



SEC+

Lesson 4: Implement Identity And Access Management

Objectives

- Implement password-based and multifactor authentication
- Implement account policies and authorization solutions
- Implement single sign-on and federated identity solutions

Lesson 4

Topic 4A

Authentication



Authentication Design

- Meet requirements for confidentiality, integrity, and availability
 - Keeps credentials secure (confidentiality)
 - Threat actors cannot bypass or subvert the authentication mechanism (integrity)
 - Mechanism does not cause undue delay or support issues (availability)
- Something you know: knowledge factor
 - Password
 - Personal identification number (PIN)

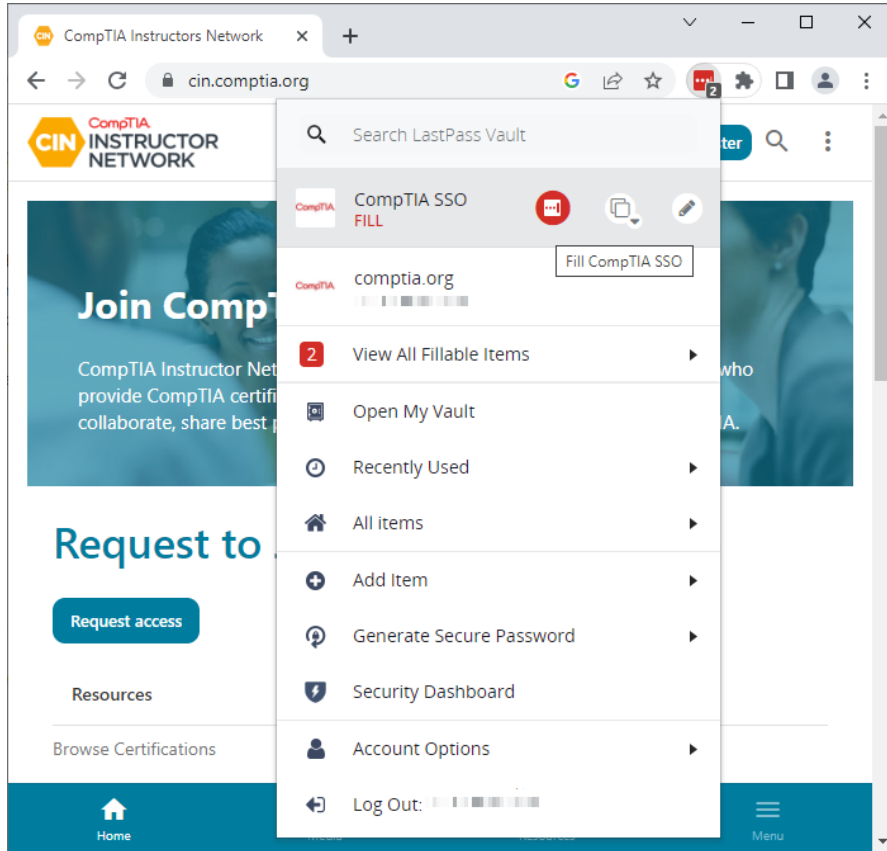


Screenshot used with permission from Microsoft.

Password Concepts

- Length
- Complexity
 - Character combinations
- Aging
- Reuse and history
 - Expiration
- NIST guidance
 - Password hints

