Titre du document

Tâche 1.6 Elaboration du contrat électronique certifié et de l'authentification

Livrable : Tâches 1.6.1 : Rapport descriptif du contrat électronique certifié (structure, fonctions, usage)

Objet du document

Sécurisation de la contractualisation électronique.

L'objectif de ce document est de prendre connaissance du cadre juridique de la contractualisation électronique, des opportunités, des risques et des modèles de mises en œuvre en matière de sécurisation de la contractualisation électronique.

Informations sur le document

Responsable	Référence	Description	Date livraison
CHONOSERVICES	T1.6.1	Version 1.0	18/04/2013
CHONOSERVICES	T1.6.1	Version 2.0	15/07/2013

Contributions

Contributeurs	Pourcentage
CHONOSERVICES	100 %

Table des matières

Objectifs du livrable

A l'heure du numérique, la contractualisation s'est naturellement dirigée vers une dématérialisation totale que ce soit dans la sphère professionnelle (BtoB) ou chez les consommateurs (BtoC).

Aujourd'hui, tous les types d'actes, de documents métier, peuvent être dématérialisés, à titre d'exemples :

- Formulaires de souscription,
- Contrat consommateur,
- Contrat client-fournisseur,
- Cahier des charges fournisseurs,
- Factures,
- PV de fin de prestation, de livraison….

L'objectif de ce document est de prendre connaissance du cadre juridique de la contractualisation électronique, des opportunités, des risques et des modèles de mises en œuvre en matière de sécurisation de la contractualisation électronique.

1 Cadre juridique de la contractualisation électronique

1.1 Introduction

La dématérialisation des procédures de contractualisation est une pratique en pleine expansion, portée par :

- Des besoins de simplification, d'accélération de la relation entre contractants ;
- Des besoins de générer des économies de traitement dans les BackOffice ;
- Un cadre juridique favorable et stable dans le temps.

Sur le plan juridique, une très grande majorité de pays modernes ont légiféré pour donner une valeur légale aux documents électroniques produits dans le cadre de procédures dématérialisés.

Ces législations sont par contre différentes en fonction des pays sur :

- Leur niveau de détail (principe soumis à appréciation du juge ou description précise des règles à respecter pour donner un caractère original à un document électronique) ;
- Le vocabulaire retenu et les définitions précises des termes utilisés ;
- Le niveau d'exigences qu'elles induisent.

1.2 Textes transverses encadrant la signature électronique

1999 (Europe) : Directive Européenne 1999/93/CE

2000 (France) : Loi n°2000-230 du 13 mars et Article 1316-4 du Code civil en découlant:

- Présomption de fiabilité de la signature électronique
- Renversement de la charge de la preuve (charge à celui qui conteste une signature électronique)

2001 (France) : Décret n° 2001-272 du 30 mars : conditions d'application de la loi, définition des termes…

- Niveaux de signature électronique (simple, sécurisée et présumée fiable)
- Dispositif sécurisé électronique de création de signature
- Dispositif de vérification de signature électronique

- Certificat électronique qualifié pour la signature présumée fiable
- Prestataires de services de certification électronique (P.S.C.E.)

2002 (France) : Arrêté du 31 mai 2002 précisant le décret n°2001-272

- Le COFRAC est chargé d'accréditer les organismes d'évaluation pour l'obtention du statut de P.S.C.E.
- L.S.T.I. est la seule société accréditée à ce jour dans ce schéma
- L'accréditation est accordée pour une durée de deux ans (renouvelable).
- La reconnaissance de la qualification des P.S.C.E. est soumise à un audit effectué par l'un des organismes accréditée par le COFRAC, et à ses frais.

2003 (Europe) : Commission du 14 juillet 2003 (2003/511/CE) établissant les normes reconnues au niveau européen pour les signatures électroniques pour…

- Produits de signatures électroniques (HSM) : CWA 14167-1 et CWA 14167-2
- Dispositifs sécurisés de création de signatures électroniques (SSCD) : CWA 14169

2004 (France) : Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (L.C.E.N.) complétant l'ensemble du dispositif

- Articles 1108-1 et 1108-2 du Code civil : reconnaissance de l'écrit électronique pour la validité des contrats
- Articles 1369-1, 1369-2 et 1369-3 du Code civil : formalités à suivre pour les professionnels exerçant une activité de commerce électronique
- Article L. 121-20-3 du Code de la consommation : responsabilité des professionnels exerçant une activité de commerce électronique
- Article L. 33-4-1 du Code des postes et télécommunications et Article L. 121-20-5 du Code de la consommation : définition et encadrement de la publicité électronique

2004 (France) : Arrêté du 26 juillet : complète l'arrêté du 31/05/2002, relatif à l'accréditation des organismes qui procèdent à l'évaluation des P.S.C.E.

- Définition du référentiel d'accréditation - norme NF EN 45012 (pour L.S.T.I. ou équivalent) ;
- En annexe :
    - La norme AFNOR AC Z74-400 (*ETSI 101 456*) devient la norme de référence en vue de reconnaître la qualification des P.S.C.E.
    - l'arrêté complète cette norme avec une série d'exigences techniques supplémentaires

De nombreux textes sectoriels référencent ce corpus juridique, pour « confirmer » les possibilités de dématérialisation dans des activités spécifiques.

