Fujitsu mPollux

Classic Security Option

White Paper

Fujitsu mPollux Version 2.1

June 2016

Second Edition   June 2016

The programs described in this document may only be used in accordance with the conditions under which Fujitsu Finland Oy supplies them.

This document is provided to your organization on the understanding that its content is and remains the intellectual property of Fujitsu Finland Oy. The document is provided on the understanding that its use is confined to the people in your organization who are responsible for evaluating its content and that there is an obligation on your organization and such people within your organization to keep its content in confidence. This document may not, without the prior written authority of Fujitsu Finland Oy, be copied or shown in whole or in part to any third party. When no longer required for the agreed purpose, the document is to be returned to Fujitsu Finland Oy.

Fujitsu Finland Oy endeavors to ensure that the information in this document is correct and fairly stated but does not accept liability for any error or omission.

The development of Fujitsu Finland Oy products and services is continuous and published information may not be up to date. It is important to check the current position with Fujitsu Finland Oy. This document is not part of a contract or license save insofar as may be expressly agreed.

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited. PalmSecure and the PalmSecure logo are registered trademarks of Fujitsu Limited. The Possibilities are Infinite is a trademark of Fujitsu Limited. mPollux, mPollux security options are trademarks or registered trademarks of Fujitsu Finland Oy and Fujitsu Limited. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Table of Contents

1 INTRODUCTION

The mPollux™ Security Server is Fujitsu Finland's multifunction security solution, which can be easily adapted for the diverse needs and security level requirements of user organizations. This is made possible by the modular architecture of mPollux™ Security Server: the Server offers a number of Security Options and the user organization chooses the Option(s) that best suit(s) its needs.

This white paper describes the functionality of the **Classic Security Option** that is designed to support basic userid and password based authentication.

The mPollux™ Security Server with Classic Security Option consists of:[1]

- The mandatory **mPollux™ Base** component, which implements the application interfaces through which mPollux™ is used, and common services like logging and an interface to a user database or directory.

- The Security Option, which can be implemented using either an SQL or LDAP user register.

---

[1] See the chapter "Overview of the mPollux Classic Server Architecture" for a more detailed description of the server architecture.

2 SPECIFICS OF USERID AND PASSWORD BASED SECURITY

The Classic functionality is based on the userid and password. These user credentials are stored in the protected user register, which can be accessed only from the authentication service. The authentication service receives authentication request from an application and checks validity of the userid and the password. The result of the check is returned to the application.

Implementation Assumptions

User Register (SQL/LDAP)

A user register is not part of the Classic Security Option, which just uses an existing user register with a standard protocol (LDAP or JDBC). The location, structure, fields and protocol of the user register are configurable items of the Classic Security Option.

LDAP Authentication

The Classic Security Option can use an existing LDAP user register with a standard LDAP authentication protocol. Connection to LDAP directory could be clear text LDAP or LDAP over SSL.

Kerberos Authentication

The Classic Security Option can use an existing Kerberos user register with a standard Kerberos V5 authentication protocol.

Mapping

The Classic Security Option can map external user identification to mPollux user identification. This can be used if authentication is done with trusted third party methods like Tupas Bank authentication.

mPollux

3   WHO WILL BENEFIT FROM THE CLASSIC SECURITY OPTION?

The Classic Security Option is an authentication solution for Web users and applications, which do not have a technical possibility or need to have stronger security. The Classic Security Option offers the lowest level of security of all mPollux™ Security Options. In some cases this level of security is, however, enough, and the setting up of an mPollux Classic™ based authentication service is not too difficult and/or costly. It is then possible to have a centralized authentication service with different levels of security (other mPollux™ Security Options) and offer authentication services suitable for various applications and security needs.

