opentext™

Access Manager

Advanced Use cases

Selvaganesh Palaniappan
Anupkumar Rajan

Access Manager

8-quarter top innovation roadmap

Current – 25.1	25.2	25.3	25.4
	Access Manager CE 25.1 (v5.1.1) • ACDI (Auditing, Compliance and Data Intelligence) • Docker enhancements • reCAPTCHA v3 • External authentication method (EAM) for Entra ID • Java 11 update		Access Manager CE 25.4 (v5.2) • Multiple certificate support for IDP • ACME 2 • Java 21 update • TLS 1.3

26.1	26.2	26.3	26.4

Access Manager CE 26.1 (v5.2.1)
• IPv6 support
• Redhat OpenShift support
• Delegated User Access for helpdesk users
 	
Access Manager CE 26.1 (v5.2.2)
• Access Manager deployment in OT Pvt Cloud
	Access Manager CE 26.1 (v5.2.3)
	• IPv6 support
		Access Manager CE 26.3 (v5.3)
		• Administration Console UX Enhancements
		  • New UI for Access Gateway and Policies
		  • AI assistant
		• Continuous authentication and authorization
		• UEBA Support
		• Interset integration for XDR	

Agenda

- Entra ID External Authentication Method(EAM) Integration
- Token Exchange (RFC 8693)
- Access LucidX

opentext™

Entra ID EAM Integration

Microsoft Entra ID: Everything You Need To Know

External Authentication Method (EAM)

- The EAM allows user to select the external authentication provider for MFA.
- The first factor by Microsoft Entra ID. The second factor by external authentication provider
- An EAM can satisfy MFA requirements from Conditional Access policies
- EAMs differ from federation; the user identity is originated and managed in Microsoft Entra ID.
- EAMs are implemented on top of Open ID Connect (OIDC)
- EAMs require at least a Microsoft Entra ID P1 license.

