Повышение безопасности доступа к ключам электронной подписи в условиях слабодоверенного окружения

С.С. Агафьин, С.В. Смышляев

***Аннотация*— Одной из проблем, непременно присутствующих при обсуждении вопросов массовой (или «гражданской») криптографии на конференциях и симпозиумах, является задача обеспечения возможности использования криптосредств (в первую очередь, средств электронной подписи) с применением массовых мобильных устройств. Слабое доверие к среде функционирования средств защиты информации в таких устройствах не позволяет тривиальным образом обеспечить безопасность функционирования таких средств, однако ряд дополнительных компенсирующих технических мер, реализованных разработчиками, позволили в последние годы существенно продвинуться в решении данной задачи, обеспечить достаточный уровень защиты и реализовать сертифицированные по требованиям государственных органов средства. При этом сохраняет актуальность вопрос об обеспечении повышенной защиты долговременных ключей с возможностью удобного и безопасного их использования с мобильных устройств. В настоящей работе производится обзор существующих подходов к хранению и использованию долговременных ключей с возможностью доступа к ним с мобильных устройств, а также, с применением разработанного к текущему моменту научного фундамента, предлагается способ решения данной задачи, основанный на современных доказуемо стойких криптографических протоколах.**

***Ключевые слова*—электронная подпись, прикладные аспекты криптографии, аутентификация.**

I. Введение

Применение в повседневной жизни мобильных устройств для доступа к электронным услугам стало распространено в той мере, что делает невозможным игнорирование или запрет применения на таких устройствах средств криптографической защиты, в том числе средств электронной подписи. Пониженный уровень доверия к среде функционирования средств защиты информации требует внедрения в такие средства специальных инженерных решений, позволяющих компенсировать проблемы слабодоверенного окружения в достаточной для сертификации по действующим требованиям степени. В частности, как обсуждалось на заседаниях и круглых столах основных российских открытых конференций по прикладной криптографии см., например, [1], с помощью мобильных приложений возможно защищенное сертифицированными средствами (с применением российских средств шифрования и криптонаборов, см. [2, 3]) взаимодействие с серверными компонентами. При этом задача о работе с долговременными ключами электронной подписи пользователей по-прежнему, несмотря на существующие сертифицированные решения, активно обсуждается специалистами по безопасности (см., например, [4]) в контексте выбора подходов к повышению защиты хранимых ключей.

Как обсуждалось в работе [5], при переносе привычных программных средств работы с электронной подписью в условия мобильного использования возможны различные подходы к порядку работы с ключами. Они выбираются с учетом ограничений мобильных устройств, при этом архитектура программных средств модифицируется для обеспечения безопасной и эффективной работы на таких устройствах. В зависимости от подхода само мобильное приложение на устройстве является либо самодостаточным средством электронной подписи, либо частью клиент-серверного решения, в котором, в свою очередь, хранение ключей может осуществляться либо на самом мобильном устройстве, либо централизованным образом в HSM («облачная» подпись). В настоящее время стремительно развивается подход, предполагающий дистанционный доступ к ключам электронной подписи: мобильное устройство пользователя используется при этом для построения аутентифицированного защищенного канала с серверными компонентами и подтверждении волеизъявлений. Этот подход, его преимущества и недостатки подробно рассматривались в работе [5], как и некоторые из аспектов подхода, предполагающего локальное хранение ключей (в частности, необходимость доверенного источника случайности). Целесообразно рассмотреть также возможность применения наиболее привычного пользователям стационарных компьютеров способа работы с электронной подписью – применения отчуждаемых ключевых носителей (токенов) совместно с мобильными устройствами. С учетом технических ограничений, накладываемых производителями мобильных устройств, контактное использование

С.С. Агафьин – ООО «КРИПТО-ПРО», начальник отдела разработки ФКН (e-mail: sagafyin@cryptopro.ru)

С.В. Смышляев – ООО «КРИПТО-ПРО», заместитель генерального директора (e-mail: svs@cryptopro.ru).

