PRODUITS/SERVICES

Guide de bonnes pratiques d'utilisation des listes de révocation des certificats

Avril 2014

À destination des éditeurs de logiciels

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Je suis éditeur de logiciel dans la sphère Santé…

… et mon produit doit interagir avec les produits de certification délivrés par l'ASIP Santé

RAPPELS CONCERNANT LES PRODUITS DE CERTIFICATION

➔ Usage des certificats électroniques

L'utilisation de certificats électroniques pour l'authentification ou la signature nécessite de vérifier que :

- le certificat provient d'une autorité de certification de confiance, c'est-à-dire que le certificat a été signé par une autorité de certification (autorité finale) dépendant directement de l'autorité de confiance (autorité racine) ;
  Ces autorités de certification doivent, au préalable, être insérées dans le coffre-fort de l'application – l'introduction doit être faite après vérification de leur authenticité (intégrité et origine) ;
- l'utilisation du certificat est bien conforme aux usages de clé autorisés précisés dans les extensions keyUsage et extendedKeyUsage ;
- le certificat est encore valide c'est-à-dire que la date de validité n'est pas dépassée et qu'il n'a pas fait l'objet d'une révocation (par exemple pour perte ou suspicion de compromission)*.

  **NB : Cette vérification s'applique également au certificat de l'autorité de certification finale ayant été utilisé pour signer le certificat utilisateur.*

Les premières vérifications se basent uniquement sur le certificat utilisé. En revanche, la vérification de la validité nécessite de faire référence à une liste à jour des certificats révoqués (CRL).
À cet effet, un Prestataire de Service de Certification Electronique (PSCE) peut mettre ces informations à disposition des utilisateurs soit par des listes de révocation des certificats (CRL), soit par l'intermédiaire d'un service OCSP qui indique pour un certificat s'il est révoqué ou non.

**NB : Un service OCSP (Online Certificate Status Protocol) sera mis en œuvre pour la future IGC-Santé.*

➔ Listes de révocation des certificats (CRLs)*

En tant que PSCE, l'ASIP Santé a choisi de mettre à disposition des utilisateurs des certificats produits (certificats inclus dans les cartes CPS et certificats serveurs) des CRLs pour l'ensemble des autorités de certification (AC) qu'elle met en œuvre (CRLs émises par les autorités racines pour la révocation des certificats des autorités finales, CRLs émises par les autorités intermédiaires – soit les classes 0 à 6 – pour la révocation des certificats utilisateurs).

**NB : On présente ici les principes de liste de révocation des certificats, indépendamment des moyens techniques pour les maintenir à jour (CRL complète systématique, ou CRL et delta-CRL) .*

Les CRLs sont mises à disposition des utilisateurs sur deux types de point de publication pour répondre aux différents besoins des utilisateurs : elles sont ainsi disponibles via un service Web (HTTP) et via un service LDAP.
Les CRLs sont publiées chaque jour[1] et ont une durée de vie de quelques jours.

1. En prenant une marge d'une heure pour tenir compte d'un éventuel retard technique de publication, 7h du matin peut être considérée comme l'heure de début de mise à disposition des nouvelles CRLs quotidiennes. A partir de ce moment, les CRLs peuvent être obtenues en configurant un retrait aléatoire sur plusieurs heures afin d'éviter la génération de pics de charge.

BONNES PRATIQUES D'UTILISATION DES CRLs CPS

Les bonnes pratiques de récupération des CRLs reposent sur les grands principes suivants d'utilisation conformes à l'état de l'art :

- **limitation du téléchargement** aux CRLs correspondant aux certificats susceptibles d'être acceptés par l'application ;
- **fréquence** de téléchargement des CRLs **en rapport avec la fréquence de publication** de celles-ci (c'est-à-dire une fois par jour pour des CRLs publiées quotidiennement) ;
- **variabilité des horaires de téléchargement** des CRLs lorsque celui-ci est automatisé (notamment pour que toutes les instances d'un même produit installé chez différents clients ne téléchargent pas les CRLs en même temps : prévoir par exemple un étalement de téléchargement « aléatoire » sur plusieurs heures) ;
- **limitation des durées de connexion** au temps nécessaire au téléchargement des CRLs (pas de maintien de session après un (ou une tentative de) téléchargement).

