Идентификация и аутентификация – основные функциональные требования безопасности электронной экономики

Анатолий Кликич
ДУИКТ

Всемирный экономический форум в Давосе

Основой роста в мировой экономике сегодня является 5 «i»:

- **Информация;**
- **Инфраструктуры;**
- **Интеллектуальный капитал;**
- **Инвестиции;**
- **Инновации.**

Сегодня информация представляет собой незаменимое сырье для выработки любого решения.

Это такое же сырье, как и любое другое, которое необходимо:

- добыть,
- переработать и
- доставить до истечения срока годности тому, кому оно необходимо.

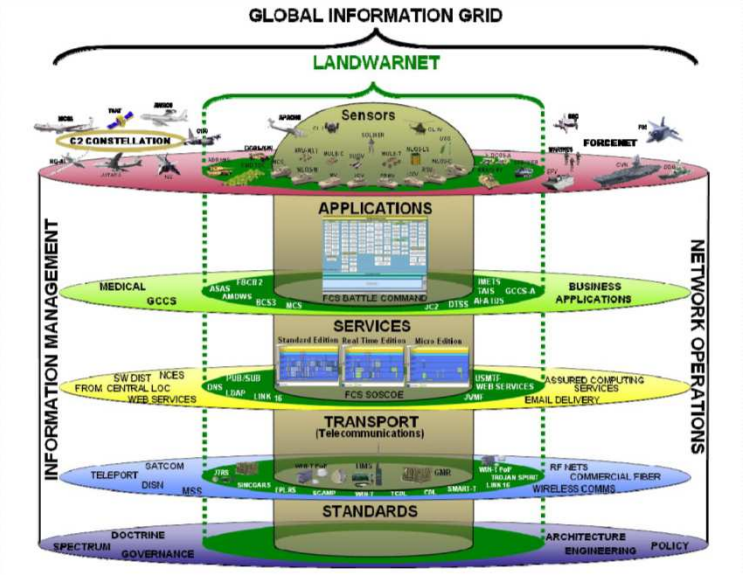
Организацию
хранение
пополнение
поддержку и
предоставление пользователям информации в соответствии с их запросами выполняет

информационная система

Одно из наиболее широких определений информационной системы дал М. Р. Когаловский:

«**информационной системой** называется комплекс, включающий вычислительное и коммуникационное оборудование, программное обеспечение, лингвистические средства и информационные ресурсы, а также системный персонал и обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей»

Информационная система Министерства обороны США.
200 млрд.дол.США.



Информационные системы становятся ключевым элементом цифровой экономики.

Человечество уверенно продвигается к информационной эпохе, экономика и бизнес становятся электронными и осуществляются в сети Интернет.

Доступ к Интернет в мире уже использовали 2 млрд.пользователей.
Уровень проникновения Интернета в Европе превысил 58%, в Украине 48%.

в инструмент ведения современного бизнеса, в основу которого заложены принципы сетевой экономики.

Интернет постепенно превращается из глобальной почтовой и информационно-поисковой системы

Развитие «электронных» услуг не только увеличило объём информации, обрабатываемой и хранящейся в информационных системах , но и повысило её значимость.

Информация стала продуктом, имеющим ценность и стоимость, причем зачастую, ее стоимость во много раз превосходит стоимость самой информационной системы, в которой она хранится и обрабатывается

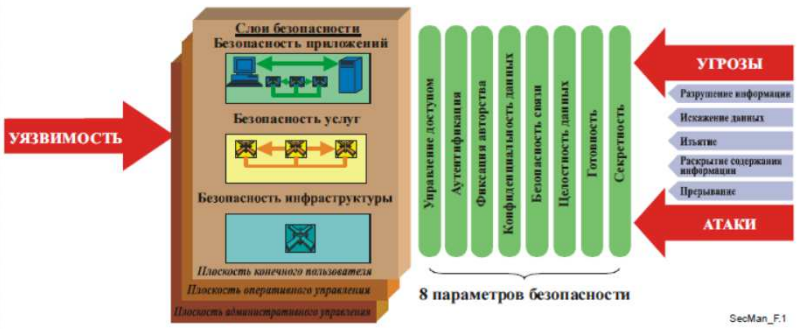


Рисунок 1
Элементы архитектуры безопасности согласно Рекомендации МСЭ-Т X.805

В ФИЗИЧЕСКОМ МИРЕ:

