КОМПЬЮТЕРНАЯ МАТЕМАТИКА

УДК 681.3.06

А.О. МЕЛАЩЕНКО, О.Л. ПЕРЕВОЗЧИКОВА, Е.С. СКАРЛАТ

ЭЛЕКТРОННАЯ ИДЕНТИФИКАЦИЯ КАК ЧАСТЬ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Аргументирована целесообразность австрийского подхода и рассмотрены детали внедрения eID, как основы электронной идентификации в информационном обществе, построенном на цифровых подписях, шифровании и аутентификации.

Введение. С 2005 г. в Украине работает Национальная система электронных цифровых подписей (НСЭЦП), как основа доверия в информационном обществе. Однако до настоящего времени НСЭЦП не интероперабельна по организационным и ряду технологических причин, что в свою очередь не дало ей развиться в полноценную отрасль и базис информационного общества.

В конце 2010 г. в поддержку интероперабельности НСЭЦП разработано около 70 стандартов и поставлен вопрос о создании Технического регламента НСЭЦП. В перспективе запланировано решить проблемы интероперабельности и кроссертификации посредством внедрения эталонной модели квалифицированной инфраструктуры открытых ключей (QPKI).

Цель данной работы – исследовать пути развертывания электронной идентификации с поддержкой услуг электронной цифровой подписи (ЭЦП), шифрования и аутентификации в Украине при условии интероперабельной НСЭЦП.

После достижения интероперабельности НСЭЦП и преследуемой, в первую очередь, государством цели развертывания информационного общества как средства «делать бизнес» требуется предоставить гражданам средства, допускающие информационные услуги с минимальной затратой ресурсов. Способ достижения поставленной задачи показан на рис. 1.

В системе электронной идентификации (eID) гражданину требуются средства для

работы с кредитно-финансовой системой и обеспечения доверия, т. е. необходимы ЭЦП, шифрование и дополнительная память для идентификационной информации. Главная задача – реализация интероперабельных программно-аппаратных средств, обеспечивающих функциональность eID.

Электронная идентификация в Европе. С 2005 г. начат проект по электронной идентификации граждан из государвств-членов ЕС. Уже 32 страны внедрили собственные профили идентификации граждан, в первую очередь, для услуг электронного правительства (eGovernment) на национальном уровне. Для развертывания систем eID и eGovernment необходима интероперабельная реализация систем всех государств-членов ЕС.

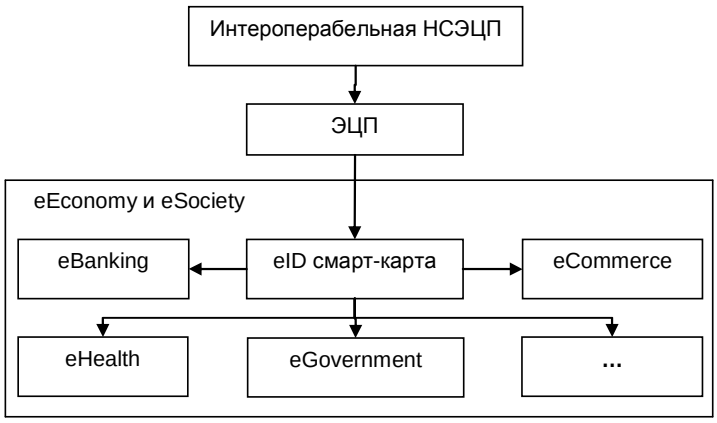

РИС. 1. Схема развертывания услуг информационного общества

Пока правительство Украины пытается создать электронную идентификацию своих граждан на национальном уровне, развитые страны переходят на новую ступень информационного общества, оптимизируя и усиливая механизмы идентификации и защиты прав человека. Системы управления идентификацией (IdM) предназначены для передачи, хранения и обработки персональных данных и составляют надежный механизм защиты информации, построенный на регистрации, аутентификации и авторизации. У каждого человека в реальном и цифровом мире может быть множество идентичностей в зависимости от его сферы деятельности, прав или привилегий. Например, работающий на государственной службе имеет личный номер служащего, а как покупатель сети магазинов имеет карту постоянного клиента, допускающую покупку товара со скидкой. Атрибуты составляют суть концепции «псевдо-идентичности», построенной на наборе данных (свойств идентичности), управляемых IdM системами.

Каждое государство разрабатывает собственные схемы управления eID, локализуя базовую архитектуру IdM системы, способной обрабатывать все модели идентификации для достижения интероперабельности, например, в пределах ЕС.

Задача сводится к профилированию и локализации базовой архитектуры систем eID и eGovernment под специфику конкретного государства (рис. 2) [1, 2].

