ФИНТЕХ
АССОЦИАЦИЯ

PKI И БЛОКЧЕЙН:
ОПЫТ ИНТЕГРАЦИИ
В ПЛАТФОРМЕ МАСТЕРЧЕЙН

Алексей Цветков,
Ассоциация ФинТех

АССОЦИАЦИЯ РАЗВИТИЯ ФИНАНСОВЫХ ТЕХНОЛОГИЙ

ФИНТЕХ АССОЦИАЦИЯ

Разрабатываем и внедряем новые технологические решения для развития финансового рынка:

программное обеспечение, стандарты и протоколы, а также готовим предложения по созданию и изменению законодательства в области цифровой экономики.

Банк России
ГАЗПРОМБАНК
НСПК
РоссельхозБанк
ВТБ
открытие БАНК
QIWI
Альфа-Банк
СБЕРБАНК
Тинькофф Банк
Ак Барс Банк
Райффайзенбанк
МОСКОВСКАЯ БИРЖА
ПСБ
МОСКОВСКИЙ КРЕДИТНЫЙ БАНК
РНКО ПЛАТЕЖНЫЙ ЦЕНТР
ВСК СТРАХОВОЙ ДОМ
Абсолют Банк
МегаФон
АЛЬФА СТРАХОВАНИЕ
РОСБАНК SOCIETE GENERALE GROUP
СОВКОМБАНК
Ростелеком
МТС
ГРУППА КОМПАНИЙ РЕГИОН
СКБ-БАНК
Ренессанс СТРАХОВАНИЕ
Русский Стандарт БАНК
Яндекс
ПОЧТА БАНК
РЕСО ГАРАНТИЯ
РОСГОССТРАХ

ПЛАТФОРМА МАСТЕРЧЕЙН

ФИНТЕХ АССОЦИАЦИЯ

Платформа распределенных реестров для финансовых институтов, сертифицирована ФСБ и соответствует требованиям Банка России.

На базе ГОСТ-криптографии реализованы:

- TLS с двусторонней аутентификацией (КриптоПро)
- протокол исполнения смарт-контрактов (EVM)
- сервис передачи конфиденциальных сообщений
- средства мониторинга и администрирования

Программный код и результаты выполнения смарт-контрактов в сети Мастерчейн имеют доступность, целостность и неотказуемость.

Как оператор сети мы требуем использовать в прикладных контрактах разработанные нами механизмы отключения и обновления кода.

```
// Контракт с возможностью отключения
contract Suspendable {

    // Флаг отключения
    bool public disabled;

    // Барьер: отключен ли контракт?
    modifier enabled() {
        require(disabled == false);
        _;
    }
    // Функция проверки прав администратора,
    // реализуется в дочерних контрактах
    function canDisable()
    public view returns(bool);

    // Отключить для изменения
    function disable() public enabled {
        require(canDisable());
        disabled = true;
```

```
// Контракт с возможностью обновления
contract Upgradable is Suspendable {

    // Адрес предыдущей версии
    Upgradable public precursor;

    // Адрес следующей версии
    Upgradable public successor;

    // Инициализировать с указанием
    // адреса предыдущей версии
    function Upgradable(Upgradable _precursor)
    public {
        if (_precursor != address(0))
            _precursor.upgradeWith(this);
        precursor = _precursor;
    }
```

```
    // Указать адрес следующей версии
    // и отключить
    function upgradeWith(Upgradable _successor)
    public {
        disable();
        successor = _successor;
    }

    // Название смарт-контракта
    function contractName()
    public pure returns(string);

    // Версия смарт-контракта
    function contractVersion()
    public pure returns(string);

}
```

ПРИЛОЖЕНИЯ НА ПЛАТФОРМЕ

ФИНТЕХ АССОЦИАЦИЯ

Взаимодействие участников сети Мастерчейн происходит по единым для всех правилам, фиксируемым в реестре.

Пилотные и промышленные кейсы:

- регистрация и учёт ценных бумаг (закладные)
- торговое финансирование (гарантии, аккредитивы)
- передача платёжной информации

ПОСТАНОВКА ЗАДАЧИ

ФИНТЕХ АССОЦИАЦИЯ

Обеспечить безопасность взаимодействия финансовых институтов.

