



Airlock Partner Tech Community Training

Episode 5 – October 2025

Token Exchange



OAuth2 & OpenID Connect (OIDC)

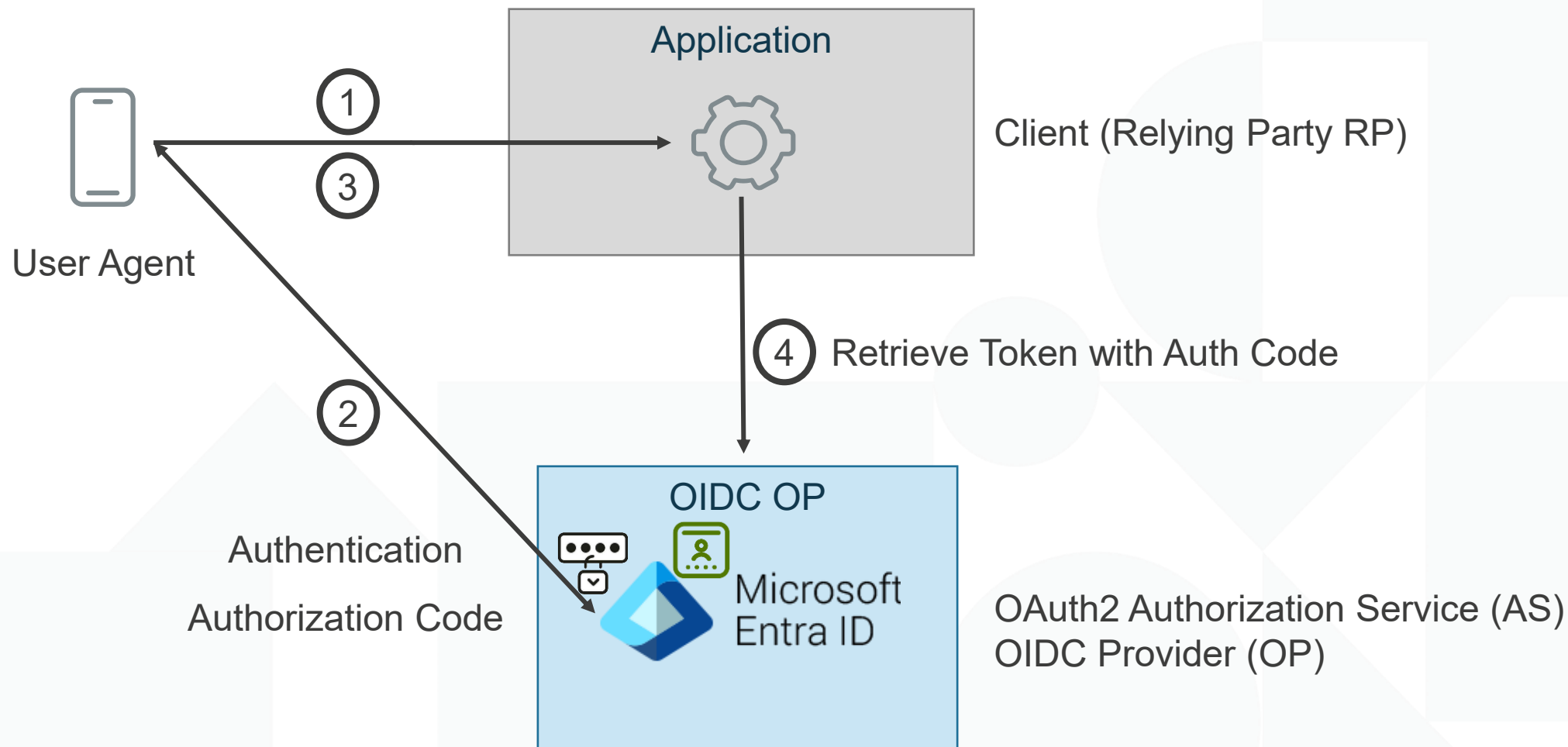
- Avoid situations where many applications learn a user's credentials (because most users tend to re-use the same username & password).
- Clear separation of concerns between
 - Authenticator
 - Access Controller
- Centralise users and their credentials
- Replace credentials with tokens for applications
 - Individual per user
 - Valid only for one session
 - Issuer verifiable
 - Can transport additional user information



It Is Time For Marketing

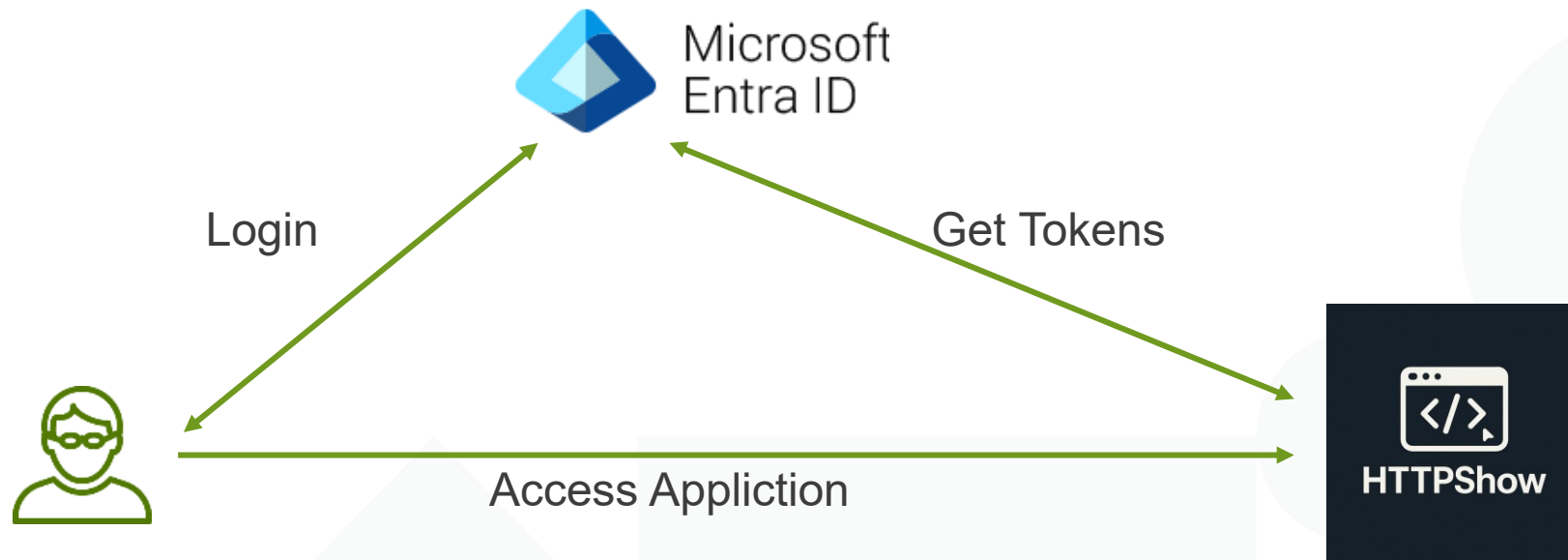
- Focus on security – with good results.
- Privacy not so great
 - Requires less trust in application providers
 - Requires **big** trust in central OAuth2 and OIDC providers
- We will address this in one of the next episodes of Tech Community Training (think SSI/DCI)