Ces bonnes pratiques sont détaillées ci-après.

Cas particulier des infrastructures hébergées constituées de multiples équipements et des points de concentration (exemple : proxy internet pour de nombreux postes, …) :
Pour ce type de configuration où de nombreux équipements sollicitent le téléchargement des mêmes CRLs via un même point d'accès Internet, il est recommandé de mettre en œuvre un mécanisme de cache, adapté à la fréquence de publication, afin de limiter les multiples requêtes identiques en provenance d'une même infrastructure.

Synthèse des bonnes pratiques de récupération des listes de révocation :
- se limiter au téléchargement des CRLs correspondant aux AC des certificats que l'on est susceptible d'accepter ;
- tenir compte de la fréquence de publication de l'IGC ;
- rendre aléatoire l'heure de téléchargement des CRLs ;
- mettre fin à la connexion dès que le téléchargement des CRLs est effectué.

MÉTHODE DE GESTION PRECONISEE POUR LE CHARGEMENT DES CRLs DE L'IGC-CPS

Le standard de référence décrivant le format des CRLs est le RFC 5280. Toutefois, la fréquence de publication est laissée libre à chaque IGC. Toute CRL contient obligatoirement la date/heure de la publication de la CRL suivante (extension nextUpdate) permettant ainsi à un vérificateur de récupérer la nouvelle CRL avant l'expiration de la CRL en cours.

L'IGC-CPS publie chaque jour une nouvelle CRL pour chaque autorité racine ainsi que pour chaque autorité intermédiaire. La durée de validité de chaque CRL de l'IGC-CPS est au minimum de 4 jours ouvrés[2].
Les CRLs sont numérotées chronologiquement pour chaque autorité (extension CRLNumber).

2. Les durées de validités exactes pour chaque classe sont rappelées en annexe.

Malgré cette durée de validité des CRLs de l'IGC-CPS, il est fortement recommandé de charger les mises à jour quotidiennement, et non juste avant l'expiration des CRLs en exploitation parce que :

- au-delà de 24 h le système travaille avec une CRL « non à jour » qui ne contient donc pas les certificats révoqués depuis la précédente publication (risque d'acceptation à tort de certificats révoqués !) ;
- il y a toujours un risque qu'il y ait un problème de chargement et que la CRL locale expire.
  Il appartient au responsable de traitement de définir, en fonction de son analyse de risques, le comportement de son service en cas d'expiration des listes de révocation locales.

Afin de traiter les CRLs de l'IGC-CPS avec les meilleures garanties (CRLs aussi « fraîches » que possible), il est fortement conseillé de respecter les règles énoncées ci-dessous.

➔ Règles de gestion des CRLs de l'IGC-CPS

1. Lors de chaque chargement des CRLs de l'IGC-CPS, les date/heure d'expiration (extension nextUpdate) de chaque CRL sont mémorisées.
   Attention : les CRLs des différentes autorités ne sont pas toutes publiées à la même heure.
2. Un chargement quotidien est mis en place pour chaque CRL en exploitation.
   Les CRLs pour une autorité donnée sont publiées tous les jours approximativement à la même heure – entre 6 h 00 et ou 7 h 00 du matin. Le chargement peut donc commencer à partir de 7 h 00. La première requête doit être planifiée aléatoirement sur plusieurs heures après 7 h 00 (algorithme intégré dans le logiciel par son éditeur devant garantir qu'il y a une répartition de charge chez ses clients).
3. S'il se produit un problème lors du chargement *(problème technique ou chargement de la même CRL)* :
   a. faire 2 ou 3 autres tentatives espacées chacune d'une demi heure,
   b. si le problème persiste, relancer le chargement toutes les 2 heures (avec plusieurs tentatives si besoin),
   c. si le problème persiste toujours, en fonction du risque évalué par le promoteur, le SI doit générer une alarme pour l'opérateur de l'exploitant (dans tous les cas bien avant l'expiration de la CRL).
4. Ce dernier doit analyser la source : problème interne, connexion Internet ou autre.
5. En cas de doute contacter la hot-line de l'ASIP Santé au N° Indigo 0 825 85 2000[3].

