Электронная цифровая подпись: использование в балтийских странах и возможности применения в вузах

Зайцева Лариса Витальевна
профессор, к.т.н., д-р инж. наук, заведующая кафедрой технологий разработки ПО,
Рижский технический университет,
ул. Межа, 1/3, г. Рига, LV-1048, Латвия, (371) 67089571
Larisa.Zaiceva@rtu.lv

Колышкин Павел Андреевич
б-р инж. наук, магистрант кафедры технологий разработки ПО,
Рижский технический университет,
ул. Межа, 1/3, г. Рига, Латвия, LV-1048, (371) 67089571
Pavels.Koliskins@gmail.com

Аннотация

В статье кратко рассмотрены теоретические аспекты электронной цифровой подписи и описано её использование в Латвии, Литве и Эстонии для получения различного рода справок, подачи деклараций и т.д. Возможности применения электронной цифровой подписи в вузах показаны на примерах подготовки экзаменационных (и зачётных) ведомостей, удалённой регистрации абитуриентов и зачисления студентов. Отмечены также другие сферы применения электронной цифровой подписи для упрощения делопроизводства вузах. Приведены результаты использования единой системы регистрации студентов в процессе приема студентов в Рижский технический университет в 2010 году.

The paper outlines theoretical aspects of a digital signature and describes a usage of it in Latvia, Lithuania and Estonia to obtain inquires of different types, to lodge declarations and so on. Possible applications of digital signature with the objective to simplify document processing in universities are described in the paper by means of the following examples: preparation of examination sheets, remote registration and admission of applicants. Some results of usage of unified system for registration and admission of applicants in Riga Technical University are outlined.

Ключевые слова

Электронная цифровая подпись, высшие учебные заведения, делопроизводство, удалённая регистрация абитуриентов

Digital signature, high learning institutions, clerical work, remote university entrant registration

Введение

Электронная цифровая подпись (ЭЦП) – это реквизит электронного документа, предназначенный для его защиты от подделки, идентификации владельца подписи, подтверждения целостности и отсутствия искажения информации в электронном документе [1]. В последнее время ЭЦП стала предметом активных дискуссий. Её использование даёт возможность оптимизировать большое количество процессов, в

которых необходимо точно идентифицировать и аутентифицировать человека. Подписанный в электронном виде документ имеет одинаковую юридическую силу с собственноручно подписанным документом [2]. Электронная цифровая подпись в настоящее время используется во многих странах (с 2002 года и в России) в банковской сфере, бухгалтерии, страховании и других областях. В России ЭЦП в основном применяют для сдачи налоговой отчетности. Так, в 2010 году свыше половины всех налоговых деклараций поступили в Федеральную Налоговую Службу в электронном виде [3]. Интересное применение ЭЦП нашли в Забайкальском крае, где особенно важен вопрос оперативной регистрации иностранных граждан (в этот регион традиционно приезжает большое количество гостей из стран Азии). Гостиницы Забайкальского края используют ЭЦП для электронной подачи форм регистрации в управление Федеральной миграционной службы, что позволяет быстро и оперативно решить вопрос, связанный с регистрацией иностранных гостей [4]. Электронное голосование, проводимое в Эстонии уже не один год, является другим прекрасным примером возможностей ЭЦП [5].

Финское предприятие Valimo, которое занимается разработкой и внедрением мобильной электронной цифровой подписи, предоставляет клиентам следующие возможности своего продукта: получать деньги из банкомата средствами мобильной аутентификации, подписывать документы и электронную почту, анонимно подтверждать свой возраст, использовать при NFC (Near Field Communication) платежах и т.д. [6]. Использование мобильной электронной подписи для получения денег из банкоматов является более безопасным способом, чем использование обычной банковской карты, поскольку магнитная лента банковской карты может быть скопирована. Несмотря на то, что в последнее время более популярным становится применение чип-карты, магнитная лента, скорее всего, еще долгое время останется на банковских картах, т.к. во многих странах она еще используется в банкоматах [7].

С точки зрения организации делопроизводства высшее учебное заведение ничем не отличается от любого другого учреждения. Это означает, что большинство всех вышеупомянутых услуг может быть использовано для оптимизации работы вуза. Однако в высших учебных заведениях существуют также уникальные процессы, в которых возможно применение электронной цифровой подписи. Цель статьи – ознакомить читателей с использованием электронной цифровой подписи в Балтийских странах и показать возможности применения ЭЦП в вузах.

