Lecture 7

Design of Secure Software Architecture

1

Design of Secure Software Architecture

- Secure Software Architecture
  - Structure of secure software system
    - Software elements (e.g., secure subsystems or components)
    - Relationships among elements (e.g., secure connectors)
- Develop initial secure software architecture
  - Synthesize from communication diagrams
  - Structure system into subsystems
- Secure subsystems determined using subsystem structuring criteria
  - Use stereotypes for subsystem structuring criteria
    - E.g., <<client>>, <<service>>
  - Depict secure subsystems on subsystem communication diagrams

2

Transition from Analysis to Design: Develop initial secure software architecture

- Start with dynamic interaction model
  - Use case-based interaction diagrams
    - Sequence diagrams
    - Communication diagrams
- Integrate use case-based interaction diagrams
  - Initial version of secure software architecture
- Structure system into secure subsystems
  - Secure subsystem contains application and security objects
- Depict secure subsystems on subsystem communication diagram
  - High-level communication diagram
  - Shows secure subsystems and their interactions
  - Use stereotypes for **subsystem structuring criteria**

3

Transition from Analysis to Design: Integration of Communication Diagrams

- Integration of communication diagrams
  - To determine overall structure of secure system
- Merging of communication diagrams
  - Start with first communication diagram
  - Superimpose other communication diagrams
    - Add new objects and new message interactions from each subsequent diagram
    - Objects and interactions that appear on multiple diagrams are only shown once
    - Consider alternative scenarios for each use case
- Integrated communication diagram
  - Shows all application and security objects and their interactions

4

Design of Secure Software Architecture

- Secure Software Architecture
  - Define overall structure of secure system
    - Secure components and secure interconnections
  - Separately from secure component internals
- Each secure subsystem
  - Contains highly coupled application and security objects
  - Relatively independent of other subsystems
  - May be decomposed further into smaller subsystems
  - Secure subsystem is aggregate or composite object

5

Separation of Subsystem Concerns

- **Aggregate/composite object**
  - Objects that are part of aggregate/composite object
  - Structure in same subsystem
- **Scope of Control**
  - Control object & objects it controls are in same subsystem
- **Geographical location**
  - Objects at different locations are in separate subsystems
- **Clients and Services**
  - Place in separate subsystems
- **User Interaction**
  - Separate client subsystem
- **Security objects for application object**
  - Security objects supporting application object
  - Structure in the same subsystem

6

Subsystem Structuring Criteria

- Client
  - Requester of one or more services
- User Interaction
  - Collection of objects supporting needs of user
- Service
  - Provides service for client subsystems
- Control
  - Subsystem controls given part of system
- Coordinator
  - Coordinates several control subsystems
- Input / Output
  - Performs I/O operations for other subsystems

7

Design Distributed Subsystem Interfaces

- Message Communication between distributed subsystems
  - Asynchronous message communication
    - Peer to peer communication
  - Synchronous message communication
    - Client / Service message communication
  - Group Message Communication
    - Broadcast message communication
    - Multicast message communication
  - Brokered Communication
    - Uses Object Broker
- Also referred to as message communication patterns

8

UML notation for messages

Simple message (analysis model)
No decision yet made about message type

«simple message»
message–name

Design model:

a) Asynchronous (loosely coupled) message communication

«asynchronous message»
message–name (argument list)

b) Synchronous (tightly coupled) message communication

«synchronous message»
message–name (argument list)

c) Synchronous (tightly coupled) message communication with reply

c1) Option 1:

«synchronous message with reply»
message–name (**in** argument list, **out** argument list)

c2) Option 2:

«synchronous message»
message–name (argument list)

«reply»

9

9

Secure Software Architecture

- Secure software architecture
  - Secure components and secure connection (connectors)
- Secure components
  - Application objects
  - Security objects
- Secure connector
  - Communication (pattern) object
  - One or more security (pattern) objects
  - Security coordinator object

10

10

Service Oriented Architecture

- Layered Architecture
  - Client, Coordinator, Service pattern
- SOA
  - Services register with Broker
  - Clients/Coordinators
    - Discover Services using Broker
    - Communicate with Services
- Design Service Interfaces

11

11

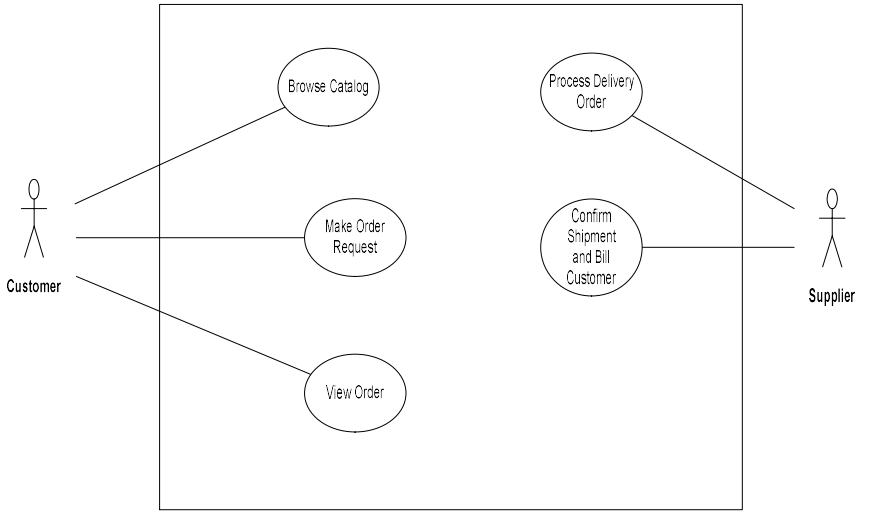
Design of Secure Service Oriented Architecture

- Each service designed as secure autonomous reusable components
- Coordination services provided
  - Instead of one service depending on another
- Secure SOA
  - Loosely coupled secure services
  - Discovered or linked by secure clients
  - With the assistance of service brokers
- Client/Server SA
  - Synchronous services
  - Fixed server configuration

12

12

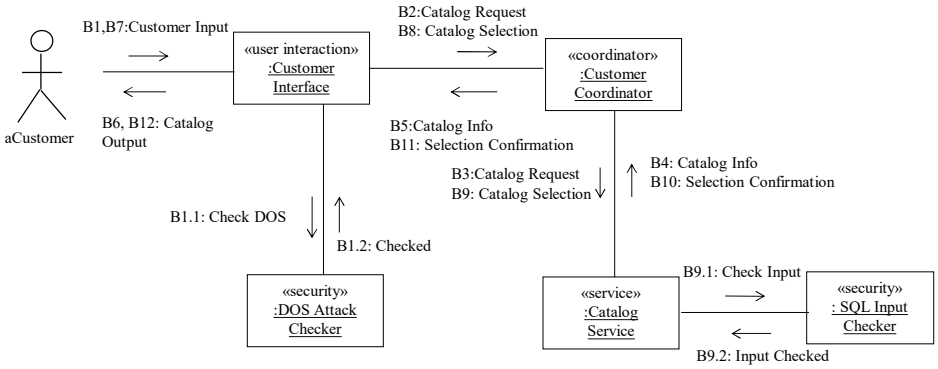
Case Study - Design of Secure Service Oriented Architecture for Online Shopping System



