Danmarks
Tekniske
Universitet

DTU

02244 Logic For Security

Project on Information Flow

By

Group 40

Tama Sarker	**s232913**
Reshma Zaman	**s233247**
Sheikh Atiqul Haque Saber	**s230045**

May 5, 2024

Contents

1 Introduction [s233247]

The core of Online Auctions Solutions A/S (OAS) is the implementation of security policies of the information flow of the system which need follow the model proposed by A. C. Myers and B. Liskov in the article [1]. Which offers a systematic approach to enforce security constraints within a software system, ensuring the sensitive information flows are controlled and prevented from leaking to unauthorized entities. We try to implement our system following this model to ensure that sensitive data, such as bidder information and bid amounts, is thoroughly protected against unauthorized access.

In our proposed OAS, we observe the sensitivity of the information, particularly in scenarios involving live bids, commission bids and reputation systems where the stakes are high. Commission bids, where bidders specify a maximum bid in advance, require careful handling to maintain the confidentiality of the bid amount until it becomes relevant to the auction outcome. Similarly, for live bidder we'll try to ensures that the bidder can place multiple live bids and tracking them systematically helps in enhancing user experience and operational efficiency. Our reputation systems will be designed to manage and secure customer credentials effectively, enabling auction houses to mitigate risks associated with first-time bidders by cooperating with the other auction houses and enhance trust among participants.

Our goal in this project is to exploring the techniques mentioned in Myers and Liskov article [1] and create a software solution that not only enhances the functionality of auction houses with seamless online bidding capabilities but also secures them with the highest standards of confidentiality and integrity.

2 System Overview [s233247]

At Online Auctions Solutions A/S (OAS), our software solution aims to revolutionize the auction industry by seamlessly integrating online bidding capabilities into traditional auction houses. With a focus on security and confidentiality, our system is built upon the decentralized model for information flow control proposed by Myers and Liskov [1].

Commission Bids Handling: Our system facilitates commission bids, where customers can set maximum bid amounts before the auction begins. During the auction, the auction house bids on behalf of the customer up to their maximum bid. To ensure fairness and confidentiality, bid information is pseudonymous, and customers are unaware of other bids' existence. Our system manages the bidding process dynamically, adjusting bids based on live bidding activity while maintaining bidder anonymity.

Information Flow Policy: The source code of our system includes an information flow policy, comprising a lattice of security labels and annotations for all program variables. This policy ensures that sensitive information, such as bid amounts and customer identities, is controlled and protected throughout the system. Additionally, we provide a proof that the source code never violates the information flow policy, demonstrating the integrity and security of our software.

Reputation System Integration: Reputation System Integration: To enhance trust and reliability, our system incorporates a reputation system. New customers are subject to bid value limits to mitigate risks, while returning customers enjoy higher bidding privileges based on their past transaction history. Furthermore, customers can leverage references from trusted auction houses to expedite registration and gain immediate "good customer" status, facilitated through secure information sharing between auction houses.

User Interface: We are using console line display with static data that ensure the requirement of the assignment that clarify to have the same result with matching values and inputs. Visual representation of our software solution is at Figure 1.

Overall in our online auction system, ordinary user could be a customer by registration on the system with or without the reference from another auction house, if has reference then customer status will be "good customer" otherwise status is by default "new customer" and for new customer bid limited and that is system defined. After buying product from auction new customer status will be changed as "good customer" that can place bid without limit amount. Then customer can participate to the auction with pseudo name in commission bid or online bid and after won in auction product is officially allocate to the corresponding customer. In addition, all activities by every participial are on record and stored to the system core database.

