IT-PLANUNGSRAT

Frankfurt am Main
28.05.2026

Sicherheitsvorgaben für APIs in der öffentlichen Verwaltung

Inhaltsverzeichnis

1 Einleitung

Dieses Rahmendokument definiert den übergreifenden organisatorischen und fachlichen Rahmen für zwei Sicherheitsvorgaben zur Absicherung von APIs in der öffentlichen Verwaltung.
Ziel dieses Rahmendokuments ist es:

- eine einheitliche Struktur für API-Sicherheitsvorgaben bereitzustellen
- die konsistente Anwendung der Sicherheitsvorgaben durch eine klare Abgrenzung der Schutzbedarfstufen sicherzustellen

2 Geltungsbereich

Dieses Rahmendokument gilt für alle Organisationseinheiten, IT-Dienstleister und Entwicklungsteams, die APIs konzipieren, entwickeln, betreiben oder nachnutzen, sofern diese APIs im Kontext der öffentlichen Verwaltung eingesetzt werden.

Der technische Geltungsbereich umfasst alle API-Technologien, bei denen OAuth 2.0 / O-Auth 2.1 oder OpenID Connect eingesetzt werden können.

3 Anwendung der Sicherheitsvorgaben

Die Sicherheitsvorgaben sind in die zwei Schutzbedarfskategorien „Normal“ und „Hoch/ Sehr Hoch“ gemäß den Schutzbedarfen des BSI-Standard 200-2 des IT-Grundschutz gegliedert. Vor der Implementierung einer API MUSS demnach eine Schutzbedarfsfeststellung gemäß BSI-Standard 200-2 in der jeweils gültigen Fassung erfolgen.

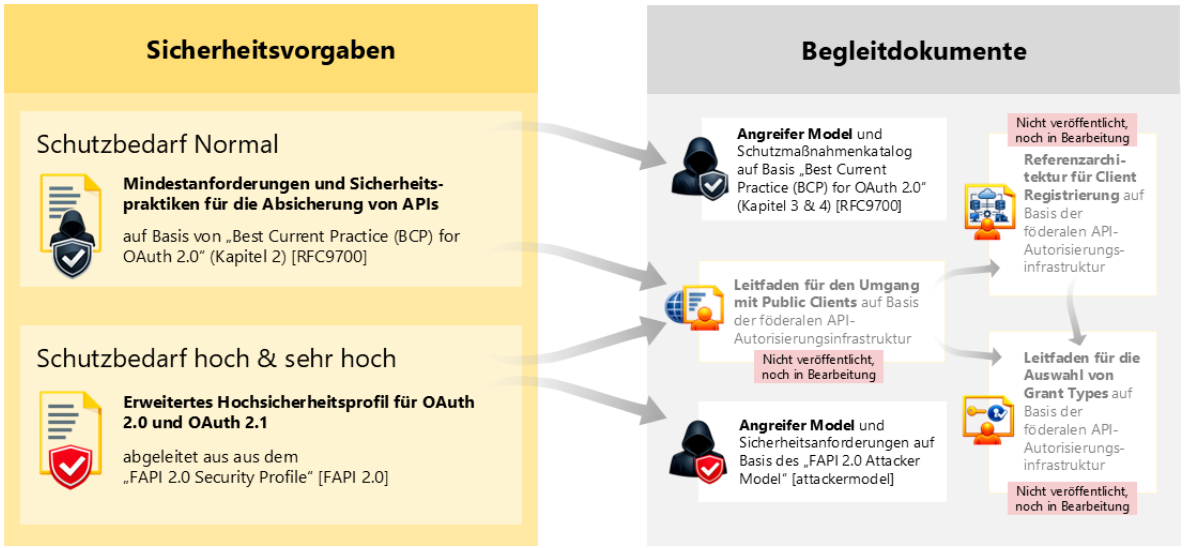

Abbildung 1: Übersicht der Sicherheitsvorgaben zur Absicherung von APIs

Das vorliegende Dokument ist stets zusammen mit dem jeweils zutreffenden Sicherheitsvorgaben zu lesen:

- Sicherheitsvorgaben für die Absicherung von APIs für den Schutzbedarf Normal
- Sicherheitsvorgaben für die Absicherung von APIs für den Schutzbedarf Hoch und Sehr Hoch

Zusätzlich werden Begleitdokumente bereitgestellt. Wie in Abbildung 1 dargestellt, werden darüber hinaus in Zukunft weitere Leitfäden bereitgestellt, die spezifische Aspekte zur Umsetzung der Sicherheitsvorgaben adressieren.

3.1 Schutzbedarf Normal

Die zugehörigen Sicherheitsvorgaben definieren Mindestanforderungen und empfehlen sinnvolle Sicherheitspraktiken auf Basis des Dokuments „Best Current Practice for OAuth 2.0 Security" [RFC 9700] für die Absicherung von APIs, die dem Schutzbedarf normal entsprechen.

Das Begleitdokument „Angreifer Modell und Schutzmaßnahmenkatalog für den Schutzbedarf Normal" definiert das Angreifer Modell und den Schutzmaßnahmenkatalog auf Basis des „Best Current Practice for OAuth 2.0 Security" [RFC 9700] Dokuments.

3.2 Schutzbedarf Hoch/ Sehr Hoch

Die zugehörigen Sicherheitsanforderungen enthalten ein für die deutsche Verwaltung aus dem FAPI 2.0 Security Profile abgeleitetes und erweitertes Hochsicherheitsprofil für OAuth, das

durch formale Analyse nachweislich dem in FAPI 2.0 angegebenen formellen Angreifer-Modell entspricht.

Das Begleitdokument „Angreifer Modell für den Schutzbedarf Hoch und Sehr Hoch“ definiert Sicherheitsanforderungen anhand von Sicherheitszielen und Angreifer-Modellen, basierend auf dem „FAPI Attacker Model“. Aus diesen Anforderungen leiten sich die im Schutzbedarf Hoch und Sehr Hoch verwendeten Sicherheitsmechanismen ab.

3.3 Verbindlichkeit

Hinweis: Das Projekt arbeitet aktuell daran die Sicherheitsvorgaben verbindlich festzulegen. Sobald das erfolgt ist, sollen folgende Bestimmungen gelten:

- Die zutreffenden Sicherheitsvorgaben sind **verpflichtend** einzuhalten.
- Abweichungen von SOLL-Anforderungen sind zu dokumentieren und zu begründen.
- Abweichungen von MUSS-Anforderungen sind **nicht zulässig**.