Cahier des charges pour le référencement des produits de sécurité et des offres de prestataires de services de confiance

Version 1

Historique des versions

Date	Version	Évolutions du document
14 févr. 2012	1.0	Première version.

Commentaires

Les commentaires sur le présent document sont à adresser à :

Service Projets
64-70 allée de Bercy
75012 Paris

rgs.dgme@finances.gouv.fr

Sommaire

1. Introduction

1.1. Présentation générale

Ce document est le cahier des charges permettant le référencement de produits de sécurité et d'offres de prestataires de services de confiance (PSCO) tel qu'appelé par le décret n° 2010-112 du 2 février 2010 ([Décret_RGS]) pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 ([Ordonnance]) relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Il formalise les règles que doivent respecter les offres de PSCO et les produits de sécurité afin d'être référencés par l'État, attestant ainsi de leur interopérabilité avec les téléservices de l'État.

Ce document s'adresse donc en premier lieu aux PSCO et fournisseurs de produits de sécurité qui souhaitent faire référencer leurs offres de services et produits. Il permet également aux autorités administratives de connaître les caractéristiques des offres de services et des produits conformes aux exigences du référencement selon l'[Ordonnance] et de mettre à niveau leurs systèmes d'information pour supporter les offres et les produits de sécurité référencés.

1.2. Périmètre

La présente version de ce cahier des charges traite du référencement des offres de PSCO et de produits de sécurité, à destination des agents de l'administration et des particuliers, utilisées dans le cadre de la mise en œuvre des fonctions de sécurité suivantes :

- « Authentification » (cf. annexes [RGS_A_2] et [RGS_A_7] du référentiel général de sécurité),
- « Signature » (cf. annexes [RGS_A_3] et [RGS_A_8] du référentiel général de sécurité).

Dans le cadre du présent cahier des charges, seules les offres de PSCO et les produits de sécurité qui ont été qualifiés au regard des niveaux de sécurité ** (2 étoiles) et *** (3 étoiles) du référentiel général de sécurité (RGS) peuvent faire l'objet d'un référencement, comme illustré ci-dessous.

Fonctions	Population			
	Administration	Entreprise	Particulier	Service applicatif
Authentification	★★ ★★★	-	★★ ★★★	-
Signature	★★ ★★★	-	★★ ★★★	-
Authentification et signature	-	-	-	-
Confidentialité	-	-	-	-
Authentification serveur	-	-	-	-
Cachet	-	-	-	-
Horodatage	-	-	-	-

Ce document ne traite pas des applications de création de signature, des modules de vérification des signatures électroniques et des formats de signature électronique (XAdES, CAdES, PAdES, etc.).

Le périmètre présenté ci-dessus pourra être étendu, en termes de « niveaux de sécurité », de « fonctions de sécurité » et de « population », afin de permettre le référencement d'offres de PSCO ou de produits de sécurité destinés à couvrir de nouveaux besoins et usages autres que ceux actuellement identifiés (exemples : carte agent, carte nationale d'identité, label IDéNUM, …). Chaque extension se traduira par une nouvelle version du présent cahier des charges.

1.3. Références documentaires

Référence	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004
[Décret_RGS]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[ETSI_CERT]	ETSI - TS 102 280 - X.509 V3 Certificate Profile for Certificates Issued to Natural Persons – version 1.1.1
[IAS_ECC]	Carte européenne pour les applications de services électroniques (e-services) et d'identité électronique (e-ID) – IAS ECC – Identification Authentication Signature – Carte Européenne du citoyen – Spécifications Techniques – Révision 1.0.1
[Ordonnance]	Ordonnance n° 2005-1516 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[RFC_5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – version de mai 2008
[RGS_A_2]	Fonction de sécurité « Authentification » – version 2.3
[RGS_A_3]	Fonction de sécurité « Signature » – version 2.3
[RGS_A_7]	Politique de certification type « Authentification » – version 2.3
[RGS_A_8]	Politique de certification type « Signature » – version 2.3
[RGS_A_14]	Profils de certificats, CRL, OCSP et algorithmes cryptographiques – version 2.3
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques – version 1.20

