CSC-370
E - Commerce
(BSc CSIT, TU)

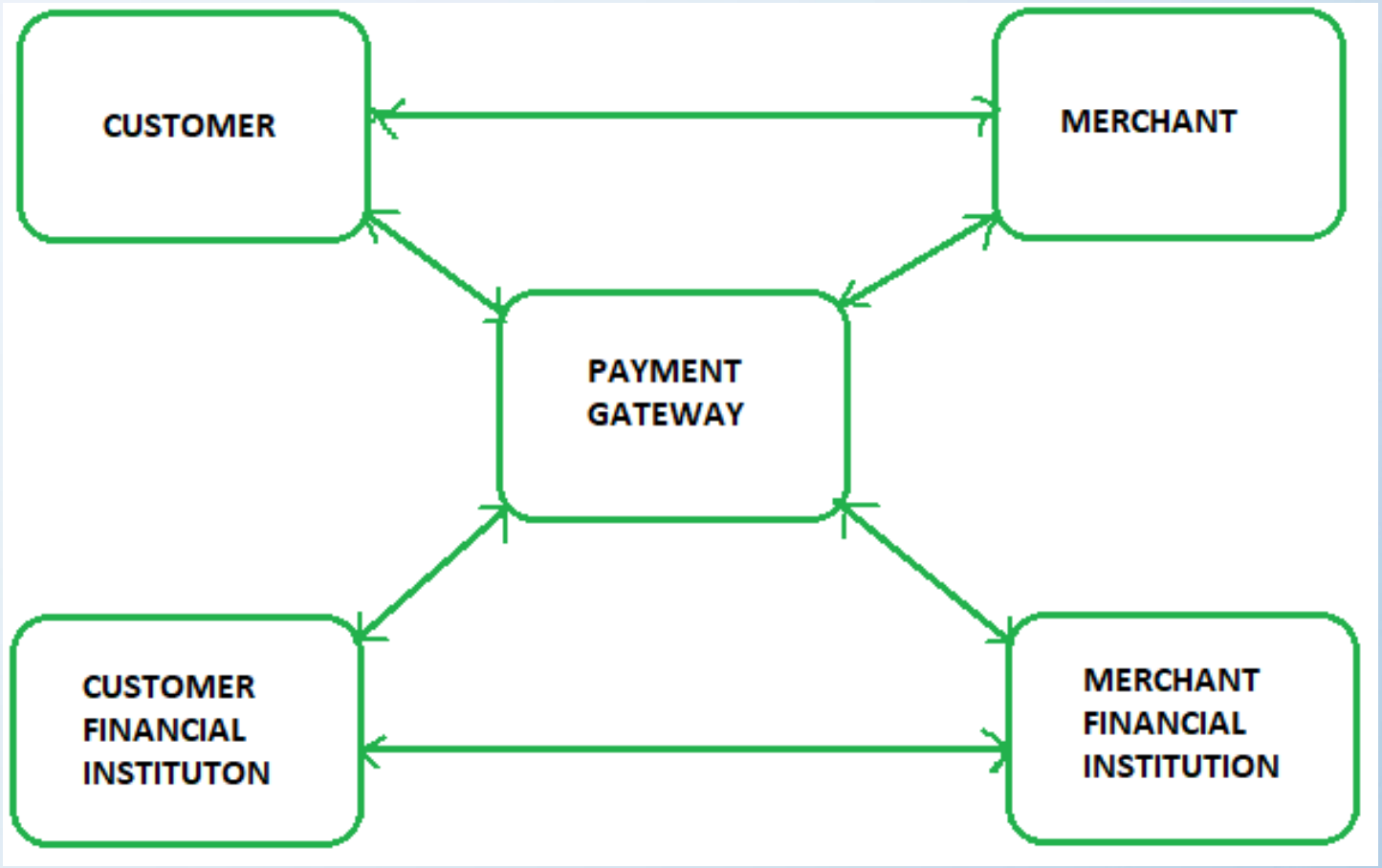
Ganesh Khatri
kh6ganesh@gmail.com

Secure Electronic Transaction(SET)

- Secure electronic transaction (SET) was an early communications protocol used by e-commerce websites to secure electronic debit and credit card payments
- SET was used to facilitate the secure transmission of consumer card information via electronic portals on the Internet. SET protocols were responsible for blocking out the personal details of card information, thus preventing merchants, hackers, and electronic thieves from accessing consumer information
- Secure electronic transaction protocols allowed merchants to verify their customers' card information without actually seeing it, thus protecting the customer against account theft, hacking, and other criminal actions

