

Fujitsu mPollux

CallSign Security Option

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	5
2.2	Authentication Response	5
2.2.1	Dialing options.....	5
2.2.2	User Response Options	5
2.3	Profiles	6
3	MPOLLUX CALLSIGN™ ARCHITECTURE.....	7
4	EXAMPLES OF MPOLLUX CALLSIGN™ USE CASES.....	8
4.1	Case 1: Accessing Confidential Web Pages.....	8
4.2	Case 2: Micropayment	9
4.3	Case 3: Purchase from a Vending Machine	10
4.4	Case 4: Physical Access Security	10
4.5	Case 5: Pre Authentication.....	11
4.6	Case 6: CallSign Authentication for VPN.....	13

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.

A straightforward method to charge for access or contents is to charge the user's telephone account. For that purpose, **mPollux CallSign™** can maintain a set of dial-in rotaries with varying charge structures. The requested services are associated with authentication phone numbers with the desired charge profile.

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 can alternatively be 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™ accept (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.

2.3 PROFILES

Profiles stored in the mPollux CallSign™ Profile Database enable the authentication to be made according to the security requirements of each application and each individual user. When the end application provides anonymous services, the user may not need a User Profile and it may not be desirable to have one. In such cases, the authentication should be made using one-time PINs to securely associate the user with a specific call for billing purposes.

The Profile Database for registered applications contains the information needed for security, billing, and user identification requirements. The Profile Database for users contains the predefined authentication and identification information required to reliably identify users for the serving application.

