ETAT-MAJOR

POLITIQUE DE CERTIFICATION

DE LA HIERARCHIE DES AUTORITES DE CERTIFICATION « SDIS DE LA DROME »

Contenu du document

Le présent document définit la politique de certification de l'ACR « SDIS DE LA DROME – Racine de confiance RGS » et des AC « SDIS DE LA DROME – Autorité secondaire personnels » et « SDIS DE LA DROME – Autorité secondaire infrastructure » mises en place dans le cadre de l'infrastructure de gestion de clés cryptographiques déployée au sein des systèmes d'information du service.

Suivi du document

Action	Version	Date	Auteur
Création du document	v1.0	Mai 2014	Col E. JUGGERY
Validation du document	v1.0	Octobre 2014	Col E. JUGGERY
Modification du document (remplacement URL accès informations publiques IGC)	v1.1	Avril 2017	Col E. JUGGERY

1. INTRODUCTION

1.1. Présentation générale

Pour assurer la sécurité des échanges d'informations au format numérique entre l'administration et les usagers, entre l'administration et ses agents, ainsi qu'entre les administrations, le service départemental d'incendie et de secours de la Drôme (SDIS) met en place une infrastructure de gestion de clés (IGC) afin de gérer l'ensemble des certificats et bi-clés correspondants.

Au sein de cette IGC, les certificats porteurs sont émis par des autorités de certification secondaires (AC) dites « en ligne ». Ces AC en ligne sont elles-mêmes signées par une autorité de certification racine (ACR) dite « hors ligne » qui permet de les authentifier.

Ainsi, les chaînes de certificats issues de l'IGC du SDIS de la Drôme possèdent la structure suivante:

- Certificat ACR (AC « hors ligne ») : certificat électronique auto-signé de la racine ;
- Certificat d'AC (AC « en ligne »): certificat électronique délivré à une AC par l'ACR ;
- Certificat porteur : certificat électronique délivré à un porteur par une AC « en ligne ».

La présente politique de certification (PC) a pour objet de décrire la gestion du cycle de vie des certificats et bi-clés :

- de l'ACR « SDIS DE LA DROME – Racine de confiance RGS »
- de l'AC « SDIS DE LA DROME – Autorité secondaire personnels »
- de l'AC « SDIS DE LA DROME – Autorité secondaire infrastructure ».

L'objectif de cette politique de certification est de définir les engagements minimum que le SDIS de la Drôme doit respecter dans la délivrance et la gestion des certificats et de leurs bi-clés tout au long de leurs cycles de vie.

Elle est conforme au RFC 3647 « X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement Framework » de l'Internet Engineering Task Force (IETF).

Elle répond également aux préconisations du référentiel général de sécurité (RGS).

1.2. Identification du document

La présente PC est dénommée « politique de certification de la hiérarchie des autorités de certification "SDIS DE LA DROME" » dans sa version 1.0 et elle est identifiée par son numéro d'identifiant d'objet (OID). D'autres éléments, plus explicites, comme par exemple le nom, numéro de version, date de mise à jour permettent également de l'identifier.

La branche d'OID du SDIS de la Drôme, {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 39953}, est enregistrée auprès de l'Internet Assigned Numbers Authority (IANA).

Le numéro d'OID attribué par le SDIS de la Drôme à la présente PC est 1.3.6.1.4.1.39953.1.1.1

1.3. Entités intervenant dans l'IGC

1.3.1. Autorités de certifications

Le SDIS de la Drôme, notamment pour garantir la cohérence avec le référentiel général de sécurité, définit ses exigences de sécurité au sein de la présente politique de certification afin de délivrer des certificats aux porteurs.

Les AC ont en charge la fourniture de prestations de gestion des certificats. Ces prestations de l'AC sont le résultat de la mise en œuvre de différentes fonctions de l'infrastructure de gestion de clés (IGC) qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats (génération, diffusion, renouvellement, révocation,...).

