ИКС-протокол и суверенная модель управления учетными записями

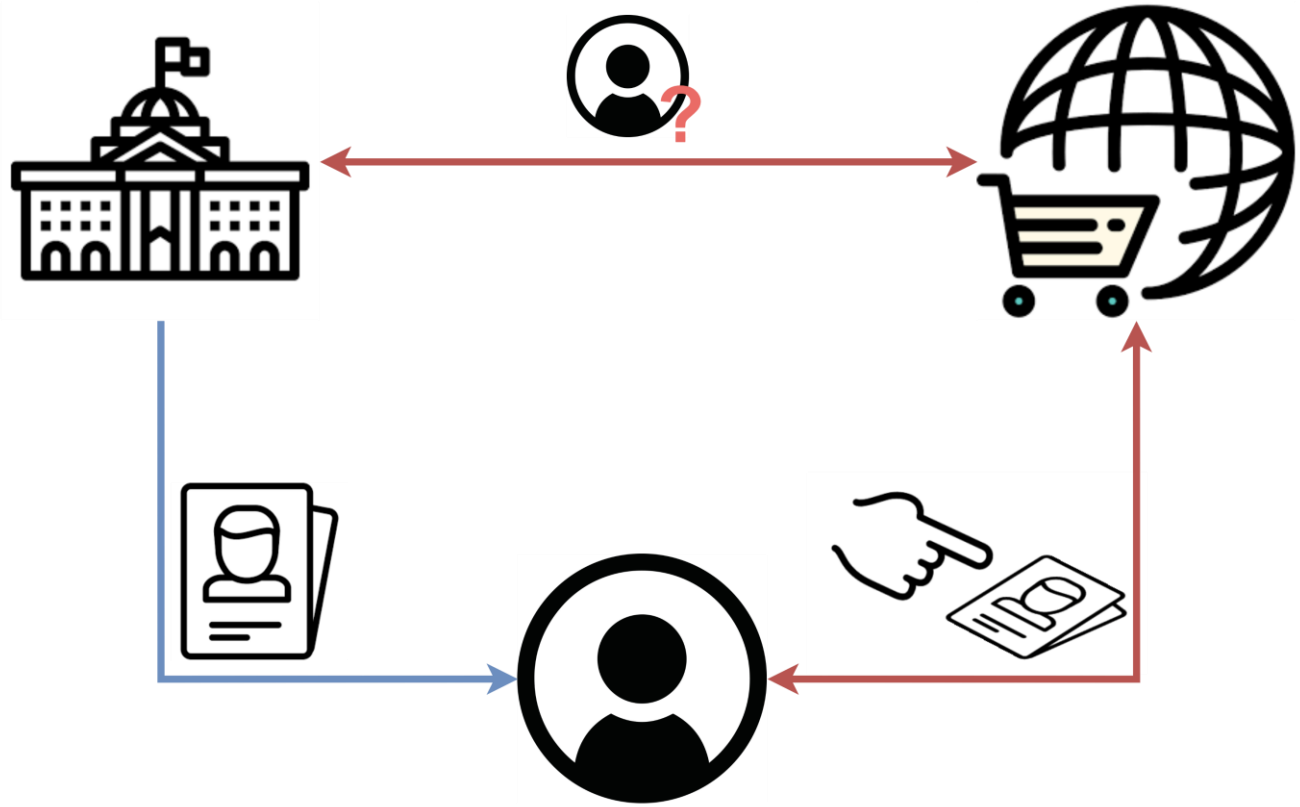
Владимир Бельский
Илья Герасимов
Василий Шишкин

КРИПТОНИТ

Управление учетными данными

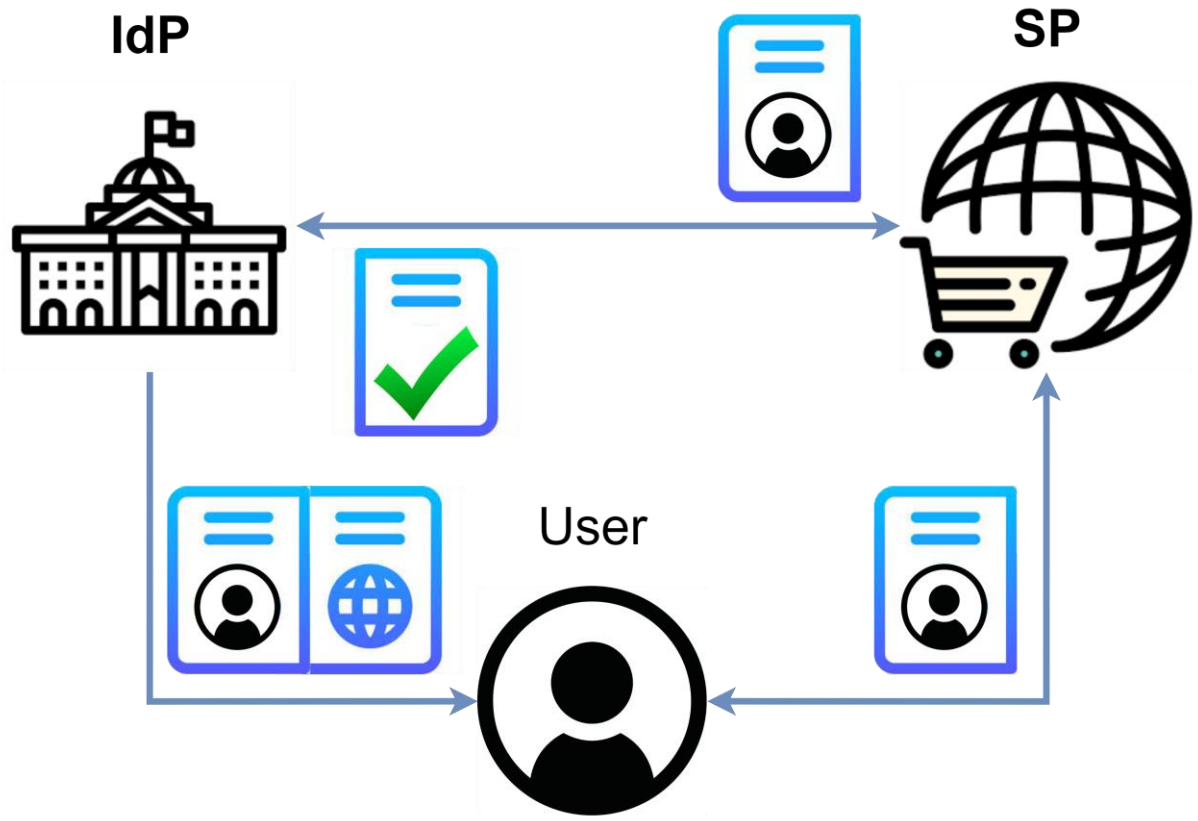
КРИПТОНИТ

Цифровизация существующих процессов требует внедрения и стандартизации систем управления учетными данными.



Управление учетными данными

ISO/IEC 24760, ГОСТ Р 58833-2020, ГОСТ Р 59381— 2021 вносят определения процессов идентификации и аутентификации, а также требования к архитектуре и участникам.



Провайдер учетных данных

(Identity Provider, IdP)

Сервис, запрашивающий аутентификацию пользователя (Service Provider, SP)

