الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مشروع المعيار الوطني للتشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية

(NSCA-1:2025)

بروتوكول الإشارة: أبيض

تصنيف الوثيقة: عام

DISCLAIMER: The following cybersecurity standards document will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.

بسم الله الرحمن الرحيم

إخلاء مسؤولية: يُطبق ويفسّر هذا المستند وفق قوانين المملكة العربية السعودية، وبناء على هذا تُعد النسخة العربية اللغة المعتمدة والمرجع الوحيد في كل ما يتصل بمعاني هذا المستند او تفسيره

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر (شخصي وسري للمستلم فقط)

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل أو خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي+ مقيد

المستلم بالإشارة البرتقالية+ يمكنه مشاركة المعلومات في نفس المنشأة فقط.

برتقالي (مشاركة محدودة)

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة فقط أو مع من يتطلب الأمر منه اتخاذ إجراء يخص المعلومة من خارج المنشأة على أساس الحاجة للمعرفة.

أخضر (مشاركة في نفس المجتمع)

المستلم بالإشارة الخضراء يمكنه مشاركة المعلومات مع آخرين من نفس المنشأة أو منشأة أخرى على علاقة بمنشأته أو بنفس القطاع، ولا يسمح بتبادل المعلومات أو نشرها من خلال القنوات العامة.

أبيض (غير محدود)

يمكن للمستلم مشاركة المعلومات من غير حدود.

قائمة المحتويات

قائمة الجداول

قائمة الأشكال

الملخص التنفيذي

تعد الهيئة الوطنية للأمن السيبراني الجهة المختصة في المملكة العربية السعودية بالأمن السيبراني، والمرجع الوطني في شؤونه، وتهدف الى تعزيزه؛ حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية العالية والخدمات والأنشطة الحكومية وذلك كما ورد في تنظيم الهيئة الصادر بالأمر الملكي الكريم رقم ٦٨٠١، وتاريخ ١٤٣٩/٢/١١هـ. وقد اشتمل تنظيم الهيئة على اختصاصها بوضع السياسات والمعايير الوطنية للتشفير، وتحديثها، ومتابعة الالتزام بها.

ومن هذا المنطلق، قامت الهيئة الوطنية للأمن السيبراني بإصدار وثيقة المعيار الوطني للتشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية (NSCA-1:2025) وذلك بهدف وضع الحد الأدنى لمتطلبات التشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية. وتهدف هذه المعايير الى تسهيل التعرف وتوثيق وحماية الجهات والمستخدمين والبيانات والأنظمة والشبكات الوطنية. وتوضح هذه الوثيقة معايير التشفير الخاصة بإدارة الشهادات الرقمية وأحدث تطبيقاتها، وإدارة دورة المفاتيح، والأمن المادي.

إن وثيقة المعايير هذه تسلط الضوء على تفاصيل معايير التشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية (NSCA-1:2025). تم اعداد وبناء هذه الوثيقة استنادًا على أحدث وثيقة للمعايير الوطنية للتشفير (NCS-1:2020) وهي متوافقة معها بشكل كامل .

المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بإصدار المعيار الوطني للتشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية (NSCA-1:2025) بعد دراسة معايير وأطر عمل دولية للتشفير، ودراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة، وبعد الاطلاع على أفضل الممارسات والتجارب في مجال التشفير والاستفادة منها.

يهدف المعيار الوطني للتشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية لوضع الحد الأدنى من متطلبات التشفير التقنية والإجرائية التي يجب الالتزام بها من قبل الجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية (ويشار لها في هذه الوثيقة بـ "هيئة الشهادات"). كما تعد هذه الوثيقة استكمالًا لوثيقة المعايير الوطنية للتشفير فيما يتعلق بجوانب إدارة الشهادات الرقمية وتطبيقاتها المشتركة، وإدارة دورة حياة المفاتيح، والأمن المادي. . وعليه، فان هذه الوثيقة تفترض الالتزام المسبق للمعايير الوطنية للتشفير.

على الرغم من ان هذه الوثيقة تحدد الحد الأدنى المقبول لمتطلبات التشفير، فإنه من المهم جداً أن يضمن الملتزمون بهذا المعيار التطبيق الصحيح والآمن لها، وذلك لتفادي الثغرات الناتجة عن أخطاء التطبيق. سيتم تحديث هذه الوثيقة عند الحاجة بحسب المستجدات في مجال التشفير. ويلغي كل إصدار جديد من هذه الوثيقة كافة الإصدارات السابقة.

الأهداف

يهدف المعيار الوطني للتشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية إلى:

- إتاحة طريقة آمنة لتشغيل عمليات الجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية.
- تعزيز قدرات وصمود الأمن السيبراني الخاص بالجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية ضد التهديدات السيبرانية.
- المساهمة في رفع مستوى الأمن السيبراني على المستوى الوطني.

النطاق

قابلية التطبيق

ينطبق هذا المعيار على الجهات الحكومية والخاصة داخل المملكة العربية السعودية المشارِكة في بنية المفاتيح العامة التحتية الوطنية (PKI) وتشمل مصدري الشهادات الجذرية، والثانوية (CAs) والتي

تُصدر وتُخزن وتدير الشهادات الرقمية؛ والمشار اليها في هذه الوثيقة بـ "الجهة". عند الإشارة للمعايير الوطنية للتشفير، ستكون الإشارة الى اخر نسخة محدثة من وثيقة المعايير الوطنية للتشفير.

بيان قابلية التطبيق

تم تطوير هذا المعيار لتحديد متطلبات التشفير اللازمة في عمليات التشغيل لمزودي خدمات إصدار الشهادات الرقمية والمنشآت ذات العلاقة بها والتي تعمل في بنية المفاتيح العامة التحتية الوطنية (PKI). يوضح المعيار الحد الأدنى من متطلبات التشفير لتحقق بيئة آمنة لمزودي خدمات إصدار الشهادات الرقمية، وإدارة دورة حياة الشهادات الرقمية، وحماية أصول التشفير، والحفاظ على قابلية المراجعة. يجب على الشهادات الجذرية، والثانوية (CAs) الالتزام بجميع المتطلبات المذكورة في هذه الوثيقة.

