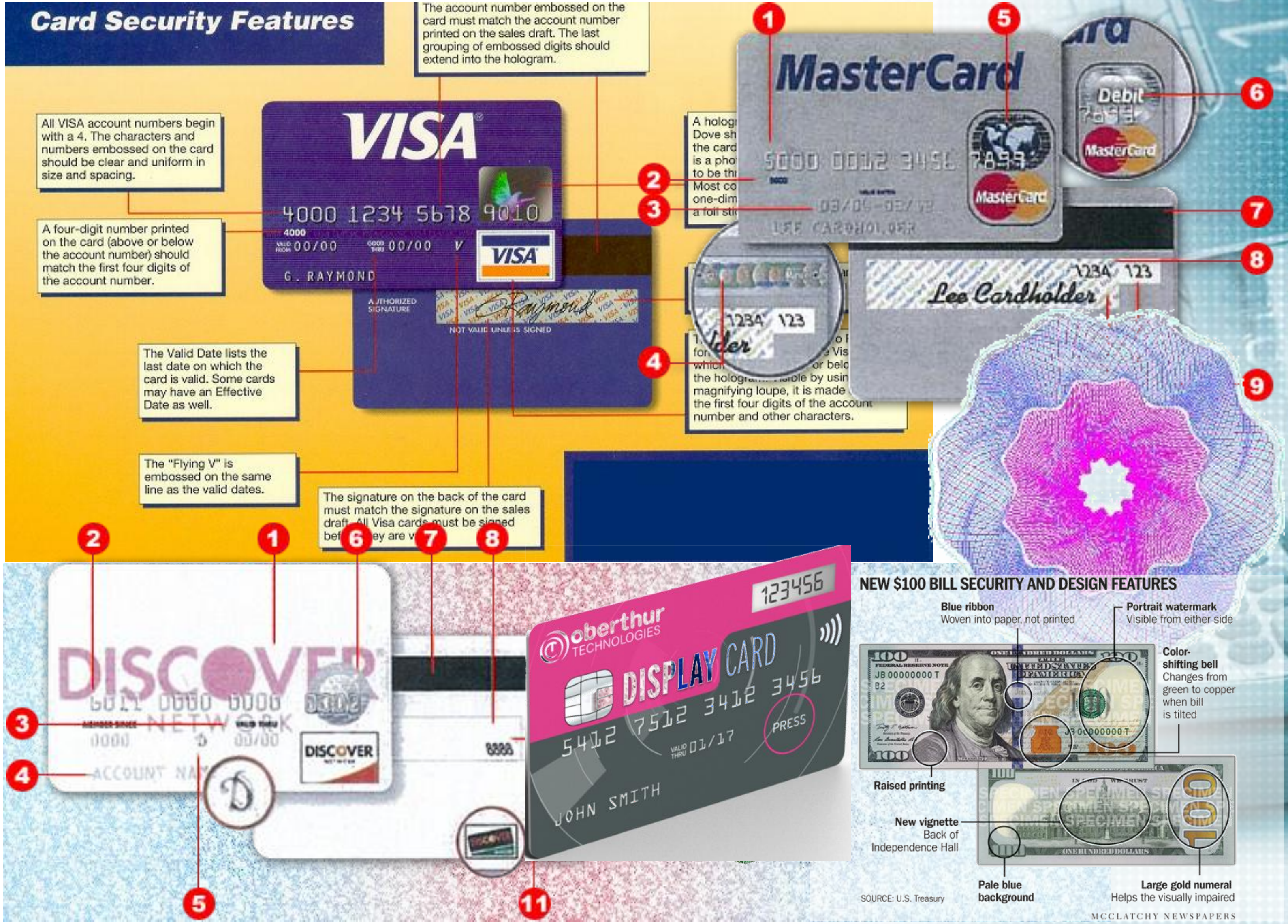
Tokenization and Payments

Philip Andreae
Oberthur Technologies

For Payments the Cards Is the Token Protected With Physical Security Features



Card Security Features

The account number embossed on the card must match the account number printed on the sales draft. The last grouping of embossed digits should extend into the hologram.

All VISA account numbers begin with a 4. The characters and numbers embossed on the card should be clear and uniform in size and spacing.

A four-digit number printed on the card (above or below the account number) should match the first four digits of the account number.

The Valid Date lists the last date on which the card is valid. Some cards may have an Effective Date as well.

The "Flying V" is embossed on the same line as the valid dates.

The signature on the back of the card must match the signature on the sales draft. All Visa cards must be signed bef ey are v

A hologr
Dove sh
the card
is a pho
to be thr
Most co
one-dim
a foil stic

T
for Vis
which or belo
the hologra isible by usin
magnifying loupe, it is made
the first four digits of the account number and other characters.

