مصدر التكنولوجيا

لخدمات النظم والبرمجيات

والتجارة العامة المحدودة

البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI)

هيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIME

بيان ممارسة الشهادات

.

التحكم بالوثيقة

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

.

سجل التغييرات

الرقم التسلسلي	الإصدار	وصف التغييرات	
0.1	17/01/2023	النسخة الأولية	مصطفى طوير
0.2	23/02/2023	مراجعة داخلية وتحديث	أحمد إبراهيم
0.3	18/07/2023	تحديث في القسم 3.2.2	مصطفى طوير
0.4	04/12/2023	إضافة قيم OID ومعلومات الاتصال ورابط المستودع وتطبيق قالب مصدر التكنولوجيا	مصطفى طوير
0.5	28/02/2024	مراجعة وتحديث استناداً إلى ملاحظات المدقق على CP/CPS للهيئة الجذرية و CP لمزود خدمات الثقة.	مصطفى طوير وياسر خان
0.6	02/05/2024	• تحديث في القسم 5.4.1 لتوضيح البيانات الواجب تسجيلها ضمن متطلبات تسجيل أنشطة "الجدار الناري والموجهات". • تطبيق التغييرات المُدخلة في إصدار متطلبات S/MIME 1.0.3	مصطفى طوير
1.0	15/07/2024	تحديثات استناداً إلى توصيات المدقق بعد تدقيق نقطة في الزمن – مصطفى طوير وياسر خان	مصطفى طوير وياسر خان
1.1	15/09/2025	• المراجعة السنوية. • تصحيح الأخطاء المطبعية.	شركة مصدر التكنولوجيا

الرقم التسلسلي	الإصدار	وصف التغييرات	
1.2	03/06/2026	• تعديل يسمح لموظف هيئة التسجيل (RA) في شركة "مصدر التكنولوجيا" بالقيام بمهام هيئة التسجيل المحلية (LRA) نيابةً عن الجهات التي لم تقم بتعيين موظف هيئة تسجيل محلي(LRAO) ، أو التي ليس لديها القدرة على تعيينه. • تعديل لتحديث أمثلة الأدلة الثبوتية التكميلية (القسم 3.2.4). • تصحيح الأخطاء المطبعية. • تعديل لتغيير مصطلح "اتفاقية المشترك" إلى "شروط وأحكام استخدام المشترك."	شركة مصدر التكنولوجيا

.

الموافقة على الوثيقة

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

الفهرس

1 المقدمة 15
1.1 نظرة عامة 16
1.1.1 مجلس إدارة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا (TS PKI GB) 17
1.2 اسم المستند ومعرّفه 18
1.3 المشاركون في البنية التحتية للمفتاح العام 18
1.3.1 هيئات التصديق 18
1.3.2 هيئات التسجيل 19
1.3.3 المشتركون 20
1.3.4 الأطراف المعتمدة 20
1.3.5 مشاركون آخرون 20
1.4 استخدام الشهادات 20
1.4.1 الاستخدامات المسموح بها للشهادات 20
1.4.2 الاستخدامات المحظورة للشهادات 20
1.5 إدارة السياسات 21
1.5.1 الجهة المسؤولة عن إدارة المستند 21
1.5.2 الشخص المسؤول عن التواصل 21
1.5.3 الشخص المسؤول عن تحديد مدى ملاءمة هذا البيان للسياسة 21
1.5.4 إجراءات اعتماد بيان ممارسة الشهادات 22
1.6 التعاريف والاختصارات والمراجع 22
1.6.1 التعاريف 22
1.6.2 الاختصارات 28
1.6.3 المراجع (References) 30
2 المسؤوليات المتعلقة بالنشر والمستودعات 30
2.1 المستودعات 30
2.2 نشر معلومات الشهادات 30
2.3 توقيت أو تكرار النشر 31

2.3.1 شهادات هيئات التصديق 31
2.3.2 قوائم إلغاء الشهادات(CRLs) 31
2.4 ضوابط الوصول إلى المستودعات 31
3 التعريف والمصادقة 32
3.1 التسمية 32
3.1.1 أنواع الأسماء 32
3.1.2 الحاجة إلى أن تكون الأسماء ذات معنى 33
3.1.3 عدم الكشف عن الهوية أو استخدام الأسماء المستعارة من قبل المشتركين 33
3.1.4 قواعد تفسير أشكال الأسماء المختلفة..... 34
3.1.5 تفرّد الأسماء..... 34
3.1.6 التعرف والمصادقة ودور العلامات التجارية 34
3.2 التحقق الأولي من الهوية 34
3.2.1 طريقة إثبات امتلاك المفتاح الخاص..... 34
3.2.2 التحقق من صلاحية أو السيطرة على صندوق البريد الإلكتروني 35
3.2.3 مصادقة الهوية الفردية..... 35
3.2.4 معلومات المشترك غير المؤكدة..... 36
3.2.5 التحقق من الصلاحية 36
3.2.6 معايير التشغيل البيني..... 36
3.3 التحقق الأولي من الهوية والتعريف والمصادقة لطلبات إعادة إصدار المفاتيح 37
3.3.1 التحقق من الهوية والمصادقة لإعادة الإصدار الروتينية . 37
3.3.2 التحقق من الهوية والمصادقة لإعادة الإصدار بعد الإلغاء 37
3.4 التحقق من الهوية والمصادقة لطلبات الإلغاء..... 37
4 المتطلبات التشغيلية لدورة حياة الشهادة 38
4.1 طلب الشهادة..... 38
4.1.1 من يمكنه تقديم طلب الشهادة..... 38

4.1.2 عملية التسجيل والمسؤوليات 38
4.2 معالجة طلب الشهادة 39
4.2.1 تنفيذ وظائف التعريف والمصادقة 39
4.2.2 الموافقة على طلبات الشهادة أو رفضها 40
4.2.3 تخويل هيئة التصديق (CAA) 41
4.2.4 الوقت اللازم لمعالجة طلبات الشهادات 41
4.3 إصدار الشهادة 41
4.3.1 إجراءات هيئة التصديق أثناء إصدار الشهادة 41
4.3.2 إشعار المشترك بإصدار الشهادة من قبل هيئة التصديق . 42
4.4 قبول الشهادة 42
4.4.1 السلوك الذي يمثل قبول الشهادة 42
4.4.2 نشر الشهادة من قبل هيئة التصديق 42
4.4.3 إشعار جهات أخرى بإصدار الشهادة من قبل هيئة التصديق 42
4.5 استخدام زوج المفاتيح والشهادة 42
4.5.1 استخدام المفتاح الخاص بالمشترك والشهادة 42
4.5.2 استخدام المفتاح العام من قبل الطرف المعتمد 43
4.6 تجديد الشهادة 43
4.6.1 حالات تجديد الشهادة 43
4.6.2 من يمكنه طلب التجديد 43
4.6.3 معالجة طلبات تجديد الشهادة 43
4.6.4 إشعار المشترك بإصدار الشهادة الجديدة 43
4.6.5 السلوك الذي يمثل قبولاً للشهادة المجددة 43
4.6.6 نشر الشهادة المجددة من قبل هيئة التصديق 43
4.6.7 إشعار جهات أخرى بإصدار الشهادة المجددة من قبل هيئة التصديق 43
4.7 إعادة إصدار المفتاح 44
4.7.1 حالات إعادة إصدار المفتاح 44
4.7.2 من يمكنه طلب شهادة لمفتاح عام جديد 44

4.7.3 معالجة طلبات إعادة إصدار الشهادة 44
4.7.4 إشعار المشترك بإصدار الشهادة الجديدة 44
4.7.5 السلوك الذي يمثل قبولاً لشهادة أعيد إصدارها 44
4.7.6 نشر شهادة إعادة الإصدار من قبل هيئة التصديق 44
4.7.7 إشعار جهات أخرى بإصدار الشهادة المعاد إصدارها من قبل هيئة التصديق 44
4.8 تعديل الشهادة 44
4.8.1 حالات تعديل الشهادة 44
4.8.2 من يمكنه طلب تعديل الشهادة 44
4.8.3 معالجة طلبات تعديل الشهادة 44
4.8.4 إشعار المشترك بإصدار الشهادة المعدلة 45
4.8.5 السلوك الذي يمثل قبولاً للشهادة المعدلة 45
4.8.6 نشر الشهادة المعدلة من قبل هيئة التصديق 45
4.8.7 إشعار جهات أخرى بإصدار الشهادة المعدلة من قبل هيئة التصديق 45
4.9 إلغاء وتعليق الشهادة 45
4.9.1 حالات إلغاء شهادات المشتركين 45
4.9.2 من يمكنه طلب الإلغاء 46
4.9.3 إجراء طلب الإلغاء 47
4.9.4 فترة السماح لطلب الإلغاء 48
4.9.5 المدة التي يجب أن تُعالج خلالها هيئة التصديق طلب الإلغاء 48
4.9.6 متطلبات التحقق من الإلغاء للطرف المعتمد 48
4.9.7 تكرار إصدار قوائم الإلغاء CRL إن وُجد 48
4.9.8 الحد الأقصى لتأخير إصدار CRL إن وُجد 49
4.9.9 توفر التحقق من الإلغاء أو الحالة عبر الإنترنت 49
4.9.10 متطلبات التحقق من الإلغاء عبر الإنترنت 49
4.9.11 أشكال أخرى متاحة للإعلان عن الإلغاء 49
4.9.12 متطلبات خاصة باختراق المفتاح 49

4.9.13 الظروف التي تستدعي التعليق 50
4.9.14 من يمكنه طلب التعليق 50
4.9.15 إجراء طلب التعليق 50
4.9.16 حدود فترة التعليق 50
4.10 خدمات حالة الشهادة 50
4.10.1 الخصائص التشغيلية 50
4.10.2 توفر الخدمة 50
4.10.3 الخصائص الاختيارية 51
4.11 إنهاء الاشتراك 51
4.12 حفظ واستعادة المفاتيح 51
4.12.1 سياسة وممارسات حفظ واستعادة المفاتيح 51
4.12.2 سياسة وممارسات تغليف واستعادة مفاتيح الجلسة 51
5 الضوابط الخاصة بالمنشآت والإدارة والتشغيل 51
5.1 الضوابط الأمنية المادية 52
5.1.1 موقع المنشأة والبناء 52
5.1.2 الوصول المادي 52
5.1.3 الطاقة وتكييف الهواء 53
5.1.4 التعرض للمياه 53
5.1.5 الوقاية من الحرائق والحماية منها 53
5.1.6 تخزين الوسائط 53
5.1.7 التخلص من النفايات 53
5.1.8 النسخ الاحتياطي خارج الموقع 53
5.2 الضوابط الإجرائية 54
5.2.1 الأدوار الموثوقة 54
5.2.2 عدد الأشخاص المطلوب لكل مهمة 55
5.2.3 التحقق من الهوية والمصادقة لكل دور 55
5.2.4 الأدوار التي تتطلب الفصل في الواجبات 55
5.3 ضوابط الأفراد 55

5.3.1 المؤهلات والخبرة ومتطلبات التصريح 55
5.3.2 إجراءات التحقق من الخلفية 56
5.3.3 متطلبات التدريب 56
5.3.4 تواتر ومتطلبات التدريب المتكرر 56
5.3.5 تواتر وتتابع تناوب الوظائف 56
5.3.6 العقوبات على الأفعال غير المصرح بها 57
5.3.7 متطلبات المتعاقدين المستقلين 57
5.3.8 الوثائق المقدمة للموظفين 57
5.4 إجراءات تسجيل السجلات التدقيقية 57
5.4.1 أنواع الأحداث المسجلة: 57
5.4.2 تكرار مراجعة سجلات العمليات 59
5.4.3 فترة الاحتفاظ بسجلات التدقيق 59
5.4.4 حماية سجلات التدقيق 60
5.4.5 إجراءات النسخ الاحتياطي لسجلات التدقيق 60
5.4.6 نظام جمع سجلات التدقيق (الداخلي مقابل الخارجي) 60
5.4.7 الإخطار إلى مصدر الحدث 60
5.4.8 تقييمات الثغرات الأمنية 60
5.5 أرشفة السجلات 61
5.5.1 أنواع السجلات المؤرشفة 61
5.5.2 مدة الاحتفاظ بالأرشيف 61
5.5.3 حماية الأرشيف 61
5.5.4 إجراءات النسخ الاحتياطي للأرشيف 62
5.5.5 متطلبات ختم الوقت للسجلات 62
5.5.6 نظام جمع الأرشيف (داخلي أو خارجي) 62
5.5.7 إجراءات الحصول على معلومات الأرشيف والتحقق منها 62
5.6 تبديل المفاتيح 62
5.7 الاستجابة للاختراقات واستعادة القدرة التشغيلية بعد الكوارث 62

5.7.1 إجراءات التعامل مع الحوادث والاختراقات 62
5.7.2 تلف الموارد الحاسوبية أو البرمجيات أو البيانات 63
5.7.3 إجراءات اختراق المفتاح الخاص للجهة 63
5.7.4 قدرات استمرارية الأعمال بعد الكوارث..... 63
5.8 إنهاء عمل هيئة التصديق أو هيئة التسجيل 64
6 الضوابط الأمنية التقنية 65
6.1 توليد أزواج المفاتيح وتثبيتها 65
6.1.1 توليد أزواج المفاتيح 65
6.1.2 تسليم المفتاح الخاص إلى المشترك 66
6.1.3 تسليم المفتاح العام إلى هيئة التصديق 67
6.1.4 تسليم المفتاح العام لهيئة التصديق إلى الأطراف المعتمدة 67
6.1.5 أحجام المفاتيح..... 67
6.1.6 توليد معلمات المفتاح العام والتحقق من جودتها 67
6.1.7 أغراض استخدام المفاتيح (وفق حقلX.509 v3) 67
6.2 حماية المفاتيح الخاصة وضوابط هندسة وحدات التشفير 67
6.2.1 معايير وضوابط وحدات التشفير..... 67
6.2.2 التحكم المتعدد في المفاتيح الخاصة(nمنm) 67
6.2.3 إيداع المفتاح الخاص..... 68
6.2.4 النسخ الاحتياطي للمفتاح الخاص 68
6.2.5 أرشفة المفتاح الخاص 68
6.2.6 نقل المفتاح الخاص إلى أو من وحدة تشفير..... 68
6.2.7 تخزين المفتاح الخاص على وحدة تشفير 68
6.2.8 طريقة تفعيل المفتاح الخاص..... 68
6.2.9 طريقة إلغاء تفعيل المفتاح الخاص 69
6.2.10 طريقة إتلاف المفتاح الخاص 69
6.2.11 تصنيف وحدة التشفير 69
6.3 جوانب أخرى من إدارة زوج المفاتيح 69

6.3.1 أرشفة المفتاح العام 69
6.3.2 فترة التشغيل وفترة استخدام المفتاح لزوج الشهادات..... 69
6.4 بيانات التفعيل..... 70
6.4.1 توليد بيانات التفعيل وتثبيتها 70
6.4.2 حماية بيانات التفعيل..... 70
6.4.3 جوانب أخرى لبيانات التفعيل 70
6.5 ضوابط أمن الحاسوب..... 70
6.5.1 المتطلبات التقنية الخاصة بأمن الحاسوب 70
6.5.2 تقييم أمن الحاسوب 71
6.6 ضوابط تقنية لدورة الحياة..... 71
6.6.1 ضوابط تطوير الأنظمة 71
6.6.2 ضوابط إدارة الأمن..... 71
6.6.3 ضوابط أمن دورة الحياة 72
6.7 ضوابط أمن الشبكة 72
6.8 ختم الوقت..... 72
7 ملفات الشهادات وقوائم الإلغاء (CRL) وخدمة التحقق عبر الإنترنت(OCSP) 72
7.1 ملف تعريف الشهادة..... 72
7.1.1 رقم الإصدار..... 72
7.1.2 امتدادات الشهادة 72
7.1.3 معرفات كائنات الخوارزميات(Algorithm Object Identifiers) 73
7.1.4 تنسيقات الاسم..... 73
7.1.5 قيود الاسم 73
7.1.6 معرف كائن سياسة الشهادة 74
7.1.7 استخدام امتداد قيود السياسة..... 74
7.1.8 صياغة مؤهلات السياسة ودلالاتها..... 74
7.1.9 دلالات المعالجة لامتداد سياسات الشهادة الحرجة 74
7.1.10 ملف تعريف شهادة هيئة التصديق لشهادة البريد الإلكتروني الآمن التابعة لشركة مصدر التكنولوجيا 75

7.1.11 ملف تعريف شهادات البريد الإلكتروني الآمن 79
7.2 ملف تعريف قائمة إلغاء الشهادات 83
7.2.1 رقم الإصدار 85
7.2.2 امتدادات قائمة الإلغاء وإدخالاتها 85
7.3 ملف تعريف خدمة التحقق من الحالة عبر الإنترنت(OCSP) ... 85
7.3.1 رقم الإصدار 88
7.3.2 امتدادات OCSP 88
8 تدقيق الامتثال والتقييمات الأخرى 91
8.1 وتيرة أو ظروف التقييم 91
8.2 هوية أو مؤهلات المدقق 91
8.3 علاقة المدقق بالجهة الخاضعة للتدقيق 91
8.4 المواضيع المشمولة في التقييم 91
8.5 الإجراءات المتخذة نتيجة أوجه القصور 92
8.6 إيصال نتائج التدقيق 92
8.7 التدقيق الذاتي 92
9 شؤون قانونية وتجارية أخرى 93
9.1 الرسوم 93
9.1.1 رسوم إصدار الشهادات أو تجديدها 93
9.1.2 رسوم الوصول إلى الشهادات 93
9.1.3 رسوم إلغاء الشهادات أو الوصول إلى معلومات الحالة 93
9.1.4 رسوم الخدمات الأخرى 93
9.1.5 سياسة الاسترداد 93
9.2 المسؤولية المالية 93
9.2.1 تغطية التأمين 93
9.2.2 أصول أخرى 93
9.2.3 تغطية تأمينية أو ضمان للمشتركين النهائيين 93
9.3 سرية المعلومات التجارية 93
9.3.1 نطاق المعلومات السرية 93

9.3.2 المعلومات الخارجة عن نطاق السرية 94
9.3.3 المسؤولية عن حماية المعلومات السرية 94
9.4 خصوصية المعلومات الشخصية 94
9.4.1 خطة الخصوصية 94
9.4.2 المعلومات التي تُعامل على أنها خاصة 95
9.4.3 المعلومات غير المصنفة كمعلومات خاصة 95
9.4.4 مسؤولية حماية المعلومات الخاصة 95
9.4.5 الإخطار والموافقة على استخدام المعلومات الخاصة 95
9.4.6 الإفصاح بموجب إجراءات قضائية أو إدارية 95
9.4.7 ظروف أخرى للإفصاح عن المعلومات 95
9.5 حقوق الملكية الفكرية 95
9.6 الإقرارات والضمانات 95
9.6.1 إقرارات وضمانات هيئة التصديق 95
9.6.2 إقرارات وضمانات وظيفة التسجيل 96
9.6.3 إقرارات وضمانات المشترك 96
9.6.4 إقرارات وضمانات الأطراف المعتمدة 97
9.6.5 إقرارات وضمانات المشاركين الآخرين 97
9.7 إخلاء المسؤولية من الضمانات 97
9.8 حدود المسؤولية 98
9.9 التعويضات 98
9.10 المدة والإنهاء 98
9.10.1 المدة 98
9.10.2 الإنهاء 99
9.10.3 أثر الإنهاء والاستمرار 99
9.11 الإشعارات الفردية والتواصل مع المشاركين 99
9.12 التعديلات 99
9.12.1 إجراء التعديل 99
9.12.2 آلية الإخطار والفترة الزمنية 99

9.12.3 الحالات التي تستوجب تغيير معرف الكائن(OID) 99
9.13 أحكام تسوية النزاعات 99
9.14 القانون الناظم 100
9.15 الامتثال للقوانين المعمول بها 100
9.16 أحكام متنوعة 100
9.16.1 الاتفاق الكامل 100
9.16.2 التنازل أو التفويض 100
9.16.3 قابلية الفصل 100
9.16.4 التنفيذ (أتعاب المحاماة والتنازل عن الحقوق) 100
9.16.5 القوة القاهرة 100
9.17 أحكام أخرى 100

1 المقدمة

يمثل هذا المستند بيان ممارسة الشهادات (CPS) الذي يصف ممارسات التصديق المعمول بها لدى هيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIMEالتابعة لشركة مصدر التكنولوجيا (ويشار إليها لاحقاً بTS) .ويتوافق هذا البيان مع سياسة شهادات مزودي خدمات الثقة (TSP) المطبقة على تقديم خدمات التصديق التي يقدمها مزودو خدمات الثقة والذين يصدرون شهادات موثوقة علنياً للأطراف النهائية تحت إشراف البنية التحتية الوطنية للمفاتيح العامة العراقية (PKI).