Dans le cas de la présente politique de certification, les agents du SDIS de Drôme concernés mettent en œuvre les fonctions suivantes :

- Génération des bi-clés et certificats d'AC : permet de générer la bi-clé d'AC (ACR et AC secondaires) et le certificat électronique correspondant ;

- Révocation de certificat : traite les demandes de révocation d'un certificat d'AC et détermine les actions à mener, dont la génération de la Liste d'AC révoquée (LAR) ;

- Publication : permet de mettre à disposition des porteurs et des utilisateurs de certificat les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales, politiques de certification publiées par l'AC, certificats d'AC …), ainsi que les informations sur l'état des certificats (LAR, OCSP, …).

1.3.2. Porteurs de certificats

Est considéré comme porteur toute entité détentrice d'une bi-clé et d'un certificat associé délivrés par l'une des AC secondaires du SDIS de la Drôme.

S'agissant de l'ACR, les porteurs de certificats sont essentiellement les autorités de certifications secondaires « en ligne ». Des certificats, en nombre limités, peuvent également être émis par l'ACR pour les besoins des composants techniques de cette partie de l'IGC, notamment pour le contrôle et l'activation des clés de l'ACR.

1.3.3. Utilisateurs de certificats (UC)

Application, personne physique ou morale, organisme administratif ou système informatique matériel qui utilise un certificat délivré par une AC du SDIS de la Drôme, afin de valider les fonctions de sécurité mises en œuvre à l'aide de ces certificats (signature, chiffrement et authentification).

1.3.4. Entités d'audit ou de qualification

Entités amenées à auditer tout ou partie de l'IGC à la demande des autorités gouvernementales pour contrôler ou qualifier cette infrastructure.

1.4. Usage des certificats d'AC

1.4.1. Domaines d'utilisation applicables

La présente PC concerne :

- La bi-clé et le certificat de signature de l'ACR autosigné qui ont vocation à signer les certificats des AC secondaires et les listes de certificats d'autorités révoqués.

- Les bi-clés et les certificats de signature des AC secondaires, signés par l'ACR, qui ont vocation à signer pour chaque AC les certificats porteurs, les listes de certificats porteurs révoqués (LCR) et les vérifications en ligne d'état des certificats (OCSP)

1.4.2. Domaines d'utilisation interdits

La bi-clé ne doit être utilisée que pour signer les objets définis ci-dessus. Elle ne doit notamment être utilisée ni à des fins de confidentialité, ni à des fins d'authentification.

Les utilisations de certificats d'AC à d'autres fins que celles prévues par la présente PC ne sont pas autorisées. Cela signifie que le SDIS de la Drôme ne peut être en aucun cas être tenu pour responsable d'une utilisation des certificats d'AC qu'il émet autre que celles prévues dans la présente PC.

Les certificats d'AC ne peuvent être utilisés que conformément aux lois en vigueur et applicables, en particulier seulement dans les limites autorisées par les lois sur l'importation et l'exportation.

1.5. Gestion de la politique de certification

1.5.1. Entité gérant la PC

Le SDIS de la Drôme est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC. A cette fin, il statue autant que de besoin sur la nécessité d'apporter des modifications à la PC.

1.5.2. Point de contact

Toute demande d'informations concernant ce document devra être transmise à :

Service départemental d'incendie et de secours de la Drôme

235 route de Montélier

B.P 147

26905 VALENCE Cedex 9

1.6. Définitions et acronymes

1.6.1. Acronymes

AA	Autorité Administrative
AC	Autorité de certification
ACR	Autorité de certification Racine
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information
CGU	Conditions Générales d'Utilisation
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
IGC	Infrastructure de Gestion de Clés
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LAR	Liste des certificats d'AC Révoqués
LCR (ou CRL)	Liste des Certificats Révoqués (ou Certificate Revocation List)
OC	Opérateur de certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de certification
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adleman
RSSI	Responsable de la Sécurité des Systèmes d'Information
SDIS	Service Départemental d'Incendie et de Secours
SHA-256	Secure Hash Algorithm 256
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
UC	Utilisateur de Certificats
URL	Uniform Resource Locator

1.6.2. Définitions

Agent - personne physique agissant pour le compte d'une autorité administrative.

Applications utilisatrices - services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat ou des besoin d'authentification ou de cachet du serveur auquel le certificat est rattaché.

