

Михаил Масленников

Инфраструктура открытых ключей. Часть 2.

18+

Михаил Масленников

**Инфраструктура
открытых ключей. Часть 2.**

«Автор»

2026

Масленников М. Е.

Инфраструктура открытых ключей. Часть 2. /

М. Е. Масленников — «Автор», 2026

Я думаю, что портал Госуслуг России знаком почти каждому читателю. А кто из них знает, что у доступа к этому portalу после 12 декабря 2026 года могут появиться проблемы? Какие проблемы, с чем они связаны? Как их избежать? Обо все этом читайте в части 2 книги «Инфраструктура открытых ключей».

© Масленников М. Е., 2026

© Автор, 2026

Содержание

Введение	5
Разбор действующего до 12.12.2026 сертификата портала Госуслуг.	6
Предназначения сертификата.	7
Конец ознакомительного фрагмента.	12

Михаил Масленников

Инфраструктура открытых ключей. Часть 2.

Введение

Эта книга – продолжение части 1 книги «Инфраструктура открытых ключей», опубликованной на портале Литрес. Как сказано в Википедии, *«инфраструктура открытых ключей — набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач, на основе закрытого и открытого ключей. В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:*

закрытый ключ (private key) известен только его владельцу;

удостоверяющий центр (УЦ или СА — certificate authority) создает электронный документ — сертификат открытого ключа, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, открытый ключ (public key) свободно передается;

никто не доверяет друг другу, но все доверяют удостоверяющему центру;

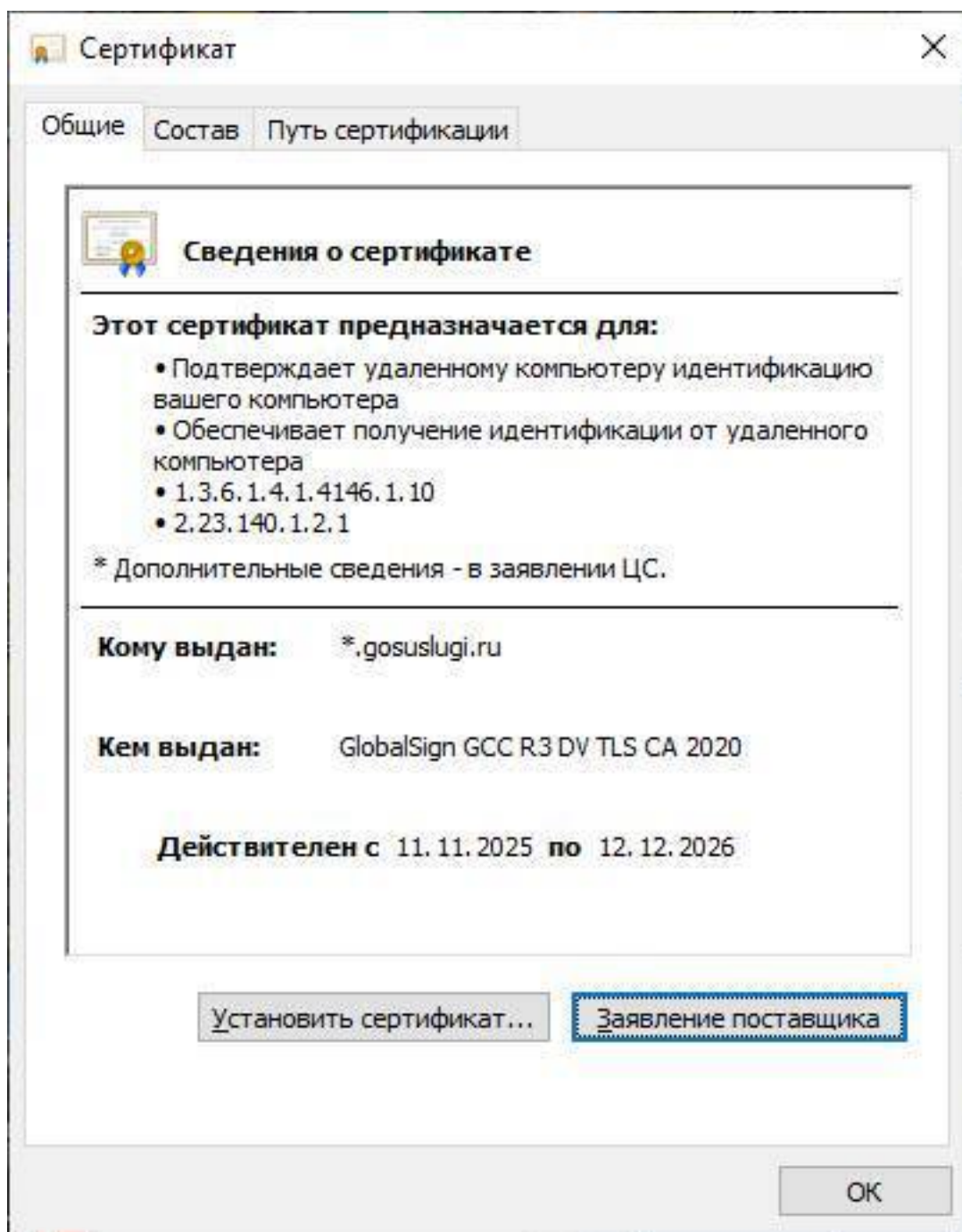
удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.»

