(1) E-commerce

Definition

Only for your Reference

Does not cover whole Mid-sem syllabus

goods ⟷ products

physical nature of items

↓

It extends beyond physical objects

- include ≠ services
- ≠ software
- ≠ intellectual creations

For whole Mid-sem Syllabus only refer to your class notes

E/com is also known as

- Anytime Commerce
- Internet Commerce

E/Com → buying & selling of goods/products/services online

- Online auction
- Internet banking
- Payment gateways
- Online ticketing

Features of E/C

- Cashless Payment
- 24 x 7 availability
- Improved sales
- Advt. & MKt. → It helps to increase the reach of advt. of product & service of business
- Support → pre-sales & post-sales assistance to customer
- Improved Comm.
- Global Reach

(3) Hardware requirement for e-commerce

① Web Server → responsible for hosting & delivering e-commerce websites ensuring seamless interaction b/w business & customers
② Database Server
③ Load Balancer
④ CDN (Content Delivery N/w)
⑤ Firewall & Security Mbs
⑥ Backup & Recovery System
⑦ Monitoring & Analytics tool

Web Server → hosts online e-com platform

to host & serve web pages to users accessing the e-com site.

Database Server

database server stores & manages
- product data
- customer information
- orders
- other related data

MySQL

Load Balancer

To distribute incoming web traffic across multiple servers to ensure optimal performance & prevent server overload

CDN ← Akamai, Amazon CloudFront

It caches static contents like
- images
- CSS files
- scripts

} to reduce load times & improve website perf

Monitoring & Analytics Tools

To track website performance
Uptime &
User behaviour to optimize the e-com platform

Database Service

- Product details (Product catalogue (contains all information about product))
- Customer information → profile, history, order history, purchase history
- Order history → order tracking
- Inventory levels
- pricing
- shipping details etc
- Recommendation System — data related to customer behaviour, preferences, purchase history

Database servers forms the backbone of e-commerce operations by efficiently managing data related to products / customers / orders / content.

Generic framework for e-commerce

#4

(1) User Interface & Experience

Website Design → user friendly, easily navigable,
Visual Elements → high quality product images / videos / graphics
Usability → intuitive layout, easy search functionality

(2) Product Mgmt.

Catalog Mgmt → organizing & categorizing products efficiently for easy browsing
Inventory Mgmt → Real-time tracking of stock levels, automated alerts for restocking
Product Recommendations → based on user behavior & preferences

(3) Order Mgmt

Shopping cart → Secure, easy to use cart functionality to (add/remove) product
Save option for later use

Checkout Process → simplified checkout process
multiple payment options →
guest / registered user checkout options

Order Tracking → order status update &
tracking, informed to customer

(4) Payment Gateway Security

PGW → using secure payment gateways for smooth Tx

SSL → SSL/TLS encryption to secure sensitive data during Tx

Fraud Prevention → fraud detection Tools

Tools & Techniques for Fraud Detection

#5

① ML Algorithms → To analyze Tx data, Customer behaviour & patterns to identify anomalies

② AVS (Address Verification System) →
To confirm the billing address provided during Tx with address on Credit Card issuer

③ CVV (Card Verification Value)
3/4 digits code on credit card
To verify the physical presence of card

④ Device fingerprinting
Totally unique characteristics of device used in Tx
IP addr / device type / OS / Browser version
To check fraud/alert fraud activity

⑤ IP Geolocation
To determine the geographical location of an IP address to verify the legitimacy of a Tx.

⑥ Behavior Analytics — Users browsing habits, purchase history

⑦ 3-D Secure (verified by Visa, MasterCard, Secure Code)
Additional layer of security by requiring customer to enter a password/code to complete Tx (created while activating card)

⑧ Tx Monitoring

Protocols

#6

TLS → encrypts data

HTTPS → Secure communication between web browser & Server

---

(5) CRM

Tech. → strategy used by business to manage interactions → deals with current & potential customers to improve customer service → interact with customers by maintaining a detailed record of Customer interaction

Customer Profiles →

Comm' Chs → chat support / email / social media

feedback mechanism → getting feedback from Customers Review → improve products & services

(6) Performance Metrics

Faculty KPIs
- conversion rates
- average order value
- Customer retention

(7) Marketing & Promotion

SEO → to improve visibility & attract relevant traffic (quality + quantity of Traffic)

Social Media Marketing → for brand promotion & customer acquisition

Email Campaigns → running targeted email campaigns for customer retention → re-engagement

8) Logistics

Shipping options → multiple options for customer convenience

Order fulfillment → efficient process of orders packing shipment handling

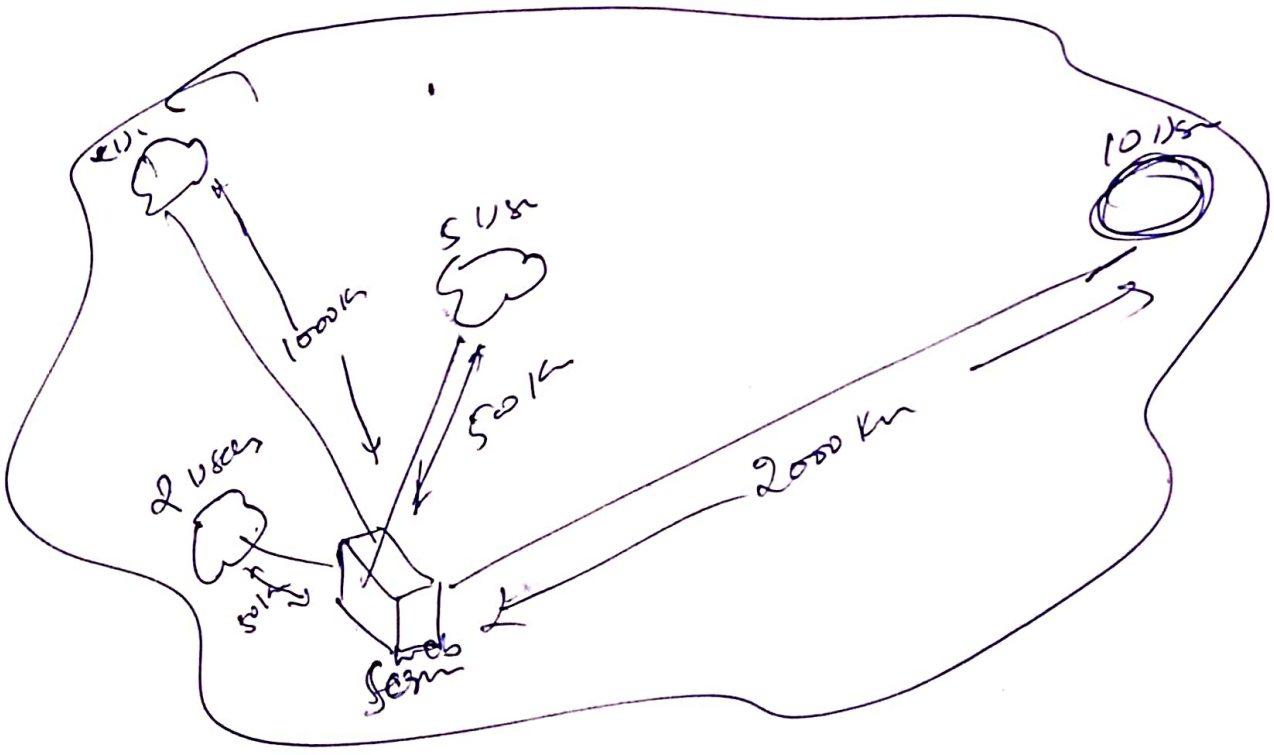
Return & Refunds → clear policies & procedures for handling returns & refunds

CDN Content Delivery N/w (=Distribution)

#8

* CDN = a n/w of interconnected servers that speeds up webpage loading for data-heavy applications.
* When a user visits a website, data from that website's server has to travel across the internet to reach the user's computer.
* If user is located far from that server, it will take a long time to load a large file.
* If the webpage content is stored on CDN servers geographically closer to the users's reaches their computer much faster.
* Primary purpose of CDN = to reduce latency (=delay)

It makes your website faster.



Anycast

#9

It allows multiple servers to share same IP.

When a client sends a request to that IP, the N/W routes it to the geographically closest server that is part of the anycast group.

It enables efficient content delivery & improved N/W performance by directly traffic to the nearest server in terms of N/W distance.