Password Managers



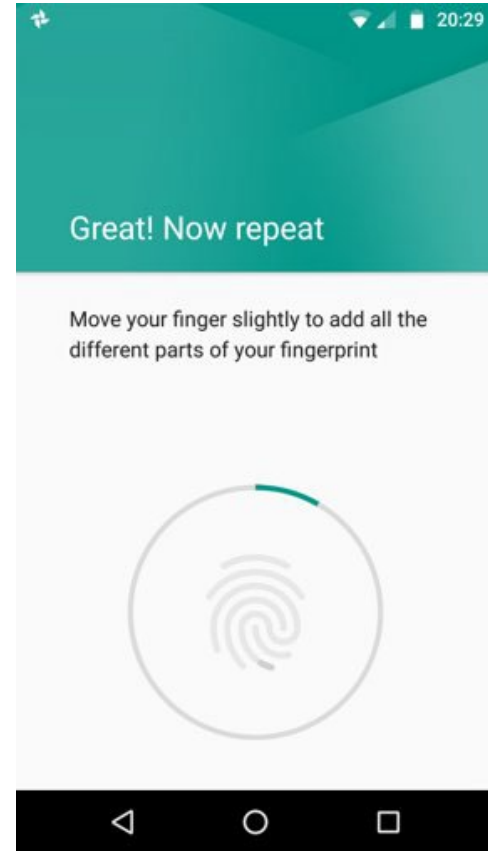
- Vault and master password
 - Built-in OS/browser password managers
 - Third-party cloud/plug-in
- Per-site password generation
- Secure filling

Multifactor Authentication

- Multifactor authentication (MFA)
 - Something you KNOW and something you HAVE
 - NOT something you KNOW and something else you KNOW
- Something you have
 - Ownership factor: hardware tokens and fobs
- Something you are/do
 - Biometric factor: fingerprint and facial scans
- Somewhere you are
 - Geolocation via location services
 - IP/network location

Biometric Authentication

- Enrollment
 - Sensor and feature extraction
 - Sensor/camera types
- Efficacy rates and considerations
 - False Rejection Rate (FRR) or Type I error
 - False Acceptance Rate (FAR) or Type II error
 - Throughput, cost, and inaccessibility
- Fingerprint recognition
- Facial recognition



Android is a trademark of Google LLC.

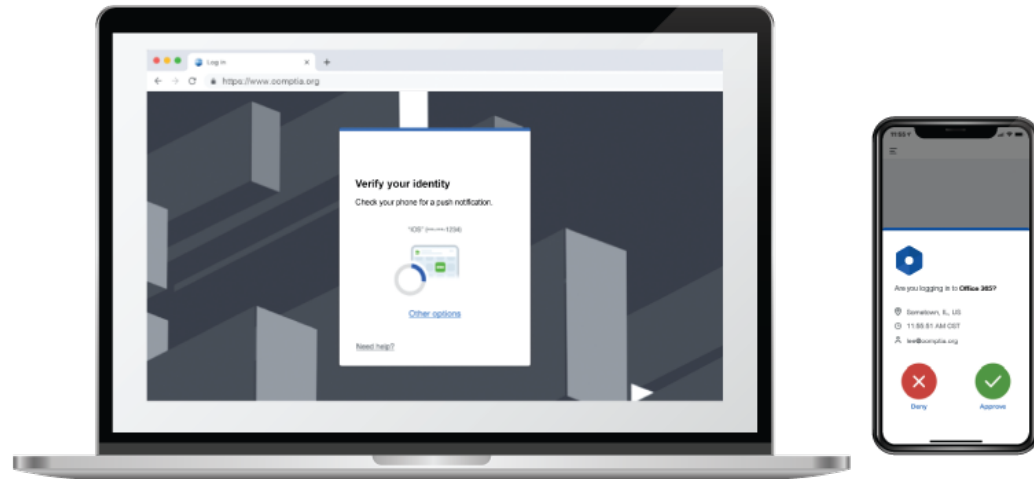
Hard Authentication Tokens



- Token generation types
 - Certificate-based (requires PKI)
 - One-time password (OTP)
 - Fast Identity Online (FIDO) Universal 2nd Factor (U2F)
- Authenticator form factors
 - Smart card
 - One-time password (OTP) fob
 - Security key
 - Activation method to show presence

Soft Authentication Tokens

- Transmit a code via an out-of-band channel
 - Short message service (SMS)
 - Email account
 - Phone call
 - Push notification
- Authenticator app
- Possibility of interception



Passwordless Authentication

- Rely on authenticator rather than password
 - Accounts identified by public/private key pair, but doesn't have to use PKI
 - Private key stored only on authenticator
 - Authenticator can require biometric or PIN proof of presence (local gesture)
- Attestation
 - Verify authenticator as root of trust

