مصدر التكنولوجيا

لخدمات النظم والبرمجيات

والتجارة العامة المحدودة

البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI)

هيئة التصديق لتوقيع المستندات

بيان ممارسة الشهادات

التحكم في الوثيقة

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 معBR 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 CP لمزود 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	• **تم التعديل ليشمل:** إصدار الشهادات الرقمية لكبار المسؤولين الحكوميين من قبل موظف جهة التسجيل التابعة لـ (مصدر التكنولوجيا). • **تم التعديل للسماح لـ:** موظف جهة التسجيل التابعة لـ (مصدر التكنولوجيا) بالقيام بمهام جهة التسجيل المحلية نيابة عن الجهات التي لم تقم بتعيين موظف تسجيل محلي، أو التي لا تملك القدرة على تعيينه.	شركة مصدر التكنولوجيا

الرقم التسلسلي	الإصدار	وصف التغييرات	

		• **تم التعديل ليعكس:** إمكانية إعادة استخدام البيانات التي تم التحقق منها مسبقاً بدلاً من إعادة التحقق الكامل عند تجديد المفتاح (المادة 3.2.2).
		• **تم التعديل لاستبدال:** التحقق القائم على شهادة التصديق (Attestation) بالتحقق المباشر (المادة 3.2.3.2).
		• **تم التعديل لتحديث:** أمثلة الأدلة التكميلية (المادة 3.2.3.1).
		• **تم التعديل لتغيير مسمى:** "اتفاقية المشترك" إلى "شروط وأحكام استخدام المشترك."
		• تعديلات في المواد:
		  • 4.3.2
		  • 4.1.1
		  • 4.9.1.2
		  • تم تحديث ممارسة التصديق (CPS) لتعكس تنفيذ إصدار الختم الإلكتروني عن بُعد.	

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

تمثل هذه الوثيقة بيان ممارسات التصديق (CPS) الذي يوضح ممارسات التصديق المطبقة من قبل شركة Technology Source يُشار إليها لاحقاً بـ TS لكل من هيئة التصديق للمواطنين الطبيعيين وهيئة التصديق لتوقيع المستندات الخاصة بالأشخاص المعنويين. يتوافق هذا البيان مع سياسة التصديق (CP) الخاصة بمقدمي خدمات الثقة (TSP) والتي تنطبق على تقديم خدمات التصديق للكيانات النهائية ضمن البنية التحتية الوطنية للمفاتيح العامة العراقية (Iraq National PKI) والتي تُدار من خلال الشركة العامة للاتصالات والمعلوماتية.

يتناول هذا البيان الجوانب التقنية والإجرائية والتنظيمية لكل من هيئتي التصديق التابعين، وهما هيئة توقيع المستندات للمواطنين الطبيعيين وهيئة توقيع المستندات للأشخاص المعنويين، واللذان أنشأتهما وتديرهما شركة Technology Source ضمن تسلسل الـ PKI العراقي الوطني، فيما يتعلق بالدورة الكاملة لحياة الشهادات الصادرة من قبل هتين الهيئتين.

ويُقصد بمصطلح **"هيئة توقيع المستندات"** في هذه الوثيقة كل من هيئتي التصديق التابعين المذكورين أعلاه، أي هيئة توقيع المستندات للأشخاص الطبيعيين وهيئة توقيع المستندات للأشخاص المعنويين.

يغطي هذا البيان إجراءات الإصدار والضوابط المحيطة بأنواع الشهادات التالية:

- **شهادات للأشخاص الطبيعيين**: وتُستخدم للأغراض التالية:
  - **شهادات توقيع مؤهلة**: تُستخدم لإنتاج توقيعات رقمية مؤهلة (عالية الموثوقية) على المعاملات والمستندات الرقمية. تُصدر هذه الشهادات للمواطنين أو الأفراد الذين لديهم صفة مهنية.
  - **شهادات توقيع متقدمة**: تُستخدم لإنتاج توقيعات رقمية متقدمة (متوسطة الموثوقية) على المستندات والمعاملات الإلكترونية.
- **شهادات للأشخاص المعنويين (شهادات الختم الإلكتروني)**: تُستخدم لتطبيق أختام إلكترونية على مستندات صادرة من كيان (شخص معنوي) لتأكيد هوية مصدر المستند وأصالته وسلامة البيانات الواردة فيه.
- **شهادات التحقق من صلاحية التوقيع**: تُستخدم لتوقيع ردود التحقق التي تُنتجها خدمة التحقق من التوقيع المقدمة من TS ضمن بنية الـ PKI العراقية.
- **شهادات مستجيب OCSP:** وهي شهادات تُستخدم لبروتوكول حالة الشهادة عبر الإنترنت (OCSP) لتوقيع استجابات OCSP المتعلقة بالشهادات التي أصدرتها هيئات التصديق التابعة.

يتوافق هذا البيان مع المتطلبات الرسمية الصادرة عن فرقة مهام هندسة الإنترنت (IETF) وفقاً لـ RFC 3647 من حيث التنسيق والمحتوى. وقد تُدرج بعض العناوين حسب الحاجة، لكن هيكلية RFC 3647 لا تُطبق بالضرورة على كل الحالات.

تلتزم لجنة حوكمة PKI الخاصة بـ TS بالحفاظ على توافق هذا البيان مع أحدث المتطلبات المنشورة على الرابط:
http://www.cabforum.org

- متطلبات أمن نظام الشهادات وشبكة منتدى CA/Browser Forum

في حال وجود تعارض بين محتوى هذه الوثيقة وأي من المتطلبات أعلاه، فإن المتطلبات المنتدى تتفوق في التطبيق.

هذه الوثيقة عامة. وإذا ورد أي ذكر لمعلومات سرية، فإنها تشير إلى وثائق مصنفة متاحة فقط للمستخدمين المخولين.

يمكن الحصول على معلومات إضافية بخصوص هذا البيان من لجنة حوكمة PKI التابعة لـTS ، وتوجد بيانات الاتصال ضمن الفقرة 1.5.

1.1 نظرة عامة

تم إنشاء البنية التحتية للمفتاح العام العراقية (Iraq National PKI) من قبل **الشركة العامة للاتصالات والمعلوماتية (ITPC)**، والتي تضم عدة هيئات تصديق جذرية تمثل البرنامج الوطني العراقي للبنية التحتية للمفتاح العام. ويهدف هذا البرنامج إلى تقديم إطار يُسهم في إنشاء مقدمي خدمات ثقة (TSP) لتوفير خدمات التصديق الرقمي والخدمات الموثوقة للجهات الحكومية وغير الحكومية.

تتكون بنية التسلسل الهرمي لـ PKI العراقي من مستويين:

المستوى 0:

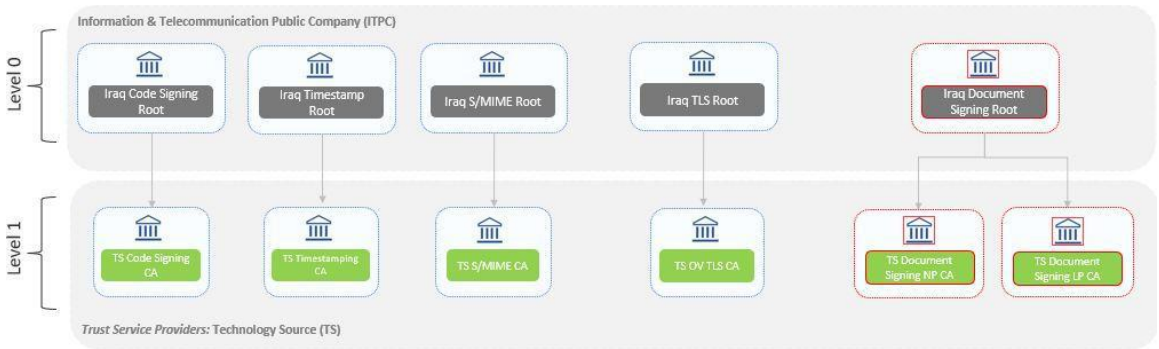
في هذا المستوى، تُنشأ خمس (5) هيئات تصديق جذرية (CA) بأنواع مختلفة من الشهادات التي يُمكن إصدارها. وتكون الشركة العامة للاتصالات والمعلوماتية (ITPC) مسؤولة عن طبقة الجذر. وبصفتها الجهة المشغلة للبنية التحتية الوطنية، فإن ITPC مخوّلة بإدارة اللجنة العليا لإدارة التوقيع الإلكتروني (PMA).

هيئات التصديق الجذرية هي كما يلي:

- 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 ضمن هذا المستوى من تسلسل البنية التحتية للمفتاح العام الوطنية، كما هو موضح في الشكل أدناه:



مصدر التكنولوجيا هي الجهة المسؤولة عن تشغيل هيئات التصديق التابعة وتقديم خدمات الثقة ذات الصلة إلى الجهات الحكومية وغير الحكومية في العراق. وبناءً على ذلك، تعمل شركة مصدر التكنولوجيا كمقدّم خدمات ثقة(TSP) ، حيث

تقدم خدماتها من خلال تسلسل هرمي من هيئات التصديق التابعة، والتي نُفذت ضمن هيئات التصديق الجذرية التابعة لـ الشركة العامة للاتصالات والمعلوماتية.(ITPC)

وقد قامت هيئات الشركة العامة للاتصالات والمعلوماتية الجذرية بتصديق هيئات التصديق التابعة الخاصة بمقدّم خدمات الثقة "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 الختم الوقتي TSAالمخصصة لتوقيع المستندات وتوقيع البرمجيات.

تُعدّ حالات الاستخدام المذكورة أعلاه من العناصر الأساسية لتمكين التحوّل الرقمي، إذ تمثّل حجر الزاوية في تأمين المعاملات الإلكترونية. إن دعم هذه الحالات ضمن نموذج ثقة موحّد وموثوق من الحكومة يُسهّل عملية التبنّي، ويُعزّز قابلية التشغيل البيني، ويُعزّز ثقة المستخدم.

يتفاعل مجلس حوكمة البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا (TS PKI GB) بشكل وثيق مع لجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية (ITPC PMA) لضمان الامتثال لهذا البيان الخاص بممارسة الشهادات (CPS) فيما يخص إصدار الشهادات وتشغيل هيئات توقيع المستندات التابعة لمصدر التكنولوجيا.

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

يُشار إلى المجلس المسؤول عن حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا، بما في ذلك هيئات توقيع المستندات، باسم مجلس حوكمة PKI لمصدر التكنولوجيا .(TS PKI GB) يتكوّن هذا المجلس من الوظائف الأساسية اللازمة، بما في ذلك السياسات والأمن والامتثال والشؤون القانونية ويضطلع بدور توجيهي استراتيجي مع إشراف مستمر على عمليات PKI الخاصة بمصدر التكنولوجيا.

يتحمّل مجلس TS PKI GB المسؤوليات التالية:

- وضع استراتيجية مصدر التكنولوجيا لـ PKI والحفاظ عليها
- تحديد خدمات مصدر التكنولوجيا لـ PKI والموافقة على نموذج تقديمها
- إعداد وصيانة السياسات والممارسات الخاصة بPKI
- تنفيذ أنشطة إشرافية دورية على فريق عملياتPKI
- اعتماد ميزانية PKI واتخاذ القرارات التجارية الكبرى

- الموافقة على التغييرات الجوهرية في البنية التحتية لPKI
- المصادقة على مراسيم المفاتيح وتكليف مدققين داخليين أو خارجيين حسب الحاجة
- المشاركة في الحوادث الكبرى واتخاذ القرارات المناسبة
- قيادة تسوية النزاعات الناشئة عن أنشطة PKI أو ذات الصلة بها
- تقييم الحوادث التي لم يلتزم فيها موظفو PKI الرئيسيون بالإجراءات الأمنية أو التشغيلية، بما في ذلك الجوانب الأخلاقية.

1.2 اسم الوثيقة ومعرّفها

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

تتضمّن هيئات توقيع المستندات هذا الـ OID ضمن امتداد سياسة الشهادات (CP extension) في الشهادات التي تصدرها، للدلالة على التزامها بالمتطلبات الحالية.

1.3 المشاركون في البنية التحتية للمفاتيح العامة (PKI)

1.3.1 هيئات التصديق

تتولى شركة **مصدر التكنولوجيا** ملكية وتشغيل هيئات توقيع المستندات من خلال مقراتها داخل جمهورية العراق. وقد حظيت هذه الهيئات بموافقة **الشركة العامة للاتصالات والمعلوماتية (ITPC)** وتم توقيعها من قبل **هيئة توقيع المستندات الجذري العراقي**، كما هو موضح في الشكل رقم 1 (في القسم 1.1).

تقدم هيئات توقيع المستندات التابعة لمصدر التكنولوجيا خدمات التصديق التالية:

- **خدمة إنشاء الشهادات:** إصدار شهادات الكيانات النهائية بناءً على عمليات التحقق التي تُجريها هيئات التسجيل.
- **خدمة النشر:** نشر شهادات OCSP و CRLوشهادات هيئة التصديق (CA) وإتاحتها للأطراف المعتمدة. وتشمل هذه الخدمة أيضاً توفير معلومات السياسات العامة وممارسات التصديق للمشتركين والأطراف المعتمدة.
- **خدمة إدارة الإلغاء:** معالجة الطلبات والتقارير المتعلقة بإلغاء الشهادات لتحديد الإجراءات المناسبة الواجب اتخاذها. وتتوفر نتائج هذه الخدمة من خلال خدمة حالة صلاحية الشهادة.
- **خدمة التحقق من حالة صلاحية الشهادة:** توفير معلومات الحالة الخاصة بصلاحية الشهادات للأطراف المعتمدة، استناداً إلى قوائم الإلغاء وبروتوكول .OCSP وتعكس معلومات الحالة دائماً الوضع الحالي للشهادات التي أصدرتها هذه الهيئات.

1.3.2 هيئات التسجيل

1.3.2.1 هيئة التسجيل – مصدر التكنولوجيا

تتولى (مصدر التكنولوجيا) إدارة مهام جهة التسجيل (RA) الخاصة بها مباشرة، ولا تعتمد على أطراف ثالثة مفوضة لتنفيذ أنشطة التسجيل؛ وتُعد وظيفة جهة التسجيل جزءاً لا يتجزأ من هيكلية عمليات البنية التحتية للمفاتيح العامة(PKI) ، وهي المسؤولة عن التحقق من الهوية والمصادقة عليها، فضلاً عن إدارة طلبات الشهادات للمؤسسات الحكومية وغير الحكومية العراقية.

تقوم جهة التسجيل بمهام التحقق من الهوية والمصادقة للأشخاص المعنويين (القانونيين) لغرض إصدار الشهادات، بما في ذلك شهادات الختم الإلكتروني (eSeal) للمؤسسات؛ بالإضافة إلى ذلك، تتولى جهة التسجيل مسؤولية التحقق من هوية

وصلاحية المؤسسات التي تسعى للعمل بصفة جهة تسجيل محلية (LRA) لإصدار شهادات الأشخاص الطبيعيين لمجتمعات المستخدمين التابعة لها (راجع المادة 1.3.2.2).

في حال عدم قيام المؤسسة مقدمة الطلب بتعيين موظف تسجيل محلي (LRAO) من داخل ملاكها، أو عدم قدرتها التشغيلية على ذلك، تتولى (مصدر التكنولوجيا) مهام التحقق من الهوية والمصادقة لموظفي تلك المؤسسة مباشرة من خلال جهة التسجيل التابعة لها؛ وفي هذه الحالات، يتحمل موظف جهة التسجيل (RA Officer) مسؤولية إثبات الهوية والمصادقة على بيانات طلبات شهادات الأشخاص الطبيعيين.

علاوة على ذلك، تُعالج طلبات الشهادات الخاصة بكبار المسؤولين الحكوميين حصرياً من قبل جهة التسجيل التابعة لـ (مصدر التكنولوجيا)، بغض النظر عما إذا كانت الجهة الطالبة تمتلك جهة تسجيل محلية خاصة بها من عدمه؛ حيث تضمن هذه المعالجة المركزية اتساق إجراءات التحقق من الهوية، وتوحيد مراجعة أدلة التفويض، والتعامل المنضبط مع بيانات طلبات الشهادات لهذه الفئة من المتقدمين.

1.3.2.2 هيئات التسجيل المحلية (LRA)

توفر شركة **مصدر التكنولوجيا** الإمكانية للجهات الحكومية وغير الحكومية العراقية لإدارة دورة حياة الشهادات الخاصة بمجتمعات مستخدميها، وذلك من خلال العمل كهيئة تسجيل محلية (LRA) للشهادات التي تُصدر للأشخاص الطبيعيين.

في هذه الحالة، تدخل الجهة المتقدمة بطلب الشهادة في علاقة تعاقدية (من خلال اتفاقية هيئة تسجيل محلية LRA) مع شركة **مصدر التكنولوجيا**، بحيث تقوم الجهة بإنشاء مكتب هيئة تسجيل محلية (LRA) يضم موظفي هيئة تسجيل تابعين لها يمارسون مهامهم من خلاله.

تفرض اتفاقية LRA مجموعة من الالتزامات تشمل – على سبيل المثال لا الحصر – ما يلي:

- المصادقة على طلبات الشهادات وطلبات الإلغاء أو الموافقة عليها أو رفضها.
- تعريف المشتركين وفقاً لاتفاقيات التسمية المعتمدة في هذا البيان(CPS) ، بما يضمن تفرّد كل مشترك وعدم وجود أي التباس في هويته.
- معالجة طلبات إصدار الشهادات وطلبات الإلغاء بالتنسيق مع هيئات توقيع المستندات التابعة لمصدر التكنولوجيا، وذلك بناءً على طلبات تم التحقق منها والموافقة عليها.
- إنشاء دفتر سجل تدقيق يُوثّق فيه جميع الأحداث الجوهرية المرتبطة بعمليات هيئة التسجيل.
- إتاحة الوصول الانتقائي إلى سجل التدقيق حسب ما هو محدد في هذا البيان.
- تنفيذ الضوابط التشغيلية الأخرى الواردة في هذا البيان.
- معالجة وتخزين المعلومات وفقاً للمتطلبات المحددة في هذا البيان (لا سيّما القسم 5).

تفوّض شركة **مصدر التكنولوجيا** الوظيفة الفنية لهيئة التسجيل من خلال تطبيق إلكتروني قائم على الويب يُتاح لموظفي هيئة التسجيل المحلية المفوضين رسمياً، والذين يعملون من مكاتب LRA محددة. ويُصدر حساب مخصص لكل موظف LRAلتمكينه من إدارة الشهادات ضمن مجتمع المستخدمين التابع للجهة التي ينتمي إليها مكتبLRA .

يجب أن يمتثل موظفو LRA للمتطلبات الواردة في القسمين 4.2 و5.3 من هذا البيان.

1.3.3 المشتركين

يتكوّن مشتركو هيئات توقيع المستندات التابعة لمصدر التكنولوجيا من الفئات التالية:

- الأشخاص الطبيعيون المصنّفون كأفراد (أي المواطنون العراقيون).

- الأشخاص الطبيعيون المصنّفون بالارتباط مع كيانات اعتبارية (أي الموظفون العراقيون بمن فيهم موظفو شركة مصدر التكنولوجيا).
- الأشخاص المعنويون (أي الجهات الحكومية وغير الحكومية العراقية، بما في ذلك شركة مصدر التكنولوجيا نفسها).

بالنسبة لأي شهادة، يوقّع المشترك أو يوافق على شروط واحكام استخدام المشترك التي تحدد الشروط والأحكام المعتمدة من قبل مصدر التكنولوجيا.

1.3.4 الأطراف المعتمدة

يتوجب على الأطراف المعتمدة الرجوع دائماً إلى خدمات التحقق من حالة الشهادات الخاصة بشركة **مصدر التكنولوجيا** أي قوائم الإلغاء CRL وخدمة OCSP وذلك قبل الاعتماد على أي معلومات واردة في الشهادة المعنية.

1.3.5 المشاركون الآخرون

تشمل الجهات الأخرى المشاركة ما يلي:

- **الجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية:(ITPC PMA)** وهي الجهة الرقابية المسؤولة عن الإشراف الكامل على نشاط مقدّم خدمات الثقة المرخّص (أي شركة مصدر التكنولوجيا). وقد جرى توضيح أدوارها ومسؤولياتها في وثيقة سياسة وممارسات التصديق الجذرية لITPC ، المنشورة على الرابط التالي:
https://pki.itpc.gov.iq.
- **مدققو WebTrust المؤهلون المستقلون:** والذين يتولّون التحقق من الامتثال للمتطلبات المحددة في القسم 8.2.

1.4 استخدام شهادات المشاركين في البنية التحتية للمفاتيح العامة

1.4.1 الاستخدامات المسموح بها للشهادات

يمكن استخدام الشهادات الصادرة عن هيئات توقيع المستندات التابعة لمصدر التكنولوجيا في الحالات التالية:

1. شهادات الأشخاص المعنويين:
   - **ختم إلكتروني(eSeal):** تُستخدم لإضافة ختم إلكتروني على مستند صادر عن كيان حكومي أو عامة أو خاصة، أو مصدّق منه.
2. شهادات الأشخاص الطبيعيين:
   - **التوقيع المتقدم:** يُستخدم لإنتاج توقيعات رقمية ذات موثوقية متوسطة على المستندات أو المعاملات الإلكترونية.
   - **التوقيع المؤهل:** يُستخدم لإنتاج توقيعات رقمية ذات موثوقية عالية على المستندات أو المعاملات الإلكترونية.
3. **شهادات التحقق من صلاحية التوقيع:** تُستخدم لتوقيع استجابة التحقق من التوقيع التي تُصدرها خدمة التحقق من التوقيع.
4. **شهادة مستجيبOCSP :** تُستخدم لتوقيع ردود بروتوكول حالة الشهادة عبر الإنترنت (OCSP) المتعلقة بالشهادات الصادرة عن هيئات توقيع المستندات التابعة لمصدر التكنولوجيا.

1.4.2 الاستخدامات المحظورة للشهادات

يُصرّح للمشتركين باستخدام شهاداتهم فقط للأغراض المحددة في القسم 1.4.1 من هذا البيان. ويُمنع تماماً استخدام الشهادات لأي أغراض أخرى غير مصرح بها.

1.5 إدارة السياسات

1.5.1 الجهة المسؤولة عن إدارة الوثيقة

تتولى **لجنة حوكمة البنية التحتية للمفاتيح العامة التابعة لمصدر التكنولوجيا (TS PKI GB)** مسؤولية إدارة هذه الوثيقة، وذلك وفقاً لنموذج التشغيل الخاص بها وبناءً على التفاعل اللازم مع لجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية(ITPC PMA) .

1.5.2 جهة الاتصال

يجب توجيه أي استفسارات تتعلق بهذا البيان (CPS) إلى العنوان التالي:

مجلس حوكمة البنية التحتية للمفاتيح العامة – مصدر التكنولوجيا
شركة مصدر التكنولوجيا
بغداد – الأربع شوارع – قرب إعدادية المأمون
البريد الإلكتروني: info@techsource.iq
رقم الهاتف: (+964) 784 136 1693.

لا يقبل مجلس TS PKI GB أي ملاحظات تتعلق بهذا البيان ما لم تُوجَّه إلى جهة الاتصال المذكورة أعلاه.

تقرير مشاكل الشهادات

تحتفظ شركة **مصدر التكنولوجيا** بقدرة استجابة داخلية على مدار الساعة وطيلة أيام الأسبوع لمعالجة طلبات الإلغاء العاجلة وتقارير مشاكل الشهادات ذات الأولوية العالية. وتوفر الشركة تعليمات متكاملة لإلغاء الشهادات والإبلاغ عن مشاكلها من خلال صفحة مخصصة في مستودعها العام، على الرابط:
https://pki.techsource.iq/repository/Certificate_Problem_Report.html.

يمكن للمشتركين والأطراف المعتمدة، وموزّدي برمجيات التطبيقات والجهات الخارجية الأخرى والإبلاغ عن حالات يُشتبه فيها بحدوث اختراق للمفتاح الخاص أو إساءة استخدام الشهادة أو أي نوع آخر من الاحتيال أو السلوك غير الملائم أو سوء الاستخدام أو أي مسألة متعلقة بالشهادات، من خلال إرسال بريد إلكتروني إلى:
certificate.problem@techsource.iq.

تقوم شركة مصدر التكنولوجيا بالتحقق من صحة طلب الإلغاء والتحقيق فيه قبل اتخاذ أي إجراء وفقاً لما هو وارد في القسم 4.9.

وفي حال رأت شركة مصدر التكنولوجيا أن الأمر يستدعي ذلك، فقد تُحيل تقارير الإلغاء إلى الجهات الأمنية المختصة.

1.5.3 الجهة المسؤولة عن تقييم مدى ملاءمة CPS للسياسة

استناداً إلى نتائج تدقيق الامتثال والتوصيات المصاحبة له، يتولى مجلس TS PKI GB تقييم مدى ملاءمة هذا البيان (CPS) وتطبيقه. وقد حاز هذا البيان على مصادقة كل من مجلس TS PKI GB والجنة العليا لإدارة التوقيع الإلكتروني(PMA) ، نظراً لوجوب توافقه مع بنود سياسة التصديق لمقدم خدمات الثقة(TSP CP) .

1.5.4 إجراءات الموافقة على CPS

يُوافق مجلس TS PKI GB بالتعاون مع الجنة العليا لإدارة التوقيع الإلكتروني (PMA) رسمياً على أي إصدار جديد من هذا البيان.

تتولى كوادر متخصصة من مجلس TS PKI GB، ممن لديهم خبرة في سياسات البنية التحتية للمفاتيح العامة، مراجعة هذا البيان في نسخته الأولية وأي تعديلات لاحقة، بهدف ضمان اتساقه مع أفضل الممارسات المعتمدة ومع سياسة التصديق الخاصة بمقدم خدمات الثقة، وذلك قبل اعتماد البيان من قبل المجلس.

يجري توثيق التعديلات ضمن جدول خاص بالتعديلات، وقد تتخذ التعديلات شكل إصدار محدث من الوثيقة أو إشعار تحديث رسمي.

يُرفع الإصدار الجديد من البيان إلى اللجنة العليا لإدارة التوقيع الإلكتروني (PMA) للموافقة النهائية، وذلك لضمان التوافق مع بنود سياسة التصديق لمقدم خدمات الثقة.

ولضمان المصداقية وتعزيز الثقة بهذا البيان وتلبية متطلبات الاعتماد والجوانب القانونية، يقوم مجلسTS PKI GB بمراجعة هذا البيان مرة واحدة على الأقل سنوياً، وقد يجري التعديلات التي يراها مناسبة أو تفرضها الظروف.

قبل أن يصبح الإصدار المحدث نافذاً، يُعلن عنه في المستودع على الرابط:
https://pki.techsource.iq.

وبمجرد نشره، يصبح الإصدار المحدث ملزماً لجميع المشتركين، بما في ذلك أولئك الذين يعتمدون على شهادات صادرة بموجب إصدار سابق من البيان.

