FUJITSU

THE POSSIBILITIES ARE INFINITE

Fujitsu mPollux

SAML Security Option

White Paper

Fujitsu mPollux Version 2.1

June 2016

Table of Contents

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.

mPollux™ Security Server provides a range of security solutions from conventional user id – password authentication, telephone call authentication to full-scale PKI based security. **mPollux™ SAML** provides web-based single sign-on functionality for the mPollux authentication service.

mPollux™ SAML implements the roles identity provider (IdP) and service provider (SP).

2 MPOLLUX SAML FUNCTIONALITY

The mPollux™ SAML implements SAML 2.0 specification's Web Browser SSO Profile and Single Logout Profile. These profiles are used to provide web-bases single sign-on functionality between security domains.

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/
- http://www.projectliberty.org/liberty/specifications__1

There are both identity provider and service provider roles. An identity provider is responsible for management of identities, authenticating user and producing assertions. A service provider redirects user to authenticate when necessary and consumes assertions produced by identity provider.
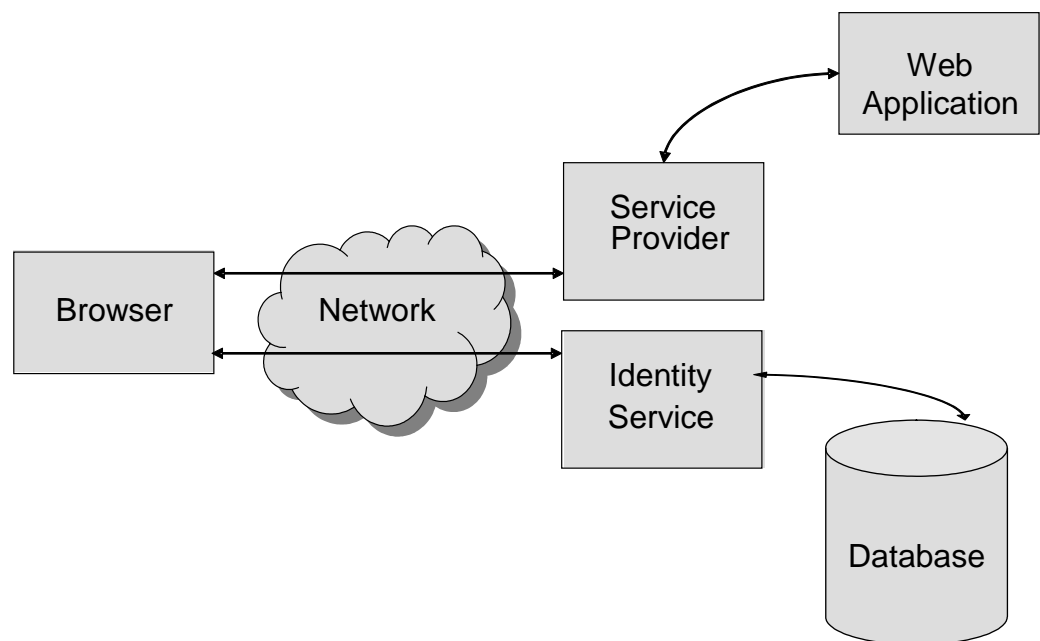

Figure 1 mPollux™ SAML provider roles

About the SAML profiles, the supported features are,

- **Web Browser SSO,** profile to provide web-bases cross-domain single sign-on functionality.

- **Single Logout**, profile to terminate own session with all session participants.

- **Attribute Query,** profile is for requesting attributes for specified subject.

2.1 WEB BROWSER SSO

Web Browser SSO profile provides web-bases cross-domain single sign-on functionality. A service provider issues an authentication request to an identity provider. The identity provider authenticates the user (or has already authenticated), and then provides an authentication assertion to the service provider.

This above is performed using profile of the SAML Authentication Request protocol.

