الجمهورية العربيّة السوريّة
وزارة الاتّصالات والتّقانة
الهيئة الوطنيّة لخدمات الشّبكة

الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

سياسة الشّهادة الرّقميّة

Certificate Policy

النّسخة الأولى

هاتف: ٣٩٣٧٠٧٨ ١١ ٩٦٣+، فاكس ٣٩٣٧٠٧٩ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني info@nans.gov.sy

الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

سجلّات التّغيير

التّاريخ	إصدار	الحالة	النّسخة
	فريق عمل الهيئة الوطنيّة لخدمات الشّبكة	مسودة	1.0
	مجلس الهيئة الوطنيّة لخدمات الشّبكة رقم:.....		
	قرار تنظيمي رقم:.....		

المراجعات

التّاريخ	الاسم	الصّفة

جدول المحتويات

١. مقدّمة

١,١. التّعريف بمفهوم التّوقيع الرّقمي وشهادات المصادقة الرّقميّة

إنَّ التّوقيع الرّقمي هو عبارة عن جملة بيانات تدرَج على وثيقةٍ إلكترونيةٍ وترتبط بها، ويتم ذلك من خلال إجراء يقوم به الشّخص الذي يريد التّوقيع على وثيقة إلكترونيّة، كالعقود والاتفاقيّات وأوامر البيع والشّراء أو المراسلات الخاصّة وغيرها من المعاملات الإلكترونيّة، بحيث يتم من خلال هذه العمليّة ربط هويّة الشّخص الّذي يقوم بالتّوقيع بالوثيقة المُوقّع عليها، بحيث يمكن لمستلم الوثيقة الموقّعة رقميّاً التّحقق من صحّة التّوقيع المدرج عليها بشكل قاطع وفوري.

كما أن التّوقيع الرّقمي يضمن توقيع الوثائق والمستندات الإلكترونيّة وتشفيرها وتبادلها بطريقةٍ آمنة بحيث لا يسمح إلا للأشخاص المُصرَّح لهم بفكِّ هذا التّشفير والاطّلاع على محتوى الرّسالة.

وأهم مجالات استخدام التّوقيع الرّقمي هي:

- التّوقيع الرّقمي
- عدم الإنكار
- سلامة ودقة المعلومات
- الخصوصيّة
- التّشفير

أمّا شهادة المصادقة الرّقميّة فهي تُمثل إثبات ارتباط توقيع رقمي إلى شخصٍ طبيعي أو اعتباري، ويتم بواسطتها الحصول على توقيع رقمي واستخدامه، وتصدر عن جهةٍ مرخص لها بمنح شهادات المصادقة الرّقميّة.

١,٢. مسرد المصطلحات:

فيما يلي مسرد لأهمّ المصطلحات المستخدمة في هذه الوثيقة:

المصطلح	الاختصار	الترجمة
Public Key Infrastructure	PKI	البنية التّحتيّة للمفتاح العام
Digital Signature	DS	التّوقيع الرّقمي
Digital Certificate	-	شهادة المصادقة الرّقميّة
Public Key	-	المفتاح العام
Private Key	-	المفتاح الخاص
Certification Authority	CA	مركز التّصديق الرّقمي
Registration Authority	RA	مركز تسجيل الشّهادات الرّقمية
Root Certification Authority	Root-CA	مركز التّصديق الرّقمي الجذري
Online Certificate Status Protocol	OCSP	بروتوكول التّحقق المباشر من الشّهادة
Simple Certificate Enrollment Protocol	SCEP	بروتوكول منح الشّهادة البسيط
Lightweight Directory Access Protocol	LDAP	برتوكول إدارة الدّخول
Certificate Revocation List	CRL	قائمة الشّهادات الملغية
certification practice statement	CPS	إجراءات التّصديق الرّقمي
Certificate Policy	CP	سياسة الشّهادة الرّقمية

١,٣. مكونات البنية التّحتيّة للمفتاح العام في الهيئة الوطنيّة لخدمات الشّبكة

- **مركز التّصديق الرّقمي:**

يمثّلُ أعلى سلطة في البنية التّحتيّة للمفتاح العام، ومصدر الثّقة الرّئيسي لكامل المنظومة، ويقوم بإدارة وإصدار وتوقيع الشّهادات الرّقمية وإلغائها أو تعليق العمل بها، كما أنه المسؤول عن سنّ السّياسات العامّة لاستخدام الشّهادات الرّقمية عبر وثيقتي سياسة الشّهادة الرّقمية، وإجراءات التّصديق الرّقمي، والإشراف على تخزين شهادات المصادقة الرّقميّة.

