*Club*PSCo

Commentaires relatifs au règlement européen

« electronic identification and trust services for electronic transactions in the internal market »

Version	Date	Description	Auteurs	Entité
1.0	20/07/2012	Document de travail	E. Combet / J. Bordier	Club PSCo

Ce document identifie les questions, les différents points d'incompréhension, identifiés par les membres du *Club***PSCo** et relatifs au projet de règlement européen « electronic identification and trust services for electronic transactions in the internal market ».

Remarques d'ordre général
Le règlement prévoit deux types de certificats (qualifiés et non qualifiés), et 3 formes de signature (simple, avancée, qualifiée), emportant des conséquences juridiques différentes, définies pour les signatures simples et qualifiées, mais non définies pour les signatures avancées. Nous souhaitons que la valeur juridique de la signature « avancée » soit établie de la façon suivante : une signature électronique laissant la charge de la preuve à son producteur, mais réunissant des conditions de sécurité et de preuve équivalentes à une signature qualifiée auditée selon d'autres conditions à définir dans le cadre du schéma de supervision fixé au sein du règlement (cf. ETSI TS 102 042 NCP par exemple).
La signature électronique qualifiée repose exclusivement sur l'usage d'un certificat qualifié. Pour l'utilisateur, il est donc nécessaire de décrire les conditions concrètes dans lesquelles la signature électronique qualifiée est produite : • Sur le plan fonctionnel : obligation de donner accès aux informations signées au signataire, mise à disposition d'une Politique de Signature ; • Sur le plan technique : obligation d'usage d'un environnement sécurisé (logiciel de signature qualifié, infrastructure, matériel, système hôte notamment).
Vis-à-vis des services « electronic delivery services » : la problématique de la confidentialité des échanges est absente. Il est nécessaire de garantir le non accès de l'opérateur aux données des messages échangés.
Nous souhaitons que les actes délégués ne concernent pas ce qui relève de standards, de normes techniques (ETSI, CEN).
Nous souhaitons que la notion de « Qualified Trust Service Provider » soit précisée par type de services dans les articles concernés (ex : préciser « Qualified Timestamp Trust Service Provider » pour les fournisseurs de services d'horodatage qualifiés)
Nous souhaitons que le système de hiérarchisation (simple, advanced, qualified) soit étendu aux autres services de confiance (archivage, horodatage, electronic delivery service, signature verification).

Numéro ou intitulé du paragraphe		
Art 2	§3	« This Regulation does not apply to aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Union law. » Doit-on comprendre que cette disposition vise les cas particuliers, tels que les problématiques de caution solidaires de personnes physiques, de contrats de location ou de prêts immobiliers et les actes authentiques ?
Art 3	§19	« 'creator of a seal' means a legal person who creates an electronic seal » Considérant que c'est une machine qui va techniquement « créer » le sceau électronique, il faudrait amender la définition pour faire la distinction entre le « creator du seal » et le « owner of the seal »
Art 9	§1	« A trust service provider shall be liable for any direct damage » Nous souhaitons que la responsabilité des TSPs ne soit pas illimitée. Chaque TSP proposera des limites de responsabilité sur les services qu'il fournit.
Art 13	§2.a	« monitoring trust service providers established » Qu'induit précisément le « monitoring ». Quelle est la différence avec les conséquences de la notion « undertaking supervision » dédiée aux TSP qualifiés ? Il faudrait définir les termes « supervision » et « monitoring », et leurs conséquences pour les TSP. Il faudrait que soient précisées les conditions de maintien des statuts des TSP pour s'assurer qu'un TSP initialement qualifié ne dégrade progressivement ses conditions de service. Il faudrait que les TSP soient audités sur une base annuelle par les « supervisory body ».
Art 13	§2.c	« ensuring that relevant information and data referred to in point (g) of Article 19(2), and recorded by qualified trust service providers are preserved and kept accessible after the activities of a qualified trust service provider have ceased, for an appropriate time with a view to guaranteeing continuity of the service. » Il faudrait que ces obligations soient à la charge des supervisory body des Etats membres pour que ce soit applicable opérationnellement.
Art 13	§2	Il faudrait que le supervisory body publie le schéma d'accréditation qu'il a défini pour les TSP qu'il a la responsabilité de superviser, monitorer.

