МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO 21188

Первое издание
2006-05-01

Инфраструктура открытых ключей для сферы финансовых услуг. Практические приемы и структура политики

Public key infrastructure for financial services — Practices and policy framework

Ответственность за подготовку русской версии несёт GOST R (Российская Федерация) в соответствии со статьёй 18.1 Устава ISO

Ссылочный номер
ISO 21188:2006(R)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Опубликовано в Швейцарии

Содержание

Страница

1 Область применения 1

2 Нормативные ссылки 1

3 Термины и определения 2

4 Сокращенные термины 10

5 Инфраструктура открытых ключей (PKI) 11
5.1 Общие положения 11
5.2 Что такое PKI? 11
5.3 Влияние деловых требований на среду RKI 12
5.4 Функциональные перспективы 16
5.5 Деловые перспективы 21
5.6 Политика в области сертификатов (CP) 24
5.7 Положение о практике сертификации (CPS) 26
5.8 Взаимосвязь между политикой в области сертификатов и положением по практике сертификации 27
5.9 Соглашения 28
5.10 Отметка времени 29

6 Требования к политике в области сертификатов и положению по практике сертификации 30
6.1 Политика в области сертификатов (CP) 30
6.2 Положение по практике сертификации (CPS) 32

7 Задачи контроля органа по сертификации 33
7.1 Общие положения 33
7.2 Задачи контроля CA в области среды 33
7.3 Задачи контроля управления жизненным циклом ключей CA 36
7.4 Задачи контроля управления жизненным циклом ключа субъектов 37
7.5 Задачи контроля управления жизненным циклом сертификатов 38
7.6 Средства контроля управления жизненным циклом сертификатов CA 39

8 Процедуры контроля, используемые органом по сертификации 39
8.1 Общие положения 39
8.2 Средства контроля среды CA 40
8.3 Средства контроля менеджмента жизненного цикла ключа CA 55
8.4 Средства контроля менеджмента для жизненного цикла ключей субъекта 59
8.5 Средства контроля менеджмента жизненного цикла сертификата 64
8.6 Средства контроля менеджмента жизненного цикла сертификата CA 71

(Приложение A (информативное) **Менеджмент с помощью политики в области сертификации** 73

Приложение B (информативное) **Элементы положения по практике сертификации** 82

Приложение C (информативное) **Идентификаторы объектов (OID)** 100

Приложение D (информативное) **Процедура генерации ключа CA** 102

Приложение E (информативное) **Соответствие документа RFC 2527 документу RFC 3647** 106

Библиография 112

Предисловие

Международная организация по стандартизации (ISO) является всемирной федерацией национальных организаций по стандартизации (комитетов-членов ISO). Разработка международных стандартов обычно осуществляется техническими комитетами ISO. Каждый комитет-член, заинтересованный в деятельности, для которой был создан технический комитет, имеет право быть представленным в этом комитете. Международные правительственные и неправительственные организации, имеющие связи с ISO, также принимают участие в работах. ISO осуществляет тесное сотрудничество с международной электротехнической комиссией (IEC) по всем вопросам стандартизации в области электротехники.

Проекты международных стандартов разрабатываются согласно правилам, привёденным в Директивах ISO/IEC, Часть 2.

Основной задачей технических комитетов является подготовка международных стандартов. Проекты международных стандартов, принятые техническими комитетами, рассылаются комитетам-членам на голосование. Для публикации в качестве международного стандарта требуется одобрение не менее 75 % комитетов-членов, принявших участие в голосовании.

Следует иметь в виду, что некоторые элементы настоящего документа могут быть объектом патентных прав. ISO не несет ответственность за определение некоторых или всех таких патентных прав.

ISO 21188 был подготовлен Техническим Комитетом ISO/TC 68, *Финансовые услуги*, Подкомитетом SC 2, *Управление безопасностью и общие банковские операции*.

Введение

Организации и посредники создают специальные инфраструктуры с целью предоставления потребителям, корпорациям и государственным органам новых возможностей для проведения электронных финансовых операций. Поскольку объем электронных финансовых операций продолжает расти, новейшие технологии обеспечения безопасности с использованием цифровых подписей и систем полномочий могут стать частью процесса финансовых операций. Системы финансовых операций, включающие в себя новейшие технологии обеспечения безопасности, имеют свои требования по защите секретности, аутентичности и целостности финансовых операций, проводимых в сетях связи.