Recap

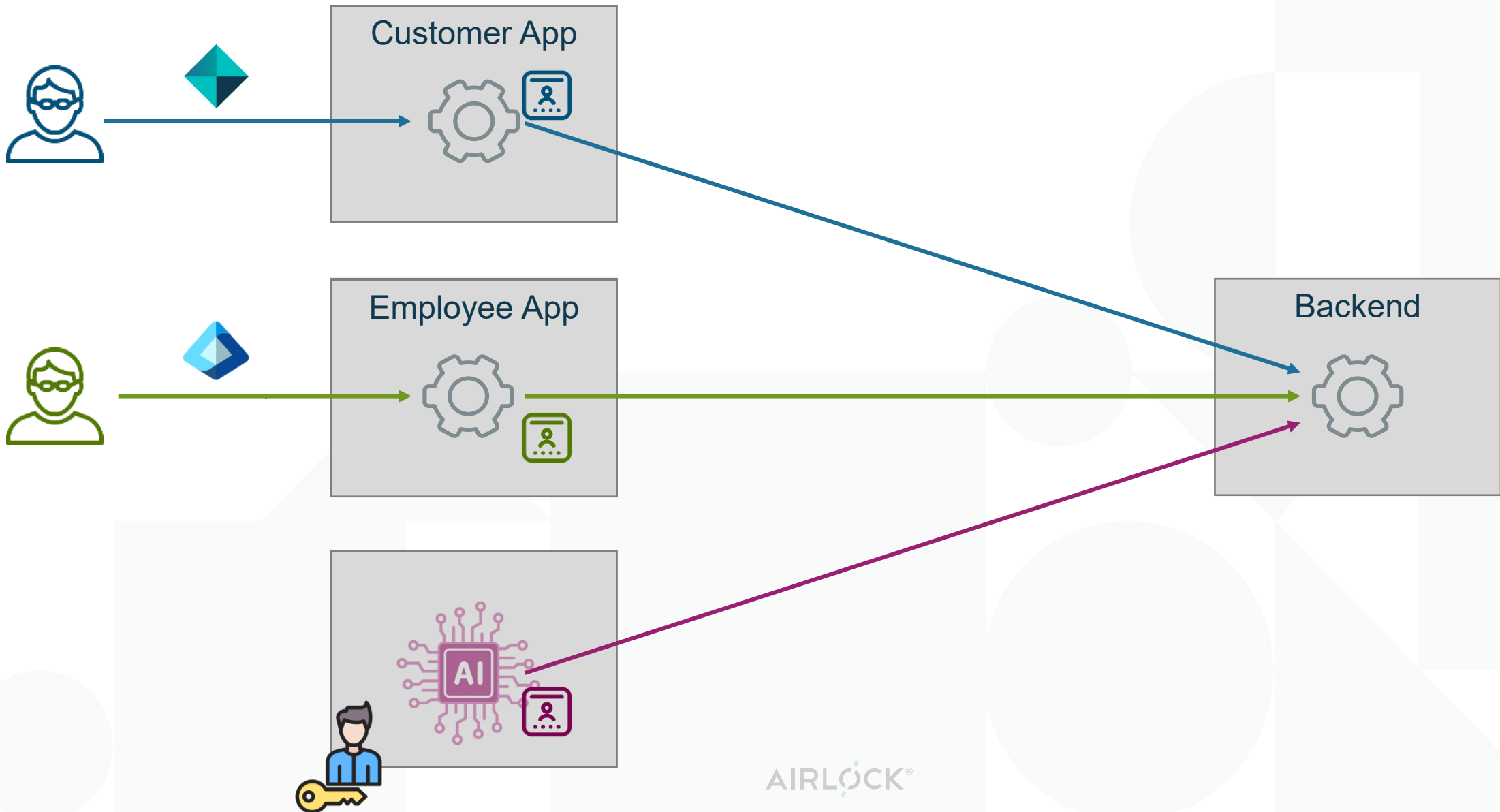




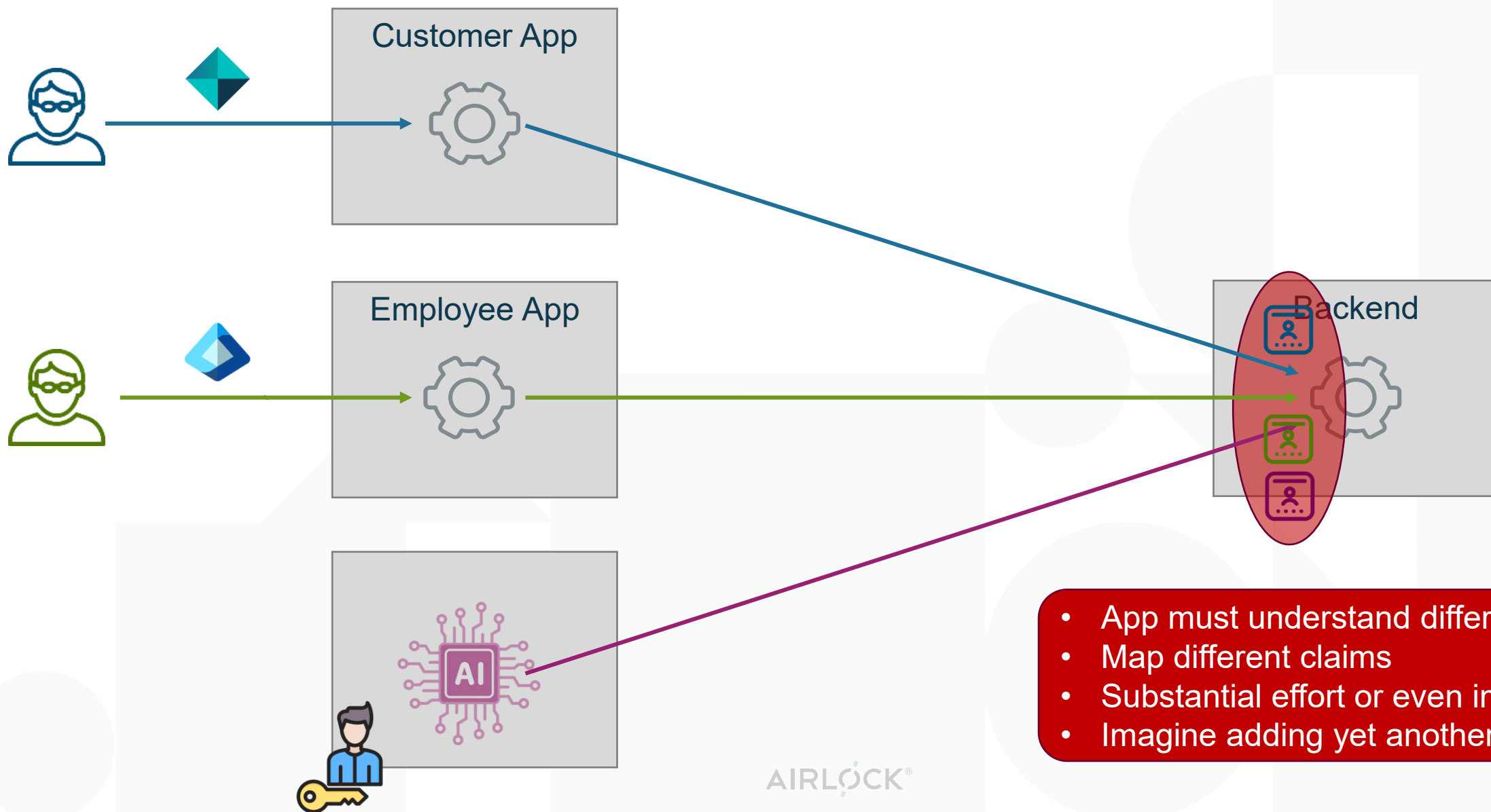
Demo 1: Setup



Scenario 1: Adding Some Fun