تشجع الهيئة الجهات على تبني إجراءات أمنية وتشغيلية أخرى إضافية على ما تم ذكره في هذه الوثيقة بما يتناسب مع مستوى المخاطر الخاص بهم وذلك لتحسين وتعزيز صمود عملياتهم.

اعتبارات

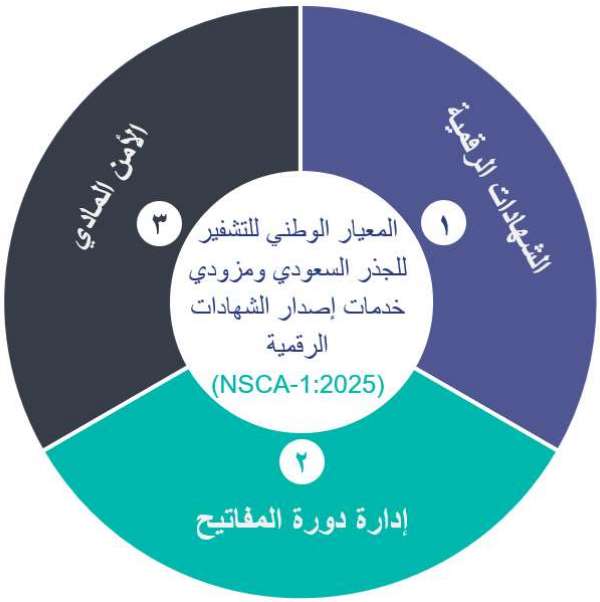
أصحاب المصلحة الرئيسيين لهذه الوثيقة

- الهيئة الوطنية للأمن السيبراني: المُصَدّر والمُرَاجع لهذا المعيار.
- هيئات الشهادات: الجهات المُلزمة بتطبيق وتحقيق الالتزام بهذا المعيار.

هيكلة الوثيقة

الأجزاء الرئيسية لهذه الوثيقة

شكل (١) يوضح الاجزاء الرئيسية لهذه الوثيقة



شكل (١) أجزاء الوثيقة

الأجزاء الفرعية للوثيقة

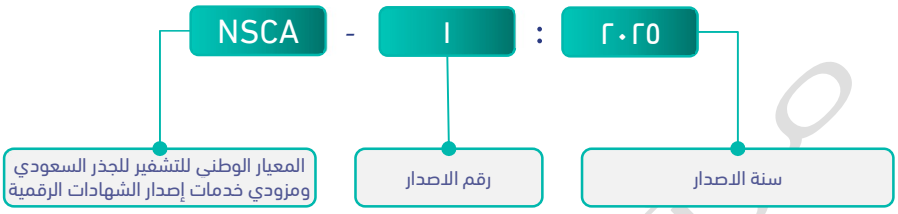
جدول (١) يستعرض الأجزاء الفرعية للمعيار الوطني للتشفير لهيئة شهادات الامن السيبراني

جدول (١) الأجزاء الفرعية للمعيار الوطني للتشفير لهيئة شهادات الامن السيبراني

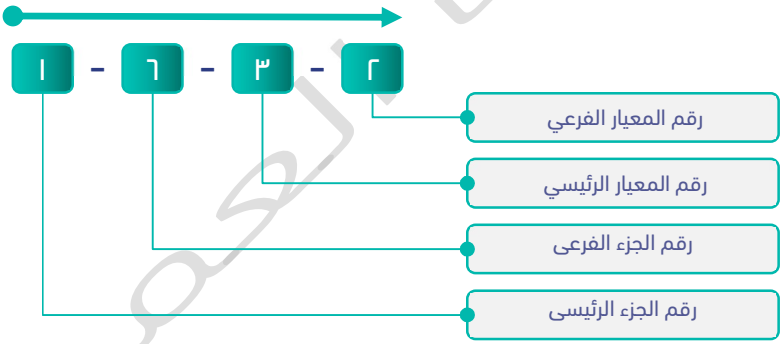
١. الشهادات الرقمية	١-١	التدقيق والتسجيل	١-٢	هيكلة الشهادات والحقول المطلوبة
	١-٣	اتفاقيات التسمية	١-٤	الخوارزميات المقبولة
	١-٥	التحقق وتوثيق هوية ملّاك الشهادة	١-٦	توليد وانشاء الشهادة
	١-٧	صلاحية الشهادات	١-٨	إيصال شهادة الجذر
	١-٩	تجديد الشهادات وتعديلها، وإعادة إصدارها باستخدام مفاتيح جديدة	١-١٠	إلغاء الشهادة
	١-١١	مصادقة مواقع الانترنت	١-١٢	التواقيع الالكترونية
	١-١٣	الأختام الالكترونية	١-١٤	الطوابع الزمنية الالكترونية
	١-١٥	خدمات التوصيل المسجلة الكترونيًا	١-١٦	صلاحيات الشهادة الرقمية
٢. إدارة دورة المفاتيح	٢-١	توليد المفاتيح	٢-٢	فترة صلاحية المفتاح
	٢-٣	نقل المفتاح	٢-٤	تخزين المفتاح
٣. الامن المادي	٣-١	متطلبات الأمن المادي	٣-٢	النسخ الاحتياطي خارج الموقع
	٣-٣	جوانب صمود الأمن السيبراني		

هيكلة ترميز الوثيقة

شكل (٢) يستعرض مخطط ترميز وثيقة المعايير ويليه شكل (٣) يبين مخطط ترميز بنود المعايير في الوثيقة:



شكل (٢) مخطط ترميز وثيقة المعايير



شكل (٣) مخطط ترميز بنود المعايير

المعيار الوطني للتشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية

تفاصيل المعيار الوطني للتشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية (NSCA)

١ الشهادات الرقمية

١,١ التدقيق والتسجيل

١,١,١ يجب تسجيل كل الأحداث المرتبطة بدورة حياة الشهادات الرقمية بشكل مناسب وآمن يمكّن من التتبع والتدقيق، وتشمل طلب الشهادات، وتوليدها، وتجديدها، وتعديلها، وإلغائها، وانتهاء صلاحيتها.

١,١,٢ يجب ألا تقل مدة الاحتفاظ بسجلات التدقيق عن 24 شهراً.

