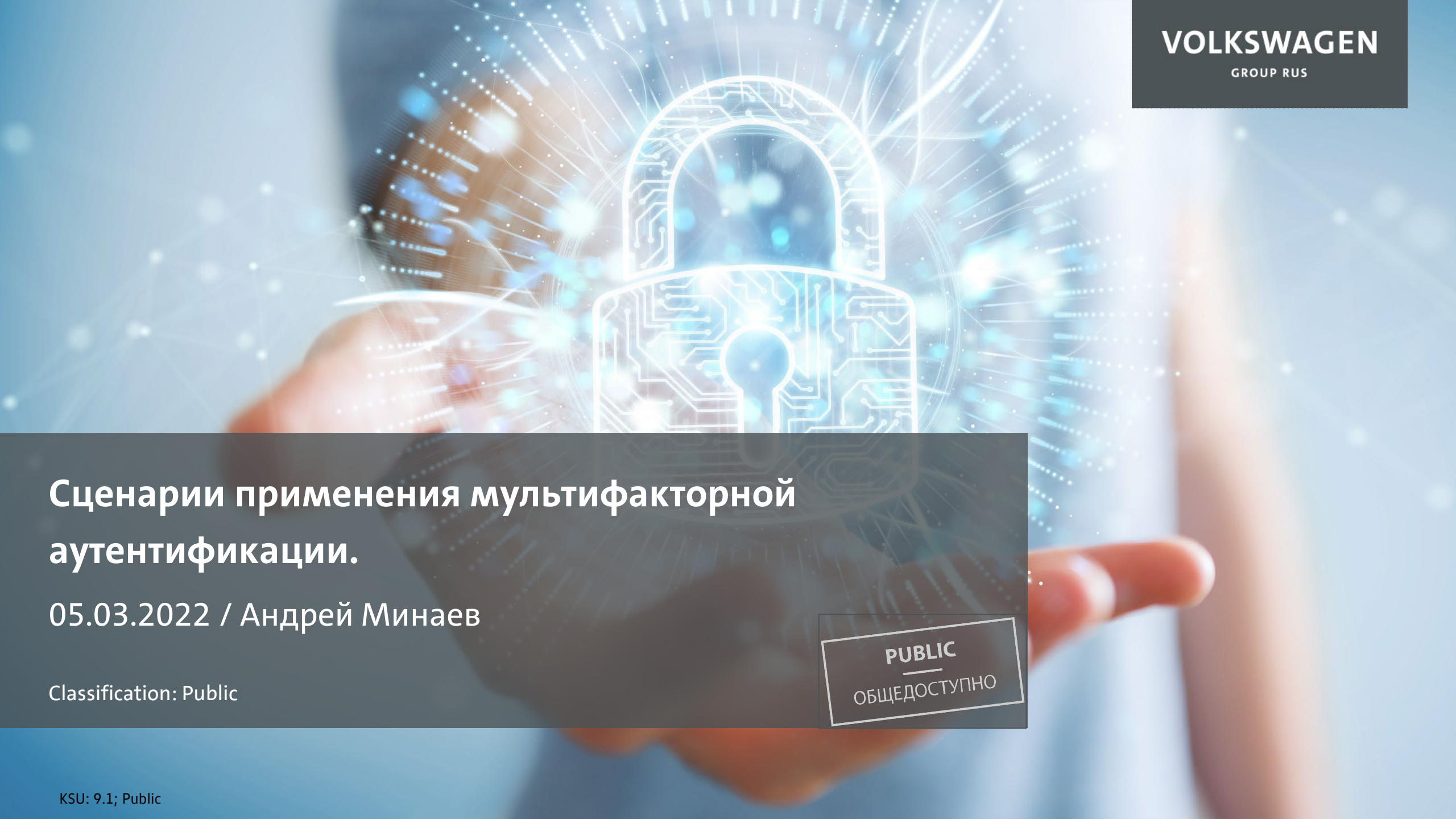


VOLKSWAGEN
GROUP RUS

Сценарии применения мультифакторной аутентификации.

05.03.2022 / Андрей Минаев

PUBLIC
ОБЩЕДОСТУПНО

Classification: Public

Аутентификация и авторизация. В чём разница?

VOLKSWAGEN
GROUP RUS

Идентификация

Ты кто такой?

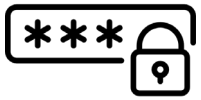
Userid/login

Иванов Иван

Идентификация – процедура, в результате выполнения которой для субъекта выявляется его уникальный признак, однозначно определяющий его в информационной системе

Аутентификация

Чем докажешь?



Пароль

Паспорт

Аутентификация – процедура проверки подлинности, например, проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных

Авторизация

На что имеешь право?

Пользователь/
Администратор

Право голоса/
Право собственности

Авторизация – предоставление определенному лицу прав на выполнение определенных действий

Важно помнить о процессе регистрации в системе

Регистрация пользователя в системе:

- Создание идентификатора (User ID)
- Привязка аутентификации (пароля)

