيت بسبب قيام مقدم الطلب بتوقيع برمجيات مشبوهة عمداً.

4.2.3.المدة الزمنية لمعالجة طلبات الشهادات

لا يوجد تنظيم محدد.

4.3.إصدار الشهادة

4.3.1.إجراءات هيئة التصديق أثناء إصدار الشهادة

عند إكمال جميع عمليات التحقق وفقاً لما ورد في القسم 4.2.1 يستخدم فريق هيئة التسجيل بوابة التسجيل الإلكترونية لبدء إصدار الشهادة من هيئة التصديق لتوقيع البرمجيات استناداً إلى طلب توقيع الشهادة (CSR) المقدَّم من المتقدّم بالطلب.

عند تقديم طلب الشهادة إلى هيئة التصديق لتوقيع البرمجيات تتحقق الهيئة من تنسيق الطلب وبنيته ثم تُولّد الشهادة وفقاً لقالب الشهادة المُعد مسبقاً. بعد ذلك تُتاح الشهادة لممثل المتقدّم بالطلب لتحميلها. تصدر هيئة التصديق الشهادة بحالة "فعّالة" لتكون جاهزة للاستخدام فور نشرها في مستودع المفاتيح المستهدف.

بالنسبة لشهادة مستجيب OCSP تُشرف هيئة التسجيل على تنفيذ مراسيم التشغيل الداخلية المعتمدة التي يصدر بموجبها مسؤول موثوق من إدارة PKI أمراً مباشراً إلى هيئة التصديق لتوقيع البرمجيات بتنفيذ عملية توقيع الشهادة. وتُراجع هيئة التسجيل الشهادة المُصدرة للتحقق من صحتها.

4.3.2. إشعار المشترك بإصدار الشهادة من قبل هيئة التصديق

يُخطر المشتركون عبر البريد الإلكتروني من قبل هيئة التصديق لتوقيع البرمجيات بأن الشهادة قد جرى توليدها. وتُتاح الشهادة لممثل المتقدّم بالطلب عبر حسابه على بوابة هيئة التسجيل الإلكترونية.(Web RA Portal)

بالنسبة لشهادة مستجيب OCSP يُخطر مسؤول إدارة PKI عند استلام الشهادة من فريق هيئة التسجيل.

4.4.قبول الشهادة

4.4.1.السلوك الذي يمثل قبولاً للشهادة

يقوم مقدّم الطلب بتحميل الشهادة من بوابة التسجيل الإلكترونية ثم يتحقق من محتواها بمقارنتها مع طلب توقيع الشهادة .(CSR)في حال وجود أي اختلافات يشرع مقدّم الطلب بالتواصل مع هيئة التسجيلوقد يؤدي ذلك إلى إلغاء الشهادة وإصدار شهادة مصححة.

تُعد الشهادة مقبولة من قبل الكيان إذا لم يتقدم مقدّم الطلب بأي اعتراض إلى هيئة التسجيل خلال عشرة أيام عمل من تاريخ استلام إشعار البريد الإلكتروني الخاص بإصدار الشهادة.

بالنسبة لشهادة مستجيب OCSP تُعد الشهادة مقبولة عند نشرها في مستودع مفاتيح OCSP كجزء من مراسيم التشغيل الداخلية المعتمدة.

4.4.2.نشر الشهادة من قبل هيئة التصديق

لا تقوم هيئة التصديق لتوقيع البرمجيات بنشر شهادات المستخدم النهائي باستثناء مشاركتها مع المشتركين المعنيين.

4.4.3.إشعار جهات أخرى بإصدار الشهادة

لا يوجد تنظيم محدد.

4.5.استخدام زوج المفاتيح والشهادة

4.5.1.استخدام المفتاح الخاص بالمشترك والشهادة

يلتزم المشتركون بالواجبات التالية:

- تقديم معلومات صحيحة ومحدّثة لهيئة التصديق لتوقيع البرمجيات كجزء من طلبهم.
- عدم التلاعب بالشهادة.
- استخدام الشهادات فقط لأغراض قانونية ومصرح بها ووفقاً للمتطلبات العامة المشتركة المنطبقة على سياسة الشهادات (CP) وهذا البيان.(CPS)
- حماية المفتاح الخاص (وجميع الأسرار المرتبطة به) من أي اختراق أو فقدان أو إفشاء أو أي استخدام غير مصرح به.
- إخطار هيئة التسجيل فوراً إذا أصبحت أي من المعلومات في الشهادة غير صالحةاو في حال حدوث أي اختراق أو فقدان أو إفشاء أو استخدام غير مصرح به.
- عدم استخدام الشهادة بعد انتهاء صلاحيتها أو بعد إلغائها.
- التوقف عن استخدام المفتاح الخاص بعد انتهاء فترة صلاحية الشهادة أو بعد إلغائها.

4.5.2.استخدام المفتاح العام من قبل الطرف المعتمد

يتعين على أي طرف يعتمد على شهادة صادرة من هيئة التصديق لتوقيع البرمجيات:

- استخدام برامج متوافقة مع معيار X.509 ومعايير IETF PKIX السارية للتحقق من توقيع الشهادة وفترة صلاحيتها.
- التحقق من الشهادة باستخدام قائمة إلغاء الشهادات (CRL) أو خدمة حالة الشهادة (OCSP) وفقاً لإجراءات التحقق من مسار الشهادة.
- الوثوق بالشهادة فقط إذا لم تكن ملغاة وكانت ضمن فترة الصلاحية.
- الوثوق بالشهادة فقط لأغراضها المخصصة ووفقاً لأحكام هذا البيان.

4.6.تجديد الشهادة

4.6.1.حالات 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 الشهادة الجديدة

غير قابل للتطبيق.

4.6.5.السلوك الذي يمثل قبولاً للشهادة المجددة

غير قابل للتطبيق.

4.6.6.نشر الشهادة المجددة من قبل هيئة التصديق

غير قابل للتطبيق.

4.6.7.إشعار جهات أخرى بإصدار الشهادة المجددة

غير قابل للتطبيق.

4.7.إعادة إصدار الشهادة(Re-Key)

تشير إعادة إصدار الشهادة إلى إصدار شهادة جديدة لمشترك حالي تتضمن فترة صلاحية جديدة بالإضافة إلى مفتاح عام مختلف في حين تُكرّر باقي المعلومات من الشهادة السابقة في الشهادة الجديدة.

تدعم هيئة التصديق لتوقيع البرمجيات عملية إعادة الإصدار وتُشابه إجراءاتها من حيث التحقق من الهوية وإصدار الشهادة والتواصل مع الأطراف ذات العلاقة عملية إصدار الشهادة الأولية.

4.7.1.حالات إعادة إصدار الشهادة

قد يُعاد إصدار الشهادة أثناء صلاحيتها أو بعد انتهاء صلاحيتها أو بعد إلغائها. وقد تؤدي عملية إعادة الإصدار إلى إبطال أي شهادات توقيع خوارزميات لا تزال فعّالة.

4.7.2.من يمكنه طلب إصدار مفتاح عام جديد
كما هو الحال في عملية إصدار الشهادة الأولية.

4.7.3.طلبات إعادة إصدار الشهادة
كما هو الحال في عملية إصدار الشهادة الأولية.

4.7.4.إشعار المشترك بإصدار شهادة جديدة
كما هو الحال في عملية إصدار الشهادة الأولية.

4.7.5.السلوك الذي يمثل قبولاً لشهادة معاد إصدارها
كما هو الحال في عملية إصدار الشهادة الأولية.

4.7.6.نشر الشهادة المعاد إصدارها من قبل هيئة التصديق
كما هو الحال في عملية إصدار الشهادة الأولية.

4.7.7.إشعار جهات أخرى بإصدار الشهادة من قبل هيئة التصديق
كما هو الحال في عملية إصدار الشهادة الأولية.

4.8.تعديل الشهادة

4.8.1.حالات 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 معدّلة
غير قابل للتطبيق.

4.8.5.السلوك الذي يمثل قبولاً لشهادة معدّلة
غير قابل للتطبيق.

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

4.8.7.إشعار جهات أخرى بإصدار الشهادة المعدّلة
غير قابل للتطبيق.

4.9.إلغاء وتعليق الشهادة

توفّر شركة مصدر التكنولوجيا إمكانية دائمة للمشتركين لتقديم طلبات الشهادات من خلال نظام إلكتروني متاح على مدار الساعة طوال أيام الأسبوع للمشتركين المصادق عليهم.

تعليق الشهادات محظور ويُسمح فقط بإلغاء الشهادات بشكل دائم.

4.9.1.حالات الإلغاء

4.9.1.1.حالات إلغاء شهادات المشتركين

بالنسبة للشهادات الصادرة للأشخاص المعنويين (أي شهادات توقيع البرمجيات)، تتولى سلطة التسجيل التابعة لشركة مصدر التكنولوجيا معالجة طلب الإلغاء وضمان قيام سلطة تصديق توقيع البرمجيات بإلغاء الشهادة خلال (24) ساعة في حال وقوع واحد أو أكثر من الأحداث الآتية:

1. طلب المشترك خطياً من سلطة التصديق إلغاء الشهادة.
2. اكتشاف أن طلب الشهادة الأصلي لم يكن مفوضاً، ولم يتم منحه التفويض لاحقاً بأثر رجعي.
3. حصول سلطة التصديق على أدلة معقولة تثبت اختراق المفتاح الخاص للمشترك المقابل لشهادة المفتاح العام.
4. إبلاغ سلطة التصديق بوجود طريقة مثبتة أو مبرهنة تتيح استخراج المفتاح الخاص للمشترك بسهولة استناداً إلى المفتاح العام الموجود في الشهادة.
5. إبلاغ سلطة التصديق بوجود طريقة مثبتة أو مبرهنة تعرض المفتاح الخاص للمشترك للاختراق، أو وجود دليل واضح على أن الطريقة المحددة المستخدمة لتوليد المفتاح الخاص كانت معيبة.
6. توفر قناعة معقولة لدى سلطة التصديق بأن الشهادة قد استُخدمت لتوقيع برمجيات مشبوهة.

وتضمن سلطة التسجيل التابعة لشركة مصدر التكنولوجيا تنفيذ إلغاء الشهادة خلال (24) ساعة، كما تقوم بإلغاء الشهادة خلال (5) أيام في حال وقوع واحد أو أكثر من الأحداث الآتية:

7. عدم امتثال الشهادة لمتطلبات القسمين (6.1.5) و(6.1.6).
8. حصول سلطة التسجيل على أدلة تثبت سوء استخدام الشهادة.
9. إبلاغ سلطة التسجيل بمخالفة المشترك لواحد أو أكثر من التزاماته الجوهرية الواردة في شروط وأحكام استخدام المشترك.
10. إبلاغ سلطة التسجيل بوقوع تغيير جوهري في المعلومات الواردة في الشهادة.
11. إبلاغ سلطة التسجيل بأن الشهادة لم تُصدر وفقاً لسياسة ممارسات التصديق هذه.
12. تحديد سلطة التسجيل أو إبلاغها بأن أي من المعلومات الواردة في الشهادة غير دقيقة.
13. كون الإلغاء متطلباً بموجب سياسة ممارسات التصديق هذه.
14. انتهاء حق سلطة التصديق في إصدار الشهادات بموجب المتطلبات المحددة في سياسة ممارسات التصديق هذه، أو إلغاؤه أو إنهاؤه، ما لم تكن شركة مصدر التكنولوجيا قد اتخذت ترتيبات للاستمرار في صيانة مستودع قوائم إلغاء الشهادات (CRL) أو بروتوكول حالة الشهادة عبر الإنترنت (OCSP).

يجوز لشركة مصدر التكنولوجيا تأجيل الإلغاء بناءً على طلب مزودي برامج التطبيقات في الحالات التي يكون فيها للإلغاء الفوري تأثير سلبي كبير ومحتمل على بيئة العمل الرقمية.

4.9.2.حالات إلغاء شهادة هيئة التصديق التابعة

على المشتركين تقديم طلبات الإلغاء وفقاً للتعليمات الموضحة في الصفحة الإلكترونية الرسمية:

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

تتولى سلطة التسجيل التابعة لشركة مصدر التكنولوجيا معالجة عمليات إلغاء الشهادات وفقاً لما يأتي:

1. طُلب الإلغاء خطياً.
2. أبلغت شركة مصدر التكنولوجيا هيئة التصديق المُصدرة (أي الهيئة الجذرية) بأن طلب الشهادة الأصلي لم يكن مفوضاً ولا يمنح التفويض بأثر رجعي.
3. حصلت شركة مصدر التكنولوجيا على دليل يثبت اختراق المفتاح الخاص لهيئة التصديق لتوقيع البرمجيات أو عدم امتثاله لمتطلبات البندين 6.1.5 و6.1.6.
4. حصلت هيئة التصديق المُصدرة (أي الهيئة الجذرية) على دليل يفيد بإساءة استخدام شهادة هيئة التصديق لتوقيع البرمجيات.
5. أُبلغت هيئة التصديق المُصدرة بأن شهادة هيئة التصديق لتوقيع البرمجيات صدرت بطريقة غير متوافقة مع هذا البيان أو أن الهيئة لم تلتزم بما ورد فيه.
6. قررت هيئة التصديق المُصدرة أن أياً من المعلومات الظاهرة في شهادة هيئة التصديق لتوقيع البرمجيات غير دقيق أو مضلل.
7. توقفت هيئة التصديق لتوقيع البرمجيات عن العمل لأي سبب ولم تضع ترتيبات لضمان استمرار الدعم لإلغاء الشهادة من قبل هيئة تصديق أخرى.
8. انتهى أو أُلغي أو أُنهي حق هيئة التصديق لتوقيع البرمجيات في إصدار الشهادات بموجب هذه المتطلبات دون أن تضع الهيئة الجذرية ترتيبات لصيانة مستودع قوائم الإلغاء CRL وOCSP.
9. اقتضت سياسة الشهادات أو بيان ممارسة الشهادات الخاص بهيئة التصديق المُصدرة إلغاء الشهادة.

4.9.3.الجهات المخوّلة بطلب الإلغاء

يجوز تقديم طلبات الإلغاء من الجهات الآتية:

- هيئة التسجيل في الحالات المبيّنة في البند 4.9.1.
- المشترك الذي يرغب في إلغاء شهادته.
- أي طرف معتمد أو مورّد لبرمجيات التطبيقات يمتلك دليلاً على اختراق شهادة المشترك أو استخدامها في توزيع برمجيات خبيثة.
- شركة مصدر التكنولوجيا بناءً على تقديرها الخاص في حال توافر معلومات عن اختراق لمفتاح هيئة التصديق.
- يجوز للمشتركين والطرف المعتمد وموزّدي البرمجيات وأي أطراف ثالثة تقديم بلاغات عن مشاكل الشهادة لإعلام شركة مصدر التكنولوجيا بوجود سبب وجيه محتمل لبدء عملية الإلغاء.

يُقبل فقط الطلب المصرّح به لإلغاء الشهادة.

4.9.4.إجراءات تقديم طلب الإلغاء

تُنفذ هيئة التسجيل في مصدر التكنولوجيا إجراءات إلغاء الشهادة وفقاً للخطوات الآتية:

1. تُخصّص هيئة التسجيل رقماً تعريفياً فريداً لطلب الإلغاء وتُسجّل الوثائق المقدمة بموجب هذا الرقم
2. تتحقق هيئة التسجيل من هوية مقدّم الطلب وفقاً لما ورد في البند 3.4
3. تتحقق هيئة التسجيل من معلومات الإلغاء المدرجة في نموذج الإلغاء
4. تُجري هيئة التسجيل التحقيق المطلوب ضمن الإطار الزمني المنصوص عليه في البند 4.9.1 وقد يتضمن ذلك التواصل مع المشترك
5. ينفّذ فريق هيئة التسجيل عملية إلغاء الشهادة
6. تُلغى الشهادة من قبل هيئة التصديق لتوقيع البرمجيات وتُحدّث حالة الشهادة
7. تُخطر هيئة التسجيل ممثل مقدم الطلب عبر البريد الإلكتروني بإتمام عملية إلغاء الشهادة
8. تُحدّث هيئة التسجيل القائمة السوداء الداخلية بإدراج تفاصيل الشهادة الملغاة وظروف الإلغاء وبناءً على ذلك يمكن تعديل تصنيف المخاطر لمقدم الطلب في القائمة السوداء الداخلية حيث يُرجع إلى هذه المعلومات قبل معالجة أي طلبات شهادة مستقبلية للمُقدِّم ذاته.

