السلطة القومية للمصادقة الالكترونية

البنية التحتية القومية للمفاتيح العمومية لدولة السودان
سلطة الجذر القومية للشهادات الرقمية
سياسة الشهادات الرقمية

معلومات عن الوثيقة

الجهة	السلطة القومية للمصادقة الالكترونية
الوحدة	سلطة الجذر للشهادات الرقمية
عنوان الوثيقة	سياسة الشهادات الرقمية
رقم الإصدار	v.0
تاريخ الإصدار	201/y/x
حالة الوثيقة	مسودة

سجل الإصدارات السابقة للوثيقة

رقم الإصدار	المؤلف/المؤلفون	التاريخ	الأنشطة
0.1	فريق سياسة الشهادات الرقمية - مركز النيل للأبحاث التقنية	2015/9/22	إنشاء الوثيقة
0.2	فريق سياسة الشهادات الرقمية - مركز النيل للأبحاث التقنية	2015/10/1	إدراج ملاحظات عند مراجعة الوثيقة
0.3	فريق سياسة الشهادات الرقمية - مركز النيل للأبحاث التقنية	2015/10/13	• فصل مسئولية مدير سلطة الشهادات الرقمية من بين الأدوار الأخرى الموثوق بها • إضافة ضابط أمن النظام لقائمة الأدوار الموثوقة
0.4	فريق سياسة الشهادات الرقمية - مركز النيل للأبحاث التقنية	2015/11/10	• تغييرات في وصف الشهادة وفترة صلاحية المفتاح الخصوصي
0.5	فريق سياسة الشهادات الرقمية - مركز النيل للأبحاث التقنية	2015/12/29	• إدراج ملاحظات من الوكالة الوطنية للمصادقة الإلكترونية لدولة تونس
0.6	فريق سياسة الشهادات الرقمية - مركز النيل للأبحاث التقنية	2016/2/18	• إدراج تعديلات للوثيقة بعد ترجمتها للغة العربية
0.7	فريق سياسة الشهادات الرقمية - مركز النيل للأبحاث التقنية	2018/5/1	• إدراج ملاحظات السلطة القومية للمصادقة الالكترونية النهائيه

فهرس المحتويات

1. مقدمة

1.1 نظرة عامة

نسبة لتزايد إنتشار إستخدام المعاملات الإلكترونية في السودان، ازدادت الحوجة لتشريع القوانين التي تحكم هذه المعاملات. وبناء على ذلك، ظهرت هنالك حاجة ملحة لأن توفر هذه المعاملات الخدمات التأمينية المناسبة مثل التحقق من صحة الهوية، السرية، وتكاملية البيانات (صحة/ سلامة البيانات) وعدم التنصل من إجراء هذه المعاملات. جميع الخدمات التأمينية السابقة تتطلب إستخدام ازواج من المفاتيح الإلكترونية و من اجل اضفاء الموثوقية على تلك المفاتيح توجب الامر بنية تحتية للمفاتيح العمومية و ذلك لتوفير المفاتيح العمومية عن طريق اصدار شهادات رقمية موثقة من قِبل جهات موثوقة لدى الجهات المعوّلة على إستخدام المفاتيح العمومية.

البنية التحتية للمفاتيح العمومية هي مجموعة من المعدات والبرامجيات، والأفراد، والسياسات، والإجراءات اللازمة لإنشاء، وإدارة، وتوزيع، وإستخدام، وتخزين، وإلغاء الشهادات الرقمية وإدارة التشفير غير المتناظر.

أما الشهادة الرقمية (لأغراض هذه الوثيقة سيتم تسميتها بالشهادة فقط) فهي وثيقة إلكترونية تصدرها سلطة التصديق الرقمية تقر بأن الجهة/ الشخص المدوّن اسمه في هذه الشهادة هو المالك الفعلي للمفتاح العمومي المضمّن في الشهادة، وأنه المالك الفعلي للمفتاح الخصوصي المقابل له.

الغاية الأساسية من البنية التحتية للمفاتيح العمومية هو إنشاء محيط للثقة في المعاملات الإلكترونية، و بذلك تسهيل النقل الإلكتروني الآمن للمعلومات، على سبيل المثال، تأمين المعاملات المصرفية عبر الانترنت أو إستخدام البريد الإلكتروني بطريقة آمنة. وتعتبر البنية التحتية للمفاتيح العمومية إحدى ركائز التداول الالكتروني والتي على أساسها تقوم الحكومة الإلكترونية و التجارة الإلكترونية و اللذان قد يساهمان مساهمة فعالّة في التنمية المستدامة للبلاد.

لذلك يتحتم وضع إطار قانوني لهذه المعاملات الإلكترونية ليحدد الضوابط الإدارية والتشغيلية و الفنية لها.
وفي مسعى لتحقيق هذه الحوجة، شرّع البرلمان قانون المعاملات الإلكترونية ليحكم و ينظّم المعاملات الإلكترونية في جميع أنحاء البلاد.
وبموجب هذا القانون تم الاتي:

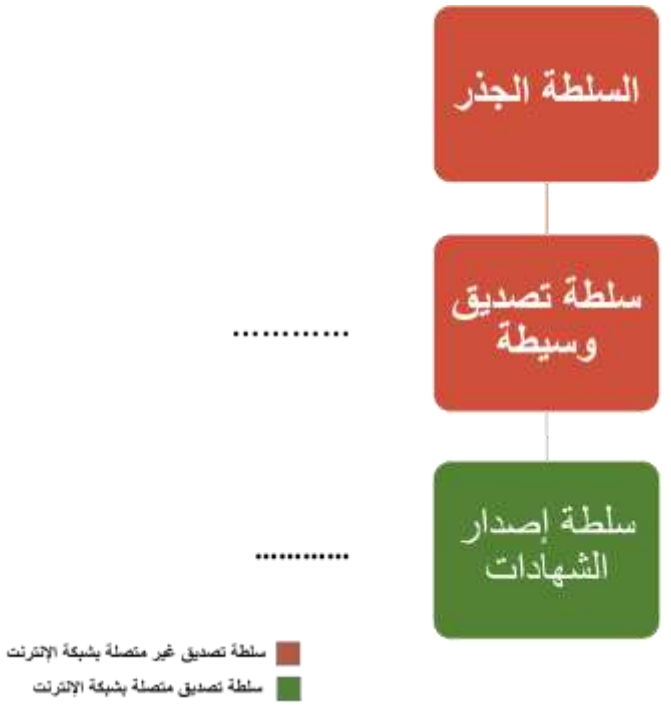
- تأسيس السلطة القومية للمصادقة الإلكترونية لتمثل الجهة القومية في السودان المنظّمة للبنية التحتية للمفاتيح العمومية
- تأسيس سلطة الجذر القومية للشهادات الرقمية (سلطة الجذر) لتكون بمثابة سلطة جذر الثقة (أعلى سلطة للشهادات الرقمية) في التسلسل الهرمي للبنية التحتية القومية للمفاتيح العمومية في السودان، و لإنشاء أي تصديق متبادل مع سلطات شهادات خارجية، سلطة الجذر تملكها و تحكمها السلطة القومية للمصادقة الإلكترونية.

نظام العمل للبنية التحتية القومية للمفاتيح العمومية في السودان هو مركزي ومفتوح، بمعنى أنه يوجد مركز ثقة جذري (رئيسي) واحد و أي جهة أخرى يمكن أن تعوّل على المعلومات الواردة في الشهادة الصادرة من احدى سلطات التصديق المصدقة من سلطة الجذر. ولأغراض هذه الوثيقة سيتم تسمية هذه الجهة بالطرف المعوّل. نموذج الثقة يتكون من ثلاث مستويات لسلطات التصديق الرقمية بحيث اثنين منهما يمثلان سلطات شهادات غير متصلة بشبكة الإنترنت وذلك لزيادة أمن النظام. هذا النموذج موضح في الرسم التوضيحي 1.

سلطة الجذر هي جهة الثقة الأصل في هذا النموذج. هي تُصدر و تُدير الشهادات لسلطات التصديق الوسيطة (السلطات الوسيطة). السلطة الوسيطة هي سلطة فرعية من السلطة الجذر تصدر شهادات توقيع رقمي للسلطات الفرعية التابعة لها لكي تمثّل بدورها سلطات إصدار شهادات رقمية لمختلف القطاعات.

سلطة إصدار الشهادات هي سلطة فرعية تابعة للسلطة الوسيطة، تُقدّم شهادات رقمية للمؤوسسات، والأجهزة و الأفراد حسب القطاع الذي تنتمي إليه.

هذه الوثيقة هي سياسة الشهادات الرقمية (سياسة الشهادات) لسلطة الجذر القومية للشهادات الرقمية (سلطة الجذر) لدولة السودان، وهي تعرّف المتطلبات والسياسات المطبّقة لدى سلطة الجذر. وهي مُعتمدة من قِبل السلطة القومية للمصادقة الإلكترونية، حيث أنها هي الجهة المسئولة عن اختيار، تحديث، وإعتماد سياسة الشهادات لسلطة الجذر.



رسم توضيحي1 نموذج الثقة للبنية التحتية للمفاتيح العمومية لدولة السودان

1.2 تعريف بالوثيقة و اسمها

عنوان الوثيقة هو سياسة الشهادات الرقمية لسلطة الجذر القومية للشهادات الرقمية في السودان، إختصارا: سياسة الشهادات لسلطة الجذر، رقم الإصدار 0.7، هذه الإصدارة مُعتمدة و سارية المفعول إعتبارا من التاريخ : 2017.

أي نسخة لسياسة الشهادات لسلطة الجذر سابقة لهذه الإصداره تُعتبر ملغية.

معرّف الكيان لهذه الوثيقة هو 2.16.729.1.1.1.1.1 تفسير هذا المعرّف موضح في الجدول التالي.

الرقم	الوصف
2	منطقة التقييس الموحد لـ ISO/IEC (منظمة المعايير الدولية/ اللجنة الكهروتقنية الدولية) و ITU-T (الاتحاد الدولي للاتصالات - قطاع تقييس الاتصالات)
16	تسجيل إشتراك (ISO/IEC و ITU_T) داخل الدولة
729	الرقم المخصص لدولة السودان
1	الرقم المخصص لتصنيف المؤسسة. هي مؤسسة حكومية – عامة
1	الرقم المخصص للسلطة القومية للمصادقة الإلكترونية
1	الرقم المخصص لسطة الجذر القومية
1	الرقم المخصص لسياسة الشهادات
2	الرقم المخصص لرقم إصدار هذه الوثيقة

1.3 المشاركون في البنية التحتية للمفاتيح العمومية

1.3.1 السلطة القومية للمصادقة الإلكترونية

بناء على مخرجات قانون المعاملات الإلكترونية لعام 2007 و التعديلات في القانون للعام 2015، تم تأسيس السلطة القومية للمصادقة الإلكترونية لتُنظّم وتحكم البنية التحتية القومية للمفاتيح العمومية في دولة السودان. ستعمل السلطة القومية للمصادقة الإلكترونية على تحديد متطلبات العمل والسياسات المطبّقة لدى سلطة الجذر و السلطات الوسيطة.

المسئوليات الرئيسية للسلطة القومية للمصادقة الإلكترونية تشمل ولكن لا تقتصر على ما يلي:

- إختيار أو تطوير سياسات الشهادة الرقمية والإتفاقيات الداعمة المستخدمة لدى سلطة الجذر
- إعتماد أي تصديق متبادل لسلطة الجذر أو إتفاقية عمل مشترك لها مع جهات خارجية
- إعتماد الممارسات التي يجب على سلطة الجذر أن تتبعها، وذلك بمراجعة ممارسات تصديق الشهادات لضمان توافقها مع سياسة الشهادات المقابلة
- إصدار شهادة رقمية لسلطة الجذر، و ذلك بعد التحقق من صحة المعلومات التي ستذكر في الشهادة
- إلغاء، وتعليق، وتغيير مفاتيح شهادة سلطة الجذر.

1.3.2 سلطة الجذر القومية للشهادات

سلطة الجذر للشهادات الرقمية (سلطة الجذر) هي سلطة الثقة الأساسية للبنية التحتية القومية للمفاتيح العمومية لدولة السودان. و تعود ملكية سلطة الجذر إلى السلطة القومية للمصادقة الإلكترونية. سلطة الجذر تصدر شهادات فقط للسلطات الوسيطة بعد إعتمادها من السلطة القومية للمصادقة الإلكترونية. لن تُصدر سلطة الجذر أي شهادات لمستخدمين أفراد.

