Access Management

Challenges in Controlling Access

- Various types of users need different levels of access
  - Internal users, contractors, outsiders, partners, etc.
- Resources have different classification levels
  - Such as confidential, internal use only, private, or public
- Diverse identity data must be kept on different types of users
  - Credentials, personal data, contact information, work-related data, digital certificates, cognitive passwords
- The corporate environment is continually changing

Challenges	Issue for users	Issue for administrators
Different password for different applications	Too many identities and credentials to manage	Frequent calls to the helpdesk for password resets
Lack of centralized web authorization and authentication service	Multiple log-ins to different applications within the enterprise	Inconsistent application security policies
Lack of identity federation support	Multiple log-ins to applications hosted outside the enterprise	Managing authorization credentials for outside users

Enterprises are trying to find the balance between two interests…

Usability expectations

Need to be secure

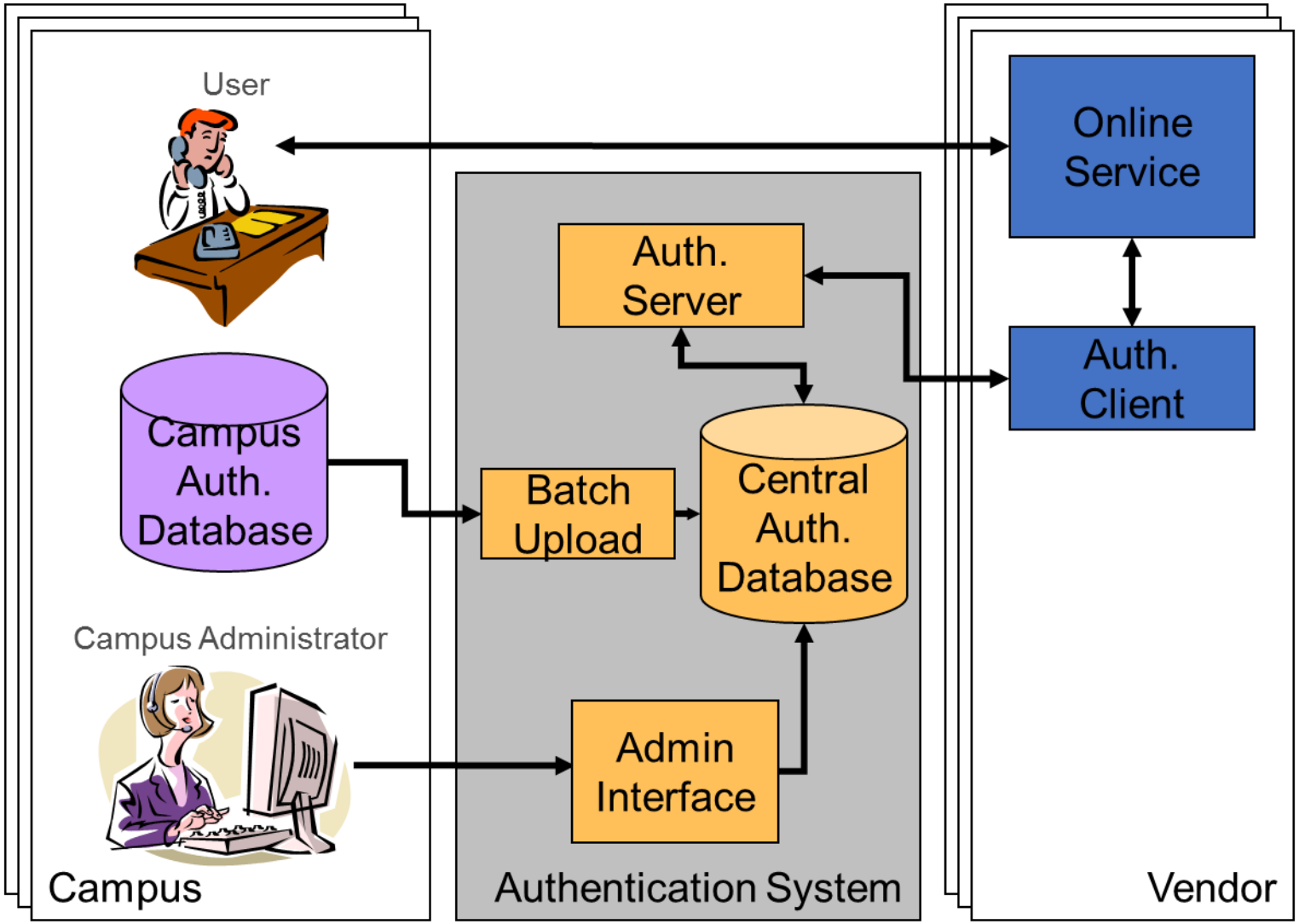
What Is Access Management?

- Authentication/Single Sign On
- Entitlements Authorization
- Auditing
- Service Provision
- Identity Propagation/Delegation
- Federation

