AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

IGC-CPS2bis

Gabarits des certificats X.509

des Classes 4, 5 et 6

21 mars 2012

Version 3.0

SOMMAIRE

1. Introduction

Ce document détaille les Certificats X.509 de clés publiques et les CRLs (Certification Revocation Lists) de l'**IGC-CPS2bis** ; c'est une mise à jour de :

« CPS2bis Certificats X-509 » version 2.1 du 14 décembre 2001

Il ne contient plus la description des certificats CPS des Classes 0 à 3 car ces certificats sont aujourd'hui gérés par l'IGC-CPS2ter.

Documents de référence de l'ASIP-Santé.

Politiques de Certification (PC)

Dernière version disponible sur le site WEB de L'ASIP-Santé.

Standards applicables

RFC 2459	Internet X.509 Public Key Infrastructure : Certificate and CRL Profile
ISO 9594-8	Information Technology – Open Systems Interconnection – The directory : authentication framework (également ITU-T recommandation X.509)
ISO 9834-1	Information Technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities

2. Symboles

0 à 9	caractères décimaux
'0' à '9' et 'A' à 'F' :	caractères hexadécimaux
'xxx'	chaîne de caractères hexadécimaux
"ABC"	chaîne de caractères alpha-numériques
<réf.>	référence vers une table de codification ou l'origine de données

α-num	1 caractère alpha-numérique est constitué de 8 bits codé conforme ISO 8859-1.
alpha	1 caractère alphabétique est constitué de 8 bits codé conforme ISO 8859-1.
bool	1 booléen occupe 1 bit.
bcd	1 caractère bcd est constitué de 4 bits.
hex	1 caractère hexadécimal est constitué de 4 bits.
oct	1 octet est constitué de 8 bits.

||	concaténation
≠	différent
[ ]	paramètre optionnel

3. Abréviations

AC	Autorité de Certification
AE	Autorité d'Enregistrement
CDE	Carte de Directeur d'Etablissement
CPA	Carte de Personnel Autorisé
CPE	Carte de Personnel d'Etablissement
CPF	Carte de Professionnel de Santé en Formation
CPS	Carte de Professionnel de Santé
CSA	Carte de Service Applicatif (type de carte abandonné)
CRL	Certificate Revocation List (liste de révocation de certificats)
DN	Distinguished Name
ICP	Infrastructure de Clés Publiques
IGC	Infrastructure de Gestion de Clés
KP	Clé Publique
PC	Politique de Certification
RDN	Relative Distinguished Name

4. Format des Certificats X.509 du Système CPS

4.1 Présentation d'un certificat X.509 version 3

4.1.1 Les champs de base

Les champs de base d'un certificat renseignent les informations suivantes :

- version
- numéro de série
- informations sur la signature du certificat par l'Autorité de Certification (algorithmes et paramètres)
- nom du fournisseur du certificat
- période de validité du certificat
- nom du porteur de certificat
- informations sur la clé publique (valeur de la clé publique, algorithme et paramètres)
- les extensions de certificat

4.1.2 Extensions de certificat

La possibilité d'ajouter des extensions à un certificat a été créée par la version 3 de la norme [ISO 9594-8].
Une implémentation de la norme choisira parmi les extensions proposées celles qui sont pertinentes pour son application et les ajoutera aux champs de base du certificat.

La séquence d'extension(s) adjointe aux champs de base du certificat est une collection d'éléments dont le cardinal peut être nul. Par conséquent, un certificat X.509v3 peut ne contenir aucune extension.

Si la norme définit plusieurs types d'extensions, d'autres extensions, dites « privées » peuvent être ajoutées pour correspondre aux besoins d'une implémentation particulière.

Chacune de ces extensions est caractérisée par trois informations :

- l'identifiant de l'extension considérée, donné par la norme,
- le fait qu'elle soit critique ou non,
- la valeur de l'extension, propre à un certificat.

4.1.3 Les différents types d'extension

Les extensions de certificat permettent de spécifier plus précisément les caractéristiques suivantes :

- informations sur les clés,
- informations sur les politiques de certification,
- fournisseur et porteur de certificat,
- contraintes sur le chemin de certification.

Des extensions spécifiques peuvent être définies à travers une recommandation de l'ITU-T ou par un organisme qui en exprime le besoin. L'identificateur de l'objet qui identifie une extension peut alors être défini selon la procédure décrite dans la norme [ISO 9834-1].

4.1.4 Les extensions critiques et non-critiques

Une extension non-critique (indicateur de criticité = FAUX) est **informative** ; une application peut ignorer les extensions non-critiques dont elle ne connaît pas la signification.

Une extension critique (indicateur de criticité = VRAI) est **restrictive** (correspond à une contrainte liée à la validité du certificat ou une restriction de l'utilisation de la clé certifiée) ; une application traitant un certificat contenant une extension critique dont elle ne connaît pas la signification doit le refuser.

4.1.5 Schéma du contenu d'un certificat X.509 version 3

CERTIFICAT

Contenu du certificat (Données certifiées)

Version 3		
Numéro de série du certificat		
Informations sur la signature du certificat par l'AC (algorithmes et paramètres)		
Nom du fournisseur du certificat		
Période de validité du certificat		
Nom du porteur de certificat		
Informations sur la clé publique (valeur de la clé publique, algorithme et paramètres)		
Extensions du Certificat		
Identifiant du type de l'extension	Criticité (oui / non)	Valeur
Identifiant du type de l'extension	Criticité (oui / non)	Valeur
Identifiant du type de l'extension	Criticité (oui / non)	Valeur
…		

Algorithme de signature du certificat par l'AC

Algorithmes
Paramètres

Signature numérique du contenu du certificat

Valeur de la signature numérique du certificat par l'AC

4.2 Les identifiants des fournisseurs des certificats et de leurs porteurs

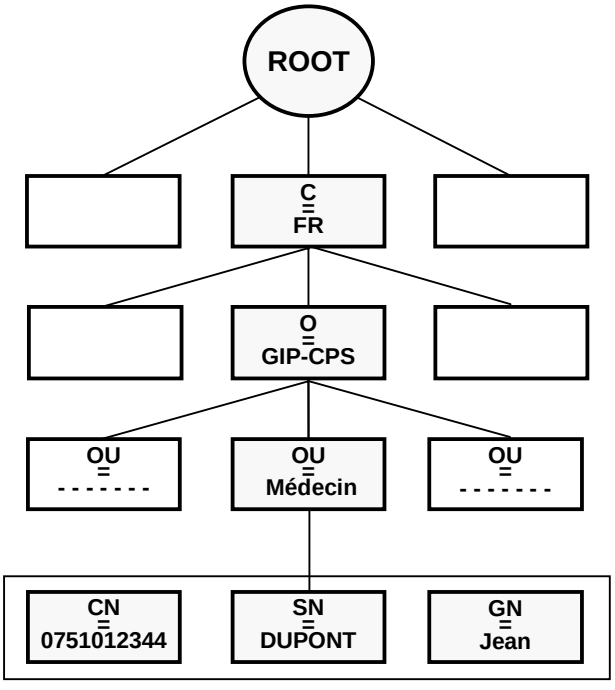
Dans chaque certificat X.509 le fournisseur (issuer) et le porteur (subject) sont identifiés par un Distinguished Name (DN) qui doit être unique.

L'ASIP-SANTÉ construit ce DN à partir des Identifications Nationales des Professionnels de Santé et des Structures.

Chaque DN d'un PS ou d'un PF est hiérarchiquement construit par la concaténation des Relative Distinguished Names (RDN) suivants : Country (France), Organisation (GIP-CPS), Organisational Unit (profession || future profession), (Common name (Identification Nationale du Professionnel de Santé), Surname (nom d'exercice) et Given name (prénom usuel)).

