

# Spécification technique des besoins

<b>Version</b>	0.1
<b>Date</b>	9 décembre 2013
<b>Rédigé par</b>	Claire SMETS
<b>Relu par</b>	X
<b>Approuvé par</b>	X

## MISES À JOUR

Version	Date	Modifications réalisées
0.1	02/12/2013	Création du Document
X	X	X

## Table des matières

<b>1</b>	<b>Objet</b>	<b>4</b>
<b>2</b>	<b>Documents applicables et de référence</b>	<b>4</b>
<b>3</b>	<b>Terminologie et sigles utilisés</b>	<b>4</b>
<b>4</b>	<b>Exigences fonctionnelles</b>	<b>5</b>
4.1	Présentation de la mission du produit logiciel . . . . .	5
4.2	UC 1 : Récupération des certificats . . . . .	5
4.3	UC 2 : Factorisation des moduli des certificats . . . . .	6
4.4	UC 3 : Présentation des résultats . . . . .	6
<b>5</b>	<b>Diagrammes de cas d'utilisation</b>	<b>7</b>
5.1	UC 1 . . . . .	7
5.2	UC 2 . . . . .	7
5.3	UC 3 . . . . .	7
<b>6</b>	<b>Exigences opérationnelles</b>	<b>7</b>
<b>7</b>	<b>Exigences d'interface</b>	<b>8</b>
<b>8</b>	<b>Exigences de qualité</b>	<b>8</b>
<b>9</b>	<b>Exigences de réalisation</b>	<b>8</b>

## 1 Objet

Le projet s'inscrit dans un cadre relatif à un fait d'actualité récemment mis à jour, lié aux révélations de Snowden sur les pratiques de la NSA. Le monde de la cryptographie est en proie à de grandes incertitudes suite à ces révélations et remet en question tous les systèmes jusqu'alors développés. Notons que ce ne sont pas les algorithmes des systèmes cryptographiques qui sont remis en cause, mais leur développement machine qui n'est pas (ou plus) considéré comme nécessairement sûr. La NSA a par exemple très bien pu introduire des backdoors, ou faiblesses dans les logiciels, de telle sorte qu'ils puissent accéder aux données claires sans difficultés. On peut par exemple remettre en questions les outils développés par des laboratoires tels que RSA Labs, ou même encore des standards proposés par des agences comme le NIST (OpenSSL, AES, sont-ils vraiment sûrs ?)

### Objectif technique :

- coder un outil permettant de récupérer un grand nombre de certificats
- coder un outil permettant de trouver d'éventuels facteurs communs aux certificats récupérés
- d'implémenter un système serveur permettant l'audit des clients. (éventuellement, selon le temps restant)

### Résultat attendu :

Une étude sur les certificats utilisés sur internet, ainsi que l'implantation d'OpenSSL très utilisée.

## 2 Documents applicables et de référence

- Appel d'offre : Audit des implantations SSL/TLS
- les standards cryptographiques

## 3 Terminologie et sigles utilisés

- **Appli RC** : Application de Récupération des Certificats
- **Appli F** : Application de Factorisation
- **Machine D** : Machine Distant
- **Machine L** : Machine Locale
- **Certificat** : Un certificat électronique (aussi appelé certificat numérique ou certificat de clé publique) peut être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier une entité physique ou morale, mais aussi pour chiffrer des échanges.  
Il est signé par un tiers de confiance qui atteste du lien entre l'identité physique et l'entité numérique (Virtuel).
- **Audit** : Procédure consistant à s'assurer du caractère complet, sincère et régulier des comptes d'une entreprise, à s'en porter garant auprès des divers partenaires intéressés de la firme et, plus généralement, à porter un jugement sur la qualité et la rigueur de sa gestion. Ici ce n'est pas une entreprise qui en sera la cible mais un programme : OpenSSL.
- **Modulus** : En mathématiques et plus précisément en théorie algébrique des nombres, l'arithmétique modulaire est un ensemble de méthodes permettant la résolution de problèmes sur les nombres entiers. Ces méthodes dérivent de l'étude du reste obtenu par une division euclidienne.