١,١,٣ يجب تخزين سجلات التدقيق بشكل آمن، وأخذ نسخ احتياطية كاملة وحفظ هذه النسخ في مكان احتياطي مناسب حسب ما ذكر في القسم رقم ٣,٢ من هذه الوثيقة.

١,٢ هيكلية الشهادات والحقول المطلوبة

١,٢,١ يجب أن تمتثل الشهادات الرقمية مع صيغة وامتدادات الشهادة القياسية (Standard Certificate Extensions) كما ورد في X.509 v3.

١,٢,٢ يجب أن تحتوي الشهادات الرقمية على الحقول الإلزامية والمذكورة في الملحق (ب) تحت المتطلبات التقنية في هذه الوثيقة.

١,٢,٣ يجب أن تحتوي الشهادات الرقمية على حقل امتداد استعمال المفتاح (Key Usage Extension) ويكون هذا الحقل مصنف على أنه حساس. كما يجب أن تكون الحقول (cRLSign) و(keyCertSign) أحادية (يتم تحديد البت الخاص بها لتكون قيمته ١).

١,٣ اتفاقيات التسمية

١,٣,١ يجب ترميز حقل المُصدِّر في الشهادات تماماً كما تم ترميزه في اسم المُصدَّر له في شهادة الجذر الموقِّعة، وذلك لتفادي التعقيدات المرتبطة بسلسلة الأسماء وتطبيق قيودها.

١,٣,٢ يجب ان يكون ترميز القيود المفروضة على الأسماء موحداً ضمن مسار شهادة الجذر. كما يجب ان يتم مقارنة قيود الأسماء المذكورة في شهادة الجذر مع حقل المُصدِّر في مسار الشهادة وذلك لضمان التطبيق الصحيح.

١,٤ الخوارزميات المقبولة

١,٤,١ يجب أن تكون الخوارزميات المستخدمة في توليد مفاتيح مالك الشهادة، والمستخدمة في إنشاء وتوقيع الشهادات الرقمية، ملتزمة ومتوافقة مع المعايير الوطنية للتشفير.

١,٤,٢ يجب دعم جميع خوارزميات التشفير المقبولة والمذكورة في معايير التشفير الوطنية الخاصة بتوليد ونشر الشهادات الرقمية، وذلك لتمكين المستفيدين من التحقق من الشهادات والتواصل مع ملاكها باستخدام أياً من الخوارزميات المقبولة.

١,٥ التحقق وتوثيق هوية ملّاك الشهادة

١,٥,١ يجب أن يتم التحقق من هوية مقدم الطلب على الشهادة قبل إصدار الشهادة حسب التالي:

١,٥,١,١ في حال أن مقدم الطلب شخص، يجب أن يتم التحقق على الأقل باستخدام وثائق هوية مقدم الطلب الرسمية.

١,٥,١,٢ في حال أن مقدم الطلب جهة، يجب أن يتم التحقق على الأقل باستخدام الوثائق القانونية الخاصة بالجهة بالإضافة الى بيانات المصادقة (الهوية) للشخص المقدم للطلب.

١,٥,٢ يجب أن يتم التحقق من أن مقدم الطلب يحمل المفتاح الخاص المتوافق مع المفتاح العام، خلال عملية طلب الشهادة.

١,٦ توليد وإصدار الشهادة

١,٦,١ يجب أن يتم التحقق من صلاحيات مالك الشهادة المرشح لامتلاك الشهادة وسلامة البيانات الواردة في طلب إصدار الشهادة. كما يجب التحقق من جميع البيانات التي تم استلامها من مالك الشهادة المحتمل قبل تضمينها في الشهادة.

١,٦,٢ يجب إنشاء وتوقيع شهادة حال استيفاء جميع متطلبات الشهادة.

١,٦,٣ يجب إبلاغ مالك الشهادة فور توليدها، وإتاحتها لمالك الشهادة. ويجب الاحتفاظ بسجل يحتوي على إقرار مالك الشهادة باستلامها. فيما يخص الشهادات المخصصة للأجهزة، يجب على مزود خدمات إصدار الشهادات الرقمية أن يبلغ الفرد المسؤول عن الجهاز وكذلك الجهة المالكة للجهاز.

١,٧ صلاحية الشهادة

١,٧,١ يجب ان تكون مدة صلاحيات الشهادات الرقمية متوافقة وممتثلة مع فترات الصلاحية المحددة في المعايير الوطنية للتشفير.

١,٧,٢ يجب أن يتم الاحتفاظ بأرشيف يحتوي على جميع الشهادات الرقمية التي تم إصدارها آخر خمس سنوات، شاملاً الشهادات منتهية الصلاحية والملغاة، وذلك لإتاحة التحقق من العمليات التي تمت خلال فترة صلاحية الشهادة.

١,٨ إيصال شهادة الجذر

١,٨,١ يجب أن تنقل شهادة الجذر الموقعة ذاتياً إلى الأطراف الناقلة بشكل آمن وذلك لمنع هجمات الاستبدال (Substitution Attacks). وتشمل طرق النقل المقبولة التالي:

١,٨,١,١ النقل الآمن للشهادة باستخدام آلية آمنة (Out-of-Band) لنقل البيانات. على سبيل المثال، تضمين قائمة شهادات الجذر ضمن قائمة الشهادات الموثوقة في أنظمة التشغيل أو متصفح الويب.

١,٨,١,٢ تحميل الشهادة من موقع إنترنت بشكل مشفر وموثق حسب ما ذكر بمعايير التشفير الوطنية وذلك باستخدام شهادة سارية الصلاحية. في هذه الحالة، يجب أن يتم التحقق من قيمة الاختزال (Hash Value) الخاصة بشهادة الجذر من خلال مقارنتها بقيمة الاختزال التي تم إتاحتها عبر قناة آمنة وموثوقة خارج النطاق (Out-of-Band).

١,٩ تجديد الشهادات وتعديلها، وإعادة إصدارها باستخدام مفاتيح جديدة

١,٩,١ يمكن تجديد الشهادة فقط إذا كانت مفاتيح مالك الشهادة لا تزال سارية الصلاحية ومتوافقة مع فترة الصلاحية المحددة في المعايير الوطنية للتشفير.