NEW $100 BILL SECURITY AND DESIGN FEATURES

SOURCE: U.S. Treasury

MCCLATCHY NEWSPAPERS

Smart Card Alliance

The Physical Security Features of the Card
Once Acted as the Secure Token

Card Security Features

Hologram

Authentication

Magnetic Stripe

Online Authentication (CSC/CID)

What You Have

Verification

Signature

What You Know

Circa 1991

No Longer

Secure

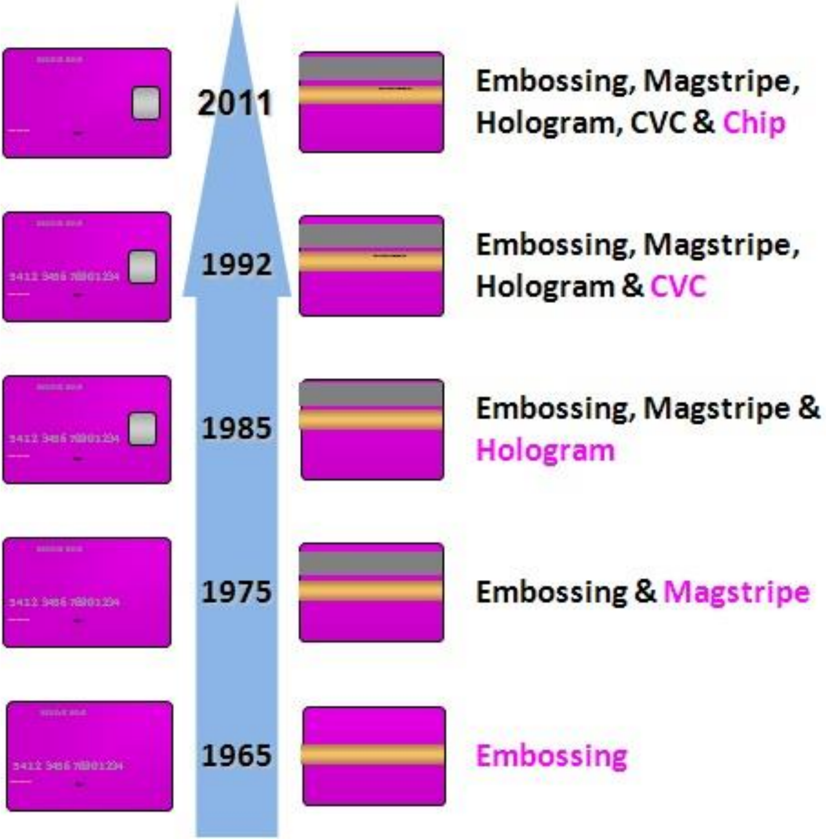
Authorization

Are You Able

Terminal Floor Limit

Securing payments is a never ending battle

The Physical World is being Protected "Chip and Choice"


2011
Embossing, Magstripe, Hologram, CVC & Chip
1992
Embossing, Magstripe, Hologram & CVC
1985
Embossing, Magstripe & Hologram
1975
Embossing & Magstripe
1965
Embossing

The Virtual World is the Target

- A card not present transaction (CNP, MO/TO, Mail Order / Telephone Order) is a payment card transaction where the cardholder does not present the card for a visual examination
- Circa 1992 Mail Order Telephone fraud demanded the introduction of CVV2/CVC2 CID or CSC2
- May 1997 SET is published It fails Contributors Amex, IBM, JCB, MasterCard, Microsoft, Netscape , RSA, Visa ... VeriSign
- Starting In 2001 American Express, Discover, MasterCard and Visa embrace and introduce 3D-Secure 1.0 unsuccessfully
- Merchants start using device fingerprints
- January 2015 EMVCo initiatives developing of 3D-Secure 2.0

Bottom Line Consumer Convenience Trumps Security

Smart Card Alliance

oberthur TECHNOLOGIES

Lets Get Back to Basics

How Do We Secure Payments and Assure Consumer Convenience?