معالجة إلغاء الشهادة من قبل هيئة التسجيل بعد استلام بلاغ عن مشكلة في الشهادة

تحافظ شركة مصدر التكنولوجيا على قدرة داخلية دائمة على مدار الساعة وطوال أيام الأسبوع للاستجابة لطلبات الإلغاء ذات الأولوية العالية وبلاغات مشاكل الشهادات. وتُوفّر تعليمات الإبلاغ عن مشاكل الشهادات وطلبات الإلغاء في صفحة مخصصة ضمن المستودع العام والمتاحة عبر الرابط: https://pki.techsource.iq/repository/Certificate_Problem_Report.html

يجوز للمشتركين والأطراف المعتمدة وموزّدي برمجيات التطبيقات وأي أطراف ثالثة تقديم بلاغات عن مشاكل الشهادات عبر البريد الإلكتروني: certificate.problem@techsource.iq

عند تقديم بلاغ عن مشكلة شهادة يُطلب من المبلّغ تضمين بيانات الاتصال الخاصة به ووصف الإساءة المشتبه بها والمعلومات المتعلقة بالموضوع محل البلاغ.

تبدأ هيئة التسجيل لدى شركة مصدر التكنولوجيا بالتحقيق في البلاغ خلال أربع وعشرين ساعة من استلامه وتقرر ما إذا كان الإلغاء أو اتخاذ إجراء مناسب آخر ضرورياً استناداً على الأقل إلى المعايير الآتية:

- طبيعة المشكلة المبلغ عنها.
- عدد البلاغات المستلمة حول الشهادة أو الموضوع محل البلاغ.
- الجهة التي قدّمت البلاغ (إذ تُمنح البلاغات الواردة من جهة مكافحة برمجيات خبيثة أو جهة إنفاذ قانون وزناً أكبر من البلاغات مجهولة المصدر).
- القوانين المحلية ذات الصلة.

في حال تقرّر إلغاء الشهادة استناداً إلى بلاغ المشكلة تُنفّذ هيئة التسجيل إجراء الإلغاء وفقاً لما ورد سابقاً في هذا القسم.

وإذا رأت شركة مصدر التكنولوجيا أن الإجراء مناسب فقد تُحيل البلاغ إلى جهة إنفاذ القانون.

4.9.5.فترة السماح لطلب الإلغاء

لا توجد فترة سماح لطلب الإلغاء. تُعالج طلبات الإلغاء فور اتخاذ قرار الإلغاء وفي جميع الحالات ضمن الأطر الزمنية المحددة في البند 4.9.1 من هذا البيان.

4.9.6.المدة التي يجب أن تعالج فيها هيئة التصديق طلب الإلغاء

تُعالج طلبات إلغاء الشهادات خلال أربع وعشرين ساعة. وفي حالة بلاغات مشاكل الشهادات تبدأ هيئة التسجيل التحقيق خلال أربع وعشرين ساعة من استلام البلاغ. وتشرع هيئة التسجيل بالتواصل مع المشترك ومع الجهات المعنية عند الاقتضاء مثل جهات إنفاذ القانون. وتُرسل رسالة أولية حول المشكلة إلى كل من المشترك ومقدم البلاغ.

تُجري هيئة التسجيل تحقيقات إضافية بمشاركة مجلس حوكمة البنية التحتية للمفتاح العامة لمصدر التكنولوجيا والمشترك والجهات ذات العلاقة مثل جهات إنفاذ القانون لاتخاذ القرار المناسب بشأن الشهادة المعنية.

في حال بيّنت نتائج التحقيق تحقق أحد أسباب الإلغاء الواردة في البند 4.9.1 تُلغى الشهادة خلال الفترة الزمنية المنصوص عليها في البند ذاته.

استناداً إلى سبب الإلغاء قد تتفق هيئة التسجيل مع المشترك على خطة لإصدار شهادة جديدة.

4.9.7.متطلبات التحقق من الإلغاء للطرف المعتمد

يقع على عاتق الطرف المعتمد وحده إجراء التحقق من إلغاء جميع الشهادات ضمن سلسلة الثقة قبل اتخاذ قرار الاعتماد على المعلومات الواردة في الشهادة. وتوفّر هيئة التصديق لتوقيع البرمجيات حالة الإلغاء من خلال آليات مدمجة في الشهادة مثل قائمة الإلغاء (CRL) وبروتوكول OCSP

4.9.8.تكرار إصدار قائمة إلغاء الشهادات (إن وُجد)

تنشر هيئة التصديق لتوقيع البرمجيات قوائم الإلغاء على فترات منتظمة وفقاً للقواعد الآتية:

- تُولّد قائمة إلغاء جديدة كل أربع وعشرين ساعة.
- تُحدّد صلاحية قائمة الإلغاء أي حقل nextUpdate بست وعشرين ساعة.

4.9.9.الحد الأقصى لتأخير نشر قائمة الإلغاء (إن وُجد)

تُصدر قوائم الإلغاء في الوقت المناسب من قبل هيئة التصديق لتوقيع البرمجيات وفقاً لتكرار الإصدار المذكور في البند 4.9.7 من هذا البيان.

4.9.10.توفر التحقق من الإلغاء/الحالة عبر الإنترنت

توفّر هذه الهيئة خدمة مستجيب OCSP متوافق مع المواصفة RFC 6960 ويحمل شهادة موقّعة من هذه الهيئة. يوفّر مستجيب OCSP المعلومات فوراً لتطبيقات الطرف المعتمد استناداً إلى إجراءات هيئة التصديق على الشهادات الصادرة تحتوي شهادة مستجيب OCSP على امتداد من نوع id-pkix-ocsp-nocheck وفقاً لما ورد في المواصفةRFC 6960

يرد عنوان URL الفعلي لمستجيب OCSP الذي يتعين على الأطراف المعتمدة الرجوع إليه داخل الشهادات الصادرة من قبل هيئة التصديق لتوقيع البرمجيات

4.9.11.متطلبات التحقق من الإلغاء عبر الإنترنت

يدعم مستجيب OCSP طريقتي HTTP GET وHTTP POST

بالنسبة لحالة شهادات المشتركين:

- تكون صلاحية استجابات OCSP ثماني ساعات أو أكثر.
- تكون صلاحية استجابات OCSP عشرة أيام أو أقل.
- إذا كانت صلاحية استجابة OCSP أقل من ست عشرة ساعة تحدث هيئة التصديق لتوقيع البرمجيات المعلومات المقدمة عبر بروتوكول التحقق من حالة الشهادة عبر الإنترنت قبل نصف مدة الصلاحية من تاريخ nextUpdate.
- إذا كانت صلاحية استجابة OCSP ست عشرة ساعة أو أكثر تحدث هيئة التصديق لتوقيع البرمجيات المعلومات المقدمة عبر بروتوكول التحقق من حالة الشهادة عبر الإنترنت قبل ثماني ساعات على الأقل من تاريخ nextUpdate ولا تتجاوز أربعة أيام بعد تاريخ thisUpdate.

إذا تلقى مستجيب OCSP طلباً بشأن رقم تسلسلي لشهادة غير مستخدم (أي لم يُصدر من قبل هيئة التصديق لتوقيع البرمجيات) فإن مستجيب OCSP يُصدر استجابة بحالة "ملغاة" وفقاً لما ورد في القسم 4.4.8 من المواصفةRFC 6960

تُراقب هيئة التصديق لتوقيع البرمجيات مستجيب OCSP لرصد الطلبات الخاصة بالأرقام التسلسلية غير المستخدمة كجزء من إجراءات المراقبة الأمنيةويؤدي أي طلب من هذا النوع إلى بدء تحقيق من قبل فرق التشغيل المختصة في مصدر التكنولوجيا.

4.9.12.أشكال أخرى لنشر معلومات الإلغاء

تعتمد هيئة التصديق لتوقيع البرمجيات فقط على بروتوكول OCSP وقوائم الإلغاء (CRL) كوسيلتين لنشر معلومات إلغاء الشهادات.

4.9.13. متطلبات خاصة بحالات اختراق المفتاح

إذا اكتشفت شركة مصدر التكنولوجيا أو توفر لديها سبب للاعتقاد بحدوث اختراق للمفتاح الخاص لهيئة التصديق لتوقيع البرمجيات تُعلن حالة طارئة مباشرة وتُفعّل خطة استمرارية الأعمال. بالإضافة إلى ذلك تقوم بما يلي:

- تحديد نطاق الشهادات التي ينبغي إبطالها.
- إبطال الشهادات المتأثرة خلال 24 ساعة ونشر قوائم الإلغاء عبر الإنترنت خلال 30 دقيقة من إنشائها.
- بذل جهود معقولة 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.

يجوز للأطراف إثبات اختراق المفتاح باستخدام إحدى الطرق التالية:

- تقديم طلب توقيع شهادة (CSR) موقعاو مفتاح خاصاو استجابة لتحدٍ موقعة باستخدام المفتاح الخاص وقابلة للتحقق بواسطة المفتاح العام.
- تقديم المفتاح الخاص نفسه.

4.9.14.الحالات التي تستدعي التعليق

لا تدعم هذه الهيئة خيار تعليق الشهادة.

4.9.15.من يمكنه طلب التعليق
غير قابل للتطبيق.

4.9.16.إجراءات طلب التعليق
غير قابل للتطبيق.

4.9.17.حدود فترة التعليق
غير قابل للتطبيق.

4.10.خدمات حالة الشهادة

يرجى الرجوع إلى القسم 4.9.6 من هذا البيان. إضافة إلى ذلك وُفِرت الأحكام التالية:

4.10.1.الخصائص التشغيلية
تنشر هيئة التصديق لتوقيع البرمجيات قوائم الإلغاء في المستودع العام المتاح للأطراف المعتمدة. كما توفر المستجيب لبروتوكول OCSP التابع للهيئة واجهة HTTP يمكن الوصول إليها علناً من قبل الأطراف المعتمدة. لا تُزال إدخالات الإلغاء في قوائم الإلغاء أو استجابات OCSP بعد انتهاء صلاحية الشهادات الملغاة. تتضمن قائمة الإلغاء الامتداد X.509 "ExpiredCertsOnCRL"كما هو معرّف في المعيار / ISO/IEC 9594-8 التوصية ITU-T X.509

4.10.2.توفر الخدمة
يُتاح المستودع العام الذي تُنشر فيه معلومات الشهادات وقوائم الإلغاء على مدار الساعة طوال أيام الأسبوع.

يُضمن توفره بنسبة لا تقل عن 99.6٪ خلال فترة عام كامل تشغّل هيئة التصديق لتوقيع البرمجيات نظام CRL و OCSP وتُحافظ عليهما باستخدام موارد تضمن وقت استجابة لا يتجاوز عشر ثوانٍ في ظل ظروف التشغيل الطبيعية تُبقي الهيئة على قدرة دائمة (7/24) للرد داخلياً على البلاغات عالية الأولوية المتعلقة بالشهادات كما هو موضح في القسم 4.9.3 من هذا البيانوتُحيل هذه البلاغات إلى الجهات القانونية المختصة و/أو تُبطل الشهادة موضوع البلاغ عند الاقتضاء.

4.10.3.الخصائص الاختيارية
لا يوجد نص محدد.

4.11.إنهاء الاشتراك

ترتبط فترة الاشتراك بفترة صلاحية الشهادةوينتهي الاشتراك بانتهاء صلاحية الشهادة أو بإبطالها.

4.12.حفظ واستعادة المفاتيح

4.12.1.سياسة وممارسات حفظ واستعادة المفاتيح
لا تدعم هيئة التصديق لتوقيع البرمجيات خيار حفظ المفاتيح.

4.12.2.سياسة وممارسات تغليف واستعادة مفتاح الجلسة
غير قابل للتطبيق.

5. الضوابط الخاصة بالمنشآت والإدارة والتشغيل

يوضح هذا القسم الضوابط الأمنية المادية والإجرائية التي تطبقها شركة مصدر التكنولوجيا ضمن عملياتها.

يتوافق برنامج إدارة الأمن الخاص بمجلس حوكمة البنية التحتية للمفاتيح العامة لمصدر التكنولوجيا مع متطلبات أمن الشبكة ونظام الشهادات الصادرة عن منتدى CA/Browser والتي تشمل ما يلي:

- الضوابط الأمنية المادية وضوابط البيئة.
- ضوابط سلامة النظام وتشمل إدارة التهيئة وتغييرات التكوين وإدارة التحديثات وإدارة الثغرات واكتشاف البرامج الضارة أو الفيروسات ومنعها.
- الحفاظ على سجل جرد بجميع الأصول وإدارتها وفقاً لتصنيفها.
- أمن الشبكة وإدارة الجدار الناري وتشمل تقييد المنافذ وتصفية عناوينIP .
- إدارة المستخدمين وتخصيص الأدوار الموثوقة بشكل منفصل وتوفير التوعية والتدريب.
- ضوابط الوصول المنطقي وتسجيل الأنشطة ومراقبتها ومراجعة صلاحيات المستخدمين بشكل دوري لضمان المساءلة الفردية.

يتضمن البرنامج الأمني لشركة مصدر التكنولوجيا تقييماً سنوياً للمخاطر يقوم بما يأتي:

1. تحديد التهديدات الداخلية والخارجية المتوقعة التي قد تؤدي إلى الوصول غير المصرح به، أو الإفصاح، أو سوء الاستخدام، أو التعديل، أو التدمير لأي من بيانات الشهادات أو عمليات إدارة الشهادات.

2. تقييم احتمالية وقوع هذه التهديدات والأضرار المحتملة الناجمة عنها، مع مراعاة درجة حساسية بيانات الشهادات وعمليات إدارة الشهادات.

3. تقييم كفاية السياسات، والإجراءات، وأنظمة المعلومات، والتقنيات، والترتيبات الأخرى التي تتبعها شركة مصدر التكنولوجيا لمواجهة تلك التهديدات.

وبناءً على تقييم المخاطر، تعمل شركة مصدر التكنولوجيا على إعداد وتنفيذ وصيانة خطة أمنية تتألف من إجراءات وتدابير ومنتجات أمنية مصممة لتحقيق الأهداف المذكورة أعلاه، ولإدارة والسيطرة على المخاطر المحددة خلال عملية التقييم، وبما يتناسب مع حساسية بيانات الشهادات وعمليات إدارة الشهادات.

تشتمل الخطة الأمنية على ضمانات إدارية، وتنظيمية، وفنية، ومادية ملائمة لحساسية بيانات الشهادات وعمليات إدارة الشهادات. كما تراعي الخطة التقنيات المتاحة وتكلفة تنفيذ تدابير محددة، وتعمل على تطبيق مستوى أمني معقول يتناسب مع الضرر الذي قد ينتج عن أي خرق أمني وطبيعة البيانات المراد حمايتها.

5.1.الضوابط الأمنية المادية

يضمن مجلس حوكمة البنية التحتية للمفاتيح العامة لمصدر التكنولوجيا تطبيق الضوابط المادية المناسبة في منشآت استضافة البنية التحتية للمفاتيح العامة. تُوثق هذه الضوابط ضمن السياسات الداخلية لشركة مصدر التكنولوجيا ويجري تطبيقها ومراجعتها بانتظام من خلال عمليات تدقيق داخلية ينفذها المجلس على فريق العمليات.

5.1.1.موقع المنشأة والبناء

تُستضيف جميع المكونات الحيوية للبنية التحتية للمفاتيح العامة داخل منشأة عالية التأمين تشغلها شركة مصدر التكنولوجيا.

تُطبق ضوابط أمنية مادية صارمة لمنع دخول الأشخاص غير المصرح لهم من خلال أربع طبقات أمنية. يوفر هذا النظام الطبقي عند دمجه مع وسائل الحماية المادية مثل الحراس وأجهزة استشعار التسلل والمراقبة بالكاميرات حماية قوية ضد الوصول غير المصرح به إلى أنظمة البنية التحتية للمفاتيح العامة الخاصة بمصدر التكنولوجيا. تقع منشآت الحوسبة التي تستضيف خدمات هيئة التصديق التابعة لشركة مصدر التكنولوجيا في بغداد في جمهورية العراق.

5.1.2.الوصول المادي

تحاط أنظمة هيئة التصديق الخاصة بشركة مصدر التكنولوجيا بضوابط أمنية مادية مكونة من أربع طبقات حيث لا يمكن الوصول إلى الطبقات الأدنى إلا بعد المرور من الطبقات الأعلى. نفذ الأنشطة التشغيلية الحساسة المرتبطة بإدارة دورة حياة الشهادات ضمن طبقات مادية مقيدة للغاية. يُسجل نظام التحكم بالوصول مرور الأفراد عبر كل طبقة.

تشمل ضوابط الأمن المادي ما يلي: مراقبة دخول المبنى من قبل حراس الأمن والمصادقة البيومترية والمراقبة بالكاميرات.

توفر هذه الضوابط الحماية لأنظمة هيئة التصديق ضد الدخول غير المصرح به وتُراقب على مدار الساعة وطوال أيام الأسبوع والسنة ما يوفر طبقات حماية متعددة للأشخاص عند الدخول والخروج من الموقع.

