

**Fujitsu mPollux**

# **SMS Security Option**

## **White Paper**

Fujitsu mPollux Version 1.9

October 2005



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. The Possibilities are Infinite is a trademark of Fujitsu Limited. mCastor, mProcess, 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 tradenames of their respective owners.

---

## Table of Contents

1	INTRODUCTION .....	4
2	SPECIFICS OF CHALLENGE - RESPONSE BASED SECURITY .....	4
3	WHO WILL BENEFIT FROM THE SMS SECURITY OPTION? .....	5
4	MPOLLUX SMS™ USE SCENARIOS .....	6
4.1	General .....	6
4.2	SMS for Web Users .....	6
4.3	SMS for VPN Users .....	7
5	OVERVIEW OF THE MPOLLUX SMS™ SERVER ARCHITECTURE .....	8
5.1	mPollux™ Base Functionality .....	8
5.2	Components of the mPollux SMS™ Security Option.....	9

## 1 INTRODUCTION

The mPollux™ Security Server is Fujitsu Services' 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 **SMS Security Option**. It is based on a challenge – response authentication sequence using GSM short messages.

The mPollux™ Security Server with SMS Security Option consists of:<sup>1</sup>

- 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 SQL or LDAP user register.
- Connection to a GSM operator's SMS center for sending short messages to the users' mobile phone.

## 2 SPECIFICS OF CHALLENGE - RESPONSE BASED SECURITY

The SMS Security Option functionality is based on a challenge and response protocol between a mobile phone and mPollux™ Security Server. The challenge is a short message sent to the users' mobile phone. The challenge contains a random authentication code. The response is the same authentication code, which is entered to the system via a different channel.

### Implementation Assumptions

#### Short Message Service Center (SMSC)

A connection to an SMSC of one or more mobile operators is needed. The SMS Security Option messaging components have to be tailored for different kind of SMSC interfaces.

mPollux SMS™ Security Option supports SMSC http interface without tailoring.

---

<sup>1</sup> See the chapter "Overview of the mPollux SMS™ Server Architecture" for a more detailed description of the server architecture.

### 3 WHO WILL BENEFIT FROM THE SMS SECURITY OPTION?

The mPollux SMS™ Security Option is an authentication solution for Web and WAP users and applications that do not have the technical possibility or need for PKI level strong security. In some cases this level of security is, however, enough, and the setting up of an mPollux SMS™ Security Option 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.

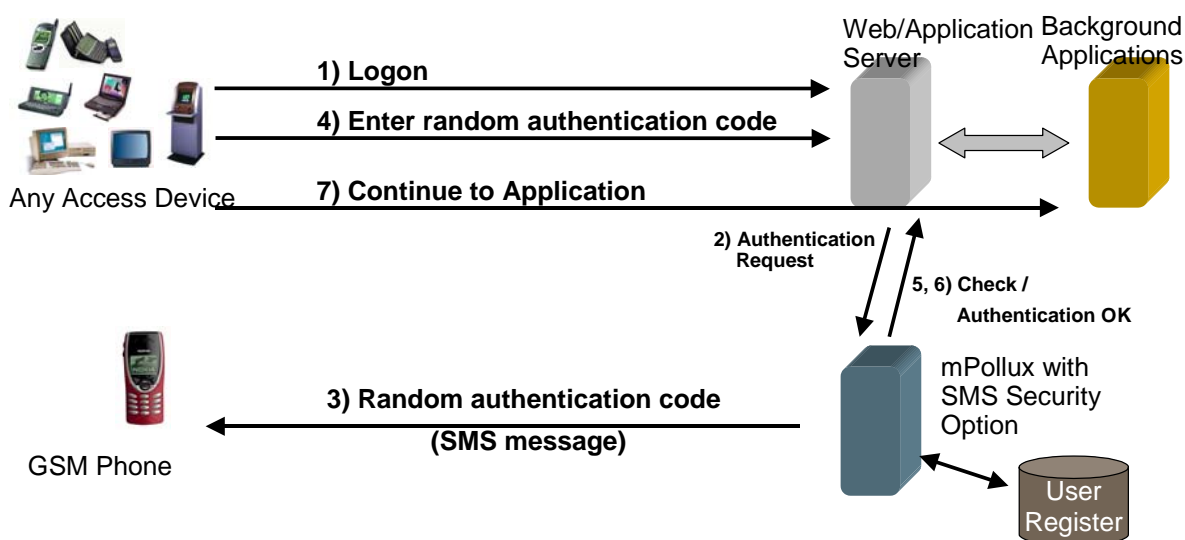
SMS Security Option is especially convenient for mobile device users, when authentication and application communication both are performed on the same device. Normally, those devices are able to receive short messages when the data connection (GSM Data or GPRS) is open.

