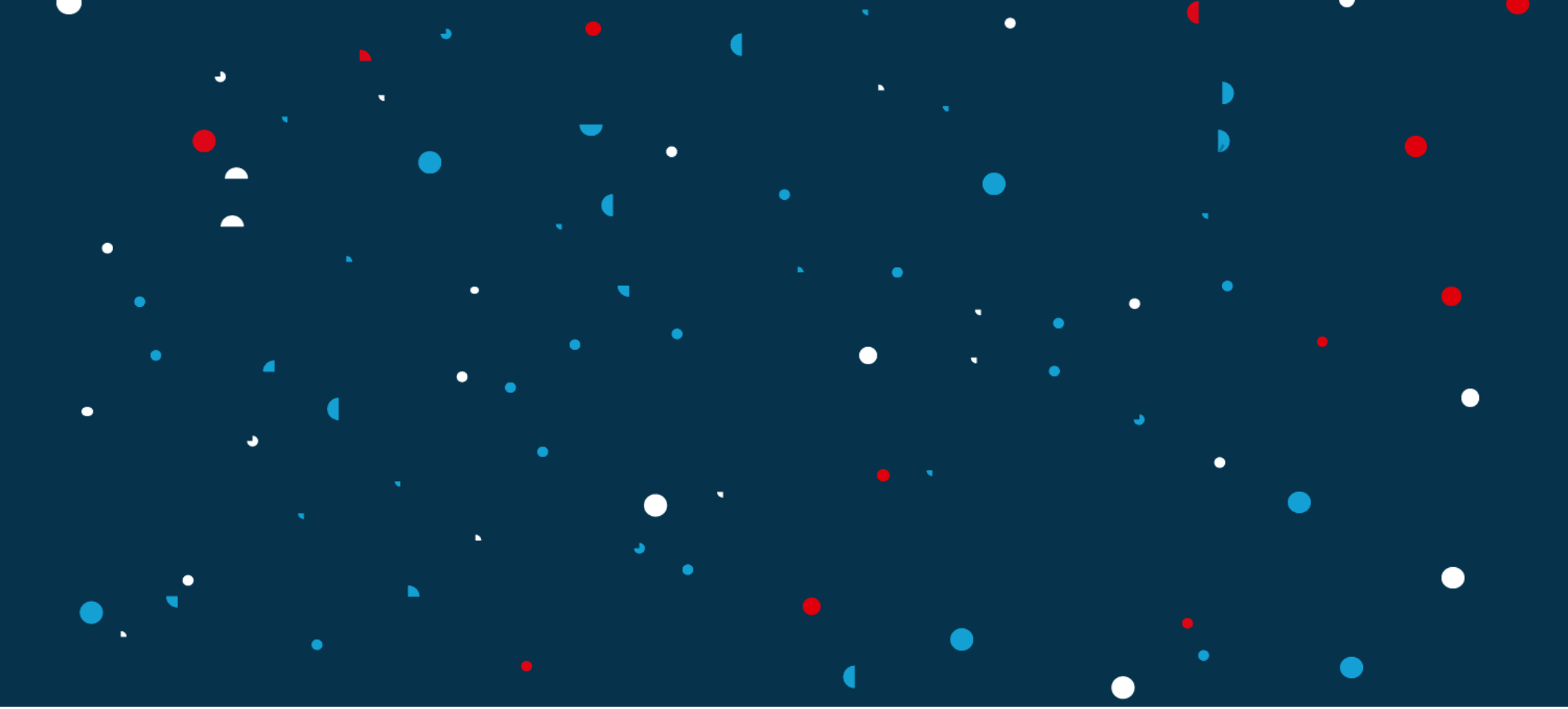


Interswitch

Electronic Payment • Technology Integration • Digital Commerce • Advisory Services

AUDITING THRID PARTY VENDORS – Card Schemes, MNOs, Processors and Switches

Governance, Risk and Control Frameworks

Interswitch

November 30 2017

Course Outline

1	Overview
2	Card Associations and Schemes Operations
3	Mobile Network Operator Services
4	Processor and Switching Services
5	Security Considerations
6	Governance Risk and Control Framework Requirements - Discussion

OVERVIEW

Interswitch

Introduction

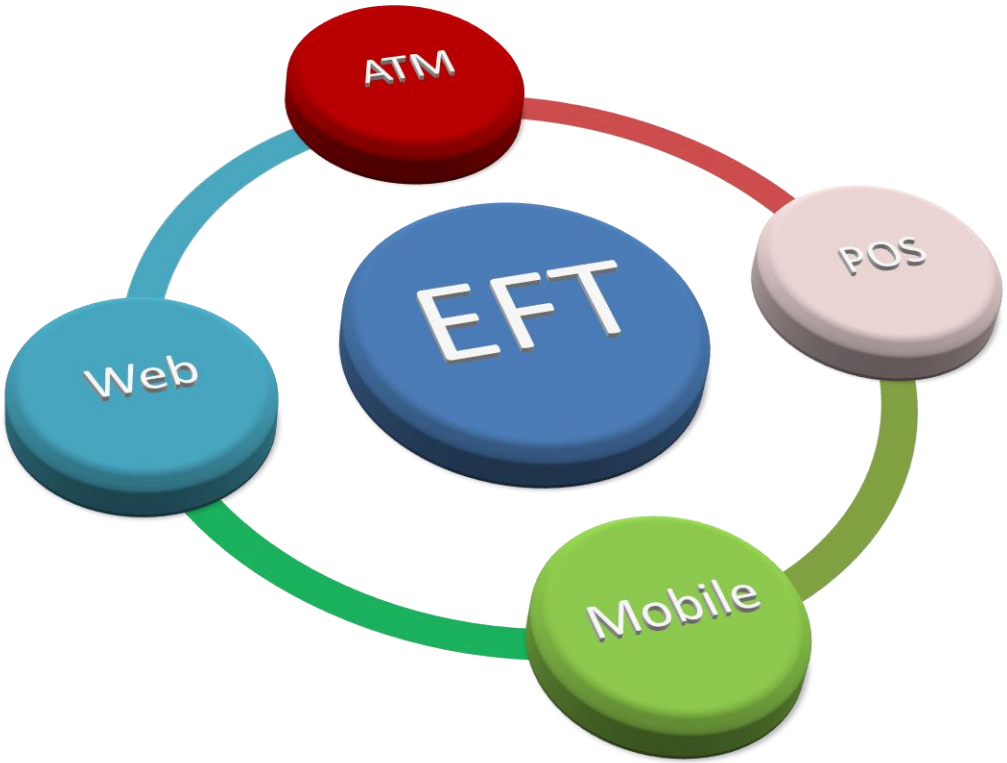
Electronic funds transfer (EFT) is a cluster of technologies that allow the execution of financial transactions by electronic messages without the necessity of a paper instrument of exchange.

Institutions that participate in an EFT system typically belong to a common network that provides a platform for initiating transactions

Transaction data in transmission or storage is best protected through encryption, which converts clear text data to cipher text that is not understood by humans

Data protection is also enhanced by establishing and adhering to policies and procedures as relevant

EFT Channels



Basic Security Components

Virtual Private Network (VPN)

- A VPN is a network that uses a public infrastructure such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

- It works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP)

- In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted

Basic Security Components

Front End Processor (FEP)

- The Front End Processor (FEP) is a computer system that interfaces between entities sending an EFT message and the bank host
- It performs vital functions that include message and transaction switching, multiplexing, transaction security, d end-to-end transaction management and reporting
- The need for these functions is especially important in mission critical transaction environments such as banking, government, point-of-sa security, and health care applications

Basic Security Components

Hardware Security Module (HSM)

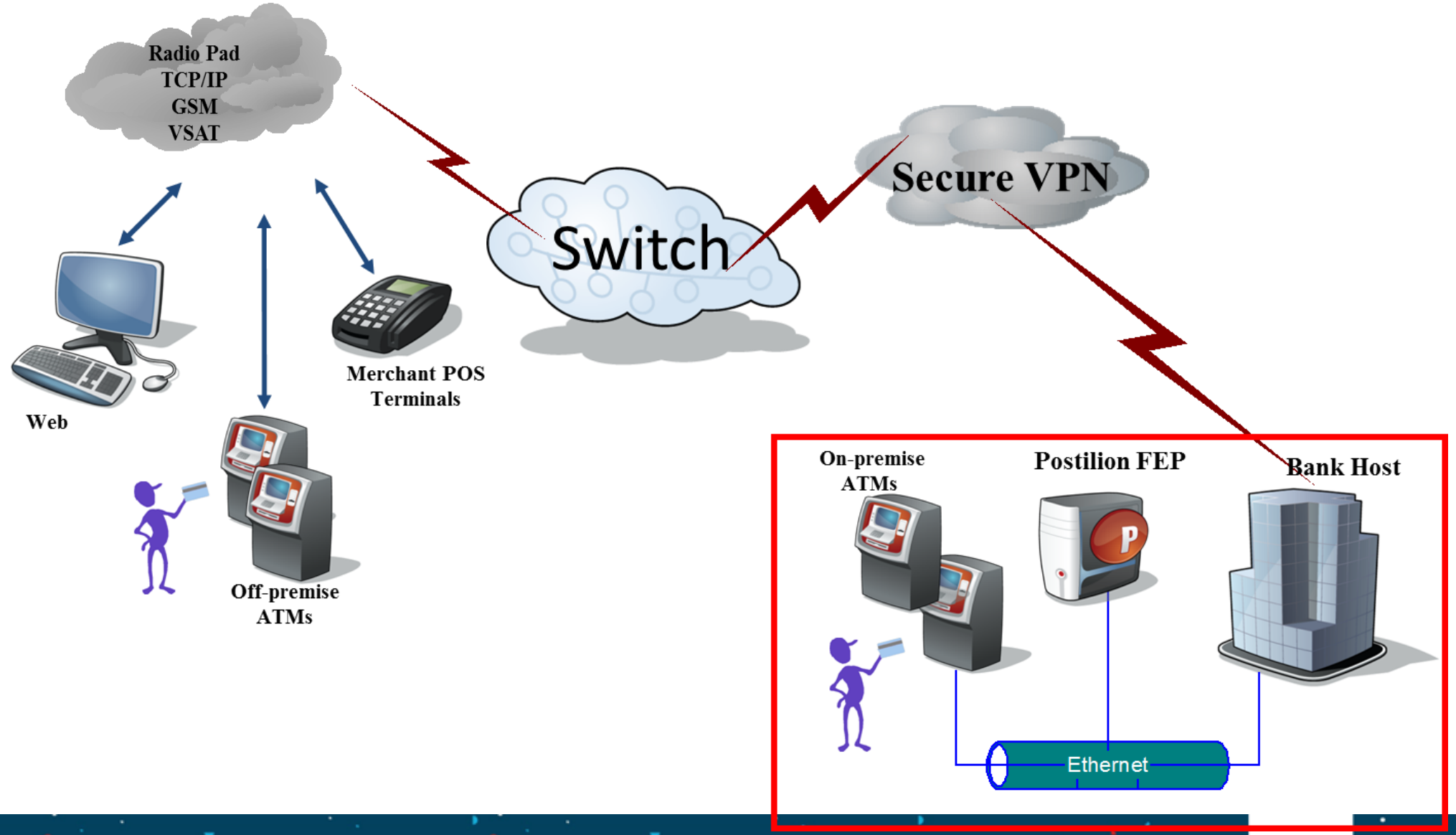
- An HSM is a hardware-based security device that generates, stores and protects cryptographic keys
- Successful physical attacks against HSM is prevented with a sophisticated anti-tamper crypto module
- The anti-tamper protection senses extreme temperature, voltage and chemical attacks, and can even be configured to detect motion of the unit once it is installed. If the crypto module is attacked it will automatically erase all keys and crypto logic information
- The HSM is armed with an alarm circuitry that can be configured to be triggered if the HSM is moved.

Basic Security Components

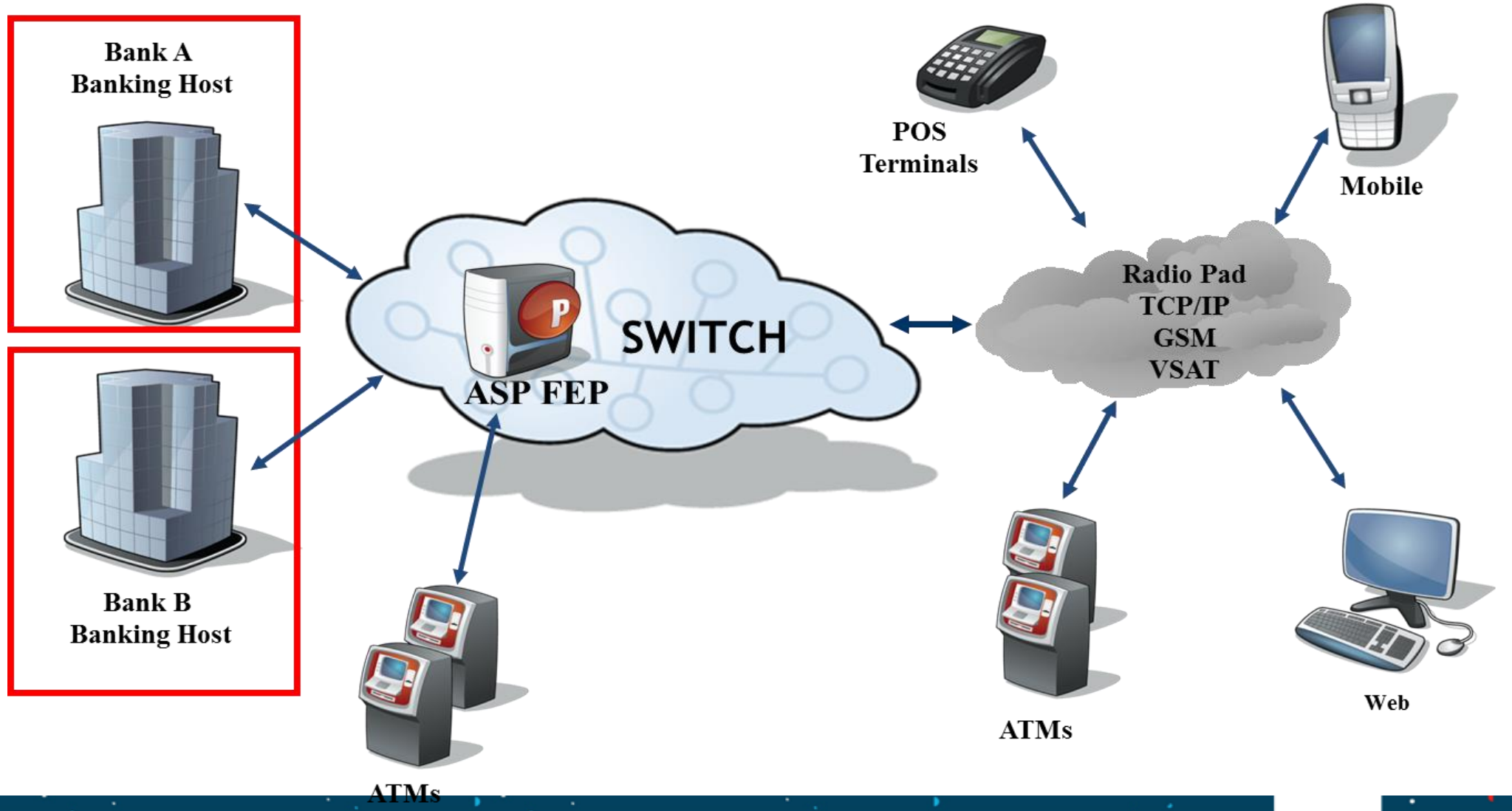
Proxy Server

- A proxy server is a server that acts as a go-between for requests from clients seeking resources from other servers
- A security advantage of using a proxy server is to keep the machines behind it anonymous
- A proxy server is an additional layer of defense and can protect against some operating system (OS) and WebServer specific attacks