➔ Les delta-CRLs de l'IGC-CPS

Les CRLs peuvent devenir volumineuses et être difficiles à exploiter (ralentissement du chargement et du traitement) par les logiciels installés.
Pour éviter aux professionnels de santé de charger quotidiennement les CRLs complètes, l'IGC CPS publie simultanément avec chaque CRL une delta-CRL contenant uniquement les certificats révoqués depuis la publication précédente. De même, pour éviter de devoir recharger les CRLs complètes si le téléchargement d'une delta-CRL n'a pas fonctionné, l'IGC-CPS publie un nombre de delta-CRL correspondant aux publications des derniers 7 jours[4].
Chaque CRL contient un numéro séquentiel croissant (extension CRLNumber) permettant de suivre la séquence chronologique (attention : la numérotation des CRL des différentes autorités de certification est indépendante). Les delta-CRLs suivent la même numérotation que les CRLs et elles contiennent en plus le numéro de séquence de la CRL de référence (extension baseCRL-Number : numéro de la CRL de la publication précédente).
Les delta-CRL ne sont disponibles que via le protocole LDAP.

3. 0,15 € TTC/min
4. Attention, ce nombre peux être variable de 0 à maximum 25.

➔ Règles de gestion des delta-CRLs de l'IGC-CPS

Les règles ci-dessous sont données pour la gestion des delta-CRLs d'une seule autorité de certification, il faut les appliquer indépendamment pour chaque autorité.

1. Pour démarrer, charger une CRL complète pour disposer d'une CRL locale initiale pour l'autorité donnée.
2. Quotidiennement, charger les delta-CRLs de l'autorité et effectuer le traitement suivant :
   - classement chronologique des delta-CRL sur la base de leur numéro séquentiel (en éliminant d'éventuels doublons),
   - vérification si la numérotation des delta-CRL suit bien la CRL locale (en éliminant les delta-CRL avec des numéros antérieurs ou égaux à la CRL locale),
   - vérification qu'il n'y ait pas de trous de séquence (numéros manquants) entre le numéro de la CRL locale et la delta-CRL la plus récente,
   - vérification que la delta-CRL la plus récente est valide (l'extension nextUpdate doit être supérieur à la date/heure du traitement),
   - si toutes les vérifications s'avèrent correctes : mise à jour de la CRL locale
     (soit en stockant les delta-CRLs avec la CRL locale de départ,
     soit en consolidant tous les contenus des (delta-)CRLs dans un seul fichier).
3. S'il se produit un problème lors du traitement, par exemple, impossibilité de reconstruire la chaîne des delta-CRL :
   - la mise à jour de la CRL locale n'a pas été effectuée depuis trop longtemps,
   - trou(s) de séquence dans la chaîne des delta-CRL,
   - pas de delta-CRL disponible avec une date/heure supérieure[5].

   il faudra supprimer la CRL locale et recommencer le processus au point 1.

Remarque : Pour éviter une augmentation sans fin, une CRL donnée ne contient que les certificats révoqués qui auraient été valides à la date de sa publication. Lorsqu'on gère uniquement des delta-CRL, la CRL locale n'est pas purgée des certificats révoqués qui ne sont plus dans leur période de validité. Pour cette raison, il est conseillé de supprimer la CRL locale au moins une fois tous les 3 mois et de recommencer le processus au point 1.

