Contribution à la validation des signatures électroniques dans le temps

Nathanaël Cottin [†] et Maxime Wack [‡] et Abdelaziz Sehili [§]

MSG-Software – Laboratoire SeT
Université de Technologie de Belfort-Montbéliard
90010 Belfort, France

Les infrastructures à clé publique supportant la signature électronique proposent des services de gestion des certificats associés aux signataires. L'octroi du label "environnement sécurisé de signature" fait non seulement appel au système physique de stockage des informations de signature (clés, certificats) mais également aux applications faisant usage de ces informations ainsi qu'aux éventuelles connexions avec l'extérieur (LAN, WAN, Internet). Les applicatifs proposés aux clients doivent utiliser correctement les services de ces infrastructures afin d'authentifier et valider ces signatures. Nous nous intéressons à l'étude des principaux moyens de validation automatique des signatures électroniques et particulièrement la liste de révocation, le protocole OCSP, la signature à long terme ETSI et la notarisation électronique via le certificat de validité.

Mots clés: signature électronique, ICP, validation, long terme

1 Introduction

La signature électronique (SE) devient incontournable. Un nombre croissant de pays se dotent de lois en la matière [1] qui confèrent un appui et une reconnaissance juridiques des signatures électroniques qualifiée et avancée [2]. La législation française, par exemple, définit l'écrit électronique comme admissible au même titre que son homologue sur support papier "sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité" ([3], art. 1316-1). *In extenso*, la SE doit fournir les éléments permettant non seulement de s'assurer de l'identité du signataire mais également d'attribuer une validité à sa signature *a posteriori*.

Nous présentons une étude critique des procédés techniques courants de validation automatique des SEs. Nous déterminons ainsi leur aptitude à valider les SEs en fonction de la durée possible de demande de validation. Cette durée s'apparente à la durée légale de conservation des actes juridiques mais s'applique à tout type de contenu susceptible d'être porté comme preuve et validé par une tierce partie plusieurs jours, mois ou années après sa création. Pour ce faire, notre étude repose sur les standards actuels tels que les Infrastructures à Clé Publique (ICP – PKI), les listes de certificats révoqués (LCRs – CRLs) [4] et le protocole de validation en ligne OCSP [5]. Nous nous appuyons également sur la signature à long terme de l'ETSI (ES-X) [6] [7] ainsi que sur le certificat de validité (CDV) [8], alternative à la validation automatique des SEs à long terme ne reposant pas sur les méthodes traditionnelles telles que les LCRs et OCSP.

Le premier chapitre définit les notions de validité à court, moyen et long terme des SEs. Les second et troisième chapitres rappellent les éléments fondateurs de notre étude, à savoir les LCRs et le protocole OCSP. Les points forts et faiblesses de ces deux éléments de validation permettent d'appréhender dans le chapitre suivant les difficultés posées par la validation à long terme des SEs. Pour cela, nous nous appuyons sur la confrontation de deux approches techniques : la signature à long terme ETSI et le CDV. La conclusion générale permet enfin d'envisager une solution technico-juridique viable quant à l'authentification à long terme des contenus comportant une ou plusieurs SEs.

[†] nathanael.cottin@msg-software.com – http://www.ncottin.net
[‡] maxime.wack@utbm.fr
[§] abdelaziz.sehili@utbm.fr

2 La validité d'une signature électronique

Une SE est un ensemble d'informations cryptographiques associées à un contenu. La combinaison du contenu et des informations de la SE permettent de garantir [9] :

- *L'authenticité du contenu* : la SE est propre à un contenu donné, sous réserve de résitance forte aux collisions de l'algorithme d'empreinte employé lors de la génération de la SE.
- *L'identification du signataire* par le biais du certificat numérique joint à la signature.
- *La non-répudiation* : le signataire ne peut nier avoir signé le contenu présenté au vérificateur. La notion de *non-répudiabilité* fait intervenir la notion de politiques de signature et de validation ([7], par. 4.2) permettant au vérificateur d'accepter ou rejeter toute contestation émanant du signataire.

Une SE peut cependant être composée d'éléments différents selon qu'elle répond à un besoin de contrôle immédiat ou temporellement éloigné de l'instant de sa création en fonction de la nature du contenu signé.

