VIII Уральский форум «Информационная безопасность финансовой сферы»

(Республика Башкортостан, «Юбилейный», февраль 2016 г.)

Международные стандарты (идентификация, аутентификация, доверие безопасности)

НПФ «КРИСТАЛЛ»

Идентификация в «бесконтактном» мире

Завершающий слайд многих презентаций Председателя ИСО/МЭК/СТК1 «Информационные технологии» ПК27 «Методы и средства обеспечения безопасности»

Lessons Learned

- "On the Internet, nobody knows you're a dog."
- "eBusiness (eGovernment, ...) will not evolve without appropriate security solutions."
- "Secure systems are 10% about security technology and 90% about organization."
- "Trust is good – control is better."
- "Standards connect the world."

"On the Internet, nobody knows you're a dog."

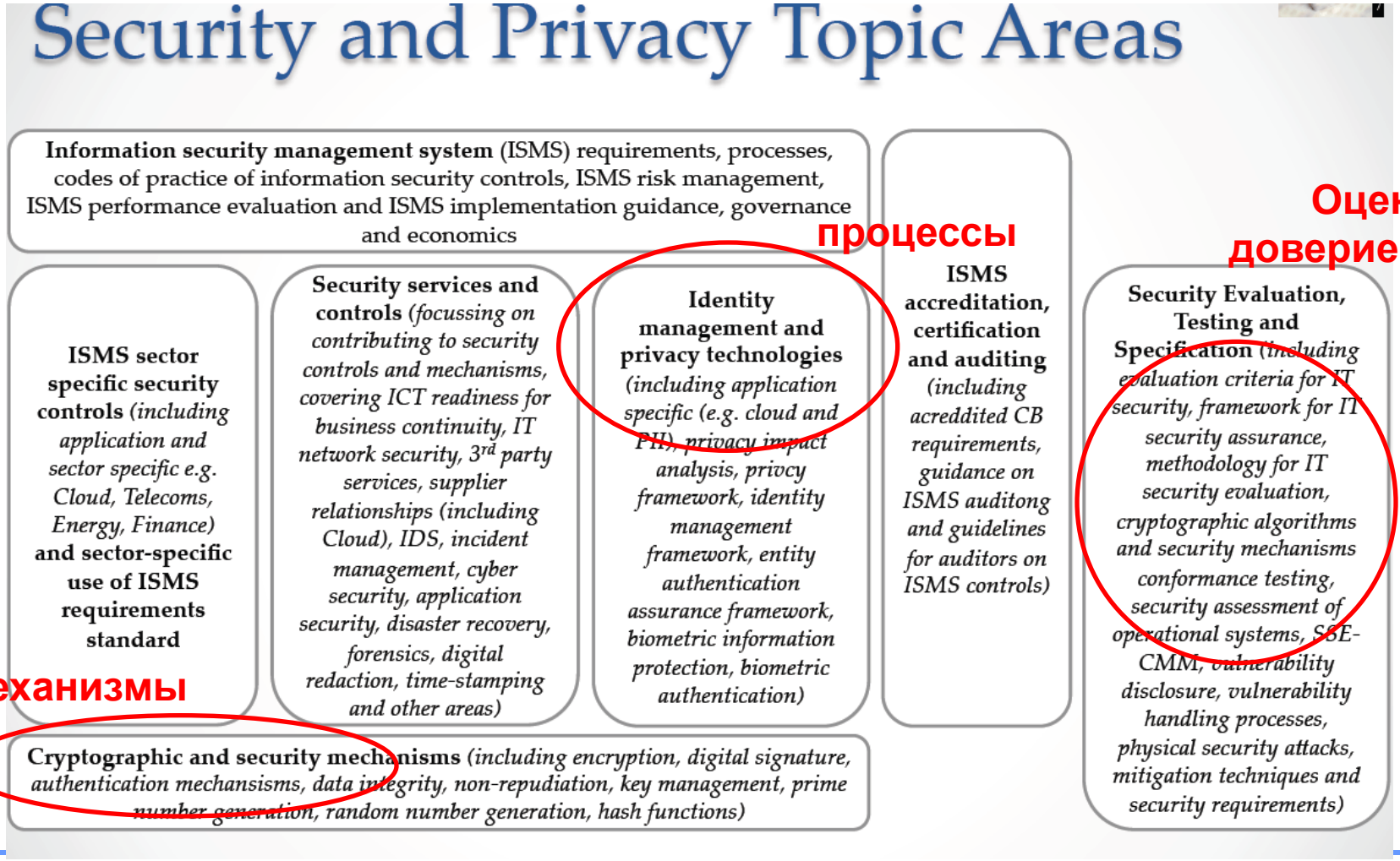
© Из коллекции New Yorker. 1993г.

Выделено:

- Безопасность систем это 10% технологии безопасности и 90% организация работ (процессы, управление);
- Доверяй, но проверяй!

