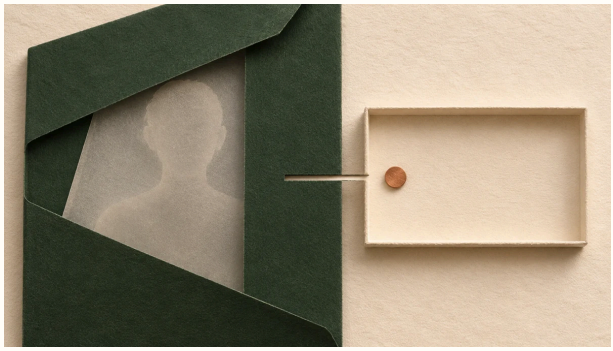


АВТОРСКАЯ АНАЛИТИЧЕСКАЯ СТАТЬЯ

Редакционная дата: 8 октября 2026 г.

Докажите, кто вы, не называя себя

Когда достаточно меньшей истины

В Калифорнии цифровое водительское удостоверение может сообщить продавцу меньше, чем пластиковая карточка, — и именно поэтому оказаться полезнее. Владелец предъявляет электронному считывателю подтверждение того, что достиг определённого возраста. Проверяющая сторона может получить ответ «возрастной порог пройден», тогда как для другой операции потребуются более подробные идентификационные данные. Департамент автотранспорта штата подчёркивает, что цифровое удостоверение пока принимают лишь в отдельных местах и сервисах. Удивительно не то, что документ переехал из кошелька в телефон. Удивительно другое: вопрос, на который мы привыкли отвечать, раскрывая имя, фотографию, адрес и дату рождения, можно закрыть гораздо меньшим фактом — этот человек подходит по возрасту.1

Такой шаг легко принять за уменьшенную копию большого документа. На деле он заново проводит границы знания. Что продавцу действительно нужно знать? Не имя покупателя, не день его рождения, не номер удостоверения и не домашний адрес, который к покупке отношения не имеет. Нужен вывод с приемлемой юридической и технической надёжностью: достиг ли человек возраста, установленного правилом? Прежняя конструкция почти целиком отдавала сотруднику личное досье и надеялась, что большую его часть тот проигнорирует. Новая пытается уравнять видимое системе с тем, что ей разрешено узнать. Здесь мы не только защищаем уже собранные данные, но и спрашиваем, зачем они вообще вошли в дверь.

Меняется и смысл слова «личность». В современных цифровых системах оно выполняет несколько разных работ, которые мы по привычке свели под одно название. При открытии банковского счёта, подпадающего под требования «знай своего клиента», может быть необходимо установить настоящее имя и проверить его. На официальном экзамене организатору, возможно, нужно убедиться, что перед ним именно зарегистрированный участник. Но тому, кто доказывает, что учится в признанном университете, живёт в районе, жители которого имеют право на услугу, или прошёл обязательное обучение перед допуском на объект, не обязательно предъявлять развёрнутую копию собственной биографии. Различие не всегда проходит между «идентификацией» и «анонимностью». Иногда оно проходит между знанием человека и знанием одного его свойства.

От карточки к удостоверению

В июле 2025 года Европейская комиссия представила технический проект проверки возраста. Он позволял государствам и цифровым сервисам строить приложения, подтверждающие возрастную правомочность без раскрытия лишних идентификационных сведений. В том же месяце начались испытания проекта и его адаптация к разным странам, платформам и группам пользователей. В октябре вышла вторая версия: она предусматривала подтверждение через паспорт и удостоверение личности, а Комиссия сообщила, что в решение включены доказательства с нулевым разглашением. К апрелю 2026 года приложение, по словам Комиссии, было технически готово, а предоставить его гражданам предполагалось позднее. Среди стран, адаптирующих решение, назывались Дания, Франция, Греция, Италия и Испания. Всё это — факты разработки, испытаний и планируемого развёртывания. Они не означают, что на момент написания статьи системой уже пользовались все европейцы.2

