مصدر التكنولوجيا

لخدمات النظم والبرمجيات

والتجارة العامة المحدودة

البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI)

هيئة التصديق لشهادات الاتصال الآمن (TLS)

بيان ممارسة الشهادات

التحكم بالوثيقة

أُعد/حُدثَ بواسطة	راجعه	وافق عليه	المالك	الإصدار	تاريخ الموافقة
			مصدر التكنولوجيا	1.3	

سجل التغييرات

الرقم التسلسلي	الإصدار	وصف التغييرات	المسؤول
0.1	08/02/2023	النسخة الأولية	مصطفى طوير
0.2	23/02/2023	مراجعة داخلية وتحديث	أحمد إبراهيم
0.3	05/07/2023	• تحديث في القسم 3.2.2.1. • تحديث القسمين 7.1.10.2 و7.1.10.3.2 بما يتماشى مع القسم 9.2 من إرشادات التحقق الموسَّع.(EV)	مصطفى طوير
0.4	29/11/2023	إزالة شهادة التحقق الموسَّع (EV) من النطاق إضافة قيم معرفات الكائن (OIDs) و معلومات الاتصال وعنوان المستودع تطبيق قالب شركة مصدر التكنولوجيا	مصطفى طوير و ياسر خان
0.5	28/02/2024	مراجعة وتحديث استناداً إلى ملاحظات المدقق بشأن سياسة الشهادات وبيان ممارسة الشهادات لهيئة التصديق الجذرية وسياسة الشهادات لمزوّد خدمات الثقة (TSP)	مصطفى طوير و ياسر خان
0.6	28/04/2024	تحديث في القسم 5.4.1 ليتماشى مع القسم 5.4.1 من الإصدار الأحدث لمتطلبات القواعد الأساسية لشهادات SSL والإصدار 2.0.4.	مصطفى طوير
0.7	15/05/2024	مراجعة وتحديث استناداً إلى ملاحظات المدقق بشأن بيانات ممارسة الشهادات.(CPSs)	مصطفى طوير و ياسر خان
1.0	15/07/2024	تحديثات استناداً إلى توصيات المدقق بعد تدقيق نقطة في الزمن	مصطفى طوير و ياسر خان
1.1	18/05/2025	• إدخال آلية التحقق متعدد المنظورات لعملية الإصدار. • المواءمة مع متطلبات برامج مخازن الجذور.	شركة مصدر التكنولوجيا

الرقم التسلسلي	الإصدار	وصف التغييرات	المسؤول
		• تصحيح الأخطاء المطبعية	
1.2	16/09/2025	"يتم حذف القيمة الخاصة بـ (تعريف هوية العميل - id-kp-clientAuth) من حقل ملحق استخدام المفتاح الممتد (EKU)؛ وذلك لضمان الامتثال لسياسة برنامج كروم للجذور (Chrome Root Program Policy)، الإصدار 1.6."	شركة مصدر التكنولوجيا.
1.3	03/06/2026	• إضافة النصوص الخاصة بالجاهزية للإلغاء الجماعي (Mass Revocation) إلى القسم 5.7.1. • فرض التحقق من صحة امتدادات أمن نظام أسماء النطاقات (DNSSEC)في استجابات الـ (DNS) قبل معالجة سجلات "تصريح جهة إصدار الشهادةCAA) ") وفقاً للقسمين 3.2.2.4 و 4.2.2.1. • تقليص فترة صلاحية شهادات طبقة المقابس الآمنة (TLS) بناءً على القرار الملحق Ballot SC081v3. • تعديل مصطلح "الشروط و الأحكام" ليصبح "شروط وأحكام استخدام المشترك". • تعديل آلية التحقق لاستبدال "التحقق القائم على الشهادة التوكيدية " (Attestation-based validation)بـ "التأكيد المباشر (Section 3.2.5)".	شركة مصدر التكنولوجيا

الموافقة على الوثيقة

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

الفهرس

1 المقدمة 16
1.1 نظرة عامة 16
1.1.1 لجنة البنية التحتية للمفاتيح العامة لدى مصدر التكنولوجيا (TS PKI GB) 18
1.2 اسم الوثيقة ومعرفها 18
1.3 المشاركون في البنية التحتية للمفاتيح العامة (PKI) 19
1.3.1 هيئات التصديق (CAs) 19
1.3.2 هيئات التسجيل (RA) 19
1.3.3 المشتركين 20
1.3.4 الأطراف المعتمدة 20
1.3.5 المشاركون الآخرون 20
1.4 استخدام الشهادات 20
1.4.1 استخدامات الشهادات المسموح بها 20
1.4.2 الاستخدامات المحظورة للشهادات 21
1.5 إدارة السياسة 21
1.5.1 الجهة المسؤولة عن إدارة الوثيقة 21
1.5.2 جهة الاتصال 21
1.5.3 الشخص المسؤول عن تحديد ملاءمة CPS للسياسة 22
1.5.4 إجراءات اعتماد CPS 22
1.6 التعاريف والاختصارات 22
1.6.1 التعاريف 22
1.6.2 الاختصارات 30
1.6.3 المراجع 33
2 المسؤوليات المتعلقة بالنشر والمستودعات 34

2.1 المستودعات 34
2.2 نشر معلومات الشهادات 34
2.3 توقيت أو تكرار النشر 35
2.3.1 شهادات هيئة التصديق 35
2.3.2 قوائم إلغاء الشهادات(CRLs) 35
2.4 ضوابط الوصول إلى المستودعات 35
3 التعريف والمصادقة 36
3.1 التسمية 36
3.1.1 أنواع الأسماء 36
3.1.2 الحاجة إلى أن تكون الأسماء ذات معنى 37
3.1.3 عدم السماح بإخفاء الهوية أو استخدام الأسماء المستعارة للمشتركين 37
3.1.4 قواعد تفسير أشكال الأسماء المختلفة 37
3.1.5 تفرّد الأسماء 37
3.1.6 التعرف على العلامات التجارية والتحقق منها ودورها 37
3.2 التحقق الأولي من هوية المشترك 38
3.2.1 طريقة إثبات حيازة المفتاح الخاص 38
3.2.2 التحقق من هوية المنظمة وهوية النطاق 38
3.2.3 التحقق من هوية الأشخاص الطبيعيين 44
3.2.4 معلومات المشترك غير المُتحقّق منها 44
3.2.5 التحقق من السلطة 44
3.2.6 معايير التشغيل البيني 45
3.3 التحقق من الهوية والمصادقة لطلبات إعادة إصدار المفتاح(Re-key) 45

3.3.1 التحقق من الهوية والمصادقة لإعادة الإصدار الروتيني 45
3.3.2 التحقق من الهوية والمصادقة بعد إلغاء الشهادة Re-key بعد الإلغاء 45
3.4 التحقق من الهوية والمصادقة لطلب الإلغاء 46
4 متطلبات تشغيل دورة حياة الشهادة 47
4.1 طلب الشهادة 47
4.1.1 من يمكنه تقديم طلب شهادة 47
4.1.2 عملية التسجيل والمسؤوليات 47
4.2 معالجة طلب الشهادة 48
4.2.1 تنفيذ وظائف التحقق من الهوية والمصادقة 48
4.2.2 الموافقة أو رفض طلبات الشهادات 50
4.2.3 مدة معالجة طلبات الشهادات 51
4.3 إصدار الشهادة 51
4.3.1 إجراءات هيئة التصديق أثناء إصدار الشهادة 51
4.3.2 إشعار المشترك بإصدار الشهادة من قبل هيئة التصديق 52
4.4 قبول الشهادة 52
4.5 السلوك الذي يُعد قبولاً للشهادة 52
4.6 تجديد الشهادة 52
4.6.1 الظروف التي تستدعي تجديد الشهادة 52
4.6.2 من يمكنه طلب التجديد 52
4.6.3 معالجة طلبات تجديد الشهادة 52
4.6.4 إشعار المشترك بإصدار شهادة جديدة 53
4.6.5 التصرف الذي يُعد قبولاً لشهادة جددت 53
4.6.6 نشر شهادة التجديد من قبل هيئة التصديق 53

4.6.7 إشعار هيئة التصديق بعملية الإصدار لجهات أخرى 53
4.7 إعادة إصدار الشهادة(Re-key) 53
4.7.1 الظروف التي تستدعي إعادة إصدار الشهادة 53
4.7.2 من يمكنه طلب اعتماد مفتاح عام جديد 53
4.7.3 معالجة طلبات إعادة إصدار الشهادة 53
4.7.4 إشعار المشترك بإصدار شهادة جديدة 53
4.7.5 التصرف الذي يُعد قبولاً لشهادة أعيد إصدارها 53
4.7.6 نشر الشهادة المعاد إصدارها من قبل هيئة التصديق 53
4.7.7 إشعار هيئة التصديق بعملية الإصدار لجهات أخرى 53
4.8 تعديل الشهادة 54
4.8.1 الظروف التي تستدعي تعديل الشهادة 54
4.8.2 من يمكنه طلب تعديل الشهادة 54
4.8.3 معالجة طلبات تعديل الشهادة 54
4.8.4 إشعار المشترك بإصدار شهادة جديدة 54
4.8.5 التصرف الذي يُعد قبولاً لشهادة معدلة 54
4.8.6 نشر الشهادة المعدلة من قبل هيئة التصديق 54
4.8.7 إشعار هيئة التصديق بعملية الإصدار لجهات أخرى 54
4.9 إبطال وتعليق الشهادة 54
4.9.1 الظروف التي تستدعي الإبطال 54
4.9.2 من يمكنه طلب الإبطال 56
4.9.3 إجراءات طلب الإبطال 56
4.9.4 فترة السماح لطلب الإبطال 57

4.9.5 الإطار الزمني الذي يجب على هيئة التصديق خلاله معالجة طلب الإبطال 58
4.9.6 متطلبات التحقق من الإبطال على الأطراف المعتمدة 58
4.9.7 وتيرة إصدار قوائم الإبطال (CRL) (إن وُجدت 58
4.9.8 الحد الأقصى للتأخير في إصدار قوائم الإبطال (إن وُجد) 58
4.9.9 حدود المسؤولية 58
4.9.10 التعويضات 59
4.9.11 المدة والإنهاء 59
4.9.12 وسائل أخرى للإعلان عن الإبطال 60
4.9.13 المتطلبات الخاصة المتعلقة باختراق المفتاح 60
4.9.14 الظروف التي تستدعي التعليق 60
4.9.15 من يمكنه طلب التعليق 60
4.9.16 إجراءات طلب التعليق 60
4.9.17 حدود فترة التعليق 61
4.10 خدمات حالة الشهادات 61
4.10.1 الخصائص التشغيلية 61
4.10.2 توفر الخدمة 61
4.10.3 الخصائص الاختيارية 61
4.11 انتهاء الاشتراك 61
4.12 إيداع المفاتيح واستعادتها 61
4.12.1 سياسة وممارسات إيداع واستعادة المفاتيح 61
4.12.2 سياسة وممارسات تغليف واستعادة مفتاح الجلسة 61
5 الضوابط المتعلقة بالمرافق والإدارة والتشغيل 62

5.1	الضوابط الأمنية الفيزيائية	62
5.1.1	موقع المنشأة وتصميمها	63
5.1.2	الوصول الفيزيائي	63
5.1.3	الطاقة والتكييف	63
5.1.4	التعرض للمياه	63
5.1.5	الوقاية من الحريق والحماية منه	63
5.1.6	تخزين الوسائط	64
5.1.7	التخلص من النفايات	64
5.1.8	النسخ الاحتياطي خارج الموقع	64
5.2	الضوابط الإجرائية	64
5.2.1	الأدوار الموثوقة	64
5.2.2	عدد الأشخاص المطلوبين لكل مهمة	65
5.2.3	تحديد الهوية والمصادقة لكل دور	65
5.2.4	الأدوار التي تتطلب فصل المهام	66
5.3	الضوابط الخاصة بالموظفين	66
5.3.1	المؤهلات والخبرة ومتطلبات التخليص الأمني	66
5.3.2	إجراءات فحص الخلفية	66
5.3.3	متطلبات التدريب	66
5.3.4	تكرار ومتطلبات التدريب المتجدد	67
5.3.5	تكرار وتتابع تدوير الوظائف	67
5.3.6	العقوبات على الأفعال غير المصرّح بها	67
5.3.7	متطلبات المتعاقدين المستقلين	67
5.3.8	الوثائق المقدمة للموظفين	67
5.4	إجراءات تسجيل السجلات التدقيقية	68
5.4.1	أنواع الأحداث المسجلة	68

5.4.2 تكرار معالجة السجلات 70
5.4.3 فترة الاحتفاظ بسجلات التدقيق 70
5.4.4 حماية سجلات التدقيق 70
5.4.5 إجراءات النسخ الاحتياطي لسجلات التدقيق 71
5.4.6 نظام جمع السجلات (داخلي مقابل خارجي) 71
5.4.7 إشعار الجهة المتسببة بالحدث 71
5.4.8 تقييم الثغرات الأمنية 71
5.5 أرشفة السجلات 72
5.5.1 أنواع السجلات المؤرشفة 72
5.5.2 فترة الاحتفاظ بالأرشيف 72
5.5.3 حماية الأرشيف 72
5.5.4 إجراءات النسخ الاحتياطي للأرشيف 72
5.5.5 متطلبات الطابع الزمني للسجلات 72
5.5.6 نظام جمع الأرشيف (داخلي أو خارجي) 73
5.5.7 إجراءات الحصول على معلومات الأرشيف والتحقق منها 73
5.6 تبديل المفاتيح 73
5.7 التعافي من الكوارث والاختراق (Compromise and Disaster Recovery) 73
5.7.1 إجراءات التعامل مع الحوادث والاختراق 73
5.7.2 إجراءات الاستعادة في حال تلف الموارد الحاسوبية أو البرمجيات أو البيانات 74
5.7.3 إجراءات الاستعادة بعد اختراق المفتاح 74
5.7.4 قدرات استمرارية الأعمال بعد وقوع كارثة 74
5.8 إنهاء عمل هيئة التصديق أو هيئة التسجيل 76
6 الضوابط الأمنية التقنية 78

6.1 توليد وتثبيت أزواج المفاتيح 78
6.1.1 توليد أزواج المفاتيح 78
6.1.2 تسليم المفتاح الخاص إلى المشترك 79
6.1.3 تسليم المفتاح العام إلى جهة إصدار الشهادات 79
6.1.4 تسليم المفتاح العام لهيئة التصديق إلى الأطراف المعتمدة 79
6.1.5 نوع الخوارزمية وأحجام المفاتيح 79
6.1.6 إنشاء معلمات المفاتيح العامة والتحقق من جودتها 79
6.1.7 أغراض استخدام المفتاح وفقاً لحقل استخدام المفتاح في X.509 v3 79
6.2 حماية المفتاح الخاص ووحدة التشفير والضوابط الهندسية 80
6.2.1 معايير وضوابط وحدة التشفير 80
6.2.2 التحكم المتعدد بالأشخاص في المفتاح الخاص n من m 80
6.2.3 إيداع المفتاح الخاص 80
6.2.4 النسخ الاحتياطي للمفتاح الخاص 80
6.2.5 أرشفة المفتاح الخاص 81
6.2.6 نقل المفتاح الخاص إلى وحدة التشفير أو منها 81
6.2.7 تخزين المفتاح الخاص في وحدة التشفير 81
6.2.8 طريقة تفعيل المفتاح الخاص 81
6.2.9 طريقة إلغاء تفعيل المفتاح الخاص 81
6.2.10 طريقة إتلاف المفتاح الخاص 81
6.2.11 تصنيف وحدة التشفير 82
6.3 جوانب أخرى لإدارة أزواج المفاتيح 82
6.3.1 أرشفة المفتاح العام 82

6.3.2 فترة تشغيل الشهادة وفترة استخدام زوج المفاتيح 82
6.4 بيانات التفعيل 82
6.4.1 إنشاء بيانات التفعيل وتثبيتها 82
6.4.2 حماية بيانات التفعيل 83
6.4.3 جوانب أخرى متعلقة ببيانات التفعيل 83
6.5 ضوابط أمن الحاسوب 83
6.5.1 المتطلبات التقنية الخاصة بأمن الحاسوب 83
6.5.2 تصنيف أمن الحاسوب 83
6.6 ضوابط الدورة الحياتية التقنية 84
6.6.1 ضوابط تطوير الأنظمة 84
6.6.2 ضوابط إدارة الأمن 84
6.6.3 ضوابط الأمان لدورة الحياة 84
6.7 ضوابط أمن الشبكة 84
6.8 خدمة ختم الوقت 85
7 ملفات الشهادات قوائم الإلغاء(CRL) ومستجيب حالة الشهادة عبر الإنترنت (OCSP) 86
7.1 ملف تعريف الشهادة 86
7.1.1 رقم الإصدار 86
7.1.2 امتدادات الشهادة 86
7.1.3 معرفات كائنات الخوارزميات 86
7.1.4 صيغ الأسماء 86
7.1.5 قيود الأسماء 87
7.1.6 معرّف كائن سياسة الشهادة 87
7.1.7 استخدام امتداد قيود السياسة 87
7.1.8 صياغة ودلالة مؤهِّل السياسة 87

7.1.9 دلالة المعالجة لامتداد سياسات الشهادات عند تمييزه كحرِج 88
7.1.10 ملف تعريف شهادة TS TLS CA 88
7.1.11 ملف تعريف شهادات التحقق من المؤسسة(OV) 92
7.2 ملف تعريف قائمة إلغاء الشهادات(CRL) 96
7.2.1 رقم الإصدار 98
7.2.2 امتدادات CRL وسجلات CRL 98
7.3 ملف تعريفOCSP 99
7.3.1 رقم النسخة 103
7.3.2 امتداداتOCSP 103
8 التدقيق على الامتثال والتقييمات الأخرى 104
8.1 تواتر أو ظروف التقييم 104
8.2 هوية/مؤهلات المقيم 104
8.3 علاقة المقيم بالجهة المقيمة 104
8.4 المواضيع التي يغطيها التقييم 104
8.5 الإجراءات المتخذة نتيجة وجود خلل 105
8.6 إيصال نتائج التدقيق 105
8.7 التدقيقات الذاتية 105
9 مسائل تجارية وقانونية أخرى 106
9.1 الرسوم 106
9.1.1 رسوم إصدار أو تجديد الشهادات 106
9.1.2 رسوم الوصول إلى الشهادات 106
9.1.3 رسوم الوصول إلى معلومات الإلغاء أو حالة الشهادة 106
9.1.4 رسوم الخدمات الأخرى 106

9.1.5 سياسة الاسترداد 106
9.2 المسؤولية المالية 106
9.2.1 التغطية التأمينية 106
9.2.2 الأصول الأخرى 106
9.2.3 التغطية التأمينية أو الضمانات للجهات النهائية 106
9.3 سرية المعلومات التجارية 106
9.3.1 نطاق المعلومات السرية 106
9.3.2 المعلومات الخارجة عن نطاق المعلومات السرية 107
9.3.3 المسؤولية عن حماية المعلومات السرية 107
9.4 خصوصية المعلومات الشخصية 107
9.4.1 خطة الخصوصية 107
9.4.2 المعلومات التي تُعامل كمعلومات خاصة 108
9.4.3 المعلومات التي لا تُعتبر خاصة 108
9.4.4 المسؤولية عن حماية المعلومات الخاصة’ 108
9.4.5 الإشعار والموافقة على استخدام المعلومات الخاصة 108
9.4.6 الإفصاح بموجب إجراء قضائي أو إداري 108
9.4.7 ظروف أخرى للإفصاح عن المعلومات 108
9.5 حقوق الملكية الفكرية 108
9.6 الإقرارات والضمانات 108
9.6.1 إقرارات وضمانات هيئة التصديق 108
9.6.2 إقرارات وضمانات هيئة التسجيل(RA) 110
9.6.3 إقرارات وضمانات المشترك 110
9.6.4 إقرارات وضمانات الأطراف المعتمدة 111
9.6.5 إقرارات وضمانات المشاركين الآخرين 111

9.7 إخلاء المسؤولية عن الضمانات 111
9.8 حدود المسؤولية 111
9.9 التعويضات 112
9.10 المدة والإنهاء 112
9.10.1 المدة 112
9.10.2 الإنهاء 112
9.10.3 أثر الإنهاء والنفاذ 112
9.11 الإشعارات والتواصل مع الأطراف الفردية 112
9.12 التعديلات 112
9.12.1 إجراءات التعديل 113
9.12.2 آلية الإشعار والفترة الزمنية 113
9.12.3 الظروف التي تستوجب تغيير OID 113
9.13 أحكام تسوية النزاعات 113
9.14 القانون الحاكم 113
9.15 الامتثال للقوانين النافذة 113
9.16 أحكام متنوعة 113
9.16.1 الاتفاق الكامل 113
9.16.2 التنازل 113
9.16.3 القابلية للفصل 114
9.16.4 التنفيذ (أتعاب المحامين والتنازل عن الحقوق) 114
9.16.5 القوة القاهرة 114
9.17 أحكام أخرى 114

1 المقدمة

تُعد هذه الوثيقة بيان ممارسة الشهادات (CPS) الذي يصف ممارسات التصديق المعتمدة لدى هيئة التصديق TLS التابعة لشركة مصدر التكنولوجيا (ويُشار إليها لاحقاً بـ TS). يتوافق هذا البيان مع سياسة الشهادات الخاصة بمزود خدمات الثقة (TSP) والتي تنطبق على تقديم خدمات التصديق من قبل مزودي خدمات الثقة الذين يُصدرون شهادات موثوقة علنياً للجهات النهائية تحت الهيكل الوطني لهيئات التصديق الجذرية في جمهورية العراق.

يتناول هذا البيان السياسات الفنية والإجرائية والتنظيمية الخاصة بهيئة التصديق TS TLS التي أنشأتها وتديرها شركة مصدر التكنولوجيا ضمن التسلسل الهرمي للبنية التحتية الوطنية للمفاتيح العامة في العراق فيما يتعلق بكامل دورة حياة الشهادات التي تُصدرها هذه الهيئة.

يشمل هذا البيان إصدار وضوابط الشهادات التالية التي تُصدرها هذه الهيئة:

- شهادات TLS لخوادم الويب التحقق التنظيمي – (OV) تُستخدم للمصادقة على الخادم وتشفير بيانات الجلسة.
- شهادة مستجيب – OCSP تُستخدم لتوقيع ردود بروتوكول حالة الشهادة عبر الإنترنت (OCSP) الخاصة بالشهادات المُصدرة من قبل هيئة التصديقTLS TS .

يتوافق هذا البيان مع المتطلبات الرسمية لفريق مهام هندسة الإنترنت (IETF) المحددة في RFC 3647 فيما يتعلق بالتنسيق والمحتوى. ورغم إدراج بعض عناوين الأقسام وفقاً لبنيةRFC 3647 قد لا تنطبق بعض المواضيع فعلياً على تنفيذ هذه الهيئة. تُشار مثل هذه الأقسام بعبارة غير قابل للتطبيق وتُدرج معلومات إضافية في الفروع الفرعية للبنية القياسية حسب الحاجة.

تلتزم لجنة البنية التحتية للمفاتيح العامة لدى TS بالحفاظ على هذا البيان بما يتوافق مع الإصدارات الحالية للمتطلبات التالية والمنشورة على الموقعhttp://www.cabforum.org :.

- المتطلبات الأساسية لمنتدى CA/Browser لإصدار وإدارة شهادات خوادم TLS الموثوقة علنياً.
- متطلبات أمن الشبكات وأنظمة الشهادات لمنتدىCA/Browser .

في حال وجود أي تعارض بين هذا المستند والمتطلبات أعلاه تكون الأولوية للمتطلبات المذكورة أعلاه.

يُعد هذا البيان وثيقة علنية وعند الإشارة إلى معلومات سرية ضمن النص فإن ذلك يُشير إلى وثائق مصنفة متاحة فقط للأشخاص المخولين.

يمكن الحصول على معلومات إضافية بخصوص هذا البيان من خلال التواصل مع لجنة البنية التحتية للمفاتيح العامة لدىTS باستخدام معلومات الاتصال المدرجة في القسم 1.5. .

1.1 نظرة عامة

أُنشئت البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI) تحت إشراف **الشركة العامة للاتصالات والمعلوماتية (ITPC)** وتضم عدداً من هيئات التصديق الجذرية التي تمثل البرنامج الوطني لهيئات التصديق الجذرية. تهدف الحكومة العراقية من خلال هذه البنية إلى توفير إطار عمل يسهّل إنشاء مزودي خدمات الثقة (TSP) الذين يقدمون خدمات التصديق الرقمي والخدمات الموثوقة للجهات الحكومية وغير الحكومية.

يتألف التسلسل الهرمي للبنية التحتية للمفاتيح العامة في العراق من مستويين كما يلي:

المستوى 0:

في هذا المستوى أُنشئت خمس (5) هيئات تصديق جذرية لإصدار أنواع مختلفة من الشهادات من قبل هيئات التصديق التابعة. تتولى الشركة العامة للاتصالات والمعلوماتية (ITPC) المسؤولية عن هذا المستوى الجذري وتُكلف بصفتها الجهة الوطنية للبنية التحتية للمفاتيح العامة بتشغيل اللجنة العليا لإدارة التوقيع الإلكتروني .(PMA) وتشمل هيئات التصديق الجذرية التابعة لـ ITPC ما يلي:

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

المستوى 1:

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

الشكل 1: التسلسل الهرمي للبنية التحتية الوطنية للمفاتيح العامة في العراق.

تُعد شركة مصدر التكنولوجيا الجهة المسؤولة عن تشغيل هيئات التصديق التابعة وتقديم خدمات الثقة المرتبطة بها إلى المجالات الحكومية وغير الحكومية في العراق. وبذلك تعمل شركة مصدر التكنولوجيا كمزود لخدمات الثقة (TSP) حيث تقدم خدماتها من خلال تسلسل هرمي من هيئات التصديق التابعة تنفيذ تحت هيئات التصديق الجذرية التابعة للشركة العامة للاتصالات والمعلوماتية .(ITPC) وقد صدّقت هيئات التصديق الجذرية التابعة لـ ITPC على هيئات التصديق التابعة الخاصة بمزود خدمات الثقة لشركة مصدر التكنولوجيا كما يلي:

- هيئة التصديق لتوقيع البرمجيات التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات لتوقيع مكتبات البرمجيات وملفات jar. و exe.و msi.وغيرها.
- هيئة التصديق للبريد الإلكتروني الآمن (S/MIME) التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات لتوقيع البريد الإلكتروني وتشفيره.

- هيئة التصديق لـ TLS التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات تحقق تنظيمي (OV) لخوادم الويب.
- هيئة التصديق لتوقيع المستندات للأشخاص الطبيعيين (NP) التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات توقيع المستندات للمواطنين والموظفين.
- هيئة التصديق لتوقيع المستندات للأشخاص الاعتباريين (LP) التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات توقيع المستندات للجهات الحكومية وغير الحكومية العراقية.
- هيئة التصديق لختم الوقت التابعة لشركة مصدر التكنولوجيا: هيئة تصديق فرعية تُصدر شهادات هيئة ختم الوقت (TSA) المستخدمة في توقيع المستندات والبرمجيات.

تُعد حالات الاستخدام أعلاه عوامل أساسية لتمكين التحول الرقمي إذ تشكل حجر الأساس في تأمين المعاملات الإلكترونية. إن دعم هذه الحالات ضمن نموذج موحد للثقة بضمان حكومي يُسهل التبني ويُمكّن التشغيل البيني ويُعزز ثقة المستخدم.

تتفاعل لجنة البنية التحتية للمفاتيح العامة لدى مصدر التكنولوجيا (TS PKI GB) بشكل وثيق مع اللجنة العليا لإدارة التوقيع الإلكتروني (ITPC PMA) التابعة لـ ITPC للحفاظ على التوافق مع هذا البيان فيما يتعلق بتصديق وتشغيل هيئات التصديق التابعة لـTS .

1.1.1 لجنة البنية التحتية للمفاتيح العامة لدى مصدر التكنولوجيا(TS PKI GB)

تُعرف الجهة المشرفة على البنية التحتية للمفاتيح العامة التابعة لشركة مصدر التكنولوجيا (بما في ذلك هيئة التصديق TS (TLSباسم لجنة PKIلمصدر التكنولوجيا .(TS PKI GB) تضم هذه اللجنة الوظائف الأساسية اللازمة مثل السياسة والأمن والامتثال والشؤون القانونية والتي تُعد ضرورية لتقديم التوجيه الاستراتيجي والإشراف المستمر على عمليات PKI الخاصة بشركة مصدر التكنولوجيا.

وتتحمل اللجنة المسؤوليات التالية بشكل خاص:

- تحديد استراتيجية TS PKI والحفاظ عليها.
- تحديد خدمات TS PKI والموافقة على نموذج تقديمها.
- تحديد وصيانة السياسات والممارسات الخاصة بـ.TS PKI .
- إجراء أنشطة إشراف منتظمة على فريق عمليات.TS PKI .
- الموافقة على ميزانية PKI واتخاذ القرارات التجارية الرئيسية.
- الموافقة على التغييرات الرئيسية في بنية PKI التحتية.
- الموافقة على مراسيم المفاتيح وتعيين المدققين الداخليين/الخارجيين حسب الحاجة.
- المشاركة في الحوادث الرئيسية واتخاذ القرارات اللازمة بشأنها.
- قيادة تسوية النزاعات الناشئة عن أو المرتبطة بأنشطة.TS PKI .
- تقييم الحوادث التي لم يلتزم فيها الموظفون الرئيسيون في TS PKI بالإجراءات الأمنية أو التشغيلية بما في ذلك الأمور الأخلاقية.

1.2 اسم الوثيقة ومعرفها

تحمل هذه الوثيقة عنوان بيان ممارسة الشهادات لهيئة تصديق TLS التابعة لمصدر التكنولوجيا ويُعرف هذا البيان برقم المعرف الكائني2.16.368.1.2.1.3 :(OID) ويُشار إليه في الوثائق ذات الصلة بالرمز[TS TLS CA CPS] .

تتضمن هيئة التصديق TS TLS CA رقم المعرف الكائني أعلاه في امتداد سياسة الشهادة (CP extension) للشهادات التي تُصدرها للإشارة إلى التوافق مع البيان الحالي.

1.3 المشاركون في البنية التحتية للمفاتيح العامة(PKI)

1.3.1 هيئات التصديق (CAs)

تُدار وتُشغل هيئة التصديق TS TLS CA (ويُشار إليها لاحقاً بـ CA من قبل شركة مصدر التكنولوجيا من مقرها في العراق. وقد جرت الموافقة على هذه الهيئة من قبل الشركة العامة للاتصالات والمعلوماتية(ITPC) ووقّعت شهادتها الهيئة الجذرية العراقية لTLS كما هو موضح في الشكل 1 (القسم 1.1).

تقدم هذه الهيئة الخدمات التالية في مجال التصديق:

- خدمة إنشاء الشهادات :إصدار شهادات للجهات النهائية استناداً إلى التحقق الذي تُجريه هيئات التسجيل (Ras).
- خدمة النشر :نشر شهادات OCSP وCRL وشهادات CA وإتاحتها للأطراف المعتمدة. كما تشمل هذه الخدمة توفير المعلومات العلنية المتعلقة بالسياسات والممارسات للمشتركين والأطراف المعتمدة.
- خدمة إدارة الإلغاء :معالجة طلبات الإلغاء والتقارير المتعلقة به لتحديد الإجراءات المناسبة التي يجب اتخاذها. وتُعرض نتائج هذه الخدمة من خلال خدمة حالة صلاحية الشهادات.
- خدمة حالة صلاحية الشهادة :تقديم معلومات حول حالة صلاحية الشهادات للأطراف المعتمدة استناداً إلى قوائم إلغاء الشهادات وخدمة مستجيب .OCSP وتعكس المعلومات المنشورة الحالة الحالية دائماً للشهادات الصادرة من قبل هذه الهيئة.

1.3.2 هيئات التسجيل(RA)

تُعد هيئة التسجيل (RA) الكيان المسؤول عن التحقق من هوية المتقدمين بطلبات الشهادات للمستخدمين النهائيين والمصادقة عليهم بالإضافة إلى الشروع في أو تمرير طلبات إلغاء الشهادات والموافقة على طلبات إصدار الشهادات وتجديدها نيابةً عن هيئة التصديق(CA) .

تُشغل شركة مصدر التكنولوجيا وظيفة هيئة التسجيل (RA) الخاصة بها داخلياً ولا تعتمد على أطراف خارجية مفوضة لأداء وظائف .RA وتُعالج هذه الهيئة بشكل أساسي طلبات شهادات TLS الصادرة للمنظمات القانونية.

تندرج وظيفة RA ضمن هيكل عمليات البنية التحتية للمفاتيح العامة .(PKI Operations) ويتحمل مسؤولو RA لدى مصدر التكنولوجيا مسؤولية التحقق من الهوية وإدارة طلبات الشهادات للجهات الحكومية وغير الحكومية وفقاً للإجراءات المبيّنة في القسم 4.2.

تشمل مهام هيئة التسجيل لدى مصدر التكنولوجيا دون حصر ما يلي:

- التحقق من طلبات الشهادات والموافقة عليها أو رفضها بما في ذلك طلبات الإلغاء.
- التحقق من هوية المشتركين وفقاً لاتفاقيات التسمية المعرّفة في هذا البيان لضمان تعريف كل مشترك بشكل فريد وواضح.

- معالجة طلبات إصدار وإلغاء الشهادات بالتعاون مع هيئة التصديق بناءً على الطلبات التي حقق منها والموافقة عليها.
- إنشاء سجل تدقيق يحتفظ بجميع الأحداث المهمة المتعلقة بعمليات هيئة التسجيل.
- توفير إمكانية وصول انتقائية إلى سجلات سجل التدقيق وفقاً لما هو محدد في هذا البيان.
- تنفيذ الضوابط التشغيلية الأخرى كما هو مذكور في هذا البيان.
- معالجة وتخزين المعلومات وفقاً للمتطلبات المحددة في هذا البيان لا سيما في القسم 5.

لا تفوض شركة مصدر التكنولوجيا عملية التحقق من ملكية أو سيطرة النطاق إلى أي هيئة تسجيل تابعة لطرف ثالث. إذ يتم تنفيذ هذه العملية فقط من قبل فريق مسؤولي هيئة التسجيل لدى مصدر التكنولوجيا.

