CLEARWAY INTEGRATION

Особенности управления сертификатами в контейнерных средах

Лучник Анна

План

- Где и зачем нужны сертификаты [в контейнерных средах]?
- TLS или mTLS?
- Рекомендации вендоров или требования законодательства?
- Что может пойти не так?
- В чем сложности реализации?
- Наш опыт после 35 000 000 выпущенных сертификатов
- Чек лист с рекомендациями

TLS = { Handshake Protocol + Record Protocol + Alert Protocol }

HTTPS = HTTP + TLS

Что обеспечивает использование TLS и mTLS?

Конфиденциальность

Целостность

Аутентификацию

Фильтрацию трафика

Разделение ролей

Zero Trust

Для чего из этого нужны сертификаты?

Конфиденциальность

Целостность

Аутентификация

Фильтрация трафика

Разделение ролей

Zero Trust

Для чего из этого нужны сертификаты?

Конфиденциальность

Целостность

Аутентификация

~~Авторизация~~

Фильтрация трафика

Разделение ролей

Zero Trust

S T R I D E






SPOOFING

In the context of information security, and especially network security, a spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.

TAMPERING

Tampering can refer to many forms of sabotage but the term is often used to mean intentional modification of products in a way that would make them harmful to the consumer.

REPUDIATION

In digital security, non-repudiation means a service that provides proof of the integrity and origin of data, or an authentication that can be said to be genuine with high confidence.

INFO DISCLOSURE

Information disclosure is the unwanted dissemination of data, technology, or privacy. legal and political issues surrounding them. It is a violation of data privacy[2] or data protection. The challenge of data privacy is to use data

DENIAL OF SERVICE

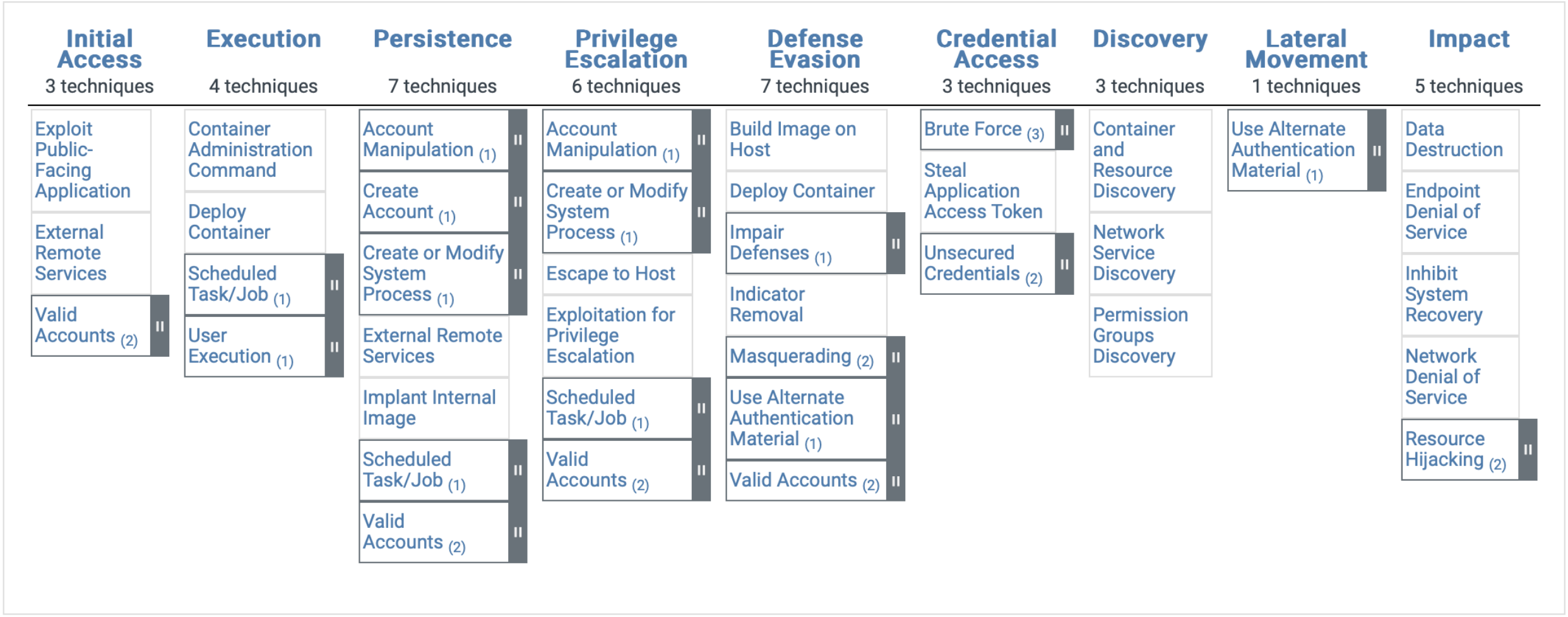
A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the