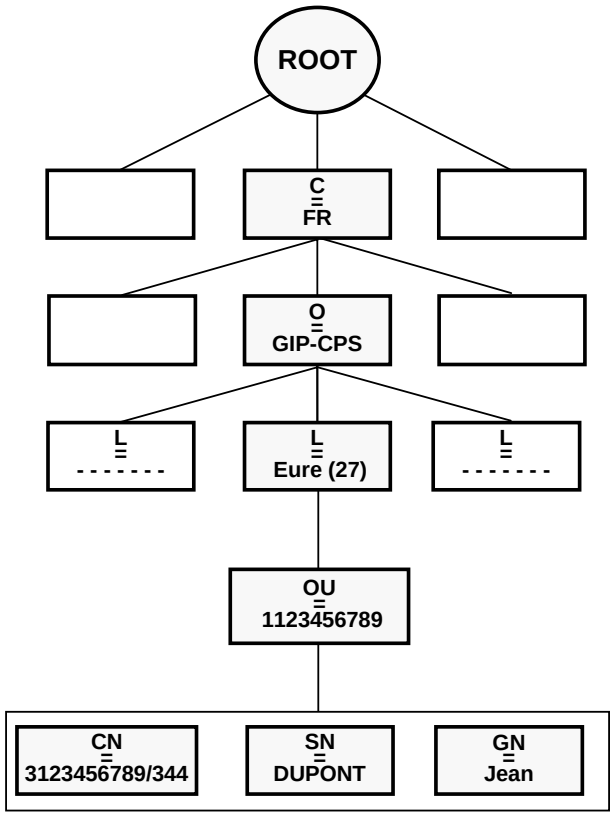
Chaque DN de personnel d'établissement est hiérarchiquement construit par la concaténation des Relative Distinguished Names (RDN) suivants : Country (France), Organisation (GIP-CPS), Locality (département), Organisational Unit (Identification Nationale de la Structure), (Common name (Identification Nationale de l'employé de la Structure), Surname (nom d'exercice) et Given name (prénom usuel)).

Exemple de DN d'un médecin :

Arbre de nommage	Relative Distinguished Name	Distinguished Name
	Racine	{ }
	Country (C) = France	{ C=FR }
	Organisation (O) =GIP-CPS	{ C=FR, O=GIP-CPS }
	OrganisationalUnit (OU) = Médecin	{ C=FR, O=GIP-CPS, OU=Médecin }
	Common name (CN) = 0751012344 Surname (SN) = DUPONT Given name (GN) =Jean	{ C=FR, O=GIP-CPS, OU=Médecin, (CN=0751012344, SN=DUPONT, GN=Jean) }

Note : Le DN des cartes de test aura "GIP-CPS-TEST" comme valeur pour le RDN Organisation.

Exemple de DN pour un employé d'une structure (quel que soit son statut) :

Arbre de nommage	Relative Distinguished Name	Distinguished Name
	Racine	{}
	Country (C) = France	{ C=FR }
	Organisation (O) =GIP-CPS	{ C=FR, O=GIP-CPS }
	Locality (L) = Eure (27)	{ C=FR, O=GIP-CPS, L=Eure (27) }
	OrganisationalUnit (OU) = 1123456789	{ C=FR, O=GIP-CPS, L=Eure (27), OU=1123456789 }
	Common name (CN) = 3123456789/344 Surname (SN) = DUPONT Given name (GN) =Jean	{ C=FR, O=GIP-CPS, L=Eure (27), OU=1123456789, (CN=3123456789/344, SN=DUPONT, GN=Jean) }

Note : Le DN des cartes de test aura "GIP-CPS-TEST" comme valeur pour le RDN Organisation.

4.3 Les autorités de certification

4.3.1 La hiérarchie des certificats

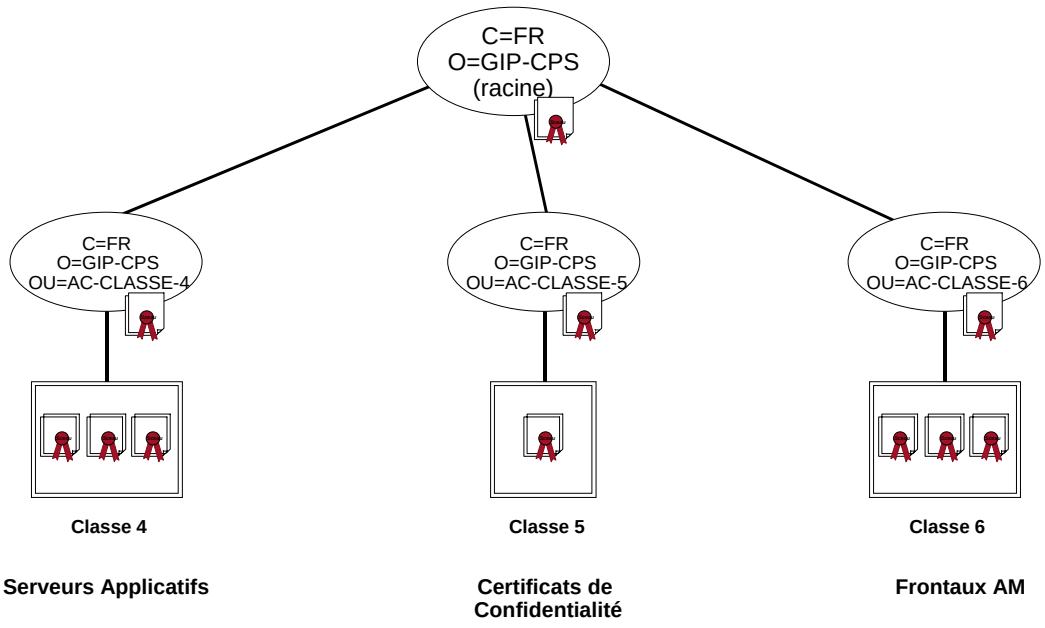
Il y a 3 niveaux de certificats :

1. Niveau "autorité de certification racine" de l'IGC-CPS2bis.
2. Niveau "autorités de certification intermédiaires"

   2.2 Autorités de certification pour les certificats applicatifs (Serveur d'Inscription) :

   - **AC-CLASSE-4 : "Serveurs applicatifs"**, contenant les certificats liés aux Services Applicatifs;
   - **AC-CLASSE-5 : "Certificats de Confidentialité"**, contenant les certificats de confidentialité utilisés pour la messagerie sécurisée, ils peuvent être demandés par des porteurs de cartes CPS (sauf par les porteurs de cartes anonymes) et par des administrateurs (AE délégués).
   - **AC-CLASSE-6 : "Certificats pour Frontaux Assurance Maladie"**, contenant les certificats de S/MIME utilisés pour envoyer des lots de feuilles de soins (FSE ou DRE) par messagerie sécurisée pour traitement par l'AM.

