ملحق H: الضوابط الفنية

١. سلطة التصديق

١-١. سياسة الشهادة وبيان ممارسة التصديق:

أ. على كل سلطة تصديق CA أن تعتمد سياسة الشهادة CP، وبيان ممارسة التصديق CPS الخاصة بها.

ب. أي تغيير في سياسة الشهادة وبيان ممارسة التصديق يجب أن يعرض على الهيئة للحصول على موافقتها قبل توقيع أي شهادات بموجب السياسة الجديدة، وفي حال وجود ترميز OID للسياسة يجب تغييره.

ج. كل سياسة شهادة وبيان ممارسة التصديق يتم بناءً عليها إصدار شهادات صالحة يجب أن يكون منشور ومتاح للجميع.

د. يجب إعداد سياسة شهادة وبيان ممارسة التصديق وفق المعيار RFC 3647.

١-٢. نظام سلطة التصديق:

أ. يجب أن يكون مخدم سلطة التصديق (والذي يستخدم لتوقيع الشهادات) جهاز مخصص لهذا الغرض فقط، بحيث لا يشغّل أي خدمات أخرى إلا تلك اللازمة لعمليات التوقيع.

ب. يجب أن تكون منظومة التجهيزات والبرمجيات المستخدمة في سلطة التصديق موجودة في بيئة آمنة حيث يكون الوصول فيه متحكم به حسب الأدوار، ومقتصر على أفراد مدربين ومحددين.

ج. يجب على منظومة التجهيزات والبرمجيات المستخدمة في سلطة التصديق، ووحدة أمن التجهيزات HSM أن تحقق على الأقل المعيار FIPS 140-2 من المستوى ٣ أو ما يعادلها.

د. يجب توثيق البيئة الآمنة والحصول على موافقة الهيئة عليها، وأن تكون هذه الوثائق ونتائج تدقيق واختبار البيئة إن وجدت متاحة لفريق الزيارة.

١-٣. مفتاح سلطة التصديق:

أ. يجب أن يكون الحد الأدنى لطول المفتاح الخاص بسلطة التصديق ٤٠٩٦ بت عند استخدام خوارزمية RSA أو طول مفتاح مكافئ له عند استخدام خوارزميات أخرى. (وبما يتوافق مع سياسة التشفير الوطنية).

ب. يجب إعداد مفتاح سلطة التصديق للاستخدام على المدى الطويل (بصلاحية من ٥ لـ ٧ أعوام مثلاً).

ج. ينبغي على بيئة عمل سلطة التصديق أن تتيح سجل (يجب أن يكون محمي ضد العبث) لكل الشهادات المصدرة وقوائم الشهادات الملغية الموقعة CRLs.

د. عند الحاجة لتغيير مفاتيح التشفير الخاصة بسلطة التصديق، يجب إدارة هذا التغيير بحيث يكون إصدار الشهادات يتم باستخدام المفاتيح الجديدة فقط، اعتباراً من وقت توزيعها.

هـ. يجب أن تعادل فترة التداخل بين المفاتيح القديمة والجديدة لأي سلطة تصديق على الأقل أطول مدة صلاحية ممنوحة للمشترك النهائي.

١-٤. إلغاء شهادة:

أ. يمكن تقديم طلب إلغاء الشهادة من قبل المشترك النهائي، وسلطات التسجيل RA، وسلطة التصديق. كما يمكن للآخرين طلب الإلغاء إذا تمكنوا من إثبات وجود اختراق أو كشف للمفتاح الخاص المرتبط.

ب. يجب أن تستجيب سلطة التصديق لأي طلب إلغاء وارد وفق ما هو وارد في لائحة الضوابط والنواظم (فقرة 4-1 واجبات المزود) وبما يتوافق مع سياسة الشهادة وبيان ممارسة التصديق المعتمدة.

ج. يجب التحقق من صلاحية وموثوقية طلبات الإلغاء بشكل صحيح.

١-٥. قائمة الشهادات الملغية:

أ. يجب على كل سلطة التصديق، إنشاء ونشر قائمة الشهادات الملغية.