Authentication

- Authentication design
 - Something you know/are/have
- Password concepts and password managers
- Multifactor authentication
- Biometric authentication
- Hard authentication tokens
 - Smart cards, OTP generators, FIDO U2F
- Soft authentication tokens
 - Two-step verification
- Passwordless authentication

Lab Activity

- Assisted Lab Managing Password Security

Lesson 4

Topic 4B

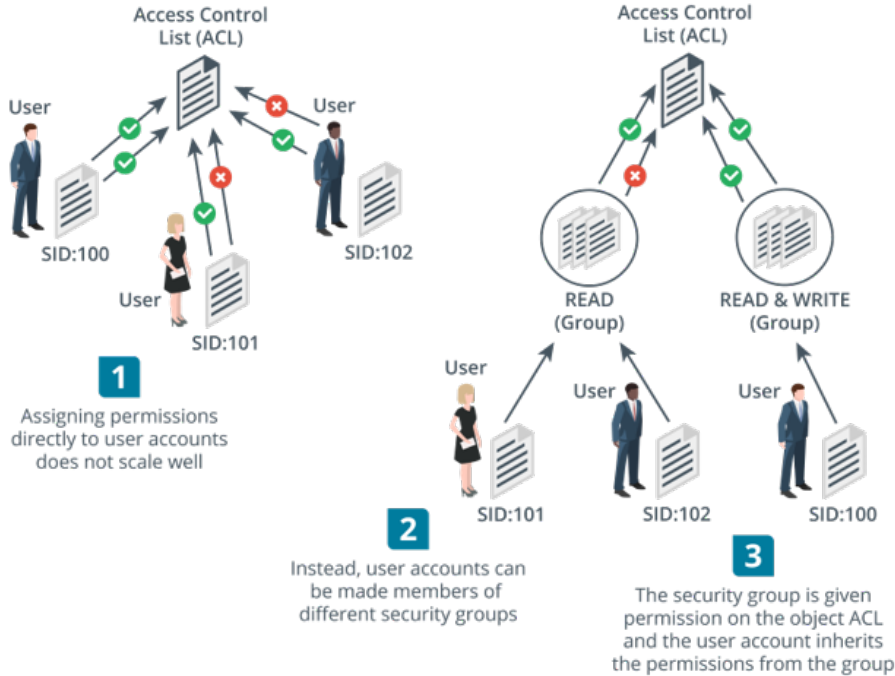
Access Management



Discretionary and Mandatory Access Control

- Access control model determines how users receive permissions/rights
- Discretionary Access Control (DAC)
 - Based on resource ownership
 - Access Control Lists (ACLs)
 - Vulnerable to compromised privileged user accounts
- Mandatory Access Control (MAC)
 - Labels and clearance
 - System policies to restrict access