يعالج هذا البيان السياسات التقنية والإجرائية والتنظيمية الخاصة بهيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIMEوالتي تنشئها وتديرها TS ضمن هيكل البنية التحتية الوطنية للمفتاح العام في العراق وذلك فيما يتعلق بكامل دورة حياة الشهادات الصادرة عن هذه الهيئة.

يشمل هذا البيان إصدار الشهادات والتحكمات المرتبطة بالأنواع التالية من الشهادات التي تصدرها هيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIME:

- شهادات البريد الإلكتروني الآمن S/MIME: الشهادات التي تصدر للأشخاص الطبيعيين لاستخدامها في توقيع البريد الإلكتروني وتشفيره.
- شهادة مستجيبOCSP : الشهادات المخصصة لمستجيب بروتوكول حالة الشهادات عبر الإنترنت (OCSP) لتوقيع استجابات OCSP المتعلقة بالشهادات الصادرة عن هيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIME.

يتوافق هذا البيان مع المتطلبات الرسمية لمجموعة مهام هندسة الإنترنت [RFC 3647] (IETF) فيما يخص الشكل والمحتوى. وعلى الرغم من إدراج عناوين بعض الفقرات وفقاً لبنية[RFC 3647] إلا أن بعض الموضوعات قد لا تنطبق فعلياً على تنفيذ خدمات البنية التحتية للمفتاح العام الخاصة بهذه الهيئة وتُحدد تلك الفقرات بعبارة "الفقرة غير قابلة للتطبيق".

يلتزم مجلس إدارة البنية التحتية للمفتاح العام التابع لـ TS بالحفاظ على هذا البيان بما يتوافق مع الإصدارات الحالية للمتطلبات المبينة أدناه والمنشورة على الرابط: http://www.cabforum.org.

- متطلبات أمان الشبكات وأنظمة الشهادات.
- المتطلبات الأساسية لإصدار وإدارة شهادات البريد الإلكتروني الآمن S/MIMEالموثوقة علنياً.

وفي حال وجود أي تعارض بين هذا المستند وبين المتطلبات المذكورة أعلاه فإن المتطلبات أعلاه هي التي تسود.

هذا البيان متاح للعامة. وكلما تمت الإشارة إلى معلومات سرية ضمن هذا النص فإن المقصود بذلك وثائق مصنفة متاحة فقط للأشخاص المخولين.

يمكن الحصول على معلومات إضافية حول هذا البيان من مجلس إدارة البنية التحتية للمفتاح العام التابع لـ TS باستخدام معلومات الاتصال الواردة في الفقرة 1.5.

1.1 نظرة عامة

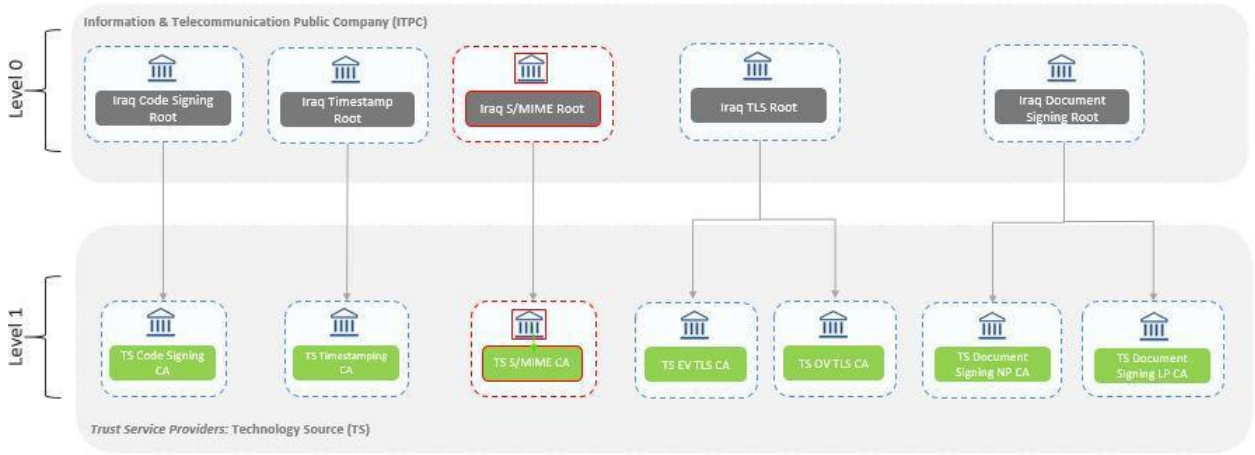
تأسست البنية التحتية الوطنية للمفتاح العام في العراق تحت إشراف الشركة العامة للاتصالات والمعلوماتية (ITPC) عبر عدة هيئات تصديق جذرية تمثل برنامج الجذر الوطني للبنية التحتية للمفتاح العام. ومن خلال هذه البنية الوطنية تهدف الحكومة العراقية إلى توفير إطار يُسهم في إنشاء مزودي خدمات الثقة الذين يقدمون خدمات التصديق الرقمي والخدمات الموثوقة للجهات الحكومية وغير الحكومية. وتتكون هرمية البنية التحتية للمفتاح العام في العراق من مستويين كما يلي:

المستوى 0:

أنشأت الشركة العامة للاتصالات والمعلوماتية (ITPC) خمس هيئات تصديق جذرية لأنواع مختلفة من الشهادات. تولّت ITPCمسؤولية هذا المستوى الجذري بصفتها الجهة الوطنية المسؤولة عن حوكمة البنية التحتية للمفتاح العام كما أدارت اللجنة العليا لإدارة التوقيع الإلكتروني .(PMA) وتضم هيئات التصديق الجذرية التابعة لـ ITPC ما يلي:

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

المستوى 1: اندرجت هيئات التصديق التابعة لشركة مصدر التكنولوجيا ضمن هذا المستوى من هيكل البنية التحتية الوطنية للمفتاح العام كما ظهر ذلك في الشكل التالي:



.

تتولى شركة مصدر التكنولوجيا تشغيل هيئات التصديق التابعة وتقديم خدمات الثقة المرتبطة بها إلى المجالات الحكومية وغير الحكومية في العراق. وبناءً على ذلك عملت مصدر التكنولوجيا كمزوّد لخدمات الثقة (TSP) وقدّمت خدماتها من خلال هيكلية من هيئات التصديق التابعة التي نُفذت ضمن هيئات التصديق الجذرية التابعة للشركة العامة للاتصالات والمعلوماتية(ITPC) . وصادقت هيئات ITPC الجذرية على هيئات التصديق التابعة الخاصة بـ TSP التابعة لمصدر التكنولوجيا على النحو التالي:

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

مثّلت حالات الاستخدام أعلاه عنصراً محورياً في تمكين التحول الرقمي كونها شكّلت حجر الأساس في تأمين المعاملات الإلكترونية. وأسهم دعم هذه الحالات من خلال نموذج موحد للثقة مع ضمان حكومي في تسهيل التبني وتحقيق التشغيل البيني وتعزيز ثقة المستخدم.

وتعاون مجلس إدارة البنية التحتية للمفتاح العام التابع لمصدر التكنولوجيا بشكل وثيق مع اللجنة العليا لإدارة التوقيع الإلكتروني في ITPC لضمان الالتزام بهذا البيان فيما يتعلق بإصدار وتشغيل هيئات التصديق التابعة لTS .

1.1.1 مجلس إدارة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا (TS PKI GB)

يُعرف مجلس الإدارة المسؤول عن حوكمة البنية التحتية للمفتاح العام لدى مصدر التكنولوجيا (بما في ذلك هيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIME) باسم مجلس إدارة .TS PKI ويضم هذا المجلس الوظائف الأساسية اللازمة مثل السياسات وامتثال والشؤون القانونية والهندسة المعمارية بهدف وضع التوجيه الاستراتيجي والإشراف المستمر على عملياتTS PKI .

وتتضمن مسؤوليات مجلس TS PKI ما يلي:

- تحديد استراتيجية TS PKI والحفاظ عليها.

- تحديد خدمات TS PKI والموافقة على نموذج تقديمها.
- تحديد سياسات وممارسات TS PKI والمحافظة عليها.
- تنفيذ أنشطة إشراف منتظمة على فريق عملياتTS PKI .
- الموافقة على ميزانية البنية التحتية للمفتاح العام واتخاذ القرارات التجارية الرئيسية.
- الموافقة على التغييرات الجوهرية في بنية البنية التحتية للمفتاح العام.
- الموافقة على المراسيم الرئيسية وتعيين المدققين الداخليين والخارجيين حسب الحاجة.
- التدخل في الحوادث الكبرى واتخاذ القرارات المناسبة.
- قيادة تسوية النزاعات الناتجة عن أو المرتبطة بأنشطةTS PKI .
- تقييم الحوادث التي لم يلتزم فيها الموظفون الأساسيون في TS PKI بالإجراءات الأمنية أو التشغيلية بما في ذلك أخلاقيات العمل.

1.2 اسم المستند ومعرّفه

يحمل هذا المستند العنوان "بيان ممارسة الشهادات لهيئة التصديق لشهادات البريد الإلكترون الآمن S/MIME الخاصة بمصدر التكنولوجيا" ويُعرف بواسطة المعرف الرقمي 2.16.368.1.2.1.4 (OID) ويُشار إليه في المستندات ذات الصلة باسم[TS S/MIME CA CPS] .

تتضمن شهادات البريد الإلكتروني الآمن S/MIMEالتي تصدرها الهيئة المعرف الرقمي المذكور في امتداد سياسة الشهادة (CP)للإشارة إلى الالتزام بالمتطلبات المعمول بها حالياً.

1.3 المشاركون في البنية التحتية للمفتاح العام

1.3.1 هيئات التصديق

تتبع هيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIMEالتابعة لمصدر التكنولوجيا (ويشار إليها لاحقاً باسم الهيئة) لشركة مصدر التكنولوجيا وتُدار من خلال مقرها في العراق. وقد صادقت عليها الشركة العامة للاتصالات والمعلوماتية ووقّعتها الهيئة الجذرية العراقية لـ S/MIME كما هو موضح في الشكل 1 (الفقرة 1.1).

تقدّم هذه الهيئة الخدمات التالية:

- **خدمة إصدار الشهادات** — إصدار شهادات الأطراف النهائية استناداً إلى عملية التحقق التي تنفذها هيئات التسجيل.
- **خدمة النشر** — نشر شهادات OCSP وقوائم الإلغاء وشهادات الهيئة وإتاحتها للأطراف المعتمدة. كما توفر هذه الخدمة سياسات وممارسات الهيئة للجمهور من المشتركين والأطراف المعتمدة.
- **خدمة إدارة الإلغاء** — معالجة الطلبات والتقارير المتعلقة بإلغاء الشهادات وتحديد الإجراء المناسب. وتُعرض نتائج هذه الخدمة من خلال خدمة حالة صلاحية الشهادة.
- **خدمة حالة صلاحية الشهادة** — تقديم معلومات حالة صلاحية الشهادات إلى الأطراف المعتمدة استناداً إلى قوائم الإلغاء وخدمة مستجيب .OCSP وتعكس معلومات الحالة دائماً الوضع الفعلي للشهادات الصادرة عن هذه الهيئة.

1.3.2 هيئات التسجيل

تشير هيئة التسجيل (RA) إلى الكيان المسؤول عن التعرف على هوية المتقدمين للحصول على شهادات المستخدمين النهائيين والتحقق منها وعن تقديم أو تمرير طلبات الإلغاء والموافقة على طلبات تجديد الشهادات نيابة عن هيئة التصديق".

1.3.2.1 هيئة التسجيل الخاصة بمصدر التكنولوجيا

تُعد وظيفة هيئة التسجيل (RA) مكوناً أساسياً ضمن هيكلية عمليات البنية التحتية للمفاتيح العامة(PKI) ، وهي المسؤولة عن إثبات الهوية والتحقق من المؤسسات التي تسعى للعمل بصفة هيئة تسجيل محلية (LRA) لإصدار شهادات (S/MIME)المصادق عليها من قبل الجهة الكفيلة (Sponsor-validated) لمجتمعات المستخدمين التابعة لها (راجع القسم 1.3.2.2).

وفي الحالات التي لا تقوم فيها المؤسسة مقدمة الطلب بتعيين موظف هيئة تسجيل محلي (LRAO) من داخل كيانها، أو لا تمتلك القدرة التشغيلية على ذلك؛ تتولى شركة مصدر التكنولوجيا مهام إثبات الهوية والتحقق لموظفي تلك المؤسسة مباشرةً من خلال وظيفة هيئة التسجيل (RA) التابعة لها. وفي هذه الحالات، يتحمل موظف هيئة التسجيل (RA) المسؤولية الكاملة عن إثبات الهوية والتحقق من بيانات طلب الشهادة لشهادات (S/MIME) المصادق عليها من قبل الجهة الكفيلة.

علاوة على ذلك، يتم حصر معالجة طلبات الشهادات الخاصة بـكبار المسؤولين الحكوميين (Governmental VIP Officials) بـ "هيئة التسجيل" التابعة لشركة مصدر التكنولوجيا حصراً، بغض النظر عما إذا كانت الجهة طالبة الشهادة تمتلك هيئة تسجيل محلية (LRA) خاصة بها أم لا. تضمن هذه المعالجة المركزية من قبل هيئة التسجيل التابعة للشركة اتساقاً في إجراءات إثبات الهوية، ومراجعة موحدة لأدلة التفويض، ومعالجة محكومة لبيانات طلبات الشهادات لهذه الفئة من المتقدمين.

1.3.2.2 هيئات التسجيل المحلية(LRA)

أتاحت شركة مصدر التكنولوجيا للجهات الحكومية وغير الحكومية العراقية إمكانية إدارة دورة حياة الشهادات لمجتمعات المستخدمين التابعة لها من خلال العمل كهيئة تسجيل محلية (LRA) لنوع معين من الشهادات الصادرة للأشخاص الطبيعيين أي شهادات البريد الإلكتروني الآمن S/MIMEمصدّقة من قبل راعٍ.

في هذه الحالة دخلت الجهة الطالبة في علاقة تعاقدية من خلال اتفاقية LRA مع مصدر التكنولوجيا بحيث أنشأت الجهة الطالبة مكتب هيئة تسجيل محلية يعمل فيه موظفو RA التابعون لها.

وتفرض اتفاقية LRA التزامات تشمل على سبيل المثال لا الحصر:

- المصادقة على طلبات إصدار الشهادات أو إلغائها أو رفضها.
- تحديد هوية المشتركين وفقاً لاتفاقيات التسمية الواردة في هذا البيان بحيث جرى تعريف كل مشترك بطريقة فريدة وواضحة.
- معالجة طلبات إصدار الشهادات أو إلغائها مع هذه الهيئة استناداً إلى الطلبات التي جرى التحقق منها والموافقة عليها.
- إنشاء سجل تدقيق وتحديثه لتوثيق جميع الأحداث المهمة المرتبطة بعملياتRA .
- إتاحة الوصول الانتقائي إلى سجلات سجل التدقيق كما ورد في هذا البيان.

- تنفيذ الضوابط التشغيلية الأخرى المبينة في هذا البيان.
- معالجة المعلومات وتخزينها وفقاً للمتطلبات المبينة في هذا البيان وبشكل خاص في القسم 5.

نفذت شركة مصدر التكنولوجيا وظيفة LRA تقنياً من خلال تطبيق إلكتروني عبر الويب مخصص لموظفي LRA المفوضين للعمل من مكاتب LRA المحددة. وصدر حساب LRA مخصص لكل موظف لتمكينه من إدارة الشهادات ضمن مجتمع المستخدمين التابع للجهة المرتبطة بمكتب LRA. وامتثل موظفو LRA للمتطلبات المبينة في الفقرتين 4.2 و5.3.

1.3.3 المشتركون

المشتركون في هيئة التصديق S/MIME التابعة لمصدر التكنولوجيا هم أشخاص طبيعيون جرى تعريفهم بالارتباط مع شخص اعتباري أي موظفون عراقيون تقدموا بطلب الحصول على شهادات البريد الإلكتروني الآمن S/MIMEمصدّقة من قبل راعٍ من هيئة التصديق S/MIME التابعة لمصدر التكنولوجيا ووافقوا على الالتزام بشروط واحكام المشترك ذات الصلة.

1.3.4 الأطراف المعتمدة

يجب على الأطراف المعتمدة الرجوع باستمرار إلى خدمات حالة صلاحية الشهادات التي تقدمها مصدر التكنولوجيا مثل قوائم الإلغاء وخدمة مستجيب OCSP قبل الاعتماد على أي معلومات واردة في الشهادة المعنية.

1.3.5 مشاركون آخرون

تشمل المشاركون الآخرون ما يلي:

- اللجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية والتي تُعد الجهة الرقابية المشرفة على مجمل أنشطة مزوّد خدمات الثقة المرخص مثل مصدر التكنولوجيا. وتُفصل أدوار ومسؤوليات اللجنة العليا لإدارة التوقيع الإلكتروني في CP/CPS الجذري الصادر عن ITPC والمنشور على الرابط: https://pki.itpc.gov.iq.
- مدققون مستقلون معتمدون من WebTrust ومؤهلون للتحقق من المتطلبات المبينة في الفقرة 8.2.

1.4 استخدام الشهادات

1.4.1 الاستخدامات المسموح بها للشهادات

يمكن استخدام الشهادات الصادرة عن هذه الهيئة في الحالات التالية:

1. **شهادات للأشخاص الطبيعيين:**
   أ. S/MIME: تُستخدم للتوقيع الرقمي، والتحقق، وتشفير رسائل البريد الإلكتروني؛ بما يضمن صدورها من عنوان بريد إلكتروني متحقق منه.
2. شهادة مستجيبOCSP : تُستخدم للتوقيع والتحقق من ردود بروتوكول حالة الشهادات الإلكترونية OCSP المتعلقة بالشهادات الصادرة عن هيئة التصديق S/MIME التابعة لمصدر التكنولوجيا.

1.4.2 الاستخدامات المحظورة للشهادات

يُصرح للمشتركين باستخدام الشهادات للأغراض المبينة في الفقرة 1.4.1 من هذا البيان. ويُمنع منعاً باتاً استخدام الشهادات لأي أغراض أخرى.

1.5 إدارة السياسات

1.5.1 الجهة المسؤولة عن إدارة المستند

أدار مجلس إدارة TS PKI هذا المستند وفقاً لنموذج تشغيله وبناءً على التفاعل مع اللجنة العليا لإدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية عند الحاجة.

1.5.2 الشخص المسؤول عن التواصل

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

مجلس حوكمة 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+)

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

تقرير مشكلة الشهادة

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

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

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

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

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

1.5.3 الشخص المسؤول عن تحديد مدى ملاءمة هذا البيان للسياسة

استناداً إلى نتائج تدقيقات الامتثال وتوصياتها يُحدد مجلس حوكمة البنية التحتية للمفاتيح العامة لشركة مصدر التكنولوجيا مدى ملاءمة هذا البيان وقابليته للتطبيق. وقد أُعتمد هذا البيان من قبل مجلس TS PKI GB وكذلك من قبل اللجنة العليا

لإدارة التوقيع الإلكتروني PMA لأنه يجب أن يمتثل في نهاية المطاف لأحكام سياسة الشهادات الخاصة بمقدم خدمات الثقة(TSP CP) .

1.5.4 إجراءات اعتماد بيان ممارسة الشهادات

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

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

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

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

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

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

1.6 التعاريف والاختصارات والمراجع

1.6.1 التعاريف

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

جهاز التوثيق الثنائي :جهاز تشفيري من نوع USB حاصل على شهادة مطابقة لمعيار FIPS 140 المستوى الثاني أو ما يعادله.

