



Master 1 Sécurité des systèmes informatiques

Rapport de projet : Chat sécurisé

Rédigé par	Charles Ango, Ismael Kabore, Julien Legras, Yves Nouafo, Jean-Baptiste Souchal
À l'attention de	Magali Bardet
Date de rendu	24 mai 2013

Introduction

Table des matières

Introduction	i
1 Présentation du projet	1
1.1 Besoins du client	1
1.2 Solutions proposées	1
1.2.1 Structure du logiciel	2
1.2.2 Détail de la couche sécurisée	3
1.2.3 Choix des langages	4
1.3 Résultat	4
1.3.1 Partie non-sécurisée	4
1.3.2 Certification	5
1.3.3 Partie sécurisée	8
1.4 Problèmes rencontrés	8
2 Manuel d'utilisation	9
2.1 Récupération du projet	9
2.1.1 En ligne de commande	9
2.1.2 En ligne	9
2.2 Compilation	9
2.2.1 Dépendances Ubuntu	9
2.2.2 Compilation des sources	9
2.3 Exécution	9
A Documents de gestion de projet	11
B Déclaration des pratiques de certification	13
B.1 Introduction	13
B.1.1 Contexte Général	13
B.1.2 Délégation d'autorité d'enregistrement	13
B.1.3 Souscripteur	13
B.2 Pré requis pour les demandes	13
B.2.1 Enregistrement d'un souscripteur	13
B.2.2 Vérification	13
B.3 Pratiques et procédures	14
B.3.1 Demande de certificats	14

B.3.2	Validation des demandes	14
B.3.3	Révocation des certificats	14
B.3.4	Expiration	14
B.3.5	Renouvellement	14
B.4	Conservation et Protection des données	14
C	Politique de certification	17
C.1	Introduction	17
C.1.1	Présentation générale	17
C.1.2	Identification	17
C.1.3	Autorités, applications et groupes d'utilisateurs concernés	17
C.1.4	Points de contact	18
C.2	Dispositions d'ordre générale	18
C.2.1	Obligations	18
C.3	Identification et authentification	21
C.3.1	Enregistrement initial	21
C.3.2	Re-génération de certificat	22
C.3.3	Authentification d'une demande de révocation	22
C.4	Besoins opérationnels	22
C.4.1	Demande de certificat	22
C.4.2	Génération de certificat	23
C.4.3	Acceptation d'un certificat	23
C.4.4	Suspension et révocation d'un certificat	23
C.4.5	Journalisation	24
C.4.6	Archives	24
C.5	Contrôle de sécurité physique et des procédures	25
C.5.1	Contrôle des procédures	25
C.6	Contrôles techniques de sécurité	25
C.6.1	Génération et Délivrance de clé	25
C.7	Profils des certificats et listes des certificats révoqués	25
C.7.1	Profil de certificat du CA	25
C.7.2	Profil de certificat d'un utilisateur	25
C.7.3	Profil d'entité	26
C.7.4	Profil de liste de révocation	26
C.8	Administration et spécification	26
C.8.1	Procédure de modification de ces spécifications	26
C.8.2	Politiques de publication et de notification	26
C.8.3	Procédures d'approbation des DPC	26

Chapitre 1

Présentation du projet

Dans le cadre de notre projet, il nous a été demandé de réaliser un chat sécurisé. Pour le mener à bien, le travail a été découpé en deux grandes phases qui sont l'analyse des besoins du client et les solutions proposées.

1.1 Besoins du client

Les besoins du logiciel sont les points indispensables, nécessaires et imposés par le client. Ce sont ces exigences qui détermineront les fonctionnalités du logiciel. Dans notre sujet, on le résume de la manière suivante :

Étudier les protocoles cryptographiques permettant à plusieurs utilisateurs de s'authentifier et de communiquer de manière sécurisée à travers un outil de messagerie instantanée.

À la fin du développement, l'outil de messagerie instantanée devra répondre aux besoins de la garantie que les messages soient échangés entre utilisateurs, de la preuve de la mise en place du système de sécurité ainsi que les protocoles déployés pour parvenir à la fin du développement.