Данные о пользователе в системе IdP

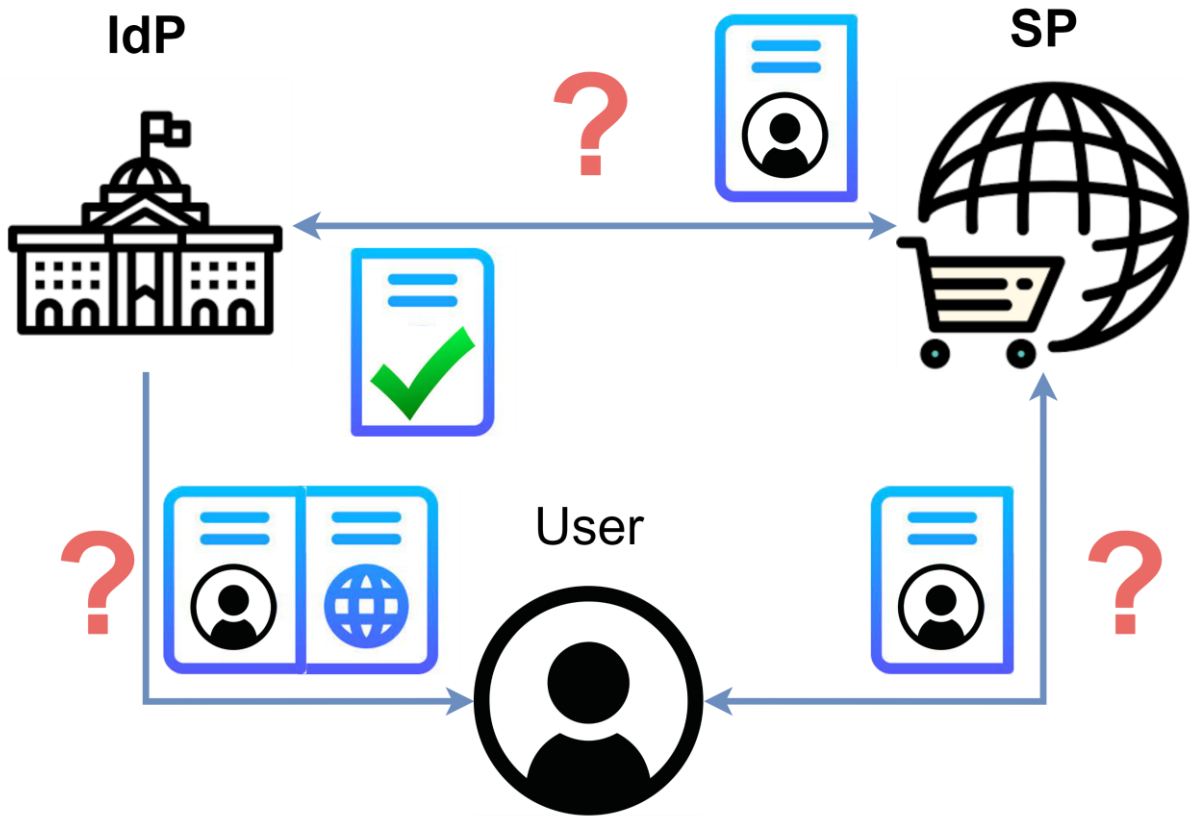
Данные аутентификации

Подтверждение аутентификации

Управление учетными данными

КРИПТОНИТ

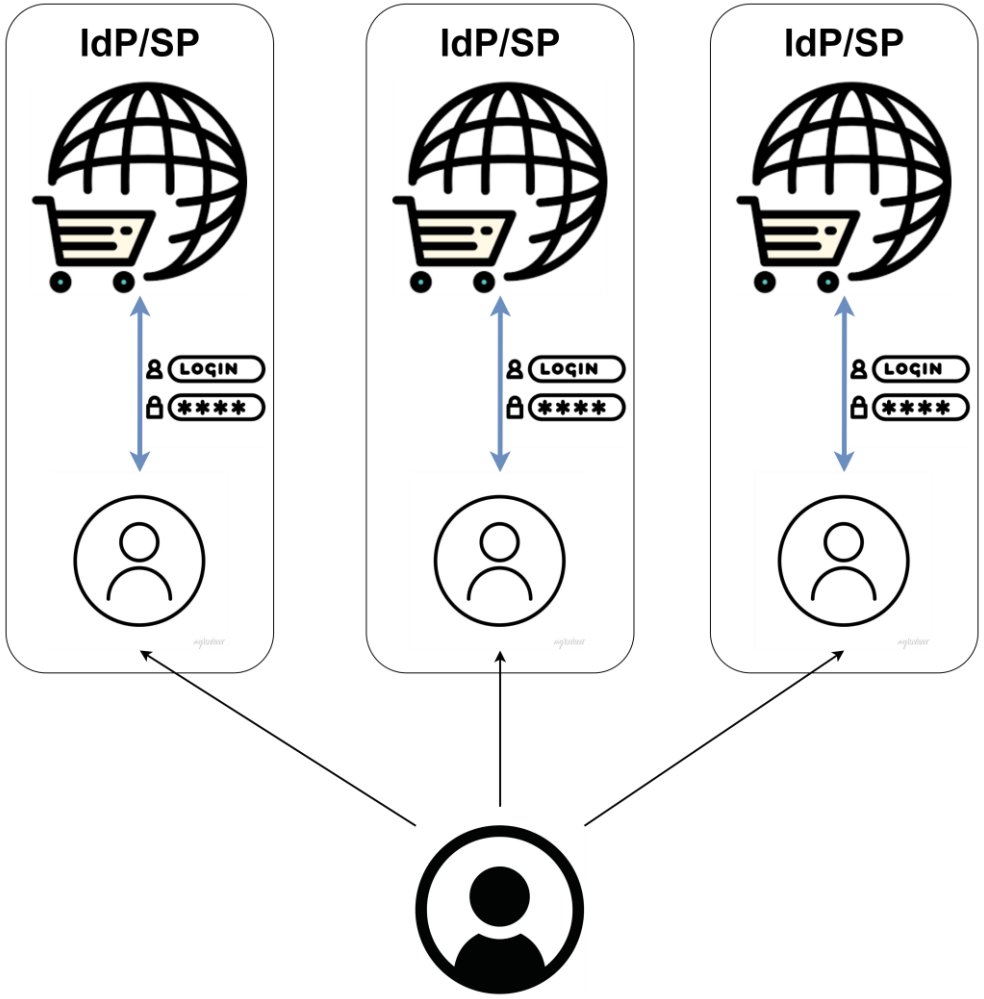
Таким образом, на разработчика накладывается ответственность реализовать систему управления учетными данными, которая соответствует всем требованиям.



Модели управления учетными данными

КРИПТОНИТ

Изолированная модель

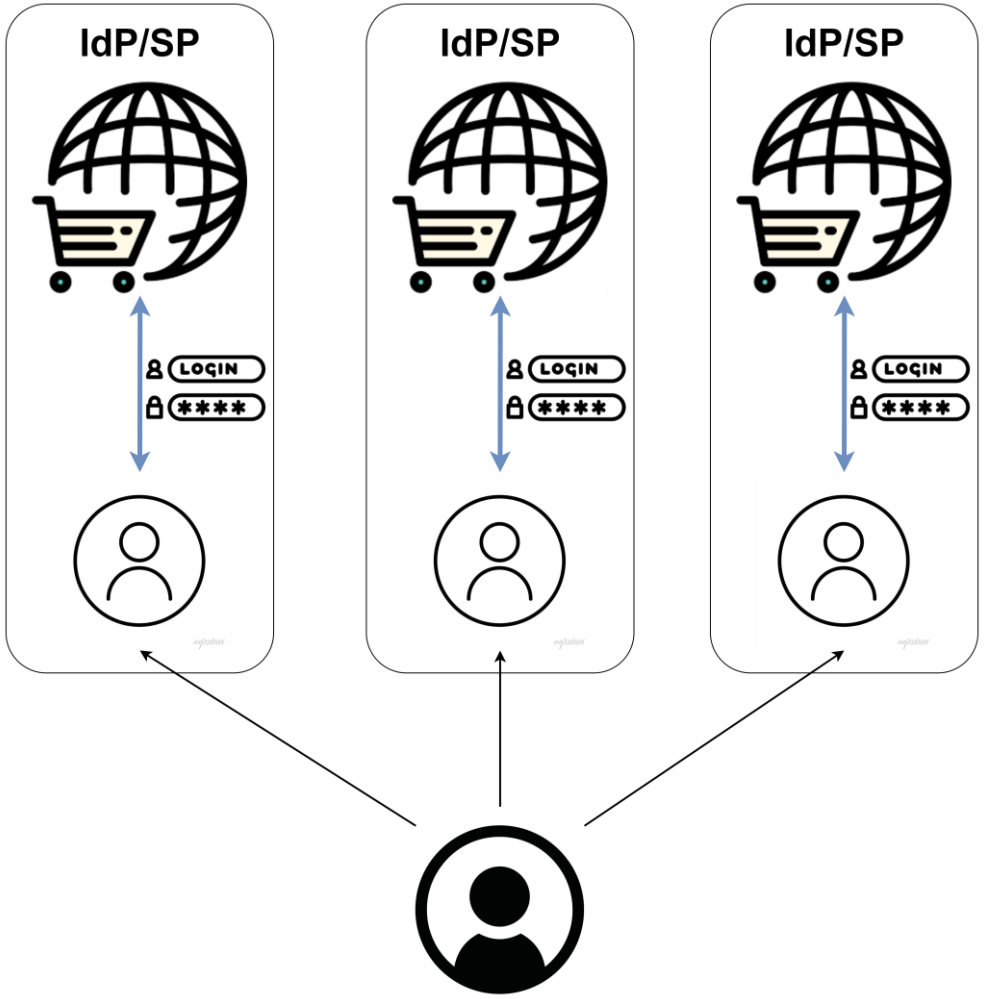


Модели управления учетными данными

КРИПТОНИТ

Изолированная модель

Проблема: один идентификатор пользователя не может быть использован для аутентификации у другого сервиса