Европейский проект стремится к большему, чем удобное окно входа. Выдавая подтверждение возраста, организация-эмитент опирается на надёжный источник: национальное удостоверение, паспорт или иной признанный способ проверки. Затем применение подтверждения предполагается отделить от эмитента, чтобы тот не получал уведомление о каждом сайте, куда заходит владелец. Цифровой сервис запрашивает подтверждение возрастного порога и получает результат, по которому разрешает или запрещает доступ. Два момента, обычно слитые воедино, здесь разнесены: сначала проверяется достоверность источника сведений, затем используется строго ограниченная их часть. Разделение может выглядеть тонкой технической процедурой. Но оно не даёт обычным попыткам человека подтвердить своё право сложиться в централизованную летопись его жизни.2

В мае 2025 года Консорциум Всемирной паутины (W3C) утвердил вторую версию модели данных проверяемых удостоверений (Verifiable Credentials Data Model 2.0). Основная идея такова: доверенная организация выпускает набор утверждений о человеке или ином субъекте так, чтобы третья сторона могла проверить целостность

удостоверения и его происхождение. Университет может подтвердить степень, профессиональная организация — лицензию, государственный орган — признак, содержащийся в реестре. Модель называет три стороны: эмитент (Issuer), держатель (Holder) и проверяющий (Verifier). Такая конструкция не создаёт единую всемирную базу данных. Она позволяет достоверному утверждению переходить между организациями с разными системами, если они согласны в том, что означает удостоверение и кто вправе его выдать.3

Но «проверяемое» не означает «истинное». Сам стандарт предупреждает: возможность проверить удостоверение ещё не доказывает соответствие действительности всего, что в нём написано. Цифровая подпись обнаружит подмену данных и свяжет их с эмитентом, но не вернётся в университетский год, чтобы удостовериться, что выпускник ходил на занятия, и не вызовет врача проверить качество подписанного им осмотра. Если исходная база ошиблась, ошибка может выйти во внешний мир в безупречно зашифрованном конверте. Поэтому система начинается с вопроса об учреждении и его процедурах, а не только с выбора алгоритма подписи.3

Раскрытие не означает несвязываемость

Представим профессиональное свидетельство: имя, дата рождения, номер членства, дата аккредитации и специальность. Платформа труда должна проверить, действует ли лицензия по нужной специальности. Первый путь — самый привычный для административного мышления — отправить свидетельство целиком. Второй — выпустить новую, сокращённую версию. Третий — дать человеку составное удостоверение, из которого он раскрывает только сведения, необходимые для сделки. Это выборочное раскрытие (Selective Disclosure). Если же можно доказать, что лицензия действует или оценка выше заданного порога, не показывая исходное значение, на котором строится вывод, мы приближаемся к другой группе инструментов — доказательствам с нулевым разглашением (Zero-Knowledge Proofs). Это не взаимозаменяемые маркетинговые выражения: у каждого метода свои математические и защитные границы.

В ноябре 2025 года Инженерный совет Интернета опубликовал RFC 9901 о выборочном раскрытии для подписанных токенов JSON — SD-JWT. Метод позволяет эмитенту создать удостоверение с криптографическими дайджестами отдельных полей, после чего держатель решает, какие поля открыть проверяющему. В простом случае можно показать статус «студент» и скрыть адрес и телефон, если поля изначально рассчитаны на раздельное раскрытие. Это сокращает объём сведений, попадающих к другой стороне. Но ни название метода, ни наличие шифрования сами по себе не доказывают, что новое предъявление невозможно связать с предыдущим.4