Art 15	§1	« Without prejudice to Article 16(1), any trust service provider **may** submit the report of a security audit carried out by a recognised independent body to the supervisory body to confirm that appropriate security measures have been taken. » Que se passe-t-il si le TSP ne soumet pas de rapport, ou si le rapport fait mention de non conformités majeures ? Quels critères permettent-ils de juger si l'auditeur est « recognised » ? Doit-il être habilité par les Etats membres ? Il faudrait affirmer l'obligation de soumettre un rapport d'audit positif avant de pouvoir se prévaloir de ce niveau et de produire les services visés. Il faudrait définir un processus d'agrément des auditeurs, par les « supervisory body ».
Art 15		Il faudrait que les TSP publient une Politique de Sécurité qui décrive le niveau de sécurité atteint par les services proposés.
Art 16	Titre	« Supervision of qualified trust service providers » Il faudrait un article supplémentaire « Monitoring of non qualified trust service providers »
Art 16	§1	« Qualified trust service providers shall be audited by a recognised independent body » Quels critères permettent-ils de juger si l'auditeur est « recognised » ? Il faudrait que ces auditeurs soient habilités par les supervisory body selon un schéma d'accréditation public
Art 17	§1	« Qualified trust service providers may start to provide the qualified trust service after they have submitted the notification and security audit report to the supervisory body. » Que se passe-t-il si le rapport fait mention de non conformités bloquantes ? Le TSP a-t-il néanmoins le droit de commencer à opérer ? Quid de la valeur des signatures électroniques produites avec des certificats qualifiés qui s'avèrent ensuite produits dans des conditions « non qualifiées » ? Il faudrait que le lancement « commercial » ou « opérationnel » des services des TSP soient conditionnés à l'acceptation par les supervisory body du rapport d'audit positif.

Art 17	§2	« Once the relevant documents are submitted to the supervisory body according to paragraph 1, the qualified service providers shall be included in the trusted » En complément à la remarque « Art 17, §1 », que se passe-t-il si un état membre fait confiance à un certificat qualifié produit dans un autre pays membre et qu'il s'avère ensuite qu'il n'était pas produit dans des conditions dignes d'obtenir le statut de « certificat qualifié »
Art 17	§3	« The supervisory body shall indicate the qualified status of the qualified service providers and the qualified trust services they provide in the trusted lists after the positive conclusion of the verification, not later than one month after the notification has been done in accordance with paragraph 1 » Cette disposition nous semble incohérente avec la précédente qui précise que le TSP a le droit de faire partie de la TSL à compter de son envoi du rapport au « supervisory body »
Art 17	§3	« If the verification is not concluded within one month, the supervisory body shall inform the qualified trust service provider specifying the reasons of the delay and the period by which the verification shall be concluded. » Combien de temps cela peut-il durer ? et que fait-on des certificats et des signatures qualifiés produits dans l'intervalle de temps ? (cf. remarques ci-dessus) Il faudrait que les délais de validation des rapports d'audit par les supervisory soient encadrés, surtout si cette validation conditionne le lancement opérationnel des services visés.

Art 17	§4	« A qualified trust service which has been subject to the notification referred to in paragraph 1 cannot be refused for the fulfilment of an administrative procedure or formality by the concerned public sector body for not being included in the lists referred to in paragraph 3. » Cette disposition nous parait susceptible de créer un certain nombre de contentieux. Sachant que le TSP peut commencer à délivrer des certificats qualifiés dès l'envoi du rapport d'audit à son « supervisory body », il n'apparaîtrait techniquement dans la TSL qu'au mieux quelques heures (jours plutôt) après. Comment une Autorité Administrative peut-elle avoir connaissance du fait que ce TSP a obtenu le droit de produire des certificats qualifiés tant qu'il n'apparait pas dans la TSL ? Par ailleurs, il faudrait laisser un délai raisonnable aux autorités administratives pour mettre à jour leurs plates-formes de téléservices, car il y aura probablement un délai de latence entre la publication d'une nouvelle TSL et sa prise en compte technique sur les plates-formes des autorités administratives
Art 19	§1	« Such information shall be verified by the qualified service provider or by an authorised thirdparty acting under the responsibility of the qualified service provider: » Le TSP qualifié se verra-t-il imposer des contraintes, des exigences, pour la contractualisation avec les « authorised thirdparty » ? Il faudrait préciser que ces « authorised thirdparty » feront partie du périmètre de l'audit du TSP qualifié.
Art 19	§2.d	« use trustworthy systems » Quelle est la définition associée à ces termes ? « an appropriate period of time » : il faudrait que ces délais soient précisés.