Теоретические аспекты электронной цифровой подписи

В основе электронной цифровой подписи лежит ассимметричное шифрование – модель, в которой применяются пары ключей: открытый ключ и соответствующий ему закрытый ключ. Открытый ключ доступен всем, а закрытый ключ хранится в надёжном месте. Отличительная черта этой модели в том, что данные, зашифрованные открытым ключом, могут быть расшифрованы только при помощи соответствующего закрытого ключа, и наоборот [8].

У каждой пары ключей имеется свой хозяин – лицо или учреждение, для которого ключи были выпущены удостоверяющим центром. Для связи принадлежности конкретного открытого ключа и физического/юридического лица, используется цифровой сертификат. Цифровой сертификат обычно содержит информацию о субъекте и о принадлежащем ему отрытом ключе. Если субъектом является физическое лицо, то

цифровой сертификат, как правило, хранит персональные данные субъекта – имя, фамилию, персональный код и т.д.

Ассимметричное шифрование имеет достаточно широкое применение – идентификация и аутентификация, подписание документов и шифрование данных. Многие интернет-ресурсы идентифицируют и аутентифицирует пользователей, используя электронную цифровую подпись. Обычно это даёт возможность узнать персональный код субъекта, который хранится в цифровом сертификате, что, в свою очередь, очень точно идентифицирует физическое лицо. Подписание документа производится при помощи закрытого ключа, что даёт возможность любому субъекту при помощи цифрового сертификата убедиться в том, что документ подписан конкретным лицом. Шифрование данных производится при помощи открытого ключа, что позволяет адресовать личное сообщение конкретному лицу. Расшифровать сообщение можно только при помощи закрытого ключа. В последней схеме часто используют подход, когда данные шифруются третьим (симметричным) ключом, а сам ключ шифруется открытым ключом. Это ускоряет процесс шифрования и дешифрования.

Электронная цифровая подпись в Балтийских странах

Электронную цифровую подпись достаточно активно используют в Балтийских странах. Практически в каждой стране есть возможность приобрести электронную цифровую подпись на таких носителях, как интеллектуальная карта, USB-флеш-накопитель, а также частный случай интеллектуальной карты – SIM карта [9, 10]. У каждого носителя есть свои преимущества и недостатки, например, для использования интеллектуальной карты необходим компьютер и считыватель карт. Использование SIM карты даёт возможность идентифицировать и аутентифицировать свою личность удалённо, используя мобильный телефон, однако процесс аутентификации занимает немного больше времени. Это связано с тем, что при использовании мобильного устройства передача данных осуществляется при помощи GSM сети, у которой есть свои ограничения.

В каждой из Балтийских стран имеется свой государственный портал, представляющий различные электронные услуги, использование которых возможно при наличии электронной цифровой подписи [11-13].

Электронная цифровая подпись на основе интеллектуальной карты (смарт-карты) в Латвии была введена в 2006 году и сразу стала использоваться во многих коммерческих предприятиях. Так, на государственном портале Латвии (www.latvija.lv) приведен перечень полезных для жителей услуг: получение информации о своём семейном враче; получение справки об отсутствии судимости; получение справки на вырубку деревьев; подача декларации нового места жительства; подача декларации в налоговую службу; подача заявления о поступлении на дневное отделение в три университета Латвии — Латвийский университет (ЛУ), Латвийский сельскохозяйственный университет (ЛСУ) и Рижский технический университет (РТУ).

Несмотря на то, что при наличии ЭЦП появилась возможность быстро получить необходимые справки и подать различные заявления, использование электронной подписи не получило широкого распространения – за четыре года было выдано лишь 29083 смарт-карты. Поэтому 1 февраля 2011 года был открыт новый виртуальный портал э-подписи (www.eparaksts.lv), позволяющий проверить и подписать документы. При этом специальные карты, устройства и программное обеспечение не требуются. Принцип

работы ЭЦП – такой же, как у интернет-банка. Более того, идентификация личности происходит через интернет-банк ставящего подпись. Таким образом удалось упростить и удешевить процесс подписания документов, что, несомненно, будет способствовать активному использованию ЭЦП в Латвии.