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

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

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

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

كبار المسؤولين الحكوميين :(Governmental VIP Officials) هم الأفراد الذين يشغلون مناصب عليا ضمن المؤسسات أو الهيئات أو الوزارات الحكومية، وتتضمن مهامهم صلاحيات واسعة في اتخاذ القرار، أو تمثيل الدولة، أو تولي مسؤوليات حيوية تتعلق بالمصلحة الوطنية. وتشمل هذه الفئة، على سبيل المثال لا الحصر: الوزراء، والوكلاء، ورؤساء الهيئات الحكومية، والسفراء، وغيرهم من كبار المسؤولين المصنفين رسمياً كشخصيات هامة (VIPs) من قبل الجهة الحكومية المختصة.

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

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

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

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

زوج المفاتيح :المفتاح الخاص والمفتاح العام المرتبط به.

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

ملف تعريف الإصدارات القديمة: توفر ملفات تعريف الإصدارات القديمة من S/MIME مرونةً لتطبيق ممارسات شهادات S/MIME الحالية المعقولة، بحيث تصبح قابلةً للتدقيق بموجب متطلبات S/MIME الأساسية. ويشمل ذلك

خيارات لسمات اسم الموضوع المميز (Subject DN) واستخدام المفتاح الإضافي (extKeyUsage) وامتدادات أخرى. سيتم إيقاف دعم ملفات التعريف القديمة في إصدار لاحق من متطلبات S/MIME الأساسية.

التحقق من صحة صندوق البريد (MV): يشير إلى موضوع الشهادة الذي يقتصر على سمات (اختيارية) subject:emailAddress و/أو subject:serialNumber.

عنوان صندوق البريد: يُعرف أيضًا باسم عنوان البريد الإلكتروني. وفقًا لـ RFC 5321: "سلسلة نصية تُحدد المستخدم الذي سيتم إرسال البريد إليه أو الموقع الذي سيتم إيداع البريد فيه."

حقل صندوق البريد: في شهادات المشترك، يحتوي على عنوان صندوق بريد الموضوع عبر قيمة rfc822Name أو otherName من نوع id-on-SmtpUTF8Mailbox في امتداد subjectAltName، أو في شهادات المرجع المصدق الفرعي عبر rfc822Name في permittedSubtrees ضمن امتداد nameConstraints.

الملف التعريفي متعدد الأغراض: تتوافق ملفات تعريف S/MIME متعددة الأغراض مع الملفات التعريفية الصارمة الأكثر تحديدًا، ولكن مع خيارات إضافية لـ extKeyUsage وامتدادات أخرى. يهدف هذا إلى توفير مرونة لحالات الاستخدام المشتركة بين توقيع المستندات والبريد الإلكتروني الآمن.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

الملف التعريفي الصارم: تُعد ملفات تعريف الجيل الصارم S/MIME هي ملف التعريف المستهدف طويل المدى لشهادات S/MIME مع استخدام extKeyUsage المحدود إلى id-kp-emailProtection، واستخدام أكثر صرامة لسمات Subject DN والامتدادات الأخرى.

الموضوع :الكيان أو المؤسسة المعرفة ضمن حقل "الموضوع" في الشهادة. الموضوع إما هو المشترك أو صندوق بريد تحت سيطرة المشترك وتشغيله.

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

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

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

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

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

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

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

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

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

1.6.2 الاختصارات

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

IT	تكنولوجيا المعلومات
ITPC	الشركة العامة للاتصالات والمعلوماتية
OCSP	بروتوكول حالة الشهادة عبر الإنترنت
OID	معرف الكائن
PIN	الرقم السري الشخصي
PKCS#1	معايير التشفير بالمفتاح العام – رقم 1
PKCS#7	صيغة الرسائل المشفرة
PKCS#10	مواصفة طلب الشهادة
PKI	البنية التحتية للمفتاح العام
PMA	اللجنة العليا لإدارة التوقيع الإلكتروني
RA	هيئة التسجيل
RSA	ريفست–شامير–أدلمن (مخترعو خوارزميةRS)
RTO	مدة استعادة الخدمة
SSL	طبقة المنافذ الآمنة
TLD	نطاق المستوى الأعلى
TSA	هيئة ختم الوقت
TS	شركة مصدر التكنولوجيا
TLS	أمن طبقة النقل
TSP	مزود خدمات الثقة
UPS	مزود طاقة غير منقطع
URI	معرف الموارد الموحد
URL	محدد الموارد الموحد

1.6.3 المراجع (References)

- X.509 : المعيار الصادر عن الاتحاد الدولي للاتصالات (ITU-T) الخاص بالشهادات الرقمية.
- RFC3647 : إطار سياسة الشهادات ومعايير ممارسات التصديق للبنية التحتية للمفاتيح العامة (X.509) الخاصة بالإنترنت.
- RFC5280 : المواصفات الفنية لشهادات البنية التحتية للمفاتيح العامة (X.509) وقائمة الشهادات المحجوبة (CRL)الخاصة بالإنترنت.
- مبادئ ومعايير WebTrust (AICPA/CPA Canada) لجهات التصديق(Certification Authorities) .
- مبادئ ومعايير WebTrust (AICPA/CPA Canada) لجهات التصديق – أمن الشبكات.
- مبادئ ومعايير WebTrust (AICPA/CPA Canada) لجهات التصديق – شهادات البريد الإلكتروني الآمن S/MIME.
- متطلبات أمن الشبكات وأنظمة الشهادات الصادرة عن منتدى(CA/Browser Forum) .
- المتطلبات الأساسية لمنتدى (CA/Browser Forum) لإصدار وإدارة شهادات (S/MIME) الموثوقة علنياً.

2 المسؤوليات المتعلقة بالنشر والمستودعات

2.1 المستودعات

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

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

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

2.2 نشر معلومات الشهادات

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

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

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

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

2.3 توقيت أو تكرار النشر

يُجري مجلس حوكمة البنية التحتية للمفتاح العام لشركة مصدر التكنولوجيا (TS PKI GB) مراجعة لبيان ممارسة الشهادات (CPS) هذا مرة واحدة على الأقل سنوياً ويُجري التعديلات المناسبة لضمان أن تبقى عمليات هيئات التصديق التابعة متوافقة تماماً مع المتطلبات المذكورة في القسم 1 من هذا البيان. كما يتم زيادة رقم إصدار CPS، ويتم تضمين إدخال سجل التغييرات المؤرخ لتوثيق المراجعة.

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

2.3.1 شهادات هيئات التصديق

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

2.3.2 قوائم إلغاء الشهادات(CRLs)

تقوم هيئة التصديق S/MIME التابعة لمصدر التكنولوجيا بإنشاء ونشر قوائم إلغاء الشهادات على النحو التالي:

- تُحدَّث القوائم بحد أقصى كل 24 ساعة حتى في حال عدم حدوث أي تغييرات منذ إصدار القائمة السابقة؛
- تُحدد صلاحية كل قائمة إلغاء بـ 26 ساعة.

2.4 ضوابط الوصول إلى المستودعات

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

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

3 التعريف والمصادقة

3.1 التسمية

3.1.1 أنواع الأسماء

تلتزم أسماء الموضوعات في شهادة TS S/MIME CA بمعايير الأسماء المميزة (DN) المحددة في التوصية .X.500 يتم التحقق من اسم الموضوع المستخدم في شهادة هيئة التصديق والتحقق منه بواسطة وظيفة هيئة التسجيل التابعة للجنة إدارة السياسات ويجب أن يكون ذا معنى وألا يُعاد تخصيصه لأي كيان آخر.

تُحدد هذه الهيئة في حقل اسم المُصدِر في شهادات المشتركين كما يلي:

شهادة TS SMIME CA

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

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

شهادات البريد الإلكتروني الآمن (S/MIME) الصادرة للمشتركين:

القيمة	السمة
الاسم الأول للمشترك المُصادق عليه	GivenName
اسم العائلة للمشترك المُصادق عليه	SurName
معرف فريد لكل مشترك تنشئه هيئة التسجيل	SERIALNUMBER (اختياري)
عنوان البريد الإلكتروني	CN (اختياري)

القيمة	السمة
الاسم الأول للمشترك المُصادق عليه	GivenName
الاسم القانوني الكامل للمنظمة التابعة لصاحب الشهادة أو اسم مستعار وإذا وُجد الاثنان يجب أن يظهر الاسم المستعار أولاً ثم يلي ذلك الاسم القانوني الكامل للمنظمة بين قوسين	O
المعرف التنظيمي للمنظمة	OrganizationIdentifier
العراق	الدولة (C)

شهادة مستجيب OCSP الخاصة بـ S/MIME CA

القيمة	السمة
TS SMIME CA G1 OCSP	CN
مصدر التكنولوجيا	O
العراق	الدولة (C)

3.1.2 الحاجة إلى أن تكون الأسماء ذات معنى

تطبق هيئة التصديق هذه القواعد التالية لضمان استخدام أسماء ذات معنى:

بالنسبة لشهادات البريد الإلكتروني الآمن S/MIMEالصادرة للأشخاص الطبيعيين: احتوت شهادات البريد الإلكتروني الآمن S/MIMEعلى اسم مميز غير فارغ (Subject DN) يتضمن المعلومات التي جرى التحقق منها للجهة التي رعت إصدار الشهادة واسم الفرد. تضمن حقل rfc822Name عنوان البريد الإلكتروني الذي يسيطر عليه الفرد مقدم الطلب لشهادة S/MIME وقد تكرر ذلك في حقل الاسم العام (Common Name).

بالنسبة لشهادة مستجيب OCSP: عُد الاسم ذا معنى لأنه أشار إلى اسم مستجيب شهادة OCSP الخاص بهيئة التصديق التابعة.

3.1.3 عدم الكشف عن الهوية أو استخدام الأسماء المستعارة من قبل المشتركين

حُظر استخدام المشتركين لأسماء مجهولة أو مستعارة.

3.1.4 قواعد تفسير أشكال الأسماء المختلفة

استُخدم في هيئة التصديق هذه أسلوب تسمية يستند إلى معيار ISO/IEC 9595 (X.500) لتمييز الأسماء(DN) .

3.1.5 تفرّد الأسماء

بالنسبة لشهادات البريد الإلكتروني الآمن S/MIMEالصادرة للأشخاص الطبيعيين: فُرض التفرّد من خلال الجمع بين اسم الفرد واسم الجهة الراعية.

بالنسبة لشهادة مستجيبOCSP : أُدرج اسم مستجيب OCSP الفريد ضمن حقل subject DN في شهادة OCSP الصادرة.

3.1.6 التعرف والمصادقة ودور العلامات التجارية

لن يُسمح للمشتركين بطلب شهادات تحتوي على أي مضمون ينتهك حقوق الملكية الفكرية لأي جهة أخرى.

احتفظت هيئة التصديق بحقها في إلغاء الشهادة بناءً على أمر موثّق وصحيح ورد من مجلس حوكمة البنية التحتية للمفتاح العام أو من محكمة مختصة تأمر بإلغاء شهادة أو شهادات تتضمن اسماً محل نزاع.

3.2 التحقق الأولي من الهوية

3.2.1 طريقة إثبات امتلاك المفتاح الخاص

قدّم مقدم الطلب طلب توقيع شهادة بصيغة PKCS#10 موقعاً رقمياً لإثبات حيازته للمفتاح الخاص المقابل للمفتاح العام المطلوب تضمينه في الشهادة. فَرَضت أنظمة هيئة التسجيل المحلية التحقق من إثبات حيازة المفتاح الخاص ضمن عملية معالجة طلب الشهادة. قُدّم إثبات الحيازة إلى هيئة التسجيل المحلية من خلال طلبات PKCS#10.

3.2.1.1 مصادقة المنظمات

جرى التحقق من هوية المنظمة المقدمة للطلب باستخدام مصادر بيانات موثوقة معتمدة ويتوجب أن توفر معلومات تفصيلية عن الكيان مثل الاسم القانوني للجهة وعنوانها ومعلومات الممثل المفوض.

اعتمدت شركة مصدر التكنولوجيا على الوقائع العراقية الرسمية أو عبر وسائل اتصال مباشرة مع الكيان أو مع الجهة القضائية المسؤولة عن إنشاء الكيان أو وجوده أو الاعتراف به عند التحقق من معلومات الجهات الحكومية واعتمدت على تواصل رسمي مع جهة تسجيل أو تأسيس الشركات العراقية للتحقق من معلومات الجهات غير الحكومية.

طلبت شركة مصدر التكنولوجيا من مقدم الطلب تقديم مستندات رسمية تثبت هوية الكيان مثل عقد تأسيس الشركة أو مستند ضريبي حكومي أو خطاب مهني صادر عن محاسب أو رأي قانوني أو مستندات أخرى ذات صلة وقد أجرت زيارة ميدانية لموقع الكيان للتحقق من العنوان.

بالإضافة إلى ذلك تحققت شركة مصدر التكنولوجيا من حق مقدم الطلب في استخدام اسم النطاق المستخدم في عنوان البريد الإلكتروني الوارد في الشهادة وفقاً للإجراءات الموضحة في القسم 3.2.3.

أكّد مسؤول هيئة التسجيل أن جميع بيانات التحقق المتعلقة بالسيطرة على صندوق البريد الإلكتروني عبر النطاق قد أُعيد جمعها والتحقق منها خلال مدة لم تتجاوز 398 يوماً من تاريخ آخر تحقق أُجري.

تحقّق مسؤول هيئة التسجيل من صحة العلاقة مع موضوع الشهادة من خلال التأكد من أن المعلومات الواردة في نموذج الطلب قد تطابقت تماماً مع المعلومات التي أُدرجت في الشهادة.

سلطة المتقدم بالطلب.

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

3.2.1.2 المصادقة للمنظمات المتقدمة لتشغيل هيئة تسجيل محلية(LRA)

ينطبق هذا السيناريو على المنظمات التي ترغب في إصدار شهادات الأشخاص الطبيعيين وإدارتها. يجري التحقق من المنظمة وممثلها المفوض وفقاً للإجراءات الموضحة أعلاه في القسم 3.2.2.1 يقوم مخوّل المؤسسة بالتوقيع على) شروط وأحكام استخدام هيئة التسجيل المحلية(LRA - ، كما يقوم بتعيين موظف (أو موظفي) هيئة التسجيل المحلي (LRAO) المخولين رسمياً بإجراء عمليات إدارة الشهادات نيابة عن المؤسسة.

وتتولى هيئة التسجيل (TS RA) التابعة لشركة مصدر التكنولوجيا مراجعة وتأكيد تعيين هؤلاء الموظفين (LRAOs) قبل تفعيل صلاحية الوصول إلى بوابة هيئة التسجيل عبر الويب Web RA Portal.

3.2.2 التحقق من صلاحية أو السيطرة على صندوق البريد الإلكتروني

قبل إصدار شهادة (S/MIME)، تتحقق هيئة التسجيل (RA) في شركة مصدر التكنولوجيا من سيطرة مقدم الطلب على جميع عناوين البريد الإلكتروني المحددة في حقول صندوق البريد (Mailbox Fields) بالشهادة. ويتم إجراء هذا التحقق من خلال تأكيد ما يلي:

- **التحقق من السيطرة على صندوق البريد عبر البريد الإلكتروني:** تقوم هيئة التسجيل (TS RA) بإرسال "قيمة عشوائية" (Random Value) إلى عنوان البريد الإلكتروني المراد التحقق منه، ويتعين على مقدم الطلب الرد باستخدام نفس القيمة العشوائية، وبذلك يثبت سيطرته الفعلية على صندوق البريد.
- **صلاحية القيمة العشوائية:** تكون القيمة العشوائية صالحة لمدة (24) ساعة من وقت إنشائها. وفي حال تلقي الرد بعد انتهاء فترة الصلاحية، يجب على هيئة التسجيل بدء طلب تحقق جديد من خلال إنشاء وإرسال قيمة عشوائية جديدة.

3.2.3 مصادقة الهوية الفردية

3.2.3.1 المصادقة للأفراد المتقدمين بطلبات شهادات الأشخاص الطبيعيين

يوضح هذا القسم الإجراءات المتبعة من قبل شركة مصدر التكنولوجيا للتحقق من هوية الأشخاص الطبيعيين كجزء من عمليات التسجيل للحصول على الشهادة.

يعتمد ضابط هيئة التسجيل المحلي على أدلة موثوقة وأدلة داعمة لتنفيذ التحقق من الهوية. تشمل أنواع الأدلة المعتمدة ما يلي:

- الأدلة الموثوقة: الدليل الأساسي المعتمد هو بطاقة الهوية الحكومية الآمنة أو جواز السفر (بما في ذلك الشريحة التي تحتوي على معلومات رقمية موقعة عن حاملها) والتي تصدر وفقاً لإجراءات إثبات وإصدار وإدارة هوية قوية.

- الأدلة الداعمة: الأدلة التكميلية: وهي الأدلة التي تُستخدم بالإضافة إلى الأدلة الرسمية (الموثوقة) لتعزيز موثوقية إثبات الهوية، أو كدليل على السمات والبيانات التي لا تثبتها الأدلة الرسمية وحدها. ومن أمثلة الأدلة الداعمة: شهادة استمرارية الخدمة (تأييد بالخدمة) أو معلومات مكافئة تُثبت العلاقة الوظيفية بين الموظف والجهة الحكومية، والبطاقات التعريفية للموظفين (الباجات).

وتُنفذ عملية التحقق من الهوية من قبل ضابط هيئة التسجيل المحلي من خلال لقاء مباشر مع الفرد أو طريقة معادلة وتتضمن الخطوات التالية:

أ) يجمع ضابط هيئة التسجيل المحلي أدلة التحقق من الهوية الداعمة للفرد من قسم الموارد البشرية كجزء من إجراءات إدخال الموظف أو من مدير مباشر في خط العمل أو من الفرد نفسه وتشمل:
- نموذج طلب شهادة مكتمل وموقع.
- تفضل الترجمة القانونية والإدارية لهذه الفقرة، بصياغة تتناسب مع متطلبات التوثيق في الدوائر الحكومية العراقية:
- "معلومات موثوقة تؤيد ارتباط الفرد بالجهة (على سبيل المثال: شهادة استمرارية الخدمة، أو هوية الموظف الحكومي، أو معلومات مكافئة)، وذلك حيثما انطبق ذلك.
- بريد إلكتروني من ممثل الجهة يطلب تسجيل الفرد في بوابة هيئة التسجيل الإلكترونية لتمكينه من الاستفادة من شهادة S/MIME حسب الحاجة الوظيفية.

ب) يتم إجراء إثبات الهوية وفقاً لمتطلبات التسجيل والتحقق من الهوية المعمول بها، ويكون مدعوماً بإجراءات توثيق التسجيل والتحقق التي تعتمدها شركة مصدر التكنولوجيا. وعند الموافقة الأولية على هوية الفرد، تبدأ إجراءات فنية يتم من خلالها تسجيل الفرد في بوابة هيئة التسجيل (Web RA Portal) وتزويده ببيانات اعتماد المصادقة متعددة العوامل (Multi-factor Authentication)، بما يتيح له تنفيذ طلبات الشهادات الرقمية وعمليات إدارة الشهادات ذات الصلة.

3.2.4 معلومات المشترك غير المؤكدة

تتحقق شركة مصدر التكنولوجيا من جميع معلومات المشترك الواردة ضمن الشهادة الصادرة من هيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIME.

3.2.5 التحقق من الصلاحية

تتحقق هيئة التسجيل في مصدر التكنولوجيا من صلاحية ممثل الكيان الرسمي بصفته الموقع على نموذج طلب الشهادة (نموذج تسجيل الكيان) واتفاقية هيئة التسجيل المحلي. كما تتحقق هيئة التسجيل من صلاحية ضابط هيئة التسجيل المحلي بصفته الشخص المفوض لتقديم طلبات الشهادات وتنفيذ عمليات إدارة الشهادات الأخرى. راجع القسم 3.2.2.2 لمزيد من التفاصيل.

3.2.6 معايير التشغيل البيني

لا يوجد نص.

3.3 التحقق الأولي من الهوية والتعريف والمصادقة لطلبات إعادة إصدار المفاتيح

3.3.1 التحقق من الهوية والمصادقة لإعادة الإصدار الروتينية

يُنفذ التحقق من الهوية والمصادقة لإعادة إصدار المفاتيح كما في التسجيل الأولي بالإضافة إلى القواعد التالية:

- يتحقق ضابط هيئة التسجيل المحلي أو هيئة التسجيل من وجود وصلاحية الشهادة المراد إعادة إصدارها ومن أن المعلومات المستخدمة للتحقق من هوية وصفات الموضوع لا تزال سارية.
- إذا طرأ أي تغيير على الشروط والأحكام الخاصة بمصدر التكنولوجيا يتم إبلاغ المشترك بهذه التغييرات من قبل هيئة التسجيل أو ضابط هيئة التسجيل المحلي.

