TÉCNICO LISBOA

MEDITRACK

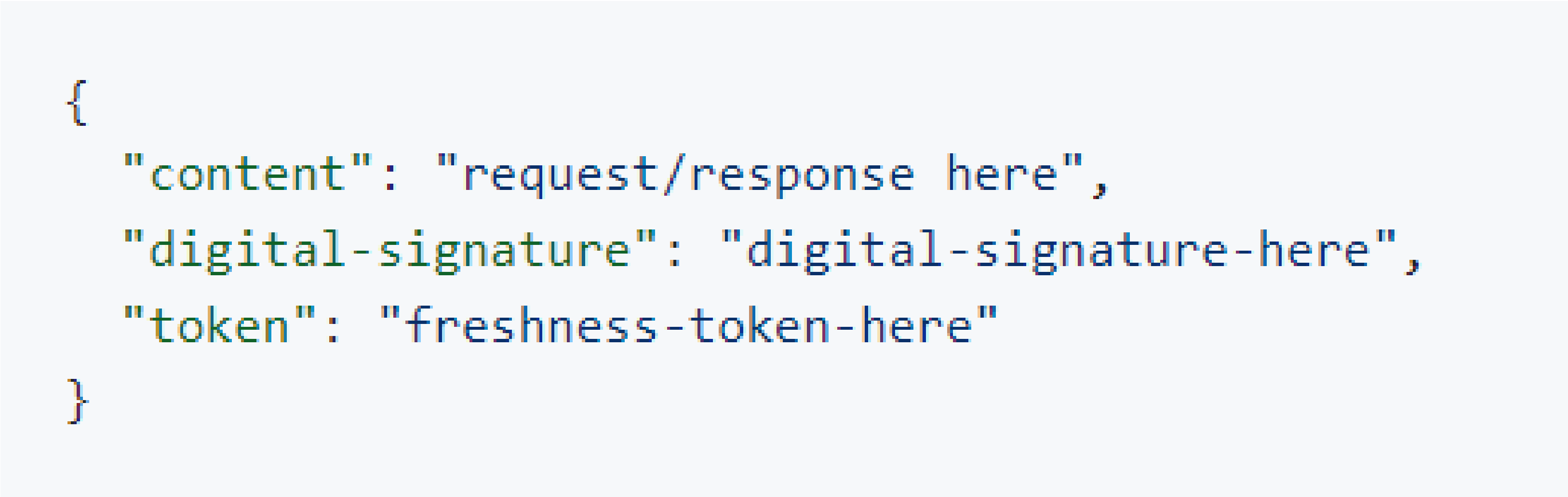
Segurança Informática em Redes e Sistemas

