УДК 681.3::002.651.028(083.73)

А. О. Мелащенко, аспирант,
О. Л. Перевозчикова, д-р физ.-мат. наук, профессор, чл.-кор. НАНУ
Институт кибернетики им. В. М. Глушкова НАН Украины, г. Киев

РОЛЬ КОМПЛЕКТОВ ПОДПИСЕЙ В КВАЛИФИЦИРОВАННОЙ ИНФРАСТРУКТУРЕ ОТРЫТЫХ КЛЮЧЕЙ

На примере реализации комплекта подписей ГОСТ 34.311+ДСТУ 4145 показаны возможные решения существующих проблем интероперабельности, даны конкретные предложения по профилированию параметров ГОСТ 34.311+ДСТУ 4145, а также по интеграции его в современные операционные среды.

Ключевые слова: *електронний цифровий підпис (ЕЦП), криптомодулі, криптоалгоритми*

Введение. Роль электронной цифровой подписи (ЭЦП) сложно переоценить в информационном обществе XXI века, когда любая транзакция любого электронного бизнеса (E-Commerce, E-Health, E-Government и т.п.) использует ЭЦП как «якорь» доверия. Проблемы интероперабельности Национальной системы электронных цифровых подписей (НСЭЦП) не допускают использовать ЭЦП во взаимодействии субъектов хозяйственной деятельности, граждан Украины и государства. Помимо проблем, описанных в [1—3], необходим международный уровень качества услуг НСЭЦП.

Аббревиатуры

НСЭЦП		Национальная система электронных цифровых подписей
ЭЦП		Электронная цифровая подпись
ЦСК		Центр сертификации ключей
ВТО		Всемирная торговая организация
ОС		Операционная система
ПКТ		Программно-технический комплекс
QPKI	Qualified public key infrastructure	Квалифицированная инфраструктура открытых ключей
PKI	Public key infrastructure	Инфраструктура открытых ключей
SSCD	Secure signature creation device	Безопасное средство создания подписей
CRL	Certificate revocation list	Список аннулированных сертификатов
OCSP	Online certificate status protocol	Онлайн-протокол статуса сертификатов
TSP	Time stamp protocol	Протокол штемпелевания времени

При решении задач неинтроперабельности и невозможности кроссертификации программно-технических комплексах (ПТК)

НСЭЦП, посредством идентификации ключевых пробелов нормативного регулирования и технологической реализации комплектов подписей, необходимо понимать важность решений включать или не включать тот или иной комплект подписи в НСЕЦП. Эти решения имеют долгосрочный характер, требуя вечного поддержания работоспособности комплектов подписей для гарантии сохранности электронных архивов в Украине.

Далее сформулированы конкретные рекомендации по интеграции комплекта подписей ГОСТ 34.311+ДСТУ 4145 в современные операционные среды и гарантировать высокий уровней интероперабельности его реализаций.

1. Общая модель подписания

На рис. 1 отображена схема наложения ЭЦП, когда подписант для получения электронного документа должен одновременно предоставить в комплекте подписи три обязательных объекта и при необходимости четвертый, полученный от ЦСК. Чтобы прочитать содержимое электронного документа адресат, используя тот же комплект подписи, что и подписант, должен последовательно получить открытый ключ и при наличии временного штемпеля иметь возможность обратиться в ЦСК подписанта за справками по удостоверению этих объектов. Причем обращение именно в ЦСК подписанта состоится по адресу, встроенному в ЭЦП документа, на основе сертификата открытого ключа подписанта, поскольку на этот сертификат ЦСК наложил свою ЭЦП.

