

Fujitsu mPollux

Security Server

White Paper

Fujitsu mPollux Version 2.0

February 2008



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

This document is provided to your organization on the understanding that its content is and remains the intellectual property of Fujitsu Services 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 Services 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 Services Oy.

Fujitsu Services 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 Services 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 Services 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 Services 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	4
2	MAIN FEATURES OF MPOLLUX™ SECURITY SERVER	4
3	BUSINESS BENEFITS.....	5
4	ARCHITECTURE OF MPOLLUX™ SECURITY SERVER	6
4.1	The mPollux™ Base	6
4.2	The mPollux™ Security Options.....	7
4.3	The mPollux™ WebFront Access Control	9
4.4	The mPollux Cookie™ Security Option.....	9
4.5	mPollux™ and SAML	10
4.6	mPollux™ and TUPAS	10
4.7	mPollux™ Front-End Servers.....	12
4.8	mPollux™ Custom Security Option Toolkit	14
4.9	mPollux™ Login Application.....	15
4.10	mPollux™ Log Browser	15
4.11	mPollux™ User Manager	15
4.12	mPollux™ Config Tool.....	15
5	MPOLLUX™ SECURITY SERVER ENVIRONMENT	15

1 INTRODUCTION

In the context of e-business, the securing of communications 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. Some of these schemes share common features and implementation level components and some don't.

It would be advantageous, if an e-business operator could run a security service that

- allows the choice of the most suitable security scheme for each purpose,
- hides the differences of various security schemes, and
- can be used through one unified interface.

This would create a more uniform operating environment and also provide a straightforward migration path from simple classic security solutions towards more sophisticated ones.

Fujitsu mPollux™ Security Server is Fujitsu Services' answer to these needs. mPollux™ is a modular, multifunction, multitechnology system that provides a state of the art solution to the requirements of quickly changing business needs and operating environments. It can easily be configured to support the technologies and interfaces needed by specific applications or specific user environments. When the requirements evolve over time, the functionality can be maintained and enhanced with the addition of relevant new options.

2 MAIN FEATURES OF MPOLLUX™ SECURITY SERVER

mPollux™ is designed to secure primarily **web and wireless applications**. It provides **authentication and authorization services** that can be used to control access to a single application, or to implement a Single Sign-On access control system for a bunch of applications. Several different user authentication methods are supported. Authorization functions can be implemented combining the use of mPollux™ services and the access control features of the Web Server product in use, or using the optional **WebFront Access Control** module of mPollux™.

In addition to the basic authentication and authorizations services, mPollux™ Security Server can generate and check **digital signatures**, and in near future it will be able to provide **time stamping services** as well. In association with the authentication services, it supports encrypted cookie generation and checking, and checking of digital certificates and Certificate Revocation Lists (CRLs).

The various optional security functions of mPollux™ are implemented by separate **Security Option** modules (the "hanging" extensions of the Security Server in *figure 1*). An organization using mPollux™ can choose exactly those Security Options that it needs. The Security Server can be easily enhanced later with additional Security Options as needed. All mPollux™ Security Options implement the primary service, authentication. The method and security level achieved is option specific. Some Security Options enable additional advanced functions such as digital signing and authentication-associated micro payments.

The services of mPollux™ Security Server are used through the **mPollux™ API** that is an interface library available for both Microsoft .NET and Java application runtime environments. mPollux™ is client neutral: the authentication client can be any device capable of participating in the selected security scheme. Maximum security can be achieved using **PKI (Public Key Infrastructure)** based solutions. If required, mPollux™ can be integrated with legacy security systems, too. This enables the in-

tegration of legacy services into the web applications, and enables controlled migration to a PKI environment whenever such is planned.

3 BUSINESS BENEFITS

For enterprises mPollux™ Security Server provides a good foundation to develop and implement new customer operation models for all services and products in different service and delivery channels. It allows a flexible way of proceeding to use new technology and utilizing existing solutions to improve and enhance your services.