En effet, les besoins techniques d'authenticité et de validation d'un paiement électronique, d'un contrat ou d'un acte de naissance ne peuvent être semblables. Si un paiement électronique ne demande qu'une validation immédiate, il n'en est de même d'un contrat valable plusieurs années et d'un acte de naissance devant fournir un moyen de preuve d'authenticité *ad vitam aeternam.*

Nous nous appuyons sur les définitions de "proche terme" et "long terme" de [10] pour distinguer trois différentes durées de validité pour une SE : les validités à court terme, moyen terme et long terme. Ces durées varient selon la période de réactualisation des LCRs et de la durée de validité des certificats impliqués.

2.1 Validité à court terme

La validité à court terme d'une signature répond principalement au cas où celle-ci doit être contrôlée quelques secondes, quelques minutes, voire quelques heures suivant l'instant de sa création. Ce laps de temps est inférieur à la période de validité de la LCR qui lui est associée et suppose que le certificat du signataire n'est pas en fin de vie. Ce cas de figure se retrouve en particulier lors d'échanges authentifiés au cours de transactions informatiques telles que les téléservices.

Cette signature "à validation unique" n'étant validée qu'une seule fois par le destinataire de la transactin signée avant rejet ou acceptation, la signature peut se contenter de n'offrir que des moyens basiques de validation et peut reposer sur des certificats éphémères.

2.2 Validité à moyen terme

Le moyen terme désigne une période de plusieurs jours, voire plusieurs mois. La SE est destinée à être validée dans un délai tel que l'évolution technologique ne remet pas en cause son authenticité tout en garantissant qu'au moins une LCR a été émise depuis son instant de création. La signature est systématiquement invalide au-delà de la période de validité du certificat du signataire.

La signature peut être contrôlée plusieurs fois par des entités différentes. Chaque contrôle de validité doit fournir un résultat similaire émanant d'une tierce partie neutre considérée comme étant de confiance (*tiers de confiance*) par le vérificateur.

2.3 Validité à long terme

L'évolution des moyens cryptographiques et de la puissance de calcul des processeurs résulte en la perte de la confiance attribuée aux SEs actuelles. Ce qui est techniquement viable aujourd'hui sera dépassé demain. Une signature valable à court ou moyen terme ne peut répondre aux exigeances techniques liées à cette évolution des technologies. C'est pourquoi la validité à long terme est un sujet préoccupant qui ne doit devenir un *facsimile* du "bug de l'an 2000".

Nous entendons par validité à long terme une période de plusieurs années ou dizaines d'années durant laquelle la SE doit pouvoir être validée sans toutefois perdre son caractère authentique tout en considérant la nécessaire expiration du certificat du signataire.

A l'identique de la validité à moyen terme, une signature valable à long terme peut être validée plus d'une fois. Cependant, des éléments supplémentaires doivent être ajoutés afin de prévenir la constitution de "vraies-fausses" signatures d'époque et d'attribuer une validité de la SE *a posteriori.*

2.4 Conclusion

Une SE étant supposée créée à un instant t_0 demeure valable à un instant $t > t_0$ fixé selon la valeur de la durée $\Delta = t - t_0$. Cette valeur détermine le type de validité requis en fonction de la durée de validité δ_{LCR} de la LCR associée et la période de validité δ_{cert} du certificat du signataire :

- Si $\Delta \in [0; \delta_{LCR}[$, alors la signature est destinée à être validée sur du court terme.
- Si $\Delta \in [\delta_{LCR}; n.\delta_{LCR}[$, la signature est valable sur du moyen terme, pour un nombre entier n de LCRs donné tel que $n \in N^*$ et $n.\delta_{LCR} \leq \delta_{cert}$.
- Si $\Delta \in [n.\delta_{LCR}; +\infty[$, la signature est définie et peut être validée sur du long terme, n correspondant à la valeur fixée précédemment.

3 Les listes de certificats révoqués

3.1 Présentation

Une LCR est un ensemble signé de certificats mis en opposition issus par une Autorité de Certification (AC) unique. Elle peut générée et publiée ([4], sec. 5) soit directement par l'AC (LCR directe) soit par le biais d'un autre organisme (LCR indirecte).