1.3.3 المشتركين

المشتركون هم الممثلون القانونيون للكيانات القانونية بما في ذلك الجهات الحكومية وغير الحكومية بالإضافة إلى شركة مصدر التكنولوجيا نفسها تحت الولاية القضائية العراقية ممن يمتلكون تفويضاً قانونياً كافياً.

ويقدمون كذلك طلباً للحصول على شهادات (OV) الموثقة للمؤسسات من جهة إصدار شهادات (TS TLS CA)، مع التعهد بالالتزام بشروط وأحكام استخدام المشتركين المعمول بها.

1.3.4 الأطراف المعتمدة

يتعين على الأطراف المعتمدة الرجوع باستمرار إلى خدمة التحقق من صلاحية الشهادات الصادرة عن شركة مصدر التكنولوجيا أي: قوائم إلغاء الشهادات CRL وخدمةOCSP قبل الاعتماد على المعلومات الواردة في الشهادة المعنية.

1.3.5 المشاركون الآخرون

تشمل الجهات الأخرى المشاركة ما يلي:

- اللجنة العليا لإدارة التوقيع الإلكتروني لدى الشركة العامة للاتصالات والمعلوماتيةITPC PMA)) وهي الجهة المشرفة المسؤولة عن الإشراف على النشاط الكامل لمزود خدمات الثقة المرخص (أي شركة مصدر التكنولوجيا). وترد أدوار ومسؤوليات اللجنة العليا لإدارة التوقيع الإلكتروني في وثيقة CP/CPS الجذرية الخاصة بـ ITPC والمنشورة على الرابط https://pki.itpc.gov.iq :
- مدقق WebTrust مستقل ومؤهل يتحقق من المتطلبات الواردة في القسم 8.2.

1.4 استخدام الشهادات

1.4.1 استخدامات الشهادات المسموح بها

يجوز استخدام الشهادات الصادرة بموجب هذا البيان للأغراض التالية:

1. شهادات TLS لخوادم الويب:
   - شهادات التحقق التنظيمي :(OV) تُستخدم للمصادقة على الخوادم وتشفير بيانات الجلسات.
2. شهادة مستجيب :OCSP تُستخدم للتوقيع والتحقق من ردود بروتوكول حالة الشهادة عبر الإنترنت (OCSP) للشهادات الصادرة عن هذه الهيئة.

1.4.2 الاستخدامات المحظورة للشهادات

يُصرّح للمشتركين باستخدام الشهادات فقط للأغراض المحددة في القسم 1.4.1 من هذا البيان. ويُحظر منعاً باتاً استخدام الشهادات لأي أغراض أخرى.

1.5 إدارة السياسة

1.5.1 الجهة المسؤولة عن إدارة الوثيقة

تُدار هذه الوثيقة الخاصة ببيان ممارسة الشهادات من قبل لجنة PKIلشركة مصدر التكنولوجيا(TS PKI GB) وفقاً لنموذج التشغيل الخاص بها وبناءً على التفاعل مع اللجنة العليا لإدارة التوقيع الإلكتروني ITPC PMA عند الحاجة.

1.5.2 جهة الاتصال

يُوجه أي طلب للحصول على معلومات بخصوص هذا البيان إلى العنوان التالي:

لجنة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا
شركة مصدر التكنولوجيا
العنوان: بغداد – الاربع شوارع – بالقرب من إعدادية المأمون

البريد الإلكتروني: info@techsource.iq

رقم الهاتف: 1693 136 784 (964+)

تقبل لجنة البنية التحتية للمفاتيح العامة لدى مصدر التكنولوجيا (TS PKI GB) التعليقات بشأن هذا البيان فقط إذا ارسلت إلى جهة الاتصال المذكورة أعلاه.

تقرير مشكلة شهادة

يجوز للمشتركين والأطراف المعتمدة وموردي برمجيات التطبيقات والأطراف الثالثة الأخرى الإبلاغ عن حالات يُشتبه فيها بحدوث اختراق للمفتاح الخاص أو إساءة استخدام الشهادة أو أي نوع آخر من الاحتيال أو الاختراق أو السلوك غير الملائم أو أي مسألة أخرى تتعلق بالشهادات عبر إرسال بريد إلكتروني إلى:

certificate.problem@techsource.iq.

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

إذا رأت شركة مصدر التكنولوجيا أن ذلك مناسب فقد تقوم بتحويل تقارير الإلغاء إلى الجهات المختصة بإنفاذ القانون. وتحتفظ الشركة بقدرة داخلية دائمة على مدار الساعة (7/24) للاستجابة لأي طلبات إلغاء عاجلة وتقارير مشاكل الشهادات. وتوفر الشركة تعليمات للإبلاغ عن مشاكل الشهادات وطلبات الإلغاء من خلال صفحة مخصصة ضمن المستودع العام والمتاحة على الرابط:

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

1.5.3 الشخص المسؤول عن تحديد ملاءمة CPS للسياسة

استناداً إلى نتائج وتوصيات عمليات تدقيق الامتثال تُحدد لجنة TS PKI GB وقابلية تطبيق هذا البيان. ويتم اعتماد هذا البيان من قبل لجنة TS PKI GB واللجنة العليا لإدارة التوقيع الإلكتروني(PMA)) نظراً لأن البيان يجب أن يتوافق في نهاية المطاف مع أحكام سياسة شهادات مزود خدمات الثقةTSP CP)).

1.5.4 إجراءات اعتمادCPS

تقوم لجنةTS PKI GB بالتعاون مع اللجنة العليا لإدارة التوقيع الإلكتروني (PMA) بالموافقة الرسمية على أي إصدار جديد من هذا البيان.

يُراجع هذا البيان موظفون مختصون في سياسات PKI من لجنةTS PKI GB وذلك لكل من المسودة الأولية وأي تعديلات لاحقة لضمان توافقه مع أفضل الممارسات المطبقة ومع سياسة شهاداتTSP وذلك قبل اعتماده من قبل اللجنة.

يمكن أن تأخذ التعديلات شكل وثيقة تحتوي على نسخة معدّلة من البيان أو إشعار تحديث. تسجل التغييرات التي تُجرى على هذا البيان ضمن جدول المراجعات.

يُقدَّم الإصدار الجديد من البيان بعد ذلك إلى اللجنة العليا لإدارة التوقيع الإلكتروني (PMA) للموافقة النهائية نظراً لضرورة توافقه مع أحكام سياسة شهادات مزود خدمات الثقةTSP CP)).

قبل دخوله حيز التطبيق يتم الإعلان عن الإصدار المُحدث من البيان في المستودع العام والمتاح عبر الرابط:

https://pki.techsource.iq.

وبمجرد نشره يصبح الإصدار الجديد ملزماً لجميع المشتركين بما في ذلك المشتركين والأطراف المعتمدة على شهادات صادرة بموجب إصدار سابق من هذا البيان.

1.6 التعاريف والاختصارات

1.6.1 التعاريف

الشركة التابعة: شركة أو شراكة أو مشروع مشترك أو كيان آخر يسيطرعلى كيان آخر أو يخضع لسيطرته أو يخضع مع كيان آخر لسيطرة مشتركة أو وكالة أو إدارة أو تقسيم سياسي أو أي كيان يعمل تحت السيطرة المباشرة لكيان حكومي.

المتقدم: الشخص الطبيعي أو الكيان القانوني الذي يتقدم بطلب للحصول على شهادة (أو يسعى إلى تجديدها). بعد إصدار الشهادة يُشار إلى المتقدم باسم المشترك . وفي سياق هذا البيان تُصدر هيئة التصديق شهادات فقط للكيانات القانونية.

ممثل المتقدم: شخص طبيعي أو راعٍ بشري يكون إما هو المتقدم ذاته أو موظفاً لدى المتقدم أو وكيلاً مفوضاً لديه تفويض صريح لتمثيل المتقدم ويقوم بما يلي: (1) توقيع وتقديم أو الموافقة على طلب الشهادة نيابةً عن المتقدم (2) توقيع وتقديم شروط وأحكام المشترك نيابةً عن المتقدم و(3) الموافقة على شروط الاستخدام نيابةً عن المتقدم عندما يكون المتقدم شركة تابعة لهيئة التصديق أو الهيئة نفسها. وفي سياق هذا البيان يكون ممثل المتقدم مسؤولاً عن تقديم طلبات الشهادات وطلبات إلغائها نيابةً عن المتقدم. وتُستخدم عبارتا ممثل المتقدم و المُقدِّم بشكل متبادل.

مزود برمجيات التطبيقات: مورد لبرمجيات متصفح الإنترنت أو برمجيات التطبيقات الأخرى الخاصة بالأطراف المعتمدة التي تعرض أو تستخدم الشهادات وتدمج الشهادات الجذرية.

فترة التدقيق: في تدقيق يغطي فترة زمنية تمثل الفترة الزمنية الواقعة بين اليوم الأول (البداية) واليوم الأخير (النهاية) من العمليات التي يشملها التقييم من قبل المدققين. (ولا تعني هذه الفترة الزمنية مدة وجود المدققين فعلياً في مقر هيئة التصديق).

تقليص النطاق: يجوز لهيئة التصديق إزالة صفر أو أكثر من تسميات النطاق من اسم النطاق المؤهل الكامل (FQDN) من اليسار إلى اليمين حتى تصل إلى اسم النطاق الأساسي ويجوز لها استخدام أي من القيم الناتجة عن عملية التقليص (بما في ذلك اسم النطاق الأساسي ذاته) لغرض التحقق من النطاق.

المنافذ المصرح بها: تشمل المنافذ التالية: (HTTP80)) (HTTPS443)) (SMTP25)) (SSH22)).

اسم النطاق الأساسي: هو الجزء من اسم النطاق المؤهل الكامل (FQDN) الذي يتكوّن من أول عقدة نطاق تقع مباشرةً على يسار لاحقة عامة أو لاحقة خاضعة لإدارة السجل بالإضافة إلى تلك اللاحقة (مثل example.co.uk أو example.com).وفي أسماء النطاق التي تكون عقدتها اليمنى نطاقاً عاماً عالي المستوى (gTLD) يخضع للمواصفة 13 الخاصة بـ ICANN ضمن اتفاقية السجل يجوز استخدام gTLD نفسه كاسم نطاق أساسي.

شهادة التصديق CAA: وفقاً لـ :(https://tools.ietf.org/html/rfc8659) RFC 8659 يسمح سجل موارد CAA في DNS لحامل اسم النطاق بتحديد هيئة أو أكثر من هيئات التصديق (CAs) المصرح لها بإصدار الشهادات لذلك النطاق. وتُتيح سجلاتCAA لهيئات التصديق العامة تنفيذ ضوابط إضافية لتقليل مخاطر إصدار شهادات غير مقصودة..

زوج مفاتيح هيئة التصديق (CA Key Pair): هو زوج مفاتيح يظهر فيه المفتاح العام ضمن معلومات المفتاح العام الخاص بالموضوع في شهادة أو أكثر من شهادات الهيئة الجذرية والهيئة الفرعية.

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

بيانات الشهادة: تشمل طلبات الشهادات والبيانات المرتبطة بها (سواء الحصول عليها من المتقدم أو بوسائل أخرى) والتي تكون في حيازة هيئة التصديق أو تحت سيطرتها أو يمكنها الوصول إليها.

عملية إدارة الشهادات: تشمل العمليات والممارسات والإجراءات المرتبطة باستخدام المفاتيح والبرمجيات والأجهزة والتي تقوم من خلالها هيئة التصديق بالتحقق من بيانات الشهادات وإصدار الشهادات وصيانة المستودع وإلغاء الشهادات.

سياسة الشهادات: مجموعة من القواعد التي تُبين قابلية تطبيق شهادة معينة على مجتمع معين وتنفيذ محدد للبنية التحتية للمفاتيح العامة (PKI) مع متطلبات أمنية مشتركة.

تقرير مشكلة شهادة: شكوى تتعلق باشتباه في اختراق مفتاح أو إساءة استخدام شهادة أو أي نوع آخر من الاحتيال أو الاختراق أو السلوك غير الملائم المرتبط بالشهادات.

قائمة إلغاء الشهادات: قائمة موقّتة ومحدّثة بانتظام تضم الشهادات التي الغيت وتقوم هيئة التصديق التي أصدرتها بإنشائها وتوقيعها رقمياً.

هيئة التصديق: منظمة مسؤولة عن إنشاء وإصدار وإلغاء وإدارة الشهادات. ينطبق المصطلح بالتساوي على الهيئات الجذرية والهيئات الفرعية.

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

ملف تعريف الشهادة: مجموعة من الوثائق أو الملفات التي تُحدد متطلبات محتوى الشهادة وامتداداتها وفقاً للقسم 7 من المتطلبات الأساسية. على سبيل المثال يقدم القسم 7 من هذا البيان قائمة بملفات تعريف الشهادات المعرّفة ضمنه.

السيطرة: السيطرة (والمعاني المرتبطة بها مثل يخضع للسيطرة أو ضمن سيطرة مشتركة تعني امتلاك القدرة بشكل مباشر أو غير مباشرعلى: (1) توجيه إدارة الكيان أو موظفيه أو موارده المالية أو خططه أو (2) السيطرة على انتخاب غالبية أعضاء مجلس الإدارة أو (3) التصويت بالنسبة المطلوبة من الأسهم التي تمنح السيطرة بموجب قانون الولاية القضائية التي تأسيس الكيان أو تسجيله على ألا تقل النسبة في أي حال عن 10%.

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

جهاز المصادقة الثنائي: جهاز تشفير من نوع USB حاصل على شهادة توافق مع المعيار FIPS 140 المستوى 2 أو ما يعادله.

مولد أرقام عشوائية آمن تشفيرياً :(CSPRNG) مولد أرقام عشوائية مخصص للاستخدام في أنظمة التشفير.

طرف ثالث مفوض: شخص طبيعي أو كيان قانوني ليس من هيئة التصديق ولا تخضع أنشطته لنطاق عمليات التدقيق المناسبة للهيئة ولكن قوض من قبل هيئة التصديق للمساعدة في عملية إدارة الشهادات من خلال تنفيذ أو استيفاء واحد أو أكثر من متطلبات الهيئة المحددة في هذا البيان.

جهة الاتصال بالبريد الإلكتروني ضمن CAA في DNS (DNS CAA Email Contact): عنوان البريد الإلكتروني المحدد في الملحق A.1.1 من المتطلبات الأساسية.

جهة الاتصال الهاتفية ضمن CAA في DNS (DNS CAA Phone Contact): رقم الهاتف المحدد في الملحق A.1.2 من المتطلبات الأساسية.

جهة الاتصال بالبريد الإلكتروني ضمن سجل TXT في DNS (DNS TXT Record Email Contact): عنوان البريد الإلكتروني المحدد في الملحق A.2.1 من المتطلبات الأساسية.

جهة الاتصال الهاتفية ضمن سجل TXT في DNS (DNS TXT Record Phone Contact): رقم الهاتف المحدد في الملحق A.2.2 من المتطلبات الأساسية.

جهة الاتصال بالنطاق: مالك اسم النطاق أو جهة الاتصال التقنية أو الإدارية أو ما يعادلها ضمن نطاقاتccTLD كما هو مذكور في سجل WHOIS لاسم النطاق الأساسي أو في سجل SOA في DNSأو كما يُحصل عليه من خلال التواصل المباشر مع مسجل اسم النطاق.

تسمية النطاق: وفقاً لـ :(https://tools.ietf.org/html/rfc8499) RFC 8499 قائمة مرتبة من صفر أو أكثر من الوحدات الثمانية (Octets) التي تُشكّل جزءاً من اسم النطاق. ومن منظور نظرية الرسوم البيانية تُحدد التسمية عقدة واحدة ضمن جزء من الرسم البياني لجميع أسماء النطاقات الممكنة..

اسم النطاق: قائمة مرتبة من تسمية واحدة أو أكثر لاسم النطاق تُسند إلى عقدة في نظام أسماء النطاقاتDNS)).

حيز أسماء النطاق: مجموعة جميع أسماء النطاقات الممكنة التي تقع ضمن تسلسل هرمي تابع لعقدة واحدة في نظام أسماء النطاقات.

مسجل اسم النطاق: يُشار إليه أحياناً بـ مالك اسم النطاق لكنه يُعرّف بشكل أدق على أنه الشخص أو الكيان المسجل لدى جهة تسجيل أسماء النطاقات بصفته صاحب الحق في التحكم بكيفية استخدام اسم النطاق كالشخص الطبيعي أو الكيان القانوني المدرج كـ المسجل في سجل WHOIS أو لدى جهة التسجيل.

جهة تسجيل اسم النطاق: شخص أو كيان يقوم بتسجيل أسماء النطاقات بموجب تفويض أو اتفاق مع:

1. هيئة الإنترنت للأسماء والأرقام المخصصةICANN)).
2. سلطة/سجل وطني لأسماء النطاقات.
3. مركز معلومات الشبكةNIC)) بما في ذلك الجهات التابعة أو المتعاقدة أو المفوضة أو الورثة أو المتنازل لهم.

تاريخ الانتهاء: التاريخ المحدد في الحقل صالح حتى في الشهادة والذي يحدد نهاية فترة صلاحية الشهادة.

اسم النطاق المؤهل بالكامل FQDN: اسم نطاق يحتوي على جميع تسميات النطاق للعقد الأعلى منه في التسلسل الهرمي لنظام أسماء النطاق على الإنترنت.

جهة حكومية: كيان قانوني أو وكالة أو إدارة أو وزارة أو فرع أو عنصر مماثل تديره الحكومة في بلد ما أو تقسيم سياسي داخل ذلك البلد (مثل ولاية أو محافظة أو مدينة أو قضاء).

طلب شهادة عالي المخاطر: طلب تضعه هيئة التصديق ضمن فئة الطلبات التي تتطلب مراجعة إضافية استناداً إلى معايير وقواعد بيانات داخلية والتي قد تشمل أسماء يشتبه باستخدامها في التصيد الاحتيالي أو الأنشطة الاحتيالية الأخرى أو أسماء واردة في طلبات شهادات مرفوضة أو شهادات ملغاة سابقاً أو الأسماء المدرجة ضمن قوائم التصيد مثل أو الأسماء التي تُحددها هيئة التصديق استناداً إلى معاييرها الخاصة بالتخفيف من المخاطر.

الاسم الداخلي: سلسلة من الأحرف وليست عنوان (IP تظهر في حقل الاسم العام أو حقل اسم بديل للموضوع في الشهادة ولا يمكن التحقق من أنها فريدة عالمياً ضمن DNS العام وقت إصدار الشهادة لأنها لا تنتهي بنطاق من المستوى الأعلى (TLD)مسجل في قاعدة بيانات الجذر الخاصة بـIANA .

عنوان IP: رقم مكوّن من 32 أو 128 بت يُخصّص لجهاز يستخدم بروتوكول الإنترنت (IP) لغرض الاتصال.

جهة الاتصال الخاصة بعنوان IP: الشخص أو الكيان المُسجَّل لدى هيئة تسجيل عناوين IP على أنّه صاحب الحق في التحكم بكيفية استخدام عنوان (أو أكثر) من عناوينIP .

هيئة تسجيل عناوين IP: هيئة تعيين أرقام الإنترنت (IANA) أو سجل الإنترنت الإقليمي مثل RIPE أو APNIC أو ARIN أو AfriNIC أوLACNIC .

هيئة التصديق المُصدِرة (Issuing CA): بالنسبة لشهادة معيّنة هي هيئة التصديق التي أصدرت الشهادة. وقد تكون هيئة جذرية أو هيئة تصديق تابعة.

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

برنامج توليد المفاتيح: خطة موثقة للإجراءات الخاصة بتوليد زوج مفاتيح هيئة التصديق.

زوج المفاتيح: المفتاح الخاص والمفتاح العام المرتبط به.

تسمية LDH: كما ورد في:RFC 5890 سلسلة تتكوّن من أحرف ASCII وأرقام وعلامة الوصل (-) مع القيد الإضافي بألا تظهر علامة الوصل في بداية أو نهاية السلسلة. وكما هو الحال مع جميع تسمياتDNS يجب ألا يتجاوز الطول الإجمالي 63 بايتاً..

الكيان القانوني: جمعية أو شركة أو شراكة أو ملكية فردية أو صندوق ائتماني أو جهة حكومية أو أي كيان يتمتع بوضع قانوني في نظام قانوني وطني.

التحليل الإحصائي: عملية يتم فيها التحقق من محتوى البيانات الموقعة رقمياً – مثل شهادة ما قبل الإصدار أو الشهادة أو قائمة إلغاء الشهاداتCRL)) أو استجابة OCSPأو كائن البيانات المطلوب توقيعه مثل – للتأكد من التوافق مع المواصفات والمتطلبات المعرّفة في هذه المتطلبات.

تأكيد الإصدار من منظور متعدد: عملية تُؤكَّد فيها النتائج التي توصل إليها أثناء تحقق المجال وفحص CAA من قبل المنظور الشبكي الأساسي بواسطة وجهات نظر شبكية أخرى قبل إصدار الشهادة.

المنظور الشبكي: مرتبط بعملية تأكيد الإصدار من منظور متعدد. هو نظام (مثل خادم مستضاف على السحابة) أو مجموعة من مكونات الشبكة (مثل شبكة VPN والبنية التحتية المرتبطة بها) تُستخدم لإرسال حركة الإنترنت الصادرة المرتبطة بطريقة تحقق من التحكم بالمجال أو فحص .CAA يُحدَّد موقع المنظور الشبكي بالنقطة التي يُسلَّم فيها عادةً أولاً تدفق الإنترنت الصادر غير المُغلف إلى البنية التحتية للشبكة التي توفّر الاتصال بالإنترنت لذلك المنظور.

تسمية LDH غير المحجوزة: كما ورد في:RFC 5890 مجموعة تسميات LDH الصالحة التي لا تحتوي على السلسلة في الموضعين الثالث والرابع.

المعرّف الكائن: معرّف فريد يتكوّن من حروف وأرقام أو أرقام فقط مُسجَّل بموجب المعيار المعتمد من قبل المنظمة الدولية للتوحيد القياسي (ISO) لكائن معيّن أو فئة كائنات معيّنة.

المُجيب OCSP: خادم عبر الإنترنت يُشغَّل تحت سلطة هيئة التصديق (CA) ويكون متصلاً بمستودعها لمعالجة طلبات حالة الشهادة يُرجى مراجعة بروتوكول حالة الشهادة عبر الإنترنتOCSP)).

اسم نطاق: onion اسم نطاق مؤهل بالكامل ينتهي باسم النطاق الخاص للاستخدام وفق RFC 7686 وهو onion على سبيل المثال:
2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion هو اسم نطاق onion بينما torproject.orgليس اسم نطاقonion. .

بروتوكول حالة الشهادة عبر الإنترنت (OCSP): بروتوكول تحقق من الشهادات عبر الإنترنت يتيح لتطبيقات الأطراف المعتمدة التحقق من حالة شهادة معيّنة. يُرجى مراجعة مُجيبOCSP .

المنظور الشبكي الأساسي: هو المنظور الشبكي الذي تستخدمه هيئة التصديق لاتخاذ القرار بشأن:

1. صلاحيتها لإصدار شهادة للنطاق أو عنوان IP المطلوب.

2. وسلطة المتقدّم بالطلب امتلاكه أو تحكمه بالنطاق أو عنوان IP المطلوب.

المفتاح الخاص: المفتاح من زوج المفاتيح الذي يحتفظ به صاحبه بسرية ويُستخدم لإنشاء التواقيع الرقمية لفك تشفير السجلات أو الملفات الإلكترونية التي شفرت بالمفتاح العام المقابل.

المفتاح العام: المفتاح من زوج المفاتيح الذي يمكن لصاحبه الإفصاح عنه علناً ويُستخدم من قبل الطرف المعتمد للتحقق من التوقيع الرقمي المُنشأ بواسطة المفتاح الخاص المقابل لتشفير الرسائل بحيث لا يمكن فك تشفيرها إلا بواسطة المفتاح الخاص المقابل.

البنية التحتية للمفتاح العام (PKI): مجموعة من الأجهزة والبرمجيات والأفراد والإجراءات والقواعد والسياسات والالتزامات التي تُستخدم لتسهيل إنشاء الشهادات وإصدارها وإدارتها واستخدامها بشكل موثوق استناداً إلى التشفير بالمفتاح العام.

شهادة موثوقة علنياً: شهادة تحظى بالثقة بناءً على كون الشهادة الجذرية المقابلة لها موزعة كنقطة ثقة في برامج التطبيقات المتاحة على نطاق واسع.

مدقق مؤهل: شخص طبيعي أو كيان قانوني يفي بمتطلبات القسم 8.2.

قيمة عشوائية: قيمة تُحدّدها هيئة التصديق للمتقدّم بالطلب وتتميّز باحتوائها على ما لا يقل عن 112 بت من العشوائية .

اسم النطاق المسجَّل: اسم نطاق سجل لدى جهة تسجيل أسماء النطاقات.

هيئة التسجيل (RA): أي كيان قانوني مسؤول عن التعرّف على مواضيع الشهادات والتحقق من هويتهم ولكنه ليس هيئة تصديقCA)) وبالتالي لا يوقّع ولا يصدر الشهادات. يمكن لهيئة التسجيل أن تُساعد في عملية طلب الشهادة أو عملية إلغائها أو كلتيهما. وعندما تُستخدمRA كصفة لوصف وظيفة أو دور فهذا لا يعني بالضرورة أنها جهة مستقلة بل يمكن أن تكون جزءاً من هيئة التصديق. في سياق بيان ممارسة الشهادات (CPS) هذا تدير شركة مصدر التكنولوجيا وظيفة هيئة التسجيل.

مصدر بيانات موثوق: وثيقة تعريفية أو مصدر بيانات يُستخدم للتحقق من معلومات هوية الموضوع ويُعترف به بشكل عام بين المؤسسات التجارية والحكومات كمصدر موثوق ويكون قد أُنشئ من قبل طرف ثالث لغرض غير متعلق بالحصول على شهادة من قبل المتقدم بالطلب. في سياق بيان ممارسة الشهادات هذا تُعد جهة التأسيس أو التسجيل العراقية المصدر الموثوق للكيانات غير الحكومية فيما تُعد الجريدة الرسمية العراقية المصدر الموثوق للكيانات الحكومية.

طريقة اتصال موثوقة: وسيلة اتصال – مثل عنوان بريدي/خدمة بريد سريع أو رقم هاتف أو عنوان بريد إلكتروني –التحقق منها باستخدام مصدر غير ممثل المتقدم بالطلب.

الطرف المعتمد: أي شخص طبيعي أو كيان قانوني يعتمد على شهادة صالحة. لا يُعدّ موفّر البرمجيات الطرف المعتمد عندما تقوم البرمجيات الموزعة منه فقط بعرض معلومات متعلقة بالشهادة.

المستودع: قاعدة بيانات إلكترونية تحتوي على مستندات حوكمة البنية التحتية للمفتاح العام (PKI) التي افصح عنها علناً – مثل سياسات الشهادات (CPs) وبيانات ممارسة الشهادات – (CPSs) إضافةً إلى معلومات حالة الشهادات إما على شكل قائمة إلغاء الشهادات (CRL) أو استجابةOCSP .

رمز الطلب: قيمة تُشتقّ بطريقة تحددها هيئة التصديق وتربط هذا الإثبات بالتحكم بطلب الشهادة. من أمثلة رموز الطلب:
((1تجزئة المفتاح العام
((2تجزئة معلومات المفتاح العام للموضوع [X.509]
((3تجزئة طلب الشهادة بصيغةPKCS#10 .

عنوان IP محجوز: عنوان IPv4 أو IPv6 يقع ضمن كتلة عناوين مُدرجة في أي من سجلات IANA التالية:

- https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml.
- https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml.

هيئة التصديق الجذرية: أعلى مستوى من هيئات التصديق وتُوزَّع شهادتها الجذرية من قبل موفّري البرامج التطبيقية وهي المسؤولة عن إصدار شهادات هيئات التصديق التابعة.

الشهادة الجذرية: شهادة موقّعة ذاتياً تصدرها هيئة التصديق الجذرية (Root CA) لتعريف نفسها ولتسهيل التحقق من الشهادات التي تصدرها لهيئات التصديق التابعة التابعة لها.

شهادة مشترك قصيرة الأجل:

- بالنسبة للشهادات الصادرة في أو بعد 15 آذار 2024 وحتى 14 آذار 2026: شهادة مشترك بفترة صلاحية لا تتجاوز 10 أيام (864,000 ثانية).
- بالنسبة للشهادات الصادرة في أو بعد 15 آذار 2026: شهادة مشترك بفترة صلاحية لا تتجاوز 7 أيام (604,800 ثانية).

الموضوع: الكيان أو المنظمة المحددة في حقل الموضوع داخل الشهادة.

معلومات هوية الموضوع: المعلومات التي تُعرّف موضوع الشهادة. لا تشمل هذه المعلومات اسم النطاق المُدرج في امتداد subjectAltNameأو الحقل commonName في الموضوع.

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

المشترك: كيان قانوني تُصدر له شهادة ويكون ملزماً قانوناً بشروط وأحكام خاصة بالمشترك أو بشروط الاستخدام.

شروط وأحكام المشترك: اتفاق بين هيئة التصديق والمتقدّم بالطلب/المشترك يحدّد حقوق والتزامات الطرفين.

شهادة هيئة تصديق تابعة مقيدة تقنياً: شهادة هيئة تصديق تابعة تَستخدم مزيجاً من إعدادات الاستخدام الموسع للمفتاح إعدادات قيود الأسماء للحدّ من النطاق الذي يمكن ضمنه إصدار شهادات مشتركين أو شهادات لهيئات تصديق تابعة إضافية.

شروط الاستخدام: أحكام تتعلّق بحفظ الشهادة واستخدامها المسموح به والتي تُطبَّق عندما يكون المتقدّم بالطلب/المشترك تابعاً لهيئة التصديق أو هو هيئة التصديق نفسها.

شهادة اختبار: لم يَعُد يُستخدم هذا المصطلح في هذه المتطلبات الأساسية.

نظام موثوق: مكونات مادية وبرمجية وإجراءات حاسوبية تتسم بما يلي:

- تأمين معقول ضد التطفّل وسوء الاستخدام.
- توفر مستوى مقبول من التوافر والموثوقية والصحة التشغيلية.
- ملاءمة معقولة للوظائف المقصودة.
- تطبيق سياسة الأمان المعتمدة.

اسم نطاق غير مسجَّل: اسم نطاق لم يتم تسجيله لدى جهة تسجيل أسماء النطاقات.

النطاق الأعلى: الجزء الأخير من اسم النطاق مثل com. أو net. أو .org. في سياق بيان ممارسة الشهادات هذا النطاق الأعلى هوIQ.

شهادة صالحة: شهادة تجتاز إجراء التحقق المحدد فيRFC 5280 .

مختصو التحقق: أشخاص يتولّون مهام التحقق من المعلومات وفقاً للمتطلبات المحددة في هذه الوثيقة. فترة الصلاحية : المدة الزمنية المحسوبة من تاريخ إصدار الشهادة حتى تاريخ انتهائها.

خدمة WHOIS: معلومات تُسترجَع مباشرة من مسجّل اسم النطاق أو مشغل السجل عبر البروتوكول المعرّف في RFC 3912أو بروتوكول الوصول إلى بيانات السجل المعرف فيRFC 7482 أو عبر موقع HTTPS .

شهادة Wildcard: شهادة تحتوي على اسم نطاق Wildcard واحد على الأقل ضمن أسماء النطاقات البديلة (SANs) في الشهادة.

تصنيف -XN: وفقاً لRFC 5890 هو نوع من التصنيفات يبدأ بالمقدمة --xn (بغض النظر عن حالة الأحرف) ويتوافق مع قواعد تصنيفاتLDH .

1.6.2 الاختصارات

AICPA	المعهد الأمريكي للمحاسبين القانونيين المعتمدين
ADN	اسم النطاق المصرح به
CA	هيئة التصديق
CAA	تفويض هيئة التصديق
ccTLD	نطاق المستوى الأعلى لرمز الدولة
CICA	المعهد الكندي للمحاسبين القانونيين المعتمدين
CCTV	كاميرات المراقبة
CP	سياسة الشهادات
CPS	بيان ممارسة الشهادات
CRL	قائمة إلغاء الشهادات
CSR	طلب توقيع الشهادة
DBA	يمارس الأعمال تحت اسم
DN	الاسم المميز
DNS	نظام أسماء النطاقات
EID	بطاقة الهوية الإلكترونية
EIDAS	خدمات التعريف والمصادقة والثقة الإلكترونية
ETSI	المعهد الأوروبي لمعايير الاتصالات
FIPS	معيار المعالجة الفيدرالي للمعلومات
FQDN	اسم النطاق المؤهل بالكامل
HSM	وحدة أمان الأجهزة
HTTP	بروتوكول نقل النص الفائق
IANA	هيئة تخصيص أرقام الإنترنت
ICANN	مؤسسة الإنترنت للأسماء والأرقام المخصصة
IETF	فرقة مهام هندسة الإنترنت

IM	المراسلة الفورية
IPSEC	بروتوكول أمان الإنترنت
ISO	المنظمة الدولية للمواصفات
IT	تكنولوجيا المعلومات
ITPC	الشركة العامة للاتصالات والمعلوماتية
NIST	المعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة)
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	صيغة طلب الشهادة
PKI	البنية التحتية للمفتاح العام
PMA	اللجنة العليا لإدارة التوقيع الإلكتروني
RA	هيئة التسجيل
RSA	ريفست-شامير-أدلمن (أسماء مبتكري خوارزميةRSA)
RTO	هدف وقت الاستعادة
SSL	طبقة المقابس الآمنة
TS	مصدر التكنلوجيا
TLD	نطاق المستوى الأعلى
TSA	هيئة ختم الوقت
TLS	بروتوكول طبقة النقل الآمنة
TSP	مزود خدمات موثوق
UPS	مزود طاقة غير منقطع
URI	معرف الموارد الموحد مثل: عنوان URL أو FTP أو البريد الإلكتروني

URL	محدد موقع الموارد الموحد
VPN	الشبكة الخاصة الافتراضية
VoIP	نقل الصوت عبر بروتوكول الإنترنت

1.6.3 المراجع

يستند هذا الوثيقة في مرجعيتها إلى المعايير التالية:

- معيار:X.509 معيار الاتحاد الدولي للاتصالات - قطاع الاتصالات (ITU-T) الخاص بالشهادات الرقمية.
- معيار:RFC3647 إطار عمل سياسات شهادات البنية التحتية للمفاتيح العامة (PKI) وممارسات التصديق عبر الإنترنت.
- معيار :RFC5280 ملف تعريف شهادات البنية التحتية للمفاتيح العامة (PKI) وقوائم إبطال الشهادات (CRL)).
- مبادئ ومعايير:WebTrust الصادرة عن (AICPA/CPA Canada) الخاصة بسلطات التصديق - المتطلبات الأساسية لTLS)).
- مبادئ ومعايير:WebTrust الصادرة عن (AICPA/CPA Canada) الخاصة بسلطات التصديق.
- مبادئ ومعايير:WebTrust الصادرة عن (AICPA/CPA Canada) الخاصة بسلطات التصديق - أمن الشبكات.
- المتطلبات الأساسية لمنتدى متصفحات وشركات التصديق:(CA/Browser Forum) المتعلقة بإصدار وإدارة شهادات خوادم (TLS) الموثوقة علناً.
- متطلبات أمن الشبكات وأنظمة الشهادات: الصادرة عن منتدى متصفحات وشركات التصديق (CA/Browser Forum)).