3.3.2 التحقق من الهوية والمصادقة لإعادة الإصدار بعد الإلغاء

يُنفذ التحقق من الهوية والمصادقة لإعادة إصدار المفاتيح كما في التسجيل الأولي.

3.4 التحقق من الهوية والمصادقة لطلبات الإلغاء

تقوم هيئة التسجيل أو ضابط هيئة التسجيل المحلي بمصادقة طلب الإلغاء من خلال إحدى الطرق التالية:

- استلام طلب إلغاء من قسم معني ومتفق عليه مسبقاً ضمن الكيان (مثل قسم الموارد البشرية أو المدير المباشر للفرد) في حال إنهاء خدمة المشترك أو تغييره لموقعه الوظيفي مما يستوجب تقديم طلب الإلغاء. وتستخدم هيئة التسجيل أو ضابط هيئة التسجيل المحلي وسائل داخلية للتحقق من صحة الطلب.
- استلام طلب الإلغاء من المشترك عبر القنوات المتفق عليها والتي قد تشمل:
  - زيارة مباشرة (وجهاً لوجه) لمكتب هيئة التسجيل (TS RA) أو مكتب هيئة التسجيل المحلية (LRAO)؛ أو إجراء مكالمة هاتفية من المشترك يقوم خلالها موظف هيئة التسجيل بطرح أسئلة للتحقق من الهوية (مثل: الرقم الوظيفي، الاسم الكامل، تاريخ الميلاد، إلخ).
  - إرسال بريد إلكتروني من المشترك باستخدام عنوان بريدي يمكن التحقق منه من قبل هيئة التسجيل (TS RA) أو(LRAO) .
  - أو من خلال بوابة هيئة التسجيل عبر الويب (Web RA Portal) باستخدام حساب المستخدم الخاص.
- سيناريو كبار المسؤولين الحكوميين (الذي تتولاه هيئة تسجيل شركة مصدر التكنولوجيا حصراً) مثل استلام طلب إلغاء (سحب) الشهادة من الجهة الحكومية المختصة التي قامت بتعيين المسؤول أو التي تشرف عليه، أو من دائرة التنسيق الحكومي المختصة.
- يتولى موظف هيئة التسجيل (TS RA Officer) المصادقة على الطلب بناءً على الوثائق الرسمية وقنوات الاتصال المعتمدة، وذلك وفقاً للإجراءات الداخلية الموثقة.

بالنسبة لشهادات مستجيب OCSP: لا ينص بيان ممارسة الشهادات الحالي على أحكام تفصيلية بشأن إلغاء أي من هذه الشهادات. ويمكن أن يُستند في الإلغاء إلى حالة اختراق أو اشتباه باختراق في المفاتيح الخاصة ذات الصلة وتُعامل هذه الحالة ككارثة وفقاً لخطة التعافي من الكوارث واستمرارية الأعمال الخاصة بشركة مصدر التكنولوجيا.

4 المتطلبات التشغيلية لدورة حياة الشهادة

4.1 طلب الشهادة

4.1.1 من يمكنه تقديم طلب الشهادة

يمكن تقديم طلبات الشهادات مباشرة من قبل مقدمي الطلبات أنفسهم من خلال بوابة هيئة التسجيل الإلكترونية. يُخوَّل ضابط هيئة التسجيل المحلي (LRAO) بمراجعة واعتماد وتقديم طلبات الشهادات. ويتحمل مقدم الطلب مسؤولية صحة جميع البيانات المقدمة كجزء من طلب الشهادة. ويحرص ضابط هيئة التسجيل المحلي على أن يصدق مقدم الطلب على شروط واحكام المشترك كجزء من عملية طلب الشهادة. يحتفظ ضابط هيئة التسجيل المحلي بقائمة سوداء تضم الأفراد التابعين للجهة الذين لن تُقبل طلبات شهاداتهم.

في الحالات التي يكون فيها مقدم طلب الشهادة هو نفسه موظف هيئة تسجيل (TS RA) أو موظف هيئة تسجيل محلي (LRAO)، يجب أن يتم اعتماد وتقديم طلب الشهادة من قبل موظف هيئة تسجيل (TS RA أو LRAO) آخر، يكون مختلفاً عن الفرد المحدد بصفته مقدم الطلب.

بالنسبة لشهادة مستجيبOCSP: تشرف هيئة التسجيل في مصدر التكنولوجيا ومدير البنية التحتية للمفتاح العام المخوّل بدور موثوق على تنفيذ المراسيم التشغيلية الداخلية المخوّلة التي يتم من خلالها إصدار شهادات OCSP الخاصة بهيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIME.

4.1.2 عملية التسجيل والمسؤوليات

تُوصف العملية كما يلي:

- يُسجل الفرد في بوابة هيئة التسجيل الإلكترونية.
- يقوم الفرد بالمصادقة على هويته عبر بوابة هيئة التسجيل الإلكترونية باستخدام المصادقة متعددة العوامل.
- يُكمل الفرد نموذج طلب الشهادة.
- تُنفَّذ عملية تقنية تؤدي إلى تخصيص زوج مفاتيح التوكن وإنشاء طلب توقيع الشهادة(CSR) .
- يصدّق الفرد على شروط واحكام المشترك ويُقدّم طلب الشهادة إلى ضابط هيئة التسجيل المحلي.
- يتم تخويل موظف هيئة التسجيل (TS RA) أو موظف هيئة التسجيل المحلي (LRAO) بمراجعة طلبات الشهادات المقدمة.
- بمجرد تسجيل الدخول إلى بوابة هيئة التسجيل (Web RA Portal)، يتولى الموظف المختص (/ TS RA LRAO) التحقق من الطلب واتخاذ الخطوات الفنية اللازمة للمصادقة عليه.
- قبل إرسال الطلب إلى سلطة التصديق (CA) المعنية، تتولى هيئة تسجيل شركة مصدر التكنولوجيا (TS RA) إجراء عملية (التحقق من السيطرة على صندوق البريد عبر البريد الإلكتروني) والتحقق من (تخويل سلطة التصديق - CAA) وفقاً للقسمين 3.2.3 و4.2.2.1.

بالنسبة لشهادة مستجيب OCSP: تشرف هيئة التسجيل في مصدر التكنولوجيا ومدير البنية التحتية للمفتاح العام المخوّل بدور موثوق على تنفيذ مراسيم تشغيلية يتم من خلالها إصدار هذه الشهادات. ويصادق مجلس حوكمة البنية التحتية للمفتاح العام في مصدر التكنولوجيا (TS PKI GB) على وثائق المراسيم التشغيلية ويُحقق في قالب الشهادة

المضمن واتفاقيات التسمية مقابل أحكام بيان ممارسة الشهادات هذا. وبعد ذلك يُفوض مجلس حوكمة البنية التحتية المراسيم ويؤكد قائمة الموظفين المشاركين بدور موثوق.

4.2 معالجة طلب الشهادة

4.2.1 تنفيذ وظائف التعريف والمصادقة

يتم تنفيذ مهام تحديد الهوية والمصادقة من قبل موظف هيئة التسجيل المحلي (LRAO) أو، حيثما انطبق ذلك، من قبل هيئة تسجيل شركة مصدر التكنولوجيا(TS RA) ، وذلك استناداً إلى وثائق التعريف والأدلة الثبوتية المقدمة من قبل المشترك. باختصار، يتم تنفيذ الأنشطة التالية:

أ) يتولى مسؤول هيئة التسجيل أو مسؤول هيئة التسجيل المحلية لـ (مصدر التكنولوجيا) ضمان تخصيص معرف فريد لكل سجل طلب شهادة رقمية.
ب) يقوم مسؤول هيئة التسجيل أو مسؤول هيئة التسجيل المحلية لـ (مصدر التكنولوجيا) بتوثيق جميع الأنشطة (المراسلات عبر البريد الإلكتروني، المكالمات الهاتفية، أدلة التحقق) وإرفاقها مع سجل طلب الشهادة.
ت) تدرج أي شهادة خبيثة أو طلب إلغاء مشبوه أو طلب يفشل لأكثر من ثلاث مرات في القائمة السوداء، على أن تتضمن القائمة كافة التفاصيل اللازمة لمنع أي غموض في تحديد الطلبات الخبيثة مستقبلاً.
ث) يجري مسؤول هيئة التسجيل أو مسؤول هيئة التسجيل المحلية لـ (مصدر التكنولوجيا) فحصاً لبيانات المتقدم بمطابقتها مع القائمة السوداء الخاصة بهيئة التسجيل، وفي حال وجود المتقدم ضمن القائمة يتم رفض طلب الشهادة فوراً.
ج) يلتزم المتقدم بالتوقيع أو المصادقة على الشروط والأحكام الخاصة بالمشتركين.
ح) يتولى مسؤول هيئة التسجيل أو مسؤول هيئة التسجيل المحلية لـ (مصدر التكنولوجيا) التحقق من هوية الشخص وفقاً للإجراءات الموضحة في القسم 3.2.4.
خ) يتحقق مسؤول هيئة التسجيل أو مسؤول هيئة التسجيل المحلية لـ (مصدر التكنولوجيا) من أهليّة الفرد للحصول على الشهادة المطلوبة وفقاً للإجراءات الداخلية للمؤسسة (على سبيل المثال: إجراء التحقق من خلال التواصل مع المدير المباشر للشخص المعني).
د) يباشر مسؤول هيئة التسجيل أو مسؤول هيئة التسجيل المحلية لـ (مصدر التكنولوجيا) بتنفيذ الإجراءات الفنية المتعلقة بالموافقة على الشهادة المطلوبة.
ذ) قبل الإرسال إلى سلطة التصديق المعنية، يقوم مسؤول هيئة التسجيل بالتحقق من ملكية البريد الإلكتروني وفقاً للقسم 3.2.3 والتحقق من تخويل سلطة التصديق (CAA) وفقاً للقسم 4.2.2.1.
ر) عند نجاح عملية التحقق، يباشر مسؤول هيئة التسجيل لـ (مصدر التكنولوجيا) بالإجراءات الفنية الخاصة بإصدار الشهادة المطلوبة.

مدة صلاحية البيانات المُحققة

يجوز لهيئة التسجيل أو لضابط هيئة التسجيل المحلي إعادة استخدام عمليات التحقق المكتملة أو الأدلة الداعمة المنفذة وفق القسم 3.2 وذلك ضمن الحدود التالية:

- السيطرة على صندوق البريد عبر النطاق: خلال فترة لا تتجاوز 398 يوماً قبل إصدار الشهادة.

- التحقق من صلاحية صندوق البريد عبر البريد الإلكتروني: خلال فترة لا تتجاوز 30 يوماً قبل إصدار الشهادة.
- مصادقة هوية المنظمة: خلال فترة لا تتجاوز 365 يوماً قبل إصدار الشهادة.
- مصادقة الهوية الفردية: خلال فترة لا تتجاوز 365 يوماً قبل إصدار الشهادة.

لا يجوز إعادة استخدام أي تحقق سابق إذا كانت البيانات أو الوثائق المستخدمة فيه قد تم الحصول عليها قبل الفترة الزمنية القصوى المحددة لإعادة الاستخدام.

4.2.2 الموافقة على طلبات الشهادة أو رفضها

يعتمد ضابط هيئة التسجيل المحلي طلب الشهادة فقط في حال تحقق المعايير التالية:

- نجاح عملية التعريف والمصادقة على جميع معلومات المشترك المطلوبة وفقاً للقسم 3.2.

يرفض ضابط هيئة التسجيل المحلي طلب الشهادة في الحالات التالية:

- تعذر إتمام التعريف والمصادقة على جميع معلومات المشترك المطلوبة وفقاً للقسم 3.2.
- فشل المشترك في تقديم الوثائق الداعمة عند الطلب.

بالنسبة لشهادة مستجيبOCSP: تشرف هيئة التسجيل ومدير البنية التحتية للمفتاح العام المخوّل بدور موثوق على تنفيذ مراسيم تشغيلية يتم من خلالها إصدار هذه الشهادات ويُصادق مجلس حوكمة البنية التحتية على وثائق المراسيم التشغيلية ويُقيّم القالب المضمن للشهادة واتفاقيات التسمية وفقاً لأحكام هذا البيان ويمنح الإذن بتنفيذ المراسيم ويؤكد قائمة الموظفين المشاركين بدور موثوق.

4.2.2.1 تخويل سلطة التصديق (CAA)

قبل إصدار شهادة (S/MIME) ، يجب على هيئة تسجيل شركة مصدر التكنولوجيا (TS RA) استرداد ومعالجة سجلات "تخويل سلطة التصديق (CAA) "وفقاً للمعيار (RFC 9495) لكل عنوان صندوق بريد مدرج في ملحق الاسم البديل للموضوع (subjectAltName) في الشهادة. يتم معالجة علامة الخاصية (issuemail) ، ويكون نطاق الجهة المصدرة المعتمد في سجلات الـ CAA هو(pki.techsource.iq) .

يتم إصدار الشهادات التي تجتاز فحص الـ (CAA) خلال فترة "زمن البقاء (TTL) "الخاصة بسجل الCAA ، أو خلال 8 ساعات، أيهما أطول.

في الحالات التي تكون فيها منطقة (DNS) المحتوية على سجل (CAA) موقعة باستخدام بروتوكول أمن نظام أسماء النطاقات(DNSSEC) ، يجب على موظف هيئة التسجيل (أو نظام التحقق) إجراء فحص (DNSSEC) على استجابة الـ DNSقبل الاعتماد على سجل الCAA ، ويجب عدم إصدار الشهادة إذا فشل فحص (DNSSEC) أو إذا أشار الفحص إلى وجود خلل في "سلسلة الثقة .(Chain of Trust) "لا تقوم شركة مصدر التكنولوجيا بتعطيل أو تجاوز فحص (DNSSEC) لأي استعلام يتعلق بسجلات الـ CAA عند وجود توقيعات(DNSSEC) .

تقوم هيئة التسجيل (TS RA) بتسجيل كافة الإجراءات المتعلقة بفحص ومعالجة سجلات الـ CAA في سجلات النظام .(Logs)بالإضافة إلى ذلك، تقوم هيئة التسجيل بتوثيق أي حالات إصدار شهادات محتملة تم منعها بسبب سجلات الـ CAA، مع تقديم تفاصيل كافية تتيح تزويد منتدى (CA/Browser Forum) بالتغذية الراجعة حول تلك الظروف.

لا تستخدم هيئة تسجيل شركة مصدر التكنولوجيا علامة الخاصية (iodef) الخاصة بسجل الـ CAA للتواصل مع جهات الاتصال المنصوص عليها في سجلات(CAA iodef) .

4.2.2.2 تأكيد الإصدار من منظورات متعددة (multi-perspective issuance corroboration)

لا تشترط شركة مصدر التكنولوجيا استرداد ومعالجة سجلات الـ CAA من "منظورات شبكة عن بُعد" إضافية (Network Perspectives) قبل إصدار الشهادة، حيث أن الطرق المستخدمة للتحقق من تخويل أو السيطرة على صندوق البريد لا تستدعي مثل هذا التأكيد.

4.2.3 تخويل هيئة التصديق (CAA)

لا تعالج شركة مصدر التكنولوجيا حالياً سجلات CAA من نوع issuemail لعناوين صناديق البريد.

4.2.4 الوقت اللازم لمعالجة طلبات الشهادات

لا يوجد نص.

4.3 إصدار الشهادة

4.3.1 إجراءات هيئة التصديق أثناء إصدار الشهادة

"يتم إصدار الشهادات من قبل سلطة تصديق (S/MIME CA) وفقاً لسياسة ممارسات التصديق (CPS) هذه، ويتضمن ذلك إجراءات تنسيقية بين موظف هيئة التسجيل المحلي (LRAO) وهيئة تسجيل شركة مصدر التكنولوجيا (TS RA) في الحالات التي تمتلك فيها مؤسسة مقدم الطلب هيئة تسجيل محلية خاصة بها؛ وبخلاف ذلك، يتم التعامل مع طلبات الشهادات -بما في ذلك الطلبات الخاصة بـكبار المسؤولين الحكوميين -(Governmental VIP Officials) مباشرة من قبل هيئة تسجيل شركة مصدر التكنولوجيا(TS RA) .

في حال معالجة طلب الشهادة من قبل موظف هيئة تسجيل محلي(LRAO) ، يتولى الموظف (LRAO) مهام التحقق من الهوية والتدقيق وفقاً للقسم (4.2.1)، بما في ذلك المصادقة على بيانات طلب الشهادة، ومراجعة المعلومات المقدمة من المشترك، والموافقة على طلب الشهادة. بعد ذلك، تقوم هيئة تسجيل شركة مصدر التكنولوجيا (TS RA) بتنفيذ خطوات التحقق الفني المطلوبة قبل الإصدار، والتي تشمل التحقق من السيطرة على صندوق البريد عبر البريد الإلكتروني ومعالجة سجلات تخويل سلطة التصديق(CAA) ، ومن ثم تقديم طلب توقيع الشهادة (CSR) إلى سلطة التصديق المعنية.

أما في حال معالجة طلب الشهادة مباشرة من قبل هيئة تسجيل شركة مصدر التكنولوجيا(TS RA) ، فتقوم السلطة (TS RA)بالمصادقة على طلب الشهادة وتنفيذ كافة خطوات التحقق الفني المطلوبة، بما في ذلك التحقق من السيطرة على صندوق البريد ومعالجة سجلات(CAA) ، وذلك قبل تقديم طلب توقيع الشهادة (CSR) إلى سلطة التصديق المعنية.

وعند استلام طلب توقيع الشهادة(CSR) ، تقوم سلطة التصديق (CA) بالتحقق من هيكلية وتنسيق الطلب، وإنشاء "شهادة أولية (Pre-certificate) "مقابلة، وإخضاع جميع العناصر المراد توقيعها لعملية الفحص الآلي (Linting) باستخدام أدوات معيارية عالمية للتأكد من المطابقة الفنية والامتثال للمعايير المعمول بها قبل التوقيع. وبعد نجاح عملية التحقق، تقوم سلطة التصديق بإنشاء الشهادة النهائية وفقاً لنموذج الشهادة المعد مسبقاً، وتجعلها متاحة للتنزيل عبر بوابة هيئة التسجيل(Web RA Portal) ، حيث تصدر سلطة التصديق الشهادة بحالة "نشطة".(Active) ".

4.3.2 إشعار المشترك بإصدار الشهادة من قبل هيئة التصديق

بالنسبة لشهادات البريد الإلكتروني الآمن S/MIME:الصادرة للأشخاص الطبيعيين: يُبلّغ المشترك عبر البريد الإلكتروني أن الشهادة قد تم إنشاؤها وتُتاح الشهادة للتنزيل من حسابه في بوابة هيئة التسجيل الإلكترونية.

بالنسبة لشهادة مستجيبOCSP: يُبلّغ المدير المعني عند استلام الشهادة من فريق هيئة التسجيل في شركة مصدر التكنولوجيا.

4.4 قبول الشهادة

4.4.1 السلوك الذي يمثل قبول الشهادة

بالنسبة لشهادات البريد الإلكتروني الآمن S/MIMEالصادرة للأشخاص الطبيعيين: يقوم المشترك بتنزيل الشهادة من بوابة هيئة التسجيل الإلكترونية ثم يتحقق من محتواها وفي حال وجود أي تناقضات يباشر المشترك التواصل مع ضابط هيئة التسجيل المحلي وقد يؤدي ذلك إلى إلغاء الشهادة وإصدار شهادة مصححة.

تُعتبر الشهادة مقبولة في حال عدم تقديم المشترك أي اعتراض إلى ضابط هيئة التسجيل المحلي خلال خمسة أيام عمل من تاريخ استلام إشعار إنشاء الشهادة عبر البريد الإلكتروني.

بالنسبة لشهادة مستجيبOCSP: تُنشر الشهادة في مستودع المفاتيح المستهدف كجزء من مراسيم التشغيل الداخلية الخاصة بشركة مصدر التكنولوجيا.

4.4.2 نشر الشهادة من قبل هيئة التصديق

لا تقوم هيئة التصديق هذه بنشر شهادات المستخدم النهائي باستثناء مشاركتها مع المشتركين.