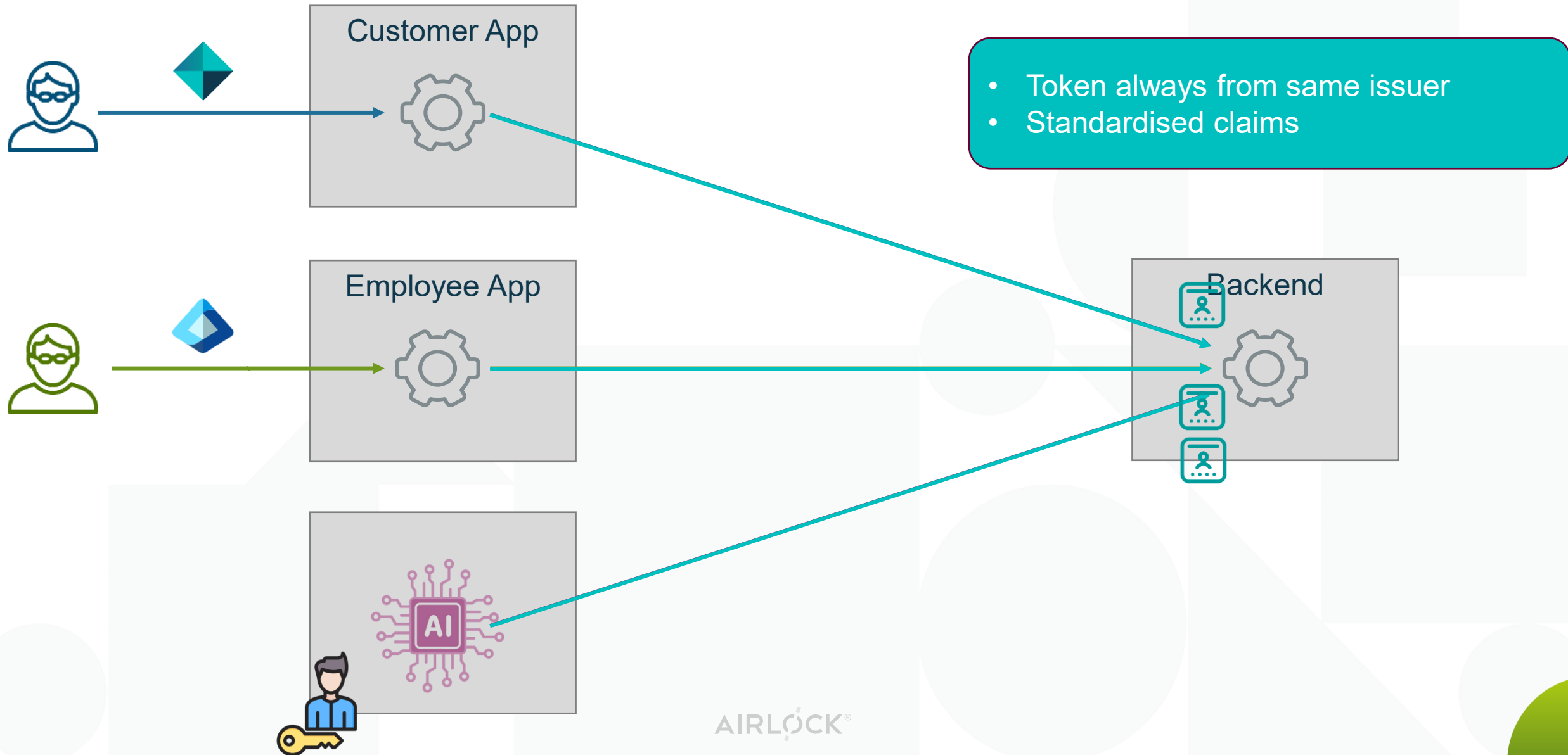


Scenario 1: Adding Some Fun



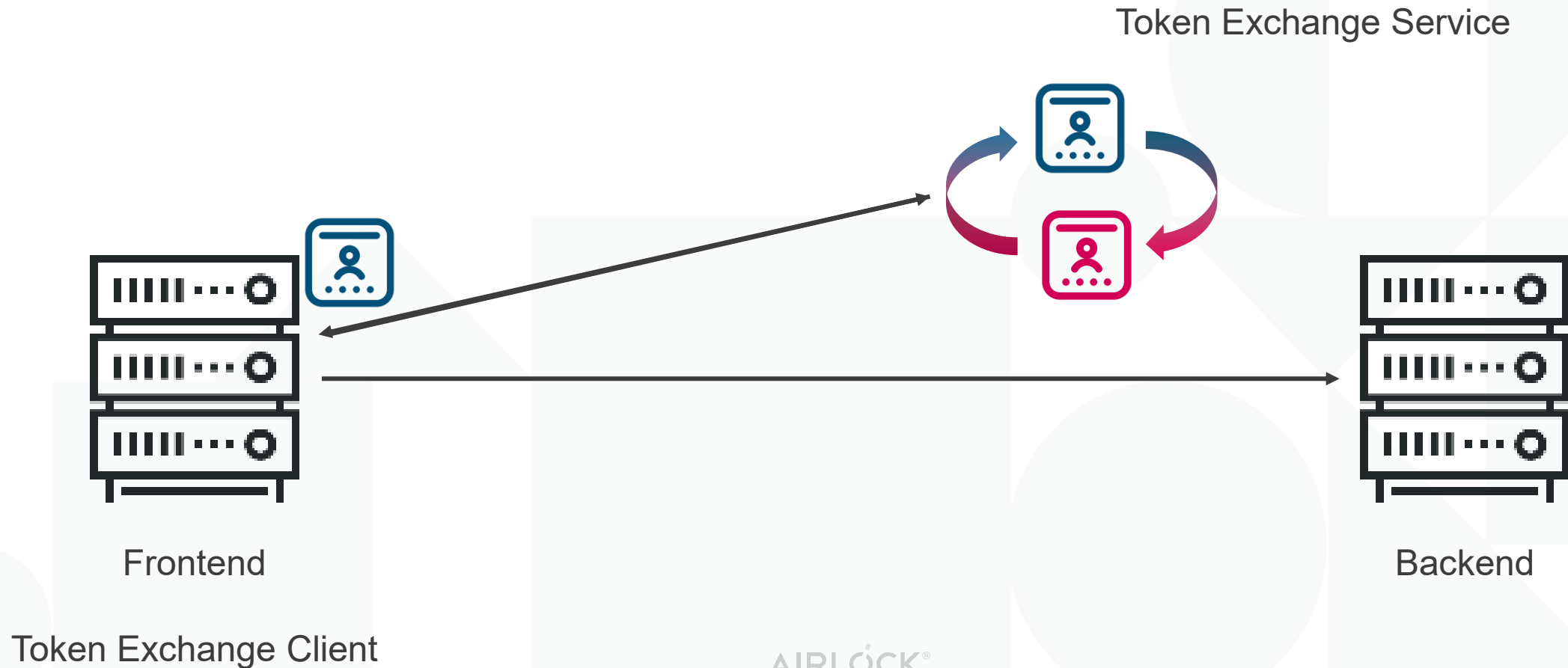
- App must understand different tokens
- Map different claims
- Substantial effort or even impossible
- Imagine adding yet another system