SET Participants

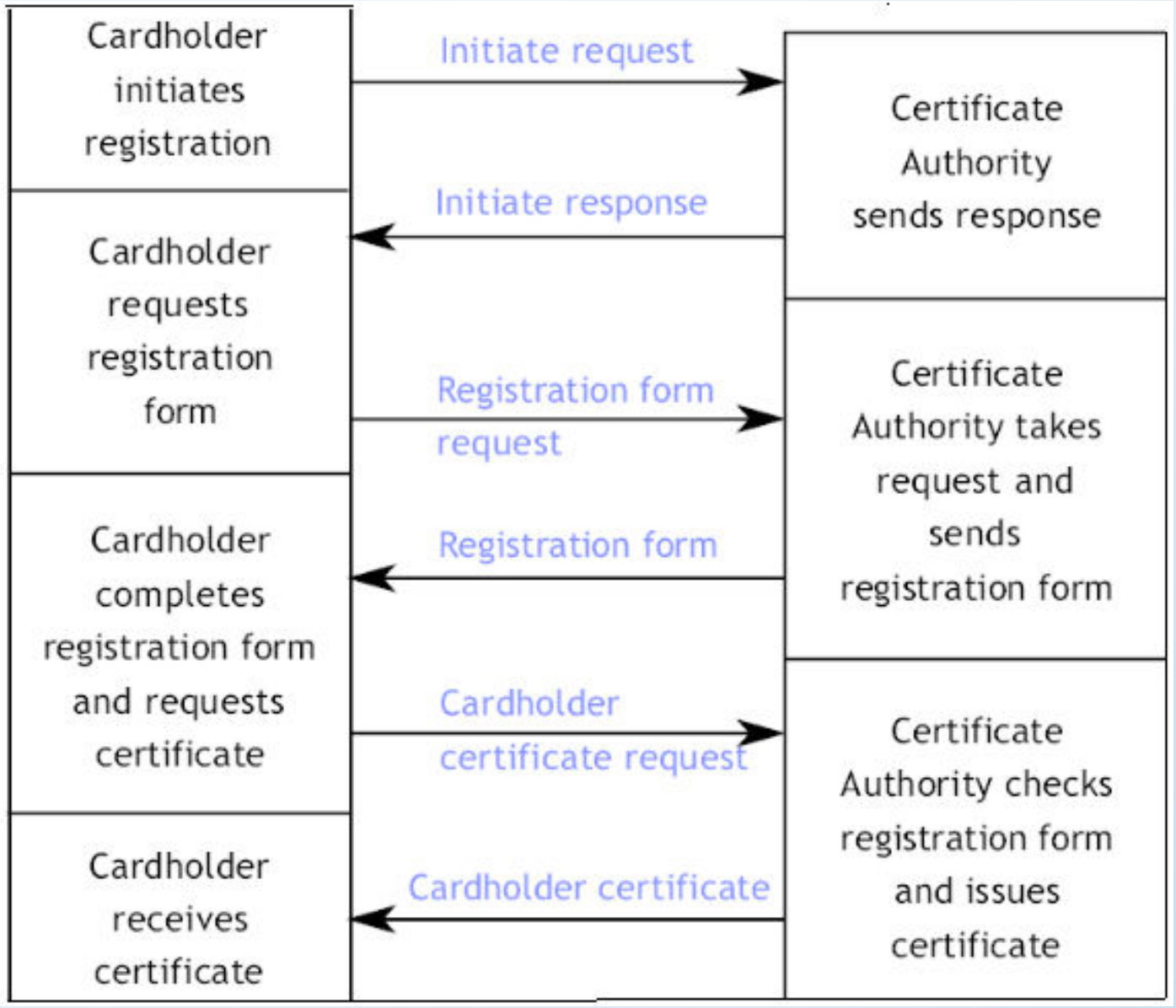
- Cardholder - customer
- Issuer - customer financial institution
- Merchant
- Acquirer - Merchant financial Institution
- Certificate authority - Authority which follows certain standards and issues certificates(like X.509V3) to all other participants
- Payment Gateway



SET functionalities / Features

- Provide Authentication
  - **Merchant Authentication :** To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.
  - **Customer / Cardholder Authentication :** SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates
- **Provide Message Confidentiality :** Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES(Data Encryption Standard) is used for encryption purpose
- **Provide Message Integrity :** SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1

Card Holder Registration in SET



Dual Signature in SET

- The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers
  - order Information (OI) for merchant
  - Payment Information (PI) for bank
- You might think sending them separately is an easy and more secure way, but sending them in a connected form resolves any future dispute possible.

