ALCATEL-LUCENT RAINBOW™

Rainbow Authentication

GETTING STARTED GUIDE Ed 1

MARCH 2020

Author: Cloud Services

Alcatel·Lucent Enterprise

Disclaimer

This documentation is provided for reference purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this documentation is provided “as is” without any warranty whatsoever and to the maximum extent permitted.

In the interest of continued product development, ALE International reserves the right to make improvements to this document and the products it describes at any time without notice or obligation.

Copyright

Contents

Glossary 4

1 Introduction 5

2 Overview 5

3 History 5

4 Related documents 5

5 Main principles 6

5.1 Authorization / Authentication 6

5.1.1 Authentication 6

5.1.2 Authorization 6

5.2 OAuth2 / OIDC / SAMLv2 6

5.2.1 SAMLv2 6

5.2.2 OAuth2 6

5.2.3 OIDC 6

6 Customer stories 7

6.1 UCAAS: Rainbow applications 7

6.1.1 Rainbow as identity provider 7

6.1.2 Rainbow and external identity providers 7

6.1.3 Supported external Identity provider 8

6.2 CPAAS: Rainbow sibling applications 8

6.2.1 CPAAS Applications and Rainbow identity 8

6.2.2 CPAAS applications and external identity providers 9

6.2.3 Multi company CPAAS applications and external identity providers 10

Glossary

ALE:	Alcatel-Lucent Enterprise
SAML:	Security Assertion Markup Language
OIDC:	Open ID Connect
OAuth:	Open Authorization
IDP:	Identity Provider
OP:	OpenID Provider
SSO:	Single Sign On
UCAAS:	Unified Communication As A Service
CPAAS:	Communication Platform As A Service

1 Introduction

This document gives a list of supported use case around Rainbow authentication.

2 Overview

Rainbow solution is Enterprise oriented. User authentication is a key feature to ensure security of the global enterprise ecosystem. Authentication of users in a company has to be done by a growing number of applications, computers, web pages and so on. Many companies implement Single Sign On (SSO). It allows users to use the same credentials for several services. Rainbow supports a set of technologies and use cases to be part of the company user authentication solution based on SAML or OIDC protocols.

3 History

Modifications	Date	Edition
Creation of document	2020-03-01	Ed 01

4 Related documents

SAML specifications	https://www.oasis-open.org/standards#samlv2.0
OAuth 2.0 Authorization framework	https://tools.ietf.org/html/rfc6749
OpenID specification	https://openid.net/developers/specs/
Rainbow kind of application	https://hub.openrainbow.com/#/documentation/doc/hub/users-authentication
Rainbow OAuth developer guide	https://hub.openrainbow.com/#/documentation/doc/sdk/web/guides/Oauth2_authentication

5 Main principles

5.1 Authorization / Authentication

Two main principles have to coexist when we are speaking about rights management.

5.1.1 Authentication

Authentication is a way to verify an identity. It is done mainly by retrieving credentials.

5.1.2 Authorization

Authorization is the security function which specifies the rights and privileges given to a resource. For example, in Rainbow, one can authorize an external application to use an account to send IM. In that case, the external application will be authorized to send an IM.

Both, authorization and authentication are often linked because to be able to give an authorization, an application must first check the identity of the requester.

5.2 OAuth2 / OIDC / SAMLv2

5.2.1 SAMLv2

Security Assertion Markup Language (SAMLv2) is a protocol used for authentication. This protocol is widely used as it is deployed in the enterprise world for a long time now. This technology is mainly based on Web browser interactions. This protocol is a way to give access to a protected resource, using a centralized authentication service without giving access to credential to external entities. For example, you can connect to your Rainbow account using your corporate login and password, but Rainbow must not have access to corporate credentials.

As there is a decorrelation between the protected resource and the element that control the identity, SAMLv2 permits to the user to use the same credential to access to a wide range of protected resources or service. This use case is also well known under the Single Sign On (SSO) principle.

5.2.2 OAuth2

OAuth2 is a framework designed to give authorization. It is more recent than SAMLv2, so it is less linked to Web browser and more API oriented. It became quickly very popular and widely used.

OAuth2 is designed to give authorization and not authentication. A lot of application used OAuth2 to also perform authentication (and it is still the case). As to request authorization you need to identify the person, it’s not an issue. But each application has to define a specific way to return the identity of the user to the external application. It is what OIDC is intended to do but under a well normalized format.

