

# Politiques de Sécurité achatpublic.com Annexes

Version 1.0

1	<i>Introduction</i>	2
2	<i>Glossaire</i>	2
3	<i>Bibliographie</i>	4

# 1 Introduction

Le présent document constitue une annexe aux Politiques de Sécurité d'achatpublic.com.

Il comporte un glossaire des termes techniques employés et une bibliographie des ouvrages de référence cités dans ces Politiques de Sécurité.

## 2 Glossaire

**AES** : Advanced Encryption Standard. C'est un algorithme à clef secrète.

**Autorité de Certification (AC ou CA)** : Elle définit la politique de certification et la fait appliquer. N'importe quelle organisation peut se déclarer autorité de certification pour ses utilisateurs. Elle utilise sa propre clef privée pour créer les certificats qu'elle délivre. Cette autorité de certification peut elle-même être certifiée par une autre autorité.

**Autorité d'enregistrement (AE)** : Il s'agit de l'organisme auquel s'adresse l'utilisateur pour obtenir son certificat et ses clefs. Celui-ci vérifie la validité et l'authenticité de la demande et la transmet à l'Opérateur de Certification.

**Bi-clef** : couple de clefs cryptographiques, composé d'une clef privée (devant être conservée secrète) et d'une clef publique, nécessaire à la mise en œuvre d'opérations de cryptographie basées sur des algorithmes asymétriques.

**Certificat** : document électronique contenant la clef publique d'un Porteur de Certificat, ainsi que certaines autres informations attestées par l'Autorité de Certification qui l'a délivré. Un Certificat contient des informations telles que :

- l'Identité du Porteur de Certificat,
- la clef publique du Porteur de Certificat,
- la durée de vie du Certificat,
- l'Identité de l'Autorité de Certification qui l'a émis,
- la signature de l'Autorité de Certification qui l'a émis.

Un format standard de Certificat est normalisé dans [RFC 3280].

**Chiffrement de données** : procédé cryptographique par lequel on rend des données inaccessibles à quiconque sauf à leur destinataire légitime.

**Clef de service** : Nom donné globalement à la bi-clef et au certificat permettant le chiffrement et le déchiffrement au sein du service Salle des Marchés d'achatpublic.com.

**Clef Publique** : Quantité numérique, attachée à une ressource ou un individu, qui la distribue aux autres afin qu'ils puissent lui envoyer des données chiffrées ou déchiffrer sa signature.

**Clef Privée** : Quantité numérique secrète attachée à une ressource ou à un individu, lui permettant de déchiffrer des données chiffrées avec la clef publique correspondante ou d'apposer une signature au bas de messages envoyés vers des destinataires.

**Common Name (CN)** : élément du champ 'subject' du certificat comportant l'identité du Porteur de Certificat

**Composante de l'ICP** : plate-forme constituée d'au moins un poste informatique, une application, un moyen de cryptographie et jouant un rôle déterminé au sein de l'ICP.

**Distinguished Name, DN** : nom distinctif X.500 du Porteur de Certificat pour lequel le Certificat est émis. Il constitue le champ subject du certificat et identifie le porteur de manière unique au sein de l'AC.

**Données d'Activation** : données connues du Porteur de Certificat uniquement lui permettant de mettre en œuvre sa clef privée.

**Génération d'un Certificat** : action réalisée par une Autorité de Certification et qui consiste à signer le gabarit d'un Certificat édité par une Autorité d'Enregistrement, après avoir vérifié la signature de l'Autorité d'Enregistrement.

**Identité** : ensemble des informations définissant un individu (nom, prénom(s)) ou une entité (dénomination).

**IETF** : Internet Engineering Task Force. Communauté internationale en charge de la définition des standards employés sur Internet.

**Infrastructure à Clef Publique (ICP) ou Public Key Infrastructure (PKI)** : ensemble de composantes, fonctions et procédures dédiés à la gestion des clefs et de Certificats utilisés par des services basés sur la cryptographie à clef publique.

**Liste de Certificats Révoqués (LCR) ou Certificate Revocation List (CRL)** : liste comprenant les numéros de série des Certificats ayant fait l'objet d'une Révocation, signée par l'AC émettrice.

**Object Identifier (OID)** : identifiants uniques enregistrés au niveau international, dont l'utilisation est standardisée.

**Opérateur de Certification** : entité chargée d'exploiter l'ICP pour le compte de l'Autorité de Certification.

**Politique de Certification (PC)** : ensemble de règles, définissant les exigences auxquelles l'Autorité de Certification se conforme pour l'émission de Certificats adaptés à certains types d'applications.

**Porteur de Certificat** : personne physique ou morale qui dispose de l'usage légitime du certificat et de la bi-clef associée.

**Renouvellement d'un Certificat** : opération effectuée à la demande d'un Porteur de Certificat, en fin de période de validité d'un Certificat, qui consiste à générer un nouveau Certificat.

**Request For Comments (RFC)** : document de spécification publié par l'IETF.

**Révocation d'un Certificat** : opération demandée par le Porteur de Certificat, par une AC ou une AE, et dont le résultat est la suppression de la garantie de l'AC sur un Certificat donné, avant la fin de sa période de validité. La demande peut être la conséquence de différents types d'événements tels que la compromission d'un bi-clef, le changement d'informations contenues dans un Certificat, etc.

**RSA** : Rivest-Shamir-Adelman : algorithme de signature à clef publique.

**SHA-1** : Secure Hash Algorithm Number 1. SHA est un algorithme de hachage

**Utilisateur de Certificat** : toute entité qui utilise le Certificat d'un Porteur de Certificat, par exemple pour chiffrer des données à l'attention du Porteur du Certificat.

### 3 Bibliographie

- [RFC 1305]** RFC de l'IETF définissant « Network Time Protocol (Version 3) ».  
<http://www.ietf.org/rfc/rfc1305.txt?number=1305>
- [RFC 2560]** RFC de l'IETF définissant « X.509 Internet Public Key Infrastructure / Online Certificate Status Protocol - OCSP »  
<http://www.ietf.org/rfc/rfc2560.txt?number=2560>
- [RFC 2630]** RFC de l'IETF définissant « Cryptographic Message Syntax »  
<http://www.ietf.org/rfc/rfc2630.txt?number=2630>
- [RFC 3161]** RFC de l'IETF définissant « Internet X.509 Public Key Infrastructure / Time-Stamp Protocol (TSP) »  
<http://www.ietf.org/rfc/rfc3161.txt?number=3161>
- [RFC 3280]** RFC de l'IETF définissant « Internet X.509 Public Key Infrastructure / Certificate and Certificate Revocation List (CRL) Profile »  
<http://www.ietf.org/rfc/rfc3280.txt?number=3280>
- [Code civil]** Articles 1316 à 1316-4 du Code civil  
<http://www.legifrance.gouv.fr/WAspad/UnCode?code=CCIVILLO.rcv>