Introduction
to
Identity Management

Sam Lee, Outblaze Ltd.

OUTBLAZE

Agenda

- Background
- Identity Management
- Single Sign-On
- Federation
- Future’s Identity management
- Conclusions

Background

- Why identity management?
  - Need to know who is the user
  - What service the user is allowed
  - Threat of identity theft increases
  - Businesses and governments strengthen identity protection
- Cases
  - Online banking
  - Hacker

Identity management (IdM)

- What is identity management?
  - Processes and technologies to manage and secure access to the resource
  - Encompasses many aspects of high level security and authentication: biometrics, credentialing, physical access

- Principal components
  - Issuing credential for authentication
  - Authenticating credential and granting access to resource after authentication

Identity life cycle

- Establishes an identity
  - Links a name with the identity
- Describes the identity
  - Assigns attributes applicable to the identity
  - What the identity can do
- Destroys the identity
  - End of the identity

Identity management functionality

- User information self-service
- Authentication and authorization
- Password management
- Workflow
- Provisioning and de-provisioning of identities from resources

Authentication

- Methods
  - Something you know (e.g. password)
  - Something you have (e.g. smart card)
  - Something you are (e.g. iris, fingerprint)

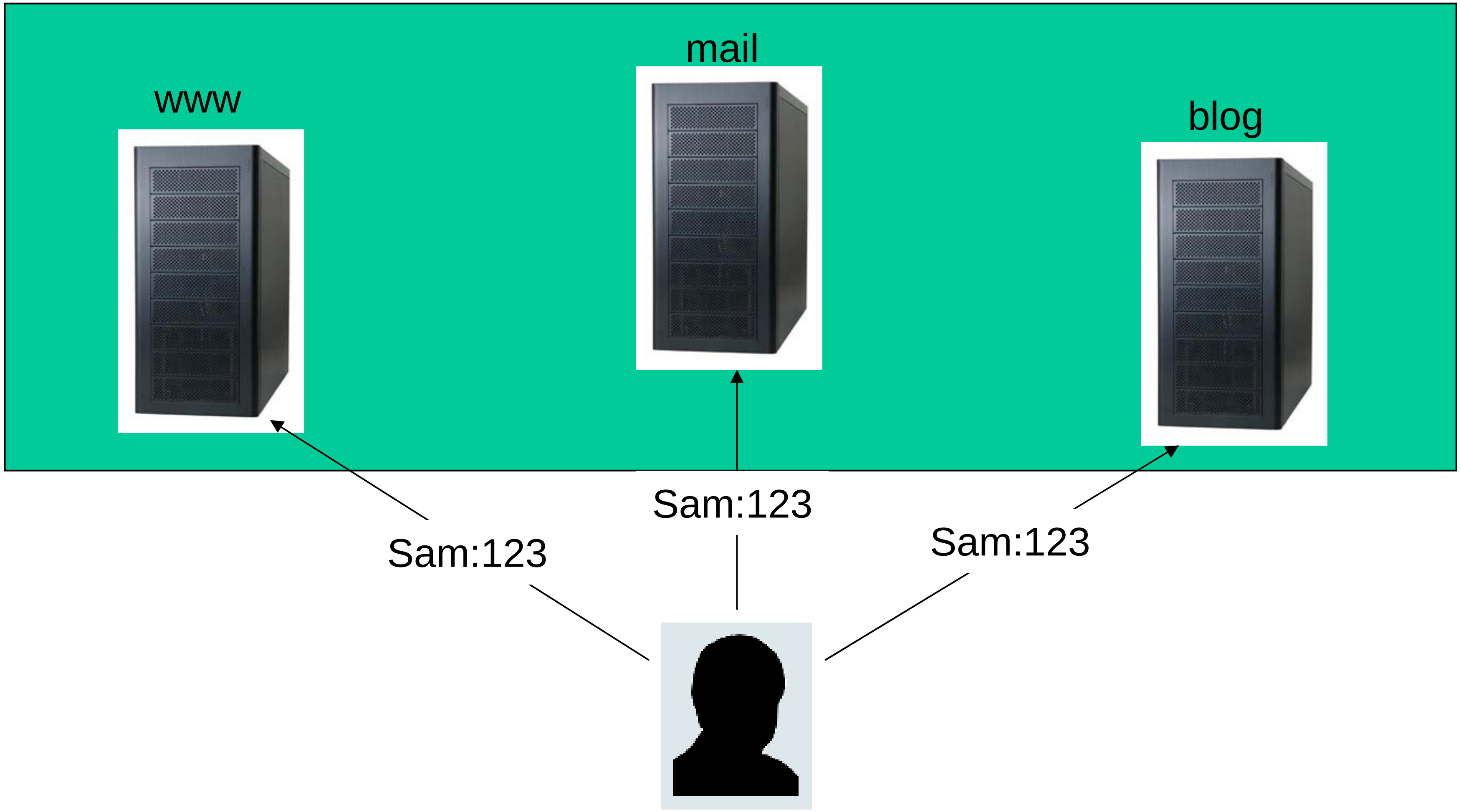
Identity management in IT

- Management of user credentials
  - Users might log on to an online system
  - Management of information which represents items Identified items in real life
- User-centric identity
  - Puts users in control of their own identity information
  - Gives users a single identity, instead of username and password
  - Examples: LiveID, OpenID, InfoCard systems (Microsoft’s CardSpace, Novell’s Digital ME)

OpenID

- An open, decentralized, shared identity service
- Allows users to use a single digital identity across different websites
- User chooses the OpenID provider, based on the needs and trust
- Not proprietary and free
- Adopt in: AOL, BBC, Google, IBM, Microsoft, Orange, Yahoo acting as providers.

Single sign-on (SSO)



Single sign-on (SSO)

- What is SSO?
  - Enables a user to authenticate once and gain access to the resources of multiple software systems.
- Benefits of SSO
  - Convenience
  - Secure
  - Reduces humor error, system failure

SSO (cont'd)

- Involving parties:
  - Identity provider (IdP)
  - Service provider (SP)
- Mechanism
  - IdP provides a security token
  - SP receives the token, authenticates the token, and allows user to access without further sign on
  - Between enterprises using federated authentication (cross-domain SSO)
- Difficult to implement

Windows Live ID

- Originally named .NET Passport
- Single sign-on service
- Supports for authentication from cell phone, televisions and Xbox 360.
- Windows XP has an option to link a Windows user account with a Windows Live ID, logging users into Windows Live ID whenever they log into Windows

Standards

- Security Assertion Markup Language (SAML)
- Liberty Alliance
  - A consortium promoting federated IdM
- Shibboleth
  - Identity standards targeted towards educational environments

Why is SAML required?