1.6 التعاريف والاختصارات

1.6.1 التعاريف

- **الشهادة المتقدمة:** وفقاً لسياق البنية التحتية للمفاتيح العامة العراقية، تُعدّ الشهادة المتقدمة نوعاً من الشهادات الرقمية تُصدر بعد إجراء تحقق متوسط من هوية الموضوع، وتُستخدم لإنتاج توقيع رقمي متقدم (متوسط الموثوقية) على المستندات والمعاملات الإلكترونية.
- **المتقدّم بالطلب(Applicant) :** هو الشخص الطبيعي أو الكيان المعنوي الذي يتقدم بطلب للحصول على شهادة (أو لتجديدها). وبمجرد إصدار الشهادة، يُشار إليه بالمشترك. أما بالنسبة للشهادات الصادرة للأجهزة، فإن المتقدّم هو الكيان الذي يتحكم أو يدير الجهاز المذكور في الشهادة، حتى وإن كان الجهاز هو من أرسل الطلب فعلياً.
- **مُمثل المتقدّم بالطلب(Applicant Representative) : هو** شخص طبيعي أو ممثل مباشر للمتقدّم، سواء كان موظفاً لديه أو وكيلاً مفوضاً عنه بشكل صريح. وتتمثل مهامه في:
(1) توقيع وتقديم أو الموافقة على طلب الشهادة نيابةً عن المتقدّم
(2) توقيع شروط واحكام استخدام المشترك نيابةً عن المتقدّم
(3) الإقرار بشروط الاستخدام نيابةً عن المتقدّم في حال كان تابعاً لهيئة التصديق أو يمثلها.
في سياق هذا البيان، يكون ممثل المتقدّم هو المسؤول عن تقديم طلبات إصدار الشهادات أو طلبات إلغائها نيابةً عن المتقدّم. ويُستخدم مصطلحا "ممثل المتقدّم" ومقدم الطلب" بشكل تبادلي.
مزوّد برمجيات التطبيقات (Application Software Supplier): هو مزود برامج متصفحات الإنترنت أو أي برمجيات تعتمد على الشهادات وتعرضها أو تستخدمها، وتتضمن الشهادات الجذرية.

- **فترة التدقيق :(Audit Period)** في التدقيق الذي يغطي فترة زمنية، تمثل الفترة بين أول يوم (بداية) وآخر يوم من العمليات (نهاية) التي يغطيها المدققون ضمن نطاق التعاقد. (وهذه تختلف عن الفترة التي يتواجد فيها المدققون فعلياً في موقع هيئة التصديق).
- **تقرير التدقيق :(Audit Report)** تقرير يصدره مدقق مؤهل يعبّر فيه عن رأيه حول مدى التزام عمليات وضوابط الكيان محل التدقيق بالأحكام الإلزامية الواردة في هذه المتطلبات.
- **زوج مفاتيح هيئة التصديق :(CA Key Pair)** زوج مفاتيح يظهر فيه المفتاح العام كجزء من معلومات المفتاح العام للموضوع (Subject Public Key Info) في شهادة هيئة جذري و/أو شهادة هيئة تابع.
- **الشهادة :(Certificate)** وثيقة إلكترونية تستخدم التوقيع الرقمي لربط مفتاح عام مع هوية معينة.
- **بيانات الشهادة :(Certificate Data)** طلبات الشهادات والبيانات المتعلقة بها (سواء تم الحصول عليها من المتقدّم أو بوسائل أخرى) والتي تمتلكها أو تتحكم بها هيئة التصديق أو تملك صلاحية الوصول إليها.
- **عملية إدارة الشهادات :(Certificate Management Process)** العمليات والممارسات والإجراءات المتعلقة باستخدام المفاتيح والبرمجيات والمعدات، والتي من خلالها تقوم هيئة التصديق بالتحقق من بيانات الشهادة، وإصدار الشهادات، وصيانة المستودع، وإلغاء الشهادات.
- **سياسة الشهادة :(Certificate Policy)** مجموعة من القواعد التي تحدد مدى قابلية تطبيق شهادة معينة على مجتمع معين و/أو ضمن تنفيذ معين للبنية التحتية للمفاتيح العامة، وفق متطلبات أمنية مشتركة.
- **تقرير مشكلة شهادة :(Certificate Problem Report)** شكوى تتعلق باشتباه في اختراق مفتاح، أو إساءة استخدام شهادة، أو أي نوع آخر من الاحتيال أو سوء الاستخدام أو السلوك غير المناسب المتعلق بالشهادات.
- **قائمة إلغاء الشهادات :(Certificate Revocation List - CRL)** قائمة محدثة زمنياً بشكل دوري للشهادات الملغاة، يتم إنشاؤها وتوقيعها رقمياً من قبل هيئة التصديق التي أصدرت تلك الشهادات.
- **هيئة التصديق :(Certification Authority - CA)** مؤسسة مسؤولة عن إنشاء الشهادات وإصدارها وإلغائها وإدارتها. ويُطلق المصطلح على هيئات التصديق الجذرية والهيئات التابعة على حد سواء.
- **بيان ممارسة الشهادات :(Certification Practice Statement - CPS)** أحد الوثائق التي تُكوّن الإطار الحاكم الذي تُنشأ وتُدار وتُستخدم فيه الشهادات.
- **ملف الشهادة :(Certificate Profile)** مجموعة من المستندات أو الملفات التي تحدد متطلبات محتوى الشهادة وامتداداتها وفق القسم 7 من المتطلبات الأساسية. (على سبيل المثال، يوضح القسم 7 من هذا البيان ملفات الشهادات المُعتمدة).
- **التحكم :(Control)** يشير إلى امتلاك القدرة، بشكل مباشر أو غير مباشر، على: (1) إدارة الكيان أو موظفيه أو موارده المالية أو خططه (2) التحكم في انتخاب غالبية أعضاء مجلس الإدارة (3) التصويت بالنسبة المطلوبة من الأسهم المُخوّلة قانونياً لإثبات السيطرة، على ألا تقل النسبة عن 10%.
- **الدولة :(Country)** إما عضو في الأمم المتحدة، أو منطقة جغرافية مُعترف بها كدولة ذات سيادة من قبل دولتين عضوين على الأقل في الأمم المتحدة.
- **رمز التشفير المحمول :(Cryptographic Token)** جهاز تشفير على هيئة USB حاصل على شهادة التوافق مع المعيار FIPS 140 المستوى 2 أو ما يعادله.
- **مولد الأرقام العشوائية للأغراض التشفيرية :(CSPRNG)** مولد أرقام عشوائية مخصص للاستخدام في أنظمة التشفير.
- **طرف ثالث مفوّض :(Delegated Third Party)** شخص طبيعي أو كيان معنوي لا يمثل هيئة التصديق، ولا تدخل أنشطته ضمن نطاق التدقيق المعتمد الخاص بهيئة التصديق، لكنه مفوض منها لأداء أو تنفيذ واحد أو أكثر من متطلباتها ضمن عملية إدارة الشهادات.

- **تاريخ الانتهاء :(Expiry Date)** تاريخ "Not After" المُدرج في الشهادة والذي يحدد نهاية فترة صلاحية الشهادة.
- **كيان حكومي :(Government Entity)** كيان معنوي تديره الحكومة، مثل هيئة أو دائرة أو وزارة أو فرع أو أي كيان مشابه ضمن حكومة دولة أو وحدة إدارية داخلها (مثل ولاية، محافظة، مدينة، أو قضاء).
- **طلب شهادة عالي المخاطر :(High Risk Certificate Request)** طلب تصنّفه هيئة التصديق على أنه عالي المخاطر استناداً إلى قواعد داخلية وقواعد بيانات تحتفظ بها الهيئة، وقد تشمل أسماء معرضة للخطر مثل التصيّد الاحتيالي أو الاستخدام الاحتيالي، أو أسماء وردت في طلبات مرفوضة سابقاً أو شهادات ملغاة، أو تلك المدرجة ضمن قوائم Miller Smiles أوGoogle Safe Browsing ، أو تلك التي تحددها الهيئة استناداً إلى معاييرها الخاصة لتخفيف المخاطر.
- **هيئة الإصدار :(Issuing CA)** تشير إلى هيئة التصديق التي أصدرت الشهادة، وقد تكون هيئةاً جذرياً أو هيئةاً تابعاً.
- **اختراق المفتاح :(Key Compromise)** يعتبر المفتاح الخاص مخترقاً إذا تم الكشف عن قيمته لشخص غير مصرح له أو تمكن من الوصول إليه.
- **نص توليد المفتاح :(Key Generation Script)** خطة موثّقة تتضمن إجراءات توليد زوج مفاتيح لهيئة التصديق.

- **زوج مفاتيح :(Key Pair)** المفتاح الخاص والمفتاح العام المرتبط به.
- **كيان قانوني :(Legal Entity)** جمعية أو شركة أو شراكة أو ملكية فردية أو صندوق استئماني أو كيان حكومي أو أي كيان آخر يتمتع بوضع قانوني في النظام القضائي للدولة.
- **معرّف الكائن :(Object Identifier - OID)** معرّف فريد مكوّن من أحرف وأرقام أو أرقام فقط، يُسجّل بموجب المعيار المعتمد لدى المنظمة الدولية للمعايير (ISO) لغرض تمثيل كائن معين أو فئة معينة من الكائنات.
- **مستجيب :OCSP** خادم إلكتروني يعمل تحت سلطة هيئة التصديق ويتصل بمستودعها لمعالجة طلبات التحقق من حالة الشهادات. (انظر أيضاً: بروتوكول حالة الشهادة عبر الإنترنت).
- **بروتوكول حالة الشهادة عبر الإنترنت :(Online Certificate Status Protocol - OCSP)** بروتوكول إلكتروني يُستخدم للتحقق من حالة الشهادة، بحيث يُمكّن برمجيات التطبيقات المعتمدة من التحقق من صلاحية الشهادة المعنية) .انظر أيضاً: مستجيب(OCSP .
- **المفتاح الخاص :(Private Key)** المفتاح الخاص من زوج المفاتيح الذي يحتفظ به صاحب الزوج بسرية، ويُستخدم لإنشاء التوقيعات الرقمية أو لفك تشفير السجلات أو الملفات الإلكترونية المشفرة بالمفتاح العام المقابل.
- **المفتاح العام :(Public Key)** المفتاح العام من زوج المفاتيح الذي يمكن لصاحبه نشره علناً، ويُستخدم من قبل الطرف المعتمد للتحقق من التوقيعات الرقمية التي أنشأها المفتاح الخاص المقابل و/أو لتشفير الرسائل بحيث لا يمكن فك تشفيرها إلا باستخدام المفتاح الخاص المقابل.
- **البنية التحتية للمفتاح العام :(Public Key Infrastructure - PKI)** مجموعة من المعدات والبرمجيات والأفراد والإجراءات والقواعد والسياسات والالتزامات، تُستخدم لتمكين إنشاء الشهادات وإصدارها وإدارتها واستخدامها بطريقة موثوقة، وذلك استناداً إلى التشفير بالمفتاح العام.
- **شهادة موثوقة علنياً :(Publicly-Trusted Certificate)** شهادة تُعد موثوقة نظراً لأن الشهادة الجذرية المقابلة لها موزعة كنقطة ثقة ضمن برمجيات التطبيقات المتوفرة على نطاق واسع.
- **مدقق مؤهل :(Qualified Auditor)** شخص طبيعي أو كيان معنوي يستوفي المتطلبات المحددة في القسم 8.2.
- **الشهادة المؤهلة :(Qualified Certificate)** وفقاً لسياق البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI)، تمثل الشهادة المؤهلة نوعاً من الشهادات الرقمية تُصدر بعد إجراء تحقق دقيق من هوية الموضوع، بدرجة عالية من الموثوقية. ويشمل هذا التحقق عادة مقابلة وجهاً لوجه أو وسائل أخرى ذات مستوى موثوقية مكافئ. وتُستخدم الشهادات المؤهلة لإنتاج توقيعات رقمية مؤهلة على المستندات والمعاملات الإلكترونية.
- **القيمة العشوائية :(Random Value)** قيمة تُحدّدها هيئة التصديق للمتقدّم بطلب الشهادة، وتحتوي على ما لا يقل عن 112 بت من العشوائية (الانتروبيا).
- **اسم نطاق مسجّل :(Registered Domain Name)** اسم نطاق جرى تسجيله لدى جهة تسجيل نطاقات الإنترنت المعترف بها.

- **هيئة التسجيل (Registration Authority - RA):** كيان قانوني مسؤول عن تعريف وتوثيق هوية موضوعات الشهادات، دون أن يكون هيئة تصديق، وبالتالي لا يصدر أو يوقّع الشهادات. قد تساهم هيئة التسجيل في عملية التقديم للحصول على الشهادة أو في إلغائها أو في كليهما. وعند استخدام مصطلح "RA" كصفة لوصف وظيفة أو دور، فهذا لا يعني بالضرورة أنه كيان مستقل، بل قد يكون جزءاً من هيئة التصديق. في سياق هذا البيان، تُشغَّل وظيفة هيئة التسجيل من قبل **مصدر التكنولوجيا**.
- **مصدر بيانات موثوق (Reliable Data Source):** مستند تعريفي أو مصدر بيانات يُستخدم للتحقق من معلومات هوية الموضوع، ويُعترف به عموماً بين الكيانات التجارية والحكومات كمصدر موثوق، وقد أُنشئ من قبل طرف ثالث لغرض غير التقدّم بطلب شهادة. وفي هذا البيان، تُعدّ **دائرة تسجيل أو تأسيس الشركات العراقية** المصدر الموثوق للجهات غير الحكومية، في حين تُعدّ **الوقائع العراقية** المصدر الموثوق للجهات الحكومية.
- **وسيلة اتصال موثوقة (Reliable Method of Communication):** وسيلة اتصال مثل عنوان بريدي/شركة توصيل، أو رقم هاتف، أو بريد إلكتروني، جرى التحقق منها باستخدام مصدر غير ممثل المتقدم بالطلب.
- **الطرف المعتمد (Relying Party):** أي شخص طبيعي أو كيان قانوني يعتمد على شهادة صالحة. ولا يُعدّ مزوّد برمجيات التطبيقات طرفاً معتمداً إذا كانت برمجياته تقتصر على عرض معلومات الشهادة دون اعتمادها فعلياً.
- **خدمة التوقيع عن بُعد (eSeal) (Remote Signing Service):** في سياق هذا البيان، تشير إلى الخدمة التي تُشغّلها **مصدر التكنولوجيا** وتلتزم بالمعايير التالية:

  ETSI EN 419 241-1: متطلبات الأمن العام للأنظمة الموثوقة التي تدعم التوقيع على الخوادم – الجزء 1.

  ETSI EN 419 241-2: الملف التعريفي للحماية QSCD لتوقيع الخوادم – الجزء 2.

- **المستودع (Repository):** قاعدة بيانات إلكترونية تحتوي على وثائق الحوكمة المنشورة علنًا للبنية التحتية للمفاتيح العامة (مثل سياسات الشهادات وبيانات ممارسات التصديق)، ومعلومات حالة الشهادات، إما على شكل قوائم إلغاء (CRL)أو ردودOCSP .
- **رمز الطلب (Request Token):** قيمة تُشتق بطريقة تُحدّدها هيئة التصديق لربط إثبات السيطرة بطلب الشهادة. تشمل أمثلة رموز الطلب:
  (1) تجزئة المفتاح العام
  (2) تجزئة معلومات المفتاح العام للموضوع[X.509]
  (3) تجزئة طلب شهادةPKCS#10 .
- **هيئة جذر (Root CA):** أعلى مستوى في تسلسل هيئات التصديق، وتُوزَّع شهادته الجذرية من قبل مورّدي برمجيات التطبيقات وتُستخدم لتوقيع شهادات الهيئات التابعة.
- **الشهادة الجذرية (Root Certificate):** شهادة موقّعة ذاتياً صادرة عن الهيئة الجذري لتعريفه وتسهيل التحقق من الشهادات الصادرة عن هيئات توقيع المستندات التابعة لمصدر التكنولوجيا.
- **الموضوع (Subject):** الشخص الطبيعي، أو الجهاز، أو النظام، أو الوحدة، أو الكيان القانوني الذي يُشار إليه في الشهادة بصفته الموضوع. ويكون الموضوع إما هو المشترك أو جهازاً يخضع لتحكمه.
- **معلومات هوية الموضوع (Subject Identity Information):** المعلومات التي تُعرّف موضوع الشهادة. لا تشمل هذه المعلومات اسم النطاق المذكور في الامتداد subjectAltName أو حقل commonName الخاص بالموضوع.
- **هيئة تابع (Subordinate CA):** هيئة تصديق موقَّعة شهادته من قبل هيئة جذري أو هيئة تابع آخر.
- **المشترك (Subscriber):** الشخص الطبيعي أو الكيان القانوني الذي تصدر له شهادة ويخضع قانونياً لشروط واحكام استخدام المشترك أو شروط الاستخدام.

- **شروط واحكام استخدام المشترك (Subscriber Agreement):** اتفاقية بين هيئة التصديق والمتقدّم/المشترك، تُحدّد حقوق والتزامات الأطراف.
- **شهادة هيئة تابع مقيدة تقنياً (Technically Constrained Subordinate CA Certificate):** شهادة هيئة تابع تحتوي على إعدادات تجمع بين خصائص Extended Key Usage و Name Constraintsلتقييد نطاق الشهادات التي يمكن إصدارها ضمن هذا الهيئة.
- **شروط الاستخدام (Terms of Use):** أحكام تتعلق بحفظ الشهادة واستخداماتها المقبولة، وفقاً للمتطلبات الأساسية، عندما يكون المتقدّم/المشترك جهة تابعة لهيئة التصديق أو الهيئة نفسها.
- **شهادة صالحة (Valid Certificate):** شهادة تتجاوز بنجاح إجراءات التحقق كما هو محدد في RFC 5280 .
- **أخصائي التحقق (Validation Specialists):** شخص يؤدي مهام التحقق من المعلومات كما هو محدد في هذه المتطلبات.
- **فترة الصلاحية (Validity Period):** الفترة الزمنية الممتدة من تاريخ إصدار الشهادة وحتى تاريخ انتهائها (Expiry Date).

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 أسماء النطاقات
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 للمفتاح العام
PMA	اللجنة العليا لإدارة التوقيع الإلكتروني
RA	هيئة التسجيل
RSA	ريفست–شامير–أدلمن (مخترعو خوارزميةRS)
RTO	مدة استعادة الخدمة
SSL	طبقة المنافذ الآمنة
TLD	نطاق المستوى الأعلى
TSA	هيئة الختم 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

- X.509: المعيار الصادر عن الاتحاد الدولي للاتصالات (ITU-T) الخاص بالشهادات الرقمية.
- RFC3647: إطار سياسات الشهادات وممارسات التصديق للبنية التحتية للمفاتيح العامة (Internet X.509 PKI).
- RFC5280: مواصفات شهادات البنية التحتية للمفاتيح العامة وقوائم إلغاء الشهادات(CRL) .
- مبادئ ومعايير (WebTrust) الصادرة عن المعهد الأمريكي للمحاسبين القانونيين (AICPA) والمعهد الكندي للمحاسبين القانونيين (CPA Canada) الخاصة بسلطات التصديق.
- مبادئ ومعايير (WebTrust) الصادرة عن (AICPA/CPA Canada) الخاصة بأمن الشبكات لسلطات التصديق.
- متطلبات أمن الشبكات وأنظمة الشهادات الصادرة عن منتدى سلطات التصديق ومتصفحات الإنترنت (CA/Browser Forum).
- المعيار الأوروبي(ETSI 319 411-1/2) .
- المعيار الأوروبي(ETSI 319 401) .

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

2.2 نشر معلومات الشهادات

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 متكررة وفقاً لما هو محدد في بيان ممارسة الشهادات هذا(CPS) .

تُوفِّر 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 المستندات (TS Document 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 العام 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 الفرعية متوافقة تماماً مع المتطلبات المذكورة في القسم 1 من هذا البيان. في الحالات التي لا تتطلب تغييرات، يتم زيادة رقم إصدار CPS، ويتم تضمين إدخال سجل التغييرات المؤرخ لتوثيق المراجعة.

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 المستندات 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 المستندات 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 المستندات مع معايير الأسماء المميزة .X.500 يتحقق مشغل وظيفة هيئة التسجيل التابعة للجنة 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 هيئة التصديق لتوقيع المستندات في حقل "الجهة المُصدِرة" في شهادات المشتركين كما يلي:

- **شهادات الأشخاص المعنويين**

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

- **شهادات الأشخاص الطبيعيين**

CN	TS NP 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.

3.1.1.1 شهادات توقيع المستندات للأشخاص المعنويين الصادرة للمشتركين

CN	الاسم الكامل المسجَّل للمنظمة
OID	معرف الكائن الرسمي للمنظمة ويكون مختلف عن أسم المنظمة الرسمي
O	الاسم القانوني للمنظمة
الدولة (C)	العراق

3.1.1.2 شهادات توقيع المستندات للأشخاص الطبيعيين الصادرة للمشتركين

Given Name	الاسم الأول الموثق للفرد
Sur Name	اللقب الموثق للفرد
SERIALNUMBER	المعرف الفريد لكل فرد كما تم إنشاؤه بواسطة سلطة التسجيل
CN	تسلسل الاسم واللقب مفصولين بحرف "مسافة"
O (اختياري للمواطنين)	الاسم التنظيمي للكيان القانوني المرتبط بالشخص الاعتيادي
الدولة (C)	العراق

3.1.1.3 شهادة التحقق من صلاحية التوقيع

CN	الاسم الكامل الذي يمثل خدمة التحقق من صلاحية التوقيع لمصدر التكنولوجيا
O	شركة مصدر التكنولوجيا
الدولة (C)	العراق

3.1.1.4 شهادة مستجيب OCSP لهيئة TS Document Signing CA

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

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

3.1.2 الحاجة إلى أن تكون الأسماء ذات معنى

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

بالنسبة لشهادات توقيع المستندات 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 الفرعية.

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

وفقاً لما ورد في القسم 3.1.1 من هذا البيان، تفرض شركة **مصدر التكنولوجيا** مبدأ التفرّد في أسماء التمييز للموضوع (Subject DNs)كما يلي:

- **بالنسبة للشهادات الصادرة للأشخاص المعنويين:**
يُفرض التفرّد من خلال الجمع بين الاسم القانوني للمؤسسة أو الجهة وبين معرف فريد للمنظمة. وحيثما ينطبق ذلك، يتم استخدام سمة "الوحدة التنظيمية" (OU)؛ إذ يُستخدم حقل الوحدة التنظيمية للتمييز بين الشهادات الصادرة لمختلف الدوائر أو الأنظمة أو الوحدات الوظيفية ضمن المؤسسة الواحدة، مما يضمن امتلاك كل شهادة

اسماً مميزاً (DN) فريداً، حتى في الحالات التي يتم فيها إصدار شهادات متعددة لنفس الشخص المعنوي (الكيان القانوني).

- **بالنسبة للشهادات الصادرة للأشخاص الطبيعيين:**
يُفرض التفرّد من خلال الجمع بين اسم العائلة، والاسم الأول، وحقل الاسم العام(CN) ، بالإضافة إلى الرقم التسلسلي الذي يُمثل معرفاً للفرد.
- **بالنسبة للشهادات الصادرة لخدمة التحقق من التوقيع:**
يتضمن اسم خدمة التحقق من التوقيع الخاصة بمصدر التكنولوجيا ضمن اسم التمييز للموضوع (Subject DN) في الشهادة الصادرة.
- **بالنسبة لشهادات مستجيبOCSP:**
يتضمن اسم مستجيب OCSP الفريد ضمن اسم التمييز للموضوع 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 العام 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

يتم فرض إثبات حيازة المفتاح الخاص كجزء من معالجة طلب الشهادة من قبل خدمة التوقيع عن بُعد التي تديرها شركة مصدر التكنولوجيا.

وبالنسبة لخدمات الختم الإلكتروني والتوقيع عن بُعد، يتم توليد أزواج المفاتيح ضمن بيئة تشفير آمنة تدار من قبل شركة مصدر التكنولوجيا، حيث تظل المفاتيح الخاصة بالمشترك دائماً داخل وحدة التشفير.

ويتم إثبات حيازة المفتاح الخاص من خلال إنشاء طلب توقيع شهادة (PKCS#10 CSR) والذي يتم توقيعه باستخدام المفتاح الخاص المقابل داخل وحدة التشفير.

تتضمن عملية إصدار الشهادة تحققاً آلياً من أن التوقيع الموجود على طلب توقيع الشهادة (CSR) يتوافق مع المفتاح العام الوارد في الطلب، مما يؤكد أن المفتاح العام المعتمد مرتبط بالمفتاح الخاص المقابل الذي تم توليده بشكل آمن داخل بيئة التشفير التي تديرها شركة مصدر التكنولوجيا.

وتُنفذ جميع أنشطة التحقق من إثبات الحيازة من خلال عمليات خاضعة للرقابة والتدقيق، بما يضمن إمكانية التتبع بين المشترك المعتمد وزوج المفاتيح المُولد.

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 التحقق من الهوية للمنظمات المتقدّمة بطلب شهادات الأشخاص المعنويين

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 كيان حكومي 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.

تتولى هيئة التسجيل لخدمات الثقة التحقق من الارتباط بصاحب الشهادة، وذلك من خلال ضمان مطابقة المعلومات الواردة في نموذج الطلب تماماً للمعلومات المراد إدراجها في الشهادة.

يجوز لهيئة التسجيل لخدمات الثقة إعادة استخدام معلومات إثبات الهوية التي تم التحقق منها مسبقاً من خلال أنشطة التدقيق الموضحة في هذا القسم، شريطة أن تظل تلك المعلومات دقيقة وموثوقة. ولا يجوز إعادة استخدام هذه المعلومات إذا كان قد تم التحقق من صحتها قبل أكثر من 365 يوماً من تاريخ إصدار الشهادة.

<u>سلطة المتقدم بالطلب</u>

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 التحقق من هوية المنظمات المتقدّمة بطلب تشغيل مكتب تسجيل محلي(LRA)

ينطبق هذا السيناريو على المنظمات التي ترغب في إصدار وإدارة شهادات الأشخاص الطبيعيين. تُخضع الشركة والجهة الممثّلة المخوّلة منها لعملية تحقق وفقاً للإجراءات الموضحة في القسم 3.2.2.1، ثم يوقّع الممثّل المفوّض **اتفاقية المكتب المحلي للتسجيل(LRA)** .

وبعد الموافقة على تسجيل المنظمة، تباشر هيئة التسجيل التابعة لشركة **مصدر التكنولوجيا** بعملية داخلية يتم من خلالها إنشاء حسابات المنظمة وضباط LRA التابعين لها على بوابة هيئة التسجيل الإلكترونية (Web RA Portal)، بحيث يتمكنوا من استخدام حساباتهم لتنفيذ طلبات إصدار الشهادات وإجراء العمليات الإدارية الأخرى المتعلقة بها.

3.2.2.3 الاسم التجاري DBA

لا تدعم هيئات توقيع المستندات التابعة لشركة **مصدر التكنولوجيا** استخدام الاسم التجاري (DBA) أو الاسم المعروف تجارياً ضمن معلومات هوية الموضوع (Subject Identity Information) في الشهادة.

3.2.2.4 التحقق من الدولة

تصدر هيئات توقيع المستندات التابعة لشركة **مصدر التكنولوجيا** الشهادات فقط للمنظمات المُنشأة داخل **جمهورية العراق** .وتتحقق هيئة التسجيل من أن القيمة الواردة في حقل "الدولة" ضمن معلومات هوية الموضوع تساوي"IQ" .

3.2.3 التحقق من هوية الأفراد

توجد حالتان للتحقق من هويات الأفراد:

أ) التحقق من هوية الفرد المتقدّم بطلب للحصول على إحدى الشهادات المخصصة للأشخاص الطبيعيين، كما هو مبيّن في القسم 3.2.3.1.

ب) التحقق من هوية الفرد الذي يتصرّف بصفته "مقدّم الطلب" لتقديم طلب شهادة تُصدر لجهة معنوية، كما هو موضّح في القسم 3.2.3.2.

