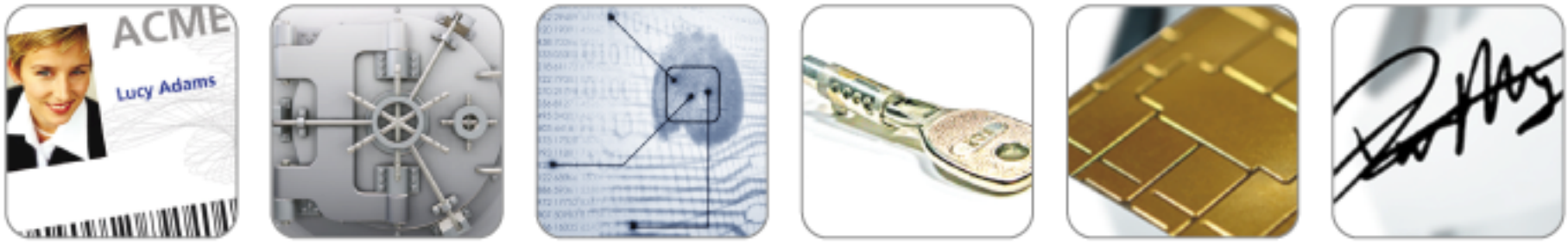
OPENTRUST™
Trust and Security Software



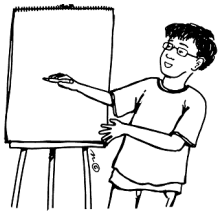
Étude et développement d'un connecteur CMC

Projet de fin d'études

Nicolas MASSÉ

Université de Caen Basse-Normandie

Sommaire



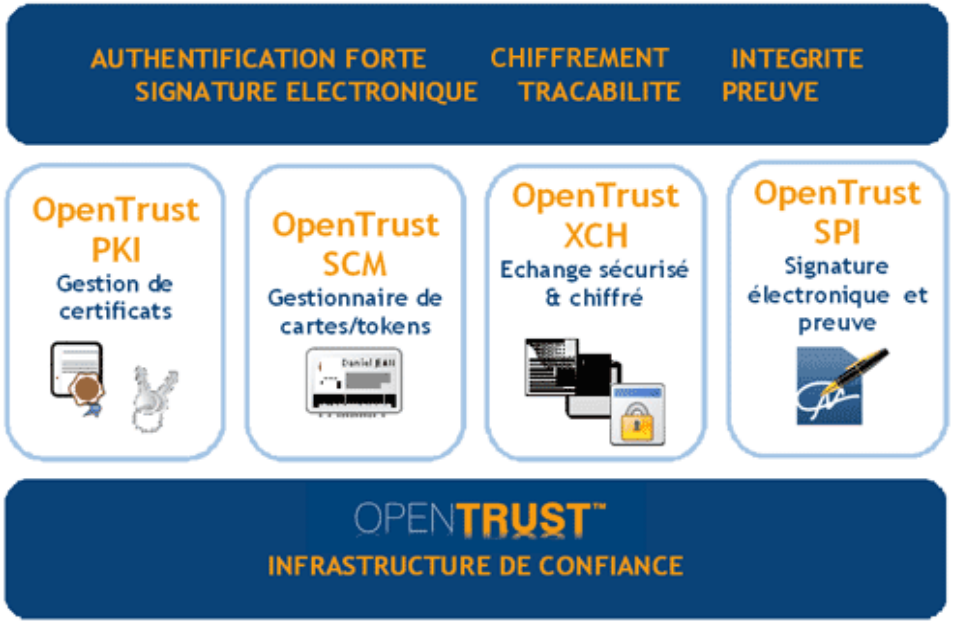
Présentation

Étude

Travail effectué

OpenTrust est un éditeur de logiciels

- Leader des infrastructures de confiance
  - Plus de 100 références dans les grands comptes et administrations
- Objectif : offrir au marché des solutions faciles et rentables rapidement



Présentation

Rappels et définitions

- Une PKI est composée de plusieurs éléments :
  - des AC (Autorité de Certification)
  - des AE (Autorité d'Enregistrement)
  - des EE (Entité d'Enrôlement)
- Un connecteur est une interface qui expose des fonctions de la PKI
- L'enrôlement est le processus de délivrance d'un certificat

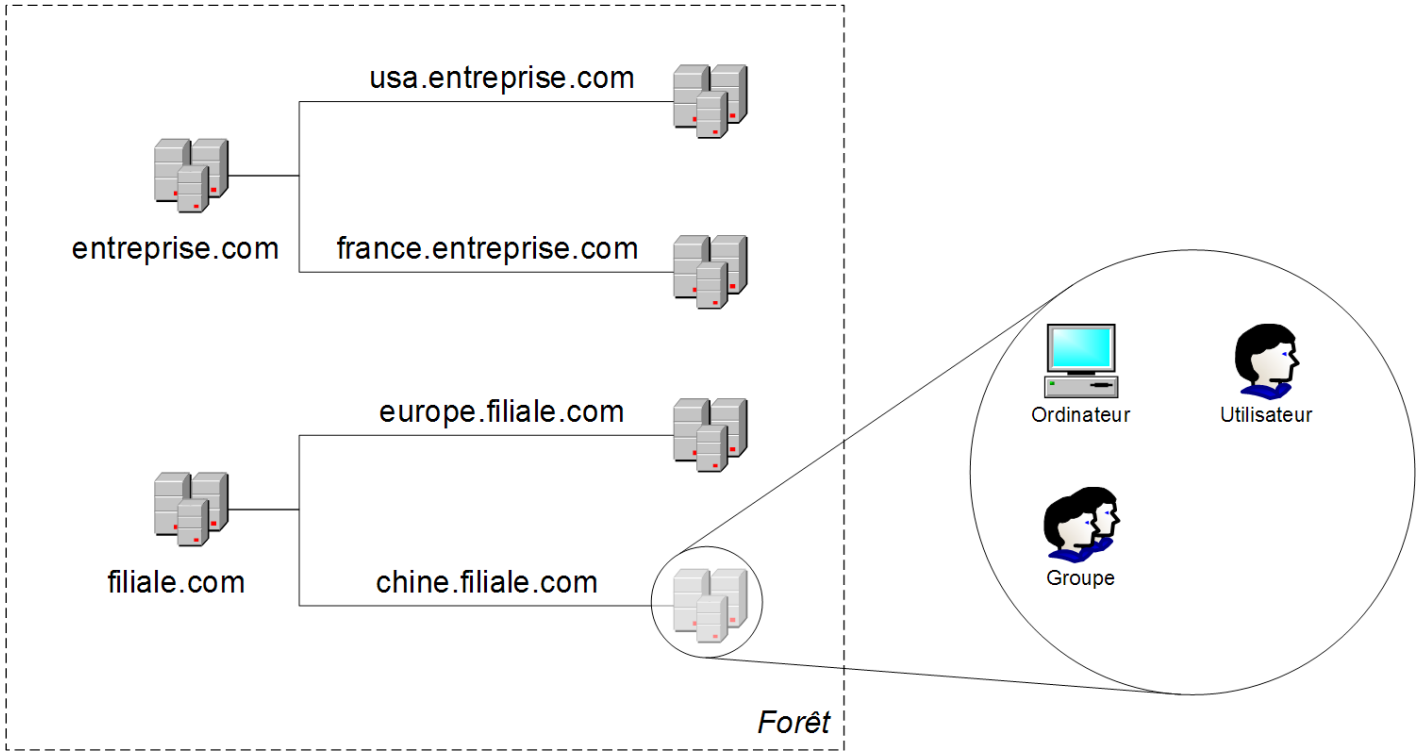
OpenTrust-PKI est une PKI Open Source, souple et robuste.

