

Eternity Service

Pavel Hlousek

Marek Janata

Jan Pechanec

Vaclav Petricek

Ivana Reisingerova

Jiri Vaculik

Supervisor: Tonda Benes

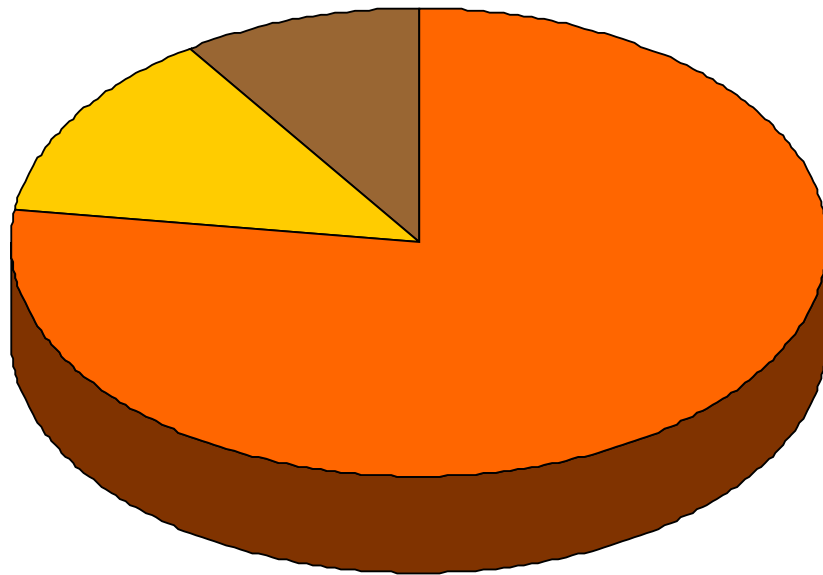
<http://www.kolej.mff.cuni.cz/~eternity>
petricek@acm.org

