FOCUS FAMILY

Befunde und Maßnahmenplan

Technischer Anhang zum ISO-Konformitätsprofil

Software Notion · Technischer Anhang · Produktstand 1.3.0 · Prüfstand 01.11.2026

Inhaltsverzeichnis

1. **Zweck und Adressat**
2. **Prüfumfang und Methodik**
    1. Geprüfte Bestandteile
    2. Vorgehen
    3. Testnachweis
    4. Was nicht geprüft wurde
3. **Befundübersicht**
4. **Geprüfte Schutzmechanismen im Detail**
    1. Schutz des Audit-Protokolls
    2. Schlüsselverwaltung und Rotation
    3. Lokale Löschkette und Löschaufträge
    4. Meldefunktion und Datenschutzriegel
    5. Anmeldung, Rechte-Obergrenze und Entzug
    6. Freigabe und Datenschutzgrenzen der Schnittstellen
5. **Befunde im Detail**
    1. F-02 · Keine mitgelieferte Alarmierung, Anwendungsprotokolle ohne Weiterleitung
    2. F-05 · Zwei-Faktor-Authentifizierung standardmäßig aus
    3. F-06 · Aktualisierungstoken 365 Tage gültig
    4. F-07 · Bildschirmschutz unter iOS und auf dem Desktop nur eingeschränkt
    5. F-08 · Container-Härtung unvollständig
    6. F-13 · Barrierefreiheit nicht mit Hilfsmitteln geprüft
    7. F-20 · Diktat mit Cloud-Rückfall der Spracherkennung
    8. F-23 · Verwaltungssitzung 180 Minuten ohne Aktivität
    9. F-24 · Schlüsselablage der Desktop-Anwendung ohne Systemschlüsselbund
    10. F-27 · Serverinformation ohne Anmeldung abrufbar
    11. F-28 · Passkey-Konten über die Anmeldeweiterleitung erkennbar
    12. F-30 · Integrationsprüfskripte veraltet
    13. F-32 · Verbindungspool ohne Gegendruck, SQL-Protokollierung in Produktion
    14. F-33 · XTA 2 und FIT-Connect nur gegen Spezifikations-Mocks geprüft
6. **Behobene Befunde**
    1. F-01 · Löschfristen für Änderungsprotokoll und Löschmarkierungen
    2. F-03 · Drittanbieter-Inventar und Stückliste
    3. F-04 · Statische Codeanalyse und Abbild-Scan
    4. F-11 · Zeitsynchronisation als Betriebsanforderung
    5. F-12 · Anforderungsspezifikation im Projektbestand
    6. F-14 · Maschinenlesbare Schnittstellenbeschreibung
    7. F-15 · Last- und Kapazitätsnachweis
    8. F-16 · Blätterfunktion in der Protokollansicht
    9. F-17 · Wiederholungsabstände im Synchronisationsclient
    10. F-18 · Gemessene Testabdeckung
    11. F-19 · Nutzungsrechtehinweis
    12. F-21 · Tagesübersicht für Watch und Widgets
    13. F-22 · Lizenzserver-Adressen in der Bereitstellungsvorlage
    14. F-25 · Selbstlöschung der pseudonymen Lizenzidentität
    15. F-26 · Secure-Attribut und verschlüsselte Schlüssel der Sitzungsverwaltung
    16. F-29 · Rückbuchung des Speicherkontingents
    17. F-31 · Docker-Kommandozeile im Server- und Updater-Abbild ohne Herstellerpflege
7. **Betreiberentscheidungen**
8. **Maßnahmenplan**
9. **Abdeckung ISO/IEC 27001 Anhang A**

1. A.5 Organisatorische Maßnahmen
2. A.6 Personenbezogene Maßnahmen
3. A.7 Physische Maßnahmen
4. A.8 Technologische Maßnahmen

10. **Abdeckung ISO/IEC 27034**
11. **Abdeckung ISO/IEC 25010**
12. **Abdeckung ISO/IEC 29147 und 30111**
13. **Verbleibende Stärken im Überblick**
14. **Gültigkeit**

Zweck und Adressat

Dieses Dokument ist der technische Anhang zum ISO-Konformitätsprofil. Es richtet sich an die **IT-Administration, den Informationssicherheitsbeauftragten und den Datenschutzbeauftragten** eines Trägers sowie an externe Prüfer.

Während das Konformitätsprofil beschreibt, *was* die Software leistet, benennt dieses Dokument *wo genau* Abweichungen bestehen, *wie sie sich auswirken* und *was zu ihrer Behebung nötig ist*. Es enthält bewusst auch Befunde, die für den Hersteller unangenehm sind.

Die Bewertung basiert auf einer Prüfung des Quellcodes, nicht auf der Produktdokumentation. Jede sicherheitsrelevante Aussage der Dokumentation wurde gegen die Implementierung gehalten; weicht beides voneinander ab, ist das als Befund vermerkt.

Prüfumfang und Methodik

Geprüfte Bestandteile

Bestandteil	Umfang
Mobile Anwendung	.NET MAUI, iOS/iPadOS und Android
Desktop-Anwendung	Avalonia, macOS und Windows
Begleit-App	watchOS
Organisationsserver	ASP.NET Core 10, PostgreSQL 17
Verwaltungsoberfläche	Blazor, serverseitig gerendert
Anmeldung über Identitätsanbieter	OpenID Connect und SAML 2.0, Notfallzugang für lokale Systemadministration
Schnittstellen zu Fremdsystemen	REST/JSON, Webhooks, CMIS 1.1 (Client und Repository), XÖV/xdomea über Verzeichnis, SFTP, XTA 2 und FIT-Connect, SCIM 2.0, iCalendar, SIEM-Weiterleitung per Syslog und CEF
Lizenzserver	eigenständiger Dienst
Bereitstellung	Docker-Compose, Reverse-Proxy-Vorlagen, Sicherungsskripte
Dokumentation	über 200 Dokumente, darunter Sicherheits-, Betriebs-, Berechtigungs- und Datenschutzdokumentation

Umfang der Codebasis: 207.796 Zeilen Produktivcode, 130.159 Zeilen Testcode in 612 Testdateien, 17 Produktiv- und 7 Testprojekte, 141 Oberflächendefinitionen (gezählt: C#-Dateien ohne Build-Ausgaben und generierte Dateien, XAML/AXAML-Dateien; dieselbe Zählgrundlage wie im Profil).

Vorgehen

1. **Strukturaufnahme** – Projektaufbau, Abhängigkeiten, Bereitstellungsartefakte.
2. **Dokumentenauswertung** – Sicherheitsdokumentation, Bedrohungsmodell, Autorisierungs- und Protokollbeschreibung, Notfallabläufe, Sicherungsverfahren.
3. **Verifikation am Code** – jede sicherheitsrelevante Aussage der Dokumentation wurde gegen die tatsächliche Implementierung geprüft, nicht übernommen.
4. **Konfigurationsprüfung** – Container, Compose-Definitionen, Reverse-Proxy, Anwendungs- und Baueinstellungen, Bauleitung.
5. **Testlauf** – Ausführung aller sieben Testreihen zur Bestätigung des Ist-Zustands, Server- und Lizenzserverreihe gegen echtes PostgreSQL.
6. **Normabgleich** – Zuordnung der Befunde zu ISO/IEC 27001 Anhang A, 27034, 25010 und 29147/30111.

Testnachweis

Größe	Wert
Ausgeführte Tests (alle sieben Projekte)	6.061
Bestanden	6.047
Übersprungen	14 (umgebungsabhängige Tests: Live-Server-Fälle im Sync-Client; Schlüsselbund-, Signatur- und Live-Server-Fälle auf dem Desktop; auf dem Server ein Live-Test gegen einen echten Identitätsanbieter und zwei Sperrprüfungstests für FIT-Connect, die unter macOS nicht laufen)
Fehlgeschlagen	0
Aufteilung	Kern 1.506, Infrastruktur 796, Sync-Client 149 (6 übersprungen), Desktop 577 (5 übersprungen), lokale KI 137, Lizenzserver 645, Server 2.251 (3 übersprungen)
Testabdeckung	88,0 % der Zeilen (76.000 von 86.362), 68,1 % der Zweige (21.397 von 31.439) (`tools/coverage.sh` über alle sieben Testreihen)
Weitere Prüfungen	Statische Sicherheitsanalyse (`tools/sast.sh`): 0 Meldungen, geprüfte Ausnahmen mit Begründung am Code (`[SuppressMessage]` , 12 Stellen), Ausnahmeliste leer; Abbild-Scan der drei ausgelieferten Abbilder (Admin-Panel amd64 und arm64, Lizenzserver) mit Trivy 0.75.0: keine behebbaren Funde der Stufen „Critical“ oder „High“, Ausnahmeliste leer, Laufzeitabbilder auf `aspnet` 10.0.14 und `sdk` 10.0.403 mit den Sicherheitsupdates vom 25.10.2026; Geheimnis-Scan mit Selbsttest bestanden; Integrationsprüfskripte: alle neun scheitern bei der Anmeldung (F-30)
Durchführung	Ein vollständiger Lauf aller sieben Testreihen am 01.11.2026; Server- und Lizenzserverreihe liefen gegen zwei PostgreSQL-17-Instanzen, einschließlich des Aktualisierungstests von einer Datenbank der Version 1.0.0. Die Schnittstellentests liefen für CMIS gegen ein Alfresco-Testsystem und für SFTP gegen einen Testserver; XTA 2 und FIT-Connect wurden gegen eigene Nachbildungen der Spezifikation geprüft (F-33)
Bewertung	Alle Testreihen grün; Migrations-, Rechte-, Ketten-, Rotations-, Parallelitäts- und Aktualisierungstests liefen gegen echtes PostgreSQL und wurden nicht übersprungen. Ein einmalig beobachteter, nicht reproduzierter Ausfall eines Tests zum Entzug einer Fallfreigabe (`SharingAssignRightTests`) trat in diesem Lauf nicht auf und bleibt Beobachtungspunkt

Was nicht geprüft wurde

Laufzeitverhalten gegen eine produktive Installation, die mobilen Anwendungen in Ausführung auf physischen Geräten, der Lizenzserver im Detail, die Betriebsumgebung eines Trägers, die Anbindung an einen produktiven Identitätsanbieter sowie Wirksamkeitsprüfungen durch Angriffssimulation (Penetrationstest), die Übertragung über XTA 2 und FIT-Connect an echte Gegenstellen (F-33) sowie die Schnittstellen im Zusammenspiel mit den produktiven Fremdsystemen eines Trägers. Die Gerätelogik der Fahrtaufzeichnung (Standortquellen, Zeitgeber, automatisches Ende) und der Apple-Watch-Steuerung ist durch Builds und Komponententests geprüft; ein Test auf echten Geräten steht aus.

Befundübersicht

Vierzehn offene Befunde: keiner mit hoher, vier mit mittlerer und zehn mit niedriger Kritikalität. Sechzehn Befunde sind im Stand der Version 1.3.0 behoben (F-01, F-03, F-04, F-11, F-12, F-14 bis F-19, F-21, F-25, F-26, F-29, F-31); der Abschnitt „Behobene Befunde“ beschreibt je Befund den umgesetzten Mechanismus und den Testnachweis, ebenso die in früheren Prüfrunden behobene Nummer F-22. F-09 und F-10 sind keine Abweichungen, sondern Betreiberentscheidungen mit sicherer Voreinstellung (Abschnitt „Betreiberentscheidungen“). F-07 ist teilweise behoben und auf den verbleibenden Teil eingegrenzt: Der Anzeigeschutz ist zentral erzwingbar, wirkt aber nur unter Android gegen Bildschirmfotos. F-30 ist offen: Die Integrationsprüfskripte scheitern derzeit bereits bei der Anmeldung. Mehrere in früheren Prüfrunden festgestellte Punkte werden im Abschnitt „Geprüfte Schutzmechanismen“ als vorhandene Mechanismen beschrieben (lokale Löschkette, Abschaltbarkeit der Absturzberichte, Datenschutzangaben der Store-Manifeste, Anmeldung und Entzug). Die Nummern behobener und umgewidmeter Befunde bleiben belegt, damit Verweise stabil bleiben.

