

## Unsigned X.509 Certificates

Сертификаты X.509 без подписи

### Аннотация

Этот документ определяет заменитель алгоритма подписи X.509, который может применяться в контексте, где не предполагается проверка подписи получателем. В этой части данный документ обновляет RFC 5280.

### Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF<sup>1</sup> и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG<sup>2</sup>. Дополнительные сведения о документах Internet Standard приведены в разделе 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <https://www.rfc-editor.org/info/rfc9925>.

### Авторские права

Авторские права (Copyright (c) 2026) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с пересмотренной лицензией BSD (Revised BSD License), как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Revised BSD License).

## Оглавление

1. Введение.....	1
2. Уровни требований.....	2
3. Создание сертификата без подписи.....	2
3.1. Подпись.....	2
3.2. Эмитент.....	2
3.3. Расширения.....	2
4. Восприятие сертификатов без подписи.....	3
5. Вопросы безопасности.....	3
6. Взаимодействие с IANA.....	3
6.1. Идентификатор модуля.....	3
6.2. Алгоритм.....	3
6.3. Атрибут Relative Distinguished Name.....	3
7. Литература.....	4
7.1. Нормативные документы.....	4
7.2. Дополнительная литература.....	4
Приложение А. Модуль ASN.1.....	4
Благодарности.....	5
Адрес автора.....	5

## 1. Введение

Сертификат X.509 [RFC5280] связывает две сущности PKI - сведения о субъекте и подтверждение от эмитента. Рассматривая PKI как граф с сущностями в качестве узлов, как в [RFC4158], сертификат можно считать границей между субъектом и эмитентом.

В некоторых случаях приложению нужна лишь информация о субъекте, а не сертификат (в модели с графом - узел, а не ребро). Например, проверка пути сертификации (раздел 6 в [RFC5280]) начинается с привязки доверия, которую иногда называют корнем удостоверяющего центра (root certification authority или root CA). Приложение доверяет сведениям об этой привязке без проверки через сеть (out-of-band) и не требует подписи эмитента.

X.509 не задаёт структуру для таких случаев и взамен привязки доверия X.509 зачастую представляются «самоподписанными» сертификатами, где ключи субъекта подписан им самим. Имеются и другие форматы (например, [RFC5914]) передачи привязок доверия, но по-прежнему широко применяются самоподписанные сертификаты.

Кроме того, в некоторых внедрениях серверов TLS [RFC8446] применяются самоподписанные сертификаты конечных сущностей (элементов), когда те не предназначены для представления выданных CA идентификаторов и

<sup>1</sup>Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

<sup>2</sup>Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

предполагается, что принимающая сторона проверяет сертификат несетевыми (out-of-band) средствами, например, по известному отпечатку (fingerprint).

Такие самоподписи обычно не имеют смысла для защиты, не проверяются получателем и служат лишь заменителями в части выполнения синтаксических требований к сертификатам X.509.

Расчёт подписей-заменителей имеет ряд недостатков:

- постквантовые алгоритмы подписей слишком громоздки и включение самоподписи значительно повышает размер передаваемых данных;
- если субъектом является конечный элемент (сущность), а не CA, расчёт подписей X.509 ведёт к риску кросс-протокольных атак с предусмотренным использованием ключа;
- неясно, требует ли такая самоподпись установки бита CA в базовых ограничениях или keyCertSign при использовании ключей; если ключ предназначен для приложений, отличных от X.509, такие возможности могут приводить к неоправданному риску;
- если субъектом является конечный элемент (сущность) и его ключ не является ключом подписи (например, ключ Key Encapsulation Mechanism или KEM), не существует алгоритма подписи для применения с ключом.

Этот документ задаёт профиль сертификатов X.509 без подписи, которые могут применяться в ситуациях, где сертификат служит лишь контейнером для передачи сведений о субъекте без указания конкретного эмитента.

## 2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

## 3. Создание сертификата без подписи

В этом разделе рассматривается создание отправителем сертификата без подписи.