Content



- What is Eternity Service
- Project goals
- Implementation
- Example

Motivation



System requirements



- search

- download

- upload

- ~~■ delete~~

- ~~■ modify~~



- anonymity

- security

History

■ Ross Anderson



■ Adam Back



■ Tonda Benes



■ we, MFF UK

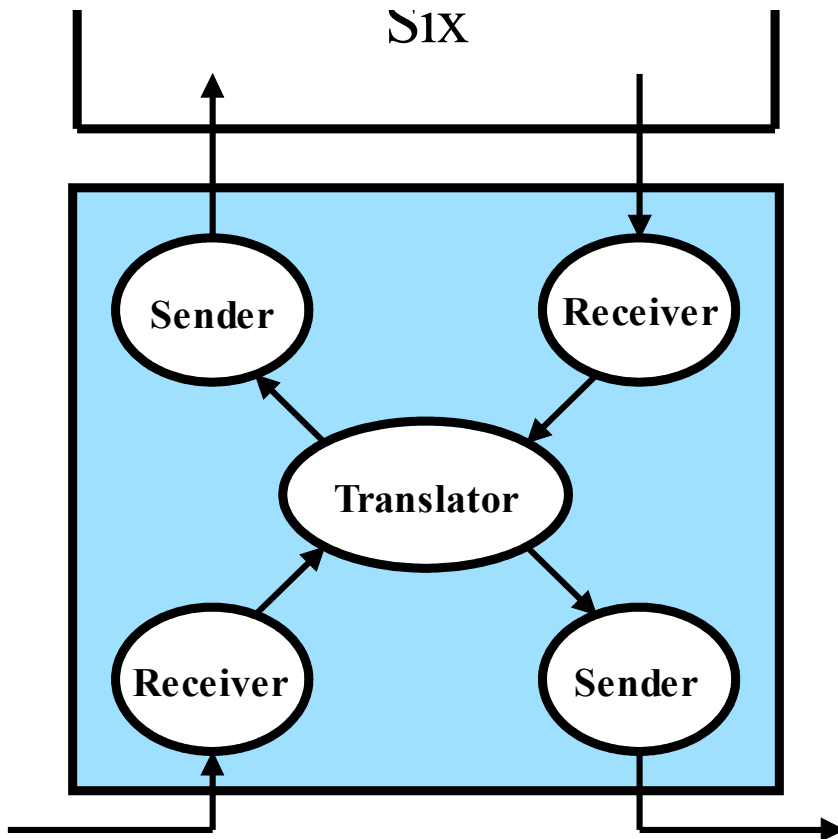


Project goals



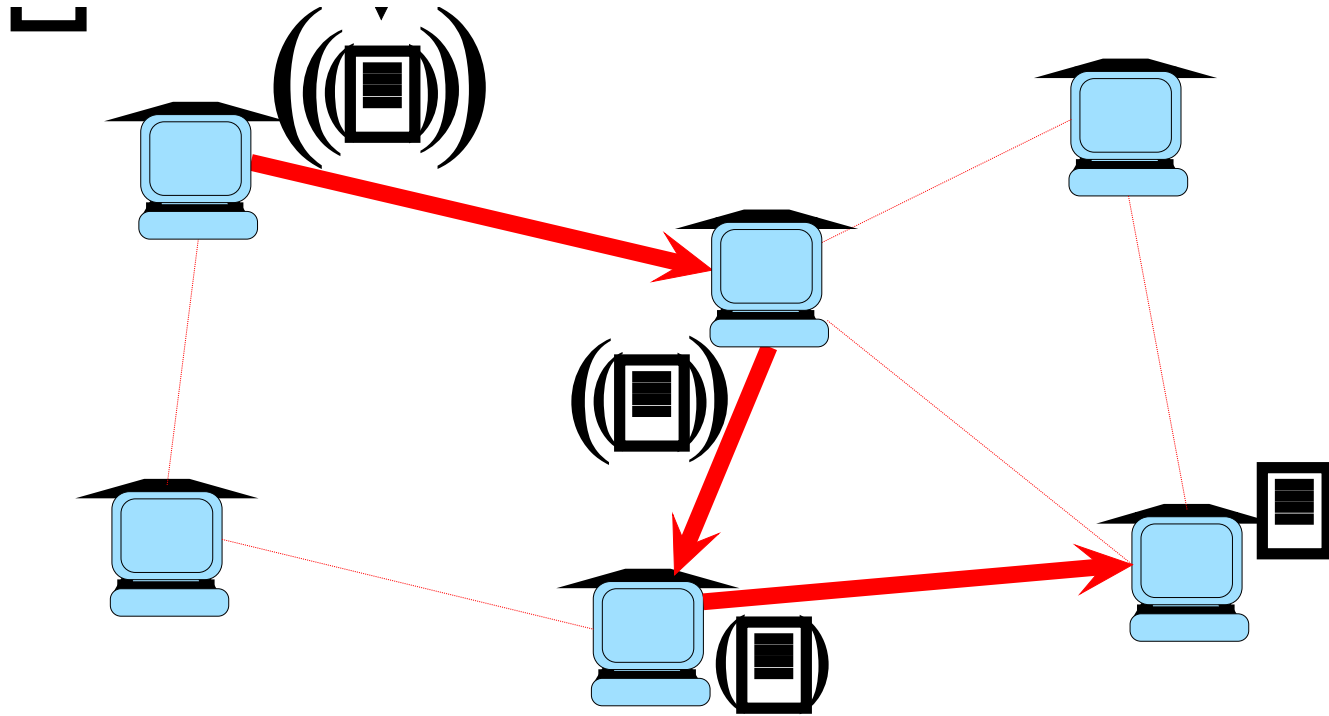
- search for data
- store data
- anonymous communication
- protocols for electronic payments
- time synchronization
- administrator interface
- extendability

