FUJITSU

THE POSSIBILITIES ARE INFINITE

Fujitsu mPollux

PalmSign Security Option

White Paper

Fujitsu mPollux Version 2.1

June 2016

Second Edition June 2016

FUJITSU

Table of Contents

1 INTRODUCTION

In the context of e-business, the need for security functions is of ever growing importance. Several different schemes exist for the authentication of the involved parties and communicated messages, or for the insurance of transaction confidentiality and non-repudiation. The problem currently is that as a rule these schemes build on special secure devices and complex infrastructure such as PKI. While the security achieved by such means is high, the threshold for applying such an infrastructure for smaller scale business cases can be high as well.

mPollux™ Security Server provides a range of security solutions from conventional user id – password authentication, telephone call authentication to full-scale PKI based security. **mPollux PalmSign™** is a Security Option that provides security for applications when high level security with biometric technology is desired or required. The security provided by **mPollux PalmSign™** is based on biometric authentication using palm vein's feature, palm vein pattern is differed from one to another, which is the proper technology of Fujitsu Ltd.

The **mPollux PalmSign™** option is a general-purpose subsystem allowing any application to use authentication.

2 MPOLLUX PALMSIGN™ FUNCTIONALITY

The mPollux PalmSign™ Security Option implements a Fujitsu's palm authentication technology which is using Fujitsu's PalmSecure sensor and SDK. The mPollux PalmSign™ option adds enrollment, authentication and management functions with utilizing Fujitsu's PalmSecure sensor and SDK in order customers to adapt the technology to their existing systems easily.

There are both server and client components. The client's main functions are to control a sensor and send the authentication data or registration data to the server, while the server component manages storing the data, identification/verification and logging.

About the registration/identification/verification, the supported features are,

- **1:N match,** identification without any identifier but biometric
- **1:1 match**, verification is required to be done with Personal identifier
- **Two Hands,** able to register two hands with one personal identifier. With this feature, user can use each of the hands in identification/verification phase.

2.1 PALMSIGN™ CLIENT

PalmSign Client provides the features as follows,

- **Registration,** able to register the authentication information to the server
- **Identification**, able to identify the registered user
- **Verification**, able to verify the registered user is the one that the user claims to be
- **Encryption**, the palm vein data from the mPollux Client to the mPollux Server is encrypted with the high secure method using asymmetric/symmetric combined encryption.

The PalmSign Client can be called from applications to add Palm Vein authentication as their authentication method. mPollux also has the ready-made login application for web applications, with which mPollux can be integrated with existing application easily.

2.2 PALMSIGN™ SERVER

mPollux PalmSign uses mPollux Bases for the basic function like logging, DB connection etc… please see "mPollux Service Description".

mPollux PalmSign server itself manages the Registration Identification and Verification based on Client request.

PalmSign Server with utilizing mPollux Bases, provides the features as follows,

- **DB connection,** mPollux Base provides DB connection for storing/fetching data from common DB (SQL Server, Oracle DB are supported. need to discuss for other DBs).
- **Registration/Identification/Verification,** According to client request, PalmSign Server proceed authentication/identification/verification utilizing PalmSecure library and mPollux Bases functions.
- **Transaction Log,** mPollux PalmSign provides the simple transaction log of client/server communication.

2.3 mPollux™ Login Application (Optional)

mPollux™ Login Application provides easy-to-integration function to mPollux PalmSign. The application runs on Java Application Server as web application.

There is ready made login user interface and well integrated with mPollux Server. With this application, mPollux PalmSign can be easily integrated with the web application

This application can also play the role of gateway even when PalmSign integrated with the client/server application, if there is public network (e.g. Internet) between client and server. Using the application as gateway, the mPollux Server can be located inside closed network to avoid attacks from public network.

2.4 Secure Data Transportation Feature

PalmSecure API already encrypts palm vein data with own algorithms. In addition to that, PalmSign encrypts the palm data between PalmSign client and PalmSign server in order to avoid theft and abuse of it when the data go through network.