По-английски, инфраструктура открытых ключей называется Public Key Infrastructure, или сокращенно PKI. Это совершенно безбрежная тема в современной криптографии. Большинство моих читателей скорее всего что-то слышали о криптографии, представляют себе асимметричную криптосистему с секретными и открытыми ключами, и очень часто ею пользуются в повседневной жизни, например, при обращении к WEB-ресурсам по протоколу HTTPS. Благодаря успехам в практической реализации алгоритмов и методов асимметричной криптографии, большинство пользователей легко и без проблем пользуются протоколом HTTPS, не забывая себе голову различными нюансами, интересными профессиональным криптографам. Что делать, если вдруг возникнут проблемы и ресурс окажется недоступным?

Перейдем ближе к делу, т.е. к части 2 книги «Инфраструктура открытых ключей». Я думаю, что портал Госуслуг России знаком почти каждому читателю. А кто из них знает, что у доступа к этому portalу после 12 декабря 2026 года могут появиться проблемы? Какие проблемы, с чем они связаны? Как их избежать? Обо все этом читайте в части 2 книги «Инфраструктура открытых ключей».

Разбор действующего до 12.12.2026 сертификата портала Госуслуг.

Давайте оставим в стороне явно нематематическую задачу – разбираться в «русской национальной криптографической политике». Там противоречие на противоречии сидит и противоречием погоняет. Попробуем разобраться в действующем SSL-сертификате портала Госуслуг, подобно тому, как мы разбирались в части 1 с сертификатом УЦ Microsoft. В процессе такой разборки будет видно, насколько сертификат УЦ отличается от SSL-сертификата.



Предназначения сертификата.

Начнем с верхушки: «Этот сертификат предназначен для:». У сертификата УЦ Microsoft было:

Все политики выдачи

Все политики применения

Проще говоря, для всего, что угодно. Вот тут-то читатель сразу же схватит за руку автора.

- В части 1 автор, разбирая «по косточкам» корневой сертификат УЦ Microsoft, утверждал, что он предназначен исключительно для подписи, в том числе заверяемых сертификатов и списков отзыва (CRL). Что же тогда значит «Все политики выдачи» и «Все политики применения»?

Давайте зададим эти вопросы ИИ.

Вопрос ИИ: «Что означает предназначение «Все политики выдачи» цифрового сертификата УЦ?»

ИИ:

Предназначение «Все политики выдачи» (в английской версии — All Issuance Policies) в свойствах цифрового сертификата является так называемой маской (wildcard).