Здесь и прячется одна из самых коварных рыночных подмен. Приложение может заявлять о защите приватности, потому что не показывает дату рождения, и при этом каждый раз отправлять один и тот же подписанный токен или устойчивый отпечаток, который сравнят два сотрудничающих сайта. Возможно, не зная имени, они выяснят, что возраст здесь и там подтверждал один посетитель. RFC 9901 прямо указывает на это ограничение: механизмы раскрытия на основе солёных дайджестов, включая SD-JWT, не гарантируют разделения эмитента и проверяющего, если недобросовестный проверяющий передаёт эмитенту исходное удостоверение. Поле мы спрятали, но могли оставить невидимый серийный номер, пригодный для новой биографии посетителя.4

Поэтому исследователи различают три свойства, которые проектировщику нельзя смешивать. Первое — минимизация раскрытия: проверяющий не узнаёт больше необходимого. Второе — несвязываемость (Unlinkability): два проверяющих не могут лишь по криптографическому материалу заключить, что оба предъявления относятся к одному удостоверению. Третье — привязка к держателю (Holder Binding): человек не может скопировать чужое удостоверение и выдать за своё. Усиление третьего свойства способно ослабить второе, если применяется один постоянный и всем известный ключ. Система может пресечь передачу удостоверений и всё же отслеживать каждое их использование. Это не неразрешимое противоречие, а набор условий, которые нужно проверять совместно, вместо того чтобы объявить победу в одном и велеть молчать об остальных.

Что именно доказывает доказательство?

Самое интригующее математическое решение начинается не с имени, а с вычислимого утверждения. Пусть скрытое значение — дата рождения, а дата операции известна. Проверяющего нужно убедить, что разница между ними достигает разрешённого возраста. Упрощённо требование можно сформулировать так: существует достоверное исходное значение, при котором условие «на день проверки возраст не менее восемнадцати лет» истинно. Если доказательство корректно, само значение проверяющему не нужно. Но здесь скрыто решающее условие: система должна доказать, что скрытая дата рождения поступила из надёжного источника, а не была придумана пользователем секунду назад. Иначе перед нами изящное математическое доказательство вымышленного факта.

В теории доказательство с нулевым разглашением объединяет три требования. Проверяющий принимает корректное доказательство истинного утверждения; тот, у кого нет корректного свидетеля, способен убедить систему в ложном утверждении лишь с малой вероятностью, заданной предпосылками безопасности; наконец, доказательство не раскрывает о скрытом свидетеле ничего сверх того, что уже следует из истинности утверждения. Эти свойства называют полнотой (Completeness), корректностью или стойкостью (Soundness) и нулевым разглашением (Zero Knowledge). Но третье не отменяет того, что фраза «мне больше восемнадцати» сообщает о человеке

реальный факт. В рамках данной математической модели она лишь исключает утечку остальной части свидетеля из самого доказательства. Она не решает проблему лица перед камерой, сетевого адреса или истории браузера.5

Кроме того, не всякое подписываемое свидетельство автоматически порождает любое нужное доказательство. Если эмитент заранее удостоверил признак «старше 18», может быть достаточно предъявить этот подписанный признак без даты рождения. Но если выпущена только сама дата, возможность доказать числовое сравнение, не раскрывая её, зависит от криптографической схемы, способа кодирования и доказательства связи подписи с признаком. Системе может понадобиться производное удостоверение эмитента или протокол, подходящий для такого вычисления. Нельзя поставить на экран логотип ZKP и считать проверку любого условия бесплатной и гарантированной. Инженерная задача не только в том, чтобы скрыть число, но и в том, чтобы доказать его источник, связь с условием и актуальность условия во времени.

