

End-to-end agent security

Microsoft Agent Framework and MCP



MC2MC
—CONNECT—

Geert Baeke

Cloud-Native & AI Architect @ Cronos & MBarQ



mbarQ



@geertbaeke.bsky.social



youtube.com/@GeertBaeke



@geertbaeke



github.com/gbaeke



linkedin.com/in/geertbaeke/



https://baeke.info

 2Pint



robopack 

wortell

INGRAM[®] MICRO



The Collective

 bechtle

 lebon.IT

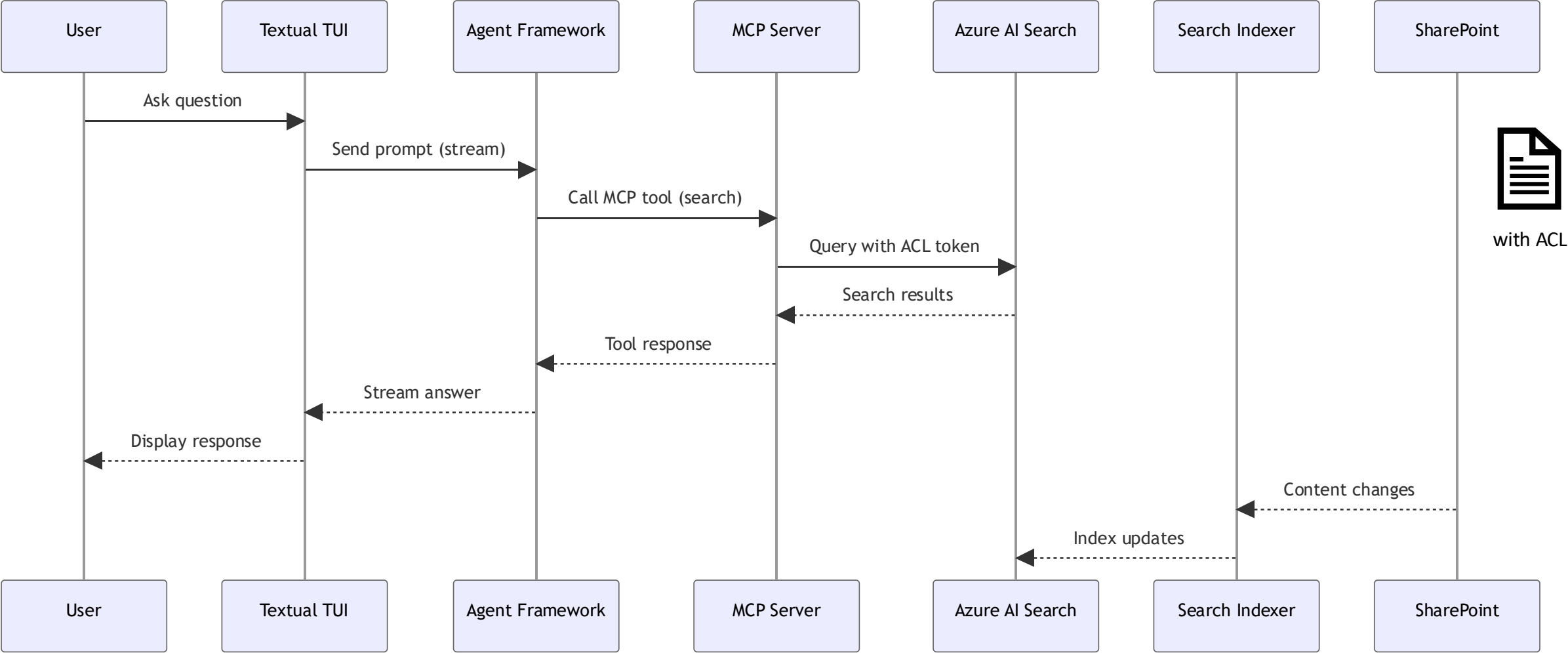


 VirtualMetric

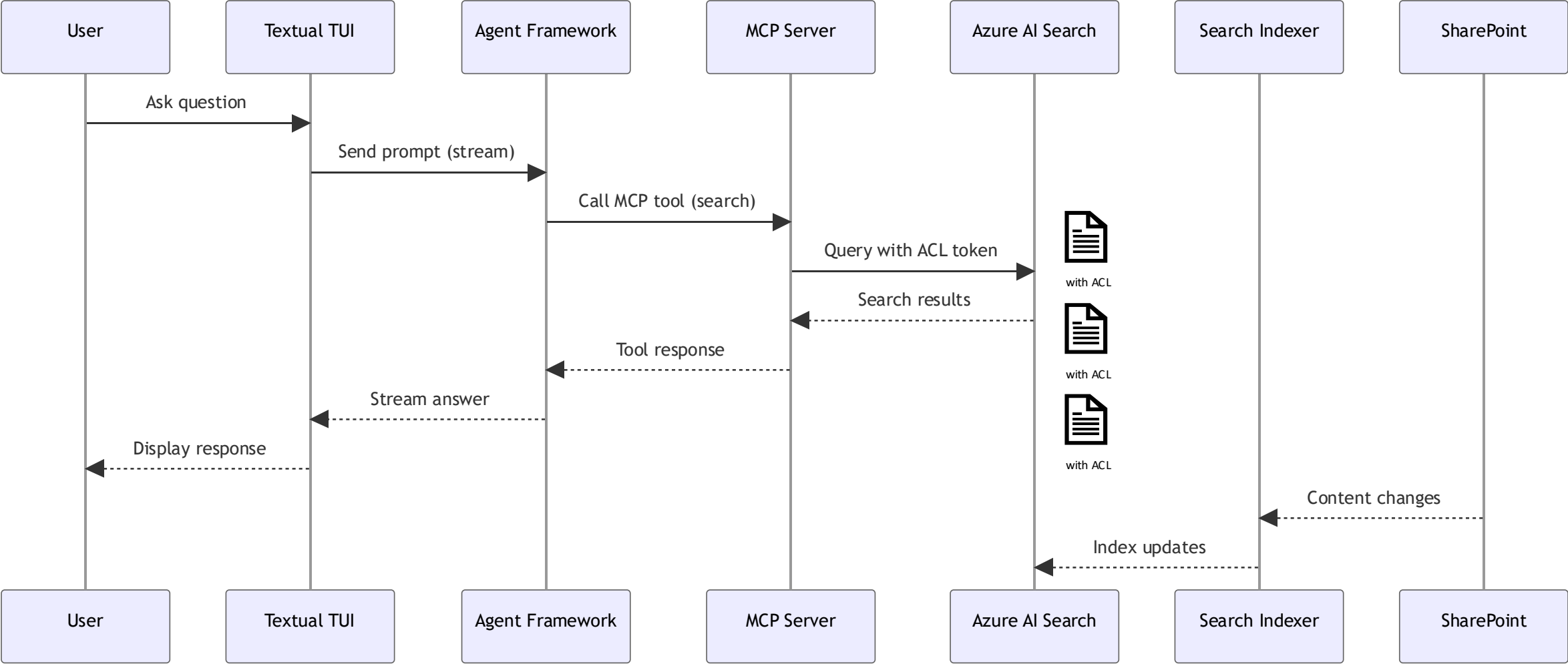
veeam

evri

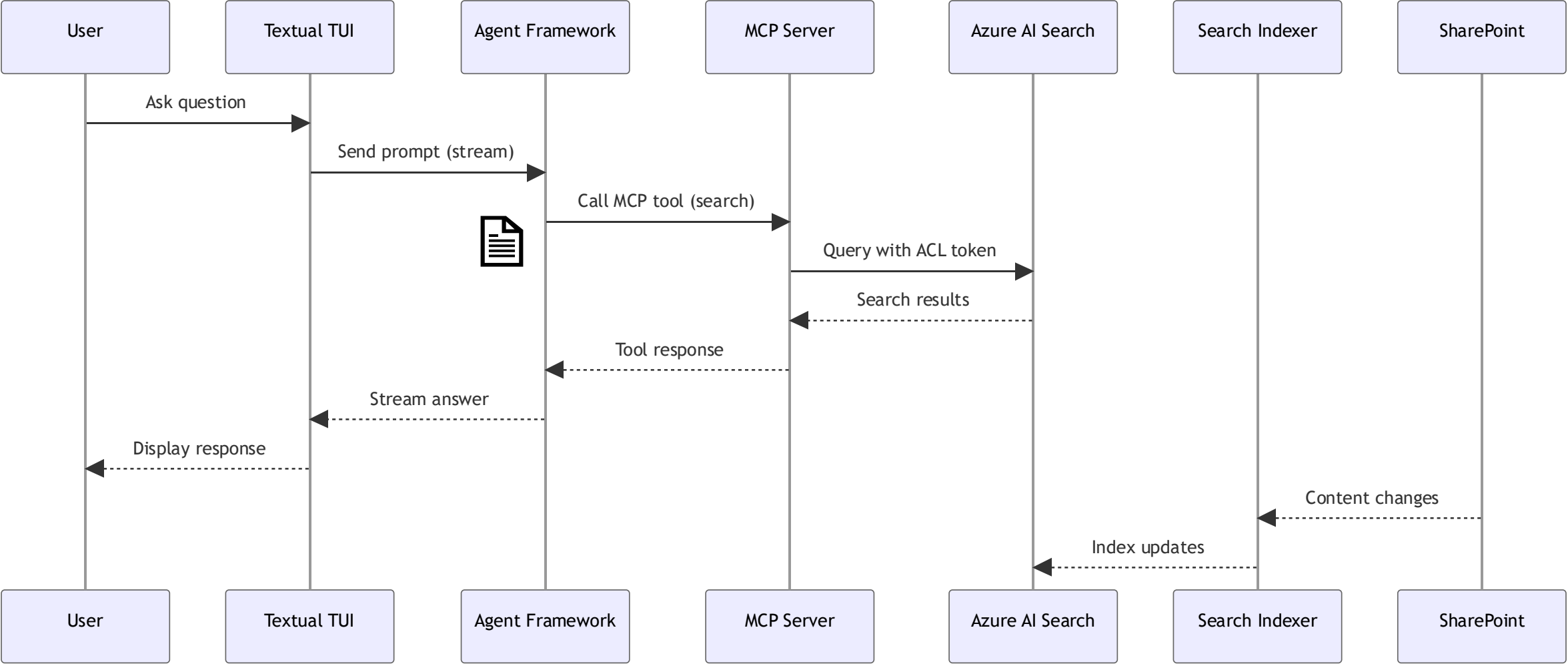
Big Picture



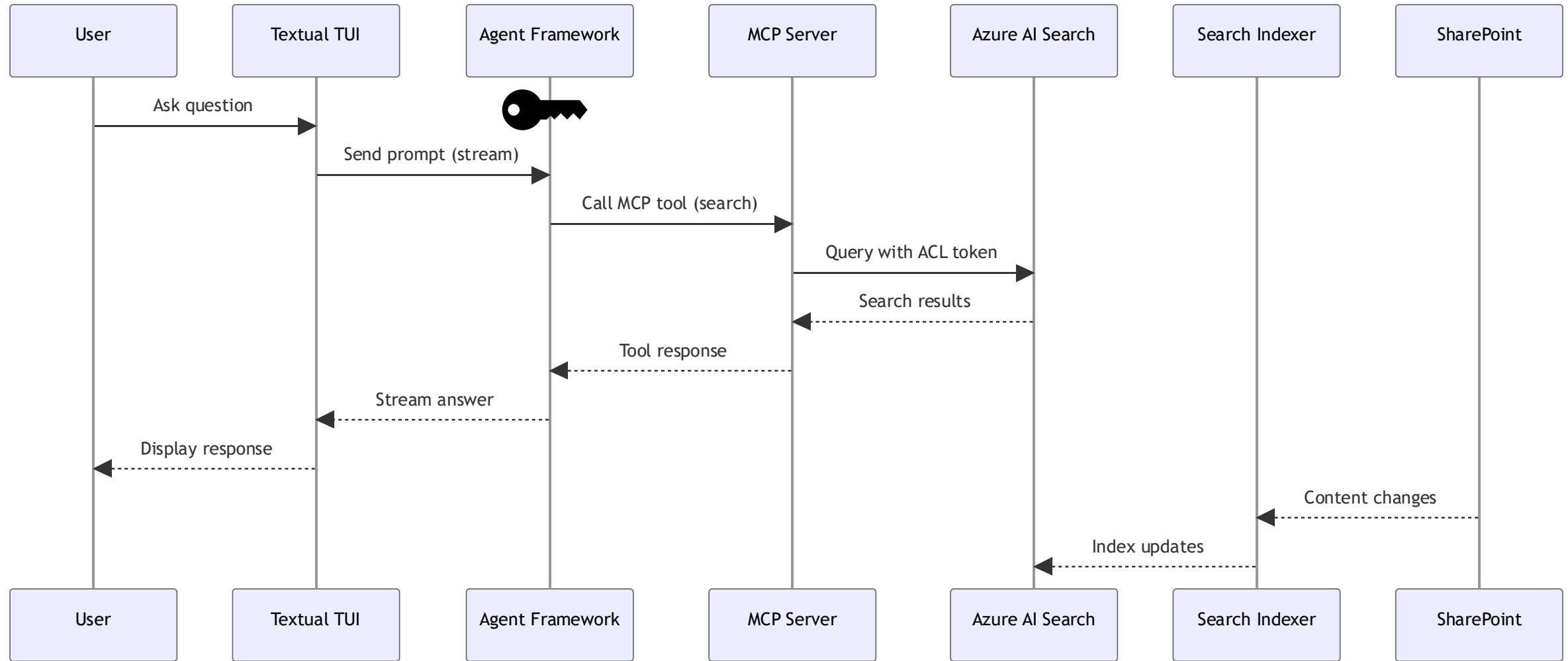
Big Picture



Big Picture



Big Picture



SharePoint

Search this library

Home

Documents

Pages

Architecture Docs

Site contents

Edit

+ New