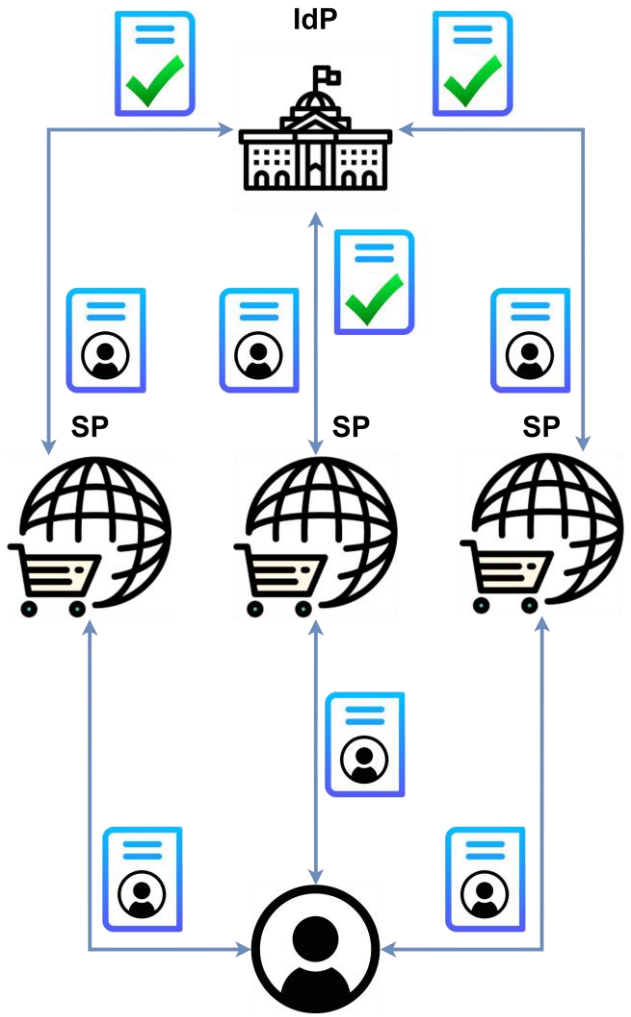
Модели управления учетными данными

КРИПТОНИТ

Изолированная модель

⇩

Центральная модель



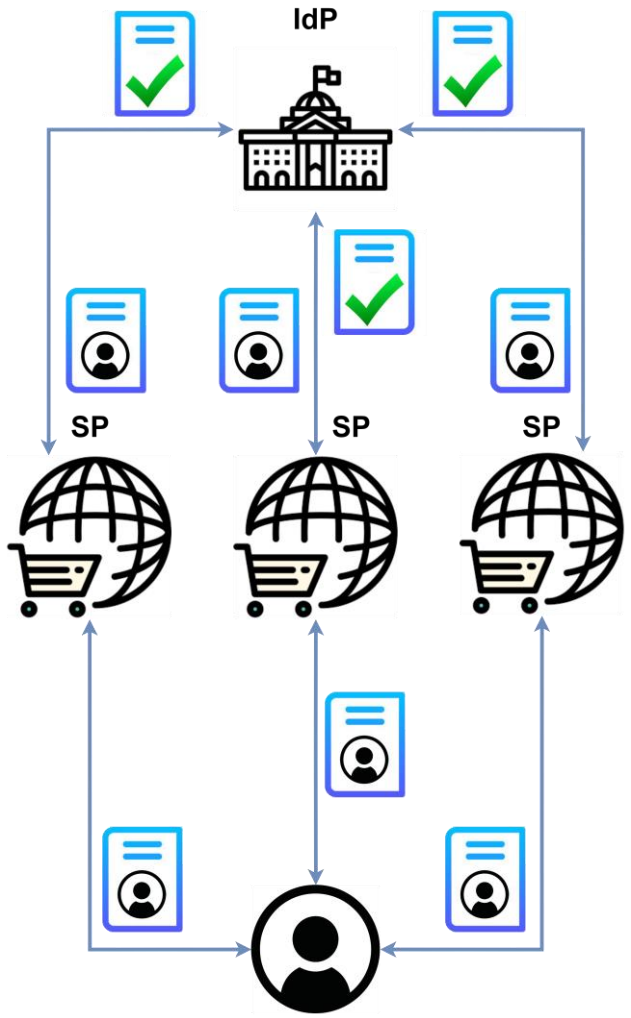
Модели управления учетными данными

КРИПТОНИТ

Изолированная модель

Центральная модель

Проблема: одна точка доступа к данным и функциям аутентификации. Не решает проблему изолированной модели в случае, когда используются несколько типов аутентификации.



Модели управления учетными данными

КРИПТОНИТ

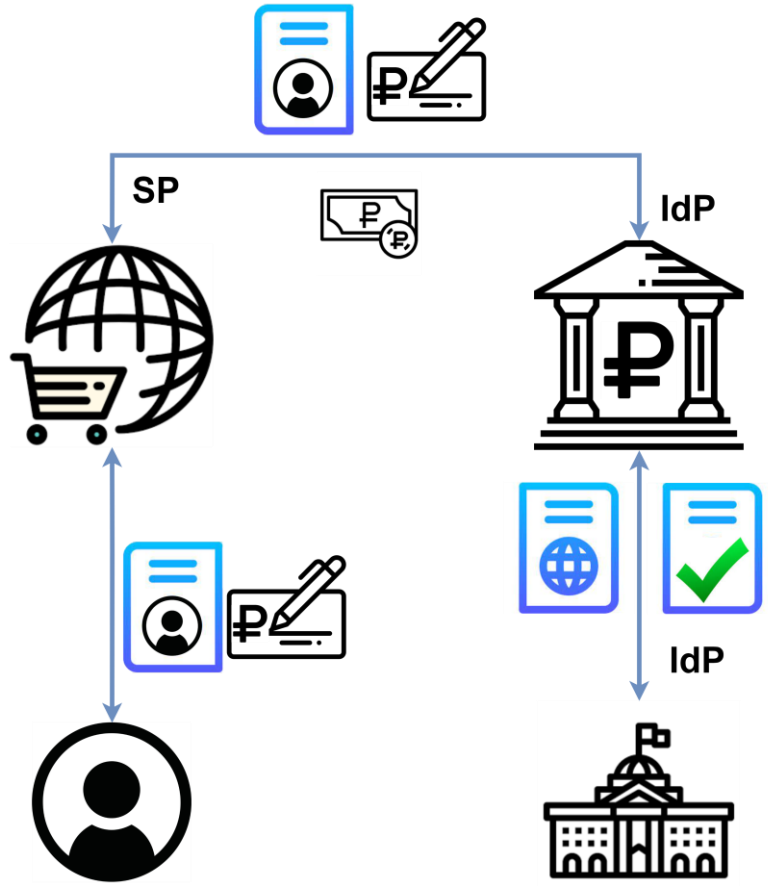
Изолированная модель

⇩

Центральная модель

⇩

Федеративная модель



Модели управления учетными данными

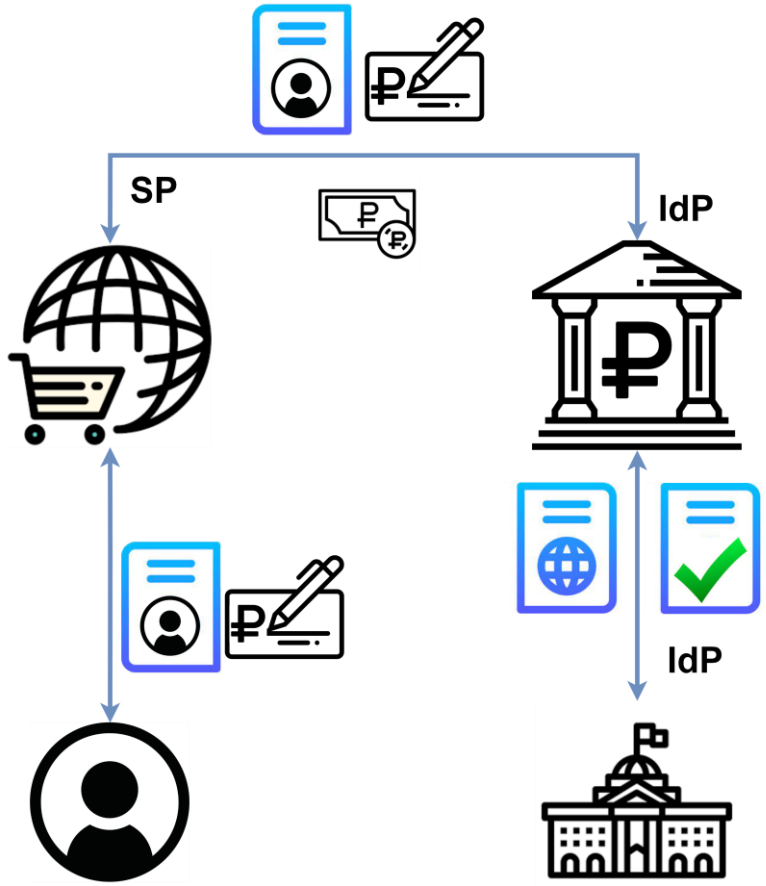
КРИПТОНИТ

Изолированная модель

Центральная модель

Федеративная модель

Проблема: после согласия на передачу данных для аутентификации, пользователь теряет контроль за распространением данных, не имея возможности предотвращать утечки на стороне сервиса.



Пример: Единая система идентификации и аутентификации

КРИПТОНИТ

Изолированная модель

⇩

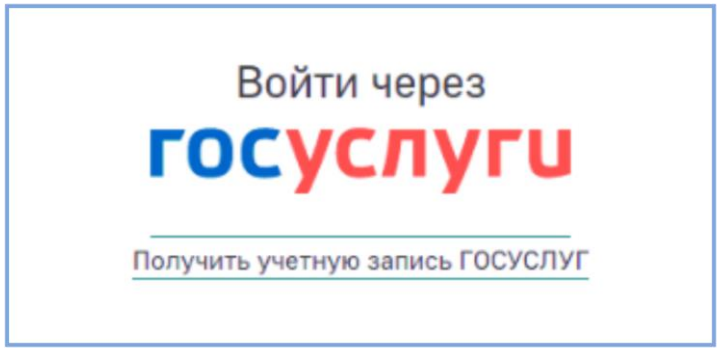
Центральная модель

⇩

Федеративная модель

Проблема: после согласия на передачу данных для аутентификации, пользователь теряет контроль за распространением данных, не имея возможности предотвращать утечки на стороне сервиса.

Единая система идентификации и аутентификации (ЕСИА) - ИС, представляющая единое «окно» доступа граждан, бизнеса и представителей исполнительной власти в инфраструктуру электронного правительства, а также другие ИС, подключенные к Системе межведомственного электронного взаимодействия (СМЭВ).