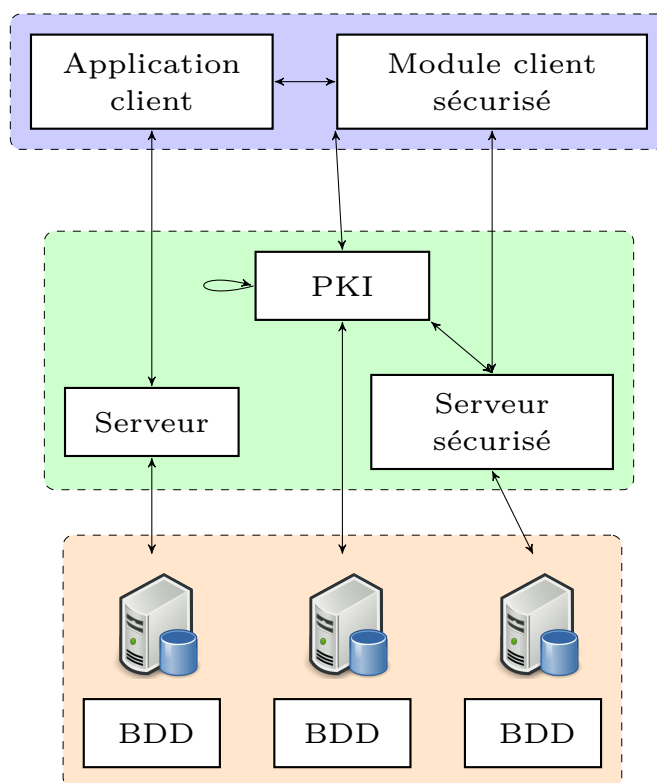
1.2 Solutions proposées

À l'issue de l'analyse des besoins du client, il a été convenu de traiter sa demande en décomposant la réalisation du logiciel en trois phases de développement.

- **Phase 1** : Mise en place du système de bavardage modèle client-serveur ;
- **Phase 2** : Installation d'une PKI (infrastructure de clés publiques) ;
- **Phase 3** : Mise en place d'une couche sécurisée pour permettre une communication chiffrée.

1.2.1 Structure du logiciel

Le logiciel est conçu et pensé de manière modulaire de tel sorte que chaque partie puisse être utilisée de manière indépendante. Son architecture se présente ainsi :



Sur le schéma précédent on voit bien la séparation de la partie logicielle de la partie sécurisée, mais aussi les différentes couches qui interviennent dans le développement du logiciel. Ces couches sont la partie logicielle, la partie réseaux et la partie base de données.

La partie logicielle met en place le côté client de l'application. Elle comporte deux modules qui sont l'application cliente et le module client sécurisé. L'application cliente permet à l'utilisateur de pouvoir communiquer avec d'autres utilisateurs de manière non sécurisée. Ce qui veut dire que chaque message pourra être lu par tout utilisateur présent dans un salon. Quant au module client sécurisé, il permet d'établir une communication sécurisée entre plusieurs utilisateurs. Une communication sécurisée masque le message à tout utilisateur n'étant pas destinataire du message en question.

Cette partie implémente les principales fonctionnalités suivantes :

- création d'un compte sécurisé ;
- envoi de message sur salon privé ;
- envoi de message sur salon général ;
- rejoindre un serveur de chat sans authentification ;
- quitter un serveur de chat ;
- envoi d'un message privé non sécurisé ;

- créer un salon privé ;
- joindre un salon privé ;
- fermeture d'un salon privé.

La partie réseaux est décomposée en trois éléments qui sont le serveur, le serveur sécurisé et la PKI. Chacun de ces éléments ont un rôle bien définis et tous distincts.

Le rôle du serveur est de distribuer les messages aux destinataires.

Le rôle du serveur sécurisé est de distribuer les clés symétriques permettant le chiffrement et le déchiffrement des messages des utilisateurs sécurisés.

La PKI est une autorité de confiance qui permet d'établir l'authenticité et l'identité d'un utilisateur sécurisé. Nous avons opté pour une pki déjà existante EJBCA qui remplira les fonctionnalités suivantes.

- ajout certificat à un utilisateur ;
- révocation d'un certificat ;
- renouvellement des clefs des salons privés.

La partie base de données décrit les données manipulées et utilisées par l'application. L'application en possède trois.

La première permet la gestion des utilisateurs non sécurisés. Cette base de données est rattachée au serveur non sécurisé. Elle est non persistante, ce qui veut dire que lors de la fin de l'utilisation du logiciel par un utilisateur, celui-ci ne sera pas conservé en base. Cette base a pour rôle de lister tout utilisateur déjà présent sur le service de chat.