1.3 Transposition dans le domaine de l'Administration

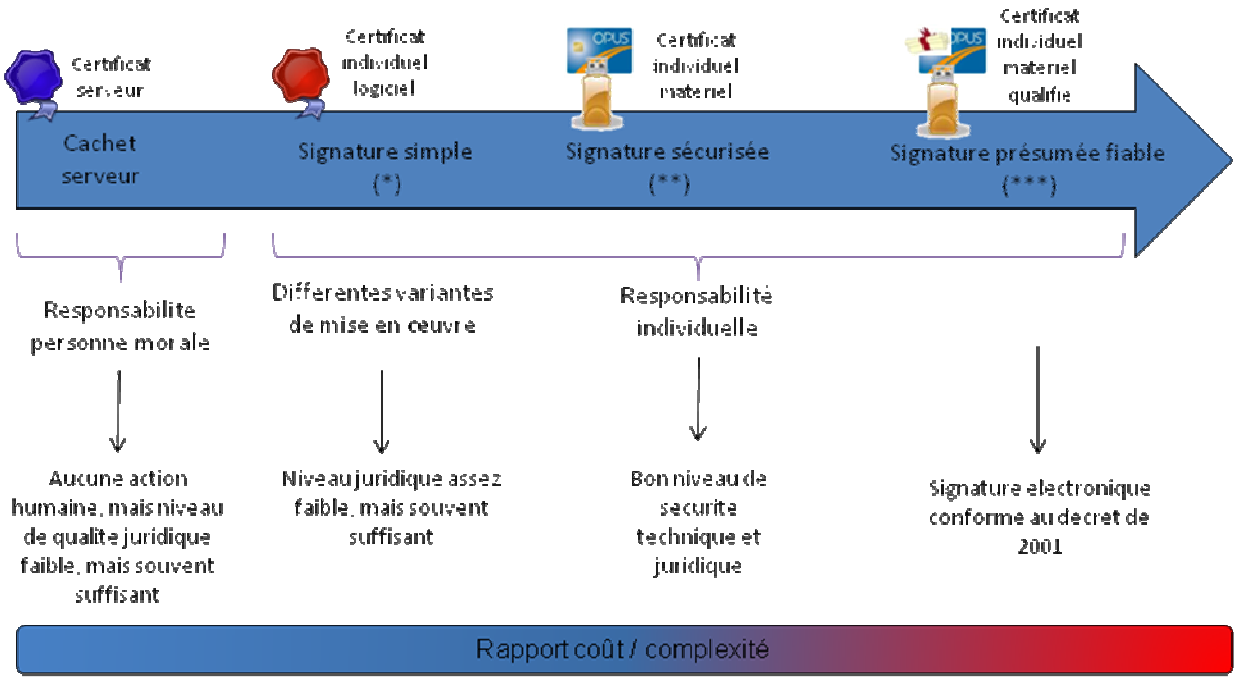
2005 (France) : Ordonnance n°2005-1516 du 8 décembre 2005, relative aux échanges [...] entre les autorités administratives

- Texte fédérateur relatif aux métiers de la dématérialisation dans la sphère publique rédigé par l'ADAE (maintenant DGME) et définissant la notion de « téléservice »
- Définit les principes de R.G.S. (Référentiel Général de Sécurité) et R.G.I. (Référentiel Général d'Interopérabilité)
- « Annule et remplace » les termes « LRAR » par « signature électronique » par exemple
- Promulgue positivement les effets de la signature électronique dans TOUS les échanges administratifs

2010 (France) : Décret n° 2010-112 du 2 février 2010, dit « décret R.G.S. » (Référentiel Général de Sécurité)

- Définit les règles et exigences de sécurité, qui s'appliquent aux autorités administratives, et aux systèmes d'information qui communiquent avec elles, selon plusieurs niveaux de « force sécuritaire » : une, deux ou trois étoiles (*, **, ***)
- Définit un ensemble de règles de sécurité pour la gestion de la sécurité de l'information
- Référence un ensemble de documents annexes définissant la marche à suivre pour émettre des certificats suivant…
    - Le type : Particulier, Entreprise, Administration, **Serveur**
    - Le service : Authentification, Signature, Confidentialité, Horodatage
    - Le niveau : *, **, ***

1.4 Synthèse : différents types de signature électronique, pour différentes valeurs juridiques



Le niveau de qualité de la signature est dépendant du type et du niveau de sécurité du certificat.

1.5 Le Règlement européen

1.5.1 Règlement Européen : Origines et objectifs

La Commission Européenne a entrepris de réformer la directive européenne sur la signature électronique datant de 1999 et de la refondre sous forme de règlement.

Ce règlement sera imposé à tous les États membres à compter de sa parution sans avoir à être transposé à chaque État membre.

Objectifs du Règlement Européen :

- Accélérer la transition vers la dématérialisation en évitant les problèmes d'interopérabilité,
- Accroître la sécurité juridique en donnant des règles simples et claires de reconnaissance mutuelle entre les services de confiance des différents Etats membres.

1.5.2 Règlement Européen : les services de confiance

De nouveaux services de confiance ont été créés. Le Règlement Européen couvre désormais les services de confiance suivants :

- L'identification électronique,
- La signature électronique **(simple, avancée, qualifiée)**,
- Les services de validation de signature ***NEW***,
- Le cachet serveur ***NEW***,
- L'horodatage ***NEW***,
- Les « services de fourniture électronique » qui désignent la transposition électronique du courrier recommandé ***NEW***,
- La conservation électronique,
- L'authentification de site web (certificat SSL) ***NEW***,

1.5.3 Règlement Européen : résumé des dispositions

L' « identification électronique »

- chaque État membre notifie à la Commission Européenne la liste des systèmes d'identification électronique qu'il délivre en son nom ou sous sa responsabilité.
- la responsabilité porte sur l'univocité du système et sur la possibilité de vérification de l'identité électronique (authentification),
- les dispositions entreprises dans le règlement sont clairement en faveur du certificat,

La « signature électronique »

- Comme dans la directive, la signature qualifiée est une signature avancée qui repose sur un **dispositif de sécurisé de création de signature** et un **certificat qualifié**.
- Le **certificat qualifié** ne nécessite plus forcément un face-à-face. La vérification de l'identité d'un titulaire peut se faire à distance à l'aide d'un **moyen d'identification électronique notifié**. Les règles de transitivité du RGS deviennent caduques.
- Le « **dispositif de création de signature** » : cet aspect est peu développé et renvoie à de futurs actes délégués. Même si elle n'est pas obligatoire, la Commission incite à la **certification** des dispositifs puisque sera publiée une liste des dispositifs certifiés.
- Affirmation plus claire du principe de reconnaissance mutuelle de la signature qualifiée par les États membres.

Le « **service de validation de signature** » :

Le Règlement Européen introduit le métier d'intermédiation pour la validation de signature qualifiée uniquement.

Le « **cachet serveur** » :

La notion de signature qualifiée de personne morale est enfin affirmée et les règles de reconnaissance mutuelle s'appliquent comme pour la signature qualifiée.

L' « **horodatage** » :

L'horodatage électronique qualifié est affirmé et les règles de reconnaissance mutuelle s'appliquent comme pour la signature qualifiée. La présomption de fiabilité porte sur l'intégrité et la date.

Le « **service de lettre recommandée électronique** » :

Un tel service permet de donner une preuve d'envoi et de réception de données. Pour être qualifié (présomption de fiabilité sur l'intégrité et la date d'envoi et de réception), le service doit être opéré par un prestataire de service de confiance qualifié.

