VIVODEPOT

Technical Concept and Datasheet

As of November 2026

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

Vivodepot is a personal depot that brings everything important in a life together in one place – family, finances, home, work, health – encrypted and kept by people themselves. It consists of a single HTML file that runs in the browser, also offline. It needs no installation and no account; on its own, the application sends no data from the depot to a server. The documents are stored encrypted with the person herself. The depots of other people she cares for, such as children, adults for whom she acts as legal carer, or relatives, she keeps as sub-depots, each with its own password.

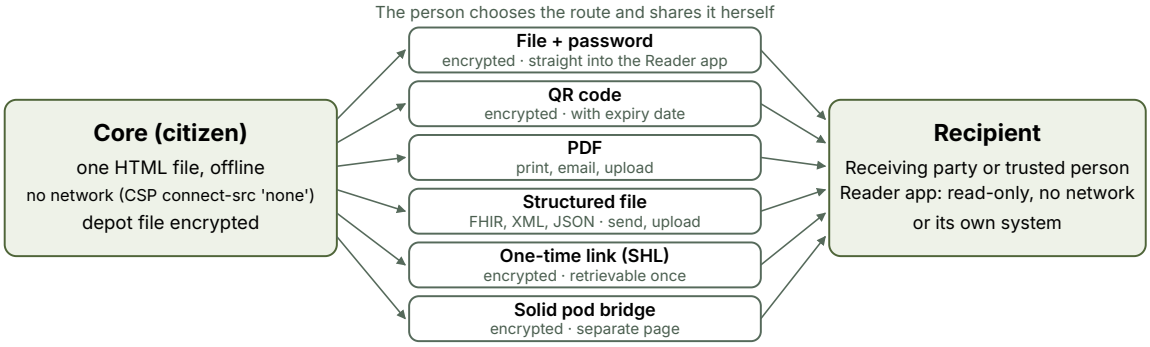
TECHNICAL CONCEPT

The person handles her own data with confidence and on an equal footing. Data protection is the precondition for this, not the goal.

- **The data stays with the person.** The depot is an encrypted file on her device. There is no account, and no Vivodepot service holds the depot.
- **One file, offline.** The application is a single HTML file and also runs offline; on its own, it sends no data from the depot to any server.
- **Sharing only at the person's initiative.** She chooses the route: encrypted file for the Reader app, QR code, PDF, structured file (FHIR, XML, JSON) to send or upload to the recipient's system, one-time link or Solid pod. She sends, uploads or hands over herself; only ciphertext passes through Vivodepot's services (storage, pod bridge).
- **Exchange through files and links, no API.** Vivodepot deliberately offers no interface through which another system accesses the depot. Institutions keep their systems; exchange happens at the transitions, through files and links that the person shares or imports.
- **Trust through signatures instead of a server.** A public key is embedded in every application; modules, templates, certificates and products are verified against this chain.
- **Fixed core, domain modules.** Language, law, documents, formats and appearance are modules; a product is the core with a fixed selection.
- **Growth through others' building blocks.** Vivodepot designs the infrastructure to grow because others build on it and reuse its building blocks, such as the Field Register identifiers (CC0), not through central collection of data. Institutions submit signed templates from the Studio to Vivodepot, and the application admits modules from other providers whose certificate chain leads to the Trust Authority.
- **One meaning per field.** Every depot field has a persistent identifier with a fixed address in the Field Register. Formats and templates refer to it instead of carrying the meaning themselves.
- **Open standards at the edges.** FHIR, SMART Health Links, W3C Verifiable Credentials, Solid.

Component	Function
Vivodepot	The person's application, as Privat and Pro: create a depot, manage documents, draw up advance care documents, share them.
Reader app	For the receiving party: opens what the person shares, read-only, without storage, without network, without an account.
Studio	For institutions: they set up Vivodepot for their people, create templates without programming and submit them to Vivodepot. studio.vivodepot.org
VC-Issuer	For the trust authority: issues certificates to providers, as a JWS with a credential following the W3C pattern.
Field Register	The public directory of all depot fields: one persistent identifier per field at `register.vivodepot.de/feld/<kennung>`, as a page for people and as JSON-LD (SKOS) for machines, with versions, licence CC0. Other standards link to the identifier: format modules, inputs and outputs map fields from FIM schemas, FHIR profiles (IPS, ISiK) and SD-JWT VC to it; imported EDCI credentials likewise. The values carry codes from LOINC, SNOMED CT, ICD-10, ATC and ISO 4217; the ISiK file carries two KDL codes once the person has loaded the KDL herself. Code lists for ESCO and the XÖV role code list are in place, not yet filled. The register is extensible: new fields are added with a new version, and references to further standards are added as new format modules without changing the core, as long as an existing reader or writer (JSON, XML) fits. From v1 onwards, assigned identifiers remain unchanged; an identifier no longer needed is deactivated, not deleted.
Services	Bridge page to the Solid pod, storage for one-time links (ciphertext only) and the download service, which delivers each product according to its signed recipe.