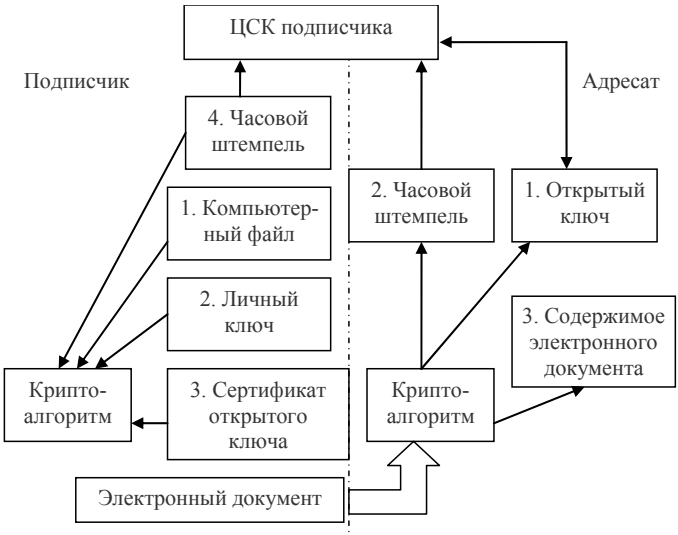

Рис. 1. *Схема наложения и валидации ЭЦП документа*

В QPKI Евросоюза согласно Директиве 1999/93/EC [4] применимы только SSCD. Согласно Решению Еврокомиссии [5] допустимы только аппаратные устройства, гарантирующие физическую защиту личных ключей. Отметим, что эта норма некорректно отражена в Законе Украины «Про електронний цифровий підпис» [6], поскольку он допускает использование программных и программно-аппаратных реализаций SSCD. Ввиду этого разногласия возникла проблема защиты секретного ключа в гетерогенной сетевой среде (с разными ОС), что гораздо труднее, чем для аппаратных средств с их встроенными ОС.

Согласно схеме на рис. 1 для подписания данных необходимы:

1) личный ключ;
2) сертификат открытого ключа;
3) комплект подписи.

В Украине действуют стандарты на все составляющие рекомендованных ETSI комплектов подписей (табл. 1), составляющие часть комплекта подписей. Ввиду взаимодействия, способного повлиять на защиту IT-систем, алгоритмы и параметры для безопасных ЭЦП необходимо использовать только в предопределенных комбинациях, именуемых комплектами подписей. Комплект подписи состоит из трех компонентов: хеш-функция, метод дополнения, алгоритм подписания с разветвленным набором параметров.

Опустим формат подписи как оконечную структуру, связывающую все составляющие, поскольку формат вообще не регламентирован нормативной базой НСЭЦП. Разумеется, рекомендуется использовать национальные стандарты ДСТУ ETSI TS 101 903:2009 и ДСТУ ETSI TS 101 733:2009 для формата подписи. Отметим, что формат личного ключа также не регламентирован нормативной базой НСЭЦП, но рассмотрим его как основной фактор отсутствия интероперабельности и потенциальное препятствие в кроссертификации Украины со странами ВТО.

В операционных средах Windows и Linux (рис. 2) сходна реализация инфраструктуры открытых ключей (PKI) как основы QPKI. Везде комплекты подписей являются основным, трастовым «якорем» в обмене данными для поддержки процедур PKI. В Windows идеологию комплектов подписей реализуют «криптопровайдеры», в Linux — набор библиотек OpenSSL (http://openssl.org/). Такая архитектура допускает произвольно выбирать/дополнять комплекты подписей, не вмешиваясь в реализацию конкретных структур данных.