Art 19	§3	« Qualified trust service providers issuing qualified certificates shall register in their certificate database the revocation of the certificate within ten minutes after such revocation has taken effect. » Parle-t-on de « certificate database » ou de « CRL » ? Les plates-formes téléservices exploitent aujourd'hui majoritairement les fichiers .CRL produits par les TSP. Qu'entend-on par ailleurs par « after such revocation has taken effect » ? (date de demande de révocation par le porteur, de prise en compte de la demande par le TSP, de validation de la demande après vérification par le TSP, d'enregistrement en base de données, de production de la CRL, de publication de la CRL ?). Le standard ETSI 101 456 prévoit une fréquence de mise à jour des CRLs de 24 heures minimum qui suivent la demande de révocation. En conséquences, nous souhaitons que le règlement soit modifié de la façon suivante : « Qualified trust service providers issuing qualified certificates shall publish certificate revocation lists within 24 hours after revocation request. »
Art 20	§2	« A qualified electronic signature shall have the equivalent legal effect of a handwritten signature. » Quelle valeur a une signature avancée ? (pas défini – cf. Remarques de fond)
Art 20	§4	« If an electronic signature with a security assurance level below qualified electronic signature is required, in particular by a Member State for accessing a service online offered by a public sector body on the basis of an appropriate assessment of the risks involved in such a service, all electronic signatures matching at least the same security assurance level shall be recognised and accepted. » Le terme « below » parait créer une confusion. Notre compréhension est qu'il n'existe que 3 niveaux de signature (qualifiée, avancée, simple). Pourquoi ne pas parler de « signature avancée » dans ce § si c'est le type de signature visée ?
Art 22	§1	« Qualified electronic signature creation devices **shall** meet the requirements laid down in » Annex IIIl faudrait transformer le ter me « shall » en « must »

Art 23	§1	« Qualified electronic signature creation devices **may** be certified » Il faudrait que cette possibilité soit transformée en obligation.
Art 25	§1.b	« the qualified certificate required is authentic » Il faudrait supprimer le terme « authentic » qui n'est pas défini et redondant avec la notion de certificat qualifié.
Art 25	§1.b	Il faudrait ajouter une exigence d'horodatage de la signature, pour se mettre en capacité de vérifier ultérieurement que le certificat est valide au moment de la signature.
Art 26	§1.b	« and bearing the **advanced electronic signature or advanced electronic seal** of the provider of the qualified validation service. » Il faudrait définir les conditions opérationnelles de production d'une « advanced signature ».
Art 27	§1	« A qualified electronic signature preservation service shall be provided by a qualified trust service provider who uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature validation data beyond the technological validity period. » Il faudrait définir une liste d'exigences applicables pour qualifier un TSP qui souhaiterait fournir ce type de services.
Art 28	§5	« Member States shall not request for accessing a service online offered by a public sector body an electronic seal with higher security assurance level than qualified electronic seals. » Comment peut-on accéder à un téléservice avec une signature électronique ? Ne confond-on pas les notions d'authentification et de signature ?
Art 33	§1.d	« it is signed using an advanced electronic signature or an advanced electronic seal of the qualified trust service provider, or by some equivalent method. » Il faudrait définir les conditions opérationnelles de production d'une « advanced signature » « equivalent method » : comment peut-on en juger ?

Art 36	§1.b	« and if appropriate » Comment le TSP délivrant ces services pourrait-il remettre un pli électronique sans être en capacité d'identifier le destinataire ? Il conviendrait de préciser la notion de « unambiguous identification ».
Annexe 1	(f)	« The certificate identity code which must be unique for the qualified trust service provider » Il ne faudrait pas imposer aux TSPs qui fournissent plusieurs gammes de services qualifiés de gérer un identifiant unique pour tous leurs clients. On pourrait par contre imposer que ce code soit unique par « service » fourni par un même TSP.
Annexe 1	(g)	« the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider » Cf. Remarques ci-dessus sur la définition et les exigences relatives aux « advanced » seal et signature.
Annexes		Il faudrait ajouter des annexes pour décrire les exigences relatives à tous les services de confiance que peuvent fournir les TSPs, et pas seulement celles applicables aux certificats (horodatage, vérification, archivage, electronic delivery service)