

ASSURANCE CASE FOR MOBILE PAYMENT SYSTEM



Ojetunde Babatunde Segun
Mehnaz Seraj

Purpose of Exercise

2

- Experience system assurance lifecycle
- Learn background of the system assurance
- Learn techniques for system assurance
 - ▣ Describing a target system
 - ▣ Analyzing risk
 - ▣ Considering architectural design
 - ▣ Considering counter measures of the risk
 - ▣ Constructing arguments showing any risk is mitigated to acceptable level

Overview of Target System

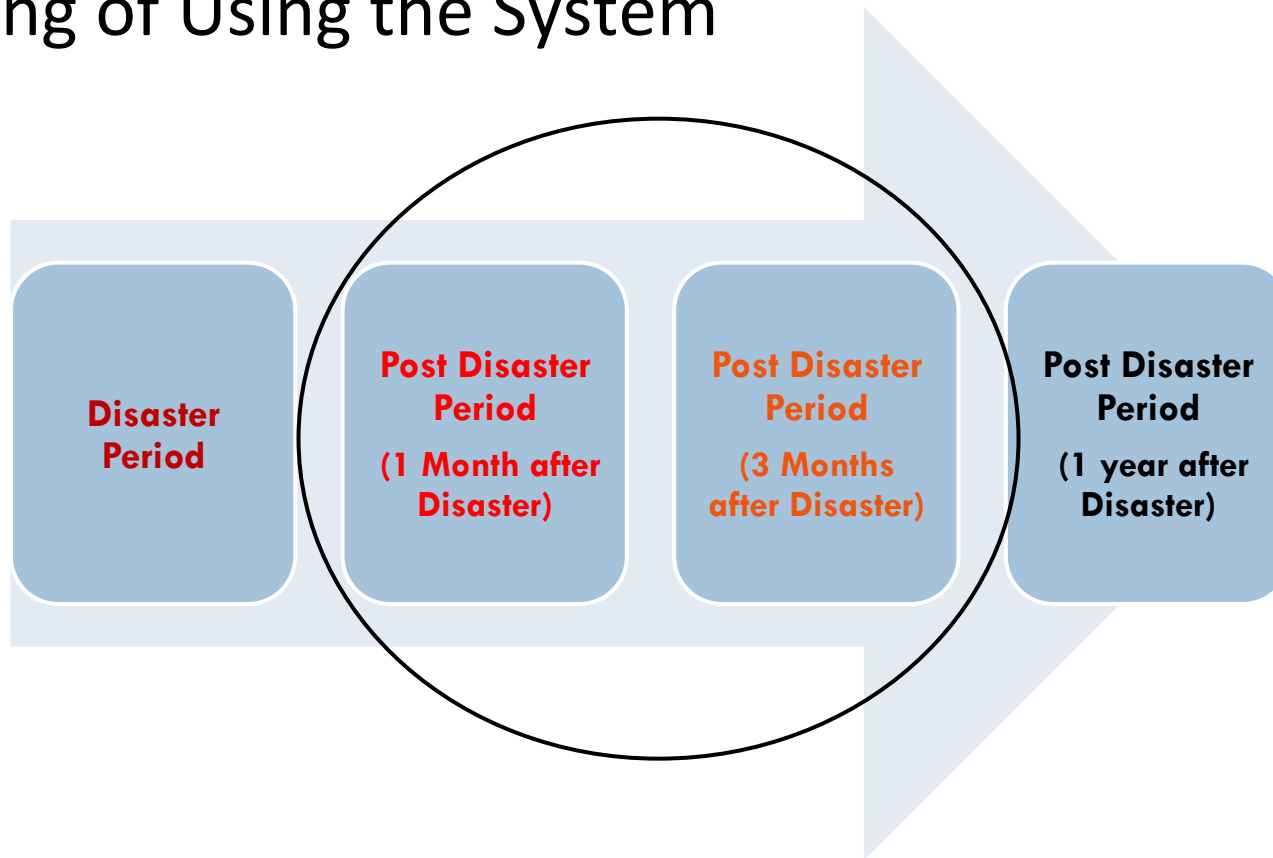
3

- Customer can purchase items from merchant using endorsement after disaster happens
- This will ease difficulty of doing transaction where there is unavailability of network infrastructure
- The assurance case for Mobile Payment Systems for this exercise is created from mobile payment point of view
 - ▣ Normal daily transaction
 - ▣ Disaster area transaction
- We focus on disaster area transactions

