



Проект развития корпоративной PKI-инфраструктуры, соответствующей методологии Zero Trust Architecture

Соколов Егор Олегович, Gazprom International

Сессия 5 «PKI и ЭП в международной цифровой повестке»

17.09.2020, г. Санкт-Петербург

Общие положения методологии Zero Trust Architecture (ZTA)

- ZTA внедряют везде, это просто **товар** или хорошая **практика**?
- ZTA помогает **бороться** с уязвимостями в **прикладном** и **общесистемном** ПО?
- ZTA позволяет **контролировать подрядчиков**, предоставляющих сервисы?
- ZTA позволяет решить большую проблему – **безопасность персонала**?

Принципы Zero Trust Architecture (ZTA)

- Модель Zero Trust, как и расширенная модель – Zero Trust eXtended (ZTX), является реализацией **принципа «Доверяй, но проверяй»**.
- Модель предполагает, что к действиям пользователя, находящегося **внутри** периметра корпоративной ИТ-инфраструктуры, **надо относиться так же подозрительно**, как и к действиям контрагентов, запрашивающих доступ **извне**.
- Модель включает:
 - ✓ оценивание контекста для пользователей (**context** в нотации ISO),
 - ✓ **выявление угроз** и **оценка рисков** (в нотации ISO, NIST, Cobit) для PKI-инфраструктуры в периметре Компаний Группы,
 - ✓ **верификацию УЦ** (CA) в периметре Компаний Группы,
 - ✓ **валидацию конечных устройств** с установленными СЗИ и СКЗИ,
 - ✓ **авторизацию доступа** к PKI-сервисам в периметре Компаний Группы,
 - ✓ **восстановление устойчивости** (Resilience)

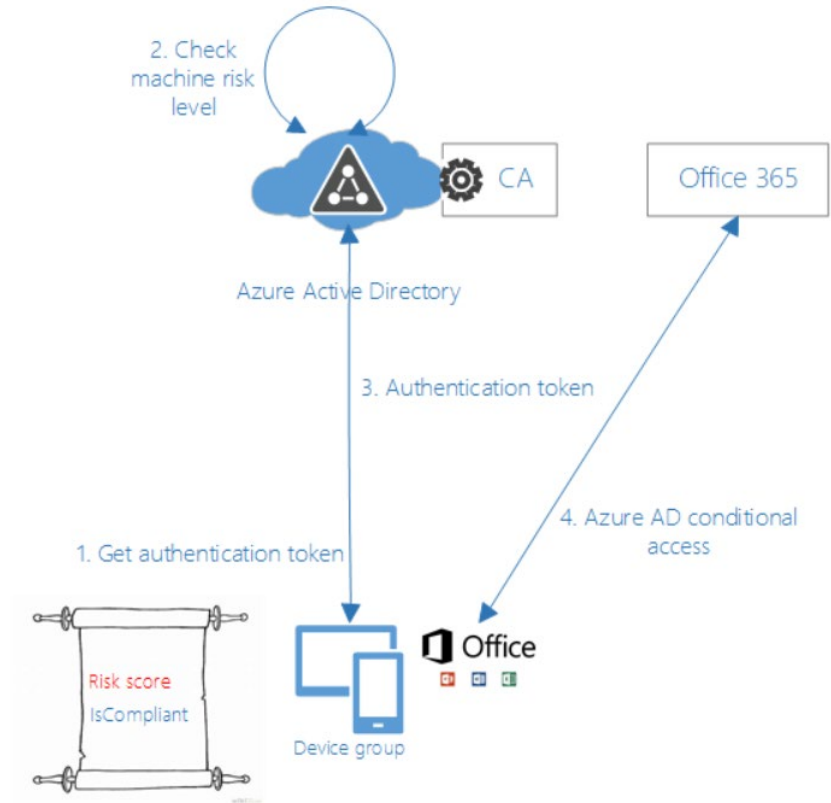
Примеры реализации Zero Trust Architecture (ZTA)

- **Building Zero Trust networks with Microsoft 365**

<https://www.microsoft.com/security/blog/2018/06/14/building-zero-trust-networks-with-microsoft-365/>

- **NIST Special Publication 800-207 «Zero Trust Architecture»**

<https://doi.org/10.6028/NIST.SP.800-207-draft2>



Основные требования к обеспечению безопасности корпоративной РКІ-инфраструктуры

- Соответствие применимым требованиям **различных юрисдикций** в части ЭП;
- Защита «**одной степени прочности**» для внутренних и/или внешних интерфейсов;
- Ориентация на **отечественные** СЗИ и СКЗИ для формирования ЭП и/или шифрования;
- Обеспечение **мгновенного** и в равной степени **безопасного** обмена документами по установленным и резервным каналам связи;
- **Разделение функций безопасности и администратора** в периметре Компаний Группы;
- Обеспечение **надежного** и безопасного **длительного архивного хранения документов**.