Front End Processor (FEP) Connectivity Model



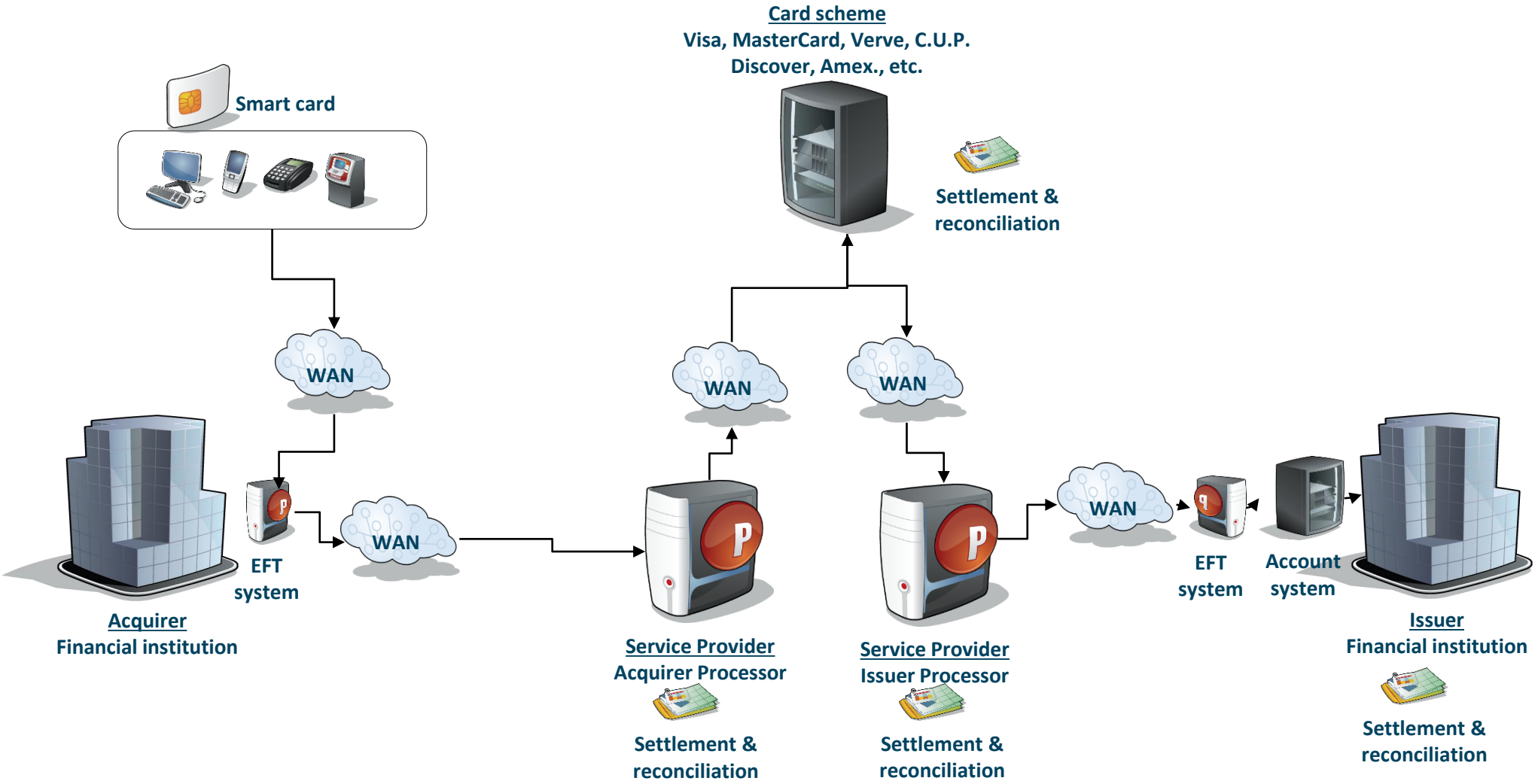
Application Service Provider (ASP) Connectivity Model



CARD ASSOCIATION AND SCHEME OPERATIONS

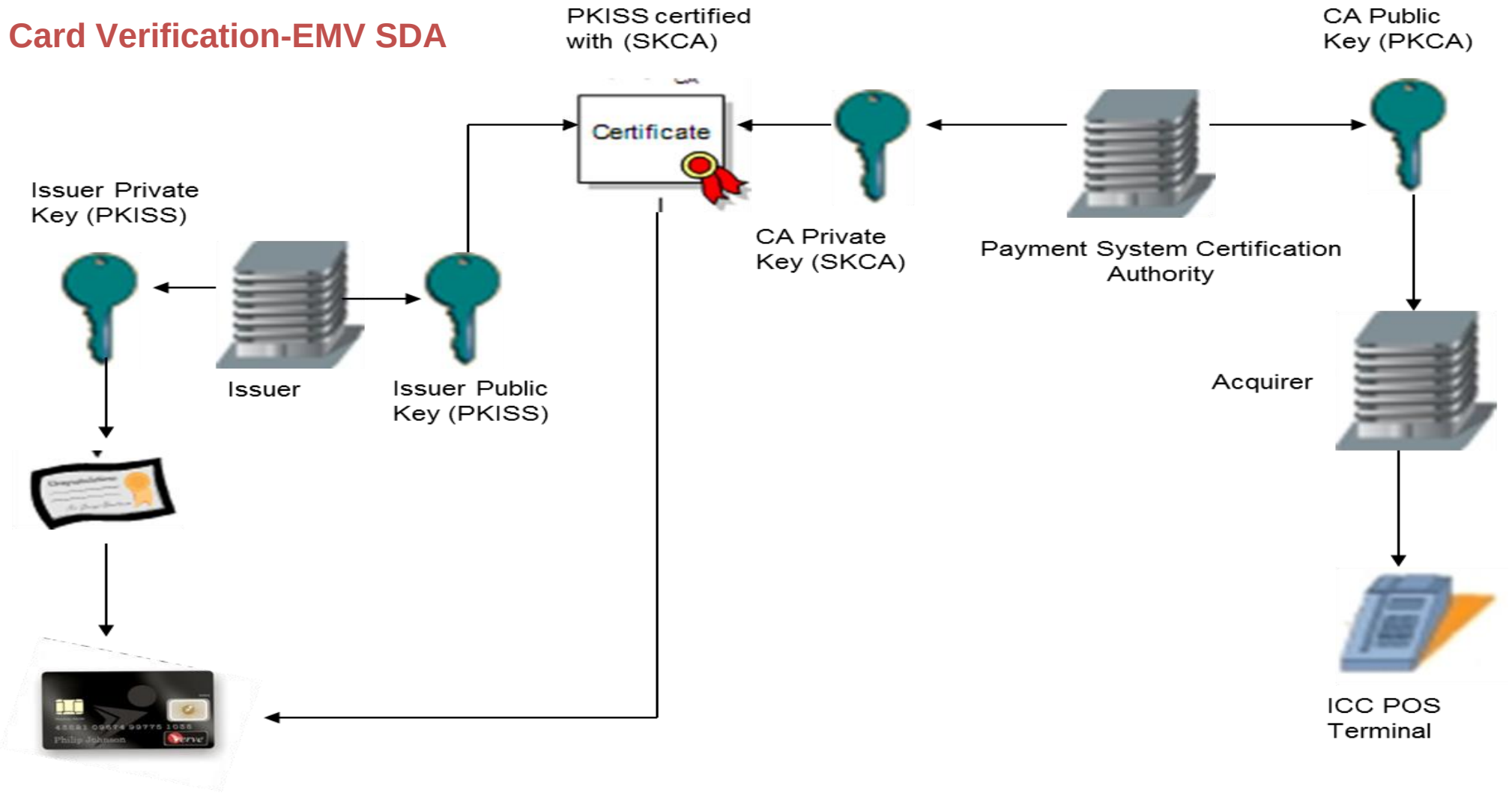
Interswitch

High level layout - Standard Card Networks



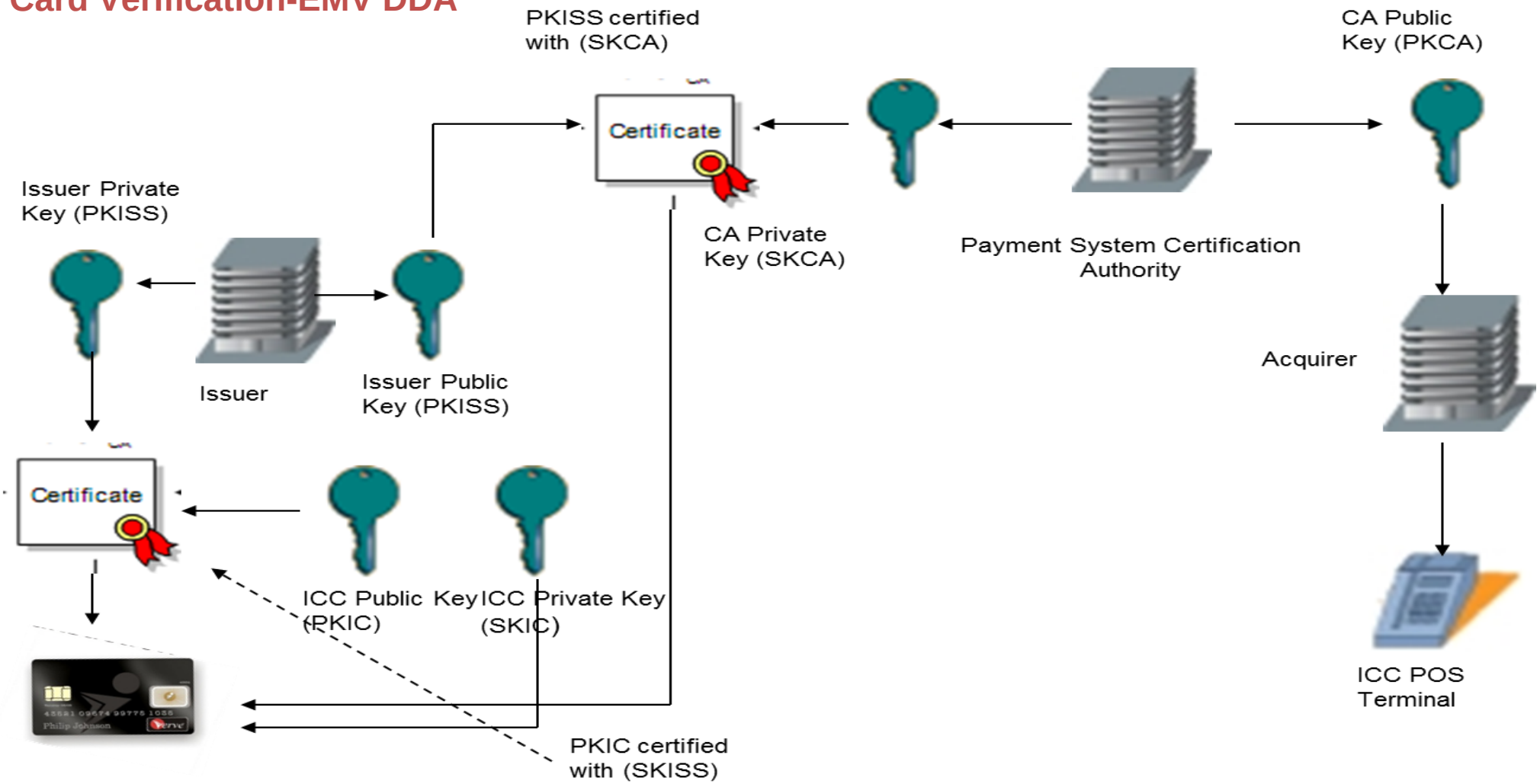
Card Scheme Role in EMV Infrastructure-SDA