13

Secure Communication Diagram for Browse Catalog use case

- Threats
  - Flood of browsing Catalog
  - SQL Injection
- Security objects
  - DoS Attack Checker
  - SQL Input Checker

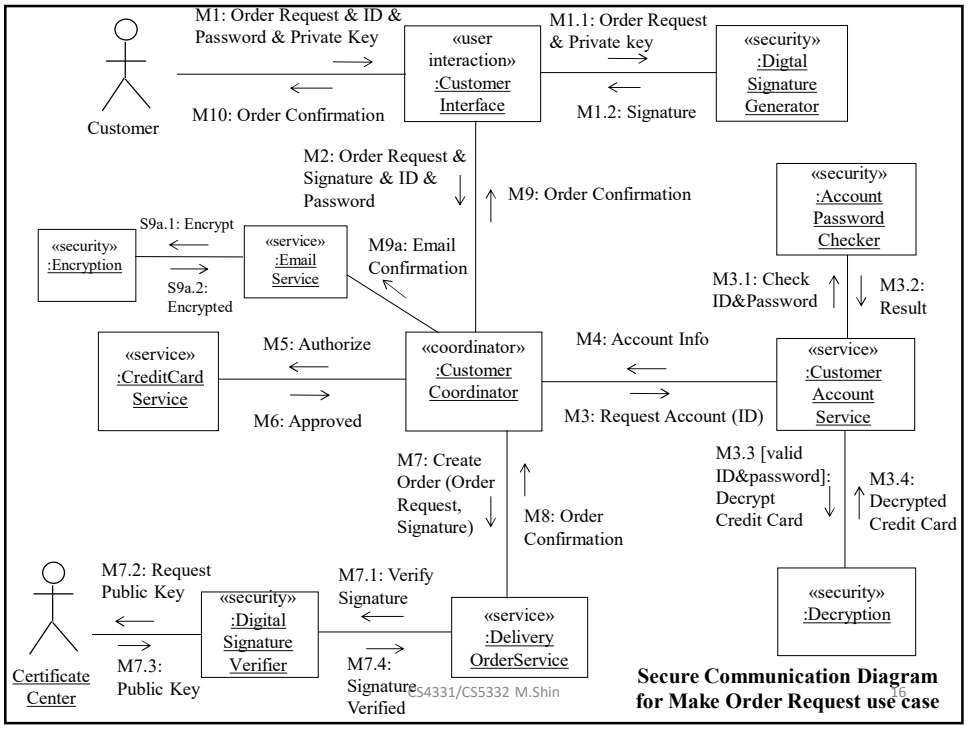


14

Secure Communication Diagram for Make Order Request use case

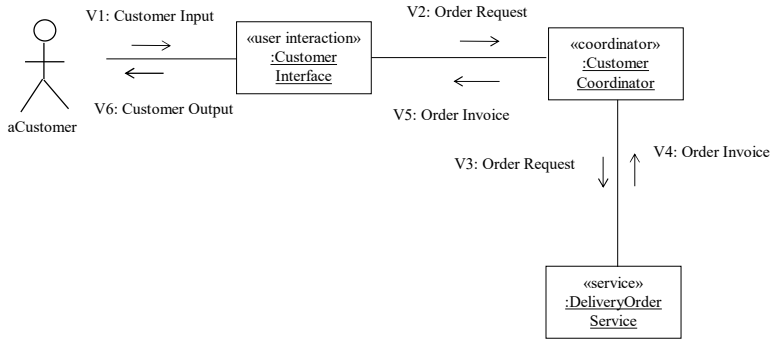
- Threats
  - Unauthenticated ID
  - Repudiation of Order Request
  - Disclosure of Customer Account
  - Disclosure of Order Confirmation Email
- Security objects
  - Account Password Checker
  - Digital Signature Generator/Verifier
  - Decryption of customer Account
  - Encryption of email