Идентификация и аутентификация

Объекты стандартизации ПК27 «Методы и средства обеспечения безопасности» СТК1 ИСО/МЭК



Остановимся на:

- Терминологии
- Алгоритмах
- Процессах, технологиях, управлении, доверии к…

Терминология (продолжение)

- **identification data** - …… [**ISO/IEC 14888-1, ISO/IEC 29150, ISO/IEC 9798-5**]
- **Identifier** – [**ISO/IEC 24745, ISO/IEC 29115**]
- **Identifier / unique identity/ distinguishing identity** –[**ISO/IEC 24760-1**]
- **identity management system (IdMS)** – system controlling entity …… [**ISO/IEC 24745**]
- **identity management (IDM)** - processes and policies ….. [**ISO/IEC 24760-1**]

Терминология (продолжение). Предварительное резюме

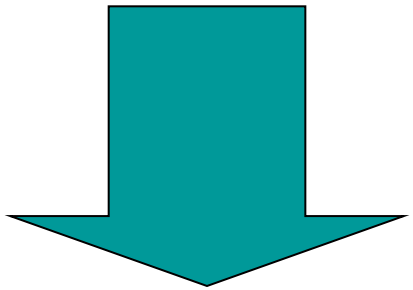
- Контекст использования идентификационной информации оказывает влияние на определение соответствующих понятий и их использование.
- Национальный контекст и контекст применения в РФ зависит от целей применения технологии, что должно найти отражение в соответствующем определении и практической реализации.

Терминология (продолжение). Прикладной контекст. Доверие/уверенность

- **identity proofing** - process by which the Registration Authority (RA) captures and verifies sufficient information to identify an entity to a **specified or understood level of assurance** [**ISO/IEC 29115**]

Доверие

- **Authentication** - the **provision of assurance** of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication). [**ISO/IEC 18028-4**]



Терминология (продолжение). Прикладной контекст. Доверие [ИБ]

ISO/IEC TR 15443-1 «Information technology - Security techniques - Security assurance framework – Part 1: Introduction and concepts» (**ГОСТ Р 54581-2011/ISO/IEC/TR15443-1:2005**)

2.4 **доверие** (assurance): Выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности.

а) основание для уверенности в том, что сущность отвечает своим целям безопасности. [ИСО/МЭК 15408-1]

2.5 **подход к обеспечению доверия** (assurance approach): Группирование методов обеспечения доверия в соответствии с исследуемым аспектом.

2.15 **стадия обеспечения доверия** (assurance stage): Стадия жизненного цикла оцениваемого объекта, на которой используется заданный метод обеспечения доверия. При обеспечении общего доверия к оцениваемому объекту учитываются результаты реализации методов обеспечения доверия, применяемых на всех стадиях его жизненного цикла.

2.16 **свидетельство доверия** (assurance evidence): Документированные результаты, представленные данными, полученными при анализе доверия к оцениваемому объекту, включая отчеты (обоснования) в поддержку утверждения о доверии.

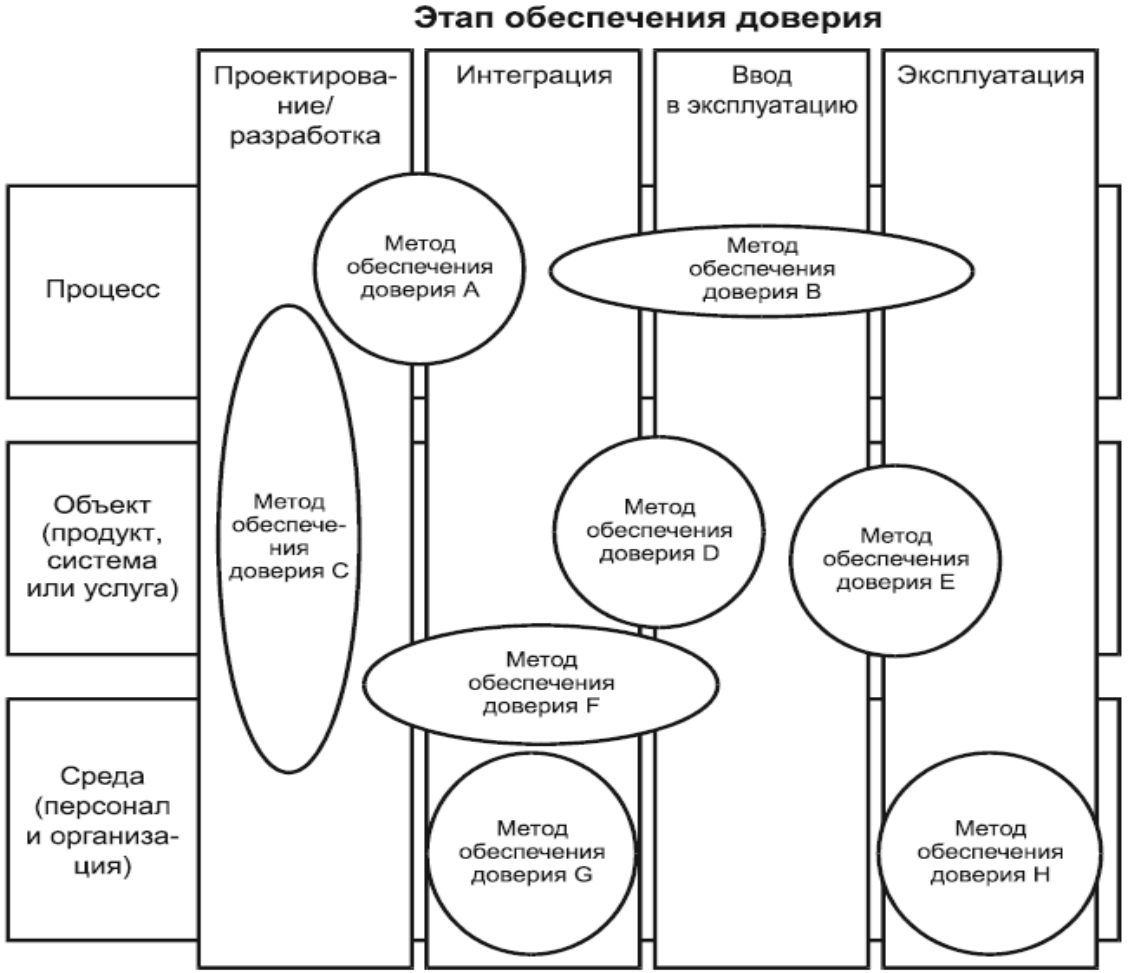
2.18 **уверенность** (confidence): Убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком (то есть корректно, надежно, эффективно, в соответствии с политикой безопасности).

