Katso - Developer's Guide

Introduction

1. Introduction 3

2. Katso 3

2.1. Integration options for Katso 3

Authentication 3

Authorization 4

2.2. Basic principles 5

Attributes of Katso users 6

2.3. Integrating web applications using SAML 2.0 Service Provider functionality 6

2.4. Integrating Web Service Providers using SAML 7

2.5. Integrating client applications using SAML and ID-WSF 8

3. Contact Information 9

1. Introduction

Katso organization authentication and authorization system offers companies a flexible way of creating and maintaining digital identities that can be used in eGovernment services. The identity life cycle is managed by the end users themselves. For the developer of eGovernment services Katso offers a variety of different approaches on integration. This document outlines the basic requirements and options that the developer must consider when integrating services to the authentication and authorization platform (Katso and tunnistus.fi).

This document refers to other documents available from the provider of Katso services, CGI Finland. Familiarity of Ubisecure products is not necessary for the developer, but it is beneficial to get acquainted with the products that are used to deliver the Katso services. Ubisecure product related material can be requested from CGI or from Ubisecure (http://www.ubisecure.com).

2. Katso

Katso is a general term describing the authentication and authorization services. Katso is also an authentication mechanism specifically designed for the service. The Katso service is divided into different modules that serve a specific purpose. For the developer of eGovernment services it is important to understand the generic architecture of the Katso system. Throughout the authentication and authorization process different services are requested from different modules of Katso.

For the developer of eGovernment services it should be pointed out that when developing the application and integrating Katso to the services, authentication happens first in the process and authorization happens after the user is successfully authenticated. The authentication itself can be handled in different ways. The authorization can happen also in different ways. It should be carefully considered which integration approach is suitable for the application under development.

2.1. Integration options for Katso

Authentication

There are two main ways to integrate Katso authentication to services. The integration depends on the nature of the service. Web based applications that can be used with a browser can be integrated with SAML 2.0. Applications that can't be used with a browser (e.g. client-server applications) must be integrated using ID-WSF 2.0 and SAML 2.0 protocols.

- SAML 2.0 WebSSO

  → Use Ubisecure SAML SP

  → Or implement the Service Provider functionality to the Application:
  see http://www.oasis-open.org/specs/index.php#samlv2.0

  → Use the platform support (if it exists)

- Liberty ID-WSF 2.0 and SAML 2.0 ECP Profile

  → Use Ubisecure WSP Proxy

→ Or implement the WSC functionality in the client application and the WSP functionality in the server application:

- Ubilogin WSC.pdf
- Ubilogin WSP.pdf
- Ubilogin WSIDP Message Exchange Example.pdf

Authorization

Authorization can happen in two ways in Katso, either through the authentication process or through a separate attribute query, which can be used to determine if the user has the authorization to utilize the service. The authentication event does not deliver any relevant authorization information, so in almost all cases it is required to use the separate SAML 2.0 AttributeQuery. Ubisecure SAMP SP integration modules have the AttributeQuery as a built-in feature.

- Authorization through the authentication process using SAML 2.0 Service provider functionality in the application

  → Use Ubisecure SAML SP

  → Or implement the Service Provider functionality to the Application: see http://www.oasis-open.org/specs/index.php#samlv2.0