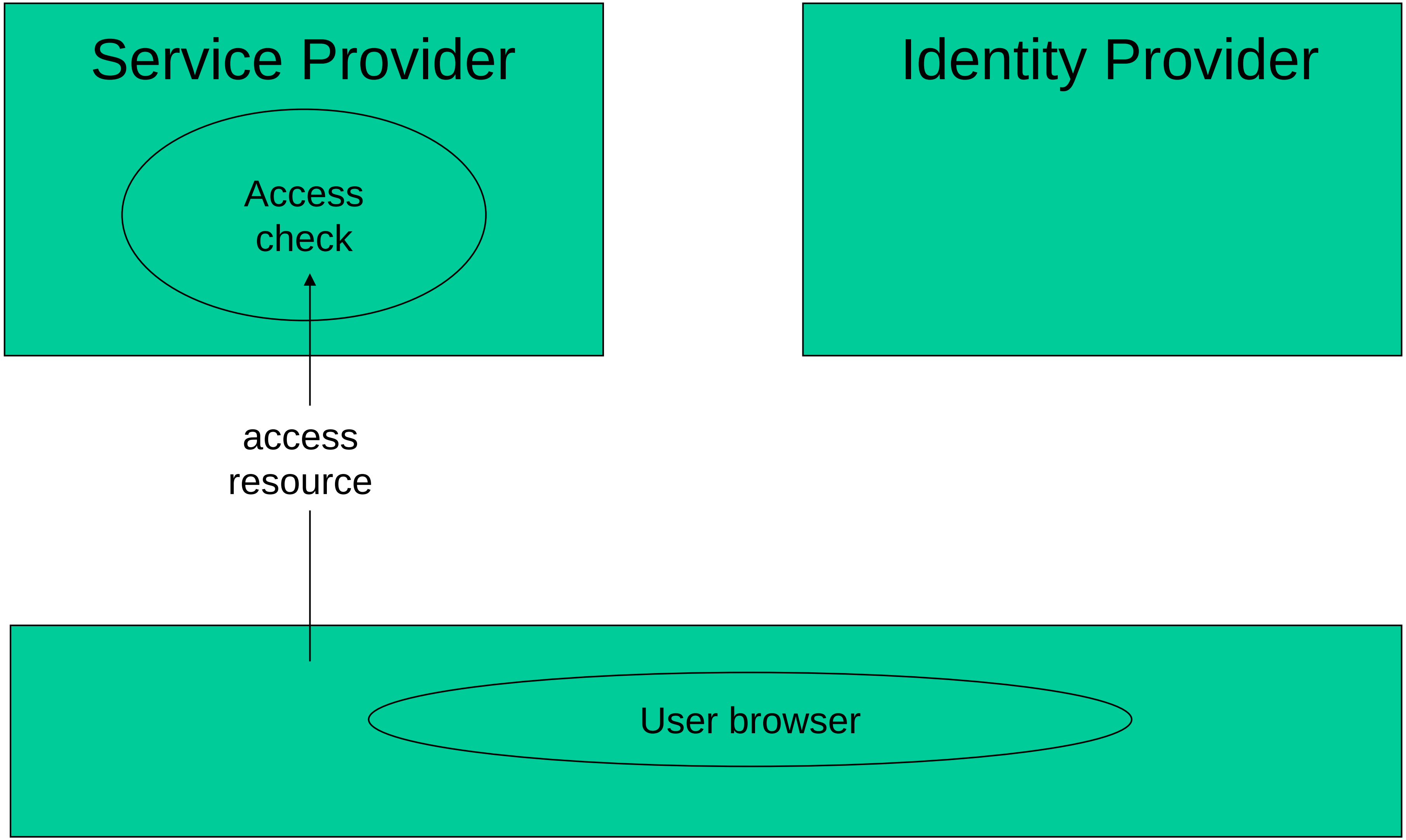
- Limitations of browser cookies
- SSO Interoperability
- Web services
- Federation

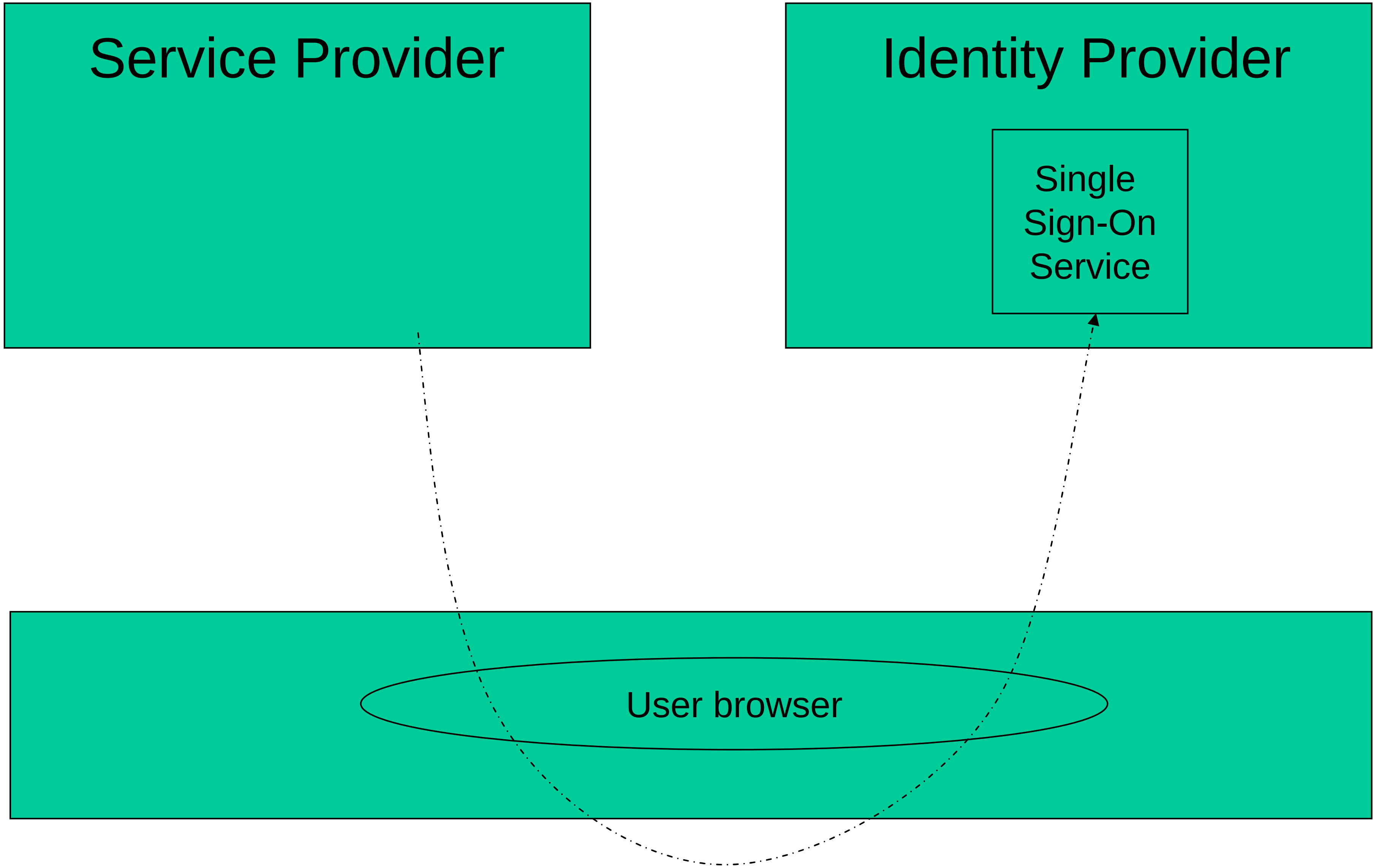
SAML

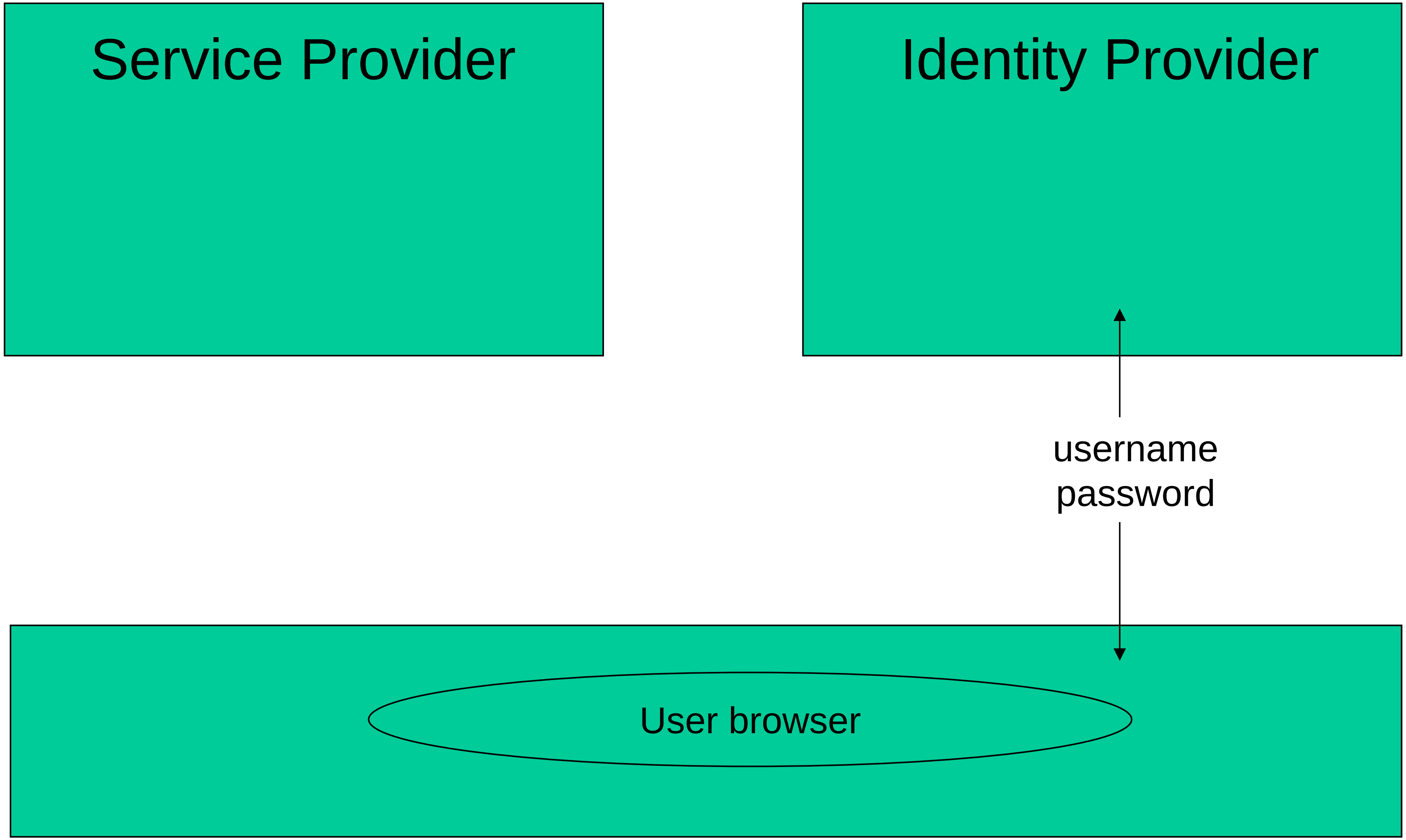
- Security Assertion Markup Language
  - Developed by OASIS Security Services Technical Committee
  - XML standard for exchanging authentication and authorization data between security domains (IdP and SP).
  - Trying to solve web single sign-on problem
  - Latest version 2.0 (up to 20-5-2008)

