SAFETECH

Импортоулучшение PKI внутри банка. И не только.

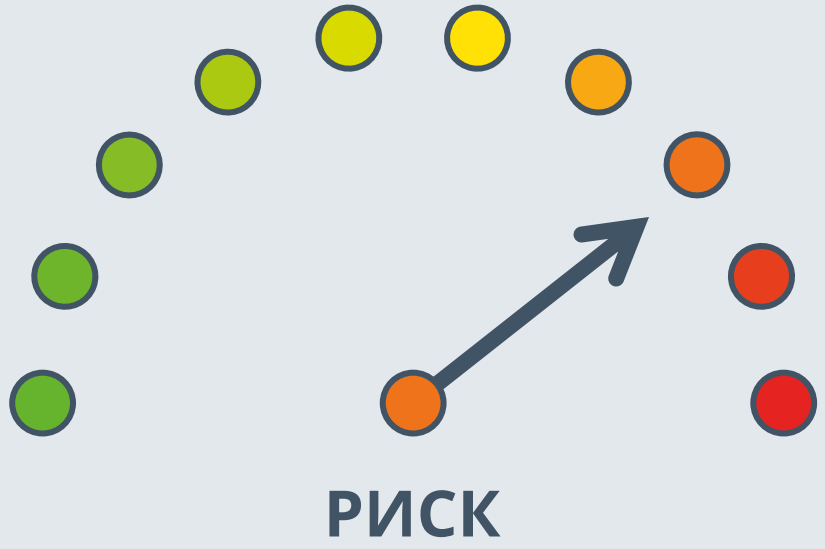
SAFETECH

Сертификаты везде в инфраструктуре любого размера

- VPN сервисы
- Аутентификация и шифрование данных
- Доменные сервисы (Active Directory)

- Email
- Взаимодействие оборудования
- Вход пользователей

- И многое другое



- Microsoft приостановил деятельность на территории России
- SSL.COM, LET'S ENCRYPT, ZERO SLL и многие другие приостановили деятельность на территории России
- Блокирующие санкции, особенно против финансового сектора
- Риск невыполнения требований законодательства в области импортозамещения

Указ Президента РФ от 30.03.2022 № 166

Указ Президента РФ от 01.05.2022 № 250

Указ Президента РФ от 07.05.2018 № 204

Приказ Министерства цифрового развития № 334 от 04.07.2017 и № 335 от 04.07.2018

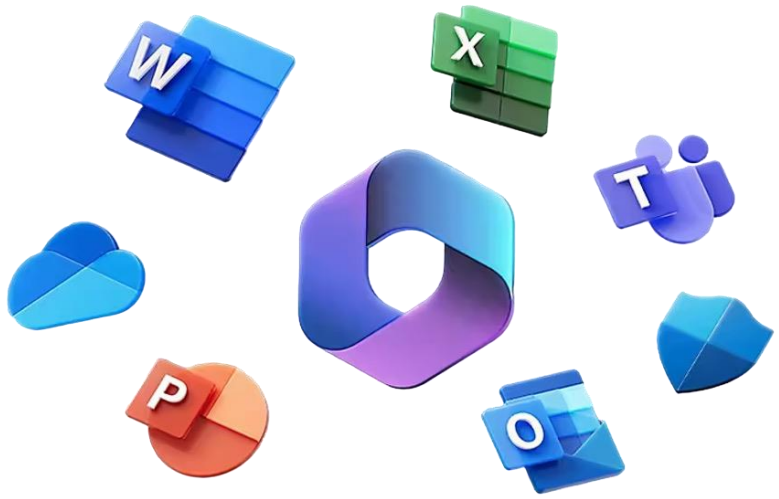
Постановление Правительства РФ №1236 от 16 ноября 2015 года

Самое время
что-то менять

SAFETECH

Есть «экосистемные» средства управления сертификатами (MS CA), но...