15



16

Communication Diagram for View Order use case

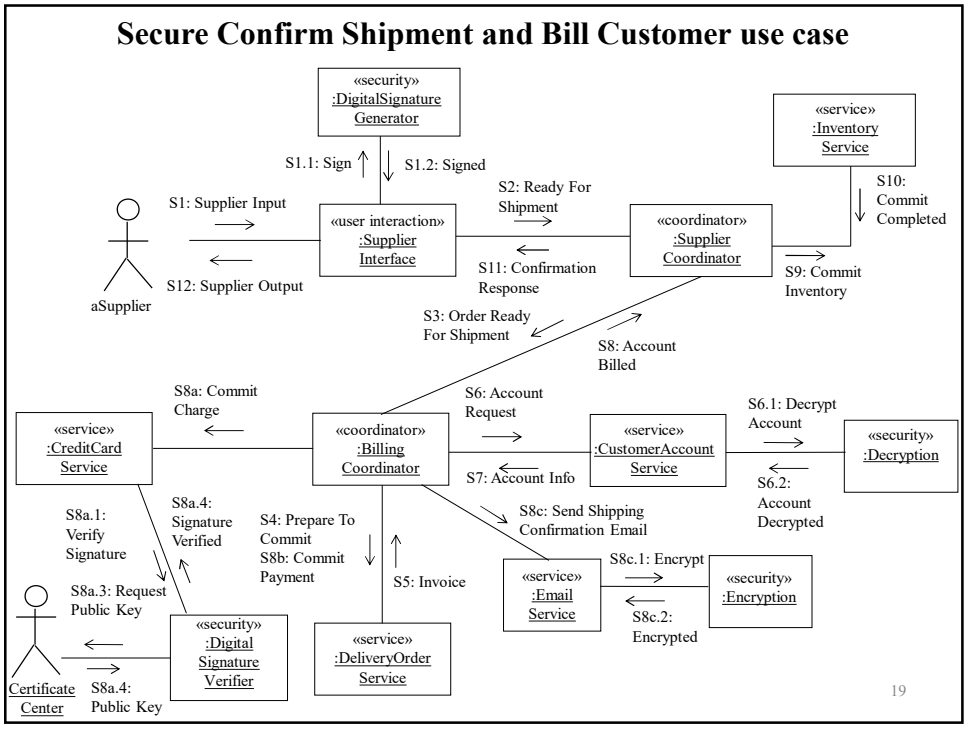


17

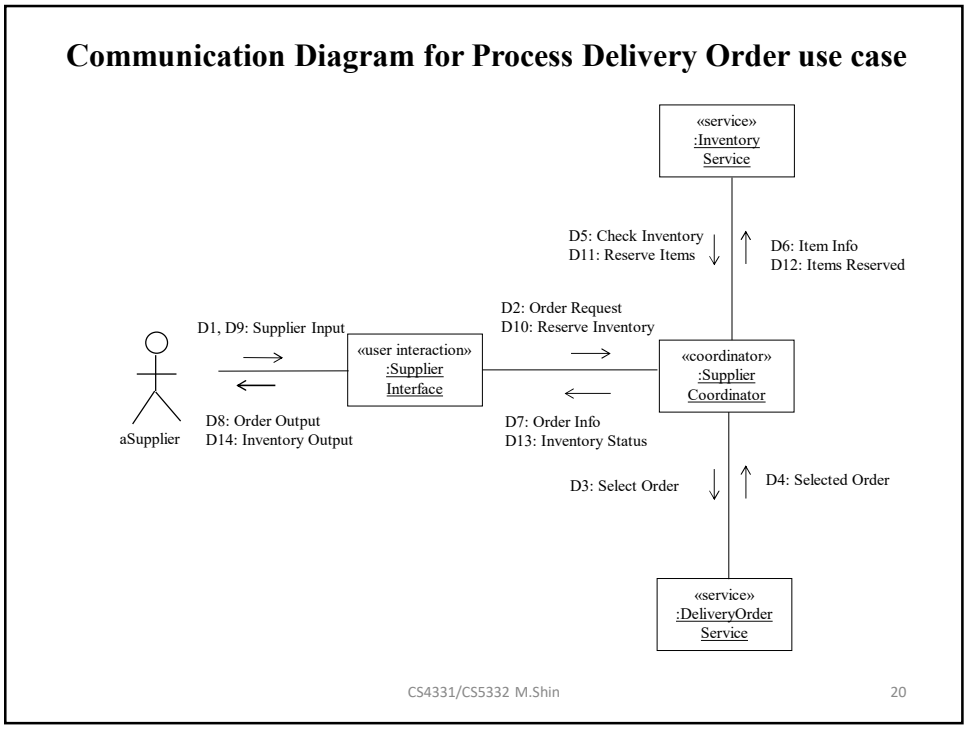
Secure Communication Diagram for Confirm Shipment and Bill Customer use case

- Threats
  - Repudiation of Payment Request
  - Disclosure of Customer Account
  - Disclosure of Shipping Confirmation Email
- Security objects
  - Digital Signature Generator/Verifier
  - Decryption of customer Account
  - Encryption of email

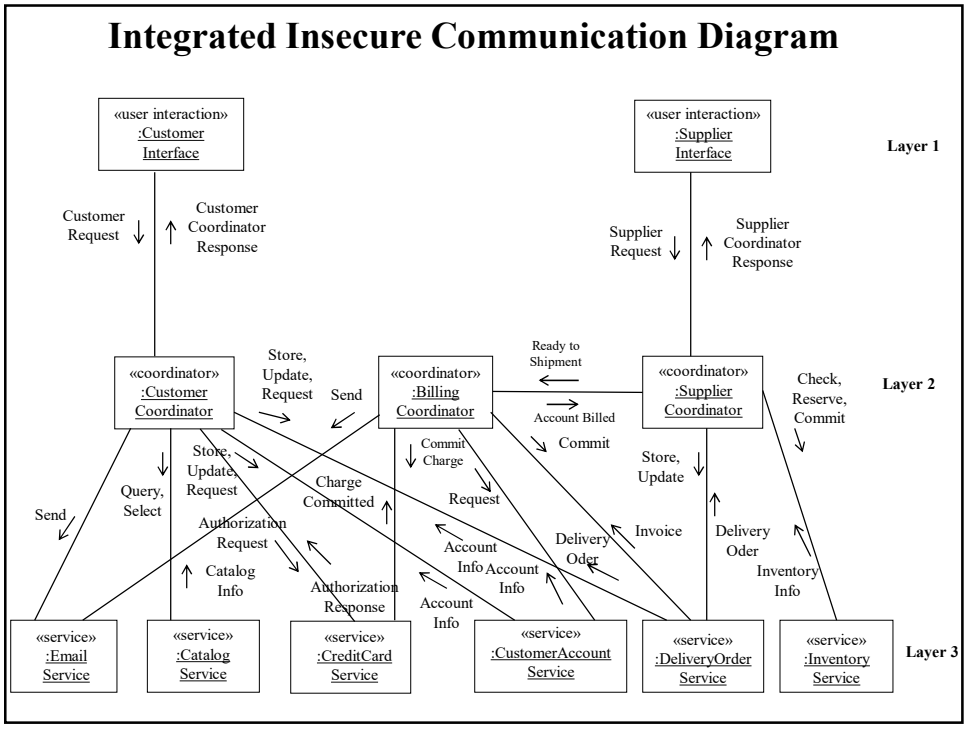
18


Secure Confirm Shipment and Bill Customer use case
«security» :DigitalSignature Generator
«service» :Inventory Service
S1.1: Sign
S1.2: Signed
S1: Supplier Input
S2: Ready For Shipment
S10: Commit Completed
«user interaction» :Supplier Interface
«coordinator» :Supplier Coordinator
S12: Supplier Output
S11: Confirmation Response
S9: Commit Inventory
aSupplier
S3: Order Ready For Shipment
S8: Account Billed
S8a: Commit Charge
S6: Account Request
S6.1: Decrypt Account
«service» :CreditCard Service
«coordinator» :Billing Coordinator
«service» :CustomerAccount Service
«security» :Decryption
S7: Account Info
S6.2: Account Decrypted
S8a.1: Verify Signature
S8a.4: Signature Verified
S4: Prepare To Commit
S8b: Commit Payment
S8c: Send Shipping Confirmation Email
S8c.1: Encrypt
S5: Invoice
«service» :Email Service
«security» :Encryption
S8a.3: Request Public Key
S8c.2: Encrypted
«security» :Digital Signature Verifier
«service» :DeliveryOrder Service
Certificate Center
S8a.4: Public Key
19

