```
{  "title": "A01 MediTrack",
   "course": Network and Computer Security,
   "group number" : "01",
   "group members":  {
                       "95552": "Diogo Silva",
                       "97281": "Allan Fernandes",
                       "99330": "Stanislaw Talejko"
                     },
   "at": Instituto Superior Técnico
}
```

```
{  "Agenda":  {
                    "03": "MediTrack Record Format",
                    "04-05": "Secure Document Format",
                    "06": "Built Infrastructure",
                    "07-08": "Security Challenge",
                    "10": "Conclusion"
                 }
}
```

```
{ "Agenda": {
                "03": "MediTrack Record Format"
              }
}
```

```
{
  "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."
}
```

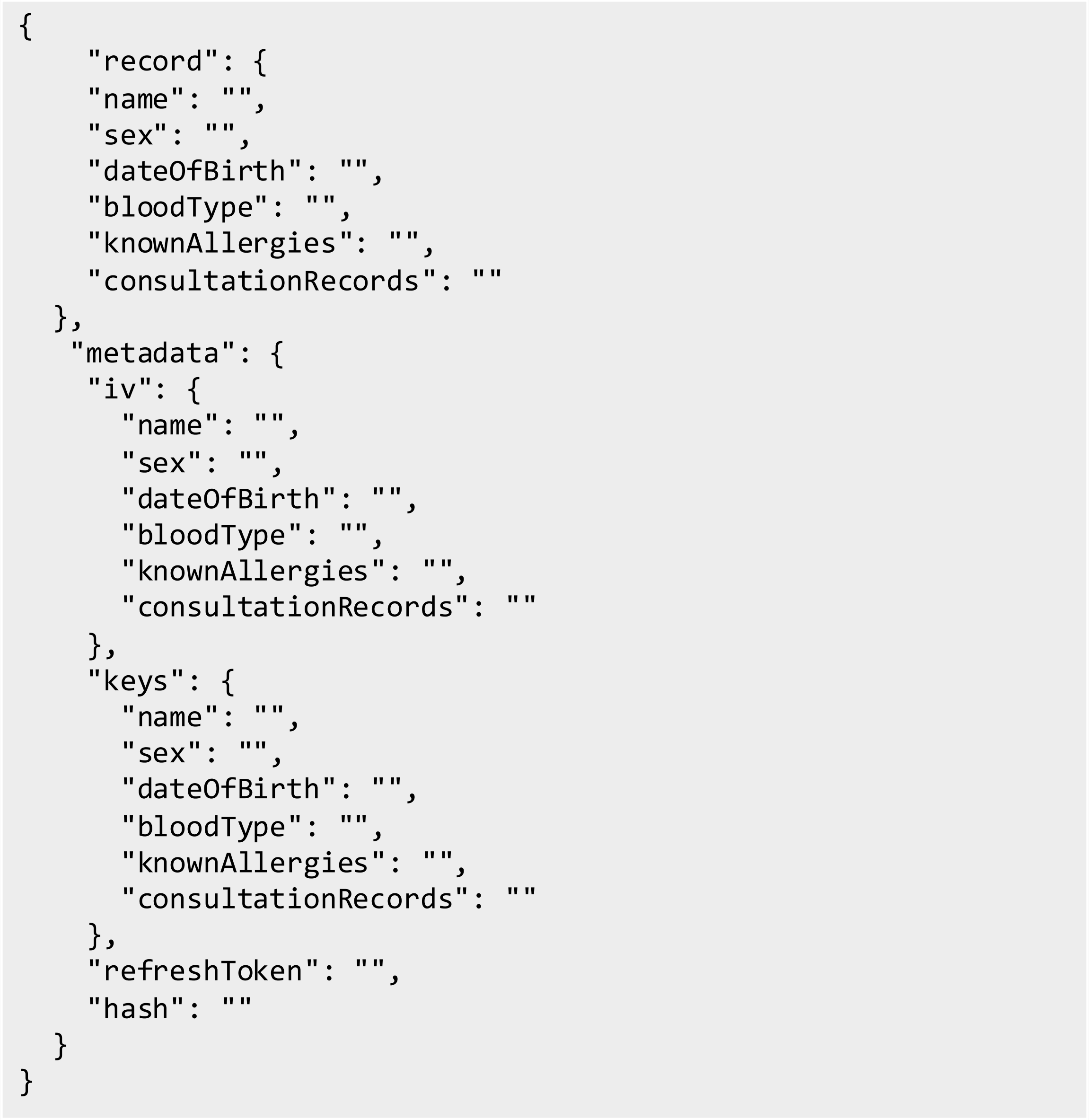
```
{ "Agenda": {
                  "04": "Secure Document Format"
               }
}
```

```
{
    "record": {
    "name": "",
    "sex": "",
    "dateOfBirth": "",
    "bloodType": "",
    "knownAllergies": "",
    "consultationRecords": ""
  }
}
```