3.2.3.1 التحقق من هوية الأفراد المتقدمين بطلب شهادات الأشخاص الطبيعيين

يعتمد ضابط المكتب المحلي للتسجيل (LRAO) على أدلة موثوقة وأخرى داعمة لإثبات هوية الأفراد. وفيما يلي أنواع الأدلة المقبولة:

- **الأدلة الموثوقة:(Authoritative Evidence)** وهي أدلة تصدر عن جهة رسمية وتُعتبر موثوقة فيما يخص سمات الهوية التي تحتويها. وتُعد بطاقة الهوية الحكومية الآمنة أو جواز السفر، اللذَين يُصدران عبر آليات تحقق قوية، الأدلة الأساسية المعتمدة.
- **الأدلة الداعمة:(Supplementary Evidence)** هي الأدلة التي تُستخدم كإضافة للأدلة المعتمدة لتعزيز موثوقية إثبات الهوية، و/أو كدليل على السمات التي لا تثبتها الأدلة المعتمدة. ومن الأمثلة على الأدلة الثانوية: شهادة الموظف أو ما يعادلها من معلومات تثبت وجود علاقة وظيفية بين الموظف والجهة الحكومية، أو هويات الخدمة المدنية (باج الوظيفة).

3.2.3.1.1 التحقق من هوية الشخص الطبيعي (حالة استخدام المواطنين)

يُجرى التحقق من هوية المواطن إما يدوياً من قبل هيئة التسجيل التابعة لشركة **مصدر التكنولوجيا**، أو عبر وسيلة مؤتمتة، وذلك بناءً على قدرة المواطن على استخدام الهاتف الذكي وتطبيق رقمي مخصّص لعملية التسجيل.

تشمل طرق التحقق ما يلي:

- **مقابلة شخصية مع موظف التسجيل في مركز خدمة العملاء،** وهو موقع مخصص أنشأته شركة مصدر التكنولوجيا لغرض التحقق من هوية المواطنين وإصدار شهادات رقمية متقدمة أو مؤهلة لهم. ويستند موظف التسجيل في عملية التحقق إلى إجراء داخلي موثّق.
- **استخدام تطبيق الهاتف المحمول الخاص بالتسجيل الرقمي،** حيث تكون عملية التواصل مع المتقدّم مؤتمتة بالكامل (دون تدخل موظف تسجيل)، وهي وسيلة توفر مستوى مكافئ من الثقة مقارنة بالحضور الفعلي.

3.2.3.1.2 التحقق من هوية الشخص الطبيعي المرتبط بجهة معنوية (حالة استخدام المستخدم المهني)

تُطبَّق هذه الحالة على الأفراد الذين يتصرّفون بصفتهم المهنية وليس كمواطنين. وعليه، تتضمّن الشهادة الصادرة للفرد سمات الهوية الخاصة به مقرونة بسمات الجهة المعنوية التي ينتمي إليها.

أ) إصدار شهادات التوقيع المتقدم(Advanced Signing Certificates)

يقوم ضابط المكتب المحلي للتسجيل (LRAO) بجمع أدلة التحقق من هوية الفرد عبر القنوات الداخلية للجهة المعنية (مثل قسم الموارد البشرية ضمن إجراءات التوظيف أو من مدير مباشر في قسم العمل أو من الفرد نفسه)، وتشمل الأدلة ما يلي:

- نسخة من مستمسك إثبات الشخصية (الهوية) الخاص بالفرد المراد إصدار الشهادة له.
- معلومات موثوقة تثبت ارتباط الفرد بالمؤسسة (مثل: تأييد استمرارية بالخدمة، أو هوية الخدمة المدنية، أو ما يعادلها من بيانات)، وحيثما ينطبق ذلك.
- بريد إلكتروني رسمي من ممثل المؤسسة لغرض تسجيل الفرد في البنية التحتية للمفاتيح العامة (PKI) وإصدار شهادة توقيع رقمي له (وفقاً لمقتضيات حاجة العمل).

تولى موظف جهة التسجيل التابعة لـ (مصدر التكنولوجيا) أو موظف التسجيل المحلي التحقق من صحة واكتمال وثائق إثبات الهوية المقدمة، ومطابقتها مع متطلبات التسجيل والتحقق من الهوية المعمول بها.

وبعد الموافقة المبدئية على هوية الفرد، يباشر LRAO إجراءً تقنياً يتم بموجبه تسجيل الفرد في بوابة هيئة التسجيل الإلكترونية(Web RA Portal) ، ويزوَّد بمعلومات الدخول المخصصة للمصادقة متعددة العوامل، التي تُستخدم لتنفيذ طلبات الشهادات وإدارة عملياتها ذات الصلة.

ب) إصدار شهادات التوقيع المؤهل(Qualified Signing Certificates)

يتولى موظف جهة التسجيل التابعة لـ (مصدر التكنولوجيا) أو موظف التسجيل المحلي التحقق من هوية الشخص الطبيعي (المشترك) لشهادة التوقيع المؤهلة؛ ويتضمن ذلك الطلبات المقدمة من كبار المسؤولين الحكوميين، والتي يتم التحقق من هويتهم مباشرة من قبل موظف تسجيل محدد ومفوض من قبل (مصدر التكنولوجيا). وتتم عملية التحقق من الهوية من خلال المقابلة الشخصية المباشرة مع الفرد المعني.

تُجرى عملية إثبات الهوية وفقاً لمتطلبات التسجيل والتحقق المعمول بها، وتستند إلى إجراءات التسجيل والتحقق الموثقة التي تعتمدها (مصدر التكنولوجيا). تُجرى عملية إثبات الهوية وفقاً لمتطلبات التسجيل والتحقق المعمول بها، وتستند إلى إجراءات التسجيل والتحقق الموثقة التي تعتمدها (مصدر التكنولوجيا). يعتمد LRAO في ذلك على إجراء داخلي موثّق للتحقق من الهوية.

وبعد الموافقة المبدئية على هوية الفرد، يُنفّذ LRAO إجراءً فنياً يتم من خلاله تسجيل الفرد في بوابة هيئة التسجيل الإلكترونية (Web RA Portal)، وتُزوّده بمعلومات دخول مخصصة للمصادقة متعددة العوامل، لاستخدامها في تقديم طلبات الشهادات وتنفيذ العمليات الإدارية المرتبطة بها.

3.2.3.2 التحقق من هوية مقدّم الطلب(Requester)

يُعد مقدّم الطلب موظفاً لدى الجهة المعنوية، وقد جرى تعيينه من قبل الممثل المخوّل للجهة لتقديم طلبات إدارة شهادات التوقيع الإلكتروني المتقدم أو المؤهل (eSeals) إلى هيئة التسجيل التابعة لشركة مصدر التكنولوجيا .وتُنفَّذ الخطوات التالية كحد أدنى من قبل هيئة التسجيل للتحقق من هوية مقدّم الطلب:

- تُجري هيئة التسجيل عملية تحقق من الهوية من خلال مقابلة شخصية يُقدّم فيها مقدّم الطلب بطاقته الرسمية الصادرة عن كيان حكومي وليس نسخة عنها.
- تتولى جهة التسجيل التابعة لـ (مصدر التكنولوجيا) المصادقة على الارتباط الوظيفي بين مقدم الطلب والمؤسسة، والتحقق من صحة طلب الشهادة من خلال التأكيد المباشر مع الممثل المخول للمؤسسة؛ ويتم ذلك باستخدام

وسيلة اتصال موثوقة تشمل العناوين البريدية الإلكترونية الرسمية للمؤسسة، وعندما تقتضي الضرورة بحسب تقدير جهة التسجيل، يمكن تنظيم مقابلة شخصية مباشرة.

وبعد الموافقة الأولية على هوية الفرد، تُباشر هيئة التسجيل إجراءً تقنياً يتم من خلاله تسجيل مقدّم الطلب في بوابة هيئة التسجيل الإلكترونية(Web RA Portal) ، ويُزوَّد بمعلومات دخول مخصصة للمصادقة متعددة العوامل، لاستخدامها في تنفيذ طلبات الشهادات وإدارة دورة حياتها.

3.2.4 معلومات المشترك غير المؤكدة

تقوم ضوابط المكتب المحلي للتسجيل (LRAO) بالتحقق من جميع الحقول التي تتكوّن منها معلومات المشترك والمكتوبة في الشهادة.

3.2.5 التحقق من الصلاحية (سلطة الطلب)

- بالنسبة للشهادات الصادرة للأشخاص المعنويين (eSeal):
يقوم الممثل المفوّض للمنظمة بترشيح مقدّم طلب من داخل الجهة لتقديم طلبات إدارة الشهادات إلى هيئة التسجيل. ويُجرى التحقق من هوية مقدّم الطلب وفقاً لما ورد في القسم 3.2.3.2، بينما يُتحقّق من صلاحيته من خلال نموذج طلب الشهادة الموقّع من قبله ومن قبل الممثل المفوّض، والذي يثبت أهليته لتقديم الطلب.
- بالنسبة لشهادات الأشخاص الطبيعيين الصادرة عبر LRA:
يُصرَّح لضابط المكتب المحلي للتسجيل (LRAO) بتقديم طلبات إصدار الشهادات نيابةً عن المشتركين.

3.2.6 معايير التشغيل البيني

لا توجد أحكام.

3.3 التحقق من الهوية والمصادقة لطلبات إعادة إصدار الشهادات(Re-key)

3.3.1 التحقق من الهوية والمصادقة لإعادة الإصدار الروتيني

يُنفّذ التحقق من الهوية والمصادقة لعملية إعادة إصدار الشهادة تماماً كما هو الحال في التسجيل الأولي، مع تطبيق القواعد التالية:

- يتحقّق تطبيق هيئة التسجيل التابعة لمصدر التكنولوجيا أو ضابط المكتب المحلي للتسجيل (TS RA / LRAO) من وجود الشهادة المراد إعادة إصدارها وصلاحيتها، ومن أن المعلومات المستخدمة في التحقق من هوية الموضوع وصفاته لا تزال صالحة.
- إذا حدث أي تغيير في الشروط والأحكام الخاصة بشركة مصدر التكنولوجيا، يقوم TS RA / LRAO بإبلاغ المشترك بهذه التغييرات.

3.3.2 التحقق من الهوية والمصادقة لإعادة الإصدار بعد الإلغاء

تتبع إجراءات التحقق من الهوية والمصادقة لإعادة إصدار الشهادة بعد الإلغاء نفس الإجراءات المطبقة في إصدار الشهادة الأولية.

3.4 التحقق من الهوية والمصادقة لطلب إلغاء الشهادة

بالنسبة للشهادات الصادرة للأشخاص المعنويين:

تشمل إجراءات التحقق من الهوية والمصادقة لطلبات الإلغاء تقديم طلب رسمي من الممثل المفوّض للجهة التي صدرت لها الشهادة. وتُفرض إجراءات إلغاء رسمية من قبل TS RA تشمل ما يلي:

- توقيع نموذج طلب الإلغاء من قبل الممثل المفوّض.
- التحقق من هوية مقدّم الطلب بناءً على المعلومات المتوفرة لدى TS RA والتي تم تقديمها أثناء تسجيل المشترك.
- التواصل مع الجهة المعنية لتوفير مستوى مقبول من التأكيد بأن ممثلها الرسمي هو من قام بتفويض عملية الإلغاء. وقد يشمل هذا التواصل، بحسب الظروف، واحدة أو أكثر من الوسائل التالية: الهاتف أو البريد الإلكتروني أو خدمة البريد السريع.

وبعد المصادقة بنجاح على طلب الإلغاء، يقوم TS RA بإلغاء الشهادة من خلال النظام الخاص بهيئة التسجيل.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين:

يقوم TS RA أو LRAO بمصادقة طلب الإلغاء باستخدام إحدى الطرق التالية:

- **في حالة المستخدمين المهنيين:** استقبال طلب الإلغاء من قسم مختص ومتّفق عليه مسبقاً داخل الجهة (مثل قسم الموارد البشرية أو المدير المباشر للفرد)، في حال تم إنهاء خدمة المشترك أو تغيّر دوره ضمن الجهة. ويقوم LRAOبالتواصل داخلياً مع قسم الموارد البشرية لتأكيد صحة طلب الإلغاء.
- **في حالة المواطنين:** استقبال طلب الإلغاء من المشترك عبر قنوات معتمدة قد تشمل:
  - زيارة شخصية إلى موظف التسجيل، أو مكالمة هاتفية يطرح خلالها موظف التسجيل أسئلة تحقق من الهوية (مثل رقم هوية المواطن، الاسم، تاريخ الميلاد، إلخ).
  - إرسال بريد إلكتروني من المشترك باستخدام عنوان بريد يمكن التحقق منه من قبل موظف التسجيل.
  - من خلال تطبيق التسجيل الرقمي المخصص للهاتف المحمول.

سيناريو كبار المسؤولين الحكوميين (تتولى معالجته هيئة التسجيل لخدمات الثقة): استلام طلب إلغاء من السلطة الحكومية المختصة التي قامت بتعيين المسؤول أو تشرف عليه، أو من قسم التنسيق الحكومي المعين. ويتولى موظف هيئة التسجيل لخدمات الثقة المصادقة على الطلب بناءً على الوثائق الرسمية وقنوات الاتصال المعتمدة، وفقاً للإجراءات الداخلية الموثقة.

بالنسبة لشهادات مستجيب OCSP وشهادة خدمة التحقق من التوقيع الخاصة بمصدر التكنولوجيا:

لا يحدّد هذا البيان أحكاماً مفصّلة لإلغاء هذه الأنواع من الشهادات. وقد يُحفَّز إلغاء هذه الشهادات في حال حدوث اختراق أو اشتباه باختراق مفاتيحها الخاصة، ويُعامل ذلك ككارثة تُعالج وفقاً لخطة التعافي من الكوارث واستمرارية الأعمال الخاصة بمصدر التكنولوجيا.

4 متطلبات تشغيل دورة حياة الشهادة

4.1 طلب الشهادة

4.1.1 من يحق له تقديم طلب الشهادة

بالنسبة للشهادات الصادرة للأشخاص المعنويين:

يمكن لمقدّم الطلب تقديم طلبات الشهادات نيابة عن الجهة أو الكيان. ويتحمّل مقدّم الطلب مسؤولية دقة المعلومات المقدّمة ضمن طلب الشهادة. وتتأكّد هيئة التسجيل لدى مصدر التكنولوجيا من موافقة الممثل المفوّض للجهة من خلال توقيعه وختمه على نموذج طلب الشهادة وشروط واحكام استخدام المشترك المرفقة.

لا تُصدر شركة **مصدر التكنولوجيا** شهادات للجهات المدرجة في قائمة سوداء داخلية3، تُعرِّف الكيانات التي يُمنع التعامل معها. ويتم التحقق من هذه القائمة من قبل فريق TS RA عند استلام أي طلب شهادة.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين عبر المكتب المحلي للتسجيل(LRA) :

يمكن تقديم طلبات الشهادات مباشرة من قبل المتقدّمين أنفسهم عبر بوابة هيئة التسجيل الإلكترونية (Web RA Portal).

يُصرَّح لضابط المكتب المحلي للتسجيل (LRAO) بالموافقة على الطلبات وتقديمها، ويتحمّل مسؤولية صحة جميع البيانات المقدّمة ضمن طلب الشهادة. ويتأكّد LRAO من مصادقة الفرد على شروط واحكام استخدام المشترك ضمن عملية تقديم الطلب.

يتحقق LRAO من عدم إدراج الأفراد ضمن القوائم الحكومية الممنوعة أو قوائم الأشخاص المحظورين أو أي قائمة داخلية للأشخاص الذين لا يُسمح بقبول طلباتهم وفقاً لقوانين جمهورية العراق.

إذا كان مقدّم الطلب هو نفسه ضابطLRAO ، فيجب أن يتولى LRAO آخر (غير مقدّم الطلب) مسؤولية الموافقة على الطلب وتقديمه.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين من خلال مركز خدمة الزبائن:

يُصرّح لموظفي التسجيل في مركز خدمة الزبائن التابع لشركة مصدر التكنولوجيا بتقديم طلبات الشهادات. وهم مسؤولون عن صحة جميع البيانات المقدّمة ضمن طلب الشهادة، ويضمنون مصادقة المواطن على شروط واحكام استخدام المشترك ضمن عملية الطلب.

كما يتحقّقون من عدم إدراج الأفراد ضمن القوائم الحكومية الممنوعة أو قوائم الأشخاص المحظورين أو أي قائمة داخلية تحظر التعامل معهم بموجب قوانين جمهورية العراق.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين من خلال نظام التسجيل الرقمي:

يُصمَّم نظام التسجيل الرقمي ليقوم تلقائياً بتفويض واعتماد وتقديم طلبات الشهادات للمواطنين. ويتحمّل المتقدّم مسؤولية صحة البيانات المقدّمة ضمن طلب الشهادة. ويتأكّد التطبيق الرقمي من مصادقة الفرد على شروط واحكام استخدام المشترك ضمن إجراءات تقديم الطلب.

بالنسبة لشهادات مستجيب OCSP وشهادة خدمة التحقق من التوقيع الخاصة بمصدر التكنولوجيا:

تشرف هيئة التسجيل بالشركة إلى جانب مدير موثوق من فريق البنية التحتية للمفتاح العام (PKI) على تنفيذ مراسيم تشغيل داخلية مصادق عليها تُصدر من خلالها هذه الشهادات.

4.1.2 عملية التسجيل والمسؤوليات

بالنسبة للشهادات الصادرة للأشخاص المعنويين:

- يقوم مقدّم الطلب في الجهة بتحميل نموذج طلب الشهادة مع شروط واحكام استخدام المشترك من المستودع العام.
- يتم تعبئة النموذج وتوقيعه من قبل الممثل المفوّض للجهة (وكذلك يجب المصادقة على شروط واحكام استخدام المشترك).
- يقوم مقدّم الطلب بتسجيل الدخول إلى بوابة هيئة التسجيل الإلكترونية (باستخدام بيانات الدخول المخصصة للمصادقة متعددة العوامل التي جرى إعدادها ضمن إجراءات التسجيل الموضّحة في مستند داخلي لهيئة التسجيل) ويقدّم طلب الشهادة متضمناً - على سبيل المثال لا الحصر - ما يلي:
  - نسخة ممسوحة ضوئياً من نموذج الطلب المكتمل والموقّع بشكل صحيح.
  - المعلومات والمستندات المطلوبة للتحقق من الهوية والصلاحية.
- تقوم هيئة التسجيل لدى شركة مصدر التكنولوجيا بمراجعة والتحقق من سلامة وصحة جميع المستندات المقدّمة، بالإضافة إلى التحقق من هوية مقدّم الطلب وفقاً لما ورد في القسم 3.2.2.1.
- تقوم هيئة التسجيل بمعالجة طلب الشهادة. يُرجى الرجوع إلى القسم 4.2.
- عند الموافقة من قبل هيئة التسجيل التابعة لشركة مصدر التكنولوجيا، يتم توليد زوج المفاتيح الخاص بالكيان عن بُعد في وحدة أمن التشفير التابعة للشركة وفقاً لمتطلبات ممارسة التصديق، كما يتم إنشاء طلب توقيع الشهادة باستخدام حقول الشهادة المعتمدة في نموذج الطلب (مثل سمات الاسم المتميز وحجم المفتاح ونوعه وغيرها)، ومن ثم يُرفع هذا الطلب إلى سلطة التصديق.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين عبر المكتب المحلي للتسجيل(LRA) :

- يقوم المتقدّم بالتسجيل في بوابة هيئة التسجيل الإلكترونية، ثم يُجري المصادقة باستخدام بيانات المصادقة متعددة العوامل التي أُعدّت أثناء عملية التسجيل وفقاً لوثيقة الإجراءات الداخلية لهيئة التسجيل.
- يُكمِل المتقدّم نموذج طلب الشهادة.
- يُصادق المتقدّم على شروط واحكام استخدام المشترك ويقدّم طلب الشهادة إلى ضابط المكتب المحلي للتسجيل (LRAO).
- يُصرَّح لضابط المكتب المحلي بمراجعة طلبات الشهادات والموافقة عليها. يقوم بتسجيل الدخول إلى بوابته الإلكترونية الخاصة ويُجري الخطوات التقنية اللازمة للتحقق والموافقة وتقديم الطلب. يحتفظ LRAO بقائمة سوداء داخلية بأسماء الأفراد التابعين للجهة ولا يُقبل طلب شهادة لأي منهم.

بالنسبة للشهادات الصادرة من خلال مركز خدمة الزبائن:

- يحضر المتقدّم إلى مركز خدمة الزبائن.
- يُكمِل المتقدّم نموذج التسجيل ويوقّعه، بالإضافة إلى شروط واحكام استخدام المشترك، أمام موظفي التسجيل في الشركة.
- تُتحقَّق هوية المتقدّم وفقاً لما ورد في القسم 3.2.3.1.1، ثم يُقدَّم طلب التسجيل من خلال تطبيق هيئة التسجيل الإلكتروني، ويتضمن هذا الطلب جميع الأدلة المجمعة ونسخة ممسوحة من النموذج. وتُتلف النسخة الورقية لاحقاً.
- بعد موافقة موظفي التسجيل، يُسجَّل المتقدّم في بوابة هيئة التسجيل ويُولَّد له مفتاح التوقيع الرقمي.

بالنسبة للشهادات الصادرة عبر نظام التسجيل الرقمي:

- يجب تثبيت تطبيق التسجيل الرقمي على هاتف المواطن الذكي، وإذا لم يكن مثبتاً، فعليه تنزيله من متجر التطبيقات المناسب.
- يتلقّى المواطن إرشادات مؤتمتة خلال عملية التحقق من الهوية.
- يُطلب من المواطن خلال العملية:
  - مسح وجهي بطاقته التعريفية أو الجواز الإلكتروني (الأمامي والخلفي) لاستخلاص الاسم الكامل وتاريخ الميلاد ورقم الهوية وصورته الشخصية.
  - التقاط صورة شخصية "سيلفي" باستخدام التطبيق، تُسجَّل عبر بث فيديو حي يخضع لفحص حيوية للتأكّد من وجود شخص حي أمام الكاميرا أثناء عملية التحقق. ويُستخدم الوجه الملتقط لربطه بالمتقدّم من خلال بصمة الوجه.
  - استكمال البيانات الشخصية مثل رقم الهاتف وعنوان البريد الإلكتروني لأغراض التحقق.
  - بعد التحقق من الحساب بنجاح، يجب تعيين كلمة مرور للحساب.
- يُخطَر المواطن بنجاح تسجيله وتوليد مفاتيح توقيعه.

بالنسبة لشهادات مستجيب OCSP وشهادة خدمة التحقق من التوقيع:

تشرف هيئة التسجيل ومدير نظام موثوق من فريق البنية التحتية للمفتاح العام (PKI) على تنفيذ مراسيم تشغيلية تصدر من خلالها هذه الشهادات. ويُوافق مجلس إدارة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا (TS GB) على وثائق المراسيم التشغيلية ويتحقق من مطابقة قالب الشهادة واتفاقية التسمية لأحكام هذا البيان. كما يصادق المجلس على المراسيم ويؤكّد قائمة الموظفين المخوّلين المشاركين فيها.

4.2 معالجة طلب الشهادة

4.2.1 تنفيذ مهام التحقق من الهوية والمصادقة

المتطلبات العامة لجميع طلبات الشهادات:

أ) يُخصص معرف فريد لكل سجل طلب شهادة.
ب) يقوم موظفو هيئة التسجيل / LRAO / نظام التسجيل الرقمي بتوثيق جميع الأنشطة (الاتصالات الإلكترونية، المكالمات الهاتفية، الأدلة) مع سجل الطلب.
ت) تُضاف أي طلبات مشبوهة أو غير ناجحة بعد ثلاث محاولات إلى قائمة سوداء تتضمن تفاصيل تمنع الالتباس في التعرف على الطلبات المستقبلية.
ث) يجري التحقّق من القائمة السوداء، وإذا تبيّن إدراج المتقدّم فيها، يُرفَض طلبه.
ج) يُوقّع المتقدّم أو يصادق على شروط واحكام استخدام المشترك المخصصة.

بالنسبة للشهادات الصادرة للأشخاص المعنويين:

أ) يُكمِل مقدّم الطلب نموذج تسجيل الجهة متضمناً المعلومات التالية:
   a. معلومات الكيان:
      i. الاسم القانوني للجهة.
      ii. العنوان الرسمي.
      iii. رقم الهاتف الرئيسي.
   b. معلومات الممثلين المخوّلين:

i. معلومات ممثل الطلب مثل رقم الهاتف، البريد الإلكتروني الرسمي، والمنصب الوظيفي.

c. معلومات مقدم الطلب (ممثل الجهة):

i. اسم مقدم الطلب ومعلومات الاتصال الخاصة به (الشخص المخوّل بتقديم طلبات إدارة الشهادات نيابةً عن الجهة).

ب) يوقّع الممثل المفوض شروط واحكام استخدام المشترك المخصصة ويصادق عليها.

ت) تُصدِر دائرة الموارد البشرية في الجهة رسالة إثبات تؤكّد ارتباط مقدم الطلب بالجهة.

ث) يُرسِل مقدم الطلب النموذج الموقّع ورسالة الإثبات وسائر مستندات التحقق المطلوبة إلى هيئة التسجيل لدى مصدر التكنولوجيا عبر البريد الإلكتروني.

ج) تقوم هيئة التسجيل بتنفيذ خطوات التحقق الإلزامية التالية على طلب التسجيل المستلم:

a. التحقق من هوية الجهة وممثلها المفوض وفقاً لما ورد في القسم 3.2.2.

b. التحقق من صلاحية مقدم الطلب كما ورد في القسم 3.2.5.

c. التحقق من رقم هاتف الجهة من خلال اتصال عشوائي.

ح) إذا تم اجتياز جميع خطوات التحقق أعلاه بنجاح، تُطلق هيئة التسجيل عملية على بوابة هيئة التسجيل الإلكترونية لتسجيل الجهة الحكومية ومقدم الطلب، بناءً على المعلومات المُجمَّعة من الأخير. عند هذه النقطة، يصبح بمقدور مقدم الطلب تسجيل الدخول إلى البوابة وتقديم طلبات الشهادات نيابةً عن جهته.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين عبر المكتب المحلي للتسجيل(LRA) :

أ) يتحقّق ضابط LRA من هوية الفرد كما هو مذكور في القسم 3.2.3.1.2.

ب) يتحقّق ضابط LRA من عدم ورود اسم الفرد في القائمة السوداء.

ت) يتحقّق من استحقاق الموظف للشهادة المطلوبة حسب الإجراءات الداخلية للجهة (مثل التواصل مع مديره المباشر).

ث) يُباشر ضابط LRA بالإجراءات التقنية الخاصة بإصدار الشهادة المطلوبة.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين عبر مركز خدمة الزبائن:

أ) يتحقّق موظف هيئة التسجيل من هوية الفرد كما ورد في القسم 3.2.3.1.1.

ب) يراجع موظف هيئة التسجيل طلب التسجيل ويوافق عليه، ويتحقّق من عدم ورود اسم الفرد في القائمة السوداء.

ت) يُباشر الموظف بالإجراءات التقنية الخاصة بإصدار الشهادة.

بالنسبة للشهادات الصادرة عبر نظام التسجيل الرقمي:

يُصمَّم نظام التسجيل الرقمي للموافقة التلقائية على الطلبات المقدمة من المواطنين وإرسالها. يتحمل المتقدّم مسؤولية صحة جميع البيانات المقدمة ضمن الطلب.

