Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1254

(09/2012)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Управление определением идентичности

Структура гарантии аутентификации объекта

Рекомендация МСЭ-Т X.1254

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	**X.1250–X.1279**
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1254

Структура гарантии аутентификации объекта

Резюме

В настоящей Рекомендации определяются четыре уровня гарантии аутентификации объекта (т. е. LoA1 – LoA4); и критерии и угрозы для каждого из этих четырех уровней гарантии аутентификации объекта. Кроме того:

- определяется структура управления уровнями гарантии;
- на основе оценки риска приводятся руководящие указания по методам контроля, которые должны использоваться в целях смягчения угроз аутентификации;
- приводится руководство по преобразованию этих четырех уровней гарантии в другие схемы гарантии аутентификации; и
- приводится руководство по обмену результатами аутентификации, которые основаны на четырех уровнях гарантии.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1254	07.09.2012 г.	17-я

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

Многие электронные транзакции в системах на базе ИКТ или между ними должны осуществляться согласно требованиям безопасности, которые зависят от понимаемого или установленного уровня уверенности в идентичности участвующих объектов. Такие требования могут включать защиту активов или ресурсов от несанкционированного доступа, для чего может использоваться механизм контроля доступа, и/или обеспечение подотчетности на основе ведения журналов проверок соответствующих событий, используемую для целей учета и начисления платы.

В Рекомендации МСЭ-Т X.1254 представлена структура гарантии аутентификации объекта. Такая гарантия в рамках настоящей Рекомендации означает надежность всех процессов, действий по управлению и методов, используемых для установления идентичности объекта и управления определением его идентичности в целях использования в транзакциях аутентификации.

Рисунок 1 – Общее представление структуры гарантии аутентификации объекта

На основании четырех определенных уровней гарантии (LoA) в настоящей Рекомендации представлены руководящие указания по методам контроля, процессам и управлению, а также критериям гарантии, которые следует использовать для смягчения угроз аутентификации при реализации указанных четырех LoA. В Рекомендации также содержится руководство по приведению других структур гарантии аутентификации к этим определенным четырем уровням гарантии, а также руководство по обмену результатами транзакций, используемыми для аутентификации. В заключение в настоящей Рекомендации приводится подробное руководство по защите связанной с процессом аутентификации информации, позволяющей установить личность.

Настоящая Рекомендация предназначена для использования в основном поставщиками регистрационных данных (CSP) и теми, кто пользуется их услугами (например, полагающимися сторонами, оценщиками и аудиторами таких услуг). Данная структура гарантии аутентификации объекта (EAAF) определяет минимальные требования к технической части, процессам и управлению для четырех LoA для гарантии эквивалентности регистрационных данных, выпущенных различными CSP. Также приводятся некоторые дополнительные соображения относительно управления и организации, которые могут влиять на гарантию аутентификации объекта, но для этих соображений не устанавливаются конкретные критерии. Настоящая Рекомендация может оказаться полезной полагающимся сторонам (RP) и другим участникам для понимания того, что обеспечивает каждый из LoA. Кроме того, она может применяться в структуре доверия в целях определения технических требований к LoA. EAAF предназначена, в том числе, для применения в моделях, базирующихся на сеансах и ориентированных на работу с документами, с использованием различных методов аутентификации. Возможны сценарии как прямого, так и посреднического доверия, в рамках как двухсторонних, так и федеративных юридических групп.

Рекомендация МСЭ-Т X.1254

Структура гарантии аутентификации объекта[1]

1 Сфера применения

В настоящей Рекомендации представлена структура гарантии аутентификации объекта в конкретном контексте. В частности, в ней:

– определяются четыре уровня гарантии аутентификации объекта;

– определяются критерии и руководящие принципы обеспечения каждого из этих четырех уровней гарантии аутентификации объекта;

– представлено руководство по приведению других структур гарантии аутентификации к этим определенным четырем LoA;

– представлено руководство по обмену результатами аутентификации, которые основаны на четырех LoA;

– представлены руководящие указания по методам контроля, которые должны использоваться в целях смягчения угроз аутентификации.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенный в других документах:

3.1.1 утверждение (assertion) [b-ITU-T X.1252]: Констатация, сделанная объектом и не сопровождаемая доказательством ее истинности.

ПРИМЕЧАНИЕ. – Принято считать, что значения терминов "заявление" и "утверждение" являются весьма схожими, но несколько различаются. В настоящей Рекомендации "утверждение" является более сильным термином, чем "заявление".

3.1.2 аутентификация (authentication) [b-ISO/IEC 18014-2]: Обеспечение гарантии идентичности объекта.

3.1.3 фактор аутентификации (authentication factor) [b-ISO/IEC 19790]: Часть информации и/или процесс, используемые для аутентификации или верификации идентичности объекта.

ПРИМЕЧАНИЕ. – Факторы аутентификации подразделяются на четыре категории:

– нечто, имеющееся у объекта (например, подпись устройства, паспорт, аппаратное устройство, содержащее регистрационные данные, закрытый ключ);

– нечто, известное объекту (например, пароль, PIN-код);

– нечто, чем является объект (например, биометрические характеристики);

– нечто, что объект обычно делает (например, шаблон поведения).

3.1.4 заявление (claim) [b-ITU-T X.1252]: Констатация того, что дело обстоит именно таким образом, без возможности представить доказательства.

ПРИМЕЧАНИЕ. – Принято считать, что значения терминов "заявление" и "утверждение" являются весьма схожими, но несколько различаются. В настоящей Рекомендации "утверждение" является более сильным термином, чем "заявление".

---

[1] Республика Корея высказала оговорку и не будет применять настоящую Рекомендацию, поскольку настоящая Рекомендация противоречит осуществляемому в Корее регулированию в отношении требуемых четырех уровней гарантии аутентификации объекта и критериев достижения каждого из четырех уровней гарантии аутентификации объекта.

3.1.5 контекст (context) [b-ITU-T X.1252]: Среда с определенными граничными условиями, в которых существуют и взаимодействуют объекты.

3.1.6 регистрационные данные (credential) [b-ITU-T X.1252]: Набор данных, представляемых как доказательство утверждаемой или заявленной идентичности и/или прав.

ПРИМЕЧАНИЕ. – Дополнительные характеристики регистрационных данных см. в Дополнении I.

3.1.7 объект (entity) [b-ITU-T X.1252]: Что-либо, что существует отдельно и обособленно и может быть определено в каком-либо контексте.

ПРИМЕЧАНИЕ. – В настоящей Рекомендации термин "объект" также используется в конкретном случае для обозначения чего-то, заявляющего свою идентичность.

3.1.8 идентичность (identity) [b-ISO/IEC 24760]: Набор атрибутов, связанных с объектом.

ПРИМЕЧАНИЕ. – В конкретном контексте идентичность может содержать один или несколько идентификаторов, которые позволяют однозначно распознать объект в данном контексте.

3.1.9 многофакторная аутентификация (multifactor authentication) [b-ISO/IEC 19790]: Аутентификация с использованием по меньшей мере двух независимых факторов аутентификации.

3.1.10 предотвращение отказа от участия (non-repudiation) [b-ITU-T X.1252]: Способность защиты, в случае если один или несколько объектов, участвующих в каком-либо действии, не признают, полностью или частично, своего участия в этом действии.

3.1.11 непризнание участия (repudiation) [b-ITU-T X.1252]: Отрицание объектом, участвующим в каком-либо действии, своего участия во всем этом действии или его части.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 протокол аутентификации (authentication protocol): Определенная последовательность сообщений между объектом и верификатором, которая позволяет верификатору заверить идентичность объекта.

3.2.2 достоверный источник (authoritative source): Хранилище, признаваемое содержащим точную и актуальную информацию.

3.2.3 поставщик регистрационных данных (credential service provider) (CSP): Доверенный участник, который выпускает регистрационные данные и/или управляет ими.

3.2.4 гарантия аутентификации объекта (entity authentication assurance) (EAA): Степень доверия, достигаемого в процессе аутентификации, в том, что объект является тем, которым, как он утверждает, является, или тем, которым, как ожидается, он является (это определение основывается на определении "гарантии аутентификации", данном в [b-ITU-T X.1252]).

ПРИМЕЧАНИЕ. – Эта уверенность основывается на степени доверия к связи между объектом и представленной идентичностью.

3.2.5 идентификатор (identifier): Один или несколько атрибутов, которые уникально характеризуют объект в конкретном контексте.

3.2.6 верификация информации об идентичности (identity information verification): Процесс проверки информации о подлинности идентичности и регистрационных данных по издателям, источникам данных или другим внутренним или внешним ресурсам в отношении аутентичности, достоверности, правильности и связи с объектом.

3.2.7 проверка подлинности идентичности (identity proofing): Процесс, в рамках которого орган регистрации (RA) осуществляет сбор и верификацию информации, достаточной для идентификации объекта с определенным или предполагаемым уровнем гарантии.

3.2.8 атака через посредника (man-in-the-middle attack): Атака, при которой злоумышленник может читать, вставлять или изменять сообщения, которыми обмениваются две стороны, таким образом, что сторонам это остается неизвестно.

3.2.9 взаимная аутентификация (mutual authentication): Аутентификация идентичности объектов, в результате которой каждый объект убеждается в идентичности другого объекта.

3.2.10 фишинг (phishing): Мошенничество, при котором пользователь электронной почты обманом вынуждается раскрыть личную или конфиденциальную информацию, которую мошенник затем может незаконно использовать.

3.2.11 орган регистрации (registration authority) (RA): Доверенный участник, который устанавливает и/или осуществляет верификацию и гарантирует идентичность какого-либо объекта для CSP.

3.2.12 полагающаяся сторона (relying party) (RP): Участник, полагающийся на утверждение или заявление идентичности.

3.2.13 соль (salt): Открытое, часто случайное, значение, используемое в процессе хэширования.

ПРИМЕЧАНИЕ. – Также может называться "песок" (sand).

3.2.14 общий секрет (shared secret): Секрет, используемый при аутентификации и известный только объекту и верификатору.

3.2.15 метка времени (time stamp): Надежный переменный во времени параметр, указывающий момент времени относительно общей точки отсчета.

3.2.16 транзакция (transaction): Отдельное событие, происходящее между объектом и поставщиком услуг в целях достижения коммерческой или программной цели.

3.2.17 структура доверия (trust framework): Набор требований и обеспечивающих механизмов для сторон, обменивающихся подтверждающей идентичность информацией.

3.2.18 доверенная третья сторона (trusted third party) (TTP): Орган или его агент, который является доверенным для других участников в отношении определенных действий (например, связанных с безопасностью действий).

ПРИМЕЧАНИЕ. – Доверенная третья сторона является доверенной для объекта и/или верификатора для целей аутентификации.

3.2.19 период действия (validity period): Период времени, в течение которого идентичность или регистрационные данные могут использоваться в одной или нескольких транзакциях.

3.2.20 верификация (verification): Процесс проверки информации путем сравнения представленной информации с ранее подтвержденной информацией.

3.2.21 верификатор (verifier): Участник, который удостоверяет информацию, подтверждающую идентичность.

ПРИМЕЧАНИЕ. – Верификатор может участвовать в нескольких этапах EAAF и осуществлять верификацию регистрационных данных и/или подтверждающей идентичность информации.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CA	Certification Authority		Орган по сертификации
CSP	Credential Service Provider		Поставщик регистрационных данных
EAA	Entity Authentication Assurance		Гарантия аутентификации объекта
EAAF	Entity Authentication Assurance Framework		Структура гарантии аутентификации объекта
ICT	Information and Communications Technology	ИКТ	Информационно-коммуникационные технологии
IdM	Identity Management		Управление определением идентичности
IP	Internet Protocol		Протокол Интернет
LoA	Level of Assurance		Уровень гарантии
LoAs	Levels of Assurance		Уровни гарантии
MAC	Media Access Control		Управление доступом к среде передачи
NPE	Non-Person Entity		Объект, не являющийся физическим лицом

PDA	Personal Digital Assistant	Персональный цифровой ассистент
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PIN	Personal Identification Number	Персональный идентификационный номер
RA	Registration Authority	Орган регистрации
RP	Relying Party	Полагающаяся сторона
SAML	Security Assertion Markup Language	Язык разметки подтверждения безопасности
TCP/IP	Transmission Control Protocol/Internet Protocol	Протокол управления передачей/протокол Интернет
TLS	Transport Layer Security	Безопасность транспортного уровня
TPM	Trusted Platform Module	Модуль доверенной платформы
TTP	Trusted Third Party	Доверенная третья сторона
URL	Uniform Resource Locator	Универсальный указатель ресурса

5 Соглашения по терминологии

В настоящей Рекомендации применяются следующие глагольные формы для формулировки положений:

a) "должен" обозначает требование;

b) "следует" обозначает рекомендацию;

c) "разрешается" обозначает разрешение;

d) "может" обозначает возможность и способность.

