ThoughtWorks®

Xi’an Security Day

从ADFS说起

王浩　*hdwang@thoughtworks.com*

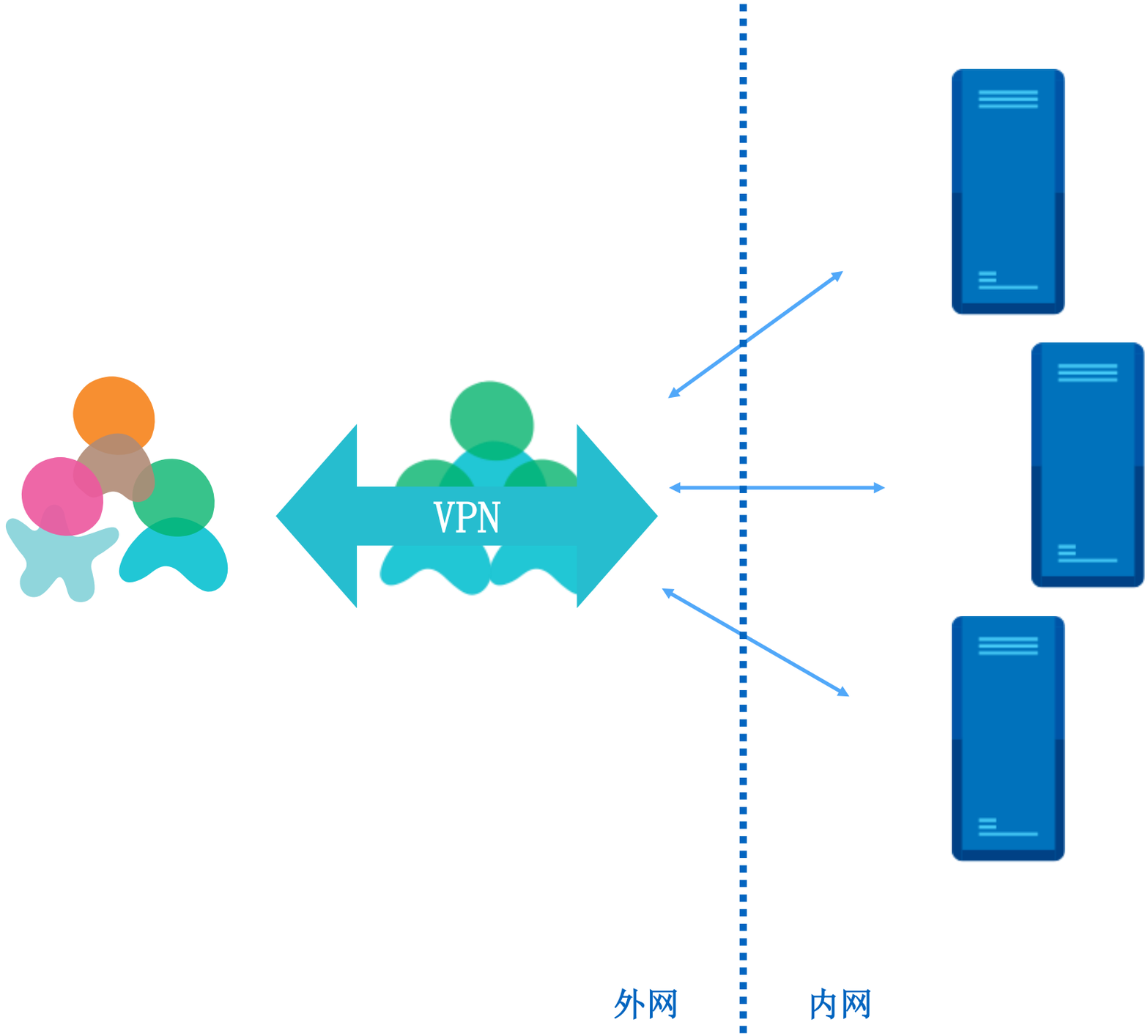
Active Directory Federation Services

活动目录联合服务

ThoughtWorks®

现代系统架构，业务场景带来的身份认证难题

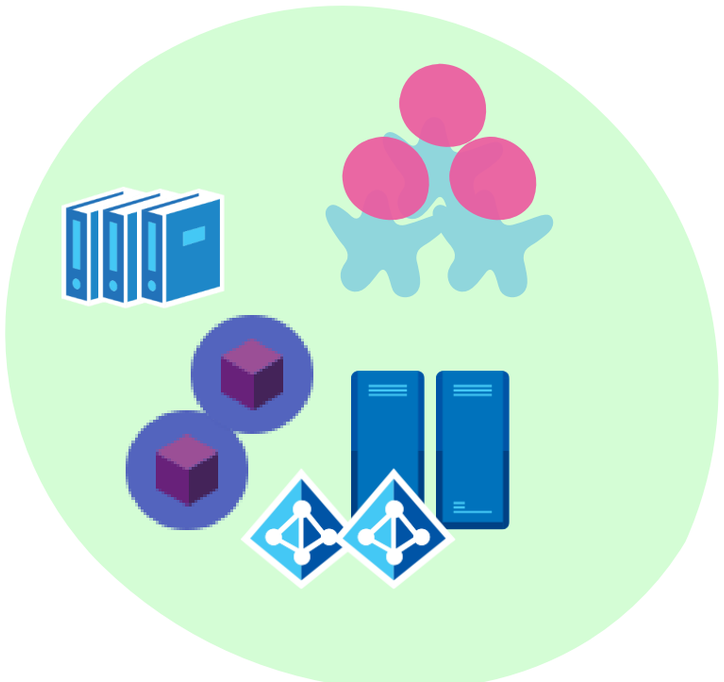
本地环境



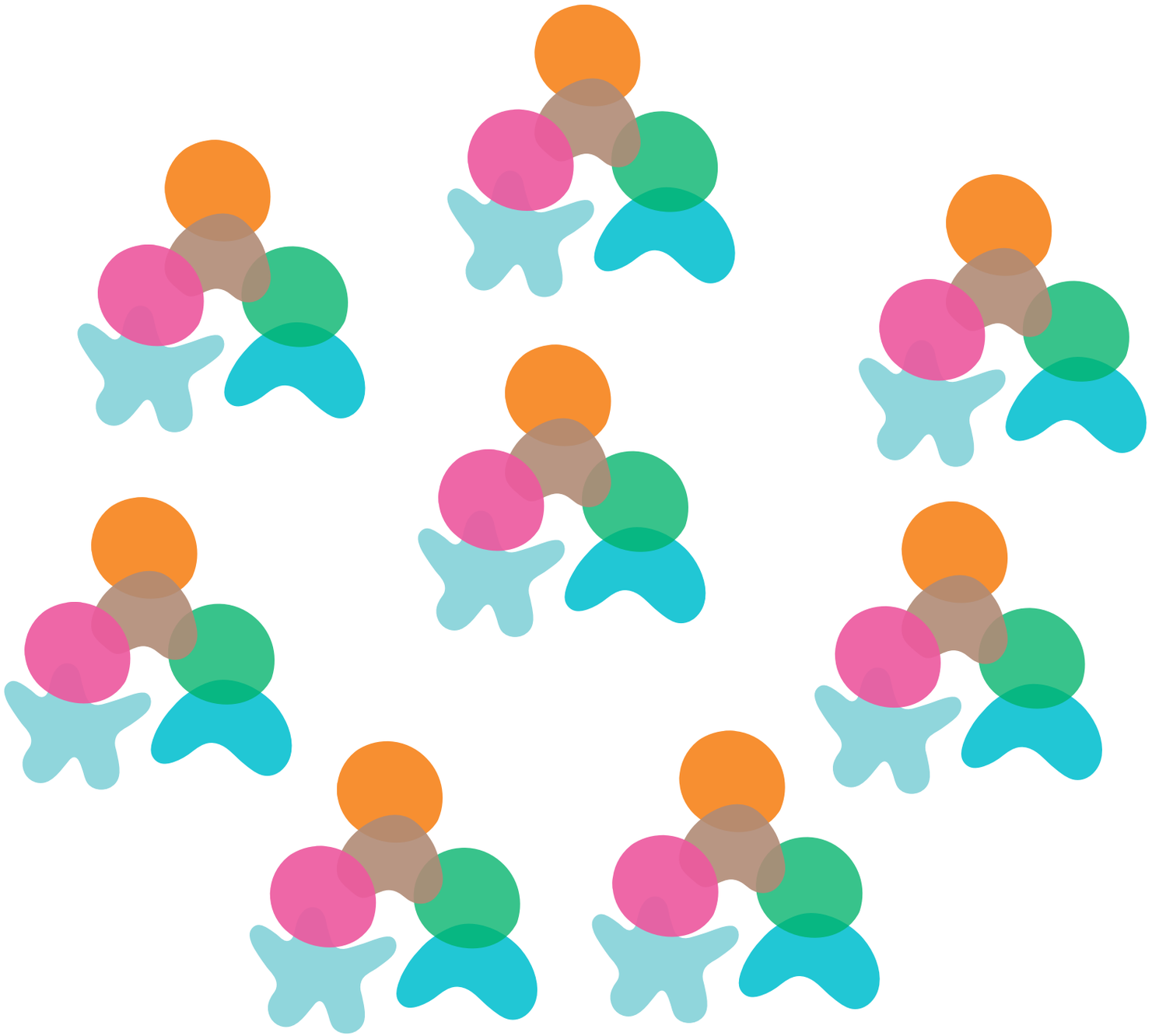
云


Microsoft Dynamics
Office 365
salesforce.com
SAP
System Center
HIGHTAIL
amazon web services
GoToMeeting
box
Microsoft Azure