That is the Imperative

The Key to Secure Identification

Multi-Factor Authentication

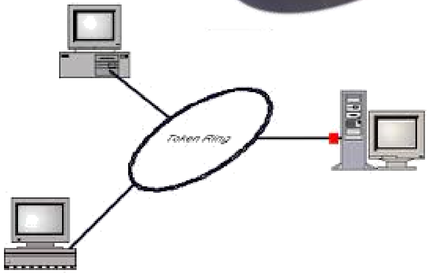
- Something You Have ✓ The Token
- Something You Know ✓ The Secret
- Something You Are ✓ Biometric

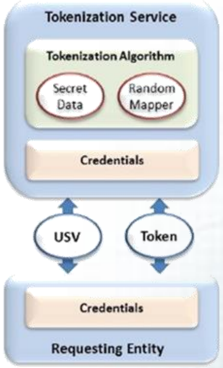
Offering Issuers & Merchants Relying Party Identification, Authentication, Verifications & Authorization

CAM	CVM
Card / Credential Authentication Method	Cardholder Verification Method

What is a Token – Extract from Wikipedia

- **Currency** - Token coin, a piece of metal or other composition used as a substitute for currency
- **Computing** - Token, an object which represents the right to perform some operation
  - Security token or hardware token, authentication token or cryptographic token, a physical device for computer authentication
  - Tokenization (data security), the process of substituting a sensitive data element
  - Session token, a unique identifier of an interaction session
- **Other uses**
  - Game piece (board game), or counter used in a game
  - Token (railway signalling), a physical object given to a locomotive driver to authorize him to use a particular stretch of single railway track




Tokenization Service

Tokenization Algorithm

Secret Data

Random Mapper

Credentials

USV

Token

Credentials

Requesting Entity

Three Capabilities Required to Assure Our Identity and Individual Security

Authentication

"What you have
A Token"

Tested Locally
Trusted Credentials
& Digital Signaturres
Tested in the Cloud

Verification

"What you know
A Secret"

Match On Card
the rightful party is
presenting the
credentials
Verified In Cloud

Authorization

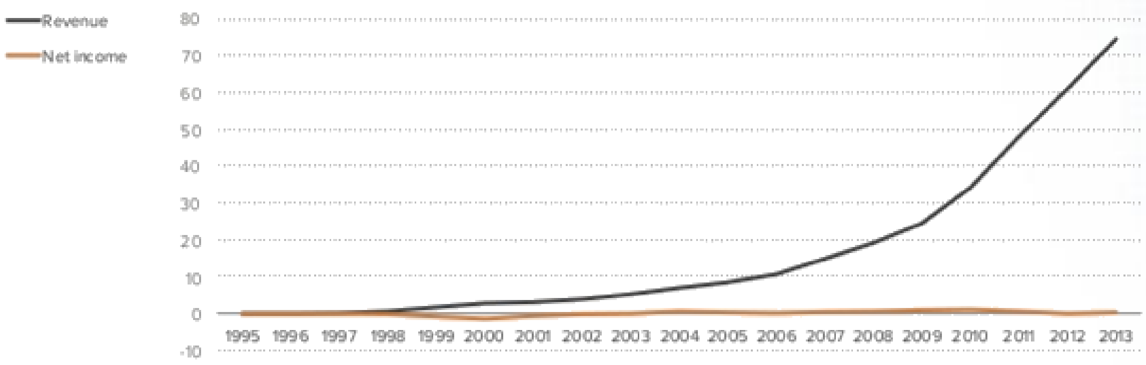
"You have the Right or the Funds
Because someone says you can"

Offline / Local
Algorithms in Card

Online / Cloud
Host Authorized

CNP and Counterfeit Fraud

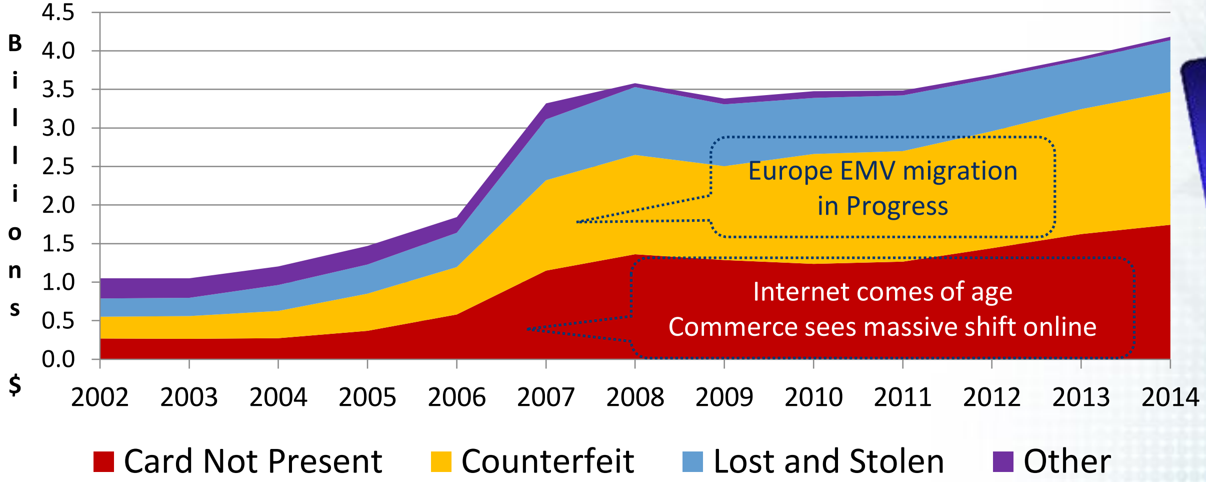
Amazon since launch ($bn)