The key business benefits of mPollux™ Security Server are:

- It offers users consistent ways of authenticating themselves while accessing the services via different channels. For service providers, this means huge cost savings, because all channels can utilize:
 - the same user, access rights, and profiles management
 - the same security infrastructure and PKI (*Public Key Infrastructure*) implementation and management
 - the same SIM (*Subscriber Identity Module*) for GSM and mobile security to provide the strong authentication and digital signature features
 - the same mPollux™ Security Options.
- Simple application interface to manage the security services. The user is able to use different security schemes while approaching the systems through different service channels.
- The Security Server can be easily expanded with new Security Options.
- Single Sign-On to web applications (and through them possibly legacy applications as well) can be implemented using mPollux™ Security Server and the mPollux™ WebFront HTTP Proxy.
- Reuse of existing components, investments, and platforms. In most cases, the same development resources and tools can be used as before.
- A rapid and flexible way of responding to changes in the markets.

4 ARCHITECTURE OF MPOLLUX™ SECURITY SERVER

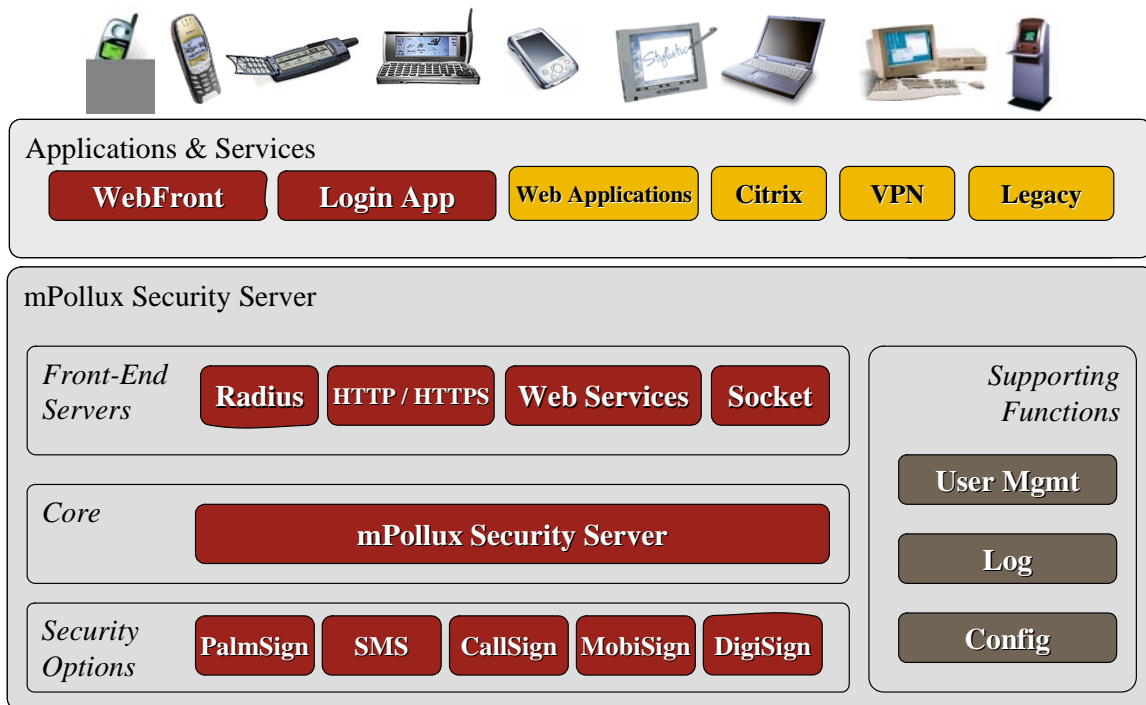


Figure 1 The modular architecture of mPollux™ Security Server

Architecturally mPollux™ Security Server consists of a common base component, the **mPollux™ Base**, and one or several **Security Options** (see *figure 1*). In addition to these, the **mPollux™ Web-Front Access Control** is available as an optional component.

4.1 THE MPOLLUX™ BASE

The mPollux™ Base is a mandatory component, which implements the application interface, basic User Register access and logging functions. The mPollux™ Base requires at least one Security Option to be attached in order to be functional. Further Options may be added as needed.

