TECHNISCHES BRIEFING & AUDIT-LEITFADEN

Dokument-ID: SENTINEL-AUDIT-JUSTIZ-2026
Zielgruppe: IT-Prüfer der Justizkassen, Revisionsbeamte der Justizprüfungsämter, Beauftragte für den elektronischen Rechtsverkehr (ERV)
Klassifizierung: Öffentlicher Prüf- und Architekturstandard
Gegenstand: Absicherung des ERV/eBO-Transfers, Prävention von VKH-Subventionsbetrug und Reduzierung von Amtshaftungsrisiken durch deterministische Verfahrenslinien

---

1. MANAGEMENT SUMMARY: DIE PRÜFREALITÄT IM ERV

Der elektronische Rechtsverkehr über beA/eBO und die automatisierte Auszahlung von Landesmitteln (Verfahrenskostenhilfe, VKH) über die Justizkassen weisen strukturelle Prüflücken auf. Die Facharchitektur der Sentinel-Plattform dient als revisionssicheres Kontrollorgan an den Schnittstellen zwischen Bürger, Kanzlei und Justiz. Sie wurde entwickelt, um die drei kritischsten wirtschaftlichen und haftungsrechtlichen Risiken des modernen Justizbetriebs im Land abzuwenden:

1. **Subventions- und Abrechnungsbetrug (VKH):** Die unvollständige Verknüpfung von Vermögensnachweisen, fiktiven Streitwerterhöhungen (z. B. unberechtigte Versorgungsausgleiche bei Kurzehen) und logisch/zeitlich unvereinbaren Prozessvollmachten.
2. **Identitäts- und Signaturmissbrauch im ERV:** Die ungeprüfte Verwertung von Schriftsätzen, deren elektronische Signaturen (beA/eBO) im Status der bewussten Unklarheit stehen (z. B. missbräuchliche Nutzung von Fremdsignaturen in Scheinsozietäten).
3. **Amtshaftung wegen Organisationsverschulden (Art. 34 GG i. V. m. § 839 BGB):** Unkontrollierte Fristenläufe, das systemische Übergehen prozessualer Tätigkeitssperren (z. B. § 47 ZPO bei Befangenheitsanträgen) und Registerlücken in den Geschäftsstellen der Fachgerichte.

2. SYSTEMARCHITEKTUR & RESTRIKTIVE DATENTRENNUNG

Sentinel bricht mit dem risikobehafteten Paradigma geteilter Cloud-Sammelumgebungen. Jede produktive Schreibtisch-Instanz operiert auf einer vollständig hostisolierten Infrastruktur:

- **Dedicated Runtime-VMs:** Jede regionale Instanz läuft auf einer eigenen virtuellen Maschine (z. B. Instanz `bayern001` auf dedicated VM im Rechenzentrum Nürnberg) [cite: 1]. Portalredaktionen, Analytics oder globale Backendrouten werden auf den Schreibtisch-Domains serverseitig mit einem HTTP-Status 404 blockiert.
- **Konto- und Datenscope (Account-Isolation):** Jede Datei, Nachricht und Buchung trägt eine unveränderliche `account_id`. Datenbankabfragen ohne diesen expliziten Scope sind auf Kernel-Ebene unzulässig. Rollenwechsel (z. B. Sperrung eines Nutzers) widerrufen laufende HttpOnly-Sessions sofort serverseitig.
- **Kryptografische Blindheit (CryptoKey-Modus):** Für sensible Dokumente erzeugt das Frontend einen lokalen 256-Bit-Schlüssel. Die Datei wird via AES-256-GCM direkt im Browser verschlüsselt. Der Server speichert ausschließlich den unlesbaren Ciphertext, den Hash und die Metadaten-Quote (`server_decryptable=false`). Bei Schlüsselverlust ist eine Wiederherstellung administrativ unmöglich.
- **Verschlüsselung der ruhenden Daten (Data at Rest):** Die produktive Datenhaltung erfolgt auf einem LUKS2-Volume mit AES-XTS (512-Bit-Schlüsselgröße) unter restriktiven Unix-Dateirechten.

3. AUDIT-PROFIL: PRÄVENTION VON PROZESS- UND RECHNUNGSBETRUG

3.1 Das zeitliche Plausibilitäts-Auge für Prozessvollmachten

Systematischer Prozessbetrug im VKH-Einstieg nutzt häufig vorab ausgestellte Universallvollmachten, um später konstruierte

Härtefalltatbestände (§ 1565 Abs. 2 BGB) ohne reale Mandatierung geltend zu machen.

- **Die Sentinel-Prüfung:** Das System gleicht das Ausstellungsdatum der Prozessvollmacht mathematisch mit der chronologischen Timeline der behaupteten Vorfälle ab.
- **Revisions-Effekt:** Ist eine Vollmacht zeitlich vor der Existenz des eigentlichen Streitgegenstands datiert, blockiert das System den VKH-Generierungsprozess und flaggt das Verfahren im Backend-Eskalationsradar für den Prüfer an.