1.4. Sites Internet

Site	Lien
Site de l'ANSSI	http://www.ssi.gouv.fr
Site de l'ANTS	http://www.ants.interieur.gouv.fr/ias/-ias-.html
Site de la DGME	http://references.modernisation.gouv.fr

2. Règles et recommandations pour assurer l'interopérabilité

Cette section présente les règles et recommandations à satisfaire pour assurer l'interopérabilité des offres des prestataires de services de confiance et des produits de sécurité avec les systèmes d'information (SI) des autorités administratives.

Les PSCO et fournisseurs de produits de sécurité sont incités à respecter les recommandations formulées dans le présent document. Celles-ci ne sont pas d'application obligatoire dans cette version du document mais devraient le devenir dans une version ultérieure.

2.1. Offres de certificats électroniques

Cette section présente les règles relatives aux gabarits de certificats qui viennent en complément de celles fixées par l'annexe [RGS_A_14] du RGS.

2.1.1. Algorithmes cryptographiques et longueurs de clés

Les algorithmes cryptographiques ainsi que les longueurs de clés utilisés pour la signature des certificats d'AC et de porteurs sont définis dans l'annexe [RGS_B_1] du RGS.

Le tableau ci-dessous présente les exigences en la matière pour le référencement. Les algorithmes et longueurs de clés qui ne figurent pas dans ce tableau ne sont pas éligibles au référencement.[1]

Il est à noter que certains algorithmes et longueurs de clés sont considérés conformes pendant une période limitée. Pour ces cas particuliers, la limite est indiquée dans le tableau.

Type	Algorithme et longueur de clé	Certificat d'AC	Certificat de porteur
Fonction de hachage	**SHA-1**	Non recommandé et interdit à partir du 6 mai 2013	Non recommandé et interdit à partir du 6 mai 2013
Fonction de hachage	**SHA-256**	Conforme	Conforme
Fonction de signature	**RSA avec clé de 2048 bits**	Conforme jusqu'en 2020	Conforme jusqu'en 2020
Fonction de signature	**RSA avec clé de 4096 bits**	Conforme	Conforme
Fonction de signature	**ECDSA P-256** [2]	Conforme	Conforme

[1] Les longueurs de clés données sont révisables dans le temps pour tenir compte de l'adoption progressive de longueurs de clés plus importantes.

[2] L'usage de cet algorithme pour la carte agent est lié aux futures évolutions de la norme IAS ECC, la version 1.0.1 de la norme ne prévoyant actuellement pas le support de cet algorithme.

2.1.2. Identification de l'AC et du porteur dans un certificat électronique

Le champ `subject` d'un certificat électronique indique le sujet du certificat, qui peut être en fonction du type de certificat et dans le cadre du présent cahier des charges, une autorité de certification (AC) ou un porteur. Le champ `issuer` représente l'émetteur du certificat. Il identifie donc l'AC qui a émis le certificat.

Le porteur et l'autorité de certification sont identifiés dans les champs mentionnés précédemment par un DN (distinguished name) qui est lui-même composé d'une série d'attributs. Le format du DN doit être conforme au [RFC_5280] ainsi qu'au chapitre VII de l'annexe [RGS_A_14] du RGS, moyennant les précisions du présent chapitre.

2.1.2.1. Identification de l'AC

La présente section concerne l'identification de l'AC qui figure dans :

- le champ `issuer` des certificats d'AC ou de porteurs,
- le champ `subject` pour les certificats d'AC.

2.1.2.1.1. Attributs

Le tableau ci-dessous présente les attributs à utiliser obligatoirement pour l'identification d'une autorité de certification. Il précise pour chacun le contenu de l'attribut et l'encodage à utiliser (cf. [RFC_5280]).

