
**Руководящие указания для
идентификации объекта, имеющего
возможность взаимодействовать с
другим объектом, и связанных систем
аутентификации для предотвращения
контрафакции и незаконной торговли**

*Guidelines for interoperable object identification and related
authentication systems to deter counterfeiting and illicit trade*

ISO 16678:2014

<https://standards.iteh.ai/catalog/standards/sist/5043cee0-3a2b-4044-81ba-d21e69a8eb61/iso-16678-2014>



iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 16678:2014

<https://standards.iteh.ai/catalog/standards/sist/5043cee0-3a2b-4044-81ba-d21e69a8eb61/iso-16678-2014>



ДОКУМЕНТ ЗАЩИЩЁН АВТОРСКИМ ПРАВОМ

© ISO 2014

Все права сохраняются. Если не указано иное, никакую часть настоящей публикации нельзя копировать или использовать в какой-либо форме или каким-либо электронным или механическим способом, включая фотокопии и микрофильмы, без предварительного письменного согласия ISO по адресу, указанному ниже, или членом ISO в стране регистрации пребывания.

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

Предисловие	iv
Введение	v
1 Область применения.....	1
2 Термины, определения, аббревиатуры и акронимы.....	1
2.1 Термины и определения.....	2
2.2 Аббревиатуры и акронимы	4
3 Обзор.....	5
3.1 Общие положения	5
3.2 Системы идентификации объекта (в процессе работы).....	6
3.3 Системы идентификации объектов (настройка).....	7
4 Ключевые принципы доступа.....	9
4.1 Доступность и своевременность отклика.....	9
4.2 Один заслуживающий доверия источник.....	10
4.3 Менеджмент данных	10
4.4 Потребность в знаниях	10
4.5 Защита данных.....	10
4.6 Конфиденциальность.....	10
4.7 Соблюдение нормативных требований	10
4.8 Обследование.....	10
4.9 Операционная совместимость	11
4.10 Генерирование UID	11
5 Руководство.....	11
5.1 Введение	11
5.2 Определение трастовых услуг.....	12
5.3 Менеджмент данных и атрибутов идентификации объектов.....	13
5.4 Обычные виды мошенничества	15
Приложение А (информативное) Цифровой сертификат (для инспекторов)	18
Приложение В (информативное) Управление эталонными данными	21
Приложение С (информативное) Иллюстративные примеры реализации	22
Библиография.....	27

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 работает в тесном сотрудничестве с Международной электротехнической комиссией (IEC) по всем вопросам стандартизации в области электротехники.

Процедуры, использованные для разработки данного документа и предназначенные для его дальнейшей поддержки, описаны в Части 1 Директив ISO/IEC. В частности, должны быть указаны различные критерии утверждения, необходимые для различных типов документов ISO. Данный документ был разработан в соответствии с правилами редактирования Части 2 Директив ISO/IEC (см. www.iso.org/directives).

Необходимо обратить внимание на то, что некоторые элементы данного документа могут быть объектом патентных прав. ISO не должна нести ответственность за идентификацию каких - либо или всех таких патентных прав. Подробные сведения о каких – либо патентных правах, установленных при разработке данного документа, будут содержаться во введении и/или перечне ISO полученных патентных деклараций (см. www.iso.org/patents).

Любые торговые наименования, использованные в данном документе, предоставлены для удобства пользователей и не являются подтверждением.

Пояснение значений специальных терминов и выражений ISO, относящихся к оценке соответствия, а также информации относительно поддержки ISO принципов WTO в области технических барьеров в торговле.

Комитет, ответственный за данный документ – ISO/TC 247, *Контрмеры по предотвращению мошенничества и контроль*.

Введение

В данном Международном стандарте используются три основных предположения. Первое состоит в том, что обнаружение контрафакта является сложной и часто трудной задачей; второе – точное определение информации относительно рассматриваемого объекта упрощает процесс определения контрафакта; и третье – точная информация относительно идентичности часто бывает трудно воспринимаемой и её трудно найти.

Основная цель данного Международного стандарта состоит в упрощении доступа к точной информации относительно идентичности уполномоченных агентов (инспекторов) в процессе установления подлинности объектов.