В Эстонии, где ЭЦП введена в 2002 году, её используют в девяти банках для замены кодовых карт и кодовых калькуляторов [14]. Предлагаются также такие возможности, как цифровое подписание и шифрование документов, покупка ID-билета и другие. Следует отметить, что Эстония является первой страной в мире, которая в 2007 году использовала электронную цифровую подпись для выборов в парламент [5]. В электронных выборах тогда приняло участие 30 000 человек, что составляет 3% процента от общего количества избирателей с правом голоса. В настоящее время в Эстонии электронной подписью на базе ID-карты (удостоверения личности в виде пластиковой карты с магнитным носителем) пользуются 85% населения.

В Литве электронную цифровую подпись используют с 2004 года для подписания документов, идентификации жителей, в том числе и на государственном портале услуг, а также для подачи электронных заявлений на возвращение налогов, что позволяет избежать использования печатных документов и существенно экономить время [15].

Возможности применения ЭЦП в вузе

Ежедневно большое количество времени в высших учебных заведениях тратится на подписание документов (экзаменационных ведомостей, приказов разного уровня, отчетов по командировкам, договоров и т.п.). Основная проблема, связанная с подписанием документов, заключается в том, что документ обычно содержит несколько подписей. Поскольку лица, подписывающие документ, часто находятся в разных местах, приходится либо пересылать документ, либо перемещаться самим, на что требуется время. Для решения проблемы необходима возможность быстро и безопасно пересылать нужные документы на подписание. Одним из возможных решений является использование электронной цифровой подписи.

В качестве примера рассмотрим процесс заполнения экзаменационных ведомостей в вузе, с которым сталкиваются преподаватели, как минимум, два раза в год (рис. 1). В заполнении экзаменационных ведомостей обычно участвуют деканат, декан и преподаватель. Как видно из схемы на рисунке 1, центральным звеном является деканат, который играет роль посредника между преподавателем и деканом. В связи с тем, что декану приходится подписывать много экзаменационных ведомостей, в целях удобства деканат готовит пустые экзаменационные ведомости заранее. Декан подписывает пустые экзаменационные ведомости и передает их обратно в деканат. Далее ведомости заполняет преподаватель, а затем они сохраняются в информационной системе университета. Помимо сложности данного процесса, существует также проблема – декан подписывает пустые экзаменационные ведомости и не видит оценок студентов.