2 المسؤوليات المتعلقة بالنشر والمستودعات

2.1 المستودعات

تحافظ شركة مصدر التكنولوجيا على مستودع إلكتروني متاح على مدار الساعة (24 × 7) ويمكن الوصول إليه عبر الرابط التالي:
https://pki.techsource.iq.

تتحمّل شركة مصدر التكنولوجيا مسؤولية توفير المعلومات التالية لنشرها في مستودعها:

- النسخ الحالية والسابقة من بيانات ممارسة الشهادات (CPS) الخاصة بشركة مصدر التكنولوجيا.
- النسخة الحالية من سياسة الشهادات وبيانات ممارسة الشهادات الخاصة بهيئة الجذرITPC وكذلك سياسة الشهادات لمزود خدمات الثقةTSP CP)).
- شروط وأحكام المشتركين ومسؤولي هيئة التسجيل المحليينLRA)) وأطراف الاعتماد بالإضافة إلى بيان إفصاح البنية التحتية للمفتاح العام (PKI) وسياسة وهيكلية هيئة ختم الوقتTSA CP/PS)) وبيان الإفصاح الخاص بهيئة ختم الوقت.
- شهادات هيئة التصديق الجذرية الموقعة ذاتياً والصالحة بالإضافة إلى شهادات هيئات التصديق التابعة التابعة لشركة مصدر التكنولوجيا وشهاداتOCSP وقوائم إلغاء الشهادات (CRLs) الصادرة عن الهيئات الفرعية.
- شهادات وحدة ختم الوقتTSU)).
- تقارير التدقيق.

2.2 نشر معلومات الشهادات

تُعد شركة مصدر التكنولوجيا الجهة المسؤولة عن توفير المعلومات للنشر كما ورد في القسم 2.1 من هذه الوثيقة.

تنشر شركة مصدر التكنولوجيا معلومات حالة صلاحية الشهادات على فترات منتظمة كما هو موضح في بيان ممارسة الشهادات .(CPS) وتُقدَّم هذه الخدمة كمصدر متاح على مدار الساعة (7/24) على النحو التالي:

- نشر قوائم إلغاء الشهادات (CRLs) متضمنة أي تغييرات طرأت منذ نشر القائمة السابقة على فترات منتظمة. تُدرج هيئة التصديق TS TLS CA رابطاً (URL) إلى قائمة الإلغاء ذات الصلة ضمن شهادات المشتركين كجزء من امتداد CDPعند توفر هذا الامتداد.
- مستجيب OCSP متوافق مع .RFC 6960 يُشار إلى عنوان URL الخاص بـ OCSP في امتداد AIA ضمن شهادات المشتركين الصادرة عن هذه الهيئة.

تستضيف شركة مصدر التكنولوجيا صفحات اختبار إلكترونية تتيح لمطوري التطبيقات اختبار برمجياتهم باستخدام شهادات المشتركين. أدناه صفحات اختبار لشهادات صالحة ملغاة ومنتهية الصلاحية:

شهادات OV التحقق التنظيمي	
الشهادات الصالحة	https://good.techsource.iq

شهادات OV التحقق التنظيمي	
الشهادات الملغاة	https://revoked.techsource.iq
الشهادات المنتهية الصلاحية	https://expired.techsource.iq

2.3 توقيت أو تكرار النشر

يُجري مجلس حوكمة البنية التحتية للمفتاح العام في مصدر التكنولوجيا (TS PKI GB) مراجعة لهذا البيان لممارسة الشهادات (CPS) مرة واحدة على الأقل سنوياً ويجري التعديلات المناسبة لضمان بقاء عمليات هيئات التصديق التابعة متماشية بالكامل مع المتطلبات المذكورة في القسم 1 من هذا البيان.

في الحالات التي لا تتطلب أي تغييرات يتم زيادة رقم إصدارCPS وإدراج سجل تغيير مؤرخ لتوثيق عملية المراجعة.
تُنشر النسخ المعدلة من CPS والاتفاقيات (شروط وأحكام المشترك واتفاقية طرف الاعتماد) في غضون خمسة أيام من اعتمادها من قبل مجلس حوكمة PKI في مصدر التكنولوجيا.

2.3.1 شهادات هيئة التصديق

تُنشر شهادات هيئات التصديق التابعة وشهادات OCSP في المستودع العام فور إصدارها وتبقى متاحة حتى انتهاء صلاحيتها أو إعادة إصدارها وإصدار شهادات جديدة بدلاً منها.

2.3.2 قوائم إلغاء الشهادات(CRLs)

تقوم هذه الهيئة الفرعية بإدارة ونشر قوائم إلغاء الشهادات كما يلي:

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

تستمر الهيئة الفرعية في إصدار قوائم الإلغاء حتى يتحقق أحد الشرطين التاليين:

- انتهاء صلاحية أو إلغاء جميع شهادات الهيئة الفرعية التي تحتوي على نفس المفتاح العام.
- أو تدمير المفتاح الخاص المقابل للهيئة الفرعية.

2.4 ضوابط الوصول إلى المستودعات

تكون المعلومات المنشورة في مستودع مصدر التكنولوجيا العام متاحة للجمهور ويُضمن الوصول المفتوح للقراءة دون قيود.

تُطبق شركة مصدر التكنولوجيا تدابير أمنية منطقية ومادية لمنع أي شخص غير مصرح له من إضافة أو حذف أو تعديل البيانات ضمن المستودع.

3 التعريف والمصادقة

3.1 التسمية

3.1.1 أنواع الأسماء

تتوافق أسماء الموضوعات في شهادة TS TLS CA مع معايير الأسماء المميزة وفق معيارX.500 .

يُجرى التحقق من اسم الموضوع المستخدم في شهادة هيئة التصديق ويُعتمد من قبل وظيفة هيئة التسجيل (RA) التابعة لاللجنة العليا لإدارة التوقيع الإلكترونيPMA)) ويجب أن يكون هذا الاسم ذو دلالة واضحة ولا يجوز إعادة تعيينه إلى كيان آخر في أي وقت.

يُعرّف TS TLS CA ضمن حقل اسم المُصدِر في شهادات المشتركين على النحو التالي:

3.1.1.1 شهادة TS TLS CA

CN	TS TLS CA G1
O	مصدر التكنولوجيا
الدولة C	IQ العراق

تستخدم الشهادات الصادرة عن هذه الهيئة أسماء مميزة وفقاً لما هو محدد في معايير التوصية .ITU-T X.500 توضح الجداول أدناه بُنى DN المعتمدة لكل نوع من أنواع الشهادات المدعومة.

3.1.1.2 شهادات التحقق التنظيمي:(OV)

السمة	القيمة
subjectAltName	عنوان IP عام أو أسماء نطاق مؤهلة بالكاملFQDNs)) أو نطاقات موثّقة تقع تحت سيطرة المشترك
O المنظمة	الاسم القانوني الكامل للمنظمة التي تُصدر لها الشهادة
الدولة C	IQ العراق
L اختياري إذا توفّر S وإلزامي بخلاف ذلك	المدينة أو الموقع الجغرافي لمقر المنظمة
S اختياري إذا توفّر L وإلزامي بخلاف ذلك	الولاية أو المقاطعة التي يقع فيها مقر المنظمة

3.1.1.3 شهادات OCSP

السمة	القيمة
CN	TS TLS CA G1 OCSP
O المنظمة	مصدر التكنلوجيا
الدولة C	IQ العراق

3.1.2 الحاجة إلى أن تكون الأسماء ذات معنى

تكون الشهادات الصادرة وفقاً لبيان ممارسة الشهادات هذا ذات معنى فقط إذا كانت الأسماء الظاهرة فيها مفهومة وقابلة للاستخدام من قبل الأطراف المعتمدة .تُستخدم الأسماء المميزة (DN) لتحديد كل من الموضوع والجهة المُصدرة للشهادة بطريقة ذات معنى.

وبناءً عليه تُصدر هيئة التصديق هذه الشهادات للمشتركين (الموضوعات) الذين يثبتون بصورة مشروعة ملكيتهم وسيطرتهم على الاسم المميزوأسماء النطاق وعناوينIP المذكورة في الاسم المميز للموضوع وفي أسماء الموضوع البديلة.

في حالة شهادة مستجيب :OCSP يكون الاسم ذا معنى لأنه يحدد اسم مستجيب شهادة OCSP لهيئة التصديق التابعة.

3.1.3 عدم السماح بإخفاء الهوية أو استخدام الأسماء المستعارة للمشتركين

لا يُسمح للمشتركين المجهولين أو الذين يستخدمون أسماء مستعارة.

3.1.4 قواعد تفسير أشكال الأسماء المختلفة

تعتمد اتفاقية التسمية المُستخدمة من قبل هذه الهيئة على معيار (X.500) ISO/IEC 9595 للأسماء المميزةDN)).

3.1.5 تفرّد الأسماء

يُفرض التفرّد من خلال استخدام أسماء نطاق DNS العامة المسجلة (FQDNs) أو عناوين IP العامة.

ويجب استخدام امتداد اسم الموضوع البديل (SubjectAltName) لتحديد النطاق المعني واسم نطاق واحد أو أكثر إضافي في الشهادة.

يُحظر استخدام أسماء النطاقات الداخلية وعناوين IP المحجوزة.

في حالة شهادة مستجيب :OCSP يُدرج الاسم الفريد لمستجيب OCSP في الاسم المميز للموضوع لشهادة OCSP الصادرة.

3.1.6 التعرف على العلامات التجارية والتحقق منها ودورها

يوافق المتقدمون عند تقديم طلب شهادة إلى هذه الهيئة على أن طلبهم لا يحتوي على أي بيانات تتعارض بأي شكل من الأشكال مع حقوق أي طرف ثالث في أي ولاية قضائية فيما يخص العلامات التجارية أو علامات الخدمة أو الأسماء التجارية أو أسماء الشركات أو أسماء العمل تحت اسم (DBA) أو أي حقوق ملكية فكرية أخرى كما يقرّون بعدم تقديم هذه البيانات لأي غرض غير قانوني.

تحتفظ هذه الهيئة بحقها في إلغاء الشهادة عند استلام أمر موثّق على نحو مناسب من مجلس حوكمة البنية التحتية للمفتاح العامTS PKI GB)) أو من محكمة ذات اختصاص قضائي تقضي بإلغاء شهادة أو شهادات تحتوي على اسم موضوع محل نزاع.

3.2 التحقق الأولي من هوية المشترك

تُستخدم الطرق الموضحة في هذا القسم للتحقق من هوية المشترك.

تتحقق هيئة التسجيل (TS RA) من هوية المتقدم بالطلب وصفاته الأخرى وتُصادق عليها قبل تضمين هذه الصفات في الشهادة.
يجوز لهيئة التسجيل رفض إصدار الشهادة وفقاً لتقديرها المطلق إذا لم تنجح عملية التحقق من الهوية.

3.2.1 طريقة إثبات حيازة المفتاح الخاص

يُقدِّم المتقدم بالطلب طلب توقيع شهادة (CSR) من نوع PKCS#10 موقعاً رقمياً لإثبات حيازته للمفتاح الخاص المقابل للمفتاح العام المراد تضمينه في الشهادة. تفرض أنظمة هيئة التسجيل (TS RA) التحقق من إثبات الحيازة كجزء من معالجة طلب الشهادة.
يُقدَّم إثبات الحيازة إلى هيئة التسجيل عبر طلبات CSR بتنسيقPKCS#10 .

3.2.2 التحقق من هوية المنظمة وهوية النطاق

3.2.2.1 الهوية

تُتحقق هوية المتقدم بالطلب من الكيانات التنظيمية من خلال مصادر بيانات موثوقة يُتوقع أن توفّر معلومات تفصيلية عن الكيان بما في ذلك الاسم القانوني العنوان ومعلومات الممثل المفوض.

تعتمد شركة مصدر التكنولوجيا على الوقائع العراقية أو وسائل اتصال مباشرة أخرى مع الكيان أو الجهة القضائية المختصة بإنشاء أو وجود أو الاعتراف القانوني بالكيان للتحقق من معلومات الجهات الحكومية وعلى اتصال رسمي مع دائرة تسجيل الشركات العراقية للكيانات غير الحكومية.

يجوز لشركة مصدر التكنولوجيا أن تطلب من المتقدم بالطلب تقديم مستندات رسمية للكيان لتأكيد هوية الموضوع مثل النظام الداخلي للشركة مستند ضريبي صادر عن جهة حكومية خطاب مهني (مثل خطاب محاسب أو رأي قانوني) أو مستندات أخرى ذات صلة وقد تُجري زيارة ميدانية لموقع الكيان للتحقق من عنوانه.

بالإضافة إلى ذلك تتحقق شركة مصدر التكنولوجيا من حق المتقدم بالطلب في استخدام اسم (أسماء) النطاق التي ستُدرج في الشهادة وفقاً للإجراءات الواردة في القسم 3.2.2.4.

تضمن هيئة التسجيل أن يتم جمع البيانات التحققية مرة أخرى والتحقق منها خلال مدة لا تتجاوز 398 يوماً من تاريخ آخر تحقق اجري.

تتحقق هيئة التسجيل من ارتباط مقدم الطلب بموضوع الشهادة من خلال ضمان أن المعلومات المقدَّمة في نموذج الطلب تتطابق تماماً مع المعلومات التي ستُدرج في الشهادة.

سلطة المتقدم بالطلب

يتخذ مسؤول هيئة التسجيل خطوات معقولة للتأكد من أن طلب الشهادة المقدَّم نيابة عن مؤسسة هو طلب مشروع ومخول أصولياً.
ويتم التحقق من سلطة الشخص الذي يقدِّم طلب الشهادة وفقاً لما ورد في القسم 3.2.5.

3.2.2.2 الاسم التجاري أو اسم يعمل تحت اسم(DBA)

لا تدعم هيئة التصديق هذه استخدام اسم يعمل تحت اسم (DBA) أوالاسم التجاري ضمن معلومات هوية الموضوع في الشهادة.

3.2.2.3 التحقق من الدولة

تُصدر هيئة التصديق هذه الشهادات فقط للمنظمات المُسجَّلة في العراق .وتتحقق هيئة التسجيل (TS RA) من أن القيمة الموجودة في حقل الدولة ضمن معلومات هوية الموضوع هيIQ .

3.2.2.4 التحقق من تفويض أو سيطرة النطاق

بالنسبة لكل اسم نطاق سيُدرج في موضوع الشهادة تتحقق هيئة التسجيل (TS RA) من سيطرة المتقدم بالطلب على اسم النطاق وفقاً لمتطلبات الأساس القسم 3.2.2.4.

تحتفظ هيئة التسجيل أيضاً بسجل لطريقة التحقق المستخدمة بما في ذلك رقم إصدار متطلبات الأساس (BR) المستخدم في التحقق من كل اسم نطاق.

يُنفّذ هذا التحقق باستخدام إحدى الطرق المعتمدة التالية لكل اسم نطاق مؤهل(FQDN)):

- التحقق عبر البريد الإلكتروني:

إرسال بريد إلكتروني يتضمن قيمة عشوائية وفريدة (صالحة لمدة لا تتجاوز 30 يوماً من إنشائها) إلى عنوان بريد إلكتروني إداري مرتبط باسم النطاق مثل.admin@organization.iq :
قد تُستخدم العناوين التالية في هذا التحقق:
admin@ administrator@ webmaster@ hostmaster@ postmaster@
وفقاً للقسم 3.2.2.4.4 من متطلبات الأساس.

- تغيير سجل نظام أسماء النطاقات(DNS) :

التحقق من وجود قيمة عشوائية فريدة أو رمز طلب ضمن سجل DNS من نوع CNAME أو TXT أو CAA لاسم نطاق التفويض أو اسم نطاق التفويض المسبوق بتسمية تبدأ بعلامة الشرطة السفلية وفقاً للقسم 3.2.2.4.7 من متطلبات الأساس.

ويجب تنفيذ هذه الطريقة من منظور شبكة رئيسية (ضمن نفس مجموعة الشبكة الخاصة بتشغيل هيئة التصديق) ومن منظور شبكة عن بُعد (ضمن مجموعة شبكة مختلفة عن تشغيل هيئة التصديق) كجزء من تنفيذ آلية إثبات الإصدار من وجهات نظر متعددة ((Multi-Perspective Issuance Corroborationكما هو مبيَّن في القسم 3.2.2.9. لكي يُعتبَر منظور الشبكة البعيدة داعماً للإصدار ويُستخدم كإذن لإصدار الشهادات يجب أن يلاحظ مسؤول هيئة التسجيل TS RA) (Officerنفس معلومات التحدي (مثل: القيمة العشوائية أو رمز الطلب) كما يلاحظها من منظور الشبكة الرئيسية. عندما تكون منطقة نظام أسماء النطاقات (DNS) الخاصة بالنطاق موقّعة رقمياً وتدعم بروتوكول أمن نظام أسماء النطاقات

DNSSEC))، تخضع جميع استعلامات الـ (DNS) المُجراة لأغراض التحقق لعملية المصادقة وفق معاييرDNSSEC))، وصولاً إلى "مرساة الثقة (Root Trust Anchor) "الخاصة بجذور الـ (DNSSEC) لدى منظمةIANA)).

- يُعد التحقق من صحة (DNSSEC) إلزامياً لمنظور الشبكة الأساسي (Primary Network Perspective) في حال توفر ميزة الـDNSSEC)).
- يُعد التحقق من صحة (DNSSEC) اختيارياً (ويوصى به) لمنظورات الشبكة البعيدة (Remote Network Perspectives).
- تلتزم "شركة مصدر التكنلوجيا (Technology Source) "بعدم تعطيل أو تجاوز عملية التحقق من صحة (DNSSEC)لأي استعلام متعلق بتفويض النطاق أو السيطرة عليه عند وجود تواقيعDNSSEC)).
- ولا تمنح "شركة مصدر التكنلوجيا (Technology Source) "شهادات (TLS) للنطاقات التي تنتهي باللاحقة (.onion)).

3.2.2.5 التحقق من ملكية عنوانIP

يُتحقق من ملكية عنوان (عناوين) IP المطلوب تضمينها في الشهادة باستخدام الطرق التالية:

- التغيير المتفق عليه على موقع الويب:

يقوم المتقدم بالطلب بإثبات سيطرته على عنوان (عناوين) IP المطلوبة من خلال تأكيد وجود قيمة عشوائية ضمن ملف موجود في مجلد /well-known/pki-validation على عنوان IP المفوض.

الوصول عبر HTTP/HTTPS إلى منفذ مفوض: يجب أن يكون الملف الذي يحتوي على القيمة العشوائية متاحاً للوصول من قبل هيئة التصديق عبر بروتوكول HTTP أو HTTPS من خلال منفذ مفوض .وفقاً للقسم 3.2.2.5.1 من متطلبات الأساس.

ويجب تنفيذ هذه الطريقة من منظور شبكة رئيسية (ضمن نفس مجموعة الشبكة الخاصة بتشغيل هيئة التصديق) ومن منظور شبكة عن بُعد (ضمن مجموعة شبكة مختلفة) كجزء من تنفيذ آلية إثبات الإصدار من وجهات نظر متعددة كما هو موضح في القسم 3.2.2.9 .لكي يُعتبَر منظور الشبكة البعيدة مؤيداً ويُستخدم كإذن لإصدار الشهادات يجب أن يلاحظ مسؤول هيئة التسجيل (TS RA Officer) نفس معلومات التحدي (مثل: القيمة العشوائية أو رمز الطلب) كما في منظور الشبكة الرئيسية.

- البحث العكسي لعناوينIP :

يُجرى استعلام عكسي لعنوان IP ثم يُتحقق من السيطرة على اسم النطاق الناتج باستخدام الطرق المدعومة .وفقاً للقسم 3.2.2.5.3 من متطلبات الأساس.

ويجب أيضاً تنفيذ هذه الطريقة من منظور شبكة رئيسية ومن منظور شبكة عن بُعد كجزء من تنفيذ آلية إثبات الإصدار من وجهات نظر متعددة ولكي يُعتبَر منظور الشبكة مؤيداً يجب أن يلاحظ نفس اسم النطاق المؤهل بالكامل (FQDN) كما في منظور الشبكة الرئيسية.

3.2.2.6 التحقق من النطاقات العامة

قبل إصدار شهادة تحتوي على محرف عام (*) في الحقل الاسم المشترك ((CNأو في امتداد SubjectAltName تُطبّق التحققات التالية:

1. تتضمن شهادات SSL العامة (Wildcard SSL) محرف النجمة (*) كأول محرف في حقل الاسم المشترك (CN) لحقل الموضوع أو في امتداد SubjectAltName.
2. يجب ألا يظهر محرف النجمة ضمن الجزء الذي يقع مباشرةً يسار لاحقة النطاق العامة أو التي تُدار من قبل السجل.
3. يُقبل إصدار الشهادة فقط إذا أثبت المتقدم بالطلب سيطرته المشروعة على مساحة أسماء النطاق بالكامل. مثلاً لا يجوز لهيئة التسجيل إصدار شهادة لـ local أو.co.iq. ولكن يمكن إصدار شهادة لexample.iq..

3.2.2.7 دقة مصادر البيانات

تستخدم شركة مصدر التكنولوجيا عملية داخلية للتحقق من دقة مصادر المعلومات وقواعد البيانات لضمان قبول البيانات.
وقبل استخدام أي مصدر بيانات كمصدر بيانات موثوق تُقيّم الشركة المصدر من حيث الموثوقية والدقة ومقاومة التعديل أو التزوير.

3.2.2.8 تأكيد الإصدار متعدد المنظور

يهدف "تأكيد الإصدار متعدد المنظور" إلى تعزيز صحة القرارات مثل نجاح أو فشل التحقق من النطاق، وصلاحيات أو قيود تخويل سلطة التصديقCAA المتخذة من "منظور الشبكة الرئيسي" عبر الاستعانة بمنظورات شبكية متعددة وعن بُعد قبل المباشرة بإصدار الشهادة.

تعتمد شركة (مصدر التكنولوجيا) مجموعات مختلفة من منظورات الشبكة عند إجراء التأكيد المتعدد للمتطلبات الآتية:

1. تخويل النطاق أو السيطرة عليه.
2. فحص سجلات تخويل سلطة التصديقCAA)).

توفر الاستجابات الواردة من منظورات الشبكة المعتمدة لـ (مصدر التكنولوجيا) المعلومات اللازمة لإجراء تقييم قطعي بشأن:

أ- وجود القيم المتوقعة: 1) القيمة العشوائية؛ 2) رمز الطلب 3) عنوان البروتوكولIP))4) عنوان الاتصال، وذلك حسب طريقة التحقق المعتمدة والمحددة في القسمين 3.2.2.4 و 3.2.2.5 من سياسة إجراءات التصديقCPS)).

ب- صلاحية (مصدر التكنولوجيا) في الإصدار للنطاقات المطلوبة، وفقاً لما ورد في القسم 3.2.2.8.

يُحظر إعادة استخدام أو تخزين النتائج والمعلومات المستحصلة من منظور شبكي واحد عند إجراء التحقق عبر منظورات لاحقة على سبيل المثال: لا يمكن للمنظورات المختلفة الاعتماد على ذاكرة تخزين مؤقت مشتركة لنظام أسماء النطاقات DNS، وذلك لمنع أي طرف معادي يسيطر على حركة البيانات من تسميم الذاكرة المستخدمة من قبل المنظورات الأخرى.

يجوز أن تُدار البنية التحتية للشبكة التي توفر الاتصال بالإنترنت لمنظور الشبكة من قبل ذات المؤسسة التي تقدم الخدمات الحسابية اللازمة لتشغيل ذلك المنظور. وتتم كافة الاتصالات بين (مصدر التكنولوجيا) ومنظورات الشبكة البعيدة عبر قنوات موثقة ومشفرة تعتمد بروتوكولات حديثة مثل .HTTPS.

يمكن لمنظور الشبكة استخدام محلل DNS تكراري غير موجود في نفس موقعه، بشرط أن يقع المحلل ضمن نفس منطقة خدمة سجل الإنترنت الإقليمي التابع لها ذلك المنظور. علاوة على ذلك، يجب ألا تقل المسافة الخطية بين أي زوج من محللات DNS المستخدمة في محاولة التأكيد المتعدد عن 500 كم.

يجوز لشركة (مصدر التكنولوجيا) إعادة محاولة التأكيد المتعدد فوراً باستخدام نفس طريقة التحقق أو طريقة بديلة. وعند الإعادة، يجب عدم الاعتماد على نتائج التأكيدات من المحاولات السابقة، ولا توجد قيود على عدد محاولات التحقق المسموح بها خلال أي فترة زمنية.

عدد منظورات الشبكة البعيدة والمتميزة المستخدمة	عدد حالات "عدم التأكيد" المسموح بها
2 - 5	1
6 فأكثر	2

تُعتبر منظورات الشبكة متميزة إذا كانت المسافة الخطية بينها لا تقل عن 500 كم، وتُعتبر "بعيدة" إذا كانت متميزة عن منظور الشبكة الرئيسي والمنظورات الأخرى الممثلة في النصاب.

يجوز لـ (مصدر التكنولوجيا) إعادة استخدام أدلة التأكيد للامتثال لنصاب سجلات (CAA) لمدة أقصاها 200 يوم. وبعد إصدار الشهادة للنطاق، يمكن للمنظورات البعيدة التغاضي عن جلب ومعالجة سجلات (CAA) لنفس النطاق أو نطاقاته الفرعية في الطلبات اللاحقة من نفس المتقدم لمدة تصل إلى 200 يوم كحد أقصى.

يجب على المنظورات البعيدة الاعتماد على شبكات (مثل مزودي خدمة الإنترنت أو شبكات مزودي السحاب) التي تطبق تدابير للحد من حوادث توجيه بروتوكول البوابة الحدودية (BGP) في نظام التوجيه العالمي.

بالنسبة لشهادات (TLS) الصادرة في أو بعد 15 آذار 2025، ستلزم (مصدر التكنولوجيا) إجراء التأكيد المتعدد باستخدام منظورين شبكيين بعيدين على الأقل، مع ضمان استيفاء كافة المتطلبات المذكورة في جدول النصاب، وفي حال عدم استيفائها، لن تباشر (مصدر التكنولوجيا) بإصدار الشهادة.

3.2.2.9 التحقق من الإصدار من وجهات نظر متعددة

تهدف آلية التحقق من الإصدار من وجهات نظر متعددة إلى تأكيد نتائج منظور الشبكة الرئيسي (مثل: نجاح/فشل التحقق من النطاق أو السماح أو الحظر بواسطة سجل CAAمن خلال وجهات نظر شبكية بعيدة متعددة قبل إصدار الشهادة.

تستخدم شركة مصدر التكنولوجيا مجموعات مختلفة من وجهات النظر الشبكية عند تنفيذ آلية التحقق من الإصدار من وجهات نظر متعددة وذلك للتحقق مما يلي:

1. تفويض النطاق أو السيطرة عليه.
2. فحوصات سجلاتCAA .

توفر مجموعة الاستجابات من وجهات النظر الشبكية المعتمدة المعلومات اللازمة التي تمكّن شركة مصدر التكنولوجيا من تقييم ما يلي:

- **أ.** وجود العناصر المتوقعة:
  1. القيمة العشوائية.
  2. رمز الطلب.
  3. عنوانIP .

4. عنوان جهة الاتصال
وفقاً لطريقة التحقق المعتمدة كما هو مذكور في القسمين 3.2.2.4 و3.2.2.5 من بيان ممارسة الشهادات هذا.

- **ب.** صلاحية شركة مصدر التكنولوجيا في إصدار الشهادة للنطاق (النطاقات) المطلوبة كما هو موضّح في القسم 3.2.2.8.

لا يُعاد استخدام أو تخزين النتائج أو المعلومات المُستحصلة من منظور شبكة واحد عند تنفيذ التحقق عبر وجهات نظر شبكية لاحقة (أي: لا يجوز أن تعتمد وجهات نظر مختلفة على ذاكرة DNS مؤقتة مشتركة وذلك لمنع الخصوم الذين يتحكمون بحركة المرور من أحد المناظير من تلويث ذاكرة DNS المؤقتة المستخدمة من قبل مناظير أخرى.

يجوز أن تُدار البنية التحتية للشبكة التي توفر الاتصال بالإنترنت لمنظور شبكة ما من قبل نفس الجهة التي توفر الخدمات الحاسوبية اللازمة لتشغيل منظور الشبكة.

تُجرى جميع الاتصالات بين منظور الشبكة البعيد وشركة مصدر التكنولوجيا عبر قناة مصادق عليها ومشفّرة تعتمد بروتوكولات حديثة مثل HTTPS :

يجوز لمنظور الشبكة استخدام مُحلل DNS تكراري لا يتواجد في نفس الموقع الجغرافي ولكن يجب أن يقع المُحلل المستخدم ضمن نفس منطقة خدمة سجل الإنترنت الإقليمي (RIR) الخاصة بمنظور الشبكة المعني.

علاوة على ذلك في أي محاولة للتحقق من الإصدار من وجهات نظر متعددة يجب أن تكون المسافة المستقيمة بين أي زوج من مُحللات DNS المستخدمة لا تقل عن 500 كم .وتُحدد موقع مُحلل DNS بالنقطة التي يتم فيها تسليم استعلامات DNS غير المغلّفة لأول مرة إلى البنية التحتية الشبكية التي توفر اتصال الإنترنت لذلك المُحلل.

يجوز لشركة مصدر التكنولوجيا إعادة تنفيذ آلية التحقق من الإصدار من وجهات نظر متعددة مباشرة باستخدام نفس طريقة التحقق أو بطريقة بديلة (مثل: يمكن لشركة مصدر التكنولوجيا إعادة المحاولة باستخدام البريد الإلكتروني إلى سجل TXTفيDNS إذا لم تؤكد طريقة التغيير المتفق عليه في الموقعACME – نتيجة التحقق.

وعند إعادة المحاولة لا يجوز الاعتماد على نتائج التحقق السابقة.
ولا يوجد حد أقصى لعدد محاولات التحقق التي يمكن تنفيذها خلال فترة زمنية معينة.

تصف جدول متطلبات النصاب القانوني متطلبات التحقق المشترك المتعلقة بآلية التحقق من الإصدار من وجهات نظر متعددة.
إذا لم تعتمد شركة مصدر التكنولوجيا على نفس مجموعة وجهات النظر الشبكية للتحقق من كل من تفويض/سيطرة النطاق وسجلاتCAA .

يجب استيفاء متطلبات النصاب القانوني لكل من مجموعتي وجهات النظر الشبكية أي: مجموعة تفويض/سيطرة النطاق ومجموعة التحقق من سجل .CAA تُعتبَر وجهات النظر الشبكية متميزة إذا كانت المسافة الخطية المباشرة بينها لا تقل عن 500 كم.

تُعتبر وجهات النظر الشبكية بعيدة إذا كانت متميزة عن منظور الشبكة الرئيسي وعن بقية وجهات النظر الشبكية الممثلة في النصاب القانوني.

يجوز لشركة مصدرالتكنولوجيا إعادة استخدام الأدلة المؤيدة للامتثال لنصاب التحقق من سجلات CAA لمدة أقصاها 200 يوماً.
وبعد إصدار شهادة لنطاق معين يجوز لوجهات النظر الشبكية البعيدة الامتناع عن استرجاع ومعالجة سجلات CAA لنفس النطاق أو نطاقاته الفرعية في طلبات الشهادات اللاحقة من نفس المتقدم بالطلب لمدة لا تتجاوز 200 يوماً.

جدول متطلبات النصاب القانوني

عدد وجهات النظر الشبكية البعيدة المتميزة المستخدمة	عدد حالات عدم التأييد المسموح بها
2- 5	1
+6	2

تكملة 3.2.2.9 التحقق من الإصدار من وجهات نظر متعددة.

يجب أن تعتمد وجهات النظر الشبكية البعيدة التي تُجري آلية التحقق من الإصدار من وجهات نظر متعددة على شبكات (مثل: مزودي خدمات الإنترنت أو شبكات مزودي الخدمات السحابية) تُنفذ تدابير للتخفيف من حوادث توجيه BGP في نظام التوجيه العالمي للإنترنت وذلك لضمان الاتصال الشبكي لمنظور الشبكة.

بالنسبة لشهادات TLS التي تُصدر في أو بعد 15 آذار 2025 تشترط شركة مصدر التكنولوجيا تنفيذ آلية التحقق من الإصدار من وجهات نظر متعددة باستخدام ما لا يقل عن اثنتين (2) من وجهات النظر الشبكية البعيدة.ويجب على شركة مصدر التكنولوجيا التأكد من استيفاء المتطلبات المحددة في جدول النصاب القانوني. إذا لم تُستوفَ هذه المتطلبات فلن تتابع شركة مصدر التكنولوجيا عملية إصدار الشهادة.

3.2.3 التحقق من هوية الأشخاص الطبيعيين

لا تُصدرهيئة التصديق هذه شهادات للأشخاص الطبيعيين وتقتصر إصداراتها على الشهادات الخاصة بالأشخاص الاعتباريين فقط.