Autorités administratives - désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité de certification (AC) – autorité à qui un ou plusieurs utilisateurs se fient pour créer et attribuer des certificats. Facultativement, l'autorité de certification peut créer les clés d'utilisateur. L'Autorité de Certification a en charge l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification.

Autorité d'enregistrement (AE) – entité qui vérifie les données propres au porteur. L'AE est une composante de l'IGC qui dépend d'au moins d'une Autorité de certification. L'AE a pour fonction de réceptionner et de traiter les demandes d'émission de certificat.

Bi-clé – couple composé d'une clé privée devant être conservée secrète par le porteur et d'une clé publique associée nécessaire à la mise en œuvre de dispositifs de cryptologie basés sur des algorithmes asymétriques.

Cérémonie de clés – procédure par laquelle une bi-clé d'AC est générée, sa clé privée transférée et éventuellement sauvegardée, sa clé publique certifiée.

Certificat électronique – fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Certificat d'AC – certificat pour une AC émis par une autre AC d'un rang supérieur dans la chaîne de certification.

Certificat d'AC racine – certificat d'AC signé par la clé privée de cette même AC.

Clé privée – clé de la bi-clé asymétrique d'un porteur qui doit être uniquement utilisée par cette entité.

Clé publique – clé de la bi-clé asymétrique d'un porteur qui peut être rendue publique.

Composante - plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC.

Compromission – violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.

Confidentialité – La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus.

Déclaration des Pratiques de Certification (DPC) – une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Dispositif d'authentification - Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre sa clé privée d'authentification.

Données d'activation – valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un PIN, une phrase secrète, …).

Fonction de hachage – fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux trois propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie;
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie;
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Infrastructure de gestion de clés (IGC) – ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Elle permet de produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués ainsi que la base dans laquelle les certificats et les LCR doivent être publiés.

Liste de Certificats Révoqués (LCR) – liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Modules cryptographiques – ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé …). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS ou critères communs), utilisé pour conserver et mettre en œuvre la clé privée AC.

Période de validité d'un certificat – période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat.

Public-Key Cryptography Standard #10 (PKCS #10) – standard mis au point par RSA Security Inc. qui définit la structure d'une Requête de Signature de Certificat (en anglais: Certificate Signing Request: CSR).

Politique de Certification (PC) – ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Porteur de secret – personne qui détient une des données d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

Produit de sécurité – dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

RSA – algorithme de cryptographique à clé publique inventé par Rivest, Shamir, et Adleman.

Système d'information – ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives. Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

Validation de certificat électronique – opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une autorité de certification (AC) et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC et la vérification de la signature électronique de l'ensemble des AC contenues dans le chemin de certification. Elle inclue également la validation du certificat de l'ensemble des AC du chemin de certification. La validation d'un certificat électronique nécessite au préalable de choisir le certificat auto-signé qui sera pris comme référence.

2. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1. Entités chargées de la mise à disposition des informations

Le SDIS de la Drôme met en œuvre au sein de son IGC un service de publication en charge de la diffusion du présent document et de tout autre document ou informations permettant d'assurer l'information des porteurs et des utilisateurs de certificats et la bonne utilisation des certificats délivrés au titre de la présente PC.

2.2. Informations publiées

Le SDIS de la Drôme publie, à destination des porteurs et des utilisateurs de certificat les informations suivantes:

- La présente PC ;
- Le certificat de l'ACR et les certificats des AC secondaires ;
- Les listes de certificats révoqués de l'ACR et des AC secondaires

Ces informations sont accessibles par internet sur le site http://www.sdis26.fr, rubrique « pratique et utile », section « IGC »

2.3. Délais et fréquences de publication

La présente PC et les informations liées à l'IGC, le certificat de l'ACR et les certificats des AC secondaires, les listes de certificats révoqués sont publiés 24 heures sur 24, 7 jours sur 7.

Les modifications de ces éléments sont actualisées sous 24 heures afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures de l'AC.

La durée maximale d'indisponibilité du service de publication par interruption de service (panne ou maintenance) est de 2h et une durée totale maximale d'indisponibilité par mois de 8h devra être assurée, ceci hors cas de force majeure.

