



*"I've hacked into our bank account."*

---

Objectifs & Introduction

—

P-F. Bonnefoi

*Version du 27 septembre 2017*



**Volume horaire 15h**

## Agenda

- ★ mercredi 27 septembre 14h-17h
- ★ mercredi 25 octobre 10h30-12h30
- ★ mercredi 15 novembre 10h30-12h30
- ★ mercredi 22 novembre 14h-17h00
- ★ mercredi 29 novembre 10h30-12h30
- ★ vendredi 1 décembre 14h-17h (Salle Informatique).

**Examen écrit d'1h, *documents non autorisés***



## Un site Web

`http://p-fb.net/master-2/cca.html`

dessus :

- ▷ les supports de cours ;
- ▷ les annales d'examen ;
- ▷ *une version imprimée des supports sera également distribuée.*

## Contact

`bonnefoi@unilim.fr`

Laboratoire XLIM, 123 av Albert Thomas, bureau 421



## Programme du DSCG

### Sécurité des Systèmes informatiques

- Mise en place d'une **architecture de confiance** :
  - ◇ Comprendre le fonctionnement d'une infrastructure à clé publique ;
  - ◇ certificat numérique, signature électronique.
- Prendre les dispositions pour garantir la **continuité de l'activité** :
  - ◇ surveillance des processus ;
  - ◇ analyse des risques ;
  - ◇ mise en place d'outils de protection techniques et juridiques.

## Programme de l'UE

- **Présentation des risques informatiques** :
  - ◇ le panorama de la «cybercriminalité» et des menaces ;
  - ◇ fonctionnement d'un réseau local ;
  - ◇ protection du réseau et du poste de travail ;
  - ◇ analyse des risques et proposition d'une politique de sécurité.
- **Introduction à la cryptographie et application** :
  - ◇ chiffrement symétrique et asymétrique ;
  - ◇ Fonction de hachage ;
  - ◇ Signature électronique ;
  - ◇ Certificat et infrastructure de confiance ;
- **Partie pratique** :
  - ◇ utilisation des certificats et chiffrement/signature du courrier électronique.



### But de l'enseignement

Présenter la sécurité dans le cadre des échanges électroniques qu'ils soient **synchrones** (communication directe avec un serveur, comme un serveur Web par exemple) ou **asynchrone** (remise de courrier, stockage de document).

Les points abordés sont :

- \* **l'authentification** des interlocuteurs ou propriétaires ;
- \* la garantie de **confidentialité** et **d'intégrité** ;
- \* la **signature électronique** et la non répudiation ;
- \* la mise en place de la confiance au travers des **certificats** et des **infrastructures à clé publiques** ;
- \* les **obligations légales** et le référentiel national d'usage ;
- \* les **risques** et les **atteintes** possibles à la fiabilité de ces opérations ;
- \* l'utilisation dans le cadre de son **activité professionnelle** et des règles administratives.

### Objectifs

Maîtriser son **identité électronique** et celle de ses interlocuteurs et assurer la **sécurité de son travail dématérialisé**.