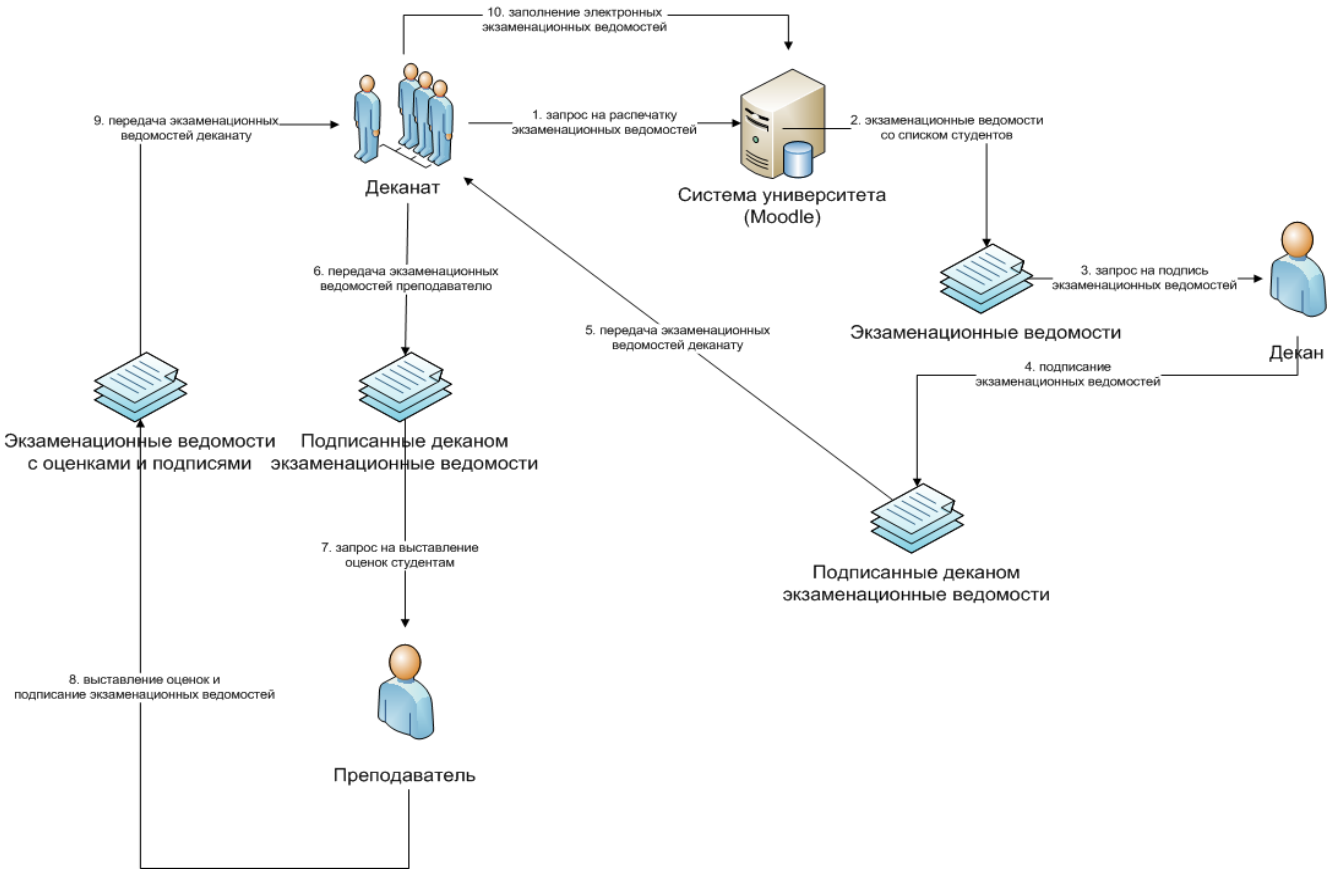

Рис. 1. Процесс заполнения экзаменационных ведомостей

Использование электронной цифровой подписи позволяет сократить время на выдачу и сдачу экзаменационных ведомостей. Основная идея заключается в том, что посредником между деканом и преподавателем становится информационная система университета, а не деканат. Улучшенный процесс может выглядеть следующим образом: деканат вводит информацию о студенте в систему, с помощью которой и подготавливаются электронные экзаменационные ведомости, преподаватель выставляет оценки и ставит свою электронную подпись, декан, получая электронное уведомление, подписывает документы, используя ЭЦП (рис. 2).

Рис. 2. Улучшенный процесс заполнения экзаменационных ведомостей

Рассмотрим основные возможности реализации улучшенной концепции. В большинстве высших учебных заведений Латвии информационные системы вузов разработаны на основе MOODLE, которая базируется на сетевых технологиях и написана на языке программирования PHP [16]. Наиболее распространёнными носителями электронной цифровой подписи являются интеллектуальная карта и SIM карта. При использовании SIM карты подписание происходит на мобильном телефоне, и передача данных между телефоном и сервером происходит через GSM сеть. Обычно данный процесс реализуется отдельным представителем услуги, который также предоставляет простой интерфейс третьим лицам для отсылки запроса и получения результата. Данные интерфейсы, как правило, используют открытые технологии (например, SOAP/XML), что позволяет довольно легко и быстро внедрить данную услугу на сетевые порталы, в том числе и на информационный портал университета [17]. При использовании интеллектуальной карты подписание происходит на самой карте через компьютер клиента, что создаёт некоторые проблемы. Сетевые технологии в целях безопасности не дают доступ к устройствам компьютера клиента, а также к файловой системе клиента. В качестве одного из решений может быть использована технология подписанной прикладной программы JAVA или, как другой вариант, ActiveX технология. Обе технологии дают возможность вызывать методы на интеллектуальной карте и отсылать полученные данные на сервер информационной системы университета [18].

В Рижском техническом университете с 2010/2011 учебного года отменены зачетные книжки студентов, а экзаменационные и зачетные ведомости заполняются преподавателями непосредственно в системе, как это показано на рисунке 2. По желанию преподавателя ведомости могут быть распечатаны делопроизводителем, который после заполнения их преподавателем вводит оценки в систему. Студенты, используя систему вуза, могут увидеть результаты сдачи ими зачетов и экзаменов.