Balancing Act

Access Management

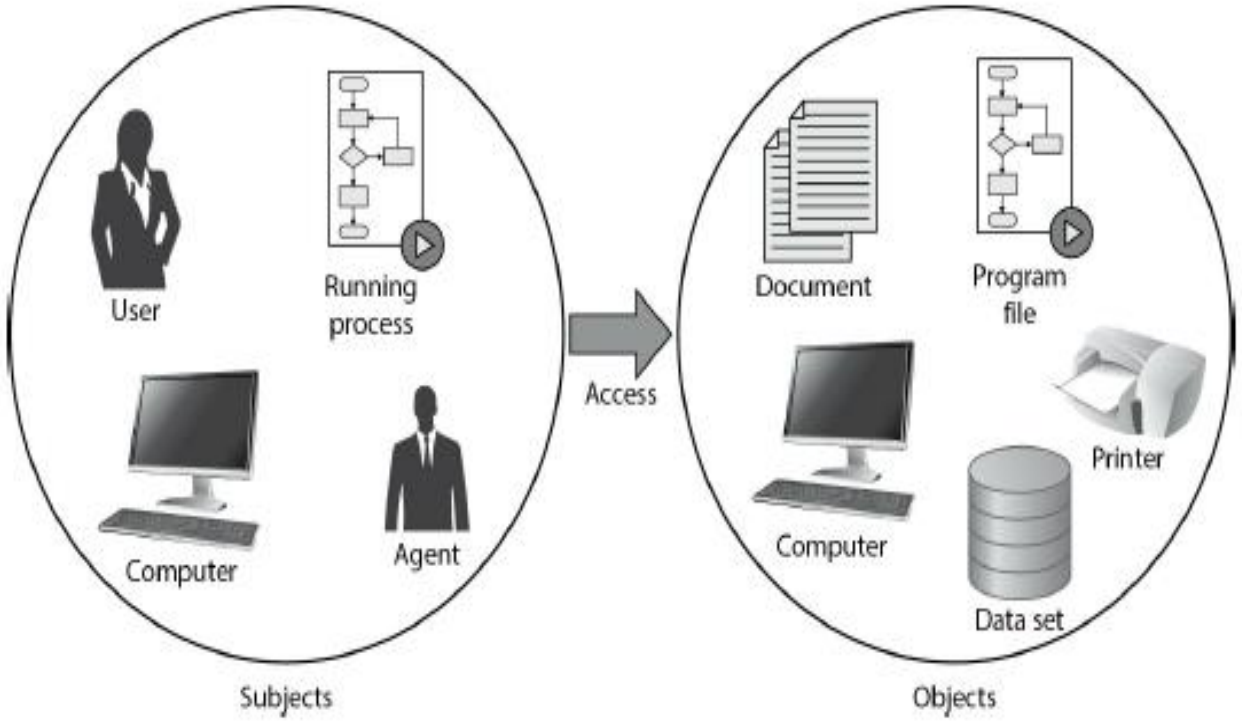
- **Authentication (AuthN):** Who goes there?
  - Verify that a person is who they claim to be
  - Identification and authentication are related but not the same
  - Determine whether access is allowed
  - Authenticate human to machine, machine to machine
  - This is where multi-factor authentication comes into play



Access Management

Authorization – Determining whether a subject is eligible to gain access to a resource or service.

- Two parts to access control. Let's Define another term
- **Authorization (AuthZ):** Are you allowe do that?
  - Once you have access, what can you do?
  - Enforces limits on actions
  - Single Sign On/Reduced Sign On
  - Security Policies
  - Access Control Lists
  - Capabilities
  - Restrictions on actions of authenticated users
- Note: Access control often used as synonym for authorization



Access Management – In simple Term

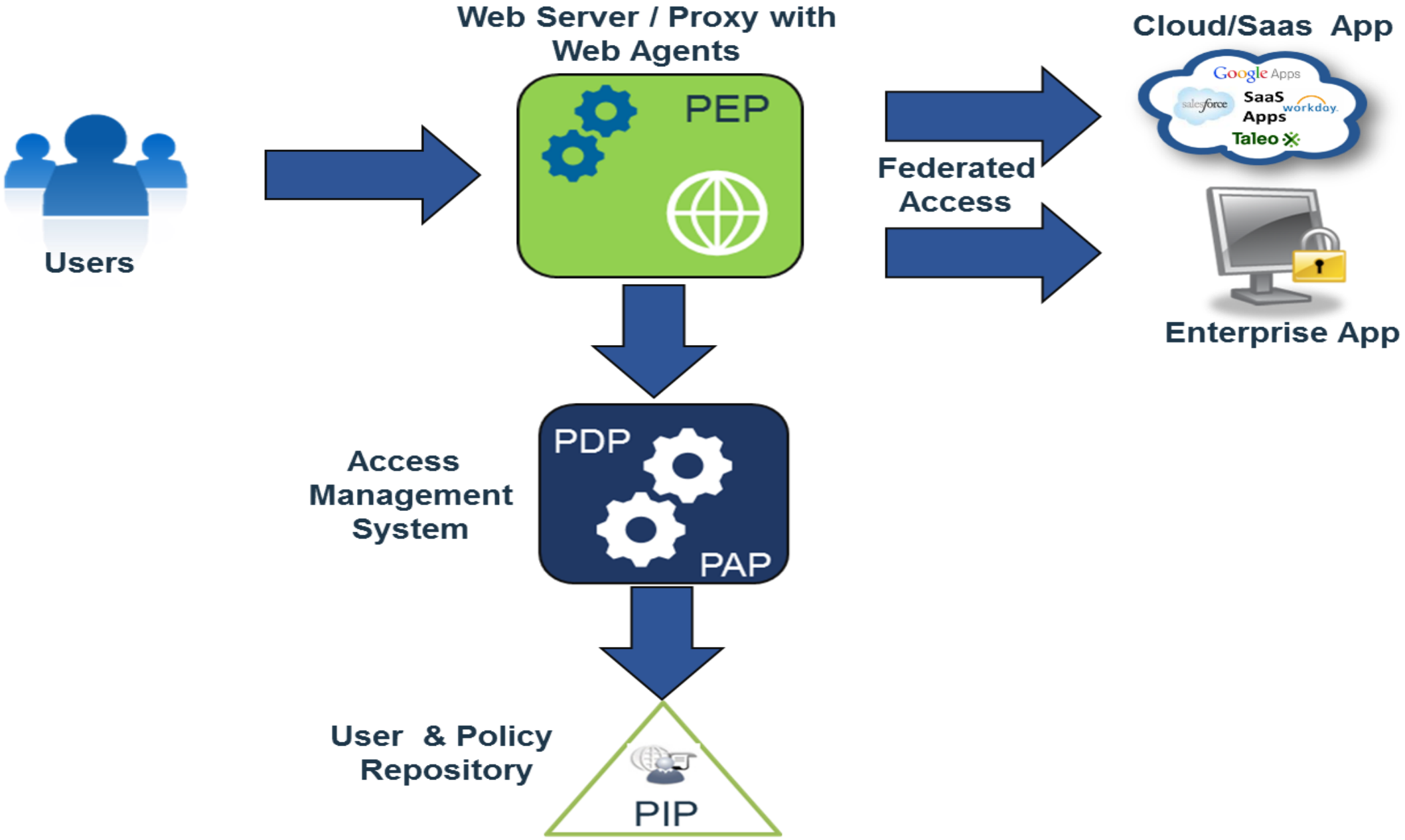
- “Hi! I’m Asha.” (*Identity*)
- “…and here’s my UserID / password to prove it.”

