

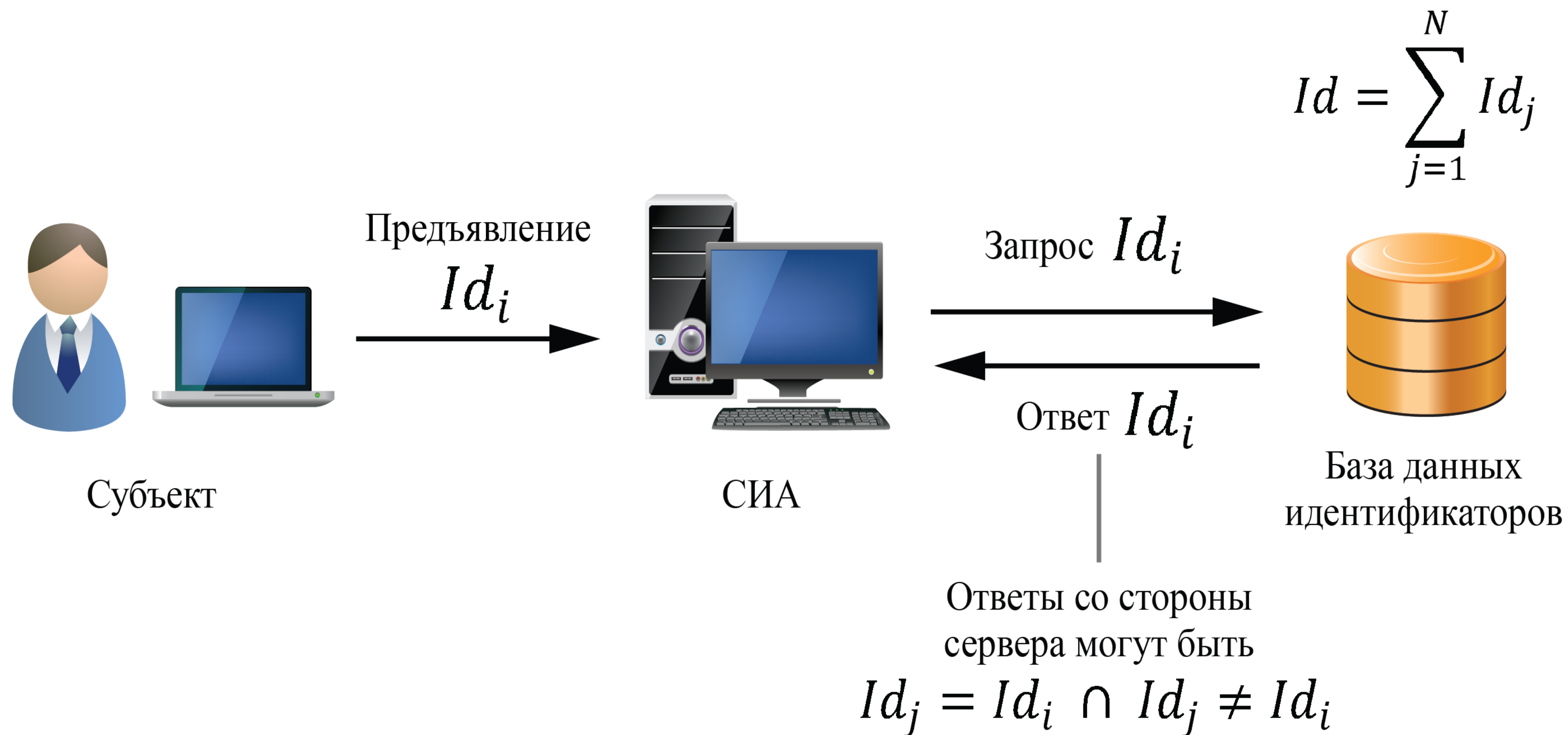
Концептуальные основы трансляции доверия к идентификации личности при удаленном электронном взаимодействии

Уральский Форум, 19 февраля 2015 г.



Алексей Сабанов
Зам. генерального директора
ЗАО «Аладдин Р.Д.»

Идентификация претендента

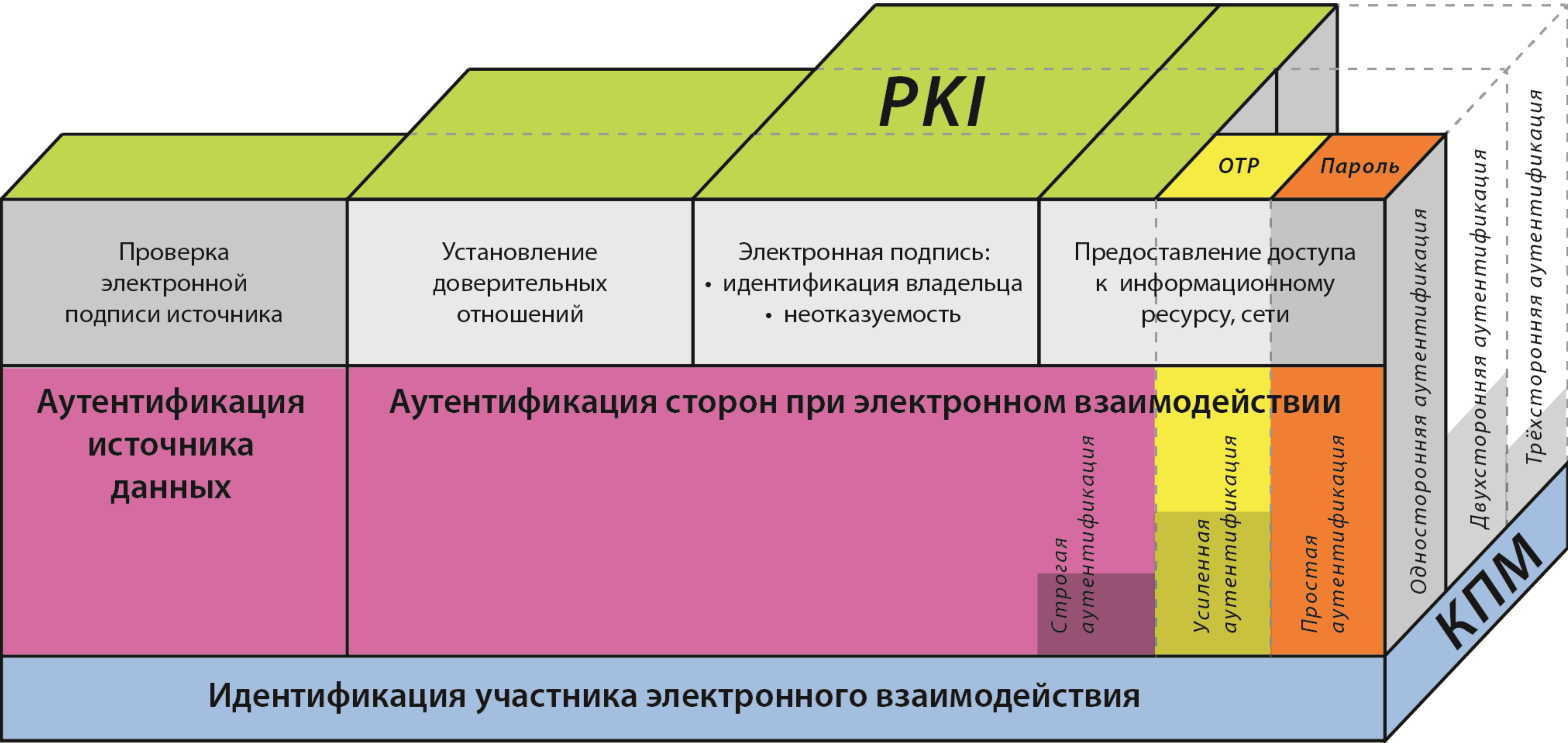


Классификация идентификаторов



ВИДЫ идентификаторов	типы систем идентификации						
	1	2	3	4	5	6	7
универсальный (У), корпоративный (К), личный (Л)	У	У	У	К	К	К	Л
анонимный (Х) или персональный (П)	УХ	УП	УП	КХ	КХ	КП	ЛП
доступ одноразовый (О) или многократный (М)	УХМ	УПО	УПМ	КХО	КХМ	КПМ	ЛПМ
аналог (пример) в реальном (физическом) мире	деньги	запись в ЗАГС	паспорт	билет в кино	абонеме нт	бум.про пуск	биоме тр.
виртуальный (электронный) пример	анонимн ый пользо ватель Интерне та	генера тор ОТР	реестр ИНН,СНИ ЛС	электрон ный билет	пополня емая карта	смарт- карта в виде пропуск а	биоме тр. на карте или сервер е