## 4 Exigences fonctionnelles

### 4.1 Présentation de la mission du produit logiciel

EF.x : xxx ;

<b>Id</b>	<b>Intitulé</b>	<b>Acteur(s)</b>	<b>Priorité</b>
UC.1	Récupération des certificats	Appli RC, Machine D	Indispensable
UC.2	Factorisation des moduli des certificats	Appli F	Indispensable
UC.3	Audit d'OpenSSL	Utilisateur	Éventuelle

RG.X xxx

### 4.2 UC 1 : Récupération des certificats

<b>Acteurs concernés</b>	Appli RC, Machine D
<b>Description</b>	Récupérer une liste des certificats sur les adresses et les ports ouverts, scannés par ZMAP
<b>Préconditions</b>	Avoir une liste de machines distantes dont les ports sont ouverts
<b>Événements déclenchants</b>	L'administrateur lance l'application
<b>Conditions d'arrêt</b>	La liste est parcourue en entier
<b>Description du flot d'événements principal</b>	
<b>Acteur(s)</b>	<b>Système</b>
1. Lire la liste 2. Se connecter à la machine distante 3. Échanger les certificats 4. Stocker le certificat	3. Échanger les certificats
<b>Flots d'exceptions</b>	Coupure de connexion : retenter une deuxième fois si la Machine distante ne répond pas

#### 4.3 UC 2 : Factorisation des moduli des certificats

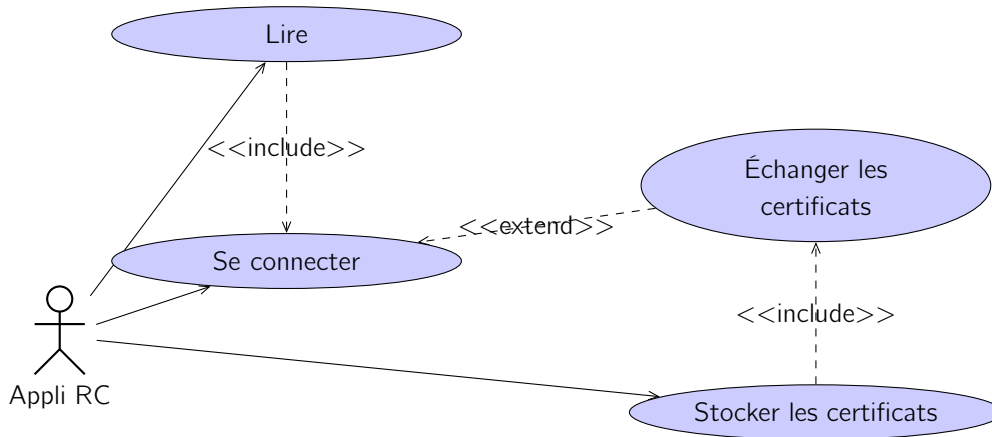
<b>Acteurs concernés</b>	Appli F
<b>Description</b>	Pour chaque certificat obtenu, on essaie de lui trouver des facteurs communs dans son modulus
<b>Préconditions</b>	Avoir une liste de certificats et donc leurs moduli
<b>Evénements déclenchants</b>	L'application est lancée
<b>Conditions d'arrêt</b>	La liste est parcourue en entier
<b>Description du flot d'événements principal</b>	
<b>Acteur(s)</b>	<b>Système</b>
1. Prendre les moduli 2. Construire l'arbre des produits 3. Construire l'arbre des restes 4. Sortir la liste des facteurs communs 5. Sortir la liste des moduli vulnérables trouvés	
<b>Flots d'exceptions</b>	Pas assez de ressources : Stocker l'arbre en dur au fur et à mesure.