Индустрия финансовых услуг полагается на некоторые проверенные временем методы электронной идентификации, санкционирования и опознания объектов и защиты финансовых операций. Эти методы включают, но не ограничиваются ими, Персональные Идентификационные Номера (PIN) и Коды Аутентификации Сообщений (MAC) для розничных и оптовых финансовых операций, Идентификационные Данные (ID) пользователей и пароли для доступа к сети и компьютеру, а также распределение ключей для связности узлов сети. За последние двадцать лет в индустрии финансовых услуг разработаны процессы управления рисками и методики для поддержки использования этих процессов для финансовых применений.

Широкое использование Интернет-технологий в индустрии финансовых услуг и потребности этой индустрии в обеспечении безопасности, конфиденциальности и надежности финансовых операций и компьютерных систем привели к возникновению новейших технологий обеспечения безопасности, включающих криптографию с открытым ключом. Криптография с открытым ключом требует оптимизированной относительно бизнеса инфраструктуры технологии, менеджмента и политики (инфраструктуры с открытым ключом или PKI, как определено в этом документе) для удовлетворения требований электронной идентификации, опознания и санкционирования в финансовых системах. Использование стандартных методов электронной идентификации, опознания и санкционирования в PKI обеспечивает более устойчивую и предсказуемую систему безопасности и доверие к электронным сетям связи. Доверие может быть достигнуто тогда, когда можно установить соответствие стандартным методам.

Прикладные программы, обслуживающие индустрию финансовых услуг, можно разработать с цифровой подписью и возможностями PKI. Безопасность и отсутствие дефектов в этих прикладных программах базируются, в частности, на реализациях и методах, предназначенных для обеспечения общей целостности инфраструктуры. Пользователи основанных на полномочии систем, которые электронным способом связывают идентичность отдельных лиц и других объектов с криптографическими материалами (например, криптографическими ключами), выигрывают от стандартных систем управления рисками и главных, доступных проверке, методов, установленных в этом стандарте.

Члены Технического комитета 68 Международной организации по стандартизации взяли на себя обязательства в области технологий с открытым ключом и разрабатывают технические стандарты и инструкции, касающиеся цифровых подписей, управления ключами, управления сертификатами и кодированию данных. ISO 15782, Части 1 и 2, определяет систему управления сертификатами для финансовой индустрии, но не включает политику в этой области и требования к практике сертификации. Настоящий стандарт дополняет ISO 15782, Части 1 и 2, предоставляя структуру управления PKI через политику сертификации, операторов практики сертификации, контрольные цели и поддерживающие процедуры. Для тех, кто внедряет эти стандарты, степень, в которой любой объект финансовой операции может полагаться на реализацию стандартов, касающихся инфраструктуры с открытым ключом, и степень взаимодействия систем на базе PKI, использующих эти стандарты, частично будут зависеть от факторов, относящихся к политике и практике, установленных в настоящем документе

Инфраструктура открытых ключей для сферы финансовых услуг. Практические приемы и структура политики

1 Область применения

Этот международный стандарт устанавливает систему требований с целью управления PKI с помощью политики сертификатов и операторов практики сертификации и содействия использованию сертификатов с открытым ключом в индустрии финансовых услуг. Он также определяет контрольные цели и поддерживающие процедуры управления рисками.

Этот международный стандарт проводит различие между системами PKI в открытой, закрытой и контрактной средах. Далее, он определяет рабочие методы с контрольными целями в информационных системах индустрии финансовых услуг. Стандарт предназначен помочь тем, кто его реализует, определить практические методы PKI, которые могут поддерживать политику сертификатов, включающую использование цифровой подписи, удаленного аутентификации и шифрования данных.

Этот международный стандарт способствует реализации рабочих базовых методов управления PKI, которые удовлетворяют требованиям индустрии финансовых услуг в контрактной среде. Хотя стандарт ориентирован на контрактную среду, его применение в других средах не возбраняется. Применительно к этому документу термин «сертификат» относится к сертификатам открытого ключа. Сертификаты атрибутов не рассматриваются в этом стандарте.

