

Fujitsu mPollux

CallSign & Citrix

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	MPOLLUX CALLSIGN™ FUNCTIONALITY	4
2.1	Authentication Challenge	4
2.2	Authentication Response	5
2.2.1	Dialing options.....	5
2.2.2	User Response Options	5
3	MPOLLUX CALLSIGN™ WITH CITRIX	6
3.1	Overall Architecture	6
3.2	mPollux Integration with IT-infrastructure	7
4	EXAMPLE OF MPOLLUX CALLSIGN™ WITH CITRIX.....	8
4.1	Authentication with Citrix Web Interface	8

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. Also, some cases may be better served with a more flexible approach that naturally permits multichannel implementations not tied to a specific device.

mPollux™ Security Server provides a range of security solutions from conventional user id – password authentication to full-scale PKI based security. **mPollux CallSign™** is a Security Option that provides security for applications when PKI level security is not desired or required. The security provided by **mPollux CallSign™** is based on a challenge – response authentication sequence using a telephone call. The **mPollux CallSign™** option is a general-purpose subsystem allowing any application to use authentication.

When integrated with **Citrix** remote access products, **mPollux™ Security Server** together with **mPollux CallSign™** option offers easy to use and manage, cost efficient and secure authentication method for end users.

2 MPOLLUX CALLSIGN™ FUNCTIONALITY

The mPollux CallSign™ Security Option implements a type of challenge– response authentication protocol. The mPollux CallSign™ option 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 are not constrained by mPollux CallSign™, but they are typically Web browser related. The authentication response is always performed over a phone line, normally using a mobile phone.

There is a comprehensive set of variations on the challenge – response sequence, enabling mPollux CallSign™ to be tailored to many different applications.

2.1 AUTHENTICATION CHALLENGE

When a service user attempts to access contents or services requiring authentication, mPollux CallSign™ issues an authentication challenge. Depending on the nature of the service and the security required, mPollux CallSign™ issues the challenge in various forms:

Silent Challenge. The user is expected to know that the challenge has been issued, but no visible evidence of this is given. The user must know the proper response in advance.

Default Challenge presents the user with a telephone number to dial for authentication.

PIN Challenge adds a request to enter the user's authentication PIN (a personal code chosen by the user during registration for the service) via the phone keypad. PIN Challenge is usually implemented in **callback mode**, i.e. so that instead of the user calling CallSign, CallSign calls back the user and then proceeds to request the user's PIN.

Variable Challenge presents a numeric one-time password and/or a one-time telephone number for authentication. The user must dial the given number and enter the given one-time password to authenticate him-/herself. Like PIN Challenge, Variable Challenge can as well be implemented in callback

mode. Callback is useful e.g. in cases where the authentication is done over an international telephone connection, which cannot generally carry calling line identification data to the called number.

2.2 AUTHENTICATION RESPONSE

2.2.1 DIALING OPTIONS

The primary authentication occurs when the user dials a given number and mPollux CallSign™ verifies the event. At the least, mPollux CallSign™ captures and verifies the number of the user's phone against a database of authorized users. The dialing opportunity is always time limited and must occur right after the challenge to dial has been made. The timeout for dialing is a configurable parameter.

Blind dialing of a predefined number after a silent challenge avoids the passing of any information about the dialing event over the Internet. The user must know in advance the number to dial and the authentication response expected after dialing. Blind dialing is especially useful when the application has no means of presenting the particulars of the dialing request to the user, or if it is desirable not to do so for security reasons (silent challenge).

Dialing a given predefined number is the default method to request authentication. There may be any number of dial-in phone numbers or rotaries. This allows a comprehensive billing structure to be built. Each number can have a specific call charge and the numbers are associated with the various services offered by the end applications.

Dialing a one-time number enhances security by making the dialing unpredictable.

Callback dialing is a possible alternative, if for some reason it is more viable that the user is called by mPollux™ instead of him/her having to call CallSign.

2.2.2 USER RESPONSE OPTIONS

When responding to the authentication challenge presented by mPollux CallSign™, the user has several options after placing the authentication call.

Simple authentication consists of a call from the user's phone to a mPollux CallSign™ dial-in number. The user passes no extra information and the call need not even be connected since mPollux CallSign™ can verify the number from the incoming call without answering it.