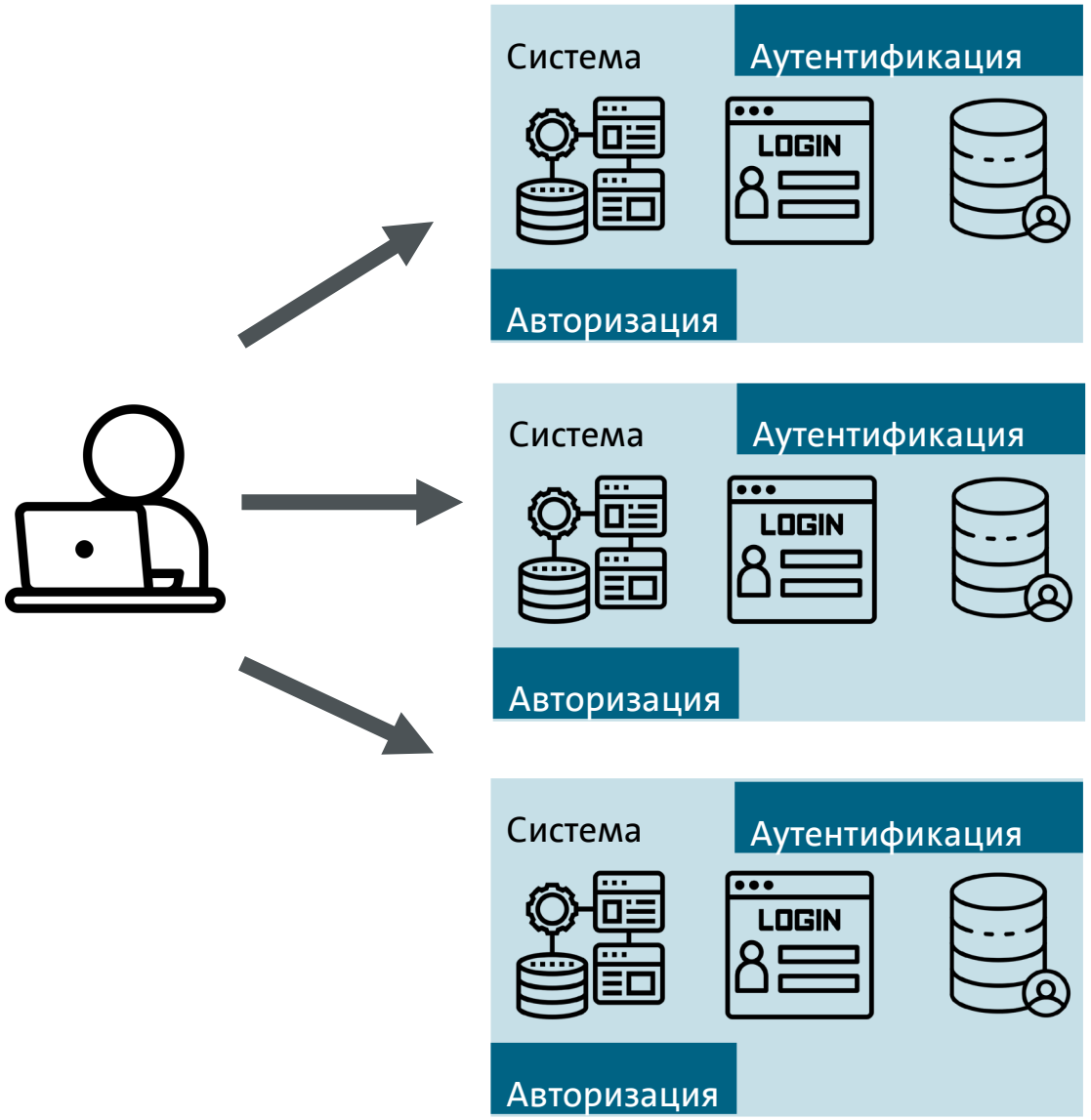
Виды регистрации:

- Административная (по заявке, либо автоматически)
- Самостоятельная

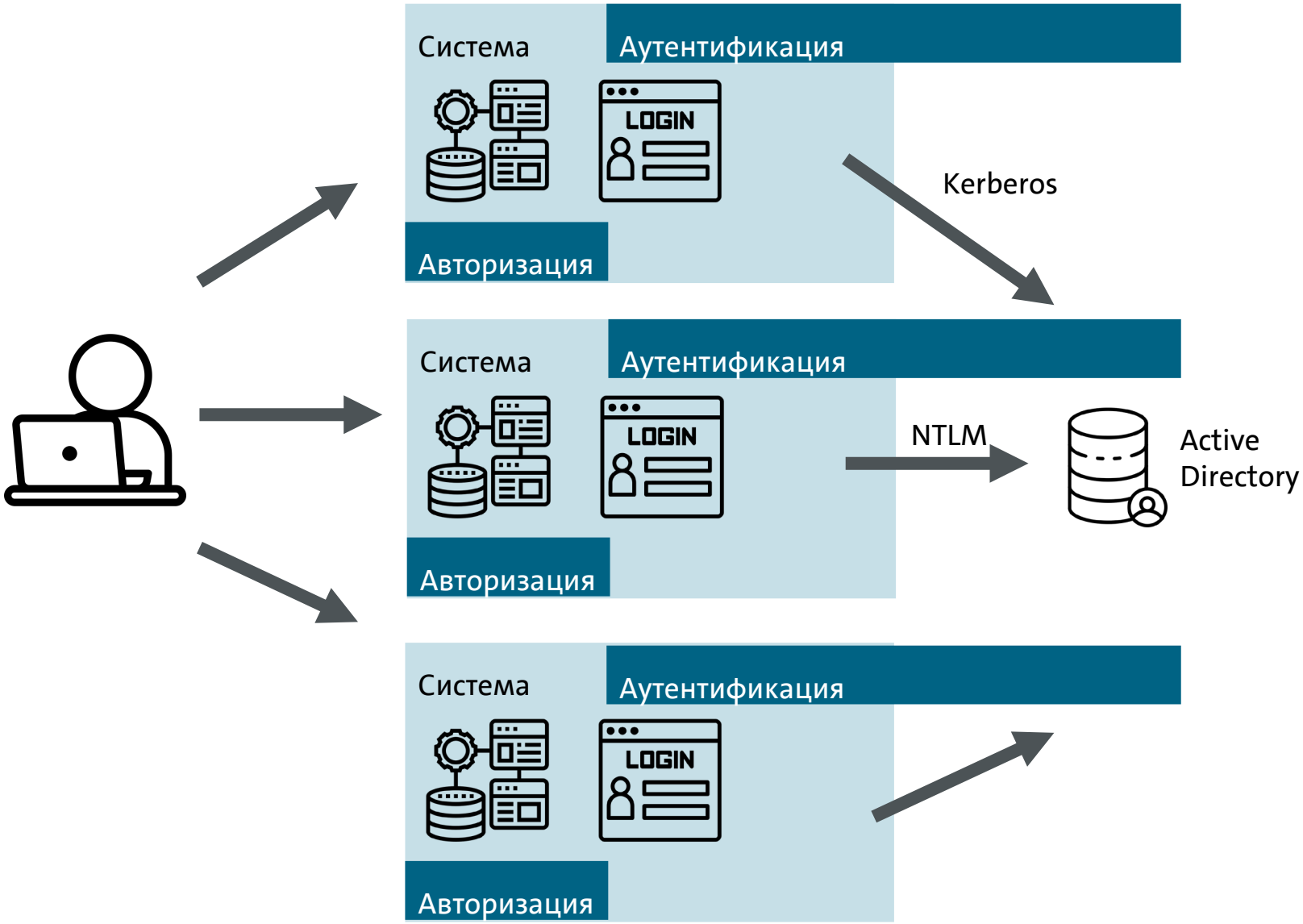
KSU: 9.1; Public

Аутентификация и авторизация в системе

Много систем - много процессов аутентификации и регистрации пользователей



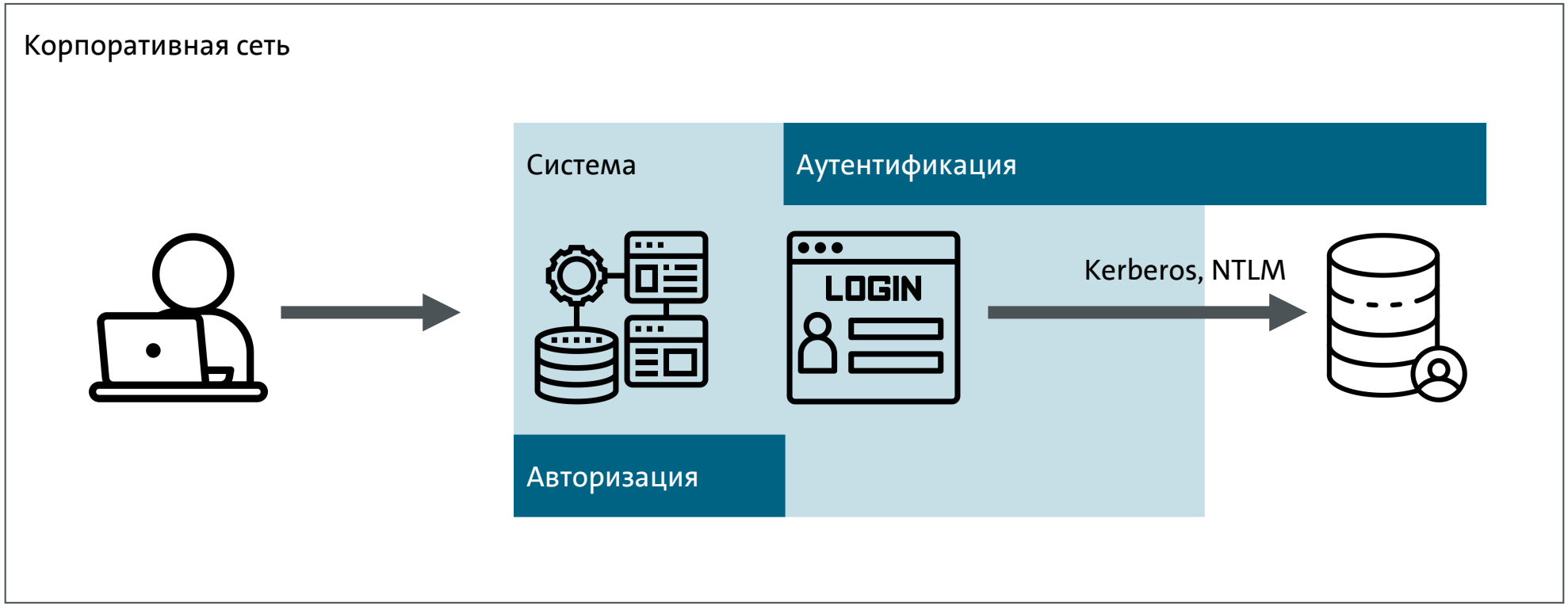
AD. Много систем - одна база пользователей, один процесс регистрации



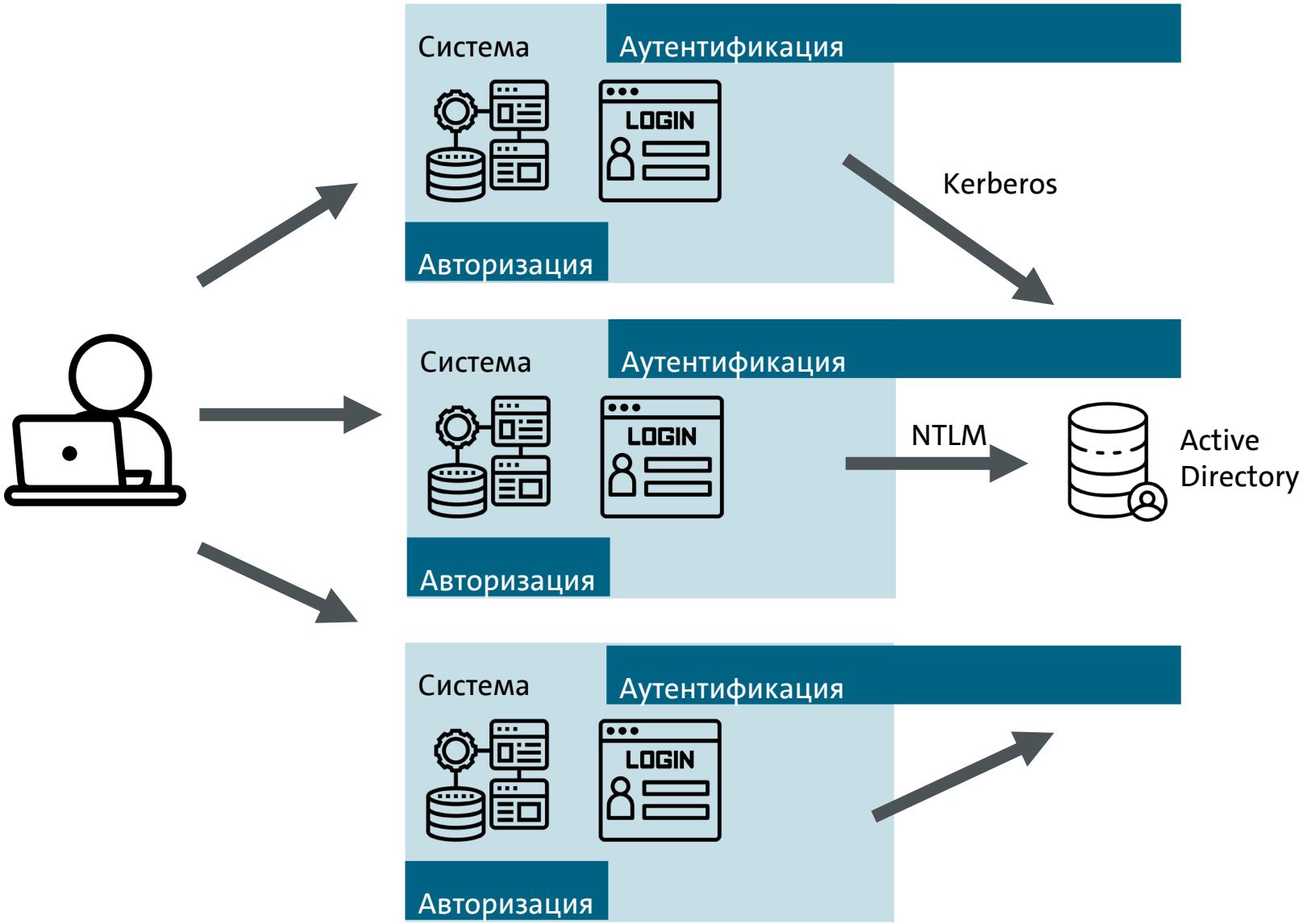
Active Directory имеет целый ряд ограничений