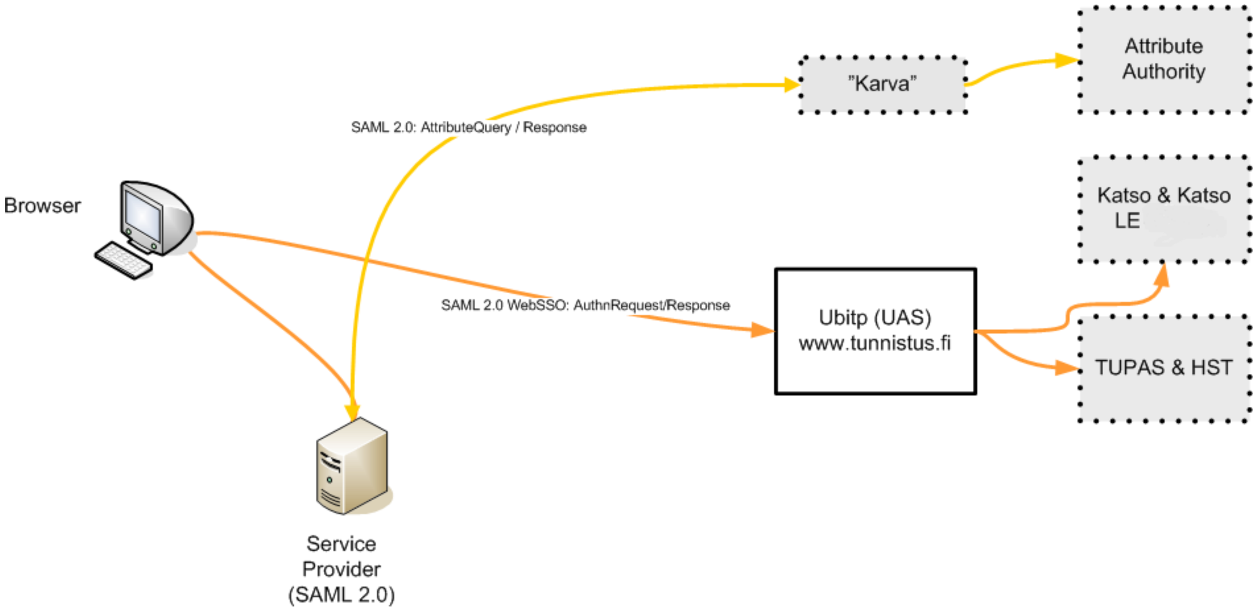
- Authorization through the authentication process using ID-WSF 2.0 and SAML 2.0 specifications
  - Ubilogin WSC.pdf
  - Ubilogin WSP.pdf
  - Ubilogin WSIDP Message Exchange Example.pdf
- Separate attribute query → SAML 2.0 AttributeQuery
  - Ubisecure SAML SP implements SAML 2.0 AttributeQuery
  - http://www.oasis-open.org/specs/index.php#samlv2.0
  - Katso-kirjautuminen ja Karva-roolikysely

Please note that a full blown, and interoperable SAML 2.0 stack could take months to develop. Using Ubisecure products

- Ubisecure SAML SP for Java
- Ubisecure SAML SP for ASP.NET
- Ubisecure AIS for Microsoft Sharepoint
- Ubilogin WSP Proxy

will considerably shorten the time to market in developing eGovernment services for Katso. With Ubisecure product components an online service can be integrated to the Katso in a few days instead of months. With the support for Java and ASP.NET practically any platform can be integrated to Katso with ease.

2.2. Basic principles


"Karva"
Attribute Authority
SAML 2.0: AttributeQuery / Response
Browser
Katso & Katso LE
SAML 2.0 WebSSO: AuthnRequest/Response
Ubitp (UAS) www.tunnistus.fi
TUPAS & HST
Service Provider (SAML 2.0)

The above picture represents a simple scenario where a service is protected using Ubisecure SAML SP (formerly depicted as Ubilogin Web Agent). The SAML SP handles the authentication of the user using either

- TUPAS (BankID)
- HST
- Katso PWD
- Katso OTP

Please note that the service can select which methods to use. Example: The upload of the passport photo, an online service provided by the Finnish police, utilizes Katso OTP and Katso PWD.

This is handled through SAML 2.0 protocol (not the Ubilogin protocol) and the only thing needed from the developer is to integrate the Ubisecure SAML SP following the installation guide, where the integration process is outlined. The documents are available from CGI.

The authorization process delivers attributes about the user to the application. These attributes are named according to the authorization policy in the tunnistus.fi service. Please contact CGI to find out what is the latest Katso authorization policy and the attributes delivered to the application. You can request the latest Katso policy document from CGI Finland.

For Katso users:

- tfi.kid = [Katso user ID, kid]
- tfi.personname = [person name, henkilön nimi]
- tfi.version = [Katso authorization policy version number]

For TUPAS users:

- id.ref = [CUSTID, tells in which attribute HETU or y-tunnus can be found]
- id.type =[which type of ID, Hetu or y-tunnus]
- tfi.CUSTID = [HETU / y-tunnus]

- name.ref = [tells in which attribute the name can be found]
- tfi.custname = [CUSTNAME, name]
- tfi.version = [Katso authorization policy version number]

For HST users:

- tfi.pin = [personal identification number, HETU]
- tfi.personname = [user name]
- tfi.version = [Katso authorization policy version number]

Attributes of Katso users

Each time a Katso user is authenticated, a unique attribute “tfi.kid” is relayed to the application. The application is responsible for finding out what are the roles associated with that particular Katso ID (tfi.kid). This can be done with a SAML 2.0 AttributeQuery. The attribute query is specified in the SAML 2.0 Core documentation and in the Ubilogin WSP.pdf.

Please note that use of the SAML 2.0 AttributeQuery is almost always necessary, and Ubisecure SAML SP implements SAML 2.0 AttributeQuery out-of-the-box.