Классификация механизмов аутентификации



3 вида ЭП – 3 типа аутентификации

Учетная запись пользователя	Секрет (аутентификатор)	Тип аутентификации
ЛОГИН	пароль	простая
Логин или поля X.509 (УЦ не аккредитован)	одноразовый пароль (технология ОТР) или Закрытый ключ	усиленная
заданные поля X.509, сформированного аккредитованным удостоверяющим центром для доступа пользователя	закрытый ключ (в терминах №1-ФЗ)	строгая

Проблемы идентификации

1. Несогласованность терминологии в законодательной и нормативной базе.
2. Проблемы доверия к идентификации клиента, проведенной аккредитованными УЦ.
3. Отсутствие простых и понятных рекомендаций для работников, занимающихся идентификацией личности. Зачастую идентификацией личности занимаются лица, не проходившие специальной подготовки. Отсутствие возможности оперативной и достоверной проверки данных, предоставленных для идентификации.
4. Сложность проверки документа, удостоверяющего личность, на подлинность.
5. Отсутствие на рабочих местах функционала, позволяющего осуществить автоматизированную проверку соответствия фотографии в документе, удостоверяющем личность с фотографией идентифицируемого лица (результат автоматизированной сверки в виде процента соответствия).
6. Низкий уровень персональной ответственности лица, осуществляющего идентификацию.
7. Отсутствие системы трансляции доверия к идентификации от одного банка другому.



Проблемы терминологии



Определение идентификации в 115-ФЗ

«**Идентификация** - совокупность мероприятий по *установлению* определенных настоящим ФЗ сведений о клиентах, их представителях, выгодоприобретателях, бенефициарных владельцах, по *подтверждению достоверности* этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий».

Другими словами, **идентификация** – это **ПРОЦЕСС** сравнения идентификатора, вводимого участником информационного взаимодействия в любую из информационных систем, указанных в пункте 4 Требований ПП-977 от 28.11.2011г., с идентификатором этого участника, содержащимся в соответствующем базовом государственном информационном ресурсе, определяемом Правительством РФ.

Идентификатор – уникальная метка для отличия одного объекта от другого. Присваивается при регистрации объекта.

Процесс – это совокупность мероприятий.

Упрощенная идентификация

упрощенная идентификация клиента - физического лица (далее также - упрощенная идентификация) - осуществляемая в случаях, установленных настоящим ФЗ, **совокупность мероприятий по установлению** в отношении клиента - физического лица фамилии, имени, отчества (если иное не вытекает из закона или национального обычая), серии и номера документа, удостоверяющего личность, и **подтверждению достоверности** этих сведений одним из следующих способов:

(в ред. ФЗ [от 05.05.2014 N 110-ФЗ](#))

с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;

(в ред. ФЗ [от 05.05.2014 N 110-ФЗ](#)) с использованием информации из информационных систем органов государственной власти, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования и (или) государственной информационной системы, определенной Правительством Российской Федерации;

(в ред. ФЗ [от 05.05.2014 N 110-ФЗ](#)) с использованием единой системы идентификации и аутентификации при использовании усиленной квалифицированной электронной подписи или простой электронной подписи при условии, что при выдаче ключа простой электронной подписи личность физического лица установлена при личном приеме.

(в ред. Федерального закона [от 05.05.2014 N 110-ФЗ](#)), т.е.тоже ПРОЦЕСС

Аутентификация

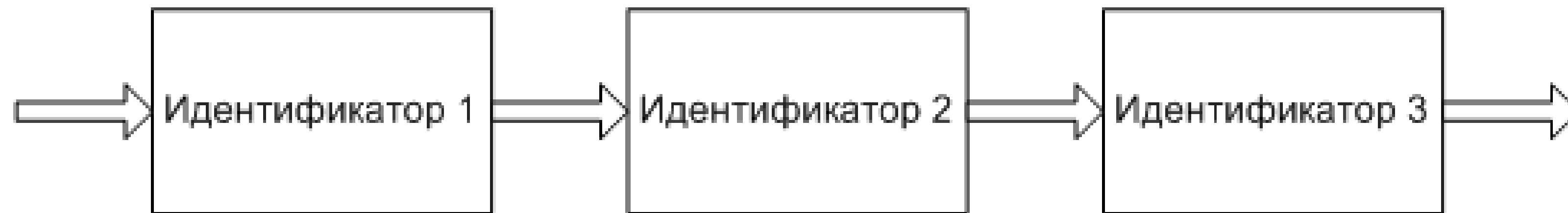
Аутентификация – это взаимосвязанные процессы **подтверждения подлинности** предъявленных заявителем идентификаторов (идентификатора) и **проверки принадлежности аутентификатора** (секрета, который знают обе стороны взаимодействия или о существовании которого знают обе стороны взаимодействия) и *идентификаторов* конкретному *лицу*.



Уровни достоверности идентификации



Модель идентификации



Вероятность отсутствия
ошибки идентификации

$$P = \prod_{k=1}^K p_k$$

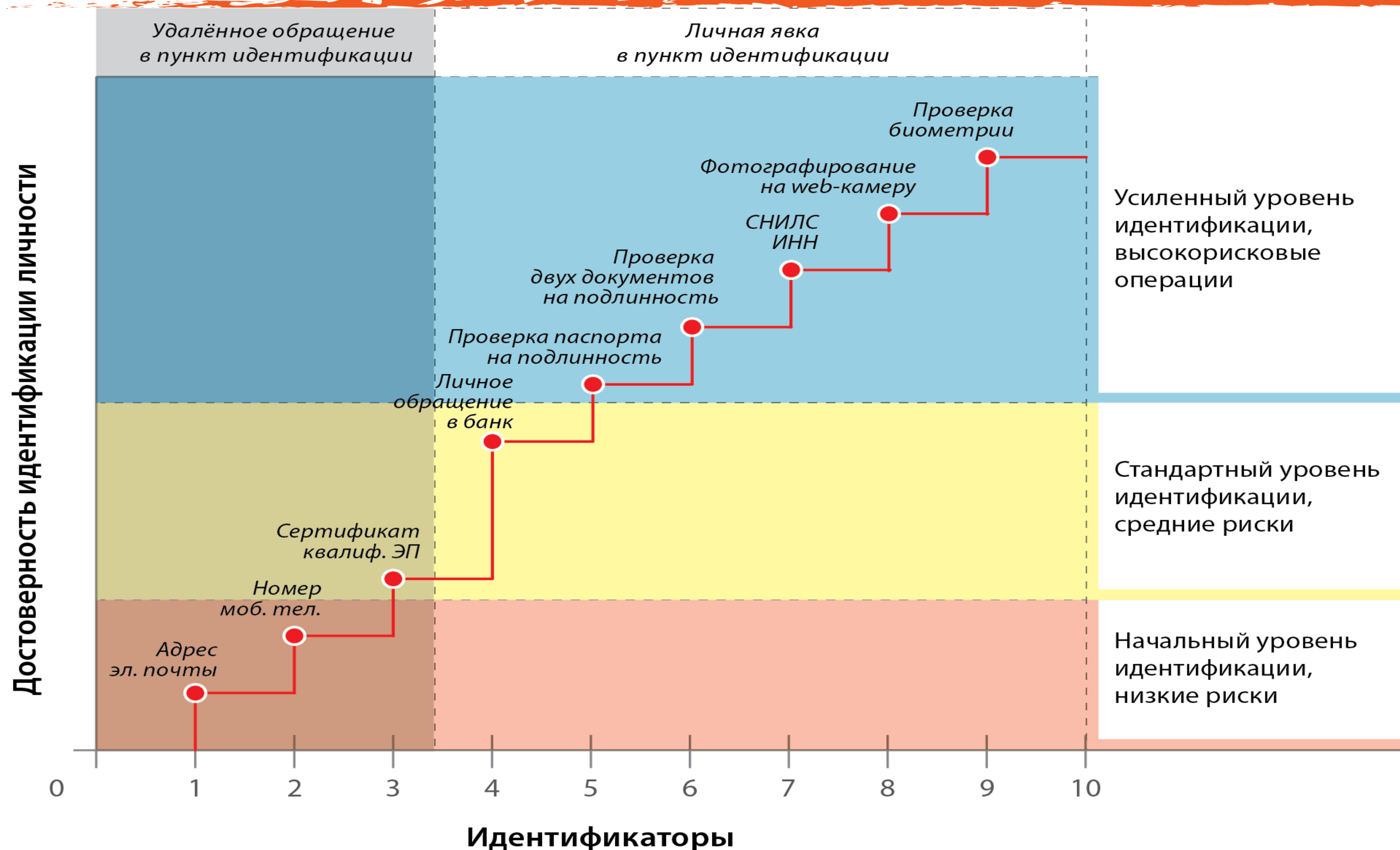
Степень достоверности = уровень безошибочности