2.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication de l'ensemble des informations, notamment d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux agents habilités de l'IGC.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Nommage

3.1.1. Types de noms

Les identités utilisées dans un certificat délivré par l'ACR sont décrites conformément aux spécifications de la norme X.500. Dans chaque certificat, l'ACR (issuer) et le porteur (subject) sont identifiés par un « Distinguished Name » DN de type X.501.

L'identité de l'ACR dans le certificat de l'ACR est :

Champ de base	Valeur
Issuer DN Subject DN	CN = SDIS DE LA DROME - Racine de confiance RGS O = SERVICE DEPARTEMENTAL D INCENDIE ET DE SECOURS DE LA DROME OU = 0002 <espace> 282612001 L = VALENCE S = DROME C = FR E = sic@sdis26.fr DC = sdis26 DC = local

L'identité des AC secondaires dans le certificat d'AC sont :

Champ de base	Valeur
Issuer DN	CN = SDIS DE LA DROME - Racine de confiance RGS O = SERVICE DEPARTEMENTAL D INCENDIE ET DE SECOURS DE LA DROME OU = 0002 <espace> 282612001 L = VALENCE S = DROME C = FR E = sic@sdis26.fr DC = sdis26 DC = local
Subject DN	CN = SDIS DE LA DROME - Autorite secondaire personnels O = SERVICE DEPARTEMENTAL D INCENDIE ET DE SECOURS DE LA DROME OU = 0002 <espace> 282612001 L = VALENCE S = DROME C = FR E = sic@sdis26.fr

Champ de base	Valeur
Issuer DN	CN = SDIS DE LA DROME - Racine de confiance RGS O = SERVICE DEPARTEMENTAL D INCENDIE ET DE SECOURS DE LA DROME OU = 0002 <espace> 282612001 L = VALENCE S = DROME C = FR E = sic@sdis26.fr DC = sdis26 DC = local
Subject DN	CN = SDIS DE LA DROME - Autorite secondaire infrastructure O = SERVICE DEPARTEMENTAL D INCENDIE ET DE SECOURS DE LA DROME OU = 0002 282612001 L = VALENCE S = DROME C = FR E = sic@sdis26.fr DC = sdis26 DC = local

3.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats émis conformément à la présente PC sont explicites.

3.1.3. Règles d'interprétation des différentes formes de nom

L'identité utilisée pour les certificats d'AC n'est ni un pseudonyme ni un nom anonyme.

3.1.4. Règles d'interprétation des différentes formes de nom

Les utilisateurs de certificat et les porteurs peuvent se servir des certificats d'AC contenus dans les chaînes de certification autorisées (voir § 1.4.1 ci-dessus), pour mettre en œuvre et valider des fonctions de sécurité en vérifiant entre autres les identités (DN) des AC telles que contenues dans les certificats d'AC.

3.1.5. Unicité des noms

Les identités contenues dans les certificats d'AC sont uniques au sein de la chaîne de certification.

Le SDIS de la Drôme s'assure de cette unicité lors de la création du certificat d'AC par l'ACR.

3.1.6. Identification, authentification et rôle de marques déposées

La présente PC ne formule pas d'exigence spécifique sur le sujet.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

La preuve de la possession de la clé privée par l'AC est assurée par la génération d'une bi-clé lors de la phase préalable à l'émission du certificat signé par l'ACR durant la même cérémonie de clés.

3.2.2. Validation des identités

La présente PC couvre uniquement des certificats d'AC du SDIS de la Drôme.

3.2.3. Informations non vérifiées du porteur

Aucune information non vérifiée n'est introduite dans les certificats d'AC.

3.2.4. Validation de l'autorité du demandeur

Les AC dépendent uniquement du SDIS de la Drôme et les cérémonies de clés ne peuvent être demandées que par le SDIS de la Drôme.

3.2.5. Critère d'interopérabilité

Le SDIS de la Drôme gère les demandes d'accords et les accords de reconnaissance avec des AC extérieures de son IGC.

Toutefois, de tels accords ne seront réalisés que si l'AC rattachée est en conformité avec le RGS.