الإلتزامات الرئيسية لسلطة الجذر كالاتي:

- تطوير و متابعة ممارسات تصديق الشهادات والتأكد من توافقها مع سياسة الشهادات والمتطلبات الأخرى للسلطة القومية للمصادقة الإلكترونية
- توليد زوج مفاتيح سلطة الجذر وإصدار شهادتها الموقعة ذاتيا
- تنفيذ وتشغيل سلطة الجذر وفقا لهذه السياسة و مايقابلها من الممارسات الفعلية لإصدار الشهادات
- إصدار، ونشر، وإدارة شهادات السلطات الوسيطة

سلطة الجذر هي سلطة شهادات غير متصلة بشبكة الإنترنت.

1.3.3السلطة الوسيطة للشهادات الرقمية

تم تصميم البنية التحتية للمفاتيح العمومية في السودان بحيث تُقدّم خدمات تصديق الشهادات الرقمية لمختلف التطبيقات في شتى القطاعات. السلطة الوسيطة للشهادات (السلطة الوسيطة) هي جهة مُعتمدة مُوافق عليها من قِبل السلطة القومية للمصادقة الإلكترونية لتصبح سلطة الثقة والسياسات لتطبيقات البنية التحتية للمفاتيح العمومية في قطاع بعينه

المفاتيح العمومية للسلطات الوسيطة يجب أن يتم تصديقها فقط من خلال سلطة الجذر. جميع المشغلين للسلطات الوسيطة يجب أن يتم تحديدهم بواسطة السلطة القومية للمصادقة الإلكترونية. جميع السلطات الوسيطة هي سلطات شهادات غير متصلة بشبكة الإنترنت.

المشتركون لسلطة الجذر هم فقط السلطات الوسيطة.

1.3.4 الأطراف المعوّلة

الطرف المعوّل هو فرد و/ أو مؤسسة تعوّل (تعتمد) على الشهادة الرقمية لإستخدام المفتاح العمومي المضمّن في تلك الشهادة. الطرف المعوّل هو المسئول عن تحديد كيفية التحقق من صحة الشهادة.

1.3.5 السلطة الإدارية للشهادات

السلطة الإدارية للشهادات (السلطة الإدارية) هي سلطة إصدار شهادات لإدارة الشهادات ذات العلاقة بتشغيل سلطة الجذر. مثال ذلك الشهادات المتعلقة بهويات الموظفين و وصولهم للمرافق المختلفة و شبكة الإتصالات الداخلية. السلطة القومية للمصادقة الإلكترونية هي المسئولة عن إدارة هذه السلطة.
السلطة الإدارية تصدر الشهادات الرقمية للإستخدامات التالية:

- **شهادة موثوقية (تحقق من هوية) المستخدم**: للتحقق من هوية المستخدم عند الوصول للمرافق أو إستخدام خدمات معينة ضمن أنظمة سلطة الجذر والسلطات الوسيطة
- **شهادة موثوقية نظام**: هي شهادة رقمية تستخدمها أنظمة سلطة الجذر والسلطات الوسيطة لأغراض التحقق من الهوية وإنشاء إتصالات آمنة. على سبيل المثال، الشهادات المستخدمة في خوادم وأجهزة الشبكة
- **شهادة توقيع رقمي**: هي شهادة رقمية تستخدمها سلطة الجذر والسلطات الوسيطة للتحقق من توقيع رقمي لمحتويات رقمية بخلاف شهادات السلطات الوسيطة و معلومات حالة الشهادات.على سبيل المثال، هذه الشهادات يمكن أن تُستخدم للتوثّق من بيانات أرشيف سلطة الجذر ووثائق تقديم طلبات الشهادات
- **شهادة سرية البيانات**: هي شهادة رقمية تستخدمها سلطة الجذر والسلطات الوسيطة لتشفير المفاتيح المتناظرة.

1.3.6 المشاركون الآخرين

لا يوجد أي مشاركون آخرين.

1.4 إستخدام الشهادة

1.4.1 الإستخدامات الملائمة للشهادة

تصدر سلطة الجذر شهادات للإستخدامات التالية:

- **شهادة موقعة ذاتياً** هي الشهادة الجذر للبنية التحتية للمفاتيح العمومية في السودان، والتي يتم إستخدامها للتحقق من صحة شهادات السلطات الوسيطة و حالة تلك الشهادات
- **شهادة توقيع رقمي للسلطة الوسيطة**: هي شهادة تستخدمها الأطراف المعوّلة للتحقق من صحة شهادات سلطات إصدار الشهادات التابعة للسلطات الوسيطة.

1.4.2 الإستخدامات المحظورة للشهادة

يُحظر أي إستخدام لشهادة رقمية صادرة بموجب هذه السياسة لأغراض أخرى غير ما تم تحديده في البند 1.4.1.

1.5 إدارة سياسة الشهادات

1.5,1 جهة إدارة الوثيقة

سياسة الشهادات لسلطة الجذر ستتولى إدارتها السلطة القومية للمصادقة الإلكترونية.

1.5,2 جهة الإتصال

أي إستفسارات، أو إقتراحات، أو ملاحظات بشأن هذه الوثيقة – سياسة الشهادات الرقمية – تُرسل إلى السلطة القومية للمصادقة الإلكترونية على العنوان التالي:

رئيس السلطة القومية للمصادقة الإلكترونية

العنوان :السلطة القومية للمصادقة الإلكترونية

البريد الإلكتروني:

الهاتف: 294+

1.5.3 المسئول عن ملائمة ممارسات تصديق الشهادات لهذه السياسة

السلطة القومية للمصادقة الإلكترونية هي الجهة المسؤولة عن تحديد مدى ملائمة ممارسات تصديق الشهادات للسلطة الجذر وتوافقها مع سياسة الشهادات هذه.

1.5.4 إجراءات إعتماد ممارسات تصديق الشهادات

أي إنشاء أو تعديل لسياسة الشهادات ومايقابلها من ممارسات تصديق الشهادات يتم إعتمادها من السلطة القومية للمصادقة الإلكترونية، الإعتماد بالموافقة يجب أن يكون متوافق مع قانون المعاملات الإلكترونية لدولة السودان لعام 2007 و التعديلات في القانون للعام 2015، ومع أي قوانين أخرى معمول بها.

1.6 التعريفات و الإختصارات

1.6.1 التعريفات

المصطلح	التعريف
بيانات التفعيل	هي بيانات، بخلاف مفاتيح التشفير، يتطلّب إستخدامها لتشغيل وحدات التشفير والتي تحتاج إلى حماية (على سبيل المثال، رقم التعريف الشخصي، كلمة المرور، أو مفتاح يدوي مشترك)
مقدم الطلب	الجهة الذي يتقدم بطلب شهادة رقمية
شهادة رقمية	وثيقة إلكترونية تستخدم التوقيع الرقمي لربط المفتاح العمومي مع هوية الجهة صاحبة الشهادة
سياسة الشهادات الرقمية	مجموعة مسماة من القواعد التي تشير إلى تطبيق شهادة رقمية لمجتمع معين و/ أو فئة من التطبيقات مع متطلبات التأمين المشتركة
ممارسات تصديق الشهادات	هي الممارسات التي تنفذها سلطة التصديق الرقمية في إصدار وإدارة، وإلغاء، وتجديد أو تغيير مفاتيح الشهادات الرقمية
تجديد الشهادة	تجديد الشهادة يعني إصدار شهادة جديدة للمشترك دون تغيير المفتاح العمومي للمشترك أو للمشاركين الآخرين أو أية معلومات أخرى في الشهادة.
تعديل الشهادة	تعديل الشهادة يعني إصدار شهادة جديدة للمشترك مع تغيير معلومات في الشهادة بخلاف المفتاح العمومي.
تغيير مفاتيح الشهادة	تغيير مفاتيح الشهادة يعني إصدار شهادة جديدة للمشترك بمفتاح عمومي مختلف، في حين أن تبقى معلومات المشترك الآخرى دون أي تغيير.
تحديد الهوية	عملية تحديد هوية الفرد أو المؤسسة، أي لإثبات أن الفرد أو المؤسسة هو الفرد أو المؤسسة التي تتدعي الهوية
زوج مفاتيح	هما المفتاح الخصوصي و المفتاح العمومي المقابل له
مجيب بروتوكول التحقق المباشر	هو تطبيق متصل بالإنترنت بحيث أنه يتصل بمستودع سلطة التصديق الرقمية وذلك لمعالجة طلبات حالة الشهادة وفقا لوصف بروتوكول التحقق المباشر من حالة الشهادة في طلب التعليقات

من حالة الشهادة	المعمول بها
مشارك	فرد أو مؤسسة يلعب دوراً ضمن البنية التحتية للمفاتيح العمومية المعطاة، وهو أحد الأدوار التالية: مشترك، أو طرف معوّل، أو سلطة شهادات، أو سلطة تسجيل، أو مزود خدمات المستودع أو جهة مماثلة
المفتاح الخصوصي	هو أحد زوج المفاتيح و الذي يتم الإحتفاظ به سرا من قِبل صاحب زوج المفاتيح، وذلك لإستخدامه في إنشاء التوقيعات الرقمية و/ أو فك تشفير محتويات وثائق أو ملفات إلكترونية و التي قد تم تشفيرها بإستخدام المفتاح العمومي المقابل له
المفتاح العمومي	أحد زوج المفاتيح الذي قد يتم الكشف عنه علنا من قِبل صاحب المفتاح الخصوصي المقابل له، والذي يتم إستخدامه من قِبل الطرف المعوّل للتحقق من التواقيع الرقمية التي قد تم إنشاؤها باستخدام المفتاح الخصوصي المقابل له، و/ أو لتشفير الرسائل بحيث يمكن فك تشفيرها فقط بإستخدام المفتاح الخصوصي المقابل له
الطرف المعوّل	الجهة التي تعوّل (تعتمد) على المعلومات الواردة في الشهادة الرقمية
مدة المهلة لحين طلب الإلغاء	مدة المهلة لحين طلب الإلغاء هو الزمن المتاح للمشترك الذي يجب عليه خلاله تقديم طلب الإلغاء، وذلك بعد أن يتم تحديد سبب واحد على الأقل للإلغاء.
صاحب الشهادة	هو الفرد، أو العملية، أو المؤسسة أو الجهاز الوارد (المذكور) اسمه في الشهادة كمشترك
المشترك	هو الجهة المعّرفه بأنه صاحب الشهادة في الشهادة الرقمية
إتفاقية المشترك	إتفاق بين المشترك من جهة وسلطة التصديق الرقمية أو سلطة التسجيل من الجهة الأخرى. ويركز الإتفاق المشترك على مسئوليات المشترك والشروط والأحكام التي على أساسها يجوز له أن يستخدم شهادته الرقمية
التحقق من صحة الهوية	عملية تحديد هوية مقدمي طلبات الشهادة. "التحقق من الهوية" هي مجموعة فرعية من "تحديد الهوية"، ويشير إلى تحديد الهوية في سياق تحديد هوية المتقدمين لطلب الشهادة الرقمية
X.509	هو معيار الإتحاد الدولي للإتصالات – قطاع تقييس الإتصالات (ITU-T) للشهادات الرقمية وإطار الموثوقية المقابلة لها.

1.6,2 الإختصارات

الإختصار	الاسم بالكامل	معناه بالعربي
CA	Certificate Authority	سلطة التصديق الرقمية
CP	Certificate Policy	سياسة الشهادات الرقمية
CPS	Certification Practice Statement	ممارسات تصديق الشهادات
CRL	Certificate Revocation List	قائمة الشهادات الملغاة
CSR	Certificate Signing Request	طلب توقيع الشهادة
DN	Distinguished Name	الاسم المميَّز
DSA	Digital Signature Algorithm	خوارزمية التوقيع الرقمي

ECDSA	Elliptic Curve Digital Signature Algorithm	خوارزمية التوقيع الرقمي بالمنحنيات الإهليلجية
FIPS	Federal Information Processing Standards	المعايير الإتحادية لمعالجة المعلومات
HSM	Hardware Security Module	وحدة التأمين المادية
OID	Object Identifier	معرف الكيان
PIN	Personal Identification Number	رقم تحديد الهوية
PKI	Public Key Infrastructure	البنية التحتية للمفاتيح العمومية
RA	Registration Authority	سلطة التسجيل
RFC	Request for Comments	طلب التعليقات
RSA	Rivest, Shamir and Adleman Algorithm	خوارزمية ريفست، شامير وأدلمان
SHA	Secure Hash Algorithm	خوارزمية بعثرة امنة
TSA	Time Stamping Authority	سلطة ضبط الوقت
UPS	Uninterruptible Power Supply	إمدادات الطاقة غير المنقطعة
URL	Uniform Resource Locator	المحدد الموحد للموارد

2. مسئوليات النشر و المستودعات

2.1 المستودعات

يجب على سلطة الجذر أن تنشر المعلومات التالية:

- شهادة سلطة الجذر الموقعة ذاتياً
- أي شهادة صادرة عن سلطة الجذر
- حالة إلغاء الشهادات
- الوثائق، على سبيل المثال سياسة الشهادات لسلطة الجذر، سياسة الشهادات للسلطة الوسيطة و الأحكام (الشروط) العامة

2.2 نشر معلومات الشهادات

يجب على سلطة الجذر أن تعمل على توفير مستودعاتها متاحة.