Электронная идентификация в Украине. Необходимость построения системы электронной идентификации в Украине обусловлена тем, что с 1 января 2015 г. будет запрещен въезд на территорию ЕС и США по паспортам с вклеенными фотографиями. Как и 189 государств-членов Международной организации гражданской авиации (ICAO), Украина взяла на себя обязательство до 1 апреля 2010 г. обеспечить своих граждан электронными загранпаспортами, в которых на микрочип записана информация о владельце (в том числе его биометрические данные).

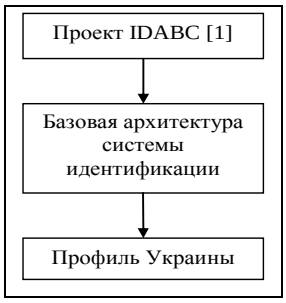

РИС. 2. Цепочка внедрения системы eID

В настоящее время Украина создает информационные ресурсы государственного значения, большинство которых будут построены на документных базах, т. е. безопасном хранении электронных документов с ЭЦП. Внедрение электронного документооборота в государственных органах значительно снизит издержки и время обработки документов. Имея государственные информационные ресурсы и ставя цель построения eGoverment как отрасли, снижающей издержки и ускоряющей документооборот, необходимо внедрить механизмы аутентификации и авторизации граждан и юридических лиц для доступа к электронным услугам.

Построенные на базе смарт-карт eID позволяют реализовать «двойную» идентификацию личности, используя привычную фотографию и / или другие цифровые средства (QPKI) (рис. 3). Карта eID каждого гражданина будет единственным используемым документом решающим четыре базовых задачи:

РИС. 3. Пример eID

– аутентификация и авторизация во множестве услуг информационного общества;
– создание и верификация ЭЦП;
– услуги шифрования;
– вмещать всю информацию, которую сейчас содержит паспорт, идентификационный код, банковские карточки, медицинские данные, биометрику, информацию, необходимую для любой легальной деятельности человека.

Карта eID избавит от множества банковских или дисконтных карточек и различных документов, подтверждающих личность.

Ресурсы систем eID. В каждой стране при введении eID необходимо определить ресурсы идентификации (электронные и традиционные), используемые для целей управления идентификацией в государстве (включая идентификационные карты и реестры), даже если эти компоненты не используются в электронном контексте. Иллюстрация возможных ресурсов для систем идентификации показана на рис. 4.

Важным понятием в ресурсах идентификации являются средства идентификации: любой hard- и software или их комбинация, содержащая достоверную информацию, например, данные, свидетельствующие о целостности атрибутов

идентификации. Примерами средств идентификации могут быть: смарт-карты, USB накопители, мобильные телефоны, содержащие сертификаты PKI или даже сами сертификаты.

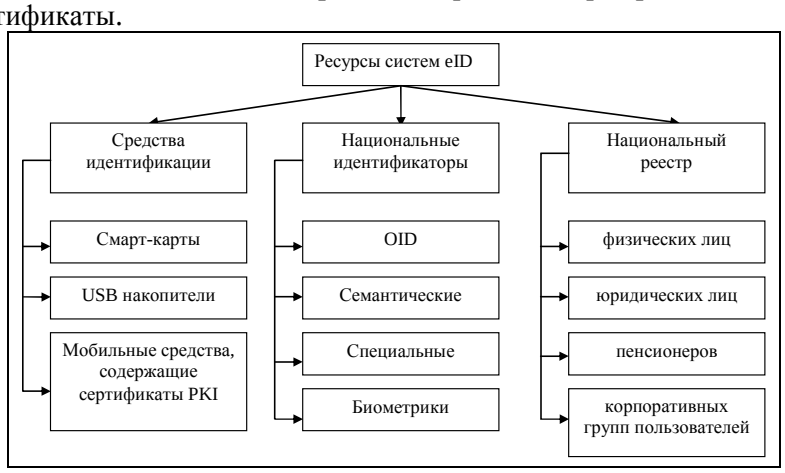

РИС. 4. Ресурсы систем eID

Одним из видов средств идентификации являются eID-карты, т. е. карты с микрочипами. В странах ЕС внедренные решения не обязательно суть смарт-карты, в стране может быть серия стандартов для создания совместимых карт. Из 32 стран 27 стран уже выпустили ID карты, из них: 7 стран используют бумажные карты идентификации, 13 стран – бумажные ID карты и разрабатывают eID карты и еще 7 стран уже используют карты eID. А пять стран (Дания, Ирландия, Норвегия, Латвия и Великобритания) не выпустили ID карты, а ориентировались сразу на eID карты. Констатируем, что ID карты являются главным методом идентификации в Европе, а eID карты в инфраструктуре QPKI считаются наиболее перспективным решением для замены бумажных ID карт уже в ближайшем будущем во всех странах ЕС.