Source: Amazon

US Total Dollar Fraud

Euromonitor Data



Europe EMV migration in Progress

Internet comes of age
Commerce sees massive shift online

The World Wide Web Broke the Token

YET ON THE INTERNET
HE TOKEN IS NOT PRESENTED

Smart Card Alliance

oberthur TECHNOLOGIES

Tokenization in the 21st Century

Chasing the Broken Token

What is Tokenization

- Tokenization
  - Is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token
  - The token has no extrinsic or exploitable meaning or value
  - The token maps back to the sensitive data through the Token Service Provider TSP
  - The mapping from the PAN to the token uses methods which render tokens infeasible to reverse in the absence of the TSP.
  - The TSP must be PCI Compliant capable to secure sensitive data, securely store the PAN, audit, authentication and authorization
  - The TSP de-tokenizes the token back to sensitive data the “PAN”

SCA white paper - Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization – Oct 2014

Defines and Describes Tokenization in the Payment Environment

- As a mechanism to remove high-value account data and replace it with something that is useless a surrogate value
- Tokens can be:
  - Merchant specific
  - Single use or multi-use
  - Stored and managed
    - In the cloud
    - In a token vault
    - At a merchant location
- A token is created using a process defined by the token solution provider
- Once created, it may used as a card on file, For individual transaction, on the payment card, or in the device.
- Two types of tokens are being used and/or defined
  - Tokens that will be used to perform a payment transaction
  - Tokens that will be stored by merchants and/or acquirer
- The tokenization creation and management process, use of tokens in a payment transaction, and business relationships differ based on the type of credential.

Smart Card Alliance

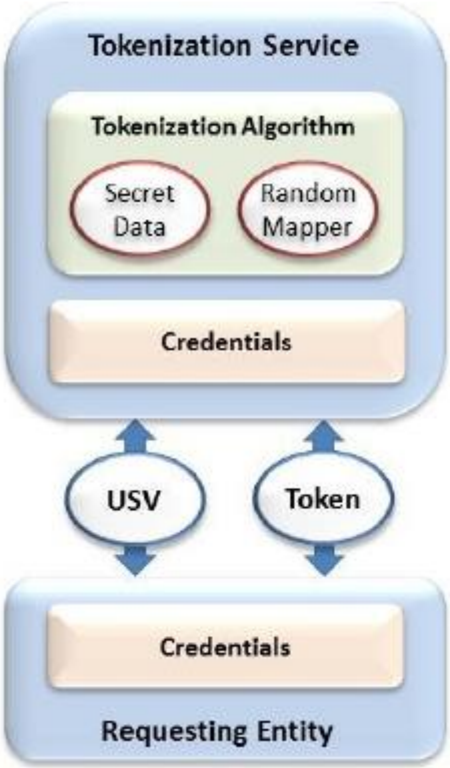
oberthur TECHNOLOGIES

Evolution of Tokenization Standards

- ISO ID1 Card Standards 7810,7811,7813, 7816 & 14443
- ANSI X9 as X9.119 Part 2
- The Clearing House
- The PCI Council
- EMVCo LLC

ANSI ASC X919

- The X9 F6 work group is working on a security tokenization standard that addresses tokens used after initial payment authorization, such as when an acquirer provides tokenization services to merchants
- X9 F6 is working on the requirements for secure design and implementation of this security tokenization process, including:
    - A list of acceptable algorithms to implement the random mapping of USVs to tokens and the required strength of those algorithms
    - Requirements for the protection of the tokenization service
    - Requirements for tokenization service access control



The Clearing House Tokenization Initiative

- The initial Secure Token Exchange standards were very similar to the EMVCo standards published in March 2014

- The Clearing House is adopting the core EMVCo messages to allow for industry interoperability while retaining proprietary provisioning, exceptions and lifecycle management flows

- The Clearing House also proposed several changes to the current EMVCo specifications to include these flows and to increase the overall safety and soundness of the framework