Overview of Target System 2

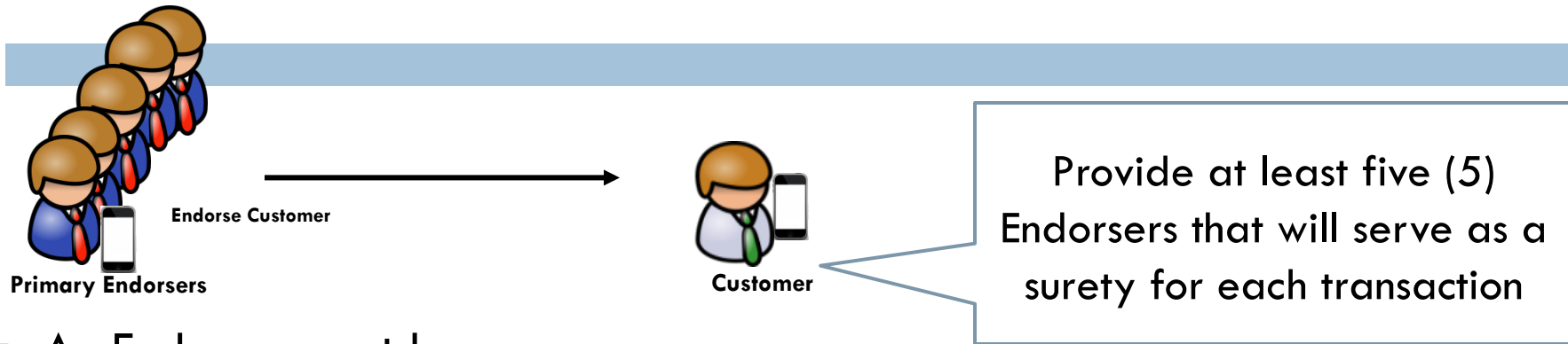
4

Timing of Using the System



Endorsement - Hoshounin

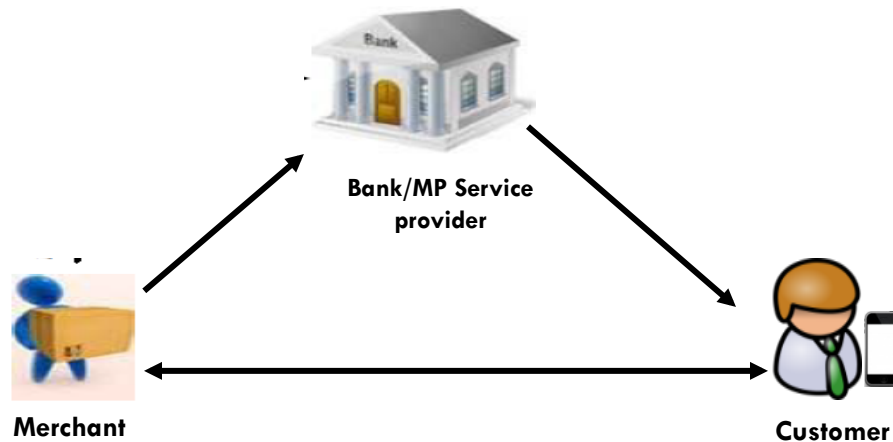
5



- An Endorser must be;
 - Known to the bank (customer of the bank)
 - Must be a user of the mobile payment system
- Minimum of 5 Endorsers is assumed to avoid one person from paying too much money in case a Customer default
- In case of non-payment, Endorsers will pay for the item purchased by the customer
- Each Endorser decides maximum amount (Price) to pay for defaulted user

Overview: Normal Transaction

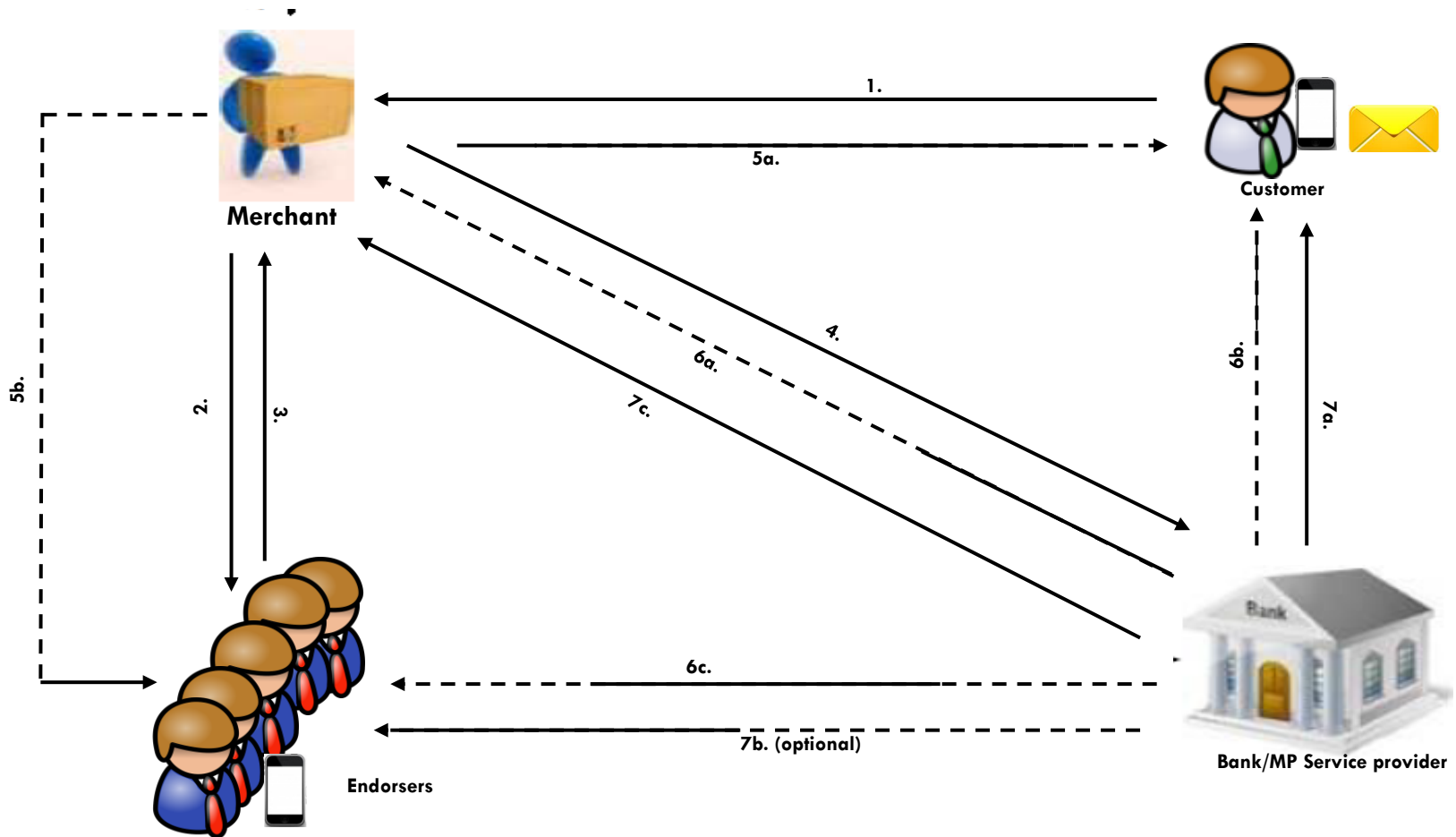
6



- The customer send transaction order to the merchant for the purchase of an item
- The Merchant forward the payment information to the bank
 - ▣ The bank deduct the money from the customer and pay the Merchant
 - ▣ If there is no money in the customer account, the transaction is declined

Overview: Disaster Area Transaction

7



Transaction Process

(1/5)

8

Send digitally signed message to the Merchant (Item Order Form which includes Item, Quantity) and digitally signed picture of the customer



Merchant

Purchase Goods/
Services



Customer



Merchant

Purchase Goods/
Services



Customer

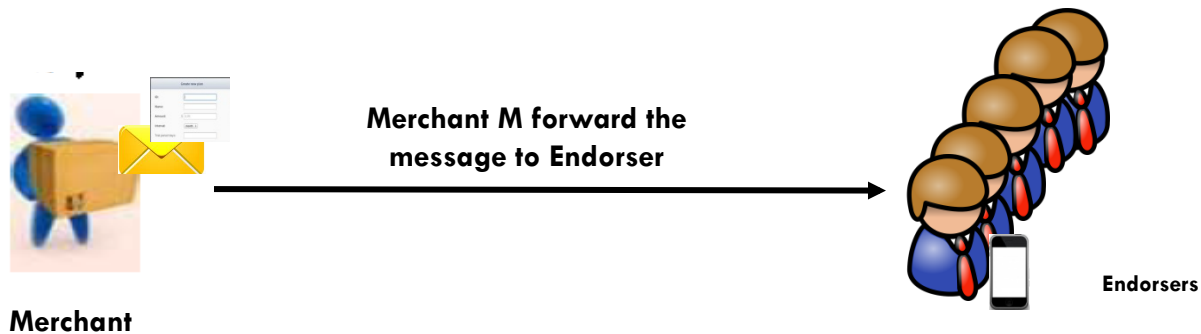
The Merchant Verify the Customer with the picture, there is no possibility the mobile phone is stolen