VOLKSWAGEN
GROUP RUS

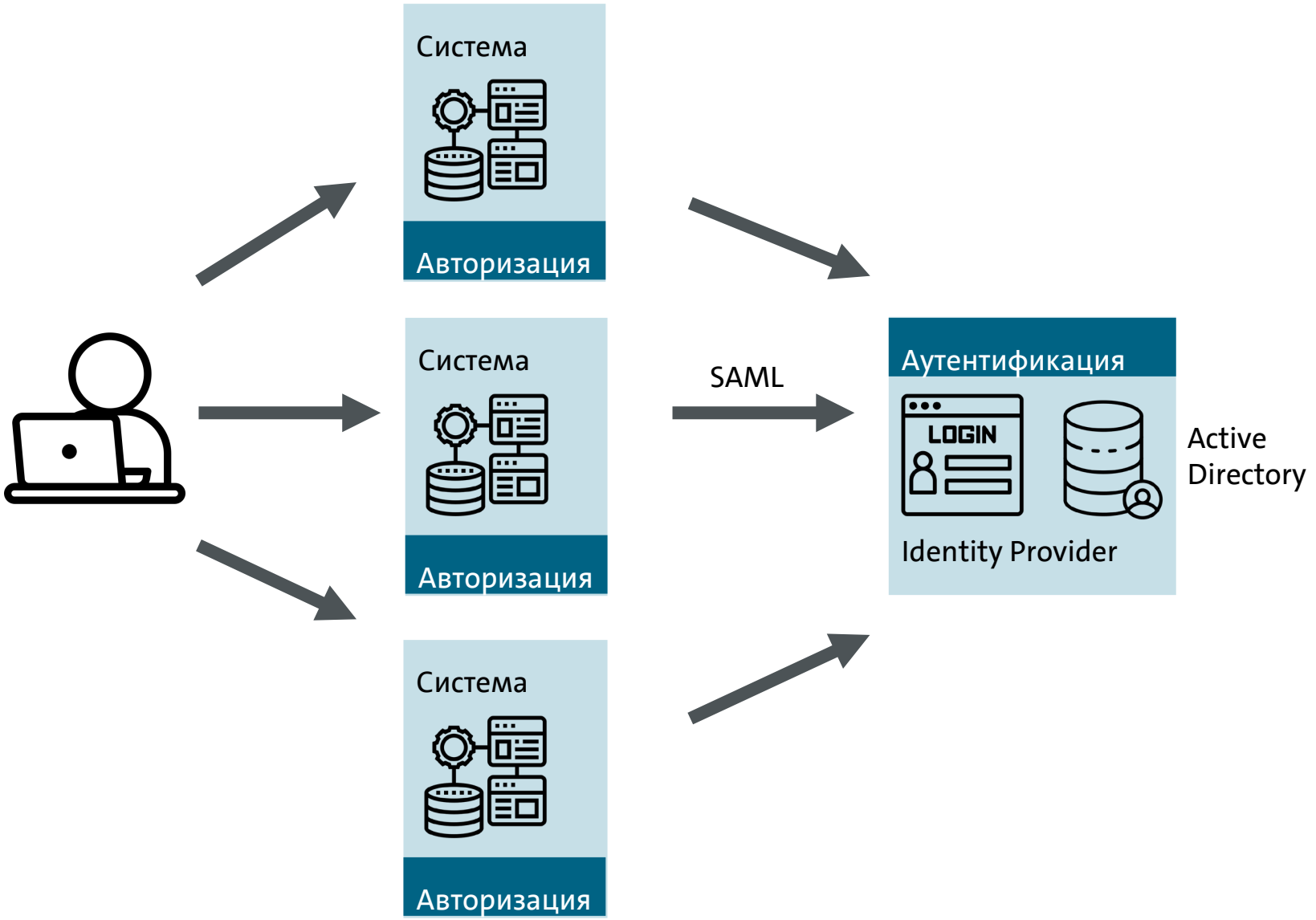
- Kerberos – работает только с доменными компьютерами
- Kerberos, NTLM – только внутри сети
- Приложение должно знать структуру AD, имя домена, доменных контроллеров, OU



