Active Directory Federation Service

Nhóm 4

ADFS

Single Sign On (sso)

Single LogOut (slo)

Multi-Factor Authentication (MFA)

Microsoft
Active Directory
Federation Services

Domain : fs.nhom4.atm

14/12/2024

Virtuazzo Hybrid Infrastructure

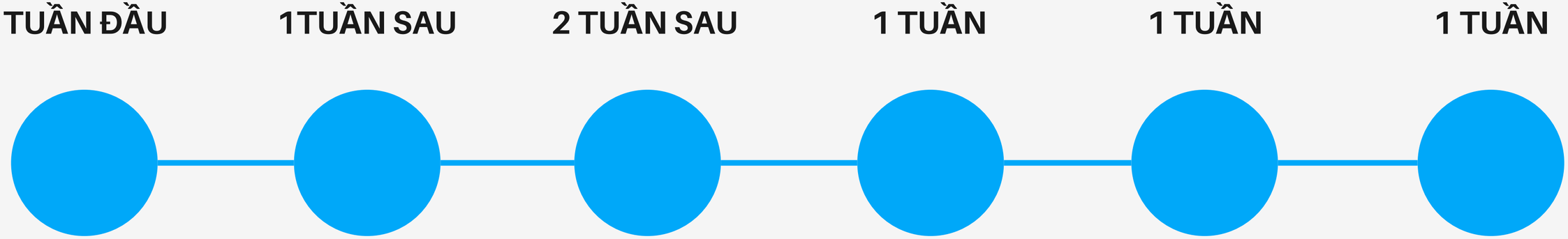
Overview

Objective:

+ Triển khai, tối ưu hóa AD và ADFS: Xây dựng hệ thống quản lý danh tính tập trung, hỗ trợ các tính năng SSO, SLO, và MFA để đảm bảo bảo mật cho hệ thống.

+ Tích hợp các giao thức xác thực liên miền gồm SAML 2.0 và OpenID Connect (OIDC) với ADFS để ứng dụng web xác thực người dùng, đảm bảo bảo mật và đơn giản hóa quá trình đăng nhập.

+ Áp dụng xác thực đa yếu tố (MFA) với giải pháp chứng chỉ số để bảo vệ tài khoản người dùng khỏi các nguy cơ truy cập trái phép.



OverView

01
Overview ADFS

02
Systems Architecture ADFS

03
OIDC - cơ chế hoạt động

04
Triển khai OIDC

05
SAML2 - cơ chế hoạt động

06
Triển khai SAML2 7. LDAP dữ liệu

07
LDAP

08
MFA và sử dụng MFA CA tích hợp

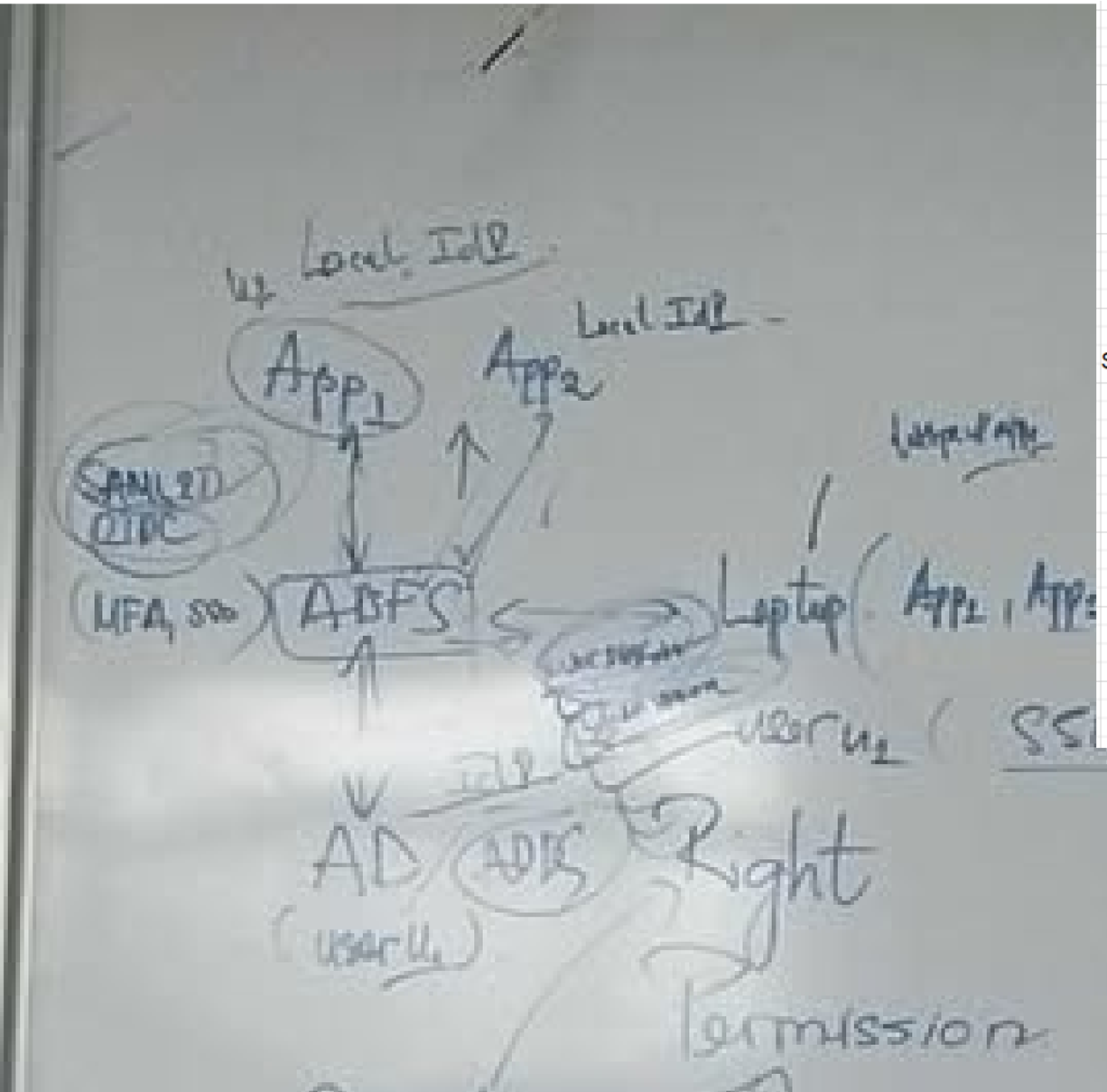
Overview ADFS

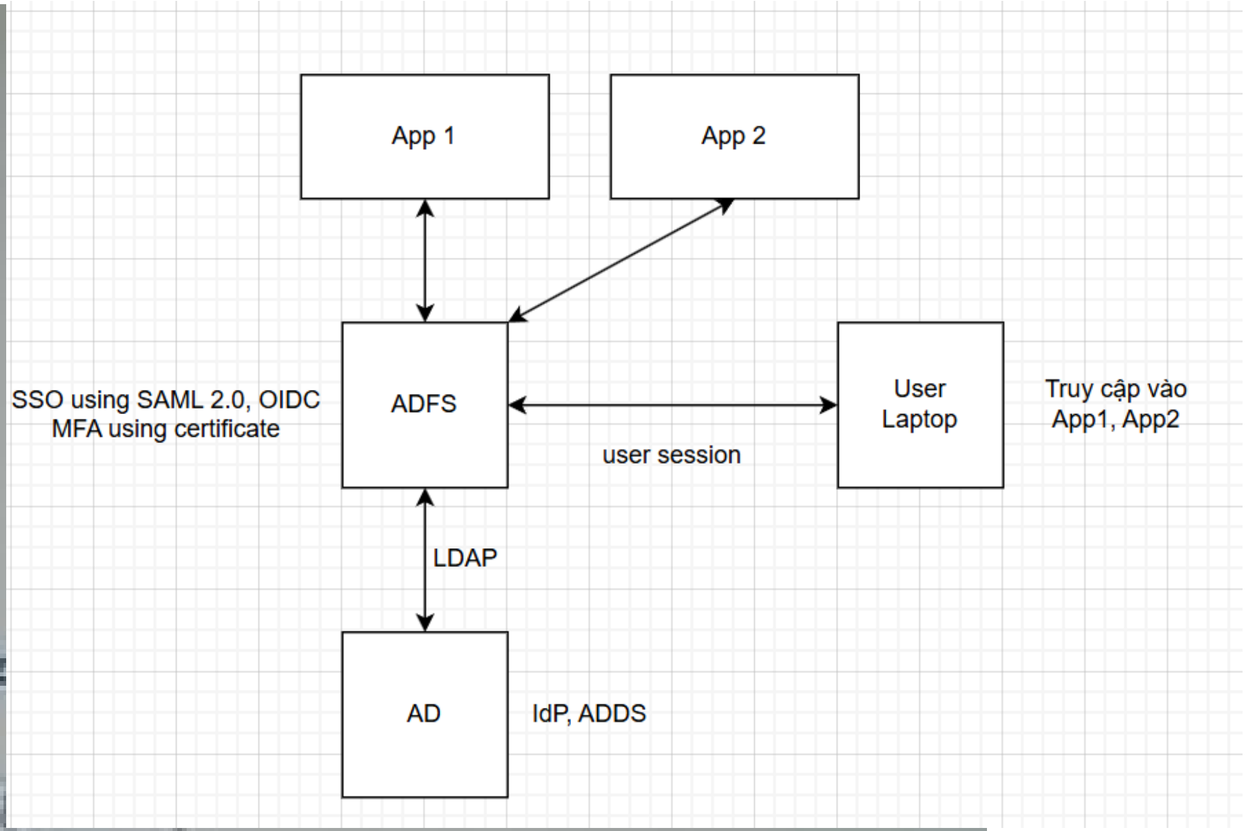
AD FS (Active Directory Federation Services):

+ Cung cấp tính năng liên kết danh tính và đăng nhập một lần (SSO)