#### 4.4 UC 3 : Présentation des résultats

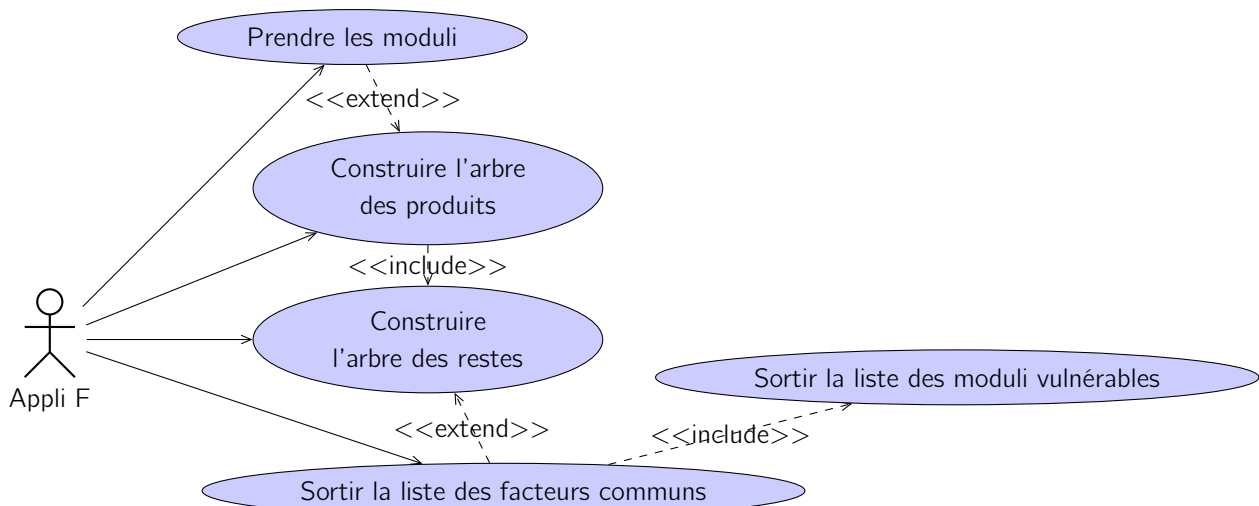
<b>Acteurs concernés</b>	Utilisateur
<b>Description</b>	Affiche les résultats produits par les précédentes fonctions
<b>Préconditions</b>	Des résultats ont été produits
<b>Evénements déclenchants</b>	Demande d'affichage des ces résultats
<b>Conditions d'arrêt</b>	Demande d'arrêt d'affichage des résultats
<b>Description du flot d'événements principal</b>	
<b>Acteur(s)</b>	<b>Système</b>
1. Ouvrir la page web 2. Sélectionner et filtrer les données affichées 3. Exporter les données	
<b>Flots d'exceptions</b>	

## 5 Diagrammes de cas d'utilisation

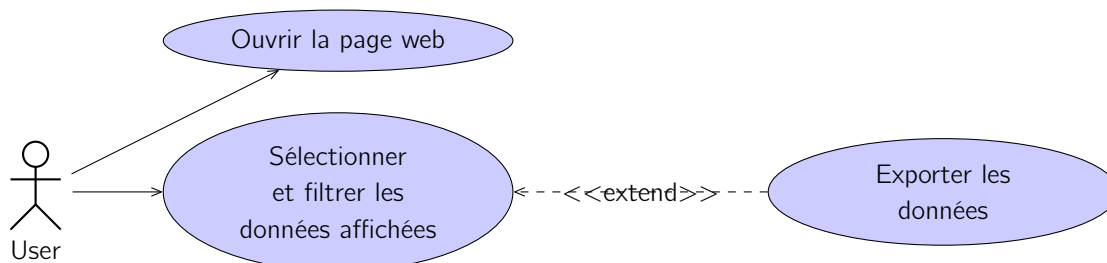
### 5.1 UC 1



### 5.2 UC 2



### 5.3 UC 3



## **6 Exigences opérationnelles**

EO.X : xxx

## **7 Exigences d'interface**

EI.X : xxx

## **8 Exigences de qualité**

EQ.X : xxx

## **9 Exigences de réalisation**

ER.X : xxx