2.3 وقت و تكرار النشر

يجب على سلطة الجذر نشر الشهادة بمجرد إصدارها، إلغائها، أو تغيير مفاتيحها العمومية.

يجب على سلطة الجذر نشر الوثائق غير السرية مثل سياسة الشهادات للسلطة الجذر و الأحكام (الشروط) العامة بعد إعتمادها من السلطة القومية للمصادقة الإلكترونية.

2.4 ضوابط الوصول للمستودعات

يتعيّن على المعلومات المخزنة في المستودعات أن تكون متاحة. ومع ذلك، سيتم تطبيق ضوابط وصول منطقية ومادية على المستودعات، وذلك لمنع أي أعمال غير مصرح بها بالإضافة، أو التعديل، أو الحذف للشهادات والوثائق التي يتم وضعها في المستودعات.

3. التحديد و التحقق من الهوية

3.1 التسمية

3.1,1 أنواع الأسماء

يجب أن تكون أنواع الأسماء المخصصة لصاحب الشهادة تتبع لشكل X.500. يجب على السلطات الوسيطة أن يكون الإسم المميز لها فريد و وفقا لمعيار X.500.

3.1.2 حوجة أن تكون الأسماء ذات معنى

يجب أن تكون الأسماء المخصصة لصاحب الشهادة ذات معنى.

3.1.3 مجهولية الهوية للمشتركين

سلطة الجذر لا تسمح بإصدار شهادة لسلطة وسيطة مجهولة الهوية.

3.1.4 قواعد تفسير مختلف صيغ الأسماء

كما هو محدد في البند 3.1.1 .

3.1.5 وحدانية الأسماء

يجب أن تكون الأسماء المخصصة لصاحب الشهادة فريدة (غير متكررة).

3.1.6 الاعتراف ،والموثوقية، ودورالعلامات التجارية

يجب على سلطة الجذر قبول العلامات التجارية المُعترف بها من الجهات المخول لها.

3.2 التحقق الإبتدائي من صحة الهوية

3.2.1 طريقة إثبات الإمتلاك للمفتاح الخصوصي

سلطة الجذر تُصدر شهادات فقط لسلطات التصديق الوسيطة، والتي تولد أزواج مفاتيحها خلال المراسم الرسمية لتوليد المفاتيح.

3.2.2 التحقق من هوية المؤسسة

سلطة الجذر تقدّم شهادات لسلطات التصديق الوسيطة التي تملكها و تشغلها السلطة القومية للمصادقة الإلكترونية، و لذلك لا توجد أي حوجة للتحقق من هوية مؤسسة ما.

3.2.3 التحقق من هوية الأفراد

سلطة الجذر لا تصدر شهادات لمستخدمين نهائيين (أفراد).

3.2.4 معلومات المشترك غير المُتَحَقق منها

يجب التحقق من صحة جميع المعلومات التي ترد في الشهادة.

3.2.5 التحقق من الصلاحيات

يجب على السلطة القومية للمصادقة الإلكترونية تحديد ممثّل مصرح له بالعمل بالنيابة عن سلطة التصديق الوسيطة لإدارة شهادتها.

3.2.6 معايير التشغيل المشترك مع جهات اخرى

لا شروط.

3.3 التحديد والتحقق من الهوية لطلبات تغيير المفاتيح

3.3.1 التحديد والتحقق من الهوية للطلبات الراتبة لتغيير المفاتيح

كما هو محدد في البند 3,2.

3.3.2 التحديد والتحقق من الهوية لطلبات تغيير المفاتيح بعد إلغاء الشهادة

كما هو محدد في البند 3,2.

3.4 التحديد والتحقق من الهوية لطلب إلغاء الشهادة

كما هو محدد في البند 3,2.

4. دورة حياة الشهادة و المتطلبات التشغيلية

4.1 تقديم الطلب للشهادة

4.1,1 المخول لهم تقديم طلب شهادة

السلطة القومية للمصادقة الإلكترونية هي المالكة والمشغّلة لجميع السلطات الوسيطة. لذا ليست هنالك أية حوجة لطلبات تقديم شهادات من جهة خارجية.ولذلك سيتم إدارة طلبات تقديم الشهادات لجميع السلطات الوسيطة عن طريق السلطة القومية للمصادقة الإلكترونية.

4.1.2 عملية التسجيل و المسئوليات

عملية التسجيل ستكون كالاتي:

- السلطة القومية للمصادقة الإلكترونية تتحقق من صحة الحوجة لإنشاء السلطات الوسيطة
- السلطة القومية للمصادقة الإلكترونية تحدد الوكيل (الممثّل) المصرح له بإدارة شهادة السلطة الوسيطة
- السلطة القومية للمصادقة الإلكترونية تطور جميع سياسات الشهادة الرقمية وممارسات تصديق الشهادات المقابلة لشهادة التوقيع الرقمي للسلطة الوسيطة و أي وثائق أخرى مطلوبة

4.2 معالجة طلب الشهادة

4.2.1 أداء مهام التحديد و التحقق من الهوية

يجب إجراء عملية التحديد والتحقق من الهوية عند طلب الشهادة وفقا للبند 3.2.

4.2.2 الموافقة أو الرفض لطلبات الشهادة

لا شروط.

4.2.3 الزمن المطلوب لمعالجة طلبات الشهادة

لا شروط.

4.3 إصدار الشهادة

4.3.1 إجراءات سلطة الجذر المتبعة خلال إصدار الشهادة

يجب على سلطة الجذر معالجة طلب الشهادة كما يلي:

- تستلم سلطة الجذر طلب الشهادة من السلطة الوسيطة
- تتحقق سلطة الجذر من طلب الشهادة، وذلك بالتحقق من صحة جميع المحتويات المقدمة في الطلب
- عندما يتم التحقق من صحة كل الوثائق والمعلومات المقدمة، ويتم إستيفاء كل الشروط، تصدر سلطة الجذر شهادة رقمية موقعة تحوي كل المعلومات المقدمة في الطلب

4.3.2 إخطار سلطة الجذر للسلطات الوسيطة بإصدار الشهادة

يجب على سلطة الجذر إخطار السلطة الوسيطة باصدار الشهادة و توفيرها لها.

4.4 قبول الشهادة

4.4.1 الإجراء المُتَخذ الدال على قبول الشهادة

يجب على السلطة الوسيطة قبول أو رفض الشهادة الصادرة من سلطة الجذر. في حالة الرفض، يجب عليها تقديم المبررات للرفض.

4.4.2 نشر سلطة الجذر للشهادة

يجب على سلطة الجذر نشر الشهادة الصادرة بعد قبول الشهادة.

4.4.3 إخطار سلطة الجذر للجهات الأخرى بإصدار الشهادة

لا شروط.

4.5 زوج المفاتيح و إستخدام الشهادة

4.5.1 المفاتيح الخصوصية للسلطات الوسيطة و إستخدام الشهادة

تلتزم السلطة الوسيطة حماية جميع مفاتيحها الخصوصية من الإستخدام غير المصرح به ويجب عليها إستخدام مفاتيحها الخصوصية كما هو محدد في الحقل الملحق لإستخدام المفتاح في الشهادات المقابلة لهذه المفاتيح. ويجب على السلطة الوسيطة التوقف عن استخدام المفتاح الخصوصي بعد إنتهاء صلاحيته أو بعد أن يتم إلغائه.

4.5.2 المفاتيح العمومية للأطراف المعوّلة و إستخدام الشهادة

يجب على الطرف المعوّل الإلتزام بالآتي:

- التعويل على الشهادات فقط عند إستخدام التطبيقات المناسبة على النحو المحدد في سياسة الشهادات هذه، و وفقا للشروط العامة
- إستخدم المفتاح العمومي على النحو المحدد في الحقول الملحقة الموضحة لإستخدام المفتاح
- التحقق من صلاحية الشهادة، وذلك من خلال الآليات المحددة في الشهادة

4.6 تجديد الشهادة

سلطة الجذر لا تدعم تجديد الشهادة للسلطات الوسيطة.

4.7 تغيير مفاتيح الشهادة

سلطة الجذر تدعم تغيير مفاتيح الشهادة.

4.7.1 الظروف التي تقتضي تغيير مفاتيح الشهادة

يتوجّب طلب تغيير مفاتيح الشهادة في الظروف التالية:

- بعد إلغاء الشهادة بسبب كشف المفتاح الخصوصي
- بعد إنتهاء مدة صلاحية الشهادة
- بعد إنتهاء مدة صلاحية إستخدام المفتاح الخصوصي
- عند أي ظرف آخر تحدده السلطة القومية للمصادقة الإلكترونية

ويمكن أيضا طلب إلغاء للشهادة عند أي ظروف اخرى تحددها السلطة القومية للمصادقة الإلكترونية.

4.7.2 المخول لهم طلب شهادة للمفتاح العمومي الجديد

يجب على السلطة الوسيطة تغيير مفاتيحها الخصوصية بعد الحصول على الموافقة من سلطة الجذر.

4.7.3 معالجة طلبات تغيير مفاتيح الشهادة

كما هو محدد في البند 3.3.1 أو 3.3.2، وذلك حسب ظروف تغيير مفاتيح الشهادة.

4.7.4 الإخطار بإصدار الشهادة الجديدة للسلطات الوسيطة

كما هو محدد في 4.3.2.

4.7.5 الإجراء المُتَخذ الدال على قبول الشهادة بعد تغيير المفاتيح

كما هو محدد في 4.4.1.

4.7.6 نشر الشهادة بعد تغيير المفاتيح بواسطة سلطة الجذر

كما هو محدد في 4.4.2.

4.7.7 إخطار سلطة الجذر للجهات الأخرى بإصدار الشهادة

كما هو محدد في 4.4.3.

4.8 تعديل الشهادة

سلطة الجذر لا تدعم تعديل الشهادة.

4.9 إلغاء وتعليق الشهادة

4,9,1 ظروف إلغاء الشهادة

يجب طلب إلغاء الشهادة إذا حدث أحد ما يلي:

- الإشتباه أو التأكد بأن المفتاح الخصوصي للشهادة أو حاوية المفتاح الخصوصي لها قد تم العبث به، أو فقدانه أو كشفه
- المعلومات الواردة في الشهادة لم تعد صالحة وتحتاج إلى تغيير
- صاحب الشهادة إستخدم الشهادة لأي تطبيق ما مخالف للسياسات المحددة في سياسة الشهادات هذه

- هنالك إدعاء بأن صاحب الشهادة لا يفي بالإلتزامات المنصوص عليها في سياسة الشهادات هذه أو في إتفاقيات موقّع عليها آنفا

4.9.2 المخول لهم طلب إلغاء الشهادة

يجوز للجهات التالية طلب إلغاء الشهادة:

- السلطة القومية للمصادقة الإلكترونية
- سلطة الجذر
- ممثلي السلطات الوسيطة المصرح لهم بذلك

4.9.3 إجراءات طلب إلغاء الشهادة

التحديد و التحقق من الهوية لطلب الإلغاء محدد في 4,3.

4.9.4 مدة المهلة لحين طلب الإلغاء

المهلة لحين طلب الإلغاء غير مسموح بها في سياسة الشهادات هذه.

4.9.5 المدة التي يجب خلالها على سلطة الجذر معالجة طلب إلغاء الشهادة

يجب على سلطة الجذر معالجة طلب الإلغاء في أسرع وقت ممكن، بمجرد أن يتم التحقق من الطلب.

4.9.6 متطلبات التحقق من إلغاء الشهادات للأطراف المعوّلة

يجب على الأطراف المعوّلة التأكد من حالة إلغاء الشهادة وذلك من خلال قائمة الشهادات الملغاة المنشورة أو مجيب بروتوكول التحقق المباشر من حالة الشهادة لسلطة الجذر.

4.9.7 دورة إصدار قائمة الشهادات الملغاة (إن وجد)

يجب على سلطة الجذر إصدار قائمة الشهادات الملغاة مرة واحدة في السنة على الأقل، وبعد كل الإلغاء.