The **mPollux™ Application Programming Interface (mPollux™ API)** is available for both **Microsoft COM+/.NET** and **Java** environments. The Java version of mPollux™ API implements also **Java Authentication and Authorization Service (JAAS)** interfaces. The basic API functions are Authentication and Signing. There are slight variations for each function based on the set of Security Options that have been installed.

Depending on the particular Security Option, the implementation of the **Authentication** function varies from a simple verification of stored user information to a more complex sequence where the user device, the application server, and the mPollux™ Security Server select and verify PKI certificates.

The **Signing** function enables the application server to present a document for signature by the user, and to create and verify signed documents.

The Security Server can write a **log** of all its service requests and their results. The log is stored on local media for security. The log can be searched and browsed, and a system administrator can print reports of security events and/or export log data to be consolidated with other auditing data of the user organization. The log can be utilized e.g. for monitoring and billing purposes.

The mPollux™ Base uses either a **database** or an **LDAP directory** as the **User Register** that is needed in the authentication and authorization operations. Existing user databases or directories can be used as mPollux™ User Register, but if required, a new register for the specific needs of mPollux™ may be created.

4.2 THE MPOLLUX™ SECURITY OPTIONS

The Security Options of mPollux™ Security Server work together with the mPollux™ Base to implement the security functionality required. All mPollux™ Base services, such as logging and user register, are available for all the Security Options.

Any Security Option can be selected for use at the same time. The application interfaces are largely Security Option independent, although some Option specific features are necessarily reflected in the mPollux™ API.

mPollux CallSign™ The **mPollux CallSign™ Security Option** adds an innovative method of using **mobile phones** for authentication and billing. The option also works using ordinary phones, but with limited functionality.

mPollux CallSign™ implements a type of challenge-response authentication protocol where the security server issues a challenge and the user must respond to it in an acceptable way to pass the security check. The channels used for the challenge, i.e. the application service delivery channels, are not constrained by mPollux CallSign™, but typically they are Web browser related. The authentication response is always performed over a phone line, normally using a mobile phone. The authentication response can be

- simply a call to CallSign server, or a response to the call-back from CallSign server
- the Personal Identification Number (PIN) of the user, or a one-time response code given by CallSign as a part of the challenge.

In the future new authentication response types like voice response are planned to be supported. The challenge-response sequence can be easily tailored to match a large range of application needs.

The implementation of the mPollux CallSign™ Security Option uses a separate physical server component, the **CallSign Server**, as an interface to the telephone network. The CallSign Server also implements the challenge-response dialog with the user under the control of mPollux™ Security Server.

mPollux PalmSign™ The **mPollux PalmSign™ Security Option** offers **biometric** authentication. It uses Fujitsu's Palm Vein technology and sensor hardware. It offers one to one and one to many biometric authentication. PalmSign Security Option can be used independently or it could be combined with other security options like DigiSign. If PalmSign is used independently, biometric data is stored in database. Combined usage with DigiSign means that biometric data is stored in smartcard.

-
- mPollux DigiSign™** The **mPollux DigiSign™ Security Option** supports **smart card based** authentication based on PKI certificates. DigiSign thus enables the use of strong client authentication on secured SSL connections for users working with smart card reader equipped workstations and using smart cards with standard X.509 certificates to identify themselves. mPollux DigiSign™ also supports digital signatures that can be used for non-repudiation of business transactions and authentication of documents transmitted on a business connection.
- The DigiSign Security Option supports the use of standard LDAP connections to Directory Services for the checking of the status of certificates and Certificate Revocation Lists (CRLs).
- mPollux MobiSign™** The **mPollux MobiSign™ Security Option** provides to the users of GSM mobile phones the corresponding functionality (PKI based authentication and non-repudiation) as above-described mPollux DigiSign™.
- mPollux MobiSign™ implements PKI level security for phones using the **SIM Toolkit technology**. This has to be done in co-operation with the involved teleoperator company/-nies, and implies always some case-specific tailoring.
- mPollux MobiSign™ uses common components with mPollux DigiSign™ to implement basic PKI services like connection(s) to the directory/-ies containing the certificates and CRLs.
- mPollux Classic™** The **mPollux Classic™ Security Option** offers traditional User ID/password authentication. It supports the use of fixed and changing passwords. The user credentials can be checked against an existing User Register or a specific new Register created for mPollux™ applications.
- mPollux SMS™** The **mPollux SMS™ Security Option** offers for users of GSM mobile phones challenge – response type authentication. It uses two channels, the **short message service** (SMS) channel for delivering random authentication code to the user and a web or WAP channel for application communication. **SMS Security Option** is similar to mPollux CallSign™ Security Option but uses SMS as the response channel.

