सी डैक
CDAC

Information Security Education & Awareness Team

C-DAC Bengaluru

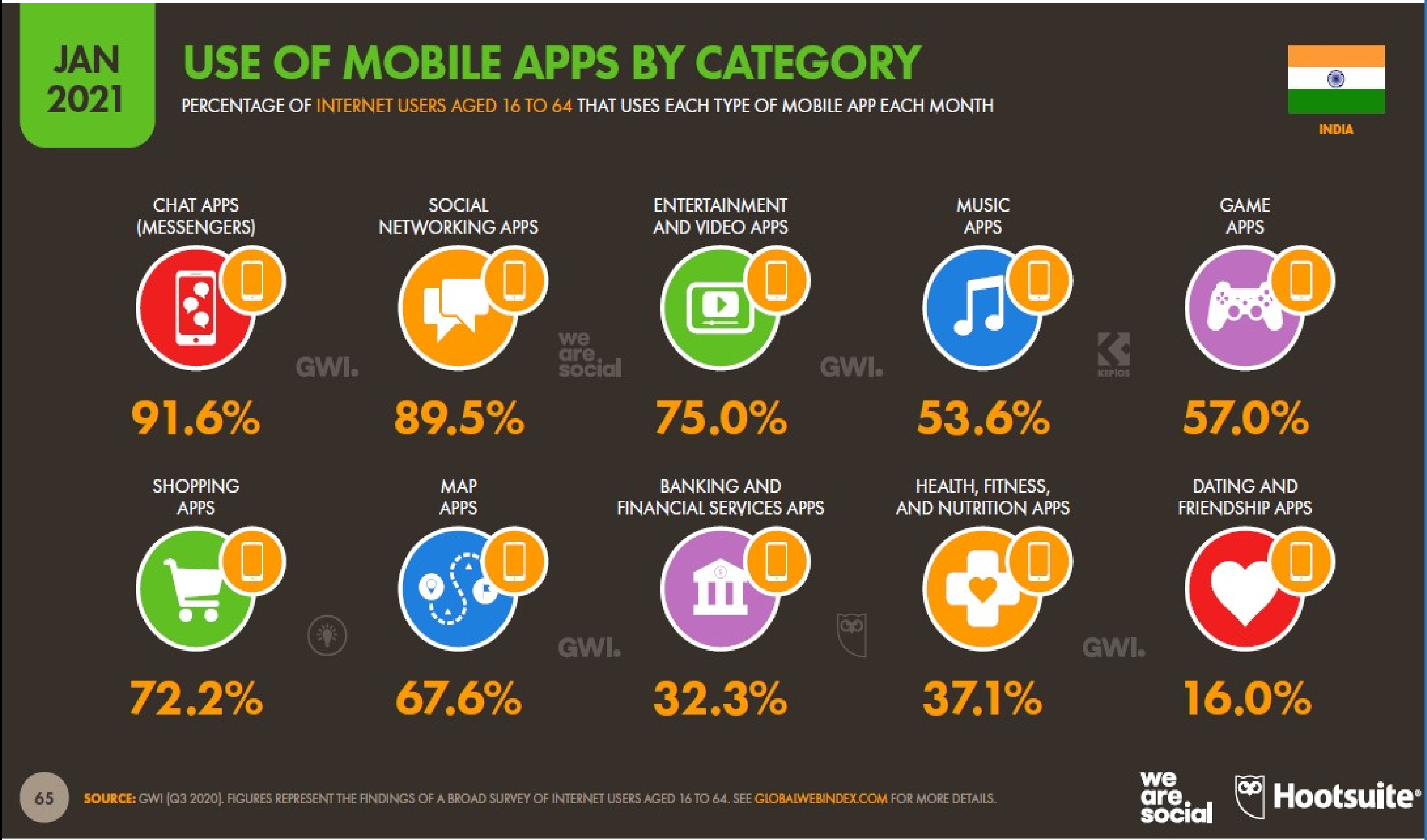
www.InfoSecawareness.in

ISEA

Online Financial Transactions: A Security Perspective

Dr. Mohammed Misbahuddin
B.E., M.Tech, PhD
Associate Director & Head
ACTS & BD
C-DAC Bangaluru

www.infosecawareness.in



JAN 2021

USE OF MOBILE APPS BY CATEGORY

PERCENTAGE OF INTERNET USERS AGED 16 TO 64 THAT USES EACH TYPE OF MOBILE APP EACH MONTH

INDIA

CHAT APPS (MESSENGERS)
91.6%

SOCIAL NETWORKING APPS
89.5%

ENTERTAINMENT AND VIDEO APPS
75.0%

MUSIC APPS
53.6%

GAME APPS
57.0%

SHOPPING APPS
72.2%

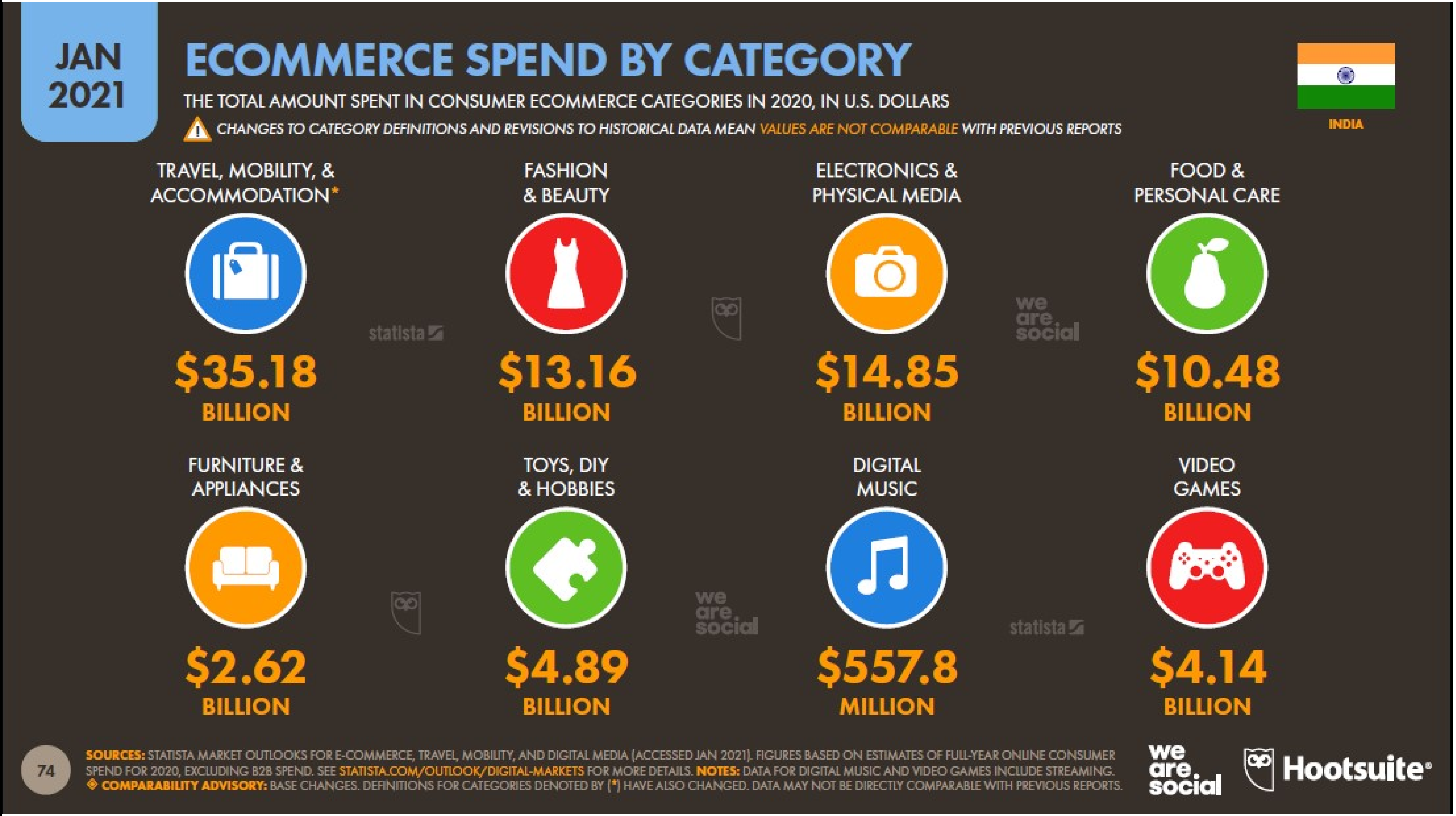
MAP APPS
67.6%

BANKING AND FINANCIAL SERVICES APPS
32.3%

HEALTH, FITNESS, AND NUTRITION APPS
37.1%

DATING AND FRIENDSHIP APPS
16.0%

SOURCE: GWI (Q3 2020). FIGURES REPRESENT THE FINDINGS OF A BROAD SURVEY OF INTERNET USERS AGED 16 TO 64. SEE GLOBALWEBINDEX.COM FOR MORE DETAILS.