يُمنح الدخول إلى الموقع بعد تقديم بطاقة الهوية الوطنية ويتم التحقق منها من قبل حارس الأمن ويُسجل في السجل اسم الشخص ووقت الوصول والمغادرة وتُمنح له شارة زائر. لا يُسمح بالدخول إلا للأشخاص المفوضين من أحد أعضاء مجلس البنية التحتية للمفاتيح العامة ويجب أن يرافق الزائر موظف موثوق من شركة مصدر التكنولوجيا.

ولا يُفتح القفص الذي تُستضاف فيه أنظمة هيئة التصديق إلا في حال وجود اثنين من الموظفين الموثوقين لفتح الباب.

5.1.3.الطاقة وتكييف الهواء

يشتمل تصميم المنشأة التي تستضيف البنية التحتية للمفاتيح العامة الخاصة بمصدر التكنولوجيا على وحدات تزويد طاقة غير منقطعة (UPS) ومولدات احتياطية توفر القدرة الكافية لدعم تشغيل أنظمة البنية التحتية في حالات انقطاع التيار الكهربائي. تتوفر وحدات UPS والمولدات الاحتياطية لتغطية كامل المنشأة. رُكِبَ نظام تكييف هواء احتياطي بالكامل في المناطق التي تستضيف أنظمة البنية التحتية للمفاتيح العامة. تضمن هذه الأنظمة استمرار عمل معدات البنية التحتية ضمن نطاق درجات الحرارة والرطوبة المسموح بها من قبل المصنعين.

5.1.4.التعرض للمياه

اتخذ مجلس حوكمة البنية التحتية للمفاتيح العامة لمصدر التكنولوجيا احتياطات معقولة لتقليل تأثير التعرض للمياه على منشأة الاستضافة. يشمل ذلك تركيب معدات البنية التحتية على أرضيات مضادة للكهرباء الساكنة مزودة بكاشفات للرطوبة.

5.1.5.الوقاية من الحرائق والحماية منها

تتبع منشأة استضافة البنية التحتية للمفاتيح العامة أفضل الممارسات والأنظمة الوقائية المعمول بها في العراق وتُراقب على مدار الساعة وطوال أيام السنة. تُجهز المنشأة بمعدات للكشف عن الحرائق والحرارة. تُركب معدات إطفاء الحرائق في المناطق المخصصة وتُفعّل تلقائياً في حالة حدوث حريق ويمكن تفعيلها يدوياً عند الضرورة.

5.1.6.تخزين الوسائط

تخضع الوسائط الإلكترونية والبصرية وغيرها من وسائط التخزين للضوابط الأمنية المادية متعددة الطبقات وتُحمى من التلف العرضي بسبب الماء أو الحريق أو التداخل الكهرومغناطيسي. تُخزن وسائط التدقيق والنسخ الاحتياطي في خزنة مقاومة للحريق ومؤمنةوتُنسخ وتُنقل إلى موقع التعافي من الكوارث.

5.1.7.التخلص من النفايات

يُتلف كل ما يُنتج من نفايات ورقية أو وسائط تخزين داخل المنشأة الآمنة قبل التخلص منه. تُقطع الوسائط الورقية باستخدام آلة تمزيق بنمط متقاطع. تنطبق الإجراءات التالية على وسائط الحاسوب القابلة للإزالة:

- يُمنح الإذن لتدمير أي وسائط حاسوب قابلة للإزالة.
- تُمحى الوسائط ثم تُدمر مادياً في حال عدم الحاجة إليها.
- يُحتفظ بسجل لعملية تدمير هذه الوسائط.
- تُفرج الوسائط بعد ذلك لأغراض التخلص منها.

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

5.1.8.النسخ الاحتياطي خارج الموقع

تُنفذ نسخ احتياطية كاملة وتزايدية بشكل روتيني لأنظمة هيئة التصديق لتوقيع البرمجيات لضمان توفر بيانات كافية لاستعادة الأنظمة عند الحاجة.

تُؤخذ نسخة احتياطية كاملة واحدة على الأقل وعدة نسخ تزايدية يومياً لأنظمة الهيئة عبر الإنترنت وفقاً للسياسات والإجراءات الموثقة للنسخ الاحتياطي المعتمدة من قبل فريق عمليات البنية التحتية.

تُؤخذ نسخ احتياطية من المعلومات الأشد أهمية مثل المفاتيح الخاصة عند انتهاء أي مراسيم مفتاح وفقاً لنص موثق للمراسيم.

تُوفر مرافق نسخ احتياطي مناسبة لضمان نقل النسخ إلى موقع التعافي من الكوارث حيث تُخزن وفقاً لنفس الضوابط المادية والفنية والإجرائية المطبقة على الموقع الأساسي.

5.2.الضوابط الإجرائية

5.2.1.الأدوار الموثوقة

يُعد جميع أعضاء الفريق الذين يعملون في عمليات إدارة المفاتيح أو الإداريين أو ضباط الأمن أو أي أفراد آخرين يشاركون في عمليات تؤثر بشكل جوهري على تلك الأنشطة في موقع موثوق (أي عاملين موثوقين). يخضع جميع الأفراد المعينين في مناصب موثوقة لفحص خلفية قبل السماح لهم بمباشرة العمل في هذه المناصب. تُحفظ نتائج فحص الخلفية وتُراجع سنوياً.

الأدوار الموثوقة التالية معتمدة لدى هيئة التصديق لتوقيع البرمجيات الخاصة بشركة مصدر التكنولوجيا:

- مسؤول البنية التحتية للمفاتيح العامة (PKI Administrator): يمتلك بيانات اعتماد برنامج هيئة التصديق ويكون مسؤولاً عن تهيئة الهيئة وصيانتها.

- مشغل البنية التحتية للمفاتيح العامة (PKI Operator): مخوّل بتنفيذ دورة العمليات الخاصة بهيئة التصديق ويشارك في العمليات الحيوية مثل إصدار شهادات المشتركين.
- ضابط الأمن: يمتلك بيانات الاعتماد التي تتيح تهيئة جهاز توليد المفاتيح الشفرية (HSM) وتطبيق سياسات البنية التحتية على الأنظمة المستهدفة أثناء مراسيم إنشاء المفاتيح.
- ضابط التسجيل (RA Officer): مخوّل بتنفيذ إجراءات التحقق من طلبات الشهادات ضمن عملية معالجة طلبات الشهادات.
- حماة مفاتيح "م-من-ن" (M-of-N Custodians): يمتلكون بيانات تنشيط جهاز توليد المفاتيح الشفرية ويُعدّون حماة خزائن هيئات التصديق التابعة.
- مالك نطاق هيئة التصديق (CA Domain Owner): يمتلك بيانات الاعتماد التي تخوّله تنفيذ عمليات النسخ الاحتياطي والاستعادة لوحدة أمان معدات هيئة التصديق التابعة.
- مدقق جهاز توليد المفاتيح الشفرية (HSM Auditor): يمتلك بيانات اعتماد استرجاع سجلات التدقيق من جهاز توليد المفاتيح الشفرية.
- حماة مركز البيانات (Data Centre Custodians): أفراد يمتلكون بيانات اعتماد فتح مركز بيانات البنية التحتية أثناء تنفيذ عمليات هيئة التصديق.
- مدير النظام (System Administrator): مخوّل بتثبيت نظام التشغيل وتهيئته واستكشافه وصيانته مع بيئة قاعدة البيانات الداعمة.
- مدير الشبكة (Network Administrator): مخوّل بتثبيت مكونات الشبكة الداعمة وتهيئتها واستكشافها وصيانتها.

5.2.2.عدد الأشخاص المطلوب لكل مهمة

تتبع عمليات البنية التحتية للمفاتيح العامة لدى مصدر التكنولوجيا إجراءات رقابة صارمة لضمان الفصل بين الواجبات حسب مسؤولية الوظيفة بهدف منع تنفيذ العمليات الحساسة من قبل شخص موثوق واحد فقط.

تتطلب المهام الأكثر حساسية مشاركة شخصين على الأقل وتشمل ما يلي:

- الدخول المادي إلى القفص الآمن الذي تُستضاف فيه أنظمة هيئات التصديق التابعة.
- الوصول إلى جهاز توليد المفاتيح الشفرية التشفيرية الخاصة بهيئة التصديق وإدارتها.
- التحقق والموافقة على إصدار الشهادات.

تُسجّل جميع الأنشطة التشغيلية التي ينفذها الأفراد المعيّنون في أدوار موثوقة وتُحفظ ضمن سجل تدقيق آمن وقابل للتحقق.

5.2.3.التحقق من الهوية والمصادقة لكل دور

قبل تنفيذ المسؤوليات المترتبة على أي دور موثوق يقوم مجلس حوكمة البنية التحتية للمفاتيح العامة بالآتي:

- التأكد من هوية الموظف وتاريخه من خلال إجراء فحوصات خلفية وأمنية.
- عند صدور التعليمات من خلال إجراءات البنية التحتية الداخلية يصدر فريق تشغيل المنشأة بطاقة دخول لكل موظف يحتاج إلى وصول مادي إلى المعدات الموجودة داخل القفص الآمن.

يقوم الموظفون المختصون في البنية التحتية للمفاتيح العامة (مثل مديري النظام) بإصدار بيانات اعتماد أنظمة تكنولوجيا المعلومات اللازمة لموظفي هيئة التصديق لتوقيع البرمجيات لتنفيذ مهامهم.

5.2.4.الأدوار التي تتطلب الفصل في الواجبات

تُحدد الأدوار الموثوقة المذكورة في القسم 5.2.1 مع تطبيق مبدأ الفصل المناسب في الواجبات.

5.3.ضوابط الأفراد

5.3.1.المؤهلات والخبرة ومتطلبات التصريح

قبل تعيين أي فرد للعمل في إطار البنية التحتية للمفاتيح العامة لدى مصدر التكنولوجيا سواء كموظف أو وكيل أو متعاقد مستقل يتحقق مجلس حوكمة البنية التحتية من إجراء فحوصات لتحديد الخلفية والمؤهلات والخبرة اللازمة لأداء المهمة المطلوبة ضمن نطاق الكفاءة المحددة. تشمل هذه الفحوصات ما يلي:

- التحقق من هوية الشخص: ويجري من خلال:
  - الحضور الشخصي أمام أفراد موثوقين مسؤولين عن الموارد البشرية أو الأمن.
  - التحقق من وثائق هوية رسمية صادرة عن جهة حكومية ومزودة بصورة شخصية.
- التحقق من موثوقية الشخص: ويشمل فحوصات خلفية تغطي على الأقل الآتي أو ما يعادله:
  - الإدانات الجنائية في الجرائم الجسيمة.
  - أي تضليل أو تحريف من قبل المرشح.
  - مدى ملاءمة المراجع المقدمة.
  - أي تصاريح إضافية تُعد ضرورية حسب تقدير الجهة المختصة.

5.3.2.إجراءات التحقق من الخلفية

اختير جميع الموظفين الذين يشغلون أدواراً موثوقة استناداً إلى النزاهة والتحقيق في الخلفية والتصريح الأمني. يضمن مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا إجراء هذه الفحوصات مرة واحدة سنوياً لجميع العاملين في الأدوار الموثوقة.

5.3.3.متطلبات التدريب

يوفر مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا تدريباً فنياً أساسياً لموظفيه لتنفيذ مهامهم بفعالية. يُحدَّث هذا التدريب بانتظام ويُنفذ سنوياً لموظفي هيئة التصديق لتوقيع البرمجيات.

يشمل برنامج التدريب مجموعة متنوعة من المواضيع ويُقدَّم من قبل موظفين ذوي خبرة من هيئة التصديق لتوقيع البرمجيات وأطراف خارجية متخصصة في الأمن والبنية التحتية للمفاتيح العامة. صُمم هذا التدريب بعناية لتلبية متطلبات الأدوار الموثوقة المختلفة المشاركة في إدارة وتقديم خدمات هيئة التصديق لتوقيع البرمجيات. وتشمل المواضيع:

- نظريات ومبادئ البنية التحتية للمفاتيح العامة.
- ضوابط البيئة وسياسات الأمن للبنية التحتية للمفاتيح العامة.
- إجراءات هيئة التسجيل بما في ذلك التحقق من الهوية والإثباتات.
- العمليات التشغيلية للبنية التحتية للمفاتيح العامة.
- تدريب عملي على منتجات البنية التحتية للمفاتيح العامة.

- إجراءات التعافي من الكوارث واستمرارية الأعمال.

يحتفظ مجلس حوكمة البنية التحتية للمفاتيح العامة بسجل كامل بجميع الموظفين الذين خضعوا للتدريب ويقيّم دورياً مستوى رضا المدرّبين. في نهاية كل جلسة تدريبية تُنظم اختبارات وتُمنح شهادات للموظفين الذين يجتازون هذه الاختبارات. ويُشترط على جميع شاغلي الأدوار الموثوقة بما في ذلك متخصصي التحقق اجتياز هذه الاختبارات قبل منحهم صلاحية أداء أدوارهم.

5.3.4.تواتر ومتطلبات التدريب المتكرر

يُقدَّم منهاج التدريب لجميع أعضاء فريق البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا. ويُراجع محتوى التدريب ويُحدَّث سنوياً ليعكس أحدث الممارسات الرائدة وأية تغييرات في إعدادات أنظمة هيئات التصديق.

5.3.5.تواتر وتتابع تناوب الوظائف

يضمن مجلس حوكمة البنية التحتية للمفاتيح العامة أن أي تغيير أو تناوب في الموظفين لا يؤثر على فعالية تشغيل خدمات هيئة التصديق لتوقيع البرمجيات أو على استمراريتها أو نزاهتها.

5.3.6.العقوبات على الأفعال غير المصرح بها

لضمان المساءلة بين موظفي البنية التحتية للمفاتيح العامة يعاقب مجلس الحوكمة الأفراد على الأفعال غير المصرح بها أو على سوء استخدام السلطة أو الأنظمة وذلك وفقاً لسياسات وإجراءات الموارد البشرية المعمول بها والقوانين العراقية ذات الصلة.

5.3.7.متطلبات المتعاقدين المستقلين

يخضع المتعاقدون المستقلون وموظفوهم لنفس إجراءات التحقق من الخلفية المطبقة على موظفي البنية التحتية للمفاتيح العامة. وتشمل هذه الفحوصات:

- الإدانة بجرائم خطيرة.
- التحريف أو التضليل من قبل المرشح.
- مدى ملاءمة المراجع المقدمة.
- أي تصاريح تراها الهيئة ضرورية.
- حماية الخصوصية.
- شروط السرية.

5.3.8.الوثائق المقدمة للموظفين

وثّق مجلس حوكمة البنية التحتية للمفاتيح العامة في شركة مصدر التكنولوجيا جميع مواد التدريب ووفّرها لموظفي البنية التحتية للمفاتيح العامة.

وضمن المجلس كذلك توفير الوثائق التشغيلية الأساسية للموظفين المعنيين وتشمل في الحد الأدنى وثيقة بيان ممارسات الشهادات وسياسات الأمن وأدلة التشغيل والوثائق الفنية المرتبطة بكل دور موثوق.

5.4.إجراءات تسجيل السجلات التدقيقية

شملت إجراءات تسجيل السجلات التدقيقية تسجيل الأحداث وتدقيق الأنظمة ونُفذت بهدف الحفاظ على بيئة آمنة وشملت الأنشطة المتعلقة بإدارة دورة حياة المفاتيح بما في ذلك إنشاء المفاتيح أو نسخها احتياطياً أو تخزينها أو استعادتها أو إتلافها وإدارة الأجهزة التشفيرية وهيئة التصديق ومجيب بروتوكول OCSP.

أُنشئت ملفات تدقيق أمني لجميع الأحداث المرتبطة بأمن هيئة التصديق أو سلطة التسجيل أو مجيبي OCSP واحتُفظ بها وراجعها فريق ضباط الأمن في مصدر التكنولوجيا وخضعت أيضاً للمراجعة ضمن عمليات التدقيق الداخلي المنتظمة التي تنفذها وحدة الامتثال على عمليات هيئة التصديق لتوقيع البرمجيات.

5.4.1.أنواع الأحداث المسجلة

يتم إنشاء سجلات تدقيق لكافة الأحداث المتعلقة بأمن وخدمات أنظمة سلطة تصديق توقيع البرمجيات التابعة لشركة مصدر التكنولوجيا. كما تقوم شركة مصدر التكنولوجيا بتسجيل الأحداث المتعلقة بالإجراءات المتخذة لمعالجة طلب الشهادة وإصدارها، بما في ذلك كافة المعلومات المتولدة والوثائق المستلمة ذات الصلة بطلب الشهادة، مع تحديد الوقت والتاريخ والكوادر المعنية.