La seconde permet la gestion des utilisateurs sécurisés. Contrairement à la première, cette base est persistante car tout utilisateur sécurisé pourra se reconnecter au service de chat autant de fois qu'il le souhaite.

La dernière permet le stockage des certificats générés par la PKI. Ces certificats définissent l'identité d'un utilisateur et sont stockés dans une base de données interne à l'application EJBCA.

1.2.2 Détail de la couche sécurisée

La couche sécurisée contient le module sécurisé, la PKI, le serveur sécurisé et la base de données qui lui est jointe. Cette couche est nécessaire pour échanger et garantir l'échange des messages sécurisés sans que celui-ci ne puisse être lu par un autre utilisateur. Pour mettre en place cette partie, on utilise la bibliothèque OpenSSL pour assurer la mise en place d'un canal de communication sécurisé entre deux utilisateurs sécurisés.

Comme dit ci-dessus, la PKI, autorité de confiance, permettra de garantir et d'identifier les utilisateurs présents sur le système de chat. On a aussi vu précédemment quel rôle joue le serveur sécurisé. Toute la mise en œuvre ainsi décrite permet de garantir un système de chat respectant les normes et les exigences du client.

Pour se rassurer que l'application fournie respecte bien les exigences du client, l'application implante des exigences fonctionnelles que l'on peut retrouver dans le cahier de recette, ou on peut voir les différents tests garantissant la mise en place de la couche sécurisée.

1.2.3 Choix des langages

Le choix des langages pour réaliser le projet sont le C pour la réalisation du serveur non sécurisé et du serveur sécurisé ainsi que des client, sécurisé et non sécurisés.

La réalisation de la base de données embarquée s'est faite en sqlite.

La partie graphique quant à été faite en Vala, car ce langage s'exporte en C très facilement.

Pour la partie sécurisé on a choisi la bibliothèque OpenSSL pour les raisons vues ci-dessus.

1.3 Résultat

Le résultat a été réparti en trois livraisons dont voici les contenus.

1.3.1 Partie non-sécurisée

La première partie consistait en le développement d'un client et d'un serveur de chat. Dans cette partie, les fonctionnalités ayant été développées sont :

- se connecter à un serveur de chat ;
- créer, rejoindre et quitter un salon de chat ;
- envoyer des messages privés aux utilisateurs connectés sur le serveur ;
- se déconnecter d'un serveur de chat.

Pour la communication entre les clients et le serveur, une structure C a été mise en place :

```
typedef struct {  
    int code;  
    char sender[MAX_NAME_SIZE];          // MAX_NAME_SIZE = 64  
    char content[MAX_MESS_SIZE];         // MAX_MESS_SIZE = 512  
    char receiver[MAX_ROOM_NAME_SIZE];   // MAX_ROOM_NAME_SIZE = 64  
} message;
```

Chaque action est représentée par un code (CONNECT, CREATE_ROOM, MESSAGE...). Le champ `sender` représente l'émetteur du message, `receiver` le destinataire. Enfin le champ `content` contient le(s) argument(s) associé(s) à l'action souhaitée. Côté client, pour envoyer une telle structure, il suffit d'appeler la fonction `int send_message(const char *mess, char **error_mess)` avec `mess` de la forme : `"/<ACTION> <ARGS>"` et `err_mess` le message d'erreur, si une erreur survient. L'affichage de message reçu se fait à la couche supérieur, dans l'interface graphique ou en lignes de commandes en appelant la fonction `int receive_message(message *m)`. Ces fonctions se trouvent dans une librairie écrite pour le client (`libclient.a`) afin de les utiliser dans l'interface graphique et en préparation à la surcouche sécurisée de la troisième livraison.

L'interface du client de chat a été développée en Vala à l'aide de la bibliothèque graphique GTK. La fenêtre a été dessinée à l'aide de Glade qui est un User Interface Designer produisant un fichier `.xml`, ce dernier étant utilisé dans le code Vala.

Côté serveur, les clients sont gérés dans des fils d'exécution séparés. Chaque message reçu est filtré selon son code d'action et le traitement correspondant est effectué. Si la connexion avec un client est perdue, le fil d'exécution s'arrête en déconnectant l'utilisateur.