JAN 2021

ECOMMERCE SPEND BY CATEGORY

THE TOTAL AMOUNT SPENT IN CONSUMER ECOMMERCE CATEGORIES IN 2020, IN U.S. DOLLARS

⚠ *CHANGES TO CATEGORY DEFINITIONS AND REVISIONS TO HISTORICAL DATA MEAN VALUES ARE NOT COMPARABLE WITH PREVIOUS REPORTS*

INDIA

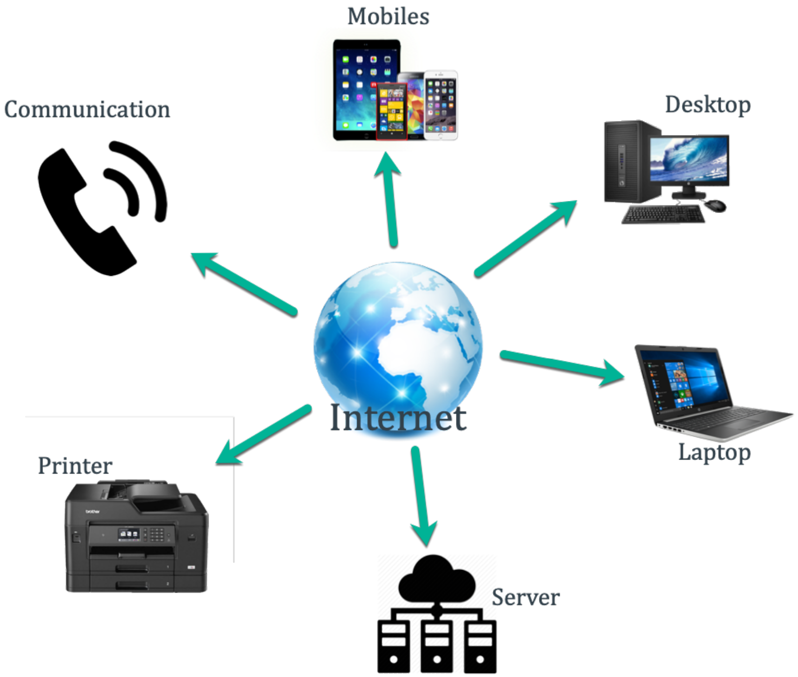
TRAVEL, MOBILITY, & ACCOMMODATION*	FASHION & BEAUTY	ELECTRONICS & PHYSICAL MEDIA	FOOD & PERSONAL CARE
$35.18 BILLION	$13.16 BILLION	$14.85 BILLION	$10.48 BILLION

FURNITURE & APPLIANCES	TOYS, DIY & HOBBIES	DIGITAL MUSIC	VIDEO GAMES
$2.62 BILLION	$4.89 BILLION	$557.8 MILLION	$4.14 BILLION

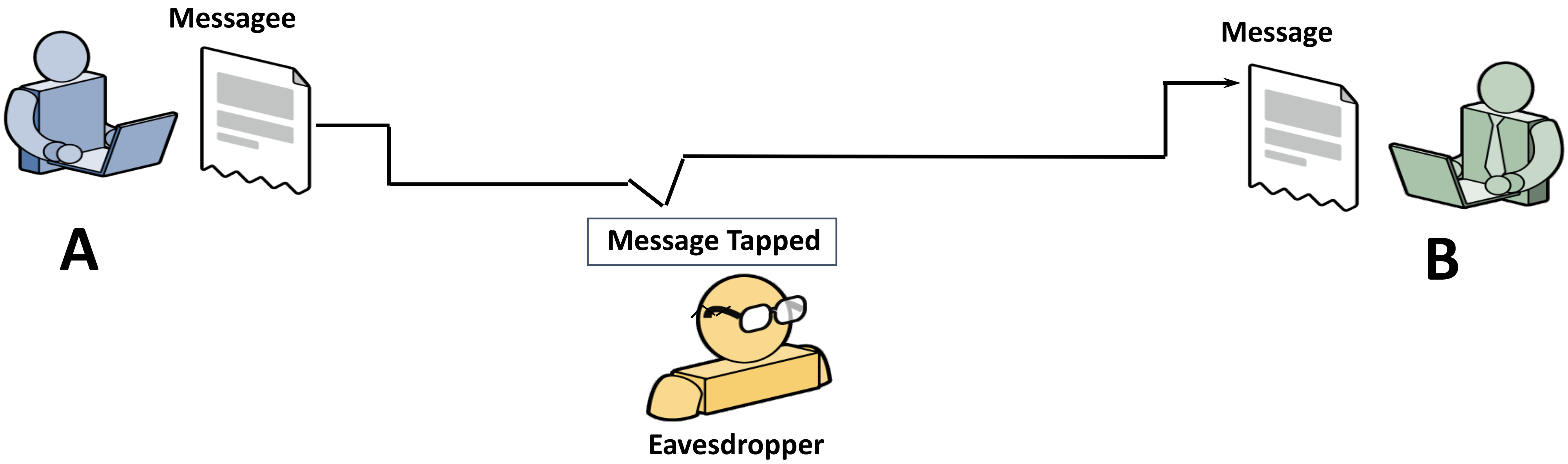
SOURCES: STATISTA MARKET OUTLOOKS FOR E-COMMERCE, TRAVEL, MOBILITY, AND DIGITAL MEDIA (ACCESSED JAN 2021). FIGURES BASED ON ESTIMATES OF FULL-YEAR ONLINE CONSUMER SPEND FOR 2020, EXCLUDING B2B SPEND. SEE STATISTA.COM/OUTLOOK/DIGITAL-MARKETS FOR MORE DETAILS. **NOTES:** DATA FOR DIGITAL MUSIC AND VIDEO GAMES INCLUDE STREAMING. ◈ **COMPARABILITY ADVISORY:** BASE CHANGES. DEFINITIONS FOR CATEGORIES DENOTED BY (*) HAVE ALSO CHANGED. DATA MAY NOT BE DIRECTLY COMPARABLE WITH PREVIOUS REPORTS.