Таблица 1

Рекомендованные ETSI комплекты подписей

Имя комплекта подписи	Имя хеш-функции	Имя метода дополнения	Имя алгоритма подписания
sha1-with-rsa	sha1	Выбирается из [12]	rsa
sha1-with-dsa	sha1	не требует дополнения	dsa
ripemd160-with-rsa	ripemd160	Выбирается из [12]	rsa
ripemd160-with-dsa	ripemd160	не требует дополнения	dsa
sha224-with-rsa	sha224	Выбирается из [12]	rsa
sha256-with-rsa	sha256	Выбирается из [12]	rsa
rsa-pss с mgf1SHA-1Identifier	mgf1SHA-1		rsa
rsa-pss с mgf1SHA-224Identifier	mgf1SHA-224		rsa
rsa-pss с mgf1SHA-256Identifier	mgf1SHA-256		rsa
sha1-with-ecdsa	sha1	не требует дополнения	ecdsa-Fp или ecdsa-F2m
sha1-with-ecgdsa	sha1	не требует дополнения	ecgdsa-Fp или ecgdsa-F2m
sha224-with-ecdsa	sha224	не требует дополнения	ecdsa-Fp или ecdsa-F2m
sha256-with-ecdsa	sha256	не требует дополнения	ecdsa-Fp или ecdsa-F2m
sha384-with-ecdsa	sha384	не требует дополнения	ecdsa-Fp или ecdsa-F2m
sha512-with-ecdsa	sha512	не требует дополнения	ecdsa-Fp или ecdsa-F2m
ecdsa-with-RIPEMD160	ripemd160	не требует дополнения	ecdsa-Fp или ecdsa-F2m

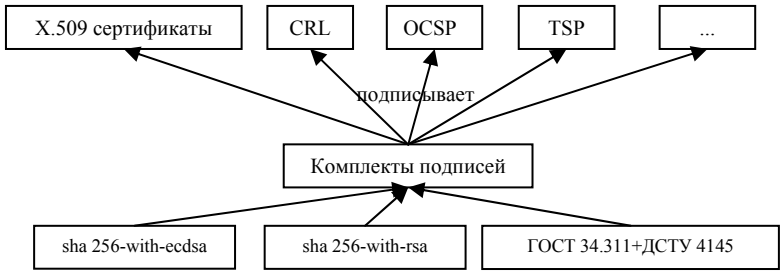

Рис. 2. *Комплекты подписей как основа QPKI*

Корректное использование архитектур реализации PKI в популярных ОС позволило, даже при наличии пока единственного ком-

плекта подписи (ГОСТ 34.311+ДСТУ 4145), предоставить качественные услуги ЭЦП в Украине. Так, при интеграции в Windows «криптопровайдера», реализующего «ГОСТ 34.311+ДСТУ 4145», пользователи получили базовый Центр сертификации ключей и клиентское программное обеспечение, т.е. реализацию форматов личных ключей, форматов подписей, CRL, OCSP и т.п. Аналогичный набор инструментов можно получить при интеграции «ГОСТ 34.311+ДСТУ 4145» в набор библиотек OpenSSL[7].

Отметим необходимость национально-украинской локализации функциональности ЦСК в среде MS Windows Server 2008 для поддержки QPKI. Национально-украинская локализация программного обеспечения — это перевод пользовательского интерфейса, документации и сопутствующих программных продуктов на украинский язык, а также их адаптация к культурным традициям Украины.

Ввиду законодательства США процедуры Microsoft по национально-культурной локализации комплектов подписей достаточно жестки. Без содействия Microsoft невозможно встроить «ГОСТ 34.311+ДСТУ 4145» в MS Windows Server для ЦСК, а стратегия Microsoft нацелена на воплощение только международных стандартов. Европейские стандарты, составляющие эталонную модель QPKI, отображены на международные де-факто стандарты RFC и признаны за рамками ЕС, например, Японией. Также инфраструктура QPKI более совершенна в юридическом отношении и позволяет избежать множества проблем, порожденных американской моделью PKI. Чтобы локализовать реализацию MS Windows Server для потребностей ЦСК, т.е. поддержки эталонной модели QPKI, необходимо доработать Windows. Лишь его разработчики способны это сделать, поскольку модуль политики безопасности — это не только ноу-хау фирмы, но и конфиденциальная часть самой ОС с позиций национальной безопасности США.

