



Композитная аутентификация HID[®] DigitalPersona[®]

Правильное сочетание факторов и условий

Конференция Код ИБ “Системы аутентификации”
9 сентября 2020 г.



Только пароля уже недостаточно

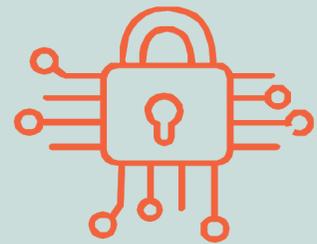
- Простые пароли легко подобрать
- Сложные пароли трудно запоминать и менять
- Много приложений – много паролей
- Один фактор (пароль) – высокий риск



Решение: композитная аутентификация DigitalPersona

Композитная аутентификация

Правильное сочетание факторов под конкретные условия



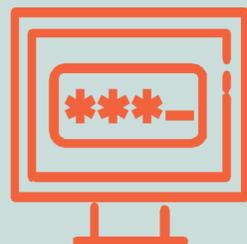
Что Вы знаете?

- Пароль
- ПИН-код
- Секретные вопросы



Кем Вы являетесь?

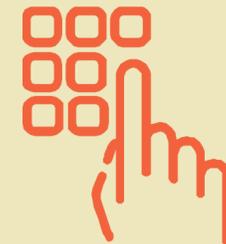
- Отпечатки пальцев
- Лицо



Что у Вас есть?

- Смарт-карта
- Карты доступа
- Устройства Bluetooth
- Одноразовые пароли (OTP)
- FIDO-токены

ФАКТОРЫ



Что Вы делаете?

- «Почерк» пароля
- Свайп (Push)



Где?

- IP-адрес
- Сетевое присутствие (IWA)



Когда и как?

- Время доступа
- Перезагрузка
- Смена пользователя

УСЛОВИЯ

Гибкая интеграция

Windows Logon

- Все факторы аутентификации
- Условия доступа

Облачный доступ

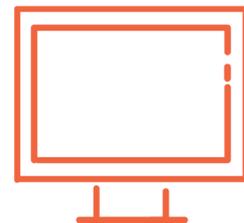
- DigitalPersona IdP
- ADFS
Azure AD
Office 365 и др.

Единый вход (SSO)

- Быстрая настройка сквозной аутентификации
- Без доработки приложений

API

- Стандартизированный WEB API (RESTful)
- Требуется доработка сервисов



Windows



Приложения



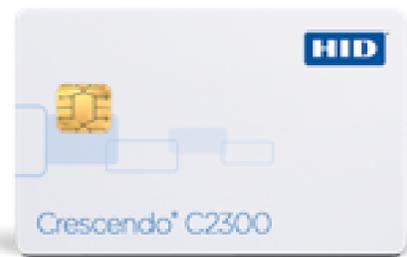
Web

Сценарии использования

-  **Windows Logon**
Защита доступа к Windows с помощью клиент-серверных модулей.
-  **Single Sign-On**
Сквозная аутентификация в корпоративные сервисы согласно точечным политикам безопасности.
-  **Облачная защита**
Безопасный доступ в облачные сервисы компании
-  **Удалённый доступ**
Защита дистанционного доступа к корпоративным ресурсам через VPN (RADIUS)

