الرقم :

التاريخ:

جدول المحتويات

أولاً: آلية إصدار الوثائق الإلكترونية

يمكن إصدار واعتماد الوثائق الإلكترونية عند توفر منظومة / برامج وآليات تحقق بمجموعها المزايا التالية على الأقل:

- دعم التوقيع الرقمي للوثائق الإلكترونية، مع مراعاة واحترام خصائص الشهادات أثناء التوقيع وخصوصاً مجال الاستخدام، والتحقق من حالة الإلغاء للشهادة.
- دعم إمكانية التحقق من التواقيع الرقمية للوثائق.
- إمكانية حفظ حالة التوقيع مع الوثيقة نفسها لإتاحة الإمكانية للتحقق من صحة التواقيع الرقمية للمستندات في أي وقت لاحق للتوقيع.
- التخزين المضمون والأرشفة لكافة الوثائق الصادرة والموقعة رقمياً بحيث يمكن الرجوع لأي وثيقة موقعة لاحقاً.
- دعم إمكانية نشر الوثائق وإتاحتها للجهات / الأشخاص المحتاجة لها، مع تأمين كامل وسائل الحماية الضرورية.

ثانياً: القوانين والتشريعات

القوانين الداعمة للتحول إلى استخدام الوثائق الإلكترونية كمرادف أو بديل للوثائق الورقية:

- القانون رقم ٧ لعام ٢٠٢٣ – قانون التصديق الرقمي وخدمات تقانة المعلومات.
- القانون رقم ٣ لعام ٢٠١٤ – قانون المعاملات الإلكترونية.

ثالثاً: كيفية الحصول على خدمة التوقيع الرقمي

تشمل خدمات التصديق الرقمي ما يلي:

- تأمين حامل إلكتروني لتوليد المفاتيح الخاصة Private Keys وحفظها مع الشهادات الرقمية المرتبطة.
- شهادة رقمية لعامل بالقطاع العام بصفته الوظيفية.
- شهادة رقمية لعامل بالقطاع الخاص بصفته الوظيفية (وهي خدمة مؤقتة لحين توفر مزودي خدمات تصديق للقطاع الخاص مرخصين أصولاً من الهيئة).
- شهادة اتصال آمن SSL Certificate للأغراض الخاصة (للتواصل الآمن عبر الشبكات المغلقة).
- شهادات اتصال آمن مخصصة (توقيع رماز Code Signing).
- شهادة رقمية لجهة وهي شهادة رقمية يتم إصدارها لتمثل جهة ما (مؤسسة/شركة/جهة حكومية ...)، ويمكن استخدامها في عمليات التوقيع الرقمي وتكون بمثابة ختم الكتروني يمثل الجهة.

يمكن الحصول على هذه الخدمات عبر التواصل مع الهيئة / مركز التصديق الرقمي وتقديم الطلبات اللازمة وفق الاستمارات الخاصة بكل نوع وهي متوفرة على الموقع الإلكتروني للمركز https://info.ecc.sy/.

رابعاً: كيفية الحصول على اعتمادية QR

- يجب أن تحصل المنظومة التي تدعم إصدار رمز الاستجابة السريع (QR) على اعتمادية من الهيئة، وذلك قبل تشغيلها، من خلال تقديم طلب رسمي لديوان الهيئة متضمناً الوثائق التّاليّة:

أ. الجهة المسؤولة عن المنظومة، وما يثبت بأنها مالكة للمنظومة، أو وكيلة لمالكها، أو مرخص لها باستخدام وتشغيل المنظومة ضمن الجمهوريّة العربيّة السّوريّة.
ب. مكان استضافة المنظومة.
ج. الفئات المستهدفة.
د. توصيف عمل المنظومة.
هـ. مكونات المنظومة.
و. وثيقة آلية قياس معايير جودة المنظومة.
ز. وثيقة استرشادية لسياسة الاستخدام.
ح. تقرير اجتياز اختبار الاختراق الاحترافي، واختبار التّوافق مع السّياسة الوطنيّة لأمن المعلومات متضمنة سياسات أمن المعلومات، وإجراءات الحماية.
ط. تعهد بالتّوافق مع الأنظمة والقوانين (قانون المعاملات الإلكترونيّة، القانون رقم /٧/ المتضمن إحداث الهيئة الوطنية لخدمات تقانة المعلومات وتعليماته التنفيذية، والضّوابط والنّواظم الخاصّة بهذه القوانين، وقانون تنظيم التّواصل على الشّبكة ومكافحة الجريمة المعلوماتيّة رقم /٢٠/ للعام ٢٠٢٢ وتعليماته التّنفيذيّة).

- تتم دراسة الطلب وإجراء الاختبارات اللازمة على المنظومة
- يتم منح المنظومة الاعتمادية.

خامساً: المطلوب تجهيزه من الجهة المستثمرة

يجب على كل مُصدِر وثيقة إلكترونية أن يراعي ما يلي:

- تأمين مستلزمات توقيع الوثائق رقمياً وهي:

أ. حامل إلكتروني يحوي المفتاح الخاص (مفتاح التوقيع) والشهادة الرقمية المرتبطة.
ب. وصول شبكي لخدمات التحقق من حالة الإلغاء للشهادة الرقمية.
ج. وصول شبكي لخدمة سلطة الختم الزمني.
د. تأمين آلية سواء كانت برمجية أو إجراءات من قبل موظفين بغاية التحقق من التواقيع الرقمية، الملحق رقم /١/.

- تأمين مستلزمات حفظ الوثائق الإلكترونية وأرشفتها بما يراعي مايلي:

أ. إمكانية حفظ الوثائق الرقمية الموقعة بشكل آمن يمنع إمكانية العبث بمحتواها.
ب. حفظ الوثائق بما يراعي القواعد والمدد الزمنية بما لا يقل عن فترة حفظ الوثائق الورقية المرتبطة.
ج. إتاحة الوثائق الإلكترونية لكل الجهات التي تحتاجها.

- يجب أن تحقق المنظومة التي تدعم إصدار رمز الاستجابة السريع (QR) مايلي:

أ. أن تحقق المنظومة معايير الجودة بما فيها سهولة الاستخدام والكفاءة والسلامة والوثوقية ....

ب. يجبّ أن توفّر المنظومة سياسة استخدام خاصّة بها توضح حقوق وواجبات ومسؤوليات كافّة الأطراف المتعاملة مع المنظومة (المستخدمين، الجهة المسؤولة عن المنظومة).
ج. أن تكون المنظومة المعلوماتية المصدرة لرمز الاستجابة السريع (QR) مملوكة من قبل الجهة المصدرة للوثيقة المدرج عليها الرمز.
د. أن يتم إصدار رمز الاستجابة السريع والبيانات المظهرة على الوثيقة المدرج عليها الرمز معاً وبشكل غير منفصل.
هـ. يمكن أن تحتوي الوثيقة على أكثر من رمز استجابة شرط أن يكون أحدها يحتوي على رابط للتحقق.

- يجب أن يحقق رمز الاستجابة السريع (QR) الذي تصدره المنظومة المعلوماتية المعايير الفنية والتشغيلية التالية:

أ. يجب أن يتوافق رمز الاستجابة السريع (QR Code) مع أحدث المعايير العالمية مثل ISO/IEC 18004:2006.
ب. أن يعرض الرمز معلومات الوثيقة المدرج عليها عند إجراء طلب للتحقق عبر الإنترنت.
ج. يُشترط لحجية الإثبات باستخدام رمز الاستجابة السريع (QR) ما يلي:

- **في حال الرمز الثابت:**
  - أن يحتوي رمز الاستجابة على معلومات الجهة المصدرة ومعرف وحيد يتعلق بالوثيقة بشكل غير قابل للبس مع وثائق أخرى من نفس الجهة.
  - أن يحتوي على بصمة زمنية لتاريخ توليد رمز الاستجابة.
  - أن يحتوي رابط يقود إلى نظام المعلومات المصدر للوثيقة.
  - أن تتطابق البيانات الموجودة على الوثيقة مع بيانات الإصدار في المنظومة المعلوماتية ومع إمكانية الوصول إليها عبر رمز الاستجابة السريع.
- **في حال الرمز المتغير**، إضافة إلى ما سبق يجب أن يحتوي الرمز البيانات التالية:
  - أن يحتوي على بيانات المستخدم حسب نوع المعاملة.
  - الهدف من العملية.

سادساً: المطلوب من الجهات بعد اعتماد الوثائق الإلكترونية

- الالتزام بكافة البنود المذكورة في المادة (٦،٨،٩) الواردة في قانون المعاملات، وفي القانون رقم /٧/ لعام ٢٠٢٣ وتعليماته التنفيذية.
- الالتزام بكافة البنود المذكورة في اللائحة رقم (NAITS/ET/01) المتعلقة بالنّواظم والضّوابط الخاصّة بحفظ الوثائق الإلكترونيّة.
- الالتزام بكافة البنود المذكورة في اللائحة رقم (NAITS/ET/02) المتعلّقة بالنّواظم والضّوابط الخاصّة بمواصفات المنظومات المعلوماتيّة للمعاملات الإلكترونيّة

ملحق /١/ – التحقق من صلاحية التوقيع الرقمي

يتطلب اجراء التوقيع الرقمي والتحقق منه ليعتبر مقبولاً قانونياً إجراءات محددة من جانب الموظف الذي يوقع الوثيقة (يشار إليه فيما بعد بالموقِّع)، والموظف الذي يتلقى/يقرأ الوثيقة (يشار إليه فيما بعد بالمستلم).

- **مسؤوليات الموقِّع:**
  - يجب على الموقِّعين الحصول على زوج من المفاتيح، مفتاح خاص (يدعى أيضاً مفتاح التوقيع، ويجب أن يتم توليده وحفظه بأمان على حامل إلكتروني) ومفتاح عام يتم توقيعه من مزود خدمة تصديق مرخص (حالياً الهيئة فقط).
  - يجب على الموقعين حماية مفتاحهم الخاص والحفاظ على سريته.
  - إذا اعتقد الموقّع أن مفتاح التوقيع الخاص به قد سُرق أو تم اختراقه بطريقة أخرى، فيجب على الموقّع الاتصال بمزود خدمة التصديق على الفور ليتم إلغاء الشهادة الرقمية المرتبطة.
- **مسؤوليات المستلم:**
  - يجب أن يتحقق المستلمون من أن المفتاح العام (الشهادة الرقمية) للموقّع قد تم توقيعه بواسطة مزود خدمة تصديق مرخص، وذلك من خلال عرض تفاصيل الشهادة الرقمية للموقع.
  - إذا كان التوقيع الرقمي للموقع غير صحيح، يجب ألا يثق المستلم بمصدر الوثيقة.
  - إذا اعتقد المستلم أنه أسيء استعمال التوقيع الرقمي، يجب عليه إبلاغ مزود خدمة التصديق.

١. التحقق من صحة التوقيع الرقمي على الوثائق الإلكترونية:

يجب توقيع وقراءة الوثائق باستخدام برنامج/تطبيق/منظومة معتمد (يتفق عليه الطرفان، الموقّع والمستلم) على أن يحقق البرنامج الميزات التالية على الأقل:

- أثناء التوقيع: يمكنه التوقيع باستخدام مفتاح التوقيع الموجود ضمن الحامل الإلكتروني.
- أثناء التوقيع: يمكنه التحقق من صلاحية الشهادة المرتبطة بمفتاح التوقيع من حيث حالة الإلغاء (هل الشهادة ملغية أم مازالت صالحة) وذلك عبر إحدى آليات التحقق التي هي إما OCSP أو CRL.
- أثناء التوقيع: يمكنه التحقق من صلاحية الشهادة المرتبطة بمفتاح التوقيع (هل مازالت ضمن فترة الصلاحية؟).
- أثناء التوقيع: يمكنه الاتصال بخدمة الختم الزمني واستخدامها وإدراجها مع بيانات التوقيع.
- أثناء التوقيع: يراعي ويحترم خصائص الشهادات وخصوصاً لجهة حقل مجال الاستخدام KeyUsage.
- أثناء التحقق: باستخدام الشهادة الرقمية المرتبطة بمفتاح التوقيع يجب التحقق من صلاحية الوثيقة (لم يطرأ تعديل عليها بعد التوقيع).
- أثناء التحقق: يجب التحقق من صلاحية الشهادة الرقمية المرتبطة بمفتاح التوقيع من حيث حالة الإلغاء بوقت التوقيع ومن حيث الصلاحية الزمنية (هل كانت ما زالت صالحة بوقت التوقيع؟)

- أثناء التحقق: يجب التحقق من كامل مسار الثقة، أي من حالة الإلغاء والصلاحية الزمنية لكافة الشهادات الوسيطة (الشهادات ضمن مسار الثقة وصولاً للشهادة الجذر)
- أثناء التحقق: يجب التأكد من وثوقية الشهادة الجذر (هل هي من ضمن الشهادات الجذر الموثوق بها ضمن نظام التشغيل و/أو المنظومة)
- أثناء التحقق: يجب التأكد من مصدر وقت التوقيع، والتحقق من أن جواب سلطة الختم الزمني موقع وصادر عن منظومة موثوقة.
- يجب أن تستخدم كامل مكونات المنظومة مصدر موثوق لمزامنة الوقت.

ملاحظة:

لتحقيق إمكانية التحقق من التوقيع طويلة الأمد LTV (حتى بعد انتهاء صلاحية الشهادة الرقمية المرتبطة بمفتاح التوقيع) يجب تخزين البيانات التالية ضمن الوثيقة الموقعة:

- الشهادة الرقمية المرتبطة بمفتاح التوقيع.
- كامل الشهادات في سلسلة الثقة وصولاً للشهاة الجذر.
- بيانات التحقق من حالة الإلغاء (مثلاً جواب المستجيب ocsp).
- بيانات وقت التوقيع بشكل موثوق (جواب خدمة الختم الزمني tsa).

٢. التحقق من صحة التوقيع الرقمي على الوثائق المطبوعة (الورقية):

يمكن اتباع الإجراء التالي على سبيل المثال:

- عند إنشاء وثيقة موقعة رقمياً وبشكلها النهائي، يتم نشرها عبر رابط خاص متاح الوصول إليه عبر الإنترنت.
- تحوي كل وثيقة على رمز استجابة سريع QR Code يتضمن عنوان الرابط الذي يحوي الوثيقة الرقمية.
- يمكن دائماً مسح رمز الاستجابة السريع QR Code وفك ترميزه للحصول على رابط نشر الوثيقة الرقمية الموقعة رقمياً والتحقق من صحتها رقمياً.
- يمكن أتمتة العمليات السابقة عبر أداة (جزء من البرنامج/ التطبيق/المنظومة) بحيث يقوم الموظف فقط بمسح رمز الاستجابة، وتقوم الأداة بفك الترميز والحصول على رابط تحميل الوثيقة الرقمية الموقّعة وتحميلها والتحقق منها وعرض النتيجة النهائية.
- لزيادة أمان الوثائق الرقمية المنشورة والمتاحة عبر الإنترنت، يمكن وضع ترميز معين لكل وثيقة يكون بمثابة كلمة مرور للوصول إليها وتحميلها، ويكون هذا الترميز جزء من الوثيقة المطبوعة، وبالتالي يمكن تحميل النسخة الرقمية من الوثيقة فقط من قبل من يملك النسخة المطبوعة.