ключевых носителей с мобильных телефонов существенно затруднено: подключить внешний носитель через кабель к телефону зачастую невозможно. Остается радиоканал: Bluetooth, NFC, Wi-Fi – конкретная технология с точки зрения общих вопросов защиты информации и криптографии нам не важна. В настоящей работе рассмотрим вопрос о том, как обеспечить удобное и безопасное применение ключевых носителей посредством радиоканала. Но сперва рассмотрим способы хранения ключей в целом, выделяя их преимущества и недостатки.

II. Виды ключевых носителей

По фактическому месту хранения ключа все ключевые носители можно разделить на несколько больших классов: локальные, отчуждаемые и удаленные («облачные»).

Локальные ключевые носители являются частью конкретной пользовательской системы и штатным образом не могут быть перенесены на другую систему. К ним можно отнести классические простые хранилища вроде директорий и разделов файловой системы или Реестр ОС Windows.

Основным преимуществом локальных ключевых носителей можно считать удобство организации системы защиты доступа к ключам: разработчик средства криптографической защиты может положиться на хорошо изученные встроенные системы разграничения доступа операционной системы.

Важнейшим недостатком локальных ключевых носителей является отсутствие возможности контроля за действиями пользователя: хранение ключей средствами операционной системы подразумевает, что пользователь с использованием этих же средств может получить доступ к ключам и выполнять с ними операции, которые при недостаточной квалификации могут показаться штатными, но фактически понижающие уровень безопасности. Другим недостатком является сложность организации системы физического контроля: в ряде случаев необходимы системы круглосуточного видеонаблюдения или защищенные физические хранилища.

Логичным развитием локальных ключевых носителей стали отчуждаемые ключевые носители. К их достоинствам можно отнести возможность использования ключа в любой системе, поддерживающей подключение носителя. Это существенно повышает мобильность пользователя и удобство использования криптографических систем, но в то же время делает обеспечение безопасности данных ключей более сложной задачей, так как существенно повышается риск кражи или утери носителя.

Наиболее простыми и широко используемыми отчуждаемыми ключевыми носителями являются простые USB-flash-накопители. Ключи на них хранятся в виде набора файлов, зашифрованных на ключе, выведенном из известного пользователю пароля. Несмотря на то, что они являются наиболее дешевыми и удобными устройствами, эти носители обладают существенными недостатками безопасности. Прежде всего, кража подобного носителя фактически сразу приводит к компрометации ключа: скопировав файлы ключа, нарушитель может провести распределенный неограниченный перебор пароля.

Решением данной проблемы является ограничение операций, которые можно совершать с устройством, и добавление аппаратной защиты от перебора пароля. Защита чаще всего представляет собой ограничение на число попыток предъявления пароля, что существенно затрудняет возможность перебора.

Наиболее распространенными носителями, обладающими данными свойствами, являются смарт-карты и USB-токены. В наиболее простом исполнении они предназначены только для хранения файлов с ключевой информацией. Будем называть подобные носители пассивными смарт-картами. Криптографические системы, использующие подобные носители, должны предъявить в него пароль, считать файлы с ключевой информацией и выполнять с их помощью криптографические преобразования в собственных вычислительных компонентах.

Несмотря на удобство и повышенную безопасность по сравнению с простыми USB-накопителями, пассивные смарт-карты обладают и недостатками. Прежде всего, их применение невозможно в системах, которые предусматривают возможность появления нарушителя в канале между устройством и прикладным средством криптографической защиты. Для компрометации ключа подобному нарушителю достаточно обладать возможностью прослушивания канала. Подобный нарушитель должен учитываться во многих прикладных случаях: использование радиоканала при подключении носителя (Bluetooth, NFC, Wi-Fi), подключение через недоверенные переходники, использование удаленного подключения.

Следующими по уровню защищенности являются активные смарт-карты – это носители, которые обладают всеми свойствами пассивных, но при выполнении криптографической операции (прежде всего, электронной подписи) не передают ключевую информацию, а сами реализуют криптографические алгоритмы. И хотя подобный подход может приводить к существенному замедлению, связанному с тем, что чипы, используемые в смарт-картах менее производительные, чем процессоры общего назначения, его использование позволяет обеспечить защиту от пассивного нарушителя.