- Plusieurs modes de fonctionnement
  - mono/bi/tri machine
- Plusieurs modes de délivrance
  - Centralisé / décentralisé
- Différents modes de validation
  - Pré-validation
  - Externe
  - Par un opérateur
- Intégration aux processus de l'entreprise via un connecteur SOAP

Question

Comment enrôler un grand nombre de contrôleurs de domaine [avec un coût minimal] ?

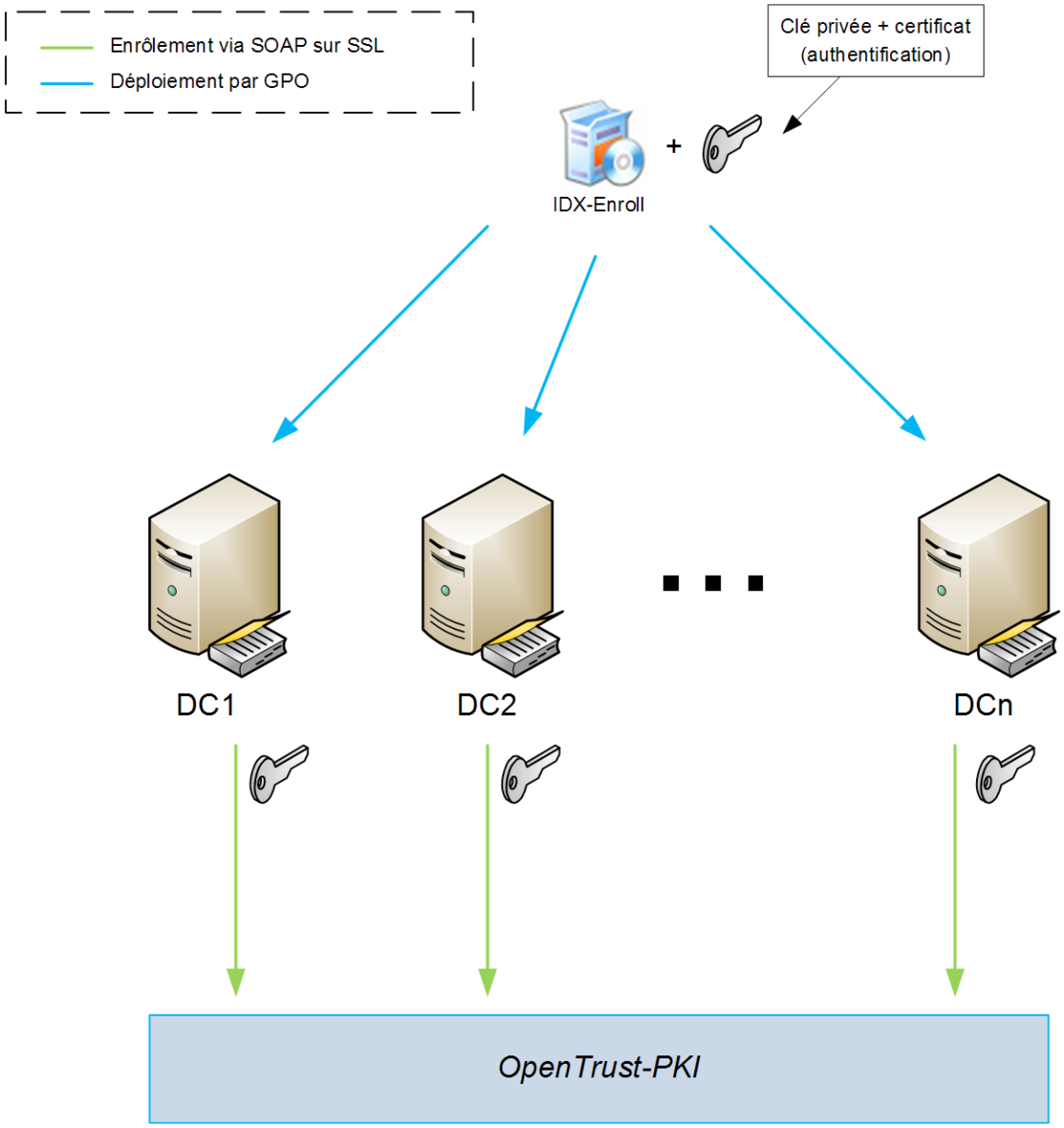
Pourquoi les contrôleurs de domaine ont-ils besoin de certificats ?



C'est un pré-requis à la mise en place du “Smartcard Logon”

Étude

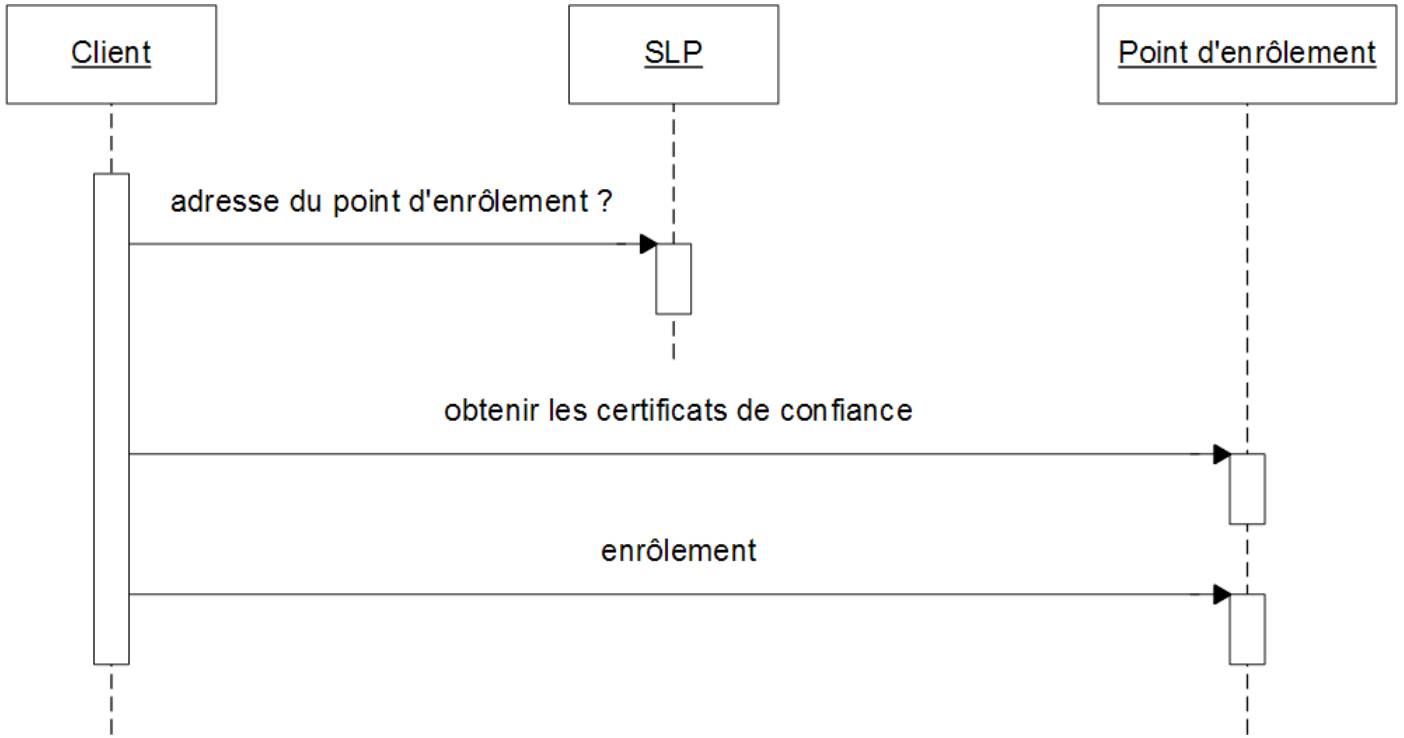
IDX-Enroll est une application d'auto-enrôlement, lourde à déployer



