THE POSSIBILITIES ARE INFINITE

Fujitsu mPollux

Cookie Security Option

White Paper

Fujitsu mPollux Version 1.9

October 2005

First Edition 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.

Table of Contents

1 INTRODUCTION

Fujitsu 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 **Cookie Security Option** that is designed to help **access control** and **single sign-on** implementations.

The mPollux™ Security Server with Cookie 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 Cookie Security Option, which can be implemented using either symmetric or asymmetric encryption algorithm.

2 SPECIFICS OF TOKEN BASED ACCESS CONTROL

With the Cookie Security Option applications can let mPollux™ create tokens and check their validity. The token is encrypted and cannot be modified without errors in access control. The only place where the token can be checked correctly is mPollux Cookie™ Security Option. The token is passed to the application by communication protocol specific method: as a HTTP cookie, as a HTTP URL parameter, within XML document, etc.

Implementation Assumptions

Symmetric encryption (3DES)

Token encryption is done with the symmetric encryption algorithm 3DES. Symmetric encryption is implemented in software. Symmetric keys are stored in the same place where Cookie Security Option configurations are. This means that a symmetrically encrypted Cookie is less secure than an asymmetrically encrypted cookie.

Asymmetric encryption (RSA)

Token encryption is done with the asymmetric encryption algorithm RSA. Asymmetric encryption and key storage are implemented in the Java software components and key storages. Asymmetric encryption is based on key pairs and key lengths are long enough to achieve high security

Validity time and shared secret

The encrypted token contains the validity and creation time of the token and shared secret information. The shared secret is created when the token is created, and the application using the token for access control should also know it. However, the

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

only place where the token can be decrypted and checked is the mPollux Cookie™ Security Option.

One-Time Credentials

One-time credentials are one type of security token (random user id and password). After creation credentials have validity time and credentials can be checked only once. During validity time mPollux Cookie™ Security Option can store authentication information. Encryption is done with the asymmetric encryption algorithm RSA. Asymmetric encryption and key storage are implemented in the Java software components. Asymmetric encryption is based on key pairs and key lengths are long enough to achieve high security.

Global session

Different applications of system might create and delete its own session. If system will use separated access control component, like mPollux WebFront, session information should be stored in centralized place. mPollux Cookie™ Security Option can store global session information and offers application interfaces to ask session status. This way different applications and separated access control can have total understanding of user's application sessions and global session.

3 WHO WILL BENEFIT FROM THE COOKIE SECURITY OPTION?

Session key and security token

The Cookie Security Option could be part of an access control and/or single sign-on solution. The solutions that use the Cookie Security Option do not need their own security token and session key implementation, so applications can concentrate on their own functionality and business logic.

Rely on external authentication

The Cookie Security Option out burdens the authentication functionality from applications. Applications need just to check the validity of tokens and rely on mPollux™ Security Server's authentication.

Using one-time credentials

The Cookie Security Option can generate and check one-time credentials and store and move mPollux™ authentication session to 3rd party applications. 3rd party applications need just to use Radius or other supported authentication protocols to check authentication status.

4 MPOLLUX COOKIE™ USE SCENARIOS

4.1 GENERAL

The fundamental operation principle of mPollux Cookie™ is the usage of a secure token. Secure tokens are created for authenticated users, and applications can rely their access control on them.

