

PKI, УЦ и сертификаты

Термины, относящиеся к PKI, удостоверяющим центрам (УЦ), электронной подписи (ЭП), сертификатам и ключам.

В этом разделе

- [Инфраструктура открытых ключей](#)
- [Удостоверяющий центр и центр регистрации](#)
- [Сертификаты](#)
- [Списки отзыва и политики](#)
- [Ключи](#)
- [Электронная подпись](#)
- [Криптография и аутентификация в PKI](#)
- [Криптографическая защита \(ГОСТ Р 34.14-2025\)](#)
- [NIST IR 7298r2 \(термины PKI на английском\)](#)
- [Рамки доверия и службы учёта данных \(EAP Trust Framework\)](#)
- [Дополнения портала](#)

PKI / инфраструктура открытых ключей

Инфраструктура открытых ключей

Термин / Англ.	Определение
Архитектура ИОК иерархическая (<i>hierarchy type PKI architecture</i>)	Древовидная система подчинения и взаимодействия центров сертификации, при которой центры более высокого уровня формируют сертификаты для центров более низкого уровня. [ПНСТ-799-2022] 2 определений. Определение 2: Древовидная система подчинения, при которой центры сертификации более высокого уровня формируют сертификаты для центров более низкого уровня. [ГОСТ Р 34.14-2025, ст. 55]
Архитектура ИОК сетевая (<i>network type PKI architecture</i>)	Система взаимодействия центров сертификации, при которой они формируют друг для друга кросс-сертификаты для обеспечения проверки в обоих направлениях. [ПНСТ-799-2022] 2 определений.

Термин / Англ.	Определение
	Определение 2: Система взаимодействия центров сертификации, при которой они формируют друг для друга кросс-сертификаты. [ГОСТ Р 34.14-2025, ст. 56]
Инфраструктура открытых ключей (ИОК) (<i>public key infrastructure, PKI</i>)	Инфраструктура, используемая в отношениях между владельцем ключа и доверяющей стороной и позволяющая доверяющей стороне использовать сертификат, связанный с владельцем ключа. К ИОК относятся УЦ, структура данных сертификата, средства получения информации о состоянии отзыва, политика сертификации и методы проверки. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.18] 3 определений. Определение 2: Инфраструктура управления ключами асимметричной криптографической системы на основе сертификатов открытых ключей. [ГОСТ Р 34.14-2025, ст. 53] 3 определений. Определение 3: Совокупность технических и процедурных мер, используемых для управления открытыми ключами, встроенными в цифровые сертификаты. Ключи в таких сертификатах могут использоваться для защиты связи и обмена данными по потенциально небезопасным сетям. [EAP Trust Framework]

Вместо термина **ИОК** во всех материалах используется более привычный и общеупотребительный английский термин **PKI**.

Удостоверяющий центр и центр регистрации

Термин / Англ.	Определение
Доверенная третья сторона (ДТС) (<i>trusted third party, TTP</i>)	Третья сторона, считающаяся доверенной в рамках протокола информационной безопасности. Понятие шире, чем УЦ, и включает штампы времени и депонирование ключей. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.23]
Доверяющая сторона (<i>relying party</i>)	Получатель сертификата, доверяющий этому сертификату или электронной подписи, проверенной с его помощью. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.21; ГОСТ Р 55811-2013, п. 3.18]
Орган по присвоению атрибутов (оа) (<i>attribute authority, AA</i>)	Уполномоченный орган, назначающий полномочия путём выдачи сертификатов атрибутов. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.1]
Пользователь сертификата (<i>relying party</i>)	Юридическое или физическое лицо, использующее сертификат ключа проверки электронной подписи для проверки электронной подписи. [ГОСТ Р 55811-2013, п. 3.18]

Термин / Англ.	Определение
Система удостоверяющих центров (система УЦ) (<i>certification authority system</i>)	Совокупность удостоверяющих центров, которые управляют сертификатами ключей проверки электронных подписей на протяжении жизненного цикла сертификата. [ГОСТ Р 55811-2013, п. 3.26]
Удостоверяющий центр (УЦ) (<i>certification authority, CA</i>)	Уполномоченный орган, которому участвующие стороны доверили создание и присвоение сертификатов. УЦ может дополнительно создавать ключи для доверяющих сторон. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.14; ГОСТ Р 55811-2013, п. 3.29] 2 определений. Определение 2: Центр доверия, предназначенный для создания сертификатов открытых ключей. [ГОСТ Р 34.14-2025, ст. 50]
Центр регистрации (ЦР) (<i>registration authority, RA</i>)	Орган, ответственный за идентификацию и аутентификацию субъектов сертификатов, но не подписывающий и не издающий сертификаты. ЦР делегировано выполнение определённой работы от имени УЦ. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.20; ГОСТ Р 55811-2013, п. 3.33] 2 определений. Определение 2: Компонент УЦ, обеспечивающий предоставление центру сертификации подтверждённых идентификационных данных лиц, обратившихся за сертификатом. [ГОСТ Р 34.14-2025, ст. 49]