## 4 MPOLLUX SMS™ USE SCENARIOS

### 4.1 GENERAL

The fundamental operation principles of mPollux SMS™ are the use of mobile phone and the challenge – response type authentication. Application asks user id from the user and passes the id to mPollux SMS™. mPollux SMS™ then generates a random authentication code and sends it to the users' mobile phone using SMS communication. The user reads the contents of the message and enters that as the response to the challenge on the application channel (Internet, GPRS, GSM Data, etc). mPollux SMS™ compares the sent challenge and the received response and authenticates the user that way.

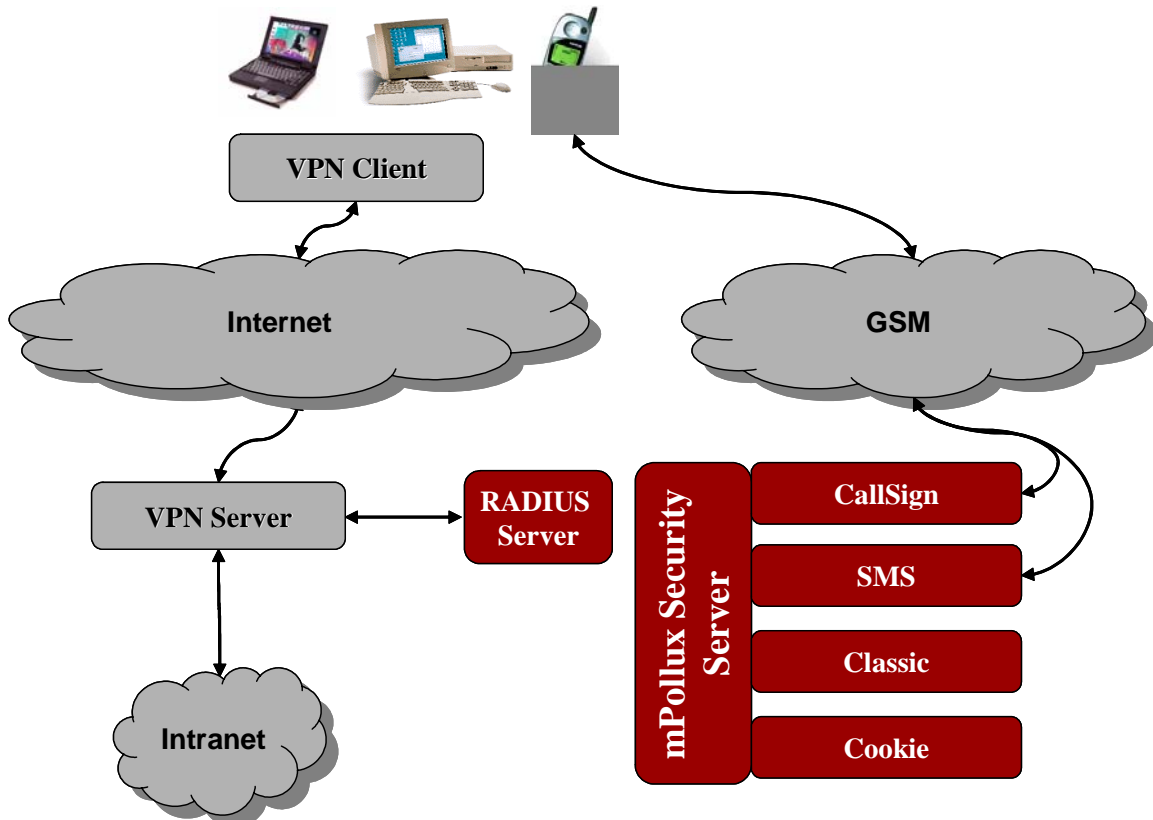
### 4.2 SMS FOR WEB USERS



**Figure 1 Authentication with mPollux SMS™**

Figure 1 presents the scenario where mPollux SMS™ is used with Web services. The only special requirement for the application is the ability to use the mPollux™ API to invoke the SMS Security Option. Figure 1 also shows the steps for mPollux SMS™ authentication.

