Forum ATENA – MEDEF

« l'e-gouvernement, les services et l'économie transformés par les identités numériques » (4ème édition du colloque sur l'identité numérique),

19 novembre 2014, Paris

Le Règlement européen EiDAS

Eric A. CAPRIOLI

Avocat au Barreau de Paris
Docteur en droit
Membre de la délégation française aux Nations Unies sur le commerce électronique
Vice-Président de la Fédération des Tiers de Confiance (FNTC)

© CAPRIOLI & Associés – Société d'Avocats - www.caprioli-avocats.com

contact@caprioli-avocats.com / contactparis@caprioli-avocats.com

Le Cabinet Caprioli & Associés est une société d'avocats en droit des affaires : conseil, audit, formation, veille juridique, contentieux et arbitrage

Spécialisé dans :

- L'informatique, les technologies de l'information et des communications électroniques (contrats, e-commerce, etc.)
- la dématérialisation des documents et des échanges (authentification/identification, contractualisation, signature, horodatage, gestion de preuve et archivage)
- La sécurité des systèmes d'information
- La protection des données à caractère personnel (réglementation, formalités, chartes, accompagnement CIL/DPD, audit, etc.)
- Les propriétés intellectuelles (noms de domaine, droit d'auteur, marques, dessins, brevets, logiciels, bases de données, …)

Adresses : **29 rue de Mogador, 75009 Paris**
9, avenue Henri Matisse, 06200 Nice
Site Web : **www.caprioli-avocats.com**
Mail : **contact@caprioli-avocats.com (Nice)**
contactparis@caprioli-avocats.com (Paris)

I. Introduction

II. Identification et services de confiance

III. Prestataires de services de confiance

Règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques du 23 juillet 2014

Cadre transnational et intersectoriel complet pour des transactions électroniques

- **identification électronique (étatique)**
- **services de confiance et prestataires (PSCo)**

Fondement de liberté : démarche volontaire et non obligatoire des acteurs.

Harmonisation des règles nationales en matière de signature électronique / aucune transposition dans les systèmes juridiques des 28 Etats membres n'est à prévoir

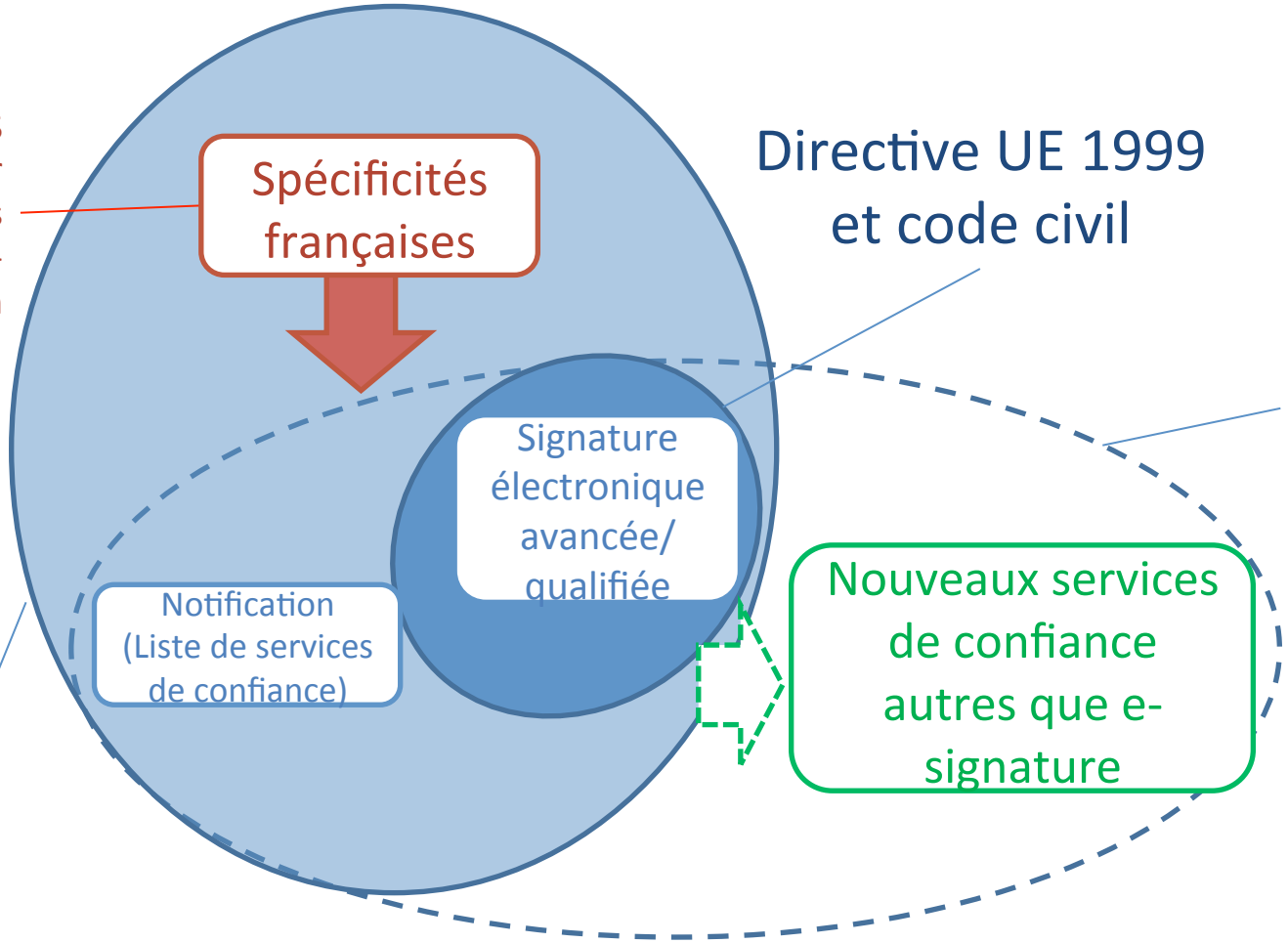
Un acte **délégué et des actes d'exécution** pour l'identification et les services de confiance **Abrogation de la directive du 13 décembre 1999 le 1er juillet 2016, mais effets jusqu'en 2010**