6 Уровни гарантии

Структура гарантии аутентификации объекта (EAAF) определяет четыре уровня гарантии (LoA) при аутентификации объекта. Каждый LoA описывает степень уверенности в процессах, приводящих к аутентификации, включая сам процесс аутентификации, обеспечивая, таким образом, гарантию того, что объект, использующий конкретную идентичность (например, объекта), является тем самым объектом, которому эта идентичность была присвоена. Для целей настоящей Рекомендации LoA является функцией процессов, деятельности по управлению и технических средств контроля, реализуемых поставщиком регистрационных данных (CSP) на каждом из этапов EAAF, основываясь на критериях, установленных в разделе 10. Гарантия аутентификации объекта (EAA) зависит от управленческих и организационных факторов, однако в настоящей Рекомендации не предлагается конкретных нормативных критериев для определения таких факторов. Объект может быть как человеком, так и объектом, не являющимся физическим лицом (NPE).

Например, LoA сети может быть функцией уровней LoA всех компонентов, которые образуют эту сеть и могут включать NPE или оконечные устройства (например, мобильные телефоны, персональных цифровых ассистентов (PDA), приставки, ноутбуки). Следовательно, возможность отличить с некоторой степенью уверенности доверенное устройство от вредоносного является основной для EAAF.

LoA1 является низшим уровнем гарантии, а LoA4 – высшим уровнем гарантии. Определение того, каким должен быть надлежащий LoA в каждой конкретной ситуации, зависит от множества факторов. В основном определение требуемого LoA основывается на риске: последствия ошибки аутентификации и/или ненадлежащего использования регистрационных данных, причиненный в результате вред и воздействие, а также вероятность их возникновения. Более высокие LoA должны использоваться для более высокого воспринимаемого риска.

В EAAF приводятся требования и руководящие указания по реализации каждого из четырех LoA. В частности, изложены требования к реализации процессов для следующих этапов:

a) запись (например, проверка подлинности идентичности, верификация информации об идентичности, регистрация);

b) управление регистрационными данными (например, выпуск регистрационных данных, их активация);

c) аутентификация.

Представлены также руководящие указания относительно управленческих и организационных факторов (например, соответствие правовым нормам, управление информационной безопасностью), которые влияют на гарантию аутентификации объекта.

Уровни гарантии определены в таблице 6-1.

Таблица 6-1 – Уровни гарантии[2]

Уровень	Описание
1 – низкий	Слабая уверенность или отсутствие уверенности в утверждаемой или заявленной идентичности
2 – средний	Определенная уверенность в утверждаемой или заявленной идентичности
3 – высокий	Высокая уверенность в утверждаемой или заявленной идентичности
4 – очень высокий	Очень высокая уверенность в утверждаемой или заявленной идентичности

Настоящая структура содержит требования, позволяющие достигать желательного LoA для каждого этапа в структуре гарантии аутентификации объекта. Общим LoA реализации, достигнутым с помощью данной структуры, будет уровень этапа с низшим LoA.

6.1 Уровень гарантии 1 (LoA1)

На уровне LoA1 существует минимальная уверенность в утверждаемой или заявленной идентичности объекта, но существует некоторая уверенность в том, что объект остается тем же после нескольких последовательных событий аутентификации. Этот LoA используется, когда ошибочная аутентификация связана с минимальным риском. Особые требования к используемым механизмам аутентификации отсутствуют, они должны обеспечивать лишь некую минимальную гарантию. Требованиям к аутентификации с таким LoA могут удовлетворять большое число существующих методов, включая регистрационные данные, связанные с более высокими LoA. Этот уровень не требует использования методов криптографии (например, основанного на криптографии протокола типа "вызов-ответ").

Например, LoA1 можно применять для аутентификации, в которой объект представляет самостоятельно зарегистрированные имя пользователя и пароль на веб-сайте поставщика услуг для создания собственной страницы, или транзакции через веб-сайты, которые требуют регистрации для доступа к материалам и документам, таким как новости или документация по продуктам.

Например, на уровне LoA1 адрес управления доступом к среде передачи (MAC) может удовлетворять требованиям к аутентификации устройства. Однако в этом случае существует лишь незначительная уверенность в том, что другое устройство не сможет использовать тот же адрес MAC.

6.2 Уровень гарантии 2 (LoA2)

На уровне LoA2 существует определенная уверенность в утверждаемой или заявляемой идентичности объекта. Этот уровень используется, когда ошибочная аутентификация связана с умеренным риском. На этом уровне допустима однофакторная аутентификация. Успешная аутентификация должна зависеть от того, как объект, используя безопасный протокол аутентификации, доказывает, что он контролирует регистрационные данные. Должны присутствовать средства контроля, позволяющие уменьшить эффективность атак перехвата информации и подбора в режиме реального времени. Должны быть также реализованы средства контроля для защиты от атак, направленных на хранящиеся регистрационные данные.

Например, поставщик услуг может вести веб-сайт, который позволяет его клиентам изменять свой зарегистрированный адрес. Транзакция, в которой получатель изменяет зарегистрированный адрес, может относиться к транзакциям аутентификации LoA2, так как эта транзакция влечет умеренный

---

[2] LoA является функцией процессов, деятельности по управлению и технических средств контроля, реализуемых CSP на каждом из этапов EAAF, основываясь на критериях, установленных в разделе 10.

риск возникновения проблем. Поскольку официальные уведомления о суммах платежей, состоянии счета и данные об изменениях направляются на зарегистрированный адрес получателя, такая транзакция дополнительно влечет умеренный риск несанкционированного раскрытия PII. Вследствие этого поставщику услуг надлежит получить по крайней мере какую-то гарантию аутентификации до разрешения осуществления такой транзакции.

6.3 Уровень гарантии 3 (LoA3)

На уровне LoA3 существует высокая уверенность в утверждаемой или заявляемой идентичности объекта. Этот уровень используется, когда ошибочная аутентификация связана с существенным риском. На этом уровне должна использоваться многофакторная аутентификация. Процедуры проверки подлинности идентичности должны зависеть от верификации идентичности. Любая секретная информация, обмен которой осуществляется в рамках протоколов аутентификации, должна быть криптографически защищена при транзите и в состоянии покоя (хотя при LoA3 не требуется применять протокол вызов/ответ на криптографической основе). На этом уровне требования к созданию или хранению регистрационных данных не предусматриваются; эти данные могут храниться или создаваться в компьютерах общего назначения или в специализированном аппаратном оборудовании.

Например, для транзакции, в которой компания представляет в электронной форме определенную конфиденциальную информацию в государственное учреждение, может требоваться использование транзакции аутентификации LoA3. Неправомерное раскрытие информации привело бы к значительному риску или финансовым убыткам. Другие примеры транзакций LoA3 включают онлайновый доступ к счетам, который позволяет объекту выполнять определенные финансовые транзакции, или использование подрядчиком – третьей стороной удаленной системы для доступа к потенциально конфиденциальным персональным данным клиентов.

6.4 Уровень гарантии 4 (LoA4)

LoA4 характеризуется очень высокой уверенностью в утверждаемой или заявляемой идентичности объекта. Этот уровень используется, когда ошибочная аутентификация связана с высоким риском. На этом уровне обеспечивается наивысший уровень гарантии аутентификации объекта, определенный в настоящей Рекомендации. Уровень LoA4 схож с уровнем LoA3, но добавляются требования к личной проверке подлинности идентичности для объектов, являющихся людьми, и использование устойчивых к взлому устройств аппаратного обеспечения для хранения всех секретных или закрытых криптографических ключей. Кроме того, вся PII и другие конфиденциальные данные, включенные в протоколы аутентификации, должны быть криптографически защищены при транзите и в состоянии покоя.

Например, услуги, сопряженные с потенциально высоким риском причинения вреда или страданий, могут потребовать защиты LoA4. Ответственной стороне требуется полная уверенность в том, что определенная критически важная информация представлены надлежащим объектом, ответственная сторона может даже нести уголовную ответственность за любое непроведение верификации информации. Наконец, утверждение транзакции, связанной с высоким риском финансовых убытков, может быть транзакцией LoA4.

На уровне LoA4 могут использоваться цифровые сертификаты (например, МСЭ-Т X.509, сертификаты контролера карты (CV)) для аутентификации таких устройств NPE, как ноутбуки, мобильные телефоны, принтеры, факсы и другие устройства, подключенные к сети. Например, процесс регистрации смартфона может потребовать загрузки цифровых сертификатов на смартфон. При этом для предотвращения несанкционированного доступа к электросети при развертывании "умных" счетчиков могут использоваться цифровые сертификаты.

6.5 Выбор надлежащего уровня гарантии

Выбор надлежащего LoA следует осуществлять на основе оценки риска транзакций или услуг, для которых объекты будут проходить аутентификацию. Приводя уровни воздействия к уровням LoA, стороны транзакции аутентификации могут определить, какой LoA им необходим, и могут приобретать услуги и, соответственно, оказывать доверие гарантированным идентичностям. В таблице 6-4 показаны возможные последствия и воздействия неверной аутентификации на разных LoA.

Таблица 6-2 – Потенциальное воздействие на каждом уровне гарантии

Возможные последствия неверной аутентификации	Потенциальное воздействие неверной аутентификации в разбивке по уровню гарантии			
	1	2	3	4
Неудобство, подрыв репутации или ущерб для репутации или положения	Мин.*	Ум.	Сущ.	Выс.
Финансовые потери или ответственность организации	Мин.	Ум.	Сущ.	Выс.
Вред для организации, ее программ или для общественных интересов	Н/П	Мин.	Ум.	Выс.
Несанкционированное раскрытие конфиденциальной информации	Н/П	Ум.	Сущ.	Выс.
Личная безопасность	Н/П	Н/П	Мин. Ум.	Сущ. Выс.
Гражданские или уголовные правонарушения	Н/П	Мин.	Сущ.	Выс.
* Мин. – минимальный, ум. – умеренный, сущ. – существенный, выс. – высокий, Н/П – неприменимо.				

Определение того, что является минимальным, умеренным, существенным и высоким риском, обусловлено критериями риска, определенными организацией, использующей настоящую Рекомендацию, для каждого из возможных последствий. Наряду с этим возможно применять сценарии с несколькими видами воздействия (например, последствия могут включать вред для организации, а также несанкционированное раскрытие конфиденциальной информации). При сценариях с несколькими видами воздействия следует использовать наиболее высокий LoA, соответствующий последствиям.

Каждый LoA должен быть определен по силе и строгости способов контроля и процессов, которые CSP применяет к предоставляемым им услугам, для каждого этапа EAAF. EAAF устанавливает необходимость в эксплуатационных критериях гарантии обслуживания на каждом LoA для CSP. Критерии гарантии обслуживания представлены в разделе 11, но конкретные требования не входят в сферу применения настоящей Рекомендации.

Могут существовать иные факторы, связанные с коммерческой деятельностью, которые не относятся к области безопасности и которые следует учитывать при использовании результатов оценки риска для определения надлежащего LoA. Такие факторы могут включать:

a) подход организации к управлению остаточным риском;

b) готовность организации к допуску риска в отношении воздействий, указанных в таблице 6-2; и

c) коммерческие цели услуг (например, услуга, коммерческой целью которой является активизация потребления, может быть обеспечена более эффективно при низком LoA с использованием таких регистрационных данных, как пароль, если в организации применяются процессы, снижающие риск мошенничества, и организация готова допустить риск мошенничества).

Оценка риска транзакции может быть проведена в рамках общей оценки рисков информационной безопасности в организации (например, ISO/IEC 27001), и ее следует проводить согласно конкретной потребности в обеспечении безопасности предполагаемых транзакций. Оценка риска должна учитывать риски, связанные с EAA. Результаты оценки риска должны сравниваться с четырьмя LoA. Выбираться должен тот LoA, который в наибольшей степени соответствует результатам оценки риска.

