MERCHANT ACQUIRERS' COMMITTEE

Tokenization/Point to Point Encryption/EMV and PCI: Cutting Through the Confusion

Merchant Acquirers’ Committee

MAC is an organization comprised of members from Banks, Acquirers, ISOs, Card Associations, Law Enforcement and others involved in risk management and compliance of the electronic payment processing industry. The purpose of MAC is to educate members in the electronic payment industries regarding the compliance with electronic payments regulations along with the detection, prevention and prosecution of those involved in electronic payment fraud. In the context of fulfilling MAC’s ongoing educational obligations to its members, this webinar is being presented by the MAC Education Committee in support of the MAC mission regarding the exchange of information and continuous education of its’ members.

Voltage Security

- Company: Founded in 2002
  out of Stanford University,
  based in Cupertino, California

- Mission: To protect the world's sensitive data
- By: Providing encryption and tokenization solutions that protect data wherever it is used or stored
- Solutions include:
  - Email and file security
  - Enterprise data protection
  - Payments data protection

Major Security Breaches continue...

…despite increased security efforts and compliance requirements

Neiman Marcus	2014
TARGET	2013
Adobe	2013
SONY	2011
Heartland PAYMENT SYSTEMS	2009

Major Security Breaches continue...

WHY?

Major Security Breaches continue...

Impossible to protect against every vulnerability –
IT infrastructures will continue to be breached

Impossible to keep all data behind a firewall –
there is no longer the concept of a "perimeter"

The data must be pervasively protected

Why has this not happened to date?