4.3 THE mPOLLUX™ WEBFRONT ACCESS CONTROL

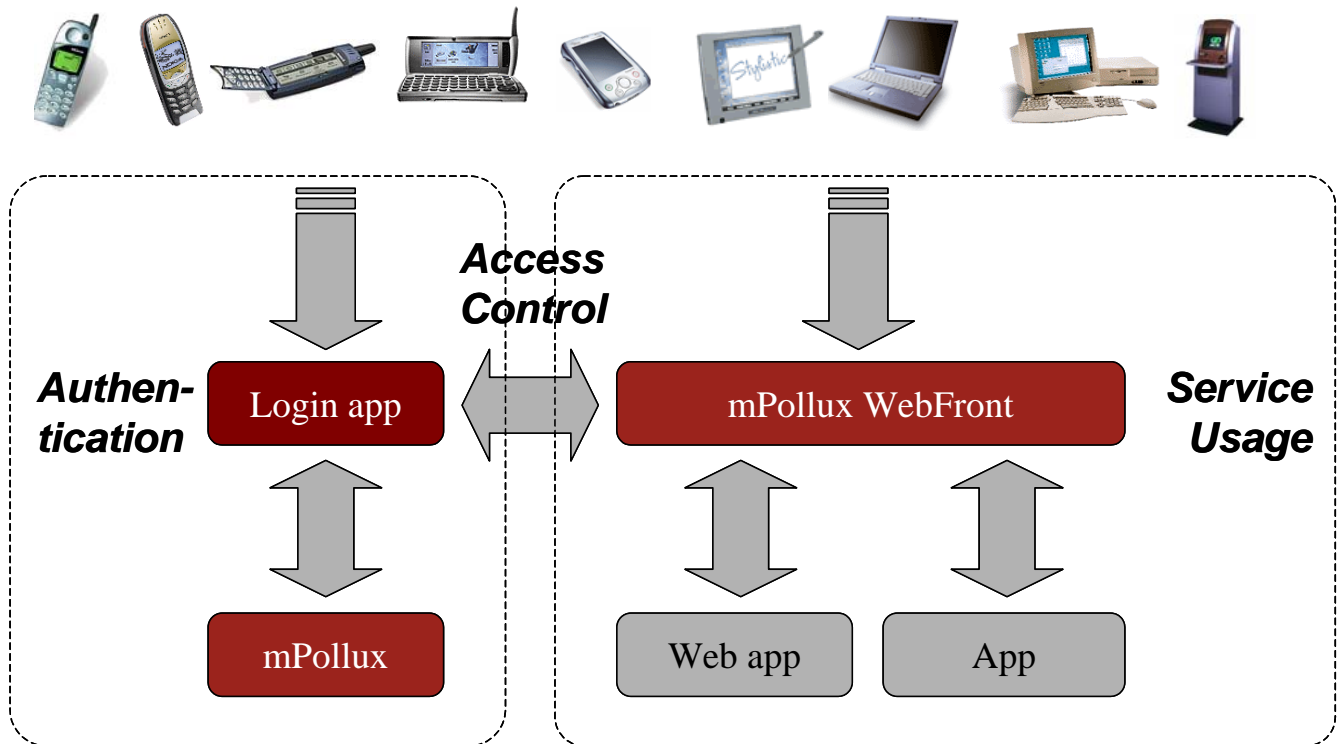


Figure 2 Operating Environment with mPollux™ Security Server and mPollux™ WebFront

The **mPollux™ WebFront Access Control** is an HTTP Proxy that can be used to implement access control into one or several Web applications. In the latter case, Single Sign-On to the concerned applications can be achieved by the help of WebFront and the mPollux™ Security Server.