4.4.3 إشعار جهات أخرى بإصدار الشهادة من قبل هيئة التصديق

لا يوجد نص.

4.5 استخدام زوج المفاتيح والشهادة

4.5.1 استخدام المفتاح الخاص بالمشترك والشهادة

يجب على المشتركين الالتزام بالواجبات التالية:

- تقديم معلومات صحيحة ومُحدّثة إلى ضابط هيئة التسجيل المحلي ضمن طلبهم.
- عدم العبث بالشهادة.
- استخدام الشهادات فقط للأغراض القانونية والمصرح بها وفقاً لمتطلبات سياسة الشهادات المعتمدة لمزود خدمات الثقة وهذا البيان.
- حماية المفتاح الخاص وجميع البيانات السرية المرتبطة به من الاختراق أو الفقدان أو الكشف أو أي استخدام غير مصرح به.
- إشعار ضابط هيئة التسجيل المحلي فوراً إذا أصبحت أي من معلومات الشهادة غير صحيحة أو في حال وقوع اختراق أو فقدان أو كشف أو استخدام غير مصرح به.

- عدم استخدام الشهادة بعد انتهاء فترة صلاحيتها أو بعد إلغائها.
- التوقف عن استخدام المفتاح الخاص بعد انتهاء صلاحية الشهادة أو إلغائها.

يرجى الرجوع إلى القسم 9.6.3 من هذا البيان لمزيد من التفاصيل التكميلية.

4.5.2 استخدام المفتاح العام من قبل الطرف المعتمد

يتوجب على الطرف المعتمد الذي يستند إلى شهادة صادرة من هيئة التصديق هذه ما يلي:

- استخدام برنامج يتوافق مع معيار X.509 ومعايير IETF PKIX ذات الصلة للتحقق من توقيع الشهادة وفترة صلاحيتها.
- التحقق من الشهادة من خلال قائمة إلغاء الشهادات أو خدمة حالة الصلاحية OCSP وفقاً لإجراءات التحقق من سلسلة الشهادات.
- الوثوق بالشهادة فقط إذا لم تُلغ وكانت ضمن فترة الصلاحية.
- الوثوق بالشهادة فقط للغرض المخصص لها ووفقاً لهذا البيان.

4.6 تجديد الشهادة

غير قابل للتطبيق.

4.6.1 حالات تجديد الشهادة

غير قابل للتطبيق.

4.6.2 من يمكنه طلب التجديد

غير قابل للتطبيق.

4.6.3 معالجة طلبات تجديد الشهادة

غير قابل للتطبيق.

4.6.4 إشعار المشترك بإصدار الشهادة الجديدة

غير قابل للتطبيق.

4.6.5 السلوك الذي يمثل قبولاً للشهادة المجددة

غير قابل للتطبيق.

4.6.6 نشر الشهادة المجددة من قبل هيئة التصديق

غير قابل للتطبيق.

4.6.7 إشعار جهات أخرى بإصدار الشهادة المجددة من قبل هيئة التصديق

غير قابل للتطبيق.

4.7 إعادة إصدار المفتاح

إعادة إصدار المفتاح هي عملية إصدار شهادة جديدة للمشترك بمفتاح عام جديد وفترة صلاحية جديدة بينما قد تظل المعلومات الأخرى في الشهادة كما هي.

تدعم هيئة التصديق لشهادات البريد الإلكتروني الآمن S/MIMEالتابعة لمصدر التكنولوجيا عملية إعادة إصدار المفتاح وتتبع العملية نفس إجراءات طلب الشهادة الأولية بما في ذلك التحقق من الهوية وإصدار الشهادة والتواصل مع الأطراف ذات الصلة.

4.7.1 حالات إعادة إصدار المفتاح

قد تتم إعادة إصدار المفتاح أثناء صلاحية الشهادة أو بعد انتهائها أو بعد إلغائها وقد تؤدي عملية إعادة الإصدار إلى إلغاء أي شهادات البريد الإلكتروني الآمن S/MIMEنشطة حالياً.

4.7.2 من يمكنه طلب شهادة لمفتاح 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 الشهادة الجديدة

وفقاً لإجراءات إصدار الشهادة الأولية.

4.7.5 السلوك الذي يمثل قبولاً لشهادة أعيد إصدارها

وفقاً لإجراءات إصدار الشهادة الأولية.

4.7.6 نشر شهادة إعادة الإصدار من قبل هيئة التصديق

وفقاً لإجراءات إصدار الشهادة الأولية.

4.7.7 إشعار جهات أخرى بإصدار الشهادة المعاد إصدارها من قبل هيئة التصديق

وفقاً لإجراءات إصدار الشهادة الأولية.

4.8 تعديل الشهادة

4.8.1 حالات تعديل الشهادة

غير قابل للتطبيق.

4.8.2 من يمكنه طلب تعديل الشهادة

غير قابل للتطبيق.

4.8.3 معالجة طلبات تعديل الشهادة

غير قابل للتطبيق.

4.8.4 إشعار المشترك بإصدار الشهادة المعدلة
غير قابل للتطبيق.

4.8.5 السلوك الذي يمثل قبولاً للشهادة المعدلة
غير قابل للتطبيق.

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

4.8.7 إشعار جهات أخرى بإصدار الشهادة المعدلة من قبل هيئة التصديق
غير قابل للتطبيق.

4.9 إلغاء وتعليق الشهادة
توفر شركة مصدر التكنولوجيا إمكانية مستمرة للمشتركين لتقديم طلبات إلغاء الشهادات من خلال نظام إلكتروني متاح على مدار الساعة للمشتركين المصادق عليهم.

يحظر تعليق الشهادات ويُسمح فقط بإلغائها بشكل دائم. تُعالج إلغاء شهادات المشتركين وفقاً للفقرات الفرعية التالية.

4.9.1 حالات إلغاء شهادات المشتركين
يتم إلغاء شهادة المشترك خلال 24ساعة في حال تحقق واحد أو أكثر من الظروف التالية:

1. طلب المشترك للإلغاء خطياً.
2. إبلاغ المشترك لشركة مصدر التكنولوجيا أو هيئة التسجيل المحلية (LRAO) بأن طلب الشهادة الأصلي لم يكن مفوضاً، وأنه لا يمنح تفويضاً لاحقاً (بأثر رجعي).
3. حصول شركة مصدر التكنولوجيا أو هيئة التسجيل المحلية (LRAO) على دليل يثبت تعرض المفتاح الخاص (Private Key)للمشترك (المقابل للمفتاح المعلن في الشهادة) لعملية اختراق أو كشف(Key Compromise) .
4. عِلم شركة مصدر التكنولوجيا بوجود طريقة مثبتة أو مبرهنة يمكن من خلالها حساب المفتاح الخاص للمشترك بسهولة بناءً على المفتاح المعلن في الشهادة (مثل مفاتيح Debian الضعيفة).
5. حصول شركة مصدر التكنولوجيا على دليل يثبت أن عملية التحقق من تفويض النطاق أو السيطرة على صندوق البريد لأي عنوان بريدي في الشهادة لم تعد موثوقة.
6. عند انتهاء صلاحية وثيقة الهوية الوطنية (البطاقة الوطنية) أو جواز السفر الإلكتروني الذي استُخدم خلال عملية التحقق من الهوية.

تضمن شركة مصدر التكنولوجيا بدء إجراءات إلغاء الشهادة خلال 24 ساعة، وتقوم بإتمام عملية الإلغاء في غضون 5أيام كحد أقصى في حال تحقق واحد أو أكثر من الظروف التالية:

7. لم تعد الشهادة متوافقة مع متطلبات القسمين (6.1.5) و(6.1.6).
8. حصول شركة مصدر التكنولوجيا أو هيئة التسجيل المحلية (LRAO) على دليل يثبت إساءة استخدام الشهادة.

9. عِلم شركة مصدر التكنولوجيا أو (LRAO) بأن المشترك قد انتهك واحداً أو أكثر من التزاماته الجوهرية المنصوص عليها في شروط وأحكام استخدام المشترك.
10. عِلم شركة مصدر التكنولوجيا أو (LRAO) بأي ظرف يشير إلى أن استخدام عنوان البريد الإلكتروني أو اسم النطاق المؤهل بالكامل (FQDN) الوارد في الشهادة لم يعد مسموحاً به قانوناً (على سبيل المثال: صدور قرار قضائي أو تحكيمي يسحب الحق في استخدام العنوان أو اسم النطاق، أو انتهاء اتفاقية الخدمة أو الترخيص ذات الصلة، أو فشل صاحب الحساب في الحفاظ على الحالة النشطة للعنوان أو النطاق).
11. عِلم شركة مصدر التكنولوجيا أو (LRAO) بحدوث تغيير جوهري في المعلومات الواردة في الشهادة.
12. عِلم شركة مصدر التكنولوجيا أو (LRAO) بأن الشهادة لم تصدر وفقاً لسياسة ممارسات التصديق (CPS) هذه.
13. تحديد أو عِلم شركة مصدر التكنولوجيا أو (LRAO) بأن أي معلومة تظهر في الشهادة غير دقيقة.
14. انتهاء أو إلغاء أو إنهاء حق شركة مصدر التكنولوجيا في إصدار الشهادات بموجب المتطلبات الأساسية (Baseline Requirements)، ما لم تكن الشركة قد خططت للاستمرار في صيانة مستودع سجلات الإلغاء (CRL)وبروتوكول التحقق من حالة الشهادة عبر الإنترنت(OCSP) .
15. إذا كان الإلغاء مطلوباً بموجب سياسة ممارسات التصديق(CPS) .
16. عِلم شركة مصدر التكنولوجيا أو (LRAO) بوجود طريقة مثبتة أو مبرهنة تعرض المفتاح الخاص للمشترك للاختراق، أو في حال وجود دليل واضح على أن الطريقة المستخدمة لإنشاء المفتاح الخاص كانت معيبة.

4.9.1.1 الظروف التي تستدعي إلغاء شهادة هيئة التصديق التابعة

تُلغى شهادة TS SMIME CA خلال سبعة (7) أيام إذا تحقق واحد أو أكثر من الظروف التالية:

1. ورد طلب الإلغاء كتابياً.
2. أخطرت شركة مصدر التكنولوجيا هيئة التصديق المُصدِرة أي الهيئة الجذرية بأن طلب الشهادة الأصلي لم يكن مُخوّلاً ولم تُمنح له صلاحية بأثر رجعي.
3. حصلت شركة مصدر التكنولوجيا على دليل يثبت أن المفتاح الخاص لهيئة TS SMIME CA المرتبط بالمفتاح العام في الشهادة قد تعرّض لاختراق أو لم يعد يمتثل لمتطلبات القسمين 6.1.5 و 6.1.6.
4. حصلت هيئة التصديق المُصدِرة أي الهيئة الجذرية على دليل يفيد بإساءة استخدام شهادةTS SMIME CA .
5. علمت هيئة التصديق المُصدِرة أي الهيئة الجذرية بأن الشهادة لم تُصدر وفقاً لهذا المستند أو أن هيئة TS SMIME CAلم تلتزم به.
6. قررت هيئة التصديق المُصدِرة أي الهيئة الجذرية أن أية معلومات واردة في شهادة TS SMIME CA غير دقيقة أو مضللة.
7. توقفت هيئة TS SMIME CA عن العمل لأي سبب من الأسباب ولم تُرتب مع هيئة تصديق أخرى لتقديم دعم إلغاء الشهادات.
8. انتهى أو أُلغي أو أُنهي حق هيئة TS SMIME CA في إصدار الشهادات بموجب هذه المتطلبات ما لم تكن الهيئة الجذرية قد رتبت للاستمرار في صيانة مستودع CRL أوOCSP .
9. تطلب الإلغاء سياسة الشهادات أو بيان ممارسات الشهادات الخاص بالهيئة المُصدِرة أي الهيئة الجذرية.

4.9.2 من يمكنه طلب الإلغاء

يمكن تقديم طلبات الإلغاء من قبل الجهات التالية:

- هيئة التسجيل TS أو مسؤول هيئة التسجيل المحلي LRAO في الحالات الموضحة في القسم 4.9.1.
- يمكن للمشترك تقديم طلب إلغاء لشهادته الخاصة.
- أي طرف معتمد أو مزود برمجيات تطبيقية يملك دليلاً على اختراق شهادة المشترك أو استخدامها في نشر برمجيات خبيثة.
- شركة مصدر التكنولوجيا حسب تقديرها إذا ثبت اختراق مفتاح الهيئة.
- يمكن للمشتركين أو الأطراف المعتمدة أو مزودي البرمجيات التطبيقية أو أطراف ثالثة أخرى تقديم تقارير مشاكل الشهادات لإبلاغ شركة مصدر التكنولوجيا بسبب وجيه للاشتباه يستدعي بدء عملية إلغاء الشهادة.

تُقبل فقط طلبات الإلغاء المصرح بها.

4.9.3 إجراء طلب الإلغاء

الإلغاء المباشر من قبل المشترك أو مقدم الطلب:

يجوز للمشترك تقديم طلب إلغاء من خلال بوابة هيئة التسجيل الإلكترونية وتُعالج هذه الطلبات تلقائياً من قبل هيئة التصديق التابعة المعنية التي تُصدر قائمة إلغاء شهادات جديدة.

يُنفذ الإلغاء من خلال هيئة التسجيل TS أو مسؤول هيئة التسجيل المحلي LRAO وفق الخطوات التالية:

- يتحقق TS RA أو LRAO من صحة طلب الإلغاء ويؤكد هوية المشترك كما هو موضح في القسم 3.4.
- يدخل TS RA أو LRAO إلى حسابه في بوابة هيئة التسجيل الإلكترونية ويصدر أمراً مباشراً إلى هيئة التصديق المعنية لإلغاء شهادة المشترك.
- تُلغي هيئة التصديق الخاصة بالبريد الإلكتروني الآمن S/MIME CA الشهادة وتُحدَّث حالة الشهادة.
- يُبلّغ TS RA أو LRAO الأقسام المعنية داخلياً مثل الموارد البشرية أو الإدارة المختصة بإتمام عملية إلغاء الشهادة.
- إذا اقتضى الأمر يُحدِّث TS RA أو LRAO قائمته السوداء الداخلية بمعلومات المشترك.

معالجة إلغاء الشهادة من قبل هيئة التسجيل TS بناءً على تقرير عن مشكلة شهادة.

تحافظ شركة مصدر التكنولوجيا على قدرة مستمرة على مدار الساعة وطيلة أيام الأسبوع للاستجابة داخلياً لأي طلبات إلغاء عاجلة أو تقارير عن مشاكل الشهادات. وتوفر تعليمات مفصلة حول إجراءات الإلغاء وتقديم تقارير المشاكل من خلال صفحة مخصصة في المستودع العام والمتاحة عبر الرابط:
.https://pki.techsource.iq/repository/Certificate_Problem_Report.html

يجوز للمشتركين أو الأطراف المعتمدة أو مزودي البرمجيات التطبيقية أو أطراف ثالثة أخرى تقديم تقارير عن مشاكل الشهادات عبر البريد الإلكتروني: .certificate.problem@techsource.iq

ويُطلب من مقدم التقرير تضمين معلومات الاتصال الخاصة به مع تفاصيل الإساءة المشتبه بها والموضوع ذي الصلة.

تبدأ هيئة التسجيل TS بالتحقيق في تقرير المشكلة خلال 24 ساعة من استلامه وتُقرر ما إذا كان الإلغاء أو اتخاذ إجراءات مناسبة أخرى ضرورياً وذلك استناداً على الأقل إلى المعايير التالية:

- طبيعة المشكلة المزعومة.
- عدد التقارير الواردة عن شهادة أو موضوع معين.
- الجهة المقدمة للتقرير مثل إشعار من منظمة مكافحة البرمجيات الخبيثة أو جهة إنفاذ القانون والذي يحمل وزناً أكبر من شكوى مجهولة.
- التشريعات المحلية ذات الصلة.

وفي حال تقرر إلغاء الشهادة بناءً على تقرير المشكلة تُنفذ هيئة التسجيل TS إجراءات الإلغاء وفقاً لما ورد سابقاً في هذا القسم.

وإذا رأت شركة مصدر التكنولوجيا أن من المناسب إحالة تقرير الإلغاء إلى الجهات الأمنية فإنها تقوم بذلك.

4.9.4 فترة السماح لطلب الإلغاء

لا توجد فترة سماح لطلبات الإلغاء. تُعالج طلبات الإلغاء في الوقت المناسب بعد اتخاذ قرار الإلغاء وفي جميع الحالات ضمن الأطر الزمنية المحددة في القسم 4.9.1 من هذا البيان.

4.9.5 المدة التي يجب أن تُعالج خلالها هيئة التصديق طلب الإلغاء

تُعالج طلبات إلغاء الشهادات خلال مدة لا تتجاوز 24 ساعة.

أما في ما يخص تقارير مشاكل الشهادات فتبدأ هيئة التسجيل TS بالتحقيق خلال 24 ساعة من استلام التقرير. وتُباشر الهيئة التواصل مع المشترك وعند الاقتضاء مع الجهات المعنية الأخرى مثل الجهات الأمنية. ويُرسل إشعار أولي حول المشكلة إلى المشترك وإلى مقدم التقرير.

تُجري هيئة التسجيل TS تحقيقات إضافية بمشاركة مجلس حوكمة البنية التحتية للمفتاح العام TS PKI GB والمشترك والجهات ذات العلاقة مثل الجهات الأمنية لاتخاذ قرار بشأن الشهادة موضوع التقرير.

وإذا أسفرت نتائج التحقيقات عن أن الحالة تندرج ضمن إحدى حالات الإلغاء الواردة في القسم 4.9.1 فسيتم إلغاء الشهادة ضمن الإطار الزمني المنصوص عليه في القسم ذاته.

وبناءً على سبب الإلغاء يجوز لهيئة التسجيل TS الاتفاق مع المشترك على خطة لإصدار شهادة جديدة.

4.9.6 متطلبات التحقق من الإلغاء للطرف المعتمد

يقع على عاتق الطرف المعتمد وحده مسؤولية إجراء التحقق من حالة الإلغاء لجميع الشهادات في سلسلة الثقة قبل اتخاذ قرار الاعتماد على المعلومات الواردة في الشهادة. وتوفر هيئة التصديق الخاصة بالبريد الإلكتروني الآمن حالة الإلغاء عبر آليات مضمنة في الشهادة مثل CRL أوOCSP .

4.9.7 تكرار إصدار قوائم الإلغاء CRL إن وُجد

تنشر هيئة التصديق الخاصة بالبريد الإلكتروني الآمن قوائم الإلغاء CRL على فترات منتظمة وتُطبق القواعد التالية:

- تُحدّث قوائم الإلغاء كل 24 ساعة.
- تُحدد فترة صلاحية القائمة أي قيمة الحقل nextUpdate بـ 26 ساعة.

4.9.8 الحد الأقصى لتأخير إصدار CRL إن وُجد

تُصدر هيئة التصديق الخاصة بالبريد الإلكتروني الآمن قوائم الإلغاء في الوقت المحدد وفقاً لتكرار الإصدار المذكور في القسم 4.9.7 من هذا البيان.

4.9.9 توفر التحقق من الإلغاء أو الحالة عبر الإنترنت

تُوفر هيئة التصديق هذه مستجيب OCSP يتوافق مع المعيار RFC 6960 وتكون شهادته موقعة من قبل الهيئة ذاتها. ويُوفر هذا المستجيب المعلومات مباشرة لتطبيقات الأطراف المعتمدة استناداً إلى إجراءات الهيئة على الشهادات المُصدرة.

تتضمن شهادة OCSP امتداداً من نوع id-pkix-ocsp-nocheck كما هو مُعرف في RFC 6960 .

ويتم تضمين عنوان URL الفعلي الذي تستعلم منه الجهات المعتمدة في الشهادات المُصدرة من قبل هيئة التصديق الخاصة بالبريد الإلكتروني الآمن S/MIME CA .

4.9.10 متطلبات التحقق من الإلغاء عبر الإنترنت

يدعم مستجيب OCSP طريقتي HTTP GET وHTTP POST .