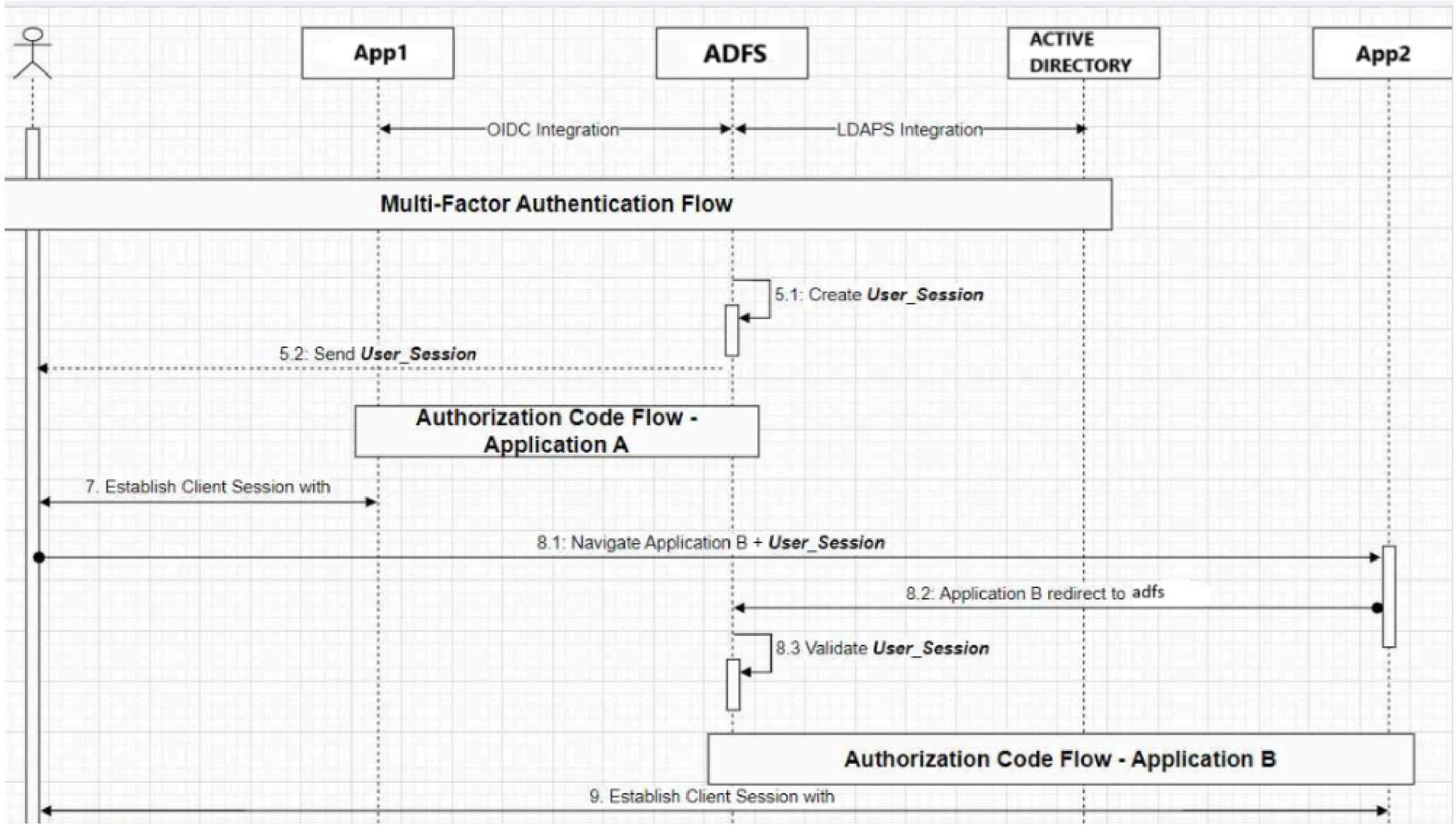
+ Quản lý rủi ro với kiểm soát truy cập đa yếu tố (dựa trên người dùng, thiết bị, hoặc vị trí mạng).