1.3.2 Certification

La seconde livraison consistait en la mise en place d'une infrastructure à clefs publiques (PKI). Pour cela nous avons utilisé EJBCA (Enterprise Java Bean Certificate Authority) qui est une application utilisant un serveur JBoss. L'installation s'est faite en quelques étapes :

Récupération de JBoss et d'EJBCA

```
$ wget http://sourceforge.net/projects/jboss/files/JBoss/JBoss-5.1.0.GA/jboss-5.1.0.GA-jdk6.zip
$ wget http://sourceforge.net/projects/ejbca/files/ejbca4/ejbca_4_0_10/ejbca_4_0_10.zip
$ unzip jboss-5.1.0.GA-jdk6.zip
$ unzip ejbca_4_0_10.zip
```

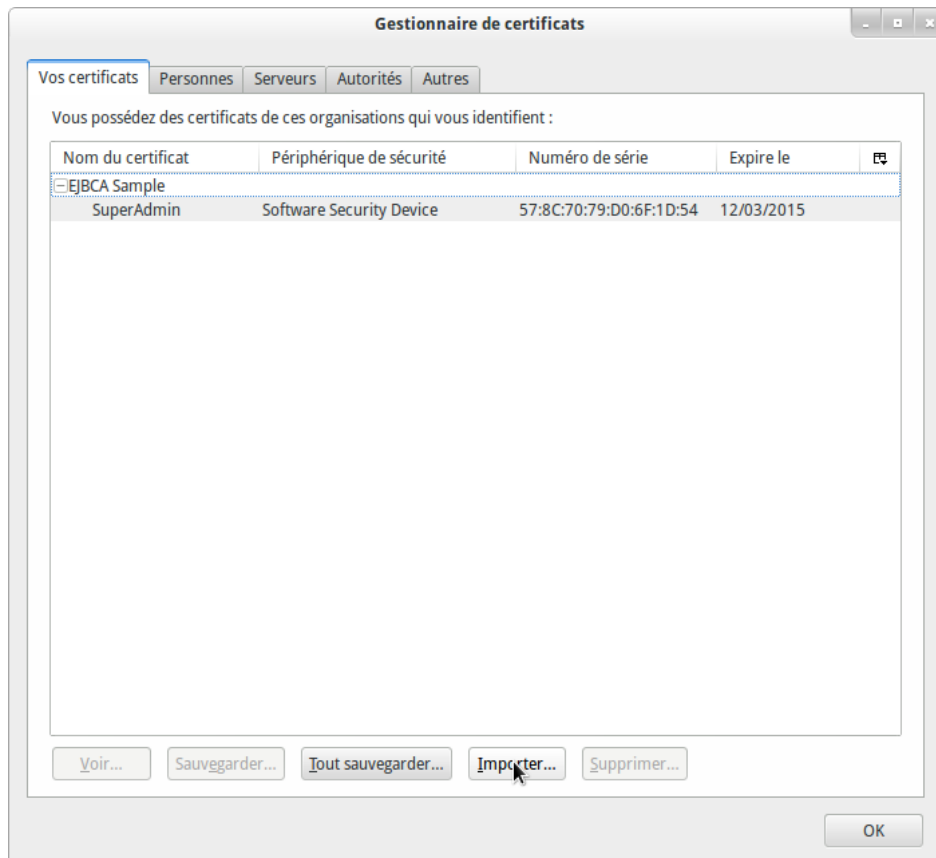
Configuration et construction d'EJBCA

```
$ echo "appserver.home=/home/user/jboss-5.1.0.GA" >> ejbca_4_0_10/conf/ejbca.properties
$ cd ejbca_4_0_10; ant bootstrap
```

Installation et déploiement d'EJBCA

```
$ /home/user/jboss-5.1.0.GA/bin/run.sh &
$ ant install
$ ant deploy
```

Pour la configuration des autorités de certification et des différents profils, EJBCA met à disposition une interface web. Il faut tout d'abord récupérer le certificat administrateur qui a été généré lors de l'installation se trouvant dans `/home/user/ejbca_4_0_10/p12/superadmin.p12` puis de l'ajouter dans les certificats du navigateur comme suit (Firefox) :



On peut alors accéder à la partie administration à partir de l'adresse :
`https://adresse_serveur:8443/ejbca/adminweb/index.jsp`

La page obtenue est la suivante :

EJBCA Administration - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils Aide

EJBCA Administration

https://192.168.56.101:8443/ejbcadminweb/index.jsp

EJBCA Administration

Version : EJBCA 4.0.10 (r14333)

Bienvenue SuperAdmin sur le portail d'administration d'EJBCA.