Nr.	Befund	Kritikalität	Norm
F-02	Keine mitgelieferte Alarmierung, Anwendungsprotokolle ohne Weiterleitung	**mittel**	27001 A.8.15, A.8.16
F-05	Zwei-Faktor-Authentifizierung standardmäßig aus	**mittel**	27001 A.8.5
F-06	Aktualisierungstoken 365 Tage gültig	**niedrig**	27001 A.5.17
F-07	Bildschirmschutz unter iOS und auf dem Desktop nur eingeschränkt	**niedrig**	27001 A.8.12, A.8.1
F-08	Container-Härtung unvollständig	**niedrig**	27001 A.8.9
F-13	Barrierefreiheit nicht mit Hilfsmitteln geprüft	**mittel**	25010, EN 301 549
F-20	Diktat mit Cloud-Rückfall der Spracherkennung	**mittel**	27001 A.5.14, A.5.19; DSGVO Art. 28
F-23	Verwaltungssitzung 180 Minuten ohne Aktivität	**niedrig**	27001 A.8.5, A.5.17
F-24	Schlüsselablage der Desktop-Anwendung ohne Systemschlüsselbund	**niedrig**	27001 A.8.24
F-27	Serverinformation ohne Anmeldung abrufbar	**niedrig**	27001 A.8.9
F-28	Passkey-Konten über die Anmeldeweiterleitung erkennbar	**niedrig**	27001 A.8.5
F-30	Integrationsprüfskripte veraltet	**niedrig**	27001 A.8.29
F-32	Verbindungspool ohne Gegendruck, SQL-Protokollierung in Produktion	**niedrig**	25010 Leistungseffizienz; 27001 A.8.6
F-33	XTA 2 und FIT-Connect nur gegen Spezifikations-Mocks geprüft	**niedrig**	25010 Kompatibilität; 27001 A.8.29

Geprüfte Schutzmechanismen im Detail

Sechs Mechanismen werden nachfolgend genauer beschrieben, weil sie für die Bewertung mehrerer Maßnahmen tragend sind und weil ihre Wirksamkeit jeweils durch einen eigenen Test belegt ist.

Schutz des Audit-Protokolls

Zwei unabhängige Schichten, weil jede für sich umgehbar wäre:

1. **Rechteentzug auf Datenbankebene.** Die Anwendungsrolle besitzt auf `AuditEvents` und `PrivacyRequestEvents` weder UPDATE noch DELETE. Der Entzug steht in derselben Prozedur wie die Rechtevergabe und wird bei jedem Migrationslauf erneut gesetzt.
2. **Hash-Kette.** Jeder Eintrag trägt eine SHA-256-Prüfsumme über seinen Inhalt **und** die Prüfsumme seines Vorgängers. Unter PostgreSQL serialisiert eine Vorgangssperre das Anhängen, sodass parallele Schreibvorgänge die Kette nicht gabeln können.

Die Administration prüft die Kette im Panel unter *Protokoll → Kette prüfen*. Die Prüfung nennt die erste gestörte Stelle mit Sequenznummer und Ursache (Eintrag verändert, entfernt oder umgestellt) und wird selbst protokolliert. Sie umfasst das gesamte Protokoll, nicht nur den in der Oberfläche angezeigten Ausschnitt. Bei jedem erfolgreichen Lauf wird ein Prüfpunkt (Sequenznummer und Prüfsumme des letzten Eintrags) in eine Tabelle geschrieben, auf der die Anwendung ebenfalls nur anhängen darf; dadurch fällt auch das nachträgliche Abschneiden des Kettenendes auf.

Grenze, die wir ausdrücklich benennen: Die Kette belegt die innere Widerspruchsfreiheit der vorhandenen Einträge und erkennt Abschneiden seit der letzten Prüfung. Sie ist **keine** unabhängige Sicherung gegen jemanden, der den Rechteentzug umgehen und einen vollständigen älteren Datenbankstand zurückspielen kann — dagegen hilft nur ein Export in einen Speicher außerhalb dieser Datenbank. Die Abrufschnittstelle dafür ist vorhanden.

Nachweis: Drei Tests gegen echtes PostgreSQL belegen, dass Änderungs- und Löschversuche mit „unzureichende Berechtigung" scheitern, während gewöhnliche Tabellen unverändert beschreibbar bleiben. Neun weitere Tests decken Kette und Panel ab, darunter eine Prüfung, die für jedes einzelne protokollierte Feld nachweist, dass seine Änderung die Prüfsumme verändert.

Schlüsselverwaltung und Rotation

Jede Hülle ruhender Daten trägt eine Schlüsselkennung und wird darüber aufgelöst:

Fläche	Format	Rotation
Lokale Fachdaten auf den Geräten	`ffenc2:<Kennung>:…`	Einstellung in der App; verschlüsselt den lokalen Bestand stapelweise um
Lokale Anhänge (Fotos, Audio, Skizzen, Dokumente)	Kopf `FFATT2` mit Kennung	im selben Lauf
Offene Synchronisationskonflikte (lokale und Serverfassung in `sync.db3`)	`ffenc2:<Kennung>:…`	im selben Lauf, bevor der alte Schlüssel verworfen wird
Dateianhänge auf dem Server	Kopfversion 2 mit Kennung	Admin-Aktion unter *System*, protokolliert
Verschlüsselte Kopien der Auskunftsvorgänge	wie Dateianhänge	im selben Lauf

Geschrieben wird stets mit dem aktiven Schlüssel, gelesen über die Kennung der jeweiligen Hülle. Bei einer Rotation wird der neue Schlüssel dem Ring hinzugefügt und **vor** der ersten Neuverschlüsselung gespeichert; ein abgebrochener Lauf lässt deshalb jeden Datensatz lesbar, ein späterer Lauf setzt fort. Alte Schlüssel dürfen erst verworfen werden, wenn nichts mehr auf ihnen liegt — die Anwendung verweigert es sonst.

Schreibende Zugriffe während des Laufs gehen nicht verloren. Für Datensätze in der Datenbank wird nur dann überschrieben, wenn der Inhalt seit dem Lesen unverändert ist; andernfalls bleibt er stehen und wird beim nächsten Lauf erfasst. Für Dateien — lokale Anhänge wie Serverdateien — prüft der Lauf unmittelbar vor dem Ersetzen, ob die Datei noch existiert und ob Größe und Änderungszeitpunkt denen beim Lesen entsprechen. Eine zwischenzeitlich bearbeitete Datei behält also ihre neuere Fassung, und eine zwischenzeitlich gelöschte Datei wird nicht wiederhergestellt. Auf dem Server gilt dasselbe für die Kopien der Auskunftsvorgänge, sodass eine parallele Schwärzung oder Fristlöschung nicht überschrieben wird.

Ein Lesefehler wird nicht als „nichts mehr offen" gedeutet. Eine Hülle, deren Kopf nicht gelesen werden kann, zählt als offen; eine Kopie, deren Schlüssel fehlt, bricht den Lauf nicht ab, sondern erscheint als übersprungen. „Vollständig" meldet der Server erst, wenn weder Dateien noch Kopien noch unlesbare Hüllen offen sind — erst dann darf ein alter Schlüssel aus der Konfiguration.

Damit das trägt, genügt ein Metadatenvergleich nicht — zwischen Prüfung und Ersetzen bliebe ein Fenster. Rotation, gewöhnliche Schreibvorgänge und Löschungen nehmen deshalb **dieselbe Sperre je Datei** über den gesamten Ablauf: auf den Geräten führen alle Schreib- und Löschpfade für Anhänge über dieselbe Stelle, auf dem Server teilen sich Dateiablage und Rotation denselben Koordinator. Der Metadatenvergleich bleibt als zweite Schranke gegen Schreiber außerhalb der Anwendung bestehen.

Offene Synchronisationskonflikte liegen in der Synchronisationsdatenbank mit demselben Datenschlüssel verschlüsselt wie der übrige Bestand. Unverschlüsselte Altzeilen werden beim Öffnen verschlüsselt, danach wird die Datei mit `secure_delete` und `VACUUM` bereinigt; scheitert die Bereinigung, wird sie beim nächsten Öffnen und nach einem Zurücksetzen wiederholt. Ein Konflikt, der sich nicht mehr entschlüsseln lässt, bleibt sichtbar und blockiert das Senden des Datensatzes. Wird für ihn die Serverfassung übernommen, ist diese Entscheidung an den lokalen Stand zum Entscheidungszeitpunkt gebunden: Eine spätere lokale Änderung erzeugt einen neuen Konflikt, statt überschrieben zu werden, und ungesendete oder private Inhalte eines serverseitig fehlenden oder gelöschten Falls bleiben erhalten. Entfernen des Konflikts, Verwerfen ausstehender Operationen und Speichern des Synchronisationsstands laufen in einer Transaktion.

Drei weitere Zusicherungen betreffen die Gleichzeitigkeit:

- **Auf den Geräten, Dateien:** Schreibende Zugriffe auf Anhänge nehmen für ihre Dauer eine Nutzungsmarke. Das Verwerfen alter Schlüssel wartet, bis keine Marke mehr offen ist, und bricht nach einer Wartezeit lieber ab, als einen Schlüssel zu entfernen, den ein laufender Schreibvorgang braucht.
- **Auf den Geräten, Datenbank:** Dieselbe Marke gilt vom Verschlüsseln bis zum Speichern einer Zeile. Ein Datensatz, der unter dem alten Schlüssel vorbereitet wurde, kann deshalb nicht gespeichert werden, nachdem dieser Schlüssel verworfen wurde. Der Schreibschlüssel wird zudem erst innerhalb der erworbenen Berechtigung bestimmt, sodass auch lange gehaltene Verweise auf den Verschlüsselungsdienst keinen entfernten Schlüssel mehr benutzen können. Marken sind je Ablauf wiedereintrittsfähig, damit verschachtelte Schreibvorgänge nicht blockieren — ein verschachtelter Aufruf erhält seine Marke aber nur, wenn der äußere Aufruf die Berechtigung tatsächlich hält, und kommt so nicht an einer laufenden Schlüsselentfernung vorbei. Ist die vorherige Marke bereits abgeschlossen oder abgebrochen, wird eine neue äußere Marke angelegt und im Ablauf des Aufrufers hinterlegt; zwei nicht abgewartete Aufrufe im selben Ablauf gelten als eigenständige Schreiber. Damit kann weder ein Wiedereintritt ins Leere greifen — was sich sonst als gegenseitiges Warten mit der Schlüsselentfernung äußert — noch ein Geschwisteraufruf an ihr vorbeikommen.
- **Auf den Geräten, Rotationsablauf:** Schlüsselwechsel, Neuverschlüsselung und Schlüsselentfernung laufen unter einer gemeinsamen Sperre. Ein zweiter Auftrag wird abgewiesen statt parallel ausgeführt — auch dann, wenn die Oberfläche zwischenzeitlich geschlossen und wieder geöffnet wurde. Damit kann kein Vorgang einen aus einem älteren Stand abgeleiteten Schlüsselring zurückschreiben und dabei einen Schlüssel entfernen, den ein anderer Vorgang gerade benutzt.
- **Auf dem Server:** Ein Rotationslauf hält für seine Dauer eine Datenbanksperre. Startet eine zweite Instanz denselben Vorgang, arbeitet sie nicht parallel, sondern meldet dem Panel, dass bereits eine Rotation läuft. Arbeitsdateien tragen zusätzlich die Kennung ihres

Laufs; liegen gebliebene Reste werden zu Beginn des nächsten Laufs entfernt, aber erst ab einem Alter von zwölf Stunden, damit ein gleichzeitig laufender Vorgang nichts verliert.