Однако, упреждая отток клиентов, вынужденных эксплуатировать другие ОС, рассчитывая на рынок услуг ЕЦП в Евросоюзе и, как следствие, в Украине, разработчики семейства ОС Windows обязаны немало сделать для своих клиентов на дальнюю и ближнюю перспективу.

1. Поддержать формат сертификата открытого ключа согласно ДСТУ ETSI TS 101 862:2009.
2. Поддержать формат подписи XAdES, что **не противоречит** стандартам OpenXML, а лишь реализации в среде MS Windows расширений XMLDigSig согласно ДСТУ ETSI TS 101 903:2009 и его профиля ДСТУ ETSI TS 102 904:2009. Целесообразно также реализовать формат подписи CAdES согласно ДСТУ ETSI TS 101 733:2009 и ее профиля ДСТУ ETSI TS 102 734:2009 в среде

разработчика для воплощения юридических требований унифицированными QPKI-средствами MS Windows.

3. Изучив степень поддержки семейством ОС Windows диапазона SSCD, интегрировать драйверы наиболее применимых таких устройств с позиций эталонной модели QPKI (ДСТУ ETSI TR 101 045:2009), поддерживающей Директиву, ДСТУ EN 14890 и CWA 14169.
4. Оценить реализацию в средствах семейства ОС требований безопасности для приложений создания подписей в соответствии с нормами ДСТУ CWA 14170 и общими рекомендациями верификации ЭЦП согласно ДСТУ CWA 14171.
5. Оценить соответствие реализованной системы управления сертификатами семейства ОС Windows стандарту ДСТУ CWA 14167-1 и стандартных модулей подписи стандартам ДСТУ CWA 14167-2, 4 и ДСТУ CWA 14167-3.
6. Обеспечить настройку службы штемпелевания времени для сервера и клиентов согласно требованиям ДСТУ ETSI TS 101 861:2009.

Опционально также необходимо реализовать поддержку алгоритма ECGDsa и хеш-функции WHIRLPOOL. Отметим, что реализация этой хеш-функции повышает безопасность хеширования, отличного от схемы sha2, которая пока единственная реализована в семействе ОС Windows.

Укажем на нецелесообразность использования только «ГОСТ 34.311+ДСТУ 4145» для взаимодействия государства, субъектов хозяйствования и граждан Украины. В Украине уже 5 лет действуют национальные стандарты [15—16], допускающие международные комплекты подписей, поддержанных в популярных ОС.

При интеграции «ГОСТ 34.311+ДСТУ 4145» в ОС необходим высокий уровень интероперабельности реализаций криптоалгоримов, поскольку этот комплект, использованный для защиты государственных тайн, имеет независимые реализации. Более того, для «ГОСТ 34.311+ДСТУ 4145», как правило, отсутствует поддержка лицензионных «коробочных» алгоритмов, они требуют инсталляции криптомодулей, также требующей валидации. Для решения поставленных задач необходимо иметь рабочий тестовый стенд (далее стенд), проводящий полномасштабное тестирование модулей криптозащиты.

В гетерогенной среде eEconomy невозможно гарантировать, что *n* субъектов взаимоотношений будут пользоваться услугами одного общего ЦСК. Гарантия, что аккредитованные ЦСК предоставляют одинаково качественные услуги, — это выполнение Закона Украины «Об ЕЦП» [6] и возможность кроссертификации, причем максимально достижимая для всех реализаций Директивы 1999/93/ЕС. Отсутст-

вие стандартов и неспособность акторов рынка НСЭЦП создать согласованные спецификации сущностей привели к полному отсутствию интероперабельности НСЭЦП в Украине. Чтобы исправить ситуацию и построить НСЭЦП согласно эталонной модели QPKI, регламентирующей высококачественные услуги ЭЦП, следует на этапе аккредитации ЦСК допускать только интероперабельные ПТК. Эта возможность появилась недавно, после гармонизации части европейских стандартов по эталонной модели QPKI (см. ДСТУ-П CWA 14172:2008). Формализация также нужна согласно Закону Украины «Об ЭЦП» для создания Технического регламента НСЭЦП.