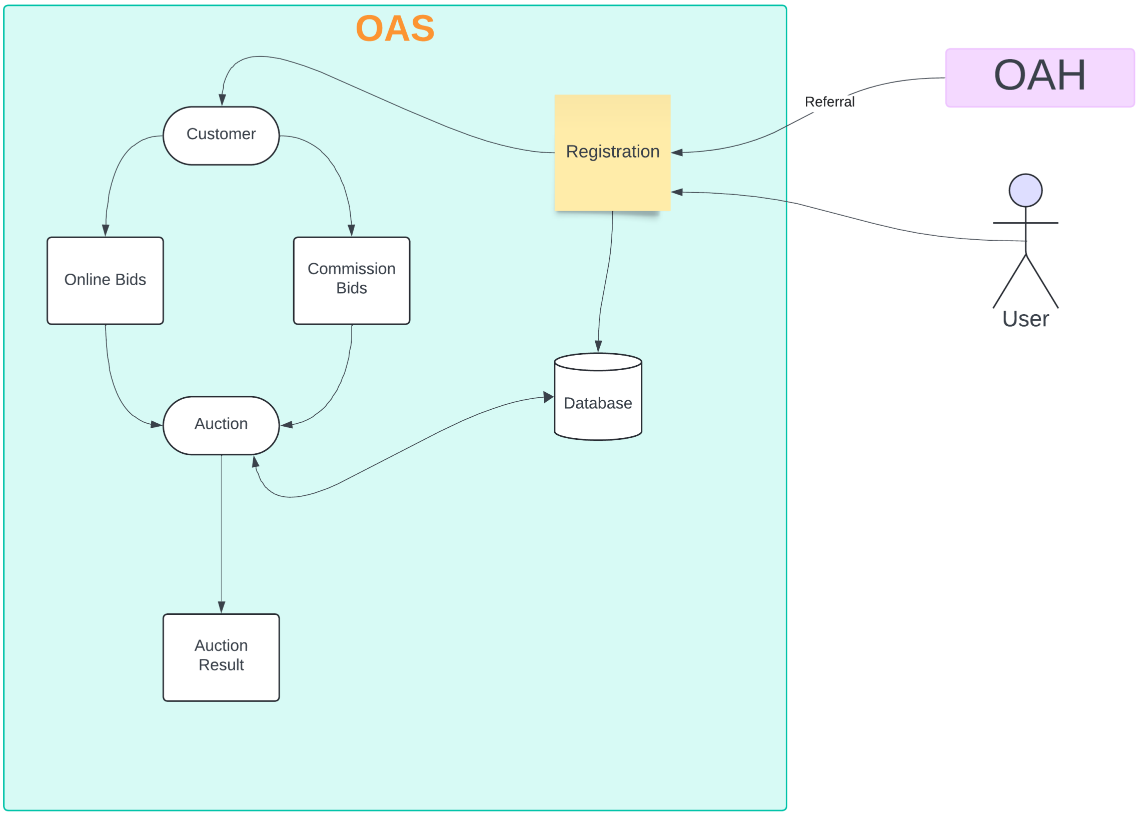


Figure 1: OAS System

By adhering to the Myers-Liskov decentralized model for information flow control [1], our software solution at OAS ensures the highest standards of security and confidentiality in online auctions. Through innovative features such as commission bids handling and reputation system integration, we empower auction houses to conduct auctions with confidence while fostering trust among bidders. OAS is committed to revolutionizing the auction industry with a secure, reliable, and user-friendly platform that sets new standards for online bidding systems.

3 Participants and Roles [s230045]

For designing the Online Auction Solution A/S (OAS) system, by considering the model of Andrew C. Myers and Barbara Liskov [1], the roles of the participants must be defined. Which emphasizes the importance of the model with a clear security label and facilitates legit control of the information flow between the participants. The list of participants and their assigned roles are given below and shown at Figure 2.

Customer (C): Customers participate in the auction by placing bids on items. They have the ability to view the current highest bid and the results of auctions in which they participate. Customers can also set up commission bids, where the auction house bids on their behalf up to a maximum specified amount. Customer has only authority of register them-self, attending auction and end of auction they can claim and pay for that product and have no access to the main system.

Auctioneer (A): The auctioneer conduct the auction, is responsible for managing the auction process. The role of it includes starting the auction, accepting bids, and declaring the final results. Also, for the commission bidder auctioneer set the max bid and system plays for the commission bidder as defined rules. The auctioneer has access to all bids and is responsible for maintaining the integrity of the auction process. In addition, Auctioneer(A) is the helping agent of core Online Auctions Solution(OAS), that other relative agents could not get access directly to the core system, supposing after strong authentication and with secure channel Auctioneer is connected to the OAS.

Online Auction Solution (OAS): The back-end infrastructure of the auctions are handled by OAS. It processes all the data related to the auction, maintains the auction and customer databases including the customer registration process and ensures that all transactions adhere to the specified security policies. OAS is the core system that is responsible for all security and information flow management. More specifically, all type of data are sanitized and process before storing to the main database to ensure no data leakage, confidentiality, authenticity and integrity.

Other Auction House (OAH): For a customer who wants to get cross reference from the other auction houses where he has a profile or status and may want to participate in joint auctions, then OAH may interact with OAS for that. This interaction allows customers from one auction house to be recognized as reputable by another, facilitating a broader trust network.

4 Security Goals [s230045]

To maintaining a robust information flow control within an Online Auctions Solutions A/S (OAS), the article of Myers and Liskov [1] outline some essential series of security goals. Which require stringent data protection/confidentiality and integrity.

4.1 Confidentiality

Confidentiality refers to prevent unauthorized access to sensitive information. Here's an overview of how we planning to ensure this security goals as per our participants of the system:

Customer: The information of customers identity and the amounts of their bids kept confidential from other bidders and the public. This ensures that no strategic bidding against a specific bidder can occur, and personal data remains secure. Customer to places offline bids knows as commission bids, where the customer sets a maximum bid in advance, are particularly sensitive as it reveal the customer's willingness to pay and it'll remain undisclosed until they influence the auction outcome.

Auctioneer: The auctioneer have access to sensitive information and ensures that this information is not disclosed inappropriately. Which includes maintaining the confidentiality of bidder identities and the amounts of their maximum bids. Auctioneers also handle internal operational data that should not be exposed to customers or external entities to maintain strategic and operational security.

OAS: The OAS system manages all data transactions and storage. All the data, especially that which is marked confidential, such as user accounts and bid information, is protected against unauthorized access. Access controls and encryption is employed for the storage of the sensitive data and transmission of the data.

OAH: When interacting with other auction houses, particularly in the context of reputation systems or cross-auction participation, the confidentiality of shared data will be maintained. This include bidder reputations and historical bid data. Agreements and protocols should define what information can be shared and the mechanisms for secure data exchange.

4.2 Integrity

Integrity refers to preserve the accuracy and completeness of data throughout its transformations. Below is the overview of how we planning to ensure this security goals as per our participants of the system:

Customer: The integrity of a customer's bid is paramount; it recorded and processed accurately to reflect the true intent of the bidder. As any sort of alteration could lead to mistrust and financial discrepancies.

