Вопросы доверия к идентификации и аутентификации: ЕС и Российская Федерация — подходы и перспективы

PKI-форум 16-18 сентября 2014 г.

Алексей Сабанов

Зам. генерального директора

ЗАО «Аладдин Р.Д.»

План доклада

- что такое доверие к идентификации
- вопросы доверия к аутентификации
- краткая новейшая история решения задач доверия к идентификации и аутентификации
- неравномерность европейских требований
- положения Regulation (EU) 910/2014 (eIDAS)
- нормативная база в России
- оценка перспектив

Определения

Идентификация – это **сравнение** идентификатора, вводимого участником информационного взаимодействия в любую из информационных систем, указанных в пункте 4 Требований (ПП-977от 28.11.2011г.), с идентификатором этого участника, содержащимся в соответствующем базовом государственном информационном ресурсе, определяемом Правительством Российской Федерации

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

Доверие к идентификации

Основной критерий – Качество идентификации – отличие одного субъекта от другого путем сравнения предъявленных идентификаторов с занесенными в БД.

Имеются ошибки первого (не идентифицирован) и второго рода (злоумышленник идентифицирован как легальный user).

Требует уровней доверия к результатам сравнения в зависимости от числа идентификаторов и механизмов сравнения. Требует протоколирования результатов для разбора конфликтных ситуаций.

Доверие к аутентификации

Только аутентификация доказывает привязку идентификаторов и аутентификатора к конкретной личности. Самая безопасная и надежная аутентификация основана на сертификате доступа с механизмом аутентификации в виде электронной подписи.

Основной Критерий – качество (безопасность и надежность) аутентификации.

Необходимо ввести уровни доверия к аутентификации.

Основная нерешенная Проблема – трансляция доверия.

Краткая история

Существенным толчком к решению задач доверия к идентификации явилось 11 сентября 2001г.

Совет Безопасности ООН принял резолюцию 1373, направленную на усиление мер против фальсификации паспортов

США: разработаны требования на основе работ НИСТ, стандарт FIPS PUB 201-1 - 2006, биопаспорта введены с 2004г.

Директива 1999/93/EC об электронной подписи

Положение и регламент Regulation 910/2014

Каждая страна шла своим путем…

Наиболее полный пакет нормативной базы был создан и продолжает развиваться в США

Канада, Австралия и ряд европейских стран с той или иной степенью глубины повторяют американский опыт

Во всех развитых странах пришли к выводу о необходимости усиления требований к первичной идентификации и решения задач трансляции доверия к идентификации и аутентификации

Документы для первичной идентификации

List 1
Evidence of link between photo & signature

- **Australian driver's licence**
- **Australian passport**
- **Australian firearm's licence**
- **Defence force/Police ID card**
- **Department of Immigration and Citizenship (DIAC) certificate** with of evidence of residence status
- **WA Photo Card, Over 18 or Proof of Age Card**
- **Australian learner driver's permit card**

List 2
Evidence of operating in the community

- **Debit or Credit card** (one or the other, not both) issued by a financial institution
- **Document of Identity** issued by the Passport Office
- **Entitlement card** issued by the Commonwealth or State Government (Centrelink, Health Care card, Veterans Affairs card etc)
- **Full birth certificate** issued in Australia (birth extracts not accepted)
- **Medicare card**
- **Naturalisation, citizenship or immigration papers** issued by Department of Immigration & Boarder Protection (DIBP)
- **Overseas passport** with current Australian Entry Permit
- **Security guard or crowd control licence** (Australian)
- **Student identity document** or **Statement of enrolment** issued by an educational institution, including Tertiary (should include photo and/or signature)
- **Working with children card**

List 3
Evidence of current residential address

- **Driver's licence renewal notice**
- **Financial institution statement** less than six months old
- **Motor vehicle registration**
- **Property lease** or **tenancy agreement**
- **Shire/water rates notice**
- **School** or other **educational report** or **certificate** less than twelve months old
- **Utility account** less than six months old (e.g. gas, electricity, home phone etc)

Норвегия

Имеется 3 системы идентификации граждан:

- Государственная Min ID (MyID - для граждан с 13 лет), использует национальный Id, возможна первичная идентификация по номеру мобильного телефона с OTP, который приходит по SMS. Доступ к онлайн-сервисам более 50 госуслуг.
- Банковская – более высокий уровень гарантий, чем Min ID. Использует набор механизмов безопасности, включая смарт-карты и ЭП на SIM. На июнь 2010г. охвачено более 2,5 млн. из 4.7 млн населения
- BuyPass. Использует смарт-карты и мобильные телефоны

Голландия

Compulsory identification

Compulsory identification at the workplace

Passports, identity cards and Dutch nationality certificates

The Citizen Service Number (BSN)

The Municipal Personal Records Database

Use of biometric data of foreign nationals

Положения Regulation 910/2014

(12) Одной из целей настоящего регламента является устранение существующих барьеров на пути трансграничного использования средств электронной идентификации, применяемых в странах - членах ЕС для аутентификации при доступе по крайней мере к государственным услугам.