Для достижения этой цели данный документ предоставляет руководство, предназначенное для облегчения поиска и использования информации, подтверждающей идентичность объекта. Данные и информация относительно идентичности могут быть найдены во многих местах, включая системы проверки и установления подлинности. Предоставление инспекторам помощи при поиске информации относительно идентичности помогает им определять фальсификацию. Это приводит к заключению, что:

Повышение операционной совместимости систем идентификации объектов и соответствующих систем аутентификации может облегчить использование этих систем инспекторами. Повышение простоты использования должно повысить применение инспекторами всего множества систем, содержащих точную информацию и, таким образом, повысить уровень обнаружения контрафакта и уменьшить потери, связанные с использованием контрафакта.

Данный Международный стандарт уделяет основное внимание вопросам маршрутизации запросов информации, относящейся к объектам, для соответствующих служб управления и затем направления ответов обратно инспекторам.

Системы идентификации объектов обычно используют Уникальные идентификаторы (UID) для ссылки на объекты информации или доступа к ним. В любом случае использование UID может повысить обнаружение контрафакта и подделки, хотя типы UID присваиваемые единичным вариантам могут быть более эффективны. Данный Международный стандарт включает шесть (6) основных разделов:

- **Область применения:** Определяет ограничения данного Международного стандарта как предназначенного для предоставления только руководства и рекомендаций. Какие-либо требования в данном стандарте отсутствуют.
- **Термины:** Определяет контекстуальные значения основных терминов при использовании в данном Международном стандарте, например “доверенный агент”, “инспектор”, и “семантическая интероперабельность”.
- **Обзор:** Общее описание способов использования информации относительно объектов для детектирования контрафакта.
- **Ключевые принципы:** Концепции и величины, рассматриваемые данным руководством.
- **Руководство:** Рекомендации, позволяющие улучшить взаимодействие систем, обеспечивающих предоставление информации об объектах инспекторам.
- **Информативные приложения:** Конкретные примеры, иллюстрирующие некоторые концепции данного Международного стандарта.

Желательные результаты

Чем больше решений в области валидации или аутентификации используется, тем более они эффективны при обнаружении и предотвращении незаконных действий, например контрафакта и

незаконных отклонений. Данный Международный стандарт предназначен для создания возможности надёжной и безопасной идентификации объектов в целях предотвращения попадания незаконных объектов на рынок.

Одна из целей данного Международного стандарта состоит в описании схемы работы, при которой совместно используются различные решения в области идентификации объектов и повышается надёжность, и которая в связи с этим используется наиболее часто. Эта структура должна также включать решения, которые просто обнаруживают некоторые варианты контрафакта без аутентификации продуктов. Аналогично, эта структура должна также включать решения, которые только выполняют оценку элемента аутентификации.

Поскольку мы также прогнозируем, что сами системы идентификации объектов также будут копироваться и быть объектом контрафакта, данный Международный стандарт устанавливает метод формального подтверждения, что удалённому описанию объекта можно доверять. Уделяется также внимание предотвращению взаимного влияния между различными независимыми вариантами реализации таких систем и разрешению использования и применения точно выраженных уникальных идентифицирующих ссылок на множественные варианты использования.

Теория, поддерживающая проектирование такой системы, состоит в том, что недостаток доверия и недостаток операционной совместимости приводит к 'разногласиям' между пользователями. При уменьшении этих разногласий будет достигнуто большая степень информированности и использования, и следовательно большая степень обнаружения и предотвращения нарушений законности.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO 16678:2014](https://standards.iteh.ai/catalog/standards/sist/5043cee0-3a2b-4044-81ba-d21e69a8eb61/iso-16678-2014)

<https://standards.iteh.ai/catalog/standards/sist/5043cee0-3a2b-4044-81ba-d21e69a8eb61/iso-16678-2014>

Руководящие указания для идентификации объекта, имеющего возможность взаимодействовать с другим объектом, и связанных систем аутентификации для предотвращения контрафакции и незаконной торговли

1 Область применения

Данный Международный стандарт содержит описание схемы идентификации и аутентификации систем. Он содержит рекомендации и руководство по практике наилучшего применения, что включает следующее

- последовательность и руководство выполнения
 - установление и проверка идентификаторов,
 - физическое выражение идентификаторов, и
 - необходимая внимательность исполнителей.
- проверка всех участников системы,
- взаимосвязь между уникальным идентификатором и возможными элементами аутентификации, связанными с ним,
- вопросы, связанные с идентификацией инспектора и любым утверждённым допуском к привилегированной информации относительно объекта, и
- история допуска инспектора (журналы).