4 MPOLLUX CLASSIC™ USE SCENARIOS

4.1 GENERAL

The fundamental operation principles of mPollux Classic™ are the use of userid and password. Application asks these user credentials from user via user interface and then use mPollux Classic™ to check the validity of user. Authentication is made via the same channel as normal application communication (Internet, GPRS, GSM Data, etc) and there is no need for an extra authentication device.
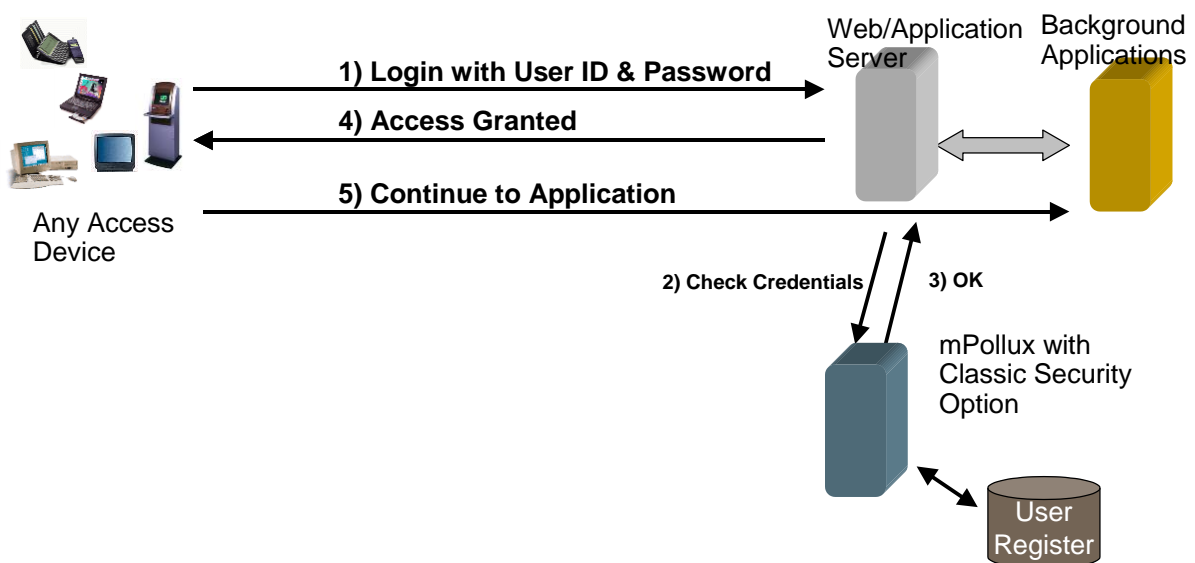
4.2 CLASSIC FOR WEB USERS