4.2 COOKIES AND WEB SERVER FILTER

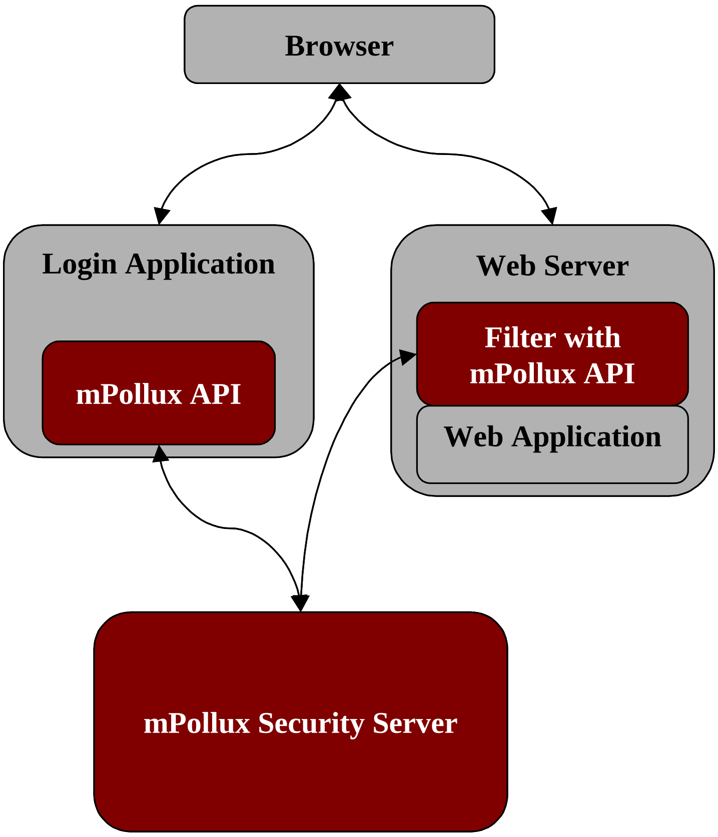

Figure 1 Web Server Filter and mPollux Cookie™

Figure 1 presents the scenario where mPollux Cookie™s are used with a web server filter. The filter checks every HTTP request to the web server and if the request needs to be authenticated, it checks the validity of secure the token (HTTP cookie).

4.3 COOKIES AND APPLICATION LEVEL ACCESS CONTROL

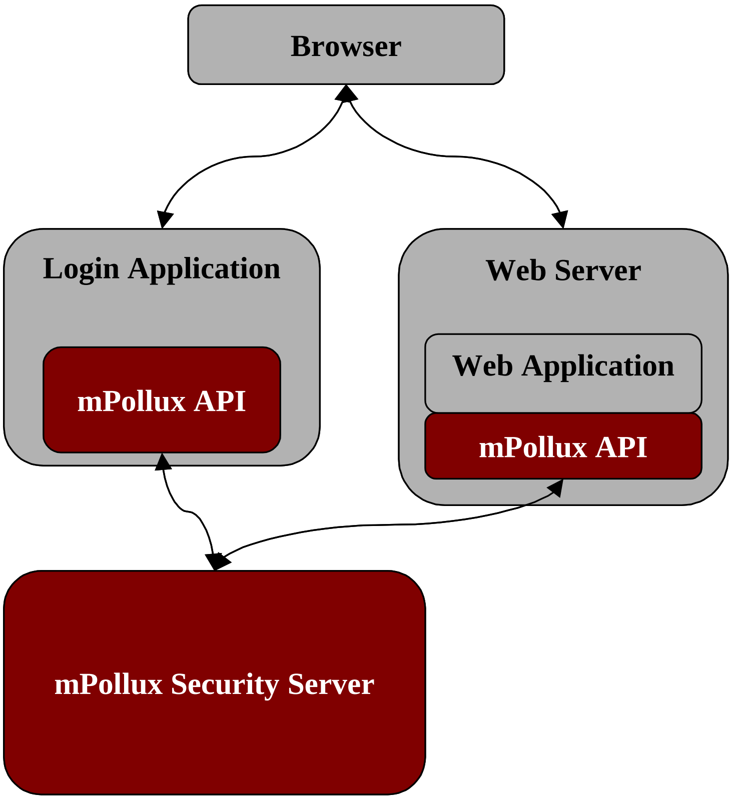

Figure 2 Application level access control and mPollux Cookie™

Figure 2 presents the scenario where mPollux Cookie™s are used with the application level access control. The application checks every request and if a request needs to be authenticated, it checks the validity of the token (i.e. HTTP cookie or URL parameter). Difference from the previous case is that some application integration is needed (mPollux™ API).