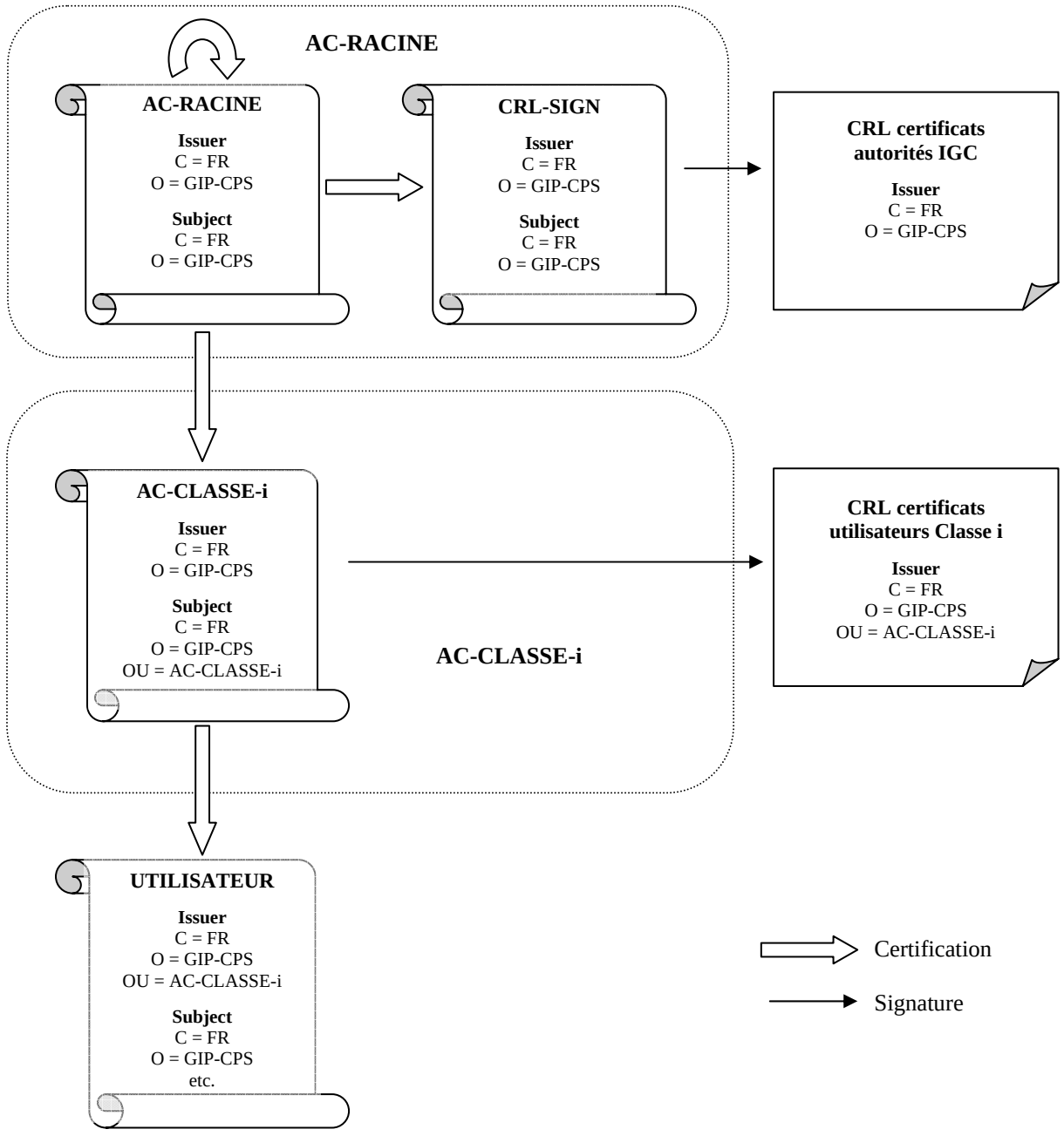
3. Niveau "utilisateurs" : certificats de clés publiques des **Serveurs applicatifs et Frontaux AM** et des **Certificats de Confidentialité**.



Note :
Les certificats des cartes de test feront partie d'une IGC de test (avec une hiérarchie identique) pour les cloisonner. Le RDN Organisation et Organisational Unit des certificats des cartes de test seront "O=GIP-CPS-TEST" et "OU=AC-CLASSE-X-TEST" (sauf pour la Classe-6 ou "O=GIP-CPS" sans "-TEST").

Chemins de certification - validation

Les certificats de clés de signature des CRL de classes sont signés par AC-RACINE (voir schéma ci-dessous) ; conformément aux standards, le DN de l'issuer de la CRL est le même que le DN de l'issuer des certificats à révoquer.



4.3.2 La durée de vie des certificats

La durée de vie des certificats de confidentialité liés aux cartes CPS (Classe-5)

La durée de vie des clés privées est égale à la durée de vie de la carte CPS contenant ces clés (3 ans pour les CPS actuelles).

La durée de vie des clés privées pour la confidentialité « partageable » liées à des cartes CPS démarre à la date de certification et finit à la date de fin de validité de la carte demandeur (à laquelle le certificat est lié).

La durée de vie des certificats des cartes CPS est égale à la :

- durée de vie de la carte pour les certificats de clés publiques d'authentification,
- durée de vie de la carte prolongée d'un mois pour les certificats de signature,
- durée de vie de la clé privée pour les certificats de clés publiques de confidentialité « partageable ».

La durée de vie des certificats de confidentialité de personnes physiques qui ne disposent pas de carte CPS (Classe-5)

La date de début de validité de ces certificats est la date de certification. Leur durée de vie sera définie dans la PC.

La durée de vie des certificats des serveurs applicatifs (Classe-4).

La date de début de validité de ces certificats est la date de certification. Leur durée de vie sera définie dans la PC.

La durée de vie des certificats des Frontaux Assurance Maladie (Classe-6).

La date de début de validité de ces certificats est la date de certification. Leur durée de vie sera définie dans la PC.

4.4 Définition ASN.1 d'un Certificat X.509 v3

```
Certificate  ::=  SEQUENCE  {
      TbsCertificate          TBSCertificate,
      SignatureAlgorithm      AlgorithmIdentifier,
      SignatureValue          BIT STRING  }

tbsCertificate  ::=  SEQUENCE  {
      version                 [0]   Version (v3),
      serialNumber                  CertificateSerialNumber,
      signature                     AlgorithmIdentifier,
      issuer                        Name,
      validity                      Validity,
      subject                       Name,
      subjectPublicKeyInfo          SubjectPublicKeyInfo,
      extensions              [3]   Extensions  }
```

Détails :

```
  Version  ::=  INTEGER  v3(2)


  CertificateSerialNumber  ::=  INTEGER


  AlgorithmIdentifier  ::= SEQUENCE  {
     Algorithm               OBJECT IDENTIFIER,
     Parameters              ANY DEFINED BY Algorithm OPTIONNAL  }


  Name  ::=  CHOICE  {RDNSequence  }
     RDNSequence  ::=  SEQUENCE OF RelativeDistinguishedName
     RelativeDistinguishedName  ::=  SET OF AttributeTypeAndValue
     AttributeTypeAndValue  ::=  SEQUENCE  {
           type              AttributeType,
           value             AttributeValue }
     AttributeType  ::= OBJECT IDENTIFIER
     AttributeValue ::= ANY DEFINED BY AttributeType


  Validity  ::=  SEQUENCE  {
     notBefore               UTCTime,
     notAfter                UTCTime  }  [1]


  SubjectPublicKeyInfo  ::=  SEQUENCE  {
     algorithm               AlgorithmIdentifier,
     subjectPublicKey        BIT STRING  }
```

[1] Un champ "UTCTime" a le format YYMMDDMMSS (heure GMT)
SS ne doit pas être à 00 (recommandation Peter GUTMANN).

```
Extensions  ::=  SEQUENCE OF Extension

Extension  ::=  SEQUENCE  {
    extnId                  OBJECT IDENTIFIER,
    critical                BOOLEAN, (default = FALSE)
    extnValue               OCTET STRING  }
```

4.4.1 Extensions standard utilisées dans les Certificats X.509 du Système CPS

4.4.1.1 authorityKeyIdentifier

Cette extension identifie la clé publique à utiliser pour la vérification de la signature du certificat.

```
AuthorityKeyIdentifier ::= SEQUENCE {
    keyIdentifier                [0]   KeyIdentifier           OPTIONAL,
    authorityCertIssuer          [1]   GeneralNames            OPTIONAL,
    authorityCertSerialNumber    [2]   CertificateSerialNumber OPTIONAL  }

KeyIdentifier ::= OCTET STRING
```