3.3. Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé d'une AC entraîne automatiquement la génération et la fourniture d'un nouveau certificat d'AC.

3.3.1. Identification et validation pour un renouvellement courant

Les vérifications relatives au renouvellement d'une bi-clé sont effectuées conformément aux procédures initiales.

3.3.2. Identification et validation pour un renouvellement après révocation

Les vérifications relatives au renouvellement d'une bi-clé après révocation du certificat de clé publique correspondant sont effectuées conformément aux procédures initiales.

3.4. Identification et validation d'une demande de révocation

Les demandes de révocation d'un certificat d'AC, qu'elles soient dues à une suspicion de compromission de clé, de perte ou de vol sont authentifiées par le SDIS de la Drôme.

La validation entraîne la révocation du certificat, l'émission et la publication immédiate d'une nouvelle liste de certificats révoqués.

4. EXIGENCES OPERATIONNELS SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. Demande d'un certificat d'AC

4.1.1. Origine d'une demande de certificat d'AC

Lorsqu'une nouvelle AC « en ligne » doit être crée, une demande de création est prise en compte par les agents concernés du SDIS de la Drôme.

4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat d'AC

La demande est établie par le service concerné et elle comprendra notamment les éléments d'identification de cette nouvelle AC.

4.2. Traitement d'une demande de certificat d'AC

4.2.1. Exécution des processus d'identification et de validation de la demande

La direction générale du SDIS de la Drôme valide la mise en œuvre de l'AC et la demande de certificat d'AC.

4.2.2. Acceptation ou rejet de la demande

La direction générale du SDIS de la Drôme autorise ou rejette la création d'un certificat d'AC.

En cas d'acceptation, la demande est transmise aux opérateurs de l'ACR afin de procéder à la cérémonie des clés de création du certificat.

4.2.3. Durée de traitement d'une demande de certificat d'AC

La durée maximale de traitement d'une demande de certificat d'AC est fixée à 7 jours.

4.3. Délivrance du certificat d'AC

4.3.1. Actions de l'ACR concernant la délivrance d'un certificat d'AC

L'AC « en ligne » est générée pendant une cérémonie de clés organisée par le SDIS de la Drôme.

Le certificat de l'AC est signé par l'ACR pendant cette cérémonie.

4.3.2. Notification de l'émission d'un certificat d'AC

La notification est effectuée directement lors de la cérémonie de clés.

4.4. Acceptation du certificat d'AC

4.4.1. Démarche d'acceptation du certificat

L'acceptation du certificat est considérée comme tacite dès lors que cette opération est réalisée par l'intégration de celui-ci lors de la cérémonie de clés.

4.4.2. Publication du certificat d'AC

Le certificat d'AC est publié dans l'annuaire de l'IGC après son installation et il est également mis à disposition des porteurs et des utilisateurs de certificats sur le site http://www.sdis26.fr, rubrique « pratique et utile », section « IGC »

4.4.3. Notification par l'ACR aux autres entités de la délivrance du certificat d'AC

La notification est réalisée par la mise à jour des informations du service de publication.

4.5. Usages de la bi-clé et du certificat d'AC

4.5.1. Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée de l'AC et du certificat associé par l'AC est strictement limitée au service d'autorités de certification subordonnées de niveau 1.

Les AC doivent respecter strictement les usages autorisés des bi-clés et des certificats.

L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés.

4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Les certificats d'AC composant la chaîne de certification du SDIS de la Drôme ne peuvent être utilisés par un utilisateur de certificat qu'à des fins de validation d'une chaîne de confiance.

Il est de la seule responsabilité de l'utilisateur de certificat de s'assurer de la validité des certificats délivrés par l'ACR ou l'AC à l'aide des listes de certificats d'autorité révoquées publiés.

4.6. Renouvellement d'un certificat d'AC

La demande de renouvellement d'un certificat d'AC nécessite le changement de la bi-clé de l'AC en même temps que la délivrance du nouveau certificat.