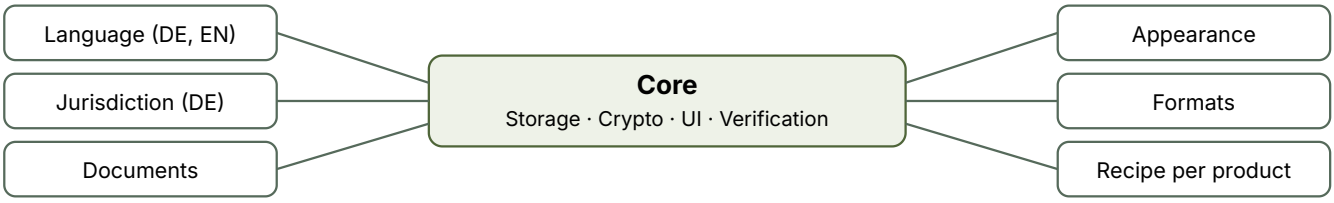
ARCHITECTURE



Component	Characteristics
Core	No network requests from the depot: the Content Security Policy sets `connect-src 'none'`. There is no telemetry. The file is checked automatically: on loading and use it makes 0 network requests. A hosted copy asks its own server for updates through its service worker.
Storage	The file is the depot. Browser storage (IndexedDB) serves only as a cache; the depot contents are held there only as ciphertext.
Cryptography	PBKDF2-HMAC-SHA-256 with 600,000 iterations, from which HKDF-SHA-256 per depot, from which AES-256-GCM. Each encryption uses a fresh, random 96-bit IV. The AAD binds the crypto version, the iterations and the KDF type. A recovery code can be set up for a forgotten password. Derivation, encryption and signing run through the Web Crypto API; only the public Ed25519 key is computed by the embedded library noble-ed25519. The secret keys of the depot and of the signature are non-extractable as CryptoKey. Test vectors per RFC 5869 (HKDF) and NIST CAVP (AES-GCM).
Signature	The holder signs with Ed25519 (JWS, `alg` Ed25519 per RFC 9864). When verifying, Vivodepot also accepts EdDSA and ES256. Credentials that the holder signs herself are self-signed; without the signature of an institution they carry no trust.
One-time link	The core generates a JWE (`dir`/`A256GCM`) locally and a `shlink:/` link per SMART Health Links. The key is only in the link. The storage holds only ciphertext. The file can be retrieved once, for at most seven days, and is deleted afterwards. These two rules are enforced by Vivodepot's storage; the standard does not prescribe them.
Solid pod	A separate bridge page handles the pod; the core stays without network. Only ciphertext crosses the boundary. Sign-in via Solid-OIDC with PKCE and DPoP, access per share via WAC. The citizen can withdraw access through the bridge page. Tested against a local Solid server.

MODULAR STRUCTURE

Vivodepot consists of a core and modules. The core provides storage, cryptography, user interface and verification; whatever varies by domain lives in modules: language, law, documents, formats and appearance. A product is the core with a fixed selection of modules, as a single file.



Module	Characteristics
Products	A product is a combination of core and modules: language, jurisdiction, areas, templates, appearance. Core and modules can be combined freely. An institution can thus get its own product, for example for Hungarian midwives with their own language, their own technical terms and their own start screen; every depot created with it inherits language and modules. Each product is one file, with the modules embedded in it. Currently built are Privat and Pro, each in German and English; publicly available is Privat DE/EN.
Language	German, too, is a language module; each product contains exactly one. A further language module can be admitted afterwards, signed, or set up from the outset as a separate product.
Jurisdiction	German law is a module; the core does not fix any country. A second jurisdiction has been tested as a mechanism; the law of another country is not included.
Documents	Advance healthcare directive, lasting power of attorney, guardianship directive and the directive on digital recreation (AI directive) – whether and on what terms texts, voice recordings, photos and videos may be used after death for an AI recreation – are document modules with a shared generator and an output layer.
Appearance	Brand and appearance are separate registers in the core.