2.21 **гарантия** (guarantee): См. определение «гарантийное обязательство» в 2.36.

Терминология (продолжение). Прикладной контекст. Доверие [ИБ]. Как это «работает»

Модель классификации существующих методов обеспечения «доверия» (ГОСТ Р 54581-2011/ISO/IEC/TR15443-1:2005)

Тезис: выдача ключей подписи физическим и юридическим лицам ≠ формированию «пространства доверия». Этого недостаточно.



Алгоритмы

Стандарты алгоритмов взаимной и многофакторной аутентификации субъектов и объектов в ИКТ

Standard	Title	Status	Abstract
ISO/IEC 9798-1	**Entity authentication** Part 1: General	3rd ed. 2010	*ISO/IEC 9798 specifies several kinds of entity authentication mechanisms that an entity to be authenticated proves its identity by showing its knowledge of a secret.*
-2	Part 2: Mechanisms using symmetric encipherment algorithms	3rd ed. 2008 *Under revision*	
-3	Part 3: Mechanisms using digital signature techniques	2nd ed. 1998 (+Amd1) *Under revision*	
-4	Part 4: Mechanisms using cryptographic check function	2nd ed. 1999	
-5	Part 5: Mechanisms using zero knowledge techniques	3rd ed. 2009	
-6	Part 6: Mechanisms using manual data transfer	2nd ed. 2010	
ISO/IEC 20009-1	**Anonymous entity authentication** Part 1: General	1st ed. 2013	*ISO/IEC 20009 specifies anonymous entity authentication mechanisms in which a verifier makes use of a group signature scheme to authenticate the entity with which it is communicating, without knowing this entity's identity, and which based on blind signatures and weak secrets.*
-2	Part 2: Mechanisms based on signatures using a group public key	1st ed. 2013	
-3	Part 3: Mechanisms based on blind signatures	*Under development*	
-4	Part 4: Mechanisms based on weak secrets	*Under development*	

ISO/IEC JTC 1/SC 27 corporate slides (version 15/April 2014)

Алгоритмы (продолжение). Практика

- Применительно к алгоритмам и протоколам криптографической защиты информации, нашедших отражение в международных стандартах, соответствующие сведения присутствуют в документе «**SC 27/WG 2 Standing Document 2 - WG 2 OID list**»
- **OIDs** обеспечивает универсальную схему идентификации постоянных объектов, основывающуюся на иерархической структуре. Она поддерживается и рекомендована как ISO/IEC, так и МСЭ-Т и используется во многих Интренет-протоколах
- Российский **ТК26 поддерживает аналогичный реестр** идентификаторов отечественных криптографических алгоритмов

Алгоритмы (продолжение). Практика

Иллюстрация содержания глобального реестра Идентификаторов объектов

|- part2(2) -- IS 9798-2:2008-12-15 [3rd ed.]	1.0.9798.2
| |- asn1-module(0) -- ASN.1 modules defined in ISO/IEC 9798-2	1.0.9798.2.0
| | L object-identifiers(0)	1.0.9798.2.0.0
| L mechanisms(1) -- Entity authentication mechanisms	1.0.9798.2.1
| |- ua-one-pass(1)	1.0.9798.2.1.1
| |- ua-two-pass(2)	1.0.9798.2.1.2
| |- ma-two-pass(3)	1.0.9798.2.1.3
| |- ma-three-pass(4)	1.0.9798.2.1.4
| |- ttp-ma-four-pass(5)	1.0.9798.2.1.5
| | L ttp-ma-five-pass(6)	1.0.9798.2.1.6

Алгоритмы многофакторной аутентификации, включенные в ISO/IEC 9798 и их идентификаторы

Готовится документ «**Cryptographic Message Syntax**», предназначенный для поддержки применения электронной подписи, шифрования на симметричных и асимметричных ключах с учетом спецификаций рекомендаций **серии X.500 (ISO/IEC 9594)**. Также будет обеспечена поддержка **ASN.1** для кодирования протокольных блоков данных сообщений.

