

Spécification technique des besoins

Version	2.1
Date	28 janvier 2014
Rédigé par	Claire SMETS
Relu par	Pascal EDOUARD
Approuvé par	Mr OTMANI

MISES À JOUR

Version	Date	Modifications réalisées
0.1	02/12/2013	Création du Document
1.0	12/12/2013	Présentation de la première version
2.0	23/01/2013	Deuxième version validée par le client
2.1	28/01/2013	Définitions des niveaux des exigences

Table des matières

1	Objet	4
2	Documents applicables et de référence	4
3	Terminologie et sigles utilisés	4
4	Exigences fonctionnelles	5
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
4.5	UC 4 : Audit d'OpenSSL	6
4.6	UC 5 : Évaluation du niveau de sécurité du navigateur client	7
4.7	UC 1	7
4.8	UC 2	8
4.9	UC 3	8
4.10	UC 5	9
5	Exigences opérationnelles	9
6	Exigences d'interface	9
7	Exigences de qualité	9
8	Exigences de réalisation	10
9	Annexes	11
9.1	Message d'Amazon	11
9.2	Maquettes de présentation des résultats	12
9.2.1	Analyse des certificats	12
9.2.2	Fonctions auditées	13

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 utilisé.

2 Documents applicables et de référence

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

3 Terminologie et sigles utilisés

- **Appli F** : Application de Factorisation
- **Appli RC** : Application de Récupération des Certificats
- **Audit** : Analyse effectuée par un passage en revue complet et minutieux. Dans le cadre de notre projet, ce sera le code d'OpenSSL.
- **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).
- **Clefs** : Nous parlons ici des clefs RSA.
- **Machine D** : Machine Distant
- **Machine L** : Machine Locale
- **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

Id	Intitulé	Acteur(s)	Priorité
UC.1	Récupération des certificats	Appli RC, Machine D	Indispensable
UC.2	Factorisation des moduli des certificats	Appli F	Indispensable
UC.3	Présentation des résultats	Utilisateur	Indispensable
UC.4	Audit d'OpenSSL	Utilisateur	Indispensable
UC.5	Évaluation du niveau de sécurité du navigateur client	Client et Serveur	Optionnel

4.2 UC 1 : Récupération des certificats

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

Information : SSH est laissé de côté après plusieurs plaintes d'Amazon (cf Annexes).

4.3 UC 2 : Factorisation des moduli des certificats

Nom	Factorisation des moduli des certificats	
Acteurs concernés	Appli F	
Description	Pour chaque certificat obtenu, on essaie de lui trouver des facteurs communs dans son modulus	
Préconditions	Avoir une liste de certificats et donc leurs moduli	
Evénements déclenchants	L'application est lancée	
Conditions d'arrêt	La liste est parcourue en entier	
Description du flot d'événements principal		
Acteur(s)		Système
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		
Flots d'exceptions	Pas assez de ressources : Stocker l'arbre en dur au fur et à mesure.	

