# Offline Personal Authenticating Device applied in Hospitals and E-banking - OffPAD

Denis Migdal, Christian Johansen, Audun Jøsang

# Offline Personal Authenticating Device Applied in Hospitals and e-Banking

OffPAD

## Motivation

The concept of Lucidman (Local User-Centric Identity Management) is an approach to providing scalable, secure and user friendly identity and authentication functionalities.

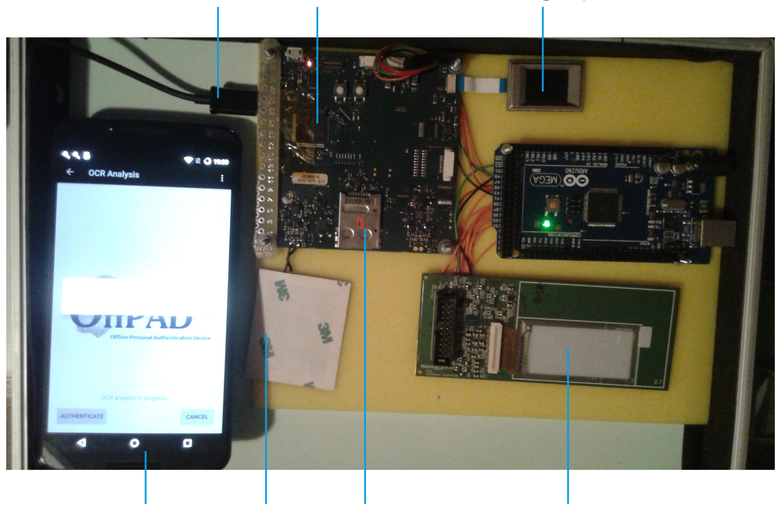
In this context we demonstrate the OffPAD as a trusted device to support different forms of authentication.

The Lucidman/OffPAD approach consists of locating the identity management and authentication functionalities on the user side instead of on the server side or in the cloud.

OffPAD aims to strengthen authentication assurance, improves usability, minimizes trust requirements, and has the advantage that trusted online interaction can be achieved even in the presence of malware infection of client platforms.

A video for this demo is available online.

## OffPAD device




Prototype OffPAD version 1 .


Nexus Phone jacket/cover designs OffPAD version 2 .

## Features

**Portability:** OffPAD is designed as a phone cover connected to its host with a standard micro-USB interface. This makes the OffPAD a portable object, but not a second electronic object in the user's pocket.

**Biometrics:** Unlocking the OffPAD is currently done through fingerprint biometrics.

**Usability:** OffPAD is intended to increase security assurance with minimal interference with the normal tasks of the user, yet automate some of the authentication and identity management related tasks.

**Anywhere security:** OffPAD allows to achieve trusted online interactions even on malware infected client platforms like the Android OS.

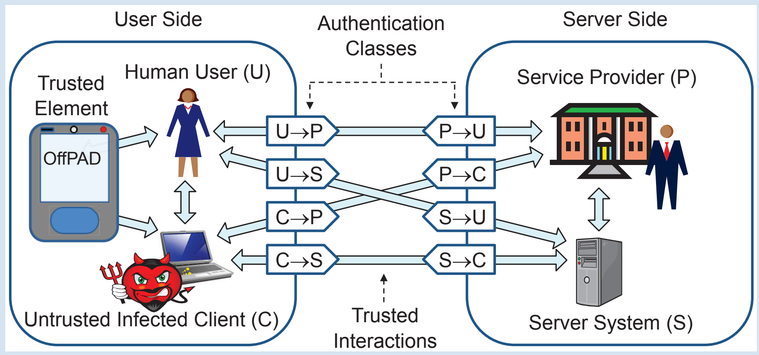
## Links

Detailed Technical Report | Video | offpad.org

## Authentication Classes and Types

### Authentication Classes

The distinction between a system entity (client or server) and a legal/cognitive entity (human or organisation) brings into play multiple entities on each side in the client-server model.




Trusted interactions in the presence of malware-infected clients.

### Three authentication types

**Syntactic** being the simplest, including X.800 certificates, which, e.g., does not prevent phishing attacks since the relying party is indifferent to the identity of the certificate owner;

**Semantic** authentication includes syntactic and moreover the verification by the relying entity that the remote entity has semantic characteristics that are compliant with a specific security policy;

**Cognitive** being the richest, requiring the relying party to have cognitive reasoning power, such as in humans or advanced AI systems. Cognitive authentication effectively prevents phishing attacks as users recognise the server identity, spotting a malicious owner of a legitimate certificate accepted by the browser.

