



AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

IGC-CPS2ter

Les certificats X.509 des cartes

CPS2ter et CPS3.1

et les CRLs

Version 1.1

30 novembre 2011

SOMMAIRE

1	Introduction	3
2	Symboles	5
3	Abréviations	5
4	Format des Certificats X.509 des cartes CPS2ter et CPS3.1	6
4.1	Présentation d'un certificat X.509 version 3 (rappel).....	6
4.2	Les identifiants des émetteurs des certificats et de leurs porteurs.....	8
4.3	Les autorités de certification.....	12
4.4	Définition ASN.1 d'un Certificat X.509 v3.....	15
4.5	Les identifiants d'objet (OID).....	23
5	Les contenus des certificats de l'IGC-CPS2ter	28
5.1	Les certificats du niveau "racine" (AC RACINES).....	28
5.2	Les certificats des classes 0 à 3 (AC Intermédiaires).....	29
5.3	Les certificats utilisateurs : les classes 0 à 3 des cartes CPS2ter et CPS3.1	30
5.4	Les certificats des cartes de la classe 3 : "Personnel habilité"	33
5.5	Les certificats utilisateurs de test des classes 0 à 3	34
6	Format des Certification Revocation Lists de l'IGC-CPS2ter	35
6.1	Présentation d'une CRL X.509 version 2.....	35
6.2	Définition ASN.1 d'une CRL.....	37
7	Les contenus des CRLs de l'IGC-CPS2ter	40
8	ASN.1 (rappels)	41
8.1	La notation ASN.1.....	41
8.2	Codification des objets en ASN.1	41
8.3	Quelques particularités sur la construction d'objets	42
9	Exemple de codage d'un certificat de signature d'une CPS3.1	44
10	D'autres exemples de codage d'extensions.....	49
11	Exemple de CRL	50
12	Tableau combinatoire avec extensions liées à l'usage des bi-clés.....	53
13	Gestion des versions	54
13.1	Version 1.0 du 10 février 2011 : Création du document	54

1 Introduction

Ce document détaille les Certificats X.509 de clés publiques et les CRLs (Certification Revocation Lists) de l'IGC-CPS2ter.

Le présent document s'applique aux cartes CPS2ter et CPS3.1.

Par rapport à la version précédente ¹, il introduit les certificats de la CPS3.1 qui se distinguent des certificats de la CPS2ter par des nouvelles fonctionnalités :

- nouvelle extension privée gipOldIDNatPS Ancien identifiant national (si changement ADELI vers RPPS),
- nouvelle extension privée gipSpecialiteRPPS Savoir-faire RPPS du titulaire,
- nouvelle extension privée gipTableauPharmacien Tableau(x) de pharmacien du titulaire,
- ajout option « Windows SmartCardLogon » dans les certificats d'authentification.

Note importante concernant la fonction Windows SmartCardLogon

L'utilisation de la fonction **Windows SmartCardLogon** nécessite l'installation de certificats d'autorité d'IGC-2ter spécifiques qui seront fournis sur demande par le support technique de l'ASIP-Santé.

Les § 4.4.1 et 4.4.2 détaillent les nouvelles extensions.

¹ Document : « CPS2ter Certificats X-509 V1-4c.doc » du 7 avril 2005

Documents de référence de l'ASIP-Santé**[1] Politiques de Certification (PC)**

Dernière version disponible sur le site WEB de l'ASIP-Santé : www.esante.gouv.fr.

Standards applicables

- [2] **RFC 3280** Internet X.509 Public Key Infrastructure : Certificate and CRL Profile
(Ce document annule et remplace le RFC 2459)
- [3] **ISO 9594-8** Information Technology – Open Systems Interconnection – The directory : authentication framework
(également ITU-T recommandation X.509)
- [4] **ISO 9834-1** Information Technology – Open Systems Interconnection
– Procedures for the operation of OSI Registration Authorities
- [5] **RFC 2253** UTF-8 String Representation of Distinguished Names
Décembre 1997

Documents d'information

- [6] **Layman's Guide to a subset of ASN.1, BER and DER**
Novembre 1993
- [7] **X.509 Style Guide de Peter GUTMANN (Conseils d'implémentation de certificats X.509)**
Mai 1999

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
ACI	Autorité de Certification Intermédiaire
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
AM	Assurance Maladie (obligatoire et complémentaire)
CDA	Carte de Directeur d'un Établissement autre que ES (ou CPA-Responsable)
CDE	Carte de Directeur d'Établissement de Santé
CPA	Carte de Personnel Autorisé
CPE	Carte de Personnel d'Établissement
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
ES	Etablissement(s) de Santé
ICP	Infrastructure de Clés Publiques
IGC	Infrastructure de Gestion de Clés
KP	Clé Publique
PC	Politique de Certification
PE	Personnel(s) d'Établissement
PF	Professionnel(s) de Santé en Formation
PS	Professionnel(s) de Santé
RDN	Relative Distinguished Name
UPN	UserPrincipalName

4 Format des Certificats X.509 des cartes CPS2ter et CPS3.1

4.1 Présentation d'un certificat X.509 version 3 (rappel)

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 de l'émetteur 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 [3] « ISO 9594-8 Information Technology – Open Systems Interconnection – The directory : authentication framework ».

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,
- informations complémentaires sur l'émetteur et le 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 [4] « ISO 9834-1 Information Technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities ».

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 de l'émetteur 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 émetteurs des certificats et de leurs porteurs

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

L'IGC-CPS2ter construit le DN de l'émetteur en fonction du domaine d'appartenance du porteur :

- domaine PROFESSIONNEL pour les professionnels de santé (PS ou PF)
- domaine STRUCTURE pour les personnels identifiés d'établissements et de structures assimilées à des établissements,
- domaine ANONYME pour les porteurs identifiés de manière indirecte (identification non nominative). Le nom et prénom de ces DN ne correspondent pas à une personne mais à une fonction ou statut (ex. Carte de dépannage, Employé 1, ...). Toutefois ce DN comporte bien un identifiant unique attaché à une structure clairement identifiée. C'est le responsable de cette structure qui doit gérer un registre qui permet de savoir à tout moment qui est le porteur pour chaque carte (pour garantir l'imputabilité des actes).

Le DN d'un porteur de certificat est construit à partir des Identifications Nationales des Professionnels de Santé et des Structures et selon son domaine d'appartenance

- Chaque DN d'un PS ou d'un PF (domaine PROFESSIONNEL) est hiérarchiquement construit avec les Relative Distinguished Names (RDN) suivants :
 - Country (France),
 - Organisation (GIP-CPS),
 - Organisational Unit (nom de la profession ou future profession),
 - RDN multivalué avec les RDN :
 - Common name (Identification Nationale du Professionnel de Santé - PS_IdNat),
 - Surname (nom d'exercice) et
 - Given name (prénom usuel),
- Chaque DN de personnel d'établissement (domaine STRUCTURE) est hiérarchiquement construit avec les Relative Distinguished Names (RDN) suivants :
 - Country (France),
 - Organisation (GIP-CPS),
 - Locality (département),
 - Organisational Unit (Identification Nationale de la Structure - Struct-IdNat),
 - RDN multivalué avec les RDN :
 - Common name (Identification Nationale de l'employé de la Structure),
 - Surname (nom d'exercice) et
 - Given name (prénom usuel).
- Les DN des porteurs identifiés indirectement (domaine ANONYME) sont construits selon les mêmes principes que ceux des personnels d'établissement en utilisant des noms et prénoms non nominatifs (par exemple des noms de fonction, de statut, ...). On nomme ces cartes « Cartes de service ».

Lorsqu'on doit renseigner un DN en tant que chaîne de texte dans des métadonnées, par exemple dans un champ du VIHf pour accéder au DMP d'un patient, il faut respecter la RFC 2253 [5].

Rappel des règles de cette RFC :

- Les RDN (chaînes séparées par des ",") doivent apparaître dans l'**ordre inverse** du certificat.
- L'**ordre des attributs à l'intérieur d'un RDN multi-valué** (les chaînes séparés par des "+") est quant à lui **indifférent**.

Exemple d'un DN de médecin Jean DUPONT avec identifiant national 0751012344 :

```
CN=0751012344+SN=DUPONT+GN=JEAN,OU=Médecin,O=GIP-CPS,C=FR
ou
SN=DUPONT+GN=JEAN+CN=0751012344,OU=Médecin,O=GIP-CPS,C=FR
ou
GN=JEAN+SN=DUPONT+CN=0751012344,OU=Médecin,O=GIP-CPS,C=FR
etc.
```

Exemple de DN d'une Autorité de Certification :

Arbre de nommage	Relative Distinguished Name	Distinguished Name dans certificat
	Racine	
	Country (C) = France	C=FR
	Organisation (O) = GIP-CPS	C=FR, O=GIP-CPS
	OrganisationalUnit (OU) = GIP-CPS PROFESSIONNEL	C=FR, O=GIP-CPS, OU=GIP-CPS PROFESSIONNEL
	CommonName (CN) = GIP-CPS CLASSE-1	C=FR, O=GIP-CPS, OU=GIP-CPS PROFESSIONNEL, CN=GIP-CPS CLASSE-1

Représentation du DN ci-dessus sous forme de chaîne de texte (RFC 2253 [5]) :

CN=GIP-CPS CLASSE-1,OU=GIP-CPS PROFESSIONNEL,O=GIP-CPS,C=FR

Note : Les DN des cartes de test comportent la mention "TEST", "VALD" ou "LABO" à la place de « GIP-CPS ».

Exemple : CN=TEST CLASSE-1,OU=TEST PROFESSIONNEL,O=TEST,C=FR

Exemple de DN d'un médecin :

Arbre de nommage	Relative Distinguished Name	Distinguished Name dans certificat
<pre> graph TD ROOT((ROOT)) --- C[C=FR] ROOT --- O[GIP-CPS] ROOT --- OU1[OU] C --- O O --- OU1 O --- O2[GIP-CPS] O --- OU2[OU] O --- OU3[OU] O2 --- CN[CN=0751012344] O2 --- SN[SN=DUPONT] O2 --- GN[GN=Jean] OU1 --- DASH1[-----] OU2 --- DASH2[-----] OU3 --- DASH3[-----] </pre>	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

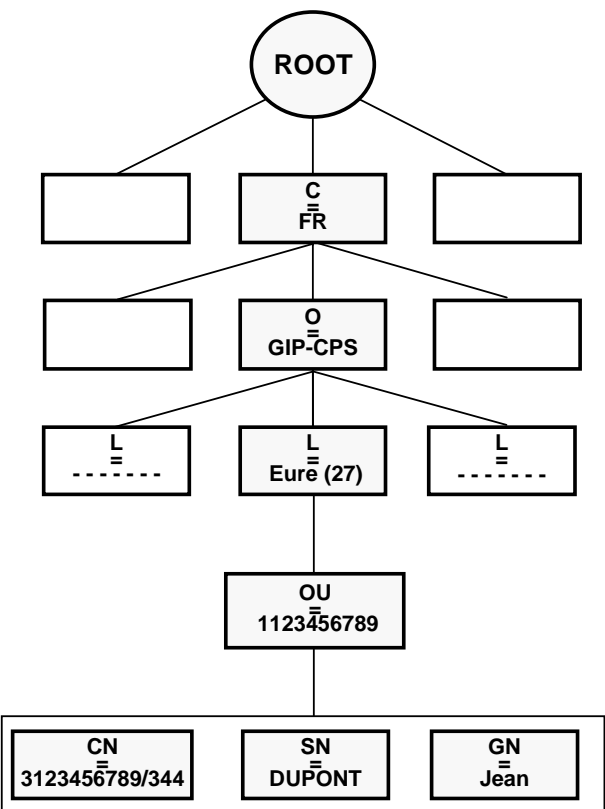
Exemple de représentation possible du DN ci-dessus sous forme de chaîne de texte (RFC 2253 [5]) :

CN=0751012344+SN=DUPONT+GN=JEAN,OU=Médecin,O=GIP-CPS,C=FR

Note : Les DN des cartes de test comportent la mention "TEST", "VALD" ou "LABO" à la place de « GIP-CPS ».

Exemple : CN=0751012344+SN=DUPONT+GN=JEAN,OU=Médecin,O=TEST,C=FR

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

Arbre de nommage	Relative Distinguished Name	Distinguished Name dans certificat
	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

Exemple de représentation possible du DN ci-dessus sous forme de chaîne de texte (RFC 2253 [5]) :

CN=3123456789/344+SN=DUPONT+GN=JEAN,OU=1123456789,L=Eure (27),O=GIP-CPS,C=FR

Note : Les DN des cartes de test comportent la mention "TEST", "VALD" ou "LABO" à la place de « GIP-CPS ».