Участники финансового рынка:

- самостоятельно управляют своей инфраструктурой
- строят бизнес-процессы обособленно

Зрелость процессов обеспечения безопасности

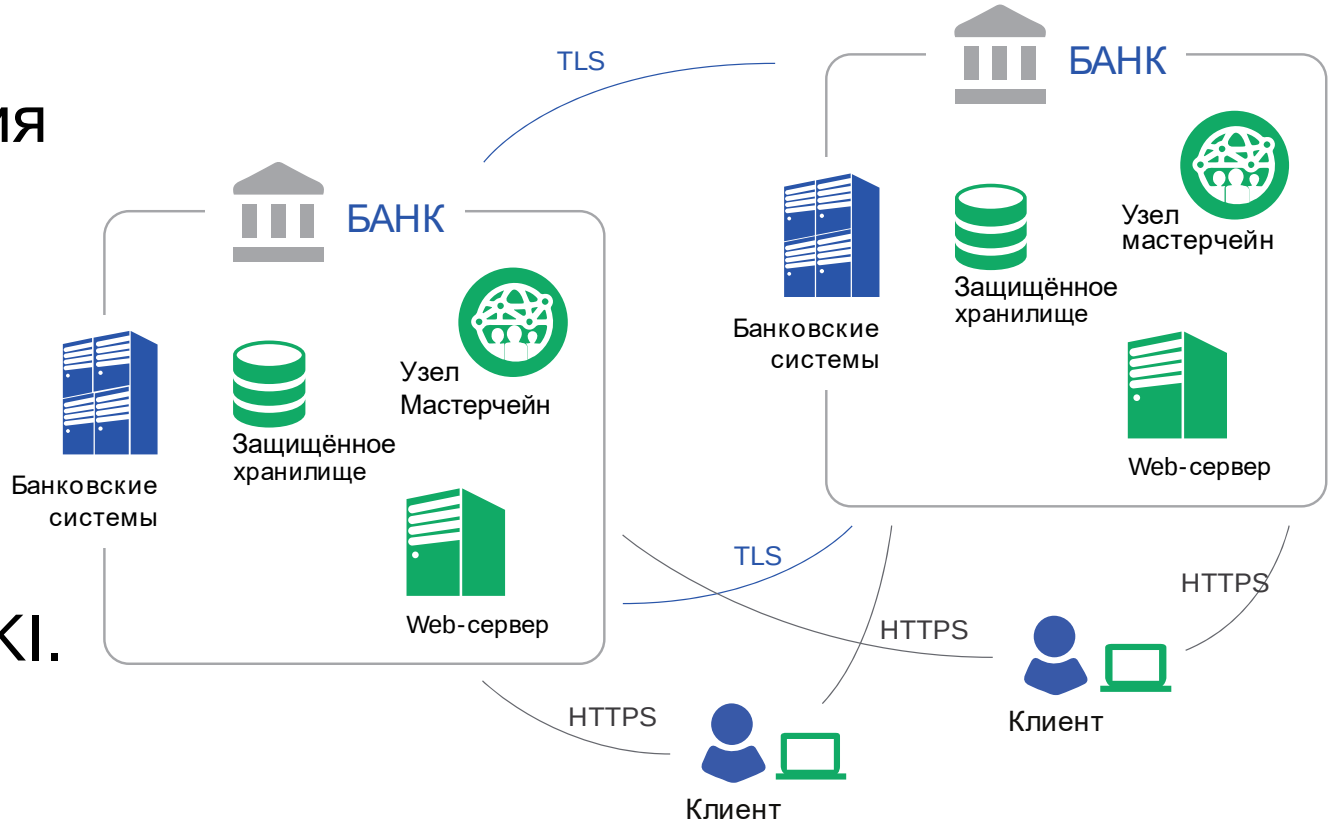
сильно различается между организациями.

ПРИМЕНИМОСТЬ ТРАДИЦИОННОГО РЕШЕНИЯ

ФИНТЕХ АССОЦИАЦИЯ

Системы распределённых реестров позволяют объединить ресурсы каждого участника в доверенную цифровую среду.

Для согласованного управления ключами электронной подписи и подтверждения цифровой идентичности используется PKI.