Role-based and Attribute-Based Access Control



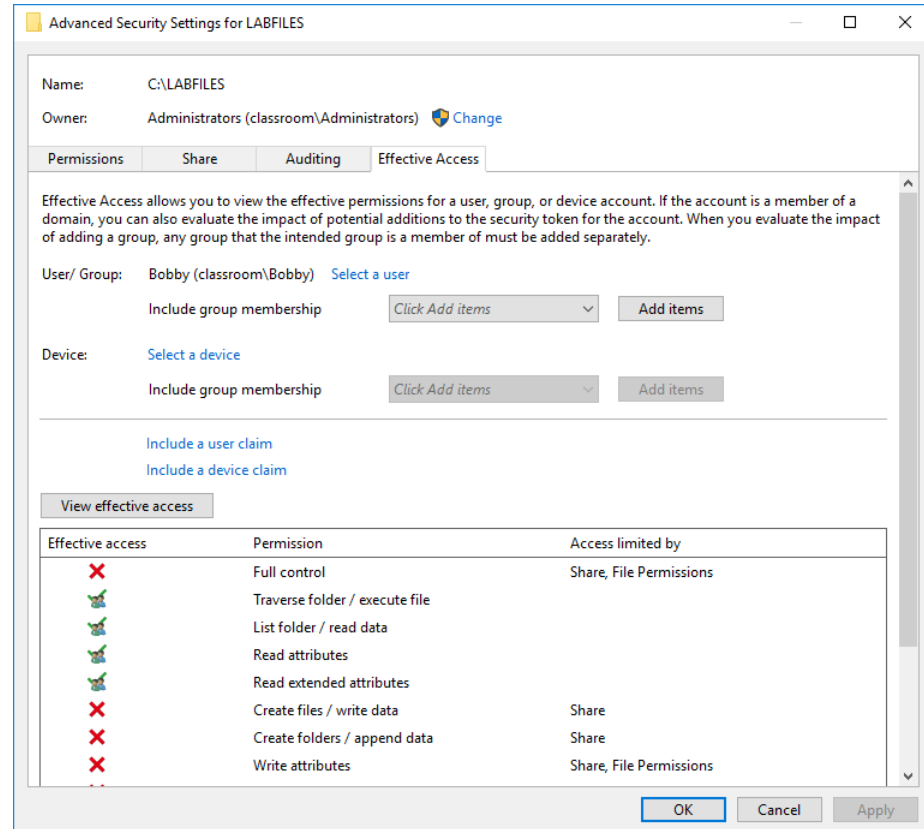
- Role-Based Access Control (RBAC)
 - Non-discretionary and more centralized control
 - Based on defining roles then allocating users to roles
 - Users should only inherit role permissions to perform particular tasks
- Security groups
 - Assign permissions to security groups and assign user accounts to relevant groups
 - Groups can be mapped to roles
- Attribute-Based Access Control (ABAC)
 - Access decisions based on a combination of subject and object attributes plus any context-sensitive or system-wide attributes

Rule-Based Access Control

- Non-discretionary
 - System determines rules, not users
 - MAC, RBAC, and ABAC
- Conditional access
 - Continual authentication
 - User account control (UAC) and sudo

Least Privilege Permission Assignments

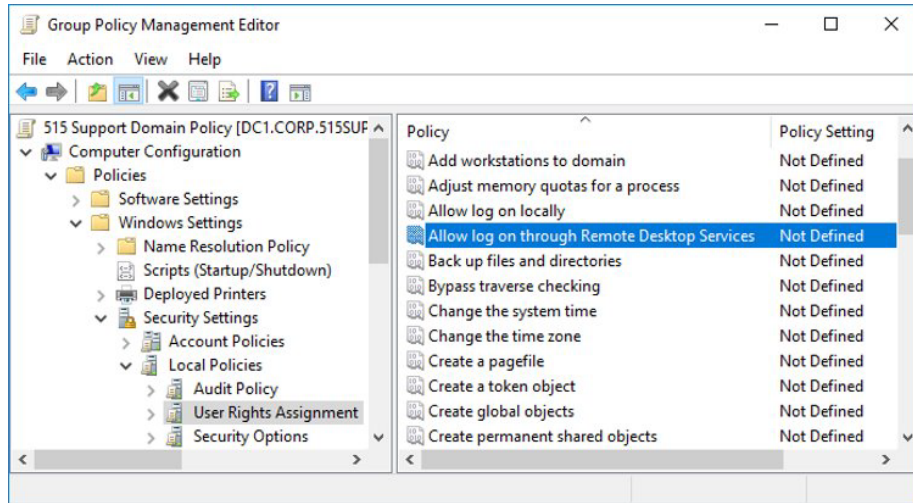
- Principle of least privilege
 - Sufficient permissions only
- Implications
 - Insufficient permissions
 - Authorization creep
 - Auditing



User Account Provisioning

- Provisioning
 - Identity proofing
 - Issuing credentials
 - Asset allocation
 - Policy awareness and security education
 - Permission assignments and implications
- Deprovisioning
 - Employees or contractors leaving company or project, or changing roles
 - Remove or disable permission assignments

Account Attributes and Access Policies



Screenshot used with permission from Microsoft.