(13) У стран - членов ЕС должен оставаться выбор в использовании или во вводе в действие средств для электронной идентификации при доступе к онлайн-услугам. Они также должны иметь возможность решать, следует ли привлекать частные компании к поставке этих средств.

Положения Regulation 910/2014

(14) В Регламенте должны быть определены некоторые условия в отношении того, какие средства электронной идентификации должны быть признаны, и как должно осуществляться уведомление об этих схемах.

(15) Обязательство признавать средства электронной идентификации относится только к тем средствам, уровень гарантии установления личности который соответствует равному или более высокому, чем уровень, требуемый для доступа к услуге, о которой идет речь.

(16) Уровни гарантии должны характеризовать степень уверенности в способности средств электронной идентификации устанавливать идентичность лица таким образом, чтобы обеспечить гарантию, что лицо, заявившее об определенной идентичности, действительно является тем лицом, которому данная идентичность была назначена.

Положения Regulation 910/2014

(19) Безопасность схем электронной идентификации является ключом к заслуживающему доверия трансграничному взаимному признанию электронных средств идентификации. В этом контексте страны - члены ЕС должны сотрудничать в вопросах обеспечения безопасности и совместимости схем электронной идентификации на уровне ЕС.

(20) Сотрудничество стран -- членов ЕС должно служить технологической совместимости заявленных схем электронной идентификации, с тем чтобы способствовать высокому уровню доверия и обеспечению безопасности, соответствующей степени риска.

(21) Настоящий регламент должен также установить общую законодательную базу для использования доверенных электронных служб.

Положения Regulation 910/2014

(30) Страны - члены ЕС должны назначить надзорный орган или надзорные органы для осуществления надзорной деятельности в соответствии с настоящим Регламентом.

(31) Надзорные органы должны сотрудничать с органами защиты данных, например путем информирования их о результатах аудита квалифицированных поставщиков доверенных служб, в тех случаях, когда, предположительно, были нарушены правила защиты персональных данных. Предоставленная информация, в частности, должна отражать инциденты безопасности и факты нарушений безопасности персональных данных.

(37) Настоящий Регламент устанавливает ответственность для всех поставщиков доверенных служб. В частности, он устанавливает режим ответственности, в соответствии с которым все поставщики доверенных служб должны нести ответственность за ущерб, причиненный любому физическому или юридическому лицу в результате несоблюдения обязательств в соответствии с настоящим Регламентом.

Регламент 910/2014, ст.6

Когда электронная идентификация, использующая средства электронной идентификации, и аутентификации определены к использованию национальным законодательством или административной практикой для доступа к службе, обеспечиваемой в онлайн-режиме организацией государственного сектора, в одной стране – члене ЕС, средства электронной идентификации, выпущенные в другой стране – члене ЕС, должны признаваться в первой стране – члене ЕС для целей трансграничной онлайн-аутентификации в этой службе, при соблюдении следующих условий:

(a) такие средства электронной идентификации выпущены в соответствии со схемой, которая включена в список, опубликованный Комиссией в соответствии со Статьей 9;

(b) уровень гарантии этих средств электронной идентификации соответствует уровню гарантии, равному или более высокому, чем уровень гарантии, требуемый соответствующей организацией государственного сектора для онлайн-доступа к этой службе в первой стране – члене ЕС, при условии что уровень гарантии этих средств электронной идентификации соответствует существенному уровню гарантии или более высокому

(c) соответствующая организация государственного сектора использует существенный уровень гарантии или более высокий в отношении онлайн-доступа к этой службе.

Регламент 910/2014, ст.8

Уровни гарантии электронных схем идентификации

1. Электронная схема идентификации, заявленная в соответствии со Статьей 9, должна указывать уровни гарантии низкий, существенный и/или высокий для электронных средств идентификации, выпущенных по этой схеме.