Transaction Process

(2/5)

9

- Here, we assume that there are Endorsers available

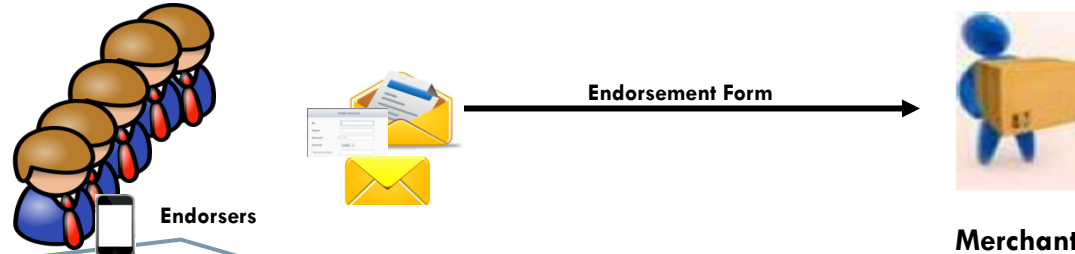


Create Billing Form and forward Billing Form and Item Order Form to Endorsers

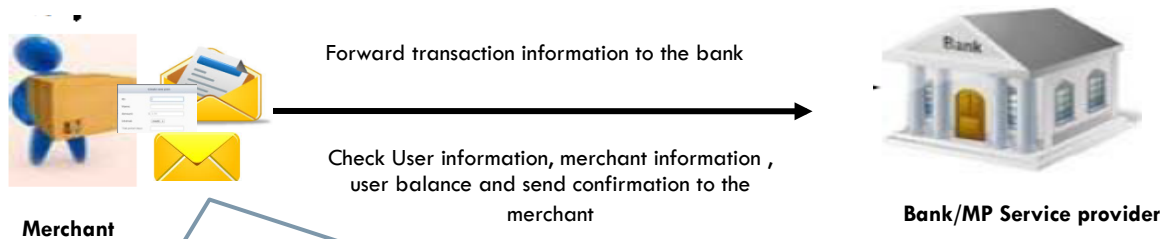
Transaction Process

(3/5)

10



Authenticate the Merchant & Create endorsement form
Send The Endorsement Form, Billing Form and Item Order form to the Merchant

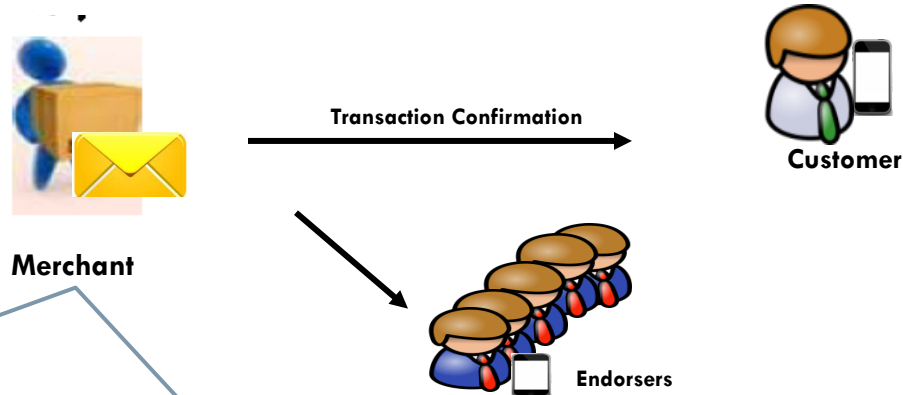


Merchant forward the Billing Form, Endorsement Form and Item Order Form to the Bank

Transaction Process

(4/5)

11



Merchant Send Transaction confirmation to Customer and copy the Endorsers



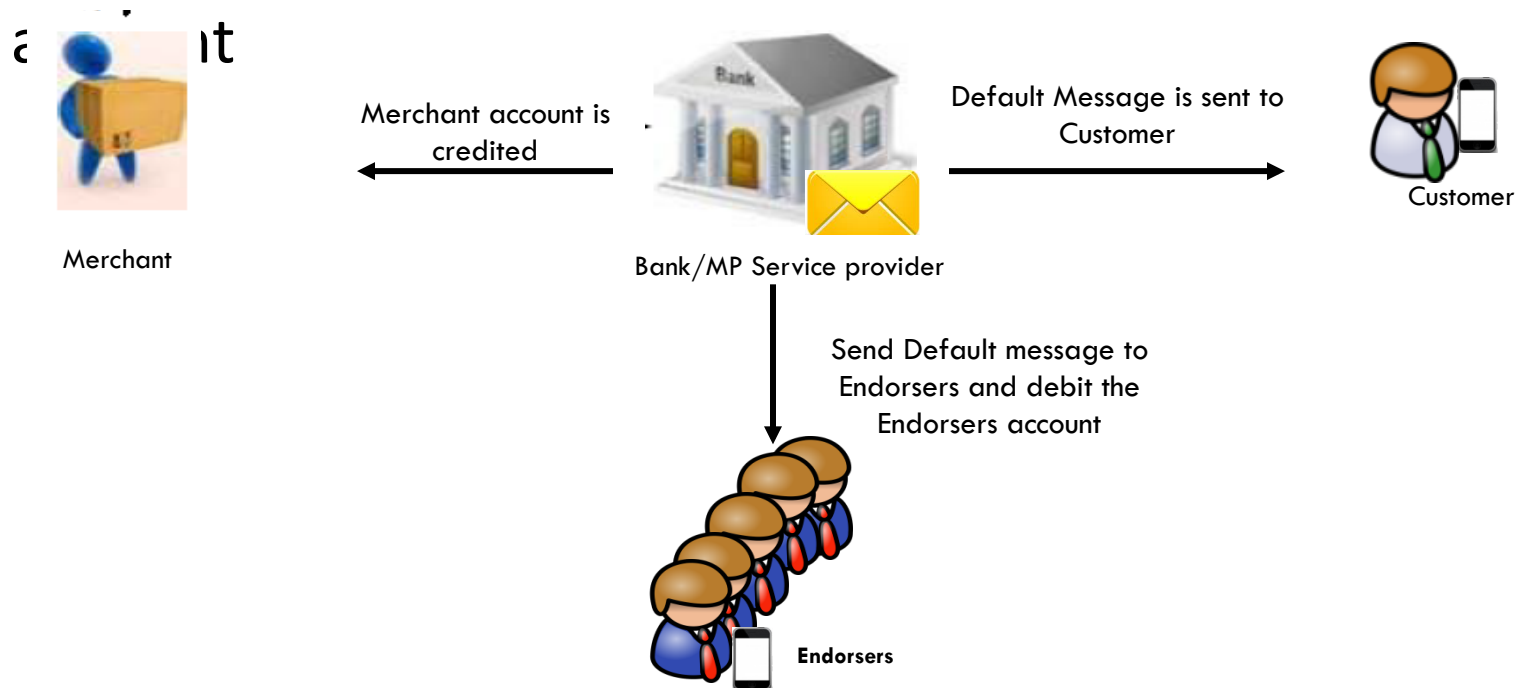
- Bank authenticate the Customer, Merchant and Endorser
- Bank B checks if the content of Item Order Form, Endorsement Form and Bill Form is consistent
- Checks if Customer has enough fund in his account and transaction value is deducted from Customer's account