## Hardware and Firmware specifications

### HW specs.

| Component | Description / Model |
|---|---|
| Controller | STM32F401 ARM Cortex-M4 32b MCU+FPU, 105 DMIPS, 256KB Flash / 64KB RAM |
| Secure display | e-Ink 2.5 inches |
| NFC transceiver | NPC1002A2EV, NFC Forum Certified |
| Secure element | Java Card / Global Platform compliant, ST33FIMFF,ST Micro |
| microUSB interface | USB OTG 2.0 (High speed) |
| Fingerprint sensor | FPC1020 Touch Fingerprint Sensor, Pixel matrix 192x192 @502 dpi |
| 3 states switch | Mechanical switch: On / Off / Maintenance |
| Flash memory | 16GB for private/secure storage |

### Firmware / API specs.

**User Authentication** by performing a biometric authentication of the holder.

**Manage certificates** in OffPAD's certificate store to check signature, s.a. for authenticating service provider's identity.

**Sign and check signature** using the OffPAD's holder private key (unlocked after successful holder's authentication).

**Show sensitive information** using the e-Ink display or the multi-color LED.

**Biometric user enrolment** on the OffPAD according to the specified biometric modality.

### Assumptions:

- We assume that the sensors integrated in the OffPAD are secure.
- OffPAD still makes use of the host phone for other sensors, like camera, thus a malware on the phone can communicate false information to the OffPAD.
- OffPAD also asks the host phone for the heavier computations, e.g., for OCR. However, all these inputs from the phone are considered in our scenarios as untrusted.
- The OffPAD is a trusted device, i.e. assumed to function as intended and to be adequately protected against relevant attacks. OffPAD jacket is designed to withstand physical or software tempering.
- OffPAD is considered offline, meaning that communications follow controlled formats, during short and restricted time periods, not involving wireless broadband capabilities.
- Being offline eliminates exposure to Internet threats. Thus we assume that attackers are unable to exploit bugs in OffPAD's firmware and applications.

## Demonstrators

**Data-US:** Authentication of user Data by the Service provider, based on OCR (Optical Character Recognition), alternatively displayed on the OffPAD e-Ink screen.

**SU:** Server authentication by the User, based on petname systems managed by the OffPAD.

**US:** User authenticated by the service provider, based on an extended challenge-response protocol XDAA (HTTP Extended DAA) between the client terminal and OffPAD.

**Auto-login:** Contextual automatic login/off based on indoor location of the OffPAD, using Sonitor's system.

**Multi-login:** Automatic access to a resource conditioned on multiple users authenticated at once, also using TellU Smarttracker system.

**Strong auth.:** Strong authentication required for accessing sensitive information or tasks, using biometric fingerprint authentication of the user by the OffPAD.

## Acknowledgements

We thank all OffPAD project members who have either put effort into parts of this demo or have contributed with great ideas or discussions; particularly to:

- Leonard Dallot, Laurent Miralabe, and Guillume Cornet (TazTag, manufacturer of secure mobile hardware),
- Knut E. Husa and Svere Morka (TellU, providing IoT platform and services),
- Marius P. Haugen (U.Oslo),
- Christophe Rosenberger and Estelle Cherrier (ENSI Caen GREYC lab),
- Amir Taherkordi (Sonitor, manufacturer of indoor locating solutions),
- Petter Taugbøl (Vallvi, managing coordinator).

## Presenters

**Denis Migdal**
denis.migdal@ensicaen.fr
GREYC Lab

**Christian Johansen**
cristi@ifi.uio.no
University of Oslo

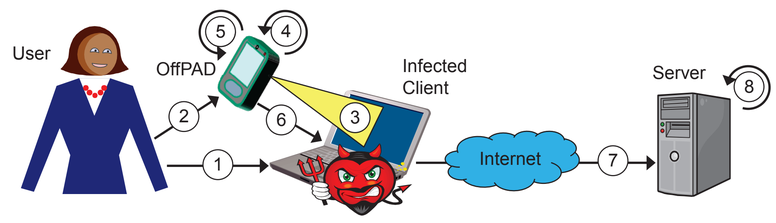
**Audun Jøsang**
audun.josang@mn.uio.no
University of Oslo

Demo given at the 23$^{rd}$ Annual ACM Conference on Computing and Communications Security (CCS 2016), during "Mayor's dinner" in Vienna.