Requirements for implementing SAML 2.0 AttributeQuery:

- Ability to create SAML 2.0 messages and process them (SAML 2.0 stack)
- Ability to create and process SOAP 1.1 messages
- Ability to check digital signatures created by the attribute authority “Karva”
- Ability to create signed messages
- Ability to create SAML 2.0 Metadata for the authentication and authorization platform, tunnistus.fi
- Ability to read the SAML 2.0 Metadata provided by the authentication and authorization platform, tunnistus.fi
- Ability to create SAML 2.0 AttributeQuery messages using a query name “roles-by-kid”

The updated list of Katso roles are maintained in http://yritys.tunnistus.fi/ under the link "Katso-roolit".

2.3. Integrating web applications using SAML 2.0 Service Provider functionality

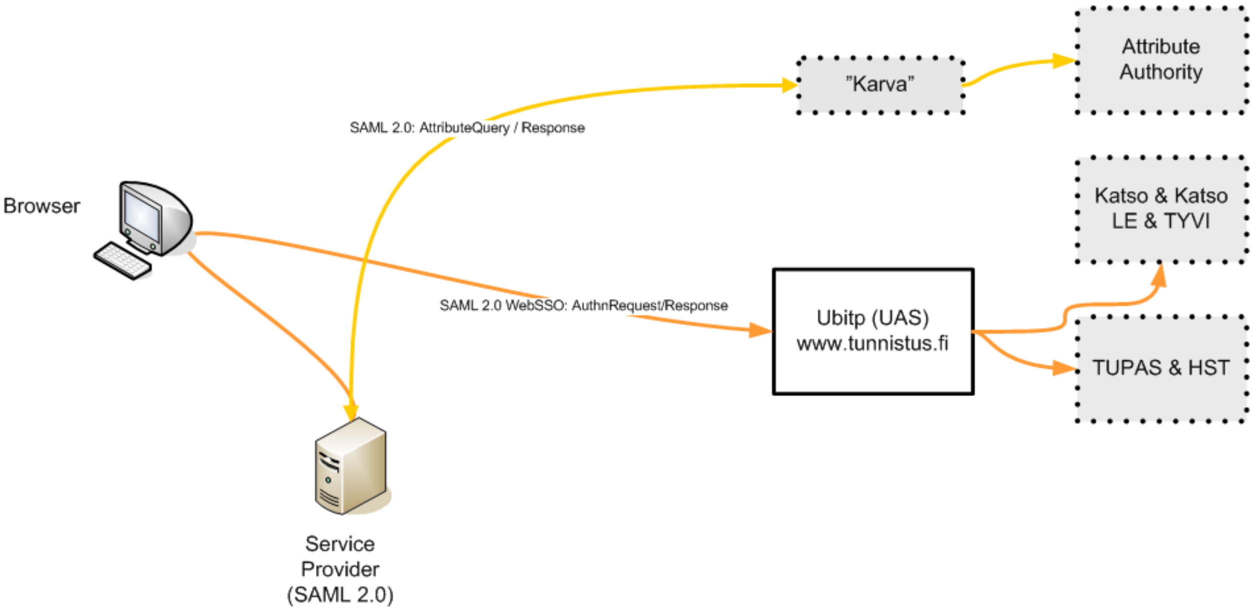
If the application developer chooses to implement his own SAML 2.0 Service Provider functionality to the web application, there are some requirements to follow.

Requirements for the inhouse development of the SAML 2.0 stack:

- Ability to create SAML 2.0 messages and process them by the SAML 2.0 Web Browser SSO Profile (i.e. a SAML 2.0 stack)
- Ability to create signed messages
- Ability to check digital signatures created by the authentication authority tunnistus.fi
- Ability to create SAML 2.0 Metadata for the authentication and authorization platform, tunnistus.fi

- Ability to read the SAML 2.0 Metadata provided by the authentication and authorization platform, tunnistus.fi
- Ability to process the SAML 2.0 assertions provided by tunnistus.fi
- Ability to create SAML 2.0 AuthnRequest messages
- Ability to uphold session information using e.g. cookies is recommended

For the developer it is essential to form a good understanding how SAML 2.0 works and familiarize himself with the SAML 2.0 standard. The IDP (tunnistus.fi) will relay the same information upon authentication as with Ubilogin Agents, and the Service Provider needs to make the same attribute queries.


Attribute Authority
"Karva"
SAML 2.0: AttributeQuery / Response
Browser
Katso & Katso LE & TYVI
SAML 2.0 WebSSO: AuthnRequest/Response
Ubitp (UAS)
www.tunnistus.fi
TUPAS & HST
Service Provider (SAML 2.0)

2.4. Integrating Web Service Providers using SAML

If the application that needs to be integrated with Katso is not a web application, tunnistus.fi offers a standard interface for authentication and authorization for the application developers. The Web Services Provider (WSP) implements the SAML 2.0 specification.