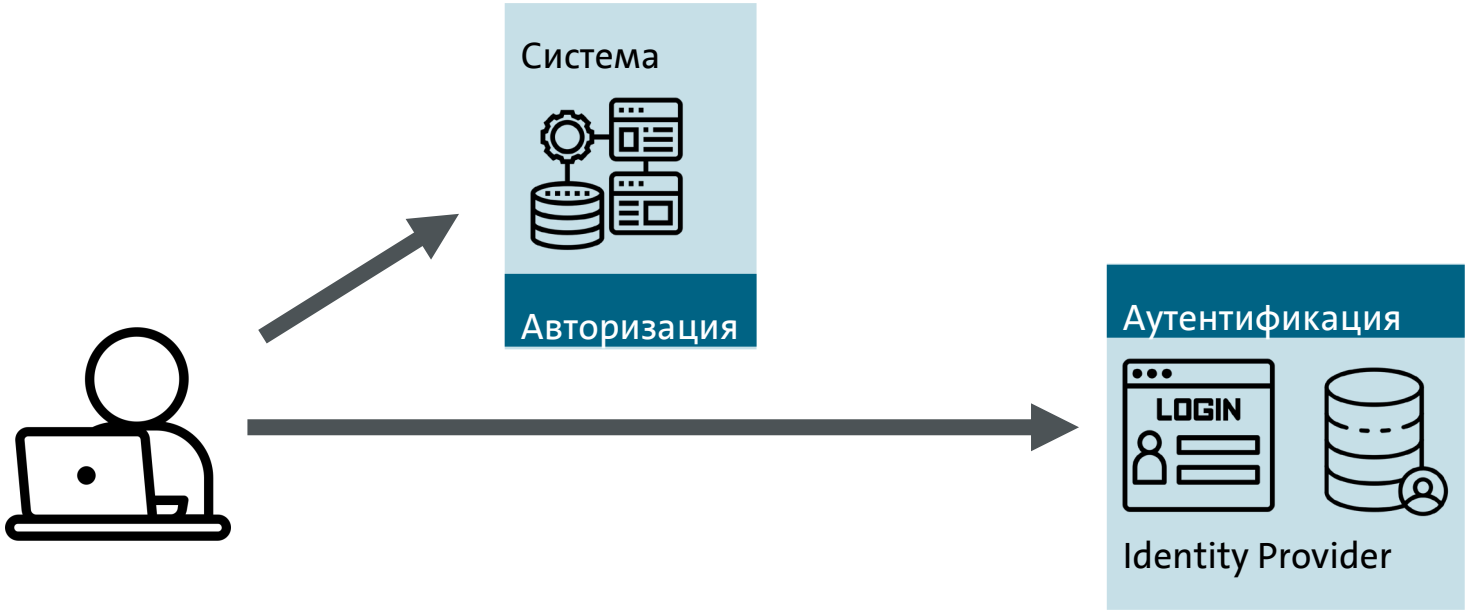
При использовании AD для каждой системы свой процесс аутентификации



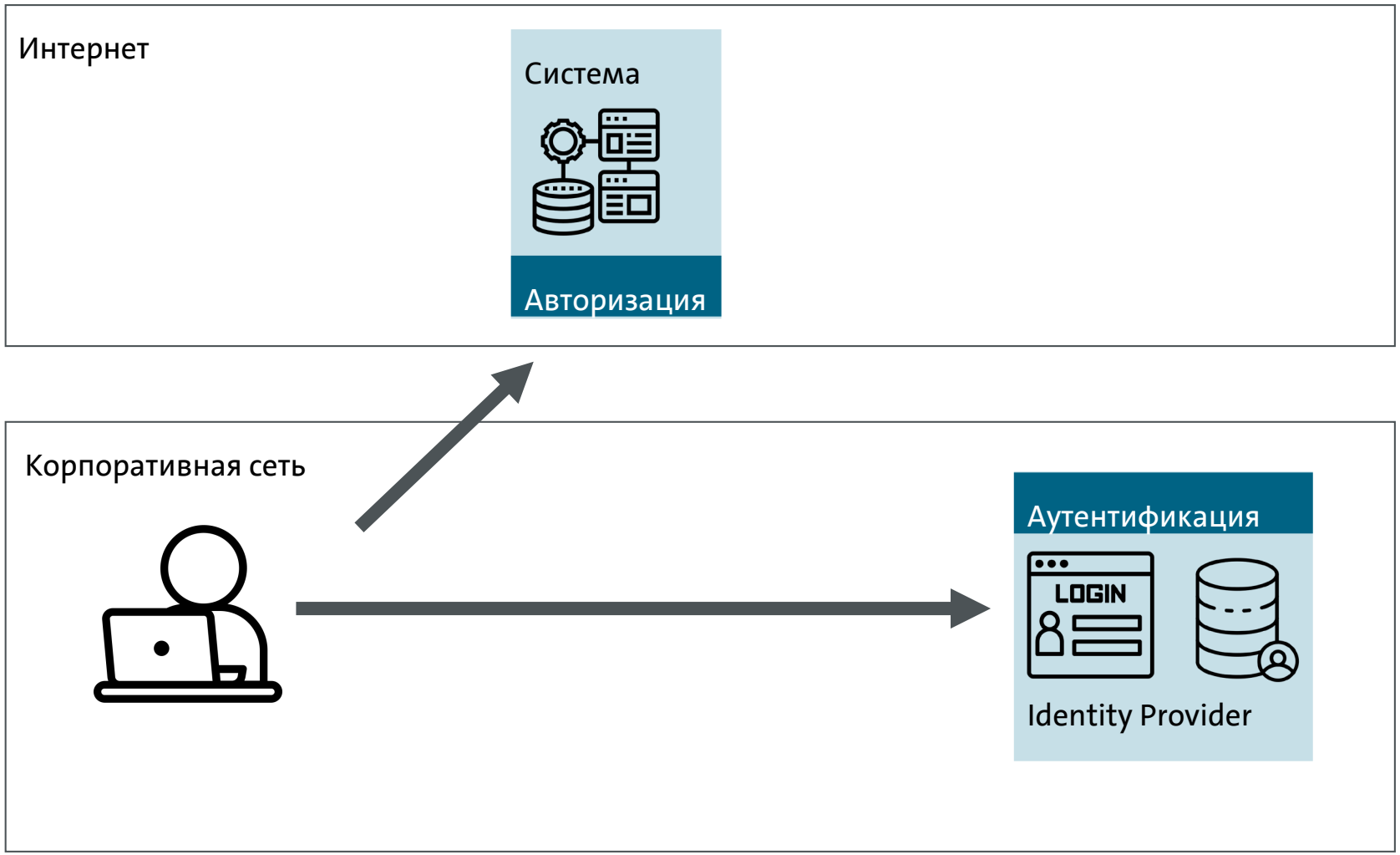
Identity Provider. Много систем - одна база пользователей, один процесс аутентификации