١,٩,٢ يجب ألا تتجاوز فترة صلاحية الشهادة المجددة فترة صلاحية مفاتيح مالك الشهادة.

١,٩,٣ يجب إعادة إصدار الشهادة باستخدام مفاتيح جديدة في الحالات التالية:

١,٩,٣,١ بلوغ الحد الأقصى لفترة استخدام المفاتيح.

١,٩,٣,٢ انكشاف أو فقدان المفتاح الخاص بمالك الشهادة.

١,٩,٤ يجب ألا يتجاوز تاريخ انتهاء الصلاحية المحدث للشهادة المعدلة تاريخ انتهاء صلاحية مفاتيح مالك الشهادة.

١,٩,٥ يجب التحقق من استخدام مفاتيح تم توليدها حديثاً في حال تم إعادة إصدار الشهادة باستخدام مفاتيح جديدة أو تم التعديل على الشهادة بشكل يشمل تغيير مفتاح مالك الشهادة العام.

١,١٠ إلغاء الشهادة

١,١٠,١ يجب إلغاء الشهادة في كل من الحالات التالية:

١,١٠,١,١ التعديل على الشهادة أو إعادة إصدار الشهادة باستخدام مفاتيح جديدة.

١,١٠,١,٢ فقد الارتباط بين الشهادة وهيئة الشهادات المُصدرة لها.

١,١٠,١,٣ مخالفة الضوابط والشروط التي وُضعت من قبل هيئة الشهادات.

١,١٠,٢ يجب أن يتم إلغاء الشهادة من قبل هيئة الشهادات المُصدّرة لها، أو من طرف ثالث مخول من قبل ذات هيئة الشهادات فقط.

١,١٠,٣ يجب أن يتم إلغاء الشهادة باستخدام أحد الطرق الثلاثة التالية: قائمة إلغاء الشهادات (CRL)، بروتوكول حالة الشهادة عبر الإنترنت (OCSP)، أو طريقة مزدوجة تجمع بين (CRL) و(OCSP).

١,١٠,٤ في حال إلغاء الشهادة باستخدام قائمة إلغاء الشهادات (CRL)، يجب:

١,١٠,٤,١ أن يكون مُصَدّر قائمة إلغاء الشهادات هو هيئة الشهادات المصدرة لها أو طرف آخر مخول من قبل ذات الهيئة لإصدار قائمة الغاء الشهادات.

١,١٠,٤,٢ أن يكون مفتاح توقيع قائمة إلغاء الشهادات مختلفاً عن المفتاح المستخدم من قبل هيئة الشهادات المصدرة لتوقيع الشهادات.

١,١٠,٤,٣ تأمين الاتصال بين الخادم الخاص بقائمة إلغاء الشهادات والطرف الطالب للشهادة من حيث السرية والموثوقية حسب ما ورد في المعايير الوطنية للتشفير.

١,١٠,٤,٤ أن يقوم مُصَدّر قائمة إلغاء الشهادات بتوليد قائمة دورية موقعة تحتوي على الأرقام التسلسلية للشهادات الملغاة. ويجب نشر هذه القائمة لتكون متاحة لجميع المستخدمين والأجهزة.

١,١٠,٤,٥ أن تحتوي قائمة إلغاء الشهادات على طابع زمني (Timestamp) يشير إلى وقت التحديث الأخير، المذكور في القسم ١،١٤ من هذه الوثيقة.

١,١٠,٤,٦ إصدار قائمة إلغاء شهادات (CRL) جديدة بشكل دوري. على ان لا تتجاوز الفترة شهرا واحدا للشهادات الثانوية (CAs) و١٢ شهرا للشهادة الجذرية (CA)

١,١٠,٤,٧ تحديث قائمة إلغاء الشهادات خلال ١٢ ساعة كحد أقصى بعد كل عملية إلغاء شهادة.

١,١٠,٤,٨ إزالة الشهادات الملغاة من قائمة إلغاء الشهادات عند انتهاء فترة صلاحيتها.

١,١٠,٤,٩ إتاحة قائمة إلغاء الشهادات عبر الإنترنت للأجهزة الطرفية التي تستخدم الشهادات الرقمية.

١,١٠,٥ في حال إلغاء الشهادة باستخدام بروتوكول حال الشهادة عبر الإنترنت (OCSP)، يجب:

١,١٠,٥,١ تأمين الاتصال بين الخادم الخاص ببروتوكول حال الشهادة عبر الإنترنت والطرف الطالب من حيث السرية والموثوقية حسب ما ورد في المعايير الوطنية للتشفير.

١,١٠,٥,٢ تضمين الشهادات الملغاة في قواعد بيانات بروتوكول حال الشهادة عبر الإنترنت خلال ١٢ ساعة كحد أقصى.

١,١٠,٥,٣ أن يكون مُصدِّر بروتوكول حال الشهادة عبر الإنترنت هو هيئة الشهادات المصدرة لها أو طرف آخر مخول من قبل ذات الهيئة لإصدار بروتوكول حال الشهادة عبر الإنترنت.

١,١٠,٥,٤ إزالة الشهادة الملغاة من قواعد بيانات بروتوكول حال الشهادة عبر الإنترنت عند انتهاء فترة صلاحيتها.

١,١١ مصادقة مواقع الإنترنت

١,١١,١ يجب أن تكون الشهادات الرقمية المستخدمة في مصادقة مواقع الإنترنت ملتزمة بالمتطلبات الواردة في هذه الوثيقة.

١,١١,٢ يجب أن يتحقق مُصدّر الشهادة الرقمية من ملكية الطرف الطالب للشهادة لنطاق الويب (Web Domain) قبل إصدارها.

١,١١,٣ يجب أن تحتوي الشهادة الرقمية على اسم النطاق واسم مالك الشهادة. يمكن للشهادة ان تحتوي على اسم نطاق واحد أو أكثر.

١,١١,٤ يجب تمكين زوار موقع الإنترنت من فحص الشهادة والتحقق من موثوقيتها.

١,١٢ التواقيع الالكترونية

١,١٢,١ يجب ان تستخدم التواقيع الالكترونية شهادات رقمية ملتزمة بالمتطلبات الواردة في هذه الوثيقة.