- **مركز تسجيل شهادات المصادقة الرّقميّة:**

وهو المركز الذي يقوم بمعالجة طلبات الرّاغبين بالحصول على شهادات المصادقة الرّقميّة ويتّصل مباشرة بمركز التّصديق الرّقمي، حيث يقوم بكافة إجراءات التّسجيل من استقبال واستلام الطّلبات، وتدقيقها، والتّحقق من هويّات المتقدّمين، واستكمال كافة البيانات المتعلّقة بطلب التّسجيل، وقبول الطّلبات، ورفعها إلى مركز التّصديق الرّقمي، وتسليم شهادة المصادقة الرّقمية للمستفيد.

- **تخزين شهادات المصادقة الرّقميّة وإدارتها:**

مركز التّصديق الرّقمي هو الجهة المسؤولة عن إصدار شهادات المصادقة الرّقمية وأرشفتها وتخزينها، ويقدم خدمة التّحقق المباشر من حالة الشّهادة وذلك عبر بروتوكول OCSP، وهو مُلزم بنشر قائمة الشّهادات المنتهية أو الملغاة على موقعه الإلكتروني بالحدِّ الأدنى، لتمكين المستخدمين من معرفة حالة شهادة المصادقة الرّقميّة.

- **المستفيدون:**

مركز التّصديق الرّقمي الحكومي يقدّم شهادات المصادقة الرّقمية للعاملين في الجهات العامّة من وزارات أو مؤسسات أو هيئات أو شركات حكومية بصفاتهم الوظيفيّة، أما مزوّدات التّصديق الرّقميّة الخاصّة الحاصلة على ترخيص من الهيئة فإنها تقدّم شهادات المصادقة الرّقمية للأفراد أو شركات القطاع الخاص.

يقوم من يرغب بالحصول على شهادة مصادقة رقميّة بتقديم طلب تسجيل لدى مركز تسجيل الشّهادات الرّقميّة، وتزويده بالمعلومات الكاملة والدّقيقة التي تثبت هويّته، بالإضافة لالتزامه بحفظ الشّهادة الرّقميّة والمفتاح الخاص بشكل آمن، مع الرّجوع لمركز التّصديق الرّقمي عند حدوث أيّة مشكلة.

١,٤. الخدمات المُقدّمة:

يقدم مركز التّصديق الرّقمي خدمات عدّة لنشر وإدارة واستخدام شهادات المصادقة الرّقميّة منها:

- منح أو تصديق شهادات المصادقة الرّقميّة للأفراد والجهات العامّة والخاصّة.
- خدمة التّوقيع الرّقمي والتّشفير.
- خدمة الختم الزّمني.
- تقديم الدّعم، والنّصح لمن يرغب بتقديم خدمات التّوقيع الرّقمي.
- الاعتراف بالشّهادات الأجنبيّة.

١,٥. الخدمات المُتاحة باستخدام التّوقيع الرّقمي :

يتيح التّوقيع الرّقمي تقديم الخدمات التّالية:

- سرّية المعلومات: والتي تمكّن المتعاملين من تبادل المعلومات فيما بينهم، بما يضمن عدم معرفة الآخرين بطبيعة تلك المعلومات.
- التّثبت من الهويّة: وتعني تمكين المتعاملين باستخدام التّوقيع الرّقمي من معرفة هويّة بعضهم البعض بشكل قاطع.
- سلامة البيانات: وتعني اكتشاف أي تغيير في شكل البيانات أو المعلومات ومحتواها، أو القيام بحذف جزء منها أو الإضافة إليها أو تعديلها بعد الإرسال.
- التّوقيع الرّقمي: ويعني قدرة المستخدم على إجراء عمليّة التّوقيع بصيغة إلكترونيّة وقدرة المستلم على التّحقق من صحة التّوقيع.
- منح الصّلاحيّة: وتعني تحديد نطاق الصّلاحية الممنوحة للشخص المفوّض بعمل ما، بحيث تختلف هذه الصّلاحيّة حسب هويّة الشّخص.
- التّوقيع على البرامج الحاسوبيّة.
- وضع الختم الزّمني للمراسلات والوثائق بهدف الإثبات القانوني لزمن إنشاء الوثيقة.
- تصديق الكتب والخطابات والمعاملات الإلكترونية لجهة معيّنة.
- التراسل الموثوق والآمن بين الأجهزة.

٢. مسؤوليّات نشر وحفظ شهادات المصادقة الرّقمية :

كما ذُكر سابقاً، فإن مركز التّصديق الرّقمي هو المسؤول عن نشر الوثائق المتعلّقة بسياسات استخدام الشّهادات الرّقميّة عبر موقعه الرسمي، وهو مسؤول عن نشر شهادات المصادقة الرّقمية وقوائم الشّهادات الملغيّة وحفظها وإدارتها عبر بروتوكولات (OCSP – LDAP)، يمكن تلخيص واجبات مركز التّصديق الرّقمي المتعلّقة بنشر الشّهادات بما يلي:

- تقديم خدمة معرفة حالة الشّهادة بشكلٍ مباشر.
- إصدار وتحديث قوائم الشهادات الملغيّة.
- تضمين مسار / العنوان الإلكتروني الخاص بتحميل قائمة الشّهادات الملغيّة في أي شهادة رقميّة.
- نشر شهادة المصادقة الرّقمية الخاصّة بمركز التّصديق الرّقمي.
- تأمين الوصول السّهل والمباشر للموقع الإلكتروني الخاص بحالة الشّهادات وقوائم الشّهادات المُلغاة، لذلك يجب نشر الشّهادات فور إصدارها أو إلغائها أو تعليقها.

غالباً تحتاج عملية تدقيق طلب تسجيل الشّهادات واستكمال البيانات النّاقصة من قبل مركز التّسجيل، ثم رفعها وتصديقها من قبل مركز التّصديق الرّقمي، ثم إعادتها لمركز تسجيل الشّهادات، وتسليمها للمستفيد خلال مدةٍ أقصاها /٩/ أيام.

أما بالنسبة لقوائم الشّهادات الملغيّة، فيجب نشرها من قبل مركز التّصديق الرّقمي بعد ساعتين على الأكثر من توليدها وتصديقها، كما يتم تجديد القائمة بشكل دوري يوميّاً.

وتتم عمليّة إدارة الشّهادات والقوائم وحفظها عبر مخدّمات مركز التّصديق الرّقمي بغرفة محكمة للحماية، وتتم الإدارة والإشراف عليها من قبل مركز التّصديق الرّقمي .

٣. مسؤوليّات التّوثيق وتحديد الهويّة:

٣,١. طرق وآليات التّسمية عند توليد الشّهادة الرّقميّة:

يعتمد مركز التّصديق الرّقمي على المعيار X.509 من أجل تحديد هويّة المستفيد/التّسمية، وتحديد البيانات الخاصّة به، وذلك بالحصول على الاسم الكامل، اسم الهيئة أو المنظمة، البلد، المدينة، الشّارع، وغيرها ... وفق ما هو وارد في استمارة طلب تسجيل شهادة رقميّة، وبالتّالي يجب أن يكون للتسمية معنى واضح وغير متكرر بما يميّز هويّة الشّخص الحامل للشهادة الرّقمية دون سواه.

٣,٢. إثبات هويّة حامل الشّهادة:

عند تسجيل المستفيد لدى مركز التّسجيل، يتم الحصول على مستندات وأوراق ثبوتية للتحقق من هويّة المستفيد، ويتطلب ذلك الحضور والتّواجد الفعلي أثناء تقديم الطّلب أو من ينوب عنه بتفويض أو توكيل رسمي.