4.9.8 الحد الأقصى لتأخير إصدار قوائم الشهادات الملغاة (إن وجد)

يجب على سلطة الجذر إصدار قائمة الشهادات الملغاة بمجرد أن تم الإنتهاء من معالجة طلب الإلغاء.

4.9.9 إتاحة التحقق المباشر من حالة/ إلغاء الشهادة

قد تقدّم سلطة الجذر التحقق المباشر من حالة الشهادة عبر الإنترنت، وذلك من خلال مجيب بروتوكول التحقق المباشر من حالة الشهادة الذي يتوافق مع طلب التعليقات رقم 2560.

4.9.10 متطلبات التحقق المباشر من إلغاء الشهادة

قد توفر سلطة الجذر مجيب بروتوكول التحقق المباشر من حالة الشهادة والذي يتوافق مع طلب التعليقات رقم 2560. برامجيات الأطراف المعوّلة ينبغي أن تكون وفقا لمتطلبات طلب التعليقات 2560.

4.9.11 الأشكال الأخرى المتوفرة لإعلانات الإلغاء

لا شروط.

4.9.12 متطلبات خاصة عند كشف المفتاح الخصوصي

لا شروط.

4.9.13 ظروف تعليق الشهادة

سلطة الجذر لا تدعم تعليق الشهادة.

4.10 خدمات الإعلان عن حالة الشهادة

يجب أن تكون خدمة التحقق من حالة الشهادة متاحة على النحو المحدد في 4.9.6 بإمكانية توافر عالية.

4.11 إنهاء الإشتراك

لا شروط.

4.12 إستيداع المفاتيح و إسترجاعها

سلطة الجذر لا تدعم إستيداع أو إسترجاع (إسترداد) المفاتيح الخصوصية للسلطات الوسيطة.

5. ضوابط المرافق، والإدارة، والتشغيل

5.1 الضوابط المادية

5.1.1 ضوابط الموقع والمباني

مواقع مرافق سلطة الجذر ومعداتها يجب أن يتم حمايتها من الكوارث البيئية.

يتضمن بناء مرافق سلطة الجذر الضوابط التالية:

- جدران صلبة تمتد من الأرض الفعلية إلى السقف الفعلي لمنع الدخول غير المصرح به إلى مرافق سلطة الجذر
- مناطق أمنية متعددة، يتم الوصول إليها من خلال نظام متعدد العوامل للتحقق من الهوية. ويجب أن يكون لهذه المناطق تصنيفات تأمينية ويجب أن يتم المرور على مالا يقل عن ثلاثة مناطق أمنية للوصول إلى المعدات أو البرامج الأكثر حساسية وأهمية

5.1.2 ضوابط الوصول

يتم تأمين مرافق سلطة الجذر والمعدات المادية من الوصول غير المصرح به من خلال الضوابط التالية:

- يتم التحكم في المرافق التشغيلية بحيث تقتصر فقط على الأشخاص المصرح لهم من خلال إستخدام آليات للتحقق من الهوية.
- تطبيق ضوابط التحقق من الهوية عند الإنتقال من منطقة إلى أخرى.
- مراقبة الدخول والخروج وغيرها من الأنشطة بإستخدام كاميرات الدائرة المغلقة.
- منطقة إستقبال لتقييد الوصول إلى المرافق التشغيلية لسلطة الجذر إلى الأفراد المصرح لهم فقط.
- وجود أفراد من حراس أمن يراقبون المرافق باستمرار 24×7×365
- جميع أنظمة الإتصالات المستخدمة داخل المنشأة قائمة على نظام الأسلاك وتكون محمية من الاعتراض والضرر.
- أي تحريك لأي من المعدات أو المواد من أو إلى المنشأة يتطلب الحصول على تصريح. ويجب تقديم مبررات معقولة قبل الحصول على هذا الإذن.

5.1.3 التيار الكهربائي و مكيفات الهواء

يجب حماية جميع المعدّات من إنقطاع التيار الكهربائي، وذلك من خلال توفير مصدر آخر للتيار. بجانب الطاقة الرئيسية، يجب تركيب إمدادات الطاقة غير المنقطعة (UPS) لضمان استمرار العمل عند غياب الكهرباء الرئيسية. تكييف الهواء يجب أن يكون كافي لتوفير درجة الحرارة التي تنصح بها الجهات المصنّعة للمعدات.

5.1.4 التعرّض للمياه

يجب تركيب جميع المعدات بطريقة تضمن أنها ليست في خطر من التعرض للمياه.

5.1.5 المنع والوقاية من الحرائق

يجب تركيب نظام المنع والوقاية من الحرائق في كل مرافق سلطة الجذر. ويجب على النظام أن يتضمن نظام الإنذار التلقائي و أن يكون غاز صديق للإنسان، ويمكن تعريضه إلى مصدر النار تلقائياً.

5.1.6 وسائط التخزين

يجب حماية جميع وسائط التخزين سواء كانت ثابتة أو قابلة للنقل من التلف العرضي. و يجب تخزين وسائط النسخ الإحتياطي في موقع منفصل فعليا وآمن، ويجب حمايته من النار و ضرر التعرض للمياه.

5.1.7 التخلص من النفايات

يجب إتلاف وسائط التخزين والوثائق الحساسة التي لم تعد هناك حوجه لها بطريقة آمنة. يجب فحص كافة عناصر المعدات التي تحتوي على وسائط تخزين للتأكد من أنها لا تحتوي على بيانات حساسة قبل التخلص منها. يجب تمزيق جميع الوثائق الورقية بطريقة تضمن أنه لا يمكن إسترجاعها مرة أخرى.

5.1.8 النسخ الإحتياطي خارج الموقع

يجب على سلطة الجذر أن تضمن نظام نسخ إحتياطي آمن خارج الموقع الرئيسي. ويجب أن يتم تنفيذ عمليات نسخ إحتياطي شاملة بصفة دورية. يجب أن يضمن نظام النسخ الاحتياطي أنه يمكن إسترجاع النظام بأكمله عند حدوث أي أعطال. كما يجب فحص عملية التعافي (إسترداد المعلومات) من النسخ الإحتياطي للبيانات بشكل دوري.

5.2 الضوابط الإجرائية

5.2.1 الأدوار الموثوقة

الدور الموثوق هو شخص يقوم باداء أعمال يمكن أن تؤدي إلى مشاكل أمنية إذا لم يتم إنجازها بطريقة صحيحة سواء كان ذلك بقصد أو بدون قصد. عدة مناهج يجب أن يتم تطبيقها لزيادة إحتمالية اداء هذه الأدوار بنجاح. هذه الأساليب تشمل الاتي:

- التأكد بأن الشخص الذي يشغل هذا الدور هو شخص جدير بالثقة و تم تدريبه تدريبا جيدا
- توزيع المهام بين أكثر من شخص واحد، بحيث أن أي عمل تخريبي يتطلب التواطؤ

الأدوار الموثوقة تتضمن على الأقل الأدوار و المسئوليات الاتية:

- **ضابط (مسؤول) الأمن**: وهو مسئول عن الاتي:
  - ضمان تطبيق السياسات و الممارسات الأمنية لسلطة الجذر
  - عمليات إدارة دورة حياة مفاتيح التشفير
  - النسخ الإحتياطي للمفاتيح الخصوصية

- **مدير نظام السلطة**: و هو مسئول عن الاتي:
  - وصف الشهادات

- إصدار، وإلغاء، وتغيير مفاتيح الشهادات
- تطوير خطة إستمرارية العمل

- **مشغل النظام**: و هو مسئول عن الاتي:
  - تثبيت ، وتهيئة، وصيانة أنظمة سلطة الجذر
  - تشغيل أنظمة سلطة الجذر و ذلك يشمل النسخ الإحتياطي للنظام و عملية إسترجاع النظام
- **مدقق النظام**: و هو مسئول عن الاتي:
  - إدارة نظام الأرشفة و سجلات التدقيق لسلطة الجذر
  - تدقيق مطابقة أنظمة سلطة الجذر و أنظمة السلطات الوسيطة مع السياسات و الممارسات المقابلة المنصوصة لها

5.2.2 عدد الأشخاص المطلوب لكل مهمة

يتم توزيع المهام في سلطة الجذر على أكثر من شخص واحد لزيادة إحتمالية عدم قدرة شخص ما من إستخدام بعض عمليات سلطة الجذر بطريقة تخريبية. عمليات سلطة الجذر التالية تتطلب شخصان أو أكثر لأدائها:

- توليد مفاتيح سلطة الجذر
- تفعيل مفتاح التوقيع الرقمي لسلطة الجذر
- النسخ الإحتياطي للمفتاح الخصوصي
- توليد بيانات التفعيل لوحدات التأمين المادية
- تفعيل و إلغاء تفعيل وحدات التأمين المادية
- إعتماد طلبات الشهادات و ذلك يشمل إصدار، وإلغاء، وتغيير المفاتيح الشهادة

5.2.3 التحديد و التحقق من الهوية لكل دور

يجب على كل الأشخاص تحديد و إثبات هوياتهم قبل السماح لهم لإنجاز أي نشاط من الأنشطة المذكورة أعلاه.

5.2.4 أدوار تتطلب الفصل بين المهام

لن يُسمح لأي شخص بأن يكون له أكثر من دور موثوق واحد ضمن نظام سلطة الجذر.

5.3 الضوابط على الأشخاص

5.3.1 متطلبات المؤهلات، والخبرة، والخلفيات الأمنية

يجب على كل الأشخاص إثبات ما لديهم من مهارات ذات صلة و معرفة وخبرات مطلوبة لأعمال الوظيفة. الأشخاص الذين يشغلون هذه الأدوار يجب أن يكونوا مواطنين سودانين و أن يتم إختيارهم على أساس الولاء والأمانة والنزاهة.

يجب أن يكون لكل الأشخاص درجات علمية ذات صلة. كما يجب أن يكونوا على دراية تامة بأسياسيات أمن المعلومات، و التشفير بالمفتاح العمومي والقوانين ذات الصلة

يجب على أي شخص التوقيع على إتفاقية السرية (عدم الإفشاء)، و ذلك كشرط للتوظيف.

5.3.2 اجراءات التحريات

يتم تحديد الهوية وفحص الخلفيات لكل الأشخاص الذين يشغلون أدوار موثوقة الخضوع قبل توليهم أي دور موثوق. هذا الفحص يجب أن يتضمن الاتي:

- التحقق من صحة هوية الشخص
- التاريخ الوظيفي
- التعليم
- مكان الميلاد
- أماكن الإقامة السابقة

- الشخصيات يمكن الرجوع إليها
- التحريات الجنائية

5.3.3 الإحتياجات التدريبية

يتلقى كل الأشخاص الذين ينجزون أعمال تشغيلية تدريبا شاملاً في كل الواجبات التي من المتوقع منهم القيام بها. و ذلك يشمل معرفة جيدة بالتدريب المناسب بالاتي:

- سياسة الشهادات و ممارسات تصديق الشهادات لسلطة الجذر
- إجراءات إستمرارية العمل و التعافي من الكوارث

يجب توضيح كافة التفاصيل لمتطلبات وإجراءات التدريب لكل دور في ممارسات تصديق الشهادات.
يجب الإحتفاظ بوثائق تحدد كل الأشخاص الذين إكتمل تدريبهم و مستوى التدريب.

5.3.4 متطلبات و دورة إعادة التدريب

يجب على سلطة الجذر توفير التدريب للعاملين لتلبية أي تغييرات في البرامجيات، أو المعدات أو العمليات التشغيلية. ويجب على الموظفين الحفاظ على مستويات المهارة المطلوبة من أجل مواصلة أعمالهم بطريقة إحترافية.

5.3.5 تسلسل و تكرار تناوب الوظائف

لا شروط.

5.3.6 العقوبات على الأفعال غير المصرح بها

يجب تطبيق إجراءات العقوبات الإدارية المناسبة على أي فرد نفّذ أي عمل ضد سياسة الشهادات هذه أو ممارسات تصديق الشهادات أو أي عملية أو إجراء مُعتَمد قامت بنشره سلطة الجذر.

5.3.7 متطلبات المتعاقدين المستقلين

يجب على المتعاقدين إثبات مالديهم من المهارات ذات الصلة، والمعرفة والخبرات المطلوبة لأعمال الوظيفة. المتعاقدين يخضعون لنفس المتطلبات المحددة في 5.3.1، وفحص الخلفيات في 5.3.2 و إجراءات إدارة شئون الأفراد كموظفين.