Если предусматриваются несколько классов транзакций, возможно применять различные LoA к каждой транзакции или группе транзакций. Другими словами, в одной организации могут быть приняты несколько LoA в зависимости от конкретной рассматриваемой транзакции.

6.6 Приведение к LoA и функциональная совместимость LoA

В разных доменах LoA могут определяться по-разному. Эти LoA не обязательно поддерживают соответствие "один к одному" с LoA, описанными в настоящей структуре. Например, в одном домене может быть принята четырехуровневая модель, а в другом – пятиуровневая. Различные критерии в различных моделях аутентификации должны определяться по отдельности и широко распространяться.

Для обеспечения функциональной совместимости различных моделей LoA в каждом домене должно быть объяснено, как используемая в нем схема приведения соотносится с LoA, определенными в настоящей Рекомендации, посредством:

a) разработки четко определенной методики гарантии аутентификации объектов, включая четкое определение категорий LoA; и

b) публикации этой методики, для того чтобы организации, желающие вступить в совместные соглашения, могли ясно понимать процессы и терминологию друг друга.

Методика LoA должна учитывать и четко определять уровни LoA в терминах оценки риска, определяя качественно и количественно следующие факторы:

a) ожидаемые угрозы;

b) уровни воздействия (т. е. минимальный) в случае реализации угроз;

c) определение угроз, которые должны контролироваться на каждом LoA;

d) рекомендованные методы и процессы обеспечения безопасности, которые следует использовать при реализации средств контроля на каждом LoA, например определение регистрационных данных, которые должны храниться на аппаратном устройстве (например, смарт-карте) или определение требований для создания и хранения регистрационных данных;

e) критерии определения эквивалентности различных комбинаций факторов аутентификации с учетом как проверки подлинности идентичности, так и связанных регистрационных данных.

При приведении в соответствие различных моделей LoA можно использовать модель четырех уровней, приведенную в настоящем документе, и осуществить приведение к другим n-уровневым моделям. Такой метод позволил бы использующим разные модели гарантии аутентификации объединениям приводить их в соответствие с четырехуровневой моделью. Приведение в соответствие должно определять порядок обработки LoA, для которых не установлено соответствие и которые можно просто игнорировать или эффективно приравнять к ближайшему нижнему уровню (поскольку может не быть основания для присваивания более высокого LoA, если это не было особо определено заранее).

6.7 Обмен результатами аутентификации на основании четырех LoA

Участникам транзакций аутентификации (например, CSP, полагающимся сторонам) может потребоваться обмен информацией для завершения транзакции или действия.

Ниже приведен не исчерпывающий перечень таких действий:

a) разрешение полагающейся стороне выразить свои ожидания в отношении LoA, согласно которому должна проходить аутентификация объекта;

b) разрешение объекту или CSP показывать фактический LoA в своих ответах;

c) разрешение объекту или CSP заявлять об уровнях LoA, для которых он был сертифицирован в отношении возможности соответствия требованиям такого уровня.

Участники транзакции аутентификации должны прийти к согласию относительно протокола, семантики, формата и структуры информации, которая будет предметом обмена. Полагающейся стороне может потребоваться определить, будет ли она принимать какой-либо ответ аутентификации, чем-либо отличающийся от того, который был запрошен; и

В то время как цифровые сертификаты являются установленным способом передачи информации, касающейся гарантии соответствующих регистрационных данных, все чаще используются метаданные как метод передачи обменивающимися сторонами своих требований к гарантии. Класс Context, такой как класс контекста аутентификации в языке разметки подтверждения безопасности (SAML) в форме универсального указателя ресурса (URL), является широко используемым механизмом, позволяющим сторонам определять классы, связанные с гарантией аутентификации, в запросах и утверждениях аутентификации. Например, типичное утверждение, передаваемое от поставщика данных идентичности, может содержать следующую информацию: "Данный пользователь – Джон Доу, его адрес электронной почты – john.doe@example.com, и он прошел аутентификацию в данной системе по паролю".

В следующей далее части настоящей структуры описана схема, в которой устанавливаются процессы и требования для услуг, а также представлены угрозы и воздействия, связанные с аутентификацией объектов. В заключение приводится обзор потребностей в критериях гарантии обслуживания, с помощью которых можно оценивать услуги, с тем чтобы обеспечить присвоение надлежащего LoA для обеспечения услуг адекватного удостоверения.

7 Участники

Участниками в рамках данной структуры являются: объекты, CSP, RA, RP, верификаторы и TTP. Эти участники могут принадлежать к одной или разным организациям. Могут существовать разные отношения и возможности, определяемые числом организаций, включая общие или взаимодействующие компоненты, системы и услуги.

7.1 Объект

Объект может иметь идентичность, прошедшую аутентификацию. Возможность аутентификации объекта зависит от ряда факторов. В контексте настоящей структуры возможность аутентификации объекта подразумевает то, что объект был зарегистрирован и CSP выпустил для него соответствующие регистрационные данные и что был определен протокол аутентификации. В процессе аутентификации объект может удостоверять собственную идентичность. Также возможна ситуация, когда существует отдельная сторона, представляющая объект в целях аутентификации.

7.2 Поставщик регистрационных данных

Поставщик регистрационных данных (CSP) выпускает регистрационные данные или оборудование, программное обеспечение и связанные данные, которые можно использовать для создания регистрационных данных, и/или управляет ими. Примерами регистрационных данных, которые могут выпускаться или управляться CSP, являются пароли и биометрические характеристики. Примером оборудования и связанных данных (используемых для создания регистрационных данных), которые могут выпускаться или управляться CSP, являются смарт-карты, содержащие закрытые ключи. CSP может также выпускать данные (или управлять ими), которые можно использовать для аутентификации регистрационных данных. Если в качестве регистрационных данных используются пароли, то они могут быть значениями односторонней функции паролей. Если регистрационные данные основываются на информации с цифровой подписью, то CSP могут создавать сертификаты открытых ключей, которые будут использоваться верификаторами. Изданные и поддерживаемые CSP регистрационные данные, а также средства защиты, реализованные CSP, являются ключевыми факторами при определении того, какой LoA будет достигнут в процессе конкретной транзакции аутентификации (см. также п. 10.3).

Для каждого объекта должен быть выпущен один или более наборов регистрационных данных или средств для создания таких данных для последующей аутентификации. Регистрационные данные или средства для их создания обычно выпускаются только после успешного завершения процесса записи, по завершении которого объект регистрируется.

7.3 Орган регистрации

Орган регистрации (RA) устанавливает и/или заверяет идентичность объекта для CSP. Орган регистрации должен пользоваться доверием со стороны CSP, с тем чтобы выполнять процессы на этапе записи и регистрировать объекты таким способом, который позволяет дальнейшее присвоение регистрационных данных CSP.

Каждый RA должен выполнять какой-либо вид проверки подлинности идентичности или верификации информации об идентичности согласно установленной процедуре. Для того чтобы отличать определенный объект от остальных объектов, такому объекту обычно присваивается один или несколько идентификаторов, которые позволяют в дальнейшем распознавать объект в применимом контексте.

7.4 Полагающаяся сторона

Полагающаяся сторона (RP) – это участник, который полагается на заявление или утверждение об идентичности. Полагающейся стороне может требоваться аутентифицированная идентичность в различных целях, таких как управление учетными записями, контроль доступа, принятие решений об аутентификации и т. д. Полагающаяся сторона может сама выполнять операции, необходимые для аутентификации объекта, или поручать эти операции третьей стороне.

7.5 Верификатор

Верификатор – это участник, который подтверждает информацию об идентичности. Верификатор может участвовать в нескольких этапах EAA и выполнять верификацию регистрационных данных и/или верификацию информации об идентичности.

7.6 Доверенная третья сторона

Доверенная третья сторона (TTP) – это орган или его агент, результатам определенной деятельности которого доверяют другие участники (например, деятельности, связанной с безопасностью). В контексте настоящей структуры TTP доверяют объект и/или верификатор при аутентификации. Примерами TTP для целей аутентификации объектов могут служить органы сертификации и службы меток времени.

8 Этапы в структуре гарантии аутентификации объекта

В данном разделе представлена модель этапов и процессов EAA. Притом что некоторые модели EAA могут отличаться по структуре от данной модели, для соответствия этой модели требуется, чтобы функциональные возможности полностью удовлетворяли требованиям, установленным в настоящей структуре. Структура является нейтральной в отношении технологии.

Организации, принимающие настоящую структуру, должны установить политику, процедуры и возможности, обеспечивающие необходимые вспомогательные процессы, и выполнять требования, определенные в настоящей структуре. Они могут различаться в зависимости от роли, выбранной конкретной организацией, и, например, LoA, с которыми организация предоставляет регистрационные данные. Например, организация может выполнять следующие условия:

a) требования в отношении конкретных действий от лица организации или ее представителей, относящихся к определенным LoA;

b) требования в отношении внешней проверки или проверки третьими сторонами эксплуатационных характеристик организации в рамках настоящей EAAF;

c) политика, действия и возможности, необходимые для установления доверенного отношения к процессам, услугам и возможностям, обеспечиваемым организациями, которые принимают настоящую структуру.

8.1 Этап записи

Этап записи состоит из четырех процессов: заявка и инициация, проверка подлинности идентичности, верификация идентичности, а также ведение записей/регистрация. Эти процессы могут целиком выполняться одной организацией или включать различные отношения и возможности, обеспечиваемые разными организациями, включая общие или взаимодействующие компоненты, системы и услуги.

Требуемые процессы различаются по строгости, определяемой применяемым LoA. В случае записи объекта с LoA1 эти процессы минимальны (например, человек может нажать на кнопку "новый пользователь" на веб-странице и создать имя пользователя и пароль). В других случаях процессы записи могут быть расширены. Например, запись с LoA4 требует личной встречи объекта и RA, а также расширенной проверки подлинности идентичности.

8.1.1 Заявка и инициация

Этап записи инициируется различными способами. Например, он может инициироваться в соответствии с запросом, сделанным объектами, которые пытаются самостоятельно получить определенные регистрационные данные (например, когда новый пользователь веб-сайта хочет получить имя пользователя и пароль). Также возможна ситуация, когда процесс записи инициируется третьей стороной, выступающей от имени объекта, или самим CSP (например, удостоверение личности, выданное государственным органом, или пропуск сотрудника). Например, при высоких LoA заявки могут приниматься только в том случае, если за объект поручается третья сторона.

В любом случае процесс инициации этапа записи для людей может включать заполнение формы заявки. Эта форма должна содержать достаточную информацию для гарантирования однозначной идентификации объекта в данном контексте (например, регистрация полного имени, даты и места

рождения). Для NPE, таких как мобильное устройство, на этапе записи может потребоваться инициализация путем установки на этом устройстве регистрационных данных, которые позволяют осуществлять уникальную идентификацию устройства и получать настройки конкретно для этого устройства на основе профиля конфигурации с криптографической защитой.

CSP должны устанавливать условия, согласно которым производится запись и должны использоваться услуги, связанные с записью. Условия предоставления услуг, связанных с записью, могут устанавливаться в соответствии с той или иной основой доверия. В надлежащих случаях, прежде чем продолжать процессы записи, объектом или от его лица должны приниматься основания освобождения от ответственности или другие юридические положения.

8.1.2 Проверка подлинности идентичности и верификация информации об идентичности

Проверка подлинности идентичности – это процесс сбора и верификации информации, достаточной для идентификации объекта с определенным или предполагаемым уровнем гарантии. Верификация информации об идентичности является частью процесса проверки информации об идентичности и включает удостоверение подтверждающей идентичность информации с помощью издателей, источников данных и других внутренних или внешних ресурсов источников в отношении аутентичности, действенности, правильности и отношения к объекту. В зависимости от контекста для соответствия требованиям проверки подлинности идентичности может использоваться различная информация, подтверждающая идентичность (например, государственные удостоверения личности, водительские удостоверения, биометрическая информация, компьютерное свидетельство, свидетельство о рождении), выданная авторитетными источниками или утвержденная ими. Реальная подтверждающая идентичность информация, представленная для выполнения требований проверки подлинности идентичности, определяется в зависимости от конкретного LoA.