В сентябре 2026 года W3C опубликовал проект кандидатской рекомендации по схемам подписи BBS для проверяемых удостоверений. При корректном применении они позволяют получать криптографические доказательства, раскрывающие часть признаков и сохраняющие несвязываемость производных доказательств. Сентябрьский документ не был окончательной рекомендацией: это проект на стадии проверки реализаций. Различие существенно для рынка, который любит выдавать формирующуюся технологию за завершённый консенсус стандартов. И даже сильная несвязываемость криптографического материала не гарантирует её в приложении, если вместе с доказательством пользователь сообщает уникальный факт, сайт повторно ставит идентификатор в браузере или поддерживает иную связь вне протокола.6

Когда контекст раскрывает скрытое шифрованием

При переходе от доказательства к человеку картина меняется ещё сильнее. Если студент небольшого университета сообщит редкую специальность и конкретный год выпуска, имя можно вывести из двух правдивых признаков, хотя прямого идентификатора в доказательстве нет. Если сотрудник команды из трёх человек подтверждает право пользоваться чувствительной системой, должности и времени может хватить, чтобы понять, кто вошёл. Алгоритм здесь не взломали. Взаимодействие раскрыло настолько узкий контекст, что неизвестный стал известным. Приватность следует измерять не числом пустых ячеек в цифровой карточке, а размером группы, в которой человек остаётся неотличимым после раскрытия.

Есть и другой, более тихий слой знания. Сайт может не знать имени и даты рождения, но видеть сетевой адрес, тип устройства, характер движения и время посещения. Профилирование или коммерческая аналитика способны связать попытку входа с прежними действиями. Сильный протокол мешает организациям сопоставлять криптографические доказательства, однако не мешает им отслеживать посетителя

другими способами. Верно и обратное: защита сети и правила хранения могут быть превосходны, хотя выбранное техническое удостоверение математической несвязываемости не даёт. Приватность — не сертификат, который выдаёт программная библиотека, а свойство всей услуги от края до края.

Отзыв, владение и парадокс живого статуса

Философия европейского проекта яснее проявляется в вопросе об источнике. Если при каждом посещении сайта платформа связывается с организацией, выдавшей возрастное удостоверение, эмитент становится свидетелем привычек пользователя. Проверка без соединения, открытые ключи и тщательно спроектированные списки статусов могут уменьшить риск. Но удостоверение могут отозвать или оно может истечь; владелец способен потерять телефон, а его ключи — оказаться скомпрометированными. Тогда проверяющему нужно знать, что свидетельство всё ещё действительно. Рекомендации Национального института стандартов и технологий США (NIST), пересмотренные в 2025 году, требуют возможности отзывать пакеты признаков, советуют ограничивать срок их действия и предупреждают: служба проверки отзыва не должна сообщать эмитенту, что конкретное удостоверение использовалось в конкретном сервисе.[7]

Так возникает «парадокс живого статуса». Мы хотим проверять свидетельство без обращения к эмитенту, чтобы оно не превратилось в инструмент наблюдения. И одновременно хотим, чтобы любой проверяющий немедленно узнал об отзыве из-за украденного устройства, изменившегося права или аннулированной лицензии. Волшебного сочетания полного отсутствия связи, нулевой задержки отзыва и отсутствия состояния у всех сторон не существует. Есть архитектуры и компромиссы: короткие сроки действия, общие реестры статуса с гранулярностью, не выделяющей человека, подходящие доказательства неотозванности, процедуры восстановления и перевыпуска, разные пределы риска для разных услуг. Если организация продаёт удостоверение, которое «никогда не обращается к источнику», стоит спросить, откуда оно знает, что вчера его не отозвали.

Следующий практический вопрос: кто стоит перед экраном телефона? Если взрослый получил доказательство возраста и переслал его младшему знакомому, приватность протокола не спасает смысл проверки. Поэтому некоторые схемы привязывают владение к закрытому ключу в защищённом устройстве и требуют, чтобы кошелёк поставил новую подпись в ответ на уникальный запрос проверяющего. Случайная величина (Nonce) уменьшает возможность повторно воспроизвести старое сообщение, а привязка ответа к конкретной стороне мешает взять доказательство для магазина и предъявить его другой платформе. Всё это сдерживает подмену держателя и повтор сообщения, но без дополнительных средств не устанавливает, что телефон держит именно тот человек, который прошёл первоначальную проверку.[7][8]