Nachweis: Achtundsechzig Tests. Darunter: Nach dem Verwerfen eines Altschlüssels ist genau die mit ihm geschriebene Hülle nicht mehr lesbar; ein Anhang bleibt nach Rotation und Neustart der Dienste lesbar; ein zwischenzeitlich geänderter Datensatz wird nicht überschrieben; ein Löschvorgang, der während der Neuverschlüsselung beginnt, wird davor bewahrt, die Datei wiederauferstehen zu lassen; eine hinter dem Rücken der Anwendung geänderte oder gelöschte Datei wird nicht überschrieben beziehungsweise nicht zurückgeholt; ein Schlüssel wird weder verworfen, solange ein Dateischreiben offen ist, noch solange ein Datenbankschreiben offen ist; ein zweiter Schreibvorgang im selben Ablauf kommt nicht an einer gehaltenen Schlüsselentfernung vorbei, während ein echter verschachtelter Schreibvorgang — auch nach einer zuvor abgeschlossenen oder abgebrochenen Marke — ohne Wartezeit erteilt wird; ein Aufruf, der beim Warten abbricht, entzieht dem nächsten Aufrufer weder dessen Sperre noch dessen Berechtigung; ein zweiter Rotationsauftrag wird abgewiesen und ein Rotationsbeginn während einer Schlüsselentfernung wartet, sodass kein veralteter Schlüsselring zurückgeschrieben wird; ein früher bezogener Protector schreibt nach der Schlüsselentfernung mit dem neuen Schlüssel; eine unlesbare oder abgeschnittene Hülle — auch in einer Datenschutzkopie — verhindert die Meldung „vollständig"; und ein zweiter Lauf gegen echtes PostgreSQL meldet die laufende Sperre, statt in denselben Bestand zu schreiben. Für jede dieser Zusicherungen wurde zusätzlich geprüft, dass der Test ohne die jeweilige Absicherung fehlschlägt.

Für die Synchronisationskonflikte belegen 19 Tests (`SyncConflictEncryptionTests`, `SyncConflictKeyLifecycleTests`), dass Konfliktinhalte nie im Klartext in die Synchronisationsdatenbank gelangen, Altzeilen verschlüsselt und Reste entfernt werden, die Rotation offene Konflikte vor dem Verwerfen des alten Schlüssels umschlüsselt, ein Konflikt ohne Schlüssel blockiert bleibt und nie gesendet wird und ungesendete oder private Fallinhalte die Übernahme der Serverfassung überstehen.

Nicht nachgewiesen: Ein Lauf auf einem Bestand in Produktionsgröße. Rechnen Sie bei großen Anhangsbeständen mit entsprechender Laufzeit und führen Sie die Rotation in einem Wartungsfenster durch.

Lokale Löschkette und Löschaufträge

Das Löschen eines Falls auf einem Gerät ist eine koordinierte Abfolge in vier Schritten:

1. **Bestandsaufnahme.** Alle Dateien des Falls (Fotos samt Vorschaubildern, Audio, Skizzen samt Zeichendaten, erzeugte Dokumente, Unterschriftsbilder an Zeiteinträgen, Verlaufseinträgen und Dokumenten, generische Anhänge) werden aus den Datensätzen ermittelt. Dateien, die ein anderer Eintrag noch referenziert, bleiben erhalten.
2. **Dauerhafte Vormerkung.** Jeder Löschauftrag wird als eigene Datei abgelegt, **bevor** ein Datensatz entfernt wird. Ein Abbruch zwischen Datensatz- und Dateilöschung hinterlässt damit einen wiederaufnehmbaren Zustand; der nächste Start arbeitet offene Aufträge ab und prüft dabei erneut, ob die Datei inzwischen wieder referenziert ist.
3. **Operationssperre.** Einreihen, Datensatzlöschung und Abarbeitung laufen unter einer gemeinsamen Sperre, sodass ein paralleler Aufräumlauf keinen noch nicht freigegebenen Auftrag verwerfen kann. Löschungen aus der Synchronisation (Tombstones, Zugriffsentzug) nutzen dieselbe Kette.
4. **Ehrliche Ergebnismeldung.** „Nicht vorhanden“, „fehlgeschlagen“ und „unlesbar“ werden getrennt gezählt; beschädigte Aufträge werden in Quarantäne verschoben statt gelöscht. Als vollständig gilt eine Löschung nur ohne offene Aufträge.

„Alle Daten löschen“ hält zusätzlich die Hintergrund-Synchronisation an, wartet auf laufende Schreib- und Rotationsvorgänge, schreibt einen dauerhaften Gesamtlöschauftrag und entfernt erst dann Datenbank und Dateien. Läuft die Wartezeit ab, ist nichts gelöscht.

Nachweis: Vierzehn Tests decken Kaskade, Referenzprüfung, Tombstones, Wiederaufnahme nach fehlgeschlagener Dateilöschung, verschränkte Aufräumläufe, Quarantäne unlesbarer Aufträge und den Gesamtlöschauftrag ab; zwei weitere belegen das Anhalten der Hintergrundarbeit.

Meldefunktion und Datenschutzriegel

Der Bericht entsteht **lokal** und wird vollständig angezeigt, bevor er das Gerät verlassen kann. Es gibt keine stille Übertragung; die Weitergabe ist immer eine ausdrückliche Handlung (Datei sichern, kopieren, E-Mail-Fenster öffnen).

Der Inhalt ist auf eine feste Feldliste begrenzt: Kategorie, Schweregrad, betroffener Bereich, Titel, Beschreibung, Schritte, freiwillige Rückmeldeadresse sowie Produktversion, Build, Plattform, Betriebssystemversion, Gerätemodell, Oberflächensprache und — nur im Admin-Panel — Serverversion und Instanzkennung. Ein Reflexionstest schlägt fehl, sobald ein Feld hinzukommt, das nicht auf dieser Liste steht.

Der Freitext durchläuft zwei Stufen:

1. **Redaktion** von E-Mail-Adressen, Telefonnummern, IBAN, Datumsangaben, langen Ziffernfolgen, Benutzerpfaden und Zugangsdaten in URLs.
2. **Harte Sperre**: Nennt der Text den Namen, Aliasnamen, die Adresse oder die Fallbezeichnung einer im Bestand gespeicherten Person, wird **kein Bericht erzeugt**. Der Abgleich läuft akzent- und großschreibungsunabhängig an Wortgrenzen, sodass „Meier" greift, „Meierei" aber nicht.

Der Riegel ist **fail-closed**: Lässt sich der Personenabgleich nicht durchführen, entsteht kein Bericht. Der fertige Text wird vor der Ausgabe ein zweites Mal geprüft.

Grenzen, die wir ausdrücklich benennen: Der Abgleich ist ein Begriffsvergleich, keine Garantie. Namen unter drei Zeichen werden nicht abgeglichen, weil sie sonst gewöhnliche Wörter träfen. Fallbezogener Freitext ohne gespeicherten Namen passiert den Filter. Der erzeugte Bericht behauptet deshalb **nicht**, frei von Fallinhalten zu sein, sondern beschreibt, was geprüft wurde, und fordert zum erneuten Lesen vor dem Versand auf. Die Entscheidung bleibt bei der Person, die den Bericht weitergibt.

Nachweis: 22 Tests auf der Prüflogik und 7 Tests über die echte HTTP-Schnittstelle des Panels, darunter: eine Meldung mit einem Personennamen aus dem Bestand wird abgewiesen und als fehlgeschlagener Versuch protokolliert; ein fremder Entwurf ist für andere Konten nicht abrufbar.

Anmeldung, Rechte-Obergrenze und Entzug

Anmeldung über den Identitätsanbieter. Die Anmeldung lässt sich an den Identitätsanbieter des Trägers abgeben (OpenID Connect oder SAML 2.0); der Server stellt danach weiterhin eigene Token aus. Ein Konto wird über die E-Mail-Adresse nur verknüpft, wenn der Anbieter sie bestätigt (OpenID Connect `email_verified`, mandantengebundene Angaben bei Microsoft Entra ID, SAML nur nach ausdrücklicher Freigabe); andernfalls gibt die Administration die Erstanmeldung einmalig für 24 Stunden frei. Je Konto gibt es höchstens eine Verknüpfung. Erneute Anmeldebestätigungen gelten nur über eine ausdrücklich erneute Anmeldung beim Anbieter, die höchstens fünf Minuten zurückliegt. Schaltet die Administration **SSO erzwingen** ein, werden lokale Sitzungen und Token sofort widerrufen, Adressen aus den SSO-Domänen werden immer zum Anbieter geleitet, und die Apps bieten nur noch die Anmeldung über die Organisation an. Lokale Systemadministrationskonten behalten als Notfallzugang ein Passwort – ausschließlich für das Admin-Panel; das letzte solche Konto lässt sich nicht umstellen. Die Pflicht zur starken Anmeldung (Passkey, MFA oder SSO) wertet Panel und Geräteprüfung der Synchronisation nach derselben Regel aus.

Einheitliche Anmeldeantworten. Unbekannte, gesperrte und passwortlose Konten durchlaufen dieselbe Passwortprüfung wie ein bestehendes Konto, sodass weder Antwort noch Rechenzeit verraten, ob ein Passwortkonto existiert (Ausnahme: F-28). Konto-, MFA- und Notfallzugriffs-Endpunkte sind mengenbegrenzt und sperren nach Fehlversuchen; die Einrichtung der Zwei-Faktor-Anmeldung gibt kein bereits aktives Geheimnis zurück.

Rechte-Obergrenze. Jede Kontoänderung im Panel – Bearbeiten, Deaktivieren, Passwort, MFA, Passkeys, Einrichtungs-QR, Anmeldeverfahren – wird abgelehnt, wenn das Zielkonto Rechte außerhalb des eigenen Vergaberahmens besitzt. Auf Bereiche beschränkte Administration ändert nur Konten, deren Bereiche und bereichsgebundene Teams vollständig im eigenen Umfang liegen, und vergibt nie fachliche Gesamtadministration oder Bereichsverwaltung.

Sofortiger Entzug. Beim Deaktivieren werden Sitzungen und Token widerrufen; die Synchronisation weist deaktivierte Konten und veraltete Sicherheitsstempel unmittelbar ab und verlangt eine Gerätekennung. Alle Verwaltungsaktionen sind gegen Anfragefälschung geschützt. Die Content Security Policy lässt als Ziel eines Formulars nur den eigenen Server, den Lizenzserver und die registrierten Rückrufadressen der Apps zu; skriptfähige Schemata werden nie aufgenommen.