Представленная на рисунке 2 концепция, включающая подготовку документа и его несколько подписаний с помощью ЭЦП, может быть использована для оптимизации остальных процессов делопроизводства вуза, например, таких, как подписание разовых договоров (о практике студентов и др.), сдача отчетов по командировкам и т.д.

Другим примером применения ЭЦП в вузе служит удалённая регистрация абитуриентов и зачисление студентов.

Ежегодно абитуриенты выбирают программу обучения и высшее учебное заведение, в котором планируют получить специальность. Часто абитуриенты подают заявления в несколько вузов одновременно: не знают, какое учебное заведения выбрать, не уверены в поступлении в желаемый вуз и т.д., а затем выбирают то учебное заведение, которое предлагает более выгодные условия (бюджетные места, стипендии, возможность обучения за границей и др.). Здесь возникают две проблемы:

- регистрация абитуриентов. Проблема связана с тем, что время подачи заявлений ограничено, поэтому большое число абитуриентов создает длинные очереди в высших учебных заведениях;
- зачисление студентов. Заявления подаются в несколько вузов, каждый из которых может зачислить абитуриента в число студентов, а учиться он будет в каком-то одном. В результате в других вузах остаются свободные места, на которые можно было бы принять следующего по рангу абитуриента.

Если первую проблему решить достаточно просто, принимая заявления и необходимые документы по электронной почте, то вторая требует особого внимания.

Для решения этой проблемы предлагается концепция удалённой регистрации абитуриентов и зачисления студентов, которая позволит при помощи одной регистрации подать заявления в несколько ВУЗов одновременно. Для более детального решения проблемы рассмотрим нынешнюю регистрацию абитуриентов в Латвии.

В 2010 году на регистрацию абитуриентов в пунктах приёма было выделено всего 8 дней, а на частично-удалённую регистрацию - 15 дней [19]. Частично-удалённая регистрация давала возможность удалённо оплатить регистрацию, а также подать базовое заявление на поступление. Для того, чтобы закончить регистрацию, абитуриенту всё равно было необходимо явиться в высшее учебное заведение и сдать свидетельство об окончании среднего учебного заведения, а также предъявить оценки по централизованным экзаменам. В связи с тем, что на регистрацию абитуриентов было выделено всего 8 дней, а количество заявлений в три университета превысило 45 000, в обслуживании абитуриентов принимало участие большое количество персонала университетов. При регистрации каждого абитуриента делаются бумажные или цифровые копии удостоверяющих документов, свидетельств об окончании средних учебных заведений, а также выписки оценок экзаменов, что, несомненно, требует дополнительного времени и дополнительных ресурсов (бумага, затраты на печать). Следует отметить, что стоимость регистрации напрямую зависит от сложности этого процесса. При использовании ЭЦП посещение абитуриентом вуза не требуется, а также снижаются расходы на регистрацию.

Обычно ранги абитуриентов создаются на основе оценок централизованных экзаменов, проверкой которых занимается специальное управление, выдающее также сертифицированную выписку оценок. Наличие интерфейса, позволяющего получить результаты централизованных экзаменов конкретного абитуриента, является ключевой необходимостью в реализации полной удалённой регистрации абитуриентов. Для успешной регистрации абитуриентов высшему учебному заведению необходимо:

1) идентифицирующий документ абитуриента (например, паспорт);
2) выписка оценок централизованных экзаменов;
3) свидетельство об окончании среднего учебного заведения;
4) декларированное место жительства и контактные данные.

Благодаря тому, что авторизация средствами электронной цифровой подписи позволяет идентифицировать субъекта, а также гарантирует правильность персональных

данных субъекта, в том числе и персонального кода, всю необходимую информацию можно было бы получить из внешних систем. Как известно, персональный код однозначно идентифицирует субъекта, что даёт возможность получить информацию о паспорте и декларированном месте жительства из системы регистра жителей. Данная услуга уже доступна жителям Латвии на официальном электронном портале страны [20].

