TÉCNICO LISBOA

Network and Computer Security

BlingBank

Group 43

99300 Pedro Rodrigues

99340 Tomás Marques

102314 Renato Martins

TÉCNICO LISBOA

The Secure Document Format

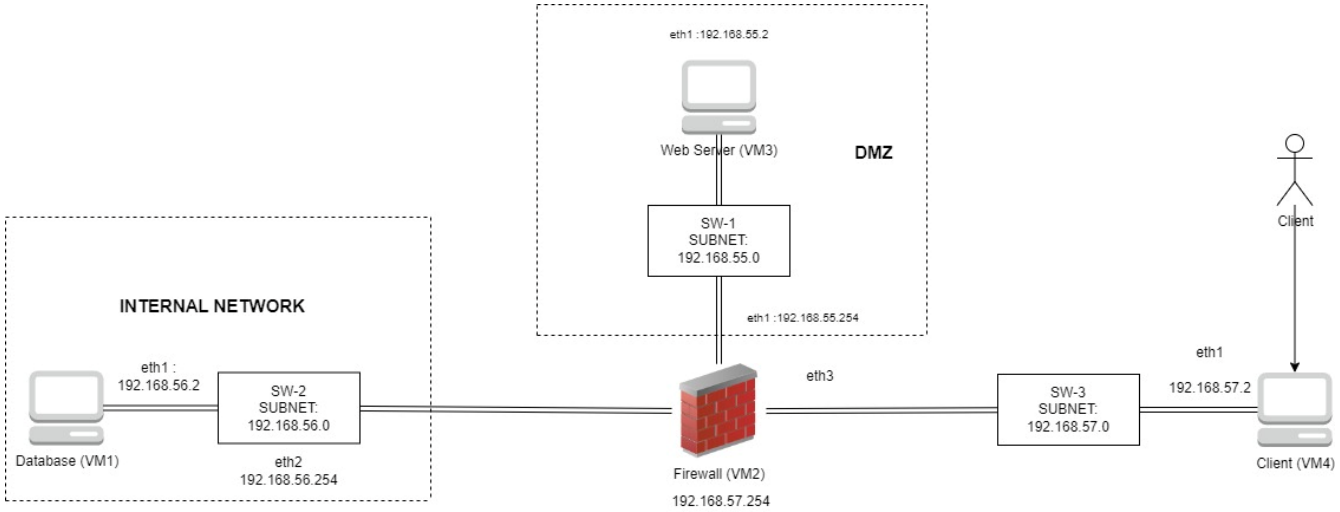
- Advanced Encryption Standard (AES) in Galois/Counter Mode (GMC)
- Digital Signatures using RSA (asymmetric criptography)


```
{
    "account": {
        "balance": 862.22,
        "currency": "EUR",
        "movements": [
            {
                "date": "09/11/2023",
                "value": 1000.0,
                "description": "Salary"
            },
            {
                "date": "15/11/2023",
                "value": -77.78,
                "description": "Electricity bill"
            },
            {
                "date": "22/11/2023",
                "value": -50.0,
                "description": "ATM Withdrawal"
            },
            {
                "date": "02/01/2024",
                "value": -10.0,
                "description": "BK"
            }
        ],
        "accountHolder": [
            "Alice",
            "John"
        ]
    }
}
```



```
{
    "account": {
        "balance": "aak6mgblvSMHC5irTro916XtkShB7qx6wDWU/v0SlXeBkwWh3R/EzTNEh0mNN
        "currency": "QpdGhh7xve8bbGXhdqqFwpeyCnIU+slWsgJ4IpHnRO055WDfz9NagvESXUbl
        "movements": [
            {
                "date": "aTCNTI3BrFgjMwxl4CWFBZxU/xvTwa6jftlh/ajEBmL6V+dN3g5T1gaC
