

VTB hackathon API 2023

Решение кейса «Алгоритмы ГОСТ»

от команды GhOSTs 

Команда GhOSTs 🧛



Юрий Лебединский
Full Stack



Леонид Безвершенко
Security Analyst

Трек 2. Алгоритмы ГОСТ

Обеспечить надежный и безопасный обмен персональными данными между системами, минимизируя риски утечки или искажения информации

Решение

Создать инструмент для безопасного обмена данными, содержащими персональную информацию, между различными системами:

Решение

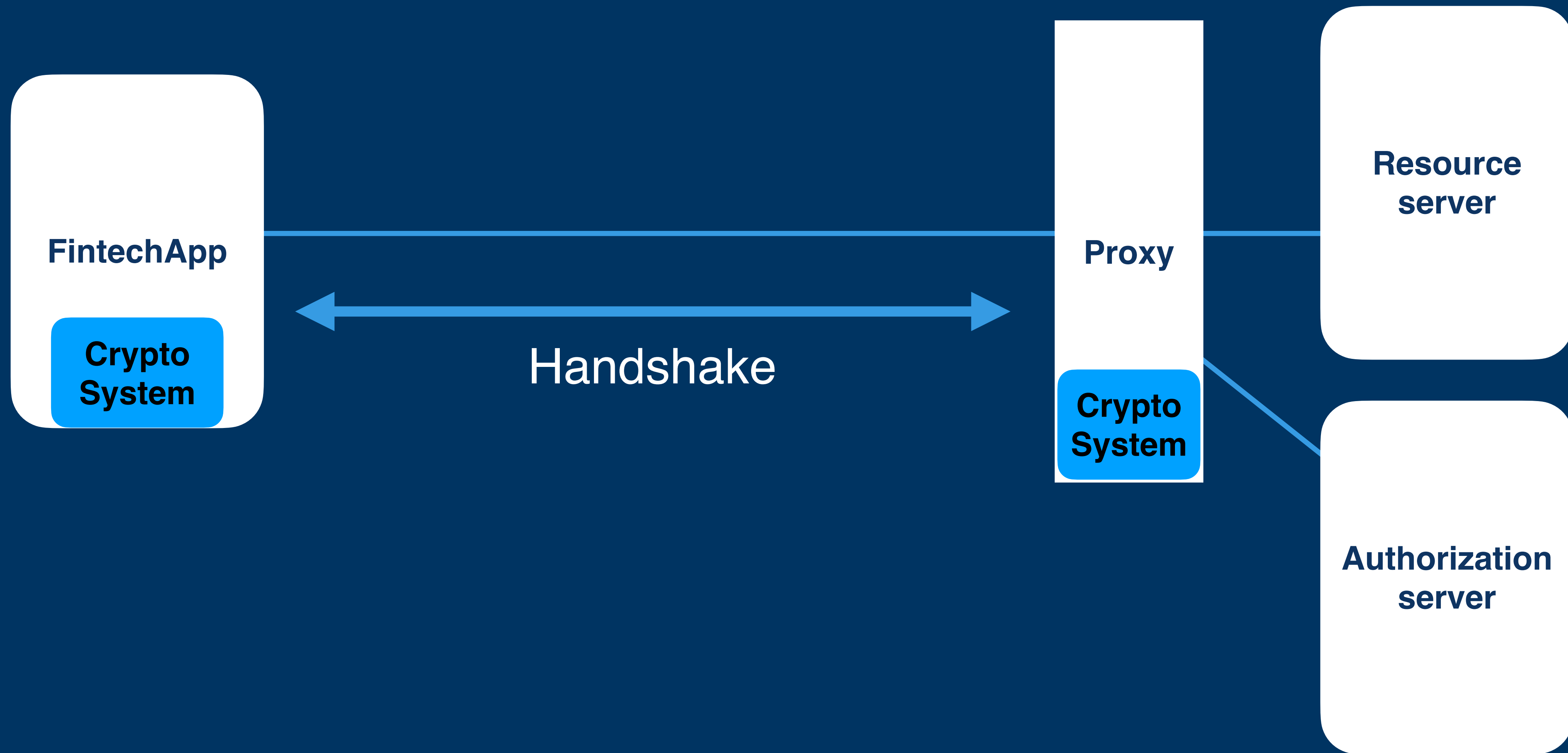
Создать инструмент для безопасного обмена данными, содержащими персональную информацию, между различными системами:

1. Аутентификация с использованием **OIDC**
2. Поддержка **sync/async** взаимодействия с API
3. Поддержка алгоритмов **ГОСТ**
4. Проверка **ФЛК**