Процессы, технологии, управление, доверие к…

ПК27 РГ 5 Цели деятельности:

Identity Management & Privacy Technologies

- Development and maintenance of standards and guidelines addressing security aspects of
  - *Identity management*
  - *Biometrics, and*
  - *Privacy*

Стандарты технологий и процессов деятельности

Standard	Title	Status	Abstract
ISO/IEC 24760-1	A framework for identity management – Part 1: Terminology and concepts	1st ed. 2011 Freely available via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html	ISO/IEC 24760-1 • defines terms for identity management, and • specifies core concepts of identity and identity management and their relationships. To address the need to efficiently and effectively implement systems that make identity-based decisions ISO/IEC 24760 specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components which operate on behalf of individuals or organizations. ISO/IEC 24760 specifies fundamental concepts and operational structures of identity management with the purpose to realize information system management so that information systems can meet business, contractual, regulatory and legal obligations. Pat 1 of ISO/IEC 24760 specifies the terminology and concepts for identity management, to promote a common understanding in the field of identity management. It also provides a bibliography of documents related to standardization of various aspects of identity management.

ISO/IEC JTC 1/SC 27 corporate slides (version 15/April 2014)

Стандарты технологий и процессов деятельности (продолжение)

Standard	Title	Status	Abstract
ISO/IEC 29100	Privacy framework	1st ed. 2011 Freely available via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html	*ISO/IEC 29100 provides a privacy framework which* • *specifies a common privacy terminology;* • *defines the actors and their roles in processing personally identifiable information (PII);* • *describes privacy safeguarding considerations; and* • *provides references to known privacy principles for IT.* *ISO/IEC 29100 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.*
ISO/IEC 29115	Entity authentication assurance framework	1st ed. 2013	*ISO/IEC 29115 provides a framework for managing entity authentication assurance in a given context. In particular, it:* • *specifies 4 levels of entity authentication assurance (LoA);* • *specifies criteria and guidelines for achieving these 4 levels;* • *provides guidance for mapping other authentication assurance schemes to the 4 LoAs and for exchanging the results of authentication that are based on the 4 LoAs; and* • *provides guidance on mitigating authentication threats.*
ISO/IEC 29191	Requirements for partially anonymous, partially unlinkable authentication	1st ed. 2012	*ISO/IEC 29191 provides a framework and establishes requirements for partially anonymous, partially unlinkable authentication.* *The term 'partially anonymous, partially unlinkable' means that an a priori designated opener, and that designated opener only, can identify the authenticated entity.*

ISO/IEC JTC 1/SC 27 corporate slides (version 15/April 2014)

Будущие стандарты (некоторые уже приняты)

