Краткий анализ международных стандартов по управлению идентификацией и идентификацией

PKI-форум 2016, 15 сентября 2016 г.

Алексей Сабанов, к.т.н.,

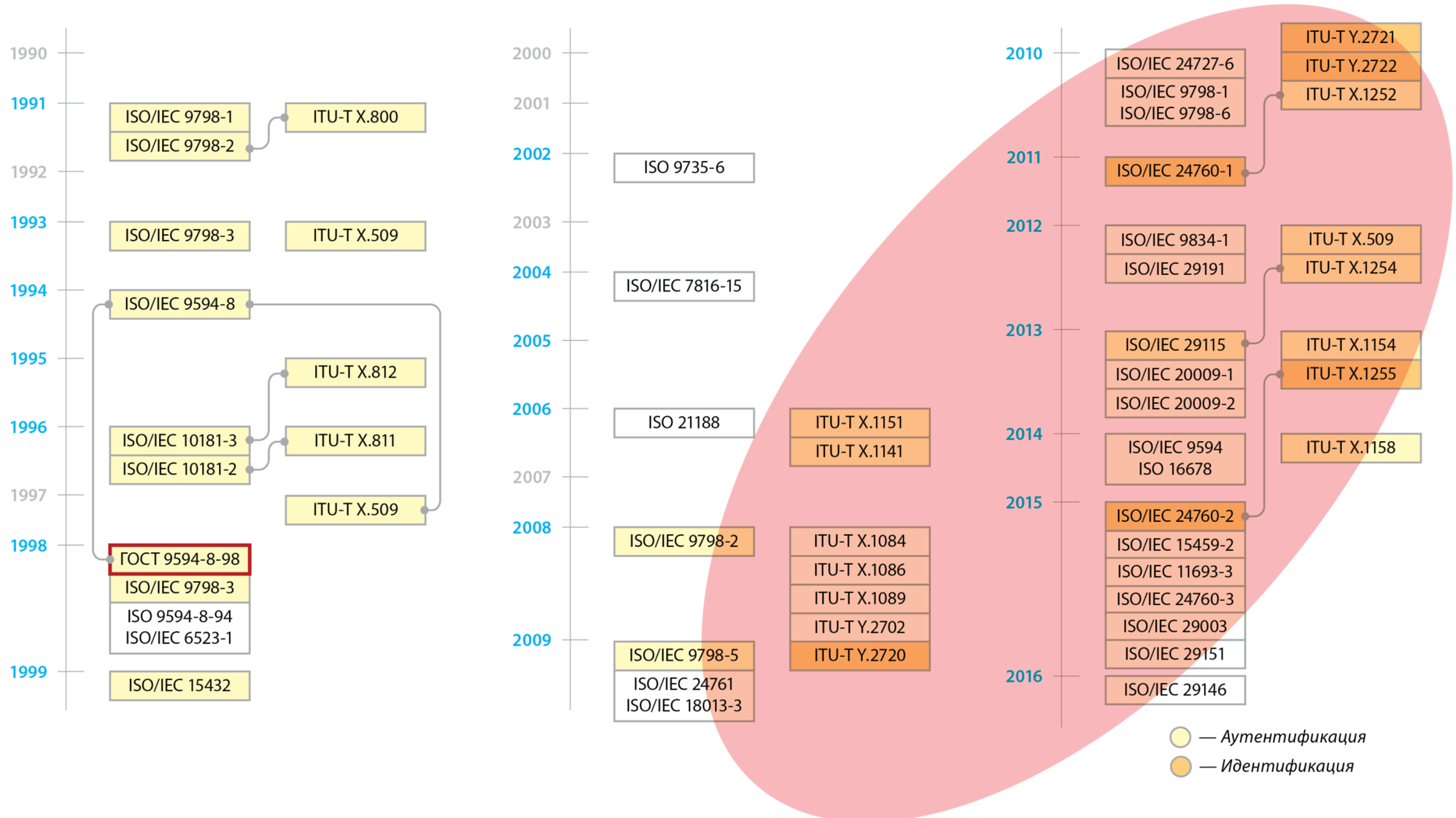
ЗАО "Аладдин Р.Д."