4.4.1.2 subjectKeyIdentifier

Cette extension identifie la clé publique qui est certifiée. Elle permet de différencier plusieurs clés d'un même abonné.

```
SubjectKeyIdentifier ::= KeyIdentifier

KeyIdentifier ::= OCTET STRING
```

4.4.1.3 keyUsage **(extension toujours critique)**

Cette extension définit la fonction de base autorisée du bi-clé dont la clé publique est certifiée.

```
KeyUsage ::= BIT STRING {
    digitalSignature       (0),        '80'  (clé d'authentification)
    nonRepudiation         (1),        '40'
    keyEncipherment        (2),        '20'  (clé de confidentialité)
    dataEncipherment       (3),              non utilisée
    keyAgreement           (4),              non utilisée
    keyCertSign            (5),        '04'  (clé de signature de certificats)
    crlSign                (6),        '02'  (clé de signature de CRLs)
    encipherOnly           (7),              non utilisée
    decipherOnly           (8) }             non utilisée
```

Note : Le KeyUsage d'une clé de signature est = 'C0'.

```
Convention :  L'objet keyUsage est codé sur 1 octet.
              Le nombre de "unused bits" = nombre de bits (lsb) à 0.
              (ex.  digitalSignature  :  nombre de "unused bits" = 7
                    keyCertSign       :  nombre de "unused bits" = 2)
```

Cf. chapitre 6 "Tableau combinatoire avec extensions liées à l'usage des bi-clé".

4.4.1.4 extKeyUsage

Cette extension définit l'utilisation applicative autorisée du bi-clé dont la clé publique est certifiée.

Cette extension est un complément d'information de l'extension keyUsage.

```
ExtKeyUsage ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId

   KeyPurposeId ::= OBJECT IDENTIFIER

      id-kp-serverAuth       : TLS Web authentification serveur
      id-kp-clientAuth       : TLS Web authentification client
      id-kp-codeSigning      : Signature coding téléchargeable
      id-kp-emailProtection  : protection E-mail
      id-kp-timeStamping     : Horodatage
```

Note : Les certificats d'une autorité de certification intermédiaire contiennent toutes les extensions de keyPurposeId autorisées dans les certificats clients qu'elle génère (sera vérifié lors de la vérification de la validité d'un certificat client).
(cf. chapitre 6 "Tableau combinatoire avec extensions liées à l'usage des bi-clé").

4.4.1.5 privateKeyUsagePeriod

Cette extension définit la période d'utilisation de la clé privée, dans le cas où cette période est différente de celle de validité du certificat.

Elle est uniquement présente dans les certificats "utilisateur" avec keyUsage = nonRepudiation (signature).

```
PrivateKeyUsagePeriod ::= SEQUENCE {
    NotBefore         [0]   GeneralizedTime : 1st day of validity
    NotAfter          [1]   GeneralizedTime : last day of validity }
```
[2]

4.4.1.6 certificatePolicies

Cette extension définit les politiques de certification que le certificat reconnaît supporter.

```
CertificatePolicies ::= SEQUENCE OF PolicyInformation

PolicyInformation ::= SEQUENCE {
    policyIdentifier       CertPolicyId  }

CertPolicyId ::= OBJECT IDENTIFIER
```

[2] Un champ "GeneralizedTime" a le format YYYYMMDDMMSS (heure GMT).

4.4.1.7 basicConstraints **(extension toujours critique)**

Cette extension, uniquement présente dans les certificats des autorités de certification, indique si le porteur du certificat peut agir comme une Autorité de Certification (CA = "TRUE" et son keyUsage = "keyCertSign").
Si tel est le cas, "pathLenConstraint" indique le nombre de niveaux d'AC "fille" autorisées.

```
BasicConstraints ::= SEQUENCE {
    CA                      BOOLEAN  (default = FALSE)
    pathLenConstraint       INTEGER  }
```

4.4.1.8 subjectAltName

Cette extension peut contenir un ou plusieurs noms alternatifs pour le porteur du certificat.

```
SubjectAltName ::= GeneralNames

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
    OtherName                   [0]   AnotherName,
    rfc822Name                  [1]   IA5String,
    dNSName                     [2]   IA5String,
    x400Address                 [3]   ORAddress,
    directoryName               [4]   Name,
    ediPartyName                [5]   EDIPartyName,
    uniformResourceIdentifier   [6]   IA5String,
    iPAddress                   [7]   OCTET STRING,
    registeredID                [8]   OBJECT IDENTIFIER }
```

Cette extension n'est pas utilisée dans les certificats des AC.

Pour les certificats des cartes CPS (Classes 0 à 3) cette extension est optionnelle.

Dans un premier temps son utilisation se limite aux certificats de confidentialité pour indiquer l'adresse e-mail (une seule par certificat) du porteur.

Pour les certificats de Serveurs Applicatifs (Classe 4) l'utilisation de cette extension est à la discrétion du demandeur.

4.4.2 Extensions Netscape utilisées dans les Certificats X.509 du Système CPS

4.4.2.1 netscapeCertType

Cette extension indique l'utilisation autorisée du bi-clé dont la clé publique est certifiée.

Elle est présente pour des besoins d'interopérabilité et notamment pour l'interopérabilité avec des produits sortis avant la finalisation du standard X.509 V3.

```
netscapeCertType ::= BIT STRING {
    client SSL                                  (0),      '80'
    serveur SSL                                 (1),      '40'
    client S/MIME                               (2),      '20'
    object signing                              (3),      non utilisé
    reserved                                    (4),      non utilisé
    autorité pour signer des certificats SSL    (5),      '04'
    autorité pour signer des certificats S/MIME (6),      '02'
    autorité pour signer des objets             (7),      non utilisé
```

Convention : L'objet netscapeCertType est codé sur 1 octet.
Le nombre de "unused bits" = nombre de bits (lsb) à 0.

Cf. chapitre 6 "Tableau combinatoire avec extensions liées à l'usage des bi-clé".

4.4.3 Extensions privées utilisées dans les Certificats X.509 du Système CPS

4.4.3.1 gipCardID

Cette extension - concernant uniquement des certificats liés aux cartes de la famille CPS - contient l'identification de l'émetteur de la carte et le numéro de série de la carte.
Format : "8025000001/9999999999" (80 250 00001 = Issuer Identification Number du GIP).

```
GipCardID ::= PrintableString
```

4.4.3.2 gipCardCategory **(extension critique pour les certificats utilisateur de test)**

Cette extension contient la catégorie de la carte (Carte de Professionnel de Santé, Carte Patient-Assuré, Module de Sécurité).

Pour éviter l'acceptation d'un certificat de test par une application en exploitation réelle, cette extension privée est marquée "critique" pour les cartes de test : toutes les applications ne connaissant pas la signification de cette extension privée, doivent refuser le certificat.

```
GipCardCategory ::= OctetString
         '00'  :  Carte de la famille CPS
         '80'  :  Carte de TEST de la famille CPS
         '03'  :  Module de sécurité              (physique ou logique)
         '83'  :  Module de sécurité de TEST
```

4.4.3.3 gipCardType

Cette extension - concernant uniquement des certificats liés aux cartes de la famille CPS - contient le type de la carte.

```
GipCardType ::= Integer
         '00'  :  CPS
         '01'  :  CPF
         '02'  :  CDE ou CPE
         '03'  :  CPA
         '04'  :  CSA     (type de carte abandonné)
```

4.4.3.4 gipProfessionCode

Cette extension - concernant uniquement des certificats liés aux cartes de type CPS - contient le code de profession du Professionnel de Santé .

```
GipProfessionCode ::= Integer
```

4.4.3.5 gipFutureProfessionCode

Cette extension - concernant uniquement des certificats liés aux cartes de type CPF - contient le code de profession du Professionnel de Santé en formation.

```
GipFutureProfessionCode ::= Integer
```

4.4.3.6 gipConfPart (optionnelle et uniquement pour les certificats de confidentialité – Classe-5)

Cette extension - concernant uniquement des certificats liés aux cartes de la famille CPS - spécifie que la clé de confidentialité certifiée est « partageable » et non « personnelle ».

