Workload Identity Management in Agentic Platform

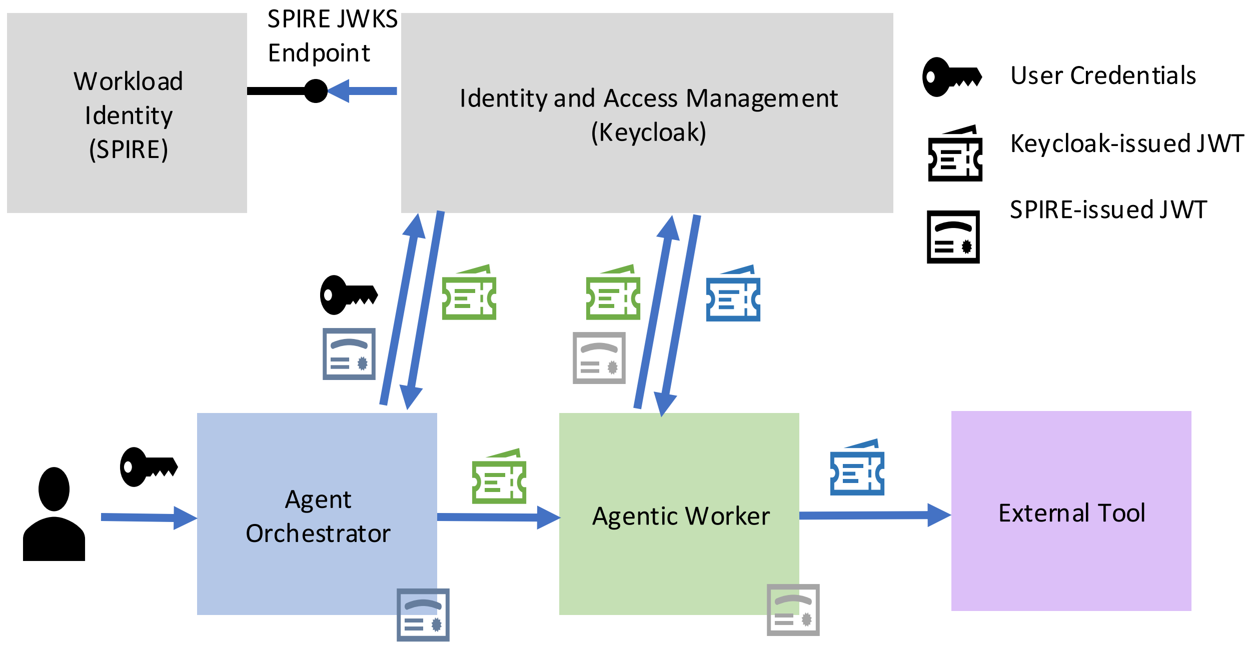
Identity and Authorization Management Summary

Challenges:

- Agents need to perform actions on behalf of users
- Static credentials (e.g., API Keys) violate zero-trust principles
- Need to give agents just the right set of permissions to perform an action

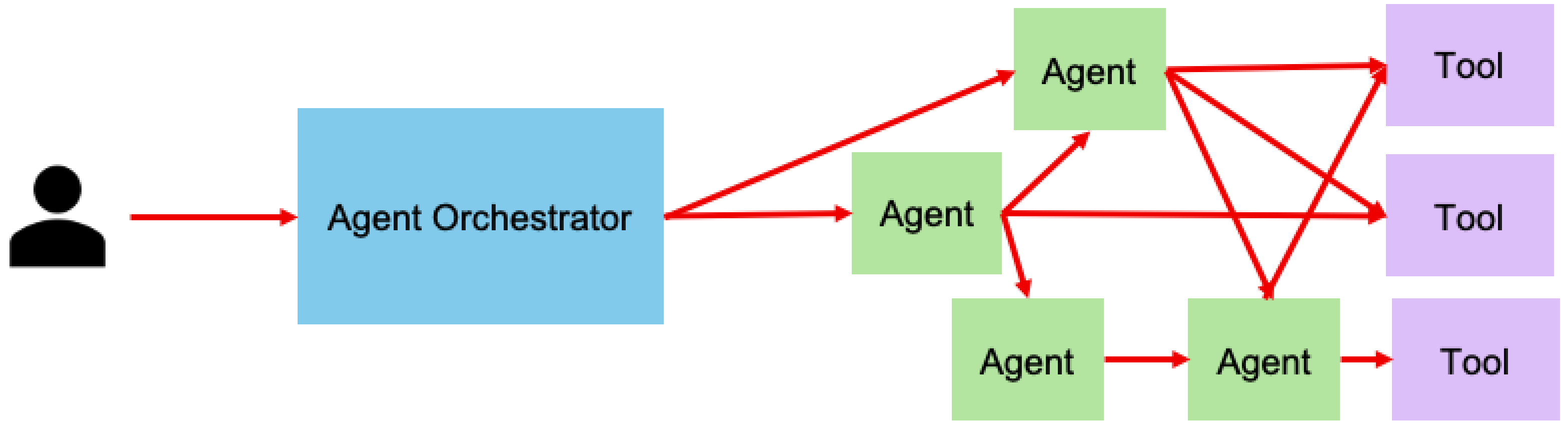
Approach:

- Leverage standardized approaches for workload identity (SPIFFE/SPIRE)
- Token Exchange: leverage identity and access management (Keycloak)