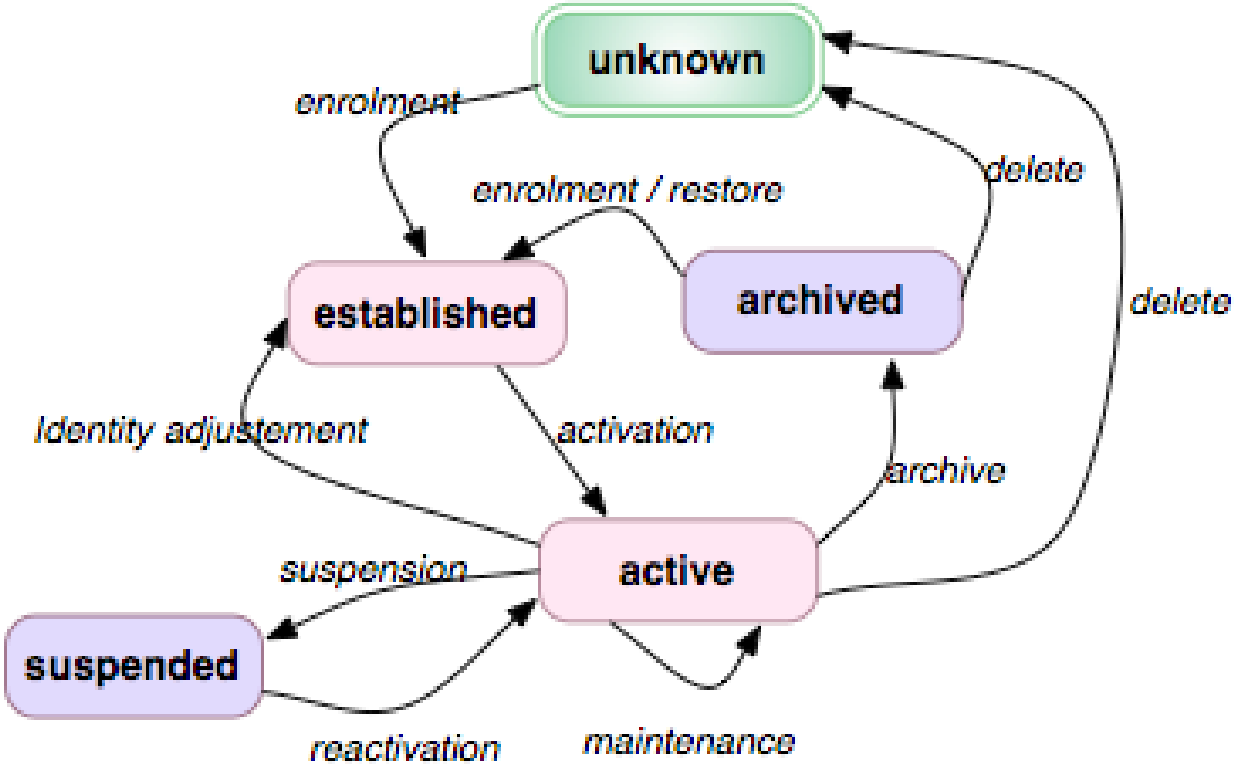
Project	Title	Status
ISO/IEC 27018	Code of practice for PII protection in public clouds acting as PII processors	To be published as IS
ISO/IEC 24760-2	A framework for identity management – Part 2: Reference architecture and requirements	DIS Ballot
ISO/IEC 29190	Privacy capability assessment model	DIS Ballot
ISO/IEC 29146	A framework for access management	3rd CD
ITU-T X.1085 | ISO/IEC 17922	Telebiometric authentication framework using biometric hardware security module	1st CD
ISO/IEC 24760-3	A framework for identity management – Part 3: Practice	1st CD
ISO/IEC 29003	Identity proofing	4th WD
ISO/IEC 29134	Privacy impact assessment – Methodology	4th WD
ISO/IEC 29151	Code of practice for PII protection	3rd WD
Study Period	Age Verification	Extended
Study Period	A privacy-respecting identity management scheme using attribute-based credentials	Starting
Standing Document 2	Privacy references list	Freely available via www.jtc1sc27.din.de/en
Standing Document 4	Standards privacy assessment	To be published

ISO/IEC JTC 1/SC 27 corporate slides (version 15/April 2014)

Что определяют указанные международные стандарты? (Примеры)

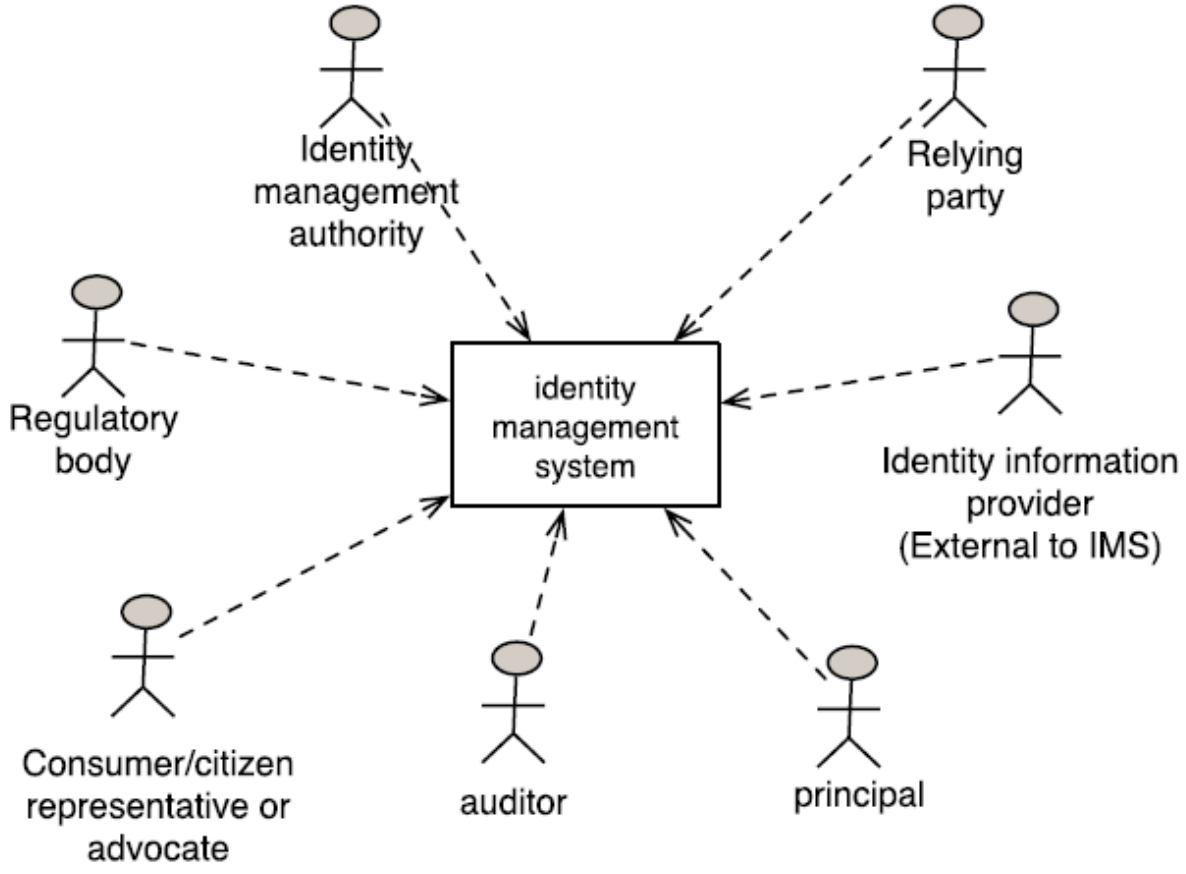
ISO/IEC 24760-1 «A framework for identity management – Part 1: Terminology and concepts»