Transaction Process

(5/5)

12

- If there is no fund in Customer account and the transaction value is deducted from the Endorsers



Debit Endorsers account for the Customer's transaction based on the Endorsed value

Send acknowledgement to Merchant, Customer and Endorser

System Assurance Lifecycle

13

1. Scope of Systems

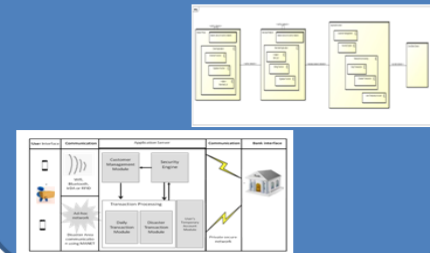
- Customer can purchase items from merchant using endorsement after disaster happens



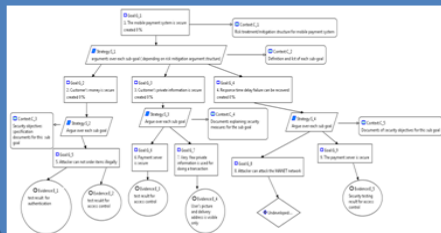
2. Possible Adverse Consequences

- Lose of Private information (user's picture, contact list, account information and text message).
- Lose money.
- Stop the Mobile Payment Service.
- Users receive spam mails.
- Lose of mobile phone.

5. Architectural Design/Deployment Diagram



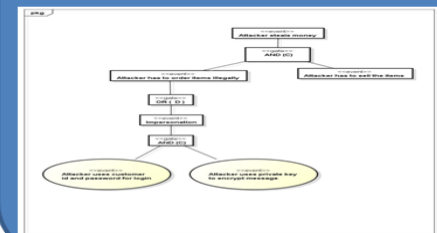
6. Assurance Case



5. Specialist Comment



4. Attack Tree



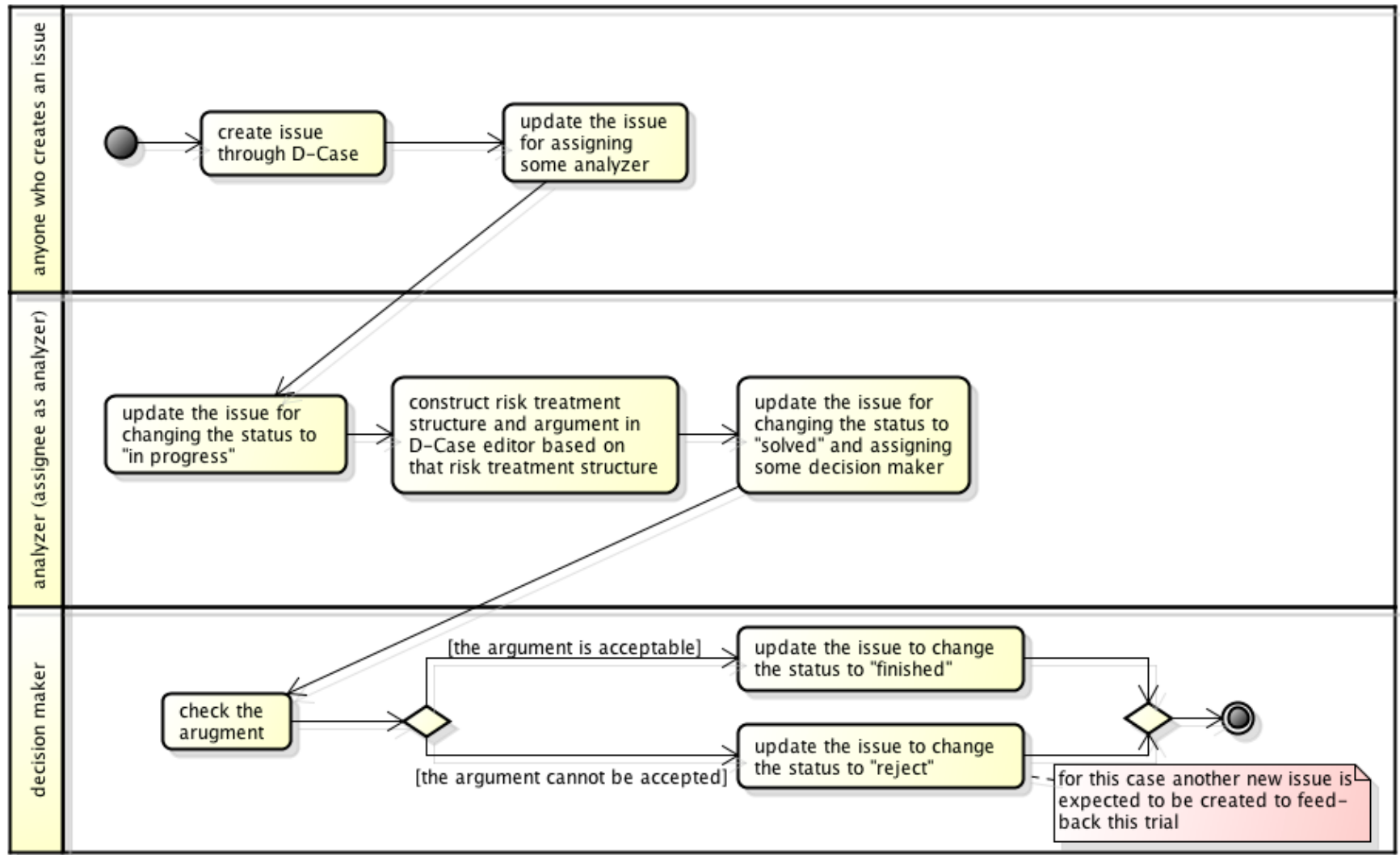
Roles of D-Case in this Exercise

14

- To show justification of using generalized common criteria framework
- Traceability
 - ▣ from threats to security objectives
 - ▣ from security objectives to security requirements