Широкий выбор аутентификаторов HID

Различные комбинации в зависимости от форм-фактора



PKI

- Вход по смарт-карте
- Защита почты и документов



OTP

- Удаленный доступ по одноразовому паролю



RFID

- Физический и логический доступ



FIDO

- Windows Hello
- Web-доступ

NEW

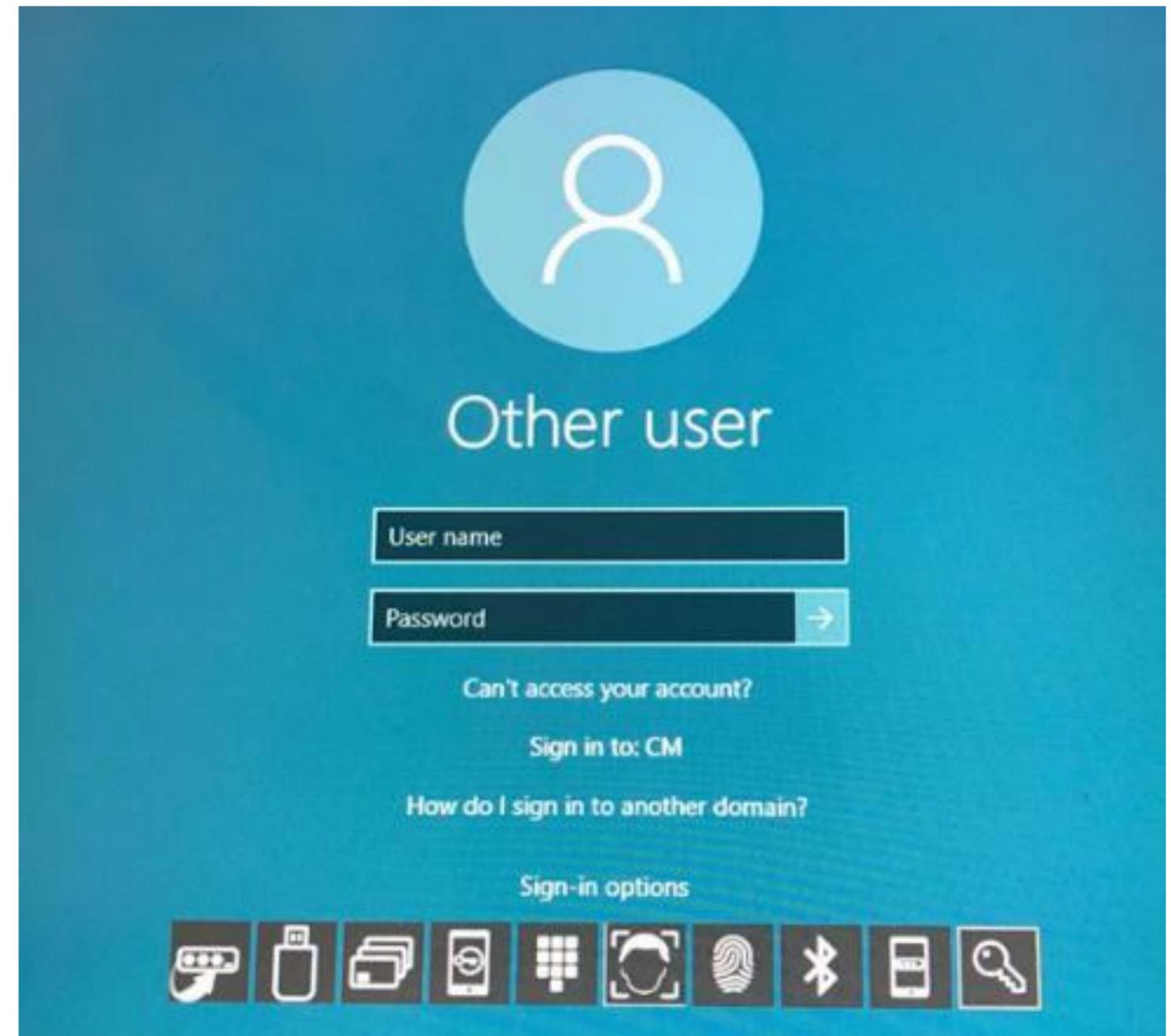


BIO

- Windows Hello
- SSO

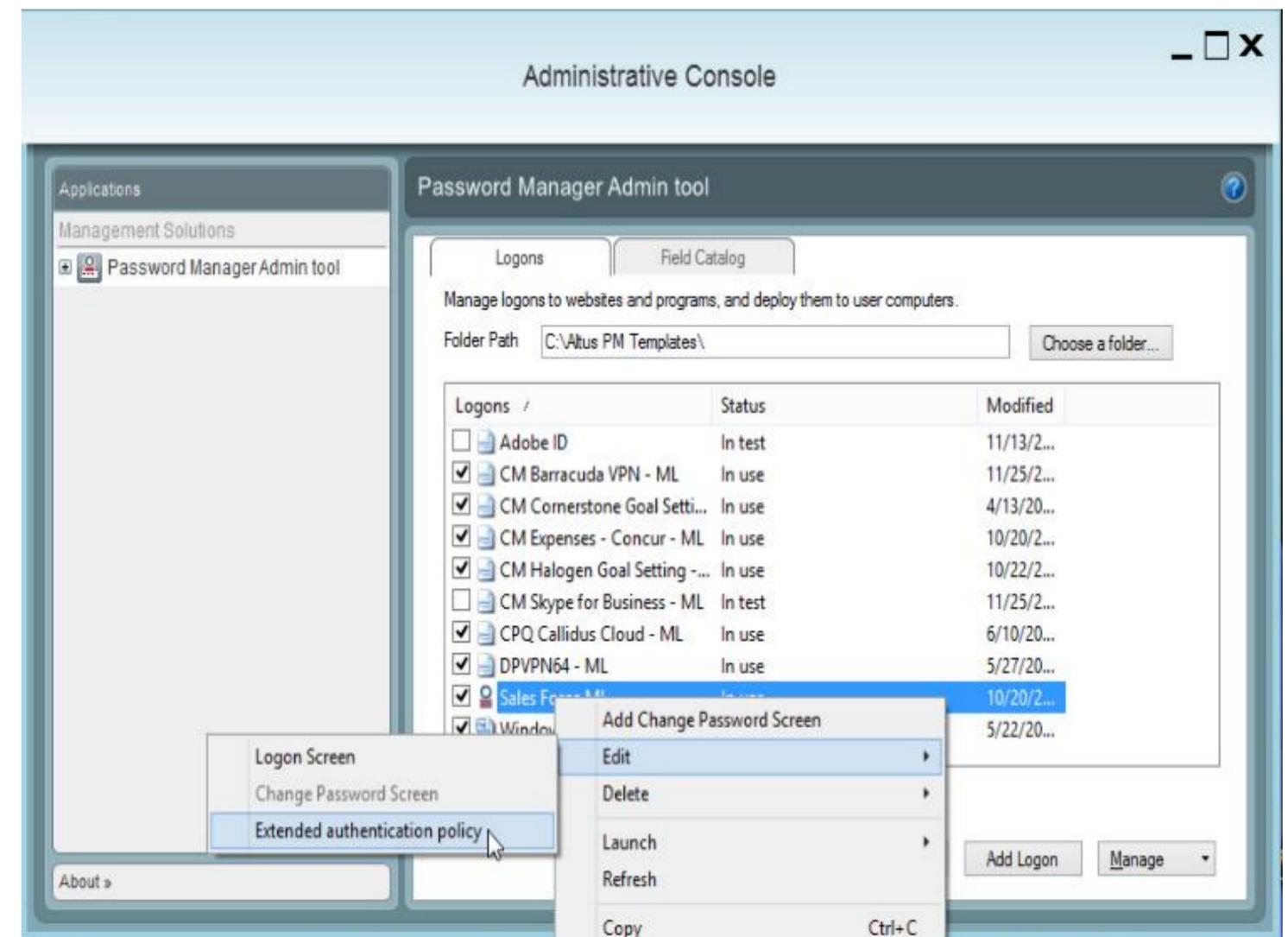
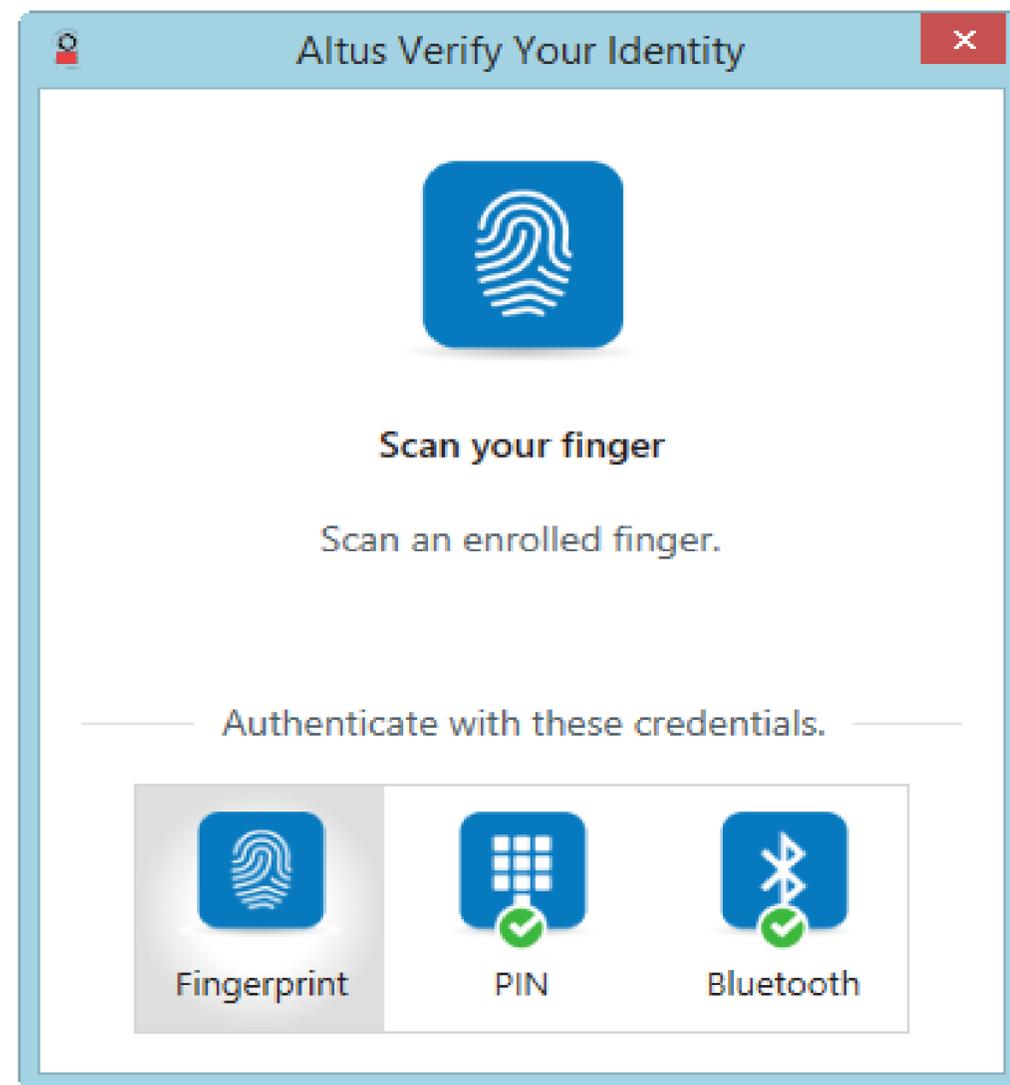
Вход в Windows

- Контрольные вопросы
- FIDO-токен
- Смарт-карта
- Пуш
- ПИН-код
- Лицо
- Отпечатки пальцев
- Bluetooth
- Одноразовый пароль
- Пароль