Module	Characteristics
Formats	Input and output formats plug in as format modules. A format module is a description, not code: it names the reader or writer, the detection and the mapping to the depot fields. Format modules can also be generated from domain schemas, for example from the schema of a FIM service.
Delivery	Each product is described as a signed recipe: core version, language, jurisdiction and area modules and templates, each with SHA-256. The delivery run builds the file from the recipe and writes its checksum into the recipe. On every request the download service checks the recipe's signature chain and the file's checksum; if either does not match, it does not deliver.

Admission. In addition to the embedded modules, modules can be admitted afterwards. The core verifies a signed module against the built-in trust anchor and displays the verification level. A person can admit an unsigned module themselves, except a brand module (name, colours, logo) and a reference to a local AI model file (name and checksum of a model file on the person's own device; in doing so the core reads no file, loads nothing and runs nothing), which the core admits only when signed; a module admitted unsigned stays marked as “unverified”. An admission cannot be undone.

CERTIFICATION AND SIGNING

Component	Characteristics
Trust anchor	A public Ed25519 key of the Vivodepot Trust Authority is embedded in the application, the Reader app and the Studio. Every certificate chain ends there. Vivodepot publishes the fingerprint for comparison in its security policy (in German) on GitHub.
Certificates	Certificates are JWS with a credential following the W3C pattern and carry an expiry date. Intermediate authorities come in three kinds: issuing authority, verification authority and institution; they certify providers. Revoked keys are listed in an embedded revocation list, without an online service; a new revocation reaches the person with the next version. Provider certificates carry an expiry date; for external providers the trust authority issues them for 18 months.
Modules and templates	A signed module comes with an issuer certificate, a provider certificate and a module signature. The application verifies the chain up to the anchor and derives the verification level solely from the certificates; if any step fails, it does not admit the module. Vivodepot reproduces the forms of the Federal Ministry of Justice (BMJ, now BMJV) and the Federal Centre for Health Education (BZgA, now BIÖG) unchanged and signs them with its own key; these bodies are not involved.
Versions	Every public release of the source code on GitHub carries its own tag; since 2 October 2026 it has been signed and can be verified with `git tag –v` against the key at vivodepot.de/.well-known/. The checksums of every delivered version are listed in the security policy (in German) on GitHub.
Conformity	On the Gazelle test platform (IHE Europe, EHDS Continuous Testing), 4 test instances hold the status “Verified”; in addition, 4 validation reports are available, with all steps and criteria passed. “Verified” applies to the tested test instances; it is not a product certification and not a security audit. Naming a standard on this page is not proof of conformity; tested results are listed per profile on the Validation page. vivodepot.de/validierung.html

DATA MODEL AND OPEN STANDARDS

- **FHIR R4 with IPS (eu-eps):** export as a FHIR Bundle. Advance healthcare directives, lasting powers of attorney and guardianship directives are included in the Advance Directives section as one Consent resource each; the directive on digital recreation and powers of attorney limited to banking are not. A Provenance resource refers to every generated resource and records that the person or her representative created it (author, activity “CREATE”, time). Self-entered data thus remains identifiable.
- **The data layer is sector-agnostic.** Domains connect through standards: health via FHIR, identity via SD-JWT VC, education via EDCI.
- **Across sector boundaries:** For transfer, Vivodepot uses SMART Health Links from medical informatics (HL7 FHIR implementation guide “SMART Health Cards and Links”, STU 1), also for documents outside medicine.
- **Code lists:** LOINC, ICD-10, ATC, SNOMED CT (allergens), ISO 4217; in place, not yet filled: ESCO, XÖV role code.
- **Field Register:** one persistent identifier per field, machine-readable (JSON-LD/SKOS), licence CC0, reference point for the mappings to FIM, FHIR, KDL and further codes in inputs and outputs; the register itself publishes the SEMIC references, extensible.
- **Authorship:** entries are appended, never overwritten. A chain of delegation is possible.

IN DEVELOPMENT

- Receiving in Nextcloud: first as a file, then as a bridge page via WebDAV.
- Transition to post-quantum cryptography, decided.

Limits: The application does not protect against malware on the device or a browser extension with access to the page; the security policy (in German) on GitHub lists these and further residual risks. An external security audit has not yet taken place.

Contact: Carola Klessen, Managing Director · Vivodepot GmbH, Körnerstraße 7–10, 10785 Berlin · info@vivodepot.de · vivodepot.de