Жизненный цикл данных идентификации [ISO/IEC 24760-1/ITU-T X1252]



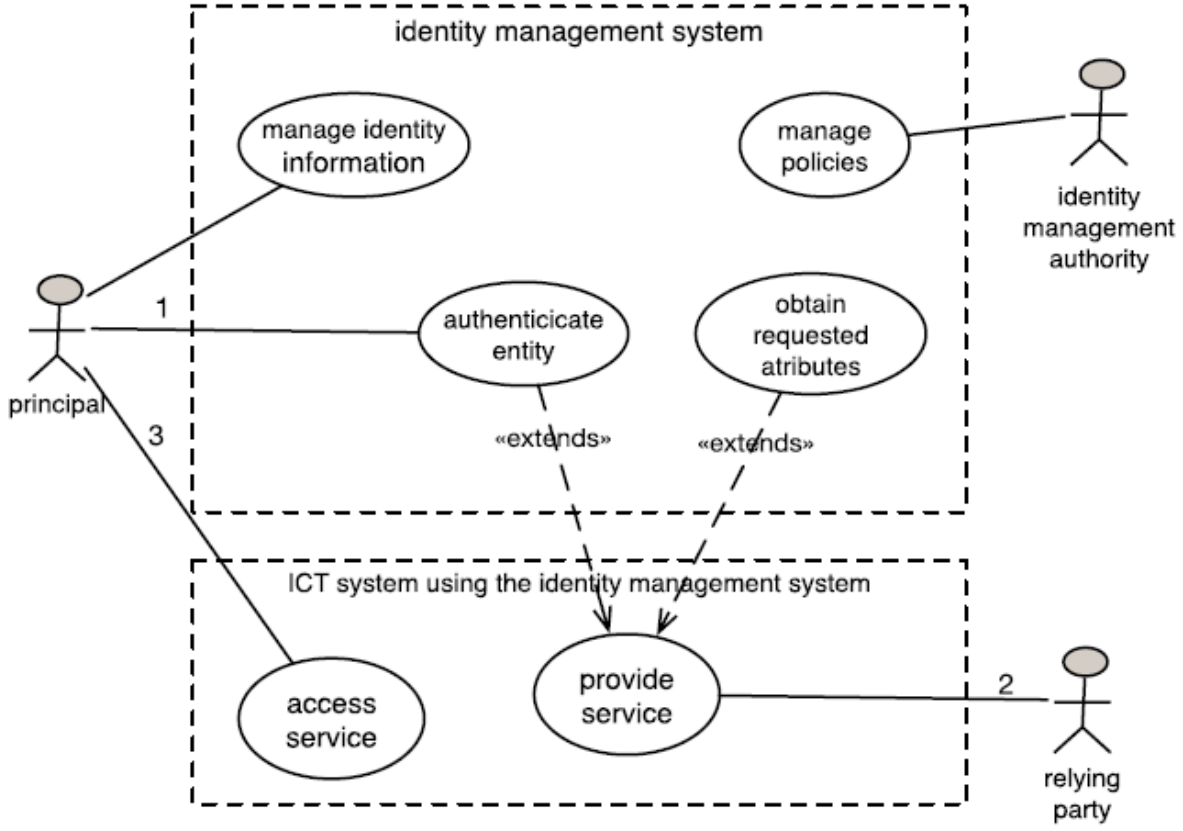
ISO/IEC 24760-2 «A framework for identity management – Part 2: Reference architecture and requirements»

Контекстная модель менеджмента идентификационных данных [ISO/IEC 24760-2]



ISO/IEC 24760-2 «A framework for identity management – Part 2: Reference architecture and requirements»