Bonus cái Architect dễ hiểu

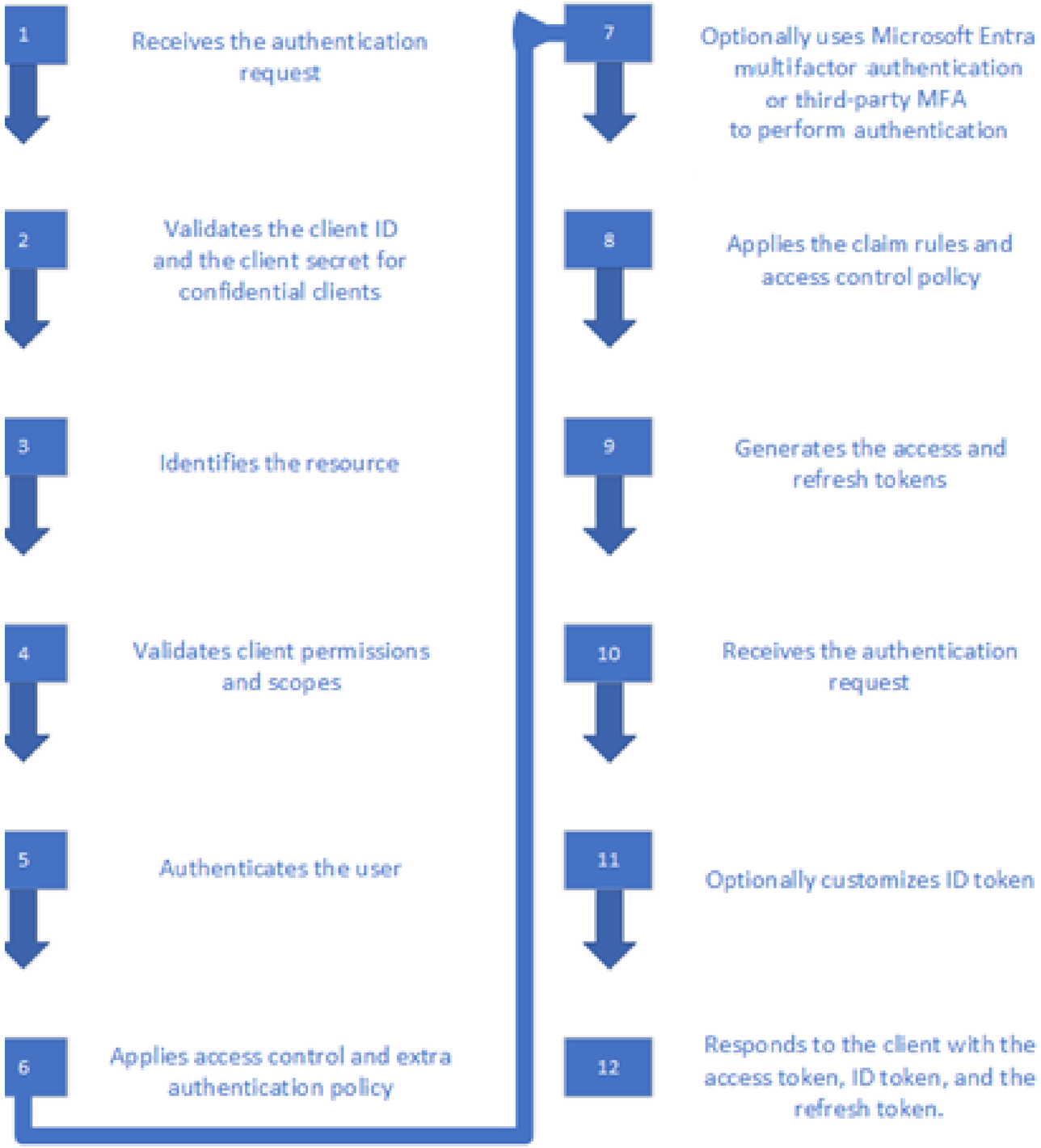




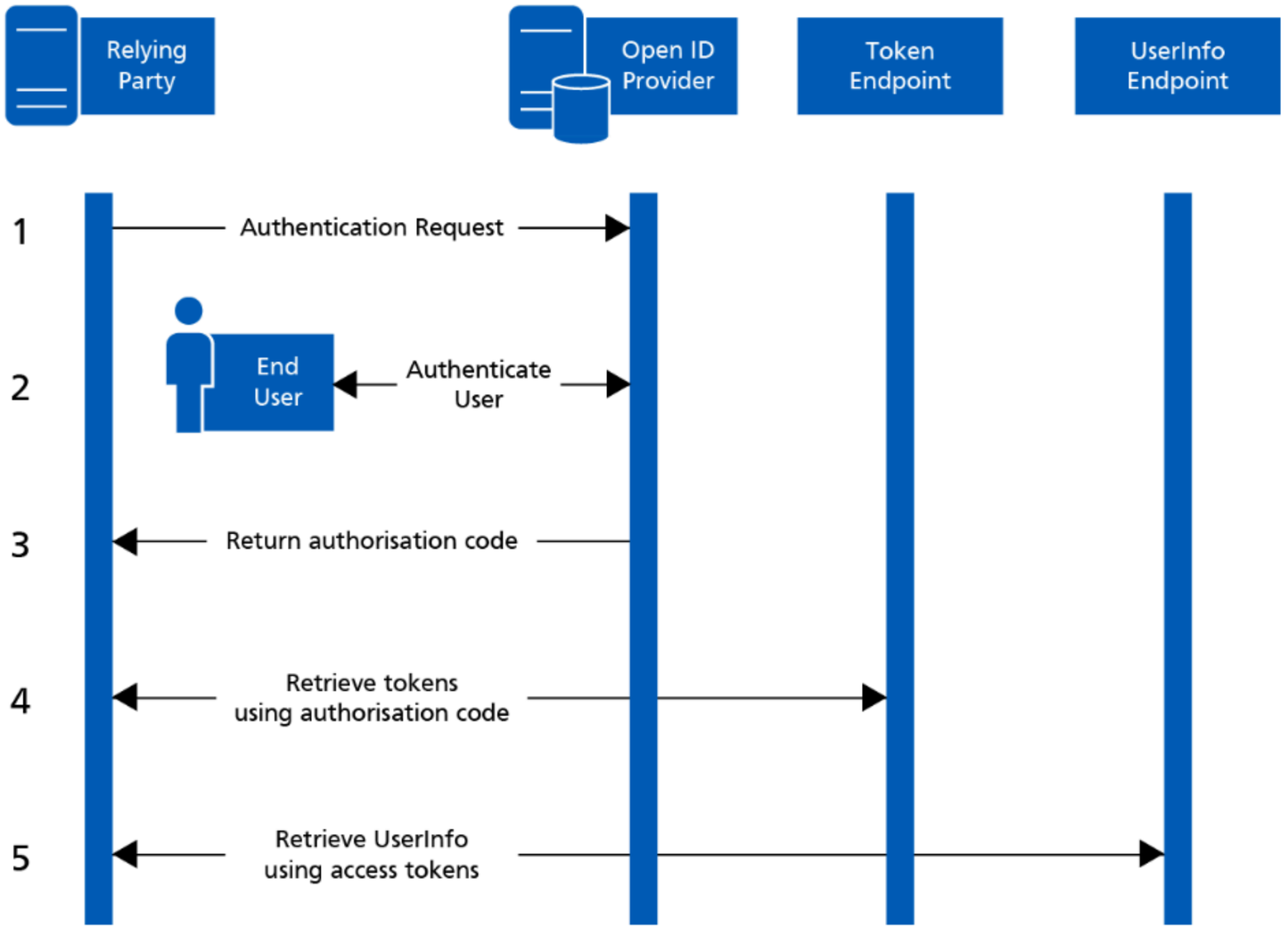
Systems Architecture ADFS



Flow Architecture ADFS



OIDC - cơ chế hoạt động

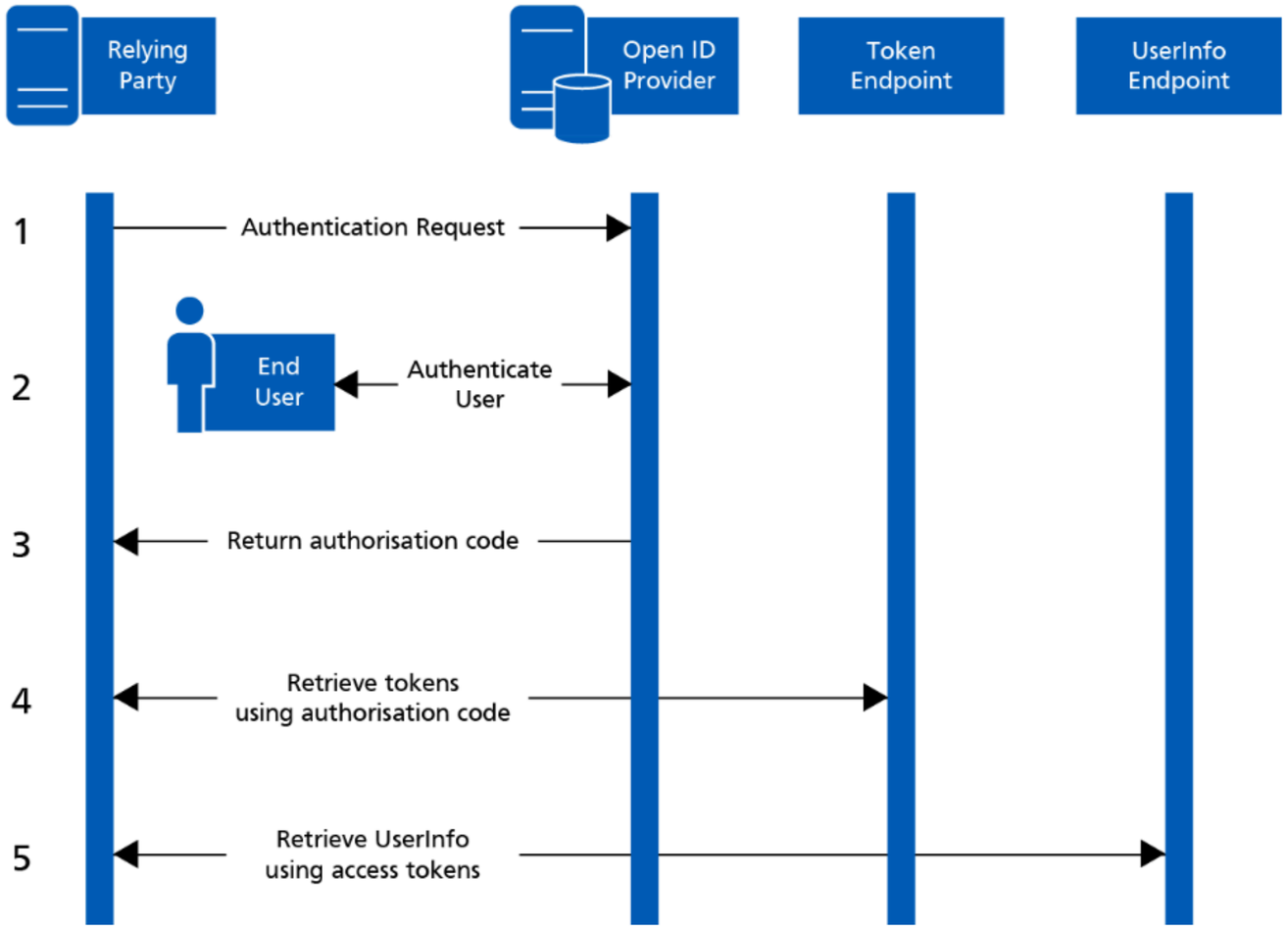


OIDC - cơ chế hoạt động

1.Gửi yêu cầu xác thực:

- Relying Party gửi yêu cầu tới OpenID Provider để xác thực người dùng (End-User).

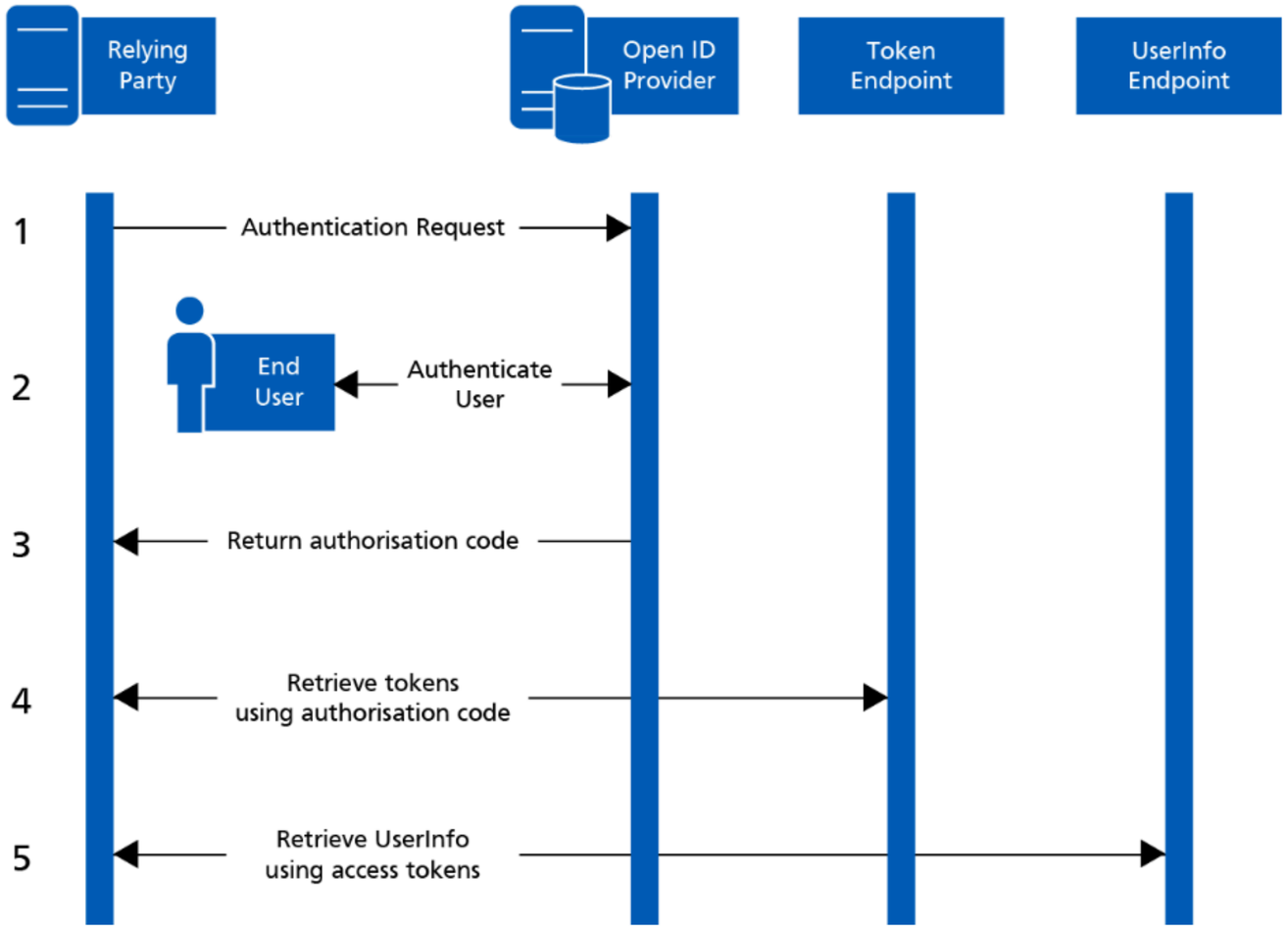
- Yêu cầu bao gồm: danh tính Relying Party, phạm vi "openid" và có thể thêm các phạm vi khác (như "email").