Exemple : CN=3123456789/344+SN=DUPONT+GN=JEAN,OU=1123456789,L=Eure (27),O=TEST,C=FR

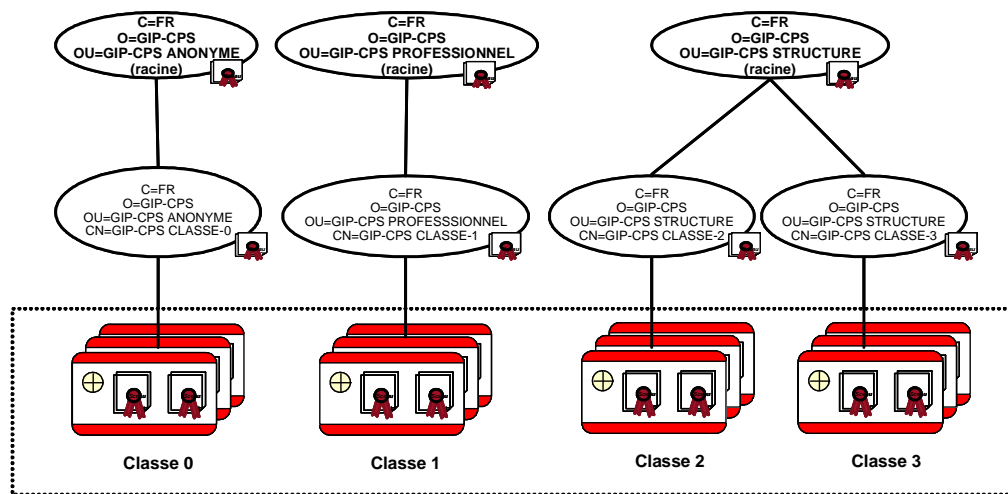
4.3 Les autorités de certification

Ce chapitre ne décrit que les certificats et les CRLs de l'IGC-CPS2ter. Les certificats utilisateurs (Classes 0 à 3) sont embarqués dans les cartes CPS2ter et CPS3.1.

4.3.1 La hiérarchie de l'IGC-CPS2ter

Il existe 3 niveaux de certificats :

1. Niveau "autorité de certification racine" de l'IGC-CPS2ter. Il y a une racine par domaine de certification :
 - **GIP-CPS ANONYME** : Pour les porteurs de type "**Indirectement identifié**" ;
 - **GIP-CPS PROFESSIONNEL** : Pour les porteurs de type "**Professionnel de Santé**" ;
 - **GIP-CPS STRUCTURE** : Pour les porteurs de type "**Employé de structure**" ;
2. Niveau "autorités de certification intermédiaires"
 - **GIP-CPS CLASSE-0 de racine GIP-CPS ANONYME** : "**Cartes de service**"
contenant les certificats des cartes CPE dont les porteurs, employés de structures, sont identifiés indirectement ;
 - **GIP-CPS CLASSE-1 de racine GIP-CPS PROFESSIONNEL** : "**Professionnels de Santé**"
contenant les certificats des cartes CPS et CPF ;
 - **GIP-CPS CLASSE-2 de racine GIP-CPS STRUCTURE** : "**Mandataires**"
contenant les certificats des cartes CDE et CDA dont les porteurs sont des responsables (statut d'exercice = 1) de structures (ES ou autres) ;
 - **GIP-CPS CLASSE-3 de racine GIP-CPS STRUCTURE** : "**Personnel habilité**"
contenant les certificats des cartes CPE et CPA dont les porteurs sont des employés de structures (avec statut d'exercice ≠ 1) ;
3. Niveau "utilisateurs" : certificats de clés publiques embarqués dans les cartes CPS2ter et CPS3.1.



Cartes CPS2ter et CPS3.1
(certificats de signature et d'authentification)

Notes :

Les certificats des cartes de test sont émis par une IGC de test (avec une hiérarchie identique) pour assurer un cloisonnement par rapport à l'IGC de production.

Les DN des certificats des Autorités de Certification de test sont :

OU=TEST <DOMAINE>,O=TEST,C=FR

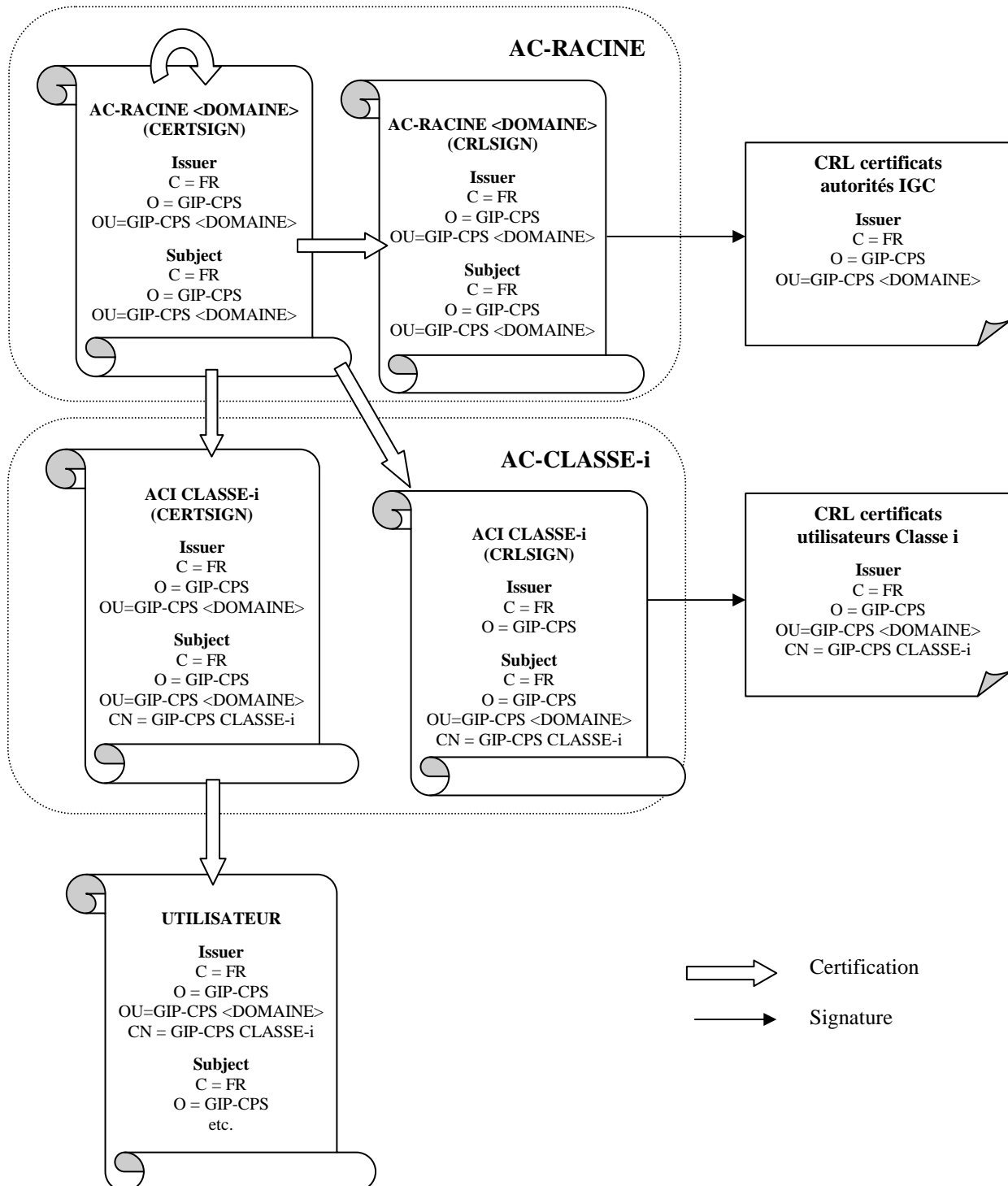
Les DN des certificats des Autorités de Certification intermédiaires de test sont :

CN= TEST CLASSE-i,OU=TEST <DOMAINE>,O=TEST,C=FR.

Chemins de certification - validation

Deux hiérarchies parallèles d'autorités sont mises en place, l'une pour la signature des certificats (certSign), l'autre pour la signature de CRL (crlSign). Dans la suite du document, en cas d'absence d'indication explicite, les autorités sont certSign.

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



4.3.2 La durée de vie des certificats

Règle de sécurité : Une clé privée d'une autorité de certification – racine ou intermédiaire - ne doit pas être utilisée pour la génération de certificats qui expireront après sa propre fin de vie.

La durée de vie des certificats liés aux cartes CPS

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

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,

La date d'expiration des premiers certificats des autorités intermédiaires est fin 2014.

Chaque AC "classe" arrêtera l'utilisation de sa clé privée au plus tard 3 ans et 1 mois (= durée de vie des certificats de clés publiques de signature des CPS) avant la fin de la vie de son certificat, soit fin novembre 2011 (à durée de vie de cartes constante).

La date d'expiration des premiers certificats de l'autorité "racine" est fin 2014.

L'AC "racine" n'utilisera pas sa clé privée pour signer des certificats d'autorités intermédiaires avec une fin de vie supérieure à fin 2014.

Avant la date de l'expiration de l'IGC-CPS2ter, une nouvelle IGC sera mise en place pour prendre le relais.

Une campagne préalable de diffusion de certificats de la nouvelle IGC sera mise en œuvre afin que les applications déployées sur le terrain soient en mesure de gérer les cartes qui embarqueront des certificats émis par cette nouvelle IGC.

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 OPTIONAL }

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 } 2

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

Extensions ::= SEQUENCE OF Extension

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

```

² Un champ "UTCTime" a le format YYMMDDMMSS (heure GMT)
SS ne doit pas être à 00 (recommandation Peter GUTMANN [7]).

4.4.1 Extensions standard utilisées dans les Certificats X.509 de l'IGC-CPS2ter

Les extensions contiennent des informations complémentaires du certificat.

Ce paragraphe contient les extensions standard utilisées dans les Certificats X.509 de l'IGC-CPS2ter.

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
```

Dans les certificats de l'IGC-CPS, l'extension `AuthorityKeyIdentifier` est le hash de la séquence complète `RSAPublicKey`.

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
```

Dans les certificats de l'IGC-CPS, l'extension `AuthorityKeyIdentifier` est le hash de la séquence complète `RSAPublicKey`.

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) }
```

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 12 « Tableau combinatoire avec extensions liées à l'usage des bi-clés ».

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 authentication serveur
id-kp-clientAuth      : TLS Web authentication client
id-kp-codeSigning     : Signature coding téléchargeable
id-kp-emailProtection : protection E-mail
id-kp-timeStamping    : Horodatage
szoid_kp_smartcard_logon : SmartCardLogon (Microsoft)
```

Notes :

- L'usage SmartCardLogon n'est présent que dans les certificats d'authentification de la CPS3.1 ;
- L'utilisation de Windows SmartCardLogon dans une structure nécessite l'installation de certificats d'IGC-CPS2ter spécifiques sur les serveurs ActiveDirectory ;
- Ces certificats seront fournis sur demande par le support technique de l'ASIP-Santé.

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).

Elle limite l'usage de la clé de signature à la date de fin de validité de la CPS ce qui permet de définir une durée de validité du certificat supérieure. Grâce à ce mécanisme, les certificats de signature peuvent être vérifiés jusqu'à un mois après la date de fin de validité de la CPS.

```
PrivateKeyUsagePeriod ::= SEQUENCE {
    NotBefore      [0]  GeneralizedTime : 1st day of validity
    NotAfter       [1]  GeneralizedTime : last day of validity } 3
```

4.4.1.6 certificatePolicies

Cette extension définit les politiques de certification dont le certificat dépend.

Cf. § 4.5 « Les identifiants d'objet (OID) » qui donne les détails concernant la construction des identifications des différentes politiques de certification de l'IGC-CPS2ter.

```
CertificatePolicies ::= SEQUENCE OF PolicyInformation
```

```
PolicyInformation ::= SEQUENCE {
    policyIdentifier      CertPolicyId }
```

```
CertPolicyId ::= OBJECT IDENTIFIER
```

³ Un champ "GeneralizedTime" a le format YYYYMMDDMMSS (heure GMT).

4.4.1.7 basicConstraints

Cette extension précise si le certificat appartient à une Autorité de Certification (Racine ou Intermédiaire) ou a un utilisateur final. Dans le premier cas, l'extension permet également de spécifier le nombre de niveaux hiérarchiques autorisés.

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

Dans l'IGC-CPS2ter, cette extension est présente dans les certificats des autorités de certification et les certificats d'utilisateurs finaux.

- Pour les Autorités de Certification, l'extension est critique et contient : CA = "TRUE" (le keyUsage doit contenir "keyCertSign") et le "pathLenConstraint" indiquant le nombre de niveaux d'AC "fille" autorisées.
- Pour les certificats d'utilisateurs finaux, l'extension n'est pas critique, elle contient uniquement une séquence vide.

4.4.1.8 crldistributionPoint

Cette extension définit l'adresse du point de distribution des CRL.

