



الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

الجمهورية العربية السورية

وزارة الاتصالات والتقانة

الهيئة الوطنية لخدمات الشبكة

إجراءات التصديق الرقمي

Certificate Practice Statement

CPS

النسخة الأولى



سجلات التغيير

التاريخ	إصدار	الحالة	النسخة
	فريق عمل الهيئة الوطنية لخدمات الشبكة	مسودة	1.0
	مجلس الهيئة الوطنية لخدمات الشبكة رقم:.....		
	قرار تنظيمي رقم:.....		

المراجعات

التاريخ	الاسم	الصفة



جدول المحتويات

رقم الصفحة	البند	رقم البند
٤	مقدمة	١
٤	معلومات عامة عن مركز التصديق الرقمي	٢
٤	سياسات الشهادات الرقمية وأنواع الشهادات الممنوحة	٣
٥	إجراءات منح وتجديد وتعليق وإلغاء الشهادات الرقمية	٤
٥	خطوات منح شهادة رقمية	٤,١
٦	خطوات تجديد الشهادة الرقمية	٤,٢
٧		٥
	خطوات تعليق العمل بالشهادة الرقمية أو إلغاؤها	
٧	خوارزميات التشفير المستخدمة وطول زوج المفاتيح	٥
٨	الأشخاص المعنيين و مهامهم	٦
٨	مُشغّل مركز التصديق الرقمي	٦,١
٨	مسؤول ومشرف النظام لدى مركز التصديق الرقمي	٦,٢
٩	مسؤول مركز التسجيل	٦,٣
٩	مدة الشهادة الرقمية وصلاحياتها	٧
٩	سياسات تعليق العمل بالشهادة الرقمية أو إلغاؤها	٨
١٠	إدارة قوائم الشهادات الملغية	٩



١. مقدمة

من خلال إجراءات التّصديق الرّقمي يستطيع المستفيد معرفة الطّرق الفنية والأمنية والإجرائية المُتبعة لإصدار الشّهادة من قبل مركز التّصديق الرّقمي، وهي تمثّل اللائحة التنفيذية لسياسة الشّهادة الرّقمية، الصّادرة باللائحة التنظيمية رقم PKI/04.

٢. معلومات عامة عن مركز التّصديق الرّقمي

يقع مركز التّصديق الرّقمي الوطني في الهيئة الوطنية لخدمات الشبكة، وهو المسؤول عن منح الشّهادات الرّقمية للعاملين في القطاع العام بصفاتهم الوظيفية

موقع المركز على الإنترنت:

المنشورات:

سياسة الشّهادة الرّقمية:

إجراءات التّصديق الرّقمي:

٣. سياسات الشّهادات الرّقمية وأنواع الشّهادات الممنوحة

تصدر كافة الشّهادات الرّقمية من مركز التّصديق الرّقمي، وهي تخوّل صاحبها استخدام كافة الخدمات التي تتضمنها الشّهادة الرّقمية والتي هي:

- التوقيع الرّقمي
 - عدم الإنكار
 - سلامة ودقة المعلومة
 - الخصوصية
- إجراءات التّصديق الرّقمي

• التشفير

و يمثل مركز التصديق الرقمي مصدر الثقة في كافة أنواع الخدمات المتاحة لحاملي الشهادات الرقمية.

يتم الحصول على شهادة رقمية ما بتسجيل طلب في مركز التسجيل وذلك إما بالحضور شخصياً أو عبر الموقع الإلكتروني لمركز التسجيل على الشبكة، <https://ra.nans.gov.sy>، حيث يتم ملء الاستمارة المطلوبة بالبيانات الصحيحة والدقيقة.

المدة الزمنية للحصول على الشهادة الرقمية، في حال صحة البيانات المقدمة، والموافقة على إصدار الشهادة، يتم خلال مدة أقصاها 9/ أيام من تقديم الاستمارة.