أي إتفاق لإبرام عقد مع متعاقدين يجب أن يسمح لسلطة الجذر بإتخاذ تدابير ضد موظفي العقود الذين يخالفون السياسات الأمنية لسلطة الجذر .التدابير الوقائية يمكن أن تشمل الاتي:

- سندات مالية على الاشخاص المتعاقدين
- التعويض عن الأضرار الناجمة عن إجراء المتعاقدين لأعمال ضارة مُرتكبة عمدا
- العقوبات المالية

أي متعاقد يجب أن يوقع على إتفاقية السرية (عدم الإفشاء) كشرط للعقد.

5.3.8 الوثائق المقدمة للموظفين

يجب أن تُقدَّم وثائق كافية لتحديد الواجبات والإجراءات لكل دور للأشخاص الذين يشغلون هذه الأدوار.

5.4 إجراءات مراجعة السجلات

5.4.1 أنواع الأحداث التي يتم تسجليها

أي أعمال تتعلق بأمن النظام ستكون قابلة للتدقيق. وهذا يشمل ولكن لايقتصر على الأحداث المتعلقة بما يلي:

- الوصول إلى نظام السلطة

- الوصول الفعلي لمرافق السلطة
- توليد مفاتيح التشفير
- دورة حياة الشهادات
- سجلات النظام
- سجلات التطبيقات
- عمليات وحدات التشفير

جميع سجلات التدقيق، سواء الإلكترونية وغير الإلكترونية، يتم الإحتفاظ بها، وفهرستها، وتخزينها، والحفاظ عليها واستنساخها بحيث تكون دقيقة، وكاملة ومقروءة، كما يجب إتاحتها خلال عمليات تدقيق المطابقة. ويجب أن يتضمن كل سجل تدقيق على الأقل ما يلي (سواء تم تسجيلها آليا أو يدويا لكل حدث قابل للتدقيق):

- نوع الحدث
- تاريخ ووقت وقوع الحدث
- مؤشر النجاح أو الفشل ، حيثما اقتضى الأمر
- هوية الجهة و/ أو المستخدم المشغّل الذي تسبب في الحدث

5.4.2 دورة مراجعة السجلات

يجب معالجة سجلات التدقيق في الحالات التالية:

- كل أسبوع على الأقل مرة واحدة
- بعد إنذار أمني أو حدث شاذ
- خلال تدقيق المطابقة

بعد كل معالجة سجل، ينبغي إتخاذ إجراءات تحسين للنظام كنتيجة لذلك ويجب توثيق كل ذلك.

5.4.3 فترة الاحتفاظ بسجلات التدقيق

كل سجلات التدقيق سواء كانت إلكترونية أو غير إلكترونية يجب حفظها خارج الموقع الرئيسي لمدة 12 شهر على الأقل منذ تاريخ وقوع الحدث المسبب لها.

5.4.4 حماية سجلات التدقيق

يجب الحفاظ على سجلات التدقيق في شكل يحول من أي تعديل، أو إستبدال أو حذف غير مصرح به، أو الوصول غير المصرح به. يجب إستخدام التوقيع الرقمي لهذه السجلات لحماية تكاملية (سلامة) ملفات التدقيق الإلكترونية. المفتاح الخصوصي الذي يتم إستخدامه للتوقيع الرقمي لا يجوز إستخدامه لأي أغراض أخرى.

5.4.5 إجراءات النسخ الإحتياطي لسجلات التدقيق

يجب أن تُنسخ جميع سجلات التدقيق نسخاً إحتياطية مرة كل شهر على الأقل. يجب إيداع نسخة من سجل التدقيق خارج الموقع الرئيسي للسلطة شهريا.

5.4.6 نظام جمع التدقيق (داخلي أم خارجي)

يجب أن يكون نظام جمع سجلات التدقيق داخل سلطة الجذر. ويمكن تنفيذ نظام تسجيل تلقائي لأي من الأنظمة التي تقوم بمعالجة الأحداث القابلة للتدقيق. من الممكن أن يتم إستدعاء هذة الأنظمة بمجرد تشغيل نظام سلطة الجذر.

5.4.7 إخطار الجهة مُسببة الحدث

ليس من المطلوب إرسال أي إخطار إلى أي شخص، أو مؤسسة، أو جهاز أو أي جهة آخرى كانت قد تسببت في الحدث القابل للتدقيق.

5.4.8 تقييم جوانب الضعف

يجب أن تستخدم سجلات التدقيق الحالية في التقييمات الدورية لجوانب الضعف في نظام السلطة التي يتم تنفيذها بواسطة سلطة الجذر.

5.5 أرشفة السجلات

5.5.1 أنواع السجلات المؤرشفة

يجب على سلطة الجذر الإبقاء على المعلومات ذات الصلة بالأنشطة التالية في أرشيفها:

- عمليات دورة حياة مفاتيح سلطة الجذر
- شهادات سلطة الجذر
- عمليات دورة حياة شهادات السلطات الوسيطة
- عمليات دورة حياة شهادات التصديق المتبادل
- سجلات التدقيق
- جميع إصدارات سياسات الشهادات والممارسات التي تم تطويرها
- بيانات تهيئة النظام قيد التشغيل
- جميع إصدارات قوائم الشهادات الملغاة والشهادات التي تم إلغائها

5.5.2 فترة الإحتفاظ بالأرشيف

يجب على سلطة الجذر الإبقاء على البيانات المحفوظة في الأرشيف لمدة 20 سنة على الأقل.

5.5.3 حماية الأرشيف

يجب على سلطة الجذر تطبيق ضوابط متنوعة من أجل حماية البيانات المؤرشفة من الوصول غير المصرح به، والتعديل والتخريب. يجب أن تكون هذه الضوابط مفصّلة في ممارسات تصديق الشهادات المعمول بها.

5.5.4 إجراءات النسخ الإحتياطي للأرشيف

يجب على سلطة الجذر أن تنسخ البيانات المؤرشفة نسخاً إحتياطية. يجب أن تصف ممارسات تصديق الشهادات كيفية نسخ وإدارة هذه البيانات المؤرشفة.

5.5.5 متطلبات ضبط الوقت للسجلات

سيتم ادراج تاريخ و وقت دقيقين لكل من الشهادات و قوائم الشهادات الملغاة و سجلات التدقيق عند انشاءها من خلال مخدم الوقت. يجب مزامنة وقت النظام مع مخدم وقت موثوق بصفة دورية.

5.5.6 نظام جمع الأرشيف (داخلي أم خارجي)

يجوز فقط لضباط الأمن سلطة الجذر، ومدققي نظام سلطة الجذر و مدراء سلطة الجذر الموثوقين و المصرح لهم الجمع و الإطلاع على البيانات المحفوظة في الأرشيف.

5.5.7 إجراءات الحصول والتحقق من معلومات الأرشيف

يجب على سلطة الجذر التحقق من معلومات الأرشيف بصفة دورية.

5.6 تحويل المفاتيح

قد تُغيّر سلطة الجذر مفتاحها الخصوصي قبل تاريخ إنتهاء صلاحية شهادتها. عندها يجب أن تصدر شهادة جديدة بالمفتاح العمومي الجديد و التي ستكون موقعة ذاتيا. ويمكن للأطراف المعولة إستخدام الشهادة القديمة طالما أنها لم تنتهِ أو لم يتم إلغائها من قِبل سلطة الجذر. ويجب الإحتفاظ بالمفاتيح القديمة من أجل إستخدامها مع السجلات القديمة.

5.7 التعافي من الكوارث وإختراق النظام

5.7.1 إجراءات التعامل مع الحوادث و الإختراق

يجب على سلطة الجذر وضع نفسها في حالة كارثة إذا تم حدوث احد الحوادث التالية:

- كشف أو فقدان مفاتيح التوقيع الرقمي لسلطة الجذر
- هجوم على أمن نظام أو أمن شبكة سلطة الجذر
- عدم توفر بنية تحتية أو مرفق ما
- ضرر كلي أو جزئي في الموقع الرئيسي لسلطة الجذر
- تزوير في إصدار، تغيير المفاتيح أو إلغاء الشهادات

يجب على سلطة الجذر إرساء الضوابط التي تقدّم ضمان معقول لإستمرارية عمليات السلطة في حالة وقوع كارثة. وهذا يشمل ولكن لا يقتصر على الاتي:

- تطوير وإختبار عملية التعافي من الكوارث للمكونات بالغة الأهمية لنظام سلطة الجذر
- التخزين لكل ما يتطّلب من وحدات التشفير الآمنة، ومواد التفعيل، والنسخ الإحتياطية للأنظمة والبيانات ومعلومات التهيئة في موقع بديل للموقع الرئيسي
- إتاحة المكان البديل والمعدات والإتصالات لتمكين التعافي من الكارثة

يجب على سلطة الجذر إخطار السلطة القومية للمصادقة الإلكترونية والمشاركين الآخرين ذوي الصلة بهذه الكارثة في غضون يوم واحد.

5.7.2 عطب موارد الحوسبة، البرامجيات، و/أو البيانات

عند حدوث عطب في موارد الحوسبة والبرامجيات، و/ أو البيانات ، يجب على سلطة الجذر الإستجابة على النحو التالي:

- إستعادة النظام بإستخدام أنظمة النسخ الإحتياطي.
- إذا دمّر هذا العطب مفاتيح التوقيع الرقمي لسلطة الجذر، فإنه يجب عليها إعادة بدء عملية التعافي مع إعطاء الأولوية لإنشاء زوج مفاتيح جديد.

5.7.3 الإجراءات المتخذة عند كشف المفتاح الخصوصي لجهة

إذا إشتبهت سلطة الجذر بأنه قد تم كشف أو فقدان لمفتاحها الخصوصي، يجب عليها إلغاء شهادتها بعد موافقة السلطة القومية للمصادقة الإلكترونية. ثم يجب تنفيذ تحقيق لتحديد نطاق وسبب هذه الحادثة. يجب على سلطة الجذر إخطار مشاركيها في غضون يوم واحد. كما يجب عليها إلغاء كل الشهادات التي أصدرتها.

يجب على سلطة الجذر تطبيق إجراءات حديثة للتأكد من أن هذه الحادثة لن تحدث مرة أخرى. بعد ذلك، يجب إصدار شهادة جديدة بمفاتيح جديدة.

5.7.4 إمكانية إستمرارية الأعمال بعد الكارثة

يجب على سلطة الجذر وضع خطط لإستمرارية الأعمال والتي تضمن أن يتم إستعادة الخدمة كاملة في أسرع وقت ممكن.

5.8 إنهاء خدمة سلطة الجذر

في حال قررت سلطة الجذر إنهاء عملها، يتعيّن عليها أن تقدّم إشعارا إلى كل المشاركين، شهادة سلطة الجذر يجب أن تبقى صالحة إلى حين إنتهاء مدة صلاحية اخر شهادة للمستخدمين النهائيين، بعد ذلك يجب على سلطة الجذر إلغاء شهادتها وإلغاء جميع الشهادات التي أصدرتها كذلك، وأن يتم نقل جميع السجلات المؤرشفة لديها إلى السلطة القومية للمصادقة الإلكترونية.

6. ضوابط التأمين الفنية

6.1 توليد و تثبيت زوج المفاتيح

6.1.1 توليد زوج المفاتيح

تولّد سلطة الجذر مفاتيحها خلال مراسم توليد المفاتيح. يتم توليد أزواج المفاتيح في بيئات آمنة ماديا، وضمن نفس جهاز وحدة التشفير الذي يتم إستخدامه في عمليات التوقيع الرقمي لسلطة الجذر. ولا يسمح بعملية إدخال المفاتيح.

العديد من ضباط الأمن سيتم التصريح لهم بتوليد أزواج مفاتيح سلطة الجذر وذلك في إطار مبدأ التحكم متعدد الأشخاص و تقنية تقاسم السرية. يجب أن يشهد مراسم توليد المفاتيح عدد من المدقّقين.

6.1.2 تسليم المفتاح الخصوصي للسلطة الوسيطة

سلطة الجذر لا تولّد أي مفتاح خصوصي للسلطات الوسيطة التابعة لها. ولذلك ليس هنالك أي تسليم لمفتاح خصوصي إلى سلطة تصديق وسيطة.

6.1.3 تسليم المفتاح العمومي لسلطة الجذر

المفاتيح العمومية للسلطة الوسيطة يتم تسليمها إلى سلطة الجذر من خلال طلب موثوق و موقع عليه من قِبل السلطة الوسيطة.