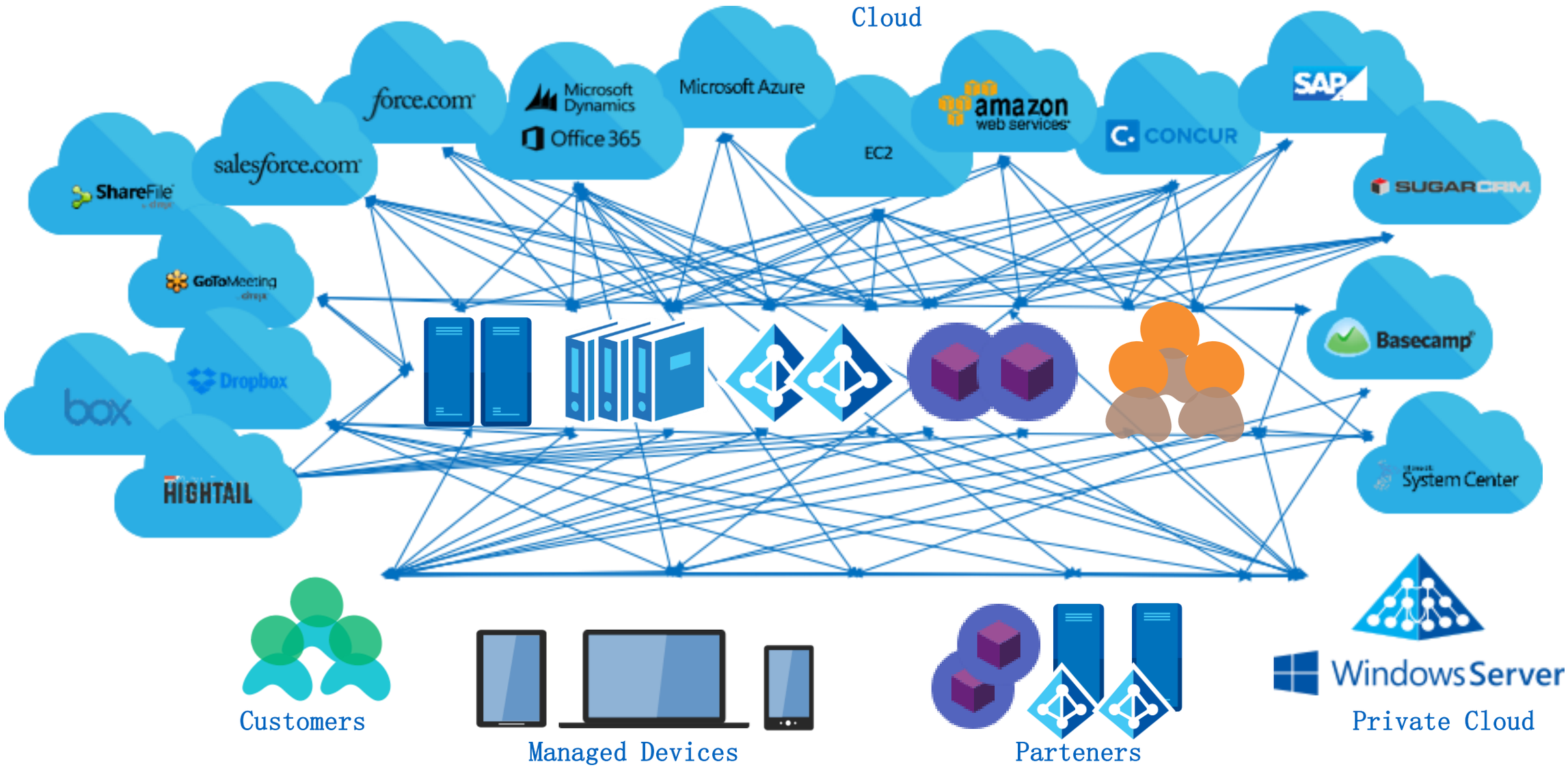
合作伙伴



用户

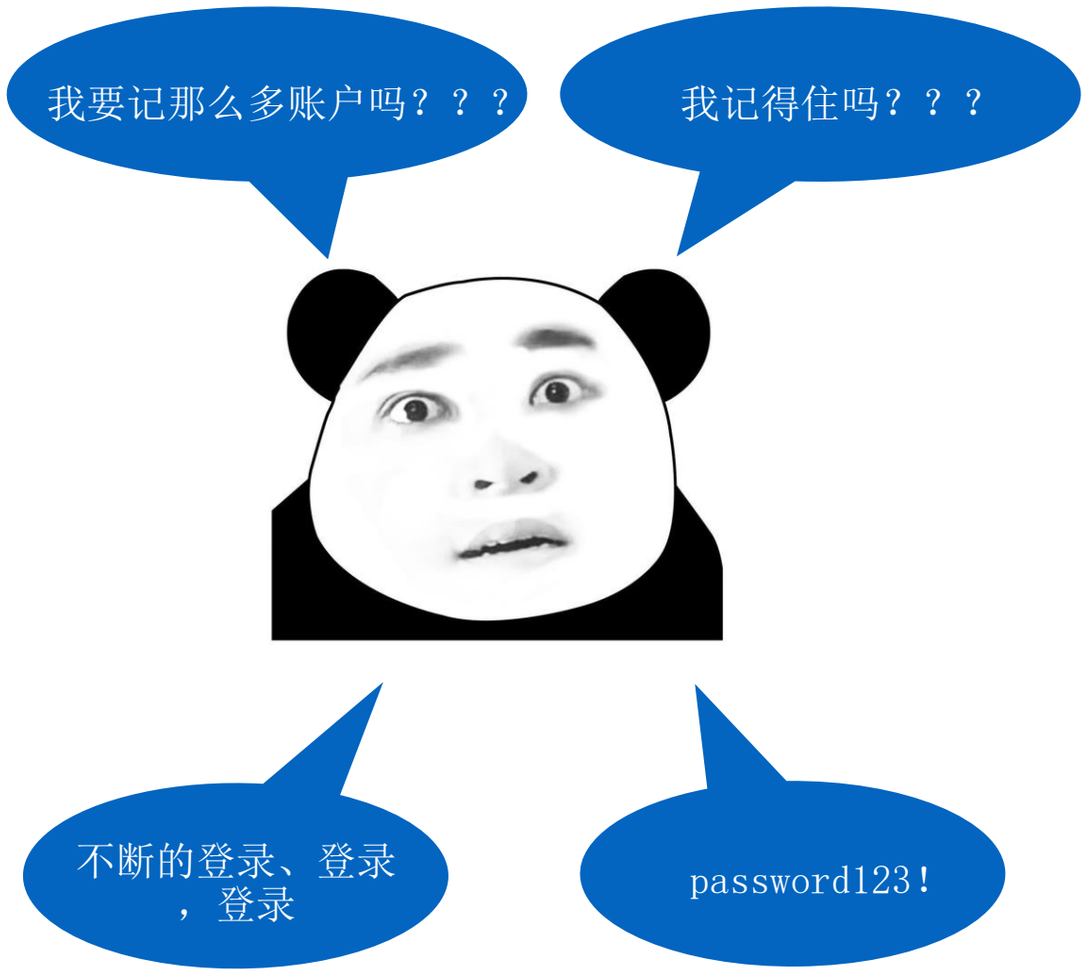


现实情况


Cloud
force.com
Microsoft Dynamics
Office 365
Microsoft Azure
EC2
amazon web services
CONCUR
SAP
salesforce.com
ShareFile
SUGARCRM
GoToMeeting
Basecamp
box
Dropbox
HIGHTAIL
System Center
Customers
Managed Devices
Parteners
Windows Server
Private Cloud

挑战


不断创建账户
复杂角色权限管理
定期清理无效账户
频繁的密码重置请求
我要辞职
用户使用弱密码


我要记那么多账户吗？？？
我记得住吗？？？
不断的登录、登录，登录
password123!

答案

- 建立一个认证框架可以被所有应用消费，无需关注应用部署在哪里