Key points

1. Geographic Routing → nearest server is used
2. Load distribution →
3. Redundancy →
4. CDNs — Anycast is commonly used in CDNs to improve the delivery of Web content, videos & other online resources. By directing users to the nearest CDN server, it accelerates content delivery & enhances user experience.
5. DNS Resolution — To improve DNS resolution times, send DNS queries from users based on proximity
6. DDOS — Distributed Denial of Service attack
7. N/W Efficiency

(5) Benefits Limitations of E/C

#10

* Advantages to Org.
* Advantages to Customers
* " " Society → rural areas access to services, products
  → product cost reduction

Disadvantages

* no universal standard for quality & reliability
* Security in e/com → must be very strong
* risk of purchasing unsatisfactory products
* Banking fraud
* ~~Loss~~ Customer data stored at Seller website is at risk of stolen

6 Generic framework of e-commerce

#11

1. User Interface & Exp. —
2. Product Mgmt —
3. Order Mgmt —
4. Payment & Security —
5. Customer Relationship Mgmt —
6. Analytics & Reports —
7. Marketing & Promotion —
8. Logistics & fulfillment —

---

1. User Interface & Exp.

Website Design → User friendly interface, easy navigation
Visual Elements →
Usability →

2. Product Mgmt

Catalog Mgmt → organizing & categorizing products for easy browsing
Inventory Mgmt → real time tracking of stocks level
Product recommendation →

3. Order Mgmt

Shopping cart → easy to-use
↘ for adding/managing

Checkout Process → simplified
↘ multiple payment options (w.r.t locality)
↘ guest checkout

Order Tracking → order status updates

#12

④ Payment & Security

Payment Gateways : secure payment gateways

SSL certificate : SSL encryption

fraud prevention : fraud detection tools & protocols to safeguard

⑤ CRM

Customer Profiles → creating/managing

Comm^n Chs → chat support / email support

feedback Mechanism →

⑥ Analytics & Reporting

Performance Metrics → Tracking KPIs → conversion rate
→ average order value
→ customer retention

Data Analysis → Using data analytics tools

A/B Testing → conducting experiment to optimize website elements

⑦ Marketing & Promotion

SEO & SEM → Search Engine optimization

Social Media Marketing →

Email campaign

⑧ Logistics & fulfillment

Shipping options → multiple options

Order fulfillment → process of orders, packaging & shipment tracking

Returns & Refunds → establishing clear policies & procedures for handling returns & refunds

#13

E-commerce & Trade Cycle

Trade Cycle [also Known as Business Cycle]

↳ Traditional Trade Cycle = It represents fluctuation in economic activity over time encompassing periods of
- (A) Expansion
- (B) Peak
- (C) Contraction
- (D) Trough

(A) Expansion Phase

Traditional Trade Cycle

Sales ↑
Prod ↑
Employment ↑

→

E-commerce Impact

enables business to reach wider audience & enter new markets

scaling operations rapidly through online platforms

(B) Peak Phase

leverages data analytics & personalized marketing to capitalize on consumer behaviour trends & optimize conversion

(C) Contraction Phase

Slowing down economic activity reduced demand/prod/employment

It provides cost-effective solutions for businesses
- to streamline operations
- to reduce OH costs
- to adapt to changing market conditions

(D) Trough phase

Lowest pt.

E/C offers opportunities for businesses to innovate, diversify revenue streams & pivot towards online sales (H...

Key aspects of E-com influencing the Trade cycle

#14

① Global Reach

② Efficiency & Automation

E/C streamlines
- supply chain process
- inventory mgt
- order fullfilment through Automation
- enhancing operational
- reducing lead time

③ Data Driven Decision Making

Vast amount of data generated by E/C platforms
Can be used for
- market analysis
- customer insights
- strategic decision-making

} to optimize their operations throughout the trade cycle.

SSL

#15

Secure Socket Layer = an encryption based Internet Security protocol

↳ its sucessor ⇒ TLS

HTTPS —means→ SSL/TLS

HTTP —means→ SSL

* SSL initiates an authentication process (= hand shake) b/t 2 communicating devices ⇒ [mutual authentication]

↓ Analogy

(When a Police officer checks your ID you also check his ID)

* SSL also digitally signs data in order to provide data integrity

(to verify that data is not tampered on the way)

SSL certification (TLS certificate) = ID card that proves someone is who they say they are

CA (Certificate Authority) = issues SSL certificates

Key technologies of e-commerce (Later)

#16

Personalized product recommendations (using ML)

chatbots for customer service

intelligent virtual assistant

predictive analytics for inventory mgmt

Blockchain for decentralised Tx.

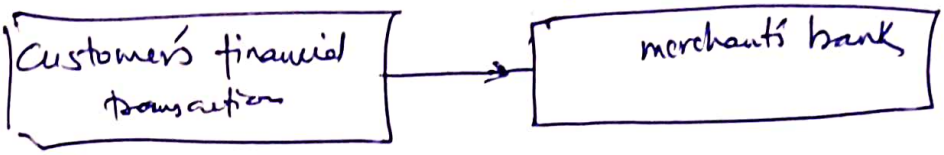
Blockchain for supply chain mgmt

#17

Payment Gateway (P/G) → PayPal

↓

acts as a bridge b/T



facilitating authorization & processing of online payments

How it works

① Customer places an order
Customer selects product/service on e-com website & proceeds to checkout page.

② Payment Information Enquiry
Payment details → credit/debit card info on P/Gateway form on the website

③ Encryption & Secure Tx
P/G encrypts the payment data to ensure secure Tx protecting sensitive data

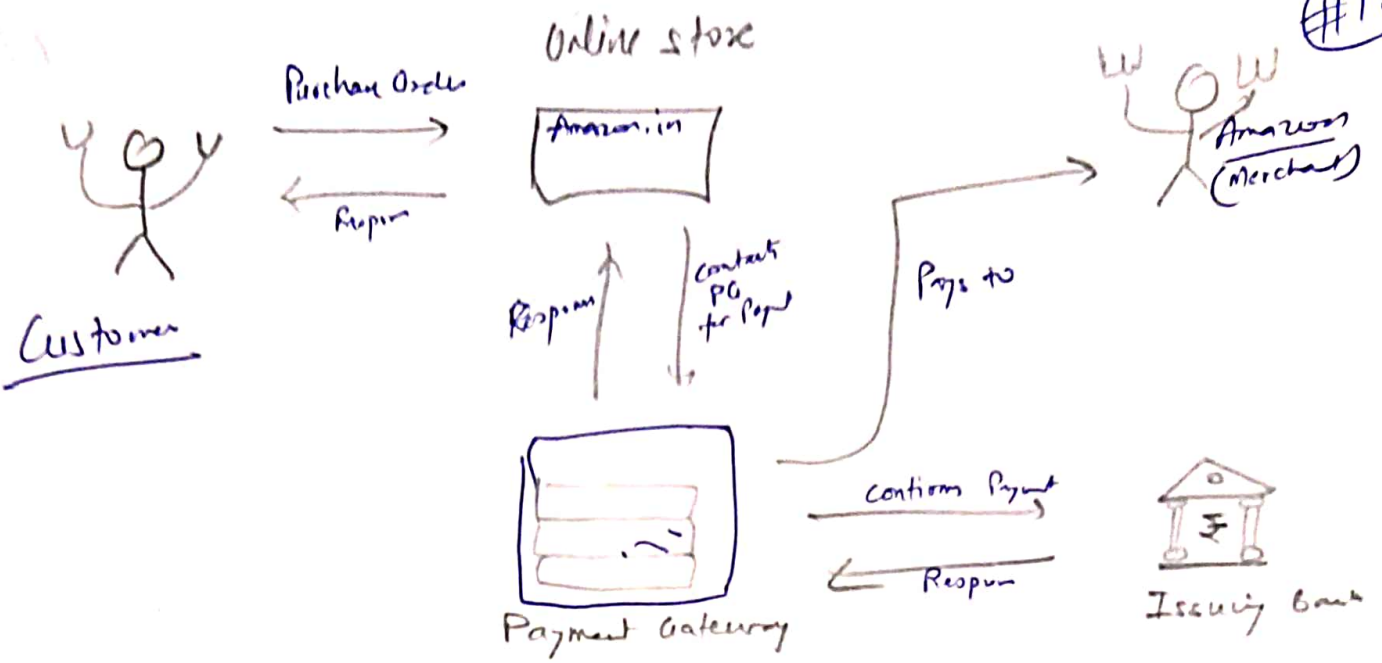
④ Authorization Request
P/G forwards the encrypted payment info. to the payment processor or acquiring bank for the payment authorization

⑤ Authorization & Verification
The acquiring bank verifies the transaction details & checks the customer's account balance to approve/decline the pay

⑥ Transaction Response
Bank responses back to P/G &
P/G forwards the approval/rejection to e-com website & customer

⑦ Payment Settlement
After approval, P/G settle the funds from Customer's A/C to Merchant's A/C

#18



- Data Integrity
- security features

EDI

Lecture #19

L-1

Definition →

What type of document →

benefits of EDI → (Important)

Evolution of EDI →

What is P.O. →

What is Invoice →

L-2

* Tech. behind EDI

Data formatting

Data Transmission

Translation & Mapping

Connectivity

* Types of EDI system & architecture

* Direct EDI ⇒ P to P

* Web-based EDI → cloud base
→ through web (Internet)

* Integrated EDI → b/t internal business process & external providers

* Outsourced EDI → 3rd party

* Key components of EDI sys

- Translator
- Comm's module
- Data Integrator
- Compliance Check
- Audit Trail & Monitoring
- Security features

To Integrate EDI sys with internal systems like ERP, CRM, Inventory sys to automate data exchange & streamline business operations.