Проверка подлинности идентичности может включать физическую проверку представленных документов об идентичности для выявления возможного мошенничества, взлома или фальсификации. Проверка подлинности идентичности может также включать проверку с целью удостовериться, что идентичность используется в других контекстах (т. е. верифицирована другими RA). Чем выше LoA, тем строже должны быть требования к проверке подлинности идентичности. Кроме того, процесс проверки подлинности идентичности должен быть более строгим для объектов, утверждающих или заявляющих свою идентичность дистанционно (например, по каналу интернета), по сравнению с представлением идентичности на месте (например, личный контакт с RA).

Строгость требований к проверке подлинности идентичности основывается на задачах, которые предстоит решить для каждого LoA. На LoA1 единственной задачей является гарантия того, что данная идентичность является уникальной в данном контексте. Идентичность не должна быть связана с двумя разными объектами. На LoA2 выполняются две задачи. Во-первых, идентичность должна быть уникальной в данном контексте. Во-вторых, объект, к которому относится данная идентичность, должен существовать объективно, т. е. идентичность не должна быть фиктивной или намеренно подделанной в мошеннических целях[3]. Например, проверка подлинности идентичности человека на LoA2 может включать проверку записей о рождении и смерти для гарантии определенного происхождения (хотя это не доказывает того, что объект, владеющий свидетельством о рождении, является тем самым человеком, к которому это свидетельство относится). Аналогичным образом, проверка подлинности идентичности на LoA2 для NPE может включать использование серийного номера для перепроверки производителя.

LoA3 включает задачи LoA1 и LoA2, а также задачу верификации подтверждающей идентичность информации с помощью одного или нескольких авторитетных источников, таких как какая-либо внешняя база данных. Верификация подтверждающей идентичность информации показывает, что данная идентичность используется и относится к данному объекту. Однако отсутствует гарантия того, что подтверждающей идентичность информацией владеет реальный или законный обладатель идентичности. Для людей на LoA4 к задачам LoA3 добавляется еще одна задача – требование засвидетельствовать объект лично для защиты от имитации законного пользователя.

Процессы проверки подлинности идентичности на более высоком уровне LoA должны включать процессы на более низких LoA. Например, проверка подлинности идентичности на LoA3 подразумевает, что выполняются требования к средствам контроля идентичности на LoA1 и LoA2.

---

[3] Это не исключает использования псевдонимов.

Таблица 8-1 – Применение задач проверки подлинности идентичности к LoA

LoA	Описание	Задача	Средства контроля	Способ обработки[4]
LoA1 – низкий	Слабая степень уверенности или отсутствие уверенности в утверждаемой или заявленной идентичности	Идентичность уникальна в рамках контекста	Собственное утверждение или заявление	Локальный или дистанционный
LoA2 – средний	Определенная степень уверенности в утверждаемой или заявленной идентичности	Идентичность уникальна в рамках контекста, и объект, владеющий идентичностью, реально существует	Проверка подлинности идентичности путем использования подтверждающей идентичность информации из авторитетного источника	Локальный или дистанционный
LoA3 – высокий	Высокая степень уверенности в утверждаемой или заявленной идентичности	Идентичность уникальна в рамках контекста, объект, владеющий идентичностью, реально существует, идентичность верифицирована, идентичность используется в других контекстах	Проверка подлинности идентичности путем использования подтверждающей идентичность информации из авторитетного источника + верификация идентичности	Локальный или дистанционный
LoA4 – очень высокий	Очень высокая степень уверенности в утверждаемой или заявленной идентичности	Идентичность уникальна в рамках контекста, объект, владеющий идентичностью, реально существует, идентичность верифицирована, идентичность используется в других контекстах	Проверка подлинности идентичности путем использования подтверждающей идентичность информации из достоверного источника + верификация идентичности + личное присутствие объекта[5]	Только дистанционный

Необходимые средства контроля для защиты против угроз записи на LoA должны определяться с использованием средств контроля, перечисленных в п. 10.1.2.

Любая реализация EAAF основывается на (подмножестве) информации об идентичности объекта и источниках, которые доступны предполагаемым объектам и/или RA.

Надежность и точность этих регистрационных данных, информации об идентичности и источников определяют реальную гарантию, обеспечиваемую на этапе записи. Соответственно, лица, реализующие EAAF, должны тщательно оценивать гарантию, обеспечиваемую инфраструктурами (управления) идентичности, которые используются различными источниками и издателями, при принятии решения о том, на чьи регистрационные данные, подтверждающую идентичность информацию и/или источники следует полагаться при проверке подлинности идентичности и верификации информации об идентичности. Любая реализация EAAF должна включать публикацию документа (например, политики проверки подлинности идентичности, согласно описанию в п. 10.1.2.1), в котором приводится обзор подтверждающей идентичность информации, источников и/или издателей, на которых следует полагаться на этапе записи.

---

[4] Дистанционная проверка подлинности идентичности выполняется по сети и, следовательно, не предполагает физического присутствия объекта, в то время как локальная проверка подлинности идентичности выполняется таким способом, который требует физического присутствия объекта.

[5] Средство контроля засвидетельствованного личного присутствия применяется только к объектам, являющимся людьми.

8.1.3 Ведение записей/процесс записи

Это процесс, завершающий запись объекта. Именно в процессе ведения записей, который является частью этапа записи, создается запись. Эта запись должна включать информацию и документацию, которые были собраны (и могут быть сохранены), информацию о процессе верификации информации об идентичности, результаты этих шагов и другие соответствующие данные. Затем выносится и регистрируется решение о принятии, отклонении или передачи записи для дальнейшей проверки или иных последующих действий.

8.1.4 Регистрация

Регистрация – это процесс, в котором объект запрашивает использование услуги или ресурса. Хотя процесс регистрации обычно считается частью этапа записи и выполняется в конце этого этапа, он также может выполняться и позже. В отличие от других процессов в рамках записи, которые, скорее всего, необходимы лишь однажды, регистрация может требоваться, когда объект запрашивает доступ к каждой услуге или каждому ресурсу в первый раз.

8.2 Этап управления регистрационными данными

Этап управления регистрационными данными включает все процессы, относящиеся к управлению жизненным циклом регистрационных данных или средств для их создания, которые дают пользователю возможность участвовать в какой-либо деятельности или в каком-либо контексте. Этап управления регистрационными данными может включать все следующие процессы или их часть: создание регистрационных данных, выпуск регистрационных данных или средств для их создания, активацию регистрационных данных или средств для их создания, хранение регистрационных данных, аннулирование и/или уничтожение регистрационных данных или средств для их создания, обновление и/или замену регистрационных данных или средств для их создания и ведение записей. Некоторые из этих процессов зависят от того, размещены ли регистрационные данные на каком-либо устройстве аппаратного обеспечения.

8.2.1 Создание регистрационных данных

Процесс создания регистрационных данных охватывает все необходимые процессы для создания в первый раз регистрационных данных или средств для их создания. Эти процессы могут включать предварительную обработку, инициализацию и привязку.

8.2.1.1 Предварительная обработка регистрационных данных

Некоторые регистрационные данные или средства для их создания требуют предварительной обработки перед выпуском, например индивидуализации личных данных, если регистрационные данные адаптируются согласно идентичности объекта. Индивидуализация личных данных может принимать разные формы в зависимости от регистрационных данных. Например, индивидуализация смарт-карты, которая содержит регистрационные данные, может включать печать (на внешней стороне карты) или запись (на чипе карты) имени объекта, для которого была выпущена карта. Существуют также регистрационные данные, не требующие индивидуализации, например пароли.

8.2.1.2 Инициализация регистрационных данных

Инициализация регистрационных данных охватывает все шаги, гарантирующие, что какое-либо средство для создания регистрационных данных впоследствии сможет обеспечивать весь планируемый набор функций. Например, чип на смарт-карте может понадобиться для вычисления пар криптографических ключей, необходимых для поддержки последующего создания цифровых подписей. Аналогичным образом, смарт-карта может быть выпущена в "заблокированном" состоянии, что потребует PIN-кода в процессе активации.

8.2.1.3 Привязка регистрационных данных

Привязка – это процесс установления связи между регистрационными данными или средствами для их создания и объектом, для которого они были выпущены. Способ привязки и уверенность в созданной связи варьируются в зависимости от LoA. Например, в онлайновом режиме в случае привязки идентификатора постоянного псевдонима объекта к записи клиента объекта в рамках процесса привязки по безопасному каналу может быть передан первоначальный "код активации" через используемый только в течение сеанса зашифрованный куки-файл. Другой вариант – код активации может быть запрошен в конце процесса, по выполнении шага привязки объекта к постоянному идентификатору, с тем чтобы привязать постоянный идентификатор к записи клиента.

8.2.2 Выпуск регистрационных данных

Выпуск регистрационных данных – это процесс обеспечения объекта определенными регистрационными данными или средствами для их создания или установления иной связи между ними. Сложность этого процесса различается в зависимости от требуемого LoA. Для более высоких LoA он потребуется защищенная доставка аппаратного устройства (например, смарт-карты), содержащей регистрационные данные, и может потребоваться личная доставка. При более низких LoA процессом выпуска может быть простая отправка пароля или PIN-кода на физический или электронный почтовый адрес объекта.

Для NPE, таких как устройства, процессы выпуска при высоких LoA обычно начинаются, когда производитель устройств массово заказывает цифровые сертификаты, представляя CSP список уникальных идентификационных номеров устройств для каждого из цифровых сертификатов. CSP в своем ответе предоставляет производителю сертификаты и закрытые ключи в формате с криптографической защитой. В процессе производства производитель может встроить в каждое устройство цифровой сертификат, который создает уникальный идентификатор устройства.

8.2.3 Активация регистрационных данных

Активация регистрационных данных является процессом, в котором регистрационные данные или средства для их создания подготавливаются к использованию. Процесс активации может включать разнообразные меры, в зависимости от регистрационных данных. Например, регистрационные данные или средства для их создания могут быть "заблокированы" после их инициализации до момента их выпуска для объекта, для предотвращения промежуточного ненадлежащего использования этих данных. В некоторых случаях активация может включать "разблокировку" регистрационных данных (например, при использовании пароля). Регистрационные данные или средства для их создания могут также активироваться после приостановки, когда их действие было временно остановлено.

8.2.4 Хранение регистрационных данных

Хранение регистрационных данных – это процесс, при котором регистрационные данные или средства для их создания безопасно хранятся таким образом, который защищает их от несанкционированного раскрытия, использования, изменения или уничтожения. В хранении регистрационных данных участвуют объект, связанный с этими регистрационными данными, и действия, требуемые для защиты от несанкционированного использования этих данных.

Хранение регистрационных данных не обязательно включает защиту информации, используемой для проверки того, что регистрационные данные имеют законную силу, если эта информация не является частью регистрационных данных. Защита информации, такой как таблицы хэшированных паролей, необходимых для аутентификации, требуется на более высоких LoA.

8.2.5 Приостановка действия, аннулирование и/или уничтожение регистрационных данных

Аннулирование – это процесс, при котором действительность регистрационных данных окончательно прекращается. Приостановка – это связанный процесс, при котором действительность регистрационных данных временно приостанавливается. Аннулирование может использоваться во многих случаях. Аннулирование должно быть проведено в следующих случаях:

a) известно, что регистрационные данные или средства для их создания утеряны, украдены или иным способом раскрыты;

b) истек срок действия регистрационных данных;

c) более не существует основания для дальнейшего существования регистрационных данных (например, при оставлении работником работодателя);

d) регистрационные данные использовались для несанкционированных целей; или

e) были выпущены другие регистрационные данные для замены тех, которые подлежат аннулированию.

Время между уведомлением о событии, требующем аннулирования, и завершением процесса аннулирования определяется политикой организации. При более высоких LoA период, разрешенный для аннулирования, обычно короче. Некоторые виды регистрационных данных, такие как данные, содержащиеся на смарт-картах, после аннулирования могут уничтожаться физически. Однако информация, связанная с регистрационными данными, не всегда может быть уничтожена.

8.2.6 Возобновление и/или замена регистрационных данных

Возобновление – это процесс, при котором продляется срок действия существующих регистрационных данных. Замена – это процесс, при котором для объекта выпускаются новые регистрационные данные или средства для их создания, с тем чтобы заменить ранее использовавшиеся регистрационные данные, которые были аннулированы. Примером замены регистрационных данных может быть ситуация, когда CSP отправляет временный пароль на адрес электронной почты объекта, что позволяет объекту создать новый пароль после получения временного. Строгость процесса обновления и замены регистрационных данных может быть различной в зависимости от LoA.