- Identity Token 可以携带更多的用户信息
- 通过信任的合作伙伴去认证他们的用户
- 基于工业化的标准协议
- 同时支持在浏览器和Web Service

联合认证 Federation Identity

- Okta
- OpenAM
- Active Directory Federation Services

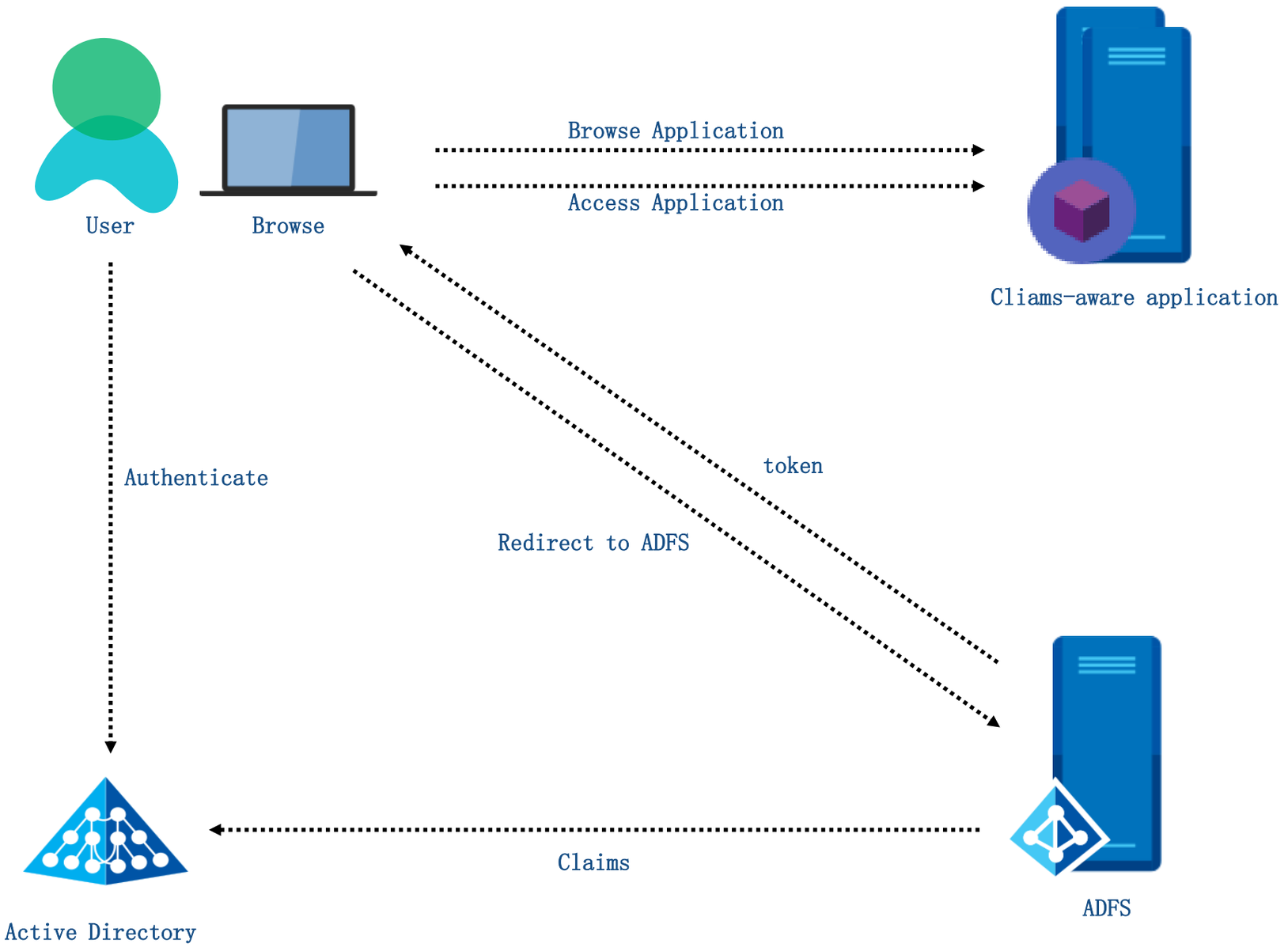
ADFS版本

- ADFS
  - ADFS 1.0 - Windows Server 2003 R2
  - ADFS 1.1 - Windows Server 2008 and Windows Server 2008 R2
  - ADFS 2.0 - Windows Server 2008 and Windows Server 2008 R2
  - ADFS 2.1 - Windows Server 2012
  - ADFS 3.0 - Windows Server 2012 R2
  - ADFS4.0 - Windows Server 2016
- Azure AD