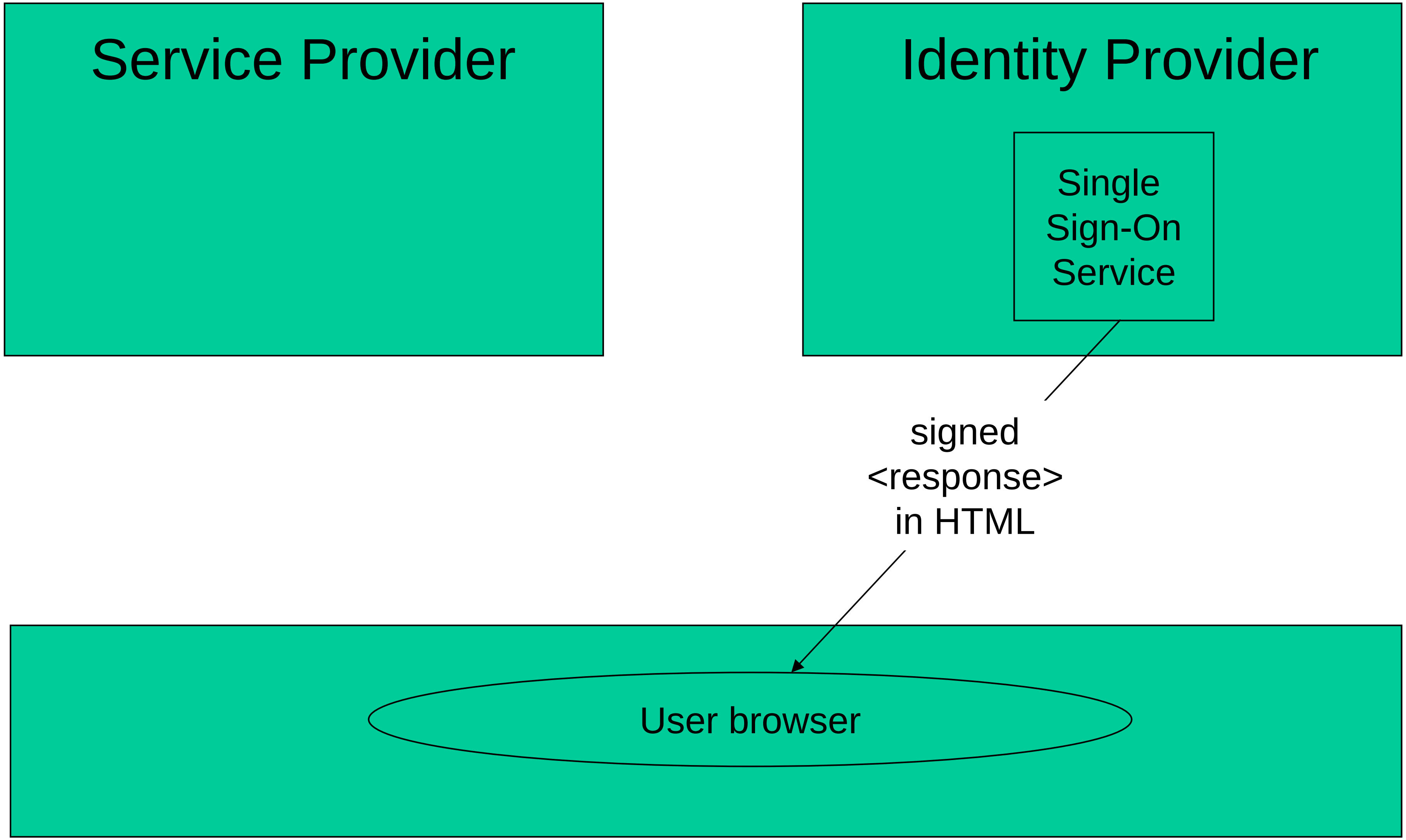
SAML (cont'd)

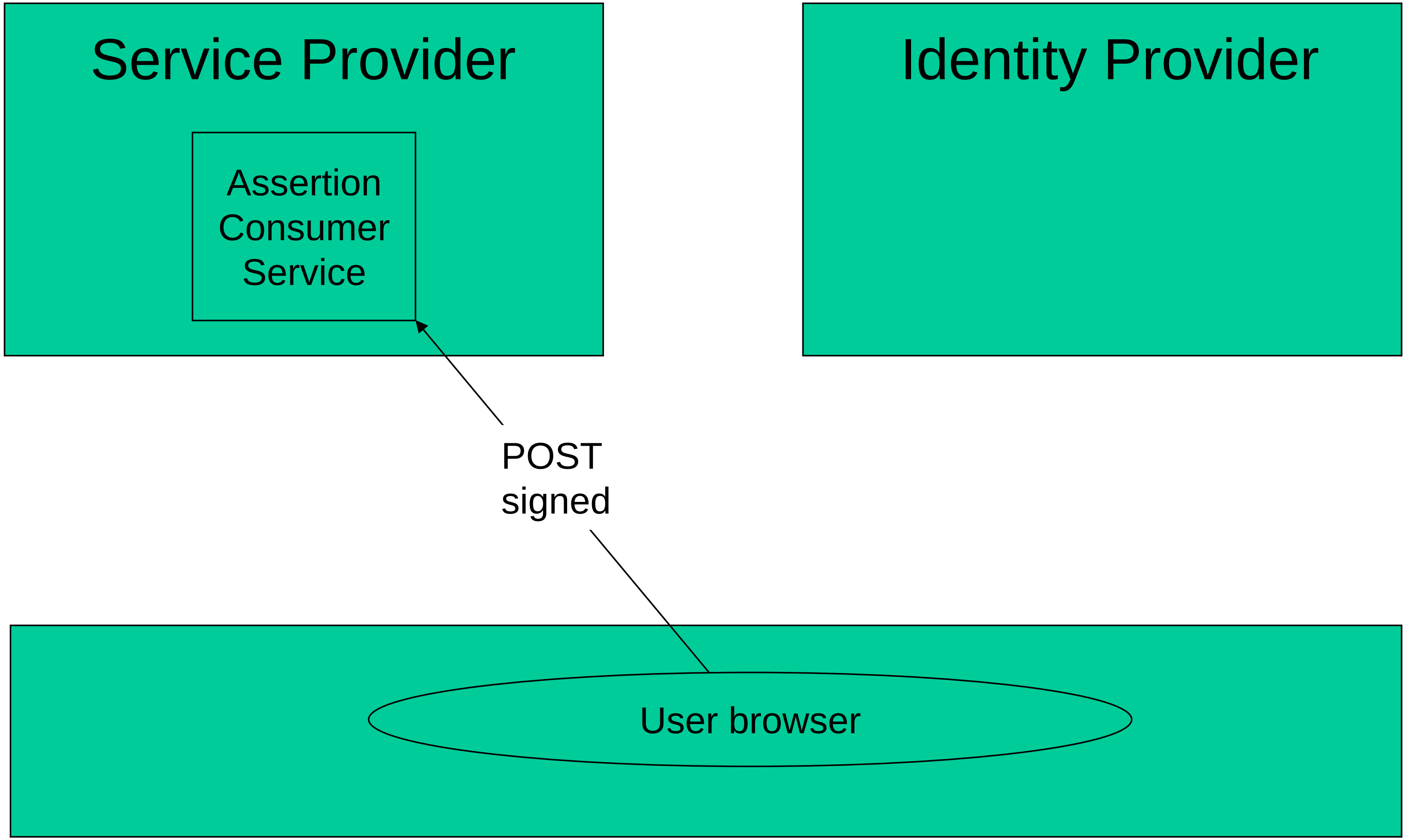
- Enrolled with at least 1 IdP
- Identity provider
  - Provides local authentication services to the principal
  - Does NOT specify the implementation of these local services.
- Service provider
  - Relies on IdP
  - Decides access control
  - Service provider