وفيما يخص حالة شهادات المشتركين:

- تكون صلاحية استجابة OCSP أكبر من أو تساوي ثماني ساعات.
- تكون صلاحية استجابة OCSP أقل من أو تساوي عشرة أيام.
- إذا كانت صلاحية استجابة OCSP أقل من ست عشرة ساعة تقوم هيئة TS S/MIME CA بتحديث المعلومات المقدمة من خلال بروتوكول التحقق من حالة الشهادات عبر الإنترنت قبل انقضاء نصف فترة الصلاحية السابقة لتاريخ nextUpdate .
- إذا كانت صلاحية استجابة OCSP أكبر من أو تساوي ست عشرة ساعة تقوم هيئة TS S/MIME CA بتحديث المعلومات المقدمة من خلال البروتوكول ذاته قبل ثماني ساعات على الأقل من nextUpdate وليس بعد أربعة أيام من thisUpdate .

إذا تلقى مستجيب OCSP طلباً عن حالة رقم تسلسلي لشهادة لم تُصدر من قبل هيئة TS S/MIME CA فإنه يرد بحالة "ملغاة" كما هو مُعرف في RFC 6960 (القسم 4.4.8: تعريف الإلغاء الموسّع).

تُراقب هيئة TS S/MIME CA مستجيب OCSP لرصد الطلبات الخاصة بالأرقام التسلسلية "غير المستخدمة" وذلك ضمن إجراءات المراقبة الأمنية وتؤدي كل حالة من هذا النوع إلى فتح تحقيق من قبل الفرق المختصة في فريق عمليات TS .

4.9.11 أشكال أخرى متاحة للإعلان عن الإلغاء

تعتمد هيئة TS S/MIME CA فقط على OCSP و CRL كوسيلتين لنشر معلومات إلغاء الشهادات.

4.9.12 متطلبات خاصة باختراق المفتاح

إذا اكتشفت شركة مصدر التكنولوجيا أو كان لديها سبب للاعتقاد بحدوث اختراق في المفتاح الخاص لهيئة TS S/MIME CA فإنها تعلن فوراً عن حالة طوارئ وتفعّل خطة استمرارية الأعمال الخاصة بها. كما تقوم بالآتي:

- تحديد نطاق الشهادات الواجب إلغاؤها.
- إلغاء الشهادات المتأثرة خلال 24 ساعة ونشر قوائم الإلغاء CRL على الإنترنت خلال 30 دقيقة من إنشائها.
- بذل جهد معقول لإبلاغ الجهات الحكومية والمشتركين والأطراف المعتمدة المحتملة بحدوث اختراق.
- توليد زوج مفاتيح جديد لهيئة التصديق وفقاً للسياسات والإجراءات التشغيلية المعتمدة لدى الشركة.

يجوز للأطراف إثبات حدوث اختراق للمفتاح باستخدام الوسائل التالية:

- تقديم طلب توقيع شهادة CSR موقع أو مفتاح خاص أو استجابة لتحدٍّ موقع باستخدام المفتاح الخاص وقابلة للتحقق باستخدام المفتاح العام.
- تقديم المفتاح الخاص نفسه.

4.9.13 الظروف التي تستدعي التعليق
غير قابل للتطبيق.

4.9.14 من يمكنه طلب التعليق
غير قابل للتطبيق.

4.9.15 إجراء طلب التعليق
غير قابل للتطبيق.

4.9.16 حدود فترة التعليق
غير قابل للتطبيق.

4.10 خدمات حالة الشهادة
يُرجى الرجوع إلى القسم 4.9.6 من هذا البيان. بالإضافة إلى ذلك تم اعتماد الأحكام التالية:

4.10.1 الخصائص التشغيلية
تنشر هيئة التصديق الخاصة بالبريد الإلكتروني الآمن S/MIME CA قوائم الإلغاء CRL في مستودع عام يمكن الوصول إليه من قبل الأطراف المعتمدة. كما يُوفر مستجيب OCSP لهيئة التصديق S/MIME CA واجهة HTTP متاحة أيضاً للأطراف المعتمدة.

لا تُزال إدخالات الإلغاء من قوائم CRL أو من استجابات OCSP بعد انتهاء صلاحية الشهادات الملغاة. وتحتوي قائمة CRL على الامتداد "ExpiredCertsOnCRL" X.509 كما هو معرّف في المعيار ISO / IEC 9594-8 أو التوصيةITU-T X.509 .

4.10.2 توفر الخدمة
يمكن الوصول إلى المستودع العام الذي تُنشر فيه معلومات الشهادات وقوائم الإلغاء على مدار الساعة وطيلة أيام الأسبوع ويضمن توفرية لا تقل عن 99.6% خلال فترة سنة واحدة. تُشغل هيئة S/MIME CA TS وتُدير إمكانيات CRL و OCSP باستخدام موارد كافية لضمان زمن استجابة لا يتجاوز عشر ثوانٍ في الظروف التشغيلية العادية.

وتحافظ هيئة TS S/MIME CA على قدرة استجابة داخلية على مدار الساعة وطيلة أيام الأسبوع للتعامل مع تقارير مشاكل الشهادات ذات الأولوية العالية كما هو موضح في القسم 4.9.3 من هذا البيان. وعند الاقتضاء تُحيل تلك الشكاوى إلى الجهات الأمنية و/أو تُلغي الشهادة موضوع الشكوى.

4.10.3 الخصائص الاختيارية

لا يوجد نص محدد.

4.11 إنهاء الاشتراك

ترتبط فترة الاشتراك بفترة صلاحية الشهادة. وينتهي الاشتراك عند انتهاء صلاحية الشهادة أو إلغائها.

4.12 حفظ واستعادة المفاتيح

4.12.1 سياسة وممارسات حفظ واستعادة المفاتيح

غير مدعومة.

4.12.2 سياسة وممارسات تغليف واستعادة مفاتيح الجلسة

غير قابل للتطبيق.

5 الضوابط الخاصة بالمنشآت والإدارة والتشغيل

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

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

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

يشتمل البرنامج الأمني لشركة مصدر التكنولوجيا على تقييم سنوي للمخاطر يتضمن ما يلي:

1. **تحديد التهديدات:** رصد التهديدات الداخلية والخارجية المتوقعة التي قد تؤدي إلى الوصول غير المصرح به، أو الإفصاح، أو إساءة الاستخدام، أو التعديل، أو التدمير لأي من بيانات الشهادات أو عمليات إدارة الشهادات.
2. **تحليل الأثر:** تقييم احتمالية حدوث هذه التهديدات والأضرار المحتملة الناجمة عنها، مع الأخذ بعين الاعتبار درجة حساسية بيانات الشهادات وعمليات إدارتها.

3. **تقييم الكفاءة:** تقييم مدى كفاية السياسات، والإجراءات ونظم المعلومات والتكنولوجيا والترتيبات الأخرى التي تتبعها شركة مصدر التكنولوجيا لمواجهة هذه التهديدات.

وبناءً على تقييم المخاطر، تقوم شركة مصدر التكنولوجيا بتطوير وتنفيذ وصيانة خطة أمنية تتكون من إجراءات وتدابير ومنتجات أمنية مصممة لتحقيق الأهداف المذكورة أعلاه، ولإدارة والتحكم في المخاطر التي تم تحديدها، وبما يتناسب مع حساسية بيانات الشهادات وعمليات إدارتها.

تتضمن الخطة الأمنية ضمانات **إدارية**، وتنظيمية، وتقنية ومادية ملائمة لحساسية البيانات والعمليات. كما تراعي الخطة التكنولوجيا المتاحة وتكلفة تنفيذ التدابير المحددة، وتعمل على تطبيق مستوى معقول من الأمن يتناسب مع الضرر الذي قد ينتج عن أي خرق أمني وطبيعة البيانات المراد حمايتها.

5.1 الضوابط الأمنية المادية

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

5.1.1 موقع المنشأة والبناء

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

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

5.1.2 الوصول المادي

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

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

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

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

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

5.1.3 الطاقة وتكييف الهواء

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

5.1.4 التعرض للمياه

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

5.1.5 الوقاية من الحرائق والحماية منها

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

5.1.6 تخزين الوسائط

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

5.1.7 التخلص من النفايات

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

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

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

5.1.8 النسخ الاحتياطي خارج الموقع

تُنفذ نسخ احتياطية كاملة وتزايدية بشكل روتيني لأنظمة هيئة التصديق للبريد الإلكتروني الآمن لضمان توفر بيانات كافية لاستعادة الأنظمة عند الحاجة.

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

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

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

5.2 الضوابط الإجرائية

5.2.1 الأدوار الموثوقة

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

الأدوار الموثوقة التالية معتمدة لدى هيئة التصديق للبريد الإلكتروني الآمن الخاصة بشركة مصدر التكنولوجيا:

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

5.2.2 عدد الأشخاص المطلوب لكل مهمة

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

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

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

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

5.2.3 التحقق من الهوية والمصادقة لكل دور

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

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

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

5.2.4 الأدوار التي تتطلب الفصل في الواجبات

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

5.3 ضوابط الأفراد

5.3.1 المؤهلات والخبرة ومتطلبات التصريح

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

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

- أي تصاريح إضافية تُعد ضرورية حسب تقدير الجهة المختصة.

5.3.2 إجراءات التحقق من الخلفية

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

5.3.3 متطلبات التدريب

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

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

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

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

5.3.4 تواتر ومتطلبات التدريب المتكرر

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

5.3.5 تواتر وتتابع تناوب الوظائف

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

5.3.6 العقوبات على الأفعال غير المصرح بها

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

5.3.7 متطلبات المتعاقدين المستقلين

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

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

5.3.8 الوثائق المقدمة للموظفين

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

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

5.4 إجراءات تسجيل السجلات التدقيقية

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

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

5.4.1 أنواع الأحداث المسجلة:

يتم إنشاء سجلات تدقيق (Audit logs) لجميع الأحداث المتعلقة بأمن وخدمات أنظمة سلطة تصديق (S/MIME CA) الخاصة بشركة مصدر التكنولوجيا.

تقوم شركة مصدر التكنولوجيا بتسجيل الأحداث المتعلقة بالإجراءات المتخذة لمعالجة طلبات الشهادات وإصدارها، بما في ذلك جميع المعلومات التي تم إنشاؤها والوثائق التي تم استلامها فيما يتعلق بطلب الشهادة، بالإضافة إلى الوقت والتاريخ، والموظفين المشاركين في تلك العملية.

تلتزم شركة مصدر التكنولوجيا بإتاحة هذه السجلات للمدقق المؤهل (Qualified Auditor) كدليل على امتثال سلطة التصديق (CA) لهذه المتطلبات.

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

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

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

تُسجّل الأحداث التالية المتعلقة بعمليات هيئة التصديق للبريد الإلكتروني الآمن:

1. أحداث إدارة دورة حياة مفتاح هيئة التصديق للبريد الإلكتروني الآمن وتشمل ما يلي:

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

2. أحداث إدارة دورة حياة شهادات هيئة التصديق للبريد الإلكتروني الآمن وشهادات المشتركين وتشمل ما يلي:

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

3. الأحداث الأمنية وتشمل ما يلي:

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

6. الدخول إلى موقع هيئة التصديق أو الخروج منه.

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

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

5.4.2 تكرار مراجعة سجلات العمليات

يضمن مجلس حوكمة البنية التحتية للمفاتيح العامة TS PKI GB قيام الموظفين المعنيين بمراجعة ملفات السجل على فترات منتظمة للتحقق من سلامة السجلات وضمان التعرف على الأحداث غير الطبيعية في الوقت المناسب. ويُطبق مجلس TS PKI GB دورة مراجعة لسجلات التدقيق على النحو التالي كحد أدنى:

- تُراجع سجلات التدقيق والأمان الخاصة بتطبيقات هيئة التصديق من قبل فريق المراقبة والامتثال شهرياً.
- تُراجع سجلات التدقيق والأمان الخاصة بأنظمة هيئة التصديق الإلكترونية مثل مستجيب OCSP من قبل فريق المراقبة والامتثال شهرياً للتحقق من سلامة عمليات التسجيل واختبار وظيفة المراقبة اليومية والتأكد من تشغيلها بشكل صحيح.
- تُراجع سجلات الدخول المادي وإدارة المستخدمين على أنظمة TS PKI من قبل فريق المراقبة والامتثال بشكل ربع سنوي للتحقق من سياسات الدخول المادي والمنطقي.
- ينفذ فريق التدقيق والامتثال في مجلس TS PKI GB تدقيقاً داخلياً على عمليات هيئة التصديق TS S/MIME CAبشكل سنوي. ويطلب المجلس عينات من تقارير مراجعة السجلات والسجلات المدققة التي تم جمعها منذ دورة التدقيق السابقة كجزء من هذا التدقيق الداخلي.
- تُجمع الأدلة على مراجعات سجلات التدقيق ونتائج عمليات المراجعة والإجراءات التصحيحية المنفذة وتُؤرشف.

5.4.3 فترة الاحتفاظ بسجلات التدقيق

يضمن فريق عمليات TS الاحتفاظ بسجلات التدقيق لمدة لا تقل عن سنتين أو وفقاً لما هو مذكور في القسم 5.5.2 على النحو التالي.

1. سجلات أحداث إدارة دورة حياة شهادات ومفاتيح هيئة التصديق كما هو موضح في القسم 5.4.1 (1) بعد تحقق أحد الأمرين التاليين أيهما يأتي لاحقاً:
   1. إتلاف المفتاح الخاص لهيئة التصديق.
   2. إلغاء أو انتهاء صلاحية آخر شهادة من شهادات هيئة التصديق ضمن مجموعة الشهادات التي تتضمن امتداد X.509v3 basicConstraints يحتوي على الحقل CA مضبوط على true والتي تشترك في مفتاح عام واحد مرتبط بالمفتاح الخاص لهيئة التصديق.

2. سجلات أحداث إدارة دورة حياة شهادة المشترك كما هو موضح في القسم 5.4.1 (2) بعد إلغاء أو انتهاء صلاحية شهادة المشترك.
3. سجلات أي حدث أمني كما هو موضح في القسم 5.4.1 (3) بعد وقوع الحدث مباشرة.

5.4.4 حماية سجلات التدقيق

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

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

5.4.5 إجراءات النسخ الاحتياطي لسجلات التدقيق

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

- خُزنت وسائط النسخ الاحتياطي محلياً في موقع هيئات التصديق التابعة ضمن موقع آمن.
- أُودعت نسخة ثانية من بيانات وسجلات التدقيق في موقع التعافي من الكوارث الذي يوفر أماناً فيزيائياً وبيئياً مماثلاً للموقع الرئيسي.

5.4.6 نظام جمع سجلات التدقيق (الداخلي مقابل الخارجي)

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

5.4.7 الإخطار إلى مصدر الحدث

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

5.4.8 تقييمات الثغرات الأمنية

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

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

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

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

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

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

جُمعت وأُرشفت أدلة تنفيذ تقييمات الثغرات الأمنية واختبارات الاختراق من قبل موظفي هيئة التصديق للبريد الإلكتروني الآمن المختصين.

5.5 أرشفة السجلات

5.5.1 أنواع السجلات المؤرشفة

أرشفت هيئات التصديق التابعة جميع سجلات التدقيق كما ورد في القسم 5.4.1 بالإضافة إلى ما يلي:

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

5.5.2 مدة الاحتفاظ بالأرشيف

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

بالإضافة إلى ذلك احتفظت هيئات التصديق التابعة بما يلي:

أ) جميع الوثائق المؤرشفة المرتبطة بأمن أنظمة هيئة التصديق وأنظمة إدارة الشهادات كما ورد في القسم 5.5.1.

ب) جميع الوثائق المؤرشفة المتعلقة بالتحقق من الطلبات أو إصدار الشهادات أو إلغائها كما ورد في القسم 5.5.1 وذلك بعد تحقق أحد الشرطين الآتيين أيهما أتى لاحقاً:

1. آخر مرة استُند فيها إلى هذه السجلات والوثائق في التحقق أو الإصدار أو الإلغاء.
2. انتهاء صلاحية شهادات المشترك التي اعتمدت على هذه السجلات والوثائق.

5.5.3 حماية الأرشيف

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

5.5.4 إجراءات النسخ الاحتياطي للأرشيف

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

5.5.5 متطلبات ختم الوقت للسجلات

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

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

5.5.6 نظام جمع الأرشيف (داخلي أو خارجي)

اعتمد نظام جمع الأرشيف الخاص بهيئة التصديق للبريد الإلكتروني الآمن على بنية داخلية.

5.5.7 إجراءات الحصول على معلومات الأرشيف والتحقق منها

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

5.6 تبديل المفاتيح

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

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

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

5.7 الاستجابة للاختراقات واستعادة القدرة التشغيلية بعد الكوارث

5.7.1 إجراءات التعامل مع الحوادث والاختراقات

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

- إذا اشتبه الفريق بحدوث اختراق في المفتاح الخاص لهيئة التصديق اعتمد الإجراءات الواردة في خطة استمرارية الأعمال واستعادة القدرة التشغيلية بعد الكوارث الخاصة بمصدر التكنولوجيا وفي الحالات الأخرى قيّم الفريق

نطاق الضرر المحتمل لتحديد ما إذا اقتضى الأمر إعادة بناء هيئة التصديق أو إلغاء بعض الشهادات أو إعلان اختراق المفتاح الخاص.

- حدّد مجلس إدارة البنية التحتية إجراءات التبليغ عن الحادث ووسائل التواصل اللازمة وفقاً لخطة استمرارية الأعمال واستعادة القدرة التشغيلية بعد الكوارث.

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

5.7.2 تلف الموارد الحاسوبية أو البرمجيات أو البيانات

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

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

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

5.7.3 إجراءات اختراق المفتاح الخاص للجهة

بالنسبة لاختراق مفتاح المشترك راجع القسم 4.9.

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

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

5.7.4 قدرات استمرارية الأعمال بعد الكوارث

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

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

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

وضعت خطة استمرارية الأعمال لمصدر التكنولوجيا البنود التالية:

- شروط تفعيل الخطة.
- الإجراءات الطارئة.
- إجراءات الرجوع.
- إجراءات الاستئناف.
- جدول صيانة للخطة.
- متطلبات التوعية والتعليم.
- مسؤوليات الأفراد.
- هدف وقت الاستعادة(RTO) .
- اختبارات دورية لخطط الطوارئ.
- خطة الحفاظ على أو استعادة العمليات التشغيلية لهيئة التصديق للبريد الإلكتروني الآمن في الوقت المناسب بعد توقف العمليات أو فشل العمليات التجارية الحرجة.
- اشتراط تخزين المواد التشفيرية الحيوية مثل الجهاز التشفيري الآمن ومواد التفعيل في موقع بديل.
- تحديد ما يُعد توقفاً مقبولاً للنظام والفترة اللازمة للاستعادة.
- وتيرة أخذ نسخ احتياطية من معلومات العمل الأساسية والبرمجيات.
- المسافة بين مرافق الاستعادة والموقع الرئيسي.
- الإجراءات المتبعة لحماية المرافق قدر الإمكان خلال الفترة الممتدة بعد الكارثة وحتى استعادة بيئة آمنة سواء في الموقع الأصلي أو في موقع بعيد.

لا تفصح شركة مصدر التكنولوجيا عن خطط استمرارية الأعمال (Business Continuity Plans) للمشتركين، أو الأطراف المعتمدة، أو مزودي برامج التطبيقات؛ ولكنها تلتزم بتزويد المدققين بخطة استمرارية الأعمال والخطط الأمنية بناءً على طلبهم.

5.8 إنهاء عمل هيئة التصديق أو هيئة التسجيل

أنهت مصدر التكنولوجيا تقديم خدمات هيئة التصديق للبريد الإلكتروني الآمن في الحالات التالية:

أ) بناءً على قرار صادر عن الإدارة التنفيذية لمصدر التكنولوجيا.
ب) بقرار مبرر صادر عن الهيئة المشرفة وهي الشركة العامة للاتصالات والمعلوماتية.
ت) بناءً على قرار قضائي نهائي لا يقبل الطعن.
ث) بعد تصفية أو إنهاء عمليات هيئة التصديق للبريد الإلكتروني الآمن.