- **Confidentialité « partageable »** (CPS2bis) : la clé privée de confidentialité, nécessaire au déchiffrement de messages, est stockée sur un poste de travail ; le déchiffrement peut être fait par le destinataire, détenteur légitime de la clé privée de confidentialité **et** par des personnes qu'il a autorisées par une délégation explicite.
- **Confidentialité « personnelle »** (CPS2bis uniquement) : la clé privée de confidentialité, nécessaire au déchiffrement de messages, est stockée dans la CPS ; le déchiffrement est donc réservé au porteur légitime de la carte CPS contenant cette clé.
  Note : la confidentialité « personnelle » est (provisoirement ?) supprimée pour les CPS2bis.

```
gipConfPart ::= Boolean
        true     : confidentialité « partageable »
        false    : confidentialité « personnelle »

La valeur par défaut (absence de l'extension) est "false".
```

Cf. chapitre 6 "Tableau combinatoire avec extensions liées à l'usage des bi-clé".

4.5 Les identifiants d'objet (OID)

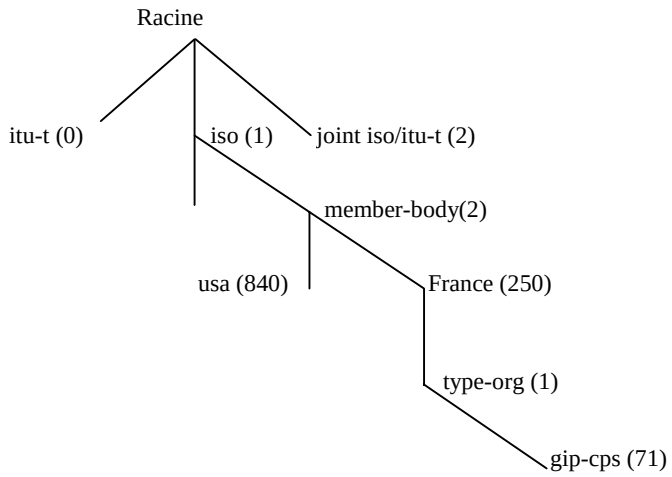
A l'intérieur des certificats, les objets sont identifiés par des identifiants d'objet (Object Identifier : OID).

Ces OID sont organisés au niveau international sous la forme d'un arbre.

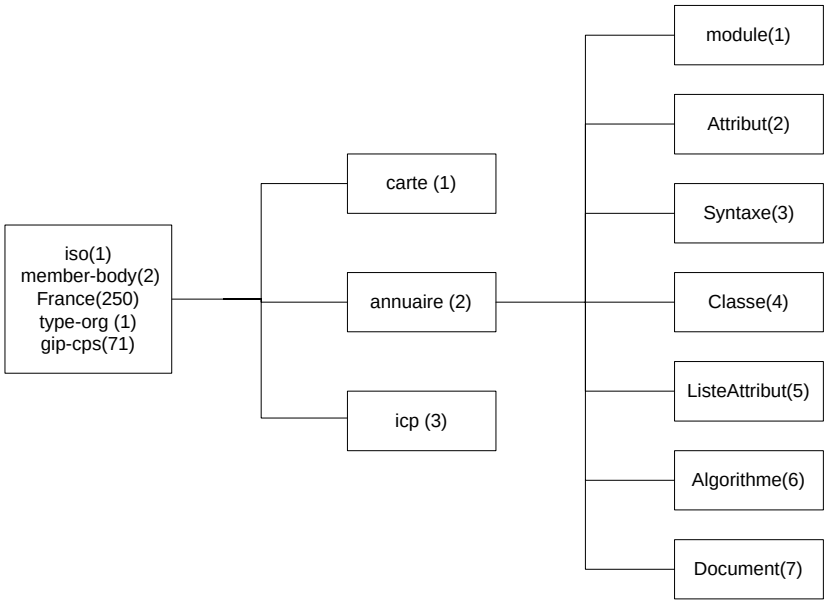
Chaque pays ou organisation (telle que la France ou l'ISO) se voit attribuer une branche.
Un identifiant est attribué définitivement et peut identifier n'importe quel type d'objet.

Le GIP « CPS » s'est fait attribuer par l'AFNOR l'identifiant 1.2.250.1.71 et peut donc affecter des identifiants sous sa branche aux objets de son choix.

Identifiant (OID) du GIP-CPS : 1.2.250.1.71



La figure suivante illustre le sous-arbre d'identificateur GIP-CPS.



Modèle du sous-arbre d'identificateurs d'objet du GIP-CPS

Note : L'ASIP-Santé a repris l'exploitation pour cette OID.

Les identifiants d'objet propriétaires utilisés dans les certificats des cartes CPS sont :

Object	Object Identifier (OID)	Object Identifier (hex)
id-gip	{ iso(1) member-body(2) France(250) type-org(1) gip-cps(71) }	2A 81 7A 01 47
id-gip-carte	{ id-gip 1 }	2A 81 7A 01 47 01
id-gip-carte-at (attribute)	{ id-gip-carte 2 }	2A 81 7A 01 47 01 02
gipJobCode	{ id-gip-carte-at 1 }	2A 81 7A 01 47 01 02 01
gipCardType	{ id-gip-carte-at 2 }	2A 81 7A 01 47 01 02 02
gipCardID	{ id-gip-carte-at 3 }	2A 81 7A 01 47 01 02 03
gipCardModel	{ id-gip-carte-at 4 }	2A 81 7A 01 47 01 02 04
gipCardCategory	{ id-gip-carte-at 5 }	2A 81 7A 01 47 01 02 05
gipProfSitCode	{ id-gip-carte-at 6 }	2A 81 7A 01 47 01 02 06
gipProfessionCode	{ id-gip-carte-at 7 }	2A 81 7A 01 47 01 02 07
gipFutureProfessionCode	{ id-gip-carte-at 8 }	2A 81 7A 01 47 01 02 08
gipConfPart	{ id-gip-carte-at 9 }	2A 81 7A 01 47 01 02 09
id-gip-icp	{ id-gip 3 }	2A 81 7A 01 47 03
id-gip-icp-doc (documentation)	{ id-gip icp 7 }	2A 81 7A 01 47 03 07
gipCertificationPolicy pour certificats de serveurs applicatifs (Classe-4)	{ id-gip-icp-doc 5 }	2A 81 7A 01 47 03 07 05
gipCertificationPolicy pour certificats de confidentialité « partageable » (Classe-5)	{ id-gip-icp-doc 6 }	2A 81 7A 01 47 03 07 06
gipCertificationPolicy pour tous les certificats de TEST des Classes-4 et 5	{ id-gip-icp-doc 4 }	2A 81 7A 01 47 03 07 04
gipCertificationPolicy pour certificats de la Classe-6 – Production et TEST	{ id-gip-icp-doc 7 }	2A 81 7A 01 47 03 07 07

Les identifiants d'objet standards utilisés dans les certificats des cartes CPS et les CRL sont :