OIDC - cơ chế hoạt động

2. Xác thực người dùng:

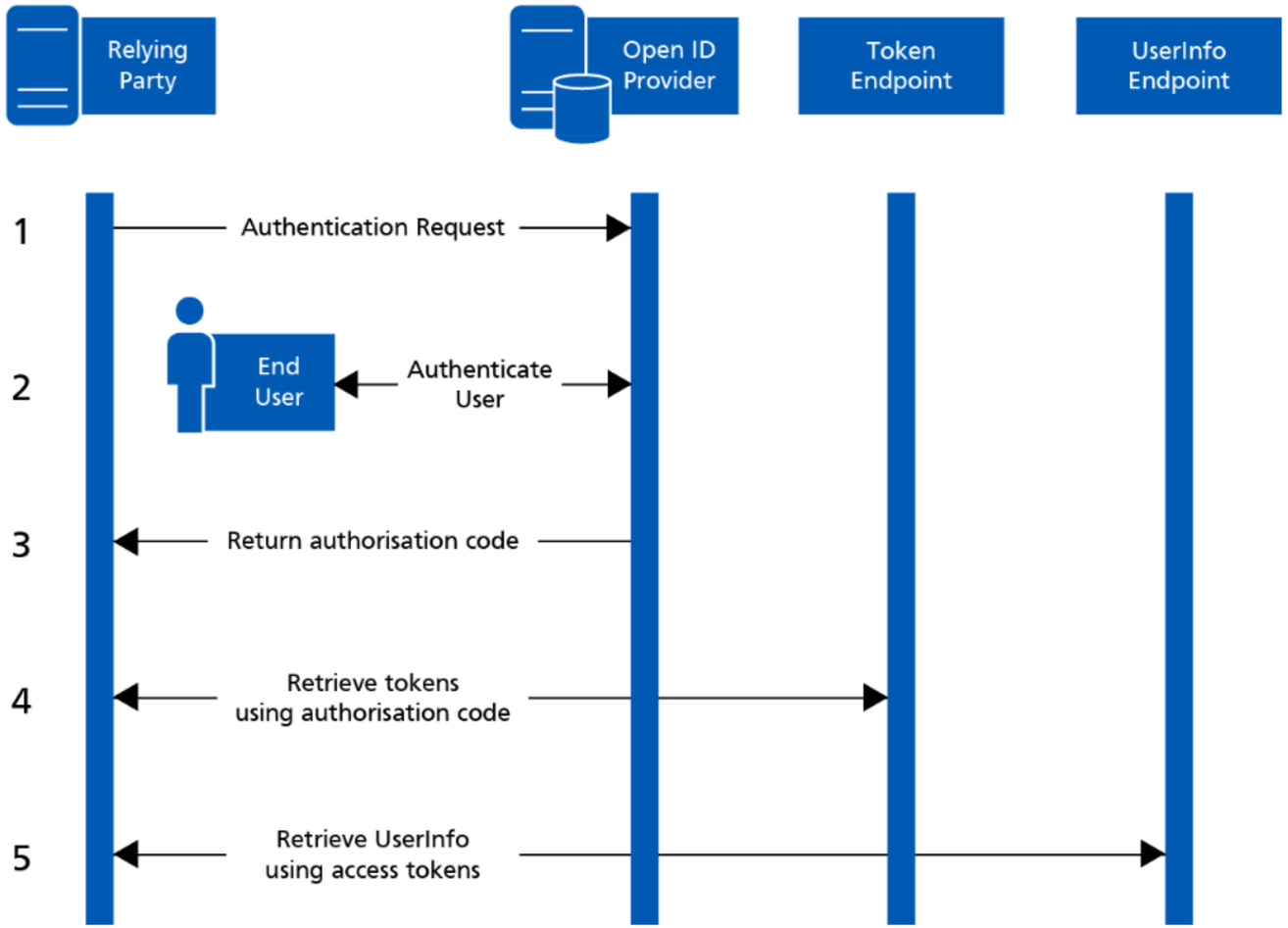
- OpenID Provider xác thực End-User bằng phương thức phù hợp và xin phép người dùng cung cấp các phạm vi được yêu cầu cho Relying Party.



OIDC - cơ chế hoạt động

3. Nhận Authorization Code

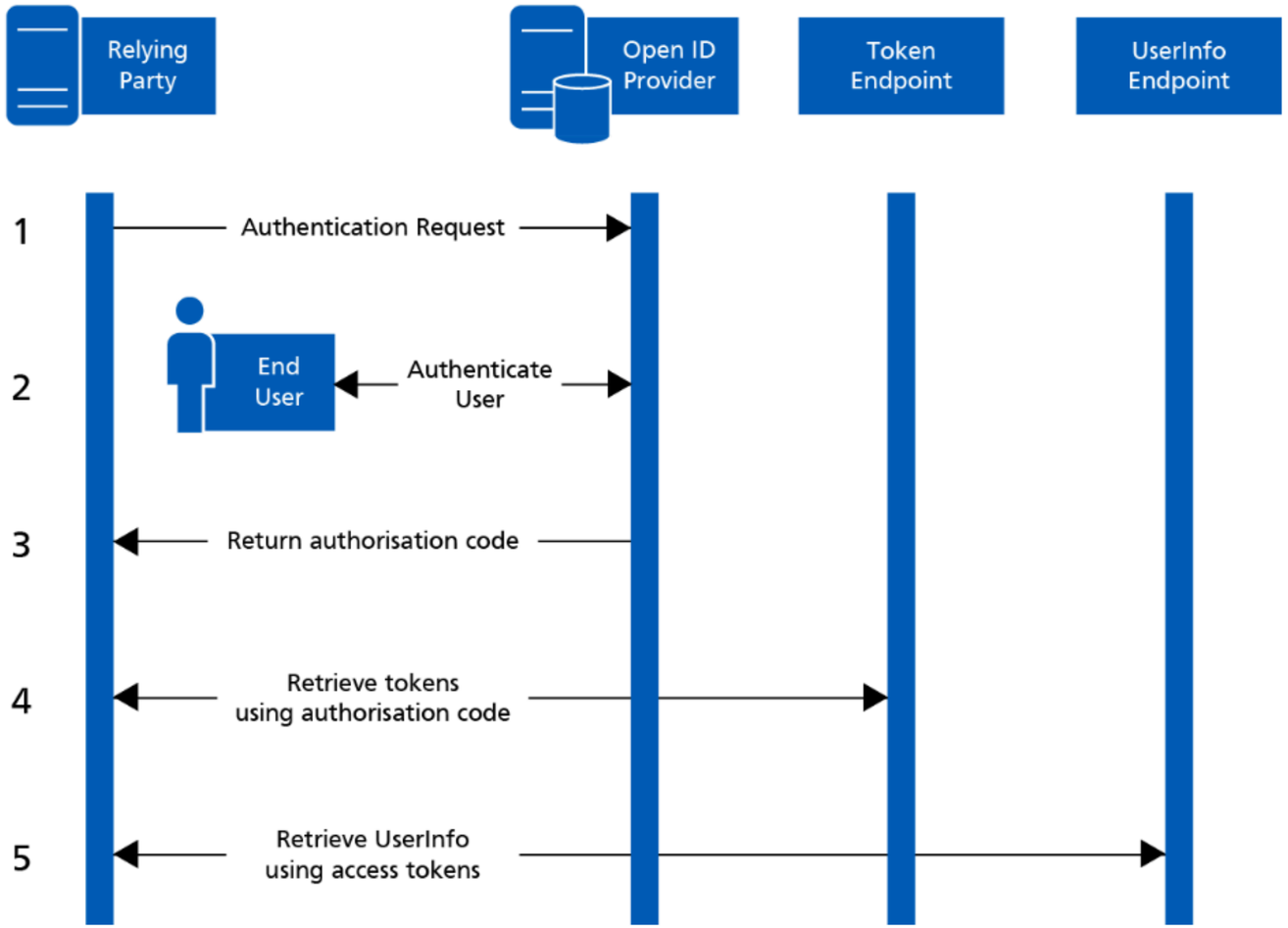
- Sau khi người dùng được xác thực và cho phép, OpenID Provider gửi Authorization Code về server của Relying Party.



OIDC - cơ chế hoạt động

4.Trao đổi Authorization Code lấy token:

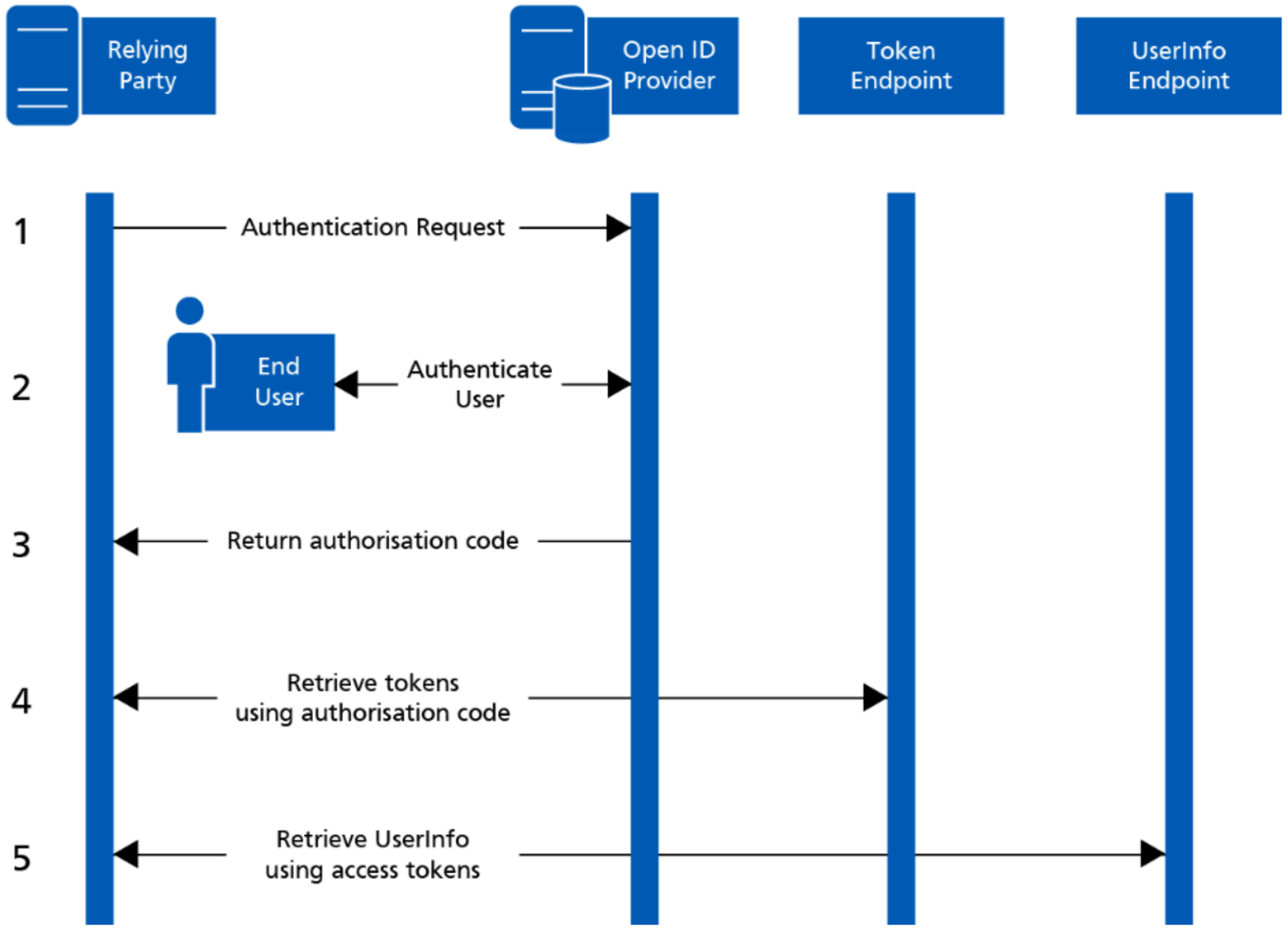
- Server của Relying Party gửi Authorization Code tới token endpoint để lấy ID Token (xác định người dùng) và tùy chọn Access/Refresh Tokens.



OIDC - cơ chế hoạt động

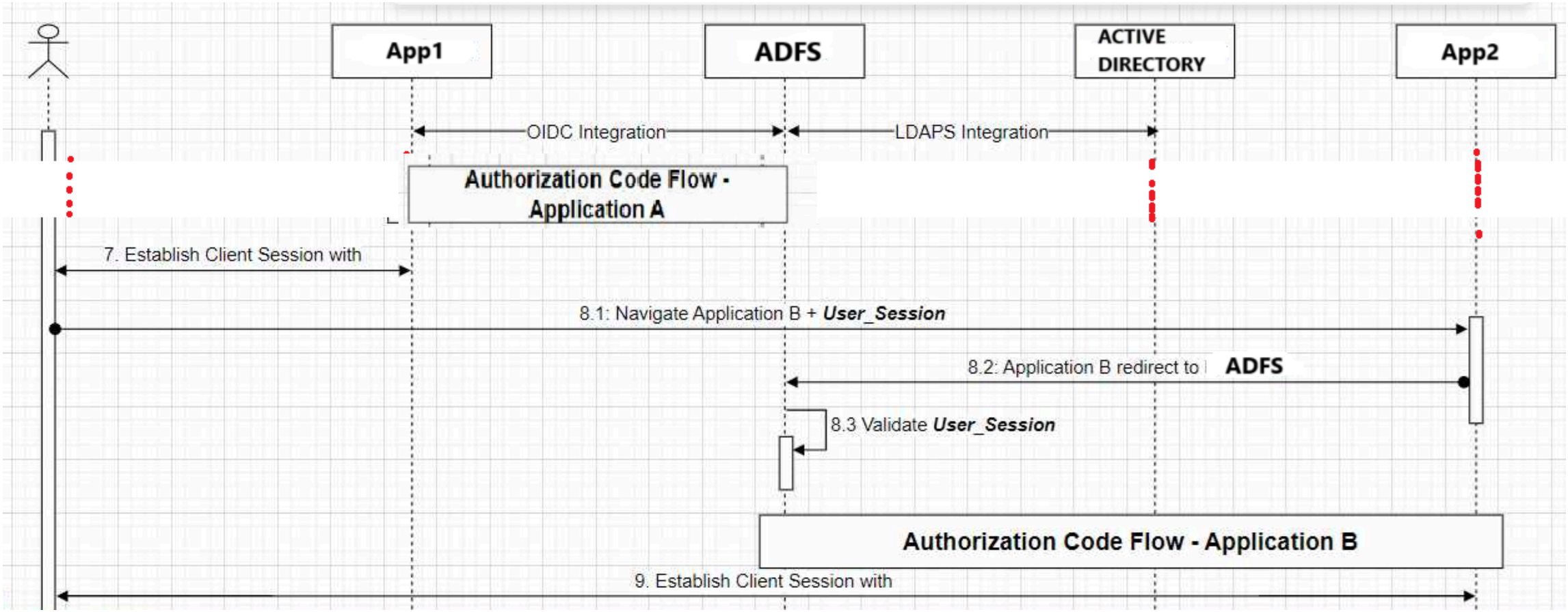
5.Truy vấn thông tin bổ sung

- Relying Party có thể sử dụng Access Token để lấy thêm thông tin người dùng từ UserInfo endpoint (ví dụ: email).



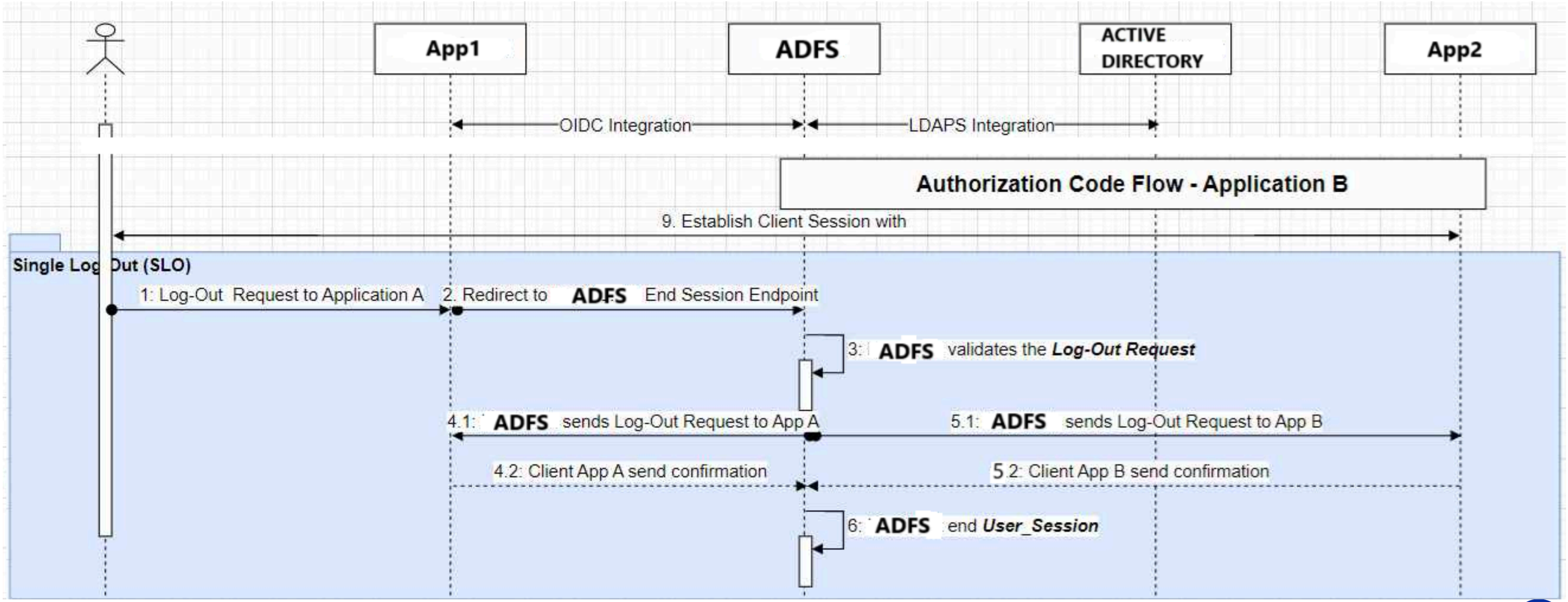
Single Sign On (SSO)

Flow Architecture



Single Log-Out (SLO)

Flow Architecture



SAML 2.0

Security Assertion Markup Language

Tiêu chuẩn cung cấp cross-domain single sign-on (SSO)

SAML 2.0 là một XML-based authentication protocol thông qua Idp quản lý và lưu trữ user credentials, trao đổi signed XAML documents (SAML Assertions) cho phép người dùng truy cập vào Service Provider (SP)

Dịch vụ request và nhận dữ liệu từ IdP được biết đến là Relying Party (RP) và dữ liệu người dùng được đóng gói trong SAML Assertion

SAML 2.0

Single sign on (SSO)
Single log out (SLO)