Dual Signature in SET

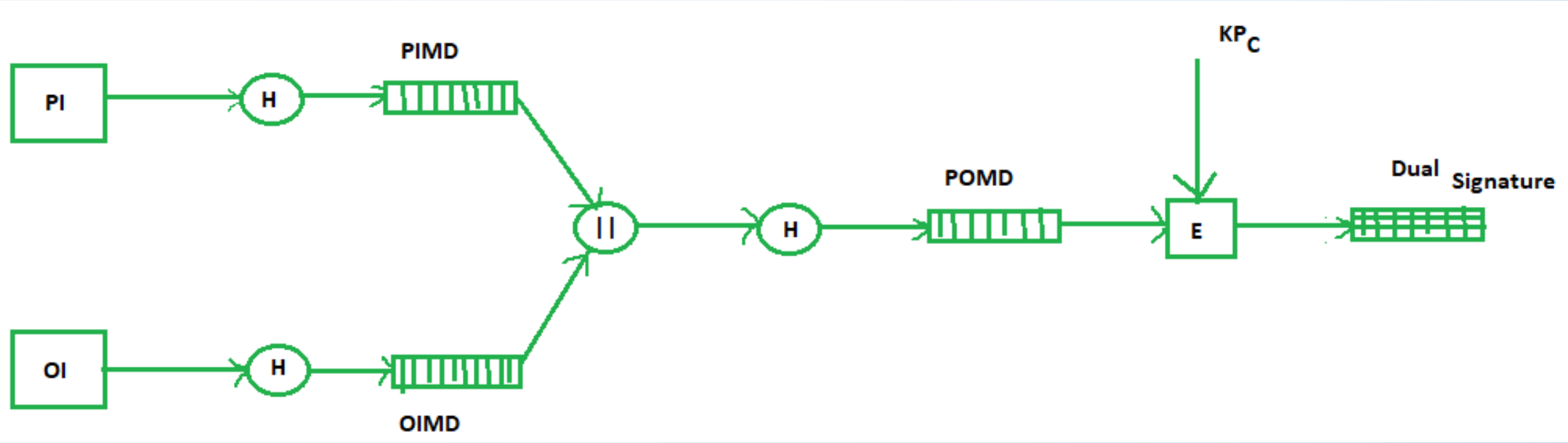


Fig : generation of dual signature:

- PI - Payment Information
- OI - Order Information
- PIMD - Payment Information Message Digest
- OIMD - Order Information Message Digest
- POMD - Payment Order Message Digest

H - Hashing

E - public key encryption

|| - append operation

Dual signature, DS= E(KPc, [H(H(PI)||H(OI))])

KP_c is customer's private key

Payment Authorization and Payment Capture

- Payment authorization is the authorization of payment information by merchant which ensures payment will be received by merchant.
- Payment capture is the process by which merchant receives payment which includes again generating some request blocks to gateway and payment gateway in turn issues payment to merchant

Global and Local Payment Systems

- As a merchant looking to enter eCommerce markets on different geographic coordinates, one of the greatest challenges you face is understanding what the most used online payment methods are.
- Based on the accessibility in geographical regions, there are two types of e-payment systems.
  - Global Payment Systems
  - Local Payment Systems

Global and Local Payment Systems

- **Global Payment Systems :**
  - consumers nowadays expect different payment methods to be featured in online stores, so they can choose the one that suits that specific need.
  - In order to be relevant to the widest audience you need to ensure your site/app has capabilities to support those payment means which are most popular online all around the world.
  - Ex : Credit & debit cards which are one of the most popular choices globally for online purchases, although their market share has been dented in recent years by eWallets.
  - Worldwide, cards accounted for 41% of eCommerce transactions in 2018.
  - Ex : E-wallets/mobile apps like google pay, paypal, bank transfers, IME, amazon, etc

Global and Local Payment Systems

- **Local Payment Systems :**
  - in order to enter some local markets, you have to understand how preferences vary in each region.
  - Some markets have a stronger preference for cards, whereas in others the eWallet is king.
  - Certain markets also employ online methods developed specifically for citizens in that region/country
  - Local payment methods can range anywhere between 10% to 50% in adoption in a country, so be sure to consider local flavors when setting up an eShop there.
  - Eg : Esewa, ATM Cards, Fare Cards for an event, Khalti, Connect IPS, Bank eWallets etc.