5.2.3 OIDC

Open ID Connect (OIDC) is a protocol based on OAuth2 that permit to do authentication (as SAML does). OIDC is also used to perform SSO. OIDC inherits OAuth2 technologies and popularity and will replace SAMLv2 at the end.

6 Customer stories

In Identity management process, we need to identify which component is responsible for controlling the identity of users. Depending on protocol this element is named an IDP (Identity provider) or an OP (OpenID provider). This component is central for a company point of view. It is often synchronized with the company directory. By default, Rainbow acts as an identity provider for Rainbow accounts. It is possible to configure an external identity service.

6.1 UCAAS: Rainbow applications

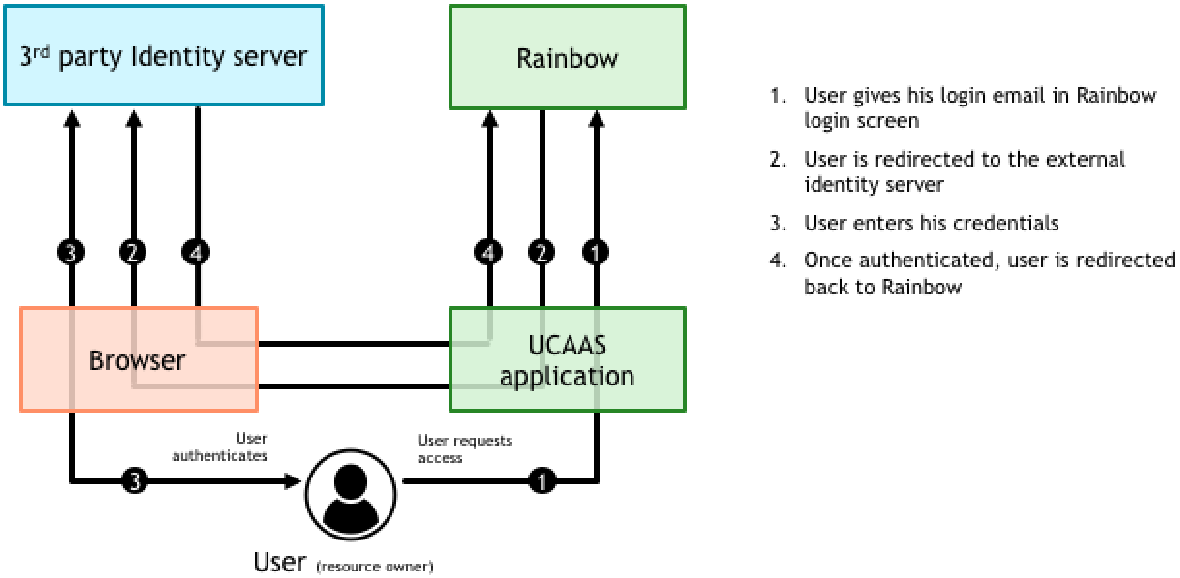
6.1.1 Rainbow as identity provider

By default, Rainbow users are authenticated against the Rainbow service. In this case Rainbow knows how to verify user credentials and is responsible for the verification. When a user opens the Rainbow UCAAS application, the Rainbow login form is presented and used for authentication.

6.1.2 Rainbow and external identity providers

Rainbow solution is able to use an external identity provider based on SAML and OIDC.

In this use case, for an administrative point of view, the administrator of the company authentication service needs to declare a new external service in the external identity service (as in the Microsoft Azure administrative interface) used by the company to let Rainbow interact with it when a user needs to log in.



1. User gives his login email in Rainbow login screen
2. User is redirected to the external identity server
3. User enters his credentials
4. Once authenticated, user is redirected back to Rainbow

6.1.2-1: SAMLv2 authentication

The administrator of the Rainbow company also needs to enable the external authentication. Rainbow identity management is based on companies. The identity management service is configured for the whole company. The administrator has to define which kind of authentication has to be used by default for the company.

Once done, for a user point of view, when he opens a Rainbow UCAAS application, he has to enter his email address and is redirected to the centralized authentication form of the company. Once he is authenticated, he comes back to Rainbow and can use it.