3.2.4 معلومات المشترك غير المُتحقّق منها

تتحقق هيئة التسجيل (TS RA) من جميع الحقول التي تُشكّل معلومات المشترك والمُدرجة في الشهادة.

3.2.5 التحقق من السلطة

يُعيّن الممثل المفوض للمنظمة شخصاً ضمن المؤسسة ليكون مقدم طلب الشهادة (ممثل المتقدم بالطلب) وهو الذي يقدم طلبات إدارة الشهادات إلى هيئة التسجيل.(TS RA) "تتولى سلطة التسجيل (RA) التابعة لشركة مصدر التكنولوجيا (Technology Source) إجراءات التحقق من هوية مقدم الطلب، وارتباطه بالجهة المعنية، وصلاحية التفويض الممنوح له، وذلك من خلال تطبيق الخطوات التالية كحد أدنى:

- تتولى سلطة التسجيل (RA) التابعة لشركة مصدر التكنولوجيا إجراءات إثبات الهوية من خلال التحقق الشخصي (المباشر) من هوية مقدم الطلب بمطابقتها مع بطاقة الهوية الصادرة عن جهة حكومية؛ حيث يتوجب على مقدم الطلب تقديم أصل البطاقة (وليس نسخة منها).
- تتحقق سلطة التسجيل (RA) في شركة مصدر التكنولوجيا من طبيعة ارتباط مقدم الطلب بالجهة المعنية، وتصادق على صحة طلب إصدار الشهادة من خلال "التأكيد المباشر" مع الممثل المخول للجهة. ويتم ذلك عبر وسيلة اتصال موثوقة تشمل البريد الإلكتروني الرسمي للمؤسسة، ولشركة مصدر التكنولوجيا الحق في تنظيم اجتماع حضوري إذا رأت ذلك ضرورياً.
- يتم التحقق من صلاحية تفويض طلب الشهادات نيابة عن الجهة استناداً إلى "نموذج طلب الشهادة" الموقع من قبل كل من مقدم الطلب والممثل المخول، والذي يؤيد الصلاحية القانونية الممنوحة لمقدم الطلب.

تكملة 3.2.5 التحقق من السلطة.

- تُجري هيئة التسجيل (TS RA) تحققاً من الهوية من خلال مقابلة شخصية يتم فيها التحقق من هوية مقدم الطلب بمقارنة بياناته مع بطاقة هوية حكومية أصلية (وليس نسخة عنها) يُقدمها بنفسه.
- تستخدم هيئة التسجيل خطاب إثبات العمل المُقدَّم ضمن طلب الشهادة للتحقق من الصلة بين مقدم الطلب والجهة.
- تتحقق هيئة التسجيل من صحة طلب الشهادة وصحة خطاب الإثبات مباشرةً مع الممثل المفوض للجهة باستخدام وسيلة تواصل موثوقة تتضمن استخدام عناوين البريد الإلكتروني الخاصة بالجهة وعند الحاجة تُنظّم هيئة التسجيل اجتماعاً حضورياً.

تُثبت سلطة مقدم الطلب على تقديم طلبات الشهادات نيابةً عن الجهة من خلال نموذج طلب شهادة موقع من كل من مقدم الطلب والممثل المفوض يُؤكد فيه على امتلاك مقدم الطلب لهذه الصلاحية.

3.2.6 معايير التشغيل البيني

لا يوجد تنظيم خاص.

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

3.3.1 التحقق من الهوية والمصادقة لإعادة الإصدار الروتيني

يتم التحقق من الهوية والمصادقة عند إعادة إصدار المفتاح بنفس طريقة التسجيل الأولي بالإضافة إلى ما يلي:

- تتحقق بوابة هيئة التسجيل من وجود وصلاحية الشهادة المطلوب إعادة إصدارها وأن المعلومات المُستخدمة للتحقق من هوية وخصائص الموضوع لا تزال سارية.
- إذا طرأت أي تغييرات على الشروط والأحكام الخاصة بشركة مصدر التكنولوجيا تقوم هيئة التسجيل بإبلاغ المشترك بها.

3.3.2 التحقق من الهوية والمصادقة بعد إلغاء الشهادة Re-key بعد الإلغاء

تتطابق إجراءات التحقق من الهوية والمصادقة في حالة إعادة الإصدار بعد الإلغاء مع الإجراءات المُتبعة أثناء التسجيل الأولي.

3.4 التحقق من الهوية والمصادقة لطلب الإلغاء

تشمل إجراءات التحقق من الهوية والمصادقة في طلبات الإلغاء تقديم طلب رسمي من الممثل المفوض للجهة التي أُصدرت لها الشهادة.
وتُطبّق هيئة التسجيل (TS RA) إجراءً رسمياً للإلغاء يتضمن ما يلي:

- توقيع نموذج طلب الإلغاء من قبل ممثل مفوض يتمتع بالصلاحية المناسبة.
- التحقق من هوية مقدمي الطلبات من خلال مقارنة بياناتهم مع المعلومات المتوفرة لدى هيئة التسجيل (TS RA) والتي جرى تقديمها أثناء تسجيل المشترك.
- التواصل مع الجهة المعنية لتوفير ضمانات معقولة تفيد بأن ممثل الجهة الرسمي هو من فوّض عملية الإلغاء.
ويجري هذا التواصل بحسب الظروف باستخدام وسيلة أو أكثر من وسائل الاتصال الموثوقة مثل الهاتف أو البريد الإلكتروني أو خدمات البريد السريع.

بالنسبة لشهادة مستجيبOCSP :

لا يُحدّد بيان ممارسة الشهادات الحالي (CPS) أحكاماً تفصيلية لإلغاء أي من هذه الشهادات. وقد يُحرَّك إجراء الإلغاء في حال اختراق أو الاشتباه باختراق المفاتيح الخاصة المرتبطة وتُعدّ هذه الحالة كارثية وتُعالَج على هذا الأساس وفقاً لخطة استمرارية الأعمال والتعافي من الكوارث الخاصة بشركة مصدر التكنولوجيا.

4 متطلبات تشغيل دورة حياة الشهادة

4.1 طلب الشهادة

4.1.1 من يمكنه تقديم طلب شهادة

يمكن لمقدم طلب الشهادة المخوّل (أي ممثل المتقدم بالطلب) تقديم طلبات الشهادات نيابةً عن المؤسسة أو الجهة.
ويتحمّل مقدم الطلب مسؤولية دقة المعلومات المقدَّمة كجزء من طلب الشهادة .تتأكد هيئة التسجيل (TS RA) من أن الممثل الرسمي للجهة يوافق على طلب الشهادة من خلال التوقيع والختم على نموذج طلب الشهادة والشروط والأحكام المرفقة الخاصة بالمشترك.

لا تُصدر شركة مصدر التكنولوجيا شهادات للجهات المدرجة في القائمة السوداء الداخلية الخاصة بها والتي تتضمن المنظمات التي لا تُقبل منها طلبات الشهادات .ويتحقق فريق TS RA من هذه القائمة عند استلام أي طلب شهادة.

بالنسبة لشهادة مستجيبOCSP :

تُشرف هيئة التسجيل (TS RA) وأحد مديري البنية التحتية للمفتاح العام المخولين (في دور موثوق) على تنفيذ إجراءات تشغيلية داخلية يتم من خلالها إصدار هذه الشهادات. ويُشركان مجلس حوكمة البنية التحتية للمفتاح العام (TS PKI GB) للموافقة على وثائق المراسيم التشغيلية وللتحقق من قوالب الشهادات المضمّنة واتفاقيات التسمية مقابل أحكام بيان ممارسة الشهادات.(CPS) ويُصرّح مجلس TS PKI GB بالمراسيم التشغيلية ويؤكد قائمة الأفراد المشاركين في الأدوار الموثوقة.

4.1.2 عملية التسجيل والمسؤوليات

تشترط هيئات التصديق (CAs) على كل متقدم بالطلب تقديم نموذج طلب شهادة ومعلومات التسجيل قبل إصدار الشهادة.
وتقوم هيئة التسجيل (TS RA) بالمصادقة على جميع الاتصالات الواردة من المتقدم بالطلب وتضمن تعبئة وتوقيع نموذج الطلب حسب المطلوب.

- يقوم المتقدم بالطلب بتنزيل نموذج طلب الشهادة وشروط وأحكام المشترك من المستودع العام.
- يُملأ نموذج طلب الشهادة ويُوقَّع من قبل الممثل المفوض للجهة (وكذلك يجب المصادقة على شروط وأحكام المشترك).
- يُنشئ الفريق الفني المعني من الجهة زوج مفاتيح وفقاً لمتطلبات بيان ممارسة الشهادات هذا (CPS) ثم يُنشئ طلب توقيع الشهادة (CSR) باستخدام الحقول المعتمدة في نموذج الطلب مثل: سمات DN حجم المفتح نوع المفتاح إلخ .ويُسلَّم هذا الطلب إلى مقدم طلب الشهادة المفوض.
- يقوم مقدم الطلب بالمصادقة على بوابة التسجيل الإلكتروني (Web RA Portal) باستخدام بيانات المصادقة متعددة العوامل التي جرى إعدادها أثناء عملية التسجيل كما هو موضح في وثيقة الإجراءات الداخلية لهيئة التسجيل ويقدِّم طلب الشهادة متضمناً ما يلي:

تكملة 4.1.2 عملية التسجيل والمسؤوليات.

- نسخة ممسوحة ضوئياً من نموذج الطلب المعبأ والموقع حسب الأصول.
- المعلومات والمستندات المطلوبة للتحقق من الهوية والتفويض المرتبط بالطلب.

- ملف طلب توقيع الشهادة(CSR) .

يتطلب إصدار شهادة TLS مشاركة اثنين (02) من أعضاء فريق هيئة التسجيل(TS RA) :

- يُراجع فريق TS RA جميع المستندات المقدمة ويتحقق من سلامتها وأصالتها بالإضافة إلى التحقق من هوية المتقدم كما هو موضح في القسم 3.2.2.
- يتحقق فريق TS RA من القائمة السوداء للمنظمات التي لا تُقبل منها طلبات الشهادات. ويتم الاستعلام عن هذه القائمة عند استلام أي طلب شهادة.
- يُعالج فريق TS RA طلب الشهادة. راجع القسم 4.2.

بالنسبة لشهادة مستجيبOCSP :

تُشرف هيئة التسجيل (TS RA) وأحد مديري البنية التحتية للمفتاح العام المخولين (في دور موثوق) على تنفيذ الإجراءات التشغيلية التي تُصدر من خلالها هذه الشهادات .يوافق مجلس حوكمة البنية التحتية للمفتاح العام (TS PKI GB) على وثائق المراسيم التشغيلية ويتحقق من تطابق قالب الشهادة المُضمّن واتفاقيات التسمية مع أحكام بيان ممارسة الشهادات (CPS).ثم يُصرّح مجلس TS PKI GB بإجراء المراسيم ويُؤكد قائمة الأفراد المشاركين في الأدوار الموثوقة.

4.2 معالجة طلب الشهادة

4.2.1 تنفيذ وظائف التحقق من الهوية والمصادقة

المتطلبات المطبقة على جميع طلبات الشهادات:

يُخصص معرّف فريد لكل سجل طلب شهادة تُسجل هيئة التسجيل (TS RA) جميع الأنشطة (مثل: المراسلات البريدية المكالمات الهاتفية أدلة التحقق ضمن سجل طلب الشهادة يُضاف أي طلب شهادة خبيث أو طلب إلغاء خبيث أو طلب فشل في التحقق أكثر من ثلاث مرات إلى القائمة السوداء الداخلية لهيئة التسجيل وتتضمن هذه القائمة تفاصيل كافية لتفادي الغموض في التعرف على الطلبات الخبيثة المستقبلية تُجري هيئة التسجيل فحصاً على قائمتها السوداء الخاصة. وإذا كان المتقدم بالطلب مدرجاً ضمنها يُرفض طلب الشهادة.

المتطلبات المطبقة على طلبات شهاداتTLS :

تُرسل هيئة التسجيل إلى المتقدم بالطلب المعلومات اللازمة بما في ذلك المستندات المطلوبة للتحقق من الهوية وشروط وأحكام المشترك بمجرد بدء تقديم الطلب من قبل الجهة المتقدمة يملأ مقدم الطلب نموذج تسجيل الجهة كما يلي:

أ. معلومات الجهة:
الاسم القانوني للجهة
العنوان الرسمي
رقم الهاتف الرئيسي.

ب. معلومات الممثلين المفوضين:
معلومات ممثل مقدم الطلب مثل: رقم الهاتف البريد الإلكتروني الرسمي المنصب.

ج. معلومات مقدم الطلب:
الاسم ومعلومات الاتصال الخاصة بمقدم الطلب (الممثل المفوض لتقديم طلبات إدارة الشهادات نيابةً عن الجهة).

ت. يُوقّع ممثل المتقدم بالطلب على شروط وأحكام المشترك المخصصة ويصادق عليها.

ث. يُصدر قسم الموارد البشرية لدى الجهة خطاب إثبات يوضح العلاقة بين مقدم الطلب والجهة.

د. يُرسل مقدم الطلب نموذج التسجيل الموقع وخطاب الإثبات بالإضافة إلى مستندات التحقق الأخرى إلى هيئة التسجيل.

(TS RA) عبر البريد الإلكتروني.

ذ. تُجري هيئة التسجيل التحققات التالية لكل طلب شهادة دون الاعتماد على أي تحقق حصل مسبقاً:

- التحقق من هوية الجهة كما هو موضح في القسم 3.2.2.1.
- التحقق من الممثل المفوض للجهة كما هو موضح في القسم 3.2.2.1.
- التحقق من تفويض مقدم طلب الشهادة كما هو موضح في القسم 3.2.5.
- التحقق من رقم هاتف الجهة من خلال إجراء مكالمة عشوائية.

إذا اجتازت جميع التحققات أعلاه تُطلق هيئة التسجيل عملية عبر بوابة التسجيل الإلكتروني (Web RA Portal) يتم من خلالها تسجيل الجهة ومقدم الطلب على البوابة بناءً على المعلومات التي جُمعت. وبذلك يصبح مقدم الطلب قادراً على تسجيل الدخول إلى البوابة وتقديم طلبات الشهادات نيابةً عن الجهة.

بمجرد تقديم طلب الشهادة يمكن لهيئة التسجيل متابعة الإجراءات على النحو التالي:

ز. التحقق من ملكية أسماء النطاق أو عناوين IP وفقاً لما ورد في القسمين 3.2.2.4 و3.2.2.5 من هذا البيان.

ر. تأكيد نتائج التحقق من النطاق عبر وجهات نظر شبكية متعددة وفقاً لما ورد في القسم 3.2.2.9.

ص. التحقق من تنسيق اسم التميز (DN) للموضوع (الوارد في ملف CSR والتأكد مما يلي:

- أن حقل اسم الجهة يطابق تماماً اسم الجهة كما سجل من قبل هيئة التسجيلTS RA)).
- أن تحتوي إضافة SubjectAltName في الشهادة على اسم نطاق مؤهل بالكامل (FQDN) واحد على الأقل أو عنوان IP واحد على الأقل.

ض. في حالة شهادات النطاقات العامةWildcard)) إجراء تحقق من صحة نطاقات Wildcard وفقاً لما ورد في القسم 3.2.2.6 من هذا البيان.

ن. التحقق من صحة امتداد النطاق العلوي (TLD) لكل نطاق مدرج في طلب الشهادة على أن يكون IQ. على الأقل وذلك عبر الخطوات التالية:

- التحقق من صلاحية TLD بمقارنة النطاق مع القوائم المنشورة من قبل IANA الخاصة بـ TLD و gTLDعلى الرابط التالي:
  .(https://data.iana.org/TLD/tlds-alpha-by-domain.txt)
- التحقق من سجلات CAA للنطاق كما هو موضح في القسم 3.2.2.8 من هذا البيان.
- تأكيد نتائج فحوصات CAA عبر وجهات نظر شبكية متعددة وفقاً لما ورد في القسمين 3.2.2.8 و3.2.2.9.

لا يُشترط إعادة التحقق من هوية المتقدم بالطلب في حال تقديم طلبات إعادة إصدار المفتاحRe-key)) شرط أن تظل الأدلة المقدمة مسبقاً للتحقق من الهوية صالحة وقابلة للتطبيق .ومع ذلك لا يجوز إعادة استخدام البيانات التي حقق منها مسبقاً لأكثر من ثلاثمائة وخمس وستون (365) يوماً. وبعد انقضاء هذه المدة يجب إعادة التحقق منها كما لو أنها تسجيل أولي.

بالنسبة لشهادة مستجيبOCSP :

تُشرف هيئة التسجيل (TS RA) وأحد مديري البنية التحتية للمفتاح العام المخولين (في دور موثوق) على تنفيذ مراسيم تشغيلية داخلية تُصدر من خلالها هذه الشهادات .يوافق مجلس حوكمة البنية التحتية للمفتاح العام (TS PKI GB) على وثائق المراسيم ويتحقق من صحة قوالب الشهادات المضمّنة واتفاقيات التسمية بما يتوافق مع أحكام بيان ممارسة الشهادات هذا .ثم يُصرّح مجلس TS PKI GB بإجراء المراسيم ويُحدد قائمة الأفراد الموثوقين المشاركين فيها .وتُنفذ المراسيم تحت إشراف هيئة التسجيل التي تُراجع طلب توقيع الشهادة (CSR) قبل معالجته من قبل هيئة التصديقCA)).

4.2.2 الموافقة أو رفض طلبات الشهادات

تخضع موافقة هيئة التسجيل (TS RA) على طلب الشهادة لما يلي:

- التحقق الناجح من الهوية والمصادقة على جميع معلومات المشترك المطلوبة وفقاً للقسم 3.2.2.
- التحقق من ملكية النطاق أو عنوانIP .
- إثبات الارتباط بين الجهة المقدِّمة للطلب والكيان الذي ستُصدر له الشهادة.
- إثبات حيازة المفتاح الخاص.
- التحقق من هوية وتفويض مقدم الطلب.

تقادم البيانات التي تمت المصادقة عليها (Age of Validated Data).

يجوز لـ سلطة التسجيل (RA) التابعة لشركة مصدر التكنولوجيا إعادة استخدام عمليات التحقق المكتملة و/أو الأدلة الثبوتية التي تم إجراؤها وفقاً للقسم (3.2) ضمن الحدود التالية:

- بيانات التحقق من اسم النطاق (Domain Name) وعنوان البروتوكول (200) :(IP Address) يوم كحد أقصى قبل تاريخ إصدار الشهادة.
- المصادقة على هوية المؤسسة (365) :(Organization Identity) يوماً كحد أقصى قبل تاريخ إصدار الشهادة.

ملاحظة :لا تمنح سلطة التصديق (CA) هذه شهادات (SSL) موثوقة علنياً لأسماء الخوادم الداخلية أو عناوين الـ (IP) المحجوزة.

4.2.2.1 سجلات تصريح جهة إصدار الشهادة(CAA Records)

يُعد سجل (CAA) سجلاً خاصاً في نظام أسماء النطاقات (DNS) يمكن لمالك النطاق تكوينه لتحديد جهة التصديق (CA) المخولة بإصدار الشهادات لذلك النطاق.

- بالنسبة لكل نطاق مدرج في ملحق "الاسم البديل للموضوع subjectAltName) ")، يقوم موظف سلطة التسجيل (أو نظام التحقق الآلي) بالتأكد من وجود سجل (CAA) وفقاً للمعيار8659 RFC)).

- تقوم سلطة التسجيل في شركة مصدر التكنولوجيا بمعالجة وسوم الخاصية (issue) و(issuewild) للتأكد من تضمنها للقيمة"pki.techsource.iq" .
- يتم إصدار الشهادات التي تجتاز فحص الـ (CAA) خلال "فترة صلاحية البقاء (TTL) "الخاصة بسجل الCAA))، أو خلال (8) ساعات، أيهما أطول.
- لا تتخذ شركة مصدر التكنولوجيا أي إجراء بناءً على وسم الخاصية (iodef)؛ أي أنها لا تستخدم هذا الوسم للتواصل مع جهات الاتصال المدرجة في سجل(CAA) .

التدقيق وفق بروتوكول (DNSSEC).

في الحالات التي تكون فيها منطقة (DNS) المحتوية على سجل (CAA) موقعة برمجياً باستخدام (DNSSEC)، يجب على موظف سلطة التسجيل (أو نظام التحقق) إجراء مصادقة (DNSSEC) على استجابة الـ (DNS) قبل اتخاذ أي إجراء بشأن سجلCAA))، ويُحظر إصدار الشهادة في حال فشل مصادقة (DNSSEC) أو إذا تبين وجود خلل في "سلسلة الثقة " .(Chain of Trust)تلتزم شركة مصدر التكنولوجيا بعدم تعطيل أو تجاوز مصادقة (DNSSEC) لأي استعلام متعلق بسجل (CAA) عند وجود تواقيع رقمية.

منظورات الشبكة والتحقق عن بُعد.

قد تتطلب بعض طرق التحقق من سيطرة مقدم الطلب على النطاق (القسم 3.2.2.4) أو عنوان الـ (IP) (القسم 3.2.2.5) قيام جهة التصديق بفحص سجلات (CAA) من منظور الشبكة الأساسي، ومن منظورات شبكة بعيدة إضافية إذا لزم الأمر قبل الإصدار. تُستخدم الفحوصات البعيدة لتأكيد الفحص الأساسي، ويجوز للشركة إصدار الشهادة حتى لو اختلفت الاستجابة البعيدة عن الأساسية، طالما أن جهة التصديق المقصودة (المدرجة كـ pki.techsource.iq) مخولة بذلك.

يجوز لشركة مصدر التكنولوجيا اعتبار فشل البحث في السجلات بمثابة إذن بالإصدار فقط في الحالات التالية:

1. إذا كان الفشل ناتجاً عن خلل خارج البنية التحتية لشركة مصدر التكنولوجيا.
2. إذا تمت إعادة محاولة البحث لمرة واحدة على الأقل.
3. إذا أكدت الشركة أن النطاق "غير آمن (Insecure) "وفقاً للمعيار4035 RFC القسم 4.3.

يتم تسجيل كافة الإجراءات المتعلقة بفحص ومعالجة سجلات (CAA) برمجياً، كما يتم توثيق أي حالات منع إصدار ناتجة عن هذه السجلات، مع توفير تفاصيل كافية لمشاركتها مع منتدى (CA/Browser Forum) عند الضرورة.

لا تُصدر هيئة التصديق هذه شهادات SSL موثوقة علنياً إلى أسماء خوادم داخلية أو عناوين IP محجوزة.

4.2.3 مدة معالجة طلبات الشهادات

لا يوجد تنظيم خاص.

4.3 إصدار الشهادة

4.3.1 إجراءات هيئة التصديق أثناء إصدار الشهادة

بعد الانتهاء من جميع خطوات التحقق كما هو موضح في القسم 4.2.1 يستخدم فريق هيئة التسجيل (TS RA) بوابة التسجيل الإلكتروني لبدء عملية إصدار الشهادة من قِبل هيئة التصديقCA)) استناداً إلى ملف طلب توقيع الشهادة (CSR) المقدم من المتقدم بالطلب.

تقوم هيئة التصديق بالتحقق من تنسيق وبنية ملف CSR وتُنشئ شهادة أولية .تخضع هذه الشهادة الأولية لعملية تحليل فني باستخدام أدوات تدقيق معيارية على مستوى الصناعة للتحقق من توافقها الفني مع المعايير المعتمدة لكل عنصر سيتم توقيعه.

بعد اجتياز التحقق بنجاح تُولَّد الشهادة النهائية وفقاً لقالب الشهادة المُهيأ مسبقاً وتُتاح للمشترك لتحميلها من بوابة التسجيل الإلكتروني.
تصدر هيئة التصديق الشهادة في حالة فعالة .

بالنسبة لشهادة مستجيب :OCSP
تُجرى عملية إصدار هذه الشهادات وإدارتها ضمن مراسيم تشغيلية يتم الموافقة عليها من قِبل عضوين على الأقل من مجلس حوكمة البنية التحتية للمفتاح العام .(TS PKI GB) وتشمل هذه الموافقات ما يلي:

1. الترخيص بتنفيذ المراسيم.
2. المصادقة على قائمة الحضور في المراسيم والتي تشمل هيئة التسجيل وأحد أعضاء إدارة عملياتTS PKI ومديرين معينين من فريق عملياتTS PKI .
3. التحقق من قوالب الشهادات المُضمّنة واتفاقيات التسمية وتطابقها مع أحكام بيان ممارسة الشهادات.

4.3.2 إشعار المشترك بإصدار الشهادة من قبل هيئة التصديق
تُتاح الشهادة للمشترك لتحميلها من حسابه على بوابة التسجيل الإلكترونيWeb RA Portal))).

4.4 قبول الشهادة

4.5 السلوك الذي يُعد قبولاً للشهادة
يقوم مقدم الطلب بتحميل الشهادة من بوابة التسجيل الإلكتروني ثم يُجري تحققاً من محتواها بمقارنتها مع طلب الشهادةCSR.

وفي حال وجود أي اختلافات يُبادر مقدم الطلب بالتواصل مع هيئة التسجيلTS RA))وقد يؤدي ذلك إلى إلغاء الشهادة وإصدار شهادة مصححة بديلة.

4.6 تجديد الشهادة
غير قابل للتطبيق.

4.6.1 الظروف التي تستدعي تجديد الشهادة
غير قابل للتطبيق.

4.6.2 من يمكنه طلب التجديد
غير قابل للتطبيق.

4.6.3 معالجة طلبات تجديد الشهادة
غير قابل للتطبيق.

4.6.4 إشعار المشترك بإصدار شهادة جديدة
غير قابل للتطبيق.

4.6.5 التصرف الذي يُعد قبولاً لشهادة جددت
غير قابل للتطبيق.

4.6.6 نشر شهادة التجديد من قبل هيئة التصديق
غير قابل للتطبيق.

4.6.7 إشعار هيئة التصديق بعملية الإصدار لجهات أخرى
غير قابل للتطبيق.

4.7 إعادة إصدار الشهادة(Re-key)
تشير إعادة إصدار الشهادة إلى عملية إصدار شهادة جديدة للمشترك باستخدام مفتاح عام جديد وفترة صلاحية جديدة مع إمكانية بقاء باقي معلومات الشهادة كما هي.

تدعم هيئة التصديق هذه عملية إعادة إصدار الشهادة. وتتطابق إجراءات إعادة الإصدار (بما في ذلك التحقق من الهوية وإصدار الشهادة والتواصل مع الأطراف ذات الصلة) مع إجراءات إصدار الشهادة الأولية.

4.7.1 الظروف التي تستدعي إعادة إصدار الشهادة
قد تتم إعادة إصدار الشهادة أثناء فترة صلاحيتها أو بعد انتهاء صلاحيتها أو بعد إبطالها. وقد تؤدي عملية إعادة الإصدار إلى إبطال أي شهادات SSL نشطة حالياً.

4.7.2 من يمكنه طلب اعتماد مفتاح عام جديد
وفقاً لإجراءات إصدار الشهادة الأولية.

4.7.3 معالجة طلبات إعادة إصدار الشهادة
وفقاً لإجراءات إصدار الشهادة الأولية.

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

4.7.5 التصرف الذي يُعد قبولاً لشهادة أعيد إصدارها
وفقاً لإجراءات إصدار الشهادة الأولية.

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

4.7.7 إشعار هيئة التصديق بعملية الإصدار لجهات أخرى
وفقاً لإجراءات إصدار الشهادة الأولية.

4.8 تعديل الشهادة

4.8.1 الظروف التي تستدعي تعديل الشهادة
غير قابل للتطبيق.

4.8.2 من يمكنه طلب تعديل الشهادة
غير قابل للتطبيق.

4.8.3 معالجة طلبات تعديل الشهادة
غير قابل للتطبيق.

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

4.8.5 التصرف الذي يُعد قبولاً لشهادة معدلة
غير قابل للتطبيق.

4.8.6 نشر الشهادة المعدلة من قبل هيئة التصديق
وفقاً لإجراءات إصدار الشهادة الأولية.

4.8.7 إشعار هيئة التصديق بعملية الإصدار لجهات أخرى
وفقاً لإجراءات إصدار الشهادة الأولية.

4.9 إبطال وتعليق الشهادة

تُوفّر شركة مصدر التكنولوجيا إمكانية مستمرة للمشتركين لتقديم طلبات الشهادات وذلك من خلال نظام إلكتروني متاح على مدار الساعة طوال أيام الأسبوع للمشتركين المُصادق عليهم.

يُحظر تعليق الشهادات. ويُسمح فقط بإبطال الشهادات بشكل دائم.

تتم معالجة إبطال شهادات المشتركين وفقاً للفقرات الفرعية التالية.

4.9.1 الظروف التي تستدعي الإبطال
لا تدعم هيئة التصديق هذه إبطال الشهادات قصيرة الأجل الخاصة بالمشتركين.

باستثناء شهادات المشتركين قصيرة الأجل تبادر هيئة التصديق هذه إلى إلغاء الشهادة خلال مدة لا تتجاوز 24 ساعة وتُرفق سبب الإبطال المناسب في حال وقوع أحد الأمور التالية:

1. قدّم المشترك طلباً خطياً لإلغاء الشهادة دون تحديد سبب للإبطال مما يستدعي استخدام رمز السبب غير محدد (0) ولا تُدرج حينها الامتداد في قائمة إبطال الشهاداتCRL)).
2. أخطر المشترك هيئة التصديق بأن طلب الشهادة الأصلي لم يكن مُصرّحاً به ولم يمنح الإذن بأثر رجعي (رمز السبب #9 سحب الامتياز.

3. حصلت هيئة التصديق على دليل معقول يُثبت أنّ المفتاح الخاص للمشترك المرتبط بالمفتاح العام الوارد في الشهادة قد تعرض للاختراق (رمز السبب #1 اختراق المفتاح keyCompromise .
4. حصلت هيئة التصديق على دليل بأنّ تحقق ملكية أو صلاحية التحكم في اسم النطاق المؤهل بالكامل (FQDN) أو عنوان IP المضمن في الشهادة لم يعد صالحاً (رمز السبب #4 الاستبدالsuperseded).
5. علمت هيئة التصديق بوجود طريقة مثبتة أو مجربة يمكن من خلالها حساب المفتاح الخاص للمشترك بسهولة استناداً إلى المفتاح العام في الشهادة (مثل مفاتيح Debian الضعيفة راجع : https://wiki.debian.org/SSLkeys)رمز السبب #1 اختراق المفتاح keyCompromise .

باستثناء شهادات المشتركين قصيرة الأجل يجوز لهيئة التصديق أيضاً إلغاء الشهادة خلال مدة لا تتجاوز 24 ساعة مع استخدام سبب الإبطال المناسب في حال تحقق أحد الأمور التالية:

1. الحصول على دليل يفيد بعدم امتثال الشهادة لمتطلبات الفقرتين 6.1.5 و6.1.6 (رمز السبب #4 الاستبدال superseded).
2. الحصول على دليل على سوء استخدام الشهادة رمز السبب #9 سحب الامتياز.

3. علم هيئة التصديق بأنّ المشترك قد خالف واحداً أو أكثر من التزاماته الجوهرية بموجب شروط وأحكام المشترك (رمز السبب #9 سحب الامتياز.

4. وجود ظرف يشير إلى أنّ استخدام اسم النطاق المؤهل بالكامل أو عنوان IP الوارد في الشهادة لم يعد مسموحاً به قانوناً (مثلاً صدور حكم قضائي أو قرار تحكيمي يُلغي حق المُسجِّل في استخدام اسم النطاق أو انتهاء صلاحية اتفاقية الترخيص أو الخدمات بين المُسجِّل ومقدم الطلب أو فشل المُسجِّل في تجديد اسم النطاق) (رمز السبب #5 التوقف عن التشغيل).

5. علم هيئة التصديق بأنّ شهادة النطاق العام استُخدمت لمصادقة اسم نطاق مؤهل بالكامل زائف أو مضلل (رمز السبب #9 سحب الامتياز.

6. إبلاغ هيئة التصديق بحدوث تغيير جوهري في المعلومات الواردة في الشهادة (رمز السبب #9 سحب الامتياز).

7. اكتشاف أنّ الشهادة قد صدرت بطريقة لا تتوافق مع إجراءات بيان ممارسة الشهادات (CPS) أو مع متطلبات الأساس (رمز السبب #4 الاستبدال).

8. علم هيئة التصديق بأنّ أية معلومات واردة في الشهادة غير دقيقة (رمز السبب #9 سحب الامتياز.

9. انتهاء صلاحية حق هيئة التصديق في إصدار الشهادات بموجب متطلبات الأساس أو إلغاؤه أو إنهاؤه ما لم تكن هيئة التصديق قد خططت مسبقاً للاستمرار في صيانة مستودع CRL/OCSP (رمز السبب غير محدد (0) مما يعني عدم إدراج امتداد في قائمة الإلغاء).

10. إذا تطلب بيان ممارسة الشهادات (CPS) الإبطال لأسباب لا تستوجب الذكر في هذه الفقرة 4.9.1 رمز السبب غير محدد (0) مما يعني عدم إدراج امتداد في قائمة الإلغاء.

11. اكتشاف وجود طريقة مثبتة أو مجربة تؤدي إلى اختراق المفتاح الخاص للمشترك أو وجود دليل واضح على أن الطريقة المستخدمة لإنشاء المفتاح الخاص كانت معيبة (رمز السبب #1 اختراق المفتاح).

4.9.1.1 الظروف التي تستدعي إبطال شهادة هيئة تصديق تابعة

تُبطل شهادة هيئة التصديق التابعة TS TLS CA خلال مدة لا تتجاوز سبعة (7) أيام إذا وقع أحد الأمور التالية:

1. تقديم طلب الإبطال كتابياً.
2. أخطرت شركة مصدر التكنولوجيا هيئة التصديق المُصدرة (أي الهيئة الجذرية) بأن طلب الشهادة الأصلي لم يكن مصرحاً به ولم تمنح الإذن بأثر رجعي.

3. حصلت شركة مصدر التكنولوجيا على دليل يُثبت أنّ المفتاح الخاص لهيئة التصديق المرتبط بالمفتاح العام في الشهادة قد تعرّض للاختراق أو لم يعد متوافقاً مع متطلبات الفقرتين 6.1.5 و6.1.6.