L-3

#20

EDI Standard formats

ANSI X12

EDIFACT

Why use Standards (benefits)

Interoperability

Data Integrity

&

compliance

Protocols in EDI comm

AS2

FTP

SFTP

Evolution of EDI

#21

Business Processes →

* P2P (Procure-to-Pay)
* O2C (Order-to-Cash)

Specs

EDI standards → each with its own set of docs

USA →	ANSI X12 standard
EU →	UN/EDIFACT

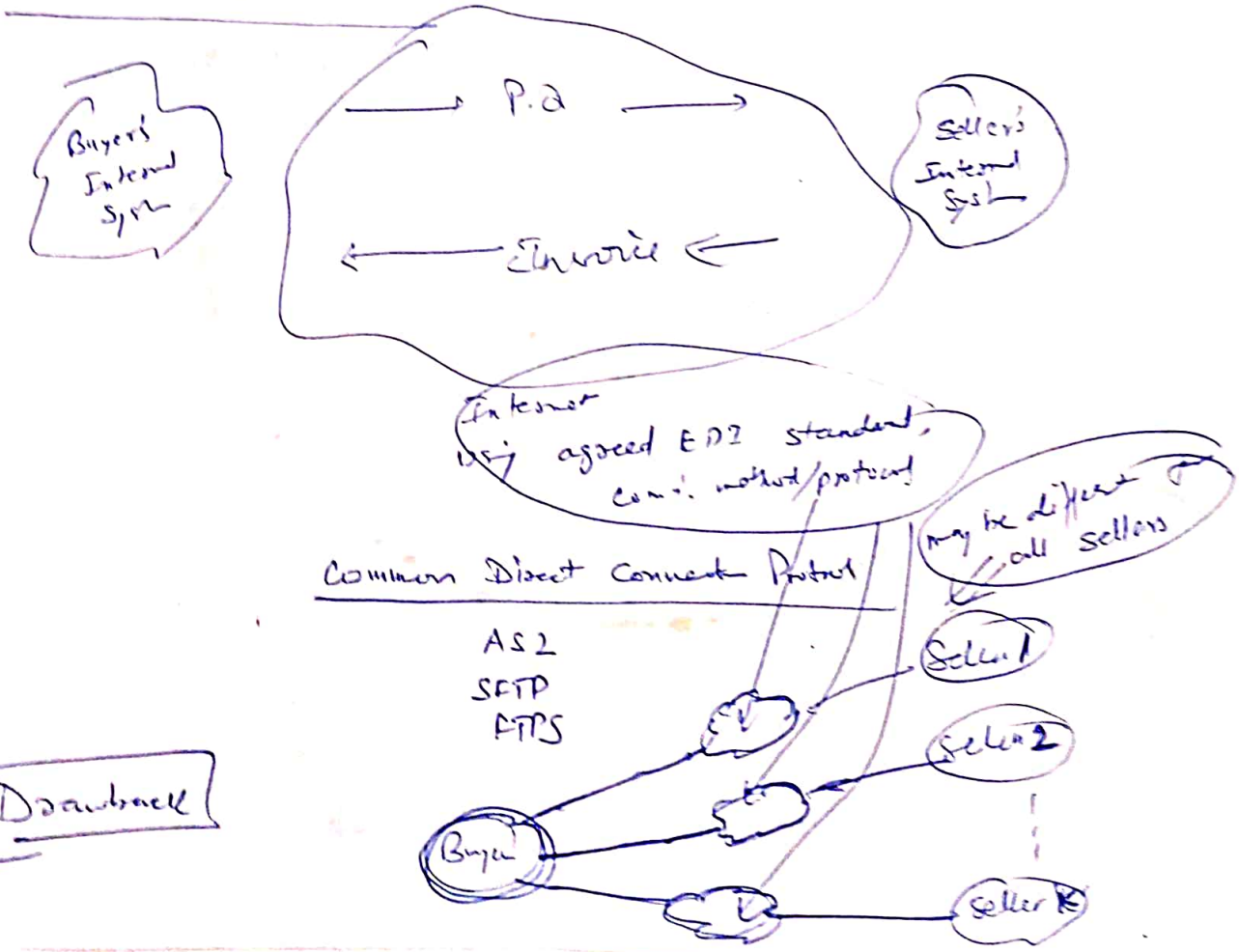
Specific Industries have developed their own EDI standards

Automotive, Telecom → ODETTE, VDA

Retail → VICS

2' Basic EDI implementation

① Direct connection model

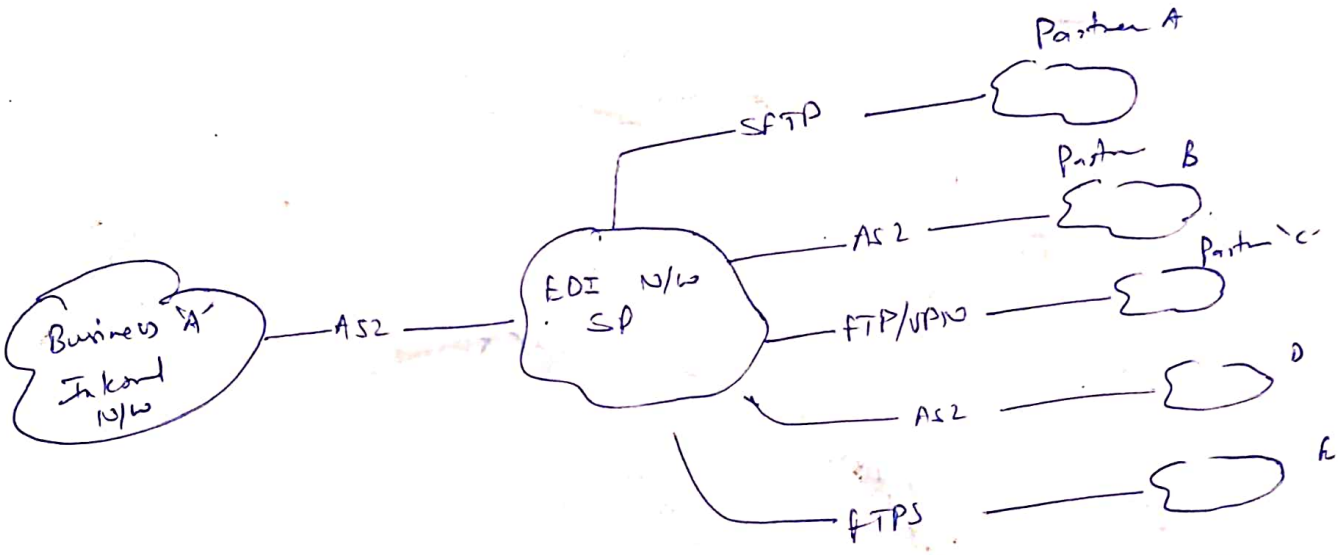


Drawback

#22

(2) Networking Model

To select an EDI SP that shields partner seller/buyer from the complexities of varied supply chain protocols required by different Business Partners



VAN

Value Added N/W

Value Add → came from Extra validation, Security & auditing capabilities that the EDI VAN provider delivered

What comprises an EDI document ?

#23

EDI document is comprised of

- data elements
- segments
- envelopes

} formatted w.r.t. particular EDI standards

Transaction Set / Message

In EDI L/G, a single business document such as P.O. / Invoice / Advance Ship notice is called a Transaction set or Message.

A Tx set is comprised of
- data elements
- segments
- envelopes.

Data element = individual items of information within the document.

eg:
- city name
- state name
- country name
- item #
- quantity
- price

Each data element in Tx set is defined in EDI standard by the type of data it represents

#24

f.g.

(Numeric data element) is different from (text data element)

(numeric data element
text data element
calender date data element) all must be distinguished from each other

The data element definition will describe

* Data Type of { numeric, alphanumeric, data, time }
* Min / Max. Length
* Code values → that must be observed with a particular type of data

f.g.

if Data Element = Unit cost

a currency code element (e.g. $) should be used to indicate what currency.