Figure 2 describes the operating environment of mPollux™ WebFront. WebFront can be used in combination with any of the authentication methods supported by the mPollux™ Security Options.

The Web applications in the figure use mPollux™ WebFront-based access control. Encrypted cookies generated at the session set-up are used to control access to the applications. mPollux™ Security Server takes care of the generation and checking of the cookies, as well as the authentication of users at log-in time. All application traffic (thick solid lines in *figure 2*) goes through the mPollux™ WebFront.

4.4 THE mPOLLUX COOKIE™ SECURITY OPTION

The **mPollux Cookie™ Security Option** differs from the other security options. It helps access control, session handling and single sign-on implementations by offering secure token creation and validation. Security tokens can be used e.g. as the session cookie. The Java software is used to perform required cryptographic operations and to store server-side private keys.

The Cookie Security Option can maintain so called “global session”. Global session is mapped to WebFront™ session and thru that different application sessions can ask status of “global” understanding of user’s session information.

4.5 mPOLLUX™ AND SAML

The Security Assertion Markup Language (SAML) standard defines an XML-based framework for describing and exchanging security information between an identity provider and a service provider. This security information is expressed in the form of portable SAML assertions that applications working across security domain boundaries can trust. The SAML standard defines precise syntax and rules for requesting, creating, communicating, and using these SAML assertions.

More information about SAML standard:

- <http://www.oasis-open.org/specs/>

mPollux Authentication Service supports SAML 2.0 specification’s Web Browser SSO Profile and Single Logout Profile. The authentication service implements the roles identity provider (IdP) and service provider (SP). The SAML provides web-based single sign-on functionality for the mPollux authentication service.

4.6 mPOLLUX™ AND TUPAS

TUPAS is Identification Service for Electronic Customer Service Providers. Finnish Bankers’ Association specifies it. The mPollux™ supports this authentication mechanism and offers user identification mapping functionality. This mapping is normally done from Banks identification to mPollux™ identification.

More information about TUPAS and Finnish Bankers’ Association:

- http://www.pankkiyhdistys.fi/sisalto_eng/upload/pdf/tupasV2eng.pdf
- <http://www.pankkiyhdistys.fi/english/index.html>