ЧЕЛОВЕКА МОЖНО УВИДЕТЬ, РАСПОЗНАТЬ ПОЧЕРК, ПАСПОРТ, ВОДИТЕЛЬСКОЕ УДОСТОВЕРЕНИЕ, СВИДЕТЕЛЬСТВО О РОЖДЕНИИ И ДР.

УЧРЕЖДЕНИЯ, ОРГАНИЗАЦИИ И БИЗНЕС СТРУКТУРЫ ИМЕЮТ АКТЫ ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ, СЧЕТА В БАНКАХ, ЮРИДИЧЕСКИЕ АДРЕСА И ДР.

В ЦИФРОВОМ МИРЕ,

ВСЕ ОБЩАЮТСЯ ДРУГ С ДРУГОМ НА ЭКРАНЕ КОМПЬЮТЕРА, А ЗНАЧИТ, РАСПОЗНАНИЕ ЛИЧНОСТИ ИНДИВИДА ИЛИ ЖЕ ЦЕЛОЙ ОРГАНИЗАЦИИ,
ДОВЕРИЯ К НИМ ВЫХОДЯТ НА ПЕРВЫЙ ПЛАН.

Идентифика́ция

в информационных системах — установление субъекта по имеющемуся у него идентификатору.

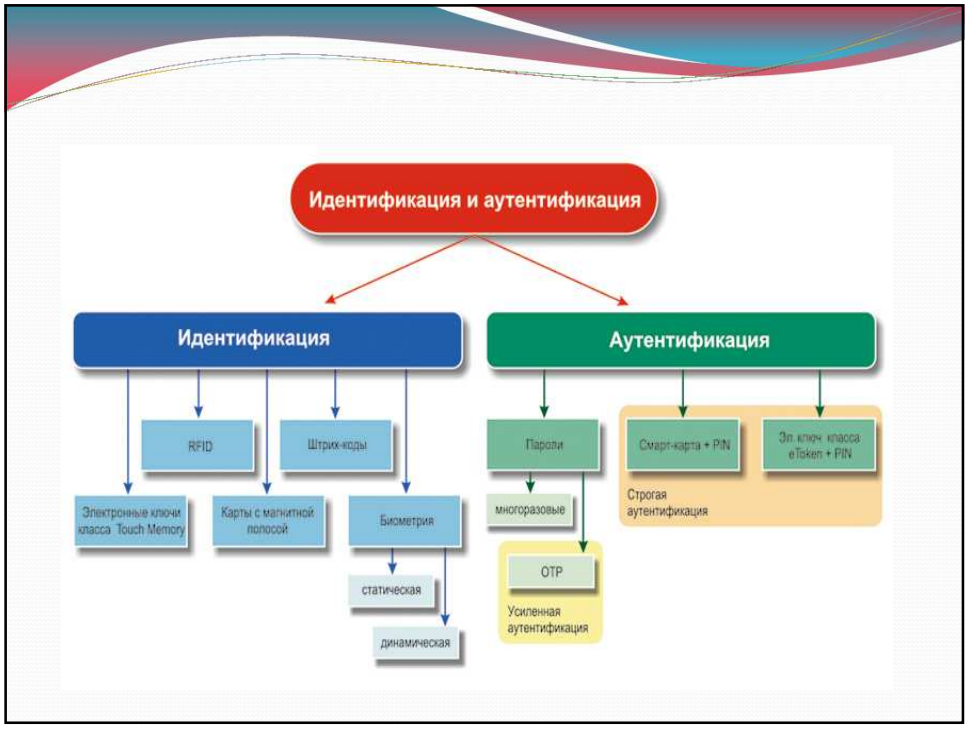
Например: идентификация товара по штрих-коду, идентификация пользователя по логину, идентификация файла по контрольной сумме.