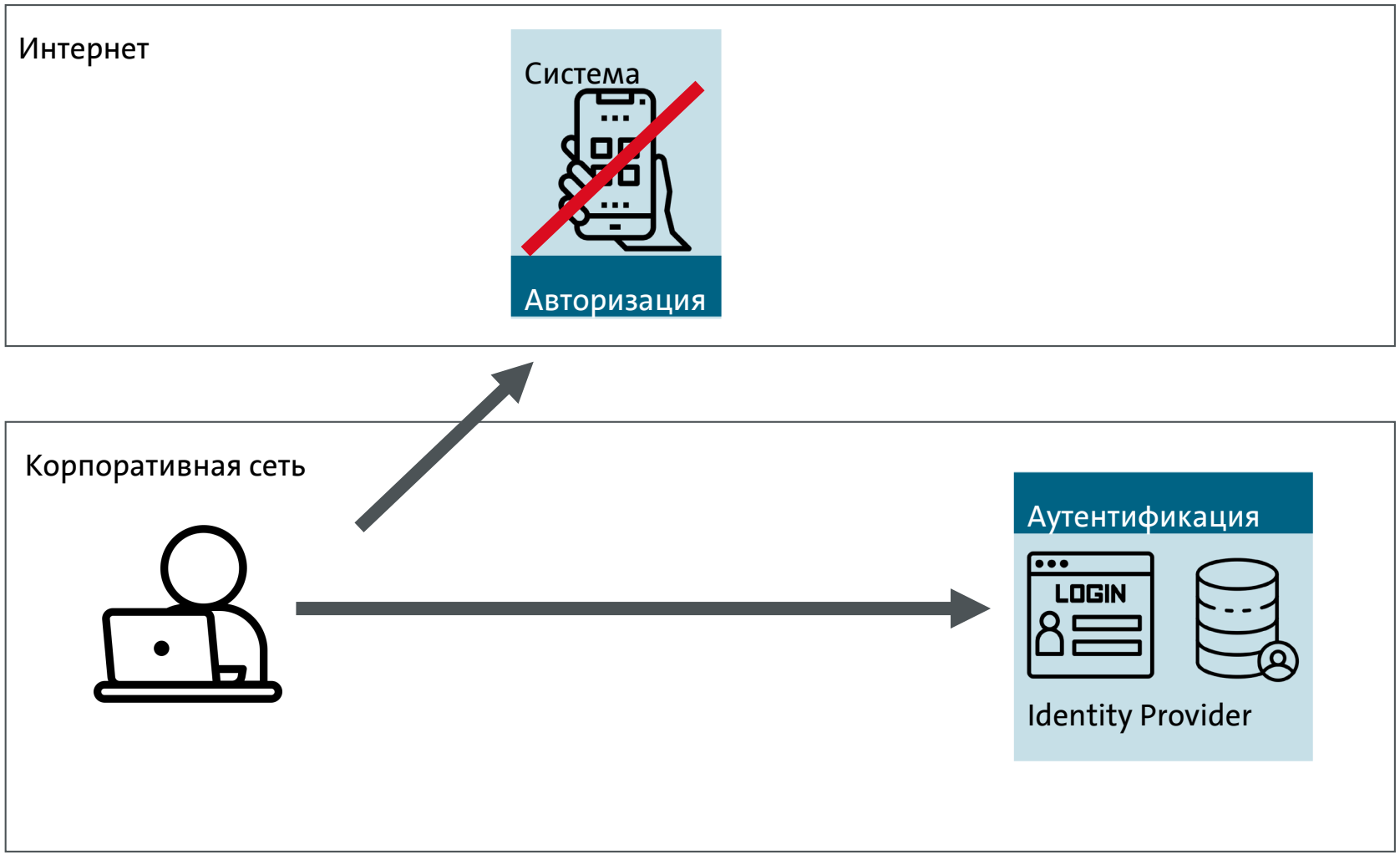
Система и Identity Provider напрямую не взаимодействуют



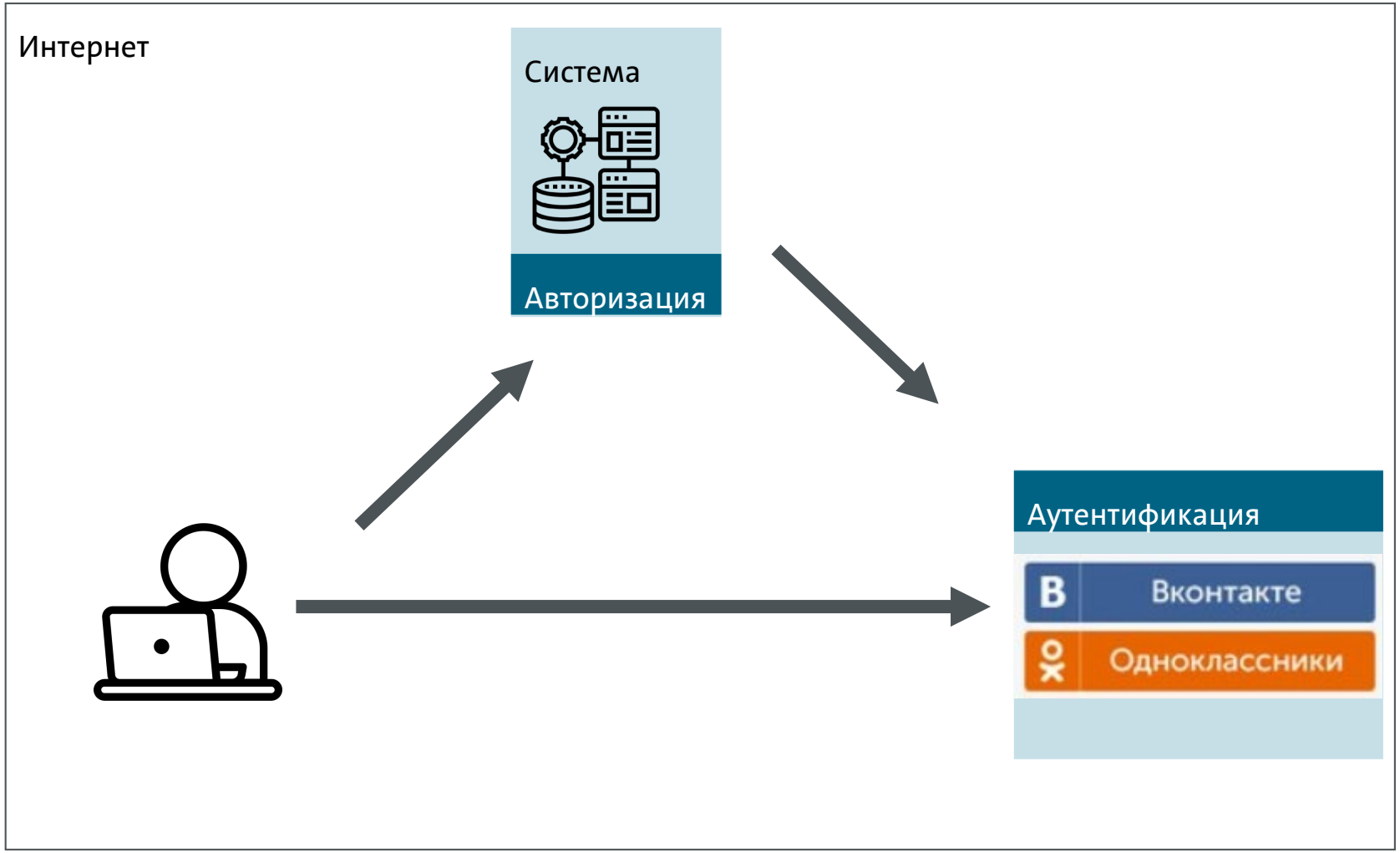
SAML позволяет аутентифицировать внутренних пользователей на внешних системах. Внешняя система не знает паролей пользователей