СЕРТИФИКАЦИЯ КЛЮЧЕЙ РАЗДЕЛЬНОГО НАЗНАЧЕНИЯ

ФИНТЕХ АССОЦИАЦИЯ

Оператор сети является оператором распределённого КриптоПро УЦ 2.0.

Он управляет выпуском и отзывом сертификатов участников сети.

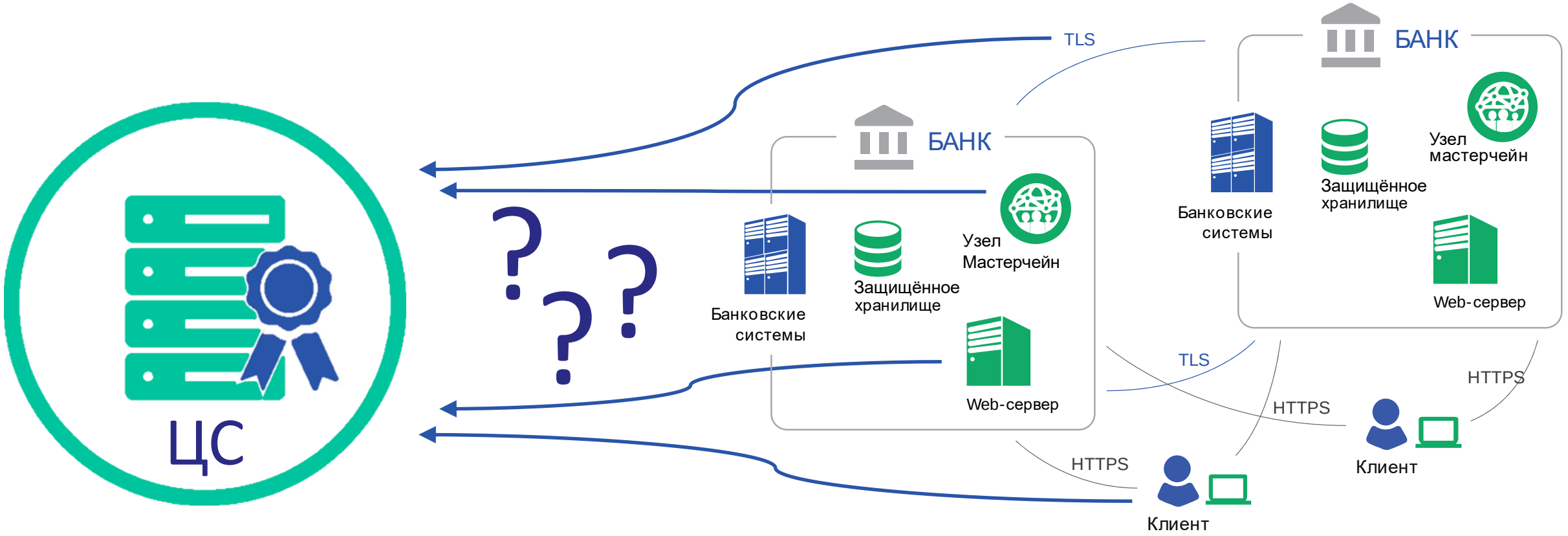
В шаблоны выпускаемых сертификатов добавлены идентификаторы расширенного назначения для разделения ключей по типам операций:

1.2.643.6.57.1.**1.1.1**	[TLS Server]	Узел Мастерчейн
1.2.643.6.57.1.**1.1.2**	[TLS Client]	Узел Мастерчейн
1.2.643.6.57.1.**1.1.3**	[TLS Server]	API узла Мастерчейн
1.2.643.6.57.1.**1.3.1**	[Sign]	Узел Мастерчейн
1.2.643.6.57.1.**2.1.1**	[TLS Server]	API СПКС
1.2.643.6.57.1.**2.1.2**	[TLS Client]	API СПКС
1.2.643.6.57.1.**2.2.1**	[Sign]	Узел СПКС
1.2.643.6.57.1.**2.4.1**	[Encryption]	Хранилище СПКС
1.2.643.6.57.1.**2.4.2**	[Encryption]	Робот ИС
1.2.643.6.57.1.**2.4.3**	[Encryption]	Менеджер ИС
1.2.643.6.57.1.**3.1.3**	[TLS Client]	АРМ Админ сети
1.2.643.6.57.1.**3.2.1**	[Sign]	Админ сети АФТ
1.2.643.6.57.1.**3.2.2**	[Sign]	Админ Whitelist
1.2.643.6.57.1.**5.1.1**	[TLS Server]	API ИС
1.2.643.6.57.1.**5.1.2**	[TLS Client]	API ИС
1.2.643.6.57.1.**5.1.3**	[TLS Client]	АРМ ИС
1.2.643.6.57.1.**5.2.1**	[Sign]	АРМ ИС Админ АФТ
1.2.643.6.57.1.**5.2.2**	[Sign]	АРМ ИС Робот
1.2.643.6.57.1.**5.2.3**	[Sign]	АРМ ИС Админ
1.2.643.6.57.1.**5.2.4**	[Sign]	АРМ ИС Менеджер