Scenario 1: Token Harmonisation

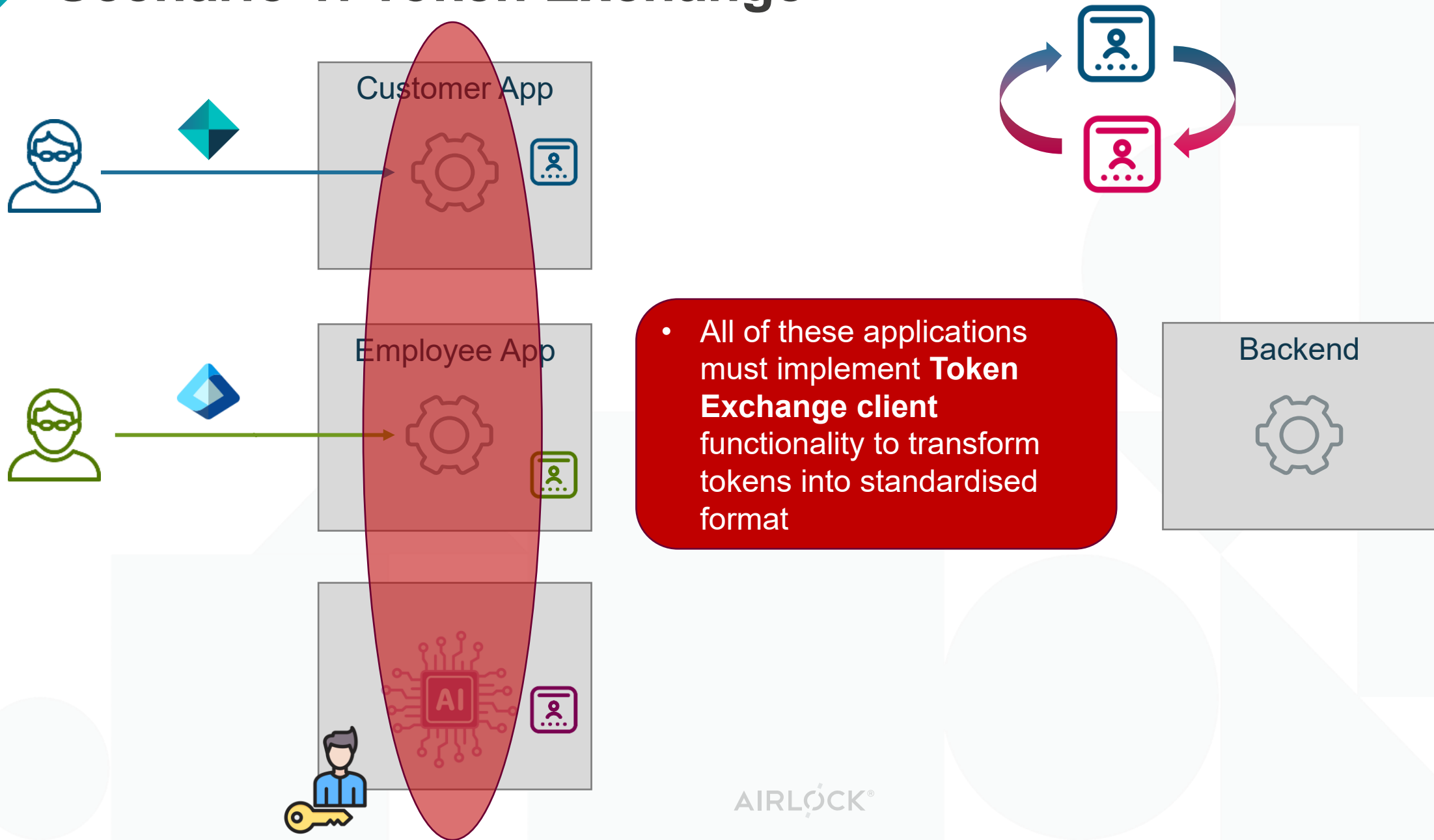


Scenario 1: Token Exchange

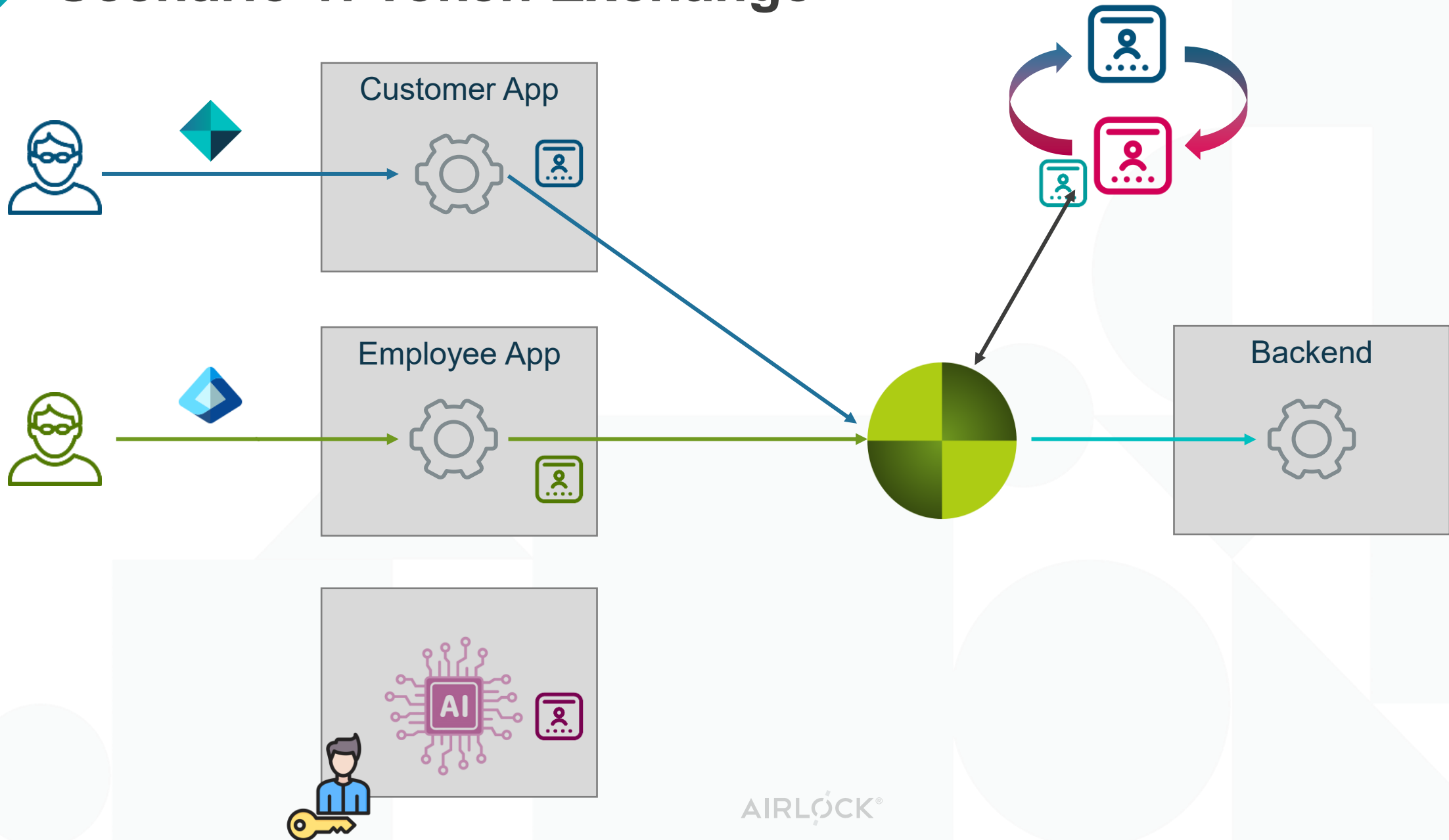
- RFC 8693: OAuth2 Token Exchange



Scenario 1: Token Exchange

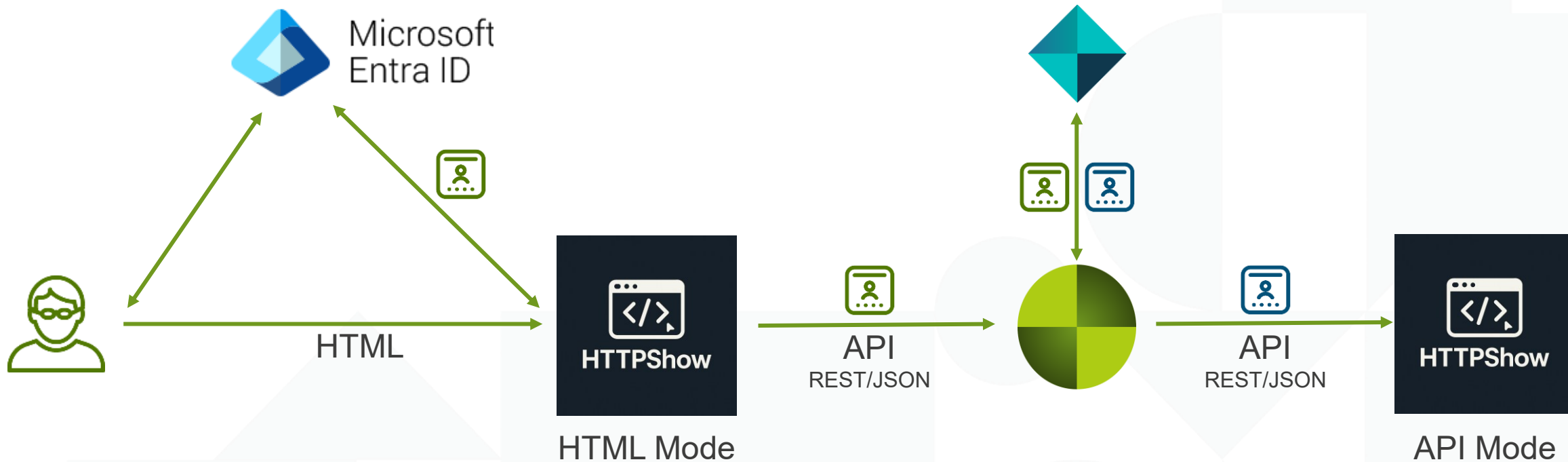


Scenario 1: Token Exchange





Demo 2: Setup



Solution 1 – Airlock Microgateway

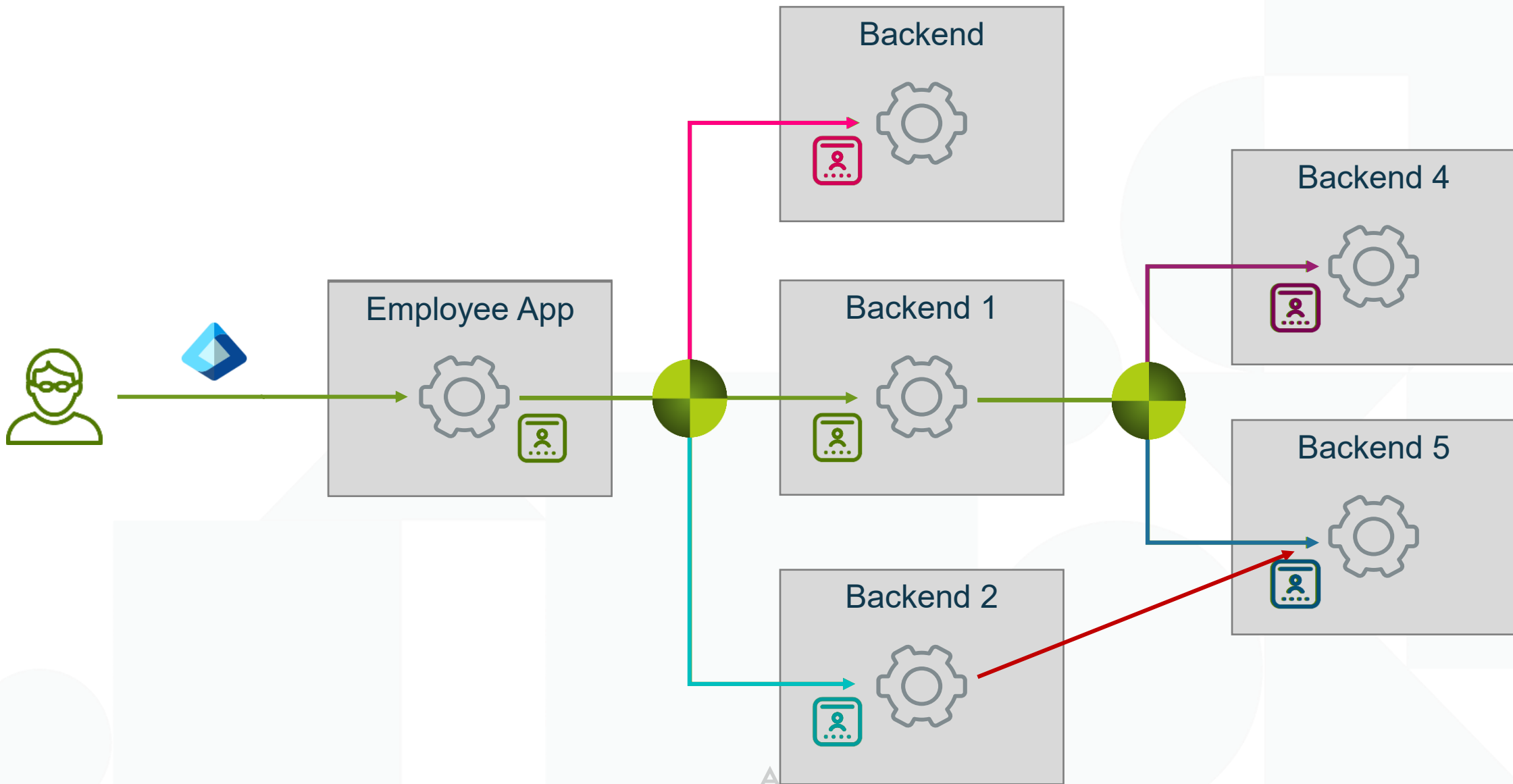


Token Exchange Client

- Upfront
- Transparent to application
- Application simply gets the correct token
- Application doesn't need to understand tokens
—► Identity Propagation with claims from token

- Benefits
 - Clean architecture
 - Simplified configuration, debugging, operations
 - Increased speed for time-to-market
 - Reduced cost