После идентификации ресурсов необходимо описать национальные идентификаторы как некий код, присвоенный конкретному объекту и однозначно его идентифицирующий среди группы объектов, так называемый объектный идентификатор OID. Большинство стран ЕС используют общие OID, не ограниченные доменом группы граждан или бизнес-сферой. Однако все правовые нормы использования таких идентификаторов могут варьироваться в зависимости от действующих законов и стандартов в конкретных странах. Например, в некоторых странах ЕС сквозные общие OID запрещены законом, поскольку они позволяют государству полностью проследить участие человека во всех сферах его деятельности и посягают на личную жизнь и свободу граждан.

Также используются семантические идентификаторы, например, дата рождения или пол граждан, однако считается, что они не безопасны для целей идентификации. Эти идентификаторы можно и не использовать непосредственно для идентификации, хотя криптопровайдеры могут требовать такую информацию для обеспечения доступа. Например, в Венгрии общие OID используются для

передачи информации в пределах разных ведомственных отделений, а атрибуты идентификации можно получить из баз данных после аутентификации вследствие ввода e-mail и имени лица.

Кроме общих, используют специальные идентификаторы, например, значение НДС (величина налогов или номер карточки социального страхования). Они требуют дополнительной ссылки на контекст использования.

Еще один важный ресурс – реестры идентификации. Официальный реестр определяется как созданный и управляемый органами государственной власти информационный фонд, в котором собраны идентификационные атрибуты объектов и к которому относятся с доверием. Определение реестра показывает их важность для систем eID, поскольку на таком базовом и надежном ресурсе государство может построить систему управления eID. Отметим, что такие реестры создаются на ведомственных уровнях, доступ к информации за пределами ведомств закрыт, что исключает утечку информации. Так, созданы реестры физических и юридических лиц, пенсионеров, инвалидов и других категорий лиц.

Верховная Рада 15 декабря 2006 года приняла в первом чтении проект Закона Украины «О Национальном демографическом реестре» [3]. В статье 9 этого законопроекта предусмотрено внесение в паспорт гражданина Украины для выезда за границу биометрических данных лица, а также применение для идентификации лиц биометрик на электронном носителе (микрочипе), который предполагается вмонтировать в правый форзац загранпаспорта.

Архитектура eID для Украины. eID-карта гражданина должна содержать набор инструментов для взаимодействия с организациями и органами власти через Интернет с обеспечением уровня доверия, эквивалентного физическим взаимодействиям в реальном мире. Как электронное средство подписания документов и идентификации личности, eID-карта должна содержать две пары ключей: одна пара используется для создания квалифицированной ЭЦП в приложениях типа eGovernment для аутентификации и авторизации граждан, а вторая – для подписания электронных документов и / или шифрования данных.

В настоящее время при построении eID систем и тесной интеграции информационных ресурсов страны для предоставления услуг eGovernment возникает проблема «большого брата», ввиду потенциального отслеживания государством всех сфер деятельности человека в нарушение ст. 32 Конституции Украины. Вторичная цель при построении eID систем – высокий уровень интероперабельности, допускающий негосударственным организациям задействовать механизмы eID в своих целях. Так, при организации электронного документооборота внутри организации можно значительно снизить издержки, связанные с построением или закупкой услуг QPKI в поддержку ЭЦП.

Для достижения поставленных целей в Украине целесообразны такие ресурсы:

– средства идентификации – смарт-карты, соответствующие CWA 14169 с API, определенные согласно ДСТУ EN 14890;

– национальные реестры, созданные согласно законопроекту «О Национальном демографическом реестре»;

– национальные идентификаторы sOID (см. рис. 5).

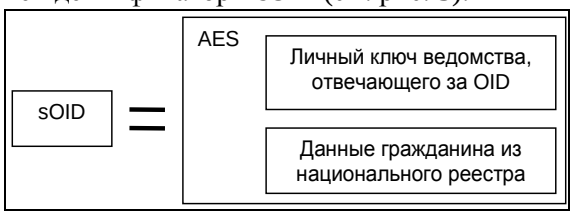

РИС. 5. Формирование sOID гражданина Украины

Национальные идентификаторы Украины. Заметим, что sOID не предназначен для прямого взаимодействия с ресурсами и службами идентификации, для этого гражданин формирует уникальный OID, основываясь на sOID и идентификаторе домена (рис. 6 и 7). Наличие sOID (или цепочек sOID) освобождает от обязательной верификации свойств гражданина в национальных реестрах всякий раз при использовании eID-карты, разумеется, сокращая ресурсы для процедур идентификации. Так, eID-карта гражданина N как предпринимателя, пенсионера и инвалида будет удостоверять наличие льгот при оплате жилищно-коммунальных услуг и проезда в городском транспорте.