Определение достоверности

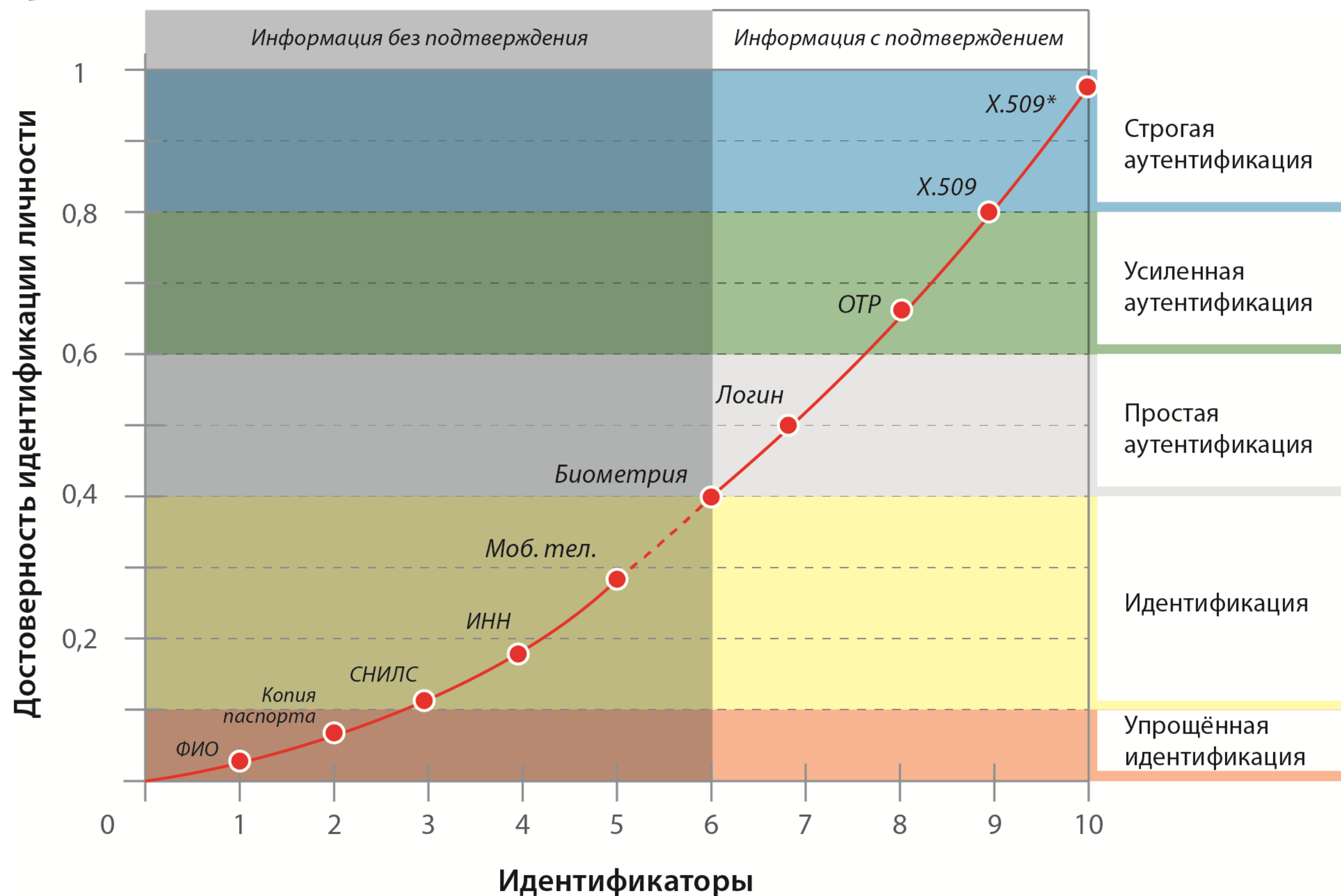
Достоверность информации - общая **точность и полнота** информации. **Достоверность** информации обратно пропорциональна вероятности возникновения ошибок в информационной системе.

Достоверность идентификации и аутентификации (ИА) определим как меру доверия к результатам идентификации и аутентификации при условии безошибочности выполнения процедур идентификации и аутентификации. Поскольку безошибочность может иметь уровни точности ее определения, также как и мера доверия к результатам ИА, то и мера доверия (то есть достоверность) может иметь уровни достоверности, называемые в западных нормативных источниках уровнями гарантий.

Достоверность можно накапливать



Достоверность идентификации



Доверие к идентификации

Основной критерий – Качество идентификации – отличие одного субъекта от другого путем сравнения предъявленных идентификаторов с занесенными в БД.

Имеются ошибки первого (легальный пользователь не идентифицирован) и второго рода (злоумышленник идентифицирован как легальный user).

Требует уровней доверия к результатам сравнения в зависимости от числа идентификаторов и механизмов сравнения. Требует протоколирования результатов для разбора конфликтных ситуаций.

Доверие к аутентификации

Только аутентификация доказывает привязку идентификаторов и аутентификатора к конкретной личности. Самая безопасная и надежная аутентификация основана на сертификате доступа с механизмом аутентификации в виде электронной подписи.

Основной Критерий – качество (безопасность и надежность) аутентификации.

Необходимо ввести уровни доверия к аутентификации.

Зачем нужна аутентификация?