### 3.1. Подпись

Для создания сертификата X.509 без подписи отправитель **должен** указать в поле сертификата signatureAlgorithm и в поле подписи TBSCertificate идентификатор алгоритма (AlgorithmIdentifier) id-alg-unsigned, как показано ниже

```
id-alg-unsigned OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 6 36 }
```

Параметры id-alg-unsigned **должны** быть опущены, значение signatureValue **должно** иметь тип BIT STRING и нулевой размер.

### 3.2. Эмитент

Сертификат без подписи заменяет самоподписанный сертификат в случаях, когда приложению нужны лишь сведения о субъекте. В нем не указывается эмитент, поэтому некоторые требования профиля [RFC5280] не могут быть применены должным образом. Однако у приложения могут быть требования, вытекающие из [X.509] и [RFC5280], поэтому отправители **могут** создавать сертификат как самоподписанный, если это требуется для совместимости.

В частности, для описания эмитента сертификата применяются поля:

- issuer (параграф 4.1.2.4 в [RFC5280])
- issuerUniqueID (параграф 4.1.2.8 в [RFC5280])

Поле issuer не является опциональным и пустые поля запрещены [X.509] и параграфом 4.1.2.4 в [RFC5280], поэтому при пустом поле не обеспечивается совместимость с имеющимися приложениями.

При непустом поле subject отправитель **может** указать его значение в поле issuer, подобно тому, как это делается в самоподписанных сертификатах. Это может быть полезно в приложениях, которые, например, ожидают привязки доверия с совпадающими значениями полей issuer и subject. Однако это лишь заменитель и сертификаты без подписи не считаются самоподписанными или самовыпущенными.

Как вариант, отправители **могут** использовать короткий заменитель поля issuer, состоящий из относительного отличительного имени, имеющего 1 атрибут типа id-rdna-unsigned с значением UTF8String нулевого размера. Идентификатор id-rdna-unsigned показан ниже:

```
id-rdna-unsigned OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 25 1 }
```

Этот заменитель в строковом представлении [RFC4514] имеет вид:

```
1.3.6.1.5.5.7.25.1=#0c00
```

Отправитель **должен** опускать поле issuerUniqueID, поскольку оно не требуется, не применимо и уже отменено в параграфе 4.1.2.8 [RFC5280].

### 3.3. Расширения

Некоторые расширения X.509 описывают эмитента сертификата и поэтому не имеют смысла а сертификате без подписи:

- authority key identifier (идентификатор ключа агентства - параграф 4.2.1.1 в [RFC5280]);
- issuer alternative name (дополнительное имя эмитента - параграф 4.2.1.7 в [RFC5280]).

Отправителям **следует** опускать расширения authority key identifier и issuer alternative name. Параграф 4.2.1.1 в [RFC5280] требует включать authority key identifier в сертификат, но допускает исключения для самоподписанных

сертификатов, применяемых при распространении открытых ключей. Данный документ обновляет [RFC5280], дополнительно разрешая опускать authority key identifier в сертификатах без подписи.

Некоторые расширения отражают роль субъекта - CA или конечный элемент:

- key usage (использование ключа - параграф 4.2.1.3 в [RFC5280]);
- basic constraints (базовые ограничения - параграф 4.2.1.9 в [RFC5280]).

Отправителям **следует** заполнять эти поля в соответствии с субъектом:

- если субъект является CA, **следует** указывать бит использования ключа keyCertSign, а также **следует** включать расширение basic constraints с cA = TRUE;
- если субъект является конечным элементом, **не следует** устанавливать бит использования ключа keyCertSign и **следует** опускать расширение basic constraints или устанавливать в нем cA = FALSE. В отличие от самоподписанных сертификатов сертификат без подписи не эмиттирует себя, поэтому не требуется использовать самоподпись в расширениях.