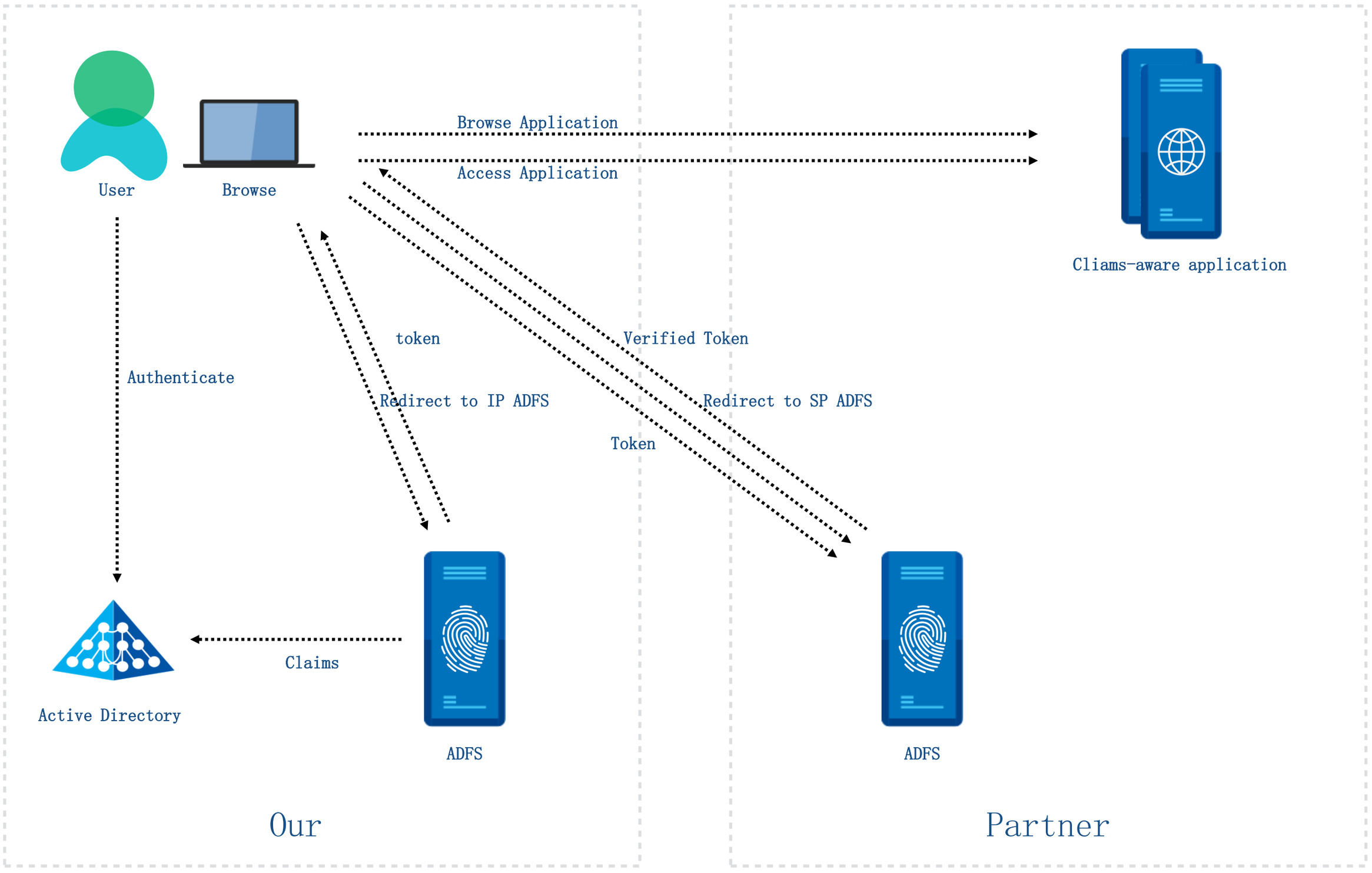
ThoughtWorks®

ADFS

关键概念

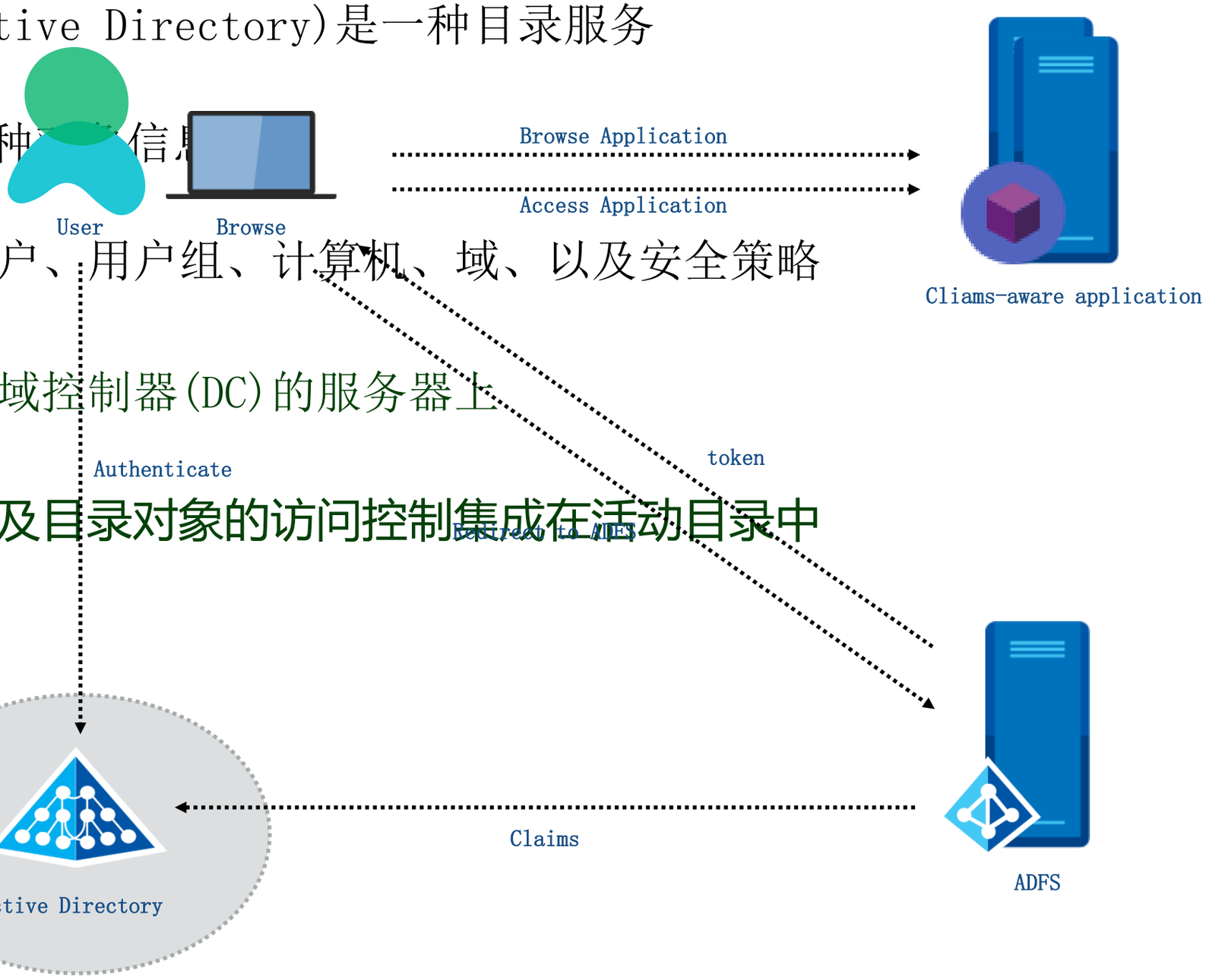

User
Browse
Browse Application
Access Application
Cliams-aware application
Authenticate
token
Redirect to ADFS
Active Directory
Claims
ADFS

关键概念


User
Browse
Browse Application
Access Application
Cliams-aware application
Authenticate
token
Verified Token
Redirect to IP ADFS
Redirect to SP ADFS
Token
Active Directory
Claims
ADFS
ADFS
Our
Partner