Тем не менее, у подобных носителей есть другой важный недостаток. Так как они не реализуют никакие механизмы защиты канала, то они оказываются уязвимы при наличии нарушителя, который умеет не только прослушивать канал между носителем и средством защиты информации, но и модифицировать данные. Нарушитель может записать команды аутентификации и подписи, а затем послать их заново, изменив подписываемое хэш-значение, что, по сути, приводит к полной компрометации ключевой информации.

С практической точки зрения обоснование использования в конкретной прикладной системе

модели нарушителя, в рамках которой он умеет анализировать данные в канале между носителем и средство криптографической защиты, но не может выполнить простое воспроизведение запомненных команд, кажется крайне сложной задачей. В связи с этим резонно считать, что набор сценариев, в которых использование активных смарт-карт представляет угрозу безопасности ключей, совпадает с указанными для пассивных носителей.

Очевидно, что наиболее простым подходом для предотвращения реализации описанных угроз является использование защиты канала криптографическими методами. Активные ключевые носители, реализующие протоколы защиты канала, будем называть функциональными ключевыми носителями (ФКН).

Существует большое число различных протоколов защиты канала, спроектированных специально для взаимодействия с носителями ключевой информации, но наибольший интерес представляет протокол SESPAKE, который описан в Рекомендациях по стандартизации Р 50.1.115–2016 [6], а также в RFC 8133 [7].

Данный двухэтапный протокол позволяет провести взаимную аутентификацию средства криптографической защиты и ключевого носителя с выработкой общего сессионного ключа. Выработанный ключ можно использовать для построения любого известного протокола обмена защищенными сообщениями. Протокол SESPAKE спроектирован, чтобы противостоять наиболее известным теоретическим и практическим атакам на протоколы аутентификации [8], что делает его наиболее подходящим для использования в системах криптографической защиты.

Так как при использовании SESPAKE в канале связи между ключевым носителем и прикладной системой не оказывается ни ключевой информации, ни иной чувствительной информации, а при аутентификации в канале происходит обмен одноразовыми случайными величинами, воспроизведение или модификация активным нарушителем данных сообщений не влияет на безопасность [9]. Это позволяет снять ограничения на используемые способы подключения ключевых носителей и разрешить использование как радиоканалов, так и удаленного подключения носителей, например, через протокол удаленных рабочих столов RDP.

В завершении обзора видов ключевых носителей опишем подход, который обладает преимуществами всех остальных: удаленное хранилище ключей. К подобным носителям относятся как серверы электронной подписи (Hardware Secure Module – HSM), так и сервисы облачной подписи (Digital Signature Service – DSS). При использовании подобных систем фактически пользовательские ключи хранятся на удаленном доверенном устройстве высокого уровня безопасности, а доступ к ключам осуществляется с помощью строгой многофакторной аутентификации.

Удаленные хранилища при корректной эксплуатации обеспечивают не только безопасность, но и удобство использования: для доступа пользователь может использовать любой терминал, но при этом не учитывать риск утери или кражи ключевого носителя, который по очевидным причинам всегда должен приниматься во внимание для отчуждаемых ключевых носителей.

Тем не менее, несмотря на описанные достоинства, у данного подхода можно выделить и недостатки. Прежде всего, в ряде случаев использование удаленных ключевых хранилищ может быть невозможно по экономическим или организационным причинам: небольшое число пользователей при высокой стоимости сервера подписи; высокая сложность корректной настройки данных систем.

Другая проблема заключается в том, что существуют пользователи, которые не доверяют решение задачи хранения криптографических ключей никаким внешним сторонам и предпочитают нести за них персональную ответственность (см. [5]). Для её решения можно использовать комбинированные подходы, которые позволяют совместить удобство и безопасность удаленных хранилищ с фактическим хранением ключа у пользователя.

III. Взаимодействие с системами электронного документооборота: комбинированное решение

С практической точки зрения важен вопрос о том, как обеспечить удобство применения таких мобильных приложений для реальных систем, в которых, как правило, сам документ формируется на серверной стороне (например, в системе электронного документооборота), а не на стороне мобильного устройства. В схемах применения дистанционной («облачной») подписи этот вопрос решается автоматически (см. [5]): сам сервер электронной подписи начинает свой протокол взаимодействия именно с получения документа от внешней информационной системы, а обращения к мобильному устройству идут уже лишь для подтверждения операции.