2. Уровни гарантии – низкий, существенный и высокий – должны удовлетворять следующим критериям соответственно:

(a) низкий уровень гарантии должен характеризовать средства электронной идентификации в контексте схемы электронной идентификации, которая обеспечивает ограниченную степень уверенности в заявленной или утвержденной подлинности лица и описывается ссылкой на технические спецификации, стандарты и процедуры, к ней относящиеся, включая технические средства управления, назначением которых является уменьшение риска ненадлежащего использования или изменения подлинности.

(b) существенный уровень гарантии должен характеризовать средства электронной идентификации в контексте схемы электронной идентификации, которая обеспечивает существенную степень уверенности в заявленной или утвержденной подлинности лица и характеризируется ссылкой на технические спецификации, стандарты и процедуры, к ней относящиеся, включая технические средства управления, назначением которых является существенное уменьшение риска ненадлежащего использования или изменения подлинности.

(c) высокий уровень гарантии должен характеризовать средства электронной идентификации в контексте схемы электронной идентификации, которая обеспечивает более высокую степень уверенности в заявленной или утвержденной подлинности лица, чем электронные средства идентификации с существенным уровнем гарантии, и характеризируется ссылкой на технические спецификации, стандарты и процедуры, к ней относящиеся, включая технические средства управления, назначением которых является предотвращение ненадлежащего использования или изменения подлинности..

ст.8. Минимум технических спецификаций

(a) процедуры доказательства и проверки подлинности физического или юридического лица, подающего заявку на выпуск средств электронной идентификации;

(b) процедуры выпуска запрошенных средств электронной идентификации;

(c) механизма аутентификации, в котором физическое или юридическое лицо использует средства электронной идентификации для подтверждения его подлинности доверяющей стороне;

(d) сущности, использующей средства электронной идентификации;

(e) любой другой организации, вовлеченной в подачу заявки на выпуск средств электронной идентификации; и

(f) технических спецификаций и спецификаций безопасности выпускаемых средств электронной идентификации.

Такие акты введения в действие должны быть приняты в соответствии с процедурой экспертизы, описанной в Статье 46(2).

Анализ изменений 1999/93 vs 910/2014

1. Требования SSCD (Security Signature Creation Device) сменились на QSCD (Qualified Signature Creation Device). Теперь все устройства генерации электронной подписи должны быть в списке квалифицированных, который утверждается Комиссией ЕС
2. Однозначно прописаны уровни доверия к идентификации и аутентификации.
3. Доверенные сервисы должны поставляться и поддерживаться квалифицированными поставщиками доверенных служб (УЦ).
4. Для аутентификации Web-сайтов необходимо выпускать квалифицированный сертификат доступа, в котором идентифицируется владелец сайта. Выпускать такие сертификаты может только квалифицированный поставщик доверенных служб

Нормативная база в РФ

Слово «идентификация» встречается 4490 раз. В том числе в названии документа.

- Пример: «Положение об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» утв. Банком России 19.08.2004 №262-П, зарег.в Минюсте РФ 06.09.2004 №6005.

Слово «аутентификация» встречается 123 раза:

- В названии 3-х Постановлений Правительства (977, 584, 1135);
- В приказе Минкомсвязи № 107 (в Положении 107 5.2-5.4) от 13.04.2012г.
- В Решении Верховного Суда РФ от 29.05.2012 N АКПИ12-645

Проблемы нормативной базы в РФ

Имеется существенное отставание отечественной нормативной базы по регулированию процессов идентификации и аутентификации (ИА) при электронном взаимодействии от уровня регулирования ИА в развитых странах.

Отличительной особенностью существующей в РФ нормативной базы в части ИА является полная независимость от технологий.

Вопросы безопасности и надежности процессов ИА не регулируются, что не позволяет проводить оценку качества сервисов ИА.

Понятийный аппарат нуждается в срочном реформировании.

Оценка перспектив

1. Имеется два подхода к решению представленных задач: быстро и правильно
2. Правильно (на федеральном уровне) задачи будут решены не скоро. Нет стратегии построения пространства доверия к аутентификации.
3. Быстро требования к идентификации и аутентификации можно выработать на уровне предприятия.
4. На отраслевом уровне решения появятся не скоро.

Выводы

1. Вопросы безопасности и надежности процессов идентификации и аутентификации в отличие от развитых стран практически не регулируются, что не позволяет проводить оценку качества, безопасности и надежности сервисов идентификации и аутентификации.
2. Необходимо введение уровней достоверности идентификации и аутентификации.
3. Сформулированные выводы должны найти отражение в нормативной базе Российской Федерации по ИБ.

Спасибо за внимание!