                "value": "JOCkQmLnfNz14u4cFOMhkNr5wHHBAc3JPObotxbYb+wQpVvWlj+QTDf
                "description": "SLvKaLpb2dQ5AvfDL1YCPVTPG20rK8swJvM+Ecvko0RlpUvNP
            },
            {
                "date": "hB9fX7jTa8Co/Iz88HTBlsy17GTunAnzdTzYxdBb/8RLISJaqUOcV9En
                "value": "K3b8IGCW7TZGe9G+79QAwvgZn6F5vjBHApGyd4LFphMvv0NxHpoyXX8
                "description": "OHzZYUgxLgWH5PSTOg/A4d2z4Hf6WBgSQCk2+S70sjubcudnt
            },
            {
                "date": "ZXXMHbQUbQrxsaxNbkTfRvKXfZMkVx5eNcf0BSDOEWy0ByofPvqwIH7T
                "value": "EQFZpEby+VNq/xjkmo86Kr1sfzzjBzjzEeZwNbKGucgvMkZ4ct4CPx7
                "description": "uqIV1yv8wvQrS8GklkLNpVuXNi6Y/BYcLM8FJ+ycHDe0K79W8
            },
            {
                "date": "pWBz6d/grV/rYiAyiID6joi+Re438WeSJe3HlHCMvusmyB/snSaTmkJm
                "value": "TgfqWS4WEuAzi8ajlk9L+qxbIq4vN1nDHlX3Ugf/bPQ3MSzjYV70Rw4
                "description": "oj1dakG4448ahTvxyhaA+J3mzlHPFh0Wij2+kY8POSHj4jq7p
            }
        ],
        "accountHolder": [
            "Sdn25bzUOIdaPYeuSOwY9NKLkA3rOl7Up11wlesL18YOoTXpCvJU8SzwuacLen/w8tAA
            "F8hVqpBx4evZolnH0l2TAJUbpN8ec+dmBOFc7jzbUc5iPL45ZomD4uQfd4Q8IZfO5mw4
        ]
    },
    "mac": "sx47yYeiKiqZmPCt4tVo+2taBUXqKMX4OXM9hCzKeJM\u003d",
    "integrity": "r3tG0fpP9XWj7uNxGMB1eKi332+HserVQVKya95MW5c\u003d",
    "timestamp": 1704215463101,
    "sequenceNumber": 1718422322
}
```