Nachweis: Ein Regressionstest sendet an jede Verwaltungsaktion eine Anfrage ohne Fälschungsschutz und erwartet die Ablehnung; Tests zählen die Passwortprüfungen für unbekannte, gesperrte und passwortlose Konten und schlagen ohne die Angleichung fehl; weitere Tests decken Rechte-Obergrenze, Bereichsgrenzen, erzwungenes SSO, die gemeinsame MFA-Regel für Panel und Synchronisation, die Ablehnung deaktivierter Konten in der Synchronisation und die zulässigen Formularziele (`AppCallbackFormActionTests`) ab. Ein Live-Test gegen einen echten Identitätsanbieter (Keycloak) liegt vor und läuft nur mit bereitgestellter Testumgebung; im Lauf dieses Prüfstands war er übersprungen.

Freigabe und Datenschutzgrenzen der Schnittstellen

Freigabe im Vier-Augen-Prinzip. API-Clients und Verbindungen entstehen als Entwurf. Datenflüsse mit Falldaten werden erst aktiv, wenn eine Person mit Datenschutzrecht sie mit lokalem Konto und erneuter Anmeldebestätigung freigibt, die die Schnittstelle weder angelegt noch zuletzt geändert hat. Die Freigabe ist an eine vom Server berechnete Revision des geprüften Stands gebunden; wurde die Schnittstelle nach dem Öffnen der Seite geändert, wird sie verweigert. Jede Änderung an Datenumfang, Ziel, Datenschutzeinstellungen oder eingehender Richtung setzt zurück auf „Wartet auf Freigabe“. Weiter öffnen als die datensparsamen Voreinstellungen (pseudonymisiert, nur finale Dokumente, Notizen und vertrauliche Dokumenttypen gesperrt) darf die Datenschutzrolle; die technische Administration nur, solange die Freigabepflicht gilt. Ein Konfigurationsimport enthält keine Geheimnisse, legt nur Entwürfe an und erweitert nie den Fallzugriff.

Sichtbarkeit bei jedem Abfluss. REST-API, CMIS-Repository und Änderungs-Feed prüfen jeden Datensatz gegen den aktuellen Stand: private, in der Verarbeitung eingeschränkte und zur Löschung vorgemerkte Datensätze sowie durch die Dokumentfilter gesperrte Dokumente erscheinen nicht. Webhooks tragen nur Kennungen und Links und werden vor jedem Zustellversuch, auch vor Wiederholungen, erneut gegen Bereich und Datenschutzeinstellungen geprüft. Jede erfolgreiche Zustellung mit Fallbezug schreibt einen Eintrag in das Offenlegungsverzeichnis mit einer Momentaufnahme des Empfängers (Name, Art, Zweck, Rechtsgrundlage); das Auskunftspaket nennt diese Empfänger.

Transport und Geheimnisse. Jede ausgehende Anfrage verweigert vor dem Senden Adressen ohne HTTPS (außer bei ausdrücklichem Schalter) und Adressen mit eingebetteten Zugangsdaten, folgt keinen Weiterleitungen und prüft die tatsächlich verbundene Adresse gegen SSRF. Gespeicherte Zugangsdaten folgen keinem geänderten Ziel, sondern müssen neu hinterlegt werden; OAuth-Tokens werden nie zwischen Verbindungen geteilt. Der CMIS-Client sendet Zugangsdaten nur an den Ursprung der eingetragenen Adresse. FIT-Connect verschlüsselt erst, wenn der Schlüssel des Zustellpunkts über seine Zertifikatskette zur Verwaltungs-PKI führt und nicht gesperrt ist.

Eingang und Löschung. Eingelieferte Dateien durchlaufen beim Empfang dieselben Prüfungen wie Anhänge (Typ, Größe, Dateisignatur, Virenscan); xdomea-Pakete werden mit Grenzen für Umfang und gelesene Bytes entpackt, XML ohne DTD gelesen. Eingänge bearbeitet nur, wer das Recht *Eingänge aus Schnittstellen prüfen und übernehmen* besitzt, und nur für Fälle im eigenen Bereich; die Übernahme läuft atomar. Die endgültige Löschung eines Falls oder Datensatzes leert die Inhalte der zugehörigen Posteingangs-Einträge, entfernt Fremdreferenzen und die Ablagepfade im Zustellverzeichnis. SCIM verwaltet nur Fachkräfte-Konten ohne Verwaltungsrechte, ändert nie Rechte und gleicht Gruppenmitgliedschaften transaktional und gegen parallele Änderungen gesperrt ab.

Grenzen, die wir ausdrücklich benennen: In Zielsystemen übermittelte Daten löscht Focus Family nicht; das Zustellverzeichnis nennt die Empfänger. Private Netze sind als Ziel bewusst erlaubt (DMS im Intranet); wer *Schnittstellen verwalten* besitzt, kann also interne Adressen ansprechen, und mit abgeschalteter Freigabepflicht entfällt die zweite Prüfung neuer Datenflüsse. Die Bedrohungen T22 bis T28 des Bedrohungsmodells beschreiben diese Restrisiken im Einzelnen.

Nachweis: 26 Testklassen der Serverreihe, darunter `IntegrationPrivacyBoundaryTests` (Vier-Augen-Freigabe gegen anlegende und zuletzt ändernde Person, Bindung an die Revision, Löschung der Schnittstellen-Kopien), `IntegrationTransportGuardTests` und `CmisClientGuardTests` (HTTPS-Wächter, SSRF, Ursprungsbindung), `IntegrationDisclosureTests` (Offenlegungsverzeichnis und Auskunftspaket), `IntegrationLicenseGateTests`, `IntegrationHardeningTests` sowie `ScimConcurrencyTests` und `IntegrationInboundConcurrencyTests` gegen echtes PostgreSQL.

Befunde im Detail

F-02 · Keine mitgelieferte Alarmierung, Anwendungsprotokolle ohne Weiterleitung

Kritikalität: mittel · **Norm:** ISO/IEC 27001 A.8.15, A.8.16 (Überwachungsaktivitäten)

Sachverhalt. Das Audit-Protokoll lässt sich als Schnittstelle an ein SIEM weiterleiten (Syslog nach RFC 5424 über TLS nach RFC 5425 oder CEF, mit Ereignisfilter, nur Kennungen und Kettenprüfsumme, keine Falldaten im Klartext); scheitert die Weiterleitung wiederholt, pausiert sie sichtbar, ohne Einträge zu verlieren. Die **Anwendungsprotokolle** dagegen werden auf die Standardausgabe geschrieben. Für sie gibt es keine Weiterleitung, keine Aufbewahrungsfrist und keinen Zugriffsschutz; beim Entfernen des Containers sind sie verloren.

Die **Datenquellen** dagegen sind vollständig vorhanden. Server und Lizenzserver liefern je eine Überwachungsschnittstelle im Prometheus-Format (`/metrics`) und dieselben Zahlen als JSON (`/monitoring/status`), einbindbar in Grafana, Uptime Kuma und vergleichbare Werkzeuge. Der Umfang deckt die sicherheitsrelevanten Signale ab: abgelehnte Aktionen der letzten 24 Stunden, offene Notfallzugriffe, Geräte in Warteposition, Speicher- und Anhangsbelegung, Alter der letzten Prüfung der Audit-Kette, nicht lesbare Verschlüsselungshüllen sowie **überfällige Auskunftsersuchen**. Die Technik-Administration schaltet die Schnittstelle im Verwaltungsbereich unter *System → Monitoring* frei (eigenes Recht *Monitoring konfigurieren*), erzeugt dort den Zugriffsschlüssel und kann den Zugriff auf bestimmte Adressbereiche begrenzen. Ohne Schlüssel antwortet sie mit „nicht gefunden" statt ungeschützt; ausgeliefert werden ausschließlich Zahlen, keine Namen und keine Fallinhalte. Scheitert eine einzelne Messung, meldet die Schnittstelle dies ausdrücklich (`degraded` , benannte Gruppe) statt eine unvollständige Erhebung als unauffällig auszugeben — ein Ausfall der Überwachung selbst bleibt damit sichtbar.

Auswirkung. Es fehlt die **auswertende und alarmierende Schicht** sowie die Weiterleitung der Anwendungsprotokolle. A.8.16 verlangt, dass anomales Verhalten erkannt **und darauf reagiert** wird. Ein Angriffsversuch wird derzeit protokolliert und ist abfragbar, erreicht aber von sich aus niemanden. Wer weder die Überwachungsschnittstelle noch die SIEM-Weiterleitung einschaltet, hat keine Überwachung.

Maßnahme. Zwei Punkte bleiben offen. Erstens mitgelieferte Alarmregeln für die naheliegenden Signale, damit jeder Träger sie nicht selbst formulieren muss. Zweitens ein dokumentierter Weg zur Weiterleitung der Anwendungsprotokolle an ein zentrales System mit Aufbewahrungsfrist und Zugriffsschutz. Die nötigen Kennzahlen liegen bereits an, einschließlich der Kennzahlen der Schnittstellen; im technischen Handbuch steht, welche sich für Alarme eignen.

F-05 · Zwei-Faktor-Authentifizierung standardmäßig aus

Kritikalität: mittel · **Norm:** ISO/IEC 27001 A.8.5 (Sichere Authentifizierung), A.8.2, A.8.9

Sachverhalt. Voreinstellungen der Organisationsrichtlinie:

Einstellung	Voreinstellung	Bewertung
App-Sperre verpflichtend	an	angemessen
Vier-Augen-Prinzip bei Auskünften	an	angemessen
Notfallzugriff freigeschaltet	aus	angemessen
Zwei-Faktor-Authentifizierung verpflichtend	**aus**	**nicht angemessen**
Gerätefreigabe durch Administration	aus	vertretbar

Auswirkung. Die Anwendung verarbeitet Sozialdaten über Familien und Minderjährige – besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO. Eine frisch aufgesetzte Instanz erlaubt die Anmeldung ohne zweiten Faktor, bis ein Administrator die Richtlinie aktiv ändert. Sämtliche technischen Voraussetzungen sind vorhanden und ausgereift: zeitbasierte Einmalkennwörter mit Wiederherstellungscodes sowie Passkeys mit erzwungener Benutzerverifikation und gerätegebundenem Schlüssel.

Abmildernd: Für den Zugriff über die Schnittstelle genügen Zugangsdaten ohnehin nicht – jede Anfrage muss zusätzlich die Gerätekontrolle passieren. Für die Anmeldung an der Verwaltungsoberfläche im Browser greift diese zusätzliche Hürde jedoch nicht.

Maßnahme. Umstellung der Voreinstellung auf „verpflichtend"; alternativ eine erzwungene bewusste Entscheidung bei der Inbetriebnahme statt einer stillen Voreinstellung.

F-06 · Aktualisierungstoken 365 Tage gültig

Kritikalität: niedrig · **Norm:** ISO/IEC 27001 A.5.17, A.8.5

Zugriffstoken sind eine Stunde, Aktualisierungstoken ein Jahr gültig. Für eine offline-fähige Anwendung nachvollziehbar, als Angriffsfenster jedoch lang. Abgemildert durch Bindung des Tokens an das registrierte Gerät, rollierende Erneuerung mit kurzer Überlappung und serverseitige Prüfung des Widerrufs. **Maßnahme:** Kopplung der Gültigkeit an die konfigurierte maximale Offline-Dauer (Voreinstellung sieben Tage) statt eines festen Jahres.