Модели управления учетными данными

КРИПТОНИТ

Изолированная модель

⇩

Централизованная модель

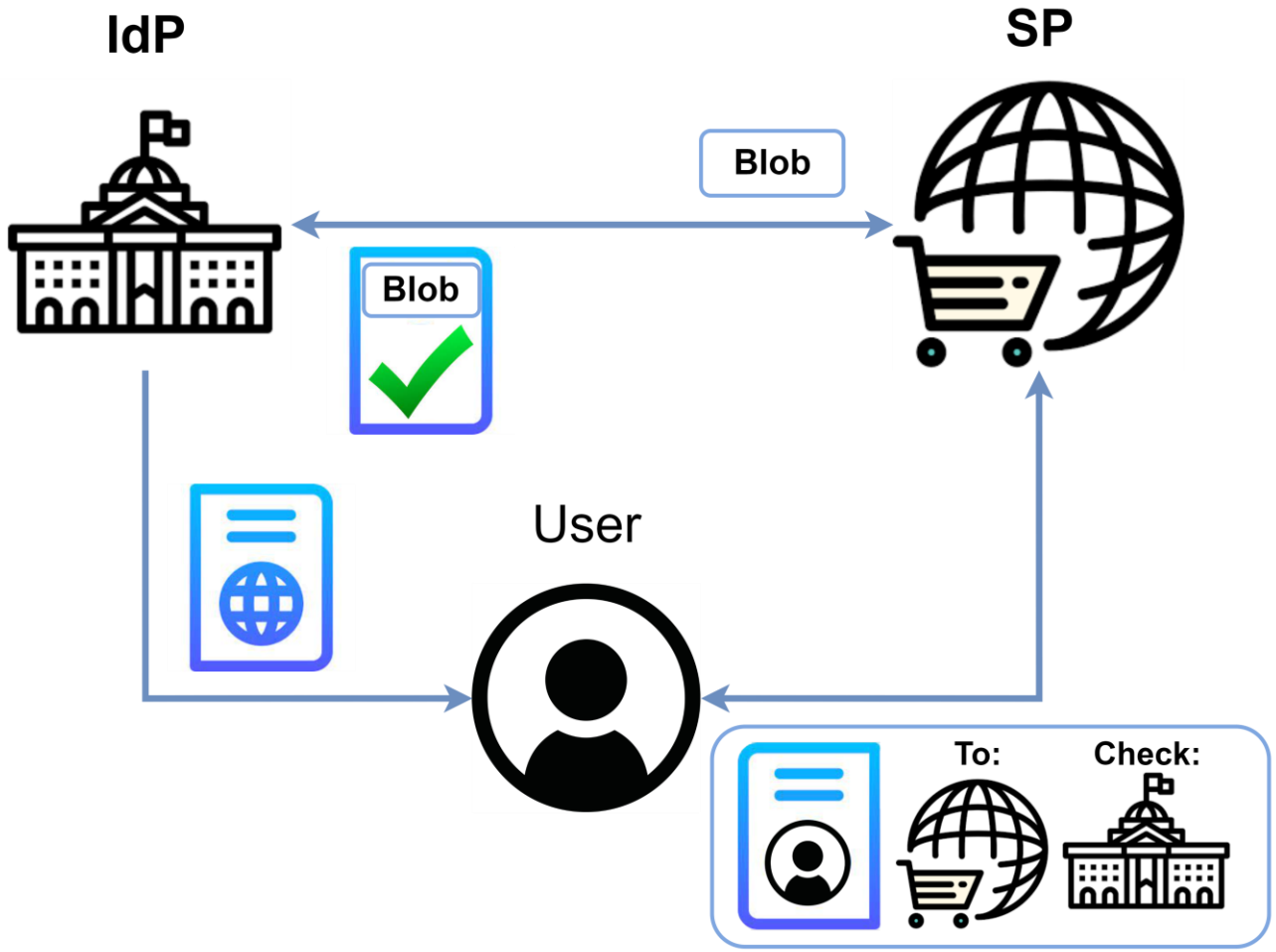
⇩

Федеративная модель

⇩

Модель,

ориентированная на пользователя



ИКС-протокол

International Journal of Open Information Technologies ISSN: 2307-8162 vol. 8, no. 6, 2020

Протокол обмена персональными данными: ИКС

В. С. Бельский, И. Ю. Герасимов, К. Д. Царегородцев, И. В. Чижов

Personal data exchange protocol: X

V. Belsky[1][0000−0002−4546−5464], I. Gerasimov[1][0000−0003−1921−823X], K. Tsaregorodtsev[1][0000−0002−9281−417X] and I. Chizhov[1][0000−0001−9126−6442]

[1]Cryptography Laboratory, SPC «Kryptonite», Moscow, Russia cryptolab@kryptonite.ru

Abstract. Personal data exchange and disclosure prevention are widespread problems in our digital world. There are a couple of information technologies embedded in the commercial and government processes. People need to exchange their personal information while using these technologies. And therefore, It is essential to make this exchange is secure. Despite many legal regulations, there are many cases of personal data breaches that lead to undesirable consequences. Reasons for personal data leakage may be adversary attack or data administration error. At the same time, creating complex service interaction and multilayer information security may lead to many inconveniences for the user. Personal data exchange protocol has the following tasks: participant's data transfer, ensuring information security, providing participants with trust in each other and ensuring service availability. In this paper, we represent a personal data exchange protocol called X[1]. The main idea is to provide personal data encryption on the user side and thus to prevent personal data disclosure and publication. This approach allows us to transfer personal data from user to service only in the form of an encrypted data packet — blob. Each blob can be validated and certified by a personal data inspector who had approved user's information. It can be any government department or a commercial organization, for example, passport issuing authority, banks, etc. It implies that we can provide several key features for personal data exchange. A requesting service cannot publish the user personal data. It still can perform a validation protocol with an inspector to validate user data. We do not depend on service data administration infrastructure and do not complicate the inspector's processes by adding additional information about the personal data request. The personal data package has a link between the personal data owner and a service request. Each blob is generated for a single request and has a time limit for a provided encrypted personal data. After this limit, the service can not use a received package. The user cannot provide invalid personal data or use the personal data of another person. We don't restrict specified cryptographic algorithms usage The X protocol can be implemented with any encryption, digital signature, key generation algorithms which are secure in our adversary model. For protocol description, Russian standardized cryptographic protocols are used. The paper also contains several useful examples of how the X protocol can be implemented in real information systems.

Keywords: X· personal data · VKO GOST · symmetric cryptography.

1 Introduction

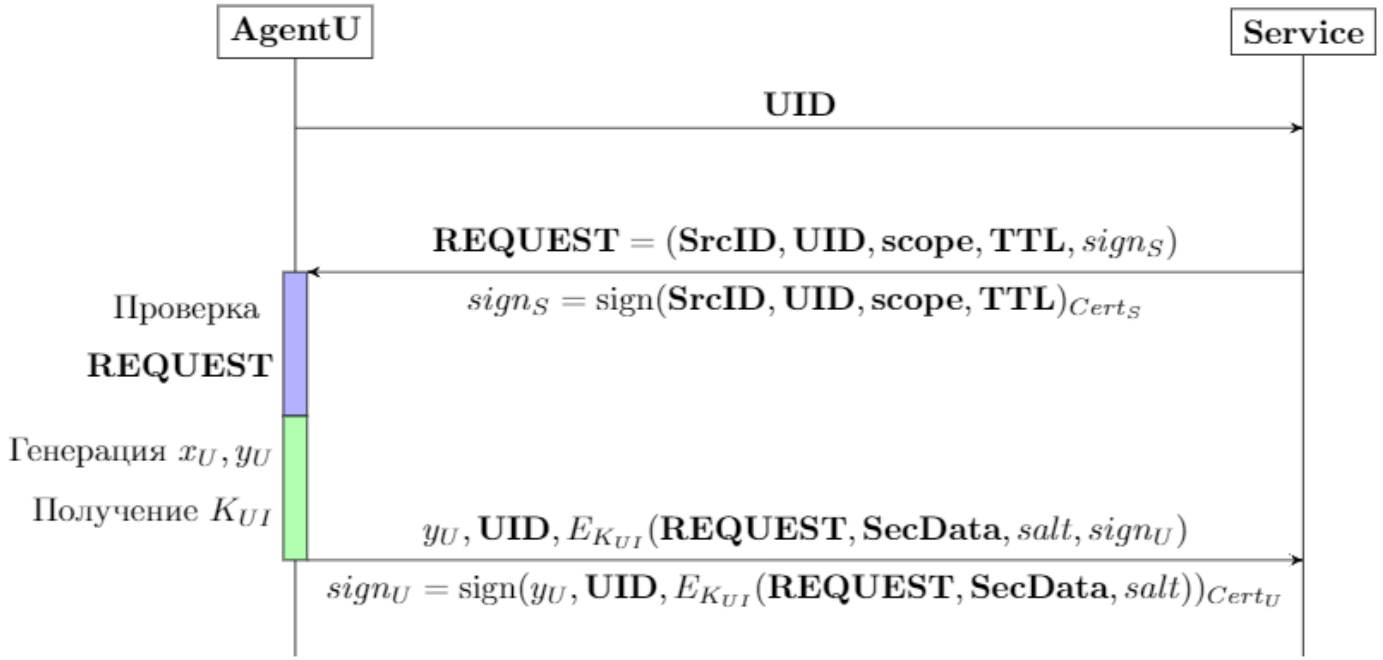
Recently information technology is being actively implemented in public service delivery processes. Digital government, public service portals and similar information systems are becoming more and more familiar in modern society. A lot of useful tasks such as taking a loan, applying for a passport, sign a contract can be done without leaving home using a computer or a mobile phone. Generally, it is necessary to provide personal data for performing these operations. Despite the rather strict regulation of personal data processing in many countries, there always occur data leakage cases as the result of administration errors or hacker attacks. It leads to undesirable consequences for people, for example, money, property and reputation loss.

Some countries increase the restriction of information security policies, but it leads to the creation of significant inconveniences for such users as services, which in turn lowers their attractiveness to citizens. Thus the creation of useful and secure personal data processing system — one of the main problems for public information services developers.

