Dissertation Thesis

Designing a privacy-oriented system for
file-storing & file-sharing

Graduate: Bișag Alexandru - Ștefan

Scientific coordinator: Cristian - Valeriu Toma, Ph.D.

ISM, 2022

The state of the present

Ownership & Trust

The state of the present

The market

The state of the present

The missing piece

The state of the present

A privacy-focused architecture

1. Zero-Knowledge

A privacy-focused architecture

2. Responsiveness

A privacy-focused architecture

3. High availability

A privacy-focused architecture

4. Fault tolerance

A privacy-focused architecture

5. Traceability

A privacy-focused architecture

6. Platform agnosticism

A privacy-focused architecture

7. Openness

A privacy-focused architecture

8. Loose coupling

A privacy-focused architecture

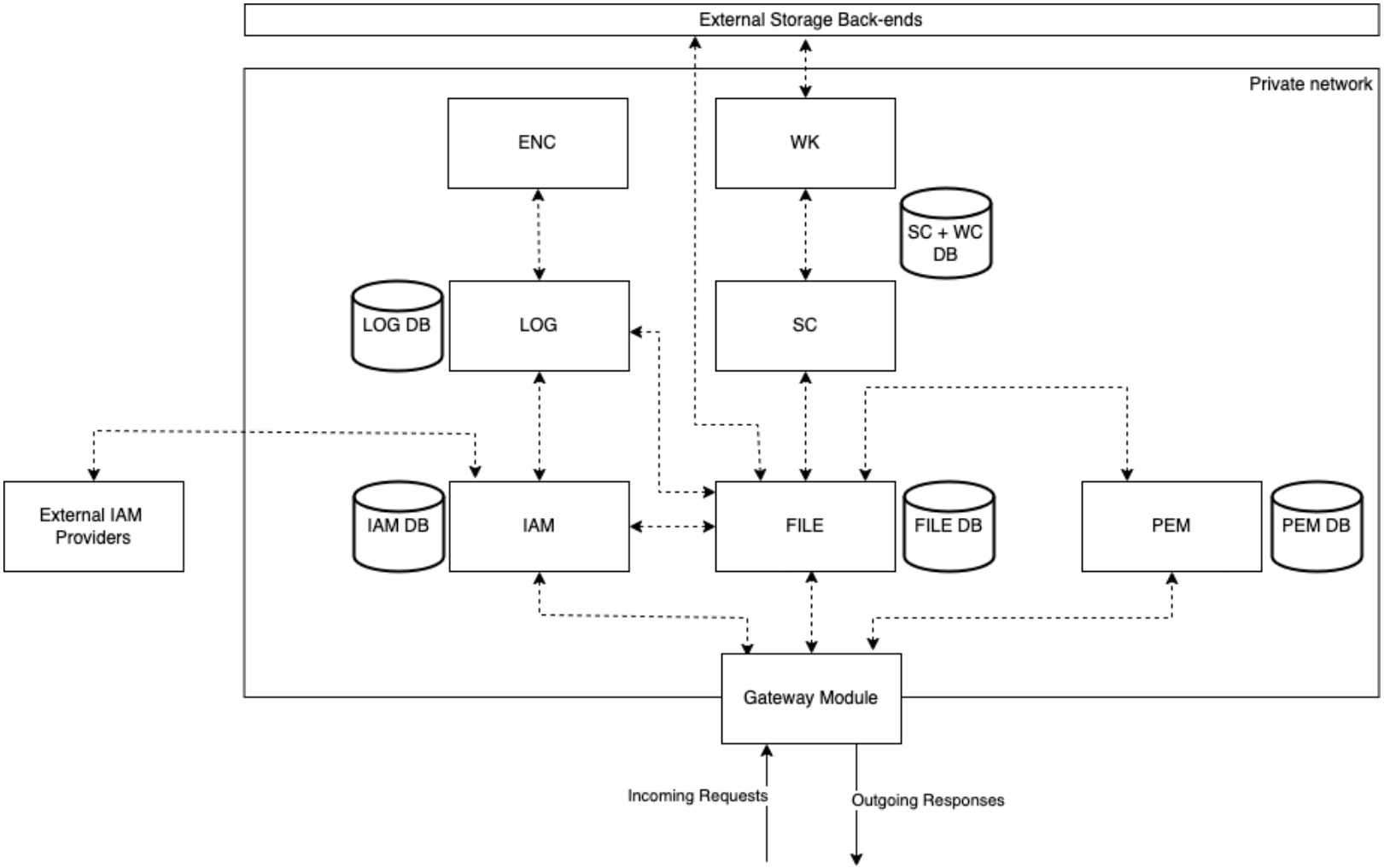
9. Access federation

A privacy-focused architecture

The core

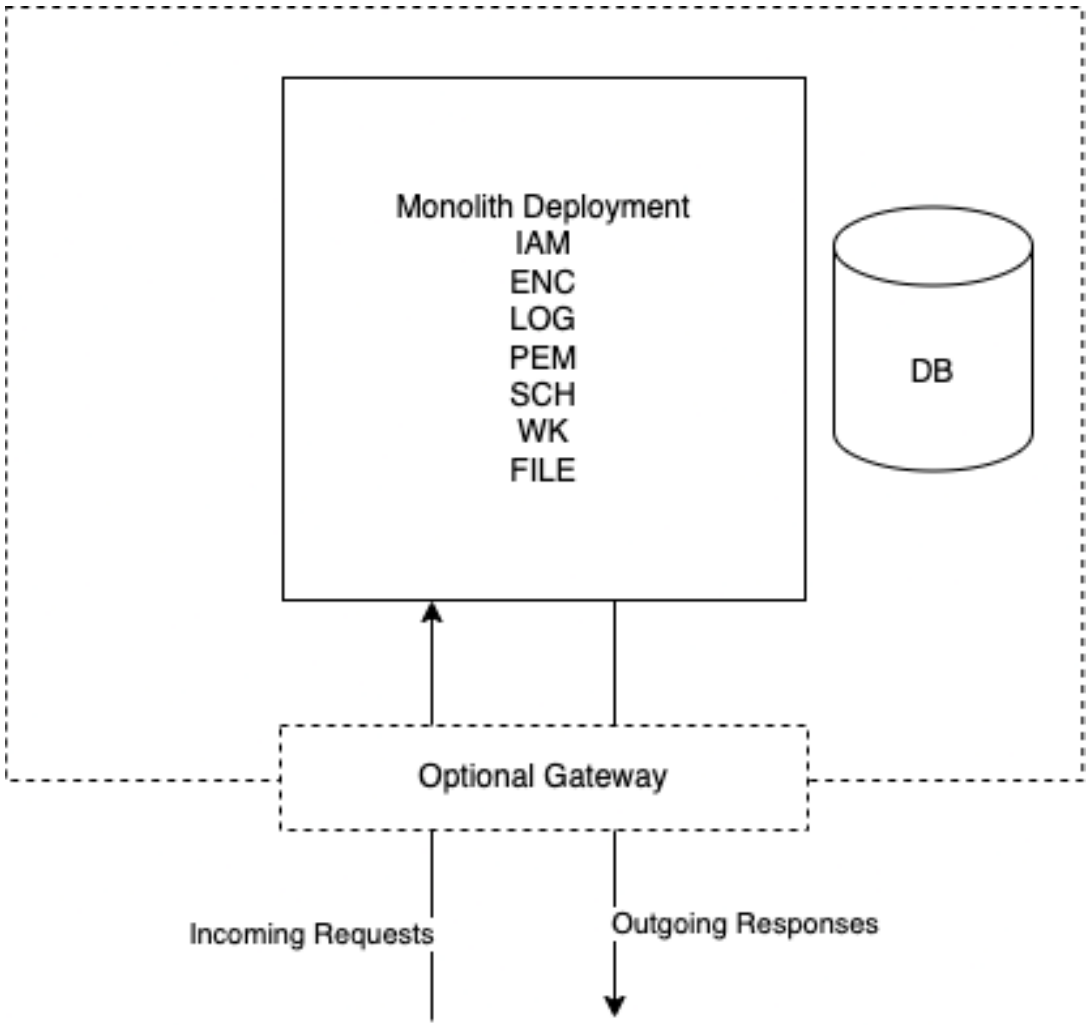
Thinking at scale

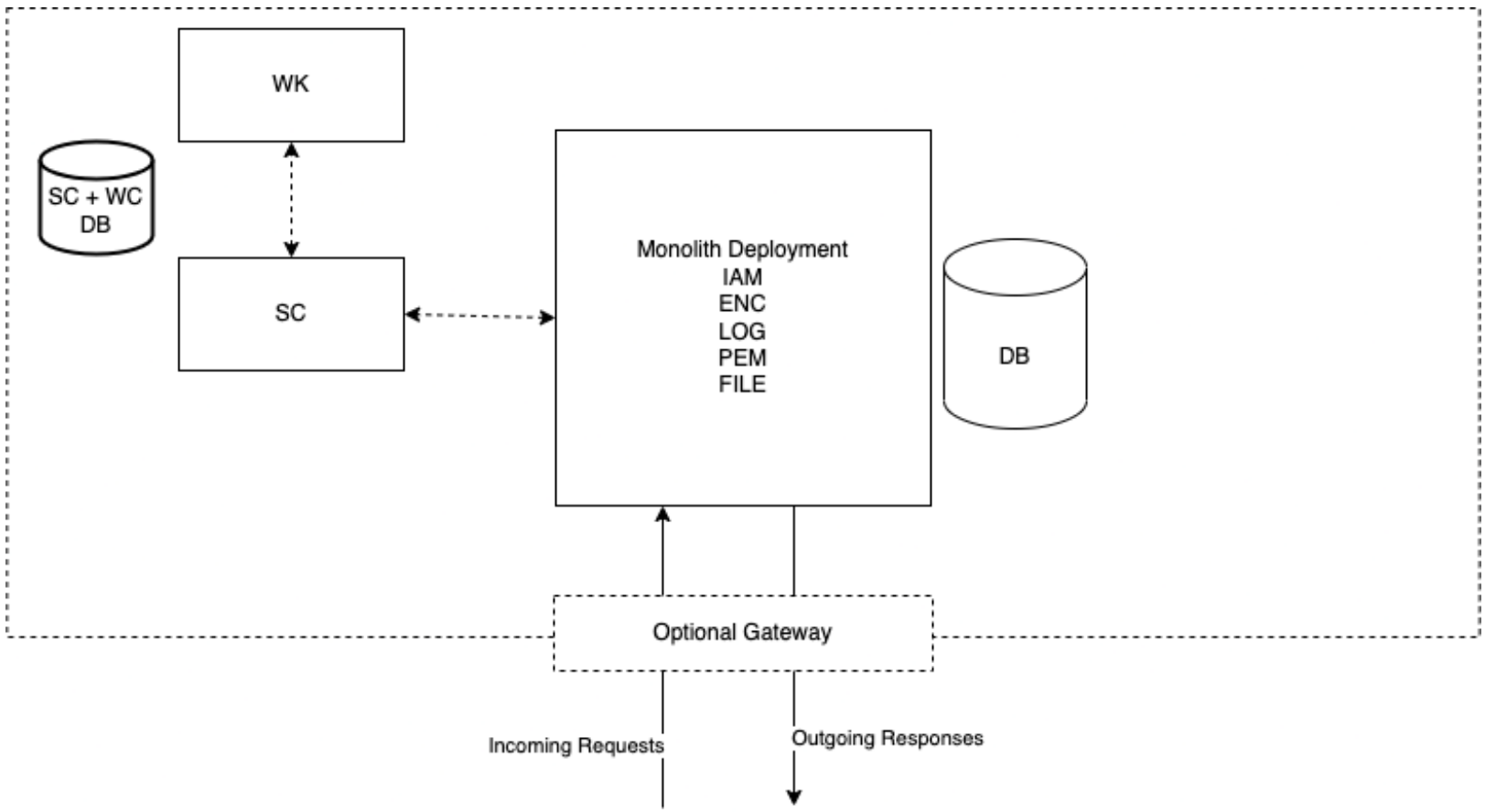
The core


External Storage Back-ends
Private network
ENC
WK
SC + WC DB
LOG DB
LOG
SC
External IAM Providers
IAM DB
IAM
FILE
FILE DB
PEM
PEM DB
Gateway Module
Incoming Requests
Outgoing Responses