Auctioneer: The auctioneer is responsible for the integrity of the auction process, ensuring that all bids are processed fairly and transparently. As a sub process of OAS, it includes overseeing that bid increments follow the set rules and that the final sale is awarded correctly according to the highest bid.

OAS: For maintaining the correctness of auction operations, from bid placement to auction conclusion its important to maintain system integrity. This includes ensuring the accuracy and reliability of data handling and processing within the system.

OAH: The integrity of data received from other auction houses or sent to them is critical, especially when such data can affect auction outcomes or bidder reputations. We will make sure to verifying the authenticity and accuracy of shared data, which is necessary to prevent fraud and misinformation.

5 Design Choices and Reasoning [s232913]

This part illustrates the implementation of security system in the auction system OAS. It construct the lattice model using security labels. Here, we ensured the data authorisation and confidentiality but with the appropriate interactions.

The security lattice for this system consists of various levels of security, representing different roles and the types of data handled in the auction system.

In the figure 2 following Mayer and Liskov[1], an oval represents a principal within the system, and is labeled with a boldface character that indicates the authority with which it acts. Arrows in the diagrams represent information flows between principals; square boxes represent information that is flowing, or databases of some sort; double ovals represent trusted agents that declassify information and can act on behalf of a participle in the system. Each principal can independently specify policies for the propagation of its information indicated by labels of the form **{O : R}** , meaning that owner allows the information to be read by readers , where is a principal and is a set of principals and owner is the source of any information having the authority of controlling the policy.

For example in OAS system, Customers represented by **C**, Auctioneer represented by **A**, Online Auction Solutions represented by **OAS**, Other Auction Houses represented by **OAH**.

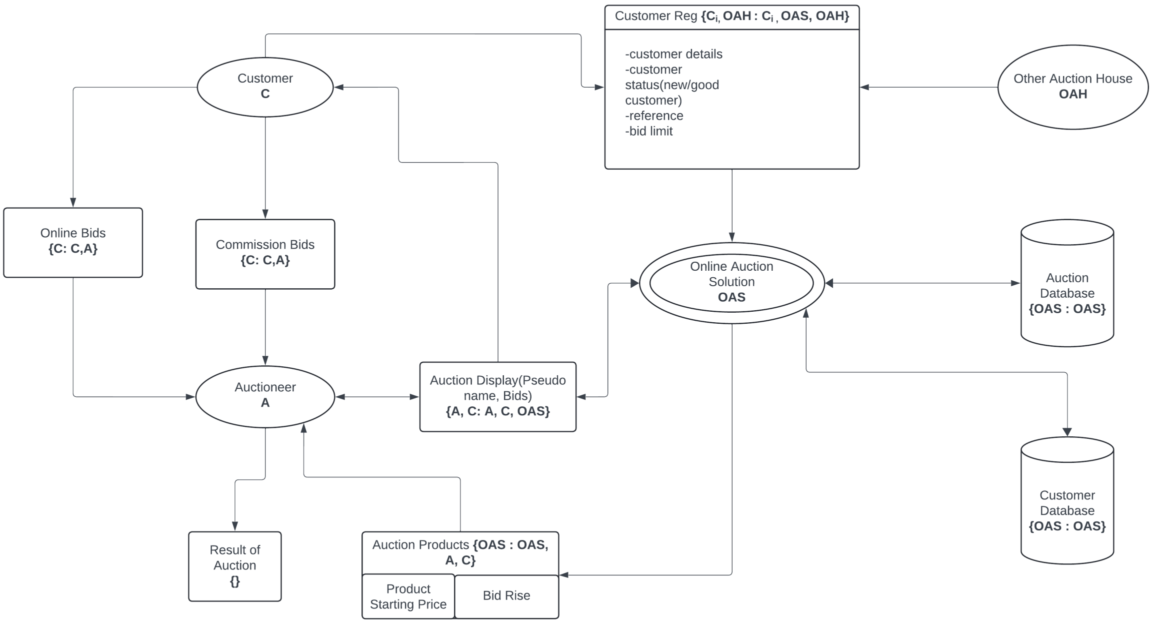


Figure 2: Information Flow of OAS

Each component of the system is labeled according to its security needs and changed depending on process to process like during login, online bids and commission bids placing, auction conducting, auction logs, databases, auction results and so on.

Customer Registration information containing customer information is labeled as {Ci, OAH : Ci, OAS, OAH} because owner of this piece of information is Ci, OAH and accessed by individual customer, OAS and OAH, if has referral, as during registration information of customer is known to these principals. Same for Online and Commission Bids labeled as {C : C, A}, Auction Display, containing information of live bid and visible to the customer about the product as well as live auction status, labeled as {A, C : A, C, OAS}. Database of Auction and Customer labeled as {OAS: OAS}, containing the auction result with the corresponding detailed of owner and other relative details. Auction products information are owned by the OAS but there are other readers A,C as starting price and bid rise is known to the customer-Auctioneer and also OAS so the label is {OAS : OAS, A, C}. At last, Result of Auction is labeled as {} since it's maintained by the corresponding owners and should only be accessed by trusted entities.

Every role has its own set of access rights. Auctioneer can retrieve any data of the commission as well as live bids while on the other hand, a customer can access auction results and their own data. This fairness comes with it being that only the authorized entities will be able to view the data.