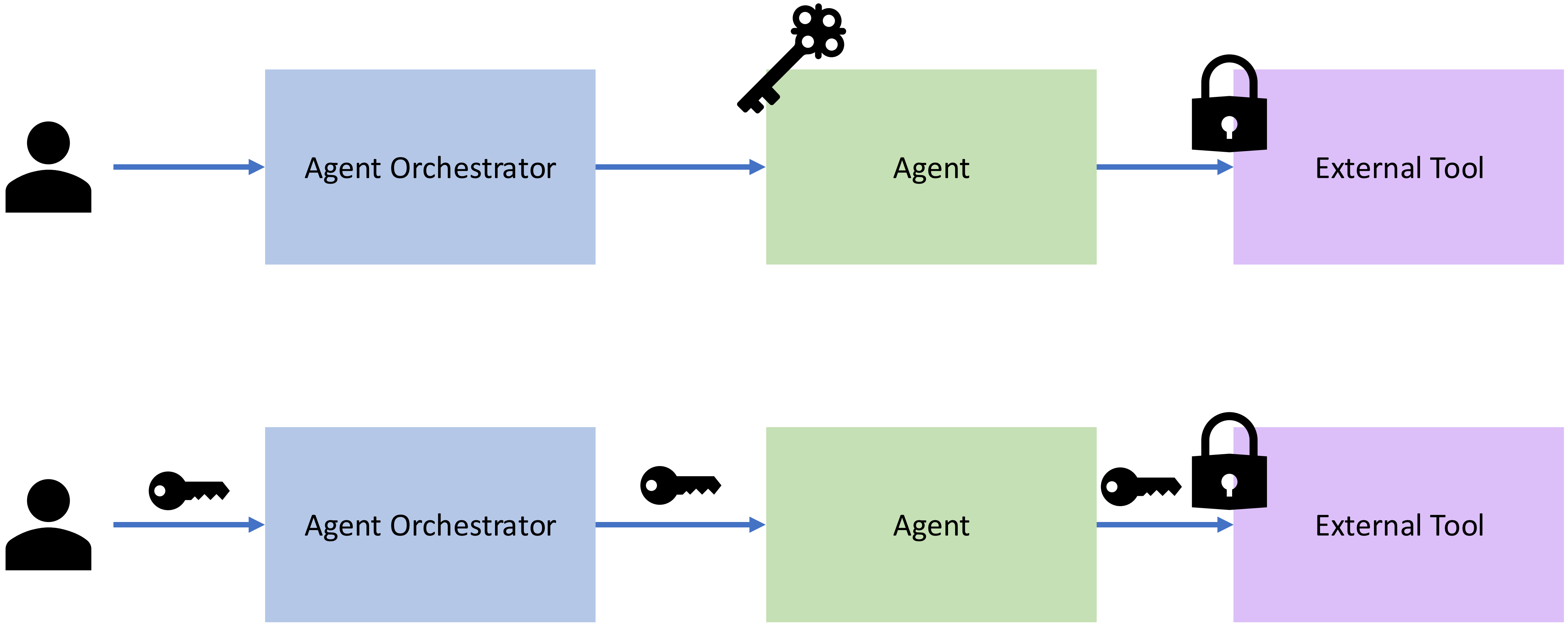


Background

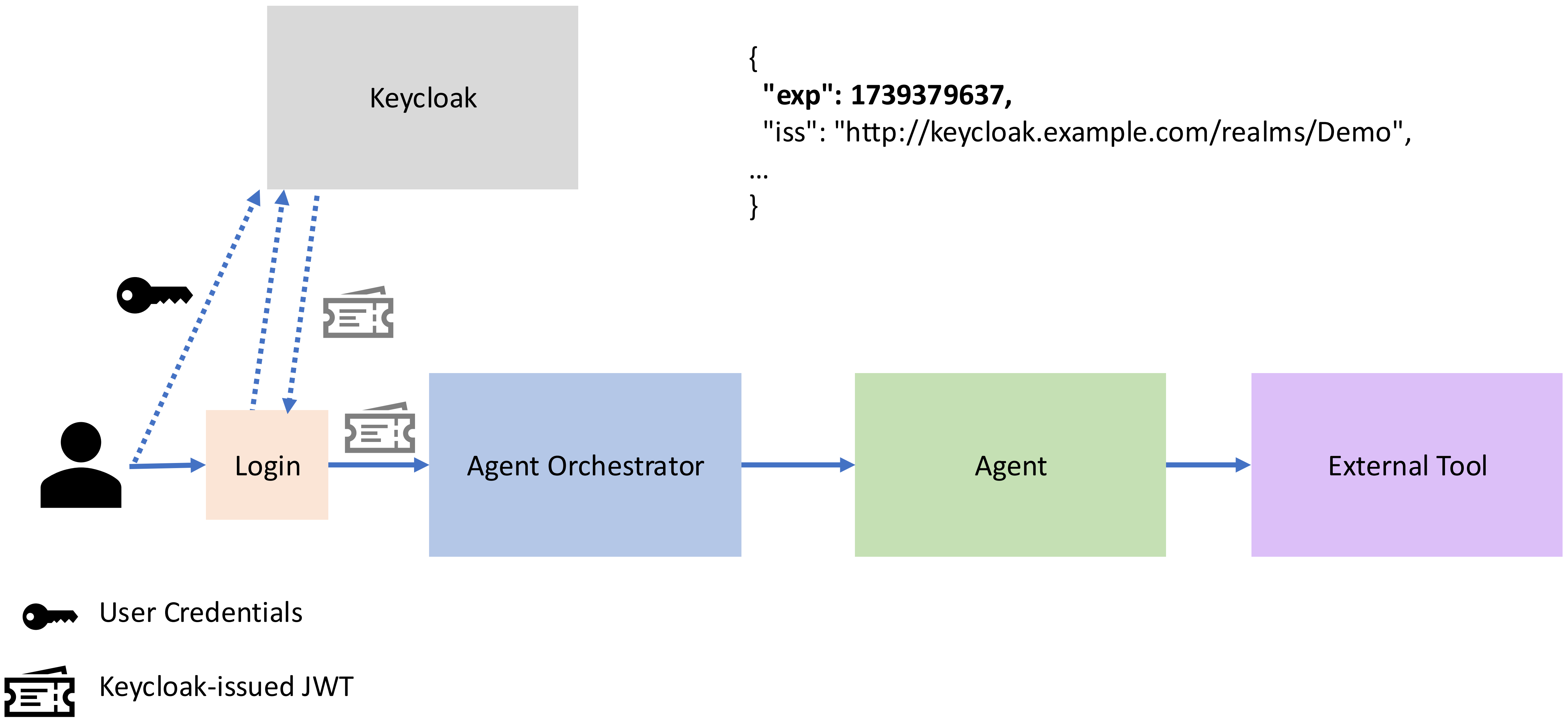
- In agentic applications, transaction flows are more **dynamic** than ever
  - Users calling agents
  - Agents calling tools on behalf of users
  - Agents calling agents



What we’re avoiding: “workloads act as users”



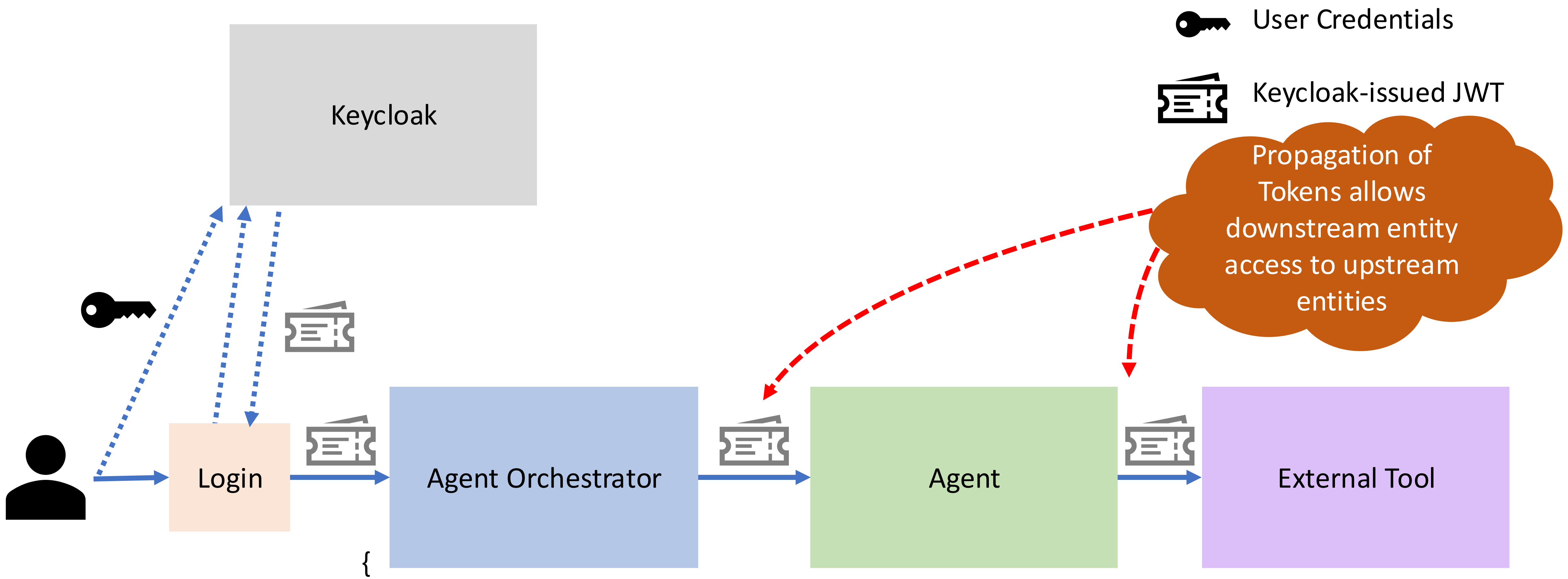
OAuth2.0 for short-lived user delegation



```
{
  "exp": 1739379637,
  "iss": "http://keycloak.example.com/realms/Demo",
…
}
```

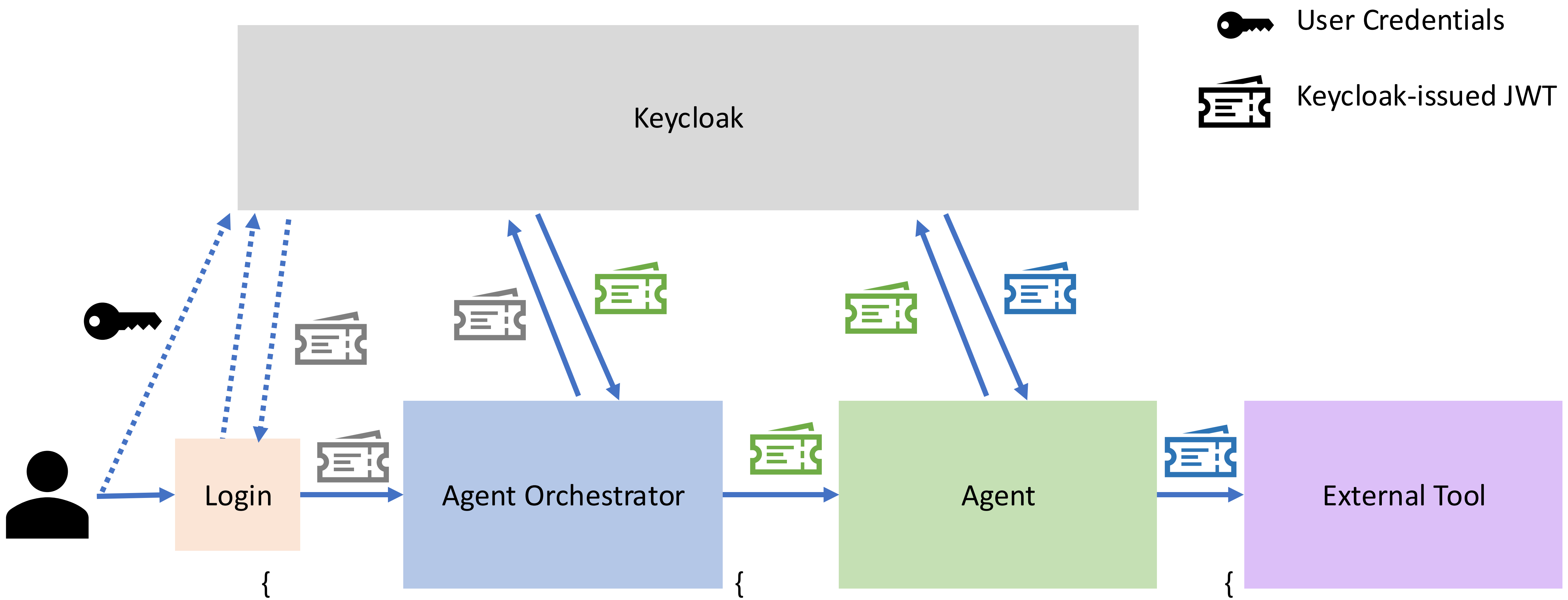
Passed access tokens should be **minimally-scoped**.