POUR ALLER PLUS LOIN

Espace CPS du site esante.gouv.fr : *esante.gouv.fr/services/espace-cps*
Espace intégrateurs : *http://integrateurs-cps.asipsante.fr/*

Points de distribution des CRLs / delta-CRLs de l'IGC-CPS2ter

Les certificats émis par l'IGC-CPS2ter (certificats d'autorités intermédiaires et certificats utilisateurs embarqués dans des cartes CPx) contiennent les points de distribution des CRLs et des delta-CRLs dans les extensions adéquates (crlDistributionPoint et freshestCRL).
Les points de distribution sont listés ci-dessous pour information :

IGC-CPS2ter - Classes 0 à 3 - CRLs accessibles en HTTP	
Racine : **Classe 0 :**	*http://annuaire.gip-cps.fr/crl/GIP-CPS ANONYME.crl* *http://annuaire.gip-cps.fr/crl/GIP-CPS CLASSE-0.crl*
Racine : **Classe 1 :**	*http://annuaire.gip-cps.fr/crl/GIP-CPS PROFESSIONNEL.crl* *http://annuaire.gip-cps.fr/crl/GIP-CPS CLASSE-1.crl*
Racine : **Classes 2 et 3 :**	*http://annuaire.gip-cps.fr/crl/GIP-CPS STRUCTURE.crl* *http://annuaire.gip-cps.fr/crl/GIP-CPS CLASSE-2.crl* *http://annuaire.gip-cps.fr/crl/GIP-CPS CLASSE-3.crl*

Note : Il n'y a pas de publication de delta-CRLs en HTTP

5. L'IGC-CPS peut, pour des raisons techniques ou pour forcer toutes les applications à se resynchroniser sur une CRL donnée, supprimer les delta-CRL dans l'annuaire et commencer la publication des delta-CRL à zéro.

IGC-CPS2ter – Classes 0 à 3 – CRLs accessibles en LDAP	
Racine : **Classe 0 :**	*ldap://annuaire.gip-cps.fr/ou=gip-cps anonyme,o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/cn=gip-cps classe-0,ou=gip-cps professionnel,o=gip-cps,c=fr?certificaterevocationlist;binary*
Racine : **Classe 1 :**	*ldap://annuaire.gip-cps.fr/ou=gip-cps professionnel,o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,ou=gip-cps professionnel,o=gip-cps,c=fr?certificaterevocationlist;binary*
Racine : **Classes 2 et 3 :**	*ldap://annuaire.gip-cps.fr/ou=gip-cps structure,o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/cn=gip-cps classe-2,ou=gip-cps professionnel,o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/cn=gip-cps classe-3,ou=gip-cps professionnel,o=gip-cps,c=fr?certificaterevocationlist;binary*
Racine : **Classes 4 à 6 :**	*ldap://annuaire.gip-cps.fr/o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/ou=ac-classe-4,o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/ou=ac-classe-5,o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/ou=ac-classe-6,o=gip-cps,c=fr?certificaterevocationlist;binary*

IGC-CPS2ter – Classes 0 à 3 – delta-CRLs accessibles en LDAP	
Racine : **Classe 0 :**	*ldap://annuaire.gip-cps.fr/ou=gip-cps anonyme,o=gip-cps,c=fr?deltarevocationlist;binary* *ldap://annuaire.gip-cps.fr/cn=gip-cps classe-0,ou=gip-cps professionnel,o=gip-cps,c=fr?deltarevocationlist;binary*
Racine : **Classe 1 :**	*ldap://annuaire.gip-cps.fr/ou=gip-cps professionnel,o=gip-cps,c=fr?deltarevocationlist;binary* *ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,ou=gip-cps professionnel,o=gip-cps,c=fr?deltarevocationlist;binary*
Racine : **Classes 2 et 3 :**	*ldap://annuaire.gip-cps.fr/ou=gip-cps structure,o=gip-cps,c=fr?deltarevocationlist;binary* *ldap://annuaire.gip-cps.fr/cn=gip-cps classe-2,ou=gip-cps professionnel,o=gip-cps,c=fr?deltarevocationlist;binary* *ldap://annuaire.gip-cps.fr/cn=gip-cps classe-3,ou=gip-cps professionnel,o=gip-cps,c=fr?deltarevocationlist;binary*