٣,٣. تجديد شهادات المصادقة الرّقميّة أو إلغائها:

يتم تجديد الشّهادة وفق إحدى الحالتين التّاليتين:

- الحالة الأولى هي تجديد الشّهادة: وهنا يكتفي المستفيد بتقديم طلب لتجديد الشّهادة مع الحضور الشّخصي، فيقوم مركز التّسجيل بتصديق شهادة المصادقة الرّقمية السّابقة مع الاحتفاظ بنفس زوج المفاتيح، أو توليد جديد للمفاتيح.
- الحالة الثّانية هي توليد شهادة جديدة: ويكون ذلك بسبب تغيير في البيانات الشّخصية أو أي من الأوراق الثّبوتية، أو لأيّ سبب آخر، ويتطلّب ذلك الحضور الشّخصي وتقديم كافة الوثائق الرّسميّة وتتم بإجراءات مماثلة لإجراءات الحصول على شهادة رقميّة أول مرة.

بالنسبة لإلغاء الشّهادة فيكون بتقديم طلب إلى مركز التّسجيل من قبل المستفيد مع ذكر السبب، وهي عمليّة تحتاج لتسجيل دخول إلى منظومة مركز التّصديق الرّقمي ومعرفة الرّقم التّعريفي الخاص بالشّهادة، أو أن يقوم مركز التّسجيل بإلغاء الشّهادة وفق ما هو وارد في القانون والنّواظم والضّوابط.

٤. دورة حياة الشّهادة والمتطلّبات التّشغيليّة:

يجب على مركز التّصديق الرّقمي تأمين خدمة عمل شهادات المصادقة الرّقمية دون انقطاع مع ضمان عمليات نشر الشّهادات والتّعديلات الحاصلة عليها وتمكين المستفيدين من الوصول لقوائم الشّهادات الملغيّة بسهولة، وعليه يجب إدارة عملية منح الشّهادات الرّقميّة ابتداءً من تسجيل الطّلب وحتى استلام الشّهادة بدقة متناهية.

٤,١. تقديم طلب الحصول على شهادة المصادقة الرّقميّة:

يمكن لأي جهة عامة في الجمهوريّة العربيّة السّوريّة تقديم طلب للحصول على شهادة مصادقة رقميّة لها أو للعاملين فيها، ويجب على مركز التّسجيل التّأكد من الأمور التّالية:

- إن كل طلب يحتوي البيانات الدقيقة الّتي تثبت - بما لا يدع مجال للشك - هويّة الشّخص، والتّأكد من الأوراق الثبوتيّة للوكيل في حالة وجود وكيل عن جهة ما.
- التّأكد من صحة كافّة البيانات المقدّمة من قبل المستفيد، وتوقيع المستفيد أو الوكيل المفوّض على الاستمارة الخاصّة بالشّهادة.

٤,٢. معالجة الطّلب:

بعد تسجيل الطّلب في مركز التّسجيل، يتم الانتقال للخطوات التّالية:

- تدقيق الطّلب: ويتم بالتّحقق من أن البيانات المقدّمة في الطّلب حقيقية وصحيحة وخالية من التّزوير.
- قبول أو رفض الطّلب: نتيجة عملية التّدقيق السّابقة، يتم اتّخاذ القرار بالقبول أو الرفض.
- المدة الزمنيّة لمعالجة الطّلب: يجب ألّا تتجاوز المدّة **/٩/** أيام عمل، ريثما تستكمل النّواقص والمستندات وعملية التّدقيق.