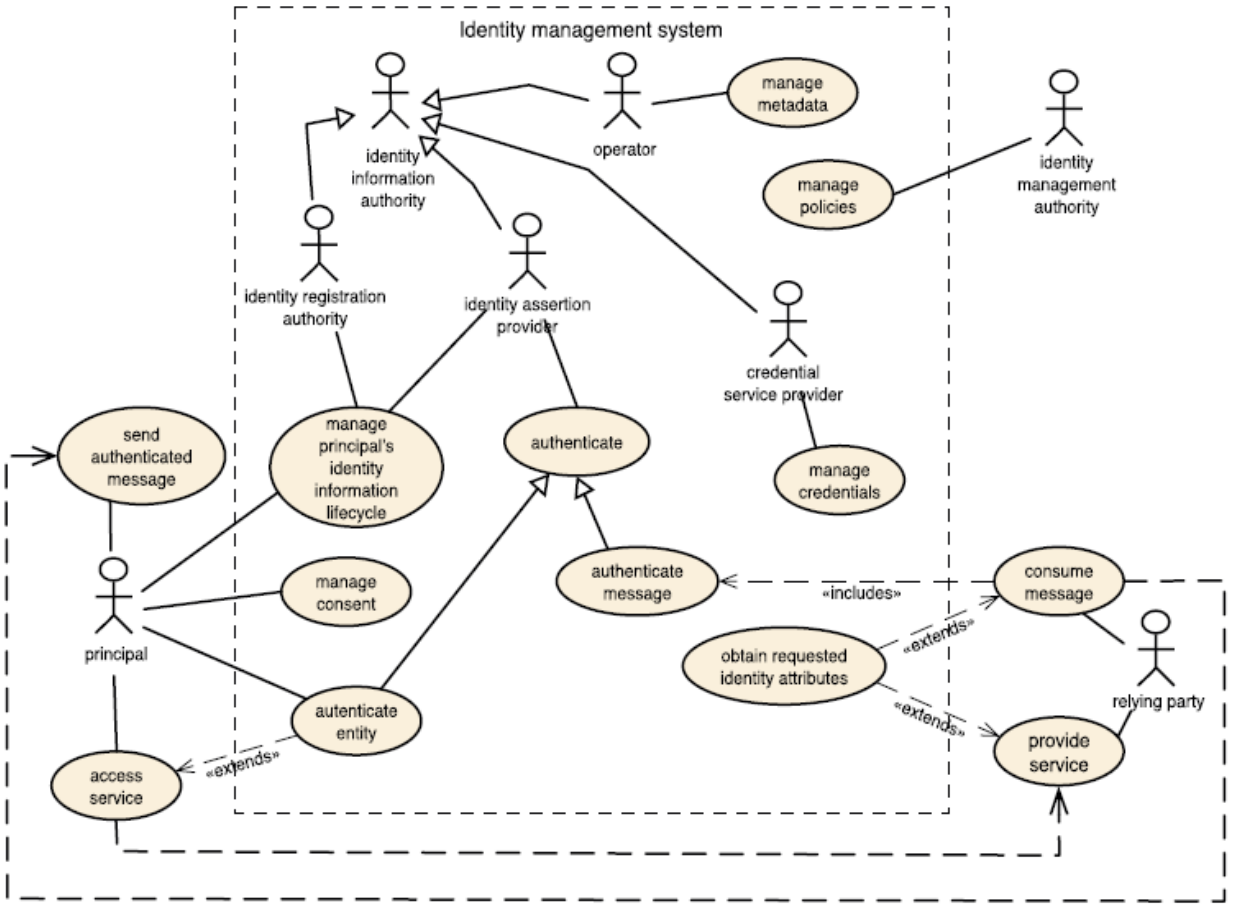
Основные направления использования идентификационной информации [ISO/IEC 24760-2]



«extends» = use case pointed to includes functions of the use case at tail
1, 2, 3 sequence of interactions for principal to acces a service