What we're avoiding: token passthrough



```
{
  "exp": 1739379637,
"aud": ["Agent Orchestrator", "Agentic Worker", "External Tool"],
"azp": ["Login"],
}
```

Token Exchange



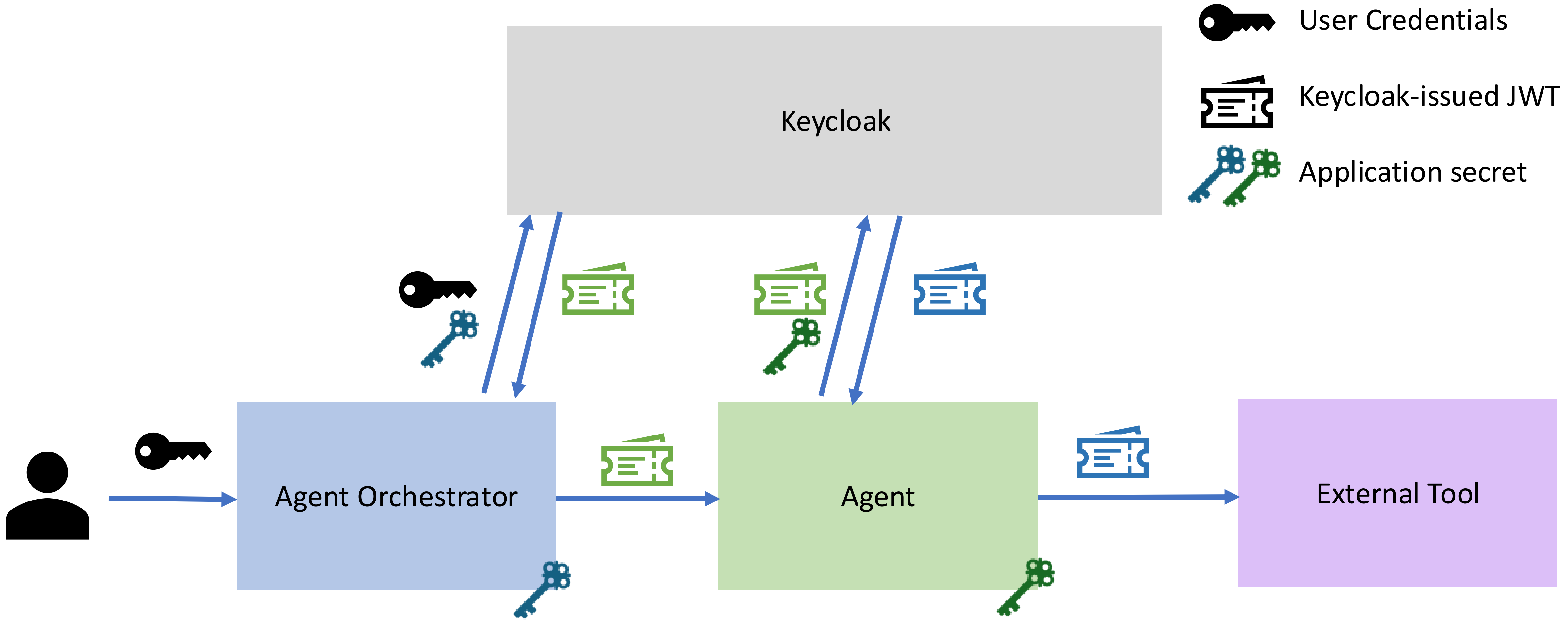
```
{
 "exp": 1739379637,
 "aud": "Agent Orchestrator",
 "azp": "Login",
}
```

```
{
 "exp": 1739379637,
 "aud": "Agentic Worker",
 "azp": "Agent Orchestrator",
}
```

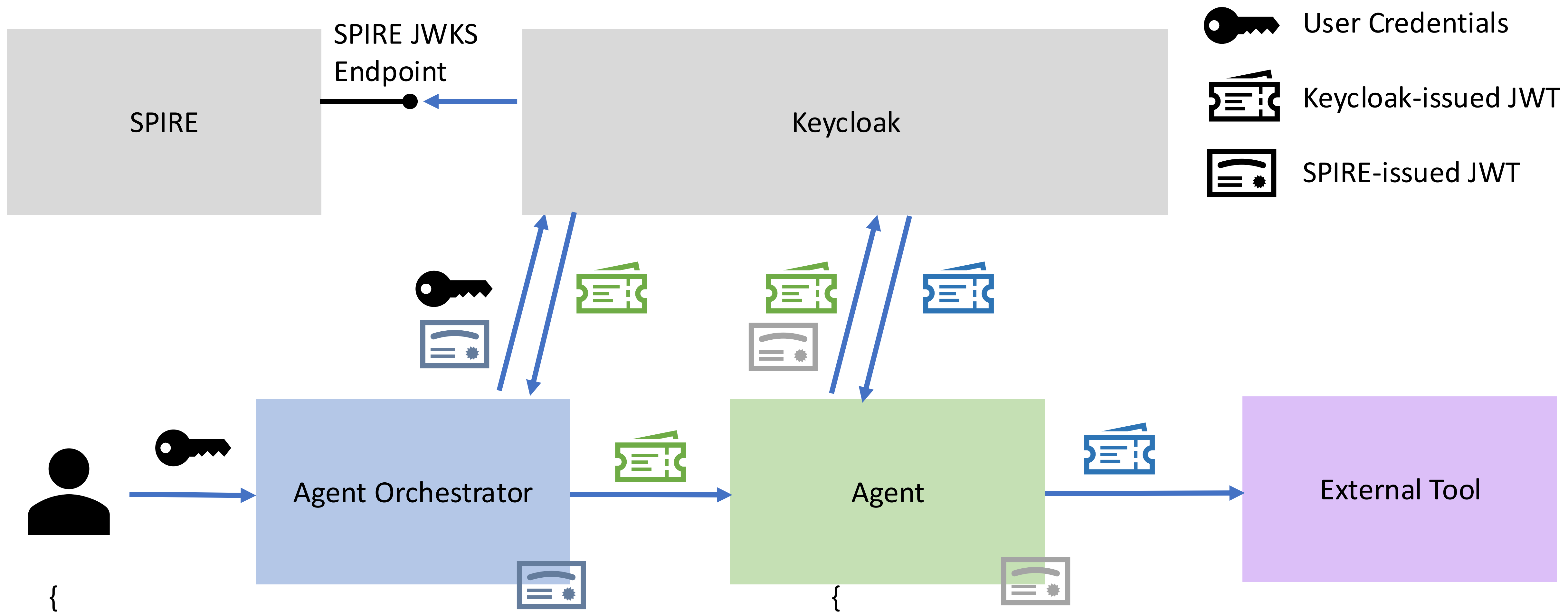
```
{
 "exp": 1739379637,
 "aud": "External Tool",
 "azp": "Agentic Worker",
}
```

Workload credentials should be **dynamic**.

What we're avoiding: static secrets



Workload Authentication with SPIRE

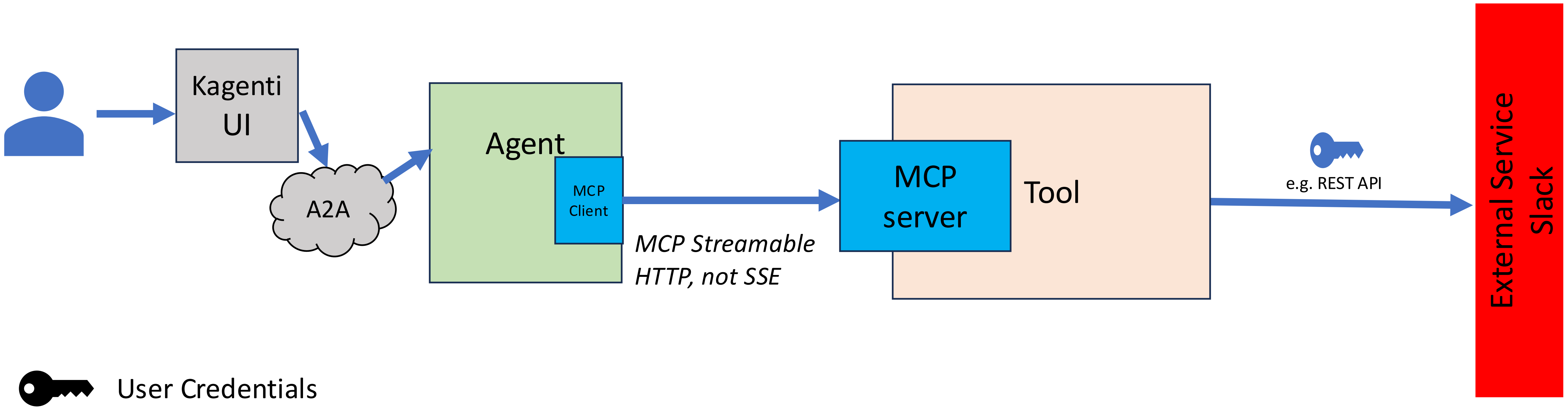


```
{
  "exp": 1739379637,
  "iss": "http://spire.example.com/oidc-discovery",
  "sub": "spiffe://example.com/agent-orchestrator",
}
```