Les spécifications fournies par l'IETF (Internet Engineering Task Force) décrivent les éléments constitutifs des LCRs. En particulier, une LCR contient ([4], par. 5.1) :

- Une date d'émission permettant de classifier les différentes listes émises et vérifier leur actualité.
- Une date de prochaine mise à jour.
- La liste des numéros de série certificats révoqués (et en théorie non expirés à la date d'émission de la LCR).
- La date de révocation de chaque certificat mentionné.

L'authenticité de la LCR est garantie par la signature de l'autorité de l'ICP en charge de son émission. Ce peut être l'AC elle-même ou une autre autorité remplissant ce service.

3.2 Limites

Le principal attrait des LCRs provient de la facilité du contrôle de la non révocation d'un certificat sans pour autant requérir une connexion systématique à l'autorité émettrice. Cependant, les LCRs souffrent de quelques défauts qui en limitent les possibilités.

3.2.1 Délai de carence

L'ETSI fait état d'un délai de carence ("*cautionary period*") entre la demande de révocation et sa publication. En effet, le service de révocation n'est pas tenu de tenir à jour la LCR en temps réel. Ce délai, au plus égal à l'intervalle entre deux mises à jour de la LCR correspondante, doit être précisé dans la politique de certification (PC) de l'AC ou de son autorité déléguée. L'objectif est de minimiser ce délai. Un compromis doit être trouvé en fonction du ratio de révocation des certificats, du taux d'émission des mises à jour et du coût induit par la création et la signature de la LCR. Le protocole de validation en ligne OCSP permet de réduire le délai de carence car il permet de consulter en direct le statut d'un certificat (actif, suspendu, révoqué). L'utilisation de delta-LCRs est également possible. En effet, contrairement à une LCR qui liste

3.2.2 Statut incomplet des certificats

Les LCRs contiennent uniquement les certificats révoqués. Ainsi le statut courant d'un certificat, parmi ceux décrits par la figure 1 tel qu'une suspension temporaire, n'y figure pas. Pourtant, un certificat suspendu ne peut être utilisé avant sa réactualisation. L'ETSI fait également état du statut de suspension dans les LCRs ([7], par. 5.4.2).

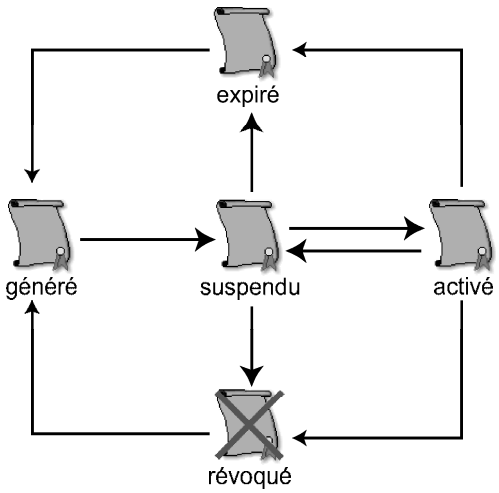

FIG. 1 – *Cycle de vie d'un certificat*

3.2.3 Téléchargement régulier

Le principal avantage d'une LCR est qu'elle permet de contrôler localement la validité d'un certificat présenté au vérificateur. Cependant, une mise à jour périodique est requise afin de disposer de la LCR la plus récente, en supposant que l'ensemble des certificats révoqués y soient mentionnés.

3.3 Conclusion

Les LCRs permettent de vérifier qu'un certificat n'est pas révoqué. Il serait également intéressant d'y ajouter les certificats suspendus. Dans ce cas, la validation de la signature fera état soit d'un rejet (lors d'un besoin immédiat de validation) ou de l'attente d'une prochaine LCR. La structure ASN.1 [11] interne de la LCR ([4], par. 5.1) doit être modifiée en conséquence :

```
TBSCertList ::= SEQUENCE {
  version                   Version OPTIONAL,
  -- if present, MUST be v2
  signature                 AlgorithmIdentifier,
  issuer                    Name,
  thisUpdate                Time,
  nextUpdate                Time OPTIONAL,
  revokedCertificates   [0] SEQUENCE OF rosCertificate OPTIONAL,
  suspendedCertificates [1] SEQUENCE OF rosCertificate OPTIONAL,
  crlExtensions         [2] EXPLICIT Extensions        OPTIONAL
  -- if present, MUST be v2
}

rosCertificate ::= SEQUENCE {
-- revoked of suspended certificate
  userCertificate    CertificateSerialNumber,
  rosDate            Time,
  crlEntryExtensions Extensions OPTIONAL
  -- if present, MUST be v2
}
```