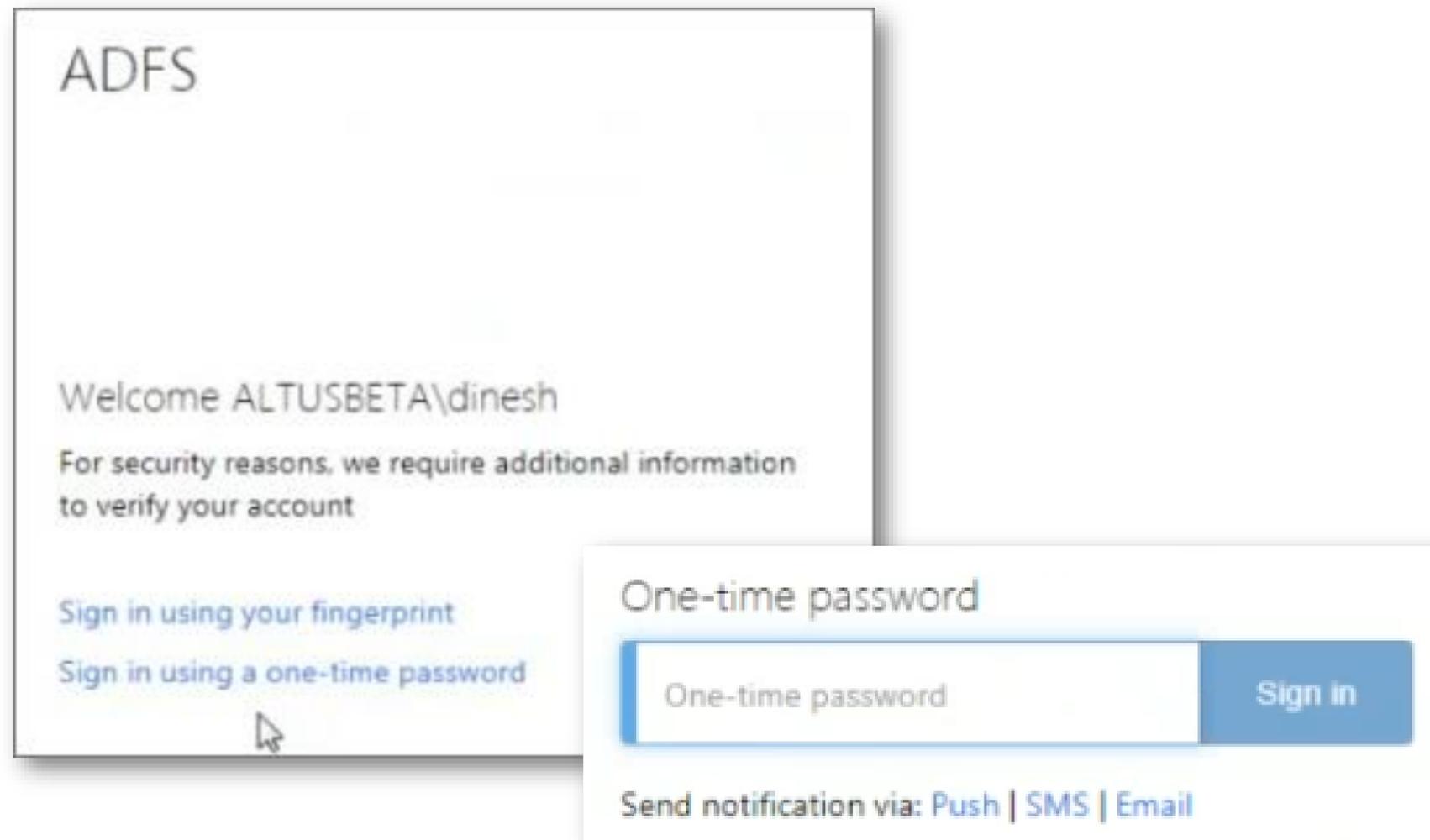
Политики сквозного доступа в приложения

Подтверждение сквозного доступа в приложения с помощью дополнительных факторов аутентификации

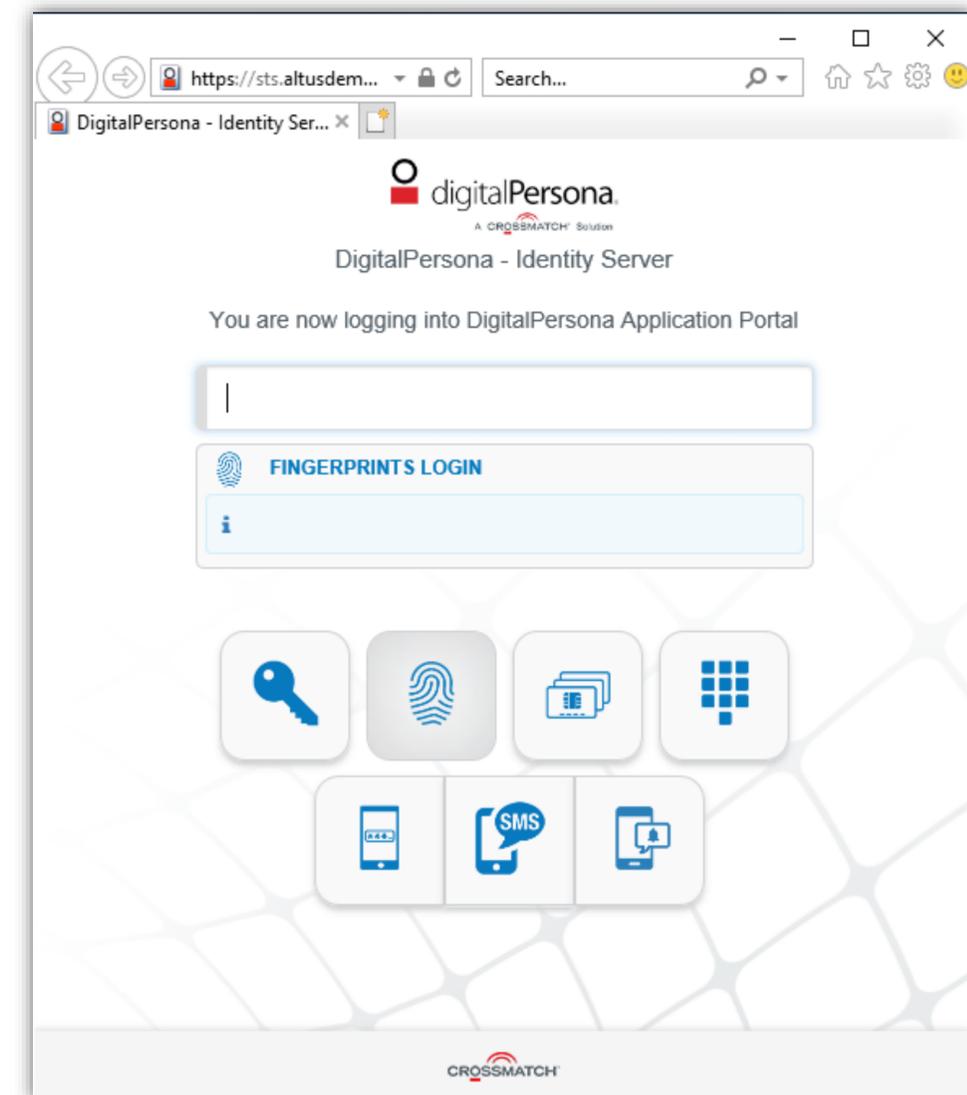


WEB-аутентификация

- DigitalPersona для ADFS
- Многофакторная аутентификация для MS OWA и других облачных сервисов