Segment ⇒ A segment in an EDI Tx set = a group of like data element

for each type of document, EDI standards define

- mandatory / optional / conditional → segments
- Each standard has its own dictionary. Every piece of information in business document has a corresponding EDI element, these EDI element are defined in a Dictionary
- required sequence of segments & elements
- How many times a segment may be repeated.

#25

In Doc like P.O./Invoice }

Data Elements such as

- City
- State
- County
- item #
- quantity
- price

Each DE in a Tx Set = [defined in the EDI standard by the type of data it represents]

Numeric / Decimal / String / Date / Time / Binary

Data Element Def. describes
- ↑ Data Type.
- Min & Max Length
- Code Values

Eg.

If DE = Unit Cost

Also use a Currency Code Element (e.g. $ or €)

... message to test the encrypted link

Segment

#26

A Segment in an EDI Tx set

= a group of like ~~Data~~ Elements

(2) Buyer

Chandler Big Enterprise
15, Yeman Road
Yemans

PO No. : 4708
PO Date : 9/30/2020

PO # 1 Segment (1)

(3) Item Details

Item No	Quantity	Unit of Means	Price	Product Cost
1	100	EA	27	331896.42

Total item : 1 Total Quantity : 100 — Summary (4)

4 sections deals with different set of information

Each section is described by → Particular segment

Each segment begins with a Segment ID

it describes the type of data element that follows

The Data Element within each segment are separated by a Data Element separator (*)

EDI

ANSI X12

ANSI

#27

Initially developed for financial TX, business documents
It covers a wide range of common
including
- P.O.s
- Invoices
- payments
- shipping notices
- ~~Loan~~ H.R. forms
- Healthcare Claims

Standard defines
- Structure
- data element
- codes
- Syntax

} for each type of document

Different ANSI X12 Standards:

		Type of Doc
X12 850	——	P.O. standard
X12 820	——	Invoice standard
X12 856	——	shipping notice standard
X12 820	——	Payment Order / remittance advice
X12 855	——	P.O. Ack
X12 862	——	Delivery

Different standards define Specific Data Elements & Codes for particular kinds of business information

There must be agreement b/t B2B on which ANSI X12 standards to use for each type of document
like P.O.
Invoice etc

... message to test the encrypted link

Video {TLS} → for Safe Comm. b/t 2 devices (#28)

4 Steps (3)

① Create a Secret-share Public Key Pair

② Use Public key crypto to establish a shared secret

③ Use the shared secret to establish a secure link using a secret-key cipher

④ Data Exchange over Encrypted Link

Step 1 **Create a key pair :**

Client creates a new pair (its Public key + its Private key) when it opens a new connection.

Step 2 **Establish a shared secret**

(i) Client sends its Public Key to the server & asks for a TLS connection.

(ii) Server creates its own key pair (Public Key + Private Key) (for this connection)

(iii) Server sends its public key to the client

(iv) Client & Server compute their "shared secret".

Client's shared secret [Client's Pvt. Key + Server's Public Key]

Server's shared secret [Server's Pvt. Key + Client's Public Key]

Step 3 **Establish Encrypted Link**

(i) Devices create crypto keys using a "hash" function. Separate keys for separate roles

(ii) Client sends message to test the encrypted link

(iii) Server sends reply to confirm the test message arrived

Step 4 Exchange Msg

#29

Hashing for Auth

Digital certificate

#30

Creating a Digital Signature — 2 steps

Data

① HASHING

Hash

② Encryption ← Pvt. Key

= Digital Signature

Data + SIG

TX

AT Receiver

Data + SIG

Hashing

Hash value

Using Public Key of Sender for Encryption

Hash value

Should match

Verifying

Digital Signature

Hashing

Hash (Data in TX)

Data

Hash

Data + SIG

P.T.O.

data with the session ...

Validating a Public Key certificate

#31

By verify its Digital Signature

a certificate has 3 main parts

- Public key
- Digital Signature → By Certificate Authority
- Owner name

Certificate is created in 2 steps at 2 locations

one is site ready the Certificate

other = certificate authority

(A) Issuing a Certificate

A website sends her Public key to CA

the CA encrypts the Public key with its Pvt key

(i) A website creates it key Pair (Pvt. Key, Public key)
Site does not share its Pvt key with anyone, even not with CA (Certificate Authority)

(ii) Site shares its Public key with CA.

(iii) CA signs (encrypts) Site's Public key with its own Private key

(iv) CA formats it into a certificate

(B) Validating a certificate

(i) Check Hash value for Data integrity ✓

(ii) Using CA's Public key encrypts certificate

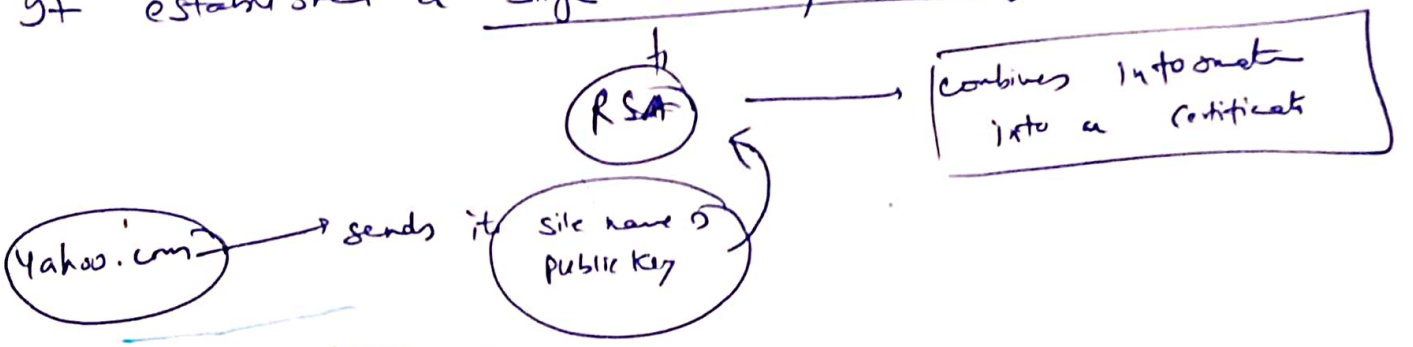
#32

7

Who signs a Public Key certificate?

TLS → need a public key certificate
// must be issued by a CA a browser recognized

Netscape introduced Secure Web site Technology using SSL/TLS
& established a single trustworthy authority to sign certificates



Anyone accessing Yahoo.com can establish/validate it certificate using RSA's Public Key
C= Trust Anchor
↳ Trusted CA's Public Key

1st validate Website's owner
then ~ ~ name

Modern browser work with many CAs
recognize

Browsers keep a collection of public Keys for recognized CA.
(= Trust Anchor)

#33

CA — an entity that issues digital certificates conforming to ITU-T X.509

- a trusted 3rd party that gives clients assurance that they are connecting to a server operated by a validated entity.
- Digital certificates certify the public key of the owner of the certificate and that the owner controls the domains being secured by the certificate.

TLS/SSL Handshake Process

1. Each TLS certificate consists of a key pair (Public Key + Private Key).
2. Every time you visit a website, the ~~client~~ server & web browser (=client) communicate to ensure secure TTL/SSL encrypted connection
3. When a Web browser (or client) directs to a secured website, the website server shares its TTL/SSL certificate & its public key with the client to establish a secure connection and a unique session key.
4. The browser confirms that it recognises & trusts the issuer (=CA) of SSL certificate (e.g. Digicert).
   The browser also checks to ensure the TTL/SSL certificate is unexpired, unrevoked & that it can be trusted.
5. The browser sends back a symmetric session key & the server decrypts the Symmetric session key using its private key.
   The server then sends back an ACK encrypted with the session key to start the encrypted session.
6. Server & web browser now encrypt all transmitted data with the session key.

Tokenization

#34

Process of replacing sensitive data in a Tx (eg. Cardholder's PAN) with non-sensitive data 'token'.

These Tokens → do not have any value/significance outside of the Tx.

- simple random values
- references that relate back to the tokenized payment data, allow it to traverse the networks it needs to complete the Tx

---

From Oct 1, 2022 → RBI mandated use of tokens for credit card & Debit card for Online Merchants

1st seek customer's consent
then raise a request for a token → (issued by card Issuing Bank or card Network ↓ Visa/Master.)

According to RBI

(F) refers to replacement of actual card details with an alternate code (= token) which shall be unique for a combination of card, token requestor & device. → (identified device)

[entity which accepts requests from the customer for tokenisation of a card & passes it on the card N/w to issue a corresponding token]

* Token is unique to a specific card # & is usable only on that particular site or mobile app.