The workflow of this project with Redmine and D-Case

15



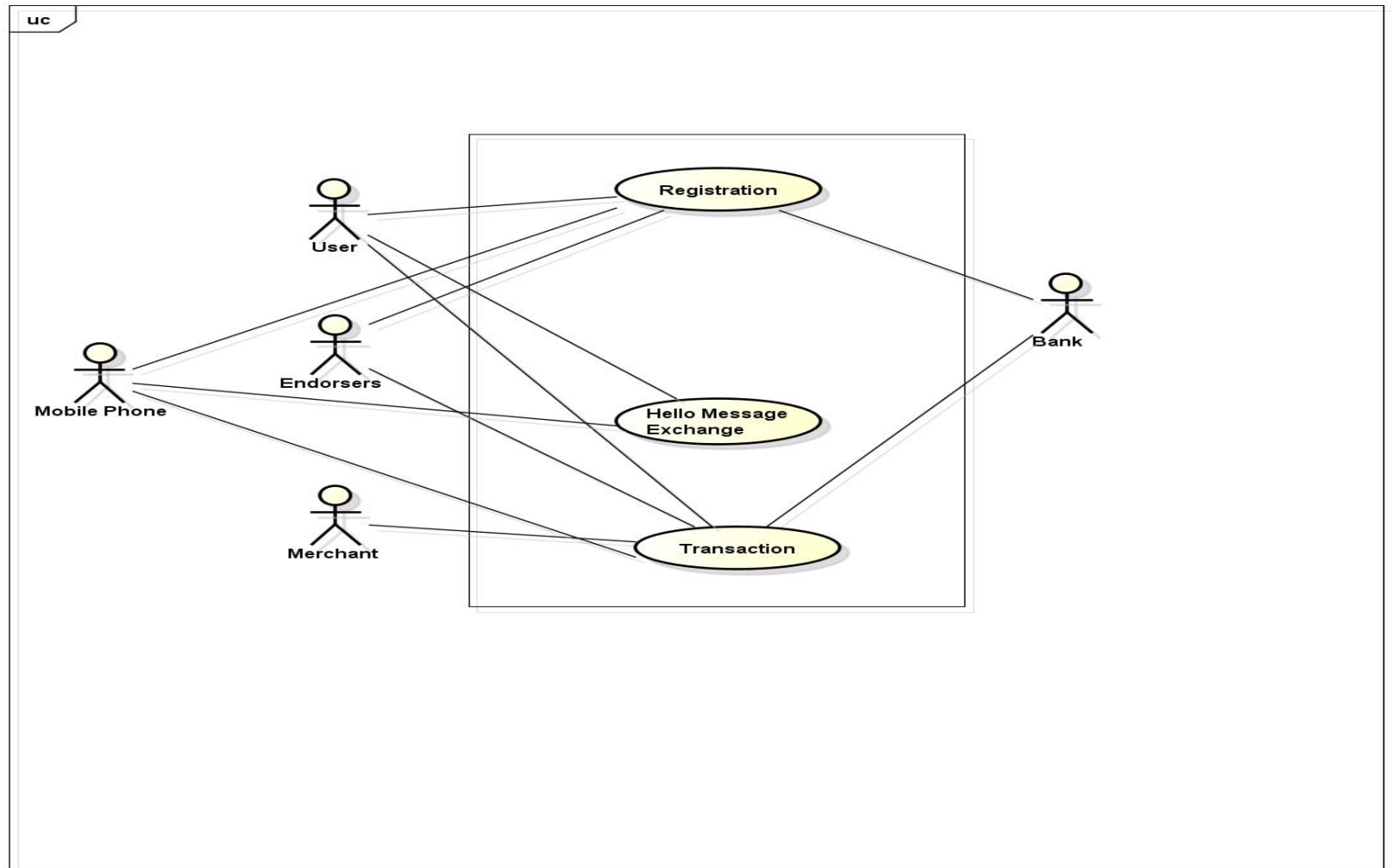
Examples of Obtained Products

16

Document ID	Description
ID1	Informal description of the target system
ID2	Informal description of physical overview
ID3	Informal description of bad scenarios
ID4	General requirements
ID5	Use case diagram in UML
ID6	Deployment diagram in UML
ID7	Message Sequence diagram in UML
ID8	Class diagram in UML
ID9	List of base standards
ID10	List of adverse consequences
ID11	Attack tree diagram in UML

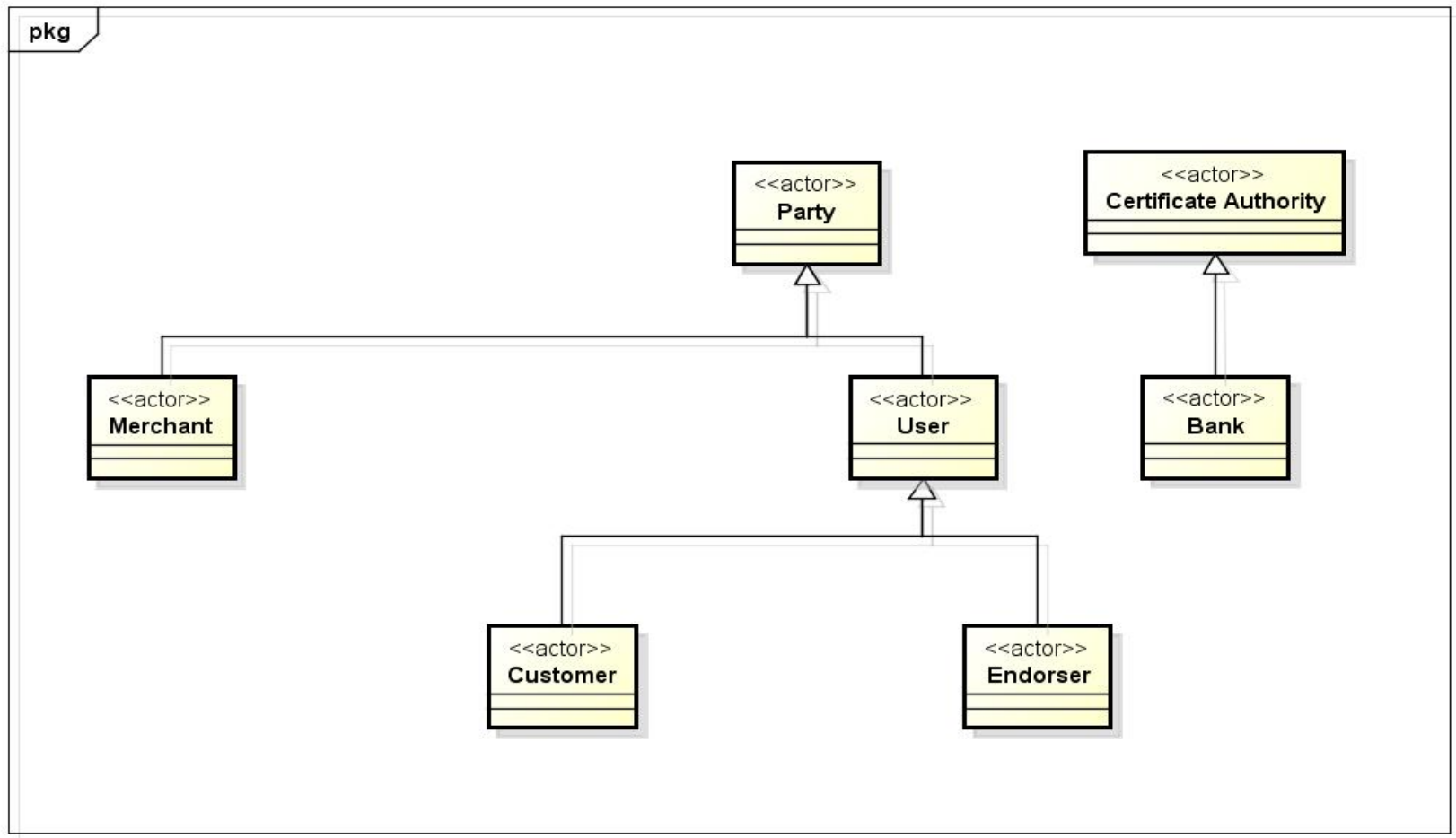
Examples of Documents content (Use case)