وتضع شركة مصدر التكنولوجيا هذه السجلات تحت تصرف مدقق الحسابات المؤهل كدليل على امتثال سلطة التصديق لهذه المتطلبات.

أُنشئت سجلات تدقيق لجميع الأحداث المرتبطة بأمن وخدمات أنظمة هيئة التصديق لتوقيع البرمجيات واحتوت كل سجل تدقيقي في الحد الأدنى على ما يلي:

- التاريخ والوقت الذي وقع فيه الحدث.
- مؤشر النجاح أو الفشل للحدث مثل توقيع من هيئة التصديق أو إلغاء شهادة أو التحقق من شهادة.
- هوية الجهة أو المشغّل الذي تسبب بالحدث.
- وصف الحدث.

وُلدت السجلات التدقيقية تلقائياً متى أمكن ذلك وإن تعذر الأمر استُخدم سجل يدوي أو استمارات ورقية واحتفظ فريق تشغيل البنية التحتية للمفاتيح العامة بالسجلات الإلكترونية وغير الإلكترونية وقد تُتاح أثناء تدقيقات الامتثال.

تُسجّل الأحداث التالية المتعلقة بعمليات هيئة التصديق لتوقيع البرمجيات:

أ. أحداث إدارة دورة حياة مفتاح هيئة التصديق لتوقيع البرمجيات وتشمل ما يلي:
1) إنشاء المفاتيح أو نسخها احتياطياً أو تخزينها أو استعادتها أو أرشفتها أو إتلافها.
2) أحداث إدارة دورة حياة الأجهزة التشفيرية.
3) طلبات الشهادات أو تجديدها أو إعادة إصدارها أو إلغاؤها.
4) الموافقة على طلبات الشهادات أو رفضها.
5) إنشاء قوائم إلغاء الشهادات.
6) توقيع استجابات بروتوكولOCSP .
7) إدخال ملفات تعريف شهادات جديدة أو إيقاف العمل بملفات تعريف شهادات حالية.

ب. أحداث إدارة دورة حياة شهادات هيئة التصديق لتوقيع البرمجيات وشهادات المشتركين وتشمل ما يلي:

1) طلبات الشهادات أو تجديدها أو إعادة إصدارها أو إلغاؤها.
2) جميع أنشطة التحقق المنصوص عليها في بيان ممارسات الشهادات.
3) قبول طلبات الشهادات أو رفضها.
4) إصدار الشهادات.

ج. الأحداث الأمنية وتشمل ما يلي:

1) محاولات الوصول الناجحة أو غير الناجحة إلى أنظمة البنية التحتية للمفاتيح العامة
2) الإجراءات المنفذة على أنظمة البنية التحتية للمفاتيح العامة أو أنظمة الأمن
3) مشكلات منصة النظام مثل الأعطال أو فشل الأجهزة أو أية حالات شاذة أخرى
4) تغييرات ملفات التعريف الأمنية
5) الأنشطة المرتبطة بالموجّهات أو جدران الحماية كما ورد في القسم 5.4.1.1
6) الدخول إلى موقع هيئة التصديق أو الخروج منه

يضمن مجلس حوكمة البنية التحتية للمفاتيح العامة في شركة مصدر التكنولوجيا كذلك الاحتفاظ بالمعلومات التالية التي لم تُنتج من قبل هيئة التصديق لتوقيع البرمجيات واحتُفظ بها إما إلكترونياً أو يدوياً من قبل فريق عمليات البنية التحتية للمفاتيح العامة:

- تبديلات أو تغييرات ملفات التعريف الأمنية لموظفي هيئة التصديق.
- جميع الإصدارات الخاصة بوثيقة بيان ممارسات الشهادات هذه.
- محاضر الاجتماعات.
- تقارير التدقيق الداخلي المتعلقة بالامتثال.
- الإصدارات الحالية والسابقة لأدلة إعداد وتشغيل هيئة التصديق لتوقيع البرمجيات.

5.4.1.1.سجلات أنشطة الموجهات وجدران الحماية

شُملت السجلات المتعلقة بأنشطة الموجهات وجدران الحماية بما يلي:

1. محاولات تسجيل الدخول الناجحة أو غير الناجحة إلى الموجهات أو جدران الحماية.
2. تسجيل جميع الإجراءات الإدارية المنفذة على الموجهات أو جدران الحماية بما في ذلك تغييرات التهيئة أو تحديثات البرمجيات الثابتة أو تعديلات التحكم في الوصول.
3. تسجيل جميع التغييرات التي أُجريت على قواعد جدران الحماية بما في ذلك الإضافات أو التعديلات أو الحذف.
4. تسجيل جميع الأحداث والأخطاء على النظام بما في ذلك أعطال الأجهزة أو توقفات البرمجيات أو إعادة تشغيل النظام.

5.4.2.تكرار معالجة السجلات

يضمن مجلس حوكمة البنية التحتية للمفاتيح العامة في شركة مصدر التكنولوجيا قيام الموظفين المخولين بمراجعة ملفات السجلات بشكل منتظم للتحقق من سلامتها وضمان التعرف على الأحداث الشاذة في الوقت المناسب. ونفذ المجلس دورة مراجعة للسجلات التدقيقية تتضمن على الأقل ما يلي:

- مراجعة فريق المراقبة والامتثال لسجلات التدقيق والأمن الخاصة بتطبيقات هيئة التصديق شهرياً.

- مراجعة فريق المراقبة والامتثال لسجلات التدقيق والأمن الخاصة بأنظمة هيئة التصديق المتصلة بالإنترنت مثل مجيب OCSP شهرياً للتحقق من سلامة عمليات التسجيل واختبار وظيفة المراقبة اليومية والتأكد من تشغيلها بالشكل الصحيح.
- مراجعة فريق المراقبة والامتثال لسجلات الدخول الفيزيائي وإدارة المستخدمين على أنظمة البنية التحتية للمفاتيح العامة في شركة مصدر التكنولوجيا كل ثلاثة أشهر للتحقق من سياسات الدخول الفيزيائي والمنطقي.
- تنفيذ وحدة التدقيق والامتثال التابعة لمجلس الحوكمة تدقيقاً داخلياً سنوياً على عمليات هيئة التصديق لتوقيع البرمجيات ويُطلب كجزء من هذا التدقيق الداخلي عينات من تقارير مراجعة السجلات وجميع السجلات التدقيقية التي جُمعت منذ آخر دورة تدقيق.
- جمع وأرشفة أدلة مراجعة السجلات التدقيقية ونتائج عمليات المراجعة والإجراءات التصحيحية المنفذة.

5.4.3.مدة الاحتفاظ بالسجلات التدقيقية

احتفظ فريق عمليات البنية التحتية للمفاتيح العامة في شركة مصدر التكنولوجيا بالسجلات لمدة لا تقل عن سنتين أو وفقاً لما ورد في القسم 5.5.2 وشملت ما يلي:

- سجلات أحداث إدارة دورة حياة شهادة هيئة التصديق ومفتاحها كما ورد في القسم 5.4.1(1) وذلك بعد تحقق أحد الشرطين الآتيين أيهما أتى لاحقاً:
  1) إتلاف المفتاح الخاص لهيئة التصديق.
  2) إلغاء أو انتهاء صلاحية آخر شهادة صادرة من هيئة التصديق ضمن مجموعة الشهادات التي تحتوي على امتداد X.509v3 basicConstraints ويتضمن حقل CA مضبوطاً على true وتتشارك المفتاح العام ذاته المرتبط بالمفتاح الخاص لهيئة التصديق.
- سجلات أحداث إدارة دورة حياة شهادة المشترك كما ورد في القسم 5.4.1(2) وذلك بعد إلغاء الشهادة أو انتهاء صلاحيتها.
- أي سجلات لأحداث أمنية كما ورد في القسم 5.4.1(3) وذلك بعد وقوع الحدث.

5.4.4.حماية سجلات التدقيق

حُميت سجلات التدقيق من خلال مزيج من الضوابط الأمنية الفيزيائية والإجرائية والفنية على النحو الآتي:

1. أنظمة هيئات التصديق التابعة في شركة مصدر التكنولوجيا أنشأت سجلات تدقيق محمية تشفيرياً.
2. جرت المحافظة على أمن سجلات التدقيق أثناء انتقالها عبر نظام النسخ الاحتياطي وعند أرشفتها.
3. فُرضت سياسات التحكم في الوصول على أنظمة البنية التحتية للمفاتيح العامة لضمان منح صلاحيات القراءة فقط للموظفين المخولين الذين تشمل مهامهم التشغيلية الاطلاع على هذه السجلات.
4. لم يُمنح الوصول إلى الأنظمة التي تُخزن فيها سجلات التدقيق إلا للأدوار المخولة وأمكن تتبّع أي محاولة للتلاعب بالسجلات إلى الموظف المعني في شركة مصدر التكنولوجيا.

5.4.5.إجراءات النسخ الاحتياطي لسجلات التدقيق

طُبّقت القواعد الآتية على النسخ الاحتياطي لسجلات التدقيق الخاصة بهيئات التصديق التابعة:

- خُزنت وسائط النسخ الاحتياطي محلياً في موقع هيئات التصديق التابعة ضمن موقع آمن.

- أُودعت نسخة ثانية من بيانات وسجلات التدقيق في موقع التعافي من الكوارث الذي يوفر أماناً فيزيائياً وبيئياً مماثلاً للموقع الرئيسي.

5.4.6.نظام جمع سجلات التدقيق (الداخلي مقابل الخارجي)

بدأت عمليات التدقيق التلقائية عند تشغيل النظام وانتهت عند إيقافه. وفي حال فشل نظام التدقيق الآلي وتعرضت سلامة النظام أو سرية المعلومات المحمية للخطر قرر مجلس الحوكمة ما إذا كان يجب تعليق عمليات هيئة التصديق المعنية لحين معالجة المشكلة.

5.4.7.الإخطار إلى مصدر الحدث

عند تسجيل حدث بواسطة نظام جمع السجلات التدقيقية لم يُشترط توجيه أي إشعار إلى الفرد أو الجهة أو الجهاز أو التطبيق الذي تسبب في الحدث.

5.4.8.تقييمات الثغرات الأمنية

أجرى فريق عمليات البنية التحتية للمفاتيح العامة تقييماً سنوياً للمخاطر شمل ما يلي:

1. تحديد التهديدات المتوقعة الداخلية أو الخارجية التي قد تؤدي إلى الوصول غير المصرح به أو الإفصاح أو سوء الاستخدام أو التعديل أو الإتلاف لبيانات الشهادات أو عمليات إدارتها.
2. تقييم احتمالية ومدى الضرر المحتمل لهذه التهديدات مع مراعاة حساسية بيانات الشهادات وعمليات إدارتها.
3. تقييم مدى كفاية السياسات والإجراءات والأنظمة المعلوماتية والتقنيات والترتيبات الأخرى التي طبقتها شركة مصدر التكنولوجيا للتصدي لتلك التهديدات.

وخضعت أنظمة وبُنى البنية التحتية للمفاتيح العامة لتقييمات أمنية منتظمة على النحو الآتي:

- خلال أسبوع واحد من تلقي طلب من منتدىCA/Browser .
- بعد أي تغييرات جوهرية على النظام أو الشبكة كما تُحددها هيئة التصديق.
- مرة واحدة على الأقل كل ثلاثة أشهر على عناوين IP العامة والخاصة المرتبطة بالنواة والبُنى الداعمة لهيئة التصديق لتوقيع البرمجيات.

نُفذ هذا التقييم الذاتي المنتظم من قبل أفراد الأمن ضمن فريق العمليات. وعلى أساس سنوي وبعد أي ترقيات أو تعديلات جوهرية على البنية التحتية أو التطبيقات كما يحدد مجلس الحوكمة نُظِّم تقييم مستقل للثغرات الأمنية واختبار اختراق بواسطة طرف ثالث.

قُدمت نتائج التقييمات المنتظمة والقضايا المحددة إلى مجلس الحوكمة وإدارة تشغيل البنية التحتية للمفاتيح العامة الذين تولوا تنظيم ومتابعة تنفيذ الإجراءات التصحيحية من قبل الفرق المعنية.

جُمعت وأُرشفت أدلة تنفيذ تقييمات الثغرات الأمنية واختبارات الاختراق من قبل موظفي هيئة التصديق لتوقيع البرمجيات المختصين.

5.5.أرشفة السجلات

5.5.1.أنواع السجلات المؤرشفة

أرشفت هيئات التصديق التابعة جميع سجلات التدقيق كما ورد 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 أو إصدار الشهادات أو إلغائها.

5.5.2.مدة الاحتفاظ بالأرشيف

احتُفظ بالسجلات المؤرشفة كما هو محدد في القسم 5.5.1 لمدة لا تقل عن سنتين وقد تمتد حتى سبع سنوات وذلك لضمان توفرها عند الحاجة للتحقيق في أي حوادث أمنية محتملة أو أحداث تتطلب مراجعة وتحليل للأنشطة السابقة.

بالإضافة إلى ذلك احتفظت هيئات التصديق التابعة بما يلي:

أ. جميع الوثائق المؤرشفة المرتبطة بأمن أنظمة هيئة التصديق وأنظمة إدارة الشهادات كما ورد في القسم 5.5.1
ب. جميع الوثائق المؤرشفة المتعلقة بالتحقق من الطلبات أو إصدار الشهادات أو إلغائها كما ورد في القسم 5.5.1 وذلك بعد تحقق أحد الشرطين الآتيين أيهما أتى لاحقاً:
   1) آخر مرة استُند فيها إلى هذه السجلات والوثائق في التحقق أو الإصدار أو الإلغاء.
   2) انتهاء صلاحية شهادات المشترك التي اعتمدت على هذه السجلات والوثائق.

5.5.3.حماية الأرشيف

أُرشفت السجلات بطريقة تضمن عدم إمكانية حذفها أو إتلافها ووضعت ضوابط تضمن السماح فقط للموظفين المخولين بإدارة الأرشيف دون الإخلال بسلامة أو أصالة أو سرية السجلات المحفوظة.

5.5.4.إجراءات النسخ الاحتياطي للأرشيف

احتُفظ بنسخة واحدة فقط من كل أرشيف رقمي في الموقع الرئيسي وموقع التعافي من الكوارث لهيئات التصديق التابعة. استخدم فريق العمليات إجراءات النسخ الاحتياطي والاستعادة والأرشفة التي وثّقت كيفية إنشاء معلومات الأرشيف ونقلها وتخزينها.

5.5.5.متطلبات ختم الزمني للسجلات

شمل كل حدث مُسجَّل أو مُؤرشف تاريخ ووقت وقوعه. وتزامن وقت أنظمة هيئات التصديق التابعة مع مصدر زمني مستمد من ساعة .GPS وبلغ إعداد خدمات ختم الزمني دقة تصل إلى زائد أو ناقص ثانية واحدة أو أفضل بالنسبة إلى التوقيت العالمي .UTC

كما طبّق فريق عمليات البنية التحتية للمفاتيح العامة إجراءً لفحص وتصحيح أي انحراف زمني في الساعات.

5.5.6.نظام جمع الأرشيف (داخلي أو خارجي)

اعتمد نظام جمع الأرشيف الخاص بهيئة التصديق لتوقيع البرمجيات على بنية داخلية.

5.5.7.إجراءات الحصول على معلومات الأرشيف والتحقق منها

سُمح فقط للموظفين المخولين والمصادق عليهم بالوصول إلى المواد المؤرشفة. استخدم فريق العمليات إجراءات النسخ الاحتياطي والاستعادة والأرشفة لهيئات التصديق التابعة والتي وثّقت كيفية إنشاء معلومات الأرشيف ونقلها وتخزينها. واحتوت هذه الإجراءات كذلك على تفاصيل نظام جمع الأرشيف.

5.6.تبديل المفاتيح

للتقليل من أثر اختراق المفتاح جرى تبديل مفتاح هيئة التصديق لتوقيع البرمجيات بتواتر يضمن أن تكون فترة صلاحية هيئة التصديق أطول من أقصى عمر افتراضي لشهادة المشترك بعد آخر عملية إصدار. يُرجى الرجوع إلى القسم 6.3.2 من وثيقة بيان ممارسات الشهادات هذه لمعرفة تواتر تبديل المفاتيح.

وُفر للمشتركين والأطراف المعتمدة المفتاح العام الجديد لهيئة التصديق عبر وسائل التوزيع الموضحة في الفصل 6.1.4.

ولغرض دعم إدارة إلغاء الشهادات المصدّرة احتُفظ بالمفاتيح الخاصة القديمة لهيئة التصديق إلى أن تنتهي صلاحية جميع الشهادات الموقعة بها.