```
CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
DistributionPoint ::= SEQUENCE {
    distributionPoint      [0]      DistributionPointName OPTIONAL, }
DistributionPointName ::= CHOICE {
    fullName              [0]      GeneralNames,
    nameRelativeToCRLIssuer [1]    RelativeDistinguishedName }
```

Dans l'IGC-CPS2ter, l'adresse du point de distribution de CRL est un identifiant de ressource (URI) avec un point d'accès LDAP et un point d'accès HTTP (le point d'accès HTTP n'ayant été ajouté que depuis octobre 2008, les CPS2ter émises avant cette date ne le contiennent pas).

4.4.1.9 freshestCRL

Cette extension définit l'adresse du point de distribution de delta-CRL. La même syntaxe ASN.1 que crldistributionPoint s'applique à cette extension.

```
FreshestCRL ::= CRLDistributionPoints
```

Dans l'IGC-CPS2ter, l'adresse du point de distribution de delta-CRL est un identifiant de ressource (URI) avec un point d'accès LDAP.

Pour chaque ACR et ACI, l'Annuaire CPS publie quotidiennement une CRL et 7 delta-CRL.

Les delta-CRL permettant aux applications de « rattraper » 7 jours sans charger une CRL complète.

Toutefois, les applications doivent être capables de gérer un nombre de delta-CRL bien supérieur pour le cas où l'ASIP-Santé déciderait de publier plusieurs CRL par jour et ainsi de multiplier d'autant le nombre de delta-CRL.

4.4.1.10 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.

Cette extension est utilisée dans les certificats d'authentification des cartes CPS3.1 (Classes 0 à 3) pour indiquer le UserPrincipalName (UPN) c'est-à-dire, l'adresse mail à utiliser pour le Windows SmartCardLogon.

L'UPN est une adresse mail construite à partir de l'identifiant national du porteur de la carte (PS_IdNat)⁴, selon les règles suivantes :

- Pour les PS et PF, le PS_IdNat du porteur de la carte est construite par la concaténation du type d'identifiant et de l'identifiant du registre désigné par le type : **<Type d'identifiant><Identifiant du registre national>**.

A partir de cet identifiant, leur UPN est construit comme suit :

<Type d'identifiant>.<Identifiant du registre national>@carte-cps.fr

- un point est inséré entre le type d'identifiant et la suite de l'identifiant.

Exemples d'UPN :

- « 0.751012344@carte-cps.fr » (construit à partir du PS_IdNat 0751012344)
- « 8.99700000011@carte-cps.fr » (construit à partir du PS_IdNat 899700000011)

- Pour les PE, le PS_IdNat du porteur de la carte est construite par la concaténation du type d'identifiant, de l'identifiant de la structure, du caractère « / » et de l'identifiant du registre interne à la structure : **<Type d'identifiant><Identifiant de la structure>/<Identifiant du registre interne>**.

A partir de cet identifiant, leur UPN est construit comme suit :

<Type d'identifiant>.<Identifiant de la structure>.<Identifiant du registre interne>@carte-cps.fr

- un point est inséré entre le type d'identifiant et la suite de l'identifiant,
- le « / » est remplacé par un point.

Exemples d'UPN :

- « 1.18751275100039.0000010@carte-cps.fr » (construit à partir du PS_IdNat 118751275100039/0000010)
- « 3.123456789.0000321@carte-cps.fr » (construit à partir du PS_IdNat 3123456789/0000321)

⁴ L'identifiant national d'un porteur, PS_IdNat, fait au maximum 31 caractères.
L'UPN fait donc au maximum 46 caractères.

4.4.1.11 issuerAltName

Cette extension peut contenir un ou plusieurs noms alternatifs pour l'émetteur du certificat.

```
IssuerAltName ::= GeneralNames
```

Dans l'IGC-CPS2ter, cette extension n'est utilisée que dans les CRLs pour donner une adresse de messagerie pour le support technique.

4.4.1.12 netscapeCertType

Cette extension spécifiée par Netscape 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 12 « Tableau combinatoire avec extensions liées à l'usage des bi-clés ».

4.4.2 Extensions privées utilisées dans les Certificats X.509 de l'IGC-CPS2ter

Les extensions contiennent des informations complémentaires du certificat.

Ce paragraphe contient les extensions privées utilisées dans les Certificats X.509 de l'IGC-CPS2ter.

4.4.2.1 gipCardID

Cette extension, toujours présente, - 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-CPS).

```
GipCardID ::= PrintableString
```

4.4.2.2 gipCardCategory

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

```
GipCardCategory ::= OctetString
```

```
'00' : Carte de la famille CPS
```

```
'80' : Carte de TEST de la famille CPS
```

Les valeurs ci-dessous ne sont pas utilisées dans les certificats cartes

```
'02' : Module de sécurité (physique ou logique)
```

```
'82' : Module de sécurité de TEST
```

Nomenclature : Table G01 – Catégories cartes

4.4.2.3 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 ou CDA (CPA-Responsable)
```

Nomenclature : Table G02 – Types de cartes CPS

4.4.2.4 gipProfessionCode (optionnel)

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

```
GipProfessionCode ::= Integer
```

Nomenclature : Table G15 – Professions

4.4.2.5 gipFutureProfessionCode (optionnel)

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
```

Nomenclature : Table G16 – Futures professions

4.4.2.1 gipOldIDNatPS (extension optionnelle – uniquement pour CPS3.1)

Cette extension optionnelle contient l'ancien identifiant national contenant un n° ADELI (PS ou personne employée dans un cabinet libéral détenu par un PS identifié par un n° ADELI).

Elle est uniquement présente lorsque « PS_IdNat » (l'attribut CN du DN subject) contient un identifiant basé sur un n° RPPS et lorsque le porteur avait un ancien identifiant contenant un n° ADELI.

```
GipOldIDNatPS ::= PrintableString
```

gipOldIDNatPS est représenté sous la forme générique des identifiants de personnes (PS_IdNat) :

```
1er caractère      : type d'identifiant
caractères suivants : identifiant (PS_IdNat)
```

4.4.2.2 gipSpecialiteRPPS (extension optionnelle – uniquement CPS3.1)

Cette extension est présente uniquement si le porteur arbore au moins un savoir-faire RPPS (la spécialité d'exercice).

```
GipSpecialiteRPPS ::= SEQUENCE SIZE (1..MAX) OF SpecialiteRPPS
```

```
SpecialiteRPPS ::= UTF8String
```

Cette extension peut contenir jusqu'à un maximum de dix savoir-faire RPPS, Si elle contient plusieurs savoir-faire, la spécialité d'exercice est toujours en première position.

Dans une première phase, cette extension ne contient qu'une seule spécialité qui est la spécialité d'exercice :

- Elle est obligatoire pour les médecins.
- Elle est facultative pour les chirurgiens dentistes.
- Elle est absente dans tous les autres cas.

Nomenclature : Table R01 – Spécialités RPPS

4.4.2.3 gipTableauPharmacien (extension optionnelle – uniquement CPS3.1)

Cette extension est présente uniquement si le porteur est un pharmacien, et elle peut alors contenir jusqu'à un maximum de cinq tableaux pharmacien.