4. حصلت هيئة التصديق المُصدرة (أي الهيئة الجذرية) على دليل يُثبت أنّ شهادة هيئة التصديق قد أُسيء استخدامها.

5. علمت هيئة التصديق المُصدرة (أي الهيئة الجذرية) أنّ شهادة هيئة التصديق لم تُصدر وفقاً لهذا المستند أو أنّ TS TLS CAلم تلتزم بمضمونه.

6. قررت هيئة التصديق المُصدرة (أي الهيئة الجذرية) أنّ أية معلومات واردة في الشهادة غير دقيقة أو مضللة.

7. توقفت TS TLS CA عن العمل لأي سبب كان ولم تضع ترتيبات بديلة مع هيئة تصديق أخرى لتوفير دعم الإبطال للشهادة.

8. انتهى حق TS TLS CA في إصدار الشهادات بموجب هذه المتطلبات أو جرى إلغاؤه أو إنهاؤه ما لم تكن الهيئة الجذرية قد رتبت للاستمرار في صيانة مستودعCRL/OCSP .

9. تطلبت سياسة شهادة الهيئة المُصدرة وبيان ممارسة الشهادات (CPS) إلغاء الشهادة.

4.9.2 من يمكنه طلب الإبطال

يجوز للجهات التالية تقديم طلبات إلغاء الشهادة:

- هيئة التسجيل TS RA في الحالات الموضحة في الفقرة 4.9.1.
- يجوز للمشترك تقديم طلب إبطال لشهادته الخاصة.
- شركة مصدر التكنولوجيا من تلقاء نفسها (على سبيل المثال في حال تأكد وجود اختراق لمفتاح هيئة التصديق).
- يمكن للمشتركين والأطراف المعتمدة وموردي برمجيات التطبيقات وأطراف ثالثة أخرى تقديم تقارير بمشكلات الشهادات لإخطار مصدر التكنولوجيا بوجود سبب معقول يستدعي بدء عملية إلغاء الشهادة.

4.9.3 إجراءات طلب الإبطال

تُنفذ عملية إبطال الشهادات كما يلي:

- يُخصّص فريق هيئة التسجيل TS RA رقماً تعريفياً فريداً لطلب الإبطال ويُسجّل المستندات المقدمة تحت هذا الرقم.
- يتحقق فريق TS RA من هوية مقدم الطلب وفقاً لما ورد في الفقرة 3.4.
- يتحقق فريق TS RA من معلومات الشهادة الواردة في نموذج طلب الإبطال.

- يُجري فريق TS RA التحقيقات اللازمة ضمن الحدود الزمنية المحددة (وفقاً لما هو مذكور في الفقرة 4.9.1 من بيان ممارسة الشهاداتCPS) وقد يتضمن ذلك التواصل مع المشترك صاحب الشهادة.
- ينفّذ فريق هيئة التسجيل عملية إلغاء الشهادة.
- تُبطل هيئة التصديق الشهادة ويتم تحديث حالة الشهادة وفقاً لذلك.
- تُرسل هيئة التسجيل TS RA إشعاراً عبر البريد الإلكتروني إلى المشترك أو الجهة التي طلبت الإبطال لتأكيد إتمام عملية إلغاء الشهادة.
- تُحدث هيئة التسجيل قائمتها السوداء الداخلية بمعلومات الشهادة المُبطلة بما في ذلك ظروف الإبطال وقد تُعدل بناءً على هذه المعلومات مستوى المخاطر المرتبط بمقدم الطلب ضمن القائمة السوداء. وتُستخدم هذه المعلومات لاحقاً من قبل هيئة التسجيل عند معالجة أي طلبات شهادات مستقبلية لهذا المتقدم.

معالجة هيئة التسجيل TS RA لإلغاء الشهادة بعد تلقي تقرير بمشكلة في الشهادة.

يجوز للمشتركين والأطراف المعتمدة وموردي برمجيات التطبيقات وأطراف ثالثة أخرى تقديم تقارير بمشكلات الشهادات عبر البريد الإلكتروني التالي:
certificate.problem@techsource.iq.

يُطلب من مُرسل التقرير تضمين معلومات الاتصال الخاصة به ووصف حالة الإساءة المشتبه بها وموضوع الشهادة ذات الصلة.

تبدأ هيئة التسجيل TS RA التحقيق في تقرير مشكلة الشهادة خلال 24 ساعة من استلامه وتقرر ما إذا كان الإبطال أو اتخاذ إجراء آخر مناسب مطلوباً بناءً على المعايير التالية على الأقل:

- طبيعة المشكلة المُبلغ عنها.
- عدد التقارير المستلمة بشأن شهادة أو موضوع معين.
- هوية الجهة المبلّغة (على سبيل المثال إشعار صادر عن جهة مكافحة البرمجيات الخبيثة أو جهة إنفاذ القانون يُعد أكثر موثوقية من بلاغ مجهول المصدر).
- التشريعات المحلية ذات الصلة.

في حال تقرر إلغاء الشهادة نتيجة تقرير بمشكلة تنفذ هيئة التسجيل إجراءات الإبطال كما ورد سابقاً في هذا القسم.

وإذا رأت شركة مصدر التكنولوجيا أنّ الأمر يستدعي ذلك فقد تُحيل تقارير الإبطال إلى جهات إنفاذ القانون.

تحتفظ شركة مصدر التكنولوجيا بقدرة داخلية دائمة للاستجابة على مدار الساعة طوال أيام الأسبوع لطلبات الإبطال العاجلة وتقارير مشكلات الشهادات. كما توفر تعليمات حول إبطال الشهادات وتقديم تقارير المشكلات في صفحة مخصصة ضمن المستودع العام على الرابط التالي:
https://pki.techsource.iq/repository/en/Certificate_Problem_Report.html.

4.9.4 فترة السماح لطلب الإبطال

لا توجد فترة سماح لطلب الإبطال. تُعالج طلبات الإبطال من قبل هيئة التسجيل TS RA فور اتخاذ قرار الإبطال وفي جميع الحالات ضمن الأطر الزمنية المحددة في الفقرة 4.9.1 من بيان ممارسة الشهاداتCPS)).

4.9.5 الإطار الزمني الذي يجب على هيئة التصديق خلاله معالجة طلب الإبطال

تُعالج طلبات إبطال الشهادات خلال مدة لا تتجاوز 24 ساعة.

فيما يخص تقارير مشكلات الشهادات تبدأ هيئة التسجيل TS RA التحقيق خلال 24 ساعة من استلام التقرير. وتبادر بالتواصل مع المشترك وعند الاقتضاء مع الجهات المعنية الأخرى (مثل الجهات الأمنية). كما يتم إرسال رسالة أولية إلى المشترك ومُرسل تقرير المشكلة بخصوص الحالة.

تُجري هيئة التسجيل مزيداً من التحقيقات بالتعاون مع مجلس حوكمة البنية التحتية للمفاتيح العامةTS PKI GB)) والمشترك والجهات المختصة الأخرى (مثل الجهات الأمنية) لتحديد الإجراء المناسب بشأن الشهادة المعنية.

إذا أظهرت نتائج التحقيق وجود سبب من الأسباب التي تستدعي الإبطال وفق الفقرة 4.9.1 تُبطل الشهادة خلال الإطار الزمني المحدد في تلك الفقرة.

واستناداً إلى سبب الإبطال يجوز لهيئة التسجيل الاتفاق مع المشترك على خطة لإصدار شهادة جديدة.

4.9.6 متطلبات التحقق من الإبطال على الأطراف المعتمدة

تتحمل الأطراف المعتمدة وحدها مسؤولية التحقق من حالة الإبطال لجميع الشهادات في سلسلة الثقة قبل اتخاذ قرار الاعتماد على المعلومات الواردة في الشهادة. وتوفّر هيئة التصديق هذه حالة الإبطال من خلال آليات مدمجة في الشهادة مثل: قائمة الإلغاء (CRL) وبروتوكولOCSP .

4.9.7 وتيرة إصدار قوائم الإبطال (CRL) (إن وُجدت)

تنشر هيئة التصديق TS TLS CA قوائم الإبطال على فترات منتظمة. وتُطبق القواعد التالية على قوائم الإبطال التي تصدرها هذه الهيئة:

- يتم توليد قائمة إبطال جديدة كل 24 ساعة.
- يتم تعيين مدة صلاحية قائمة الإلغاء(أي قيمة حقل nextUpdate) إلى 26 ساعة.

4.9.8 الحد الأقصى للتأخير في إصدار قوائم الإبطال (إن وُجد)

تُصدر هذه الهيئة قوائم الإبطال في الوقت المناسب وفقاً لتواتر الإصدار المبين في الفقرة 4.9.7 من هذا البيان.

4.9.9 حدود المسؤولية

- لا تتحمل شركة مصدر التكنولوجيا أي مسؤولية تجاه المشتركين في حال نجم الضرر عن إهمالهم أو احتيالهم أو سوء سلوكهم المتعمد.
- لا تتحمل شركة مصدر التكنولوجيا أي مسؤولية عن استخدام الشهادات أو أزواج المفاتيح العامة/الخاصة الصادرة بموجب بيان ممارسة الشهادات هذا في أي غرض آخر غير ما ورد في هذا المستند. ويجب على المشتركين تعويض شركة مصدر التكنولوجيا فوراً عن أي مسؤوليات أو تكاليف أو مطالبات تنشأ نتيجة ذلك.
- لا تكون شركة مصدر التكنولوجيا مسؤولة تجاه أي طرف عن أي أضرار مباشرة أو غير مباشرة ناجمة عن انقطاع لا يمكن السيطرة عليه في خدماتها.
- يتحمل المشتركون المسؤولية الكاملة عن أي تحريف للمعلومات الواردة في الشهادة تجاه الأطراف المعتمدة حتى وإن كانت هذه المعلومات قد اعتُمدت من قبل شركة مصدر التكنولوجيا.

- يلتزم المشتركون بتعويض الطرف المعتمد الذي يتكبد خسائر نتيجة إخلال مزود خدمات الثقة بشروط وأحكام المشترك.
- يتحمل الأطراف المعتمدون تبعات فشلهم في تنفيذ واجباتهم كأطراف معتمدة.
- تنفي شركة مصدر التكنولوجيا أي مسؤولية مالية أو من أي نوع آخر عن الأضرار أو الأعطال الناتجة عن عمليات هيئة التصديق لخوادم TLS التابعة لها.

4.9.10 التعويضات

غير قابل للتطبيق.

4.9.11 المدة والإنهاء

4.9.11.1 المدة

يبقى بيان ممارسة الشهادات هذا سارياً بعد اعتماده من قبل مجلس حوكمة البنية التحتية للمفاتيح العامة (TS PKI GB) إلى أن يُنشر أي تعديل عليه في المستودع العام لشركة مصدر التكنولوجيا.

4.9.11.2 الإنهاء

تُطبق التعديلات على هذا المستند بعد اعتمادها من قبل مجلس حوكمة البنية التحتية للمفاتيح العامة(TS PKI GB) ويُشار إلى ذلك بإصدار جديد للمستند. ويُصبح الإصدار الجديد نافذاً بمجرد نشره في المستودع العام لشركة مصدر التكنولوجيا بينما تُؤرشف الإصدارات السابقة في المستودع نفسه.

4.9.11.3 توافر التحقق من الإبطال/الحالة عبر الإنترنت

توفّر هيئة التصديق هذه مستجيباً لبروتوكول OCSP يتوافق مع المعيار6960 RFC وتوقّع شهادته من قبل هيئة التصديق TS TLS CA ويُتيح مستجيب OCSP المعلومات مباشرة لتطبيقات الأطراف المعتمدة بناءً على إجراءات هيئة التصديق على الشهادات المُصدرة.

تتضمن شهادة OCSP امتداداً من نوع **id-pkix-ocsp-nocheck** كما هو معرّف في6960 RFC .

ويتم تضمين عنوان URL الفعلي لمستجيبOCSP المطلوب الاستعلام عنه من قبل الأطراف المعتمدة ضمن الشهادات المُصدرة من قبل هذه الهيئة.

4.9.11.4 متطلبات التحقق من الإبطال عبر الإنترنت

يدعم مستجيب OCSP طريقتي HTTP GET وHTTP POST.

وتتمثل فترة صلاحية استجابة OCSP بالفارق الزمني بين حقلي **thisUpdate**و**nextUpdate** ويُحتسب الفارق وفق القيم الزمنية التالية:

- 3600 ثانية = ساعة واحدة.
- 86400 ثانية = يوم واحد

مع تجاهل الثواني الكبيسة.

فيما يخص حالة شهادات المشتركين:

- يجب أن تكون فترة صلاحية استجابات OCSP أكبر من أو تساوي ثماني ساعات.
- ويجب أن تكون أقل من أو تساوي عشرة أيام.
- إذا كانت فترة صلاحية استجابة OCSP أقل من ست عشرة ساعة تقوم هيئة التصديق TS TLS CA بتحديث المعلومات عبر بروتوكول OCSP قبل منتصف فترة الصلاحية وقبل الوصول إلى وقت.
- إذا كانت فترة صلاحية استجابة OCSP أكبر من أو تساوي ست عشرة ساعة تُحدث هيئة التصديق TS TLS CA المعلومات قبل ثماني ساعات على الأقل من وقت وبحد أقصى أربعة أيام بعد وقت.

في حال تلقى مستجيب OCSP طلباً للتحقق من رقم تسلسلي غير مستخدم (أي لم تصدره هذه الهيئة) يستجيب المستجيب بحالة مُبطلة وفقاً للمادة 4.4.8 (تعريف الإبطال الممتد) في RFC 6960 .

يراقب فريق TS PKI مستجيب OCSP لاكتشاف أي طلبات تتعلق بأرقام تسلسلية غير مستخدمة كجزء من إجراءات الرصد الأمني. وتؤدي أي حالة من هذا النوع إلى فتح تحقيق من قبل الفرق المختصة في TS PKI .

4.9.12 وسائل أخرى للإعلان عن الإبطال

تستخدم هيئة التصديق هذه بروتوكول OCSP وقائمة الإلغاء CRL فقط كوسيلتين لنشر معلومات إبطال الشهادات.

4.9.13 المتطلبات الخاصة المتعلقة باختراق المفتاح

إذا اكتشفت شركة مصدر التكنولوجيا أو كان لديها سبب للاعتقاد بحدوث اختراق للمفتاح الخاص لهيئة التصديق TS TLS CA تعلن على الفور حالة الطوارئ وتفعّل خطة استمرارية الأعمال الخاصة بها كما ستقوم بالآتي:

- تحديد نطاق الشهادات التي يجب إبطالها.
- إبطال الشهادات المتأثرة خلال 24 ساعة ونشر قوائم الإبطال (CRLs) عبرالإنترنت خلال 30 دقيقة من إنشائها.
- بذل جهود معقولة لإبلاغ الجهات الحكومية والمشتركين والأطراف المعتمدة المحتملة بوقوع اختراق للمفتاح.
- توليد زوج مفاتيح جديد لهيئة التصديق وفقاً لسياسات وإجراءات التشغيل الخاصة بشركة مصدر التكنولوجيا.

يجوز للأطراف المعتمدة إخطار شركة مصدر التكنولوجيا بوجود اختراق للمفتاح الخاص باستخدام إحدى الطرق التالية:

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

4.9.14 الظروف التي تستدعي التعليق

لا تدعم هيئة التصديق هذه تعليق الشهادات.

4.9.15 من يمكنه طلب التعليق

غير قابل للتطبيق.

4.9.16 إجراءات طلب التعليق

غير قابل للتطبيق.

4.9.17 حدود فترة التعليق
غير قابل للتطبيق.

4.10 خدمات حالة الشهادات
يُرجى الرجوع إلى الفقرة 4.9.6 من هذا البيان .(CPS) بالإضافة إلى ذلك اعتماد الأحكام التالية:

4.10.1 الخصائص التشغيلية
تنشر هيئة التصديق هذه قوائم الإبطال (CRLs) في المستودع العام المتاح للأطراف المعتمدة.

كما يوفّر مستجيب OCSP التابع لهيئة التصديق واجهة HTTP متاحة أيضاً للأطراف المعتمدة عبر الإنترنت.

لا تُزال إدخالات الإبطال من قائمة الإلغاء (CRL) أو من استجابات OCSP بعد تاريخ انتهاء صلاحية الشهادات المُبطلة.

تتضمن قائمة الإلغاء الامتداد وفقاً لتعريف معيار X.509 في / ISO / IEC 9594-8 توصيةITU-T X.509 .

4.10.2 توفر الخدمة
المستودع العام الذي تُنشر فيه معلومات الشهادات وقوائم الإبطال (CRLs) متاح 24 ساعة في اليوم 7 أيام في الأسبوع ويضمن نسبة توافر لا تقل عن 99.6٪ خلال فترة سنة كاملة.

تُشغّل هيئة التصديق هذه وتُدير قدرات CRL وOCSP لديها باستخدام موارد كافية لضمان زمن استجابة لا يتجاوز عشر ثوانٍ في ظروف التشغيل العادية.

تُحافظ هيئة التصديق على قدرة داخلية دائمة على مدار الساعة وطوال أيام الأسبوع للاستجابة لتقارير مشكلات الشهادات ذات الأولوية القصوى كما هو موضح في الفقرة 4.9.3 من هذا البيان وعند الاقتضاء تُحيل تلك البلاغات إلى الجهات الأمنية المختصة وتُبطل الشهادة محل الشكوى.

4.10.3 الخصائص الاختيارية
لا يوجد اشتراط.

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

4.12 إيداع المفاتيح واستعادتها

4.12.1 سياسة وممارسات إيداع واستعادة المفاتيح
لا تدعم هيئة التصديق هذه خاصية إيداع المفاتيح.

4.12.2 سياسة وممارسات تغليف واستعادة مفتاح الجلسة
غير قابل للتطبيق.

5 الضوابط المتعلقة بالمرافق والإدارة والتشغيل

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

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

- الضوابط الأمنية الفيزيائية والبيئية.
- ضوابط سلامة النظام بما يشمل إدارة التهيئة والتغييرات وإدارة التحديثات وإدارة الثغرات والكشف عن البرمجيات الخبيثة أو الفيروسات والوقاية منها.
- الحفاظ على سجل لجميع الأصول وإدارتها وفقاً لتصنيفاتها.
- أمن الشبكة وإدارة جدران الحماية بما في ذلك تقييد المنافذ وتصفية عناوينIP .
- إدارة المستخدمين وتخصيص الأدوار الموثوقة بشكل منفصل والتعليم والتوعية والتدريب.
- ضوابط الوصول المنطقي وتسجيل الأنشطة ومراقبتها ومراجعة وصول المستخدمين بشكل دوري لضمان المساءلة الفردية.

يتضمن برنامج الأمن الخاص بشركة مصدر التكنولوجيا تقييماً سنوياً للمخاطر يتضمن ما يلي:

1. تحديد التهديدات الداخلية والخارجية المتوقعة التي قد تؤدي إلى الوصول غير المصرح به أو الكشف أو إساءة الاستخدام أو التعديل أو الإتلاف لأي من بيانات الشهادات أوعمليات إدارة الشهادات.
2. تقييم احتمالية حدوث هذه التهديدات والضرر المحتمل المترتب عليها مع الأخذ بعين الاعتبار حساسية بيانات الشهادات وعمليات إدارتها.
3. تقييم كفاية السياسات والإجراءات وأنظمة المعلومات والتقنيات والترتيبات الأخرى المتوفرة لدى شركة مصدر التكنولوجيا لمواجهة هذه التهديدات.

واستناداً إلى تقييم المخاطر تقوم شركة مصدر التكنولوجيا بوضع وتنفيذ وصيانة خطة أمنية تتضمن إجراءات وتدابير ومنتجات أمنية تهدف إلى تحقيق الأهداف المذكورة أعلاه وإدارة المخاطر المحددة والسيطرة عليها بما يتناسب مع حساسية بيانات الشهادات وعمليات إدارتها.

وتتضمن هذه الخطة الأمنية ضمانات إدارية وتنظيمية وتقنية وفيزيائية مناسبة لحساسية بيانات الشهادات وعمليات إدارتها كما تأخذ الخطة في الاعتبار التكنولوجيا المتاحة وتكلفة تنفيذ التدابير المحددة وتطبق مستوى معقولاً من الأمان يتناسب مع حجم الضرر المحتمل الناتج عن أي خرق أمني وطبيعة البيانات الواجب حمايتها.

5.1 الضوابط الأمنية الفيزيائية

يحرص مجلس حوكمة البنية التحتية للمفاتيح العامة لدى مصدر التكنولوجيا (TS PKI GB) على تنفيذ ضوابط أمنية فيزيائية مناسبة في مرافق استضافة البنية التحتية للمفاتيح العامة .(PKI) وقد جرى توثيق هذه الضوابط ضمن السياسات الداخلية لشركة مصدر التكنولوجيا ويجري تطبيقها والتحقق منها بانتظام من خلال عمليات تدقيق داخلية ينفذها مجلس TS PKI GBعلى فريق عملياتPKI .

5.1.1 موقع المنشأة وتصميمها

تستضيف منشأة شديدة التأمين تديرها شركة مصدر التكنولوجيا جميع المكونات الحيوية لحل البنية التحتية للمفاتيح العامة. وتُطبق ضوابط أمنية فيزيائية لضمان منع وصول الأشخاص غير المخولين من خلال أربع طبقات من الحماية الفيزيائية وعند دمج هذا التحكم المتعدد الطبقات مع وسائل الحماية الفيزيائية مثل الحراس وأجهزة كشف التسلل وكاميرات المراقبةCCTV)) فإن ذلك يوفر مستوى قوياً من الحماية ضد الدخول غير المصرح به إلى أنظمةTS PKI .

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

5.1.2 الوصول الفيزيائي

تحمي أنظمة هيئة التصديق لدى شركة مصدر التكنولوجيا ضوابط أمنية فيزيائية متعددة الطبقات (أربع طبقات) ولا يمكن الوصول إلى الطبقات الأدنى إلا بعد المرور أولاً من خلال الطبقات الأعلى. وتُجرى الأنشطة التشغيلية الحساسة المتعلقة بدورة حياة الشهادات ضمن أكثر الطبقات الفيزيائية تقييداً. ويسجل نظام التحكم بالوصول حركة الأفراد خلال كل منطقة (أي طبقة).

تشمل الضوابط الأمنية الفيزيائية مراقبة الدخول إلى المبنى من قبل حراس أمن والمصادقة البيومترية والمراقبة بكاميرات CCTV وتُراقب هذه الضوابط على مدار الساعة وطوال أيام السنة مما يوفر مستويات حماية متعددة للأفراد الداخلين والخارجين من المبنى.

يُمنح الدخول إلى المنشأة فقط بعد إبراز بطاقة الهوية الوطنية الخاصة بالفرد حيث يتحقق منها حارس الأمن ويُسجل المعلومات الضرورية مثل هوية الشخص ووقت الوصول والمغادرة ويُزود الزائر ببطاقة تعريف. ولا يُسمح بالدخول ما لم يكن الشخص مخولاً بذلك من قبل أحد أعضاء مجلس PKIويجب أن يكون برفقة أحد الموظفين الموثوقين فيTS .

كما لا يُسمح بالدخول إلى الحجرة المحصنة التي تستضيف أنظمة هيئة التصديق إلا بوجود اثنين من الموظفين الموثوقين لفتح باب الحجرة بشكل متزامن.

5.1.3 الطاقة والتكييف

يضمن تصميم المنشأة التي تستضيف TS PKI توفير أنظمة UPS ومولدات احتياطية بقدرة كافية لدعم تشغيل أنظمة البنية التحتية للمفاتيح العامة في حالات انقطاع التيار الكهربائي. وتتوفر وحدات UPS ومولدات احتياطية لخدمة المنشأة بأكملها.

تركيب نظام تكييف هواء احتياطي بالكامل في المناطق التي تستضيف أنظمة البنية التحتية للمفاتيح العامة (PKI) وتضمن جميع هذه الأنظمة تشغيل معدات PKI ضمن نطاق درجات الحرارة والرطوبة المسموح به من قبل الشركات المصنّعة.

5.1.4 التعرض للمياه

اتخذ مجلس حوكمة TS PKI الاحتياطات المعقولة للتقليل من أثر التعرض للمياه في منشأة استضافة .TS PKI وتشمل هذه الاحتياطات تركيب معدات TS PKI على أرضيات مضادة للكهرباء الساكنة مزودة بكواشف رطوبة.

5.1.5 الوقاية من الحريق والحماية منه

تتبع منشأة استضافة TS PKI أفضل الممارسات المعتمدة واللوائح الأمنية المعمول بها في العراق وتخضع للمراقبة على مدار الساعة وطوال أيام السنة ومزودة بأجهزة الكشف عن الحريق والحرارة.

وقد ركب معدات إخماد الحرائق في المناطق المخصصة وتُفعَّل تلقائياً في حال حدوث حريق ويمكن تشغيلها يدوياً عند الحاجة.

5.1.6 تخزين الوسائط

تخضع الوسائط الإلكترونية والبصرية وغيرها من وسائط التخزين لضوابط الأمن الفيزيائي متعدد الطبقات وتحظى بالحماية من الأضرار العرضية (مثل الماء أو الحريق أو التداخل الكهرومغناطيسي).

يتم تخزين وسائط النسخ الاحتياطي والتدقيق في خزنة آمنة مقاومة للحريق وتُنسخ وتُخزن أيضاً في موقع مخصص لاستعادة البيانات في حالات الكوارث.

5.1.7 التخلص من النفايات

يُدمّر كل الورق ووسائط التخزين التي تُنتج داخل المنشأة المؤمنة قبل التخلص منها. وتُفرم الوسائط الورقية باستخدام آلة فرم بنمط شبكي .(crosshatch) وتُطبق الإجراءات التالية على وسائط الحاسوب القابلة للإزالة:

- يُمنح الإذن بتدمير وسائط الحاسوب القابلة للإزالة.
- تُمحى الوسائط ثم تُدمّر فيزيائياً إذا لم تعد مطلوبة.
- يُحفظ سجل بعملية تدمير هذه الوسائط.
- تُطلق الوسائط بعد ذلك للتخلص منها.

أما الأجهزة التشفيرية فيُجرى تدميرها فيزيائياً أو تصفيرها وفقاً لتعليمات الشركة المصنّعة قبل التخلص منها.

5.1.8 النسخ الاحتياطي خارج الموقع

تُجرى نسخ احتياطية كاملة وتزايدية بشكل دوري لأنظمة TS TLS CA لضمان توفر بيانات كافية للاستعادة عند الحاجة.

وتُؤخذ نسخة احتياطية كاملة واحدة على الأقل إضافة إلى عدة نسخ تزايدية يومياً لأنظمة TS TLS CA العاملة وذلك وفقاً لسياسات وإجراءات النسخ الاحتياطي الموثقة والمعتمدة من قبل فريق عملياتTS PKI .

تُجرى نسخ احتياطية للمعلومات الأشد حساسية (مثل المفاتيح الخاصة) فور الانتهاء من أي مراسيم مفاتيح وفقاً لنص مراسيم المفاتيح الموثق.

تضمن مرافق النسخ الاحتياطي المناسبة نقل النسخ إلى موقع استعادة البيانات في حالات الكوارث حيث تُخزَّن وفق نفس الضوابط الفيزيائية والتقنية والإجرائية المعتمدة في المنشأة الأساسية.

5.2 الضوابط الإجرائية

يتبع مجلس حوكمة TS PKI ممارسات إدارية وبشرية تضمن بدرجة معقولة من الثقة أمانة وكفاءة موظفيTS PKI وأداءهم المرضي لمهامهم في مجالات حوكمة وتشغيل وتقديم خدماتPKI .

وتشمل الضوابط الإجرائية العناصر التالية:

5.2.1 الأدوار الموثوقة

يُعد كل من الأفراد المعنيين بتشغيل عمليات إدارة المفاتيح والمديرين ومسؤولي الأمن أو أي عمليات تؤثر بشكل جوهري على تلك المهام من الموظفين الذين يشغلون مناصب موثوقة (أي عاملين موثوقين).

يخضع جميع الموظفين المعيّنين في هذه المناصب لفحص خلفياتهم قبل مباشرة العمل ويُحتفظ بسجلات الفحص وتُراجع سنوياً.

وفيما يلي الأدوار الموثوقة ضمنTS TLS CA :

- مدير البنية التحتية للمفاتيح :(PKI Administrator) يمتلك بيانات اعتماد برنامج هيئة التصديق ويتولى مسؤولية تهيئة الهيئة وصيانتها.
- مشغّل البنية التحتية للمفاتيح :(PKI Operator) مخوّل بتنفيذ دورة التشغيل ويشارك في العمليات الحرجة مثل إصدار شهادات المشتركين.
- مسؤول الأمن :(Security Officer) يمتلك بيانات اعتماد تتيح له تهيئة أجهزة HSMوتطبيق سياسات PKI على الأنظمة المستهدفة أثناء مراسيم توليد المفاتيح.
- موظف هيئة التسجيل :(RA Officer) مخوّل بالتحقق من طلبات الشهادات ضمن إجراءات إصدارها.
- أوصياء :M-of-N يمتلكون بيانات تفعيلHSM ويشرفون على خزائن هيئات التصديق التابعة.
- مالك نطاق هيئة التصديق :(CA Domain Owner) يمتلك بيانات اعتماد تخوّله تنفيذ عمليات النسخ والاستعادة لأجهزة HSMالتابعة.
- مدقق :HSM يمتلك بيانات اعتماد لاسترجاع سجلات تدقيقHSM .
- أوصياء مركز البيانات :موظفون يمتلكون بيانات اعتماد لفتح مركز بيانات PKI أثناء تنفيذ عمليات هيئة التصديق.
- مسؤول النظام :(System Administrator) مخوّل بتركيب وتكوين واستكشاف وصيانة بيئة نظام التشغيل وقواعد البيانات الداعمة.
- مسؤول الشبكة :(Network Administrator) مخوّل بتركيب وتكوين واستكشاف وصيانة أجهزة الشبكة الداعمة.

5.2.2 عدد الأشخاص المطلوبين لكل مهمة

يتبع فريق عمليات TS PKI إجراءات رقابية صارمة لضمان فصل المهام وفقاً للمسؤوليات الوظيفية ومنع قيام شخص موثوق واحد بتنفيذ عمليات حساسة بشكل منفرد.

تتطلب المهام الحساسة التالية مشاركة شخصين على الأقل:

- الوصول الفيزيائي إلى الحجرة الآمنة التي تستضيف أنظمة هيئة التصديق التابعة لTS .
- الوصول إلى وحدات الأجهزة الأمنية المشفّرة (HSM) الخاصة بهيئة التصديق وإدارتها.
- التحقق والموافقة على إصدار الشهادات.

تُسجل جميع الأنشطة التشغيلية التي يُجريها الموظفون الذين يشغلون أدواراً موثوقة وتُحفظ في سجل تدقيق آمن وقابل للتحقق.

5.2.3 تحديد الهوية والمصادقة لكل دور

قبل تولي مسؤوليات دور موثوق يُجرى ما يلي:

- يتحقق مجلس حوكمة TS PKI من هوية الموظف وسجله المهني من خلال فحوصات خلفية أمنية.

- عند استكمال الإجراءات الداخلية لTS PKI يصدر فريق عمليات المنشأة بطاقة وصول لكل موظف يحتاج إلى دخول فيزيائي إلى الأجهزة داخل الحجرة الآمنة.
- يُصدر موظفو TS PKI المختصون (مديرو النظام) بيانات الاعتماد اللازمة لأنظمة تقنية المعلومات لموظفي هيئات التصديق التابعة لتمكينهم من تنفيذ وظائفهم.

5.2.4 الأدوار التي تتطلب فصل المهام

تُنشأ الأدوار الموثوقة المشار إليها في الفقرة 5.2.1 مع تطبيق فصل مناسب في المهام بينها.

5.3 الضوابط الخاصة بالموظفين

5.3.1 المؤهلات والخبرة ومتطلبات التخليص الأمني

قبل توظيف أي عضو في طاقمTS PKI سواء كان موظفاً أو وكيلاً أو متعاقداً مستقلاً يحرص مجلس TS PKI GB على إجراء التحقق من الخلفية والمؤهلات والخبرة المطلوبة للعمل ضمن نطاق كفاءة الوظيفة المحددة.

- التحقق من هوية الشخص :يجب التحقق من الهوية من خلال حضور الشخص شخصياً أمام موظفين موثوقين يتولون مهام الموارد البشرية أو الأمن.
- التحقق من وثائق تعريف رسمية معترف بها :ويجب أن تتضمن صورة شخصية صادرة عن جهة حكومية.
- التحقق من موثوقية الشخص :ويشمل التحقق من الموثوقية إجراء فحوصات خلفية تتناول على الأقل ما يلي أو ما يعادله:
  - الإدانات الجنائية في جرائم خطيرة.
  - التزوير أو المعلومات الكاذبة التي يقدمها المرشح.
  - مدى مناسبة المراجع.
  - أي تصاريح أمنية أخرى يُعتبر منحها ضرورياً.

5.3.2 إجراءات فحص الخلفية

يُختار جميع الموظفين الذين يشغلون أدواراً موثوقة بناءً على النزاهة والتحقق من الخلفية والحصول على التخليص الأمني. ويتولى مجلس TS PKI GB التأكد من إجراء هذه الفحوصات مرة واحدة سنوياً لجميع الأفراد في الأدوار الموثوقة.

5.3.3 متطلبات التدريب

يوفر مجلس TS PKI GB تدريباً فنياً أساسياً لموظفيه لتمكينهم من أداء مهامهم بفعالية. ويُحدث هذا التدريب بانتظام ويُنفذ سنوياً لموظفيTS TLS CA .

يشمل برنامج التدريب مجموعة واسعة من المواضيع ويُقدَّم من قبل موظفين ذوي خبرة في TS TLS CA إلى جانب خبراء خارجيين متخصصين في الأمن و .PKIوقد جرى تصميم البرنامج بعناية ليتوافق مع متطلبات الأدوار الموثوقة المختلفة المشاركة في إدارة وتقديم خدماتTS TLS CA .

وتشمل المواضيع التي يغطيها التدريب ما يلي:

- نظريات ومبادئ البنية التحتية للمفاتيح العامة(PKI) .
- الضوابط البيئية وسياسات الأمن في PKI.