Рассмотрим вопрос о том, как совместить предусматривающий формирование подписываемого документа во внешней системе порядок работы с применением защищенных отчуждаемых ключевых носителей посредством мобильного устройства, сохранив связанные с безопасностью преимущества схемы дистанционной подписи.

Наиболее простым вариантом решения, не требующим модификации системы дистанционной подписи в целом, является хранение ключей аутентификации на отчуждаемых носителях. При таком подходе сохраняются все преимущества схемы, описанной в работе [5], при этом обеспечивается повышенная защита ключа аутентификации.

Но что если по тем или иным причинам владельцу ключа электронной подписи требуется хранить и применять его на персональном ключевом носителе в неизвлекаемом виде – не имея возможности его восстановить в случае утери или повреждения носителя, но зато самолично обеспечивая полный контроль за этим ключом? Рассмотрим альтернативную схему, предполагающую хранение самих ключей электронной

подписи в неизвлекаемом виде на отчуждаемых носителях. Разработку такого комбинированного подхода, объединяющего схемы дистанционной подписи и хранения ключа в неизвлекаемом виде на персональном ключевом носителе, с учетом сказанного выше и в работе [5], целесообразно производить с целью обеспечить следующие свойства:

1) Возможность поддержки удобных и безопасных сценарии для использования токенов, работающих по NFC или Bluetooth, с мобильным устройством.

2) Удобство применения мобильного устройства не для формирования подписываемых документов, а именно для подтверждения операции с документом, сформированным извне.

3) Поддержка существующих процессов работы с ЭП, то есть, тех систем документооборота и прикладного программного обеспечения, в которых более двух десятков лет применяются интегрированные программные криптопровайдеры (CSP), функционирующие на тех же самых устройствах.

4) Возможность опционально добавлять второй фактор аутентификации.

Оказывается возможным выполнить все эти условия, если взять за основу описанную в [5] схему и общий порядок взаимодействия компонент, заменив при этом финальное действие, саму команду на формирование подписи. В исходной схеме она производится посредством самого HSM, а для целей использования носителей с неизвлекаемым ключом требуется заменить ее на обращение к ключевому носителю. Основной проблемой оказывается как раз рассмотренная выше в настоящей работе задача о защите канала связи между ключевым носителем и вызывающими компонентами (в рассматриваемой схеме – серверными компонентами системы дистанционной подписи, HSM и сервером подписи). Но рассмотрение именно этой задачи приведено выше в полном объеме, ведь ограничений по порядку размещения компонент мы не вводили, а значит, метод использования протокола SESPAKE и построения защищенного канала на его основе применим без дополнительных модификаций: в момент обращения к HSM для формирования подписи сам HSM (в паре с сервером подписи) может установить защищенное соединение с ключевым носителем, используя канал связи с мобильным устройством для передачи данных, а мобильное устройство – в роли бесконтактного считывателя для ключевого носителя. Обратим внимание, что защищенный посредством SESPAKE канал теперь строится не между мобильным устройством и ключевым носителем, а напрямую между ключевым носителем и сервером подписи (и HSM), обеспечивая защиту в рамках транзакции подписи даже от уязвимостей на стороне мобильного устройства (которое в рамках этой операции играет не более значимую роль, чем, скажем, сетевой маршрутизатор, через который проходит шифрованный трафик).

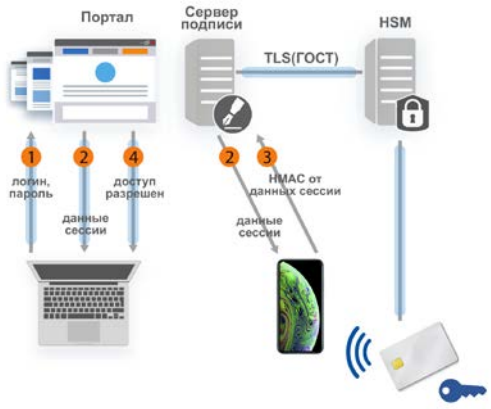

Рис.1. Схема использования персонального ключевого носителя с сервером облачной подписи посредством мобильного устройства

Такая схема позволяет в полном объеме переиспользовать всё уже созданное в системе дистанционной подписи для безопасной работы с документами: схемы интеграции, доверенную визуализацию, возможность управления ключами аутентификации (владение которыми теперь может являться дополнительными факторами аутентификации), подробный доверенный аудит с использованием HSM. Кроме того, за счет технологии «облачных» ключевых носителей (трансляция операций вместо локального криптопровайдера в средство дистанционной подписи) бесшовно поддерживается всё программное обеспечение, уже работающее с локальными криптопровайдерами, без необходимости переработок или доработок на стороне стационарных компьютеров или систем документооборота.