Свидетельство об окончании среднего учебного заведения может быть выдано при успешной сдаче централизованных экзаменов. Управление, занимающееся проверкой централизованных экзаменов, выдаёт результаты экзаменов для конкретного человека и для конкретного среднего учебного заведения. Из этого следует, что информацию об оценках абитуриента и об оконченном среднем учебном заведении можно получить от управления, занимающегося проверкой централизованных экзаменов. Получив все необходимые данные об абитуриенте, высшие учебные заведения могли бы упорядочить его по запрошенным программам вуза и вернуть результат системе регистрации абитуриентов. Таким образом, в конечном итоге абитуриент получит информацию о своем текущем ранге во всех запрошенных высших учебных заведениях. Графически концепция удалённой регистрации показана на рисунке 3. В целом, данная схема решает проблему регистрации абитуриентов, но актуальным остается вопрос, связанный с зачислением студентов. После конечного выбора учебной программы необходимо оповестить те вузы, в которых абитуриент учиться не будет. Это даст возможность обновить текущие таблицы рангов, что сможет повлиять на решение других абитуриентов (после отказа одного абитуриента другой сможет получить его бюджетное место, стипендию). На рисунке 4 изображена концепция оповещения выбора абитуриента.

Когда абитуриент определился с конечной учебной программой, он с помощью ЭЦП подтверждает свой выбор в системе регистрации абитуриентов. Далее происходит автоматическое оповещение всех вузов, в которые были поданы заявления. Один из вузов, который выбрал абитуриент, получает положительное оповещение, а все остальные – отрицательное. Далее происходит автоматическое обновление рангов других абитуриентов. При существенных изменениях рангов (абитуриент получил бюджетное место или стипендию) происходит рассылка информативных сообщений абитуриентам.

В среднем процесс на подачу заявления и конечный выбор учебной программы занял бы у абитуриента не более 10 минут. Помимо того, что данный подход является более быстрым и удобным, чем очная регистрация, он также обладает большим преимуществом – система предоставляет самые последние ранги абитуриентов, что довольно трудно осуществить при очной регистрации. При необходимости данную концепцию можно изменить, добавив в нее другие звенья, например, возможность оплаты.

Таким образом, преимуществами использования ЭЦП являются: сокращение временных затрат абитуриента (отпадает необходимость посещения вуза) и приемной комиссии за счет автоматизации расчета ранга абитуриента и составления списка зачисленных; сокращение финансовых затрат на процесс приёма студентов (меньший состав приемной комиссии, не требуется копирование документов и т.п.). Недостаток использования ЭЦП – получение сертификата ЭЦП и подписание документов требуют определенных финансовых затрат.