ب. يجب على كل سلطة تصديق إصدار قائمة جديدة بالشهادات الملغية مباشرة بعد أي عملية إلغاء لشهادة.

ج. بمجرد إصدار قائمة الشهادات الملغية، يجب أن يتم نشرها في مستودع الشهادات المعتمد والذي يمكن الوصول إليه عبر الشبكة.

د. يجب أن تتوافق قائمة الشهادات الملغية مع المعيار RFC5280.

١-٦. سجلات المحفوظات:

أ. يجب على كل سلطة تصديق، تسجيل وأرشفة جميع طلبات الحصول على الشهادات، إلى جانب جميع الشهادات الصادرة، وجميع طلبات الإلغاء، وجميع قوائم الشهادات الملغية، ومعلومات تسجيل الدخول والخروج وإعادة التشغيل للمخدم المستخدم لإصدار الشهادات.

ب. يجب أن تكون هذه السجلات متاحة للتدقيق عند الحاجة.

١-٧. التدقيق:

أ. يجب على كل سلطة تصديق إجراء تدقيق تشغيلي على موظفي سلطات التسجيل/التصديق مرة واحدة على الأقل كل عام.

١-٨. النشر ومسؤوليات مستودع الشهادات:

أ. يجب أن يكون مستودع الشهادات متاح على أساس أفضل جهد ممكن، مع نية أن يكون متوفر على مدار ٧/٢٤.

ب. يجب على كل سلطة تصديق فرعية أن تنشر لمشتركيها، وللأطراف المعتمدين، مايلي:

١. شهادة الجذر لسلطة التصديق الفرعية أو مجموعة من شهادات الجذر وصولاً إلى الشهادة الجذر لسلطة التصديق الوطنية.

٢. عنوان https للوصول لشهادة سلطة التصديق بتنسيقPEM .

٣. عنوان https للوصول لقائمة الشهادات الملغية بتنسيق PEM و DER.

٤. عنوان https لصفحة الويب الخاصة بسلطة التصديق للحصول على معلومات عامة عنه.

٥. وثائق السياسات (سياسة الشهادة وبيان ممارسة التصديق) وأي وثائق أخرى مرتبطة.

٦. رابط لنظام الشكاوى ورعاية الزبائن والدعم الفني.

٧. رابط الاتصال بالمزود، والذي يحتوي على عناوين الموقع الجغرافي وعنوان بريد إلكتروني وأرقام هواتف، إلخ.

١-٩. ضوابط سلطة التصديق:

أ. يجب أن تكون جميع التجهيزات والبرامج المستخدمة مستضافة في مركز معطيات آمن ضمن أراضي الجمهورية العربية السورية حصراً.

ب. يقتصر الوصول المنطقي والفيزيائي إلى أنظمة وبيانات سلطة التصديق على أفراد مخولين ومدربين بشكل جيد.

ج. يجب الحفاظ على استمرارية عمليات إدارة المفاتيح والشهادات.

د. تتم عمليات تطوير وصيانة وتشغيل أنظمة سلطة التصديق بتصاريح مدروسة وموثوقة، وغاية تنفيذها الحفاظ على سلامة أنظمة سلطة التصديق.

١-١٠. سلامة الخدمة:

أ. تفرض سلطة التصديق ضوابط فعالة لتضمن بشكل كافي ما يلي:

١. ضمان سلامة وحماية المفاتيح والشهادات التي يديرها طوال دورة حياتها.

٢. ضمان صحة معلومات المشترك (دور موظف سلطة التسجيل).

١-١١. الخصوصية والسرية:

أ. يجب على سلطة التصديق المعتمدة تعريف سياسة الخصوصية وكشف البيانات التي ستعتمدها بحيث تتوافق مع القوانين والتشريعات ذات الصلة.

ب. عند التحقق من بيانات المشترك، فإن سلطة التصديق هي الجهة المسؤولة عن تسجيل وحفظ مايكفي من البيانات المتعلقة بالمشترك للتعرف عليه بشكل كافي، ولا يحق لسلطة التصديق الإفصاح عن هذه المعلومات لأي جهة كانت ما لم تطلب بشكل رسمي ووفق القوانين والتشريعات الناظمة.