  (*Authentication*)
- “I want to do some financial approval.”

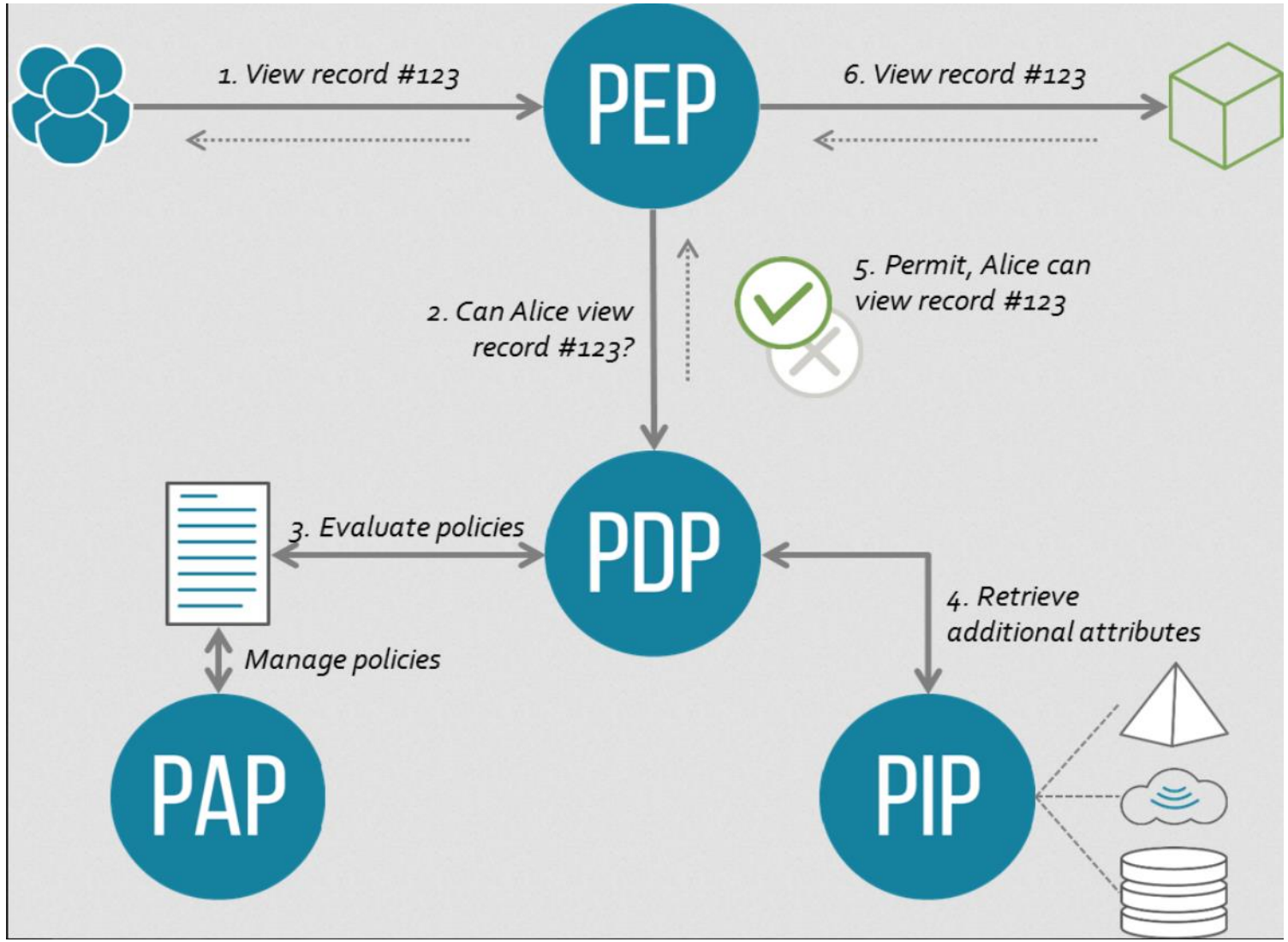
  (*Authorization* ☺: Allowing Asha to use the services for which she’s authorized)
- “And I want to change my grade in last semester’s Statistics course.”

