

IAM | Ivan Notes 2022

▼ access control services

- identification

▼ authentication

▼ knowledge

- password
- passphrase
- questions

▼ ownership

▼ OTPs

- hard tokens
- soft tokens
- synchronous
- asynchronous

▼ characteristics - Biometric

▼ psychological

- fingerprint
- hand geometry
- vascular pattern
- facial
- iris
- retina

▼ behavioral

- voice
- signature
- key stroke
- gait (walk)

▼ Errors

- Type 1 - false reject
 - Type 2 - false accept
 - crossover error rate (CER)
- single/multifactor
- authenticator assurance levels (AAL)
- ▼ Authorization
 - ▼ discretionary (owner decides)
 - Rule
 - Role
 - Attribute / content
 - non-discretionary
 - mandatory (system decides)
- ▼ Accountability
 - principle of access control
- ▼ **SSO**
 - ▼ single sign-on, access systems within the same org
 - ▼ Kerberos
 - ▼ components
 - user/client
 - key distribution center
 - authentication service
 - TGT
 - ticket granting service
 - service tickets
 - service
 - symmetric encryption only
 - ▼ Sesame
 - symmetric & asymmetric encryption
- ▼ **Federation**
 - ▼ federated identity mgmt (FIM), access systems across multiple entities

- ▼ trust relationship
 - principal / user
 - identity provider
 - relying party / service provider
- ▼ SAML
 - tokens
 - assertions written in XML
 - ▼ components
 - profiles
 - bindings
 - protocol
 - assertion
- WS-federation
- OpenID
- OAuth

- **session management**

- ▼ **Access control principles**

- SoD
 - Need to know
 - Least Priv

- ▼ **Administration approaches**

- centralized
 - decentrazlied
 - hybrid

- ▼ **IDaaS Identities**

- cloud
 - synced
 - linked
 - federated