In the most general case, the following tasks are set for personal data processing systems:

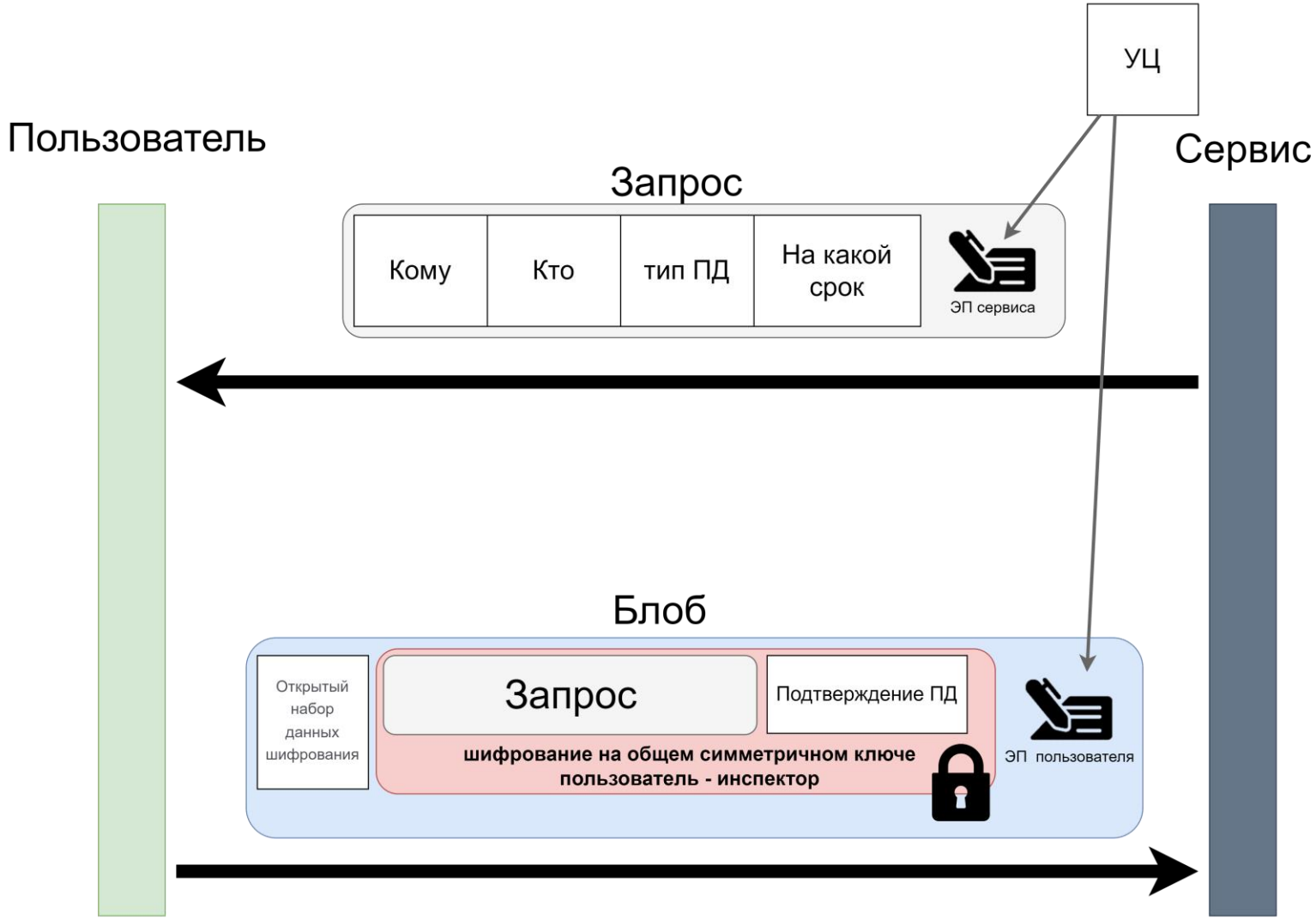
[1] The paper was published in Russian in International Journal of Open Information Technologies ISSN: 2307-8162 vol. 8, no. 6, 2020

ИКС-протокол позволяет с помощью криптографических методов обеспечить передачу персональных данных от пользователя к сервису в виде зашифрованного блока. Сервис может проверить валидность переданных данных с помощью инспектора персональных данных, который эти данные для пользователя создал (зарегистрировал).



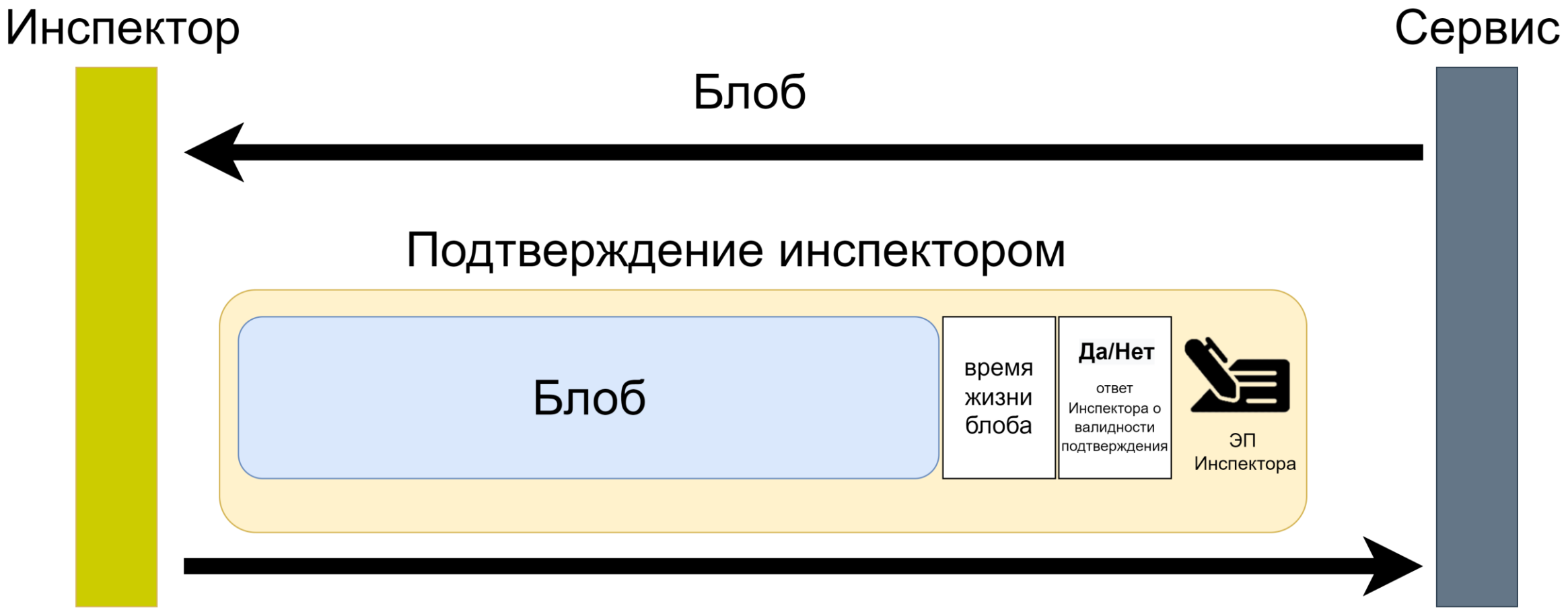
ИКС-протокол: подтверждение ПД

КРИПТОНИТ



ИКС-протокол: проверка блоба

КРИПТОНИТ



Свойства протокола

КРИПТОНИТ

- Решается проблема федеративной модели. Пользователь самостоятельно осуществляет контроль за подтверждением данных, и только он отвечает за шифрование данных, не давая сервису возможности раскрыть данные;

Свойства протокола

КРИПТОНИТ

- Решается проблема федеративной модели. Пользователь самостоятельно осуществляет контроль за подтверждением данных, и только он отвечает за шифрование данных, не давая сервису возможности раскрыть данные;
- Компрометация идентификатора пользователя не ведет к раскрытию всех данных пользователя. Более того, не существует единого места, где хранятся все персональные данные пользователя в связке с этим идентификатором;

Свойства протокола

КРИПТОНИТ

- Решается проблема федеративной модели. Пользователь самостоятельно осуществляет контроль за подтверждением данных, и только он отвечает за шифрование данных, не давая сервису возможности раскрыть данные;
- Компрометация идентификатора пользователя не ведет к раскрытию всех данных пользователя. Более того, не существует единого места, где хранятся все персональные данные пользователя в связке с этим идентификатором;
- Обеспечение приватности и целостности данных осуществляется классическими криптографическими механизмами цифровой подписи, согласования ключей и шифрования, прошедшими процесс стандартизации.

Проблемы модели, ориентированной на пользователя

КРИПТОНИТ

- Не обеспечивается анонимность пользователя и сервиса. С одной стороны, пользователь не хочет, чтобы сервис знал идентификатор пользователя в системе. С другой стороны, сервис не хочет, чтобы оператор учетных данных знал о том, кто запрашивает проверку данных;

Проблемы модели, ориентированной на пользователя

КРИПТОНИТ

- Не обеспечивается анонимность пользователя и сервиса. С одной стороны, пользователь не хочет, чтобы сервис знал идентификатор пользователя в системе. С другой стороны, сервис не хочет, чтобы оператор учетных данных знал о том, кто запрашивает проверку данных;
- Аутентификация является выполненной только после получения положительного результата проверки от инспектора, что требует постоянного активного соединения с инспектором (нет offline аутентификации).