6.1.4 تسليم مفتاح سلطة الجذر العمومي للأطراف المعوّلة

شهادة سلطة الجذر هي شهادة موقعة ذاتيا. يجب على الأطراف المعوّلة التحصّل على المفتاح العمومي في شهادة سلطة الجذر من الموقع الإلكتروني الموثوق للسلطة القومية للمصادقة الإلكترونية أو في دليل عمومي.

6.1.5 اطوال المفاتيح

يجب على سلطة الجذر إستخدام ما لا يقل عن 4096 بت لمفاتيحها الخصوصية عند إستخدام خوارزمية RSA، في حين يجب على السلطات الوسيطة إستخدام ما لا يقل عن 2048 بت لمفاتيحها الخصوصية عند إستخدام خوارزمية RSA. ويمكن إستخدام خوارزمية المنحنى الإهليلجي بطول 384 بت للمفتاح على الأقل، حيث أن هذه الخوارزمية يمكن إستخدامها في بعض التطبيقات. للتوقيع الرقمي، يجب أن تستخدم ما لا يقل عن SHA-256 لخوارزمية البعثرة الآمنة.

6.1.6 إنشاء مُعامِلات المفتاح العمومي وفحص الجودة

يجب على سلطة الجذر تطبيق أفضل الممارسات وأحدث المعايير لتوليد مُعامِلات المفتاح العمومي وفحص جودتها.

6.1.7 أغراض إستخدام المفتاح (كما في حقل إستخدام مفتاح X.509 v3)

يتم إستخدام أزواج مفاتيح سلطة الجذر في التطبيقات التالية:

- التوقيع الرقمي للشهادات الرقمية
- التوقيع الرقمي لقوائم الشهادات الملغاة أو مجيب التحقق المباشر من حالة الشهادة

6.2 ضوابط وحدات التشفير وحماية المفتاح الخصوصي

6.2.1 معايير وضوابط وحدات التشفير

يجب على سلطة الجذر إستخدام أجهزة تشفير وحدة التأمين المادية (HSM) و التحقق من أنها حاصلة على شهادة على الأقل في المستوى 3 أو المستوى 4 حسب معايير معالجة المعلومات الفيدرالية للولايات المتحدة رقم 140 (FIPS 140) في التأمين المادي للعتاد. كل المفاتيح الخصوصية لسلطة الجذر يجب توليدها وتخزينها ضمن وحدة التشفير هذه. لا يسمح للمفتاح الخصوصي بالبقاء في أي جهاز آخر بخلاف عتاد حاصل على شهادة ما لا يقل عن (FIPS 140) المستوى 3 في التأمين المادي للعتاد.

يجب إرسال وحدات التشفير من الجهة المصنّعة لمرافق سلطة الجذر بطريقة يمكن ان تكشف عن العبث (التلاعب).

6.2.2 ضوابط التحكم متعدد الأشخاص بالمفتاح الخصوصي

يجب أن تكفل سلطة الجذر ضرورة تعدد ضباط الأمن لتوليد، وتفعيل، وإلغاء تفعيل، والنسخ الاحتياطي وإستخدام مفاتيحها الخصوصية.

6.2.3 إستيداع المفتاح الخصوصي

لن تسمح سلطة الجذر بعملية الإستيداع لمفاتيحها الخصوصية.

6.2.4 النسخ الإحتياطي للمفتاح الخصوصي

يجب على سلطة الجذر نسخ مفاتيحها الخصوصية نسخاً احتياطية في أجهزة وحدة التأمين المادية مع نفس الشروط المحددة في البند 6.2.1 من قِبل عدد من ضباط الأمن. يجب أن يتم تخزين وحدة التشفير التي تحتفظ بالمفتاح الخصوصي المنسوخ إحتياطيا في مكان خارج الموقع الرئيسي لسلطة الجذر.

6.2.5 أرشفة المفتاح الخصوصي

لا يجوز أن يتم أرشفة أي مفاتيح خصوصية.

6.2.6 نقل المفتاح الخصوصي من أو إلى وحدة التشفير

لا يجوز نقل المفتاح الخصوصي إلى أو من وحدة التشفير إلا في حالة إنشاء نسخ إحتياطية للمفاتيح الخصوصية من وحدة التشفير الرئيسية إلى وحدة التشفير للنسخ الإحتياطي.
يجب على سلطة الجذر تطبيق متطلبات التحكم متعدد الأشخاص من أجل تنفيذ هذه العملية. ويجب على جميع وحدات التشفير أن تستوفي المتطلبات المحددة في 6.2.1.

6.2.7 تخزين المفتاح الخصوصي في وحدة التشفير

يجب على سلطة الجذر تخزين مفاتيحها الخصوصية في وحدة التشفير كما هو محدد في البند 6.2.1.

6.2.8 طريقة تفعيل المفتاح الخصوصي

يقوم ضباط الأمن بتفعيل المفاتيح الخصوصية لسلطة الجذر من خلال التحكم متعدد الأشخاص. ويجب أن يستخدم هؤلاء الأشخاص المصرح لهم شيء يعرفونه وشيء يمتلكونه أثناء عملية التفعيل.

6.2.9 طريقة إلغاء تفعيل المفتاح الخصوصي

يجب على ضباط الأمن إلغاء تفعيل المفاتيح الخصوصية لسلطة الجذر من خلال التحكم متعدد الأشخاص. يقوم الموظفون المصرح لهم بذلك إستخدام شيء يعرفونه وشيء يمتلكونه أثناء عملية إلغاء التفعيل.

6.2.10 طريقة إتلاف المفتاح الخصوصي

يجب على سلطة الجذر إتلاف المفاتيح الخصوصية للتوقيع الرقمي عندما تنتهي مدة صلاحيتها أو يتم إلغائها. وتتم عملية الإتلاف لها بطريقة تمنع فقدانها، أو سرقتها، أو تعديلها، أوإفشاؤها بغير ترخيص أو إستخدامها بدون تصريح. ويجب توثيق هذا الإتلاف.

6.2.11 تقييم وحدة التشفير

كما هو محدد في البند 6.2.1.

6.3 الجوانب الأخرى لإدارة زوج المفاتيح

6.3.1 أرشفة المفتاح العمومي

يجب على سلطة الجذر أرشفة مفاتيحها العمومية بعد إنتهاء مدة صلاحيتها أو إلغائها. الحوجه إلى هذا الأرشيف لتمكين التحقق من صحة الوثائق التي وُقِعت رقميا بعد أن تم إلغاء هذه الشهادات أو إنتهاء مدة صلاحيتها.

6.3.2 الفترات التشغيلية للشهادة وفترات الإستخدام لزوج المفاتيح

يوضح الجدول التالي الإستخدامات الممكنة لزوج مفاتيح سلطة الجذر مع الفترات التشغيلية لكل منها.

نوع الشهادة	فترة صلاحية المفتاح الخصوصي	فترة صلاحية الشهادة
شهادة التوقيع الذاتي لسلطة الجذر	10 سنوات	20 سنة
شهادة سلطة التصديق الوسيطة	5 سنوات	10 سنوات

يجب على سلطة الجذر والسلطات الوسيطة ألّا يصدروا شهادات تمتد فترة صلاحيتها إلى ما بعد تاريخ إنتهاء الشهادة الخاصة بهم.

6.4 بيانات التفعيل

6.4.1 توليد وتثبيت بيانات التفعيل

بيانات التفعيل هي البيانات المطلوبة لتفعيل أو إلغاء تفعيل المفاتيح الخصوصية. يجب على سلطة الجذر إستخدام اثنين من عوامل التحقق من الهوية لتفعيل أو إلغاء تفعيل مفاتيحها الخصوصية.

6.4.2 حماية بيانات التفعيل

يجب على سلطة الجذر تطبيق الضوابط اللازمة لضمان عدم الإختراق (الكشف) لبيانات التفعيل. ويجب على سلطة الجذر تطبيق القواعد اللازمة لمنع أي فرد من تبادل أية بيانات تفعيل مع أفراد غير مصرح لهم بذلك.

6.4.3 الجوانب الأخرى لبيانات التفعيل

يجب على سلطة الجذر عدم إجراء أي نسخ إحتياطية أو أرشفة لبيانات التفعيل.

6.5 ضوابط تأمين الحواسيب

6.5.1 المتطلبات التقنية التأمينية للحواسيب

يجب على سلطة الجذر تطبيق الضوابط التأمينية للحواسيب لجميع المعدات والبرامجيات الثابتة والبرامجيات الأخرى وذلك من أجل حماية سلامة نظام سلطة الجذر بأكمله. وهذا يشمل ولكن لا يقتصر على مايلي:

- التحديد والتحقق من هوية المستخدمين لأنظمة الحاسوب وذلك قبل السماح لهم للوصول إلى موارد الحوسبة
- تمييز الوصول لأنظمة سلطة الجذر إستنادا على نظام الفصل بين المهام والوظائف المختلفة للأفراد الموثوق بهم
- إستخدام مرافق المراقبة والإنذار للكشف عن، وتسجيل، والتصرف في الوقت المناسب في حالة الوصول غير المصرح به إلى موارد الحوسبة والمستودعات
- تشغيل نظام الإختبار الذاتي وإختبار الإختراق بشكل دوري
- تثبيت البرامجيات والحزم البرامجية الموثوقة فقط في أنظمة الحواسيب
- إزالة التطبيقات غير الضرورية المثبتة تبعا للإعدادات الإفتراضية في نظام التشغيل وذلك من خلال تأمين نظام التشغيل المؤمن
- تسجيل وأرشفة جميع الأنشطة

6.5.2 معايير تأمين الحواسيب

يجب على أنظمة الحواسيب لسلطة الجذر إستخدام البرامجيات المُعتَمدة للبنية التحتية للمفاتيح العمومية وفقا للمعايير المشتركة بحيث أن يكون تقييمها على الأقل مستوى ضمان 4.

6.6 الضوابط التقنية لدورة الحياة

6.6.1 ضوابط تطوير النظام

سلطة الجذر قد تطوّر نظم داخلية لتلبية بعض المتطلبات الحديثة للحفاظ على رضا العملاء . يجب على سلطة الجذر تصميم وتطوير وإختبار وتركيب وتشغيل أي نظام داخلياً وذلك بإستخدام نماذج قياسية، و التي قد تمت مراجعتها والموافقة عليها من قِبل مجموعة من الخبراء. كما يجب عليها ضمان الضوابط التي تقدّم ضمان معقول بأن أنشطة التطوير والصيانة للنظم قد تم توثيقها، وإختبارها وتصريحها و تنفيذها على النحو الصحيح للحفاظ على سلامة نظام السلطة.

يجب على سلطة الجذر ضبط عمليات الشراء والتعديل الخارجي للبرامجيات التي تم تطويرها خارج السلطة وذلك من أجل حماية القنوات الخفية الممكنة والشفرات التخريبية. وهذا يشمل التحقق من الكود الأساسي وحزم المستودعات.

6.6.2 ضوابط إدارة التأمين

يجب على سلطة الجذر الحفاظ على تنفيذ الأدوات والإجراءات اللازمة للتأكد من أن الأنظمة التشغيلية وشبكات الحاسوب تلتزم باعدادات التأمين. وهذا يشمل ولكن لا يقتصر على ما يلي:

- مراقبة تكوين أنظمة سلطة الجذر بحيث أن التغييرات فيها من شأنها أن تنذر بخطر ما
- منع العبث بوحدات التشفير خلال وجودها و استخدامها في السلطة
- التحقق من صحة وسلامة البرامجيات الثابتة، والبرامجيات الأخرى والمعدّات بشكل دوري بحيث يمكن الكشف عن أي جزء مثبت زائف من التعليمات البرامجية

6.6.3 الضوابط التأمينية لدورة الحياة

لا شروط.

6.7 الضوابط التأمينية للشبكات

يجب على سلطة الجذر الحفاظ على متطلبات أمن الشبكات لحماية نظام الشبكات من خلال ضوابط معيّنة تشمل ما يلي:

- إستخدام الجدار الناري المناسب ونظام كشف الدخلاء لمنع الوصول غير المصرح به من مجالات الشبكات الخارجية
- تأمين الإتصالات الداخلية لضمان أن المعلومات التي يتم تبادلها لم يتم تغيرها أو اعتراضها من قِبل مستخدمين غير مصرح لهم
- يتم تحديث تكوين شبكة الأجهزة الداخلية والبرامجيات الثابتة بشكل دوري للحفاظ على مستوى عالي من الأمان و الآداء
- يتم تشفير البيانات الحساسة عند تبادلها عبر الشبكات العامة أو غير الآمنة
- لا يسمح بالوصول عن بعد إلى نظام سلطة الجذر وأنظمة وحدات التشفير
- إزالة خدمات الشبكة غير الضرورية وغير المستخدمة
- إستخدام الآليات المناسبة لمنع الأضرار الناجمة عن هجوم قطع الخدمة

6.8 ضبط الوقت

يجب على سلطة الجذر دعم خدمة ضبط الوقت لتزويد الأطراف المعنيّة ببيان قابل للتحقق منه بأن الشهادات الصادرة، وقائمة الشهادات الملغاة ومجيب بروتوكول التحقق المباشر من الشهادة قد تم توقيعهم بينما كانت شهادة التوقيع الرقمي لسلطة الجذر سارية المفعول.