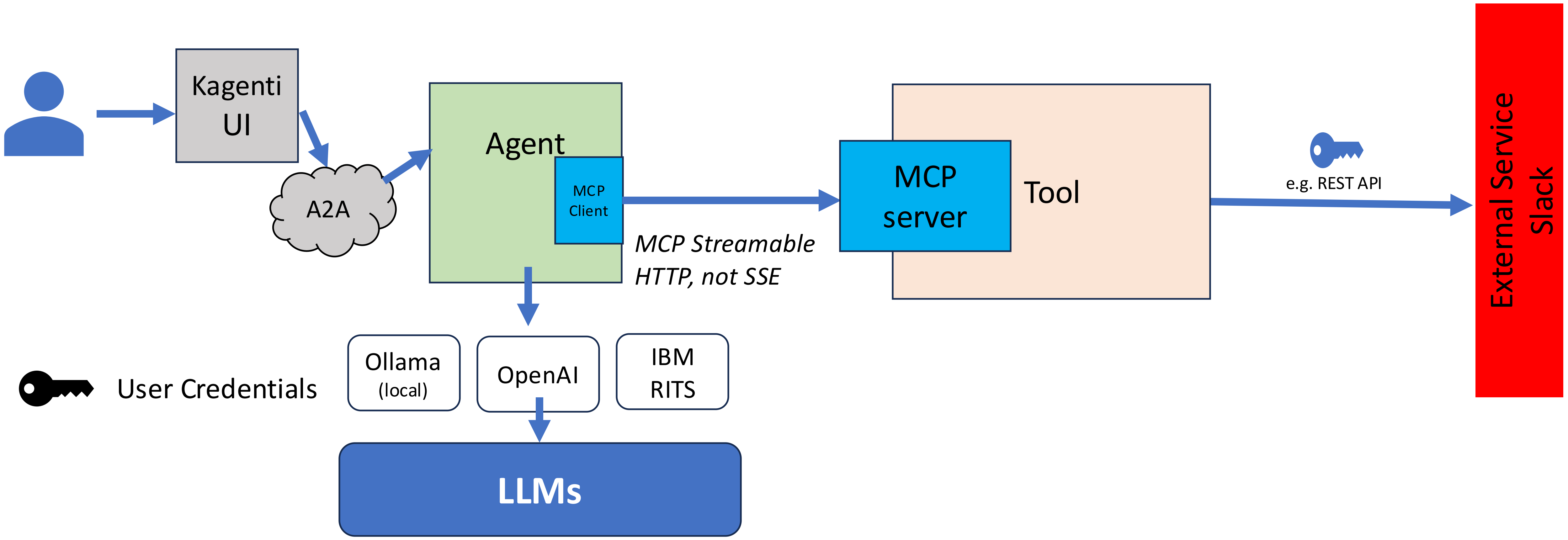
```
{
  "exp": 1739379637,
  "iss": "http://spire.example.com/oidc-discovery",
  "sub": "spiffe://example.com/agent-worker",
}
```