Это означает, что у данного сертификата отсутствуют какие-либо ограничения на правила и юридические условия выпуска нижестоящих сертификатов. Данный узел в цепочке доверия полностью одобряет любые регламенты применения.

В технической структуре сертификата (стандарт X.509) этому назначению соответствует глобальный универсальный идентификатор объекта (OID): 2.5.29.32.0.

Давайте проверим ИИ и напрямую посмотрим ASN.1 дерево этого сертификата.

Нет! Крест на пузе, нет в ASN.1 дереве корневого сертификата Microsoft объекта с OID 2.5.29.32.0. Хватаем за горло ИИ.

Вопрос к ИИ: «Почему в сертификате "Microsoft Root Certificate Authority 2011" нет объекта с OID 2.5.29.32.0?»

ИИ:

В сертификате «Microsoft Root Certificate Authority 2011» (как и во многих других глобальных корневых сертификатах крупных вендоров) расширение Certificate Policies (Политики сертификата, 2.5.29.32) и маска «Все политики выдачи» (2.5.29.32.0) отсутствуют по следующим техническим и архитектурным причинам:

1. Правило «Неявного одобрения» (Implicit Wildcard) по стандарту RFC 5280

Согласно международным стандартам построения инфраструктуры открытых ключей (RFC 5280), самоподписанные корневые сертификаты по умолчанию обладают абсолютным доверием.

Если в корневом сертификате (Root CA) расширение политик полностью отсутствует, операционная система и криптографические библиотеки автоматически трактуют это так, будто корень неявно одобряет абсолютно любые политики применения и выдачи (Any Policy).

Внедрять явную маску 2.5.29.32.0 технически избыточно — корень и без нее является абсолютной вершиной доверия в своей цепочке.

А «Все политики применения»?

Вопрос ИИ: «Что означает предназначение «Все политики применения» цифрового сертификата УЦ?»

ИИ:

«Все политики применения» (в английской версии Windows — All Application Policies) в свойствах цифрового сертификата означает, что данный ключ не имеет никаких ограничений на технические сценарии его использования.

Если у сертификата включено это предназначение, криптографическая система операционной системы считает его абсолютно универсальным. Ему разрешено выполнять любую техническую задачу, поддерживаемую криптографией.

В кодировке стандартов ИТ (X.509) этому понятию соответствует глобальный универсальный идентификатор объекта (OID): 2.5.29.37.0 (также известный как Any Extended Key Usage или AnyEKU).

Вопрос к ИИ: «Почему в сертификате "Microsoft Root Certificate Authority 2011" нет объекта с OID 2.5.29.37.0?»

ИИ:

В корневом сертификате «Microsoft Root Certificate Authority 2011» объекта с OID 2.5.29.37.0 («Все политики применения» / Any EKU) нет по двум фундаментальным причинам: стандарту интернет-архитектуры PKI и принципу безопасности корпорации Microsoft.

*Если в расширении сертификата поле **Enhanced Key Usage** (Улучшенное использование ключа, OID 2.5.29.37) **отсутствует целиком**, операционные системы и криптографические библиотеки автоматически интерпретируют это как **неявное одобрение любых технических сценариев применения**.*

Внедрение явной маски «Any EKU» (2.5.29.37.0) в Корневой УЦ технически избыточно. Для Windows этот корень и без нее является абсолютной вершиной доверия.

Как пел мой любимый В.С. Высоцкий:

Что ж, идеи нам близки

Первым — лучшие куски

А вторым — чего уж тут, он все выверил

В утешение дадут кости с ливером...

Короче, предназначения сертификата - это крипто-чиновничьи кости с ливером.