The lattice architecture provides a joining operation which accommodates security labels, and the restriction operation operates to prevent flow of data to unauthorized entities.

6 Justification for Declassification [s232913]

Declassification is a critical component in the management of information flow within secure systems, particularly when dealing with sensitive or classified information that can become less sensitive over time or under certain conditions [3]. The process during which security classification is removed from certain documents and their information spreads to more extensive audiences. In this section, we'll justify when and why declassification is required in our proposed system. Below are the few scenarios for Declassification:

- **Customer Registration Declassification:** During customer registration information of individual customer C and in-case of reference from other auction house OAH is owner of that information but after registration completion OAS will save that into system database that is only accessed and control by the OAS. For that reason as a trusted agent OAS act behalf of the owner of this information and declassify the label from {Ci, OAH : Ci, OAS, OAH} to {OAS: OAS}.

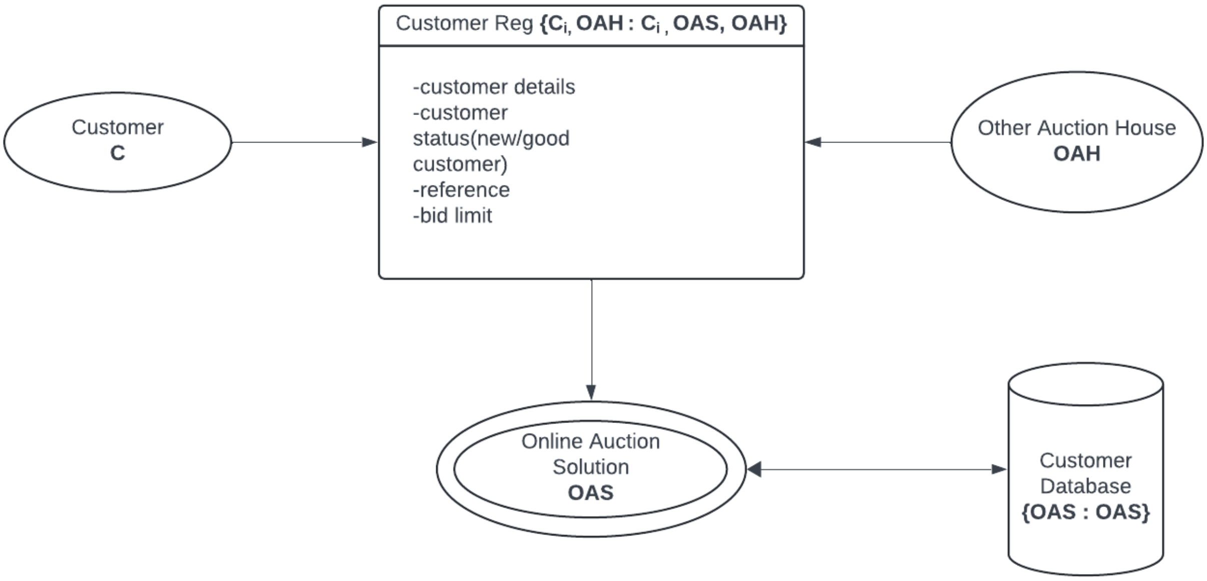


Figure 3: Registration Declassification

- **Commission and Online Bids Declassification:** Declassification is required when a live bid matches or exceeds a commission bid. This ensures the auction house can conduct the auction correctly, informing live bidders of their status without revealing the maximum commission bid. During placing bids the security lattice was owned by the customer C and reader was C and Auctioneer A but on the display screen information was shared to the other customers and also OAS for keep tracking of the auction so here needs declassification to adding the owner A as {C : C, A} to {A,C : A, C, OAS} and then OAS again declassify to save to the core database so that restricted data accessed by only OAS, labeled changed as {A,C : A, C, OAS} to {OAS: OAS}.