Object	Object Identifier (OID)	Object Identifier (hex)
RsaEncryption	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 1 }	2A 86 48 86 F7 0D 01 01 01
sha-1WithRSAEncryption	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }	2A 86 48 86 F7 0D 01 01 05
id-pkix	{ iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) }	2B 06 01 05 05 07
id-kp (keyPurpose)	{ id-pkix 3}	
id-kp-serverAuth	{ id-kp 1}	2B 06 01 05 05 07 03 01
id-kp-clientAuth	{ id-kp 2}	2B 06 01 05 05 07 03 02
id-kp-codeSigning	{ id-kp 3}	2B 06 01 05 05 07 03 03
id-kp-emailProtection	{ id-kp 4}	2B 06 01 05 05 07 03 04
id-kp-timeStamping	{ id-kp 8}	2B 06 01 05 05 07 03 08
id-at : AttributeType	{ joint iso/itu-t(2) directoryX500(5) AttributeType(4) }	55 04
commonName	{ id-at 3 }	55 04 03
surName	{ id-at 4 }	55 04 04
serialNumber	{ id-at 5 }	55 04 05
countryName	{ id-at 6 }	55 04 06
localityName	{ id-at 7 }	55 04 07
organizationName	{ id-at 10 }	55 04 0A
organizationalUnitName	{ id-at 11 }	55 04 0B
givenName	{ id-at 42 }	55 04 2A
id-ce : extensions	{ joint iso/itu-t(2) directoryX500(5) extension(29) }	55 1D
subjectKeyIDentifier	{ id-ce 14}	55 1D 0E
keyUsage	{ id-ce 15}	55 1D 0F
privateKeyUsagePeriod	{ id-ce 16}	55 1D 10
subjectAltName	{ id-ce 17}	55 1D 11
issuerAltName	{ id-ce 18}	55 1D 12
basicConstraints	{ id-ce 19}	55 1D 13
crlNumber	{ id-ce 20}	55 1D 14
deltaCRLIndicator	{ id-ce 27}	55 1D 1B
certificatePolicies	{ id-ce 32}	55 1D 20
authorityKeyIdentifier	{ id-ce 35}	55 1D 23
extKeyUsage	{ id-ce 37}	55 1D 25
netscape	{ joint iso/itu-t(2) country-assigmants(16) USA(840) US-company-arc(1) Netscape(113730) }	60 86 48 01 86 F8 42
netscape-cert-extension	{ netscape 1 }	60 86 48 01 86 F8 42 01
netscapeCertType	{ netscape-cert-extension 1 }	60 86 48 01 86 F8 42 01 01

5. Les contenus des certificats de l'IGC-CPS2bis+

5.1 Les certificats du niveau "racine" (AC-RACINE)

1. Certificat de la clé de certification (self-signed [3])
2. Certificat de la clé de signature des CRL du AC-RACINE (révocation des certificats niveau racine et immédiatement inférieur et, plus tard, révocation des clés "cross-certifiées").

Objet	Format	Certificat clé de certification AC-RACINE	Certificat clé de signature des CRL
Certificate	Sequence		
TbsCertificate	Sequence		
version	Integer	2 (version 3)	2 (version 3)
serialNumber	Integer	n° de certificat	n° de certificat
signature	OID	Sha-1WithRSAencryption	Sha-1WithRSAencryption
issuer	PrintString	{ C=FR, O=GIP-CPS }	{ C=FR, O=GIP-CPS }
validity	UTC-Time	NotBefore « date de création » NotAfter « fin 2020 »	NotBefore « date de création » NotAfter « fin2020 »
subject	PrintString	{ C=FR, O=GIP-CPS }	{ C=FR, O=GIP-CPS }
subjectPublicKeyInfo	Sequence		
algorithmIdentifier	OID	RSAencryption (Parameter = NULL)	RSAencryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 2.048 bits + exp. pub. (=2E16+1) = KP AC-RACINE	clé publique de 2.048 bits + exp. pub. (=2E16+1) = KP AC-RACINE
extensions	Sequence		
authorityKeyId	OctString	objet absent	« SHA1 KP AC-RACINE »
subjectKeyId	OctString	« SHA1 de KP AC-RACINE »	« SHA1 de subjectPublicKey »
keyUsage	Sequence		
critical	Boolean	true	true
value	BitString	'04' : keyCertSign (clé de signature de certificats)	'02' : crlSign (clé de signature de CRL)
extKeyUsage	Sequence	objet absent	objet absent
certificatePolicies certPolicyId	Sequence OID	{ id-gip-icp-doc 3 } gipCertificationPolicy	{ id-gip-icp-doc 3 } gipCertificationPolicy
Basic constraints	Sequence		objet absent
critical	Boolean	true	
CA	Boolean	true	
pathLength	Integer	1	
subjectAltName	IA5string	objet absent	objet absent
netscapeCertType	BitString	objet absent	objet absent
SignatureAlgorithm	OID	Sha-1WithRSAencryption	Sha-1WithRSAencryption
SignatureValue	BitString	« signature sur certificat, calculée avec la clé privée AC-RACINE » (256 octets)	« signature sur certificat, calculée avec la clé privée AC-RACINE » (256 octets)

[3] Un certificat "self-signed" a les caractéristiques suivantes : issuer=subject **et** keyUsage= keyCertSign (authorityKeyId est absent).

5.2 Le certificat "autorité de certification intermédiaire" de la classe 4

Objet	Format	Certificat de la clé ACI de la Classe 4
Certificate	Sequence	
TbsCertificate	Sequence	
version	Integer	2 (version 3)
serialNumber	Integer	n° de certificat
signature	OID	Sha-1WithRSAencryption
issuer	PrintString	{ C=FR, O=GIP-CPS }
validity	UTC-Time	NotBefore « date de création » NotAfter « fin 2020 »
subject	PrintString	{ C=FR, O=GIP-CPS, OU=AC-CLASSE-4 }
subjectPublicKeyInfo	Sequence	
algorithmIdentifier	OID	RSAencryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 1.024 bits + exp. pub. (=2E16+1) = KP AC-CLASSE-4
extensions	Sequence	
authorityKeyId	OctString	« SHA1 KP AC-RACINE »
subjectKeyId	OctString	« SHA1 de subjectPublicKey »
keyUsage	Sequence	
critical	Boolean	true
value	BitString	'06' : keyCertSign (clé de signature de certificats) et crlSign (clé de signature de CRL)
extKeyUsage value(s)	Sequence OID	 id-kp-clientauth + id-kp-serverauth + id-kp-emailProtection
certificatePolicies	Sequence	
certPolicyId	OID	{ id-gip-icp-doc 5 } gipCertificationPolicy
Basic constraints	Sequence	
critical	Boolean	true
CA	Boolean	true
pathLength	Integer	0
subjectAltName	IA5string	objet absent
netscapeCertType	BitString	'06' : autorité pour certificats SSL + S/MIME
SignatureAlgorithm	OID	Sha-1WithRSAencryption
SignatureValue	BitString	« signature sur certificat, calculée avec la clé privée AC-RACINE » (256 octets)

5.3 Le certificat "autorité de certification intermédiaire" de la classe 5

Objet	Format	Certificat de la clé ACI de la Classe 5
Certificate	Sequence	
TbsCertificate	Sequence	
version	Integer	2 (version 3)
serialNumber	Integer	n° de certificat
signature	OID	Sha-1WithRSAencryption
issuer	PrintString	{ C=FR, O=GIP-CPS }
validity	UTC-Time	NotBefore « date de création » NotAfter « fin 2008 »
subject	PrintString	{ C=FR, O=GIP-CPS, OU=AC-CLASSE-5 }
subjectPublicKeyInfo	Sequence	
algorithmIdentifier	OID	RSAencryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 1.024 bits + exp. pub. (=2E16+1) = KP AC-CLASSE-5
extensions	Sequence	
authorityKeyId	OctString	« SHA1 KP AC-RACINE »
subjectKeyId	OctString	« SHA1 de subjectPublicKey »
keyUsage	Sequence	
critical	Boolean	true
value	BitString	'06' : keyCertSign (clé de signature de certificats) et crlSign (clé de signature de CRL)
extKeyUsage value(s)	Sequence OID	 id-kp-emailProtection
certificatePolicies	Sequence	
certPolicyId	OID	{ id-gip-icp-doc 6 } gipCertificationPolicy
Basic constraints	Sequence	
critical	Boolean	true
CA	Boolean	true
pathLength	Integer	0
subjectAltName	IA5string	objet absent
netscapeCertType	BitString	'02' : autorité pour certificats S/MIME
SignatureAlgorithm	OID	Sha-1WithRSAencryption
SignatureValue	BitString	« signature sur certificat, calculée avec la clé privée AC-RACINE » (256 octets)

