Politique de certification

Version	0.2
Date	18 Décembre 2012
Rédigé par	Ambroise Ismael Kabore
Relu par	Julien Legras
Approuvé par	

MISES À JOUR

Version	Date	Modifications réalisées
0.1	16/12/2012	Création
0.2	18/12/2012	Après relecture par Julien

Table des matières

1 Introduction

1.1 Présentation générale

Le groupe F du Master professionnel 1 SSI (2012-2013), dans le cadre de son projet annuel doit étudier et réaliser un outil de chat sécurisé. L'objectif de ce projet est d'étudier les protocoles cryptographiques permettant à plusieurs utilisateurs de s'authentifier et de communiquer de manière sécurisée à travers un outil de messagerie instantanée.

1.2 Identification

Ce document est la politique de certification du chat sécurisé Bavardage et est identifié par le nom Bavardage-pc.

1.3 Autorités, applications et groupes d'utilisateurs concernés

1.3.1 Autorité administrative (AA)

Composante de l'IGC qui définit et fait appliquer les politiques de certification et les déclarations des pratiques de certification par la PKI, ainsi que la politique de sécurité générale de la PKI.

1.3.2 Autorité de certification (AC)

C'est l'autorité à laquelle les utilisateurs font confiance pour émettre et gérer des clés,des certificats, et des révocations. L'AC est gérée par l'administrateur du serveur sécurisé du chat.

1.3.3 Autorité d'enregistrement (AE)

Une autorité d'enregistrement est une composante de l'Infrastructure de Gestion des Clés qui vérifie les données propres au demandeur de certificat ainsi que les contraintes liées à l'usage d'un certificat, conformément à la politique de certification. Elle assure le lien entre l'Autorité de Certification et les utilisateurs.

1.3.4 Autorité de dépôt (AD)

C'est l'autorité qui stocke les certificats numériques ainsi que les listes de révocation.

1.3.5 Utilisateur demandeur (UD)

C'est la personne physique ayant directement par la loi ou par délégation, le pouvoir de demande de certificat portant le nom du chat et du signataire de la convention.

1.3.6 Utilisateur Final (UF)

C'est la personne physique qui utilise les certificats. C'est en général les utilisateurs du chat.

1.3.7 Utilisateur signataire convention (USC)

C'est la personne physique ayant directement par la loi ou par délégation, le pouvoir de signer les conventions passées avec Bavardage. Tous les certificats porteront le nom du chat et le nom du signataire de la convention passée bavardage.

1.3.8 Type d'applications concerné

L'usage des certificats doit permettre l' identification et l'authentification d'un utilisateur Bavardage décline toute responsabilité pour tout usage de certificat qui serait sans rapport avec le chat.

1.4 Points de contact

1.4.1 Autorité de sécurité compétente dans l'accréditation des composants d'une PKI

À compléter

1.4.2 Personnes à contacter concernant ce document Sans objet

1.4.3 Personnes habilitées à déterminer la conformité de la DPC avec la politique de certification

Les personnes habilitées à déterminer la conformité de la DPC avec la politique de certification sont nommées par l'Autorité Administrative(AA).

2 Dispositions d'ordre générale

2.1 Obligations

Les obligations suivantes sont communes à toutes les composantes de la PKI : Protéger sa clé privée et ses données d'activation en intégrité et en confidentialité. N'utiliser ses clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, en vertu de la présente politique. Respecter et appliquer la PC. Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles l'entité concernée s'engage.

2.1.1 Obligations des acteurs

Autorité Administrateur	– Valider la politique de certification – Établir la conformité entre la PC et la DPC
Autorité d'enregistrement	– Respecter la législation relative au respect des données d'identification personnelles – Publier un formulaire de demande de certification. – Vérifier l'exactitude des mentions qui établissent l'identité du demandeur et de l'entreprise. – Si elle est saisie d'une demande de révocation, elle doit en vérifier l'origine et l'exactitude. – Traiter les demandes de certificat. – Conserve et protège en confidentialité et intégrité toutes les données collectées lors de la demande de certificat. – Doit se soumettre à tout contrôle technique et audits que pourrait demander l'AA.
Autorité de certification	– S'engager à diffuser publiquement la politique de certification, la liste des certificats révoqués, et la liste des certificats auxquels la clé racine de l'IGC est subordonnée. – Documenter les schémas de certification qu'elle entretient avec d'autres AC ou d'autres PKI. – Respecter le résultat d'un contrôle de conformité et remédier aux non conformités qu'il révèle – Documenter ses procédures internes de fonctionnement. – Respecter la PC et appliquer la DPC. – Doit se soumettre à tout contrôle technique et audits que pourrait demander l'AA.
Utilisateur Demandeur	– Il doit respecter la convention avec le chat bavardage et la PC – Il doit procéder sans délais aux révocations en cas de perte ou compromission des clés privées.
Utilisateur Final	– Se conformer aux règles de la présente politique de certification. – Respecter les conditions d'utilisation des clés et certificats, et protéger ceux-ci. – A défaut de remplir cette obligation il assume seul tous les risques de ses actions non conformes aux exigences de la présente politique.

