VIVODEPOT

Technisches Konzept und Datenblatt

Stand November 2026

Vivodepot GmbH, Berlin
Quelltext: github.com/vivodepot/vivodepot (EUPL-1.2)

Vivodepot ist ein persönliches Depot, das alles Wichtige eines Lebens an einem Ort zusammenbringt – Familie, Finanzen, Wohnen, Arbeit, Gesundheit –, verschlüsselt und bei den Menschen selbst. Es besteht aus einer einzelnen HTML-Datei, die im Browser läuft, auch offline. Es braucht weder Installation noch Konto; von sich aus sendet die Anwendung keine Daten aus dem Depot an einen Server. Die Unterlagen liegen verschlüsselt bei der Person selbst. Die Depots anderer Menschen, für die sie sorgt, etwa Kinder, betreute Menschen oder Angehörige, führt sie als Sub-Depots mit, jedes mit eigenem Passwort.

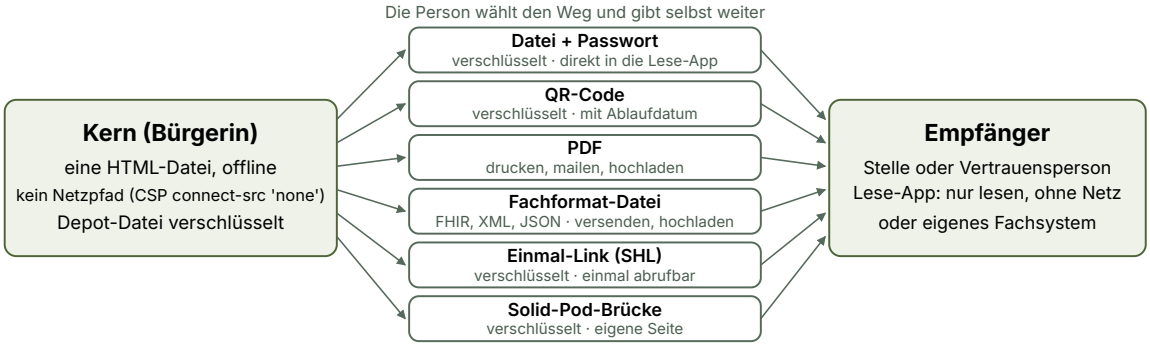
TECHNISCHES KONZEPT

Die Person geht souverän und auf Augenhöhe mit ihren eigenen Daten um. Datenschutz ist dafür die Voraussetzung, aber nicht das Ziel.

- **Die Daten bleiben bei der Person.** Das Depot ist eine verschlüsselte Datei auf ihrem Gerät. Es gibt kein Konto, und das Depot liegt bei keinem Dienst von Vivodepot.
- **Eine Datei, offline.** Die Anwendung ist eine einzelne HTML-Datei und läuft auch offline; von sich aus sendet sie keine Daten aus dem Depot an einen Server.
- **Weitergabe nur auf Veranlassung der Person.** Sie wählt den Weg: verschlüsselte Datei für die Lese-App, QR-Code, PDF, Fachformat-Datei (FHIR, XML, JSON) zum Versenden oder Hochladen ins System der Stelle, Einmal-Link oder Solid-Pod. Mailen, Hochladen oder Übergeben tut sie selbst; über die Dienste von Vivodepot (Ablage, Pod-Brücke) läuft nur Chiffrat.
- **Austausch über Dateien und Links, ohne API.** Vivodepot bietet mit Absicht keine Schnittstelle, über die ein fremdes System auf das Depot zugreift. Einrichtungen behalten ihre Systeme; der Austausch läuft an den Übergängen, über Dateien und Links, die die Person weitergibt oder einliest.
- **Vertrauen über Signaturen statt über einen Server.** Ein öffentlicher Schlüssel ist in jede Anwendung eingebettet; Module, Vorlagen, Zertifikate und Produkte werden gegen diese Kette geprüft.
- **Fester Kern, fachliche Module.** Sprache, Recht, Dokumente, Formate und Erscheinungsbild sind Module; ein Produkt ist der Kern mit einer festen Auswahl.
- **Wachstum durch Bausteine anderer.** Vivodepot legt die Infrastruktur so an, dass sie wächst, weil andere darauf bauen und Bausteine wiederverwenden, etwa die Feldkennungen des Registers (CC0), nicht durch zentrale Sammlung von Daten. Einrichtungen reichen Vorlagen aus dem Studio signiert bei Vivodepot ein, und die Anwendung lässt Module anderer Anbieter ein, deren Zertifikatskette bis zur Trust-Authority führt.
- **Eine Bedeutung je Feld.** Jedes Depot-Feld hat im Feldregister eine dauerhafte Kennung mit fester Adresse. Formate und Vorlagen verweisen darauf, statt die Bedeutung mitzuführen.
- **Offene Standards an den Rändern.** FHIR, SMART Health Links, W3C Verifiable Credentials, Solid.