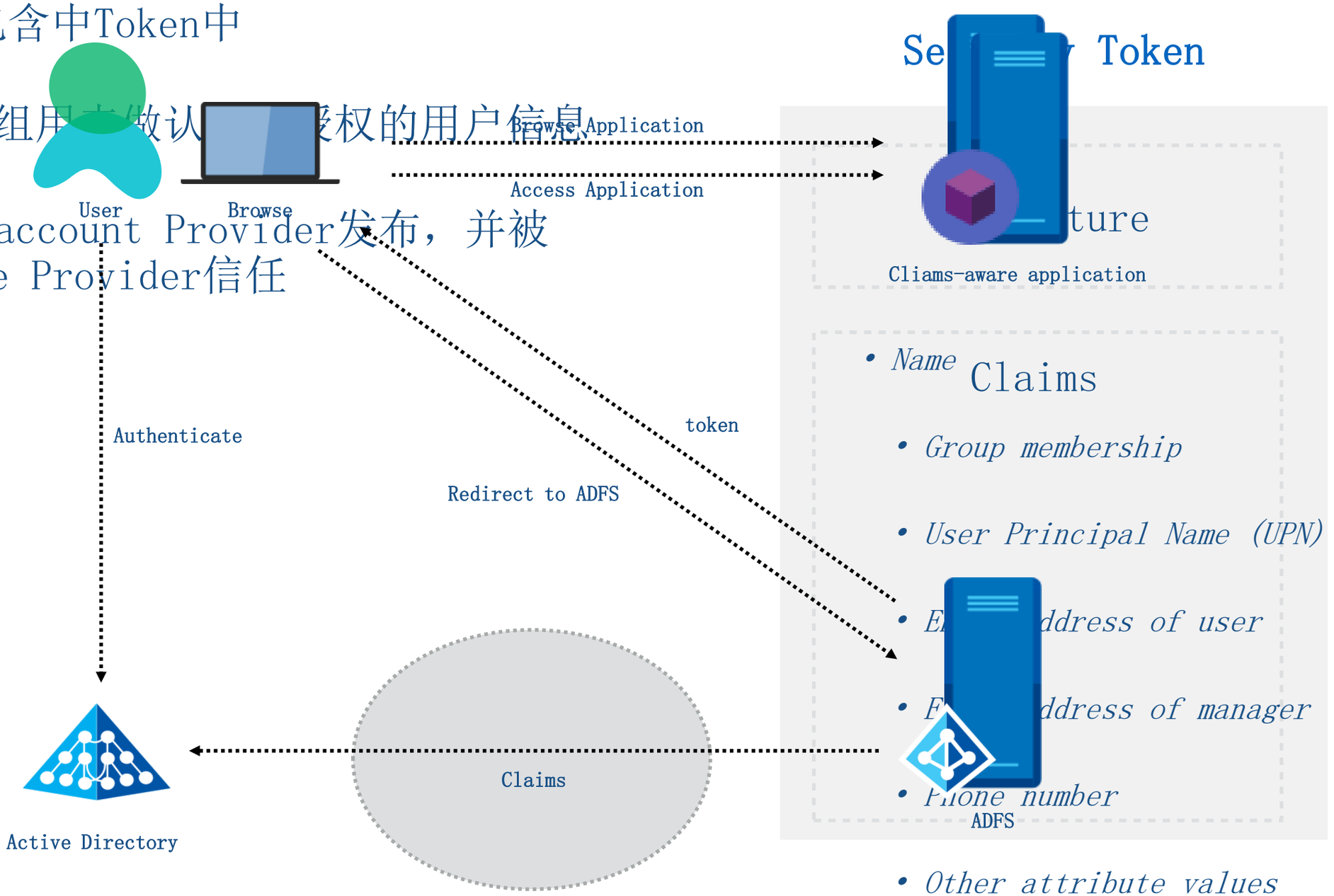
活动目录

- 活动目录(Active Directory)是一种目录服务
- 目录存储各种[illegible]信息
- 对象包括用户、用户组、计算机、域、以及安全策略
- 目录存储在域控制器(DC)的服务器上
- 身份验证以及目录对象的访问控制集成在活动目录中

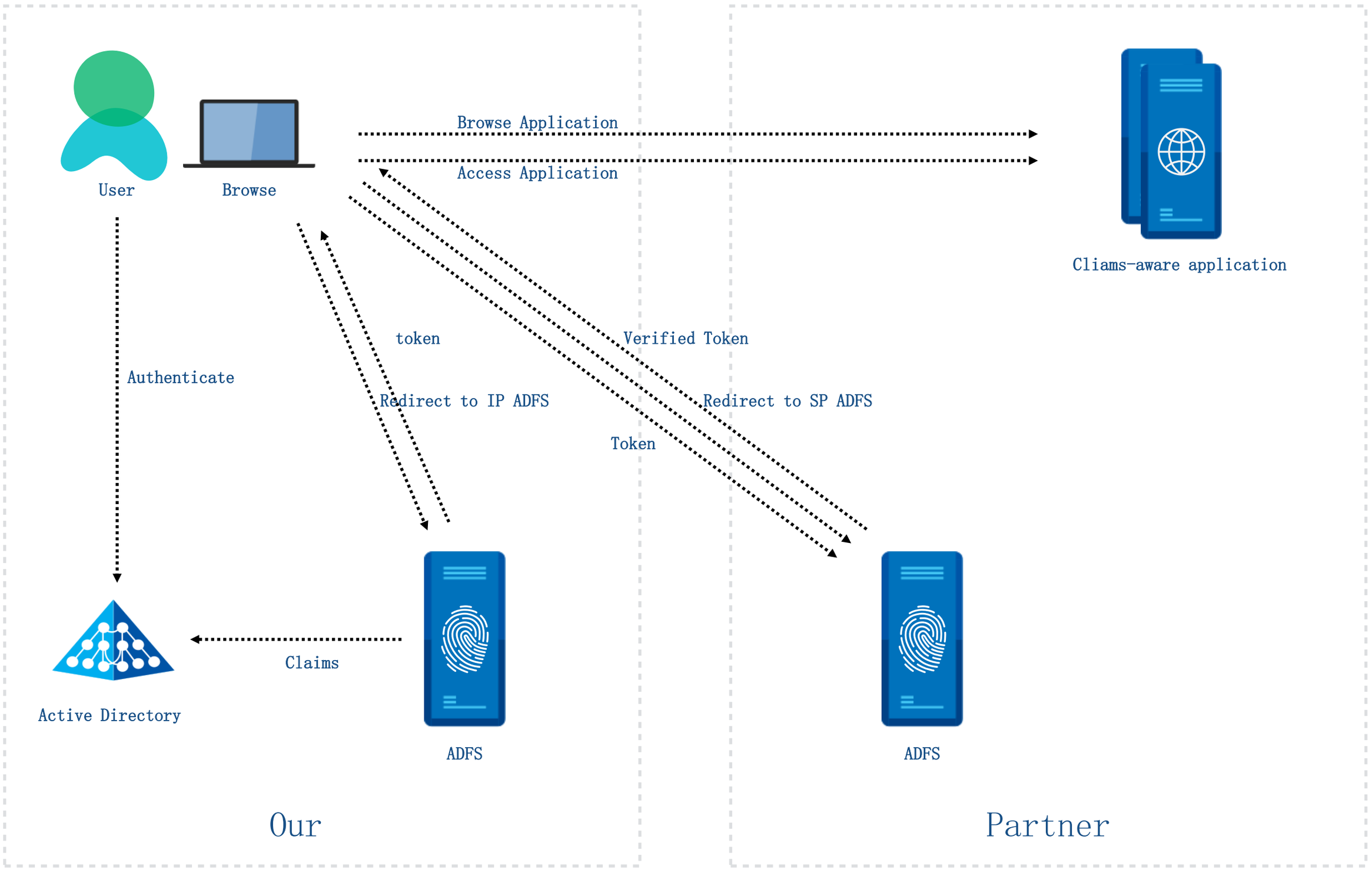


声明

- Claims包含中Token中
- 包含了一组用户做认[illegible]授权的用户信息
- Claims由account Provider发布，并被Resource Provider信任

