BFH (Bern University of Applied Sciences), CH-2501 Biel, Switzerland

UniCert Architecture Specification

Version 0.1

Philémon von Bergen

September 10, 2014

Revision History

Revision	Date	Author(s)	Description
0.1	September 10, 2014	Philémon von Bergen	Initial draft.

Contents

1 Introduction **4**

2 Components and Process **5**

2.1 Components 5

2.2 Authentication Process 5

2.3 Certificate Issuance Process 5

1 Introduction

This document presents the architectural specification of UniCert. UniCert is a certification authority, that issues digital certificates used to authenticate users, to sign and/or encrypt messages. UniCert provides an interface where the user can authenticate themselves and request a certificate corresponding to their needs. UniCert uses UniBoard to publish all issued certificates. A general description of what UniCert does and how it works is available in document [1].

This document presents the detail certificate issuing process and focuses on architectural and technical specifications.

2 Components and Process

To give an overview of how UniCertworks, we give a high-level picture of the architecture and the processes that compose UniCert.

2.1 Components

UniCertis composed of two components. The fist one, the authentication component, has following functions:

- authenticate the user
- allow the user to generate a key pair and select some options
- send all data to issuer component
- return the private key (stored locally) and the issued certificate (received from the issuer component) to the user.

The second component, the issuer component, has following functions:

- issue the certificate based on the data received
- publish the certificate on UniBoard(optional)
- return the certificate to the authentication component

2.2 Authentication Process

Currently, the authentication component supports two identity providers to authenticate the user, namely SwitchAAI and Google. Since they do not use the same technologies, the flow of the authentication process is slightly different. Following paragraphs describes the process for each of them.

SwitchAAI authentication SwitchAAI uses a Shibboleth module of Apache webserver to make the redirection to the authentication webpage and back. fig. 2.1 shows how the process works.

Google authentication Google uses protocol OAuth to manage the authentication.

2.3 Certificate Issuance Process

The rest of the process is issuance of the certificate. This works in the same way independently of the identity provider used. The process is shown in Figure 2.3