١,١٢,٢ يجب أن تكون الشهادات الرقمية المستخدمة في التواقيع الالكترونية بمستوى أمان مماثل أو أعلى من مستوى أمان أساسيات التشفير (Cryptographic Primitives) المستخدمة في توليد التواقيع الالكترونية. على سبيل المثال، دوال الاختزال والخوارزميات غير المتماثلة.

١,١٢,٣ يجب أن يحتوي العنصر الرقمي المراد توقيعه على طابع زمني كما ورد تفصيله في القسم ١،١٤ ن هذه الوثيقة وذلك لتحديد تواريخ وأوقات كل من التوليد والتوقيع.

١,١٢,٤ يجب أن تكون الشهادة الرقمية مخصصة للمُوَقِّع بشكل فريد.

١,١٢,٥ يجب أن يحتوي التوقيع الالكتروني على معرِّفات خاصة وفريدة تخص المُوَقِّع والشهادة الرقمية المستخدمة.

١,١٣ الأختام الالكترونية

١,١٣,١ يجب أن يكون الختم الالكتروني ملتزما بمتطلبات التوقيع الالكتروني في هذه الوثيقة.

١,١٣,٢ يجب أن يحتوي كل عنصر رقمي مختوم الكترونياً على توقيعين: (١) التوقيع الالكتروني الخاص بالمنظمة و(٢) التوقيع الالكتروني الخاص بالموظف. وذلك لتمكين التعرف على الطرف الذي قام بختم الوثيقة.

١,١٣,٣ يجب أرشفة الوثائق المختومة الكترونياً بالإضافة الى الشهادات الرقمية المستخدمة وذلك لإتاحة التحقق منها مستقبلاً.

١,١٤ الطوابع الزمنية الالكترونية

١,١٤,١ يجب أن تربط الطوابع الزمنية الالكترونية التاريخ والوقت بعنصر رقمي بطريقة تمنع إمكانية تغيير العنصر الرقمي بشكل غير قابل للكشف.

١,١٤,٢ يجب أن تُضَمَّن الطوابع الزمنية في الشهادات وقائمة إلغاء الشهادات (CRL) وسجلات النظام بالإضافة لأي قواعد بيانات خاصة بالإلغاء.

١,١٤,٣ يجب أن يؤخذ التاريخ والوقت المستخدم في الطوابع الزمنية من مزودين معتمدين من الهيئة السعودية للمواصفات والمقاييس والجودة (SASO) ومتزامنين مع ساعة دقيقة مثل ساعة نظام التموضع العالمي (GPS). بالإضافة الى المحافظة على وقت متزامن، يجب أن يكون هناك إجراءات للتحقق وتعديل الاختلافات الزمنية.

١,١٤,٤ يجب أن تكون الطوابع الزمنية الالكترونية موقعة بتوقيع الكتروني أو مختومة بختم الكتروني مبنية على شهادة رقمية قابلة للتحقق.

١,١٤,٥ يجب أن تكون أساسيات وتصاميم التشفير المستخدمة في توليد الطوابع الزمنية الالكترونية ملتزمة بمستوى الأمان المناسب والمتوافق مع المعايير الوطنية للتشفير .

١,١٥ خدمات التوصيل المسجلة الكترونياً

١,١٥,١ يجب أن تكون خدمات التوصيل المسجلة الكترونياً مقدمة من قبل واحد أو أكثر من مزوّدي الخدمة الموثوق بهم والمؤهلين.

١,١٥,٢ يجب أن تحتوي خدمات التوصيل المسجلة الكترونياً على هوية المرسل وتكون ضامنة لها.

١,١٥,٣ يجب على خدمات التوصيل المسجلة الكترونياً أن تتحقق من هوية المستقبل قبل توصيل العنصر الرقمي.

١,١٥,٤ يجب أن تكون عمليات نقل واستقبال العناصر الرقمية محمية بتوقيع الكتروني أو ختم الكتروني من قبل مزودي خدمات الثقة المؤهلين وذلك لضمان قابلية كشف ومنع أي تعديل على العنصر الرقمي.

١,١٥,٥ يجب تنبيه المرسل والمستقبل معاً بأي تعديل مطلوب على العنصر الرقمي لأغراض الارسال أو الاستقبال.

١,١٥,٦ يجب استخدام طابع زمني إلكتروني (Timestamp) للدلالة على تواريخ وأوقات الإرسال والاستقبال وتعديل البيانات.

١,١٥,٧ يجب الالتزام بالمتطلبات الواردة في هذه الوثيقة عند نقل العنصر الرقمي بين اثنين وأكثر من مزودي خدمات الثقة.

١,١٦ صلاحيات الشهادة الرقمية

١,١٦,١ يجب على جميع مصدري الشهادات الامتناع عن إصدار أي شهادة لنطاق معيّن إلا في حال عدم وجود أي سجلات صلاحيات هيئة الشهادات (CAA) للنطاق، أو توافق طلب الشهادة مع السجلات المعتمدة لذلك النطاق.

٢ إدارة دورة المفتاح

٢,١ توليد المفتاح

٢,١,١ يجب توليد مفاتيح هيئات الشهادات بمنشأة آمنة حسب متطلبات القسم ٣ في هذه الوثيقة، وبحضور شخصين مخوَّلين.

٢,١,٢ يجب استخدام وحدة أمن الأجهزة (HSM) ممتثلة بمتطلبات المستوى ٣ على الأقل من وثيقة (FIPS 140-3) وكذلك المستوى ٤ (EAL 4) على الأقل من وثيقة (Common Criteria) لتوليد مفاتيح هيئة الشهادات.

٢,١,٣ يجب استخدام مولدات آمنة للأعداد العشوائية (RNGs) لتوليد مفاتيح التوقيع لهيئات الشهادات. على سبيل المثال، مولدات الأعداد تامة العشوائية (TRNG) أو المولدات الكمية للأعداد العشوائية (QRNG) كما هو مذكور في المعايير الوطنية للتشفير.

٢,١,٤ يجب أن تضمن هيئة الشهادات تدمير مفاتيح التوقيع الخاصة بها في حال انتهاء صلاحيتها أو في حال تعطل خدمات هيئة الشهادات لأي سبب كان.

٢,١,٥ يجب تفعيل دوال التصفير واستخدامها في جميع وحدات أمن الأجهزة (HSM) المستخدمة في توليد وتخزين مفاتيح التوقيع لمزودي خدمات إصدار الشهادات الرقمية.