Upload

Edit in grid view

Forms

New

Add shortcut to OneDrive

Pin to Quick access

Automate

In

Architecture Docs

Name

How to start a new AI Project at Inity.d

SharePoint

BROWSE

PERMISSIONS

Delete unique permissions

Grant Permissions

Edit User Permissions

Remove User Permissions

Check Permissions

Inheritance

Grant

Modify

Check

Home

Documents

Pages

Architecture Docs

Site contents

EDIT LINKS

This library has unique permissions.

	Type	Permission Levels
<input type="checkbox"/> <input type="checkbox"/> Name		
<input type="checkbox"/> <input type="checkbox"/> Communicatiesite - Bezoekers	SharePoint Group	Read
<input type="checkbox"/> <input type="checkbox"/> Communicatiesite - Eigenaars	SharePoint Group	Full Control
<input type="checkbox"/> <input type="checkbox"/> Communicatiesite - Leden	SharePoint Group	Edit
<input type="checkbox"/> <input type="checkbox"/> grp-search-filter	Domain Group	Edit

sp-custom-index

⚡

snippet_vector

SingleCollection

✓

metadata_spo_item_

String

✓

metadata_spo_item_

String

✓

metadata_spo_item_

String

✓

metadata_spo_item_

DateTimeOffset

✓

metadata_spo_item_

Int64

✓

metadata_spo_item_

String

✓

metadata_spo_item_

String

✓

metadata_author

String

✓

metadata_creation_d

DateTimeOffset

✓

metadata_last_modif

DateTimeOffset

✓

metadata_title

String

✓

metadata_content_ty

String

✓

Department

String

✓

UserIds

StringCollection

✓

GroupIds

StringCollection

✓

sp-custom-indexer

Indexer

▶ Run

↺ Reset

💾 Save

🔄 Refresh

{ } Edit JSON

🗑 Delete

Execution history

Settings

Number of recent runs to show

10

32

24

16

8

0

3.26

31.12

1.98

2.57

7.63

2.88

1.91

2.04

2.26

1.95

1/21...

1/22...

1/23...

1/24...

1/25...

1/26...

1/27...

1/28...

1/29...

1/30...

Success

Failed

In Progress

Reset

Partial Success

Status

Start time

Duration

✓ Success

1/30/2026, 1:19...

1 s

✓ Success

1/29/2026, 1:19...

2 s

✓ Success

1/28/2026, 1:19...

2 s

✓ Success

1/27/2026, 1:19...

1 s

✓ Success

1/26/2026, 1:19...

2 s

✓ Success

1/25/2026, 1:19...

7 s

✓ Success

1/24/2026, 1:19...

2 s

✓ Success

1/23/2026, 1:19...

1 s

✓ Success

1/22/2026, 1:19...

31 s

✓ Success

1/21/2026, 1:19...

