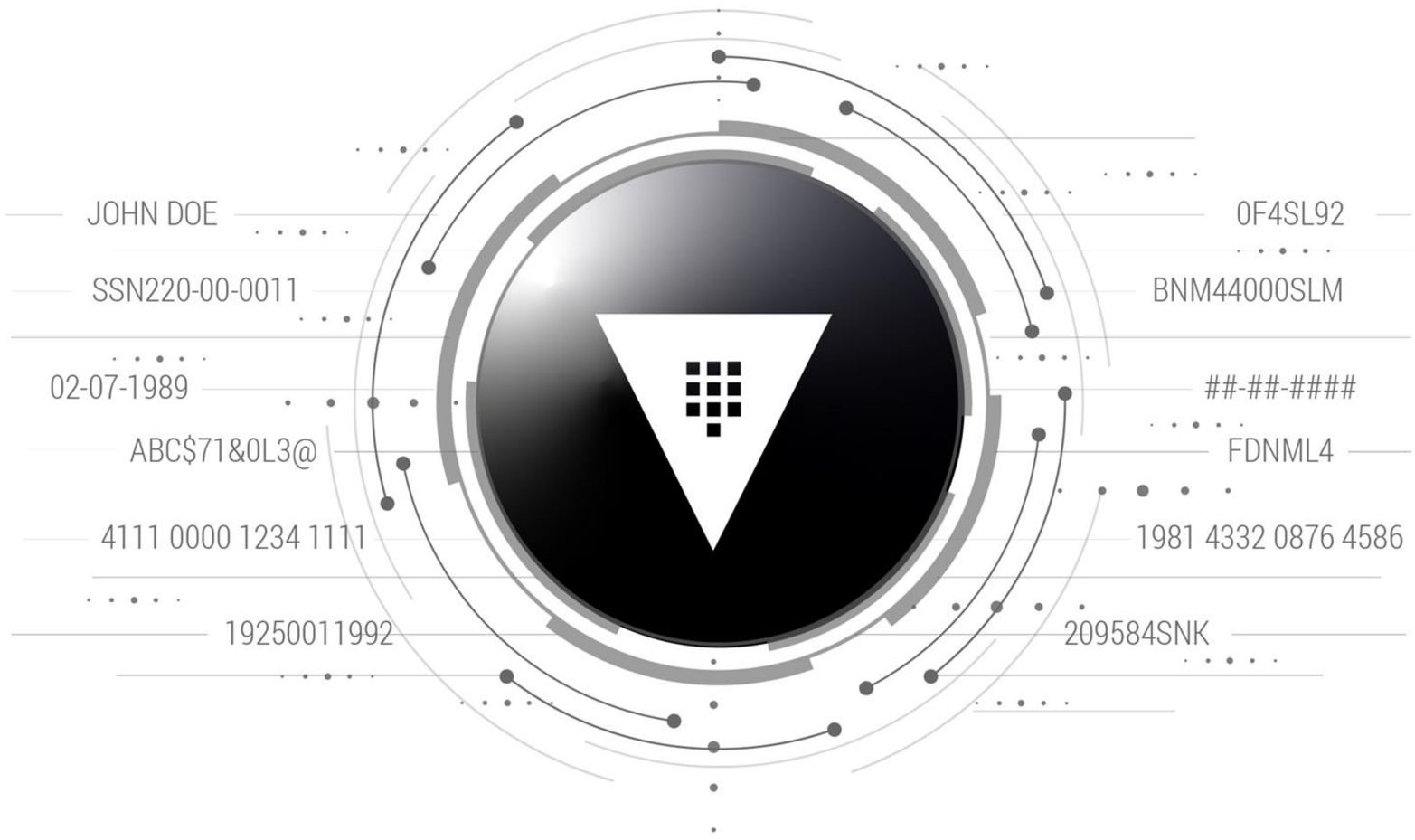
Vault

Transform

Vault Enterprise Brief

Advanced Data Protection



Introducing Vault Transform

Vault Transform is here!

