ETSI MSS Mobile PKI - SSO

This document describes the overall architecture related to ETSI MSS.
ETSI MSS comprises the architectural components and dependency systems listed in the following table:

Component	DESCRIPTION
SSO Server	The SSO server product against which the User authenticates
Authentication Server (UAS)	A component of SSO server. Some configuration changes are applied specifically to this component or its files.
Mobile PKI method (MPKI)	An SSO Server method that handles sending and receiving of ETSI MSS requests to MSSP. Conforms to ETSI TS 102 204 standard
Security Assertion Markup Language Service Provider (SAML SP)	A SAML-based service provider configured to intercept authentication requests on behalf of a web application server
Mobile Signature Service Provider (MSSP)	Mobile Phone Operator's service that supports sending SMS authentication requests and returning responses to SSO for verification. Conforms to ETSI TS 102 204 standard
Web application	A web application integrated to SSO by using SAML SP.
Mobile phone	User's mobile phone.
Browser	User's compatible web browser.

Basic Login Sequence

This section describes ETSI MSS login sequence in simple terms.
Figure 1 Presents a simplified ETSI MSS login sequence:

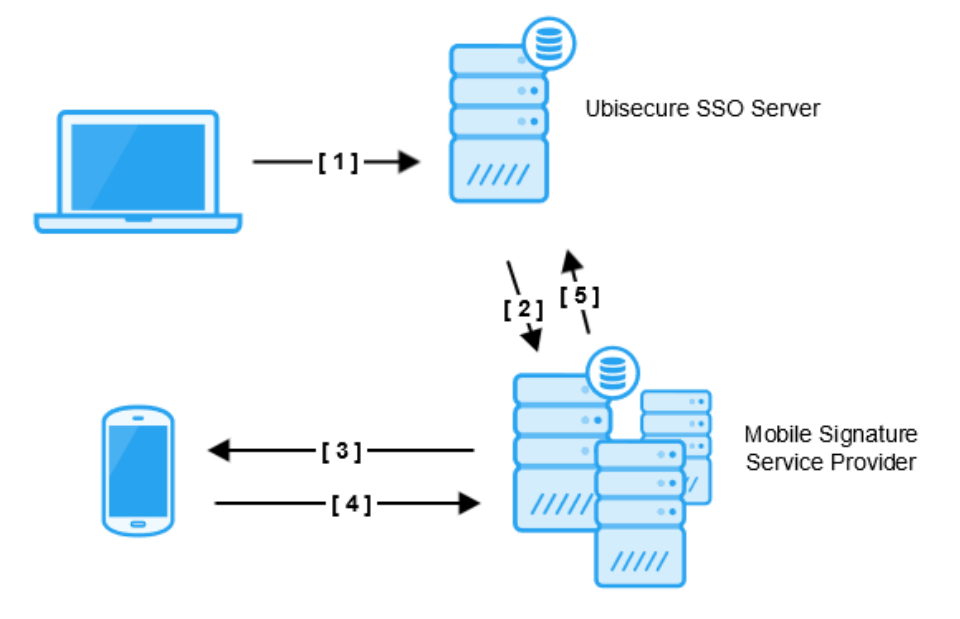

Figure 1 Simplified ETSI MSS login sequence

The following steps describe the sequence presented in Figure 1.

1. User initiates authentication process using a web browser
2. SSO Server prompts for user's mobile phone number and an optional misuse prevention code, and sends the authentication request to a MSSP (mobile operator).
3. MSSP sends the request to User's mobile phone.
4. User signs the request and sends the signature back to the MSSP.
5. MSSP sends the signature with user's certificate back to SSO Server where the signature is verified.

Detailed Login Sequence Diagram

Figure 2 presents the login sequence in more detail:

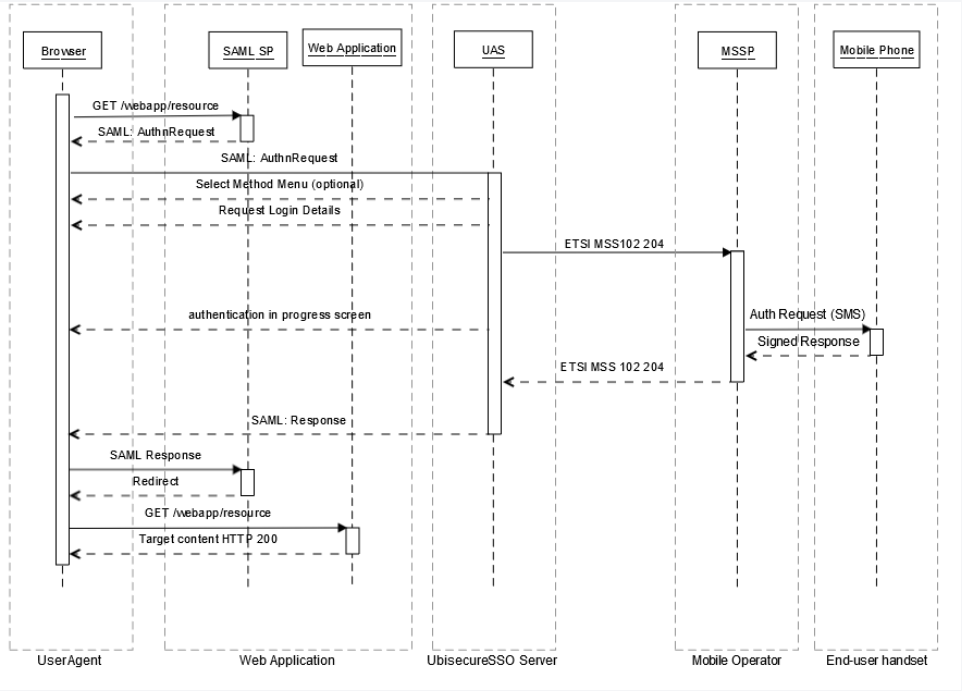

Figure 2 Detailed login sequence

Limitations

Here are listed the known limitations related to ETSI MSS.

- Only asynchronous messaging mode is supported
- The only supported signature profile is authentication
- Refer to *MSS FiCom Implementation guideline 2.2* for an explanation of the terms.