Определения

Идентификация – процесс **сравнения** идентификатора, вводимого участником информационного взаимодействия, с идентификатором этого участника, содержащимся в базе данных системы доступа в составе информаиционной системы.

Аутентификация – это процессы **подтверждения подлинности** предъявленного заявителем идентификатора и **проверка принадлежности** аутентификатора (секрета, который знают обе стороны взаимодействия или о существовании которого знают обе стороны взаимодействия) и идентификатора конкретному субъекту или объекту.

Международные стандарты по идентификации и аутентификации



Развитие стандартов. 1988г.

- Появление первой версии рекомендаций X.509 Международного союза электросвязи (на тот момент времени – Международный консультационной комитет по телефонии и телеграфии, МККТТ, при соответствующей комиссии ООН, с 1995г. преобразован в международный союз в области электросвязи, МСЭ, ООН).
- С первой версии этого документа по третью, изданную в 1997г., рекомендация X.509 называлась «Директория: основы аутентификации».
- Приводятся два вида аутентификации: простая с применением в качестве аутентификатора пароля, и строгая (одно-, двух- и трех-факторная) с применением криптографических функций. Текст стандарта полностью идентичен стандарту ISO/IEC 7498-2:1989.

Развитие стандартов. 1991г.

- Одним из первых стандартов по аутентификации пользователей открытых систем, разработанных ИСО, также является стандарт ISO/IEC 9798-1 «Общая модель механизмов аутентификации объектов».
- Стандарт по архитектуре безопасности для взаимосвязи открытых систем, технически согласованный с рекомендацией МСЭ X.800, в котором подробно рассмотрены базовые услуги безопасности, в первую очередь, «аутентификация», на семи уровнях эталонной модели взаимодействия открытых систем (OSI).
- Стандарт ISO/IEC 9798, первоначально состоящий из трех частей (первые 2 части вышли в 1991г., третья часть – в 1993г.), переиздавался несколько раз. Например, часть 2 впервые была опубликована в 1991г., второй раз – в 1996г., последний раз – в 2008г.

Развитие стандартов. 1993г.

- стандарт ISO/IEC 9594-8-95, разработанный в 1991-1994 гг. Восьмая часть данного стандарта явилась развитием X.509, подробно описывающим два вида аутентификации: простую (парольную) и строгую, на основе применения открытого и закрытого ключей.
- Секретный ключ, согласно третьей части стандарта 9798, служит в качестве аутентификатора и его генерация может осуществляться внутри смарт-карты пользователем, удостоверяющим центром или доверенной третьей стороной.
- Через три года данный стандарт был переведен на русский язык и вошел в нормативную базу Российской Федерации. До сих пор данный стандарт 9594-8 является единственным стандартом по идентификации и аутентификации пользователей РФ

Развитие стандартов. 1997г.

- Выходит в свет полностью пересмотренная версия стандарта МСЭ Rec.X.509
- Описаны и специфицированы простая и строгая аутентификация (одно-, двух- и трехфакторная) с применением асимметричной криптографии.
- Представлены основные сервисы безопасности на базе инфраструктуры открытых ключей: аутентификация (источника данных и взаимная аутентификация), управление доступом, целостность и неотказуемость.
- Определены основные механизмы, применяющиеся в указанных сервисах: простая и строгая аутентификация, шифрование и целостность данных, электронная подпись

Развитие стандартов. 2009г.