Attribut	Contenu	Encodage
`commonName`	Nom de l'AC	`UTF8String`
`organizationName`	Nom de l'organisation responsable de l'AC	`UTF8String`
`organizationalUnitName`	Identification de l'organisation responsable de l'AC	`UTF8String`
`countryName`	Pays où est enregistré l'AC	`PrintableString`

Les sections suivantes précisent les règles et recommandations concernant ces attributs. L'utilisation d'attributs autres que ceux listés précédemment n'est pas recommandée.

*2.1.2.1.2. Nom de l'AC (attribut **`commonName`**)*

Le nom de l'AC doit être indiqué dans le DN en utilisant l'attribut `commonName`. Ce nom doit être significatif et être cohérent avec le nom officiel de l'AC. L'utilisation des attributs `givenName` et `surname` n'est pas autorisée.

*2.1.2.1.3. Nom et identification de l'entité responsable de l'AC (attributs **`organizationName`** et **`organizationalUnitName`**)*

L'attribut `organizationName` doit être présent et contenir un nom significatif de l'entité de l'AC émettant le certificat. Ce nom doit être cohérent avec le nom officiel de l'entité. Il est recommandé de renseigner dans cet attribut le nom officiel complet de l'AC émettant le certificat tel qu'enregistré auprès des autorités compétentes.

En complément de cet attribut, au moins une instance de l'attribut `organizationalUnitName` doit être présente et doit contenir l'identification de cette entité.

On distingue deux situations :

- entités disposant d'une immatriculation en France,
- entités n'étant pas immatriculées en France.

Situation	Règles
Entité immatriculée en France	La valeur de l'attribut `organizationalUnitName` doit être conforme à la norme ISO 6523. Elle est constituée de l'ICD (international code designator) et de l'identification de l'organisme séparés par un caractère espace, comme illustré ci-dessous. `[ICD][caractère_espace][identifiant_organisme]` Pour un organisme immatriculé en France, l'ICD est `0002` et l'identifiant de l'organisme est le numéro de SIREN / SIRET, sans aucun espace. Exemple : `0002 732829320`
Entité n'étant pas immatriculée en France	La valeur de la première instance de l'attribut `organizationalUnitName` doit, dans la mesure du possible, être constituée, conformément à la norme ISO 6523, de l'ICD et de l'identification de l'organisme séparés par un caractère espace, comme illustré ci-dessous. `[ICD][caractère_espace][identifiant_organisme]` Option 1 : Si l'entité dispose d'un numéro d'identification dans l'un des schémas d'identification pour lequel un ICD est défini, la norme ISO 6523 doit être reprise. Option 2 : S'il n'existe pas d'ICD pour l'entité, la valeur de l'attribut `organizationalUnitName` est libre mais ne doit pas commencer par 4 chiffres. L'option 1 doit être privilégiée. L'option 2 est à utiliser uniquement s'il n'existe pas d'ICD pour identifier l'entité.

Note : Dans le cas où l'AC dépend de plusieurs entités distinctes (ex : deux ministères), une seule de ces entités doit être renseignée dans les attributs `organizationalName` et `organizationalUnitName`.

*2.1.2.1.4. Pays de l'AC (attribut **`countryName`**)*

L'attribut `countryName` doit être présent et doit indiquer le pays de l'autorité compétente (tribunal de commerce, ministère, etc.) auprès de laquelle l'entité qui a émis le certificat d'AC est officiellement enregistrée. Le pays est représenté par le codet alpha-2 du pays dans l'ISO 3166-1. Le codet pour la France est « FR ».

2.1.2.2. Identification du porteur

La présente section concerne l'identification du porteur qui figure dans le champ `subject` des certificats de porteurs.

Le porteur d'un certificat électronique représente la personne qui détient le certificat.

2.1.2.2.1. Protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

2.1.2.2.2. Attributs

Le tableau ci-dessous présente les attributs qui peuvent être utilisés à maxima pour l'identification d'un porteur.