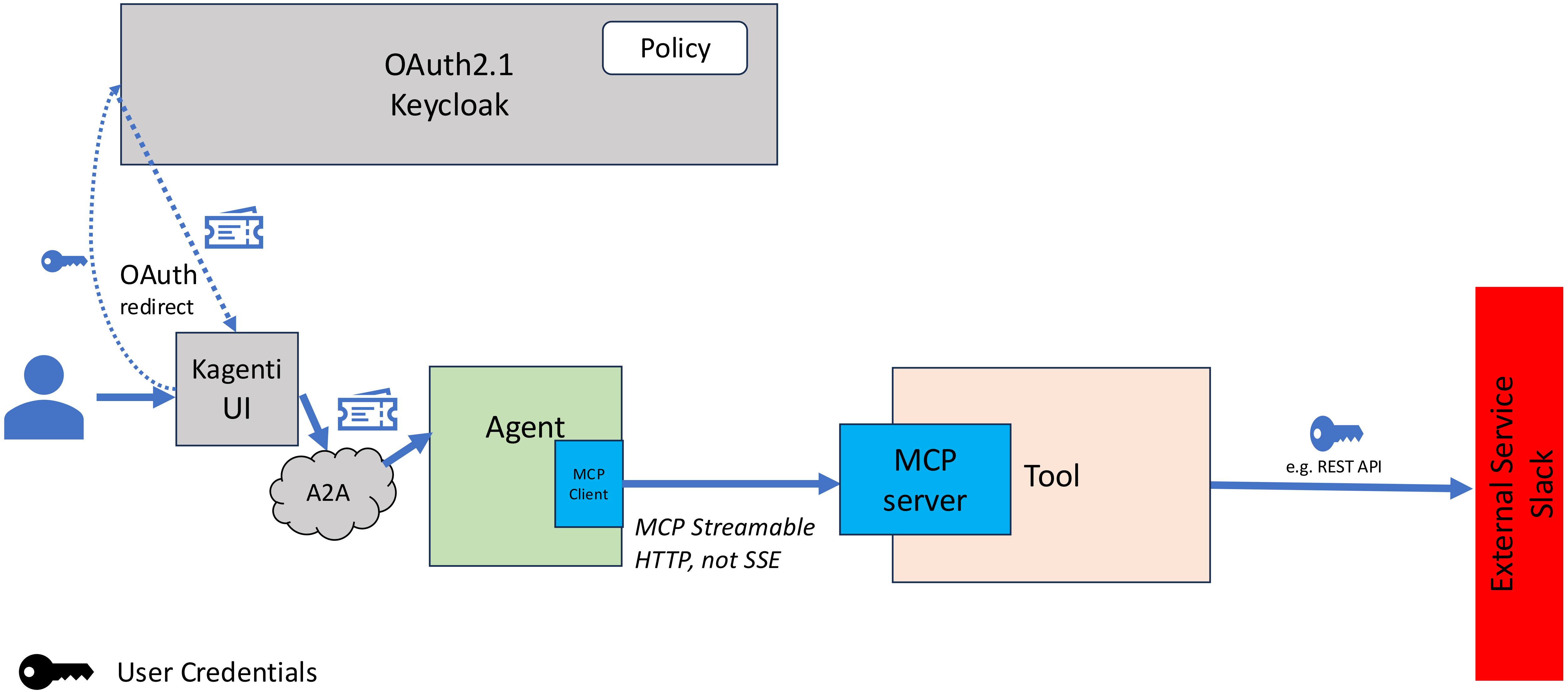
How this fits into a Kagenti platform

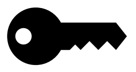
Kagenti before authn/authz



Kagenti before authn/authz

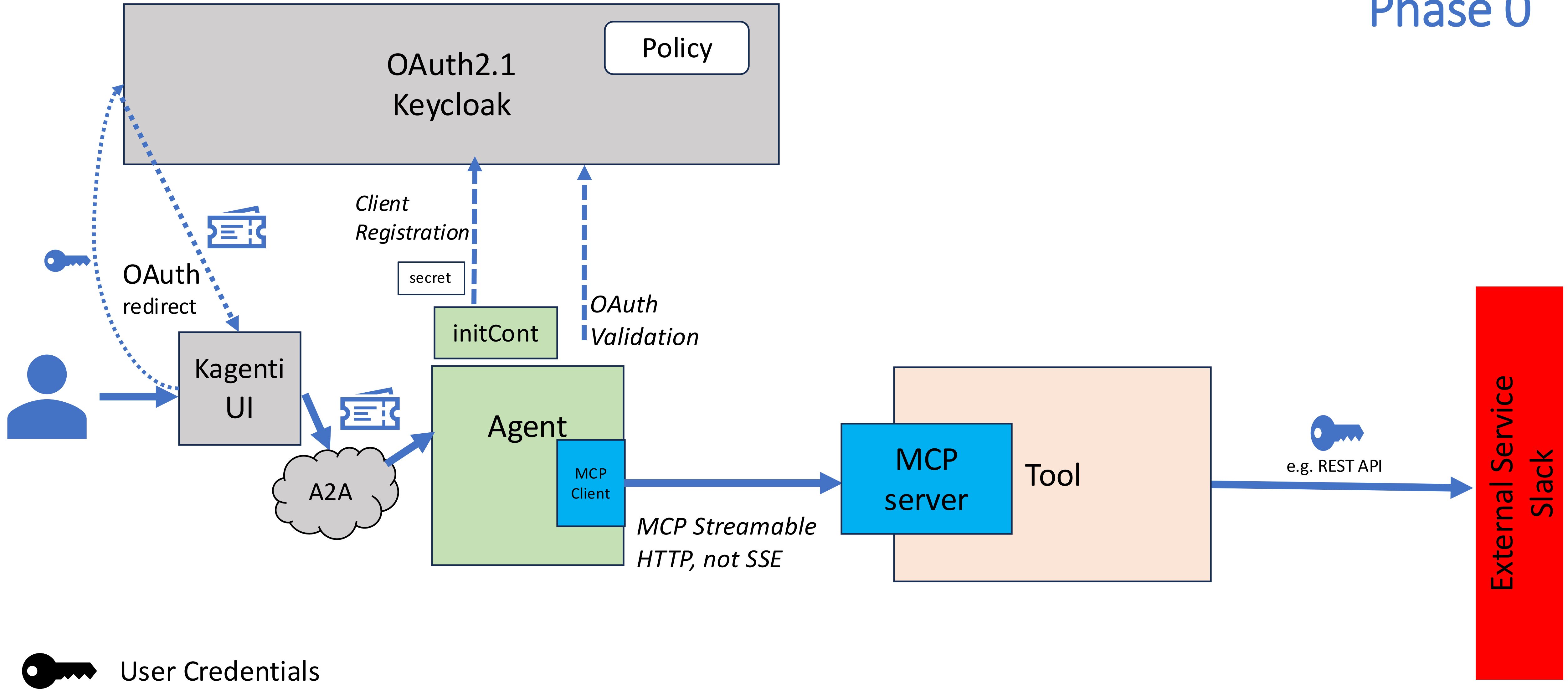




 User Credentials

Keycloak-issued JWT

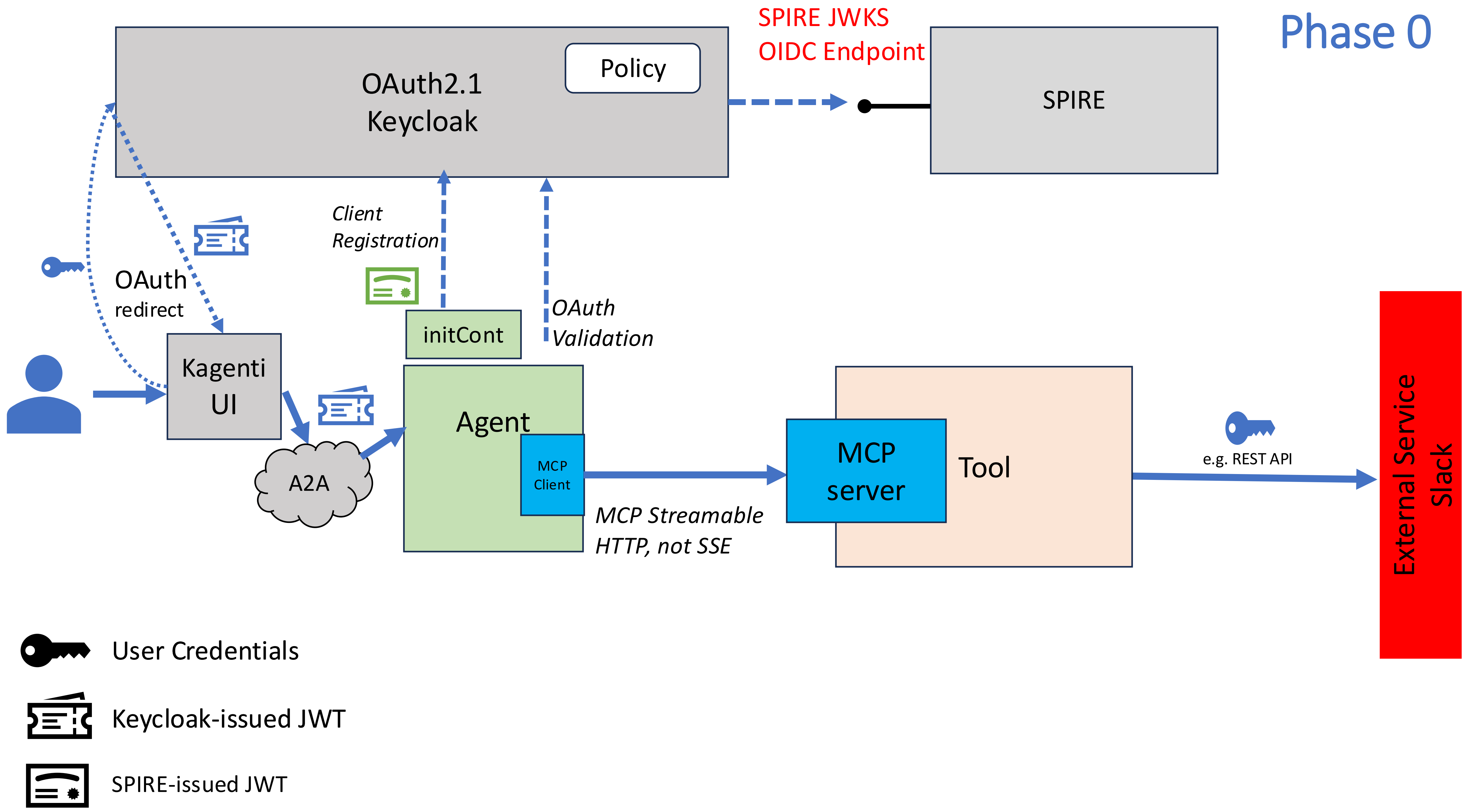
Phase 0



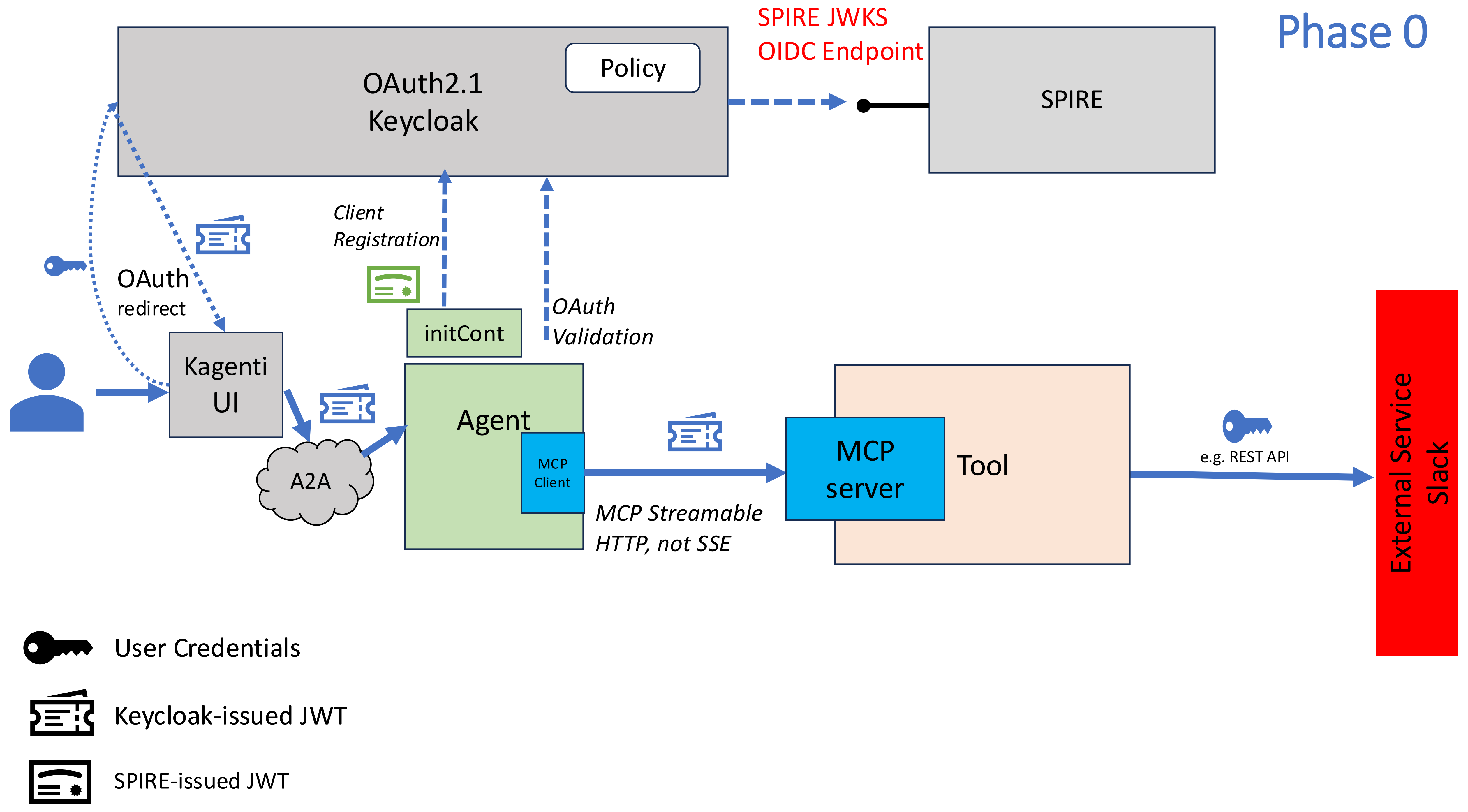
User Credentials

Keycloak-issued JWT

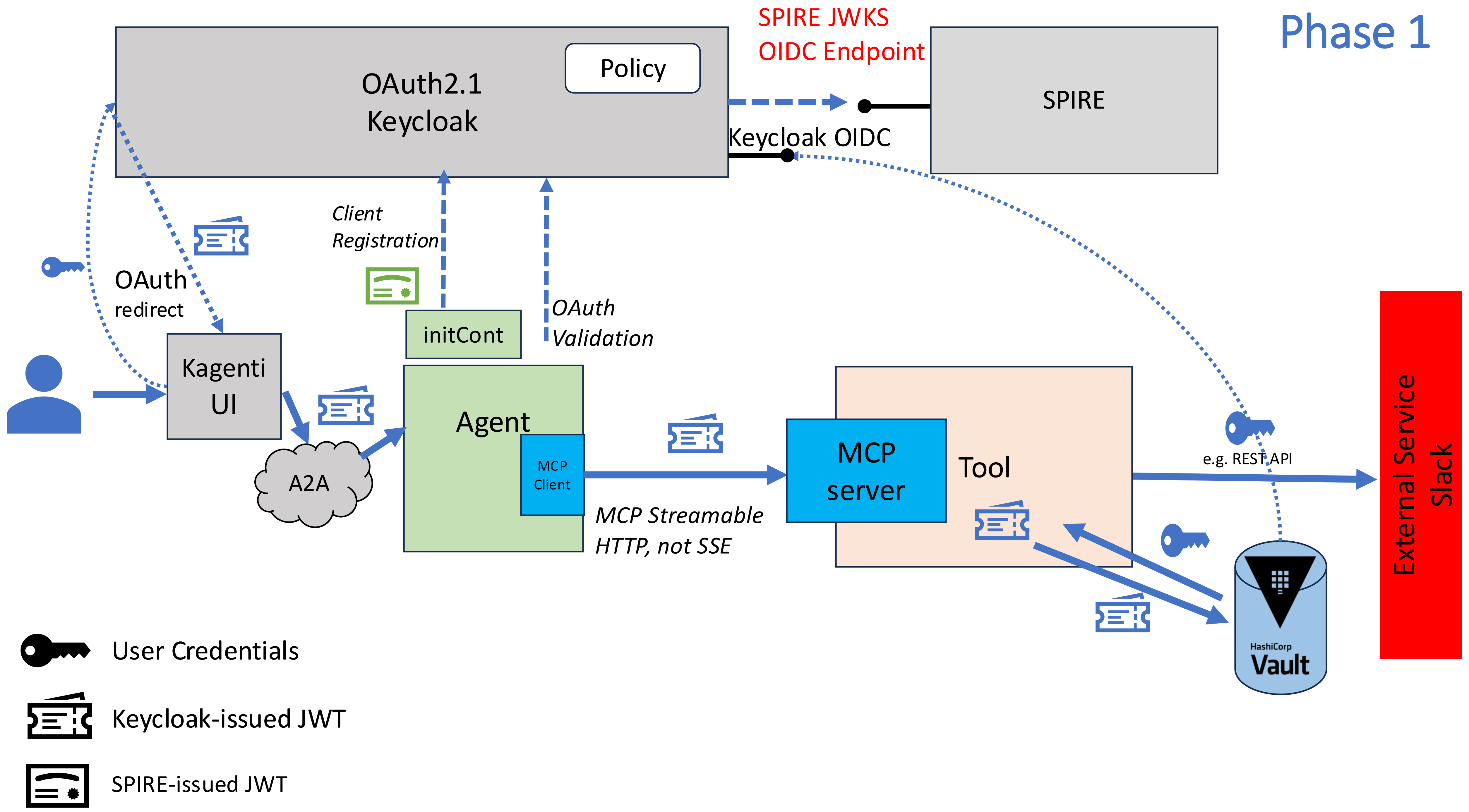
Phase 0


OAuth2.1
Keycloak
Policy
SPIRE JWKS
OIDC Endpoint
SPIRE
Client
Registration
OAuth
redirect
OAuth
Validation
initCont
Kagenti
UI
A2A
Agent
MCP
Client
MCP Streamable
HTTP, not SSE
MCP
server
Tool
e.g. REST API
External Service
Slack
User Credentials