A PalmSign data is encrypted with private key crypto system at first and the private key is encrypted with public key crypto system. Different keys are created for each session. The bellows are the supported encryption methods.

Key algorism	Encryption Method
Private key cryptosystem	AES256bit
Public key cryptosystem	RSA1024bit

***In some country AES256bit is prohibited to use. Please check the country policy when you plan to use AES256bit.**

3 MPOLLUX PALMSIGN™ ARCHITECTURE

For an overview of the overall architecture of the mPollux™ Security Server, see the mPollux™ Security Server White Paper. Figure 1 shows the architecture of the mPollux™ Security Server with PalmSign Security Option.

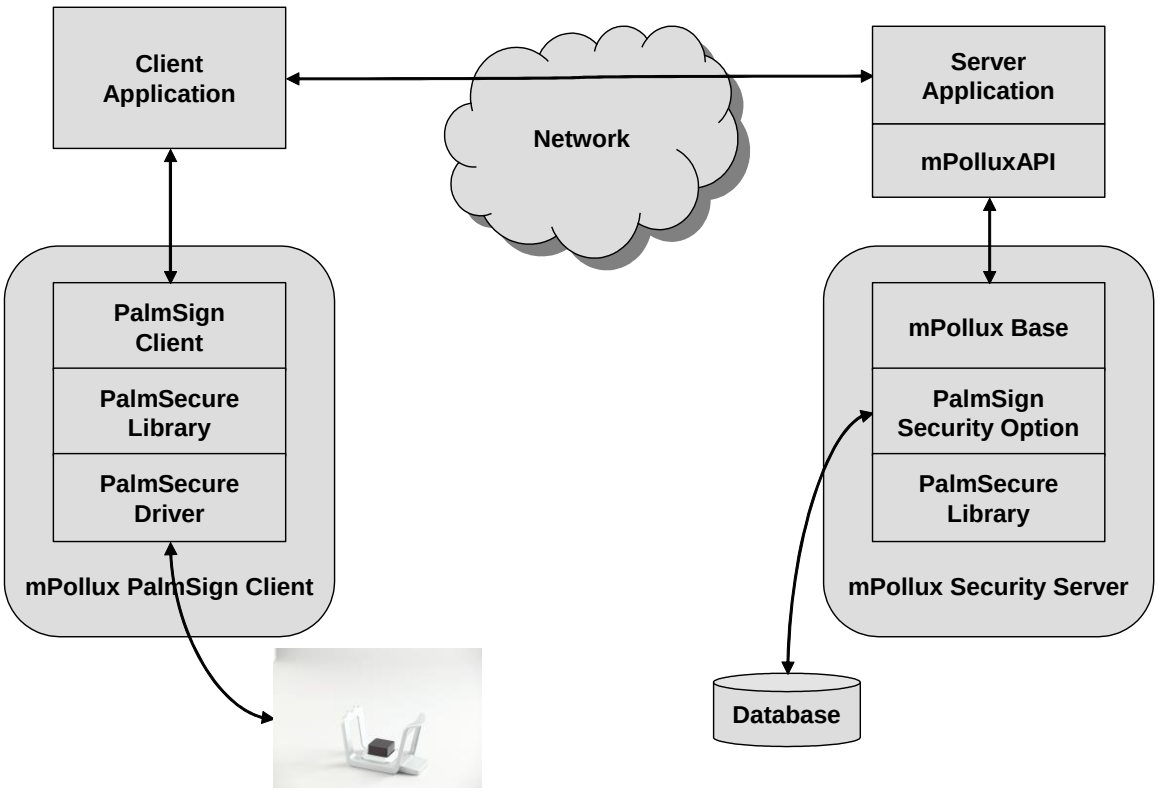

Figure 1 The Architecture of mPollux™ PalmSign Security Option

As *figure 1* shows, the main components of mPollux PalmSign™ are

- **mPollux™ API** and **mPollux™ Base**, which are the common components for all mPollux™ Security Options, and
- **PalmSign Client** and **PalmSign Server**, which are the specific components of mPollux™ Security Server PalmSign Security Option.
- **PalmSecure Library** (SDK) is the library to control PalmSecure Sensor.