Komponente	Aufgabe
Vivodepot	Die Anwendung der Person, als Privat und Pro: Depot anlegen, Unterlagen führen, Vorsorgedokumente erstellen, weitergeben.
Lese-App	Für die empfangende Stelle: öffnet, was die Person weitergibt, nur lesend, ohne Speicher, ohne Netz, ohne Konto.
Studio	Für Einrichtungen: Sie richten Vivodepot für ihre Menschen ein, erstellen Vorlagen ohne Programmierung und reichen sie bei Vivodepot ein. studio.vivodepot.org
VC-Issuer	Für die Vertrauensstelle: stellt Anbietern Zertifikate aus, als JWS mit einem Credential nach W3C-Muster.
Feldregister	Das öffentliche Verzeichnis aller Depot-Felder: eine dauerhafte Kennung je Feld unter `register.vivodepot.de/feld/<kennung>`, für Menschen als Seite, für Maschinen als JSON-LD (SKOS), mit Fassungen, Lizenz CC0. An die Kennung knüpfen andere Standards an: Format-Module, Ein- und Ausgaben ordnen ihr Felder aus FIM-Schemata, FHIR-Profilen (IPS, ISiK) und SD-JWT VC zu; eingelesene EDCI-Nachweise ebenso. Die Werte tragen Codes aus LOINC, SNOMED CT, ICD-10, ATC und ISO 4217; die ISiK-Datei trägt zwei KDL-Codes, sobald die Person die KDL selbst geladen hat. Für ESCO und die XÖV-Rollencode-Liste sind Code-Listen angelegt, noch ohne Codes. Das Register ist ergänzbar: Neue Felder kommen mit einer neuen Fassung hinzu, Bezüge zu weiteren Standards kommen als neue Format-Module hinzu, ohne den Kern zu ändern, solange ein vorhandener Leser oder Schreiber (JSON, XML) passt. Ab v1 bleiben vergebene Kennungen unverändert; eine nicht mehr gebrauchte wird deaktiviert, nicht gelöscht.
Dienste	Brückenseite zum Solid-Pod, Ablage für Einmal-Links (nur Chiffrat) und der Download-Dienst, der jedes Produkt nach seinem signierten Rezept ausliefert.

ARCHITEKTUR



Komponente	Merkmale
Kern	Keine Netzanfragen aus dem Depot: Die Content-Security-Policy setzt `connect-src 'none'`. Es gibt keine Telemetrie. Automatisch geprüft wird die Datei: Beim Laden und Benutzen stellt sie 0 Anfragen ins Netz. Eine gehostete Kopie fragt über ihren Service Worker beim eigenen Server nach Aktualisierungen.
Speicherung	Die Datei ist das Depot. Der Browserspeicher (IndexedDB) dient nur als Zwischenspeicher; die Depotinhalte liegen dort nur als Chiffrat.
Kryptografie	PBKDF2-HMAC-SHA-256 mit 600.000 Iterationen, daraus HKDF-SHA-256 je Depot, daraus AES-256-GCM. Jede Verschlüsselung erhält einen frischen, zufälligen 96-Bit-IV. Die AAD bindet Kryptoversion, Iterationen und KDF-Typ. Für ein vergessenes Passwort lässt sich ein Wiederherstellungs-Code einrichten. Ableitung, Verschlüsselung und Signatur laufen über die Web Crypto API; nur den öffentlichen Ed25519-Schlüssel berechnet die eingebettete Bibliothek noble-ed25519. Die geheimen Schlüssel des Depots und der Signatur sind als CryptoKey nicht extrahierbar. Testvektoren nach RFC 5869 (HKDF) und NIST CAVP (AES-GCM).
Signatur	Die Halterin signiert mit Ed25519 (JWS, `alg` Ed25519 nach RFC 9864). Beim Prüfen nimmt Vivodepot auch EdDSA und ES256 an. Nachweise, die die Halterin selbst signiert, sind selbst signiert; ohne die Signatur einer Institution tragen sie kein Vertrauen.
Einmal-Link	Der Kern erzeugt lokal eine JWE (`dir/A256GCM`) und einen Link `shlink:/` nach SMART Health Links. Der Schlüssel steht nur im Link. Die Ablage speichert nur Chiffrat. Die Datei ist einmal abrufbar, höchstens sieben Tage lang, und wird danach gelöscht. Diese beiden Regeln setzt die Ablage von Vivodepot durch; der Standard schreibt sie nicht vor.
Solid-Pod	Eine eigene Brückenseite übernimmt den Pod; der Kern bleibt ohne Netz. Über die Grenze geht nur Chiffrat. Anmeldung per Solid-OIDC mit PKCE und DPoP, Zugriff je Freigabe per WAC. Die Bürgerin kann den Zugriff über die Brückenseite zurücknehmen. Erprobt gegen einen lokalen Solid-Server.