7. وصف الشهادة الرقمية، قائمة الشهادات الملغاة و بروتوكول التحقق المباشر من حالة الشهادة

7.1 وصف الشهادة

يجب على سلطة الجذر أن تصدر الشهادات بحيث تتفق مع معيار شهادة البنية التحتية للمفتاح العمومية للإنترنت (X.509) على النحو المحدد في طلب التعليقات 5280.

7.1.1 رقم الإصدار

يجب على سلطة الجذر أن تصدر الشهادات بحيث تتفق مع X.509 الإصدار رقم 3.

7.1.2 ملحقات الشهادة

بالإضافة إلى الحقول الأساسية لشهادة X.509 ، يجب على سلطة الجذر إستخدام الحقول الملحقة التالية عند إصدار شهادة:

- إستخدام المفتاح
- نقاط توزيع قائمة الشهادات الملغاة
- سياسات الشهادة

جميع الحقول الملحقة أعلاه يتم وضع علامة عليها بأنها حرجة و ذلك بإستثناء حقول القيود الأساسية التي يجب أن يتم وضع علامة حرجة عليها فقط عندما يكون ملحق إستخدام المفتاح لهذه الشهادة هو التوقيع الرقمي للمفاتيح.

الحقول الملحقة التالية تعتبر إختيارية، يتم إستخدامها باعتبارها ملحقات ليست حرجة:

- معرّف صاحب المفتاح
- معرّف مفتاح السلطة (وتستثنى شهادات سلطة الجذر الموقعة ذاتيا)
- معلومات الوصول لصاحب الشهادة (وتستثنى شهادات سلطة الجذر الموقعة ذاتيا)
- معلومات الوصول للسلطة (وتستثنى شهادات سلطة الجذر الموقعة ذاتيا)

قد تحدد وتستخدم سلطة الجذر ملحق محلي خاص عند الضرورة. حينها، يجب تحديد هذه الحقول الملحقه وتوثيقها في ممارسات التصديق للشهادات. جميع الملحقات المعرّفة الجديدة يتم تصنيفها بأنها غير حرجة.

يرجى الرجوع إلى الملحق (أ) لمزيد من التفاصيل.

7.1.3 معرّف كيان الخوارزمية

يجب على سلطة الجذر إستخدام إحدى الخوارزميات التالية عند التوقيع على شهادات:

خوارزمية التوقيع الرقمي	دالة الخلاصة	معرّف الكيان
التشفير بRSA	SHA256	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
ECDSA	SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ECDSA	SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }

7.1.4 صيغ الأسماء

يجب على سلطة الجذر ملء حقلي صاحب ومُصدر الشهادة في الشهادات التي تصدرها بالأسماء المميزة تبعا لمعيار X.500.

7.1.5 القيود على الاسماء

سلطة الجذر قد تُدرج قيود على الاسماء متى ما كان مناسبا.

7.1.6 معرّف كيان سياسة الشهادات

يجب على سلطة الجذر إدراج معرّف الكيان لسياسة الشهادات الخاصة بها.

7.1.7 إستخدام ملحق قيود السياسة

قد تفرض سلطة الجذر قيود على السياسة متى ما كان مناسبا.

7.1.8 معاني و دلالات ملحق معرِّفات السياسة

قد تُضمّن سلطة الجذر إشعار للمستخدم لعرض بعض المسائل القانونية في شهاداتها.

7.1.9 دلالات معالجة حقول الملحقات الحرجة لسياسات الشهادة

لا شروط.

7.2 وصف قائمة الشهادات الملغاة

يجب على سلطة الجذر إصدار قوائم الشهادات الملغاة بحيث تتفق مع طلب التعليقات 3280.

7.2.1 رقم الإصدار

يجب على سلطة الجذر إصدار قوائم الشهادات الملغاة بحيث تتفق مع قائمة الشهادات الملغاة X.509 الإصدار رقم 2.

7.2.2 الحقول الملحقة و المدخلة لقوائم الشهادات الملغاة

يجب على سلطة الجذر إستخدام الحقول الملحقة التالية لقائمة الشهادات الملغاة:

- رقم قائمة الشهادات الملغاة، والذي يشير إلى الرقم المخصص لقائمة الشهادة الملغاة . ويجب أن يتم تعريف هذا الملحق بانه حرج
- نقطة توزيع الإصدار، للإشارة إلى أن قائمة الشهادات الملغاة تشمل فقط شهادات سلطة التصديق. يجب أن يتم تعريف هذا الملحق بانه حرج
- معرّف مفتاح السلطة، للإشارة إلى معرّف المفتاح المستخدم للتوقيع على قائمة الشهادات الملغاة .يجب أن يتم تعريف هذا الملحق أنه ليس حرج

بالإضافة إلى الحقول الملحقه، يجب على سلطة الجذر إستخدام حقول ملحقة لكل مدخل من الشهادات و سوف تُعلّم على انها المدخلة غير حرجه و هي كالاتي:

- رمز السبب، والذي يوفّر رمز يدل على سبب ظهور الشهادة في هذه القائمة
- مُصدر الشهادة، والذي هو سلطة الجذر
- تاريخ الإلغاء، والذي هو التاريخ الذي كان معروفا قبله أن المفاتيح الخصوصية آمنة

يرجى الرجوع إلى الملحق (ب) لمزيد من التفاصيل.

7.3 وصف بروتوكول التحقق المباشر من حالة الشهادة

قد تدعم سلطة الجذر مجيب بروتوكول التحقق المباشر من حالة الشهادة على النحو المحدد في طلب التعليقات 6960.

7.3.1 رقم الإصدار

إذا تم دعم بروتوكول التحقق المباشر من حالة الشهادة، يجب على سلطة الجذر إستخدام بروتوكول التحقق المباشر من حالة الشهادة الإصدار رقم 1.

7.3.2 ملحقات بروتوكول التحقق المباشر من حالة الشهادة

إذا تم إستخدام بروتوكول التحقق المباشر من حالة الشهادة ، يجب على سلطة الجذر أن تُضمّن الحقل الملحق غير المتكرر لمنع هجوم الإعادة.

8. تدقيق المطابقة والتقييمات الأخرى

8.1 تكرار أو ظروف التقييم

يجب أن تخضع سلطة الجذر لتدقيق سنوي لتحديد إلى أي مدى تعمل سلطة الجذر وفقا للسياسات والممارسات المعلنة.

8.2 هوية / مؤهلات المُقيّم

يجب أن تنفّذ عملية تدقيق المطابقة بواسطة فريق مؤهل. و يتعيّن عليهم أن يكون لديهم المعرفة الكافية في مجال التوقيع الرقمي، و معيار X.509 للبنية التحتية للمفاتيح العمومية إستنادا إلى طلب التعليقات 5280 وسياسة الشهادات، وإطار ممارسات تصديق الشهادات إستنادا إلى قانون السودان للمعاملات الإلكترونية لعام 2007 والتعديلات للقانون للعام 2015 و قواعده و لوائحه.

8.3 علاقة المقيّم بجهة التقييم

يجب أن يكون المدققين محايدون ومستقلون من الجهات التي ينتمي لها المشاركين في نظام سلطة الجذر.

8.4 مواضيع التقييم

تتضمن الموضوعات التي يشملها التقييم ما يلي:

- وثائق سياسة الشهادات و ممارسات وإجراءات التصديق
- السياسات والممارسات ذات الصلة
- مدى فعالية الممارسات والإجراءات المنصوصة

8.5 الإجراءات المتخذة كنتيجة للقصور

سيتم إتخاذ إجراءات تصحيحية لعلاج القصور كنتائج من التقييم.

8.6 الإبلاغ عن النتائج

يجب إنشاء تقرير يصف نتائج التقييم وتقديمها إلى سلطة الجذر و السلطة القومية للمصادقة الإلكترونية.

9. المسائل التجارية والقانونية الأخرى

9.1 القيم المالية

9.1.1 القيمة المالية لإصدار أو تجديد شهادة

قد تتحصل سلطة الجذر على مقابل مادي لإصدار الشهادة و تغيير المفاتيح.

9.1.2 القيم المالية للوصول الى الشهادة

يجب على سلطة الجذر ألّا تتقاضى مقابل مادي من الأطراف المعوّلة مقابل الحصول على أي شهادة أصدرتها.

9.1.3 القيم المالية للحصول على معلومات إلغاء أو حالة الشهادة

لا شروط.

9.1.4 القيم المالية للخدمات الأخرى

لا شروط.

9.1.5 سياسة إسترداد القيم المالية

لا شروط.

9.2 المسئولية المالية

9.2.1 تغطية التأمين

لا شروط.

9.2.2 الأصول الأخرى

لا شروط.

9.2.3 تغطية التأمين أو الضمان للمستخدمين النهائيين

لا شروط.

9.3 سرية معلومات العمل

9.3.1 نطاق المعلومات السرية

أي معلومات حول أعمال سلطة الجذر والمشاركين فيها التي لا تصنّف على أنها محمية أو سرية بموجب هذه السياسة يجوز أن تكون متاحة للعامة لأغراض الشفافية.

9.3.2 معلومات ليست ضمن نطاق المعلومات السرية

كما هو محدد في البند 9.3.1.

9.3.3 مسئولية حماية المعلومات السرية

يجب على جميع المشاركين لسلطة الجذر مسئولية حماية المعلومات السرية الخاصة بهم المنصوص عليها في سياسة الشهادة هذه و وفقا للقوانين المعمول بها.

9.4 خصوصية المعلومات الشخصية

9.4.1 خطة الخصوصية

يجب على سلطة الجذر وجميع المشاركين فيها إنشاء ومتابعة خطة الخصوصية لوصف كيفية التعامل مع المعلومات الشخصية لعملائها.

9.4.2 معلومات تُعتبر خاصة

يجب أن تتم معاملة كل المعلومات الشخصية لسلطة الجذر أو السلطات الوسيطة على أنها خاصة ما لم يحدد غير ذلك في سياسة الشهادات هذه.

9.4.3 معلومات لا تعتبر خاصة

جميع المعلومات الظاهرة في الشهادات الصادرة عن سلطة الجذر لا يجب اعتبارها خاصة.

9.4.4 مسئولية حماية المعلومات الخاصة

يجب على سلطة الجذر والمشاركين فيها مسئولية حماية معلوماتهم الخاصة من الوصول غير المصرح به.

9.4.5 الإخطار والموافقة على إستخدام المعلومات الخاصة

يجب على سلطة الجذر إخطار المشاركين فيها في حال حدوث أي كشف عن معلوماتهم الخاصة تتطلّبتها عملية قضائية أو إدارية.

9.4.6 الكشف وفقا للإجراءات القضائية أو الإدارية

يجب على سلطة الجذر أن تكشف عن المعلومات الخاصة إلى حيث يقتضيه القانون.

9.4.7 ظروف أخرى للإفشاء عن المعلومات

لا توجد ظروف للكشف عن أية معلومات غير تلك الظروف المحددة في 9.4.6.