Étude

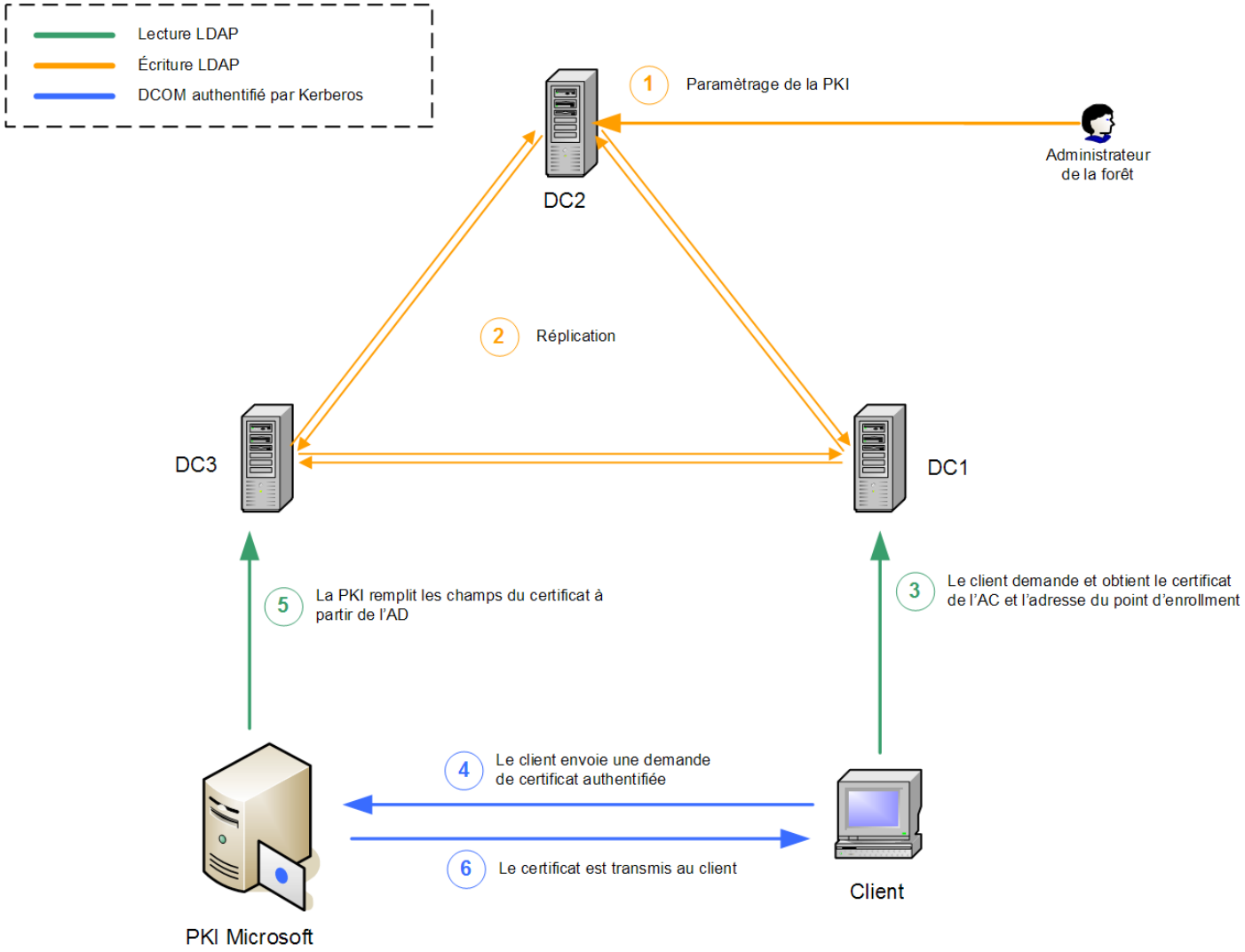
L'auto-enrôlement est à la PKI ce que le DHCP est aux réseaux IP

- **L'auto-enrôlement est un processus automatique (sans intervention humaine) de délivrance d'un certificat.**



Étude

Les clients standards d'auto-enrôlement Microsoft utilisent le protocole CMC



Étude

CMC est un protocole cryptographique d'enrôlement

- CMC: “Certificate Management over CMS”
- CMS: “Cryptographic Message Syntax” (PKCS#7)

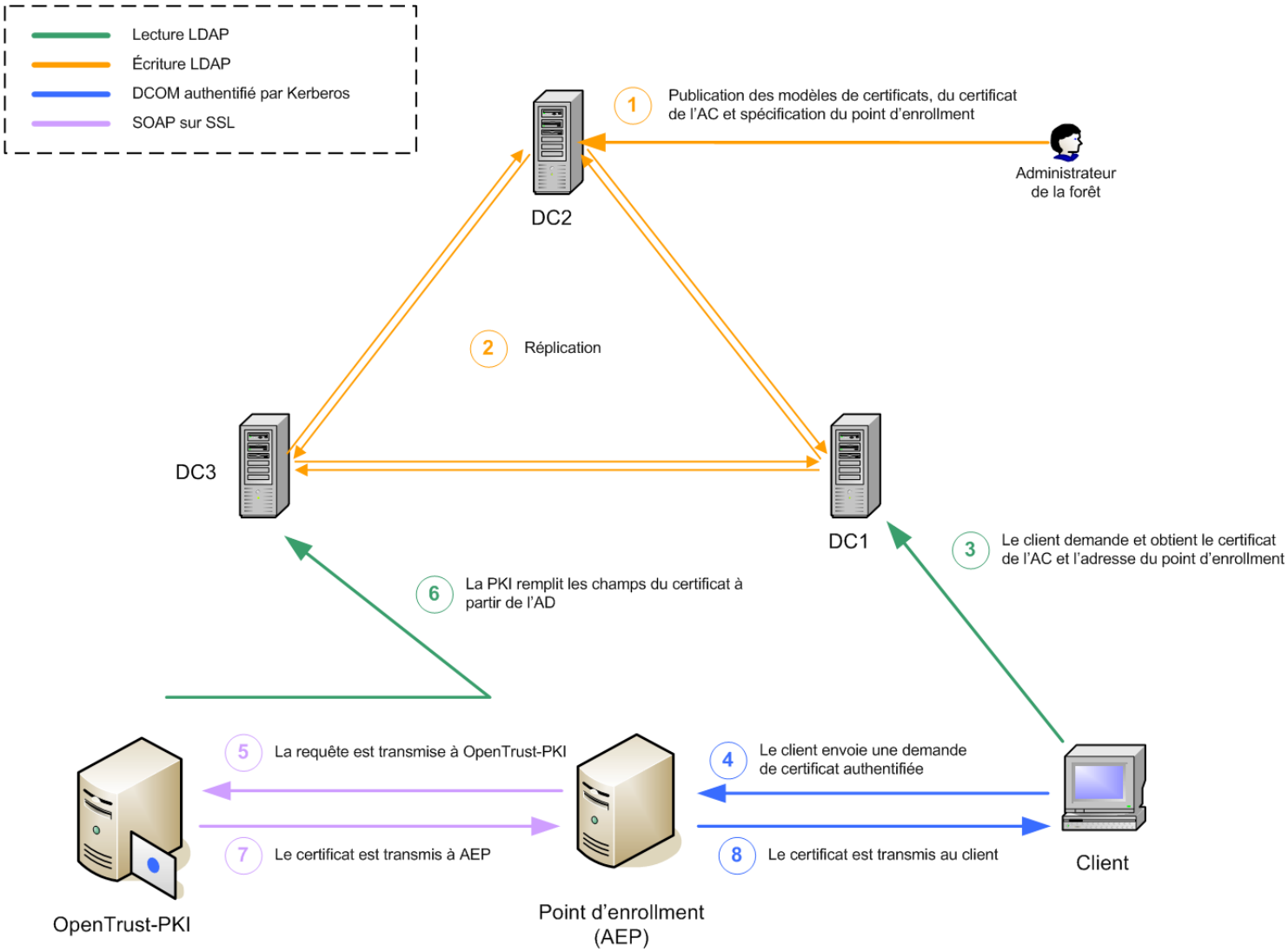
- Deux modes de fonctionnement
  - Simple (PKCS#10 + PKCS#7)
  - Complet (Objet ASN.1 dans un PKCS#7)

- Le mode simple est préféré lorsque c'est possible

- Un protocole complet et complexe
  - La norme n'est (à priori) pas implémentée en totalité par les clients Microsoft

Étude

AEP est un serveur mandataire authentifiant

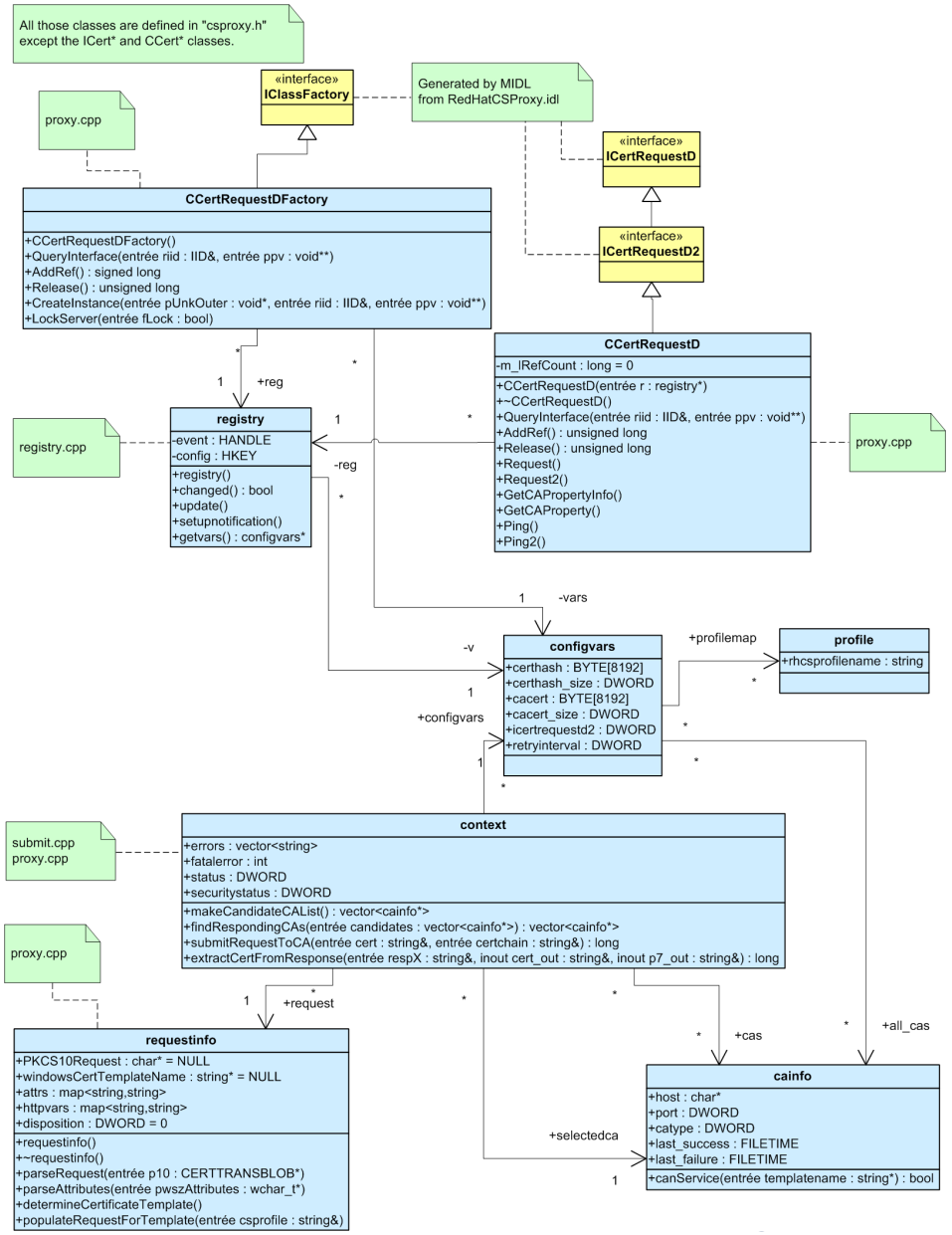


Travail effectué

Diagramme UML d'AEP

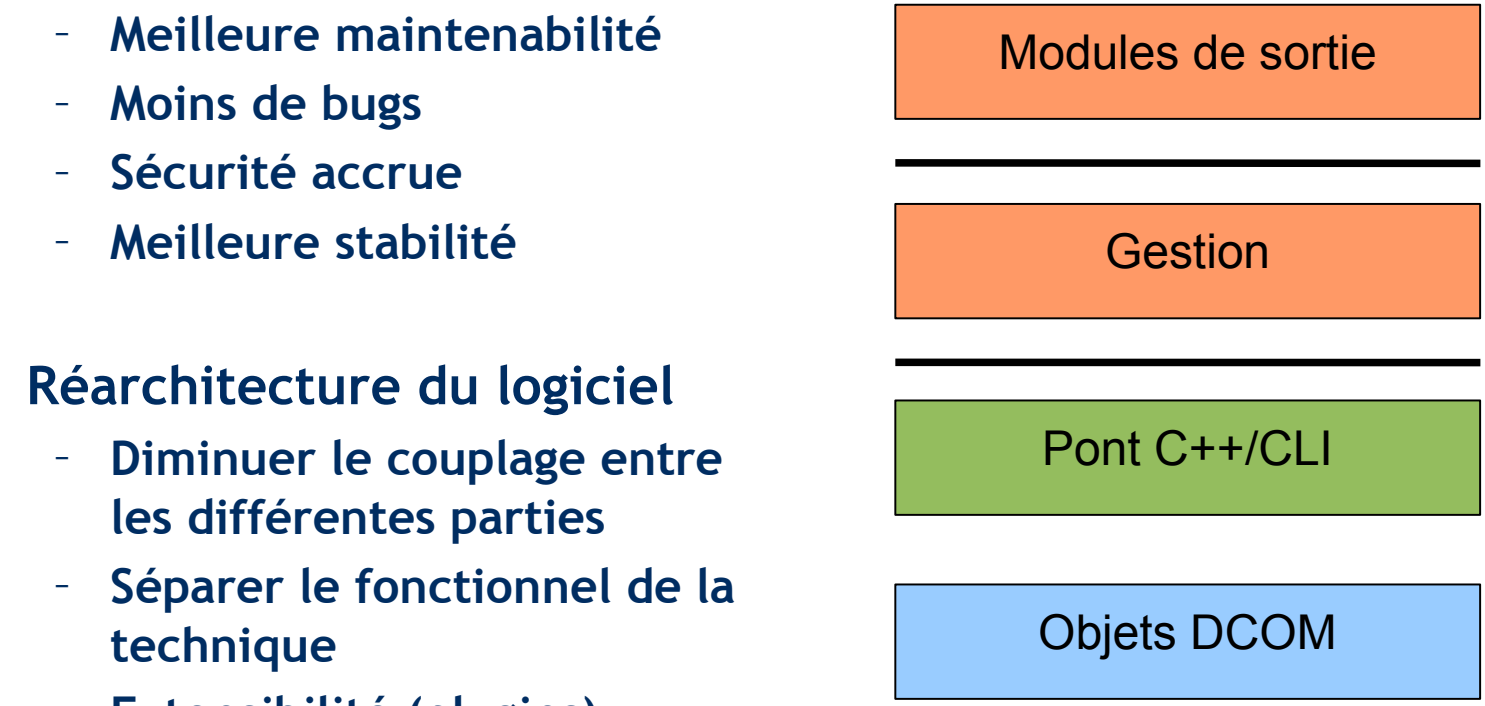
- AEP est codé en C++
- Les fuites de mémoire sont documentées (sic)
- Un diagramme UML inutilement complexe
- Aucune interface

Travail effectué



Les évolutions d'AEP

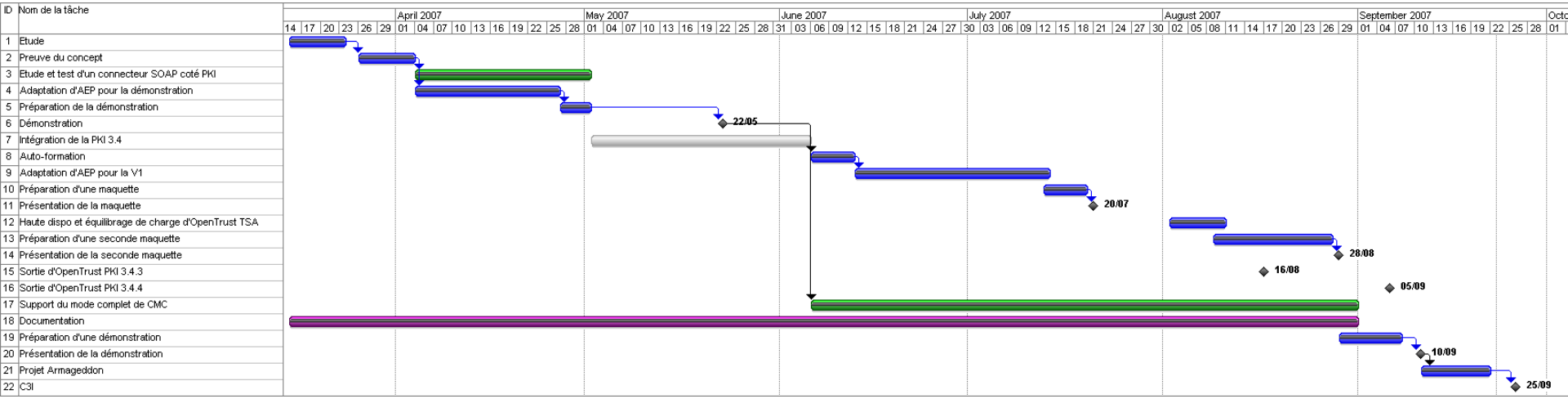
- Migration vers .NET 2.0
  - Meilleure maintenabilité
  - Moins de bugs
  - Sécurité accrue
  - Meilleure stabilité
- Réarchitecture du logiciel
  - Diminuer le couplage entre les différentes parties
  - Séparer le fonctionnel de la technique
  - Extensibilité (plugins)



Travail effectué

Présentation du stage

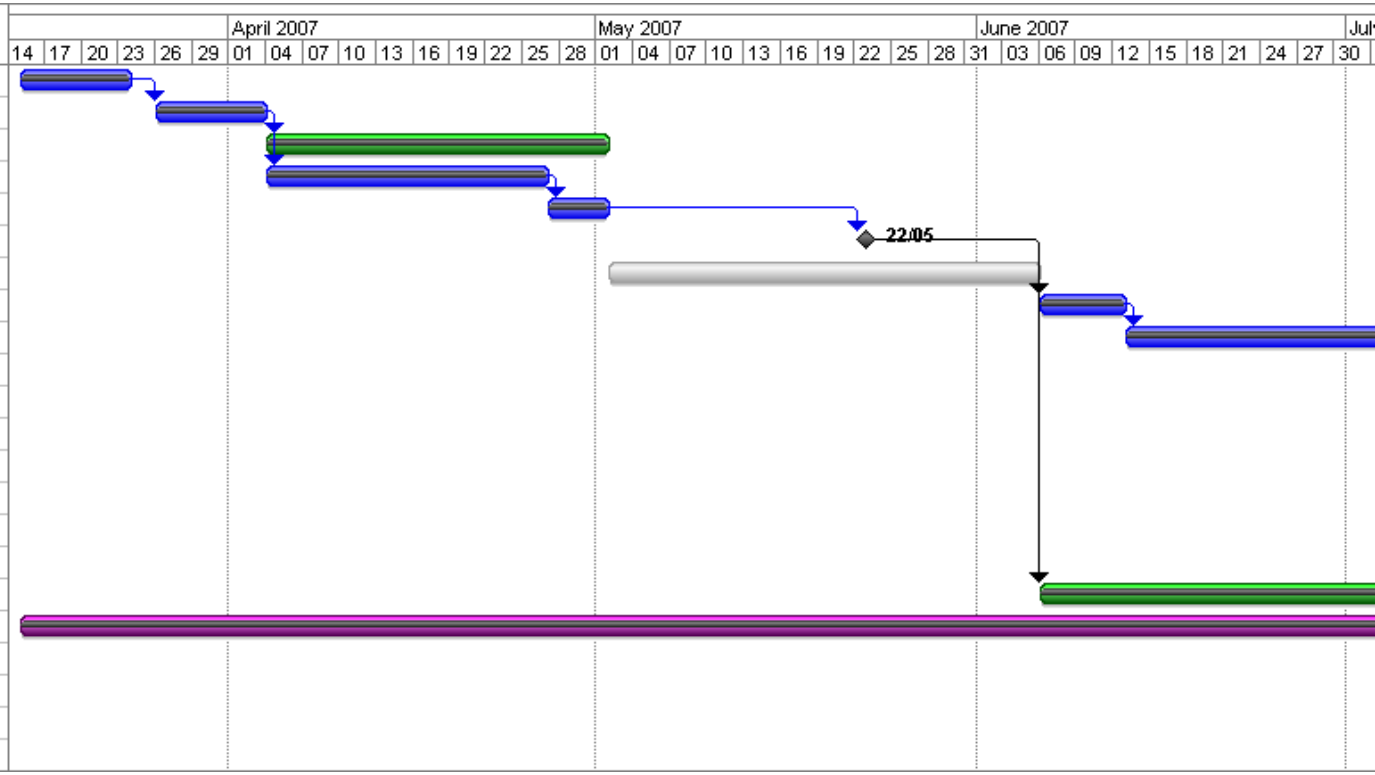
- Objectif : permettre l'utilisation du client Microsoft avec OpenTrust-PKI.
- Durée: 5 mois (+5 semaines d'intégration)
- Travail en équipe
  - avec un autre stagiaire : David



Travail effectué

Organisation temporelle du stage (1)

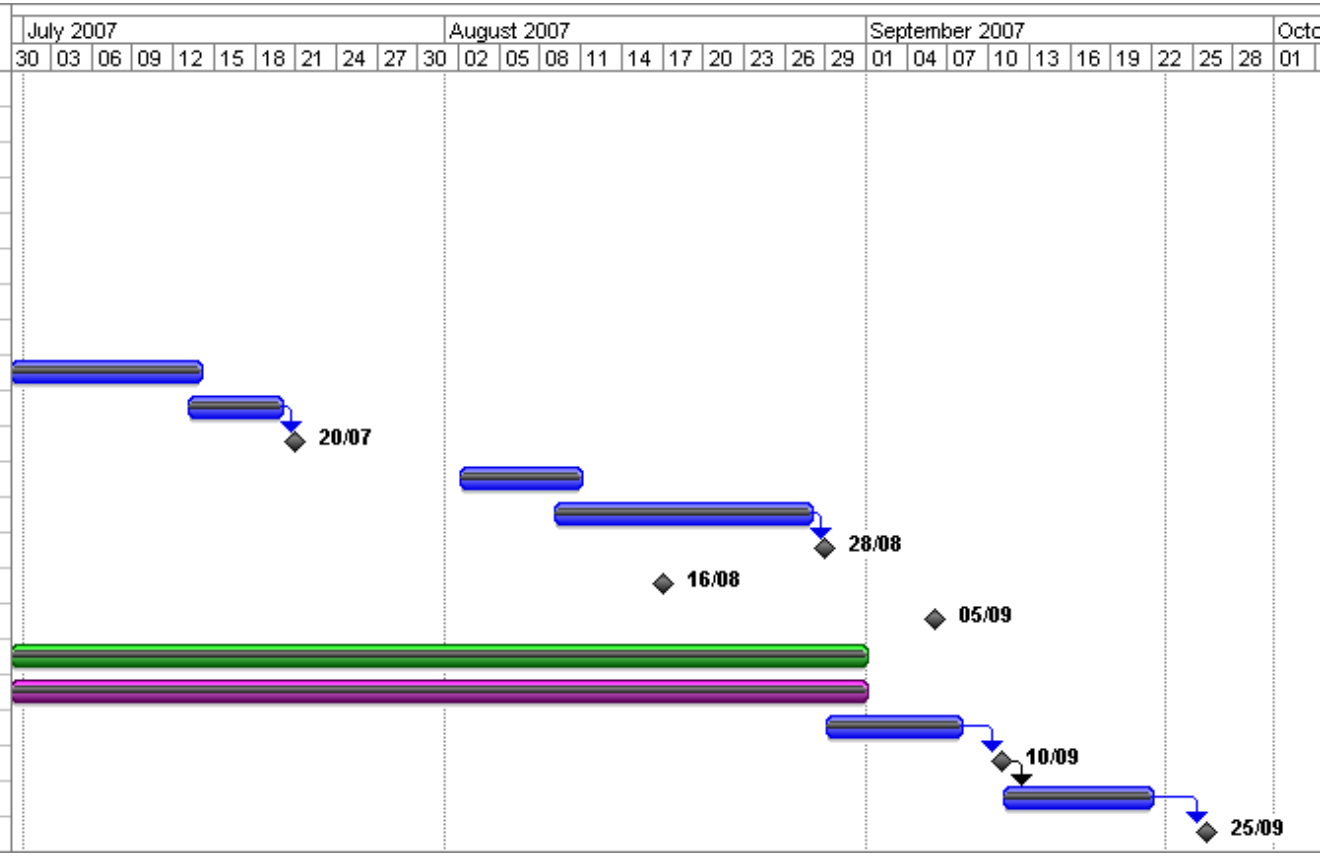
ID	Nom de la tâche
1	Etude
2	Preuve du concept
3	Etude et test d'un connecteur SOAP coté PKI
4	Adaptation d'AEP pour la démonstration
5	Préparation de la démonstration
6	Démonstration
7	Intégration de la PKI 3.4
8	Auto-formation
9	Adaptation d'AEP pour la V1
10	Préparation d'une maquette
11	Présentation de la maquette
12	Haute dispo et équilibrage de charge d'OpenTrust TSA
13	Préparation d'une seconde maquette
14	Présentation de la seconde maquette
15	Sortie d'OpenTrust PKI 3.4.3
16	Sortie d'OpenTrust PKI 3.4.4
17	Support du mode complet de CMC
18	Documentation
19	Préparation d'une démonstration
20	Présentation de la démonstration
21	Projet Armageddon
22	C3I



Travail effectué

Organisation temporelle du stage (2)

ID	Nom de la tâche
1	Etude
2	Preuve du concept
3	Etude et test d'un connecteur SOAP coté PKI
4	Adaptation d'AEP pour la démonstration
5	Préparation de la démonstration
6	Démonstration
7	Intégration de la PKI 3.4
8	Auto-formation
9	Adaptation d'AEP pour la V1
10	Préparation d'une maquette
11	Présentation de la maquette
12	Haute dispo et équilibrage de charge d'OpenTrust TSA
13	Préparation d'une seconde maquette
14	Présentation de la seconde maquette
15	Sortie d'OpenTrust PKI 3.4.3
16	Sortie d'OpenTrust PKI 3.4.4
17	Support du mode complet de CMC
18	Documentation
19	Préparation d'une démonstration
20	Présentation de la démonstration
21	Projet Armageddon
22	C3I



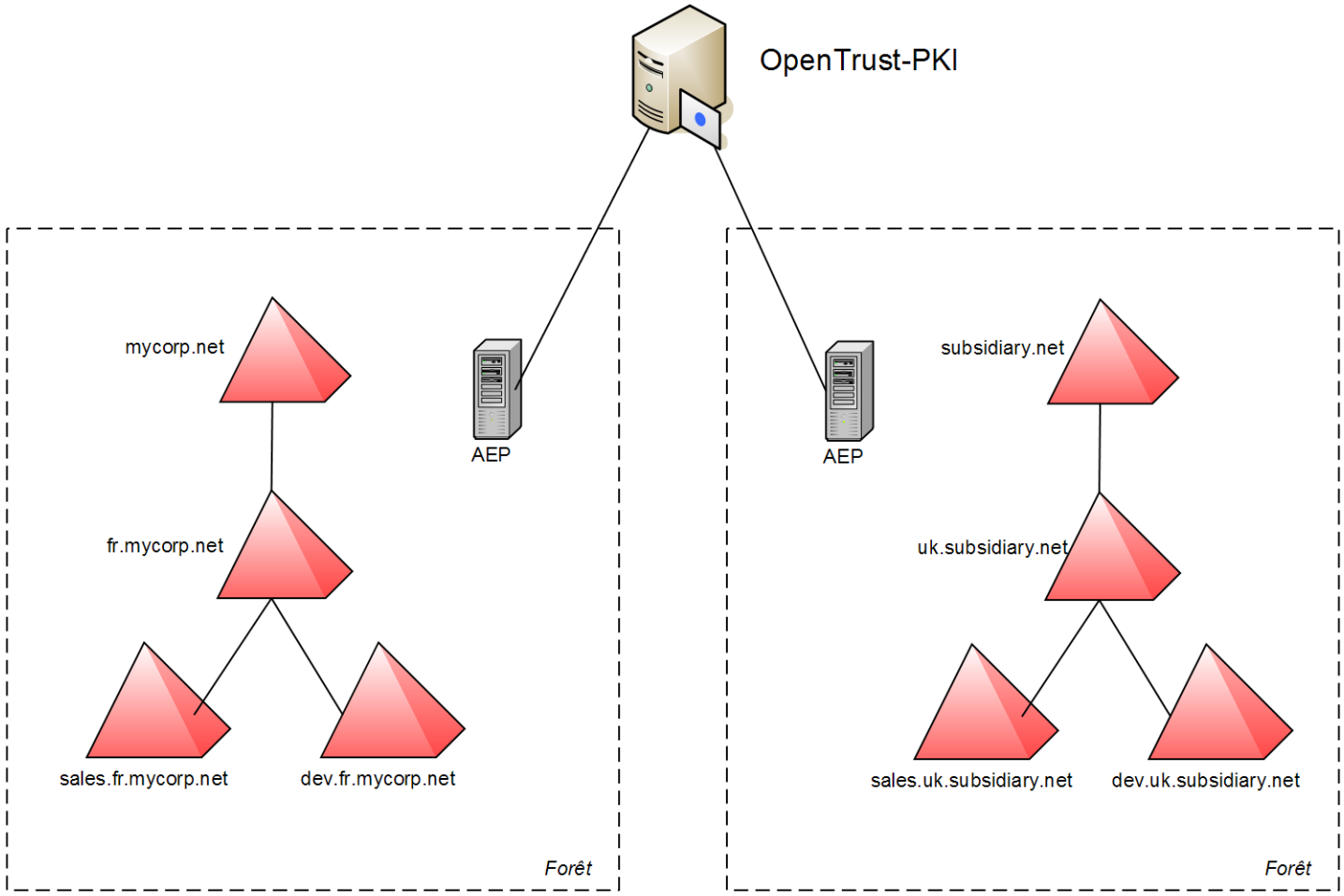
Travail effectué

Les problèmes que j'ai rencontrés sont dûs à un manque de documentation

- Interfaces d'enrôlement non documentées
  - Aide de Steve Parkinson
  - Méthodologie “Hypothèse / expérience”
- Technologie DCOM dépréciée et peu documentée
  => Lecture de “Professionnal DCOM Programming”
- Programmation Windows difficile
  => Lecture de “The .NET developer's guide to windows security”
- Déverminage délicat
  => Utilisation de Procmon, Wireshark, dumpasn1