Этот международный стандарт обращен к нескольким категориям пользователей, имеющим несхожие интересы, так что для каждой категории документ будет представлять различный интерес.

Менеджеры в бизнесе и аналитики — это те пользователи, которым нужна информация относительно использования технологии PKI в их развивающемся бизнесе (например, при электронной торговле), и им следует сосредоточиться на пунктах с 1 по 6.

Технические проектировщики и конструкторы — это те пользователи, которые создают свои политики сертификатов и положение(я) практики сертификации, и им следует сосредоточиться на пунктах от 6 до 8 и Приложениях с A до F.

Оперативное руководство и аудиторы — это те пользователи, которые отвечают за каждодневные операции PKI и подтверждение их соответствия этому документу, и им следует сосредоточиться на пунктах с 6 до 8.

2 Нормативные ссылки

Следующие ссылочные документы необходимы для использования данного документа. Для жестких ссылок применимо только указанное издание. Для плавающих ссылок применимо последнее издание ссылочного документа (включая все изменения).

Следующие ссылочные документы необходимы для использования данного документа. Для жестких ссылок применимо только указанное издание. Для плавающих ссылок применимо последнее издание ссылочного документа (включая все изменения).

ISO/IEC 7810, *Карточки идентификационные. Физические характеристики*

ISO/IEC 7811, *Карточки идентификационные. Методы записи* (Части 1—5)

ISO/IEC 7813, *Карточки идентификационные. Карточки финансовых операций*

ISO/IEC 7816, *Карточки идентификационные. Карточки на* микросхемах (Части 1—12 и 15)

ISO/IEC 9594-8:1995*, Информационные технологии. Взаимосвязь открытых систем. Директория: система понятий аутентификации*

ISO/IEC 9834-1:1993, *Информационные технологии. Взаимосвязь открытых систем. Процедуры для работы регистрационных органов в системе OSI: Часть 1. Общие процедуры и высшие разряды дерева идентификаторов объекта ASN.1*

ISO 10202, *Карточки банковские для финансовых операций. Архитектура безопасности систем финансовых операций, использующих смарт-карты.* (восемь частей)

ISO/IEC 10646-1, *Информационные технологии. Универсальный многооктетный набор кодированных знаков. Часть 1. Архитектура и основная многоязычная матрица*

ISO/IEC 15408, *Информационные технологии. Методы защиты. Критерии оценки для информационных технологий (три части)*

ISO 15782-1:2003*, Менеджмент сертификатов для финансовых услуг. Часть 1. Сертификаты с открытым ключом*

ISO 15782-2, *Банковское дело. Менеджмент сертификатов. Часть 2. Расширения сертификата*

ISO/IEC 17799, *Информационные технологии. Методы защиты. Свод правил по менеджменту информационной безопасностит*

ISO 18014-2, *Информационные технологии. Методы защиты. Услуги по созданию метки даты/времени. Часть 2. Механизмы создания независимых маркеров*

ISO 18014-3, *Информационные технологии. Методы защиты. Услуги по созданию метки даты/времени. Часть 3. Механизмы создания связанных маркеров*

ISO/IEC 18032, *Информационные технологии. Методы защиты. Генерация простых чисел*

ISO 18033, *Информационные технологии. Методы защиты. Алгоритмы шифрования* (Части 1—4)

3 Термины и определения

В данном документе используются следующие термины и определения.

3.1
данные активизации
activation data
значения данных, кроме ключей, которые нужны для функционирования криптографических модулей и которые должны быть защищены (например, PIN, фразой паролем, биометрической или поддерживаемой вручную частью ключа)

3.2
аутентификация
authentication
подтверждение идентичности, заявляемой лицом

a) при регистрации, акт оценивания мандатов конечных объектов (например, подписчиков), как свидетельство заявленной ими идентичности;

b) во время использования, акт сравнения электронного представления идентичности и мандатов (например, ID и пароль пользователя) с хранящимися значениями для доказательства идентичности

3.3
данные аутентификации
authentication data
информация, используемая для подтверждения заявленной идентичности объекта, например, личности, определенного ролевого имени, корпорации или организации