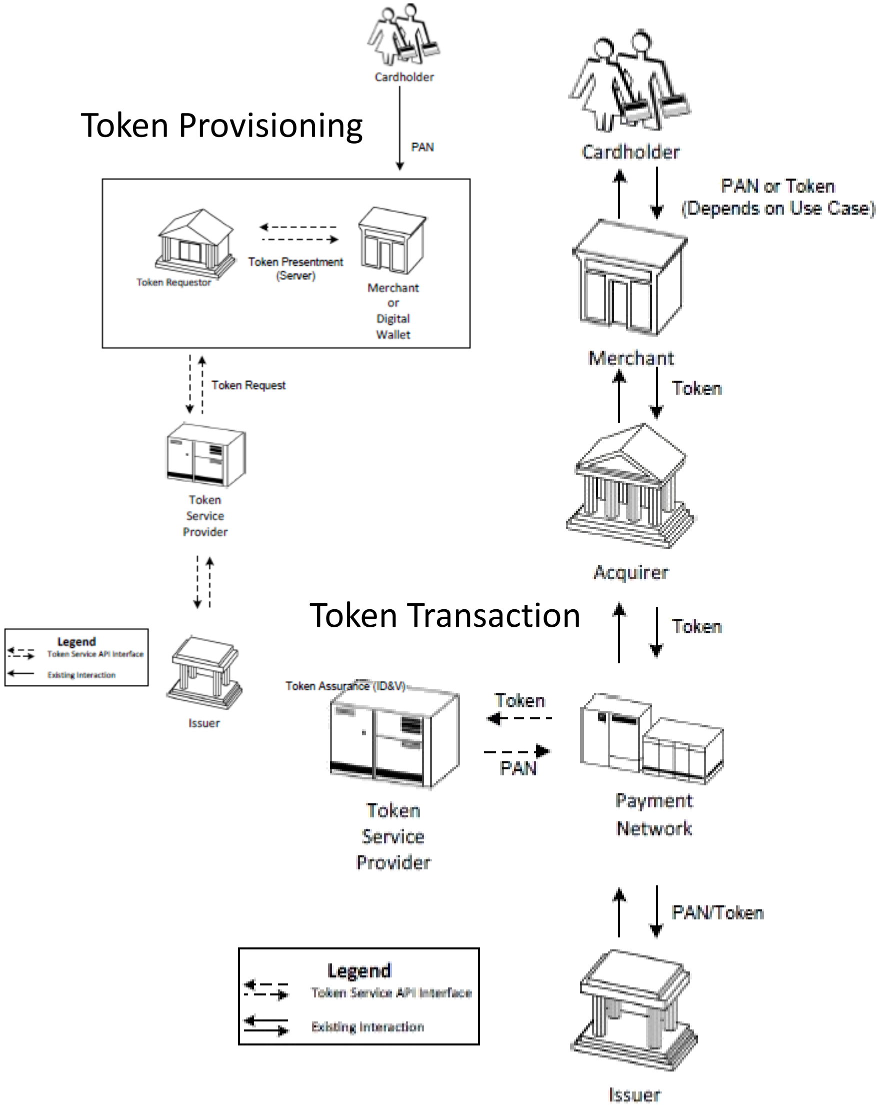
- It is the position of U.S. banks that greater standardization of tokenization specifications will allow for faster adoption and innovation