Стенд — это набор программных тестов для специальных и/или контрольных испытаний разнообразных объектов для достижения интероперабельных реализаций базовых сущностей НСЭЦП. Назначение стенда — ранжировать реализации ПТК (А)ЦСК по уровню интероперабельности и гарантировать интероперабельные реализации всех базовых сущностей НСЭЦП.

2. Личный ключ

Сейчас интероперабельным форматом личного ключа считают PKCS#8. Для усиления защиты этого формата его помещают в PKCS#5 или PKCS#12, которые защищают его паролем или шифрованием. Ныне нет международных (де-юре) и/или европейских стандартов (в частности ETSI) формата личного ключа для QPKI, это обеспечено идеологией Директивы 1999/93/EC. Для квалифицированных подписей она требует использовать только аппаратные SSCD, которые, по определению, блокируют доступ к личному ключу извне, следовательно, они защищены физически. Тогда технологические решения аппаратно-зашитой организации получения личного ключа в процессе генерации подписи нецелесообразно подвергать стандартизации.

Игрокам рынка НСЭЦП логично было бы использовать формат личного ключа PKCS#8 как кроссплатформный, но отсутствие норм и правил привело к созданию множества закрытых форматов. Так, на рис. 3 отображен DER-кодированный личный ключ (согласно ASN.1)

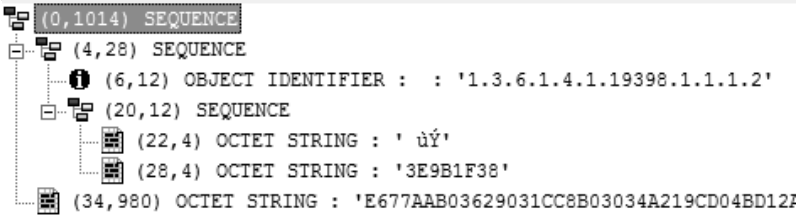

Рис. 3. *ASN.1-нотация DER-кодированного личного ключа одного из украинских ПТК*

В Листинге 1 приведена ASN.1-нотация PKCS#8.

```
AlgorithmIdentifier { ALGORITHM-
IDENTIFIER:InfoObjectSet } ::= SEQUENCE {
   algorithm ALGORITHM-IDENTIFIER.&id({InfoObjectSet}),
   parameters ALGORITHM-IDENTIFIER.&Type({InfoObjectSet}
   {@algorithm}) OPTIONAL }
-- Синтаксис информации о личном ключе

PrivateKeyInfo ::= SEQUENCE {
   version Version,
privateKeyAlgorithm AlgorithmIdentifier
   {{PrivateKeyAlgorithms}},
   privateKey PrivateKey,
   attributes [0] Attributes OPTIONAL }

Version ::= INTEGER {v1(0)} (v1,...)
PrivateKey ::= OCTET STRING
Attributes ::= SET OF Attribute
-- Синтаксис информации о зашифрованном личном ключе
EncryptedPrivateKeyInfo ::= SEQUENCE {
    encryptionAlgorithm AlgorithmIdentifier
   {{KeyEncryptionAlgorithms}},
   encryptedData EncryptedData
}
EncryptedData ::= OCTET STRING
```

Листинг 1. *ASN.1-нотация PKCS#8*

Как видим, в листинге 1 представлен необходимый минимальный и достаточный набор данных о личном ключе, а на. рис.3 регламентирован нестандартный набор параметров в закрытой для сторонних разработчиков ASN.1-нотации, что существенно препятствует интероперабельным реализациям. Более того, для внутренней интероперабельности на территории Украины, не говоря уже о кроссертификации, необходим стандартный формат личного ключа, например, на основе де-факто стандарта PKCS#8.