- Hybrid encryption
- Asymmetric keys: 2048 bits
- Record fields: AES/CBC/PKCS5Padding; key size of 128 bits
- Main keys: RSA/ECB/PKCS1Padding
- Hash: SHA-256 + RSA/ECB/PKCS1Padding
- Refresh token: timestamp encrypted with RSA/ECB/PKCS1Padding; 1 min lifetime

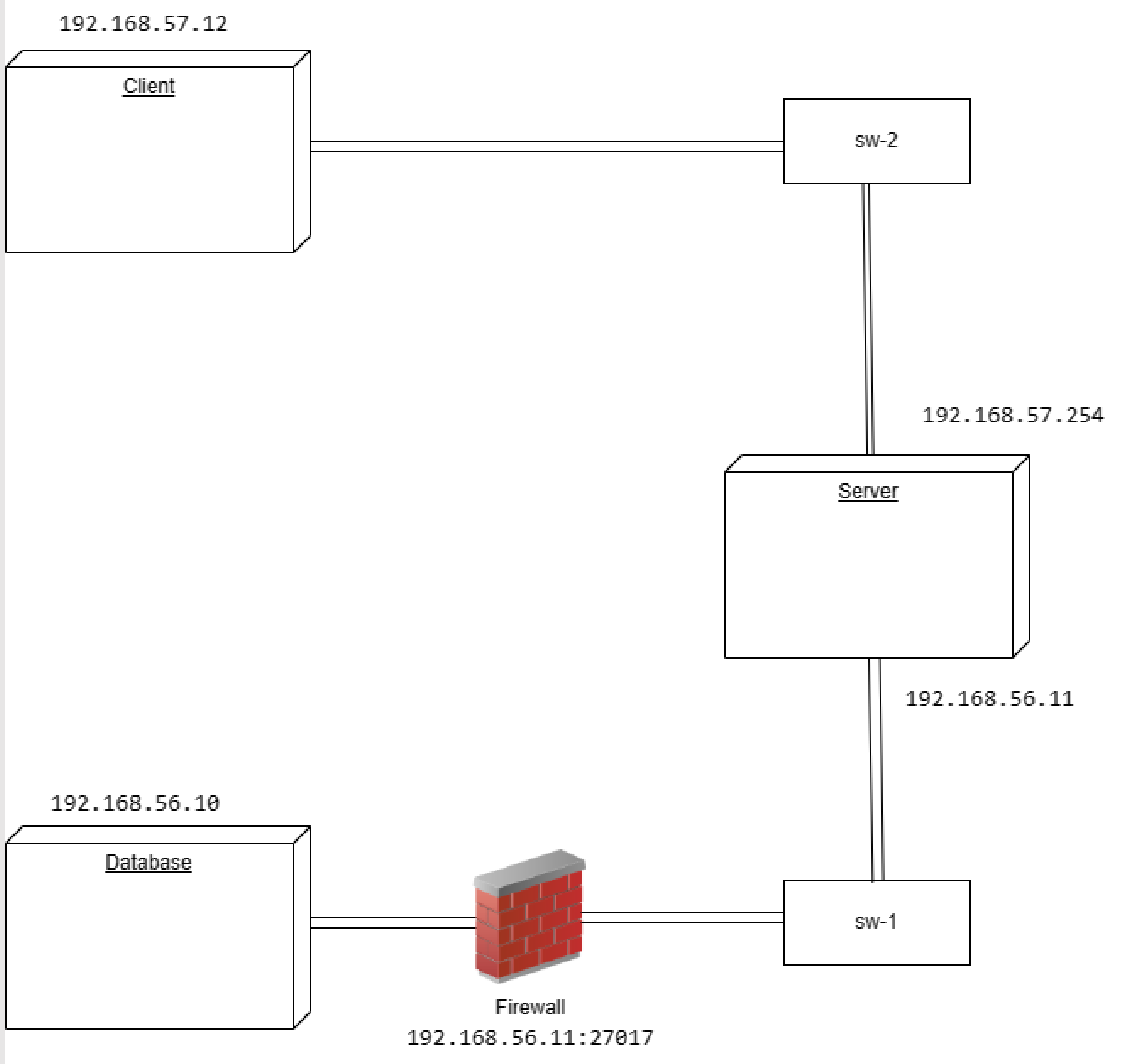
```
{
  "metadata": {
    "iv": {
      "name": "",
      "sex": "",
      "dateOfBirth": "",
      "bloodType": "",
      "knownAllergies": "",
      "consultationRecords": ""
    },
    "keys": {
      "name": "",
      "sex": "",
      "dateOfBirth": "",
      "bloodType": "",
      "knownAllergies": "",
      "consultationRecords": ""
    },
    "refreshToken": "",
    "hash": ""
  }
}
```

```
{ "Agenda": {
                    "05": "Secure Document Format"
                  }
}
```



```
{
    "record": {
    "name": "",
    "sex": "",
    "dateOfBirth": "",
    "bloodType": "",
    "knownAllergies": "",
    "consultationRecords": ""
  },
   "metadata": {
    "iv": {
      "name": "",
      "sex": "",
      "dateOfBirth": "",
      "bloodType": "",
      "knownAllergies": "",
      "consultationRecords": ""
    },
    "keys": {
      "name": "",
      "sex": "",
      "dateOfBirth": "",
      "bloodType": "",
      "knownAllergies": "",
      "consultationRecords": ""
    },
    "refreshToken": "",
    "hash": ""
  }
}
```

```
{ "Agenda": {
                    "06": "Built Infrastructure"
                 }
}
```



```
{ "Agenda": {
                    "07": "Security Challenge – Emergency access"
                  }
}
```