F-07 · Bildschirmschutz unter iOS und auf dem Desktop nur eingeschränkt

Kritikalität: niedrig · **Norm:** ISO/IEC 27001 A.8.12, A.8.1

Teilweise behoben und auf den verbleibenden Teil eingegrenzt. **Umgesetzt** ist die zentrale Erzwingbarkeit: Die verwaltete Einstellung `ScreenProtectionEnforced` lässt sich im Admin-Panel für jeden Geltungsbereich setzen und wird an verbundene Geräte ausgeliefert. Die mobile App schaltet dann „Inhalte im App-Switcher verbergen" ein und sperrt den Schalter, solange das Gerät an den Server gebunden ist. Die tatsächliche Schutzwirkung hängt jedoch von der Plattform ab:

Plattform	Bildschirmfotos und -aufnahmen	Vorschau im App-Umschalter
Android	verhindert (`FLAG_SECURE`)	verdeckt (`FLAG_SECURE`)
iOS und iPadOS	**nicht verhindert**; die App erkennt Aufnahmen auch nicht	verdeckt (Unschärfe-Ebene beim Wechsel in den Hintergrund)
Desktop (macOS, Windows, Linux)	**nicht verhindert**; die Einstellung wird nicht ausgewertet	**nicht verdeckt** durch die Einstellung; nur bei eingerichteter App-Sperre verdeckt die App ihren Inhalt, sobald kein Fenster aktiv ist

Was die Tests belegen. `ScreenProtectionPolicyTests` (Kern) prüfen die Auswertung der Einstellung: Normalisierung der Werte, Sperre des Benutzerschalters nur im gebundenen Zustand, Verhalten beim Entfernen der Vorgabe. `ScreenProtectionManagedSettingTests` (Server) prüfen Katalog, Eingabeprüfung im Panel, Auslieferung des spezifischsten Werts und die Beschriftungen in allen Sprachen. Die Wirkung auf Betriebssystemebene (Setzen von `FLAG_SECURE` , Unschärfe-Ebene unter iOS) belegt kein automatisierter Test; sie ist am Code geprüft.

Restrisiko. Auf iPhone, iPad und am Desktop lassen sich Bildschirminhalte mit Fallbezug per Bildschirmfoto oder Bildschirmaufnahme festhalten, auch wenn der Träger den Anzeigeschutz erzwingt. Der Hinweis im Admin-Panel und die Handbücher nennen diese Grenze.

Maßnahme. iOS: laufende Bildschirmaufnahmen erkennen (`UIScreen.isCaptured`) und den Inhalt währenddessen verdecken. Desktop: Anzeige-Ausschluss (`SetWindowDisplayAffinity` unter Windows, `NSWindow.sharingType` unter macOS) an die Einstellung koppeln. Bis dahin auf verwalteten iOS-Geräten Bildschirmfotos per MDM-Beschränkung unterbinden und die Grenze in die Dienstanweisung aufnehmen.

F-08 · Container-Härtung unvollständig

Kritikalität: niedrig · **Norm:** ISO/IEC 27001 A.8.9, A.8.6

Die Bereitstellungsdefinition setzt weder ein schreibgeschütztes Wurzeldateisystem noch den Entzug von Kernelfähigkeiten, noch die Sperre für Rechteerweiterung, noch Begrenzungen für Arbeitsspeicher und Rechenzeit. Ohne Ressourcengrenzen kann ein einzelner Container den Wirt beeinträchtigen.

Gut gelöst und ausdrücklich anzuerkennen: Ausführung ohne Systemrechte, Bereitschaftsprüfung, sämtliche dauerhaften Daten auf benannten Datenträgern, Datenbank und Virenscanner nicht nach außen erreichbar, Anwendung nur an die lokale Schleife gebunden, Basisabbilder exakt versioniert.

F-13 · Barrierefreiheit nicht mit Hilfsmitteln geprüft

Kritikalität: mittel · **Norm:** ISO/IEC 25010 (Interaktionsfähigkeit, Inklusivität); EN 301 549; BITV 2.0; Barrierefreiheitsstärkungsgesetz

Sachverhalt. Umgesetzt sind: Beschriftungen für Bildschirmlesegeräte auf **allen** rein symbolischen Bedienelementen (60 in der mobilen App, 30 in der Desktop-Anwendung), Beschriftung der Formularfelder, Sprungmarke zum Inhalt und sichtbarer Tastaturfokus in der Verwaltungsoberfläche, Lokalisierung der Oberflächen in sieben Sprachen, Schriftskalierung nach Systemeinstellung, heller und dunkler Modus. Eine Erklärung zur Barrierefreiheit liegt bei (`docs/ACCESSIBILITY.de.md`). Ein Regressionstest schlägt fehl, sobald ein symbolisches Bedienelement ohne Beschriftung hinzukommt.

Nicht umgesetzt oder nicht nachgewiesen:

1. **Keine Prüfung mit echten Hilfsmitteln.** Beschriftungen sind vorhanden und im Code nachweisbar, ein durchgehender Lauf mit VoiceOver, TalkBack, NVDA oder JAWS steht aus. Eine vorhandene Beschriftung garantiert noch keine sinnvolle Vorlesereihenfolge.
2. **Kontrastwerte sind nicht gemessen.**
3. **Vorlesereihenfolge und Überschriftenhierarchie** der mobilen Ansichten sind nicht geprüft.
4. **Erzeugte PDF-Dokumente sind nicht getaggt.**
5. **Zeichenflächen** (Skizzen, Handschrift, Unterschriften) setzen ein Zeigegerät voraus; eine gleichwertige Alternative gibt es nicht.

Auswirkung. Für öffentliche Träger unmittelbar relevant, da sie für ihre eingesetzte Informationstechnik der Barrierefreie-Informationstechnik-Verordnung unterliegen. Focus Family ist **teilweise konform** mit EN 301 549; die fünf genannten Punkte gehören in die eigene Erklärung des Trägers als nicht barrierefreie Inhalte. Unabhängig von der Rechtslage bleiben Fachkräfte mit Seh- oder Motorikeinschränkung von einzelnen Funktionen ausgeschlossen.

Maßnahme. Prüfung mit VoiceOver und TalkBack über die täglichen Abläufe, Messung und Korrektur der Kontrastwerte, Überschriftenhierarchie der mobilen Ansichten, getaggte PDF-Ausgabe, anschließend externe Prüfung.

F-20 · Diktat mit Cloud-Rückfall der Spracherkennung

Kritikalität: mittel · **Norm:** ISO/IEC 27001 A.5.14, A.5.19; DSGVO Art. 28

Die Diktierfunktion nutzt die Spracherkennung des Betriebssystems. Auf iOS wird die Erkennung auf dem Gerät nur erzwungen, wenn das Gerät sie unterstützt; sonst verarbeitet Apple die Aufnahme auf eigenen Servern. Android setzt lediglich eine Bevorzugung der Offline-Erkennung. Diktierte Gesprächsinhalte können damit auf Geräten ohne lokale Erkennung an Apple oder Google gelangen, ohne dass der Träger dies steuern kann. Die Datenschutzerklärung zur App benennt den Rückfall. **Maßnahme:** Diktat auf Geräten ohne lokale Erkennung abschalten oder als Trägerrichtlinie steuerbar machen; bis dahin Hinweis in der Oberfläche vor dem ersten Diktat.

F-23 · Verwaltungssitzung 180 Minuten ohne Aktivität

Kritikalität: niedrig · **Norm:** ISO/IEC 27001 A.8.5, A.5.17

Die Sitzung der Verwaltungsoberfläche läuft nach 180 Minuten Leerlauf ab (konfigurierbar, gleitend verlängert). Für eine Oberfläche mit Zugang zu Falldaten sind 15 bis 30 Minuten üblich. **Maßnahme:** Voreinstellung auf 30 Minuten senken; Hinweis in der Betriebsdokumentation.

F-24 · Schlüsselablage der Desktop-Anwendung ohne Systemschlüsselbund

Kritikalität: niedrig · **Norm:** ISO/IEC 27001 A.8.24

Sachverhalt. Auf Linux liegt der Hauptschlüssel ausschließlich im Secret Service des Systems (libsecret-Schnittstelle, derselbe Weg wie für die Lizenzgeheimnisse). Ist kein Secret Service erreichbar, startet die Anwendung mit einem Hinweis und beendet sich, ohne Schlüssel oder Datenbank anzulegen; ein Klartext-Rückfall existiert nicht (Nachweis: `DesktopSecureKeyStoreBackendTests`, Installationstest in Ubuntu 24.04 und Fedora 42 mit und ohne Schlüsselbund). Auf Windows schützt DPAPI den Schlüssel. Auf macOS wird der Schlüssel dem Werkzeug `security` als Prozessargument übergeben und ist für Prozesse desselben Benutzers kurzzeitig sichtbar; das ist der verbleibende Befund. **Maßnahme:** Ablage über die Keychain-Programmierschnittstelle.

F-27 · Serverinformation ohne Anmeldung abrufbar

Kritikalität: niedrig · **Norm:** ISO/IEC 27001 A.8.9

Die Schnittstelle, mit der sich Apps vor der Anmeldung über den Server informieren, liefert ohne Anmeldung Organisationsname, Serverversion, Instanzkennung, unterstützte Anmeldeverfahren und bei aktivem SSO den Anzeigenamen des Identitätsanbieters. Für die Einrichtung der Apps ist ein Teil davon nötig; Version und Organisationsname erleichtern aber die Erkundung eines öffentlich erreichbaren Servers. **Maßnahme:** Ausgabe vor der Anmeldung auf das für die Einrichtung Erforderliche reduzieren.

F-28 · Passkey-Konten über die Anmeldeweiterleitung erkennbar

Kritikalität: niedrig · **Norm:** ISO/IEC 27001 A.8.5

Die Anmeldeantworten sind für Passwortkonten vereinheitlicht. Konten, die auf Passkey-Anmeldung umgestellt sind, werden jedoch auf die Passkey-Seite weitergeleitet; daran lässt sich erkennen, dass zu einer Adresse ein Passkey-Konto besteht. Die Weiterleitung wird für den Passkey-Ablauf der Apps benötigt und ist deshalb bewusst beibehalten. Abgemildert durch die Mengenbegrenzung der Anmeldung. **Maßnahme:** Passkey-Auswahl unabhängig von der eingegebenen Adresse anbieten.

F-30 · Integrationsprüfskripte veraltet

Kritikalität: niedrig · **Norm:** ISO/IEC 27001 A.8.29 (Sicherheitstests in Entwicklung und Abnahme)

Die neun Integrationsprüfskripte (`tests/integration`, gestartet über `run-all.sh`) laufen als eigene Stufe der Bauleitung gegen einen frisch migrierten Server mit eigener PostgreSQL-Instanz. Derzeit scheitern alle neun bereits bei der Anmeldung über OpenID Connect: Der Anmeldeablauf der Skripte erhält kein Zugriffstoken (`missing_token`), sodass die eigentlichen Prüfungen nicht zur Ausführung kommen. Dahinter liegen weitere Abweichungen: Die Skripte verwenden frühere Rollenbezeichnungen und senden leere Nutzdaten, die der Server zu Recht ablehnt. Scheitert ein Skript, scheitert die Stufe; ist auf dem Bau-Agenten keine Linux-Docker-Engine verfügbar, wird sie mit Hinweis übersprungen. Jeder Lauf kennzeichnet seinen Datenbankcontainer mit einer Laufkennung und entfernt Container, Serverprozess und temporäre Dateien des Laufs auch nach Fehlern und Abbrüchen. Die abgedeckten Abläufe, einschließlich Anmeldung und Tokenausgabe, sind zusätzlich durch die xUnit-Testreihen gegen echtes PostgreSQL geprüft; die Skripte sind damit derzeit kein eigenständiger Nachweis. **Maßnahme:** Anmeldeablauf der Skripte an den aktuellen Anmeldeweg anpassen und Rollen und Nutzdaten aktualisieren.