MODULARER AUFBAU

Vivodepot besteht aus einem Kern und Modulen. Der Kern bringt Speicherung, Kryptografie, Oberfläche und Prüfung mit; was fachlich wechselt, steht in Modulen: Sprache, Recht, Dokumente, Formate und Erscheinungsbild. Ein Produkt ist der Kern mit einer festen Modulauswahl, als eine einzelne Datei.



Modul	Merkmale
Produkte	Ein Produkt ist eine Kombination aus Kern und Modulen: Sprache, Rechtsraum, Bereiche, Vorlagen, Erscheinungsbild. Kern und Module sind frei kombinierbar. Eine Einrichtung kann so ein eigenes Produkt bekommen, etwa für ungarische Hebammen mit eigener Sprache, eigenen Fachbegriffen und eigenem Startbildschirm; jedes Depot, das damit entsteht, erbt Sprache und Module. Jedes Produkt ist eine Datei, die Module stecken eingebettet darin. Gebaut werden heute Privat und Pro, je auf Deutsch und Englisch; öffentlich abrufbar ist Privat DE/EN.
Sprache	Auch Deutsch ist ein Sprachmodul; je Produkt steckt genau eines darin. Ein weiteres Sprachmodul lässt sich signiert nachträglich einlassen oder von vornherein als eigenes Produkt anlegen.
Rechtsraum	Das deutsche Recht ist ein Modul; der Kern legt kein Land fest. Ein zweiter Rechtsraum ist als Mechanik geprüft, Recht eines anderen Landes ist nicht enthalten.
Dokumente	Patientenverfügung, Vorsorgevollmacht, Betreuungsverfügung und die Verfügung zur digitalen Nachbildung (KI-Verfügung) – ob und unter welchen Bedingungen Texte, Sprachaufnahmen, Fotos und Videos nach dem Tod für eine KI-Nachbildung genutzt werden dürfen – sind Dokumentmodule mit einem gemeinsamen Generator und einer Ausgabeschicht.

Modul	Merkmale
Erscheinungsbild	Marke und Erscheinungsbild sind eigene Register im Kern.
Formate	Ein- und Ausgabeformate docken als Format-Module an. Ein Format-Modul ist eine Beschreibung, kein Code: Es nennt Leser oder Schreiber, Erkennung und die Zuordnung zu den Depot-Feldern. Format-Module lassen sich auch aus Fachschemata erzeugen, etwa aus dem Schema einer FIM-Leistung.
Auslieferung	Jedes Produkt ist als signiertes Rezept beschrieben: Kern-Stand, Sprach-, Rechtsraum- und Bereichsmodule und Vorlagen, je mit SHA-256. Der Auslieferungslauf baut aus dem Rezept die Datei und schreibt ihre Prüfsumme mit ins Rezept. Der Download-Dienst prüft bei jedem Abruf die Signaturkette des Rezepts und die Prüfsumme der Datei; stimmt eine nicht, liefert er nicht aus.

Einlass. Neben den eingebetteten Modulen lassen sich Module nachträglich einlassen. Ein signiertes Modul prüft der Kern gegen den eingebauten Vertrauensanker und zeigt die Prüfstufe an. Ein unsigniertes Modul kann die Person selbst einlassen, außer einem Marken-Modul (Name, Farben, Logo) und einem Verweis auf eine lokale KI-Modelldatei (Name und Prüfsumme einer Modelldatei auf dem eigenen Gerät; der Kern liest dabei keine Datei, lädt nichts und führt nichts aus), die der Kern nur signiert einlässt; ein unsigniert eingelassenes Modul bleibt als „ungeprüft“ gekennzeichnet. Ein Einlass lässt sich nicht rückgängig machen.