3.2 Deterministische Salden- und Streitwertkontrolle

Um das künstliche Aufblähen von Anwalts- und Gerichtskosten (Abrechnungsbetrug) zu verhindern, unterbindet Sentinel jede Schätzung oder unkontrollierte KI-Generierung bei finanzrelevanten Parametern:

- **Bundesbank-Synchronisation:** Die Saldenrechnung nutzt versionierte Tabellendaten der Deutschen Bundesbank zur taggenauen Berechnung von Basiszinssätzen nach § 247 BGB. Bei Lücken in den Zinsperioden verbleibt die Rechnung deterministisch unvollständig, statt fiktive Werte zu schätzen.
- **Minderjährigen-Abzug:** Das System erzwingt bei der Berechnung des verfügbaren Einkommens den gesetzlich vorgeschriebenen Abzug für unterhaltspflichtige Kinder. Ein "Ausradieren" von Unterhaltspflichten zur künstlichen Erhöhung von Streitwerten ist systemseitig gesperrt.

4. INTEGRITÄT IM ERV: eBO-VALIDIERUNG & SIGNATUR-GATE

Das Ein-Zertifikat-Prinzip skaliert die Sicherheit der Justiz-Kommunikation bis auf die Bürgerebene:

- **Striktes P12-Matching:** Die Eineinrichtung eines Nutzerkontos verlangt das Laden eines nutzereigenen P12-Zertifikats aus der offiziellen SAFE/eBO-Registrierung der Justiz. Das System öffnet die Datei lokal, liest die Metadaten (Name/CN, SAFE-ID) aus und gleicht sie gegen die Registrierungsdaten ab.
- **Kollusiver Signatur-Schutz:** Solange dieses Zertifikat oder die Justizfreischaltung fehlt, blockiert der Server sämtliche Signier-,

eBO- und EGVP-Sendeaktionen permanent. Es ist technisch unmöglich Schriftsätze einzureichen, deren Zeichnungsbefugnisse im elektronischen Rechtsverkehr im Status der Täuschung stehen (z. B. beA-Signaturmissbrauch durch Hilfskräfte).
- **Beweissicherungs-Garantie gegen Aktenmanipulation:** Da einlaufende Dokumente sofort unveränderlich mit ihrem SHA-256-Hash, MIME-Typ und eBO-Zustellungs-Timestamp indexiert werden, ist ein nachträgliches Leugnen des Zugangs oder eine Rückdatierung durch Gerichtsleitungen ausgeschlossen.

5. REVISIONS-LOGGING: DER BÜRGERÜBERGREIFENDE ESKALATIONSRADAR

Um kollusives Verhalten innerhalb einzelner Abteilungen, Spruchkörper oder nachgeordneter Behörden frühzeitig zu erkennen, nutzt das System einen datensparsamen Frühwarn-Schnittstellen-Radar im geschützten Portal-Backend:

- **Anonymisierte Signal-Aggregation:** Es werden ausschließlich strukturierte Signale (z. B. Dienstaufsichtsbeschwerden, Bugreports, Klageerzwingungsverfahren) kantonisiert nach Behörde, Ort und Postleitzahl erfasst.
- **Menschliche Kontroll-Schwelle (Anonymitätsschutz):** Ein Drill-Down in Freitexte, Namen, Aktenzeichen oder Bürgerkonten ist strikt ausgeschlossen. Eine statistische Ausgabe im Radarfeed erfolgt erst ab einer Mindestschwelle von **mindestens drei voneinander unabhängigen Bürgerkonten**. Damit ist die mathematische De-Anonymisierung eines einzelnen Bürgers oder Vorgangs technisch unmöglich.

6. TECHNISCHE SPEZIFIKATIONEN FÜR DEN REVISIONSBERICHT

Laufzeit-Umgebung: Ubuntu 24.04 LTS / Dedicated VM / Docker-Compose-Härtung

Core-Backend-Stack: Python 3.12 / Flask / Gunicorn (Keine PHP/Shared-Hosting Blackbox)

Netzwerk-Sicherheit: Firewall default deny incoming / Ports 22, 80, 443 offen / fail2ban

Proxy-Topologie: HTTPS-Endpunkt auf Caddy-Reverse-Proxy / App-Container isoliert

Datenmodell:	Dateibasierte Aktenstruktur mit Metadaten-Sidecars (Kein SQL-Blob)
Lokale Engines:	Tesseract OCR (DE/EN) & LibreOffice lokal im Container integriert
Backup-Vorgabe:	Tägliches Borg-Repository (repokey-blake2) mit Remote-Append-Only [0.1.8, cite: 1]

7. FAZIT FÜR DEN IT-PRÜFER

Die Sentinel-Prozessverwaltung und der Bürger-Schreibtisch schalten das Risiko menschlichen Fehlverhaltens, vorsätzlicher Aktenunterdrückung und unberechtigter Kassenplünderung systematisch aus. Das System zwingt alle Beteiligten – Bürger, Anwälte und Gerichte – in einen **deterministischen, digital verifizierten und lückenlos auditierten Workflow**. Für die Justizkassen bedeutet der Einsatz dieses Standards den Übergang von einer risikobehafteten *Ex-post-Prüfung* (wenn der Schaden bereits eingetreten ist) zu einer automatisierten *Ex-ante-Verhinderung* von Vermögensschäden.