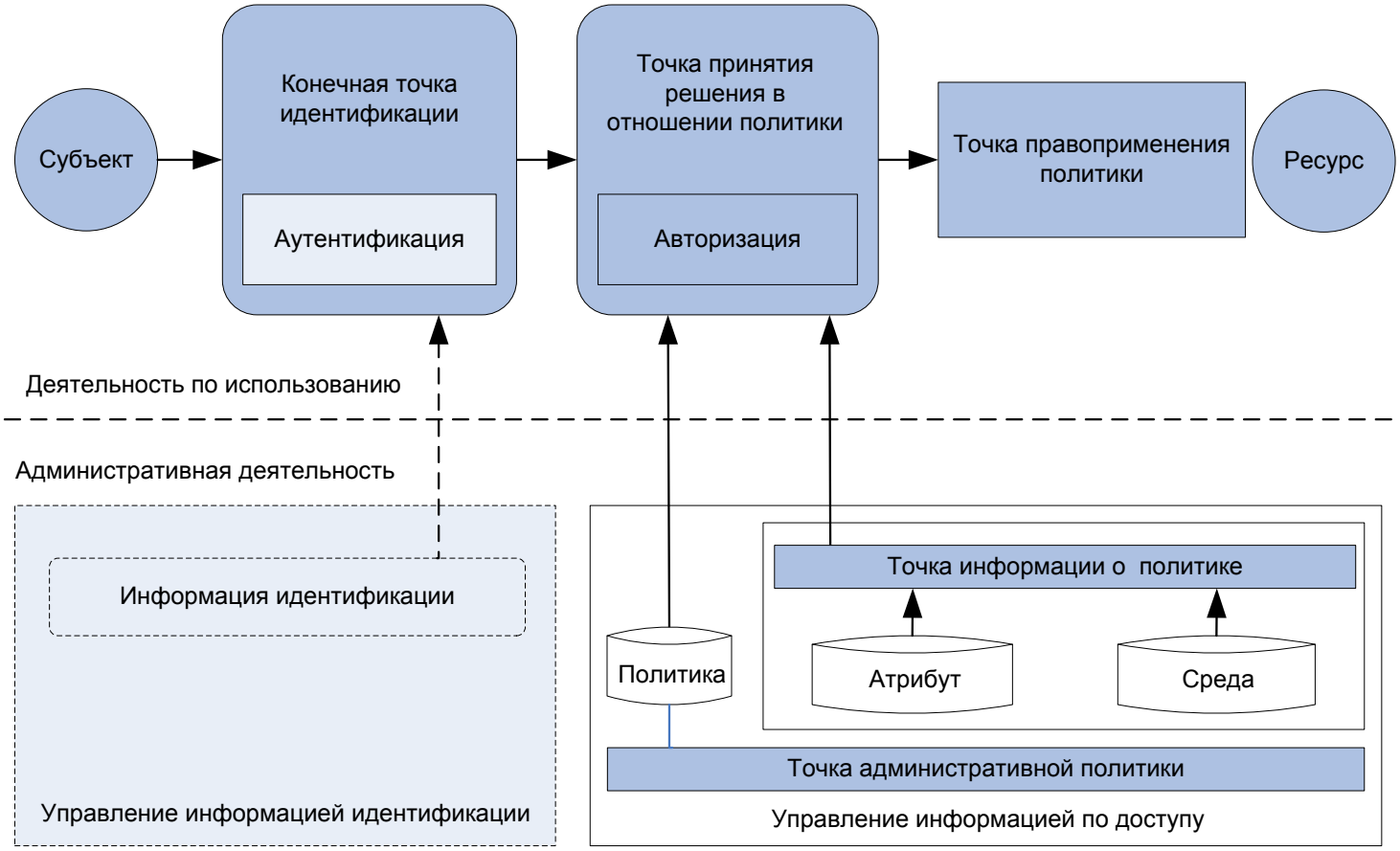
ISO/IEC 24760-2 «A framework for identity management – Part 2: Reference architecture and requirements»

Примерная диаграмма работы Системы управления идентификационными данными [ISO/IEC 24760-2]



ISO/IEC 29146 «A framework for access management»

Модельная архитектура Системы управления доступом [ISO/IEC 29146]



ISO/IEC 29115 «Entity Authentication Assurance Framework»

Основные задачи, имеющие отношение к доверию аутентификации сущности [ISO/IEC 29115/ITU-T Recommendation X.1254]

	Технические	Управленческие и организационные
Этап регистрации	• Заявление и инициирование • Подтверждение идентификационных атрибутов и верификация идентификационной информации • Ведение учета/фиксирование	• Организация услуг • Соответствие правовым и договорным требованиям • Финансовое обеспечение • Менеджмент и аудит информационной безопасности • Компоненты внешних услуг • Операционная инфраструктура • Измерение операционных возможностей
Этап менеджмента мандатов	• Создание мандатов • Выпуск мандатов • Активация мандатов • Хранение мандатов • Приостановка, аннулирование и/или уничтожение мандатов • Пролонгация и/или замена мандатов • Ведение учета	
Этап аутентификации сущности	• Аутентификация • Ведение учета	

ISO/IEC 29115 «Entity Authentication Assurance Framework»

Уровни доверия (основываются на свидетельствах) [ISO/IEC 29115/ITU-T Recommendation X.1254]

Level	Description
1 – Low	Little or no confidence in the claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

Уровень	Описание
1 – Низкий	***Небольшая или нулевая уверенность*** в заявленном или представленном идентификационном атрибуте.
2 – Средний	***Некоторая уверенность*** в заявленном или представленном идентификационном атрибуте.
3 – Высокий	***Высокая уверенность*** в заявленном или представленном идентификационном атрибуте.
4 – Очень высокий	***Очень высокая уверенность*** в заявленном или представленном идентификационном атрибуте.

Без наличия стандартизированных решений, детализирующих соответствующее законодательство, нас ждет хаос

Спасибо за внимание!

В.Б. Голованов
Зам. научного директора

НПФ «КРИСТАЛЛ»
г. Пенза
Email: crystall@sura.ru
www.npf-crystall.ru