17



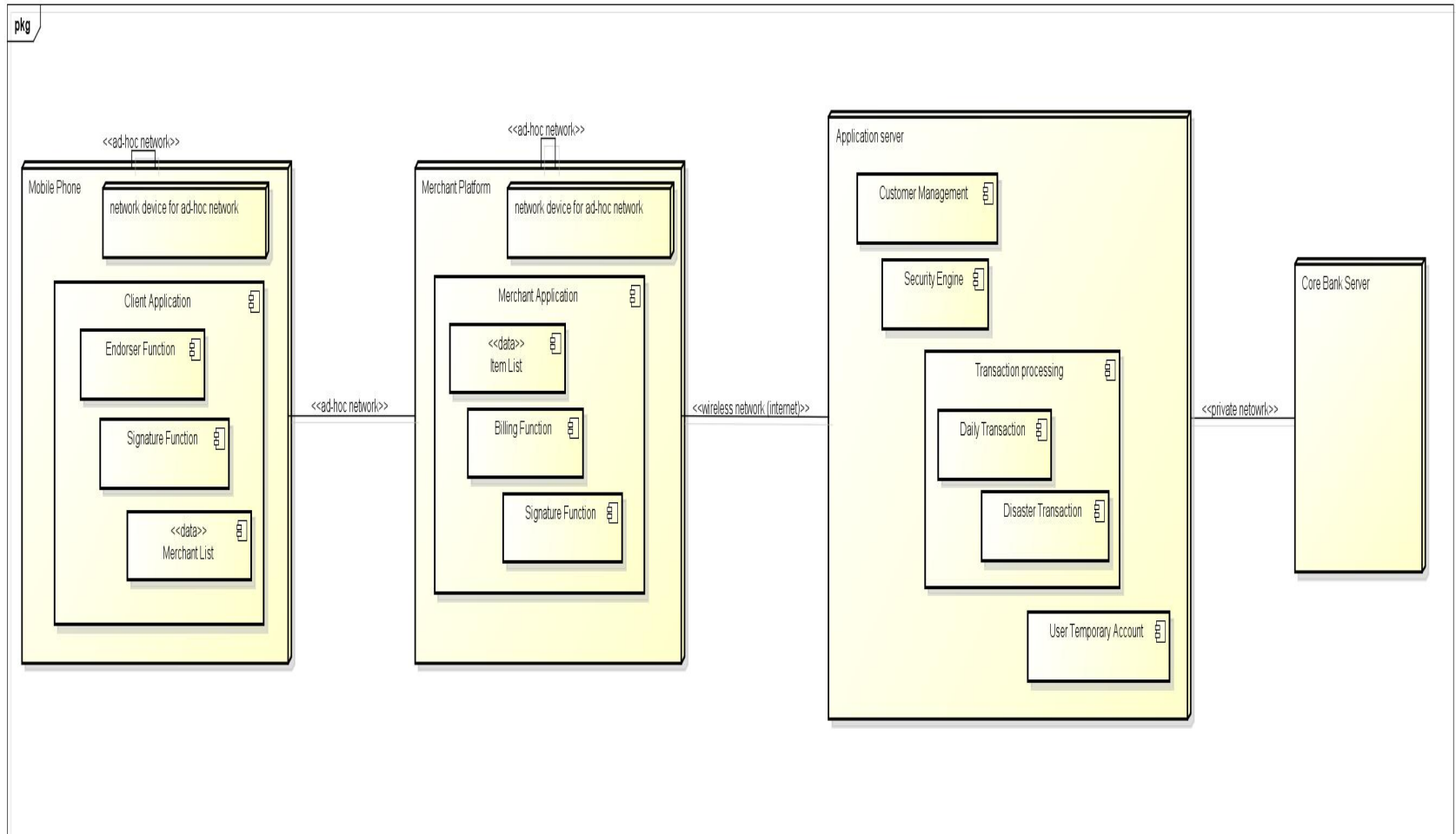
Examples of Documents content (Specification of Participants)