Token is like a Train Metro ticket → valid only for that route

#35

Token on file →

Card on file →

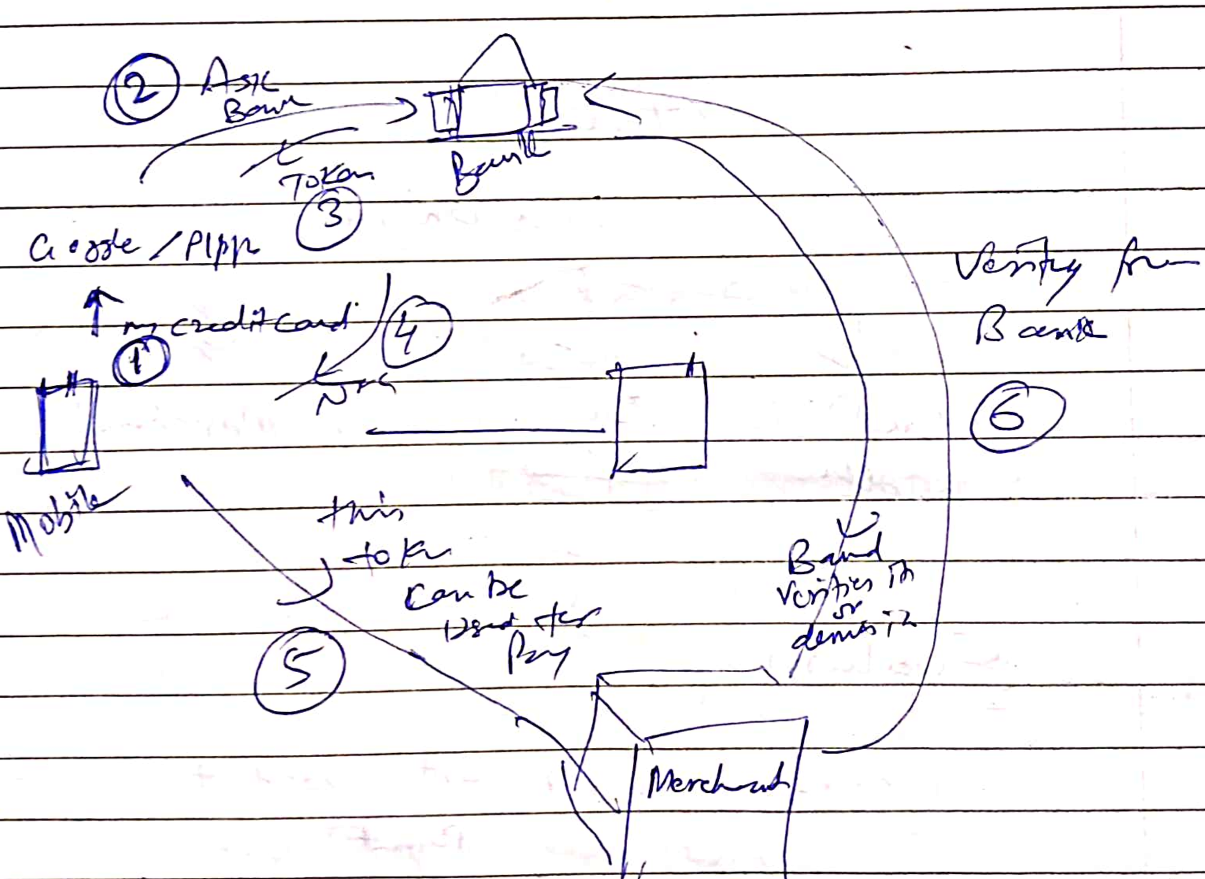
Token on device →

Tokenization

[Process of replacing sensitive data with a surrogate value]

Credit Card # ⟷ (Nonrelationship between them) Surrogate value

How to correlate them with each other?

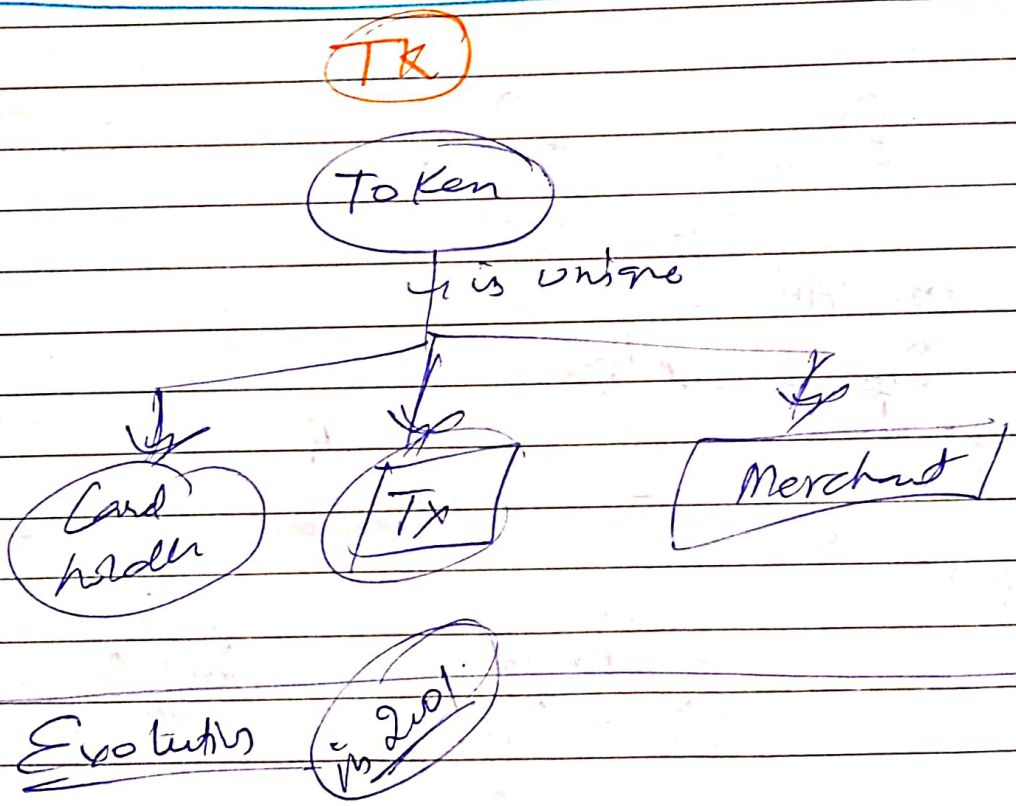


Merchant never see your Credit Card #

(T)

featured offered by Payment Gateway to better protect merchants from a potential data breach

(T) allows merchants to reduce their PCI scope by delegating the storage of sensitive payment card and consumer data to a PG.



Evolution in 2001

(classmate.com) Ist used it to secure TT Payment syst

Guideline from UID to secure the Adhaar Data in the Token vault

Tokenization ⟷ De-tokenization

#38

Use cases

Token on file

Card on file

Token & Card = in the web or on device

eg Myntra, FlipKart

Token on device → generate a Token but that token stays in the Mobile

X

RBI guidelines

eg Google Pay, Jio Pay

User can create a token of his/her card number and then use his/her mobile phone for Tap & Pay transaction

Same like Card Present Tx

Tap & Pay with wearable = also Token enabled

Token Keywords

Token on File — Token reference has been stored at merchant app or browser for ecom Tx

Token on device — Token presents at merchant app and can be used to perform POS.

Payment Token — Token generated to pay

Token Cryptogram — Dynamic CVV
Tx unique value

ID & V during provisioning — Identification & verification through SMS / email / customer care

Token Explanation

Token explanation → refers to Token value after card expiry

There is a (Key) associated with each Token → can't be expired → can't be updated.