Проблемы модели, ориентированной на пользователя

КРИПТОНИТ

- Не обеспечивается анонимность пользователя и сервиса. С одной стороны, пользователь не хочет, чтобы сервис знал идентификатор пользователя в системе. С другой стороны, сервис не хочет, чтобы оператор учетных данных знал о том, кто запрашивает проверку данных;
- Аутентификация является выполненной только после получения положительного результата проверки от инспектора, что требует постоянного активного соединения с инспектором (нет offline аутентификации).
- Существует единая точка доступа к системе аутентификации в виде удостоверяющего центра. Удостоверяющий центр является единым местом хранения информации обо открытых ключах пользователей и требует доверия по выполнению соответствующих требований;

Модели управления учетными данными

КРИПТОНИТ

Изолированная модель

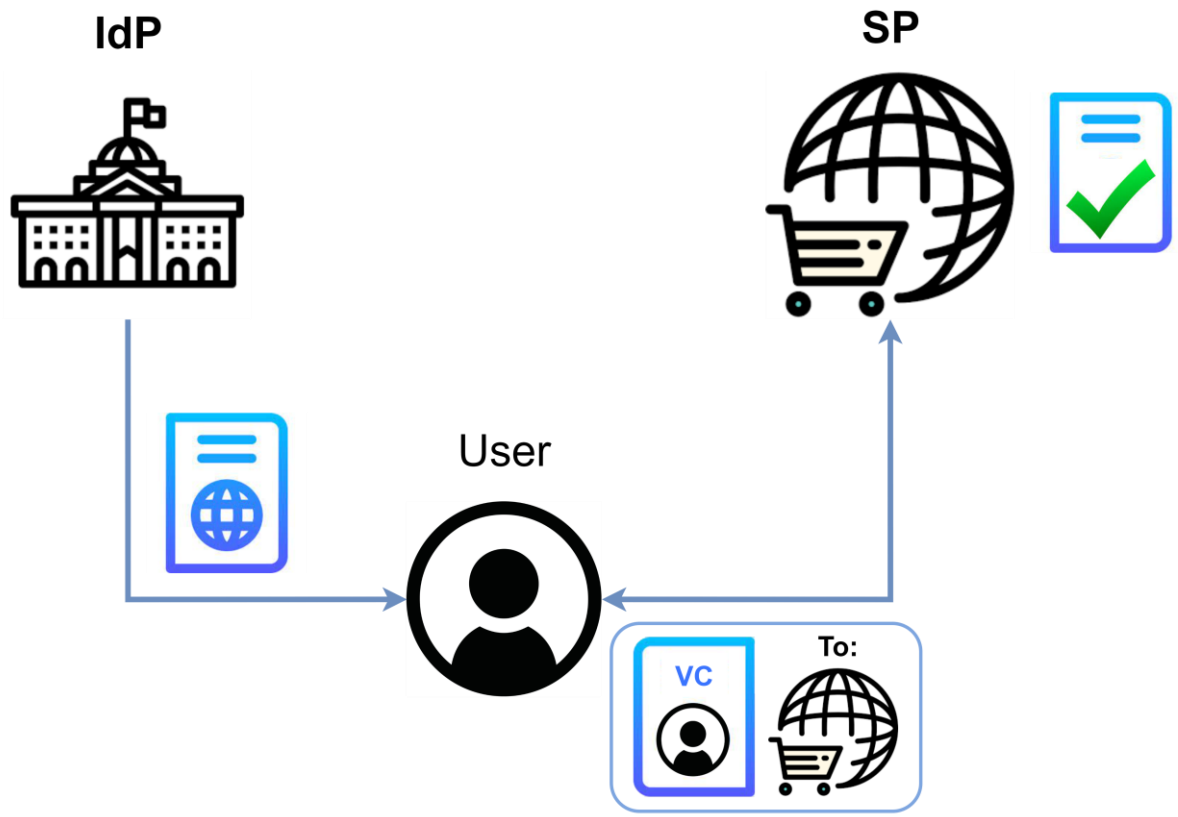
Централизованная модель

Федеративная модель

Модель,

ориентированная на пользователя

Суверенная модель



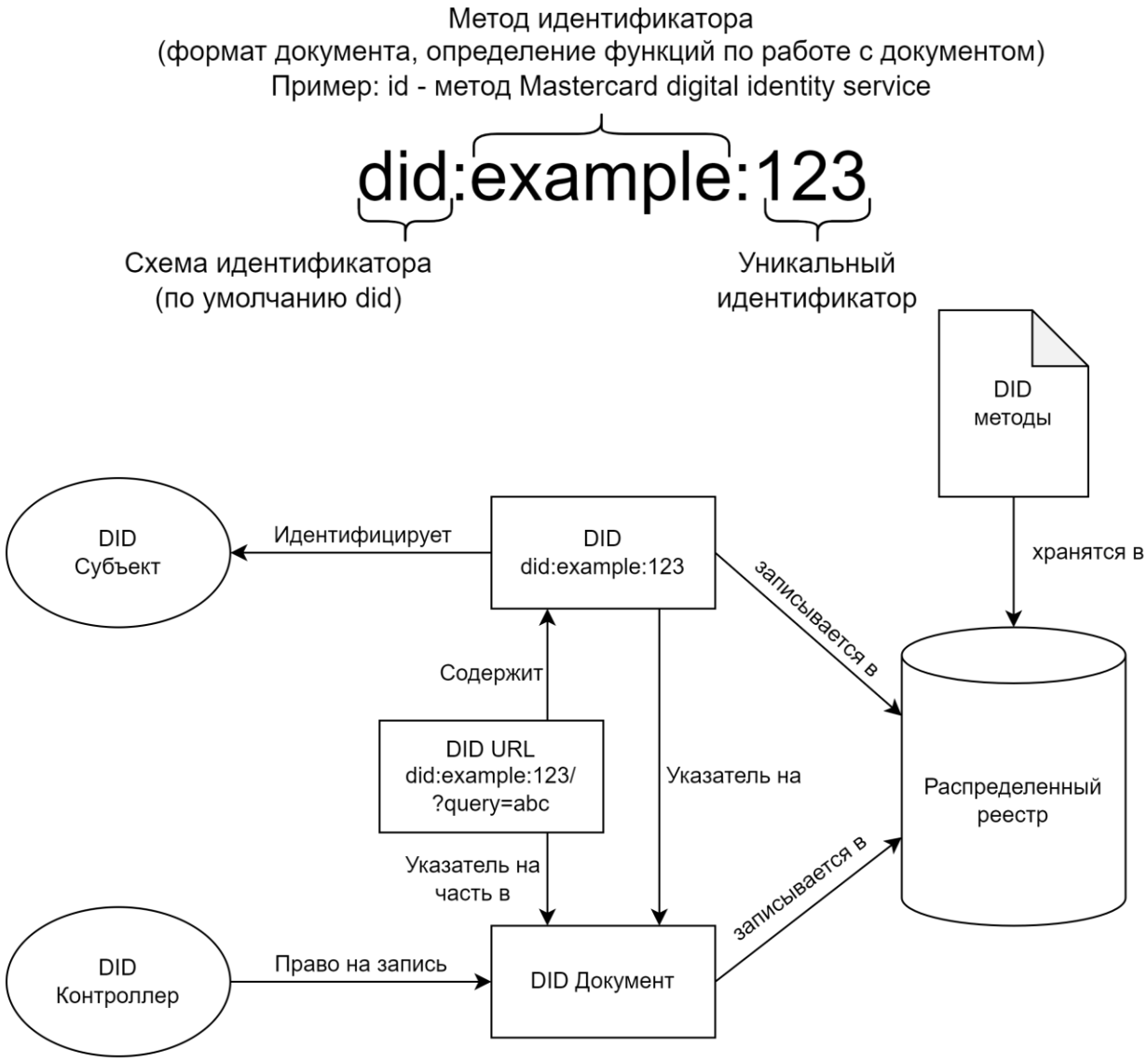
W3C децентрализованные идентификаторы (DIDs)

КРИПТОНИТ

Суть: определение формата идентификатора, для которого:

1) Вместе с идентификатором хранится схема верификации идентифицируемого субъекта
2) Верификация может быть сделана независимо любым участником
3) Децентрализованное хранение идентификатора

https://www.w3.org/TR/did-core/



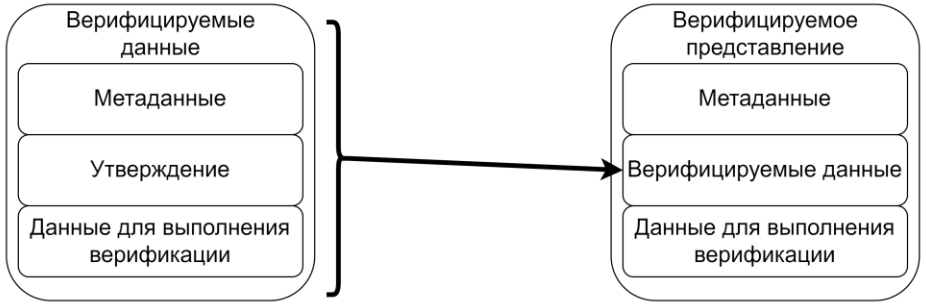
W3C верифицируемые учетные данные (VCs)

