Integration checklist: Introducing passkeys into existing infrastructure

Checkpoint	Description	Status (✔/✖/⚠)	Comments
1. IAM System available	Centrally managed identity and access management with FIDO2/WebAuthn support		e.g., Azure AD, Okta, ForgeRock
2. Authentication server set up	Backend for registering, managing, and validating passkeys		Standalone or integrated into IAM
3. Web applications compatible	Applications support OIDC, SAML, or can be connected to IdP		Adjust front end/back end if necessary
4. Interface standards available	OpenID Connect, OAuth2, SAML, or AD FS implemented		Required for integration into third-party systems
5. Device and authenticator strategy defined	Choice between platform and roaming authenticators depending on user group		See guidelines (point 3)
6. Recovery/fallback strategies planned	Coverage for loss or replacement of devices (e.g., cloud sync, backup key)		Important for user support
7. Pilot environment set up	Tested application area with clearly defined user group		e.g., internal portal or test system
8. Training & documentation prepared	User education, help desk briefing, self-service FAQ available		Success factor for acceptance
9. MDM integration for device management	Management of security policies, device approvals, and certificates		Optional for BYOD relevant
10. Compliance & data protection checked	Processing of biometric data, cloud storage, logging evaluated		Implement in compliance with GDPR