Updated secure document format:

```
{
    "record": {
    "name": "",
    "sex": "",
    "dateOfBirth": "",
    "bloodType": "",
    "knownAllergies": "",
    "consultationRecords": ""
  },
   "metadata": {
    "iv": {
      "name": "",
      ...
    },
    "keys": {
      "name": "",
      ...
    },
    "SOS": {
      "name": "",
      ...
    },
    "refreshToken": "",
    "hash": ""
  }
}
```

```
{ "Agenda": {
                    "08": "Security Challenge – Consultation record signature"
                  }
}
```

Updated Consultation Record

```
{
  "date": "2022-05-15",
  "medicalSpeciality": "Orthopedic",
  "doctorName": "Dr. Smith",
  "practice": "OrthoCare Clinic",
  "treatmentSummary": "Fractured left tibia; cast
applied.",  "digitalSignature":"LvHqgLN24fWLDjZ0sPSPT09V10U//LKmuHPr7aZPzqy6Qxvj25HfqWnx0Dbg0c
i5K7g6ZJpcAG7udHCeexmE/a8UustPnVnoNAgRlVFjWzmRVf8on5MOkFq7s8KioDm1NHQVPUFf1BaPSfZKlBt
Anod6f8UhwdrOEwAAQo3UTKtGaG3Cql6S1JRwbqiR/rrx+YrLZJ+rj+F70nmO3feSqfdczYpYYDUHM72+8eBEU
QgAfe2YSzeEIN9ZmTNCl9PB4C9caiRBUnljJ6z7zuiduSFzO4D3mbcfvHQt80TxzKKNA23a+4YnVm7Z1AgshTbr7
EhWGEohGyuc05kL2gSCUQ\u003d\u003d"
}
```

- Algorithm used for signature: SHA256withRSA

```
{ "Agenda": {
                    "09": "Security Challenge – Selective sharing"
                }
}
```

- The patient personally encrypts the keys for specific fields with the keys of the doctor he intends to share the contents with.

- The keys are then stored on a database.

```
{ "Agenda": {
                    "10": "Conclusion"
                 }
}
```

Things that could be improved

- Add a special authentication mechanism when SOS is used

- Shift from AES-128 to AES-256