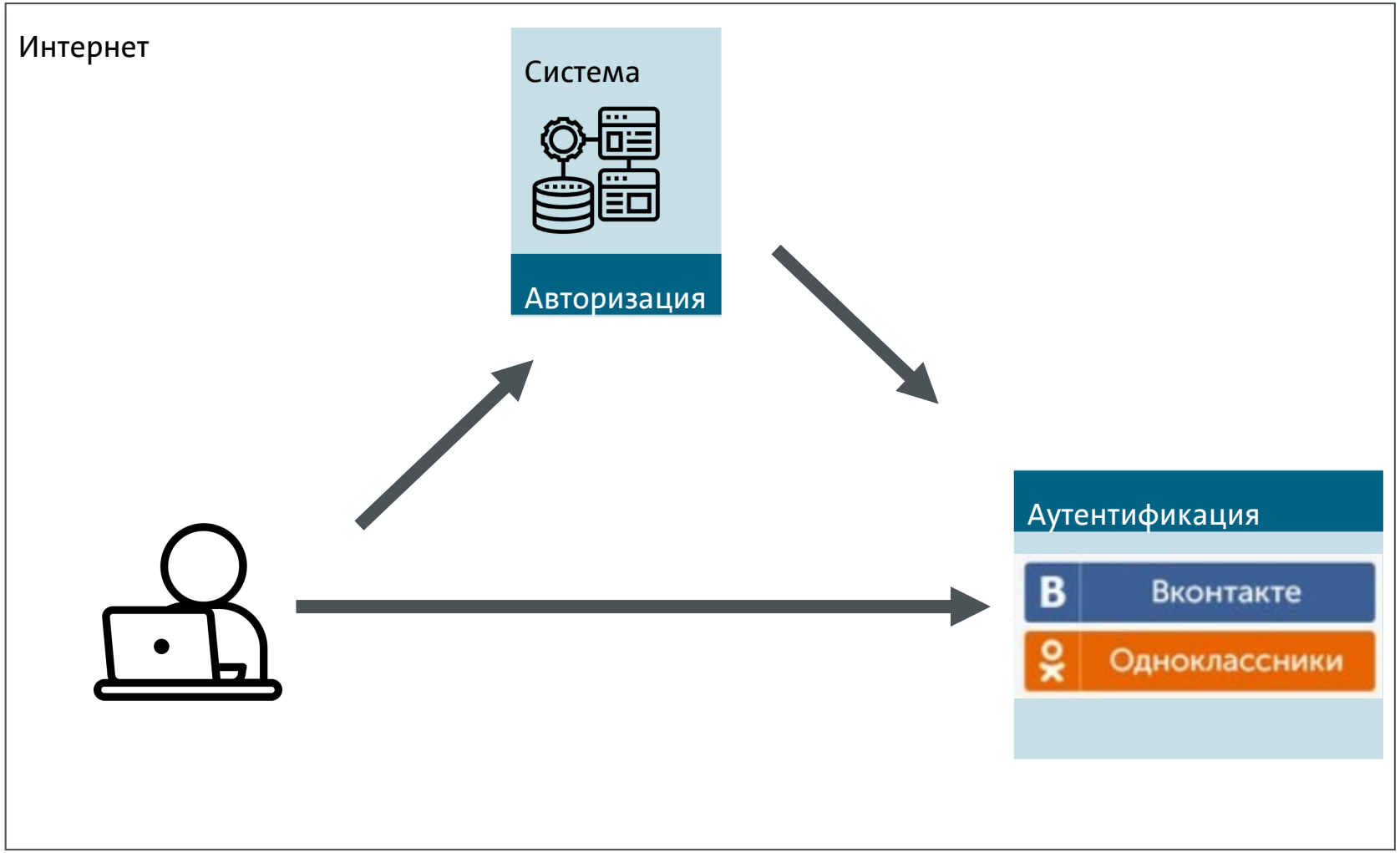
SAML не работает с мобильными приложениями. Клиент – это браузер