СПЕЦИФИКА РАСПРЕДЕЛЁННЫХ РЕЕСТРОВ

ФИНТЕХ АССОЦИАЦИЯ

В среде распределённых реестров PKI должна быть встроена так, чтобы сохранить отказоустойчивость и производительность.



СМАРТ-КОНТРАКТ РЕЕСТРА МАСТЕРЧЕЙН

ФИНТЕХ АССОЦИАЦИЯ

В системном контракте в блокчейне перечислены:

- веб-сервисы сети (узлы) с указанием организации-владельца
- организации участники-сети с перечислением их сертификатов
- сертификаты X.509 и назначенные им должностные полномочия

РАСШИРЕННАЯ СХЕМА ЭЛЕКТРОННОЙ ПОДПИСИ

ФИНТЕХ АССОЦИАЦИЯ

Цели и причины использования:

- совместимость с протоколом Ethereum
- сокращение объёма хранимой и передаваемой информации

ИДЕНТИФИКАЦИЯ СЕРТИФИКАТОВ И СПИСКОВ ОТЗЫВА

ФИНТЕХ АССОЦИАЦИЯ

В качестве идентификатора сертификата в смарт-контракте реестра участников используется поле X.509 v2 Subject Key Identifier. Его значение не должно иметь коллизии в рамках одного УЦ.

- 160 бит SKID соответствуют формату адреса Ethereum
- для использования сертификатов разных УЦ в одной сети требуется включить в структуру транзакции поле Authority KID
- сертификаты УЦ и списки отзыва доступны в реестре по AKID
- компоненты ИС могут обновлять COC из реестра, а не из CDP

РЕЕСТР НЕКВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ

ФИНТЕХ АССОЦИАЦИЯ

Распределённый реестр с авторизацией, автоматизацией операций в смарт-контрактах, с контролем целостности и доступностью в LAN.

Отметка об отзыве сертификата, о сроках годности полномочий и ОРГН владельца сертификата доступны для логики смарт-контрактов.

```
/// @notice Реестр AKID => SKID => запись о ключе
mapping(address => mapping(address => Key)) public keys;

/// @notice Запись о ключе
struct Key {
    bool      enabled;        /// флаг действительности/блокировки
    bytes32   owner;          /// ID организации из сертификата
    bytes     certificate;    /// байты сертификата ключа
    bytes     revocationList; /// байты списка отзыва ключа УЦ
    bytes32   revocationHMAC; /// HMAC списка отзыва в СПКС
    address   profile;        /// ID контейнера с профилем ключа
/// ...
```

РЕЕСТР НЕКВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ

ФИНТЕХ АССОЦИАЦИЯ

Распределённый реестр с авторизацией, автоматизацией операций в смарт-контрактах, с контролем целостности и доступностью в LAN.

```
12  /// ...
13      bytes32[] functionIds;    /// список ID функций ключа
14      /// реестр записей о функциях ключа
15      mapping(bytes32 => Function) functions;
16  }
17
18  /// @notice Запись о функции ключа
19  struct Function {
20      bytes32 reasonHMAC; /// HMAC архива с основанием для функции
21      uint64  startTime;  /// метка времени начала действия функции
22      uint64  expiryTime; /// метка времени окончания действия функции
23  }
```

Документы-основания для назначенных ключам полномочий,

а также COC для ключей УЦ доступны в распределённом файловом слое.

СОЧЕТАНИЕ PKI И БИЗНЕС-ЛОГИКИ ПРИЛОЖЕНИЙ

ФИНТЕХ АССОЦИАЦИЯ

Внедрить PKI в логику бизнес-процессов бывает сложно,
так как необходимо заменять ключи с течением времени.