Figure 1 Authentication with mPollux Classic™

Figure 1 presents the scenario where mPollux Classic™ is used with Web services. The only special requirement for the application is the ability to use the mPollux™ API to invoke the required security operations. The application level authentication of the user is based on a userid and password. Figure 1 also shows the steps for mPollux Classic™ authentication.
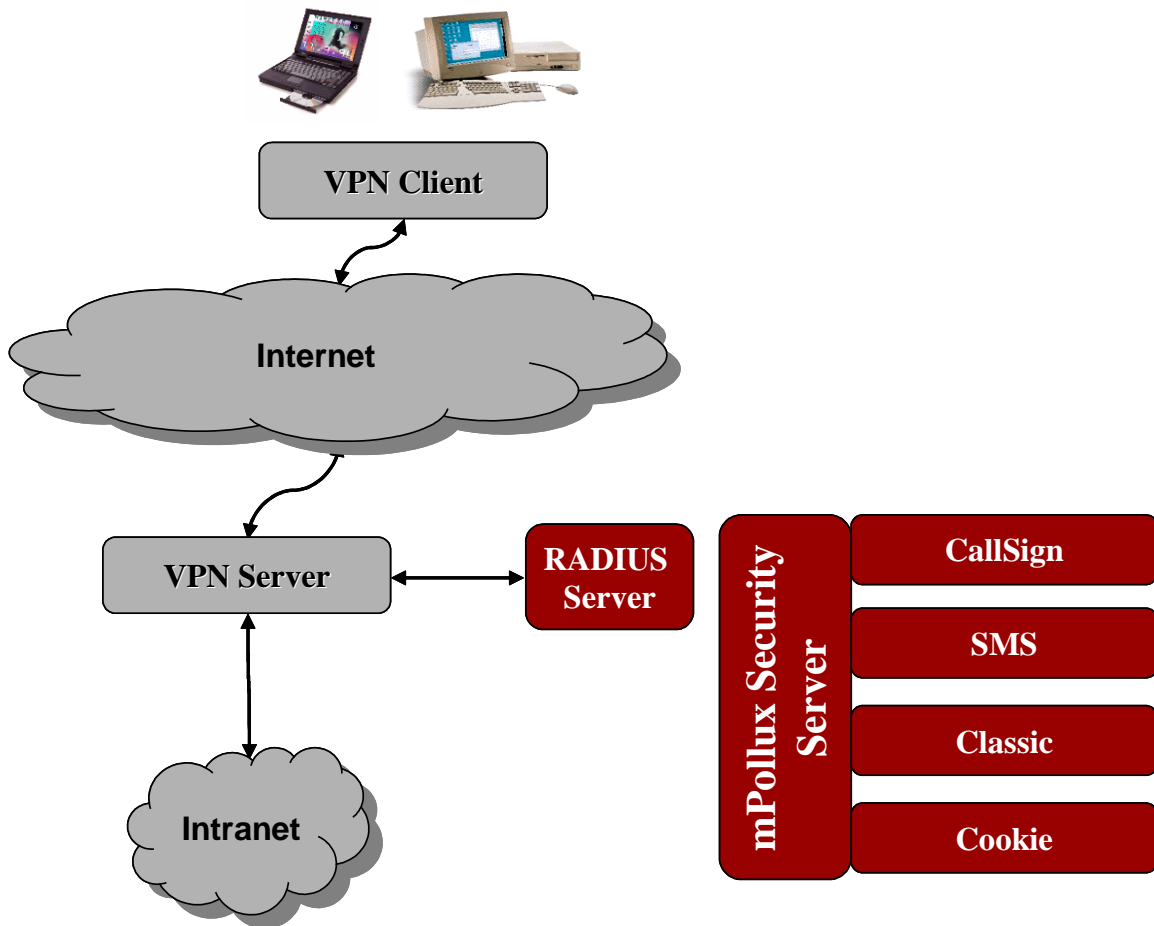
4.3 CLASSIC FOR VPN USERS

Figure 2 VPN Authentication with mPollux Classic™

Figure 2 presents the scenario where mPollux Classic™ is used with VPN services. The only special requirement for the application is the ability to use the Radius authentication protocol.