ELEVATION OF PRIVLEGE

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

https://developer.ibm.com/articles/threat-modeling-microservices-openshift-4/

MITRE ATT&CK for Containers Matrix



https://attack.mitre.org/matrices/enterprise/containers/

Рекомендации по использованию mTLS

Рекомендации по использованию mTLS - Kubernetes

«**TLS should be enabled for every component** that supports it to prevent traffic sniffing, verify the identity of the server, and (for mutual TLS) verify the identity of the client.»

https://kubernetes.io/blog/2018/07/18/11-ways-not-to-get-hacked/#1-tls-everywhere

Рекомендации по использованию mTLS - OWASP

«Since **securing microservices is hard**, there are many tools that address microservices security. However, the **service mesh is the most elegant solution** for addressing encryption of on-the-wire traffic within the network.»

Рекомендации по использованию mTLS - OWASP

«Since **securing microservices is hard**, there are many tools that address microservices security. However, the **service mesh is the most elegant solution** for addressing encryption of on-the-wire traffic within the network.

It **provides defense with mutual TLS (mTLS)** encryption of the traffic between your services, and the mesh can automatically encrypt and decrypt requests and responses, which removes that burden from application developers.»

https://cheatsheetseries.owasp.org/cheatsheets/Kubernetes_Security_Cheat_Sheet.html

Рекомендации по использованию mTLS – Istio и OpenShift

«**Istio** will automatically encrypt traffic using Mutual TLS whenever possible. However, proxies are configured in **permissive mode by default,** meaning they will accept both mutual TLS and plaintext traffic.

While this is required for incremental adoption or allowing traffic from clients without an Istio sidecar, it also weakens the security stance. It is **recommended to migrate to strict mode when possible**, to enforce that mutual TLS is used.»

https://istio.io/latest/docs/ops/best-practices/security/#mutual-tls

«By default, **mTLS** in **OpenShift** Service Mesh is **enabled and set to permissive mode**, where the sidecars in Service Mesh accept both plain-text traffic and connections encrypted using mTLS.

Enabling mTLS across the mesh at the control plane level **secures all the traffic in the service mesh without rewriting hosted applications and workloads**...»

https://www.redhat.com/en/blog/service-mesh-mtls

Рекомендации по использованию mTLS – Istio и OpenShift

По умолчанию **permissive mode**

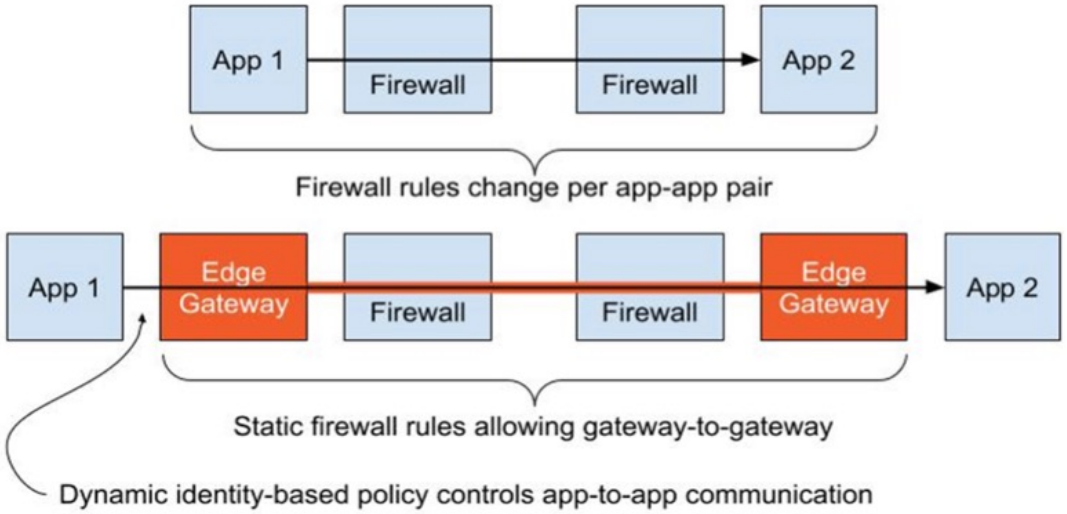
Рекомендуется переводить на **strict mode**