Авторизация бизнес-операций должна происходить на основании отношений между организациями.

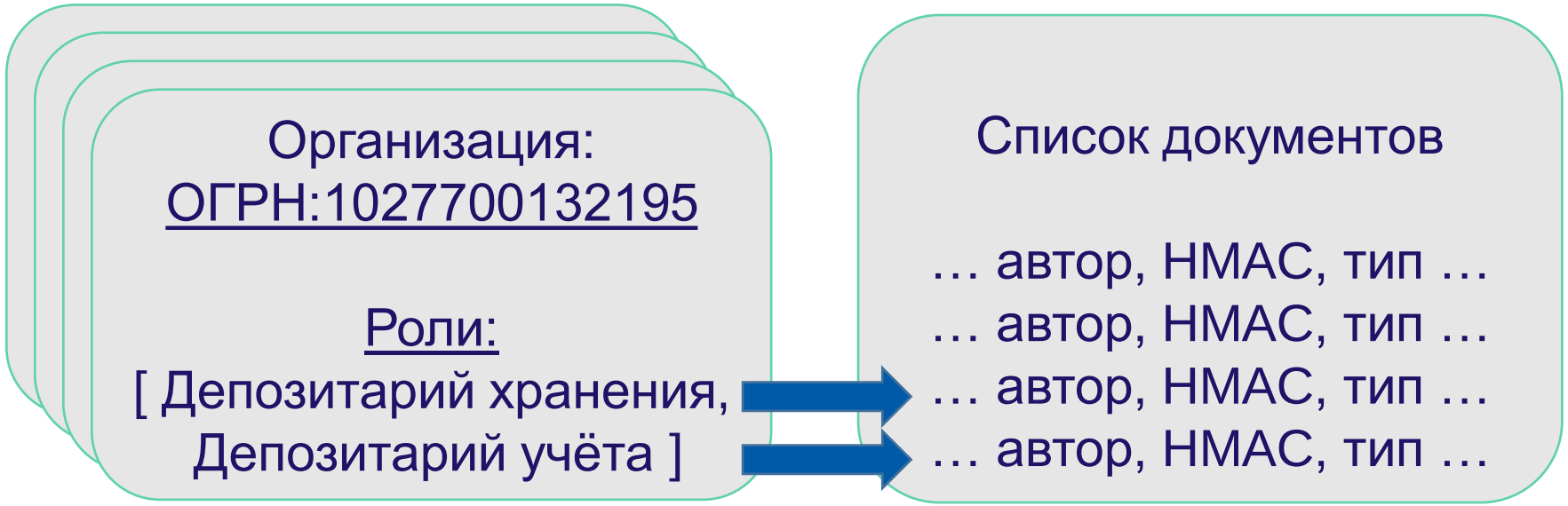
Структура отношений в сделке может быть многоуровневой, она не привязана к сертификатам.

СМАРТ-КОНТРАКТ БИЗНЕС-ПРОЦЕССА

ФИНТЕХ АССОЦИАЦИЯ

Каждая сделка в блокчейне представлена перечислением:

- организаций-участников и их ролей в процессе
- конфиденциальных документов (сертификат автора, HMAC, тип, …)