www.InfoSecawareness.in

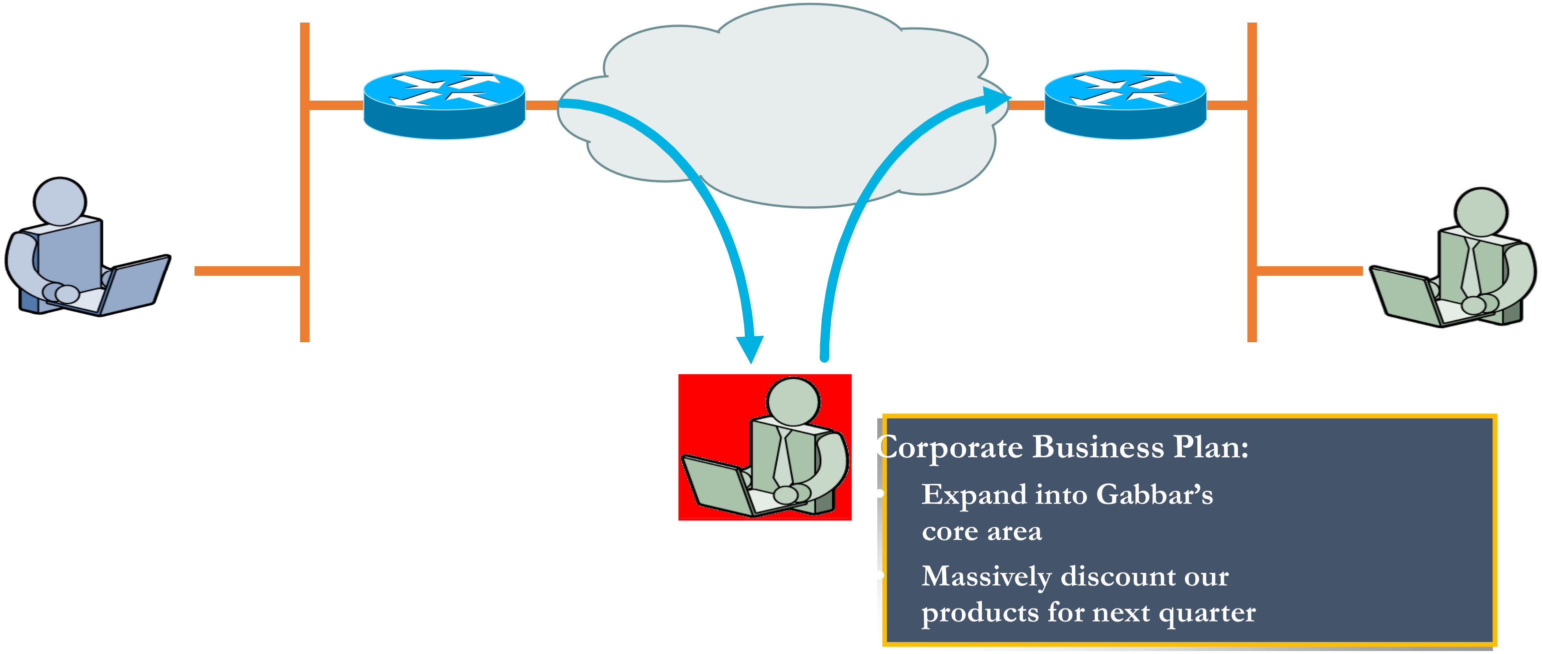
Internet


Mobiles
Communication
Desktop
Internet
Laptop
Printer
Server

Attacks on Confidentiality / Secrecy – Packet Sniffing



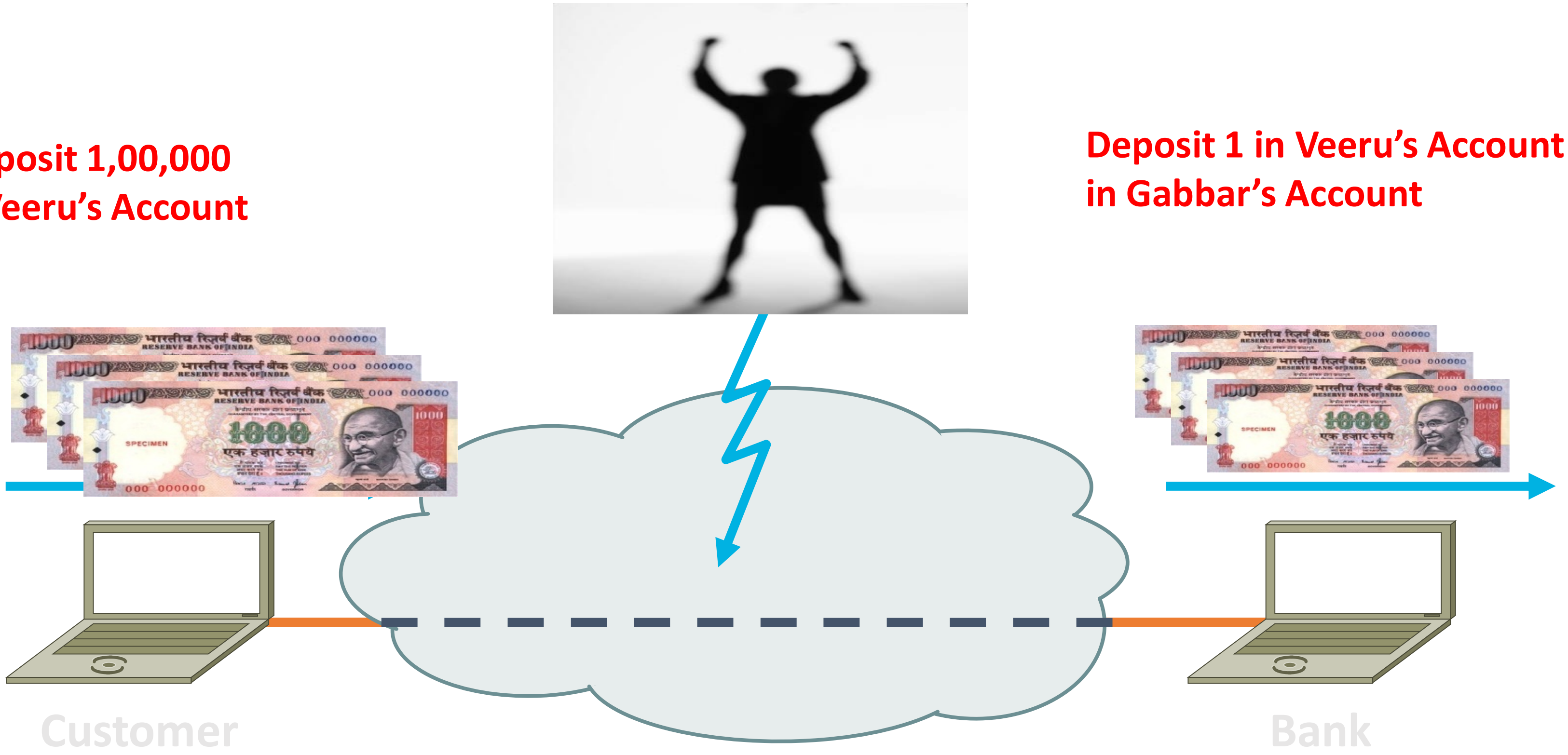
Attacks on Confidentiality / Secrecy – Data Theft



Corporate Business Plan:

- Expand into Gabbar’s core area
- Massively discount our products for next quarter