٤,٣. تصديق الطّلب:

عملية تصديق الشّهادة من قبل مركز التّسجيل تعتبر بمثابة القبول النّهائي لطلب التّسجيل، حيث يقوم مركز التّسجيل بتوقيع شهادات المصادقة الرّقمية بمفتاحه الخاص، ثم يقوم بإعادة الشّهادات الموقّعة إلى مركز التّسجيل لتسليمها للمستفيدين، وهنا يقوم مركز التّصديق الرّقمي بإعلام المستفيد برسالة بريد إلكتروني أو بأيّة طريقة أخرى بأنّ شهادته قد تمّ تصديقها وبإمكانه الحصول عليها، ويجب الحصول على رد من المستفيد بأنّه قد أصبح على علم بذلك. كما يجب أن يحصل مزود التّصديق الرّقمي أيضاً على موافقة من المستفيد بأنّه قد قبل الشّهادة بعد التجريب.

٤,٤. نشر الشّهادة:

بعد استلام الشّهادة من قبل المستفيد واستلام مركز التّصديق الرّقمي رسالة تأكيد من المستفيد بقبوله الشّهادة، على مركز التّصديق الرّقمي أن يقوم بنشر الشّهادة لتصبح البيانات المسموح بنشرها متاحة في قاعدة بيانات مركز التّصديق الرّقمي، وذلك عبر بروتوكول الـ LDAP.

٤,٥. شروط استخدام الشّهادة مع زوج المفاتيح:

تحدد شروط استخدام الشّهادة الرّقمية وزوج المفاتيح، المفتاح العام والخاص، بالنّقاط التّالية:

- معرفة عامة عن كيفيّة استخدام شهادة المصادقة الرّقمية وعن آليّة عمل البنية التّحتيّة للمفتاح العام.
- تزويد مركز التّصديق الرّقمي ومركز التّسجيل بالمعلومات الصّحيحة والدّقيقة أثناء المراسلة معهم.
- الاطّلاع والموافقة على كامل الشّروط والسّياسات والضّوابط والنّواظم الموضوعة والمنشورة من قبل مركز التّصديق الرّقمي .
- استخدام الشّهادة لأهداف قانونيّة ومشروعة حسب القانون والنّواظم والضّوابط الصّادرة عن الهيئة.
- إعلام مركز التّصديق الرّقمي بأيّة تغييرات تحصل على البيانات الخاصّة بالشّهادة.
- التّوقف عن العمل بشهادة المصادقة الرّقميّة في حال أصبحت البيانات المُتضمنة فيها خاطئة أو غير صالحة، أو عند انتهاء صلاحيّة الشّهادة.
- عندما تنتهي صلاحيّة الشّهادة، يجب إزالتها من أيّ جهاز أو مخدّم أو تطبيق كانت تُستخدم فيه.
- اتّخاذ الإجراءات الكفيلة بمنع فقدان أو سرقة أو استخدام غير مشروع للمفتاح الخاص.
- اتّخاذ الإجراءات الكفيلة بحفظ المفتاح الخاص بشكل آمن.
- الطّلب من مركز التّصديق الرّقمي تعليق العمل بالشّهادة أو إلغائها عند حدوث مشكلة ما.

٤,٦. تجديد الشّهادة:

إنّ عمليّة تجديد الشّهادة تحتاج لوجود صاحب العلاقة شخصيّاً، حيث يقوم بتقديم طلب لتجديد شهادته الرّقميّة، ويمكن أن يتم تجديد نفس الشّهادة ثلاث مرات بنفس زوج المفاتيح، أو مفاتيح جديدة ولمدة ثلاث سنوات متتالية، ولكن بعد انقضاء فترة الثلاث سنوات يجب تجديد الشّهادة مع توليد زوج جديد من المفاتيح، وتتضمن عملية تجديد الشّهادة ما يلي:

- **حالة تجديد الشّهادة بنفس زوج المفاتيح في الشّهادة القديمة:**

يتطلّب الحضور الشّخصي للمستفيد أو الوكيل المفوّض، ويتم التّحقق من بيانات المستفيد والتّأكد من وجود أي تعديلات على بياناته المُسجلة مسبقاً، ومن ثم تسير العملية بنفس تراتبية طلب الشّهادة، أي يتمُّ تدقيقها ومن ثم تصديقها من قبل مركز التّصديق الرّقمي ، وإعلام المستفيد بذلك، ثم إرسالها إلى مركز التّسجيل لتسليمها للمستفيد وأخذ موافقة منه أنّه قبل الشّهادة.