3.4
бюро карточек
card bureau
представитель **органа по сертификации** (**CA)** (3.18) или **органа по регистрации (RA)** (3.46) который персонализирует **карточку на микросхеме (ICC)** (3.32), содержащую (как минимум) личный ключ подписчика

3.5
владелец кредитной карточки
cardholder
субъект, которому была выдана карточка на микросхеме, содержащая пары секретных и открытых ключей и **сертификаты** (3.6)

3.6
сертификат
certificate
открытый ключ и идентичность объекта вместе с некоторой другой информацией, которую, как считается, нельзя подделать путем подписи информации в сертификате секретным ключом органа по сертификации, который выдал этот сертификат открытого ключа

3.7
приостановление сертификата
certificate hold
certificate suspension
приостановление действия **сертификата** (3.6)

3.8
эмитент сертификата
certificate issuer
организация, чье название находится в поле эмитента **сертификата** (3.6)

3.9
изготовитель сертификата
certificate manufacturer
агент, который выполняет задачи применения цифровой подписи в сертификате , подписывая требование от имени эмитента **сертификата** (3.6)

3.10
политика в области сертификатов
certificate policy
CP
определенный набор правил, который указывает применяемость сертификата к конкретному сообществу и/или классу применения с общими требованиями безопасности

3.11
профиль сертификата
certificate profile
спецификация требуемого формата (включая требования к использованию стандартных полей и расширений) для данного типа **сертификата** (3.6)

3.12
повторный ключ для сертификата
certificate re-key
процесс, с помощью которого объект с существующей парой ключей и **сертификатом** (3.6) получает новый **сертификат** для нового открытого ключа после генерирования новой пары ключей

3.13
возобновление сертификата
продление
certificate renewal
rollover
процесс, с помощью которого объекту выдается новый экземпляр существующего сертификата с новым сроком действия

3.14
перечень отмены сертификатов
certificate revocation list
CRL
перечень отмененных **сертификатов** (3.6)

3.15
услуга по подтверждению сертификата
certificate validation service
услуга, предоставляемая **CA** (3.18) или его агентом, который выполняет подтверждение срока действия **сертификата** (3.6) **стороне** (3.49), **использующей сертификат**

3.16
провайдер услуг по подтверждению сертификата
certificate validation service provider
CVSP
организация (3.29), которая предоставляет услугу по подтверждению сертификата потребителям со стороны, использующей сертификат

3.17
сертификация
certification
процесс создания сертификата с открытым ключом для **организации** (3.29)

3.18
орган по сертификации
certification authority
CA
организация, которой одна или несколько других организаций поручают создавать, присваивать, отзывать или оставлять у себя сертификат с открытым ключом

3.19
цепочка сертификации
certification path
заданная последовательность сертификатов организаций, которая, вместе с открытым ключом начальной организации в цепочке, может быть обработана с целью получения открытого ключа конечной организации в цепочке

3.20
положение по практике сертификации
certification practice statement
CPS
положение по практике, которое **орган по сертификации** (3.18) применяет при выдаче сертификатов, и в котором определяются оборудование, методика и процедуры, используемые **CA** для удовлетворения требований, заданных в заявлениях о политике сертификатов, поддерживаемых им

3.21
запрос о сертификации
certification request
представление запроса о подтверждении регистрации **органом по регистрации (RA)** (3.46), его агентом или подчиненным ему органом в **CA** (3.18) для регистрации открытого ключа подчиненного органа, помещаемого в **сертификате** (3.6)

3.22
ответ на запрос о сертификации
certification response
сообщение от **CA** (3.18), посылаемое после сертификации в ответ на запрос о сертификате

3.23
пригодность сертификата
certificate validity
validity
применяемость (годность к предназначенному использованию) и статус (действителен, приостановлен, отозван или истек) **сертификата** (3.6)

3.24
компрометация
compromise
нарушение безопасности системы, после которого может произойти несанкционированное раскрытие информации

3.25
перекрестная сертификация
cross certification
процесс согласно которому два **CA** (3.18) взаимно сертифицируют открытые ключи друг друга

ПРИМЕЧАНИЕ. Этот процесс может быть автоматическим.