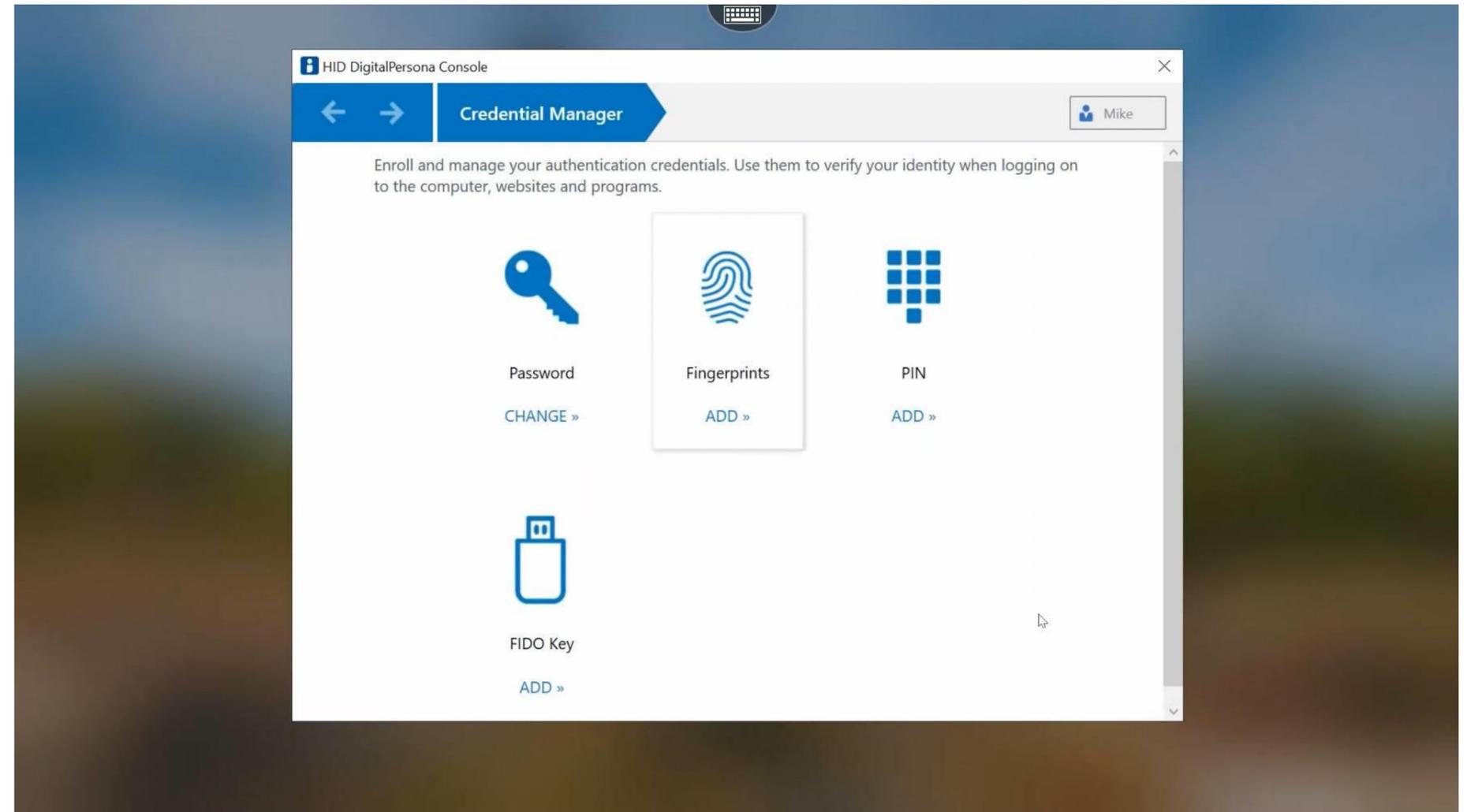


- Портал DigitalPersona IdP (облачный провайдер HID)



Регистрация учетных данных

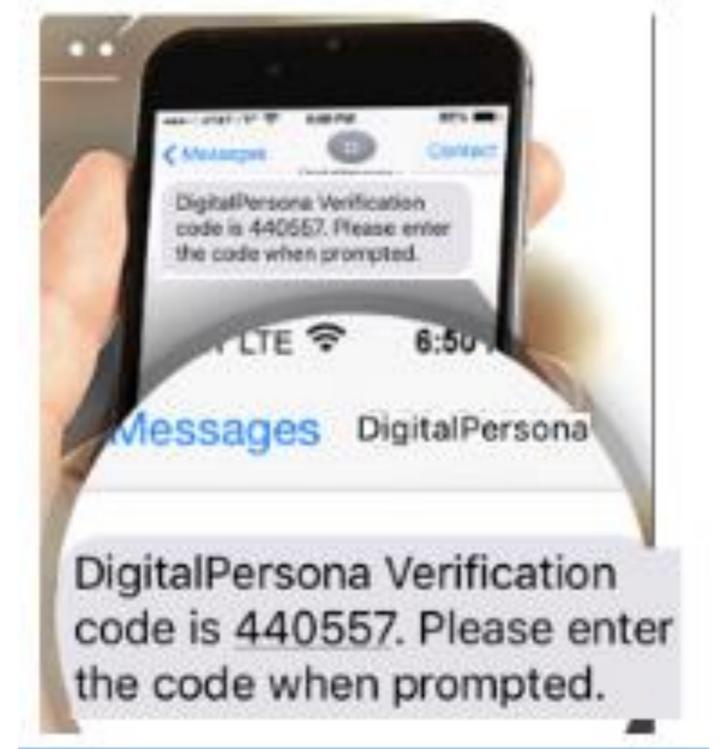
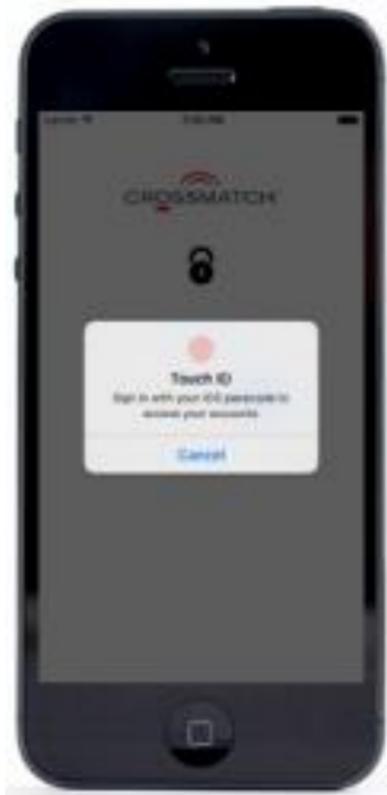
- Оператором или самостоятельно пользователем
- Через программный клиент либо веб-портал
- До входа в систему - на экране Windows Logon **NEW**



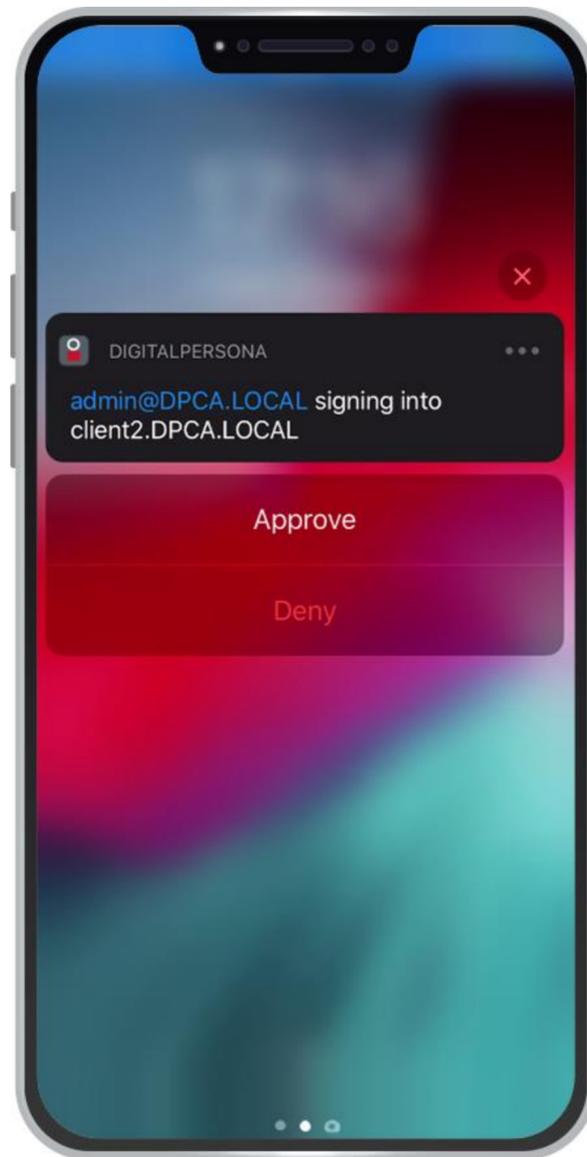
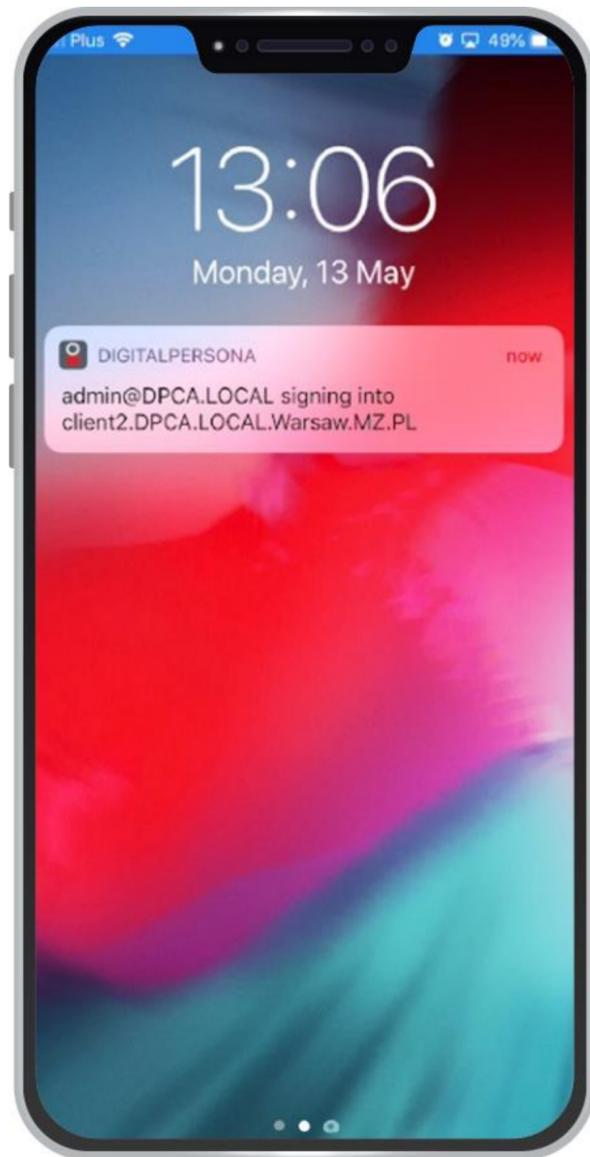
Одноразовые пароли (OTP)

