Infrastructure Security Using Linux

Computer science / Cybersecurity

Single Sign-On

17 →

Single Sign-On

Single Sign-On (SSO)

- *Allows users to access multiple systems with the same credentials*
  - Simplifies login across an environment
  - Widely needed by both users and administrators
- *SSO is based on two key concepts:*
  - **Identity**: Represents the user
    - Includes attributes like username, password, user ID, and email
  - **Authentication**: Proves ownership of the identity
    - Ensures the user is who they claim to be

Core SSO Elements

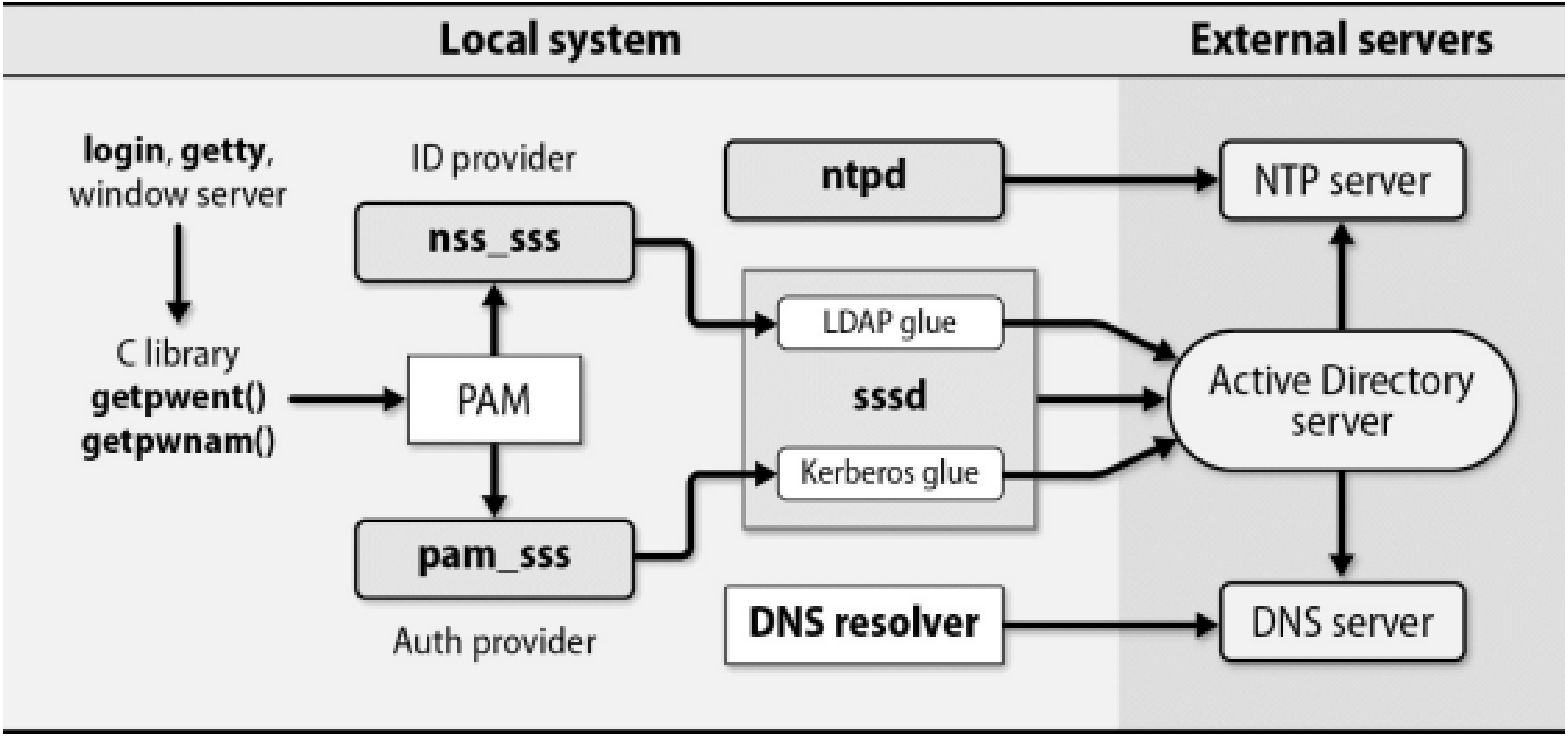
- *Four key components are required for implementing Single Sign-On:*

1. **Central Directory Store**
    1. Stores user identity and authorization data
    2. Commonly LDAP-based (e.g., OpenLDAP)
    3. Mixed environments often use *Microsoft Active Directory* (custom LDAP variant)
2. **User Management Tool**
    1. For LDAP: *phpLDAPadmin*, *Apache Directory Studio*
    2. For Active Directory: *Microsoft Management Console (MMC)*