Les LCRs sont un moyen sûr et efficace de vérifier la révocation des certificats présentés au vérificateur quelques temps après l'instant de création de la signature contrôlée. Le nécessaire délai de mise à jour les

rend peu aptes à valider des signatures à court et moyen terme sans l'utilisation complémentaire de delta-LCRs [12]. Elles sont par contre recommandées -mais insuffisantes- pour valider les signatures à long terme. Le protocole OCSP apporte un complément efficace lorsqu'une validation à court terme est nécessaire.

4 Le protocole OCSP

4.1 Présentation

OCSP permet d'interroger un serveur connecté à Internet afin de lui demander en direct le statut d'un certificat contrôlé par le vérificateur d'une SE. Ce serveur doit être reconnu comme *tiers de confiance* par ce dernier afin de considérer la réponse comme fiable et opposable.

Le certificat contrôlé est fourni au serveur sous la forme d'un ensemble d'informations comprenant :

- L'empreinte numérique du nom distinctif (ND) de l'AC émettrice du certificat.
- L'empreinte numérique de sa clé de vérification (clé publique de l'AC).
- Le numéro de série du certificat demandé.

En retour, le serveur OCSP indique le statut de validité en cours du certificat demandé parmi "actif" (*good*) ou "révoqué" (*revoked*). Contrairement aux LCRs, cette valeur n'est donc plus uniquement négative.

Le principal apport d'OCSP est l'affranchissement de l'incertitude liée au délai de publication des LCRs, réduite au minimum (court terme). Ainsi, OCSP n'est pas un concurrent des LCRs mais plutôt un complément nécessaire lors de la validation à court terme des SEs.

4.2 Limites

Bien qu'OCSP soit un outil indispensable au même titre que les LCRs, certains défauts demeurent.

4.2.1 Connexion requise

Le vérificateur d'une SE doit disposer d'une connexion lui permettant d'interroger à distance le serveur OCSP dont dépend le certificat contrôlé afin de valider -partiellement- la SE qui lui est soumise. Si une telle connexion ne peut s'établir, l'emploi des LCRs est alors inévitable, bien que ces dernières n'apportent ni des informations à jour ni un statut complet faisant intervenir l'état de suspension.

4.2.2 Validité immédiate

La valeur de statut retournée indique l'état courant du certificat et non son état à une date donnée. Partant du prédicat qu'aucune date non certifiée n'est fiable, le vérificateur ne peut fournir cette date à moins que la SE n'inclue un horodatage.

4.2.3 Volatilité de la réponse

Une requête OCSP est une transaction. Elle est en ce sens volatile et ne demeure valable que sur le court terme. De fait, la signature du serveur OCSP ne peut répondre au besoin de validation à moyen et long terme.

4.3 Conclusion

Actuellement, le protocole fait état des statuts "actif", "révoqué" et "inconnu". La suspension est traitée comme un cas particulier de révocation ([5], par. 2.2). A l'ensemble de ces valeurs de statut possibles peuvent néanmoins être ajoutées les valeurs "suspendu" et "expiré" afin d'indiquer que le certificat n'est ni révoqué ni actif, conformément au cycle de vie du certificat (figure 1) :

```
CertStatus ::= CHOICE {
  good      [0] IMPLICIT NULL,
  revoked   [1] IMPLICIT RevokedInfo,
  unknown   [2] IMPLICIT UnknownInfo,
  suspended [3] IMPLICIT SuspendedInfo
  expired   [4] IMPLICIT NULL
```

```
}

SuspendedInfo ::= SEQUENCE {
  suspendedTime       GeneralizedTime,
  suspendedReason [0] EXPLICIT SuspendedReason OPTIONAL
}
```

La mention d'expiration est utile puisqu'elle permet de s'affranchir de l'horloge locale, si tant est que le serveur OCSP détienne une horloge comparable à un horodatage sécurisé [13].