- Заточены на экосистему
- Очень упрощенное управление
- Нет поддержки различных протоколов



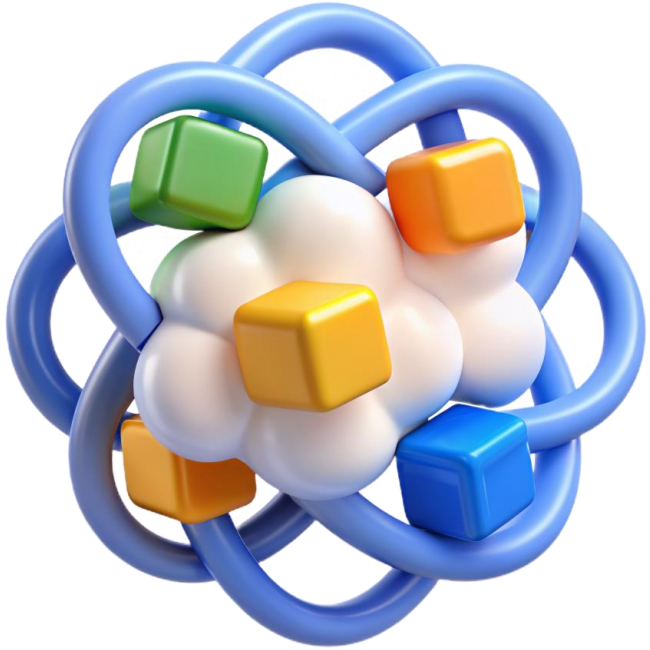
- Нет API
- Ограничения со стороны ОС
- «Бедный» UI

- И многое другое

SAFETECH

Очень фрагментированный и гетерогенный IT-ландшафт

- машины на MS Windows
- «Железо» от разных производителей
- iOS / Android - устройства



- Машины на MacOS / Linux
- Софт собственное разработки
- Софт от разных производителей

- И многое другое

С ЧЕМ СТОЛКНУЛИСЬ IT-шники БАНКОВ

ЗАДАЧИ

НАЛАДИТЬ УПРАВЛЕНИЕ СЕРТИФИКАТАМИ

РАЗВЕРНУТЬ CA

ПОВЫСИТЬ УРОВЕНЬ ИБ

ВРЕМЯ УЛУЧШАТЬ! ИМПОРТОУЛУЧШАТЬ!

