# Projet annuel - Audit des implantations SSL/TLS

William Boisseleau – Pascal Edouard – Mathieu Latimier –
Julien Legras – Claire Smets

Master 2 Sécurité des Systèmes Informatiques

20/12/2013

# Sommaire

1 Présentation du projet

2 Cas d'utilisation

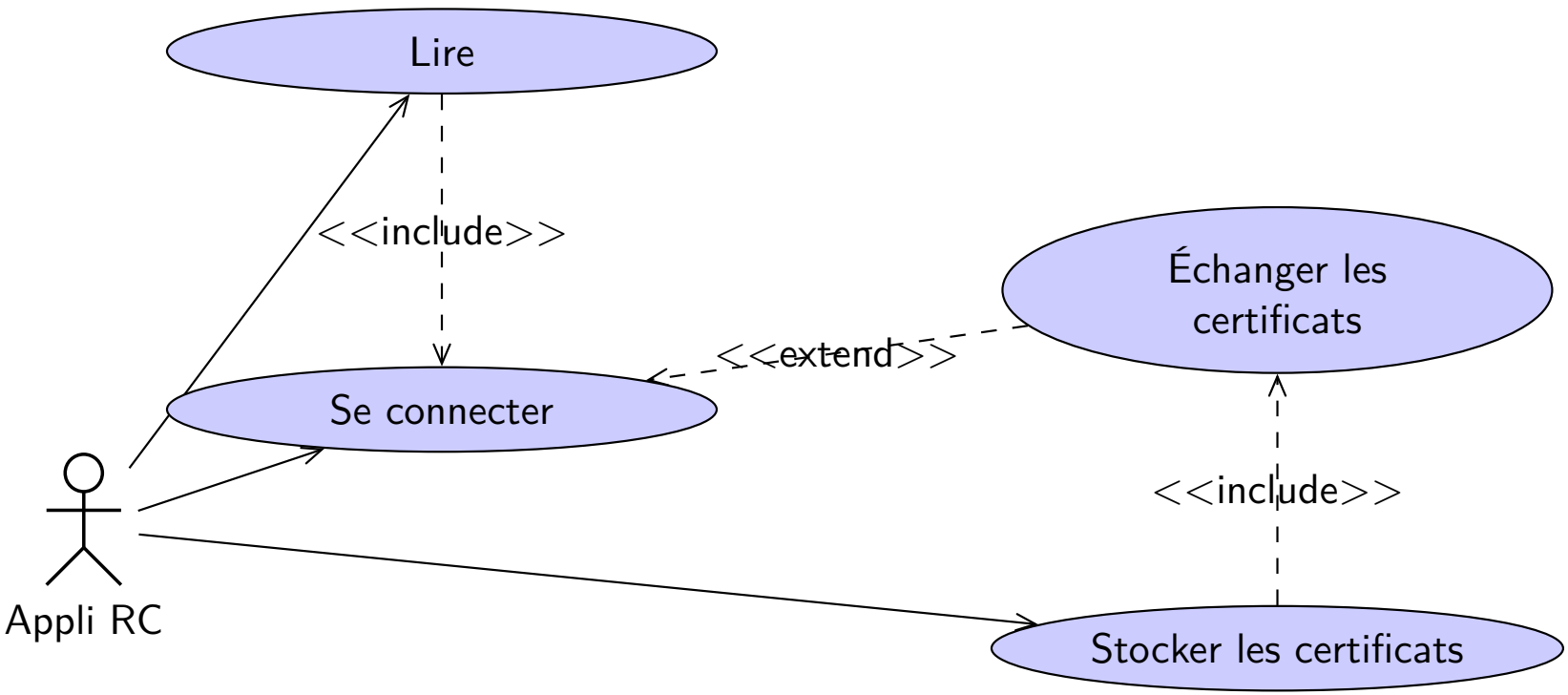
3 Planning de développement

# Présentation du projet

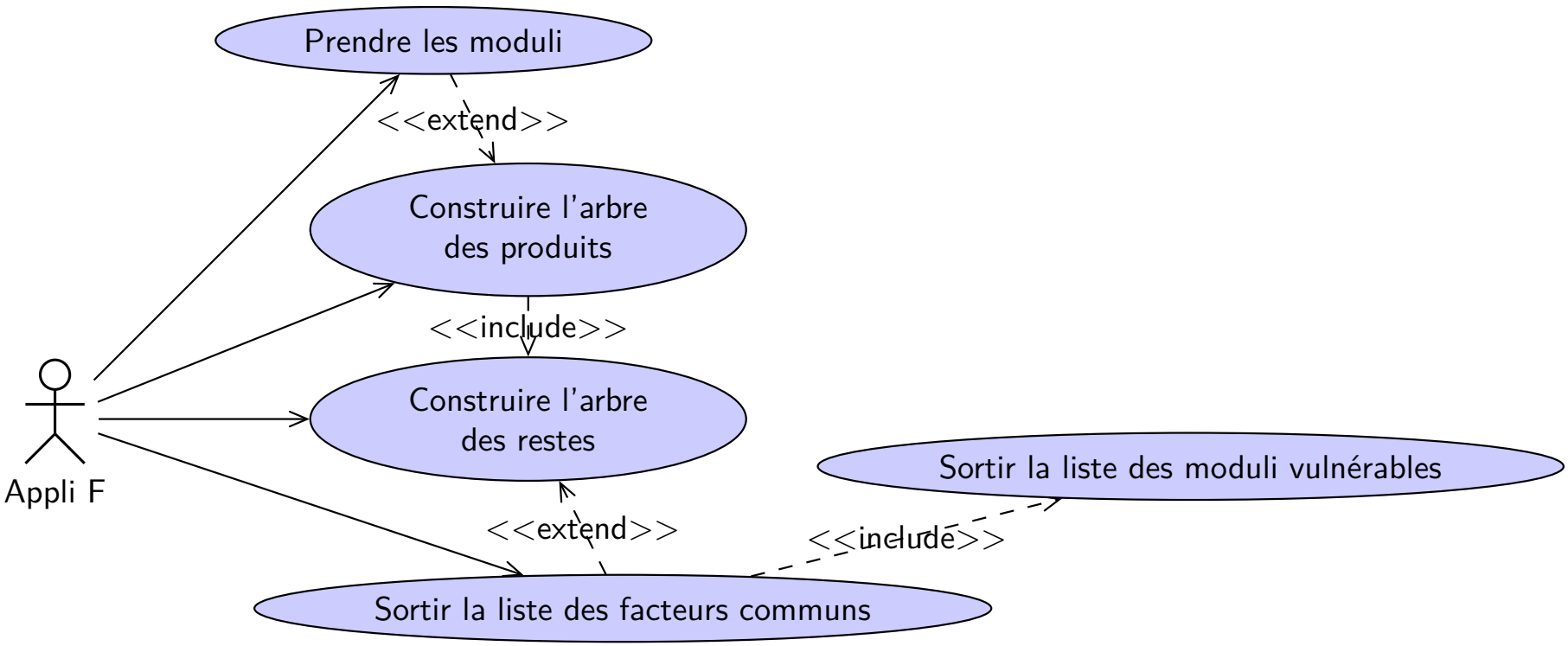
## Sujet proposé par Ayoub Otmani

1. audit des clefs cryptographiques
2. analyse statique de la bibliothèque OpenSSL
3. analyse dynamique du niveau de sécurité d'un navigateur web

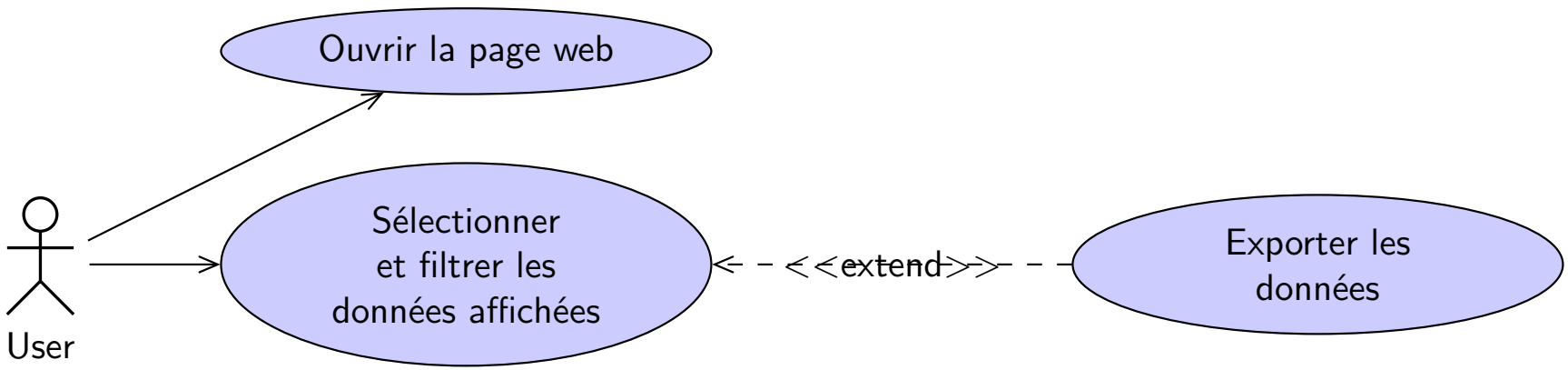
# Cas d'utilisation I



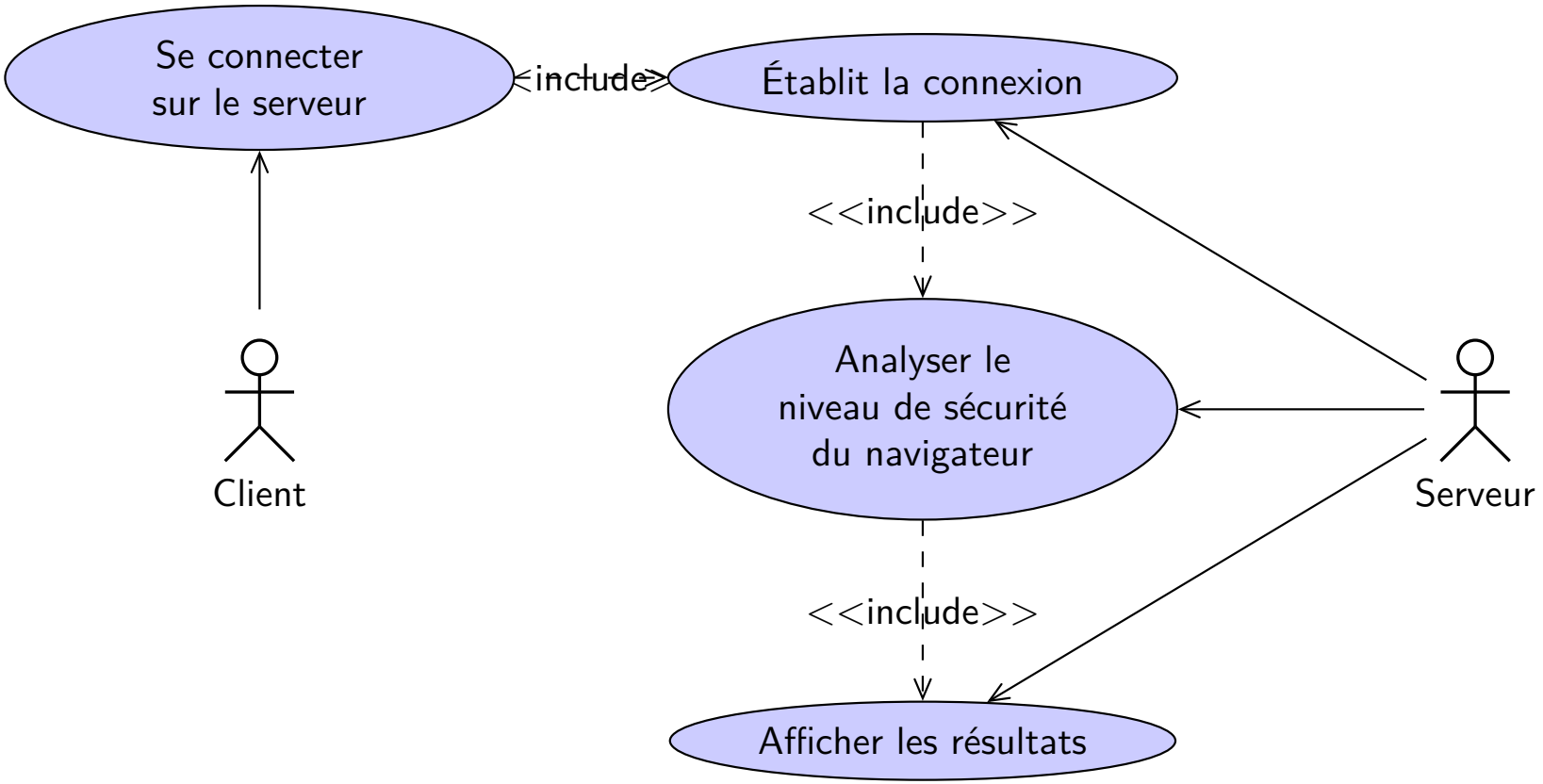
# Cas d'utilisation II



# Cas d'utilisation III



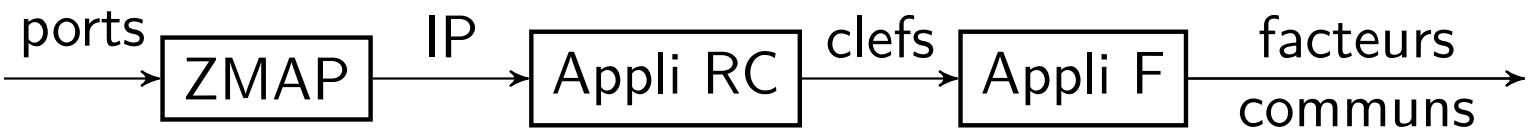
# Cas d'utilisation IV



# Planning de développement I

## Sprint 1 : Récupération des certificats et factorisation

- Outils de récupération des certificats SSL et SSH.
- Outils de factorisation des clefs cryptographiques.



# Planning de développement II

## Sprint 2 : Audit d'OpenSSL

- Détermination des fonctions à auditer et des standards associés.
- Développer des outils de tests d'OpenSSL.
- Documentation et présentation des résultats de l'analyse.

# Planning de développement III

## Sprint 3 : Analyse dynamique des navigateurs web

- Serveur HTTPS analysant la poignée de main SSL/TLS.
- Présentation des résultats de l'analyse.