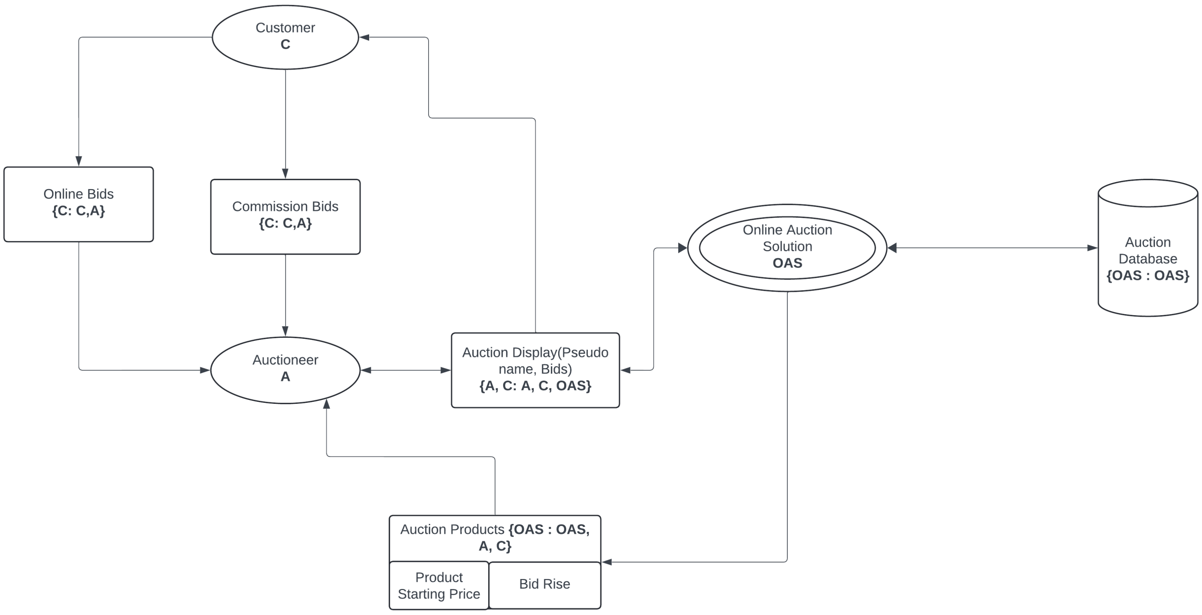


Figure 4: Bids Declassification

- **Auction Results Declassification:** The final auction result must be declassified in two part with multiple steps, one is for storing auction result to the system database and other is for public declaration, this justifies revealing which customer won the auction and the final bid price. During auction there was finite owner and restricted view but for storing to the database there is only one owner and reader that the label changed from {A,C : A, C, OAS} to {OAS: OAS}. For auction result, it is open for public so there are no specific owner and everyone is reader, here denoted as { } and the data is declassified from {OAS: OAS} to {A,C : A, C, OAS} to { }.

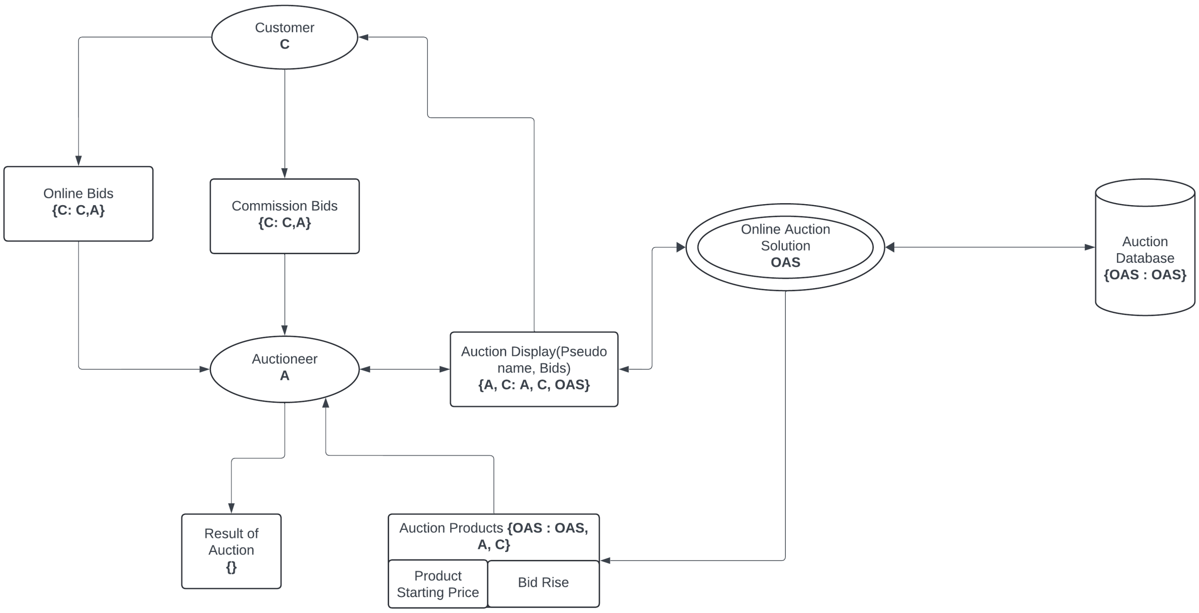


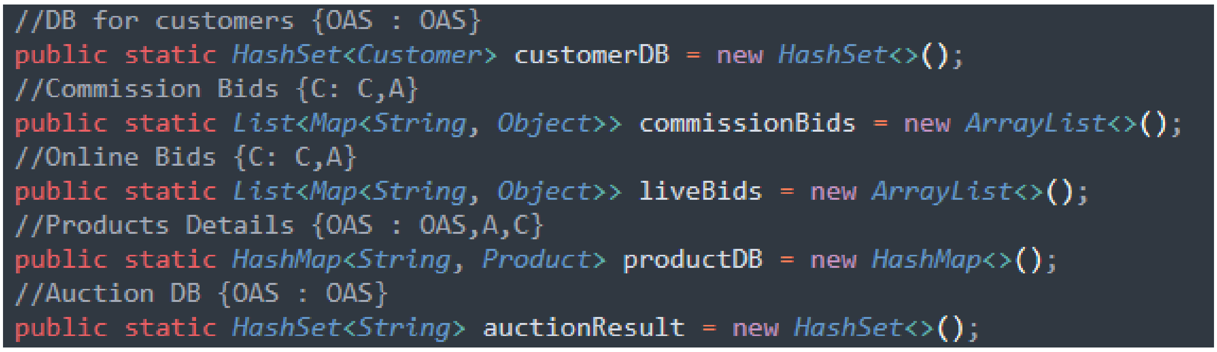
Figure 5: Auction Result Declassification

So, declassification is carefully controlled to avoid unintended information leakage. The system ensures that declassification only occurs in specific scenarios, like registration or matching bids or public auction results, thus the auction system can maintain security and confidentiality while allowing for necessary information flow and public visibility.