  (*Authorization* ☹: Preventing her from doing things she’s not supposed to do)

Access Management System



Access Management with Policies



Purpose:

- Enforce security policies by gating access to, and via identification, authentication, & authorization processes

Functions:

- Access control monitoring and enforcement: Policy Enforcement Point/Policy Decision Point/ Policy Administration Point
- Identification and authentication mechanisms, including verification of secrets, MFA
- Authorization mechanisms, to include attributes, privileges, and permissions
- Enforcement mechanisms, including failure handling, bypass prevention, banners, timing and timeout, event capture etc

Access Management Use Cases

Authentication & Authorization
Identify users based on supplied credentials and allow/deny access based on configured policies

Single Sign On
Log in once and access all authorized application without additional login

Multifactor Authentication
Require more than on factor of application for authentication

Risk Based Authentication
Dynamically applying additional controls based on risk score captured on non standard context

Session Management
Manage active and inactive sessions and terminate sessions as needed

Federation
A trust based authentication mechanism that can span across enterprise boundaries. Supports federation standards SAML, OAuth, OpenIDConnect, WS-Fed etc

Basis of Identification (Factors)

- Something you know…
  - Passwords, PINs, Secret or key
- Something you possess…
  - Physical devices: magnetic cards, smart cards, tokens, bluetooth, password generators, cellphones…
- Something you are…
  - Biometrics (fingerprints, iris recognition, voice, handwriting), keyboarding characteristics
- Others
  - Someplace you are… (e.g. GPS location)
  - Some way you behave
- Ideally, more than one factor (Two-factor authentication)
- In some applications real-time identification is required

Password Attacks

- Replay attacks
  - Observe typing, find written or in another system, key loggers
  - Eavesdropping on a cleartext or hashed communication channel
- Exhaustive search
  - Randomly or systematically trying passwords against online verifier
  - Offline search against password file – enough that one user chose a weak password
- Password guessing
  - Assumes that not all passwords are equally likely
- Attack password distribution
  - Some systems come with fixed out-of-the-box passwords
- Many tools for password cracking/auditing

Multi Factor Authentication Overview

Multi factor authentication requires the use of at least two of the multiple authentication factors: Something only the user:

- Knowledge Factors (Knows) like password, PIN, secret answer
- Possession Factor (Has) like ATM card, mobile phone, hard token
- Inherence Factors (Is) like fingerprint or biometric – iris etc

13

Multi Factor Authentication

"Something You Know....."

- User Id & Password
- PIN (Personal Identification Number)
- Account Number
- Certificates

"Something You Have...."

A Token which is in the sole possession of the valid owner, and of which only one physical copy exists.

USB Token

Smart Cards

Tokens

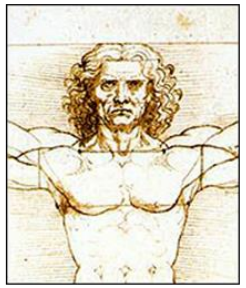
Multi-Function Devices

OTP Token

"Something You Are...." Biometrics

Retinal Scan

Finger Print Recognition



Voice Recognition

Authentication Categories

Who You Are Biometric	What you know	What you have	What you Do	Context

Physical Biometric
• Immutable and unique
• Facial recognition
• Iris Scan
• Retinal Scan
• Fingerprint Palm Scan
• Voice
• Liveliness biometric factors include Pulse. Captcha etc
Behavioral Biometric
• based on person's physical behavioural activity patterns
• Keyboard signature
• Voice
	• User Name and Password (UN/PW), A passphrase, a PIN
	• Very often used alone or in combinations with KBA methods.
	• Knowledge Based Authentication (KBA)
	  • Static KBA
	  • Dynamic KBA
		• One Time Password (OTP)
		• Smart card
		• X.509 and PKI
		• Rarely used alone
		• Used in combination with UN/PW and a PIN
			• Browsing patterns
			• Time of access
			• Type of device
			• Used in Combination with other methods
				• Location; Time of access;
				• Subscriber identity module (SIM)
				• Frequency of access;
				• Source and endpoint identity attributes such as
				• Used in Combination of other methods

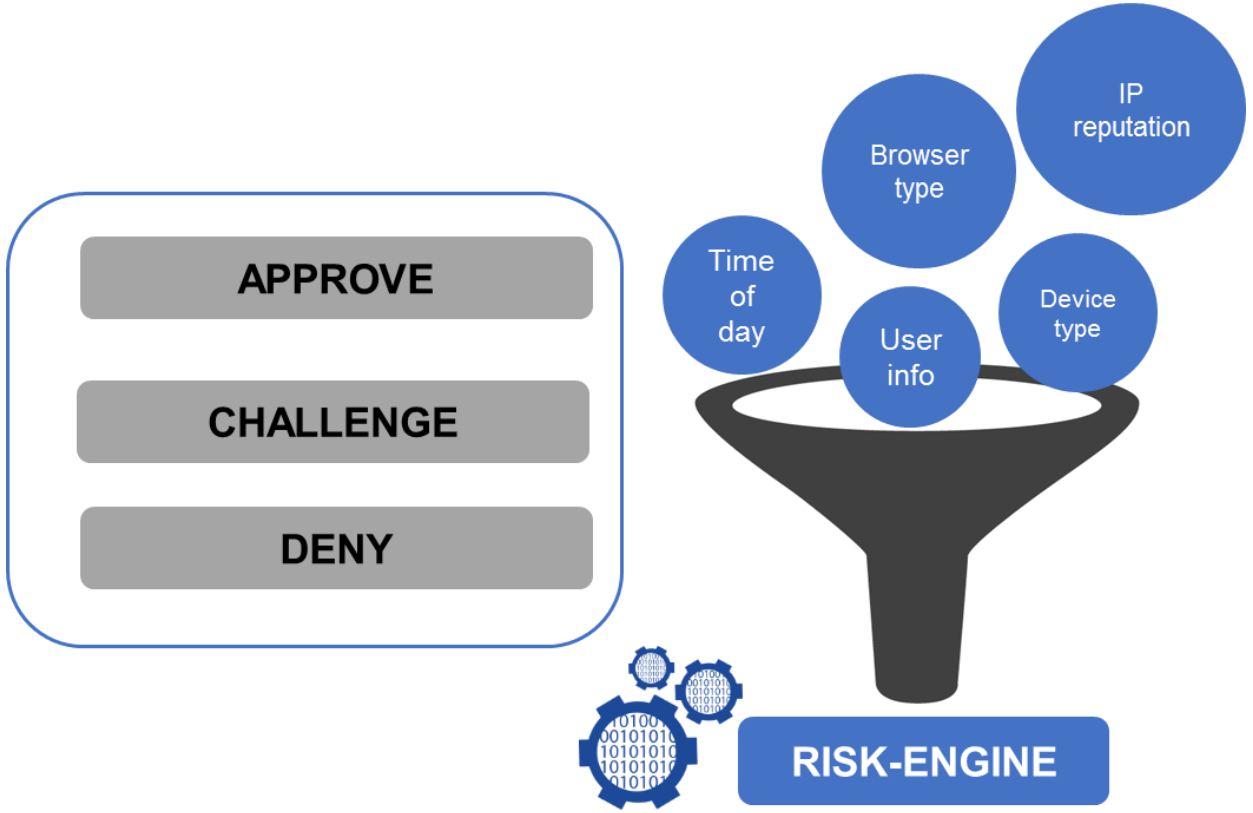
Why risk-based authentication?