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

غطت خطة الإنهاء الحد الأدنى من النقاط التالية:

- إرسال إشعار خطي إلى مدير لجنة إدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية حول نية التوقف عن ممارسة أنشطة هيئة التصديق وإرفاق نسخة من خطة الإنهاء الخاصة بمصدر التكنولوجيا قبل تسعين (90) يوماً على الأقل من:
  - التاريخ المتوقع للتوقف عن تنفيذ أنشطة هيئة التصديق.
  - انتهاء صلاحية تفويض مصدر التكنولوجيا لممارسة أنشطة هيئة التصديق إن وجدت دون نية لتجديد التفويض.
- ترتيب مصدر التكنولوجيا لحفظ سجلات الأرشفة وفقاً لما ورد في القسم 5.5.
- ترتيب مقدم خدمات الثقة للحفاظ على روابط خدمات التحقق من حالة الشهادات كما وردت في الشهادات الصالحة للفترة المقررة بعد الإنهاء.
- الإعلان عن نية مصدر التكنولوجيا لإنهاء أنشطة هيئة التصديق للبريد الإلكتروني الآمن في الصحف اليومية أو من خلال الوسائل التي يحددها مدير لجنة إدارة التوقيع الإلكتروني في الشركة العامة للاتصالات والمعلوماتية وذلك قبل ستين (60) يوماً على الأقل من تاريخ الإنهاء الفعلي أو انتهاء التفويض أيهما أسبق.
- تنفيذ الاتصالات اللازمة مع الأطراف المعنية وترتيب نقل سجلات هيئة التصديق المؤرشفة إلى جهة وصاية مناسبة.
- وضع خطة لدعم المشتركين الحاليين لمصدر التكنولوجيا قدر الإمكان خلال انتقالهم إلى مقدم خدمات ثقة آخر.
- إلغاء جميع الشهادات غير الملغاة أو غير المنتهية التي صدرت عن هذه الهيئة في نهاية فترة الإشعار بغض النظر عن طلب المشتركين لذلك.
- اتخاذ التدابير اللازمة لضمان عدم التسبب في أي اضطراب للمشتركين أو الأطراف المعتمدة نتيجة توقف العمليات.
- وضع ترتيبات تضمن بشكل كافٍ الاستمرار في صيانة الأنظمة وتنفيذ التدابير الأمنية المتعلقة بالبيانات الحساسة والدقيقة.

6 الضوابط الأمنية التقنية

6.1 توليد أزواج المفاتيح وتثبيتها

6.1.1 توليد أزواج المفاتيح

6.1.1.1 توليد زوج مفاتيح هيئة التصديق

يُولد زوج مفاتيح هيئة التصديق للبريد الإلكتروني الآمن TS ضمن ذاكرة جهاز HSM معتمد وفقاً للمعيار FIPS 140-2 المستوى الثالث.

وتُسجَّل مراسيم توليد مفاتيح هيئة التصديق للبريد الإلكتروني الآمن TS بالفيديو وتُحفظ بشكل آمن لأغراض التدقيق.

يشهد على مراسيم توليد مفاتيح هيئة التصديق للبريد الإلكتروني الآمن TS مدقق داخلي أو خارجي بهدف إصدار تقرير تقييم يفيد بأن شركة مصدر التكنولوجيا:

1. وثّقت إجراءات توليد وحماية مفاتيح هيئة التصديق وفقاً لهذا البيان ووثيقة سياسة مقدم خدمات الثقة TSP CP.
2. تضمّنت التفاصيل المناسبة في سيناريو توليد مفاتيح هيئة التصديق.
3. نفّذت الإجراءات بحضور النصاب القانوني من الموظفين المخوّلين بما فيهم ممثلين عن مجلسTS PKI GB .
4. حافظت على ضوابط فعّالة توفر مستوى معقول من التأكيد على أن زوج مفاتيح هيئة التصديق تم توليده وحمايته بما يتماشى مع الإجراءات المنصوص عليها في هذا البيان والبيانات ذات الصلة.
5. نفّذت جميع الإجراءات المطلوبة خلال عملية توليد مفاتيح هيئة التصديق وفقاً لسيناريو توليد المفاتيح الخاص بها.

6.1.1.2 توليد زوج مفاتيح المشترك

تُولد مفاتيح المشتركين وفقاً للمتطلبات التالية:

- شهادات البريد الإلكتروني الآمن المُولدة على وحدات تشفير مادية: تُولد أزواج مفاتيح المشتركين داخل ذاكرة أجهزة تشفير مادية مطابقة للمعيار FIPS 140 المستوى الثاني وتمنع التصدير. يجب توليد الأزواج باستخدام خوارزمية توليد مفاتيح وأطوال مفاتيح كما هو موضح في القسمين 6.1.5 و 6.1.6 من هذا البيان.

ترفض شركة مصدر التكنولوجيا أي طلب شهادة إذا تحقق أحد الشروط التالية:

1. لم يستوفِ زوج المفاتيح متطلبات القسمين 6.1.5 أو 6.1.6.
2. وُجد دليل واضح على وجود خلل في الطريقة المستخدمة لتوليد المفتاح الخاص.
3. كانت هيئة التصديق على علم بطريقة مثبتة أو مثبتة تجريبياً تُعرض المفتاح الخاص للاختراق.
4. سبق لهيئة التصديق أن علمت بأن المفتاح الخاص قد تعرض للاختراق كما هو موضح في القسم 4.9.1.1.
5. كانت هيئة التصديق على علم بطريقة مثبتة أو مثبتة تجريبياً تُتيح حساب المفتاح الخاص بسهولة استناداً إلى المفتاح العام مثل مفتاح Debian الضعيف (راجع https://wiki.debian.org/SSLkeys).

6.1.2 تسليم المفتاح الخاص إلى المشترك

لا تقوم شركة مصدر التكنولوجيا بإنشاء المفاتيح الخاصة (Private Keys) للمشتركين للحصول على شهادات (S/MIME)الموثوقة عامةً، كما أنها لا تقوم بعمليات إيداع المفاتيح(Key Escrow) ، أو استردادها، أو الاحتفاظ بنسخ احتياطية منها.

وفي حال اكتشاف شركة مصدر التكنولوجيا أو اشتباهها في أنه قد تم إفشاء المفتاح الخاص للمشترك إلى شخص غير مخول أو مؤسسة غير تابعة للمشترك، تقوم الشركة فوراً بإلغاء جميع الشهادات التي تتضمن المفتاح المعلن (Public Key) المقابل للمفتاح الخاص الذي تم إفشاؤه.

6.1.3 تسليم المفتاح العام إلى هيئة التصديق

تقبل هذه الهيئة طلبات توقيع الشهادات (CSRs) فقط بعد تحققها داخل بوابة هيئة التسجيل على الويب.

6.1.4 تسليم المفتاح العام لهيئة التصديق إلى الأطراف المعتمدة

تُنشر شهادات المفاتيح العامة لهيئة التصديق للبريد الإلكتروني الآمن في مستودع مصدر التكنولوجيا العام.

6.1.5 أحجام المفاتيح

مفاتيح المشتركين تعتمد 2048 بت RSA أو 4096 بت RSA وفقاً للتوصية.

حجم مفاتيح هيئة التصديق للبريد الإلكتروني الآمن هو 384 بتECDSA .

6.1.6 توليد معلمات المفتاح العام والتحقق من جودتها

6.1.6.1 هيئة التصديق للبريد الإلكتروني الآمن

وُلدت المفاتيح الخاصة والعامة باستخدام تقنيات متقدمة لضمان جودة المعلمات أوفى جهاز HSM والبرمجيات التابعة له في الهيئة بمتطلبات FIPS 186-2 من حيث التوليد العشوائي والتحقق من الأوّلية استند فريق العمليات إلى القسم 6.1.6 من متطلبات الأساس لمعايير التحقق.

6.1.6.2 المشتركون

اعتمدت هيئة التسجيل والمسؤول المحلي عن التسجيل تقنيات مناسبة للتحقق من ملاءمة المفاتيح العامة المقدّمة.
رفضت المفاتيح الضعيفة استناداً إلى التوجيهات الواردة في القسم 6.1.6 من متطلبات الأساس لمنتدىCA/B .

6.1.7 أغراض استخدام المفاتيح (وفق حقلX.509 v3)

احتوت الشهادات الصادرة على سلسلة استخدام مفاتيح متوافقة مع[RFC 5280] .راجع القسمين 7.1 و7.3 من بيان الممارسة.

6.2 حماية المفاتيح الخاصة وضوابط هندسة وحدات التشفير

6.2.1 معايير وضوابط وحدات التشفير

اعتمدت وحدات أمنية مادية معتمدة وفق FIPS 140-2 المستوى 3 لتوليد وتخزين المفاتيح الخاصة. جُعلت وحدات HSMضمن أعمق مناطق الأمان داخل مرافق الاستضافة التابعة لهيئات مصدر التكنولوجيا الفرعية.

6.2.2 التحكم المتعدد في المفاتيح الخاصة(nمنm)

خضعت المفاتيح الخاصة لرقابة دائمة من قبل عدد من الأشخاص المخولين. وُثقت الأدوار الموثوقة المرتبطة بإدارة هذه المفاتيح ضمن إجراءات توليد المفاتيح وغيرها من المستندات الداخلية.

كُلّف الموظفون بأدوارهم من قبل مجلس حوكمة البنية التحتية لضمان الفصل الوظيفي وتطبيق مبادئ السيطرة المتعددة والمعرفة المنقسمة. نُفذ التحكم المتعدد باستخدام أسلوب معرفة المفتاح المنقسم m من n بحيث يشترط وجود شخصين على الأقل من أصل ثلاثة أمناء مفاتيح إضافة إلى مسؤولي HSM لتفعيل أو إعادة تفعيل المفتاح الخاص.

احتفظ المجلس بسجلات ورقية قابلة للتدقيق بشأن توزيع الرموز وكلمات المرور. سُجّل توزيع الرموز وكلمات المرور عند تغيير الأفراد.

6.2.3 إيداع المفتاح الخاص
لا تُودَع المفاتيح الخاصة لهيئة التصديق للبريد الإلكتروني الآمن.

6.2.4 النسخ الاحتياطي للمفتاح الخاص
احتُفِظ بنُسخ مفاتيح TS S/MIME CA الخاصة بشكل آمن داخل خزائن حصرية ضمن أعمق المناطق الأمنية في مرافق استضافة الهيئات الفرعية التابعة لشركة مصدر التكنولوجيا.

نُفذت عمليات النسخ الاحتياطي ضمن مراسيم توليد المفاتيح الخاصة بـTS S/MIME CA . نُفذت عملية النسخ الاحتياطي تحت إشراف السيطرة المتعددة والمعرفة المنقسمة نفسها المعتمدة على المفتاح الأساسي. خضعت عملية استرجاع المفتاح الاحتياطي للمبادئ نفسها في ما يخص السيطرة المتعددة والمعرفة المنقسمة.

شملت مراسيم المفاتيح الخاصة بـ TS S/MIME CA عملية النقل المادي للنسخة الاحتياطية من المرفق الأساسي إلى مرفق الاستعادة. شارك موظفون مخصصون في أدوار موثوقة في عملية النقل التي رافقها حراس أمن. أُخذت أحكام القسم 6.2.2 بعين الاعتبار أثناء النقل.

6.2.5 أرشفة المفتاح الخاص
لم تحتفظ الهيئة بأرشيف للمفاتيح الخاصة.

6.2.6 نقل المفتاح الخاص إلى أو من وحدة تشفير
اقتصر نقل أزواج مفاتيح هيئة التصديق على نسخ مباشر بين رمزين تشفيريين متوافقين من حيث المواصفات كما ورد في القسم 6.2.11. نُفذ النقل عبر مسار موثوق وتحت إشراف مشترك لعدة أشخاص.

لم تُنسخ المفاتيح الخاصة لهيئة التصديق في أي مرحلة إلى قرص أو أي وسيط تخزين آخر.

6.2.7 تخزين المفتاح الخاص على وحدة تشفير
لا توجد اشتراطات إضافية بخلاف ما ورد في الأقسام 6.2.1 و6.2.2 و6.2.4 و6.2.6.

6.2.8 طريقة تفعيل المفتاح الخاص

6.2.8.1 هيئة التصديق للبريد الإلكتروني الآمن
فُعّل المفتاح الخاص استناداً إلى مبادئ السيطرة الثنائية والمعرفة المنقسمة. استُخدم جهاز إدخال رقم التعريف الشخصي PINالموصول بوحدة HSM الخاصة بالهيئة ضمن إجراء التفعيل.

6.2.8.2 المشتركون
تحمّل المشتركون مسؤولية تفعيل مفاتيحهم الخاصة وحمايتها بما يتماشى مع الالتزامات المنصوص عليها في شروط واحكام المشترك.

أدخل المشتركون جهاز التوثيق الثنائي المخصص للبنية التحتية للمفاتيح العامة في قارئ البطاقة أو المنفذ المناسب. عند المطالبة قدّموا رقم التعريف الشخصي PIN المرتبط بالمفتاح لتفعيل المفتاح الخاص.

6.2.9 طريقة إلغاء تفعيل المفتاح الخاص

6.2.9.1 هيئة التصديق للبريد الإلكتروني الآمن

عُطلت المفاتيح الخاصة لهيئة التصديق وفقاً للتعليمات والوثائق التي زود بها مصنّع وحدة الأمن المادي.

6.2.9.2 المشتركون

أوكلت إلى المشتركين مسؤولية إلغاء تفعيل مفاتيحهم وحماية الوصول إليها طبقاً لما هو موضح في شروط واحكام المشترك.

6.2.10 طريقة إتلاف المفتاح الخاص

6.2.10.1 هيئة التصديق للبريد الإلكتروني الآمن

في الحالات الخارجة عن انتهاء عمر المفتاح اقتضى إتلاف المفتاح إجراء تحقيق وتفويض خاص من مجلس حوكمة البنية التحتية للمفاتيح العامة في مصدر التكنولوجيا. اشتملت عملية الإتلاف على تعيين موظفين محددين.

تتبع عملية الإتلاف إجراءات موثقة ويجب أن تشارك فيها كوادر مُعينة في أدوار موثوقة (Trusted Roles) بحد أدنى ثلاثة موظفين من الكادر الموثوق، وبحضور ممثل واحد على الأقل من مجلس إدارة البنية التحتية للمفاتيح العامة (PKI GB). علاوة على ذلك، يجب أن تتم عملية الإتلاف بشهادة مدقق مؤهل (Qualified Auditor).

أُتلفت مفاتيح TS S/MIME CA من خلال إجراءات موثقة تضم موظفين في أدوار موثوقة بحد أدنى ثلاثة أفراد وبحضور ممثل واحد على الأقل من مجلس الحوكمة. فرضت هذه الإجراءات مبدأ السيطرة المتعددة والمعرفة المنقسمة. ضمنت هذه الإجراءات إزالة المفاتيح من جميع وحدات الأجهزة بشكل دائم ونهائي.

6.2.10.2 المشترك

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

6.2.11 تصنيف وحدة التشفير

حصلت وحدات التشفير الخاصة بهيئة TS S/MIME CA على شهادة/تحقق من التوافق مع المعيار FIPS 140-2 المستوى 3.

6.3 جوانب أخرى من إدارة زوج المفاتيح

6.3.1 أرشفة المفتاح العام

راجع البند 5.5 للاطلاع على شروط الأرشفة.

6.3.2 فترة التشغيل وفترة استخدام المفتاح لزوج الشهادات

تكون صلاحية شهادات TS S/MIME CA ست سنوات وفترة استخدام المفتاح ثلاث سنوات. تُحدد أقصى مدة مسموح بها لصلاحية شهادة المشترك في القسم 7.1.

لا يُستخدم المفتاح الخاص لهيئة التصديق التابعة بعد انتهاء صلاحية الشهادة العامة المرتبطة به. ولا يُستخدم أيضاً لتوقيع شهادات المستخدمين النهائيين بعد انتهاء فترة استخدام المفتاح الخاص باستثناء شهادات قائمة الإلغاء وشهادات مستجيبي OCSP لخدمة تحقق الصلاحية.

لا يجوز أن تتجاوز صلاحية شهادات المشتركين 825 يوماً.

6.4 بيانات التفعيل

6.4.1 توليد بيانات التفعيل وتثبيتها

6.4.1.1 هيئةTS S/MIME CA

يُولَّد المفتاح الخاص وبيانات تفعيل HSM خلال مراسيم توليد المفاتيح. راجع القسمين 6.1.1 و6.2.8 لمزيد من التفاصيل.

6.4.1.2 المشترك

يقوم المشترك بإعداد وحماية بيانات التفعيل لمفاتيحه الخاصة بالقدر الكافي لمنع الفقدان أو السرقة أو الكشف غير المصرح به أو إساءة الاستخدام. تُعرض هذه الالتزامات على المشترك ضمن شروط واحكام المشترك.

6.4.2 حماية بيانات التفعيل

6.4.2.1 هيئةTS S/MIME CA

تضمن سياسة إدارة المفاتيح وإجراءات المراسيم الخاصة بهيئات التصديق التابعة لدى TS تطبيق مبادئ السيطرة المتعددة والمعرفة المنقسمة بشكل دائم لحماية مفاتيح الهيئة وبيانات تفعيل وحداتHSM .

خلال مراسيم توليد المفاتيح تبقى بيانات التفعيل تحت عهدة موظفي هيئات التصديق التابعة المعينين.

راجع القسمين 6.1 و6.2 لمزيد من التفاصيل.

6.4.2.2 المشترك

يحمي المشترك بيانات التفعيل لمفاتيحه الخاصة بالقدر اللازم لمنع الفقدان أو السرقة أو الكشف غير المصرح به أو الاستخدام غير المشروع. تُدرج هذه الالتزامات ضمن شروط واحكام المشترك.

6.4.3 جوانب أخرى لبيانات التفعيل

لا توجد اشتراطات محددة.

6.5 ضوابط أمن الحاسوب

6.5.1 المتطلبات التقنية الخاصة بأمن الحاسوب

حرصت شركة مصدر التكنولوجيا على تنفيذ ضوابط أمن الحاسوب بما يتوافق مع المعايير التقنية وإرشادات تعزيز الأمان الموصى بها من قبل المزودين كحد أدنى. وُثقت الضوابط الأمنية المطبقة ضمن سياسة العمل الداخلية الخاصة بهيئات

التصديق التابعة في مصدر التكنولوجيا. خضعت أنظمة هيئات التصديق التابعة في مصدر التكنولوجيا وعملياتها على وجه الخصوص للضوابط التالية:

1. فصل المهام وتطبيق السيطرة الثنائية على عمليات هيئة التصديق.
2. فرض السيطرة على الوصول المادي والمنطقي.
3. تدقيق الأحداث المتعلقة بالتطبيقات والأمان.
4. مراقبة مستمرة لأنظمة هيئات التصديق التابعة وحماية نقاط النهاية.
5. آليات نسخ احتياطي واستعادة لأنشطة هيئات التصديق التابعة.
6. تعزيز نظام تشغيل خوادم هيئات التصديق التابعة وفقاً لأفضل الممارسات وتوصيات المزودين.
7. بنية أمن شبكي معمّقة تشمل جدران حماية طرفية وداخلية وجدران حماية لتطبيقات الويب بالإضافة إلى أنظمة كشف التسلل.
8. إدارة استباقية للتحديثات ضمن عمليات التشغيل المعتمدة في هيئات التصديق التابعة.
9. فرض المصادقة متعددة العوامل على جميع الحسابات القادرة على إصدار الشهادات بشكل مباشر.

6.5.2 تقييم أمن الحاسوب

خضعت الجوانب التقنية لأمن الحاسوب لمراجعات دورية.

6.6 ضوابط تقنية لدورة الحياة

6.6.1 ضوابط تطوير الأنظمة

يُشحن العتاد أو البرمجيات المشتراة داخل حاويات مختومة مقاومة للتلاعب ويُركّب من قبل موظفين مؤهلين. تُشترى التحديثات للعتاد والبرمجيات بنفس الآلية المتبعة عند شراء المعدات الأصلية. يشارك موظفون موثوقون مخصصون في تنفيذ إعدادات هيئات التصديق التابعة في TS وفقاً لإجراءات تشغيل موثقة.

جُربت التطبيقات وطُورت ونُفذت بما يتماشى مع أفضل الممارسات في الصناعة الخاصة بإدارة التطوير والتغيير. لم يُنشر أي برنامج أو تحديث أو جهاز على الأنظمة الحية إلا بعد المرور بإجراءات إدارة التغيير والتكوين التي ينفذها فريق تشغيل البنية التحتية للمفاتيح العامة في مصدر التكنولجيا.

جُرى تعزيز جميع المنصات البرمجية والعتادية الخاصة بهيئات التصديق التابعة باستخدام أفضل الممارسات وتوصيات المزودين.

