

# Cahier de recettes

<b>Version</b>	1.0
<b>Date</b>	12/12/13
<b>Rédigé par</b>	Boisseleau W. et Latimier M.
<b>Relu par</b>	Pascal Edouard
<b>Approuvé par</b>	Ayoub Otmani

## MISES À JOUR

Version	Date	Modifications réalisées
0.1	10/12/13	Création et complétion
0.2	11/12/13	Complétion
1.0	12/12/13	Correctifs appliqués

## Table des matières

<b>1</b>	<b>Objet</b>	<b>4</b>
<b>2</b>	<b>Terminologie et sigles utilisés</b>	<b>4</b>
<b>3</b>	<b>Documents applicables et de référence</b>	<b>4</b>
<b>4</b>	<b>Environnement de test</b>	<b>4</b>
4.1	Lieu . . . . .	4
4.2	Machines utilisées . . . . .	4
4.3	Base de données de test . . . . .	5
4.4	Contraintes . . . . .	5
<b>5</b>	<b>Responsabilités</b>	<b>5</b>
<b>6</b>	<b>Stratégie de tests</b>	<b>6</b>
6.1	Gestion des tâches de tests . . . . .	6
6.2	La campagne de test . . . . .	6
6.3	Critères d'arrêt . . . . .	6
<b>7</b>	<b>Gestion des anomalies</b>	<b>6</b>
<b>8</b>	<b>Procédures de test</b>	<b>7</b>
8.1	ZMAP . . . . .	7
8.2	RC . . . . .	8
8.3	SD . . . . .	8
8.4	F . . . . .	9

## 1 Objet

L'objet de ce cahier de recettes est de lister les tests que nous allons pratiquer sur les différentes fonctionnalités liées au projet "Audit des implantations SSL/TLS" avant sa livraison au client. Il décrit notamment une série de scénarios précisant les démarches à suivre afin de prouver l'efficacité des différents produits. Il permet en effet de vérifier que la série de logiciels/services est conforme aux spécifications définies avec le client et qu'elles répondent efficacement au cahier des charges.

## 2 Terminologie et sigles utilisés

Les acronymes suivants peuvent être utilisés dans le rapport ci-présent :

- **Appli RC** : Application de Récupération des Certificats
- **Appli F** : Application de Factorisation
- **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).
- **Appli SD** : réfère au logiciel de suppression de doublons.

Des sigles sont également définis et utilisés localement pour faciliter la définition des procédures de tests.

## 3 Documents applicables et de référence

## 4 Environnement de test

### 4.1 Lieu

L'ensemble des procédures de tests s'effectueront en salle machine U2.2.34 de l'Université de Rouen, en compagnie d'un ou deux testeurs minimum. Quelques tests peu gourmands en temps et en mémoire, mais nécessaires à la validation des fonctionnalités du produit final, pourront être effectués sur des machines personnelles. Cependant, la majorité d'entre eux nécessiteront la monopolisation d'une machine pour plusieurs heures, voire plusieurs jours.

### 4.2 Machines utilisées

Nous serons amenés à utiliser des machines virtuelles lors de tests mettant en scène un réseau complexe simulant à petite échelle un réseau internet, ceci sous différents scénarii possibles (mécanisme de pare-feu, zone (dé)militarisée, ports ouverts/fermés pour des connexions SSH, ...).

Nous avons choisi le logiciel de virtualisation de réseau Netkit pour mener à bien ces tests. Le DAL indiquera l'ensemble des machines réelles utilisables pour la plate-forme de tests et/ou de développement.

### **4.3 Base de données de test**

Plusieurs fonctionnalités du projet seront déjà implantées et pourront servir d'appui pour nos tests (dont ZMAP ou l'algorithme de factorisation).

Nos procédures de tests se succèdent pour la plupart, les résultats des précédents tests nous serviront de faits pour les phases de tests suivantes.

### **4.4 Contraintes**

La modification - même minimale - de la partie applicative de notre projet aura pour conséquence le relancement de toutes les procédures de tests directement et indirectement concernées.

Nous aurons des contraintes de temps selon le planning prévu dans le plan de développement. Les procédures de tests doivent être fonctionnelles rapidement afin de valider l'avancement du projet.

Nos procédures de tests doivent être les plus simples possibles afin d'éviter toute perte de temps, et toute contrainte d'espace (ce qui n'enlève en rien à l'efficacité des tests).

## **5 Responsabilités**

M. Latimier et W. Boisseleau sont les principaux testeurs sur ce projet, ils devront mener à bien la conception, l'exécution et la vérification de chacun d'entre eux. D'autres membres du projet pourront consacrer leur temps sur les tests en cas de demande explicite du chef de projet, ou durant leur temps libre (considéré comme non planifié).