Сертификаты

Термин / Англ.	Определение
Владелец сертификата (<i>certificate holder</i>)	Организация или лицо, указанное субъектом в действительном сертификате. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.11]
Восстановление действия сертификата (<i>certificate release</i>)	Восстановление удостоверяющим центром действия сертификата, которое было приостановлено. [ГОСТ Р 55811-2013, п. 3.2]
Замена сертификата (<i>certificate re-key</i>)	Процесс получения нового сертификата на новый ключ проверки электронной подписи после создания новой пары ключей. [ГОСТ Р 55811-2013, п. 3.7]
Квалифицированный сертификат (<i>qualified certificate</i>)	Сертификат, основное назначение которого — идентификация личности с высокой степенью достоверности в открытых службах неоспоримости. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.19]
Конечный владелец сертификата (<i>end entity</i>)	Владелец сертификата ключа проверки электронной подписи, за исключением УЦ, использующий свой ключ для целей, отличных от подписания сертификатов. [ГОСТ Р 55811-2013, п. 3.11]

Термин / Англ.	Определение
Кросс-сертификат (<i>cross-certificate</i>)	Сертификат посреднического УЦ, обеспечивающий масштабное развёртывание приложений открытых ключей между разными доменами УЦ. [ГОСТ Р ИСО 17090-2-2016, п. 5.3]
Отзыв сертификата (<i>certificate revocation</i>)	Аннулирование связи между сертификатом и его владельцем по причине утраты доверия. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.10]
Приостановка действия сертификата (<i>certificate suspension</i>)	Временное прекращение удостоверяющим центром действия сертификата ключа проверки электронной подписи. [ГОСТ Р 55811-2013, п. 3.19]
Проверка сертификата (<i>certificate verification</i>)	Проверка аутентичности сертификата. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.12]
Продление сертификата (<i>certificate renewal</i>)	Процесс выдачи нового сертификата на существующий ключ проверки электронной подписи с новым сроком действия. [ГОСТ Р 55811-2013, п. 3.20]
Профиль сертификатов (<i>certificate profile</i>)	Спецификация структуры и допустимого содержания сертификата определённого типа. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.9]
Расширение сертификата (<i>certificate extension</i>)	Поля расширений в сертификатах X.509, обеспечивающие связывание дополнительных атрибутов с пользователями или ключами. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.6]
Сертификат (<i>certificate</i>)	Сертификат открытого ключа. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.4]
Сертификат атрибута (<i>attribute certificate</i>)	Информационный объект, содержание которого заверено электронной подписью ОА, привязывающий значения атрибута к идентификации владельца. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.2]
Сертификат ключа проверки электронной подписи (<i>public key certificate</i>)	Электронный документ, выданный УЦ и подтверждающий принадлежность ключа проверки электронной подписи владельцу. [ГОСТ Р 55811-2013, п. 3.24]
Сертификат открытого ключа (СОК) (<i>public key certificate, PKC</i>)	Сертификат, соответствующий X.509, обеспечивающий связь идентичности с открытым ключом. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.17]
Сертификат уполномоченного органа (<i>authority certificate</i>)	Сертификат, выпущенный для удостоверяющего центра или органа по присвоению атрибутов. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.3]
Сертификат УЦ (<i>certification authority public key certificate</i>)	Сертификат ключа проверки электронной подписи, владельцем которого является удостоверяющий центр. [ГОСТ Р 55811-2013, п. 3.25]

Термин / Англ.	Определение
Управление сертификатами (<i>certificate management</i>)	Процедуры: генерация, распространение, архивирование и отзыв сертификатов. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.8]
Цепочка сертификатов (<i>certification path</i>)	Упорядоченная последовательность сертификатов, позволяющая установить доверие конечному сертификату, исходя из доверия первому. [ГОСТ Р 55811-2013, п. 3.35]

