متطلبات الاعتراف بالتوقيع الرقمي

يتطلب اجراء التوقيع الرقمي والتحقق منه ليعتبر مقبولاً قانوناً 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 ايضاً 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.

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 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 تحقق 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)

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 ركز 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.