Dès lors qu'un outil ou parti d'outil sujet à des procédures de test est développé, les testeurs auront la responsabilité de lancer les procédures de tests sur celui-ci afin de permettre une gestion des erreurs efficace et la plus en amont possible.

De plus, les testeurs s'appliqueront à respecter ou faire respecter les conditions de tests définies dans ce rapport.

Dans les cas où des erreurs sont mises en évidence, l'équipe de testeurs devra d'une part analyser l'origine du problème et d'autre part communiquer aux développeurs et au chef de projet les problèmes identifiés. Lorsque c'est possible, ils soumettront une proposition de solution ou de piste solutionnante.

## 6 Stratégie de tests

### 6.1 Gestion des tâches de tests

Les outils de tests devront être développés en parallèle aux développements des fonctionnalités du projet. L'écart entre le développement et les tests ne doit pas être trop grand, afin d'optimiser le rendement de chaque acteur.

Les procédures de tests sont les plus fines possibles, elles mettent en place individuellement un test spécifique ; ceci afin de les distribuer plus facilement lors de la répartition des tâches, et de pouvoir gagner du temps dans nos phases de débogage.

De plus, elles devront avoir le moins d'inter-dépendance possible, pour éviter des modifications en cascade lors des modifications des procédures parentes. Lorsqu'un outil de test est validé par l'équipe, il est inutile d'y apporter des améliorations. Nous y reviendrons uniquement lors de modifications éventuelles des fonctionnalités du projet.

### 6.2 La campagne de test

Elle s'effectuera principalement sur la première partie de notre projet "Audit de clefs cryptographiques", et éventuellement sur la troisième partie "Analyse dynamique" selon le planning et l'attente du client (non exigé pour l'instant).

La seconde partie "Analyse statique" ne nécessite pas d'exigences techniques particulières, mais plutôt une réflexion sur un problème cryptographique.

### 6.3 Critères d'arrêt

Une procédure de tests sera considérée comme valide lors de l'envoi des livrables fonctionnels lui étant associée et le retour favorable du client.

## 7 Gestion des anomalies

Lors de nos phases de tests, l'ensemble des anomalies rencontrées devront être signalées dans un document intitulé au format CSV (ou ODS). Lorsqu'une anomalie est rencontrée, nous devons calculer son taux de criticité sur le projet et le cahier des charges. Si une exigence technique du client s'en trouve affectée, elle doit être réglée au plus vite.

Une politique de prévention doit être mise en place afin d'éviter tout renouvellement, en cas de modification d'un logiciel par exemple.

## 8 Procédures de test

### 8.1 ZMAP

#### Terminologie.

Sont définis les acronymes suivants :

- R : réseau virtuel fixé représentant toutes les configurations réseau envisageables,
- R' : réseau virtuel altéré de R,
- 1A : liste d'adresses prédéfinie de machines de R,
- A1 : liste d'adresses de machines ayant des ports SSH ouverts sur R,
- A2 : liste d'adresses de machines ayant des ports SSH protégés et fermés sur R,
- A1' : liste d'adresses de machines ayant des ports SSH ouverts sur R',
- A2' : liste d'adresses de machines ayant des ports SSH protégés et fermés sur R',
- VA1 : liste d'adresses de machines attendues ayant des ports SSH ouverts sur R,
- VA2 : liste d'adresses de machines attendues ayant des ports SSH protégés et fermés sur R,
- VA1' : liste d'adresses de machines attendues ayant des ports SSH ouverts sur R',
- VA2' : liste d'adresses de machines attendues ayant des ports SSH protégés et fermés sur R'.

#### Procédures.

Objet testé : ZMAP		Version : 1.0		
Objectif de test : ZMAP reconnaît port O/F/N-A				
Procédure P1 : TestPortsZMAP(ZMAP,R,R',IA,VA1,VA2,VA1',VA2')				
N.	Actions	Résultats attendus	Exig.	OK/NOK
1	On lance ZMAP sur R avec 1A en entrée	ZMAP retourne A1 et A2. On vérifie que A1=VA1 et A2=VA2.		/
2	On relance ZMAP sur R' avec A2 en entrée	ZMAP retourne A1' et A2'. On vérifie que A1'=VA1' et A2'=VA2'.		/

Objet testé : ZMAP		Version : 1.0		
Objectif de test : Tester la portabilité du résultat de ZMAP pour l'application RC				
Procédure P2 : Portabilité(ZMAP,IA,R)				
N.	Actions	Résultats attendus	Exig.	OK/NOK
1	Sur le système Linux, on lance ZMAP sur R avec 1A en entrée. On récupère A1 et A2. On relance ZMAP sur A1 et A2	ZMAP s'exécute correctement sur A1 à A2	P1	/
2	Même procédé sur le système Windows	ZMAP se termine correctement sur A1 à A2	P1	/

