SIRS project – Insurance & Banking: BlingBank

Group 49

Gonçalo Silva   96925
Miguel Vale   99113
Renato Custódio 110948
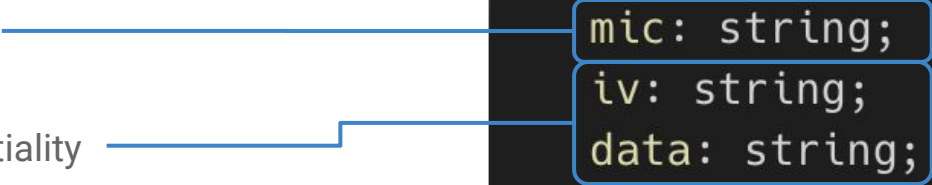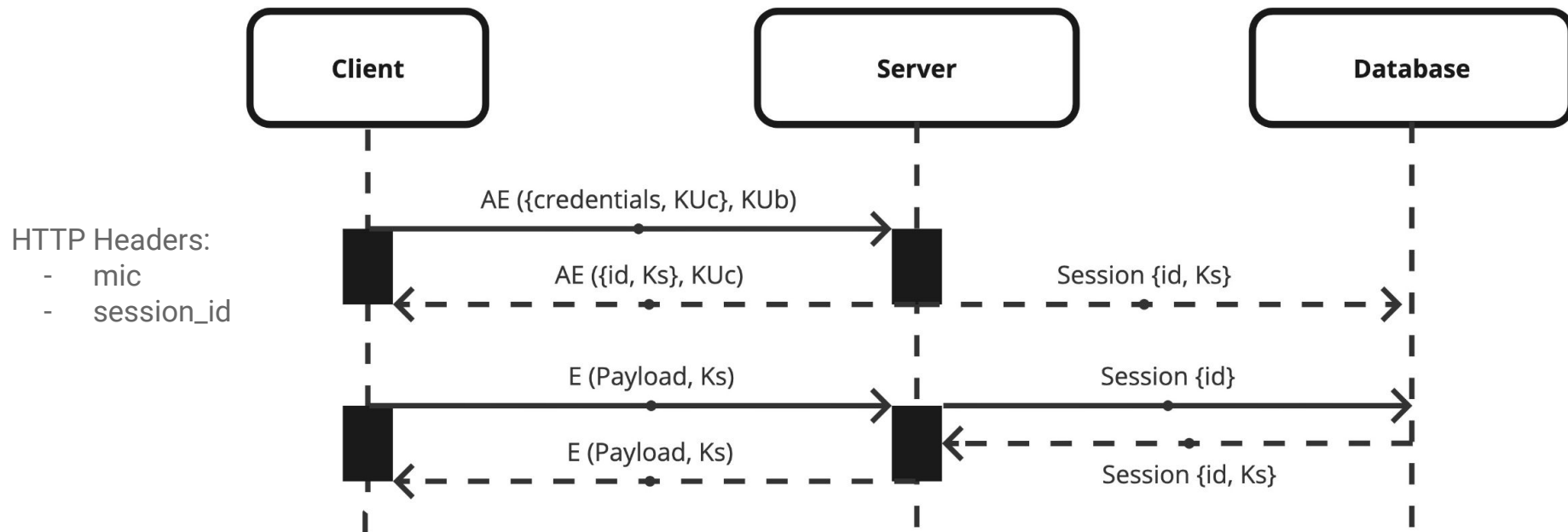
Secure Document
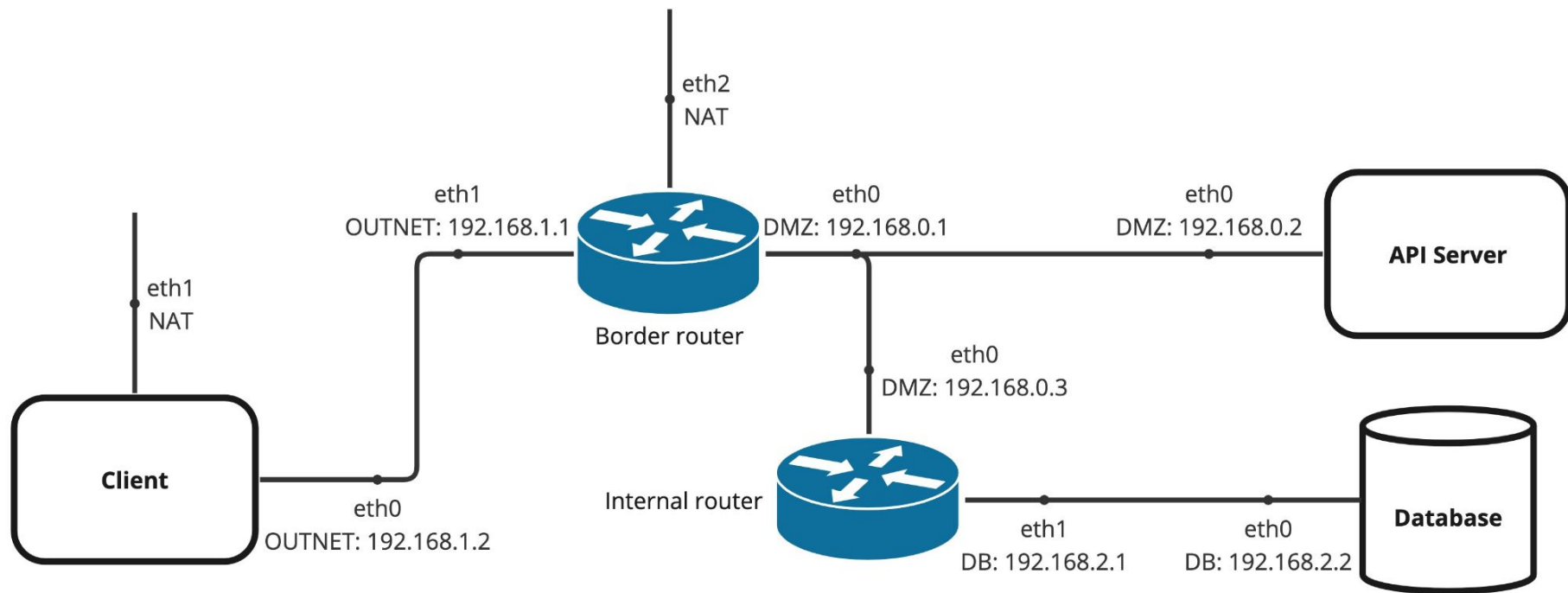
Integrity