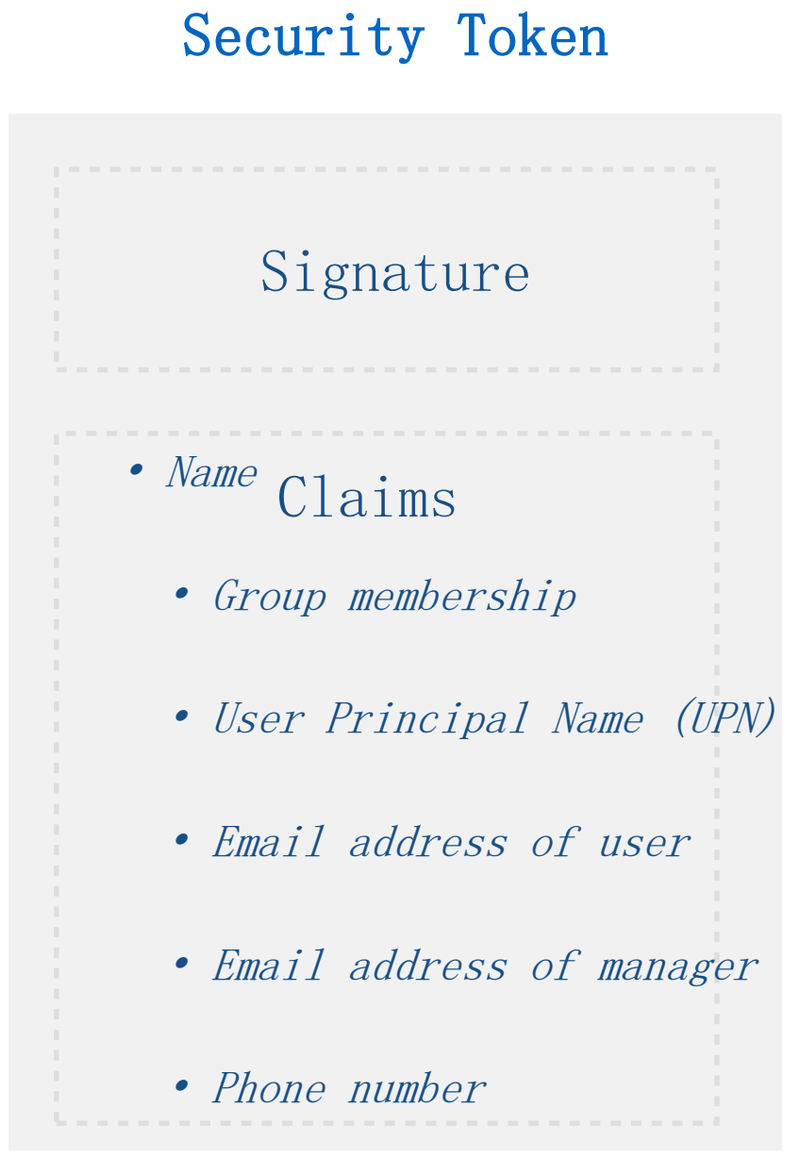


关键概念


User
Browse
Browse Application
Access Application
Cliams-aware application
Authenticate
token
Verified Token
Redirect to IP ADFS
Redirect to SP ADFS
Token
Active Directory
Claims
ADFS
ADFS
Our
Partner

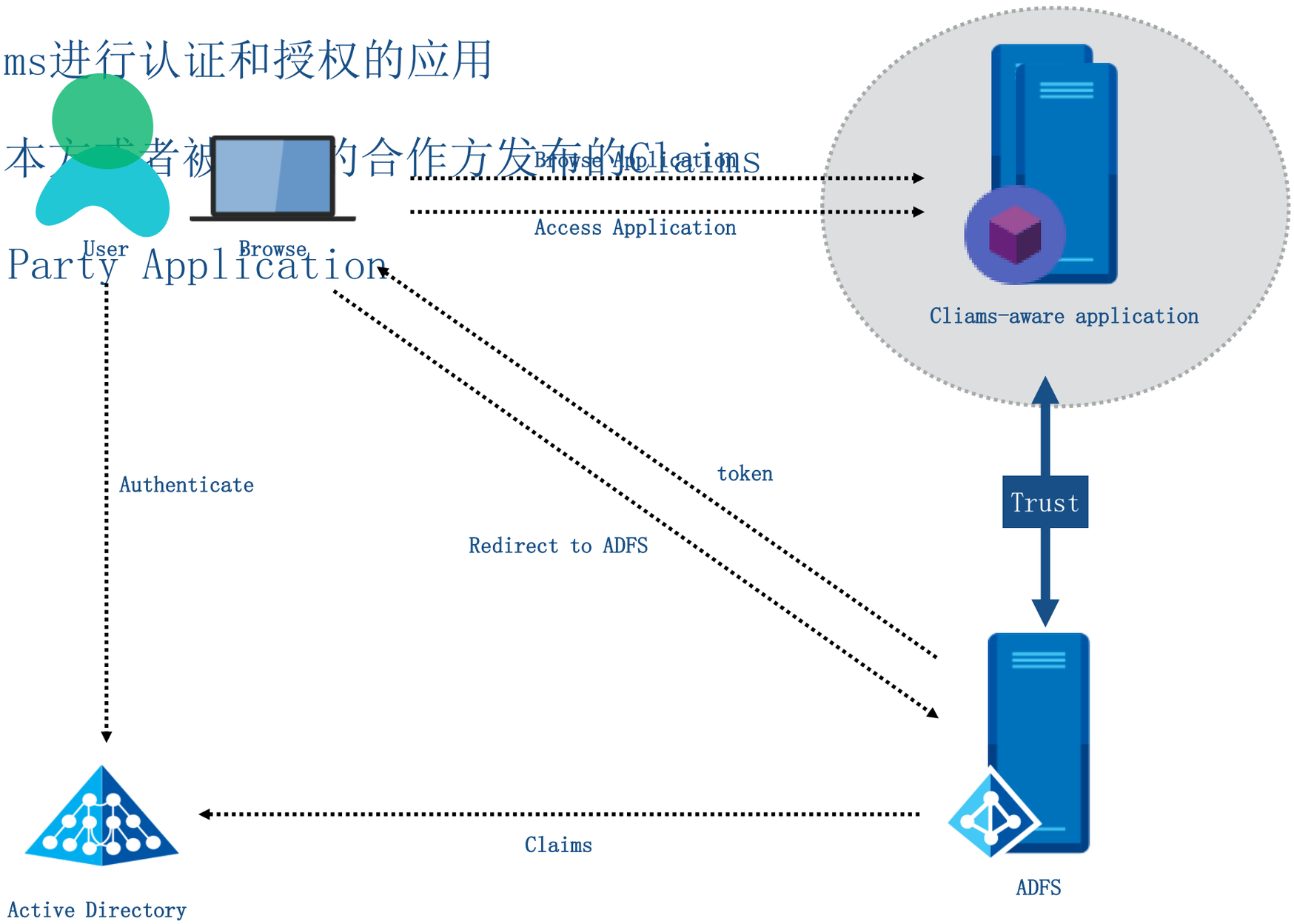
声明

- Claims包含中Token中
- 包含了一组用来做认证和授权的用户信息
- Claims由account Provider发布，并被 Resource Provider信任
- Resource Provider根据Claims对用户授权