Keycloak-issued JWT
SPIRE-issued JWT

Phase 0

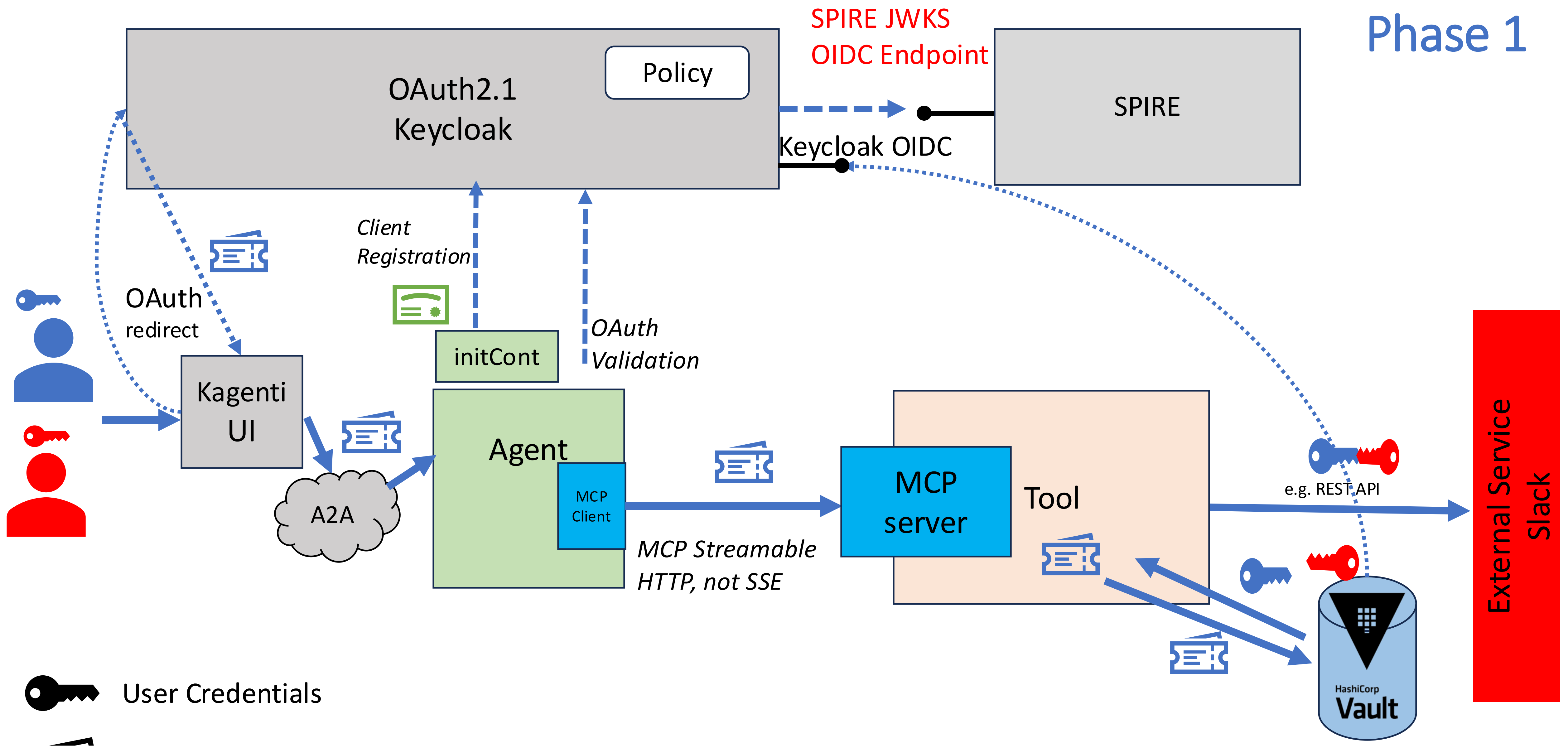

SPIRE JWKS
OIDC Endpoint
OAuth2.1
Keycloak
Policy
SPIRE
Client
Registration
OAuth
redirect
initCont
OAuth
Validation
Kagenti
UI
A2A
Agent
MCP
Client
MCP
server
Tool
MCP Streamable
HTTP, not SSE
e.g. REST API
External Service
Slack
User Credentials
Keycloak-issued JWT
SPIRE-issued JWT

Phase 1



OAuth2.1
Keycloak
Policy
SPIRE JWKS
OIDC Endpoint
SPIRE
Keycloak OIDC
Client Registration
OAuth redirect
initCont
OAuth Validation
Kagenti UI
A2A
Agent
MCP Client
MCP Streamable HTTP, not SSE
MCP server
Tool
e.g. REST API
External Service
Slack
HashiCorp Vault
User Credentials
Keycloak-issued JWT
SPIRE-issued JWT