Service requests from applications using mPollux™ Security Server are transmitted from mPollux™ API in an XML message over a secure (if required) TCP/IP socket connection to mPollux™ Base. mPollux™ Base determines which Security Option instance has been called (there may be several instances of different or the same Security Options running in a mPollux™ installation) and forwards the service call to the right receiver. The called Security Option – in this case PalmSign – executes the

service call and returns result via mPollux™ Base to the application. This is in brief the way mPollux™ Security Server operates.

PalmSign module coordinates and controls the user authentication process driven by the service calls from the user application and according to the PalmSign profile relevant to the user.

Because of the architecture, mPollux™ Security Server functionality can be run either on the Application or Web server platform or on a separate server.

4 EXAMPLES OF MPOLLUX PALMSIGN™ USE CASES

4.1 CASE 1: WEB AUTHENTICATION

This case is for the login method of current/new application. Using mPollux PalmSign™ , Palm Vein authentication can be integrated web applications easily.

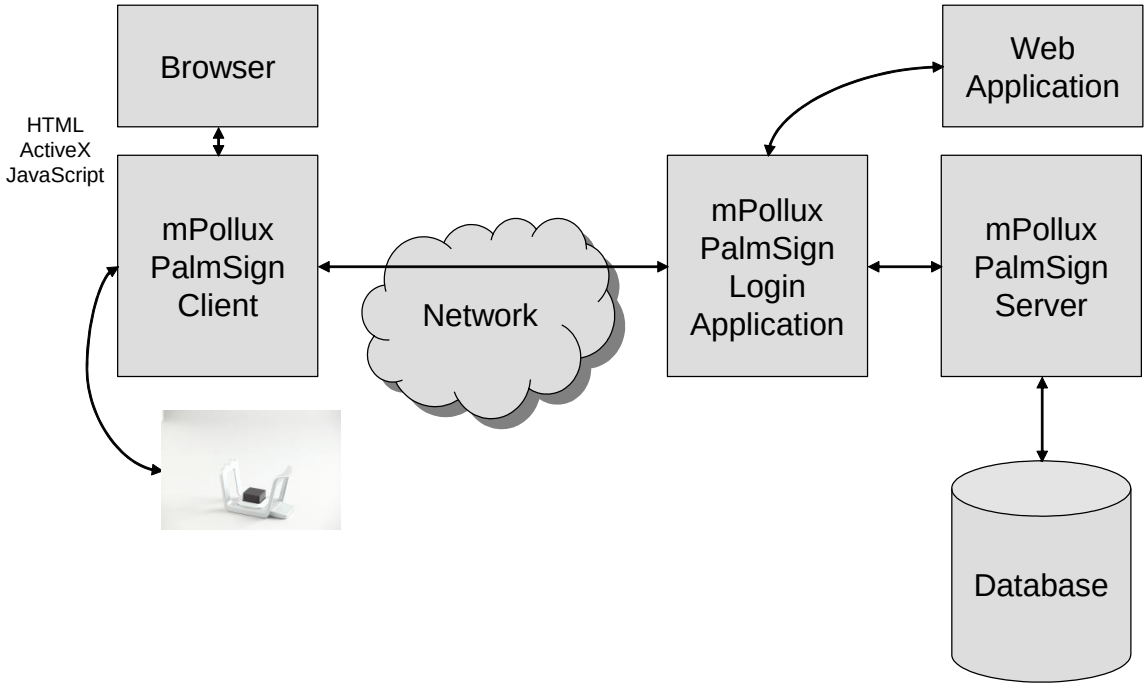

Figure 2 mPollux PalmSign™ web authentication

The sample access sequence proceeds as follows

1. User open a web application with a browser
2. The web application redirects to mPollux PalmSign™ Login Application, when user does not yet login.
3. mPollux PalmSign™ Login Application show the login screen and start to communicate with PalmSign™ Client to control Palm Secure Sensor
4. After the user give his hand over the Sensor, PalmSign Login Application fetch the data and send to mPollux PalmSign™ Server
5. Then mPollux PalmSign™ Server verify the data with that user's template and return the result to mPollux PalmSign Login Application