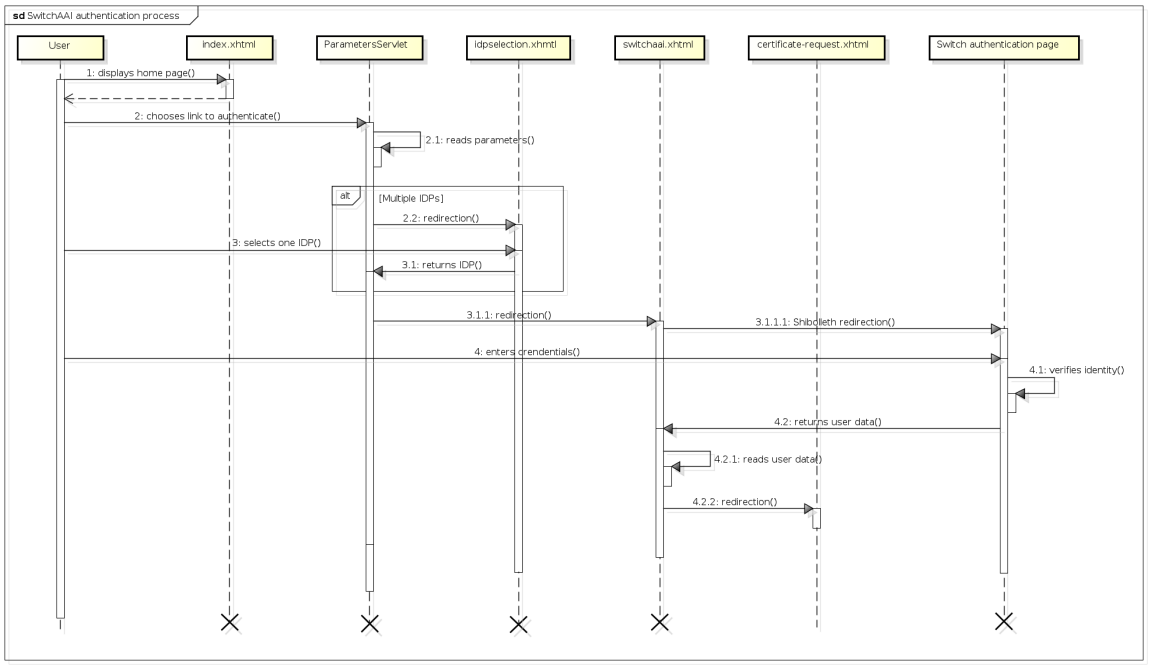

Figure 2.1: Authentication process with SwitchAAI

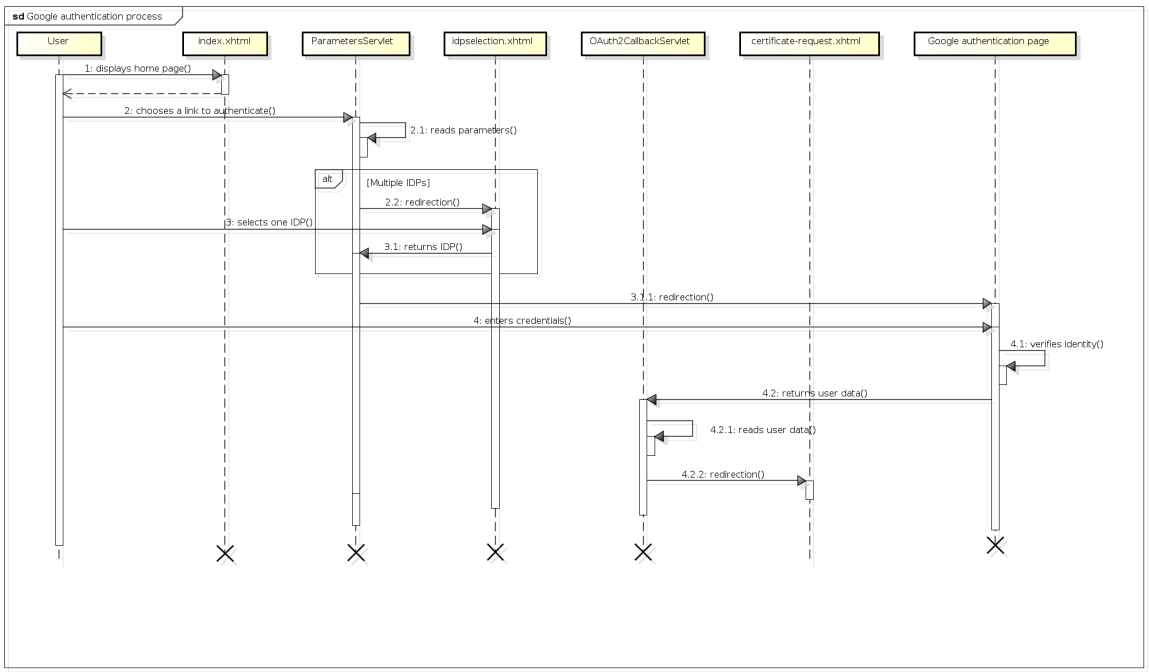

Figure 2.2: Authentication process with Google OAuth

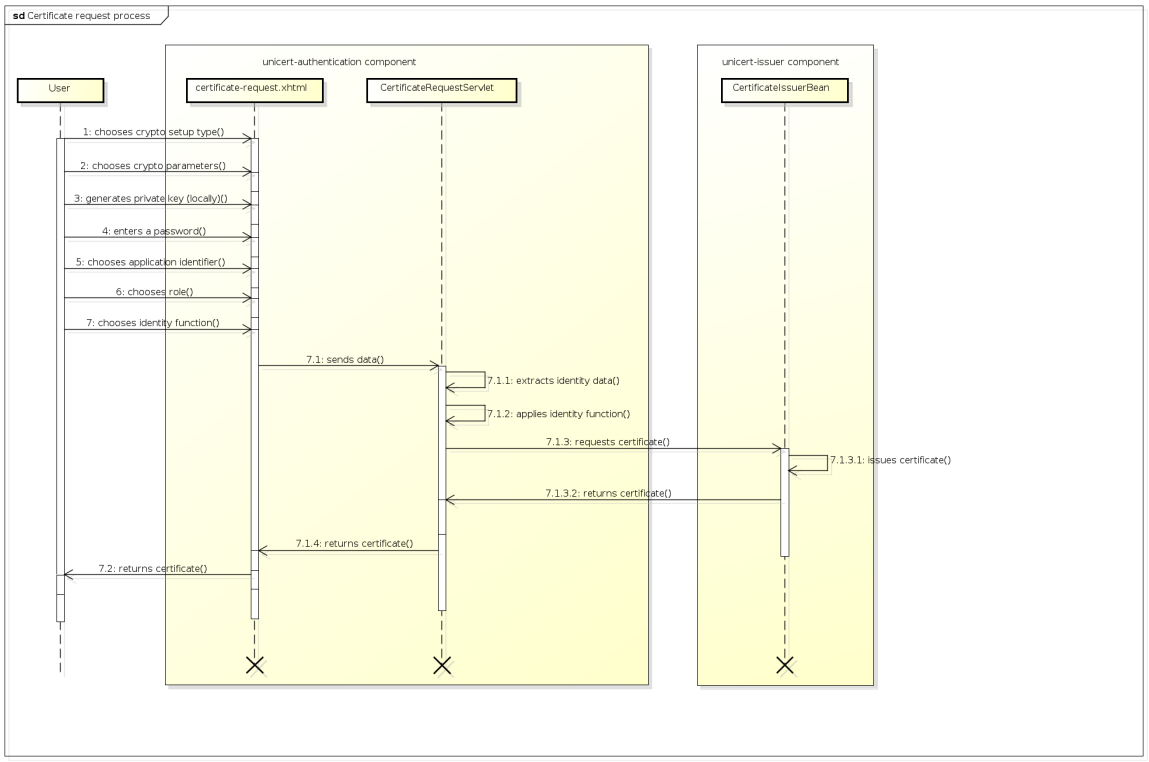

Figure 2.3: Process of requesting a certificate

Bibliography

[1] R. Haenni, R. Koenig, S. Hauser, P. von Bergen, P. Locher, S. Fischli . UniVote System Specification. Technical report, 2014.