Challenges with Data Protection

Need to change data structures and applications

7412 3456 7890 0000

Fully encrypted data is unusable until decrypted

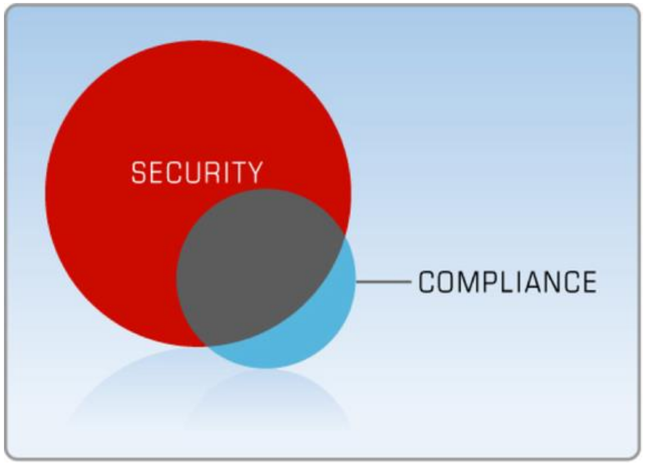
8juYE%Uks&dDFa2345^WFLERG

Key Management can be a nightmare

Requires multiple, piecemeal solutions, which create multiple security gaps

PCI DSS Compliance

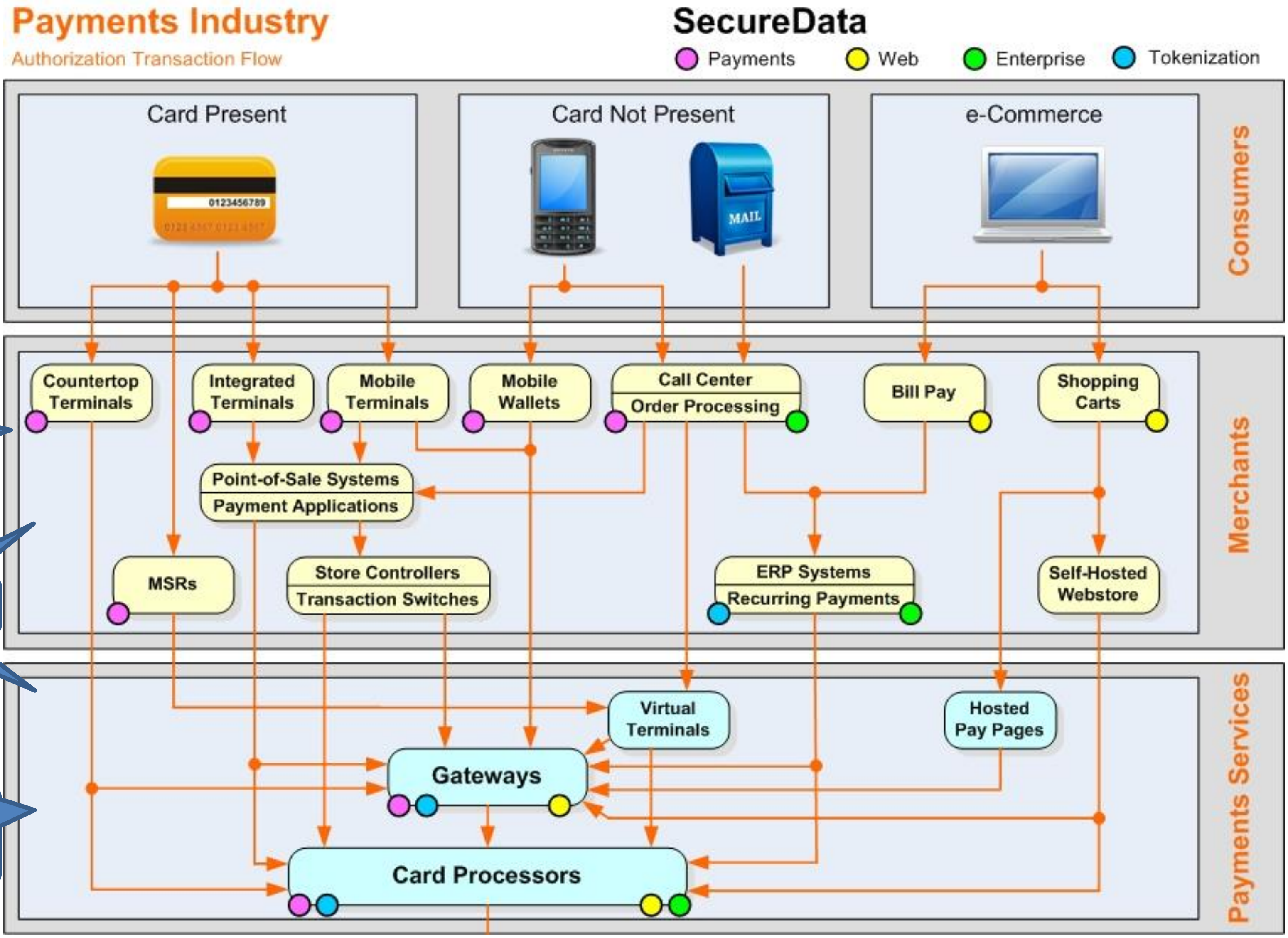
- PCI DSS compliance is required of any organization that “stores, processes or transmits cardholder data”.
- Subsets of PCI DSS standard are:
  - PTS : payment devices
  - PA-DSS: SW that touches card data
  - Anti-virus, malware protections
  - Human controls
- EMV is NOT part of PCI compliance.
- PCI DSS compliance reporting includes:
  - Level 1&2: QSA annual audit
  - Level 4: SAQ
- **Being PCI DSS compliant does not necessarily mean your data is safe.**



Current Best Practices

- EMV
  - Card user **authentication** to prevent card-present fraud
- Encryption
  - Format-preserved, algorithmic protection of PCI data for **transmission** to payment processor.
- Security Tokens
  - Safe, PCI-compliant long term **storage** of post-authorization payment data

Payments Landscape



Payments Industry

Authorization Transaction Flow

SecureData

● Payments ● Web ● Enterprise ● Tokenization

Consumers

Card Present

Card Not Present

e-Commerce

Merchants

Countertop Terminals

Integrated Terminals

Mobile Terminals

Mobile Wallets

Call Center
Order Processing

Bill Pay

Shopping Carts

Point-of-Sale Systems
Payment Applications

MSRs

Store Controllers
Transaction Switches

ERP Systems
Recurring Payments

Self-Hosted Webstore

Payments Services

Virtual Terminals

Hosted Pay Pages

Gateways

Card Processors

EMV

Encrypt

Pass thru

Decrypt/ Tokenize

FUTURE Best Practices

- EMV
  - Card user **authentication** to prevent card-present fraud
- Payment Tokens NEW!
  - Short-lived tokens for **consumer-initiated** mobile and eComm transactions
- Encryption
  - Format-preserved, algorithmic protection of PCI data for **transmission** to payment processor.
- Security Tokens
  - Safe, PCI-compliance long term **storage** of post-authorization payment data