Infrastructure



INTERFACE	SUBNET	ADAPTER	ADAPTER NAME
Client Machine 1	192.168.57.2	eth1	SW-3
Firewall Machine 1	192.168.55.254	eth1	SW-1
2	192.168.56.254	eth2	SW-2
3	192.168.57.254	eth3	SW-3
Webserver Machine 1	192.168.0.2	eth1	SW-1
Database Machine 1	192.168.1.2	eth1	SW-2

Network Table

TÉCNICO LISBOA

Secure Channels and Key Distribution

- Dynamic key distribution system that regularly updates user keys
- TLS Secure Sockets between client and server entities
- Mutual Authentication to ensure confidentiality
- Servers and Client have own certificate and private key save in the keystore
- Each entity have other entity certificate and CA certificate in the truststore
- Each entity validates the other certificate chain with the CA's certificate

Key Distribution	
Client	Server
Server	Database

TÉCNICO LISBOA

Security Challenge

1. Introduce a *new document format for payment orders* ensuring confidentiality, authenticity and non-repuditation
2. Implement robust freshness measures to *prevent duplicate executions* of the order
3. Require *authorization and non-repudiation* from all owners of an *account with multiple owners*

TÉCNICO LISBOA

Security Challenge

1. Introduce a ***new document format for payment orders*** ensuring confidentiality, authenticity and non-repudiation

```
{
    "date": "02/01/2024",
    "value": "10.0",
    "description": "BK ",
    "destinationAccountHolder": "Bob"
}
```

```
{
    "date": "AsuTt62FPFMar+ch+HQkjh8SrKtB6S9yJKv1b5BXgLG/Pgx7Kf3PAHi+r+/QgnyMYS0jZ2fCM5JGZ5klp8SXMEB+Ek
    "value": "WeTSxK0QqbjzKxk+sNvlSTBCc0bbXifO0QfpXOd9+97qusG0lMhvl3hljZoOgzHw4sqBHewJPXYPLnHOx4DBg9wf2
    "description": "DF57qiAFrA6n3TAAsTIYrEWVA9htejDD5MifVH1ESwzxPUiREho7YfAlxSBJMMhEdpoGKtBsqg3RqF6ufxc
    "destinationAccountHolder": "seno2FXG2VLlaLhBeixzXK5Wes3CmI7D5AYuBDVWhamU85ExBdDv/JWtBNt6ugGbHU0yeI
    "mac": "pN9qhU4drDCrpLDIJD6M72z14YWsDnx36IuCFbI/9Xs\u003d",
    "integrity": "9Sgn7YFSy2q6aQE67nSAhHSuajXcgZgl8JQ4Km0Tkks\u003d",
    "timestamp": 1704215409439,
    "sequenceNumber": -23597283
}
```

TÉCNICO LISBOA

Security Challenge

2. **Implement robust freshness measures to *prevent duplicate executions* of the order**

UNIQUE SEQUENCE NUMBER AND TIMESTAMP FOR EACH TRANSATION AND SERVER VERIFICATION

Security Challenge

3. Require ***authorization and non-repudiation*** from all owners of an ***account with multiple owners***

```
Welcome to A43 Insurance & Banking: BlingBank
Please enter your username to login: Alice
Type: 'exit' to close the connection

client received 50 bytes: connection (login) processed by server sucessfully

payment Bob 10.0 BK
sending message: payment Bob 10.0 BK
debug: secret key updated
debug: mac added
debug: integrity hash added
debug: timestamp added
debug: unique sequence number added
debug: message has been signed
```

```
[INFO]
[INFO] ------------------------< pt.tecnico.sirs:A43 >-------------------------
---
[INFO] Building A43 1.0.0-SNAPSHOT
[INFO] --------------------------------[ jar ]---------------------------------
---
[INFO]
[INFO] --- exec-maven-plugin:1.6.0:java (default-cli) @ A43 ---
Welcome to A43 Insurance & Banking: BlingBank
Please enter your username to login: John
Type: 'exit' to close the connection

client received 50 bytes: connection (login) processed by server sucessfully
```

```
Welcome to A43 Insurance & Banking: BlingBank
Please enter your username to login: Alice
Type: 'exit' to close the connection

client received 50 bytes: connection (login) processed by server sucessfully

payment Bob 10.0 BK
sending message: payment Bob 10.0 BK
debug: secret key updated
debug: mac added
debug: integrity hash added
debug: timestamp added
debug: unique sequence number added
debug: message has been signed

client received 39 bytes: payment processed by server sucessfully
```

```
[INFO] Building A43 1.0.0-SNAPSHOT
[INFO] --------------------------------[ jar ]---------------------------------
---
[INFO]
[INFO] --- exec-maven-plugin:1.6.0:java (default-cli) @ A43 ---
Welcome to A43 Insurance & Banking: BlingBank
Please enter your username to login: John
Type: 'exit' to close the connection

client received 50 bytes: connection (login) processed by server sucessfully

confirm payment Bob 10.0 BK
sending message: confirm payment Bob 10.0 BK
debug: message has been signed

client received 39 bytes: confirm processed by server sucessfully
```

SIGNATURE OF EACH TRADED MESSAGE ENSURE NON-REPUDIATION

TÉCNICO LISBOA

Main Results and Conclusions

- The security framework implemented in the project is a robust and comprehensive solution
- Recognize the inherent impossibility of complete security
- One potential improvement is introducing secure and encrypted password for each client stored in database while account creation