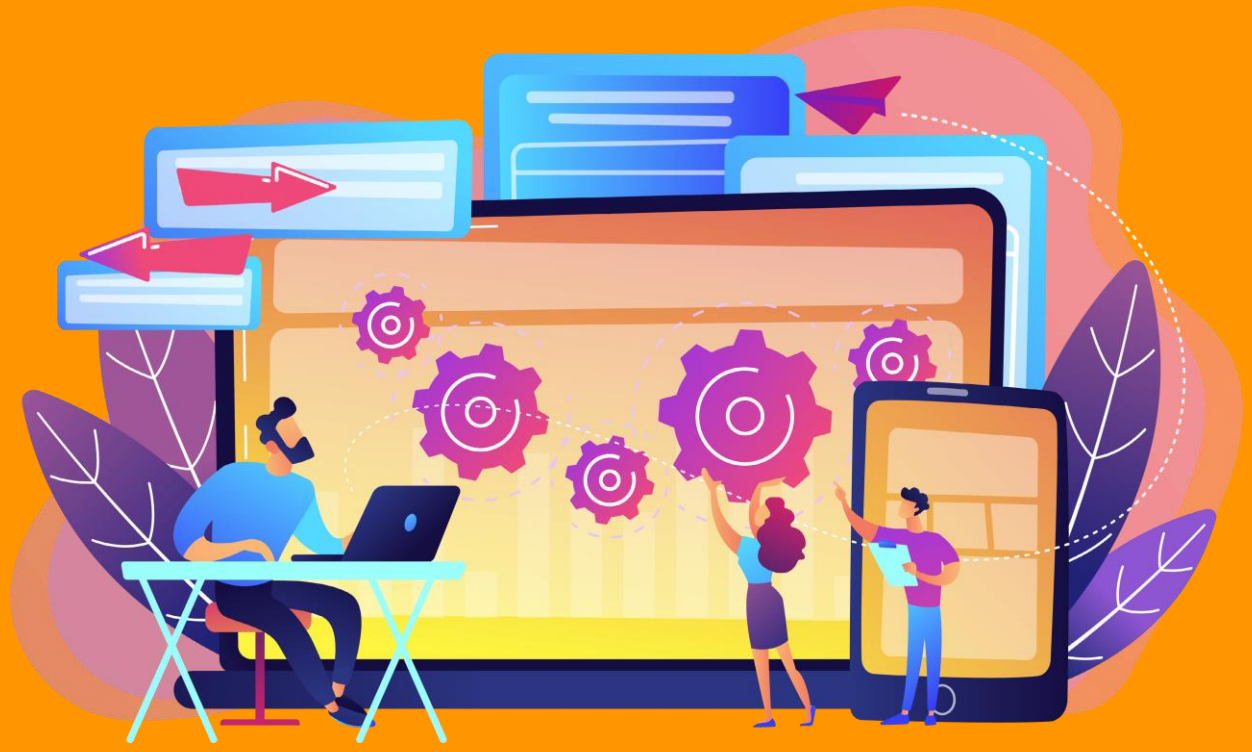
Учесть ландшафт

Повысить управляемость

Повысить безопасность

Делать «на вырост»