- Опубликован стандарт МСЭ Rec.Y.2720, обобщающий наработки многих рекомендаций, в том числе МСЭ Rec.X.1151, МСЭ Rec.X.1141 для управления идентификацией объектов и субъектов в сетях нового поколения. В системе ISO/IEC первая часть аналогичного назначения стандарта (терминология и концепции) появится лишь в 2011 г. (ISO/IEC 24760-1).
- Положения стандарта ИСО рассматривают те же категории, что и стандартом МСЭ Rec.Y.2721 (2010)

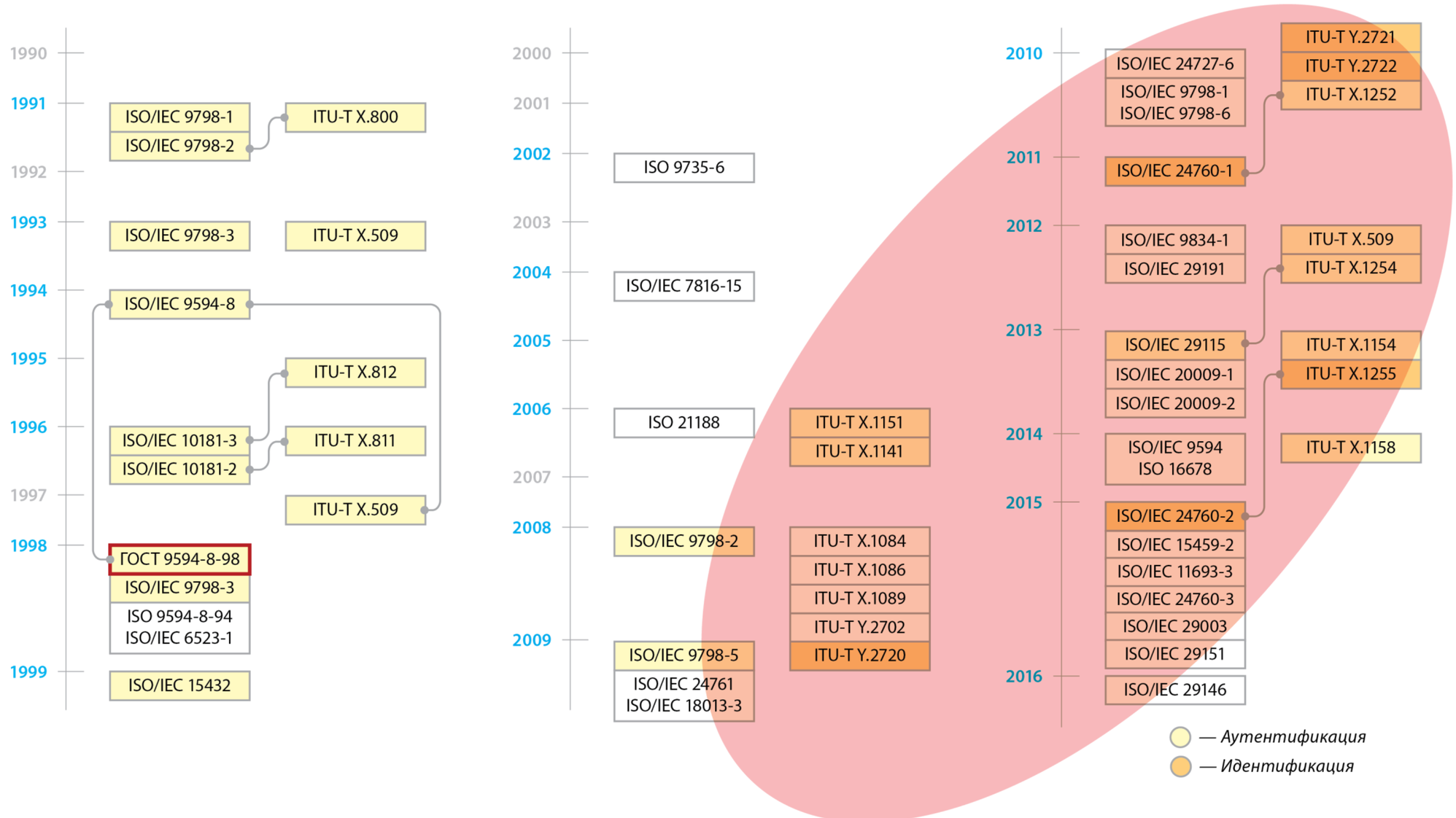
Развитие стандартов. 2013-2016гг.