A Review of EMV

- Card-present payment transactions only
  - PIN vs signature
- Merchants must have EMV-supporting devices
  - PTS v3.0+ payment devices are required
- Processor/Acquirers required to be EMV-ready by April 2013
- Additional transaction step for merchants
  - Many POS systems are taking a semi-integrated approach to managing EMV authentications.
- Liability shift
  - Merchant must be EMV-ready by Oct 2015 to avoid fraud/counterfeit risk.
    - Petro deadline is further out.
- **Does not protect cardholder data in transit to processor.**

Encryption (E2EE or P2PE)

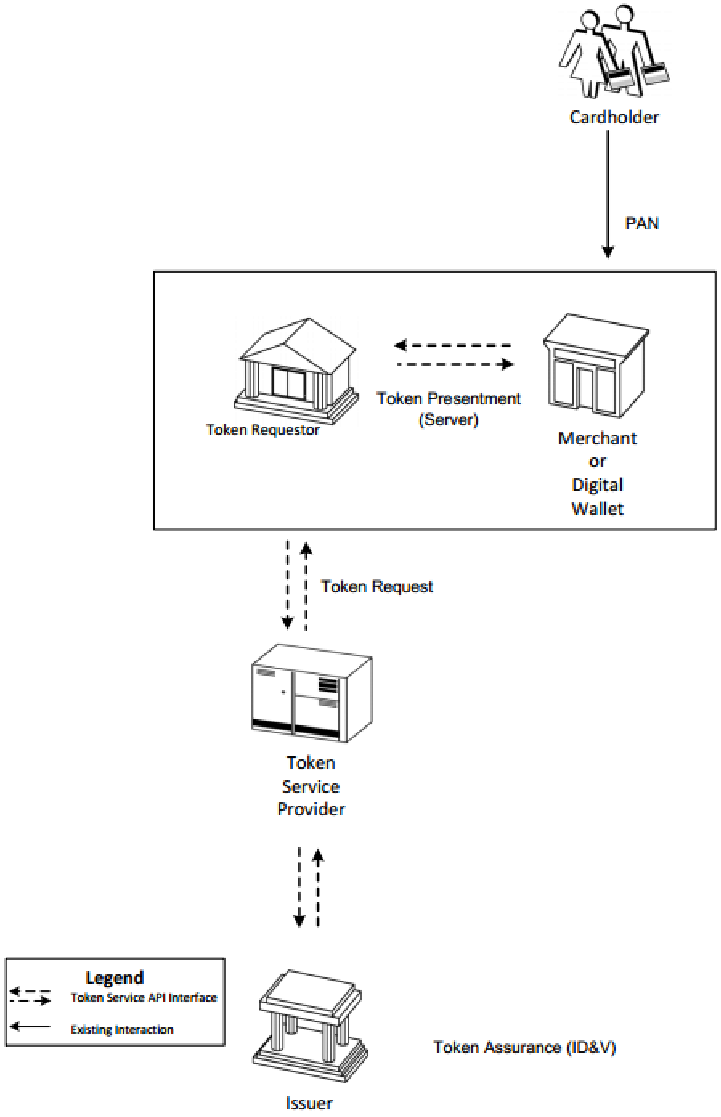
- Encrypt as ‘close-to-the-customer’ as possible
  - In a PTS-certified payment device or web browser session
- Consider impact on intermediary systems
  - FPE minimizes impact of encrypting cardholder data
  - Some solutions require changes to transaction flow
- Decryption may occur at a corporate data center or a third party.
  - Decryption point is in-scope for PCI DSS audits
- PCI DSS audit scope reduction requires:
  - No clear-card data, ability to decrypt, or access to keys
- P2PE Validated Solutions list
  - Designed for Level 4 merchants.
  - There are only 3 solutions on the list to-date.