- عمليات هيئة التسجيل في PKIبما في ذلك إجراءات التحقق والتدقيق.
- العمليات التشغيلية لPKI .
- تدريب عملي على منتجاتPKI .
- إجراءات استعادة العمل في حالات الكوارث واستمرارية الأعمال في PKI.

يحتفظ مجلس TS PKI GB بسجلات شاملة لجميع الموظفين الذين خضعوا للتدريب ويُقيِّم بانتظام مدى رضا المدربين عن التدريب. وفي نهاية كل دورة تدريبية تُجرى اختبارات وتُمنح شهادات للموظفين الذين يجتازونها بنجاح. ويُعد اجتياز هذه الاختبارات شرطاً إلزامياً لجميع الأدوار الموثوقة بما في ذلك المختصين في التحقق قبل التصريح لهم بمزاولة المهام في هذه الأدوار.

5.3.4 تكرار ومتطلبات التدريب المتجدد

يُقدَّم منهج التدريب إلى جميع موظفي .TS PKI ويُراجع محتوى التدريب ويُحدَّث سنوياً ليعكس أحدث الممارسات الرائدة والتعديلات التي تطرأ على تهيئة أنظمة هيئة التصديق.

5.3.5 تكرار وتتابع تدوير الوظائف

يحرص مجلس حوكمة TS PKI على أن أي تغيير في طاقم العمل لدى هيئات التصديق التابعة لـ TS لا يؤثر على الكفاءة التشغيلية أو استمرارية أو سلامة خدمات الهيئة.

5.3.6 العقوبات على الأفعال غير المصرّح بها

لضمان المساءلة على موظفيPKI TS يفرض مجلس TS PKI GB عقوبات على الأفعال غير المصرّح بها أو الاستخدام غير المشروع للصلاحيات أو للأنظمة وذلك وفقاً لسياسات وإجراءات الموارد البشرية المعتمدة والقوانين العراقية ذات الصلة.

5.3.7 متطلبات المتعاقدين المستقلين

يخضع المتعاقدون المستقلون وموظفوهم لنفس فحوصات الخلفية التي تُطبّق على موظفي .TS PKI وتشمل هذه الفحوصات ما يلي:

- الإدانات الجنائية في جرائم جسيمة.
- التزوير أو المعلومات الكاذبة من قِبل المرشح.
- مدى مناسبة المراجع.
- التصاريح الأمنية كما تُعتبر مناسبة.
- حماية الخصوصية.
- شروط السرية.

5.3.8 الوثائق المقدمة للموظفين

يوثّق مجلس حوكمة TS PKI جميع المواد التدريبية ويوفّرها لموظفيPKI TS .

كما يحرص المجلس على توفير الوثائق التشغيلية الأساسية للموظفين المعنيين وتشمل هذه الوثائق كحد أدنى: وثيقة ممارسات هيئة التصديق(CPS) وسياسات الأمن وأدلة التشغيل والوثائق الفنية المرتبطة بكل دور موثوق.

5.4 إجراءات تسجيل السجلات التدقيقية

شمل إجراءات التدقيق تسجيل الأحداث وتدقيق الأنظمة وتُنفذ بغرض الحفاظ على بيئة آمنة. وتشمل هذه الإجراءات أنشطة إدارة دورة حياة المفاتيح بما في ذلك توليد المفاتيح والنسخ الاحتياطي والتخزين والاسترداد والتدمير وإدارة الأجهزة التشفيرية وهيئة التصديق ومستجيبOCSP .

تُولّد ملفات سجلات التدقيق الأمني لجميع الأحداث المتعلقة بأمن هيئة التصديق وهيئة التسجيل ومستجيبات OCSP وتُحفظ. ويُراجع هذه السجلات مسؤول الأمن فيTS .

تُراجع السجلات أيضاً ضمن عمليات التدقيق الداخلي المنتظم التي تُجريها وحدة الامتثال في TS على عملياتTS TLS CA .

5.4.1 أنواع الأحداث المسجلة

تُولّد سجلات التدقيق لجميع الأحداث المتعلقة بأمن وخدمات أنظمة.TS TLS CA
تُسجل شركة الأحداث المرتبطة بالإجراءات المتخذة لمعالجة طلب الشهادة وإصدارها بما في ذلك جميع المعلومات المتولدة والوثائق المستلمة المرتبطة بطلب الشهادة وتاريخ ووقت الحدث والأشخاص المعنيين.

تُتاح هذه السجلات للمدقق المؤهل لدى كدليل على التزام هيئة التصديق بهذه المتطلبات.

وتتضمن كل سجل تدقيقي على الأقل ما يلي:

- تاريخ ووقت وقوع الحدث.
- مؤشر نجاح أو فشل الحدث (مثل توقيع من قِبل هيئة التصديق حدث إلغاء شهادة حدث تحقق من شهادة).
- هوية الكيان والمشغّل المتسبب بالحدث.
- وصف الحدث.

وعندما يكون ذلك ممكناً تُولَّد السجلات التدقيقية تلقائياً وفي الحالات التي لا يمكن فيها ذلك يُستخدم سجل يدوي أو نماذج ورقية. تُحتفظ بهذه السجلات سواء الإلكترونية أو غير الإلكترونية من قبل فريق عملياتPKI ويجوز إتاحتها أثناء عمليات تدقيق الالتزام.

يُسجّل ما يلي من أحداث تتعلق بعملياتTS TLS CA :

1. أحداث دورة حياة شهادات ومفاتيحTS TLS CA بما في ذلك:
   - توليد المفاتيح النسخ الاحتياطي التخزين الاسترداد الأرشفة والتدمير.
   - أحداث إدارة دورة حياة الأجهزة التشفيرية.
   - طلبات الشهادات التجديد إعادة توليد المفاتيح والإلغاء.
   - الموافقة أو الرفض على طلبات الشهادات.
   - توليد قوائم الشهادات الملغاةs(CRL) .
   - توقيع ردودOCSP .
   - إدخال ملفات تعريف جديدة للشهادات وإيقاف العمل بملفات التعريف السابقة.
2. أحداث إدارة دورة حياة شهادات المشتركين بما في ذلك:
   - طلبات الشهادات التجديد إعادة توليد المفاتيح والإلغاء.

- جميع أنشطة التحقق المنصوص عليها في هذه الوثيقة (مثل التاريخ الوقت الاتصالات والأشخاص المتواصل معهم).

3. الموافقة أو الرفض على طلبات الشهادات.
4. إصدار الشهادات.
5. محاولات التحقق متعددة المنظورات من كل منظور شبكي مع تسجيل المعلومات التالية كحد أدنى:
   - معرّف يميز بشكل فريد منظور الشبكة المستخدم.
   - اسم النطاق وعنوان IP الذي جرى التحقق منه.
   - نتيجة المحاولة (مثل: "نجح/فشل تحقق النطاق" "إذن/حظر"CAA).
6. نتائج التوافق ضمن النصاب لمحاولات التحقق متعددة المنظورات لأسماء النطاق أو عناوين IPالمشار إليها في طلب الشهادة.
3. الأحداث الأمنية بما في ذلك:
   - محاولات الوصول الناجحة والفاشلة إلى أنظمةPKI .
   - الإجراءات المنفذة على أنظمة PKI وأنظمة الأمن.
   - الأنشطة ذات الصلة بأجهزة التوجيه وجدران الحماية (كما هو موضح في القسم 5.4.1.1).
   - التغييرات في ملفات تعريف الأمان.
   - مشكلات منصات الأنظمة (مثل الأعطال) الأعطال المادية والاضطرابات الأخرى.
   - تثبيت أو تحديث أو إزالة البرمجيات على نظام الشهادات.
   - الدخول إلى منشأة هيئة التصديق والخروج منها.

يحرص مجلس حوكمة TS PKI أيضاً على ضمان الاحتفاظ بالمعلومات التالية سواء إلكترونياً أو يدوياً من قبل فريق العمليات فيTS رغم أنها لا تُنتَج من قِبل هذه الهيئة مباشرة:

1. تغييرات/تدوير ملفات تعريف الأمان الخاصة بموظفي هيئة التصديق.
2. جميع نسخ هذه الوثيقة(CPS) .
3. محاضر الاجتماعات.
4. تقارير التدقيق الداخلي الخاصة بالامتثال.
5. النسخ الحالية والسابقة من ملفات التهيئة وأدلة التشغيل لهيئات التصديق التابعة لTS .

5.4.1.1 سجلات أنشطة أجهزة التوجيه وجدران الحماية

تشمل أنشطة أجهزة التوجيه وجدران الحماية التي تُسجَّل ما يلي:

1. محاولات تسجيل الدخول الناجحة والفاشلة إلى أجهزة التوجيه وجدران الحماية.
2. تسجيل جميع الإجراءات الإدارية المنفذة على أجهزة التوجيه وجدران الحماية بما في ذلك تغييرات الإعدادات تحديثات البرمجيات الثابتة وتعديلات ضوابط الوصول.
3. تسجيل جميع التعديلات التي تتم على قواعد جدران الحماية بما في ذلك الإضافات والتعديلات والحذف.
4. تسجيل جميع أحداث النظام والأخطاء بما في ذلك الأعطال المادية وانهيارات البرمجيات وإعادة تشغيل النظام.

5.4.2 تكرار معالجة السجلات

يضمن مجلس حوكمة TS PKI قيام الموظفين المخصصين بمراجعة ملفات السجلات على فترات منتظمة للتحقق من سلامة السجلات وضمان اكتشاف الأحداث غير الاعتيادية في الوقت المناسب. ويُنفَّذ كحد أدنى ما يلي من دورات مراجعة السجلات من قبل مجلسTS PKI GB :

- تُراجع سجلات التدقيق والأمن لتطبيقات هيئة التصديق من قبل فريق المراقبة والامتثال شهرياً.
- تُراجع سجلات التدقيق والأمن لأنظمة هيئة التصديق المتصلة بالشبكة (مثل مستجيب OCSP) شهرياً من قبل فريق المراقبة والامتثال للتحقق من سلامة عمليات التسجيل والتأكد من أن وظيفة المراقبة اليومية تُؤدى بالشكل المناسب.
- تُراجع سجلات الدخول الفعلي وإدارة المستخدمين على أنظمة TS PKI كل ثلاثة أشهر من قبل فريق المراقبة والامتثال للتحقق من التزام السياسات الخاصة بالدخول المادي والمنطقي.
- يُجري قسم التدقيق والامتثال في مجلس TS PKI GB تدقيقاً داخلياً على عمليات هيئات التصديق التابعة لـ TS مرة واحدة سنوياً. وتشمل عملية التدقيق هذه مراجعة عينات من تقارير مراجعة السجلات والسجلات المدققة منذ آخر دورة تدقيق.
- تُجمع أدلة مراجعة سجلات التدقيق ونتائج عمليات المراجعة والإجراءات التصحيحية المُنفّذة وتُؤرشف.

5.4.3 فترة الاحتفاظ بسجلات التدقيق

يحتفظ فريق عمليات TS بالسجلات لمدة لا تقل عن سنتين أو بحسب ما يُنص عليه في القسم 5.5.2 وتتضمن:

1. سجلات دورة حياة شهادات ومفاتيح هيئة التصديق (كما هو مذكور في القسم 15.4.1) بعد حدوث أي من الحدثين التاليين أيهما يأتي لاحقاً:
   a. تدمير المفتاح الخاص لهيئة التصديق.
   b. إبطال أو انتهاء صلاحية آخر شهادة هيئة تصديق (CA Certificate) ضمن مجموعة الشهادات التي تتضمن امتدادX.509v3 مع ضبط حقل CA على"true" والتي تشترك بمفتاح عام واحد يُقابل المفتاح الخاص لهيئة التصديق.
2. سجلات دورة حياة شهادات المشتركين (كما ورد في القسم 25.4.1))) بعد إبطال أو انتهاء صلاحية شهادة المشترك.
3. أي سجلات لأحداث أمنية (كما ورد في القسم 35.4.1))) بعد وقوع الحدث مباشرة.

5.4.4 حماية سجلات التدقيق

تُحمى سجلات التدقيق من خلال مجموعة من الضوابط الأمنية الفيزيائية والإجرائية والتقنية على النحو التالي:

1. تولّد أنظمة هيئات التصديق التابعة لـ TS سجلات تدقيق محمية تشفيرياً.
2. تُحافظ على أمن سجلات التدقيق أثناء نقلها عبر نظام النسخ الاحتياطي وأثناء أرشفتها.
3. تفرض سياسات التحكم بالوصول المعتمدة على أنظمة TS PKI السماح بالوصول للقراءة فقط للموظفين المصرح لهم كجزء من مهامهم التشغيلية.
4. يُمنح الوصول إلى الأنظمة التي تُخزن فيها سجلات التدقيق للأدوار المصرح بها فقط ويُسجل أي محاولة للتلاعب بالسجلات مع إمكانية تتبعها إلى موظف TS المسؤول.

5.4.5 إجراءات النسخ الاحتياطي لسجلات التدقيق

تُطبق القواعد التالية على نسخ سجلات التدقيق الخاصة بهيئات التصديق التابعة لTS :

- تُخزّن وسائط النسخ الاحتياطي محلياً في الموقع الرئيسي لهيئات التصديق التابعة لTS في موقع آمن.
- تُخزّن نسخة ثانية من بيانات وسجلات التدقيق في موقع استعادة الكوارث والذي يوفر مستوى مماثلاً من الأمان الفيزيائي والبيئي كما في الموقع الرئيسي.

5.4.6 نظام جمع السجلات (داخلي مقابل خارجي)

تُفعّل عمليات التدقيق التلقائية عند بدء تشغيل النظام وتُغلق عند إيقاف تشغيله.

وفي حال فشل نظام التدقيق الآلي وتعرضت سلامة النظام أو سرية المعلومات المحمية للخطر يُقرر مجلس حوكمة TS PKIما إذا كان ينبغي تعليق عمليات هيئة التصديق المعنية حتى حل المشكلة.

5.4.7 إشعار الجهة المتسببة بالحدث

عند تسجيل حدث بواسطة نظام جمع السجلات لا يُشترط تقديم إشعار إلى الفرد أو المؤسسة أو الجهاز أو التطبيق الذي تسبب بالحدث.

5.4.8 تقييم الثغرات الأمنية

تنفذ عمليات TS PKI تقييماً سنوياً للمخاطر يتضمن ما يلي:

1. تحديد التهديدات المحتملة الداخلية والخارجية التي قد تؤدي إلى وصول غير مصرح به أو كشف أو سوء استخدام أو تعديل أو إتلاف لأي من بيانات الشهادات أو عمليات إدارة الشهادات.
2. تقييم احتمالية وتأثير هذه التهديدات مع أخذ حساسية بيانات الشهادات وعمليات إدارتها بنظر الاعتبار.
3. تقييم كفاية السياسات والإجراءات وأنظمة المعلومات والتقنيات والترتيبات الأخرى المتوفرة لدى TS لمواجهة تلك التهديدات.

وتخضع أنظمة وبنية TS PKI التحتية أيضاً لتقييمات أمنية منتظمة على النحو التالي:

- خلال أسبوع واحد من استلام طلب من منتدى المتصفح وهيئة التصديق(CA/Browser Forum) .
- بعد أي تغييرات على النظام أو الشبكة تُعتبر جوهرية من قِبل هيئة التصديق.
- مرة واحدة على الأقل كل ثلاثة أشهر على عناوين IP العامة والخاصة المُحددة ضمن أنظمة البنية التحتية الأساسية والمساندة لـ TS TLS CA. تُنفَّذ هذه التقييمات الذاتية الدورية من قِبل أفراد الأمن ضمن فريق عمليات TS PKI.

وعلى أساس سنوي وبعد ترقيات أو تعديلات جوهرية في البنية التحتية أو التطبيقات كما يحددها مجلس حوكمة TS PKIيُنسق المجلس تنفيذ اختبار اختراق وتقييم مستقل للثغرات من طرف ثالث على أنظمةTS PKI .

تُعرض نتائج التقييمات الدورية والقضايا المكتشفة على مجلس حوكمة TS PKI وإدارة عملياتPKI المسؤولة عن تنظيم ومتابعة تنفيذ الإجراءات التصحيحية من قبل الفرق المعنية.

ويُسجّل موظفو TS TLS CA دليلاً يُثبت أن كل مسح للثغرات أو اختبار اختراق يُنفذ من قِبل أفراد أو جهات تملك المهارات والأدوات والكفاءة اللازمة وتلتزم بمدونة سلوك مهني وتتمتع بالاستقلالية اللازمة لضمان نتائج موثوقة. وتُجمع الأدلة الخاصة بهذه الأنشطة وتُؤرشف من قِبل موظفي Technology Source المعنيين.

5.5 أرشفة السجلات

5.5.1 أنواع السجلات المؤرشفة

تُؤرشف هيئات التصديق التابعة لـ TS كافة سجلات التدقيق (كما ورد في القسم 5.4.1) بالإضافة إلى ما يلي:

1. الوثائق المتعلقة بأمن أنظمة هيئة التصديق وأنظمة إدارة الشهادات.
2. الوثائق المتعلقة بعمليات التحقق وإصدار الشهادات وإبطال طلبات الشهادات والشهادات نفسها.

5.5.2 فترة الاحتفاظ بالأرشيف

تُحتفظ بسجلات التدقيق المؤرشفة كما هو موضح في القسم 5.5.1 لمدة لا تقل عن سبع (7) سنوات. وتضمن هذه الفترة توفر السجلات لأغراض التحقيق في الحوادث الأمنية المحتملة أو غيرها من الأحداث التي تتطلب الرجوع إلى الأنشطة السابقة وتحليلها.

بالإضافة إلى ذلك تحتفظ هيئات التصديق التابعة لTS لمدة لا تقل عن سبع (7) سنوات بـ:

1) جميع الوثائق المؤرشفة المتعلقة بأمن أنظمة هيئات التصديق وأنظمة إدارة الشهادات (كما ورد في القسم 5.5.1).
2) جميع الوثائق المؤرشفة المتعلقة بالتحقق وإصدار الشهادات وإبطال طلبات الشهادات والشهادات (كما ورد في القسم 5.5.1) بعد وقوع أحد الأمرين التاليين أيهما كان لاحقاً:
   a) آخر مرة تم فيها الاعتماد على تلك السجلات والوثائق في عمليات التحقق أو إصدار أو إبطال الشهادات.
   b) انتهاء صلاحية شهادات المشتركين التي استندت إلى تلك السجلات والوثائق.

5.5.3 حماية الأرشيف

تُؤرشف السجلات بطريقة تمنع حذفها أو إتلافها وتُطبّق ضوابط تضمن أن الأفراد المخولين فقط يمكنهم إدارة الأرشيف دون التأثير على سلامة السجلات أو أصالتها أو سريتها.

5.5.4 إجراءات النسخ الاحتياطي للأرشيف

يُحتفظ بنسخة واحدة فقط من كل أرشيف رقمي في كل من مرفق الموقع الرئيسي وموقع استعادة الكوارث الخاص بهيئات التصديق التابعة لـ .TS ويستخدم فريق عمليات TS PKI إجراءات نسخ احتياطي واسترجاع وأرشفة موثقة تُبيّن كيفية إنشاء بيانات الأرشيف ونقلها وتخزينها.

5.5.5 متطلبات الطابع الزمني للسجلات

تتضمن جميع الأحداث المسجلة والمؤرشفة تاريخ ووقت وقوع الحدث. ويُزامن توقيت الأنظمة الإلكترونية لهيئة TS TLS CAمع مصدر زمني من ساعة تعتمد على نظام .GPS وتُحقق خدمات الطابع الزمني دقة تُعادل ±1 ثانية أو أفضل بالمقارنة مع التوقيت العالمي المنسقUTC))ويطبّق فريق عمليات PKI إجراءً يُلزم بالتحقق من انحراف الوقت وتصحيحه عند الحاجة.

5.5.6 نظام جمع الأرشيف (داخلي أو خارجي)

يعتمد جمع الأرشيف لدى هيئات التصديق التابعة لـ TS على نظام داخلي.

5.5.7 إجراءات الحصول على معلومات الأرشيف والتحقق منها

يُسمح فقط للموظفين المخولين والمُوثقين بالوصول إلى المواد المؤرشفة. ويستخدم فريق عمليات TS PKI إجراءات النسخ الاحتياطي والاسترجاع والأرشفة الخاصة بهيئات التصديق التابعة لـTS والتي توثّق كيفية إنشاء المعلومات المؤرشفة ونقلها وتخزينها. وتشتمل هذه الإجراءات أيضاً على تفاصيل نظام جمع الأرشيف.

5.6 تبديل المفاتيح

لتقليل أثر اختراق المفتاح يُبدّل مفتاح هيئة التصديق وفق تكرار يضمن أن فترة صلاحية هيئة التصديق التابعة لـ TS تتجاوز العمر الأقصى لشهادة المشترك بعد آخر عملية إصدار .راجع القسم 6.3.2 من هذا المستند لمعرفة تكرار تبديل المفاتيح.

ويُقدّم الشهادة الجديدة التي تحتوي على المفتاح العام لهيئة التصديق إلى المشتركين والأطراف المعتمدة من خلال وسائل التسليم الموضحة في الفصل 6.1.4.

ولأغراض إدارة إبطال الشهادات الصادرة يُحتفظ بالمفاتيح الخاصة القديمة لهيئة التصديق حتى انتهاء صلاحية جميع الشهادات التي وُقعت باستخدام ذلك المفتاح الخاص.

5.7 التعافي من الكوارث والاختراق(Compromise and Disaster Recovery)

5.7.1 إجراءات التعامل مع الحوادث والاختراق

5.7.1.1 خطط الاستجابة للحوادث والتعافي من الكوارث

في حال كشف محاولة اختراق محتملة أو أي شكل من أشكال الانتهاك لسلطة التصديق (CA) من قبل مجلس إدارة البنية التحتية للمفاتيح العامة(TS PKI GB) ، يتم إجراء تحقيق لتحديد طبيعة وحجم الضرر وفقاً للآتي:

- أولاً: في حال الاشتباه باختراق المفتاح الخاص (Private Key) لسلطة التصديق، تُطبق الإجراءات المحددة في "خطة استمرارية الأعمال والتعافي من الكوارث" الخاصة بالشركة. بخلاف ذلك، يتم تقييم نطاق الضرر المحتمل لتحديد ما إذا كانت سلطة التصديق بحاجة إلى إعادة بناء، أو الاكتفاء بإلغاء بعض الشهادات، و/أو الإعلان عن اختراق مفتاح سلطة التصديق.
- ثانياً: يحدد مجلس إدارة (TS PKI GB) أيضاً آليات الإبلاغ عن الاختراق والاتصالات ذات الصلة كجزء من خطة استمرارية الأعمال والتعافي من الكوارث.
- ثالثاً: بعيداً عن حالات اختراق المفاتيح، تحدد الشركة إجراءات التعافي المستخدمة في حال تلف موارد الحوسبة، أو البرمجيات، و/أو البيانات، أو الاشتباه في تلفها.

5.7.1.2 خطط الإلغاء الجماعي (Mass Revocation Plans)

تلتزم شركة مصدر التكنولوجيا بالحفاظ على خطة شاملة وقابلة للتنفيذ للإلغاء الجماعي، تحدد إجراءات واضحة لضمان استجابة سريعة ومتسقة وموثوقة لأحداث إلغاء الشهادات واسعة النطاق.

- لا تُطالب الشركة بالكشف علناً عن تفاصيل خطة الإلغاء الجماعي أو إجراءاتها التفصيلية، ولكن يجب تقديمها للمدققين عند الطلب.

- تخضع الخطة للاختبار والمراجعة والتحديث سنوياً لاستيعاب الدروس المستفادة والمتطلبات التشغيلية والأمنية المتطورة.
- تغطي خطة الإلغاء الجماعي، كحد أدنى، الأحكام التالية:

1. معايير التفعيل: تحديد عتبات محددة وموضوعية وقابلة للقياس يتم بموجبها تفعيل خطة الإلغاء الجماعي بناءً على ملف المخاطر، وحجم الإصدار، والقدرات التشغيلية.
2. معلومات الاتصال بالعملاء: كيفية تخزين وصيانة وتحديث بيانات الاتصال الخاصة بالمشتركين والعملاء.
3. نقاط الأتمتة: العمليات المؤتمتة (أو التي يمكن أتمتتها) والعمليات التي تتطلب تدخلاً بشرياً.
4. الأهداف والجدول الزمني: لتصنيف الحوادث، وبدء الإلغاء، واستبدال الشهادات، ومراجعة ما بعد الحدث.
5. طرق إخطار المشتركين: الآليات المتبعة لإبلاغ المشتركين المتأثرين.
6. توزيع الأدوار: مهام ومسؤوليات الموظفين المسؤولين عن إطلاق وتنسيق وتنفيذ الخطة.
7. التدريب والتعليم: أنشطة التدريب والتوعية والجاهزية للموظفين المسؤولين عن الخطة أو الداعمين لها.

5.7.2 إجراءات الاستعادة في حال تلف الموارد الحاسوبية أو البرمجيات أو البيانات

تنفذ شركة مصدر التكنولوجيا (TS) التدابير اللازمة لضمان الاستعادة الكاملة لخدمات هيئات التصديق التابعة لها في حال وقوع كارثة أو تلف في الخوادم أو البرمجيات أو البيانات ويخضع ذلك لتفويض مجلس حوكمة البنية التحتية للمفاتيح العامة التابع لـ TSلتفعيل إجراءات الاستجابة للحوادث.

تحدّد وثيقة خطة استمرارية الأعمال والتعافي من الكوارث الخاصة بهيئات التصديق التابعة التابعة لـ TSالظروف التي تستدعي تفعيل هذه الإجراءات والتي قد تتضمن استخدام موقع التعافي من الكوارث عند الحاجة.

تُختبر خطة استمرارية الأعمال والتعافي من الكوارث لهيئات التصديق التابعة التابعة لـ TSمرة واحدة على الأقل سنوياً وتشمل سيناريوهات التحول التلقائي إلى موقع التعافي من الكوارث.

5.7.3 إجراءات الاستعادة بعد اختراق المفتاح

للاطلاع على حالات اختراق مفاتيح المشتركين يُرجى مراجعة القسم 4.9.

يُعد اختراق المفتاح الخاص لهيئة التصديق TLS التابعة لـ TSأو بيانات التفعيل المرتبطة به أو شهادة مستجيبOCSP حادثاً بالغ الأهمية يستدعي تفعيل عملية وإجراءات مفصلة مبيّنة ضمن خطة استمرارية الأعمال والتعافي من الكوارث الخاصة بـTS.

نظراً لحساسية هذا النوع من الحوادث وتأثيره المباشر على البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI) يعقد مجلس حوكمة البنية التحتية للمفاتيح العامة التابع لـ TSاجتماعاً طارئاً لاتخاذ الإجراءات اللازمة والتعامل مع الجوانب الاتصالية وذلك وفقاً لخطة التعامل مع اختراق المفاتيح وإنهاء هيئات التصديق. راجع القسمين 4.9.1 و4.9.3 للمزيد من التفاصيل.

5.7.4 قدرات استمرارية الأعمال بعد وقوع كارثة

في حال حدوث كارثة أو تلف في الخوادم أو البرمجيات أو البيانات تُفعّل خطة استمرارية الأعمال والتعافي من الكوارث الخاصة بـ TS بهدف استعادة القدرات التشغيلية الأساسية لهيئة التصديق TLS التابعة لها خلال فترة زمنية مناسبة.

تركّز الخطة على استعادة الخدمات التالية سواء في الموقع الرئيسي أو في موقع التعافي من الكوارث:

- خدمات التصديق (إصدار الشهادات وإلغاؤها).
- المستودع العام الذي تُنشر فيه قوائم إلغاء الشهادات وشهادات هيئات التصديق.
- خدمات OCSP.

تُتاح سيناريوهات التحول التلقائي إلى موقع التعافي من الكوارث بفضل نظام النسخ الاحتياطي الخاص بهيئة التصديق TLS التابعة لTS والذي يتيح التكرار المستمر للبيانات الحرجة من الموقع الرئيسي إلى موقع التعافي. وتُتيح هذه الآلية استعادة الخدمات الحيوية لهيئة التصديق خلال فترة لا تتجاوز اثنتي عشرة (12) ساعة كحد أقصى من زمن الاستعادة(RTO) .

وتُحدّد خطة استمرارية الأعمال الخاصة بـ TSما يلي:

1. الشروط اللازمة لتفعيل الخطة.
2. الإجراءات الطارئة.
3. إجراءات الرجوع:
تتضمن الخطة إجراءات الرجوع إلى الأنظمة الأصلية أو إلى بيئة بديلة عند تعذر الاستعادة الكاملة في الموقع المتضرر لضمان استمرارية العمل في حالات الطوارئ الممتدة.
4. إجراءات الاستئناف: تحدد الخطة خطوات استئناف العمليات الاعتيادية بعد اكتمال عملية الاستعادة الأولية بما في ذلك التحقق من سلامة الأنظمة واستقرار البيئة التشغيلية.
5. جدول صيانة الخطة:
تشتمل الخطة على جدول زمني محدد لصيانتها وتحديثها دورياً لضمان ملاءمتها وتماشيها مع التغيرات التقنية والتشغيلية.
6. متطلبات التوعية والتعليم:
توفر شركة مصدر التكنولوجيا برامج توعوية وتدريبية دورية لجميع المعنيين لضمان فهمهم الكامل لدورهم ضمن خطة استمرارية الأعمال والتعافي من الكوارث.
7. مسؤوليات الأفراد:
تحدد الخطة بوضوح مسؤوليات كل فرد ضمن فرق الطوارئ وتشمل فرق الاستجابة والاستعادة والتوثيق والدعم الفني.
8. هدف وقت الاستعادة:(RTO)
تسعى الخطة إلى استعادة الخدمات الأساسية خلال مدة لا تتجاوز اثنتي عشرة (12) ساعة من وقت وقوع الحادث لضمان استمرارية العمليات الحيوية.
9. الاختبار الدوري لخطط الطوارئ:
تُجرى اختبارات منتظمة لخطط استمرارية الأعمال والتعافي من الكوارث بما في ذلك اختبارات التحول التلقائي إلى مواقع الطوارئ لضمان جهوزيتها الفعلية.
10. خطة استمرارية أو استعادة تشغيل هيئة التصديق TLS التابعة لـ:TS
تتضمن الخطة آليات استئناف أو استعادة العمليات التجارية الحيوية لهيئة التصديق TLS التابعة لـ TSبشكل سريع بعد أي انقطاع أو فشل في العمليات الأساسية.
11. اشتراط تخزين المواد التشفيرية الحساسة في موقع بديل:
يُشترط تخزين الأجهزة التشفيرية الآمنة ومواد التفعيل الخاصة بها في موقع بديل لضمان توفرها عند الحاجة للاستعادة.

12. تعريف الانقطاع المقبول للنظام ومدة الاستعادة:
تحدد الخطة معايير مقبولة لانقطاع الأنظمة ويُعد أي انقطاع يتجاوز هدف وقت الاستعادة المحدد حادثاً بالغ الأثر يتطلب تدخلاً فورياً.
13. وتيرة أخذ نسخ احتياطية من المعلومات والبرمجيات الحيوية:
تُأخذ النسخ الاحتياطية من البيانات والبرمجيات الحساسة بشكل يومي بالإضافة إلى نسخ إضافية قبل وبعد أي تغيير جوهري في البيئة التشغيلية.
14. المسافة بين مرافق الاستعادة والموقع الرئيسي:
تُحدَّد مرافق الاستعادة على مسافة مناسبة من الموقع الرئيسي لتقليل احتمالية تأثرهما بنفس الحادث.
15. الإجراءات الأمنية لحماية الموقع بعد الكارثة:
تتضمن الخطة إجراءات لتأمين الموقع المتأثر إلى أقصى حد ممكن خلال الفترة الانتقالية التي تسبق استعادة بيئة تشغيل آمنة سواء في الموقع الأصلي أو موقع بديل.

لا تُفصح شركة مصدر التكنولوجيا عن خطط استمرارية الأعمال للمشتركين أو الأطراف المعتمدة أو موردي البرمجيات التطبيقية إلا أنها توفّر خطة استمرارية الأعمال وخطط الأمان للمدققين عند الطلب.

5.8 إنهاء عمل هيئة التصديق أو هيئة التسجيل

يُنهى تقديم خدمات هيئة التصديق TLS التابعة لشركة مصدر التكنولوجيا في الحالات التالية:

أ) بقرار من الإدارة التنفيذية لشركة مصدر التكنولوجيا.
ب) بقرار مبرر من السلطة المشرفة الشركة العامة للاتصالات والمعلوماتية. (ITPC)
ت) بحكم قضائي نهائي وغير قابل للطعن.
ث) عند تصفية أو إنهاء عمليات هيئة التصديق التابعة لشركة مصدر التكنولوجيا.

عند اتخاذ مجلس حوكمة البنية التحتية للمفاتيح العامة لTS واللجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية (ITPC PMA) قراراً بضرورة إنهاء خدمات هيئة التصديقTLS ينفّذ مجلس الحوكمة خطة الإنهاء المتفق عليها مسبقاً مع اللجنة العليا لإدارة التوقيع الإلكتروني.

تغطي خطة الإنهاء الخاصة بـ TSعلى الأقل الجوانب التالية:

- تقديم إشعار خطي إلى اللجنة العليا لإدارة التوقيع الإلكتروني بنيتها التوقف عن تشغيل أنشطة هيئة التصديق مرفقاً بنسخة من خطة الإنهاء قبل موعد التوقف عن هذه الأنشطة بتسعين (90) يوماً على الأقل أو قبل تاريخ انتهاء صلاحية التفويض الخاص بشركة مصدر التكنولوجيا لتقديم خدمات هيئة التصديق متى ما كانت الشركة لا تنوي التقدم بطلب لتجديد التفويض.
- الترتيبات المعتمدة من شركة مصدر التكنولوجيا للاحتفاظ بسجلات السجلات المؤرشفة وفقاً لما ورد في القسم 5.5 .
- الترتيبات المعتمدة من مزود خدمات الثقة للحفاظ على روابط خدمات التحقق من الحالة المذكورة في الشهادات التي تظل سارية خلال الفترة المعنية بعد الإنهاء .
- نشر إعلانات حول نية شركة مصدر التكنولوجيا بإنهاء أنشطة هيئة التصديق لخوادمTLS قبل ما لا يقل عن ستين (60) يوماً من تاريخ الإنهاء الفعلي أو انتهاء صلاحية الترخيص أيهما يحدث أولاً وذلك في الصحف اليومية أو عبر

وسائل أخرى وبالطريقة التي تحددها لجنة إدارة سياسة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية .

- تنفيذ إجراءات الاتصال مع الأطراف ذات العلاقة بغرض نقل سجلات هيئة التصديق المؤرشفة إلى جهة وصاية مناسبة .
- وضع خطة لمساعدة المشتركين في شركة مصدر التكنولوجيا قدر الإمكان في الانتقال إلى مزود خدمات ثقة آخر إلغاء جميع الشهادات التي أصدرتها هذه الهيئة والتي لا تزال غير مُلغاة أو لم تنتهِ صلاحيتها بنهاية فترة الإشعار سواء طلب المشتركون إلغاءها أم لم يطلبوا .
- اتخاذ التدابير اللازمة لضمان أن التوقف عن تقديم الخدمات لا يؤدي إلى تعطيل المشتركين أو الأطراف المعتمدة تنفيذ ترتيبات كافية لضمان استمرارية صيانة الأنظمة وتدابيرالأمان الخاصة بالبيانات الحساسة والدقيقة.

6 الضوابط الأمنية التقنية

6.1 توليد وتثبيت أزواج المفاتيح

6.1.1 توليد أزواج المفاتيح

6.1.1.1 هيئة التصديق لخوادم TLS التابعة لشركة مصدر التكنولوجيا

يُولَّد زوج مفاتيح هيئة التصديق ويُخزَّن ضمن ذاكرة وحدة أمان المعدات (HSM) المعتمدة والمطابقة لمتطلبات القسم 6.2.11.

يتم تسجيل مراسيم توليد مفاتيح هيئة التصديق التابعة لمزود خدمات الثقة (TSP CA Key Generation Ceremonies)بالفيديو وحفظها في موقع آمن لأغراض التدقيق.

يشهد مراسيم توليد المفاتيح الخاصة بمزود خدمات الثقة مدقق داخلي أو خارجي بهدف إصدار رأي تقويمي يؤكد أنّ شركة مصدر التكنولوجيا:

1. وثقت إجراءات توليد وحماية مفاتيح هيئة التصديق الخاصة بها بما يتوافق مع بيان ممارسات الشهادات (CPS) وسياسة الشهادات (CP) الخاصة بمزود خدمات الثقة.
2. أدرجت التفاصيل المناسبة في نص سيناريو توليد مفاتيح هيئة التصديق.
3. نفذت مراسيم التوليد بحضور النصاب القانوني للأشخاص المخوَّلين بما يشمل ممثلين عن مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا(TS PKI GB) .
4. حافظت على ضوابط فعالة لتوفير ضمان معقول بأن زوج مفاتيح هيئة التصديق قد جرى توليده وحمايته بما يتوافق مع الإجراءات المُعلنة في بيان ممارسات الشهادات.
5. نفذت خلال عملية توليد مفاتيح هيئة التصديق جميع الإجراءات المطلوبة والمنصوص عليها في نص سيناريو توليد المفاتيح الخاص بهيئة التصديق.

6.1.1.2 توليد أزواج مفاتيح المشترك

تُولّد مفاتيح المشترك وفقاً للمتطلبات التالية:

نوع الشهادة	التحقق من هوية المنظمة (OV)
متطلبات إنشاء المفاتيح	يُنشئ الزوج المفتاحي باستخدام أداة إنشاء المفاتيح المُضمنة مع برنامج خادم الويب.

ترفض شركة مصدر التكنولوجيا طلب الشهادة إذا تحقق واحد أو أكثر من الشروط التالية:

1. لم يستوفِ الزوج المفتاحي المتطلبات المنصوص عليها في البندين 6.1.5 و 6.1.6.
2. وُجد دليل واضح على وجود خلل في الطريقة المستخدمة لتوليد المفتاح الخاص.
3. علمت هيئة التصديق بوجود طريقة مثبتة أو مثبت فعاليتها قد تؤدي إلى تعريض المفتاح الخاص للاختراق.
4. كانت هيئة التصديق قد علمت مسبقاً بأن المفتاح الخاص تعرّض لاختراق كما هو موضح في أحكام البند 4.9.1.1.

5. في حال علمت سلطة التصديق (CA) بوجود طريقة مؤكدة أو مثبتة تتيح احتساب المفتاح الخاص (Private Key) بسهولة استناداً إلى المفتاح العام (Public Key) المدرج في الشهادة؛ فإنه يجب عليها اتخاذ التدابير الاحترازية اللازمة، بما في ذلك التدابير المحددة في القسم (6.1.1.3، الفقرة 5) من المتطلبات الأساسية (Baseline Requirements)."

6.1.2 تسليم المفتاح الخاص إلى المشترك

لا تُنشئ شركة مصدر التكنولوجيا المفاتيح الخاصة للمشتركين في شهادات SSL المعتمدة علنياً ولا تُنفّذ إجراءات إيداع المفاتيح أو استردادها أو نسخها احتياطياً .وفي حال اكتشفت شركة مصدر التكنولوجيا أو اشتبهت بأن المفتاح الخاص للمشترك قد انشئ لشخص غير مخوّل أو إلى جهة غير تابعة للمشترك فإن الشركة تُلغي جميع الشهادات التي تتضمّن المفتاح العام المقابل لذلك المفتاح الخاص المُفشَى.

6.1.3 تسليم المفتاح العام إلى جهة إصدار الشهادات

تقبل هيئة التصديق طلبات إنشاء الشهادات (CSRs) فقط إذا جرى التحقق من صحتها عبر بوابة هيئة التسجيل الإلكترونية(Web RA Portal) .

6.1.4 تسليم المفتاح العام لهيئة التصديق إلى الأطراف المعتمدة

يتم نشر شهادات مفاتيح هيئات التصديق الخاصة بخدمة TLS ضمن المستودع العام لمصدر التكنولوجيا.

6.1.5 نوع الخوارزمية وأحجام المفاتيح

تُستخدم مفاتيح RSA بحجم 2048 بت أو 4096 بت (مُوصى به) للمشتركين .أما مفاتيح هيئة التصديق TLS التابعة لمصدر التكنولوجيا (TS TLS CA) فتستخدم ECDSA بحجم 384 بت.

6.1.6 إنشاء معلمات المفاتيح العامة والتحقق من جودتها

6.1.6.1 هيئة التصديق TS TLS CA

تتم عملية إنشاء المفاتيح الخاصة والعامة لهيئات التصديق باستخدام تقنيات متقدمة لإنشاء المعلمات. وتلبي أجهزة HSMالتابعة لهيئات التصديق التابعة لمصدر التكنولوجيا (TS Subordinate CAs) والبرمجيات المرتبطة بها متطلبات المعيار FIPS 186-2 فيما يتعلق بإنشاء الأرقام العشوائية وفحوصات أولية الأعداد. ويستند فريق عمليات البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا إلى القسم 6.1.6 من متطلبات القواعد الأساسية للتحقق من الجودة.

6.1.6.2 المشتركين

تستخدم هيئات التسجيل أساليب معقولة للتحقق من مدى ملاءمة المفاتيح العامة المُقدَّمة من قِبل المشتركين. ويتم فحص المفاتيح المعروفة بأنها ضعيفة ورفضها كما هو موضح في القسم 6.1.6 من متطلبات القواعد الأساسية لمنتدى CA/B.

6.1.7 أغراض استخدام المفتاح وفقاً لحقل استخدام المفتاح في X.509 v3

تتضمن الشهادات الصادرة عن هيئة التصديق هذه سلسلة بتات لاستخدام المفتاح وفقاً للوثيقة.[RFC 5280]
يرجى الرجوع إلى القسمين 7.1 و7.3 من بيان ممارسة الشهادات (CPS) هذا.

6.2 حماية المفتاح الخاص ووحدة التشفير والضوابط الهندسية

6.2.1 معايير وضوابط وحدة التشفير

يتم استخدام جهاز توليد المفاتيح الشفرية (HSMs) المعتمدة أو المتوافقة مع المستوى الثالث من المعيار FIPS 140-2 لإنشاء وتخزين المفاتيح الخاصة لهيئة التصديق. تُخزَّن أجهزة HSMضمن المنطقة الأمنية الأشد حماية في مرفق استضافة البنية التحتية للمفاتيح العامة(TS PKI) .

تُشفّر شركة مصدر التكنولوجيا مفتاحها الخاص باستخدام خوارزمية وطول مفتاح قادرين وفقاً لأحدث ما توصلت إليه التقنية على مقاومة الهجمات التحليلية التشفيرية طوال العمر المتبقي للمفتاح المشفَّر أو جزء منه.

6.2.2 التحكم المتعدد بالأشخاص في المفتاح الخاص n منm

تخضع المفاتيح الخاصة لهيئة التصديق لرقابة دائمة من قبل عدة أشخاص مخولين حيث تُوثَّق الأدوار الموثوقة ذات الصلة بإدارة مفاتيح هيئة التصديق (وأسرارها ذات الصلة) ضمن إجراءات مركز إدارة المفاتيح (TS KGC) وسائر الوثائق الداخلية.

يتم تعيين موظفي هيئة التصديق في الأدوار الموثوقة من قبل مجلس حوكمة البنية التحتية للمفاتيح العامة(TS PKI GB) لضمان فصل المهام وتطبيق مبادئ التحكم المتعدد والمعرفة المقسّمة .يُطبَّق التحكم المتعدد في مفاتيح هيئة التصديق الخاصة من خلال نظام معرفة مفتاح من نوع "m من n". ويعني ذلك وجوب تواجد عدد معين من الأشخاص(m) لا يقل عن اثنين (2) من بين عدد إجمالي (n) من الأشخاص والبالغ عددهم ثلاثة (3) حماة مفاتيح بشكل متزامن إلى جانب مسؤولي أجهزة HSM من أجل تفعيل أو إعادة تفعيل المفتاح الخاص لهيئات التصديق التابعة التابعة لمصدر التكنولوجيا . يحتفظ مجلس حوكمة البنية التحتية للمفاتيح العامة بسجلات مكتوبة وقابلة للتدقيق لتوزيع الرموز وكلمات المرور المرتبطة بها على العاملين الموثوقين وحماة المفاتيح .وفي حال تقرر استبدال أحد العاملين الموثوقين أو حماة المفاتيح يتابع المجلس عملية تجديد الرموز وتوزيع كلمات المرور.

6.2.3 إيداع المفتاح الخاص

لا تُودع المفاتيح الخاصة لهيئة التصديق. تُنفَّذ إجراءات مخصصة للنسخ الاحتياطي والاستعادة لمفاتيح هيئة التصديق الخاصة من قبل مجلس حوكمة البنية التحتية للمفاتيح العامة(TS PKI GB) .

6.2.4 النسخ الاحتياطي للمفتاح الخاص

يتم نسخ المفاتيح الخاصة لهيئة التصديق احتياطياً وتُخزَّن بأمان داخل خزائن مخصصة محفوظة في المناطق الأمنية الداخلية الأشد حماية في مرافق استضافة هيئات التصديق التابعة التابعة لمصدر التكنولوجيا .تُنفّذ عمليات النسخ الاحتياطي كجزء من مراسيم إنشاء المفاتيح الخاصة بهيئات التصديق التابعة. وتُنسخ مفاتيح هيئة التصديق لخدمة TLS التابعة لمصدر التكنولوجيا(TS TLS Cas) تحت ذات ضوابط التحكم المتعدد بالأشخاص.

تُستخدم المعرفة المقسّمة كعنصر أساسي للتحكم. وتخضع عملية استرجاع المفتاح الاحتياطي لنفس مبادئ التحكم المتعدد والمعرفة المقسّمة .تتضمن إجراءات مراسيم المفاتيح الخاصة بهيئة التصديق لخدمة TLS التابعة لمصدر التكنولوجيا (TS TLS CA) عملية نقل مادي للمفتاح الاحتياطي من مرفق الاستضافة الأساسي إلى مرفق التعافي من الكوارث .(DR) ويشارك موظفون مخصصون في أدوار موثوقة في عملية النقل هذه والتي تتم بمرافقة حرس أمني. كما تُؤخذ في الاعتبار الأحكام المنصوص عليها في القسم أثناء عملية النقل.

6.2.5 أرشفة المفتاح الخاص

لا يقوم مجلس حوكمة البنية التحتية للمفاتيح العامة (TS PKI GB) بأرشفة المفاتيح الخاصة لهيئات التصديق.

6.2.6 نقل المفتاح الخاص إلى وحدة التشفير أو منها

يُسمح فقط بنقل أزواج مفاتيح هيئة التصديق إلى وحدة تشفير أجهزة أخرى من نفس المواصفات كما هو موضح في القسم 6.2.11 من خلال عملية نسخ مباشر من وحدة إلى وحدة عبر مسار موثوق وتحت رقابة متعددة الأشخاص .ولا يتم في أي وقت نسخ المفاتيح الخاصة لهيئة التصديق إلى قرص أو أي وسائط أخرى خلال هذه العملية.

6.2.7 تخزين المفتاح الخاص في وحدة التشفير

لا توجد اشتراطات إضافية بخلاف تلك المنصوص عليها في البنود 6.2.1 6.2.2 6.2.4 و6.2.6.

6.2.8 طريقة تفعيل المفتاح الخاص

6.2.8.1 هيئة التصديق TS TLS CA

يُفعّل المفتاح الخاص وفقاً لمبادئ التحكم الثنائي والمعرفة المقسّمة. وتُستخدم في هذه العملية وحدة إدخال رقم سري (PIN)موصولة بوحدة HSM التابعة لهيئة التصديق.

6.2.8.2 المشتركين

يتحمل المشتركون مسؤولية تفعيل مفاتيحهم الثنائية وحمايتها وذلك وفقاً للالتزامات الواردة في شروط وأحكام المشترك.

6.2.9 طريقة إلغاء تفعيل المفتاح الخاص

6.2.9.1 هيئة التصديق TS TLS CA

تعمد شركة مصدر التكنولوجيا إلى إلغاء تفعيل مفاتيح هيئة التصديق الخاصة وفقاً لتعليمات ووثائق الشركة المصنّعة لوحدة أمان الأجهزة(HSM) .

6.2.9.2 المشتركين

يتحمل المشتركون مسؤولية إلغاء تفعيل مفاتيحهم الثنائية وحمايتها وذلك بما يتماشى مع الالتزامات المنصوص عليها في شروط وأحكام المشترك.

6.2.10 طريقة إتلاف المفتاح الخاص

6.2.10.1 هيئة التصديقTS TLS CA

"يخضع إجراء إتلاف المفتاح الخاص (Private Key) لسلطة التصديق في حالات خارج سياق انتهاء فترة صلاحيته لتحقيق دقيق وتفويض خاص من قبل مجلس إدارة البنية التحتية للمفاتيح العامة(TS PKI GB) ؛ حيث يتضمن قرار الإتلاف تحديد الموظفين المكلفين بالمهمة. وتتم عملية الإتلاف وفقاً لإجراءات موثقة وبحضور أفراد معينين في أدوار موثوقة (Trusted Roles)، على ألا يقل عددهم عن ثلاثة موظفين موثوقين، وبحضور ممثل واحد على الأقل من مجلس الإدارة (PKI GB)، بالإضافة إلى وجوب حضور مدقق مؤهل بصفة شاهد على عملية الإتلاف.

وتُعزز هذه الإجراءات مبدأ "الرقابة المتعددة (Multi-person control) "وتجزئة المعرفة Split knowledge كما تضمن الإجراءات إتلاف مفاتيح سلطة التصديق نهائياً من خلال مسحها بشكل دائم من أي وحدات برمجية أو أجهزة (Hardware Modules) تم خزن المفاتيح عليها".

6.2.10.2 المشتركين

يتحمل المشتركون مسؤولية إتلاف مفاتيحهم الخاصة وفقاً للالتزامات المنصوص عليها في شروط وأحكام المشترك. ويمكن للمشتركين حذف مفاتيحهم وشهاداتهم باستخدام البرامج المقدّمة من الشركة المُصنّعة المناسبة.

6.2.11 تصنيف وحدة التشفير

تُعد وحدات التشفير الخاصة بهيئة التصديق معتمدة/موثقة وفقاً للمستوى الثالث من معيار[FIPS 140-2] .

6.3 جوانب أخرى لإدارة أزواج المفاتيح

6.3.1 أرشفة المفتاح العام

يرجى الرجوع إلى البند 5.5 للاطلاع على شروط الأرشفة.

6.3.2 فترة تشغيل الشهادة وفترة استخدام زوج المفاتيح

تكون شهادات هيئة التصديق صالحة لمدة ست (6) سنوات مع فترة استخدام المفتاح لمدة ثلاث (3) سنوات.
تُحدد أقصى مدة لصلاحية شهادات المشتركين في القسم 7.1 .ولا يُستخدم المفتاح الخاص لهيئة التصديق التابعة بعد انتهاء صلاحية شهادة المفتاح العام المرتبطة به .وبالإضافة إلى ذلك لا يُستخدم لتوقيع شهادات الكيانات النهائية بعد انتهاء فترة استخدام المفتاح الخاص باستثناء لوائح إلغاء الشهادات (CRLs) وشهادات مستجيب حالة الشهادة عبر الإنترنت (OCSP) الخاصة بخدمة التحقق من حالة الشهادة .وتبلغ أقصى مدة صلاحية لشهادة كيان نهائي خاصة بالمشترك 398 يوماً .ولأغراض الحساب يُحسب اليوم على أنه 86,400 ثانية. ويُعتبر أي وقت يزيد عن ذلك بما في ذلك الكسور العشرية أو الثواني الكبيسة مدة إضافية.

ولهذا السبب لا ينبغي إصدار شهادات المشتركين لمدة الحد الأقصى المسموح به بشكل افتراضي من أجل مراعاة مثل هذه التعديلات الزمنية.

6.4 بيانات التفعيل

6.4.1 إنشاء بيانات التفعيل وتثبيتها

6.4.1.1 هيئة التصديقTS TLS CA

تُنشأ مفاتيح هيئة التصديق الخاصة وبيانات تفعيل أجهزة HSMأثناء مراسيم إنشاء المفاتيح الخاصة بها .يرجى الرجوع إلى القسمين 6.1.1 و6.2.8 من بيان ممارسة الشهادات (CPS) هذا لمزيد من التفاصيل.

6.4.1.2 المشتركين

يقوم المشتركون بإنشاء بيانات التفعيل الخاصة بمفاتيحهم الخاصة وحمايتها إلى الحد اللازم لمنع فقدانها أو سرقتها أو الكشف غير المصرّح به عنها أو استخدامها.
ويُعرض هذا الالتزام على المشتركين ضمن شروط وأحكام المشترك.

6.4.2 حماية بيانات التفعيل

6.4.2.1 هيئة التصديقTS TLS CA

تضمن سياسة إدارة مفاتيح هيئات التصديق التابعة ومراسيم المفاتيح التابعة لمصدر التكنولوجيا (TS Subordinate CAs) تطبيق مبادئ التحكم المتعدد والمعرفة المقسّمة بشكل دائم لحماية مفاتيح هيئة التصديق وبيانات تفعيل أجهزة HSM. وخلال مراسيم مركز إدارة المفاتيحKGCs)) تبقى بيانات التفعيل بعهدة موظفي هيئات التصديق التابعة المُعيّنين.
يرجى الرجوع إلى القسمين 6.1 و6.2 لمزيد من التفاصيل.

6.4.2.2 المشتركين

يحمي المشتركون بيانات التفعيل الخاصة بمفاتيحهم الخاصة بالقدر اللازم لمنع فقدانها أو سرقتها أو الكشف غير المصرّح به عنها أو استخدامها.
ويُعرض هذا الالتزام على المشتركين ضمن شروط وأحكام المشترك.

6.4.3 جوانب أخرى متعلقة ببيانات التفعيل

لا توجد اشتراطات.

6.5 ضوابط أمن الحاسوب

6.5.1 المتطلبات التقنية الخاصة بأمن الحاسوب

تضمن شركة مصدر التكنولوجيا تنفيذ ضوابط أمن الحاسوب بما يتوافق على الأقل مع المعايير التقنية وإرشادات تعزيز الأمان الصادرة عن الشركة المُصنّعة.
ويتم توثيق ضوابط أمن الحاسوب المُنفذة كجزء من الوثائق الداخلية الخاصة بسياسات هيئات التصديق التابعة التابعة لمصدر التكنولوجيا.

تخضع أنظمة هيئات التصديق التابعة التابعة لمصدر التكنولوجيا وعملياتها على وجه الخصوص لضوابط الأمان التالية:

1. فصل المهام وتطبيق التحكم الثنائي في عمليات هيئة التصديق.
2. تطبيق ضوابط الوصول الفيزيائي والمنطقي.
3. تدقيق الأحداث المرتبطة بالتطبيقات والأمن.
4. المراقبة المستمرة لأنظمة هيئات التصديق التابعة وحماية نقاط النهاية.
5. آليات النسخ الاحتياطي والاستعادة لعمليات هيئات التصديق التابعة.
6. تعزيز نظام تشغيل خوادم هيئات التصديق التابعة وفقاً لأفضل الممارسات وتوصيات الشركات المُصنّعة.
7. بنية أمان شبكيّة معمّقة تشمل جدران حماية خارجية وداخلية وجدران حماية لتطبيقات الويب ونظم كشف التسلل.
8. إدارة استباقية للتحديثات كجزء من عمليات هيئات التصديق التابعة.
9. تفرض أنظمة هيئات التصديق التابعة المصادقة متعددة العوامل على جميع الحسابات القادرة على تنفيذ إصدار الشهادات بشكل مباشر.

6.5.2 تصنيف أمن الحاسوب

تخضع الجوانب التقنية لأمن الحاسوب إلى تدقيقات دورية.

6.6 ضوابط الدورة الحياتية التقنية

6.6.1 ضوابط تطوير الأنظمة

يجب أن يتم شحن الأجهزة أو البرمجيات المُشتراة في حاويات مختومة ومضادة للعبث وأن تُركّب بواسطة موظفين مؤهلين.
ويجب الحصول على تحديثات الأجهزة والبرمجيات بنفس الطريقة التي تم بها الحصول على المعدات الأصلية.
ويُكلف موظفون موثوقون مخصصون بتنفيذ إعدادات هيئات التصديق التابعة وفقاً للإجراءات التشغيلية الموثقة.

تُختبر التطبيقات وتُطوَّر وتُطبَّق وفقاً لأفضل ممارسات تطوير البرمجيات وإدارة التغييرات المعتمدة في القطاع.
ولا يُنشر أي برنامج (أو تصحيح برمجي) أو جهاز في الأنظمة الحية قبل مروره عبر عمليات إدارة التغيير والتهيئة التي يفرضها فريق عمليات البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا.(TS PKI Operations) كما تخضع إعدادات أنظمة شركة مصدر التكنولوجيا لفحوصات دورية منتظمة، على ألا تتجاوز المدة الفاصلة بين فحص وآخر أسبوعاً واحداً كحد أقصى.

تُعزَّز جميع المنصات البرمجية والأجهزة المستخدمة في هيئات التصديق التابعة وفقاً لأفضل الممارسات المتبعة في القطاع وتوصيات الشركات المُصنّعة.

6.6.2 ضوابط إدارة الأمن

تُخصص الأجهزة والبرمجيات المُستخدمة في إعداد هيئات التصديق التابعة لأداء مهام هيئة التصديق فقط. ولا توجد أي تطبيقات أو أجهزة أو اتصالات شبكية أو برمجيات مكونة غير تابعة للبنية التحتية للمفاتيح العامة لمصدر التكنولوجيا (TS PKI)متصلة أو مثبّتة على أجهزة هيئات التصديق.

يُطبَّق إجراء لإدارة التهيئة لضمان توثيق وضبط تهيئة أنظمة هيئات التصديق التابعة وتعديلها وتحديثها من قبل إدارة عمليات البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا.

ويُطبَّق إجراء لإدارة الثغرات الأمنية لضمان فحص معدات هيئات التصديق التابعة للكشف عن الأكواد الخبيثة عند أول استخدام وبشكل دوري بعد ذلك .ويدعم إجراء إدارة الثغرات معالجة الثغرات الحرجة التي لم تُعالَج مسبقاً من قبل فريق عملياتTS PKI خلال مدة لا تتجاوز 96 ساعة من وقت اكتشافها.

6.6.3 ضوابط الأمان لدورة الحياة

يرجى الرجوع إلى القسم 6.6.1 للاطلاع على التفاصيل.

6.7 ضوابط أمن الشبكة

قامت شركة مصدر التكنولوجيا بتنفيذ بنية قوية لأمن الشبكة تتضمن جدران حماية مُدارة ونُظم كشف التسلل.
وقد جرى تقسيم الشبكة إلى عدة مناطق بناءً على العلاقة الوظيفية والمنطقية والفيزيائية بينها. وتُطبق حدود الشبكة للحد من الاتصال بين الأنظمة داخل المناطق المختلفة وكذلك الاتصال بين هذه المناطق مع قواعد تدعم فقط الخدمات والبروتوكولات والمنافذ والاتصالات التي حددتها هيئات التصديق التابعة على أنها ضرورية للعمليات مع تعطيل جميع الحسابات والتطبيقات والخدمات والبروتوكولات والمنافذ غير المُستخدمة في عمليات هيئات التصديق.

وتُحاط أنظمة الإصدار وأنظمة إدارة الشهادات وأنظمة دعم الأمن داخل منطقة شبكية عالية الأمان.

تُجرى عمليات فحص الثغرات (Vulnerability Scans) للشبكات بصفة دورية (ربع سنوية) على الأقل، كما تُجرى اختبارات الاختراق (Penetration Tests) سنوياً كحد أدنى. وتُحدد الجداول الزمنية لمعالجة الثغرات بناءً على مستوى خطورتها؛ حيث تتم معالجة الثغرات الحرجة (Critical) خلال 24 ساعة، والثغرات عالية الخطورة (High) خلال 48 ساعة، في حين تتم معالجة الثغرات ذات الخطورة المنخفضة والمتوسطة خلال 96 ساعة. ويتم توثيق أي استثناءات وإخضاعها لتقييم المخاطر وتسجيلها رسمياً.

6.8 خدمة ختم الوقت

تُزامَن مكونات هيئة التصديق TLS التابعة لمصدر التكنولوجيا (TS TLS CA) بانتظام مع خدمة وقت موثوقة.
ويُحقق إعداد خدمات ختم الوقت دقة تبلغ ±1 ثانية أو أفضل بالنسبة للتوقيت العالمي المنسق(UTC) .

7 ملفات الشهادات قوائم الإلغاء(CRL) ومستجيب حالة الشهادة عبر الإنترنت(OCSP)

7.1 ملف تعريف الشهادة

7.1.1 رقم الإصدار

تصدر هيئات التصديق التابعة التابعة لمصدر التكنولوجيا (TS Subordinate CAs) شهادات X.509 الإصدار الثالث كما هو مبيّن في الوثيقةRFC 5280 .

7.1.2 امتدادات الشهادة

تلتزم هيئة التصديق هذه بالوثيقة RFC 5280 ومتطلبات القواعد الأساسية في جميع الشهادات التي تصدرها. تتضمن شهادات هيئة التصديق التابعة وشهادات الكيانات النهائية امتداد "الاستخدام الموسّع للمفتاح" الذي يحتوي على أغراض استخدام المفتاح التالية:

- id-kp-serverAuth.
- id-kp-clientAuth.

ولا يجوز تضمين معرف الغرض ضمن الشهادات.

7.1.3 معرفات كائنات الخوارزميات

تُصدر الشهادات من قبل هيئة التصديق باستخدام الخوارزميات المشار إليها بواسطة معرّف الكائن التالي:(OID) (OIDs)

الخوارزمية	معرّف الكائنObject 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 صيغ الأسماء

7.1.4.1 ترميز الاسم

تصدر هيئة التصديق هذه الشهادات باستخدام صيغ أسماء تتوافق مع الوثيقة RFC 5280 ومع القسم 7.1.4 من متطلبات القواعد الأساسية.

7.1.4.2 معلومات الموضوع – شهادات المشتركين

تُحدد معلومات الموضوع المطبقة على شهادات TLS الخاصة بالكيانات النهائية في الجدول أدناه.
تصدر هيئة التصديق هذه شهادات TLS تتوافق فيها بيانات امتداد اسم الموضوع البديل ومحتوى حقول اسم الموضوع (Subject DN)مع التعاريف المقابلة لها كما وردت في القسم 7.1.4 من متطلبات القواعد الأساسية.
وبالإضافة إلى ذلك لن تحتوي السمات ضمن حقل الموضوع على بيانات وصفية فقط مثل الأحرف '.' أو '-' أو فراغ (' ') أو أي مؤشرات أخرى تدل على أن القيمة غائبة أو غير مكتملة أو غير قابلة للتطبيق.

اسم الموضوع البديل (Subject Alternative Name)	اسم الموضوع	نوع شهادة TLS
DNSName عنوان (IPAddress) IP	الاسم الشائع	شهادات TLS للتحقق التنظيمي
	اسم المنظمة	
	اسم المدينة أو اسم الولاية/المقاطعة	
	اسم الدولة	

7.1.4.3 معلومات الموضوع – شهادات هيئات التصديق التابعة

تتضمن شهادة هيئة التصديق التابعة التابعة لمصدر التكنولوجيا السمات التالية: الاسم الشائع اسم المنظمة واسم الدولة . ويُشكّل تجمع هذه البيانات مُعرّفاً فريداً يُميز هيئة التصديق عن غيرها من الهيئات.

7.1.5 قيود الأسماء

تلتزم شركة مصدر التكنولوجيا بمتطلبات القسم 7.1.5 من متطلبات القواعد الأساسية الخاصة بشهادات TLS المعتمدة علنياً.

7.1.6 معرّف كائن سياسة الشهادة

تستخدم شركة مصدر التكنولوجيا مخطط OID المحدد لسياسة البنية التحتية للمفاتيح العامة الوطنية العراقية.
يرجى الرجوع إلى قالب الشهادة التالي للاطلاع على مزيد من التفاصيل.تُدرج معرّفات الكائن (OIDs) المستخدمة ضمن ملفات تعريف الشهادات .وبالإضافة إلى ذلك تُستخدم معرّفات الكائن التالية أيضاً:

معرّف السياسة	الوصف
2.23.140.1.2.2	سياسة مخصصة لشهادات TLS للتحقق التنظيمي

7.1.7 استخدام امتداد قيود السياسة

لا توجد اشتراطات.

7.1.8 صياغة ودلالة مؤهِّل السياسة

تتضمن شهادة هيئة التصديق التابعة التابعة لمصدر التكنولوجيا مؤهِّلاً لسياسة CPS يُشير إلى بيان ممارسة الشهادات المعمول به.

7.1.9 دلالة المعالجة لامتداد سياسات الشهادات عند تمييزه كحرِج

لا توجد اشتراطات.

7.1.10 ملف تعريف شهادة TS TLS CA

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 TLS 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 TLS CA G1	UTF8 encoded

SubjectPublicKeyInfo	False	M	D		
AlgorithmIdentifier		M	D	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M	D		Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M	S		
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.itpc.gov.iq	OCSP responder URL
AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	http://pki.itpc.gov.iq /repository/cert/tls_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/tls_root_ca.crl	CRL download URL.

Subject Properties					
SubjectKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M	S		
keyCertSign, cRLSign		M	S	True	
Policy Properties					
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.2.2	CA/B BR Reserved Certificate Policy for OV TLS Certificates
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.16.368.1.1.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.itpc.gov.iq/repository/cps	
Extended Key Usage Properties					
extKeyUsage	False	M	S		
clientAuth, serverAuth		M	S	True	
Basic Constraints Properties					
basicConstraints	True	M	S		

	cA		M	S	True	
	pathLenConstraint		M	S	0	

7.1.11 ملف تعريف شهادات التحقق من المؤسسة(OV)

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	The issuing Subordinate CA Signature.	The issuing 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 TLS 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 + **[200]** days	Maximum 200 days validity allowed (Baseline Requirement)
Subject	False				
CountryName		M	D	Country Name	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
stateOrProvinceName		M/O	D	State Or Province	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.

localityName		M/O	D	Locality	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
OrganizationName		M	D	Organization name of the legal entity	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1)	
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	160-bit SHA-1 Hash of the Subordinate Issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.techsource.iq	OCSP responder URL

	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://pki.techsource.iq/repository/certs/ts_tls_ca.p7b	Subordinate Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/ts_tls_ca.crl	CRL download URL.
Key Usage Properties						
keyUsage		True	M			
	digitalSignature		M	S	True	RSA
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.23.140.1.2.2	CA/B BR Reserved Certificate Policy for OV Certificates
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.3	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.1.3.3.2	

Extended Key Usage Properties					
extKeyUsage	False	M			
serverAuth,		M	S	True	
Subject Alternative Name Properties					
subjectAlternativeName	False	M			
dNSName or iPAddress		M	D	dNSNames with verified ownership or IPv4 or IPv6 address with verified ownership	Contains either a Fully-Qualified Domain Name or Wildcard Domain Name or Contains an IPAddress

7.2 ملف تعريف قائمة إلغاء الشهادات(CRL)

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

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

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

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

7.2.1 رقم الإصدار

تدعم هيئة التصديق TS TLS إصدار قائمة إلغاء الشهادات (CRL) من النوع X.509 الإصدار 2 (راجع القسم 7.2 أعلاه).

7.2.2 امتدادات CRL وسجلات CRL

تقديم ملف تعريف CRL في القسم 7.2 أعلاه.

7.2.2.1 رمز السبب (OID 2.5.29.21)

يجوز استخدام حقل رمز السبب للشهادات المُلغاة. ويجب ألا يكون رمز السبب المستخدم غير محدد (0). وإذا استُخدم الرمز غير المحدد (0) فإن هيئة التصديق لا تُدرج إدخال رمز السبب في قائمة الإلغاءCRL)).

