How the Vine Actually Grows

A connection is not a link. It is a growth path.

February 2026

The power of connecting

The biggest misconception about Zero-Knowledge Trust is that it requires everything to change at once. That the world has to flip a switch: one day your data lives in centralized databases, the next day every system supports user-held keys and encrypted vaults. That is not how it works. That is not how any technology transition works.

ZKT starts with a connection. A single connection between a user's vault and an existing system. And that connection can start impossibly thin — just authentication — and grow into full user sovereignty over time, at whatever pace the existing system can absorb.

This is the part of the vine that matters most and is hardest to see from the outside: the connection itself is a growth path. The vine does not just connect to things as they are today. It grows into them.

Medical records: the gradual path

Medical records software is one of the most heavily regulated, deeply entrenched systems in existence. The database holds patient records, login credentials, consent forms, insurance information, and audit logs. Asking the entire healthcare industry to rebuild around user-held keys on day one is not realistic. But asking for a single integration point is.

> **Day one:** The medical records software makes one change. Instead of managing user credentials in its own database, it uses a vault connection for authentication and authorization. The user logs in through their vault. The software still works the same way internally. The database still stores records the same way. But the user's login credentials are no longer in the software's database. That is one integration point, and it eliminates one of the most commonly breached data categories for that system.
>
> **Six months later:** The software starts using the service connection to store sensitive keys and supplementary data in the user's vault sandbox. Maybe encryption keys for

the user's records. Maybe consent forms that the patient controls. Maybe a sharing manifest that determines which providers can see which records. The records still live in the medical system's database, but pieces of the security model are migrating to the user's control.

Eventually: The user holds their own encryption keys for their medical records. The software stores encrypted records that it cannot read without the user's vault authorizing access. The user can grant access to a new doctor by establishing a new vault connection. The user can revoke access to an old provider by severing a connection. Full alignment — the user holds the keys to their own health data.

Nobody had to rip out the medical records system. Nobody had to rebuild the database. The vine grew into the connection, one capability at a time, at a pace the existing system could absorb. The first step was small. The last step was transformative. And every step in between delivered real value.

> *ZKT does not require a revolution. It requires a connection. The connection starts thin and grows as both sides are ready. The vine meets existing systems where they are and grows into them.*

This pattern works everywhere

The medical records example is specific, but the pattern is universal. Any existing system can follow the same progression.

System	Start here	Grow into	Full alignment
Banking	Authentication via vault connection	Transaction signing with user's keys	User holds keys to all financial records and credentials
Employer HR	SSO through vault	Expense and time-off requests via connection	Employee controls all personal and benefits data
Crypto exchange	Vault-based login and KYC	Transaction signing without exchange holding keys	User holds all keys; exchange is execution only
Retail	Checkout authentication	Payment credentials served from vault on demand	No payment data in retailer's database
AI agents	Agent authenticates	Agent requests	Agent has zero stored

	via vault connection	credentials per task, scoped and logged	credentials; all access via vault

Every row follows the same pattern. Start with authentication. Grow the connection. Arrive at sovereignty. The pace is different for each system, but the direction is the same.

Your vine: who I am, what I have, what I can do

From the user's perspective, the vine is simple. You look at your vault and you see three things.

Who I am

Your identity. Name, email, phone, address, organization, verification status. You control which pieces are shared with which connections. Your doctor sees your phone number and address. A retailer sees your name and email. A friend sees what you choose to share. This is not a single public profile. It is a set of controlled projections, each tailored to the relationship — the same way you share different information with your employer, your doctor, and your friends.

What I have

Your inventory. This includes your personal information and the metadata about your secrets. Your vault knows you have a Visa ending in 4242, a CA Driver's License, a Bitcoin key labeled btc_main, and a company signing key. It shows you this inventory. It shows connected services enough metadata to offer you the right options — the retailer knows you can pay with Visa, the exchange knows you have a Bitcoin key — without ever exposing the actual credential data. The card number, the private key, the

license number stay inside the vault until you explicitly authorize a specific operation.

What I can do

Your capabilities in the context of each connection. This is not a raw list of technical features. It is what you see when you look at a specific branch of your vine. When you look at your exchange connection, you see: trade, deposit, withdraw, sign transactions. When you look at your employer connection, you see: submit expenses, request time off, sign documents. When you look at a friend, you see: message, call, share location.

These capabilities are the intersection of what both sides offer. The exchange has to support trading. Your vault has to support transaction signing. When both sides can do their part, the capability appears. When a connection updates its profile — adds a new capability, changes its terms — your vault learns about it automatically. What you can do with each connection evolves as both sides evolve.