Википедия

Аутентифика́ция (англ. *Authentication*)

процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля с паролем в базе данных пользователей; подтверждение подлинности электронного письма путём проверки цифровой подписи письма по ключу шифрования отправителя; проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла. Термин применяется в основном в сфере информационных технологий.

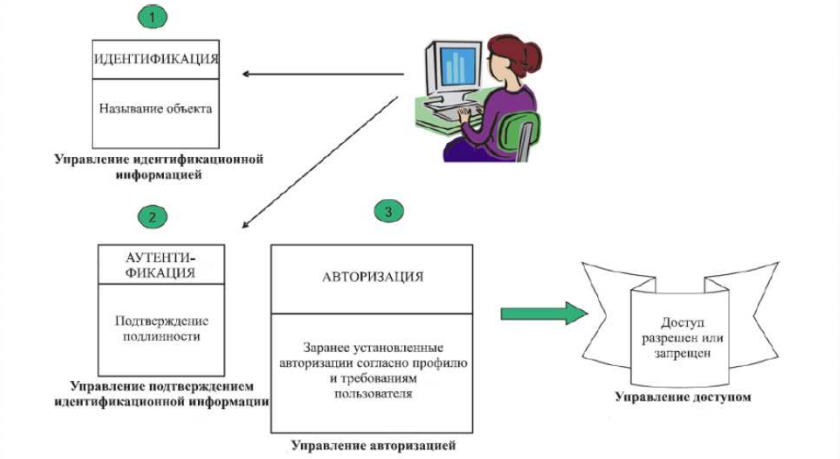
Википедия



Многофакторная аутентификация

Для успешного прохождения процедуры аутентификации пользователь должен

Основные компоненты логического управления доступом



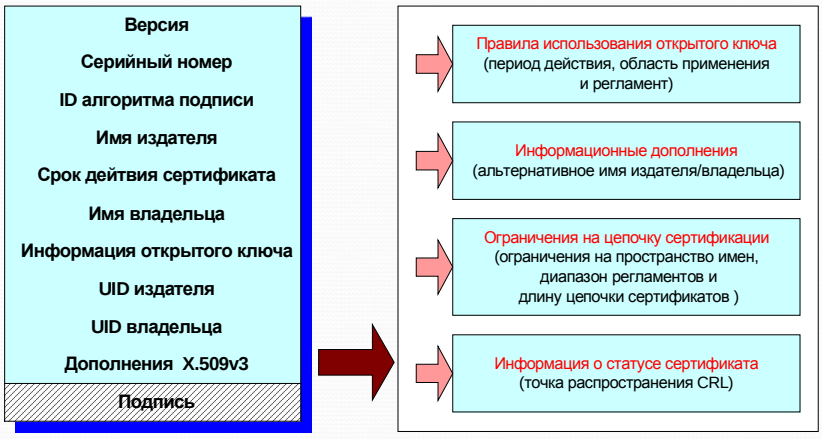
На сегодняшний день активно и спользуется два основных способа аутентификации пользователей в Интернете

парольная защита и

использование цифровых сертификатов.

Для работы с массовыми пользователями широко используется
аутентификация на основе цифровых сертификатов стандарта X.509 и инфраструктуры публичных ключей (PKI),
которая получает все большее распространение в Internet.

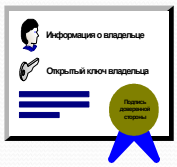
Сертификат X.509



20

Сертификаты позволяют:

• разбить пользователей на несколько классов и
• предоставлять доступ в зависимости от принадлежности пользователя к определенному классу.



Инфраструктура публичных ключей(PKI): позволяет проверить подлинность предъявленного сертификата за счет проверки подлинности цифровой подписи сертифицирующей организации

При усложнении схем бизнеса **с помощью Internet.** появляются различные категории массовых клиентов, которым нужно давать разные права доступа.

Для аутентификации массовых клиентов традиционные схемы на основе индивидуальных паролей неэффективны, так как требуют ввода в систему и хранения каждого пароля, и, следовательно, плохо масштабируются.