٢,١,٦ يجب أن يتم توليد مفاتيح المستخدم من قِبل المستخدم نفسه أو من قِبل هيئة الشهادات الثانوية المصدرة لشهادة المستخدم.

٢,١,٧ يجب أن تكون عملية توليد المفاتيح ملتزمة بمعايير توليد المفاتيح ذات العلاقة والمذكورة في المعايير الوطنية للتشفير

٢,٢ فترة صلاحية المفتاح

٢,٢,١ يجب أن تكون فترة صلاحية المفاتيح ملتزمة بمعايير حماية المفاتيح وصلاحيتها المذكورة في المعايير الوطنية للتشفير.

٢,٣ نقل المفتاح

٢,٣,١ في حال تم توليد المفاتيح العامة والخاصة من قبل هيئة الشهادات الجذرية أو هيئة الشهادات الثانوية بالنيابة عن مالك الشهادة، فيجب نقلها إلى مالك الشهادة بطريقة آمنة بحسب ماورد بمعايير توزيع المفاتيح وتثبيتها في المعايير الوطنية للتشفير.

٢,٣,٢ في حال تسليم المفاتيح الخاصة الكترونياً، يجب تشفير مادة المفاتيح (Key Material) باستخدام خوارزمية تشفير وحجم مفتاح لا يقل مستوى أمانه عن مستوى أمان المفتاح الخاص.

٢,٣,٣ في حال تسليم المفاتيح الخاصة بواسطة جهاز مادي، يجب الحفاظ على مسؤولية موقع الجهاز المادي وحالته من قبل الجهة المسلمة للمفاتيح حتى يقبل مالك الشهادة المحتمل استلامها.

٢,٣,٤ يجب حماية المفاتيح الخاصة أثناء عملية التوصيل ضد التفعيل أو الاختراق أو التعديل.

٢,٣,٥ يجب إتاحة مفاتيح التفعيل لمالك الشهادة باستخدام قناة آمنة ومختلفة عن تلك التي استخدمت لتوصيل المفاتيح الخاصة، على سبيل المثال، التوصيل بواسطة قناة خارج النطاق (out-of-Band).

٢,٣,٦ يجب على مالك الشهادة المحتمل أن يؤكد استلامه للمفاتيح الخاصة.

٢,٣,٧ يجب توصل المفاتيح العامة وهوية مالك الشهادة المحتمل الى هيئة الشهادات بطريقة موثوقة وآمنة وذلك لإصدار الشهادة. كذلك يجب ان تربط قناة التسليم هوية مالك الشهادة المحتمل المتحقق منها بالمفتاح العام. في حال استعمال التشفير لتحقيق هذا الربط، فانه يجب ألا يقل مستوى أمان التشفير المستخدم عن مستوى أمان مفاتيح مالك الشهادة المحتمل.

٢,٣,٨ يجب ان تضمن طريقة التسليم أن أداة التوثيق وبيانات التفعيل (Tokens) الصحيحة سلمت الى مالك الشهادة المحتمل الصحيح.

٢,٣,٩ يجب على هيئة الشهادات الاحتفاظ بسجل يثبت إقرار مالك الشهادة المحتمل باستلامه لأداة التوثيق.

٢,٤ تخزين المفتاح

٢,٤,١ يجب تخزين مفاتيح توقيع هيئة الشهادات بطريقة آمنة في وحدة تشفير، مثل وحدة أمن الأجهزة (HSM)، أداة التوثيق (Token)، بطاقة ذكية (Smart Card)، أو وحدة المنصة الموثوقة (TPM)، وعلى ان تكون وحدة التشفير ممتثلة بمتطلبات المستوى ٣ على الأقل من وثيقة (FIPS 140-3) وكذلك المستوى ٤ (EAL 4) على الأقل من وثيقة (Common Criteria).

٢,٤,٢ يجب أن تكون وحدات التشفير المستخدمة لتخزين مفاتيح التوقيع الخاصة بهيئة الشهادات ملتزمة بالمعايير ذات العلاقة المذكورة في المعايير الوطنية للتشفير.

٢,٤,٣ يجب على هيئة الشهادات الجذرية الحفاظ على شبكة معزولة تماماً عن الشبكات الأخرى واستخدامها عند تخزين مفتاح التوقيع الخاص بها، بالإضافة لأي بيانات حساسة أخرى، مثل النسخ الاحتياطية لمفاتيح التوقيع.

٢,٤,٤ يجب أن تحافظ هيئات الشهادات على أرشيف لا يقل عن ٥ سنوات يحتوي على مفاتيح التحقق الخاصة بها، سواءً الحالية أو السابقة.

٢,٤,٥ يجب عدم أرشفة مفاتيح التوقيع الخاصة بهيئة الشهادات.

٢,٤,٦ يجب حصر صلاحيات الوصول الى أرشيف هيئة الشهادات على الأشخاص المخوَّلين فقط.

٢,٤,٧ يجب حماية جميع أجهزة تخزين التشفير بواسطة نظام مصادقة ثنائي كحد أدنى.

٢,٤,٨ يجب عدم تسليم مفاتيح التوقيع الخاصة بهيئة الشهادات لطرف ثالث نهائياً، وعدم حفظها بطريقة غير مشفرة.

٣ الأمن المادي

٣,١ متطلبات الأمن المادي

٣,١,١ يجب على هيئة الشهادات تطبيق ضوابط الوصول المادي والمنطقي وذلك لحماية الأصول ضد السرقة، والضياع، والوصول غير المصرح به.

٣,١,٢ يجب حماية جميع الأجهزة والمعدات ذات العلاقة بتوليد وتخزين المفاتيح أو الشهادات ضد الوصول المادي أو المنطقي غير المصرح به وذلك باستخدام ضوابط مادية تشمل:

٣,١,٢,١ أنظمة تحكم في الوصول متعددة، باستخدام أبواب مزودة بأقفال إلزامية.

٣,١,٢,٢ مصادقة متعددة العناصر لأنظمة التحكم في الوصول.

٣,١,٢,٣ مراقبة مستمرة بواسطة كاميرات المراقبة على مدار الساعة وطوال أيام الأسبوع.