OTP через аппаратные и софт-токены, Email и SMS*

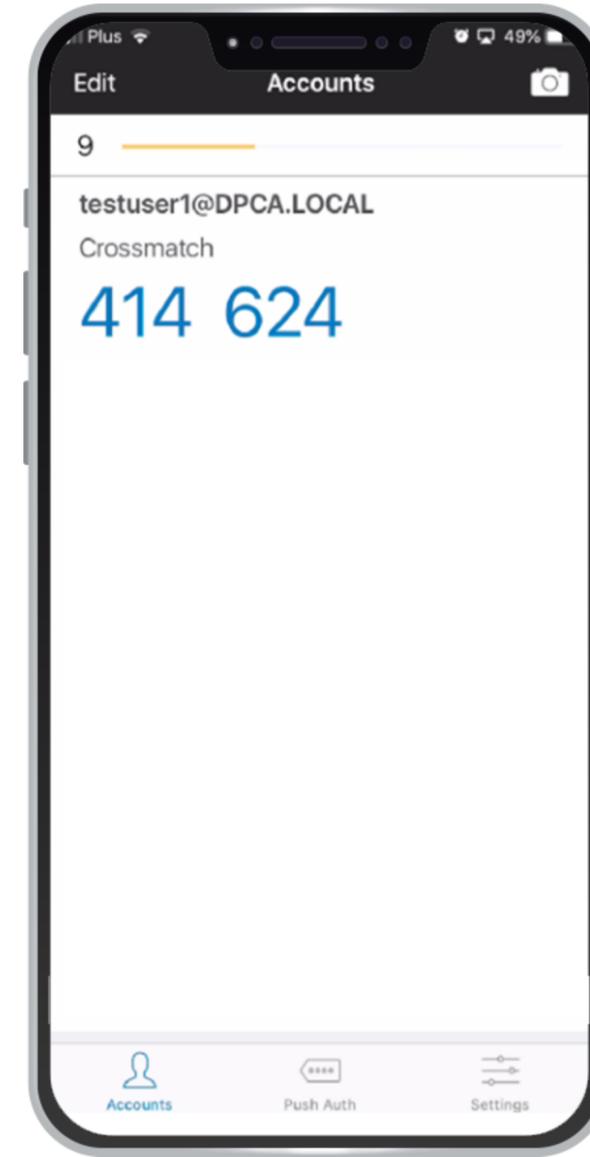
- Windows Logon
- Сквозная аутентификация в приложения (SSO)
- DP IdP для доступа к облачным сервисам (Office365 и др.)



Мобильное приложение (софт-токен)



PUSH

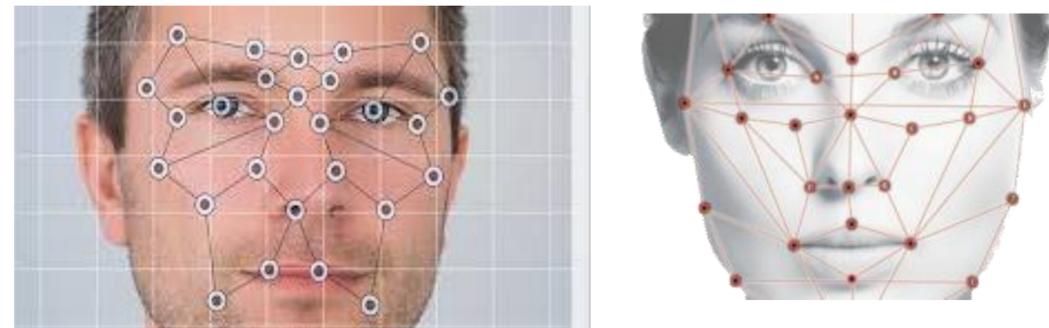


OTP

Продвинутая аутентификация

По лицу через обычные WEB-камеры

- Windows Logon
- Сквозная аутентификация (SSO)



Условия доступа (политики безопасности)

Windows Logon

- Время с прошлого входа
- Была перезагрузка, сон, гибернация?
- Сетевая идентификация (IWA)
- Удаленный доступ (RDP, VPN)
- Смена (новый) пользователя

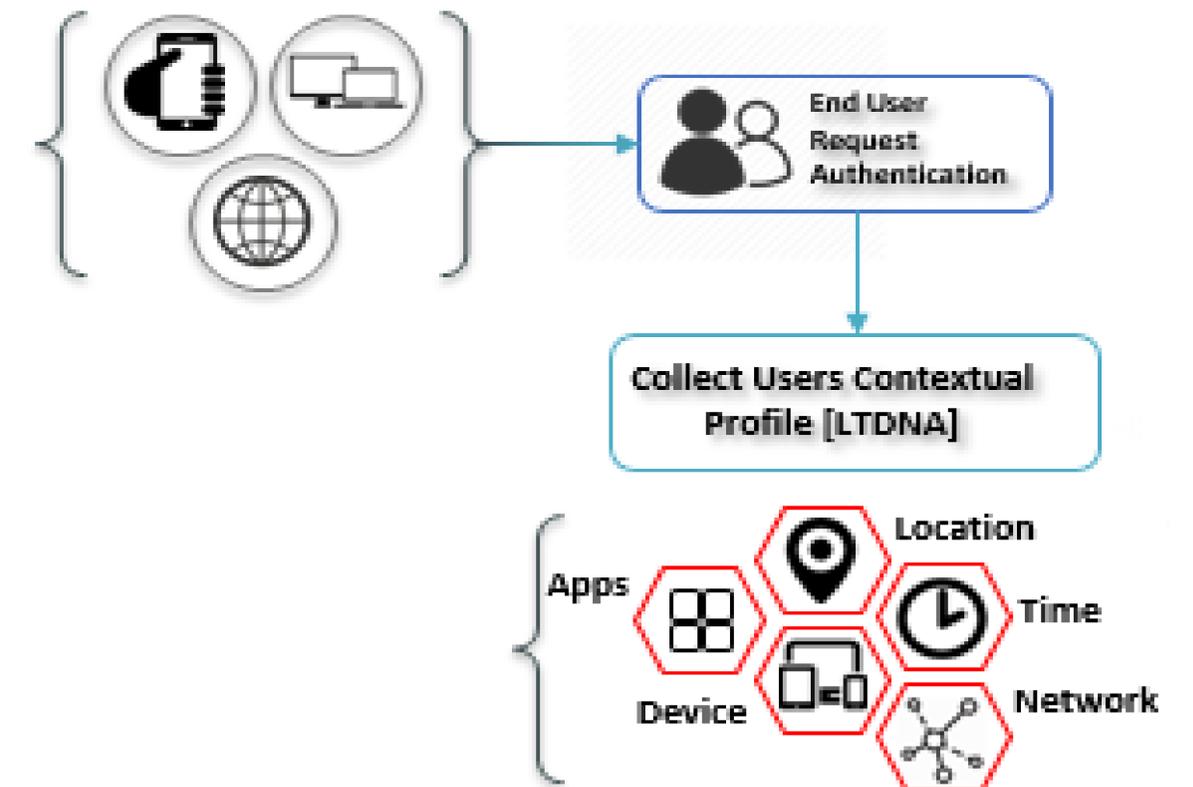
Облачный доступ (DP IdP)