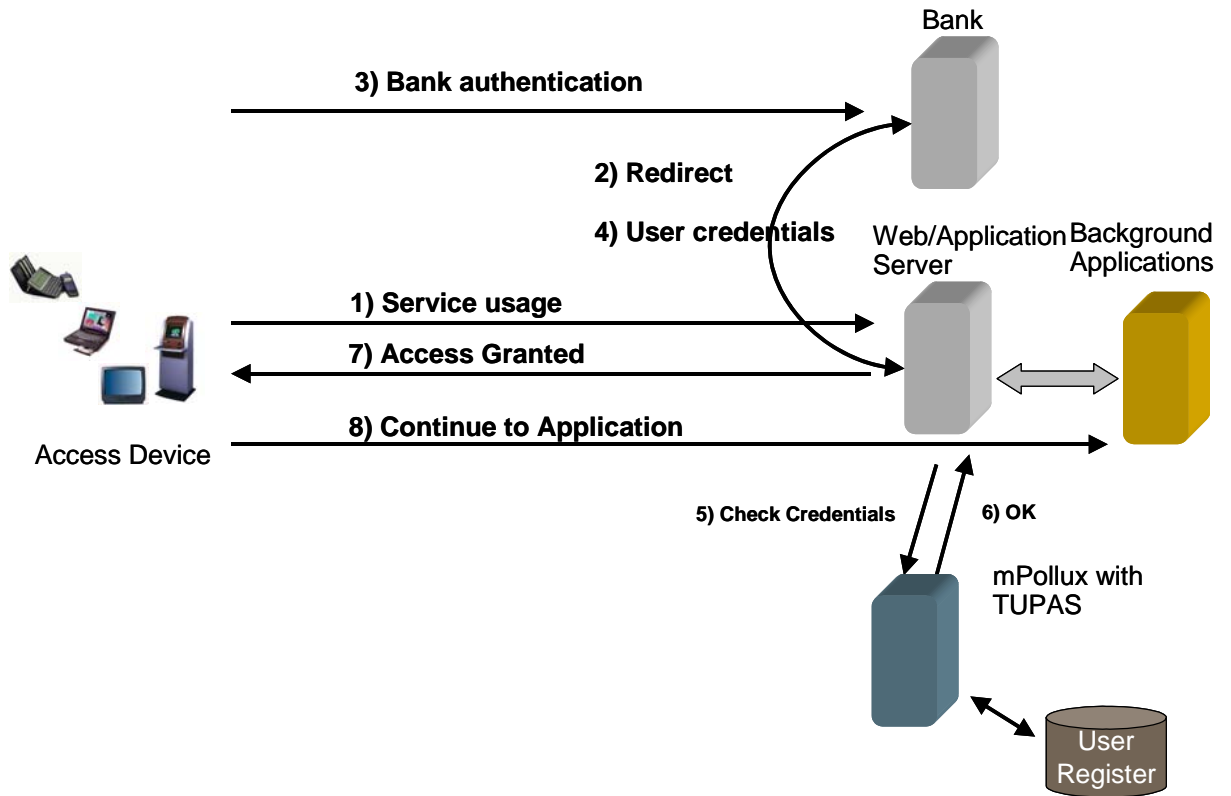


Figure 3 mPollux™ with TUPAS authentication flow

4.7 mPOLLUX™ FRONT-END SERVERS

The mPollux™ Security Server Base interface is a TCP/IP socket server, which can be used via mPollux™ API. There are also standard authentication protocols that existing products like operating systems, web servers and VPN servers use. mPollux™ offers optionally the RADIUS and Web Services authentication protocols as front-end server components.

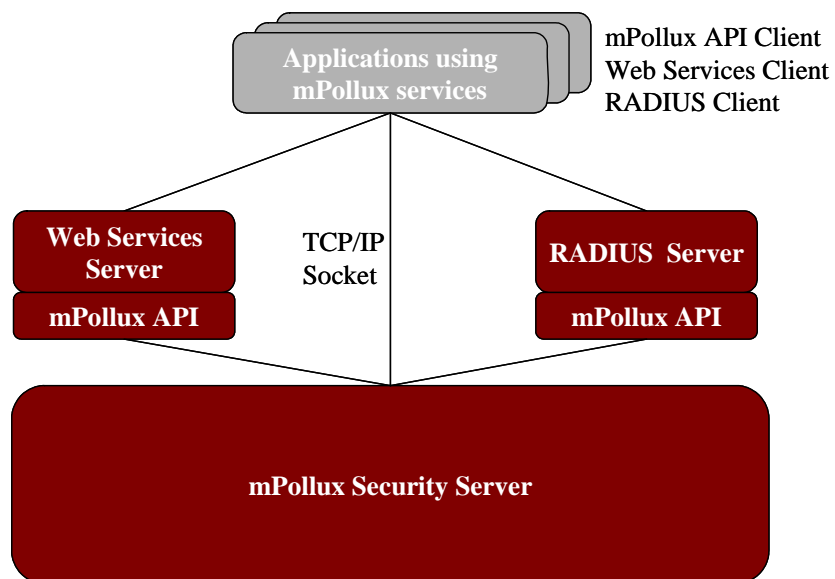


Figure 4 The modular architecture of mPollux™ Front-End Servers

mPollux™ RADIUS Server

mPollux™ RADIUS Server is an optional component of the product family. RADIUS authentication requests can be redirected to the selected mPollux™ Security Option and users can be authenticated in the security option specific way. The choice of possible authentication methods available for existing products is hereby increased without the need for multiple user registers.