Сертификат X.509 – расширения

Расширения сертификата – механизм снабжения открытого ключа дополнительной информацией, необходимой для его использования

Виды дополнений

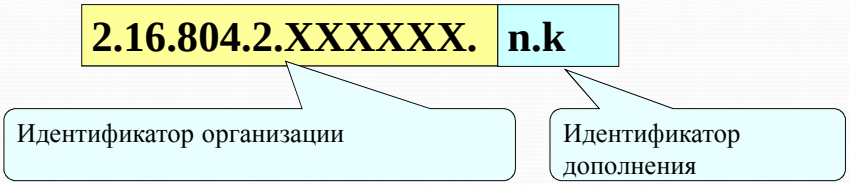
- *Стандартные:* определены в рамках стандарта X.509
- *Специальные:* определяются разработчиками прикладных систем для служебных целей
- *Пользовательские:* определяются конечным пользователем прикладной системы

23

Аутентификация на основе сертификатов может применяться не только к массовым клиентам, но и к сотрудникам предприятий-партнеров, а также и к собственным сотрудникам.

Сертификат X.509 – пользовательские расширения

- Определяются: пользователем
- Содержат:
  - Идентификатор дополнения (OID)
  - Любую значимую для пользователя информацию в виде последовательности байт



25

Процедура классификации объектных идентификаторов (OID) штата Аризона

примеры:
2-16-840-3-04-01-001-01-001 = губернатор
2-16-840-3-04-01-002-01-001 = госсекретарь
2-16-840-3-04-01-002-01-002 = помощник госсекретаря
2-16-840-3-04-01-002-02-999 = Орган политики
2-16-840-3-04-01-002-02-002 = Отдел выборов
2-16-840-3-04-01-002-00-001 = SecState веб-сервер 1
2-16-840-3-04-01-002-02-002-01-001 = Отдел выборов Manger
2-16-840-3-04-01-002-02-002-00-001 = Отдел выборов веб-сервер 1

IV. Сертификаты, выпускаемые для ФНС РФ

Значение ветки OID, зарегистрированной в ГНИВЦ ФНС РФ:

OID	Описание области назначение OID
1.2.643.3.131.1015	Область (области) использования ключа, при которых ЭД с ЭЦП будет иметь юридическое значение

Значения OID, применяемые в сертификатах конечных пользователей услуг:

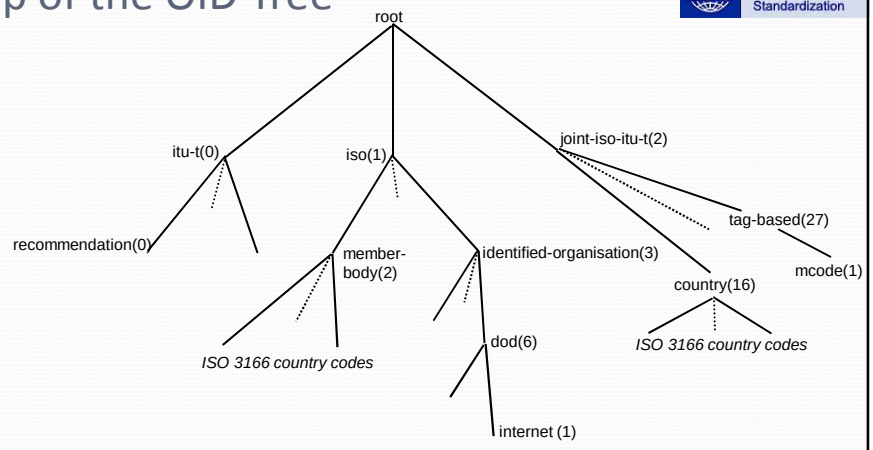
Место размещения	OID	Описание области назначение OID
ExtendedKeyUsage:	1.2.643.3.131.1015.0.3.1.1	ФНС (ИРУЦ), сертификат формируется руководителю организации
	1.2.643.3.131.1015.0.3.2.1	ФНС (ИРУЦ), сертификат формируется главному бухгалтеру организации
	1.2.643.3.131.1015.0.3.3.1	ФНС (ИРУЦ), сертификат формируется руководителю организации, подписывающего документы за главного бухгалтера
	1.2.643.3.131.1015.0.3.4.1	ФНС (ИРУЦ), сертификат формируется налоговому представителю
	1.2.643.3.131.1015.0.3.5.1	ФНС (ИРУЦ), сертификат формируется индивидуальному предпринимателю
	1.2.643.3.131.1015.0.3.6.1	ФНС (ИРУЦ), сертификат формируется сотруднику без права подписи (шифровальщику)

