

Rapport Final

Audit des implantations SSL/TLS

Date	5 février 2014
Rédigé par	Claire Smets, William Boisseleau, Julien Legras, Mathieu Latimier, Pascal Edouard
À l'attention de	Ayoub Otmani

Table des matières

Introduction	6
1 Audit de clefs cryptographiques	7
1.1 Ex section	7
1.1.1 Ex subsection	7
1.1.1.1 Ex subsubsection	7
1.1.1.1.1 Ex subsubsubsection	7
2 Analyse Statique : audit d'OpenSSL	8
2.1 Ex section	8
2.1.1 Ex subsection	8
2.1.1.1 Ex subsubsection	8
2.1.1.1.1 Ex subsubsubsection	8
3 Analyse dynamique	9
3.1 Ex section	9
3.1.1 Ex subsection	9
3.1.1.1 Ex subsubsection	9
3.1.1.1.1 Ex subsubsubsection	9
Conclusion	10

Table des figures

1.1	Exemple 1	7
2.1	Exemple 1	8
3.1	Exemple 1	9

Liste des tableaux

1.1	Exemple tableau	7
2.1	Exemple tableau	8
3.1	Exemple tableau	9

Listings

Introduction

Intro rapport final

Chapitre 1

Audit de clefs cryptographiques

1.1 Ex section

1.1.1 Ex subsection

1.1.1.1 Ex subsubsection

1.1.1.1.1 Ex subsubsubsection

Exemple item :

- item1 ;
- item2 ;
- itemFin.

Exemple enum :

1. enum1 ;
2. enum2 ;
3. enumFin.



FIGURE 1.1 – Exemple de figure avec titre raccourci

Identifiant	KeyExch	Authn	Enc	MAC
TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA	SRP SHA1	SRP SHA1	3DES CBC	SHA1

TABLE 1.1 – Exemple tableau

Chapitre 2

Analyse Statique : audit d'OpenSSL

2.1 Ex section

2.1.1 Ex subsection

2.1.1.1 Ex subsubsection

2.1.1.1.1 Ex subsubsubsection

Exemple item :

- item1 ;
- item2 ;
- itemFin.

Exemple enum :

1. enum1 ;
2. enum2 ;
3. enumFin.



FIGURE 2.1 – Exemple de figure avec titre raccourci

Identifiant	KeyExch	Authn	Enc	MAC
TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA	SRP SHA1	SRP SHA1	3DES CBC	SHA1

TABLE 2.1 – Exemple tableau

Chapitre 3

Analyse dynamique

3.1 Ex section

3.1.1 Ex subsection

3.1.1.1 Ex subsubsection

3.1.1.1.1 Ex subsubsubsection

Exemple item :

- item1 ;
- item2 ;
- itemFin.

Exemple enum :

1. enum1 ;
2. enum2 ;
3. enumFin.



FIGURE 3.1 – Exemple de figure avec titre raccourci

Identifiant	KeyExch	Authn	Enc	MAC
TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA	SRP SHA1	SRP SHA1	3DES CBC	SHA1

TABLE 3.1 – Exemple tableau

Chapitre 4

Vie de projet

4.1 Ex section

4.1.1 Ex subsection

4.1.1.1 Ex subsubsection

4.1.1.1.1 Ex subsubsubsection

Exemple item :

- item1 ;
- item2 ;
- itemFin.

Exemple enum :

1. enum1 ;
2. enum2 ;
3. enumFin.



FIGURE 4.1 – Exemple de figure avec titre raccourci

Identifiant	KeyExch	Authn	Enc	MAC
TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA	SRP SHA1	SRP SHA1	3DES CBC	SHA1

TABLE 4.1 – Exemple tableau

Conclusion

Conclusion rapport final