Scenario 2: Fight The Almighty



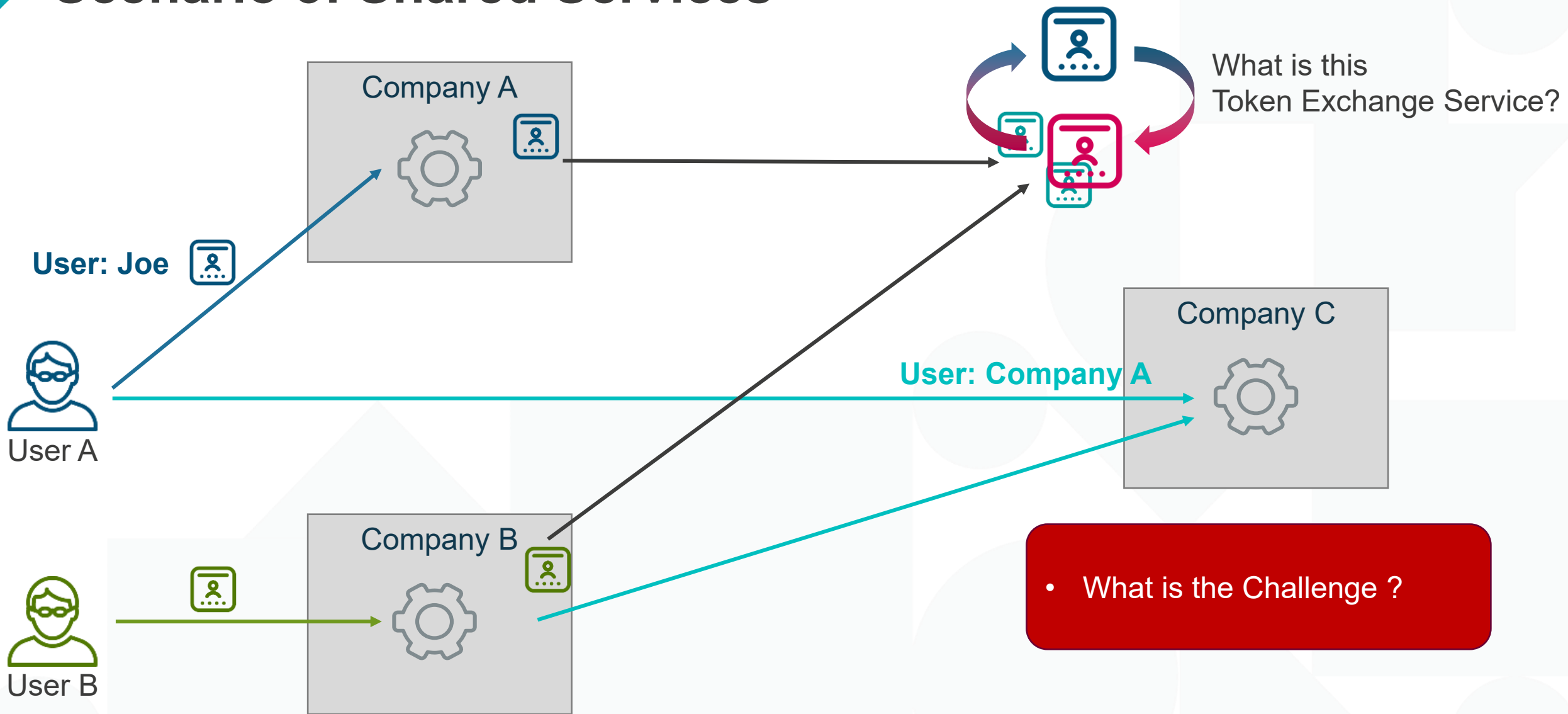
Solution 2 – No Almighty Token



Token Exchange Client

- Each Service has its own dedicated token
- Rogue services cannot access other services because they lack the correct token
- Benefits
 - Improved security
 - Clear separation of concerns
 - Well-known access patterns
 - Less debugging