Attacks on Integrity – Data Alteration

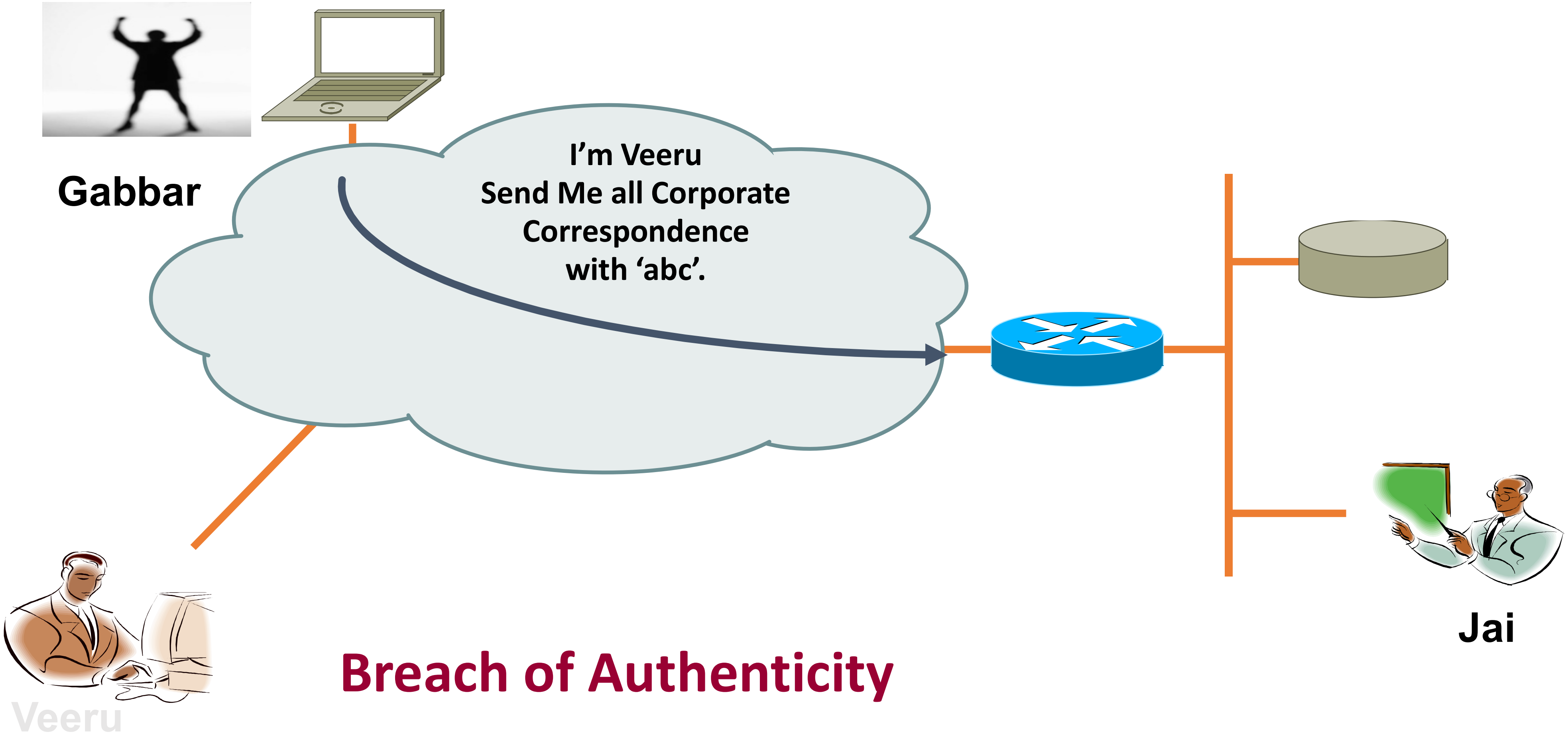


**Deposit 1,00,000
in Veeru's Account**

**Deposit 1 in Veeru's Account and 99,999
in Gabbar's Account**

Breach of Integrity

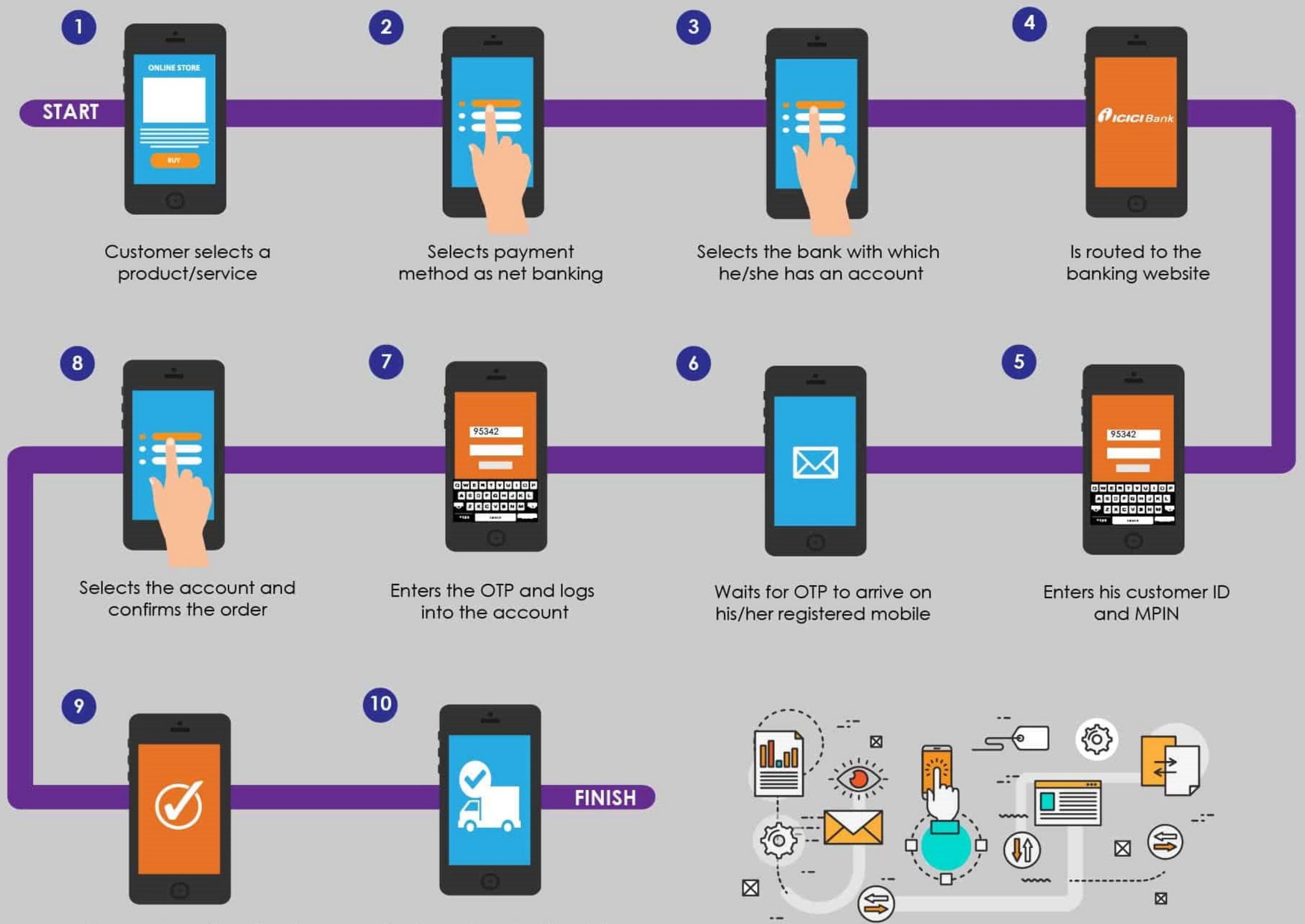
Attacks on Authenticity - Spoofing



Breach of Authenticity

Electronic World

Internet Banking



1 Customer selects a product/service

2 Selects payment method as net banking

3 Selects the bank with which he/she has an account

4 Is routed to the banking website

5 Enters his customer ID and MPIN

6 Waits for OTP to arrive on his/her registered mobile

7 Enters the OTP and logs into the account

8 Selects the account and confirms the order

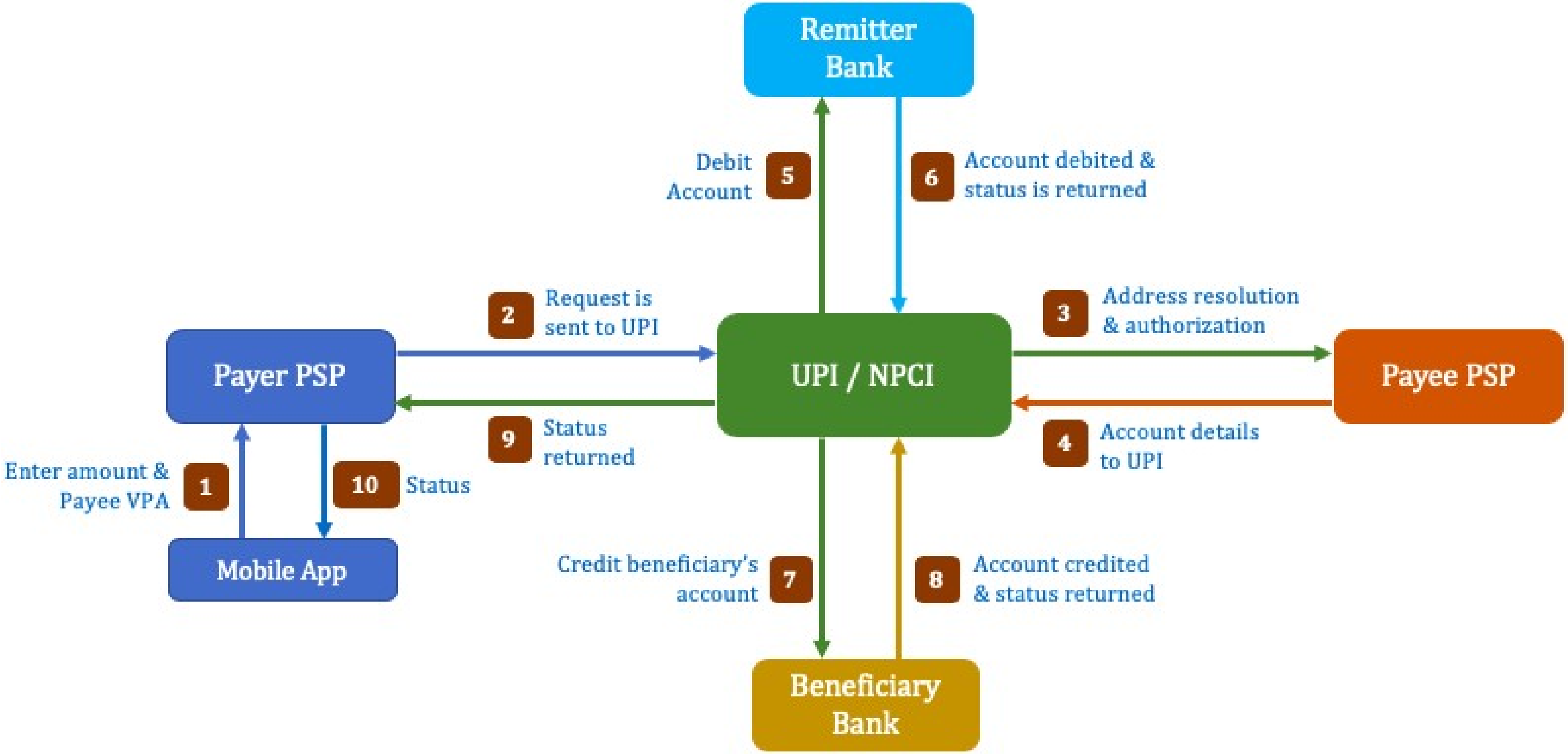
9 Payment confirmation / rejection message received