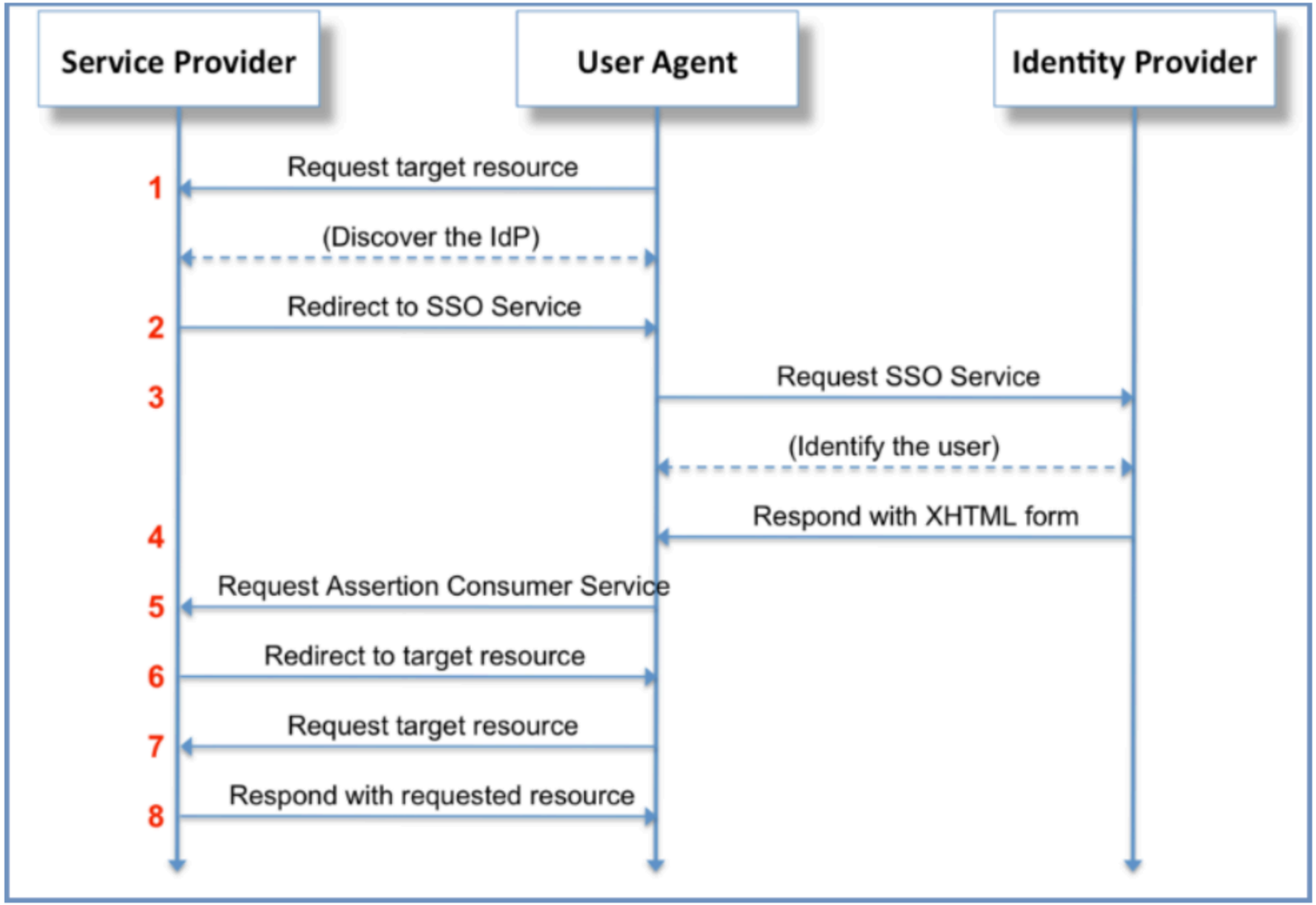
SAML 2.0 dựa trên relying party trust do ADFS cung cấp để xác thực người dùng

Relying party trust object bao gồm các indentifiers, name, rules được dùng để nhận diện partner hoặc web-application tới Federation Service

SAML 2.0 single logout protocol cho phép IdP end session trên application đồng thời chỉ với một single logout request

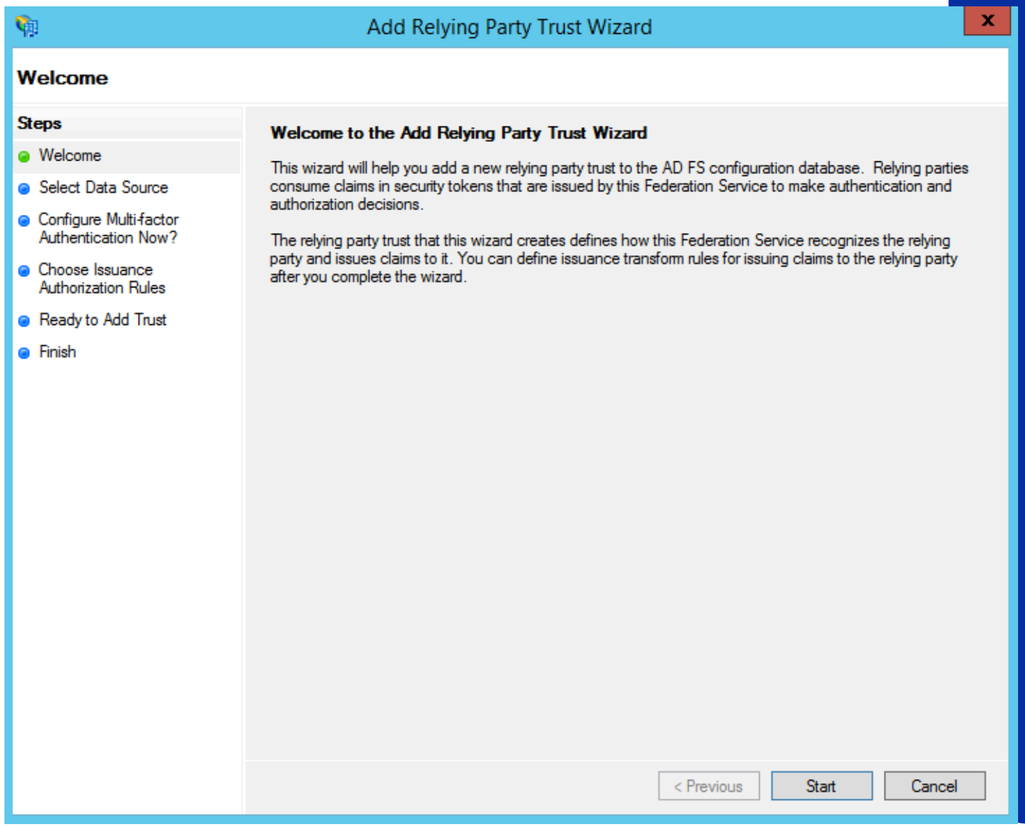
SAML 2.0 – cơ chế hoạt động

SAML Web SSO Authentication:



SAML 2.0

Triển khai trên ADFS



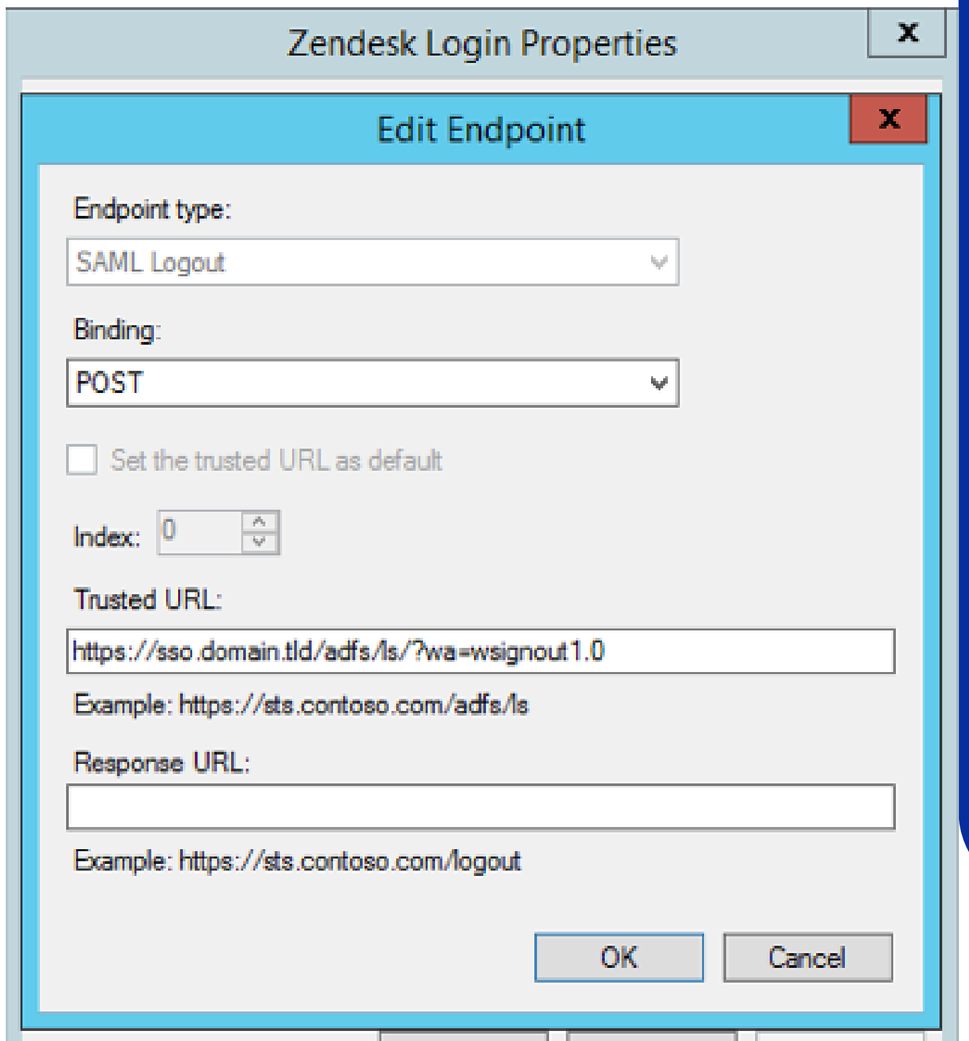
1. Tạo AD FS relying party trust

Cấu hình relying party trust trong ADFS bao gồm Display name, profile, certificate, identifier