## 4. Восприятие сертификатов без подписи

Подписи X.509 типа id-alg-unsigned недействительны, если:

- при обработке сертификатов X.509 без проверки подписей получателя **может** воспринимать id-alg-unsigned;
- при проверке подписей X.509 получатель **должен** отвергать (reject) id-alg-unsigned.

В частности, валидаторам X.509 **недопустимо** воспринимать id-alg-unsigned вместо подписи в пути сертификации.

Предполагается, что большинство неизменённых приложений X.509 уже соответствует этому руководству. Приложениям X.509 **рекомендуется** выполнять эти требования, игнорируя данный документ и считая взамен id-alg-unsigned нераспознанным алгоритмом подписи. Неизменённый валидатор X.509 не сможет проверить подпись (п. а.1 в параграфе 6.1.3 [RFC5280]) и, таким образом, отвергнуть путь сертификации. И наоборот, в случаях игнорирования приложением X.509 самоподписей id-alg-unsigned будет игнорироваться более эффективно.

В ином контексте может потребоваться внесение изменений в приложение или ограничение определёнными формами неподписанных сертификатов. Например, приложение может проверять самоподписи для классификации локально настроенных сертификатов как привязок доверия или недоверенных посредников. Таким приложениям может потребоваться изменение своей модели конфигурации или пользовательского интерфейса перед использованием сертификатов без подписи в качестве привязок доверия.

## 5. Вопросы безопасности

Принято использовать криптографические ключи лишь с одной целью. Если ключ применяется в разных контекстах, для приложений возникает риск кросс-протокольных атак, когда разные применения конфликтуют между собой. Однако в приложениях, использующих самоподписанные сертификаты конечных элементов, ключи субъектов обязательно применяются в двух вариантах - самоподпись X.509 и протокол конечного элемента. Сертификаты без подписи устраняют многократное применение ключей за счёт исключения самоподписей X.509.

Если приложение воспринимает id-alg-unsigned как часть пути сертификации или в ином контексте, где требуется проверка подписи X.509, такую проверку можно обойти. Раздел 4 запрещает это и рекомендует приложениям обрабатывать id-alg-unsigned так же, как другие нераспознанные алгоритмы подписи. Не выполняющие это условие приложения подвержены риску уязвимостей, аналогичных описанным в [JWT] и параграфе 1.1 [JOSE].

Подпись в самоподписанном сертификате имеет ограниченную применимость для передачи доверия. Однако некоторые приложения могут, например, использовать её для проверки целостности с целью защиты от случайных повреждений хранилища. Сертификат без подписи не обеспечивает проверки целостности. Приложениям, проверяющим самоподпись для контроля целостности, **следует** использовать иные механизмы, такие как внешний кэш, который можно проверить помимо сети (out-of-band).

## 6. Взаимодействие с IANA

### 6.1. Идентификатор модуля

Агентство IANA добавило указанную в таблице 1 запись в реестр SMI Security for PKIX Module Identifier [RFC7299].

Таблица 1.

Значение	Описание	Документ
122	id-mod-algUnsigned-2025	RFC 9925

### 6.2. Алгоритм

Агентство IANA добавило указанную в таблице 2 запись в реестр SMI Security for PKIX Algorithms [RFC7299].

Таблица 2.

Значение	Описание	Документ
36	id- alg-unsigned	RFC 9925

### 6.3. Атрибут Relative Distinguished Name

Для выделения id-rdna-unsigned в этом документе вводится новое значение PKIX OID arg для атрибутов относительного отличительного имени (relative distinguished name).

Агентство IANA добавило указанную в таблице 3 запись в реестр SMI Security for PKIX [RFC7299].

Значение	Описание	Документ
25	Relative Distinguished Name Attribute	RFC 9925

Агентство IANA создало реестр SMI Security for PKIX Relative Distinguished Name Attribute а группе реестров Structure of Management Information (SMI) Numbers (MIB Module Registrations).

Описание нового реестра имеет вид iso.org.dod.internet.security.mechanisms.pkix.rdna (1.3.6.1.5.5.7.25).