Security vs Payment Tokens

- Payment Tokens
  - Initiate transactions, short-lived
  - Issued externally (i.e. a Token Service Provider)
  - Globally meaningful
- Security Tokens
  - Analysis values (fraud, marketing)
  - Issued internally (i.e. the data owner)
  - Locally meaningful
- Security and payment tokens work together

Payment Token Issuance

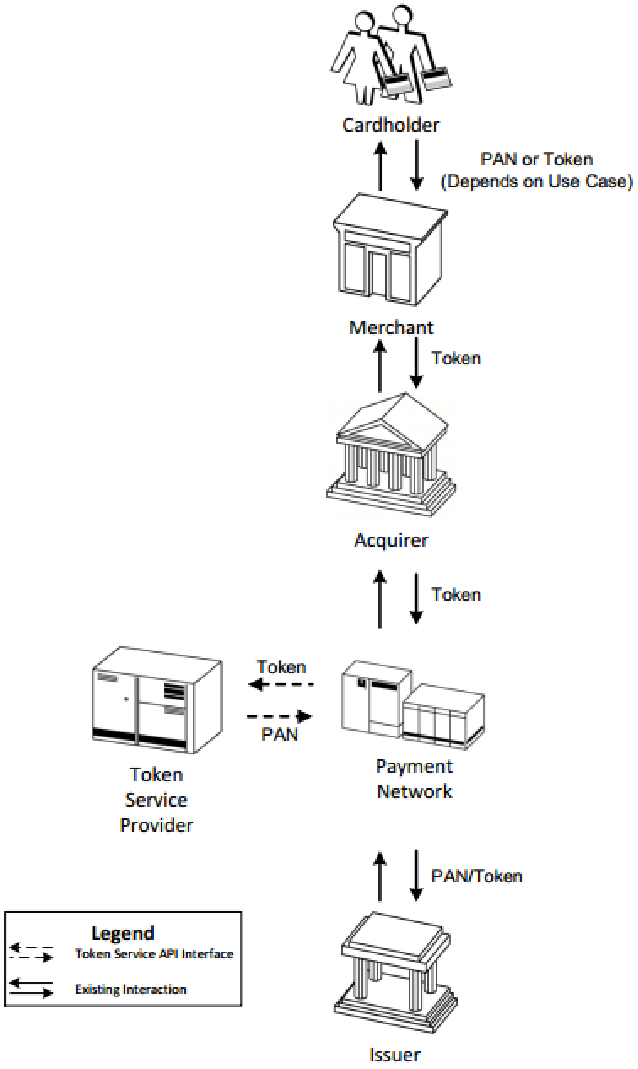
Figure 1: Payment Token Provisioning Overview



- At time of payment, merchant communicates PAN to TSP.
- TSP responds back to merchant with Payment Token.
- Payment Token is valid as a surrogate PAN value for a short period of time (e.g. one transaction, one day).
- **Payment Tokens have sensitivity during their life cycle.**

Payment/Security Token Usage

Figure 2: Payment Token Transaction Overview



- Payment Token is transmitted by Merchant as normal.
- Payment Token is format preserved.
- **Processor/Acquirer must consider effect of receiving surrogate PAN value from merchant.**
- Payment Network communicates with TSP to de-tokenize and communicate clear value to Issuer.
- Security Token issued for post-authorization.

Tokenization Standards Authorities

- Current standardization efforts under way
  - X9.119 part 2 (security tokens)
  - PCI Tokenization (security tokens)
  - EMVCo (payment tokens)
    - The Clearing House now in this effort
  - Future Fed activity?

PCI Security Standards Council

EMVCo

ANSI American National Standards Institute

United States Federal Reserve System

The Clearing House At the Center of Banking Since 1853

PCI SSC Tokenization Standard?