```
GipTableauPharmacien ::= SEQUENCE SIZE (1..MAX) OF TableauPharmacien
```

```
TableauPharmacien ::= UTF8String
```

Nomenclature : Table G05 – Tableaux des pharmaciens

4.5 Les identifiants d'objet (OID)

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

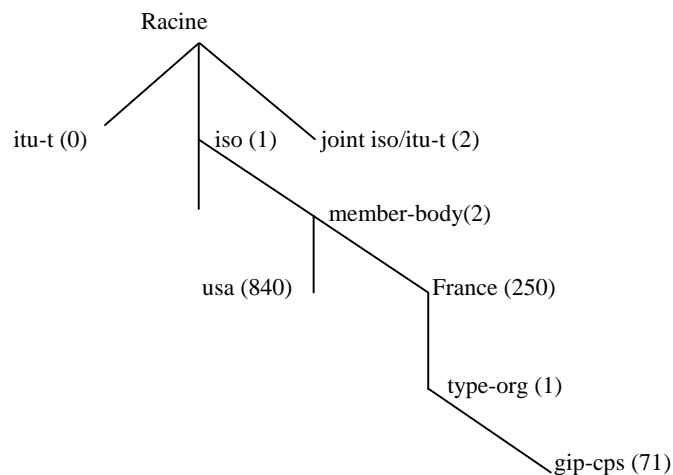
Ces OID sont organisés au niveau international sous la forme d'un arbre.

Chaque pays ou organisation (telle que la France ou l'ISO) se voit attribuer une branche.

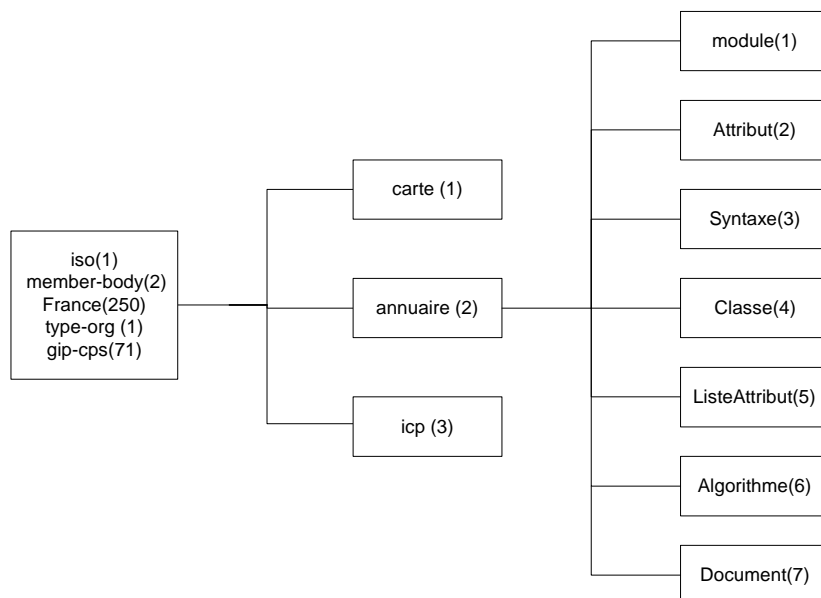
Un identifiant est attribué définitivement et peut identifier n'importe quel type d'objet.

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. Sa gestion a été reprise par l'ASIP-Santé en décembre 2009 :

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

4.5.1 Les identifiants d'objet standard utilisés dans l'IGC-CPS2ter

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
md5WithRSAEncryption	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 4 }	2A 86 48 86 F7 0D 01 01 04
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
CRLDistributionPoints	{ id-ce 31 }	55 1D 1F
authorityKeyIdentifier	{ id-ce 35 }	55 1D 23
extKeyUsage	{ id-ce 37 }	55 1D 25
freshestCRL	{ id-ce 46 }	55 1D 2E
netscape	{ joint iso/itu-t(2) country-assigments(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
Microsoft Enrollment Infrastructure	{ iso(1) identified-organization(3) dod(6) internet(1) private(4) IANA registred private enterprises(1) microsoft(311) enrollment infrastructure(20) }	2B 06 01 04 01 82 37 14
enroll_certtype_extension	{ microsoft_enrollment_infrastructure 2 }	2B 06 01 04 01 82 37 14 02
szoid_kp_smartcard_logon	{ enroll_certtype_extension 2 }	2B 06 01 04 01 82 37 14 02 02

4.5.2 Les identifiants d'objets privés utilisés dans l'IGC-CPS2ter

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
<i>gipJobCode (RFU)</i>	{ 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
<i>gipCardModel (obsolète)</i>	{ 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
<i>gipProfSitCode (RFU)</i>	{ 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
<i>gipConfPart (uniquement utilisé dans l'IGC-CPS2bis Classe-5)</i>	{ id-gip-carte-at 9 }	2A 81 7A 01 47 01 02 09
id-gip-ann (annuaire)	{ id-gip 2 }	2A 81 7A 01 47 02
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 de l'IGC-CPS2bis de TEST pour les certificats de TEST (classe-4 à 6 de TEST))	{ id-gip-icp-doc 4 }	2A 81 7A 01 47 03 07 04
gipCertificationPolicy de l'IGC-CPS2bis de production pour les certificats de serveurs applicatifs (classe-4)	{ id-gip-icp-doc 5 }	2A 81 7A 01 47 03 07 05
gipCertificationPolicy de l'IGC-CPS2bis de production pour les certificats de confidentialité classe-5)	{ id-gip-icp-doc 6 }	2A 81 7A 01 47 03 07 06
gipCertificationPolicy de l'IGC-CPS2bis de production pour les certificats des Frontaux AM (classe-6)	{ id-gip-icp-doc 7 }	2A 81 7A 01 47 03 07 07
id-gip-icp-doc-pc2004-exploit (racine des PC de l'IGC-CPS2ter de production)	{ id-gip-icp-doc 8 }	2A 81 7A 01 47 03 07 08
id-gip-icp-doc-pc2004-test (racine des PC de l'IGC-CPS2ter de TEST)	{ id-gip-icp-doc 9 }	2A 81 7A 01 47 03 07 09
id-gip-ext	{ id-gip 4 }	2A 81 7A 01 47 04
id-gip-ext-at (attribute)	{ id-gip-ext 2 }	2A 81 7A 01 47 04 02
gipOldIDNatPS	{ id-gip-ext-at 3 }	2A 81 7A 01 47 04 02 03
gipSpecialiteRPPS	{ id-gip-ext-at 5 }	2A 81 7A 01 47 04 02 05
gipTableauPharmacien	{ id-gip-ext-at 6 }	2A 81 7A 01 47 04 02 06

4.5.3 Les identifiants d'objet des PC de l'IGC-CPS2ter

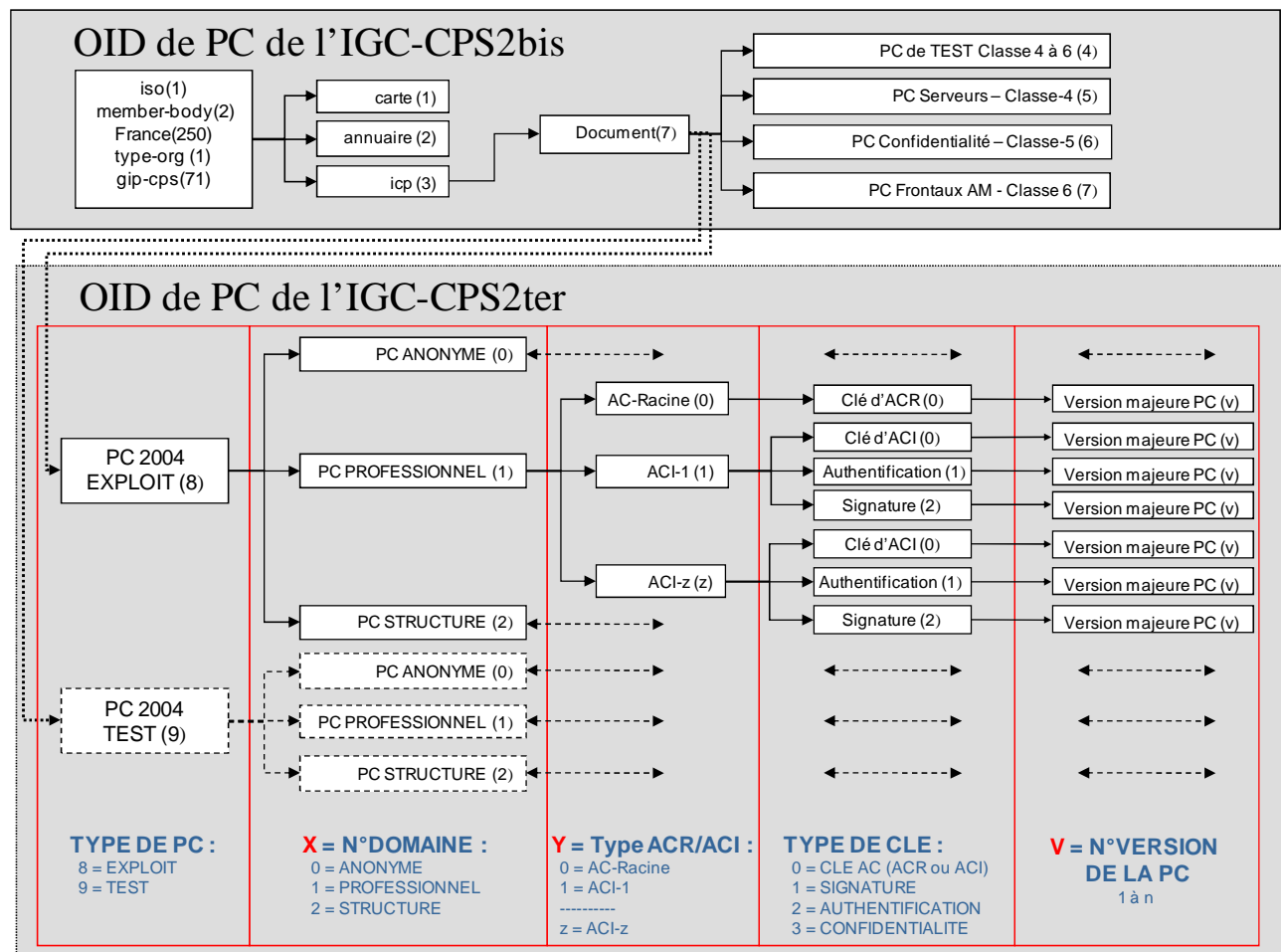
Une extension au sous-arbre d'identificateur d'objets GIP-CPS a été définie afin d'être en mesure de référencer les OID des politiques de certification (PC) des certificats de clés des cartes CPS2ter et CPS3.1.

Il existe un OID distinct pour les PC correspondant aux certificats de clés de signature et ceux de clés d'authentification.

La structure finale d'un OID de PC de l'IGC-CPS2ter est la suivante :

- Une politique de certification est attachée à chaque type de clé.
- L'OID de la PC attachée à un certificat est construit à partir de l'OID définissant les documents de l'IGC-CPS2ter { id-gip-icp-doc-pc2004-exploit } (ou { id-gip-icp-doc-pc2004-test }) complété par les informations relatives au type de certificat selon le schéma ci-après :

{ id-gip-icp-doc-pc2004-exploit }	X = N° du Domaine de certification (ACR)	Y = Type de l'AC/ACI dans ce domaine	Type de clé certifiée	V = N° de Version de la PC applicable à ce certificat }
{ id-gip-icp-doc-pc2004-test }				



La correspondance avec les classes de certificats utilisateurs finaux de la PC de l'IGC-CP2ter est donnée dans le tableau ci-dessous :

NOM DE LA CLASSE	N° DOMAINE (X)	Type d'AC (Y)	Type de clé	N° VERSION (V)
CLASSE-0 Carte de porteur identifié indirectement	ANONYME X = 0	Y = 1	1 = clé authentification 2 = clé signature	V
CLASSE-1 Carte de Professionnel de Santé	PROFESSIONNEL X = 1	Y = 1	1 = clé authentification 2 = clé signature	V
CLASSE-2 Carte d'employé Responsable de structure	STRUCTURE X = 2	Y = 1	1 = clé authentification 2 = clé signature	V
CLASSE-3 Carte d'employé de structure	STRUCTURE X = 2	Y = 2	1 = clé authentification 2 = clé signature	V

Le tableau ci-dessous donne les valeurs des OID de PC pour chacune des classes ainsi définie :

OID DE LA CLASSE DE CERTIFICATS	OBJECT IDENTIFIER (OID)	OBJECT IDENTIFIER (HEX)
id-gip-icp-doc-pc2004-exploit (applicable CPS2ter)	{ id-gip-icp-doc 8 }	2A 81 7A 01 47 03 07 08
gipCertificationPolicy pour tous les certificats du domaine ANONYME	{ id-gip-icp-doc-pc2004-exploit 0 }	2A 81 7A 01 47 03 07 08 00
Certificat d'Autorité du domaine ANONYME - ACR	{ id-gip-icp-doc-pc2004-exploit 0 0 0 V }	2A 81 7A 01 47 03 07 08 00 00 00 V
Certificat d'Autorité de CLASSE-0 – ACI -	{ id-gip-icp-doc-pc2004-exploit 0 1 0 V }	2A 81 7A 01 47 03 07 08 00 01 00 V
Certificat user de CLASSE-0 – Clé d'authentification -	{ id-gip-icp-doc-pc2004-exploit 0 1 1 V }	2A 81 7A 01 47 03 07 08 00 01 01 V
Certificat user de CLASSE-0 – Clé de signature -	{ id-gip-icp-doc-pc2004-exploit 0 1 2 V }	2A 81 7A 01 47 03 07 08 00 01 02 V
gipCertificationPolicy pour tous les certificats du domaine PROFESSIONNEL	{ id-gip-icp-doc-pc2004-exploit 1 }	2A 81 7A 01 47 03 07 08 01
Certificat d'Autorité du domaine PROFESSIONNEL - ACR	{ id-gip-icp-doc-pc2004-exploit 1 0 0 V }	2A 81 7A 01 47 03 07 08 01 00 00 V
Autorité de CLASSE-1 – ACI -	{ id-gip-icp-doc-pc2004-exploit 1 1 0 V }	2A 81 7A 01 47 03 07 08 01 01 00 V
Certificat user de CLASSE-1 – Clé d'authentification -	{ id-gip-icp-doc-pc2004-exploit 1 1 1 V }	2A 81 7A 01 47 03 07 08 01 01 01 V
Certificat user de CLASSE-1 – Clé de signature -	{ id-gip-icp-doc-pc2004-exploit 1 1 2 V }	2A 81 7A 01 47 03 07 08 01 01 02 V
gipCertificationPolicy pour tous les certificats du domaine STRUCTURE	{ id-gip-icp-doc-pc2004-exploit 2 }	2A 81 7A 01 47 03 07 08 02
Certificat d'Autorité du domaine STRUCTURE - ACR	{ id-gip-icp-doc-pc2004-exploit 2 0 0 V }	2A 81 7A 01 47 03 07 08 02 00 00 V
Autorité de CLASSE-2 – ACI -	{ id-gip-icp-doc-pc2004-exploit 2 1 0 V }	2A 81 7A 01 47 03 07 08 02 01 00 V
Certificat user de CLASSE-2 – Clé d'authentification -	{ id-gip-icp-doc-pc2004-exploit 2 1 1 V }	2A 81 7A 01 47 03 07 08 02 01 01 V
Certificat user de CLASSE-2 – Clé de signature -	{ id-gip-icp-doc-pc2004-exploit 2 1 2 V }	2A 81 7A 01 47 03 07 08 02 01 02 V
Autorité de CLASSE-3 – ACI -	{ id-gip-icp-doc-pc2004-exploit 2 2 0 V }	2A 81 7A 01 47 03 07 08 02 02 00 V
Certificat user de CLASSE-3 – Clé d'authentification -	{ id-gip-icp-doc-pc2004-exploit 2 2 1 V }	2A 81 7A 01 47 03 07 08 02 02 01 V
Certificat user de CLASSE-3 – Clé de signature -	{ id-gip-icp-doc-pc2004-exploit 2 2 2 V }	2A 81 7A 01 47 03 07 08 02 02 02 V

Pour les cartes de test, l'OID de base est { id-gip-icp-doc-pc2004-test } soit en hexadécimal : 2A 81 7A 01 47 03 07 09.

Par exemple, la valeur de l'OID pour un certificat de clé d'authentification de classe-1 de TEST devient :

Certificat user de CLASSE-1-TEST – Clé d'authentification -	Valeur complète de l'OID	Valeur hexadécimale de l'OID
{ id-gip-icp-doc-pc2004-test 1 1 1 V }	1.2.250.1.71.3.7.9.1.1.1.V	2A 81 7A 01 47 03 07 09 01 01 01 V

V = N° de version de la PC.

5 Les contenus des certificats de l'IGC-CPS2ter

5.1 Les certificats du niveau "racine" (AC RACINES)

1. Certificats ACR (auto-signés⁵) pour la génération des certificats des ACI.
2. Certificats ACR pour la signature des CRL des AC RACINE (révocation des certificats de niveau immédiatement inférieur).
3. Il y a 3 racines distinctes correspondant à chaque domaine de certification : ANONYME, PROFESSIONNEL et STRUCTURE.
4. Les clés RSA du niveau ACR ont une taille de 2048 bits.

Dans le présent paragraphe l'exemple est donné pour les certificats ACR d'un <DOMAINE>.

Objet	Format	Certificat « certSign auto-signé » d'une AC RACINE <DOMAINE>	Certificat « crlSign » d'une AC RACINE <DOMAINE>
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=GIP-CPS <DOMAINE>	
validity	UTC-Time	NotBefore : 11 octobre 2004 00:00 ⁰¹ UTC NotAfter : 31 décembre 2015 23:23 ⁵⁹ UTC	
subject	PrintString	C=FR,O=GIP-CPS, OU=GIP-CPS <DOMAINE>	
subjectPublicKeyInfo	Sequence		
algorithmIdentifier	OID	RSACryption (Parameter = NULL)	
subjectPublicKey	BitString	clé publique de 2.048 bits + exp. pub. (=2E16+1) = KP "AC RACINE <DOMAINE>"	
extensions	Sequence		
authorityKeyId	OctString	objet absent	« SHA1 KP "ACR <DOMAINE>" (certSign) »
subjectKeyId	OctString	« SHA1 KP "ACR <DOMAINE>" (certSign) »	« SHA1 KP "ACR <DOMAINE>" (crlSign) »
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	
certificatePolicies	Sequence		
certPolicyId	OID	{ id-gip-icp-doc-pc2004-exploit X 0 0 V } gipCertificationPolicy	
basicConstraints	Sequence		
critical	Boolean	true	objet absent
CA	Boolean	true	
pathLength	Integer	1	
subjectAltName	IA5string	objet absent	
netscapeCertType	BitString	objet absent	
signatureAlgorithm	OID	Sha-1WithRSAEncryption	
signatureValue	BitString	Signature sur certificat, calculée avec la clé privée "ACR <DOMAINE>" (certSign)	

certPolicyId : En fonction du DOMAINE, X prend les valeurs suivantes :

DOMAINE = ANONYME : X = 0

DOMAINE = PROFESSIONNEL : X = 1

DOMAINE = STRUCTURE : X = 2

V = N° de version de la PC.

⁵ Un certificat "auto-signé" a les caractéristiques suivantes :

- DN issuer = DN subject,
- keyUsage= keyCertSign,
- l'extension authorityKeyId est absente.

5.2 Les certificats des classes 0 à 3 (AC Intermédiaires)

1. 1 certificat de clé de certification pour chaque Autorité de Certification Intermédiaire (ACI) de chaque domaine. Ces certificats ACI sont signés par la clé de certification "racine" du domaine.
2. 1 certificat de clé de signature des CRL pour chaque classe de chaque domaine (révocation des certificats des cartes CPS de sa classe). Ces certificats sont signés par la clé de certification "racine" du domaine.
3. Les clés RSA du niveau ACI ont une taille de 2048 bits

Dans le présent paragraphe l'exemple est donné pour les certificats ACI (classe "i") d'un <DOMAINE>.

Objet	Format	Certificat « certSign » de la ACI-Classe i	Certificat « crlSign » de la ACI-Classe i
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=GIP-CPS <DOMAINE>	
validity	UTC-Time	NotBefore : 11 octobre 2004 00:00 ⁰¹ UTC NotAfter : 31 décembre 2015 23:23 ⁵⁹ UTC	
subject	PrintString	C=FR,O=GIP-CPS, OU=GIP-CPS <DOMAINE>, CN=GIP-CPS CLASSE-i	
subjectPublicKeyInfo	Sequence		
algorithmIdentifier	OID	RSAEncryption (Parameter = NULL)	RSAEncryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 2.048 bits + exp. pub. (=2E16+1) = KP "ACI CLASSE-i" (certSign)	clé publique de 2.048 bits + exp. pub. (=2E16+1) = KP "ACI CLASSE-i" (crlSign)
extensions	Sequence		
authorityKeyId	OctString	« SHA1 KP "ACR <DOMAINE>" (certSign)»	
subjectKeyId	OctString	« SHA1 KP "ACI CLASSE-i" (certSign) »	« SHA1 KP "ACI CLASSE-i" (crlSign) »
keyUsage	Sequence		
critical	Boolean	True	True
value	BitString	'04' : keyCertSign (clé de signature de certificats)	'02' : crlSign (clé de signature de CRL)
extKeyUsage	Sequence		
value(s)	OID	id-kp-clientauth + id-kp-emailProtection ⁶	objet absent
certificatePolicies	Sequence		
certPolicyId	OID	{ id-gip-icp-doc-pc2004-exploit X Y 0 V }	
crlDistributionPoint	Sequence	« ldap://annuaire.gip-cps.fr/ ou=gip-cps <Domaine>.o=gip-cps,c=fr?certificaterevocationlist;binary »	
basicConstraints	Sequence		
critical	Boolean	True	objet absent
CA	Boolean	True	
pathLength	Integer	0	
subjectAltName	IA5string	objet absent	objet absent
netscapeCertType	BitString	'06' : autorité pour certificats SSL + S/MIME ⁷	objet absent
signatureAlgorithm	OID	Sha-1WithRSAEncryption	
signatureValue	BitString	Signature du certificat, calculée avec la clé privée "ACR <DOMAINE>" (certSign)	

certPolicyId : En fonction de la CLASSE, X et Y prennent les valeurs suivantes :

CLASSE-0 (DOMAINE = ANONYME) :	X = 0	Y=1
CLASSE-1 (DOMAINE = PROFESSIONNEL) :	X = 1	Y=1
CLASSE-2 (DOMAINE = STRUCTURE) :	X = 2	Y=1
CLASSE-3 (DOMAINE = STRUCTURE) :	X = 2	Y=2

V = N° de version de la PC.

⁶ Les certificats ACI d'IGC-CPS2ter spécifiques pour SmartCardLogon ne contiennent pas l'extension extKeyUsage.

⁷ Les certificats ACI d'IGC-CPS2ter spécifiques pour SmartCardLogon ne contiennent pas l'extension netscapeCertType.

5.3 Les certificats utilisateurs : les classes 0 à 3 des cartes CPS2ter et CPS3.1

Il y a 2 certificats de clé dans les cartes CPS2ter et CPS3.1 :

1. Certificat de la clé publique de signature ; la clé de signature a une taille de 2048 bits.
2. Certificat de la clé publique d'authentification ; la clé d'authentification a une taille de 1024 bits.

Chaque type de certificat de clé publique dispose de son propre OID de PC (`certPolicyId`).

5.3.1 Les certificats des cartes de la classe 0 : "Cartes de service"

Les certificats de cette classe sont en tous points identiques aux certificats de la classe 3 : "Personnel habilité", sauf :

- L'issuer est CN=GIP-CPS CLASSE-0,OU=GIP-CPS ANONYME,O=GIP-CPS,C=FR,;
- Les porteurs sont identifiés indirectement (ex. Nom = « EMPLOYEE-1 », Prénom = « AA » mais dans une structure clairement identifiée) ;