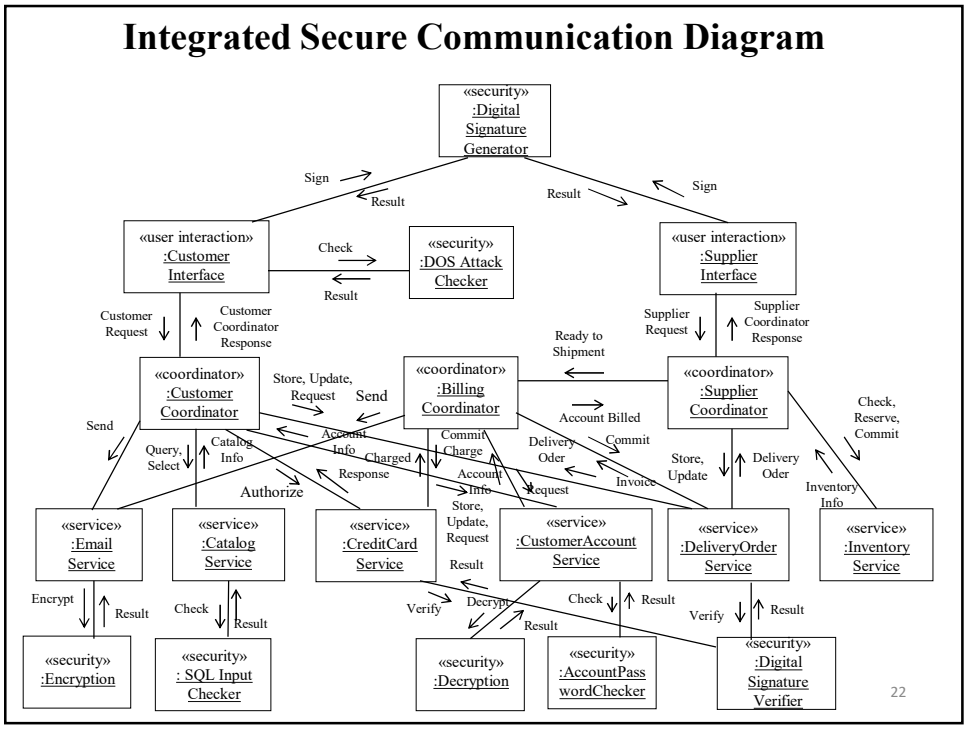
19


Communication Diagram for Process Delivery Order use case
«service» :Inventory Service
D5: Check Inventory
D11: Reserve Items
D6: Item Info
D12: Items Reserved
D2: Order Request
D10: Reserve Inventory
D1, D9: Supplier Input
«user interaction» :Supplier Interface
«coordinator» :Supplier Coordinator
aSupplier
D8: Order Output
D14: Inventory Output
D7: Order Info
D13: Inventory Status
D3: Select Order
D4: Selected Order
«service» :DeliveryOrder Service
CS4331/CS5332 M.Shin
20

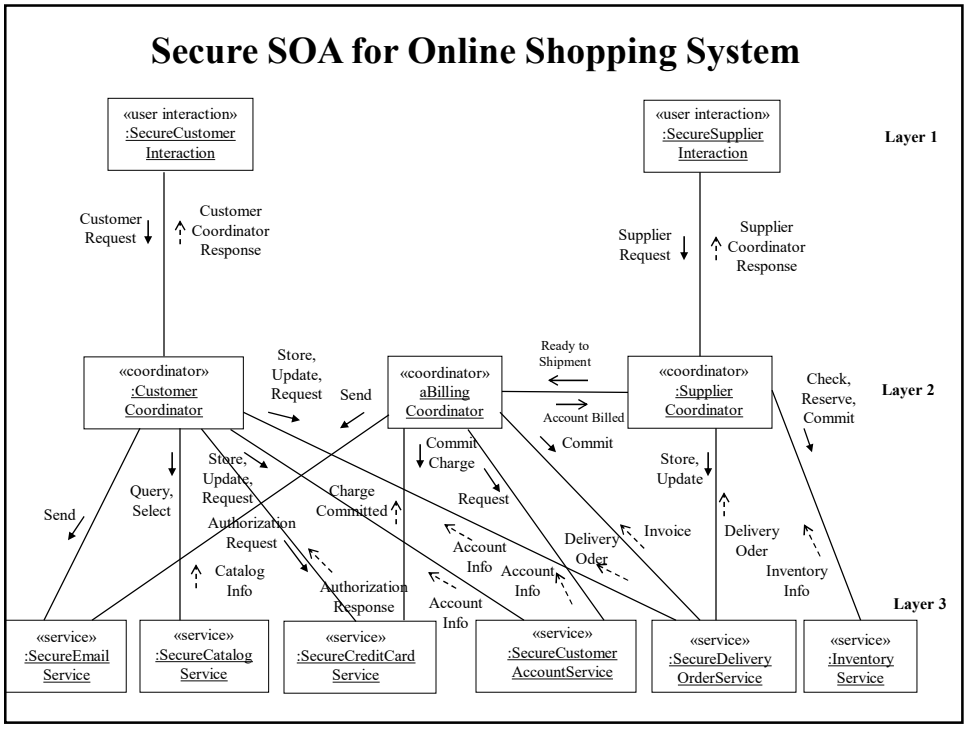
20


Integrated Insecure Communication Diagram
«user interaction» :Customer Interface
«user interaction» :Supplier Interface
Layer 1
Customer Request
Customer Coordinator Response
Supplier Request
Supplier Coordinator Response
«coordinator» :Customer Coordinator
«coordinator» :Billing Coordinator
«coordinator» :Supplier Coordinator
Layer 2
Store, Update, Request
Send
Ready to Shipment
Account Billed
Check, Reserve, Commit
Commit
Commit Charge
Store, Update
Store, Update, Request
Query, Select
Charge Committed
Request
Send
Authorization Request
Account Info
Delivery Oder
Invoice
Delivery Oder
Catalog Info
Account Info
Inventory Info
Authorization Response
Account Info
«service» :Email Service
«service» :Catalog Service
«service» :CreditCard Service
«service» :CustomerAccount Service
«service» :DeliveryOrder Service
«service» :Inventory Service
Layer 3