Проблема юридической силы электронных документов:

- Необходимо определить личность владельца электронной подписи (идентификация)
 - Проверка полномочий на подписание (реестр)
 - Подтверждение целостности (электронная подпись)
 - Обеспечить неотказуемость от подписи (аутентификация, электронная подпись, валидация сертификата ключа подписи, метка времени)
-

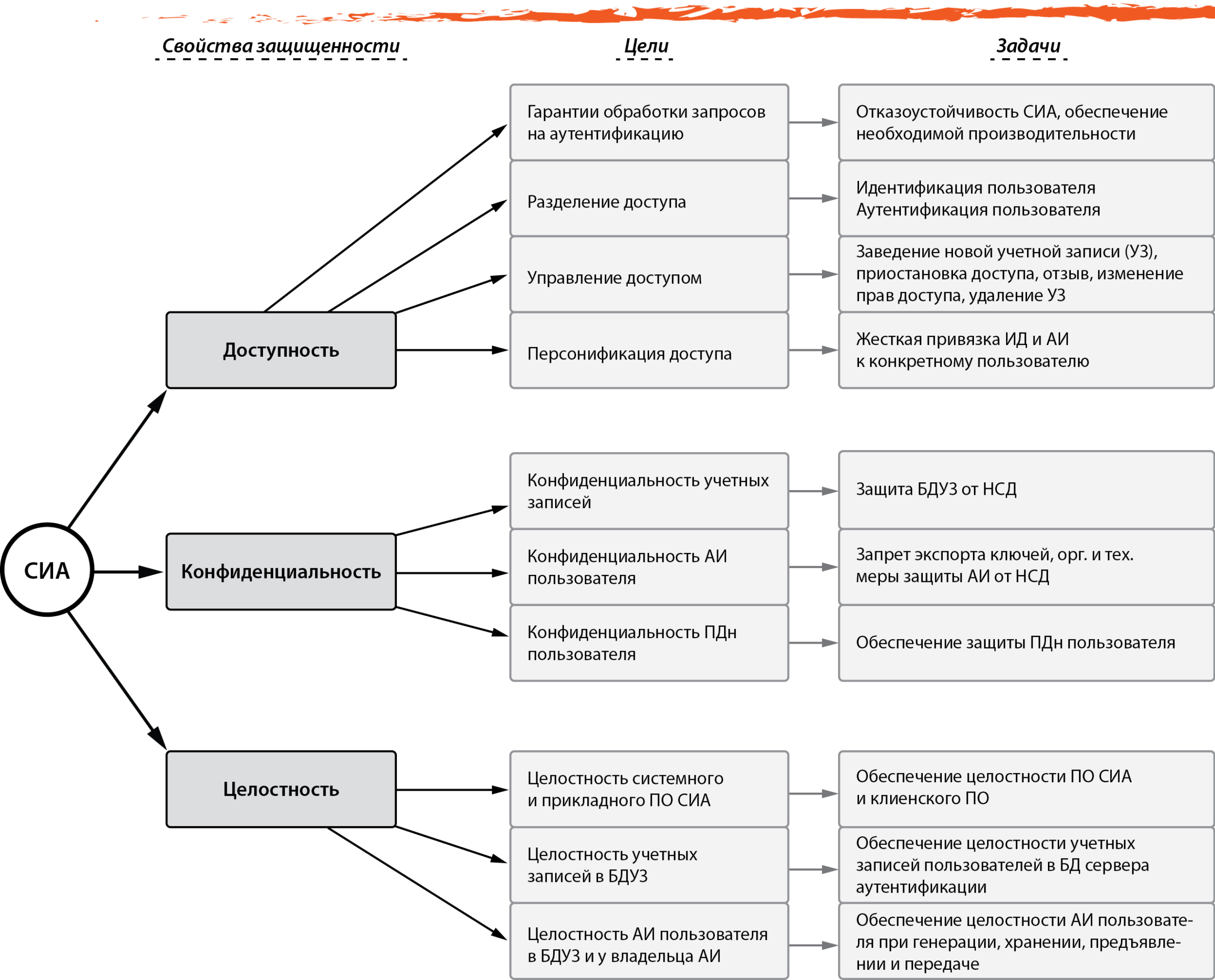
Уровни аутентификации и подписи

	виды ЭП		
Типы аутентификации	простая	усиленная	строгая
простая	+	-	-
усиленная	+	+	-
строгая	+	+	+

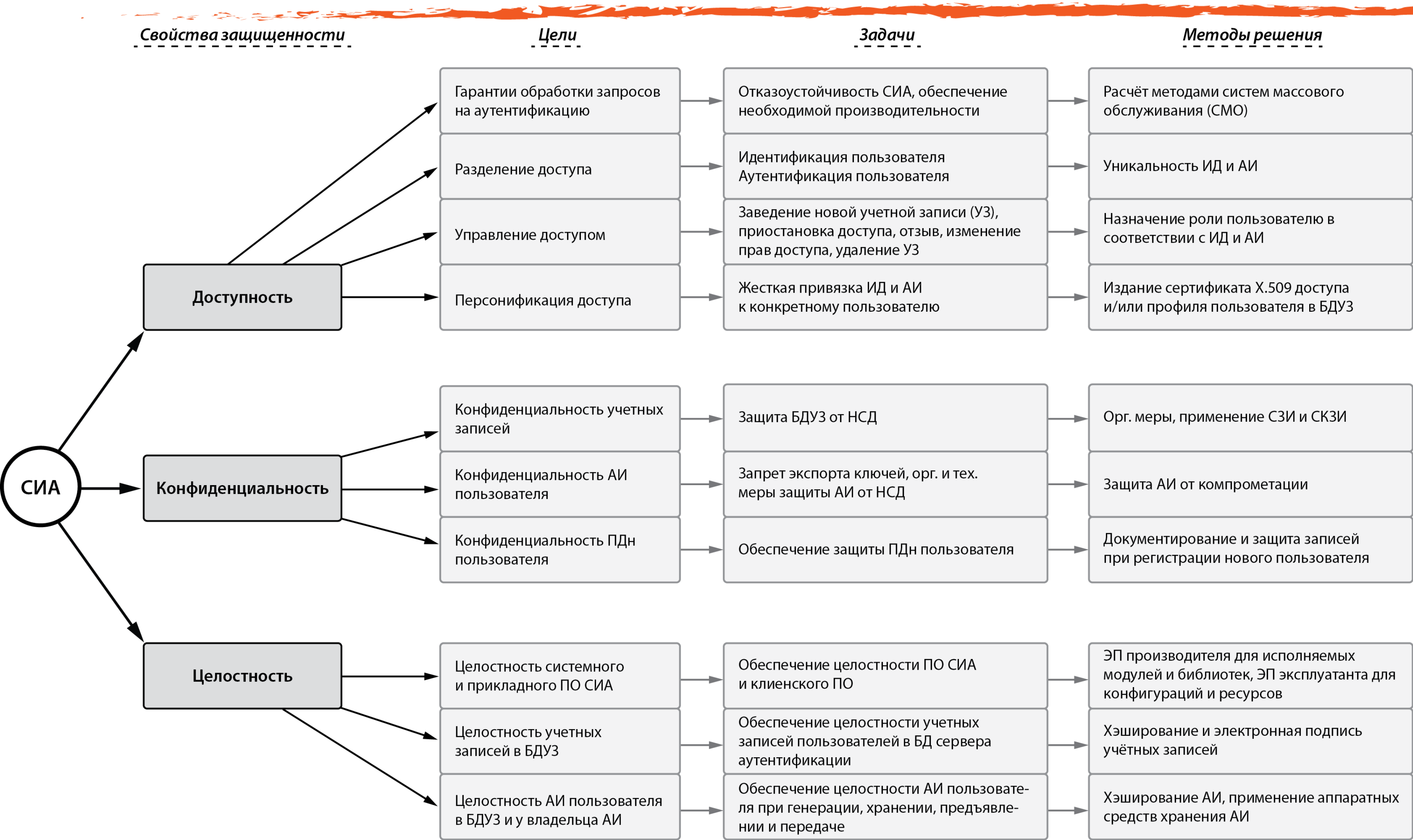
Триада информационной безопасности

Уровни достоверности (типы аутентификации)	Доступность	Целостность	Конфиденциальность
Простая (пароль)	+	-	-
Усиленная (ОТР)	+	-	-
Усиленная (сертификат доступа X.509)	+	+	+
Строгая (X.509 выдан доверенным УЦ)	+	+	+