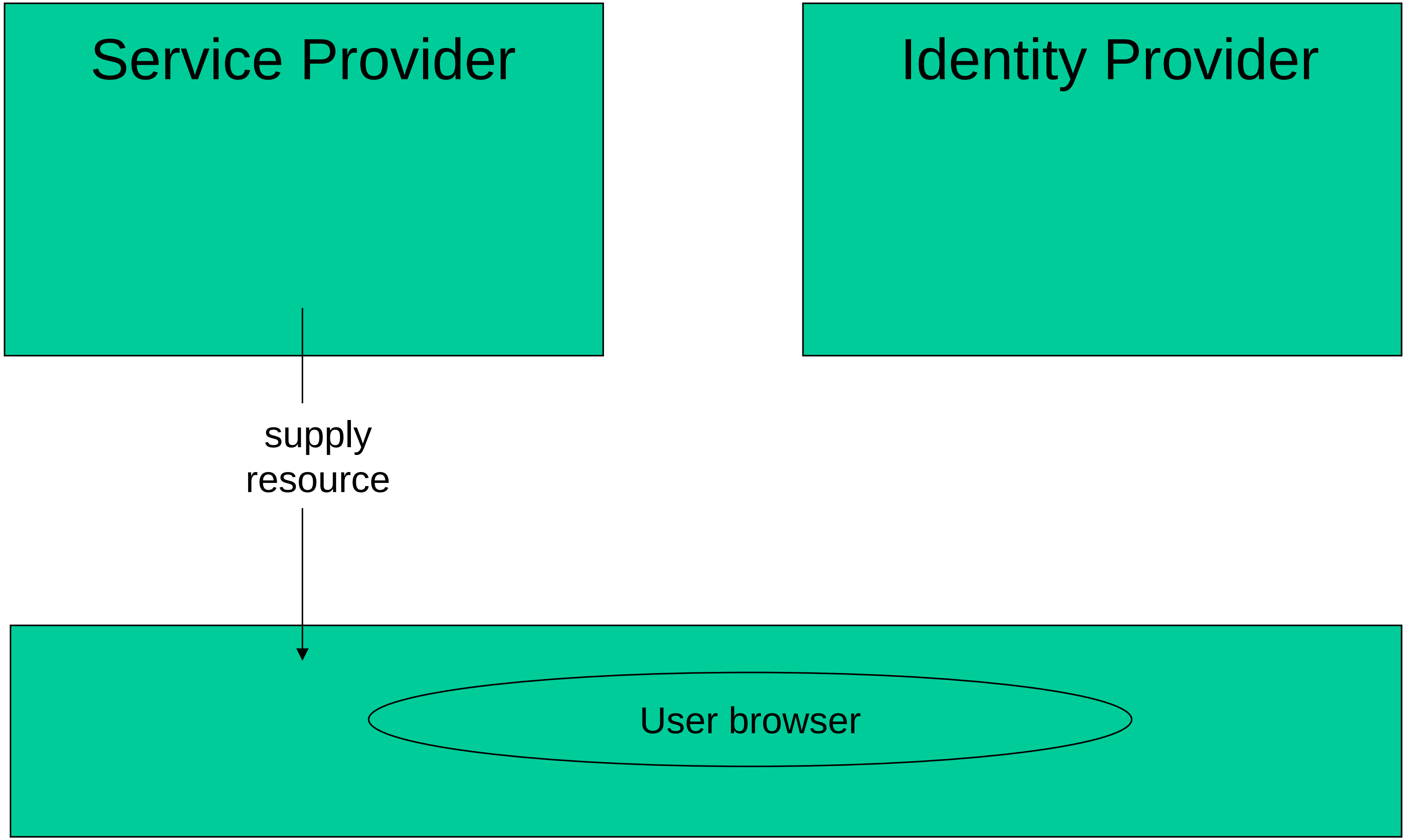

Service Provider
Identity Provider
Access check
access resource
User browser


Service Provider
Identity Provider
Single Sign-On Service
User browser

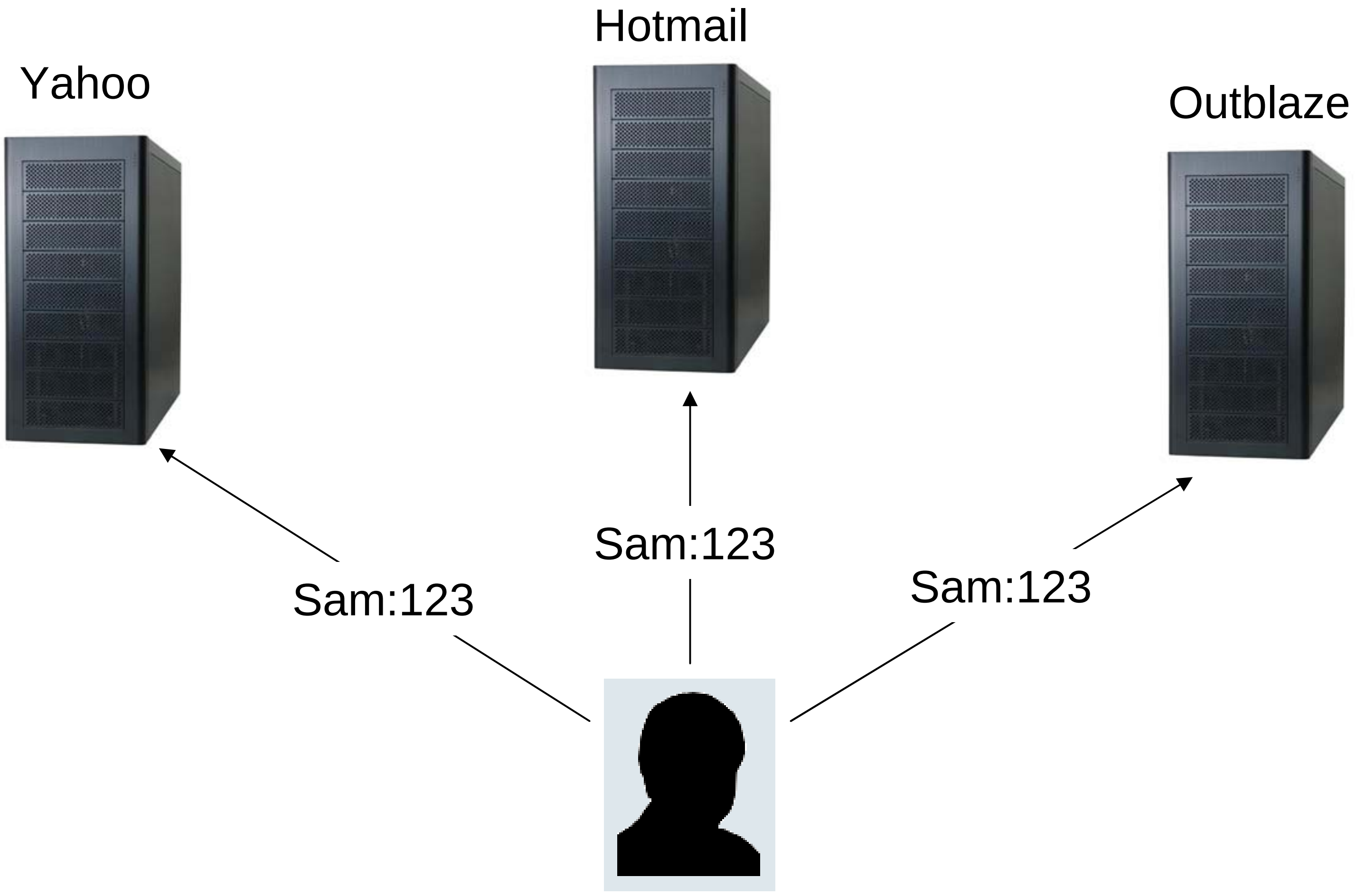

Service Provider
Identity Provider
username
password
User browser


Service Provider
Identity Provider
Single Sign-On Service
signed <response> in HTML
User browser


