

Функциональные и технические характеристики

Avanpost SA

ОГЛАВЛЕНИЕ

АННОТАЦИЯ	3
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	4
СТРУКТУРА И АРХИТЕКТУРА	6
Общие сведения	6
Структура Avanpost SA	6
ТЕХНОЛОГИЧЕСКАЯ ПЛАТФОРМА	8
Обзор технологической платформы	8
ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ	9
Обзор функциональности	9
ИНТЕГРАЦИОННЫЕ ИНТЕРФЕЙСЫ И СЕРВИСЫ	10
Обзор интеграционных возможностей	10
КОНТАКТЫ	12
СПИСОК РИСУНКОВ	13
СПИСОК ТАБЛИЦ	14

АННОТАЦИЯ

Avanpost CA — это центр сертификации, обеспечивающий полный набор функций для управления цифровыми сертификатами в соответствии с принципами PKI и стандартом X.509.

Настоящий документ описывает функциональные и технические характеристики системы Avanpost CA. В документе рассмотрены архитектура, технологическая платформа, основные функциональные возможности по управлению жизненным циклом сертификатов, а также предоставляемые системой интеграционные интерфейсы.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Таблица 1 – Термины

Термин	Определение
ACL (Access Control List)	Список управления доступом. Набор правил, определяющий, какие пользователи или системы имеют права на выполнение определенных операций с объектом (например, с шаблоном сертификата). Права могут включать: чтение (read), запрос (request), изменение (write), утверждение (approve), удаление (delete)
Avanpost CA (Avanpost Certification Authority)	Центр сертификации, разработанный компанией Avanpost
CA (Certification Authority)	Центр сертификации. Удостоверяющий центр, который выпускает, подписывает и отзывает сертификаты, являясь доверенной третьей стороной
CRL (Certificate Revocation List)	Список отозванных сертификатов. Список, содержащий серийные номера сертификатов, отозванных до истечения срока их действия. Используется для проверки валидности сертификата
Key usage	Основные операции, для которых может использоваться ключ, указанный в сертификате, например, DigitalSignature, KeyEncipherment, CertSign

OCSP (Online Certificate Status Protocol)	Протокол онлайн-проверки статуса сертификата
SCEP (Simple Certificate Enrollment Protocol)	Простой протокол регистрации сертификатов

СТРУКТУРА И АРХИТЕКТУРА

ОБЩИЕ СВЕДЕНИЯ

Avanpost CA может применяться в инфраструктурах для решения основных задач:

- Реализация механизмов доверия и цепочек PKI как в открытых, так и в корпоративных сетях;
- Обеспечение работы PKINIT для Kerberos;
- Поддержка современных систем идентификации и аутентификации на базе 802.1X;
- Взаимное подтверждение подлинности цифровых сервисов в современных инфраструктурах (SSL/TLS, mTLS);
- Защита электронной почты (S/MIME).

СТРУКТУРА AVANPOST CA

С физической точки зрения Avanpost CA состоит из следующих компонентов:

- Приложение CA;
- База данных CA.

С логической точки зрения Avanpost CA состоит из следующих компонентов:

- Основной сервис (ядро);
- Сервис выпуска сертификатов;
- Сервис валидации сертификатов;
- Интерфейсы стандартных интеграций;
- Интерфейс администрирования;
- Сервисы обеспечения безопасности и мониторинга.

На рисунке ниже схематично отражена концептуальная архитектура Avanpost CA:

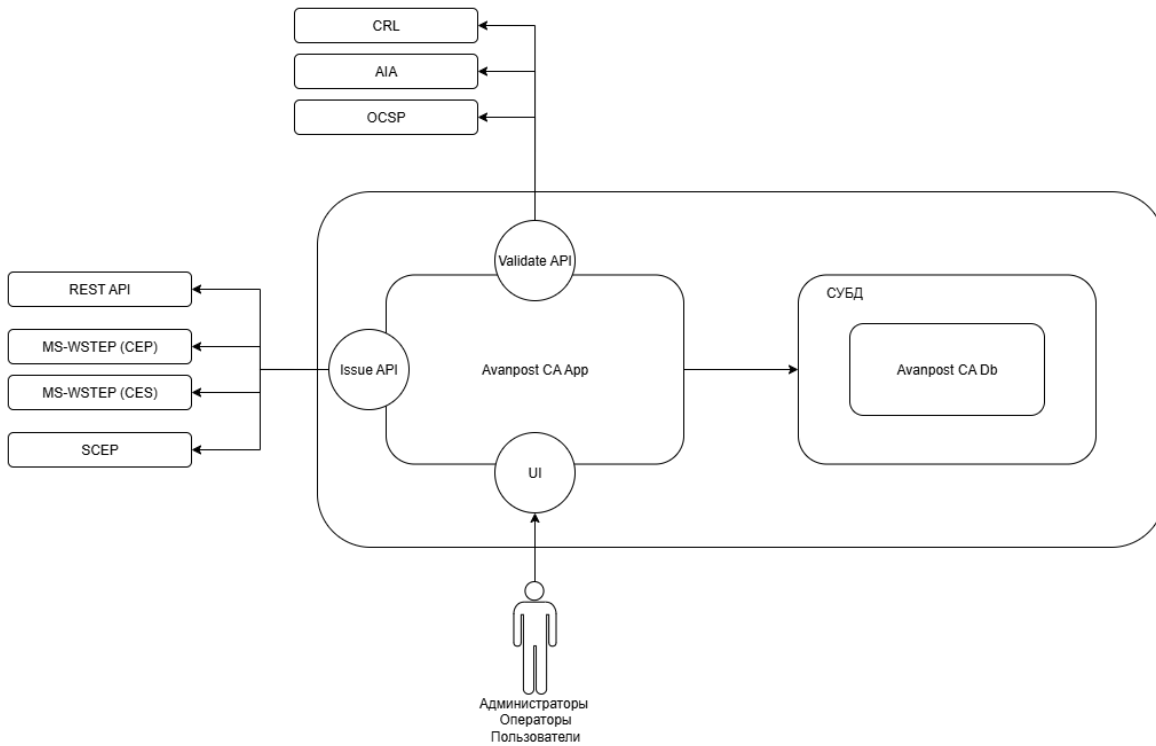


Рисунок 1 — Концептуальная архитектура Avanpost CA

ТЕХНОЛОГИЧЕСКАЯ ПЛАТФОРМА**ОБЗОР ТЕХНОЛОГИЧЕСКОЙ ПЛАТФОРМЫ**

Avanpost SA разработан на языке программирования Go (golang).

Таблица 2 — Описание технологической платформы

Компонент	Поддерживаемые решения
Операционная система	<ul style="list-style-type: none">• Astra Linux SE• Альт Сервер• RedOS• CentOS Stream / RHEL• Ubuntu• прочие linux-дистрибутивы
СУБД	<ul style="list-style-type: none">• PostgreSQL• Postgres Pro• Tantor• прочие версии postgres

ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ**ОБЗОР ФУНКЦИОНАЛЬНОСТИ**

Avanpost CA предоставляет полный набор функций для управления сертификатами. Основные возможности системы включают управление сертификатами, валидацию запросов и сертификатов, работу с шаблонами.

Таблица 3 — Основные функциональные возможности

Функциональный блок	Основные функции
Управление сертификатами	<ul style="list-style-type: none"> • Выпуск новых сертификатов; • Продление (перевыпуск) сертификатов; • Приостановка/возобновление действия сертификатов; • Отзыв сертификатов; • Публикация сертификатов; • Поддержка работы с запросами: одобрение / отклонение
Валидация запросов и сертификатов	<ul style="list-style-type: none"> • Проверка запроса на соответствие шаблону; • Создание и публикация CRL; • Поддержка протокола OCSP
Управление шаблонами	<ul style="list-style-type: none"> • Создание и редактирование шаблонов сертификатов; • Поддержка основных характеристик: длина ключа, срок действия, key usage; • Поддержка дополнительных характеристик: EKU; • Поддержка ACL для шаблонов; • Редактирование справочника EKU

ИНТЕГРАЦИОННЫЕ ИНТЕРФЕЙСЫ И СЕРВИСЫ**ОБЗОР ИНТЕГРАЦИОННЫХ ВОЗМОЖНОСТЕЙ**

Avanpost CA поддерживает стандартные протоколы и API для интеграции с различными системами.

Таблица 4 — Основные интеграционные возможности

Компонент	Описание
Avanpost Linux Enrollment Service	Набор сервисов и механизмов, обеспечивающих функции автоматического выпуска и обновления (autoenrollment) сертификатов для компьютеров и серверов под управлением ОС семейства Linux. Дополнительно поддерживает возможность интеграции со службой каталогов Avanpost DS и функции централизованного управления выпуском и обновлением сертификатов через доменные политики и разграничение доступа к шаблонам сертификатов по доменным группам безопасности
SCEP	Сервис для автоматизации выпуска сертификатов для компьютеров и устройств под управлением MacOS и iOS (через промежуточные MDM-системы: Jamf, AirWatch, MobileIron, MS Intune и т.д.), а также для сетевых устройств и оборудования Cisco
MS-WSTEP (CEP / CES)	Набор сервисов (CEP — сервис политик, CES — сервис выпуска сертификатов) для поддержки протокола Microsoft WS-Trust X.509v3 Token Enrollment Extensions. Позволяет полностью заместить функции автоматического выпуска и обновления (autoenrollment) сертификатов для компьютеров и серверов под управлением MS Windows

REST API CA	Полный набор методов для взаимодействия с СА в части выпуска и валидации сертификатов. Подходит как для интеграции с внешними системами (PKI, ITSM и т.д.), так и для использования в скриптах/сценариях автоматизации
-------------	--

КОНТАКТЫ

Avanpost CA разработан и поддерживается ООО «Аванпост».

Адрес: 129085, г. Москва, ул. Годовикова, д. 9, стр. 17

Телефон: +7 (495) 877 30 77

E-mail: info@avanpost.ru (общий), partners@avanpost.ru (партнерство), support@avanpost.ru (поддержка)

Сайт: <https://www.avanpost.ru/>

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

СПИСОК РИСУНКОВ

Рисунок 1 — Концептуальная архитектура Avanpost SA..... 7

СПИСОК ТАБЛИЦ

Таблица 1 – Термины.....	4
Таблица 2 — Описание технологической платформы.....	8
Таблица 3 — Основные функциональные возможности.....	9
Таблица 4 — Основные интеграционные возможности.....	10