5.7.الاستجابة للاختراقات واستعادة القدرة التشغيلية بعد الكوارث

5.7.1.إجراءات التعامل مع الحوادث والاختراقات

عند رصد محاولة اختراق أو أي شكل من أشكال التهديد لهيئة التصديق من قبل مجلس إدارة البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا بادر المجلس بإجراء تحقيق لتحديد طبيعة الحادث ومستوى الضرر:

- إذا اشتبه الفريق بحدوث اختراق في المفتاح الخاص لهيئة التصديق اعتمد الإجراءات الواردة في خطة استمرارية الأعمال واستعادة القدرة التشغيلية بعد الكوارث الخاصة بمصدر التكنولوجيا وفي الحالات الأخرى قيّم الفريق نطاق الضرر المحتمل لتحديد ما إذا اقتضى الأمر إعادة بناء هيئة التصديق أو إلغاء بعض الشهادات أو إعلان اختراق المفتاح الخاص.
- حدّد مجلس إدارة البنية التحتية إجراءات التبليغ عن الحادث ووسائل التواصل اللازمة وفقاً لخطة استمرارية الأعمال واستعادة القدرة التشغيلية بعد الكوارث.

وفي غير حالات اختراق المفاتيح وصف الفريق إجراءات الاستعادة المعتمدة عندما تتعرض الموارد الحاسوبية أو البرمجيات أو البيانات للتلف أو يظهر احتمال تلفها.

5.7.2.تلف الموارد الحاسوبية أو البرمجيات أو البيانات

نفذت مصدر التكنولوجيا التدابير الضرورية لاستعادة خدمات هيئات التصديق التابعة لها بالكامل عند حدوث كارثة أو تلف في الخوادم أو البرمجيات أو البيانات وذلك بعد حصولها على موافقة من مجلس إدارة البنية التحتية لتفعيل إجراءات الاستجابة للحوادث.

وضّحت وثيقة استمرارية الأعمال واستعادة القدرة التشغيلية بعد الكوارث الظروف التي استدعت تفعيل هذه الإجراءات وبيّنت الحالات التي تطلبت استخدام موقع الاستعادة.

اختبرت مصدر التكنولوجيا خطة الاستعادة مرة واحدة على الأقل خلال كل سنة وشمل الاختبار تنفيذ سيناريوهات التحويل إلى موقع الاستعادة.

5.7.3.إجراءات اختراق المفتاح الخاص للجهة

بالنسبة لاختراق مفتاح المشترك راجع القسم 4.9.

عدّت مصدر التكنولوجيا اختراق المفتاح الخاص لهيئة التصديق لتوقيع البرمجيات أو بيانات التفعيل المرتبطة به أو شهادة مستجيب OCSP حادثاً بالغ الخطورة استدعى تفعيل الإجراءات الموضحة في خطة استمرارية الأعمال واستعادة القدرة التشغيلية بعد الكوارث.

نظراً لخطورة الحادث وتأثيره على البنية التحتية الوطنية للمفاتيح العامة في العراق عقد مجلس إدارة البنية التحتية اجتماعاً طارئاً لاتخاذ قرارات فورية وتنفيذ الاتصالات الرسمية اللازمة ضمن خطط التعامل مع اختراق المفاتيح أو إنهاء عمل هيئة التصديق وراجع القسمين 4.9.1 و4.9.3 لمزيد من التفاصيل.

5.7.4. قدرات استمرارية الأعمال بعد الكوارث

عند وقوع كارثة أو تلف في الخوادم أو البرمجيات أو البيانات فعّلت مصدر التكنولوجيا خطة استعادة القدرة التشغيلية واستمرارية الأعمال لاسترجاع الحد الأدنى من القدرات التشغيلية المطلوبة لهيئة التصديق لتوقيع البرمجيات في الوقت المناسب. وركزت الخطة على استعادة الخدمات الآتية سواء في الموقع الرئيسي أو في موقع الاستعادة:

- خدمات التصديق (الإصدار والإلغاء)
- المستودع العام الذي نُشرت فيه قوائم إلغاء الشهادات وشهادات هيئات التصديق
- خدماتOCSP

مكّنت سيناريوهات التحويل إلى موقع الاستعادة التابع لمصدر التكنولوجيا من خلال نظام النسخ الاحتياطي الخاص بهيئة التصديق لتوقيع البرمجيات الذي دعم النسخ المتواصل للبيانات الحيوية من الموقع الرئيسي إلى موقع الاستعادة. وساهم هذا الإجراء في استعادة الخدمات الحرجة لهيئة التصديق لتوقيع البرمجيات في موقع الاستعادة خلال فترة لا تتجاوز اثنتي عشرة (12) ساعة وفق هدف وقت الاستعادة المحدد.

وضعت خطة استمرارية الأعمال لمصدر التكنولوجيا البنود التالية:

- شروط تفعيل الخطة.
- الإجراءات الطارئة.
- إجراءات الرجوع.
- إجراءات الاستئناف.
- جدول صيانة للخطة.
- متطلبات التوعية والتعليم.
- مسؤوليات الأفراد.
- هدف وقت الاستعادة(RTO) .
- اختبارات دورية لخطط الطوارئ.

- خطة الحفاظ على أو استعادة العمليات التشغيلية لهيئة التصديق لتوقيع البرمجيات في الوقت المناسب بعد توقف العمليات أو فشل العمليات التجارية الحرجة.
- اشتراط تخزين المواد التشفيرية الحيوية مثل الجهاز التشفيري الآمن ومواد التفعيل في موقع بديل.
- تحديد ما يُعد توقفاً مقبولاً للنظام والفترة اللازمة للاستعادة.
- وتيرة أخذ نسخ احتياطية من معلومات العمل الأساسية والبرمجيات.
- المسافة بين مرافق الاستعادة والموقع الرئيسي.
- الإجراءات المتبعة لحماية المرافق قدر الإمكان خلال الفترة الممتدة بعد الكارثة وحتى استعادة بيئة آمنة سواء في الموقع الأصلي أو في موقع بعيد.

لا تفصح شركة مصدر التكنولوجيا عن خطط استمرارية الأعمال للمشتركين، أو الأطراف المعتمدة، أو مزودي برامج التطبيقات، ولكنها ستقوم بتزويد المدققين بخطة استمرارية الأعمال والخطط الأمنية بناءً على طلبهم.

5.8.إنهاء عمل هيئة التصديق أو هيئة التسجيل

أنهت مصدر التكنولوجيا تقديم خدمات هيئة التصديق لتوقيع البرمجيات في الحالات التالية:

أ. بناءً على قرار صادر عن الإدارة التنفيذية لمصدر التكنولوجيا.
ب. بقرار مبرر صادر عن الهيئة المشرفة وهي الشركة العامة للاتصالات والمعلوماتية.
ج. بناءً على قرار قضائي نهائي لا يقبل الطعن.
د. بعد تصفية أو إنهاء عمليات هيئة التصديق لتوقيع البرمجيات.

إذا قرر مجلس إدارة البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا أو مدير لجنة إدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية ضرورة إنهاء خدمات هيئة التصديق لتوقيع البرمجيات نفذ المجلس خطة الإنهاء المتفق عليها مسبقاً مع الشركة العامة للاتصالات والمعلوماتية.

غطت خطة الإنهاء الحد الأدنى من النقاط التالية:

- إرسال إشعار خطي إلى مدير لجنة إدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية حول نية التوقف عن ممارسة أنشطة هيئة التصديق وإرفاق نسخة من خطة الإنهاء الخاصة بمصدر التكنولوجيا قبل تسعين (90) يوماً على الأقل من:
  - التاريخ المتوقع للتوقف عن تنفيذ أنشطة هيئة التصديق.
  - انتهاء صلاحية تفويض مصدر التكنولوجيا لممارسة أنشطة هيئة التصديق إن وجدت دون نية لتجديد التفويض.
- ترتيب مصدر التكنولوجيا لحفظ سجلات الأرشفة وفقاً لما ورد في القسم 5.5.
- ترتيب مقدم خدمات الثقة للحفاظ على روابط خدمات التحقق من حالة الشهادات كما وردت في الشهادات الصالحة للفترة المقررة بعد الإنهاء.
- الإعلان عن نية مصدر التكنولوجيا لإنهاء أنشطة هيئة التصديق لتوقيع البرمجيات في الصحف اليومية أو من خلال الوسائل التي يحددها مدير لجنة إدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية وذلك قبل ستين (60) يوماً على الأقل من تاريخ الإنهاء الفعلي أو انتهاء التفويض أيهما أسبق.

- تنفيذ الاتصالات اللازمة مع الأطراف المعنية وترتيب نقل سجلات هيئة التصديق المؤرشفة إلى جهة وصاية مناسبة.
- وضع خطة لدعم المشتركين الحاليين لمصدر التكنولوجيا قدر الإمكان خلال انتقالهم إلى مقدم خدمات ثقة آخر.
- إلغاء جميع الشهادات غير الملغاة أو غير المنتهية التي صدرت عن هذه الهيئة في نهاية فترة الإشعار بغض النظر عن طلب المشتركين لذلك.
- اتخاذ التدابير اللازمة لضمان عدم التسبب في أي اضطراب للمشتركين أو الأطراف المعتمدة نتيجة توقف العمليات.
- وضع ترتيبات تضمن بشكل كافٍ الاستمرار في صيانة الأنظمة وتنفيذ التدابير الأمنية المتعلقة بالبيانات الحساسة والدقيقة.

6. الضوابط الأمنية التقنية

6.1.تولید أزواج المفاتيح وتركيبها

6.1.1.تولید أزواج المفاتيح

6.1.1.1.تولید زوج مفاتيح هيئة التصديق

أنشأت هيئة التصديق لتوقيع البرمجيات التابعة لمصدر التكنولوجيا زوج مفاتيحها داخل ذاكرة جهاز تشفير معتمد وفق المعيار FIPS 140-2 بالمستوى الثالث.

سجّلت مراسيم توليد مفاتيح هيئة التصديق لتوقيع البرمجيات بالفيديو واحتُفظ بها في موقع آمن لأغراض التدقيق.

شهد مدقق داخلي أو خارجي مراسيم توليد مفاتيح هيئة التصديق لتوقيع البرمجيات بهدف إصدار تقرير يبيّن ما يلي:

1. وثّقت مصدر التكنولوجيا إجراءات توليد وحماية مفاتيح هيئة التصديق وفقاً لما ورد في بيان ممارسة الشهادات هذا وسياسة الشهادات الخاصة بمقدم خدمات الثقة.
2. أدرجت تفاصيل مناسبة في نص إجراءات توليد مفاتيح هيئة التصديق.
3. نفذت الإجراءات بحضور النصاب القانوني من الأشخاص المخولين بما في ذلك ممثلو مجلس إدارة البنية التحتية للمفاتيح العامة.
4. حافظت على ضوابط فعّالة توفر ضماناً معقولاً بأن توليد وحماية زوج مفاتيح هيئة التصديق جرى بما يتوافق مع الإجراءات الموضحة في هذا البيان والبيانات الأخرى ذات الصلة.
5. نفذت خلال عملية توليد المفاتيح جميع الإجراءات المنصوص عليها في نص توليد مفاتيح هيئة التصديق.

6.1.1.2.تولید زوج مفاتيح المشترك.

لم تقدم هذه الهيئة خدمات توليد مفاتيح المشترك. تولى المشترك توليد المفتاح الخاص لشهادة توقيع البرمجيات واستخدامه وتخزينه في وحدة تشفير استوفت أو تجاوزت متطلبات معيار FIPS 140-2 بالمستوى الثاني أو معيار Common Criteria EAL 4+.

6.1.2.تسليم المفتاح الخاص إلى المشترك

لا تنشئ شركة مصدر التكنولوجيا المفاتيح الخاصة بالمشتركين لشهادات توقيع البرمجيات الموثوقة عاماً، كما أنها لا تقوم بإجراءات إيداع المفاتيح أو استعادتها أو الاحتفاظ بنسخ احتياطية منها.

وفي حال كشفت شركة مصدر التكنولوجيا أو اشتبهت في تسريب المفتاح الخاص للمشترك إلى شخص غير مخول أو منظمة غير تابعة للمشترك، فإن شركة مصدر التكنولوجيا تقوم بإلغاء كافة الشهادات التي تتضمن المفتاح العام المقابل للمفتاح الخاص المسرب.

6.1.3.تسليم المفتاح العام إلى مصدر الشهادة

قبلت هيئة التصديق لتوقيع البرمجيات التابعة لمصدر التكنولوجيا طلبات توقيع الشهادات فقط بعد التأكد من توثيق هذه الطلبات داخل بوابة هيئة التسجيل الإلكترونية.

6.1.4.تسليم المفتاح العام لهيئة التصديق إلى الأطراف المعتمدة

نُشرت شهادات المفتاح العام لهيئة التصديق لتوقيع البرمجيات التابعة لمصدر التكنولوجيا في المستودع العام الخاص بمصدر التكنولوجيا.

6.1.5.نوع الخوارزمية وحجم المفاتيح

6.1.5.1.هيئة التصديق لتوقيع البرمجيات

استخدمت هيئة التصديق لتوقيع البرمجيات خوارزمية ECDSA بحجم 348 بت.

6.1.5.2.المشتركون

اشترطت مصدر التكنولوجيا ألا يقل حجم مفتاح RSA للمشترك عن 3072 بت.

6.1.6.توليد معلمات المفتاح العام والتحقق من جودتها

6.1.6.1.هيئة التصديق لتوقيع البرمجيات

ولّدت هيئة التصديق المفاتيح الخاصة والعامة باستخدام أحدث آليات توليد المعلمات. استوفت وحدات HSM والبرمجيات المرتبطة بها في هيئة التصديق لتوقيع البرمجيات متطلبات المعيار FIPS 186-2 الخاصة بالتوليد العشوائي واختبارات أولية الأعداد. استند فريق عمليات البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا إلى القسم 6.1.6 من متطلبات الأساس للتحقق من الجودة.

6.1.6.2.المشتركون

اعتمدت هيئة التسجيل في مصدر التكنولوجيا تقنيات معقولة للتحقق من صلاحية المفاتيح العامة المقدّمة من المشتركين. واختبرت المفاتيح الضعيفة المعروفة ورفضتها وفقاً لما ورد في القسم 6.1.6 من متطلبات الأساس لمنتدى CA/B.

6.1.7. أغراض استخدام المفاتيح (وفقاً لحقل الاستخدام في شهادةX.509 v3)

احتوت الشهادات الصادرة عن هذه الهيئة على سلسلة بتات لاستخدام المفتاح وفقاً للمواصفة .[RFC 5280] راجع القسمين 7.1 و7.3 من بيان ممارسة الشهادات هذا.

6.2. حماية المفتاح الخاص وضوابط تصميم وحدات التشفير

6.2.1.معايير وضوابط وحدة التشفير

استخدمت مصدر التكنولوجيا وحدات أمنية عتادية معتمدة أو متوافقة مع معيار FIPS 140-2 بالمستوى الثالث لإنشاء المفاتيح الخاصة بهيئة التصديق لتوقيع البرمجيات وتخزينها. وخُزّنت وحدات HSM في المنطقة الأكثر أماناً والأعمق ضمن منشأة استضافة البنية التحتية للمفاتيح العامة التابعة لمصدر التكنولوجيا.

وفيما يخص المفاتيح الخاصة بالمشتركين طُبّق ما ورد في القسم 6.1.1.2.

6.2.2.التحكم الجماعي في المفتاح الخاص باستخدام نموذج (م من ن).

أخضعت مصدر التكنولوجيا المفاتيح الخاصة بهيئة التصديق لتوقيع البرمجيات لرقابة دائمة من قبل عدة أشخاص مخولين. وثّقت الأدوار الموثوقة المرتبطة بإدارة المفاتيح الخاصة والأسرار ذات الصلة ضمن إجراءات توليد المفاتيح الخاصة بها ووثائقها الداخلية الأخرى. عيّن مجلس إدارة البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا موظفي هيئة التصديق لتوقيع البرمجيات في الأدوار الموثوقة بما يضمن الفصل بين المهام وتطبيق مبدأ الرقابة المتعددة ومعرفة المعلومات بشكل مجزأ. وحققت الهيئة التحكم الجماعي في المفاتيح الخاصة باستخدام نموذج معرفة مجزأة من نوع (م من ن)، حيث احتاجت العملية إلى وجود عدد معين من الأشخاص (م) لا يقل عن اثنين (2) من أصل ثلاثة (3) أشخاص (العدد الكلي لحاملي المفاتيح) بالتزامن مع مديري وحدات HSM لتفعيل المفتاح الخاص لهيئة التصديق التابعة.

