ملحق (١): المواصفات والمعايير الفنية

تطبق المواصفات والمعايير الفنية المنصوص عليها في هذا الملحق من قبل جهات التوثيق الإلكتروني في المملكة وفقا لكل من أحكام قانون المعاملات الالكتروني الأردني و نظام ترخيص واعتماد جهات التوثيق الالكتروني وتعديلاته والتعليمات الصادرة بموجبه.

أولا: منظومة التوثيق الالكتروني PKI

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

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

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

٢. أن تعتمد المنظومة في جميع اعمالها بشكل عام على استخدام خوارزمية واحدة على الأقل لكل نوع من الخوارزميات المذكورة أدناه وعلى أن تتوافق مع المعيارين (ETSI TR 199 300, ETSI TS 119 312):

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

٢. 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 اصدار الشهادات على أن لا تقل عن ثلاث سنوات.

٣. يجب أن يتوافر نظام يتيح وييسر للهيئة التحقق من صحة بيانات إنشاء التوقيع الالكتروني, وبخاصة في إطار أعمال الفحص والتحقق من جانب الهيئة.

ثانيا: مدونة الممارسات وسياسة اصدار الشهادات

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

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

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

٥. أن تتوافق مدونة الممارسات وسياسة إصدار الشهادات التي تعدها الجهة التي تصدر شهادات التوثيق الإلكتروني أوتقدم الخدمات المتعلقة بها مع كل من المعيارين (ETSI 319 401, ETSI 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 Practice Statement –PKI Jo

ثالثا: نظام رفض الشهادات

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

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

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

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

رابعا: أجهزة إنشاء التوقيع الالكتروني

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

١١. أن يتم استخدام أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني آمنة تحتوي على شريحة إلكترونية تتضمن معالج إلكتروني وعناصر تخزين وبرمجيات تشغيل بحيث تكون غير قابلة للاستنساخ ومحمية بكود سري، تحتوي على عناصر متفردة للموقّع وهي بيانات إنشاء التوقيع الإلكتروني وشهادة التوثيق الإلكتروني.

خامسا: البصمة الزمنية

١٢. يجب على جهة التوثيق الإلكتروني في حال تقديمها لخدمة البصمة الرقمية أن يلتزم بالمعايير: EN 319 421, EN 319 422

سادسا: سياسة الخصوصية والحماية

١٣. يجب أن يتوافر نظام تأمين للمعلومات وحماية البيانات وخصوصيتها لدى جهة التوثيق الالكتروني 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.

١٤. يجب أن يتوافر سياسة لدى جهة التوثيق الالكتروني للحفاظ على السرية الخصوصية في تقديمها لخدماتها.