Mix

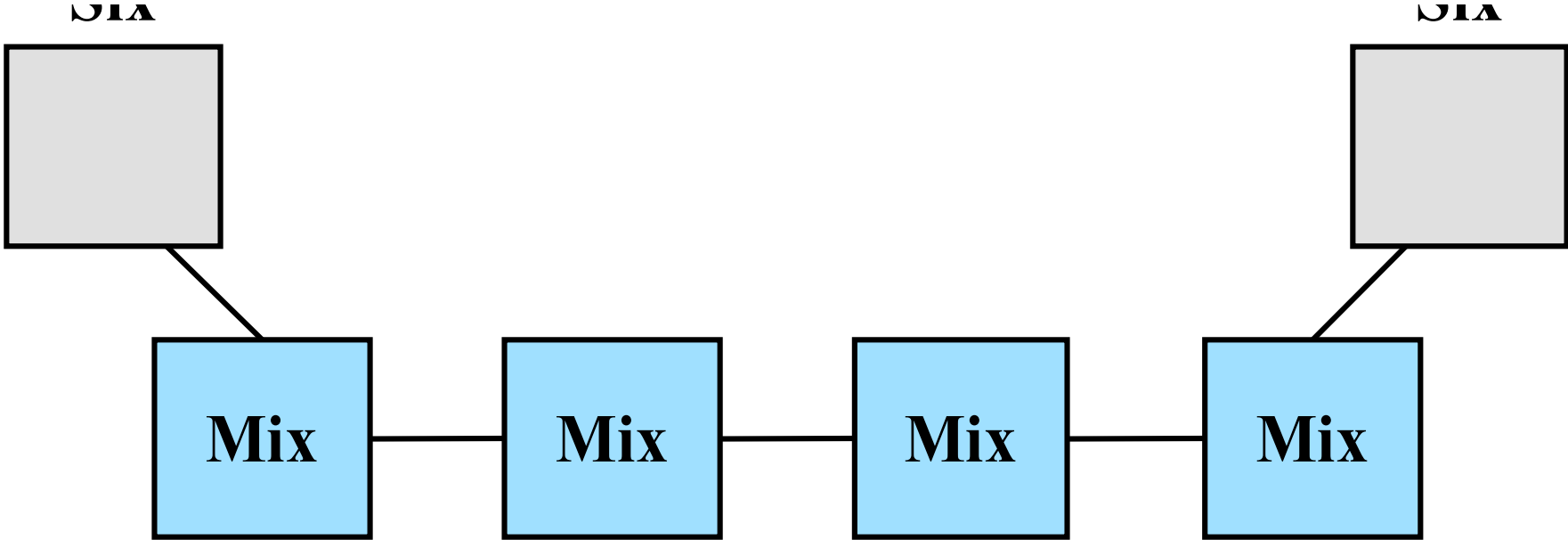


- onion routing
- traffic padding
- header padding
- data padding
- certificates for Six