В соответствии с этим данный Международный стандарт устанавливает схему и описание функциональных подразделений, выполняющих работы по обеспечению надёжности и взаимодействия таких систем.

Данный Международный стандарт не определяет специальные технические решения, но вместо этого содержит описания процессов, функций, и функциональных единиц, использующих общую модель для иллюстрации, какие решения имеются в целом.

Системы идентификации объектов могут включать другие функции и параметры, например относящиеся к прослеживанию цепочки поставок, проверка качества, рыночной активности, и другого, но эти аспекты не входят в область применения данного Международного стандарта.

ПРИМЕЧАНИЕ Данный Международный стандарт не применяется к специальным требованиям промышленности, например номерам глобальный номер предмета торговли.

2 Термины, определения, аббревиатуры и акронимы

Для целей данного документа применяются следующие термины и определения.

2.1 Термины и определения

2.1.1

система менеджмента данных атрибутов
attribute data management system
ADMS

система, предназначенная для хранения, управления и контроля доступа к относящимся к объектам данным

2.1.2

аутентификация
authentication

процесс поддержания объектов или атрибутов, с установленным или понятным уровнем гарантии

[ИСТОЧНИК: ISO/IEC 29115]

2.1.3

функция аутентификации
authentication function

функция, выполняющая аутентификацию

2.1.4

достоверный источник
authoritative source

источник официального происхождения атрибута несущий также ответственность за поддержание этого атрибута

2.1.5

сохраняемая копия
custodian copy

дубликат, подчинённый источнику полномочий [ISO 16678:2014](https://standards.iteh.ai/catalog/standards/sist/5043cee0-3a2b-4044-81ba-d21e69a8eb61/iso-16678-2014)

2.1.6

объект
entity

отдельно и обособленно существующий объект, который может быть идентифицирован в контексте

Примечание 1 для входа: Объект может быть человеком, организацией, физическим объектом, классом объектов, или невоспринимаемым объектом.

[ИСТОЧНИК: ISO/IEC 29115]

2.1.7

идентификация
identification

процесс опознавания атрибутов, которые идентифицируют объект

[ИСТОЧНИК: ISO/IEC 29115]

2.1.8

идентификатор
identifier

установленный набор атрибутов, присвоенных объекту для целей идентификации

2.1.9

идентичность
identity

набор атрибутов, относящихся к объекту

Примечание 1 для входа: Идентичность может иметь уникальные атрибуты, которые позволяют рассматривать объект отдельно от всех других объектов.

Примечание 2 для входа: Идентичность может рассматриваться в терминах, относящихся к человеку, организации, и объектам (физическим и не воспринимаемым).

2.1.10

инспектор **inspector**

любое лицо, выполняющее функцию проверки объекта с целью его оценки

Примечание 1 для входа: Любой участник системы может быть инспектором.

Примечание 2 для входа: Инспекторы могут иметь различные уровни квалификации и обучения.

Примечание 3 для входа: Инспектором может быть автоматическая система.

2.1.11

история доступа инспектора **inspector access history**

журналы доступа, содержащие подробные сведения о датах проверки уникальных кодов идентификатора (UID) , опционально каким (привилегированным) инспектором, и опционально из какого конкретного места

Примечание 1 для входа: Часто используются штампы с указанием времени.

2.1.12

взаимодействие с другим объектом **interoperability**

возможность одной точки входа направлять запросы относительно объектов, имеющих уникальные коды идентификатора (UID) в ответственный имеющий полномочия источник для выполнения функции доверительной проверки (TVF)

Примечание 1 для входа: Способность множественных систем аутентификации предоставлять аналогичные ответы группам пользователей.

2.1.13

объект **object**

любая единичная и отдельная сущность, которая может быть идентифицирована

2.1.14

функция проверки объекта **object examination function** **OEF**

процесс поиска или определения UID или других атрибутов предназначенных для аутентификации

Примечание 1 для входа: В этом процессе при оценке UID могут оказывать помощь другие атрибуты.