ГОСТ Р 57580.1-2017

ЗВС.1 Применение сетевых протоколов, обеспечивающих **защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии двухсторонней аутентификации** при осуществлении логического доступа с использованием телекоммуникационных каналов и (или) линий связи, не контролируемых финансовой организацией

NIST Special Publications

- SP 800-207A
  A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments
- SP 800-204A
  Building Secure Microservices-Based Applications Using Service Mesh Architecture
- SP 800-204B
  Attribute-Based Access Control for Microservices-Based Applications Using a Service Mesh



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.pdf

Что может пойти не так?

Просроченные сертификаты

Проверка отзыва сертификатов

Высокая нагрузка

Мониторинг

Что может пойти не так?

Просроченные сертификаты

Пример 1

8 апреля 2023 года в работе SpaceX Starlink произошёл глобальный сбой из-за просроченных сертификатов наземных станций. Пользователи по всему миру более чем на два часа остались без доступа к спутниковому интернету, так как их абонентские устройства не получали сигналы от наземных станций Starlink

SpaceX Starlink outage caused by expired ground station certificates

Пример 2

31 мая 2022 года пользователи платформы Spotify более восьми часов не могли получить доступ к своим любимым подкастам. Сбои в работе системы возникли из-за того, что компания не смогла вовремя обновить сертификат безопасности Megaphone (одного из сервисов подкастов Spotify).

Spotify's failure to renew security certificate causes massive podcast outage

Что может пойти не так?

Проверка отзыва сертификатов

Проверка CRL и OCSP

Сроки действия сертификатов

Эфемерные сертификаты и их контроль

Что может пойти не так?