9.5 حقوق الملكية الفكرية

سلطة الجذر لديها الحق في إثبات ملكيتها الفكرية لما يلي:

- أي منتجات تم تطويرها من خلال مهام معينة ضمن نظام البنية التحتية للمفاتيح العمومية
- أي وثائق للسياسات ، والممارسات والإتفاقيات الداعمة تم تطويرها

9.6 التعهدات والضمانات

9.6.1 تعهدات و ضمانات سلطة الجذر

يجب على سلطة الجذر أن تتعهّد وتضمن في جميع الجوانب المادية أنها تعمل وفقا لمتطلبات سياسة الشهادات الحالية والقوانين المعمول بها. وهذا يشمل ولكن لا يقتصر على ما يلي:

- أن المعلومات الواردة في الشهادات الصادرة ستكون مؤكّده، ودقيقة وكاملة
- أن دورة حياة الشهادات تتوافق مع سياسة الشهادات الحالية و ممارسات تصديق الشهادات
- أن وحدة التأمين المادية المستخدمة لدى سلطة الجذر مستوفية لمتطلبات المعايير الفيزيائية معالجة المعلومات الفيدرالية (FIPS– 140) مستوى 3 أو 4

9.6.2 تعهدات وضمانات السلطة القومية للمصادقة الإلكترونية

يجب على السلطة القومية للمصادقة الإلكترونية أن تتعهّد وتضمن في جميع الجوانب المادية أنها تعمل بالتوافق مع متطلبات سياسة الشهادات الحالية والقوانين المعمول بها. وهذا يشمل ولكن لا يقتصر على ما يلي:

- أن المعلومات المقدّمة لإصدار الشهادة ستكون مؤكدة، ودقيقة وكاملة
- أن دورة حياة الشهادات تتوافق مع سياسة الشهادات الحالية و ممارسات تصديق الشهادات

9.6.3 تعهدات وضمانات السلطات الوسيطة

يجب على السلطات الوسيطة أن تتعهد وتضمن في جميع الجوانب المادية أنها تعمل وفقا لمتطلبات سياسة الشهادات الحالية وإتفاقية السلطات الوسيطة .وهذا يشمل ولكن لا يقتصر على ما يلي:

- أن المعلومات المقدّمة من قِبل السلطة الوسيطة في طلب الشهادة ستكون صحيحة ودقيقة وستبقى صالحة خلال فترة سريان الشهادة، ما لم تُخطر السلطة الوسيطة سلطة الجذر أو السلطة القومية للمصادقة الإلكترونية أن المعلومات الواردة في الشهادة قد تم تغييرها.
- أن يتم إنشاء المفتاح الخصوصي للسلطات الوسيطة بشكل آمن ووفقا لمتطلبات المفاتيح الخصوصية المنصوص عليها في سياسة الشهادات هذه
- أن يتم حماية المفتاح الخصوصي للسلطات الوسيطة من الكشف والإتلاف غير المصرح به أثناء فترة سريان شهادة السلطة الوسيطة.
- أنه في حالة حدوث إختراق للنظام، ستتوقّف السلطة الوسيطة عن استخدام المفتاح الذي تم كشفه وتقديم طلب إلغاء إلى السلطة القومية للمصادقة الإلكترونية
- أن إستخدام السلطة الوسيطة للشهادة سيكون وفقا لمجموعة الإستخدامات الممكنة للمفتاح التي تظهر في الشهادة.

9.6.4 تعهدات و ضمانات الطرف المعوّل

الأطراف المعوّلة الذين يعوّلون على إستخدام الشهادات الصادرة عن سلطة الجذر يجب أن يتعهّدوا ويضمنوا في جميع الجوانب المادية أن يعملوا وفقا لمتطلبات سياسة الشهادات الحالية والأحكام سلطة التصديق الوسيطة سلطة التصديق الوسيطة الأحكام (الشروط العامة). وهذا يشمل ولكن لا يقتصر على ما يلي:

- أن يكون إستخدامه للشهادة وفقا للإستخدامات الظاهرة في الشهادة

- أن يتحقق من توقيع الشهادة إذا كانت وُقّعت بواسطة سلطة الجذر
- أن يتحقق من صلاحية سريان الشهادة
- أن يتحقق من حالة الشهادة ومعرفة ما إذا كان تم إلغائها من قبل سلطة الجذر

9.6.5 تعهدات و ضمانات المشاركين الآخرين

لا شروط.

9.7 إخلاء المسئولية عن الضمانات

سلطة الجذر لا تتحمل أي مسؤولية بإستثناء ما نصّت عليه الإتفاقيات ذات الصلة المتعلقة بإدارة الشهادات.

9.8 حدود المسؤولية

لن تكون سلطة الجذر مسئولة عن أي أضرار للأطراف المعوّلة أو أي أطراف أخرى ناجمة عن سوء إستخدام أو تعويل على الشهادات الصادرة عن سلطة الجذر بصرف النظر عن إذا ما تم إلغاء الشهادة، أو انتهت صلاحيتها، أو تم العبث بها أو تم كشف مفتاحها الخصوصي.

9.9 التعويضات

لا شروط.

9.10 المدة والإنهاء

9.10.1 أجل إعتماد الوثيقة

ستكون سياسة الشهادات هذه فعالة بمجرد إعتمادها من قِبل السلطة القومية للمصادقة الإلكترونية.

9.10.2 إنهاء الخدمة

ستظل سياسة الشهادات هذه فعالة ما لم تحدث إحدى الظروف التالية:

- تمت الموافقة و إعتماد إصدار نسخة حديثة من سياسة الشهادات لسلطة الجذر
- تم إنهاء خدمات سلطة الجذر بواسطة السلطة القومية للمصادقة الإلكترونية

9.10.3 تأثير إنهاء الخدمة و ما تبقى بعد الانهاء

لا شروط.

9.11 الإخطارات الفردية والإتصالات مع المشاركين

يجب أن تكون جميع الإتصالات بين سلطة الجذر والمشاركين فيها من خلال إحدى الوسائل التالية:

- خطاب كتابي مختوم بختم مناسب
- خطاب إلكتروني موقّع رقميا

يجب أن تُرسل البيانات التي يتم تصنيفها على أنها سرية بطريقة مشفّرة على النحو المتفق عليه مع المشاركين.

9.12 التغييرات

9.12.1 إجراء التغيير

يجب على السلطة الجذر مراجعة سياسة الشهادات بصورة دورية. قد يقترح أي من المشاركين تغييرات لسياسة الشهادات. يجب أن تراجع السلطة القومية للمصادقة الإلكترونية التغييرات المقترحة ومن ثم يتم إعتماد المخرجات قبل أن تُنشر في المستودعات العامة. ويجب أن يتم كتابة رقم الإصدار وتاريخ الإعتماد في الوثائق المعدّلة.

يجب وضع ضوابط لمنع التعديلات غير المصرح بها لسياسة الشهادات و ممارسات التصديق المقابلة لها.

9.12.2 آلية الإخطار ومدته

قد تُخطِر سلطة الجذر المشاركين بسياسة الشهادات المُقترحة، وذلك عن طريق إرسال بريد إلكتروني موقّع إلكترونيا ومحدّد فيه الموعد النهائي لتلقّي التعليقات .وبمجرد الموافقة عليها وإعتمادها، يجب أن يتم نشرها في المستودعات العامة.

9.12.3 الظروف التي تتوجّب تغيير رقم معرّف الكيان

السلطة القومية للمصادقة الإلكترونية هي الطرف الذي يحدد ما إذا كان يجب تغيير معرّف الكيان.

9.13 أحكام تسوية المنازعات

يجب أن يتم وصف سياسة وممارسات تسوية المنازعات بواسطة السلطة القومية للمصادقة الإلكترونية.

9.14 القانون الحاكم

تخضع سياسة الشهادات هذه لقانون المعاملات الإلكترونية لعام 2007 و التعديلات للقانون للعام 2015 و قواعده و لوائحه.

9.15 الإمتثال للقانون المعمول به

يتعيّن على سلطة الجذر والمشاركين فيها الإمتثال لأي قوانين معمول بها.

9.16 أحكام متنوعة

9.16.1 مجمل الإتفاقية

لا شروط.

9.16.2 التعيين

يجب على كل الجهات التي تعمل وفقا لسياسة الشهادات هذه عدم تخصيص واجباتها أو مسئولياتها إلى أي طرف ثالث دون الحصول على إذن موقّع من السلطة القومية للمصادقة الإلكترونية.

9.16.3 قابلية التنفيذ

إذا تم تحديد أي بند من سياسة الشهادات هذه أنه غير صحيح أو غير صالح فانه لن يؤثر على بقية البنود الأخرى من هذه السياسة و ستكون سارية المفعول حتى يتم تحديث هذه السياسة . وصف عملية التحديث لسياسة الشهادات محدد في البند 9.12.

9.16.4 الإنفاذ (أتعاب المحاماة والتنازل عن الحقوق)

لا شروط.

9.16.5 القوة القاهرة

تعرّف سلطة الجذر وقوع أي أحداث خارجة عن تحكمها بإسم القوة القاهرة. لن تتحمل السلطة القومية للمصادقة الإلكترونية وسلطة الجذر أية مسئولية عن أي خرق للضمان أو تأخير أو خلل في الآداء الذي ينتج عن أحداث القوة القاهرة مثل، ولكن لا تقتصر على ما يلي:

- أعمال الحروب
- أعمال الإرهاب
- الإضرابات
- الكوارث الطبيعية والأوبئة
- فشل من الموردين أو البائعين في آداء إلتزاماتهم
- فشل في شبكة الإنترنت أو غيرها من البنى التحتية
- أي كوارث طبيعية أخرى أو كوارث من صنع الإنسان

9.17 أحكام أخرى

لا شروط.

APPENDEX

A. Certificate Profile

A.1 Root CA

X.509 Field	Possible Value	Is Critical
Version	3	Yes
Serial Number	<Generated from Certificate Manufacturing Software>	
Signature Algorithm	SHA512WithRSA	Yes
Issuer	CN = Sudan National Root CA1 OU=Root CA O = National Authority for Digital Certification C=SD	Yes
Validity –Not Before	<Approved Issuance Date>	Yes
Validity –Not After	<Approved Issuance Date + 20 years>	Yes
Subject	CN = Sudan National Root CA1 OU=Root CA O = National Authority for Digital Certification C = SD	Yes
Subject Public Key	<pubic key of the root CA key that should be the first certification point for Sudan PKI>	Yes
Key Usage	Certificate Singing CRL Signing	Yes
CRL Distribution Point	http://crl.nadc.gov.sd/sudannationalrootca1.crl	Yes
Certificate Policies	2.16.729.1.1.1.1.1	Yes
Certificate Basic	<Is a Certificate Authority with unlimited length of intermediate CAs	Yes if Key

Constrains	(if Key Certificate Signing)>	Certificate Signing is used
Subject Key Identifier	<160-bit SHA-1 hash of the value of the Subject Public Key (excluding the tag, length, and number of unused bits)>	No

A.2 Intermediate CA

X.509 Field	Possible Value	Is Critical
Version	3	Yes
Serial Number	<Generated from Certificate Manufacturing Software>	
Algorithm ID	RSA-SHA256	Yes
	ECDSA- SHA256	
	ECDSA- SHA384	
Issuer	CN= Sudan National Root CA1 OU=Root CA O = National Authority for Digital Certification C=SD	Yes
Validity –Not Before	<Approved Issuance Date>	Yes
Validity –Not After	<Approved Issuance Date + 10 years>	Yes
Subject	CN = < Intermediate CA Name> OU= Intermediate CA O = National Authority for Digital Certification C = SD	Yes
Subject Public Key	<pubic key of the subject that needs to be certified>	Yes
Key Usage	Certificate Singing	Yes
	CRL Signing	

CRL Distribution Point	<http/ldap:url>	Yes
Certificate Policies	<Intermediate CA certificate policy OID>	Yes
Certificate Basic Constrains	<it is a Certificate Authority with unlimited length of intermediate CAs (if Key Certificate Signing)>	Yes if Key Certificate Signing is used
Subject Key Identifier	<160-bit SHA-1 hash of the value of the Subject Public Key (excluding the tag, length, and number of unused bits)>	No
Subject Information Access	<OCSP responder URL location>	No
Authority Key Identifier	<160-bit SHA-1 hash of the value of the Root CA Public Key of the corresponding private key that is used to sign this certificate(excluding the tag, length, and number of unused bits)>	No

B. CRL Profile

X.509 Field	Possible Value	Note
Version	2	Basic Field
Revoked Certificates	<List of revoked certificates>	Basic Field
Signature Algorithm	SHA512WithRSA	Basic Field
Signature Value	<Signature of this CRL>	Basic Field
Issuer Name	CN = Sudan National Root CA1 OU = Root CA O = National Authority for Digital Certification C = SD	Basic Field
This Update	<Approved Issuance Date>	Basic Field
Next Update	<Approved Issuance Date + 12 months>	Basic Field
CRL Number	<counter of CRL number>	Non Critical Extension
Issuing Distribution Point	< Indicates that this CRL for CA certificates only>	Critical Extension
Authority Key Identifier	<160-bit SHA-1 hash of the value of the Root CA Public Key of the corresponding private key that is used to sign this CRL(excluding the tag, length, and number of unused bits)>	Non Critical Extension
Reason Code	<Reasons of revoking the certificate in this list. Reasons based on 5.3.1 in RFC 5280>	Entry Non Critical Extension
Invalidity Date	<The date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid>	Entry Non Critical Extension
Certificate Issuer	CN = Sudan National Root CA1 OU = Root CA O = National Authority for Digital Certification C=SD	Entry Non Critical Extension