2.1.15

собственник **owner**

юридическое лицо, которое законно осуществляет функции контроля лицензирования, авторских прав пользователя, и распределения объектов, ассоциированных с данным UID

2.1.16

**участник
participant**

провайдеры решений относительно идентификации совместно используемых объектов и относящихся к ним систем аутентификации, а также группы пользователей этих объектов и систем, включая, но не ограничиваясь этим, правообладателей, таможенных инспекторов, дистрибьюторов, и потребителей

2.1.17

**семантическая операционная совместимость
semantic interoperability**

способность двух или более систем или служб автоматически интерпретировать и использовать информацию, которая была получена при точном обмене

2.1.18

**синтаксическая операционная совместимость
syntactic interoperability**

способность двух или более систем или служб обмениваться структурированной информацией

2.1.19

**функция обработки достоверного запроса
trusted query processing function**

TQPF

функция, предоставляющая межсетевой интерфейс функции доверенной верификации (TVF) и системе данных менеджмента атрибутов (ADMS)

Примечание 1 для входа: Это включает программное обеспечение, работающее локально на ручных устройствах.

2.1.20

**функция доверительной проверки
trusted verification function**

TVF

функция, выполняющая проверку действительности полученного UID, и управление ответом в соответствии с правилами и привилегиями доступа

2.1.21

**уникальный идентификатор
unique Identifier**

UID

код, соответствующий единичному и специальному набору атрибутов, относящемуся к определённому объекту или классу объектов в течение их существования в определённом домене и области системы идентификации объектов

2.1.22

**проверка
verification**

проверка, что UID существует и действителен в системе идентификации объектов

Примечание 1 для входа: Проверка может обнаруживать некоторые типы ложных данных, но сама не доказывает аутентичность объекта.

2.2 Аббревиатуры и акронимы

ADMS	Система менеджмента данных атрибутов
AI	Идентификатор применения (см. MH10.8.2)
CA	Орган сертификации
DI	Идентификатор данных (см. MH10.8.2)

OEF	Функция проверки объекта
RFF	Функция форматирования отклика
TQPF	Функция обработки доверительного запроса
TVF	Функция доверительной проверки
UID	Уникальный идентификатор

3 Обзор

3.1 Общие положения

Преимущество интероперабельности данных систем состоит в повышении возможности обнаружения контрафакта и мошенничества следующими средствами

- увеличением использования специальными группами пользователей,
- повышением числа контролируемых объектов,
- увеличением доступа к надёжным источникам, и
- снижением расходов:
 - обучением;
 - оборудованием;
 - развитием;
 - развёртыванием;
 - временем проверок.

Если возможность взаимодействия с другими системами достигнута и эти системы широко развёрнуты, инспектор может использовать идентификатор для выполнения запросов относительно объекта в целях обеспечения руководства решениями о развитии, относящимися к объекту. Инспектор должен получить надёжные свидетельства, что информация, предоставленная по запросам точная и заслуживающая доверия.

Всем участникам рекомендуется выполнять свои роли с необходимым вниманием.

- Необходимо выполнение аудита и проверки провайдеров услуг для обеспечения гарантии, что их работа заслуживает доверия и отсутствуют агенты действующие незаметно по принципу “поддержания видимости”.
- Проведение аудита и проверки производителей должно рассматриваться как гарантия, что их работа соответствует документально оформленным процессам и в системы передаётся точная информация.
- Заинтересованные стороны, имеющие потребность в информации, должны получать точные данные по запросам относительно процесса, таким образом, чтобы правообладатель мог выпустить информацию с соблюдением социальной ответственности.

3.2 Системы идентификации объекта (в процессе работы)

3.2.1 Общие положения

Системы идентификации объектов обычно состоят из функциональных блоков, показанных на схеме модели (Рисунок 1) ниже.