4.4 UC 3 : Présentation des résultats

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

4.5 UC 4 : Audit d'OpenSSL

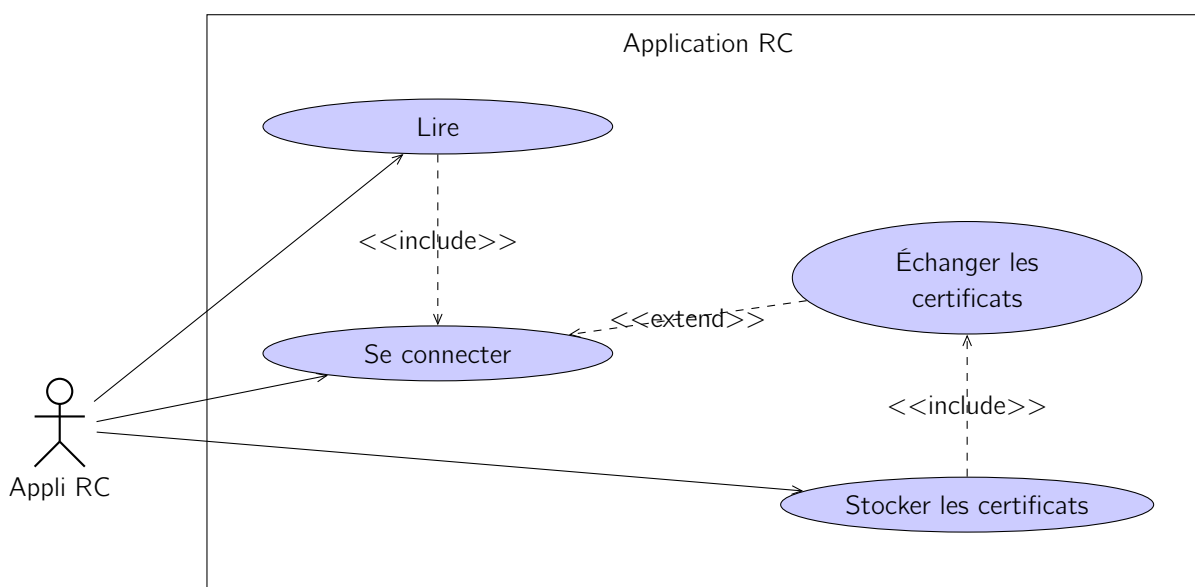
1. Nous étudierons tout d'abord les recommandations et les standards actuels (cf. PKCS) sous forme d'état de l'art, et nous en choisirons de façon argumentée un standard sur lequel nous baserons nos analyses.
2. Nous analyserons dans un deuxième temps le code source d'OpenSSL (la dernière version), en particulier sa partie développant la génération d'éléments aléatoires et ses primitives cryptographiques. Nous en fe-

rons de plus une description détaillée. Nous comparerons ensuite nos résultats avec les recommandations choisies, puis nous concluons en déterminant si cette génération est efficace.

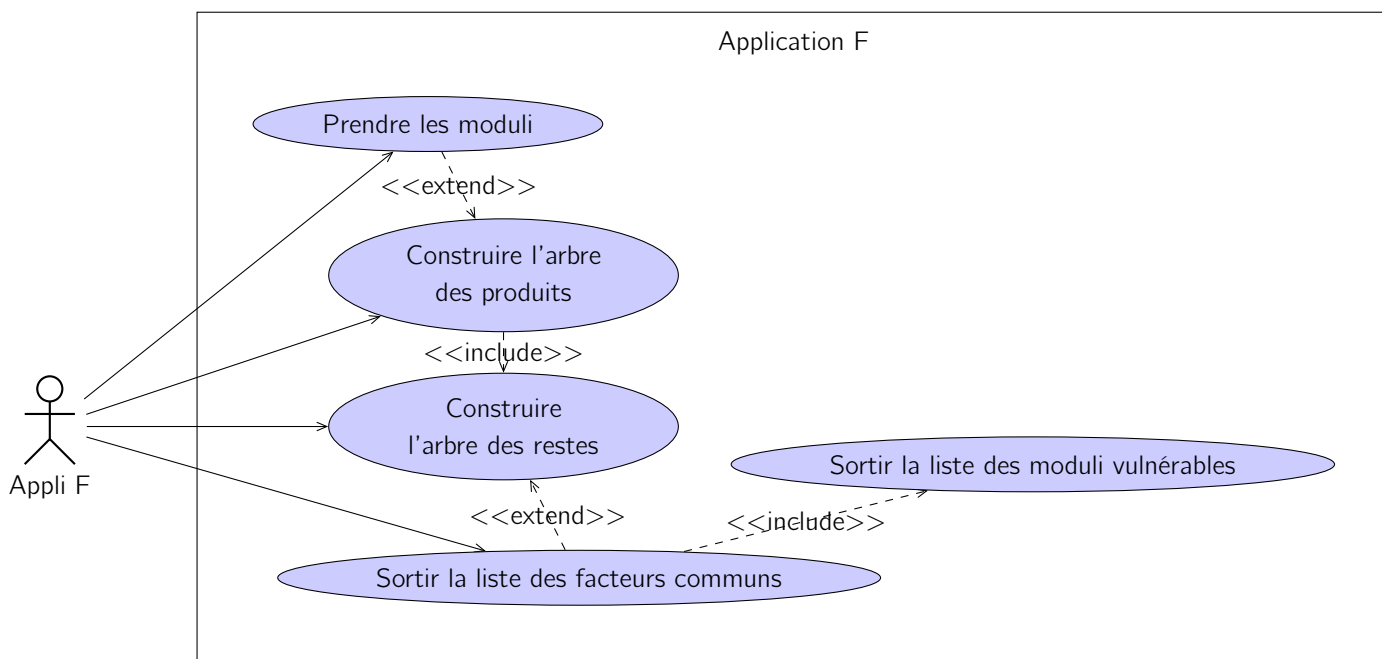
4.6 UC 5 : Évaluation du niveau de sécurité du navigateur client