2.2 SINGLE LOGOUT

Single Logout profile is used to terminate user session with all session participants. After Web Browser SSO profile is used, user's sessions exist in the identity provider and service providers, which are used during that session. When user or session authority wants to terminate user's global session, Single Logout request is sent to all session participants. Asynchronous front-channel binding is required when user session exists in a user agent in the form of cookie.

2.3 ATTRIBUTE QUERY

Attribute Query messages from Assertion Query/Request profile is used for requesting attributes for specified subject. This profile uses synchronous SAML SOAP binding and is performed using back-channel after user is authenticated.

2.4 IDENTITY PROVIDER

Identity provider is SAML participant role that is defined to support Multi-Domain Single Sign-On. An identity provider is responsible for management of identities, authenticating user and producing assertions.

2.5 SERVICE PROVIDER

Service provider is SAML participant role that is defined to support Multi-Domain Single Sign-On. A service provider redirects user to authenticate when necessary and consumes assertions produced by identity provider.

3 MPOLLUX SAML 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 SAML.
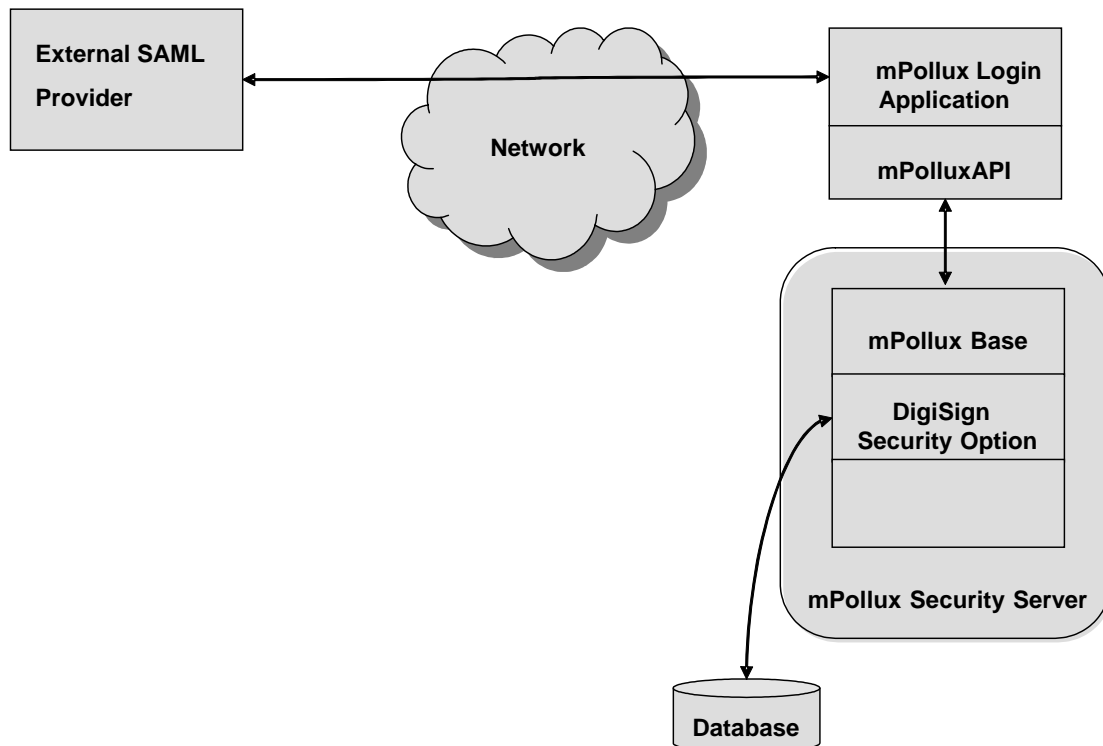

Figure 2 The Architecture of mPollux™ Security Server with SAML

As *figure 1* shows, the main components of mPollux™ Security Server with SAML are

- **mPollux™ API** and **mPollux™ Base**, which are the common components for all mPollux™ Security Options, and

- **mPollux™ Login Application,** which provides user interface,

- **External SAML Provider**, a service provider or an identity provider

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

Because of the architecture, mPollux™ Security Server functionality can be run either on the Application or Web server platform or on a separate server.