- Геолокация (DP IdP)
- Скорость смены геопозиции

Поведенческий анализ

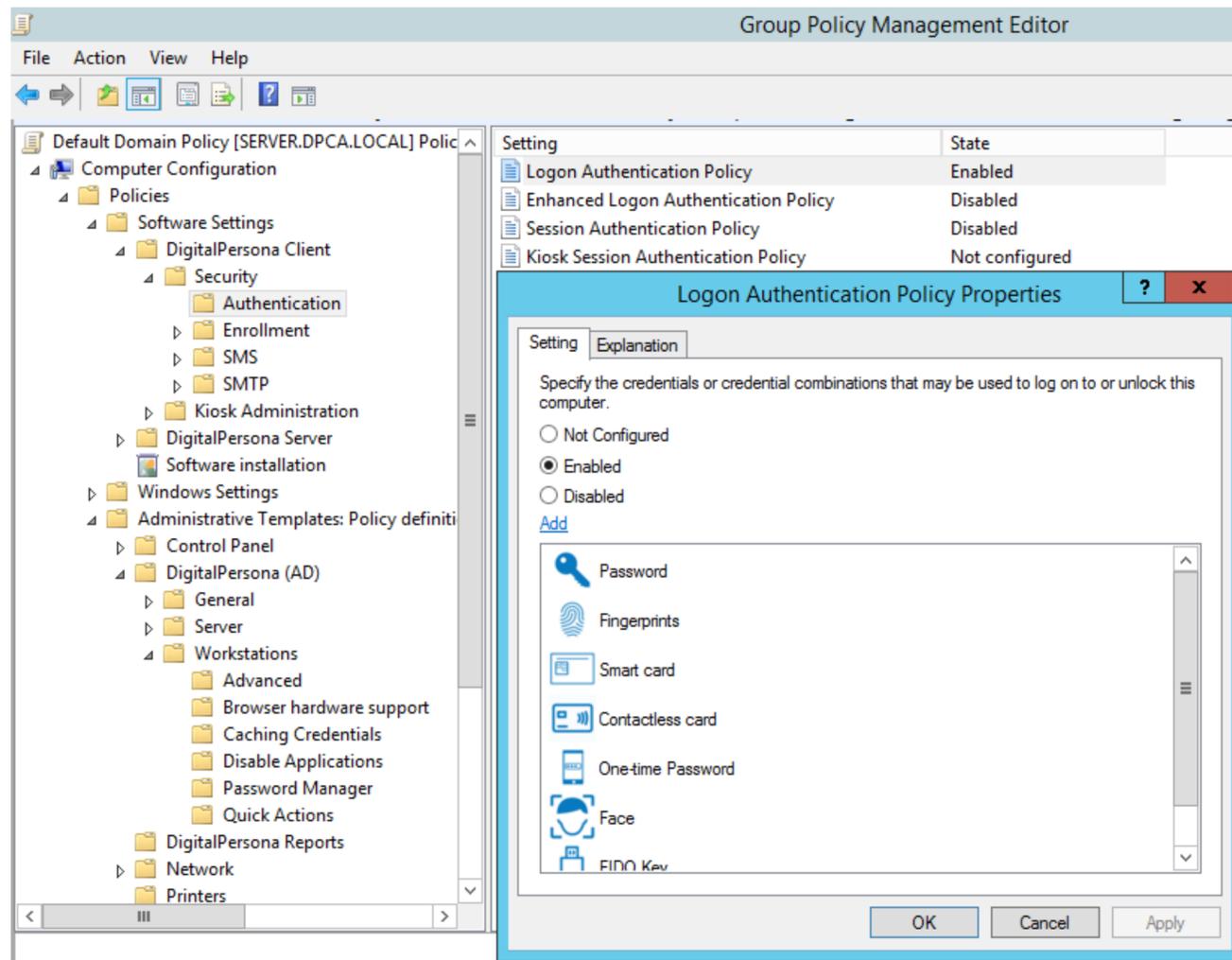
- «Почерк» пароля
- Свайп (Push)

Desktop, Web, Mobile Application

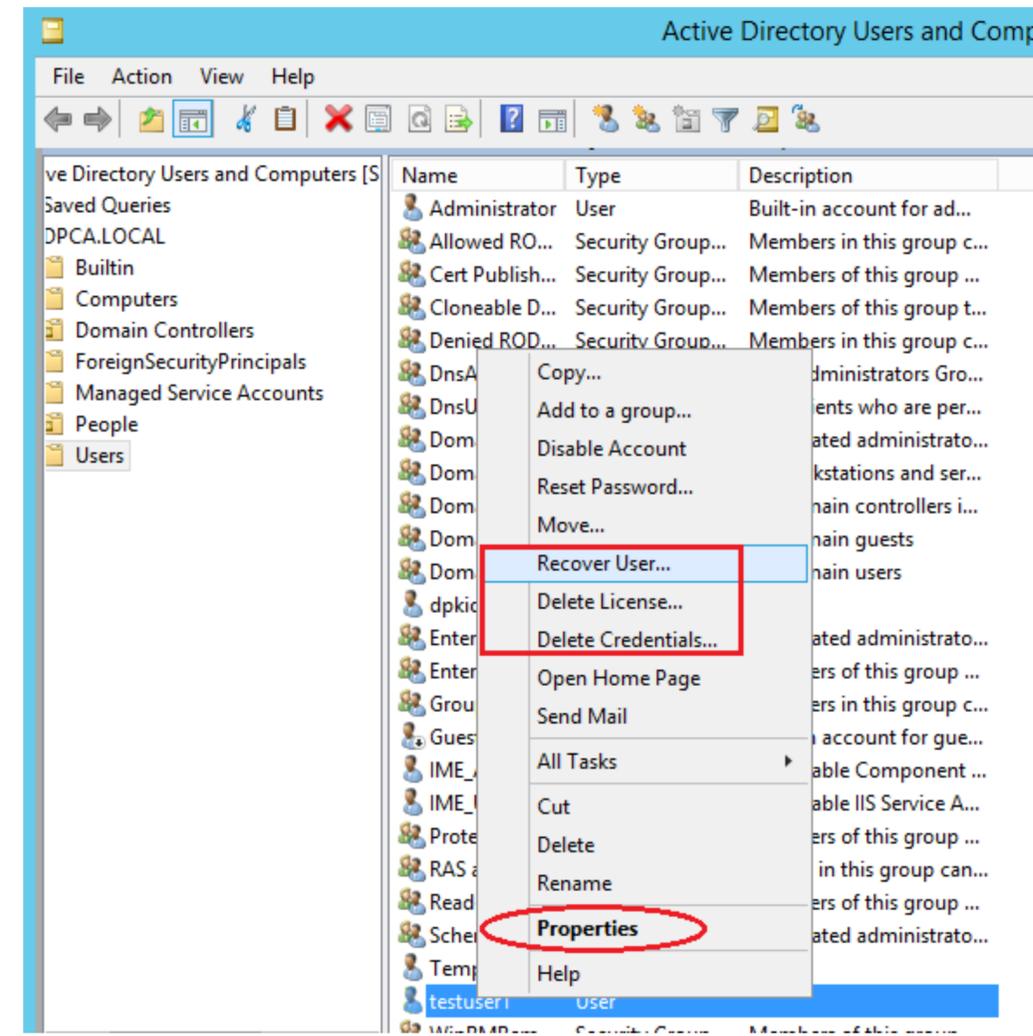


Администрирование

Через стандартные групповые политики (GPO)