PCI Tokenization Initiative

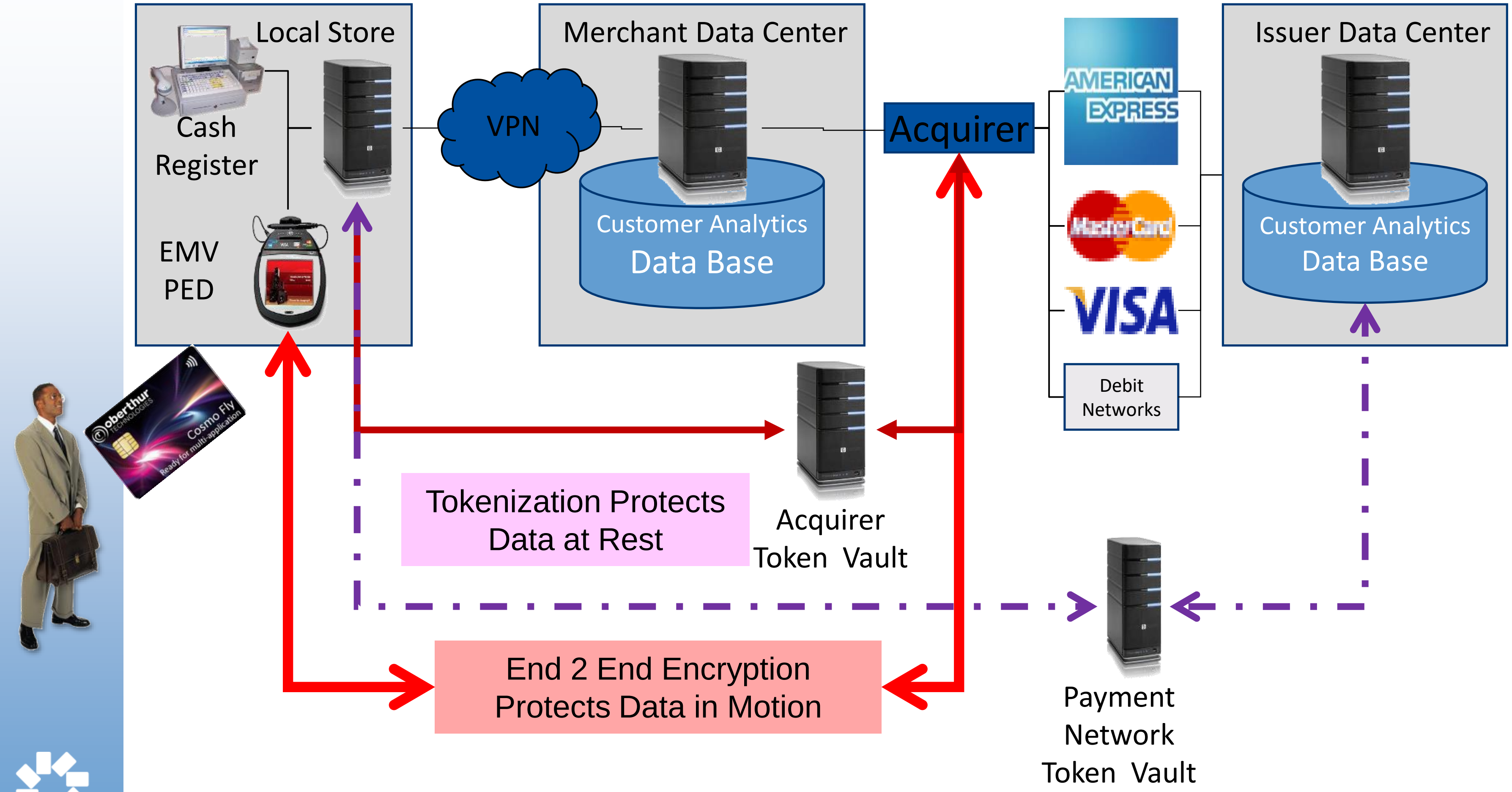
- The PCI SSC is developing security requirements for tokens that replace a PAN with a token
- The tokenization processes described by PCI include functionality to exchange a token back to the original PAN (“de-tokenization”) as well as “irreversible” tokens for which there is no mechanism supported to reproduce the PAN
- The goal to remove the need to store PANs, reducing the risk of unauthorized disclosure, and is focused on tokens used in the acquiring environment.

EMV Payment Tokenization Specification

- March '14, EMVCo version 1.0
- The key stakeholder is the TSP
- The framework outlines Provisioning and Transaction processing
- The TSP shall implement
  - An assurance level identifying the level of "Identification and Verification" ID&V performed when provisioning the token
  - Restrict tokens by domain
  - A set Application Programming Interfaces or APIs
- The Focus was Web Payments
- Apple Pay embraced what American Express had already done enabling MasterCard and Visa to develop the TSP