Francisco Gil Mata 99221
Luís Marques 110859
Marta Félix 99276

SECURE DOCUMENTS

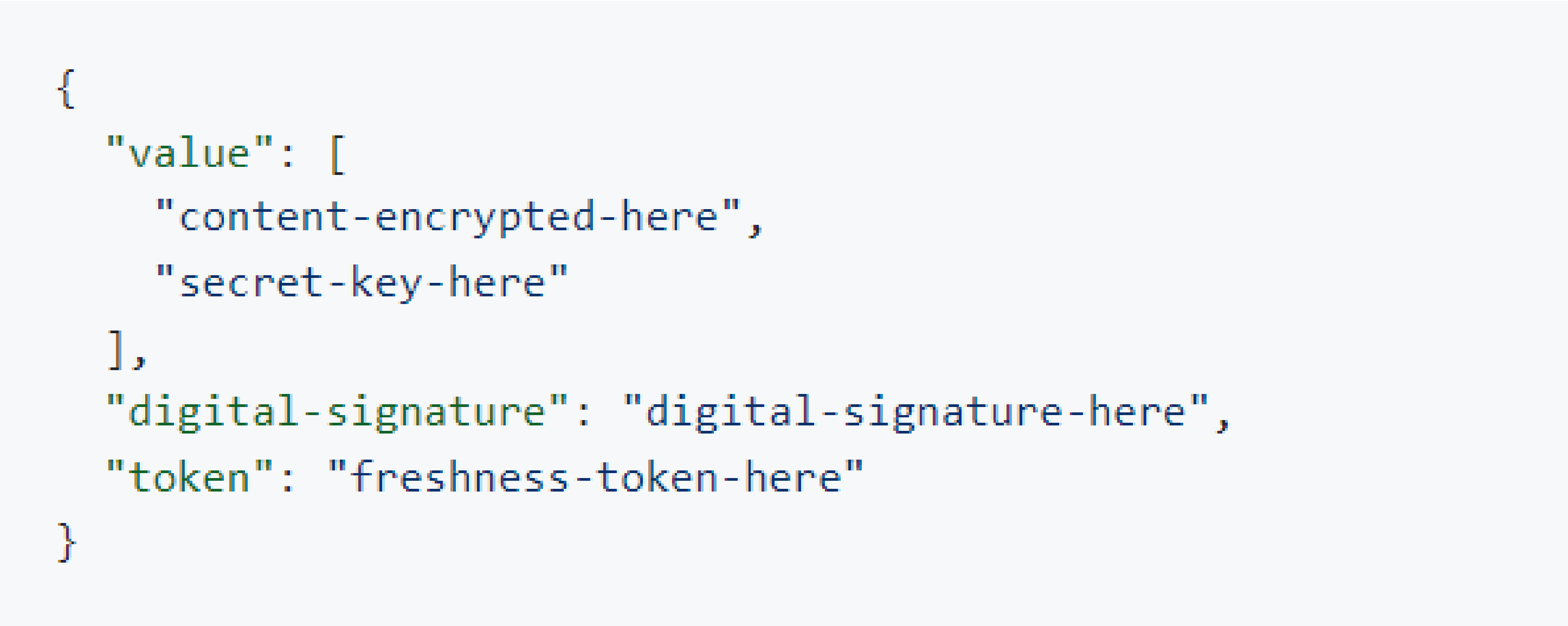
- Implemented using Java,
- From the Java Cryptography Architecture (JCA)
- Two versions
- Encryption using a hybrid mode
- Digital Signature and Freshness token

1. Unprotected Document



```
{
  "content": "request/response here",
  "digital-signature": "digital-signature-here",
  "token": "freshness-token-here"
}
```