Vault Enterprise - Advanced Data Protection now includes Transform. Transform allows Vault to encode and decode sensitive values residing in external systems such as databases or file systems. This capability allows Vault to ensure that even in the event the system that encoded values reside within is breached (such as their resident database being hacked and its data exfiltrated) that the encoded secrets within remain safe, while balancing the high availability of secrets in these systems, and protecting these secrets pursuant to strict compliance requirements such as PCI-DSS and HIPAA.

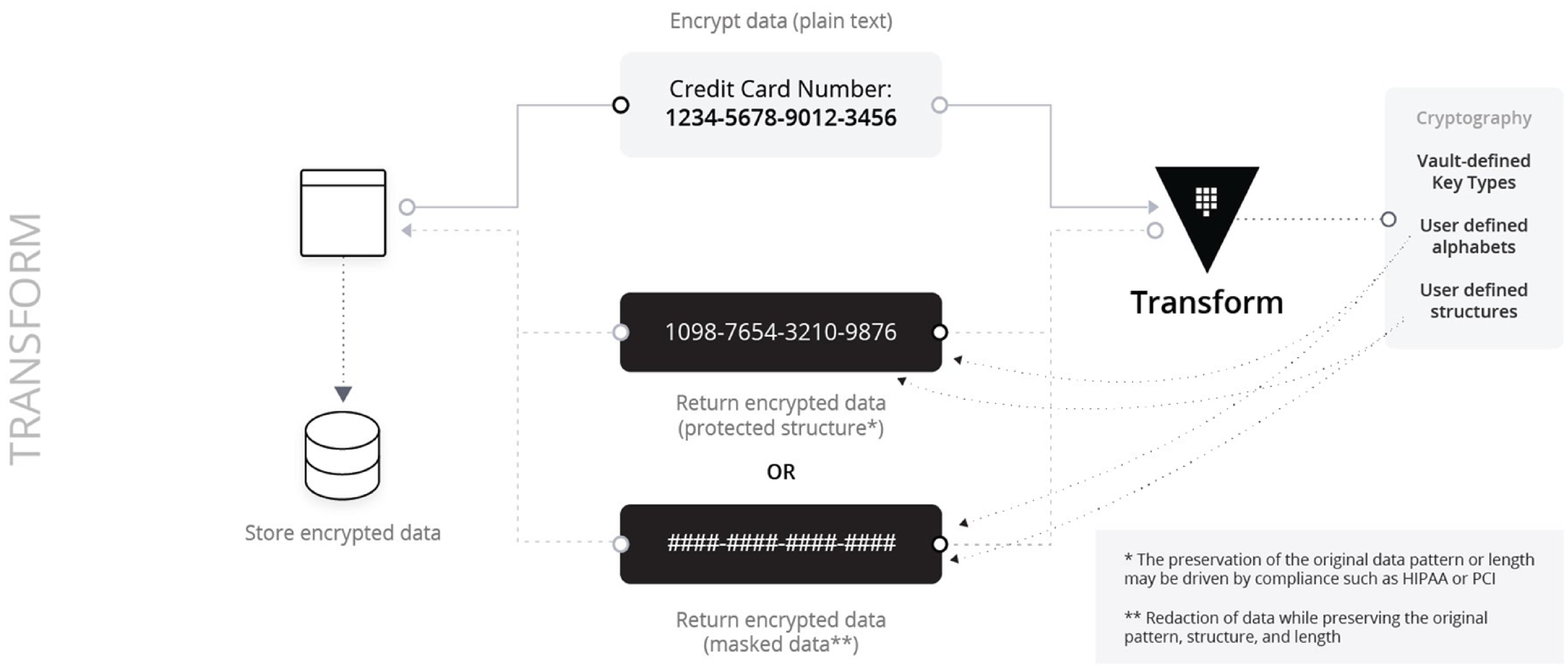
How Does Transform Work

A common request we've had with Vault Enterprise is to protect application secrets stored in external untrusted or semi-trusted systems. Balancing the locality of secrets in these systems, and protecting these secrets pursuant to strict compliance requirements such as PCI-DSS and HIPAA standards.