3 s

Client Application

```
o AgentTui

Authenticated. Ask a question to begin.

You: How to start a project at Inity?

Assistant:
To start a project at Inity, follow these steps:

1 Get the project name.
2 Create a Foundry project in Azure.
3 Deploy models.
4 Ask Geert to start coding the app.

For more detailed instructions, you can refer to the official document here: How to start a new AI Project at Inity.
(Source: [1])

Sources (Top 3)
1. How to start a new AI Project at Inity.docx
  • How to start a new AI Project at Inity:
    • Get project name
    • Create Foundry project in Azure
    • Deploy models
    • Ask Geert to start coding the app
    AI Project success rates

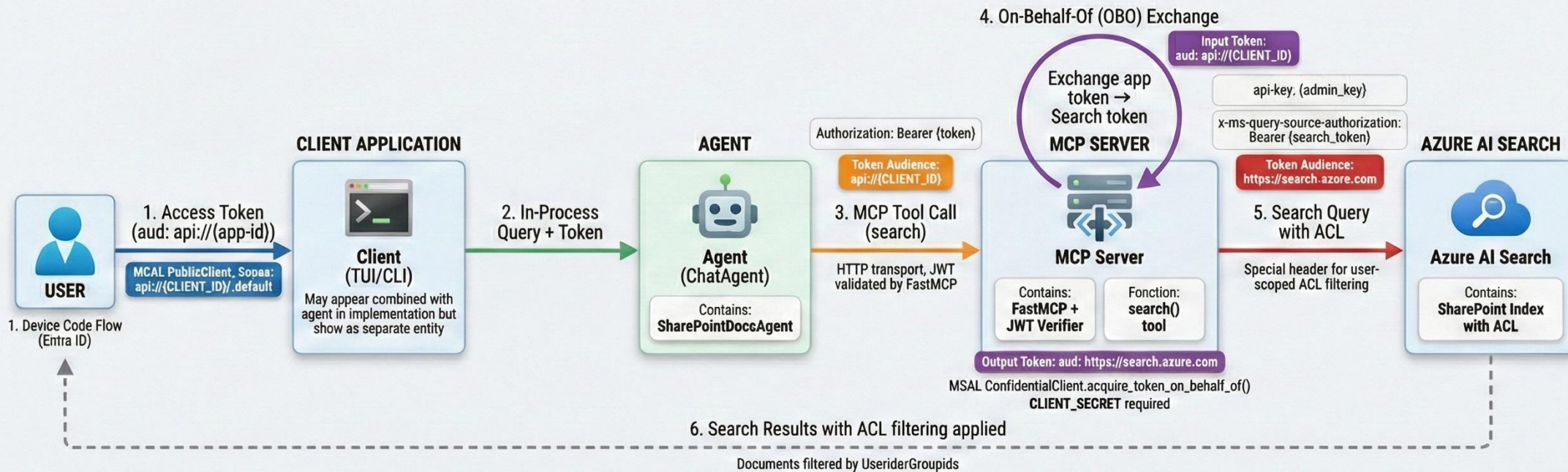
image.png

Idle • Signed in as live.com#geert@baeke.info

Ask a question...

^q Quit ^l Clear esc Cancel f2 Toggle Raw ^p palette
```

Authentication Flow



Key Security Highlights:

1. Token Scopes

- User Token: `api://{CLIENT_ID}/.default`
- Search Token: `https://search.azure.com/.default`

2. OBO Flow Requirements

- Confidential Client (`CLIENT_SECRET`)
- Original user token with delegated permissions
- Target scope: Azure AI Search

3. ACL Enforcement

- Azure AI Search receives user identity via **x-ms-query-source-authorization**
- Filters results by **UserIds** and **GroupIds** fields
- Only returns documents user has permission to access



Version Info: FastMCP with HTTP transport, MSAL 1.25+

API Versions: Azure AI Search API: 2025-11-01-preview (for ACL support)

Security Note: Documents filtered per-user based on Azure AD group membership

The Agent

- Basic agent written in Microsoft Agent Framework
- Uses gpt-4.1 provided by Microsoft Foundry
- Agent is co-located with the TUI

```
instructions = (  
    "You answer questions using the MCP search tool. "  
    "Always call the MCP tool to retrieve relevant documents before answering. "  
    "If no documents are found, say you could not find relevant content."  
)  
  
async with (  
    MCPStreamableHTTPTool(  
        name="SharePoint Search MCP",  
        url=MCP_SERVER_URL,  
        headers=headers,   
    ) as mcp_tool,   
    ChatAgent(  
        chat_client=chat_client,  
        name="SharePointDocsAgent",  
        instructions=instructions,  
    ) as agent,  
):  
    result = await agent.run(query, tools=mcp_tool)
```

Authorization: Bearer ey...

- Agent calls the search tool
- MCP server verifies the token
- Search tool exchanges app token for Azure AI Search token
- Search API called with token in special header

```
url = f"{search_endpoint}/indexes/{resource_prefix}-index/docs/search"
body = {
    "search": query,
    "select": "snippet,metadata_title,metadata_spo_item_name,metadata_spo_item_weburi",
    "top": top,
    "count": True,
}
headers = {
    "api-key": api_key,
    "x-ms-query-source-authorization": search_token,
    "Content-Type": "application/json",
}

try:
    response = post_with_retry(
        url,
        params={"api-version": api_version},
        headers=headers,
        body=body,
    )
except requests.exceptions.RequestException as exc:
    return {"authenticated": True, "error": str(exc)}
```

Last thoughts

- This approach is very flexible and can deliver high quality results

 However:

- Copilot Studio and Microsoft 365 Agents **automatically** filter documents
- Azure AI Search knowledge sources can query SharePoint directly **without building an index** (Foundry IQ)

 **Thoroughly consider your options and use agent evaluations to determine the valid approach**

Session feedback
available in home feed
of the app after the
session



Thank You



MC2MC
—CONNECT—