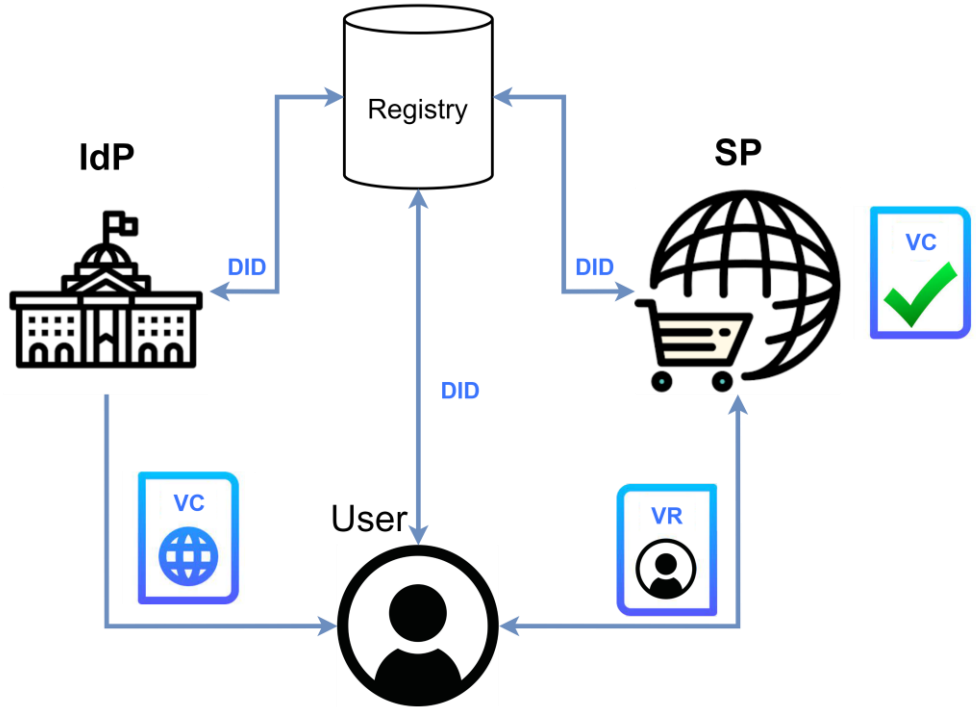
КРИПТОНИТ

Суть: определение формата данных, для которого:

1) Возможно представление в виде утверждений о децентрализованных идентификаторах
2) Представление является валидным только при условии, что их сформировал владелец данных
3) Верификация предоставленных данных может быть сделана независимо любым участником

https://www.w3.org/TR/vc-data-model/

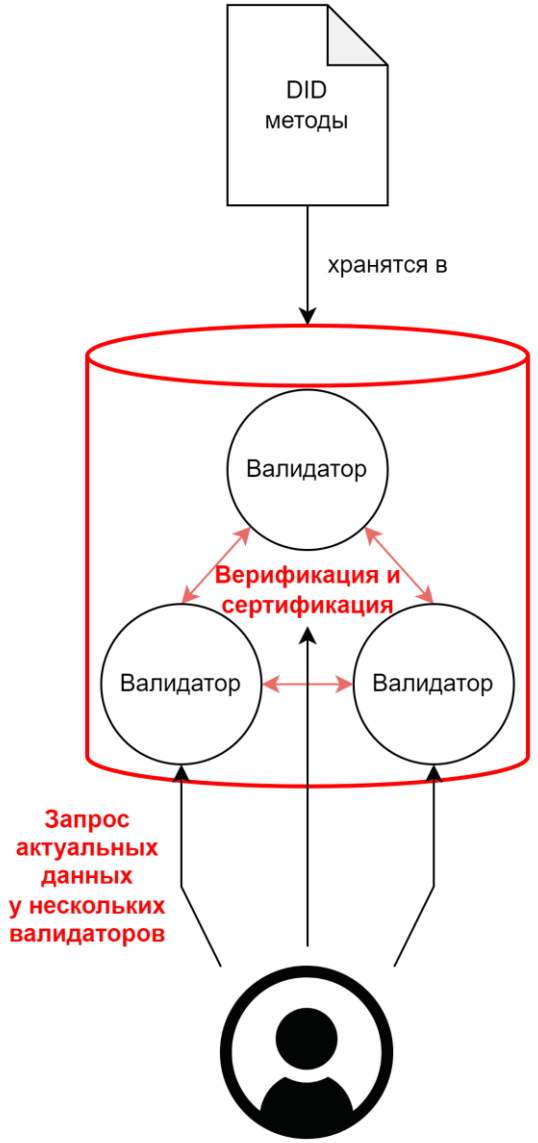




Анализ: трудности по реализации

КРИПТОНИТ

- Каждый новый метод должен быть сертифицирован каждым валидатором.
- Необходимо поддерживать активное состояние с несколькими валидаторами, чтобы получить актуальное и корректное состояние реестра.



Анализ: анонимность

КРИПТОНИТ

Не обеспечивается анонимность пользователя и сервиса. С одной стороны, пользователь не хочет, чтобы сервис знал идентификатор пользователя в системе. С другой стороны, сервис не хочет, чтобы оператор учетных данных знал о том, кто запрашивает проверку данных;

- Используются протоколы неинтерактивного доказательства с нулевым разглашением, которые не стандартизированы в РФ.

HYPERLEDGER ANONCREDS

Camenisch J., Lysyanskaya A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation (EUROCRYPT 2001)

HYPERLEDGER ARIES

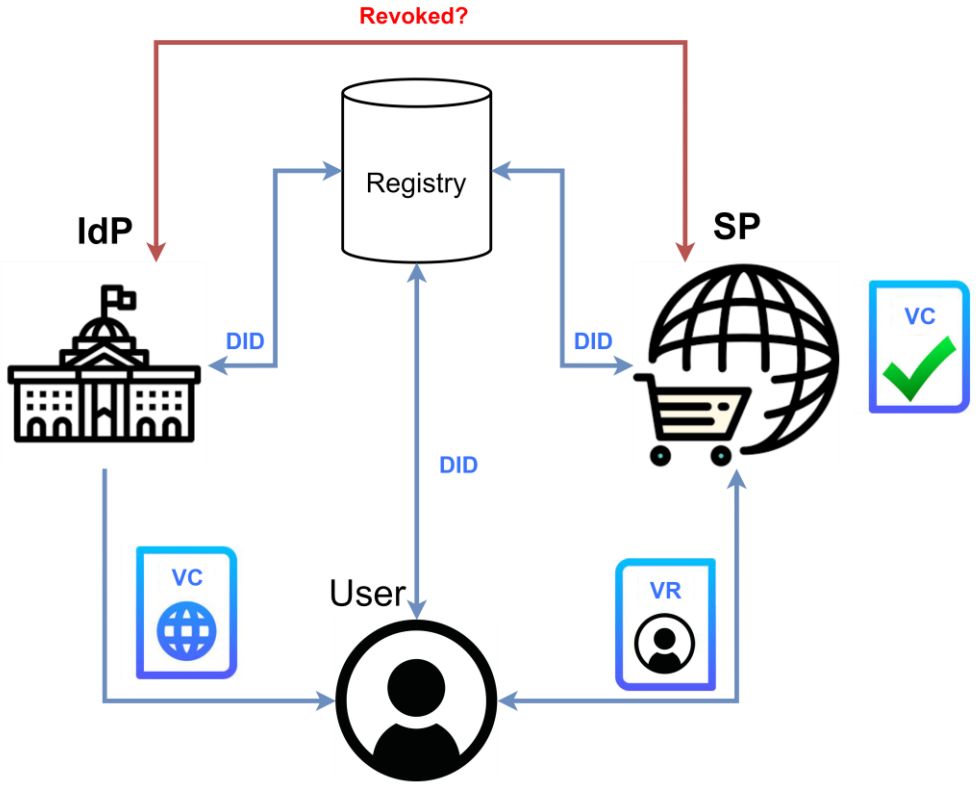
Au M. H., Susilo W., Mu Y. Constant-size dynamic k-TAA //Security and Cryptography for Networks: 5th International Conference (2006)

Анализ: offline режим аутентификации

Аутентификация является выполненной только после получения положительного результата проверки от инспектора, что требует постоянного активного соединения с инспектором (нет offline аутентификации).

- Данные об отзыве учетных данных невозможно получить от пользователя или реестра.

StatusList2021Credential:
https://www.w3.org/TR/vc-status-list/

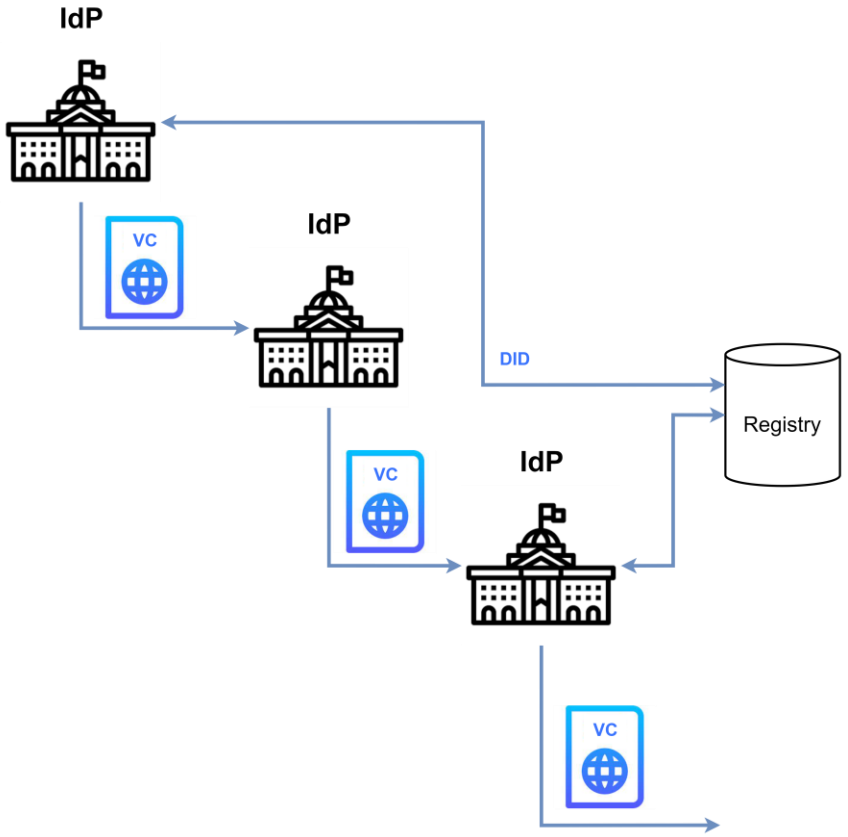


Анализ: удостоверяющий центр как единое место доступа

КРИПТОНИТ

Существует единая точка доступа к системе аутентификации в виде удостоверяющего центра. Удостоверяющий центр является единым местом хранения информации обо открытых ключах пользователей;