3 MPOLLUX CALLSIGN™ 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 CallSign Security Option.

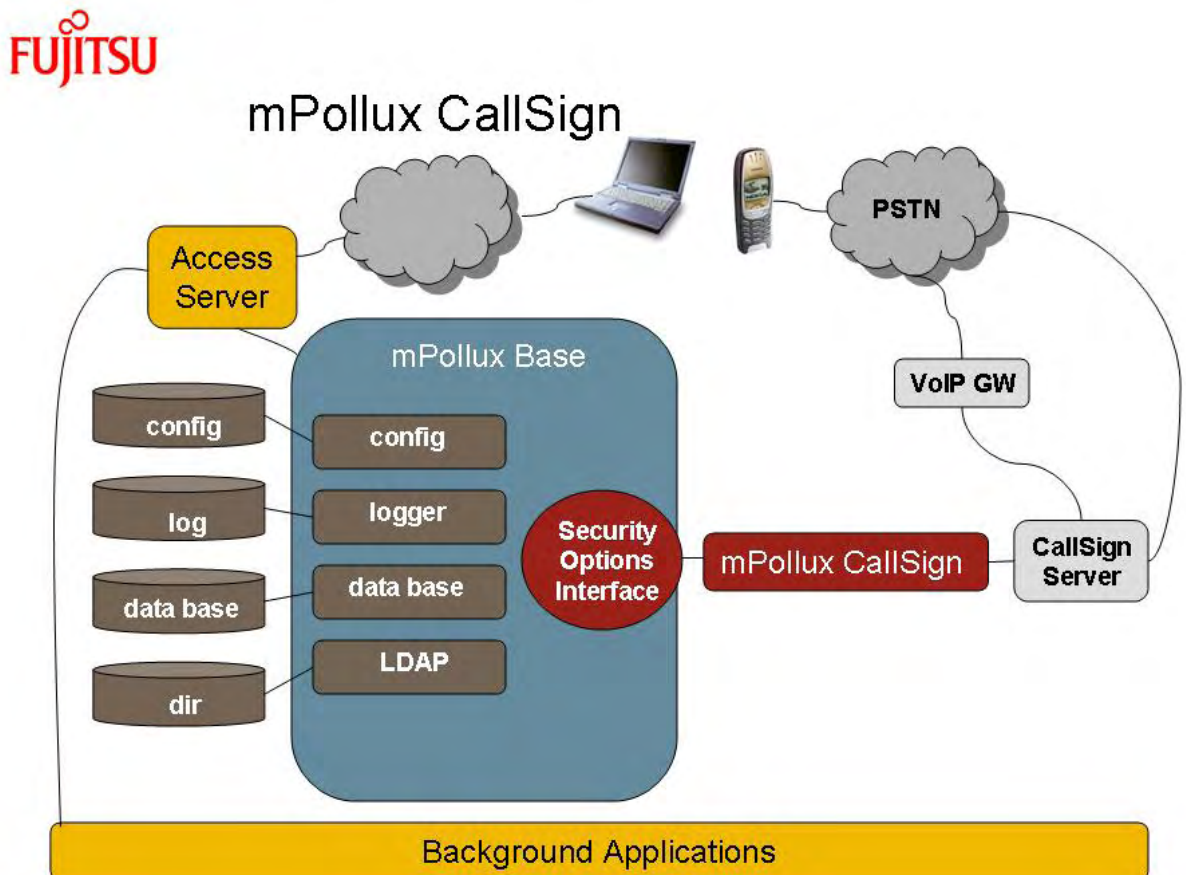


Figure 1 The Architecture of mPollux™ Security Server with CallSign Security Option

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

- **mPollux™ API** and **mPollux™ Base**, which are the common components for all mPollux™ Security Options, and
- **CallSign Security Option (SO)** and **CallSign Server**, which are the specific components of mPollux™ Security Server with CallSign Security Option.

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 CallSign – executes the ser-

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

CallSign SO module coordinates and controls the user authentication process driven by the service calls from the user application and according to the CallSign profile relevant to the user. The role of the CallSign Server is to supervise and control the telephone lines (ISDN and VoIP H.323 or SIP connections) connected to it, receive user input and hand it over to CallSign SO for validation, and the generation of voice responses to the user during the authentication dialog. CallSign SO controls the CallSign Server over a secured TCP/IP sockets connection using an internal service interface.

Because of the architecture, mPollux™ Security Server functionality can be run either on the Application or Web server platform or on a separate server. The CallSign Server is a separate piece of hardware that may be situated in the same site as the other concerned servers or in a remote site. The CallSign server runs on Red Hat Enterprise Linux 4 operating system using standard PC hardware. CallSign is connected to the public switched telephone network (PSTN) through ISDN or VoIP H.323 or SIP interface.

4 EXAMPLES OF MPOLLUX CALLSIGN™ USE CASES

4.1 CASE 1: ACCESSING CONFIDENTIAL WEB PAGES

A user accesses the contents of a Web site. Some or all of the contents are confidential with restricted access. The user is identified by a UserID/password combination. In addition, the system requires an authentication call to a given number combined with a one-time PIN.