Authentication with PIN requires that mPollux CallSign™ accepts (or make) the call and record the PIN entered by the user. The PIN may be a fixed one given to the user, or it may be a one-time password that mPollux CallSign™ generates for this particular authentication attempt.

3 MPOLLUX CALLSIGN™ WITH CITRIX

3.1 OVERALL ARCHITECTURE

For an overview of the overall architecture of the mPollux™ Security Server, see the **mPollux™ Security Server White Paper**. For more detailed information of the mPollux CallSign™, see the **mPollux™ CallSign White Paper**.

Figure 1 shows one possible architecture of the mPollux™ Security Server and CallSign Security Option when integrated with Citrix Web Interface. In general, mPollux CallSign is integrated with the Citrix Web Interface and all the Citrix systems that use Web Interface for authentication can also use mPollux CallSign as an authentication method. This includes e.g. users using browser to access MetaFrame Farm applications and also VPN users using Access Gateway.

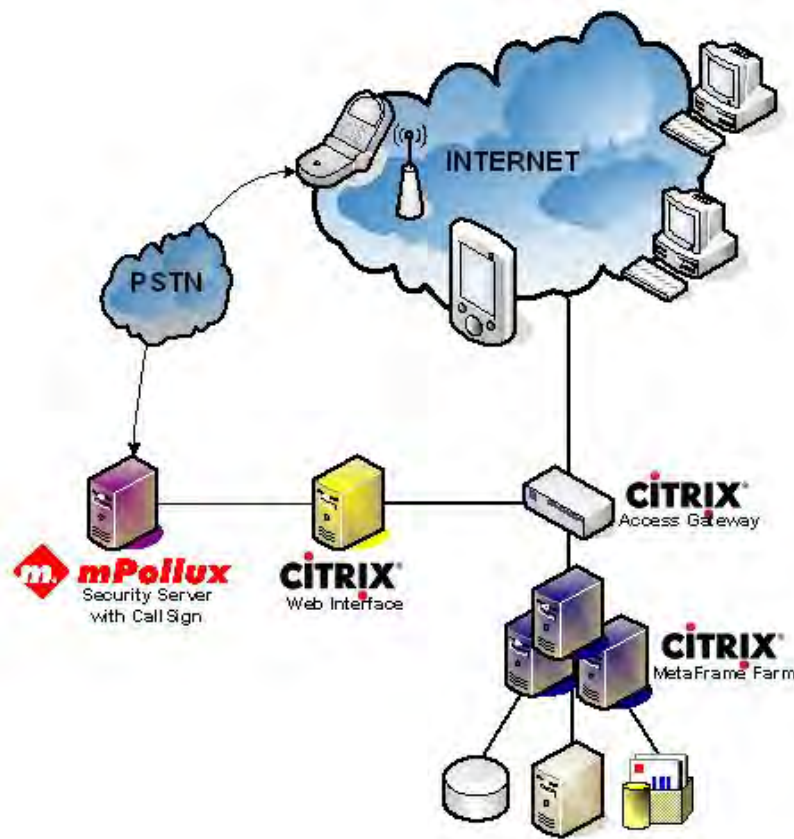


Figure 1 The Architecture of mPollux™ Security Server with Citrix

The main components of mPollux CallSign™ are

- **mPollux™ API** and **mPollux™ Base**, which are the common components for all mPollux™ Security Options. mPollux™ API is installed to the Citrix Web Interface server.
- **CallSign Security Option (SO)** and **CallSign Server**, which are the specific components of mPollux™ Security Server with CallSign Security Option.

3.2 MPOLLUX INTEGRATION WITH IT-INFRASTRUCTURE

mPollux™ Security Server can use any standard LDAP directory or Database with JDBC connectivity as a user directory. Typically in corporate environment, Microsoft Active Directory or some other directory is used to store CallSign authentication related data.