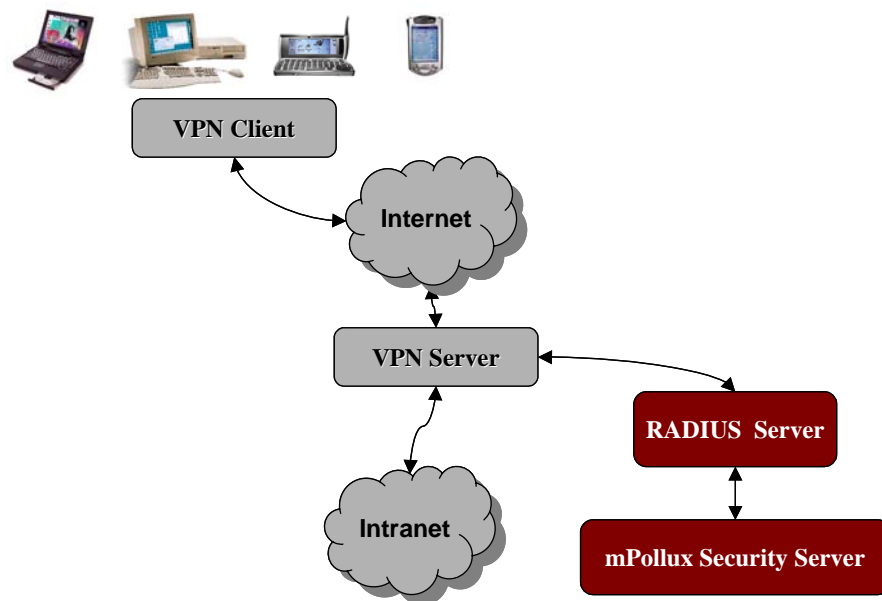


Figure 5 mPollux™ RADIUS Server Use Case

mPollux™ Web Services Server

mPollux™ Web Services Server is an optional component of the product family. Web Services is easy and standard way to build mPollux™ Security Server connectivity. Web Services Server implements HTTP and HTTPS protocols and enables standard way to integrate applications with mPollux™. Communication between mPollux™ API and mPollux™ Security Server can be encrypted with it and both sides can authenticate each other. The component uses the standard secure HTTPS protocol and certificates. The need for this component is obvious, if mPollux™ Security Server operates in public network (internet) or if network security level is otherwise not good enough. It is also standard and easy way to integrate 3rd party applications.

4.8 mPOLLUX™ CUSTOM SECURITY OPTION TOOLKIT

In addition to a wide range of existing security options, mPollux™ offers a robust infrastructure that makes the development of custom security options easy and cost-efficient. The toolkit includes Java interfaces and development documentation.

Examples of when a custom security option is needed:

- Need to use tailored security methods through mPollux™.
- Need to implement proprietary security features and functions.
- Need to interact with external user registers, which cannot be used with JDBC or LDAP.

The toolkit also includes Java interfaces and development documentation of mPollux™ plug-ins and external programs. mPollux™ plug-ins and external programs are tailored software components which could be used with security options of mPollux™ product..