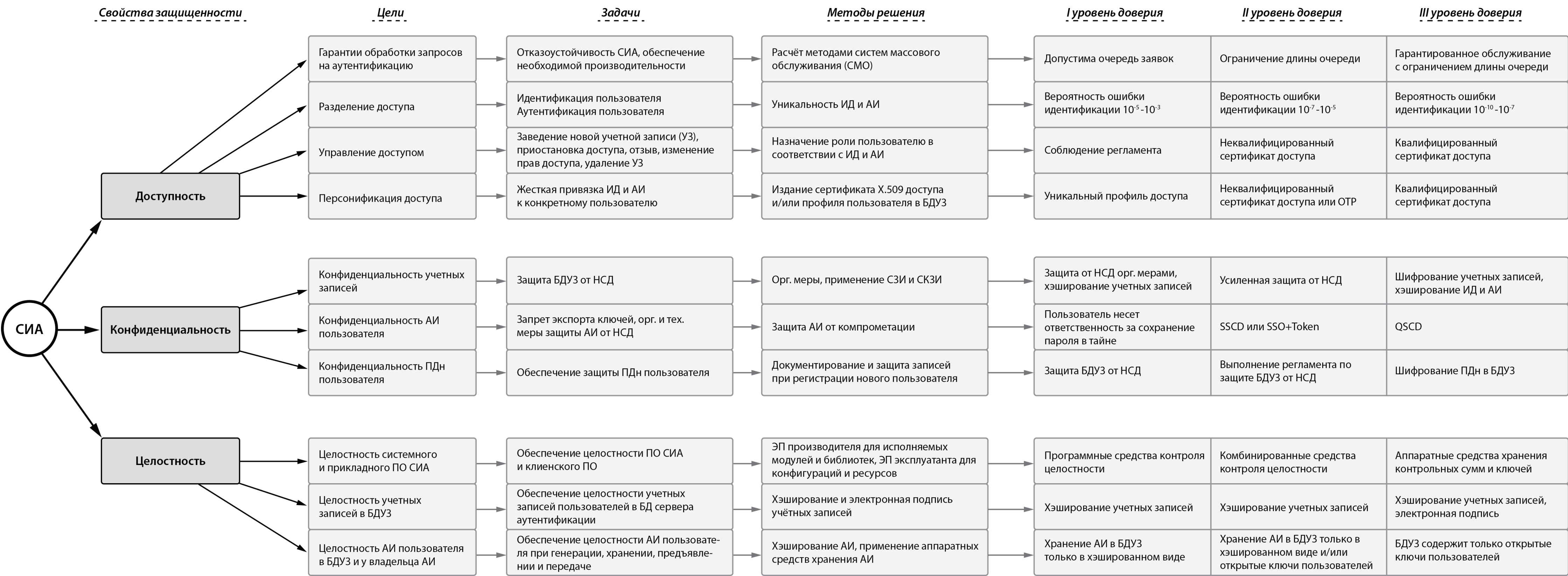
Классификация систем идентификации и аутентификации (СИА)



Классификация систем идентификации и аутентификации-2



Классификация систем идентификации и аутентификации-3





Связь уровней идентификации с банковскими рисками



Матрица рисков и уровни идентификации

СВР угроз ИБ	Уровни идентификации в зависимости от СТП нарушения ИБ			
	минимальная	средняя	высокая	критическая
нереализуемая	Низкий	Низкий	Средний	Высокий
минимальная	Низкий	Средний	Высокий	Запрещенная операция
средняя	Средний	Высокий	Запрещенная операция	Запрещенная операция
высокая	Средний	Запрещенная операция	Запрещенная операция	Запрещенная операция
критическая	Запрещенная операция	Запрещенная операция	Запрещенная операция	Запрещенная операция

Методика оценки рисков нарушения ИБ. Распоряжение Банка России от 11.11.2009 № Р-1190



Зарубежный опыт



Документы для первичной идентификации

List 1 Evidence of link between photo & signature	List 2 Evidence of operating in the community	List 3 Evidence of current residential address
•Australian driver's licence •Australian passport •Australian firearm's licence •Defence force/Police ID card •Department of Immigration and Citizenship (DIAC) certificate with of evidence of residence status •WA Photo Card, Over 18 or Proof of Age Card •Australian learner driver's permit card	•Debit or Credit card (one or the other, not both) issued by a financial institution •Document of Identity issued by the Passport Office •Entitlement card issued by the Commonwealth or State Government (Centrelink, Health Care card, Veterans Affairs card etc) •Full birth certificate issued in Australia (birth extracts not accepted) •Medicare card •Naturalisation, citizenship or immigration papers issued by Department of Immigration & Boarder Protection (DIBP) •Overseas passport with current Australian Entry Permit •Security guard or crowd control licence (Australian) •Student identity document or Statement of enrolment issued by an educational institution, including Tertiary (should include photo and/or signature) •Working with children card	•Driver's licence renewal notice •Financial institution statement less than six months old •Motor vehicle registration •Property lease or tenancy agreement •Shire/water rates notice •School or other educational report or certificate less than twelve months old •Utility account less than six months old (e.g. gas, electricity, home phone etc)

Пример Норвегии

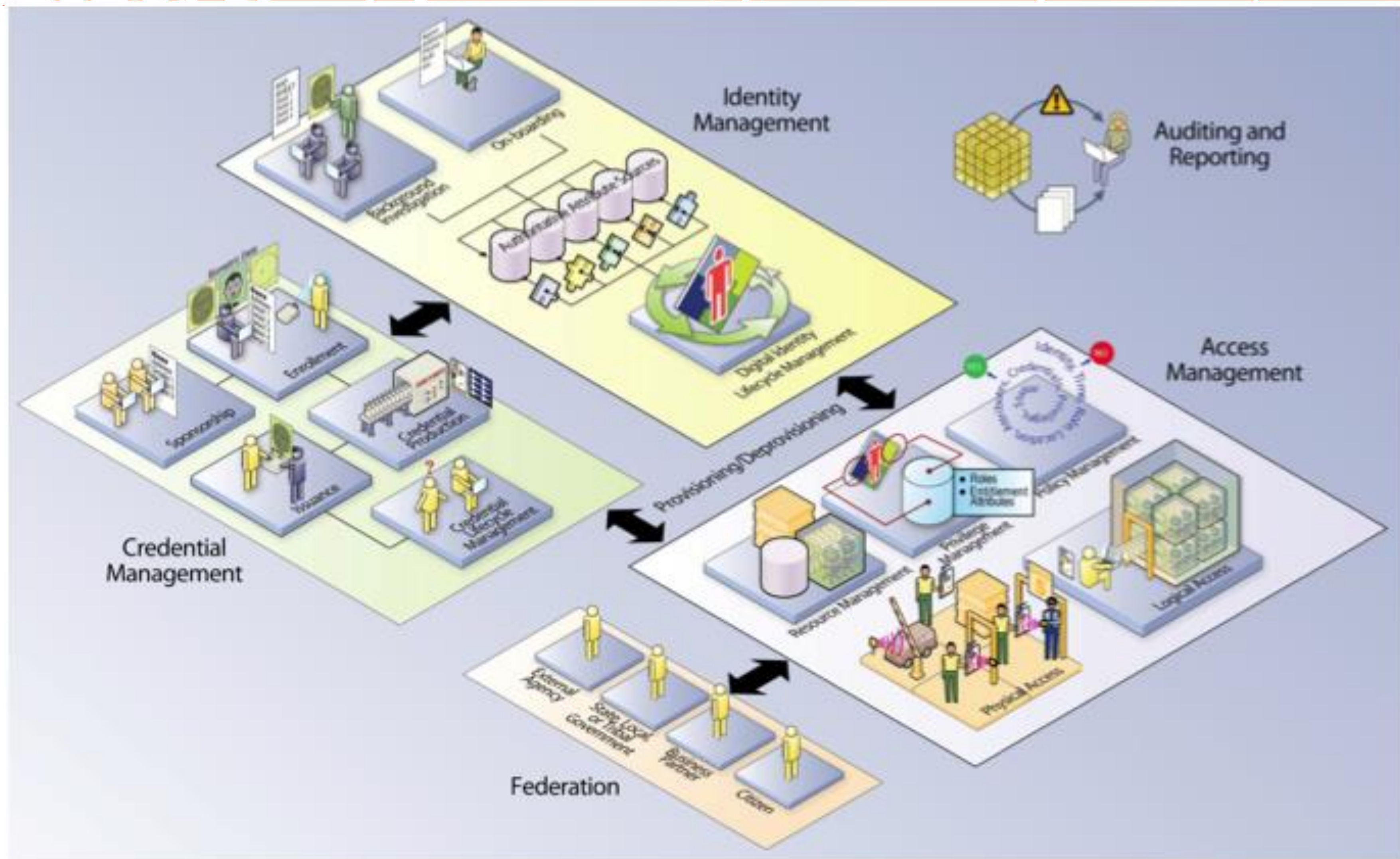
Имеется 3 системы идентификации граждан:

Государственная Min ID (MyID - для граждан с 13 лет), использует национальный Id, возможна первичная идентификация по номеру мобильного телефона с OTP, который приходит по SMS. Доступ к онлайн-сервисам более 50 госуслуг.