8.2.7 Ведение записей

Ведение соответствующих записей должно осуществляться в течение всего жизненного цикла регистрационных данных. Если записи поддерживаются, то как минимум записи должны вестись для регистрации следующей информации:

a) факт создания регистрационных данных;

b) идентификатор регистрационных данных (в соответствующих случаях);

c) объект, для которого были выпущены регистрационные данные (в соответствующих случаях); и

d) статус регистрационных данных (в соответствующих случаях).

Записи должны вестись по каждому (применимому) процессу, входящему в этап управления регистрационными данными. Если регистрационные данные были выпущены для объектов-людей, то ведение записей, скорее всего, будет включать обработку PII. См. Дополнение I.

8.3 Этап аутентификации объекта

На этапе аутентификации объекта объект использует свои регистрационные данные, с тем чтобы удостоверить свою идентичность для RA. Процесс аутентификации касается исключительно установления (или неустановления) уровня уверенности в утверждении или заявлении об идентичности и не имеет какого-либо отношения к действиям, которые полагающаяся сторона может предпринять на основании этого утверждения или заявления.

8.3.1 Аутентификация

Процесс аутентификации включает использование протокола, доказывающего владение и/или управление регистрационными данными, для установления уверенности в идентичности. Требования к протоколу аутентификации варьируются в зависимости от применяемого LoA. Например, для низкого LoA аутентификация может включать использование пароля. На более высоком LoA аутентификация может включать использование криптографического протокола типа запрос-ответ. На еще более высоких LoA требуется многофакторная аутентификация. Не все факторы аутентификации обеспечивают одинаковую стойкость, поэтому для повышения уровня гарантии используются несколько факторов. См. раздел 10.

8.3.2 Ведение записей

Мониторинг событий и ведение записей об этих событиях на этапе аутентификации может потребоваться в различных целях, таких как обеспечение обслуживания, соответствие, учет и/или правовые нормы.

В случае участия объектов-людей информация, содержащаяся в этих записях, может включать конфиденциальную информацию. Управление этими записями должно осуществляться таким способом, который учитывает необходимость защиты и минимизации PII. См. также Дополнение I.

9 Соображения в отношении управления и организации

EAA зависит не только от технических факторов, но и от нормативных положений, договорных соглашений и соображений о том, как осуществляется управление предоставлением услуг и его организация. В отсутствие надлежащего управления и организации работы любое технически надежное решение может потерять свой потенциал обеспечения безопасности при обеспечении EAA.

Данный раздел носит информативный характер и содержит соображения организационного и управленческого характера, которые могут влиять на EAA. Конкретные критерии для каждого LoA не устанавливаются. Конкретные критерии и оценка соответствия в отношении организационных и управленческих соображений не входят в сферу применения настоящей Рекомендации, но их следует включать в структуру доверия.

9.1 Установление обслуживания

Установление обслуживания охватывает как юридический статус поставщика услуг, так и функциональный статус обеспечения обслуживания. Например, если известно, что поставщик услуг управления определением идентичности и аутентификации является зарегистрированным юридическим лицом, то это дает уверенность в том, что CSP является пользующейся доверием организацией в рамках своей юрисдикции. Важность этого возрастает, когда компоненты обслуживания управляются различными юридическими лицами (например, если регистрация является отдельной функцией).

Хотя основные требования являются одинаковыми для всех LoA, на более высоких LoA следует обеспечить бóльшую зависимость от полноты и надежности обслуживания. Например, на LoA3 и выше следует поддерживать более высокую гарантию относительно обеспечения обслуживания, в том числе с учетом знания корпоративных связей и понимания уровня независимости, разрешенного при операциях.

9.2 Соответствие правовым нормам и договорным условиям

Все участники EAAF должны понимать требования закона, возложенные на них в связи с организацией и предоставлением услуг, и обеспечивать соответствие этим требованиям. Это включает, в том числе, тип информации, которая может запрашиваться, порядок выполнения проверки подлинности идентичности и определение информации, которая может быть сохранена. Работа с PII является отдельной правовой проблемой (см. Дополнение I). Следует учитывать все юрисдикции, в рамках которых действуют участники. На LoA2 и выше должны быть определены также конкретные требования политики и договорные условия.

9.3 Финансовые положения

Если объект и полагающиеся стороны предполагают долгосрочную доступность услуг, то необходимо продемонстрировать финансовую стабильность, достаточную для гарантирования непрерывного обслуживания и соглашения о степени потенциальной ответственности сторон. Маловероятно, что такие положения будут рассматриваться для LoA1, но следует учитывать необходимость в них для услуг, обеспечивающих более значительные транзакции, при LoA2 и выше.

9.4 Управление информационной безопасностью и аудит

При LoA2 и выше участники EAAF должны обеспечивать документально оформленные практику управления информационной безопасностью, стратегии, подходы к управлению рисками и другие признанные средства контроля, с тем чтобы обеспечивать применение эффективных методов. При LoA3 и выше следует использовать официальную систему управления информационной безопасностью (например, [b-ISO/IEC 27000]).

В зависимости от соглашения о соответствии правовым нормам, договорным условиям и техническим характеристикам участники должны гарантировать, что стороны выполняют обязательства и могут обеспечить перспективу возмещения в случае их нарушения. При LoA2 и выше такая гарантия должна поддерживаться проверками безопасности, как внутренними, так и внешними, и безопасным хранением записей о важных событиях, включая эти проверки. Аудит может использоваться для проверки того, что методы участвующих сторон соответствуют соглашениям. В случае разногласий могут использоваться услуги разрешения споров.

9.5 Внешние компоненты обслуживания

Если организация привлекает для обеспечения части своих услуг третьи стороны, то общая гарантия обеспечения обслуживания будет зависеть от управления действиями этих сторон и надзора за ними. Содержание и масштаб договоренностей должны быть пропорциональны требуемому LoA и применяемой системе управления информационной безопасностью. При LoA1 такая гарантия должна оказывать минимальное воздействие, но на LoA2 и далее эти меры будут влиять на общий уровень обеспечиваемой гарантии.

9.6 Операционная инфраструктура

Для обеспечения крупномасштабных сетей доверия может использоваться та или иная структура доверия. В структуре доверия участники поддерживают информационные потоки между собой. В зависимости от соглашений возможно обращение к дополнительным участникам, с тем чтобы обеспечить выполнение всеми сторонами обязательств и перспективы возмещения в случае нарушения.

9.7 Измерение эксплуатационных характеристик

Директивные органы устанавливают технические и договорные требования в отношении структур доверия. Технические требования могут включать, например, уровни версий продукта, конфигурацию системы, настройки и протоколы, а договорные требования могут содержать правила честного использования информации. При установлении таких требований директивные органы должны включать в них критерии, по которым можно измерить потенциальные объекты структуры доверия. Вместо разработки таких критериев директивные органы могут пожелать использовать стандартные критерии, уже разработанные экспертами, например настоящую Рекомендацию. Чем шире директивные органы будут использовать стандартные критерии в различных структурах доверия, тем проще будет объектам согласованно понимать и применять эти критерии. Кроме того, имеющие имена наборы критериев могут служить в качестве условного обозначения различных степеней и типов строгости требований или возможностей для разных LoA.

10 Угрозы и средства контроля

В данном разделе описаны угрозы на каждом этапе структуры гарантии аутентификации объекта и определяются требуемые средства контроля на каждом LoA.

10.1 Угрозы и средства контроля на этапе записи

10.1.1 Угрозы на этапе записи

В таблице 10-1 определены и описаны угрозы на этапе записи.

Таблица 10-1 – Угрозы на этапе записи

Угроза	Примеры
Имитация законного пользователя	Примерами имитации законного пользователя является незаконное использование объектом подтверждающей идентичность информации другого объекта или при регистрации устройства в сети с использованием измененного адреса MAC.

10.1.2 Требуемые средства контроля по LoA для защиты от угроз на этапе записи

В таблице 10-2 определены требуемые средства контроля угроз на этапе записи в соответствии с LoA.

Таблица 10-2 – Средства контроля на этапе записи в соответствии с LoA

Угрозы	Средства контроля	Требуемые средства контроля			
		LoA1	LoA2	LoA3	LoA4
Имитация законного пользователя	Проверка подлинности идентичности: соблюдение политики	№ 1	№ 1	№ 1	№ 1
	Проверка подлинности идентичности: личная				№ 2
	Проверка подлинности идентичности: достоверная информация	№ 3	№ 4	№ 5	№ 6

ПРИМЕЧАНИЕ. – В вышеприведенной таблице идентификаторы №№ 1–6 соответствуют конкретным средствам контроля, требуемым для обеспечения защиты на каждом LoA. Каждое из этих средств контроля подробно описано в п. 10.1.2.1. Ячейки в таблице с диагональной линией показывают, что соответствующее средство контроля не применимо на указанном LoA.

10.1.2.1 Средства контроля угроз на этапе записи

Следующие средства контроля угроз на этапе записи соответствуют №№ 1–6, перечисленным в таблице 10-2.

Проверка подлинности идентичности: соблюдение политики

№ 1. Опубликование политики проверки подлинности идентичности и выполнение всех проверок подлинности идентичности в соответствии с опубликованной политикой проверки подлинности идентичности.

Проверка подлинности идентичности: личная

№ 2. Для людей должна использоваться личная проверка подлинности идентичности.

Проверка подлинности идентичности: достоверная информация

№ 3. Подтверждающая идентичность информация может быть самостоятельно заявленной или самостоятельно утверждаемой.

№ 4. Применяются следующие средства контроля:

- все средства контроля № 3;

  а кроме того:

- объект должен предоставить подтверждающую идентичность информацию не менее чем от одного достоверного источника подтверждающей идентичность информации, соответствующего политике.

a) Для людей

i) Личное представление:

- гарантировать, что объект владеет идентификационным документом, который получен не менее чем из одного достоверного источника подтверждающей идентичность информации, соответствующего политике, и который содержит фотографию владельца, соответствующую его внешности; и
- гарантировать, что представленный идентификационный документ выглядит подлинным, надлежащим образом выпущенным и является действительным на момент проверки.

ii) Неличное представление:

- объект должен предоставить свидетельство того, что он/она владеет информацией, подтверждающей личную идентичность, которая соответствует политике (примерами допустимой подтверждающей идентичность информации могут служить водительское удостоверение или паспорт); и
- существование и действительность предоставленных свидетельств должны быть подтверждены в соответствии с требованиями политики.

b) Для NPE:

- записать информацию из достоверного источника подтверждающей идентичность информации, такую как стандартное название, описание, серийный номер, адрес MAC, владелец, местоположение, производитель и т. д.

№ 5. Применяются следующие средства контроля:

- все средства контроля № 4;

а кроме того:

a) Для людей

i) Личное представление:

- проверить точность представленной в идентификационном документе контактной информации, используя ее для установления связи с объектом;
- проверить по крайней мере один идентификационный документ (например, свидетельство о рождении, браке или въезде), сравнив его с реестрами в соответствующем достоверном источнике;
- подтвердить личную информацию, сравнив ее с применимыми достоверными источниками информации и (если это возможно) источниками из других областей, достаточными для гарантии уникальной идентичности; и
- проверить информацию, предоставленную объектом ранее или, вероятно, известную только объекту.

ii) Неличное представление:

- гарантировать проверку доверенной третьей стороной утверждения или заявления объекта относительно текущего владения регистрационными данными LoA3 (или выше) из достоверного источника; и/или
- проверить информацию, предоставленную объектом ранее или, вероятно, известную только объекту.

b) Для NPE:

– доверенное оборудование (например, TPM) должно использоваться на LoA3;

– в случае уже использующихся NPE должна использоваться физическая запись регистрационных данных LoA3, выпущенных людьми, с помощью RA устройства. Если используется доверенное оборудование, оно должно быть разрешено к использованию;

– еще не приобретенное NPE должно заказываться с использованием аутентификации людьми с LoA3 или цифровой подписи для подтверждения того, что заказывающий объект имеет право заказывать NPE. RA производителя должен зарегистрировать NPE, допустить к использованию любое доверенное оборудование и проконтролировать выпуск и индивидуализацию NPE. Доверенное оборудование будет инициализировано при подключении к сети;
– для NPE, которые не являются компьютерами, привязка устройства, владельца, сети или оператора связи и органа регистрации должна быть криптографически защищена таким способом, который аналогичен используемому для доверенных компьютеров; и
– при использовании программного обеспечения код должен быть снабжен цифровой подписью, содержащей регистрационные данные, выданные человеком с LoA3 до выпуска, и должен быть подписан удостоверяющей подписью RA в доказательство того, что пройдена приемка перед вводом в использование.