Здесь калифорнийский опыт вновь важен не потому, что достиг идеала, а потому, что возвращает проверку на своё место. Департамент подчёркивает: цифровое удостоверение — не фотография карточки, предъявлять его следует через электронную проверку; просто показывать экран другому человеку не рекомендуется. Магазинам и сервисам предстоит установить совместимые считыватели, разобраться, что запрашивается и что приходит в ответ, и отработать случаи, когда телефон отказал или считывателя нет. Чего стоит удостоверение, сохраняющее приватность внутри кошелька, если при неисправности устройства сотрудник требует полную копию документа?1

Из лаборатории в организацию

Можно вообразить более широкие применения, но считать их следует проектными гипотезами, а не уже достигнутыми результатами. Сайт со стажировкой только для студентов может запросить действующее подтверждение зачисления в признанное учебное заведение. Исследовательский центр с чувствительными данными — доказательство недавнего курса по этике без копирования сертификата и его номеров. Город может дать льготу жителям административной территории, не спрашивая точный домашний адрес, если право определяется принадлежностью адреса к району. Профессиональное объединение — подтвердить действительность лицензии специалиста, не раскрывая номер другого документа. Во всех примерах критерием успеха становится проверяемый признак, соразмерный конкретному решению, а не копия документа, из которой после получения зачеркнули лишнее.

Но финансовые системы быстро показывают пределы лозунга. Если человек открывает банковский счёт в юрисдикции, где действует процедура «знай своего клиента» (Know Your Customer, KYC), банк не может заменить обязанность установить личность абстрактной фразой «ему больше восемнадцати». Руководство Группы разработки финансовых мер борьбы с отмыванием денег (FATF) по цифровой идентификации, опубликованное в марте 2020 года, поясняет: цифровые решения в KYC применяются с учётом надёжности системы идентификации и риска финансовых отношений. Цифровая проверка — средство более точного соблюдения требований, а не способ уклониться от надлежащей проверки. При этом организация всё же может не собирать лишние признаки или проверять частное право через третью сторону, не раскрывая повторно все детали. Приватность не освобождает учреждение от обязанности; она требует знать, где обязанность начинается и где заканчивается аппетит к сбору.9

Это меняет и устройство конкуренции. Платформа, привыкшая под лозунгом «упрощённой проверки» собирать дату рождения, адрес и копию документа каждого пользователя, на деле создавала огромный и опасный информационный актив, который мог быть вовсе не нужен услуге. Каждую дополнительную запись приходится защищать, назначать срок хранения, объяснять её использование и, в зависимости от права, сообщать регулятору или людям об утечке. Информация из маркетингового

топлива превращается в обязательство на годы. Организация, принимающая лишь надёжное доказательство права, уменьшает поверхность атаки на данные, но всё равно обязана защищать доказательства проверки, ограничения сессий и сохраняемые события мошенничества. Экономика здесь не только в удалённой базе: учреждение выбирает собственную ответственность за знание до того, как та станет инцидентом безопасности.

Поэтому правила Европейского союза имеют практическое значение. Исполнительный регламент о европейских кошельках идентификации, принятый в ноябре 2024 года, говорит о передаче уполномоченным сторонам минимально необходимых данных и о разделении транзакций, ограничивающем их связывание. Запросы признаков и проверка запрашивающих сторон проектируются внутри известной рамки. Одной технологии мало, чтобы убедить бизнес не спрашивать имя. Регистрация и управление должны позволить выяснить, есть ли у стороны законное основание его требовать. Технический стандарт даёт средство; институциональное правило определяет, когда и в каких пределах им пользоваться.10

Остаётся социальное ограничение, которое не исчезнет от силы подписи. Что делать человеку без современного телефона? Тому, кто потерял устройство и закрытый ключ? Тому, кто не может получить исходный документ из-за расхождения данных реестра? Тому, кто не желает отдавать личный телефон работодателю? Система «приватности по замыслу» рискует стать новой дверью исключения, если окажется единственным путём к государственной услуге. Нужны признанные альтернативные каналы, безопасное восстановление, которое не отдаст удостоверение мошеннику через службу поддержки, механизм исправления ошибки источника и ясная ответственность за отклонение верного доказательства. Это не любезные гуманитарные дополнения к криптографической работе. Это условия исправности системы после выхода из лаборатории.