When protecting secrets such as credit card numbers and other PII data in untrusted/semi-trusted systems pursuant to compliance requirements such as PCI-DSS and HIPAA, companies typically protect data through the use of tokenization. Tokenization is a process that protects secrets by generating random token identifiers for data under its protection, brokering access to that data for trusted applications via a table or ledger associating tokens with their secrets.

Quality tokenization, combined with a strong random number generator, ensures that protected secrets remain secure wherever they reside. However, the format of protected secrets is not retained with traditional tokenization methods utilizing a lookup table or ledger, making it very hard, sometimes impossible, to manage tokenized data within an application or in storage itself. This presents often insurmountable challenges to implementation of a tokenization initiative.

Unlike traditional tokenization, Vault Transform procedure generates **ciphertext** that protects the data's structure and format while maintaining the encoded values' security. With full support for regular expressions, users can customize a pattern and enforce the encoded value subscribing to the schema of that pattern.



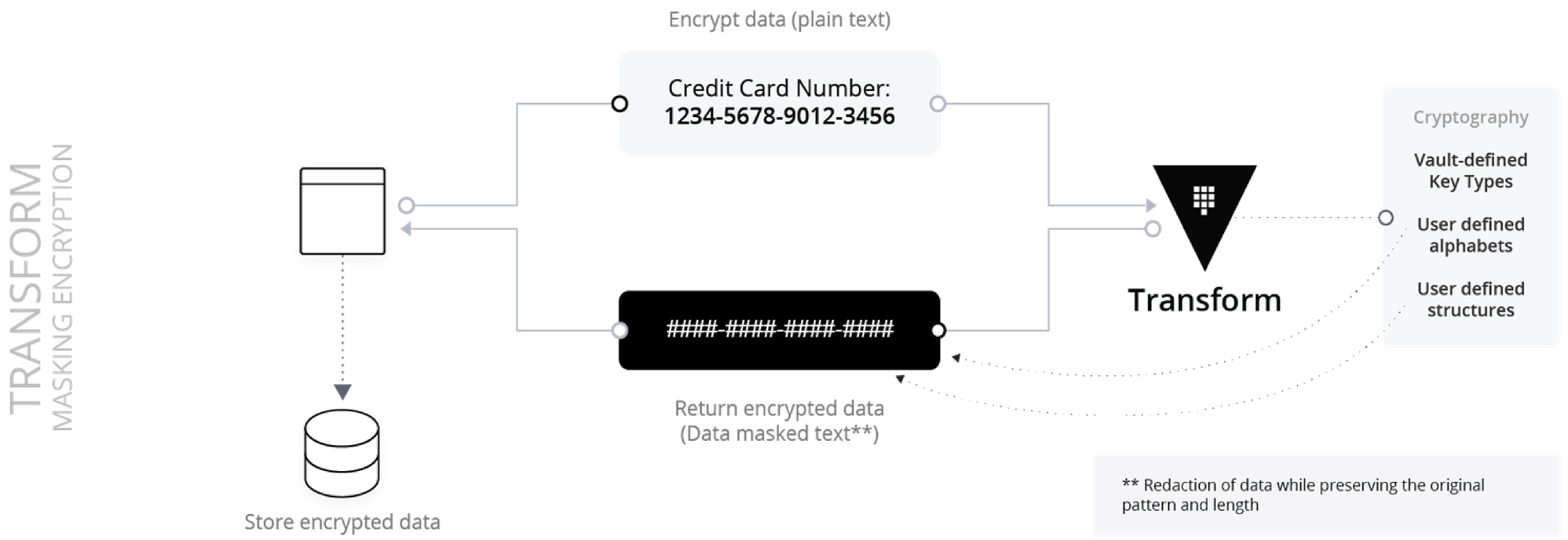
Vault is able to ensure these encoded ciphertexts are secure thanks to its use of **AES FF3-1**, a revision to the FF3 algorithm that proves the algorithm's resilience against chosen-ciphertext attacks and external attacks from future supercomputers while retaining the algorithm's speed and performance. AES FF3-1 is a NIST-approved algorithm recommended in the upcoming NIST SP800-38G standard.