Use Cases

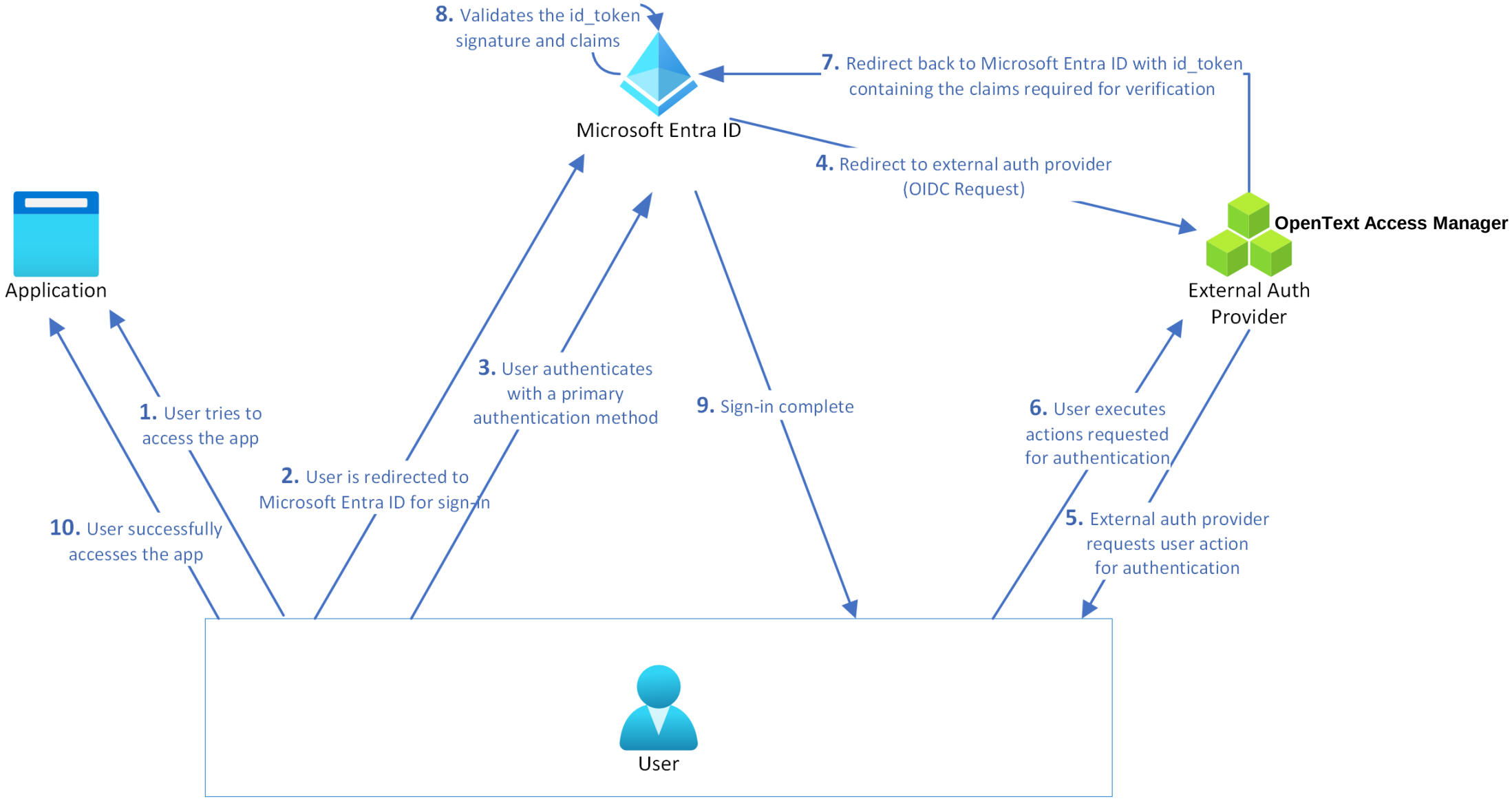
Entra ID tenant/NAM Administrator

Adam registers OAuth client application with NAM; and configures conditional access policy with external authentication method in Entra ID admin center to satisfy MFA by the external authentication provider NAM.