# Offline Personal Authenticating Device Applied in Hospitals and e-Banking

Demonstrators

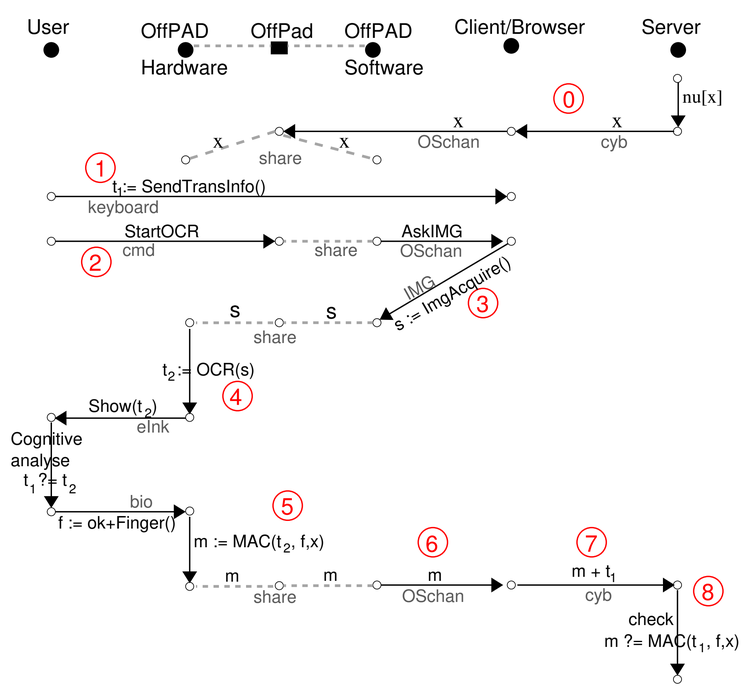
## Data authentication demonstrator




Sequence of messages/actions for data authentication:

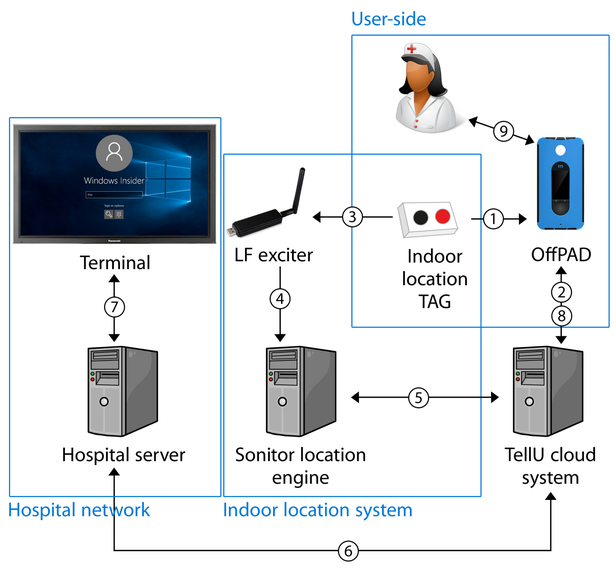
**Nr. Message / action description**

1. User types the transaction data in a browser window on the client computer.
2. User activates the OffPAD to take a snapshot of the browser window.
3. Snapshot is taken of the text displayed in the browser window on the untrusted client.
4. The OCR (or QR code) function recovers the transaction data from the snapshot.
5. MAC generation with the transaction data and the user-password as input.
6. OffPAD sends MAC to client computer.
7. Client computer sends transaction data together with MAC to server.
8. Server verifies that the MAC corresponds to the received transaction data.




**Run** described using Actor Network Procedures.

## eHospital Infrastructure




**OffPAD** to:

- manage User credentials, perform security operations (certificate validation, biometric auth.) ;
- automatic login by interacting with other systems ;
- perform strong authentication using biometrics ;
- convey trustworthy information to user.

**Decision support system** provided by TellU partner:

- can communicate with OffPAD device ;
- manage location information of the OffPAD device
- manage decision processes, e.g., based on location
- interact with hospital system.

**Hospital network** includes:

- Terminals, where users (nurses, doctors, patients) can login to see specific information (like current task to be done, or access to personal TV setup) ;
- hospital/health information Servers (e.g., Access Control engines).

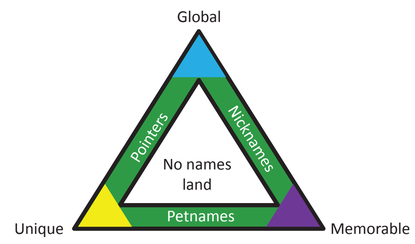
**Indoor location system** provided by Sonitor partner:[a]

- TAGs to locate the users ;
- LF exciters to locate the fixed terminals ;
- Sonitor indoor location server.