Банковская – более высокий уровень гарантий, чем Min ID. Использует набор механизмов безопасности, включая смарт-карты и ЭП на SIM. На июнь 2010г. охвачено более 2,5 млн. из 4.7 млн населения

BuyPass. Использует смарт-карты и мобильные телефоны

США: централизованная схема и федерация



Официальные документы США

- [04.2006 - NIST Special Publication 800-63 Version 1.0.2 Electronic Authentication Guideline](#) | [Download](#)
- [Backend Attribute Exchange \(BAE\) Governance](#) | [Download](#)
- [Backend Attribute Exchange \(BAE\) Overview](#) | [Download](#)
- [Federal ICAM Identity Scheme Adoption Process](#) | [Download](#)
- [Federal ICAM Privacy Guidance for Trust Framework Assessors and Auditors](#) | [Download](#)
- [Federal ICAM Trust Framework Provider Adoption Process for Levels of Assurance 1, 2, Non-PKI 3](#) | [Download](#)
- [Federated Physical Access Control System \(PACS\) Guidance](#) | [Download](#)
- [FICAM Roadmap and Implementation Guidance](#) | [Download](#)
- [Fingerprint Exception Handling Guidelines](#) | [Download](#)
- [GSA Memorandum Acquisitions of Products and Services for Implementation of HSPD-12](#) | [Download](#)
- [GSA Memorandum Federal Child Care Center Workers Facility Access Credentialing](#) | [Download](#)
- [GSA Technical Supplement in support of OMB issued memorandum M-05-05](#) | [Download](#)
- [Identity, Credential, and Access Management \(ICAM\) Roadmap Snapshot](#) | [Download](#)
- [Modernizing Federal Logical Access Control Systems \(LACS\) Brochure](#) | [Download](#)
- [Modernizing Federal Physical Access Control Systems \(PACS\) Brochure](#) | [Download](#)
- [NIST SP800-63 E-Authentication Guideline](#) | [Download](#)
- [OMB M-04-04 E-Authentication Guidance for Federal Agencies](#) | [Download](#)
- [OMB Memorandum dated October 6, 2011 Requirements for Accepting Externally-Issued Identity Credentials](#) | [Download](#)
- [OMB Memorandum M-05-05 Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services](#) | [Download](#)
- [Password/PIN Entropy Tool](#) | [Download](#)
- [SAML Identifier and Protocol Profiles for BAE](#) | [Download](#)
- [SAML Metadata Profile for BAE](#) | [Download](#)
- [Security Assertion Markup Language \(SAML\) Web Browser Single Sign-on \(SSO\) Profile](#) | [Download](#)
- [Trust Framework Provider Assessment Package Application](#) | [Download](#)



Как поднять качество идентификации в каждом финансовом учреждении

Способы идентификации

- Внедрение программно-аппаратных комплексов, позволяющих производить проверку защитных признаков идентификатора (проверка защитных признаков идентификатора, например, паспорта – проверка в различных спектрах излучения, фотографирование идентифицируемого лица, с последующей автоматизированной сверкой полученной фотографии фотографией в паспорте);
- Проверка биометрических данных заграничного паспорта;
- Проверка нескольких идентификаторов (основной идентификатор - паспорт, дополнительные - водительское удостоверение, военный билет, заграничный паспорт и т.д.);
- Проверка информации, указанной в предъявляемом идентификаторе посредством обращения к внешним источникам данных (реестры, регистры и т.д.);
- Видеофиксация процедуры идентификации;
- Проверка дееспособности идентифицируемого лица;
- Внедрение принципа солидарной ответственности за проведение процедуры идентификации;
- Выработка критериев качества идентификации (разработка процентной шкалы, позволяющей принимать решение о качестве идентификации).

Повышение ответственности

- Доведение под роспись статей уголовного и иных кодексов, предусматривающих ответственность за недобросовестное исполнение служебных обязанностей, мошенничество.
- Разъяснение последствий нарушения установленной процедуры идентификации (объявление взыскания, лишение премии и т.д.);
- Строгая регламентация действий, которые необходимо выполнить при проведении процедуры идентификации.
- В зависимости от предоставленных документов и результатов проверки установить уровень доверия (например, низкий, средний и высокий) по утвержденным в зависимости от уровня рисков финансовых операций.

Проект регламента

- Запросить документ, удостоверяющий личность.
 - Визуально проверить соответствие лица, изображенного на фотографии, с лицом обратившегося.
 - Проверить паспорт на сайте федеральной миграционной службы ([Проверка по списку недействительных российских паспортов](#)).
 - Проверить страницу с фотографией на предмет замены фотографии.
 - Попросить назвать данные, указанные в паспорте (например, адрес предыдущего места регистрации или уточнить дату и место рождения). В случае возникновения сомнений, запросить еще один документ, подтверждающий личность (водительское удостоверение, заграничный паспорт).
 - Зафиксировать в информационной системе паспортные данные и результат проверки паспорта.
 - Запросить иные документы при необходимости фиксации дополнительной информации об обратившемся.
 - Внести в информационную систему дополнительные сведения об обратившемся.
 - Сфотографировать обратившегося на веб-камеру.
 - Вывести на печать заявление, необходимое для получения соответствующей услуги.
 - Попросить обратившегося подписать заявление (ФИО полностью собственноручно, подпись). Сравнить подпись на заявлении с подписью в паспорте, результат сравнения зафиксировать в информационной системе.
 - Поставить на заявлении отметку о принятии, подпись.
 - Подписать сведения в информационной системе электронной подписью (электронная подпись должна находиться на носителе с неизвлекаемыми ключами, для подписания необходимо два фактора, пин-код и скан отпечатка пальца).
 - Информирование руководителя подразделения о готовности к оказанию услуги, передача паспорта обратившегося руководителю подразделения.
-