Nom d'hôte du nœud : bavardage-server
Date et heure du serveur : 2013-04-10 11:46:34+02:00

État de santé des AC [?]

Nom de l'AC	Service AC	Statut LCR
AdminCA1	✓	⚠
CABavardage	✓	✓

Statut des files d'attente de publication [?]

Service de publication	Long.
BAVARDAGE_PUBLISHER	0

Développée par PrimeKey Solutions AB, 2002-2012.

Fonctions d'AC

- Fonctions de base
- Activation d'AC
- Profils de certificats**
- Services de publication
- Éditer/créer des AC**

Fonctions d'AE

- Sources de données externes
- Profils d'entités**
- Ajouter une entité**
- Chercher/éditer des entités

Fonctions de supervision

- Actions d'approbation
- Consulter les journaux
- Configuration des journaux

Fonctions système

- Configuration du système
- Gestion des services
- Gestion des administrateurs
- Mes préférences

Interface publique

- Documentation
- Déconnexion

Les parties importantes ont été entourées en rouge et voici leurs descriptions.

Profils de certificats C'est dans cette section que l'on crée les différents profils de certificats :

- BAVARDAGESERVER : profil pour le serveur sécurisé ;
- BAVARDAGEUSER : profil pour les utilisateurs sécurisés.

Ces profils sont décrits en détail dans le document annexe : Politique de certification

Éditer/créer des AC Une AC (autorité de certification) est une entité dont la mission est de vérifier les données du demandeur de certificat, de signer et de maintenir une liste des certificats et une liste des révocations. Sur la capture d'écran ci-dessus, on voit la liste des AC contenant celle relative à notre projet : **CABavardage**

Profils d'entités Chaque type d'entité a un profil associé :

- BAVARDAGE_SERVER : profil pour le serveur sécurisé ;
- BAVARDAGE_USER : profil pour les utilisateurs sécurisés.

Ajouter une entité Lorsqu'un utilisateur désire obtenir un certificat, un administrateur doit au préalable lui créer une entité associée. Il pourra ensuite récupérer son certificat pour sa clef RSA.

1.3.3 Partie sécurisée

La troisième livraison consistait en la surcouche sécurisée du client de chat et d'un serveur « sécurisé » dont le rôle est de gérer les utilisateurs sécurisés.

Il a tout d'abord fallu ouvrir une connexion SSL entre le client sécurisé et le serveur sécurisé grâce aux fonctions d'OpenSSL. Ensuite, nous avons créé des codes d'actions spécifiques à l'utilisation sécurisée du chat comme `CONNECT_SEC`, `CREATE_ROOM_SEC`... La gestion des clients dans le serveur sécurisé est similaire au serveur classique avec un fil d'exécution par client et une socket SSL.

Côté client, la surcouche sécurisée se base sur la librairie du client classique et utilise la même logique. Ainsi nous avons deux fonctions principales :

- `int send_message_sec (const char *mess, char **err_mess)`
- `int receive_message_sec (message *m)`

On rajoute également des fonctions de chiffrement/déchiffrement de messages :

- `char *aes_encrypt (unsigned char *key, unsigned char *iv, char *plaintext, int *len)`
- `char *aes_decrypt (unsigned char *key, unsigned char *iv, char *ciphertext, int *len)`

Comme les noms des fonctions l'indiquent, nous utilisons AES-256-CBC pour chiffrer les messages envoyés (champ `content`)

1.4 Problèmes rencontrés

Nous avons rencontré un problème pour la livraison du sprint 2. En effet, nous devions configurer un serveur, ce que nous avons fait dans une machine virtuelle. Cependant, le format de livraison utilisé jusqu'alors n'était plus utilisable car la machine faisait plusieurs giga octets de données. Nous avons alors convenu avec Mme Bardet de livrer sur une clef USB dans un premier temps et de configurer une machine mise à disposition par Mr Macadré.