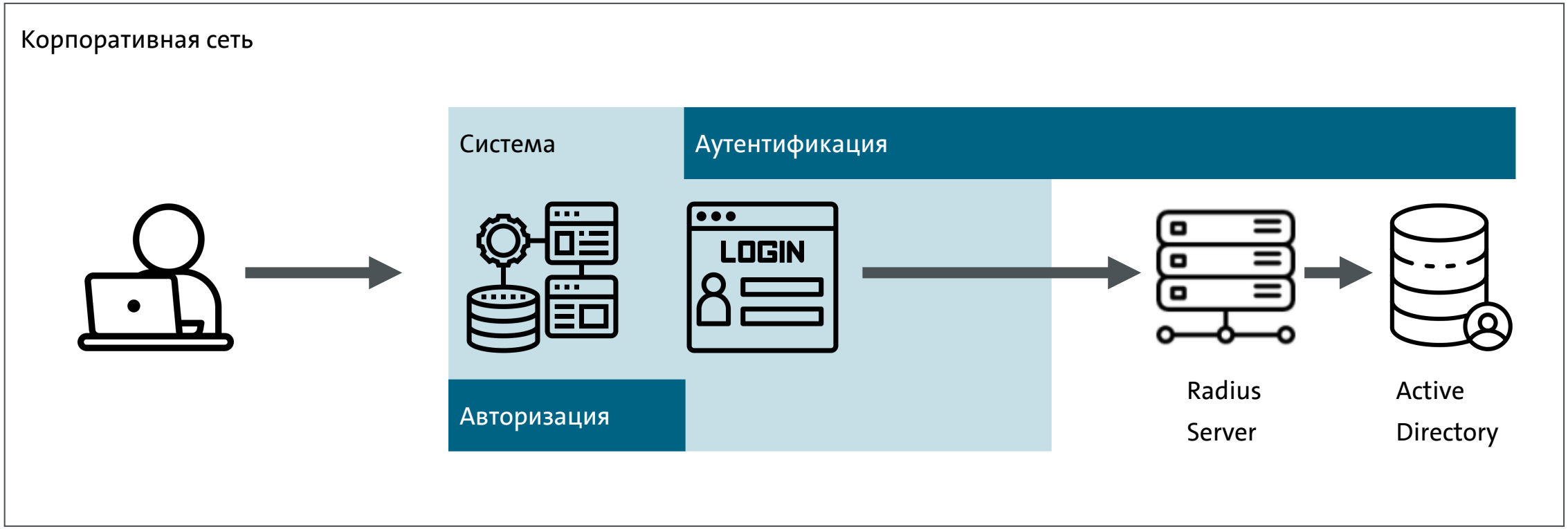
OAuth 2 чаще применяется в публичных системах. Работает с мобильными приложениями. Система напрямую взаимодействует с Identity Provider (Authorization Server).



OAuth 2 и SAML в первую очередь применяются для WEB систем т.к. используется перенаправление пользователя с целевой системы на систему аутентификации



Для сетевых систем (VPN, VDI) чаще всего используется протокол Radius



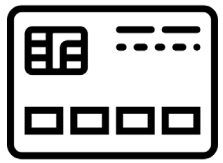
Факторы аутентификации

VOLKSWAGEN
GROUP RUS

То что Вы знаете

Пароль
PIN код
Кодовое слово

То что у Вас есть

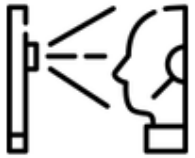


PKI Card

USB Token

Приложение
SMS TOTP
APP TOTP (Authenticator)
Звонок

То что Вас описывает

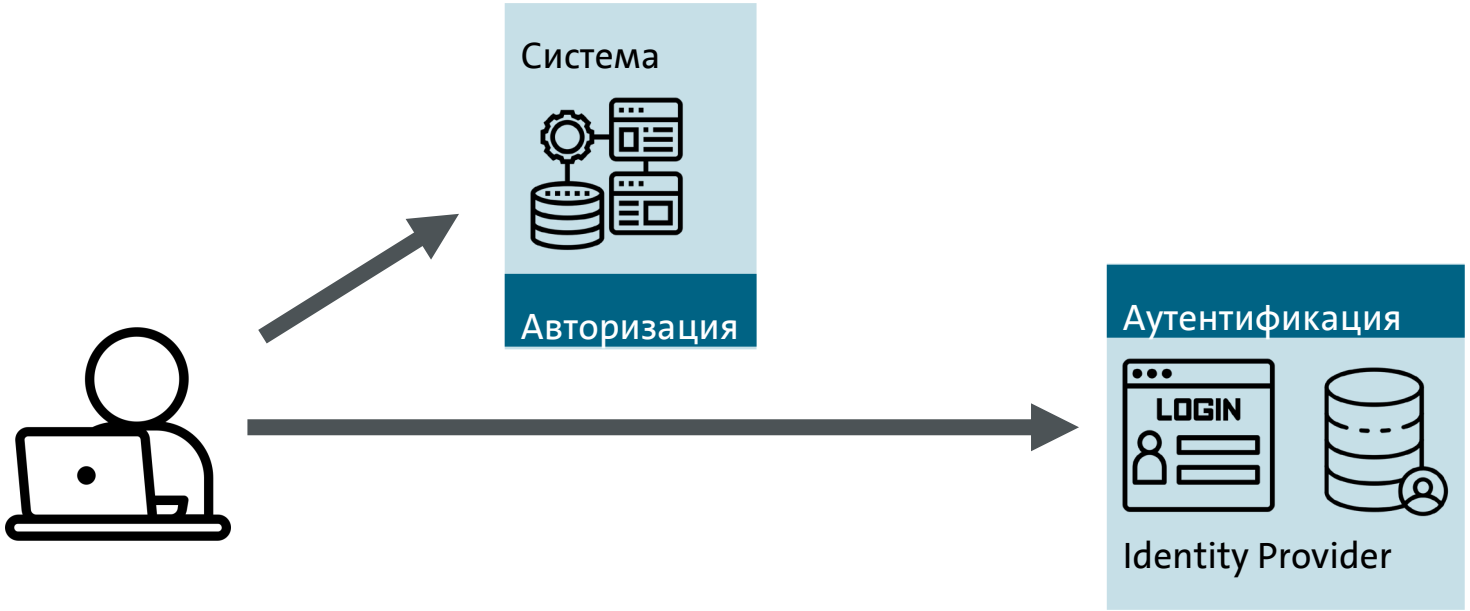


Лицо

Отпечаток пальца

Голос

Многофакторную аутентификацию проще всего внедрять централизованно на уровне Identity Provider



Вопросы, которые надо задать перед внедрением MFA

VOLKSWAGEN
GROUP RUS

- Для кого внедряется система? Внешние или внутренние пользователи?
- Для каких систем будет внедрятся MFA? Какие протоколы (SAML, Oauth 2.0, Radius) поддерживают существующие системы?
- Каков процесс регистрации пользователей? Ручной или самостоятельный?
- Поддерживает ли Identity Provider самостоятельное включение второго фактора?
- Как будет восстановлен доступ, если пользователь потеряет доступ ко второму фактору?
- Если будет использован USB Token или PKI Card, то как они будут доставляться/меняться

Выводы

- ✓ Оцените для каких систем и пользователей внедряете MFA
- ✓ Выбирайте системы с поддержкой SAML и OAuth 2.0
- ✓ Экономьте за счёт внедрения централизованной системы аутентификации

Андрей Минаев

Andrey.Minaev@vwgroup.ru

www.vwgroup.ru

VOLKSWAGEN
GROUP RUS