# LUK — Limited Usage Key
LUK = Key which is going to generate a token

Token Reference ⇒ (Reference of a particular token)

- Every merchant does not have capability to map Token at his/her end
- 97 is never used for Tx
- Merchant stores it and when Merchant wants to do a transaction

PAR (PAN A/c Reference) →

Card — PAR → Token 1, Token 2, ..., Token N

- never used for any Tx,
- To know all the Tokens issued on a single card

Purpose of PAR → only for Merchant reference
[not stores Token]

Token Service Provider → Visa
→ MasterCard
→ Rupay
→ Card Issuer like SBI

#40

Page No. 5
Date

Token Domain — To specify where the token will be used
→ E-comm Tx
→ POS Tx
→ ATM

Stakeholders involved in Tokenization 00:16:36

Token Service Provider → MasterCard, Visa, RuPay
providing Token service to all merchants (Flipkart, Amazon)

Token Requestor → PG → Razorpay, PayU
who requests for a Token on behalf of consumer
Merchant can be a TR also, there are RBI guidelines who can be TR, who cannot be

Issuer → Bank who issues Tokens
→ Eg. SBI
SBI can also be TSP for all Tokens issued by SBI
→ i.e. All SBI card can be managed by SBI as a TSP

(PG)
TR → manages the Token life cycle
→ stores token at their end
→ hosts token Wallet at their end
→ maintains all the consumer card credentials
RBI → Guidelines who can be a TR → get a license

Merchant → only stores token Ref. # not stores Token

Small Merchants → store only Token Reference #

↓

with Token Ref #, they just knock the TR down to give a Token

TR only TSP to provide a Token

Token Life Cycle

- Maintain Token
- Creating Token credential
- Update Token when it expires
- Replenish a Token & associated Key

Token on Device → only on NFC enabled phone

can be done with Bluetooth ✗

→ [Samsung Pay already in / Jio Pay → Pilot project]

But it comes more power so No Samsung prefer it

→ [very famous in Singapore]

Card credential in device

↓

NFC to establish connection with POS or ATM

Register your credit card

is Google by Application with all details

Google Pay will use ID & V methods to verify your identity

Page No. 42
Date

#42

↓ after successful registration

Your Phone with 'Google Pay' becomes a physical card so the card becomes personalized in the mobile.

↓

which can be used on POS or ATM for Tx (Contact Tx)

↓

But your Device is in Non-Secure Zone

↓

So need for Tokenization the card before it is personalized in the mobile

Token Issuer will be about to know that the Tx is being done using Token or device not physical card,

↓ H/w is not a dedicated H/w.

Entire Token value can be copied / cloned by any hacker

↓ to secure it

White Box Cryptography to secure your data that is associated with a card

(very complicated to implement in Mobile)

Token Device can be divided into 2 implementation

Page No. #43
Date

HCE

Host card Emulation

It is based on White Box Cryptography

Secure Element

Creating your Secure Area on a particular H/W

Analogy

Room

Laptop on Table not safe

Room

Locker

Safe with Lock

ways to Implement

Embedded Secure Element

put additional H/W as a secure element in motherboard

dedicated H/W dedicated memory

UICC

By creating a dedicated H/W on SIM as Secure Element

on μSD Card

Secure Elem → Apple Pay
G Pay
Samsung Pay
Jio Pay

00:30:46

Registered your card in Mobile App

↓

Now your phone works like a physical card

↓ Exactly like

(Card Present TX)

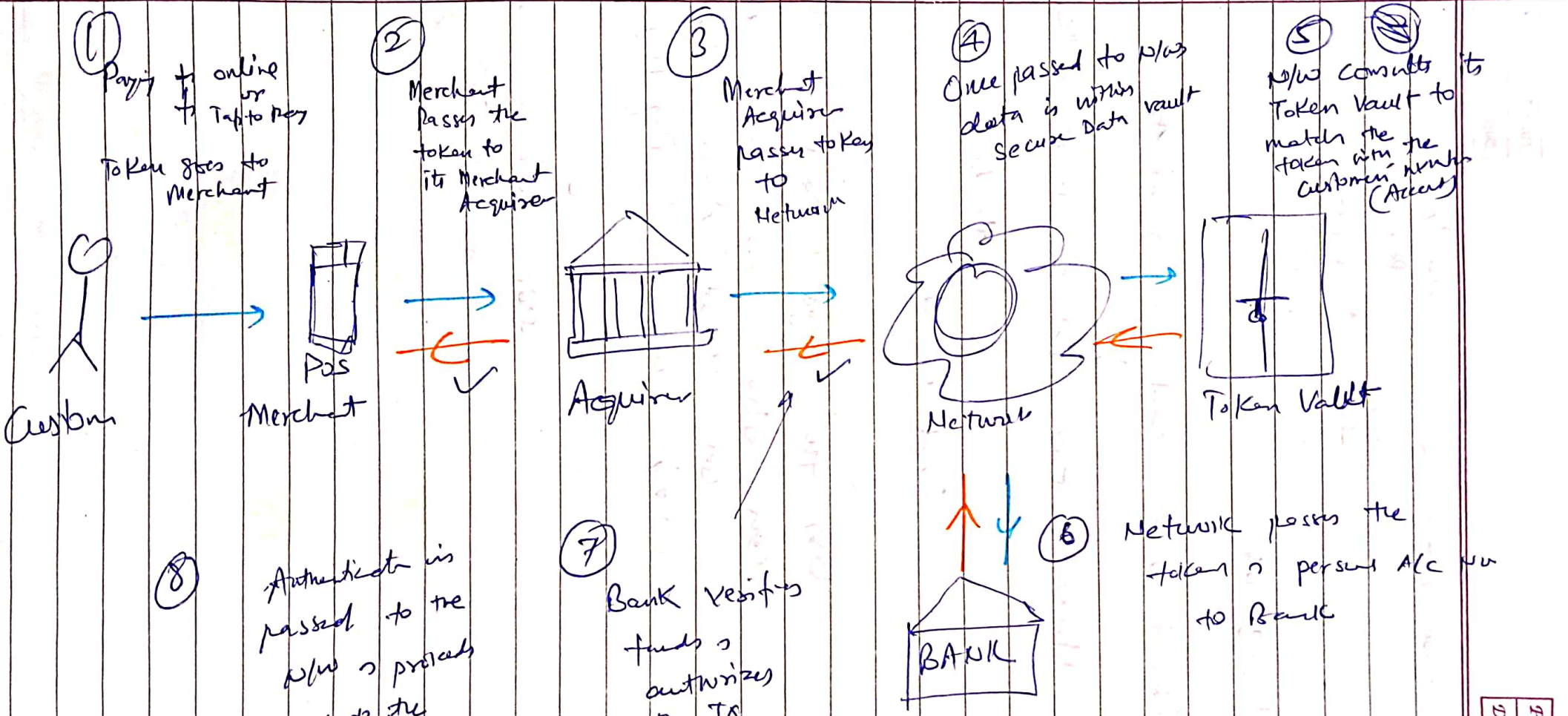
↓

Using this Registered card in M/App can also pay online eg on Flipcart / Amazon by choosing option "Pay Using Google Pay"

↓

this mode is called

In-App TX


1
Paying in online or Tap to Pay
Token goes to Merchant
2
Merchant Passes the token to its Merchant Acquirer
3
Merchant Acquirer passes token to Network
4
Once passed to N/w data is within secure Data vault
5
N/w consults its Token Vault to match the token with the customer number (Account)
Customer
POS
Merchant
Acquirer
Network
Token Vault
BANK
6
Network passes the token & personal A/C no to Bank
7
Bank verifies funds & authorizes the TX
8
Authentication is passed to the N/w & proceeds handle to the Merchant Acquirer & to Merchant

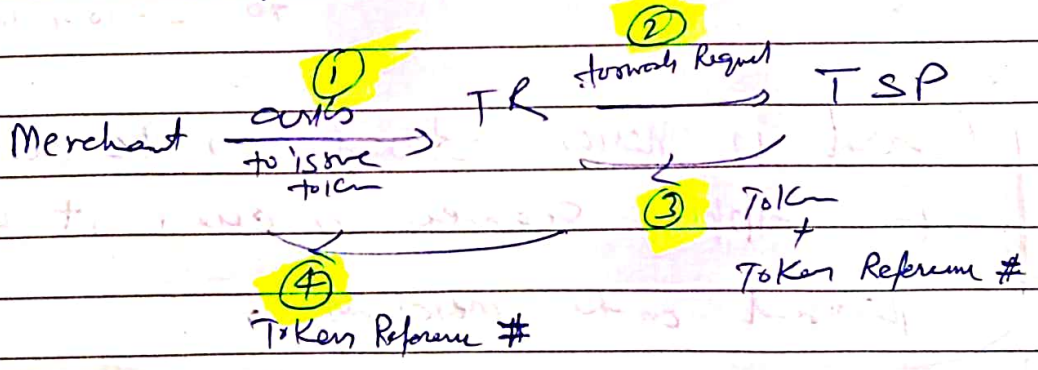
Card on File Tokenization

A card on file or stored credentials
= Card info is stored by a merchant, PG, Digital Wallet
to process future transactions

RBI Guidelines on Card on file

None of the merchant can store the real Card # at their end,
(1) It has to be tokenized
(2) out of 16 digit card #
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
these must be initial 4 or last 4 for customer to correlate.
(for selecting Card to Pay)

So only these 4 digits stored at merchant website, rest of the digits is tokenized form



Token Reference # = Unique for each Token
PAR = 1 - 1 Card

Apple Pay

Page No. 44
Date

* Pay on iPhone, iPad, Mac & Apple watches by adding preferred payment methods
  - credit card
  - debit card
* Contactless payment on POS or Online Payment
* Send money (with A/Pay, Apple cash) to other Apple users
* request money with A/Pay
* No need to enter card details everytime

Once you have added your Credit/Debit card to your wallet, you can use your phone for [TAP & PAY] by your Passcode or Biometrics to confirm the payment

Card is never stored on the device or on Apple server & even it is not passed on to merchant.