2013г. Применение методов управления рисками к задачам идентификации и аутентификации, а также появление ряда работ NIST способствовали появлению первого стандарта ИСО по уровням гарантии аутентификации (ISO/IEC 29115), гармонизированного с ITU-T Rec.X.1254 (2010);

2015г. Вышел стандарт ISO/IEC 24760-2, соответствующий рекомендациям по управлению идентификацией. Основные положения этих стандартов опираются на X.1254 и X.1255;

2016г. Опубликован ISO/IEC 29146 по управлению доступом для совершения транзакций разного уровня рисков с применением уровней доверия к аутентификации субъектов доступа.

Международные стандарты по идентификации и аутентификации



Соответствие стандартов

Стандарты МСЭ (ITU-T)	Стандарты ИСО
ITU-T X.800 (1991) Методы защиты. Аутентификация объектов. Архитектура безопасности для взаимодействия открытых систем	ISO/IEC 9798-2:1989 Аутентификация объектов. Архитектура безопасности для взаимодействия открытых систем
ITU-T X.509 (1997) Взаимодействие открытых систем. Справочник сертификатов. Основы аутентификации	ISO/IEC 9594-8:1998 Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации
ITU-T X.811 (1995) Теоретические основы аутентификации	ISO/IEC 10181-2:1996 Основы безопасности для открытых систем. Часть 2. Основы аутентификации
ITU-T X.1252 (2010) Базовые термины и определения в области управления идентификацией	ISO/IEC 24760-1:2011 Руководство по управлению идентификацией. Часть 1. Терминология и понятия
ITU-T X.1254 (2012) Структура гарантии аутентификации объекта	ISO/IEC 29115:2013 Схема обеспечения идентификации объекта
ITU-T X.1255 (2013) Структура обнаружения информации по управлению идентификацией	ISO/IEC 24760-1:2015 Общие основы управления идентификацией. Часть 2. Эталонная архитектура и требования