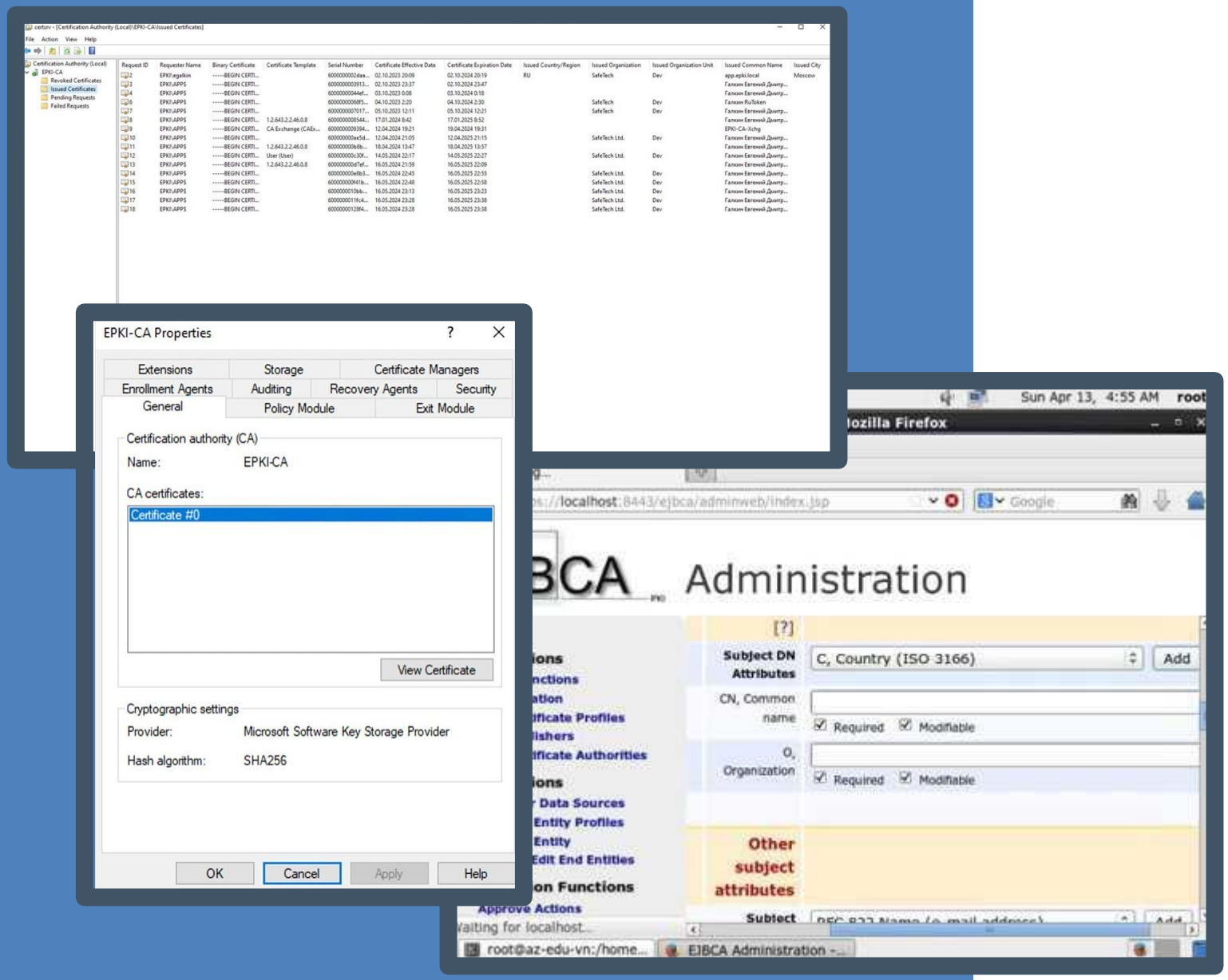
SAFETECH



- **MS-WSTEP**: замена Microsoft CA
- **SCEP**: рабата с MacOS, iOS, Android, Linux, Cisco
- **ACME**: TLS для веб-порталов, Kubernetes, Openshift
- **CMP**: Базовый стандарт для API OpenSSL, Bouncy Castle, Nexus и других
- **EST**: системы MDM
- **REST API**: интеграция сторонних систем самостоятельной и сторонней разработки

УПРАВЛЯЕМОСТЬ

SAFETECH



ЭТО БОЛЬ...