3.26
криптографическое устройство
cryptographic hardware
cryptographic device
hardware security module
механический криптографический модуль

3.27
цифровая подпись
digital signature
криптографическое преобразование, при котором, когда он соединяется с блоком данных, обеспечиваются услуги по первоначальной аутентификации, интеграции данных и не отказу от подписавшего

3.28
конечная организация
end entity
субъект сертификата, который использует его секретный ключ не в целях подписи

3.29
организация
entity
CA (3.18), **RA** (3.46) или **конечная организация** (3.28)

3.30
журнал событий
контрольный журнал
event journal
audit journal
audit log
хронологические записи деятельности системы, которых достаточно, чтобы реконструировать, проанализировать и проверить последовательность условий и действий, происходивших вокруг или приведших к каждому событию на пути операции, начиная от ее отправной точки и кончая конечным результатом

3.31
функциональные испытания
functional testing
часть испытаний безопасности, при которых заявленные характеристики системы испытываются на правильность функционирования

3.32
карточка на микросхеме
integrated circuit card
ICC
карточка, в которую вставлен один или несколько электронных компонентов в виде микросхем для выполнения функций обработки и памяти

3.33
выпускающий орган сертификации
выпускающий CA
issuing certification authority
issuing CA
в контексте данного сертификата, выпускающий **CA** (3.18) — это **CA,** который выпускает сертификат

3.34
условное депонирование ключа
key escrow
управленческая функция, которая позволяет санкционированной стороне получить доступ к тиражированному секретному ключу шифрования

ПРИМЕЧАНИЕ. Может быть законным требование дать возможность официальным лицам правоприменительных органов получить доступ к секретному конфиденциальному ключу организации и/или CA.

3.35
восстановление ключа
key recovery
возможность восстановить секретный ключ или ключ симметричного шифрования организации из безопасного хранения в случае их потери, порчи или в том случае, когда по какой-либо другой причине они стали недоступными

3.36
многостороннее управление
multiple control
условие, при котором две или несколько сторон отдельно и конфиденциально владеют компонентами единственного ключа, так что, не будучи соединены, они не позволяют узнать полный криптографический ключ

3.37
идентификатор объекта
object identifier
OID
уникальная последовательность целых чисел, которая однозначно идентифицирует информационный объект

3.38
онлайновый механизм выяснения статуса сертификата
online certificate status mechanism
механизм, который позволяет **зависимым сторонам** (3.49) запрашивать и получать информацию о статусе сертификата без требования использовать **CRL** (3.14)

3.39
онлайновый протокол статуса сертификата
online certificate status protocol
OCSP
протокол для определения текущего статуса сертификата вместо проверки или в дополнение к ней по периодическому **CRL** (3.14), который устанавливает данные, подлежащие обмену между прикладной программой, проверяющей статус, и сервером, обеспечивающим этот статус

3.40
срок действия
operating period
период действия сертификата, начинающийся со дня и времени его выпуска в **CA** (3.18) (или, если указано в сертификате, с более позднего дня и времени), и заканчивающийся днем и временем его истечения или аннулирования

3.41
заявление о раскрытии информации PKI
PKI disclosure statement
документ, который дополняет **CP** (3.10) или **CPS** (3.20) путем раскрытия критической информации о политике и практике **CA** (3.18)/**PKI** (3.45)

ПРИМЕЧАНИЕ Заявление о раскрытии информации PKI является средством для раскрытия и подчеркивания информации, обычно подробно охватываемой связанными с ней документами CP и/или CPS. Следовательно, PDS не предназначено заменять CP или CPS.

3.42
орган по разработке политики
policy authority
PA
сторона или орган с конечными полномочиями определять **политику в области сертификатов** (3.10), обеспечивать практику и средства управления **CA** (3.18), как определено **CPS** (3.20), и полностью поддерживать установленную **политику в области сертификатов**

3.43
составление схемы политики
policy mapping
признание того факта, что, когда **CA** (3.18) одного домена сертифицирует **CA** другого домена, конкретная **политика в области сертификатов** (3.10) второго домена может быть рассмотрена полномочным органом первого домена, чтобы сделать ее эквивалентной (но необязательно идентичной во всех аспектах) конкретной **политике в области сертификатов** первого домена

ПРИМЕЧАНИЕ См. 3.25, перекрестная сертификация.

3.44
квалификатор политики
policy qualifier
зависимая от политики информация, которая сопровождает идентификатор **политики в области сертификатов** (3.10) в сертификате X.509

3.45
инфраструктура открытых ключей
public key infrastructure
PKI
структура, состоящая из аппаратного обеспечения, программного обеспечения, персонала, процессов и политики, которая использует технологию цифровой подписи для поддержки проверяемой связи между открытым компонентом пары асимметричных ключей и данным подписчиком, который владеет соответствующим секретным ключом

ПРИМЕЧАНИЕ Открытый ключ может быть предоставлен для проверки цифровой подписи, аутентификации субъекта коммуникационного диалога и/или обмена или согласования шифровального ключа для сообщений.

3.46
орган по регистрации
registration authority
RA
организация, которая несет ответственность за идентификацию и отождествление держателей сертификатов, но не является **CA** (3.18), и, следовательно, не подписывает и не выпускает сертификаты

ПРИМЕЧАНИЕ RA может оказывать помощь в процессе применения сертификата или в процессе отмены его или в том и другом случае. RA может не быть отдельным органом, а может быть частью CA.

3.47
запрос о регистрации
registration request
представление организацией в **RA** (3.46) [или **CA** (3.18)] для регистрации ее открытый ключ организации в сертификате

3.48
ответ на запрос о регистрации
registration response
сообщение, посылаемое **RA** (3.46) [или **CA** (3.18)] организации в ответ на ее запрос о регистрации

3.49
зависимая сторона
relying party
RP
получатель сертификата, который действует, будучи уверен в этом сертификате, цифровых подписях, проверяемых с использованием этого сертификата, или в том и другом случае

3.50
репозиторий
repository
система хранения и распределения сертификатов и относящейся к ним информации (то есть, хранение сертификатов, распределение сертификатов, **политика в области сертификатов** (3.10), статус сертификатов и т.д.)

3.51
корневой CA
root CA
CA (3.18) на вершине иерархии **CA**

3.52
сигнатурная верификация
signature verification
⟨в привязке к цифровой подписи⟩ точное определение: проверка того, что

a) цифровая подпись была создана в рабочий период действия сертификата секретным ключом, соответствующим открытому ключу, имеющемуся в **сертификате** (3.6);

b) сообщение не было изменено с момента создания цифровой подписи.

3.53
субъект
subject
организация, чей открытый ключ сертифицирован в сертификате

3.54
CA субъект
subject CA
CA (3.18), который сертифицирован выпускающим **CA,** и потому соответствует **политике в области сертификатов** (3.10) выпускающего **CA**

3.55
конечная организация — субъект
subject end entity
конечная организация, которая является субъектом **сертификата** (3.6)

3.56
подчиненный CA
subordinate CA
sub-CA
CA (3.18), который в иерархии **CA** стоит ниже другого **CA**

3.57
подписчик
subscriber
организация (3.18), оформившая подписку в органе по сертификации от имени одного или нескольких субъектов

3.58
вышестоящий CA
superior CA
CA (3.18), который в иерархии **CA** стоит выше другого [**подчиненного CA** (3.56)], но не корневой **CA**

3.59
свидетельствующий о попытке подделки
tamper evident
обладающий характеристикой, которая обеспечивает свидетельство о том, что была сделана попытка подделки

3.60
стойкий к попыткам подделки
tamper resistant
обладающий характеристикой, которая обеспечивает пассивную физическую защиту от попытки подделки

3.61
доверительная роль
trusted role
рабочая служба, выполняющая критические функции, которые, в случае их неудовлетворительного выполнения могут оказать отрицательное влияние на степень доверия, обеспечиваемого **CA** (3.18)

3.62
провайдер доверительных услуг
trust services provider
TSP
утвержденная организация (определенная сторонами контракта), обеспечивающая доверительные услуги с помощью ряда **органов по сертификации** (3.18) своим потребителям, которые могут действовать как подписчики или **зависимые стороны** (3.49)

ПРИМЕЧАНИЕ Провайдер доверительных услуг может также предоставлять услуги по проверке достоверности сертификата.

3.63
запрос службе подтверждения
validation service request
запрос **зависимой стороны** (3.49) в службу проверки юридической силы **сертификата** (3.6)