7 Information Flow Analysis [s230045]

The information flow analysis we delve into the mechanisms by which data moves throughout the Online Auction Solutions A/S (OAS) system, ensuring strict adherence to established security policies, particularly focusing on maintaining confidentiality and integrity across different security levels defined in Denning's model. This analysis will detail the flow of sensitive information within the system, identifying potential risks and ensuring that data flows do not violate the security labels assigned based on the principles outlined in Denning's IFC approach[2]. Here's an analysis of our java code is provided:

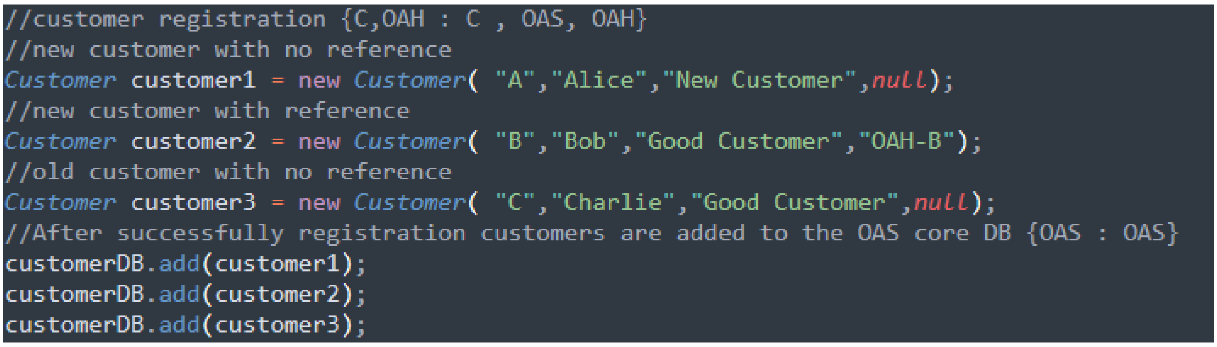
Database and its accessibility is mentioned in the Figure 6, where the security label followed by the article of Myers and Liskov [1] is described through comments in the code.



```
//DB for customers {OAS : OAS}
public static HashSet<Customer> customerDB = new HashSet<>();
//Commission Bids {C: C,A}
public static List<Map<String, Object>> commissionBids = new ArrayList<>();
//Online Bids {C: C,A}
public static List<Map<String, Object>> liveBids = new ArrayList<>();
//Products Details {OAS : OAS,A,C}
public static HashMap<String, Product> productDB = new HashMap<>();
//Auction DB {OAS : OAS}
public static HashSet<String> auctionResult = new HashSet<>();
```

Figure 6: Databases Accessibility

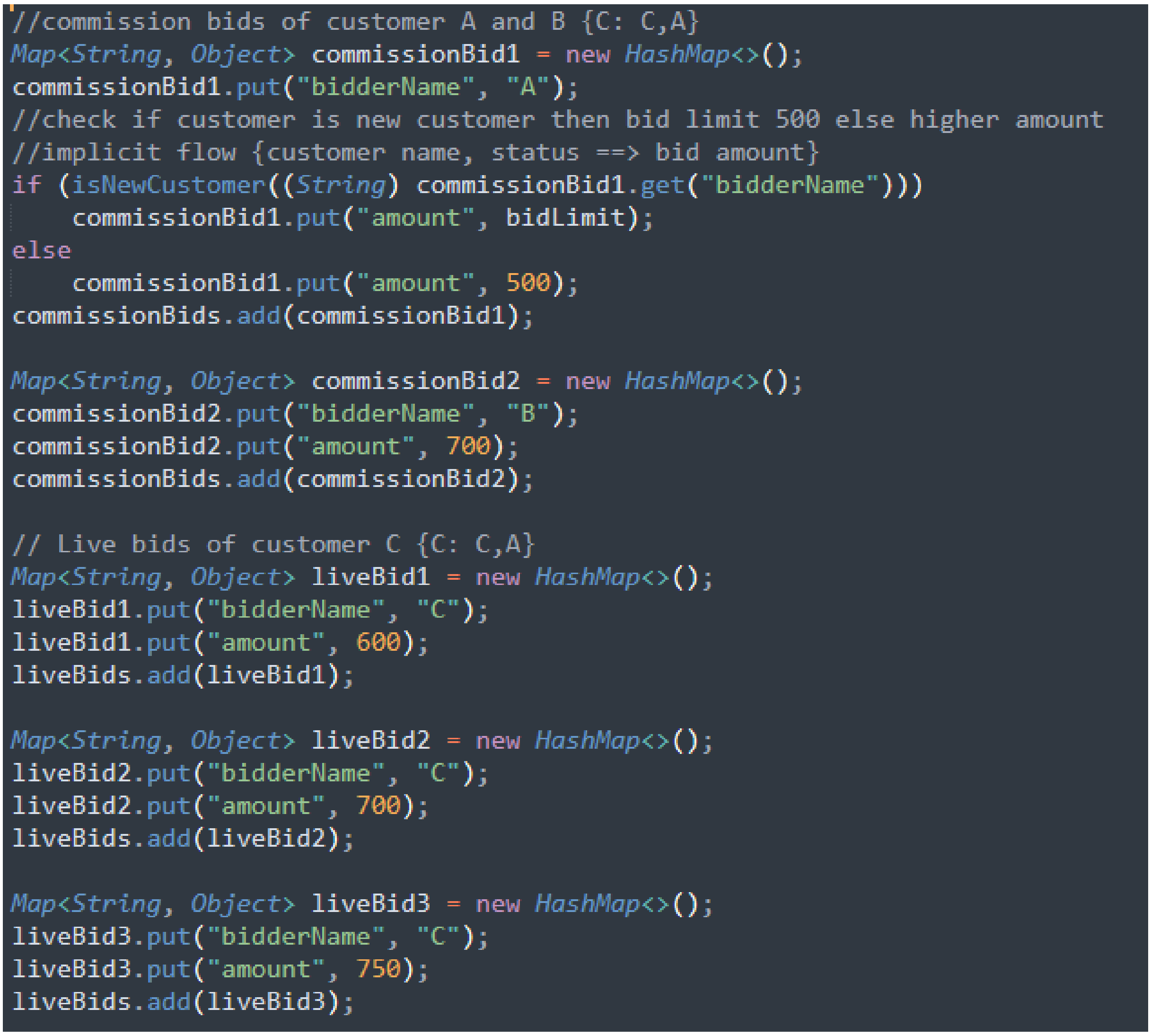
While a new customer is registering in the system showed in Figure 7, either customer with or without reference, the data flow from customer interface to system core database, where the labeled changed from {C, OAH : C , OAS, OAH} to {OAS : OAS}.



```
//customer registration {C,OAH : C , OAS, OAH}
//new customer with no reference
Customer customer1 = new Customer( "A","Alice","New Customer",null);
//new customer with reference
Customer customer2 = new Customer( "B","Bob","Good Customer","OAH-B");
//old customer with no reference
Customer customer3 = new Customer( "C","Charlie","Good Customer",null);
//After successfully registration customers are added to the OAS core DB {OAS : OAS}
customerDB.add(customer1);
customerDB.add(customer2);
customerDB.add(customer3);
```