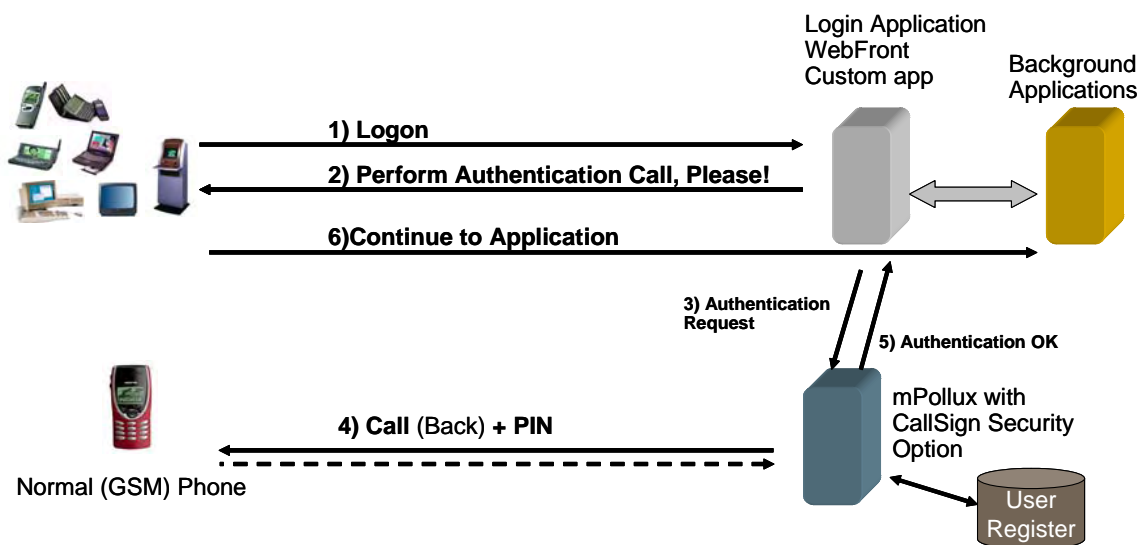


Figure 2 mPollux CallSign™ applied to Web User Authentication

- The **Web Server** provides users with contents that are either restricted or subject to payment or licensing. The Web Server uses **mPollux CallSign™** to authenticate users and/or register payments for licensed content.
- The **mPollux™ Security Server** provides user authentication services to the Web Server. The authentication is based on the identification of the telephone call as originating from the user requesting a specific service. The

user places the call when requested by the Web Server, will hereby be identified by the telephone network, and finally validated by mPollux CallSign™ SO. There is no built-in restriction on the number of Web Servers that one mPollux CallSign™ Server can handle.

- The **mPollux CallSign™ Server** interfaces with an ISDN rotary or VoIP H.323 or SIP at the local telephone exchange to receive authentication calls from users. The user is identified by mPollux CallSign™ with the phone number that is stored in a local or remote user database or directory.

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

1. The user attempts to access restricted contents. The application in the Web Server makes a request via the mPollux™ API to start the authentication sequence.
The Web application presents the user with a login form. The user enters his/her User ID and optional password or PIN.
2. Using a secure connection, the Web application passes the login information through mPollux™ API to mPollux CallSign™ for authentication.
3. The user's profile is retrieved from a local or remote database or directory by mPollux CallSign™, which generates an authentication scheme. The scheme may include an additional one-time PIN to be entered from the phone, a specific one-time call number from the dial-in rotary, and/or some other additional identification information. The scheme is sent to the Call-Sign Server ISDN, H.323 or SIP interface for verification.
The user places a call to the given number, optionally entering the extra information, and terminates the call.
4. The mPollux CallSign™ Server records the call event and any received extra info presenting them to mPollux CallSign™ Security Option. The identification is validated by CallSign that informs the Web application of the result through mPollux™ Base and mPollux™ API.
5. Based on the reported result, the Web application grants or denies access to the requested contents.

4.2 CASE 2: MICROPAYMENT

The user buys a new operator logo and ring tone for his/her mobile phone.

1. The user browses the logos and ring tones on the vendor's Web page, selects the ones he/she wants, and starts the purchase function.
2. The Web Server passes the authentication request to mPollux CallSign™ indicating the cost attached to the selection the user made.
3. A challenge is formulated for the user by mPollux CallSign™. The indicated phone number that is to be dialed reflects the charge accumulated for the logo and ring tone. To reliably associate this particular user with the transaction, a one-time PIN is generated. The challenge is returned to the Web Server for presentation to the user. At the same time, the challenge is passed to mPollux CallSign™ for verification.

4. When the user places the call and enters the given PIN, payment has been made (via the phone bill). The phone number is intercepted by mPollux CallSign™ for transaction completion. The logo and the ring tone are sent e.g. as SMS messages to the user's phone.

4.3 CASE 3: PURCHASE FROM A VENDING MACHINE

A vending machine offers goods that can be bought by phone and paid for via a phone bill. The machine is connected to mPollux CallSign™ using a suitable network interface.

The vending machine displays a number to dial for purchasing. When the user dials the number, mPollux CallSign™ confirms the call and enables the vending machine via the network connection. The user selects a product.

If the product prices vary, more features are needed in the solution. Assuming the vending machine can display information that changes, the purchase sequence can be generated in cooperation with mPollux CallSign™:

1. The user selects a product.
2. The vending machine requests authentication from mPollux™, indicating the item price.
3. A suitable phone number with the correct call charge is picked by mPollux™, which returns this to the vending machine for display
4. The user calls the given number. The call is verified by mPollux CallSign™, which authorizes the vending machine to release the product.

Finally, in complex cases mPollux CallSign™ can generate any phone charge on the fly and pass it to the local phone exchange provided the exchange has a suitable interface and permits this kind of configuration.