No matter what level of security you require…

…**risk-based authentication** is the most basic step towards increasing security without compromising user convenience.

Adapt and enforce access based on risk

- Risk-based authentication, sometimes called adaptive authentication
- Described as a matrix of variables whose combination results in a risk profile.
- Based on that risk profile, additional authentication requirements may be added before certain functions can be performed



Single Sign on Definition

Why Single Sign On

- Multiple systems typically require multiple sign-on dialogues
  - Eg. Desktop logon, email, Application systems, external resources
  - Multiple sets of credentials
  - Presenting credentials multiple times
- Headache for administration and users
- The more security domains, the more sign-ons required

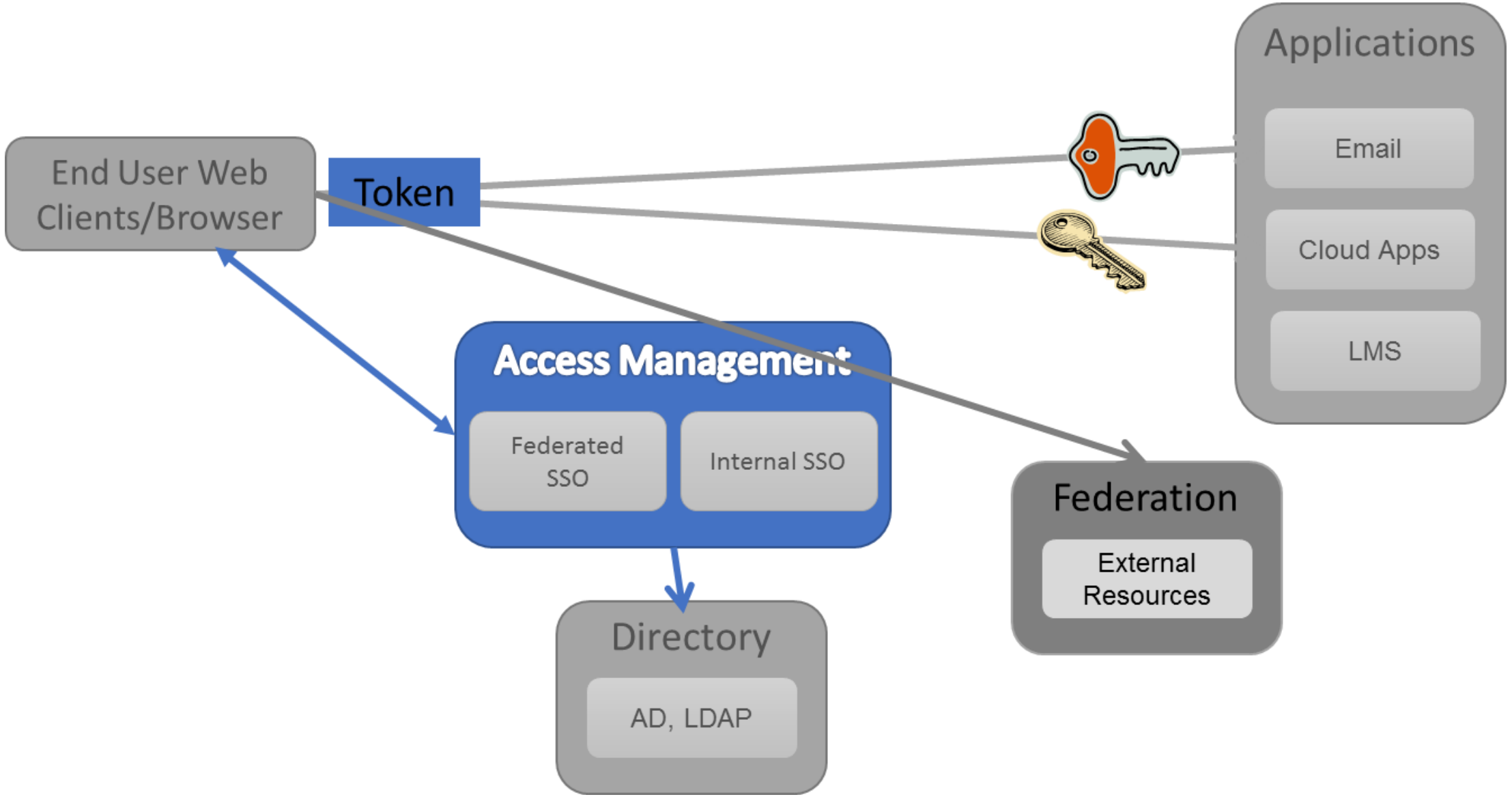
SSO

- Fantasy
  - One Password For Everything!
- Reality
  - Most Systems And Applications Already Have Their Proprietary Login Functionality
  - Reduced Logins For Discreet Systems
    - Corporate Systems
    - Shared Intranet/Web Applications
    - Web Logon Aggregators

Single Sign-on Business Requirements

- Is There A Problem Here?
  - Mushrooming Passwords
  - Need For Re-use
  - “Sticky Note” Password Cache
  - Unencrypted Text Files On Laptops and PDAs
- Deceptively Intuitive
  - Reduce Costs
  - Increase Security
  - Increase Efficiency
  - Increase Convenience
  - My Boss Told Me I Have To
- Be Honest About the Cost / Benefit Analysis
  - Use Hard Numbers
    - What Does it Cost to Reset a Password?
    - How Much Time is Spent Logging into Multiple Systems Each Morning?
    - What is The Real Cost of Integration?
    - Will Additional Authentication Methods Need to be Purchased?