To facilitate migration cases, the type of authentication can be overridden on a per user basis: an administrator can configure an external identity provider and keep the Rainbow authentication as the default one for the company. He can select some alpha testers in his company by selecting the external authentication for these users. Once tests are finished, he can set the external identity management as the default way to authenticate users in his company.

To permit rollback in case of wrong configuration, a company administrator is still able to login to his Rainbow account using his Rainbow credential, even if an external identity service has been configured and enabled for everyone in this company.

6.1.3 Supported external Identity provider

The SAMLv2 and OIDC protocols are generic. So, in theory, they can be used against all servers compliant with these protocols.

Rainbow Integration tests confirm that Rainbow SAMLv2 protocol implementation is compatible with a set of servers.

	SAMLv2	**OIDC**
Microsoft Azure	OK(1)	OK
Microsoft ADFS (windows server 2016)	OK(2)	KO
Ping Identity	-	OK
SimpleSamlPHP (1.18.3)	OK	-

For other IDP service providers deployment or interoperability tests using OIDC (preferred) or SAMLv2, please contact Rainbow customer care services for consulting.

Configuration guides:

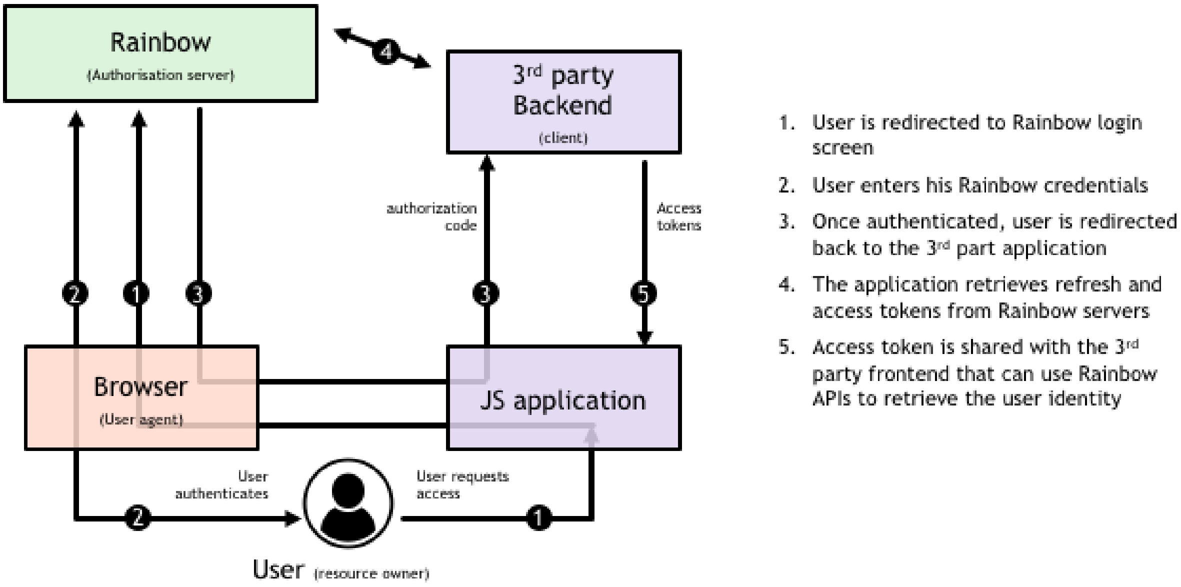
1. How to Activate the Single Sign-On between Azure Active Directory and my Company (using SAML)?
2. How to Activate the Single Sign-On between ADFS and my Rainbow Company (using SAML)?

6.2 CPAAS: Rainbow sibling applications

We call Rainbow sibling applications, any applications based on Rainbow APIs and that needs to authenticate to Rainbow on behalf of the user. This kind of application can be a connector, an extension or a Rainbow plugin that allows to access your Rainbow account and data in order to leverage your Rainbow experience. These applications augment the Rainbow features and integration with other platforms and services.