10 Customer is routed back to e-commerce site

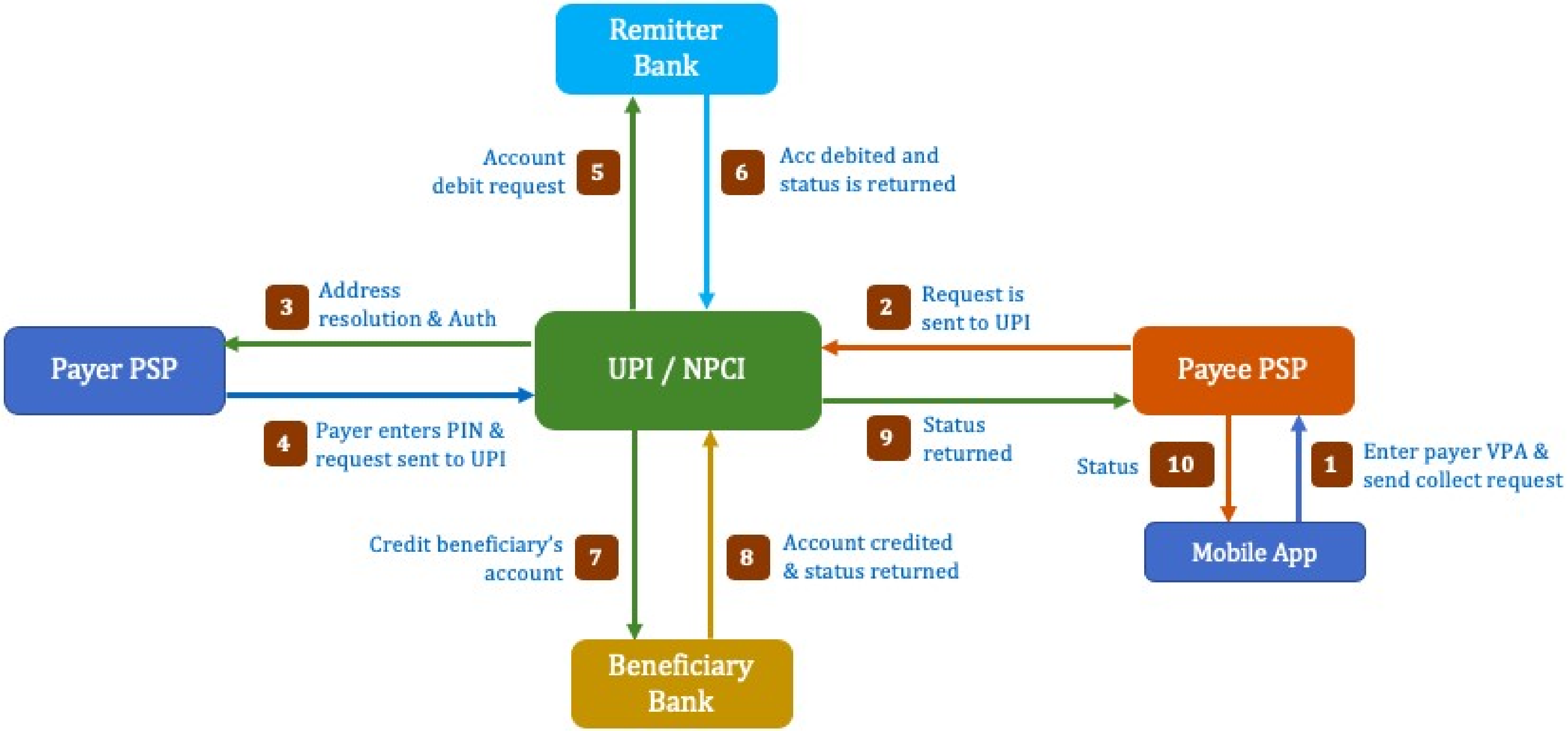
DIGITAL UNCOVERED

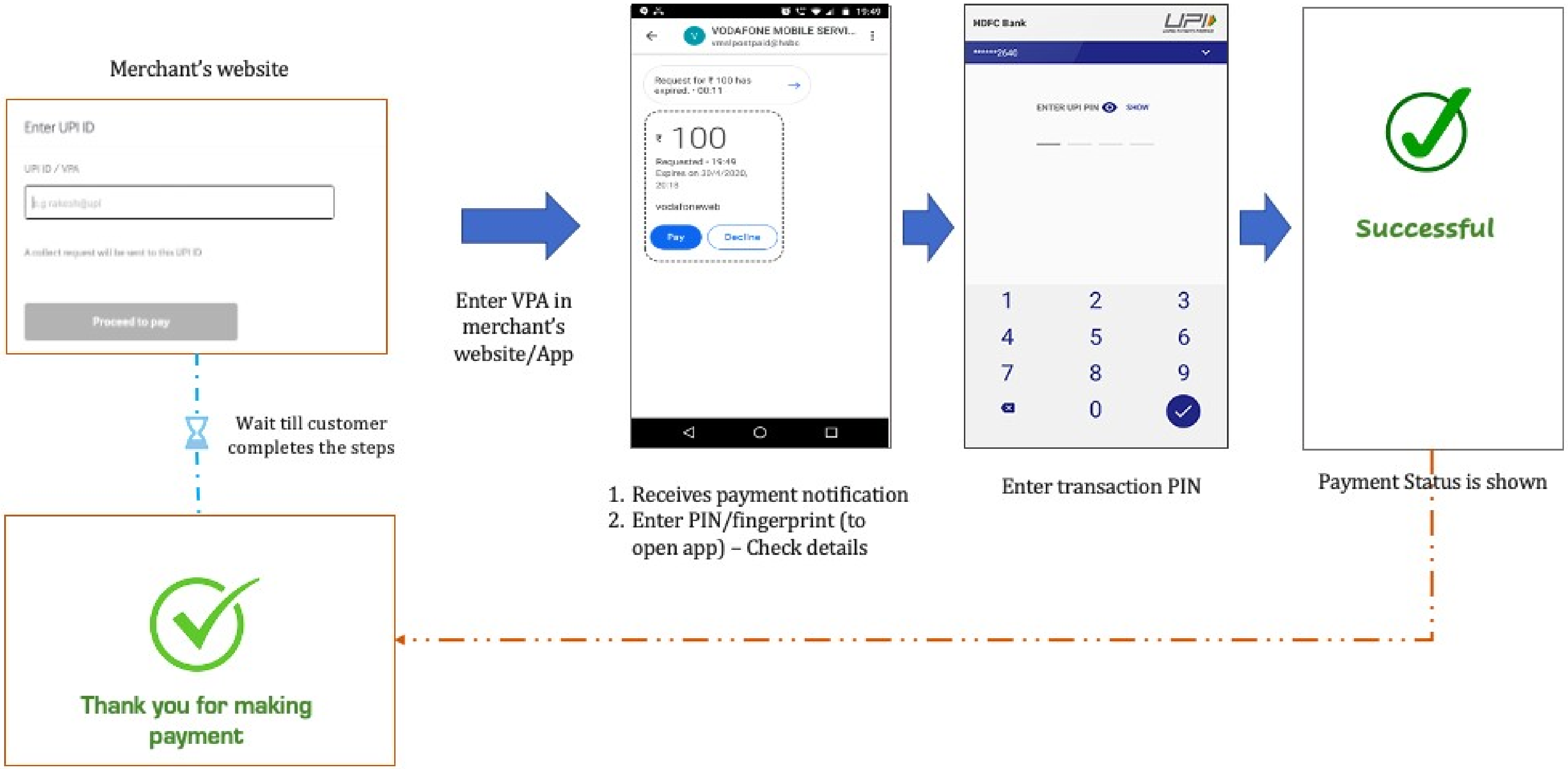
Unified Payment Interface

Payer Initiated P2P Transfer (Push Payment)



Payee Initiated P2P Transfer (Pull Payment)


Remitter Bank
Account debit request
5
6
Acc debited and status is returned
3
Address resolution & Auth
2
Request is sent to UPI
Payer PSP
UPI / NPCI
Payee PSP
4
Payer enters PIN & request sent to UPI
9
Status returned
Status
10
1
Enter payer VPA & send collect request