La « **conservation électronique** » :

Le Règlement Européen introduit le métier de « tiers-archiveur ».

Le « **certificat serveur SSL** » :

Le Règlement Européen introduit un certificat SSL qualifié sans plus de précision.

1.5.4 Règlement Européen : Ce qu'il faut retenir

Le Règlement Européen a pour objectif :

- D'accélérer le passage à la dématérialisation,
- De forcer l'interopérabilité entre les États membres,

Le Règlement Européen fait apparaître plusieurs nouveautés :

- Clarification des pratiques relatives à la signature électronique,
- Renforcement des obligations de reconnaissance mutuelle entre les services de confiance des différents pays membres,
- Création de nouveaux services de confiance,

1.6 Le décret « R.G.S. »

Le décret fixe les règles auxquelles les S.I. mis en place par les **autorités administratives** doivent se conformer pour assurer la sécurité des informations échangées,

- **confidentialité** des données échangées

- **intégrité** des données
- **disponibilité** des services
- **intégrité** des systèmes d'information
- **identification** de leurs utilisateurs

La conformité d'un produit de sécurité et d'un service de confiance à un niveau de sécurité donné peut être attestée par une **qualification R.G.S.**

Pour protéger son S.I., l'organisation concernée doit…

- Procéder à une analyse de risques
- Fixer les objectifs de sécurité, pour couvrir ces risques
- **En déduire les fonctions de sécurité et leur niveau qui permettent d'atteindre ces objectifs.**

En conséquence, les utilisateurs des téléservices doivent se doter de moyens de sécurité adaptés aux choix des Autorités Administratives (et leurs fournisseurs faire qualifier ces moyens vis à vis du bon niveau cible, au moins).

Le décret définit la procédure administrative de demande de qualification

- pour un fournisseur de produits et services de sécurité
- pour un Prestataire de Service de Confiance (définition du P.S.C.O., dont la couverture fonctionnelle est potentiellement plus large que le P.S.C.E.)

Le décret définit également les conditions de garantie du niveau de sécurité dans le temps

- La qualification est valable pour une durée maximale de trois ans
- La qualification s'obtient sur la base d'un audit, réalisé en deux temps (au minimum)
  - Audit documentaire
  - Audit terrain (techniques & procédures)
  - (optionnellement) pré-audit amont

Certificats électroniques & validation de certificats : l'A.N.S.S.I. met en place une procédure de validation des certificats électroniques délivrés aux autorités administratives ou à leurs agents

Le décret définit les pré-requis au référencement d'une offre de services ou d'un produit d'un P.S.C.O.

- Le référencement est postérieur à la qualification
- Le référencement vise l'interopérabilité, et la couverture fonctionnelle des produits et services, et va donc au-delà de la qualification

Les "autorités administratives" doivent se conformer au R.G.S.

- dans un délai de 3 ans pour les anciennes applications
- dès maintenant pour les nouvelles applications

1.6.1 L'arrêté R.G.S.

Le décret est complété par un arrêté, qui référence les documents « contenu du R.G.S. », intégrant

- Le RGS v1.0 (évolution de la version 0.99 avec simple changement de numéro de version)
- Les documents annexes : plusieurs dizaines de P.C. types et de documents d'exigences techniques.

RGS Annexes A

- « P.C. Types » pour les certificats (Authentification, Signature, Confidentialité, Authentification & signature, Authentification serveur / cachet)
- « P.H. Type » pour l'horodatage
- Fonctions de sécurité nécessaires pour ces différents mécanismes, et exigences de qualification, de conformité à des profils de protection de l'A.N.S.S.I.
- Variables de temps
    - Exigences de disponibilité
    - Exigences de continuité de service
    - Exigences de délais de prise en charge d'incidents
    - Exigences de durée d'archivage
    - Exigences de fréquence d'audit interne, de fréquence d'analyse des traces
    - Exigences de durée de vie des certificats, de fréquence de mise à jour des CRL
    - Exigences de délais de prise en compte de demande de révocation notamment

RGS Annexes B, règles et recommandations relatives…

- Au choix et au dimensionnement des mécanismes cryptographiques
- À la gestion des clés utilisées dans des mécanismes cryptographiques
- Aux mécanismes d'authentification

En cas d'évolution des documents annexes, seul l'arrêté sera à mettre à jour.

Informations utiles sur le R.G.S.

- Ordonnance du 8 décembre 2005 sur les téléservices http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&dateTexte=vig
- Décret « Référentiel Général de Sécurité » du 2 février 2010 http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000021779444&dateTexte=&oldAction=rechJO&categorieLien=id
- Arrêté « Référentiel Général de Sécurité » du 6 mai 2010 http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000022220429&dateTexte=&oldAction=rechJO&categorieLien=id
- Documents associés au R.G.S. : http://www.references.modernisation.gouv.fr/rgs-securite

1.6.2 Contenu du R.G.S. – Principes

Le R.G.S. reprend les principes contenus dans le décret et l'arrêté et les détaille.

Définition du terme « Autorité Administrative » (qui reste encore à préciser pour certains types de professionnels, et d'établissements publics, exerçant une obligation de service public par exemple).

Restriction du périmètre aux seules « Autorités Administratives » qui mettent en œuvre des systèmes d'information susceptibles d'échanger des informations avec d'autres A.A. ou avec des usagers.

Le R.G.S. impose d'intégrer la S.S.I. dans le cycle de vie des S.I. et des applications.

Le R.G.S. définit le principe « d'homologation de sécurité du système d'information » avant sa mise en production

- L'Autorité Administrative doit définir une « Autorité d'Homologation » et lui demander une « attestation formelle » pour valider l'homologation d'un S.I. (qui peut être refusée, ou accordée avec réserve)
- Le R.G.S. définit les outils utiles pour gérer la S.S.I. dans les applications métiers : la Fiche FEROS (fiches d'expression rationnelle d'objectifs de sécurité)

Le R.G.S. définit un cadre méthodologique pour bien gérer les problématiques S.S.I.