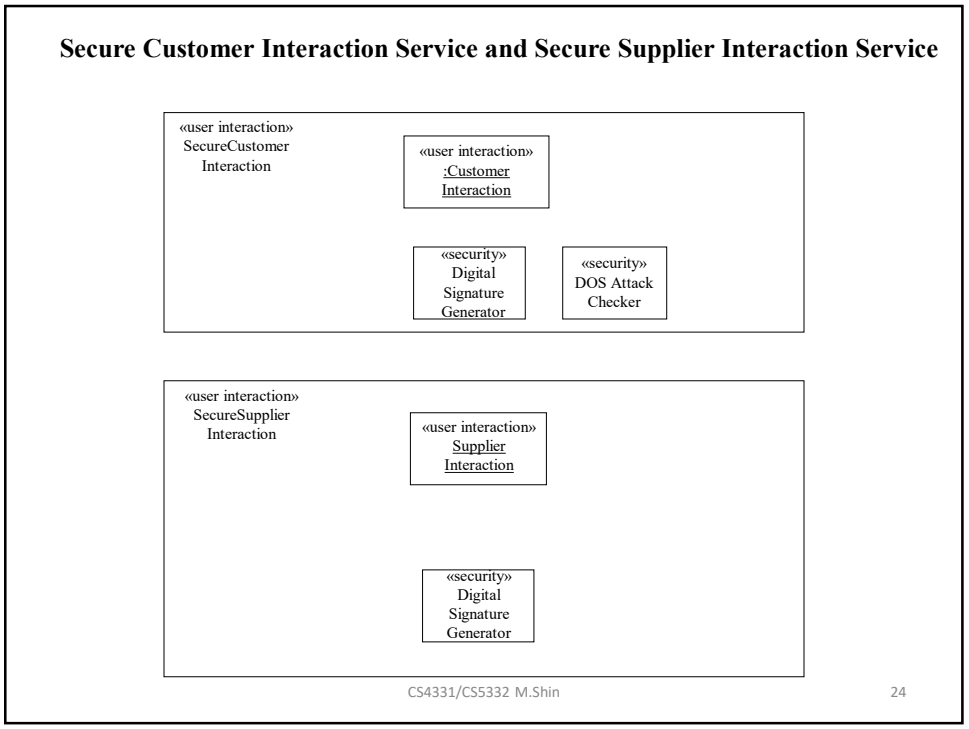
21


Integrated Secure Communication Diagram
«security» :Digital Signature Generator
Sign
Result
Result
Sign
«user interaction» :Customer Interface
Check
Result
«security» :DOS Attack Checker
«user interaction» :Supplier Interface
Customer Request
Customer Coordinator Response
Supplier Request
Supplier Coordinator Response
Ready to Shipment
«coordinator» :Customer Coordinator
Store, Update, Request
Send
«coordinator» :Billing Coordinator
«coordinator» :Supplier Coordinator
Account Billed
Check, Reserve, Commit
Send
Account Info
Commit Charge
Delivery Oder
Commit
Query, Select
Catalog Info
Charged Response
Account Info
Store, Update
Delivery Oder
Authorize
Request
Invoice
Inventory Info
Store, Update, Request
«service» :Email Service
«service» :Catalog Service
«service» :CreditCard Service
«service» :CustomerAccount Service
«service» :DeliveryOrder Service
«service» :Inventory Service
Result
Encrypt
Result
Check
Result
Verify
Decrypt
Result
Check
Result
Verify
Result
«security» :Encryption
«security» : SQL Input Checker
«security» :Decryption
«security» :AccountPassWordChecker
«security» :Digital Signature Verifier
22

22

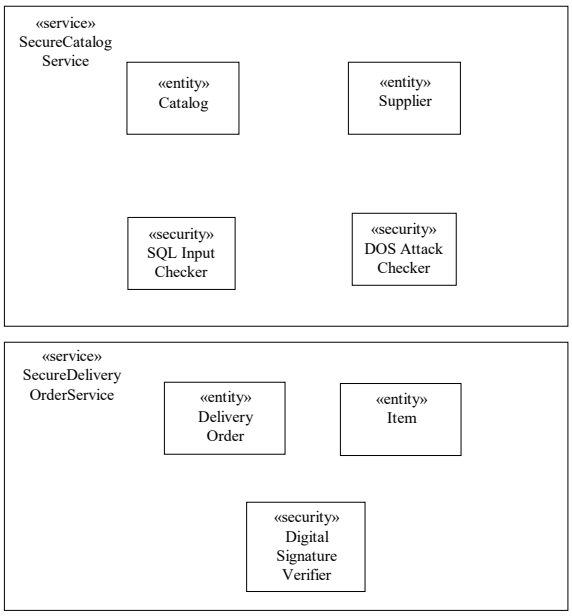

Secure SOA for Online Shopping System
«user interaction» :SecureCustomer Interaction
«user interaction» :SecureSupplier Interaction
Layer 1
Customer Request
Customer Coordinator Response
Supplier Request
Supplier Coordinator Response
«coordinator» :Customer Coordinator
«coordinator» aBilling Coordinator
«coordinator» :Supplier Coordinator
Layer 2
Store, Update, Request
Send
Ready to Shipment
Account Billed
Commit
Commit Charge
Request
Store, Update
Check, Reserve, Commit
Query, Select
Store, Update, Request
Charge Committed
Authorization Request
Catalog Info
Authorization Response
Account Info
Delivery Oder
Invoice
Delivery Oder
Inventory Info
Layer 3
«service» :SecureEmail Service
«service» :SecureCatalog Service
«service» :SecureCreditCard Service
«service» :SecureCustomer AccountService
«service» :SecureDelivery OrderService
«service» :Inventory Service

23


Secure Customer Interaction Service and Secure Supplier Interaction Service
«user interaction» SecureCustomer Interaction
«user interaction» :Customer Interaction
«security» Digital Signature Generator
«security» DOS Attack Checker
«user interaction» SecureSupplier Interaction
«user interaction» Supplier Interaction
«security» Digital Signature Generator
CS4331/CS5332 M.Shin
24

24

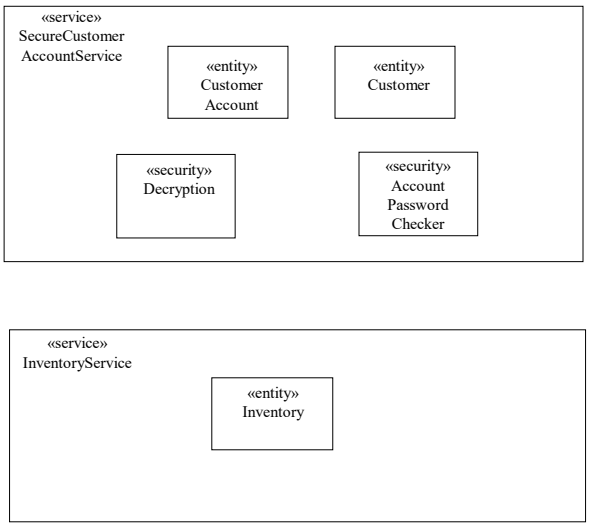
Secure Catalog Service and Secure Delivery Order Service



25

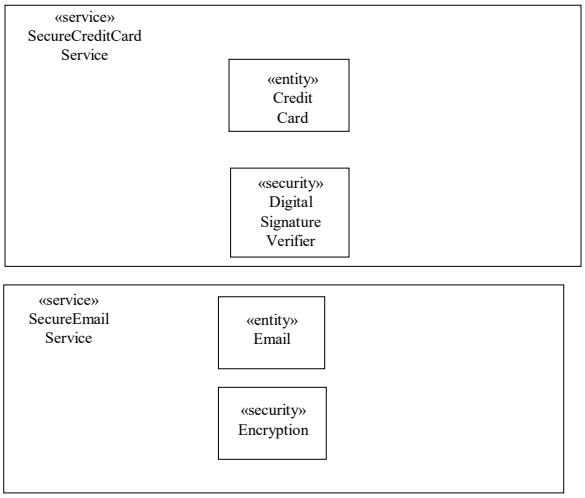
25

Secure Customer Account Service and Inventory Service



26

Secure Credit Card Service and Secure Email Service



27

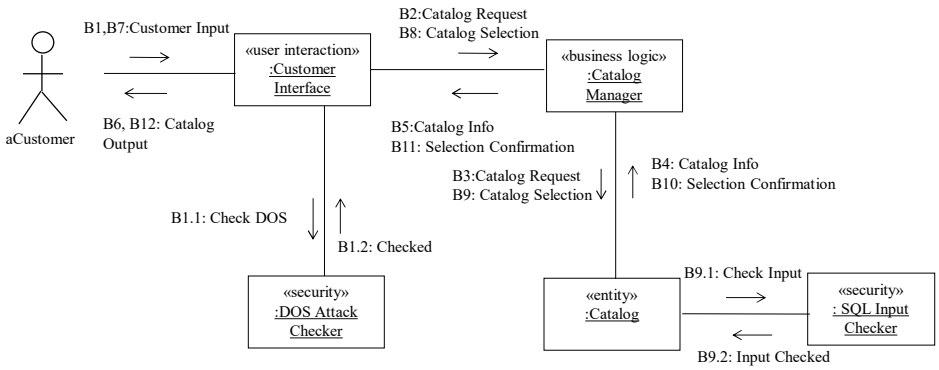
Design of Secure Client/Server Architecture