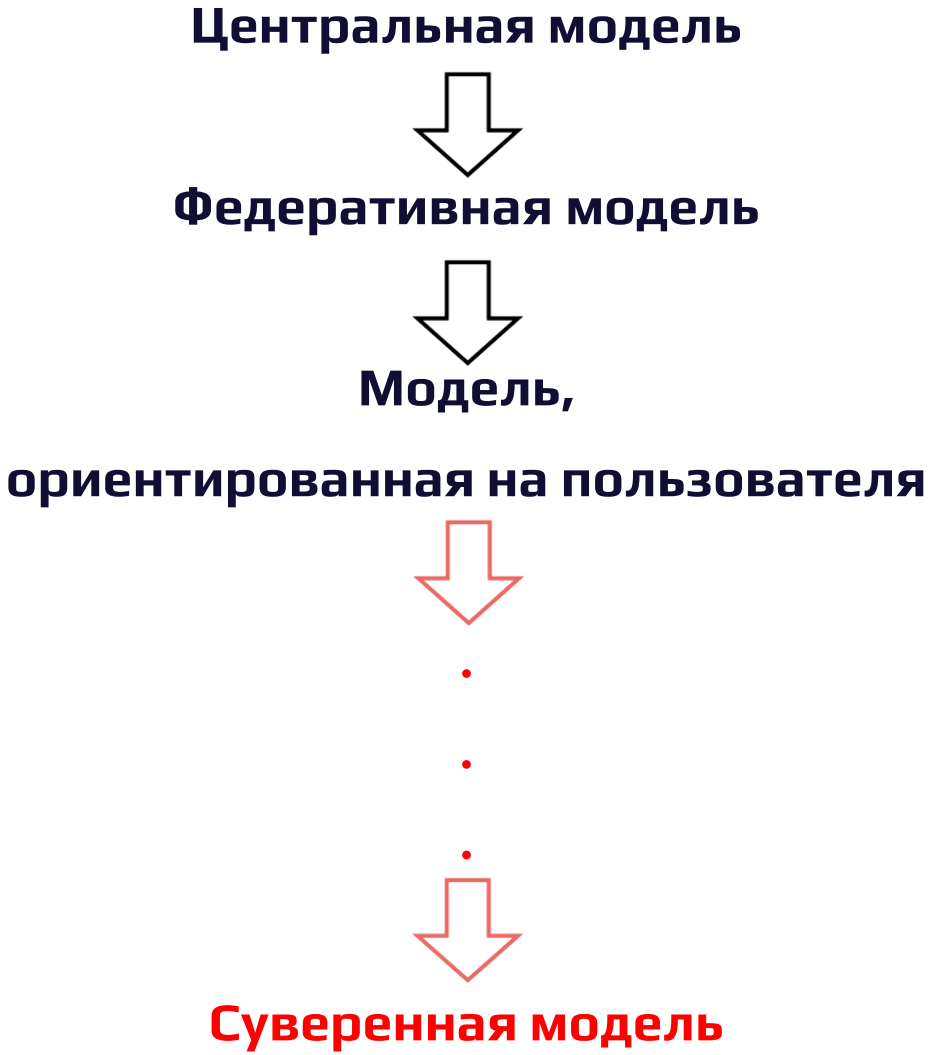
- Необходима авторизация всех провайдеров на наличие права выдачи верифицируемых данных вплоть до аутентификации корневого провайдера с помощью реестра.



Итог

КРИПТОНИТ

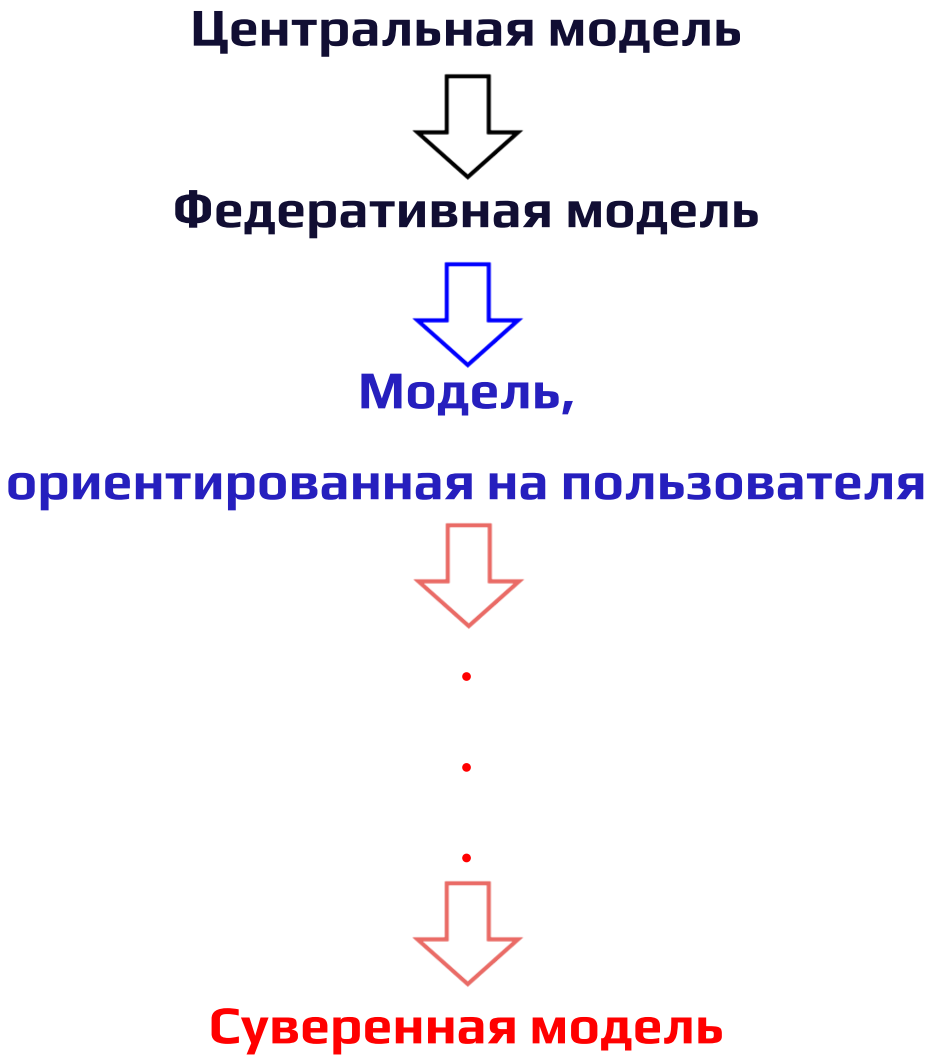
- Суверенная модель обеспечивает все свойства федеративной и ориентированной на пользователя, моделей, дополнительно решая задачи анонимности, offline аутентификации. Однако практическая реализация ещё далека от суверенной модели.



Итог

КРИПТОНИТ

- Суверенная модель обеспечивает все свойства федеративной и ориентированной на пользователя, моделей, дополнительно решая задачи анонимности, offline аутентификации. Однако практическая реализация ещё далека от суверенной модели.
- Перспективным является решение поставленных задач на этапе модели, ориентированной на пользователя. В частности использование одноразовых идентификаторов для анонимности с контролем от инспектора учетных данных и использование выдаваемых провайдером учетных данных токенов на этапе формирования подтверждения данных пользователем.



Итог

КРИПТОНИТ

- При этом на основе текущего подхода наработки в части практической реализации модели, ориентированной на пользователя, могут в последствии быть использованы в практической реализации суверенной модели на этапе подтверждения/верификации учетных данных.

Итог

КРИПТОНИТ

- При этом на основе текущего подхода наработки в части практической реализации модели, ориентированной на пользователя, могут в последствии быть использованы в практической реализации суверенной модели на этапе подтверждения/верификации учетных данных.
- С нашей стороны, ведется активное развитие модели, ориентированной на пользователя, в рамках разработки и внедрения Платформы Цифрового Доверия (ПЦД) при поддержке Минцифры. Готовятся первые эксперименты по использованию платформы.

https://kryptonite.ru/articles/modern-approaches-to-personal-data-protection/

https://www.itu.int/en/ITU-D/Conferences/ET/2021/Pages/Programme.aspx

https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2023/0828/Pages/programme.aspx

Спасибо за внимание!

Если у Вас в будущем будут еще вопросы, контактные данные докладчика:

Илья Герасимов, i.gerasimov@kryptonite.ru

КРИПТОНИТ