

ملحق (١): المواصفات والمعايير الفنية

تطبق المواصفات والمعايير الفنية المنصوص عليها في هذا الملحق من قبل جهات التوثيق الإلكترونية في المملكة وفقاً لكل من أحكام قانون المعاملات الإلكترونية رقم (١٥) لسنة ٢٠١٥ و نظام ترخيص واعتماد جهات التوثيق الإلكتروني رقم (١١) لسنة ٢٠١٤ وتعديلاته والتعليمات الصادرة بموجب كل منها.

أولاً: منظومة التوثيق الإلكتروني

١. يتوجب على أي جهة تصدر شهادات التوثيق الإلكتروني أوتقدم الخدمات المتعلقة بها الالتزام بالمواصفات والمعايير الفنية التالية لدى تشغيلها منظومة التوثيق الإلكتروني الخاصة بها:

أ. أن تستند المنظومة إلى تقنية المفاتيح الجذريين العام والخاص والى المفتاح الجذري الخاص بها والصادر عن منظومة التوثيق الإلكتروني للشهادة الجذرية؛ ووفقاً للمواصفات والمعايير الفنية التالية:

١. أن تتوافق إدارة عمليات البنية التحتية للمفتاح العام (PKI) وإصدار شهادات التوثيق الإلكتروني مع المعيار الدولي المتعلق بهذا الخصوص (Recommendation ITU-T X.509)

٢. أن تعتمد المنظومة في جميع أعمالها بشكل عام على استخدام خوارزمية واحدة على الأقل لكل نوع من الخوارزميات المذكورة أدناه وعلى أن تتوافق مع المعيارين (ETSI TR 119 300, ETSI TS 119 312):

- Symmetric algorithms
- Asymmetric algorithms-minimum 1024 Bits
- Hash algorithms

ب. يجب أن يتوافر نظام لحفظ سجلات شهادات التوثيق الإلكتروني الصادرة عن جهة التوثيق الإلكتروني وإتاحتها للاطلاع إلكترونياً بصورة مستمرة طوال المدة المقررة في أي من مدونة الممارسات أو سياسة إصدار الشهادات على أن لا تقل عن ثلاث سنوات، وإتخاذ ما يلزم لحفظ هذه السجلات من التغيير.

(الملحق رقم ١)

ج. يجب أن يتوافر نظام يتيح ويبسر للهيئة التحقق من صحة بيانات إنشاء التوقيع الإلكتروني، وبخاصة في إطار أعمال الفحص والتحقق من جانب الهيئة.

ثانياً: مدونة الممارسات وسياسة إصدار الشهادات

٢. يجب أن تتضمن مدونة الممارسات كافة الآليات والإجراءات التي سيتم اتباعها وبشكل واضح للقيام بما يلي كحد أدنى:

- إدارة شهادات التوثيق الإلكتروني.
- إدارة المفاتيح الشفوية.
- إدارة الأعمال الداخلية.
- إدارة التأمين والكوارث.

٣. أن تتوافق الإجراءات والآليات أعلاه مع المعيارين (ETSI EN 319 401, ETSI EN 319 411).

٤. أن تتوافق مدونة الممارسات وسياسة إصدار الشهادات التي تعدها الجهة التي تصدر شهادات التوثيق الإلكتروني أوتقدم الخدمات المتعلقة بها مع كل من المعيارين (ETSI EN 319 401, ETSI EN 319 411) ومتطلبات الوثائق المرجعية التالية المنشورة على الموقع الإلكتروني للجهة المسؤولة عن إدارة منظومة التوثيق الجذرية بالمملكة:

- Certification Policy B2B Personnel & Server Certificate
- Certification Policy G2B&C
- Certification Practice Statement –PKI JO

ثالثاً: نظام رفض الشهادات

٥. يجب أن يتوافر لدى جهة التوثيق الإلكتروني نظام لإيقاف الشهادة الصادرة عنه وفقاً للمتطلب الفني (IETF RFC 5280) والمعايير الفنية (ETSI EN 319 401, ETSI EN 319 411).

٦. يجب أن يتوافر نظام لتحديد تاريخ ووقت إصدار شهادات التوثيق الإلكتروني، وإيقافها، وتعليقها، وإعادة تشغيلها، وإلغائها.

٧. يجب أن يتوفر موقع إلكتروني لنشر قائمة الشهادات الموقوفة أو الملغاة.

٨. يجب أن يتوافر نظام لإلغاء أو إيقاف شهادة التوثيق الإلكتروني يتضمن التحقق من صحة طلب الايقاف أو الالغاء.

(الملحق رقم ١)

رابعاً: أجهزة إنشاء التوقيع الإلكتروني

٩. يجب أن تكون الأجهزة المتوفرة من خلال جهة التوثيق الإلكتروني لمشاركتها لإنشاء التوقيع الإلكتروني والتحقق منه متوافقة مع المعيار
(FIPS 140-1 level 3 or higher) Security Evaluation ITSEC E4،
أو ما يماثلها من معايير مشابهة صادرة عن المنظمة العالمية للمعايير International Organization for Standardization.

١٠. أن يتم استخدام أداة أو أدوات أو أنظمة آمنة لإنشاء التوقيع الإلكتروني؛ بحيث تحتوي على شريحة إلكترونية تتضمن معالج إلكتروني وعناصر تخزين وبرمجيات تشغيل غير قابلة للمسح والاستنساخ ومحمية بكود سري، وتحتوي على عناصر متفردة للموقع وهي بيانات إنشاء التوقيع الإلكتروني وشهادة التوثيق الإلكتروني.

خامساً: الختم الزمني (Time Stamp)

١١. يجب على جهة التوثيق الإلكتروني في حال تقديمها لخدمة الختم الزمني أن يلتزم بالمعايير:
ETSI EN 319 421, ETSI EN 319 422

سادساً: سياسة الخصوصية والحماية

١٢. يجب أن يتوافر نظام تأمين للمعلومات وحماية البيانات وخصوصيتها لدى جهة التوثيق الإلكتروني بمستوى حماية لا يقل عن المستوى المذكور في المعايير والقواعد الآتية:

- General security management codes of practice, such as ISO 27001 and,
- (ETSI EN 3017 401) or equivalent standard.

١٣. يجب أن يتوافر سياسة لدى جهة التوثيق الإلكتروني للحفاظ على الأمن والسرية والخصوصية في تقديمها لخدماتها.