- **Les certificats de cette classe ne sont pas publiés dans l'Annuaire-CPS ;**
- Une CRL contenant les certificats révoqués de cette classe est publiée dans l'Annuaire-CPS ;

5.3.2 Les certificats des cartes de la classe 1 : "Professionnels de Santé"

Pour distinguer de façon sûre un certificat d'un Professionnel de Santé de celui d'un Professionnel en formation, en plus du DN comportant la (future) profession l'extension privée `gipFutureProfessionCode` a été créé :

- Certificat CPS `gipProfessionCode` = identifiant profession selon la table "Professions" (l'objet `gipFutureProfessionCode` n'est alors pas renseigné)
- Certificat CPF `gipFutureProfessionCode` = identifiant future profession selon la table "Futures professions"⁸ (l'objet `gipProfessionCode` n'est alors pas renseigné)

Le tableau ci-dessous présente la structure des certificats de CLASSE-1 pour les cartes CPS et CPF.

Exemple de DN pour un médecin :

CN=0751012344+SN=DUPONT+GN=Jean,OU=Médecin,O=GIP-CPS,C=FR

Exemple de DN pour un médecin en formation :

CN=298100112344+SN=DUPONT+GN=Jean,OU=Médecin en formation,O=GIP-CPS,C=FR

⁸ Uniquement pour les futurs Médecins, Pharmaciens, Sages-Femmes et Chirurgiens-Dentistes

Certificats de clé publique de signature et d'authentification :

Objet	Format	Certificat clé de signature d'une CPS et CPF	Certificat clé d'authentification d'une CPS et CPF
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=GIP-CPS PROFESSIONNEL, CN=GIP-CPS CLASSE-1	
validity	UTC-Time	NotBefore : date début de validité carte NotAfter : date fin de validité carte + 1 mois	NotBefore : date début de validité carte NotAfter : date fin de validité carte
subject	PrintString T61String PrintString T61String T61String	C=FR,O=GIP-CPS, OU= « nom de la (future) profession », CN= « PS_IdNat », SN= « nom d'exercice », GN= « prénom usuel »	
subjectPublicKeyInfo	Sequence		
algorithmIdentifier	OID	RSAEncryption (Parameter = NULL)	RSAEncryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 2.048 bits + exp. pub. (=2E16+1)	clé publique de 1.024 bits + exp. pub. (=2E16+1)
extensions	Sequence		
authorityKeyId	OctString	« SHA1 KP "ACI CLASSE-1" (certSign) »	
subjectKeyId	OctString	« SHA1 subjectPublicKey »	
keyUsage	Sequence		
critical	Boolean	true	true
value	BitString	'C0' : digitalSignature & nonRepudiation	'80' : digitalSignature (clé d'authentification)
extKeyUsage	Sequence OID	id-kp-emailProtection	id-kp-clientauth si CPS3.1 : + szoid_kp_smartcard_logon
privateKeyUsagePeriod	GenTime	NotBefore : date début de validité carte NotAfter : date fin de validité carte	objet absent
certificatePolicies	Sequence		
certPolicyId	OID	{ id-gip-icp-doc-pc2004-exploit 1 1 2 V }	{ id-gip-icp-doc-pc2004-exploit 1 1 1 V }
basicConstraints	Sequence	Séquence vide – non-critique	
crlDistributionPoint	Sequence	« http://annuaire.gip-cps.fr/crl/gip-cps-professionnel/classe-1.crl » « ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,ou=gip-cps professionnel,o=gip-cps,c=fr ?certificaterevocationlist;binary »	
freshestCrl	Sequence	« ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,ou=gip-cps professionnel,o=gip-cps,c=fr ?deltarevocationlist;binary »	
subjectAltName	Sequence	objet absent	LogonNT (UPN - UserPrincipalName)
netscapeCertType	BitString	'20' : client S/MIME	'80' : client SSL
gipCardID	PrintString	issuerID "/" cardserialnumber	
gipCardCategory	OctString	'00' (Carte PS)	
gipCardType	Integer	'00' si CPS '01' si CPF	
gipProfessionCode	Integer	« code de la profession »	- que pour les CPS
gipFutureProfessionCode	Integer	« code de la future profession »	- que pour les CPF
gipOldIdNatPS	PrintString	Ancien « PS_IdNat »	- optionnel - que pour les CPS
gipSpecialiteRPPS	Sequence	Liste des spécialités RPPS	- optionnelle - que pour les CPS Médecins et Chirurgiens dentistes
gipTableauPharmacien	Sequence	Liste des tableaux pharmacien	- optionnelle - que pour les CPS Pharmaciens
signatureAlgorithm	OID	Sha-1WithRSAEncryption	
signatureValue	BitString	Signature du certificat, calculée avec la clé privée "ACI CLASSE-1" (certSign)	

certPolicyId : V = N° de version de la PC.

5.3.3 Les certificats des cartes de la classe 2 : "Mandataires"

Une CDE est une CPE destinée aux directeurs d'établissement de santé (ES). Son type et sa structure interne sont identiques à la CPE. En dehors du fait qu'elle se trouve dans la classe 2, elle se distingue par la mention "Directeur" sur la face avant de la carte et son Statut = 1 (responsable) est inscrit dans les données carte hors certificat (situation d'exercice).

Une CDA (ou CPA-Responsable) est une CPA destinée aux responsables de structures « non-ES ». Son type et sa structure interne sont identiques à une CPA "employé". En dehors du fait qu'elle se trouve dans la classe 2, elle se distingue uniquement par son Statut = 1 (responsable) inscrit dans les données carte hors certificat (situation d'exercice).

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

CN=3123456789/344+SN=DUPONT+GN=Jean,OU=1123456789,L=Eure (27),O=GIP-CPS,C=FR

Le tableau ci-dessous présente la structure des certificats de CLASSE-2 pour les cartes CDE et CDA.

Certificats de clé publique de signature et d'authentification :

Objet	Format	Certificat clé de signature cartes CDE et CDA Responsables de structures	Certificat clé d'authentification cartes CDE et CDA Responsables de structures
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=GIP-CPS STRUCTURE , CN=GIP-CPS CLASSE-2	
validity	UTC-Time	NotBefore : date début de validité carte NotAfter : date fin de validité carte + 1 mois	NotBefore : date début de validité carte NotAfter : date fin de validité carte
subject	PrintString T61String PrintString PrintString T61String T61String	C=FR,O=GIP-CPS, L= « nom département » « (N°) », OU= « id-nat-struct », CN= « PS_IdNat », SN= « nom d'exercice », GN= « prénom usuel »	
subjectPublicKeyInfo	Sequence		
algorithmIdentifier	OID	RSAEncryption (Parameter = NULL)	RSAEncryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 2.048 bits + exp. pub. (=2E16+1)	clé publique de 1.024 bits + exp. pub. (=2E16+1)
extensions	Sequence		
authorityKeyId	OctString	« SHA1 KP "ACI CLASSE-2" (certSign) »	
subjectKeyId	OctString	« SHA1 subjectPublicKey »	
keyUsage	Sequence		
critical	Boolean	true	true
value	BitString	'C0' : digitalSignature & nonRepudiation	'80' : digitalSignature (clé d'authentification)
extKeyUsage	Sequence OID	id-kp-emailProtection	id-kp-clientauth si CPS3.1 : + szoid_kp_smartcard_logon
privateKeyUsagePeriod	GenTime	NotBefore : date début de validité carte NotAfter : date fin de validité carte	objet absent
certificatePolicies	Sequence		
certPolicyId	OID	{ id-gip-icp-doc-pc2004-exploit 2 1 2 V }	{ id-gip-icp-doc-pc2004-exploit 2 1 1 V }
basicConstraints	Sequence	Séquence vide – non-critique	
crlDistributionPoint	Sequence	«http://annuaire.gip-cps.fr/crl/gip-cps-professionnel/classe-2.crl » « ldap://annuaire.gip-cps.fr/cn=gip-cps classe-2,ou=gip-cps structure,o=gip-cps,c=fr ?certificateRevocationList;binary »	
freshestCrl	Sequence	« ldap://annuaire.gip-cps.fr/cn=gip-cps classe-2,ou=gip-cps structure,o=gip-cps,c=fr ?deltaRevocationList;binary »	
subjectAltName	Sequence	objet absent	LogonNT (UPN - UserPrincipalName)
netscapeCertType	BitString	'20' : client S/MIME	'80' : client SSL
gipCardID	PrintString	issuerID "/" cardserialnumber	
gipCardCategory	OctString	'00' (Carte PS)	
gipCardType	Integer	'02' Si CDE '03' Si CDA (CPA-Responsable)	
signatureAlgorithm	OID	Sha-1WithRSAEncryption	
signatureValue	BitString	Signature sur certificat, calculée avec la clé privée "ACI CLASSE-2" (certSign)	

certPolicyId : V = N° de version de la PC.

5.4 Les certificats des cartes de la classe 3 : "Personnel habilité"

Ces certificats sont destinés aux porteurs de carte de type "Employé de structure".

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

CN=3123456789/344+SN=DUPONT+GN=Jean,OU=1123456789,L=Eure (27),O=GIP-CPS,C=FR

Le tableau ci-dessous présente la structure des certificats de CLASSE-3 pour les cartes CPE et CPA d'employés.

Certificats de clé publique de signature et d'authentification :

Objet	Format	Certificat clé de signature d'une CPE ou CPA Employé	Certificat clé d'authentification d'une CPE ou CPA Employé
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=GIP-CPS STRUCTURE , CN=GIP-CPS CLASSE-3	
validity	UTC-Time	NotBefore : date début de validité carte NotAfter : date fin de validité carte + 1 mois	NotBefore : date début de validité carte NotAfter : date fin de validité carte
subject	PrintString T61String PrintString PrintString T61String T61String	C=FR,O=GIP-CPS, L= « nom département » « (N°) », OU= « id-nat-struct », CN= « PS_IdNat », SN= « nom d'exercice », GN= « prénom usuel »	
subjectPublicKeyInfo algorithmIdentifier	Sequence OID	RSAEncryption (Parameter = NULL)	RSAEncryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 2.048 bits + exp. pub. (=2E16+1)	clé publique de 1.024 bits + exp. pub. (=2E16+1)
extensions	Sequence		
authorityKeyId	OctString	« SHA1 KP "ACI CLASSE-3" (certSign) »	
subjectKeyId	OctString	« SHA1 subjectPublicKey »	« SHA1 subjectPublicKey »
keyUsage	Sequence		
critical	Boolean	true	true
value	BitString	'C0' : digitalSignature & nonRepudiation	'80' : digitalSignature (clé d'authentification)
extKeyUsage value(s)	Sequence OID	id-kp-emailProtection	id-kp-clientauth si CPS3.1 : + szoid_kp_smartcard_logon
privateKeyUsagePeriod	GenTime	NotBefore : date début de validité carte NotAfter : date fin de validité carte	objet absent
certificatePolicies	Sequence		
certPolicyId	OID	{ id-gip-icp-doc-pc2004-exploit 2 2 2 V }	{ id-gip-icp-doc-pc2004-exploit 2 2 1 V }
basicConstraints	Sequence	Séquence vide – non-critique	
crlDistributionPoint	Sequence	« http://annuaire.gip-cps.fr/crl/gip-cps-professionnel/classe-3.crl » « ldap://annuaire.gip-cps.fr/cn=gip-cps classe-3,ou=gip-cps structure,o=gip-cps,c=fr ?certificaterevocationlist;binary »	
freshestCrl	Sequence	« ldap://annuaire.gip-cps.fr/cn=gip-cps classe-3,ou=gip-cps structure,o=gip-cps,c=fr ?deltarevocationlist;binary »	
subjectAltName	Sequence	objet absent	LogonNT (UPN - UserPrincipalName)
netscapeCertType	BitString	'20' : client S/MIME	'80' : client SSL
gipCardID	PrintString	issuerID "/" cardserialnumber	
gipCardCategory	OctString	'00' (Carte PS)	
gipCardType	Integer	'02' Si CPE '03' Si CPA	
gipOldIDNatPS	PrintString	Ancien « PS_IdNat »	- optionnel – que pour les CPE des cabinets libéraux
signatureAlgorithm	OID	Sha-1WithRSAEncryption	
signatureValue	BitString	Signature sur certificat, calculée avec la clé privée "ACI CLASSE-3" (certSign)	

certPolicyId : V = N° de version de la PC.

5.5 Les certificats utilisateurs de test des classes 0 à 3

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

1. Le Distinguished name de l'issuer contient :
 - O="TEST" ou "VALD" ou "LABO"
 - et OU="TEST" ou "VALD" ou "LABO"<DOMAINE>
 - et CN="TEST" ou "VALD" ou "LABO" CLASSE-i" ;
2. Le Distinguished name du subject contient : O="TEST" ou "VALD" ou "LABO" ;
3. L'extension certificationPolicy commence par { id-gip-icp-doc-pc2004-test }
4. Par exemple, la valeur de l'OID pour un certificat de clé d'authentification **de test** de classe-1 devient :

Certificat user de CLASSE-1-TEST – Clé d'authentification -	Valeur complète de l'OID	Valeur hexadécimale de l'OID
{ id-gip-icp-doc-pc2004-test 1 1 1 V }	1.2.250.1.71.3.7.9.1.1.1.V	2A 81 7A 01 47 03 07 09 01 01 01 V

V = n° de version de la PC.

6 Format des Certification Revocation Lists de l'IGC-CPS2ter

6.1 Présentation d'une CRL X.509 version 2

6.1.1 Les champs de base

Les champs de base d'une CRL renseignent les informations suivantes :

- version
- informations sur la signature de la CRL par l'AC (algorithmes et paramètres)
- nom de l'émetteur de la CRL
- date de l'émission de la CRL
- date de l'émission de la prochaine CRL
- liste de certificats révoqués composée :
 - du numéro de série du certificat révoqué
 - de la date de révocation.
 - des extensions d'entrée de CRL
- les extensions de CRL.

Extensions d'entrée de CRL

Une extension d'entrée de CRL qualifie un certificat révoqué, c'est-à-dire une entrée de la liste de certificats révoqués. Elle ne qualifie que l'entrée à laquelle elle est associée et n'affecte que le certificat identifié dans cette entrée.

Lorsqu'une implémentation traite une CRL qui ne reconnaît pas une extension d'entrée de CRL critique, elle doit supposer, au minimum, que le certificat identifié a été révoqué, qu'il n'est plus valide et les mesures conséquentes édictées dans la politique de certification doivent être prises.

- Code raison (valeur par défaut = '0' : undefined)
- Date (supposée) d'incident provoquant la révocation

6.1.2 Extensions de CRL

Une extension de CRL qualifie la liste de certificats révoqués dans son ensemble.

Lorsqu'une implémentation ne reconnaît pas une extension de CRL critique, elle doit le rejeter.

Les extensions de CRL permettent, entre autres, de spécifier plus précisément les caractéristiques suivantes :

- numéro de CRL,
- indicateur delta-CRL,
- informations sur la clé du signataire de la CRL,
- nom alternatif de l'émetteur de la CRL.

6.1.3 Schéma du contenu d'une CRL version 2

CRL (Certification Revocation List)

Contenu de la CRL (données signées)

Version 2
Informations sur la signature de la CRL par l'AC (algorithmes et paramètres)
Nom de l'émetteur de la CRL
Date d'émission de la CRL
Date d'émission de la prochaine CRL

Liste des certificats révoqués

Numéro de série du certificat révoqué	Date de révocation	Extensions d'entrée de CRL		
		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
		...		
Numéro de série du certificat révoqué	Date de révocation	Extensions d'entrée de CRL		
		Identifiant du type de l'extension	Criticité (oui / non)	Valeur
		Identifiant du type de l'extension	Criticité (oui / non)	Valeur
		...		
...				

Extensions du CRL

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 de la CRL par l'AC

Algorithmes
Paramètres

Signature numérique du contenu de la CRL

Valeur de la signature numérique du CRL par l'AC
--

6.2 Définition ASN.1 d'une CRL