2.1.2 Responsabilité des acteurs

Autorité Administrateur	– Résolution des litiges
Autorité d'enregistrement	– Enregistrement d'une demande en provenance des utilisateurs (UD). – Conservation et protection en confidentialité et en intégrité des données personnelles d'identification transmises pour l'enregistrement. – Seule l'AC peut mettre en cause la responsabilité de l'AE, ce qui exclut explicitement tout engagement de l'AE envers les utilisateurs demandeurs ou finaux.
Autorité de certification	– Génération des certificats dans le cadre des procédures définies dans la PC et DPC. – Assure la responsabilité du service de publication, elle est responsable de l'information des utilisateurs des procédures à suivre tout au long du cycle de vie des certificats.
Utilisateur Demandeur	– Il réalise les opérations de demande et révocation de certificats.
Utilisateur Final	– Il est responsable de la sécurité de son poste de travail.

2.1.3 Interprétation de la loi

- Loi Suivant la législation nationale : Les données à caractère personnel d'une personne physique doivent être protégées suivant la loi ... À compléter
- Résolution de litiges Sans objet

2.1.4 Publication et Services associés

- Publication d'informations sur la PKI
  Les informations concernant la PKI publiées sont les suivantes :
  - La Politique de certification (PC)
  - La liste des certificats révoqués(LCR)
- Fréquence de publication
  Les informations seront publiées suivant un temps T
- Service de publication
  L' AC rend un service de publication des certificats qui se matérialisera par un annuaire. Ce service de publication met à disposition des utilisateurs suivant TEMPS=TempDispoPub les informations suivantes :

- les informations concernant la PKI
- la liste des certificats révoqués

2.1.5 Politique de confidentialité

- Type d'informations considérées comme confidentielles
  Cas des informations confidentielles à caractère secret (obligation de discrétion). Il s'agit d'informations nécessaires au bon fonctionnement de la PKI :
  - clés privées propres à la composante concernée
  - Politique de Certification
  - Archives des conventions cryptographiques
  - La DPC

  Cas des informations confidentielles à caractère privatif (exigence de séclusion). Il s'agit d'informations nécessaires à l'opérabilité de l'IGC : données personnelles d'identification nominative d'un utilisateur demandeur (identifiants nominatifs), les utilisateurs demandeurs disposent d'un droit d'accés, de rectification et d'opposition à la cession de toute information les concernant.

- Type d'informations considérés comme non confidentielles
  Les informations publiées sur la PKI (cf. 2.1.4) sont considérées comme non confidentielles.

- Délivrance aux autorités légales
  les autorités légales peuvent réclamer l'identité de l'individu ou de l'organisme qu'il représente. En aucun cas, le recouvrement de clé de signature ni de clé de certification ne doit être effectué.

- Délivrance à la demande du propriétaire
  Les informations relatives à un utilisateur final et définies comme confidentielles en 2.1.6 ne peuvent être divulguées qu'à leur propriétaire (demandeur du certificat).

3 Identification et authentification

3.1 Enregistrement initial

3.1.1 Convention de noms

Le nom de l'Abonné figure dans le champ "Nom de l'organisation" du certificat au format X.509. Cette mention est obligatoire. Il est constitué du prénom usuel et du nom patronymique. Ce nom est celui de l'Abonné tel qu'il figure dans les documents d'État Civil.

3.1.2 Nécessité d'utilisation de noms explicites

Les informations portées dans les champs du certificat CA Certificat sont décrites ci-dessous de manière explicite :

- Pays : le code du pays sur 2 lettres
- Mot de passe : requis pour la signature
- Password : confirmation du mot de passe

- État ou nom de province :
- Localité : la ville
- Nom de l'organisation : Nom de l'entreprise ou de la personne
- Unité organisationnelle : département
- Adresse eMail : Adresse électronique de l'abonné

3.1.3 Règles d'interprétation des différentes formes de nom

Ces informations sont établies par le groupe de projet et reposent essentiellement sur les règles suivantes :

- Tous les caractères sont sans accents ni caractères spécifiques à la langue française ;
- les prénoms et noms composés sont séparés par des tirets « - ».

3.1.4 Unicité des noms

L'unicité d'un certificat est basée sur l'unicité de son numéro de série au sein de l'AC.