№ 6. Применяются следующие средства контроля:

- все средства контроля № 5;

  а кроме того:

  a) Для людей
     – Объект должен представить подтверждающую идентичность информацию не менее чем от одного дополнительного соблюдающего политику авторитетного источника.
  b) Для NPE:
     – дополнительные устройства, подключенные к компьютеру, смартфону или аналогичному процессору, должны быть записаны во время выпуска, и должна существовать криптографическая привязка к главному устройству (например, разрешенному доверенному устройству, устройству чтения биометрических данных, смарт-карте, устройству геоаутентификации по GPS);
     – любые изменения в порядке выполнения привязки устройств должны осуществляться через орган регистрации; если это возможно, функция управления сетью должна предупреждать орган регистрации или службу управления сетью о любых изменениях во взаимосвязях устройств и предпринятых корректирующих мерах;
     – должна быть реализована возможность предотвращения вступления в силу любых изменений во взаимосвязях устройств; и
     – программный код с LoA4 должен быть снабжен цифровой подписью с LoA4, регистрационными данными, выданными человеком, и должен быть подписан удостоверяющей подписью RA в доказательство того, что пройдена приемка перед вводом в использование.

10.2 Угрозы и средства контроля на этапе управления регистрационными данными

10.2.1 Угрозы на этапе управления регистрационными данными

В таблице 10-3 перечислены угрозы на этапе управления регистрационными данными.

Таблица 10-3 – Угрозы при управлении регистрационными данными

Угроза	Примеры
Создание регистрационных данных: подделка	Злоумышленник изменяет информацию при ее прохождении от процесса записи к процессу создания регистрационных данных.
Создание регистрационных данных: несанкционированное создание	Злоумышленник побуждает CSP создать регистрационные данные, основываясь на информации о фиктивном объекте.
Выпуск регистрационных данных: раскрытие	Регистрационные данные, созданные CSP для объекта, копируются злоумышленником и переносятся от CSP к объекту во время установки регистрационных данных.

Таблица 10-3 – Угрозы при управлении регистрационными данными

Угроза	Примеры
Активация регистрационных данных: несанкционированное владение	Злоумышленник получает регистрационные данные, которые ему/ей не принадлежат, и маскируется под правомочный объект, побуждая CSP активировать эти регистрационные данные.
Активация регистрационных данных: недоступность	1 Объект, связанный с регистрационными данными или средствами для их создания, не находится в обычном местоположении и не может выполнить адекватную аутентификацию своей идентичности для CSP. 2 Доставка регистрационных данных или средств для их создания отсрочена, и активация в течение предписанного срока невозможна.
Хранение регистрационных данных: раскрытие	Регистрационные данные, хранящиеся в системном файле, становятся открытыми. Например, злоумышленник получает доступ к хранящимся записям имен пользователей и паролей.
Хранение регистрационных данных: подделка	Файл, который устанавливает соответствие регистрационных данных именам пользователей, становится открытым таким образом, что изменяется это соответствие, и существующие регистрационные данные заменяются регистрационными данными, к которым злоумышленник имеет доступ.
Хранение регистрационных данных: дублирование	Злоумышленник использует сохраненную информацию для создания дублированных регистрационных данных (например, дублируя смарт-карту, которая может генерировать регистрационные данные), которые могут использоваться неправомочным объектом.
Хранение регистрационных данных: раскрытие объектом	Объект хранит письменную запись своих имени пользователя и пароля в доступном для других лиц месте.
Аннулирование регистрационных данных: отсроченное аннулирование	Несвоевременное распространение информации об аннулировании позволяет объекту с аннулированными регистрационными данными воспользоваться аннулированными регистрационными данными для аутентификации до проведения проверки регистрационных данных и обновления последней информации об аннулировании.
Аннулирование регистрационных данных: использование после списания	Пользовательские учетные записи не удалены после увольнения сотрудника, что приводит к возможному ненадлежащему использованию старых учетных записей неправомочными лицами. – Регистрационные данные, хранящиеся в устройстве, используются после аннулирования их криптографических ключей.
Обновление регистрационных данных: раскрытие	Регистрационные данные, обновленные для объекта CSP, копируются злоумышленником во время передачи.
Обновление регистрационных данных: подделка	Новые регистрационные данные, созданные объектом, изменяются злоумышленником при представлении их CSP для замены устаревших регистрационных данных.
Обновление регистрационных данных: несанкционированное обновление	Злоумышленник может воспользоваться слабым протоколом обновления регистрационных данных, для того чтобы увеличить срок действия регистрационных данных для данного объекта. Злоумышленник обманывает CSP, побуждая его выпустить новые регистрационные данные для текущего объекта, и новые регистрационные данные привязывают идентичность текущего объекта к регистрационным данным, полученным от злоумышленника. Для NPE примером может быть повторная маркировка (повторный выпуск) системного компонента (например, RAM) как нового после его использования.
Ведение записей регистрационных данных: непризнание участия	Объект утверждает или заявляет, что законные регистрационные данные подделаны или содержат неверную информацию, для того чтобы ложно отрицать использование им этих регистрационных данных.

10.2.2 Требуемые средства контроля по LoA для защиты от угроз на этапе управления регистрационными данными

В таблице 10-4 определены требуемые средства контроля угроз на этапе управления регистрационными данными в соответствии с LoA.

Таблица 10-4 – Средства контроля при управлении регистрационными данными в соответствии с LoA

Угрозы	Средства контроля	Требуемые средства контроля			
		LoA1	**LoA2**	**LoA3**	**LoA4**
Создание регистрационных данных: подделка	Создание надлежащих регистрационных данных	№ 1	№ 1	№ 2	№ 2
	Только оборудование				№ 3
	Заблокированное состояние				№ 4
Создание регистрационных данных: несанкционированное создание	Отслеживание ресурсов	№ 5	№ 5	№ 5	№ 5
Выпуск регистрационных данных: раскрытие	Выпуск надлежащих регистрационных данных	№ 6	№ 7	№ 7	№ 8
Активация регистрационных данных: несанкционированное владение Активация регистрационных данных: недоступность	Активация объектом	№ 9	№ 9	№ 10	№ 11
Хранение регистрационных данных: раскрытие Хранение регистрационных данных: подделка Хранение регистрационных данных: дублирование Хранение регистрационных данных: раскрытие объектом	Безопасное хранение регистрационных данных	№ 12	№ 13	№ 14	№ 15
Аннулирование регистрационных данных: отсроченное аннулирование Аннулирование регистрационных данных: использование после списания	Безопасное аннулирование и уничтожение регистрационных данных	№ 16	№ 16	№ 16	№ 16
Обновление регистрационных данных: раскрытие Обновление регистрационных данных: подделка Обновление регистрационных данных: несанкционированное обновление	Безопасное обновление регистрационных данных	№ 17	№ 17	№ 18	№ 19
Ведение записей регистрационных данных: непризнание участия	Сохранение записей	№ 20	№ 20	№ 21	№ 21

ПРИМЕЧАНИЕ. – В вышеприведенной таблице идентификаторы №№ 1–21 соответствуют конкретным средствам контроля, требуемым для обеспечения защиты на каждом LoA. Каждое из этих средств контроля подробно описано в п. 10.2.2.1. Ячейки в таблице с диагональной линией показывают, что соответствующее средство контроля не применимо на указанном LoA.

10.2.2.1 Средства контроля угроз на этапе управления регистрационными данными

Следующие средства контроля угроз на этапе управления регистрационными данными соответствуют номерам, перечисленным в таблице 10-4.

Создание надлежащих регистрационных данных

№ 1. Применяются следующие средства контроля:

- Для создания регистрационных данных должны использоваться формализованные и документируемые процессы.
- Перед окончательной привязкой регистрационных данных к объекту, CSP должен получить адекватные гарантии того, что эти регистрационные данные привязаны и остаются привязанными к правильному объекту.

№ 2. Применяются следующие средства контроля:

- все средства контроля № 1;

  а кроме того:

- привязка регистрационных данных должна обеспечивать защиту от подделки. При этом используются:
  a) цифровые подписи; или
  b) механизмы, описанные в пункте "Заблокированное состояние", для регистрационных данных, хранящихся на устройстве.

Только оборудование

№ 3. Регистрационные данные должны храниться в модуле защиты оборудования[6].

Заблокированное состояние

№ 4. Регистрационные данные, хранящиеся в устройстве, по окончании процесса создания должны быть переведены в заблокированное состояние.

Отслеживание ресурсов

№ 5. Если регистрационные данные или средства для их создания находятся в устройстве, то это устройство должно храниться таким образом, который обеспечивает его физическую безопасность, и хранение этого ресурса должно отслеживаться. Например, неиндивидуализированные смарт-карты следует хранить в безопасном месте и их серийные номера должны быть записаны для защиты от кражи и последующих попыток создать несанкционированные регистрационные данные.

Выпуск надлежащих регистрационных данных

№ 6. Для выпуска регистрационных данных должны использоваться формализованные и документируемые процессы.

№ 7. Применяются следующие средства контроля:

- все средства контроля № 6;

  а кроме того:

- процесс выпуска должен включать механизм, с помощью которого гарантируется выдача регистрационных данных истинному объекту или санционированному представителю. Если регистрационные данные не выдаются лично, то должен использоваться механизм, с помощью которого проверяется существование адреса доставки и его законная связь с данным объектом.

№ 8. Применяются следующие средства контроля:

- все средства контроля № 7;

  а кроме того:

- если регистрационные данные не выдаются лично, то доставка должна производиться по защищенному каналу и объект или его санкционированный представитель должен подписывать документ, подтверждающий получение регистрационных данных.

Активация объектом

№ 9. Должна существовать процедура, гарантирующая, что регистрационные данные или средства для их создания активируются только под контролем соответствующего объекта. В отношении данной процедуры конкретных требований не предусмотрено.

№ 10. Должна существовать процедура, гарантирующая, что регистрационные данные или средства для их создания активируются только под контролем соответствующего объекта. Данная процедура должна подтверждать, что объект действительно обязан активировать регистрационные данные (например, протокол типа "вызов-ответ").

№ 11. Должна существовать процедура, гарантирующая, что регистрационные данные или средства для их создания активируются только под контролем соответствующего объекта. Такая процедура должна:

a) подтверждать, что объект действительно обязан активировать регистрационные данные (например, протокол типа "вызов-ответ"); и

b) предоставление возможности активации только в течение периода, определенного политикой.

---

6 Границы модуля защиты оборудования определены в стандарте ИСО/МЭК 19790:2012.

Безопасное хранение регистрационных данных

№ 12. Применяются следующие средства контроля:

- регистрационные данные, основанные на общем секрете, должны быть защищены средствами контроля доступа, ограничивающими доступ только теми администраторами и приложениями, для которых он требуется; и
- политика защиты хранящихся регистрационных данных должна быть описана в документации, относящейся к использованию регистрационных данных, которые предоставляются объекту.

№ 13. Применяются следующие средства контроля:

- все средства контроля № 12;

  а кроме того:

- такие файлы с общим секретом не должны содержать пароли или секреты, записанные открытым текстом; может использоваться альтернативный метод защиты общего секрета.

№ 14. Применяются следующие средства контроля:

- все средства контроля № 13;

  а кроме того:

- общие секреты должны быть защищены средствами контроля доступа, ограничивающими доступ только теми администраторами и приложениями, для которых он требуется. Такие общие секреты должны быть зашифрованы. Ключ шифрования для общего секрета должен быть сам зашифрован и должен храниться в криптографическом модуле (в аппаратном или программном оборудовании). Ключ шифрования для общего секрета должен расшифровываться только в тот момент, когда он требуется для операции аутентификации; и
- объекты или их уполномоченные представители должны подтверждать понимание этих требований и давать согласие на обеспечение защиты регистрационных данных в соответствии с этими требованиями.

№ 15. Применяются следующие средства контроля:

- все средства контроля № 14;

  а кроме того:

- объекты или их уполномоченные представители должны подписывать документ, подтверждающий понимание ими требований к хранению регистрационных данных, и давать согласие на обеспечение защиты регистрационных данных соответствующим образом.