Отсутствие формата личного ключа не допускает разработчикам использовать созданные стандартные библиотеки в интероперабельных реализациях для обработки личных ключей вне зависимости от производителя ПТК.

3. Сертификат открытого ключа

Формат сертификата открытого ключа регламентирован [8], замечания к которому изложены в табл. 2.

Самое весомое замечание к [8] — отсутствие валидного модуля ASN.1-нотации, определяющего ASN.1-синтаксис сертификата открытого ключа. Так, констатируем полное дублирование специфика-

ций международных стандартов, например, нотаций `Certificate` и `TBSCertificate` из устаревшего RFC 3280.

Таблица 2.

Замечания к совместному приказу [8]

№	Пункт	Комментарии
1	1.1.1	Нормы ISO/IEC 9594-8 не действуют в Украине. Имеем пять версий этого стандарта, не указано, какая версия использована в [8]. Стандарт ISO/IEC 9594—8 формулирует основные составляющие сертификатов открытых ключей, но недостаточно точно для интероперабельных реализаций
2	1.1.3	Серия стандартов ДСТУ 8824:2009 имеют значительное количество исправлений, не отраженных в ссылке на ANS.1 синтаксис. Следовательно, большинство приведенных в [8] спецификаций программ и данных ошибочны
3	1.1.2	Согласно 1.1.2 «…определение формата сертификата не дублирует указанный стандарт, а лишь описывает особенности содержания сертификата и форматов его полей». Формат дублирует базовые нотации с ошибками и неточностями (см. далее «Ошибки в ASN.1-нотациях»). Зачем использовать кодировку UTF-8, если минимальной достаточной кодировкой украиноязычных текстов является KOI8-U. На основании какого стандарта кодируется UTF-8, если ДСТУ 4354-1:2004 допускает в Украине только UTF-16.
4	1.3.6	Почему разработчики формата пренебрегли международными (RFC 3739) правилами размещения параметров алгоритма в поле parameters нотации AlgorithmIdentifier. В этом причина отсутствия интероперабельности НСЕЦП
5	1.3.10	Почему формат не пересмотрен после вступления в силу национальных стандартов [12—14]. Жесткая регламентация используемых криптоалгоритмов и хеш-функций напрямую не способствует развитию НСЕЦП для достижения интероперабельности и кроссертификации со странами ВТО.
6	1.3.11	Описание параметров ДСТУ 4145 проведено с нарушениями синтаксиса ASN.1 согласно серии ДСТУ ISO/IEC 8824:2009. При описании параметров допущена избыточность параметров. Так, согласно ДСТУ 4145 можно установить «степень расширения основного поля» согласно «порядка базовой точки». Размещение параметров ДСТУ 4145 в рамках формата сертификата выполнено с нарушением международной практики, что делает невозможным достижение интероперабельных реализаций
7	1.3.11.2, 1.3.11.8	Неправомерно использованы OID для идентификации базовых объектов, поскольку только Держспоживстандарт имеет право устанавливать идентификаторы OID
8	1.3.11.7, 1.3.11.10	Описание параметров ГОСТ 34.310-95 проведено с нарушениями синтаксиса ASN.1 согласно серии ДСТУ ISO/IEC 8824:2009.

		Размещение параметров ГОСТ 34.310-95 в рамках формата сертификата выполнено с нарушением международной практики, что делает невозможным достижение интероперабельных реализаций внутри Украины. Этот ГОСТ пересмотрела Россия, гармонизировала его с ISO/IEC 14888:2008, но пересмотренный ГОСТ не действует в Украине. Целесообразно отменить ГОСТ 34.311-95, чтобы не засорять НСЕЦП Украины.
9	1.3.11.8	Российским алгоритмам недопустимо предоставлять OID в украинской ветви 804!
10	Нотации 1.4	Констатируем наибольшее количество ошибок в ASN.1-нотации именно в специфических для Украины объектах