Использование на электронных площадок отобранных для проведения аукционах в электронной форме(OID 1.2.643.6.3.1.1)
Области использования согласно заявлению клиента:

a.Тип участника (один вариант из списка)

i.Юридическое лицо(OID 1.2.643.6.3.1.2.1)
ii.Физическое лицо(OID 1.2.643.6.3.1.2.2)
iii.Индивидуальный предприниматель(OID 1.2.643.6.3.1.2.3)
a.Тип организации:
iv.Участник размещения заказа(OID 1.2.643.6.3.1.3.1)
a.Полномочия (множественный выбор):
v.Администратор организации (OID 1.2.643.6.3.1.4.1)
vi.Уполномоченный специалист(OID 1.2.643.6.3.1.4.2)
vii.Специалист с правом подписи Контракта (OID 1.2.643.6.3.1.4.3)

Top of the OID Tree



Example: {joint-iso-itu-t(2) tag-based(27) mcode(1)}

Note: The name of the 3 top-level arcs do not imply a hierarchical dependency to ISO or ITU-T.

Национальное дерево OID-tree Украины

должно начинаться с главного узла, значение которому присвоено в соответствии с международными рекомендациями.

OID-TREE 2.16.804

{joint-iso-itu-t (2) country (16) ua (804)}

/Joint-ISO-ITU-T/16/804

Стратегия «Европа 2020»

Семь направлений деятельности

1. ***Инновационный Союз*** – улучшение условий и возможностей финансирования исследований и инноваций
2. ***Движение молодежи*** – повышение качества и международной привлекательности высшего образования Европы
3. ***План развития цифровых технологий в Европе*** – развитие высокоскоростного интернета и предоставление возможностей участия в общем цифровом коммерческом пространстве для частных физических и юридических лиц
4. ***Целесообразное использование ресурсов в Европе*** – переход к ресурсосберегающей, низко-углеродной экономике
5. ***Индустриальная политика, направленная на глобализацию***
6. ***План по развитию новых способностей и увеличению количества рабочих мест*** – модернизация рынков труда
7. ***Европейская политика против бедности***

Цифровая повестка дня EU

Семь приоритетных направлений действий:

- создание единого цифрового рынка
- улучшение условий для взаимодействия продуктов и услуг ИКТ
- повышение доверия и безопасности в Интернет
- обеспечение предоставления широкополосного доступ к Интернет
- стимулирование инвестиций в исследования и разработки
- повышение компьютерной грамотности, навыков
- применение ИКТ для решения социальных проблем, таких как изменение климата, рост расходов на здравоохранение и старение населения

Чем больше мы зависим от интернета - тем больше мы зависим от его безопасности.

В 2011 году Генеральной Ассамблеей ООН Резолюцией 65/141 продлила мандат Форума по вопросам управления Интернетом еще на пять лет.

Фундаментальным понятием безопасности (защищенности) является доверие.

Это связано с человеком как субъектом безопасности. Любая защита, сколь бы надежной она ни была, не создаст ощущения безопасности, если человек ей не доверяет.

Особое внимание необходимо сосредоточить на проблеме безопасности ведения бизнеса и предоставления услуг через сеть Интернет.

И здесь на первый план выходит создание пространства доверия для безопасного ведения бизнеса.

США разработали

Национальную Стратегию Доверенной Идентификации в Киберпространстве.

Аналогичное направления выбрал и Европейский союз.

Ключевым действием 16 цифровой повестки дня предусмотрено принятие в 2012 Решения Совета и Правительства о гарантии взаимного признания электронной идентификации и аутентификации в ЕС на основе "услуг аутентификации" онлайн.