И при этом появляются все преимущества безопасного использования ключей на токенах: ключи подписи никогда не покидают отчуждаемый носитель, всегда находясь под контролем пользователя, причем не требуется как-либо модифицировать ключевые носители (на их стороне, как и прежде, необходимо лишь выполнять протокол SESPAKE и защищенное соединение на его основе). Таким образом, основные преимущества системы дистанционной подписи успешно реализуются в схеме, в которой подпись формируется локально.

IV. Заключение

Несмотря на ограничения, накладываемые мобильными устройствами, посредством применения современных протоколов установления защищенного соединения возможно построить схемы взаимодействия с ключевыми носителями с помощью мобильных устройств. Что еще более важно, благодаря таким протоколам удается разработать схему взаимодействия, обладающую преимуществами (как в части безопасности, так и в части удобства) двух идеологий применения долговременных ключей: локального и дистанционного. Разработанный подход может быть

применен при существенном переиспользовании существующих решений, без их доработки.

Библиография

[1] С.В. Смышляев, “Настоящее и будущее криптопротоколов в сети Интернет”, доклад на научно-практической конференции РусКрипто’2020, 2020 г., https://www.ruscrypto.ru/resource/archive/rc2020/files/01_smyshlyaev.pdf

[2] Рекомендации по стандартизации Р 1323565.1.020-2020 “Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)”, Москва, Стандартинформ, 2020, https://tc26.ru/standarts/rekomendatsii-po-standartizatsii/r-1323565-1-020-2020-informatsionnaya-tekhnologiya-kriptograficheskaya-zashchita-informatsii-ispolzovanie-kriptograficheskikh-algoritmov-v-protokole-bezopasnosti-transportnogo-urovnya-tls-1-2-.html

[3] L.R. Akhmetzyanova, E.K. Alekseev, G.K. Sedov, S.V. Smyshlyaev “On Security of TLS 1.2 Record Layer with Russian Ciphersuites”, труды 8-го симпозиума “Современные тенденции в криптографии (CTCrypt 2019), с. 253-292.

[4] А.Г. Сабанов, “Анализ международных стандартов по идентификации и аутентификации“, доклад на X Уральском форуме “Информационная безопасность финансовой сферы“, 2018.

[5] П.В. Смирнов, С.В. Смышляев, “ Обеспечение безопасности систем дистанционного формирования электронной подписи в условиях слабодоверенного окружения”, International Journal of Open Information Technologies, том 8, № 12, 2020, с. 77-84, http://injoit.org/index.php/j1/article/view/1011

[6] Рекомендации по стандартизации Р 50.1.115–2016 “Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля”, Москва, Стандартинформ, 2016, https://tc26.ru/standarts/rekomendatsii-po-standartizatsii/r-50-1-115-2016-informatsionnaya-tekhnologiya-kriptograficheskaya-zashchita-informatsii-protokol-vyrabotki-obshchego-klyucha-s-autentifikatsiey-na-osnove-parolya.html

[7] Smyshlyaev, S., Ed., Alekseev, E., Oshkin, I., Popov, "The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol ", RFC 8133, March 2017, https://www.rfc-editor.org/rfc/rfc8133.html

[8] Алексеев Е.К., Ахметзянова Л.Р., Ошкин И.Б., Смышляев С.В. “Обзор уязвимостей некоторых протоколов выработки общего ключа с аутентификацией на основе пароля и принципы построения протокола SESPAKE”, Математические вопросы криптографии, том 7, №4, 2016, с.7–28, http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=mvk&paperid=201