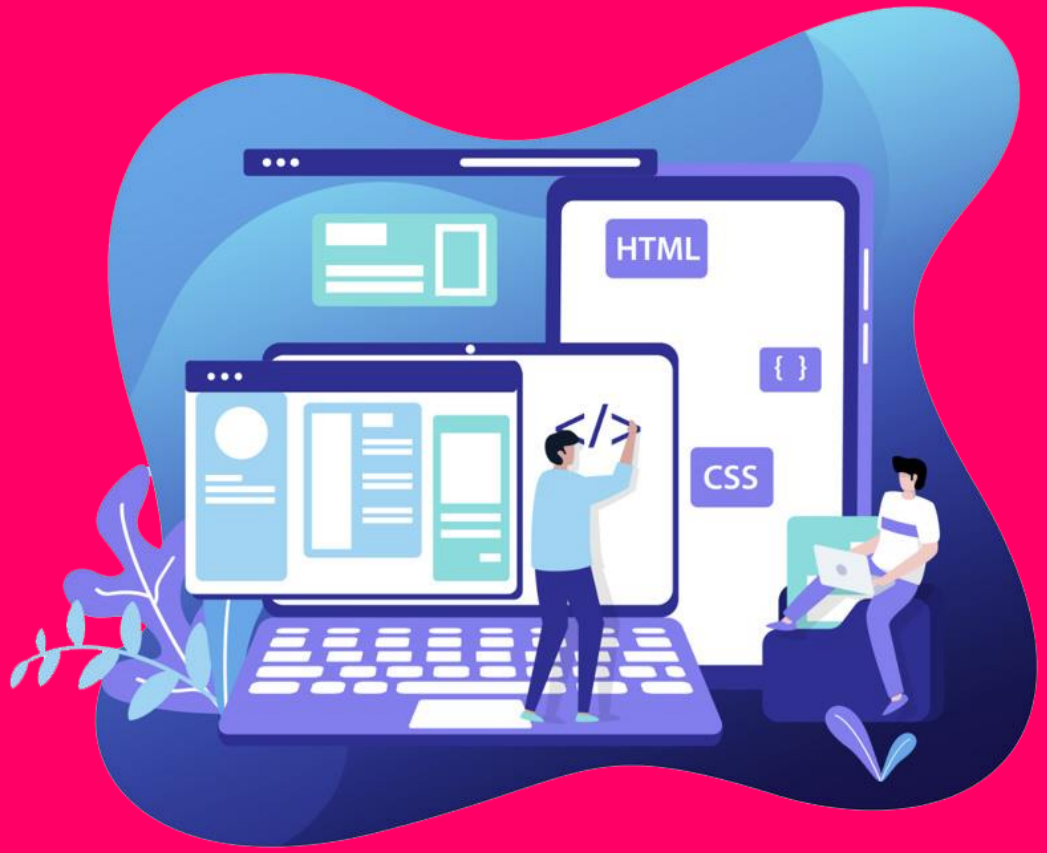
SAFETECH

Аудит, регистрация событий, интеграция с внешними системами (SIEM, IPS/IDS)

Ролевая модель доступа (включая базовые роли Администратора, Аудитора, Оператора)

Поддержка современных протоколов управления доступом (OIDC, Kerberos и пр.)

SAFETECH



- Российская и западная криптография, HSM
- Классическая виртуализация
- Контейнеризация (*Docker, OpenShift/K8S*)
- Поддержка отечественных ОС и СУБД
- Масштабируемая архитектура
- Изоляция PKI-сервисов
- Общепринятые метрики быстродействия и доступности

Сами с усами

SAFETECH

РАЗОБРАТЬСЯ ВО ВСЕЙ ЭТОЙ КУХНЕ

Форматы
Протоколы
Особенности разных ОС
Возможные ошибки с конфигурациями
Оборудование и криптографическое ПО

НАПИСАТЬ СВОИ ОБВЯЗКИ

Очень вряд ли что-то из Open Source будет удовлетворять Вашим требованиям сразу

И потом понадобится поддержка

СДЕЛАТЬ ЭТО УДОБНО

Оно должно работать и «не шуршать»

ВНЕДРИТЬ И ПОДДЕРЖИВАТЬ

Скрестить реализации со своими системами, поставить и настроить

КАК ПРИМЕР – ДАВАЙТЕ ПОСМОТРИМ НА MS-XCEP

SAFETECH

supersededPolicies: An instance of a SupersededPolicies object as defined in section 3.1.4.1.3.25. A value of nil indicates that the corresponding CertificateEnrollmentPolicy object does not supersede another.

privateKeyFlags: The <privateKeyFlags> element is an unsigned integer that MUST be a bitwise OR of zero or more of the following possible values. For more information about the relationship between the <privateKeyFlags> element and the <msPKI-Private-Key-Flag> attribute, see [MS-WCCE] section 3.1.2.4.2.2.2.8.

Integer value	Meaning
0x00000001	Instructs the client to archive the private key.
0x00000010	Instructs the client to allow the private key to be exported.
0x00000020	Instructs the client to protect the private key.

subjectN
OR of

Inte valu
0x0(
0x0(
0x0(
0x0(
0x01
0x02
0x04
0x08
0x1(

0x20000000	The CA adds the value of the mail attribute from the requestor's user object in Active Directory as the Subject extension of the issued certificate.
0x40000000	The CA sets the Subject Name to the cn attribute value of the requestor's user object in Active Directory.
0x80000000	The CA sets the Subject Name to the distinguishedName attribute value of the requestor's user object in Active Directory.
0x00000008	The client reuses the values of the Subject Name and Subject Alternative Name extensions from an existing, valid certificate when creating a renewal certificate request. This flag can only be used when the SubjectNameEnrolleeSupplies (0x00000001) or SubjectAlternativeNameEnrolleeSupplies (0x00010000) flag is specified.

enrollmentFlags: The <enrollmentFlags> element is an unsigned integer that MUST be a bitwise OR of zero or more of the following values.

