MediTrack

Guilherme Patrão | Guilherme Baracho | Miguel Eleutério

Introduction

Key Features

1. Confidential Communication
2. Secure Record Authenticity
3. Command-line & Code Integration

Secure Document

Secure Document - Overview

Main Functionalities:

Protect: Cipher a document.

Unprotect: Decipher a document.

Check: Verify integrity of a ciphered document.

Usage Commands:

protect <input-file> <output-file> <client>
unprotect <input-file> <output-file> <client>
check <input-file> <client>

Design Considerations:

Focus on JSON handling.

Security through private key usage.

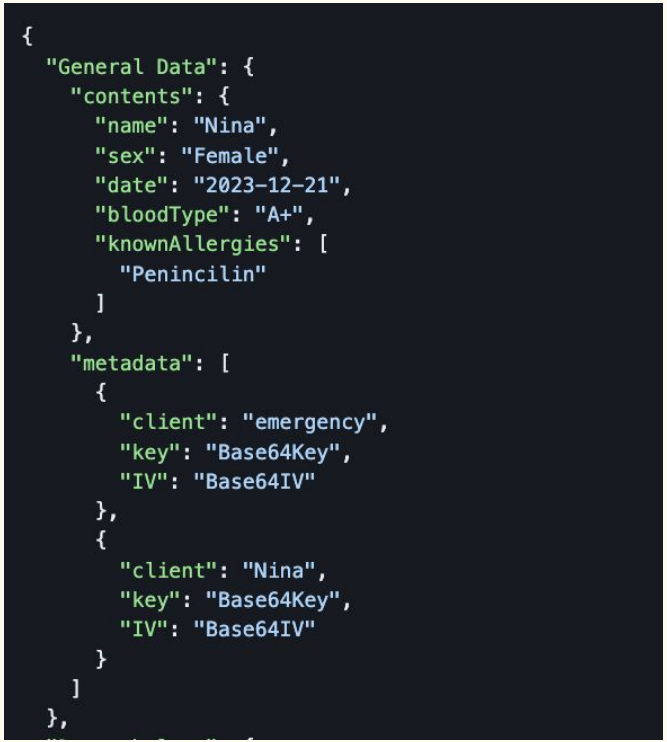
File Division:

Sections contain contents and metadata.

Contents: Encrypted or in real format.

Metadata: Key and IV encrypted with user's public key.

Secure Document - JSON Format



```
{
  "General Data": {
    "contents": {
      "name": "Nina",
      "sex": "Female",
      "date": "2023-12-21",
      "bloodType": "A+",
      "knownAllergies": [
        "Penincilin"
      ]
    },
    "metadata": [
      {
        "client": "emergency",
        "key": "Base64Key",
        "IV": "Base64IV"
      },
      {
        "client": "Nina",
        "key": "Base64Key",
        "IV": "Base64IV"
      }
    ]
  },
```

```
  "Dermathology": {
    "contents": {
      "consultations": [
        {
          "date": "2023-12-21",
          "speciality": "Dermathology",
          "doctor": "Dr. Jordan",
          "practice": "Clinic",
          "summary": "Prescribed some cream"
        }
      ]
    },
    "metadata": [
      {
        "client": "emergency",
        "key": "Base64Key",
        "IV": "Base64IV"
      },
      {
        "client": "Nina",
        "key": "Base64Key",
        "IV": "Base64IV"
      }
    ]
  }
}
```

Secure Document - Implementation

Algorithms:

Symmetric encryption - AES/GCM w/ 128 bits key

Asymmetric encryption - RSA w/ 2048 bits key

Libraries Used:

JSON Handling: com.google.gson

Encryption/Decryption: javax.crypto

Key Handling: java.security

Infrastructure

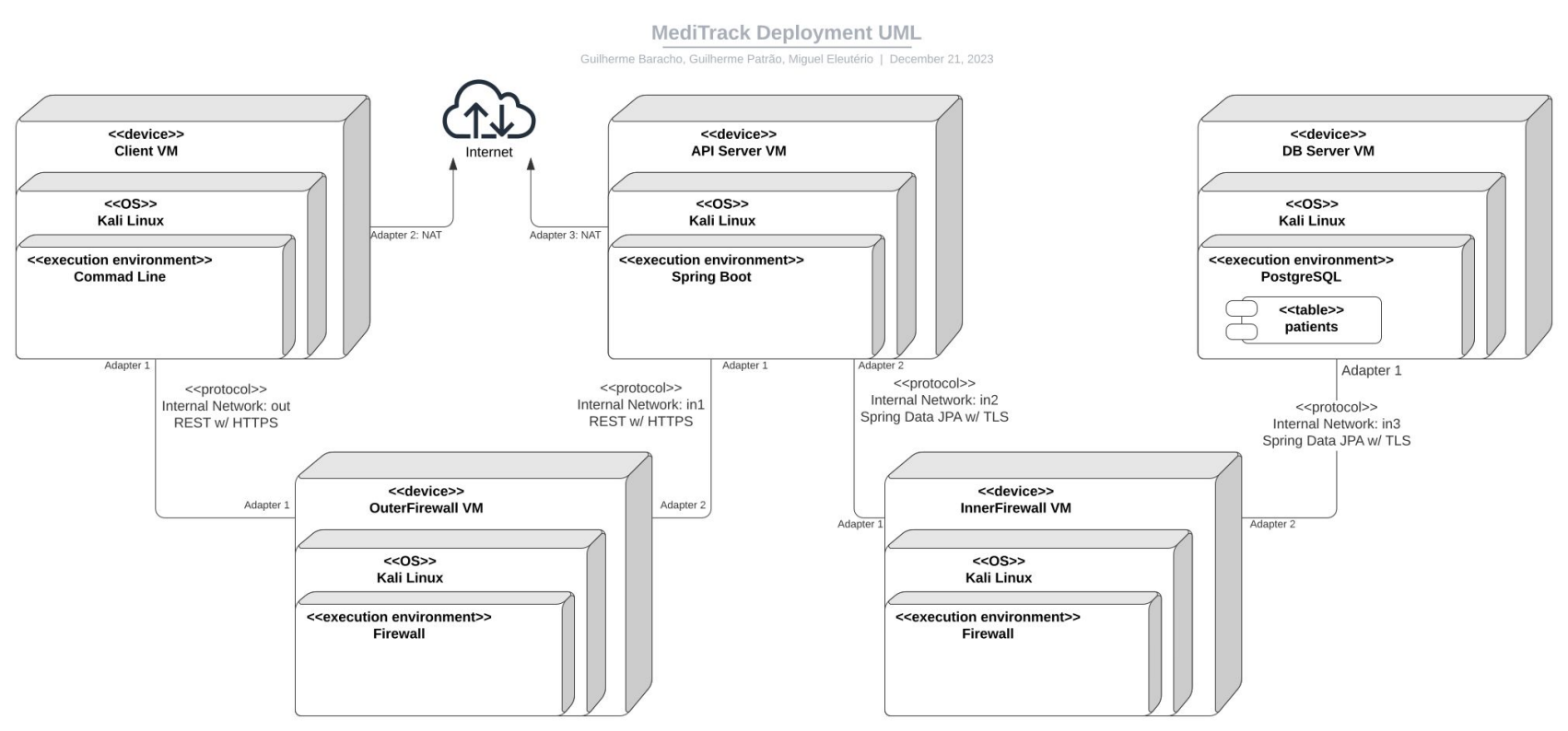
Application Infrastructure

Client Application

Application Server

Database

Infrastructure



Secure Channels - Request Format


```
{
  "command": "register",
  "info": {
    "sender": "UserName",
    "patient": "PatientName",
    "consultation": {
      "date": "2022-05-13",
      "speciality": "Dermathology",
      "doctor": "UserName",
      "practice": "Clinic",
      "summary": "Prescribed some cream",
    },
    "consultationSignature": "Base64SignatureOfConsultation"
  },
  "uuid": "uuid",
  "signature": "Base64Signature"
}
```

Security Challenge

Security Challenge

Challenges:

Non-repudiable Doctor Signatures

Controlled Sharing Implementation

Solutions:

Consultation Signature Verification

Section-wise Document Access Control

Live Demo

Conclusion

Achievements

Fully functional system from scratch

Real-world Infrastructure Emulation

Key Focus Areas:

- Infrastructure & Network Setup
- Data Storage & Security