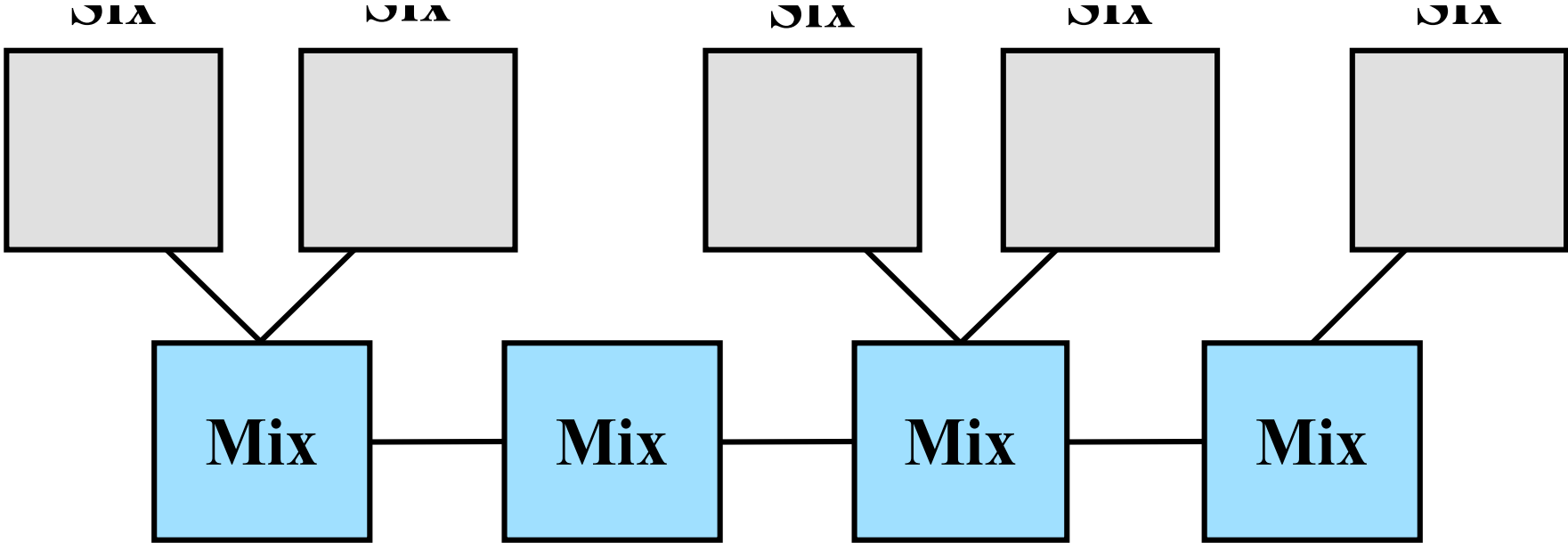
Onion routing



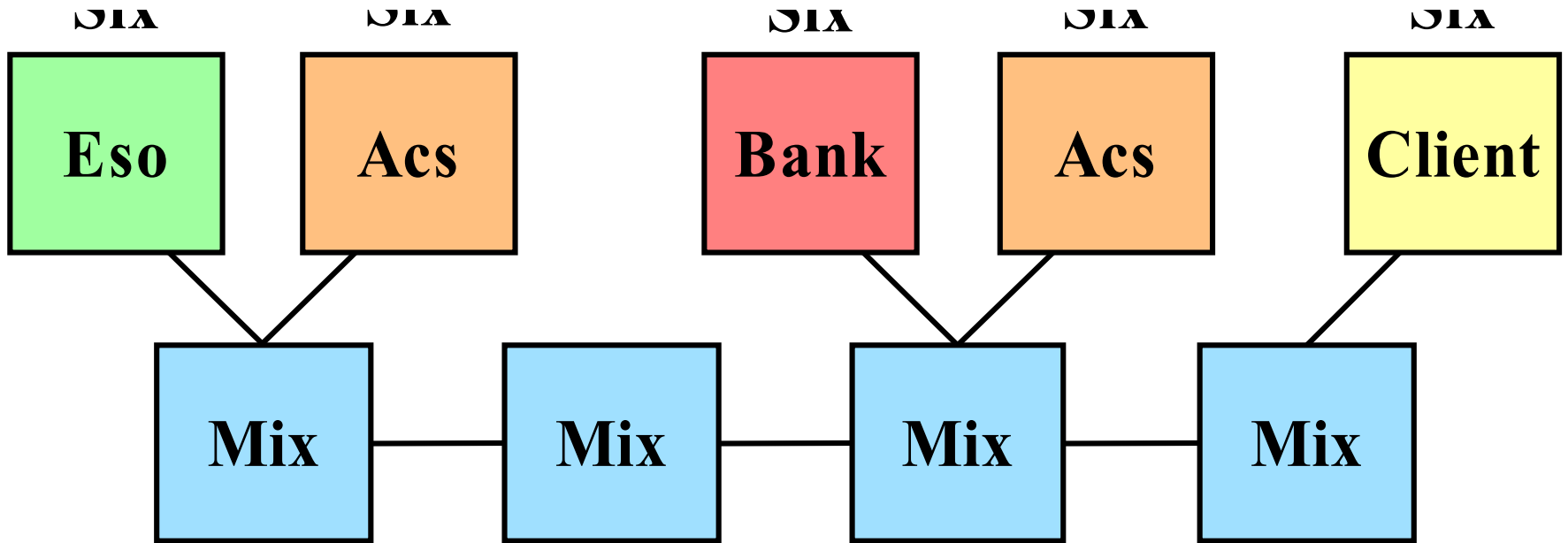
Six