6. According to the result, mPollux PalmSign Login Application send the necessary information to the server application

4.2 CASE 2: ACCESS CONTROL

mPollux PalmSign can be utilized as part of access control function. Access Controller can rely on PalmSign for the client/server palm vein authentication part.

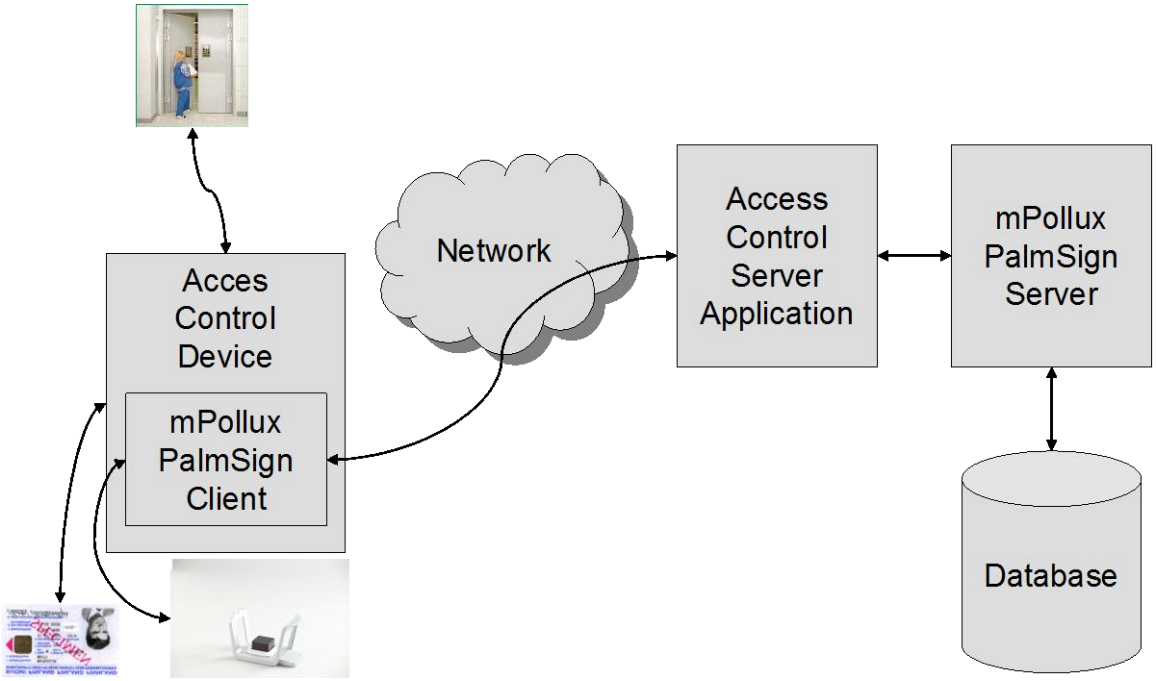

Figure 3 mPollux PalmSign™ Access Control integration

The architecture to realize the access control integration are varied. One example is as follows,

1. User input the identifier (e.g. insert card or enter PIN), then access control device call PalmSign client
2. PalmSign Client tell the device when it's ready, the device show it to the user
3. After user shows his hand over the sensor, PalmSign Client send the data to Access Control server Application
4. After access control server proceeds necessary procedure, it sends the data to PalmSign Server to verify the user.
5. PalmSign Server sends back the result to access control server
6. access control server send back the result to the device
7. according to the result, the device open the door, or does other operation.