- Adopter une démarche globale : cohérence des moyens, des processus, des niveaux différents de sécurité physique et logique notamment

- Adapter la S.S.I. selon les enjeux : les moyens doivent être proportionnels aux risques et aux conséquences potentielles d'une défaillance ou de la survenance d'une menace
- Gérer les risques S.S.I. : de l'analyse de risques au plan d'action sécurité (EBIOS et ISO27005 recommandés)
- Élaborer une politique S.S.I. : recommandé
- Utiliser les produits et prestataires labellisés pour leur sécurité : recommandé ;
- Viser une amélioration continue : mise en place d'un système de management de la sécurité de l'information » (SMSI / ISO 27001 recommandé)

1.6.3 Contenu du R.G.S. – Fonctions de sécurité

Authentification client

- Authentification par mot de passe statique non recommandé
- *A minima*, vérifier la complexité du mot de passe, pour éviter qu'il soit trop facile à deviner
- Authentification d'un client par certificat électronique, sous réserve d'utiliser des certificats *, **, ou ***, servant à l'authentification ou à la signature (* et ** seulement pour les certificats double usage)
- Certificats délivrés par des P.S.C.E. exclusivement

Authentification serveur

- Authentification d'un serveur par certificat électronique, sous réserve d'utiliser des certificats *, **, ou ***, servant à l'authentification, et respectant les conditions d'émission fixées dans la *Politique de Certification Type authentification serveur*

Signature électronique

- Distinction entre signature électronique "personne physique" et "cachet serveur" (signature "personne morale", scellement de l'intégrité d'un flux)
- Signature électronique sur la base de certificats émis par des P.S.C.E., au niveau *, **, ou *** suivant les cas de figure
- Principe d'équivalence « automatique » entre un certificat RGS *** (personne physique) et un certificat permettant de produire des signatures « présumées fiables » (arrêté du 26 juillet 2004)

Confidentialité

- Idem. : utilisation de certificats *, **, ou ***, émis par un P.S.C.E., conformément à la *PC Type confidentialité*

1.6.4 Contenu du RGS – Horodatage et accusés de réception

Horodatage

- Définition du terme « P.S.H.E. » : Prestataire de services d'horodatage électronique
- Officialisation de la *Politique d'Horodatage Type*

Accusé de réception électronique

- Rappel des principes définis dans l'ordonnance du 8 décembre 2005 (accusé d'enregistrement et accusé de réception)
- Recommandations faites aux autorités administratives de…
    - Horodater ces accusés d'enregistrement et de réception
    - Les faire signer par un agent ou un serveur (cachet) de l'autorité administrative
    - Sauvegarder les accusés d'enregistrement et de réception tant que peuvent survenir d'éventuelles réclamations de la part des usagers
- Une fois de plus, les Autorités Administratives doivent déterminer le niveau de sécurité de leurs S.I. après analyse de risques, et déterminer le niveau de confiance requis (*, **, ***).

1.6.5 Équivalences avec les procédures européennes

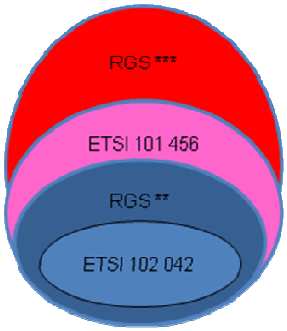
Le RGS est « heureusement » compatible avec les normes ETSI existantes, permettant d'attester de la qualité des infrastructures de confiance mises en œuvre

- *ETSI 102 042*
- *ETSI 101 456*

Certaines équivalences existent, mais leur réciproque n'est pas toujours vraie, compte tenu de certaines exigences RGS (notamment sur les variables de temps, et sur les matériels à utiliser dans le cadre de la mise en oeuvre des infrastructures de confiance)

Exemples

- Un référencement RGS ** permet d'obtenir un certificat de conformité *ETSI 102 042*
- Un référencement RGS *** permet d'obtenir un certificat de conformité *ETSI 101 456*
- Dans ces deux cas, la réciproque n'est pas automatique.



1.6.6 Ce qu'il faut retenir

Au travers de ces différents textes, la législation française et le cadre européen distinguent trois niveaux de validité juridique différents :

- la « signature électronique » ou « signature simple » (pas de moyen spécifique prédéterminé, en pratique un scellement technique est au moins nécessaire pour garantir l'intégrité de la transaction),
- La « signature sécurisée » (**),
- la « signature électronique présumée fiable » (***),

2 Opportunités, risques et modèles de mise en œuvre

2.1 Bénéfices de contractualisation électronique ou Opportunités

Les maîtres mots des bénéfices de la mise en œuvre d'une solution de contractualisation électronique sont les suivants :

- **Économies** (sur les fais postaux, sur les coûts de traitement « backoffice », sur les coûts de conservation),
- **Efficacité** (accélération des processus de décisions),
- **Évolutivité** (optimisation de nouvelles offres marketing et commerciales on line),
- **Développement** (amélioration de son positionnement marché, différenciation par rapport à la concurrence, développement durable),

La « contractualisation électronique » sécurisée permet:

- **d'optimiser le taux de conversion :**

  Pourcentage de clients aboutissant leur démarche par une contractualisation.

- **de réduire les frais d'impression, les frais postaux et les frais de déplacement**
- **d'accélérer les échanges :**

  Une telle solution permet à plusieurs contractants, géographiquement éloignés, de signer le même document en quelques minutes.

- **de simplifier les processus :**
  - de contractualisation,
  - de conservation des contrats,

  Par exemple : les contrats signés électroniquement peuvent être archivés au sein du SI de l'entreprise dans un environnement sécurisé.

- **de renforcer l'image :**

  Une société, mettant en œuvre une telle solution, verra son image renforcée auprès de ses clients (image de précurseur, …).

2.2 Les risques à appréhender : falsification - répudiation

La mise en œuvre d'une solution de contractualisation électronique doit prendre en compte les risques de falsification, de répudiation :

- le contractant peut, à posteriori, contester avoir signé ou donné son accord au document (cf. exemple – Jugement du TI d'Epinal du 12 décembre 2011).

- le contractant peut contester le contenu du contrat et préciser que le contenu avant signature est différent du contenu après signature.
- sans date de signature, le contractant peut contester la date d'exécution du contrat.

Pour réduire ces risques, la solution mise en place devra répondre aux exigences suivantes :

- Le consentement du contractant doit être effectué via une solution de signature **« fiable »** et non répudiable permettant d'identifier le contractant/signataire.
- Le contenu du contrat signé ne doit subir aucune modification.
- La date de signature doit apparaître sur le contrat et ne doit pas être contestable.

Le niveau de « fiabilité » attendu dépend du niveau de risque pris lors de la contractualisation…

L'évaluation et la gestion de ces risques doivent être étudiées méthodiquement. On procède alors à une « **analyse de risques** ».