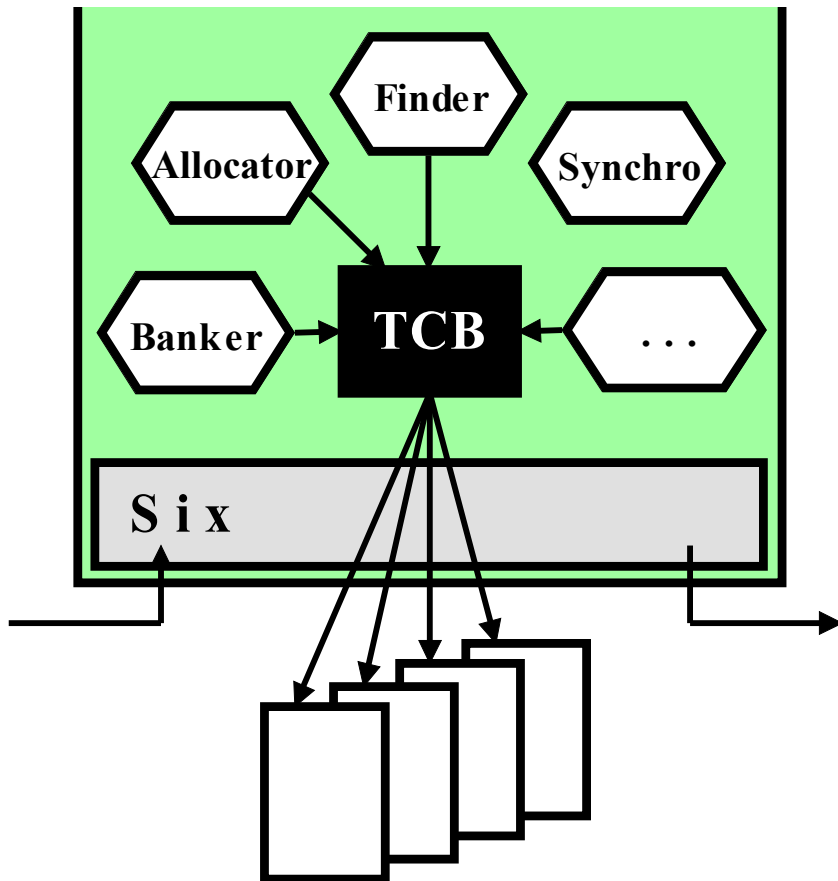
Six



Six

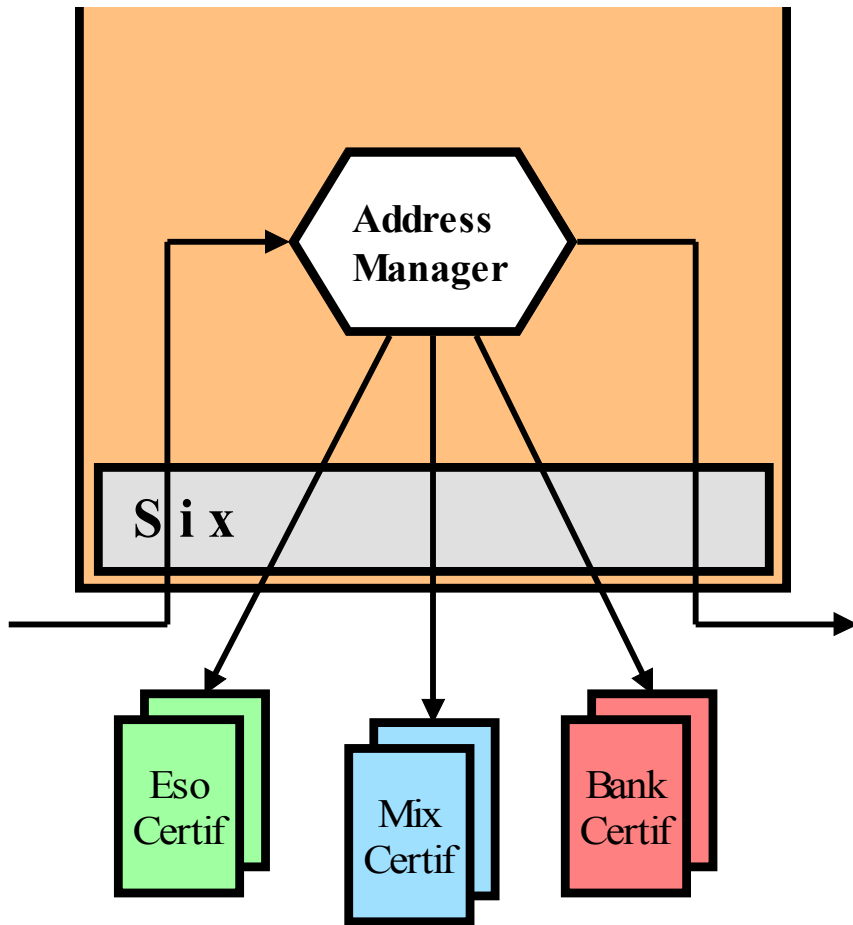


Eso



- search data
- store data
