УДК 004.056

Н.А. Богульская, М.М. Кучеров, В.П. Кушнир

Разработка алгоритмов защищенных приложений для социальных карт

Рассмотрены разработка и применение аутентификационного устройства на основе пластиковой карты. Данное устройство может применяться не только для СКУД, но и для проверки принадлежности к группам и подгруппам в Сибирском федеральном университете.

Ключевые слова: социальная карта, аутентификация, ключ, защита информации.

Устойчивость и сбалансированность масштабной системы мер социальной поддержки населения, реализуемой в настоящее время в Российской Федерации, возможно обеспечить только посредством активного использования современных информационных технологий, позволяющих создать интегрированную информационную систему предоставления и учета адресных социальных услуг на основе унифицированных электронных носителей.

Начиная с 2008 г. в Красноярском крае реализуется проект «Единая социальная карта Красноярского края». Это направление было определено важным как с точки зрения повышения эффективности использования выделяемых бюджетных средств, так и с точки зрения обеспечения безопасного доступа населения к индивидуальным персонифицированным ведомственным базам данных. Проект охватит слои населения Красноярского края, имеющие право на социальную поддержку в соответствии с законодательством. На первом этапе – это жители края, получающие поддержку за счет федерального, регионального и муниципального бюджетов. В дальнейшем возможно, что «Единая социальная карта Красноярского края» станет универсальным электронным удостоверением каждого жителя Красноярского края.

«Единая социальная карта Красноярского края» – именная пластиковая карта (СК), которая выдается лицу, имеющему право на получение мер социальной поддержки в соответствии с законодательством России и Красноярского края, и служит индивидуальным электронным ключом к информации о персональных данных ее держателя, имеющихся в ведомственных информационных базах. Составляющие элементы карты представлены на рис. 1.

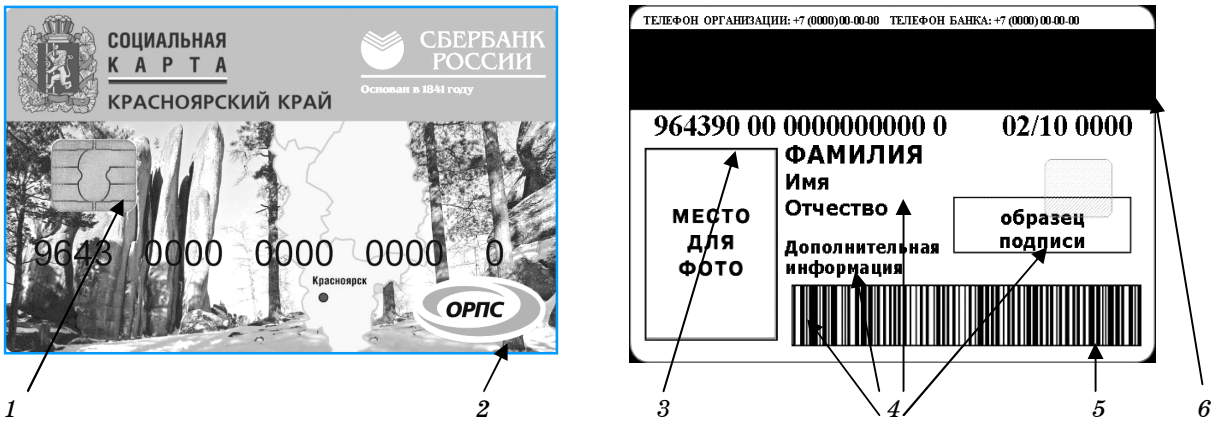

Рис. 1. Единая социальная карта Красноярского края

Технические характеристики карты Optelio Contactless производства компании Gemalto: микропроцессор (*1*), поддерживающий контактный и бесконтактный радиоинтерфейс, с размещенными на нем нефинансовыми и финансовым приложениями; признак платежной системы (*2*); социальный номер держателя карты (*3*); персональные данные (*4*); штриховой код, содержащий социальный номер держателя карты (*5*); магнитная полоса (*6*). Карта Optelio Contacless позволяет осуществлять внутренний обмен данными между контактной и бесконтактной частью микропроцессора.

На унифицированной социальной карте размещены следующие приложения: социальное, транспортное, ЖКХ, медицинское, налоговое, пенсионное, дисконтное и бан-

ковское. По мере развития проекта на карте могут появиться дополнительные приложения. Одновременно с выдачей ПК должны формироваться планы организации инфраструктуры их обслуживания в соответствующих районах Красноярского края.

Для того чтобы сделать более удобными повседневные действия студентов, преподавателей и персонала СФУ, необходима система, которая позволит использовать в СФУ социальные карты. Данное устройство может проверять аутентификацию и принадлежность к группам и подгруппам в СФУ. При использовании устройств, присоединенных к корпоративной сети СФУ, система дает возможность облегчить работу и упорядочить использование оборудования и других ресурсов [1].