3.1.5 Procédures de résolution des litiges sur la revendication d'un nom

Lorsque le nom à inclure dans un certificat provoque un litige avec un autre utilisateur, l'autorité d'enregistrement à qui la demande de certification a été formulée proposera une procédure de résolution amiable du litige.

3.1.6 Preuve de la possession d'une clé privée

Génération du bi-clé par le demandeur et utilisation d'un protocole adapté.

3.1.7 Authentification de l'identité d'un individu

Seul l'utilisateur demandeur (UD) est authentifié. L'authentification de l' UD est réalisée lors de la procédure de connexion au serveur sécurisé du chat.

3.2 Re-génération de certificat

Les certificats sont à renouveler suivant un temps T = temps de validité du certificat. L'utilisateur demandeur refait une nouvelle demande de certificat. Un certificat révoqué ne peut pas être régénéré.

3.3 Authentification d'une demande de révocation

L'authentification d'une demande de révocation est effectuée par l'Autorité d'Enregistrement. Sont demandés :

- le nom du demandeur,
- le prénom du demandeur,
- le motif de révocation,
- l'adresse électronique de l'Abonné.

4 Besoins opérationnels

4.1 Demande de certificat

Elle se déroule en deux temps :
- L'utilisateur demandeur remplit le formulaire de demande de création d'un compte sécurisé.
- Après réception du formulaire, l'AC traite la demande, génère le certificat et l'envoi à l'utilisateur demandeur qui devient un utilisateur final.

4.2 Génération de certificat

- l'UD transmet une demande de certificat conformément au 4.1.
- L'autorité d'enregistrement vérifie la validité des informations portées par le formulaire de demande
- Si le formulaire est valide, il est transmis à l'AC qui génère le certificat, le transmet à l'utilisateur demandeur et le stocke dans l'autorité de dépôt.
- En cas de non validité des informations un message avec le motif du rejet est envoyé à l'utilisateur demandeur.

4.3 Acceptation d'un certificat

Sans réponse à l'envoi du certificat à l'UD. Envoyé par l'AC, il est considéré comme accepté par l'UD qui reconnaît de fait les termes et les conditions d'utilisations et assume les responsabilités liées à son utilisation. L'acceptation d'un certificat vaut acceptation de la PC en référence.

4.4 Suspension et révocation d'un certificat

4.4.1 Causes possibles de révocation d'un certificat

Les causes de révocation du certificat d'une AC peuvent être :
- Compromission, suspicion de compromission, vol, perte de certificat.
- Compromission de clé publique d'une AC
- Compromission, suspicion de compromission, vol, perte de la clé privée d'une AC
- Non respect de la politique de certification ou de la déclaration des pratiques de certification.
- Décision suite à un contrôle de conformité.
- Cessation d'activité de l'AC.

Les causes possibles de révocation du certificat d'un utilisateur final sont les suivantes :
- Compromission, suspicion de compromission, vol ou perte de la clé privée de l'utilisateur final.
- Compromission, suspicion de compromission, vol ou perte du certificat de l'utilisateur final
- Compromission de clé publique de l'utilisateur final.
- Révocation du certificat de l'AC émettrice du certificat.
- Non respect du contrat ou de la convention liant un utilisateur final à la PKI.
- Changement d'informations contenues dans le certificat (changement de fonctions de l'utilisateur, changement de nom, etc.)

4.4.2 Publication des causes de révocation

Elles ne sont pas publiées.

4.4.3 Contrôle de la Liste de révocation

Les utilisateurs finaux sont autorisés à consulter la liste de révocation.

4.4.4 Personnes habilitées à demander une révocation

Les personnes habilitées à demander une révocation sont :
- L'AC
- L'AE
- L'AA
- Le serveur de chat sécurisé

4.4.5 Procédure de demande de révocation

La demande de révocation se fait soit en envoyant un mail à l'AA, soit en remplissant un formulaire qui sera envoyé à l'AE.

4.4.6 Temps de traitement d'une révocation

Les demandes de révocation doivent être traitées suivant un temps T = temps de révocation.

4.4.7 Fréquence de mise à jour de la liste des certificats révoqués

L'AC garantit aux utilisateurs de ses certificats la mise à disposition d'une liste de certificats révoqués à jour suivant un temps T = fréquence mise à jour liste de révocation.

4.5 Journalisation

4.5.1 Types d'événements enregistrés

Les opérations réalisées sur la PKI seront enregistrées.

4.5.2 Fréquence de traitement des journaux d'événement

Le processus de journalisation enregistre en temps réel les opérations effectuées, le contournement du processus n'est pas possible.

4.5.3 Durée de rétention d'un journal d'événements

Les journaux doivent être conservés pour une période minimale T = temps rétention journal d'événements.