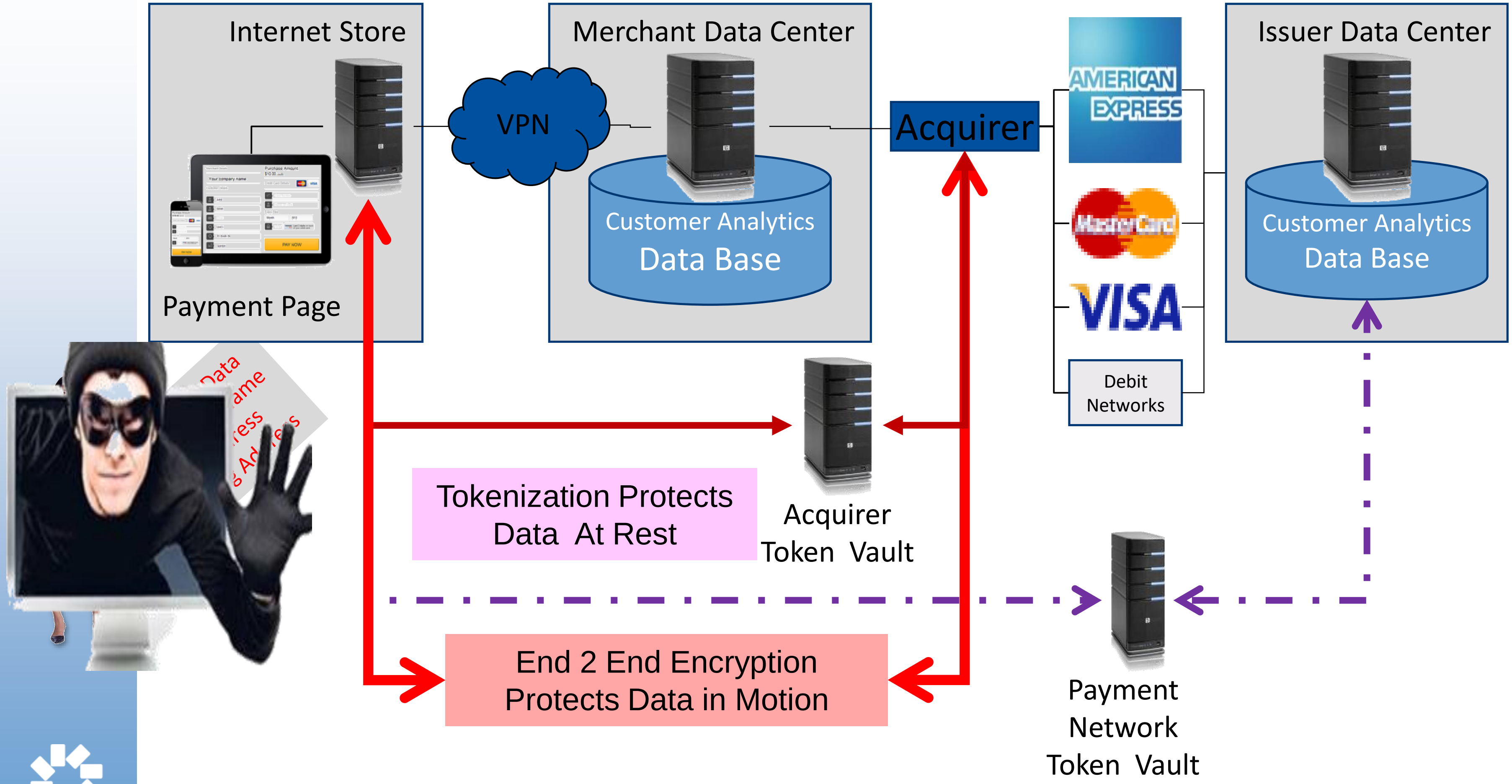
For the Physical World
A Layered Approach with EMV at the Point of Sales Works



