Geräte-Checkliste: Voraussetzungen für die Nutzung von Passkeys

Kriterium	Erklärung	Erfüllt? (Ja/Nein)	Hinweise / Maßnahmen
Aktuelles Betriebssystem	Windows 10/11, macOS 13+, iOS 16+, Android 9+		Veraltete OS-Versionen ggf. upgraden
TPM/Secure Enclave vorhanden	TPM 2.0 bei Windows, Secure Enclave bei Apple		BIOS/UEFI prüfen, ggf. aktivieren
Aktivierte Gerätesperre	PIN, Fingerabdruck oder Gesichtserkennung		Voraussetzung für Plattform-Authentifikatoren
Kompatibler Browser installiert	Chrome, Edge, Safari, Firefox (aktuelle Version)		WebAuthn-Unterstützung notwendig
Biometrischer Sensor verfügbar	Fingerabdrucksensor oder Kamera für Face ID / Windows Hello		Alternativ: PIN-Login als Fallback
MDM oder Gerätemanagement verfügbar	Zentrales Management (z. B. Intune, JAMF, VMware Workspace ONE)		Wichtig für Richtliniensteuerung und Recovery
Synchronisation mit Cloud-Dienst erlaubt (optional)	iCloud, Google Password Manager		Je nach Compliance-Vorgabe aktivieren oder deaktivieren
Externe Authentifikatoren anschließbar (optional)	USB, NFC oder Bluetooth-fähige Geräte		Für hybride oder Hochsicherheitsanwendungen