4.7. Délivrance d'un nouveau certificat d'AC suite à changement de la bi-clé

Les bi-clés doivent être périodiquement renouvelées :

- selon les recommandations émises par l'ANSSI en matière de cryptanalyse, afin de minimiser les possibilités d'attaques cryptographiques,
- pour que l'ACR puisse continuer à délivrer des certificats d'AC d'une durée constante,
- en cas de compromission, suspicion de compromission, vol, dysfonctionnement ou perte des moyens de reconstruction de la clé privée de l'AC.

Le changement de bi-clé entraîne alors le changement de certificat et la procédure à suivre est identique à la procédure initiale de certification.

4.8. Modification d'un certificat d'AC

La modification d'un certificat d'AC n'est pas autorisée par la présente PC.

4.9. Révocation et suspension d'un certificat d'AC

Le SDIS de la Drôme ne prévoit pas que les certificats d'AC puissent être suspendus et la révocation est abordée ci-après.

4.9.1. Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC et notamment un certificat d'AC :

- changement d'information nécessaire dans le certificat ;
- cessation d'activité de l'ACR ou de l'AC ;
- suspicion de compromission, compromission, perte ou vol de la clé privée de l'AC ou de l'ACR ou des moyens de reconstitution de la clé privée de l'AC ou de l'ACR ;
- non-respect de la politique de certification et de la déclaration des pratiques de certification de l'ACR ou de l'AC ;
- obsolescence des procédés de cryptographie utilisés au regard des exigences du RGS.

4.9.2. Origine d'une demande de révocation

La révocation d'un certificat d'AC ne peut être décidée que par le SDIS de la Drôme, ou par les autorités judiciaires via une décision de justice.

4.9.3. Procédure de traitement d'une demande de révocation

La demande de révocation est transmise aux opérateurs de l'ACR afin de révoquer le certificat concerné.

L'ACR informera dans les plus brefs délais et par tout moyen, si possible par anticipation, l'ensemble des porteurs concernés que leurs certificats ne sont plus valides. Une notification sera également publiée sur le site internet dédié à l'IGC.

4.9.4. Délai accordé au porteur pour formuler la demande de révocation

Dès qu'une personne autorisée a connaissance qu'une des causes possibles de révocation est avérée, il formule sa demande de révocation sans délai.

4.9.5. Délai de traitement par l'AC d'une demande de révocation

La révocation d'un certificat de l'ACR ou de l'AC doit être effectuée dans les meilleurs délais par le service de révocation, particulièrement dans le cas de la compromission de la clé.

La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat d'AC est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LAR, OCSP…) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

4.9.7. Fréquence d'établissement des LAR

La liste ces certificats d'autorités révoqués est émise tous les ans. En cas de révocation d'AC, cette liste est publiée dès qu'elle est générée.

4.9.8. Délai maximum de publication d'une LAR

La liste des certificats d'autorités révoqués doit être publiée dans un délai maximum de trente minutes suivant sa génération.

4.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Le service OCSP mis en œuvre par le SDIS de la Drôme au sein de l'IGC respecte les exigences de disponibilité et de délai de publication décrits aux § 4.9.7 et au § 4.9.8

4.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Voir paragraphe précédent.

4.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet

4.9.12. Exigences spécifiques en cas de compromission de la clé privée

En cas de compromission de la clé privée d'une AC, outre les exigences prévues au § 4.9.3, le SDIS de la Drôme interrompra immédiatement et définitivement l'usage de cette clé privée et de son certificat associé.

4.10. Fonction d'information sur l'état des certificats

4.10.1. Caractéristiques opérationnelles

L'information sur l'état des certificats est mise à la disposition des utilisateurs de certificats par la consultation libre des listes de certificats révoqués, au format v2, publiées sur le site internet http://www.sdis26.fr, rubrique « pratique et utile », section « IGC ». Ces LCR sont également utilisées par le service OCSP.

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.

Le SDIS de la Drôme veille à ce que cette fonction ait une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h et une durée maximale totale d'indisponibilité de 8h par mois.

4.11. Fin de la relation entre l'ACR et l'AC

Sans objet.

4.12. Séquestre et recouvrement de clés

Les bi-clés et les certificats d'AC émis conformément à la présente PC ne font pas l'objet de séquestre ni de recouvrement.