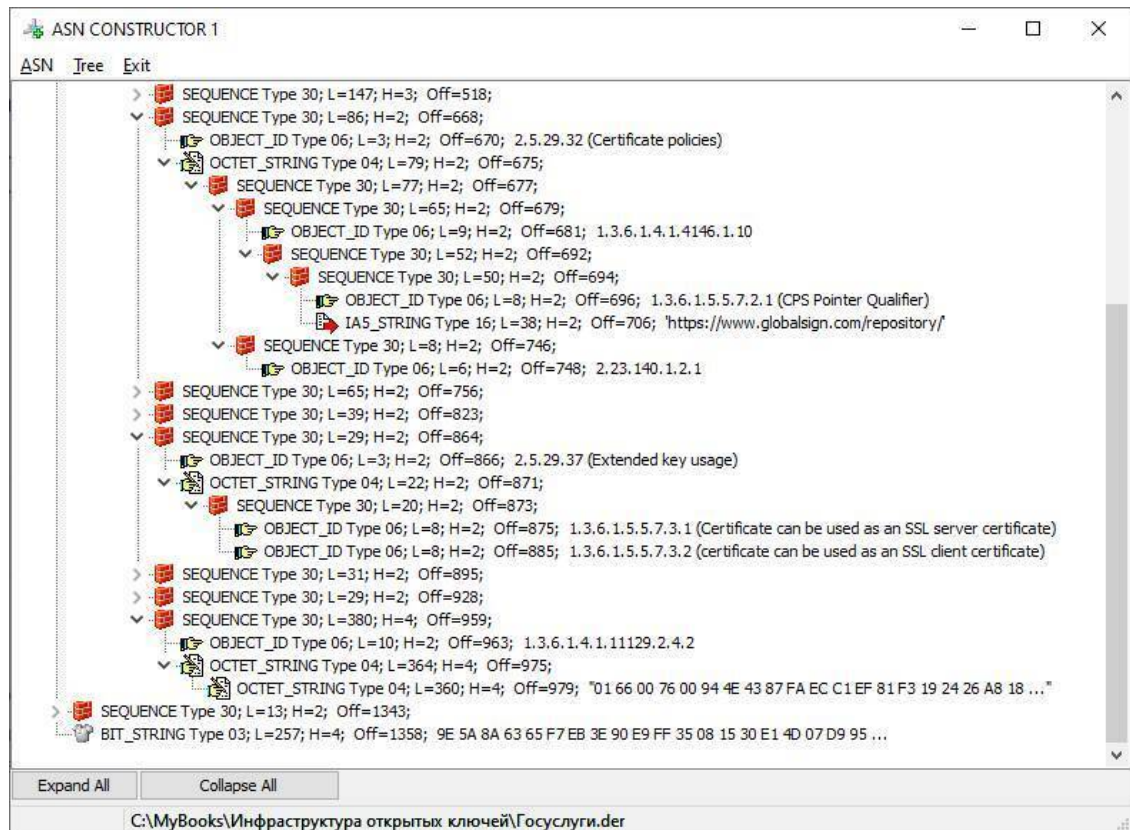
А теперь давайте попробуем поискать эти предназначения в SSL-сертификате портала Госуслуг.

Предназначение № 1. **Подтверждает удаленному компьютеру идентификацию вашего компьютера.**