PCi Security Standards Council

Payment Card Industry (PCI)
Non-Payment Tokenization Technical Standard

RFC

Solution Requirements:
General Principles, Irreversible and Reversible Tokens
Version 0.7 – RFC
April 2014

DRAFT

- This is a **draft** only for feedback. It defines methods for generating Security Tokens.
  - It is not for use by QSA's yet. We are part of the Task Force process and so very close to this and have provided input and feedback.
- Payment Tokens are not covered by the draft - it is called "Non-Payment Tokenization Standard"
- How do various tokenization designs map to this draft?
  - Random Tokens map to "Reversible Non-Cryptographic Tokens"
  - PAN encryption maps to "Reversible Cryptographic Tokens"
    - Not PCI DSS audit scope reducing.

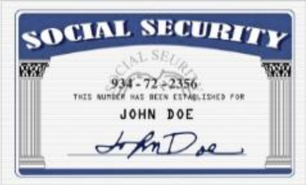
Tokenization Techniques

- Two steps to tokenization:
  - Mapping PAN to token
  - Associating token with state or context
- PAN to token map techniques
  - Database
    - Write mappings into a database
    - Costly, scale issues
  - Cryptographic
    - Create mappings using an AES key
    - Clean, some folklore security concerns
      - Not PCI DSS audit scope reducing
  - Static table-based
    - Create mappings through a pre-generated table
    - Removes scale issues

Tokenization considerations

- Token formatting
  - Format preservation vs ‘Obviously’ tokenized
- Vendor/solution lock-in
  - The ‘pain’ of change increases over time
- Synchronicity of token instances
  - Necessary for collision avoidance
- Scalability of token infrastructure
  - Token uniqueness required across LOBs, merchants which can cause infrastructure bloat.

Comparing approaches



	Credit Card	Tax ID
	7412 3456 7890 0000	934-72-2356
Table-based Tokenization	7412 34**87 8346** 0000	**774-96-**2356
Database Tokenization	7412 3456 7890 0000 7412 34**87 8346** 0000	934-72-2356 **774-96-**2356

- Both approaches can support format-preservation.
- Chosen solution should have be provably secure, crypto-analyzed and have a publically-available design publication.
- Table-based tokenization reduces PCI scope more than any other approach – no database, but still random mapping
- Table-based tokenization eliminates the costly “token database sync” problem
- Table-based has higher performance, lower cost, and is simpler to deploy/manage