Pour le sprint 3, nous avons eu également eu des problèmes au niveau de l'apprentissage d'OpenSSL. En effet, nous n'avions aucune expérience avec cette bibliothèque et les exemples sont nombreux mais très différents. Finalement, Mme Bardet nous a conseillé un très bon ouvrage : *Network Security with OpenSSL*. OpenSSL

Chapitre 2

Manuel d'utilisation

2.1 Récupération du projet

Les sources du projet sont disponibles sur un dépôt git. Elles peuvent être récupérées en ligne de commande ou en ligne.

2.1.1 En ligne de commande

Placez vous dans un terminal et exécutez la commande suivante :

```
$ git clone git://github.com/legrajul/bavardage.git
```

2.1.2 En ligne

Une archive contenant le projet peut être téléchargé à l'adresse :

2.2 Compilation

2.2.1 Dépendances Ubuntu

Pour la compilation du projet il faut d'abord vérifier si toutes les dépendances sont satisfaites :

- cmake : permet de compiler un projet pour différentes plateformes.
- valac-0.18 : compilateur Vala qui traduit le code source vala en code source C.
- libgtk-3-dev : outil multi plateformes pour créer des interfaces graphiques.
- libgee-dev : librairies de collections fournissant des classes basées sur GObject.
- libglib2.0-dev : fichiers de développement pour la bibliothèque GLib.
- libssl-dev : bibliothèque de développement SSL.
- libsqlite3-dev : bibliothèque de développement SQLite.

2.2.2 Compilation des sources

Les commandes suivantes doivent être exécuter dans le dossier du projet git bavardage :

```
$ mkdir src/build  
$ cd src/build  
$ cmake ..  
$ make
```

2.3 Exécution

Annexe A

Documents de gestion de projet

Annexe B

Déclaration des pratiques de certification

B.1 Introduction

B.1.1 Contexte Général

La PKI mise en place pour le projet de chat sécurisé fournit des certificats (Durée : 2 ans) aux utilisateurs sécurisés du chat. Ces certificats sont utilisés sur le chat pour s'authentifier.

B.1.2 Délégation d'autorité d'enregistrement

Pas de délégation du rôle d'Autorité d'Enregistrement dans notre cas. La PKI assurera ce rôle.

B.1.3 Souscripteur

Le souscripteur est l'utilisateur du chat souhaitant se connecter au chat sécurisé. Le souscripteur est identifié dans chaque certificat. Une fois acceptée, l'adhésion au service pour le souscripteur est valable pour la totalité de la période de validité du certificat sauf révocation.

B.2 Pré requis pour les demandes

B.2.1 Enregistrement d'un souscripteur

- Le souscripteur fournit à la RA toutes les informations nécessaires à son enregistrement.
- Le souscripteur s'engage à fournir des informations correctes et précises et avertir la RA en cas de mise à jour nécessaire de ces informations tout au long de la période de validité du certificat par le moyen de communication le plus adapté.

B.2.2 Vérification

L'AE doit :

- Vérifier le remplissage correct de tous les champs par le souscripteur en respectant les conventions.
- Enregistrer le souscripteur.
- Transmettre la demande à la CA.

L'AE a le droit de refuser toute demande.

B.3 Pratiques et procédures

B.3.1 Demande de certificats

Lorsque l'utilisateur fait une demande de certificat, la RA vérifie si les informations respectent les conventions, si les données respectent, la demande est automatiquement envoyée à l'autorité de certification pour génération du certificat. La demande se fait via un formulaire disponible sur l'application cliente du chat.

B.3.2 Validation des demandes

Le délai moyen entre la réception des demandes complètes et la délivrance d'un certificat est de 1 jour. En cas de non validation des informations, la RA rejette la demande. Le demandeur peut refaire sa demande suite à un rejet.

B.3.3 Révocation des certificats

La révocation entraîne la fin de validité du certificat avant la date de fin initialement prévue. La RA vérifie que la demande de révocation est :

- Soit faite par l'utilisateur ayant fait la demande de certificat : la demande de révocation sera traitée.
- Soit faite par une entité disposant des droits nécessaires : la RA révoquera le certificat. La demande de révocation et l'identité de l'entité seront conservées.

B.3.4 Expiration

La PKI doit s'efforcer de prévenir le souscripteur par email, 30 jours avant l'expiration de son certificat.

B.3.5 Renouvellement

Idem que pour demande de certificat.