3.1 MPOLLUX™ SERVER

mPollux Server uses mPollux Bases for the basic function like logging, DB connection etc… please see "mPollux Service Description".

mPollux Server itself manages the SignXML, SignPKCS1, CheckXMLSignature and CheckPKCS1Signature based on Client request.

mPollux Server with utilizing mPollux Bases, provides the features as follows,

- **Data connections,** mPollux Base provides connections for fetching data from common SQL DB and LDAP directory.

- **SignXML/SignPKCS1/CheckXMLSignature/CheckPKCS1Signature**, mPollux Server proceed signing/checking utilizing mPollux Bases functions.

- **Authentication methods**: mPollux CallSign™, mPollux PalmSign™. mPollux DigiSign™, mPollux MobiSign™, mPollux Classic™ and mPollux SMS™.

- **Transaction Log,** mPollux Server provides the simple transaction log of client/server communication.

3.2 MPOLLUX™ LOGIN APPLICATION

mPollux™ Login Application provides identity provider and service provider functionality with mPollux Server integration. Its functionality and user interface is configurable and it can be used in multi customer environments. The application runs on Java Application Server as web application.

When mPollux™ Login is used as service provider, Login component acts as an access controller to the actual application server where user is about to enter.

When mPollux™ Login is used as identity provider, Login component authenticates users using authentication methods that mPollux™ Server provides.

4 EXAMPLES OF MPOLLUX SAML USE CASES

4.1 CASE 1: MPOLLUX AS SAML IDENTITY PROVIDER

When you need to offer authentication services for web applications, mPollux as SAML identity provider provides solution.
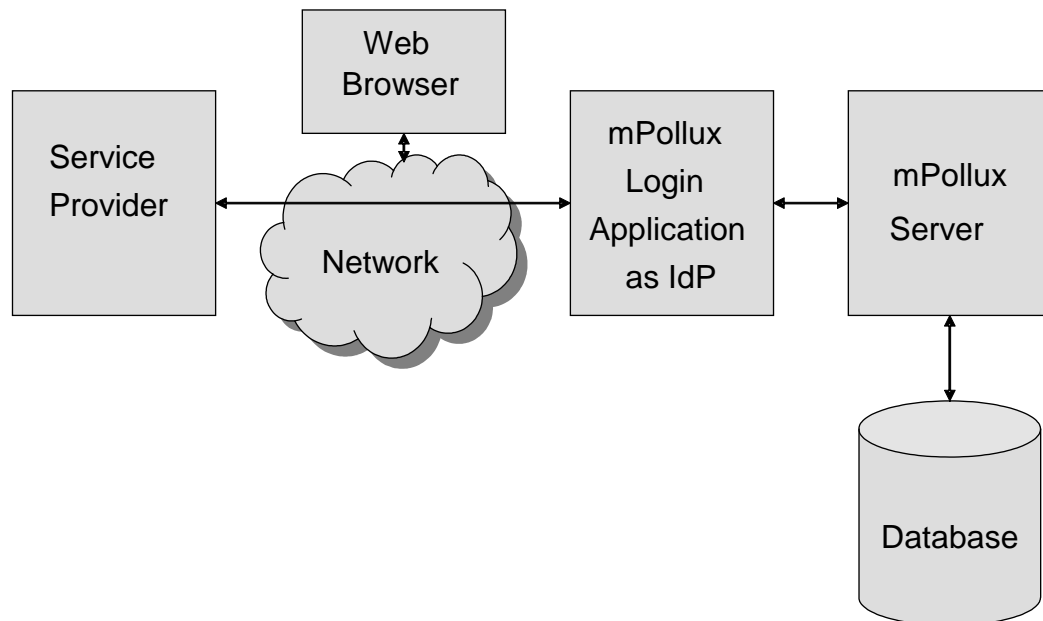

Figure 3 mPollux™ as SAML Identity Provider

- The **Service Provider** provides the necessary mechanism to request Identity Provider for authenticate user.