```

CertificateList ::= SEQUENCE {
    tbsCertList      TBSCertList,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue   BIT STRING }

tbsCertList ::= SEQUENCE {
    version          Version OPTIONAL,
                    -- if present, shall be v2
    signature        AlgorithmIdentifier,
    issuer           Name,
    thisUpdate       Time,
    nextUpdate       Time OPTIONAL,
    revokedCertificates SEQUENCE OF SEQUENCE {
        userCertificate      CertificateSerialNumber,
        revocationDate       Time,
        crlEntryExtensions   Extensions OPTIONAL
                    -- if present, shall be v2
    } OPTIONAL,
    crlExtensions           [0] EXPLICIT Extensions OPTIONAL
                    -- if present, shall be v2
}

```

Note : Lorsqu'une (delta)-CRL est vide (pas de certificats révoqués);
revokedCertificates est une séquence de longueur 0 ('30 00').

Détails :

```
Version ::= INTEGER v2(1)
```

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

```

```
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
```

```
Extensions ::= SEQUENCE OF Extension
```

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

```

```
CertificateSerialNumber ::= INTEGER
```

6.2.1 crlEntryExtensions : Extensions liées aux certificats révoqués

Les `crlEntryExtensions` contiennent des informations complémentaires concernant le contexte de la révocation des certificats.

Les `crlEntryExtensions` `reasonCode` et `invalidationDate` ne sont pas utilisées dans l'IGC-CPS2ter.

6.2.2 crlExtensions : CRL Extensions utilisées dans les CRLs de l'IGC-CPS2ter

Les `crlExtensions` contiennent des informations complémentaires de la CRL.

6.2.2.1 authorityKeyIdentifier

Cette extension non critique identifie la clé publique à utiliser pour la vérification de la signature du CRL.

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

```
KeyIdentifier ::= OCTET STRING
```

6.2.2.2 crlNumber

Cette extension non critique donne un numéro croissant séquentiel pour chaque (delta)-CRL émise par une Autorité de Certification.

Les `crlNumbers` sont gérés de façon indépendante pour chaque émetteur de CRL : les ACR des domaines ANONYME, PROFESSIONNEL et STRUCTURE ainsi que leurs AC-Intermédiaires associées (les classes).

```
crlNumber ::= INTEGER
```

6.2.2.3 deltaCRLIndicator

Cette extension **critique** identifie la CRL comme étant une delta-CRL.

L'émission d'une delta-CRL se fait obligatoirement en même temps qu'une CRL complète (les deux ont le même `crlNumber`).

Une delta-CRL ne contient que les changements intervenus depuis la dernière CRL dont le numéro apparaît dans le champ **baseCRLNumber**.

```
deltaCRLIndicator ::= BaseCRLNumber
```

```
BaseCRLNumber ::= crlNumber
```

6.2.2.4 issuerAltName

Cette extension peut contenir un ou plusieurs noms alternatifs pour l'émetteur du certificat.