- payments for storage
- time synchronization

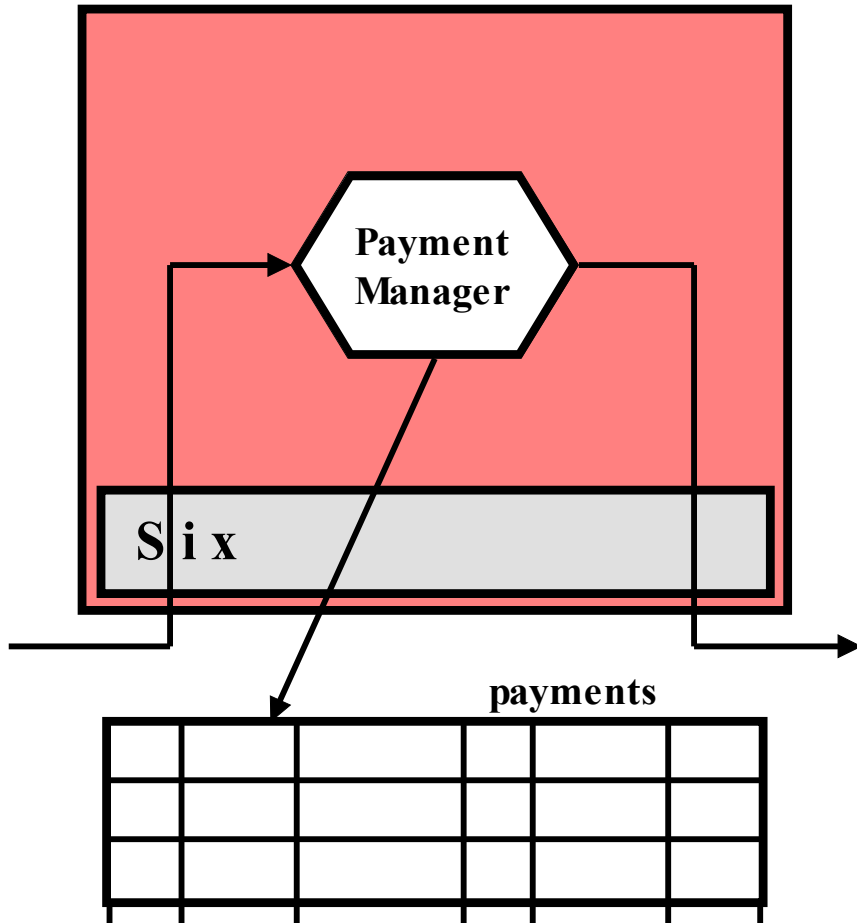
Acs



Management
of certificates of:

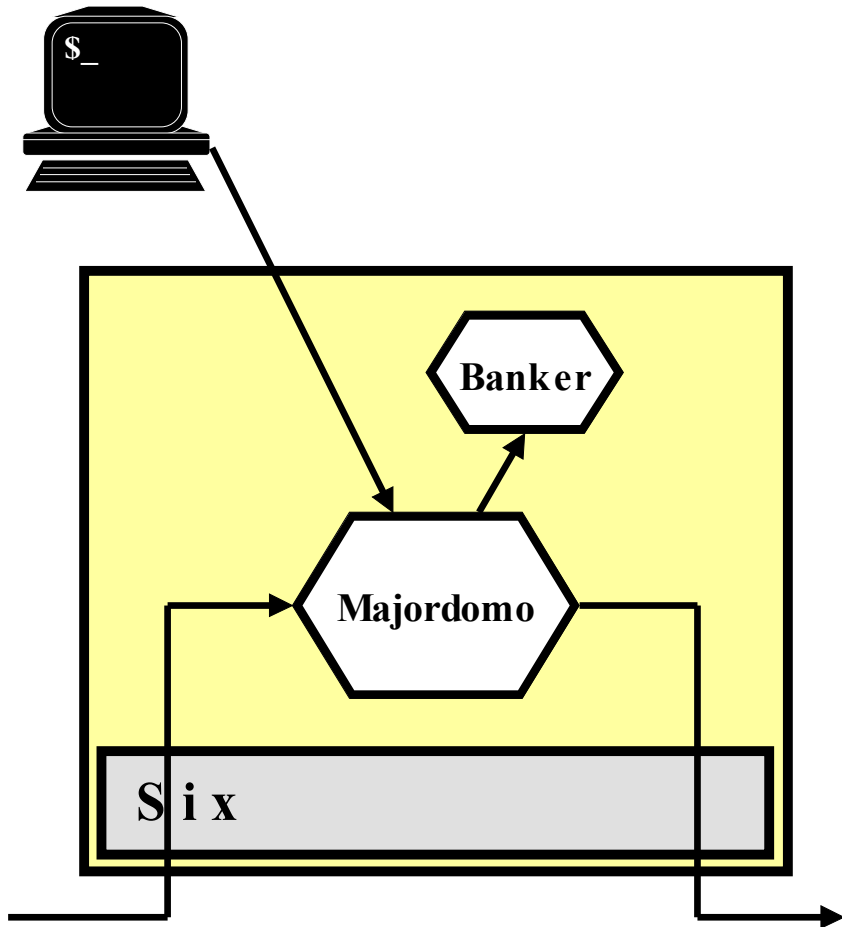
- Esos
- Mixes
- Banks

Bank



- Accepts money from clients
- management of anonymous accounts
- payments to Esos (payment's validity checks)

Client

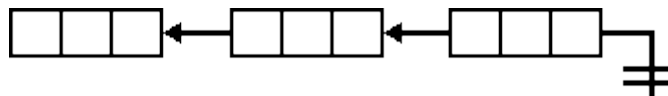
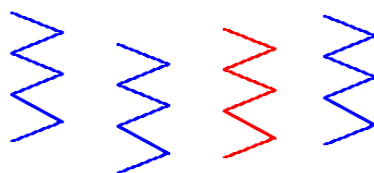


operations:

- upload file
- search for file
- download file

Technology used

- objects
- threads
- FreeBSD
- STL
- RSAEuro



RSA Data Security.

Upload file



Request for Eso certificates

Request for storage

File to store

Upload file



Request for Eso certificates

Request for storage

File to store

Upload file

A horizontal brushstroke in a vibrant yellow color, with a slightly textured, painterly appearance, extending across the width of the slide below the title.

Request for Eso certificates

Request for storage

File to store

Search for file



Request for Eso certificates

Request to search for file

Search for file



Request for Eso certificates

Request to search for file

Download file



Request for Eso certificates

Request for file

Download file




Request for Eso certificates

Request for file

Summary



- search for data
- store data
- anonymous communication
- protocols for e-payments
- time synchronization
- administrator interface
- extendability
- Eso - TCB, Client
- Eso - TCB, encryption
- Mix, onion routing
- Bank, Bankers
- Scheduler, Synchronizer
- config & log files
- Six, GMessage



Eternity Service

<http://www.kolej.mff.cuni.cz/~eternity>