Card Verification-EMV SDA



Card Scheme Role in EMV Infrastructure-DDA

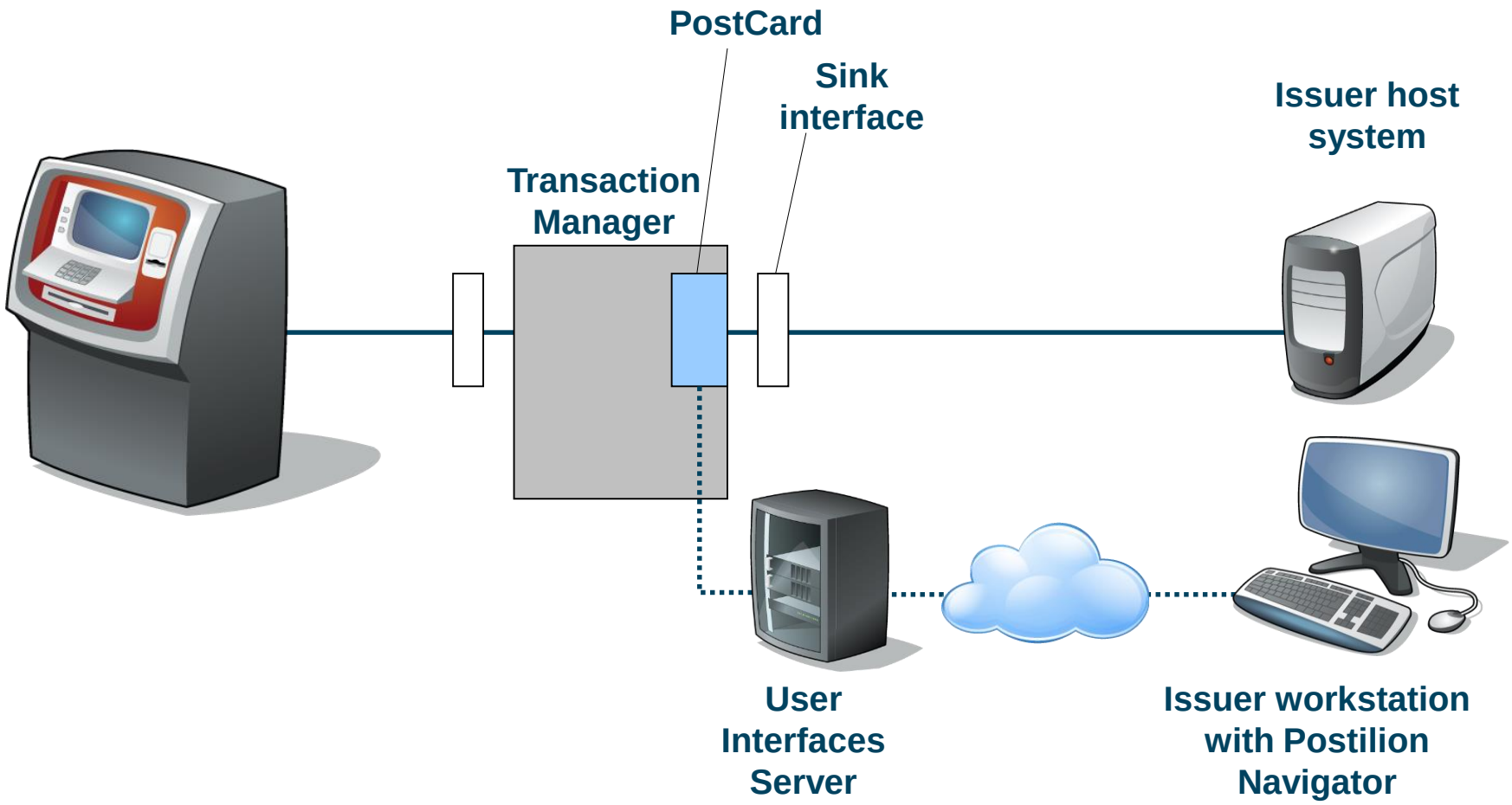
Card Verification-EMV DDA



PROCESSOR AND SWITCHING SERVICES

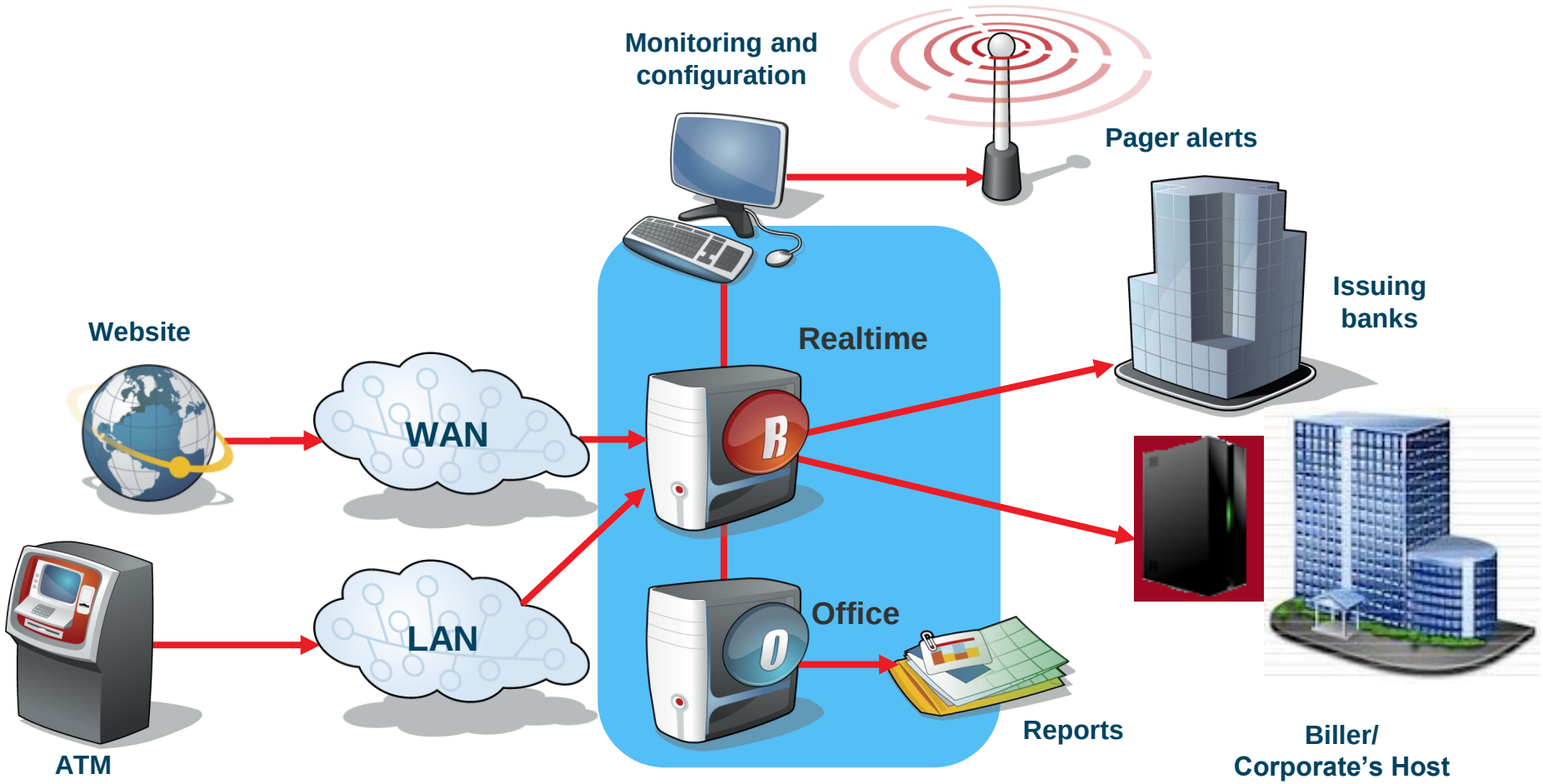
Interswitch

Card Management System Architecture



EFT Transaction Processing Flows

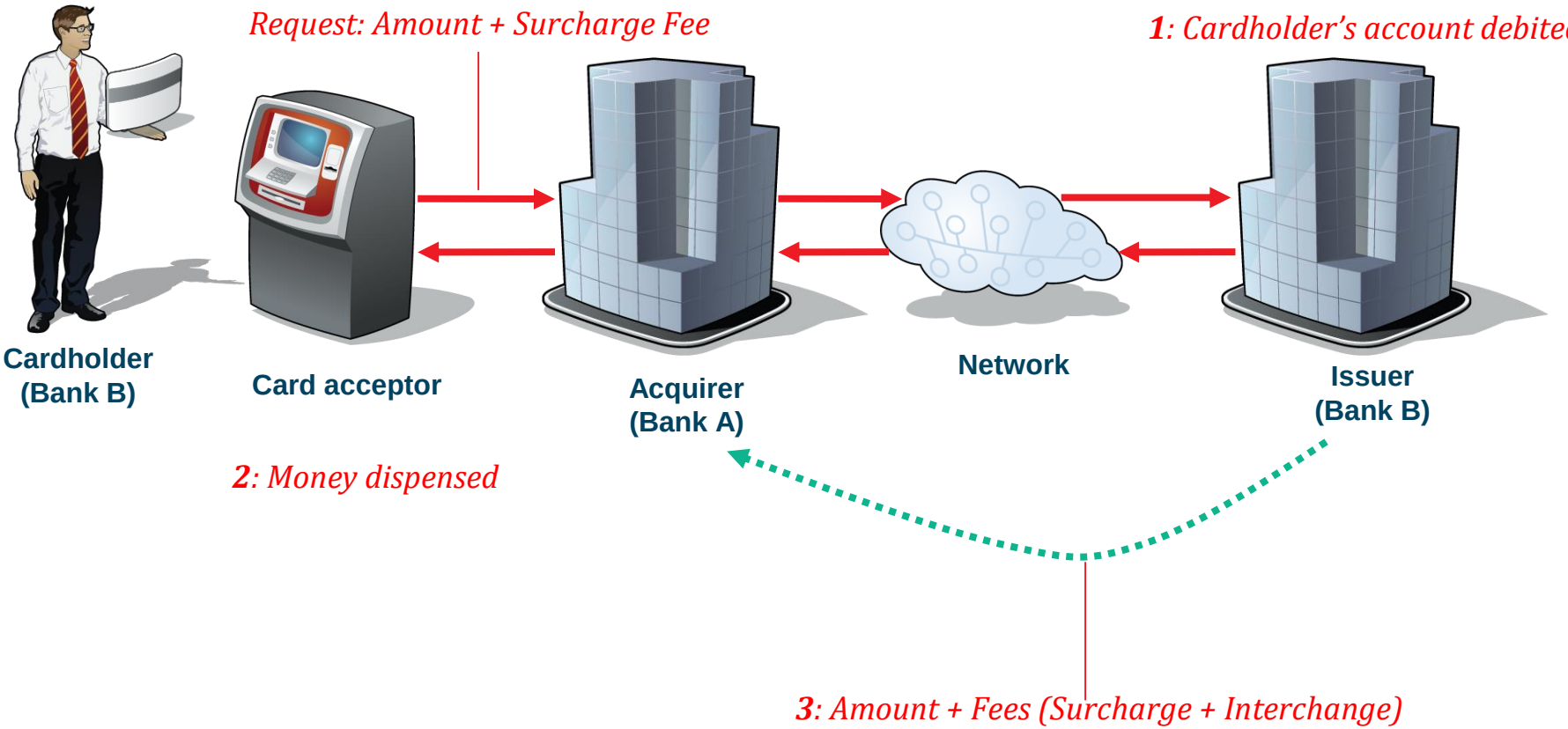
Products Bill Payments Processing



EFT Transaction Payment Lifecycle Flow

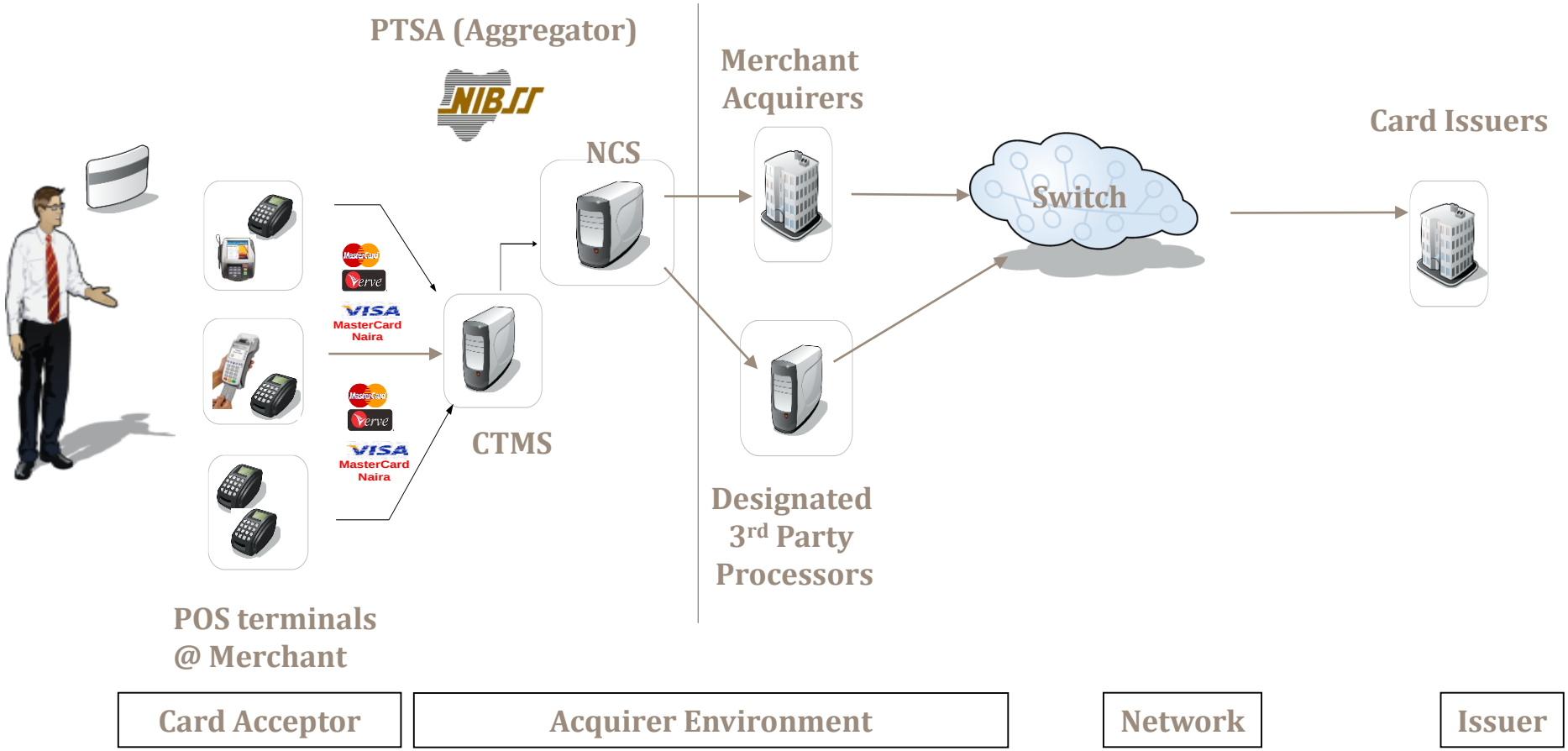
Payment Cycle for Surcharged Transactions:

ATM Cash Withdrawals

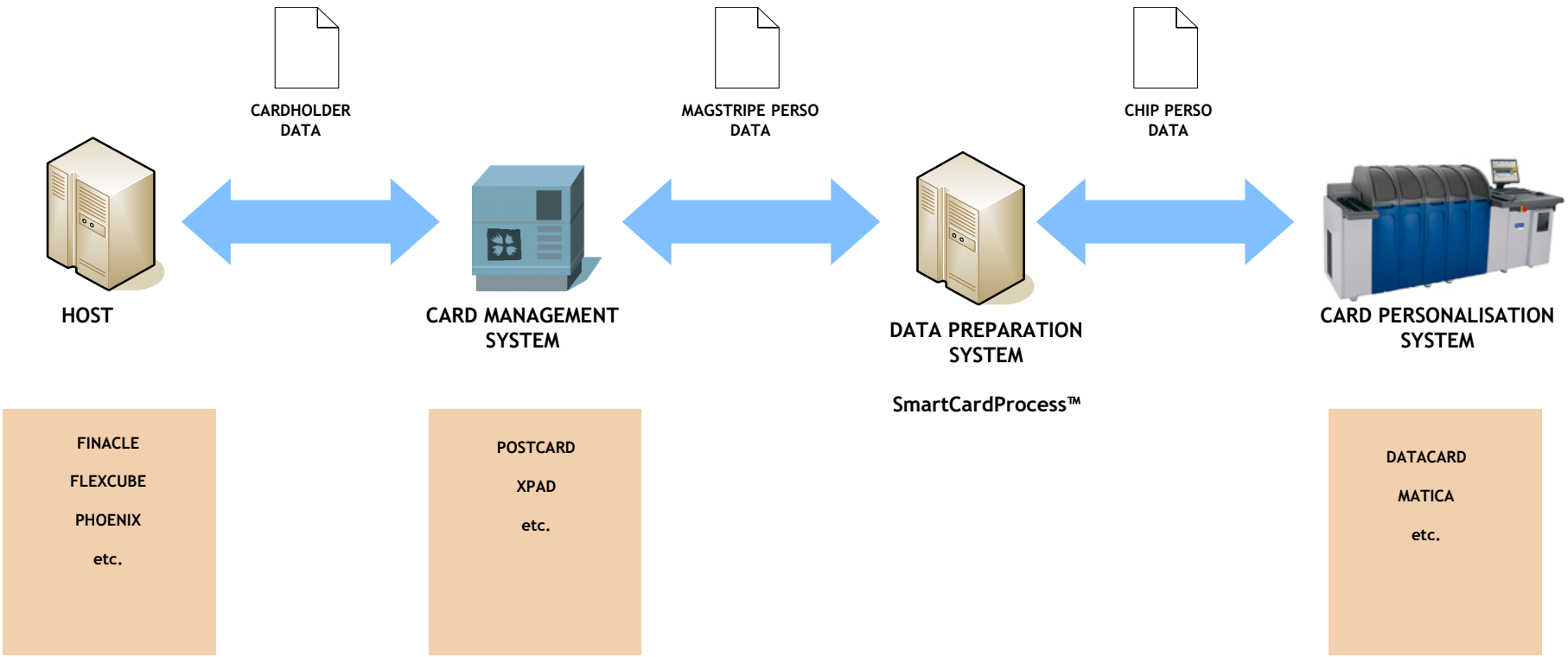


EFT Transaction Processing Flows

The POS Processing Environment in Nigeria

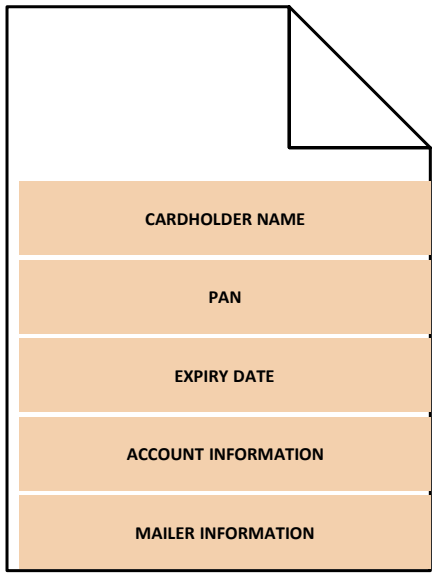


Overview of Card Production

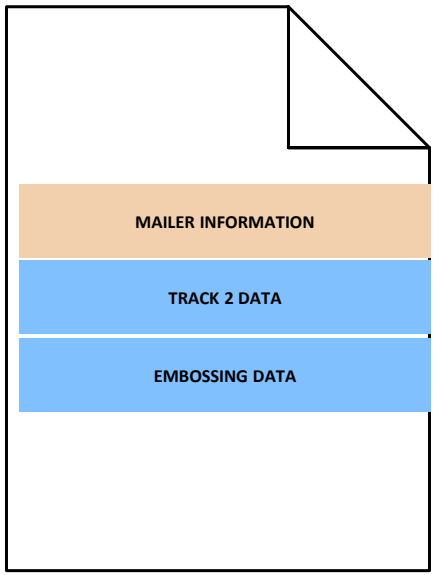


Overview of Card Production

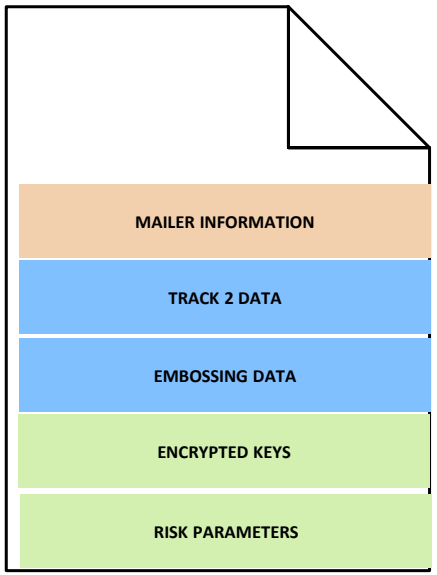
What's in the files?