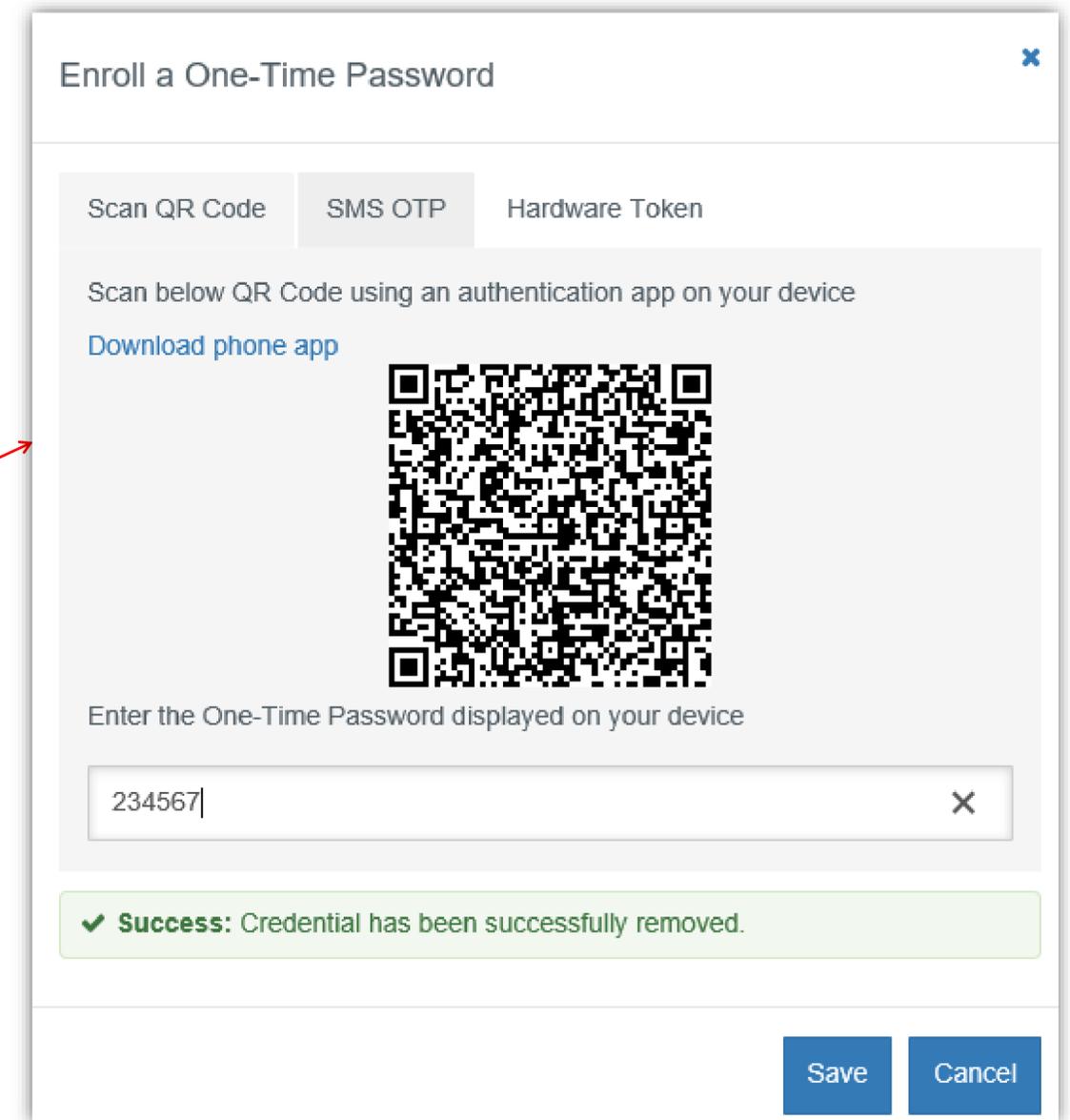
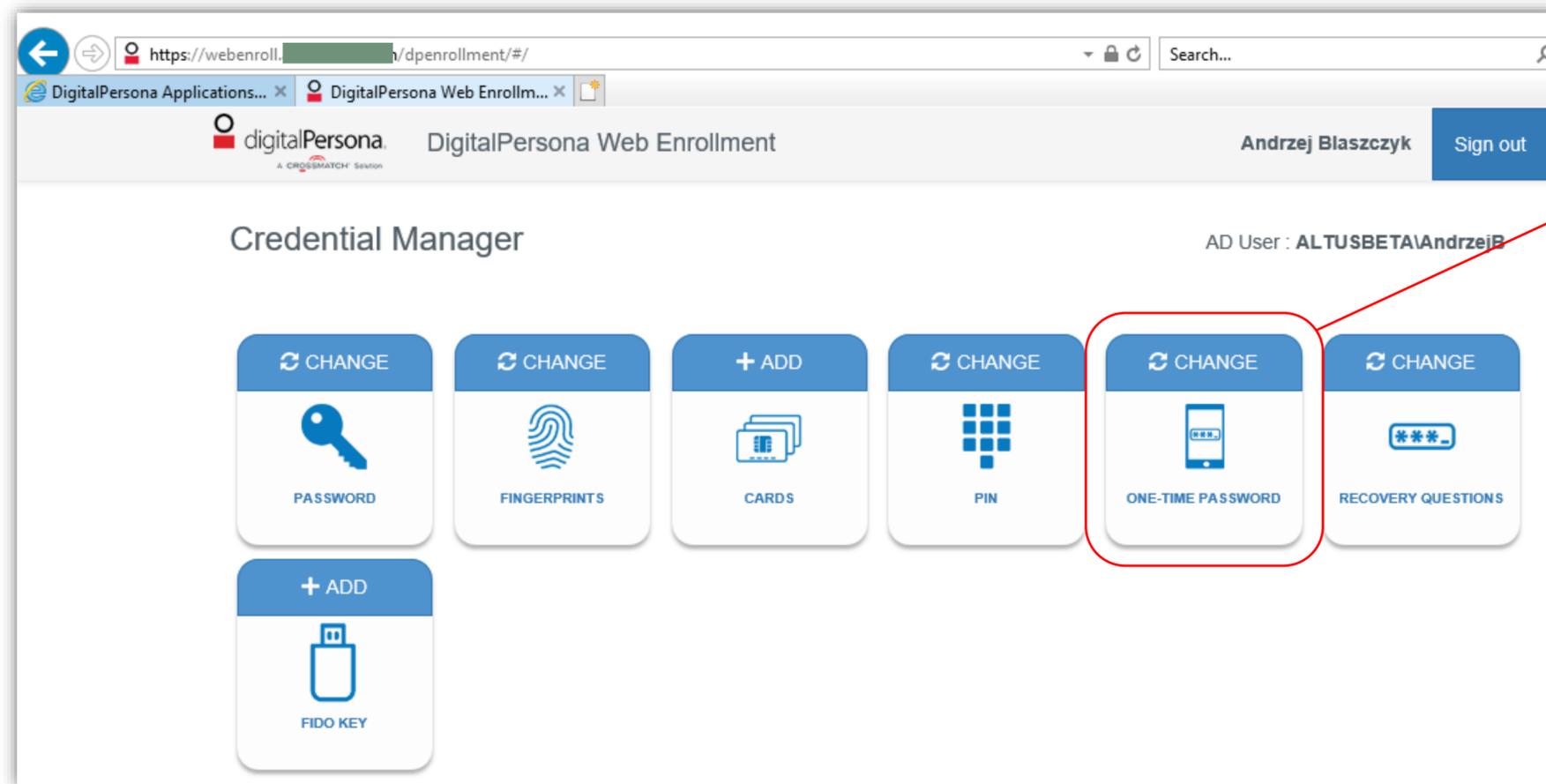