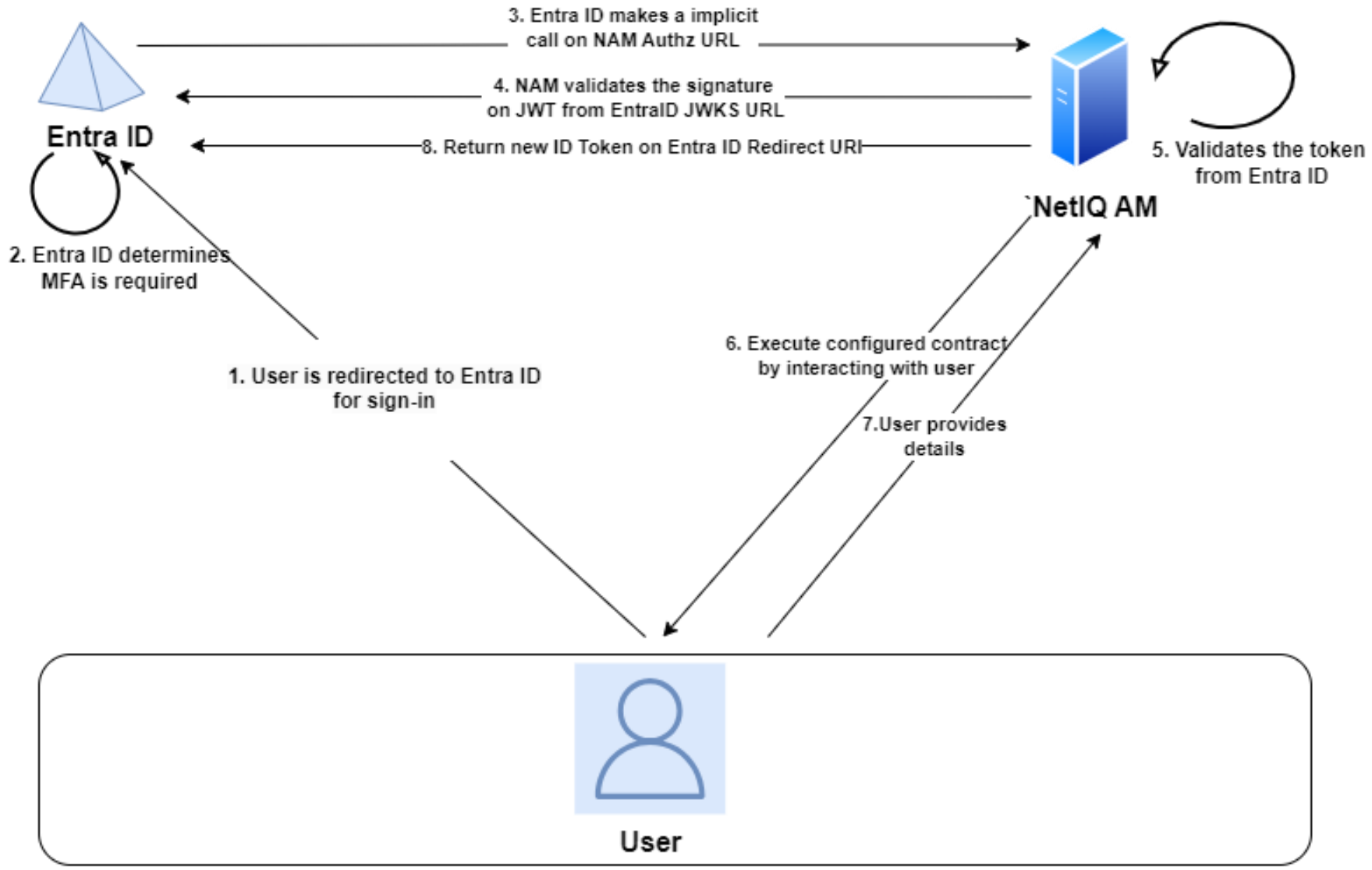
Entra ID protected application user

Maria accesses the application protected by Entra ID which requires MFA. The 1st factor authentication by Entra ID and the 2nd factor by NAM configured as external authentication provider in Entra ID.

Architecture



Architecture



Configuring EAM Integration

Step 1

Prep

- Know the OIDC discovery metadata endpoints of both NAM and Entra ID
- NAM authorization endpoint
- NAM OAuth public certificate and Entra ID - JWKS URI endpoint
- Entra ID redirect URI

Step 2

opentext™ | Access Manager

- Register Entra ID as OAuth Client application
- Configure Entra ID metadata and JWKS URI endpoints
- Configure id_token sub claim from id_token_hint
- Configure amr (authentication method reference) in contract
- Assign contract to the OAuth client application.

Step 3

Microsoft Entra ID

- Register an application with NAM's authorization endpoint as redirect URI.
- Configure EAM with above registered app ID and AM's client ID & discovery endpoint.
- Add permission of openid, profile & don't publish any scopes as it is just for authentication

Step 4

Verify

- Verify the authentication.

Reference Links

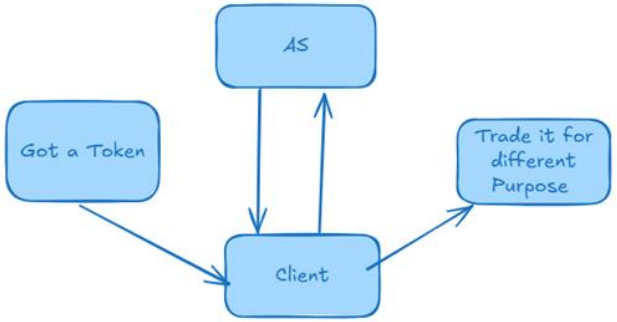
- Public preview: External authentication methods in Microsoft Entra ID
- External authentication provider with Entra ID
- Managing authentication methods for Entra ID
- Managing EAM in Entra ID