- **حالة شهادة جديدة مع توليد مفتاحين جديدين عام وخاص:**

في هذه الحالة يتوجّب وجود سبب أو شرط يوجب الحصول على شهادة جديدة بمفتاحين جديدين، قد يكون انقضاء فترات التّجديد الرّوتينية المحدّدة بثلاث سنوات، أو أيّة تغييرات في بيانات المستفيد أو أن البيانات القديمة غير صالحة ...الخ، ويكون الإجراء المتبع هو الحضور الشّخصي للمستفيد، والمتابعة في الإجراءات وكأنه يقدّم طلب للحصول على شهادة رقمية للمرة الأولى.

٤,٧. تعديل الشّهادة:

أي تعديل في بيانات الشّهادة المقدّمة من المستفيد يتطلّب تجديد الشّهادة وفق البند (٤,٦).

٤,٨. إيقاف أو تعليق الشّهادة الرّقمية:

يمكن أن تتم هذه العملية بناءً على طلب المستفيد، وقد تبقى الشّهادة معلّقة أو ملغاة إلى حين تقديم طلب آخر من قبل المستفيد مبرر بإعادة تفعيلها، أو يمكن أن يقوم مركز التّسجيل بتعليق أو إلغاء شهادة ما وفق ما هو وارد في هذه الوثيقة.

وفي كلتا الحالتين على مركز التّسجيل أن يُعلم بقية المستفيدين بوضع أيّة شهادة يتم تعليقها أو إلغاؤها عبر برتوكول الـ LDAP والّذي يتيح الوصول للمعلومات العامّة والمسموح نشرها عن الشّهادات الرّقميّة، وذلك عبر قوائم الشّهادات الملغاة.

أما بالنّسبة لأهم أسباب إلغاء الشّهادة الرّقمية:

- فقدان أو سرقة الشّهادة، أو الحصول على المفتاح الخاص من قبل طرف ثالث بطريقة غير مشروعة.
- الإخلال بالشروط والإجراءات المُدرجة في وثيقتي سياسات التّصديق الرّقمي وإجراءات التّصديق الرّقمي، أو الإخلال بالقانون والنّواظم والضّوابط الملحقة به.
- الإخلال بأحد بنود العقد.

بالنسبة للوقت المطلوب لهذه العملية: عند تقديم طلب تعليق أو إلغاء شهادة يجب ألا يستغرق أكثر من ساعة واحدة، كما يجب أن يستجيب مركز التّصديق الرّقمي خلال ساعة واحدة على الأكثر.

٤,٩. حالة الشّهادة الرّقمية:

تعتبر خدمة الشّهادات الفعّالة هي المسؤولة عن معرفة حالة الشّهادة وهي تزود مخدّم الـ LDAP والموقع الإلكتروني الخاص بمركز التّصديق الرّقمي، بحالة الشّهادات الرّقمية وهما بدورهما يقدّمان الخدمة للمستفيدين. ذلك لأن أي مستفيد قبل أن يباشر باستخدام شهادته الرّقمية عليه التّحقق من الشّهادات الفعّالة والشّهادات الملغيّة على التّرتيب.

إنّ خدمة الشّهادات الفعّالة يجب أن تكون متاحة على مخدّمات مركز التّصديق الرّقمي ٧/٢٤.

تفقد الشّهادة الرّقميّة لأيٍّ مستفيد صلاحيتها عندما تنتهي مدّتها الزمنيّة أو عندما تُلغى، أو عندما تتوقّف خدمة التّوقيع الرّقمي.

٤,١٠. إجراءات حفظ المفاتيح:

من أهم واجبات مركز التّصديق الرّقمي هي حفظ المفاتيح المتعلقة بالشّهادات الرّقميّة مع الاحتفاظ بنسخة احتياطيّة، ويفضّل أن تكون النّسخة الاحتياطيّة مشفّرة، وأن لا تكون في مكان واحد، كما يجب مراعاة الأجهزة الّتي سيتم الحفظ عليها، مع الأخذ بعين الاعتبار من هم الأشخاص المخوّل لهم الدخول والعمل على هذا المستوى من المنظومة.