[a] Can be replaced by other systems, e.g., based on wireless points.

## User and Server authentication and HTTP XDAA

### Petnames systems for Cognitive authentication




Zooko's triangle for Petname Models.

Bryce "Zooko" Wilcox-O'Hearn described in 2005 **three** fundamental desirable **properties** of names:

- global (like DOIs or URLs) ;
- unique (collision-free within a domain) ;
- memorable (or human-meaningful).

Zooko explains with supporting evidence why *no name space can have all three properties*!

**The Petname Model** consists of two name spaces:

- one of global and unique names (pointers) ;
- one of memorable and unique names (petnames) ;
- mapping a name space of pointers to individual name spaces of petnames, which thereby combines all three desirable properties.

### HTTP Extended DAA (XDAA)

HTTP Digest Access Authentication (HTTP DAA, RFC 7616) is an user authentication protocol :

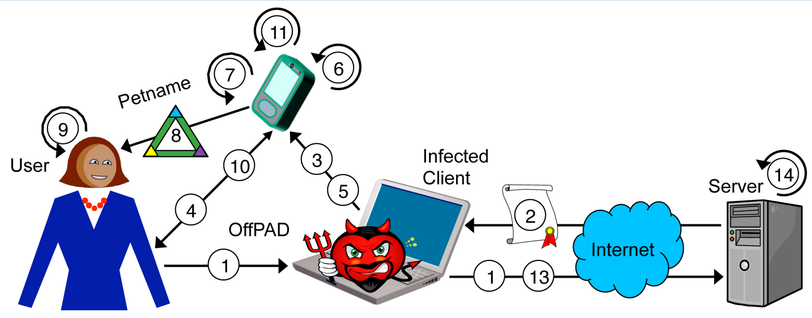
1. client sends a query (HTTP GET) ;
2. server responds with a Challenge (HTTP 401)
3. client prompts for username and password ;
4. client computes the Response ;
5. client sends a new query, with the Response ;
6. server answer the query (HTTP 200).

Response = hash( HA1 ":" Challenge ":" HA2)
HA1 = Hash(username ":" realm ":" password)
HA2 = Hash("GET" ":" uri)

Klevjer, Varmedal, & Jøsang extend HTTP DAA :

- challenge forwarded to the OffPAD ;
- password generated from user biometric ;
- HA1 can be precomputed and stored on the OffPAD.

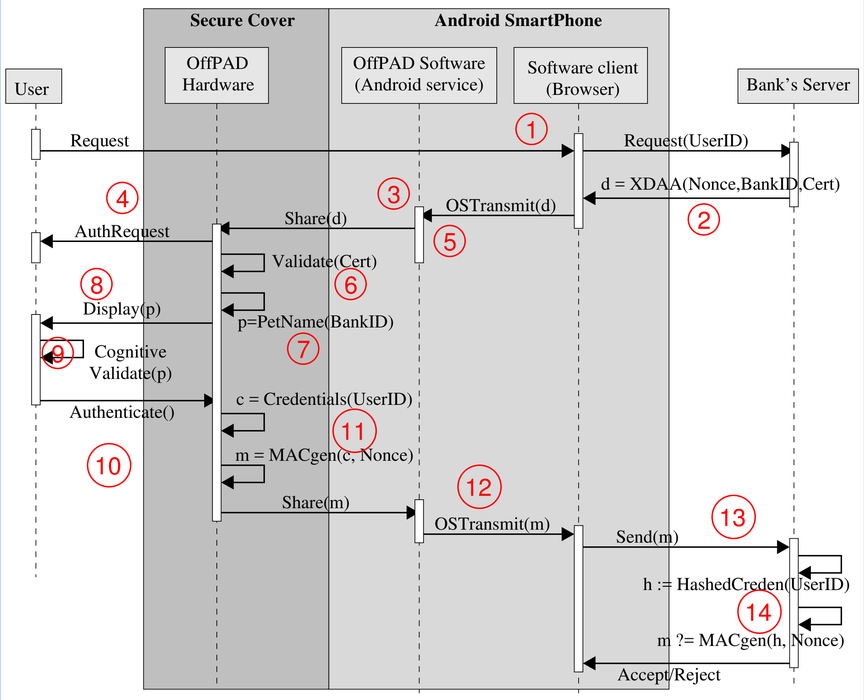
### Mutual authentication using Petnames and XDAA




Sequence of messages/actions for user and server authentication ceremony:

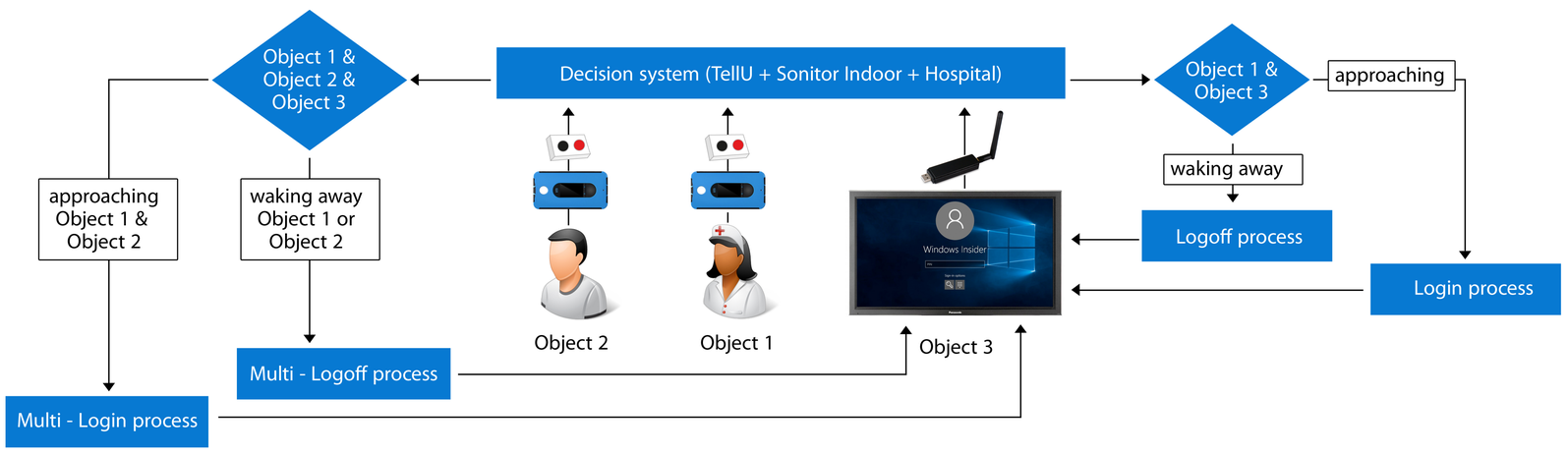
**Nr. Message / action description**

1. User initiates connection with Bank's server through the client/browser (which is not trusted).
2. Server sends HTTP XDAA challenge to client, along with the Bank's ID in a certificate (maybe using DNSSEC).
3. Challenge and BankID are forwarded by browser to OffPAD.
4. OffPAD presents user authentication request to user.
5. Server certificate is forwarded to OffPAD.
6. Server certificate is validated (**syntactic server authentication**).
7. Server certificate/BankID is mapped to petname.
8. Petname is presented to user.
9. User performs **cognitive server authentication**.
10. User approves authentication request.
11. OffPAD computes response to challenge from server.
12. Response is sent from OffPAD to client.
13. Client forwards response to server.
14. Server verifies response which completes user authentication.




Sequence diagram for User authentication ceremony and Cognitive authentication of Server by User.

## Automatic login-logoff and Multi-login




### Pairing and Take in use

- Nurse takes OffPAD in use at beginning of shift by authenticating through biometric fingerprint.
- Device loads user profile and registers to TellU.
- Nurse pairs location TAG to OffPAD device.
- Pairing information sent to TellU system
  Now the TAG tracked by the Sonitor system is known to TellU as being attached to the User that activated the respective OffPAD.

### Context based Access Control

- Indoor location of Objects (Nurse/Patient/ Doctor) tracked in real-time by the Sonitor system.
- When Nurse approaches a Terminal the TellU decision system is notified and a login event is triggered through the Hospital system.
- When Nurse walks away, the TellU system is notified by Sonitor, and triggers a logoff event.
- Continuous biometric authentication methods can ensure that OffPAD is in User's possession.

### Multiple users Access Control

- Both Nurse and Patient are in front of a Terminal.
- TellU system triggers an access control event parametrized by the objects.
- Sensitive information can now be displayed, e.g. Patient Record can be shown only when the Patient is in the room.

### Strong authentication

- Context authentication may be not good enough for some sensitive operations or information, e.g. signing a receipt, or ending a task.
- Hospital system may require the Nurse to authenticate through the OffPAD using biometric fingerprint before allowing access.