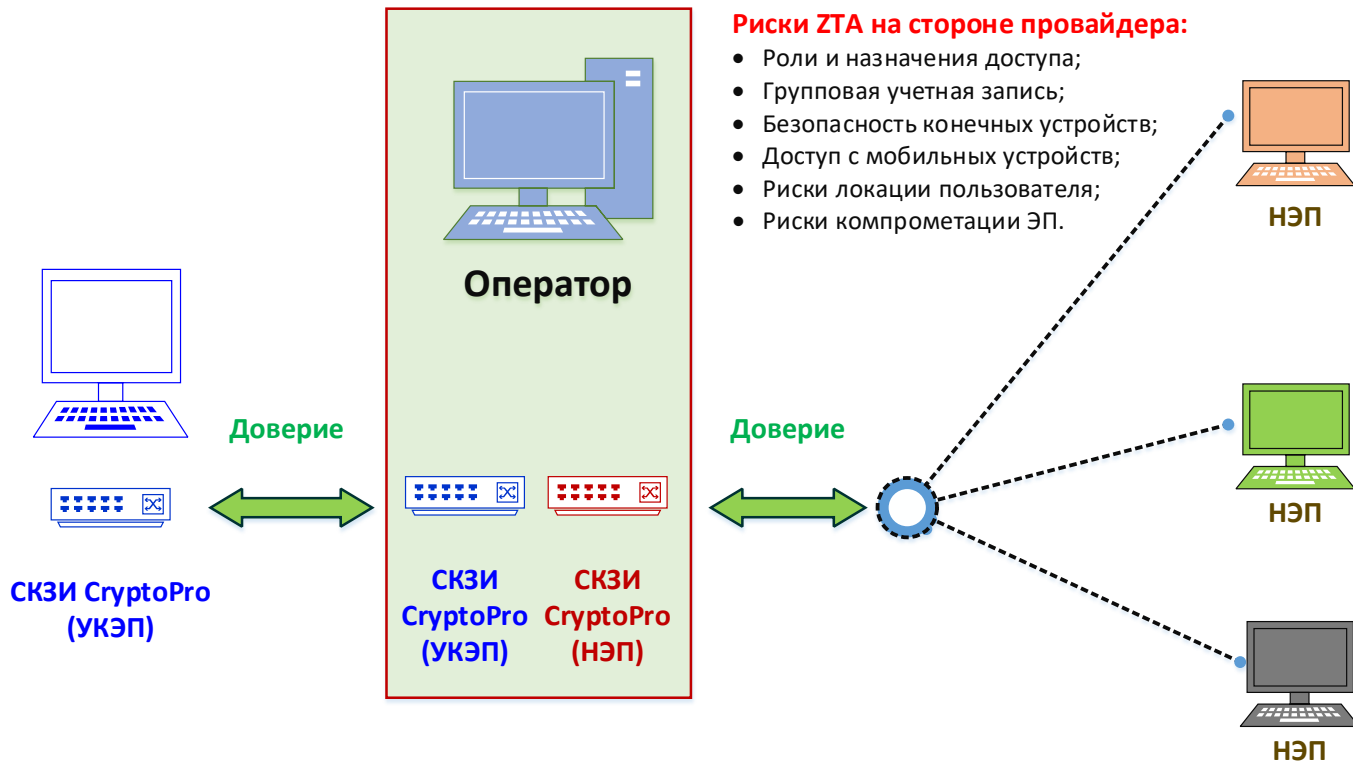
Реализация пилотного проекта для Компаний Группы

- Формирование **междисциплинарной** рабочей группы в периметре Компаний Группы.
- Определение **приоритетных бизнес-процессов** для цифровой трансформации.
- Формирование перечня **цифровых сервисов**, доступных на объектах Компании Группы.
- Определение **состава** и технических **характеристик** СЗИ и СКЗИ для формирования ЭП и/или шифрования в периметре Компаний Группы с учетом методологии ZTA.
- Заключение необходимых **сервисных контрактов** с учетом методологии ZTA

Описание концепции технического решения для пилотного проекта

Контрагенты (РФ)

Контрагенты (В мире)



Преимущества проекта развития корпоративной РКІ-инфраструктуры

Основные преимущества проекта развития корпоративной РКІ-инфраструктуры:

- интеграция современных технологий ЭДО и средств защиты – СЗИ и СКЗИ для шифрования и/или удостоверения ЭП внутренних и/или внешних документов, обращающихся во всех юрисдикциях в периметре Компаний Группы.
- Методология Zero Trust Architecture (ZTA) позволяет проектировать и управлять полным жизненным циклом цифровых сервисов исходя из равных предположений о доверенных соединениях внутри и извне по отношению к корпоративной ИТ-структуре.

В перспективе планируется завершить пилотирование и развернуть полномасштабный действующий рабочий проект в масштабе всех Компаний Группы, полностью соответствующих применимым национальным и международным нормативным требованиям в области информационной безопасности.

A decorative graphic on the left side of the slide, consisting of several overlapping, semi-transparent blue chevron shapes pointing to the right, layered over a background image of an offshore oil rig at sea.

Благодарю за внимание!

Соколов Егор Олегович, Gazprom International
E.Sokolov@gazprom-international.com