Token Exchange

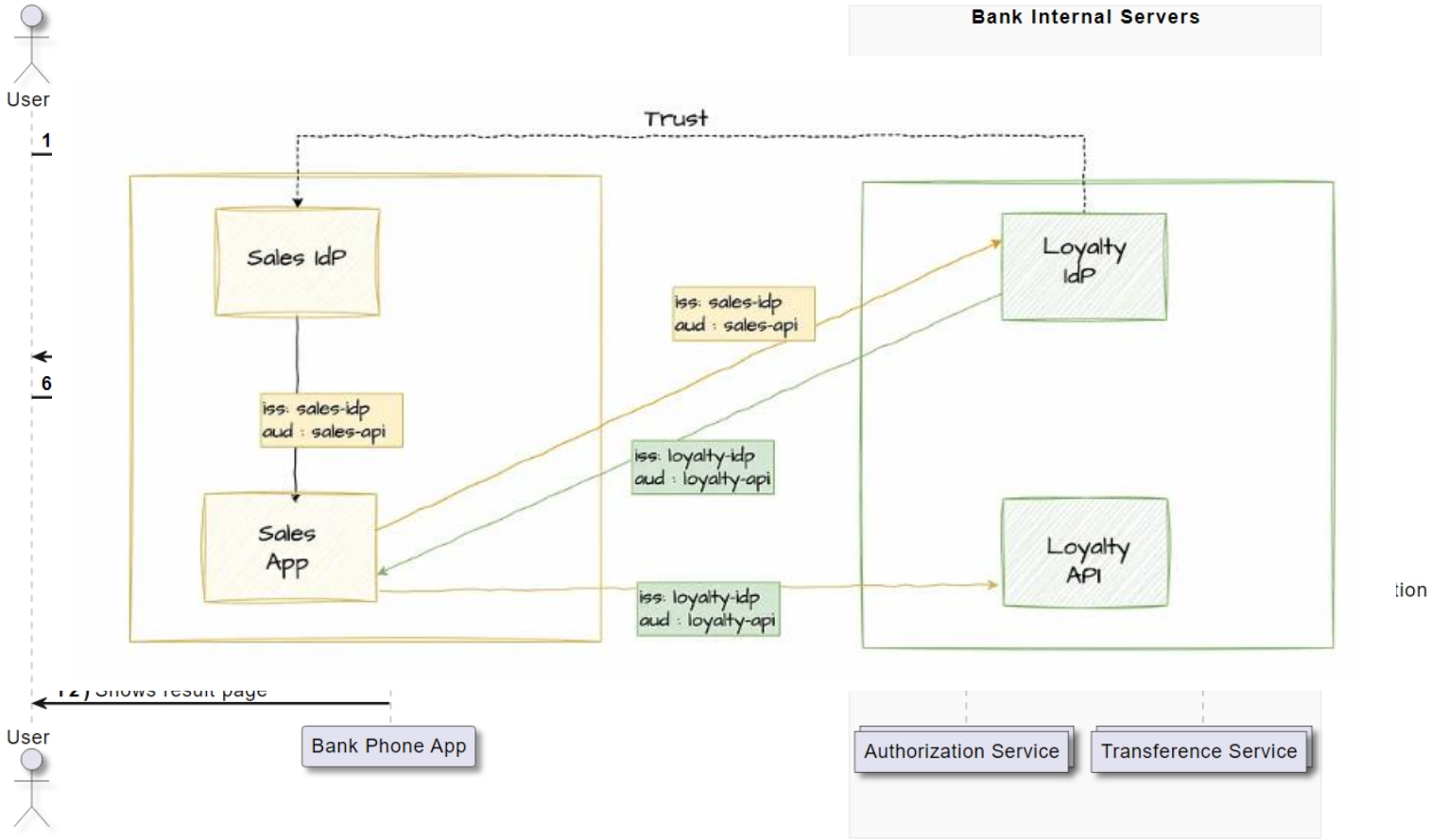
RFC 8693

Use Cases

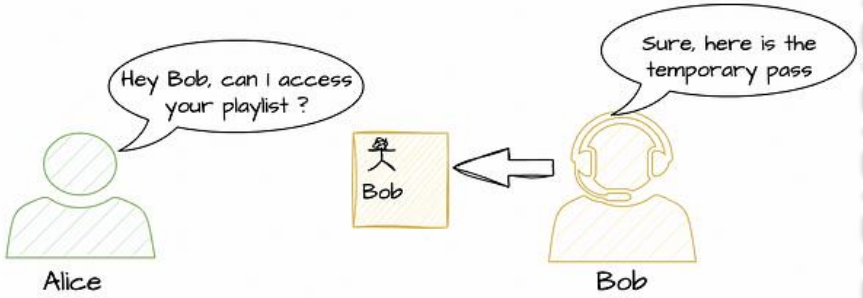
- ✓ Trade one token for another

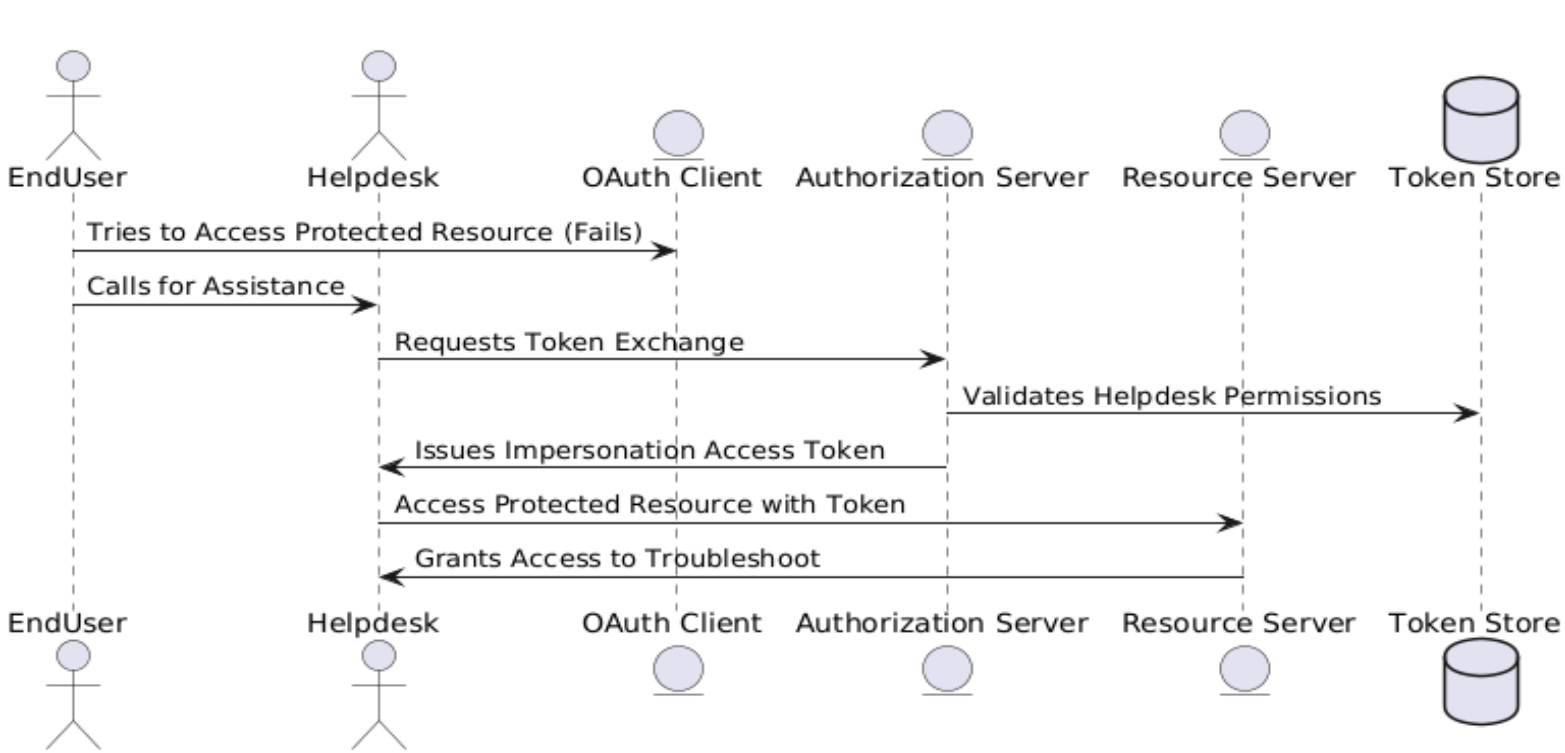


- ✓ Access to Heterogenous systems
  - principle of least privilege
  - cross domain
  - microservices
  - client is a RP or Gateway
  - impersonation/delegation