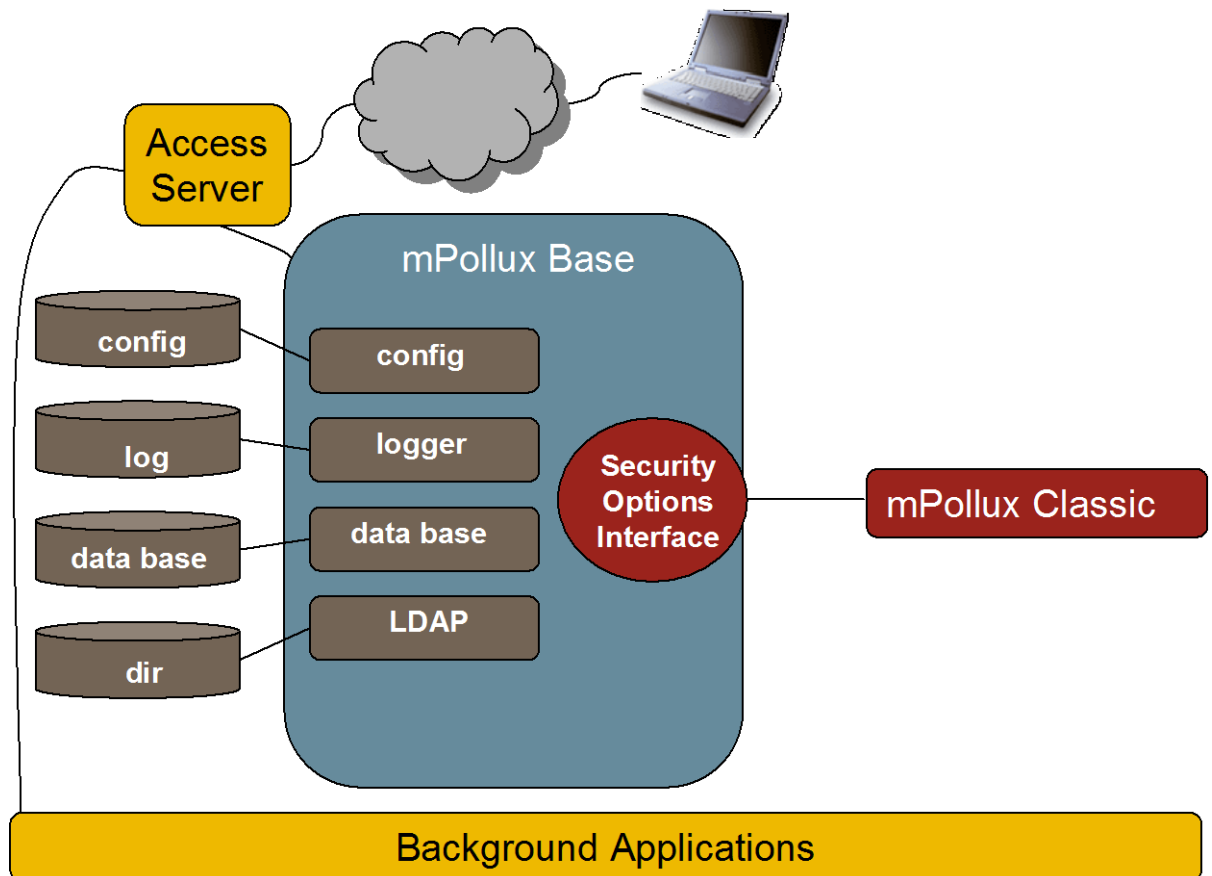# 5 OVERVIEW OF THE MPOLLUX CLASSIC™ SERVER ARCHITECTURE

Figure 3 mPollux™ with the Classic Security Option Server Architecture

Figure 3 illustrates the general architecture of the mPollux™ Security Server with the Classic Security Option.

5.1 MPOLLUX™ BASE FUNCTIONALITY

Application Interfaces to mPollux Classic™

The Application Programming Interfaces to the mPollux Classic™ Security Option are implemented by the common mPollux™ Base component. Microsoft **.NET** and **Java** environments are supported.

Logging   The logging functions of mPollux™ Base are used to log all security related operations of the mPollux Classic™ Security Option.

Access to User Register

A user register is needed to store the information of mPollux Classic™ users. It can be a local database or a private **LDAP** directory. Access to this user database/directory is implemented as an mPollux™

mPollux

Base function. Also two common authentication protocols to other user registers is possible. These two are LDAP authentication and Kerberos V5 authentication.

5.2 COMPONENTS OF THE MPOLLUX CLASSIC™ SECURITY OPTION

mPollux Classic™ Server

The mPollux Classic™ Server is the component that handles the authentication requests for the Classic Security Option and takes care of the responses to the requesting application. It uses the common base components for connection to the user register (SQL or LDAP), logging etc.

6 MPOLLUX KERBEROS SINGLE SIGN-ON

The mPollux™ authentication and access control system (mPollux Secure Portal) can trust domain authentication and use that authentication for the web applications. This "domain to web" single sign-on reuse mPollux Classic™ Security Option's Kerberos V5 component among other mPollux components.

The Client implementation is part of the mPollux API for .NET .