CARDHOLDER DATA



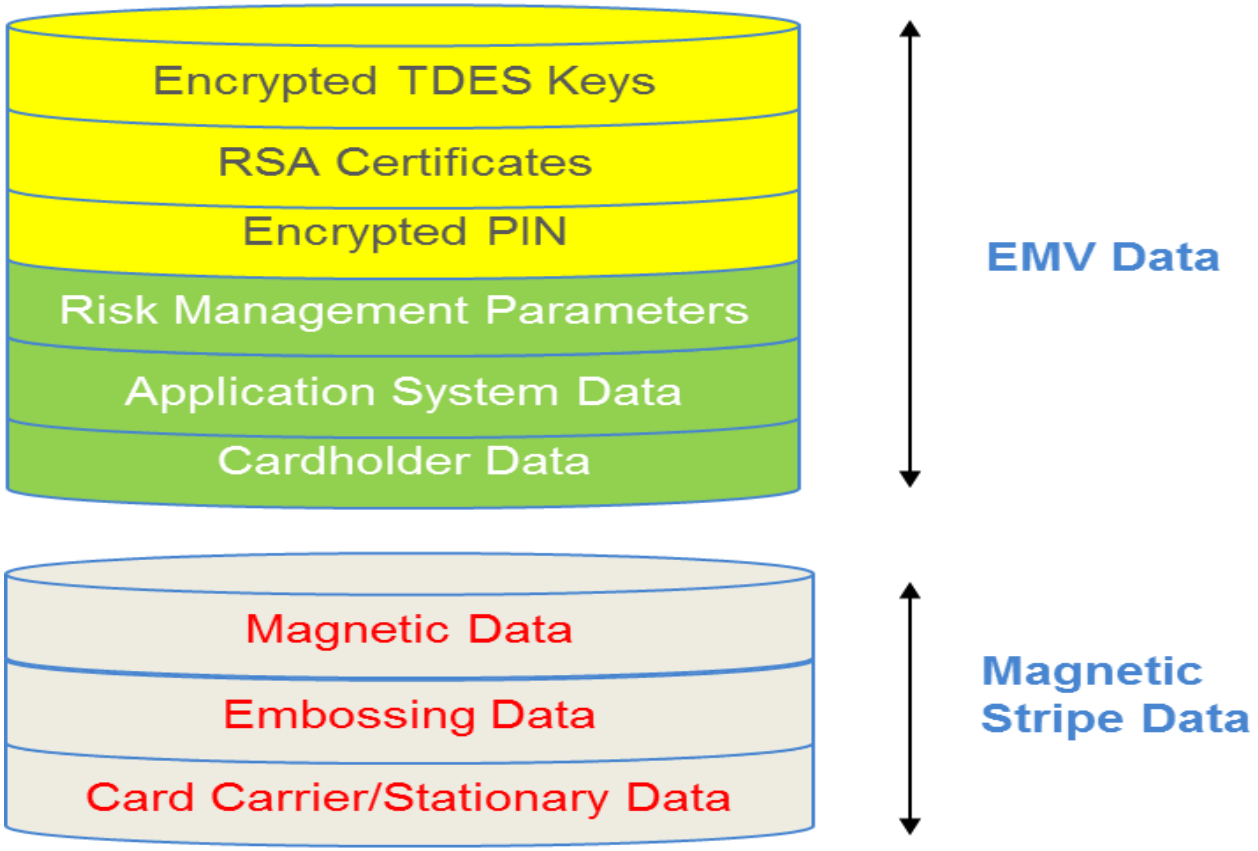
MAGSTRIPE PERSO DATA



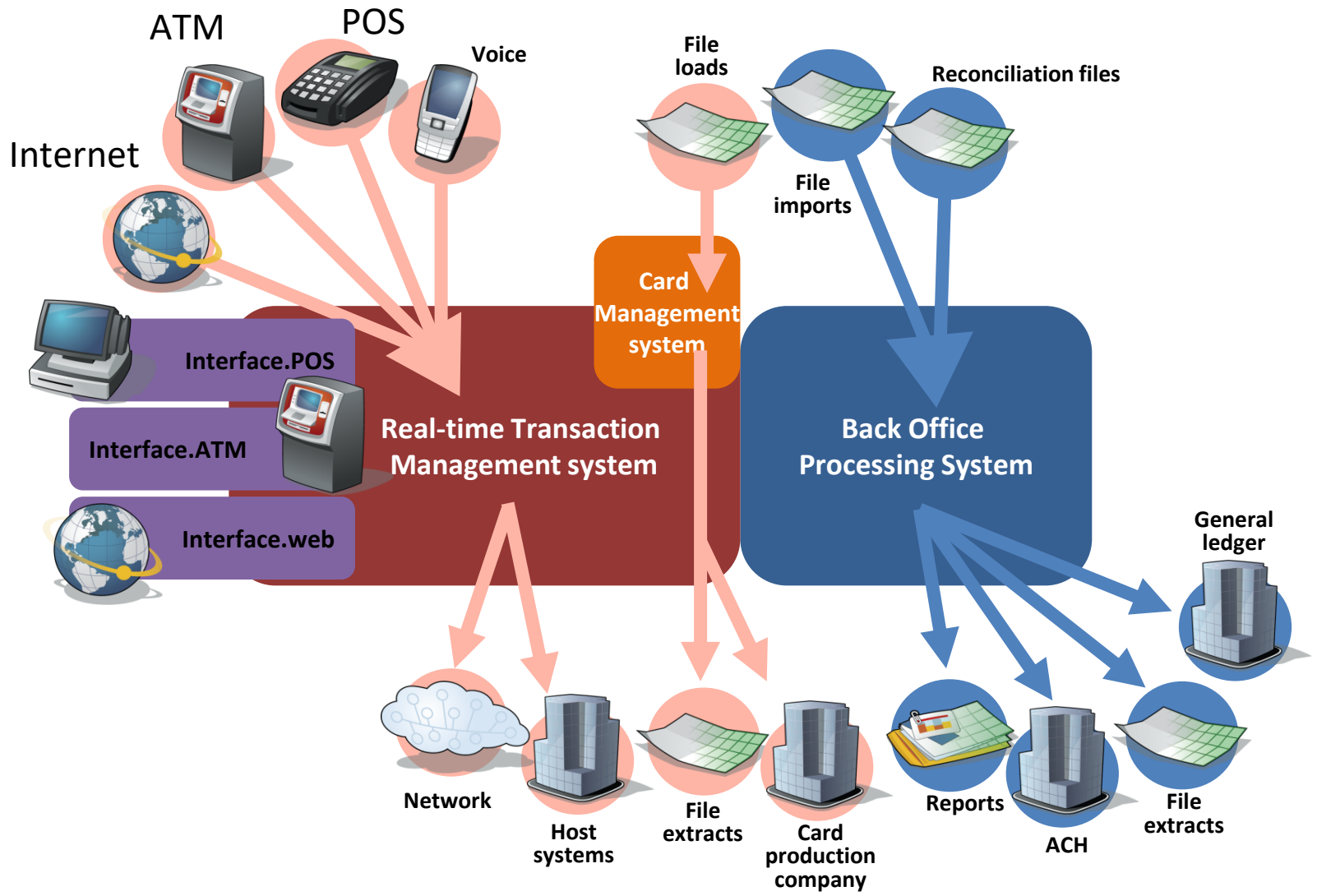
CHIP PERSO DATA

EMV Card Production - Personalization

Data required for chip card personalization



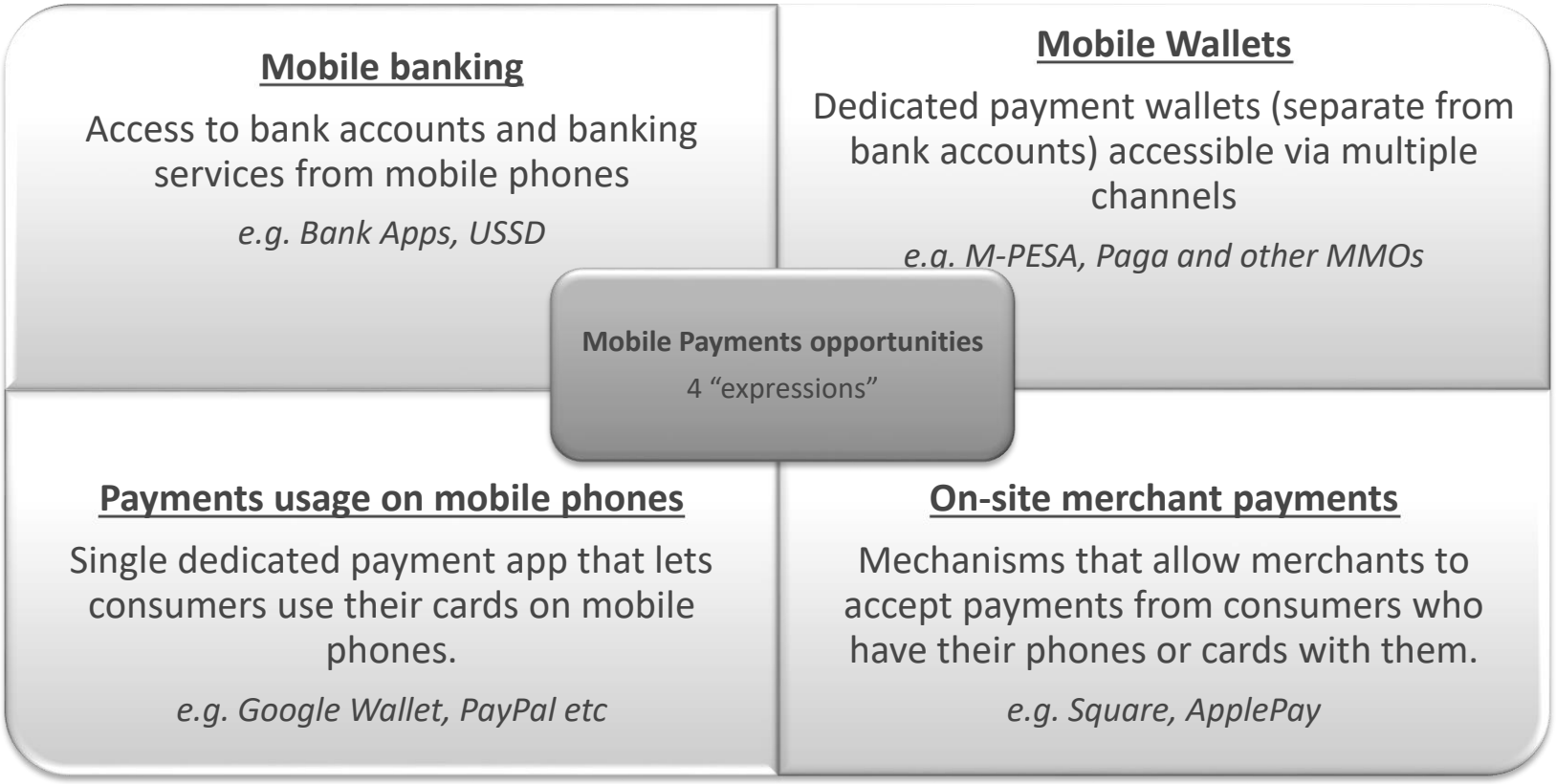
EFT Processing Architecture



MOBILE NETWORK OPERTOR SERVICES

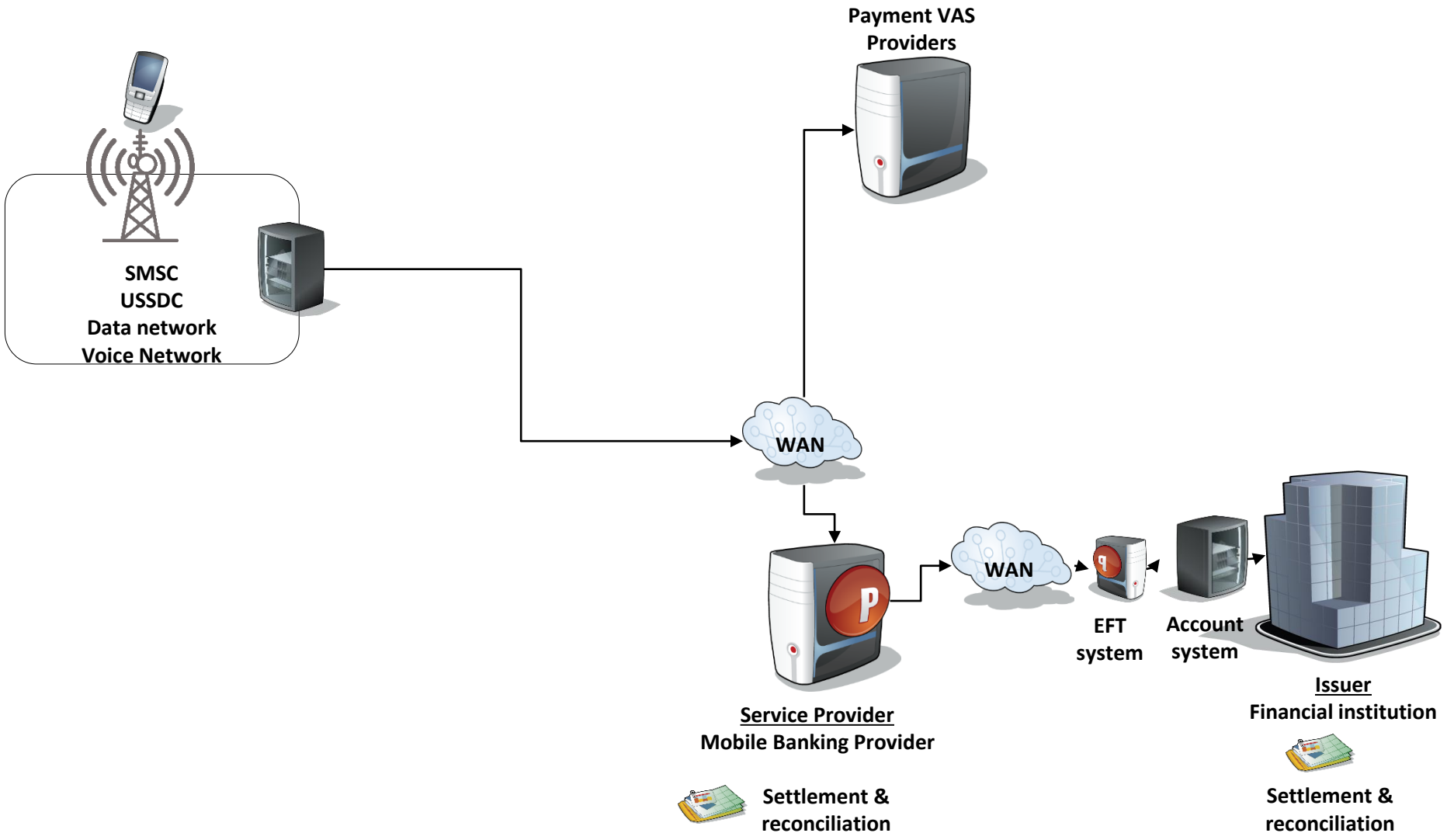
Interswitch

Dimensions of M-Commerce and Mobile Payments



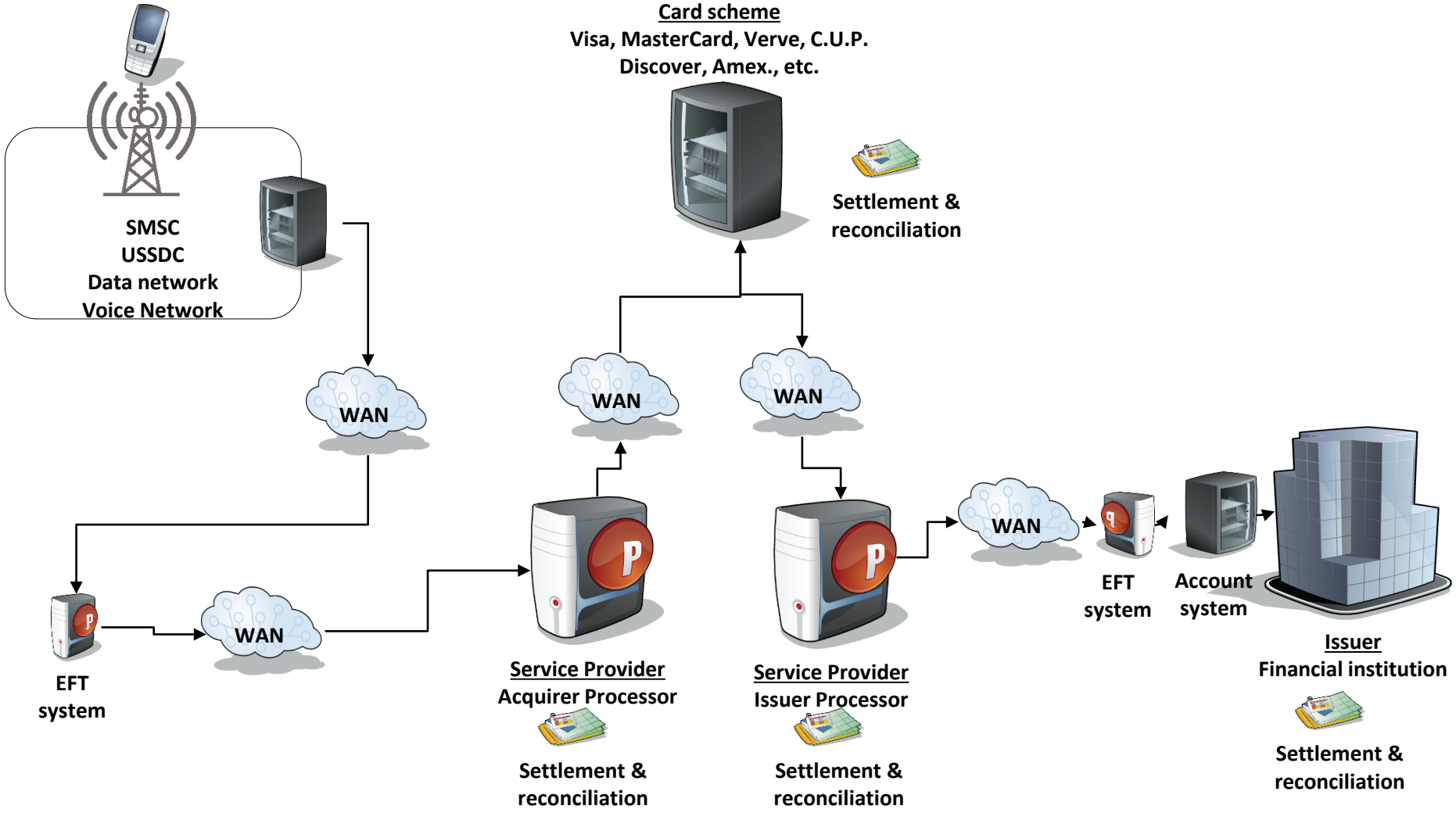
Different markets and players pick any of the "expressions" and pursue them based on the current state of development and adoption of electronic payments in general in that market

Mobile Banking - Architecture



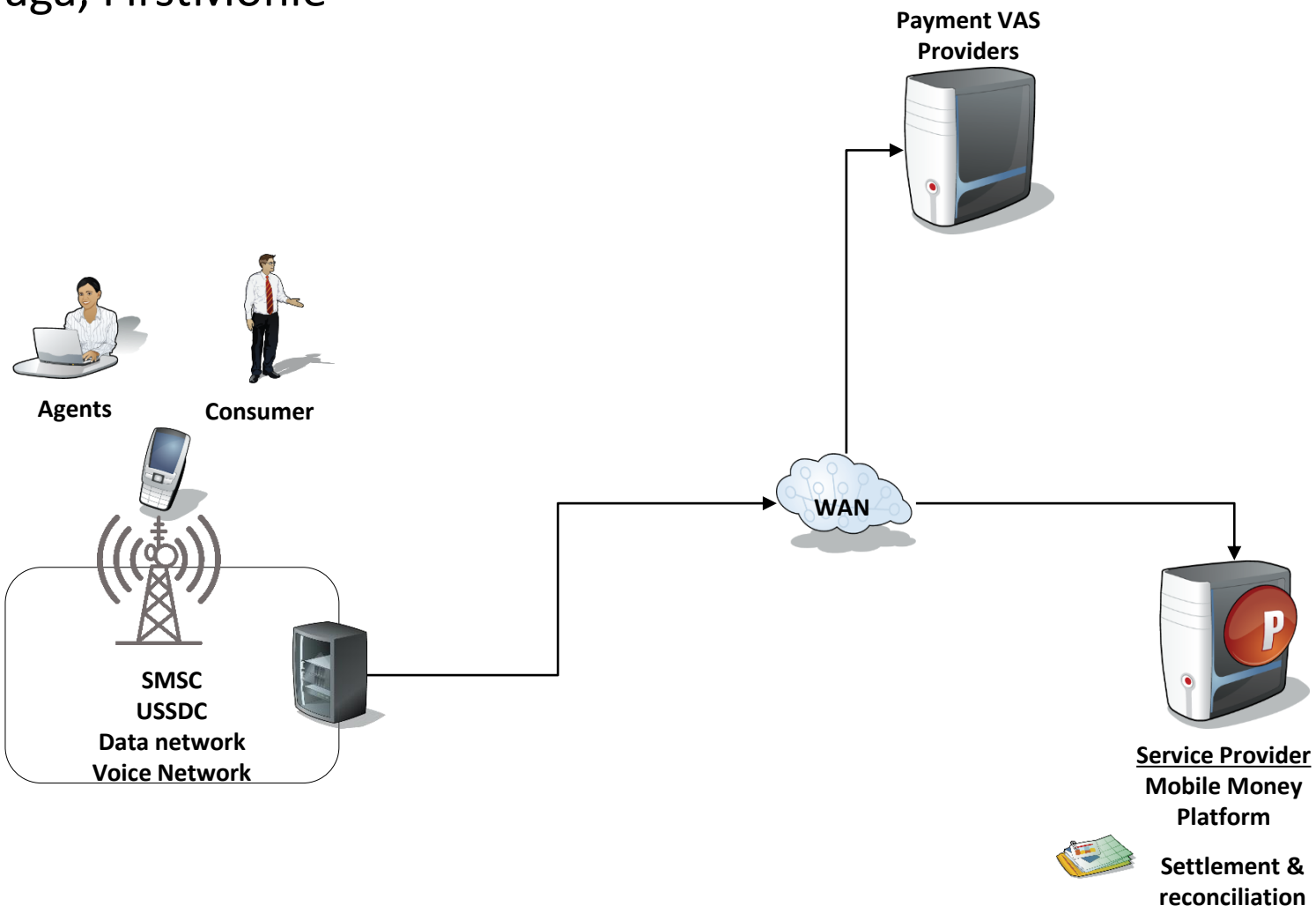
Payments on Mobile Phones - Architecture

E.g. PayPal, Google Wallet



Mobile Money (wallets) - Architecture

E.g. Paga, FirstMonie



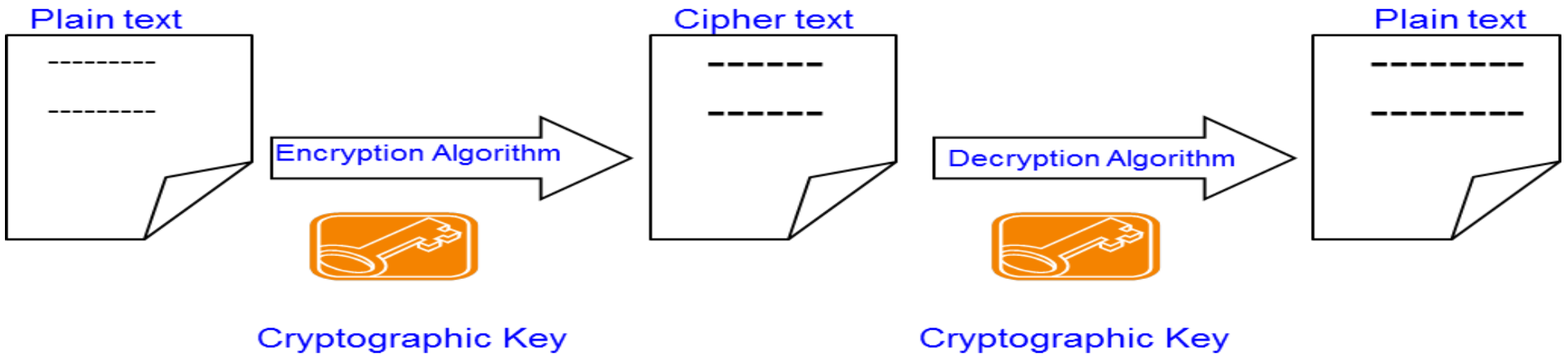
SECURITY CONSIDERATIONS

Interswitch

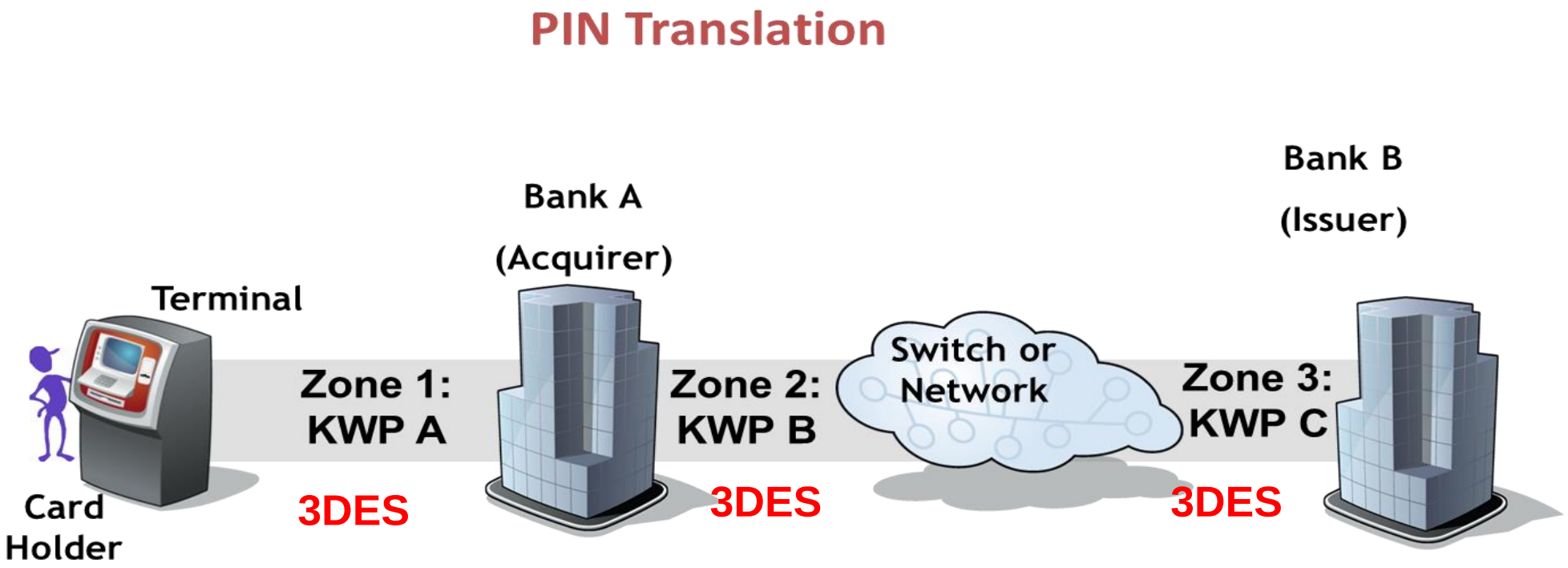
Zone-based PIN translation - Transaction Security