Apple Pay

At Client Side ⇒ native Apple Pay integration

(C) Adding Card to Apple Wallet

Manually using Apple Wallet UI

or

using Apps that can automatically add cards to iOS wallet (= PUSH Provisioning)

Both

Ensuring the protection of cardholder data

DPAN = Device PAN

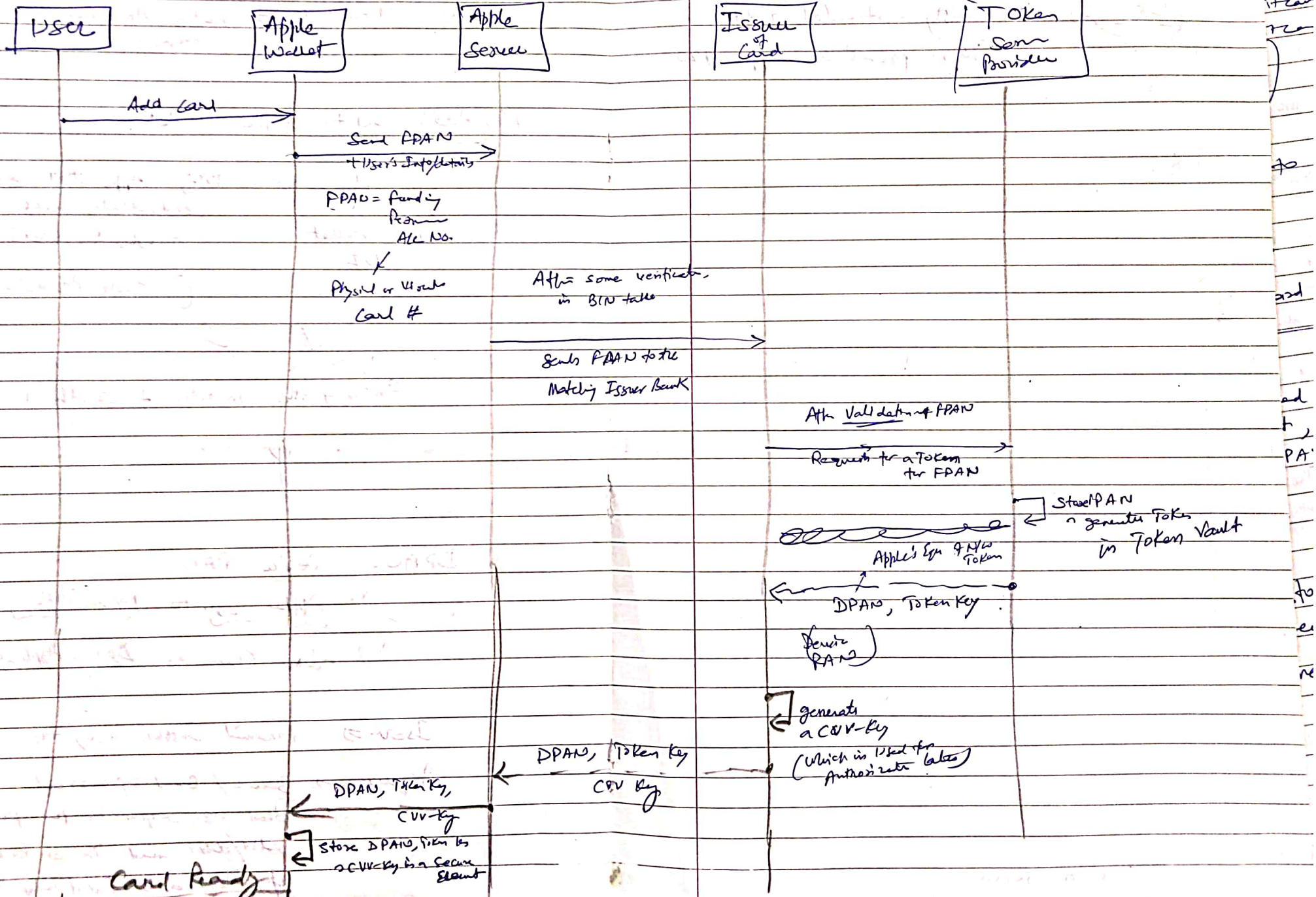
↳ Applies Eqn to N/W Token

↳ also known as PAN / Applicat PAN

Issuer ⇒ Financial Institution issuing the Card

Acquirer ⇒ Bank / Bank sponsored entity that is responsible for processing credit/debit card Tx on behalf of Merchants facilitating Bank of funds in Customer A/c to Merchant A/c

Add a Card to Apple Wallet

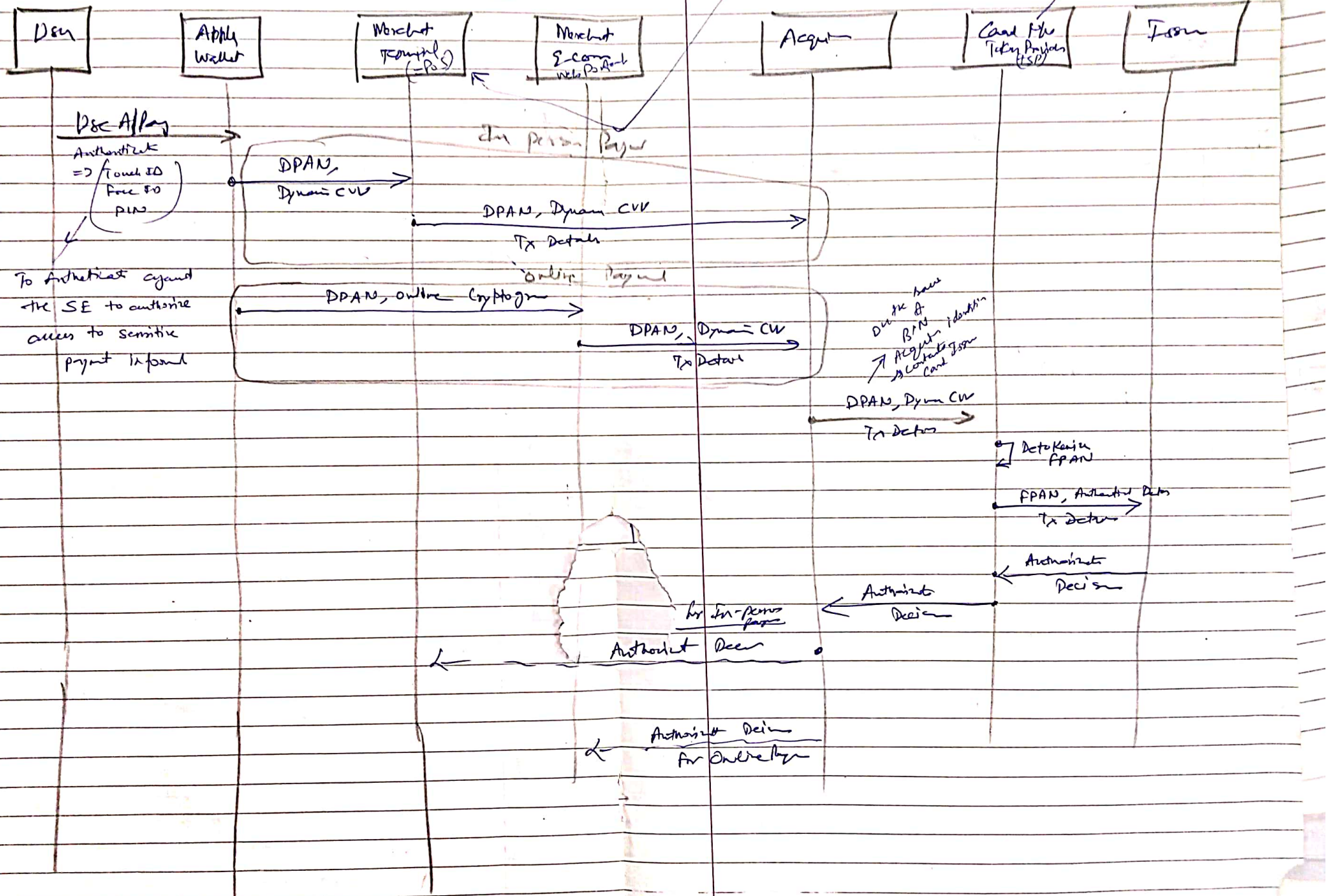


Page No.
Date

#51

SE :- Industry - standard certified
Chip present in Apple H/w

Using Apple Pay in Transactions



(1) OEM (Original Equipment Manufacturers) Wallet

↓ eg

Samsung Pay
Apple Pay
Google Pay

↙

Provide UIs to pay via → NFC (Tap & Go)
→ QR Code
→ In-App Payment

↙

One App to other App

~~In App Payment~~

(2) Issuer Wallet / Payment Apps

↓ ↘

Banks Apps → eg → YONO SBI, PAYZAPP (HDFC), pockets (ICICI)