With data type protection, Transform does not actually store the protected secret. Instead it protects only the key material necessary to decrypt the secret's ciphertext. This maximizes encode/decode performance for applications, while also minimizing the possibility of exposure of that secret.

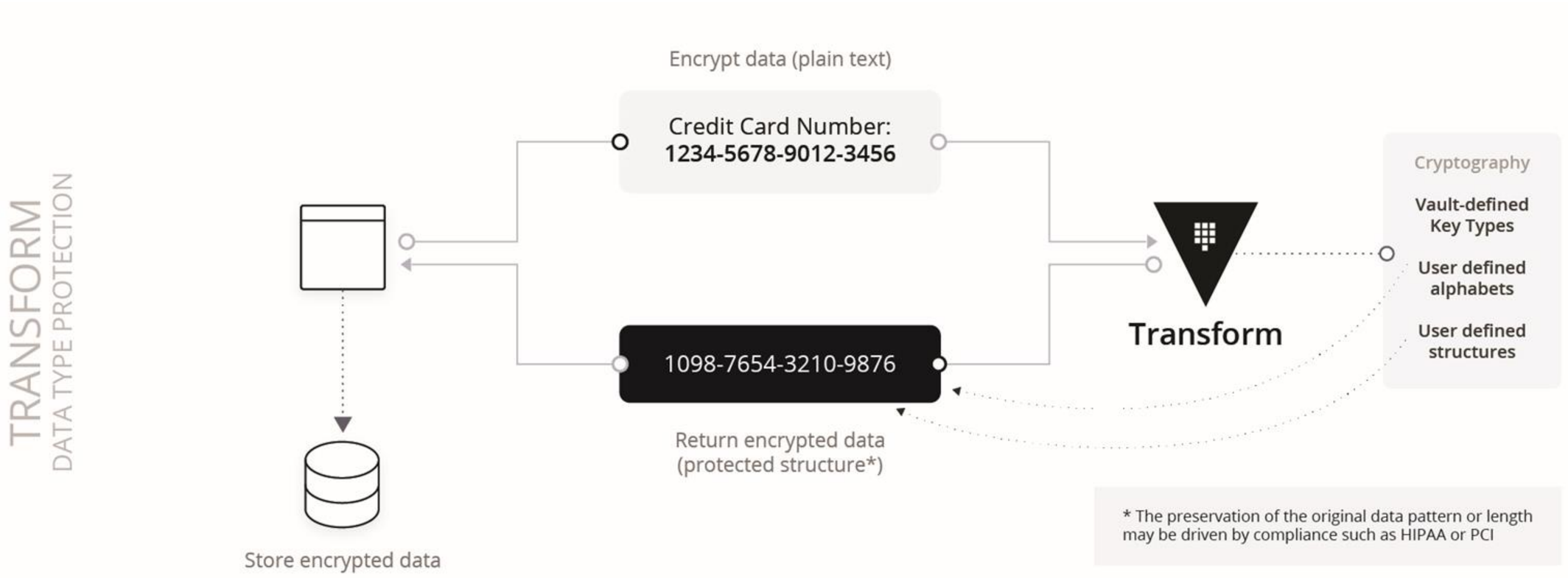
Transform Use Cases

Transform is a Secret Engine that allows Vault to encode and decode sensitive values residing in external systems such as databases or file systems. This capability allows Vault to ensure when an encoded secret's residence system is compromised (such as when a database is breached and its data is exfiltrated), that those encoded secrets remain uncompromised even when held by an adversary.

Transform is capable of two types of transformations. **Masking** is a one-way transformation that allows for Vault to anonymize data per a custom character mask: for example the stars or ampersands displayed on an ATM screen when you type in a debit card's PIN number.



Data type protection is another mode Vault is capable of by performing two-way transformation that allows Vault to quickly and securely encode and decode sensitive data while protecting the structure of the data being encrypted.