F-32 · Verbindungspool ohne Gegendruck, SQL-Protokollierung in Produktion

Kritikalität: niedrig · **Norm:** ISO/IEC 25010 (Leistungseffizienz, Zuverlässigkeit); ISO/IEC 27001 A.8.6

Der Lasttest (`docs/server/CAPACITY.de.md`) zeigt zwei Punkte. Erstens ist der Verbindungspool der Datenbankanbindung (100 Verbindungen) so groß wie `max_connections` von PostgreSQL (100); bei Überlast lehnt die Datenbank neue Verbindungen ab, und der Server antwortet mit HTTP 500 statt die Anfragen warten zu lassen oder mit 503 abzuweisen. Zweitens protokolliert der Server in Produktion jeden ausgeführten SQL-Befehl auf Stufe Information, was unter Last Protokollvolumen und Rechenbedarf erhöht. **Maßnahme:** Poolgröße unterhalb von `max_connections` festlegen und eine Erschöpfung des Pools mit HTTP 503 beantworten; die Befehlsprotokollierung der Datenbankschicht in Produktion auf Stufe Warnung setzen.

F-33 · XTA 2 und FIT-Connect nur gegen Spezifikations-Mocks geprüft

Kritikalität: niedrig · **Norm:** ISO/IEC 25010 (Kompatibilität, Interoperabilität); ISO/IEC 27001 A.8.29

Die Aktenabgabe nach xdomea lässt sich über vier Transporte versenden. Der Verzeichnis-Transport arbeitet auf einem eingebundenen Dateisystem; SFTP ist gegen einen echten Testserver geprüft, einschließlich Hostschlüssel-Pin und Zeitgrenzen. XTA 2 Version 4 und FIT-Connect sind nach Spezifikation umgesetzt, aber nur gegen eigene Nachbildungen geprüft (`XoevGatewayTests`: mTLS, MTOM, technische Fehler, Importbestätigung, JWE-Verschlüsselung, Zertifikatskette und Sperrprüfung des Zustellpunkts). Eine Abnahme gegen eine echte XTA-2-Gegenstelle oder die FIT-Connect-Testumgebung steht aus. Zwei Tests der FIT-Connect-Sperrprüfung laufen nur unter Linux bzw. Windows und waren im Lauf dieses Prüfstands übersprungen. Abweichungen zwischen Nachbildung und realer Gegenstelle würden sich erst im Betrieb zeigen; ein Fehlversuch führt nicht zu Datenverlust, sondern zu Wiederholung und automatischer Pause der Verbindung. FIT-Connect ist nur für den Versand umgesetzt. **Maßnahme:** Abnahme beider Transporte gegen reale Gegenstellen; bis dahin vor produktiver Nutzung eine Testübertragung mit der eigenen Gegenstelle durchführen.

Behobene Befunde

Die folgenden Befunde sind im Stand der Version 1.3.0 behoben. Beschrieben sind der umgesetzte Mechanismus und der Nachweis; die Nummern bleiben belegt.

F-01 · Löschfristen für Änderungsprotokoll und Löschmarkierungen

Ein täglicher Hintergrunddienst (`SyncRetentionService`) entfernt Einträge des Synchronisations-Änderungsprotokolls und Löschmarkierungen, die älter als die in der Organisationsrichtlinie konfigurierten Fristen sind, und hält jeden Durchlauf im Audit-Protokoll fest; der Bereinigungsstand je Organisation liegt in einer eigenen Tabelle (Schritt 31 des Migrationsregisters). Geräte, deren letzter Abgleich vor dem bereinigten Bereich liegt, erhalten die Aufforderung zum vollständigen Neuabgleich, laden den Serverstand neu und gleichen ihren Bestand damit ab; ungesendete Änderungen an inzwischen entfernten Datensätzen werden als Konflikt angezeigt. Entzugs- und Löscheinträge werden stapelweise entfernt; jeder Stapel hebt die Neuabgleichsgrenze in derselben Transaktion an, sodass ein Abbruch nie einen Entzug verliert, den kein Gerät erhalten hat. Ältere App-Versionen ohne diese Unterstützung erhalten transparent den vollständigen Stand. Einschränkung: Datensätze, die serverseitig im bereinigten Bereich gelöscht oder entzogen wurden, bleiben auf solchen Geräten bis zur Aktualisierung der App erhalten. Das erzeugte Löschkonzept beschreibt die automatische Durchsetzung. **Nachweis:** `SyncRetentionTests` (auch Abbruch nach dem Löschen unter SQLite und PostgreSQL), `SyncFullResyncEndpointTests`, Neuabgleich in den Testreihen des Synchronisationsclients und der Desktop-Anwendung, Aktualisierungstest von einer Datenbank der Version 1.0.0.

F-03 · Drittanbieter-Inventar und Stückliste

`tools/sbom.sh` erzeugt Stücklisten im CycloneDX-Format für Server, Lizenzserver, App und Desktop-Anwendung; die Bauleitung legt sie als Artefakt ab. Die Komponentenübersicht (`THIRD-PARTY-NOTICES.md`) ist neu aufgestellt, und `ThirdPartyInventoryTests` schlägt fehl, sobald sie von den zentral gepinnten oder den tatsächlich aufgelösten Paketversionen abweicht. Die beiden veralteten Risikoaussagen sind korrigiert.

F-04 · Statische Codeanalyse und Abbild-Scan

`tools/sast.sh` baut den ausgelieferten Code mit allen Sicherheitsregeln der .NET-Analyse und den EF-Core-Regeln gegen SQL-Injektion; jede Meldung bricht ab, sofern sie nicht am betroffenen Code per `[SuppressMessage]` mit Begründung unterdrückt ist oder mit Begründung in der Ausnahmeliste steht. Im geprüften Stand stehen alle geprüften Ausnahmen am Code (12 Stellen: MD5 für stabile Kennungen, Suchpfade nativer Aufrufe, Sperrlistenprüfung von Zertifikaten, Migrations-SQL), die Ausnahmeliste ist leer, 0 Meldungen blockieren. `tools/scan-images.sh` prüft die gebauten Abbilder und Basisabbilder mit Trivy; behebbare Schwachstellen „Critical“ und „High“ lassen den Scan scheitern, Ausnahmen tragen Begründung und Ablaufdatum. Die Integrationsprüfskripte laufen als eigene Stufe der Bauleitung (zu ihrem Zustand siehe F-30). Jeder Lauf der Bauleitung entfernt am Ende, auch nach Fehlern und Abbrüchen, die Container, Serverprozesse, Berichte und temporären Dateien des eigenen Laufs. Übersicht: `docs/security/QUALITY-GATES.de.md`.

F-11 · Zeitsynchronisation als Betriebsanforderung

Die Zeitsynchronisation des Wirts ist ausdrückliche Anforderung (NFR-OPS-01 der Anforderungsspezifikation). Das technische Handbuch führt sie in den Installationsvoraussetzungen und beschreibt im Abschnitt „Zeitsynchronisation prüfen“, welche Mechanismen von der Serveruhr abhängen – Gerätenachweis (±5 Minuten), Offline-Grants, Token, Zwei-Faktor-Codes, Gültigkeitsfenster der SSO-Antworten, Lizenz-Assertions (2 Minuten Toleranz), Zeitstempel des Audit-Protokolls und Fristläufe – und wie der Betreiber sie prüft (`timedatectl status`, `chronyc tracking`, Vergleich mit der Containerzeit). Betriebsablaufplan und Bereitstellungsanleitung nennen sie als Voraussetzung. Die Durchführung bleibt Aufgabe des Betreibers; das Admin-Panel zeigt keine Uhrabweichung an. **Nachweis:** `docs/handbooks/admin-technical.de.md` (Voraussetzungen, „Zeitsynchronisation prüfen“), `docs/deploy/RUNBOOK.de.md` (Goldene Regel 8), `deploy/docker/README.de.md` (Voraussetzungen), `docs/requirements/REQUIREMENTS.de.md` (NFR-OPS-01, Abschnitt 5.8.1); jeweils mit englischer Fassung.

F-12 · Anforderungsspezifikation im Projektbestand

`docs/requirements/REQUIREMENTS.de.md` (englisch `REQUIREMENTS.md`) legt Zweck und Geltungsbereich, Interessengruppen und Rollen, Systemkontext, funktionale Anforderungen nach Fachbereich (Fälle, Dokumentation und E-Akte, Planung, Zeit und Abrechnung, Fahrten, Synchronisation, Admin-Panel, Datenschutz-Workflows, Lizenzierung, lokale KI) sowie nichtfunktionale Anforderungen fest. Jede Anforderung trägt eine stabile Kennung, einen Status und als Abnahmekriterium die belegende Testklasse. Die Sicherheitsanforderungen sind als Anwendungssicherheitsmaßnahmen nach ISO/IEC 27034 mit Verifikationsmessung geführt (Autorisierung, Eingabeprüfung, Protokollierung ohne Inhalte, Schlüsselverwaltung, signierte Update-Kette, Prüfstufen der Bauleitung). Eine Rückverfolgbarkeitsmatrix verbindet Anforderung, Entwurfsdokument und Testnachweis; nicht erfüllte Anforderungen sind mit ihrer Befundnummer ausgewiesen; der Änderungsprozess legt die Pflege je Version und Prüfrunde fest.

Die Ursprungsdokumente der Paragrafenverweise sind nicht überliefert. Eine Konkordanz löst die Verweise der Server-, Lizenz- und App-Spezifikation aus ihrem Verwendungskontext auf und ordnet sie den neuen Kennungen zu; die Bedeutung jeder Nummer ist damit für Prüfer nachvollziehbar. **Einschränkung:** Die Konkordanz ist eine Rekonstruktion, nicht das Original. Maßnahmenbibliothek und Ziel-Vertrauensniveau nach ISO/IEC 27034 bleiben offen (Maßnahmenplan). **Nachweis:** `docs/requirements/REQUIREMENTS.de.md`, `docs/requirements/REQUIREMENTS.md`.

F-14 · Maschinenlesbare Schnittstellenbeschreibung

`docs/api/openapi.v1.json` beschreibt die App- und Verwaltungsschnittstelle im Format OpenAPI 3.1 (67 Pfade, Anmeldeverfahren, Fehlercodes; ohne Verwaltungsoberfläche), `docs/api/openapi.integration-v1.json` die Integrations-API (23 Pfade, Scopes, Fehlercodes

`integration.*`). `OpenApiDocumentTests` und `IntegrationApiTests` schlagen fehl, sobald eine Datei nicht mehr zur Schnittstelle passt; in Produktion stellt der Server keinen OpenAPI-Endpunkt bereit, die Beschreibung der Integrations-API lässt sich im Admin-Panel herunterladen.

F-15 · Last- und Kapazitätsnachweis

k6-Lasttests (`tools/loadtest/run.sh`) mit realistisch angemeldeten Geräten und signierten Anfragen; Ergebnis in `docs/server/CAPACITY.de.md`. Bei 50 gleichzeitigen virtuellen Fachkräften lag der Abruf bei p95 232 ms ohne Fehler, bei 100 bei p95 4,9 s mit 0 % Fehlern, bei 200 erschöpften sich die Datenbankverbindungen (siehe F-32). Dimensionierungsaussage: Bis zu 200 gleichzeitig arbeitende Fachkräfte mit dem Standard-Synchronisationsintervall sind auf 4 vCPUs und 8 GB RAM mit großer Reserve abgedeckt; darüber ist die Messung auf der Zielhardware zu wiederholen.

F-16 · Blätterfunktion in der Protokollansicht

Die Protokollansicht blättert seitenweise durch alle Einträge, behält dabei die Filter bei, und Hinweise auf eine gebrochene Kettenposition verweisen auf die Seite mit dem betroffenen Eintrag. **Nachweis:** `AuditPagingTests`.