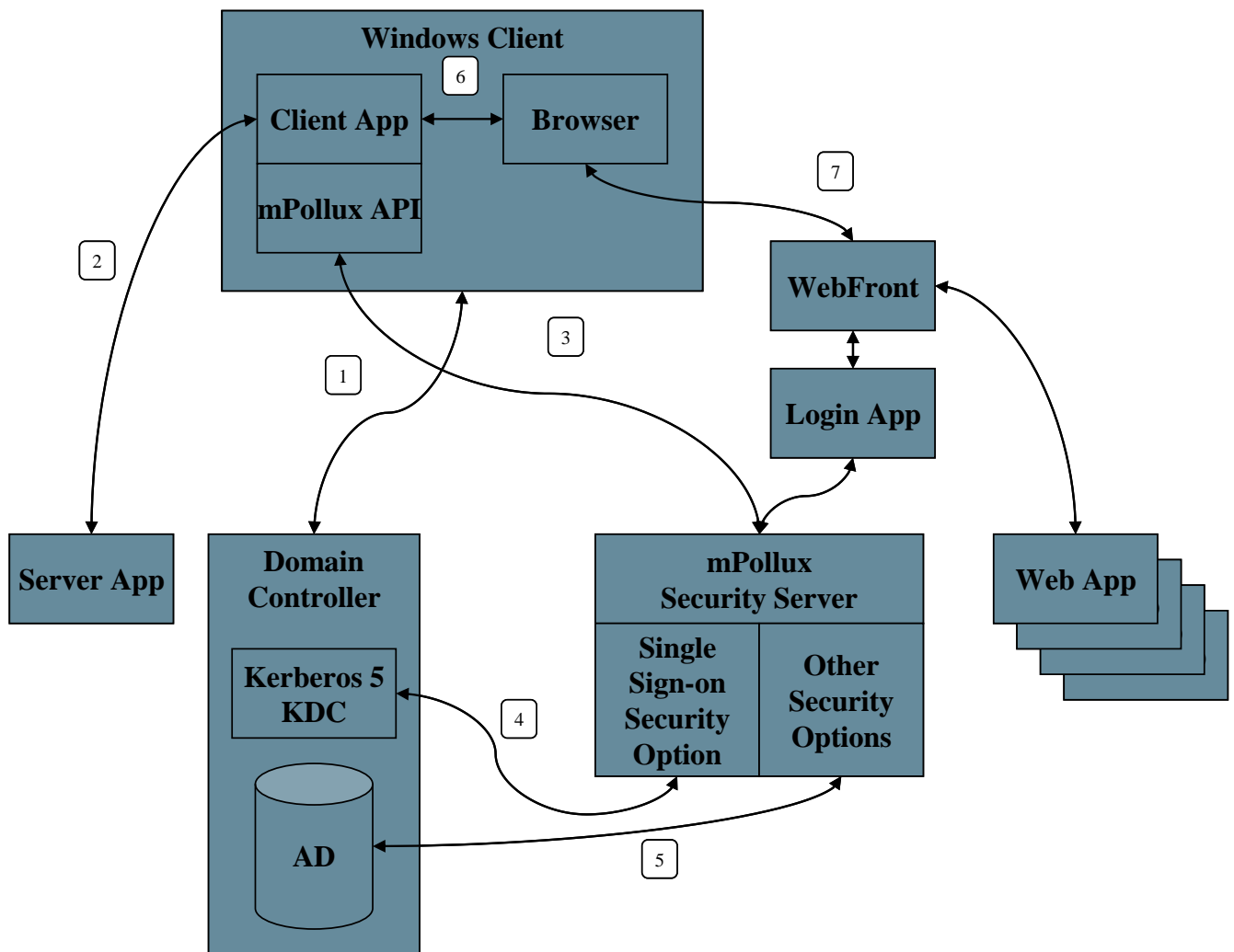mPollux Kerberos Single Sign-On is separately licensed set of components.

Figure 4 mPollux™ Kerberos Single Sign-On Architecture