6.2.1 CPAAS Applications and Rainbow identity

Sibling applications have to authenticate users. If the user identity is managed by Rainbow and to avoid that external application have access to Rainbow credentials, these applications have to implement the OAuth2 flows as described on the Rainbow development platform (hub.openrainbow.com)



1. User is redirected to Rainbow login screen
2. User enters his Rainbow credentials
3. Once authenticated, user is redirected back to the 3rd part application
4. The application retrieves refresh and access tokens from Rainbow servers
5. Access token is shared with the 3rd party frontend that can use Rainbow APIs to retrieve the user identity

6.2.1-1: CPAAS application and OAuth2

In this flow, When the user tries to login on the 3rd party application, the user is redirected to the Rainbow login screen to enters his Rainbow credentials. After he entered his login and password, he has to authorize the external application to use his Rainbow account and then his identity.

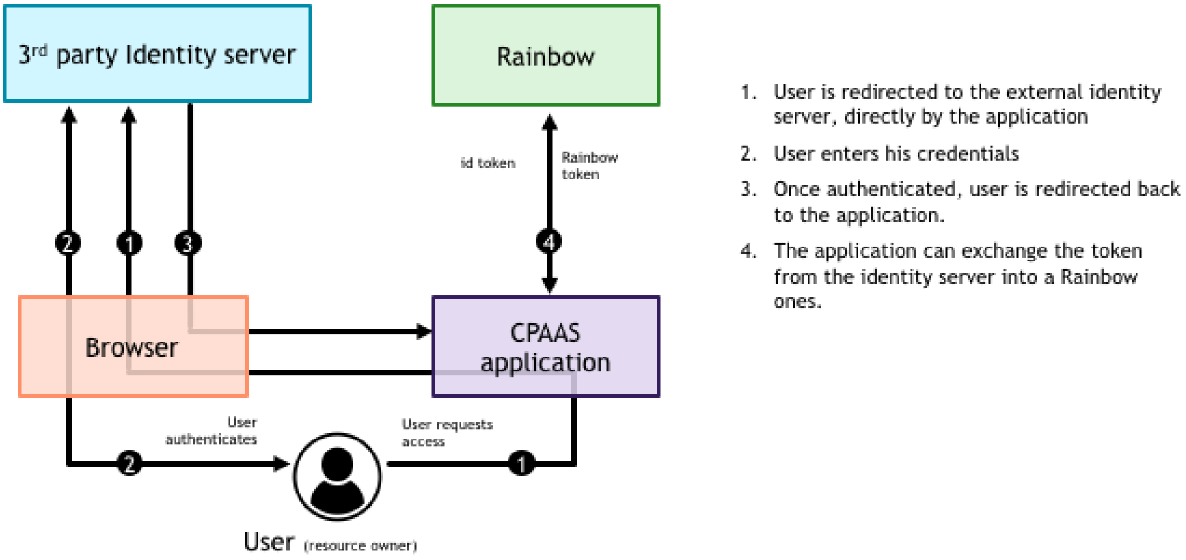
6.2.2 CPAAS applications and external identity providers

The exchange described in previous chapter works well for sibling applications in company using Rainbow as identity provider. But what's happen if it is not the case?

Taking a company using an external identity service. This company needs to develop a specific Rainbow CPAAS application. This application has to use the external identity service to control credentials and then has to use Rainbow services.

This use case is only possible with Rainbow using OIDC. Rainbow company administrator has to declare an external identity server based on OIDC. By configuring this, the administrator gives the ability to Rainbow to trust tokens given by the external identity server.

The external applications have to directly use the external identity provider to check the user identity. The external identity server returns the token that can be verified by Rainbow. This token permits to Rainbow to have the user identity. Then, It is converted into a Rainbow token that gives access to the CPAAS application to Rainbow APIs.



1. User is redirected to the external identity server, directly by the application
2. User enters his credentials
3. Once authenticated, user is redirected back to the application.
4. The application can exchange the token from the identity server into a Rainbow ones.

6.2.2-1: CPAAS application and external Identity server

UCAAS applications connected to this Rainbow company have to also use the same external OIDC server as the CPAAS application.

6.2.3 Multi company CPAAS applications and external identity providers

A CPAAS application can be developed by a developer that want to resell it to several companies. Depending on companies, the identity can be controlled by Rainbow or by an external service and may be based on SAMLv2 or OIDC.

In that case, the CPAAS application has to display the Rainbow authentication screen to ask for Rainbow login (as described in 6.2.1). Once user enters his login, Rainbow will redirect the application or not depending on Identity provider configuration linked to the company of the user.

The CPAAS application inherit automatically of the company authentication without any further development.

End of Document