Requirements:

- Ability to create SAML 2.0 messages and process them by the SAML 2.0 ECP Profile (i.e. a SAML 2.0 stack)
- Ability to create signed messages
- Ability to create and process SOAP 1.1 messages
- Ability to use the Reverse SOAP binding (PAOS)
- Ability to check digital signatures created by the authentication authority tunnistus.fi
- Ability to create SAML 2.0 Metadata for the authentication and authorization platform, tunnistus.fi
- Ability to read the SAML 2.0 Metadata provided by the authentication and authorization platform, tunnistus.fi
- Ability to process the SAML 2.0 assertions provided by tunnistus.fi

- Ability to create SAML 2.0 AuthnRequest messages and process them

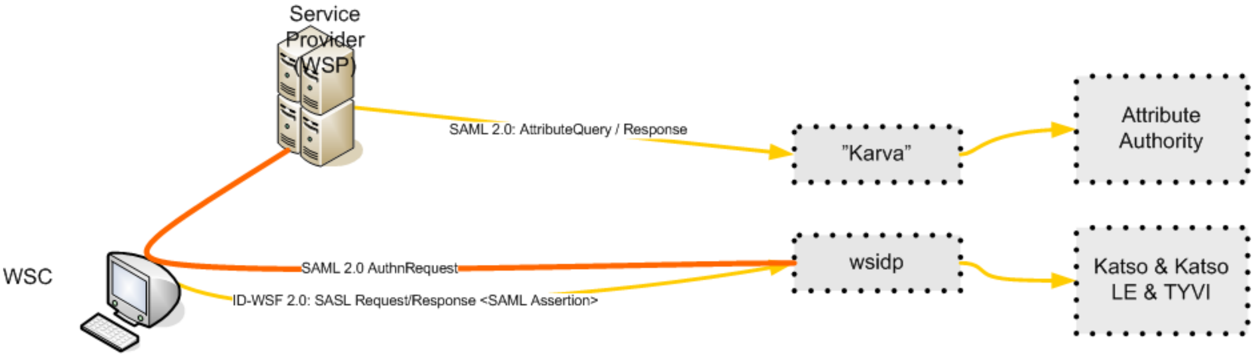
Ubilogin WSP Proxy implements the SAML 2.0 Web Service Provider functionality. For more information regarding Ubilogin WSP Proxy or other Ubisecure integration solutions, contact Ubisecure Solutions.

2.5. Integrating client applications using SAML and ID-WSF

For the integration of Web Service Clients (WSC) with the above mentioned Web Service Provider (WSP), tunnistus.fi offers a web service interface consisting of SAML and ID-WSF messages. However, all SAML messages are created at the WSP. The WSC should implement the Liberty ID-WSF specification 2.0 final.

Requirements:

- Ability to create ID-WSF 2.0 SASLRequest messages
- Ability to process SOAP 1.1 messages
- Ability to process the Reverse SOAP binding (PAOS) messages issued by the Web Service Provider
- Ability to read the SAML 2.0 Metadata provided by the authentication and authorization platform, tunnistus.fi
- Ability to read the Liberty metadata provided by the authentication and authorization platform, tunnistus.fi
- Ability to check the validity period from a SAML assertion
- Ability to attach the SAML assertions in SOAP messages using the Web Services Security SAML Token Profile
- Ability to process the SAML 2.0 assertions provided by tunnistus.fi



3. Contact Information

Ubisecure Solutions, Inc.

www.ubisecure.com
info@ubisecure.com

<firstname.lastname>@ ubisecure.com

Tekniikantie 14
FIN-02150 Espoo, FINLAND

tel. +358-46 7121100

Registered in Espoo, Finland
reg. nr. FI17487214

About Ubisecure

Ubisecure Solutions, Inc. is a leading partner in providing advanced authentication, access control and identity management solutions for Internet, Intranet and Extranet services. Ubisecure provides application developers, integrators, solution providers, OEMs and end-user organizations with IT-security software solutions that maximize the competitive advantage of its customers. The Ubisecure product line consists of Ubilogin SSO solutions for authentication, access control, Web Single Sign On and federated access to Internet, Intranet, Extranet services and Web Services applications; and Ubilogin eIDM solutions for extranet identity management. Ubisecure has offices in Finland and Sweden.

For more information, visit Ubisecure 's web site at www.ubisecure.com