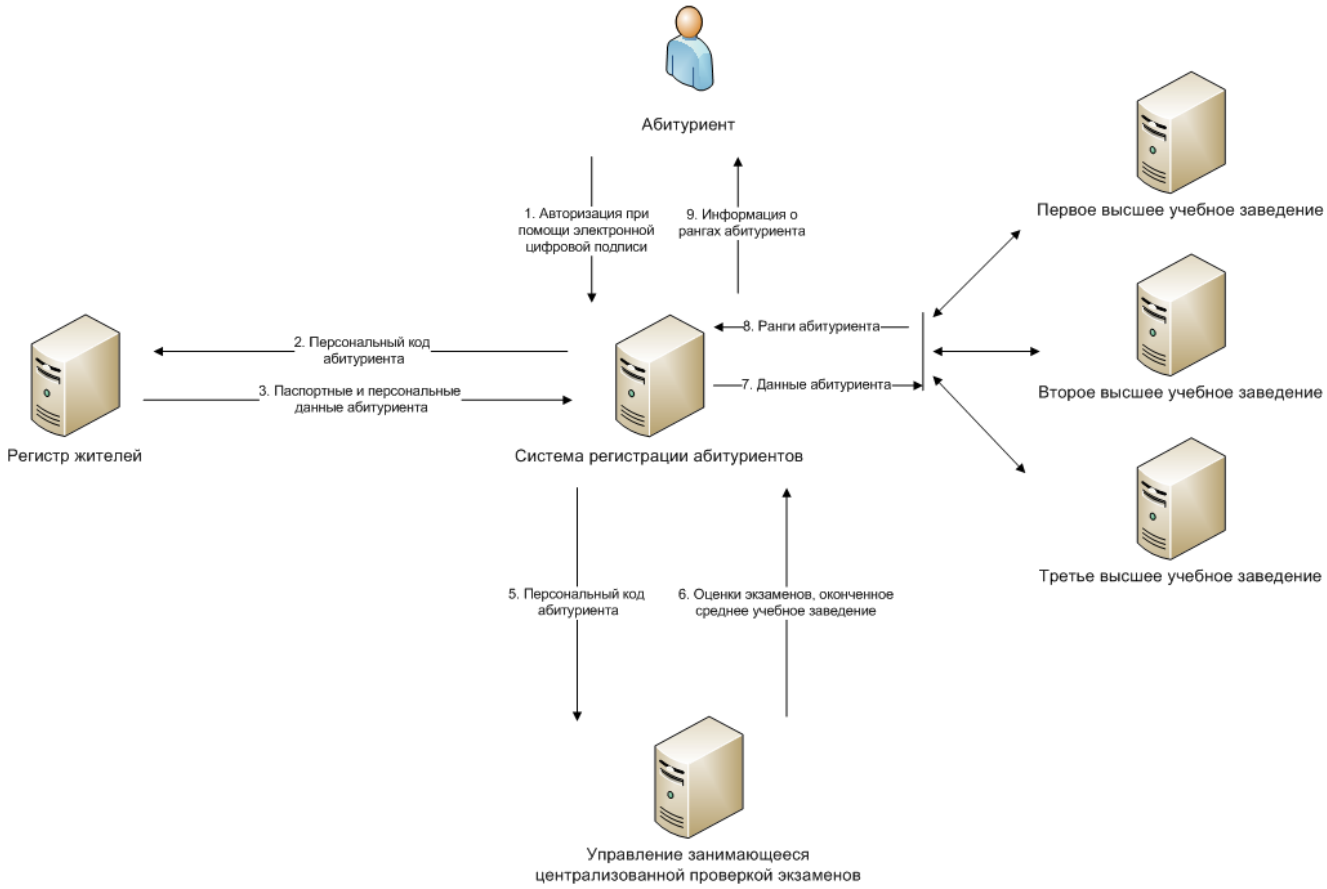

Рис. 3. Концепция удалённой регистрации

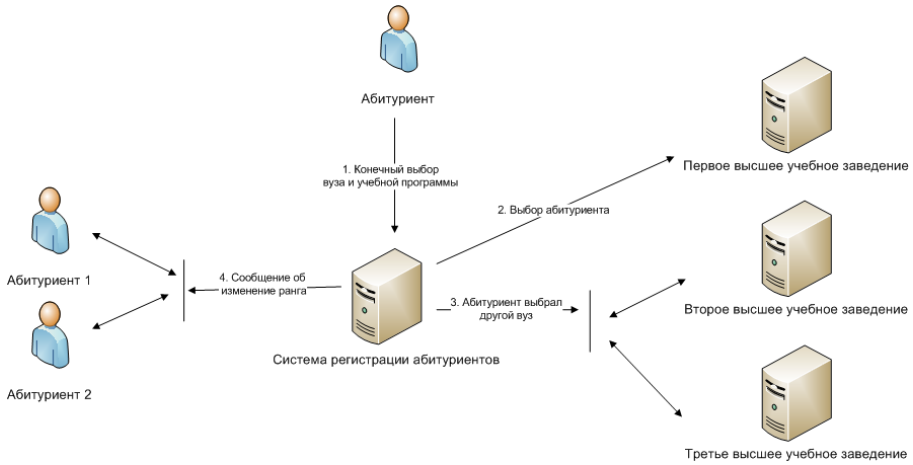

Рис. 4. Концепция оповещения выбора абитуриента

Заключение

В Латвии с привлечением средств Европейских фондов была разработана единая система регистрации студентов, в которой частично реализована концепция, представленная на рисунке 3 (без использования ЭЦП). Система была опробована в 2010 году при приеме студентов в три крупнейших вуза республики: ЛУ (Рига), ЛСУ (Елгава), РТУ (Рига). Используя систему, заявления в вуз подали 8950 абитуриетнов, а число ее пользователей превысило 13000. При подаче заявления абитуриент мог указать несколько выбранных программ этих трех вузов в порядке их приоритета. При зачислении на первую из выбранных программ сведения автоматически поступали ответственным за остальные программы. Это позволило устранить дублирование при зачислении студентов в вуз. В результате в РТУ число «свободных» мест сократилось на 22,9% и составило лишь 7,7% [17]. Подобные системы также успешно применяются в Литве и Эстонии.