Безопасное аннулирование и уничтожение регистрационных данных

№ 16. CSP аннулируют или уничтожают (если это возможно) регистрационные данные (включая основанные на общих секретах) в рамках конкретного срока, определенного политикой организации для каждого LoA.

Безопасное обновление регистрационных данных

№ 17. Применяются следующие средства контроля:

- CSP должен устанавливать адекватную политику обновления и замены регистрационных данных;
- объект должен представлять доказательство владения регистрационными данными, срок действия которых на текущий момент не истек, до того как CSP разрешит обновление и/или замену;
- пароли должны соответствовать минимальным требованиям политики CSP в отношении надежности и повторного использования паролей;
- по истечении срока действия регистрационных данных не должно разрешаться обновление; и
- любые взаимодействия должны осуществляться по защищенному каналу.

№ 18. Применяются следующие средства контроля:

- все средства контроля № 17;

  а кроме того:

- выполнение проверки подлинности идентичности на LoA2 согласно п 10.1.2.1 (Проверка подлинности идентичности: соблюдение политики; Проверка подлинности идентичности: достоверная информация).

№ 19. Применяются следующие средства контроля:

- все средства контроля № 17;

  а кроме того:

- выполнение проверки подлинности идентичности при LoA3 согласно п. 10.1.2.1 (Проверка подлинности идентичности: соблюдение политики; Проверка подлинности идентичности: достоверная информация).

Сохранение записей

№ 20. Запись о регистрации, истории событий и статусе всех регистрационных данных (включая аннулирование) должен вести CSP. Продолжительность хранения должна определяться политикой CSP.

№ 21. Применяются следующие средства контроля:

- все средства контроля № 20; и
- должны быть разработаны формализованные и документируемые процедуры обеспечения сохранности для каждой записи.

10.3 Угрозы и средства контроля на этапе аутентификации

10.3.1 Угрозы на этапе аутентификации

Угрозы на этапе аутентификации включают как угрозы, связанные с использованием регистрационных данных во время аутентификации, так и общие угрозы аутентификации. Общие угрозы аутентификации включают, в том числе, следующие угрозы: вредоносное ПО (например, вирусы, трояны, клавиатурные регистраторы), социальную психологию (например, подсматривание, кража аппаратных устройств и PIN-кодов), ошибки пользователей (например, ненадежные пароли, отсутствие защиты информации для аутентификации), ложное непризнание участия, несанкционированный перехват и/или изменение данных аутентификации во время передачи, отказ в обслуживании, ненадежность процедур. За исключением случая использования многофакторной аутентификации, средства контроля общих угроз аутентификации не входят в сферу применения настоящей Рекомендации. Данный раздел посвящен угрозам, связанным с использованием регистрационных данных для аутентификации, описанию этих угроз и перечислению средств контроля для каждого типа угрозы.

Описание конкретных средств контроля в терминах LoA на этапе аутентификации, исключая требование к использованию многофакторной аутентификации на LoA3 и LoA4, нецелесообразно. Не все средства контроля соответствуют всем контекстам. Например, средства контроля для аутентификации пользователей, получающих доступ к подписке на интернет-журнал, вероятно, отличаются от средств контроля, предназначенных для медицинских работников, получающих доступ к историям болезни. Поэтому, учитывая рост рисков и тяжести последствий расшифровки, поставщикам регистрационных данных рекомендуется тщательно оценивать состояние безопасности, (например разделять средства контроля по уровням в соответствии с операционной средой, приложениями и LoA). Решения о том, как, когда и в каком сочетании использовать эти средства, принимает разработчик системы на основе анализа рисков.

Существует большое число угроз в отношении регистрационных данных при их использовании для аутентификации. В таблице 10-5 перечислены некоторые широкие категории угроз, существующих при использовании регистрационных данных, и приводятся конкретные примеры для иллюстрации этих угроз.

Таблица 10-5 – Обзор угроз при использовании регистрационных данных на этапе аутентификации

Угроза	Примеры
Общие угрозы	Общие угрозы аутентификации включают множество категорий угроз, общих для любого типа ИКТ. Примерами являются клавиатурные регистраторы, методы социальной психологии и ошибки пользователей. За исключением случая использования многофакторной аутентификации средства контроля для общих угроз аутентификации не входят в сферу применения настоящей Рекомендации. Следует отметить, что многофакторная аутентификация не обеспечивает защиту от всех возможных общих угроз.
Подбор в реальном времени	Злоумышленник повторяет попытки входа в систему, пытаясь угадать возможное значение регистрационных данных.
Подбор без подключения	Секреты, связанные с созданием регистрационных данных, изучаются с использованием аналитических методов за рамками транзакции аутентификации. Взлом пароля часто основывается на методах перебора, таких как использование словарных атак. При словарных атаках злоумышленник использует программу, повторяющую все слова из словаря (или нескольких словарей разных языков), вычисляет хэш-значение для каждого слова и сверяет полученное хэш-значение со значением в базе данных. Другим способом взлома пароля является использование радужных таблиц. Радужные таблицы – это вычисленные заранее таблицы с точными парами текст – хэш-значение. Радужные таблицы работают быстрее, чем атаки по методу перебора, поскольку при этом используются функции редукции для уменьшения поискового пространства. После создания или получения радужные таблицы могут многократно использоваться злоумышленником.
Дублирование регистрационных данных	Регистрационные данные объекта или средства для их создания незаконно скопированы. Примером может служить несанкционированное копирование закрытого ключа.
Фишинг	Объект вовлекается во взаимодействие с подложным верификатором, и в результате у него обманным образом выведывается пароль или конфиденциальные личные данные, которые могут использоваться для маскировки под этот объект. Например, объект может получить письмо по электронной почте, которое перенаправляет его/ее на мошеннический сайт, где ему/ей предлагается войти в систему с использованием своего имени и пароля.
Подслушивание	Злоумышленник пассивно прослушивает транзакцию аутентификации в целях сбора информации, которую в дальнейшем можно использовать для активных атак, маскируясь под этот объект.
Атака повторного воспроизведения	Злоумышленник может заново воспроизвести ранее перехваченные сообщения (между правомочным пользователем и полагающейся стороной), для того чтобы пройти в качестве этого объекта аутентификацию с полагающейся стороной.
Взлом сеанса	Злоумышленник имеет возможность включить себя между объектом и верификатором после успешного аутентификационного обмена между этими двумя сторонами. Злоумышленник может выдать себя за объект перед полагающейся стороной или, наоборот, контролировать обмен данными в сеансе. Например, злоумышленник может получить контроль над сеансом, аутентификация которого уже выполнена, путем подслушивания или предсказания значения аутентификационных куки-файлов, используемых для пометки запросов HTTP, отправленных объектом.
Атака через посредника	Злоумышленник размещается между объектом и полагающейся стороной так, что может перехватывать и изменять содержимое сообщений протокола аутентификации. Как правило, злоумышленник выдает себя за полагающуюся сторону перед объектом и одновременно выдает себя за объект перед верификатором. Проведение активного обмена одновременно с обеими сторонами может позволить злоумышленнику использовать сообщения аутентификации, отправленные одной правомочной стороной в целях успешной аутентификации для другой стороны.
Кража регистрационных данных	Устройство, генерирующее или содержащее регистрационные данные, похищено злоумышленником.

Таблица 10-5 – Обзор угроз при использовании регистрационных данных на этапе аутентификации

Угроза	Примеры
Спуфинг и маскировка	Спуфинг и маскировка означают ситуации, когда злоумышленник выдает себя за другой объект, что позволяет ему выполнять действия, которые в противном случае были бы ему недоступны (например, получить доступ к недоступному иным образом активу). Это возможно осуществить, используя регистрационные данные объекта или другим способом выдавая себя за этот объект (например, подделав регистрационные данные). Например, злоумышленник, выдающий себя за какой-либо объект, подделывает одну или несколько биометрических характеристик, создавая "гуммированный" отпечаток пальца, который совпадает с образцом объекта; или злоумышленник подделывает адрес MAC, имея устройство, транслирующее адрес MAC, принадлежащий другому устройству, которое имеет разрешение работать в конкретной сети; или злоумышленник выдает себя за правомочного издателя программного обеспечения, ответственного за онлайновую загрузку и/или обновление программных приложений.

10.3.2 Требуемые средства контроля по LoA для защиты от угроз при использовании регистрационных данных

В таблице 10-6 определены требуемые средства контроля угроз при использовании регистрационных данных в соответствии с LoA.

Таблица 10-6 – Обзор средств контроля угроз при использовании регистрационных данных в соответствии с LoA

Угрозы	Средства контроля	Требуемые средства контроля				
		LoA*	LoA1	LoA2	LoA3	LoA4
Общие угрозы**	Многофакторная аутентификация				№ 1	№ 1
Подбор в реальном времени	Надежный пароль Блокирование регистрационных данных Использование учетной записи по умолчанию Аудит и анализ	№ 2 № 3 № 4 № 5				
Подбор без подключения	Хэшированный пароль с "солью"	№ 6				
Дублирование регистрационных данных	Противодействие фальсификации	№ 7				
Фишинг	Выявление фишинга по сообщениям Применение практики антифишинга Взаимная аутентификация	№ 8 № 9 № 10				
Подслушивание	Отсутствие передачи пароля Аутентификация с криптографической защитой Другой параметр аутентификации	№ 11 № 12 № 13				
Атака повторного воспроизведения	Другой параметр аутентификации Метка времени Физическая безопасность	№ 13 № 14 № 15				
Взлом сеанса	Сеанс с криптографической защитой Устранение уязвимостей протоколов Обмен сообщениями с криптографической защитой	№ 16 № 17 № 18				
Атака через посредника	Взаимная аутентификация Сеанс с криптографической защитой	№ 10 № 16				

Таблица 10-6 – Обзор средств контроля угроз при использовании регистрационных данных в соответствии с LoA

Угрозы	Средства контроля	Требуемые средства контроля				
		LoA*	LoA1	LoA2	LoA3	LoA4
Кража регистрационных данных	Активация регистрационных данных	№ 19				
Спуфинг и маскировка	Цифровая подпись кода Определение реальности	№ 20 № 21				
LoA* – эти средства контроля следует применять, если их необходимость обусловлена результатами оценки рисков. Общие угрозы** – Многофакторная аутентификация может противостоять не всем общим угрозам.						

ПРИМЕЧАНИЕ. – В вышеприведенной таблице идентификаторы №№ 1–21 соответствуют конкретным средствам контроля, требуемым для обеспечения защиты на каждом LoA. Каждое из этих средств контроля подробно описано в п. 10.3.2.1.

10.3.2.1 Средства контроля угроз при использовании регистрационных данных на этапе аутентификации

Следующие средства контроля угроз при использовании регистрационных данных на этапе аутентификации соответствуют №№ 1–21, перечисленным в таблице 10-6.

Многофакторная аутентификация

№ 1. Должны использоваться два или несколько наборов регистрационных данных, реализующих различные факторы аутентификации (например, что-то в сочетании с чем-то, что вы знаете).

Надежный пароль

№ 2. Должно требоваться использование надежных паролей (например, сложных строк не из словарей, содержащих комбинацию символов в верхнем и нижнем регистрах, цифр и специальных символов).

Блокировка регистрационных данных

№ 3. Должен использоваться механизм блокировки или приостановки после определенного числа неуспешных попыток ввода пароля.

Использование учетной записи по умолчанию

№ 4. Не должны использоваться имена пользователей и пароли учетных записей, заданных по умолчанию (например, в настройках производителя).

Аудит и анализ

№ 5. Должны использоваться журналы аудита неуспешных попыток входа для анализа методов подбора пароля в режиме реального времени.

Хэшированный пароль с "солью"

№ 6. Должен использоваться хэшированный пароль с "солью", с тем чтобы ограничить использование атак перебором и радужных таблиц.

Противодействие фальсификации

№ 7. На устройствах, содержащих регистрационные данные, должны быть реализованы меры противодействия фальсификации (например, голограммы, микропечать).

Выявление фишинга по сообщениям

№ 8. Должны быть реализованы средства контроля, специально разработанные для отслеживания фишинговых атак (например, фильтр Байеса, черные списки IP-адресов, фильтры по URL, эвристические структуры и отпечатки пальцев).

Применение практики антифишинга

№ 8. Для защиты объекта от фишинговых атак должны использоваться такие методы, как отключение изображений, отключение гиперссылок от сомнительных источников, обеспечение визуальных подсказок в почтовых клиентах.