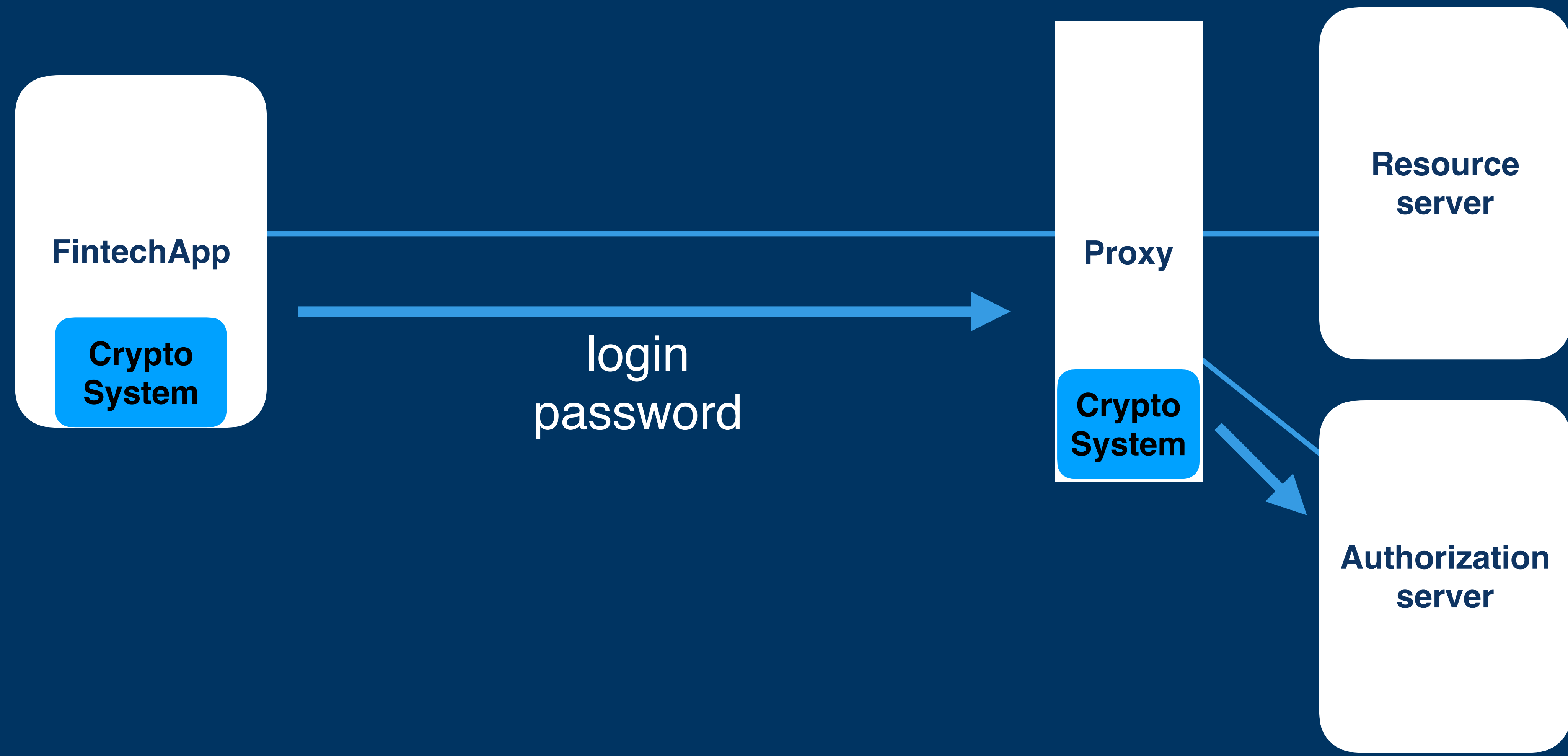
Cxema



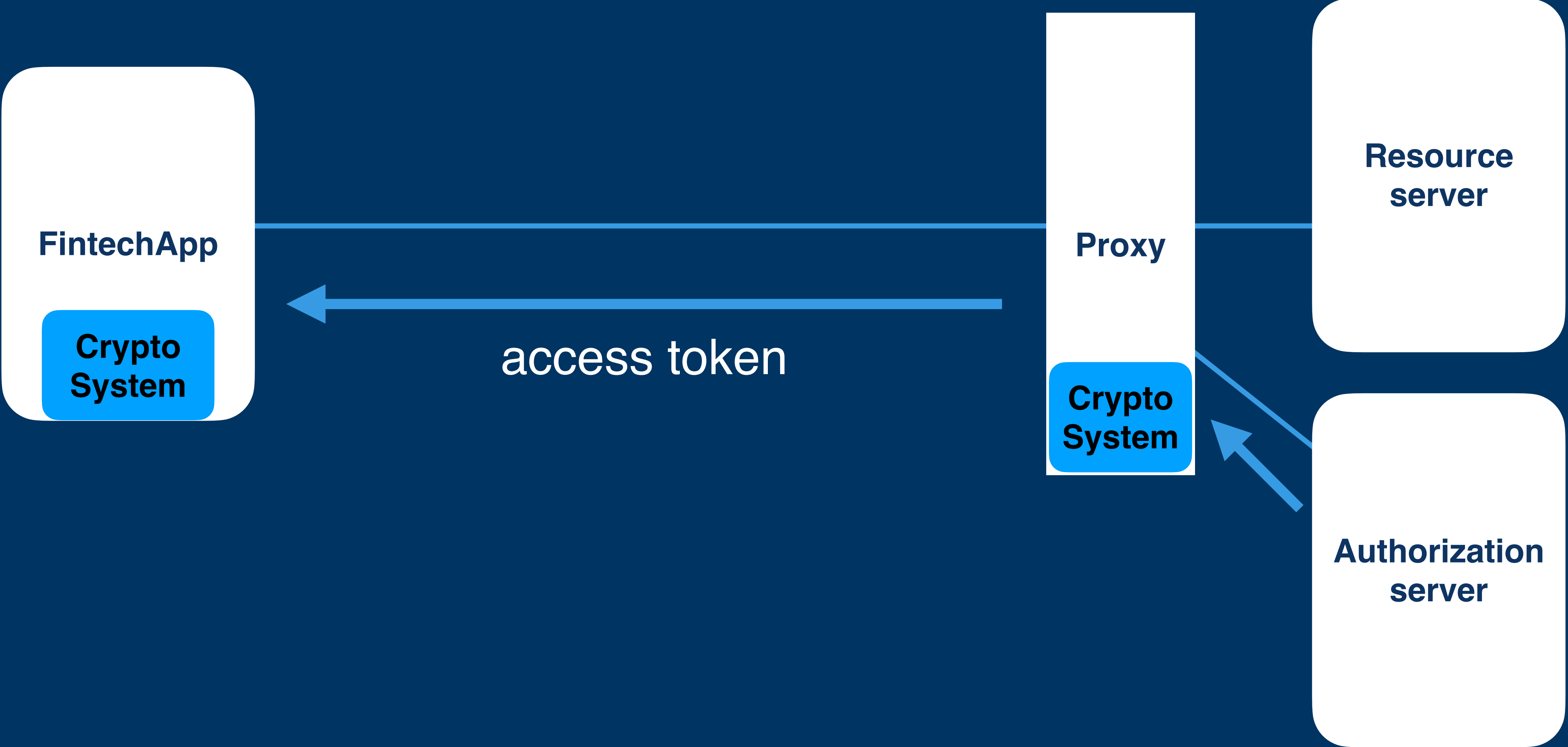
Cxema



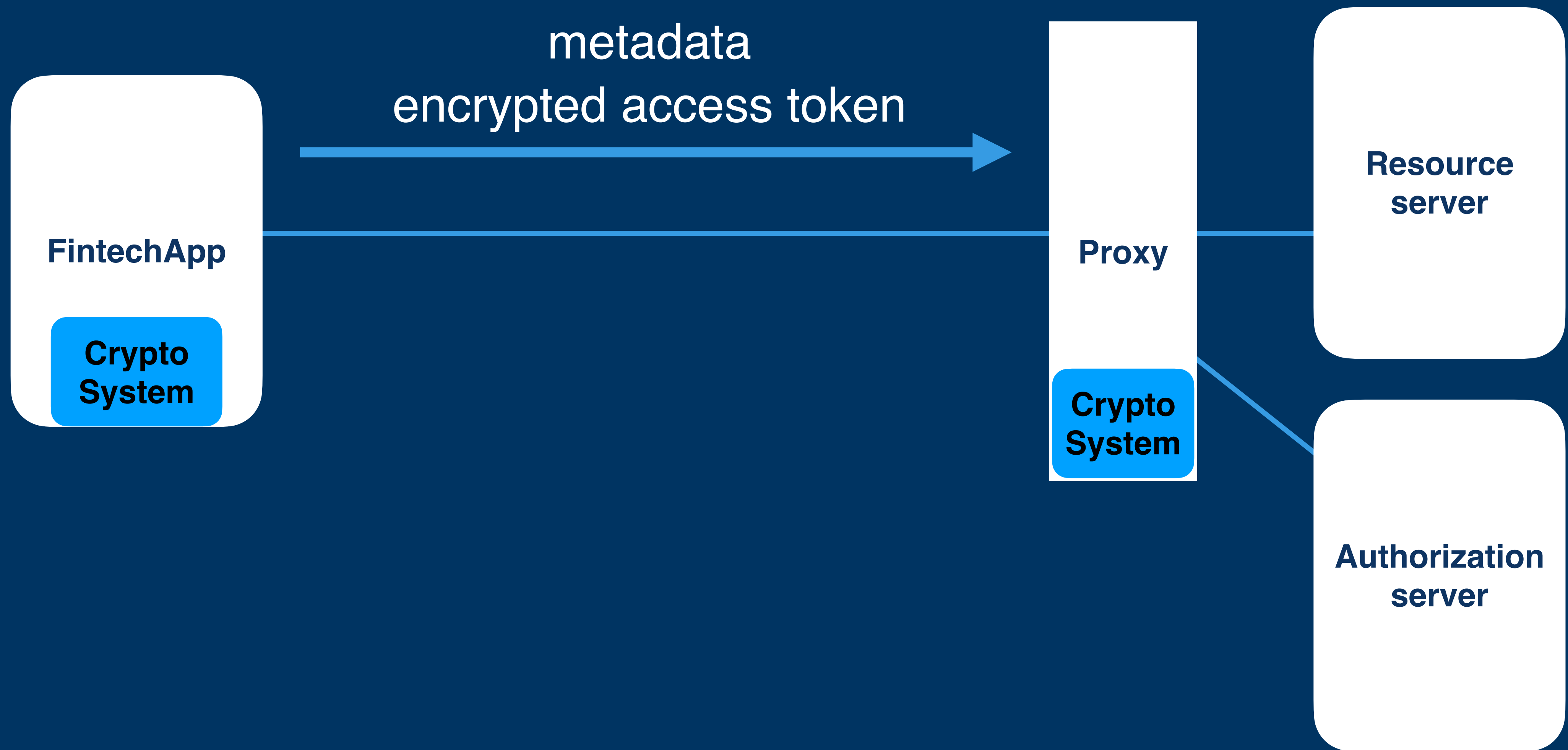