Однако такие безусловно полезные системы предусматривают лишь частично-удаленную регистрацию абитуриентов. Использование электронной цифровой подписи позволило бы еще больше автоматизировать процесс регистрации абитуриентов и зачисления студентов в вузы, сократив количество персонала приемных комиссий вузов.

В настоящее время электронная цифровая подпись является быстро развивающимся продуктом, и, несомненно, в ближайшем будущем она станет такой же неотъемлемой частью повседневной жизни, каким на данный момент является электронная почта.

Литература

1. ОАО „АК „ЦНИИСУ” / Интернет – http://www.akcniisu.ru/services/ud-centre/ (дата обращения: 10.01.2011)
2. Federal Trade Commission - ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT / Интернет – http://www.ftc.gov/os/2001/06/esign7.htm (дата обращения: 03.01.2011)
3. Кордон-Налог - Отдел средств криптографической защиты информации / Интернет – http://www.lenta.ru/articles/2010/08/02/digising/ (дата обращения: 18.01.2011)
4. EKEY.RU Удостоверяющий центр – ЭЦП ekey.ru для регистрации иностранных граждан в России / Интернет – http://www.ekey.ru/news/422 (дата обращения: 20.01.2011)
5. Estonian ministry of foreign affairs - Estonian e-voting system / Интернет – http://www.vm.ee/?q=en/node/5693 (дата обращения: 13.12.2010)
6. Valimo Wireless - Benefits of Using Valimo Mobile ID / Интернет – http://www.valimo.com/partners/benefits (дата обращения: 30.12.2010)
7. iPhone Development Summit - Valimo Wireless' Mobile Signatures Combat ATM Fraud / Интернет – http://iphonedevmar08.sys-con.com/node/499948 (дата обращения: 02.01.2011)
8. Баричев С. Криптография без секретов – Горячая Линия - Телеком, 2008. – 47 р.
9. ID.EE - Электронное голосование / Интернет – http://www.id.ee/11069?id=11076 (дата обращения: 16.12.2010)

10. Skaitmeninio Sertifikavimo Centras – Įvadas (центр цифровой сертификации – введение) / Интернет – http://www.ssc.lt/?name=menu_p&act=main (дата обращения: 16.12.2010)
11. EESTI.EE – Avaleht (главная страница портала) / Интернет – http://www.eesti.ee/est/ (дата обращения: 19.12.2010)
12. Elektroniniai valdžios vartai (электронный правительственный портал) / Интернет – http://www.epaslaugos.lt (дата обращения: 18.12.2010)
13. Latvija.lv - Ceļvedis e-Latvija (путеводитель) / Интернет – https://www.latvija.lv/Default.aspx (дата обращения: 20.12.2010)
14. ID.EE - Web-based services with ID-card support / Интернет – http://www.id.ee/11108 (дата обращения: 20.12.2010)
15. BITE.LT - Mobile electronic signature / Интернет – http://www.bite.lt/en/bc/esign? (дата обращения: 03.01.2011)
16. MOODLE - About Moodle / Интернет – http://docs.moodle.org/en/About_Moodle (дата обращения: 26.12.2010)
17. Суковскис У. Результаты приема студентов. Единый прием // Jaunais inženieris. – 2010. – № 1388. – с. 10-11 (на латышском языке)
18. Preliteiro M., Zefferer T. STORK Work Item 3.2.5 eID OSS Middleware – STORK-eID Consortium, 2008. – 39 p.
19. Latvija.lv - Kā pieteikties studijām? (как подать заявление в вуз) / Интернет – https://www.latvija.lv/LV/WebLinks/portal/ka-pieteikties.htm (дата обращения: 22.12.2010)
20. Latvija.lv - Mani dati Iedzīvotāju reģistrā (мои данные в регистре жителей) / Интернет – https://www.latvija.lv/LV/LDV/EServiceDescription.aspx?catid=1DZIV_VIETA_NEKIP_BUV&srvid=URN:IVIS:100001:EP-EP01-v1-1 (дата обращения: 22.12.2010)
21. AS Sertifitseerimiskeskus - DigiDocService specification / Интернет – http://www.sk.ee/files/DigiDocService_spec_eng.pdf (дата обращения: 28.12.2010)