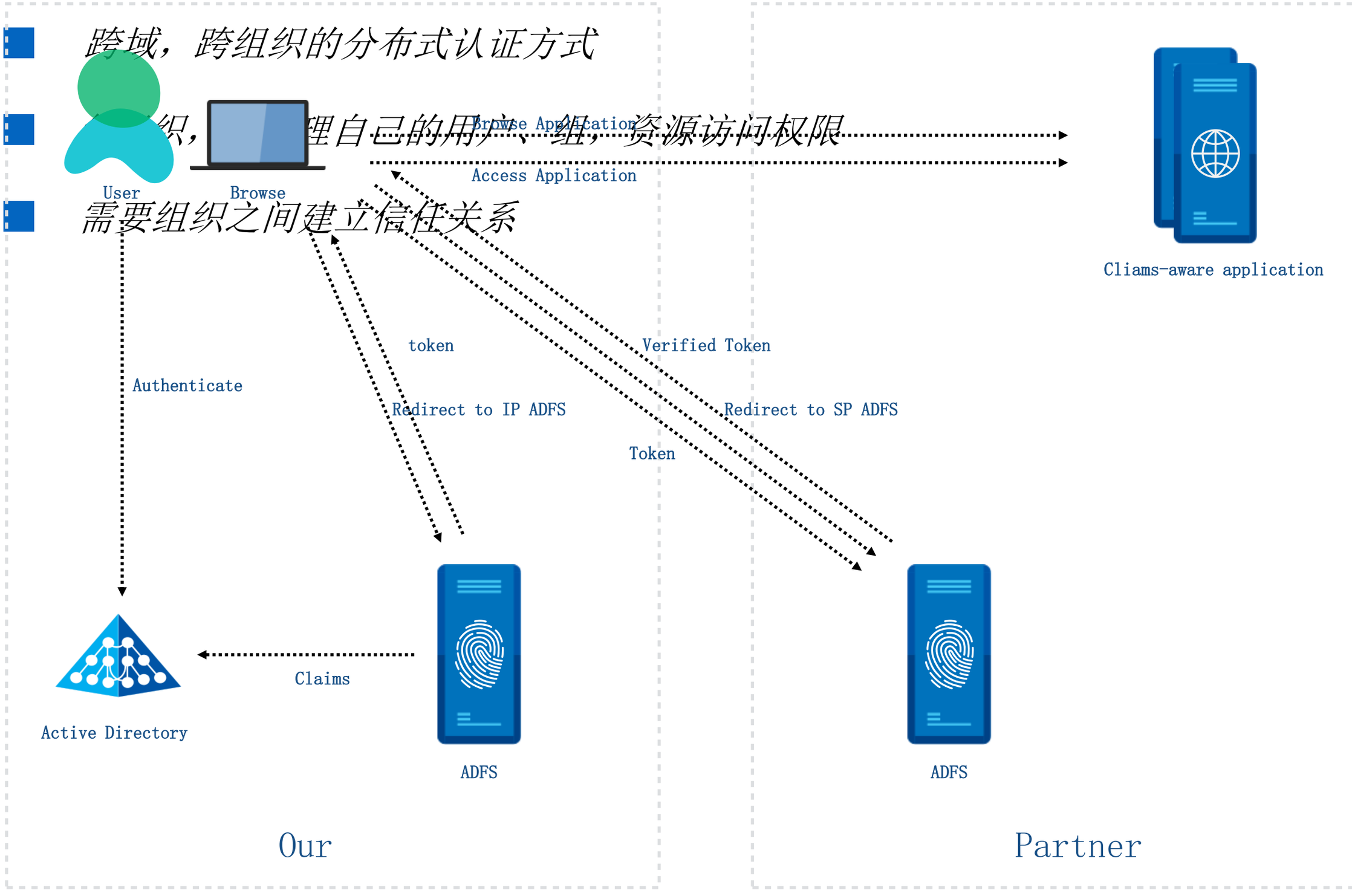
基于声明的应用

- 依据Claims进行认证和授权的应用
- 接收来自本方或者被信任的合作方发布的Claims
- Relaying Party Application

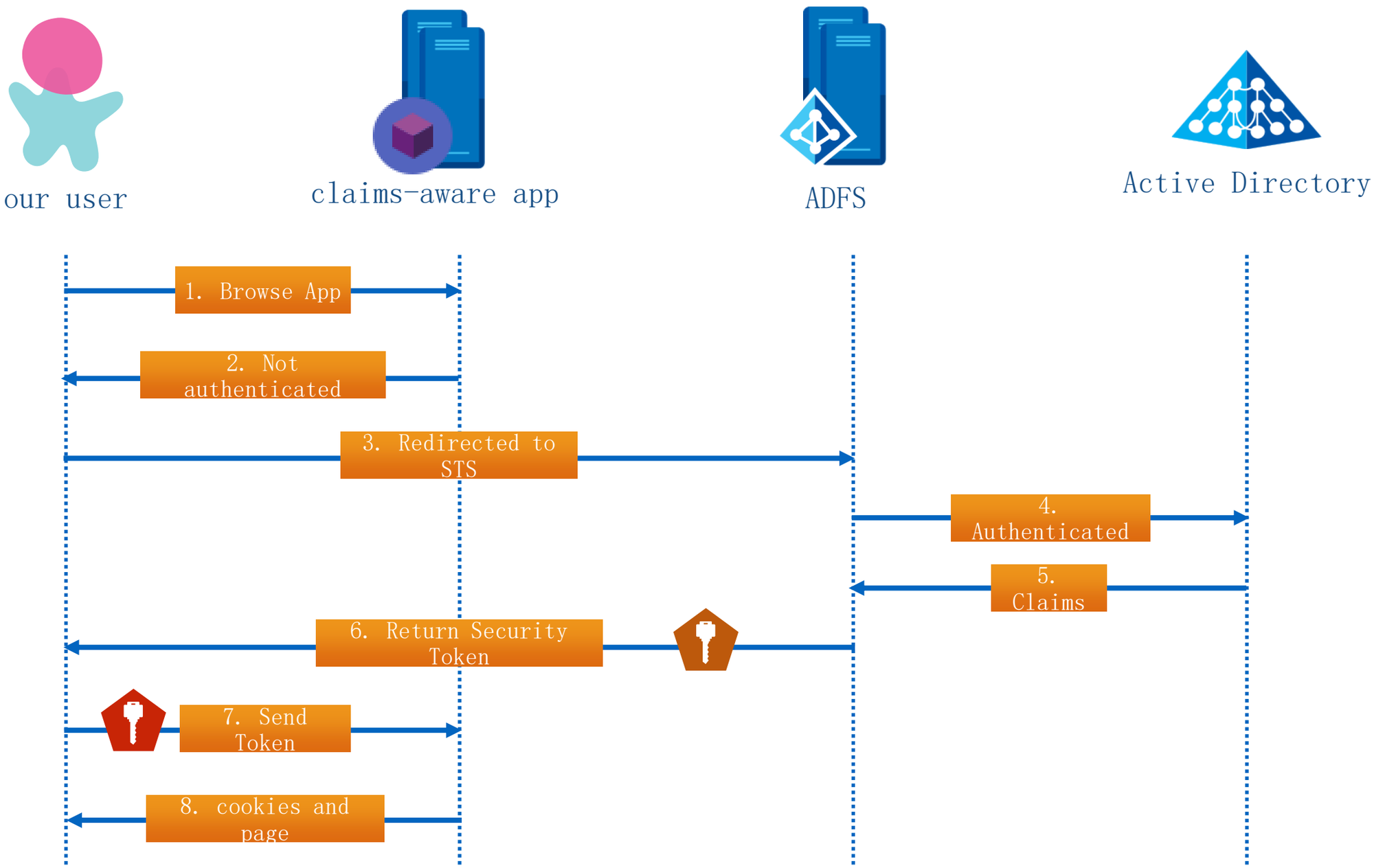


联合认证

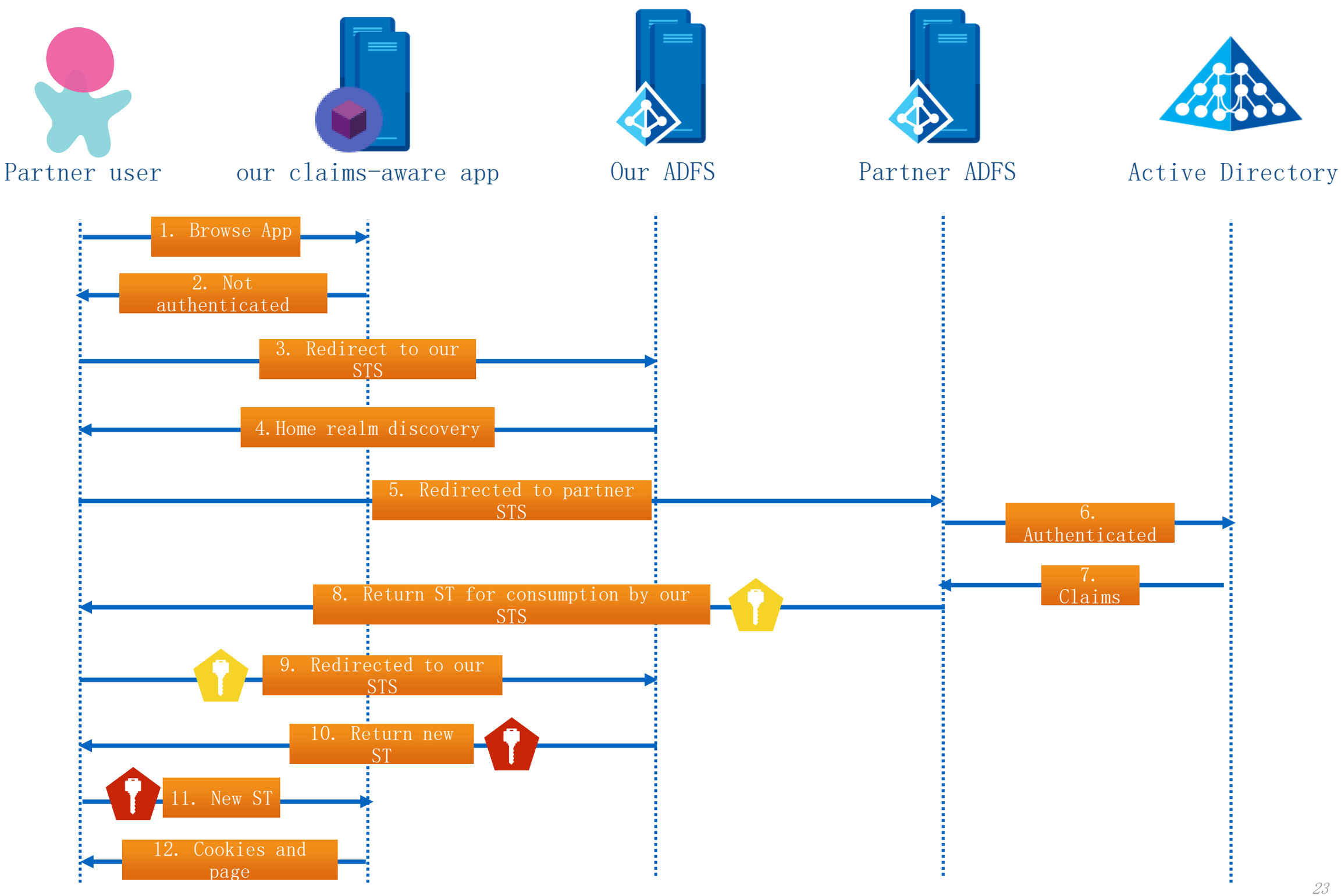
- *跨域，跨组织的分布式认证方式*
- *组织，管理自己的用户、组，资源访问权限*
- *需要组织之间建立信任关系*



认证流程


our user
claims-aware app
ADFS
Active Directory
1. Browse App
2. Not authenticated
3. Redirected to STS
4. Authenticated
5. Claims
6. Return Security Token
7. Send Token