Payment Service Provider → eg → PhonePe, Pay TM, MobiKwik, freecharge, Amazon Pay

Traditionally Bank provides an EMV Chip Card

What is a N/W Token

Surrogate value for Card #

Token # is just like a Card #

(BIN + Seq # + Check-Digit)

It offers no changes to acquiring infrastructure

Reversible + Non-cryptographic

One Card → Many Tokens

Stakeholders in Tokenization

TR (Token Requestor)

→ Authorized Entity to request Tokens

eCOM Website / App

→ Can be OEM / MNO payment wallet (Samsung Pay, Apple Pay, Google Pay)

→ Can be an Issuer wallet (~~Kotak~~ ~~SBI~~ provided by Kotak)

→ Typically a combination of End device and Wallet Secure

M/Card
Visa
Reply

Token Service Provider

Handles Token Request from TR

Controls Token Assurance Process
(How to Authicate End device)
(" " " Customer)

Issues Tokens

Maintain Token Vault
↳ It contains
Mapping bit
[Card # ↔ Token #]

Provisions EMV token profile

Handles Issuer Interface for
↳ IDnV
↳ Life Cycle Mgmt

Tx proceing

Token Assurance process of validating of a customer whether that customer is the rightful owner of Credit Card or not

#57

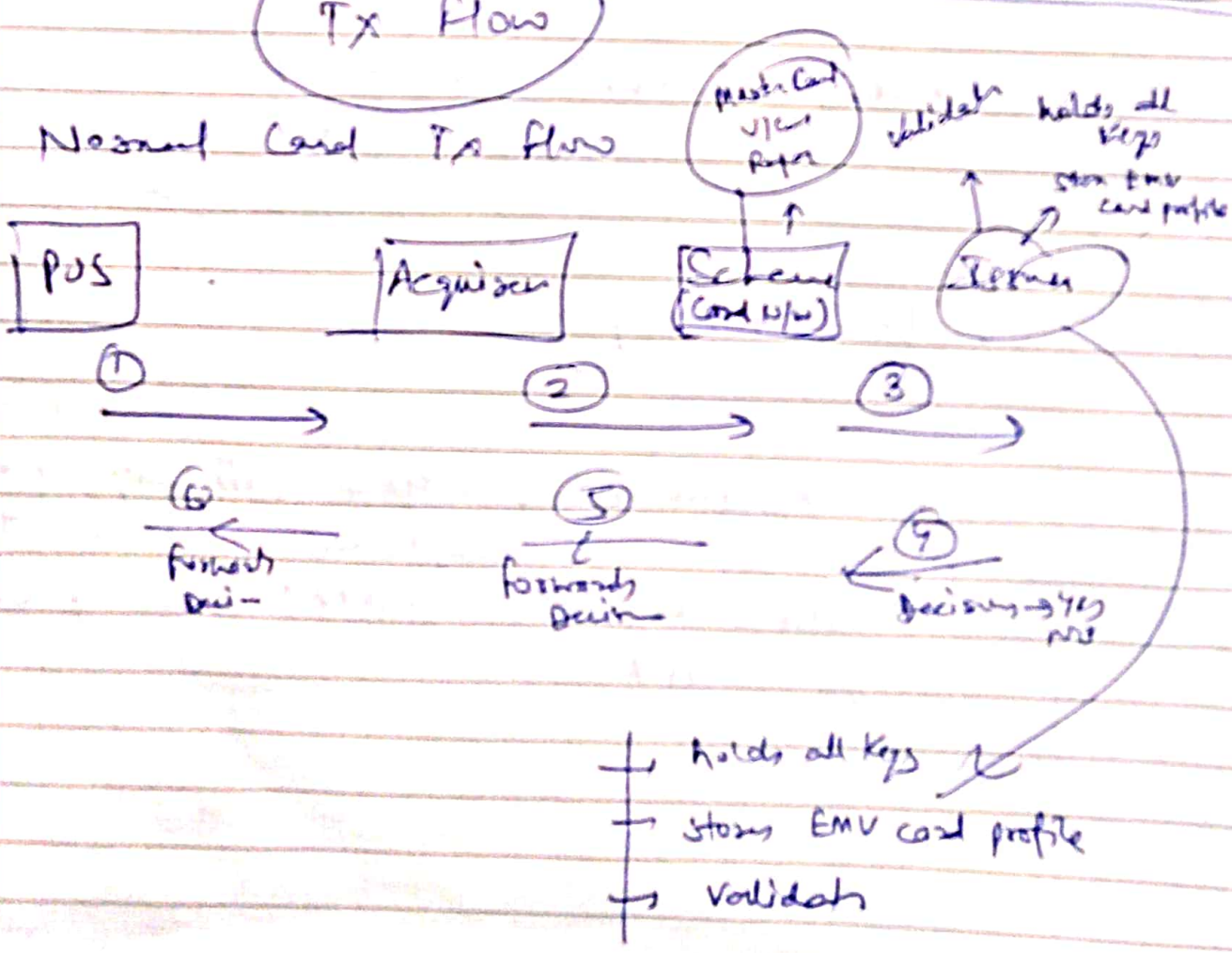
Token Creation: Process of generating a Token # and Token expiry date for a given PAN #

Token Issuance: process of generating all associated data for a Token + personalized data including keys (e.g. EMV Data)

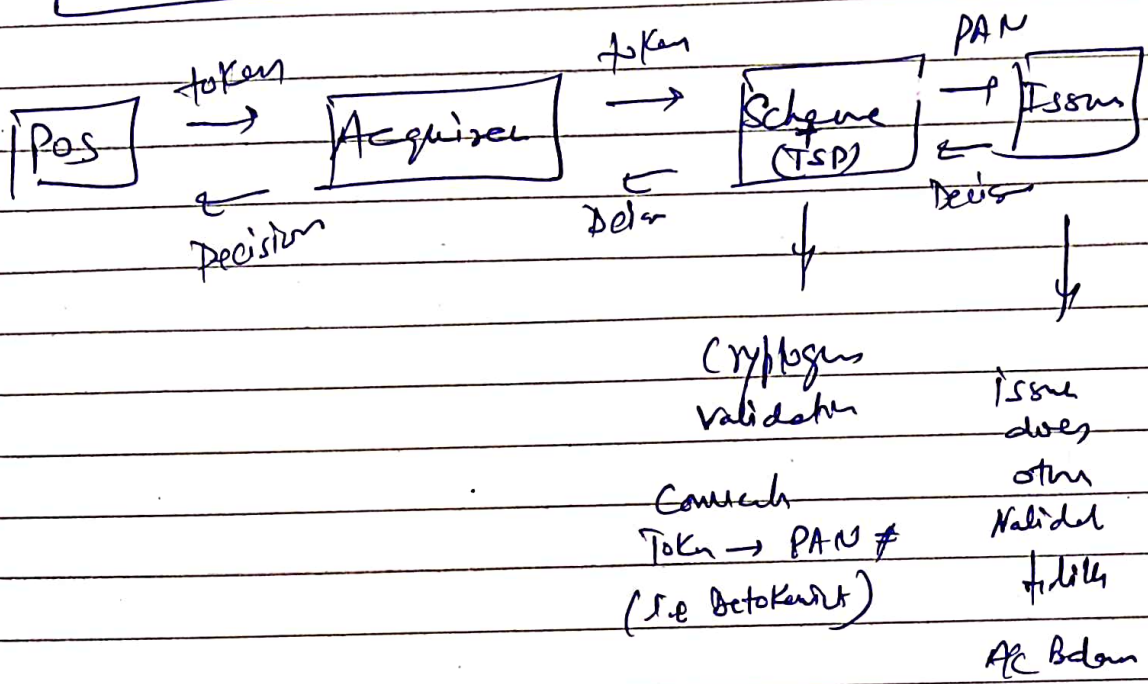
Token Provisioning: Process of delivering Token and associated data to the Token location i.e. Mobile Payment Application

Tx Flow

Normal Card Tx flow



Tokenization Based Tx Flow



Token Issuance