بالنسبة لشهادات مستجيب OCSP وشهادة خدمة التحقق من التوقيع:

يشرف كل من هيئة التسجيل ومدير البنية التحتية للمفتاح العام المخوّل على تنفيذ المراسيم التشغيلية التي تُصدر من خلالها هذه الشهادات. يوافق مجلس إدارة PKI على وثائق المراسيم التشغيلية ويتحقق من مطابقة قالب الشهادة واتفاقيات التسمية لأحكام هذا البيان. ثم يصادق المجلس على المراسيم ويؤكد قائمة الموظفين المخوّلين المشاركين.

4.2.2 الموافقة أو الرفض لطلبات الشهادات

توافق هيئة التسجيل LRA على طلب الشهادة فقط إذا توفرت المعايير التالية:

- النجاح في التحقق من هوية كافة بيانات المشترك المطلوبة وفقاً للقسم 3.2.

وترفض هيئة التسجيل LRA طلب الشهادة إذا:

- تعذّر التحقق من هوية كافة بيانات المشترك المطلوبة وفقاً للقسم 3.2.
- فشل المشترك في تقديم المستندات الداعمة المطلوبة.

بالنسبة لشهادات مستجيب OCSP وخدمة التحقق من التوقيع:

تُوافق لجنة إدارة PKI على طلب الشهادة ضمن مراسيم تشغيلية داخلية معتمدة من مصدر التكنولوجيا.

4.2.3 مدة معالجة طلبات الشهادات

لا يوجد نص محدد.

4.3 إصدار الشهادة

4.3.1 إجراءات الهيئة المصدرة أثناء إصدار الشهادة

بالنسبة للشهادات الصادرة للأشخاص المعنويين:

تتولى سلطة التصديق (CA) التحقق من تنسيق وهيكلية طلب توقيع الشهادة (CSR) وإنشاء شهادة أولية (Pre-certificate) مقابلة له، وتخضع الشهادة الأولية لعملية الفحص التقني (Linting) باستخدام أدوات قياسية برمجية لتقييم مطابقتها التقنية وامتثالها (لكل عنصر مراد توقيعه قبل إجراء عملية التوقيع) مع المعايير المعمول بها. وعقب نجاح عملية التحقق، يتم إنشاء الشهادة النهائية وفقاً لنموذج الشهادة المعد مسبقاً، وإتاحتها للتنزيل عبر بوابة جهة التسجيل على شبكة الإنترنت. وتصدر سلطة التصديق الشهادة وهي في حالة "نشطة" (Active)، لضمان جاهزيتها للاستخدام فور تنصيبها في مستودع المفاتيح المستهدف.

وتبدأ صلاحية كل شهادة صادرة من وقت إصدارها.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين عبر المكتب المحلي للتسجيل(LRA) :

تتولى هيئة التصديق (CA) التحقق من تنسيق وهيكلية طلب توقيع الشهادة (CSR) وإنشاء شهادة أولية (Pre-certificate) مقابلة له؛ وتخضع الشهادة الأولية لعملية الفحص التقني (Linting) باستخدام أدوات قياسية برمجية لتقييم مطابقتها التقنية وامتثالها (لكل عنصر مراد توقيعه قبل إجراء عملية التوقيع) مع المعايير المعمول بها. وعقب نجاح عملية التحقق، يتم إنشاء الشهادة النهائية وفقاً لنموذج الشهادة المعد مسبقاً، وإتاحتها للتنزيل عبر بوابة جهة التسجيل على شبكة الإنترنت. وتصدر هيئة التصديق الشهادة وهي في حالة "نشطة" (Active)، لضمان جاهزيتها للاستخدام فور تنصيبها في مستودع المفاتيح المستهدف (الرمز الإلكتروني - e-Token).

بالنسبة للشهادات الصادرة عبر مركز خدمة الزبائن:

يتبع موظفو هيئة التسجيل في مصدر التكنولوجيا نفس الإجراءات المشار إليها أعلاه، حيث يتم توليد زوج مفاتيح المشترك باستخدام بوابة التسجيل الإلكتروني ثم إصدار الشهادة من الهيئة المصدرة الفرعية بعد التحقق من CSR. وتُتاح الشهادة للتنزيل في حالتها "النشطة" لاستخدامها الفوري.

بالنسبة للشهادات الصادرة عبر نظام التسجيل الرقمي:

تستلم الهيئة المصدرة طلب الشهادة من نظام التسجيل الرقمي، وتتحقق من صحة تركيب الطلب ثم تُصدر الشهادة وفقاً لقالب الشهادة المُعتمد. تُعاد الشهادة تلقائياً إلى نظام التسجيل الرقمي بحالة "نشطة" بحيث تكون جاهزة للاستخدام.

بالنسبة لشهادات مستجيب OCSP وشهادة خدمة التحقق من التوقيع:

يحدث إصدار وإدارة هذه الشهادات ضمن مراسيم تشغيلية مُعتمدة من قِبل عضوين على الأقل من مجلس إدارة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا، بهدف:

1. المصادقة على تنفيذ المراسيم.
2. الموافقة على قائمة المشاركين في المراسيم، والتي تشمل هيئة التسجيل وعضواً من إدارة عمليات PKI ومجموعة من مديري النظام المخوَّلين.
3. التحقق من قوالب الشهادة المُضمّنة واتفاقيات التسمية وفقاً لأحكام هذا البيان.

4.3.2 إشعار المشترك من قبل الهيئة بإصدار الشهادة

بالنسبة للشهادات الصادرة للأشخاص المعنويين:

يتم إشعار المشترك عبر البريد الإلكتروني بأن الشهادة المطلوبة قد تم إنشاؤها. وتُتاح الشهادة للتنزيل لمقدم الطلب (أي ممثل الجهة) عبر حسابه في بوابة التسجيل الإلكتروني.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين:

يُرسل إشعار للمشترك عبر البريد الإلكتروني فور إصدار الشهادة، وتُصبح متاحة للتنزيل من بوابة التسجيل الإلكتروني أو التطبيق الرقمي. وبالنسبة للشهادات الصادرة للأفراد عبر نظام التسجيل الرقمي، يقوم التطبيق على الهاتف المحمول الخاص بالتسجيل الرقمي بإخطار المستخدم بإصدار الشهادة فور استلامها من جهة إصدار الشهادات. ويتم ذلك من خلال التفاعل (الرسالة المعروضة) بين المستخدم وتطبيق الهاتف المحمول الخاص بالتسجيل الرقمي.

بالنسبة لشهادات مستجيب OCSP وشهادة خدمة التحقق من التوقيع:

يُشعَر المدير المعني عند استلام الشهادة من هيئة التسجيل.

4.4 قبول الشهادة

4.4.1 التصرفات التي تُعد قبولاً للشهادة

بالنسبة للشهادات الصادرة للأشخاص المعنويين:

يقوم مقدم الطلب بتنزيل الشهادة من بوابة التسجيل الإلكتروني والتحقق من محتواها مقارنةً مع نموذج الطلب .CSR/وفي حال وجود أي تناقضات، يبدأ مقدم الطلب التواصل مع هيئة التسجيل مما قد يؤدي إلى إبطال الشهادة وإصدار شهادة بديلة.
تُعد الشهادة مقبولة من قبل الجهة في حال عدم تقديم أي اعتراض من قبل مقدم الطلب إلى هيئة التسجيل خلال عشرة أيام عمل من تاريخ إرسال إشعار إصدار الشهادة.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين:

يقوم المشترك بتنزيل الشهادة أو مراجعتها عبر بوابة التسجيل الإلكتروني أو تطبيق التسجيل الرقمي، ثم يتحقق من محتواها. وفي حال وجود أي تناقضات، يتواصل المشترك مع ضابط التسجيل المحلي أو موظفي هيئة التسجيل مما قد يؤدي إلى إبطال الشهادة وإصدار شهادة بديلة.

بالنسبة للشهادات الصادرة للأشخاص الطبيعيين من خلال نظام التسجيل الرقمي الذاتي

ويُعد قبول الشهادة ضمناً عند استلام المشترك إشعاراً من التطبيق يؤكد إتمام عمليات التسجيل، وتوليد المفاتيح، وإصدار الشهادة، أو عند استخدام المشترك للشهادة في أي عملية توقيع رقمي. وبمجرد تحقق أي من هذه الحالات، يُعتبر المشترك قد راجع المعلومات الواردة في الشهادة وصادق على دقتها، كما يُعتبر مسؤولاً عن حماية واستخدام المفتاح الخاص المرتبط بها وفقاً لشروط وأحكام استخدام المشترك وسياسة ممارسات التصديق (CPS) المعمول بها. بالنسبة لشهادات المستجيب OCSP وشهادة خدمة التحقق من توقيع TS: يتم نشر الشهادة على مخزن المفاتيح المستهدف كجزء من مراسم التشغيل الداخلية لـ TS.

4.4.2 نشر الشهادة من قبل الهيئة المصدرة

لا تقوم الهيئات المصدرة لدى مصدر التكنولوجيا بنشر شهادات المستخدم النهائي، باستثناء مشاركتها مع المشتركين أنفسهم.

4.4.3 إشعار إصدار الشهادة من قبل الهيئة المصدرة إلى جهات أخرى

لا يوجد نص خاص.

4.5 استخدام زوج المفاتيح والشهادة

4.5.1 استخدام المفتاح الخاص والشهادة من قبل المشترك

يتوجب على المشتركين الالتزام بالواجبات التالية:

- تقديم معلومات صحيحة ومُحدّثة إلى الهيئة المصدرة (مثل مصدر التكنولوجيا) ضمن طلب الشهادة؛
- عدم التلاعب بمحتوى الشهادة.
- استخدام الشهادات فقط لأغراض قانونية ومصرّح بها، ووفقاً لمتطلبات سياسة مقدم خدمات الثقة(TSP CP) وهذا البيان.
- إشعار هيئة التسجيل في مصدر التكنولوجيا أو ضابط التسجيل المحلي فوراً في حال أصبحت أي من معلومات الشهادة غير صالحة أو في حال تم اختراق أو فقدان أو إفشاء المفتاح الخاص أو استخدامه بشكل غير مصرح به.
- عدم استخدام الشهادة بعد انتهاء فترة صلاحيتها أو بعد إبطالها.

راجع القسم 9.6.3 من هذا البيان للاطلاع على تفاصيل مكتملة.

4.5.2 استخدام المفتاح العام والشهادة من قبل الطرف المعتمد

على الطرف الذي يعتمد على الشهادة الصادرة عن الهيئات المصدرة لدى مصدر التكنولوجيا أن:

- يستخدم برنامجاً متوافقاً مع معيار X.509 ومعايير IETF PKIX للتحقق من توقيع الشهادة وفترة صلاحيتها؛
- يتحقق من صلاحية الشهادة باستخدام قوائم الشهادات الملغاة (CRL) أو خدمة حالة صلاحية الشهادة (OCSP) وفقاً لإجراءات التحقق من مسار الشهادة؛
- يثق في الشهادة فقط إذا لم تُلغَ وكانت ضمن فترة صلاحيتها؛

- يستخدم الشهادة فقط لغرضها المحدد ووفقاً لما يحدده هذا البيان.

4.6 تجديد الشهادة

غير قابل للتطبيق.

4.6.1 الظروف المؤدية إلى تجديد الشهادة

غير قابل للتطبيق.

4.6.2 الجهة المخوّلة بطلب 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 التصرفات التي تُعد قبولاً لشهادة مجددة

غير قابل للتطبيق.

4.6.6 نشر الشهادة المجددة من قبل الهيئة المصدرة

غير قابل للتطبيق.

4.6.7 إشعار إصدار الشهادة من قبل الهيئة المصدرة إلى جهات أخرى

غير قابل للتطبيق.

4.7 إعادة إصدار الشهادة (Re-Key)

إعادة إصدار الشهادة هي عملية إصدار شهادة جديدة للمشترك تتضمن مفتاحاً عاماً جديداً وفترة صلاحية جديدة، بينما قد تظل بقية معلومات الشهادة كما هي.

تدعم الهيئات المصدرة الفرعية لدى مصدر التكنولوجيا عملية إعادة إصدار الشهادة. وتتشابه عملية إعادة الإصدار (بما في ذلك التحقق من الهوية وإصدار الشهادة والتواصل مع الأطراف المعنية) مع عملية إصدار الشهادة الأساسية. يلتزم هذا النظام بمتطلبات طلب الشهادة الأولية، ما لم يُسمح بإعادة استخدام المعلومات التي تم التحقق من صحتها مسبقًا وفقًا لهذا النظام.

4.7.1 الظروف المؤدية إلى إعادة إصدار الشهادة

قد تتم إعادة إصدار الشهادة أثناء كونها لا تزال فعالة، أو بعد انتهاء صلاحيتها، أو بعد إبطالها. وقد تؤدي عملية إعادة الإصدار إلى إبطال أي شهادات أخرى فعالة من نفس النوع للمشترك.

4.7.2 الجهة المخوّلة بطلب شهادة لمفتاح عام جديد

وفقاً لإجراءات إصدار الشهادة الأساسية.

4.7.3 معالجة طلبات إعادة إصدار الشهادات
وفقاً لإجراءات إصدار الشهادة الأساسية.

4.7.4 إشعار المشترك بإصدار الشهادة الجديدة
وفقاً لإجراءات إصدار الشهادة الأساسية.

4.7.5 الأفعال التي تُعد قبولاً لشهادة مُعادة الإصدار
وفقاً لإجراءات إصدار الشهادة الأساسية.

4.7.6 نشر الشهادة المُعادة إصدارها من قبل الهيئة المصدرة
وفقاً لإجراءات إصدار الشهادة الأساسية.

4.7.7 إشعار إصدار الشهادة من قبل الهيئة المصدرة إلى جهات أخرى
وفقاً لإجراءات إصدار الشهادة الأساسية.

4.8 تعديل الشهادة

4.8.1 الظروف المؤدية إلى تعديل الشهادة
غير قابل للتطبيق.

4.8.2 الجهة المخوّلة بطلب تعديل الشهادة
غير قابل للتطبيق.

4.8.3 معالجة طلبات تعديل الشهادة
غير قابل للتطبيق.

4.8.4 إشعار المشترك بإصدار الشهادة المعدلة
غير قابل للتطبيق.

4.8.5 الأفعال التي تُعد قبولاً لشهادة معدلة
غير قابل للتطبيق.

4.8.6 نشر الشهادة المعدلة من قبل الهيئة المصدرة
غير قابل للتطبيق.

4.8.7 إشعار إصدار الشهادة المعدلة من قبل الهيئة المصدرة إلى جهات أخرى
غير قابل للتطبيق.

4.9 إبطال وإيقاف الشهادات
توفر مصدر التكنولوجيا إمكانية مستمرة للمشتركين وهيئة التسجيل وخدمة ضباط التسجيل المحليين لتقديم طلبات إبطال الشهادات عبر نظام إلكتروني متاح على مدار الساعة للمستخدمين المصادق عليهم.

لا يُسمح بإيقاف الشهادات مؤقتاً، إذ يُسمح فقط بالإلغاء الدائم.

يتم التعامل مع إبطال شهادات المشتركين وفقاً للأقسام التالية:

4.9.1 الظروف المؤدية إلى الإلغاء

4.9.1.1 شهادات الأشخاص المعنويين

تُبطل هيئة التسجيل الشهادة خلال 24 ساعة إذا تحقق أحد الأمور التالية:

1. استلام طلب كتابي من المشترك أو ممثل مفوض من الكيان؛
2. اكتشاف أن طلب الشهادة الأصلي لم يكن مصرحاً به ولا يمنح صلاحية بأثر رجعي؛
3. اكتشاف الهيئة المصدرة أو توافر أسباب معقولة للاعتقاد بوجود اختراق لمفتاح التوقيع الخاص؛
4. أصبحت المعلومات في الشهادة غير دقيقة.

4.9.1.2 شهادات الأشخاص الطبيعيين

يجوز للمشترك تقديم طلب إلغاء الشهادة (Revocation Request) عبر حساب جهة التسجيل على شبكة الإنترنت، أو من خلال زيارة مركز خدمة الزبائن، أو عبر تطبيق الهاتف المحمول الخاص بنظام التسجيل الرقمي الذاتي.

وتقوم جهة التسجيل التابعة لـ (مصدر التكنولوجيا) أو موظف التسجيل المحلي بمعالجة طلبات الإلغاء المتعلقة بالشخص الطبيعي خلال (24) ساعة في حال تحقق واحدة أو أكثر من الحالات الآتية:

1. استلام طلب إلغاء عبر الإجراءات الداخلية للمؤسسة؛ ومن الأمثلة الشائعة على ذلك إنهاء ارتباط الموظف بالمؤسسة واتخاذ إجراءات الانفكاك التي تتضمن إلغاء شهاداته الرقمية النشطة.
2. تقديم المشترك طلباً للإلغاء عبر القنوات المتاحة والمتفق عليها (مثل: الهاتف، البريد الإلكتروني، المقابلة الشخصية، أو تطبيق الهاتف المحمول الخاص بنظام التسجيل الرقمي الذاتي، وغيرها).
3. الحصول على دليل يثبت استخدام المشترك للشهادة بطريقة لا تتوافق مع إجراءات سياسة ممارسات التصديق (CPS)هذه، أو مع شروط وأحكام استخدام المشترك الموقعة.
4. التحقق من انتهاء صلاحية البطاقة الوطنية الموحدة أو جواز السفر الإلكتروني المستخدم في عملية التحقق من الهوية.

4.9.1.3 أي شهادات صادرة عن الهيئات الفرعية لدى مصدر التكنولوجيا

تضمن الهيئات المصدرة تنفيذ الإلغاء خلال 24 ساعة وتُبطل الشهادة خلال خمسة أيام إذا تحقق أحد الأمور التالية:

1. ثبوت أن الشهادة لم تعد متوافقة مع الفقرات 6.1.5 أو 6.1.6.
2. ثبوت سوء استخدام الشهادة.
3. انتهاك المشترك لالتزامات جوهرية في الاتفاقية.
4. تغيّر جوهري في معلومات الشهادة.
5. إصدار الشهادة خلافاً لهذا البيان.
6. احتواء الشهادة على معلومات غير دقيقة أو مضللة.
7. انتهاء أو إلغاء حق مصدر التكنولوجيا في إصدار الشهادات.
8. اشتراط هذا البيان للإبطال.
9. وجود طريقة مؤكدة أو مثبتة لاختراق المفتاح الخاص، أو إثبات خلل في طريقة توليده مثلاً المفاتيح الضعيفة في Debian.
10. صدور حكم بعدم أهلية المشترك قانونياً.

4.9.1.4 إبطال شهادة الهيئة الفرعية

تُبطل شهادة الهيئة الفرعية خلال سبعة أيام في حال تحقق أحد الشروط التالية:

1. استلام طلب إبطال كتابي.
2. إخطار مصدر التكنولوجيا للهيئة المصدرة بأن الطلب الأصلي غير مصرح به.
3. ثبوت اختراق المفتاح الخاص أو عدم التوافق مع الفقرتين 6.1.5 و6.1.6.
4. ثبوت سوء استخدام الشهادة.
5. اكتشاف مخالفة هذا البيان أثناء إصدار الشهادة.
6. اكتشاف أن الشهادة تحتوي معلومات مضللة أو غير دقيقة.
7. توقف الهيئة الفرعية عن العمل دون وجود جهة بديلة لدعم الإلغاء.
8. انتهاء أو إلغاء حق الهيئة الفرعية في إصدار الشهادات دون وجود ترتيبات للحفاظ على مستودعCRL/OCSP .
9. تُعد الإلغاء ضرورياً إذا نصّت سياسة الشهادات أو بيان ممارسات الشهادات للهيئة المصدرة (أي الجذرية) على ذلك.

لا يحدد هذا البيان الظروف الخاصة بإبطال شهادة مستجيب OCSP أو شهادة خدمة التحقق من التوقيع الخاصة بمصدر التكنولوجيا، باستثناء اختراق زوج المفاتيح المرتبط، والذي يُعد كارثة وفقاً لإجراءات التعافي من الكوارث واستمرارية الأعمال المعتمدة لدى مصدر التكنولوجيا. تركز الفقرات الفرعية التالية فقط على أحكام الإلغاء التي تنطبق على شهادات الكيانات النهائية الصادرة عن الهيئات الفرعية لمصدر التكنولوجيا.

4.9.2 الجهات المخوّلة بطلب الإلغاء

يجوز تقديم طلبات الإلغاء من الجهات التالية:

- هيئة التسجيل لدى مصدر التكنولوجيا أو ضباط التسجيل المحليين في الحالات الموضحة في القسم 4.9.1،
- المشترك نفسه فيما يتعلق بشهادته،
- أي طرف موثوق أو مزود برنامج تطبيقات يمتلك دليلاً على اختراق شهادة المشترك أو استخدامها في الترويج لبرمجيات خبيثة،
- مصدر التكنولوجيا وفقاً لتقديره (مثلاً، عند وجود اختراق معروف لمفتاح الهيئة المصدرة)،
- المشتركين، الأطراف الموثوقة، مزودي البرامج، وأي أطراف ثالثة أخرى يمكنهم تقديم بلاغات عن مشاكل الشهادات لإخطار مصدر التكنولوجيا بسبب معقول لبدء عملية الإلغاء.

لا تُقبل إلا طلبات الإلغاء المصرّح بها.

4.9.3 إجراءات طلب الإلغاء

إبطال شهادة شخص طبيعي مباشرة من قبل المشترك:

يجوز للمشترك تقديم طلب إبطال عبر بوابة Web RA أو تطبيق التسجيل الرقمي. تُعالج هذه الطلبات تلقائياً من قبل الهيئة المصدرة ذات الصلة.

معالجة الإلغاء من قبل هيئة التسجيل لشهادات الأشخاص المعنويين:

1. تُخصص هيئة التسجيل معرفاً فريداً لطلب الإلغاء، وتُسجّل المستندات المقدّمة تحت هذا المعرف.
2. تتحقق هيئة التسجيل من هوية مقدم الطلب كما هو موضح في القسم 3.4.

3. تتحقق هيئة التسجيل من صحة معلومات طلب الإلغاء.
4. تُجري هيئة التسجيل أي تحقيق مطلوب ضمن الأطر الزمنية المحددة في القسم 4.9.1، وقد يتضمن ذلك التواصل مع المشترك.
5. تنفذ هيئة التسجيل عملية الإلغاء.
6. تُبطل الهيئة المصدرة الشهادة، ويتم تحديث حالتها.
7. تُخطر هيئة التسجيل المشترك أو الكيان مقدم الطلب عبر البريد الإلكتروني بإتمام عملية الإلغاء.
8. تُحدّث هيئة التسجيل القائمة السوداء الداخلية بمعلومات الشهادة المبطلَة وظروف الإلغاء، مما قد يؤدي إلى تعديل ملف المخاطر الخاص بالمشترك. ويُطلب من المشترك تقديم هذه المعلومات قبل معالجة أي طلبات مستقبلية.

معالجة الإلغاء استناداً إلى بلاغات مشاكل الشهادات:

تحتفظ مصدر التكنولوجيا بقدرة مستمرة على مدار الساعة للاستجابة داخلياً لأي طلبات إبطال عالية الأولوية أو بلاغات عن مشاكل الشهادات. وتوفر تعليمات واضحة عبر صفحة مخصصة ضمن المستودع العام: https://pki.techsource.iq/repository/Certificate_Problem_Report.html.

يمكن للمشتركين، الأطراف الموثوقة، مزودي البرامج، وأي أطراف ثالثة إرسال البلاغات إلى: certificate.problem@techsource.iq.

ينبغي أن يتضمن البلاغ بيانات الاتصال الخاصة بالمرسل، نوع الاشتباه، والجهة المعنية(Subject) .

تباشر هيئة التسجيل تحقيقاً في بلاغ المشكلة خلال 24 ساعة من استلامه، وتقرر ما إذا كان ينبغي تنفيذ الإلغاء أو اتخاذ إجراءات أخرى، استناداً إلى المعايير التالية على الأقل:

- طبيعة المشكلة المزعومة.
- عدد البلاغات المستلمة بخصوص شهادة أو جهة معينة.
- الجهة المقدّمة للبلاغ (مثلاً، تُعد البلاغات الصادرة عن هيئة مكافحة البرمجيات الخبيثة أو جهة تنفيذ قانون أكثر موثوقية من البلاغات المجهولة).
- التشريعات المحلية ذات الصلة.

إذا تقرر إبطال الشهادة بناءً على بلاغ المشكلة، تُنفذ هيئة التسجيل إجراء الإلغاء وفق ما ورد أعلاه.

عند الاقتضاء، قد تُحيل مصدر التكنولوجيا هذه البلاغات إلى الجهات المختصة.

إجراء الإلغاء من قبل موظف التسجيل لشركة مصدر التكنولوجيا/ موظف هيئة التسجيل المحلية لشهادات الأشخاص الطبيعيين:

- يتحقق موظف التسجيل لشركة مصدر التكنولوجيا من طلب الإلغاء ويُطابق هوية المشترك كما هو موضح في القسم 3.4.
- يجوز موظف التسجيل لشركة مصدر التكنولوجيا/ موظف هيئة التسجيل المحلية التواصل مع المشترك و/أو داخلياً ضمن المؤسسة فيما يتعلق بطلب الإلغاء لتحديد ظروف الإلغاء بشكل أدق. ويتوقع موظف التسجيل لشركة مصدر التكنولوجيا/ موظف هيئة التسجيل المحلية بريداً إلكترونياً من القسم المعني (مثلاً، الإدارة المباشرة أو الموارد البشرية) يؤكد فيه أنه يمكنه المضي في تنفيذ عملية الإلغاء.

- يدخل موظف التسجيل لشركة مصدر التكنولوجيا/ موظف هيئة التسجيل المحلية إلى حسابه على بوابة Web RAويصدر أمراً مباشراً إلى الهيئة المصدرة المعنية لإبطال شهادة المشترك.
- تُبطل الهيئة المصدرة المعنية الشهادة، ويتم تحديث حالتها.
- يُخطر موظف التسجيل لشركة مصدر التكنولوجيا/ موظف هيئة التسجيل المحلية الأقسام المعنية داخلياً (مثل الموارد البشرية، أو الإدارة المباشرة) بإتمام عملية إبطال الشهادة.
- إذا اقتضى الأمر، يُحدّث موظف التسجيل لشركة مصدر التكنولوجيا/ موظف هيئة التسجيل المحلية القائمة السوداء الداخلية بالمعلومات الخاصة بالمشترك.

4.9.4 فترة السماح لطلب الإلغاء

لا توجد فترة سماح لطلب الإلغاء. تُعالج طلبات الإلغاء من قبل هيئة التسجيل لدى مصدر التكنولوجيا بشكل فوري بعد اتخاذ قرار الإلغاء، وفي جميع الأحوال ضمن الأطر الزمنية المحددة في القسم 4.9.1 من هذا البيان.

4.9.5 الإطار الزمني الذي يجب على الهيئة المصدرة فيه معالجة طلب الإلغاء

تُعالج طلبات إبطال الشهادات خلال 24 ساعة.

أما في حال بلاغات مشاكل الشهادات، تبدأ هيئة التسجيل لدى مصدر التكنولوجيا التحقيق خلال 24 ساعة من استلام البلاغ، وتباشر التواصل مع المشترك ومع الجهات المعنية (مثل سلطات إنفاذ القانون) عند الضرورة. ويُرسل إشعار مبدئي بالمشكلة إلى المشترك والجهة المبلّغة.