Figure 7: Data Flow on Customer Registration

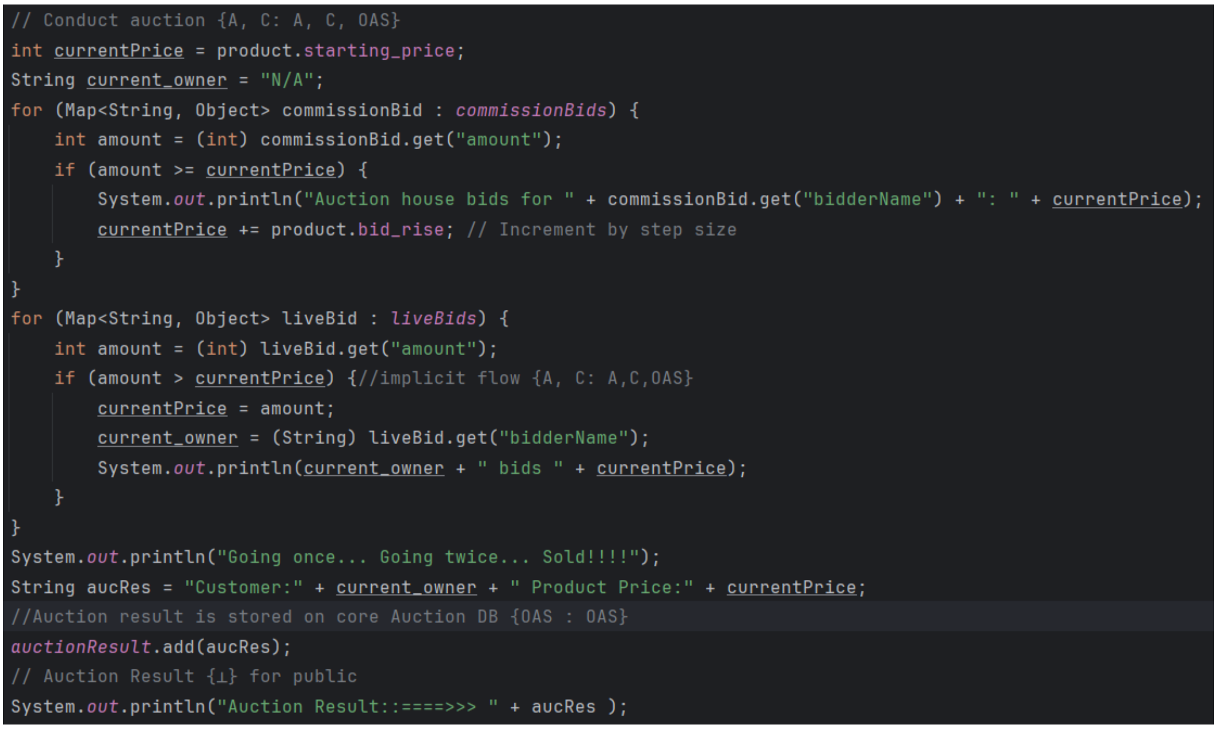
Figure8, demonstrates how the system handles bids from various customers, distinguishing between new and returning customers for commission bids and managing multiple live bids from the same customer. Also, using the (HashMap and List) aids in logging and auditing bid activities implies the essential for dispute resolution and system transparency. During online and commission bids the confidentiality of the customer and auctioneer are followed by the security label which indicate its transparency and during auction data flow from auctioneer to OAS core database, labeled as {C: C,A} to {A, C: A, C, OAS}.



```
//commission bids of customer A and B {C: C,A}
Map<String, Object> commissionBid1 = new HashMap<>();
commissionBid1.put("bidderName", "A");
//check if customer is new customer then bid limit 500 else higher amount
//implicit flow {customer name, status ==> bid amount}
if (isNewCustomer((String) commissionBid1.get("bidderName")))
    commissionBid1.put("amount", bidLimit);
else
    commissionBid1.put("amount", 500);
commissionBids.add(commissionBid1);

Map<String, Object> commissionBid2 = new HashMap<>();
commissionBid2.put("bidderName", "B");
commissionBid2.put("amount", 700);
commissionBids.add(commissionBid2);

// Live bids of customer C {C: C,A}
Map<String, Object> liveBid1 = new HashMap<>();
liveBid1.put("bidderName", "C");
liveBid1.put("amount", 600);
liveBids.add(liveBid1);

Map<String, Object> liveBid2 = new HashMap<>();
liveBid2.put("bidderName", "C");
liveBid2.put("amount", 700);
liveBids.add(liveBid2);

Map<String, Object> liveBid3 = new HashMap<>();
liveBid3.put("bidderName", "C");
liveBid3.put("amount", 750);
liveBids.add(liveBid3);
```