2. Protected document

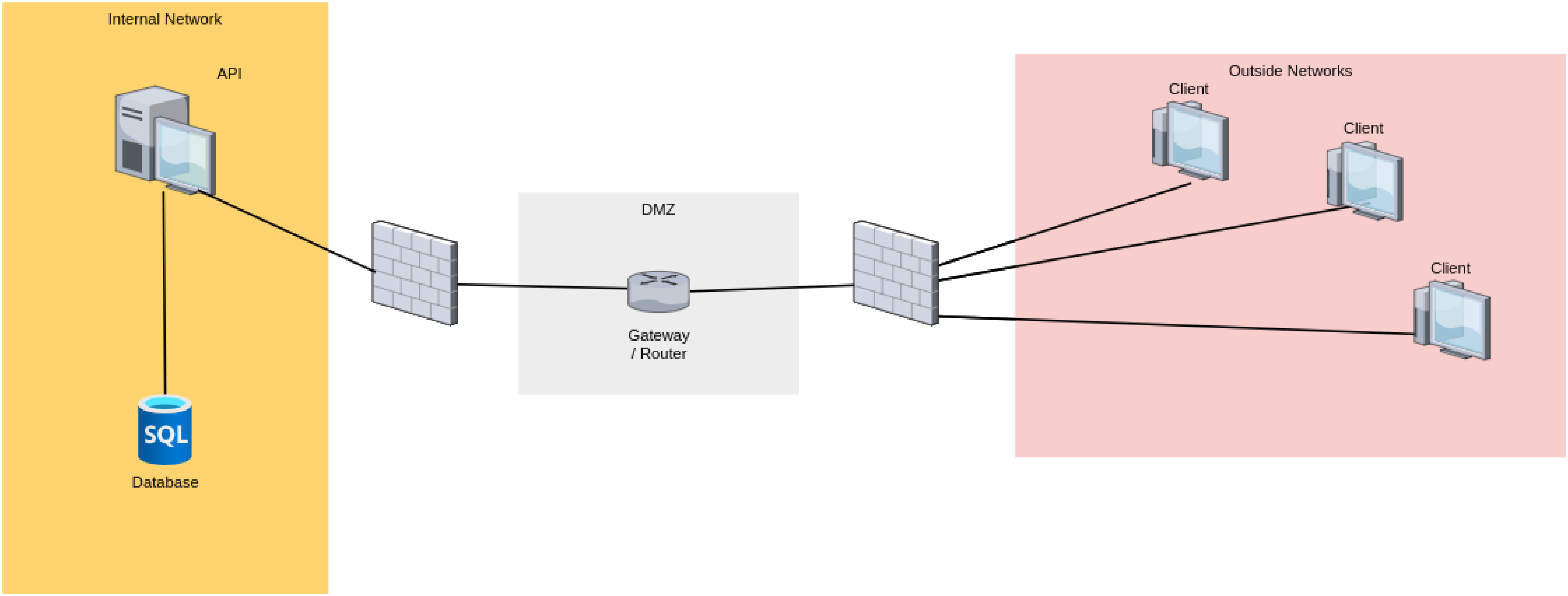


```
{
  "value": [
    "content-encrypted-here",
    "secret-key-here"
  ],
  "digital-signature": "digital-signature-here",
  "token": "freshness-token-here"
}
```

INFRASTRUCTURE

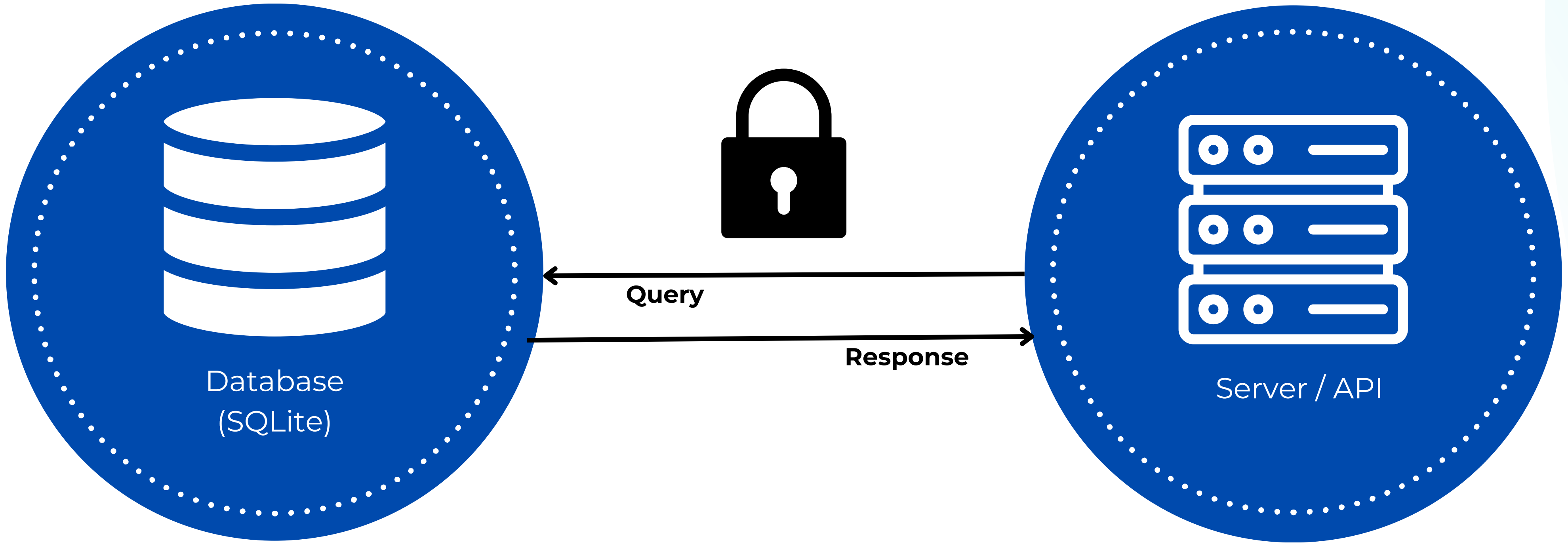
The infrastructure contains 4 VMs, each with its own configurations and firewall rules.