La confiance : pierre angulaire de la proposition de règlement européen

CONFIANCE

- Fiabilité
- Garanties
- Sécurité

Conjonction des cadres juridiques



I. Introduction

II. Identification et services de confiance

III. Prestataires de services de confiance

Authentification et identification numériques

- Les États membres acceptent **les systèmes d'identification électronique nationaux** qui ont été officiellement notifiés à la Commission (Chapitre II Identification électronique)
- « *En cas* ***d'atteinte ou d'altération*** *partielle du schéma d'identification électronique notifié (…), ou de l'authentification (…), telle qu'elle affecte la fiabilité de l'authentification transfrontalière de ce schéma,* ***l'État membre notifiant suspend ou révoque, immédiatement, cette authentification*** *transfrontalière* ***ou les éléments altérés en cause****, et en informe les autres États membres et la Commission* » (art. 10)
- **Responsabilité des Etats membres** (art. 11)

⇒ Aucune responsabilité concernant des transactions entre parties privées s'appuyant sur les moyens d'identification étatique : art. 11-5)

Authentification et identification numériques

France

Uniquement identification étatique
(identification privée hors scope)

- §3.2 du RGS : « ***l'authentification*** *a pour but de vérifier l'identité dont une entité (personne ou serveur) se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer une identité préalablement enregistrée, s'authentifier c'est apporter la preuve de cette identité* »
- **Identification numérique** : projet de la mise en service d'une carte nationale d'identité (électronique) spécifique, avec un objectif « *d'identification générale et non des usages spécifiques, comme le permis de conduire ou le passeport* ».

⇒ **France Connect (projet) :** système permettant aux usagers, s'ils le souhaitent, de fédérer leurs comptes créés auprès des différents services publics (soumis à la CNIL)

Authentification et identification numériques

- Délit **d'usurpation d'identité numérique** (art. 226-4-1 du Code pénal): « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur* ***un réseau de communication au public en ligne***».