F-17 · Wiederholungsabstände im Synchronisationsclient

Nach Netzwerkfehlern, Zeitüberschreitungen und Überlastantworten wächst der Abstand bis zum nächsten Versuch exponentiell mit zufälliger Streuung bis höchstens eine Stunde; eine `Retry-After`-Angabe des Servers wird eingehalten. **Nachweis:** `SyncRetryBackoffTests`.

F-18 · Gemessene Testabdeckung

`tools/coverage.sh` misst die Abdeckung aller sieben Testreihen und führt sie zusammen; die Bauleitung veröffentlicht den Bericht. Gemessen: 88,0 % der Zeilen und 68,1 % der Zweige.

F-19 · Nutzungsrechtehinweis

Der Projektbestand enthält eine Lizenzdatei (`LICENSE`), die die Nutzungsrechte regelt.

F-21 · Tagesübersicht für Watch und Widgets

Bei aktivem Verbergen ersetzt die App vor dem Schreiben jeden Fallalias durch einen Platzhalter und lässt Orte weg, und die Datei wird mit der Schutzklasse „vollständig“ abgelegt; gelingt das nicht, wird sie verworfen. **Nachweis:** `CompanionSnapshotTests`, `WatchLogicTests` (Apple-Testziel).

F-22 · Lizenzserver-Adressen in der Bereitstellungsvorlage

Die Vorlage nennt nur HTTPS-Adressen, und der Server startet außerhalb der Entwicklungsumgebung nicht mit unverschlüsselten Lizenzadressen.

F-25 · Selbstlöschung der pseudonymen Lizenzidentität

Ein Endpunkt des Lizenzservers löscht die pseudonyme Identität samt zugehöriger Datensätze nach Nachweis des Wiederherstellungscodes; von der Organisation verwaltete Identitäten und Identitäten mit aktivem Platz werden nicht gelöscht, und der Endpunkt ist mengenbegrenzt. Die App bietet die Löschung in den Lizenzeinstellungen an und entfernt danach den lokalen Lizenzstand. **Nachweis:** 13 Tests in `StandaloneIdentityDeletionTests`.

F-26 · Secure-Attribut und verschlüsselte Schlüssel der Sitzungsverwaltung

In Produktion erhalten Sitzungs- und Schutzmarken-Cookies stets das Secure-Attribut, auch hinter einem Proxy, der intern über HTTP weiterleitet; ausgenommen ist nur eine ausdrücklich für HTTP freigegebene Testinstallation (siehe Betreiberentscheidungen). Der Schlüsselring der Sitzungsverwaltung wird mit dem Zertifikat `encryption.pfx` verschlüsselt; bestehende unverschlüsselte Schlüssel werden beim Start neu verschlüsselt abgelegt. Sicherungen, die vor diesem Schritt entstanden sind, enthalten die Schlüssel weiterhin unverschlüsselt und sind entsprechend zu schützen oder zu ersetzen. **Nachweis:** `CookieSecurityProductionTests`, `AntiforgeryCookieSecureTests`, `DataProtectionKeyRingTests`.

F-29 · Rückbuchung des Speicherkontingents

Jeder Löschweg – Bereinigung verwaister Dateien, endgültiges Entfernen archivierter Tätigkeitsnachweise, Löschen der Dateien eines Benutzers – bucht den freigegebenen Speicher im selben Vorgang atomar auf das Kontingent zurück, nie unter null. Bei der Bereinigung verwaister Dateien und beim Löschen der Dateien eines Benutzers landen die physischen Löschaufträge in derselben Transaktion in der dauerhaften Löschwarteschlange; scheitert das Löschen auf dem Datenträger oder endet der Prozess nach dem Festschreiben, wiederholt der stündliche Lauf den Auftrag. **Nachweis:** `QuotaCreditTests` (scheiternde Dateilöschung, Abbruch nach dem Festschreiben, SQLite und PostgreSQL).

F-31 · Docker-Kommandozeile im Server- und Updater-Abbild ohne Herstellerpflege

Server- und Prebuilt-Abbild (darin läuft auch der Updater) übernehmen die Docker-Kommandozeile aus dem gepflegten Basisabbild `docker:29-cli` statt aus `docker:27-cli`; das nicht mehr ausgelieferte eigenständige Updater-Abbild ist entfernt. Die Compose-Erweiterung wird beim Bau aus dem Quellcode des Release-Stands gebaut (Commit beim Bau gegen die Prüfsumme geprüft, derzeit mit `golang.org/x/net` 0.62.0), damit Korrekturen von Go und `golang.org/x/net` auch dann enthalten sind, wenn der Hersteller noch keine neue Version veröffentlicht hat; die Buildx-Erweiterung wird nicht ausgeliefert. Der Basisabbild-Scan der Bauleitung prüft beim Docker-Abbild nur die tatsächlich übernommene Kommandozeile; das selbst gebaute Compose deckt er über die im Repository festgehaltenen Modulstände, die Compose-Version selbst, das Go-Bauabbild und einen Abgleich der Versionsangaben ab. Basisabbilder werden für beide ausgelieferten Plattformen (`linux/amd64`, `linux/arm64`) geprüft. Ergebnis: keine behebbare Schwachstelle „Critical“ oder „High“ in den ausgelieferten Abbildern, die Ausnahmeliste des Scans ist leer. **Nachweis:** Abbild-Scan (`tools/scan-images.sh`, gebaute Abbilder und Basisabbilder) ohne Ausnahmen bestanden; Kompatibilitätstest aller vom Updater verwendeten Docker- und Compose-Befehle gegen Docker Engine 20.10, 23, 24, 25, 26, 27, 28 und 29.

Betreiberentscheidungen

Die Nummern F-09 und F-10 bezeichnen keine Abweichungen. Beide Punkte sind Einstellungen, die ein Betreiber bewusst setzt; die Voreinstellung ist sicher, und die Betriebsdokumentation beschreibt die Wirkung. Die Nummern bleiben belegt.

Nr.	Einstellung	Sichere Voreinstellung	Empfehlung
F-09	`OPENIDDICT_ALLOW_INSECURE_HTTP` lässt die Anmeldung über unverschlüsseltes HTTP zu	aus; in Produktion werden Sitzungs- und Schutzmarken-Cookies ohne diese Einstellung stets mit Secure-Attribut gesetzt	nur für Testinstallationen ohne TLS setzen, nie für Installationen mit Falldaten
F-10	`REVERSE_PROXY_ALLOWED_HOST` beschränkt die angenommenen Hostnamen	alle Hostnamen; weitergeleitete Absenderangaben werden ausschließlich aus dem festen Proxy-Netz angenommen, die mitgelieferten Proxy-Vorlagen legen den Servernamen fest	beim Betrieb unter einer Domain auf den Hostnamen des Servers setzen

Maßnahmenplan

Sortiert nach Verhältnis von Wirkung zu Aufwand. Behobene Befunde sind nicht aufgeführt.

Rang	Maßnahme	Befund	Aufwand	Norm
1	Zwei-Faktor-Authentifizierung als Voreinstellung	F-05	gering	27001 A.8.5
2	Diktat ohne lokale Erkennung abschalten oder per Richtlinie steuern	F-20	gering	27001 A.5.14
3	Container-Härtung und Ressourcengrenzen	F-08	gering	27001 A.8.9
4	Verwaltungssitzung auf 30 Minuten Leerlauf begrenzen	F-23	gering	27001 A.8.5
5	Verbindungspool unter `max_connections` mit HTTP 503 bei Erschöpfung, Befehlsprotokollierung in Produktion auf Warnung	F-32	gering	25010, 27001 A.8.6
6	Integrationsprüfskripte an den aktuellen Anmeldeweg, die Rollen und die Nutzdaten anpassen	F-30	gering	27001 A.8.29
7	Serverinformation vor der Anmeldung reduzieren, Passkey-Auswahl unabhängig von der Adresse	F-27, F-28	gering	27001 A.8.5, A.8.9
8	Bildschirmschutz unter iOS (Aufnahmen erkennen und verdecken) und auf dem Desktop (Anzeige-Ausschluss) an die Einstellung koppeln	F-07	mittel	27001 A.8.12
9	Alarmregeln mitliefern, Anwendungsprotokolle weiterleiten	F-02	mittel	27001 A.8.16
10	XTA 2 und FIT-Connect gegen reale Gegenstellen abnehmen	F-33	mittel	25010, 27001 A.8.29
11	Maßnahmenbibliothek und Vertrauensniveau ableiten	—	mittel	27034
12	Desktop-Schlüssel auf macOS über Keychain-Schnittstelle (Linux-Teil erledigt: Secret Service verpflichtend)	F-24	mittel	27001 A.8.24
13	Gültigkeit des Aktualisierungstokens an Offline-Dauer koppeln	F-06	gering	27001 A.5.17
14	Barrierefreiheit mit Hilfsmitteln prüfen, Kontraste messen, PDF taggen	F-13	hoch	25010, EN 301 549
15	Unabhängiger Penetrationstest	—	hoch	27001 A.5.35

Die Ränge mit geringem Aufwand sind zusammen wenige Arbeitstage. Der Barrierefreiheits-Punkt ist der aufwendigste und für öffentliche Träger der folgenreichste Punkt.

Abdeckung ISO/IEC 27001 Anhang A

Legende: erfüllt · teilweise · offen · organisatorisch (beim Träger) · nicht anwendbar

A.5 Organisatorische Maßnahmen

Nr.	Maßnahme	Status
5.1	Informationssicherheitsrichtlinien	organisatorisch
5.2	Rollen und Verantwortlichkeiten	teilweise
5.3	Aufgabentrennung	erfüllt
5.4	Verantwortung der Leitung	organisatorisch
5.5	Kontakt zu Behörden	erfüllt
5.6	Kontakt zu Interessengruppen	erfüllt
5.7	Bedrohungsinformationen	teilweise
5.8	Sicherheit im Projektmanagement	erfüllt
5.9	Inventar der Werte	erfüllt
5.10	Zulässiger Gebrauch von Werten	erfüllt
5.11	Rückgabe von Werten	erfüllt
5.12	Klassifizierung von Informationen	erfüllt
5.13	Kennzeichnung von Informationen	erfüllt
5.14	Informationsübertragung	erfüllt
5.15	Zugangssteuerung	erfüllt
5.16	Identitätsverwaltung	erfüllt
5.17	Authentifizierungsinformationen	teilweise
5.18	Zugangsrechte	teilweise
5.19–5.22	Lieferantenbeziehungen	teilweise
5.23	Cloud-Dienste	erfüllt
5.24–5.27	Ereignisplanung, Bewertung, Reaktion, Lernen	teilweise
5.28	Sammlung von Beweismitteln	erfüllt
5.29	Sicherheit bei Störungen	erfüllt
5.30	Bereitschaft für Betriebsfortführung	teilweise
5.31	Rechtliche Anforderungen	erfüllt
5.32	Geistiges Eigentum	erfüllt
5.33	Schutz von Aufzeichnungen	teilweise
5.34	Schutz personenbezogener Daten	erfüllt
5.35	Unabhängige Überprüfung	teilweise
5.36	Einhaltung von Richtlinien	organisatorisch
5.37	Dokumentierte Betriebsabläufe	erfüllt

A.6 Personenbezogene Maßnahmen

Nr.	Maßnahme	Status
6.1	Sicherheitsüberprüfung	**organisatorisch**
6.2	Beschäftigungsbedingungen	**organisatorisch**
6.3	Bewusstsein und Schulung	**organisatorisch**
6.4	Disziplinarverfahren	**organisatorisch**
6.5	Verantwortung nach Beendigung	**organisatorisch**
6.6	Vertraulichkeitsvereinbarungen	**organisatorisch**
6.7	Remote-Arbeit	**technisch unterstützt**
6.8	Meldung von Sicherheitsereignissen	**erfüllt**

A.7 Physische Maßnahmen

Nr.	Maßnahme	Status
7.1–7.14	Sicherheitsbereiche, Zutritt, Betriebsmittel, Verkabelung, Wartung, Entsorgung	**vollständig organisatorisch**

Die erzeugte Maßnahmenübersicht fragt die relevanten Punkte strukturiert ab und bildet damit die Schnittstelle zum ISMS des Trägers.