احتفظ مجلس إدارة البنية التحتية بسجلات مكتوبة وقابلة للتدقيق حول توزيع الرموز السرية وكلمات المرور المرتبطة بها على الموظفين الموثوقين وحاملي المفاتيح. وعند استبدال أي منهم وثّق المجلس الرموز أو كلمات المرور المجددة.

6.2.3.الاحتفاظ بالمفتاح الخاص لأغراض الأمان

لم تحتفظ هيئة التصديق لتوقيع البرمجيات بالمفاتيح الخاصة لأغراض الأمان.

6.2.4.النسخ الاحتياطي للمفتاح الخاص

نسخت هيئة التصديق لتوقيع البرمجيات مفاتيحها الخاصة واحتفظت بها في خزائن مخصصة مؤمنة داخل المناطق الأمنية الأعمق في مرافق استضافة هيئات التصديق التابعة لمصدر التكنولوجيا.

نفّذت عمليات النسخ الاحتياطي كجزء من مراسيم توليد المفاتيح، وأُجري النسخ الاحتياطي تحت نفس ضوابط التحكم الجماعي ومعرفة المعلومات المجزأة المفروضة على المفتاح الأساسي. وخضعت عملية استرجاع المفاتيح الاحتياطية لنفس المبادئ.

شملت مراسيم توليد المفاتيح أيضاً نقل النسخة الاحتياطية مادياً من موقع المصدر إلى موقع الاستعادة بمرافقة حراس أمن وضمن إشراف أشخاص موثوقين. وراعى الفريق الضوابط الموضحة في القسم 6.2.2 أثناء عملية النقل.

6.2.5.أرشفة المفتاح الخاص

لم تحتفظ هيئة التصديق لتوقيع البرمجيات بمفاتيحها الخاصة في الأرشيف.

6.2.6.نقل المفتاح الخاص إلى أو من وحدة تشفير

نقلت الهيئة أزواج المفاتيح الخاصة فقط إلى وحدة تشفير عتادية أخرى من نفس المواصفات الموضحة في القسم 6.2.11 باستخدام النسخ المباشر من وحدة إلى وحدة عبر مسار موثوق وتحت إشراف عدة أشخاص.

ولم تُنسخ المفاتيح الخاصة إلى الأقراص أو أي وسائط أخرى خلال هذه العملية في أي وقت.

6.2.7. تخزين المفتاح الخاص في وحدة التشفير

6.2.7.1.تخزين المفتاح الخاص لمفاتيح هيئة التصديق

لم تُدرج شروط إضافية غير الواردة في البنود 6.2.1 و6.2.2 و6.2.4 و6.2.6.

شهادة مستجيب :OCSP وُلّد زوج مفاتيح OCSP داخل ذاكرة وحدة أمان عتادية معتمدة وفق معيار FIPS 140-2 بالمستوى الثالث.

6.2.7.2.حماية والتحقق من المفتاح الخاص للمشترك.

حماية المفتاح الخاص للمشترك.

ضمنت مصدر التكنولوجيا توليد المفتاح الخاص لشهادة توقيع البرمجيات واستخدامه وتخزينه بطريقة صحيحة ضمن وحدة تشفير تستوفي أو تتجاوز متطلبات FIPS 140-2 بالمستوى الثاني أو معيار Common Criteria EAL 4+ وذلك من خلال الآتي:

- استخدم المشترك وحدة تشفير عتادية تستوفي المتطلبات المحددة.
- استخدم المشترك حلاً قائماً على السحابة لتوليد وحماية المفتاح يتضمن ما يلي:
  - احتفظ بتوليد المفتاح الخاص وتخزينه واستخدامه داخل الحدود الأمنية لوحدة التشفير العتادية لحل الحوسبة السحابية المتوافق مع المتطلبات المحددة في هذا القسم.
  - فعّل الاشتراك بمستوى يتيح تسجيل كل عمليات الوصول والتشغيل والتعديلات التي تُجرى على الموارد التي تحمي المفتاح الخاص.
- استخدم المشترك خدمة توقيع تستوفي متطلبات القسم 6.2.7.3 من وثيقة "متطلبات الأساس لإصدار وإدارة شهادات توقيع البرمجيات المعتمدة علنياً".

<u>التحقق من المفتاح الخاص للمشترك</u>

اعتمدت هيئة التسجيل التابعة لمصدر التكنولوجيا أحد الخيارات الموضحة في القسم 6.2.7.4.2 من وثيقة "متطلبات الأساس لإصدار وإدارة شهادات توقيع البرمجيات المعتمدة علنياً" لضمان أن المفتاح الخاص للمشترك قد جرى توليده وتخزينه واستخدامه ضمن وحدة تشفير عتادية مناسبة تستوفي أو تتجاوز المتطلبات المحددة في القسم 6.2.7.4.1.

6.2.8.طريقة تفعيل المفتاح الخاص

6.2.8.1.هيئة التصديق لتوقيع البرمجيات

فعّلت المفاتيح الخاصة وفقاً لمبادئ الرقابة المزدوجة ومعرفة المعلومات المجزأة. واستخدمت إجراء التفعيل جهاز إدخال PINموصولاً بوحدة HSM الخاصة بهيئة التصديق.

6.2.8.2.المشتركون

تحمل المشتركون مسؤولية تفعيل مفاتيحهم الخاصة وحمايتها وفق الالتزامات المنصوص عليها في شروط واحكام استخدام المشترك.

6.2.9.طريقة إلغاء تفعيل المفتاح الخاص

6.2.9.1.هيئة التصديق لتوقيع البرمجيات

ألغت مصدر التكنولوجيا تفعيل المفاتيح الخاصة لهيئة التصديق وفقاً للتعليمات والوثائق التي قدّمها مصنع وحدة الأمان العتادية.

6.2.9.2.المشتركون

تحمّل المشتركون مسؤولية إلغاء تفعيل مفاتيحهم الخاصة وحماية الوصول إلى أزواج مفاتيحهم وفقاً للالتزامات المحددة في شروط واحكام استخدام المشترك.

6.2.10.طريقة إتلاف المفتاح الخاص

6.2.10.1.هيئة التصديق لتوقيع البرمجيات

نفّذت عملية إتلاف المفتاح الخاص لهيئة التصديق قبل انتهاء فترة صلاحيته فقط في حال وجود تحقيق أو تفويض خاص صادر عن مجلس إدارة البنية التحتية للمفاتيح العامة. واشتمل قرار الإتلاف على تحديد الأفراد المكلفين بالتنفيذ.

تخضع عملية الإتلاف لإجراءات موثقة، ويجب أن تشمل أفراداً مكلفين بمهام ائتمانية؛ وبحد أدنى ثلاثة أعضاء من الكادر الائتماني، مع حضور ممثل واحد على الأقل من الهيئة الإدارية للبنية التحتية للمفاتيح العامة. بالإضافة إلى ذلك، يجب أن تتم عملية الإتلاف تحت إشراف مدقق حسابات مؤهل.

نفّذت إجراءات إتلاف مفاتيح هيئة التصديق لتوقيع البرمجيات من خلال خطوات موثقة شملت مشاركة أفراد في أدوار موثوقة (ثلاثة موظفين على الأقل) وبحضور ممثل واحد على الأقل من مجلس إدارة البنية التحتية. وفرضت هذه الإجراءات مبدأ الرقابة المتعددة ومعرفة المعلومات المجزأة. كما ضمنت إزالة المفاتيح نهائياً من جميع الوحدات العتادية التي خُزّنت عليها.

6.2.10.2.المشتركون

تحمّل المشتركون مسؤولية إتلاف مفاتيحهم وفقاً للالتزامات المحددة في شروط واحكام استخدام المشترك.

6.2.11.تصنيف وحدات التشفير

حصلت وحدات التشفير التابعة لهيئة التصديق لتوقيع البرمجيات على اعتماد وفق معيار FIPS 140-2 بالمستوى الثالث.

6.3.جوانب أخرى من إدارة أزواج المفاتيح

6.3.1.أرشفة المفتاح العام

راجع البند 5.5 للاطلاع على شروط الأرشفة.

6.3.2.فترات صلاحية الشهادات وفترات استخدام أزواج المفاتيح

تكون شهادات هيئة التصديق لتوقيع البرمجيات صالحة لمدة ست (6) سنوات، بينما تمتد فترة استخدام المفاتيح الخاصة لثلاث (3) سنوات.

لا يُستخدم المفتاح الخاص لهيئة التصديق التابعة بعد انتهاء صلاحية شهادة المفتاح العام المرتبطة به. ولا يُستخدم كذلك في توقيع شهادات الكيانات النهائية بعد انتهاء فترة استخدام المفتاح الخاص، باستثناء توقيع قوائم إلغاء الشهادات وشهادات مستجيب OCSP لخدمة التحقق من صلاحية الشهادات.

حددت مدة الصلاحية القصوى لشهادة توقيع البرمجيات الخاصة بالمشترك في القسم 7.1.

6.4. بيانات التفعيل

6.4.1.تولید بيانات التفعيل وتركيبها

6.4.1.1.هيئة التصديق لتوقيع البرمجيات

ولّدت المفاتيح الخاصة لهيئة التصديق وبيانات التفعيل الخاصة بوحدة HSM خلال مراسيم توليد المفاتيح الخاصة. راجع القسمين 6.1.1 و6.2.8 من هذا البيان لمزيد من التفاصيل.

6.4.1.2.المشتركون

حدّد المشتركون بيانات التفعيل الخاصة بمفاتيحهم الخاصة وحموها بالدرجة الكافية لمنع فقدانها أو سرقتها أو الكشف غير المصرح به عنها أو استخدامها. واشتملت شروط واحكام استخدام المشترك على هذا الالتزام.

6.4.2.حماية بيانات التفعيل

6.4.2.1.هيئة التصديق لتوقيع البرمجيات

ضمنت سياسة إدارة المفاتيح وإجراءات المراسيم الخاصة بهيئات التصديق التابعة لمصدر التكنولوجيا تطبيق مبدأ الرقابة المتعددة ومعرفة المعلومات المجزأة بشكل دائم لحماية مفاتيح هيئة التصديق وبيانات تفعيل وحدات HSM. واحتفظ موظفو الهيئات التابعة المعينون ببيانات التفعيل تحت إشرافهم الدائم خلال مراسيم توليد المفاتيح. راجع القسمين 6.1 و6.2 لمزيد من التفاصيل.

6.4.2.2.المشتركون

حمى المشتركون بيانات التفعيل لمفاتيحهم الخاصة بالدرجة الكافية لمنع فقدانها أو سرقتها أو الكشف غير المصرح به عنها أو استخدامها. واشتملت شروط واحكام استخدام المشترك على هذا الالتزام.

6.4.3.جوانب أخرى لبيانات التفعيل

لم يُذكر شرط خاص.

6.5.ضوابط أمن الحواسيب

6.5.1.متطلبات أمن الحواسيب التقنية المحددة

ضمنت مصدر التكنولوجيا تنفيذ ضوابط أمن الحواسيب وفقاً للمعايير التقنية وإرشادات تعزيز الأمان من مزودي الحلول كحد أدنى.

وثّقت الضوابط الأمنية للحواسيب كجزء من السياسات الداخلية لهيئات التصديق التابعة لمصدر التكنولوجيا.

وخضعت أنظمة هيئات التصديق التابعة وعملياتها لضوابط الأمان التالية:

1. فصل المهام وتطبيق الرقابة المزدوجة على عمليات هيئة التصديق.
2. فرض الرقابة على الوصول الفعلي والمنطقي.
3. تدقيق الأحداث المرتبطة بالتطبيق والأمان.
4. المراقبة المستمرة لأنظمة هيئات التصديق التابعة وحماية نقاط النهاية.
5. آليات النسخ الاحتياطي والاستعادة لعمليات هيئات التصديق التابعة.
6. تعزيز نظام تشغيل خوادم هيئات التصديق التابعة وفق أفضل الممارسات وتوصيات المزودين.
7. بنية أمنية شبكية عميقة تشمل جدران حماية محيطية وداخلية وجدران حماية لتطبيقات الويب وأنظمة كشف التسلل.
8. إدارة استباقية للتحديثات الأمنية ضمن العمليات التشغيلية لهيئات التصديق التابعة.
9. فرض المصادقة متعددة العوامل على جميع الحسابات القادرة على إصدار الشهادات بشكل مباشر.

6.5.2.تصنيف أمن الحواسيب

خضعت الجوانب التقنية لأمن الحواسيب لعمليات تدقيق دورية.

6.6.الضوابط التقنية لدورة الحياة

6.6.1.ضوابط تطوير الأنظمة

استُلمت المعدات والبرمجيات التي تم شراؤها في حاويات مختومة مقاومة للعبث، وركّبها موظفون مؤهلون. وجرى اقتناء تحديثات المعدات والبرمجيات بنفس الأسلوب المتبع عند الحصول على المعدات الأصلية. وشارك موظفون موثوقون مخصصون في تنفيذ التهيئة المطلوبة لهيئات التصديق التابعة وفقاً لإجراءات تشغيل موثقة.

واختُبرت التطبيقات وطُوّرت ونُفّذت بما يتوافق مع أفضل الممارسات في الصناعة لإدارة التطوير والتغيير. ولم تُنشر أي برمجيات أو ترقيات أو معدات على الأنظمة الحية قبل المرور عبر عمليات إدارة التغيير والتهيئة المفروضة من قبل فريق عمليات البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا.

وعُزّزت جميع منصات المعدات والبرمجيات الخاصة بهيئات التصديق التابعة باستخدام أفضل ممارسات الصناعة وتوصيات المزودين.

6.6.2.ضوابط إدارة الأمان

خُصصت المعدات والبرمجيات المستخدمة في إعداد هيئات التصديق التابعة لمصدر التكنولوجيا لتنفيذ مهام هيئة التصديق فقط. ولم تُوصل أو تُركب أي تطبيقات أو أجهزة أو اتصالات شبكية أو مكونات برمجية أخرى لا تنتمي إلى البنية التحتية للمفاتيح العامة التابعة لمصدر التكنولوجيا على أجهزة هيئات التصديق.

وطُبقت عملية إدارة التهيئة لضمان توثيق وضبط تهيئة وتعديل وترقية أنظمة هيئات التصديق التابعة من قبل إدارة عمليات البنية التحتية.

وطُبقت عملية إدارة الثغرات لضمان فحص معدات هيئات التصديق التابعة لاكتشاف البرمجيات الضارة عند أول استخدام وبشكل دوري بعد ذلك. ودعمت هذه العملية معالجة الثغرات الحرجة خلال مدة لا تتجاوز ست وتسعين (96) ساعة من اكتشافها في حال لم يعالجها فريق عمليات البنية التحتية سابقاً.

6.6.3.ضوابط الأمان لدورة الحياة

راجع القسم 6.5.1.

6.7.ضوابط أمن الشبكة

نفّذت مصدر التكنولوجيا ضوابط قوية لأمن الشبكات شملت جدران حماية مُدارة وأنظمة كشف التسلل. وقُسمت الشبكة إلى عدة مناطق استناداً إلى علاقاتها الوظيفية والمنطقية والمادية. وفُرضت حدود بين الشبكات للحد من الاتصال بين الأنظمة داخل المناطق وكذلك بين المناطق المختلفة، وذلك عبر قواعد تسمح فقط بالخدمات والبروتوكولات والمنافذ والاتصالات التي حددتها هيئات التصديق التابعة كمطلوبة لعملياتها، وعُطّلت جميع الحسابات والتطبيقات والخدمات والبروتوكولات والمنافذ غير المستخدمة في عمليات هيئات التصديق.

وتُجرى عمليات فحص الثغرات الأمنية للشبكات بصورة ربع سنوية على الأقل، كما تُنفذ اختبارات الاختراق سنوياً كحد أدنى. وتستند جداول المعالجة الزمنية إلى درجة الخطورة؛ حيث يتم التعامل مع الثغرات الحرجة خلال (24) ساعة، والثغرات عالية الخطورة خلال (48) ساعة، بينما يتم معالجة المشكلات ذات الخطورة المنخفضة والمتوسطة خلال (96) ساعة. ويتم توثيق أي استثناءات، وتقييم مخاطرها، وتسجيلها بشكل رسمي. ضعت أنظمة الإصدار وأنظمة إدارة الشهادات وأنظمة دعم الأمان ضمن منطقة شبكية عالية الأمان.

6.8.الطابع الزمني

جرى مزامنة مكونات هيئة التصديق لتوقيع البرمجيات التابعة لمصدر التكنولوجيا بشكل منتظم مع خدمة توقيت موثوقة. وبلغ إعداد خدمات الطابع الزمني دقة تصل إلى ثانية واحدة (+/- 1 ثانية) أو أفضل مقارنة بالتوقيت العالمي المنسق UTC.

