**Task #69: Evaluate Authentication Features**

**Authentication Features Comparison Matrix**

**Session Management vs Token-Based Authentication vs Passwordless Login**

| **Feature** | **Session-Based Authentication** | **Token-Based Authentication (JWT)** | **Passwordless Authentication** |
| --- | --- | --- | --- |
| **How It Works** | Server creates session, stores user info server-side, client gets session ID cookie[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Server generates signed token (JWT), client stores token, includes in every request[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Eliminates passwords entirely using biometrics, security keys, or push notifications[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **State Management** | **Stateful** - Server maintains session data[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | **Stateless** - Token contains all info, no server-side storage[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | **Stateless** - Uses cryptographic keys or biometric verification[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Security** | Can be immediately invalidated; vulnerable to CSRF attacks[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Self-contained and signed; can't be invalidated until expiration; resistant to CSRF[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Highly resistant to phishing, brute-force, credential stuffing; eliminates password-related attacks[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Performance** | Quick lookups, but requires session storage on every request[supertokens](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Fewer database lookups, but larger request payloads[supertokens](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Minimal server overhead; authentication handled by device/key[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Scalability** | Requires sticky sessions or shared session storage across servers[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Excellent for distributed systems due to statelessness[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Highly scalable; no session state to manage[mojoauth](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Cross-Domain Support** | Limited; cookies don't work well across domains[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Excellent; tokens easily used across multiple domains[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Excellent; FIDO2 and biometrics work across domains[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Session Termination** | **Immediate** - Can revoke session instantly[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | **Delayed** - Must wait for token expiration[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | **Immediate** - Can revoke device/key access instantly[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Mobile Support** | Moderate; cookies can be problematic[supertokens](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Excellent; natural fit for mobile apps[supertokens](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Excellent; biometrics native to mobile devices[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Implementation Complexity** | Simple for monolithic apps[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Moderate; requires token management[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Moderate to High; requires device enrollment and fallback mechanisms[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Best Use Cases** | Monolithic apps, browser-heavy apps, e-commerce with complex carts[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Microservices, APIs, distributed systems, mobile apps, SSO[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | High-security enterprise apps, modern web/mobile apps, zero-trust environments[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **User Experience** | Moderate; requires password entry and management[supertokens](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Moderate; still requires initial authentication[supertokens](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | **Excellent** - No passwords to remember; faster login[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Cost/Overhead** | Server storage costs for sessions[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Minimal; stateless reduces infrastructure needs[supertokens](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ | Device/key provisioning costs; reduced help desk costs (60-70% fewer password reset calls)[mojoauth](https://mojoauth.com/ciam-101/passwordless-mfa-guide" \t "_blank)​ |

**Multi-Factor Authentication (MFA) Support**

**MFA Options Comparison**

| **MFA Method** | **Security Level** | **User Convenience** | **Implementation Difficulty** | **Cost** | **Platform Support** |
| --- | --- | --- | --- | --- | --- |
| **SMS/Text Codes** | **Low-Medium** - Vulnerable to SIM swapping[mojoauth](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ | Moderate - Requires phone access | Easy | Low - Carrier costs only | Universal |
| **Authenticator Apps (TOTP)** | **Medium-High** - Time-based codes resistant to replay[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ | Good - Works offline | Easy | Free | Cross-platform (Google Authenticator, Microsoft Authenticator)[mojoauth](https://mojoauth.com/ciam-101/passwordless-mfa-guide" \t "_blank)​ |
| **Push Notifications** | **High** - Real-time approval with context[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ | **Excellent** - One-tap approval | Moderate | Low | Requires app installation[mojoauth](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Biometrics (Fingerprint/Face)** | **High** - Unique physical traits[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ | **Excellent** - Seamless, fast | Moderate | Hardware-dependent | Modern devices only[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **FIDO2 Security Keys** | **Very High** - Phishing-resistant hardware keys[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ | Good - Requires physical key | Moderate | Medium ($20-50 per key) | Growing support (YubiKey, Google Titan)[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Hardware Tokens** | **High** - Physical device generates codes | Moderate - Separate device needed | Easy | Medium-High | Universal |
| **Voice Recognition** | **Medium** - Can be spoofed with recordings | Good - Hands-free | Complex | Medium | Limited platform support[mojoauth](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |

**Passwordless Authentication Methods**

**Detailed Method Comparison**

| **Method** | **Technology** | **Security Features** | **User Experience** | **Platform Requirements** |
| --- | --- | --- | --- | --- |
| **Windows Hello for Business** | Biometric + TPM chip | Hardware-backed keys, anti-spoofing[learn.microsoft+1](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless)​ | Seamless login with face/fingerprint | Windows 10+, compatible hardware[learn.microsoft](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless)​ |
| **Microsoft Authenticator** | Push notification + biometric | Device-bound credentials, number matching[learn.microsoft+1](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless)​ | One-tap approval with biometric confirmation | iOS/Android app required[learn.microsoft](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless)​ |
| **FIDO2 Security Keys** | Public key cryptography | Phishing-resistant, hardware-isolated keys[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ | Plug in key and touch button | USB-A/C, NFC, or Bluetooth key[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Passkeys (FIDO2)** | Device-synced credentials | End-to-end encrypted, cross-device sync[learn.microsoft](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods)​ | Biometric or PIN on any enrolled device | iOS 16+, Android 9+, modern browsers[learn.microsoft](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods)​ |
| **Certificate-Based Auth** | Digital certificates (X.509) | PKI-based, device-bound | Transparent to user after enrollment | PKI infrastructure required[learn.microsoft](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless)​ |
| **Magic Links (Email)** | One-time login links | Time-limited, single-use tokens | Click link in email | Email access required |
| **Biometric Cards** | Fingerprint + card chip | Offline verification, no phone needed | Tap card + fingerprint | Specialized hardware |

**Recommendations for Varsity Sports Platform**

**Primary Recommendation: Hybrid Token + Passwordless Approach**

**Implementation Strategy:**

1. **Base Layer:** Token-based authentication (JWT) for API access and scalability[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​
2. **User Authentication:** Passwordless MFA using Microsoft Authenticator or FIDO2 keys[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​
3. **Session Management:** Short-lived refresh tokens (15-30 min) with longer refresh tokens (7-14 days)[supertokens](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication" \t "_blank)​

**Rationale:**

* **Distributed architecture:** Token-based auth supports microservices and CDN integration[geeksforgeeks+1](https://www.geeksforgeeks.org/computer-networks/session-vs-token-based-authentication/)​
* **Enhanced security:** Passwordless methods eliminate 100% of password-related breaches[rsa+1](https://www.rsa.com/resources/blog/passwordless/what-is-passwordless-authentication/)​
* **User experience:** One-tap biometric login reduces friction while maintaining security[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​
* **Cost efficiency:** 60-70% reduction in help desk password reset calls[mojoauth](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​

**MFA Configuration**

**Recommended MFA Stack:**

1. **Primary:** Biometric authentication (fingerprint/Face ID) via device[learn.microsoft+1](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless)​
2. **Secondary:** Push notifications through authenticator app[learn.microsoft+1](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods)​
3. **Fallback:** TOTP codes for users without compatible devices[learn.microsoft+1](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods)​
4. **Admin/High-Security:** FIDO2 hardware keys for privileged accounts[learn.microsoft+1](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless)​

**Implementation Timeline**

| **Phase** | **Duration** | **Tasks** |
| --- | --- | --- |
| **Phase 1** | Week 1-2 | Implement JWT-based API authentication; set up token generation/validation[supertokens](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​ |
| **Phase 2** | Week 3-4 | Integrate Microsoft Authenticator or Auth0 passwordless; configure push notifications[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Phase 3** | Week 5-6 | Deploy biometric enrollment flow; implement FIDO2 support for compatible devices[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Phase 4** | Week 7-8 | Add TOTP fallback option; configure MFA policies and adaptive authentication[mojoauth+1](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |
| **Phase 5** | Week 9-10 | Testing, monitoring, and rollout to pilot user group[mojoauth](https://mojoauth.com/ciam-101/passwordless-mfa-guide)​ |

**Decision Framework**

**Choose Token-Based Auth if:**[geeksforgeeks+1](https://www.geeksforgeeks.org/computer-networks/session-vs-token-based-authentication/)​

* Building distributed systems or microservices ✓
* Need cross-domain authentication ✓
* Primarily mobile or API-driven ✓
* Building for scale from the start ✓

**Choose Session-Based Auth if:**[supertokens+1](https://supertokens.com/blog/token-based-authentication-vs-session-based-authentication)​

* Monolithic application architecture
* Browser-only access
* Need instant session termination frequently
* Simple personalization requirements

**Choose Passwordless MFA if:**[rsa+1](https://www.rsa.com/resources/blog/passwordless/what-is-passwordless-authentication/)​

* High security requirements ✓
* Want to eliminate password-related help desk costs ✓
* Modern user base with compatible devices ✓
* Compliance requires strong authentication ✓