AD User & Computers

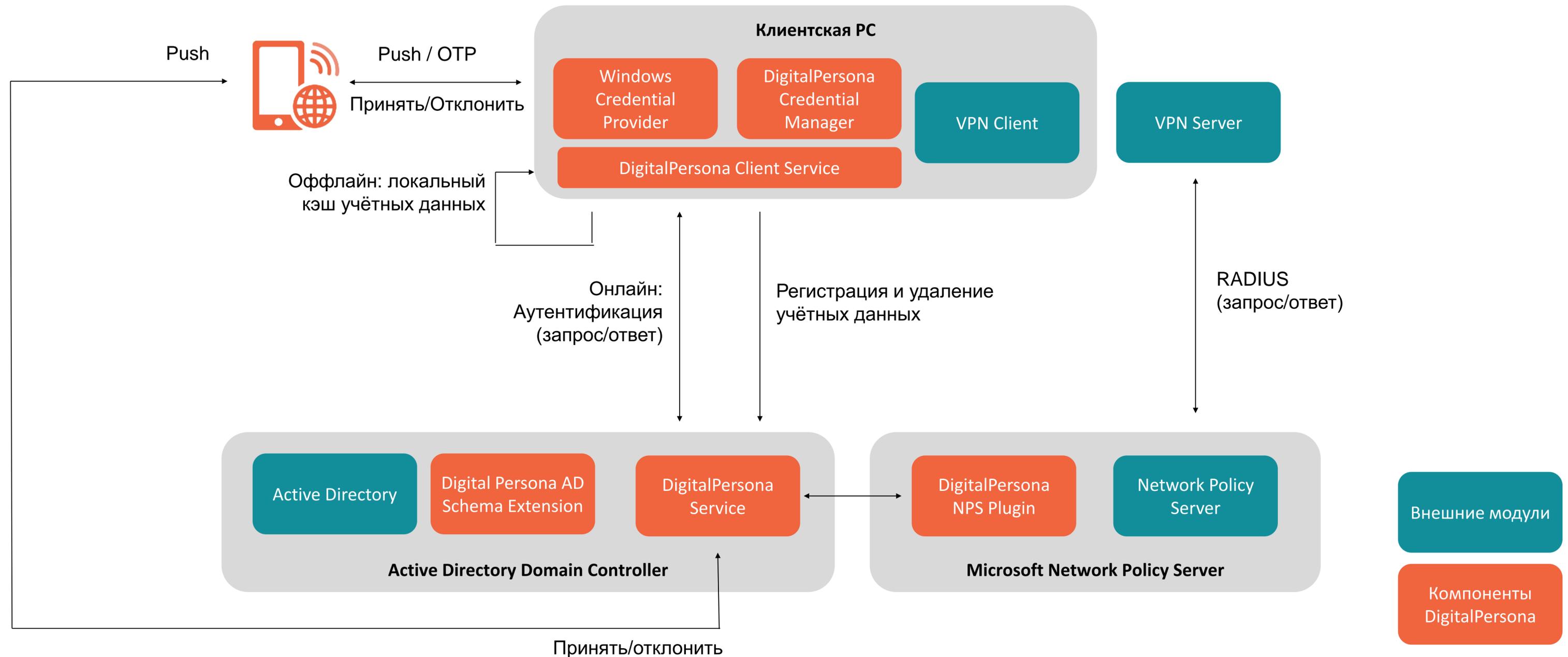


Web-сервисы управления

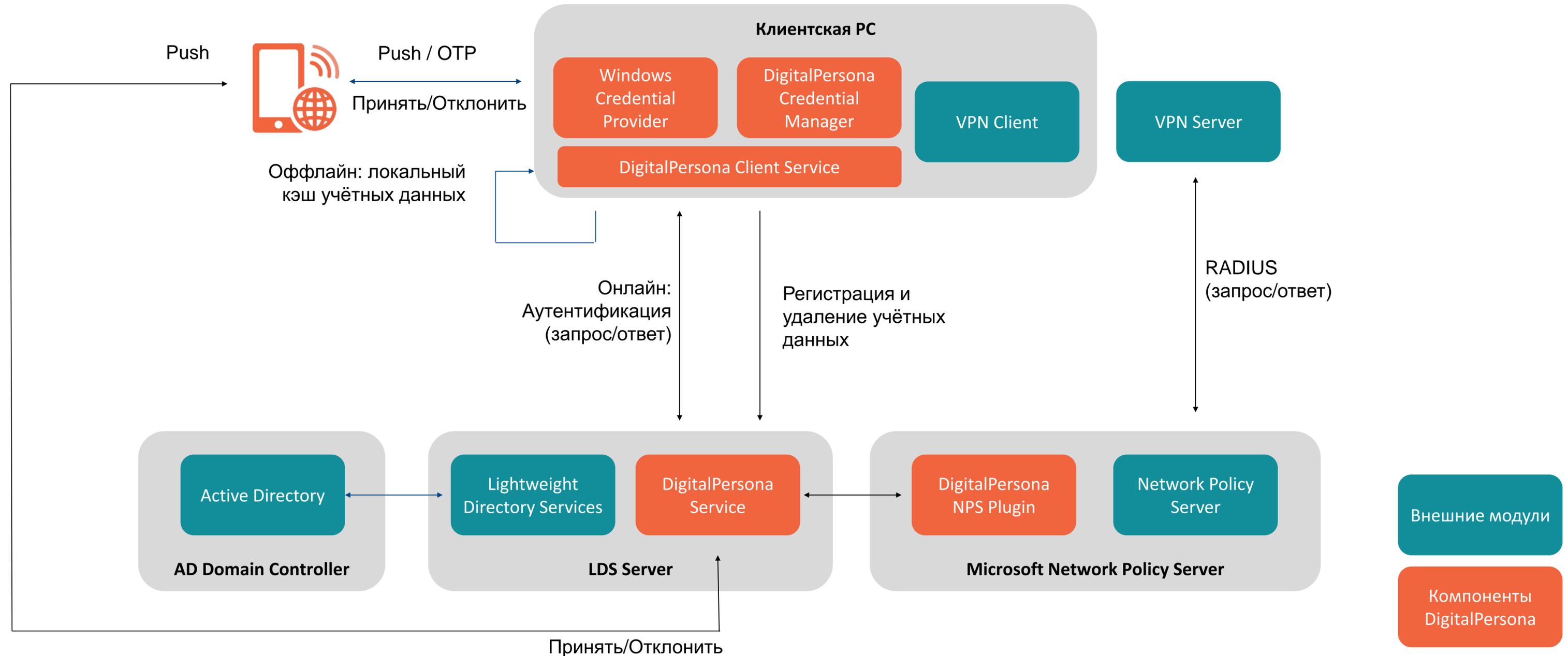
- Портал регистрации пользователей
- Портал администрирования



Интеграция с Active Directory



Интеграция с Active Directory LDS



Лицензирование

Бессрочные лицензии по количеству активных пользователей

- **Базовая лицензия Windows Logon**

Все методы (кроме лица) и условия продвинутой многофакторной аутентификация для входа на доменные машины (Windows Logon)

- **Лицензия Premium**

Включает базовую лицензию Windows Logon + сквозной доступ в корпоративные приложения и веб-ресурсы (SSO)

- **Дополнительная лицензия FaceID для аутентификации по лицу**

Надёжная аутентификация по лицу через встроенные или обычные веб-камеры

- **Дополнительная лицензия Behavior для поведенческого анализа**

Анализ ввода пароля при аутентификации

Преимущества HID DigitalPersona

- Все возможные методы продвинутой многофакторной аутентификации в одном решении
- Любые сочетания методов в зависимости от разнообразных условий доступа, включая поведенческий анализ
- Надёжная аутентификация по лицу через встроенную или обычную ВЕБ-камеру
- Различные сценарии регистрации учётных данных – самим пользователем или оператором
- Регистрация учетных данных до входа в систему (на экране Windows Logon)
- Сквозная аутентификация в приложения и веб-ресурсы (SSO)
- Поддержка общих рабочих станций (режим «киоска»)
- Развёртывание в архитектуре компании или облачный сервис
- Установка и настройка в доменной инфраструктуре за несколько простых шагов
- Не требуется выделенный сервер в базовой конфигурации
- Администрирование через стандартные групповые политики или ВЕБ-портал управления
- Бессрочные лицензии только по числу пользователей

Спасибо за внимание!

Михаил Ашарин

 AsharinM@terralink.ru

 +7 (495) 721-1721, доб. 233



www.terralink.ru