Integer value	Meaning
0x00000001	Instructs the client and CA to include an S/MIME extension, as specified in [RFC4262].
0x00000008	Instructs the CA to append the issued certificate to the userCertificate attribute, on the user object in Active Directory.
0x00000010	Instructs the CA to check the user's userCertificate attribute in Active Directory, as specified in [RFC4523], for valid certificates that match the template enrolled for.
0x00000040	This flag instructs clients to sign the renewal request using the private key of the existing certificate. For more information, see [MS-WCCE] section 3.2.2.6.2.1.4.5.6. This flag also instructs the CA to process the renewal requests as specified in [MS-WCCE] section 3.2.2.6.2.1.4.5.6.

Integer value	Name	Meaning
0x00000400	Reserved	This flag value is reserved.
0x00040000	Reserved	This flag value is reserved.
0x00080000	Reserved	This flag value is reserved.
0x00001000	Reserved	This flag value is reserved.

hashAlgorithmOIDReference: An integer value that references an existing <oIDReferenceID> element as defined in section 3.1.4.1.3.16. The hash algorithm is used when signing operations are performed during the **certificate enrollment** process. If the value of the <policySchema> element for this Attributes object is 3 and the hash algorithm is defined for the policy, the value of the <hashAlgorithmOIDReference> element MUST be an integer that references the <oIDReferenceID> of the corresponding hash algorithm definition. If the value of the

lefined,

1.

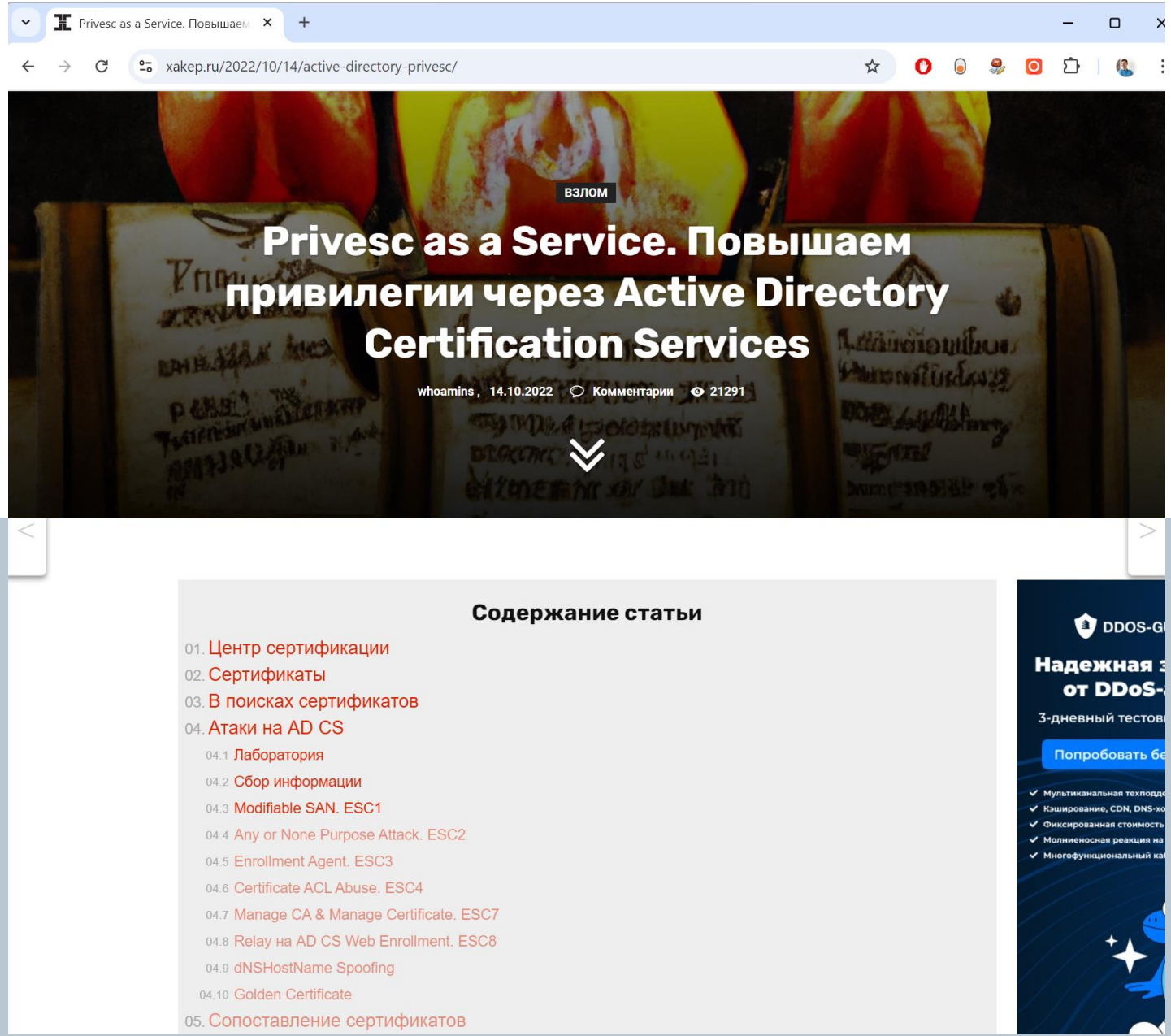
l.