18



Examples of Documents content

19



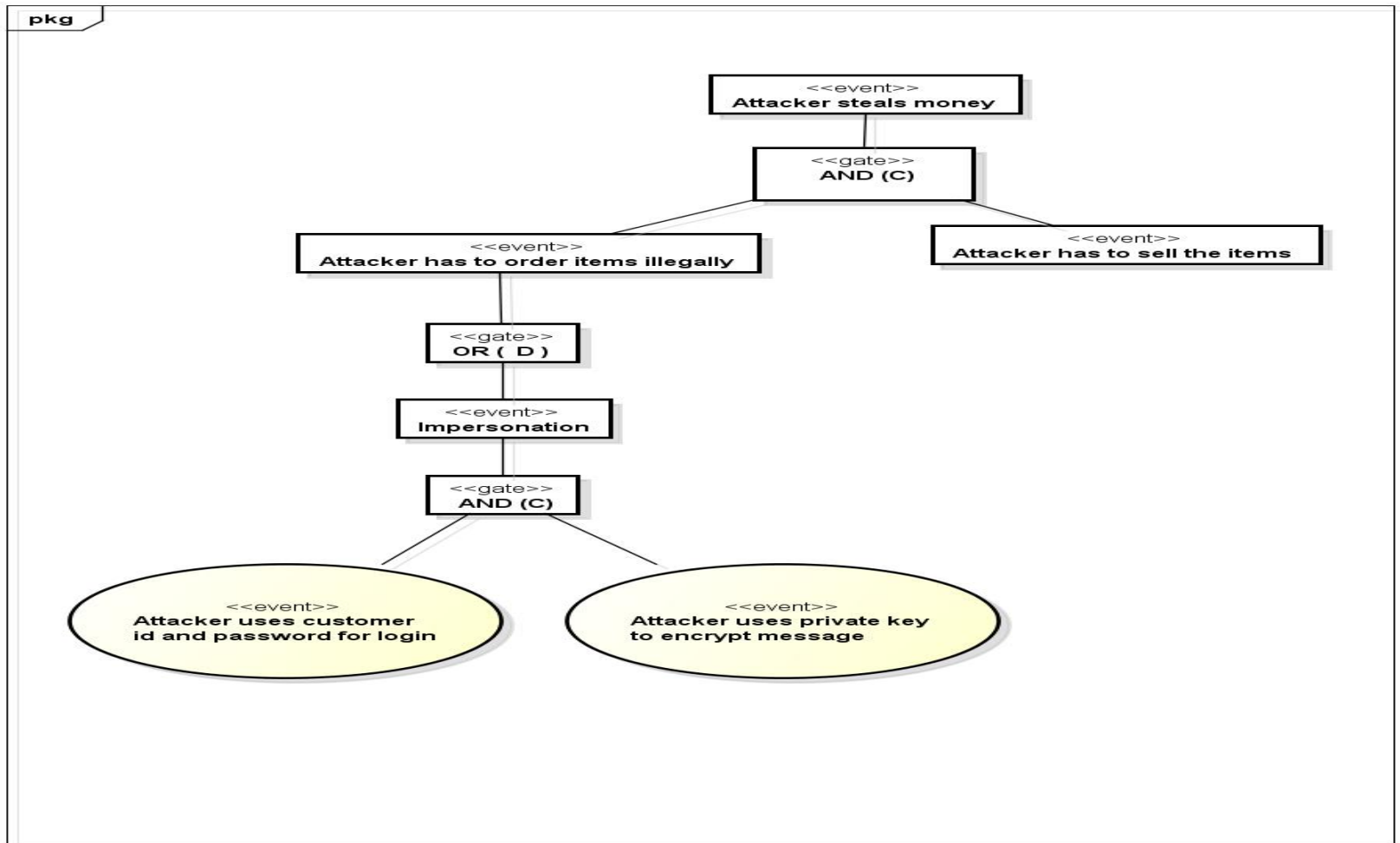
Examples of Documents content (Message Sequence)

20



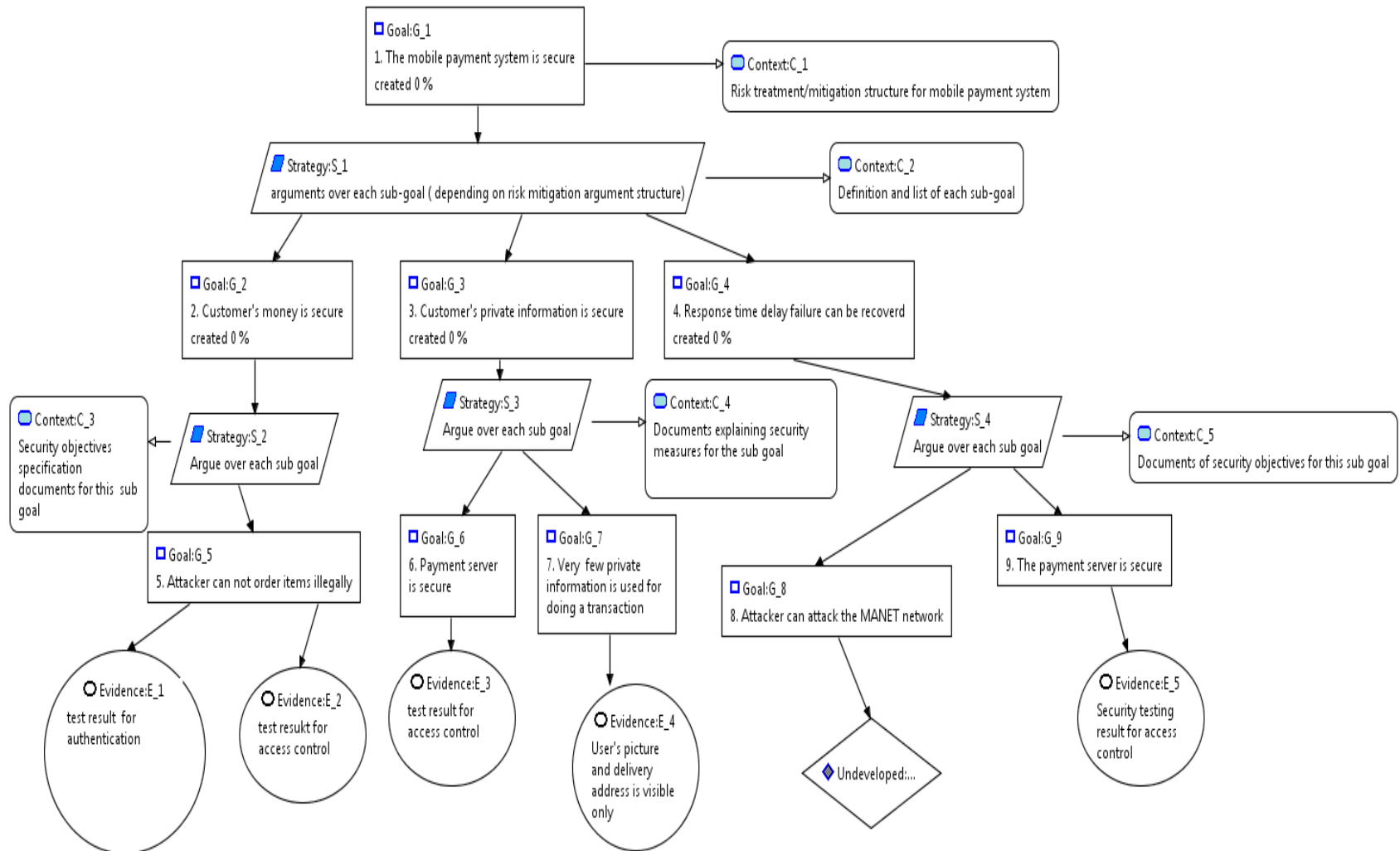
Examples of Documents content (Attack tree)