```
issuerAltName ::= 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 }
```

Dans l'IGC-CPS2ter, cette extension n'est utilisée que dans les CRLs pour donner une adresse de messagerie pour le support technique.

7 Les contenus des CRLs de l'IGC-CPS2ter

Objet	Format	CRL d'un <DOMAINE> (ACR)	CRL d'une CLASSE-i (ACI)
CertificateList	Sequence		
TbsCertList	Sequence		
Version	Integer	1 (version 2)	
signature	OID	Sha-1WithRSAEncryption	
issuer	PrintString	C=FR,O=GIP-CPS, OU=GIP-CPS <DOMAINE>	C=FR,O=GIP-CPS, OU=GIP-CPS <DOMAINE>, CN = GIP-CPS CLASSE-i
thisUpdate	UTC-Time	« date / heure d'émission CRL »	
nextUpdate	UTC-Time	« date / heure d'émission prévue prochaine CRL »	
revokedCertificates	SEQ integer Time	liste de certificats révoqués, pour chaque entrée : userCertificate revocationDate crlEntryExtensions	
crlExtensions	Sequence		
authorityKeyId	OctString	« SHA1 de la clé de signature »	
crlNumber	Integer	n° séquentiel de la CRL (<i>la numérotation est indépendante pour toutes les ACR et ACI</i>)	
deltaCrlIndicator	Sequence	<i>(uniquement pour delta-CRL)</i>	
critical	Boolean	true	
baseCrlNumber	BitString	n° séquentiel de la CRL de base	
issuerAltName	IA5string	ac-gip@gip-cps.fr ⁹	
signatureAlgorithm	OID	Sha-1WithRSAEncryption	
signatureValue	BitString	Signature de la CRL, calculée avec la clé privée "ACR <DOMAINE>" (crlSign)	Signature de la CRL, calculée avec la clé privée "ACI CLASSE-i " (crlSign)

Avec <DOMAINE> = ANONYME (CLASSE-0)
PROFESSIONNEL (CLASSE-1)
STRUCTURE (CLASSE-2 et 3)

Note : Les DN des CRLs de test comportent la mention "TEST", "VALD" ou "LABO" à la place de « GIP-CPS ».

⁹ Le domaine « GIP-CPS » n'étant plus utilisé, l'adresse ac-gip@gip-cps.fr est désormais routée sur l'adresse support-production@asipsante.fr.

8 ASN.1 (rappels)

8.1 La notation ASN.1

L'ISO décrit à travers le modèle OSI (Open Systems Interconnection) une architecture standardisée régissant les interconnexions de systèmes informatiques. La description de ce système complexe nécessite un haut niveau d'abstraction. La méthode utilisée dans le cadre de l'OSI pour spécifier des objets abstraits est appelée ASN.1 (Abstract Syntax Notation One). Chaque objet est identifié par un code qui lui est attribué de manière définitive.

L'ensemble de règles utilisé pour représenter des objets tels que des chaînes de « 1 » et de « 0 » est nommée « BER » (Basic Encoding Rules). ASN.1 est une notation souple qui permet de définir un grand nombre de types de données, qu'ils soient simples, tels que des entiers ou des chaînes de bits, basés sur des structures telles que des ensembles ou des séquences, ou complexes, c'est-à-dire définis à partir de types simples et de structures. BER décrit comment représenter ou coder les valeurs de chaque type ASN.1 comme par exemple un octet (une chaîne de 8 bits). Il y a le plus souvent plusieurs façons de coder en BER une valeur donnée.

Un autre ensemble de règles, le « DER » (Distinguished Encoding Rules), sous-ensemble du BER, donne une manière unique de coder les valeurs ASN.1.

L'ensemble de règles DER est utilisé pour des applications dans lesquelles une seule manière de coder une valeur est requise, comme c'est le cas pour la signature numérique lorsqu'elle est codée à partir des valeurs ASN.1. (En effet, une même information codée par deux méthodes différentes rendra deux signatures différentes, et empêchera tout vérification d'intégrité).

Par conséquent, la description du certificat X.509 telle qu'elle est donnée dans ce document devra être codée en ASN.1 DER.

8.2 Codification des objets en ASN.1

Chaque objet a le format TLV (TAG – LENGTH – VALUE) :

- le champ TAG indique le type d'objet,
- le champ LENGTH indique la longueur de l'objet et
- le champ VALUE contient la valeur de l'objet.

Codification du champ TAG :

Les bits 8 et 7 indiquent la classe.

Le bit 6 indique si le TAG est construit (= 1) ou simple (= 0) ; un objet construit contient 1 ou plusieurs autres objets.

Les bits 5 à 1 donnent le numéro de TAG.

Classe	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
Universal	0	0	X	Numéro du TAG				
Application	0	1	X					
Context-specific	1	0	X					
Private	1	1	X					

Si le numéro de TAG vaut 63 (bits 1 à 5 = '11111'), le TAG est sur plusieurs octets (le bit 8 de chaque octet suivant, sauf le dernier, valant 1).

Les valeurs des TAGs universels utilisés sont :

Type d'objet	Tag number (hexa)
End-of-contents (length = 0)	00
BOOLEAN	01
INTEGER	02
BIT STRING	03
OCTET STRING	04
NULL	05
OBJECT IDENTIFIER	06
SEQUENCE and SEQUENCE OF (simple)	10
SEQUENCE and SEQUENCE OF (constructed)	30 (10 + 20)
SET and SET OF (simple)	11
SET and SET OF (constructed)	31 (11 + 20)
PrintableString	13
T61String	14
IA5String	16
UTCTime	17
Generalised-time	18

Codification du champ LENGTH :

Sur 1 Octet	Sur 2 Octets	Sur 3 Octets	Etc...
L1 < 80			
81	L1		
82	L1	L2	

Note : Length = '80' : longueur indéfinie (à éviter).

8.3 Quelques particularités sur la construction d'objets

Les "INTEGER" sont codés sur n octets signés, exemples :

Valeur à coder	Format de l'objet
0	02 01 00
127	02 01 7F
128	02 02 00 80
256	02 02 01 00
-128	02 01 80
-129	02 02 FF 7F

Note : Dans l'encodage "DER" utilisé dans les certificats, la taille de l'objet doit être optimisée : tous les octets de poids fort à 0 inutiles doivent être supprimés.
La valeur de l'objet ne peut que commencer avec un 0 pour éviter qu'un integer positif soit interprété comme une valeur négative (cf. exemple pour la valeur 128).

Une "BIT STRING" commence par un octet donnant le nombre de bits non utilisés à la fin de la chaîne des octets.

Valeur à coder	Format de l'objet
1 bit à '1'	03 02 07 80
7 bits à '1'	03 02 01 FE

Un "BOOLEAN" est codé comme suit :

Valeur à coder	Format de l'objet
TRUE	01 01 FF
FALSE	01 01 00

9 Exemple de codage d'un certificat de signature d'une CPS3.1

Objet	Format	Certificat clé de signature CPS
Certificate	Sequence	
TbsCertificate	Sequence	
version	Integer	2 (version 3)
serialNumber	Integer	999999999
signature	OID	Sha-1WithRSAEncryption
issuer	PrintString	C= FR,O= GIP-CPS,OU= GIP-CPS PROFESSIONNEL,CN =GIP-CPS CLASSE-1
validity	UTC-Time	NotBefore : date début de validité carte 06 septembre 2004 00:00 ⁰¹ GMT NotAfter : date fin de validité carte+ 1 mois 30 novembre 2007 21:23 ⁵⁹ GMT
subject	PrintString T61String PrintString T61String T61String	C=FR,O=GIP-CPS, OU= Médecin, CN= 89970000011, SN= Ericsson, GN= Maria
subjectPublicKeyInfo	Sequence	
algorithmIdentifier	OID	RSAEncryption (parameter = NULL)
subjectPublicKey	BitString	clé publique de 2.048 bits + exp. pub. (=2E16+1)
extensions	Sequence	
authorityKeyId	OctString	« SHA1 KP ACI CLASSE-1 » (certSign)
subjectKeyId	OctString	« SHA1 subjectPublicKey »
keyUsage	Sequence	
critical	Boolean	true
value	BitString	'C0' : digitalSignature & nonRepudiation
extKeyUsage	Sequence	
value(s)	OID	id-kp-emailProtection
privateKeyUsagePeriod	GenTime	NotBefore : date début de validité carte 06 septembre 2004 00:00 ⁰¹ UTC NotAfter : date fin de validité carte 31 octobre 2007 21:23 ⁵⁹ UTC
certificatePolicies	Sequence	
certPolicyId	OID	{ id-gip-icp-doc-pc2004-exploit 1 1 2 1 } (V = 1)
basicConstraints	Sequence	End-User par défaut - Séquence vide – non-critique
crlDistributionPoint	Sequence	« http://annuaire.gip-cps.fr/crl/professionnel/classe-1.crl,» « ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,ou=gip-cps professionnel,o=gip-cps,c=fr?certificaterevocationlist;binary »
freshestCrl	Sequence	« ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,ou=gip-cps professionnel, o=gip-cps,c=fr?deltarevocationlist;binary »
certPolicyId	OID	{ id-gip-icp-doc-pc2004-exploit 1 1 2 V } gipCertificationPolicy
subjectAltName	Sequence	objet absent
gipCardID	PrintString	issuerID "/" cardserialnumber
gipCardCategory	OctString	'00' (Carte PS)
gipCardType	Integer	'00' (CPS)
gipProfessionCode	Integer	10 = médecin
gipFutureProfessionCode	Integer	objet absent
gipOldIDNatPS	PrintString	Ancien « PS_IdNat » = "0751012345" (identifiant ADELI)
gipSpecialiteRPPS	Sequence	Spécialités RPPS = "SM26"
signatureAlgorithm	OID	Sha-1WithRSAEncryption
signatureValue	BitString	Signature sur certificat, calculée avec la clé privée "ACI CLASSE-1" (certSign)

```

30 82 LL LL -- SIGNED SEQUENCE (Certificate)
  30 82 LL LL -- SEQUENCE (TbsCertificate)
    A0 03 -- [0] Version:
      02 01 -- INTEGER
        02 -- 2 (version 3)

    -- Serial Number:
    02 05 -- INTEGER (positive)
      'xx xx' -- << 999999999 >>

    -- signatureAlgorithm algorithmIdentifier:
    30 0D -- SEQUENCE
      06 09 -- OBJECT IDENTIFIER:
        -- sha-1WithRSAEncryption
        -- << 1 2 840 113549 1 1 5 >>

        2A 86 48 86 F7 0D 01 01 05 -- NULL (Parameters)
        05 00

    -- Issuer :
    30 5A -- SEQUENCE OF (relDistName)

```

```

31 0B          -- SET OF (AttValueAssertion)
30 09          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 04 06      -- Country
13 02          -- PRINTABLE STRING
46 52          -- «FR»

31 10          -- SET OF (AttValueAssertion)
30 0E          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 04 0A      -- Organisation
13 07          -- PRINTABLE STRING
                -- «GIP-CPS»
47 49 50 2D 43 50 53

31 1E          -- SET OF (AttValueAssertion)
30 1C          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 04 0B      -- Organisational unit
13 15          -- PRINTABLE STRING
                -- «GIP-CPS PROFESSIONNEL»
47 49 50 2D 43 50 53 20
50 52 4F 46 45 53 53 49 4F 4E 4E 45 4C

31 19          -- SET OF (AttValueAssertion)
30 17          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 04 03      -- Common Name
13 10          -- PRINTABLE STRING
                -- «GIP-CPS CLASSE-1»
47 49 50 2D 43 50 53 20
43 4C 41 53 53 45 2D 31

                -- validity:
30 1E          -- SEQUENCE
17 0D          -- UTC-Time (NotBefore)
                -- «040906000001Z» (Z=GMT)
30 34 30 39 30 36 30 30 30 30 30 31 5A --
17 0D          -- UTC-Time (NotAfter)
                -- «071130215959Z» (Z=GMT)
30 37 31 31 33 30 32 31 35 39 35 39 5A

30 LL          -- subject :
                -- SEQUENCE OF (RelDistName)

31 0B          -- SET OF (AttValueAssertion)
30 09          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 04 06      -- Country
13 02          -- PRINTABLE STRING
46 52          -- «FR»

31 10          -- SET OF (AttValueAssertion)
30 0E          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 04 0A      -- Organisation
13 07          -- PRINTABLE STRING
                -- «GIP-CPS»
47 49 50 2D 43 50 53

31 10          -- SET OF (AttValueAssertion)
30 0E          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 04 0B      -- Organisational Unit
14 07          -- T61 STRING
4D E9 64 65 63 69 6E -- "Médecin"

31 LL          -- SET OF (AttValueAssertion)
30 11          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 04 03      -- CommonName = PS-IdNat
13 0C          -- printable string: «RPPS 89970000011»
38 39 39 39 30 30 30 30 30 30 31 31
30 0F          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 04 04      -- Surname
14 08          -- T61 STRING: «Ericsson»
45 72 69 63 73 73 6F 6E
30 0C          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER

```

```

55 04 2A          -- Given name
14 05            -- T61 STRING: «Maria»
30 82 01 22      -- SubjectPublicKeyInfo:
30 0D            -- SEQUENCE
06 09           -- SEQUENCE (algorithmIdentifier)
                -- OBJECT IDENTIFIER:
                -- RSAEncryption
                -- << 1 2 840 113549 1 1 1 >>
2A 86 48 86 F7 0D 01 01 01
05 00           -- NULL (Parameter)
03 82 01 0F      -- BIT STRING (SubjectPublicKey)
00             -- 0 unused bits at the end of the string

30 82 01 0A      -- séquence RSAPublicKey sur 2.048 bits
02 82 01 01     -- integer (256 ou 257 bytes)
00             -- 0 byte to force positive value
                -- obligatoire si premier octet
                -- du modulo > '7F', sinon facultatif
                -- + modulo sur 2048 bits :
FF 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
02 03         -- integer
01 00 01     -- public exponent = 2E16+1

A3 LL          -- [3] Extensions:
30 LL         -- SEQUENCE OF Extension

30 1F         -- SEQUENCE
06 03        -- OBJECT IDENTIFIER
55 1D 23     -- authorityKeyId
04 18        -- OCTET STRING
30 16        -- sequence
80 14        -- keyIdentifier:
XX ... XX   -- SHA-1 de la clé ACI CLASSE-1 (certSign)

30 1D         -- SEQUENCE
06 03        -- OBJECT IDENTIFIER
55 1D 0E     -- subjectKeyID
04 16        -- OCTET STRING
04 14        -- octet string
XX ... XX   -- SHA-1 de la séquence contenant la clé certifiée
                -- 160 bits calculés sur la séquence RSAPublicKey
                -- incluant le tag et la longueur