4.4 SSO WITH ONE-TIME CREDENTIALS

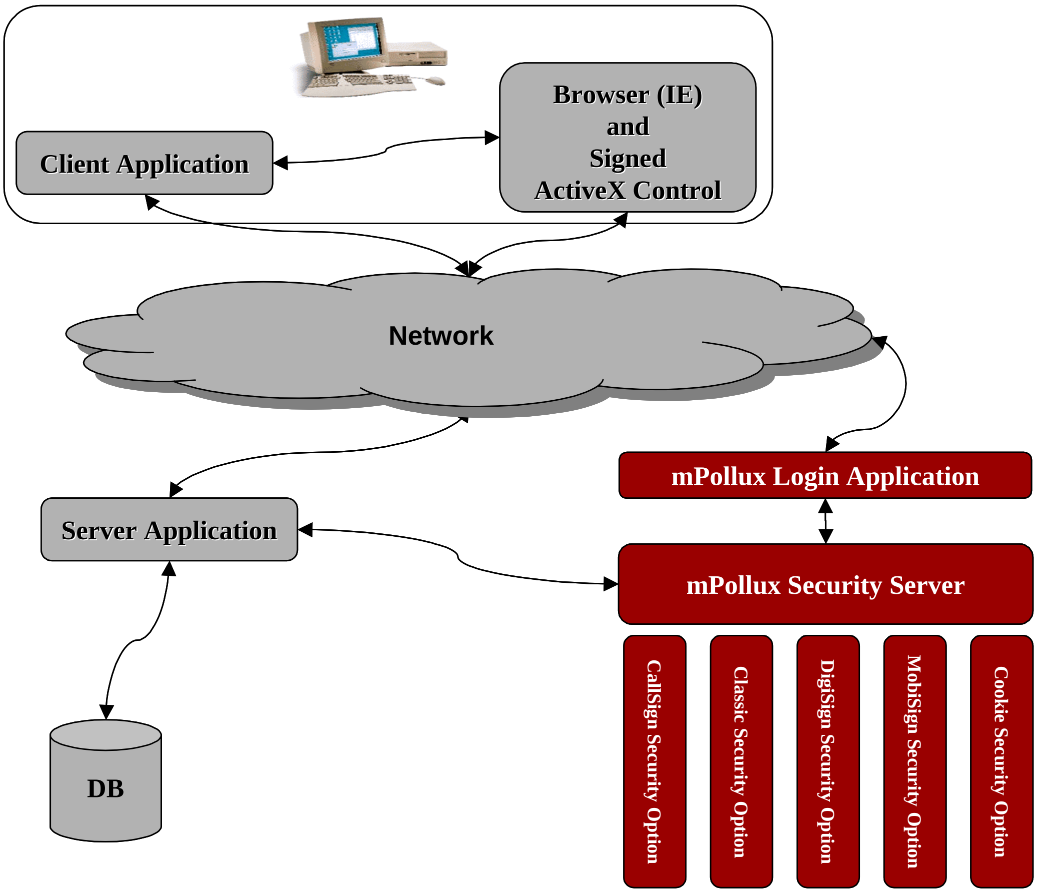

Figure 3 One-Time Credentials and mPollux Cookie™

Figure 3 presents the scenario where mPollux Cookie™ Security Option is used for creating and checking one-time credentials. After successful authentication, Login Application can ask one-time credentials (random user id and password) from mPollux Cookie Security Option and pass those via browser (ie. Signed ActiveX component) to other client applications. Other application use for example mPollux Radius authentication interface and that way Cookie Option checks one-time credentials validity. This is scenario where for example mPollux DigiSign™ authentication can be used with native VPN client without adding smart card and PKI functionality to VPN system.