Основные применения включают подтверждение личности (аутентификация), управление группами (включая создание, удаление и сохранение списков членства), удостоверение принадлежности к группе (доказательство членства в группе, возможно, анонимное) и, возможно, передачу принадлежности к группе другим лицам в течение некоторого периода времени. Во многих случаях должна сохраняться индивидуальная конфиденциальность. Доказательство принадлежности к группе должно выполняться без того, чтобы показывать конкретную идентичность пользователя. Система может делать запись в журнале всех элементов или отдельных избранных элементов (например, неудачных попыток). Следует учитывать возможность изменений требований персоналом, управляющим системой безопасности СФУ, относительно информации, которая может потребоваться ему в дальнейшем.

Будут использованы следующие базовые средства:

– симметричное шифрование / дешифрование;

– симметричный код аутентификации сообщения (КАС) и проверка;

– шифрование с открытыми ключами/ дешифрование;

– цифровые подписи и проверка;

– подпись или имитовставка, чтобы доказать владение ключом;

– генерирование ключа для симметричных алгоритмов или алгоритмов с открытыми ключами;

– криптографические хэши.

Для начала может оказаться достаточным рассмотрение подмножества этих средств.

Для обеспечения надежности базы данных разработаны на основе мажорирования и семантики протокола AFS [2]. Новым элементом является отсутствие *аннулирующих сообщений* со стороны сервера в случае открытия клиентской программой базы данных в режиме чтения. Это позволяет уменьшить нагрузку на сервер и на сеть, позволяя одному серверу обслуживать большее число клиентов.

К концу первого года в СФУ будут закончены:

– проект аппаратной платформы для СК: сервисных, интерфейсных и аутентификационных модулей; полный проект системы, включая серверы, интерфейсные устройства и сети; опытный образец аппаратной платформы для СК, используя имеющиеся в наличии компоненты и традиционные процедуры конструирования везде, где возможно минимизировать риск разработки.

К концу второго года будут закончены:

– стабильная аппаратная платформа для СК, используя специально разработанные компоненты и процессы, предназначенные для достижения требуемых показателей защищенности, стоимости и надежности; опытная версия программного обеспечения для СК, сервисных модулей, интерфейсных и аутентификационных модулей и серверов; опытный образец системы, включая все элементы в малом масштабе.

Математическая модель доступов строится с использованием многозначной логики. Новым является подход, рассматривающий модификацию объектов, как конфиденциальность, а запрет изменений, напротив, как указание на более низкий уровень классификации [3, 4]. Это позволяет совместно учесть требования конфиденциальности и эффективного доступа.

Литература

1. Вергейчик А.В. Моделирование систем физической защиты / А.В. Вергейчик, В.П. Кушнир // Докл. ТУСУР. – Томск, 2008. № 2(18), ч. 1. – С. 22–27.

2. KAFS: AFS filesystem // http://lxr.linux.no/linux-bk+v2.6.10/Documentation /filesystems/

3. Муллер А.А. Проблема доступности в модели информационной безопасности / А.А. Муллер, М.М. Кучеров //Современные проблемы информатизации в анализе и синтезе технологических и программно-телекоммуникационных систем: сб. трудов / под ред. д.т.н. О.Я. Кравца. – Воронеж: Научная книга, 2008. – Вып. 13– С. 375–385.

4. Ларченко М.В. Универсальная идентификация – важное средство борьбы с киберпреступностью / М.В. Ларченко, М.М. Кучеров // Докл. ТУСУР. – Томск, 2008. № 2(18), ч. 1. – С. 89–94.

Богульская Нина Александровна
ГОУ ВПО «Сибирский федеральный университет»,
Институт космических и информационных технологий (ИКИТ),
доцент каф. прикладной математики и компьютерной безопасности,
научно-учебная лаборатория информационной безопасности (НУЛ ИБ)
Эл. адрес: NBogulskaya@sfu-kras.ru

Кучеров Михаил Михайлович
ГОУ ВПО «Сибирский федеральный университет»,
Институт космических и информационных технологий (ИКИТ),
профессор каф. прикладной математики и компьютерной безопасности НУЛ ИБ,
к.ф.-м.н., доцент
Эл. адрес: MKucherov@sfu-kras.ru

Кушнир Виктор Петрович
ООО «МОПНИЭИ–КрасКрипт», Красноярск,
профессор каф. прикладной математики и компьютерной безопасности НУЛ ИБ ИКИТ СФУ,
к.т.н., доцент

N.A. Bogulskaya,M.M. Kucherov,V.P. Kushnir

Development of algorithms of the protected applications for social cards

Development and application of the device of authentication on the basis of a plastic card is considered. This device can be applied not only in the systems of monitoring and access control (SMAC), but also for check of an accessory to groups and subgroups among the students, faculty, and stuff of the Siberian Federal University.

Keywords: social card, autentification, key, information security.
