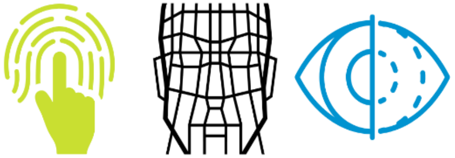
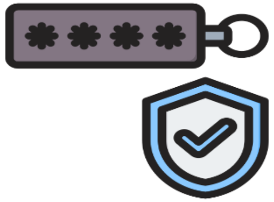
# Authentication Types Cheat Sheet

| Feature | Password-based Authentication | Certificate-based Authentication | Biometric Authentication | Token-based Authentication |
|---|---|---|---|---|
| | | |  |  |
| **Definition** | Uses a secret word or phrase known only to the user. | Uses digital certificates issued by a Certificate Authority (CA). | Uses unique biological characteristics of the user. | Uses physical or software tokens to generate a one-time password (OTP). |
| **Authentication Factor** | Something you know | Something you have | Something you are | Something you have |
| **Common Use Cases** | Online accounts, applications, systems | Secure communications, email encryption, VPN access | Access control systems, mobile devices, secure facilities | Online banking, two-factor authentication, secure systems |
| **Security Level** | Moderate | High | High | High |
| **Ease of Use** | Relatively easy | Moderate (requires certificate management) | Easy (after initial setup) | Moderate (requires possession of token) |
| **Vulnerability** | Susceptible to phishing, brute-force attacks, and password reuse | Susceptible to theft or loss of the certificate, certificate spoofing | Susceptible to spoofing or sensor hacking (though difficult) | Susceptible to theft or loss of the token, man-in-the-middle attacks |
| **Implementation Cost** | Low | High (requires infrastructure for PKI) | High (requires biometric hardware) | Moderate (cost of tokens and management) |
| **Scalability** | High | High | Moderate (depends on biometric hardware) | High |
| **Revocability** | Easy to change/reset | Moderate (requires revoking and reissuing certificates) | Difficult (biometric traits cannot be changed) | Easy to deactivate and replace tokens |
| **User Experience** | Users must remember passwords | Users must manage and store certificates | Users simply present biometric data | Users must carry and use a token |
| **Example Technologies** | Password managers, standard login forms | SSL/TLS certificates, smart cards | Fingerprint scanners, facial recognition systems | Hardware tokens, mobile authentication apps |