Database Tokenization

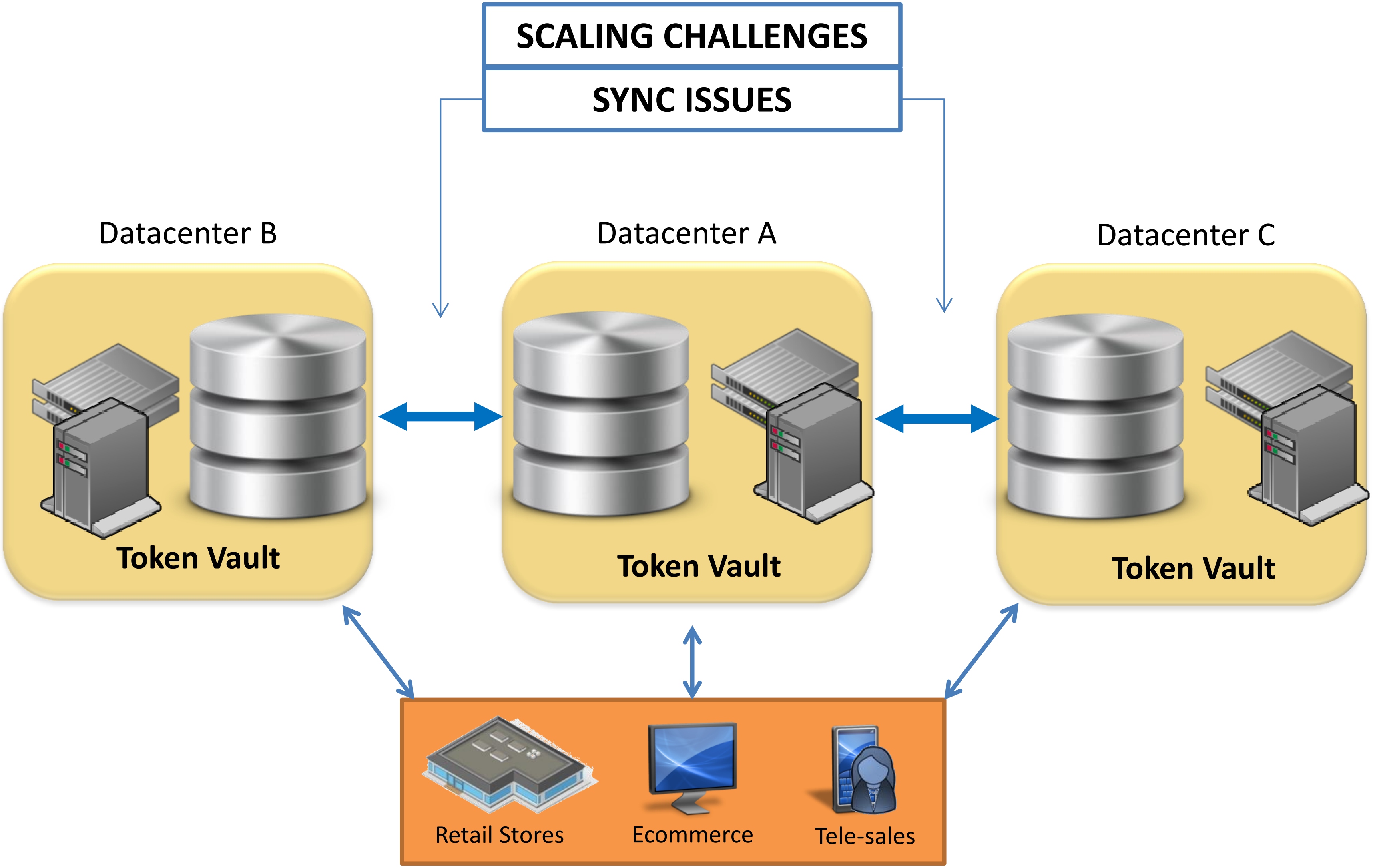
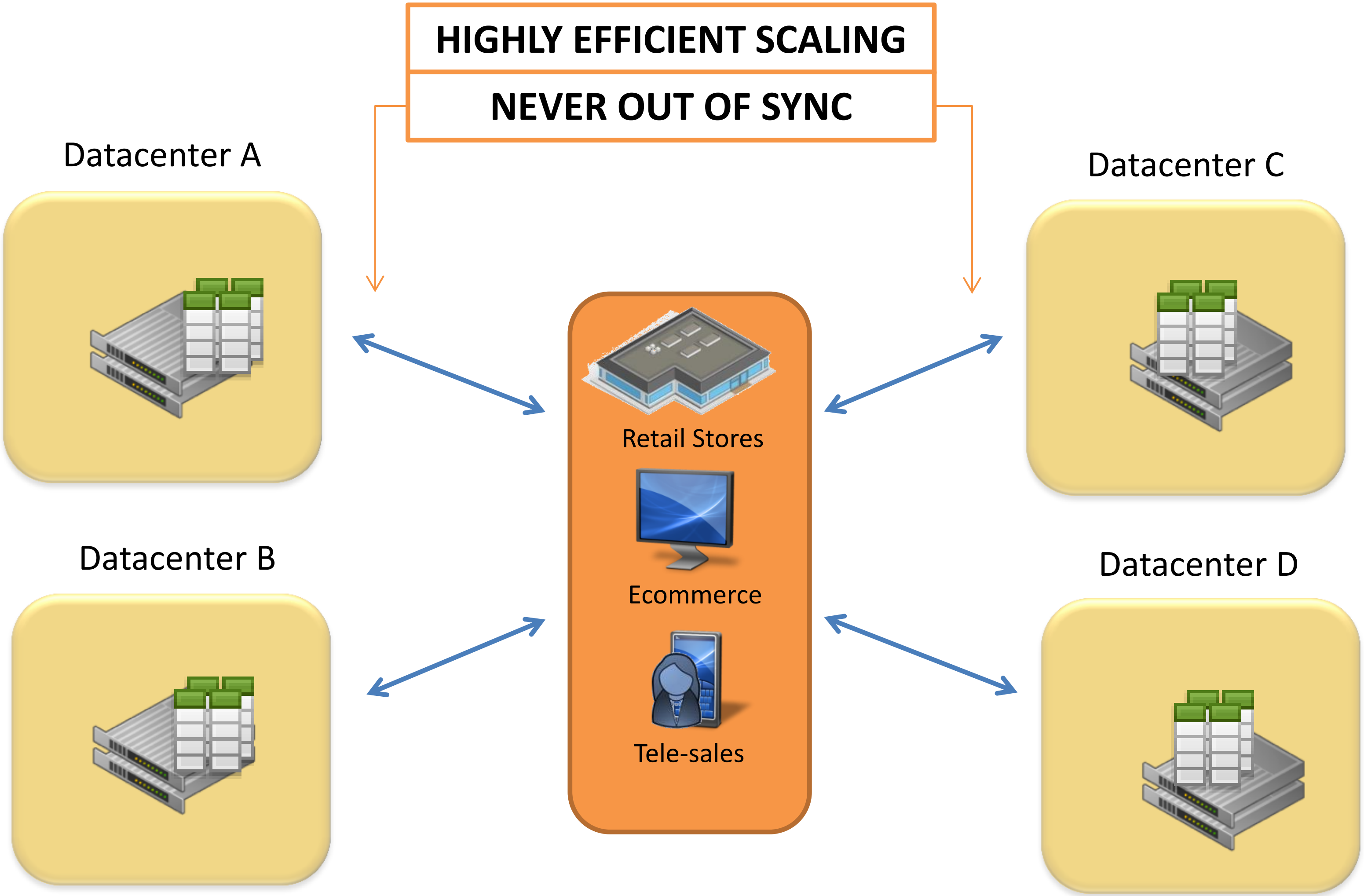