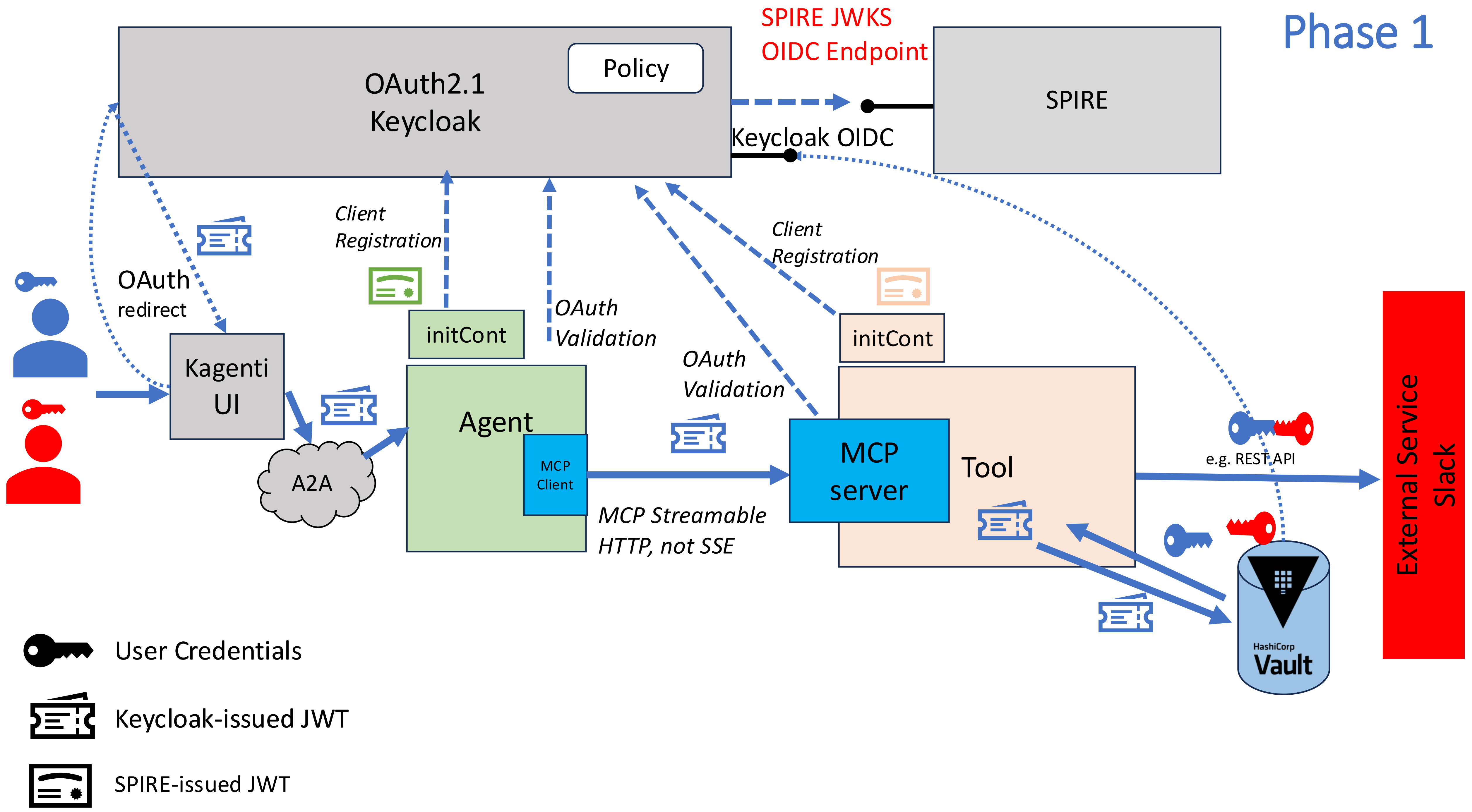
Phase 1



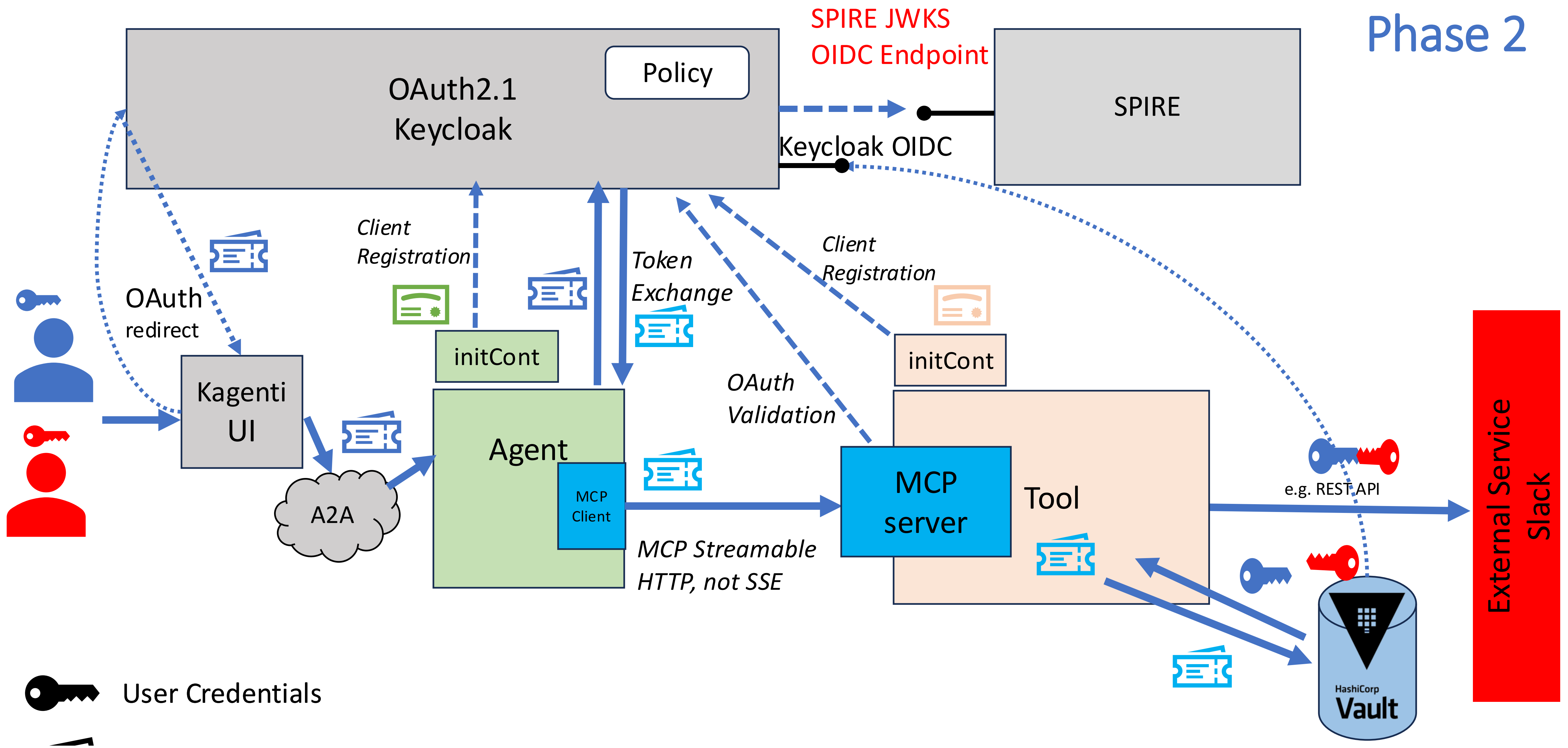
User Credentials

Keycloak-issued JWT

SPIRE-issued JWT


Phase 1
SPIRE JWKS
OIDC Endpoint
OAuth2.1
Keycloak
Policy
SPIRE
Keycloak OIDC
Client
Registration
Client
Registration
OAuth
redirect
OAuth
Validation
OAuth
Validation
initCont
initCont
Kagenti
UI
A2A
Agent
MCP
Client
MCP Streamable
HTTP, not SSE
MCP
server
Tool
e.g. REST API
External Service
Slack
HashiCorp
Vault
User Credentials
Keycloak-issued JWT
SPIRE-issued JWT