Tokenization Protects Data at Rest

End 2 End Encryption Protects Data in Motion

For the Virtual World
Two Factor Authentication is Required



Internet Store

Payment Page

VPN

Merchant Data Center

Customer Analytics
Data Base

Acquirer

AMERICAN EXPRESS

MasterCard

VISA

Debit
Networks

Issuer Data Center

Customer Analytics
Data Base

Tokenization Protects
Data At Rest

Acquirer
Token Vault

End 2 End Encryption
Protects Data in Motion

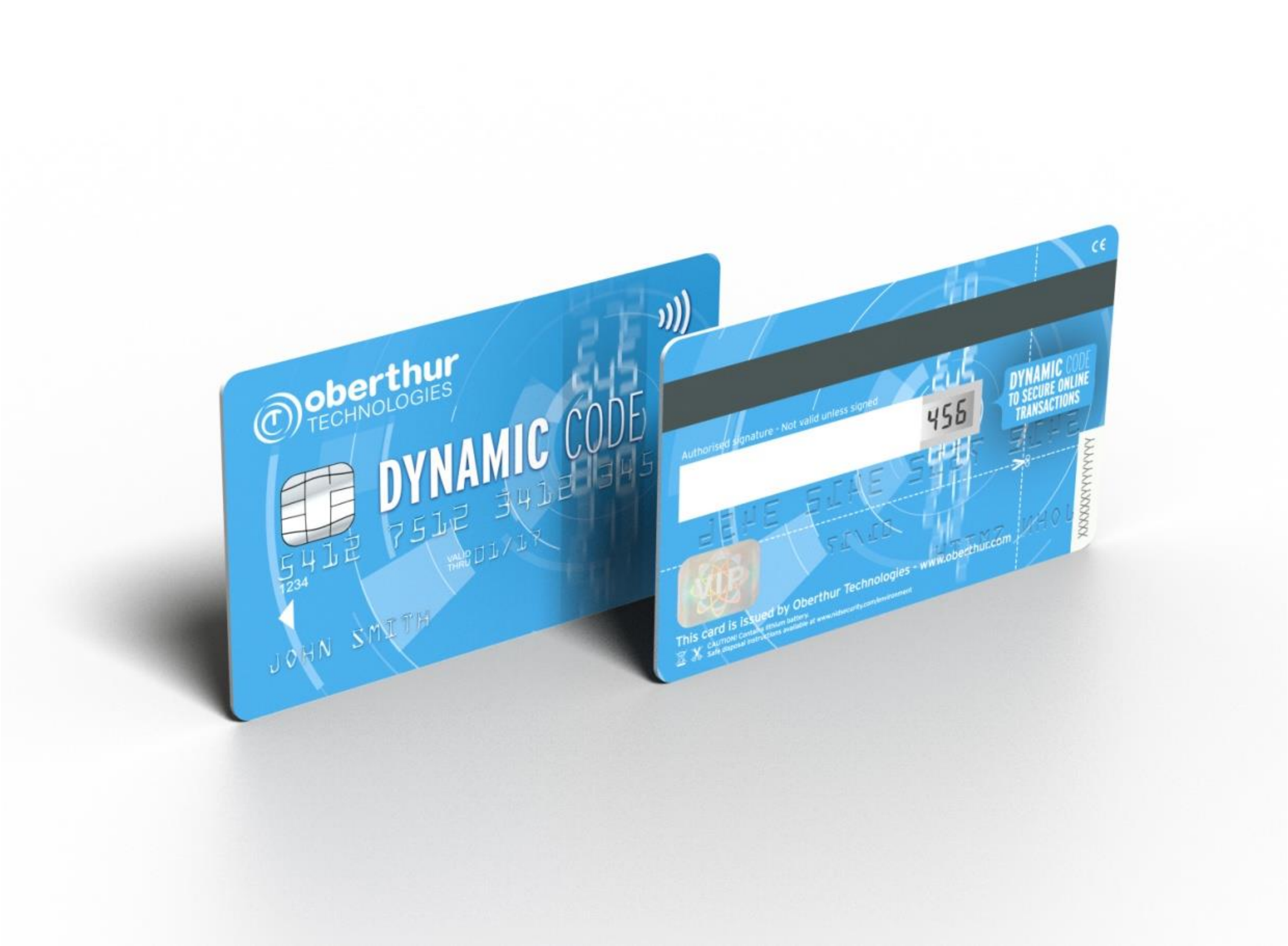
Payment
Network
Token Vault

One Time Passwords
Offers Two Factor Authentication

COSMO DISPLAY ONE

COSMO DISPLAY TWELVE

Dynamic Card Verification Value Offers Two Factor Authentication

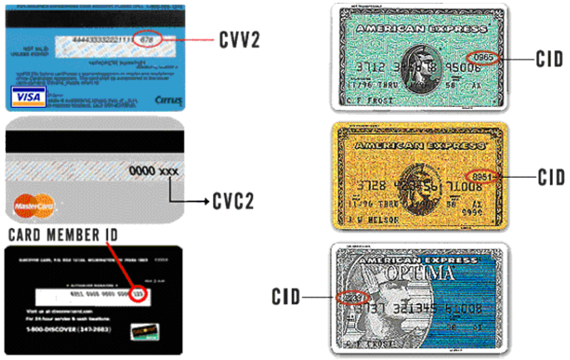

oberthur TECHNOLOGIES
DYNAMIC CODE
5412 7512 3412 3456
1234
VALID THRU 01/17
JOHN SMITH
Authorised signature - Not valid unless signed
456
DYNAMIC CODE TO SECURE ONLINE TRANSACTIONS
This card is issued by Oberthur Technologies - www.oberthur.com

Current Thinking Suggests a Layered approach

Card Present

- **EMV at the POI**
  - Offline Data Authentication proves to the merchant the card is genuine
  - The Chip creates the ARQC and TC to prove to the Issuer the card and transaction are genuine and unique
- **End to End Encryption**
  Protects the PAN, expiry date, cardholder name, amount, merchant ID and other transaction data as it travels from the POI to the Issuer
- **Tokenization**
  Turn the PAN into a useless set of digits for storage within the merchant and Acquirers systems
- **Support data analytics**
- **Support disputes handling**

Card Not Present



- 3D-Secure 1.0
- Device Fingerprinting
- EMVCo Tokenization
  - Card On File
  - Mobile Applets

- EMVCo 3D-Secure 2.0

Thank You

Philip Andreae
Vice President Field Marketing
p.andreae@oberthur.com
+1 404 680 9640

THE M COMPANY