تُجري هيئة التسجيل تحقيقات إضافية بمشاركة مجلس حوكمة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا، والمشترك، وسلطات أخرى عند اللزوم، لتحديد الإجراء الواجب اتخاذه بشأن الشهادة موضوع البلاغ.

إذا خلُص التحقيق إلى وجود سبب من الأسباب المحددة في القسم 4.9.1، تُبطل الشهادة خلال الإطار الزمني المنصوص عليه.

بناءً على سبب الإلغاء، قد تتفق هيئة التسجيل مع المشترك على خطة لإصدار شهادة جديدة.

4.9.6 متطلبات التحقق من الإلغاء للأطراف الموثوقة

تقع مسؤولية التحقق من حالة الإلغاء لجميع الشهادات في السلسلة على الطرف الموثوق قبل أن يقرر الاعتماد على معلومات الشهادة. وتُوفر الهيئات المصدرة لمصدر التكنولوجيا معلومات الإلغاء من خلال الآليات المُدمجة ضمن الشهادة، وهي قائمة الإلغاء (CRL) وبروتوكول حالة الشهادة على الإنترنت(OCSP) .

4.9.7 تكرار إصدار قائمة الإلغاء (CRL)

تنشر الهيئات المصدرة لمصدر التكنولوجيا قوائم الإلغاء وفق جدول زمني منتظم، ويُطبق ما يلي:

- تُنشأ قائمة إبطال جديدة كل 24 ساعة،
- تُحدد صلاحية قائمة الإلغاء حقل nextUpdate بـ 26 ساعة.

4.9.8 أقصى زمن تأخير لقوائم الإلغاء

تُصدر القوائم من قبل الهيئات المصدرة لمصدر التكنولوجيا بشكل منتظم وفقاً للتكرار المذكور في القسم 2.3 من هذا البيان.

4.9.9 توفر التحقق من الإلغاء عبر الإنترنت

توفر الهيئات المصدرة لمصدر التكنولوجيا مستجيب OCSP متوافقاً مع6960 RFC ، وتُوقع شهادته من قبل نفس الهيئة. ويُتيح المستجيب المعلومات فوراً لتطبيقات الأطراف الموثوقة استناداً إلى إجراءات الهيئة بشأن الشهادات.

تتضمن شهادة OCSP الامتداد من نوع id-pkix-ocsp-nocheck حسب6960 RFC .

ويُذكر رابط OCSP الفعلي داخل الشهادات الصادرة عن الهيئات المصدرة لمصدر التكنولوجيا.

4.9.10 متطلبات التحقق من الإلغاء عبر الإنترنت

يدعم مستجيب OCSP طرائق HTTP GET وHTTP POST.

لحالة شهادات المشتركين:

- تكون صلاحية الاستجابات OCSP ثماني ساعات أو أكثر.
- لا تتجاوز صلاحية الاستجابة عشرة أيام.
- إذا كانت فترة الصلاحية أقل من 16 ساعة، تُحدث الهيئة المعلومات قبل منتصف الفترة.
- إذا تجاوزت الفترة 16 ساعة، تُحدث الهيئة المعلومات قبل ثماني ساعات من nextUpdate، ولا تتجاوز أربعة أيام بعد thisUpdate.

إذا تلقى مستجيب OCSP طلباً بخصوص رقم تسلسلي غير مستخدم، يُجيب بحالة "مُبطلة" حسب .6960 RFC وتراقب مصدر التكنولوجيا هذه الحالات كجزء من إجراءات المراقبة الأمنية، وأي حالة مماثلة تُحفّز تحقيقاً إضافياً.

4.9.11 أشكال أخرى لإعلان الإلغاء.

تعتمد الهيئات المصدرة لمصدر التكنولوجيا فقط على CRL و OCSP لنشر معلومات الإلغاء.

4.9.12 متطلبات خاصة متعلقة باختراق المفتاح

إذا اكتشفت مصدر التكنولوجيا أو اشتبهت باختراق المفتاح الخاص لأي من هيئاتها، تُعلن فوراً عن كارثة وتفعّل خطة استمرارية الأعمال. وتشمل الإجراءات ما يلي:

- تحديد نطاق الشهادات التي يجب إبطالها.
- إبطال الشهادات المتأثرة خلال 24 ساعة ونشر قائمة الإلغاء خلال 30 دقيقة.
- بذل جهود لإخطار الجهات الحكومية، المشتركين، والأطراف الموثوقة المحتملين.
- توليد زوج مفاتيح جديد للهيئة وفق السياسات والإجراءات التشغيلية.

طرق إثبات اختراق المفتاح:

- تقديم طلب CSR موقع بالمفتاح الخاص أو استجابة تحدٍ يمكن التحقق منها بالمفتاح العام،
- أو تقديم المفتاح الخاص نفسه.

4.9.13 ظروف التعليق

لا تدعم الهيئات المصدرة لمصدر التكنولوجيا إيقاف الشهادات مؤقتاً(Suspension) ، بل تقتصر الإجراءات على الإلغاء الدائم.

.

4.9.14 من يحق له طلب التعليق
غير قابل للتطبيق.

4.9.15 إجراءات طلب التعليق
غير قابل للتطبيق.

4.9.16 حدود فترة التعليق
غير قابل للتطبيق.

4.10 خدمات حالة الشهادات
يرجى الرجوع إلى القسم 4.9.6 من هذا البيان. بالإضافة إلى ذلك، تم اعتماد الأحكام التالية:

4.10.1 الخصائص التشغيلية
تنشر الهيئات المصدرة لشهادات التوقيع الرقمي لدى مصدر التكنولوجيا قوائم الإلغاء (CRLs) في المستودع العام الذي يمكن للأطراف الموثوقة الوصول إليه.

ويُوفر مستجيب OCSP التابع لهذه الهيئات واجهة HTTP متاحة علنًا للأطراف الموثوقة.

لا تُزال قيود الإلغاء من قائمة CRL أو من استجابات OCSP بعد انتهاء صلاحية الشهادات المُلغاة. وتضم قائمة CRL الامتداد "ExpiredCertsOnCRL" وفق تعريف معيار X.509 الصادر عن / ISO / IEC 9594-8 وتوصية ITU-T X.509 .

4.10.2 توفر الخدمة
يُتاح المستودع العام الذي تُنشر فيه معلومات الشهادات وقوائم الإلغاء على مدار الساعة وطوال أيام الأسبوع، مع ضمان توفر لا يقل عن 99.6% خلال فترة سنة واحدة.

وتشغّل الهيئات المصدرة لشهادات مصدر التكنولوجيا خدمات CRL و OCSPوتُديرها بموارد كافية لضمان وقت استجابة لا يتجاوز عشر ثوانٍ في الظروف التشغيلية الاعتيادية.

كما تُحافظ الهيئات المصدرة على جاهزية داخلية دائمة (7/24) للاستجابة الفورية لبلاغات مشاكل الشهادات ذات الأولوية العالية كما هو موضح في القسم 4.9.3، وتُحيل الشكاوى إلى سلطات إنفاذ القانون عند الاقتضاء أو تُبطل الشهادة موضوع الشكوى.

4.10.3 الميزات الاختيارية
لا يوجد نص خاص.

4.11 نهاية الاشتراك
ترتبط فترة الاشتراك بفترة صلاحية الشهادة. وينتهي الاشتراك عند انتهاء صلاحية الشهادة أو إبطالها.

4.12 حفظ واسترداد المفاتيح

4.12.1 سياسة وإجراءات حفظ واسترداد المفاتيح
لا تدعم الهيئات المصدرة لشهادات التوقيع الرقمي لدى مصدر التكنولوجيا حفظ المفاتيح الخاصة.

4.12.2 سياسة وإجراءات تغليف واسترداد مفاتيح الجلسات.

غير قابل للتطبيق.

5 الضوابط الخاصة بالمرافق والإدارة والتشغيل

يُحدد هذا القسم الضوابط الأمنية الفيزيائية والإجرائية التي تُطبقها مصدر التكنولوجيا ضمن عملياتها.

يُطبق برنامج إدارة أمن حوكمة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا (TS PKI GB) متطلبات أمن الشبكة وأنظمة الشهادات الصادرة عن منتدى المتصفحات وهيئات الشهادات(CA/Browser Forum) ، بما يشمل:

- الضوابط الأمنية الفيزيائية والبيئية.
- ضوابط سلامة الأنظمة، بما في ذلك إدارة التكوين والتغيير، إدارة التحديثات، إدارة الثغرات، واكتشاف أو منع البرمجيات المضرة.
- الحفاظ على سجل لجميع الأصول وإدارتها وفقاً لتصنيفها.
- أمان الشبكة وإدارة الجدران النارية، بما في ذلك تقييد المنافذ وتصفية عناوينIP .
- إدارة المستخدمين، فصل الأدوار الموثوقة، التوعية والتدريب.
- ضوابط الوصول المنطقي، تسجيل ومراقبة الأنشطة، والمراجعة المنتظمة لصلاحيات المستخدمين لضمان المحاسبة الفردية.

يتضمن البرنامج الأمني لـ (مصدر التكنولوجيا) إجراء تقييم سنوي للمخاطر يهدف إلى:

1. تحديد التهديدات الداخلية والخارجية المتوقعة التي قد تؤدي إلى الوصول غير المصرح به، أو الإفصاح، أو سوء الاستخدام، أو التعديل، أو الإتلاف لأي من بيانات الشهادات أو عمليات إدارتها.
2. تقييم احتمالية حدوث هذه التهديدات والأضرار المحتملة الناجمة عنها، مع مراعاة درجة حساسية بيانات الشهادات وعمليات إدارتها.
3. تقييم مدى كفاية السياسات والإجراءات وأنظمة المعلومات والتقنيات والتدابير الأخرى التي تتبعها (مصدر التكنولوجيا) لمواجهة تلك التهديدات.

وبناءً على نتائج تقييم المخاطر، تعمل (مصدر التكنولوجيا) على تطوير وتنفيذ وصيانة خطة أمنية تتألف من إجراءات وتدابير ومنتجات أمنية مصممة لتحقيق الأهداف المذكورة آنفاً، ولإدارة والسيطرة على المخاطر المحددة، وبما يتناسب مع مستوى حساسية بيانات الشهادات وعمليات إدارتها.

وتشتمل الخطة الأمنية على ضمانات إدارية وتنظيمية وتقنية ومادية ملائمة لحساسية بيانات الشهادات وعمليات إدارتها؛ كما تأخذ الخطة بنظر الاعتبار التقنيات المتاحة وتكلفة تنفيذ التدابير المحددة، مع تطبيق مستوى أمني معقول يتناسب مع الضرر الذي قد ينتج عن أي خرق أمني وطبيعة البيانات المراد حمايتها.

5.1 الضوابط الأمنية الفيزيائية

يضمن مجلس حوكمة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا تنفيذ ضوابط أمنية فيزيائية مناسبة في مرافق استضافة البنية التحتية. وتُوثّق هذه الضوابط كجزء من السياسات الداخلية وتُراجع بانتظام عبر تدقيقات داخلية تُجريها لجنة الحوكمة على فريق عمليات البنية التحتية.

5.1.1 موقع البناء وتصميمه

تُؤوي منشأة عالية الأمان تابعة لمصدر التكنولوجيا جميع المكونات الحرجة للبنية التحتية، حيث تُفرض ضوابط أمنية فيزيائية تمنع وصول الأشخاص غير المصرح لهم عبر أربع مستويات أمنية. وعند الجمع بين هذه الطبقات وآليات الحماية كالحراس، وأجهزة الاستشعار، والمراقبة بالكاميرات، يُتحقق مستوى عالٍ من الحماية من الوصول غير المصرح.

تقع منشآت الحوسبة التي تستضيف خدمات الهيئات المصدرة في مدينة بغداد، العراق.

5.1.2 الوصول الفيزيائي

تُحمي أنظمة الهيئة المصدرة التابعة لمصدر التكنولوجيا بطبقات أمنية فيزيائية متعددة (أربع مستويات)، ولا يمكن الوصول إلى المستويات الأدنى إلا بعد اجتياز المستويات الأعلى. وتُنفذ الأنشطة التشغيلية الحساسة ضمن مستويات أمنية مشددة.

تشمل الضوابط الأمنية الفيزيائية مراقبة الحراس للمداخل، التحقق الحيوي (البصمة)، والمراقبة عبر الكاميرات على مدار الساعة وطوال السنة، وتشكل طبقات متعددة من الحماية.

يُمنح الوصول للموقع عند تقديم بطاقة الهوية الوطنية والتي يتحقق منها الحارس، ويُسجل الاسم، ووقت الدخول والمغادرة، ويُسلّم الزائر بطاقة تعريفية. ولا يُسمح بالدخول ما لم يتم التصريح من أحد أعضاء مجلس الحوكمة ويجب أن يكون الزائر برفقة موظف موثوق.

ويُسمح بالدخول إلى حجرة الهيئة المصدرة فقط عند وجود موظفين موثوقين اثنين معاً.

5.1.3 الطاقة والتبريد

يوفر تصميم المنشأة وحدات UPS ومولدات احتياطية قادرة على دعم عمليات البنية التحتية في حالات انقطاع التيار. وتتوفر أنظمة UPS والمولدات لكامل المنشأة.

كما تم تركيب نظام تكييف مزدوج بالكامل في المناطق التي تحتوي على الأنظمة. وتُحافظ هذه الأنظمة على التشغيل في النطاق المحدد لدرجات الحرارة والرطوبة.

5.1.4 التعرض للماء

اتخذ مجلس حوكمة البنية التحتية إجراءات احترازية معقولة لتقليل تأثير تسرب الماء، بما في ذلك تركيب المعدات فوق أرضيات مضادة للكهرباء الساكنة ومزودة بكواشف للرطوبة.

5.1.5 الوقاية من الحريق والحماية منه

تلتزم المنشأة بالممارسات الرائدة واللوائح الأمنية المطبقة في العراق، وتُراقب على مدار الساعة، ومزودة بكواشف حرارة ودخان.

تُركب أنظمة إطفاء حرائق في المناطق المخصصة وتُفعل تلقائياً في حال نشوب حريق، ويمكن تفعيلها يدوياً عند الحاجة.

5.1.6 تخزين الوسائط

تُخزّن الوسائط الإلكترونية والبصرية وغيرها ضمن الضوابط الأمنية الفيزيائية المتعددة وتُحمى من التلف العرضي (الماء والحريق والتداخل الكهرومغناطيسي).

تُخزن وسائط النسخ الاحتياطي والتدقيق في خزنة مقاومة للحريق، وتُنسخ وتُحفظ في موقع التعافي من الكوارث.

5.1.7 التخلص من النفايات

يُتلف كل ورق أو وسائط تخزين يتم إنشاؤها داخل المنشأة الآمنة قبل التخلص منها. ويُفرم الورق باستخدام آلة تمزيق بنمط متقاطع. وتُطبق الإجراءات التالية على وسائط الحاسوب القابلة للإزالة:

- تُمنح الموافقة على إتلاف وسائط الحاسوب القابلة للإزالة.
- تُمحى الوسائط ثم تُتلف مادياً إذا لم تعد مطلوبة.
- يُحتفظ بسجل لعملية إتلاف الوسائط.
- تُرسل الوسائط بعد ذلك للتخلص منها.

تُتلف الأجهزة التشفيرية مادياً أو تُصفّر (zeroized) وفقاً لإرشادات الشركة المصنعة قبل التخلص منها.

5.1.8 النسخ الاحتياطي خارج الموقع.

تُنفّذ نسخ احتياطية كاملة وتزايدية بشكل دوري لأنظمة الهيئات المصدرة لشهادات التوقيع الرقمي لدى مصدر التكنولوجيا لضمان توفر بيانات كافية لاستعادة الأنظمة عند الحاجة.

تُؤخذ نسخة احتياطية كاملة واحدة على الأقل، بالإضافة إلى عدة نسخ تزايدية يومياً من الأنظمة العاملة للهيئات المصدرة، وفقاً لسياسات وإجراءات النسخ الاحتياطي الموثقة والتي يلتزم بها فريق عمليات البنية التحتية.

أما النسخ الاحتياطية للمعلومات الحساسة جداً (مثل المفاتيح الخاصة) فتُجرى فور انتهاء أي مراسيم مفاتيح، وفقاً لنص إجراءات المراسيم الموثقة.

تضمن مرافق النسخ الاحتياطي المناسبة نقل النسخ إلى موقع التعافي من الكوارث حيث تُخزن تحت نفس الضوابط الفيزيائية والتقنية والإجرائية المُطبقة في المنشأة الأساسية.

5.2 الضوابط الإجرائية

يتبع مجلس حوكمة البنية التحتية لمصدر التكنولوجيا ممارسات إدارية وشخصية تضمن بشكل معقول نزاهة وكفاءة موظفي البنية التحتية وأداءهم المرضي لمهامهم ضمن مجالات الحوكمة، التشغيل، وتقديم خدمات البنية التحتية.

تشمل الضوابط الإجرائية ما يلي:

5.2.1 الأدوار الموثوقة

يُعد جميع أفراد الطاقم الذين يشاركون في عمليات إدارة المفاتيح، أو مسؤولين، أو إداريين، أو ممن يؤدون مهام تؤثر جوهرياً على هذه العمليات، في مواقع موثوقة. ويُشترط إخضاع أي موظف مُعيّن في موقع موثوق إلى تحقق من الخلفية الأمنية قبل مباشرته للعمل، وتُراجع هذه الخلفية سنوياً.

الأدوار الموثوقة المعتمدة للهيئات المصدرة لشهادات التوقيع الرقمي تشمل:

- **مسؤول البنية التحتية للمفتاح العام (PKI Administrator):** يمتلك بيانات اعتماد برنامج الهيئة المصدرة، مسؤول عن إعداد وصيانة الهيئة.
- **مشغل البنية التحتية (PKI Operator):** مخول بتنفيذ دورة تشغيل الهيئة ويشارك في العمليات الحرجة كإصدار الشهادات للمشتركين.
- **مسؤول الأمن (Security Officer):** يمتلك بيانات اعتماد تتيح إعداد وحدات HSM وسياسات البنية التحتية أثناء مراسيم المفاتيح ذات الصلة.

- **موظف التسجيل (RA Officer):** مخول بتنفيذ عملية التحقق من طلبات الشهادات كجزء من معالجة طلبات الشهادات.
- **حراس بيانات التفعيل (M-of-N Custodians):** يحتفظون ببيانات تفعيل وحدات HSM وصناديق الهيئات التابعة.
- **مالك نطاق الهيئة (CA Domain Owner):** يمتلك بيانات اعتماد تخوله تنفيذ عمليات النسخ والاستعادة لوحدات HSM الخاصة بالهيئات التابعة.
- **مدقق وحدات HSM:** يمتلك بيانات اعتماد استخراج سجلات تدقيق وحداتHSM .
- **حراس مركز البيانات:** يمتلكون بيانات فتح مركز بيانات البنية التحتية أثناء تنفيذ عمليات الهيئة.
- **مسؤول الأنظمة:** مخول بتثبيت، إعداد، حل مشاكل، وصيانة أنظمة التشغيل وقواعد البيانات الداعمة.
- **مسؤول الشبكة:** مخول بتثبيت، إعداد، حل مشاكل، وصيانة معدات الشبكة الداعمة.

5.2.2 عدد الأشخاص المطلوبين لكل مهمة

يتبع فريق عمليات البنية التحتية لمصدر التكنولوجيا إجراءات تحكم صارمة لضمان فصل المهام بناءً على المسؤوليات الوظيفية، بحيث لا يمكن لأي شخص موثوق تنفيذ العمليات الحساسة بمفرده.

وتتطلب المهام الحساسة التالية مشاركة شخصين أو أكثر:

- الوصول الفيزيائي إلى الحجرة الآمنة التي تستضيف أنظمة الهيئات التابعة.
- الوصول إلى وحدات HSM وإدارتها.
- التحقق من طلبات الشهادات والموافقة على إصدارها.

يُسجل كل نشاط تشغيلي يتم تنفيذه من قبل الأشخاص ذوي الأدوار الموثوقة في سجل تدقيق آمن ويمكن التحقق منه.

5.2.3 التحقق من الهوية والمصادقة لكل دور

قبل مباشرة المهام المتعلقة بدور موثوق:

- يتحقق مجلس حوكمة البنية التحتية لدى مصدر التكنولوجيا من هوية وسجل الموظف من خلال إجراء فحوصات خلفية وأمنية.
- عند صدور تعليمات بذلك وفقاً لإجراءات البنية التحتية الداخلية، تُصدر فرق تشغيل المنشأة بطاقة دخول لكل موظف بحاجة إلى الوصول الفيزيائي إلى المعدات داخل الحجرة الآمنة.
- يصدر الطاقم المخصص في البنية التحتية (مثل مسؤولي الأنظمة) بيانات اعتماد أنظمة تقنية المعلومات اللازمة لموظفي الهيئات المصدرة لشهادات التوقيع الرقمي كي يتمكنوا من أداء مهامهم.

5.2.4 الأدوار التي تتطلب فصل المهام

تُحدّد الأدوار الموثوقة المذكورة في القسم 5.2.1 وفقاً لمبدأ فصل المهام المناسب.

5.3 ضوابط الموارد البشرية

5.3.1 المؤهلات والخبرات ومتطلبات التصريح الأمني

قبل تعيين أي موظف ضمن فريق البنية التحتية، سواء بصفة موظف، أو وكيل، أو متعاقد مستقل، يضمن مجلس حوكمة البنية التحتية لدى مصدر التكنولوجيا إجراء فحوصات للتحقق من الخلفية، والمؤهلات، والخبرة المطلوبة لأداء المهام المرتبطة بالوظيفة. وتشمل هذه الفحوصات:

- التحقق من هوية الشخص :يجب أن تتم من خلال:
  - التواجد الشخصي أمام موظفين موثوقين من قسم الموارد البشرية أو الأمن،
  - التحقق من وثائق تعريف صادرة عن جهات حكومية ومعترف بها دولياً وتحتوي على صورة شخصية.
- **التحقق من الموثوقية :**ويشمل إجراء فحص للخلفية يتناول على الأقل:
  - السوابق الجنائية للجرائم الجسيمة،
  - حالات التضليل أو الكذب من قبل المرشح،
  - مدى مناسبة الهيئات المُقدّمة،
  - وأي تصاريح أمنية تُعتبر ملائمة.

5.3.2 إجراءات التحقق من الخلفية

يُختار جميع الموظفين المعينين في أدوار موثوقة استناداً إلى النزاهة، والتحقق من الخلفية، والتصريح الأمني. ويحرص مجلس حوكمة البنية التحتية على إجراء هذه الفحوصات مرة واحدة سنوياً لجميع الأفراد في الأدوار الموثوقة.

5.3.3 متطلبات التدريب

يوفر مجلس الحوكمة التدريب الفني الأساسي لجميع الموظفين لتمكينهم من أداء مهامهم بكفاءة. ويُحدث هذا التدريب ويُنفذ سنوياً لموظفي الهيئات المصدرة لشهادات التوقيع الرقمي.

ويغطي البرنامج التدريبي مجموعة متنوعة من المواضيع ويقدمه مزيج من موظفي الهيئات ذوي الخبرة وخبراء خارجيين متخصصين في مجال الأمن والبنية التحتية. ويتوافق البرنامج مع متطلبات كل دور موثوق. وتشمل المواضيع ما يلي:

- نظرية ومبادئ البنية التحتية للمفتاح العام(PKI) .
- الضوابط البيئية وسياسات الأمن الخاصة بPKI .
- عمليات التسجيل والتحقق الخاصة بPKI .
- العمليات التشغيلية لPKI .
- تدريب عملي على منتجاتPKI .
- إجراءات التعافي من الكوارث واستمرارية الأعمال.

يحتفظ مجلس الحوكمة بوثائق شاملة تتضمن أسماء جميع الموظفين الذين خضعوا للتدريب، ويُقيّم باستمرار مستوى رضا المدربين. وفي نهاية كل دورة تدريبية، تُنظم اختبارات يحصل من ينجح فيها على شهادة رسمية. ويُعد اجتياز هذه الاختبارات إلزامياً لجميع الأدوار الموثوقة، بما في ذلك أخصائيي التحقق، قبل منحهم التصريح بالعمل في أدوارهم.

5.3.4 وتيرة ومتطلبات إعادة التدريب

يُقدَّم المنهاج التدريبي لجميع أفراد فريق البنية التحتية. ويُراجع ويُعدّل محتوى التدريب سنوياً ليتماشى مع أفضل الممارسات الحديثة وتحديثات أنظمة الهيئة.

5.3.5 وتيرة وتسلسل التناوب الوظيفي

يحرص مجلس الحوكمة على ألا يؤثر أي تغيير في موظفي الهيئات المصدرة على الكفاءة التشغيلية، أو استمرارية الخدمة، أو سلامة خدمات الهيئة.

5.3.6 العقوبات على التصرفات غير المصرح بها

لضمان المساءلة، يفرض مجلس حوكمة البنية التحتية عقوبات على الموظفين في حال ارتكاب تصرفات غير مصرح بها أو استخدام غير مصرح للأنظمة أو السلطات، وذلك استناداً إلى سياسات وإجراءات الموارد البشرية، والقوانين العراقية السارية.

5.3.7 متطلبات المتعاقدين المستقلين

يخضع المتعاقدون المستقلون وفرق عملهم لنفس إجراءات التحقق من الخلفية المطبقة على موظفي البنية التحتية لدى مصدر التكنولوجيا. وتشمل هذه الفحوصات:

- وجود سوابق جنائية تتعلق بجرائم جسيمة.
- التضليل أو تقديم معلومات خاطئة من قبل المرشح.
- مدى مناسبة الهيئات المقدّمة.
- التصاريح الأمنية المناسبة.
- حماية الخصوصية.
- الالتزام بشروط السرية.

5.3.8 الوثائق المقدمة إلى الموظفين

يوثّق مجلس الحوكمة جميع المواد التدريبية ويجعلها متاحة لجميع موظفي البنية التحتية.
كما يضمن المجلس أن الوثائق التشغيلية الأساسية متاحة للموظفين المعنيين، وتشمل على الأقل:
وثيقة ممارسات إصدار الشهادات (CPS) والسياسات الأمنية والأدلة التشغيلية والوثائق الفنية ذات الصلة بكل دور موثوق.

5.4 إجراءات تدقيق السجلات

تشمل إجراءات تدقيق السجلات تسجيل الأحداث وتدقيق الأنظمة، وتُنفذ بهدف الحفاظ على بيئة آمنة. يشمل ذلك أنشطة إدارة دورة حياة المفاتيح، مثل إنشاء المفاتيح والنسخ الاحتياطي والتخزين والاسترداد والإتلاف وإدارة الأجهزة التشفيرية والهيئة المصدرة (CA) ومستجيب حالة الشهادات(OCSP) .

يتم توليد سجلات تدقيق أمنية لجميع الأحداث المرتبطة بأمن الهيئة المصدرة، وهيئة التسجيل(RA) ، ومستجيبات OCSP، ويتم الاحتفاظ بها. ويُراجع فريق ضباط أمن المعلومات لدى مصدر التكنولوجيا هذه السجلات، وتخضع كذلك للمراجعة ضمن عمليات التدقيق الداخلي المنتظمة التي تُجريها وظيفة الامتثال على عمليات الهيئات المصدرة لشهادات التوقيع الرقمي.

