

CARD NETWORK TOKENIZATION.



A network token looks like a real card number to existing payment infrastructure, but it maps back to the actual PAN only inside the card network's own vault. **Domain restriction and a fresh cryptogram per transaction are what make a stolen token nearly worthless outside the exact context it was issued for.**

- NETWORK TOKENIZATION
- DOMAIN RESTRICTION
- DYNAMIC CRYPTOGRAMS
- TOKEN LIFE-CYCLE

01 THE MECHANISM

A Token That Looks Like a Card, Isn't One

A network token is issued in the same format as a real card number so it works with existing payment infrastructure, but it **maps to the real PAN only inside the card network's own secure token vault.**

Domain Restriction Limits Where It Works

Each token is bound to a specific device, merchant, or payment channel at the moment it's provisioned, so a **token extracted from one context generally can't be replayed in another.**

A Fresh Cryptogram for Every Transaction

Beyond the token itself, each transaction carries a one-time dynamic cryptographic value, so **even a captured token can't simply be resubmitted** without it.

02 THE FLOW

The Properly Tokenized Wallet Transaction

CONTAINED

- A card added to a mobile wallet is provisioned as a network token **cryptographically bound to that specific device's secure element**, not general storage.
- Every tap-to-pay transaction generates a fresh, one-time cryptogram alongside the token, so **intercepted transaction data can't be replayed** for a second purchase.
- If the phone is lost, the network token is remotely deactivated in isolation — **the real card number was never exposed** to the device and doesn't need reissuing.

The Compromised Card-on-File Database

EXPOSED

- A merchant's card-on-file database is breached, but the stored values are **network tokens domain-restricted to that merchant**, not usable real card numbers.
- An attacker who extracts the tokens finds they're **rejected everywhere outside the exact merchant and channel context** they were provisioned for.
- The card network revokes and reprovisions only the affected tokens; **no physical card needs to be reissued**, and customers see no fraudulent transaction.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Token Vault / Token Service Provider	The card network's secure system mapping each network token back to the real PAN, accessible only to the network itself.
Domain Restriction	Binding each token to a specific device, merchant, or channel at provisioning, so it functions only in the context it was actually issued for.
Dynamic Cryptograms	A one-time cryptographic value generated per transaction, preventing a captured token from being replayed for a new purchase.
Token Life-Cycle Management	Suspending, updating, or deleting individual tokens independently of the underlying card, without requiring physical card reissuance.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Storing Real Card Numbers for Recurring Transactions	No	Every merchant or wallet holding the real PAN becomes a full-value target; a single breach exposes data usable anywhere.
Merchant-Generated Tokens With No Domain Restriction	No	A token with no binding to a specific device, merchant, or channel can potentially still be replayed wherever the format is accepted.
Tokenization Without Per-Transaction Cryptograms	No	A static token without a fresh cryptogram is still vulnerable to simple replay if it's ever captured in transit.
Treating Network Tokens and Merchant Tokens as Interchangeable	No	They serve different purposes with different scope; confusing them can leave gaps in what's actually protected.
Network Tokens + Domain Restriction + Per-Transaction Cryptograms + Life-Cycle Management	Yes	Combines format compatibility with real cryptographic protection at both the token and transaction level.

CARD NETWORK TOKENIZATION.

TOKENIZE · RESTRICT · VERIFY

05 PROGRAM OPERATIONS

A stolen network token is worth far less to an attacker than a stolen real card number, since it's functionally useless outside the specific device, merchant, or channel it was provisioned for.

Domain restriction is what separates network tokenization from simple format-preserving substitution — the binding to a specific context is the actual security control.

Network tokens update automatically when a card is reissued, which is why a subscription doesn't fail just because a customer's physical card was replaced.

Merchant-side PCI tokenization and network-level tokenization solve different problems and can both exist in the same transaction — reducing compliance scope isn't the same as reducing fraud value.

06 CONTROL MAPPING

EMVCO TOKENISATION SPEC

The cross-industry standard, jointly owned by the major card networks, defining how network tokenization actually works.

VISA TOKEN SERVICE / MASTERCARD MDES

The network-operated token vaults and provisioning infrastructure that issue and manage tokens on behalf of issuers.

TOKEN DOMAIN CONTROLS

The EMVCo framework for restricting a token's validity to a specific device, merchant, or channel at provisioning.

PCI DSS TOKENIZATION GUIDELINES

The merchant-focused counterpart addressing how tokenization interacts with cardholder data environment scope, distinct from network-level tokenization.

07 WHAT THIS DOES NOT SOLVE

Endpoint or Wallet App Compromise

Tokenization protects the credential itself; it **doesn't stop a compromised device or app** from initiating fraudulent transactions using a token it's authorized to use.

Social Engineering the Cardholder

A domain-restricted token doesn't stop a victim from being **talked into authorizing a transaction directly**, since the token still works exactly as intended in that context.

Issuer-Side Card Data Exposure

Tokenization protects what merchants and wallets store; it **doesn't address a breach at the card issuer itself**, where the real PAN necessarily still exists.

Universal Merchant Adoption

Tokenization's fraud-reduction benefit depends on merchants and wallets **actually adopting network tokens** instead of continuing to store raw card numbers.

08 MYTHS VS. REALITY

MYTH "A network token and a merchant PCI token are the same thing."	REALITY They solve different problems — network tokens are cross-industry and domain-restricted; merchant tokens typically only reduce that merchant's own compliance scope.
MYTH "If a network token is stolen, it works just like a real card number."	REALITY Domain restriction means a token generally only works in the specific device, merchant, or channel it was provisioned for.
MYTH "Tokenization means no cryptographic protection beyond the token itself."	REALITY Each tokenized transaction also carries a dynamic, one-time cryptogram, preventing simple replay even if a token is captured.
MYTH "Getting a new physical card breaks every subscription tied to the old number."	REALITY Network tokens update automatically behind the scenes, so most tokenized recurring payments continue without interruption.
MYTH "Tokenization is just EMV chip technology applied to online payments."	REALITY EMV chip cryptography protects the physical card-present transaction; network tokenization is a related but distinct standard protecting stored and remote credentials.

09 SPEAK THE PROGRAM — KEY TERMS

NETWORK TOKEN

A card-network-issued substitute for a real card number, formatted to be compatible with existing payment systems but **mapped to the PAN only inside the network's vault**.

TOKEN SERVICE PROVIDER (TSP)

The card network's secure system that issues tokens and is the **only party able to map a token back** to the real card number.

DOMAIN RESTRICTION

Binding a token's validity to a **specific device, merchant, or payment channel** at the moment it's provisioned.

CRYPTOGRAM

A dynamic, one-time cryptographic value generated for each transaction, **preventing captured token data from being simply replayed**.

TOKEN LIFE-CYCLE MANAGEMENT

Suspending, updating, or deleting a token independently of the underlying card, **without requiring the physical card to be reissued**.

EMVCO

The standards body jointly owned by the major card networks that **publishes the specification defining how payment tokenization works** across the industry.