ZERTIFIZIERUNG UND SIGNATUR

Komponente	Merkmale
Vertrauensanker	Ein öffentlicher Ed25519-Schlüssel der Vivodepot Trust-Authority ist in die Anwendung, die Lese-App und das Studio eingebettet. Jede Zertifikatskette endet dort. Den Fingerabdruck veröffentlicht Vivodepot zum Abgleich in seiner Sicherheitsrichtlinie auf GitHub.
Zertifikate	Zertifikate sind JWS mit einem Credential nach W3C-Muster und tragen ein Ablaufdatum. Zwischenstellen gibt es in drei Arten: Ausgabestelle, Prüfstelle und Institution; sie zertifizieren Anbieter. Gesperrte Schlüssel stehen in einer eingebetteten Sperrliste, ohne Online-Dienst; eine neue Sperrung erreicht die Person mit der nächsten Fassung. Anbieter-Zertifikate tragen ein Ablaufdatum; für externe Anbieter stellt die Vertrauensstelle sie auf 18 Monate aus.
Module und Vorlagen	Ein signiertes Modul kommt mit Aussteller-Zertifikat, Anbieter-Zertifikat und Modul-Signatur. Die Anwendung prüft die Kette bis zum Anker und leitet die Prüfstufe allein aus den Zertifikaten ab; schlägt ein Schritt fehl, lässt sie das Modul nicht ein. Vivodepot gibt die Muster des Bundesjustizministeriums (BMJ, heute BMJV) und der BZgA (heute BIÖG) unverändert wieder und signiert sie mit einem eigenen Schlüssel. Beide Stellen sind daran nicht beteiligt.
Fassungen	Jede öffentliche Fassung des Quellcodes auf GitHub trägt einen eigenen Tag; seit dem 2. Oktober 2026 ist er signiert und lässt sich mit `git tag –v` gegen den Schlüssel unter vivodepot.de/.well-known/ prüfen. Die Prüfsummen jeder ausgelieferten Fassung stehen in der Sicherheitsrichtlinie auf GitHub.
Konformität	Auf der Testplattform Gazelle (IHE Europe, EHDS Continuous Testing) tragen 4 Testinstanzen den Status „Verified“; außerdem liegen 4 Validierungsberichte vor, alle Schritte und Kriterien bestanden. „Verified“ gilt für die geprüften Testinstanzen; das ist keine Produktzertifizierung und kein Sicherheitsaudit. Die Nennung eines Standards auf dieser Seite ist kein Konformitätsnachweis; geprüfte Ergebnisse stehen je Profil auf der Seite Validierung. vivodepot.de/validierung.html

DATENMODELL UND OFFENE STANDARDS

- **FHIR R4 mit IPS (eu-eps):** Export als FHIR-Bundle. Eine Provenance-Ressource verweist auf jede erzeugte Ressource und hält fest, dass die Person oder ihre Vertretung sie angelegt hat (Autorin, Vorgang „CREATE“, Zeitpunkt). So bleiben selbst eingetragene Daten erkennbar.
- **Die Datenschicht ist sektor-agnostisch.** Andock-Schichten: Medizin über FHIR, Identität über SD-JWT VC, Bildung über EDCI.
- **Über Sektorgrenzen:** Für die Übertragung nutzt Vivodepot SMART Health Links aus der Medizininformatik (HL7-FHIR-Leitfaden „SMART Health Cards and Links“, STU 1), auch für Unterlagen außerhalb der Medizin.
- **Codelisten:** LOINC, ICD-10, ATC, SNOMED CT (Allergene), ISO 4217; angelegt, noch ohne Codes: ESCO, XÖV-Rollencode.
- **Feldregister:** eine dauerhafte Kennung je Feld, maschinenlesbar (JSON-LD/SKOS), Lizenz CC0, Bezugspunkt für die Zuordnungen zu FIM, FHIR, KDL und weiteren Codes in den Ein- und Ausgaben; das Register selbst veröffentlicht die SEMIC-Bezüge, ergänzbar.
- **Urheberschaft:** Einträge werden angehängt, nie überschrieben. Eine Vollmachtskette ist möglich.

IN ENTWICKLUNG

- Empfang in Nextcloud: zuerst als Datei, danach als Brückenseite über WebDAV.
- Übergang zu Post-Quanten-Kryptografie, beschlossen.

Grenzen: Gegen Schadsoftware auf dem Gerät oder eine Browser-Erweiterung mit Zugriff auf die Seite schützt die Anwendung nicht; die Sicherheitsrichtlinie auf GitHub nennt diese und weitere Restrisiken. Ein externes Sicherheitsaudit hat bisher nicht stattgefunden.

Kontakt: Carola Klessen, Geschäftsführerin · Vivodepot GmbH, Körnerstraße 7–10, 10785 Berlin · info@vivodepot.de · vivodepot.de