- Secure Client Subsystem sends request to Secure Server Subsystem
  - Waits for response
- Secure Server Subsystem
  - Receives Client requests
  - Processes each Client request in the order received
    - First-In First-Out (FIFO)
  - Sends response to Secure Client Subsystem

28

28

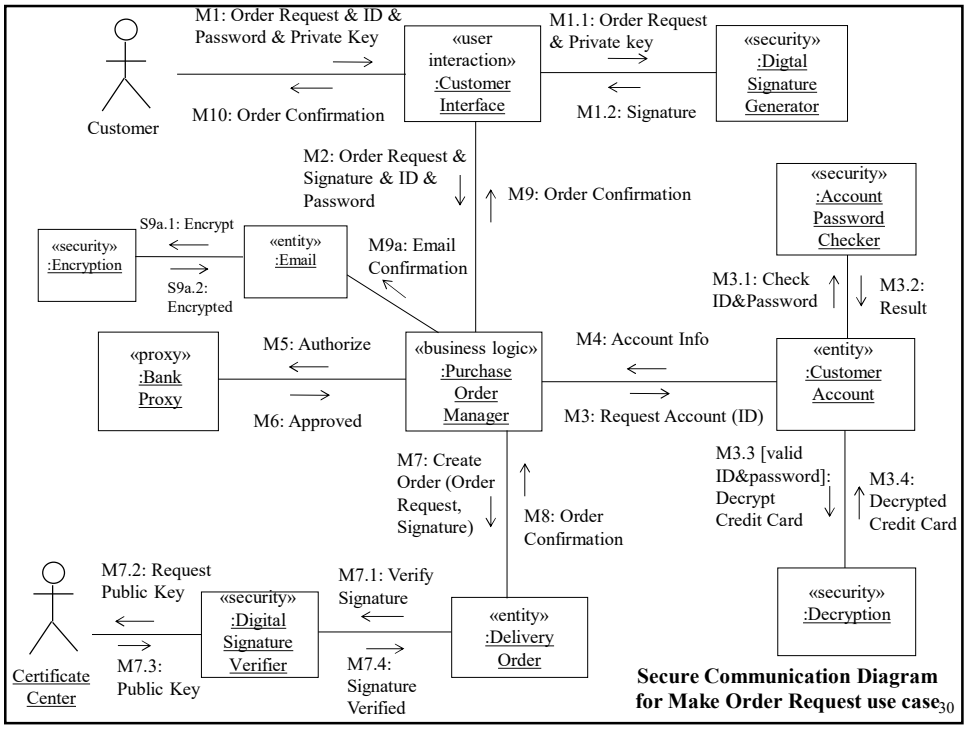
Secure Communication Diagram for Browse Catalog use case



CS4331/CS5332 M.Shin

29

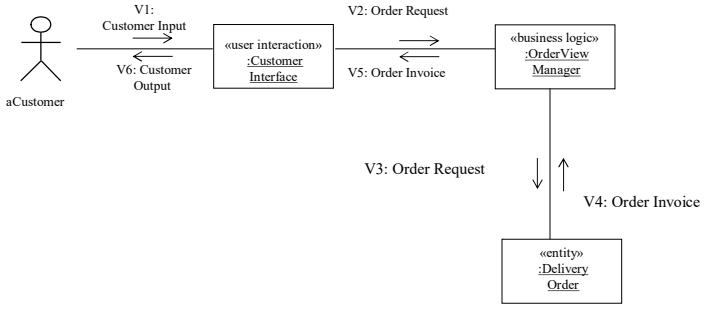
29



30

30

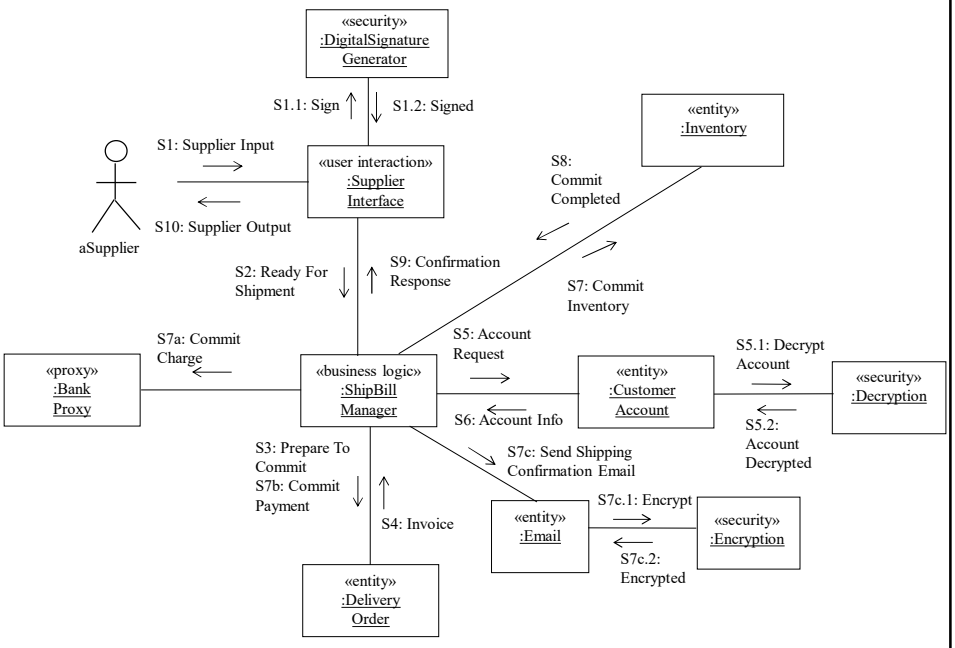
Secure Communication Diagram for View Order use case