Service Provider
Assertion Consumer Service
Identity Provider
POST signed
User browser


Service Provider
Identity Provider
supply resource
User browser

Federation



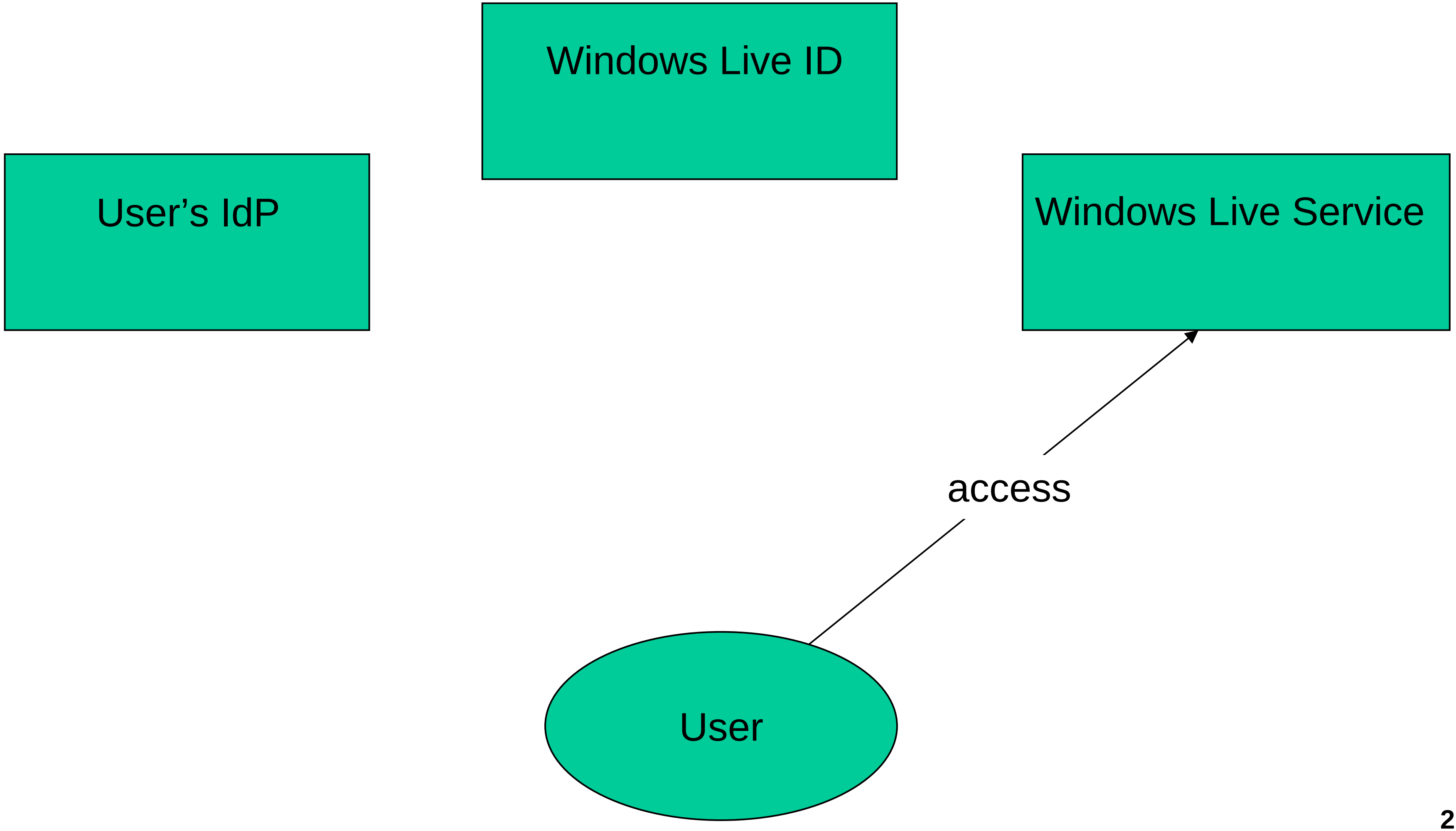
Federation

- Solve cross-domain SSO problem
- A trust-based agreement between two organizations
- Involving parties
  - Identity provider
  - Service provider
- Relationship
  - Unidirectional or bidirectional

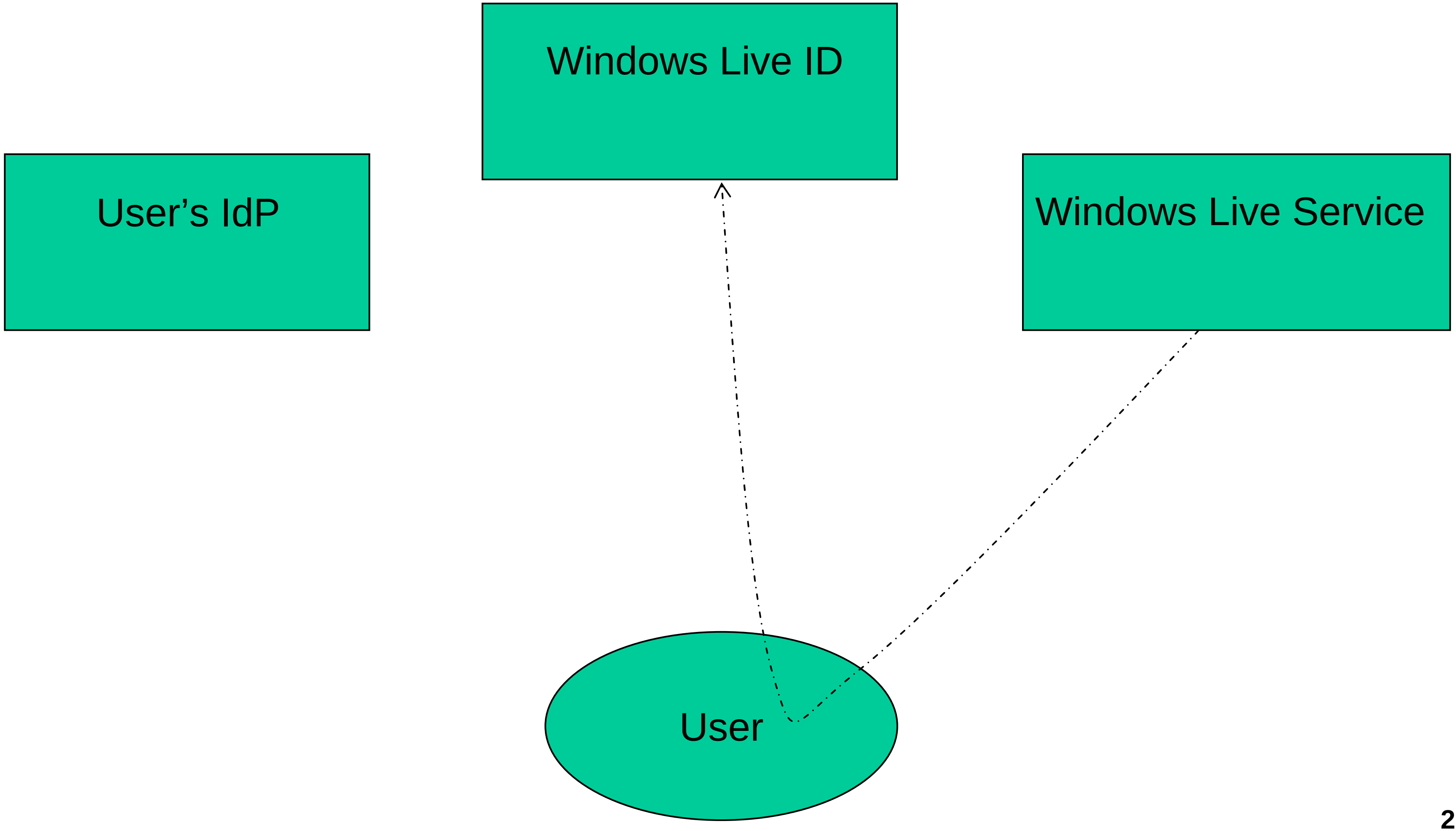
Advantages of Federation

- Single sign-on
- Each party controls its own users accounts
- Identities are created and maintained easily
- Mapping between identity provider and service provider