> *Who I am. What I have. What I can do. That is the entire view from inside your vault. Your identity, your inventory, and your capabilities — organized by connection, controlled by you, and visible at a glance.*

Branches keep it manageable

As your vine grows, branches keep it organized. Your root connects to a few major branches: financial, professional, personal, healthcare. Each branch is a connection to an entity that runs its own vault with its own connections behind it. The exchange has connections to blockchain networks. Your employer has connections to payroll and HR systems. Your healthcare provider has connections to labs and insurance.

You do not see what is behind each branch. You do not need to. You see what each branch offers you and what each branch asks of you. When a branch needs your secrets — a signature, a credential, a piece of personal data — that request comes back to your vault. You see it, you authorize it, and the branch handles the rest through its own vine. Your root stays lean. Each branch manages its own complexity.

And every request that touches your data is logged. You cannot see through the vine, but nothing that involves your secrets happens without passing through your vault. The vine is opaque outward and transparent inward.

Your vault is a control plane, not an everything-app

The vault handles the moments that matter: signing a transaction, releasing sensitive data for the first time, reviewing a contract update, revoking a connection. Everything else — the browsing, the shopping, the messaging, the dashboards — happens in the services' own apps, with their own interfaces and their own capabilities. A retailer still has a shopping app. Your company still has an HR portal. Your exchange still has a trading interface.

The vault is where authorization decisions are made. It is not where you live your digital life. It is where you govern it. Routine access that you have already approved in a contract happens automatically. Only new, unusual, or out-of-scope requests need your attention. The vault is a choke point by design, and a well-designed choke point is what lets everything else flow.

Multiple vaults: possible, not ideal

Nothing in ZKT prevents you from creating more than one vault. If you want completely separate identities with completely separate connections

and capabilities — one vault for your professional life, another for personal, a third for a side business — you can do that. Each vault would have its own root, its own branches, its own credentials. No connection between them.

This is worth mentioning because it is an honest option, and some users will want it. But it comes with a trade-off: you are creating your own complexity. Multiple vaults mean multiple PINs, multiple passwords, multiple backup responsibilities, and no shared identity across them. The branch model exists precisely to avoid this — a well-organized vine with distinct branches gives you separation without the overhead of managing multiple roots. A professional branch and a personal branch on the same vine are isolated from each other but governed from one place.

For most people, one vault with thoughtful branches is simpler and more secure than multiple vaults. But the architecture does not prevent you from choosing otherwise. It is your digital life.

The vault provider ecosystem

Here is a question people do not think to ask: who said there has to be only one vault provider?

ZKT is an architectural pattern. VettID is one implementation. But the pattern is open, and different providers can specialize in different things. The capabilities a vault offers are determined by the programs the vault provider builds and deploys inside the enclave. Different providers can build different capabilities, serve different markets, and compete on what they do best.

What VettID focuses on

VettID is designed to handle the most critical security and privacy operations for the individual: authentication, authorization, transaction signing, secure messaging with important connections via text, voice, and video, and location tracking. These are the capabilities that touch your secrets, your identity, and your real-time safety. They are the operations that should never be delegated to a system you do not fully trust.

VettID is not trying to be a healthcare platform, a financial trading system, or an enterprise collaboration tool. It is trying to be the one place where the critical operations — the ones that involve your keys, your identity, and your consent — are handled with the highest possible security.

What other providers could focus on

The ecosystem can specialize.

> **A healthcare vault provider** might add capabilities for medical consent management, record-sharing authorization, insurance verification, and clinical trial participation. A patient whose primary concern is health data sovereignty would choose a provider that specializes in those capabilities.
>
> **A financial vault provider** might specialize in multi-party transaction authorization, regulatory reporting, cross-border compliance, and advanced key management for institutional trading. A user managing significant financial assets would choose a provider with deep expertise in financial operations.
>
> **An enterprise vault provider** might focus on organizational key management, role-based access policies, audit trail integration with compliance systems, and fleet management for employee vaults. A company rolling out ZKT across its workforce would choose a provider built for that scale.

The user's vine works the same regardless of provider. The profiles, the connections, the branches, the consent model — these are properties of the ZKT pattern, not of any single implementation. What differs is the set of

capabilities the vault offers. And because capabilities are declared in the profile, every connection on the vine knows what any given vault can do.

The individual chooses

This is the final piece of user sovereignty: you choose the vault that matches your life. If your primary concern is financial security, you choose a provider that excels at financial operations. If your primary concern is healthcare privacy, you choose a provider that specializes in medical data. If you want the broadest coverage of critical security operations, you choose a provider like VettID that focuses on the universal essentials.

The vine does not lock you into a provider. Your connections, your data, your identity — they are yours. The provider is a service, not a custodian. And because ZKT is a pattern rather than a product, the ecosystem can grow, specialize, and compete in the way that best serves individuals.

> *VettID handles the critical operations: authentication, authorization, signing, secure messaging, location. Other providers can specialize in healthcare, finance, enterprise, or domains that have not been invented yet. The user picks the vault that fits their life. The vine grows the same way regardless.*