OCSP est une alternative aux LCRs appréciable pour une validation à court terme des SEs. Il n'est cependant pas recommandé de l'utiliser tel quel sur du moyen ou long terme puisque la réponse fournie ne répond pas à une conservation à long terme et peut être sujette à controverse.

Nous proposons cependant une extension possible à OCSP en ajoutant à la requête la mention d'une date optionnelle :

```
Request ::= SEQUENCE {
  reqCert                    CertID,
  date                    [0] EXPLICIT GeneralizedTime OPTIONAL,
  singleRequestExtensions [1] EXPLICIT Extensions      OPTIONAL
}
```

Lorsque présente, le serveur OCSP doit répondre en indiquant la validité du certificat à cette date via l'extension "archive cutoff" ([5], par. 4.4.4).

Notes : Une notion d'intervalle de temps peut être envisagée selon la politique de validation souhaitée. La date mentionnée dans la requête peut également être intégrée dans les extensions afin d'éviter la modification de sa structure interne.

5 La validation à long terme des SEs

Nous avons établi les rôles complémentaires des LCRs et du protocole OCSP pour valider les SEs en fonction de leur durée de conservation. Il apparaît que la version actuelle d'OCSP offre une approche adéquate à la validation à court terme des SEs alors que les LCRs sont efficaces lorsqu'il s'agit de valider partiellement des SEs sur le moyen et le long terme.

5.1 Problématique

Les recherches actuelles en matière de SE sont beaucoup orientées vers l'attribution d'un statut définif à une signature, indépendant du temps alors que les éléments constitutifs des SEs ne peuvent être pérennes. Par exemple :

- Les certificats expirent ou sont révoqués (les certificats racines en particulier). Par conséquent les chemins de certification deviennent obsolètes et ne jouent plus leur rôle de transmission de la confiance.
- Les clés d'époque sont inefficaces face aux évolutions technologiques et peuvent être compromises sans difficulté particulière lorsque les moyens mis en œuvre permettent de forcer les clés dans un délai raisonnable.
- Les algorithmes d'empreinte utilisés lors de la génération des SEs et des valeurs d'horodatage sont affaiblis et n'offrent plus de résistance forte aux collisions. Les signatures peuvent ainsi être détournées du contenu originel au profit d'un faux.

Diverses solutions techniques existent pour répondre à certains des problèmes soulevés. Nous proposons d'étudier les systèmes ES-X et CDV, tous deux reposant sur les normes des ICPs et offrant deux solutions divergentes au problème de la validation à long terme des SEs.

5.2 La signature à long terme ETSI

L'ETSI définit la signature électronique comme "une donnée numérique permettant d'établir la preuve qu'un engagement a été contracté conformément à une politique de signature, à une date donnée, par un signataire identifié et agissant éventuellement sous une certaine fonction".

Cette définition fait intervenir les éléments imbriqués suivants [14], présentés dans la figure 2 :

- *ES* désigne une SE comportant une valeur de signature (également appelée "signature numérique"), une politique de signature ainsi que des attributs tels que la date locale de signature, l'identifiant du certificat du signataire, l'alogithme d'empreinte utilisé et le type du contenu signé.
- *ES-T* est une extension de la SE basique à laquelle est ajouté un horodatage. Cet horodatage permet non seulement d'attribuer une date justifiant l'existence de la SE mais également d'étendre la validité de la SE sur le moyen terme. La validité de la SE est conservée jusqu'à expiration du certificat de l'horodatage.
- *ES-C* est une SE comportant l'ensemble des informations nécessaires à sa validation locale, telles que les LCRs associées. ES-C est cependant toujours soumise à l'évolution des technologies et la possibilité de créer dans le futur des "vraies-fausses" signatures d'aujourd'hui.
- *ES-X* apporte la réponse au problème posé par ES-C. Un second horodatage est apposé afin de sceller l'ensemble des informations que comporte ES-C. Cet horodatage doit être réactualisé avant que le certificat qu'il renferme n'expire ou que la technologie puisse le désavouer.