6.6.2 ضوابط إدارة الأمن

تُخصص الأجهزة والبرمجيات المُستخدمة في إعداد هيئات التصديق التابعة لشركة مصدر التكنولوجيا لتنفيذ المهام المرتبطة بهيئات التصديق فقط. ولا يتم توصيل أو تثبيت أي تطبيقات أو أجهزة أو وصلات شبكية أو برمجيات مكونة لا تُعد جزءاً من بنية المفتاح العام لشركة مصدر التكنولوجيا على معدات هيئات التصديق.

يُفرض إجراء لإدارة التهيئة بهدف ضمان توثيق وضبط تهيئة أنظمة هيئات التصديق التابعة لشركة مصدر التكنولوجيا وتعديلاتِها وتحديثاتها من قبل إدارة عمليات البنية التحتية للمفتاح العام الخاصة بالشركة. يتم فحص إعدادات أنظمة شركة مصدر التكنولوجيا بشكل منتظم، بحيث لا تتجاوز المدة الفاصلة بين فحص وآخر أسبوعاً واحداً كحد أقصى.

كما يُفرض إجراء لإدارة الثغرات لضمان فحص معدات هيئات التصديق التابعة لشركة مصدر التكنولوجيا لاكتشاف البرمجيات الخبيثة عند أول استخدام وبعد ذلك بشكل دوري. ويدعم هذا الإجراء معالجة الثغرات خلال مدة لا تتجاوز 96 ساعة من اكتشاف ثغرات حرجة لم تتم معالجتها سابقاً من قبل فريق عمليات البنية التحتية للمفتاح العام.

6.6.3 ضوابط أمن دورة الحياة

راجع القسم 6.5.1.

6.7 ضوابط أمن الشبكة

اعتمدت شركة مصدر التكنولوجيا ضوابط قوية لأمن الشبكة من خلال استخدام جدران نارية مُدارة وأنظمة كشف التسلل. تقسم الشبكة إلى عدة مناطق بناءً على العلاقة الوظيفية والمنطقية والمادية. تُطبق حدود الشبكة لتقييد الاتصال بين الأنظمة داخل المنطقة الواحدة أو بين المناطق المختلفة باستخدام قواعد تدعم فقط الخدمات والبروتوكولات والمنافذ ووسائل الاتصال التي حددتها هيئات التصديق التابعة على أنها ضرورية للعمليات مع تعطيل جميع الحسابات والتطبيقات والخدمات والبروتوكولات والمنافذ غير المستخدمة في عمليات هيئات التصديق. تُحاط أنظمة الإصدار وأنظمة إدارة الشهادات وأنظمة دعم الأمن ضمن منطقة شبكة عالية الأمان.

يتم إجراء فحوصات كشف الثغرات (Vulnerability scans) للشبكات مرة واحدة في كل ربع من السنة على الأقل، كما يتم إجراء اختبارات الاختراق (Penetration tests) سنوياً كحد أدنى. وتستند الجداول الزمنية لمعالجة الثغرات إلى درجة خطورتها، حيث تتم معالجة الثغرات الحرجة (Critical) خلال 24 ساعة، والثغرات عالية الخطورة (High) خلال 48 ساعة، بينما يتم حل المشكلات ذات الخطورة المنخفضة والمتوسطة خلال 96 ساعة. ويتم توثيق أي استثناءات، وتقييم مخاطرها، وتسجيلها رسمياً.

6.8 ختم الوقت

تُزامَن مكونات هيئة التصديق لشهادة S/MIME مع خدمة وقت موثوقة بدقة عالية. يدعم إعداد خدمة ختم الوقت دقة تصل إلى ±1 ثانية أو أفضل بالنسبة إلى التوقيت العالمي المنسق UTC.

7 ملفات الشهادات وقوائم الإلغاء (CRL) وخدمة التحقق عبر الإنترنت(OCSP)

7.1 ملف تعريف الشهادة

7.1.1 رقم الإصدار

تصدر هيئات التصديق التابعة لشركة مصدر التكنولوجيا شهادات X.509 بالإصدار الثالث كما هو محدد فيRFC 5280 .

7.1.2 امتدادات الشهادة

تلتزم شركة مصدر التكنولوجيا بمعايير RFC 5280 ومتطلبات الخط الأساسي (Baseline Requirements) في جميع الشهادات الصادرة عنها. تتضمن شهادات هيئات التصديق التابعة وشهادات الكيانات النهائية امتداد الاستخدام الموسّع للمفتاح (Extended Key Usage) الذي يحتوي على معرف غرض الاستخدامid-kp-emailProtection . لا يجوز تضمين معرف KeyPurposeId خاص أو أي ExtendedKeyUsage غير معرف في الشهادات.

7.1.3 معرفات كائنات الخوارزميات(Algorithm Object Identifiers)

تُصدر الشهادات من قبل هيئة التصديق باستخدام الخوارزميات الموضحة بمعرفات الكائن التالية:

الخوارزمية	معرف الكائن(OID)
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 تنسيقات الاسم

7.1.4.1 ترميز الاسم

تصدر شركة مصدر التكنولوجيا شهادات باستخدام تنسيقات أسماء تتوافق مع RFC 5280 والبند 7.1.4 من متطلبات الخط الأساسي.

7.1.4.2 معلومات الموضوع - شهادات المشتركين

تُحدَّد معلومات الموضوع ذات الصلة بشهادات البريد الإلكتروني الآمن S/MIMEفي الجدول التالي.

تصدر شركة مصدر التكنولوجيا شهادات تحتوي على حقول اسم الموضوع (Subject DN) بما يتوافق مع التعاريف المرتبطة بها كما ورد في البند 7.1.4 من متطلبات الخط الأساسي.

نوع الشهادة	اسم الموضوع(Subject DN)	اسم الموضوع البديل (Alternative Subject Name)
S/MIME	commonName - و organizationNameو organizationIdentifier و givenNameو surname. SERIALNUMBER - وcountryName	rfc822Name

7.1.4.3 معلومات الموضوع - شهادة هيئة التصديق التابعة لشهادةS/MIME

في شهادة S/MIME التابعة لشركة مصدر التكنولوجيا تتضمن السمات commonName و organizationName و countryName يشكّل جمع هذه المحتويات معرفاً يميّز هيئة التصديق بشكل فريد عن غيرها من هيئات التصديق الأخرى.

7.1.5 قيود الاسم

غير قابل للتطبيق.

7.1.6 معرف كائن سياسة الشهادة

يُستخدم معرف كائن سياسة الشهادة وفقاً لما ورد في RFC 3739 وRFC 5280 .

تستخدم هيئة التصديق لشهادة S/MIME معرفات كائن سياسة الشهادة المحددة ضمن مخطط OID للبنية التحتية للمفتاح العام الوطني العراقي. راجع قالب الشهادة في القسمين 7.1.10 و 7.1.11 للمزيد من التفاصيل.

7.1.7 استخدام امتداد قيود السياسة

لا يوجد شرط.

7.1.8 صياغة مؤهلات السياسة ودلالاتها

يُدعم استخدام مؤهلات السياسة كما هو معرّف فيRFC 5280 وتُحدَّد مؤهلات السياسة المستخدمة ضمن ملفات تعريف الشهادات في القسمين 7.1.10 و 7.1.11.

7.1.9 دلالات المعالجة لامتداد سياسات الشهادة الحرجة

لا يوجد شرط.

7.1.10 ملف تعريف شهادة هيئة التصديق لشهادة البريد الإلكتروني الآمن التابعة لشركة مصدر التكنولوجيا

CE2 = Critical Extension O/M3: O = Optional M = Mandatory

CO4 = Content: S = Static, D = Dynamic

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 SMIME 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 SMIME CA G1	UTF8 encoded
SubjectPublicKeyInfo	False	M	D		
AlgorithmIdentifier		M	D	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	

	SubjectPublicKey		M	D	Value of the key	
Extensions						
Authority Properties						
AuthorityKeyIdentifier		False	M	D		Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	
AuthorityInfoAccess		False	M	S		
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.itpc.gov.iq	OCSP responder URL
	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://pki.itpc.gov.iq /repository/cert/smime_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/smime_root_ca.crl	CARL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M	D		
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be

					supported as a minimum
Key Usage Properties					
keyUsage	True	M	S		
keyCertSign, cRLSign		M	S	True	
Policy Properties					
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.16.368.1.1.1.1	ITPC root CP/CPS
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.itpc.gov.iq/repository/cps	
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.5.3.3	Sponsor-validated Strict
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.5.4.3	Individual-validated Strict
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.5.2.3	Organization-validated Strict
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.5.1.3	Mailbox-validated Strict
Extended Key Usage Properties					
extKeyUsage	False	M	S		
emailProtection		M	S	True	

Basic Constraints Properties					
basicConstraints	True	M	S		
cA		M	S	True	
pathLenConstraint		M	S	0	

7.1.11 ملف تعريف شهادات البريد الإلكتروني الآمن

CE2 = Critical Extension O/M3: O = Optional M = Mandatory

CO4 = Content: S = Static, D = Dynamic

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

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

OrganizationName		M	D	The Subject's full legal organization name and/or an Assumed Name. If both are included, the Assumed Name SHALL appear first, followed by the full legal organization name in parentheses.	UTF8 encoded
OrganizationIdentifier		M	D	Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme.	a PrintableString or UTF8String
GivenName		M	D	Given Name of the Subject	UTF8 encoded
Surname		M	D	Surname of Subject	UTF8 encoded
SERIALNUMBER		M	D	an identifier assigned by the CA or RA to identify and/or to disambiguate the Subject	PrintableString encoded
CommonName		M	D	Mailbox address	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1) Null	
SubjectPublicKey		M	D	Public Key Key length: Key length: 2048 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M	D		

	KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate CA public key	
AuthorityInfoAccess		False	M			
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.techsource.iq	OCSP responder URL
	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://pki.techsource.iq/repository/certs/smime_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crlsCRLS/smime_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties						
keyUsage		True	M			
	digitalSignature, keyEncipherment		M	S	True	

Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.2.1.4	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.23.140.1.5.3.3	Sponsor-validated Strict
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.368.1.1.3.1.3	
Extended Key Usage Properties					
extKeyUsage	False	M			
emailProtection		M	S	True	
Subject Alternative Name Properties					
subjectAlternativeName	False	M			
rfc822name		M	D	One or more email addresses of the certificate owner	

7.2 ملف تعريف قائمة إلغاء الشهادات

CE2 = Critical Extension O/M3: O = Optional M = Mandatory

CO4 = Content: S = Static, D = Dynamic

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 SMIME 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 هيئات التصديق قوائم إلغاء الشهادات بالإصدار الثاني من X.509 راجع القسم 7.2 أعلاه.

7.2.2 امتدادات قائمة الإلغاء وإدخالاتها

يُعرض ملف تعريف قائمة الإلغاء في القسم 7.2 أعلاه.

7.3 ملف تعريف خدمة التحقق من الحالة عبر الإنترنت(OCSP)

CE2 = Critical Extension O/M3: O = Optional M = Mandatory

CO4 = Content: S = Static, D = Dynamic

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 SMIME 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 SMIME 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			

7.3.1 رقم الإصدار

وفقاً لملف تعريف شهادة OCSP الوارد في القسم 7.3.

7.3.2 امتدادات OCSP

وفقاً لملف تعريف شهادة OCSP الوارد في القسم 7.3.

هيكلية استجابة بروتوكول الاستعلام الآني عن حالة الشهادة.

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

Field	Value	Comment
responseStatus	"0" Response has valid confirmations	Result of the query. If the value of responseStatus is other than "0", the responseBytes field is not set.
responseBytes		
responseType	id-pkix-ocsp-basic	
BasicOCSPResponse		

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

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

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

8 تدقيق الامتثال والتقييمات الأخرى

تستهدف الإجراءات الموضحة في بيان ممارسة الشهادات (CPS) هذه المواءمة مع المتطلبات المحددة في القسم (1)، كما أنها تغطي كافة العناصر المعمول بها في معايير البنية التحتية للمفاتيح العامة (PKI) الحالية ذات الصلة بقطاعات الصناعة التي تعمل فيها شركة مصدر التكنولوجيا.

8.1 وتيرة أو ظروف التقييم

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

وأُجريت أيضاً تدقيقات داخلية وفق خطة تدقيق معتمدة من هيئة .PMA وفي حالات خاصة مثل حدوث خرق أمني جرى تنفيذ تدقيقات غير مخطط لها بناءً على طلب من هيئةPMA .

8.2 هوية أو مؤهلات المدقق

نُفذت التدقيقات الخارجية من قبل مدققين مؤهلين استوفوا المتطلبات التالية:

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

8.3 علاقة المدقق بالجهة الخاضعة للتدقيق

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

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

8.4 المواضيع المشمولة في التقييم

خضعت هذه الهيئة لتدقيقات امتثال للمعايير التالية:

- مبادئ ومعايير WebTrust الخاصة بهيئات التصديق.
- مبادئ ومعايير WebTrust الخاصة بهيئات التصديق – متطلبات شهادة البريد الإلكتروني الآمن.

- مبادئ ومعايير WebTrust الخاصة بهيئات التصديق – أمن الشبكات.

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

8.5 الإجراءات المتخذة نتيجة أوجه القصور

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

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

8.6 إيصال نتائج التدقيق

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

يتم نشر تقارير تدقيق (WebTrust) السنوية للعلن في موعد لا يتجاوز ثلاثة (3) أشهر من نهاية فترة التدقيق. وفي حال حدوث تأخير يتجاوز ثلاثة (3) أشهر، تقوم شركة مصدر التكنولوجيا بتقديم خطاب توضيحي موقع من قبل المدقق المؤهل. يمكن العثور على تقارير تدقيق (WebTrust) الخاصة بشركة مصدر التكنولوجيا على الرابط التالي: https://pki.techsource.iq/repository/ar/index.html.

8.7 التدقيق الذاتي

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

- تدقيقات ذاتية على عينات عشوائية تُشكل ثلاثة بالمئة على الأقل من الشهادات التي أصدرتها هيئة التصديق للبريد الإلكتروني الآمن الخوارزميات بدءاً من الفترة التي تلت مباشرة آخر عينة سُحِبت.

9 شؤون قانونية وتجارية أخرى

9.1 الرسوم

9.1.1 رسوم إصدار الشهادات أو تجديدها
تُحدد الرسوم المطبقة إن وُجدت بالاتفاق بين مصدر التكنولوجيا والمشتركين.

9.1.2 رسوم الوصول إلى الشهادات
لم يُذكر شرط خاص.

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

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

9.1.5 سياسة الاسترداد
لا تُقدّم أي مبالغ مستردة عن الرسوم المدفوعة.

9.2 المسؤولية المالية

9.2.1 تغطية التأمين
ضمنت مصدر التكنولوجيا شمول هيئة التصديق للبريد الإلكتروني الآمن بتغطية تأمينية قائمة.

9.2.2 أصول أخرى
لم يُذكر شرط خاص.

9.2.3 تغطية تأمينية أو ضمان للمشتركين النهائيين
راجع القسم 9.6.1.

9.3 سرية المعلومات التجارية

9.3.1 نطاق المعلومات السرية
اعتبرت مصدر التكنولوجيا المعلومات التالية معلومات سرية:

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

9.3.2 المعلومات الخارجة عن نطاق السرية

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

9.3.3 المسؤولية عن حماية المعلومات السرية

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

9.4 خصوصية المعلومات الشخصية

9.4.1 خطة الخصوصية

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

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

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

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

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

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

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

- الاتصالات بين أنظمة التسجيل ومشتركي الشهادات.
- الاتصالات بين أنظمة التسجيل وأنظمة هيئة التصديق للبريد الإلكتروني الآمن.
- الجلسات المخصصة لتسليم الشهادات.

9.4.2 المعلومات التي تُعامل على أنها خاصة

تُعتبر جميع المعلومات الشخصية غير المتاحة للعموم في محتوى الشهادة أو قائمة إلغاء الشهادات (CRL) معلومات خاصة.

9.4.3 المعلومات غير المصنفة كمعلومات خاصة

لا تُعتبر المعلومات الواردة في الشهادة أو قائمة إلغاء الشهادات (CRL) معلومات خاصة.

9.4.4 مسؤولية حماية المعلومات الخاصة

يتعامل موظفو TS PKI والموردون والمتعاقدون مع TS مع المعلومات الشخصية بسرية تامة بموجب التزامات TS التعاقدية التي لا تقل حمايةً عن الشروط المحددة في البند 9.4.1.

9.4.5 الإخطار والموافقة على استخدام المعلومات الخاصة

تضمن TS استخدام المعلومات الشخصية التي تم جمعها لأغراض إدارة دورة حياة الشهادة فقط بموافقة المشتركين.

9.4.6 الإفصاح بموجب إجراءات قضائية أو إدارية

لن تفصح TS عن أي معلومات خاصة دون موافقة مالك البيانات الشرعي أو إذن صريح بموجب أمر قضائي. راجع البند 9.4.1 لمزيد من التفاصيل.

9.4.7 ظروف أخرى للإفصاح عن المعلومات

لا يوجد شرط

9.5 حقوق الملكية الفكرية

تمتلك TS وتحتفظ بجميع حقوق الملكية الفكرية المتعلقة بقواعد بياناتها ومواقعها الإلكترونية وشهادات هيئات التصديق الرقمية وأي منشورات أخرى صادرة عن البنية التحتية للمفاتيح العامة (PKI)، بما في ذلك هذا المستند.

عندما تستخدم TS برامج من موردين خارجيين، تظل هذه البرامج ملكية فكرية لموردي المنتجات، ويخضع استخدامها من قبل هيئات التصديق التابعة لـ TS لاتفاقيات ترخيص بين TS وهؤلاء الموردين.

9.6 الإقرارات والضمانات

9.6.1 إقرارات وضمانات هيئة التصديق

عند إصدار شهادة قدّمت هيئة التصديق للبريد الإلكتروني الآمن الضمانات التالية لمستفيدي الشهادات.

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

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

وشملت الضمانات ما يلي.

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

9.6.2 إقرارات وضمانات وظيفة التسجيل

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

9.6.3 إقرارات وضمانات المشترك

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

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

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

9.6.4 إقرارات وضمانات الأطراف المعتمدة

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

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

9.6.5 إقرارات وضمانات المشاركين الآخرين

لم يُذكر شرط خاص.

9.7 إخلاء المسؤولية من الضمانات

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

- دقة أي معلومات واردة في الشهادات إلا بالقدر الذي يضمنه المشترك الذي يتحمل مسؤولية صحة ودقة جميع البيانات التي يرسلها إلى مصدر التكنولوجيا بغرض إدراجها في شهادة صادرة عن هيئة التصديق.

- أي أضرار غير مباشرة ناتجة عن أو مرتبطة باستخدام الشهادات أو إصدارها أو عدم إصدارها أو تقديم التواقيع الرقمية.
- الأفعال المتعمدة لأي طرف ثالث ينتهك القوانين المعمول بها في العراق بما في ذلك على سبيل المثال لا الحصر قوانين حماية الملكية الفكرية أو البرمجيات الخبيثة أو الوصول غير القانوني إلى أنظمة الحاسوب.
- أي أضرار مباشرة أو غير مباشرة ناتجة عن انقطاع لا يمكن السيطرة عليه في خدمات هيئة التصديق للبريد الإلكتروني الآمن.
- أي تحريف للمعلومات من قبل المشتركين أو الأطراف المعتمدة بناءً على المعلومات الواردة في هذا البيان أو أي وثائق أخرى صادرة عن مجلس إدارة البنية التحتية للمفاتيح العامة والمتعلقة بخدمات هيئة التصديق للبريد الإلكتروني الآمن.

9.8 حدود المسؤولية

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

9.9 التعويضات

لا ينطبق.

9.10 المدة والإنهاء

9.10.1 المدة

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

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

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

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

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

9.12.1 إجراء التعديل
راجع القسم 9.12.

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

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

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

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

9.14 القانون الناظم

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

9.15 الامتثال للقوانين المعمول بها

يتوافق هذا البيان وتقديم خدمات هيئة التصديق للبريد الإلكتروني الآمن مع القوانين النافذة والمعمول بها في جمهورية العراق.

9.16 أحكام متنوعة

9.16.1 الاتفاق الكامل

لا ينطبق.

9.16.2 التنازل أو التفويض

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

9.16.3 قابلية الفصل

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

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

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

9.16.4 التنفيذ (أتعاب المحاماة والتنازل عن الحقوق)

لا ينطبق.

9.16.5 القوة القاهرة

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

9.17 أحكام أخرى

لا ينطبق.