٣,١,٣ يجب تطبيق أنظمة يدوية والكترونية لمراقبة الوصول غير المصرح به أو التسلل بجميع الأوقات.

٣,١,٤ يجب جمع سجلات الدخول التفصيلية وتخزينها بشكل آمن وفحصها بشكل دوري.

٣,١,٥ يجب تخزين سجلات الدخول لمدة لا تقل عن ١٨ شهراً.

٣,١,٦ يجب أن تتطلب عمليات توليد المفاتيح وعمليات توقيع الشهادات وجود وموافقة شخصين مخوَّلين على الأقل.

٣,١,٧ يجب استضافة جميع البنى التحتية الخاصة بهيئة الشهادات، وتشمل جميع المواقع الرئيسية والاحتياطية، محلياً داخل المملكة العربية السعودية.

٣,١,٨ يجب تنقية وتدمير جميع معدات وأجهزة التخزين الخاصة بهيئة الشهادات قبل التخلص منها بناءً على الوثائق التنظيمية ذات الصلة للهيئة الوطنية للأمن السيبراني.

٣,٢ النسخ الاحتياطي خارج الموقع

٣,٢,١ يجب الاحتفاظ بنسخ احتياطية دورية كافية للاستعادة في حال فشل الأنظمة كما ورد في الوثائق التنظيمية ذات العلاقة والمنشورة من قبل الهيئة الوطنية للأمن السيبراني.

٣,٢,٢ يجب إجراء نسخ احتياطي مرة واحدة أسبوعياً على الأقل.

٣,٢,٣ يجب الاحتفاظ بما لا يقل عن نسخة احتياطية كاملة واحدة خارج الموقع ومفصولة عن المعدات الرئيسية لهيئة الشهادات، على أن يتم تحديثها شهرياً.

٣,٢,٤ يجب حفظ النسخ الاحتياطية في موقع يطبق ضوابط مادية وإجرائية متكافئة مع الموقع الرئيسي لعمليات هيئة الشهادات.

٣,٢,٥ يجب حفظ النسخ الاحتياطية لمفاتيح التوقيع في وحدة تشفير ملتزمة بالضوابط المذكورة في ٢،٤،١.

٣,٢,٦ يجب إيصال جميع البيانات المنقولة الى مواقع النسخ الاحتياطية بطريقة موثوقة ومشفرة.

٣,٣ جوانب صمود الأمن السيبراني

٣,٣,١ يجب تحديد وتطبيق إجراء يضمن الحفاظ على استمرار إدارة وتشغيل عمليات الشهادات الرقمية في حال فشل الأنظمة، مثل خدمات التحقق من الشهادات وإلغاء الشهادات، بحيث يضمن الإجراء عدم تأثر وصول العميل.

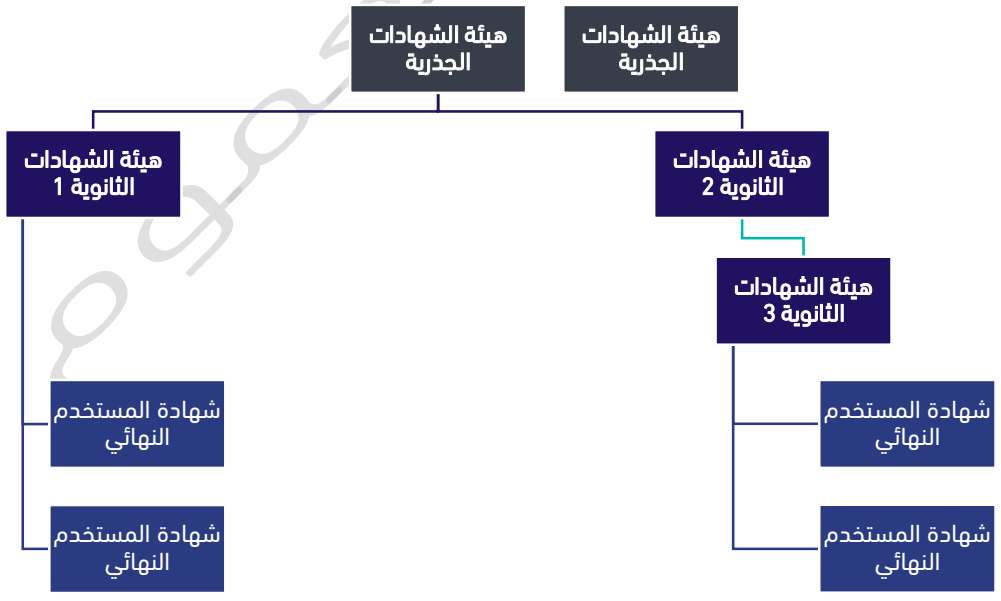
الملحقات

الملحق (أ): التسلسل الهرمي وتصنيف هيئات الشهادات

تُصنَّف هيئات الشهادات إلى هيئات الشهادات الجذرية وهيئات الشهادات الثانوية. يوضح الشكل (٤) التسلسل الهرمي وتصنيف هيئات الشهادات.

تشكل هيئة الشهادات الجذرية عمود الثقة في التسلسل الهرمي لهيئة الشهادات. تكون الشهادة الرقمية لهيئة الشهادات الجذرية موقعة ذاتياً ومدمجة مع أنظمة التشغيل، والبرمجيات مثل متصفح الانترنت. في حال توفر العديد من هيئات الشهادات الجذرية، تكون الشهادة الجذرية الخاصة بهيئة الشهادات قابلة للتوقيع المتبادل من قبل هيئات الشهادات الجذرية الأخرى باشتراط دراسة مخاطر الأمن السيبراني ذات العلاقة، وتطبيق إجراءات الحد من المخاطر بشكل صحيح. وعادةً لا يتم إصدار الشهادات من قبل هيئة الشهادات الجذرية إلا لهيئات الشهادات الثانوية فقط.

بالمقابل، تصدر هيئة الشهادات الثانوية الشهادات للمستخدم النهائي أو لهيئات الشهادات الثانوية الأخرى. عندما تصدر هيئة الشهادات الثانوية شهادة الى هيئة شهادات ثانوية أخرى، فانه من المتعارف عليه ان تسمى "هيئة شهادات متوسطة" حيث أنها تشغل مكانةً متوسطة في تسلسل الثقة بين هيئة الشهادات الجذرية وهيئة الشهادات الثانوية. على سبيل المثال، في الشكل رقم (٤) أدناه يمكن تسمية (هيئة الشهادات الثانوية ٢) بهيئة الشهادات المتوسطة.