## 8.2 RC

### Terminologie.

Sont définis les acronymes suivants :

- LAd : liste d'adresses de machines ayant des ports ouverts générées par ZMAP,
- $M_i$  : machine  $i$  de la LAd,
- $C_i$  : certificat ou chaîne de certification de la machine  $i$  selon RC,
- $VC_i$  : certificat ou chaîne de certification de la machine  $i$  selon  $M_i$ ,
- $C'_i$  : certificat ou chaîne de certification de la machine  $i$  selon RC,
- $VC'_i$  : certificat ou chaîne de certification de la machine  $i$  après stockage.

### Procédures.

Objet testé : RC		Version : 1.0		
Objectif de test : Établissement de connexion avec RC				
Procédure P3 : conRC(RC,IA)				
N.	Actions	Résultats attendus	Exig.	OK/NOK
1	RC lit LAd.	RC ne retourne pas d'erreur, il reconnaît les $M_i$ comme valides	P2	/

Objet testé : RC		Version : 1.0		
Objectif de test : Récupération des certificats				
Procédure P4 : recCertifRC(RC,IA)				
N.	Actions	Résultats attendus	Exig.	OK/NOK
1	RC échange de certificats avec $M_i$ .	Si $M_i$ autorise l'échange, récupération de $C_i$ et $C_i = VC_i$ , sinon RC passe à $M_{i+1}$	P3	/
2	RC stocke dans une base de données le certificat s'il existe	Le certificat est stocké correctement et $C_i$ et $C'_i = VC'_i$	P3	/

## 8.3 SD

### Terminologie.

Sont définis les acronymes suivants :

- B base de données contenant des certificats uniques et des certificats identiques,
- BA base de données B après suppression des doublons selon SD,
- VBA base de données B sans doublons



#### Procédure.

Objet testé : SD		Version : 1.0		
Objectif de test : Tests de suppression de doublons				
Procédure P4 : supD(SD,B,VBA)				
N.	Actions	Résultats attendus	Exig.	OK/NOK
1	SD s'exécute sur B	SD s'exécute correctement et BA=VBA		/

## 8.4 F

#### Terminologie.

Sont définis les acronymes suivants :

- $IA_1$  : liste de taille impaire d'entiers de même taille binaire,
- $IA_2$  : liste de taille paire d'entiers de même taille binaire,
- $F_1$  : section de l'algorithme de  $F$  calculant l'arbre des produits,
- $F_2$  :  $F - F_1$  section de l'algorithme de  $F$  calculant l'arbre des restes,
- $IF_1$  : liste des fils de  $IA_1$  calculée suivant  $F_1$  sur  $IA_1$ ,
- $IF_2$  : liste des fils de  $IA_2$  calculée suivant  $F_1$  sur  $IA_2$ ,
- $VIF_1$  : liste des fils attendue pour  $IA_1$ ,
- $VIF_2$  : liste des fils attendue pour  $IA_2$ ,
- $P$  : entier produit de facteurs après lancement de  $F_1$  sur  $IA_A$ ,
- $modP_1$  : élément gauche après calcul du modulo de  $P$  suivant  $F_2$ ,
- $modP_2$  : élément droite après calcul du modulo de  $P$  suivant  $F_2$ ,
- $VmodP_1$  : élément gauche modulo de  $P$  suivant  $F_2$ ,
- $VmodP_2$  : élément droite modulo de  $P$  suivant  $F_2$ .

#### Procédures.

Objet testé : F		Version : 1.0		
Objectif de test : Calcul des fils selon $F1$ suivant une liste				
Procédure P5 : $\text{calcF1}(F1, IA_1, IA_2, VIF_1, VIF_2)$				
N.	Actions	Résultats attendus	Exig.	OK/NOK
1	On calcule $F1(IA_1) = IF_1$	$F1$ s'exécute correctement et $IF_1 = VIF_1$		/
2	On calcule $F1(IA_2) = IF_2$	$F1$ s'exécute correctement et $IF_2 = VIF_2$		/

Objet testé : F		Version : 1.0		
Objectif de test : Calcul des modulus fils avec $F2$ suivant P				
Procédure P6 : $\text{calcF2}(F2,P,V_{\text{mod}P1},V_{\text{mod}P2})$				
N.	Actions	Résultats attendus	Exig.	OK/NOK
1	On calcule $F2(P) = (modP1, modP2)$	$F2$ s'exécute correctement et $modP1 = V_{\text{mod}P1}$ et $modP2 = V_{\text{mod}P2}$	P5	/