Agent administratif	Particulier
`givenName` (recommandé)	`givenName` (recommandé)
`surname` (recommandé)	`surname` (recommandé)
`commonName`	`commonName`
`organizationName`	`countryName`
`organizationalUnitName`[3]	
`countryName`	
`uID` (optionnel[4])	

L'utilisation d'attributs autres que ceux listés précédemment n'est pas recommandée.

Si l'adresse de messagerie électronique du porteur est renseignée dans le certificat, celle-ci doit l'être en utilisant de préférence dans le champ `rfc822Name` de l'extension `subjectAltName`. Il est alors encodé en `IA5String`. L'utilisation de l'attribut `emailAddress` dans le DN n'est pas recommandée.

Conformément au document [ETSI_CERT] et compte tenu des attributs utilisables pour identifier un porteur (cf. tableau précédent), l'unicité du DN du porteur doit être assurée en utilisant un sous-ensemble des attributs suivants :

- `countryName`,
- `commonName`,
- `surname` (si renseigné),
- `givenName` (si renseigné),
- `organizationName` (pour les agents administratifs uniquement), et
- `organizationalUnitName` (pour les agents administratifs uniquement).

Le contenu des attributs ci-dessus ainsi que l'encodage à utiliser (cf. [RFC_5280]) sont précisés dans le tableau suivant :

Attribut	Contenu	Encodage
`givenName`	Prénom(s) du porteur	`UTF8String`
`surname`	Nom de famille du porteur	`UTF8String`

[3] organizationnalUnitName peut être multi-valué dans le DN

[4] L'uid ne peut être utilisé pour assurer l'unicité du DN

Attribut	Contenu	Encodage
commonName	Dépend de l'option choisie par l'AC (cf. section 2.1.2.2.3)	UTF8String
organizationName	Nom de l'organisation à laquelle est rattaché le porteur	UTF8String
organizationalUnitName	Identification de l'organisation à laquelle est rattaché le porteur	UTF8String
countryName	Pays de l'AC délivrant le certificat	PrintableString
uID	Identifiant du porteur	PrintableString

*2.1.2.2.3. État civil du porteur (attributs **givenName, surname et commonName**)*

On distingue deux types de certificats pour les porteurs :

- certificat pour lequel l'identité du porteur est définie par son état civil (l'identité du porteur ne contient pas de pseudonyme) ;
- certificat dit « certificat pseudonyme » pour lequel l'identité du porteur est définie par un pseudonyme.

Les certificats de cette dernière catégorie ne sont pas éligibles au référencement.

L'état civil du porteur est renseigné de la manière suivante :

- cas 1 : utilisation des attributs `givenName` et `surname`, éventuellement complétés de l'attribut `commonName` pour distinguer les cas d'homonymie au sein du domaine de l'AC ;
- cas 2 : utilisation de l'attribut `commonName`.

Le chapitre VII.2.2 de l'annexe [RGS_A_14] du RGS précise les règles de construction des attributs `givenName`, `surname` et `commonName` dans les deux cas ci-dessus.

Le nom de famille ainsi que les prénoms indiqués dans le certificat doivent être ceux indiqués dans la pièce d'identité du porteur présenté lors de l'enregistrement. Conformément à l'annexe [RGS_A_14], il n'y a pas d'obligation à renseigner tous les prénoms de l'individu. Seul le premier est obligatoire.

L'utilisation du cas 1 est recommandée.

*2.1.2.2.4. Nom de l'entité à laquelle est rattaché le porteur (attributs **organizationName** et **organizationalUnitName**)*

Les attributs `organizationName` et `organizationalUnitName` sont renseignés uniquement lorsque le porteur du certificat est un agent d'une autorité administrative. Ils ne s'appliquent pas aux certificats de particuliers. Les règles à suivre sont alors les suivantes :

- L'attribut `organizationName` doit contenir un nom significatif de l'entité de laquelle dépend le porteur tel qu'enregistré auprès des autorités compétentes (cf. [ETSI_CERT]). Ce nom doit être cohérent avec le nom officiel de l'entité. Il est recommandé de renseigner dans cet attribut le nom officiel complet de l'entité.
- En complément de cet attribut, une instance de l'attribut `organizationalUnitName` doit être présente et doit contenir l'identification de cette entité. Les mêmes règles que celles exposées au chapitre « 2.1.2.1.3 Nom et identification de l'entité responsable de l'AC (attributs `organizationName` et `organizationalUnitName`) » s'appliquent ici.