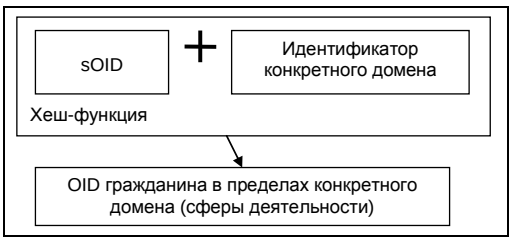

РИС. 6. Порядок получения идентификатора гражданина для конкретного домена

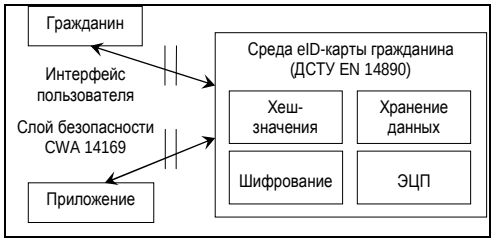

РИС. 7. Взаимодействие в системе eID

Построить такие eID системы достаточно сложно хотя бы потому, что необходимо решить нетривиальную задачу кодирования sOID для разветвленной инфраструктуры национальных реестров и потенциальных причинно-следственных связей и зависимостей между ними. Причем упрощение механизмов использования OID не снижает сложности задачи защиты информации от киберпреступников, с годами набирающихся опыта в своих попытках украсть идентичность.

Заключение. Построение систем электронной идентификации заключается в профилировании трех составляющих базовой архитектуры eID: средств идентификации, национальных реестров и национальных идентификаторов.

Особое внимание сосредоточено на формировании национальных идентификаторов, способных защитить граждан от сквозного отслеживания их деятельности государством. Наиболее целесообразный подход основан на форми-

ровании OID, с использованием базового sOID и идентификатора домена. Так можно обойтись без дорогостоящей техники, например, сканеров биометрических данных (сетчатки глаза, отпечатков пальцев и т. д).

Архитектура средств идентификации должна быть максимально простой для минимизации угроз безопасности и снижения нагрузок на каналы коммуникации. Этот принцип реализован в австрийской eID-карте, на основе которой предложена архитектура украинской eID с задействованием трех функций смарт-карты: шифрование, хеширование и хранение данных идентификации.

А.О. Мелащенко, О.Л. Перевозчикова, О.С. Скарлат

ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ ЯК ЧАСТИНА ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Обґрунтовано доцільність австрійського підходу та розглянуто деталі впровадження eID, як основи електронної ідентифікації в інформаційному суспільстві, побудованому на цифрових підписах, шифруванні та автентифікації.

A. Melashenko, O. Perevozchykova, O. Skarlat

ELECTRONIC IDENTIFICATION AS AN INTEGRAL PART OF INFORMATION SOCIETY

The main reasonable arguments of expediency are specified and the implementation details of the eID as a part of information society that supports the services of electronic digital signature, encoding, and authentication are considered.

1. *eID* Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability, November 2007/ http://ec.europa.eu/idabc/en/document/6484
2. *CWA* 15264 Architecture for a European interoperable eID system within a smart card infrastructure.
3. *Проект* Закону України «Про національній демографічний регістр», № 0878 від 23.11.2007, 1 сесія VI скликання ВР.
4. *Проект* Закону України «Про паспорт громадянина України та інші документи, що посвідчують особу і підтверджують громадянство України» № 7384-2 від 25.05.2005, 7 сесія IV скликання ВР.
5. *CWA* 14169 Secure signature-creation devices “EAL 4+”
6. *ДСТУ* EN 14890. Прикладний інтерфейс для смарт-карток, які використовують безпечні засоби створення підписів.
7. *ДСТУ-П* CWA 14355:2008. Рекомендації з реалізації безпечних засобів створення підписів.

Получено 09.12.2010

Об авторах:

Мелащенко Андрей Олегович,
младший научный сотрудник и аспирант Института кибернетики
имени В.М. Глушкова НАН Украины,

Перевозчикова Ольга Леонидовна,
член-корреспондент НАН Украины, доктор физико-математических наук,
профессор, зав. отделом Института кибернетики имени В.М. Глушкова НАН Украины,

Скарлат Елена Сергеевна,
младший научный сотрудник и аспирантка Института кибернетики
имени В.М. Глушкова НАН Украины.