شكل (٤) التسلسل الهرمي وتصنيف هيئات الشهادات

الملحق (ب): المتطلبات التقنية

حقول إلزامية للمعيار رقم 1.2.2

الجدول أدناه يحدد الحقول المطلوبة للمعيار رقم ١،٢،٢ في هيكلة الشهادة X.509 v3.

جدول (٢) الحقول المطلوبة للشهادات الرقمية X.509 V3.

الحقل	مطلوب؟
رقم النسخة (Version Number)	✓
الرقم التسلسلي (Serial Number)	✓
رقم تعريف خوارزمية التوقيع (Signature Algorithm ID)	✓
اسم المُصدِّر (Issuer Name)	✓
فترة الصلاحية: بصياغة تحتوي على (بدءاً من) و(بحد اقصى) (Validity period including Not Before and Not After)	✓
اسم المُصدَّر له (Subject name)	✓
معلومات المفتاح العام للمُصدَّر له (Subject Public Key Info: including public key algorithm and subject (public key.	✓
الرقم التعريفي الفريد للمُصدِّر (Issuer Unique Identifier)	✓
الرقم التعريفي الفريد للمُصدَّر له (Subject Unique (Identifier	✓
امتدادات (Extensions)	
خوارزمية توقيع الشهادة (Certificate Signature (Algorithm	✓
توقيع الشهادة (Certificate Signature)	✓

الملحق (ج): مصطلحات وتعريفات

جدول (٣) مصطلحات وتعريفات

المصطلح	التعريف
Certificate Authority (CA) **هيئة الشهادات**	كيان موثوق، مسؤول عن إصدار شهادات المفاتيح العامة وإلغائها.
Certificate Renewal **تجديد الشهادة**	عملية استحداث شهادة جديدة باستخدام رقم تسلسلي جديد وتاريخ صلاحية جديد مع الاحتفاظ على جميع الحقول الأخرى والمفتاح العام الخاص بالمالك على وجه الخصوص بالشهادة كما هي.
Certificate Re-keying **إعادة تصدير الشهادة باستخدام مفاتيح جديدة**	عملية توليد شهادة جديدة برقم تسلسلي جديد ومفتاح عام جديد لمالك الشهادة.
Certificate Modification **تعديل الشهادة**	عملية استحداث شهادة جديدة برقم تسلسلي جديد مع تعديل حقل أو حقول أخرى. قد يضمن هذا التعديل المفتاح العام الخاص بالمالك.
Electronic timestamping **الطبع الزمني الالكتروني**	عملية تربط بين الوقت والتاريخ مع عنصر رقمي بطريقة الكترونية وذلك لإتاحة دليل على وجود العنصر الرقمي أو تنفيذه في ذلك الوقت والتاريخ المحدد.
Electronic seal **ختم الكتروني**	ختم الكتروني مرتبط بكيان قانوني كشركة أو منظمة على سبيل المثال. يمكن استخدام الختم الالكتروني بواسطة شخص أو اشخاص متعددين داخل هذا الكيان القانوني.
Electronic signature **توقيع الكتروني**	نظير رقمي للتوقيع الخطي التقليدي. يستخدم التوقيع الرقمي لتأكيد ادعاء التوقيع على انه المصدر الصحيح لتوقيع العنصر الرقمي.
Digital signature **توقيع رقمي**	التوقيع الرقمي يستخدم لكشف ما إذا كان العنصر الرقمي قد تم تغييره بعد التوقيع ام لا.
PKI **بنية المفاتيح العامة التحتية**	قائمة من الشروط والقوانين والعتاد والبرمجيات والمهام التي تحوكم اصدار الشهادات الرقمية لحماية البيانات الحساسة بحيث توفر هويات رقمية حصرية للمستخدمين.
ERDS **خدمات التوصيل المسجلة الكترونيا**	خدمات الكترونية امنة تمثل دليل قانوني عبر الإنترنت لإرسال واستقبال البيانات بين الأطراف
OSCP **بروتوكول حالة الشهادة عبر الانترنت**	بروتوكول انترنت يسمح للمستخدمين التحقق من صلاحية الشهادات الرقمية وحالة سريانها

المصطلح	التعريف
CRL **قائمة الشهادات الملغية**	خدمة تقدمها هيئة الشهادات للتحقق من قائمة موقعة رقميا للشهادات الرقمية الملغاة
Digital Object **العنصر الرقمي**	هيكلة للبيانات تحمل معلومات أمنية تتعلق بالشهادات الرقمية بتنسيق موحد وقابل للتحقق

الملحق (د): اختصارات

جدول (٤) اختصارات

المختصر	التعريف
NCA	National Cybersecurity Authority الهيئة الوطنية للأمن السيبراني
NSCA	National Standard of Cryptography for Saudi Root and Digital Certificate Authorities المعيار الوطني للتشفير للجذر السعودي ومزودي خدمات إصدار الشهادات الرقمية
NCS	National Cryptographic Standards المعايير الوطنية للتشفير
CA	Certificate Authority هيئة الشهادات
CAA	Certificate Authority Authorization صلاحيات هيئة الشهادات
PKI	Public Key Infrastructure بنية المفاتيح العامة التحتية
CRL	Certificates Revocation List قائمة إلغاء الشهادات
OCSP	Online Certificate Status Protocol بروتوكول حال الشهادة عبر الإنترنت
ERDS	Electronic Registered Delivery Services خدمات التوصيل المسجلة الكترونياً
HSM	Hardware Security Module وحدة أمن الأجهزة
TPM	Trusted Platform Module وحدة المنصة الموثوقة
RNG	Random Number Generator مولد أعداد عشوائية
QRNG	Quantum Random Number Generator مولد كمي للأعداد العشوائية
SASO	Saudi Standards, Metrology and Quality Organization الهيئة السعودية للمواصفات والمقاييس والجودة
DGA	Digital Government Authority هيئة الحكومة الرقمية


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority