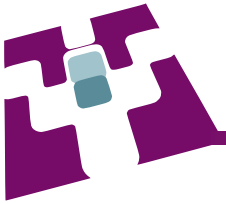
OffPAD – Objet Personnel d'Authentification Hors-ligne appliqué aux hôpitaux et banques en ligne

Denis Migdal

Normandie Université
ENSICAEN - CNRS – Université de Caen Normandie
FRANCE



Projet OffPAD

Projet Eurostar (E !8324, 2013-2017)

- Participants : GREYC, Université d'Oslo, TazTag, TellU, Vallvi ;
- Suite du projet Lucidman (Eureka n°7161, 2011-2013) ;
- Gestion d'identité et d'authentification côté utilisateur.

Démonstrations :

- ACM CCS 2016 (Vienne, Autriche)
- Fête de la science (Caen, 2016)

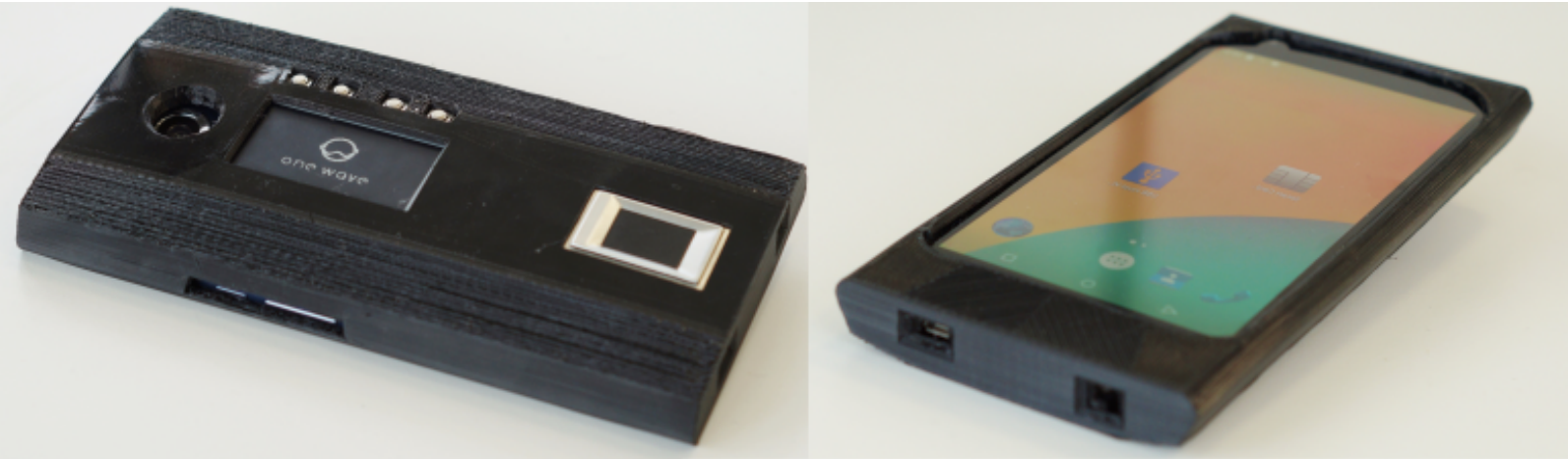


FIGURE 1 – Photos de l'OffPAD v.1

Principes :

- Les clients peuvent être corrompus.
- Les utilisateurs ont plusieurs identités.
- L'authentification doit rester ergonomique.
- Pas d'objet supplémentaire.

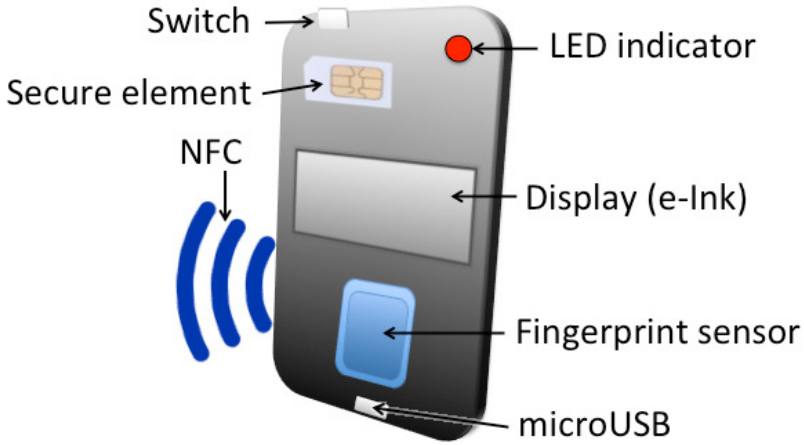
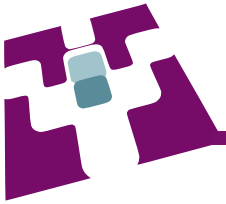


FIGURE 2 – Schéma des composants OffPAD v.1

Fonctions :

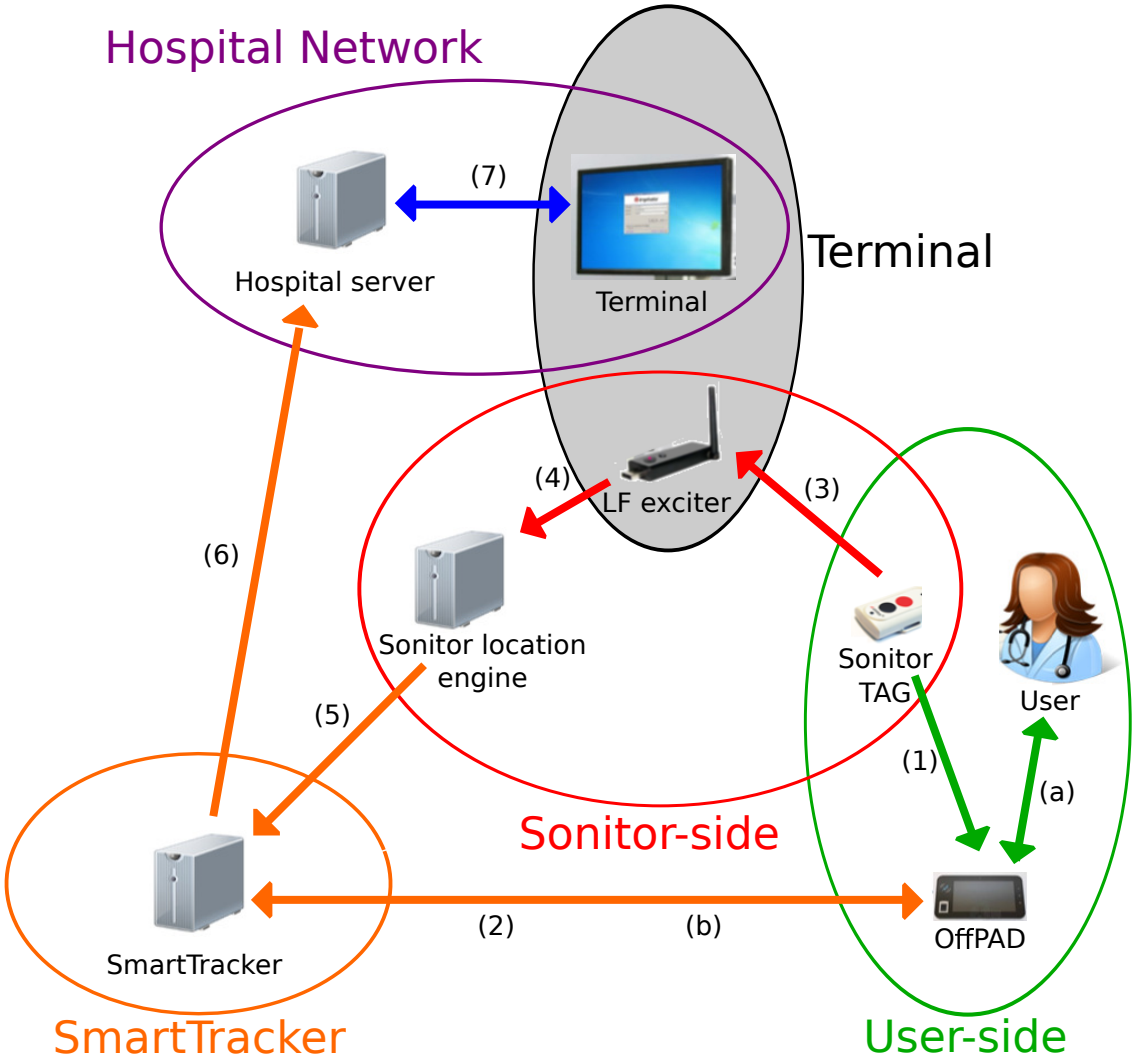
- Authentification du porteur ;
- Gestion de certificats ;
- Signature et vérification ;
- Affichage des informations sensibles ;
- Enrôlement biométrique.



eHealth

Motivations :

- Environnement mouvementé.
- Sécurité et confidentialité des dossiers médicaux.
- Connexions/déconnexions, chronophage et distractif.
- Travail nomade, mais postes fixes.
- Travail collaboratif.


Hospital Network
Hospital server
(7)
Terminal
Terminal
LF exciter
(4)
(3)
(6)
Sonitor location engine
Sonitor TAG
User
(5)
(1)
(a)
Sonitor-side
SmartTracker
(2)
(b)
OffPAD
SmartTracker
User-side

Types d'authentifications :

- Syntaxique ;
- Sémantique ;
- Cognitive.

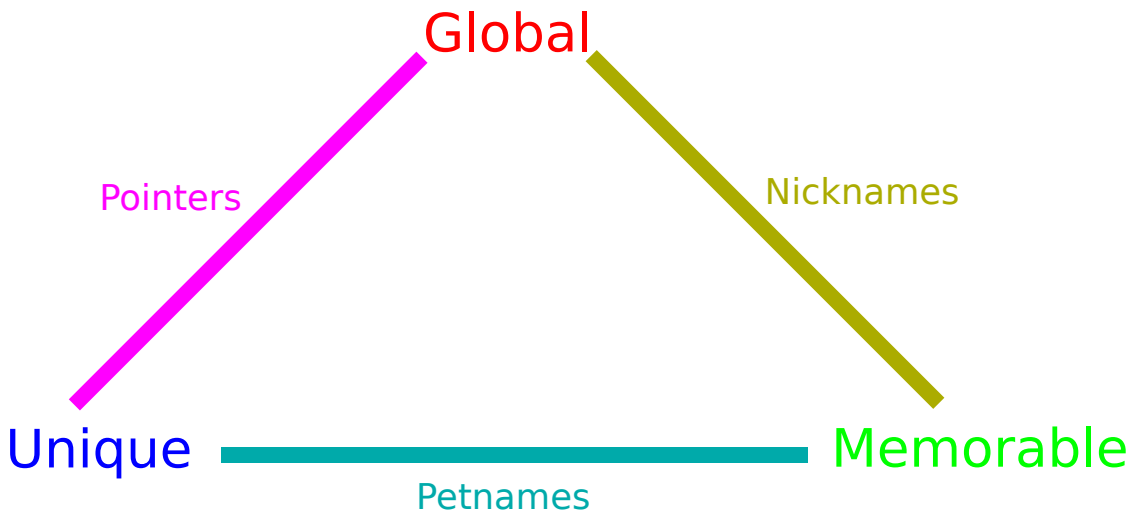


FIGURE 3 – Triangle de Zooko

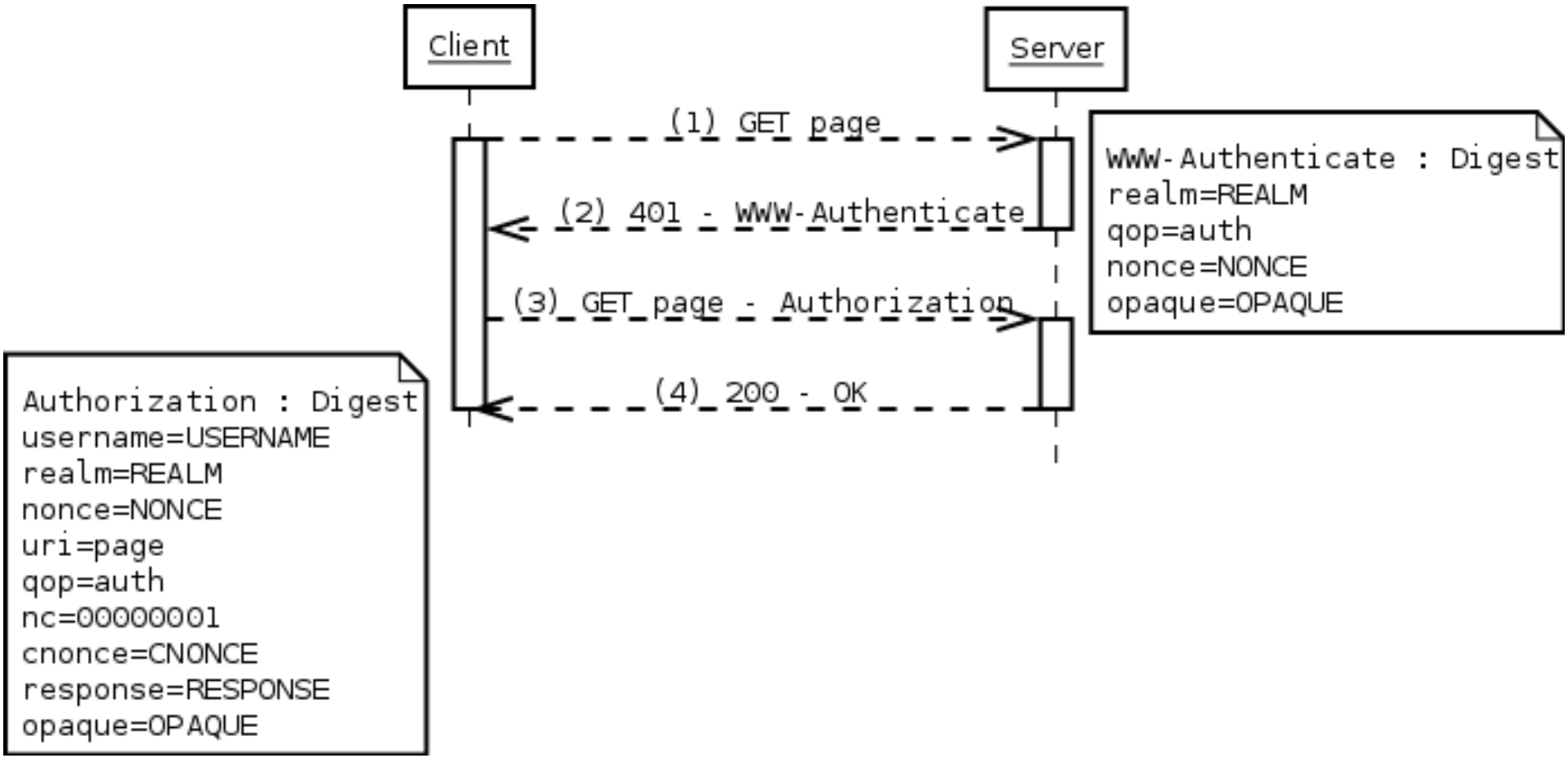


FIGURE 4 – HTTP DAA

OffPAD – Objet Personnel d'Authentification Hors-ligne appliqué aux hôpitaux et banques en ligne

Denis Migdal

Normandie Université
ENSICAEN - CNRS – Université de Caen Normandie
FRANCE