4.4 CASE 4: PHYSICAL ACCESS SECURITY

A secure site requires secondary confirmation of the identity of a person entering. There are numerous variations of this scenario. In this case, minimal visible evidence of access security is assumed.

A silent alarm system guards the secure site. There is no need for any extra keypads or card readers for access control, other than those required to unlock the door. Instead, a call authentication within specific timeout must confirm any physical access attempt, otherwise an alarm is issued. Persons entering must be aware of the procedure in advance.

1. The user opens the door that the alarm system guards.
2. The alarm system informs mPollux CallSign™ of the identity of the opened door.
3. mPollux CallSign™ prepares itself to expect a call to a given number within a specific time period.
4. If a call is received within the timeout period, mPollux CallSign™ verifies that the phone number has been granted access rights and passes the key-

pad data or extra data back to the alarm system for verification. Alternatively, special functions in CallSign can verify the data and pass the result to the alarm system. If no call is received or false data is sent, a failure is reported to the alarm system, which then goes into an alarm state.

The authentication scheme that mPollux CallSign™ expects would typically be a combination of the identities of the door accessed and the person entering or leaving. If the doors have access security devices with a display, a one-time PIN could be shown as a challenge.

In later mPollux CallSign™ product versions, integration with mobile phone location services will be possible. When mPollux™ can verify the physical proximity of the phone, CallSign can in some cases grant access (by unlocking a door) without keys, keycards, etc.

4.5 CASE 5: PRE AUTHENTICATION

Normal CallSign™ authentication is not always possible for technical reasons. Then CallSign™ pre-authentication can be used. Technical reasons could be for example.

- Phone is used as network connection device (modem)
- Browser resides in same phone and GSM data is used

Pre-authentication means that authentication session is created with CallSign™ before actual application usage and application login procedure uses that authentication session.

1. mPollux CallSign™ answers to users phone call in service specific number.
2. Users phone number is checked form user register.
3. Authentication PIN code is asked from user and checked towards user register.
4. Session PIN code is asked from user and stored to authentication session. Authentication session is valid for example two minutes.
5. CallSign™ usage is ended.
6. User starts Web session with same phone and navigates to service.
7. Service requires users phone number and session PIN code. If phone number is in user register and session PIN code can be verified, then authentication is successfully done.

Service indication messages can be used to help users to establish connection and navigate to service. Message is sent then after CallSign™ usage.

