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.

**Motivation**

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

**Authentication Classes**

Trusted interactions in the presence of malware-infected clients.

**Hardware and Firmware specifications**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description / Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>STM32F441 ARM Cortex-M4 320 MHz, 160 DMIPS, 256 KB Flash / 64 KB RAM</td>
</tr>
<tr>
<td>Secure display</td>
<td>e-Link 2.5 inches</td>
</tr>
<tr>
<td>NFC transceiver</td>
<td>NFC1020AZEV, NFC Forum Certified</td>
</tr>
<tr>
<td>Secure element</td>
<td>Java Card / Global Platform compliant, ST33FMFPIST Micro</td>
</tr>
<tr>
<td>microUSB interface</td>
<td>USB OTG 2.0 (High speed)</td>
</tr>
<tr>
<td>Fingerprint sensor</td>
<td>FPC1020 Touch Fingerprint Sensor, Pixel matrix 192x192 @502 dpi</td>
</tr>
<tr>
<td>3 states switch</td>
<td>Mechanical switch: On / Off / Maintenance</td>
</tr>
<tr>
<td>Flash memory</td>
<td>16GB for private/secure storage</td>
</tr>
</tbody>
</table>

**Firmware / API specs.**

- User Authentication by performing a biometric authentication of the holder.
- Manage certificates in OffPAD’s certificate store to check signature, e.g., 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 tampering.
- 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), alternately displayed on the OffPAD e-Ink screen.

**SU:** Server authentication by the User, based on petname systems managed by the 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 Mirlalae, and Guillaume Cornet (TurTag, manufacturer of secure mobile hardware),
- Koen E Huis and Sven Marka (TellU, providing IoT platform and services),
- Martin P Haugen (U Oslo),
- Christophe Rosenberger and Estelle Chevrier (ENSI Caen GREYC lab),
- Amir Taberkoudi (Sonitor, manufacturer of indoor locating solutions),
- Petter Taugbøl (ValVi, managing coordinator).

**Presenters**

Denis Migdal
Benjamin Fr
GREYC Lab

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

Audun Jøsang
audun.josang@mn.uio.no
University of Oslo
Offine Personal Authenticating Device Applied in Hospitals and E-Banking

**Sequence of messages/actions for data authentication:**

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.

**Sequence of messages/actions for data authentication:**

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.
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.

**Petnames systems for Cognitive authentication:**

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 (pet-names)
- 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 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 answers the query (HTTP 200).

Response = hash(HA1 + Challenge + HA2)

HA1 = Hash(username : realm : password)

 HA1 can be precomputed and stored on the device.

Klevjer, Yarmeidi, & Jassang 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**

**eHospital Infrastructure**

- **OFPAD**:
  - 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 OFPAD device
- manage location information of the OFPAD 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:

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

**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 mechanisms can ensure that OffPAD is in User’s possession.

**Automatic login-logoff and Multi-login**

- **Paring and Take in use**:
  - Nurse takes OH4PAd in use at beginning of shift by authenticating through biometric fingerprint.
  - Device loads user profile and registers to TellU.
  - Nurse pairs location TAG to OH4PAd device.
  - Pairing information sent to TellU system.
  - Tagged device is monitored and tracked by TellU system.

**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.