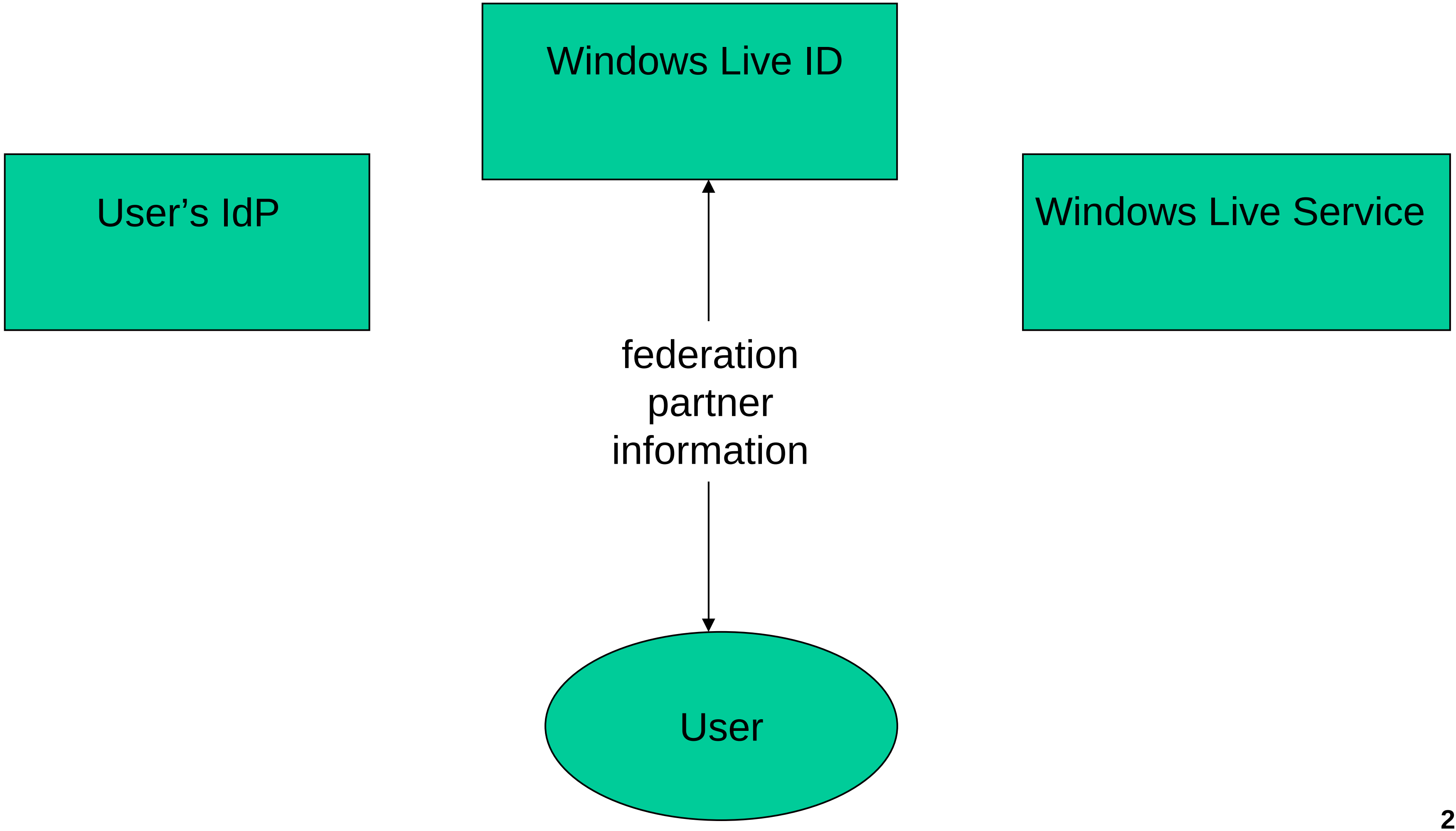
Windows Live ID Federation



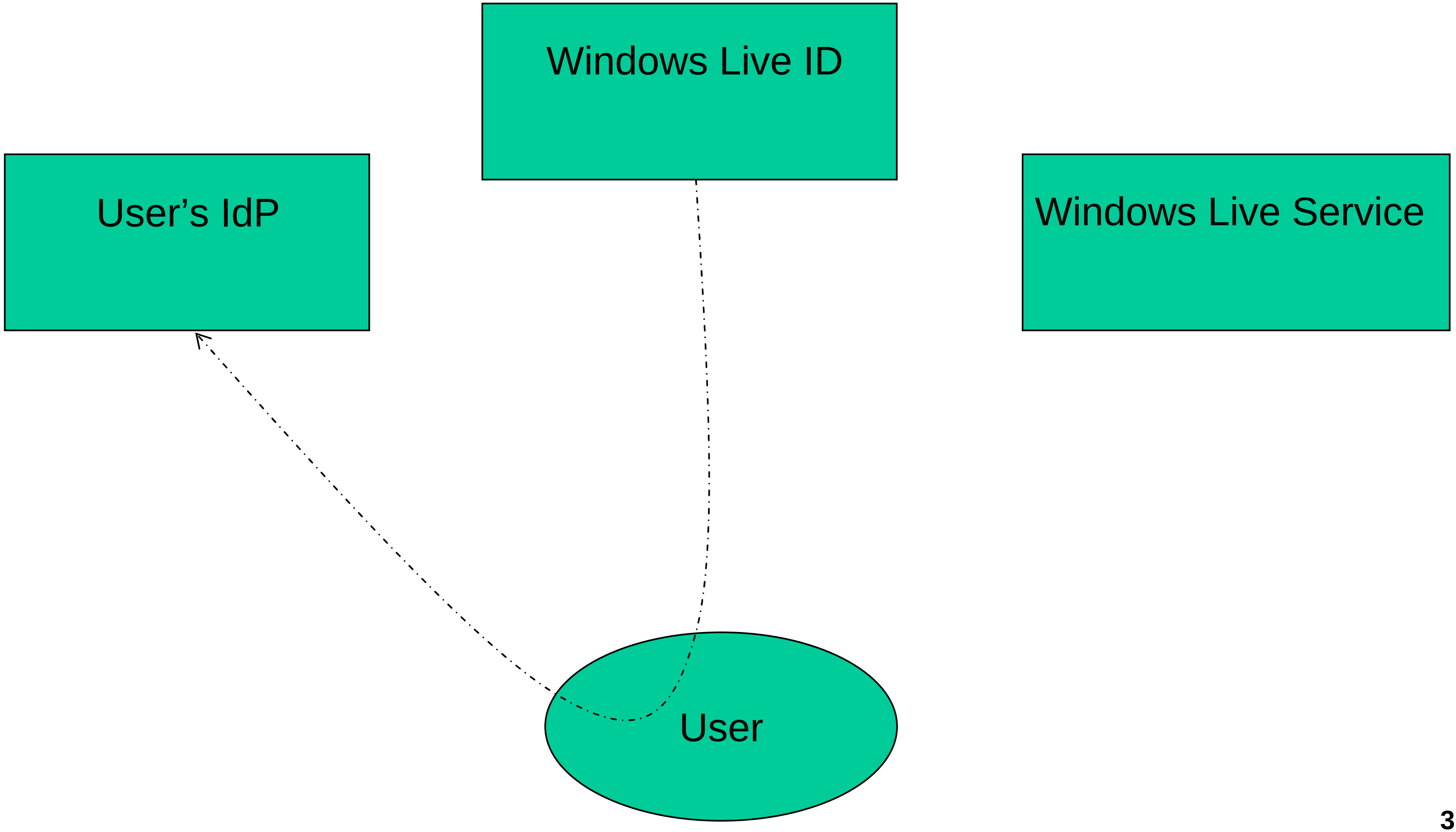
Windows Live ID Federation



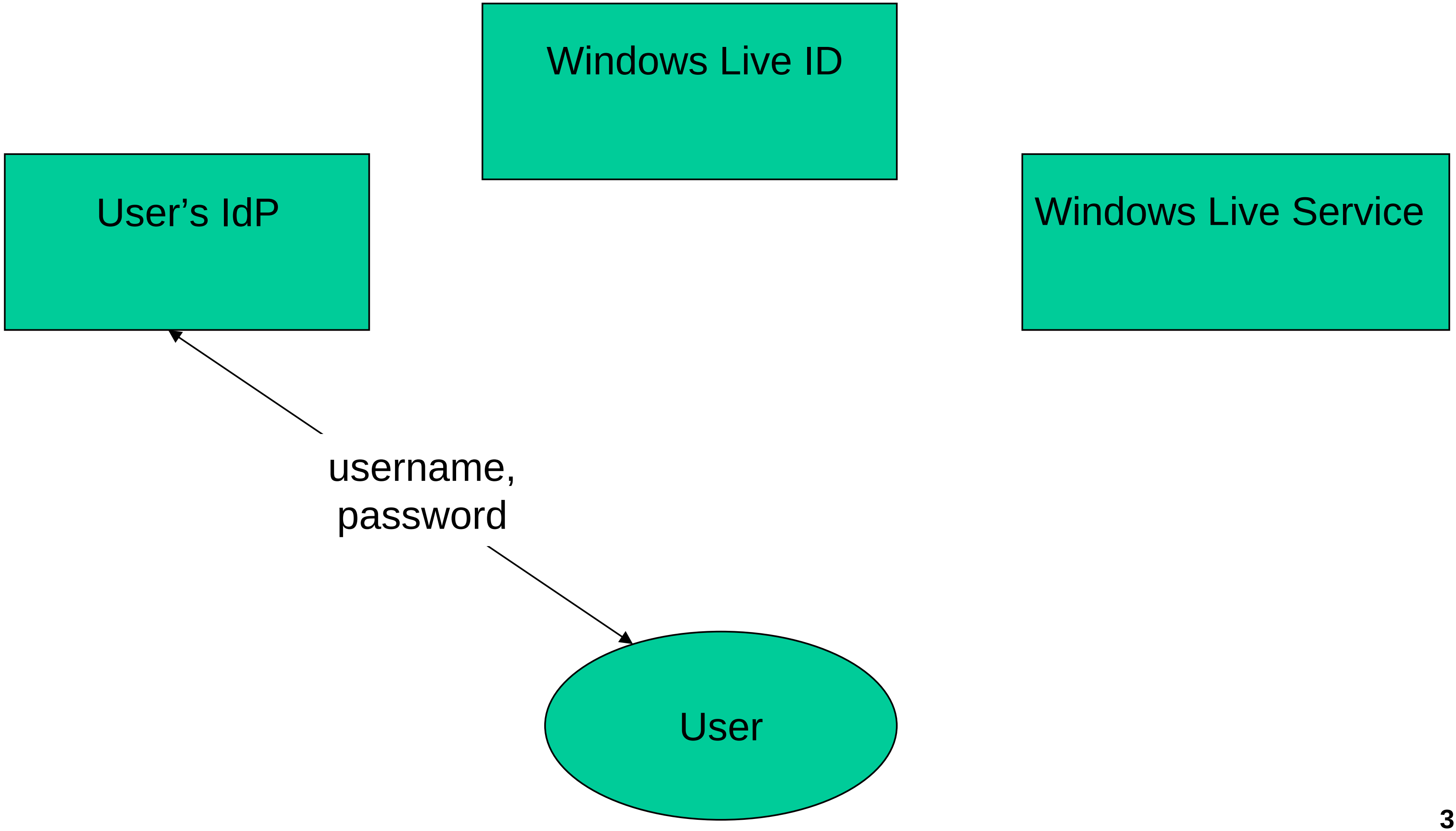
Windows Live ID Federation



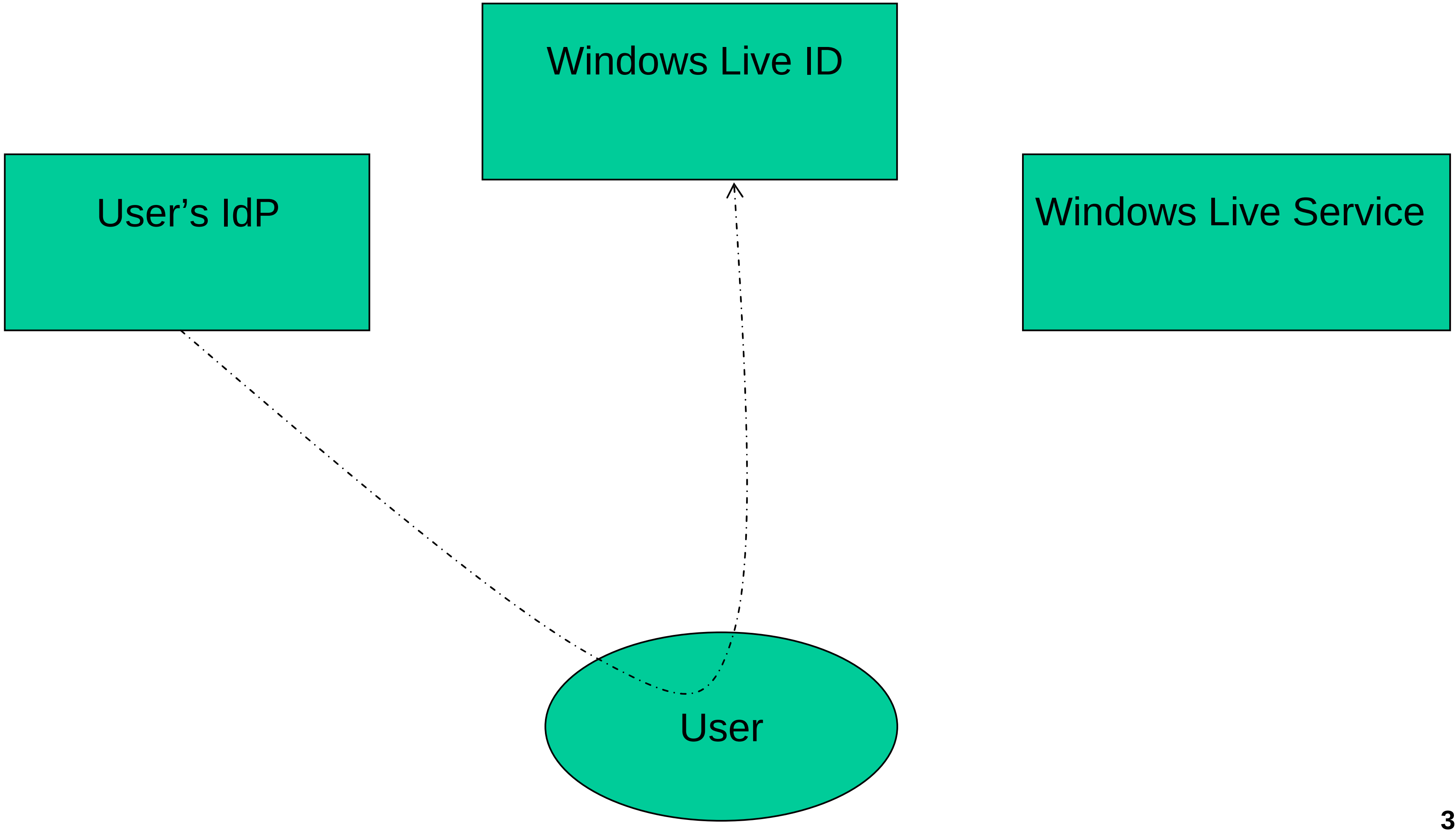
Windows Live ID Federation