Transaction messages are encrypted during transmission to avoid manipulations through any form of attack

Encryption and decryption is done by applying an algorithm and cryptographic key to data

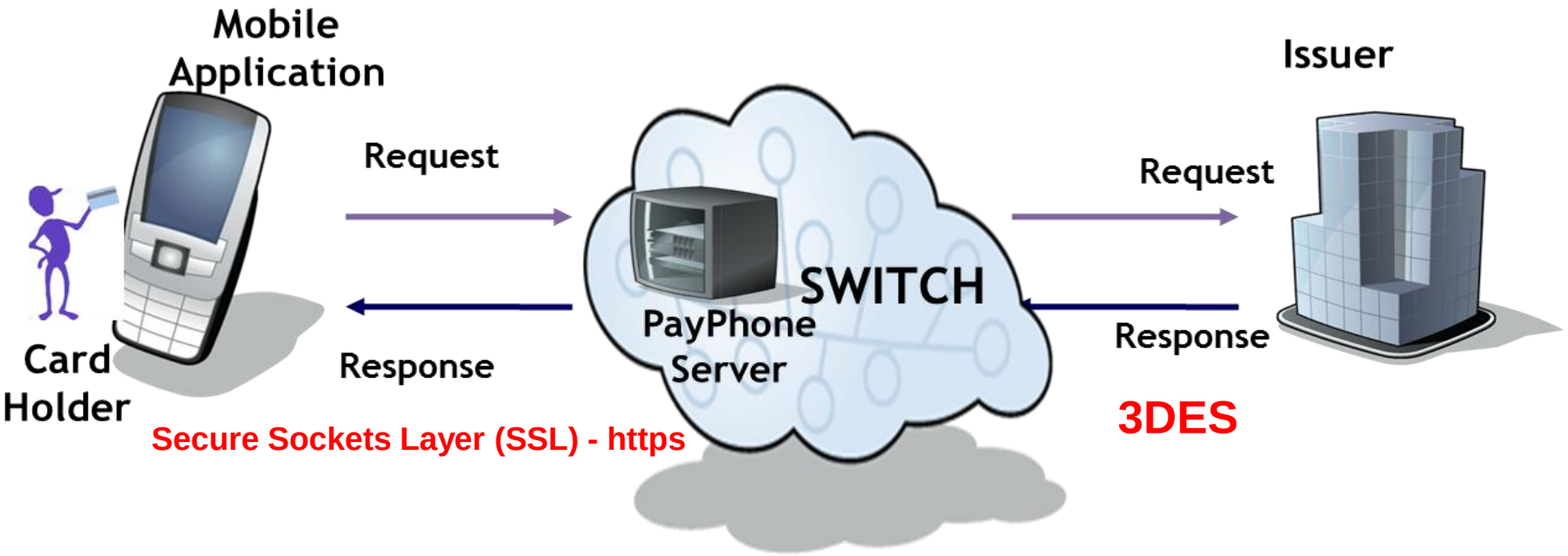


Zone-based PIN translation - Transaction Security



Triple Data Encryption Standard - 3DES

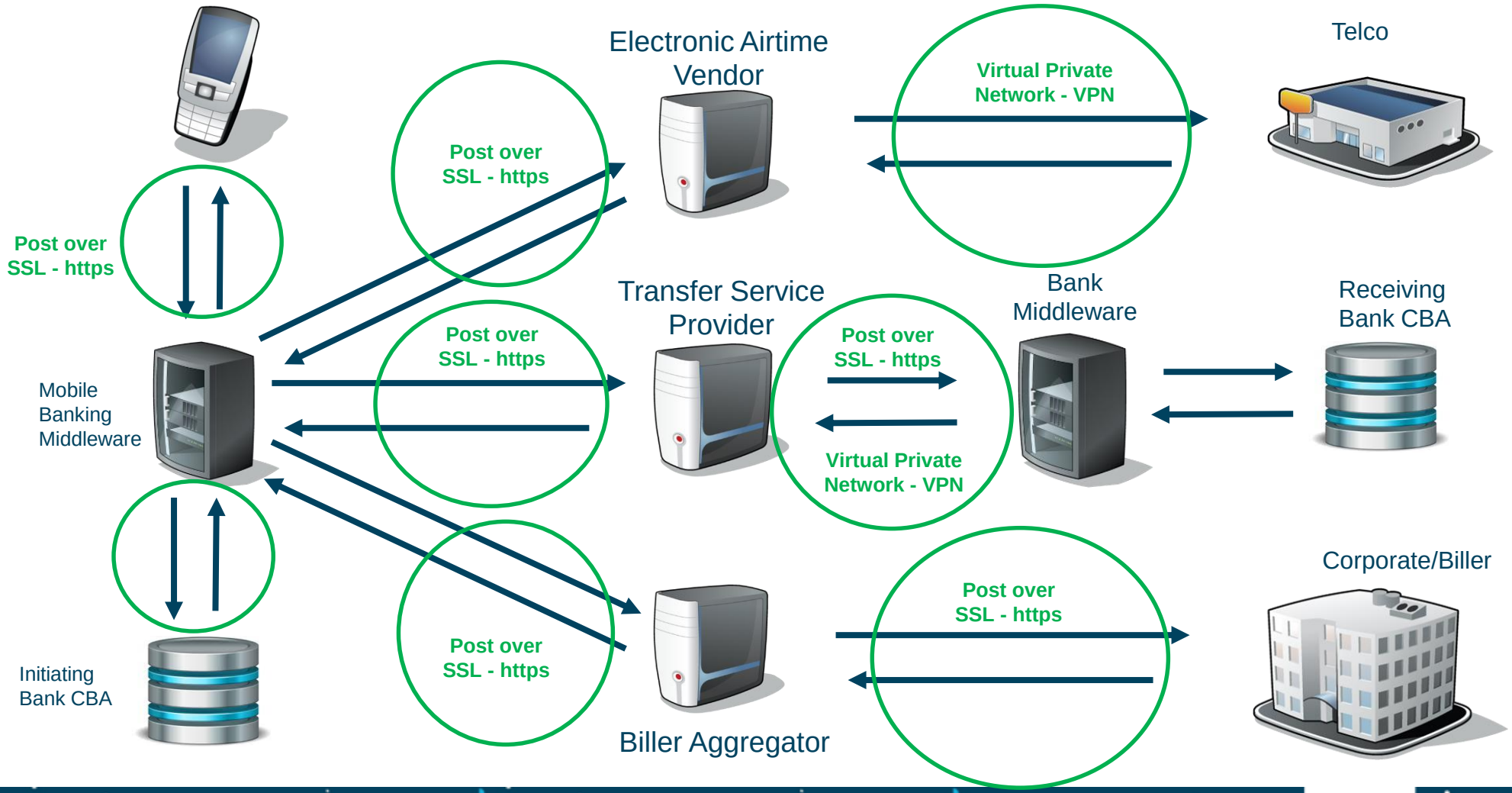
Mobile Environment - Security



Mobile Environment – Mobile Banking App

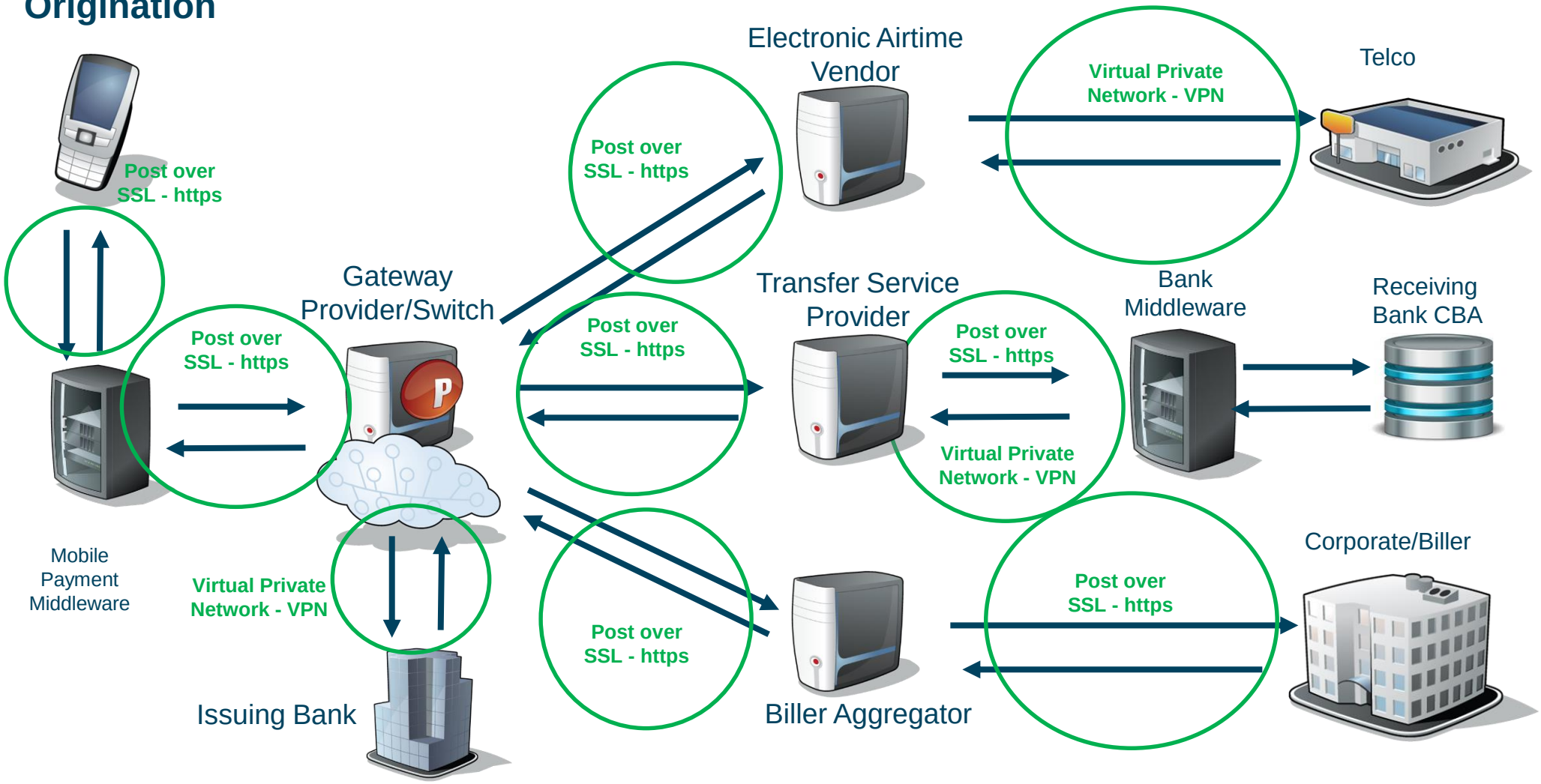