Организацию можно представить не как издателя фактов о людях, а как издателя вопросов. При каждом взаимодействии система спрашивает: вправе ли этот человек сделать это сейчас? Когда вопрос точен, можно сконструировать ограниченный ответ. Когда он расплывчат, список данных разрастается «на всякий случай». Поэтому первый шаг к услуге, уважающей приватность, — не выбор кошелька и не контракт с поставщиком криптографических доказательств, а разбор самого решения. Какой признак меняет исход? Кто уполномочен его удостоверить? Как долго он действителен? Достаточно ли знать, что признак существует, или требуется знать конкретного владельца, чтобы одно право не потребовали несколько раз?

Последний вопрос обнажает трудность проектирования пособий и однократных прав. Организация может хотеть убедиться, что заявитель имеет право получить помощь один раз, не создавая общий профиль, связывающий его действия в других сервисах. Простое доказательство «он имеет право» не мешает предъявить его десять раз. Можно создать псевдоним, ограниченный областью применения, или одноразовый токен

программы, если он не станет универсальным ключом слежения. Некоторые криптографические схемы поддерживают псевдонимы для заданной области; проект BBS рассматривает способы их получения. Но в государственной услуге необходимо совместно проверить предотвращение повторной выплаты, несвязываемость за пределами программы и право на исправление ошибки. Секретность без исполнения правила разрушит общественное доверие, а исполнение без границ — приватность.6

Бюджет раскрытия

Чтобы эти принципы не превратились в буклет по связям с общественностью, предлагаю предварительный инженерный тест — «бюджет раскрытия». Я не выдаю его за существующий регуляторный стандарт или результат опубликованного эксперимента; это проектная рамка, которую можно испытать. Сначала организация одним предложением формулирует требуемое решение. Затем для каждого признака отмечает необходимость, источник, кто видит исходное значение, кто — доказательство, срок хранения и возможность связать применения. После этого проводит два враждебных опыта: объединяет журналы условных проверяющих и ищет повторяющиеся связи; затем предполагает сговор одного из них с эмитентом и выясняет, можно ли по следу предъявления назвать держателя. Наконец, проверяет отзыв, потерю телефона, повторный запрос и отказ сети. Уменьшение числа полей не считается успехом, если следить стало возможно по другому постоянному следу.

Главной метрикой не может быть одна лишь доля пользователей, завершивших проверку. Следует измерять долю верных решений без лишнего раскрытия, долю отклонённых корректных доказательств, долю принятых ложных утверждений, время распространения отзыва, долю случаев вынужденного перехода к полному документу и вероятность связывания проверяющими в заданной модели угроз. Выборка должна включать недорогие устройства и пользователей разного возраста и цифрового опыта. Система может пройти криптографический тест и провалить проверку услуги. И наоборот: предельно удобный интерфейс иногда быстрее, чем бумага, наделяет доверием поддельное удостоверение.

По мере развития таких систем возникнет новый рынок, но не рынок «продажи новых личностей». На нём будут эмитенты, специализирующиеся на признаках, кошельки для защиты ключей держателя, проверяющие, управляющие политикой запроса, органы, задающие нормы доверия и ключи признанных учреждений, а также инструменты оценки приватности и устойчивости к мошенничеству. Создавать ценность стоит не вокруг знания всё большего о людях, а вокруг способности полагаться на меньшее знание. Поэтому недостаточно выпустить эффектное приложение со словами «децентрализованная идентичность». Кошелёк может лежать на телефоне пользователя, а все решения — зависеть от списка допуска, которым

единолично управляет оператор; или эмитент будет получать сигнал о каждом применении. Децентрализованного хранения мало, если контроль над решением остался централизованным.