Масштабирование и перезапуск кластера

ЦУГИ в цифрах

ВЫПУЩЕНО СЕРТИФИКАТОВ

>15 000 000

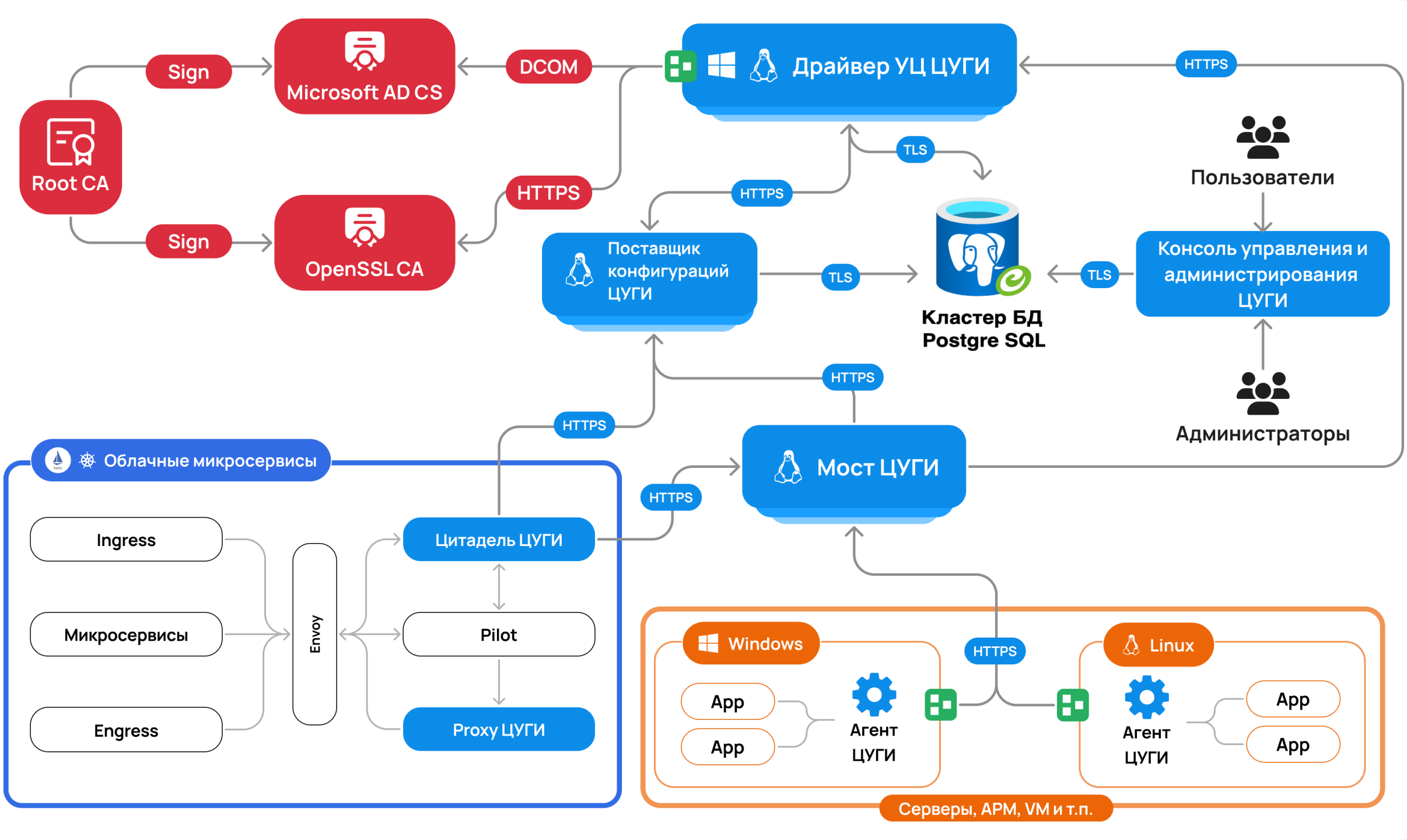
Для тестовых сред

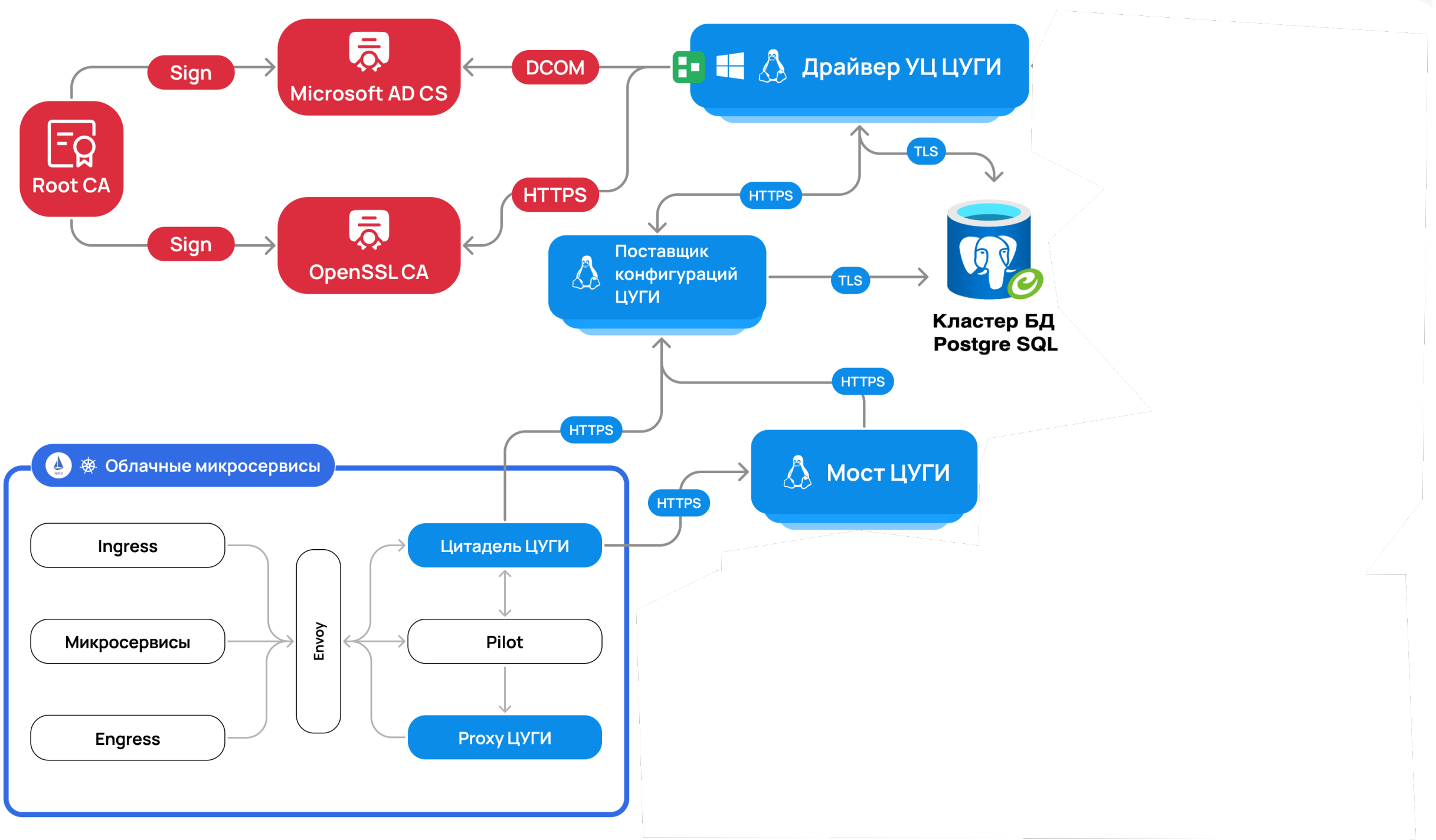
>1 000 000

Для сред разработки

>6 000 000

Для промышленной среды


Sign
Microsoft AD CS
DCOM
Драйвер УЦ ЦУГИ
HTTPS
Root CA
Sign
OpenSSL CA
HTTPS
TLS
HTTPS
Пользователи
Поставщик конфигураций ЦУГИ
TLS
Кластер БД Postgre SQL
TLS
Консоль управления и администрирования ЦУГИ
HTTPS
Администраторы
HTTPS
Мост ЦУГИ
HTTPS
Облачные микросервисы
Ingress
Микросервисы
Engress
Envoy
Цитадель ЦУГИ
Pilot
Proxy ЦУГИ
HTTPS
Windows
App
App
Агент ЦУГИ
HTTPS
Linux
Агент ЦУГИ
App
App
Серверы, АРМ, VM и т.п.


Sign
Microsoft AD CS
DCOM
Драйвер УЦ ЦУГИ
Root CA
Sign
OpenSSL CA
HTTPS
TLS
HTTPS
Поставщик конфигураций ЦУГИ
TLS
Кластер БД Postgre SQL
HTTPS
HTTPS
Облачные микросервисы
HTTPS
Мост ЦУГИ
Ingress
Цитадель ЦУГИ
Микросервисы
Envoy
Pilot
Engress
Proxy ЦУГИ

Что может пойти не так?

Мониторинг

Мониторинг доступности компонентов PKI и аудит доступа к ключам

- Все внешние и внутренние компоненты PKI
- Синтетический мониторинг PKI
- Контроль отзыва сертификатов
- Возможность мониторинга инфраструктуры PKI ГОСТ
- Контроль как срока действия ключа, так и срока действия сертификата
- Самодиагностика системы мониторинга
- Мониторинг сертификатов и шаблонов с потенциально опасными сочетаниями атрибутов

Чек лист

- mTLS везде
- Внешний УЦ
- Отказоустойчивость и балансировка нагрузки
- Срок жизни сертификата несколько дней
- Логирование и активный мониторинг

CLEARWAY INTEGRATION

Спасибо за внимание!

Для связи с нами

Clearwayintegration.net