Списки отзыва и политики

Термин / Англ.	Определение
Кросс-сертификация (<i>cross-certification</i>)	Процесс, при котором два удостоверяющих центра взаимно подтверждают ключи проверки электронных подписей друг друга. [ГОСТ Р 55811-2013, п. 3.13]
Политика применения сертификатов (<i>public key certificate policy</i>)	Поименованный набор правил, определяющий порядок применения сертификата ключа проверки ЭП для определённой совокупности бизнес-приложений. [ГОСТ Р 55811-2013, п. 3.17]
Политика сертификата (ПС) (<i>certificate policy, CP</i>)	Именованный свод правил, описывающий применимость сертификата в конкретном кругу субъектов и/или классе приложений. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.15; ГОСТ Р 55811-2013, п. 3.17]
Регламент выдачи сертификатов (РВС) (<i>public key certification practice statement</i>)	Совокупность правил, регулирующих порядок выдачи и управления сертификатами ключей проверки ЭП на протяжении их жизненного цикла. [ГОСТ Р 55811-2013, п. 3.22]
Реестр сертификатов (<i>certificate register</i>)	Совокупность данных, включающая список выданных УЦ сертификатов и информацию о датах прекращения действия или аннулирования. [ГОСТ Р 55811-2013, п. 3.23]
Свод правил по сертификации (СПС) (<i>certification practice statement, CPS</i>)	Формулировка правил, которые УЦ использует при издании сертификатов. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.16]
Список недействительных сертификатов (САС) (<i>certificate revocation/non-action list</i>)	Список сертификатов, включая сертификаты с истёкшим сроком, приостановленные и аннулированные. [ГОСТ Р 55811-2013, п. 3.27]
Список отозванных сертификатов (СОС) (<i>certificate revocation list, CRL</i>)	Список сертификатов, объявленных недействительными до истечения срока действия. [ГОСТ Р ИСО 17090-1-2015, п. 4; ГОСТ Р 55811-2013, п. 3.27] 2 определений. Определение 2: Перечень досрочно прекративших действие сертификатов открытых

Термин / Англ.	Определение
	ключей, формирование и доступ к которому обеспечивает УЦ. [ГОСТ Р 34.14-2025, ст. 57]

Ключи

Термин / Англ.	Определение
Доверенный ключ проверки ЭП (<i>trusted CA public key</i>)	Ключ проверки ЭП, полученный доверенным образом и используемый для проверки первого сертификата в цепочке. [ГОСТ Р 55811-2013, н. 3.5]
Закрытый ключ (<i>private key</i>)	Ключ из состава асимметричной пары ключей, сформированных для объекта, который должен быть использован только этим объектом. [ГОСТ Р 58833-2020, н. 3.18]
Закрытый ключ неизвлекаемый (<i>non-extractable private key</i>)	Закрытый ключ, который невозможно извлечь из устройства аутентификации, в котором он был создан. [ГОСТ Р 58833-2020, н. 3.19]
Ключ (<i>key</i>)	Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование. [ГОСТ Р 58833-2020, н. 3.26; ГОСТ Р 34.12-2015]
Ключ проверки электронной подписи (<i>public key</i>)	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности ЭП. [ГОСТ Р 55811-2013, н. 3.8]
Ключ электронной подписи (<i>private key</i>)	Уникальная последовательность символов, предназначенная для создания электронной подписи. [ГОСТ Р 55811-2013, н. 3.9]
Ключевая информация (<i>keying material</i>)	Данные, необходимые для выполнения криптографических операций (например, изготовления ключей). [ГОСТ Р 55811-2013, н. 3.10]
Криптографический ключ (<i>cryptographic key</i>)	Параметр, определяющий работу криптографической функции. [ГОСТ Р 55811-2013, н. 3.12]
Открытый ключ (<i>public key</i>)	Ключ из состава асимметричной пары ключей, который может быть общедоступным. [ГОСТ Р 58833-2020, н. 3.39]
Пара ключей (<i>key pair</i>)	Совокупность ключа проверки электронной подписи и соответствующего ему ключа электронной подписи. [ГОСТ Р 55811-2013, н. 3.16]
Разделённое знание (<i>split knowledge</i>)	Метод хранения криптографического ключа, при котором два (или более) лица по отдельности имеют части ключа, не дающие сведений о полном ключе. [ГОСТ Р 55811-2013, н. 3.21]
Управление ключами (<i>key management</i>)	Генерация, сохранение, распределение, удаление, архивирование и применение ключей в соответствии с политикой безопасности.