٥. الإجراءات الإداريّة والتّشغيليّة:

٥,١. الأشخاص المعنيين ومهامهم:

مشغّل مركز التّصديق الرّقمي :

- وضع السياسات الأمنيّة والإشراف عليها.
- نشر وثائق سّياسات الشّهادة الرّقمية وإجراءات التّصديق الرّقمي .
- منح وتجديد وإلغاء الشّهادات الرّقمية.
- توليد ونشر قوائم الشّهادات الملغيّة.
- تدقيق ومراقبة سجلّات العمليّات المُنفّذة على مخدّم مركز التّصديق الرّقمي .

مسؤول ومشرف النّظام :

- إدارة وصيانة التجهيزات البرمجيّة والعتاد الصّلب.
- أخذ النّسخ الاحتياطيّة واستعادتها في حال حدوث مشاكل أو أخطاء معيّنة.
- تطوير البرمجيّات وترقيتها.
- متابعة برامج الحماية والثّغرات الأمنيّة المُكتشفة.
- تدقيق ومراقبة سجلّات العمليات المنفّذة على مخدّم مركز التّصديق الرّقمي .

مسؤولي مركز التّسجيل:

- استقبال طلبات الحصول على الشّهادات الرّقمية أو تجديدها أو تعليقها أو إلغائها.
- التّحقق من هويّة وبيانات المستفيد أثناء تقديم الطّلبات.
- نقل الطّلبات إلى مركز التّصديق الرّقمي .
- تدقيق ومراقبة سجلّات العمليات المنفّذة على مخدّم مركز التّسجيل.

بالنّسبة لعدد الأشخاص المقترحين وفق المهام:

الوظيفة	عدد الأشخاص المقترح
مشغّل مركز التّصديق الرّقمي	٣
مسؤول ومشرف النظام	٤
موظفو مركز التّسجيل	٤
موظفو الدّعم وخدمات الزبائن	٨

وسيتم وضع جدول لمؤهلات وخبرات العاملين في منظومة البنية التّحتيّة لمنظومة المفتاح العام.

٥,٢. نظام إدارة المخاطر:

يجب على إدارة مركز التّصديق الرّقمي وضع خطة شاملة تضمن عمل منظومة البنية التحتيّة لمنظومة التّوقيع الرّقمي باستمرار دون توقّف، وكذلك توثيق الخطوات اللّازمة لاستعادة المنظومة وإعادتها للعمل بالسرعة القصوى في حالة حدوث أي خلل أو مشكلة سواء للتجهيزات أو للبرمجيات.

٦. أدوات التّحكم الفنيّة والحمايات الأمنيّة:

٦,١. توليد زوج المفاتيح /العام والخاص:

إن عملية توليد أي شهادة رقميّة تقتضي توليد زوج من المفاتيح وهما المفتاح العام والمفتاح الخاص، وبما أن المفتاح العام يتم نشره وتداوله لأي شهادة رقميّة، فإن السرّية يجب أن تكون من نصيب المفتاح الخاص لذلك يجب ألّا تحفظ نسخة منه، وهذا ينطبق على الجميع اعتباراً من رأس الهرم وهو سلطة التّوقيع الإلكتروني الجذرية وانتهاءً بالمستخدم العادي.

إنّ عملية توليد زوج المفاتيح لسلطة التّوقيع الإلكتروني الجذريّة، تتم عبر تجهيزات وبرمجيات خاصّة ويتم حفظه وفق إجراءات أمنيّة مشدّدة، وذلك لمنع تسرّبه وانتشاره للعموم.

أما توليد زوج المفاتيح للمستخدمين العاديين فيتم بإحدى الطريقتين:

- الأولى عبر التّسجيل أثناء تسجيل المستفيد لطلب الحصول على الشّهادة الرّقميّة.
- والثانية أن يقوم المستخدم بتوليد زوج المفاتيح الخاص به.