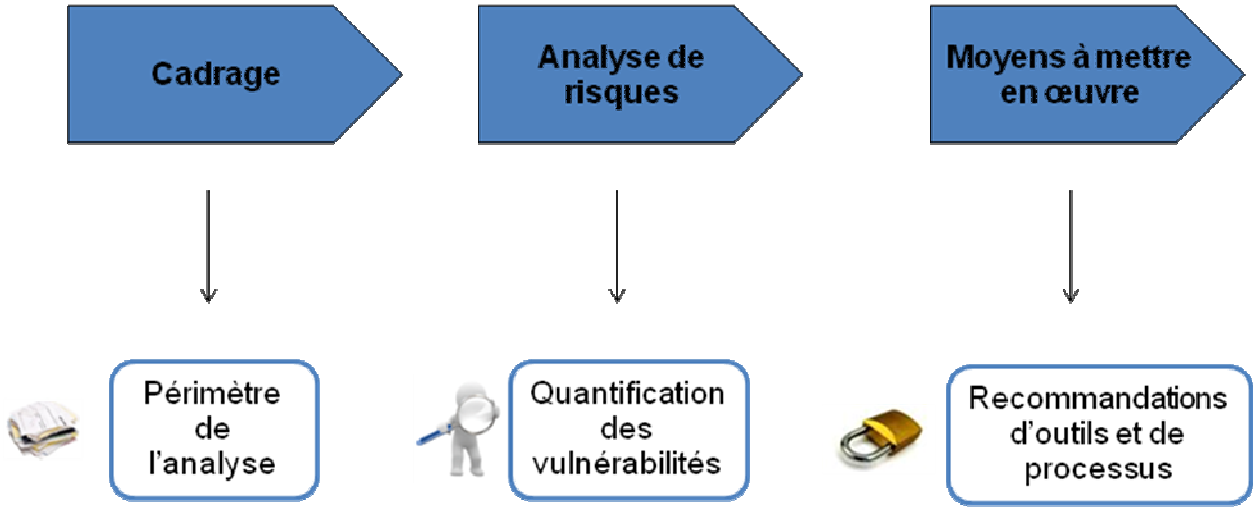
2.3 Analyse de risques

Dans ce contexte précis, une analyse de risques a pour objet d'obtenir une évaluation précise, méthodique et aussi exhaustive que possible des risques que représente la mise en œuvre d'une solution de contractualisation électronique.

La méthode utilisée consiste :

- en une recherche de l'ensemble des événements redoutés,
- leur évaluation en termes de conséquences et d'occurrence,
- puis la détermination des moyens de réduction des causes et/ou des conséquences possibles de ces événements en fonction des objectifs de réduction du risque à atteindre.

2.4 Principe de l'analyse de risques



FEROS : Fiche « objectifs de sécurité » faisant apparaître les risques couverts et les risques résiduels

2.5 Cadrage : Prérequis à l'analyse

2.5.1 ETAPE 1 - définition des parties prenantes et de leur rôle (exemple)

Parties Prenantes / Actions	**RAC** : Responsable du périmètre de l'étude ;	**RSSI-MOA** : Responsable définition des objectifs de sécurité	**MOE :** Responsable de la mise en œuvre	**RSSI-MOE**: Responsable mise en œuvre objectifs de sécurité	**USR** : utilisateurs
Objectif de l'analyse de risques	**R**	**A**	**C**	**C**	**I**
Contexte général	**R**	**C**	**C**	**C**	**C**
Périmètre de l'analyse	**R**	**A**	**C**	**C**	**I**
Paramètres à prendre en compte	**R**	**C**	**C**	**C**	**C**
Identification des sources de menaces	**R**	**A**	**C**	**A**	**C**

R : Responsable de la mise en œuvre de l'activité ;

A : Autorité légitime pour approuver l'activité ;

C : Contributeur ;

I : Informé des résultats de l'activité

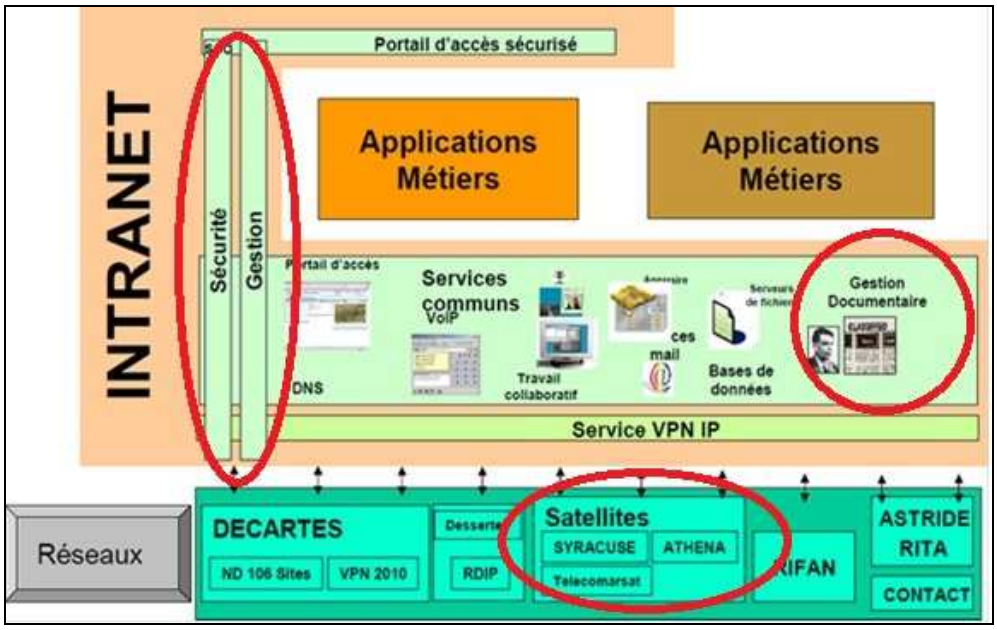
2.5.2 ETAPE 2 – Définition des métriques de l'analyse (exemple)