Взаимная аутентификация

№ 9. Должна использоваться взаимная аутентификация.

Отсутствие передачи пароля

№ 11. Должны использоваться механизмы аутентификации, которые не передают пароли по сети (например, протокол "Kerberos").

Аутентификация с криптографической защитой

№ 12. Если в процессе аутентификации необходим обмен по сети, то данные должны быть зашифрованы до передачи.

Другой параметр аутентификации

№ 13. При каждой транзакции аутентификации должны использоваться разные параметры аутентификации (например, разовый пароль, сеансовые регистрационные данные).

Метка времени

№ 14. Каждое сообщение должно быть снабжено не подделываемой меткой времени.

Физическая безопасность

№ 15. Должны использоваться механизмы обеспечения физической безопасности (например, защита от вскрытия, обнаружение и реагирование).

Сеанс с криптографической защитой

№ 16. Должны использоваться сеансы с криптографической защитой.

Устранение уязвимостей протоколов

№ 17. Для устранения уязвимостей протоколов (например, TCP/IP) должны использоваться обновления операционной системы.

Обмен сообщениями с криптографической защитой

№ 18. Должен использоваться обмен сообщениями, основанный на криптографии (например, TLS).

Активация регистрационных данных

№ 19. При использовании регистрационных данных должно требоваться применение функции активации (например, ввод PIN-кода или биометрической информации в устройство, содержащее регистрационные данные).

Цифровая подпись кода

№ 20. Цифровые подписи должны быть верифицированы с использованием какого-либо доверенного источника для предотвращения загрузки программного обеспечения, измененного сторонами, не имеющими полномочий.

Определение реальности

№ 21. Должны применяться методы определения реальности для выявления использования искусственных биометрических характеристик (например, поддельных отпечатков пальцев).

11 Критерии гарантии обслуживания

Операторы, действующие в рамках структуры доверия и добивающиеся соответствия настоящей Структуре, должны установить конкретные критерии выполнения требований каждого LoA, которые они планируют обеспечивать, и должны оценить CSP, которые заявляют соответствие Структуры этим критериям. Аналогично, CSP должны определить LoA, на котором их услуги соответствуют настоящей Структуре, с помощью оценки своих общих рабочих процессов и технических механизмов на соответствие конкретным критериям.

Приложение A

Характеристики регистрационных данных

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

a) Регистрационные данные являются данными.

Регистрационные данные не включают каких-либо физических контейнеров или устройств, содержащих данные. Они также не включают средство для создания регистрационных данных. Таким образом, генератор пароля, а также смарт-карта, с помощью которой подписываются данные, ПО, которое создает цифровые подписи, или бумага, на которой что-либо написано, ни при каких условиях не являются частью регистрационных данных.

b) Регистрационные данные должны содержать данные, которые являются доказательством идентичности и/или определенного права.

Примерами таких доказательств являются:

1) нечто известное (например, неизменный пароль);
2) биометрические характеристики или представление аналогичных характеристик; или
3) данные, созданные чем-то, находящимся во владении (например, одноразовый пароль, созданный генератором паролей, данные, которые содержат цифровую подпись, созданную оборудованием или ПО с использованием закрытого ключа, которыми, как предполагается, должен владеть объект).

c) Регистрационные данные могут сопровождаться другими данными, которые могут быть полезными для процессов аутентификации и идентификации, но которые не являются частью реальных регистрационных данных.

Примерами таких данных могут быть имя объекта и сертификат открытого ключа. Они не являются необходимыми доказательствами идентичности или прав, но целесообразны в протоколах аутентификации. Связывание имени объекта с регистрационными данными подтверждает идентичность. Связывание сертификата открытого ключа с регистрационными данными дает информацию, которая помогает проверить доказательство, а также, возможно, дает информацию об идентичности или правах объекта.

d) Регистрационные данные могут также быть получаемыми регистрационными данными.

В этом случае такие получаемые регистрационные данные могут представлять собой подборку информации, получаемой на основе набора регистрационных данных, обычно создаваемых и направляемых объектом верификатору регистрационных данных для аутентификации. Например, для некоторых типов анонимной аутентификации объект преобразует регистрационные данные, предоставляемые CSP, в получаемые регистрационные данные, используемые для аутентификации.

e) Не все данные, являющиеся регистрационными данными, необходимо держать в секрете.

f) Регистрационные данные могут использоваться для аутентификации, идентификации или авторизации объекта или сочетания этих трех процедур.

g) Регистрационные данные должны быть верифицированы, перед тем как они могут быть приняты как подлинные и доверенные в рамках их конкретного назначения (например, аутентификация, идентификация, авторизация).

h) Для верификации регистрационных данных должны быть выполнены несколько шагов. Такими шагами могут быть шаги, перечисленные ниже.

1) проверка аутентичности регистрационных данных для гарантии того, что они были выпущены известным издателем;
2) подтверждение действительности и доверенности регистрационных данных (например определение того, существует ли прямая ссылка на корневого известного издателя от издателя регистрационных данных);
3) подтверждение точности вычислений математических/криптографических операций.

i) Регистрационные данные могут быть подлинными, но не действительными во всех контекстах (например, регистрационные данные на смарт-карте, такой как телефонная карта с предоплатой, могут быть подлинными, но могут действовать только для вызовов с использованием технических средств издателя).

Дополнение I

Конфиденциальность и защита PII

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Соответствие конкретного способа аутентификации конкретному использованию будет определяться не только по результатам оценки эффективности аутентификации, но также рисками и степенью их допустимости для участвующих организаций. Ненадлежащее использование или отсутствие адекватной защиты PII объектов влечет за собой значительные риски для организаций – от ущерба репутации до юридической ответственности. Поэтому следует тщательно оценивать и планировать использование PII для аутентификации и защиту PII. В данном Дополнении приведена руководящая информация, относящаяся к некоторым соображениям о конфиденциальности, которые должны учитываться организациями при принятии решения об использовании и реализации определенного способа аутентификации.

Если объекты являются физическими лицами, то большинство способов аутентификации будут включать обработку PII в процессе одного или нескольких следующих этапов:

a) на этапе записи при сборе, проверке подлинности и проверке данных идентичности и другой информации, относящихся к объектам;

b) при создании и выпуске регистрационных данных объектов и управлении этими данными;

c) при использовании регистрационных данных объектом и их верификации полагающимися сторонами и верификаторами.

Возможно организовать жесткую аутентификацию и прочную защиту конфиденциальности. Существует множество криптографически надежных способов аутентификации, которые имеют ограниченные негативные последствия для конфиденциальности (например, анонимные регистрационные данные, групповые подписи). Кроме того, следует отметить, что повышение уровня гарантии (например, LoA4 вместо LoA2) может, но необязательно должно отрицательно влиять на защиту личной информации. Многое будет зависеть от выбранного способа аутентификации и его реализации. При принятии таких решений каждая организация должна тщательно проанализировать необходимость защиты PII объектов, а также необходимость защиты их ресурсов и обеспечения подотчетности объектов в случае несанкционированных действий.

Большинство способов аутентификации включают использование отличительных идентификаторов, позволяющих однозначно отличить один объект от других возможных объектов в контексте аутентификации. Использование отличительных идентификаторов часто необходимо и для других задач, таких как управление учетными записями и ведение соответствующих журналов аудита. Основные вопросы конфиденциальности в связи с использованием отличительных идентификаторов касаются не использования этих отличительных идентификаторов как таковых, а, скорее, относятся к повторному использованию того же идентификатора в различных ситуациях. Например, номер учетной записи, присвоенный для одной цели, обычно считается менее уязвимым, чем государственный административный номер, используемый для нескольких целей (например, налоги, здравоохранение, пенсия). В некоторых случаях могут также существовать законодательные ограничения на использование определенных идентификаторов.

В свете вышесказанного, организациям следует реализовать эффективные меры по защите PII объектов на этапах и в процессах, определенных в настоящей EAAF. В частности, выбранный способ аутентификации должен быть разработан и реализован таким способом, который в целом сводит к минимуму обработку PII. Кроме того, использование отличительных идентификаторов, которые также используются в других контекстах и доменах, должно быть ограничено случаями, когда это необходимо и когда это разрешено в рамках соответствующей(их) юрисдикции(й).

Дополнительное руководство ИСО/МЭК по защите PII содержится в двух источниках:

a) В [b-ISO/IEC 29100] описаны базовые требования обеспечения конфиденциальности на основе трех основных факторов: 1) юридические и нормативные требования к мерам по защите конфиденциальности объектов и защите его/ее PII; 2) конкретные бизнес-требования и требования сценария использования; и 3) индивидуальные предпочтения в отношении конфиденциальности PII объекта. В [b-ISO/IEC 29100] описаны следующие базовые принципы конфиденциальности: согласие и выбор, определение цели, ограничение сбора, ограничение на использование, хранение и разглашение, минимизация данных, точность и качество, открытость, прозрачность и информация, личное участие и доступ, подотчетность, средства контроля безопасности, а также соответствие. Наряду с оценкой рисков для анализа угроз организации должны выполнять оценку воздействия выбранного способа аутентификации на конфиденциальность, с тем чтобы оценить, какие компоненты их систем потребуют особого внимания в аспекте мер по защите конфиденциальности.

b) В [b-ISO/IEC 29101] представлены руководящие указания по архитектуре систем ИКТ, обрабатываемых PII. Эта архитектура представляет собой выражение озабоченности и нескольких архитектурных подходов. Предусматривается набор компонентов для реализации систем на базе ИКТ, с тем чтобы установить надлежащий порядок обработки PII. Эта основа предназначена для использования с целью строительства системных архитектур, которые следуют принципам конфиденциальности, содержащимся в [b-ISO/IEC 29100].

Для получения более подробных руководящих указаний относительно требований, принципов и проектов систем в аспекте защиты PII читателям предлагается обращаться к вышеупомянутым стандартам.

Библиография

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности*.

[b-ITU-T Y.2702] Рекомендация МСЭ-Т Y.2702 (2008 г.), *Требования к аутентификации и авторизации для СПП варианта 1*.

[b-ITU-T Y.2720] Рекомендация МСЭ-Т Y.2720 (2009 г.), *Структура управления определением идентичности в СПП*.

[b-ITU-T Y.2721] Рекомендация МСЭ-Т Y.2721 (2010 г.), *Требования к управлению определением идентичности СПП и случаи применения*.

[b-ITU-T Y.2722] Рекомендация МСЭ-Т Y.2722 (2010 г.), *Механизмы управления определением идентичности в СПП*.

[b-ISO/IEC 9798] ISO/IEC 9798:2010, *Information technology – Security techniques – Entity authentication*.

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-ISO/IEC 19792] ISO/IEC 19792:2009, *Information technology – Security techniques – Security evaluation of biometrics*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management system – Requirements*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.

[b-ISO/IEC 29101] ISO/IEC 29101, *Information technology – Security techniques – Privacy architecture framework*.

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011, *Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-NIST SP800-36] NIST Special Pub 800-36 (2003), *Guide to Selecting Information Technology Security Products*.
<http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>

[b-NIST SP800-63] NIST Special Pub 800-63 (2006), *Electronic Authentication Guideline Version 1.0.2*.
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

[b-AGGPKI] *Australian Government Gatekeeper Public Key Infrastructure*.
http://www.gatekeeper.gov.au/

[b-DuD] Van Alsenoy B., and De Cock, D. (2008), *'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card', Datenschutz und Datensicherheit*, Vol.32, No.3, pp.178-183.

[b-EoI] New Zealand Standard: *Evidence of Identity Standard Version 2.0, 2009.* <http://www.dia.govt.nz/EOI/pdf/EOIv2.0.pdf>

[b-ENISA] ENISA, *Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0.*

[b-IAF] *Kantara Initiative Identity Assurance Framework v2.0.* http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework

[b-MOV] Menezes, A., van Oorschot, P., and Vanstone, S. (1997), *'Handbook of Applied Cryptography'*, pp. 3-4. <http://www.cacr.math.uwaterloo.ca/hac/>

[b-NeAF] *The National e-Authentication Framework.* <http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html>

[b-OECD] OECD (2007), *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication.* <http://www.oecd.org/dataoecd/32/45/38921342.pdf>

[b-OMB] OMB M-04-04 (2003), *e-Authentication Guidance for Federal Agencies* <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

[b-PEA] Industry Canada (2004), *Principles for Electronic Authentication: A Canadian Framework.* <http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2013 г.