١-١٢. المخاطر والتعافي من المخاطر:

يجب أن يكون لدى سلطة التصديق إجراء مناسب لاستعادة القدرة على العمل بعد الكوارث، ويجب عدم الكشف عن هذا الإجراء في سياسة الشهادة أو بيان ممارسة التصديق

٢. سلطة التسجيل

٢-١. تعريف الكيانات:

أ. يجب على سلطة التصديق تحديد دور سلطة التسجيل، وتكون هذه الأخيرة مسؤولة عن التحقق من هوية المستخدم النهائي وفق سياسة التعريف والتحقق.

ب. لكي تتمكن سلطة التسجيل من التحقق من هوية شخص ما، يجب على الشخص المعني التواصل مع سلطة التسجيل وجهاً لوجه، وإبراز معرف معتمد يحوي الصورة الشخصية (هوية أو جواز سفر) و/أو مستندات رسمية أخرى صالحة والتي تأكد أنه مستوفٍ لشروط الاشتراك حسب سياسة الشهادة وبيان ممارسة التصديق.

ج. في حال كان طلب الحصول على شهادة بشكل غير شخصي (عبر ممثل/وكيل/مفوض)، يجب على سلطة التسجيل التحقق من صحة هوية وأهلية الشخص المفوض باستخدام طريقة مناسبة موثوقة.

د. عند طلب شهادة لمخدم أو خدمة، يجب أن تضمن سلطة التسجيل أن يكون مقدم الطلب مخولًا بشكل مناسب من قِبل مالك المخدم أو الخدمة، لأن يستخدم الاسم/المعرف (FQDN) المقترن في الشهادة، وفي حال كان الاسم المعرف FQDN هو نطاق أسماء، يجب أن تضمن سلطة التسجيل التحقق من عائدية نطاق الأسماء للجهة الطالبة.

هـ. يجب على سلطة التسجيل التحقق من صحة طلب توقيع الشهادة CSR.

و. يجب أن تحتفظ سلطتي التصديق والتسجيل بالثبوتيات اللازمة لإثبات المطابقة (مشترك/شهادة)، وفي جميع الأحوال فإن طلب الحصول على الشهادة يجب أن يخضع لإجراءات التحقق من الهوية.

ز. يجب أن توفر سلطة التصديق وسيلة للتحقق من سلامة الشهادة الجذر (مصدر الثقة) الخاص بها.

٢-٢. تفرد الأسماء:

يجب أن يرتبط حقل الموضوع Subject (DN) في أي شهادة رقمية بكيان واحد فقط طوال فترة صلاحية الشهادة الجذر لسلطة التصديق.

٢-٣. شهادات المشترك النهائي والمفاتيح:

أ. يجب مراعاة سياسة التشفير الوطنية عند اختيار الخوارزميات، وأطوال المفاتيح لشهادات المستخدم النهائي (شخص طبيعي – مخدم – اسم نطاق).

ب. يمنع مشاركة شهادات المشترك.

ج. تصدر السلطة شهادات X.509 v3 إلى المشتركيين النهائيين اعتماداً على مفاتيح تم إنشاؤها بواسطة مقدم الطلب، أو إلى مفاتيح يتم توليدها وحفظها بواسطة مقدم الطلب على أجهزة مخصصة (الحامل الإلكتروني).

د. يجب على كل سلطة تصديق أن تبذل ما يكفي من جهود للتأكد من أن المشتركين مدركين لمدى ضرورة حماية بياناتهم الخاصة بالشكل الصحيح.

هـ. يجب التأكد بأن كافة الاسماء/العناوين ضمن حقلي subject و subjectAltName في كل شهادة مملوكة أو تابعة للمشترك النهائي.

و. يجب أن تعرف سياسة الشهادة وبيان ممارسة التصديق، كم مرة يمكن تجديد الشهادة (نفس المفاتيح أو بمفاتيح جديدة) ومتى يجب إعادة التأكد من هوية المشترك بشكل شخصي.