Single Sign On



Other considerations

- Most SSO systems are HTTP based
  - Browser cookies (restricted to the authentication domain)
  - HTTP redirects
  - Placement of tokens in querystring
- May require integration with application
  - Agent-based architecture
  - SSO protocol
- Needs to interface with authentication system
- Needs protocol between authentication domain and target application
  - Token/ticket-based
  - SAML POST/artifact profiles

SSO dependencies

- SSO system relies on other infrastructure
  - Authentication system
  - Requires interface with web server
  - Identity management/registration
- Need to provide for authorisation
  - Applications often need more than just authentication information
  - Attribute information
  - Shibboleth or other architectures

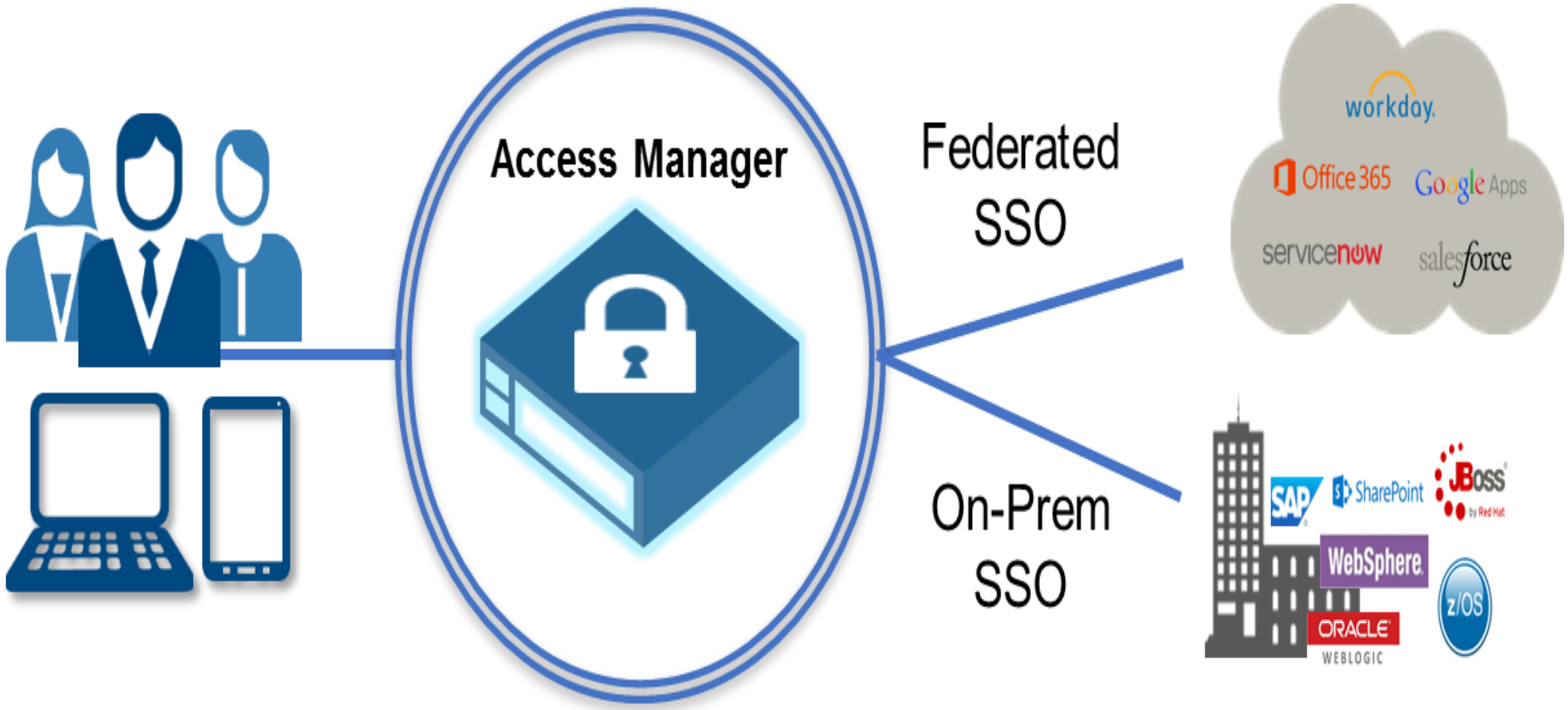
Federation

- A *federated identity* is a portable identity, and its associated entitlements, that can be used across business boundaries.
- It allows a user to be authenticated across multiple IT systems and enterprises.
- Identity federation is based upon linking a user's otherwise distinct identities at two or more locations without the need to synchronize or consolidate directory information.
- Federated identity offers businesses and consumers a more convenient way of accessing distributed resources and is a key component of e-commerce.