Phase 2

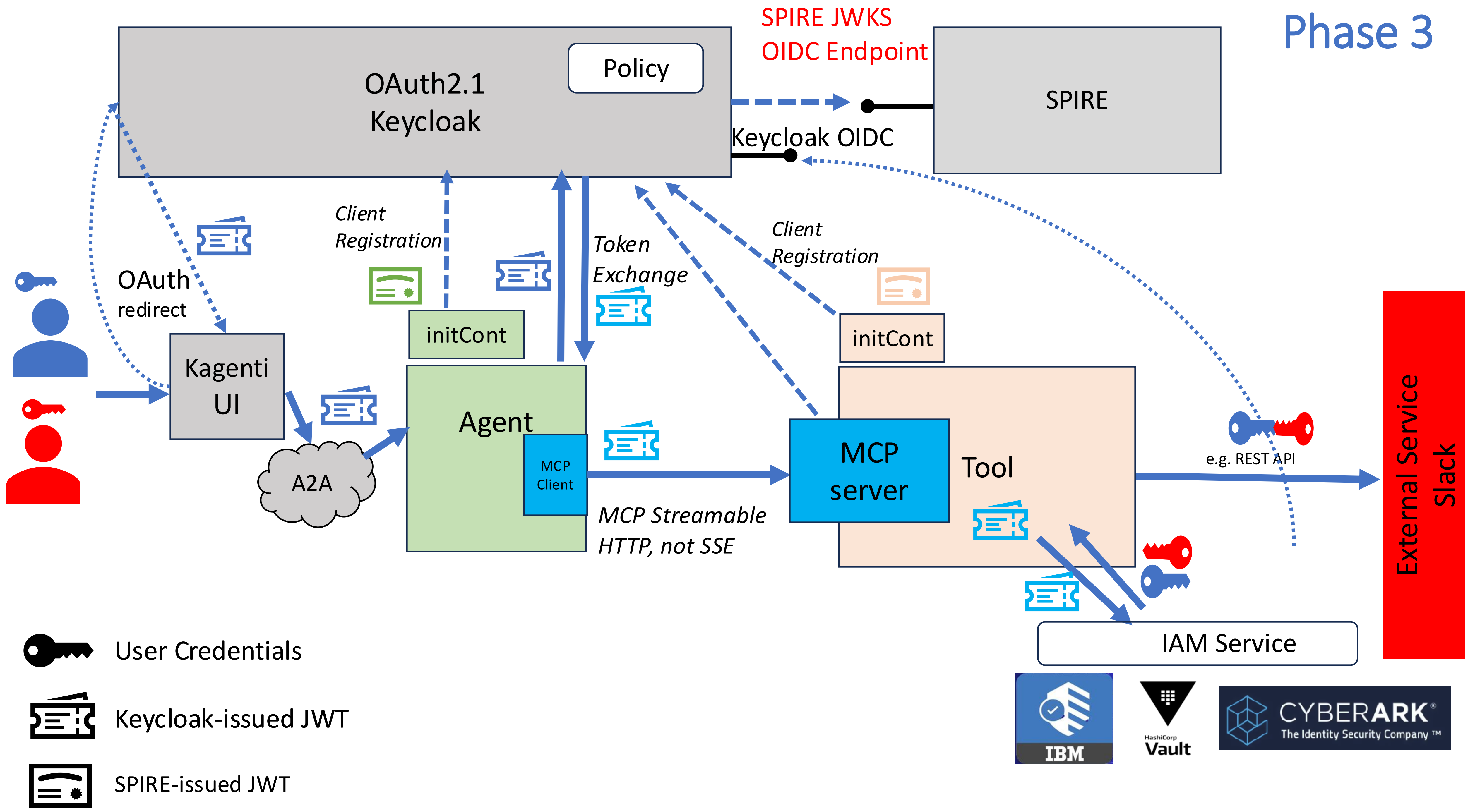


🔑 User Credentials

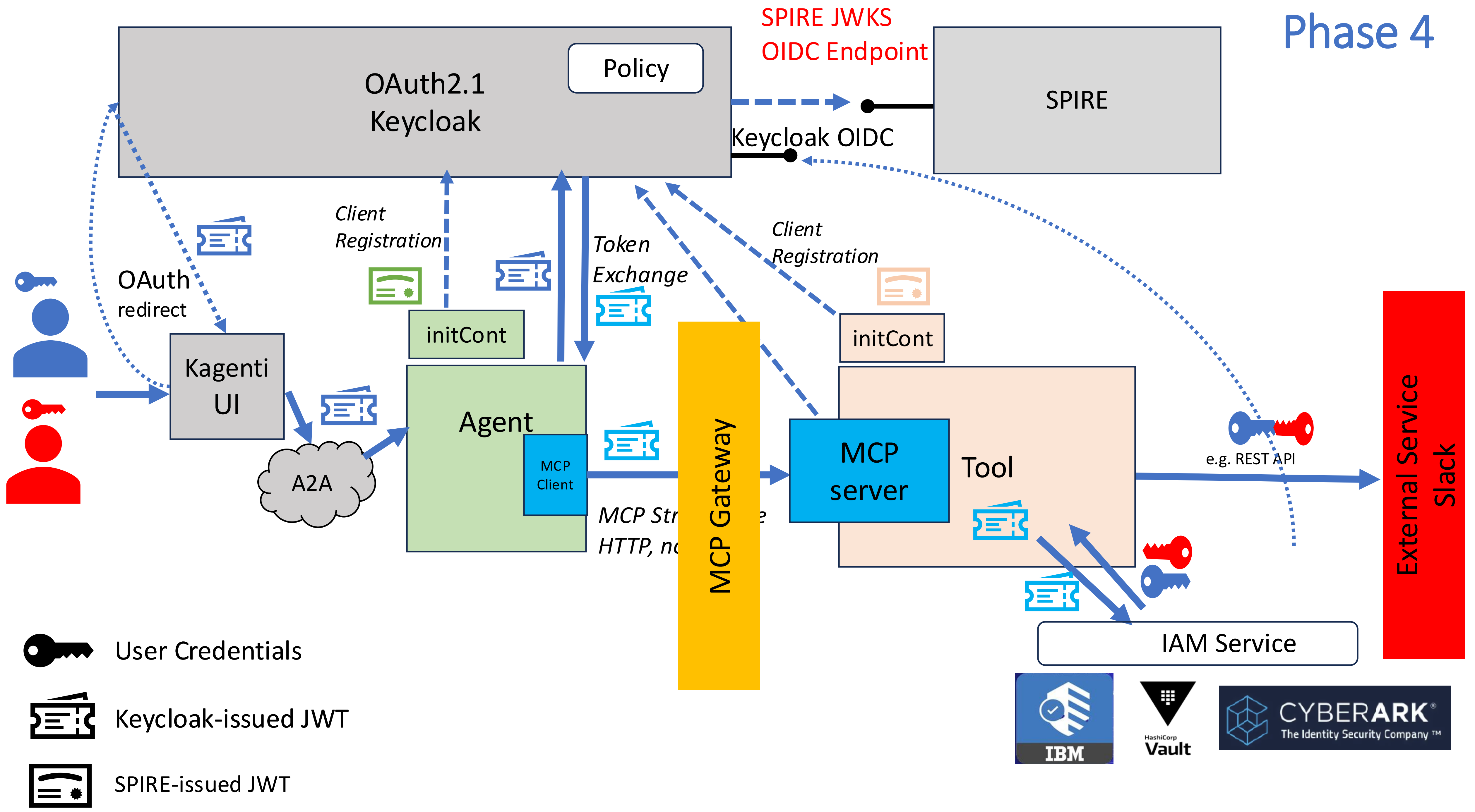
🎫 Keycloak-issued JWT

▭ SPIRE-issued JWT

Phase 3

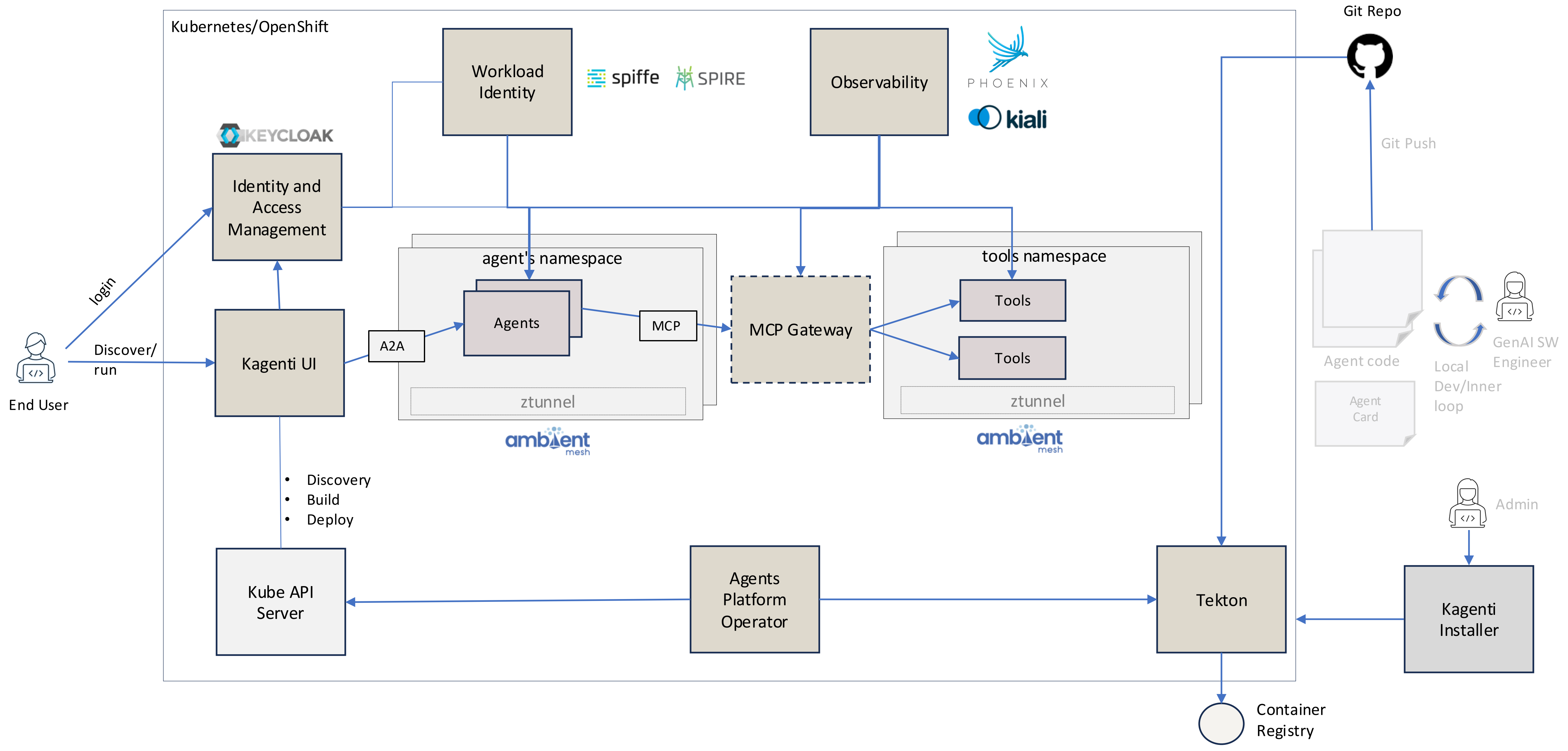

SPIRE JWKS
OIDC Endpoint
OAuth2.1
Keycloak
Policy
SPIRE
Keycloak OIDC
Client
Registration
Token
Exchange
Client
Registration
OAuth
redirect
initCont
initCont
Kagenti
UI
Agent
MCP
Client
A2A
MCP
server
Tool
MCP Streamable
HTTP, not SSE
e.g. REST API
External Service
Slack
IAM Service
IBM
HashiCorp
Vault
CYBERARK
The Identity Security Company ™
User Credentials
Keycloak-issued JWT
SPIRE-issued JWT

Phase 4



SPIRE JWKS
OIDC Endpoint
OAuth2.1
Keycloak
Policy
SPIRE
Keycloak OIDC
Client
Registration
Token
Exchange
Client
Registration
OAuth
redirect
initCont
initCont
Kagenti
UI
A2A
Agent
MCP
Client
MCP Gateway
MCP Str
HTTP, no
MCP
server
Tool
e.g. REST API
External Service
Slack
IAM Service
IBM
HashiCorp
Vault
CYBERARK
The Identity Security Company
User Credentials
Keycloak-issued JWT
SPIRE-issued JWT

Kagenti – Putting it all together


Kubernetes/OpenShift
Workload Identity
spiffe
SPIRE
Observability
PHOENIX
kiali
KEYCLOAK
Identity and Access Management
agent's namespace
Agents
A2A
MCP
ztunnel
ambient mesh
MCP Gateway
tools namespace
Tools
Tools
ztunnel
ambient mesh
login
Discover/ run
End User
Kagenti UI
Discovery
Build
Deploy
Kube API Server
Agents Platform Operator
Tekton
Git Repo
Git Push
Agent code
Agent Card
Local Dev/Inner loop
GenAI SW Engineer
Admin
Kagenti Installer
Container Registry