CS4331/CS5332 M.Shin

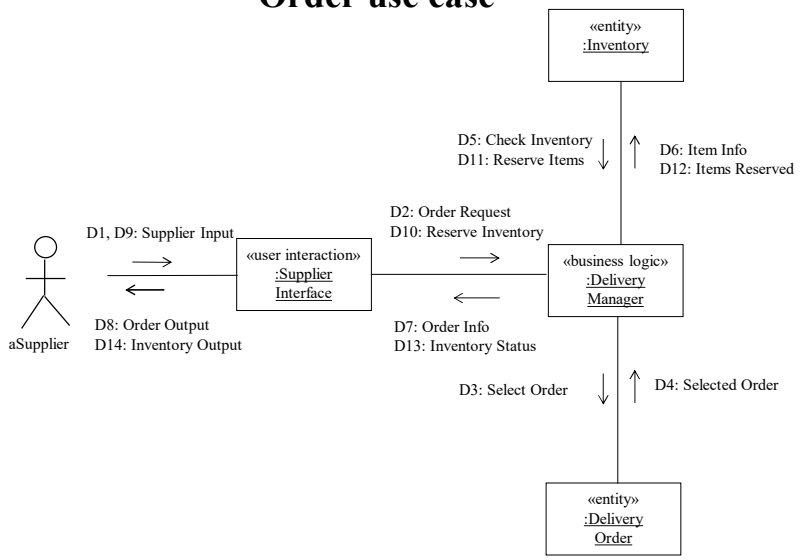
31

Secure Confirm Shipment and Bill Customer use case



32

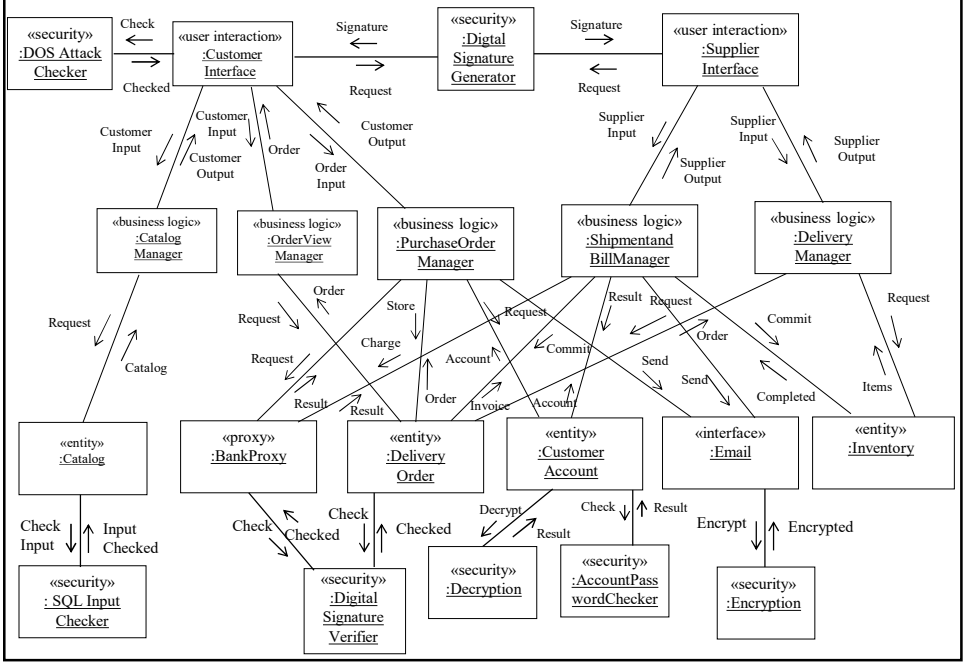
Communication Diagram for Process Delivery Order use case