A.8 Technologische Maßnahmen

Nr.	Maßnahme	Status	Bezug
8.1	Endgeräte	teilweise	F-07
8.2	Privilegierte Zugangsrechte	erfüllt	
8.3	Einschränkung des Informationszugangs	erfüllt	
8.4	Zugang zum Quellcode	organisatorisch	
8.5	Sichere Authentifizierung	teilweise	F-05, F-06, F-28
8.6	Kapazitätssteuerung	teilweise	F-08, F-32
8.7	Schutz vor Schadsoftware	erfüllt	
8.8	Umgang mit technischen Schwachstellen	erfüllt	
8.9	Konfigurationsmanagement	teilweise	F-08, F-27
8.10	Löschung von Informationen	erfüllt	
8.11	Datenmaskierung	erfüllt	
8.12	Verhinderung von Datenlecks	teilweise	F-07
8.13	Sicherung von Informationen	teilweise	
8.14	Redundanz	teilweise	
8.15	Protokollierung	teilweise	F-02
8.16	Überwachungsaktivitäten	teilweise	F-02
8.17	Uhrensynchronisation	erfüllt	
8.18	Privilegierte Hilfsprogramme	erfüllt	
8.19	Software auf Produktivsystemen	erfüllt	
8.20	Netzwerksicherheit	erfüllt	
8.21	Sicherheit von Netzwerkdiensten	erfüllt	
8.22	Netzwerksegregation	erfüllt	
8.23	Web-Filterung	nicht anwendbar	
8.24	Verwendung von Kryptografie	erfüllt	
8.25	Sicherer Entwicklungslebenszyklus	erfüllt	
8.26	Anforderungen an Anwendungssicherheit	erfüllt	
8.27	Sichere Systemarchitektur	erfüllt	
8.28	Sicheres Codieren	erfüllt	
8.29	Sicherheitstests	teilweise	F-30, F-33
8.30	Ausgelagerte Entwicklung	nicht anwendbar	
8.31	Trennung Entwicklung, Test, Produktion	erfüllt	
8.32	Änderungsmanagement	erfüllt	
8.33	Testinformationen	erfüllt	
8.34	Schutz bei Audit-Prüfungen	organisatorisch	

Zusammenfassung: Von 93 Maßnahmen sind 66 durch eine Software adressierbar. Davon **40 vollständig und 26 teilweise umgesetzt, keine offen**. Die übrigen 27 liegen beim Träger (25) oder sind nicht anwendbar (2). Die Zeilen der Tabelle fassen zusammengehörige Maßnahmen teilweise zu Bereichen zusammen; die Zahlen zählen jede Maßnahme einzeln.

Abdeckung ISO/IEC 27034

Bestandteil	Status	Anmerkung
Anforderungen und Umfeld spezifiziert	**erfüllt**	Anforderungsspezifikation mit stabilen Kennungen, Testnachweisen und Konkordanz der Altverweise
Sicherheitsrisiken bewertet	**erfüllt**	28 Bedrohungsszenarien mit benanntem Restrisiko, davon sieben zu den Schnittstellen
Anwendungsspezifisches Rahmenwerk	**offen**	
Maßnahmenbibliothek	**faktisch vorhanden**	Sicherheitsanforderungen als Anwendungssicherheitsmaßnahmen mit Verifikationsmessung in der Anforderungsspezifikation; als Bibliothek mit Vertrauensniveau nicht ausgewiesen
Maßnahmen mit Verifikationsmessung verknüpft	**erfüllt**	Zu jedem Befund ein Test, der bei Rücknahme fehlschlägt
Ziel-Vertrauensniveau festgelegt	**offen**	
Sicherheit über den Lebenszyklus	**gelebt, nicht beschrieben**	
Bereitstellung und Betrieb	**erfüllt**	Betriebsablaufplan, Notfallabläufe, Migrationsverfahren
Prüfung der Anwendungssicherheit	**teilweise**	Mehrere vom Hersteller veranlasste Prüfrunden, darunter Gesamtprüfung vom 03.10.2026, werkzeuggestützte Zweitprüfung vom 08.10.2026 und Prüfrunden der Integrationsschnittstellen vom 28.10. bis 01.11.2026; keine unabhängige Prüfung

Einschätzung. Die inhaltliche Substanz für ISO/IEC 27034 ist überwiegend vorhanden, und die Anforderungsspezifikation als erster Schritt des Prozesses liegt bei. Was fehlt, ist die übrige von der Norm erwartete Struktur. Aus dem Bedrohungsmodell, der Berechtigungsdokumentation und der vorhandenen Testreihe lässt sich eine Maßnahmenbibliothek mit zugehörigen Verifikationsmessungen mit überschaubarem Aufwand ableiten. Dies ist unter allen vier Normen das beste Verhältnis von Aufwand zu erzielbarem Nachweis.

Abdeckung ISO/IEC 25010

Merkmal	Status	Wesentliche Grundlage bzw. Lücke
Funktionale Eignung	**erfüllt**	Vollständiger Fachablauf, vier Handbücher und Schnittstellenhandbuch, ~2.250 Servertests
Leistungseffizienz	**teilweise**	Indizes, Streaming, Kontingente, Lastnachweis mit Dimensionierungsaussage – Überlastverhalten des Verbindungspools offen (F-32)
Kompatibilität	**erfüllt**	Fünf Plattformen, offene Exportformate, Schnittstellenbeschreibungen im Format OpenAPI 3.1, dokumentierte Standardschnittstellen (REST, Webhooks, CMIS 1.1, XÖV/xdomea, SCIM 2.0, iCalendar, Syslog/CEF) – Abnahme von XTA 2 und FIT-Connect gegen reale Gegenstellen offen (F-33)
Interaktionsfähigkeit	**teilweise**	Sieben Sprachen, Bedienhilfen-Beschriftungen und Erklärung vorhanden – Prüfung mit Hilfsmitteln offen (F-13)
Zuverlässigkeit	**erfüllt**	Offline-Fähigkeit, Konfliktanzeige, Idempotenz, geprüfte Wiederherstellung
Sicherheit	**erfüllt**	Siehe Anhang-A-Tabelle
Wartbarkeit	**erfüllt**	17 Teilprojekte, Testverhältnis 0,63, gemessene Testabdeckung 88,0 % der Zeilen und 68,1 % der Zweige, Korrelationskennungen
Flexibilität	**erfüllt**	Fünf Plattformen aus einer Codebasis, Selbstbetrieb, zentrale Einstellungen
Gefahrlosigkeit	**teilweise**	Keine automatischen fachlichen Entscheidungen, Fail-Closed – keine fachliche Gefährdungsbetrachtung

Abdeckung ISO/IEC 29147 und 30111

Anforderung	Norm	Status
Veröffentlichte Meldungsrichtlinie	29147	**erfüllt**
Meldeweg und Kontaktangabe	29147	**erfüllt**
Empfangsbestätigung und Fristen	29147	**erfüllt**
Koordinierte Offenlegung	29147	**Frist veröffentlicht, noch nie angewandt**
Sicherheitsmeldungen an Betreiber	29147	**Vorlage und Weg festgelegt**
Entgegennahme von Meldungen	30111	**Postfach eingerichtet**
Verifikation	30111	**gelebte Praxis**
Entwicklung der Behebung	30111	**gelebte Praxis**
Wirksamkeitsnachweis der Behebung	30111	**erfüllt**
Bereitstellung	30111	**Weg festgelegt (signiertes Update mit Rückstufungsschutz), noch nicht für eine Sicherheitsbehebung genutzt**
Nachbetrachtung	30111	**verpflichtend beschrieben, noch nie durchlaufen**
Beschriebener Prozess mit Rollen und Fristen	30111	**erfüllt**
Schweregradbewertung	30111	**erfüllt**

Einschätzung. Der substanzielle Teil von 30111 – Verifikation, Behebung, Wirksamkeitsnachweis – wird nachweislich gelebt. Die Außenschnittstelle nach 29147 ist eingerichtet: Richtlinie, Kontaktadresse mit `security.txt`, veröffentlichte Fristen, Meldevorlage und Meldefunktion in den Oberflächen. Offen ist ausschließlich der Nachweis aus dem Betrieb – koordinierte Offenlegung, Sicherheitsmeldung an Betreiber und Nachbetrachtung sind beschrieben, aber noch nie durchlaufen, weil bisher keine Auslieferung eine gemeldete Schwachstelle schließen musste.

Verbleibende Stärken im Überblick

Damit dieser Bericht nicht den falschen Eindruck hinterlässt – die folgenden Eigenschaften sind in einem Produkt dieser Größenordnung ungewöhnlich und würden in einer Prüfung positiv auffallen:

1. **Ehrliche Grenzziehung.** Die Dokumentation sagt ausdrücklich, was das Produkt nicht leistet: keine Ende-zu-Ende-Verschlüsselung, keine Fernlöschung, kein Zertifizierungsanspruch, Lesbarkeit der Inhalte durch den Betreiber. Bei der Prüfung wurde jede sicherheitsrelevante Aussage der Dokumentation gegen den Code gehalten; es blieb keine Zusicherung stehen, die der Code nicht einlöst.
2. **Durchgängiges Fail-Closed-Verhalten.** Virenscanner nicht erreichbar in Produktion – Upload abgelehnt. Überwachungsschnittstelle ohne Zugriffstoken in Produktion – nicht gefunden. Signaturschlüssel fehlt – Ablehnung. Migrationsregister nicht auflösbar – Abbruch. Dieses Muster ist konsequent, nicht punktuell.
3. **Nachweise statt Behauptungen.** Zu jeder Sicherheitsmaßnahme existiert ein Test, der fehlschlägt, sobald sie entfernt wird. Das ist der Unterschied zwischen „umgesetzt" und „nachweisbar umgesetzt".
4. **Aus der Realität erzeugte Rechtsdokumente.** Maßnahmenverzeichnis, AVV-Vorlage und Löschkonzept entstehen aus der Live-Konfiguration der jeweiligen Instanz. Eine Abweichung zwischen dokumentiertem und tatsächlichem Zustand ist damit ausgeschlossen – eine Eigenschaft, die in der Praxis selten erreicht wird.
5. **Schwachstellenprüfung der Fremdbibliotheken als Baufehler.** Ab Schweregrad „niedrig", einschließlich transitiver Abhängigkeiten. Strenger als üblich.

Gültigkeit

Dieser Bericht beschreibt den Produktstand 1.3.0 (Build 26302) zum Prüfstand 1. November 2026. Er ist eine Selbstauskunft des Herstellers auf Grundlage einer strukturierten Prüfung des Quellcodes und ersetzt kein Audit einer akkreditierten Stelle.

Software Notion · Sebastian Kruse · Kornblumenring 40 · 31600 Uchte · Deutschland · https://software-notion.de