4.3 CASE 3: MPOLLUX PALMSIGN WITH SMARTCARD

mPollux has the other authentication option to utilize PKI technology: mPollux DigiSign. mPollux can realize the authentication with Smart Card/Palm Vein combination.

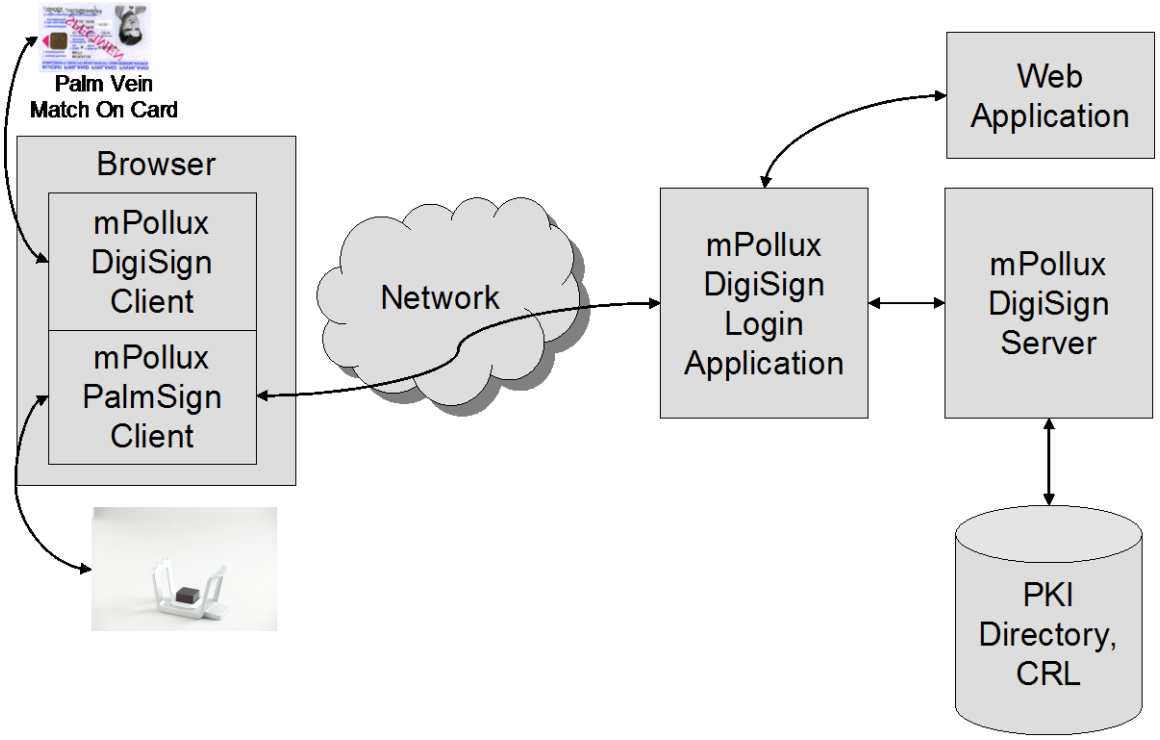

Figure 4 mPollux PalmSign™ with smart card

The sample access sequence proceeds as follows

1. User opens an application (e.g. web application), which requires PKI authentication and insert his smart cart.
2. When DigiSign Client recognize the cart, DigiSign Client call PalmSign client to get the user's palm vein data.
3. After the user show his hand over the sensor, PalmSign send the data to DigiSign Client
4. DigiSign Client send command and data to verify the data internally in the card
5. When the verification succeeded, DigiSign start the PKI's authentication flow.
6. After PKI's process, user can access to the application

*To implement the match on card mechanism, Fujitsu Japan's additional component for smart card is needed.

4.4 CASE 4: WINDOWS WORKSTATION LOGIN

Workstation Login can be one example of the specific case of smart card integration. With this, login comes to be high secure with biometric (Palm Vein) and PKI combination.