CISSP Domain 5 — Identity and Access Management

Domain 5 — Identity and Access Management

Powerful system accounts are obvious targets: `root` on UNIX-family, `Administrator` on Windows.

Built-in Windows accounts

The final number is what matters.

SID: S-1-5-21domain-**500**
Name: Administrator
SID of *-500 is Local Administrator, regardless of any renaming.

SID: S-1-5-21domain-**501**
Name: Guest
Should be disabled, or carefully monitored

SID: S-1-5-21domain-**512**
Name: Domain Admins
More powerful, like Administrator across several machines simultaneously.

Biometric failure modes

You either know the exact passphrase or you don't. Or, you have the needed physical token or you don't. But with biometrics, the system always has to conclude "close enough". So, there will be errors. You must know them by two sets of names.

False Rejection or Type I: Failure to recognize the legitimate user.

False Acceptance or Type II: Erroneously allowing an imposter in.

Crossover Error Rate: You have adjusted the thresholds so the False Rejection and False Acceptance error rates are equal.

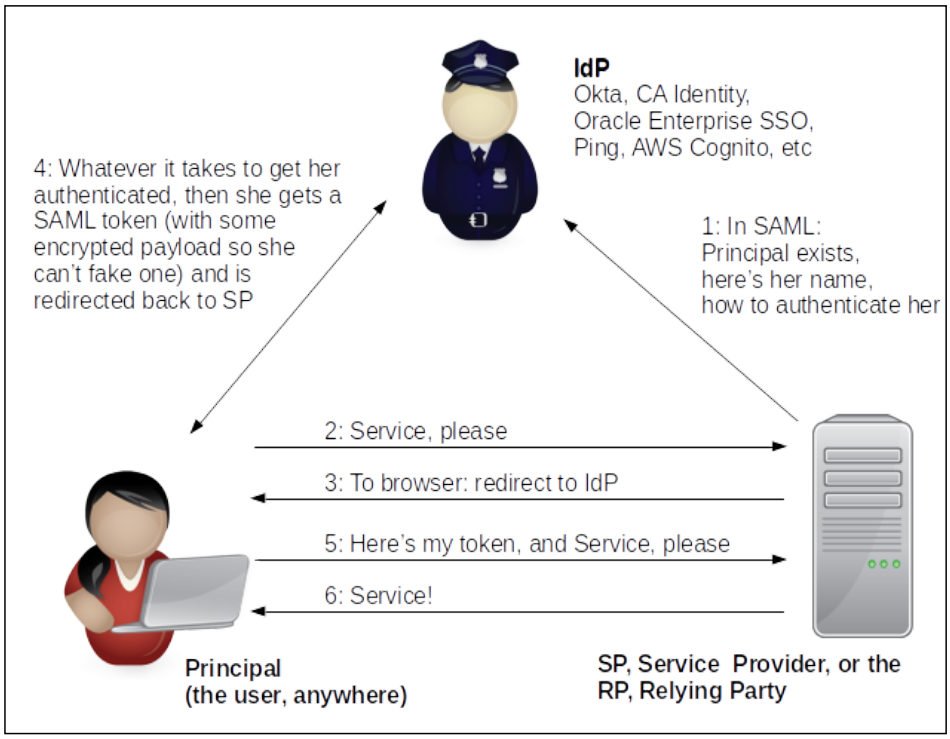
Identity Assurance

- **IAL1:** Attributes are self-asserted and should not be trusted.
- **IAL2:** Either remote or in-person identity proofing is required.
- **IAL3:** In-person identity proofing is required. Identifying attributes must be verified by an authorized Credential Service Provider or cSP.
    - **Authenticator Assurance Level or AAL:** Refers to the authentication process
    - **Federation Assurance Level or FAL:** Refers to the strength of an assertion in a federated environment

IAM Protocols for Federated Environments

SAML defines an XML framework. It **focuses on authentication** (and some authorization).

Three roles:
Identity Provider or IdP
Service Provider or Relying Party
User or Principal



OAuth enables a 3rd-party application to obtain controlled access to an HTTP service. It **focuses on authorization.** This is what happens if you point your browser to Pinterest or Instagram, and that site offers the ability to sign in with your Google or Facebook credentials. Exam questions will probably focus on cases where social media is involved.

Four roles:
Resource owner
Resource server
Client application
Authorization server

Also know about **OpenID** and **WS-Federation.**

SAML and WS-Federation are more commonly used within an enterprise.

OAuth and OpenID are more commonly used across the Internet, between organizations.

Access Control Models

Know these:
Discretionary Access Control or DAC
Mandatory Access Control or MAC
Nondiscretionary Access Control or NDAC (simply all except DAC)
Role-Based Access Control or RBAC
Rule-Based Access Control or RBAC (confusing!)
Attribute-Based Access Control or ABAC (can use attributes of the user, the resource, the environment, etc)