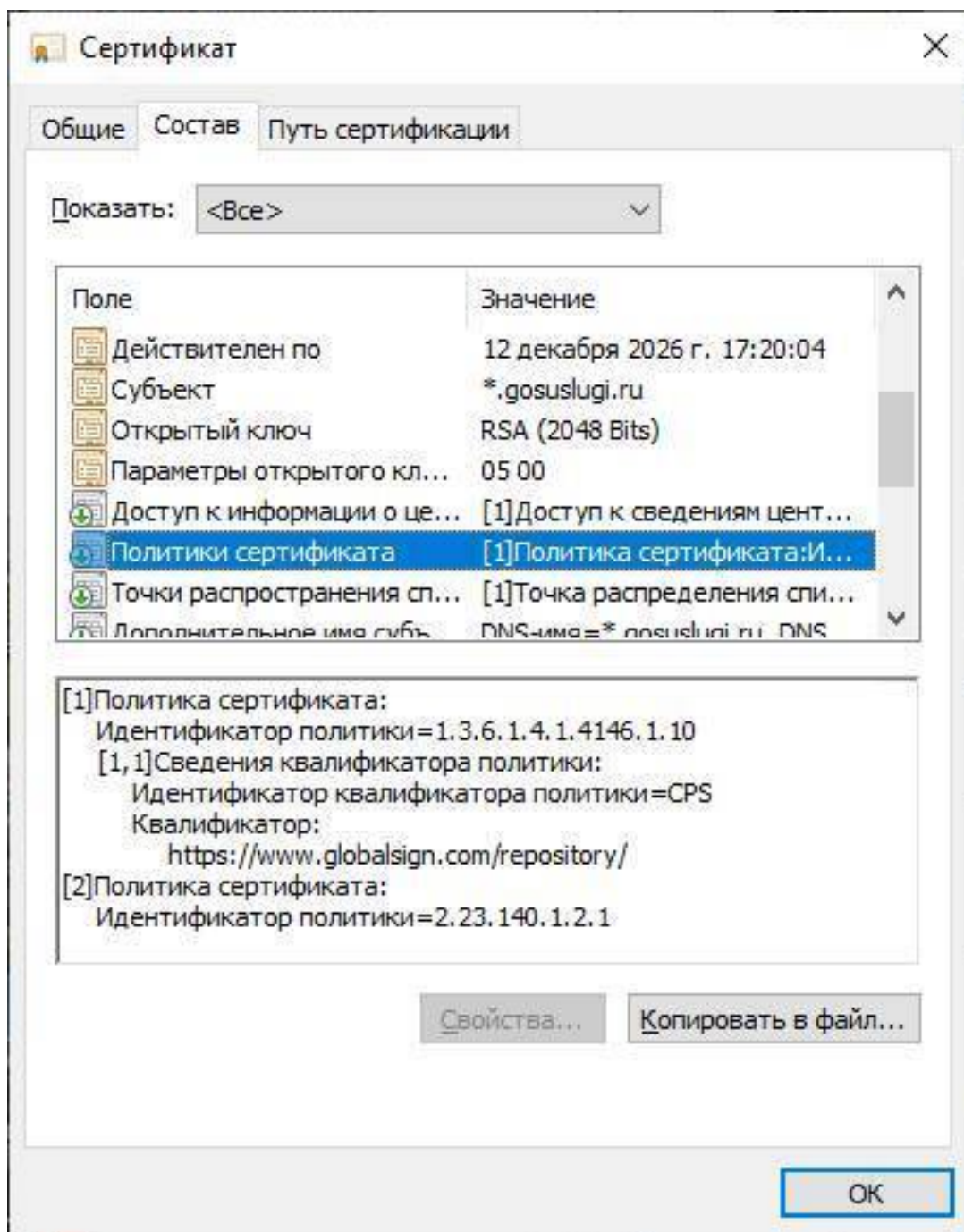
Предназначение № 2. **Обеспечивает получение идентификации от удаленного компьютера.**

Предназначение № 3. **1.3.6.1.4.1.4146.1.10.**

Предназначение № 4. **2.23.140.1.2.1.**



Два последних предназначения находятся в Certificate policies.



Разбираемся с каждым из них.

Вопрос ИИ: «Что означает политика сертификата с идентификатором 1.3.6.1.4.1.4146.1.10?»

ИИ:

Политика сертификата с идентификатором (OID) 1.3.6.1.4.1.4146.1.10 означает Политику сертификатов с проверкой домена (Domain Validation Certificates Policy), принадлежащую международному удостоверяющему центру GlobalSign

Если этот OID присутствует в расширении Certificate Policies цифрового сертификата, это сообщает операционной системе, браузеру или проверяющему софту о следующем:

Тип выпуска: Это стандартный SSL/TLS-сертификат начального уровня с проверкой домена (DV SSL). При его выдаче робот УЦ проверил только то, что заявитель действи-

тельно управляет указанным сайтом (например, через добавление DNS-записи или файла на сервер). Личность владельца или юридический статус компании при этом не проверялись.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.