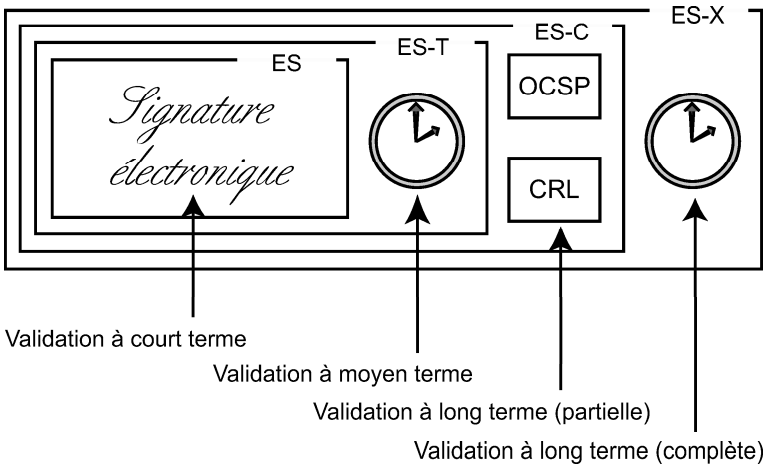

FIG. 2 – *Signature ETSI valable à long terme*

5.3 Le certificat de validité

Les approches traditionnelles de validation des SEs à long terme par des notaires électroniques [16] font appel à des services en lignes chargés de donner le statut de validité du certificat du signataire à partir de la SE qui leur est présentée.

Cependant, une connexion aux notaires impliqués est requise à chaque validation afin de confirmer les différents statuts de validitié des certificats. Un contenu multi-signé [18], c'est à dire comportant plus d'une signature, demande ainsi au mieux une unique connexion (tel est le cas présenté par [15] puis [16]) et au pire autant de connexions que de signatures avant d'être en mesure de statuer sur la validité générale du contenu signé [17].

A contrario le certificat de validité (CDV) est une pièce justificative jointe à la signature et présentée au vérificateur (figure 3). Le CDV renseigne sur le statut de validité du certificat du signataire. Il est authentifié soit par un notaire électronique soit par un service de l'ICP implémentant un service de validation de signature (SVS) [19].

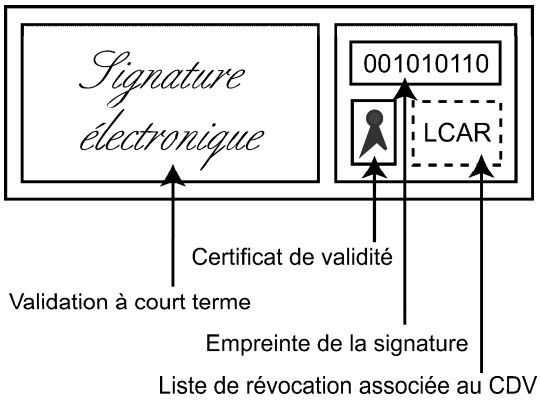

FIG. 3 – *Apposition d'un certificat de validité à une signature*

Le CDV est soit demandé au moment de la création ou de la validation de la signature. Une connexion au SVS est alors requise afin de joindre ce justificatif de statut à la signature. L'intérêt de recourir au CDV est qu'aucune connexion supplémentaire n'est nécessaire, du moment que le CDV est intégré à la SE. Il protège de plus la valeur de la signature en lui conférant une validité jusqu'à expiration ou révocation du certificat du SVS.

Le CDV est composé des éléments suivants :

- *SignatureValidity* : renferme l'empreinte numérique de la signature certifiée (source) envoyée par le demandeur ainsi qu'une valeur de statut de validité (valide, expirée, révokée, etc.) et une donnée temporelle optionnelle. Cette date locale au SVS peut être remplacée par un horodatage.
- *Signature* : la signature électronique du SVS visant à sceller le CDV. Le statut de la signature du SVS est alors omis, le SVS étant un tiers de confiance.