5.4.1 أنواع الأحداث المُسجلة

تلتزم (مصدر التكنولوجيا) بتوثيق كافة الأحداث المتعلقة بالإجراءات المتخذة لمعالجة طلبات الشهادات وإصدارها، بما في ذلك جميع المعلومات المتولدة والوثائق المستلمة ذات الصلة بطلب الشهادة، مع تثبيت الوقت والتاريخ، وتحديد الموظفين المعنيين بالتنفيذ. تتيح (مصدر التكنولوجيا) هذه السجلات لمدققها المؤهل كدليل على امتثال هيئة التصديق (CA) لهذه المتطلبات.

تُولَّد سجلات تدقيق لجميع الأحداث المتعلقة بأمن وخدمات أنظمة الهيئات المصدرة لشهادات التوقيع الرقمي لدى مصدر التكنولوجيا. ويشمل كل سجل تدقيق، كحد أدنى، المعلومات التالية:

- تاريخ ووقت وقوع الحدث.
- مؤشر نجاح أو فشل الحدث (مثل: توقيع من الهيئة وإلغاء شهادة وتحقق من صحة شهادة).
- هوية الجهة أو المشغل الذي تسبب في الحدث.
- وصف الحدث.

حيثما أمكن، تُولَّد سجلات التدقيق تلقائياً، وإذا تعذّر ذلك، تُستخدم دفاتر أو نماذج ورقية. تحتفظ فرق تشغيل البنية التحتية بهذه السجلات سواء كانت إلكترونية أو غير إلكترونية، وقد تُعرض خلال عمليات التدقيق.

تُسجَّل الأحداث التالية المرتبطة بعمليات الهيئات المصدرة لشهادات التوقيع الرقمي:

1. أحداث إدارة دورة حياة مفاتيح الهيئات المصدرة لشهادات التوقيع الرقمي:
   - إنشاء، نسخ احتياطي، تخزين، استرداد، أرشفة، وإتلاف المفاتيح،
   - إدارة دورة حياة الأجهزة التشفيرية.
   - طلبات إصدار الشهادات والتجديد وإعادة الإصدار أو الإلغاء.
   - الموافقة أو رفض طلبات الشهادات.
   - توليد قوائم الإلغاء (CRLs) .
   - توقيع استجابات OCSP .
   - تقديم ملفات تعريف جديدة للشهادات أو إيقاف الملفات الحالية.
2. أحداث دورة حياة شهادة المشترك والهيئة المصدرة:
   - طلبات الشهادات وإعادة الإصدار والإلغاء.
   - جميع الشهادات الصادرة بما في ذلك الملغاة والمنتهية.
   - أدلة أنشطة التحقق (مثل التاريخ والوقت والاتصالات).
   - قبول ورفض طلبات الشهادات.
   - إصدار الشهادات.
   - تحديثات CRL بما في ذلك تحديثات OCSP إن وجدت.
   - توقيع استجابات OCSP .
3. الأحداث الأمنية، بما في ذلك:
   - محاولات الدخول الناجحة وغير الناجحة إلى أنظمة البنية التحتية.
   - العمليات الأمنية المنفذة.
   - تغييرات ملفات التهيئة الأمنية.
   - إدارة المستخدمين.
   - أعطال الأنظمة أو الأجهزة وغيرها من الحالات غير الطبيعية.
   - أنشطة أجهزة التوجيه وجدران الحماية.
   - الدخول والخروج من مرفق الهيئة.

كما يضمن مجلس الحوكمة الاحتفاظ بالمعلومات التالية التي لا تُنتَج مباشرة من قبل الهيئات المصدرة:

- بيانات موظفي الهيئة المصدرة وتغييرات ملفاتهم الأمنية.
- جميع نسخ وثيقةCPS .
- محاضر الاجتماعات.
- تقارير التدقيق الداخلي للامتثال.
- نسخ حالية وسابقة من ملفات التهيئة والدلائل التشغيلية للهيئات المصدرة.

5.4.1.1 سجلات أنشطة أجهزة التوجيه وجدران الحماية

تشمل السجلات ما يلي:

1. محاولات الدخول الناجحة وغير الناجحة إلى أجهزة التوجيه وجدران الحماية.
2. تسجيل جميع العمليات الإدارية على هذه الأجهزة (مثل تغييرات التهيئة، تحديثات البرامج الثابتة، وتعديلات التحكم في الوصول).
3. تسجيل جميع التعديلات على قواعد جدار الحماية (إضافة، تعديل، حذف).
4. تسجيل جميع أحداث النظام والأخطاء (مثل أعطال الأجهزة وتوقف البرامج وإعادة التشغيل).

5.4.2 حماية سجلات التدقيق

تحظى سجلات التدقيق بالحماية من خلال مزيج من الضوابط الأمنية الفيزيائية والإجرائية والتقنية على النحو التالي:

- تولّد أنظمة الهيئات المصدرة لشهادات التوقيع الرقمي سجلات تدقيق محمية تشفيرياً.
- تُحافظ على أمان سجلات التدقيق أثناء انتقالها عبر نظام النسخ الاحتياطي وأثناء أرشفتها.
- تُفرض سياسات التحكم بالوصول في أنظمة البنية التحتية لضمان منح صلاحيات القراءة فقط للأفراد المصرّح لهم كجزء من مهامهم التشغيلية.
- لا يمكن الوصول إلى الأنظمة التي تُخزّن فيها سجلات التدقيق إلا من قبل الأدوار المصرّح بها، وتُسجل أي محاولات للعبث بالسجلات وربطها بالموظف المسؤول.

5.4.3 إجراءات نسخ سجلات التدقيق احتياطياً

تنطبق القواعد التالية على نسخ سجلات التدقيق احتياطياً:

- تُخزّن وسائط النسخ الاحتياطي محلياً في الموقع الرئيسي للهيئات المصدرة لشهادات التوقيع الرقمي، في موقع آمن.
- تُخزَّن نسخة ثانية من بيانات وسجلات التدقيق في موقع التعافي من الكوارث الذي يوفر نفس مستوى الحماية الفيزيائية والبيئية المتوفرة في الموقع الرئيسي.

5.4.4 نظام تجميع السجلات (داخلي أو خارجي)

تبدأ العمليات الآلية للتدقيق تلقائياً عند تشغيل النظام وتنتهي عند إيقافه. في حال فشل النظام الآلي للتدقيق ووجود خطر على سلامة النظام أو سرية المعلومات المحمية، يقرر مجلس حوكمة البنية التحتية ما إذا كان يجب تعليق عمليات الهيئة المصدرة ذات العلاقة لحين تصحيح المشكلة.

5.4.5 الإخطار للجهة المسببة للحدث

عند تسجيل حدث من قبل نظام تجميع السجلات، لا يُطلب تقديم إشعار للفرد أو الجهة أو التطبيق الذي تسبب بالحدث.

5.4.6 تقييم الثغرات

تُجري فرق تشغيل البنية التحتية تقييماً سنوياً للمخاطر يتضمن ما يلي:

1. تحديد التهديدات المتوقعة الداخلية والخارجية التي قد تؤدي إلى الوصول غير المصرح به، أو الكشف أو التلاعب أو الإتلاف لأي بيانات شهادات أو عمليات إدارة الشهادات.
2. تقييم احتمالية هذه التهديدات وتأثيرها المحتمل مع مراعاة حساسية البيانات والعمليات.
3. تقييم مدى كفاية السياسات والإجراءات والأنظمة والتقنيات والترتيبات الأخرى لمواجهة هذه التهديدات.

كما تخضع الأنظمة والبنية التحتية لتقييمات أمنية دورية كما يلي:

- خلال أسبوع من تلقي طلب من منتدى المتصفحات وشهادات الجذر(CA/Browser Forum) .
- بعد أي تغييرات كبيرة على النظام أو الشبكة.
- كل ثلاثة أشهر على الأقل، على العناوين العامة والخاصة لأنظمة البنية التحتية الداعمة للهيئات المصدرة.

ينفذ هذا التقييم الدوري ذاتياً من قبل أفراد أمن المعلومات ضمن فريق التشغيل، كما يُنسّق مجلس الحوكمة إجراء تقييم خارجي واختبار اختراق سنوي من طرف ثالث بعد أي تغييرات جوهرية.

تُشارك نتائج التقييم مع مجلس الحوكمة والإدارة التشغيلية وتُنفّذ الإجراءات التصحيحية بناءً عليها. وتُجمع أدلة تنفيذ هذه التقييمات وتُؤرشف.

5.5 أرشفة السجلات

5.5.1 أنواع السجلات المؤرشفة

تقوم الهيئات المصدرة لشهادات التوقيع الرقمي بأرشفة جميع سجلات التدقيق كما هو مبيّن في القسم 5.4.1، بالإضافة إلى:

1. الوثائق المتعلقة بأمن أنظمة الهيئة المصدرة وأنظمة إدارة الشهادات.
2. الوثائق المتعلقة بالتحقق، الإصدار والإلغاء لطلبات الشهادات والشهادات نفسها.

5.5.2 مدة الاحتفاظ بالأرشيف

تُحتفَظ بسجلات التدقيق المؤرشفة لمدة لا تقل عن سنتين (2) وحتى سبع (7) سنوات. ويهدف ذلك لضمان توفرها عند الحاجة إلى التحقيق في حوادث أمنية أو مراجعة أحداث سابقة.

بالإضافة إلى ذلك، تحتفظ الهيئات المصدرة بما يلي:

- جميع الوثائق المؤرشفة المتعلقة بأمن أنظمة الهيئة وأنظمة إدارة الشهادات،
- جميع الوثائق المؤرشفة المتعلقة بالتحقق والإصدار والإلغاء لطلبات الشهادات،

وذلك حتى وقوع أحد الأمرين لاحقاً:

- آخر مرة تم فيها الاعتماد على هذه السجلات في عمليات التحقق أو الإصدار أو الإلغاء.
- أو انتهاء صلاحية شهادات المشترك ذات الصلة.

5.5.3 حماية الأرشيف

تُؤرشف السجلات بطريقة تضمن عدم إمكانية حذفها أو إتلافها. وتُطبّق ضوابط لضمان أن إدارة الأرشيف مقتصرة على موظفين مخولين فقط دون التأثير على سلامة أو موثوقية أو سرية السجلات المؤرشفة.

5.5.4 إجراءات نسخ الأرشيف

تُحتفَظ بنسخة واحدة فقط من كل أرشيف رقمي في كل من منشأة الهيئة الرئيسية وموقع التعافي من الكوارث. تستخدم فرق تشغيل البنية التحتية إجراءات موثقة للنسخ والاسترجاع والأرشفة تشرح كيفية إنشاء وتخزين ونقل بيانات الأرشيف.

5.5.5 متطلبات الطابع الزمني للسجلات

تشمل جميع الأحداث المُسجلة والمؤرشفة تاريخ ووقت وقوع الحدث. ويتم مزامنة وقت أنظمة الهيئة مع مصدر توقيت GPS.وتوفر خدمات الطابع الزمني دقة ±1 ثانية أو أفضل مقارنة بالتوقيت العالمي.UTC
ويُنفّذ الفريق التشغيلي إجراءً منتظماً للتحقق من أي انحراف في التوقيت وتصحيحه.

5.5.6 نظام جمع الأرشيف (داخلي أو خارجي)

يُدار نظام جمع الأرشيف من قبل الهيئة المصدرة داخلياً.

5.5.7 الإجراءات المتبعة للحصول على معلومات الأرشيف والتحقق منها

يُسمح فقط للموظفين المصرّح لهم والمصادق على هويتهم بالوصول إلى المواد المؤرشفة. تستخدم فرق تشغيل البنية التحتية لدى مصدر التكنولوجيا إجراءات النسخ الاحتياطي والاسترجاع والأرشفة الخاصة بهيئات التوقيع الرقمي، والتي توثّق كيفية إنشاء، ونقل، وتخزين معلومات الأرشيف. كما توفّر هذه الإجراءات معلومات عن نظام جمع الأرشيف.

5.6 تغيير المفتاح

للحد من تأثير اختراق المفتاح، يُستبدل مفتاح الهيئة المصدرة وفقاً لجدول زمني يضمن أن فترة صلاحية هيئة التوقيع الرقمي تتجاوز الحد الأقصى لمدة صلاحية شهادات المشتركين الصادرة بعد آخر إصدار.
يرجى الرجوع إلى القسم 6.3.2 من هذه الوثيقة لمعرفة تكرار تغيير المفتاح.
تُوفّر شهادات المفاتيح العامة الجديدة للمشتركين والأطراف المعتمدة من خلال طرق التوصيل المبينة في القسم 6.1.4.
ولأغراض إدارة الإلغاء، يُحتفظ بالمفاتيح الخاصة القديمة حتى انتهاء صلاحية جميع الشهادات الموقّعة بها.

5.7 اختراق النظام والتعافي من الكوارث

5.7.1 إجراءات التعامل مع الحوادث والاختراقات

عند رصد محاولة اختراق أو أي شكل آخر من أشكال الاختراق لهيئة التوثيق من قبل مجلس حوكمة البنية التحتية، يجري تحقيق لتحديد طبيعة ودرجة الضرر:

- في حال الاشتباه باختراق المفتاح الخاص للهيئة، تُتبع الإجراءات الواردة في خطة استمرارية الأعمال والتعافي من الكوارث الخاصة بمصدر التكنولوجيا.
- إن لم يكن الأمر متعلقاً بالمفتاح، تُقيّم مدى الأضرار لتحديد ما إذا كانت الهيئة بحاجة لإعادة البناء، أو أن بعض الشهادات فقط يجب إلغاؤها، أو أن المفتاح ينبغي اعتباره مخترقاً.
- يحدّد مجلس الحوكمة الإجراءات المتعلقة بالإبلاغ والتواصل ضمن خطة استمرارية الأعمال والتعافي من الكوارث. بخلاف حالات اختراق المفاتيح، تحدد خطة الطوارئ إجراءات الاستعادة عند تلف أو الاشتباه في تلف الموارد البرمجية أو البيانات.

5.7.2 تلف الموارد البرمجية أو البيانات

يُطبّق مصدر التكنولوجيا التدابير اللازمة لضمان استعادة خدمات الهيئات المصدرة لشهادات التوقيع الرقمي بالكامل في حال حدوث كارثة أو تلف في الخوادم أو البرمجيات أو البيانات، بناءً على موافقة مجلس الحوكمة لتفعيل إجراءات الاستجابة للحوادث.
تُفصّل خطة استمرارية الأعمال والتعافي من الكوارث الظروف التي تقتضي تفعيل إجراءات الطوارئ، والتي قد تشمل استخدام موقع التعافي من الكوارث. وتُختبر الخطة مرة واحدة سنوياً على الأقل، بما في ذلك سيناريوهات الانتقال إلى موقع التعافي.

5.7.3 إجراءات الاستعادة بعد اختراق المفتاح

في حال اختراق مفتاح أحد المشتركين، يُرجى الرجوع إلى القسم 4.9.
أما إذا اختُرِق المفتاح الخاص للهيئات المصدرة أو بيانات التفعيل المرتبطة به أو شهادةOCSP ، فإن ذلك يُعد حادثاً بالغ الخطورة يُفعّل الإجراءات المحددة في خطة الطوارئ واستمرارية الأعمال.

وبالنظر إلى الأهمية القصوى لهذا النوع من الحوادث وتأثيره على البنية التحتية الوطنية للمفاتيح العامة في العراق، يعقد مجلس الحوكمة اجتماعاً طارئاً لاتخاذ القرارات اللازمة وإدارة التواصل ضمن إطار خطط التعامل مع اختراق المفتاح وإنهاء الهيئة.
يرجى الرجوع إلى القسمين 4.9.1 و4.9.3 لمزيد من التفاصيل.

5.7.4 قدرات استمرارية الأعمال بعد الكوارث

عند حدوث كارثة أو تلف في الخوادم أو البرمجيات أو البيانات، تُفعّل خطة استمرارية الأعمال والتعافي من الكوارث لاستعادة القدرات التشغيلية الأساسية للهيئات المصدرة خلال مدة زمنية مناسبة.
وتركّز الخطة على استعادة الخدمات التالية، سواءً في الموقع الرئيسي أو في موقع التعافي:

- خدمات إصدار وإلغاء الشهادات.
- المستودع العام الذي تُنشر فيه قوائم الإلغاء وشهادات الهيئة.
- خدماتOCSP .

يتيح نظام النسخ الاحتياطي المستمر إمكانية الانتقال السلس إلى موقع التعافي خلال مدة لا تتجاوز اثنتي عشرة (12) ساعة (RTO).
تتضمن خطة استمرارية الأعمال العناصر التالية:

- شروط تفعيل الخطة.
- إجراءات الطوارئ.
- إجراءات التحويل والعودة.
- جدول الصيانة الدورية.
- متطلبات التوعية والتدريب.
- تحديد المسؤوليات.
- زمن استعادة الخدمة(RTO) .
- اختبار منتظم لخطة الطوارئ.
- خطة للحفاظ على أو استعادة العمليات الحيوية.
- متطلبات تخزين المواد التشفيرية في موقع بديل.
- تحديد فترة التوقف المقبولة.
- تكرار نسخ المعلومات والبرمجيات الأساسية.
- المسافة بين الموقع الرئيسي وموقع التعافي.
- إجراءات تأمين المقر خلال فترة ما بعد الكارثة.

5.8 إنهاء عمل الهيئة المصدرة أو الهيئة المسجِّلة

يتم إنهاء خدمات الهيئات المصدرة لشهادات التوقيع الرقمي في الحالات التالية:

أ) بقرار من الإدارة التنفيذية لمصدر التكنولوجيا.
ب) بقرار مبرّر من الجهة المشرفة الشركة العامة للاتصالات والمعلوماتية.
ت) بحكم قضائي نهائي وقطعي.
ث) عند تصفية أو إنهاء أعمال الهيئة.

عند تقرير اللجنة العليا لإدارة التوقيع الإلكتروني (ITPC PMA) ضرورة إنهاء الخدمات، ينفّذ مجلس الحوكمة خطة الإنهاء المتفق عليها مسبقاً مع الهيئة المشرفة.
تشمل خطة الإنهاء، على أقل تقدير، ما يلي:

- إخطار الهيئة المشرفة كتابياً قبل تسعين (90) يوماً من تاريخ التوقف عن تقديم خدمات الهيئة، مع تزويدها بنسخة من خطة الإنهاء.
- تفاصيل انتهاء أو عدم نية تجديد الترخيص إن وجد.
- ترتيبات الاحتفاظ بالسجلات المؤرشفة كما في القسم 5.5.
- ترتيبات الحفاظ على خدمات التحقق من صلاحية الشهادات طوال فترة صلاحية الشهادات المتبقية.
- إعلان نية الإنهاء في الصحف اليومية أو عبر الوسائل التي تحددها الهيئة المشرفة قبل ستين (60) يوماً من الإنهاء الفعلي أو تاريخ انتهاء الترخيص، أيهما أسبق.
- إجراء الاتصالات اللازمة مع الأطراف المعنية ونقل السجلات المؤرشفة الخاصة بهيئات التوقيع الرقمي إلى جهة وصاية مناسبة.
- وضع خطة لدعم المشتركين لدى مصدر التكنولوجيا في الانتقال إلى مزوّد خدمات موثوقة آخر قدر الإمكان.
- إلغاء جميع الشهادات الصادرة عن هذه الهيئة الفرعية والتي لم تُلغَ بعد أو لم تنتهِ صلاحيتها في نهاية فترة الإشعار، سواء طلب المشتركون إلغاءها أم لا.
- اتخاذ التدابير اللازمة لضمان عدم التسبب في أي انقطاع أو اضطراب للمشتركين أو الأطراف المعتمدة.
- ترتيب ما يلزم لضمان استمرار صيانة الأنظمة والإجراءات الأمنية الخاصة بالبيانات الحساسة والدقيقة.

6 الضوابط الأمنية التقنية

يحدد هذا القسم التدابير الأمنية التي تعتمدها مصدر التكنولوجيا لحماية مفاتيحها التشفيرية وبيانات التفعيل مثل: رموز PIN أو كلمات المرور أو رموز الوصول إلى المفاتيح (الخاصة بهيئات التوقيع الرقمي.

6.1 إنشاء أزواج المفاتيح وتثبيتها

6.1.1 إنشاء أزواج المفاتيح

6.1.1.1 الهيئات الفرعية لمصدر التكنولوجيا:

يتم إنشاء أزواج المفاتيح الخاصة بهيئات التوقيع الرقمي وتخزينها داخل ذاكرة وحدة أمن الأجهزة (HSM) الحاصلة على شهادة مطابقة لمتطلبات القسم 6.2.11.
ويُسجَّل حفل إنشاء المفاتيح بالفيديو ويُخزن بشكل آمن لأغراض التدقيق.

تحضر جهة تدقيق داخلية أو خارجية حفل إنشاء مفاتيح الهيئة، ويهدف هذا الحضور إلى إصدار تقرير يؤكد الآتي:

1. قامت مصدر التكنولوجيا بتوثيق إجراءات إنشاء وحماية مفاتيح الهيئة بما يتوافق مع بيان ممارسات الشهادات (CPS) وسياسة مزود خدمات التوثيق(TSP CP) .
2. تضمن نص سيناريو حفل إنشاء المفتاح تفاصيل مناسبة.
3. نُفذ الحفل بحضور النصاب القانوني من الأشخاص المصرح لهم، بمن فيهم ممثلو مجلس حوكمة البنية التحتية.
4. طُبقت ضوابط فعّالة توفر ضماناً معقولاً بأن زوج مفاتيح الهيئة قد أُنشئ وحُمي وفقاً للإجراءات الموثقة.
5. نُفذت جميع الإجراءات المطلوبة في نص سيناريو إنشاء المفتاح أثناء الحفل.

نوع الشهادة	متطلبات إنشاء المفاتيح
الشهادات الصادرة للأشخاص المعنويين شهاداتeSeal	يتم توليد زوج المفاتيح داخل وحدة أمن تشفير آمنة (HSM) ممتثلة لمعايير (FIPS 140-2) المستوى الثالث، أو المعايير المشتركة(Common Criteria EAL 4+) ، أو ما يعادلها، وتديرها شركة مصدر التكنولوجيا كجزء من خدمة التوقيع والختم الإلكتروني عن بُعد. ويظل المفتاح الخاص بالمشترك دائماً داخل وحدة التشفير، كما تُحدد خوارزميات توليد المفاتيح وأحجامها وفقاً لما ورد في القسمين (6.1.5) و(6.1.6) من سياسة ممارسة التصديق هذه.
الشهادات الصادرة للأشخاص الطبيعيين	**بالنسبة للشهادات المُنشأة على رمز تشفير عتادي :**يُنشأ زوج مفاتيح المشترك داخل ذاكرة جهاز تشفير عتادي يتوافق مع معيار FIPS 140 المستوى 2 ويمنع التصدير.
	بالنسبة لشهادات التوقيع عن بُعد المؤهلة: تُنشأ مفاتيح المشترك داخل وحدة أمن أجهزة (HSM) بمستوى FIPS 140-2 المستوى 3 وتُشغّل من قبل مصدر التكنولوجيا. تُستخدم خوارزمية إن إنشاء المفاتيح وأحجام المفاتيح وفقاً لما هو مذكور في القسمين 6.1.5 و6.1.6 من هذا البيان.

6.1.2 تسليم المفتاح الخاص للمشترك

لا يتم تسليم المفاتيح الخاصة للمشتركين.

بل يتم توليد المفاتيح الخاصة بالمشتركين وتخزينها بشكل آمن ضمن خدمة التوقيع والختم الإلكتروني عن بُعد التابعة لشركة مصدر التكنولوجيا، وذلك في بيئة تشفير خاضعة للرقابة. وتظل هذه المفاتيح داخل تلك البيئة في جميع الأوقات، ولا يتم عرضها للمشترك أو تمكينه من الوصول إليها بصيغتها النصية الصريحة.

يُمنح المشترك صلاحية التحكم في استخدام المفتاح الخاص من خلال آليات توثيق وتفويض قوية، دون السماح له بالوصول إلى المادة البرمجية للمفتاح الخاص نفسه.

6.1.3 تسليم المفتاح العام إلى جهة إصدار الشهادة

تقبل سلطات إصدار الشهادات الخاصة بتوقيع المستندات لدى مصدر التكنولوجيا طلبات توقيع الشهادة (CSR) فقط إذا صدرت عن ضابط التسجيل أو ضابط التسجيل المحلي الذين جرى التحقق من هويتهم من خلال بوابة الويب الخاصة بضابط التسجيل.

6.1.4 تسليم المفتاح العام لجهة الاعتماد

تنشر سلطات إصدار الشهادات الخاصة بتوقيع المستندات لدى مصدر التكنولوجيا شهادات مفاتيحها العامة في المستودع العام الخاص بها.

6.1.5 نوع الخوارزمية وأحجام المفاتيح

تُستخدم مفاتيح مشتركي الخدمة بأطوال 2048 بت RSA أو 4096 (بت RSA موصى بها).
تُستخدم مفاتيح سلطات إصدار الشهادات الخاصة بتوقيع المستندات لدى مصدر التكنولوجيا بخوارزمية ECDSA بحجم 384 بت.

6.1.6 إنشاء معلمات المفتاح العام والتحقق من جودتها

6.1.6.1 السلطات التابعة لمصدر التكنولوجيا

تُنشأ مفاتيح المصدر العام والخاص بواسطة خوارزميات حديثة وفقاً لمتطلبات FIPS 186-2 في التوليد العشوائي وفحوصات الأعداد الأولية. ويستند فريق عمليات البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا إلى القسم 6.1.6 من المتطلبات الأساسية للتحقق من الجودة.

6.1.6.2 المشتركون

يستخدم ضابط التسجيل المحلي تقنيات مناسبة للتحقق من صلاحية المفاتيح العامة المقدمة من قبل المشتركين.
وتُرفض المفاتيح المعروفة بأنها ضعيفة وفقاً لما ورد في القسم 6.1.6 من المتطلبات الأساسية لمنتدىCA/B .

6.1.7 أغراض استخدام المفاتيح حسب حقل Key Usage في X.509 V3

تتضمن الشهادات الصادرة عن سلطات توقيع المستندات التابعة لمصدر التكنولوجيا سلسلة بتات توضح استخدام المفتاح، وفقاً للوثيقة .[RFC 5280] يُرجى الرجوع إلى القسمين 7.1 و7.3 من هذا البيان.

6.2 حماية المفاتيح الخاصة وضوابط هندسة وحدات التشفير

6.2.1 معايير وضوابط وحدات التشفير

تُستخدم وحدات أمن عتادية معتمدة وفق معيار FIPS 140-2 المستوى 3 لإنشاء وتخزين المفاتيح الخاصة بسلطات توقيع المستندات. وتُحفظ هذه الوحدات داخل المنطقة الأشد أماناً في مرفق استضافة البنية التحتية للمفتاح العام.

6.2.2 السيطرة المتعددة n من m على المفتاح الخاص

تخضع المفاتيح الخاصة لسلطات توقيع المستندات لسيطرة مستمرة من قبل عدة أشخاص مخوّلين. يُوثق توزيع الأدوار الموثوقة والمسؤوليات المتعلقة بالمفاتيح الخاصة والبيانات السرية المرتبطة بها ضمن إجراءات إنشاء المفاتيح الداخلية الخاصة بمصدر التكنولوجيا.
تُعيَّن الأدوار الموثوقة من قبل مجلس إدارة البنية التحتية للمفتاح العام لضمان الفصل بين الواجبات، وتطبيق مبدأ السيطرة المتعددة والمعرفة المجزأة.
ويُطبّق نموذج m" من "n للتحكم، بحيث يتطلب تفعيل أو إعادة تفعيل المفتاح الخاص وجود ما لا يقل عن شخصين من بين ثلاثة من الحراس المعتمدين للمفاتيح، بحضور مديري وحداتHSM .