Nom	Test d'un client
Acteurs concernés	Client, serveur de test
Description	Lors de la connexion d'un client, analyse des paquets échangés
Préconditions	Le client possède une version de navigateur récente
Événements déclenchants	Demande de connexion d'un client
Conditions d'arrêt	Les paquets ont été échangés et analysés
Description du flot d'événements principal	
Acteur(s)	Système
1. Se connecter sur le serveur	2. Établir la connexion 3. Analyser le niveau de sécurité du navigateur 4. Afficher les résultats
Flots d'exceptions	

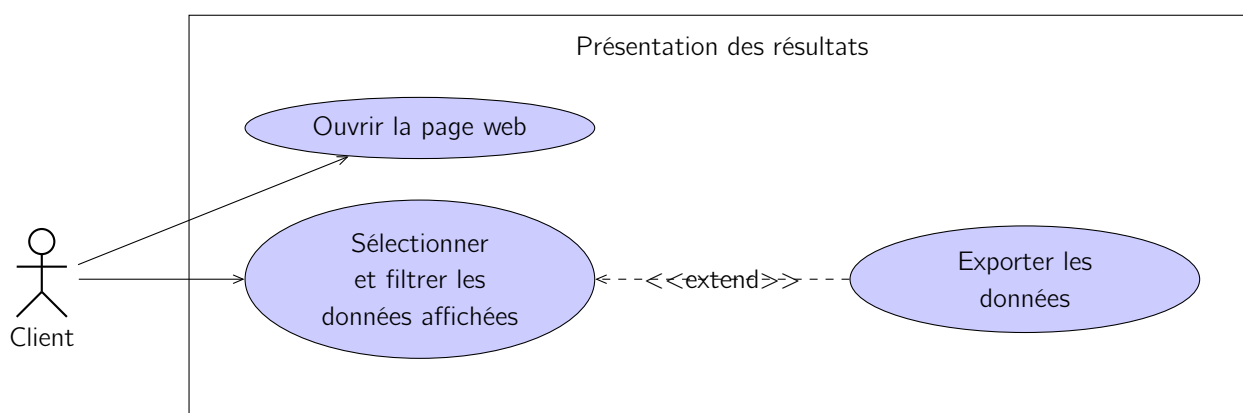
4.7 UC 1



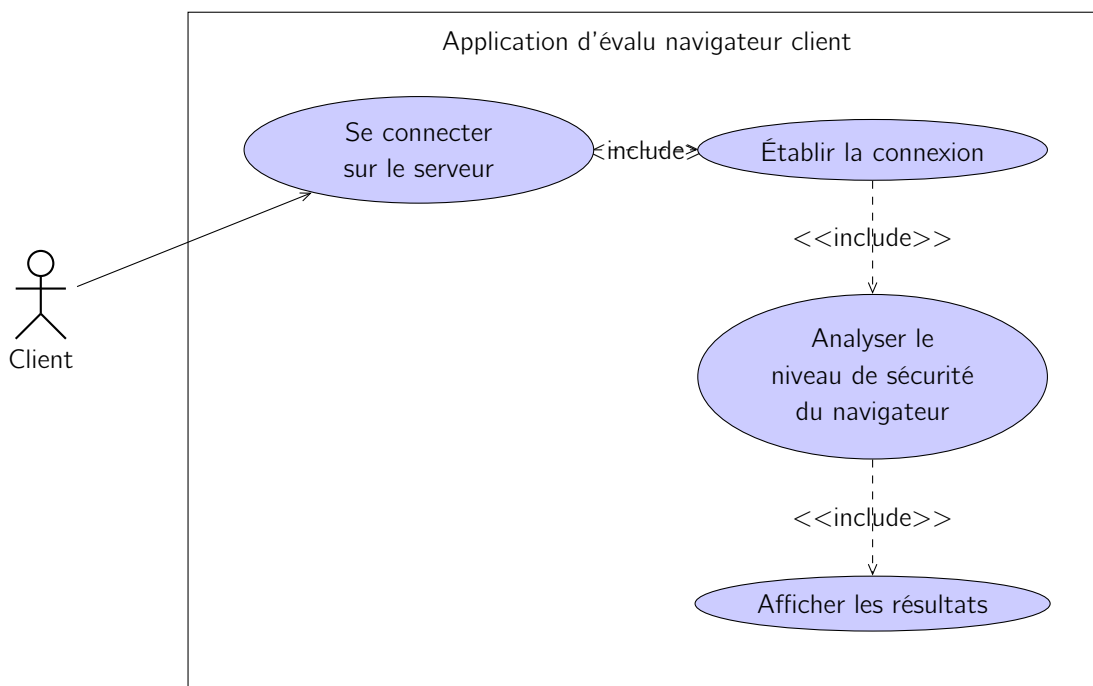
4.8 UC 2



4.9 UC 3



4.10 UC 5



Notre sujet étant constitué de plusieurs blocs sans réel lien entre eux, regrouper les cas d'utilisation en un seul constituerait une redondance du document.

5 Exigences opérationnelles

Id	Intitulé	Acteur(s)	Priorité
EO.1 (cf. UC1)	Lors de la récupération des certificats, les protocoles visés seront SSL/TLS	Appli RC	Indispensable

6 Exigences d'interface

Pas d'exigence d'interface.

7 Exigences de qualité

Id	Intitulé	Acteur(s)	Priorité
EQ.1	L'application de la factorisation des clefs se fait dans un temps proportionnel à la durée du projet	Appli F	Recommandé

Id	Intitulé	Acteur(s)	Priorité
EQ.2	Présentation des résultats sous forme de formulaires, dont la maquette est ci-jointe (cf annexes).	Application évaluation	Recommandé

8 Exigences de réalisation