Scenario 3: Shared Services



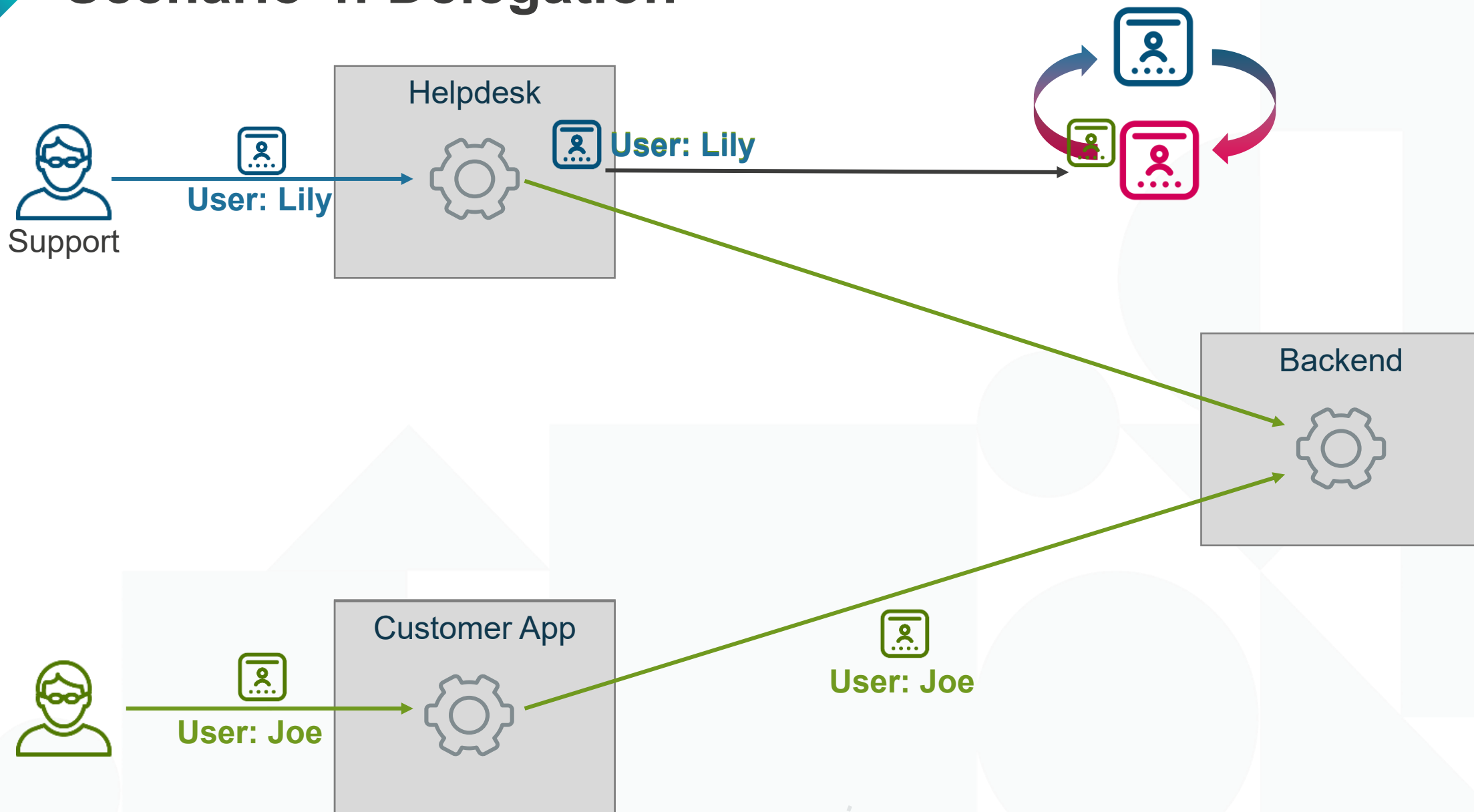
Solution 3 – Airlock IAM



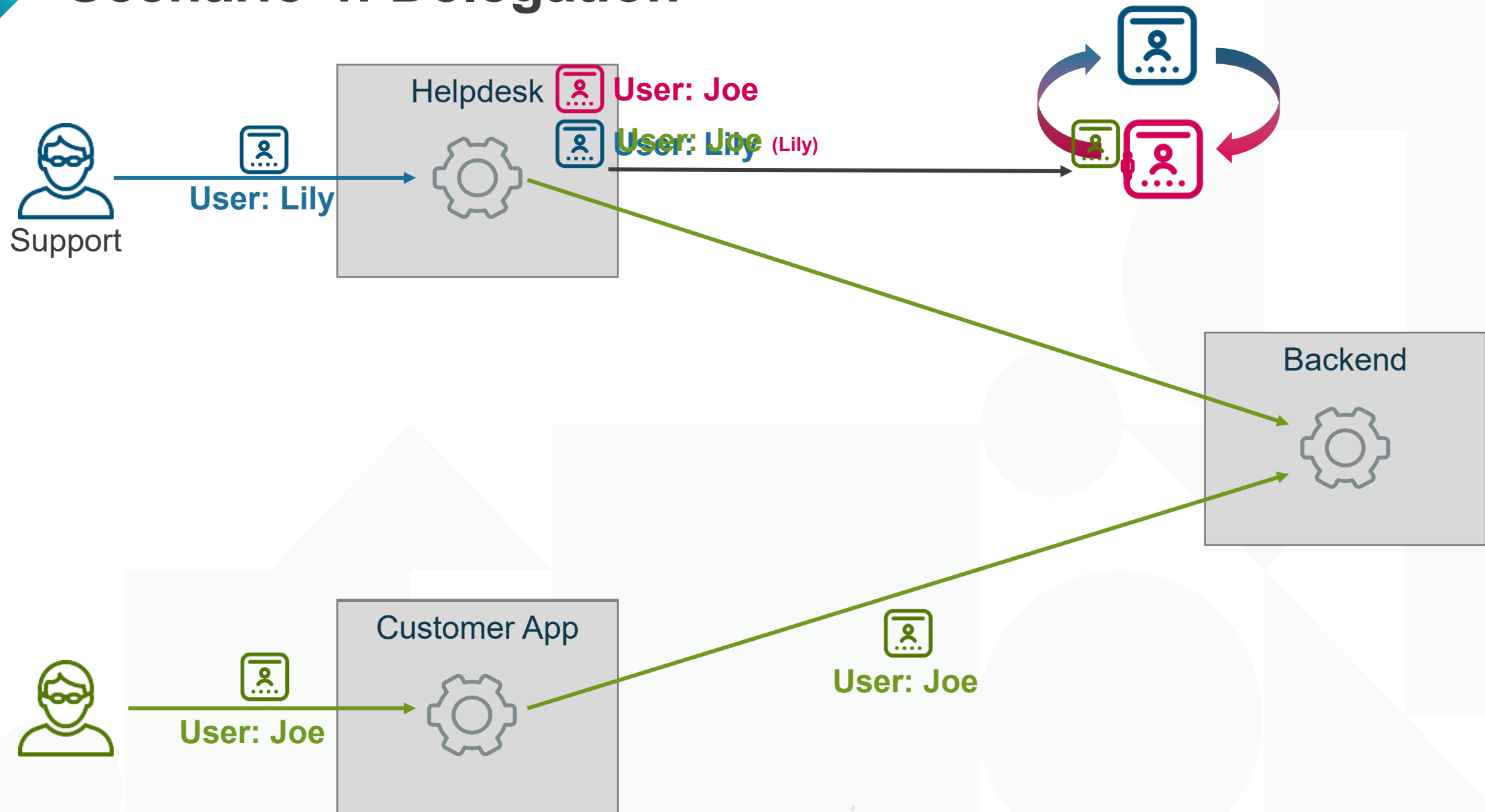
Token Exchange Service

- Rule-based conversion from one token to another
- Not very many systems do it correctly
- Things to look out for
 - Exchange tokens from 3rd-party issuers
 - Introspect source token
 - Impersonation & Delegation
- Benefits
 - Enables new business cases
 - Extended functionality

Scenario 4: Delegation



Scenario 4: Delegation





The Solution – Airlock IAM and Airlock Microgateway



Token Exchange Service



Token Exchange Client

**If You Think
Tokens
Think Airlock**

Airlock

Sie haben Fragen zu unseren Produkten oder wünschen ein Onlinedemo des Airlock Secure Access Hub?

Einfach anrufen **+41 44 268 87 00**