1. **Authentication Mechanism**
    1. LDAP or *Kerberos* (ticket-based system)
    2. Windows AD uses a customized Kerberos
    3. On Unix/Linux:
        1. Authentication goes through *PAM (Pluggable Authentication Modules)*
        2. *sssd* used to integrate PAM with identity/auth services
2. **Library Routines for Attribute Lookup**
    1. C library functions must support centralized identity/authentication

- ***Additional Note:*** When using Kerberos (e.g., with Active Directory), *time synchronization (via NTP)* and *hostname resolution (via DNS)* are critical
    - Tickets are time-stamped and expire quickly if clocks or hostnames mismatch

Exhibit A: SSO components



LDAP (Lightweight Directory Access Protocol)

- *A directory service optimized for frequent reads and attribute-based data*
- **Core Assumptions:**
  - Data objects are small
  - Directory is widely replicated and cached
  - Data is organized by attributes
  - Read-heavy, write-light workload
  - Efficient searching is essential
- *Despite the name, LDAP is not lightweight*
  - Originated as a gateway to the older X.500 directory service
  - Now a standalone protocol
- **Common Implementations:**
  - *Microsoft Active Directory*: Most widely used, supports both Windows and Unix
  - *OpenLDAP*: Popular in Unix-only environments

OpenLDAP

- OpenLDAP Components
  - slapd: Main LDAP server daemon
  - slurpd: Handles replication from master to slave servers
- Configuration File: /etc/openldap/slapd.conf

```
database        bdb
suffix          "dc=abacus,dc=net"
rootdn          "cn=admin,dc=abacus,dc=net"
rootpw          {crypt}xjsifuFDGRs
directory       /var/lib/ldap
```