Impersonation





Impersonation Use Case

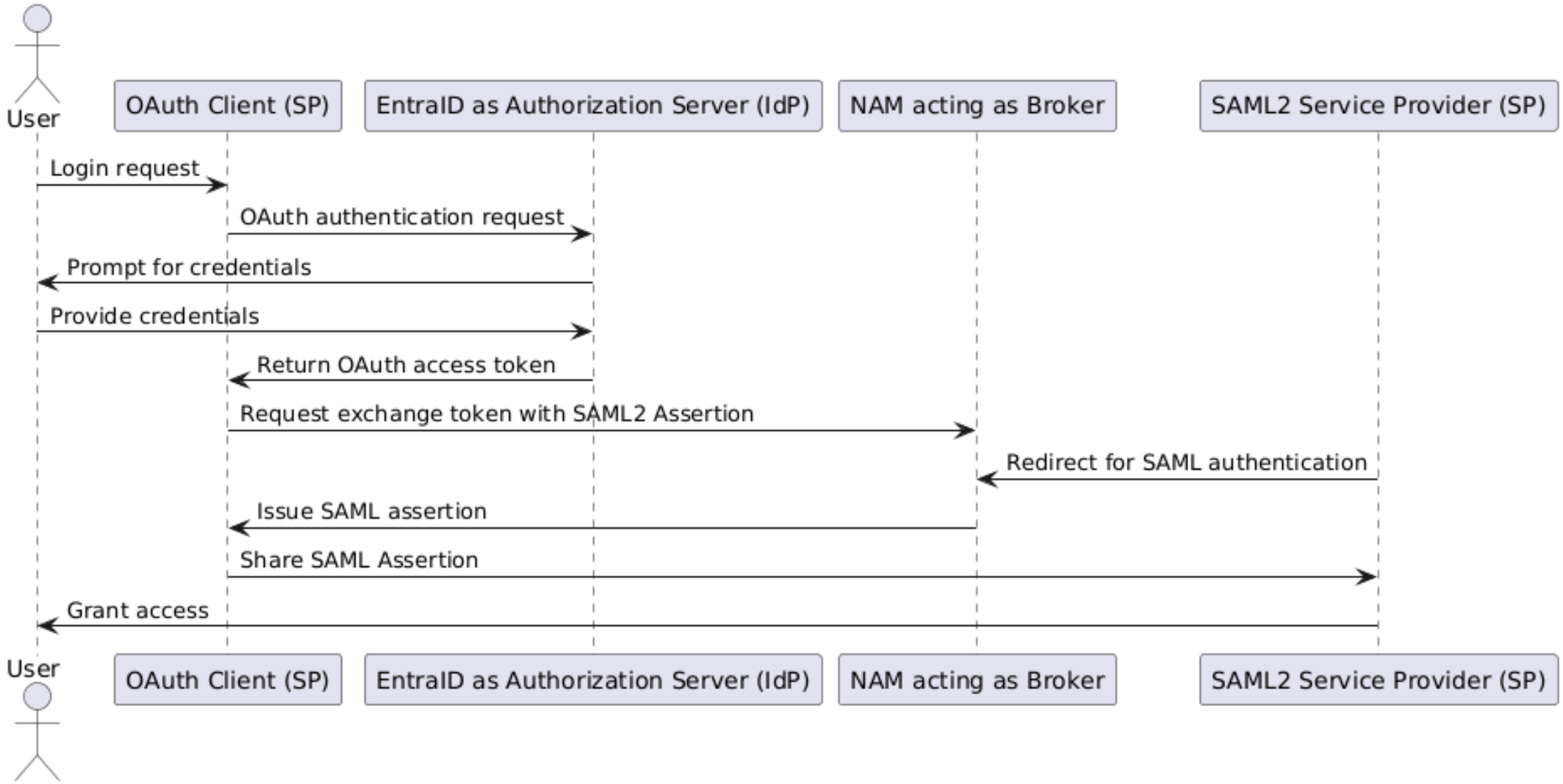
Alice
(End user)

Alice is facing issue with getting her email ID populated in the business application that prevents her from proceeding with a critical business operation.

Bob
(Help desk)

The help ticket gets assigned to Bob who needs to access the application as Alice to see the issue and resolve.

Brokering



opentext™

Access LucidX

Problem Statement

5.0 ★★★★★

Tremendous cross-protocol access management tool.

Reviewed on Dec 1, 2020

Reviewer Function: Software Development | Company Size: <50M USD | Industry: Industry

We've used NAM to federate all our major SaaS applications including Mic soft, Google, Adob as well as reverse proxy and load balance all our internal systems. Tremendous toolbo

Interconnectable features

4.0 ★★★★☆ Review Source:

NetIQ Access Manager, our trusted Access Management solution for more than 10 years

Reviewed on Feb 15, 2022

Reviewer Function: Management / Business Consulting | Company Size: Gov't/PS/ED 5,000 - 50,000 Employees | Industry: Education Industry

We have been using this product for over 10 years and it has never let us down. It is a very solid product with unique features that competitors simply do not have. The integration with Advanced Authentication allows our organisation to technically support almost any scenario. The product ...

Read Full Review

Growing product integrations

Longer learning curve

5.0 ★★★★★ Review Source:

NAM is a powerful product that can do everything you need it to and more

Reviewed on Jan 24, 2024

Reviewer Function: Software Development | Company Size: Gov't/PS/ED <5,000 Employees | Industry: Education Industry

Overall experience with NAM has been great. Powerful tool that can do a lot once you dive into it

Read Full Review

Expanding feature capabilities

IT Security and Risk | Company Size: 30B + USD | Industry: Energy and Utilities Industry

t. Breadth of feature coverage. Stability of the implemented product.