يحتفظ مجلس إدارة البنية التحتية بسجلات مكتوبة وقابلة للتدقيق حول توزيع الرموز السرية وكلمات المرور. وعند استبدال أي من الحراس أو المشغلين الموثوقين، يُتابع المجلس تجديد الرموز وتحديث معلومات التوزيع.

6.2.3 إيداع المفتاح الخاص

لا تُودع المفاتيح الخاصة لسلطات توقيع المستندات لدى أي طرف ثالث. بل تُطبق إجراءات مخصصة للنسخ الاحتياطي والاستعادة يديرها مجلس إدارة البنية التحتية.

6.2.4 نسخ احتياطي للمفتاح الخاص

يُحتفظ بنسخ احتياطية من المفاتيح الخاصة داخل خزائن مخصصة ضمن المناطق الأمنية القصوى لمرفق الاستضافة.
تُنفّذ عمليات النسخ كجزء من مراسيم إنشاء المفاتيح، وتُخضع عملية الاسترجاع لنفس ضوابط السيطرة المتعددة والمعرفة المجزأة.
يشمل إجراء المراسيم نقل النسخة الاحتياطية إلى موقع الاستعادة من الكوارث بمرافقة أفراد أمن معتمدين.

6.2.5 أرشفة المفتاح الخاص

لا يقوم مجلس إدارة البنية التحتية بأرشفة المفاتيح الخاصة لسلطات التوقيع.

6.2.6 نقل المفتاح الخاص إلى/من وحدة تشفير

يُسمح فقط بنقل أزواج المفاتيح إلى وحدة تشفير أخرى من نفس المواصفات وبشكل مباشر بين الأجهزة عبر قناة موثوقة وتحت إشراف عدة أشخاص.
ولا تُنسخ المفاتيح الخاصة على أي قرص أو وسائط أثناء هذه العملية.

6.2.7 تخزين المفتاح الخاص على وحدة تشفير

لا توجد أحكام إضافية خلاف ما ورد في الفقرات 6.2.1 و6.2.2 و6.2.4 و6.2.6.

6.2.8 طريقة تفعيل المفتاح الخاص

6.2.8.1 السلطات التابعة لمصدر التكنولوجيا

تُفعَّل المفاتيح الخاصة بموجب مبدأ السيطرة المزدوجة والمعرفة المجزأة باستخدام جهاز إدخال PIN متصل بوحدات HSMالخاصة بالسلطة.

6.2.8.2 المشتركون

بالنسبة لمفاتيح الأشخاص الطبيعيين المخزّنة على رموز تشفير عتادية: يقوم المشترك بربط الرمز بجهاز القارئ المناسب، وعند الطلب، يُدخل الرقم السري (PIN) المرتبط لتفعيل مفتاحه الخاص.

المفاتيح الخاصة لتوقيع الأشخاص الطبيعيين عن بُعد:
يتم تفعيل المفتاح الخاص بالتوقيع عن بُعد للمشترك من خلال بروتوكول توثيق وتفويض آمن يمتثل لمعيار (EN 419 241-2) بمستوى ضمان ثانٍ. ويتطلب هذا البروتوكول مشاركة المشترك لتفعيل المفتاح الخاص بالتوقيع أو الختم الإلكتروني عن بُعد.

6.2.9 طريقة إلغاء تفعيل المفتاح الخاص

6.2.9.1 السلطات التابعة لمصدر التكنولوجيا

تُلغى مفاتيح سلطات إصدار الشهادات الفرعية لدى مصدر التكنولوجيا وفقاً للتعليمات والوثائق الصادرة عن الشركة المصنّعة جهاز توليد المفاتيح الشفرية(HSM) .

6.2.9.2 المشتركون

يتحمّل المشتركون مسؤولية إلغاء تفعيل وحماية الوصول إلى أزواج مفاتيحهم، وذلك وفقاً للالتزامات الواردة في شروط واحكام استخدام المشترك.

6.2.10 طريقة إتلاف المفتاح الخاص

6.2.10.1 السلطات التابعة لمصدر التكنولوجيا

يُعدّ إتلاف المفتاح الخاص لسلطة إصدار الشهادات الفرعية خارج سياق انتهاء صلاحيته إجراءً خاصاً يتطلب تحقيقاً وموافقة خاصة من مجلس إدارة البنية التحتية للمفتاح العام.
وتشمل هذه العملية تعيين الأشخاص المشاركين.

تخضع عملية الإتلاف لإجراءات موثقة، ويجب أن تتم بمشاركة أشخاص مكلفين بأدوار موثوقة، وبحد أدنى ثلاثة موظفين من الملاك الموثوق، وبحضور ممثل واحد على الأقل من الهيئة الحاكمة للبنية التحتية للمفاتيح العامة (PKI GB)؛
بالإضافة إلى ذلك، يجب أن تتم عملية الإتلاف تحت إشراف ومددقة مدقق مؤهل.
يُتلف مفتاح سلطات توقيع المستندات من خلال إجراءات موثقة يُشارك فيها أفراد من أصحاب الأدوار الموثوقة (ثلاثة موظفين موثوقين على الأقل) وبحضور ممثل واحد على الأقل من مجلس الإدارة.
تُنفَّذ هذه الإجراءات وفقاً لمبدأ السيطرة المتعددة والمعرفة المجزأة، وتكفل إزالة المفتاح الخاص بشكل دائم من أي وحدة عتادية تم تخزينه فيها.

6.2.10.2 المشتركون

تُتلف المفاتيح الخاصة المرتبطة بخدمات التوقيع والختم الإلكتروني عن بُعد من قبل شركة مصدر التكنولوجيا داخل بيئة التشفير الخاضعة للرقابة (وحدة أمن التشفير) وفقاً لإجراءات إدارة دورة حياة المفاتيح المعتمدة.

وتضمن شركة مصدر التكنولوجيا إتلاف مفاتيح التوقيع فور إلغاء شهادة المفتاح العام المقابلة لها، إضافة إلى إتلافها بناءً على طلب المشترك. وتُنفذ عملية إتلاف المفاتيح بشكل آمن، بما في ذلك إزالة أي نسخ احتياطية مرتبطة بها.

ويتولى المشتركون مسؤولية طلب إلغاء شهاداتهم وفقاً للالتزامات المحددة في سياسة ممارسة التصديق هذه وشروط وأحكام استخدام المشترك.

6.2.11 تصنيف وحدات التشفير

تُعتمد وحدات التشفير المستخدمة من قبل سلطات توقيع المستندات لدى مصدر التكنولوجيا بموجب المعيار [FIPS 140-2]المستوى 3.

6.3 جوانب أخرى من إدارة أزواج المفاتيح

6.3.1 أرشفة المفتاح العام

يرجى الرجوع إلى القسم 5.5 للاطلاع على شروط الأرشفة.

6.3.2 مدة تشغيل الشهادة وفترة استخدام زوج المفاتيح

تكون شهادات سلطات توقيع المستندات صالحة لمدة ست (6) سنوات، مع فترة استخدام للمفتاح الخاص مدتها ثلاث (3) سنوات.
لا يُستخدم المفتاح الخاص للسلطة الفرعية بعد انتهاء صلاحية شهادة المفتاح العام المقترنة به.

كما لا يُستخدم لتوقيع شهادات الأطراف النهائية بعد انتهاء فترة استخدام المفتاح الخاص، باستثناء القوائم السوداء CRLs وشهادات مستجيب OCSP الخاصة بخدمة التحقق من صلاحية الشهادة.

تُحدد أقصى مدة صلاحية مسموح بها لشهادات المشتركين في القسم 7.1.

6.4 بيانات التفعيل

6.4.1 إنشاء بيانات التفعيل وتثبيتها

6.4.1.1 السلطات التابعة لمصدر التكنولوجيا

يُنشأ المفتاح الخاص وبيانات تفعيل وحدات HSM أثناء مراسيم إنشاء المفاتيح الخاصة بسلطات توقيع المستندات. يرجى الرجوع إلى القسمين 6.1.1 و6.2.8 من هذا البيان لمزيد من التفاصيل.

6.4.1.2 المشتركون

يقوم المشتركون بتعيين وحماية بيانات التفعيل الخاصة بمفاتيحهم الخاصة، بالقدر الكافي الذي يمنع فقدانها أو سرقتها أو الكشف عنها أو استخدامها بشكل غير مصرح به. وتُعرض هذه الالتزامات على المشتركين ضمن شروط واحكام استخدام المشترك.

6.4.2 حماية بيانات التفعيل

6.4.2.1 السلطات التابعة لمصدر التكنولوجيا

تضمن سياسة إدارة المفاتيح وإجراءات المراسيم لسلطات إصدار الشهادات الفرعية لدى مصدر التكنولوجيا تطبيق مبادئ السيطرة المتعددة والمعرفة المجزأة بشكل دائم لحماية المفاتيح وبيانات التفعيل الخاصة بوحدات HSM.
وأثناء مراسيم إنشاء المفاتيح (KGC)، تبقى بيانات التفعيل تحت حيازة الموظفين المعيّنين الموثوقين في هيئات الشهادات التابعة. يرجى الرجوع إلى القسمين 6.1 و6.2 لمزيد من التفاصيل.

6.4.2.2 المشتركون

يحمي المشتركون بيانات التفعيل الخاصة بمفاتيحهم الخاصة إلى الحد الذي يمنع فقدانها أو سرقتها أو الكشف غير المصرح به عنها أو استخدامها من دون إذن. وتُعرض هذه الالتزامات على المشتركين ضمن شروط واحكام استخدام المشترك.

6.4.3 جوانب أخرى لبيانات التفعيل

لا ينطبق.

6.5 ضوابط أمن الحاسوب

6.5.1 المتطلبات التقنية الخاصة بأمن الحاسوب

تضمن شركة مصدر التكنولوجيا تطبيق ضوابط أمن الحاسوب بما يتوافق على الأقل مع المعايير التقنية وإرشادات تعزيز الأمان التي تصدر عن الشركات المصنّعة. وتُوثق ضوابط أمن الحاسوب المطبّقة ضمن السياسات الداخلية لسلطات توقيع المستندات التابعة للشركة.

وتخضع أنظمة سلطات توقيع المستندات وعملياتها على وجه الخصوص للضوابط الأمنية التالية:

1. الفصل بين المهام وتطبيق آليات التحكم المزدوج لعمليات سلطات الشهادات.

2. تطبيق ضوابط الوصول الفيزيائي والمنطقي.
3. تسجيل الأحداث المتعلقة بالتطبيقات والأمن.
4. المراقبة المستمرة لأنظمة سلطات توقيع المستندات، وحماية نقاط النهاية.
5. آليات النسخ الاحتياطي والاستعادة الخاصة بعمليات سلطات توقيع المستندات.
6. تعزيز نظام التشغيل لخوادم سلطات توقيع المستندات وفق أفضل الممارسات وتوصيات الشركات المصنّعة.
7. بنية أمن شبكي متعمقة تتضمن جدران حماية داخلية وخارجية، وجدران حماية لتطبيقات الويب، وأنظمة كشف التسلل.
8. إدارة تصحيحات أمنية استباقية ضمن العمليات التشغيلية لسلطات توقيع المستندات.
9. تطبيق المصادقة متعددة العوامل على جميع الحسابات القادرة على تنفيذ إصدار الشهادات مباشرة.

6.5.2 تصنيف أمان الحاسوب

تخضع الجوانب التقنية لأمن الحاسوب لمراجعات دورية.

6.6 ضوابط دورة حياة التقنية

6.6.1 ضوابط تطوير الأنظمة

يُشحن أي عتاد أو برمجيات يتم شراؤها في حاويات مختومة ومضادة للعبث، ويقوم بتركيبها موظفون مؤهلون. ويتم اقتناء التحديثات الخاصة بالعتاد أو البرمجيات بنفس الطريقة التي تم بها اقتناء الأجهزة الأصلية. ويشارك موظفون موثوقون في تنفيذ إعدادات سلطات توقيع المستندات وفقاً لإجراءات تشغيل موثقة.

يُجرى اختبار وتطوير وتنفيذ التطبيقات وفقاً لأفضل الممارسات في مجال تطوير البرمجيات وإدارة التغييرات. ولا يُنشر أي برنامج أو تصحيح أو عتاد على الأنظمة الحيّة قبل أن يخضع لإجراءات التغيير والإعداد التي تفرضها عمليات البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا.

ويجري تعزيز جميع منصات الأجهزة والبرمجيات المستخدمة من قبل سلطات توقيع المستندات وفقاً لأفضل الممارسات والتوصيات الصادرة عن الشركات المصنّعة.

6.6.2 ضوابط إدارة الأمان

تُكرَّس الأجهزة والبرمجيات المستخدمة في إعداد سلطات توقيع المستندات لأداء مهام سلطات الشهادات فقط، ولا توجد تطبيقات أو أجهزة أو اتصالات شبكية أو مكونات برمجية أخرى غير تابعة للبنية التحتية للمفتاح العام متصلة بأجهزة سلطات الشهادات أو منصبة عليها.

ويُطبَّق إجراء لإدارة الإعدادات لضمان أن التكوينات والتعديلات والترقيات الخاصة بأنظمة سلطات توقيع المستندات موثّقة ومُسيطَر عليها من قبل إدارة عمليات البنية التحتية للمفتاح العام. يتم فحص تكوينات نظام شركة مصدر التكنولوجيا بانتظام، بحد أقصى فاصل زمني قدره أسبوع واحد بين عمليات الفحص.

كما يُنفَّذ إجراء لإدارة الثغرات لضمان فحص معدات سلطات توقيع المستندات للكشف عن البرمجيات الخبيثة عند الاستخدام الأول، وبعد ذلك بشكل دوري. ويُلزم هذا الإجراء بالاستجابة خلال 96 ساعة لاكتشاف أية ثغرة أمنية حرجة لم تُعالَج مسبقاً من قبل فريق العمليات.

6.6.3 ضوابط أمان دورة الحياة

يرجى الرجوع إلى القسم 6.6.1 للاطلاع على التفاصيل.

6.7 ضوابط أمن الشبكة

نفّذت شركة مصدر التكنولوجيا بنية قوية لأمن الشبكة تتضمن جدران حماية مدارة وأنظمة كشف التسلل. وقد تم تقسيم الشبكة إلى عدة مناطق بحسب العلاقات الوظيفية والمنطقية والفيزيائية.
وتُطبّق حدود شبكية لتقييد الاتصالات بين الأنظمة داخل المنطقة الواحدة وبين المناطق المختلفة، من خلال قواعد تدعم فقط الخدمات والبروتوكولات والمنافذ والاتصالات التي تم تحديدها كضرورية لعمليات سلطات توقيع المستندات، مع تعطيل كافة الحسابات والتطبيقات والخدمات والبروتوكولات والمنافذ غير المستخدمة في العمليات.

تُحفظ أنظمة الإصدار وأنظمة إدارة الشهادات وأنظمة الدعم الأمني ضمن منطقة شبكية عالية الأمان.

تُجرى فحوصات الثغرات الأمنية للشبكات بصورة دورية ربع سنوية (كل ثلاثة أشهر) كحد أدنى، كما تُنفذ اختبارات الاختراق سنوياً كحد أدنى. وتُحدد الفترات الزمنية للمعالجة بناءً على مستوى الخطورة؛ حيث يتم معالجة الثغرات "الحرجة" (Critical) خلال (24) ساعة، والثغرات "العالية" (High) خلال (48) ساعة، في حين يتم معالجة الثغرات ذات الخطورة "المنخفضة والمتوسطة" خلال (96) ساعة. ويتم توثيق أي استثناءات وإخضاعها لتقييم المخاطر وتسجيلها رسمياً.

6.8 الطابع الزمني

تُزامَن مكونات سلطات توقيع المستندات لدى مصدر التكنولوجيا بانتظام مع مصدر زمني موثوق. وتصل دقة خدمات الطابع الزمني إلى ±1 ثانية أو أفضل بالنسبة للتوقيت العالمي المنسق(UTC) .

7 الشهادات وقوائم الإلغاء وخدمة التحقق من حالة الشهادة(OCSP)

7.1 ملف الشهادة

7.1.1 رقم الإصدار

تصدر سلطات توقيع المستندات التابعة لشركة مصدر التكنولوجيا شهادات من الإصدار X.509 الإصدار 3 كما هو محدد في RFC 5280 .

7.1.2 امتدادات الشهادة

تُدعَم امتدادات X.509 v3 وتُستخدم بما يتماشى مع متطلبات CA/B Forum Baseline كما هو موضح في القسمين 7.1.10 و7.1.11 من هذه الوثيقة، حيث تُحدد تفاصيل محتوى الشهادات الصادرة عن سلطات توقيع المستندات التابعة لشركة مصدر التكنولوجيا.

7.1.3 معرفات كائنات الخوارزميات(OID)

تُصدر الشهادات باستخدام الخوارزميات المُشار إليها في معرف الكائن التالي:

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

7.1.4 نماذج الأسماء

تُحدد نماذج الأسماء في الشهادات الصادرة عن سلطات توقيع المستندات التابعة لشركة مصدر التكنولوجيا كما هو مذكور في القسم 3.1.1. يُرجى الرجوع إلى القسمين 7.1.10 و7.1.11 من هذه الوثيقة للاطلاع على تفاصيل محتوى الشهادات الصادرة.

7.1.5 قيود الأسماء

غير مطابق.

7.1.6 معرف كائن سياسة الشهادة

يُستخدم معرف كائن سياسة الشهادة كما هو محدد في RFC 3739 و.RFC 5280
تستخدم شركة مصدر التكنولوجيا معرفات كائن سياسة الشهادة المُعرّفة ضمن مخطط OID الوطني للبنية التحتية للمفتاح العام في العراق. وتُحدَّد المعرفات المستخدمة ضمن ملفات الشهادات في القسمين 7.1.10 و7.1.11.

7.1.7 استخدام امتداد قيود السياسة

لا يُدعَم استخدام امتداد قيود السياسة.

7.1.8 صياغة وتأويل مؤهِلات السياسة (Policy Qualifiers)

تتضمن شهادات شركة مصدر التكنولوجيا الصادرة للأطراف النهائية مؤهلاً لسياسة CPS يشير إلى وثيقة ممارسة الشهادة المعنية.

7.1.9 دلالات معالجة امتداد سياسات الشهادة الحرج

يجب معالجة امتدادات سياسات الشهادة وفقاً لما هو منصوص عليه في الوثيقةRFC 5280 .

7.1.10 ملفات شهادات هيئات التوقيع الرقمي لشركة مصدر التكنولوجيا

7.1.10.1 ملف شهادة الهيئة المصدِّق للأشخاص الطبيعيين لشركة مصدر التكنولوجيا

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Root CA Signature	Root CA's signature value
TBSCertificate					
Version	False	M			
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		<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 Document Signing Root 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 + **[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
CommonName		M	S	TS NP CA G1	UTF8 encoded
SubjectPublicKeyInfo	False	M			
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			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	
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.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/ds_root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://pki.itpc.gov.iq /repository/crls/ds_root_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M			

	keyCertSign, cRLSign		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.1.1.1	Root CPS OID
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://pki.itpc.gov.iq/repository/cps	
Basic Constraints Properties						
basicConstraints		True	M			
	cA		M	S	True	
	pathLenConstraint		M	S	0	

7.1.10.2 ملف شهادة الهيئة المصدِّق للأشخاص المعنويين لشركة مصدر التكنولوجيا

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Root CA Signature	Root CA's signature value
TBSCertificate					
Version	False	M	S		
Version		M	S	2	Version 3
SerialNumber	False	M	D		
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M	S		
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M	S	<Root CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)

OrganizationName		M	S	Informatics & Telecommunications Public Company	UTF8 encoded
CommonName		M	S	ITPC Document Signing 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
CommonName		M	S	TS LP 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	
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/ds_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/ds_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	2.16.368.1.1.1.1	Root cps OID
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.itpc.gov.iq/repository/cps	
Basic Constraints Properties					
basicConstraints	True	M	S		
cA		M	S	True	
pathLenConstraint		M	S	0	

7.1.11 الشهادات النهائية للجهات المشتركة

7.1.11.1 ملف شهادة الشخص الطبيعي المؤهل

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Natural Person Subordinate CA Signature.	Natural Person 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 NP 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	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
GivenName		M	D	Given Name of the natural person	UTF8 encoded
Surname		M	D	Surname of the natural person	UTF8 encoded
SERIALNUMBER		M	D	<Unique Identifier for each individual >	PrintableString encoded
OrganizationName		O	D	The Official name of the organization to which the natural person is affiliated	UTF8 encoded
CommonName		M	D	Concatenation of given name and surname as in government-issued ID card separated by a "space" character	UTF8 encoded

SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA	
SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate CA public key	
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/ts_np_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/ts_np_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST

						be supported as a minimum
Key Usage Properties						
keyUsage		True	M			
	nonrepudiation		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.2	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.1.3.1.2	Referring to Qualified Signing Certificate

7.1.11.2 ملف شهادة التوقيع المؤهل عن بُعد للشخص الطبيعي

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Natural Person Subordinate CA Signature.	Natural Person 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 NP 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	S	IQ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
GivenName		M	D	Given Name of the natural person	UTF8 encoded
Surname		M	D	Surname of the natural person	UTF8 encoded
SERIALNUMBER		M	D	<Unique Identifier for each individual >	PrintableString encoded
OrganizationName		O	D	The Official name of the organization to which the natural person is affiliated	UTF8 encoded
CommonName		M	D	Concatenation of given name and surname as in government-issued ID card separated by a “space” character	UTF8 encoded
SubjectPublicKeyInfo	False	M			

	AlgorithmIdentifier		M	D	RSA	
	SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions						
Authority Properties						
AuthorityKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate CA public key	
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/ts_np_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/ts_np_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum

Key Usage Properties					
keyUsage	True	M			
nonrepudiation		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.2.1.2	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.1.3.1.5	Referring to Remote Qualified Signing Certificate

7.1.11.3 ملف شهادة الشخص الطبيعي المتقدمة

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Natural Person Subordinate CA Signature.	Natural Person 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 NP 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	S	IQ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
GivenName		M	D	Given Name of the natural person	UTF8 encoded
Surname		M	D	Surname of the natural person	UTF8 encoded
SERIALNUMBER		M	D	<Unique Identifier for each individual >	PrintableString encoded
OrganizationName		O	D	The Official name of the organization to which the natural person is affiliated	UTF8 encoded
CommonName		M	D	Concatenation of given name and surname as in government-issued ID card separated by a “space” character	UTF8 encoded
SubjectPublicKeyInfo	False	M			

	AlgorithmIdentifier		M	D	RSA	
	SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions						
Authority Properties						
AuthorityKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate CA public key	
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/ts_np_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/ts_np_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum

Key Usage Properties					
keyUsage	True	M			
nonrepudiation		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.2.1.2	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.1.3.1.1	Referring to Advanced Signing Certificate

7.1.11.4 ملف شهادة التوقيع المتقدمة عن بُعد للشخص الطبيعي

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Natural Person Subordinate CA Signature.	Natural Person 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 NP 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	S	IQ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
GivenName		M	D	Given Name of the natural person	UTF8 encoded
Surname		M	D	Surname of the natural person	UTF8 encoded
SERIALNUMBER		M	D	<Unique Identifier for each individual >	PrintableString encoded
OrganizationName		O	D	The Official name of the organization to which the natural person is affiliated	UTF8 encoded
CommonName		M	D	Concatenation of given name and surname as in government-issued ID card separated by a “space” character	UTF8 encoded
SubjectPublicKeyInfo	False	M			

	AlgorithmIdentifier		M	D	RSA	
	SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions						
Authority Properties						
AuthorityKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate CA public key	
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/ts_np_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/ts_np_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum

Key Usage Properties					
keyUsage	True	M			
nonrepudiation		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.2.1.2	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.1.3.1.4	Referring to Remote Advanced Signing Certificate

7.1.11.5 ملف شهادة توقيع الشخص الاعتباري (الختم الإلكتروني)

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Legal Person Subordinate CA Signature.	Legal Person 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 LP 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	S	IQ	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	D	The Official name of the organization	UTF8 encoded
OrganizationalUnit		O	D	organizational unit name within the legal entity	UTF8 encoded
OrganizationIdentifier		M	D	An identification of the subject organization different from the organization name	UTF8 encoded
CommonName		M	D	A name commonly used by the subject to represent itself	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA	
SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	

Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate CA public key	
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/ts_lp_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/ts_lp_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M			
nonrepudiation		M	S	True	

Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.2.1.2	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.1.3.2.1	Referring to eSeal Certificate

7.1.11.6 ملف شهادة توقيع استجابة التحقق

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Subordinate CA Signature.	Subordinate CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M			
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 LP 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	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	Signature Verification Service	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	SHA-1 Hash of the Infrastructure CA's 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/ts_lp_ca.p7b	Subordinate Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/ts_lp_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Policy Properties						
keyUsage		True	M			
	digitalSignature		M	S	True	
Certificate Policies		False	M			
	policyIdentifier		M	S	2.16.368.1.2.1.2	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
Certificate Policies		False	M			
	policyIdentifier		M	S	2.16.368.1.1.3.3.3	

7.2 ملف قائمة الشهادات الملغاة(CRL)

7.2.1 رقم النسخة

تدعم الهيئات الفرعية لدى مصدر التكنولوجيا إصدار CRL الإصدار 2(X.509 v2) .

7.2.2 امتدادات CRL وامتدادات إدخالCRL

تستخدم هيئات توقيع المستندات لدى مصدر التكنولوجيا امتدادات CRL وامتدادات إدخال CRL كما هو موضح في القسم 7.2.3.

7.2.3 ملفات شهادات CRL للهيئات الفرعية

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

Natural Person Subordinate CA's CRL					
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 NP 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>

Legal Person Subordinate CA's CRL					
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 LP 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>

7.3 ملف بروتوكول التحقق من حالة الشهادة عبر الإنترنت(OCSP)

7.3.1 رقم النسخة

وفقاً لملف شهادة OCSP كما هو مذكور في القسم 7.3.3.

7.3.2 امتداداتOCSP

وفقاً لملف شهادة OCSP كما هو مذكور في القسم 7.3.3.

7.3.3 ملف شهادة OCSP لهيئات توقيع المستندات لدى مصدر التكنولوجيا

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

Natural Person Subordinate CA's OCSP Responder Certificate					
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 NP 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 + validity period	**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 NP CA G1 OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	

Extensions		M			
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Authority Properties					
AuthorityKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of the public key of the CA issuing the OCSP Certificate	
Policy Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			

هيكلية استجابة بروتوكول الاستعلام الآني عن حالة الشهادة

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

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

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

[1] In the current implementation of the OCSP, the ''ArchiveCutoff'' extension is included in OCSP responces only for certificates that have expired

8 التدقيق على الالتزام والتقييمات الأخرى

تهدف الإجراءات الموضحة في سياسة ممارسات التصديق (CPS) هذه إلى المواءمة مع المتطلبات المحددة في القسم (1)، وتغطية كافة العناصر المعمول بها في معايير البنية التحتية للمفاتيح العامة (PKI) الحالية ذات الصلة بقطاعات العمل التي تنشط فيها (مصدر التكنولوجيا).

8.1 تكرار أو ظروف التقييم

تنظم شركة مصدر التكنولوجيا تدقيقاً خارجياً وفق معيار WebTrust مرة واحدة على الأقل سنوياً، لضمان توافقها مع المتطلبات والمعايير والإجراءات ومستويات الخدمة المطبقة.
وتلتزم الشركة بقبول التدقيق على ممارساتها وإجراءاتها وتنشر تقرير التدقيق علناً في غضون ثلاثة أشهر كحد أقصى من نهاية فترة التدقيق.
يقوم مجلس حوكمة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا (TS PKI GB) واللجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية (ITPC PMA) بتقييم نتائج هذه التدقيقات قبل تنفيذ التوصيات ذات الصلة.