Ce protocole est fiable du fait que la signature électronique utilisée octroie intrinsèquement la possibilité de joindre cette information de validité ("CertifiedSignatureValidity"). Les définitions IETF et ETSI de la signature comme étant la combinaison d'une chaîne de bits et d'un certificat numérique ne permettent pas en l'état une telle intégration :

```
Signature ::= SEQUENCE {
  version     INTEGER {v2(2)},
  sign        Sign,
  policy  [0] Policies                    OPTIONAL,
  ts      [1] TimeStamps                  OPTIONAL,
  status  [2] CertifiedSignatureValidity OPTIONAL,
  counter [3] Signatures                  OPTIONAL,
  extns   [4] Extensions                  OPTIONAL
}

CertifiedSignatureValidity ::= SEQUENCE {
  version     INTEGER {v1(1)},
  validity    SignatureValidity,
  sign        Signature,
  extns       Extensions     OPTIONAL
}

SignatureValidity ::= SEQUENCE {
  sign        MessageImprint,
  -- empreinte de la signature du demandeur (TSP)
```

```
  status      ValidityStatus,
  ts          GeneralizedTime OPTIONAL
  extns       Extensions      OPTIONAL
}

ValidityStatus ::= PKIStatus
```

La validité de la SE étant conditionnée par le CDV, le vérificateur doit s'assurer de son authenticité. Pour ce faire, il lui suffit de s'assurer que le certificat du SVS n'est pas mentionné dans une liste de certificats d'autorités révoqués (LCAR – ACRL). Une LCAR est une LCR ne comportant que des identifiants de certificats d'autorités. Sa mise à jour est donc beaucoup moins fréquente qu'une LCR car une LCAR doit -en théorie- demeurer vide.

La validité sur le long terme des SEs certifiées par un CDV est obtenue par la traçabilité interne au SVS. En effet, ce dernier conserve une trace de chaque CDV généré afin de permettre une réactualisation lorsque le vérificateur souhaite obtenir des informations de validité acualisées (faisant appel aux dernières technologies). La réactualisation d'un CDV conserve le statut de validité originel afin que la validité de la signature soit figé dans le temps.

5.4 Conclusion

La SE à long terme de l'ETSI (ES, ES-T, ES-C et ES-X) fait appel à deux niveaux d'horodatage. Le premier horodatage (ES-T) permet de dater le moment de signature afin de permettre une validation *a posteriori*. En revanche, le second horodatage (ES-X) sert uniquement de protection de la signature ES-C contre l'évolution technologique. Ce ne devrait donc pas être un horodatage mais un service similaire dont le but ultime n'est pas la non-répudiation mais la sécurité des informations d'époque. De plus, la validation d'une SE de type ES-X implique au moins quatre contrôles : l'un pour valider l'horodatage ES-X, l'autre pour valider la signature de la LCR ES-C (en supposant qu'il n'y en ait qu'une), le troisième pour valider l'horodatage ES-T et le dernier pour valider le certificat du signataire ES.

Le CDV offre une validation à long terme sous réserve que sa réactualisation n'introduise pas de changement dans la valeur de validité qu'il renferme. En particulier, le cas où deux vérificateurs demandent la génération d'un CDV à des moments différents peut introduire une incohérence dans la valeur certifiée par le SVS si le signataire a révoqué son certificat entre les deux demandes et que cette révocation est publiée. Le SVS doit donc non seulement tenir compte du statut courant du certificat du signataire mais également considérer le premier CDV généré comme référence pour les CDV suivants. En contrepartie, une seule validation critique est nécessaire, celle de la signature apposée par le SVS sur le CDV justifiant la validité de la SE contrôlée. Cette validation s'effectue par le biais d'une LRA et non d'une LCR.

6 Conclusion générale

Après avoir défini les notions de validité à court, moyen et long terme, nous avons étudié les principales méthodes visant à valider les signatures électroniques au cours du temps. L'intérêt des protocoles de validation à court terme tels qu'OCSP s'est montré relativement faible et supplanté par les LCRs lors d'un besoin de validation à moyen et long terme. Nous avons considéré les propositions de validation à long terme des SEs par le biais de la signature ETSI et du certificat de validité (CDV) et mis l'accent sur leurs points forts et leurs faiblesses. Dans les deux cas, la preuve de validité à long terme repose sur la mise à jour régulière des informations annexées à la signature telles que l'horodatage ou le renouvellement du CDV. Il apparaît alors que la preuve d'authenticité des SEs sur le long terme ne doit reposer non seulement sur l'ICP et les procédés de validation (horodatage, CDV) mais également sur la notarisation électronique et l'archivage sécurisé [20]. Il sera alors du ressort de l'archiveur de tenir à jour sa propre signature électronique apposée aux archives lors de leur restitution.