5.4 Le certificat "autorité de certification intermédiaire" de la classe 6

Objet	Format	Certificat de la clé ACI de la Classe 6
Certificate	Sequence	
TbsCertificate	Sequence	
version	Integer	2 (version 3)
serialNumber	Integer	n° de certificat
signature	OID	Sha-1WithRSAencryption
issuer	PrintString	{ C=FR, O=GIP-CPS }
validity	UTC-Time	NotBefore « date de création » NotAfter « fin 2020 »
subject	PrintString	{ C=FR, O=GIP-CPS, OU=AC-CLASSE-6 }
subjectPublicKeyInfo	Sequence	
algorithmIdentifier	OID	RSAencryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 1.024 bits + exp. pub. (=2E16+1) = KP AC-CLASSE-6
extensions	Sequence	
authorityKeyId	OctString	« SHA1 KP AC-RACINE »
subjectKeyId	OctString	« SHA1 de subjectPublicKey »
keyUsage	Sequence	
critical	Boolean	true
value	BitString	'86' : keyCertSign (clé de signature de certificats) et crlSign (clé de signature de CRL) Client SSL
extKeyUsage value(s)	Sequence OID	 objet absent
certificatePolicies	Sequence	
certPolicyId	OID	{ id-gip-icp-doc 7 } gipCertificationPolicy
Basic constraints	Sequence	
critical	Boolean	true
CA	Boolean	true
pathLength	Integer	0
subjectAltName	IA5string	objet absent
netscapeCertType	BitString	objet absent
SignatureAlgorithm	OID	Sha-1WithRSAencryption
SignatureValue	BitString	« signature sur certificat, calculée avec la clé privée AC-RACINE » (256 octets)

5.5 Les certificats utilisateurs : la classe 4 des Serveurs Applicatifs

Un Serveur Applicatif peut disposer jusqu'à 2 certificats :

1. Certificat S/MIME ;
2. Certificat SSL ;

Lors de la demande de certification, le responsable du Serveur Applicatif soumet le gabarit des certificats souhaités. Ce gabarit permet une certaine liberté en ce qui concerne les champs des certificats, mais il doit répondre aux exigences de la Politique de Certification de l'IGC CPS et le DN du porteur doit être conforme à l'architecture de l'annuaire du GIP.

La seule extension privée est gipCardCategory indiquant que le "porteur" du certificat est un "Module de Sécurité" (physique ou logique) du Serveur Applicatif.

Objet	Format	Certificat serveur applicatif S/MIME
Certificate	Sequence	
TbsCertificate	Sequence	
version	Integer	2 (version 3)
serialNumber	Integer	n° de certificat
signature	OID	Sha-1WithRSAencryption
issuer	PrintString	{ C=FR, O=GIP-CPS, OU=AC-CLASSE-4 }
validity	UTC-Time	NotBefore : date début de validité NotAfter : date fin de validité + 1 mois
subject	PrintString T61String PrintString PrintString	{ C=FR, O=GIP-CPS, L= « nom département » « (N°) », OU= « id-nat-struct », CN= « nom application » }
subjectPublicKeyInfo	Sequence	
algorithmIdentifier	OID	RSAencryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 1.024 bits & exp. pub. (=$2^{E}16+1$)
extensions	Sequence	
authorityKeyId	OctString	« SHA1 KP AC-CLASSE-4 »
subjectKeyId	OctString	« SHA1 subjectPublicKey »
keyUsage	Sequence	
critical	Boolean	true
value	BitString	'E0' : digitalSig & nonRep & keyEnc
extKeyUsage value(s)	Sequence OID	 id-kp-emailProtection
privateKeyUsagePeriod	GenTime	NotBefore : date début de validité NotAfter : date fin de validité
certificatePolicies	Sequence	
certPolicyId	OID	{ id-gip-icp-doc 5 } gipCertificationPolicy
subjectAltName	IA5string	adresse e-mail (obligatoire)
netscapeCertType	BitString	'20' : client S/MIME
gipCardCategory	OctString	'03' (Module de Sécurité)
SignatureAlgorithm	OID	Sha-1WithRSAencryption
SignatureValue	BitString	« signature sur certificat, calculée avec la clé privée AC-CLASSE-4 » (128 octets)

Objet	Format	Certificat serveur applicatif SSL
Certificate	Sequence	
TbsCertificate	Sequence	
version	Integer	2 (version 3)
serialNumber	Integer	n° de certificat
signature	OID	Sha-1WithRSAencryption
issuer	PrintString	{ C=FR, O=GIP-CPS, OU=AC-CLASSE-4 }
validity	UTC-Time	NotBefore : date début de validité NotAfter : date fin de validité
subject	PrintString T61String PrintString PrintString	{ C=FR, O=GIP-CPS, L= « nom département » « (N°) », OU= « id-nat-struct », CN= « nom domaine » }
subjectPublicKeyInfo	Sequence	
algorithmIdentifier	OID	RSAencryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 1.024 bits & exp. pub. (=$2^{E}16+1$)
extensions	Sequence	
authorityKeyId	OctString	« SHA1 KP AC-CLASSE-4 »
subjectKeyId	OctString	« SHA1 subjectPublicKey »
keyUsage	Sequence	
critical	Boolean	true
value	BitString	'A0' : digitalSig & keyEnc
extKeyUsage value(s)	Sequence OID	 id-kp-clientauth + id-kp-serverauth
privateKeyUsagePeriod	GenTime	objet absent
certificatePolicies	Sequence	
certPolicyId	OID	{ id-gip-icp-doc 5 } gipCertificationPolicy
subjectAltName	IA5string	nom domaine internet (par défaut idem CN)
netscapeCertType	BitString	'C0' : client et serveur SSL
gipCardCategory	OctString	'03' (Module de Sécurité)
SignatureAlgorithm	OID	Sha-1WithRSAencryption
SignatureValue	BitString	« signature sur certificat, calculée avec la clé privée AC-CLASSE-4 » (128 octets)

Exemple DN pour un **Serveur Applicatif (certificat SSL)** :

{ C=FR, O=GIP-CPS, L=Paris (75), OU=318003000900013, CN=annuaire.gip-cps.fr }

5.6 Les certificats utilisateurs : la classe 5 des Certificats de Confidentialité « partageable »

Les porteurs de cartes CPS2bis des classes 1 à 3 ainsi que ceux des cartes CPS2 ont la possibilité de demander des certificats de confidentialité « partageable » au Serveur d'Inscription pour les bi-clés de confidentialité générés sur son poste (demande signée).

Les champs des certificats de confidentialité « partageable » sont :

- soit imposés par X.509 (ex. version),
- soit spécifique au Serveur d'Inscription (ex. DN issuer et authorityKeyId),
- soit spécifique au certificat généré (ex. keyUsage et gipConPart),
- soit copiés à partir du certificat de signature (notamment les extensions privées),
- soit fournis par le demandeur (ex. clé publique et adresse e-mail).