8. cookies and page

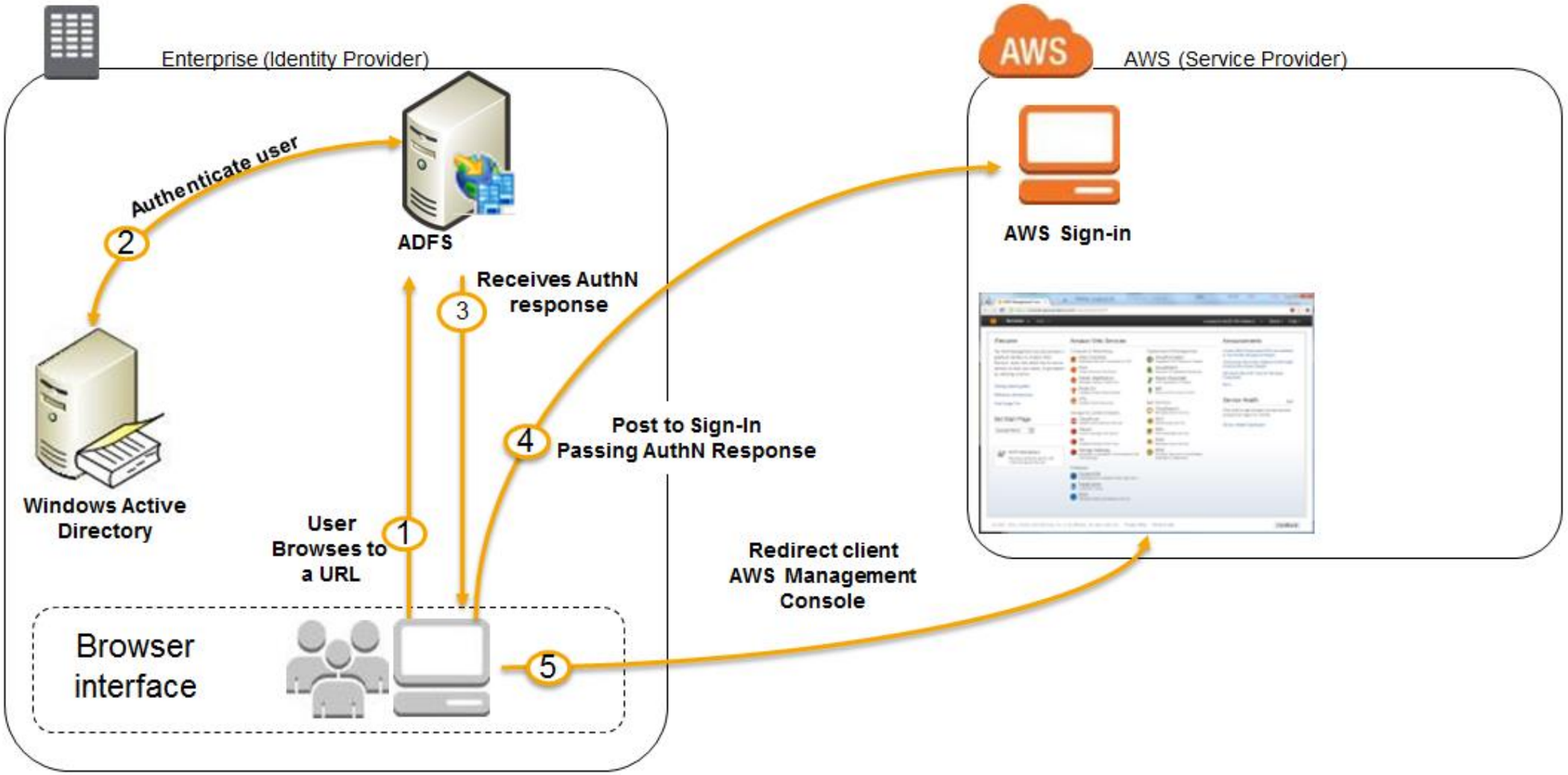
包含PARTNER的认证流程



协议

- SAML
- OAuth
- WS-Federation
- WS-Trust

AWS 集成ADFS


Enterprise (Identity Provider)
AWS
AWS (Service Provider)
Authenticate user
2
ADFS
AWS Sign-in
Receives AuthN response
3
4
Post to Sign-In
Passing AuthN Response
Windows Active Directory
User Browses to a URL
1
Redirect client AWS Management Console
Browser interface
5

谢谢

王浩
hdwang@thoughtworks.com

ThoughtWorks®

活动反馈