يجب عدم وضع علامة الامتداد هذا كامتداد حرج. ويجب على المشترك أو هيئة التصديق اختيار السبب الأنسب من بين الأسباب التالية:

1. **(1):** يشير إلى وجود علم أو اشتباه بأن المفتاح الخاص بالمشترك قد تعرّض للاختراق.
2. **(3):** يشير إلى أن اسم الموضوع أو أي معلومة تعريفية أخرى في الشهادة قد تغيّرت دون وجود ما يدعو للاشتباه في اختراق المفتاح الخاص للشهادة.
3. **(4):** يشير إلى أن الشهادة يتم استبدالها لأحد الأسباب التالية: طلب المشترك شهادة جديدة امتلاك هيئة التصديق دليل معقول بأن التحقق من ملكية أو صلاحية التحكم في اسم النطاق أو عنوان IP المدرج في الشهادة لم يعد موثوقاً أو إلغاء الشهادة لأسباب تتعلق بالامتثال مثل عدم توافقها مع متطلبات منتدى CA/Browser الأساسية أو مع بيان ممارسة الشهادات (CPS) هذا.
4. **(5):** يشير إلى أن الموقع الإلكتروني المرتبط بالشهادة قد أُغلق قبل تاريخ انتهاء صلاحيتها أو أن المشترك لم يعد يمتلك أو يتحكم باسم النطاق قبل انتهاء صلاحية الشهادة.
5. **(9):** يشير إلى وجود مخالفة من طرف المشترك لا ترتبط باختراق المفتاح مثل تقديم معلومات مضللة في طلب الشهادة أوعدم الوفاء بالتزامات مادية ضمن شروط وأحكام المشترك أو شروط الاستخدام.

يُعد السبب الافتراضي للإلغاء هو "غير محدد (0)" مما يعني عدم إدراج رمز السبب في CRL. ولا تستخدم هيئة التصديق رمز السبب **(6)**.

لا يُتاح رمز السبب **(9)**للمشترك.

إذا حصلت شركة مصدر التكنولوجيا على دليل على اختراق مفتاح لشهادة لا يحتوي إدخالها في CRL على امتداد أو يحتوي على رمز سبب غير **(1)** فقد تقوم الشركة بتحديث رمز السبب في CRL إلى **(1)**.

7.2.2.2 نقطة توزيع الإصدارات(OID 2.5.29.28)

لا تدعم قوائم إلغاء الشهادات (CRLs) امتداد نقطة توزيع الإصدارات(Issuing Distribution Point) .

7.3 ملف تعريف OCSP

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	CA's Signature.	CA's Signature.
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			

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

تنسيق استجابة OCSP

يصف ملف التعريف أدناه استجابة OCSP وفقاً للمواصفة6960 RFC :

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

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

		value According to ETSI EN 319 411-2 / CSS-6.3.10-10.
extended-revoked definition	Null	the responder supports the extended definition of the "revoked" status to also include non-issued certificates
signatureAlgorithm	Sha384withRSAEncryption	Signing algorithm
signature		signature value
certs		Certificate corresponding to the private key used to sign the response. Only OCSP responder certificate is included in the OCSP response.

7.3.1 رقم النسخة

وفقاً لملف تعريف شهادةOCSP القسم 7.3.

7.3.2 امتدادات OCSP

وفقاً لملف تعريف شهادةOCSP القسم 7.3.

8 التدقيق على الامتثال والتقييمات الأخرى

تتوافق الإجراءات الموضحة في هذا البيان مع المتطلبات المحددة في القسم 1 وتغطي جميع العناصر ذات الصلة من معايير البنية التحتية للمفاتيح العامة (PKI) المعتمدة في القطاعات الصناعية التي تنشط فيها شركة مصدر التكنولوجيا.

8.1 تواتر أو ظروف التقييم

تنظّم شركة مصدر التكنولوجيا تدقيقاً خارجياً وفق معيارWebTrust وذلك لضمان امتثالها للمتطلبات والمعايير والإجراءات ومستويات الخدمة المعمول بها ويتم ذلك مرة واحدة على الأقل سنوياً.

تقبل شركة مصدر التكنولوجيا إخضاع ممارساتها وإجراءاتها للتدقيق وتتيح تقرير التدقيق علناً في موعد لا يتجاوز ثلاثة أشهر من نهاية فترة التدقيق.

يقوم كل من مجلس حوكمة البنية التحتية للمفاتيح العامة (TS PKI GB) ومدير لجنة إدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية (ITPC PMA) بتقييم نتائج هذه التدقيقات قبل اعتمادها بشكل نهائي.

بالإضافة إلى ذلك تُجرى تدقيقات داخلية وفق خطة تدقيق معتمدة من قبل لجنة إدارة التوقيع الإلكتروني .(PMA) وفي ظروف خاصة مثل خرق أمني يمكن إجراء تدقيقات وتقييمات غير مخطط لها بطلب من اللجنة المذكورة.

8.2 هوية/مؤهلات المقيم

يُجري التدقيقات الخارجية مدققون مؤهلون يستوفون المتطلبات التالية:

- الاستقلال التام عن الجهة الخاضعة للتدقيق.
- القدرة على إجراء تدقيق يتماشى مع معايير WebTrust الخاصة بهيئات التصديق.
- امتلاك خبرات في تقنيات البنية التحتية للمفاتيح العامة وأدوات وتقنيات أمن المعلومات وتدقيق أمن تكنولوجيا المعلومات وخدمات إثبات الطرف الثالث.
- الحصول على ترخيص منWebTrust .
- الخضوع للقانون أو اللوائح الحكومية أو قواعد السلوك المهني.
- باستثناء وكالات التدقيق الحكومية الداخلية يجب أن يكون لدى المدققين تأمين مهني ضد المسؤولية أو الأخطاء والإغفال بحد أدنى مليون دولار أمريكي.

8.3 علاقة المقيم بالجهة المقيمة

فيما يتعلق بالتدقيق الداخلي تحتفظ شركة مصدر التكنولوجيا بوظيفة تدقيق مستقلة ضمن مجلس حوكمة البنية التحتية للمفاتيح العامة(TS PKI GB) ومنفصلة عن فريق عمليات البنية التحتية للمفاتيح العامة(TS PKI Operations) .

أما التدقيقات الخارجية فتُجريها جهات مستقلة من ممارسيWebTrust ولا يجوز أن يكون لهم أي ارتباط مباشر أو غير مباشر مع الشركة العامة للاتصالات والمعلوماتية (ITPC) أو أي طرف آخر لديه تضارب في المصالح في هذا السياق.

8.4 المواضيع التي يغطيها التقييم

تخضع هذه الهيئة التصديقية للتدقيق للتأكد من امتثالها للمعايير التالية:

- مبادئ ومعايير WebTrust لجهات التصديق(Certification Authorities) .

- مبادئ ومعايير WebTrust لجهات التصديق – أمن الشبكات.
- مبادئ ومعايير WebTrust لجهات التصديق – المتطلبات الأساسية لبروتوكولTLS .

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

8.5 الإجراءات المتخذة نتيجة وجود خلل

يُبلّغ مجلس حوكمة البنية التحتية للمفاتيح العامة (TS PKI GB) بجميع القضايا والملاحظات الناتجة عن التقييم.

وفيما يتعلق بتدقيق الامتثال لعمليات هيئة التصديق لشهاداتTLS (TS TLS CA) فإن أي استثناءات أو نواقص ملحوظة تُكتشف خلال عملية التدقيق تستوجب اتخاذ قرار بشأن الإجراءات اللازمة. ويتخذ مجلس TS PKI GB هذا القرار بالتشاور مع المدقق.

في حال وجود استثناءات أو نواقص يتحمل مجلس TS PKI GB مسؤولية وضع وتنفيذ خطة إجراءات تصحيحية. وبعد تنفيذ الخطة يباشر المجلس تدقيقاً إضافياً لضمان معالجة النواقص المُحددة.

8.6 إيصال نتائج التدقيق

يعكس مجلس TS PKI GB النتائج الإجمالية للتدقيق في المستودع العام لمصدر التكنولوجيا.

أما تقارير التدقيق الداخلي فيُبلّغ بها مجلسTS PKI GB ولا تُفصح لأي أطراف ثالثة غير مخولة.

تُتاح تقارير تدقيق WebTrust للجمهور في موعد لا يتجاوز ثلاثة (3) أشهر من نهاية فترة التدقيق. وفي حال حدوث تأخير يتجاوز هذه المدة تُقدّم شركة مصدر التكنولوجيا رسالة توضيحية موقعة من قبل المدقق المؤهل.

يمكن الاطلاع على تقارير تدقيق WebTrust الخاصة بمصدر التكنولوجيا من خلال الرابط التالي:
https://pki.techsource.iq.

8.7 التدقيقات الذاتية

تراقب شركة مصدر التكنولوجيا من خلال وظيفة الامتثال الخاصة بها مدى التزامها الصارم بالإجراءات المدرجة في هذا البيان وبمتطلبات الخط الأساس من خلال إجراء تدقيقات داخلية دورية (مرة واحدة على الأقل كل ربع سنة).

وتشمل هذه التدقيقات عينات عشوائية تغطي ما لا يقل عن 3% من شهادات TLS المُصدرة منذ آخر تدقيق داخلي.

9 مسائل تجارية وقانونية أخرى

9.1 الرسوم

9.1.1 رسوم إصدار أو تجديد الشهادات
يُتفق على الرسوم المعتمدة إن وُجدت بين شركة مصدر التكنولوجيا والمشتركين.

9.1.2 رسوم الوصول إلى الشهادات
لا توجد أحكام.

9.1.3 رسوم الوصول إلى معلومات الإلغاء أو حالة الشهادة
لا تُفرض أي رسوم على الوصول إلى معلومات إلغاء الشهادات أو حالتها.

9.1.4 رسوم الخدمات الأخرى
يجوز لشركة مصدر التكنولوجيا فرض رسوم على خدمات أخرى وفقاً لاحتياجات العمل.

9.1.5 سياسة الاسترداد
لا تُعاد أي رسوم مدفوعة.

9.2 المسؤولية المالية

9.2.1 التغطية التأمينية
تضمن شركة مصدر التكنولوجيا شمول هذه الهيئة التصديقية بالتغطيات التأمينية القائمة.

9.2.2 الأصول الأخرى
لا توجد أحكام.

9.2.3 التغطية التأمينية أو الضمانات للجهات النهائية
يُرجى الرجوع إلى القسم 9.6.1.

9.3 سرية المعلومات التجارية

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

- المعلومات الشخصية للمشترك التي لا تظهر ضمن الشهادات أو قوائم إلغاء الشهادات(CRLs) .
- المراسلات بين المشترك ووظيفة هيئة التسجيل أثناء معالجة إدارة الشهادات (بما يشمل بيانات المشترك التي جُمعت).
- الاتفاقيات التعاقدية بين شركة مصدر التكنولوجيا والموردين.
- الوثائق الداخلية لشركة مصدر التكنولوجيا (عمليات العمل العمليات التشغيلية...).
- المعلومات السرية الخاصة بالموظفين.

9.3.2 المعلومات الخارجة عن نطاق المعلومات السرية

تُعدّ أي معلومات لا تُعرّفها شركة مصدر التكنولوجيا كمعلومات سرية معلومات عامة بما في ذلك المعلومات المنشورة في المستودع العام الخاص بها.

9.3.3 المسؤولية عن حماية المعلومات السرية

تحمي شركة مصدر التكنولوجيا المعلومات السرية من خلال تدريب الموظفين والمقاولين والمورّدين وتطبيق السياسات المعتمدة.

9.4 خصوصية المعلومات الشخصية

9.4.1 خطة الخصوصية

تراعي شركة مصدر التكنولوجيا قواعد خصوصية البيانات الشخصية وسريتها على النحو الوارد في هذا البيان. ويُنفّذ مجلس حوكمة البنية التحتية للمفاتيح العامة (TS PKI GB) هذه الأحكام من خلال هيئة التسجيل(TS RA) .

يُرجى الرجوع إلى القسم 9.4.2 لتحديد نطاق المعلومات الخاصة وإلى القسم 9.4.3 لتحديد العناصر غير المصنفة كمعلومات خاصة.

يمكن أن تخضع المعلومات الخاصة وغير الخاصة على حد سواء لقواعد خصوصية البيانات في حال احتوائها على بيانات شخصية.

يُسمح فقط لموظفين موثوقين ومخوّلين بالوصول إلى المعلومات الخاصة بالمشتركين بهدف إدارة دورة حياة الشهادة.

تحترم شركة مصدر التكنولوجيا جميع القوانين والأنظمة المعمول بها بشأن الخصوصية والمعلومات الخاصة وأينما انطبق أسرار التجارة بالإضافة إلى سياسة الخصوصية المنشورة لديها في ما يتعلق بجمع واستخدام والاحتفاظ والكشف عن المعلومات غير العامة.

ولا تكشف شركة مصدر التكنولوجيا عن المعلومات الخاصة للمشتركين باستثناء المعلومات المتعلقة بهم أنفسهم وذلك فقط في إطار الاتفاقية التعاقدية المبرمة بين الشركة العامة للاتصالات والمعلوماتية (ITPC) والمشتركين.

لن تفصح شركة مصدر التكنولوجيا عن أي معلومات خاصة دون موافقة صاحب البيانات الشرعي أو تفويض صريح بأمر قضائي. وعند الإفصاح عن معلومات خاصة ستتخذ الشركة الوسائل المعقولة لضمان استخدام هذه المعلومات فقط للأغراض المطلوبة.

ويجب على الجهات التي يُمنح لها حق الوصول أن تؤمّن البيانات الخاصة من أي خرق وألا تستخدمها أو تفصح عنها لأي طرف ثالث. كما يجب على هذه الجهات الالتزام بقواعد خصوصية البيانات الشخصية وفقاً للقوانين ذات الصلة في جمهورية العراق.

تضمن جميع قنوات الاتصال مع شركة مصدر التكنولوجيا الحفاظ على خصوصية وسرية أي معلومات خاصة متبادلة. وتُستخدم تقنيات التشفير عند استخدام قنوات الاتصال الإلكترونية مع أنظمة هيئة التصديق لشهادات TLS (TS TLS CA).

- الاتصالات بين أنظمة هيئة التسجيل (TS RA) والمشتركين.

- الاتصالات بين هيئة التسجيل (TS RA) وأنظمة هيئة التصديق(CA) .
- الجلسات المخصصة لتسليم الشهادات.

9.4.2 المعلومات التي تُعامل كمعلومات خاصة

تُعتبر جميع المعلومات الشخصية التي لا تتوفر علنًا ضمن محتوى الشهادة أو قائمة إلغاء الشهادات (CRL) معلومات خاصة.

9.4.3 المعلومات التي لا تُعتبر خاصة

لا تُعد المعلومات المُدرجة في الشهادة أو في قائمة إلغاء الشهادات (CRL) معلومات خاصة.

9.4.4 المسؤولية عن حماية المعلومات الخاصة'

يتعامل موظفو البنية التحتية للمفاتيح العامةTS PKI)) والموردون والمقاولون مع المعلومات الشخصية بسرية تامة بموجب الالتزامات التعاقدية مع شركة مصدر التكنولوجيا على أن تكون هذه الالتزامات على الأقل بنفس مستوى الحماية الوارد في القسم 9.4.1.

9.4.5 الإشعار والموافقة على استخدام المعلومات الخاصة

تضمن شركة مصدر التكنولوجيا استخدام المعلومات الشخصية التي يتم جمعها حصراً لغرض إدارة دورة حياة الشهادة وبما يتوافق مع موافقة المشتركين.

9.4.6 الإفصاح بموجب إجراء قضائي أو إداري

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

9.4.7 ظروف أخرى للإفصاح عن المعلومات

لا توجد أحكام.

9.5 حقوق الملكية الفكرية

تحتفظ شركة مصدر التكنولوجيا بجميع حقوق الملكية الفكرية المتعلقة بقاعدة بياناتها ومواقعها الإلكترونية وشهادات هيئات التصديق الصادرة عنها وأي منشورات أخرى صادرة عن البنية التحتية للمفاتيح العامة(PKI) بما في ذلك هذا البيان (CPS).

عند استخدام شركة مصدر التكنولوجيا لأي برامج من مورّدين خارجيين تبقى هذه البرامج مملوكة ملكية فكرية لمورّديها ويخضع استخدامها من قبل هيئات التصديق التابعة لشركة مصدر التكنولوجيا لاتفاقيات الترخيص المبرمة بين الشركة وهؤلاء المورّدين.

9.6 الإقرارات والضمانات

9.6.1 إقرارات وضمانات هيئة التصديق

عند إصدار شهادة تقدم هيئة التصديق (CA) الضمانات التالية إلى المستفيدين من الشهادة:

- المشترك الذي يُعد طرفاً في شروط وأحكام المشترك.
- جميع موردي برمجيات التطبيقات الذين تبرم معهم الهيئة الجذرية الوطنية العراقية اتفاقيات لإدراج شهادتها الجذرية في البرمجيات التي يوزعها هؤلاء الموردون.
- وجميع الأطراف المعتمدة التي تعتمد بشكل معقول على شهادة صالحة.

تُقر شركة مصدر التكنولوجيا وتضمن للمستفيدين من الشهادات بأنه خلال فترة صلاحية الشهادة تكون هيئة التصديق لشهادات TLS التابعة لها (TS TLS CA) قد التزمت بمتطلبات الخط الأساس وبيان ممارسة الشهادات (CPS) الخاص بها أثناء إصدار وإدارة الشهادة.

وتتضمن ضمانات الشهادة على وجه التحديد دون حصر ما يلي:

- حق استخدام اسم النطاق أو عنوانIP :

عند إصدار الشهادة تكون هيئة التصديق TS TLS CA قد:

1. نفّذت إجراءً للتحقق من أن المتقدم بالطلب يمتلك الحق في استخدام أو يتحكم في أسماء النطاقات أو عناوينIP المدرجة في حقل subject وامتداد subjectAltName في الشهادة (أو فقط في حالة أسماء النطاقات قد مُنح هذا الحق أو التحكم من طرف يمتلكه قانوناً).
2. التزمت بتنفيذ هذا الإجراء أثناء إصدار الشهادة.
3. وصفت هذا الإجراء بدقة في سياسة الشهادات وبيان ممارسة الشهادات الخاصة بها.

- تفويض إصدار الشهادة:

عند إصدار الشهادة تكون هيئة التصديق TS TLS CA قد:

1. نفّذت إجراءً للتحقق من أن الكيان موضوع الشهادة قد فوّض إصدار الشهادة وأن ممثل المتقدم بالطلب مخوّل لتقديم الطلب نيابة عن الكيان.
2. التزمت بتنفيذ هذا الإجراء أثناء إصدار الشهادة.
3. وصفت هذا الإجراء بدقة في بيان ممارسة الشهادات(CPS) .

- دقة المعلومات:

عند إصدار الشهادة تكون هيئة التصديق TS TLS CA قد:

1. نفّذت إجراءً للتحقق من دقة جميع المعلومات الواردة في الشهادة (باستثناء سمة organizationalUnitName ضمن حقل.
2. التزمت بتنفيذ هذا الإجراء أثناء إصدار الشهادة.
3. وصفت هذا الإجراء بدقة في بيان ممارسة الشهادات(CPS) .

- هوية المتقدم بالطلب:

في حال احتواء الشهادة على معلومات تعريفية عن الكيان تكون هيئة التصديق TS TLS CA قد:

1. نفّذت إجراءً للتحقق من هوية المتقدم بالطلب وفقاً لأحكام القسمين 3.2 و11.2.
2. التزمت بتنفيذ هذا الإجراء أثناء إصدار الشهادة.

3. وصفت هذا الإجراء بدقة في بيان ممارسة الشهادات(CPS) .

- شروط وأحكام المشترك :إذا لم تكن هيئة التصديق TS TLS والمشترك كيانين تابعين لبعضهما فإن المشترك وهيئة التصديق يُعدان طرفين في اتفاقية مشترك قانونية وسارية وقابلة للتنفيذ وتفي بهذه المتطلبات وإذا كانت هيئة التصديق والمشترك كياناً واحداً أو كيانين تابعين فإن ممثل المتقدم بالطلب يكون قد أقر بشروط الاستخدام.
- الحالة :تحتفظ هيئة التصديق TS TLS بمستودع إلكتروني متاح للجمهور على مدار الساعة يحتوي على معلومات محدثة حول حالة (صالحة أو ملغاة) جميع الشهادات غير المنتهية.
- الإلغاء :تلتزم هيئة التصديق TS TLS بإلغاء الشهادة لأحد الأسباب المحددة في هذه المتطلبات.

9.6.2 إقرارات وضمانات هيئة التسجيل(RA)

تُقر شركة مصدر التكنولوجيا وتضمن أنها تؤدي وظائف هيئة التسجيل وفقاً للأحكام المنصوص عليها في بيان ممارسة الشهادات (CPS) هذا.

9.6.3 إقرارات وضمانات المشترك

تُنفذ شركة مصدر التكنولوجيا عملية لضمان أن كل اتفاقية مشترك أو شروط استخدام قابلة للتنفيذ قانوناً ضد المتقدم بالطلب. وفي كلتا الحالتين يجب أن تنطبق الاتفاقية على الشهادة التي ستُصدر استناداً إلى طلب الشهادة. وتُستخدم اتفاقية منفصلة لكل طلب شهادة. تتضمن شروط وأحكام المشترك أو شروط الاستخدام أحكاماً تُحمّل المتقدم بالطلب نفسه (أو يُقر بها المتقدم بالطلب نيابةً عن موكله أو وكيله ضمن علاقة تعاقد من الباطن أو خدمة استضافة) الالتزامات والضمانات التالية:

- دقة المعلومات :التزام وضمان بتقديم معلومات دقيقة وكاملة في جميع الأوقات إلى هيئة التسجيل TS سواء في طلب الشهادة أو عند طلبها في سياق إصدار الشهادات من قبل هذه الهيئة.
- حماية المفتاح الخاص :التزام وضمان من المتقدم بالطلب باتخاذ جميع التدابير المعقولة لضمان التحكم بالمفتاح الخاص المقابل للمفتاح العام الذي سيتم تضمينه في الشهادة المطلوبة والحفاظ على سريته وحمايته بشكل مناسب في جميع الأوقات (بما في ذلك أي بيانات أو أجهزة تفعيل مرتبطة مثل كلمة المرور أو الرمز المميز).
- قبول الشهادة :التزام وضمان بأن المشترك سيقوم بمراجعة محتوى الشهادة والتحقق من دقته.
- استخدام الشهادة :عند طلب شهادات لأشخاص طبيعيين أو اعتباريين يلتزم ويضمن المشترك باستخدام الشهادة فقط بما يتوافق مع القوانين المعمول بها ووفقاً لشروط وأحكام المشترك أو شروط الاستخدام.
- الإبلاغ والإلغاء :التزام وضمان بالقيام بما يلي: (أ) طلب إلغاء الشهادة فوراً والتوقف عن استخدامها وعن استخدام المفتاح الخاص المرتبط بها في حال وقوع أو الاشتباه بوقوع إساءة استخدام أو اختراق للمفتاح الخاص للمشترك.
- الإبلاغ والإلغاء (متابعة):

(ب) الالتزام بطلب إلغاء الشهادة فوراً والتوقف عن استخدامها في حال تبيّن أن أية معلومات واردة في الشهادة غير صحيحة أو أصبحت كذلك.

- إنهاء استخدام الشهادة :التزام وضمان بالتوقف فوراً عن استخدام المفتاح الخاص المقابل للمفتاح العام المُدرج في الشهادة عند إلغاء تلك الشهادة بسبب اختراق المفتاح.
- الاستجابة :التزام بالاستجابة لتعليمات مصدر التكنولوجيا بشأن اختراق المفتاح أو إساءة استخدام الشهادة خلال فترة زمنية محددة.

- الإقرار والقبول :إقرار وقبول بأن لهيئة التسجيل TS الحق في إلغاء الشهادة فوراً إذا خالف المتقدم بالطلب شروط شروط وأحكام المشترك أو شروط الاستخدام أو إذا تطلب الإلغاء من قبل هيئة التصديق هذه أو متطلبات القواعد الأساسية.

9.6.4 إقرارات وضمانات الأطراف المعتمدة

على الأطراف المعتمدة التي تعتمد على الشهادات الصادرة عن مصدر التكنولوجيا:

- استخدام الشهادة للغرض الذي أُصدرت من أجله كما هو موضح في بيانات الشهادة (مثل امتداد استخدام المفتاح key usage).
- التحقق من صلاحية الشهادة والتأكد من أنها غير منتهية.
- تأسيس الثقة في هيئة التصديق التي أصدرت الشهادة من خلال التحقق من سلسلة الشهادات وفقاً للإرشادات المعتمدة في تعديل النسخة 3 من معيارX.509 .
- التأكد من أن الشهادة لم تُلغَ من خلال الوصول إلى حالة الإلغاء المحدثة من الموقع المحدد في الشهادة محل الاعتماد.
- التأكد من أن الشهادة توفر الضمانات الكافية لغرض استخدامها المقصود.

9.6.5 إقرارات وضمانات المشاركين الآخرين

لا توجد أحكام.

9.7 إخلاء المسؤولية عن الضمانات

في حدود ما يسمح به القانون العراقي واستثناءً من حالات الاحتيال أو الإساءة المتعمّدة لا تتحمل شركة مصدر التكنولوجيا المسؤولية عن ما يلي:

- دقة أي معلومات واردة في الشهادات، باستثناء ما يضمنه المشترك، وهو الطرف المسؤول عن صحة ودقة جميع البيانات المرسلة إلى مصدر التكنولوجيا بقصد إدراجها في شهادة هيئة إصدار الشهادات.
- الأضرار غير المباشرة الناتجة عن أو المتعلقة باستخدام أو تسليم أو ترخيص أو أداء أو عدم أداء الشهادات أو التوقيعات الرقمية.
- سوء السلوك المتعمد من جانب أي طرف ثالث مشارك يخالف أيًا من القوانين السارية في العراق، بما في ذلك على سبيل المثال لا الحصر، القوانين المتعلقة بحماية الملكية الفكرية، والبرمجيات الخبيثة، والوصول غير القانوني إلى أنظمة الحاسوب.
- أي أضرار تلحق بالمشتركين، سواء بشكل مباشر أو غير مباشر، نتيجة انقطاع خارج عن السيطرة لخدمات هيئة إصدار شهادات SSL/TLS.
- أي شكل من أشكال تحريف المعلومات من قبل المشتركين أو الأطراف المعتمدة على المعلومات الواردة في هذه الوثيقة أو أي وثائق أخرى صادرة عن مجلس (TS PKI GB) والمتعلقة بخدمات هيئة إصدار شهادات SSL/TLS.

9.8 حدود المسؤولية

- لا تتحمل شركة مصدر التكنولوجيا أي مسؤولية تجاه المشتركين في حال نتجت هذه المسؤولية عن إهمالهم أو احتيالهم أو سوء سلوكهم المتعمد.

- لا تتحمل شركة مصدر التكنولوجيا أي مسؤولية على الإطلاق فيما يتعلق باستخدام الشهادات أو أزواج المفاتيح العامة/الخاصة المرتبطة بها، الصادرة بموجب هذه الوثيقة، لأي استخدام آخر غير ما هو منصوص عليه فيها. يلتزم المشتركون بتعويض شركة مصدر التكنولوجيا فورًا عن أي مسؤولية أو تكاليف أو مطالبات تنشأ عن ذلك.
- لا تتحمل شركة مصدر التكنولوجيا أي مسؤولية تجاه أي طرف عن أي أضرار، سواء كانت مباشرة أو غير مباشرة، ناجمة عن انقطاع خدماتها لأسباب خارجة عن إرادتها.
- يتحمل المشتركون مسؤولية أي تحريف للمعلومات الواردة في الشهادة للأطراف المعتمدة، حتى وإن كانت شركة مصدر التكنولوجيا قد قبلت هذه المعلومات.
- يلتزم المشتركون بتعويض أي طرف معتمد يتكبد خسارة نتيجة إخلال مزود خدمات الاتصالات بشروط وأحكام استخدام المشترك.
- تتحمل الأطراف المعتمدة تبعات عدم وفائها بالتزاماتها.
- تنفي شركة مصدر التكنولوجيا أي مسؤولية مالية أو غيرها عن الأضرار أو الاختلالات الناتجة عن عمليات هيئة إصدار شهادات TLS التابعة لها.

9.9 التعويضات

غير مطبق.

9.10 المدة والإنهاء

9.10.1 المدة

تمت الموافقة على نظام حماية البيانات الحالي من قبل مجلس (TS PKI GB) ويظل ساري المفعول حتى يتم نشر التعديلات في المستودع العام للبنية التحتية للمفاتيح العامة.

9.10.2 الإنهاء

تُطبق التعديلات على هذه الوثيقة وتُعتمد من قبل مجلس (TS PKI GB) ويتم تمييزها بإصدار جديد من الوثيقة. عند نشرها في المستودع العام للبنية التحتية للمفاتيح العامة، يصبح الإصدار الأحدث ساري المفعول. كما يتم أرشفة الإصدارات الأقدم من هذه الوثيقة في المستودع العام للبنية التحتية للمفاتيح العامة.

9.10.3 أثر الإنهاء والنفاذ

يتولى مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا (TS PKI GB) التواصل بشأن شروط وأثر إنهاء بيان ممارسة الشهادات هذا باستخدام الآليات المناسبة.

9.11 الإشعارات والتواصل مع الأطراف الفردية

يمكن توجيه الإشعارات المتعلقة ببيان ممارسة الشهادات هذا إلى عنوان التواصل مع مجلس TS PKI GB المذكور في القسم 1.5.

9.12 التعديلات

عندما تستدعي الحاجة إجراء تغييرات على بيان ممارسة الشهادات هذا يُدرج مجلس TS PKI GB التغييرات ضمن إصدار جديد من المستند ويقوم بعد الموافقة عليه بنشر الإصدار الجديد. يحمل المستند الجديد رقماً جديداً للإصدار.

9.12.1 إجراءات التعديل

يُرجى الرجوع إلى القسم 9.12.

9.12.2 آلية الإشعار والفترة الزمنية

عند نشر النسخة الجديدة في المستودع العام لشركة مصدر التكنولوجيا تصبح سارية المفعول. وتُؤرشف النسخ السابقة من هذا المستند في نفس المستودع.

يتولى مجلس TS PKI GB تنسيق الاتصالات المتعلقة بتعديلات هذا البيان وما يترتب عليها من آثار.

يحتفظ مجلس TS PKI GB بحق تعديل بيان ممارسة الشهادات هذا دون إشعار مسبق في حال كانت التعديلات غير جوهرية بما في ذلك - على سبيل المثال لا الحصر - تصحيح الأخطاء المطبعية أو إدخال تحسينات طفيفة.

9.12.3 الظروف التي تستوجب تغييرOID

تحتفظ شركة مصدر التكنولوجيا بحق تعديل محتوى أي بيان ممارسة شهادات منشور. ولا يؤدي أي تعديل جوهري على هذا البيان إلى تغيير قيمة معرّف الكائن (OID) الخاصة به كما هو منشور في المستودع العام لشركة مصدر التكنولوجيا. وتعكس قيمة OID النسخة السارية والمعتمدة من هذا البيان.

9.13 أحكام تسوية النزاعات

تُحال جميع النزاعات المرتبطة بأحكام بيان ممارسة الشهادات هذا وخدمات هيئة التصديق لخوادم TLS التابعة لشركة مصدر التكنولوجيا بدايةً إلى القسم القانوني لمجلس TS PKI GB. وإذا لم تُثمر الوساطة التي يجريها هذا القسم تُحال النزاعات إلى المحاكم المختصة في جمهورية العراق.

9.14 القانون الحاكم

تخضع قابلية التنفيذ والتفسير والصياغة والصلاحية القانونية لبيان ممارسة الشهادات هذا لقوانين جمهورية العراق.

9.15 الامتثال للقوانين النافذة

يتوافق بيان ممارسة الشهادات هذا وتقديم خدمات هيئة التصديق لخوادم TLS التابعة لشركة مصدر التكنولوجيا مع القوانين ذات الصلة والنافذة في جمهورية العراق.

9.16 أحكام متنوعة

9.16.1 الاتفاق الكامل

لا يوجد نص محدد.

9.16.2 التنازل

باستثناء الحالات المنصوص عليها في عقود أخرى لا يجوز لأي طرف نقل أو تفويض الحقوق أو الالتزامات الواردة في بيان ممارسة الشهادات هذا دون موافقة خطية مسبقة من شركة مصدر التكنولوجيا.

9.16.3 القابلية للفصل

إذا تقرر أن أي حكم من أحكام هذا البيان غير صالح أو غير قابل للتنفيذ تبقى الأحكام الأخرى سارية المفعول حتى يتم تحديث هذا البيان.

في حال وجود تعارض بين متطلبات القواعد الأساسية وأي تنظيم قانوني في جمهورية العراق يجوز لشركة مصدر التكنولوجيا تعديل المتطلب المتعارض بالحد الأدنى اللازم لجعل المتطلب قانونياً وسارياً في العراق.

يُطبّق هذا فقط على العمليات أو إصدار الشهادات الخاضعة لذلك القانون. وفي هذه الحالة تُدرج شركة مصدر التكنولوجيا فوراً (وقبل إصدار أي شهادة بموجب المتطلب المعدل) مرجعاً مفصلاً في هذا القسم يتضمن القانون الذي استدعى التعديل والتعديل المحدد الذي نُفذ على متطلبات القواعد الأساسية.

كما تقوم شركة مصدر التكنولوجيا (وقبل إصدار الشهادة) بإبلاغ منتدى CA/Browser بالمعلومات المضافة حديثاً إلى بيان ممارسة الشهادات. ويُوقف العمل بأي تعديل أُجري بموجب هذا القسم عندما يصبح القانون غير نافذ أو عند تعديل متطلبات القواعد الأساسية بما يسمح بالامتثال لها وللقانون معاً. ويُنفذ التغيير المناسب في الممارسات وتعديل هذا البيان وإشعار منتدىCA/Browser خلال مدة لا تتجاوز 90 يوماً.

9.16.4 التنفيذ (أتعاب المحامين والتنازل عن الحقوق)

لا يوجد نص محدد.

9.16.5 القوة القاهرة

لا تتحمل شركة مصدر التكنولوجيا أي مسؤولية عن أي إخفاق أو تأخير في تنفيذ التزاماتها بموجب أحكام بيان ممارسة الشهادات هذا نتيجة أسباب خارجة عن نطاق سيطرتها المعقولة بما في ذلك - على سبيل المثال لا الحصر - عدم توفر خدمات الاتصالات أو انقطاعها أو تأخرها.

9.17 أحكام أخرى

غير قابل للتطبيق.