Echelle d'évaluation des besoins de sécurité				
Niveau	**Disponibilité**	**Intégrité**	**Confidentialité**	**Preuve**
4	Vital	Vital	Strictement Confidentiel	Critique
	Interruption jamais supérieure à « n » heures	Aucune altération de données ne doit être possible	L'accès doit être limité un nombre très restreint de personnes habilitées	Besoin de preuve opposable
3	Essentiel	Essentiel	Confidentiel	Essentiel
	Interruption jamais supérieure à « m » heures	Altération de données tolérable mais devant être détectée et corrigée immédiatement	L'accès doit être limité à des personnes habilitées	Besoin d'imputabilité des actions réalisées
2	Important	Important	Interne à l'entreprise	Important
	Interruption jamais supérieure à « o » heures	Une altération de données est tolérable si elle est détectée et corrigée *a posteriori*	Information pour laquelle une divulgation à l'extérieur serait inappropriée ou indélicate.	Besoin d'identification des actions
1	Faible	Faible	Public	Faible
	pas de taux de disponibilité précis	Aucune conséquence en cas d'altération de données	L'information est diffusable sans limitation	Il n'est pas nécessaire de tracer les accès

Echelle d'impacts					
Nature des conséquences / gravité	0	1	2	3	4
Perte financière	> 100 € < 1000 €	> 1000 € < 10 000 €	> 10 000 € < 100 000 €	>100 000 M€ < 1 Million €	> 1 Million €
Juridique			Remise en question des prérogatives de l'organisme	Condamnation civile	Condamnation pénale
Image	Quelques plaintes	Nombreuses plaintes	Impact client important	Altération sérieuse	Perte totale d'image

Echelle de potentialité					
Probabilité	0	1	2	3	4
	Très improbable	Peu probable	Possible	Probable	Très probable

2.5.3 ETAPE 3 – Identification des biens intervenants dans l'analyse (exemple sur la base du schéma d'architecture applicative)



- Numérotation de chaque bien (actif)
- Identification de son objectif
- Identification du type de bien (matériel, logiciel, humain…)

2.6 Analyse des risques

Ces informations permettent alors **d'étudier les risques** en établissant :

- La liste des menaces par bien identifié dans le périmètre
- La liste des événements redoutés
- Les potentialités d'occurrences des événements redoutés
- Les conséquences des menaces

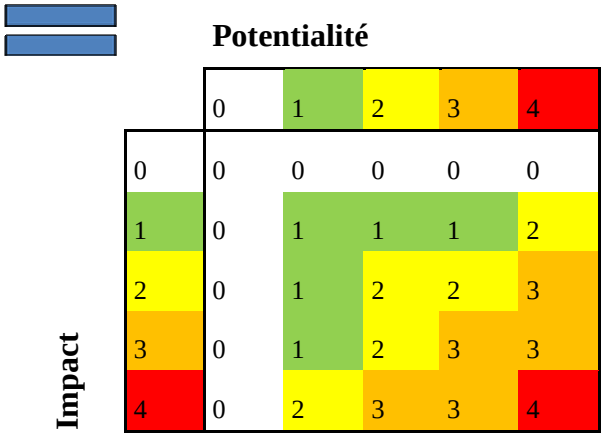
Ces résultats permettent alors de présenter **une matrice des risques** identifiant les risques (**dans l'absolu**)

Impact \ Potentialité	1	2	3	4
1				
2	Un opérateur d'enregistrement délégué utilise un badge d'identification non attribué	Impossibilité de renouveler un certificat		
3	Perte des secrets de l'AC empêchant la révocation du certificat de l'AC			Inscriptions d'information erronées dans la SIM vis-à-vis du certificat du porteur Impossibilité de révoquer un certificat Un certificat révoqué n'apparaît pas dans la CRL Un opérateur décide de saisir des demandes de certificats pour son usage personnel
4		Génération d'un certificat suite à la saisie de mauvaises informations		

2.7 Méthode de calcul du risque

Echelle de potentialité				
0	**1**	**2**	**3**	**4**
L'évènement ne peut pas arriver	L'évènement n'est jamais arrivé et à peu de chances d'arriver	L'évènement n'est jamais arrivé mais pourrait arriver	L'évènement est déjà arrivé occasionnellement	L'évènement est déjà arrivé régulièrement

Echelle d'impacts					
Nature des conséquences / gravité	**0**	**1**	**2**	**3**	**4**
Perte financière	> 100 € < 1000 €	> 1000 € < 10 000 €	> 10 000 € < 100 000 €	>100 000 M€ < 1 Million €	> 1 Million €
Juridique			Perte de la qualification RGS	Condamnation civile	Condamnation pénale
Image	Quelques plaintes	Nombreuses plaintes	Impact client important	Altération sérieuse	Perte totale d'image
Secret	Faille confidentielle	Accès aux secrets depuis les infrastructures internes	Accès aux secrets depuis l'équipement mobile du porteur	Publication en clair des secrets	Modification des secrets privés du certificat du porteur



2.8 Moyens à mettre en œuvre

Au final l'analyse permet de présenter les **mesures à mettre en œuvre (ou déjà mises en œuvre)** pour couvrir les risques et faire ressortir **les risques résiduels** que devra prendre le porteur du projet

Risque	**Niveau**	**Mesures à prendre (ou déjà mises en œuvre)**	Envisagé (E) Effectué (X)	Résiduel
Impossibilité de révoquer un certificat	3	Prévoir un second site d'hébergement des services de l'IGC	X	0
Un certificat révoqué n'apparaît pas dans la CRL	3	Prévoir un second site d'hébergement des services de l'IGC	X	2
Un opérateur décide de saisir des demandes de certificats pour son usage personnel	3	Appliquer des audits récurrents sur plusieurs points de vente pour s'assurer	E	3
Génération d'un certificat suite à la saisie de mauvaises informations	2	Améliorer les interfaces de présentation du certificat pour informer le porteur des données contenues dans son certificat	X	1
Perte des secrets de l'AC empêchant la révocation du certificat de l'AC	1	Séparer les secrets entre l'AC et l'OSC et les stocker dans des endroits physiquement séparés	X	0
Inscriptions d'information erronées dans la carte vis-à-vis du certificat du porteur	1	Faire qualifier la carte au niveau renforcé	X	0
Un opérateur d'enregistrement délégué utilise un badge d'identification non attribué	1	Délivrer des badges nominatifs personnels aux opérateurs d'enregistrement délégués		1
Impossibilité de renouveler un certificat	1	Prévoir un second site d'hébergement des services de l'IGC		1

2.9 Ce qu'il faut retenir

Seule une analyse de risques permet de déterminer « objectivement » les moyens à mettre en œuvre pour couvrir les risques de falsification, de répudiations identifiées.