Origination

Receiving

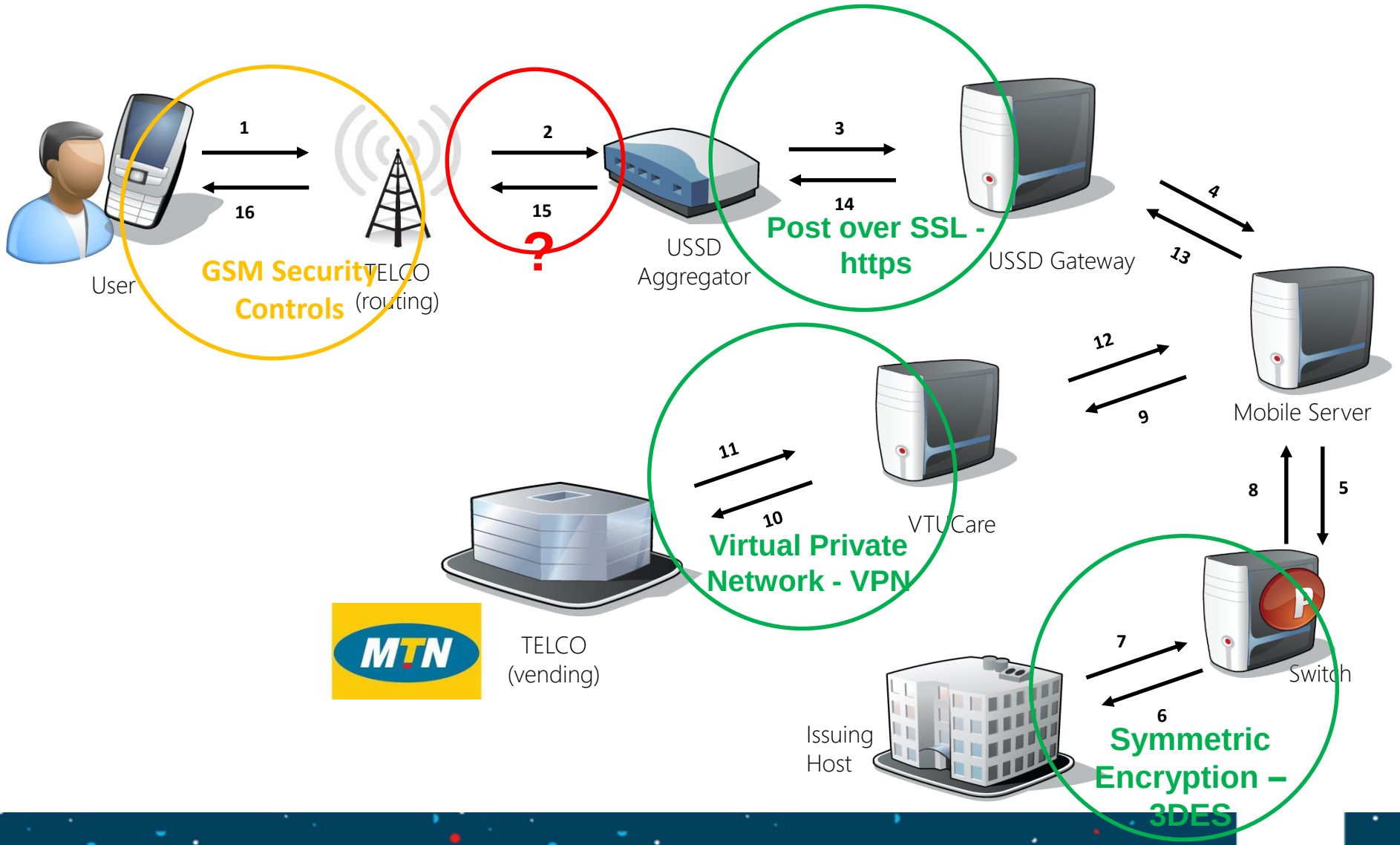


Mobile Environment – Mobile Payment App

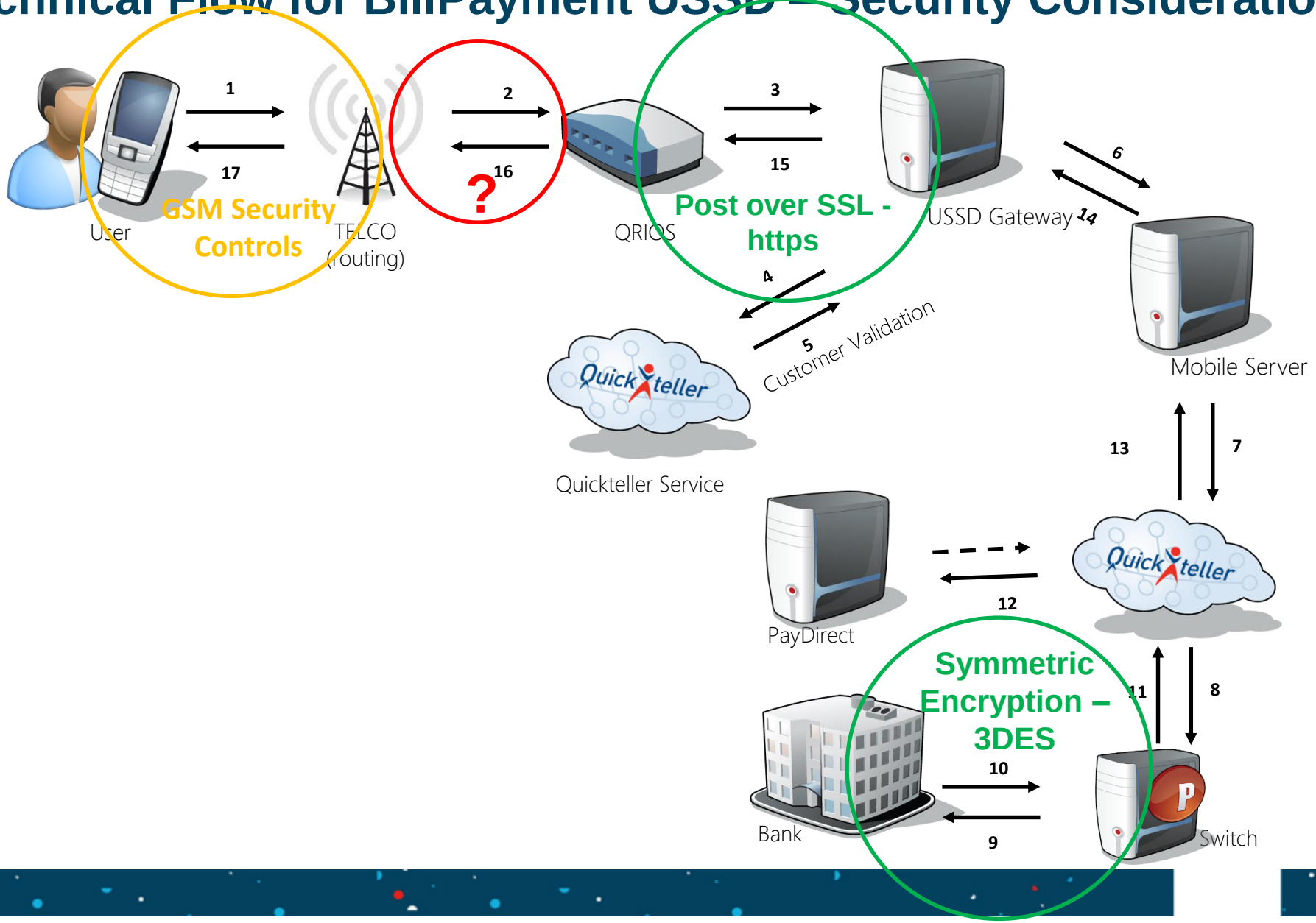
Origination



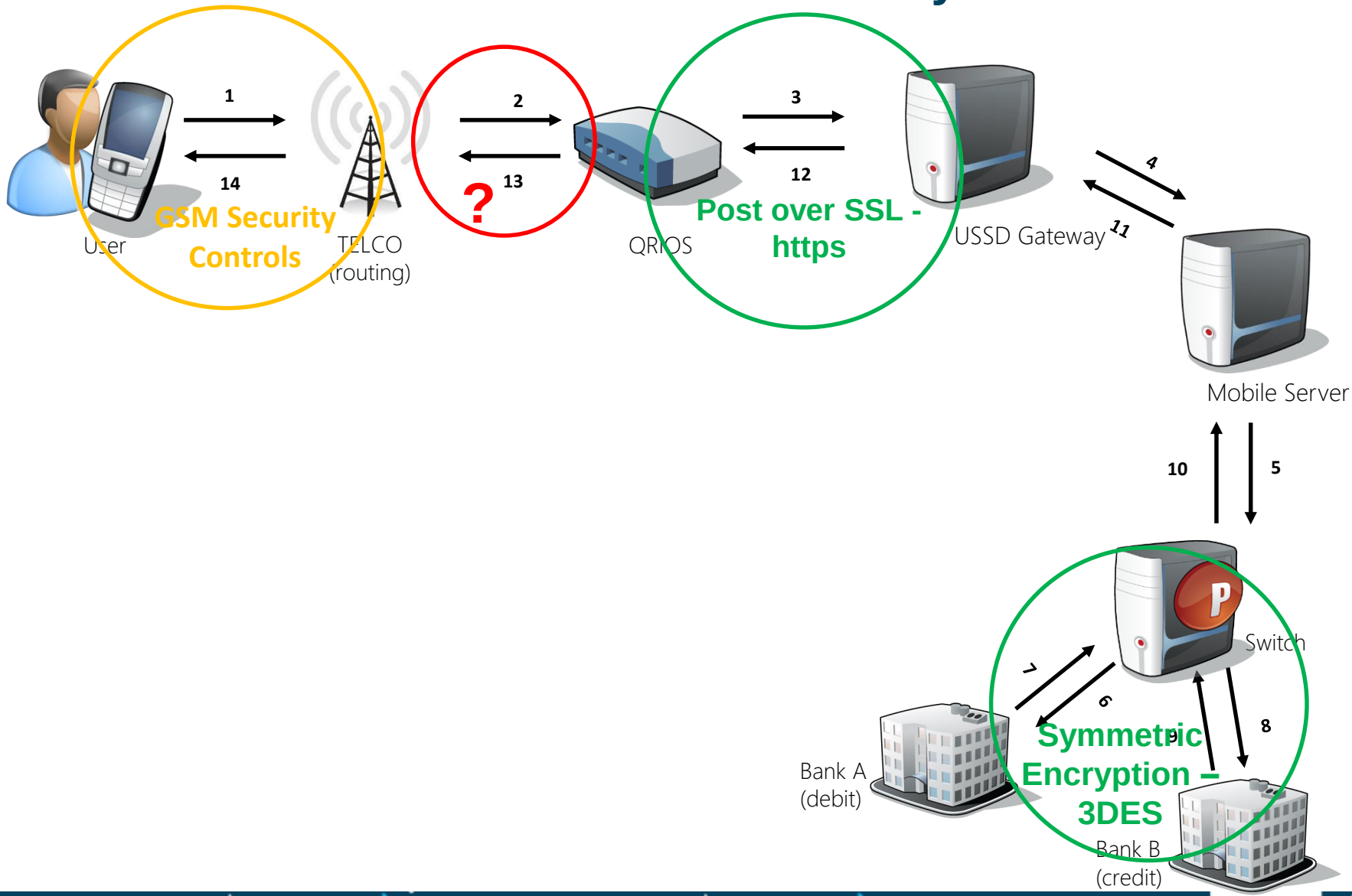
Technical Flow for Airtime USSD – Security Considerations



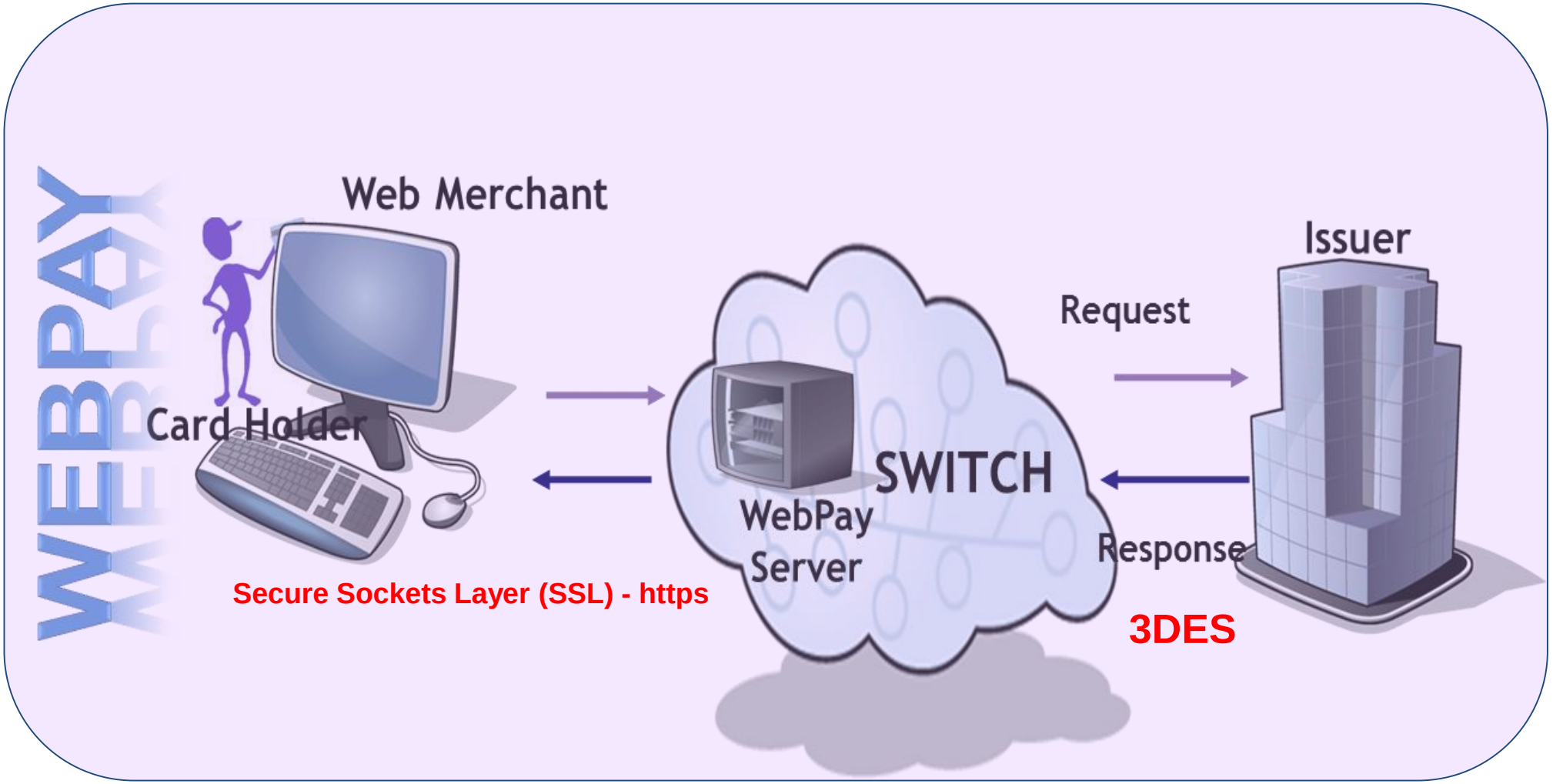
Technical Flow for BillPayment USSD – Security Considerations



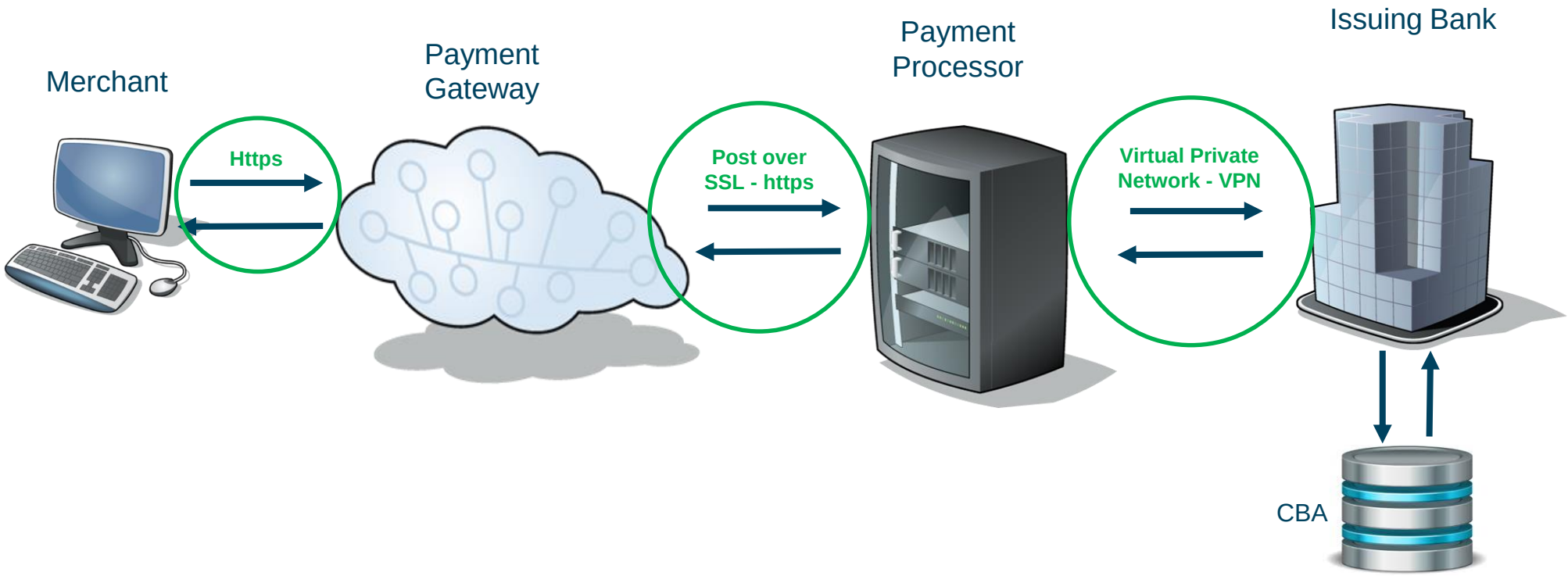
Technical Flow for Transfer USSD – Security Considerations