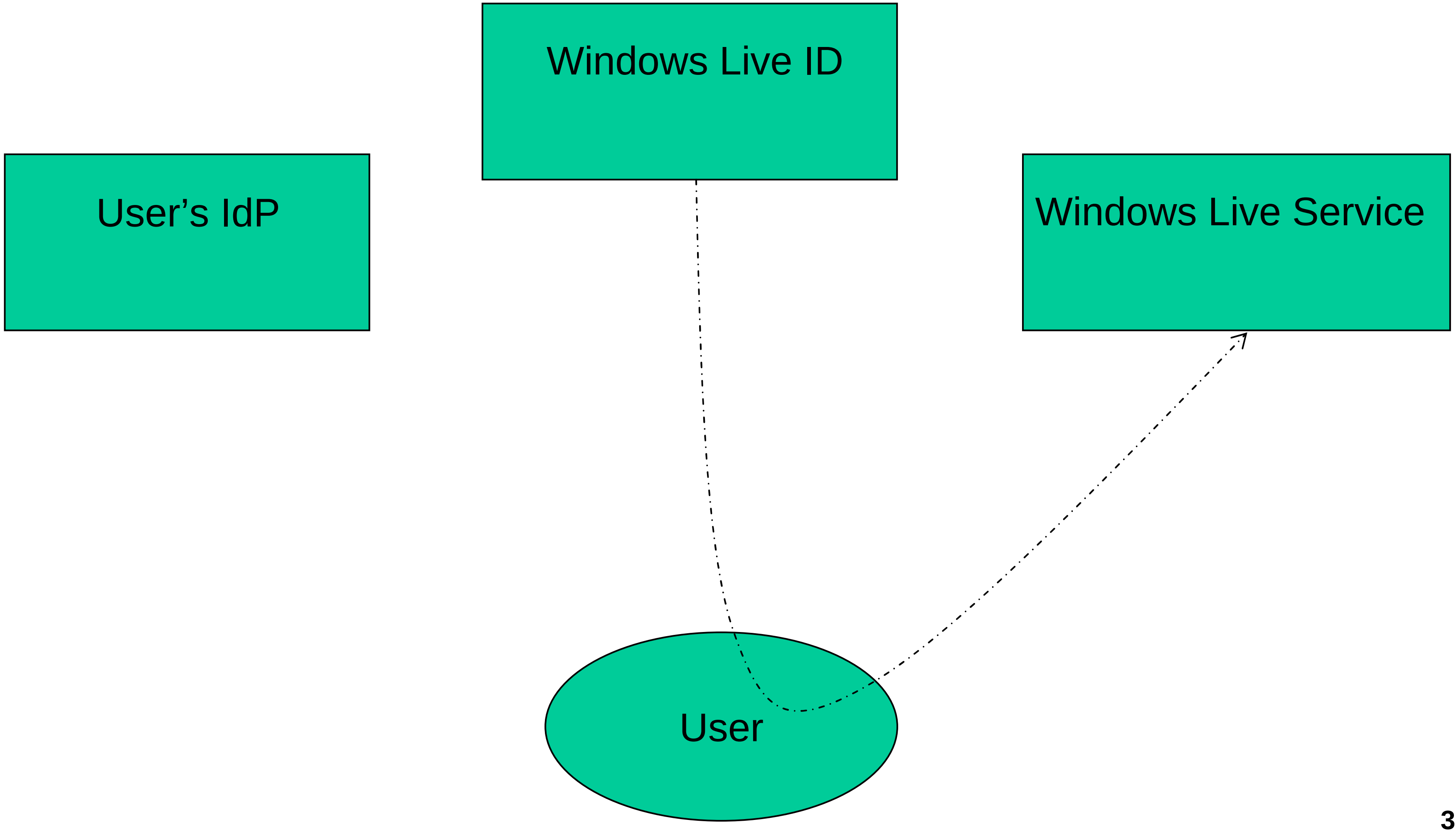
Windows Live ID Federation



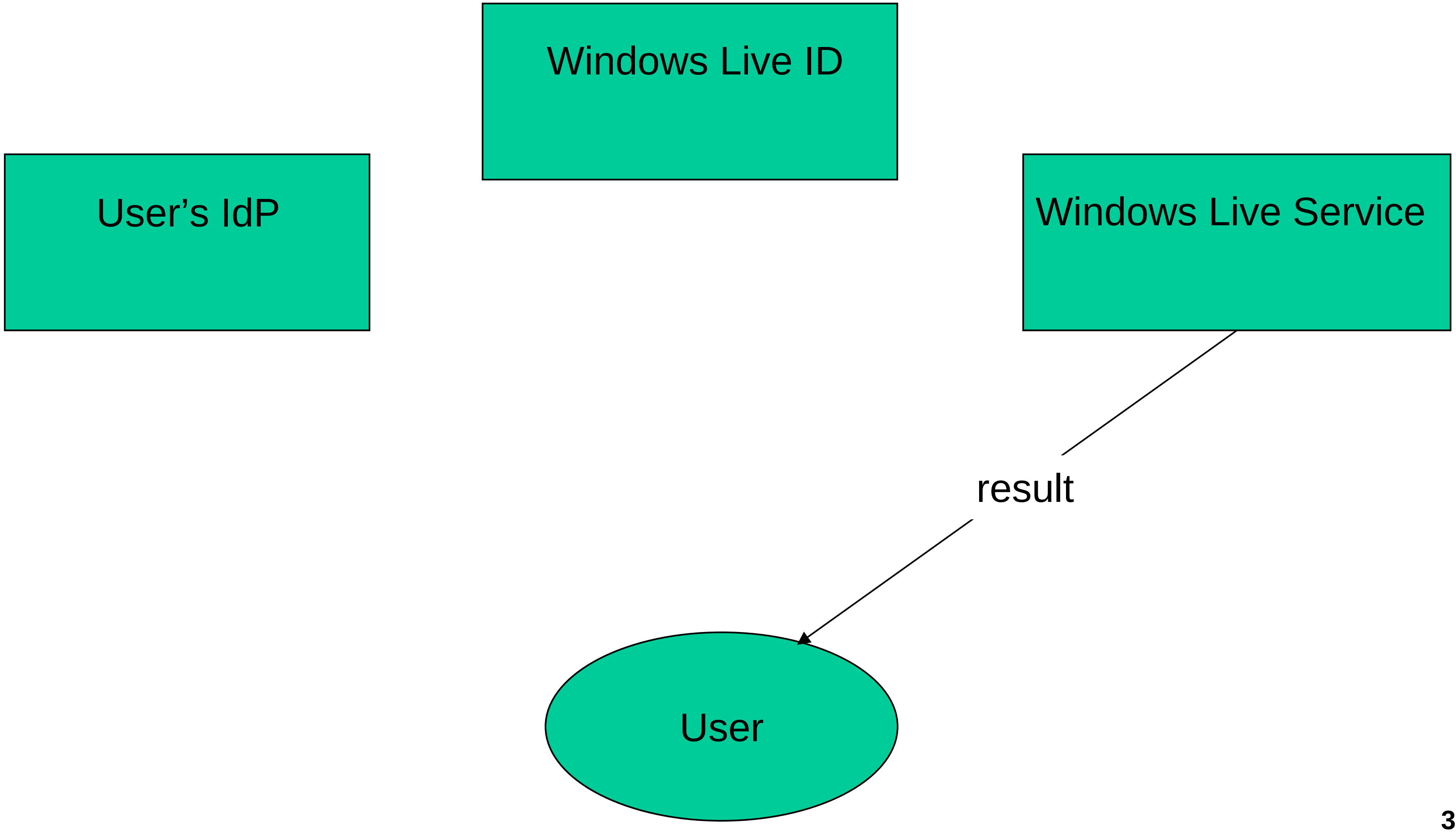
Windows Live ID Federation



Windows Live ID Federation



Windows Live ID Federation



Shibboleth

- Developed by Internet2 Middleware Initiative
- Shibboleth 2.0 was released on March 08
- SSO and federating software
- Focus on cross-domain SSO
- Interoperate with SAML and ADFS

Conclusions

- Identity Management
  - OpenID
- Single Sign-On
  - Windows Live ID
  - SAML
- Federation
  - Windows Live ID Federation

Q&A