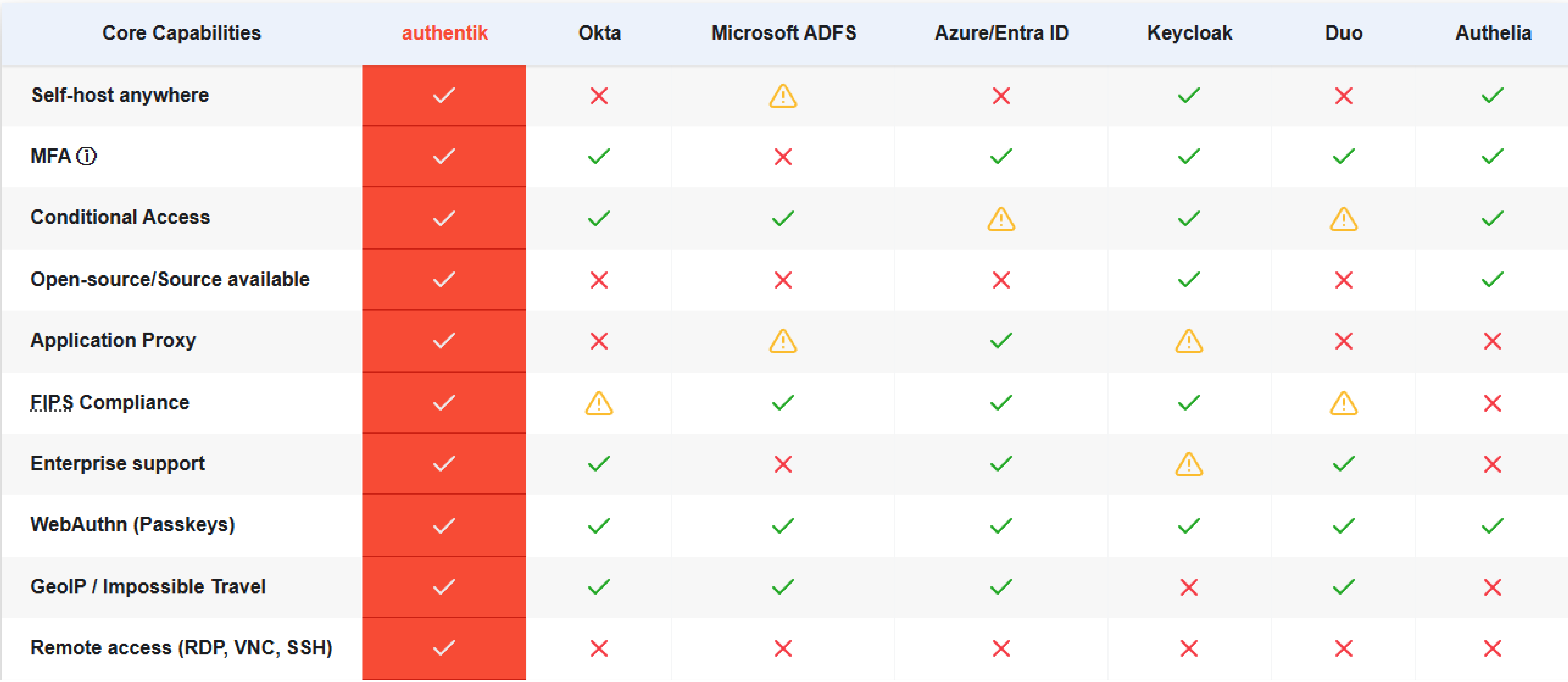
Key Configuration Details

- **Database**: Uses Berkeley DB by default
- **Suffix**: Root of the LDAP hierarchy (like DNS domain)
- **RootDN**: Admin user's distinguished name
- **RootPW**: Admin password (encrypted)
- **Directory**: Path to database file storage

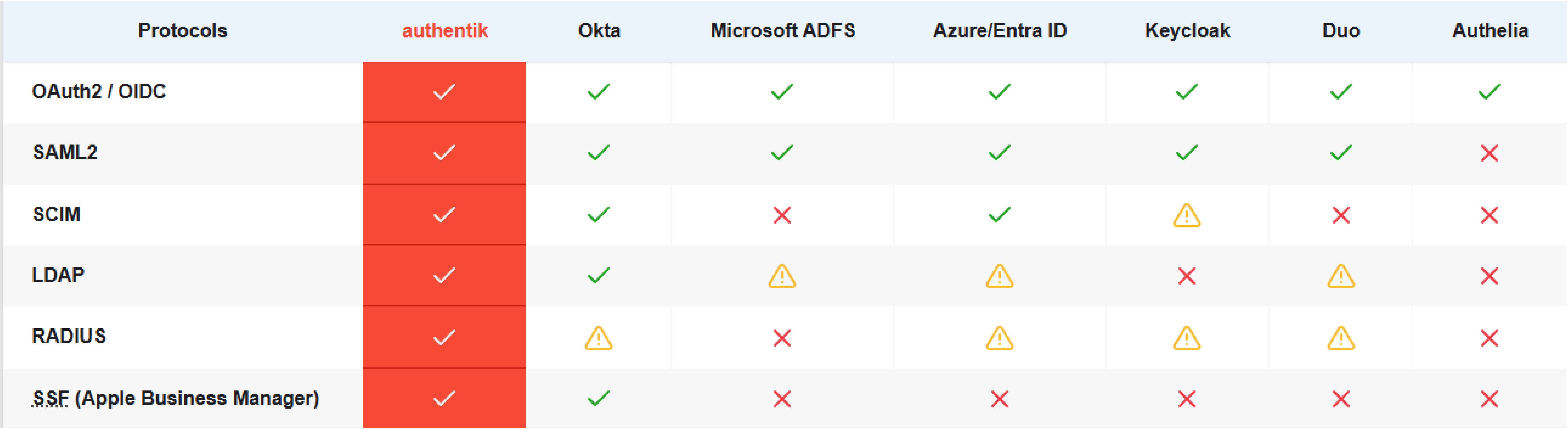
Best Apps for SSO!