When mPollux™ Security Server with CallSign Security Option is integrated with Citrix for end-user authentication, there are several advantages over other authentication approached:

- Users are authenticated with strong two-factor authentication in addition to normal Windows authentication.
- There is no need for additional security tokens or other hardware components for every user, users are using their mobile phones for authentication. This greatly reduces costs (hardware, logistics, management, ...).
- There is no need for an additional user directory for CallSign, e.g. existing Active Directory can be used.
- CallSign Security Option can use e.g. user's mobile phone number stored in Active Directory. This can be managed through normal user management processes; there is no need for additional management.
- CallSign Security Option authentication can check from the Active Directory whether user account in Windows domain is disabled or locked and does not allow authentication in these situations. Also other sophisticated access control rules can be defined.
- In Citrix Web Interface login, users do not need to enter additional codes or information, normal Windows credentials are sufficient. This enables user-friendly experience for end-users and reduces errors.

4 EXAMPLE OF MPOLLUX CALLSIGN™ WITH CITRIX

4.1 AUTHENTICATION WITH CITRIX WEB INTERFACE

A user accesses remotely corporate applications through Internet using Citrix. User uses Citrix Web Interface application to login and launch applications. During Web Interface authentication, user is authenticated both with CallSign authentication call and ordinary Windows authentication. CallSign authentication is performed through separate channel (mobile phone network) which further increases the security of the system.

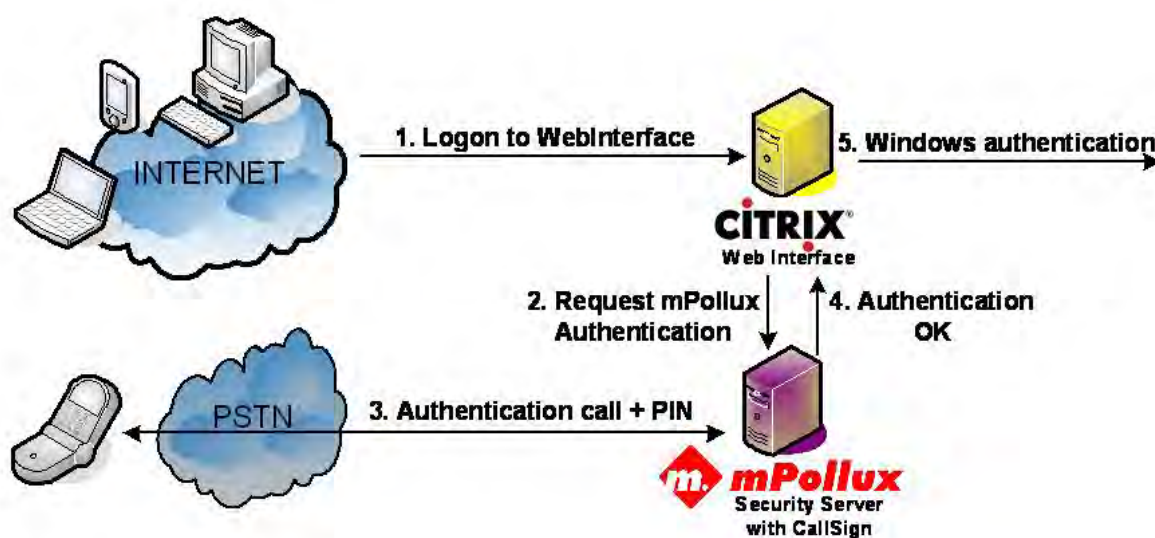


Figure 2 mPollux CallSign™ applied to Citrix Web Interface Authentication

The access sequence proceeds as follows (refer to **figure 2**):

1. User browses to Web Interface login-page and enters valid Windows credentials (username & password) to log in.
2. Using a secure connection, the mPollux™ API requests CallSign™ authentication for the user.
3. The user's profile is retrieved from a local or remote database or directory by mPollux Call-Sign™, which generates an authentication scheme. Typically this includes the mobile phone number and user's PIN code. The scheme is sent to the CallSign Server ISDN, H.323 or SIP interface for verification.

CallSign Server places a call to the user's mobile phone, and asks user to authenticate using his/her PIN-code.

4. The mPollux CallSign™ Server records the call event and any received extra info and presents them to mPollux CallSign™ Security Option. The identification is validated by CallSign that informs the Citrix Web Interface of the result through mPollux™ API.
5. If CallSign authentication is successful, Citrix Web Interface continues normally authenticating user's Windows credentials.