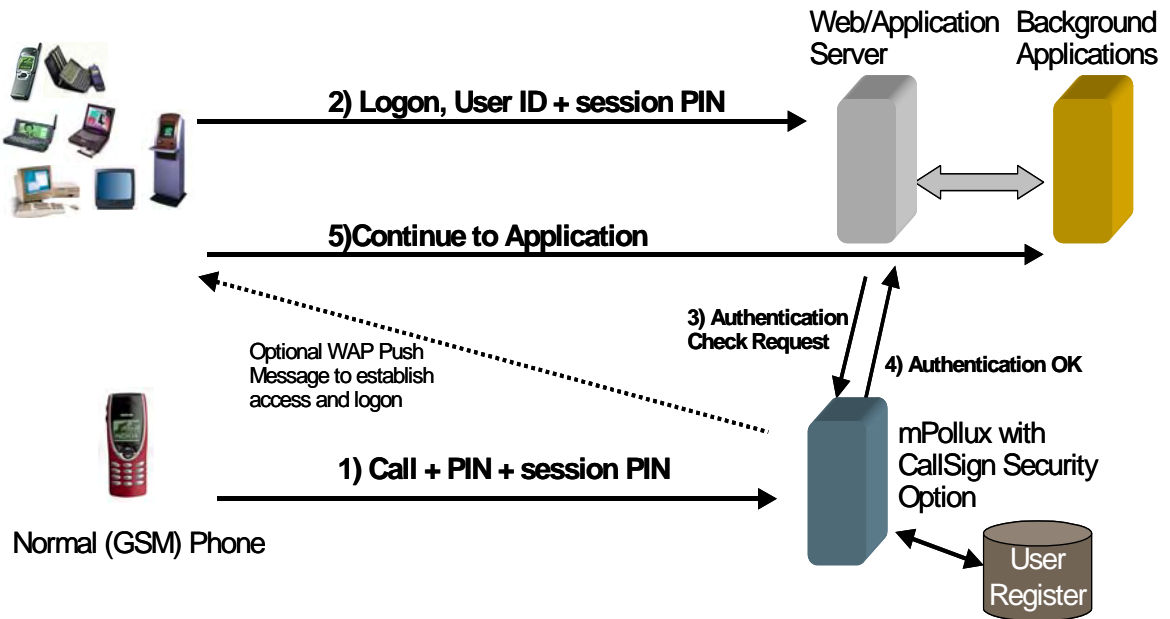


Figure 3 mPollux CallSign™ pre-authentication

4.6 CASE 6: CALLSIGN AUTHENTICATION FOR VPN

CallSign authentication can be used with VPN. Then mPollux Radius Server is needed between VPN server and mPollux Security Server and VPN server must be Radius enabled. Authentication steps are similar than in web authentication case.

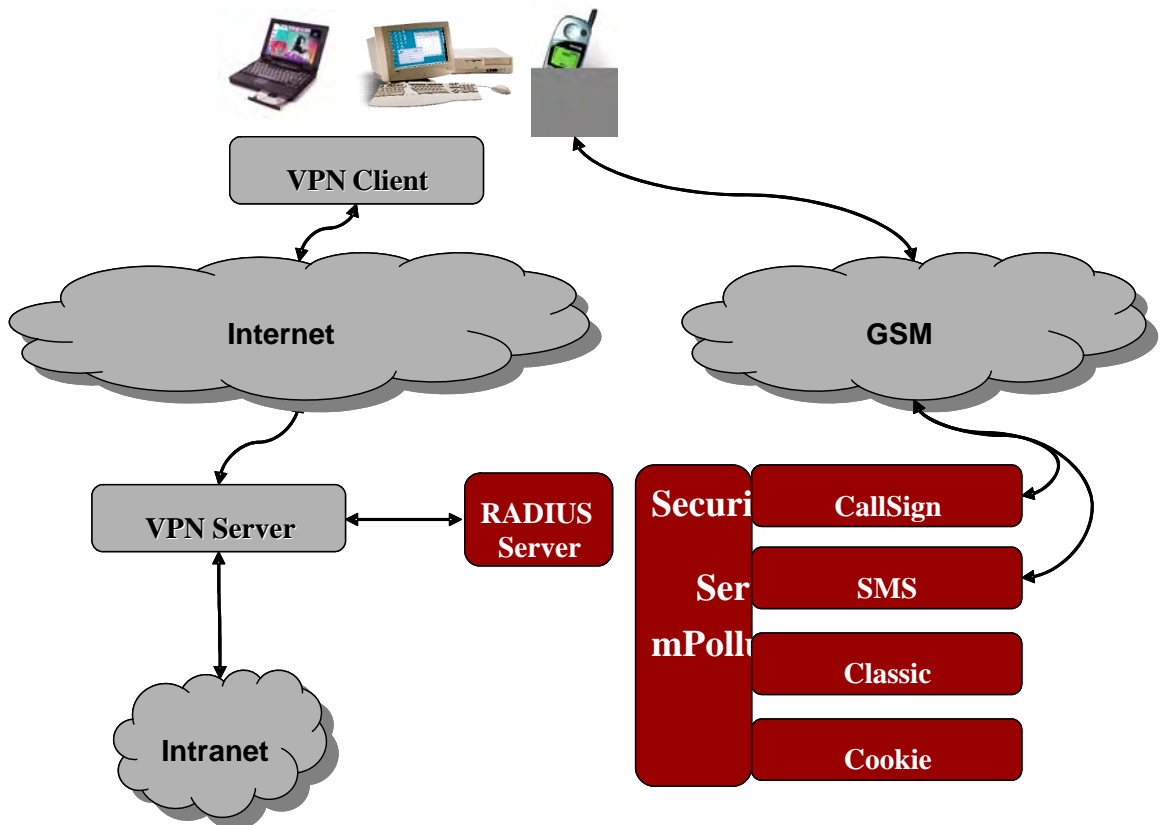


Figure 4 mPollux CallSign™ authentication for VPN