Tracking intricacies

5.0 ★★★★★ Review Source:

A "Swiss Army Knife" of Access Management

Reviewed on Feb 4, 2024

Reviewer Function: IT Services | Company Size: <50M USD | Industry: IT Services Industry

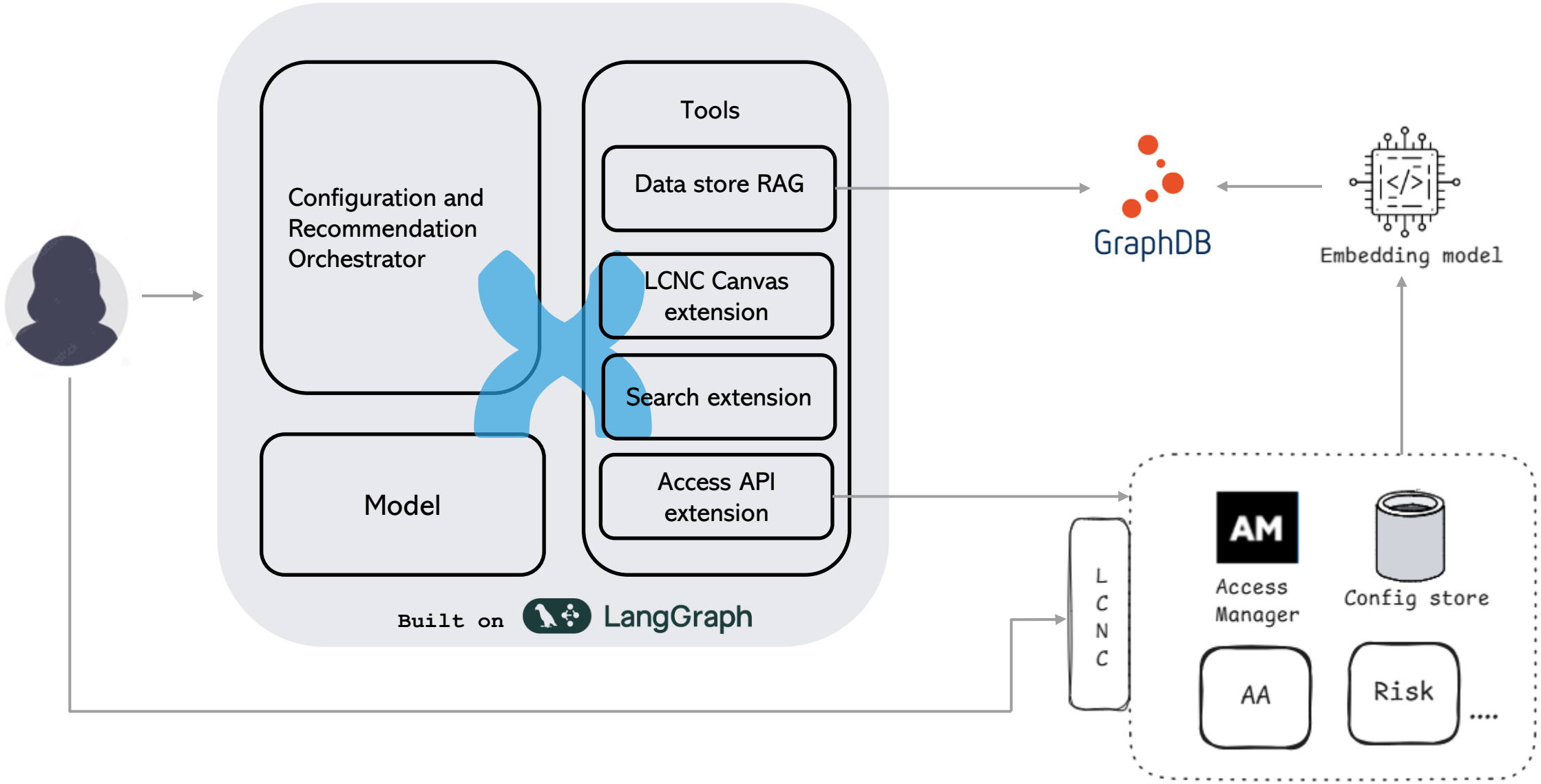
Accepts a lot of input on future direction of the product's features. Responsive to customer needs and wants. Very price competitive. Base product includes an incredible amount of features. Product is a true "Swiss Army Knife" of Access Management. ...