Federated Identity Management

- Federation: An association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions.
- All participants in a federation agree on the same policies and procedures related to identity management and the passing of attributes.
- Instead of one-to-one relationships, the federation allows one-to many relationships.
- Parties agree to leverage the identity provider’s database, rather than creating separate data stores
- Identity provider does the authentication; service provider does the authorization
- Attributes are the key – maintain privacy and security

Manage access in the world of hybrid cloud thru Federation Standards



Federation vs FIDO

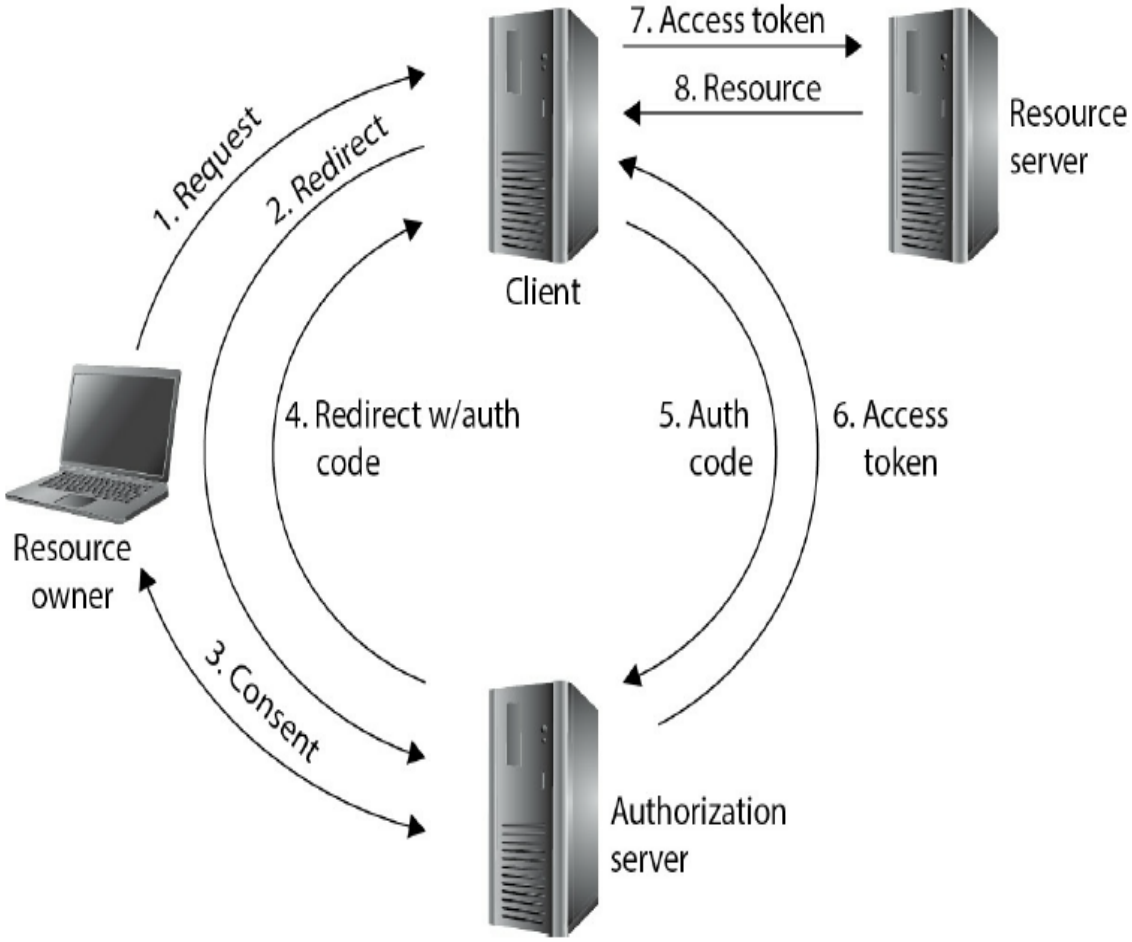
- Federation and FIDO. Fortunately these two technologies — are complementary.
- FIDO and federation technology have some things in common.
- FIDO authentication capability is amplified by a federated system, where the federation system extends the benefits of a FIDO authentication to applications and services without requiring FIDO to be directly integrated with those applications.
- Both seek to simplify the end - user's experience in authenticating to applications provided my multiple
- But there are also significant differences between the two – an important one being the trust model that is defined in their scenarios

SAML

- Security Assertion Markup Language (SAML) is a product of the OASIS Security Services Technical Committee.
- Dating from 2001, SAML is an XML-based open standard for exchanging authentication and authorization data between parties.
- The SAML specification defines three roles:
  - The principal, which is typically the user looking to verify his or her identity
  - The identity provider (idP), which is the entity that is capable of verifying the identity of the end user
  - The service provider (SP), which is the entity looking to use the identity provider to verify the identity of the end user