Table-based Tokenization



HIGHLY EFFICIENT SCALING

NEVER OUT OF SYNC

Datacenter A

Datacenter C

Retail Stores

Ecommerce

Tele-sales

Datacenter B

Datacenter D

MAC

Voltage security

Top Global Credit Card Company

Enabling Future Payments Platform

Solution Components
Table-based tokenization
PII encryption
In-house Deployment

- Use Case
  - Mobile wallet offering to millions of consumers
  - How to secure payment vehicles connected to wallet
- Approach
  - Table-based tokenization of mission critical payment data
  - Support for all global credit card brands
- Results
  - Scales up to ~2bn cardholders
  - >50% lower operations cost vs. other approaches
  - Higher PCI Scope reduction than other approaches

World's 4th Largest Internet Retailer

Reducing PCI DSS Scope and reducing risk in payment data use

Solution Components
eCommerce encryption
Table-based tokenization

- Use case
  - PCI DSS scope reduction for eCommerce environment
  - Encrypt every card purchase & tokenize all stored cards
  - Avg 56M transactions/month
- Approach
  - Table-based Tokenization – Data at rest inside private cloud
  - In-browser eComm encryption – Data in transit from consumer browsers
- Results
  - Projected $1M/year savings
  - De-scope ~600 servers per datacenter in phase 1.

The Worlds Top Internet Payment Processor

Enabling secure merchant services and reducing compliance costs

Solution Components
Device-based encryption
eCommerce encryption
Table-based tokenization

- Use case
  - Security as a competitive driver in the payments processing/acquiring segment
- Approach
  - eComm encryption + table-based tokenization
  - Internal tokenization, encryption – business advantage to reduce merchant risk
- Results
  - Global deployment
  - Solution scales up to:
    - >500,000 merchants
    - ~ 50% of global internet eCommerce
    - >24 Bn transactions/year

Thank you!

George Rice
Voltage Security, Inc.
george.rice@voltage.com
703-470-3055