Cxema



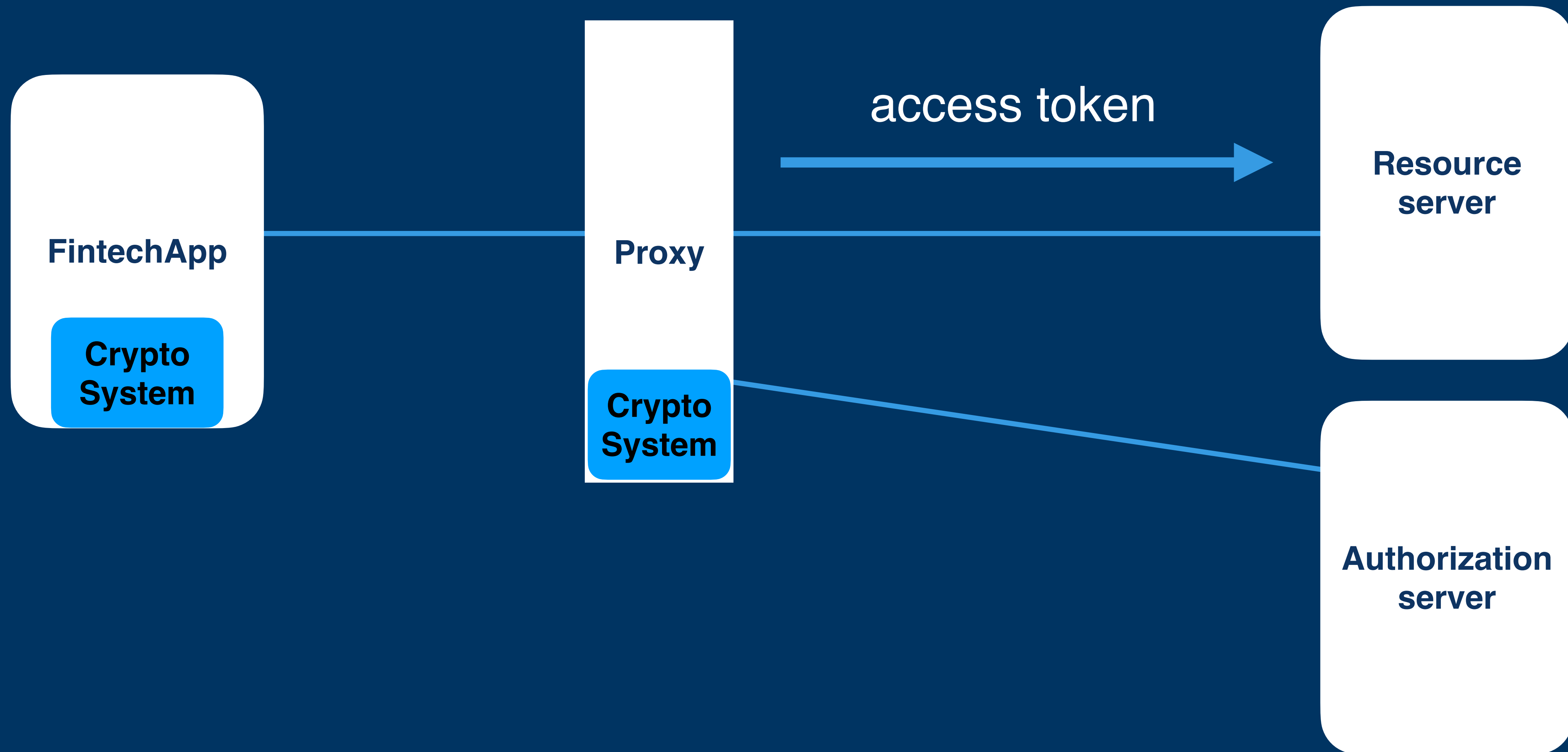
Cxema



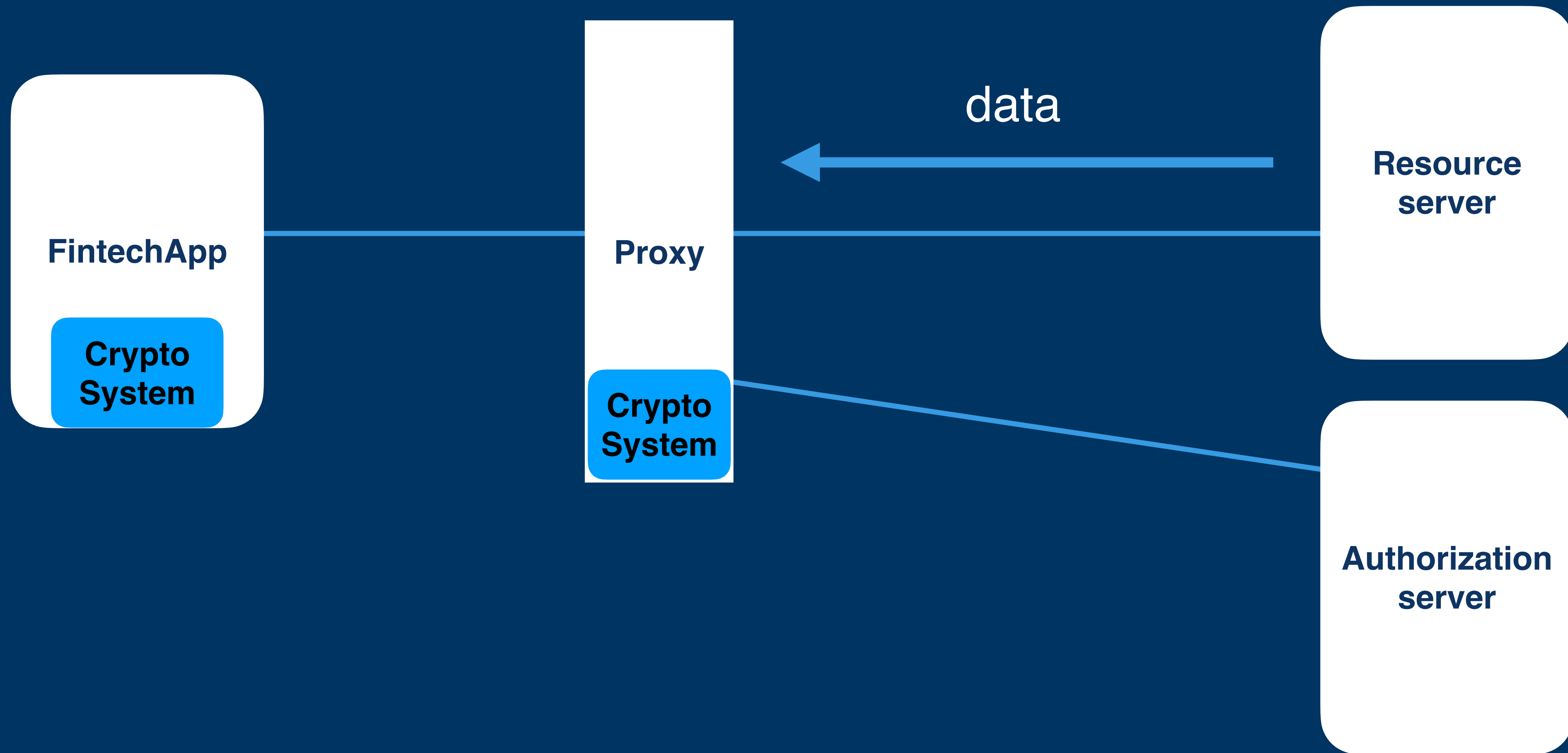
Cxema