Note : Dans le cas où l'agent d'une autorité administrative dépend de plusieurs entités distinctes (ex : deux ministères), les attributs `organizationalName` et `organizationalUnitName` sont complétés avec les éléments de l'autorité administrative fournissant les certificats.

*2.1.2.2.5. Pays (attribut **countryName**)*

L'attribut `countryName` est obligatoire pour tout certificat de porteur. Il est représenté par le codet alpha-2 du pays dans l'ISO 3166-1. Il indique le pays de l'autorité compétente auprès de laquelle l'entité qui a émis le certificat de porteur est officiellement enregistrée (tribunal de commerce, ministère, etc.). Le codet pour la France est « FR ».

*2.1.2.2.6. Identifiant (attribut **uID**)*

Lorsque l'on souhaite que l'identifiant d'un agent de l'administration apparaisse dans un certificat porteur, il est recommandé de renseigner cet identifiant dans l'attribut optionnel `uID`.

2.1.3. Langue de la politique de certification

La politique de certification doit être disponible a minima en français.

De plus, dans le cas de familles de certificats éligibles à figurer dans la trust-service status list (TSL), les règles spécifiques à celle-ci s'appliquent également : disponibilité de la politique de certification en anglais ainsi que dans la langue du pays où est située l'AC.

En cas de litige, la version française de la politique de certification est celle qui fera foi.

2.1.4. Certificats de test

Les certificats d'AC ou de porteurs utilisés à des fins de test doivent répondre aux mêmes exigences que celles définies pour les certificats de production. De plus, ils doivent être identifiables comme certificats de test. Pour cela les règles suivantes s'appliquent :

- Le nom d'une AC de test (renseigné dans l'attribut `commonName` des champs `issuer` et, pour les certificats d'AC, dans le champ `subject`) doit être préfixé par « TEST ».
- Dans le cas où une AC de production souhaite émettre des certificats de test de porteur, , l'attribut `commonName` du DN d'un porteur (champ `issuer`) doit également être préfixé par « TEST ».

Le choix du délimiteur séparant « TEST » du reste du texte renseigné dans l'attribut `commonName` est l'espace.

2.2. Produits de sécurité

Les dispositifs d'authentification et de signature délivrés aux agents de l'administration et aux particuliers doivent être conformes aux spécifications **[IAS_ECC]** et versions suivantes.

3. Tests techniques

3.1. Offres de certificats électroniques

3.1.1. Référentiel de test

Les tests suivants doivent être exécutés avec succès pour vérifier l'interopérabilité des offres de certificats électroniques avec les services électroniques de l'État :

- Vérification de la conformité des profils des objets.
- Vérification des règles du présent cahier des charges qui ne sont pas testées par les deux outils ci-dessus.

3.1.2. Fourniture des objets de test

Le prestataire de service de confiance s'engage à fournir gratuitement en vue du référencement des certificats et LCR de test.

3.2. Produits de sécurité

3.2.1. Référentiel de test

Le référentiel de test des dispositifs d'authentification et de signature délivrés aux agents de l'administration et aux particuliers repose sur un schéma à 3 volets défini par l'ANTS :

- Interopérabilité : attestation de conformité à la norme [IAS_ECC],
- Durabilité : attestation du maintien des fonctionnalités électriques et physiques dans le temps, selon les contraintes liées à l'utilisation du produit définis par l'ANTS,
- Sécurité : attestation de qualification RGS au niveau requis par le présent cahier des charges.

3.2.2. Fourniture des produits de test

L'éditeur de produits de sécurité s'engage à fournir gratuitement en vue du référencement des produits de test.