4.5.4 Copie de sauvegarde des journaux d'événements

Des copies de sauvegardes des journaux d'événements doivent être faites suivant un temps T = temps sauvegarde journaux d'événements. Les archives de journaux d'événements sont protégés au même niveau que les journaux d'événements originaux.

4.5.5 Imputabilité

L'imputabilité d'une action revient à la personne, ou le système l'ayant exécutée et dont le nom figure dans le champ « nom de l'exécutant » du journal d'événements.

4.6 Archives

4.6.1 Type de données à archiver

Les données à archiver sont au moins les suivantes :
- Certificats d'utilisateurs (2 ans).
- Liste de révocation (2 ans).
- Données relatives à la demande de certificats (2 ans).
- Les notifications (messages, etc) (2 ans).
- Les journaux d'événements (2 ans).

4.6.2 Période de rétention des archives

Les archives sont conservées pendant un temps T = temps conservation archive.

5 Contrôle de sécurité physique et des procédures

5.1 Contrôle physique

Pas concerné(Nous ne construirons pas de sites pour la PKI).

5.2 Contrôle des procédures

5.2.1 Rôle

On distingue un unique administrateur.

5.2.2 Nombre de personnes nécessaire à chaque tâche

Pas de spécification

5.2.3 Identification et authentification

La connexion d'un exploitant à la PKI nécessite son identification, identification à laquelle est associée son rôle au sein de la PKI.

6 Contrôles techniques de sécurité

6.1 Génération et Délivrance de clé

6.1.1 Génération de bi-clé

L'UD génère lui-même sa bi-clé. l'AC décline toute responsabilité pour une utilisation autre que celle définie dans la PC, y compris pour l'authentification et l'identification mutuelle de deux UF.

6.1.2 Génération de clé privée

Pas concerné(Le serveur de chat sécurisé génère les clés privées dans notre cas).

6.1.3 Délivrance de clé privée

Pas concerné(Le serveur de chat sécurisé génère les clés privées dans notre cas).

6.2 Protection de clé privée

Pas concerné (Le serveur de chat sécurisé génère les clés privées dans notre cas).

7 Profils des certificats et listes des certificats révoqués

7.1 Profil de certificat

Les certificats utilisés sont les certificats X.509 v3.

Version	Numéro de version du certificat
Serial number	Numéro de série du certificat
signature	Identifiant de l'algorithme de signature de l'AC
Issuer	Nom de l'AC
Validity Period	Période de validité
Subject	Nom de l'entité
Subject public key info	Identifiant de l'algorithme d'usage de la clé publique contenue dans le certificat, et valeur de la clé publique
Issuer unique identifier	Identification unique de l'AC
Subject unique identifier	Identifiant unique de l'entité
Extensions	Les extensions sont soit standardisées, soit à la discrétion de l'autorité de certification

7.2 Profil de liste de révocation

Version	Numéro de version de la liste de révocation
Signature	Identifiant de l'algorithme de signature de l'AC
Issuer	Nom de l'AC qui signe les certificats
ThisUpdate	Date de génération de la liste de révocation
NextUpdate	Prochaine date à laquelle cette Liste de révocation sera mise à jour
RevokedCertificates	liLte des numéros de série des certificats révoqués, contenant les champs suivants : – userCertificate : Numéro de série du certificat révoqué – revocationDate : Date à laquelle le certificat a été révoqué
CrlExtensions	liste des extensions de la LCR : – authorityKeyIdentifier : identifiant de la clé publique de l'AC qui a signé la liste de révocation – CRLNumber : numéro de série de la liste de révocation

8 Administration et spécification

8.1 Procédure de modification de ces spécifications

Toute modification jugée par l'administrateur de l'AC comme pouvant entraîner une perte de la conformité d'un certificat avec la politique de certification ou avec la DPC doit être approuvée par l'Autorité administrative.

8.2 Politiques de publication et de notification

l'AC avertit les UF des modifications apportées aux spécifications par courrier électronique.

8.3 Procédures d'approbation des DPC

L'approbation d'une DPC est confiée à l'Autorité administrative qui vérifie l'adéquation de la DPC fournie avec la politique de certification.

Acronymes

AA	Autorité Administrative
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AD	Autorité de Dépôt
UD	Utilisateur Demandeur
UF	Utilisateur Final
USC	Utilisateur Signataire Convention
PC	Politique de Certification
DPC	Déclaration des Pratiques de Certification
PKI	Public Key Infrastructure
IGC	Infrastructure de Gestion de clés
LCR	Liste de Certificats Révoqués

Documents applicables et de référence

- RFC 2527
- Livre Blanc : "Les PKI : Vers une Infrastructure Globale de Sécurité ?"
- PAMPC1 (Politique de Certification : Grand Port Maritime de Marseille)