- Account attributes
 - Security identifier (SID, account name, credential)
 - Extended profile attributes
 - Per-app settings and files
- Access policies
 - File permissions
 - Access rights
 - Active Directory Group Policy Objects (GPOs)

Account Restrictions

- Location-based policies
 - Network/logical location
 - Geolocation
 - By IP address
 - By Location Services
- Time-based restrictions
 - Logon hours
 - Logon duration
 - Impossible travel time/risky login
 - Temporary permissions

Privileged Access Management

- Policies, procedures, and technical controls to prevent the malicious abuse of privileged accounts
 - Accounts with system-wide access
 - Secure administrative workstations
- Policies for zero standing privileges for administrators
 - Temporary elevation
 - Password vaulting/brokering
 - Ephemeral credentials

Access Management

- Discretionary and mandatory access control
- Role-based and attribute-based access control
- Rule-based access control
- Least privilege permission assignments
- User account provisioning
 - Identity proofing, secure credentials, asset allocation, policy/awareness training, permissions assignments
- Account attributes and access policies
- Account restrictions
 - Location- and time-based
- Privileged access management
 - Zero standing privileges and ephemeral/vaulted credentials

Lab Activity

- Assisted Lab: Managing Permissions

Lesson 4

Topic 4C

Identity Management



Local , Network, and Remote Authentication

- Authentication providers
 - Passwords versus password hashes
- Windows authentication
 - Local sign-in
 - Network sign-in (Kerberos and NTLM)
 - Remote sign-in
- Linux authentication
 - /etc/passwd and /etc/shadow
 - Pluggable authentication modules (PAMs)

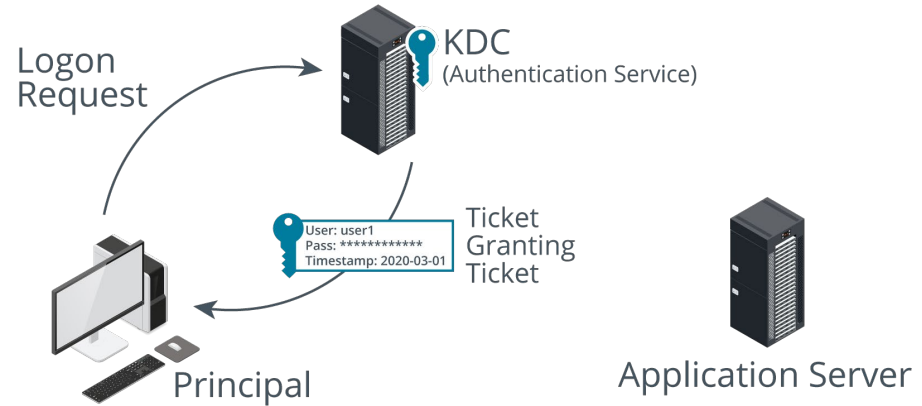
Directory Services

- Database of subjects
 - Users, computers, security groups/roles, and services
- Access Control Lists (authorizations)
- X.500 and Lightweight Directory Access Protocol (LDAP)
 - Distinguished names
 - Attribute=Value pairs