30 0E         -- SEQUENCE
06 03        -- OBJECT IDENTIFIER
55 1D 0F     -- keyUsage
01 01 FF     -- BOOLEAN : Critical=true
04 04        -- OCTET STRING
03 02        -- bit string
06          -- 6 unused bits at the end of string
C0          -- bits 0+1 := TRUE, digitalSig & nonRepudiation

30 14         -- SEQUENCE
06 03        -- OBJECT IDENTIFIER
55 1D 25     -- Extended keyUsage
04 0D        -- OCTET STRING
30 0A        -- SEQUENCE OF keyPurposeId
06 08        -- OID
2B 06 01 05 05 07 03 04
                -- id-kp-emailProtection

```

```

30 2B          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 1D 10      -- privateKeyUsagePeriod
              -- only if keyUsage = non Repudiation
04 24          -- OCTET STRING
30 22          -- SEQUENCE
80 0F          -- Generalised-Time (not Before)
              -- 20040906000001Z
32 30 30 34 30 39 30 36 30 30 30 30 31 5A
81 0F          -- Generalised-Time (not After)
              -- 20071031215959Z
32 30 30 37 31 30 33 31 32 31 35 39 35 39 5A

30 19          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 1D 20      -- certificatePolicies
04 12          -- OCTET STRING
30 10          -- sequence PolicyInformation
30 0E          -- sequence (certPolicyId)
06 0C          -- object identifier:
              -- { id-gip-icp-doc-pc2004-exploit 1 1 2 1 }
              -- gipCertificationPolicy
2A 81 7A 01 47 03 07 08 01 01 02 01

30 09          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 1D 13      -- basicConstraints
04 02          -- OCTET STRING
30 00          -- SEQUENCE

30 81 CB       -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 1D 1F      -- crlDistributionPoints
04 81 C3       -- OCTET STRING
30 81 BE       -- SEQUENCE of DistributionPoints
30 3F          -- SEQUENCE DistributionPoint
A0 3D          -- DistributionPointName
A0 3B          -- GeneralNames
86 39          -- uniformResourceIdentifier IMPLICIT IA5STRING
              -- << http://annuaire.gip-cps.fr/crl/professionnel
              -- /classe-1.crl >>
68 74 74 70 3A 2F 2F 61 6E 6E 75 61 69 72 65 2E
67 69 70 2D 63 70 73 2E 66 72 2F 63 72 6C 2F 70
72 6F 66 65 73 73 69 6F 6E 6E 65 6C 2F 63 6C 61
73 73 65 2D 31 2E 63 72 6C

30 7D          -- SEQUENCE DistributionPoint
A0 7B          -- DistributionPointName
A0 79          -- GeneralNames
86 77          -- uniformResourceIdentifier IMPLICIT IA5STRING
              -- << ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,
              -- ou=gip-cps professionnel,o=gip-cps,c=fr?
              -- certificaterevocationlist;binary >>
6C 64 61 70 3A 2F 2F 61 6E 6E 75 61 69 72 65 2E
67 69 70 2D 63 70 73 2E 66 72 2F 63 6E 3D 67 69
70 2D 63 70 73 20 63 6C 61 73 73 65 2D 31 2C 6F
75 3D 67 69 70 2D 63 70 73 20 70 72 6F 66 65 73
73 69 6F 6E 6E 65 6C 2C 6F 3D 67 69 70 2D 63 70
73 2C 63 3D 66 72 3F 63 65 72 74 69 66 69 63 61
74 65 72 65 76 6F 63 61 74 69 6F 6E 6C 69 73 74
3B 62 69 6E 61 72 79

30 81          -- SEQUENCE
06 03          -- OBJECT IDENTIFIER
55 1D 2E      -- freshestCRL
04 7A          -- OCTET STRING
30 78          -- SEQUENCE of DistributionPoints
30 76          -- SEQUENCE DistributionPoint
A0 74          -- DistributionPointName
A0 72          -- GeneralNames
86 70          -- uniformResourceIdentifier IMPLICIT IA5STRING
              -- << ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,
              -- ou=gip-cps professionnel,o=gip-cps,c=fr?
              -- deltarevocationlist;binary >>
6C 64 61 70 3A 2F 2F 61 6E 6E 75 61 69 72 65 2E
67 69 70 2D 63 70 73 2E 66 72 2F 63 6E 3D 67 69

```



```

01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00
01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00
01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00
01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00
01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00
01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00
01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00

```

10 D'autres exemples de codage d'extensions

Ci-dessous quelques exemples de codage d'extensions absentes dans l'exemple ci-dessus.

Extension subAltName contenant un UPN à partir d'un identifiant RPPS « 899700000011 »

```

30 LL -- SEQUENCE
 06 03 -- OBJECT IDENTIFIER
    55 1D 11 -- subAltName
 04 LL -- OCTET STRING
    30 LL -- sequence of generalName
      A0 LL -- Other Name
        06 0A -- OID : Microsoft UPN
          2B 06 01 04 01 82 37 14 02 03
        A0 1C -- SEQUENCE
          0C 1A -- UTF8 string : identifiant RPPS « 899700000011 »
            -- << 8.99700000011@carte-cps.fr >>
            38 2E 39 39 37 30 30 30 30 30 30 30 31 31 2D 63 61
            72 74 65 2D 63 70 73 2E 66 72

```

Extension gipTableauPharmacien pour un pharmacien

```

30 1C -- SEQUENCE
 06 08 -- OID : gipTableauPharmacien
 2A 81 7A 01 47 04 02 06
 04 08 -- OCTET STRING
 30 06 -- SEQUENCE
 0C 01 -- UTF8 string:
 41 Tableau Pharmacien 1 «A» (titulaire officine)
 0C 01 -- UTF8 string:
 47 Tableau Pharmacien 2 «G» (biologiste)

```

11 Exemple de CRL

Exemple de CRL version 2.

L'issuer est : CN=GIP-CPS CLASSE-3,OU=GIP-CPS STRUCTURE,O=GIP-CPS,C=FR.

La date d'émission est le 12/07/04 et la prochaine date d'émission est le 12/09/04.

Deux certificats (les numéros 18 et 24) sont révoqués, en date respectivement du 05/07/04 et du 09/07/04.

Numéro de CRL = 25.

En ajoutant l'extension deltaCRLIndicator (encadrée dans l'exemple ci-dessous), cette CRL devient une delta-CRL numéro 25 contenant uniquement les modifications par rapport à la CRL numéro 24,

```

30 82 LL LL          -- SIGNED SEQUENCE (CertificateList)
  30 82 LL LL        -- SEQUENCE (TBSCertList)
    02 01            -- Version
      01              -- INTEGER
                        -- 1 (version 2)
    30 0D            -- signatureAlgorithm algorithmIdentifier:
      06 09          -- SEQUENCE
                        -- OBJECT IDENTIFIER:
                        -- sha-1WithRSAEncryption
                        -- << 1 2 840 113549 1 1 5 >>
        2A 86 48 86 F7 0D 01 01 05
        05 00        -- NULL (Parameters)
    30 56            -- Issuer :
      SEQUENCE OF (RelDistName)
        31 0B        -- SET OF (AttValueAssertion)
          30 09      -- SEQUENCE
            06 03    -- OBJECT IDENTIFIER
              55 04 06 -- Country
            13 02    -- PRINTABLE STRING
              46 52    -- «FR»
        31 10        -- SET OF (AttValueAssertion)
          30 0E      -- SEQUENCE
            06 03    -- OBJECT IDENTIFIER
              55 04 0A -- Organisation
            13 07    -- PRINTABLE STRING
              47 49 50 2D 43 50 53 -- «GIP-CPS»
        31 1A        -- SET OF (AttValueAssertion)
          30 09      -- SEQUENCE
            06 03    -- OBJECT IDENTIFIER
              55 04 0B -- Organisational Unit
            13 11    -- PRINTABLE STRING
              47 49 50 2D 43 50 53 20
              53 54 52 55 43 54 55 52 45
        31 19        -- SET OF (AttValueAssertion)
          30 09      -- SEQUENCE
            06 03    -- OBJECT IDENTIFIER
              55 04 03 -- Organisational Unit
            13 10    -- PRINTABLE STRING
              47 49 50 2D 43 50 53 20
              43 4C 41 53 53 45 2D 33
    17 0D            -- UTC-Time (Date d'émission)
      -- «040712000000Z» (Z=GMT)
    30 34 30 37 31 32 30 30 30 30 30 30 5A --
    17 0D            -- UTC-Time (Date prévue prochaine CRL)
      -- «040912000000Z» (Z=GMT)
    30 34 30 39 31 32 30 30 30 30 30 30 5A --

```

```

30 LL -- SEQUENCE OF (liste des certificats révoqués)

30 12 -- SEQUENCE (Certificat révoqué)
02 01 -- INTEGER
12 -- 18 (n° de série)

17 0D -- UTC-Time (Date de révocation)
-- «0407050000Z» (Z=GMT)
30 34 30 37 30 35 30 30 30 30 30 30 5A --

30 12 -- SEQUENCE (Certificat révoqué)
02 01 -- INTEGER
18 -- 24 (n° de série)

17 0D -- UTC-Time (Date de révocation)
-- «0407090000Z» (Z=GMT)
30 34 30 37 30 39 30 30 30 30 30 30 5A -

A0 LL -- [0] crlExtensions
30 LL -- SEQUENCE OF Extension

30 1F -- SEQUENCE
06 03 -- OBJECT IDENTIFIER
55 1D 23 -- authorityKeyId
04 18 -- OCTET STRING
30 16 -- sequence
80 14 -- keyIdentifier:
XX ... XX -- SHA-1 de la clé CRL-Sign de la CLASSE-3

30 0A -- SEQUENCE
06 03 -- OBJECT IDENTIFIER
55 1D 14 -- CRLNumber {id-ce 20}
04 03 -- OCTET STRING
02 01 -- INTEGER
19 -- N° 25

```

Extension conditionnelle : uniquement présente si la présente CRL est une delta-CRL :

```

30 0E -- SEQUENCE
06 03 -- OBJECT IDENTIFIER
55 1D 1B -- deltaCRLIndicator {id-ce 27}
01 01 FF -- BOOLEAN : Critical=true
04 03 -- OCTET STRING
02 01 -- INTEGER
18 -- N° 24

```

```

30 1C -- SEQUENCE
06 03 -- OBJECT IDENTIFIER
55 1D 12 -- issuerAltName
04 15 -- OCTET STRING
30 13 -- sequence of generalName
81 11 -- rfc822name: IMPLICIT IA5STRING
-- << ac-gip@gip-cps.fr >> 10
61 63 2D 67 69 70 40 67 69 70 2D 63 70 73 2E 66 72

```

¹⁰ Idem note bas de page 40 du chapitre 7.

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

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

Type de certificats	keyUsage (critique)	extendedKeyUsage	netscapeCertType
Certificats des AC-RACINE	'04' : keyCertSign	absent	absent
Certificats des AC intermédiaires (classes 0 à 3)	'04' : keyCertSign	id-kp-clientauth id-kp-emailProtection	'06' : autorité pour signer certificats SSL + S/MIME
Certificats de signature de CRL (AC-RACINE et AC intermédiaires)	'02' : crlSign	absent	absent
Certificats des Cartes CPS2ter et CPS3.1 (Classe 0 à 3) :			
Certificat de Signature	'C0' : digitalSig & nonRep	id-kp-emailProtection	'20' : client S/MIME
Certificat d'Authentification	'80' : digitalSignature	id-kp-clientauth si CPS3.1 : + szoid_kp_smartcard_logon	'80' : client SSL

Note importante concernant la fonction Windows SmartCardLogon

Lorsqu'un établissement souhaite mettre en œuvre le Windows SmartCardLogon avec des CPS, il ne faut pas installer les certificats de l'IGC-CPS2ter officiels sur les serveurs ActiveDirectory.

L'utilisation de cette fonction nécessite l'installation de « **certificats AC Intermédiaires d'IGC-CPS2ter spécifiques pour SmartCardLogon** » qui seront fournis sur demande par le support technique de l'ASIP-Santé.

Les gabarits spécifiques de ces certificats ACI sont identiques à ceux des « certificats ACI officiels » mais ils ne contiennent pas les extensions **extendedKeyUsage** et **netscapeCertType**.

13 Gestion des versions

13.1 Version 1.0 : Création du document

1. Reprise à partir du document « CPS2ter Certificats X-509 V1-4c.doc » du 7 avril 2005.
2. Intégration des évolutions associées à la CPS3.1.
 - intégration de nouvelles extensions privées gipOldIDNatPS, gipSpecialiteRPPS et gipTableauPharmacien,
 - ajout option « Windows SmartCardLogon ».
3. Mise en conformité des DN au standard RFC 2253 [5].

13.2 Version 1.1 : Modification mineure

1. Suppression du document précédemment référencé [2].