A private cloud

The core


Monolith Deployment
IAM
ENC
LOG
PEM
SCH
WK
FILE
DB
Optional Gateway
Incoming Requests
Outgoing Responses


WK
SC + WC
DB
SC
Monolith Deployment
IAM
ENC
LOG
PEM
FILE
DB
Optional Gateway
Incoming Requests
Outgoing Responses

The client

Owner of cryptography

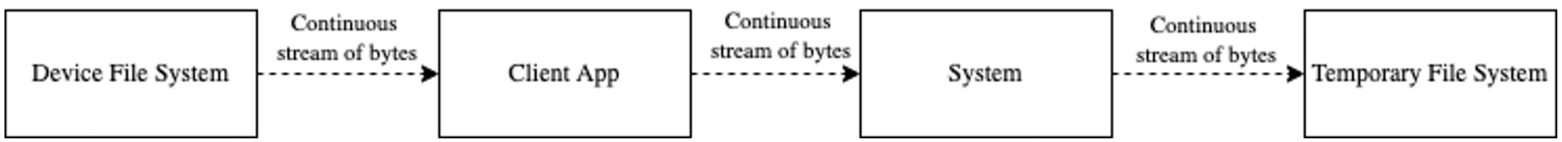
The client

Resource conscious

The client

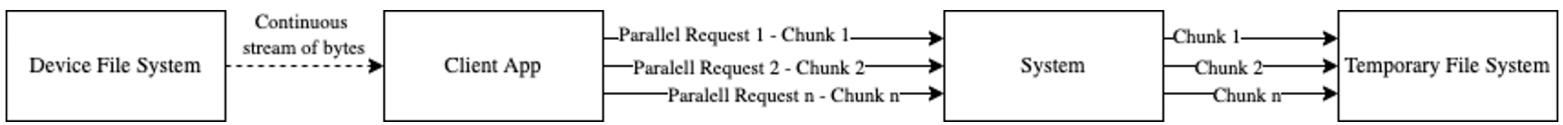
Streaming upload

The client


Device File System
Continuous stream of bytes
Client App
Continuous stream of bytes
System
Continuous stream of bytes
Temporary File System

Chunked upload

The client


Device File System
Continuous
stream of bytes
Client App
Parallel Request 1 - Chunk 1
Paralell Request 2 - Chunk 2
Paralell Request n - Chunk n
System
Chunk 1
Chunk 2
Chunk n
Temporary File System

Security highlights

Privacy & Integrity

Security highlights

ChaCha20-Poly1305

AES-GCM

Ownership

Security highlights

RSA-4096

Technical highlights

(demo)

Login

Technical highlights

RSA

AES-GCM

Streamed + Chunked Upload

Technical highlights

RSA

AES-GCM

File reconstruction

Technical highlights

Streamed download

Technical highlights

RSA

AES-GCM

A selection of tools

Server

A selection of tools

Java / Spring WebFlux

MongoDB

GridFS / AWS S3

Docker / Kubernetes / Helm

Client

A selection of tools

Web

Streaming API

File System Access API

WebWorkers

WebAssembly

A future of privacy

(conclusions)

Everything open

A future of privacy

Privacy by default

A future of privacy

Secure pluggable systems

A future of privacy

Dissertation Thesis

Designing a privacy-oriented system for
file-storing & file-sharing

Graduate: Bișag Alexandru - Ștefan

Scientific coordinator: Cristian - Valeriu Toma, Ph.D.

ISM, 2022