Authentik

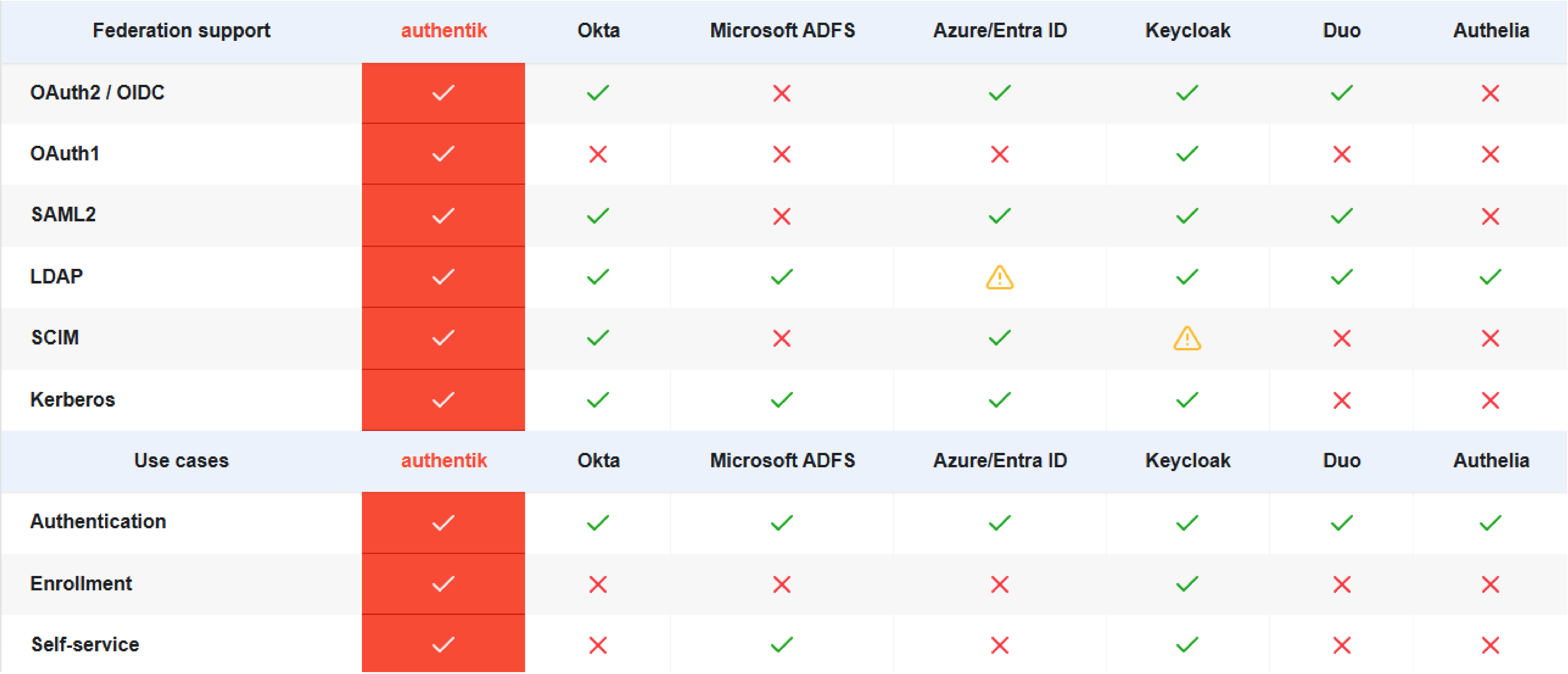
- https://youtu.be/N5unsATNpJk?si=Ye7LoYubfvEjHGHk
- https://www.youtube.com/watch?v=Nh1qiqCYDt4&list=PLH73rprBo7vSkDq-hAuXOoXx2es-1ExOP



Core Capabilities	authentik	Okta	Microsoft ADFS	Azure/Entra ID	Keycloak	Duo	Authelia
Self-host anywhere	✓	✗	⚠	✗	✓	✗	✓
MFA ⓘ	✓	✓	✗	✓	✓	✓	✓
Conditional Access	✓	✓	✓	⚠	✓	⚠	✓
Open-source/Source available	✓	✗	✗	✗	✓	✗	✓
Application Proxy	✓	✗	⚠	✓	⚠	✗	✗
FIPS Compliance	✓	⚠	✓	✓	✓	⚠	✗
Enterprise support	✓	✓	✗	✓	⚠	✓	✗
WebAuthn (Passkeys)	✓	✓	✓	✓	✓	✓	✓
GeoIP / Impossible Travel	✓	✓	✓	✓	✗	✓	✗
Remote access (RDP, VNC, SSH)	✓	✗	✗	✗	✗	✗	✗



Protocols	authentik	Okta	Microsoft ADFS	Azure/Entra ID	Keycloak	Duo	Authelia
OAuth2 / OIDC	✓	✓	✓	✓	✓	✓	✓
SAML2	✓	✓	✓	✓	✓	✓	✗
SCIM	✓	✓	✗	✓	⚠	✗	✗
LDAP	✓	✓	⚠	⚠	✗	⚠	✗
RADIUS	✓	⚠	✗	⚠	⚠	⚠	✗
SSF (Apple Business Manager)	✓	✓	✗	✗	✗	✗	✗



Federation support	authentik	Okta	Microsoft ADFS	Azure/Entra ID	Keycloak	Duo	Authelia
OAuth2 / OIDC	✓	✓	✗	✓	✓	✓	✗
OAuth1	✓	✗	✗	✗	✓	✗	✗
SAML2	✓	✓	✗	✓	✓	✓	✗
LDAP	✓	✓	✓	⚠	✓	✓	✓
SCIM	✓	✓	✗	✓	⚠	✗	✗
Kerberos	✓	✓	✓	✓	✓	✗	✗
Use cases	**authentik**	**Okta**	**Microsoft ADFS**	**Azure/Entra ID**	**Keycloak**	**Duo**	**Authelia**
Authentication	✓	✓	✓	✓	✓	✓	✓
Enrollment	✓	✗	✗	✗	✓	✗	✗
Self-service	✓	✗	✓	✗	✓	✗	✗