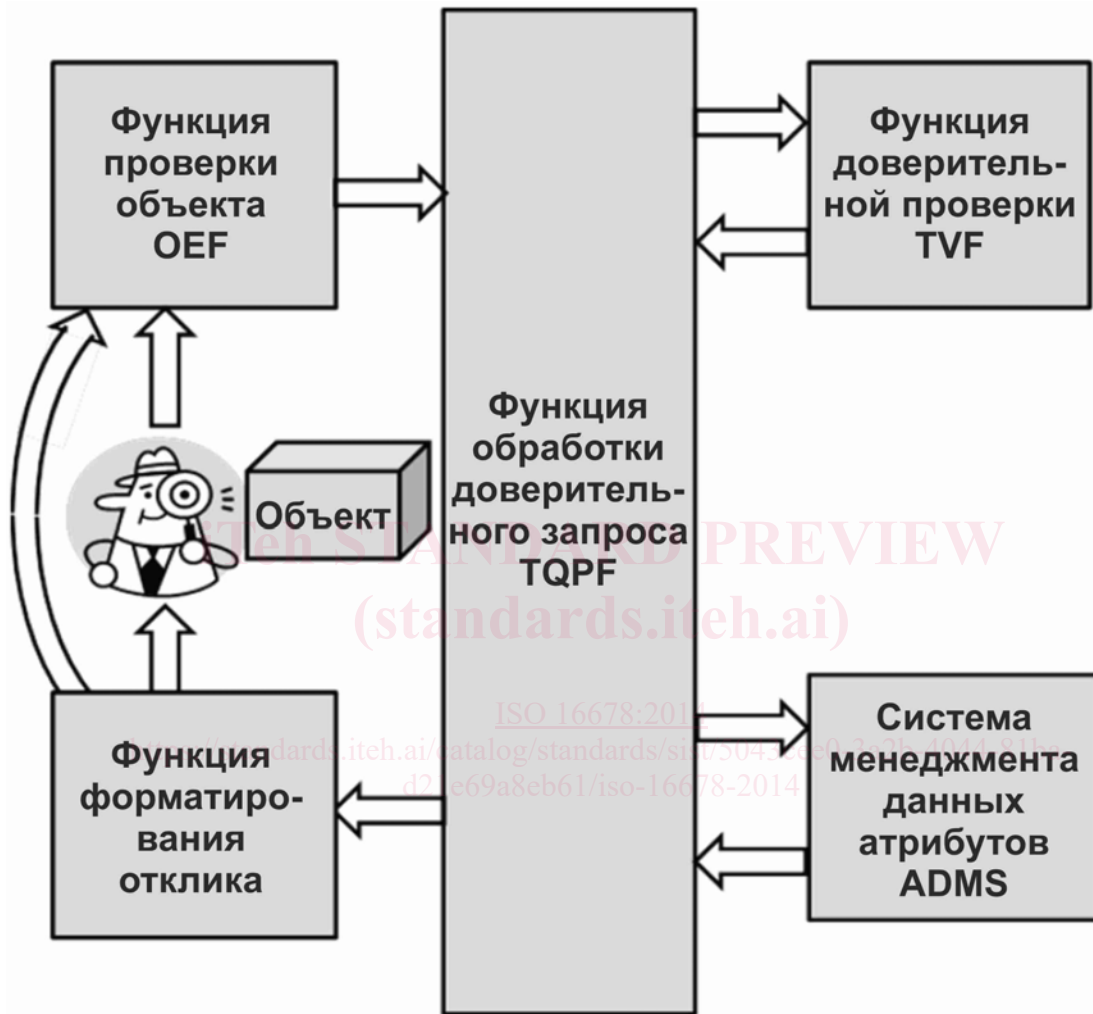


Рисунок 1 — Модель контроля объекта

Модель не содержит никаких предположений относительно способов выполнения функций. В системе могут существовать множественные варианты функций. Различные функции могут комбинироваться в единую службу.

Иллюстрирующие примеры реализации этой модели включены в Приложение С.

3.2.2 Функция проверки объекта (OEF)

Инспектор выполняет проверку представляющего интерес объекта (например материальных средств) для определения, наличия у объекта UID. Если UID обнаружен, может потребоваться дальнейшая проверка для определения, какая функция(и) обработки доверительных запросов должна вероятно иметь сведения относительно данного UID. Эта функция формирует запрос который может состоять только из UID, комбинации UID с полномочиями инспекторов, или данных других физических атрибутов включающих действительные элементы аутентификации, которые могут уникально идентифицировать