Figure 8: Data Flow on Placing bids and Conducting Auction

At the end of the auction, the result is published with pseudo-name of the customer for the public at Figure9, where declassification happened and data flow from auction display to public, labeled as {A, C: A, C, OAS} to { }. And before that an implicit flow {A, C: A, C, OAS}, reflecting the sensitive nature of the auction operations where data flows carefully managed to prevent unauthorized information leakage. Also for storing the auction result to the code database declassification labeled as {A, C: A, C, OAS} to {OAS : OAS }, where all changes to current_owner and currentPrice logged with timestamps and bidder information in the database to enable traceability and auditing.



```
// Conduct auction {A, C: A, C, OAS}
int currentPrice = product.starting_price;
String current_owner = "N/A";
for (Map<String, Object> commissionBid : commissionBids) {
    int amount = (int) commissionBid.get("amount");
    if (amount >= currentPrice) {
        System.out.println("Auction house bids for " + commissionBid.get("bidderName") + ": " + currentPrice);
        currentPrice += product.bid_rise; // Increment by step size
    }
}
for (Map<String, Object> liveBid : liveBids) {
    int amount = (int) liveBid.get("amount");
    if (amount > currentPrice) {//implicit flow {A, C: A,C,OAS}
        currentPrice = amount;
        current_owner = (String) liveBid.get("bidderName");
        System.out.println(current_owner + " bids " + currentPrice);
    }
}
System.out.println("Going once... Going twice... Sold!!!!");
String aucRes = "Customer:" + current_owner + " Product Price:" + currentPrice;
//Auction result is stored on core Auction DB {OAS : OAS}
auctionResult.add(aucRes);
// Auction Result {⊥} for public
System.out.println("Auction Result::====>>> " + aucRes );
```

Figure 9: Data Flow on Auction Result

So, with these considerations of declassification, audit-ability and traceability, role base access and proper label management, the information flow analysis ensures that the program adheres to handle the sensitive information in prescribed security boundaries. And the information is only declassified and made public under controlled and secure conditions. Which shows the integrity and confidentiality of the auction process, thereby maintaining trust and reliability in the auction system's operations.

8 Conclusion [s233247]

In conclusion, as we wrap up our exploration into the development of a secure online bidding system for small auction houses, it is evident that the decentralized model for information flow control proposed by Myers and Liskov serves as the cornerstone of our approach at Online Auctions Solutions A/S (OAS). Through meticulous adherence to this model, we have endeavored to ensure the highest standards of security and confidentiality within our software solution.

The use cases of commission bids and reputation systems have underscored the importance of maintaining strict confidentiality measures while facilitating seamless transactions within the auction environment. With commission bids, our system must guarantee that bidders remain pseudonymous to each other and that bid information is disclosed only as necessary to facilitate fair bidding. Similarly, in reputation systems, the exchange of information between auction houses must be handled securely to prevent unauthorized access to customer data.

By delivering source code with an information flow policy that includes a lattice of security labels and comprehensive annotations, along with a proof of adherence to this policy, OAS aims to instill confidence among auction houses in the security and reliability of our software solution. As a student working on this project, I am confident that our commitment to the Myers-Liskov model will pave the way for a new standard of excellence in online auction technology, setting OAS apart as a trusted partner in the auction industry.

References

[1] Barbara Liskov Andrew C. Myers. “A Decentralized Model for Information Flow Control”. In: *Proceedings of the 16th ACM Symposium on Operating Systems Principles*. ACM. 1997, pp. 129–142.

[2] Dorothy E Denning and Peter J Denning. “Certification of programs for secure information flow”. In: *Communications of the ACM* 20.7 (1977), pp. 504–513.

[3] Richard Sizer. *Security and Control of Information Technology in Society: Proceedings of the IFIP TC9/WG9. 6 Working Conference on Security and Control of Information Technology in Society on Board M/S Ilich and Ashore at St. Peterburg, Russia, 12-17 August 1993.* Vol. 43. North-Holland, 1994.