B.4 Conservation et Protection des données

La PKI conserve les données relatives aux certificats pendant 2 ans minimum après expiration ou révocation des certificats. La PKI garde des copies des certificats quel que soit leur statut et conserve les logs pendant une période de 2 ans ou pour une période conforme à la loi.

La PKI respecte les règles applicables sur la protection des données personnelles jugées par la loi comme confidentielles.

Acronymes

CA	Certification Authority
AE	Registration Authority
DPC	Déclaration des Pratiques de Certification
PKI	Public Key Infrastructure
CNRS	Centre National de la Recherche Scientifique
TCS	Terena Certificate Service

Documents applicables et de référence

- PC (Politique de certification)
- Déclaration des pratiques de certification TCS (CNRS)

Annexe C

Politique de certification

C.1 Introduction

C.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.

C.1.2 Identification

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

C.1.3 Autorités, applications et groupes d'utilisateurs concernés

Autorité administrative (AA)

Composante de la PKI qui définit et fait appliquer les politiques de certification et les déclarations des pratiques de certification par la PKI.

Autorité de certification (CA)

C'est l'autorité à laquelle les utilisateurs font confiance pour gérer les certificats(générer, publier, révoquer), et les révocations. Le CA est gérée par l'administrateur du serveur sécurisé du chat. Le Common Name du CA sera BavardageCA.

Autorité d'enregistrement (RA)

Une autorité d'enregistrement est une composante de la PKI 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.

Autorité de dépôt (AD)

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

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.

Utilisateur Final (UF)

C'est la personne physique qui utilise les certificats. C'est un utilisateur du chat.

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.

Type d'applications concerné

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

C.1.4 Points de contact

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

À compléter

Personnes à contacter concernant ce document

Toute personne desirant contacter Bavardage concernant ce document peut envoyer un mail à l'adresse bavardage@gmail.com.

Personnes habilitées à déterminer la conformité de la DPC avec la PC

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

C.2 Dispositions d'ordre générale

C.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.

Obligations des acteurs

Autorité Administrative	<ul style="list-style-type: none">– Valider la politique de certification– Établir la conformité entre la PC et la DPC
Autorité d'Enregistrement	<ul style="list-style-type: none">– 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.– 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	<ul style="list-style-type: none">– S'engager à diffuser publiquement la politique de certification, la liste des certificats révoqués, et la liste des certificats.– 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	<ul style="list-style-type: none">– Il doit respecter la convention avec le chat bavardage et la PC
Utilisateur Final	<ul style="list-style-type: none">– 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.

Responsabilité des acteurs

Autorité Administrative	<ul style="list-style-type: none">– Résolution des litiges
Autorité d'Enregistrement	<ul style="list-style-type: none">– 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 la CA peut mettre en cause la responsabilité de la RA, ce qui exclut explicitement tout engagement de la RA envers les utilisateurs demandeurs ou finaux.
Autorité de Certification	<ul style="list-style-type: none">– 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	<ul style="list-style-type: none">– Il réalise les opérations de demande et révocation de certificats.
Utilisateur Final	<ul style="list-style-type: none">– Il est responsable de la sécurité de son poste de travail (clefs et certificats).

Interpretation de la loi

- Loi Suivant la législation nationale : Les données à caractère personnel d'une personne physique doivent être protégées suivant la loi.

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
La CA 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

Contrôle de conformité

À compléter

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 :
 - La DPC

- Cas des informations confidentielles à caractère privatif (exigence de séclusion). Il s'agit d'informations nécessaires à l'opérabilité de la PKI : données personnelles d'identification nominative d'un utilisateur demandeur (identifiants nominatifs), les utilisateurs demandeurs disposent d'un droit d'accès, 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 (cf. 2.1.2) ne peuvent être divulguées qu'à leur propriétaire (demandeur du certificat).

C.3 Identification et authentification

C.3.1 Enregistrement initial

Convention

La convention est le règlement que tout détenteur du certificat doit respecter. Seul l'UD peut signer la convention. Il doit obligatoirement se présenter physiquement à l'AA pour signer la convention.

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 usuel. Ce nom est celui de l'Abonné tel qu'il figure dans les documents d'État Civil.

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
- Etat 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

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 " - ".

Unicité des noms

L'unicité d'un certificat est basée sur l'unicité de son numéro de série au sein de la CA et du nom de l'abonné.