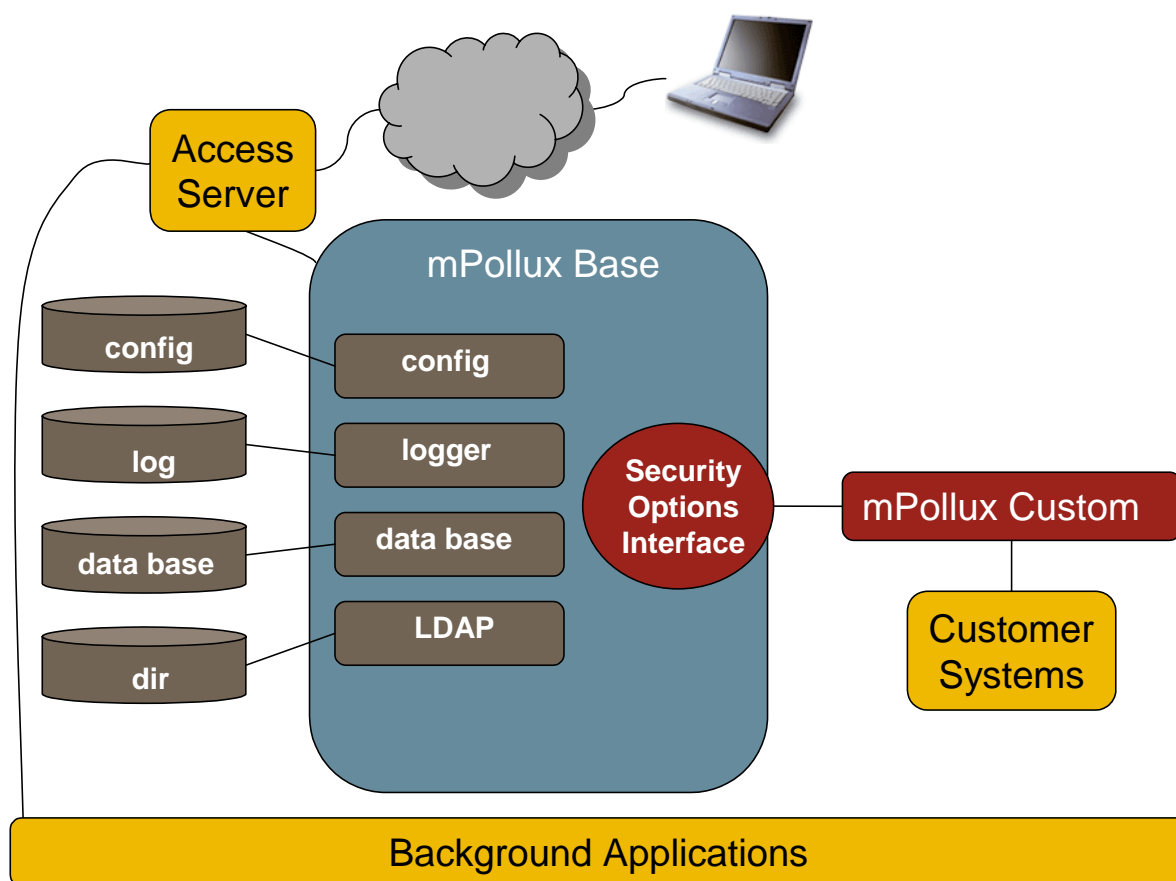


Figure 6 mPollux™ Custom Security Option

4.9 MPOLLUX™ LOGIN APPLICATION

The **Login Application** is a component, which acts as an access controller to the actual application server where user is about to enter. Login Application is an example of how to use mPollux™ API component and mPollux™ Security Server's functionality. Its functionality and user interface is configurable and it can be used in multi customer environments. Its main feature is multi-device and multi-channel support.

The Login Application can be also implemented to the Microsoft platform by using mPollux API for .NET. It uses then Microsoft Internet Information Server, Active Server Pages (ASP), ISAPI Filter, COM+ and .NET techniques.

4.10 MPOLLUX™ LOG BROWSER

The **Log Browser Tool** is an administration tool for mPollux™ Security Server, which enables the tracing and logging information browsing. The tool is made for system administrators to help them to analyze the log more easily.

Log Browser Tool is not part of basic Fujitsu mPollux Security Server delivery. Usage of Log Browser can be agreed separately.

4.11 MPOLLUX™ USER MANAGER

The **User Manager** is an administration tool, which enables the administration of user information saved in mPollux™ user register (SQL). The tool is made for system administrators to help them to add, edit and delete user relating information. Application supports multi customer environments and messaging. With messaging features User Manager can inform user's password and PIN changes via e-mail or SMS.

User Manager is not part of basic Fujitsu mPollux Security Server delivery. Usage of User Manager can be agreed separately.

4.12 MPOLLUX™ CONFIG TOOL

The **Config Tool** is an administration tool for mPollux™ Security Server, which enables view and edit functions for configuration files. The tool is made for system administrators to help them to change the configurations more easily.

Config Tool is not part of basic Fujitsu mPollux Security Server delivery. Usage of Config Tool can be agreed separately.

5 MPOLLUX™ SECURITY SERVER ENVIRONMENT

The following list separates the operational environments.

Operating System

- Microsoft Windows
- Sun Solaris
- IBM AIX
- Others, to be validated

Java Virtual Machine

- JDBC driver
- Sun J2SE v 1.5
 - Others, to be validated
- Java Application Server
- Microsoft SQL Server
 - Oracle
 - Postgre
 - MySQL Connector
 - IBM DB2
 - Others, to be validated
- Apache Tomcat 5.5.9
 - Others, to be validated