0x00800000	The CA adds the value of the userPrincipalName attribute from the requestor's user object in Active Directory to the Subject Alternative Name extension of the issued certificate.
0x01000000	The CA adds the value of the objectGUID attribute from the requestor's user object in Active Directory to the Subject Alternative Name extension of the issued certificate.
0x02000000	The CA adds the value of the userPrincipalName attribute from the requestor's user object in Active Directory to the Subject Alternative Name extension of the issued certificate.

0x00000002	Reserved	This flag value is reserved.
0x00000004	Reserved	This flag value is reserved.
0x00000008	Reserved	This flag value is reserved.
0x00000010	Reserved	This flag value is reserved.
0x00000020	Reserved	This flag value is reserved.
0x00000100	Reserved	This flag value is reserved.
0x00000200	Reserved	This flag value is reserved.

ЧТО ~~КУ...~~ ИМЕЛ ВВИДУ АВТОР?..

SAFETECH


Privesc as a Service. Повышаем
xakep.ru/2022/10/14/active-directory-privesc/
ВЗЛОМ
Privesc as a Service. Повышаем привилегии через Active Directory Certification Services
whoamins , 14.10.2022 Комментарии 21291
Содержание статьи
01. Центр сертификации
02. Сертификаты
03. В поисках сертификатов
04. Атаки на AD CS
04.1 Лаборатория
04.2 Сбор информации
04.3 Modifiable SAN. ESC1
04.4 Any or None Purpose Attack. ESC2
04.5 Enrollment Agent. ESC3
04.6 Certificate ACL Abuse. ESC4
04.7 Manage CA & Manage Certificate. ESC7
04.8 Relay на AD CS Web Enrollment. ESC8
04.9 dNSHostName Spoofing
04.10 Golden Certificate
05. Сопоставление сертификатов
DDOS-G
Надежная
от DDoS-
3-дневный тестов
Попробовать бе
Мультиканальная техподде
Кэширование, CDN, DNS-хо
Фиксированная стоимость
Молниеносная реакция на
Многофункциональный ка

Можно...

Но сложно...

ИМПОРТОЗАМЕЩАЙТЕ!
УЛУЧШАЙТЕ!

САМОЕ ВРЕМЯ!

SAFETECH

Спасибо
за внимание!

safe-tech.ru
+7 (495) 120-99-09
info@safe-tech.ru