ويقوم مركز التصديق بمنح أنواع الشهادات الموضحة في الجدول أدناه:

الوصف	اللاحقة
صيغة قياسية لشهادة الاتصال الآمن، وهي مصممة بشكل آمن لإدراجها ضمن لغة الآلة أو في النصوص الكبيرة مثل البريد الإلكتروني	.pem
صيغ شائعة للشهادات الرقمية	.cer, .crt, .der
صيغة قياسية لتشفير جملة الرسالة، وتستخدم لنشر الشهادات	.p7b, .p7c - PKCS#7
صيغة قياسية لتبادل المعلومات الشخصية، وتستخدم عادة لتخزين المفاتيح الخاصة	.p12 - PKCS#12
صيغة أخرى لـ PKCS#12	.pfx - PFX

٤. إجراءات منح وتجديد وتعليق وإلغاء الشهادات الرقمية

٤.١. خطوات منح شهادة رقمية

- الحضور الشخصي إلى مركز التسجيل.
- تقديم طلب في مركز التسجيل
- ملء الاستمارة والتي يمكن الحصول عليها من الموقع الإلكتروني.

- تدقيق الطلبات في مركز التسجيل.
 - نقل الطلبات إلى مركز التصديق الرقمي.
 - مراجعة الطلبات من قبل مركز التصديق الرقمي.
 - إصدار الشهادات الرقمية، وتوقيعها من قبل مركز التصديق الرقمي.
 - إرسال الشهادات الرقمية الموقعة إلى مركز التسجيل، مع إعلام المستخدم عبر البريد الإلكتروني.
 - استلام الشهادات الرقمية من قبل المستخدم وإقراره بذلك.
 - نشر الشهادة الرقمية من خلال مركز التصديق الرقمي على الموقع الإلكتروني.
- ٤,٢ . خطوات تجديد الشهادة الرقمية

- الحضور الشخصي.
- تقديم طلب خطي في حال عدم وجود تغيير في بيانات المستخدم.
- ملء استمارة جديدة في حال حصول أي تغييرات في بيانات الشهادة القديمة.
- طلب إلغاء الشهادة القديمة في حال حدوث أي تغييرات في بياناتها.
- نقل طلبات التجديد من مركز التسجيل إلى مركز التصديق الرقمي.
- مراجعة الطلبات من قبل مركز التصديق الرقمي.
- إصدار الشهادات الرقمية وتوقيعها من قبل مركز التصديق الرقمي.
- إعادة الشهادات الرقمية الموقعة إلى مركز التسجيل، مع إعلام المستخدم عبر البريد الإلكتروني.
- استلام الشهادات من قبل المستخدم وإقراره بذلك.
- نشر الشهادة من خلال مركز التصديق الرقمي على الموقع الإلكتروني.

- نشر الشَّهادة الملغاة على الموقع الإلكتروني في قوائم الشَّهادات الملغية.

٤,٣. خطوات تعليق العمل بالشَّهادة الرقمية أو إلغائها

يتم تعليق أو إلغاء الشَّهادات الرقمية إما بناءً على طلب المستخدم، أو من قبل مركز التصديق الرقمي وفق ما هو وارد في القانون، والنواظم والضوابط، وهذه الوثيقة، ويكون طلب التعليق/الإلغاء من قبل المستخدم وفق ما يلي:

- الحضور الشخصي
- تقديم طلب تعليق/إلغاء مع ذكر الأسباب الموجبة بالتفصيل.
- نقل طلبات الإلغاء/التعليق من مركز التسجيل إلى مركز التصديق الرقمي.
- مراجعة الطلبات من قبل مركز التصديق الرقمي.
- تأكيد الإلغاء/التعليق من قبل مركز التصديق الرقمي.
- نشر الشَّهادة الملغاة/المعلقة في قوائم الشَّهادات الملغية مع ذكر تاريخ الإلغاء/التعليق.

٥. خوارزميات التشفير المستخدمة وطول زوج المفاتيح

بالنسبة لخوارزميات التشفير موضحة في الجدول أدناه:

الوصف	الخوارزمية
خوارزمية لتشفير المفتاح العام	RSA
خوارزمية التوقيع الرقمي	DSA
خوارزمية التوقيع الرقمي بالمنحني الاهليجي، وهي بديل عن خوارزمية DSA	ECDSA

أما بالنسبة لأطوال زوج المفاتيح فهي موضحة في الجدول:

قوة المفتاح	طول المفتاح	المستخدم النهائي
ضعيف	512	NA
أساسي	1024	المستخدم العادي
قوي	2048	المخدمات
متقدم	4096	سلطة التسجيل
الأقوى	8192	سلطة تصديق فرعية

٦. الأشخاص المعنيين و مهامهم

٦,١. مُشغّل مركز التّصديق الرّقمي

- وضع السياسات الأمنية والإشراف عليها.
- نشر وثائق سياسات التّصديق الرّقمي وإجراءات التّصديق الرّقمي.
- منح وتجديد وإلغاء الشّهادات الرّقمية.
- توليد ونشر قوائم الشّهادات والشّهادات الملغية.
- تدقيق ومراقبة سجلات العمليات المُنفذة على مخدّم مركز التّصديق الرّقمي.