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.

Preuve de la possession d'une clé privée

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

Authentification de l'identité d'un individu

L'authentification d'un individu est réalisée lors de la procédure de demande d'un certificat. L'individu doit se présenter physiquement à l'AA.

C.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 regénéré.

C.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.

C.4 Besoins opérationnels

C.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, la CA traite la demande, génère le certificat et l'envoi à l'utilisateur demandeur qui devient un utilisateur final.

C.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 la CA 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.

C.4.3 Acceptation d'un certificat

Sans réponse à l'envoi du certificat à l'UD. Envoyé par la CA, 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.

C.4.4 Suspension et révocation d'un certificat

Causes possibles de révocation d'un certificat

Les causes de révocation du certificat de la CA peuvent être :

- Compromission de clé publique de la CA
- Compromission, suspicion de compromission, vol, perte de la clé privée de la CA
- 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 la CA.

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.
- Révocation du certificat de la CA 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.)

Publication des causes de révocation

Elles ne sont pas publiées.

Contrôle de la Liste de révocation

Toute personne est autorisée à consulter la liste de révocation.

Personnes habilitées à demander une révocation

Les personnes habilitées à demander une révocation sont :

- La CA
- La RA
- L'AA
- Le serveur de chat sécurisé
- L'UF

Procédure de demande de révocation

La demande de révocation se fait soit en envoyant un mail à l'AA et en s'authentifiant, soit en s'authentifiant et en remplissant un formulaire qui sera envoyé à la RA.

Temps de traitement d'une révocation

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

Fréquence de mise à jour de la liste des certificats révoqués

La CA 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.

C.4.5 Journalisation

Types d'évènements enregistrés

Les opérations réalisées sur la PKI seront enregistrées.

Fréquence de traitement des journaux d'évènement

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

Durée de retention d'un journal d'évènements

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

Copie de sauvegarde des journaux d'évènements

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

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'évènements.

C.4.6 Archives

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'évènements (2 ans).

Période de rétention des archives

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

C.5 Contrôle de sécurité physique et des procédures

C.5.1 Contrôle des procédures

Rôle

On distingue un unique administrateur.

Nombre de personnes nécessaire à chaque tâche

Pas de spécification

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.

C.6 Contrôles techniques de sécurité

C.6.1 Génération et Délivrance de clé

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

C.7 Profils des certificats et listes des certificats révoqués

C.7.1 Profil de certificat du CA

Type of CA	x509
Signing Algorithm	SHA1WithRSA
RSA key size	2048 bits
Validity	2y
Description	Initial CA
DN	CN=BavardageCA, O=Université de Rouen, L=Rouen, ST = Seine-Maritime
Sign by	Self signed
Certificate Profile	ROOTCA

C.7.2 Profil de certificat d'utilisateur

Type of CA	x509
Signing Algorithm	SHA1WithRSA
RSA key size	2048 bits
Validity	2y
Description	User certificate
DN	CN=username, O=Université de Rouen, L=Rouen, ST = Seine-Maritime
Sign by	BavardageCA
Certificate Profile	BavardageCA

C.7.3 Profil d'entité

Username	
Password	
Subject DN Attributes	
CN	
Default Certificate Profile	ENDUSER
Default CA	BavardageCA
Available CAs	BavardageCA

C.7.4 Profil de liste de révocation

Version	Numéro de version de la liste de révocation
Signature	Identifiant de l'algorithme de signature de la CA
Issuer	Nom de la CA 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	liste des numéros de série des certificats révoqués, contenant les champs suivants : <ul style="list-style-type: none">– userCertificate : Numéro de série du certificat révoqué– revocationDate : Date à laquelle le certificat a été révoqué
CrlExtensions	liste des extensions de la LCR : <ul style="list-style-type: none">– authorityKeyIdentifier : identifiant de la clé publique de la CA qui a signé la liste de révocation– CRLNumber : numéro de série de la liste de révocation

C.8 Administration et spécification

C.8.1 Procédure de modification de ces spécifications

Toute modification jugée par l'administrateur de la CA 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.

C.8.2 Politiques de publication et de notification

La CA avertit les UF des modifications apportées aux spécifications par courrier électronique.

C.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	Administrative Authority
CA	Certification Authority
RA	Registration Authority
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
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)