Услуги будут предложены всем странам-участницам (с возможным использованием официальных гражданских документов, выпущенных государственным или частным сектором)

Цифровая Идентичность– это набор атрибутов человека или компании в определенной области. Объект может иметь несколько Цифровых Идентичностей

Цифровая Идентичность

Идентичность- это набор атрибутов присущих объекту (человеку/ компании) в конкретной области

Объект может иметь несколько идентичностей, таких как:
- Учетная запись электронной почты (личная и корпоративная)
- Учетные записи социальных сетей (Facebook, Twitter, Вконтакте и др.)
- Учетные записи Е-коммерции (Amazon, eBay)
- Банковские карты
- Учетная запись для покупки авиа и ж/д билетов.
- Телефонная SIM-карта
- Е-паспорт
- Медицинские карты
- Военный билет

Примеры

Identity Ecosystem

Экосистема Идентичности, представляет собой интернет-среду, в которой отдельные лица, организации, службы и устройства могут доверять друг другу, потому что авторитетные источники установили подлинность их цифровых удостоверений.

Цифровые сертификаты X.509 МСЭ уже служат основой доверия и безопасности в онлайновом мире.

Теперь новая работа, проводимая при помощи Глобальной инициативы МСЭ-Т по стандартам управления определением идентичности, касающейся всеобщего доверия к IdM и функциональной совместимости. Применение Рекомендации X.1250 приведет к разработке структуры для завтрашних инфраструктур и услуг сетей на базе IP.

IdM дизайн модели

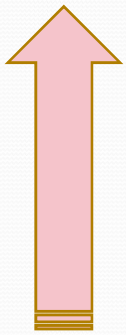
- Идентификаторы объектов являются основными объектами IdM системы и они формируют основу IdM структуры.
- Базовые модели IdM являются неотъемлемыми компонентами, которые строят структуру Мета IDM.
- Структура не зависит от сетевого уровня, охраны окружающей среды, применение сценариев и т.д.
- Система IdM зависит от окружения сети и приложений, с настроенными интерфейсами к другим функциям безопасности / не безопасности для обеспечения сопутствующих ID услуг.
- IdM сеть состоит из нескольких систем IdM, между которыми применяются коммуникационные протоколы и механизмы, например, SAML, SSO.

IdM Сети

IdM Системы

Базовые модели IdM / Мета Структура IdM

Объектные идентификаторы



Мета Структура IdM

- IdM Мета Структура включает в себя основные компоненты IdM , концентрированные объектными идентификаторами.
- Для объектных идентификаторов они должны различить расширения для обеих локальных id действий идентификатора и сетевых функций основанных на IdM.
- Основные ID расширения дают возможность изолированным метаструктурам IdM.
- Расширения высшего уровня Id включают IdM сеть для безопасности / эффективности и т.д

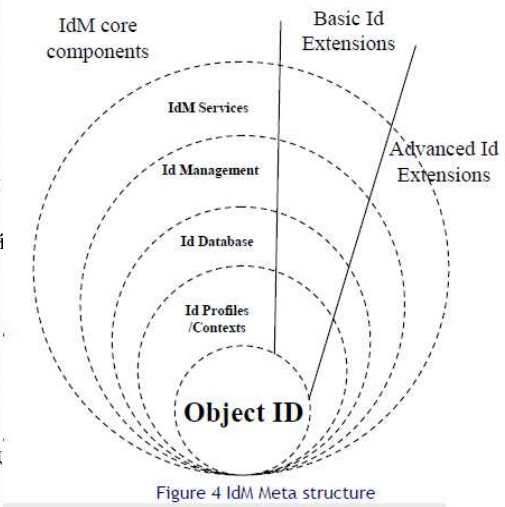


Figure 4 IdM Meta structure

Женева, 6 марта 2012 года

Бюро стандартизации электросвязи

Вопрос 8/17 – Безопасность облачных вычислений

В сферу охвата данного Вопроса по состоянию на 2 марта 2012 года входят следующие Рекомендации и Добавления: МСЭ-Т X.ccsec, X.sfcse, X.fssvpn.

Спасибо за внимание