Read Full Review

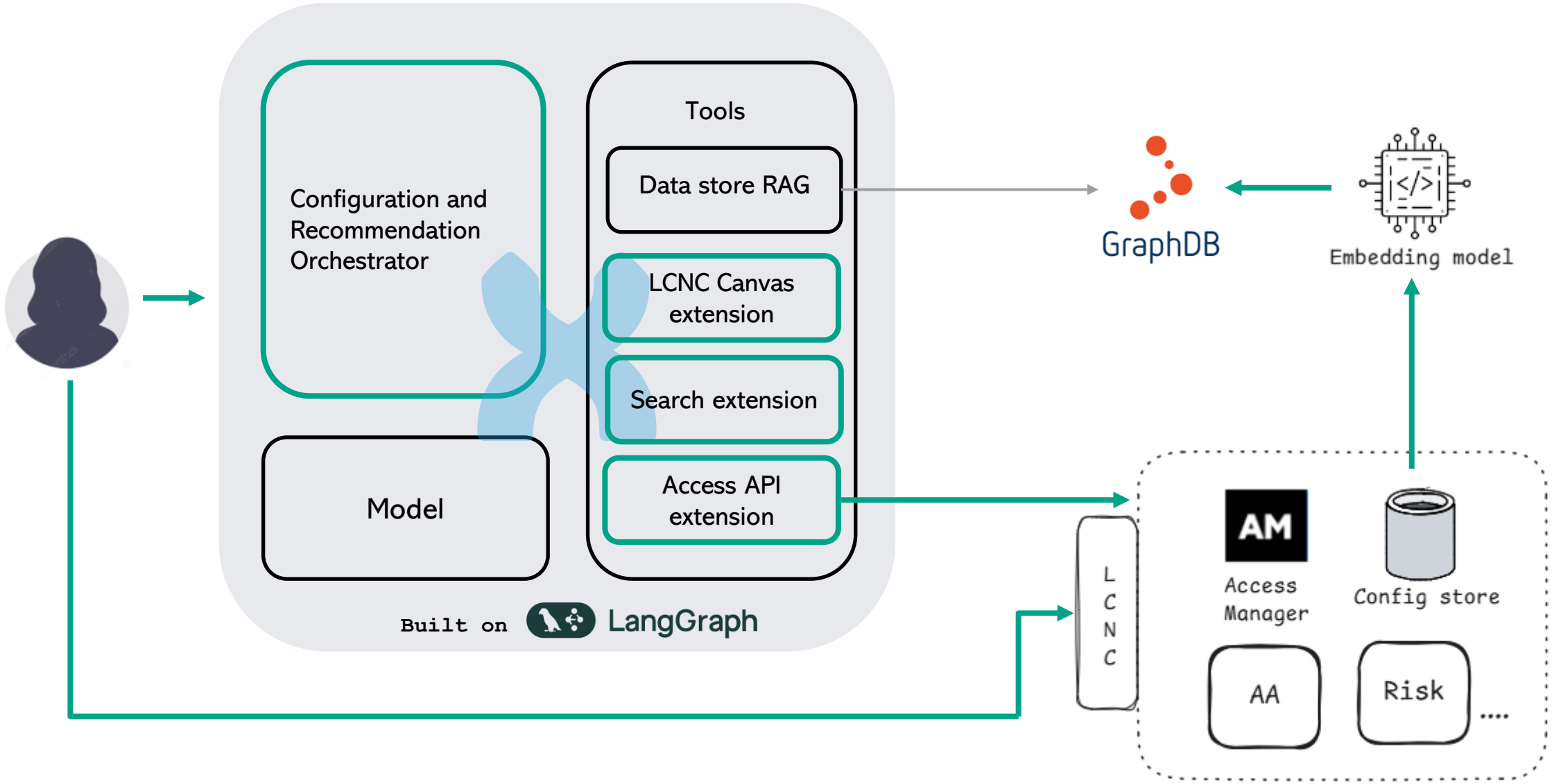
Larger turnaround time

opentext™

Architecture



Scope



Demo

PURPOSE

Access assistant

Configure
Visualize
Manage

Observe and troubleshoot

BENEFIT

Builds Trust

Integrations
ROI

Faster turnaround

“Make it simple, clear and then eXecute”


opentext™