Credit beneficiary's account
7
8
Account credited & status returned
Mobile App
Beneficiary Bank



Merchant's website

Enter UPI ID

UPI ID / VPA

e.g rakesh@upi

A collect request will be sent to this UPI ID

Enter VPA in merchant's website/App

Wait till customer completes the steps

Request for ₹ 100 has expired. · 00:11

₹ 100

Requested · 19:49
Expires on 30/1/2020, 20:18

vodafoneweb

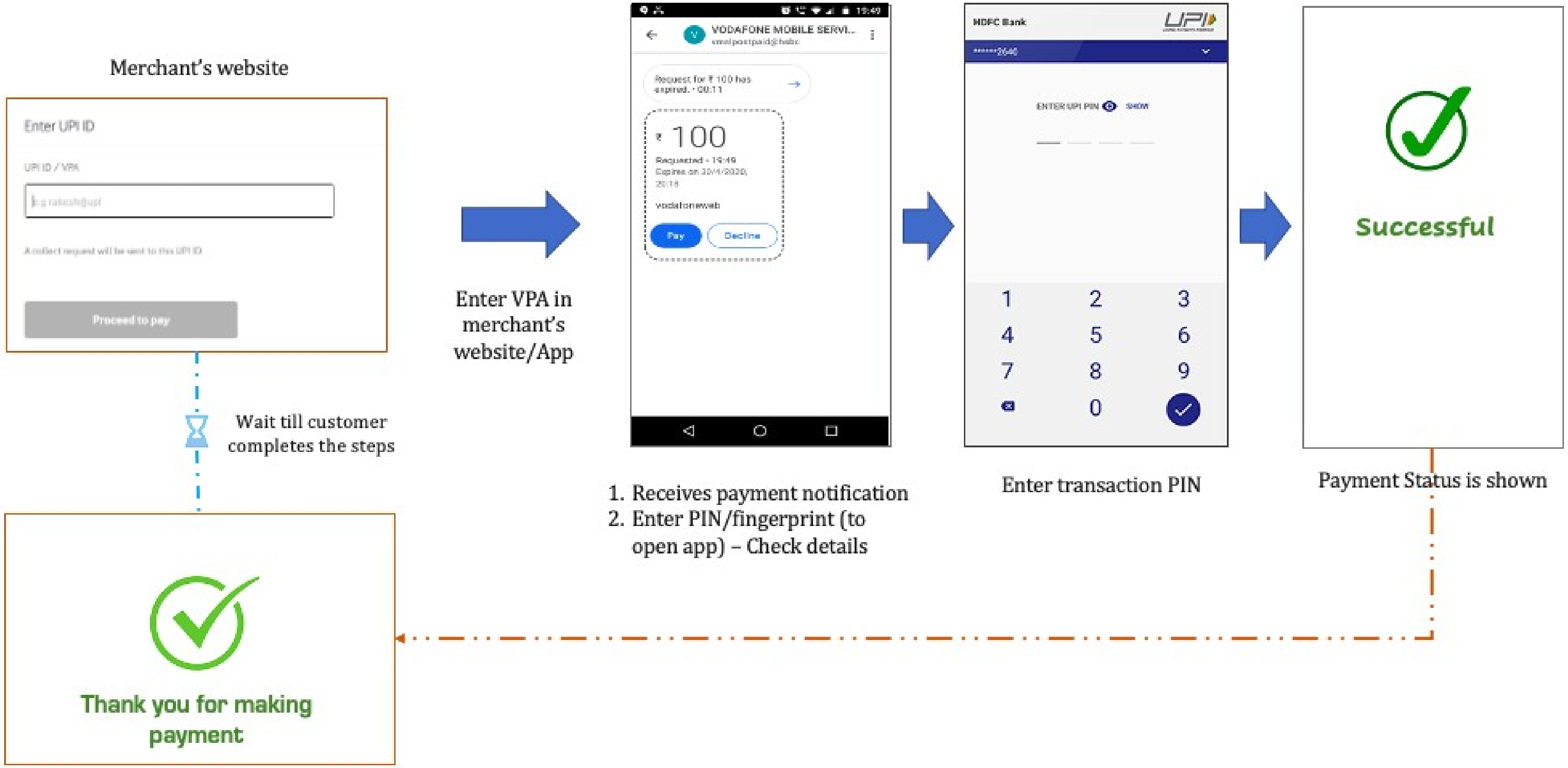
1. Receives payment notification
2. Enter PIN/fingerprint (to open app) – Check details