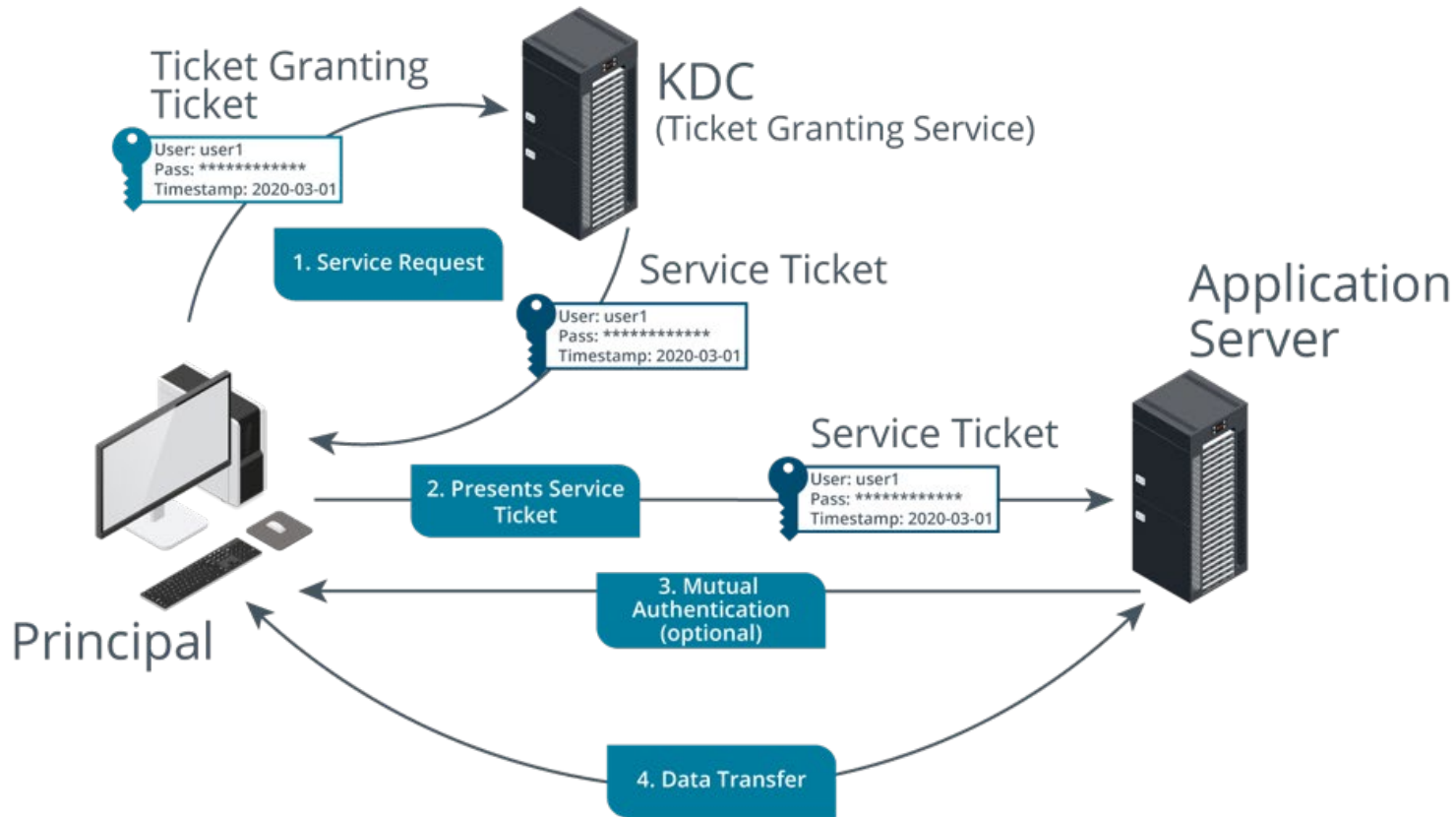
CN=WidgetWeb, OU=Marketing, O=Widget, C=UK, DC=widget, DC=foo

Single Sign-on Authentication

- Kerberos
 - Clients
 - Application servers
 - Key Distribution Center (KDC)
- Authentication Service – Ticket Granting Ticket
- Ticket Granting Service – Service Ticket