[9] Алексеев Е.К., Смышляев С.В. “О безопасности протокола SESPAKE”, Прикладная дискретная математика, том 50, 2020, с.5–41, http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=pdm&paperid=719

Providing security to usage of long-term keys in case of semi-trusted secure environment

Sergey Agafyin, Stanislav Smyshlyaev

***Abstract*— The task of enabling usage of cryptographic software (especially, for working with digital signature) with general-purpose mobile devices (e.g., smartphones with iOS or Android operation systems) is inevitably discussed during all conference discussions dedicated to mass-market cryptography. Users are used to performing their everyday operations with smartphones. Lower level of trust to such devices as environment for cryptographic software must always be kept in mind while developing systems involving them in processes; nevertheless, integrated additional security measures have made possible significant increase of security on such devices and, therefore, certification and usage of cryptographic software for mobile devices. At the same time, the question of providing secure and convenient ways of using long-term keys in hardware tokens with mobile devices still requires further research. In the current paper, we do a review of existing ways of using cryptographic tokens with long-term keys via mobile devices and develop approaches for solving this task in real-world scenarios based on recently developed protocols for password-based authenticated key establishment with proven security.**

***Keywords*—digital signature, applications of cryptography, authentication**

REFERENCES

[1] S.V. Smyshlyaev, “Present and Future of Cryptographic Protocols in Internet”, talk at the RusCrypto’2020 Conference, 2020 (in Russian), https://www.ruscrypto.ru/resource/archive/rc2020/files/01_smyshlyaev.pdf

[2] “Information technology. Cryptographic data security. The use of the Russian cryptographic algorithms in the Transport Layer Security protocol (TLS 1.2”». Recommendations on standardization R 1323565.1.020-2020, Federal Agency for Technical Regulation and Metrology (ROSSTANDART), 2020 (in Russian), https://tc26.ru/standarts/rekomendatsii-po-standartizatsii/r-1323565-1-020-2020-informatsionnaya-tekhnologiya-kriptograficheskaya-zashchita-informatsii-ispolzovanie-kriptograficheskikh-algoritmov-v-protokole-bezopasnosti-transportnogo-urovnya-tls-1-2-.html

[3] L.R. Akhmetzyanova, E.K. Alekseev, G.K. Sedov, S.V. Smyshlyaev “On Security of TLS 1.2 Record Layer with Russian Ciphersuites”, proceedings of 8-th Workshop on Current Trends in Cryptology (CTCrypt 2019), pp. 253-292.

[4] A.G. Sabanov, “Analysis of International Standards on Identification and Authentication“, talk at the X Ural Forum “Information security of financial sphere“, 2018 (in Russian).

[5] P.V. Smirnov, S. V. Smyshlyaev, “Providing security to remote digital signature systems in case of semi-trusted secure environment”, in International Journal of Open Information Technologies, vol. 8, № 12, 2020, pp. 77-84 (in Russian), http://injoit.org/index.php/j1/article/view/1011

[6] “Information technology. Cryptographic data security. Password Authenticated Key Establishment Protocol”. Recommendations on standardization R 50.1.115-2016, Federal Agency for Technical Regulation and Metrology (ROSSTANDART), 2016 (in Russian), https://tc26.ru/standarts/rekomendatsii-po-standartizatsii/r-50-1-115-2016-informatsionnaya-tekhnologiya-kriptograficheskaya-zashchita-informatsii-protokol-vyrabotki-obshchego-klyucha-s-autentifikatsiey-na-osnove-parolya.html

[7] Smyshlyaev, S., Ed., Alekseev, E., Oshkin, I., Popov, "The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol ", RFC 8133, March 2017, https://www.rfc-editor.org/rfc/rfc8133.html

[8] E.K. Alekseev, L.R. Akhmetzyanova, I.B. Oshkin, S.V. Smyshlyaev, “A review of the password authenticated key exchange protocols vulnerabilities and principles of the SESPAKE protocol construction”, Matem. Vopr. Kriptogr., vol. 7, № 4, 2016, pp. 7-28, http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=mvk&paperid=201

[9] E.K. Alekseev, S.V. Smyshlyaev, “On security of the SESPAKE protocol”, Prikl. Diskr. Mat., vol. 50, 2020, pp. 5-41, http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=pdm&paperid=719