D'autres risques peuvent également être identifiés dans le cadre de l'analyse (sur les « axes » traçabilité, confidentialité), et peuvent nécessiter la mise en œuvre de moyens complémentaires

Cette démarche est également un moyen de communication efficace pour fédérer les visions de différentes directions (juridique, DSI, MOA) qui n'ont souvent pas la même compréhension des moyens à mettre en œuvre pour sécuriser la contractualisation électronique.

2.10 Modèles de mise en œuvre

Aujourd'hui, la « contractualisation électronique » est déclinée sous les modèles suivants :

Par internet,

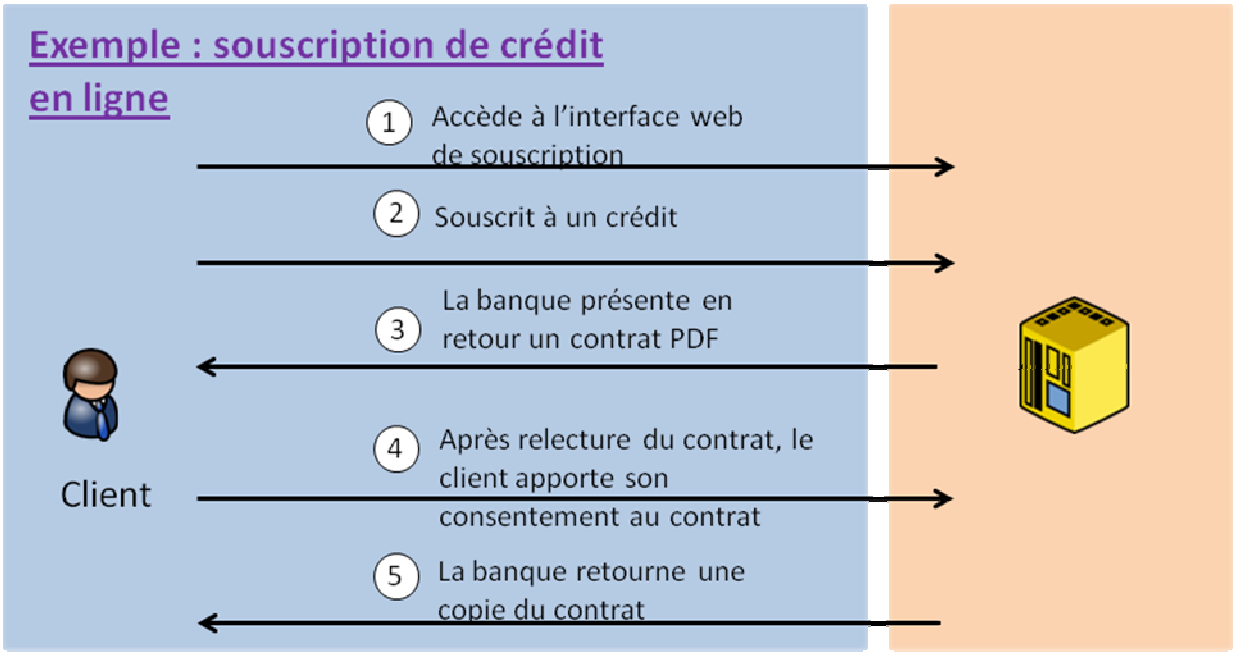
En agence,

- Sur appareil nomade (exemple : tablette),

Les cas d'usages sont multiples et ont lieu :

- En BtoC,
- En BtoB,
- Voire BtoA,

2.11 Modèle de mise en œuvre : Souscription par internet



Avantages :

- Ce modèle permet au contractant d'effectuer sa démarche à distance,
- Aucun agent pour la souscription n'est requis à priori,

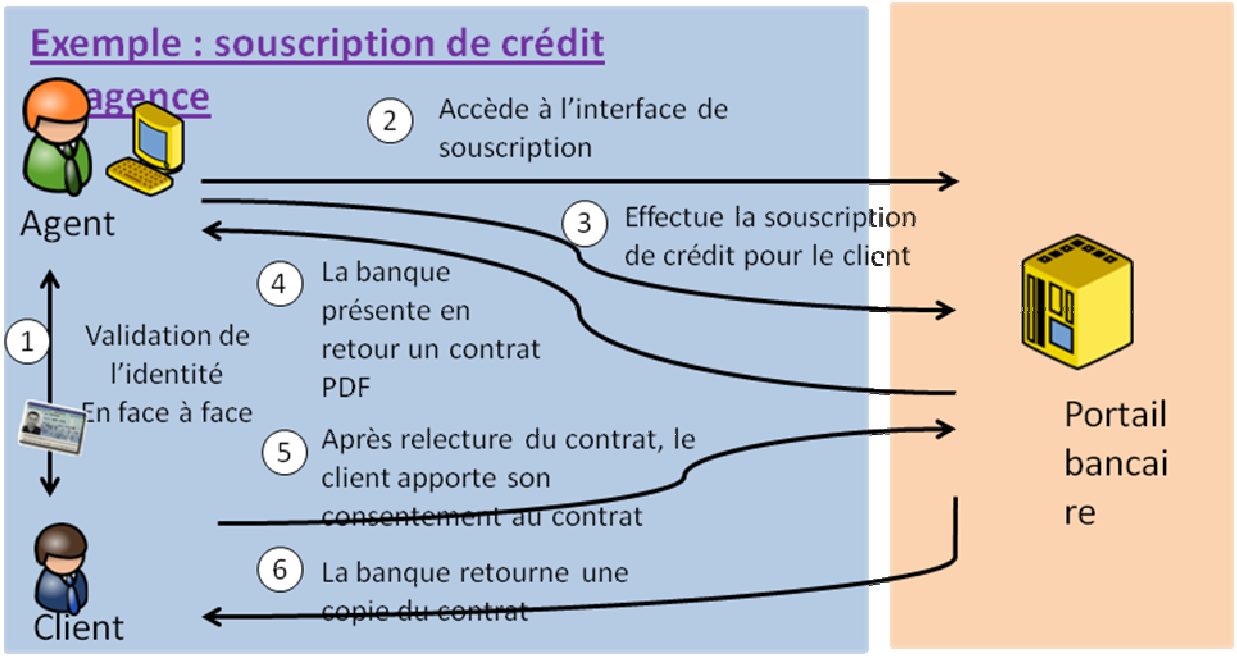
Inconvénients :

- L'absence de face-à-face ne permet pas de garantir l'identité réelle du prospect.