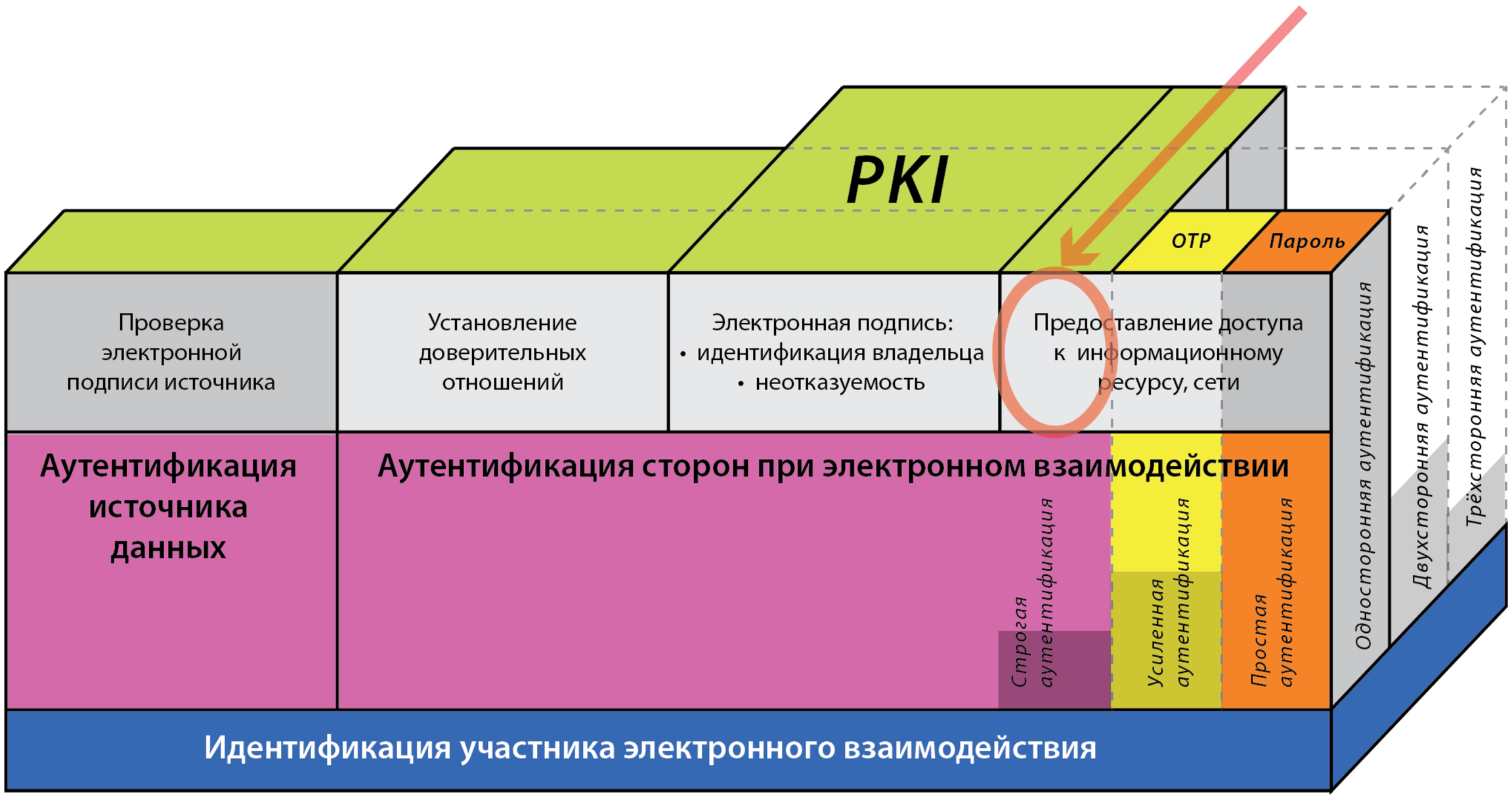
Этапы развития стандартов

1991 – 1999гг. Стадия накопления знаний о процессах аутентификации, протоколах обмена и "увязки" сервисов безопасности с уровнями OSI. Разработка стандартов аутентификации с применением симметричных и асимметричных криптографических алгоритмов.

2000-2007гг. Дальнейшая проработка механизмов аутентификации, появление широко используемых стандартов. Опубликование национальных стандартов с учетом опыта международных (например, стандарт США FIPS Pub1). Становление и развитие стандартов по идентификации.

2008 – наше время. Уровни достоверности результатов аутентификации связаны с уровнем рисков. Зрелые стандарты. Интенсивный рост числа стандартов. Проникновение стандартов по аутентификации в новейшие технологии (облачные вычисления, интернет вещей, активные сети).