Термин / Англ.	Определение
	[ГОСТ Р ИСО 17090-1-2015, п. 3.2.20; ГОСТ Р 55811-2013, п. 3.30] 2 определений. Определение 2: Организация и управление процессами выработки, регистрации, сертификации, распределения, применения, хранения, архивирования, восстановления, отзыва, замены и уничтожения криптографических ключей. [ГОСТ Р 34.14-2025, ст. 36]
Часть ключа (<i>key fragment</i>)	Фрагмент ключа, переданный на хранение лицу для реализации метода разделения знаний. [ГОСТ Р 55811-2013, п. 3.31]

Электронная подпись

Термин / Англ.	Определение
Неоспоримость (<i>non-repudiation</i>)	Услуга, обеспечивающая каждой из участвующих сторон доказательство целостности и происхождения данных. [ГОСТ Р ИСО 17090-1-2015, п. 3.2.21]
Хэш-функция (<i>hash-function</i>)	Функция, отображающая строки бит в строки бит фиксированной длины с заданными свойствами криптостойкости. [ГОСТ Р 55811-2013, п. 3.32; ГОСТ Р 34.11-2012]
Электронная подпись (ЭП) (<i>digital signature</i>)	Данные, добавленные к блоку данных, или криптографическое преобразование, позволяющие убедиться в подлинности источника и целостности данных. [ГОСТ Р ИСО 17090-1-2015, п. 3.2.14; ГОСТ Р 55811-2013, п. 3.36]

Криптография и аутентификация в PKI

Термин / Англ.	Определение
Асимметричный алгоритм шифрования (<i>asymmetric cryptographic algorithm</i>)	Алгоритм, в котором ключи зашифрования и расшифрования различаются. [ГОСТ Р ИСО 17090-1-2015, п. 3.2.3]
Аттестация (<i>certification</i>)	Процедура, при которой третья сторона предоставляет гарантию соответствия системы обработки данных требованиям ИБ. [ГОСТ Р ИСО 17090-1-2015, п. 3.3.13]
Аутентификация источника данных (<i>data origin authentication</i>)	Подтверждение того, что источник полученных данных соответствует заявленному. [ГОСТ Р ИСО 17090-1-2015, п. 3.2.12]
Данные запроса на сертификат (<i>request data on public key certificate</i>)	Подписанная информация в запросе на сертификат, включающая ключ проверки ЭП и идентификационные данные. [ГОСТ Р 55811-2013, п. 3.3]

Термин / Англ.	Определение
Двойной контроль (<i>dual control</i>)	Процесс совместного участия двух или более лиц, действующих в целях защиты. [ГОСТ Р 55811-2013, н. 3.4]
Журнал аудита (<i>audit journal</i>)	Хронологическая запись системной активности, достаточная для реконструкции и анализа событий. [ГОСТ Р 55811-2013, н. 3.6]
Зашифрование (<i>encipherment, encryption</i>)	Криптографическое преобразование данных для получения шифротекста. [ГОСТ Р ИСО 17090-1-2015, н. 3.2.15]
Криптографический алгоритм (<i>cryptographic algorithm, cipher</i>)	Метод преобразования данных для сокрытия или предотвращения несанкционированной модификации. [ГОСТ Р ИСО 17090-1-2015, н. 3.2.10]
Криптография (<i>cryptography</i>)	Дисциплина, охватывающая принципы и методы преобразования данных для сокрытия их содержания. [ГОСТ Р ИСО 17090-1-2015, н. 3.2.9]
Отличительное имя (<i>distinguished name</i>)	Уникальный идентификатор владельца сертификата ключа проверки электронной подписи. [ГОСТ Р 55811-2013, н. 3.15]
Расшифрование (<i>decipherment, decryption</i>)	Процесс получения исходных данных из шифротекста. [ГОСТ Р ИСО 17090-1-2015, н. 3.2.13]
Уведомление по дополнительному каналу (<i>out-of-band notification</i>)	Уведомление с использованием средств связи, независимых от основных. [ГОСТ Р 55811-2013, н. 3.28]
Шифротекст (<i>ciphertext</i>)	Данные, получаемые в результате шифрования, смысловое содержание которых недоступно. [ГОСТ Р ИСО 17090-1-2015, н. 3.2.7]
Электронное удостоверение (<i>electronic credential</i>)	Совокупность идентификационной и аутентификационной информации, подлинность которой подтверждена доверенной третьей стороной. [ГОСТ Р 58833-2020, н. 3.62]