Enter transaction PIN

Successful

Payment Status is shown

Thank you for making payment



Merchant's website

Enter UPI ID

UPI ID / VPA

e.g rakesh@upi

A collect request will be sent to this UPI ID

Proceed to pay

Wait till customer completes the steps

Enter VPA in merchant's website/App

19:49

VODAFONE MOBILE SERVI...
vmsl postpaid@hdfc

Request for ₹ 100 has expired. · 00:11

₹ 100

Requested · 19:49
Expires on 30/4/2020, 20:18

vodafoneweb

Pay Decline

1. Receives payment notification
2. Enter PIN/fingerprint (to open app) – Check details

HDFC Bank

******2646

ENTER UPI PIN SHOW

Enter transaction PIN

Successful

Payment Status is shown

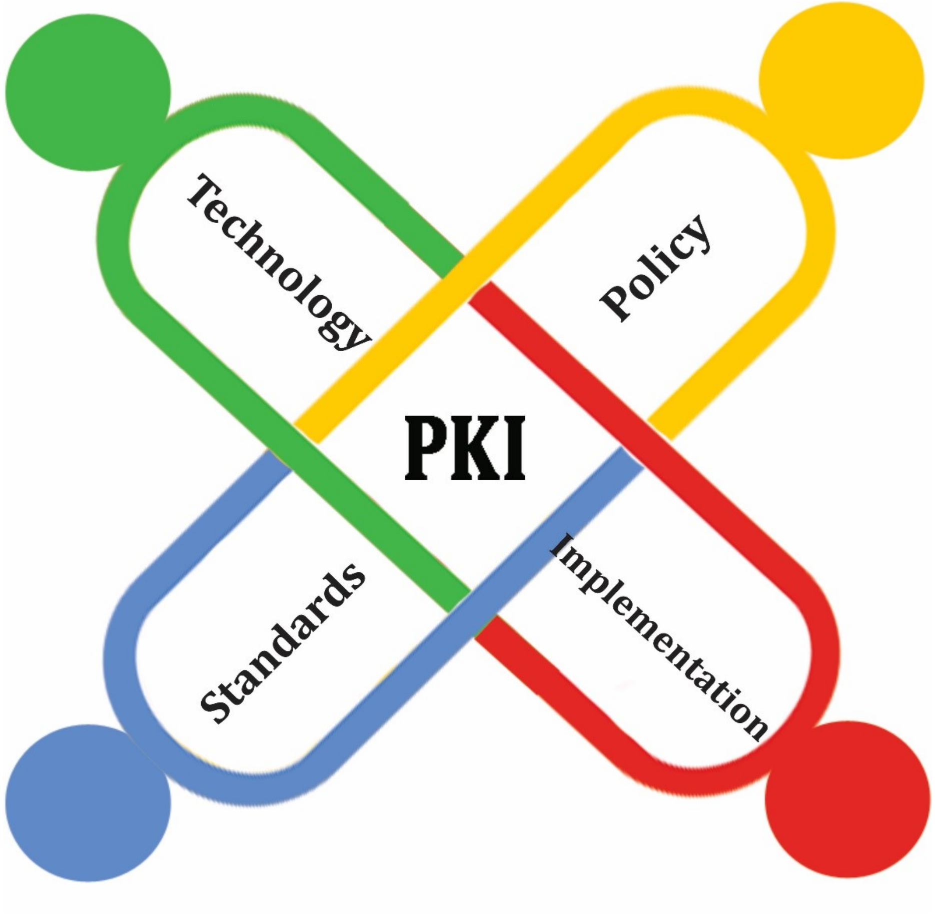
Thank you for making payment

Basic Elements of Trust

- **Privacy (Confidentiality):** Ensuring that **only authorized** persons read the Data/Message/Document
- **Authenticity:** Ensuring that Data/Message/Document originated from the **claimed** signer / sender
- **Integrity** : Ensuring that Data/Message/Document are **unaltered** by any unauthorized person
- **Non-Repudiation:** Ensuring that one **cannot deny** their signature or origination of a message

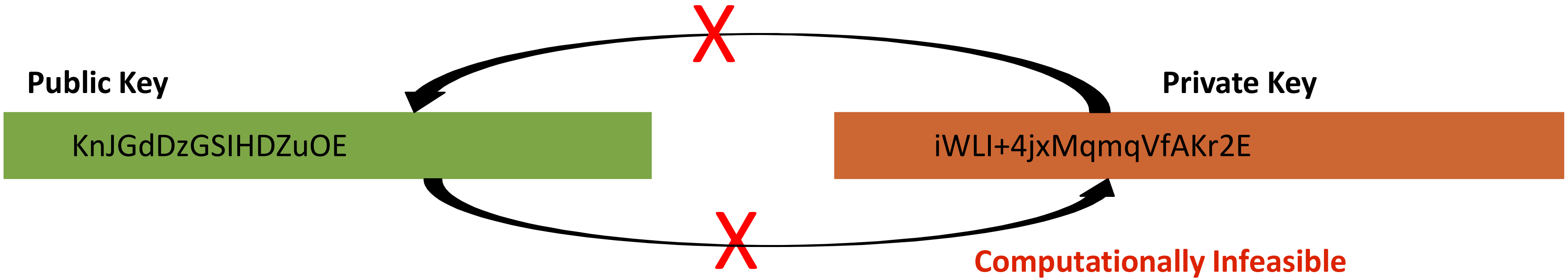
Backbone of
Trust in e-Transactions

PKI Ecosystem of Trust



Asymmetric Key Cryptography

- Also known as **Public Key Cryptography**
- Knowledge of the ***encryption key*** doesn't give you knowledge of the ***decryption key***



Computationally Infeasible

What is a key pair?

Private Key

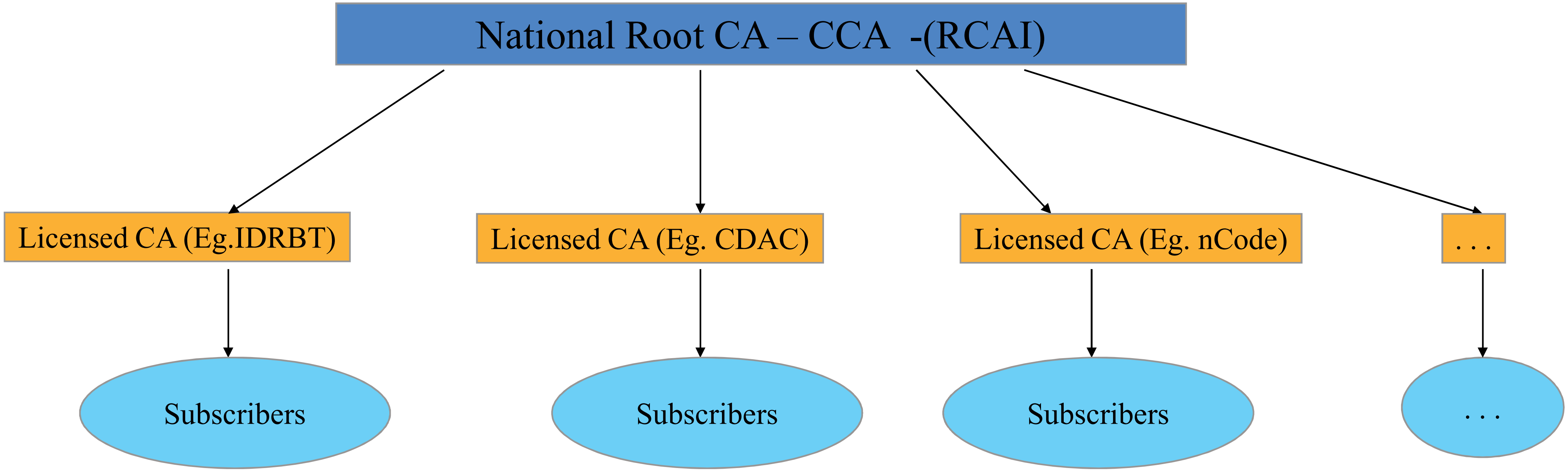
```
3082 010a 0282 0101 00b1 d311 e079 5543 0708 4ccb 0542 00e2 0d83 463d
e493 bab6 06d3 0d59 bd3e c1ce 4367 018a 21a8 efbc ccd0 a2cc b055 9653
8466 0500 da44 4980 d854 0aa5 2586 94ed 6356 ff70 6ca3 a119 d278 be68
2a44 5e2f cfcc 185e 47bc 3ab1 463d 1ef0 b92c 345f 8c7c 4c08 299d 4055
eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd
e6b7 a991 942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b2f0 1cd5 5ffb
6bed 6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16 6c89 2aca
da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629 4c2a d02a 63d1 6559
b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a 54fb ff78 41bc bd71 28f4 bb90
bcff 9634 04e3 459e a146 2840 8102 0301 0001
```