Note : Les CRL des autorités racine étant vides, il est inutile d'exploiter les delta-CRLs correspondantes.

Points de distribution des CRLs / delta-CRLs de l'IGC-CPS2bis

Les certificats émis par l'IGC CPS2bis (certificats d'autorités intermédiaires et certificats utilisateurs logiciels) ne contiennent pas de points de distribution.
Les points de distribution sont listés ci-dessous :

IGC-CPS2bis – Classes 4 à 6 – CRLs accessibles en HTTP	
Racine : **Classes 4 à 6 :**	*http://annuaire.gip-cps.fr/crl/GIP-CPS.crl* *http://annuaire.gip-cps.fr/crl/AC-CLASSE-4.crl* *http://annuaire.gip-cps.fr/crl/AC-CLASSE-5.crl* *http://annuaire.gip-cps.fr/crl/AC-CLASSE-6.crl*

Note : Il n'y a pas de publication de delta-CRLs en HTTP

IGC-CPS2bis – Classes 4 à 6 – CRLs accessibles en LDAP	
Racine : **Classes 4 à 6 :**	*ldap://annuaire.gip-cps.fr/o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/ou=ac-classe-4,o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/ou=ac-classe-5,o=gip-cps,c=fr?certificaterevocationlist;binary* *ldap://annuaire.gip-cps.fr/ou=ac-classe-6,o=gip-cps,c=fr?certificaterevocationlist;binary*

IGC-CPS2bis – Classes 4 à 6 – delta-CRLs accessibles en LDAP	
Racine : **Classes 4 à 6 :**	*ldap://annuaire.gip-cps.fr/o=gip-cps,c=fr?deltarevocationlist;binary* *ldap://annuaire.gip-cps.fr/ou=ac-classe-4,o=gip-cps,c=fr?deltarevocationlist;binary* *ldap://annuaire.gip-cps.fr/ou=ac-classe-5,o=gip-cps,c=fr?deltarevocationlist;binary* *ldap://annuaire.gip-cps.fr/ou=ac-classe-6,o=gip-cps,c=fr?deltarevocationlist;binary*

Note : Les CRL des autorités racine étant vides, il est préférable de ne pas utiliser les delta-CRLs correspondantes.

Durées de validité des CRLs / delta-CRLs des IGC-CPS

Les CRLs sont générées quotidiennement. Les delta-CRLs sont générées simultanément et ont la même durée de vie que leurs CRLs correspondantes.

IGC-CPS2ter	
CRL émise par les Autorités Racine : **CRL émise par les Autorités Intermédiaires (Classes 0 à 3) :**	*4 jours ouvrés (entre 4 et 6 jours calendaires)* *4 jours ouvrés (entre 4 et 6 jours calendaires)*

IGC-CPS2bis	
CRL émise par les Autorités Racine : **CRL émise par les Autorités Intermédiaires (Classes 4 à 6) :**	*4 jours ouvrés (entre 4 et 6 jours calendaires)* *7 jours calendaires*

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

Pour accéder directement à l'espace CPS :
esante.gouv.fr/services/espace-cps

Pour en savoir plus
CPS Info Service :
24h/24 - 7j/7

N° Indigo 0 825 85 2000
0,15 € TTC / MN

esante.gouv.fr

asipsanté
Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

PRODUITS/SERVICES / Guide de bonnes pratiques d'utilisation des listes de révocation des certificats – Avril 2014