Confidentiality

```
export interface ProtectedDocument {
  mic: string;
  iv: string;
  data: string;
}
```

Secure channel establishment

HTTP Headers:
- mic
- session_id

Client → Server: AE ({credentials, KUc}, KUb)

Server → Client: AE ({id, Ks}, KUc)

Server → Database: Session {id, Ks}

Client → Server: E (Payload, Ks)

Server → Database: Session {id}

Server → Client: E (Payload, Ks)

Database → Server: Session {id, Ks}
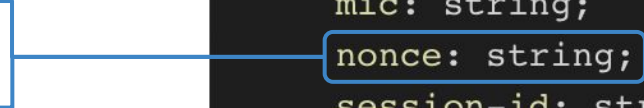
Infrastructure

Security Challenge

HTTP packet format
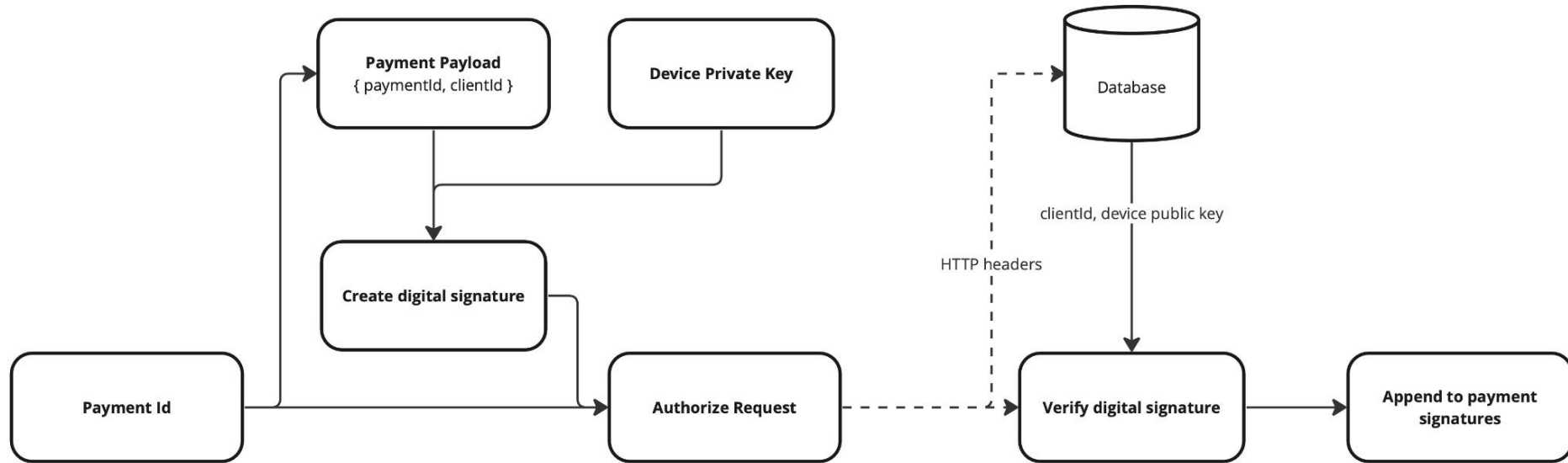
Freshness
IV

```
export interface SecureData {
  headers: {
    mic: string;
    nonce: string;
    session-id: string;
  }
  data: string;
}
```

Security Challenge

Payments system

Demonstration

Q/A