Id	Intitulé	Acteur(s)	Priorité
ER.1	Le programme de récupération des certificats.	Appli RC	Indispensable

Id	Intitulé	Acteur(s)	Priorité
ER.2	Le programme de factorisation des clefs de certificat	Appli F	Indispensable

Id	Intitulé	Acteur(s)	Priorité
ER.3	Analyse des résultats obtenus sur la factorisation des clefs.	Application évaluation	Indispensable

Id	Intitulé	Acteur(s)	Priorité
ER.4	Document détaillant l'audit réalisé sur OpenSSL.	–	Indispensable

9 Annexes

9.1 Message d'Amazon



Dear Amazon EC2 Customer,

We've received a report that your instance(s):

Instance Id: i-6394312c
IP Address: 54.194.102.0

has been port scanning remote hosts on the Internet; check the information provided below by the abuse reporter.

This is specifically forbidden in our User Agreement: <http://aws.amazon.com/agreement/>

Please immediately restrict the flow of traffic from your instances(s) to cease disruption to other networks and reply this email to send your reply of action to the original abuse reporter. This will activate a flag in our ticketing system, letting us know that you have acknowledged receipt of this email.

It's possible that your environment has been compromised by an external attacker. It remains your responsibility to ensure that your instances and all applications are secured.

Case number: 11135140320-1

Additional abuse report information provided by original abuse reporter:

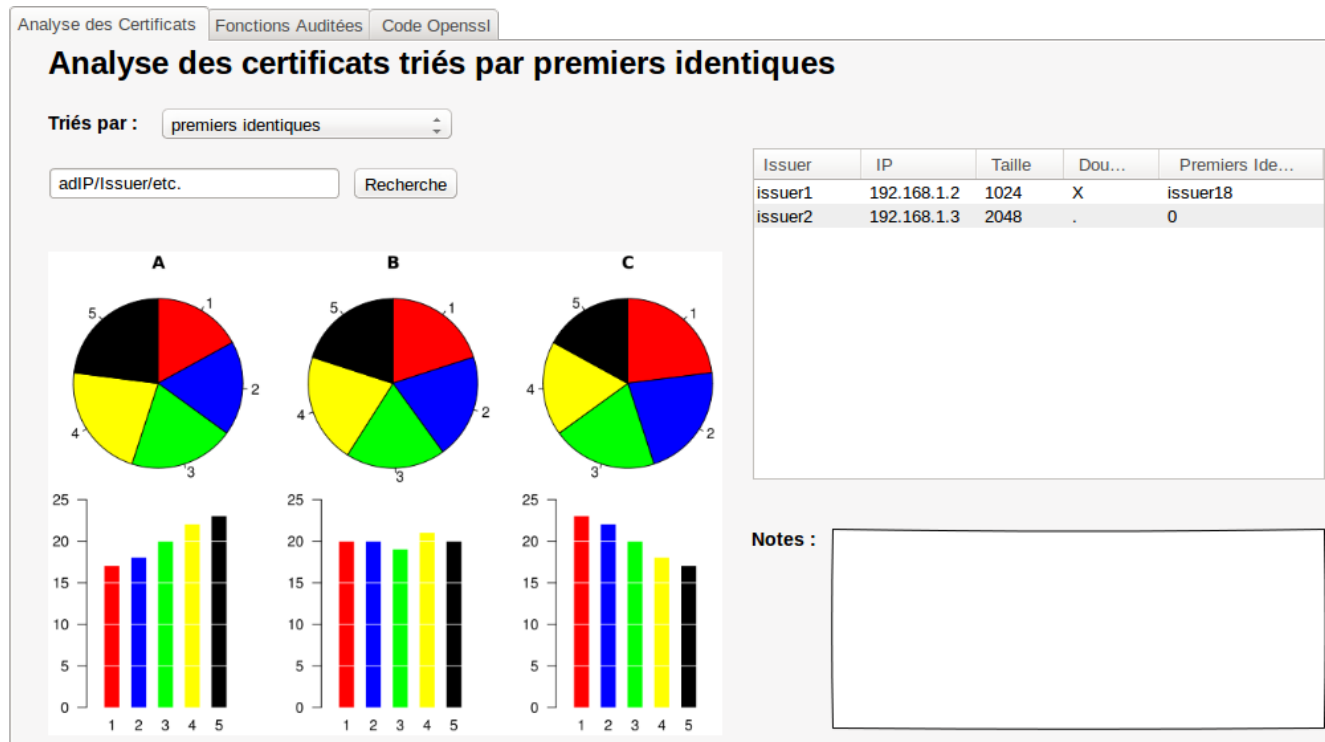
* Destination IPs:
* Destination Ports: 22
* Destination URLs:
* Abuse Time: Sun Jan 19 11:36:00 UTC 2014
* Log Extract:

<<<
54.194.102.0 was observed probing caltech.edu for security holes. It
has been blocked at our border routers. It may be compromised.

(time zone of log is PST, which is UTC-08:00, date is MMDD)
log entries are from Cisco netflow, time is flow start time
date.time srcIP srcPort dstIP dstPort proto #pkts

9.2 Maquettes de présentation des résultats

9.2.1 Analyse des certificats



9.2.2 Fonctions auditées

Analyse de Certificats

Fonctions Auditées

Code Openssl

Liste des fonctions auditées

[Fonction1](#)
[Fonction2](#)
[Fonction3](#)

Créer nouvel audit

Analyse des Certificats Fonctions Auditées Code Openssl

Fonction auditée : <nom_fonction>

Auteurs : William, Mathieu, Claire, Julien, Pascal **Date :** 01/01/2001

Lien vers le code : <http://doxygen.com/fonction>

Implantation : [openssl1.0.0/fonction_appelante/interm1/.../intermN/fonction_auditee](https://opendss11.0.0/fonction_appelante/interm1/.../intermN/fonction_auditee)

Description technique :

Algorithme :
Entrées : *liste_d_entrees*
Sortie : *sortie*

Début

instructions;

Fin

Normes visées :

Nom de(s) norme(s) : RFC 4949

Date : 01/01/2001

Liens : <http://norme.com>

Points importants :

Ici, il faut faire un résumé descriptif de la norme, et soulever les points importants de la norme que doit respecter la fonction auditée.

Audit :

Respect de la norme :

Ici, nous indiquerons dans quelle mesure la norme est-elle respectée, si elle respecte les consignes de sécurité, et si elle prend en compte les recommandations.

Suggestion d'améliorations :

Ici, vous noterez vos suggestions d'améliorations, par exemple des améliorations techniques (sur le code, les structures utilisées), des choix différents d'implémentation en rapport aux critères définis par la ou les normes utilisées.

Enregistrer