Криптографическая защита (ГОСТ Р 34.14-2025)

Термин / Англ.	Определение
Архитектура ИОК (<i>PKI architecture</i>)	Система взаимодействия удостоверяющих центров и входящих в них центров сертификации и регистрации. [ГОСТ Р 34.14-2025, см. 54]
Дешифрование (<i>breaking an encipherment system</i>)	Раскрытие зашифрованной информации методами криптографического анализа без предварительного полного знания применяемого криптографического ключа. [ГОСТ Р 34.14-2025, см. 27]
Жизненный цикл ключа (<i>key life cycle</i>)	Последовательность этапов работы с криптографическим ключом от момента выработки до момента уничтожения. [ГОСТ Р 34.14-2025, см. 38]

Термин / Англ.	Определение
Информация об открытом ключе (<i>public key information</i>)	Структура данных, содержащая открытый ключ и идентификационные данные владельца, а также информацию об УЦ, области использования, сроке действия. [ГОСТ Р 34.14-2025, см. 46]
Инфраструктура управления ключами (<i>key management infrastructure</i>)	Комплекс центров доверия, аппаратно-программных и технических средств, обеспечивающих управление криптографическими ключами. [ГОСТ Р 34.14-2025, см. 37]
Ключевой материал (<i>keying material</i>)	Данные, позволяющие сформировать секретные криптографические ключи. [ГОСТ Р 34.14-2025, см. 35]
Компрометация ключа (<i>key compromise</i>)	Нарушение конфиденциальности криптографического ключа или ключевого материала. [ГОСТ Р 34.14-2025, см. 40]
Множество ключей (<i>key space</i>)	Множество всех возможных значений криптографического ключа для конкретного криптографического алгоритма. [ГОСТ Р 34.14-2025, см. 33]
Невозможность отрицания создания	Свойство криптографической системы, при котором субъект не может отрицать факта создания данных. [ГОСТ Р 34.14-2025, см. 150]
Параметр схемы цифровой подписи (<i>domain parameter</i>)	Элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем. [ГОСТ Р 34.14-2025, см. 135; ГОСТ Р 34.10-2012]
Постквантовая криптография (<i>post-quantum cryptography</i>)	Раздел криптографии, связанный с синтезом криптографических систем, обеспечивающих защиту от атак с применением квантовых компьютеров. [ГОСТ Р 34.14-2025, см. 29]
Проверка подписи (<i>verification process</i>)	Процесс, в котором используются подписанное сообщение, ключ проверки и параметры схемы, результатом которого является заключение о корректности подписи. [ГОСТ Р 34.14-2025, см. 134]
Система цифровой подписи (<i>digital signature system</i>)	Асимметричная криптографическая система, предназначенная для обеспечения аутентификации данных и невозможности отрицания создания. [ГОСТ Р 34.14-2025, см. 24]
Срок действия ключа (<i>key life time</i>)	Установленный временной интервал, в течение которого криптографический ключ разрешается использовать. [ГОСТ Р 34.14-2025, см. 39]
Схема цифровой подписи (<i>digital signature scheme</i>)	Совокупность двух криптографических протоколов (алгоритмов), предназначенных для формирования и проверки подписи. [ГОСТ Р 34.14-2025, см. 129]
Формирование подписи (<i>signature process</i>)	Процесс, результатом которого для заданного сообщения, ключа подписи и параметров схемы является цифровая подпись. [ГОСТ Р 34.14-2025, см. 130]
Центр сертификации (<i>certification center</i>)	Компонент УЦ, обеспечивающий создание сертификатов открытых ключей, формирование реестра и списка отозванных сертификатов. [ГОСТ Р 34.14-2025, см. 48]

Термин / Англ.	Определение
Цифровая подпись с восстановлением (<i>digital signature with message recovery</i>)	Цифровая подпись, при которой сообщение или его часть могут быть извлечены из подписи. [ГОСТ Р 34.14-2025, ст. 132]
Цифровая подпись с дополнением (<i>digital signature with appendix</i>)	Цифровая подпись, при которой никакая часть подписываемого сообщения не может быть извлечена из подписи. [ГОСТ Р 34.14-2025, ст. 133]
Штамп времени (<i>time-stamp token</i>)	Структура, криптографически связывающая набор данных со временем её создания. [ГОСТ Р 34.14-2025, ст. 51]

Вместо термина **ИОК** во всех материалах используется более привычный и общеупотребительный английский термин **PKI**.