СМАРТ-КОНТРАКТ РОЛЕВОЙ МОДЕЛИ

ФИНТЕХ АССОЦИАЦИЯ

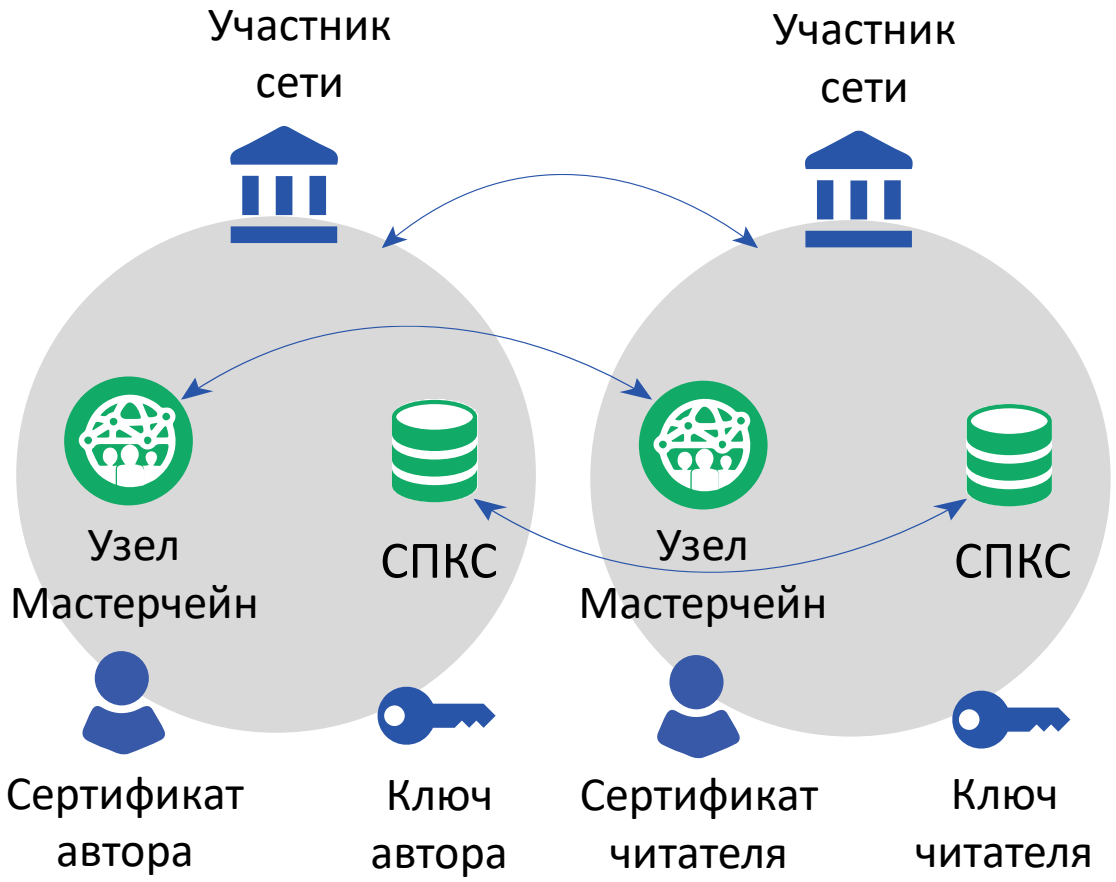
Разработчик приложения записывает матрицу прав доступа в контракт.

Права	Тип объекта доступа	Полномочия ключа	Роли организаций
Чтение	Ипотечная закладная	Менеджер	[Депозитарий хранения]
Запись	Черновик гарантии	Операционист	[Банк-гарант]
Чтение	Документ-основание для назначения роли	*Любые*	[*Любые*]
Запись	Назначение полномочий ключа	Администратор	[Оператор сети]

СЕРВИС ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНЫХ СООБЩЕНИЙ

ФИНТЕХ АССОЦИАЦИЯ

Веб-сервис предоставляет доступ к документам согласно ролевой модели.



1. Аутентификация запросов и ответов производится по сертификатам.
2. В реестре публикуются события о сохранении документов на узлах.
3. Читатель по записи в реестре находит узел и запрашивает документ.
4. Копию документа читатель сохраняет на своём узле сети.

РОЛЕВАЯ МОДЕЛЬ МАСТЕРЧЕЙН

ФИНТЕХ АССОЦИАЦИЯ

Системные смарт-контракты платформы обеспечивают:

- независимость бизнес-процессов от процесса управления ключами
- конфиденциальность документов, их целостность и неотказуемость

Мастерчейн полноценно использует и расширяет концепцию PKI.

Средства платформы позволяют повысить доступность
и удобство использования сертификатов.

Ролевая модель и средства администрирования позволяют
отделить управление сертификатами ключей от бизнес-логики.

Дополнительные механизмы авторизации реализованы
в виде программного кода в распределённом реестре.

СПАСИБО ЗА ВНИМАНИЕ!

ФИНТЕХ АССОЦИАЦИЯ

Добро пожаловать для вопросов и предложений!

Алексей Цветков

Руководитель разработки,

Развитие технологии распределённых реестров

Ассоциация ФинТех

alexey.tsvetkov@fintechru.org