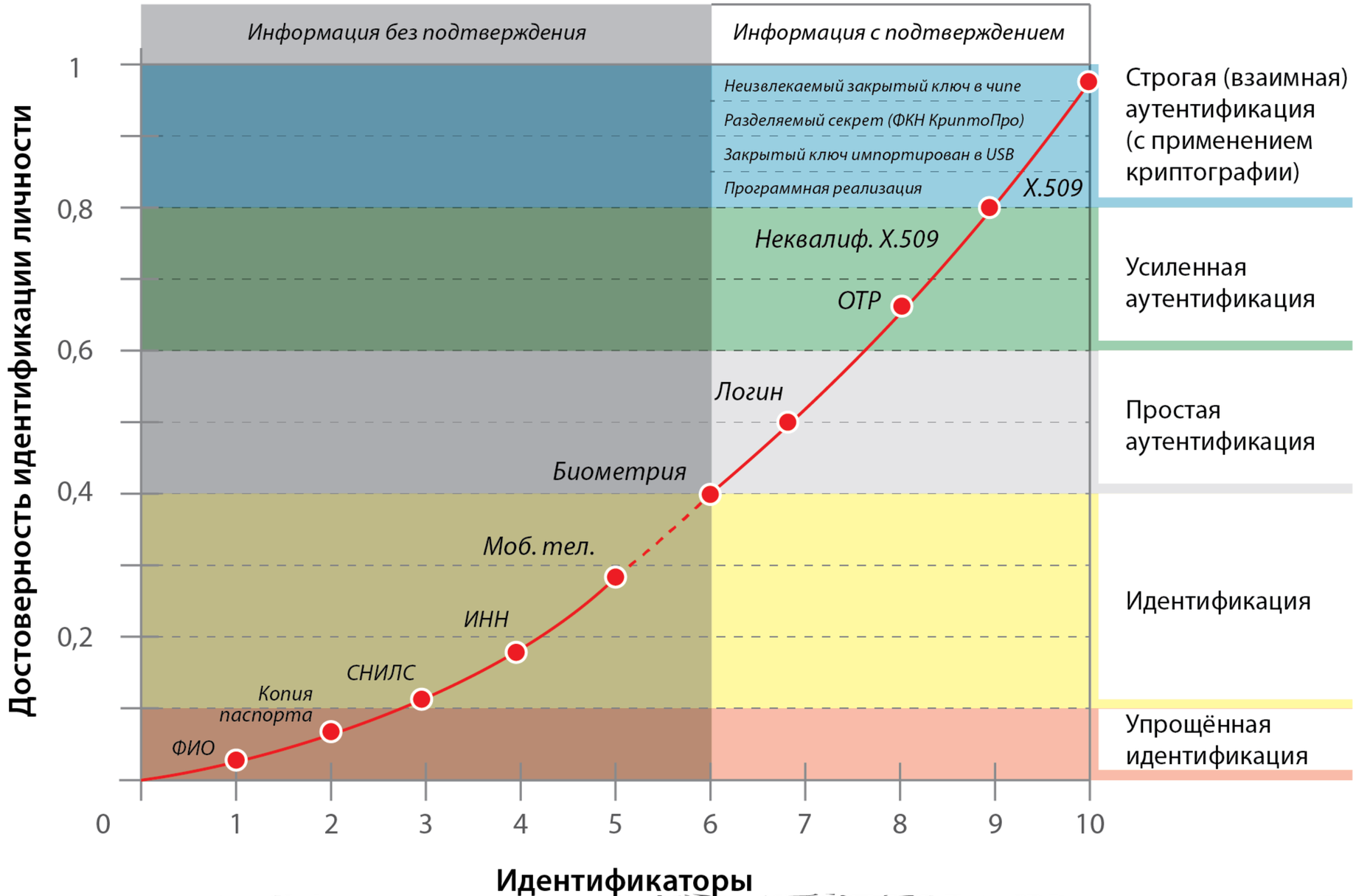
Классификация механизмов аутентификации



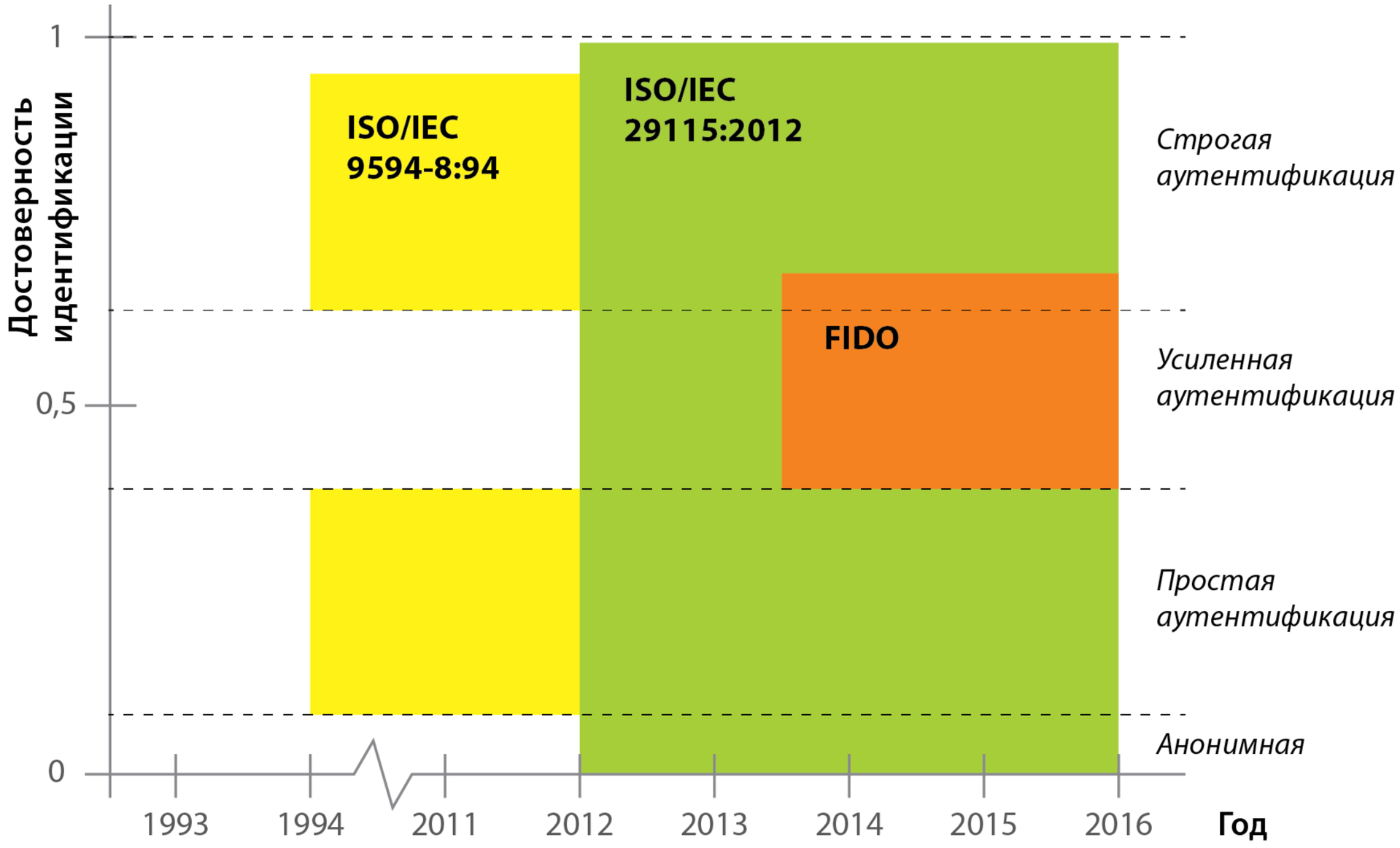
Уровни идентификации личности

Уровень	Описание	Задача	Средства контроля
Уровень 1 - низкий	Слабая степень уверенности в заявленной идентичности	Идентичность уникальна в рамках контекста	Собственное утверждение или заявление
Уровень 2 - средний	Определенная степень уверенности в заявленной идентичности	Идентичность уникальна в рамках контекста, и объект, владеющий идентичностью, реально существует	Проверка подлинности идентичности путем использования информации из авторитетного источника
Уровень 3 - высокий	Высокая степень уверенности в заявленной идентичности	Идентичность уникальна в рамках контекста, объект реально существует, идентичность верифицирована, идентичность используется в других контекстах	Проверка подлинности идентичности путем использования информации из авторитетного источника + верификация идентичности
Уровень 4 - очень высокий	Очень высокая степень уверенности в утверждаемой или заявленной идентичности	Идентичность уникальна в рамках контекста, объект реально существует, идентичность верифицирована, идентичность используется в других контекстах	Проверка подлинности идентичности путем использования информации из достоверного источника + верификация идентичности + личное присутствие объекта

Достоверность идентификации



Уровни достоверности идентификации



Спасибо за внимание!

a.sabanov@aladdin-rd.ru