Ngoài ra, AD FS có chức năng “Enable Support for the SAML 2.0 WebSSO protocol” cho phép SSO service hỗ trợ Web-browser-based claims providers

SAML 2.0

Triển khai trên ADFS



2. Điều chỉnh trust settings

AD FS cho phép thay đổi các thuộc tính liên quan đến secure hash algorithm

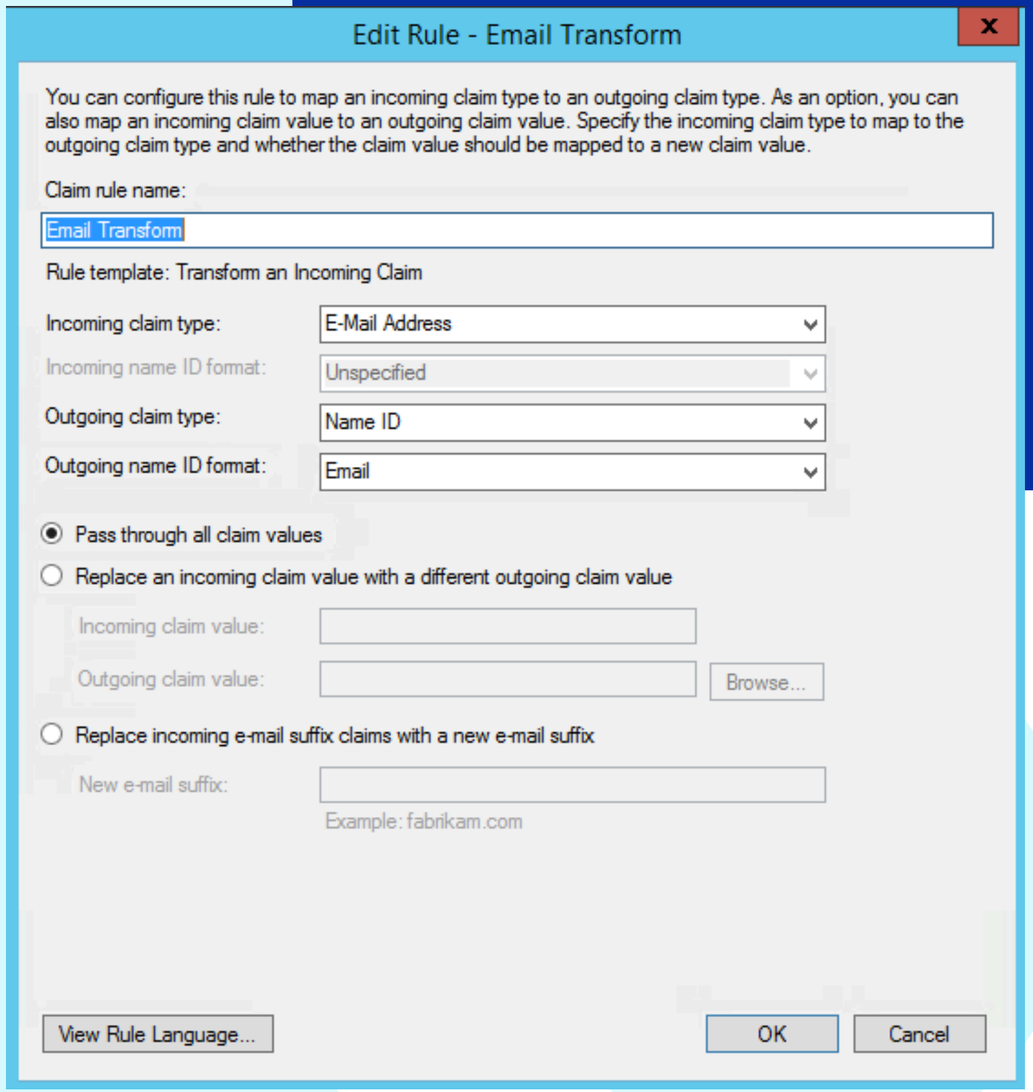
Endpoint: SAML Logout, SAML Acs

Cấu hình Accepted Claims

Claim Rules - LDAP

AD FS cung cấp template LDAP cho claim rule để lấy các thông tin của người dùng có trong Active Directory, send as claim tới relying party.

Giả sử, LDAP Attribute cung cấp thuộc tính là E-Mail Addresses là Incoming claim type và Name ID là Outgoing claim type, thì ứng dụng trong relying party có thể lấy dữ liệu E-Mail Addresses của người dùng trong AD để hiển thị hoặc xử lý.



Multifactor authentication

MFA in ADFS

Trong ADFS, MFA được sử dụng như một phần của global hoặc per-relying-party authentication policy. Nó cho phép áp dụng một yêu cầu xác thực mạnh mẽ hơn cho toàn bộ user hoặc một nhóm user có yêu cầu nào đó (MFA cho người dùng bên ngoài, MFA cho người dùng thuộc nhóm Admin Domains...)

MFA có thể được sử dụng thông qua các third-party providers hoặc hai phương thức sẵn có là Certification Authentication và Azure AD