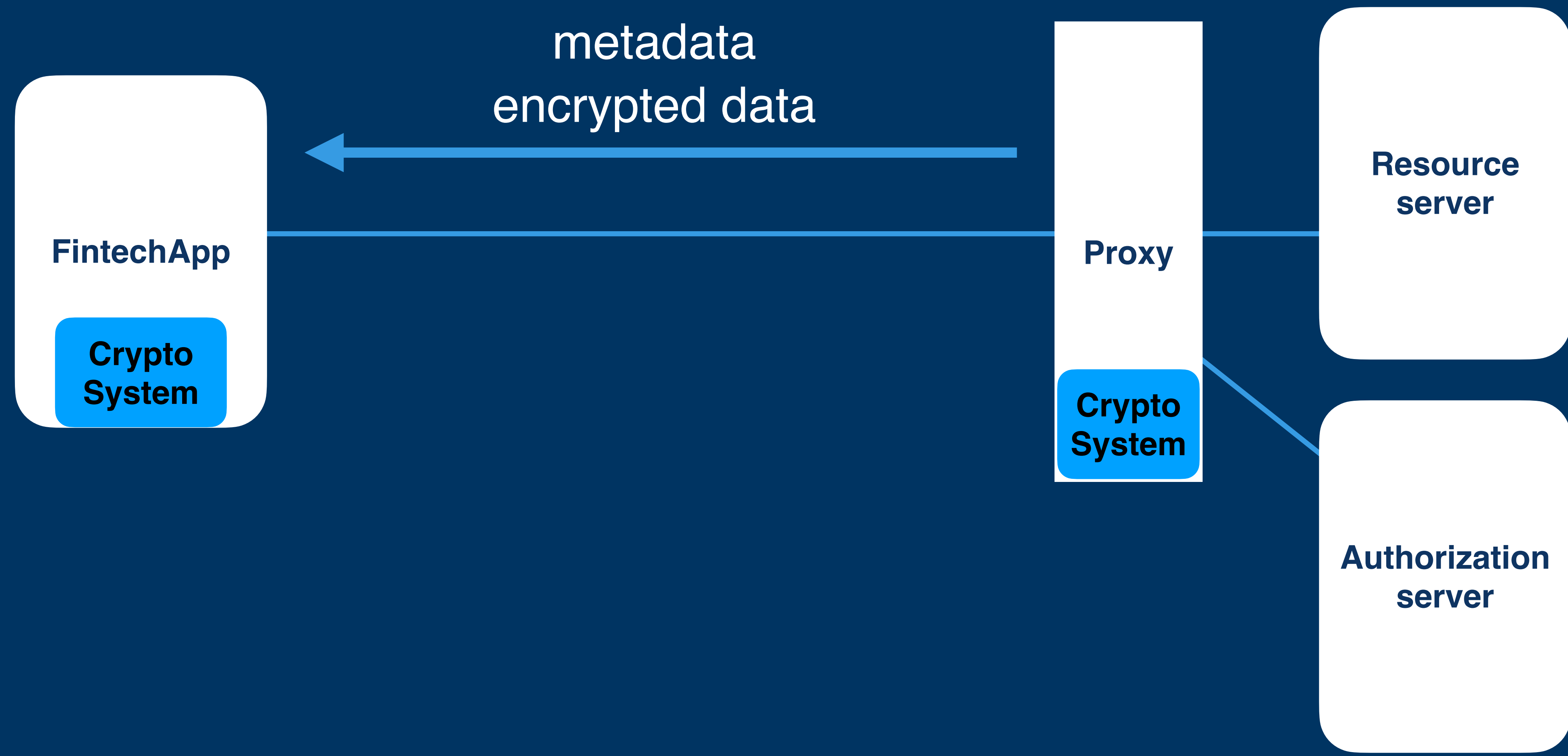
Cxema



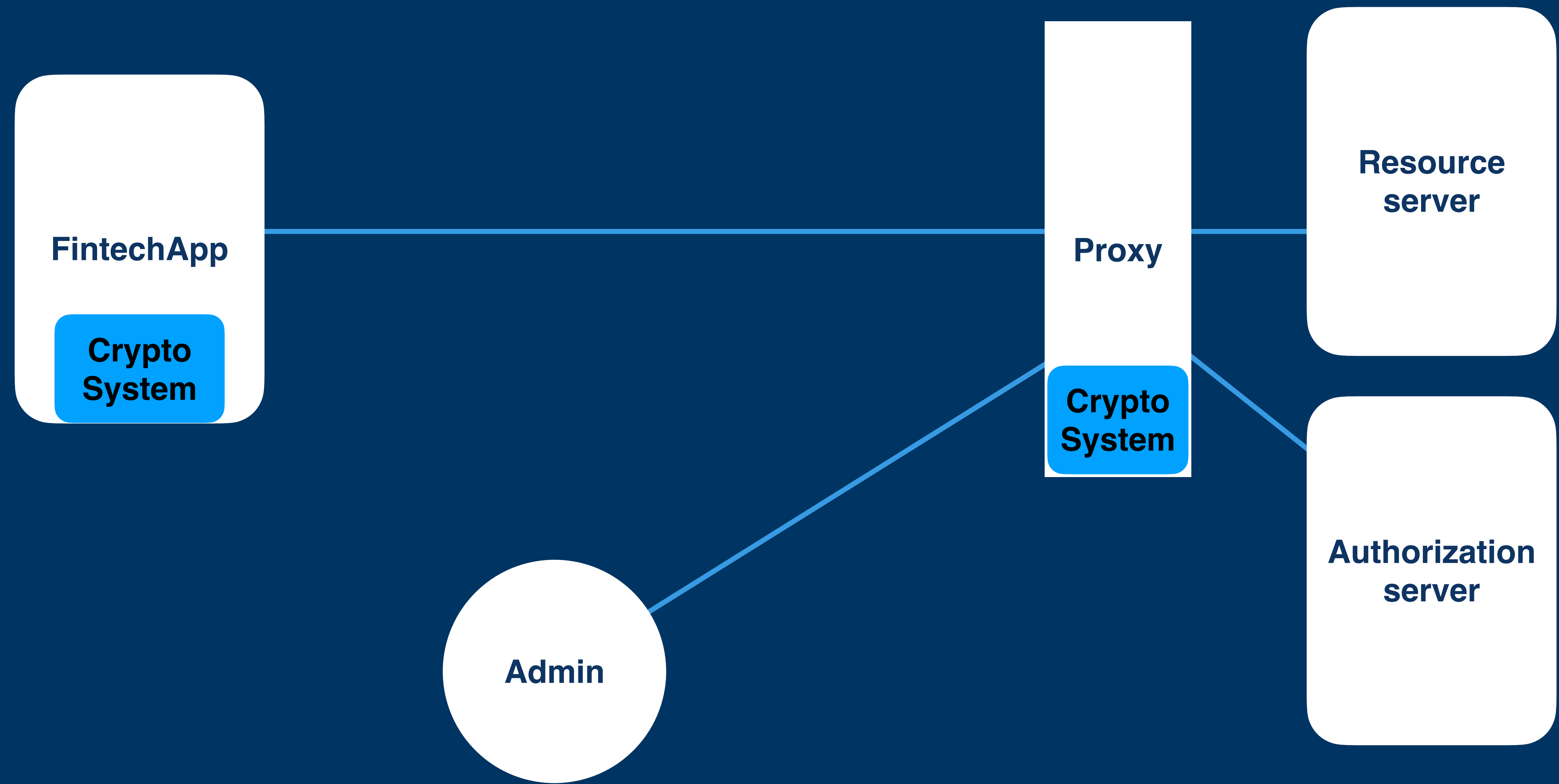
Cxema



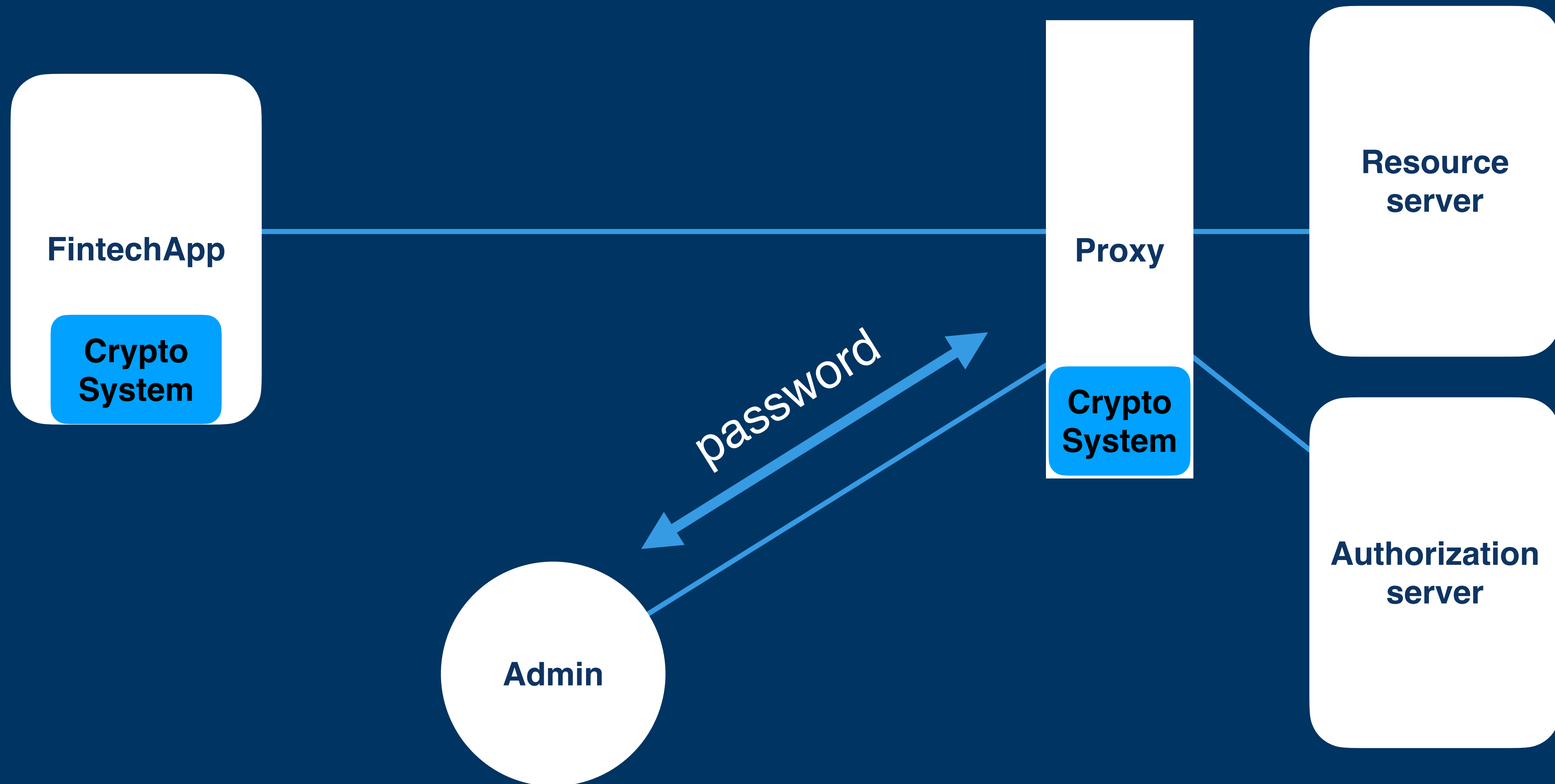
Cxema



Cxema



Cxema



Поддерживаемые алгоритмы

Цифровая подпись:

- Алгоритмы формирования и проверки ЭЦП: ГОСТ, RSA

Хэш-функция:

- SHA-2, SHA-3, ГОСТ

Шифры:

- Асимметричный: RSA
- Симметричный: AES, Кузнечик, Магма

Поддерживаемые алгоритмы

Цифровая подпись:

- Алгоритмы формирования и проверки ЭЦП: ГОСТ, RSA

Хэш-функция:

- SHA-2, SHA-3, ГОСТ

Шифры:

- Асимметричный: RSA

- Симметричный: AES, Кузнечик, Магма

Дополнительно:

- Авторизация: ГОСТ

- Аутентификация с использованием **OIDC**

VTB hackathon
API 2023

Спасибо за внимание!