Remarques :

- Le type de certificat fourni au contractant dans ce modèle dépendra des enjeux (politiques, financiers, …) et de la criticité du contexte.

2.12 Modèle de mise en œuvre : Souscription en agence



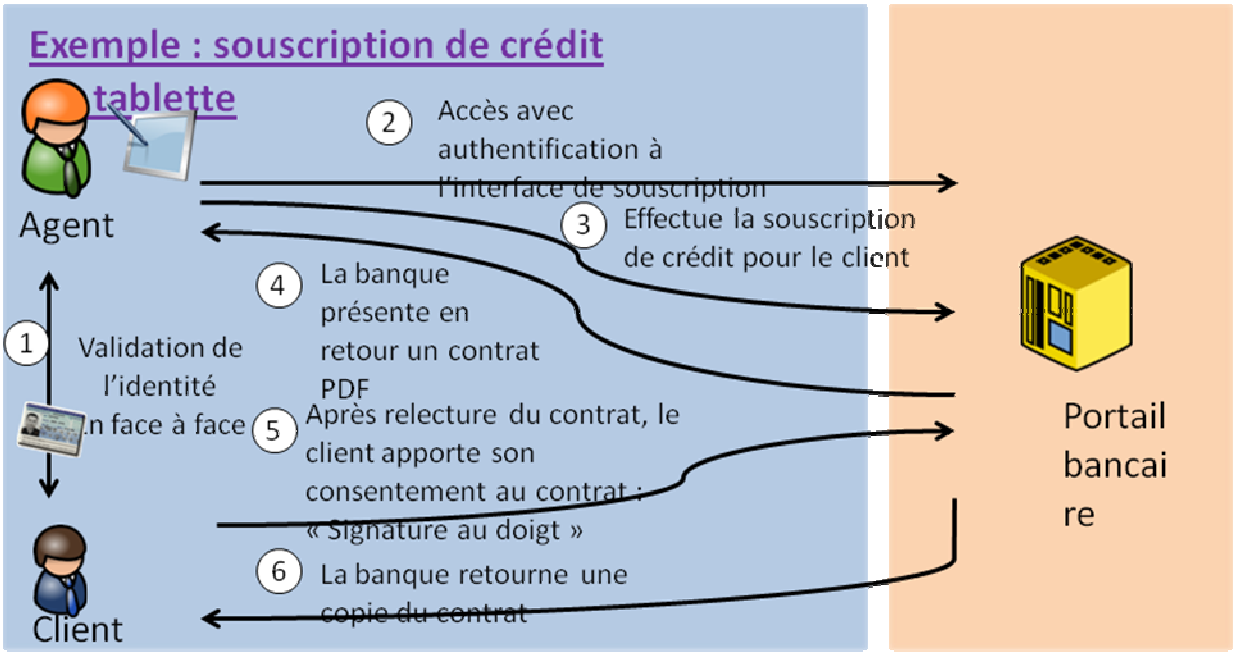
Avantages :

- L'identité du contractant est clairement validée suite au face-à-face avec présentation d'une pièce d'identité,

Inconvénients :

- Un agent doit être dépêché pour chaque souscription,
- Le contractant doit se déplacer physiquement pour effectuer sa souscription,

2.13 Modèle de mise en œuvre : Souscription sur tablette



Avantages :

- L'identité du contractant est clairement validée suite au face-à-face avec présentation d'une pièce d'identité,
- L'agent peut avoir un comportement « nomade » et effectuer des souscriptions en dehors de son bureau d'enregistrement,
- Le processus de « signature graphique » est un atout psychologique majeur dans l'acceptation d'une contractualisation électronique par le contractant,

Inconvénients :

- Un agent doit être dépêché pour chaque souscription,
- Pour des raisons techniques, il est difficile de délivrer et d'utiliser un certificat sur tablette.

2.14 Variantes des modèles de mises en œuvre

Ces différents modèles de mise en œuvre sont, en général, déclinés de façon particulière selon l'organisme souhaitant déployer sa solution de contractualisation électronique.

En fonction du contexte, des enjeux et des moyens, une adaptation de ces modèles est envisageable sur les plans :

- Technique

  Exemple : pour la contractualisation sur internet, l'authentification du contractant peut s'établir de diverses méthodes (récupération d'informations déclaratives, OTP, certificat, etc …)

La signature « manuscrite » (image) peut être récupérée ou non en fonction des choix de mise en œuvre.

- Organisationnel

Exemple : des processus métiers peuvent être ajoutés dans la cinématique de contractualisation (fourniture de pièces scannées par le contractant, etc …).

- Juridique

Compte tenu de la spécificité possible sur les plans technique et organisationnel, le référentiel documentaire, dont le détail sera abordé plus loin, doit être adapté.

2.15 Validation d'une stratégie de signature électronique

Compte tenu du cadre légal et du principe de signature électronique reposant sur l'utilisation d'un certificat électronique, il convient d'identifier les critères de décision d'une stratégie de contractualisation électronique :

- Le volume de signatures

Exemple : en dessous de 100 signatures/an, la mise en œuvre d'une solution n'est pas nécessaire.

- La fréquence des signatures

En fonction de la fréquence, les signataires seront équipés d'un certificat à usage unique ou d'un certificat permanent.

- La connaissance des signataires

Pour des signataires connus et en nombre limité, la fourniture d'un certificat permanent est pertinente,

Pour des signataires inconnus (visiteurs du site), la fourniture d'un certificat temporaire est préférable,

- La propension à contester la signature

Le contractant sera plus sujet à contester le contenu du contrat que la signature elle-même.

- Les enjeux en cas de contestation de la signature

En fonction des enjeux financiers (valeur des contrats gérés), la stratégie de contractualisation sera différente.

2.16 Conclusion

Quelque soit le modèle de mise en œuvre, la « contractualisation électronique » se doit d'être **sécurisée** et doit respecter la réglementation française et européenne. Par conséquent elle a besoin d'embarquer une solution permettant :

- d'identifier le contractant,

Pour éviter toute usurpation d'identité,

- Au contractant de conclure le contrat via un processus de signature « fiable » au regard des risques,

Pour que le contractant marque son engagement et pour garantir la non-répudiation,

- d'empêcher l'altération du contrat,

Pour garantir l'intégrité du document signé,

- d'apposer une date sur le contrat,

Pour garantir la date d'exécution du contrat,

- d'archiver le contrat et les preuves de l'engagement,

Pour le fournir comme preuve le cas échéant,