Peut-on pour autant prétendre que tout contenu archivé et comportant une SE valide sur le long terme est authentique, sachant que les fonctions de hachage actuellement employées ne seront plus résistantes aux collisions dans le futur ? Il sera alors possible de falsifier des documents à valeur légale et signés

électroniquement... Il convient cependant de garder à l'esprit que la preuve d'authenticité d'un contenu est déterminée par un juge. Les outils de validation des SEs apportent leur expertise au juriste en lui fournissant des éléments de réponse quant à l'appréciation objective de l'authenticité du contenant porté comme preuve. Le juriste peut ainsi porter son attention sur le contenu. Il est cependant concevable qu'un contenu signé électroniquement de manière non conforme aux normes en vigueur et indiquant des signatures invalides soit retenu au même titre qu'un contenu auquel sont apposées des SEs avancées valides à long terme et générées à l'aide de certificats électroniques qualifiés dans un environnement sécurisé de signature.

Références

[1] Sénat français, "La signature électronique : note de synthèse", 2001

[2] European Electronic Signature Standardization Initiative (EESSI), "Final Report of the EESSI Expert Team", par. 4.2, p. 27, juillet 1999

[3] Assemblée nationale, Sénat français, "Loi n° 200-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique", Journal Officiel n° 62 du 14 mars 2000, p. 3968

[4] R. Housley, W. Polk, W. Ford, D. Solo, "RFC 3280 : Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile", avril 2002

[5] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "RFC2560 : X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP", juin 1999

[6] European Telecommunications Standards Institute, ETSI TS 101 733 V1.4.0, "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats", spécification technique, septembre 2002

[7] European Telecommunications Standards Institute, ETSI ES 201 733 V1.1.3, "Electronic Signature Formats", spécification technique, mai 2000

[8] Trustronic, TT TD S01-1.2d, "EDCI ASN.1 data structures v1.2d", documentation technique, disponible sur www.trustronic.org, janvier 2003

[9] N. Cottin, B. Mignot, M. Wack, "Authentification and Enterprise Secured Data Storage", invited paper, IEEE Emerging Technogies and Factory Automation, ETFA 2001, Sophia-Antipolis, France, octobre 2001

[10] H. Nilsson, D. Pinkas, "Validation of Electronic Signatures", rapport interne, mars 1999

[11] O. Dubuisson, "ASN.1 : Communication between Heterogeneous Systems", Morgan Kaufmann Publishers, ISBN 0-12-6333361-0, juin 2000

[12] D. A. Cooper, "A More Efficient Use of delta-CRLs", IEEE Symposium on Security and Privacy, pp. 190-202, mai 2000

[13] Groupe de Travail Commun Horodatage, CSOEC, IALTA france, EDIFICAS, "Recommandations pour l'horodatage électronique", à paraître

[14] G. Endersz, "Electronic Signature and PKI Standardisation in Europe: Work-plan & Current Status", rencontre FPKI TWG, Gaithersburg, juin 2000

[15] A. Buldas, M. Roos, J. Willemson, "On Long-Term Validation of E-Documents", Valdo Praust, Estonian Data Protection Inspectorate, Baltic IT, review 2, 2000

[16] A. Ansper, A. Buldas, M. Roos, J. Willemson, "Efficient long-term validation of digital signatures", Advances in Cryptology - PKC 2001, Springer-Verlag, LNCS 1992, pp. 402-415, février 2001

[17] C. Adams, R. Zuccherato, "Notary Protocols", Internet Draft, disponible sur le site IETF 'draft-adams-notary-01.txt', février 1997

[18] D. Rieupet, N. Cottin, "Scénarios d'apposition de multiples signatures", version 1.0, rapport interne, janvier 2003

[19] N. Cottin, M. Wack, A. Sehili, "Time-stamping electronic documents and signatures", rapport interne, décembre 2002

[20] Groupe de Travail Commun Archivage, CSOEC, IALTA france, EDIFICAS, "Guide de l'archivage électronique sécurisé", juillet 2000