Концепция трансляции доверия

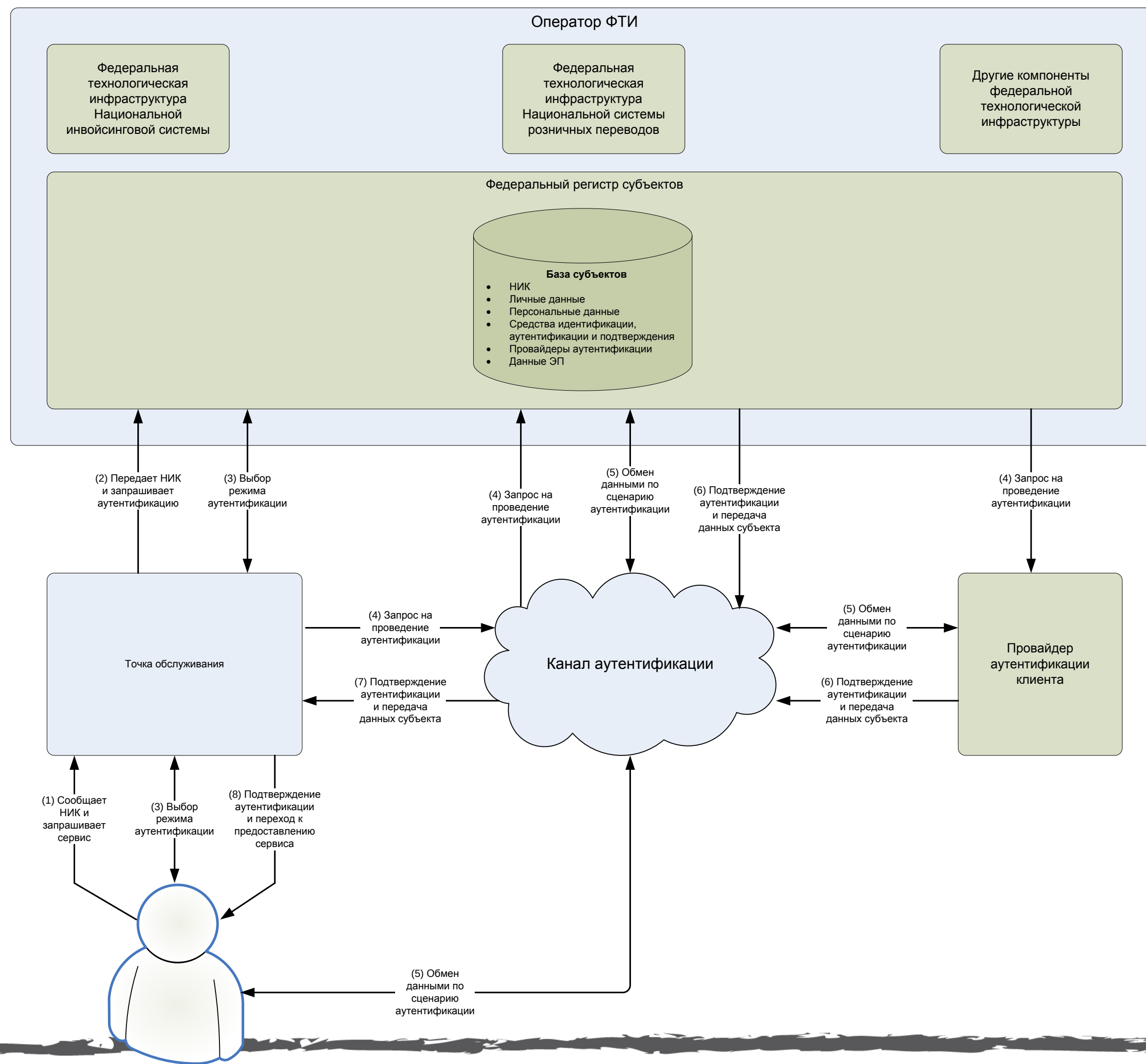
Изложенное выше касается общетеоретических проблем идентификации

