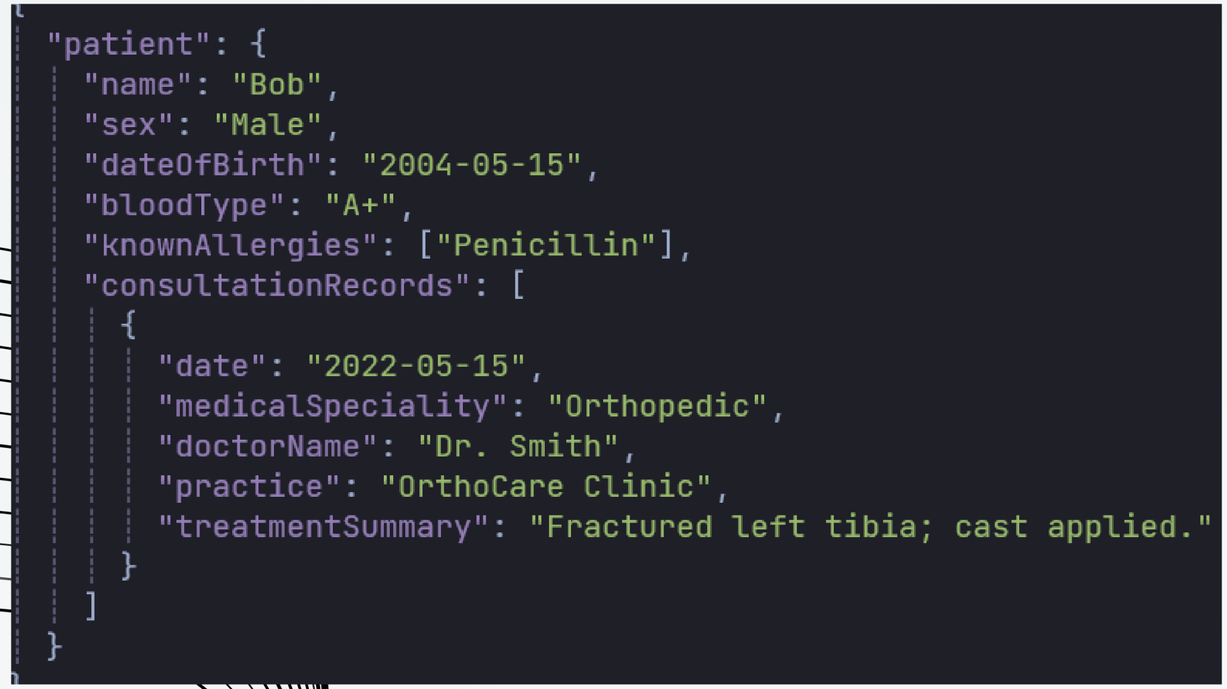
A31-MEDITRACK

SIRS
PROJECT

GUILHERME SOARES 96392
TILDE EINE 108444

CONTENT

SECURE DOCUMENTS



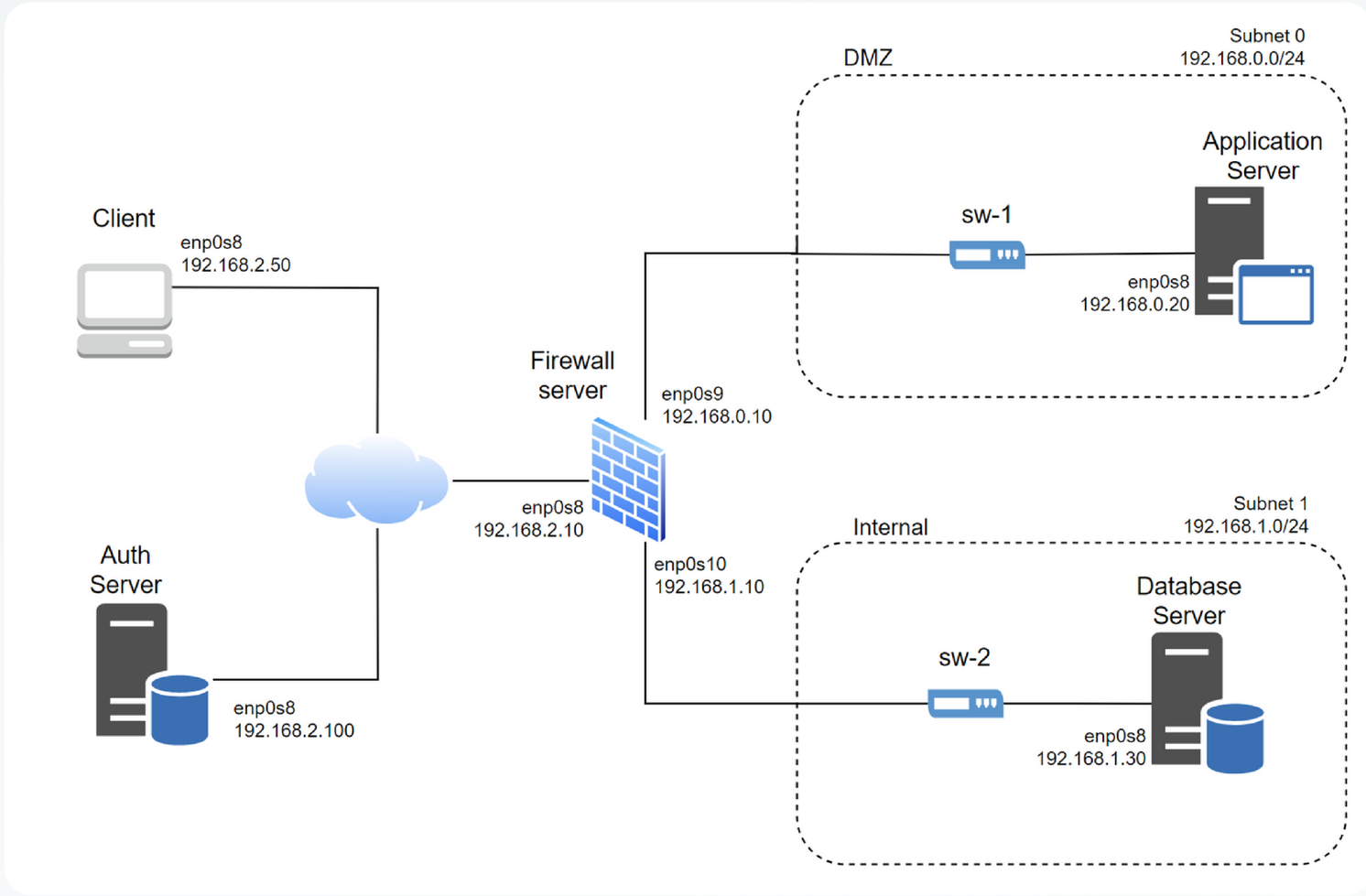
```
{
  "patient": {
    "name": "Bob",
    "sex": "Male",
    "dateOfBirth": "2004-05-15",
    "bloodType": "A+",
    "knownAllergies": ["Penicillin"],
    "consultationRecords": [
      {
        "date": "2022-05-15",
        "medicalSpeciality": "Orthopedic",
        "doctorName": "Dr. Smith",
        "practice": "OrthoCare Clinic",
        "treatmentSummary": "Fractured left tibia; cast applied."
      }
    ]
  }
}
```

```
{
  "patient": {
    "name": "Tn1F4DHsKmLDE/OGpuPDFQ==",
    "sex": "yYCZQlkyAkK4uydiDpP2Nw==",
    "dateOfBirth": "zbB3\u002BRuax8szY\u002BIMGbVr3Q==",
    "bloodType": "rp2no\u002BGhKJBi0xHYYCcVPg==",
    "knownAllergies": [
      "s1SRDyJu7U9VCm0Gq/MIIg=="
    ],
    "consultationRecords": [
      {
        "date": "DRYqKQ6UMcyMftw/qBXWcA==",
        "medicalSpeciality": "ZoYSPlLwEWeARtQO9qPWew==",
        "doctorName": "SO7TMRIWCPbOVdmpmIvRcQ==",
        "practice": "ClhYSrnK45GPtjc9gDjfMpApSGYgk29J0KmK061B4\u002Bc=",
        "treatmentSummary": "9G9qMQgIy/0lzVNKNgIUgH4AsUOUYlInK02f7UQCPTQbUNjY
      }
    ]
  }
}
```

INFRASTRUCTURE

Machines

Client – Physician or patient
App server – Secure documents, .NET
Database – MySQL
Auth server – Key distribution, .NET
Firewall – iptables, NAT



SECURE CHANNELS

Secure Channels

- SSL/TLS
  - Client - App server
  - App server - Auth server
  - Client - Auth server
  - App server - Database
- Document encryption

Key Distribution

- Handled by authentication server
- Everyone has their own private and public keys upon setup, as well as pre-signed certificates (self-signed)
- Consult the authentication server to get physician public keys
  - Verifying signatures

SECURITY CHALLENGE

DIGITAL SIGNATURES

Physicians sign their consultations.
Verified every time the signed consultation is requested.

Required the setup of an authentication server to keep track of physician public keys.

CONTROLLED SHARING

A physician only has access to patients' consultation records with the same speciality as themselves.

When sending EHR's, the consultations that don't match the physician's speciality are encrypted with a random key.

EMERGENCY OVERRIDE

When there is an emergency all consultation records are made available to the physician who requested them.
Ideally, we would use a trusted authority to classify what is an emergency.

MAIN RESULTS

- Successful implementation of secure documents for EHR’s, complete with digital signatures and both symmetric and asymmetric cryptography.
- We set up a fully automated functioning infrastructure, with a firewall server between the external and internal machines, using Vagrant.
- We set up secure channels with TLS/SSL and asymmetric encryption.
- We successfully implemented controlled sharing.