Common Use Cases

Data type protection:

- Customer that must store PII data and have compliance requirements such as PCI-DSS and HIPAA (Gov, Retail, Health, Finance, etc)
- Data Analytics workloads; Work with encoded data using the same workflow as production data
- Dev, Test, and Debug envs with real data
- Dev, Test, and Debug envs where they can work with realistic data
- Sharing of dataset where specific users must not be identifiable (edited)
- Analytic software that needs access to data without exposing sensitive information

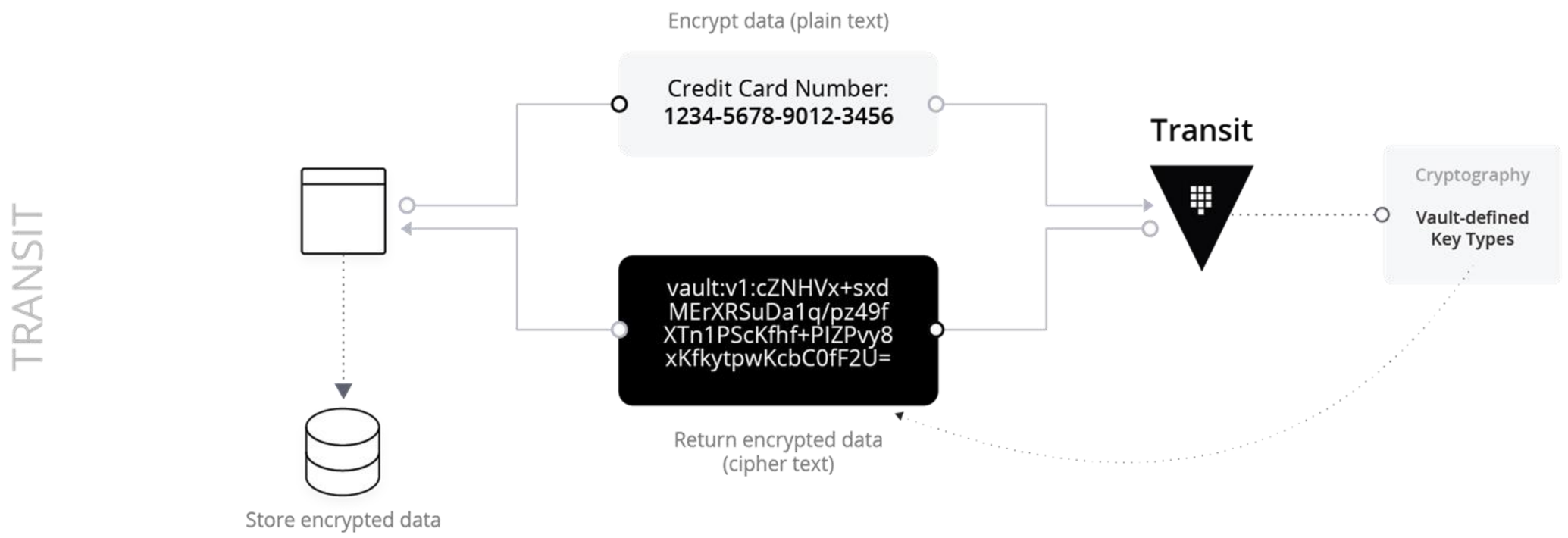
Masking:

- Displaying redacted credit card, phone numbers, or other sensitive data
- ATM screen when you type in a debit card's PIN number

Transform and Transit

Transit (available in Vault Open Source) — handles cryptographic functions on data in-transit. It can also be viewed as "cryptography as a service" or "encryption as a service" by encrypting plaintext into ciphertext. Transit can also sign and verify data; generate hashes and HMACs of data; and act as a source of random bytes. The primary use case for Transit is to encrypt data from applications while still storing that encrypted data in some primary data store. This relieves the burden of proper encryption/decryption from application developers and pushes the burden onto the operators of Vault.

For more, checkout vaultproject.io



Transform (available in Vault Enterprise) — is a different form of encryption that focuses more on user-defined encryption parameters and structures, so that organizations can protect highly sensitive information while retaining the structure and mapping the output. This empowers developers, operations, and security staff to securely work within their own workflows, data parsing, discoverability, while maintaining compliance and governance, all within a single endpoint.

For more, checkout https://www.hashicorp.com/products/vault/advanced-data-protection/