- The **mPollux™ Login Application** as Identity Provider

- The **mPollux™ Server**

The sample access sequence proceeds as follows

1. When user browses to page that requires authentication, the service provider forward user to Login application to authenticate.

2. mPollux Login Application authenticates user and calls mPollux Server.

3. Then mPollux Server verify the user's credentials and return the result to mPollux Login Application.

4. According to the result, mPollux Login Application sends the necessary information to the service provider.

mPollux

4.2 CASE 2: MPOLLUX AS SAML SERVICE PROVIDER

When you want to secure your web applications with access control, authenticate users using external SAML identity provider and offer Single Sign-On service to web applications, mPollux as Service Provider provides solution.
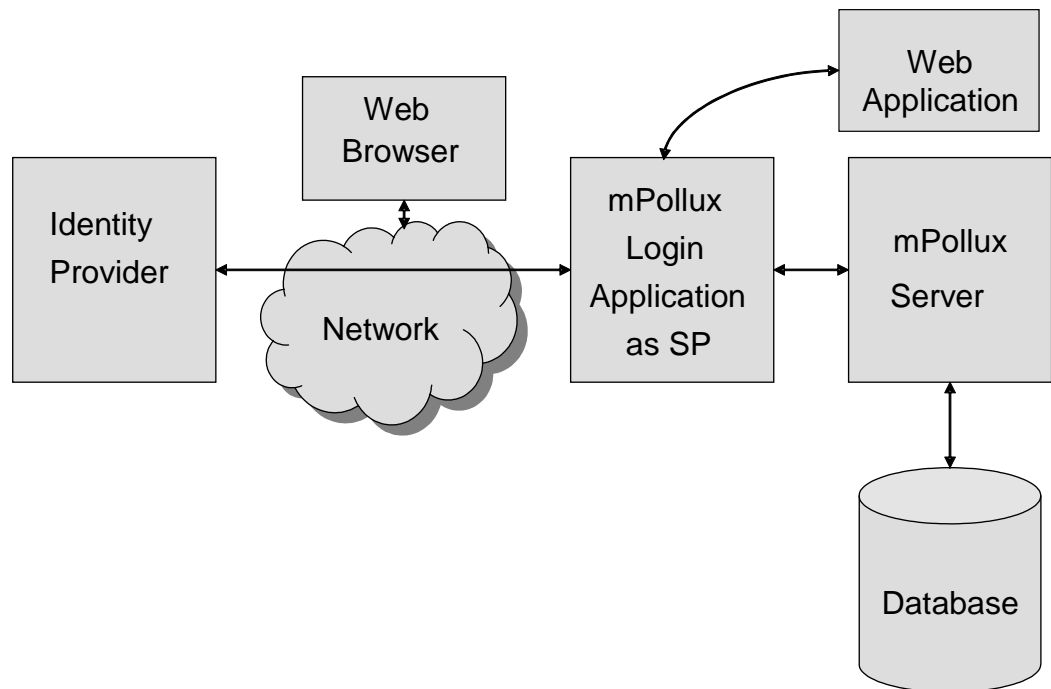

Figure 4 mPollux™ as SAML Service Provider

The sample access sequence proceeds as follows

1. User open a web application with a browser

2. The web application redirects to mPollux™ Login Application, when user does not yet login.

3. mPollux™ Login Application forwards user to Identity Provider to authenticate

4. Identity Provider authenticates user

5. According to the result, Identity Provider sends the necessary information to the service provider (mPollux Login Application).

6. According to the result, mPollux Login Application sends the necessary information to the web application