21



Examples of Documents content (Assurance Case)

22



Review of our project

23

❖ Visiting companies

- National Institute of Advanced Science and Technology (AIST)
- Nagoya Institute of Technology
- Atelier Corporation

Comments from AIST

24

- System failure
 - ▣ If the system fails by itself what measure can be taken
- Mobile vulnerability
 - ▣ Issues that concern the mobile phone that are not related to the payment system
- False disaster alert
 - ▣ Counter measures to prevent attacker from given false disaster alert
- Consider common criteria framework for threat analysis
- What are the assumptions of the environment of the system

Comments from Nagoya Institute of Technology

25

- What are the set rules/constraints to using the system
 - ▣ Upper limit of purchase
 - ▣ Number of transaction per day
- Attack tree should be created from attacker's view point
- How or what level data is gathered
- Highlight the vulnerabilities of the system

Comments from Atelier Corporation

26

- Specify asset, threat and counter measures required by common criteria
- Show traceability from threats to security objectives and from security objectives to security requirements
- Show why our constraints are necessary and complete

Record/ log of activities

27

Jan, 28

Intensive
Lectures

Feb, 10

Tunde-san's ppt
Slides

Initial list of adverse
consequence

Risk table based on
EVITA

Feb, 25

Threat, adverse
consequence,
prevention, etc. in
natural language

Use case diagram
(detailed version)

Feb, 10

Feb 21
Visit AIST

Feb 27 Visit
Nagoya Institute
of Technology

Atelier

Notice that
FTA and
attack tree
are different
things

Fixing
limitation of
the amount
of
transactions

Organizing
documents
based on
common criteria
framework

FTA/Attack
tree

Attack tree

Product

Activity

Event

Mar, 4

Matsuno-Sensei's
D-Case lecture

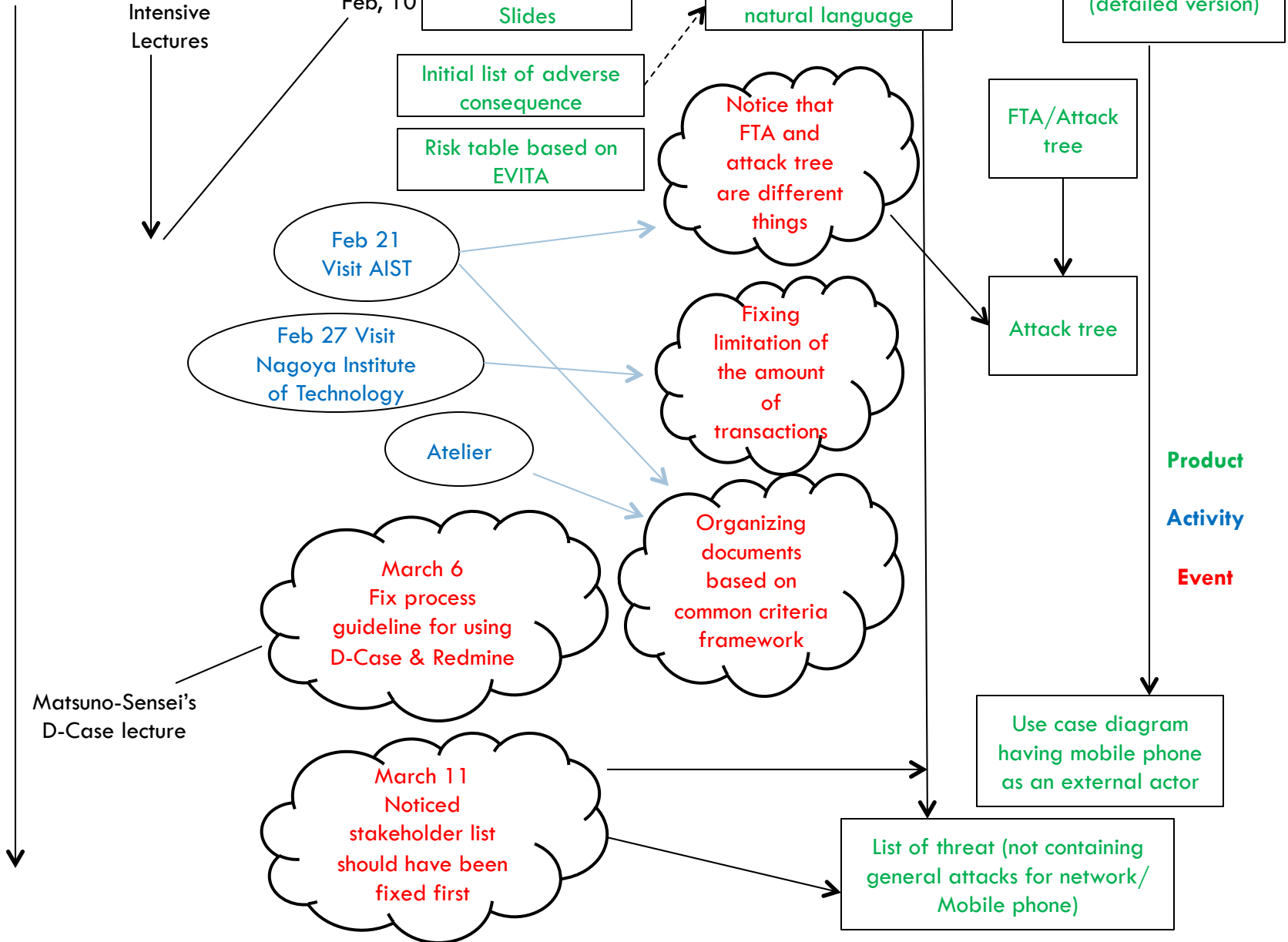
March 6
Fix process
guideline for using
D-Case & Redmine

March 11
Noticed
stakeholder list
should have been
fixed first

Use case diagram
having mobile phone
as an external actor

List of threat (not containing
general attacks for network/
Mobile phone)

Mar, 18



Current problems of D-case methodology

28

- ❑ Too many view point of argument structure
 - ❑ No guideline for integrating them
- ❑ Effectiveness of D-case from a view of **one** aspect is not clear.

Problematic Characteristics of our system

29

- Boundary is unclear
- Involve other huge system
- Changing it's configuration continuously
- Relating a number of users
- Expected to work correctly in emergency

Acknowledgement

30

- We are grateful to Dr. Taguchi, Prof. Koshijima, Dr. Daichi Mizuguchi, Dr. Hiroki Takamura, Dr. Matsuno for their valuable comments.

THANK YOU