٦,٢. مسؤول ومشرف النظام لدى مركز التّصديق الرّقمي

- إدارة وصيانة التجهيزات البرمجيات والعتاد الصلب.

- أخذ النسخ الاحتياطية واستعادتها في حال حدوث مشاكل أو أخطاء معينة.
- تطوير البرمجيات وترقيتها.
- متابعة برامج الحماية والثغرات الأمنية المكتشفة.
- تدقيق ومراقبة سجلات العمليات المنفذة على مخدّم مركز التصديق الرقّمي.

٦,٣ . مسؤول مركز التسجيل

- استقبال طلبات الحصول على الشّهادات الرّقمية أو تجديدها أو تعليقها أو إلغائها.
- التحقق من هوية وبيانات الزبون أثناء تقديم الطلبات.
- نقل الطلبات إلى مركز التصديق الرّقمي.
- تدقيق ومراقبة سجلات العمليات المنفذة على مخدّم مركز التسجيل.

٧ . مدة الشّهادة الرّقمية وصلاحيّتها

موضحة في الجدول التالي:

مستخدم الشّهادة	صلاحيّتها	تجديد زوج المفاتيح
مركز التصديق الوطني الجذري	١٠ - ٢٠ سنة	كل ١٠ سنوات
مركز التصديق الرّقمي	١٠ سنين	كل ٥ سنوات
مركز التسجيل	٦ سنين	كل ٣ سنوات
المؤسسات/ الجهات	٣	كل ٣ سنوات أو سنوياً
المستخدم العادي	١	كل ٣ سنوات أو سنوياً

٨ . سياسات تعليق العمل بالشّهادة الرّقمية أو إلغائها

يمكن أن تتم هذه العملية بناءً على طلب المستخدم وفي هذه الحالة تبقى الشهادة معلقة أو مُلغاة إلى حين تقديم طلب من الزبون مبرر بإعادة تفعيلها، أو يمكن أن يقوم مركز التصديق الرقمي بتعليق أو إلغاء شهادة ما بناءً على أسباب سيأتي ذكرها لاحقاً.

وفي كلتا الحالتين على مركز التصديق الرقمي أن يعلم بقية المستخدمين بوضع أي شهادة يتم تعليقها أو إلغائها عبر بروتوكول خاص /LDAP/ يتيح الوصول للمعلومات العامة والمسموح نشرها، والمتعلقة بقوائم الشهادات الرقمية، وقوائم الشهادات المُلغاة.

أما بالنسبة لأهم أسباب إلغاء الشهادة الرقمية من قبل مركز التصديق:

- بناءً على طلب صاحب الشهادة.
- عند إعلام مُزوّد خدمات التصديق الرقمي بوفاة الشخص الطبيعي أو حل الشخص الاعتباري (المُرتبط بشخص طبيعي) صاحب الشهادة.
- في حال ثبوت أنّ الشهادة قد استعملت بغرض التّدليس أو الغش.
- في حال ثبوت أنّه جرى انتهاك منظومة إنشاء التّوقيع الرقمي.
- في حال ثبوت أنّ المعلومات المتضمّنة في الشهادة قد تغيّرت، أو أن المعلومات المتضمّنة في الشهادة غير صحيحة.
- بناءً على أمرٍ معلّل من الهيئة.
- فقدان أو سرقة الشهادة، أو الحصول على المفتاح الخاص من قبل طرف ثالث بطرق غير مشروعة.
- الإخلال بالشروط والإجراءات المدرجة في وثيقتي سياسات الشهادة الرقمية، وجراءات التصديق الرقمي.
- الإخلال بأحد بنود العقد.

٩. إدارة قوائم الشهادات الملغية



يشرف على هذه العملية مركز التصديق الرقمي، حيث يقوم بتجهيز قائمة بالشهادات الملغية أو التي تم تعليق العمل بها مع تاريخ إلغاء/تعليق الشهادة، وتجري هذه العملية بشكل دوري كل يوم، ويقوم التصديق الرقمي بنشرها بشكل آني عبر بروتوكول خاص /LDAP/ على الموقع الإلكتروني، بما يُمكن المستخدمين من معرفة حالة أي شهادة.