7. الشهادات وقوائم الإلغاء وخدمات التحقق عبرOCSP

7.1.ملف الشهادة

7.1.1.رقم النسخة

أصدرت هيئات التصديق التابعة لمصدر التكنولوجيا شهادات X.509 بالإصدار الثالث وفقاً لما ورد في المعيارRFC 5280 .

7.1.2.امتدادات الشهادة

امتثلت مصدر التكنولوجيا للمعيار RFC 5280 ولمتطلبات الأساس لإصدار وإدارة شهادات توقيع البرمجيات المعتمدة علنياً في جميع الشهادات الصادرة عنها.

واحتوت شهادات هيئات التصديق التابعة وشهادات الكيانات النهائية لأغراض توقيع البرمجيات على امتداد "الاستخدام الممتد للمفتاح" يتضمن الغرضid-kp-codeSigning ولم تُدرج القيمة AnyExtendedKeyUsage ضمن حقول الاستخدام الممتد للمفتاح في الشهادات.

7.1.3.معرفات خوارزمية التوقيع

أصدرت هيئة التصديق الشهادات باستخدام البرمجيات المحددة بالمعرفات التالية:

الخوارزمية	معرف الكائن (Object Identifier)
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

7.1.4. صيغ الأسماء

7.1.4.1.ترميز الاسم

أصدرت مصدر التكنولوجيا الشهادات باستخدام صيغ أسماء متوافقة مع المعيار RFC 5280 والبند 7.1.4 من متطلبات الأساس.

7.1.4.2.معلومات الموضوع – شهادات المشتركين

بيّنت الجدول الآتي المعلومات الخاصة بحقول اسم الموضوع DN الخاصة بشهادات توقيع البرمجيات وختم الزمني. وأصدرت مصدر التكنولوجيا الشهادات بما يتوافق مع التعاريف المحددة في القسم 7.1.4 من متطلبات الأساس.

نوع الشهادة	حقول اسم الموضوع Subject DN
شهادات توقيع البرمجيات	• الاسم المشترك. • اسم المؤسسة. • اسم المدينة أو اسم المحافظة. • اسم الدولة

.

7.1.4.3.معلومات الموضوع – شهادات هيئات التصديق التابعة لمصدر التكنولوجيا

احتوت شهادات هيئة التصديق لتوقيع البرمجيات على الحقول commonName و organizationName و countryName. وشكّلت هذه الحقول عند دمجها معرفاً يميز الهيئة بشكل فريد عن غيرها من هيئات التصديق.

7.1.5.قيود الاسم

لم يُذكر شرط خاص.

7.1.6.معرف سياسة الشهادة(OID)

استخدمت مصدر التكنولوجيا مخطط OID محدد ضمن سياسة البنية التحتية للمفاتيح العامة الوطنية العراقية. وورد مزيد من التفاصيل في قالب الشهادة المشار إليه.

واستخدمت المعرفات التالية أيضاً:

سياسات شهادات الكيانات النهائية	الغرض
2.23.140.1.4.1	سياسة مخصصة لشهادات توقيع البرمجيات

7.1.7. استخدام امتداد قيود السياسة

لم يُذكر شرط خاص.

7.1.8.صياغة وتأويل مؤهلات السياسة

احتوت شهادات توقيع البرمجيات الصادرة عن مصدر التكنولوجيا على مؤهل سياسة CPS يشير إلى بيان ممارسة الشهادة المطبّق. وحددت مؤهلات السياسة المستخدمة ضمن ملفات تعريف الشهادات في القسمين 7.1.10 و7.1.11.

7.1.9.تأويل معاني سياسات الشهادات الحرجة

لم يُذكر شرط خاص.

7.1.10.ملف تعريف شهادة هيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا

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 CS 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 06 years
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

					As defined in BR.
CommonName		M	S	TS CS 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/cs_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/cs_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	
Policy Properties					
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.4.1	CA/B BR Reserved Certificate Policy for Code Signing
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	
Extended Key Usage Properties					
extKeyUsage	False	M	S		
codeSigning		M	S	True	
Basic Constraints Properties					

basicConstraints		True	M	S		
	cA		M	S	True	
	pathLenConstraint		M	S	0	

7.1.11.ملف تعريف شهادات توقيع البرمجيات

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	CS Subordinate CA Signature.	CS 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 CS 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	
Subject	False				
CountryName		M	D	Country Name	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Organization name of the legal entity	UTF8 encoded As defined in BR.
localityName		M/O	D	Locality	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
stateOrProvinceName		M/O	D	State Or Province	UTF8 encoded. Mandatory if the localityName field is not present, optional if the

					localityName is present.
CommonName		M	D	Subject's legal name	UTF8 encoded As defined in BR.
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/cs_ca.p7b	Subordinate Issuing CA Certificate/Chain

					download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/cs_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160 bit SHA 1 hash of the SubjectPublicKey	
Key Usage Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.23.140.1.4.1	CA/B BR Reserved Certificate Policy for Code Signing
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.2.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.1.3.2.2	
Extended Key Usage Properties					
extKeyUsage	False	M			

	codeSigning		M	S	True	

7.2.ملف تعريف قائمة إلغاء الشهادات

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 CS 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 الإصدار

تدعم هيئة التصديق قوائم إلغاء الشهادات بالإصدار الثاني من X.509 .

7.2.2.امتدادات قائمة إلغاء الشهادات وسجلاته

ورد ملف قائمة إلغاء الشهادات في القسم 7.2 أعلاه.

7.3.ملف تعريف بروتوكول حالة الشهادات عبر الإنترنت

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 CS 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 CS 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 حالة الشهادات عبر الإنترنت

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.

8تدقيق الامتثال والتقييمات الأخرى

تستهدف الإجراءات الموضحة في سياسة ممارسات التصديق هذه التوافق مع المتطلبات المحددة في القسم (1)، وتغطي كافة العناصر المعمول بها في المعايير الحالية للبنية التحتية للمفاتيح العامة ذات الصلة بالقطاعات الصناعية التي تعمل فيها شركة مصدر التكنولوجيا.

7.4.وتيرة أو ظروف التقييم

نظّمت مصدر التكنولوجيا تدقيقاً خارجياً عبر WebTrust لضمان التزامها بالمتطلبات والمعايير والإجراءات ومستويات الخدمة المعتمدة، وذلك مرة واحدة على الأقل سنوياً وقبلت مصدر التكنولوجيا تدقيق ممارساتها وإجراءاتها، وأتاحت تقرير التدقيق للجمهور خلال مدة لا تتجاوز ثلاثة أشهر من نهاية فترة التدقيق. وقيّم كل من مجلس إدارة البنية التحتية للمفاتيح العامة واللجنة العليا لإدارة التوقيع الإلكتروني PMA التابعة للشركة العامة للاتصالات والمعلوماتية نتائج هذه التدقيقات قبل تنفيذ ما يترتب عليها من إجراءات.

وأُجريت أيضاً تدقيقات داخلية وفق خطة تدقيق معتمدة من وفي حالات خاصة مثل حدوث خرق أمني، جرى تنفيذ تدقيقات غير مخطط لها بناءً على طلب من اللجنة العليا لإدارة التوقيع الإلكتروني PMA.

7.5.هوية أو مؤهلات المدقق

نُفذت التدقيقات الخارجية من قبل مدققين مؤهلين استوفوا المتطلبات التالية:

- الاستقلال الكامل عن الجهة الخاضعة للتدقيق.
- القدرة على إجراء تدقيق يغطي المعايير المحددة في معيارWebTrust .
- توظيف أفراد يمتلكون الكفاءة في تقنيات البنية التحتية للمفاتيح العامة، وأدوات وتقنيات أمن المعلومات، وتدقيق أمن تقنية المعلومات، ومهام التصديق من طرف ثالث.
- الحصول على ترخيص منWebTrust .
- الالتزام بالقانون أو اللوائح الحكومية أو المدونة المهنية للأخلاقيات.
- امتلاك تأمين مهني ضد الأخطاء والإهمال بقيمة لا تقل عن مليون دولار أمريكي، باستثناء هيئات التدقيق الحكومية الداخلية.

7.6.علاقة المدقق بالجهة الخاضعة للتدقيق

خصّص مجلس إدارة البنية التحتية للمفاتيح العامة وظيفة تدقيق داخلية مستقلة تماماً عن فريق عمليات البنية التحتية.

واعتمدت التدقيقات الخارجية على مدققين مستقلين من جهات WebTrust دون أي ارتباط مباشر أو غير مباشر مع مصدر التكنولوجيا أو أي طرف آخر لديه مصالح متعارضة في هذا السياق.

7.7.المواضيع المشمولة في التقييم

خضعت هذه الهيئة لتدقيقات امتثال للمعايير التالية:

- مبادئ ومعايير WebTrust الخاصة بهيئات التصديق.
- مبادئ ومعايير WebTrust الخاصة بهيئات التصديق – متطلبات الأساس لتوقيع البرمجيات.
- مبادئ ومعايير WebTrust الخاصة بهيئات التصديق – أمن الشبكات.

راجع القسم 8.1 للاطلاع على وتيرة التدقيقات، والقسم 8.2 للاطلاع على مؤهلات المدقق.

7.8.الإجراءات المتخذة نتيجة أوجه القصور

رُفعت المشكلات والاستنتاجات الناتجة عن التقييم إلى مجلس إدارة البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا.

وفيما يخص تدقيقات امتثال عمليات هيئة التصديق لتوقيع البرمجيات، أدّت أي استثناءات أو نواقص جوهرية اكتُشفت أثناء التدقيق إلى إصدار قرار بالإجراءات اللازمة. وصدر هذا القرار عن مجلس إدارة البنية التحتية بعد التشاور مع المدقق. وفي حال وجود استثناءات أو نواقص، تولى المجلس مسؤولية إعداد وتنفيذ خطة إجراءات تصحيحية. وبعد تنفيذ الخطة، بادر المجلس بإجراء تدقيق إضافي لضمان معالجة جميع أوجه القصور المحددة.

7.9.إيصال نتائج التدقيق

أُدرجت النتائج العامة للتدقيقات من قبل مجلس إدارة البنية التحتية على المستودع العام التابع لمصدر التكنولوجيا ورُفعت تقارير التدقيق الداخلي إلى مجلس إدارة البنية التحتية، ولم تُفصح لأي أطراف ثالثة غير مخوّلة.

تُنشر تقارير تدقيق (ويب-ترست) السنوية للعامة في مدة لا تتجاوز ثلاثة (3) أشهر من تاريخ انتهاء فترة التدقيق. وفي حال حدوث تأخير يتجاوز الثلاثة (3) أشهر، تقوم شركة مصدر التكنولوجيا بتقديم خطاب توضيحي موقع من قبل مدقق الحسابات المؤهل. ويمكن الاطلاع على تقارير تدقيق (ويب-ترست) الخاصة بشركة مصدر التكنولوجيا عبر الرابط الآتي:

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

7.10.التدقيق الذاتي

راقب مجلس إدارة البنية التحتية للمفاتيح العامة، من خلال وظيفة الامتثال الخاصة به، مدى التزامه بالإجراءات المدرجة في هذا البيان من خلال تنفيذ ما يلي:

- تدقيقات ذاتية على عينات عشوائية تُشكل ثلاثة بالمئة على الأقل من الشهادات التي أصدرتها هيئة التصديق لتوقيع البرمجيات، بدءاً من الفترة التي تلت مباشرة آخر عينة سُحِبت.

8. شؤون قانونية وتجارية أخرى

8.1. الرسوم

8.1.1.رسوم إصدار الشهادات أو تجديدها

تُحدد الرسوم المطبقة، إن وُجدت، بالاتفاق بين مصدر التكنولوجيا والمشتركين.

8.1.2.رسوم الوصول إلى الشهادات

لم يُذكر شرط خاص.

8.1.3.رسوم إلغاء الشهادات أو الوصول إلى معلومات الحالة

لم تُفرض أي رسوم مقابل إلغاء الشهادات أو الوصول إلى معلومات حالتها.

8.1.4.رسوم الخدمات الأخرى

يجوز لمصدر التكنولوجيا فرض رسوم على خدمات أخرى حسب احتياجات العمل.

8.1.5.سياسة الاسترداد

لا تُقدّم أي مبالغ مستردة عن الرسوم المدفوعة.

8.2.المسؤولية المالية

8.2.1.تغطية التأمين

ضمنت مصدر التكنولوجيا شمول هيئة التصديق لتوقيع البرمجيات بتغطية تأمينية قائمة.

8.2.2.أصول أخرى

لم يُذكر شرط خاص.

8.2.3.تغطية تأمينية أو ضمان للمشتركين النهائيين

راجع القسم 9.6.1.

8.3.سرية المعلومات التجارية

8.3.1.نطاق المعلومات السرية

اعتبرت مصدر التكنولوجيا المعلومات التالية معلومات سرية:

- المعلومات الشخصية للمشترك التي لا تظهر في الشهادات أو قوائم الإلغاء.
- المراسلات مع وظيفة التسجيل خلال عمليات إدارة الشهادات (بما في ذلك بيانات المشترك المُجمّعة).
- الاتفاقيات التعاقدية بين مصدر التكنولوجيا والمورّدين.
- الوثائق الداخلية لمصدر التكنولوجيا (إجراءات العمل والإجراءات التشغيلية...).
- المعلومات السرية الخاصة بالموظفين.

8.3.2.المعلومات الخارجة عن نطاق السرية

تعتبر مصدر التكنولوجيا أي معلومات لم تُصنّف على أنها سرية معلومات عامة. وشمل ذلك المعلومات المنشورة على المستودع العام لمصدر التكنولوجيا.

8.3.3.المسؤولية عن حماية المعلومات السرية

تحمي مصدر التكنولوجيا المعلومات السرية من خلال تدريب الموظفين وتطبيق السياسات على الموظفين والمتعاقدين والمورّدين.

8.4.خصوصية المعلومات الشخصية

8.4.1.خطة الخصوصية

تلتزم مصدر التكنولوجيا بقواعد خصوصية البيانات الشخصية وقواعد السرية كما وردت في هذا البيان. ونفّذت مصدر التكنولوجيا هذه الأحكام من خلال وظيفة التسجيل التابعة لها.

راجع القسم 9.4.2 لتحديد نطاق المعلومات الخاصة، والقسم 9.4.3 لتحديد العناصر غير المصنفة على أنها معلومات خاصة.

وتخضع كل من المعلومات الخاصة وغير الخاصة لقواعد خصوصية البيانات إذا احتوت على بيانات شخصية. وسُمح فقط لأفراد موثوقين ومحدودين بالوصول إلى معلومات المشتركين الخاصة لأغراض إدارة دورة حياة الشهادة.

تحترم مصدر التكنولوجيا جميع القوانين والأنظمة المطبقة المتعلقة بالخصوصية والمعلومات الخاصة وأسرار التجارة أينما كان ذلك ممكناً بالإضافة إلى سياسة الخصوصية المنشورة الخاصة بها عند جمع واستخدام وحفظ وكشف المعلومات غير العامة.

ولن تكشف مصدر التكنولوجيا أي معلومات خاصة للمشتركين سوى ما يتعلق بهم شخصياً ووفقاً لما نصّت عليه الاتفاقيات التعاقدية بينهم وبين مصدر التكنولوجيا.

ولن تُفرج مصدر التكنولوجيا عن أي معلومات خاصة دون موافقة صريحة من مالك البيانات الشرعي أو أمر قضائي صريح. وعند الإفراج عن المعلومات الخاصة تضمن مصدر التكنولوجيا عبر وسائل معقولة استخدام هذه المعلومات فقط للأغراض المحددة المطلوبة. تتولى الأطراف المصرّح لها الوصول إلى المعلومات مسؤولية حماية البيانات الخاصة من أي اختراق وامتنعت عن استخدامها أو مشاركتها مع أي أطراف ثالثة. ووجب على هذه الأطراف الالتزام بقواعد خصوصية البيانات الشخصية وفق القوانين المعمول بها في جمهورية العراق.

تحافظ جميع قنوات الاتصال مع مصدر التكنولوجيا على خصوصية وسرية أي معلومات خاصة تم تبادلها. واستُخدم التشفير عند التواصل الإلكتروني مع أنظمة هيئة التصديق لتوقيع البرمجيات. وشمل ذلك:

- الاتصالات بين أنظمة التسجيل ومشتركي الشهادات.
- الاتصالات بين أنظمة التسجيل وأنظمة هيئة التصديق لتوقيع البرمجيات.
- الجلسات المخصصة لتسليم الشهادات.

8.5.الإقرارات والضمانات

8.5.1.إقرارات وضمانات هيئة التصديق

عند إصدار شهادة قدّمت هيئة التصديق لتوقيع البرمجيات الضمانات التالية لمستفيدي الشهادات.