Public Key

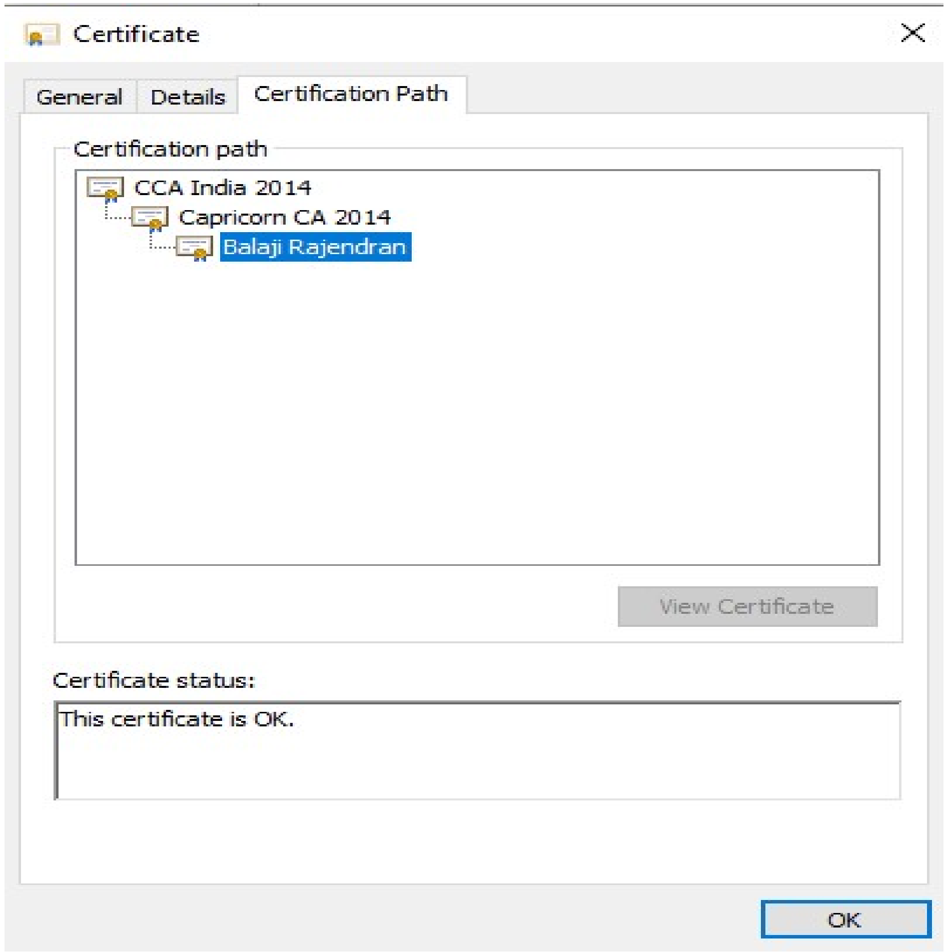
```
3082 01e4 f267 0142 0f61 dd12 e089 5547 0f08 4ccb 0542 00e2 0d83 463d e493
bab6 0673 0d59 bf3e c1ce 4367 012a 11a8 efbc ccd0 a2cc b055 9653 8466 0500
da44 4980 d8b4 0aa5 2586 94ed 6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc
185e 47bc 3ab1 463d 1df0 b92c 345f 8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7
8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd e6b7 a991 942c e478 4824
1a25 193a eb95 9c39 0a8a cf42 b250 1cd5 5ffb 6bed 6856 7b39 2c72 38b0 ee93
a9d3 7b77 3ceb 7103 a938 4a16 6c89 2aca da33 1379 c255 8ced 9cbb f2cb 5b10
f82e 6135 c629 4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a
54fb ff78 41bc bd71 28f4 bb90 bcff 9634 04de 45de af46 2240 8410 02f1 0001
```

Hierarchical Trust Model

- For a Digital Signature to have legal validity in **India**, it must derive its trust from the Root CA certificate



Certificate Chain & Trust Hierarchy



Certification path

- CCA India 2014
  - Capricorn CA 2014
    - Balaji Rajendran

Certificate status:

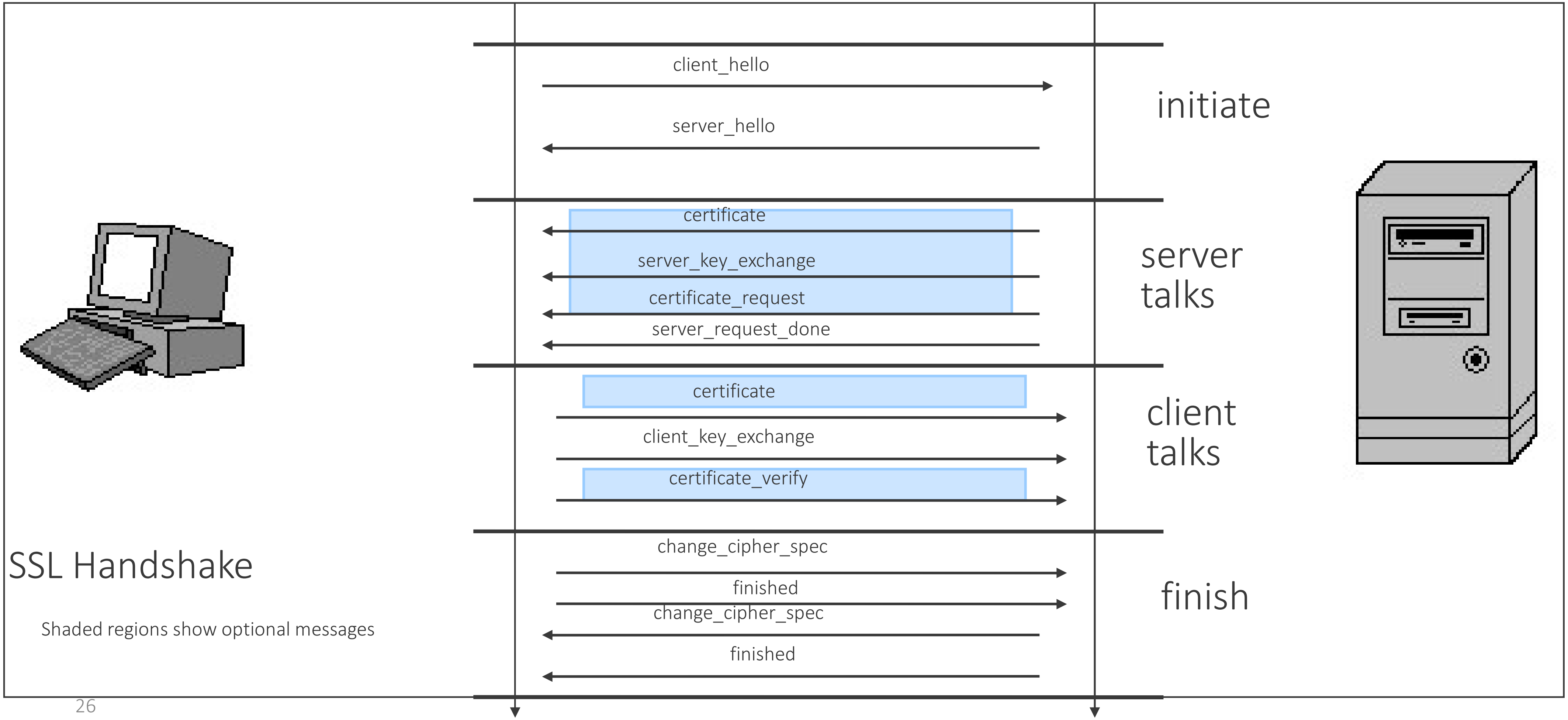
This certificate is OK.

Types of Certificates

Types of Certificates

- Signing Certificate (**DSC**)
  - Issued to a person for signing of electronic documents
- Encryption Certificate
  - Issued to a person for the purpose of Encryption;
- SSL/TLS Certificate
  - Issued to a Internet domain name (Web Servers, Email Servers etc…)

SSL/TLS Handshake Protocol



client_hello

server_hello

initiate

certificate

server_key_exchange

certificate_request

server_request_done

server talks

certificate

client_key_exchange

certificate_verify

client talks

change_cipher_spec

finished

change_cipher_spec

finished

finish

SSL Handshake

Shaded regions show optional messages

DEMO

Thank You