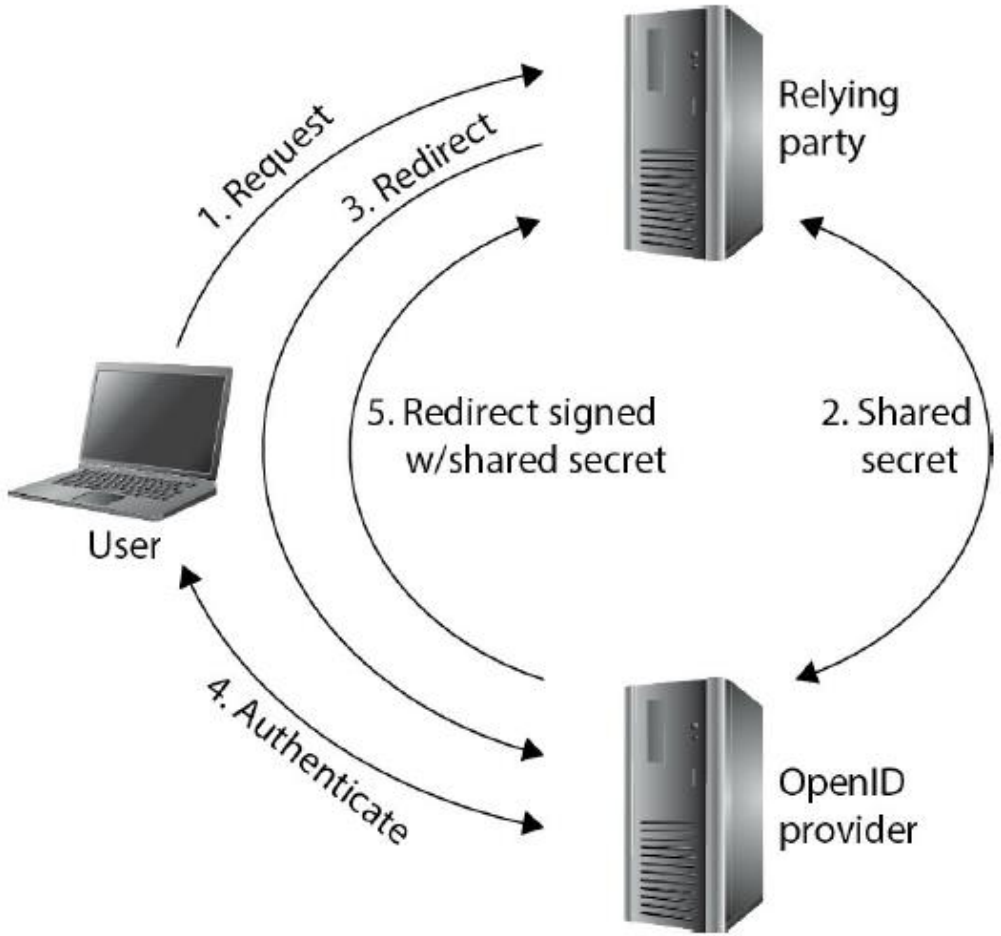
OAuth

- *OAuth* is an open standard for authorization (not authentication) to third parties.
- OAuth is different than OpenID and SAML in being exclusively for authorization purposes and not for authentication purposes.
- The OAuth specifications define the following roles:
  - The end user or the entity that owns the resource in question
  - The resource server (OAuth Provider), which is the entity hosting the resource
  - The client (OAuth Consumer), which is the entity that is looking to consume the resource after getting authorizatic from the client
- OAuth solves a different but complementary problem than OpenID:
  - instead of a third party allowing a user to access a websit a user allows a website to access a third party.



OpenID

- OpenID is an open standard sponsored by Facebook Microsoft, Google, PayPal, Ping Identity, Symantec, and Yahoo.
- OpenID allows user to be authenticated using a third- party services called identity providers.
- Users can choose to use their preferred OpenID providers to log in to websites that accept the OpenID authentication scheme.
- The OpenID specification defines three roles:
  - The end user or the entity that is looking to verify its identity
  - The relying party (RP), which is the entity looking to verif the identity of the end user
  - The OpenID provider (OP), which is the entity that registers the OpenID URL and can verify the end user's identity



Session Management

- A *session* is an agreement between two parties to communicate interactively
- Information systems use sessions all the time.
- When you show up for work and log onto your computer, you establish an authenticated session with the operating system that allows you to launch your e-mail client.
- Session management is the process of establishing, controlling, and terminating sessions, usually for security reasons.
- The session establishment usually entails authentication and authorization of one or both endpoints.
- If the session is an authenticated one, then authentication happens at the beginning and then everything else is trusted until the session ends.
- That trust is the reason we need to be very careful about how we deal with our sessions
- The SSO application maintains a session
- The target application usually maintains a session
- Logging out of the target application may not log you out of the SSO application
- Single Sign-On ⇒ Single Sign-Out!
  - Application specific

Session Management

Timeout

- When sessions are established, the endpoints typically agree on how long they will last.
- Be careful to make this time window as short as possible without unduly impacting the business

Inactivity

- Some sessions could go on for very long periods of time, provided that the user is active.
- Sessions that are terminated for inactivity tend to have a shorter window than those that are triggered only by total duration (i.e., timeout).

Anomaly

- Anomaly detection is an additional control added to a session that is triggered by timeouts or inactivity (or both).
- This control looks for suspicious behaviors in the session, such as requests for data that are much larger than usual or communication with unusual or forbidden destinations.
- These can be indicators of session hijacking.

The Importance of Segregation / Separation of Duties

Segregation of Duties means that tasks, system accesses, and access to physical assets are assigned so that no one individual is able to control multiple stages of a process or sub-process

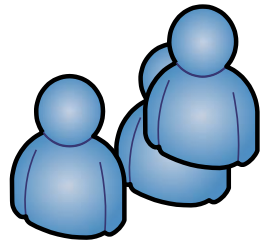
- In general, an employee should not be permitted to perform activities which combine the following:
  - Authorization/approval
  - Recording
  - Processing
  - Custody
  - Reporting/reconciliation

- In addition, an employee should not be permitted to have system accesses that combine conflicting tasks in the following roles:
  - Development
  - System administrator
  - Security administrator
  - Business process user

- A Segregation Of Duties (SOD) assessment is an internal control which provides management with reasonable assurance that no one individual has responsibilities or accesses that would allow employees to misuse or divert company assets.

Example: SoD and IT

- IT relies on RBAC for SoD and compliance
- SoD items include
  - Identification of a requirement (business)
  - Authorization and approval (governance)
  - Design and development (developer)
  - Review, inspection, and approval (separate developer)
  - Implementation (systems administrators/operations)
- Successful SoD implementation includes
  - Align authorization rights with organizational role
  - Align authentication method with value of data
  - Watch the watchers



Separation
Of Duties

- Critical for internal controls
- Implements checks and balances on individuals
- Reduces danger/risk of individual actions
- Can be difficult and expensive to implement
- Separate or Compensate
- Bread and butter of audit/compliance

Thank You