Есть и философское искушение, которому стоит сопротивляться. Кто-то скажет: больше всего человека уважает система, которая вообще о нём ничего не знает. Но ответственной услуге иногда требуется достоверный факт и понятная возможность подотчётности. Цель не в том, чтобы каждый гражданин стал призраком, а в том, чтобы знание учреждения было соразмерно праву или риску, которым оно управляет. В одних дверях имя — законное условие, в других знание имени становится бесполезным вторжением. Ошибочно обещать, что доказательства с нулевым разглашением разрешат правовые и общественные противоречия. Их сила в другом: они расширяют пределы математически доказуемого без раскрытия всего свидетеля. А что доказывать, кому и кто вправе это требовать — вопросы, на которые одна криптография не ответит.

Институциональная скромность

Цифровое удостоверение Калифорнии рассказывает о частичном переходе от открытой карточки к требуемому признаку. Европейская попытка — о стремлении отделить выдачу доверия от наблюдения за его использованием; стадии разработки и внедрения здесь не следует выдавать за полную готовность. SD-JWT показывает, что выборочное раскрытие не обязательно делает удостоверение неотслеживаемым; разработки BBS предлагают более глубокую защиту самих следов предъявления, но требуют различать проект и окончательный стандарт. Рекомендации NIST напоминают: отзыв, защита ключа и ошибки — не примечания к идентичности, а часть её достоверности. Эти подходы не соревнуются за звание «самого зашифрованного». Они раскрывают слои проблемы, которую мы слишком долго прятали за фотографией удостоверения.

Возможно, такие технологии приведут системы к редкой добродетели — институциональной скромности. Сервис спрашивает ровно столько, сколько даёт ему право принять решение, и на этом останавливается. Тогда главным достижением станет не скрытое имя и не сложное доказательство, успешно обработанное быстрым процессором. Им станет способность учреждения отличить право проверить от любопытства знать. Десятилетиями мы учили устройства узнавать нас повсюду. Пора научить их более трудному: поверить нам в одном конкретном обстоятельстве, закрыть досье и оставить нам остальную жизнь.

Источники и литература

[1] California DMV, Mobile Driver's License FAQs — действующая официальная страница; проверена 9 ноября 2026 года.

[2] European Commission, Blueprint for an age verification solution — первая версия: июль 2025 года; вторая: октябрь 2025 года; о технической готовности объявлено в апреле 2026 года; страница обновлена 22 сентября 2026 года.

[3] W3C, Verifiable Credentials Data Model v2.0 — рекомендация W3C от 15 мая 2025 года.

[4] IETF, RFC 9901, Selective Disclosure for JSON Web Tokens — опубликованный RFC, ноябрь 2025 года; см. §§ 4 и 10.1.

[5] Goldwasser, Micali, Rackoff, The Knowledge Complexity of Interactive Proof Systems — SIAM Journal on Computing 18(1), февраль 1989 года.

[6] W3C, Data Integrity BBS Cryptosuites v1.0 — Candidate Recommendation Draft от 10 сентября 2026 года, не окончательная Recommendation.

[7] NIST, SP 800-63C, Digital Identity Guidelines: Federation and Assertions — окончательная Revision 4 за 2025 год; § 5.4 о кошельках под управлением подписчика.

[8] OpenID Foundation, OpenID for Verifiable Presentations 1.0 — окончательная спецификация 2025 года.

[9] FATF, Guidance on Digital ID — 6 марта 2020 года.

[10] European Commission, Implementing Regulation (EU) 2024/2982 — 28 ноября 2024 года; текст EUR-Lex.

[11] NIST, Zero-Knowledge Proof, Cryptographic Glossary — официальный терминологический источник; дата обращения: ноябрь 2026 года.