- المشترك الذي أبرم اتفاقية مشترك.
- جميع مورّدي البرمجيات الذين أبرموا اتفاقاً مع الهيئة الجذرية الوطنية العراقية لإدراج الشهادة الجذرية في البرمجيات التي يوزعونها.
- جميع الأطراف المعتمدة التي اعتمدت بشكل معقول على شهادة صالحة.

أقرّ مجلس إدارة البنية التحتية للمفاتيح العامة بأن هيئة التصديق لتوقيع البرمجيات التزمت بمتطلبات الأساس وببيان ممارسات الشهادة عند إصدار الشهادة وإدارتها خلال فترة صلاحيتها.

وشملت الضمانات ما يلي.

- **الامتثال**: التزمت الهيئة بمتطلبات الأساس لتوقيع البرمجيات وبسياسة الشهادة المعتمدة وبيان الممارسات المعتمد عند إصدار كل شهادة وتشغيل البنية التحتية للمفاتيح العامة.
- **هوية المشترك**: عند الإصدار طبّقت الهيئة أو خدمة التوقيع إجراء للتحقق من هوية المشترك يلبي على الأقل المتطلبات المحددة في القسم 3.2 واتّبعت هذا الإجراء بالكامل ووصفت هذا الإجراء بدقة في هذا البيان.
- **تفويض الشهادة**: عند الإصدار تحقّقت الهيئة من أن مقدم الطلب فوّض إصدار الشهادة واتّبعت هذا الإجراء ووصفت هذا الإجراء بدقة في هذا البيان.
- **صحة المعلومات**: عند الإصدار تحقّقت الهيئة من صحة ودقة جميع المعلومات المدرجة في الشهادة باستثناء الحقل subject:organizationalUnitName واتّبعت هذا الإجراء ووصفت هذا الإجراء بدقة في هذا البيان.
- **حماية المفتاح**: زوّدت الهيئة المشترك عند الإصدار بوثائق توضّح كيفية تخزين مفاتيح التوقيع الخاصة وحمايتها من سوء الاستخدام أو في حال استخدام خدمة توقيع قامت الهيئة بتخزين هذه المفاتيح ومنعت إساءة استخدامها.
- **شروط واحكام استخدام المشترك**: أبرمت الهيئة أو خدمة التوقيع اتفاقية مشترك قانونية وصالحة مع مقدم الطلب تحقق المتطلبات المحددة أو في حال وجود علاقة ارتباط أقر ممثل مقدم الطلب بشروط الاستخدام وقَبِل بها.
- **الحالة**: حافظت الهيئة على مستودع عام متاح على مدار الساعة طيلة أيام الأسبوع يحتوي على معلومات حالية حول الشهادات الصالحة أو الملغاة.
- **الإلغاء**: ألغت الهيئة الشهادة عند تحقق أي من الأسباب المحددة في هذا البيان.

8.5.2.إقرارات وضمانات وظيفة التسجيل

أقرت مصدر التكنولوجيا بأنها تؤدي وظائف التسجيل وفقاً للأحكام المنصوص عليها في هذا البيان.

8.5.3.إقرارات وضمانات المشترك

نفّذت مصدر التكنولوجيا إجراءً يضمن أن كل اتفاقية مشترك أو شروط استخدام تكون ملزمة قانوناً لمقدم الطلب. وينبغي أن تنطبق الاتفاقية على الشهادة المطلوب إصدارها وفقاً لطلب الشهادة. ويُستخدم اتفاق مستقل لكل طلب شهادة. وتحتوي شروط واحكام استخدام المشترك أو شروط الاستخدام على أحكام تُلزم مقدم الطلب نفسه أو تُقدّم نيابةً عن صاحب العمل أو العميل بموجب علاقة تعهيد أو استضافة بالالتزامات والضمانات التالية:

- دقة المعلومات: التزام وضمان بتقديم معلومات دقيقة وكاملة في جميع الأوقات إلى وظيفة التسجيل سواء في طلب الشهادة أو بناءً على طلب مصدر التكنولوجيا.
- حماية المفتاح الخاص: التزام وضمان من مقدم الطلب باتخاذ جميع التدابير المعقولة لضمان التحكم بالمفتاح الخاص والحفاظ عليه بسرية وتأمينه بشكل مناسب في جميع الأوقات وفقاً للقسم 6.2.7.2 بما في ذلك بيانات التفعيل أو الجهاز المرتبط مثل كلمات المرور أو الرموز.
- منع إساءة الاستخدام: التزام وضمان بتوفير حماية أمنية للشبكة والأنظمة الأخرى لمنع إساءة استخدام المفتاح الخاص وأن مصدر التكنولوجيا سيلغي الشهادة دون إشعار مسبق إذا تم الوصول غير المصرّح به إلى المفاتيح الخاصة.
- قبول الشهادة: التزام وضمان بمراجعة محتوى الشهادة والتحقق من دقته.

- استخدام الشهادة: التزام وضمان باستخدام الشهادة والمفتاح الخاص المرتبط بها فقط لأغراض قانونية ومصرّح بها بما في ذلك الامتناع عن استخدام الشهادة لتوقيع شيفرة مشبوهة واستخدامها بما يتوافق مع القوانين المعمول بها وشروط الاتفاقية.
- الإبلاغ والإلغاء: التزام وضمان بالتوقف الفوري عن استخدام الشهادة والمفتاح الخاص المرتبط بها وتقديم طلب إلغاء للشهادة فوراً في حال اعتقد المشترك أن أياً من المعلومات الواردة في الشهادة غير صحيحة أو أن المفتاح الخاص المرتبط بالمفتاح العام قد أُخترق أو أن الشهادة استُخدمت لتوقيع شيفرة مشبوهة.
- مشاركة المعلومات: التزام وضمان بأنه إذا حُدِدت الشهادة أو مقدم الطلب كمصدر لشيفرة مشبوهة أو تعذّر التحقق من صلاحية إصدار الشهادة أو أُلغيت الشهادة لأسباب غير متعلقة بطلب المشترك مثل اختراق المفتاح الخاص أو اكتشاف برامج خبيثة فإن مصدر التكنولوجيا مخوّل بمشاركة المعلومات المتعلقة بمقدم الطلب أو التطبيق الموقع أو الشهادة أو الظروف المحيطة مع هيئات تصديق أخرى أو مجموعات صناعية مثل منتدى المتصفحات وهيئات التصديق.
- إنهاء استخدام الشهادة: التزام وضمان بالتوقف الفوري عن استخدام المفتاح الخاص المرتبط بالمفتاح العام الوارد في الشهادة عند انتهاء صلاحيتها أو إلغائها.
- الاستجابة: التزام بالاستجابة لتعليمات مصدر التكنولوجيا المتعلقة باختراق المفاتيح أو إساءة استخدام الشهادة خلال فترة زمنية محددة.
- الإقرار والقبول: إقرار وقبول بأن مصدر التكنولوجيا يملك الحق في إلغاء الشهادة فوراً إذا خالف مقدم الطلب شروط شروط واحكام استخدام المشترك أو شروط الاستخدام أو إذا تطلب الإلغاء وفقاً لهذا البيان.

8.5.4.إقرارات وضمانات الأطراف المعتمدة

الأطراف المعتمدة التي تعتمد على الشهادات الصادرة عن مصدر التكنولوجيا تلتزم بما يلي:

- استخدام الشهادة للغرض الذي أُصدرت من أجله كما هو مبيّن في معلومات الشهادة مثل امتداد استخدام المفتاح.
- التحقق من صلاحية الشهادة من خلال التأكد من عدم انتهائها.
- التحقق من مسار الثقة وفق معايير التحقق المحددة في المعيار X.509 الإصدار الثالث.
- التأكد من أن الشهادة لم تُلغَ عبر الاطلاع على حالة الإلغاء من الموقع المحدد في الشهادة.
- التأكد من أن الشهادة توفّر مستوى كافياً من الضمانات بالنسبة للغرض المطلوب استخدامها فيه.

8.5.5.إقرارات وضمانات المشاركين الآخرين

لم يُذكر شرط خاص.

8.6.إخلاء المسؤولية من الضمانات

في حدود القانون العراقي وباستثناء حالات الاحتيال أو الإساءات المتعمدة لا تتحمّل مصدر التكنولوجيا المسؤولية عما يلي:

- دقة أي معلومات واردة في الشهادات إلا بالقدر الذي يضمنه المشترك الذي يتحمل مسؤولية صحة ودقة جميع البيانات التي يرسلها إلى مصدر التكنولوجيا بغرض إدراجها في شهادة صادرة عن هيئة التصديق.
- أي أضرار غير مباشرة ناتجة عن أو مرتبطة باستخدام الشهادات أو إصدارها أو عدم إصدارها أو تقديم التواقيع الرقمية.
- الأفعال المتعمدة لأي طرف ثالث ينتهك القوانين المعمول بها في العراق بما في ذلك على سبيل المثال لا الحصر قوانين حماية الملكية الفكرية أو البرمجيات الخبيثة أو الوصول غير القانوني إلى أنظمة الحاسوب.

- أي أضرار مباشرة أو غير مباشرة ناتجة عن انقطاع لا يمكن السيطرة عليه في خدمات هيئة التصديق لتوقيع البرمجيات.
- أي تحريف للمعلومات من قبل المشتركين أو الأطراف المعتمدة بناءً على المعلومات الواردة في هذا البيان أو أي وثائق أخرى صادرة عن مجلس إدارة البنية التحتية للمفاتيح العامة والمتعلقة بخدمات هيئة التصديق لتوقيع البرمجيات.

8.7.حدود المسؤولية

- لا تتحمّل مصدر التكنولوجيا أي مسؤولية تجاه المشتركين إذا كانت المسؤولية ناتجة عن إهمالهم أو احتيالهم أو سوء نيتهم.
- لا تتحمّل مصدر التكنولوجيا أي مسؤولية عن استخدام الشهادات أو أزواج المفاتيح العامة والخاصة المرتبطة بها لأي استخدام غير متوافق مع هذا البيان ويتعيّن على المشتركين تعويض مصدر التكنولوجيا عن أي مسؤوليات أو تكاليف أو مطالبات ناتجة عن ذلك.
- لا تتحمّل مصدر التكنولوجيا أي مسؤولية تجاه أي طرف عن أي أضرار ناتجة مباشرة أو غير مباشرة عن انقطاع لا يمكن السيطرة عليه في خدماتها.
- يتحمّل المشترك المسؤولية عن أي تحريف للمعلومات الواردة في الشهادة تجاه الأطراف المعتمدة حتى وإن كانت تلك المعلومات قد قُبلت من قبل مصدر التكنولوجيا.
- يتعيّن على المشترك تعويض أي طرف معتمد تكبّد خسارة نتيجة لخرق المشترك لشروط واحكام استخدام المشترك.
- يتحمّل الطرف المعتمد نتائج عدم الالتزام بواجباته.
- تنفي مصدر التكنولوجيا أي مسؤولية مالية أو من أي نوع عن الأضرار أو الأضرار الجانبية الناتجة عن تشغيل هيئة التصديق لتوقيع البرمجيات.

8.8.التعويضات

لا ينطبق.

8.9.المدة والإنهاء

8.9.1.المدة

أُقرّ هذا البيان من قبل مجلس إدارة البنية التحتية للمفاتيح العامة ويظل ساري المفعول حتى يُنشر تعديل له على المستودع العام لمصدر التكنولوجيا.

8.9.2.الإنهاء

تُطبّق التعديلات على هذا البيان وتُعتمد من قبل مجلس إدارة البنية التحتية للمفاتيح العامة وتُميز بإصدار جديد وعند نشره على المستودع العام لمصدر التكنولوجيا يصبح الإصدار الجديد ساري المفعول وتُؤرشف الإصدارات القديمة أيضاً على المستودع العام.

8.9.3.أثر الإنهاء والاستمرار

يتولى مجلس إدارة البنية التحتية للمفاتيح العامة إعلام الأطراف بالشروط والتبعات الناتجة عن إنهاء هذا البيان باستخدام الآليات المناسبة.

8.10.الإشعارات الفردية والتواصل مع المشاركين

يمكن توجيه الإشعارات المتعلقة بهذا البيان إلى عنوان الاتصال الخاص بمجلس إدارة البنية التحتية للمفاتيح العامة كما هو مذكور في القسم 1.5.

8.11.التعديلات

عند الحاجة إلى تعديل هذا البيان سيقوم مجلس إدارة البنية التحتية للمفاتيح العامة بإدراج التعديلات في إصدار جديد من هذا المستند وبعد اعتماده يُنشر الإصدار الجديد مع رقم إصدار جديد.

8.11.1.إجراء التعديل

راجع القسم 9.12.

8.11.2.آلية الإخطار والفترة الزمنية

عند نشر الإصدار الجديد من هذا البيان على المستودع العام لمصدر التكنولوجيا يصبح الإصدار الجديد ساري المفعول وتُؤرشف الإصدارات السابقة على نفس المستودع. يتولى مجلس إدارة البنية التحتية للمفاتيح العامة التنسيق اللازم فيما يتعلق بالتعديلات وتأثيراتها.

يحتفظ مجلس الإدارة بحق تعديل هذا البيان دون إخطار إذا كانت التعديلات غير جوهرية مثل تصحيح الأخطاء الطباعية أو تحسينات بسيطة.

8.11.3.الحالات التي تستوجب تغيير معرف الكائن(OID)

تحتفظ مصدر التكنولوجيا بحق تعديل محتوى أي بيان منشور لممارسات هيئة التصديق ولا يؤدي أي تعديل جوهري في هذا البيان إلى تغيير معرف الكائن المنشور في المستودع العام لمصدر التكنولوجيا. يتطابق معرف الكائن مع الإصدار المعتمد والساري حالياً لهذا البيان.

8.12.أحكام تسوية النزاعات

تُحال جميع النزاعات المرتبطة بأحكام هذا البيان وخدمات هيئة التصديق لتوقيع البرمجيات إلى الدائرة القانونية التابعة لمجلس إدارة البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا وفي حال تعذّرت الوساطة القانونية تحال النزاعات إلى المحاكم المختصة في جمهورية العراق.

8.13.القانون الناظم

تخضع قابلية التنفيذ والتفسير والصياغة القانونية لهذا البيان لقوانين جمهورية العراق.

8.14.الامتثال للقوانين المعمول بها

يتوافق هذا البيان وتقديم خدمات هيئة التصديق لتوقيع البرمجيات مع القوانين النافذة والمعمول بها في جمهورية العراق.

8.15.أحكام متنوعة

8.15.1.الاتفاق الكامل

لا ينطبق.

8.15.2.التنازل أو التفويض

باستثناء ما تنص عليه العقود الأخرى لا يجوز لأي طرف التنازل عن الحقوق أو تفويض المهام المنصوص عليها في هذا البيان دون الحصول على موافقة خطية مسبقة من مصدر التكنولوجيا.

8.15.3.قابلية الفصل

إذا تبيّن أن أحد أحكام هذا البيان غير صالح أو غير قابل للتنفيذ تبقى الأحكام الأخرى سارية حتى يُحَدث هذا البيان وفي حال وجود تعارض بين المتطلبات الأساسية وأي تنظيم قانوني في العراق يجوز لمصدر التكنولوجيا تعديل الشرط المتعارض إلى الحد الأدنى اللازم لجعله قانونياً وسارياً في العراق.

وينطبق ذلك فقط على العمليات أو إصدار الشهادات الخاضعة لهذا القانون وفي هذه الحالة تدرج مصدر التكنولوجيا في هذا القسم مرجعاً تفصيلياً إلى القانون الذي استوجب التعديل وإلى التعديل المطبق على المتطلبات الأساسية.

وتقوم مصدر التكنولوجيا أيضاً قبل إصدار أي شهادة وفقاً للمتطلبات المعدلة بإبلاغ منتدى متصفحات وهيئات التصديق بمحتوى التعديل المضاف حديثاً إلى هذا البيان ويُنهى العمل بهذا التعديل في حال زوال سبب التعديل أو تعديل المتطلبات الأساسية بما يسمح بالامتثال للقانون والمتطلبات معاً ويُجرى التعديل على الممارسة وتحديث البيان وإبلاغ المنتدى خلال مدة لا تتجاوز تسعين يوماً.

8.15.4.التنفيذ (أتعاب المحاماة والتنازل عن الحقوق)

لا ينطبق.

8.15.5.القوة القاهرة

لا تتحمّل مصدر التكنولوجيا أي مسؤولية عن فشل أو تأخير في تنفيذ أي بند من بنود هذا البيان إذا كان ذلك بسبب ظروف خارجة عن السيطرة المعقولة مثل انقطاع أو تأخر خدمات الاتصالات.

8.16.أحكام أخرى.

لا ينطبق.