وتنفذ وظيفة الالتزام في مصدر التكنولوجيا تدقيقات سنوية على الهيئات المحلية لتسجيل الشهادات(LRAs) ، للتحقق من التزام موظفي هذه الهيئات (LRAOs) بالممارسات والمتطلبات المنصوص عليها في بيان ممارسات الشهادات(CPS) .

وبالإضافة لذلك، تُنفذ تدقيقات داخلية وفقاً لخطة تدقيق معتمدة من اللجنة العليا لإدارة التوقيع الإلكتروني .(PMA) ويمكن أيضاً إجراء تدقيقات غير مخططة في ظروف خاصة مثل خرق أمني، بناءً على طلب الهيئة.

8.2 هوية أو مؤهلات المُقيِّم

تُجرى تدقيقات WebTrust الخارجية من قبل مدققين مؤهلين يستوفون المتطلبات التالية:

- الاستقلالية عن الجهة الخاضعة للتدقيق.
- القدرة على إجراء تدقيق يتناول المعايير المحددة في WebTrust لهيئات التصديق.
- توظيف أفراد ذوي كفاءة في فحص تقنيات البنية التحتية للمفتاح العام، وأدوات وتقنيات أمن المعلومات، وتدقيق أنظمة المعلومات، ووظائف المصادقة من طرف ثالث.
- مرخص له من قبل WebTrust .
- الالتزام بالقانون أو التنظيم الحكومي أو مدونة مهنية للأخلاقيات.
- باستثناء الهيئات الحكومية الداخلية للتدقيق، يجب أن يحتفظ بتأمين مسؤولية مهنية ضد الأخطاء والسهو بقيمة لا تقل عن مليون دولار أمريكي.

8.3 علاقة المُقيِّم بالجهة الخاضعة للتقييم

في التدقيق الداخلي، لدى مجلس حوكمة البنية التحتية للمفتاح العام وظيفة تدقيق مستقلة عن فريق تشغيل البنية التحتية.
أما المدققون الخارجيون فهم جهات مستقلة مرخصة منWebTrust .

8.4 المواضيع المشمولة في التقييم

يُجرى التدقيق على هيئات توقيع المستندات لدى مصدر التكنولوجيا للتحقق من التزامها بالمعايير التالية:

- المبادئ والمعايير الخاصة بـ WebTrust لهيئات التصديق
- المبادئ والمعايير الخاصة بـ WebTrust لهيئات التصديق – أمن الشبكات–

راجع القسم 8.1 بشأن دورية التدقيقات. وراجع القسم 8.2 للاطلاع على مؤهلات المدققين.

8.5 الإجراءات المتخذة نتيجة وجود قصور

تُرفع القضايا والملاحظات الناتجة عن التقييم إلى مجلس حوكمة البنية التحتية للمفتاح العام.(TS PKI GB)
فيما يتعلق بتدقيق الالتزام على عمليات هيئات توقيع المستندات، فإن أي استثناءات أو أوجه قصور تُكتشف أثناء التدقيق تؤدي إلى اتخاذ قرار بالإجراءات اللازمة.
يتولى مجلس حوكمة البنية التحتية للمفتاح العام اتخاذ هذا القرار بالتشاور مع المدقق.
وفي حال ظهور استثناءات أو نواقص، يتحمل المجلس مسؤولية إعداد وتنفيذ خطة تصحيحية.
وبعد تنفيذ الخطة، يُطلق المجلس تدقيقاً إضافياً للتأكد من معالجة أوجه القصور التي تم تحديدها.

8.6 التواصل بنتائج التدقيق

يتم إرسال تقارير التدقيق الداخلي إلى TS PKI GB ولا يتم الكشف عنها لأطراف ثالثة غير مصرح لها. كما تُنشر تقارير تدقيق (WebTrust)السنوية للعامة في موعد لا يتجاوز ثلاثة (3) أشهر من تاريخ انتهاء فترة التدقيق؛ وفي حال حدوث تأخير يتجاوز هذه المدة، تلتزم (مصدر التكنولوجيا) بتقديم خطاب توضيحي موقع من قبل المدقق المؤهل. ويمكن الاطلاع على تقارير تدقيق (WebTrust) الخاصة بـ (مصدر التكنولوجيا) عبر الرابط الآتي:

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

8.7 التدقيق الذاتي

ترصد شركة مصدر التكنولوجيا من خلال وحدة الالتزام مدى تقيدها الصارم بالإجراءات المنصوص عليها في وثيقة بيان ممارسات الشهادات (CPS) وبمتطلبات خط الأساس الأحدث، من خلال إجراء تدقيقات داخلية منتظمة (بمعدل لا يقل عن ربع سنوي)، تشمل عينة عشوائية لا تقل عن 3% من الشهادات التي أُصدرت منذ آخر تدقيق داخلي.

9 أمور تجارية وقانونية أخرى

9.1 الرسوم

9.1.1 رسوم إصدار أو تجديد الشهادات

يتم الاتفاق على الرسوم، إن وجدت، بين مصدر التكنولوجيا والمشتركين.

9.1.2 رسوم الوصول إلى الشهادات

لا يوجد نص خاص.

9.1.3 رسوم الوصول إلى معلومات حالة الشهادة أو إلغائها

لن تُفرض رسوم مقابل الوصول إلى معلومات إلغاء الشهادات أو حالتها.

9.1.4 رسوم مقابل خدمات أخرى

قد تفرض شركة مصدر التكنولوجيا رسوماً مقابل خدمات أخرى حسب احتياجات العمل.

9.1.5 سياسة الاسترداد
لا تُقدم استردادات على أي رسوم تم تحصيلها.

9.2 المسؤولية المالية

9.2.1 تغطية التأمين
تضمن شركة مصدر التكنولوجيا أن تكون هيئات توقيع المستندات لديها مشمولة بأحكام التأمين القائمة.

9.2.2 أصول أخرى
لا يوجد نص خاص.

9.2.3 تغطية التأمين أو الضمان للجهات النهائية
راجع القسم 9.6.1.

9.3 سرية المعلومات التجارية

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

- المعلومات الشخصية للمشتركين التي لا تظهر ضمن الشهادات أو قوائم الإلغاء(CRLs) .
- المراسلات بين المشترك ووظيفة التسجيل أثناء إجراءات إدارة الشهادات (بما يشمل بيانات المشترك المُجمعة).
- الاتفاقيات التعاقدية بين مصدر التكنولوجيا وموردیها.
- الوثائق الداخلية الخاصة بمصدر التكنولوجيا (كإجراءات العمل والعمليات التشغيلية...).
- معلومات الموظفين السرية.

9.3.2 المعلومات الخارجة عن نطاق السرية
تُعدّ أي معلومات لم تُصنّف على أنها سرية من قبل شركة مصدر التكنولوجيا معلومات عامة. يشمل ذلك المعلومات المنشورة في مستودع مصدر التكنولوجيا العام.

9.3.3 المسؤولية عن حماية المعلومات السرية
تحمي شركة مصدر التكنولوجيا المعلومات السرية من خلال تدريب الموظفين وتطبيق السياسات على الموظفين والمتعاقدين والموردين.

9.4 خصوصية المعلومات الشخصية

9.4.1 خطة الخصوصية
تلتزم شركة مصدر التكنولوجيا بقواعد حماية البيانات الشخصية وخصوصية البيانات وفقاً لما ورد في سياسة الشهادات الحالية .(CP) راجع القسم 9.4.2 لنطاق المعلومات الخاصة، والقسم 9.4.3 للمعلومات غير المصنفة كمعلومات خاصة.
قد تُخضع المعلومات الخاصة وغير الخاصة لقواعد حماية البيانات إذا كانت تتضمن بيانات شخصية.
يُسمح فقط للموظفين الموثوق بهم بالوصول إلى المعلومات الخاصة بالمشتركين لغرض إدارة دورة حياة الشهادة.
لا تُفصح شركة مصدر التكنولوجيا عن أي معلومات خاصة دون موافقة مالك البيانات الشرعي أو بأمر قضائي صريح. وعند الإفصاح، تضمن الشركة عبر وسائل مناسبة ألا يُستخدم هذه المعلومات لأي غرض بخلاف الغرض الذي طُلبت من أجله.

وتلتزم الأطراف المخوّلة بالوصول بعدم الكشف عنها لطرف ثالث، وبالامتثال لقوانين حماية البيانات الشخصية ذات الصلة في جمهورية العراق.
وتحترم شركة مصدر التكنولوجيا جميع قوانين وأنظمة الخصوصية والمعلومات الخاصة والأسرار التجارية (عند الاقتضاء) المعمول بها، إضافةً إلى سياسة الخصوصية المنشورة الخاصة بها، وذلك في ما يتعلق بجمع المعلومات غير العامة واستخدامها والاحتفاظ بها والإفصاح عنها.
وتُستخدم القنوات الآمنة للحفاظ على سرية وخصوصية المعلومات المتبادلة بين المشترك وهيئة التسجيل أو بين الأنظمة، ويُستخدم التشفير الإلكتروني في الاتصالات مع أنظمة هيئة التصديق، ويشمل ذلك:

- الاتصالات بين أنظمة هيئة التسجيل والمشتركين؛
- الاتصالات بين أنظمة هيئة التصديق وأنظمة هيئة التسجيل؛
- الجلسات المخصصة لتسليم الشهادات.

9.4.2 المعلومات المصنفة كمعلومات خاصة

تُعد جميع المعلومات الشخصية غير المنشورة ضمن محتوى الشهادة أو قائمة الإلغاء معلومات خاصة.

9.4.3 المعلومات غير المصنفة كمعلومات خاصة

لا تُعد المعلومات الواردة في الشهادة أو قائمة الإلغاء معلومات خاصة.

9.4.4 المسؤولية عن حماية المعلومات الخاصة

يتعامل موظفو البنية التحتية للمفتاح العام ومورديها ومتعهديها مع المعلومات الشخصية بسرّية تامة، وفقاً للالتزامات التعاقدية لشركة مصدر التكنولوجيا، والتي توفر على الأقل نفس الحماية المنصوص عليها في القسم 9.4.1.

9.4.5 إشعار وموافقة على استخدام المعلومات الخاصة

تضمن شركة مصدر التكنولوجيا أن تُستخدم المعلومات الشخصية التي جُمعت فقط لغرض إدارة دورة حياة الشهادة، وبما يوافق عليه المشترك.

9.4.6 الإفصاح وفقاً للإجراءات القضائية أو الإدارية

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

9.4.7 حالات أخرى للإفصاح عن المعلومات

لا يوجد نص خاص.

9.5 حقوق الملكية الفكرية

تحتفظ شركة مصدر التكنولوجيا بجميع حقوق الملكية الفكرية المتعلقة بقاعدة بياناتها ومواقعها الإلكترونية وشهادات هيئات التصديق وأي منشور آخر صادر عن البنية التحتية للمفتاح العام، بما في ذلك هذه الوثيقة.(CPS)
وفي حال استخدام شركة مصدر التكنولوجيا برامج من موردين خارجيين، تبقى هذه البرامج ملكية فكرية لمورديها، ويخضع استخدامها لاتفاقيات الترخيص بين الطرفين.

9.6 التصريحات والضمانات

9.6.1 تصريحات وضمانات هيئة التصديق

تضمن شركة مصدر التكنولوجيا تنفيذ إجراءاتها وفقاً لما ورد في وثيقةCPS ، وأن جميع الشهادات الصادرة بموجب هذه الوثيقة تتوافق مع الأحكام المنصوص عليها.
وبمجرد إصدار الشهادة، تضمن شركة مصدر التكنولوجيا التصريحات التالية لفئات المستفيدين منها:

- المشترك الذي أبرم اتفاقية مشترك.
- جميع موردي البرمجيات التطبيقية الذين تربطهم اتفاقية مع IQ-NR-CA لإدراج الجذر في منتجاتهم.
- جميع الأطراف المعتمدة الذين يعتمدون بشكل معقول على الشهادة الصالحة.

وتؤكد شركة مصدر التكنولوجيا للمستفيدين من الشهادات أنه خلال فترة صلاحية الشهادة، التزمت هيئات توقيع المستندات لديها بمتطلبات خط الأساس وبوثيقة CPS في إصدار وإدارة الشهادات.

تشمل الضمانات تحديداً -دون حصر- ما يلي:

- **تفويض الشهادة:**
  أنها، في وقت الإصدار:
  - نفذت إجراءً للتحقق من أن الموضوع قد فوّض إصدار الشهادة.
  - طبقت هذا الإجراء عند إصدار الشهادة.
  - وصفت الإجراء بدقة في هذه الوثيقة.
- **دقة المعلومات:**
  أنها، في وقت الإصدار:
  - طبقت إجراءً للتحقق من دقة جميع المعلومات الواردة في الشهادة) باستثناء سمة subject:organizationalUnitName.
  - نفذت هذا الإجراء.
  - وصفت الإجراء بدقة في هذه الوثيقة.
- عدم وجود معلومات مضللة:
  أنها، في وقت الإصدار:
  - نفذت إجراءً للحد من احتمالية أن تكون سمة subject:organizationalUnitName مضللة.
  - طبقت هذا الإجراء.
  - وصفت الإجراء بدقة في هذه الوثيقة.
- **هوية مقدم الطلب:**
  إذا احتوت الشهادة على معلومات تعريف للموضوع، فإنها:
  - نفذت إجراءً للتحقق من هوية مقدم الطلب وفقاً للقسم 3.2.
  - طبقت هذا الإجراء.
  - وصفت الإجراء بدقة في هذه الوثيقة.
- **شروط واحكام استخدام المشترك:**
  إذا لم يكن المشترك كياناً تابعاً لهيئة التصديق، فإن اتفاقية قانونية صالحة تلزم الطرفين
  أما إذا كان المشترك كياناً تابعاً لها، فعلى ممثل مقدم الطلب تأكيد شروط الاستخدام.

- **الحالة:** تلتزم هيئات توقيع المستندات التابعة لشركة مصدر التكنولوجيا بتوفير مستودع متاح للجمهور على مدار الساعة طوال أيام الأسبوع يحتوي على معلومات محدثة حول حالة جميع الشهادات غير المنتهية (صالحة أو موقوفة).
- **الإيقاف:** تضمن شركة مصدر التكنولوجيا إيقاف الشهادة لأي سبب من الأسباب المحددة في هذه المتطلبات.

9.6.2 تصريحات وضمانات هيئة التسجيل

تضمن شركة مصدر التكنولوجيا قيامها بوظائف هيئة التسجيل وفقاً لما هو منصوص عليه في هذه الوثيقة(CPS) .

9.6.3 تصريحات وضمانات المشترك

المشتركون هم أفراد أو كيانات مؤسسية تُصدر الشهادات لصالحهم.

1. تقع على عاتق المشترك المسؤوليات الآتية:

- تقديم معلومات دقيقة وكاملة دائماً لشركة مصدر التكنولوجيا، سواء في طلب الشهادة أو أثناء عملية التحقق المحددة من قبل الشركة لنوع الشهادة المعني المراد إصداره من قبل سلطات تصديق توقيع المستندات التابعة للشركة.
- مراجعة محتويات الشهادة والتحقق من دقتها.
- تأمين المفتاح الخاص واتخاذ الاحتياطات المعقولة واللازمة لمنع ضياعه أو الكشف عنه أو تعديله أو استخدامه غير المصرح به ويشمل ذلك كلمة المرور أو الرمز المميز للأجهزة أو بيانات التفعيل الأخرى المستخدمة للتحكم في الوصول إلى المفتاح الخاص بالمشترك.
- استخدام شهادة المشترك للأغراض المخصصة لها فقط كما هو محدد في ممارسة التصديق هذه.
- إخطار شركة مصدر التكنولوجيا في حال كانت أي معلومات في الشهادة غير صحيحة أو أصبحت غير دقيقة.
- إخطار شركة مصدر التكنولوجيا فوراً في حال اختراق المفتاح أو كلما كان لدى المشترك سبب للاعتقاد بأن مفتاحه الخاص قد فُقد، أو تم الوصول إليه من قبل فرد آخر، أو تعرض للاختراق بأي شكل آخر.
- استخدام شهادة المشترك بطريقة لا تخالف القوانين النافذة في جمهورية العراق.
- التوقف فوراً عن استخدام المفتاح الخاص المقابل للمفتاح العام الوارد في شهادة المشترك عند إنهاء شروط وأحكام استخدام المشترك، أو عند إلغاء الشهادة أو انتهاء صلاحيتها.

2. يوافق المشترك على أن أي استخدام لشهادة المشترك للتوقيع أو الموافقة على محتويات أي سجل أو رسالة إلكترونية يُنسب إليه، كما يوافق على الالتزام قانوناً بمحتويات أي سجل أو رسالة إلكترونية من هذا القبيل.
3. يلتزم المشترك بتعويض شركة مصدر التكنولوجيا وهيئة التسجيل التابعة لها وإخلائهما من المسؤولية عن أي أضرار (بما في ذلك الرسوم القانونية) أو خسائر أو مطالبات أو دعاوى ناشئة عن:

- استخدام شهادة المشترك بطريقة غير مصرح بها أو تتعارض مع أحكام شروط وأحكام استخدام المشترك أو ممارسة التصديق وسياسة التصديق هذه.
- التلاعب بشهادة المشترك من قبل المشترك نفسه.
- وجود معلومات غير دقيقة أو مضللة في الطلب. كما يلتزم المشترك بتعويض شركة مصدر التكنولوجيا عن أي أضرار ورسوم قانونية تنشأ عن دعاوى أو مطالبات من قبل أطراف ثالثة تعتمد على شهادة المشترك أو تستخدمها، عندما تتعلق تلك الدعوى أو المطالبة بإخلال المشترك بالتزاماته الموضحة في ممارسة التصديق هذه أو شروط وأحكام الاستخدام، أو استخدام المشترك للشهادة أو الاعتماد عليها في أعماله التجارية، أو فشله في حماية مفتاحه الخاص، أو المطالبات المتعلقة بالمحتوى أو المعلومات والبيانات الأخرى التي قدمها المشترك أو كان ملزماً بتقديمها.

.

9.6.4 تصريحات وضمانات الطرف المعتمد

يتحمل الأطراف المعتمدون الذين يعتمدون على الشهادات الصادرة بموجب شركة مصدر التكنولوجيا الالتزامات التالية:

- استخدام الشهادة للغرض الذي أُصدرت من أجله، كما هو مبين في بيانات الشهادة (مثل امتداد استخدام المفتاح).
- التحقق من صلاحية الشهادة من حيث عدم انتهاء صلاحيتها.
- التأكد من مصدر الشهادة من خلال التحقق من مسار الشهادة وفقاً لتوصيات تعديل X.509 الإصدار الثالث.
- التأكد من أن الشهادة لم تُوقف، من خلال التحقق من حالة الإيقاف في المكان المحدد داخل الشهادة.
- التأكد من أن الشهادة توفر ضمانات كافية لاستخدامها المقصود.

9.6.5 تصريحات وضمانات المشاركين الآخرين

لا يوجد نص خاص.

9.7 إخلاء المسؤولية عن الضمانات

في حدود القانون العراقي، وبدون الإخلال بحالات الاحتيال أو سوء الاستخدام المتعمد، لا تتحمل شركة مصدر التكنولوجيا المسؤولية عن:

- دقة المعلومات الواردة في الشهادات، باستثناء ما يضمنه المشترك الذي يتحمل مسؤولية صحة ودقة جميع البيانات المُقدمة لشركة مصدر التكنولوجيا بغرض إدراجها في الشهادة.
- الأضرار غير المباشرة الناتجة عن أو المتعلقة باستخدام أو تقديم أو إصدار أو عدم إصدار الشهادات أو التواقيع الرقمية.
- أي إساءة استخدام من طرف ثالث يخالف القوانين العراقية، بما يشمل انتهاك حقوق الملكية الفكرية أو نشر البرمجيات الخبيثة أو الوصول غير القانوني إلى أنظمة الحاسوب.
- أي أضرار مباشرة أو غير مباشرة ناتجة عن توقف غير قابل للتحكم في خدمات هيئات توقيع المستندات.
- أي شكل من أشكال التحريف أو التمثيل الخاطئ للمعلومات من قبل المشتركين أو الأطراف المعتمدة بناءً على المعلومات الواردة في هذه الوثيقة أو أي وثائق عامة ذات صلة.

9.8 حدود المسؤولية

- لا تتحمل شركة مصدر التكنولوجيا المسؤولية تجاه المشتركين عن أية أضرار ناجمة عن إهمالهم أو احتيالهم أو سوء استخدامهم المتعمد.
- لا تتحمل الشركة أي مسؤولية تتعلق باستخدام الشهادات أو أزواج المفاتيح العامة أو الخاصة خارج نطاق الاستخدام المحدد في هذه الوثيقة. ويلتزم المشترك بتعويض الشركة عن أية مسؤوليات وتكاليف تنشأ عن هذا الاستخدام.
- لا تتحمل الشركة أي مسؤولية تجاه أي طرف عن أية أضرار ناجمة عن انقطاع خارج عن السيطرة في خدماتها.
- يتحمل المشترك المسؤولية عن أي تحريف للمعلومات في الشهادة، حتى وإن كانت شركة مصدر التكنولوجيا قد وافقت على تلك المعلومات.
- يلتزم المشترك بتعويض الطرف المعتمد في حال تكبده خسائر بسبب إخلال الشركة بشروط واحكام استخدام المشترك.
- يتحمل الطرف المعتمد نتائج تقصيره في الالتزام بواجباته.
- تنفي الشركة مسؤوليتها المالية أو غيرها عن الأضرار الناتجة عن تشغيل هيئات توقيع المستندات.

.

9.9 التعويضات

غير قابل للتطبيق.

9.10 المدة والإنهاء

9.10.1 المدة

تُعتمد هذه الوثيقة (CPS) من قبل مجلس إدارة البنية التحتية للمفتاح العام (TS PKI GB) وتبقى سارية حتى يتم إصدار تعديل ونشره في مستودع مصدر التكنولوجيا العام.

9.10.2 الإنهاء

تُطبَّق التعديلات على هذه الوثيقة وتُعتمد من قبل مجلس إدارةTS PKI ، وتُحدد من خلال إصدار نسخة جديدة. وبمجرد نشر النسخة المحدثة في المستودع العام، تصبح سارية المفعول. وتحتفظ شركة مصدر التكنولوجيا بالنسخ الأقدم مؤرشفة في مستودعها العام.

9.10.3 أثر الإنهاء واستمرارية الأحكام

يتولى مجلس إدارة البنية التحتية للمفتاح العام في مصدر التكنولوجيا (TS PKI GB) التواصل بشأن شروط وآثار إنهاء هذه الوثيقة (CPS) عبر الآليات المناسبة.

9.11 الإشعارات الفردية والتواصل مع المشاركين

يمكن توجيه الإشعارات المتعلقة بهذه الوثيقة إلى عنوان التواصل مع مجلس إدارة TS PKI كما هو مذكور في القسم 1.5.

9.12 التعديلات

عند الحاجة لإجراء أي تعديل على هذه الوثيقة، يدمج مجلس إدارة TS PKI هذا التعديل في نسخة جديدة ويقوم، بعد الموافقة عليها، بنشر النسخة الجديدة، والتي تحمل رقماً جديداً.

9.12.1 إجراءات التعديل

يرجى الرجوع إلى القسم 9.12.

9.12.2 آلية وفترة الإشعار

تصبح النسخة الأحدث من هذه الوثيقة نافذة المفعول فور نشرها في المستودع العام لمصدر التكنولوجيا. تُؤرشف النسخ السابقة في ذات المستودع.

يتولى مجلس إدارة TS PKI تنسيق الاتصالات المتعلقة بتعديلات هذه الوثيقة وتأثيراتها.

يحتفظ المجلس بالحق في تعديل الوثيقة دون إشعار مسبق، في حال كانت التعديلات غير جوهرية، بما في ذلك، على سبيل المثال لا الحصر، تصحيح الأخطاء الطباعية أو إجراء تحسينات طفيفة.

9.12.3 الظروف التي تتطلب تغييرOID

تحتفظ شركة مصدر التكنولوجيا بحق تعديل محتوى أي وثيقة CPS منشورة. ولا يتم تغيير معرف الكائن (OID) نتيجة لتعديلات كبيرة على هذه الوثيقة، ما دامت النسخة المعدلة صالحة ومعمول بها ضمن مستودع الشركة العام.

9.13 أحكام تسوية النزاعات

يُعالج أي نزاع متعلق بأحكام هذه الوثيقة وخدمات هيئات توقيع المستندات من قبل الشؤون القانونية في مجلس إدارة TS PKI. وفي حال عدم نجاح الوساطة، تُحال القضية إلى المحاكم المختصة في جمهورية العراق.

9.14 القانون الحاكم

تخضع قابلية التنفيذ والتفسير والصياغة القانونية وصحة هذه الوثيقة لأحكام قوانين جمهورية العراق.

9.15 الامتثال للقوانين المعمول بها

تتوافق هذه الوثيقة وتقديم خدمات هيئات توقيع المستندات مع القوانين العراقية المعمول بها.

9.16 أحكام متنوعة

9.16.1 الاتفاق الكامل

لا يوجد نص.

9.16.2 التنازل عن الحقوق

باستثناء ما هو محدد في العقود الأخرى، لا يجوز لأي طرف نقل أو تفويض الحقوق أو الالتزامات المنصوص عليها في هذه الوثيقة دون موافقة خطية مسبقة من شركة مصدر التكنولوجيا.

9.16.3 القابلية للفصل

في حال تقرر أن أي حكم من أحكام هذه الوثيقة غير صالح أو غير قابل للتنفيذ، تبقى باقي الأحكام سارية حتى يتم تحديث هذه الوثيقة.

وفي حال تعارض أي من متطلبات الخط الأساسي مع القوانين العراقية، يجوز لشركة مصدر التكنولوجيا تعديل المتطلب المتعارض بالحد الأدنى اللازم لجعله قانونياً في العراق. وينطبق ذلك فقط على العمليات أو إصدارات الشهادات الخاضعة لهذا القانون.

في مثل هذه الحالات، تُدرج شركة مصدر التكنولوجيا في هذا القسم مرجعاً مفصلاً للقانون الذي يتطلب التعديل، والتعديل المطبق على المتطلبات.

كما تُخطر الشركة منتدى CA/Browser بالمعلومات المضافة إلى وثيقة CP/CPS قبل إصدار أي شهادة تخضع لهذا التعديل.

يُلغى هذا التعديل عند زوال سبب التعديل القانوني أو عند تعديل متطلبات الخط الأساسي بشكل يتيح التوافق مع القانون. ويُنفذ التعديل المناسب في الممارسة، ويُعدَّل CP/CPS ويُرسل الإشعار إلى منتدى CA/Browser خلال مدة أقصاها تسعون (90) يوماً.

9.16.4 التنفيذ (أتعاب المحامين والتنازل عن الحقوق)

لا يوجد نص.

9.16.5 القوة القاهرة

لا تتحمل شركة مصدر التكنولوجيا المسؤولية عن أي تأخير أو فشل في الأداء بموجب هذه الوثيقة إذا كان ناتجاً عن أسباب خارجة عن إرادتها المعقولة، بما في ذلك، على سبيل المثال لا الحصر، انقطاع أو تأخر خدمات الاتصالات.

9.17 أحكام أخرى

لا يوجد نص.