Web Environment - WebPay



Web Payment – The Current State



Risk and Control Framework

A Guide to the Discussion

Interswitch

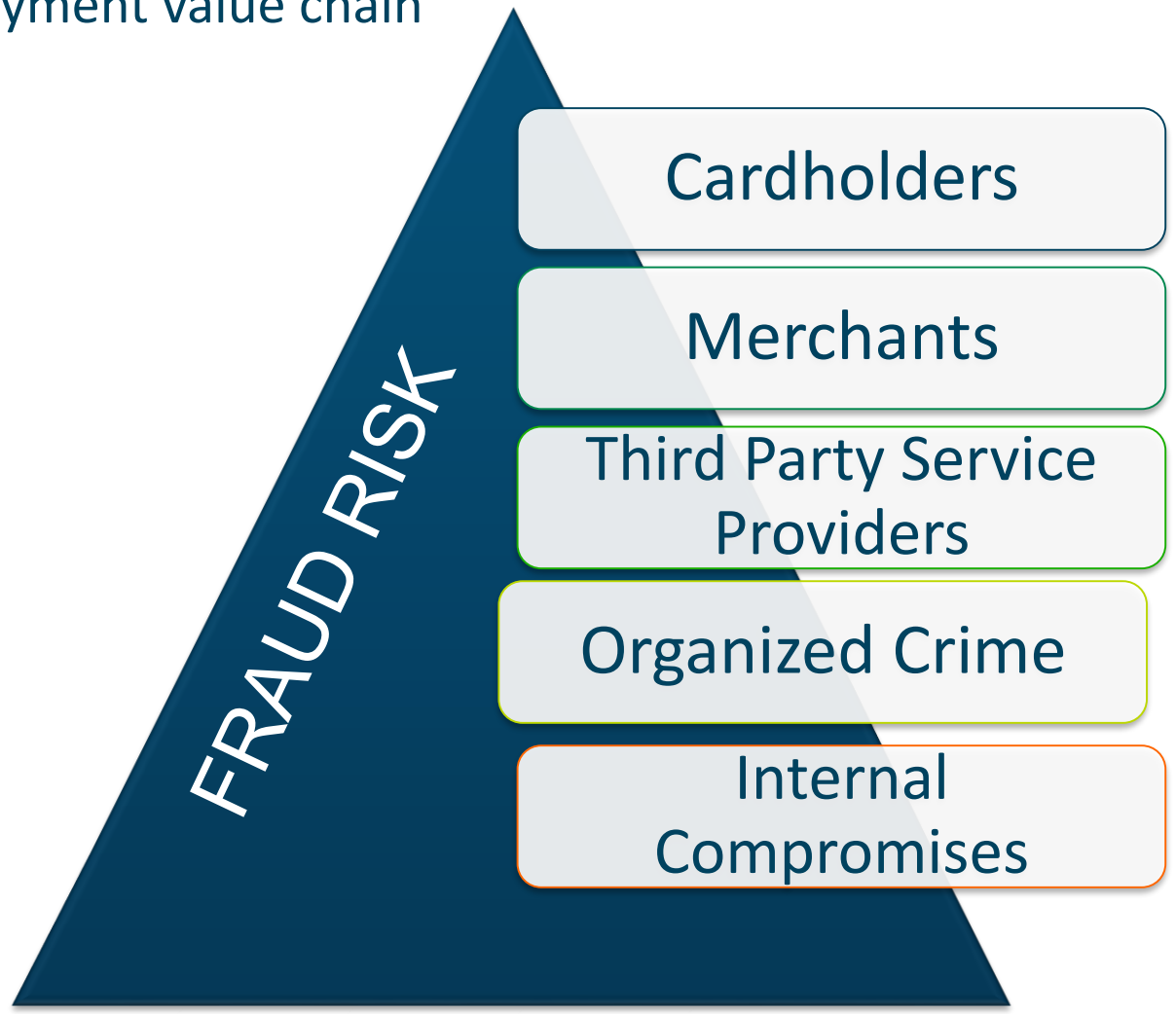
Enterprise Risk Management Framework

Our Ability to answer the following questions:

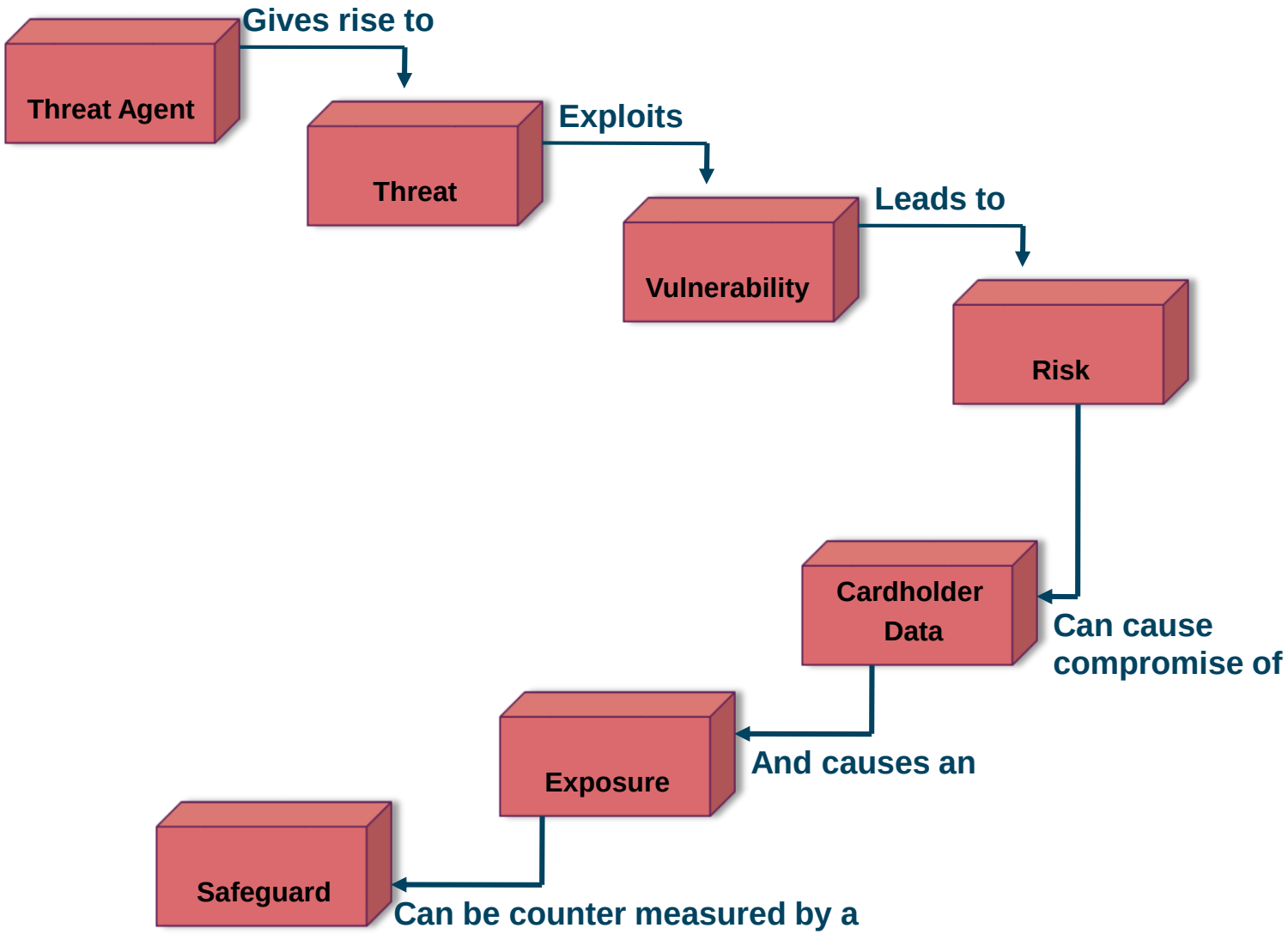
- Circular depiction is highly intentional
- Components are meant to be dynamic (reviewed back/forth in any sequence)
- Having the right culture is key

Sources of Risk

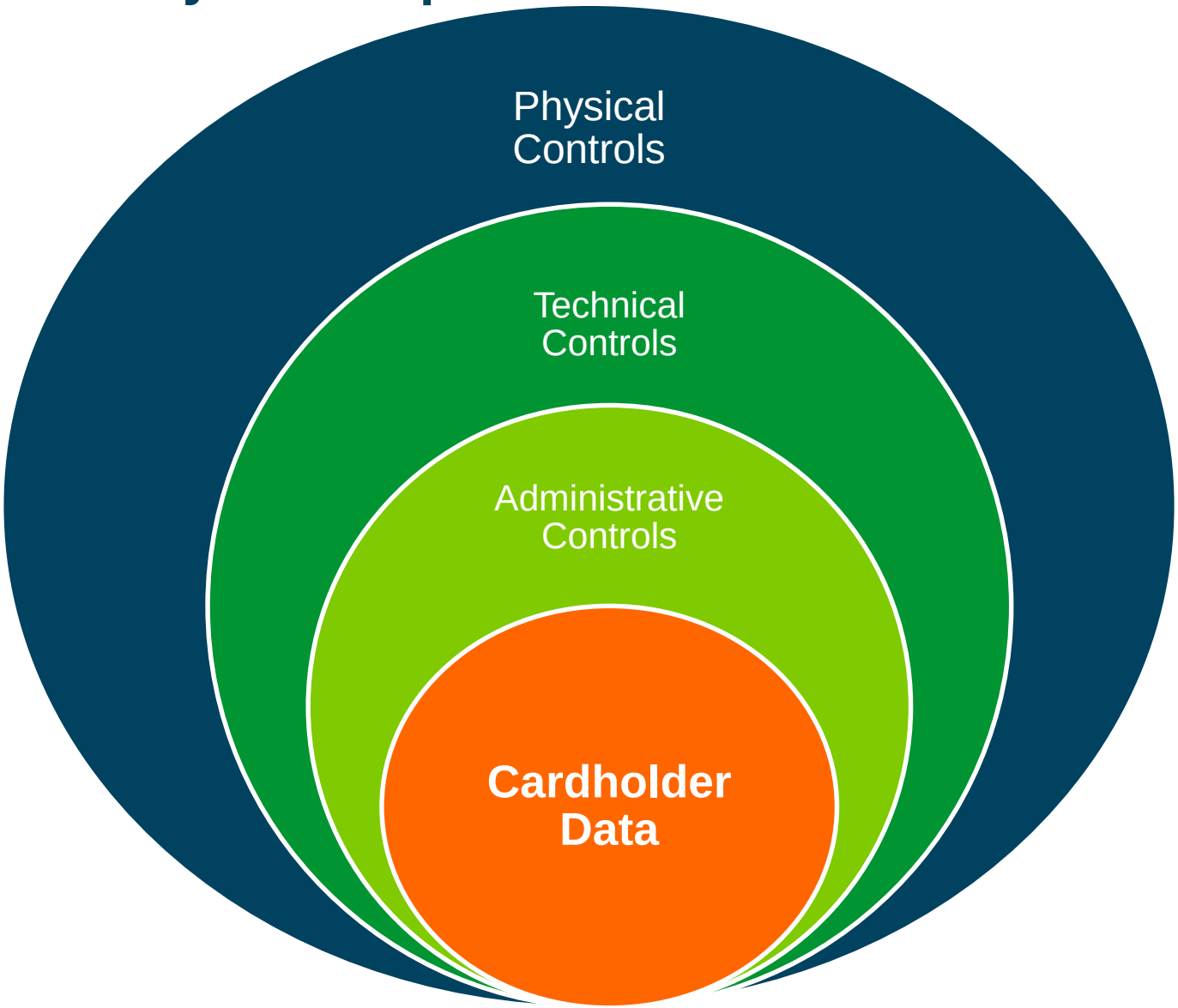
Risk is presented by different parties, in various forms across the card payment value chain



Relationship Between Security Components

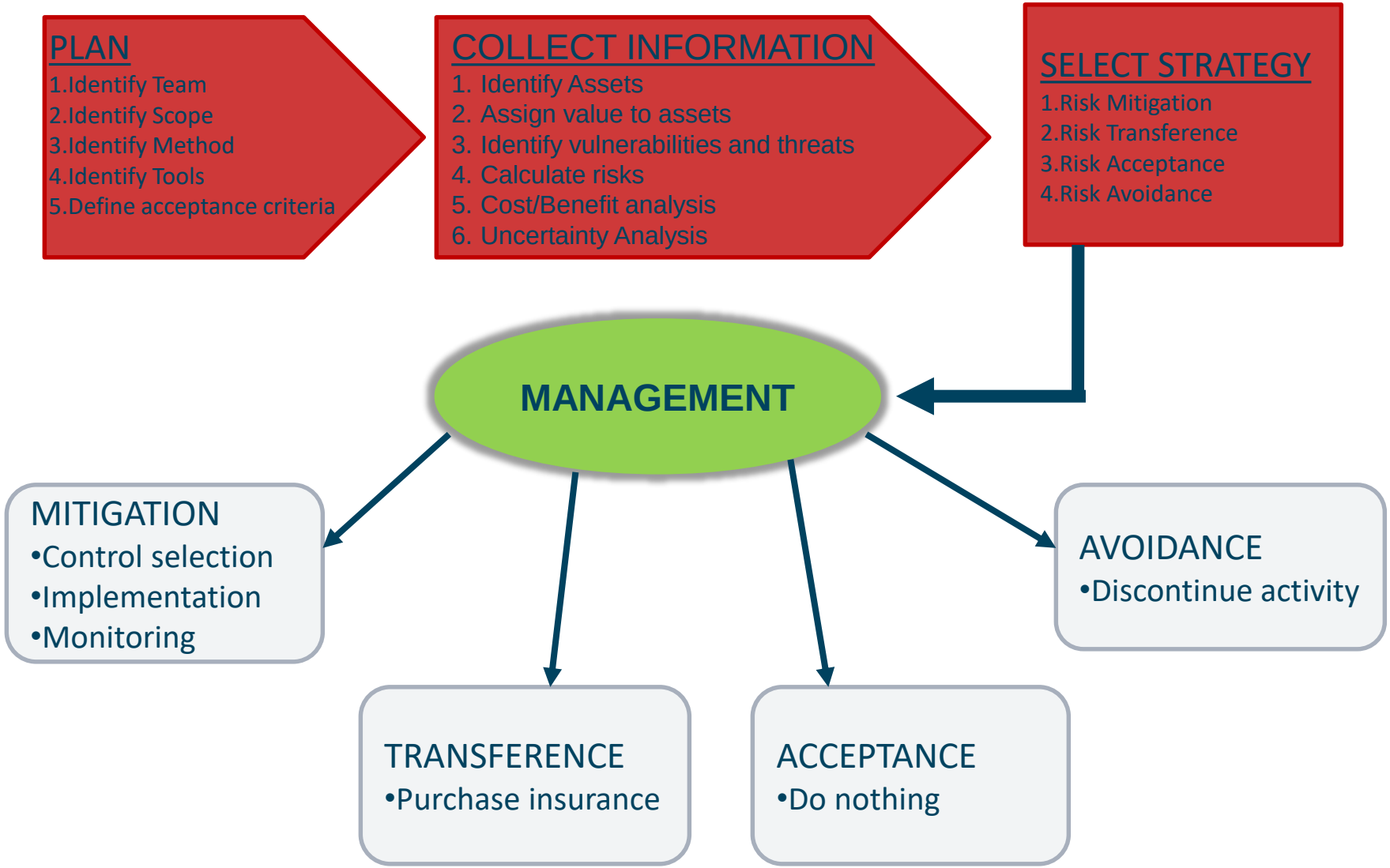


EFT Security Techniques



EFT Security Objectives

Risk Management Set Up



Recommendations on Governance and Controls

Define Standards for Third Party Connections to internal systems

ACAEBIN Role in defining Industry Risk Governance Frameworks

Regulator Guidance

Minimum Security Standards to Service Providers providing processing and Hosting services

Vendor Management Programs – Audits, Reconcilliation

QUESTIONS

Interswitch

Interswitch

www.interswitchgroup.com