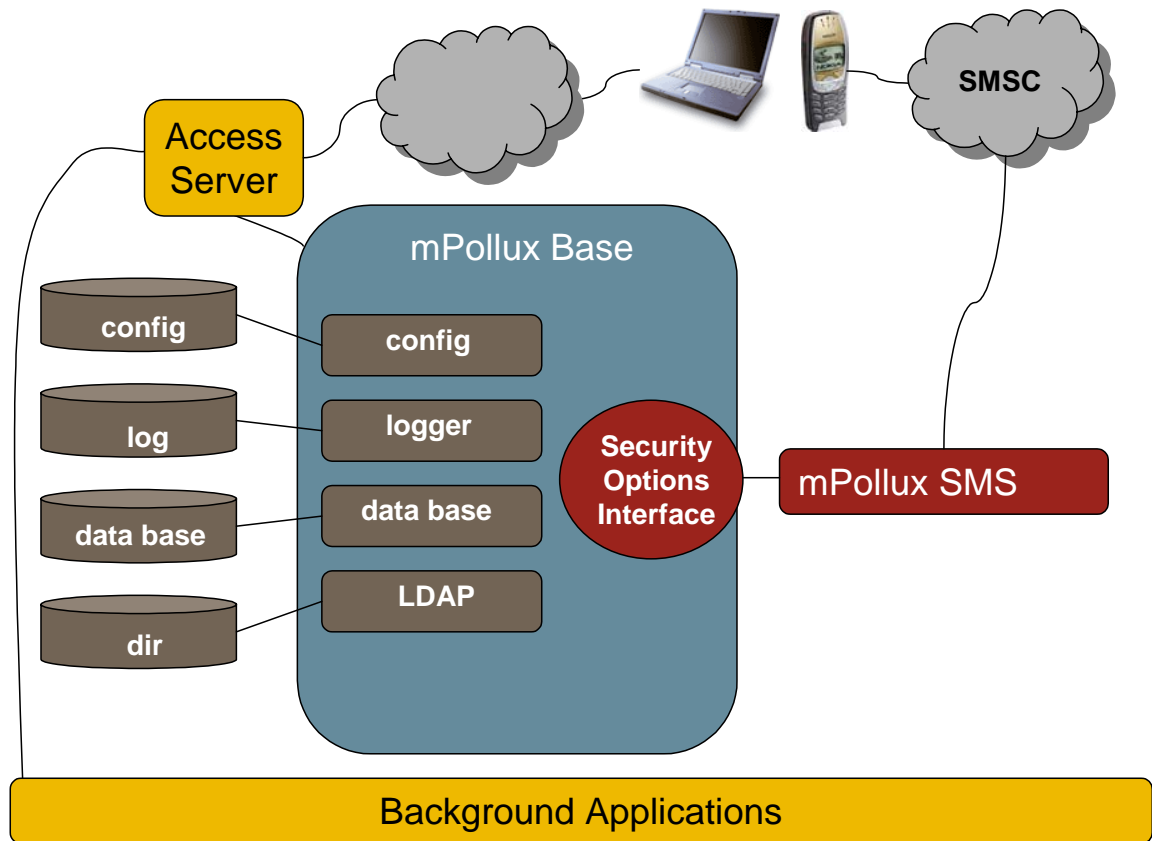
### 4.3 SMS FOR VPN USERS



**Figure 2 VPN Authentication with mPollux SMS™**

Figure 2 presents the scenario where mPollux SMS™ is used with VPN services. The only special requirement for the VPN is the ability to use Radius challenge – response authentication protocol. Also mPollux Radius Server is needed to establish this use case scenario.

## 5 OVERVIEW OF THE MPOLLUX SMS™ SERVER ARCHITECTURE



**Figure 3 mPollux™ with the SMS Security Option Server Architecture**

Figure 2 illustrates the general architecture of the mPollux™ Security Server with the SMS Security Option.

### 5.1 MPOLLUX™ BASE FUNCTIONALITY

#### Application Interfaces to mPollux SMS™

The Application Programming Interfaces to the mPollux SMS™ 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 SMS™ Security Option.

#### Access to User Register

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

## 5.2 COMPONENTS OF THE MPOLLUX SMS™ SECURITY OPTION

### mPollux SMS™ Server

The mPollux SMS™ Server is the component that handles the SMS Security Option authentication requests, and takes care of the responses to the requesting application. It uses the common base components for connection to user register (SQL or LDAP), logging etc. It also use tailored messaging component for sending and receiving the short messages.