Безусловно применимо к одному домену доверия

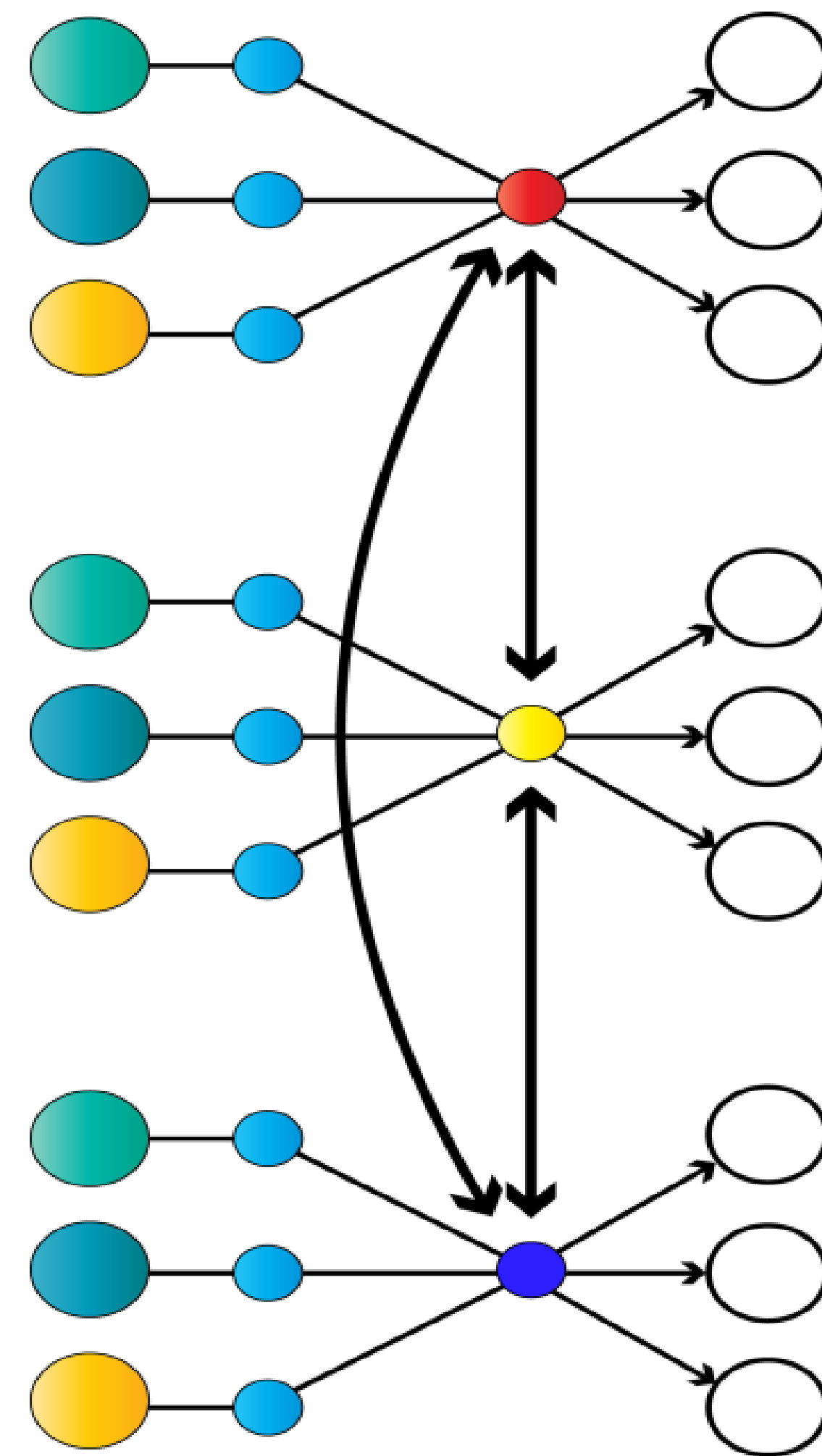
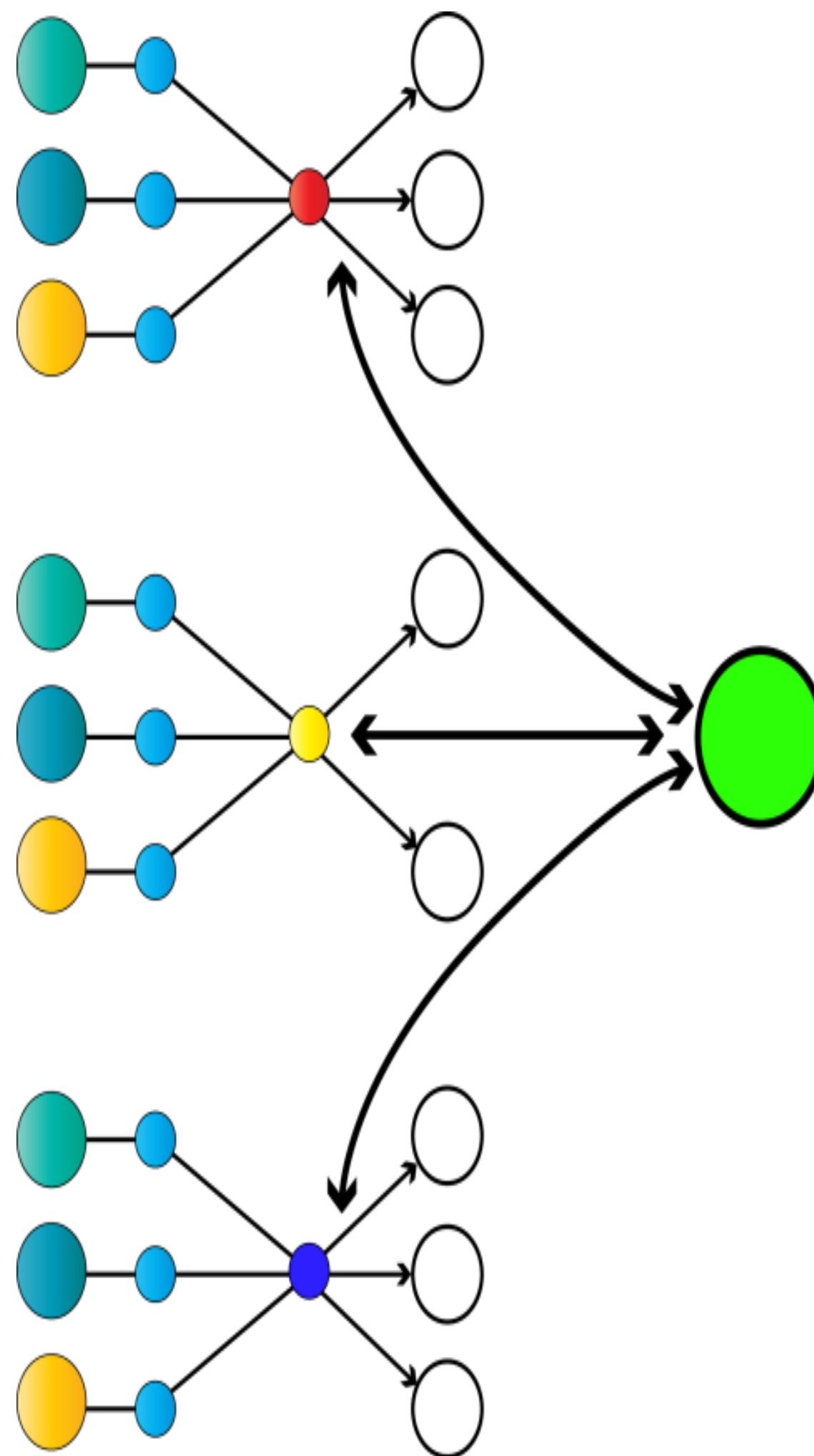
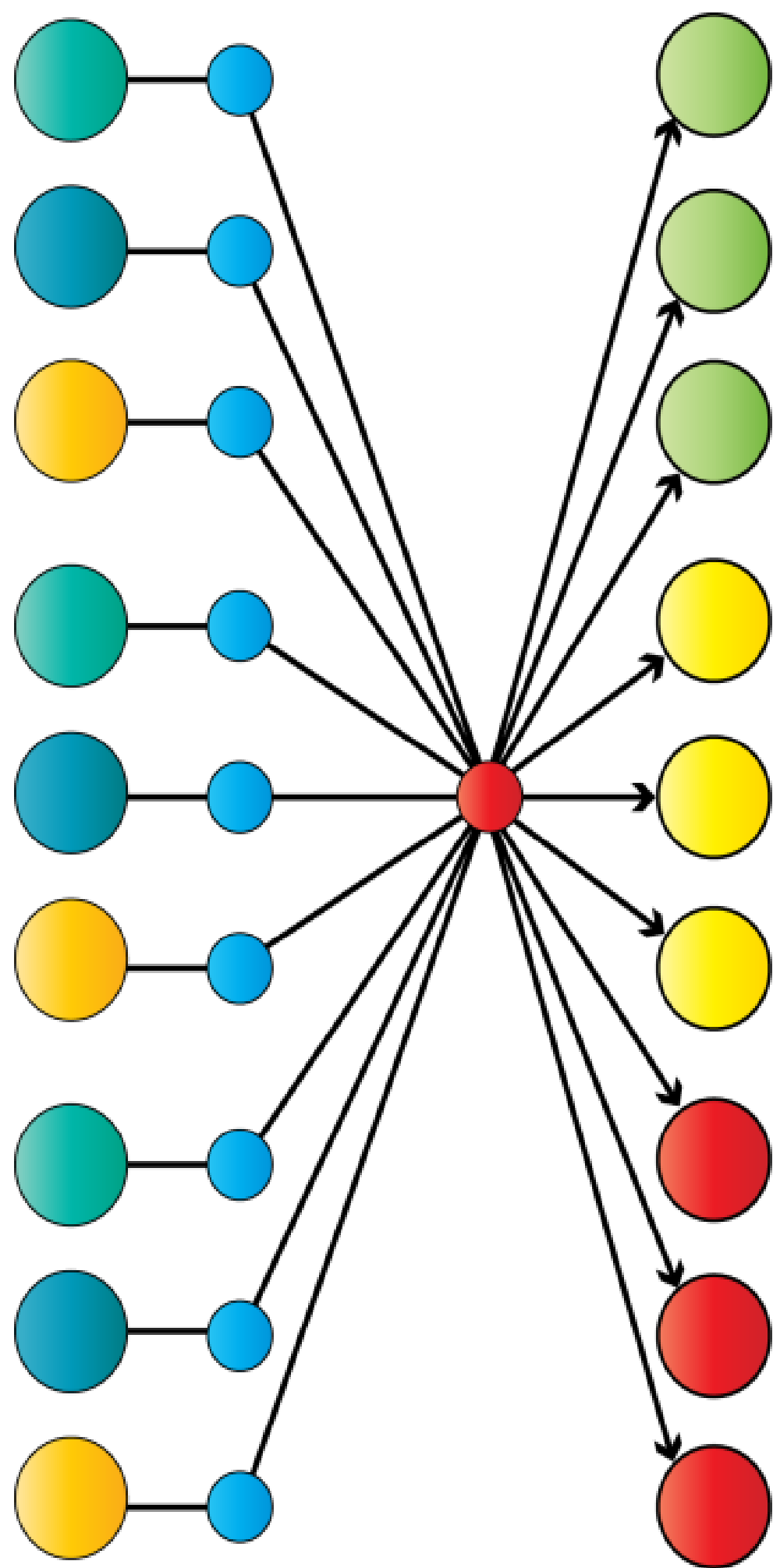
Для решения задачи в масштабах межбанковского взаимодействия необходимы принятые банковским сообществом как надежные процедуры трансляции доверия к первичной идентификации личности

Рассмотрим варианты решения задачи трансляции доверия в разных плоскостях, обобщая различные предложения

Одно из предложений



Варианты архитектуры



Сценарии организационной модели

- Несколько ведущих банков учреждают сервис идентификации
 - Банк России поддерживает и управляет этим процессом или самоустраняется
 - Росфинмониторинг возглавляет этот процесс или самоустраняется
 - Участники финансово-кредитной сферы присоединяются по мере необходимости
-

Сценарии разделения по рискам

Для малорисковых операций можно использовать облегченные модели и технологии идентификации

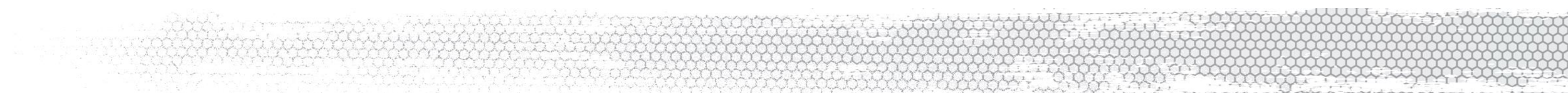
Для среднерисковых операций требуется создание и использование федеративной модели трансляции доверия

Высокий уровень СВР угроз и СТП последствий требует создания высоконадежных схем и технологий трансляции доверия

Спасибо за внимание!



a.sabanov@aladdin-rd.ru

A decorative footer pattern at the bottom of the slide, featuring a light gray background with a subtle, repeating hexagonal or honeycomb texture.