ولكن بكلتا الحالتين يجب استخدام خوارزميات تشفير مقبولة وفق المعيار المذكور في هذه الوثيقة.

يعتبر مركز التّسجيل هو المسؤول عن نشر المفتاح العام للمستفيد، كون المفتاح العام يجب أن يكون متداولاً، ويجب بعد ذلك أن يوقع المستفيد على استلامه للشهادة الرّقميّة وزوج المفاتيح ليصبح هو المسؤول عن حماية المفتاح الخاص.

في الحالة الأخرى، عندما يقوم المستفيد بتوليد زوج المفاتيح، على المستفيد أن يتعهّد بتقديم المفتاح العام دون تعديلات عليه إلى مركز التّسجيل ليتم نشره.

٦,٢. طول زوج المفاتيح:

يجب أن يكون طول زوج المفاتيح كافياً لمنع إمكانية الحصول على المفتاح الخاص أثناء فترة الاستخدام، ولذلك يجب مراعاة الشروط التالية بالحد الأدنى:

- طول زوج المفاتيح الخاص بسلطة التّوقيع الإلكتروني الجذرية يجب أن يكون 8192 bits.
- في حال وجود مركز تصديق رقمي فرعي يجب أن يكون طول زوج المفاتيح 4096 bits.
- طول زوج المفاتيح للمستخدمين العاديين: 1024 bits.

٦,٣. حفظ المفاتيح:

كل المفاتيح الخاصة التي يتم توليدها من قبل البنية التّحتيّة للمفتاح العام يتم حفظها وأرشفتها وحمايتها من قبل المنظومة.

٦,٤. المخدّمات والشّبكة:

إنّ التّجهيزات المتواجدة في منظومة البنية التّحتيّة للمفتاح العام، تتمتع بمواصفات فنية تمكّنها من توفير خدمات التّوقيع الرّقمي، وهناك إجراءات أمنية مشددة تمنع اختراقها، وهذا الأمر ينطبق أيضاً على الشّبكة الداخلية لمنظومة البنية التّحتيّة للمفتاح العام وغير المتّصلة بالشّبكة الخارجية.

٦,٥. الختم الزّمني:

الخدمة الإلكترونية الموثوقة التي يوفرها المزوّد لتحديد الوقت والتّاريخ واستخدامها في عمليات المصادقة والتّحقق.

٧. إدارة الشّهادات وقوائم الشّهادات الملغاة

٧,١. توصيف مكوّنات الشّهادة:

جميع برمجيات منظومة البنية التّحتيّة للمفتاح العام وما ينتج عنها من وثائق وشهادات ومفاتيح وقوائم شهادات ملغيّة وغيرها، متوافقة مع المعايير العالميّة مثل: RFC 3280 , X.509،

بالتّالي جميع الشّهادات التي يتم توليدها من قبل البنية التّحتيّة للمفتاح العام يجب أن تحتوي الحقول التّالية:

- الإصدار: رقم الإصدار والمعيار العالمي المتوافق معه.
- رقم تسلسلي للشهادة: رقم فريد ووحيد وعنيد.
- المانح: اسم المؤسّسة أو الهيئة أو الاسم المميز لمركز التّصديق الرّقمي ..
- الصلاحيّة: تاريخ البدء وتاريخ الانتهاء.
- عنوان الشّهادة: اسم حاملها مثلاً.
- المفتاح العام.
- خوارزميّة التّشفير.
- بالإضافة لمعلومات أخرى.

٧,٢. توصيف قائمة الشّهادات الملغية:

يجب أن تحتوي قوائم الشّهادات الملغيّة على الحقول التّالية:

- الإصدار: رقم الإصدار والمعيار العالمي المتوافق معه.
- المانح: اسم المؤسسة أو الهيئة أو الاسم المميز لمركز التّصديق الرّقمي .
- خوارزمية التّشفير.
- آخر تحديث.
- تاريخ التّحديث التّالي: ٣٠ يوم مثلاً.
- قائمة بالشّهادات الملغيّة: تحتوي على الأرقام التّسلسلية للشهادات الملغيّة وتاريخ الإلغاء.