NIST IR 7298r2 (термины PKI на английском)

Термин / Англ.	Определение
Certificate management	Процесс, при котором сертификаты генерируются, хранятся, защищаются, передаются, загружаются, используются и уничтожаются. [NIST IR 7298r2; CNSSI-4009]
Hash function	Функция, отображающая битовую строку произвольной длины в строку фиксированной длины. [NIST IR 7298r2; FIPS 198]
Non-repudiation	Услуга ИБ, при которой участвующие стороны не могут отрицать факта участия в обмене данными. [NIST IR 7298r2]
Trust anchor	Открытый ключ и имя центра сертификации (CA), используемые для проверки первого сертификата в последовательности. [NIST IR 7298r2]

Рамки доверия и службы учёта данных (EAP Trust Framework)

Термин / Англ.	Определение
Заявитель (<i>claimant</i>)	Сторона, личность которой должна быть проверена. [EAP Trust Framework]
Заявление о практике (<i>practice statement</i>)	Формальное заявление о практиках, соблюдаемых субъектом аутентификации (например, ЦР, поставщиком служб учёта данных или проверяющим), определяющее конкретные шаги по регистрации и проверке личностей, выпуску учётных данных и аутентификации заявителей. [EAP Trust Framework]

Термин / Англ.	Определение
Поставщик службы проверки личности (<i>identity proofing service provider</i>)	Поставщик службы электронного доверия, предлагающий как самостоятельную услугу проверку личности. Иногда называется агентом/центром регистрации (ЦР). <i>[EAP Trust Framework]</i>
Поставщик службы учёта данных; CSP (<i>credential service provider</i>)	Поставщик службы электронного доверия, управляющий одной или несколькими службами учётных данных. Может включать центр регистрации. <i>[EAP Trust Framework]</i>
Привязка личности (<i>identity binding</i>)	Степень, в которой электронному учётному данные можно доверять как представителю указанного в нём субъекта. <i>[EAP Trust Framework]</i>
Проверка личности (<i>identity proofing</i>)	Процесс проверки информации, относящейся к личности, для идентификации человека со степенью уникальности и достоверности, достаточной для целей использования этой личности. <i>[EAP Trust Framework]</i>
Рамки доверия (<i>trust framework</i>)	Совокупность документов, совместно определяющих отраслевую саморегулируемую структуру для служб электронного доверия, включая описания критериев, правил, процедур, процессов и иных документов. <i>[EAP Trust Framework]</i>
Служба учёта данных (<i>credential service</i>)	Тип службы электронного доверия, обеспечивающий проверку личностей, выпуск утверждений/учётных данных/токенов, связанных с личностью, и последующее управление этими учётными данными (продление, отзыв, предоставление статуса и служб аутентификации). <i>[EAP Trust Framework]</i>
Служба электронного доверия (<i>electronic trust service; ETS</i>)	Служба, повышающая доверие и уверенность в электронных транзакциях, как правило (но не обязательно) с использованием криптографических методов или конфиденциальных материалов, таких как PIN-коды и пароли. <i>[EAP Trust Framework]</i>
Токен (<i>token</i>)	Объект, которым заявитель владеет и контролирует (как правило, ключ или пароль), используемый для аутентификации личности заявителя. <i>[EAP Trust Framework]</i>
Учётные данные (<i>credential</i>)	Объект, проверяемый при предъявлении в транзакции аутентификации. Может быть связан с лицом, которому он выпущен, либо быть предъявительским. Электронные учётные данные — цифровые документы, связывающие личность или атрибут с токеном подписчика. <i>[EAP Trust Framework]</i>
Эмитент (<i>issuer</i>)	Лицо или объект, официально предоставляющий или распространяющий что-либо. <i>[EAP Trust Framework]</i>

Дополнения портала

Термин / Англ.	Определение
Центр валидации (VA)	(англ. validation authority, VA) Служба инфраструктуры открытых ключей, обеспечивающая проверку действительности сертификатов: статуса отзыва и срока действия — как правило, по протоколу OCSP или через списки отзыва сертификатов (CRL). RFC 5280; RFC 6960

Источники

Полный перечень источников с переходами от шифров — в разделе ["Источники и литература"](#).