Healthcare: MediTrack Network Architecture



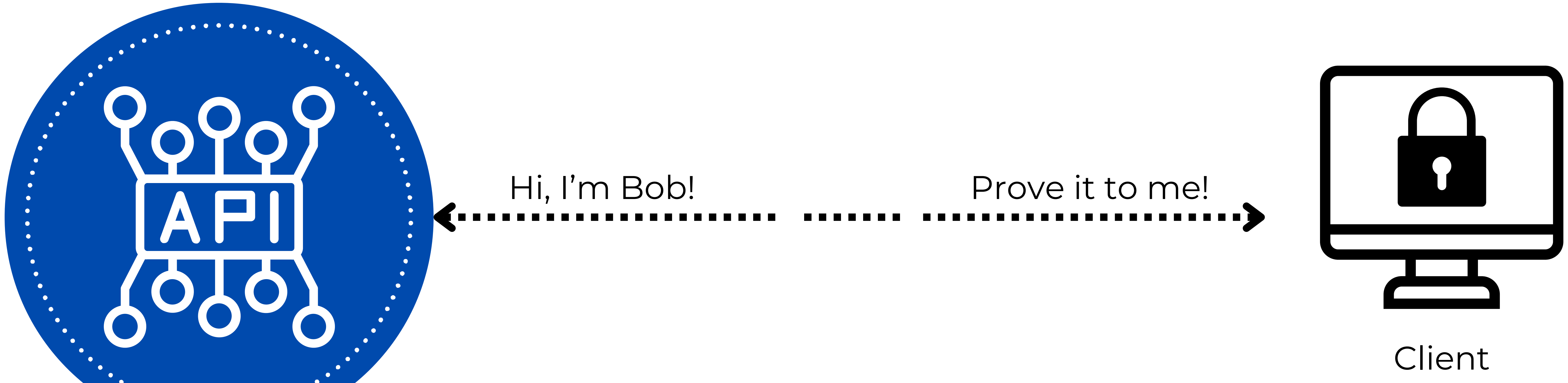
INFRASTRUTURE

WebSockets



- Used **SQLite** for the database
- Does **not** support encryption-at-rest
- Comunication using secure WebSockets

CHALLENGE RESPONSE



Hi, I’m Bob!

Prove it to me!

Client

SECURE CHANNELS

Database ⟷ API

- Secure Sockets
- Internal network
- Assuming its security negates the need for data encryption

API ⟷ Client

- HTTPS
- API as the communication server
- Secure Documents library for encryption

KEY DISTRIBUITION

- **Hybrid process**

  Using an asymmetric cipher to encode the secret key for content encryption.

- **Value fields encrypted**

  With a secret key using the "AES" cipher

- **Simplified key pairs**

  For the clients to simulate acess.

- **Authentication**

  Required before every operation. In a real scenario, users would have logins and sessions

SECURITY CHALLENGE

“SOS” Mode

- Only Doctors can activate the SOS Mode
- Allows the Doctor access to a patient records
- Active for 2 minutes
- Requires Reauthetication

IN CONCLUSION

- Achieve our primary goal
  - Establish secure connections between the database, API, and clients
  - Data Encryption

- A real-world scenarios would demand more sophisticated system