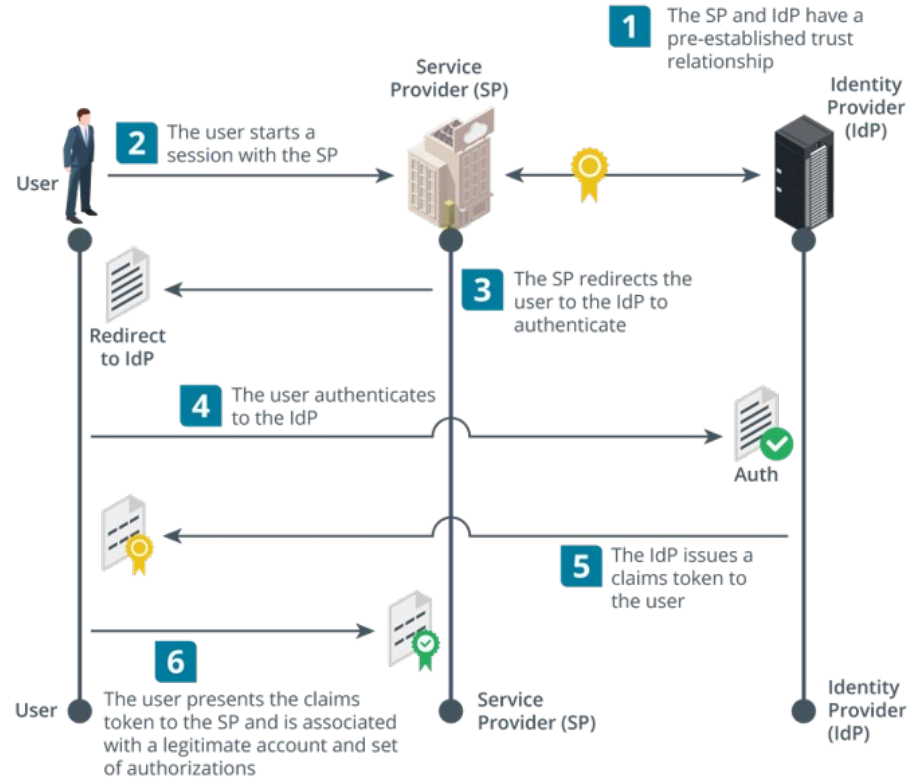


Single Sign-on Authorization



Federation

- Networks under separate administrative control share user identities
- Identity providers and claims
- Interoperability
 - Service providers and identity providers
 - Shared frameworks and protocols



Security Assertion Markup Language

- Open standard for implementing identity and service provider communications
- Attestations/assertions
 - XML format
 - Signed using XML signature specification
- Communications protocols
 - HTTPS
 - Simple Object Access Protocol (SOAP)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="200"
Version="2.0"
IssueInstant="2020-01-01T20:00:10Z"
Destination="https://sp.foo/saml/acs" InResponseTo="100".
<saml:Issuer>https://idp.foo/sso</saml:Issuer>
<ds:Signature>...</ds:Signature>
<samlp:Status>...(success)...</samlp:Status>
<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="2000" Version="2.0"
IssueInstant="2020-01-01T20:00:09Z">
<saml:Issuer>https://idp.foo/sso</saml:Issuer>
<ds:Signature>...</ds:Signature>
<saml:Subject>...
<saml:Conditions>...
<saml:AudienceRestriction>...
<saml:AuthnStatement>...
<saml:AttributeStatement>
  <saml:Attribute>...
  <saml:Attribute>...
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

Open Authorization

- “User-centric” federated services better suited to consumer websites
 - Representational State Transfer (REST) Application Programming Interfaces (APIs) (RESTful APIs)
 - Framework for implementation not a protocol
- OAuth
 - Designed to communicate authorizations, rather than explicitly authenticate a subject
 - Client sites and apps interact with OAuth IdPs and resource servers that hold the principal’s account/data
 - Different flow types for server to server or mobile app to server
 - JavaScript object notation (JSON) web token (JWT)

Identity Management

- Local, network, and remote authentication
- Directory services
 - LDAP and distinguished name attributes
- Single sign-on authentication and authorization
 - Kerberos
- Federation
 - Identity providers and service providers
- Security Assertion Markup Language
- Open authorization (OAuth)

CompTIA Security+ Exam SY0-701

Lesson 4



Summary