Quay lại Chương trình

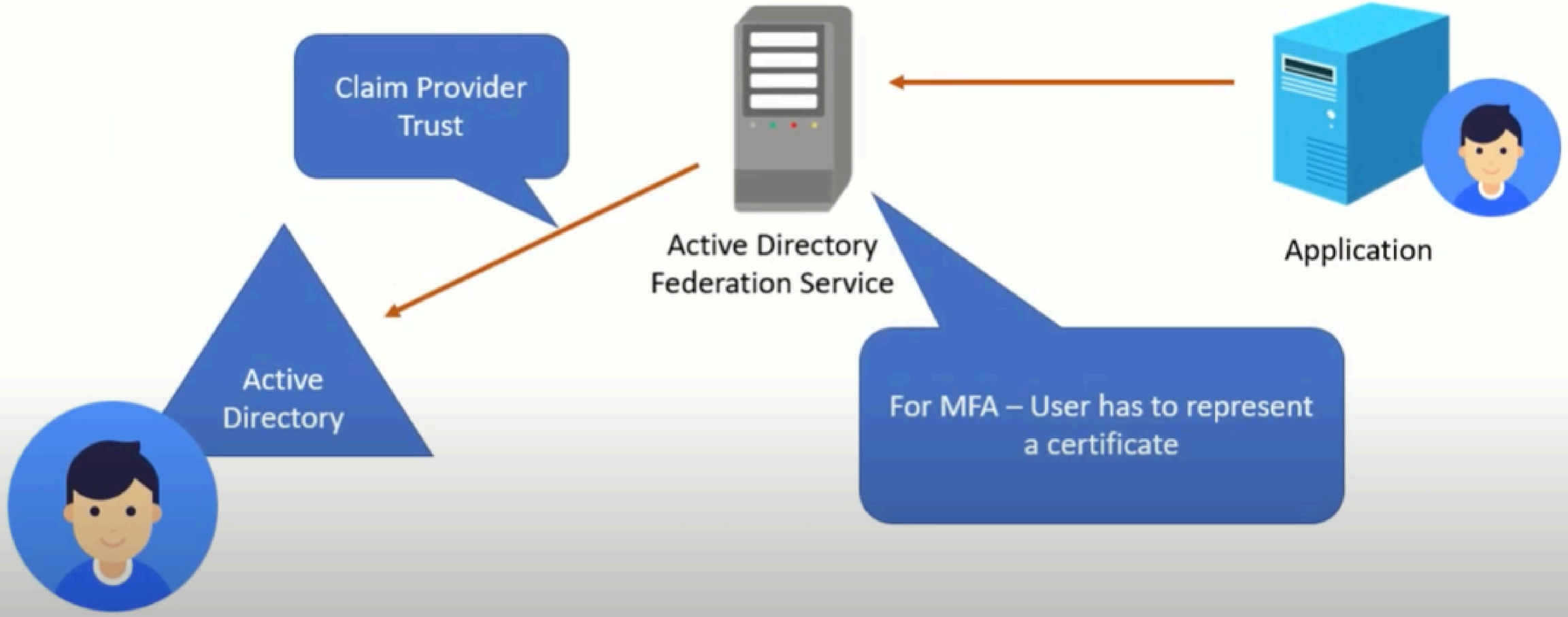
Multifactor authentication

MFA in ADFS using Certificate Authentication

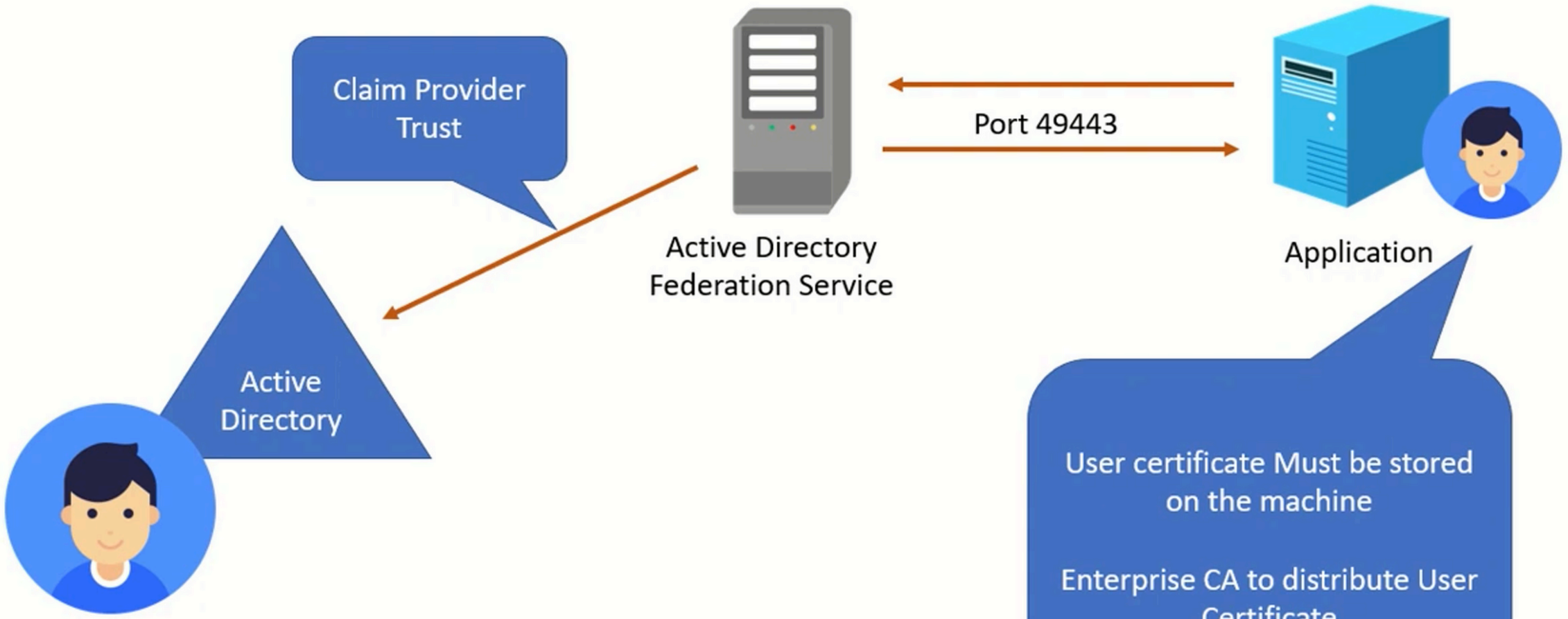
Xác thực bằng Chứng chỉ (Certificate Authenticatioon) yêu cầu người dùng cung cấp một chứng chỉ số làm yếu tố xác thực thứ hai. Phương pháp này sử dụng Public Key Infracstrure (PKI) hoặc các bên tin cậy để xác thực danh tính người dùng, xác minh rằng người dùng thực sự sở hữu chứng chỉ, tăng cường bảo mật loại bỏ nguy cơ truy cập trái phép khi mật khẩu bị đánh cắp

Quay lại Chương trình

Multi – Factor Authentication – Certificate Authentication

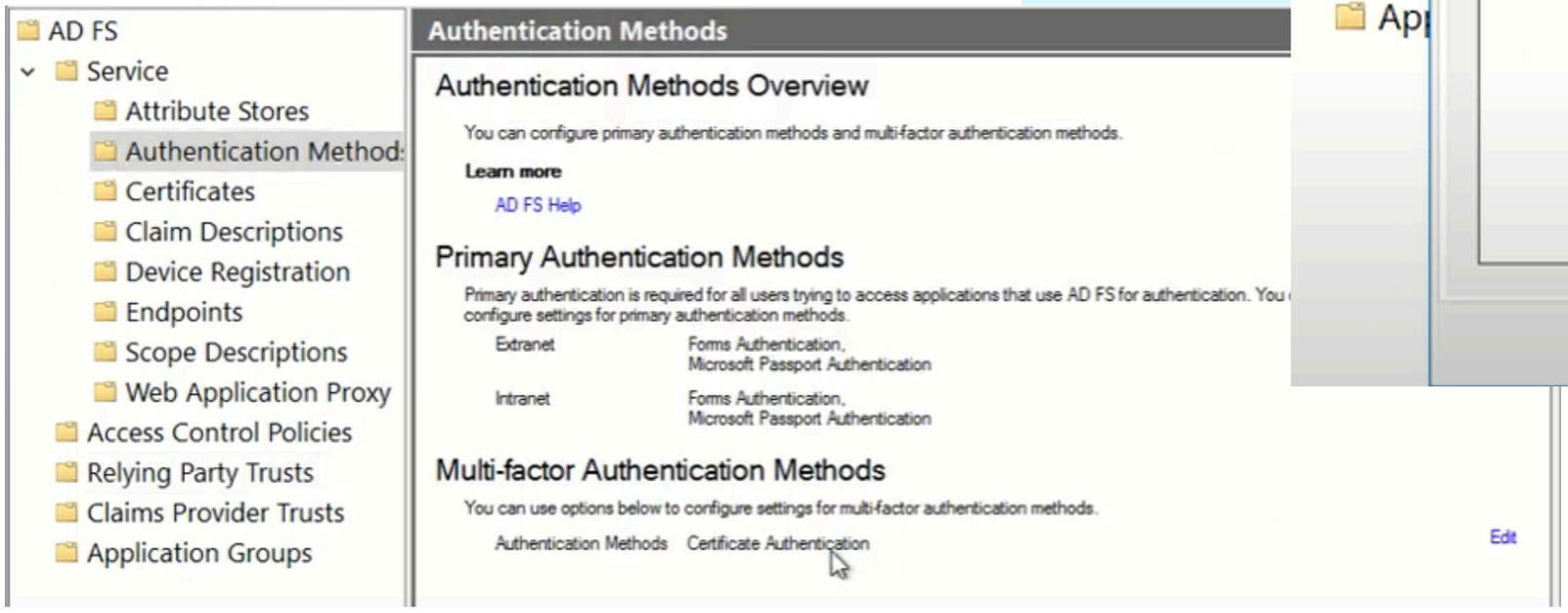


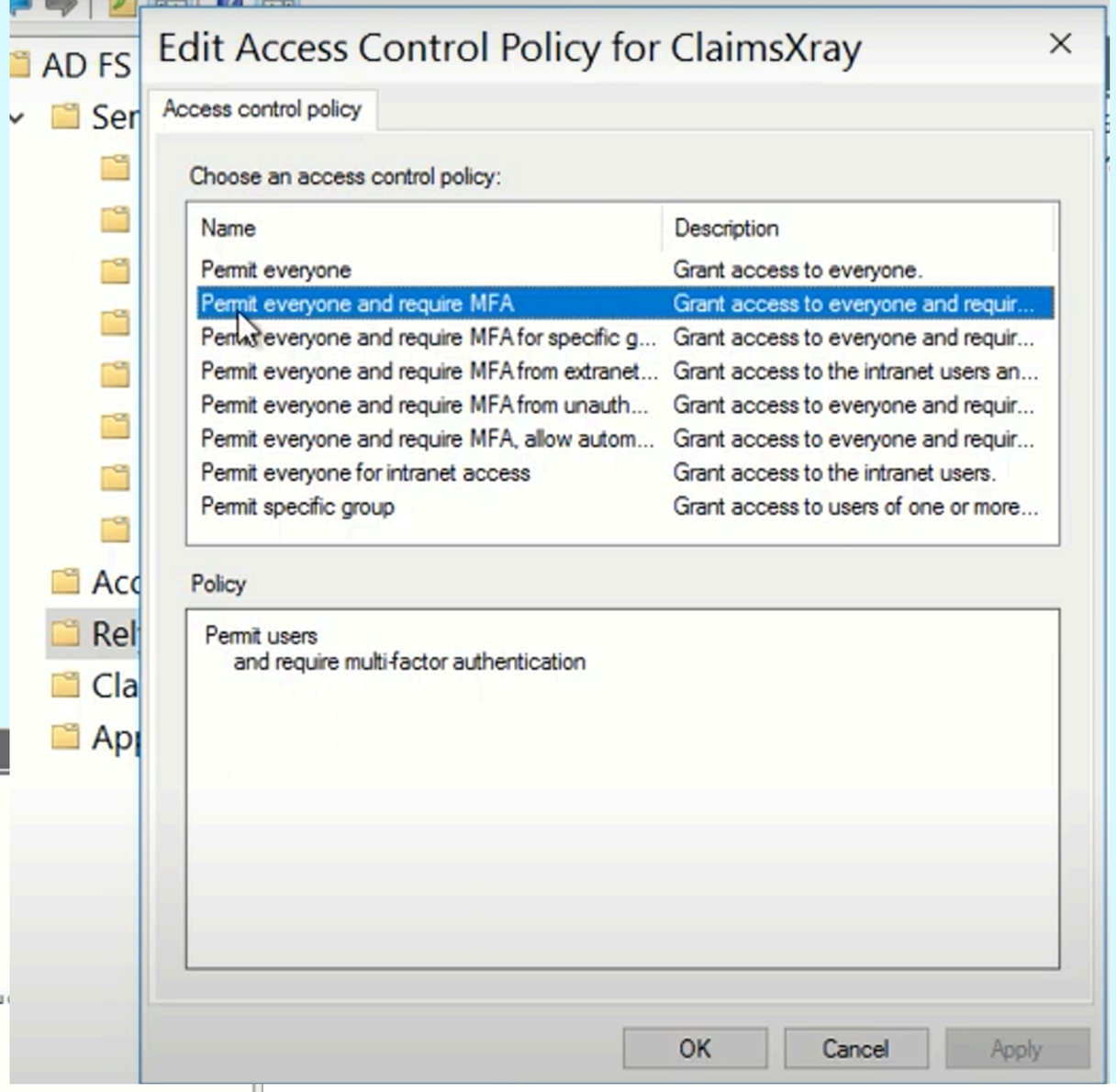
Multi – Factor Authentication



Multifactor authentication

MFA in ADFS using Certificate Authentication





DEMO 1

Xác thực User bằng giao thức OIDC(SSO& MFA) và SLO

Quay lại Chương trình

DEMO 2

XÁC THỰC USER BẰNG GIAO THỨC SAML 2.0(Không MFA) VÀ LADP

Quay lại Chương trình

DEMO 3

Tạo user mới(user bình thường) sau đó tiến hành SSO+MFA

Quay lại Chương trình

DEMO 4

Lấy JWT từ devtool sau đó decode để xem thông tin

Quay lại Chương trình