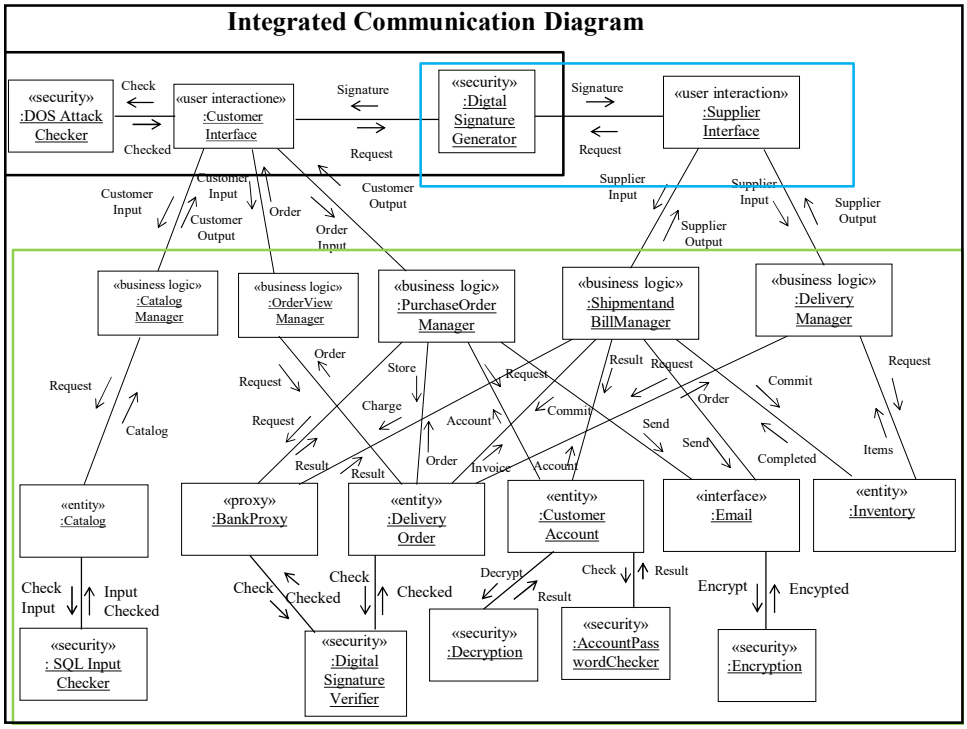
CS4331/CS5332 M.Shin

33

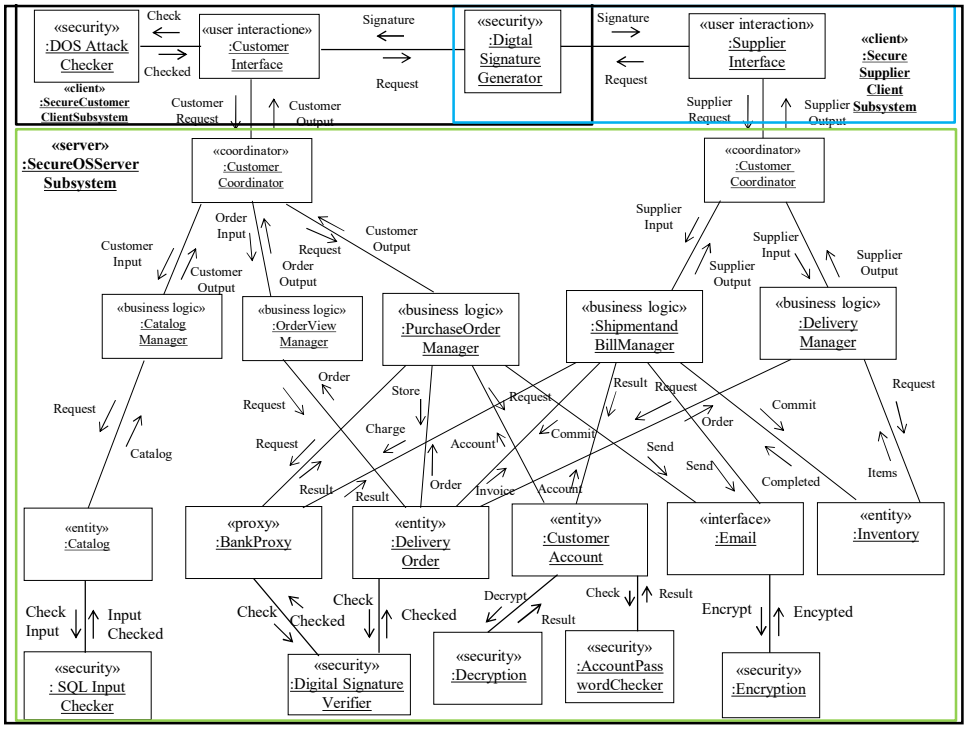
Integrated Communication Diagram



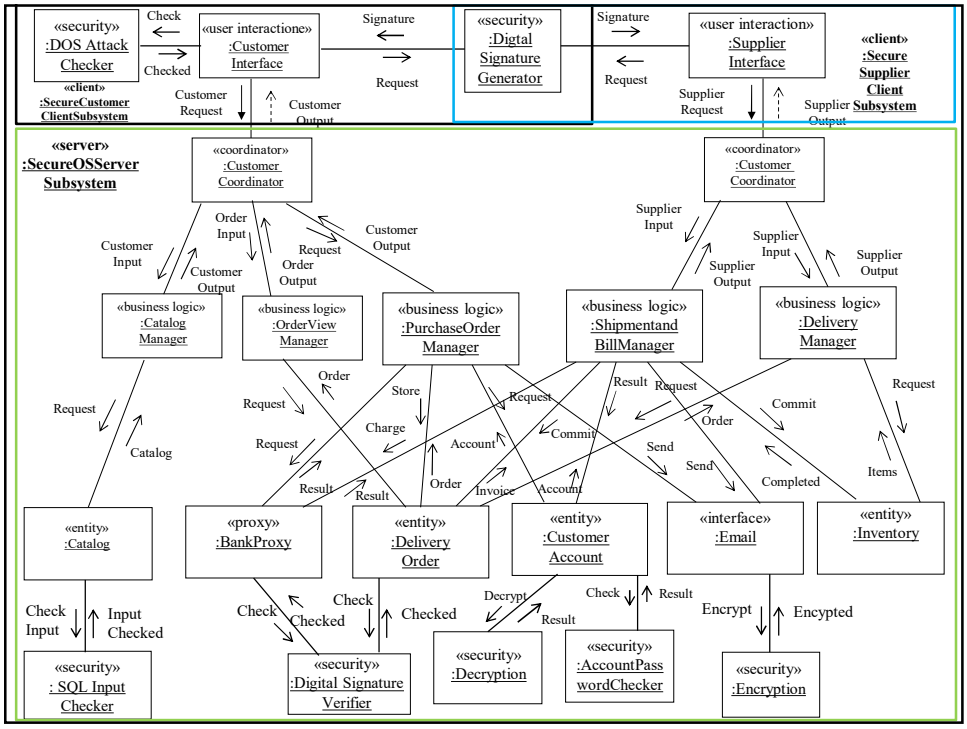
34


Integrated Communication Diagram
«security» :DOS Attack Checker
«user interactione» :Customer Interface
«security» :Digtal Signature Generator
«user interaction» :Supplier Interface
«business logic» :Catalog Manager
«business logic» :OrderView Manager
«business logic» :PurchaseOrder Manager
«business logic» :Shipmentand BillManager
«business logic» :Delivery Manager
«entity» :Catalog
«proxy» :BankProxy
«entity» :Delivery Order
«entity» :Customer Account
«interface» :Email
«entity» :Inventory
«security» : SQL Input Checker
«security» :Digital Signature Verifier
«security» :Decryption
«security» :AccountPass wordChecker
«security» :Encryption
Check
Checked
Signature
Request
Customer Input
Customer Output
Order
Order Input
Supplier Input
Supplier Output
Store
Charge
Account
Commit
Result
Invoice
Send
Completed
Items
Catalog
Decrypt
Encrypt
Encypted
Input Checked

35

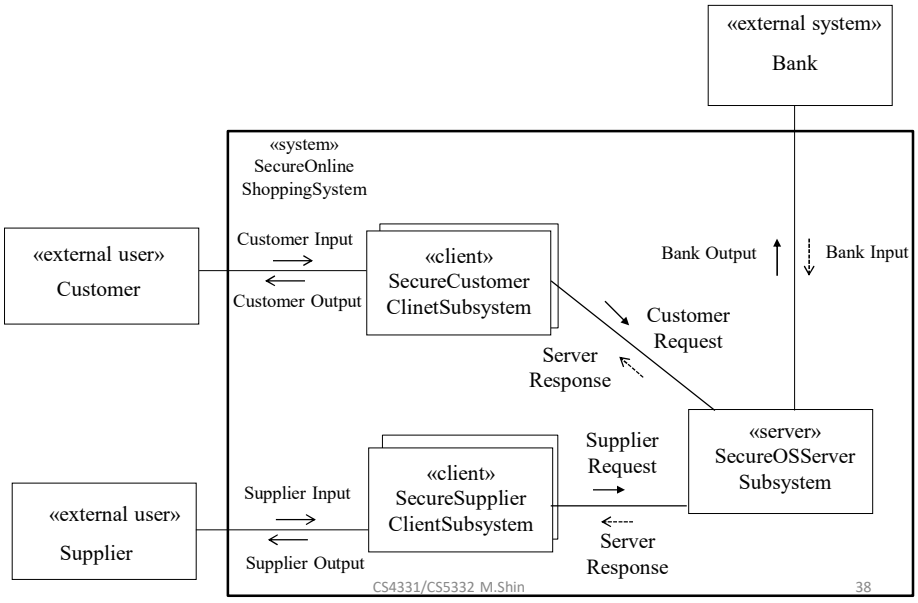

«client» :SecureCustomer ClientSubsystem
«client» :Secure Supplier Client Subsystem
«server» :SecureOSServer Subsystem
«coordinator» :Customer Coordinator
«security» :DOS Attack Checker
«user interactione» :Customer Interface
«security» :Digtal Signature Generator
«user interaction» :Supplier Interface
«business logic» :Catalog Manager
«business logic» :OrderView Manager
«business logic» :PurchaseOrder Manager
«business logic» :Shipmentand BillManager
«business logic» :Delivery Manager
«entity» :Catalog
«proxy» :BankProxy
«entity» :Delivery Order
«entity» :Customer Account
«interface» :Email
«entity» :Inventory
«security» : SQL Input Checker
«security» :Digital Signature Verifier
«security» :Decryption
«security» :AccountPass wordChecker
«security» :Encryption
Check
Checked
Signature
Request
Customer Request
Customer Output
Supplier Request
Supplier Output
Order Input
Order Output
Customer Input
Supplier Input
Store
Charge
Account
Commit
Result
Invoice
Send
Completed
Items
Catalog
Decrypt
Encrypt
Encypted
Input Checked

36



37

Secure Client/Server Architecture for Online Shopping System



38