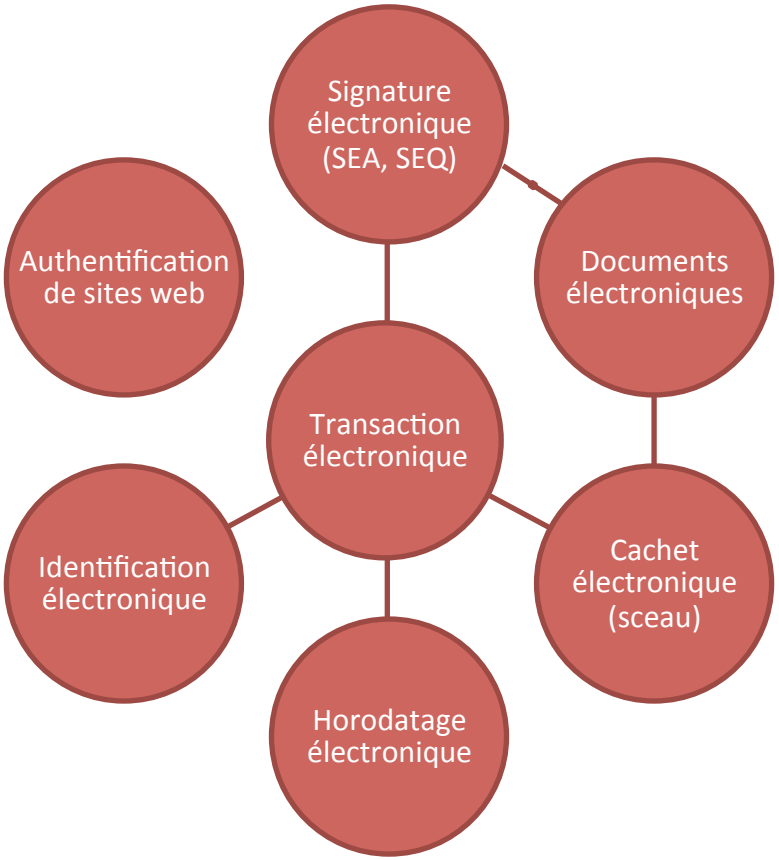
  → **CA Paris 10 octobre 2014** : **condamnation de l'usurpateur à 10 mois d'emprisonnement avec sursis et 30.000 € de dommages et intérêts.**

- **Authentification des sites Web** : trois niveaux de sécurité pour les certificats électroniques émis par des prestataires de services de certification – v. *Politique de Certification Type Authentification serveur* du RGS.

Définition d'un service de confiance (art. 3 du Règlement)

Un service électronique consistant à **la création, la vérification, la validation, le traitement et la conservation de signatures électroniques, de cachets électroniques, d'horodatage électronique, de documents électroniques, de services de fourniture électronique, d'authentification de sites Web et de certificats électroniques, y compris de certificats de signature électronique et de cachet électronique**.

Quels services de confiance ?



a) Signature électronique

Règlement UE

❖ L'article 3 énonce **3 niveaux de signatures (idem France mais une seule valable !) :**

Signature électronique simple : « *des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données électroniques et que le signataire utilise pour signer* » (qu'est-ce que signer ?)

Signature électronique avancée : elle doit au surplus être uniquement liée au signataire, permettre de l'identifier, avoir été créée à l'aide des données de création que le signataire peut utiliser sur son contrôle exclusif et être liée aux données auxquelles elle est associée de telle sorte que toute modification ultérieure des données soit détectable (intégrité)

Signature électronique qualifiée : « *une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié et qui repose sur un certificat qualifié de signature électronique* » **(équivalent signature électronique sécurisée présumée fiable en France : art. 1316-4 c. civ. et articles 1 et 2 du décret du 30 mars 2001).**

Signature électronique

Règlement UE (art. 25 et s)

- La signature électronique qualifiée **reçoit le même effet juridique que la signature manuscrite** et doit faire l'objet de la reconnaissance et de l'acceptation mutuelle dans les Etats membres.
- Non discrimination vis-à-vis des SE non qualifiées.
- Certification des dispositifs de création des signatures électroniques qualifiées
- Aspects de la **signature électronique dans le secteur public**
- Intégration des **services de validation et de conservation** des signatures électroniques qualifiées
- Intégration des **signatures électroniques centralisées** (activées à distance) (considérant 52)

Le Règlement, tout comme la directive n° 1999/93, ne prévoit pas que la signature électronique garantisse expressément le consentement du signataire au contenu juridique de l'acte signé contrairement à l'article 1316-4, al. 1 c. civ.

Exemple pratique :

TI Epinal, 12 décembre 2011

- **Décision TI** : *document « fichier preuve de la transaction » est à lui seul insuffisant pour s'assurer non seulement de l'engagement de M. X puisqu'aucun élément de la prétendue signature électronique ne permet de faire le lien entre l'offre de prêt non signée et le document produit, en l'état simple fichier imprimé,* ***sans garantie d'authenticité, ni justification de la sécurisation employée*** *»*

⇒ **Non prise en compte de l'avenant électronique pour faire débuter le délai de forclusion et donc action forclose.**

CA Nancy, 14 février 2013

- Appel de la décision du TI Epinal du 12 décembre 2011
  - Fichier de preuve de la transaction, produit aux débats, a été émis par l'autorité de certification
  - Démonstration en justice du mode de fonctionnement/Attestation de l'AC
  - « *la mention du numéro de l'avenant sur le fichier de preuve permet de vérifier que c'est bien cet avenant qui a été signé électroniquement par Monsieur X* ».

⇒ **Action en paiement non forclose pour la Banque (Voir égal en ce sens : CA Douai 2 mai 2013).**

Scellement

- **Cachets électroniques qui** « *devraient servir à prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document* ».
- Intervention nécessaire d'une **personne physique** – c'est elle qui crée le cachet électronique.
- **Trois niveaux de sécurité** : cachet électronique **simple, avancé, qualifié** (ce dernier bénéficiant de la **présomption de fiabilité** et faisant l'objet de **la reconnaissance et de l'acceptation mutuelles)**

  → ***RGS :*** *la fonction « Signature » couvre le cas de la signature réalisée par un individu, pendant qu'une signature effectuée par un serveur (ex : signature d'un accusé de réception) constitue la fonction « Cachet ».*

Scellement

- **Certificat de serveur (signature technique //signature « juridique ») :** « signature » de la personne morale, fonctions d'authentification et d'intégrité, pas de consentement

- Question sur l'intervention d'une **personne physique (ou morale)** dans le processus de scellement

- Ex.: **Dématérialisation des factures** **:** Art.289 du CGI
- ou **bulletin de paie** (art.L.3243-2 et s. du code du travail).

Horodatage

- **Deux niveaux de sécurité : horodatage simple ou qualifié.**
- **Horodatage simple :** « *des données sous forme électronique qui associent d'autres données électroniques à un instant particulier et établissent la preuve que ces données existaient à cet instant* »
- **Horodatage qualifié :**

- lié avec l'exactitude au temps universel coordonné (TUC) de manière à exclure toute possibilité de modification indétectable des données
- basé sur une horloge exacte
- délivré par un prestataire de services de confiance qualifié
- signé au moyen d'une signature électronique avancée ou d'un cachet électronique avancé du prestataire de service de confiance **qualifié**, ou par une méthode équivalente.

Horodatage

- **Art. 1369-7 du Code civil** : « *l'apposition de la date d'expédition résulte d'un procédé électronique dont la fiabilité est présumée, jusqu'à preuve contraire, lorsqu'il satisfait à des exigences fixées par décret en Conseil d'Etat* ».
- **RGS : Politique d'Horodatage Type -** afin de sécuriser les systèmes d'informations sous la responsabilité d'une autorité administrative avec une fonction d'horodatage, celle-ci doit utiliser des jetons d'horodatage délivrés par des Prestataires des Services d'Horodatage Electronique conformes à la Politique d'Horodatage Type.

Service d'envoi recommandé électronique

- **Deux niveaux de sécurité : Service d'envoi recommandé simple ou qualifié.**
- **Service d'envoi recommandé électronique:** « *un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée* »
- **Service d'envoi recommandé qualifié :**

- Un ou plusieurs prestataires
- Garantie de l'identification de l'expéditeur avec un degré élevé et **garantie** de l'identification du destinataire avant la fourniture de données
- Sécurisation de l'envoi et de la réception de données avec une signature électronique ou un cachet électronique avancés d'un PSCo qualifié
- Toute modification des données doit être signalée
- Recours à un horodatage électronique qualifié pour la date et l'heure d'envoi et de réception

Service d'envoi recommandé

- **Lettre Recommandée Electronique :** article 1369-8 du Code civil et son décret d'application : le décret n°2011-144 du 2 février 2011 relatif à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat.
- **Ordonnance n° 2014-1330 du 6 novembre 2014 relative au droit des usagers de saisir l'administration par voie électronique**

Horodatage

- **Deux niveaux de sécurité** : procédé d'horodatage fiable (art. 2 Décret 2011-434) ou pas :

Pour bénéficier d'une présomption de fiabilité, le procédé doit être établi par un **PSHE répondant à des exigences formulées dans l'art. 3** et le module d'horodatage doit être **certifié conformément** aux exigences du décret.

Documents électroniques

- **Art. 46 :** L'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique

⇒ **Rappel du principe de non discrimination médiatique**

I. Introduction

II. Identification et services de confiance

III. Prestataires de services de confiance

Prestataire de services de confiance (PSCo) et responsabilité

- **Définition (art. 3.19) :** *« une personne physique ou morale qui fournit un ou plusieurs services de confiance »*

- **Quelle(s) responsabilité(s) (art. 13) ?**

Responsabilité du PSCo vis à vis des **dommages causés intentionnellement ou par négligence en raison d'un manquement à ses obligations**

Le PSCo qualifié est présumé avoir agi intentionnellement ou par négligence sauf preuve contraire

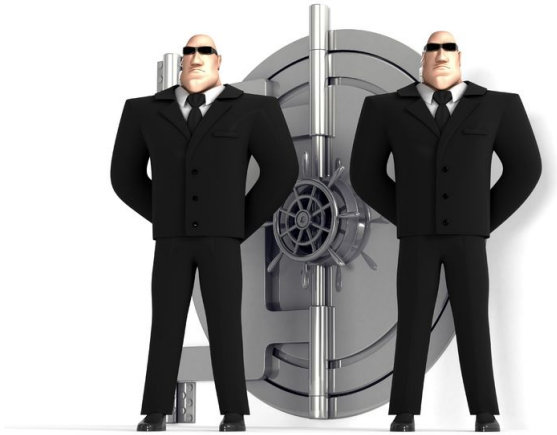
- **Un degré de contrainte plus élevé**

=

Respect des obligations mises à la charge du prestataire

Deux obligations majeures pour les prestataires de services de confiance

Exigences de Sécurité **&** **notification des failles de sécurité**



PSCo et notifications (art. 19)

CNIL.

Responsabilité des prestataires de services de confiance qualifiés

Rôle de l'organe de contrôle

- Surveillance des PSCo établis sur le territoire de l'Etat membre qui a procédé à la désignation afin de s'assurer du respect des exigences ;
- Contrôle des PSCo qualifiés et des services de confiance qu'ils fournissent pour le respect des exigences prévues par le règlement.
- Veille pour la préservation et l'accessibilité des informations et données enregistrées par le PSCo après la cessation de son activité pour garantie la continuité du service.

Pouvoirs de l'organe de contrôle (art. 17 et suivants)

Vérification du respect du règlement, enjoindre le PSCo à corriger les manquements

Audit des PSCo qualifiés

Informe l'autorité de protection des données à caractère personnel des manquements à la règlementation

Décide d'accorder ou de retirer le statut de PSCo qualifié

Rapport annuel (activités, notifications des failles, statistiques)

Gestion des listes de confiance

Qualification du PSCo

Ouverture d'un service de confiance qualifié

- Notification de l'intention de fournir un tel service à l'organe de contrôle
- Audit de sécurité par un organisme indépendant reconnu

Inscription sur les listes de confiance

- Mise à jour et publication des listes de confiance
- Informations relatives aux prestataires de confiance et aux services fournis
- Mise à disposition du public par la Commission via un canal sécurisé

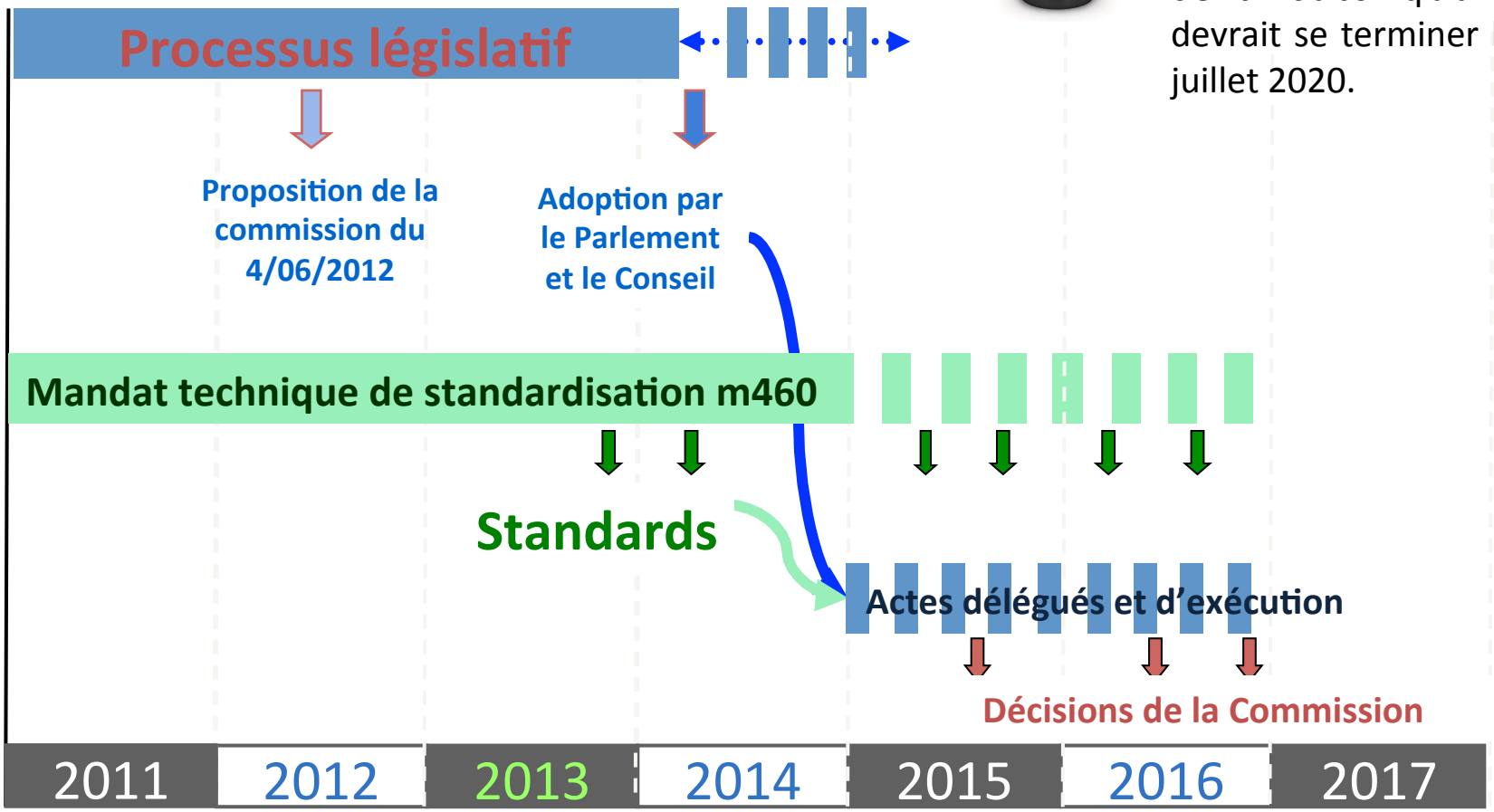
Présomption de fiabilité du service et interopérabilité

- Inversement de la charge de la preuve en cas de litige
- Confiance accrue

La Commission précisera à l'aide d'actes d'exécution et d'actes délégués les moyens techniques permettant de disposer d'un service de confiance qualifié et d'un PSCo lui même qualifié.

Process indicatif

La migration pour les certificats qualifiés devrait se terminer le 1er juillet 2020.



? ? ? ? ? ? ? ?

Avez-vous des questions ?

Merci de votre attention !

Eric A. Caprioli
Avocat à la Cour, Docteur en droit
Vice-Président de la FNTC
Membre de la délégation française à l'ONU

e.caprioli@caprioli-avocats.com

© CAPRIOLI & Associés, Société d'avocats
29, rue de Mogador, 75009 Paris / Tél. 01 47 70 22 12
9, avenue Henri Matisse, 06200 Nice / Tél. 04 93 83 31 31
www.caprioli-avocats.com
mél : contactparis@caprioli-avocats.com
Certaines images dans cette présentation sont la propriété de la société EPICTURA ou de ses fournisseurs et ayants droits. Le contenu ne peut être exploité sans licence ni sans l'autorisation expresse, par écrit de la société EPICTURA