Реестр содержит 3 колонки и инициализируется приведёнными в таблице 4 значениями.

Таблица 4.

Значение	Описание	Документ
1	id-rdna-unsigned	RFC 9925

Обновления этой таблицы должны выполняться по процедуре Specification Required, заданной в [RFC8126].

## 7. Литература

### 7.1. Нормативные документы

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <<https://www.rfc-editor.org/info/rfc5912>>.
- [RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, [RFC 8126](#), DOI 10.17487/RFC8126, June 2017, <<https://www.rfc-editor.org/info/rfc8126>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

### 7.2. Дополнительная литература

- [JOSE] Madden, N., "JOSE: Deprecate 'none' and 'RSA1\_5'", Work in Progress, Internet-Draft, draft-ietf-jose-deprecate-none-rsa15-03, 19 September 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-jose-deprecate-none-rsa15-03>>.
- [JWT] Sanderson, J., "How Many Days Has It Been Since a JWT alg:none Vulnerability?", <<https://www.howmanydayssinceajwtalgnonevuln.com/>>.
- [RFC4158] Cooper, M., Dzambasow, Y., Hesse, P., Joseph, S., and R. Nicholas, "Internet X.509 Public Key Infrastructure: Certification Path Building", RFC 4158, DOI 10.17487/RFC4158, September 2005, <<https://www.rfc-editor.org/info/rfc4158>>.
- [RFC4514] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names", RFC 4514, DOI 10.17487/RFC4514, June 2006, <<https://www.rfc-editor.org/info/rfc4514>>.
- [RFC5914] Housley, R., Ashmore, S., and C. Wallace, "Trust Anchor Format", RFC 5914, DOI 10.17487/RFC5914, June 2010, <<https://www.rfc-editor.org/info/rfc5914>>.
- [RFC7299] Housley, R., "Object Identifier Registry for the PKIX Working Group", RFC 7299, DOI 10.17487/RFC7299, July 2014, <<https://www.rfc-editor.org/info/rfc7299>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", [RFC 8446](#), DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.
- [X.509] ITU-T, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, ISO/IEC 9594-8:2020, October 2019, <<https://www.itu.int/rec/t-rec-x.509/en>>.

## Приложение A. Модуль ASN.1

В приведённом модуле ASN.1 используются соглашения, заданные в [RFC5912].

```
SignatureAlgorithmNone
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-algUnsigned-2025(122) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
SIGNATURE-ALGORITHM
FROM AlgorithmInformation-2009 -- in [RFC5912]
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-algorithmInformation-02(58) }
ATTRIBUTE
FROM PKIX-CommonTypes-2009 -- in [RFC5912]
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-pkixCommon-02(57) } ;
```

```
-- Алгоритм неподписанной подписи (Unsigned Signature Algorithm)

id-alg-unsigned OBJECT IDENTIFIER ::= { iso(1)
  identified-organization(3) dod(6) internet(1) security(5)
  mechanisms(5) pkix(7) alg(6) 36 }

sa-unsigned SIGNATURE-ALGORITHM ::= {
  IDENTIFIER id-alg-unsigned
  PARAMS ARE absent
}

id-rdna-unsigned OBJECT IDENTIFIER ::= { iso(1)
  identified-organization(3) dod(6) internet(1) security(5)
  mechanisms(5) pkix(7) rdna(25) 1 }

at-unsigned ATTRIBUTE ::= {
  TYPE UTF8String (SIZE (0))
  IDENTIFIED BY id-rdna-unsigned
}

END
```

## Благодарности

Спасибо Bob Beck, Nick Harper, Sophie Schmieg за обзор ранних вариантов документа, Alex Gaynor за ссылку на статью [JWT], Russ Housley за дополнительную информацию.

## Адрес автора

David Benjamin  
Google LLC  
Email: [davidben@google.com](mailto:davidben@google.com)

## Перевод на русский язык

Николай Малых  
[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)