5 OVERVIEW OF THE MPOLLUX COOKIE™ SERVER ARCHITECTURE

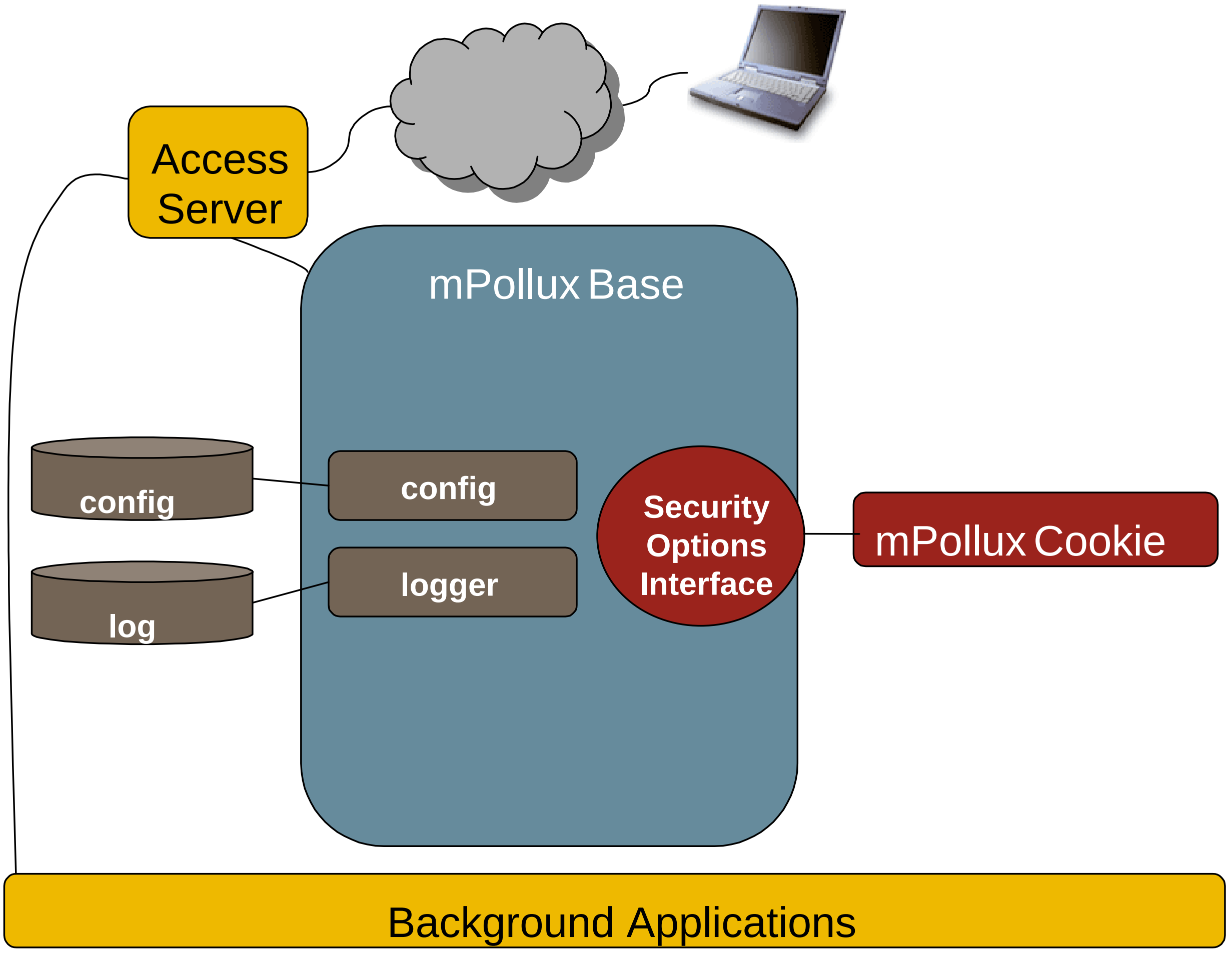

Figure 4 mPollux™ with the Cookie Security Option Server Architecture

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

5.1 MPOLLUX™ BASE FUNCTIONALITY

Application Interfaces to mPollux Cookie™

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

5.2 COMPONENTS OF THE MPOLLUX COOKIE™ SECURITY OPTION

mPollux Cookie™ Server

The mPollux Cookie™ Server is the component that handles Cookie creations and validity checking.