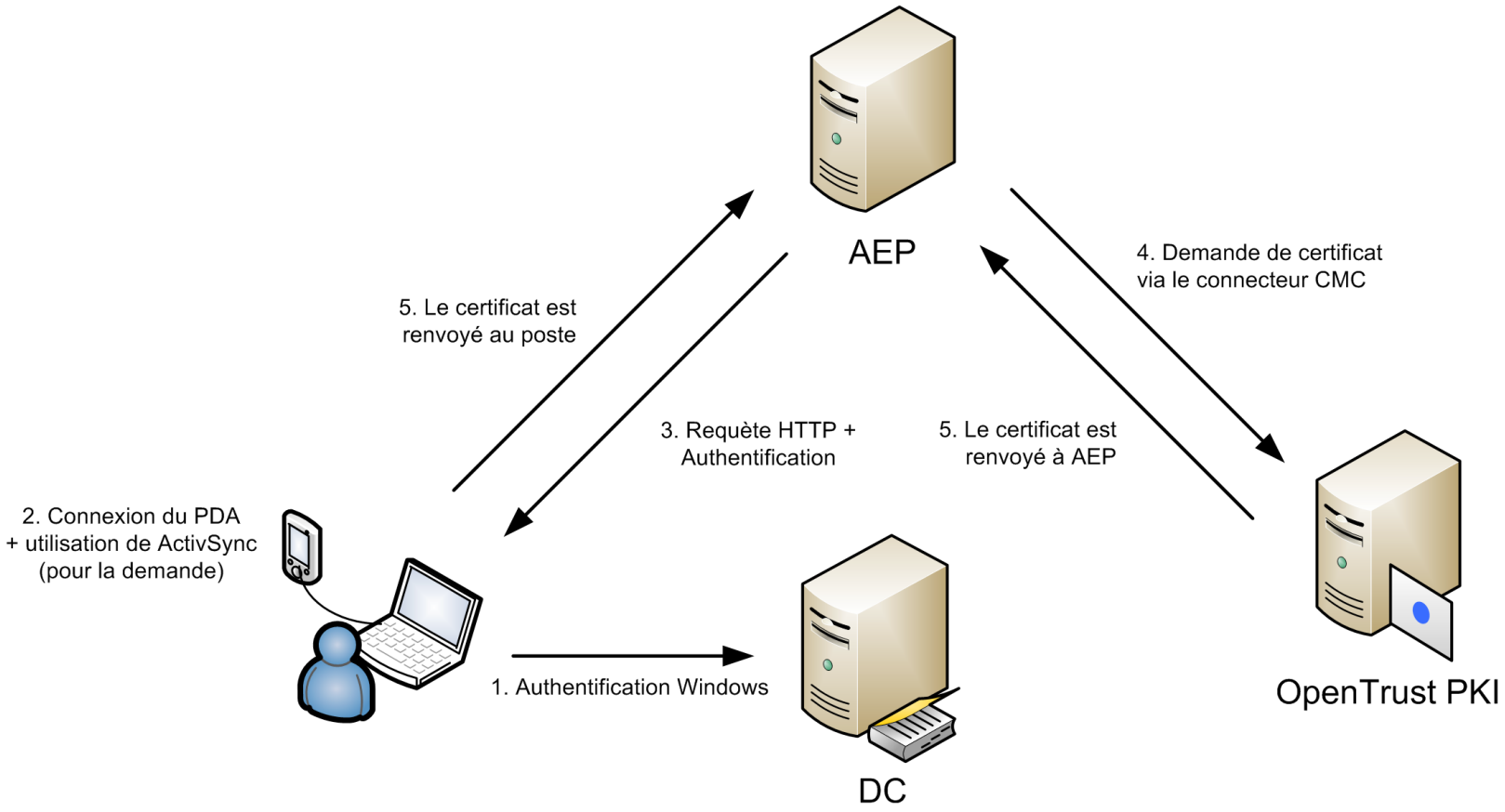
Travail effectué

Avantages de la solution



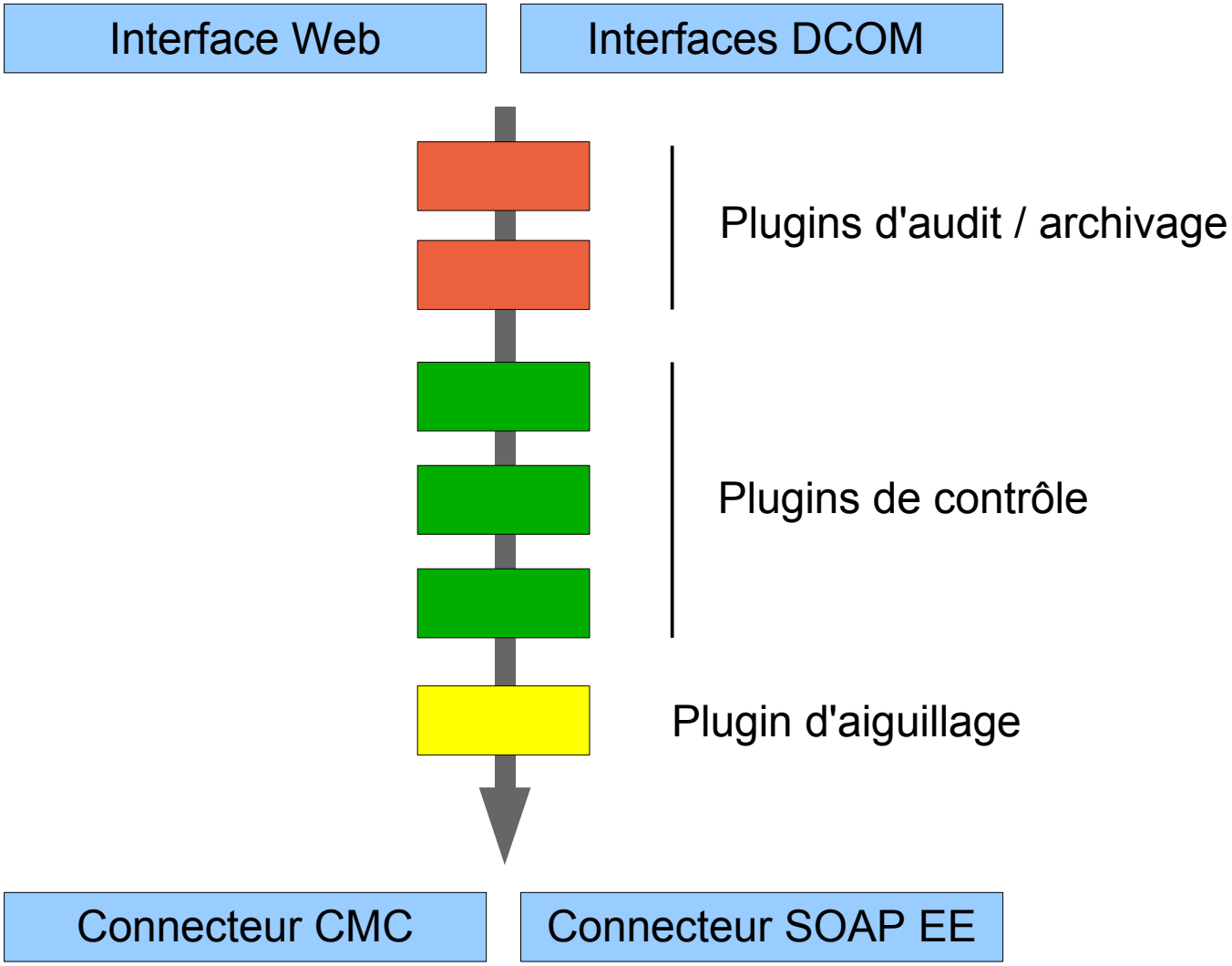
Travail effectué

Et bien plus encore...



Travail effectué

The next step



Travail effectué

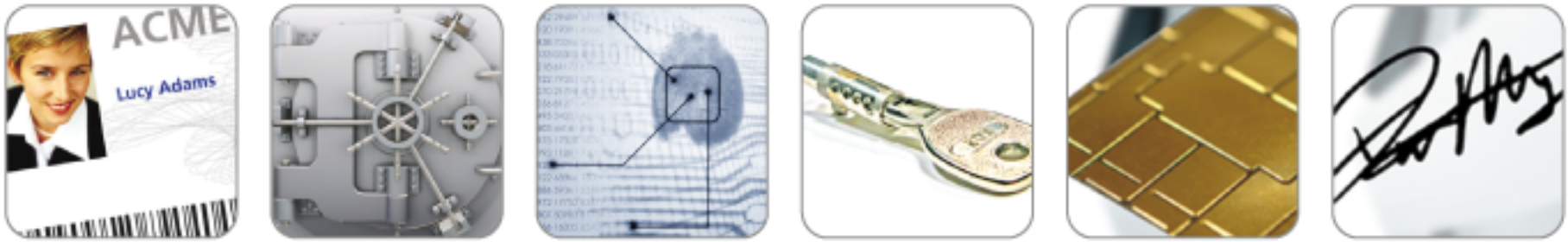
Bilan et résultats

- Connaissances acquises
  - Sécurité Windows
  - Programmation Win32
  - Réseaux Windows
  - SOAP
  - DCOM
  - Perl
  - .NET
  - Produits OpenTrust
  - Périmètre fonctionnel de la PKI

- Apport pour OpenTrust
  - Intégration de la PKI 3.4
  - Un produit industriel intégré à l'offre OpenTrust

- Compétences développées
  - Organisation
  - Communication
  - Génie Logiciel
  - Travail en équipe

Vers de nouvelles aventures...



Étude et développement d'un connecteur CMC

Projet de fin d'études

Nicolas MASSÉ

Université de Caen Basse-Normandie