Attention :

1. Si le demandeur du certificat de confidentialité « partageable » est un PS (classe-1), le DN du porteur sera :
   - la copie de celui du demandeur, si l'adresse e-mail est indépendante d'une situation d'exercice
   - construit à partir du DN de la structure et le CN du PS, si l'adresse e-mail est liée à une situation d'exercice.
2. Si le demandeur du certificat de confidentialité « partageable » n'est pas un PS (classe ≠ 1), le DN du porteur sera la copie de celui du demandeur (adresse e-mail toujours liée à une situation d'exercice).
3. Pour les CPS2, le DN de référence du subject est celui publié dans l'Annuaire !

Exemple de génération d'un certificat de confidentialité « partageable » liée à une situation d'exercice, à partir d'un certificat de signature d'une CPS.

Objet	Format	Certificat de confidentialité « partageable » d'une CPS
Certificate	Sequence	
TbsCertificate	Sequence	
version	Integer	2 (version 3)
serialNumber	Integer	n° de certificat, attribué par l'AC lors de l'inscription
signature	OID	Sha-1WithRSAencryption
issuer	PrintString	{ C=FR, O=GIP-CPS, OU=AC-CLASSE-5 }
validity	UTC-Time	NotBefore : date de demande NotAfter : date fin de validité carte (= NotAfter du privateKeyUsagePeriod)
subject PS (classe-1) et @ e-mail liée à une situation d'exercice	PrintString T61String T61String PrintString T61String T61String	{ C=FR, O=GIP-CPS, L= « nom département » « (N°) », OU= « id-nat-struct », (CN= « id-nat-ps », SN= « nom d'exercice », GN= « prénom usuel ») }
subjectPublicKeyInfo	Sequence	
algorithmIdentifier	OID	RSAencryption (Parameter = NULL)
subjectPublicKey	BitString	**clé publique** de 128 octets + exp. pub. (=2E16+1) **générée et fournie par demandeur**
extensions	Sequence	
authorityKeyId	OctString	« SHA1 KP AC-CLASSE-5 »
subjectKeyId	OctString	« SHA1 subjectPublicKey »
keyUsage	Sequence	
critical	Boolean	true
value	BitString	'20' : keyEncipherment (clé de chiffrement de clés)
extKeyUsage value(s)	Sequence OID	 id-kp-emailProtection
gipConfPart	Boolean	true
privateKeyUsagePeriod	GenTime	objet absent
certificatePolicies	Sequence	
certPolicyId	OID	{ id-gip-icp-doc 6 } gipCertificationPolicy
subjectAltName	Sequence	**adresse e-mail fournie par demandeur**
netscapeCertType	BitString	'20' : client S/MIME
gipCardID	PrintString	issuerID "/" cardserialnumber
gipCardCategory	OctString	'00' (Carte PS)
gipCardType	Integer	'00' (CPS)
gipCardModel	BitString	objet optionnel
gipProfessionCode	Integer	« code de la profession »

Objet	Format	Certificat de confidentialité « partageable » d'une CPS
gipFutureProfessionCode	Integer	objet absent
gipProfSitCode	Integer	objet optionnel
SignatureAlgorithm	OID	Sha-1WithRSAencryption
SignatureValue	BitString	« signature sur certificat, calculée avec la clé privée AC-CLASSE-5 du Serveur d'Inscription » (128 octets)

5.7 Les certificats utilisateurs de la classe 6 : Frontaux Assurance Maladie

Durée de validité = 6 ans

Objet	Format	Certificat Frontal AM S/MIME
Certificate	Sequence	
TbsCertificate	Sequence	
version	Integer	2 (version 3)
serialNumber	Integer	n° de certificat
signature	OID	Sha-1WithRSAencryption
issuer	PrintString	{ C=FR, O=GIP-CPS, OU=AC-CLASSE-6 }
validity	UTC-Time	NotBefore : date début de validité NotAfter : date fin de validité + 1 mois
subject	PrintString T61String PrintString PrintString	{ C=FR, O=GIP-CPS, L= Sarthe (72), OU= 339172288100045 (=GIE-SV), CN= xxyyy@yyy.xx6.rss.fr» } (= @ bàl frontal pour FSE ou DRE)
subjectPublicKeyInfo	Sequence	
algorithmIdentifier	OID	RSAencryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 1.024 bits & exp. pub. (=2^E16+1)
extensions	Sequence	
authorityKeyId	OctString	« SHA1 KP AC-CLASSE-6 »
subjectKeyId	OctString	« SHA1 subjectPublicKey »
keyUsage	Sequence	
critical	Boolean	true
value	BitString	'E0' : digitalSig & nonRep & keyEnc
extKeyUsage value(s)	Sequence OID	 id-kp-emailProtection
privateKeyUsagePeriod	GenTime	NotBefore : date début de validité NotAfter : date fin de validité
certificatePolicies	Sequence	
certPolicyId	OID	{ id-gip-icp-doc 7 } gipCertificationPolicy
subjectAltName	IA5string	adresse mail du CN (obligatoire)
netscapeCertType	BitString	'20' : client S/MIME
gipCardCategory	OctString	'03' (Module de Sécurité)
SignatureAlgorithm	OID	Sha-1WithRSAencryption
SignatureValue	BitString	« signature sur certificat, calculée avec la clé privée AC-CLASSE-4 » (128 octets)

5.8 Les certificats utilisateurs de test des classes 4 et 5

Les certificats de test sont identiques aux certificats d'exploitation sauf :

1. Le Distinguished name de l'issuer contient : "O=GIP-CPS-TEST" et "OU=AC-CLASSE-i-TEST" ;
2. Le Distinguished name du subject contient : "O=GIP-CPS-TEST" ;
3. L'extension certificationPolicy est { id-gip-icp-doc 4 } : gipCertificationPolicy de TEST.

5.9 Les certificats utilisateurs de test de la classe 6

Les certificats de test sont identiques aux certificats d'exploitation sauf :

1. Le Distinguished name de l'issuer contient : "O=GIP-CPS-TEST" et "OU=AC-CLASSE-i-TEST" ;
2. Le Distinguished name du subject contient : **"O=GIP-CPS"** ;
3. L'extension certificationPolicy est { id-gip-icp-doc 7 }.

6. Tableau combinatoire avec extensions liées à l'usage des bi-clés

Le tableau ci-dessous résume les différentes extensions par type de certificat.

Certificat	keyUsage (critique)	extendedKeyUsage	gipConfPart	netscapeCertType
AC-RACINE	'04' : keyCertSign			
AC-CLASSE-4	'04' : keyCertSign	id-kp-clientauth id-kp-serverauth id-kp-emailProtection		'06' autorité pour signer certificats SSL + S/MIME
AC-CLASSE-5	'04' : keyCertSign	id-kp-emailProtection		'02' autorité pour signer certificats S/MIME
AC-CLASSE-6	'04' : keyCertSign	id-kp-emailProtection		'02' autorité pour signer certificats S/MIME
Certificats des CRL ACI et ACR	'02' : crlSign	-		
Classe 4 : Serveurs Applicatifs				
Certificat S/MIME	'E0' : digitalSig & nonRep & keyEnc	id-kp-emailProtection		'20' client S/MIME
Certificat SSL	'A0' : digitalSig & keyEnc	id-kp-clientauth id-kp-serverauth		'C0' client et serveur SSL
Classe 5 : Certificats Confidentialité « partageable »				
Confidentialité « partageable »	'20' : keyEncipherment	id-kp-emailProtection	true	'20' client S/MIME
Classe 6 : Certificats Frontaux Assurance Maladie				
Confidentialité « partageable »	'E0' : digitalSig & nonRep & keyEnc	id-kp-emailProtection		'20' client S/MIME