Ошибки в ASN.1-нотациях

№	Название нотации	Ошибки
1	`AttributeValue, parameters, value, statementInfo, version, DSTU4145Params, BinaryField, Gost34310Params, keyUsage, QCStatement`	Несоответствие синтаксису ASN.1 согласно серии ДСТУ ISO/IEC 8824:2009
2	`version`	Отсутствует определение нотации Version. Согласно ДСТУ ISO/IEC 8824:2002 нотация состоит из идентификатора и определения типа. Поскольку Version не есть базовый тип ДСТУ ISO/IEC 8824:2009, необходимо его доопределить
3	`keyIdentifier`	Отсутствует определение нотации keyIdentifier (см. пункт 1 этой таблицы)
4	`policyQualifiers`	Отсутствует определение нотации PolicyQualifierInfo (см. пункт 1 этой таблицы)
5	`x400Address`	Отсутствует определение нотации ORAddress (см. пункт 1 этой таблицы)
6	`type`	Отсутствует определение нотации Attributetype (см. пункт 1 этой таблицы)

Подход «кусочно-непрерывных» интерпретаций норм международных и де-факто стандартов привел к разнообразным реализациям сертификатов открытых ключей, не говоря уже о списках аннулированных сертификатов. Ситуацию усугубляет игнорирование полномочными органами подхода к нормативному регулированию через национальные гармонизированные стандарты и отсутствие формализованной (на основе норм стандартов) методики оценки соответствия базовых объектов НСЭЦП соответствующим стандартам.

Эклектичный отбор норм международных стандартов в составе [8] обусловил невозможность использовать/разработать стандартные библиотеки в интероперабельных реализациях для обработки сертификатов открытых ключей. Проанализировав инструктивный материал, изложенный в проектах технических спецификаций [9—11], констатируем его не просто низкий уровень, а неспособность решить текущие проблемы интероперабельности. Основной причиной создания этих инструктивных материалов и попыткой использовать их как стандарты является неоправданные игнорирование [12—14] и желание включить только [15—17] в функцирнирующую PKI.

Отметим, что включение национальных негармонизированных стандартов в эталонную модель PKI грамотно выполнено в России, вследствие создания RFC 4491, регламентирующего использование положений [16] в сертификатах открытых ключей и списках аннулированных сертификатов.

4. Комплекты подписей

Согласно [8] комплекты подписей ограничены только двумя, не включенными в табл. 1 (т.е. не рекомендованными в Евросоюзе):

- ДСТУ 4145 +ГОСТ 34.311;
- ГОСТ 34.310-95+ГОСТ 34.311.

Рассмотрим первый комплект, поскольку второй устарел и не используется даже в СНГ.

Основными проблемами реализации ДСТУ 4145 является отсутствие профилей защиты на параметры криптоалгоритмов и тестовых стендов, гарантирующих интероперабельность реализаций. При реализации ДСТУ 4145 необходим следующий набор параметров:

1) основное поле, которое представляется
   a) степенью основного поля;
   b) примитивный трехчлен или пятичлен;
2) коэффициент A эллиптической кривой;
3) коэффициент B эллиптической кривой;
4) порядок базовой точки;
5) базовая точка эллиптической кривой;
6) открытый ключа;
7) личный ключ.

С представлением практически каждого параметра связаны проблемы интероперабельных реализаций ДСТУ 4145. Например, открытый ключ ДСТУ 4145 состоит из двух составляющих R и S, а совместный приказ регламентирует его хранение в сертификате открытого ключа как сжатый образ согласно п. 5.3 ДСТУ 4145. Но многие реализации сертификатов открытых ключей ДСТУ 4145 не выполня-

ют этого требования или выполняют «по-своему». Сложившаяся ситуация привела к алгоритму подписания сертификата открытого ключа, составленного из следующих шагов.

Шаг 1. Коэффициент B необходимо записать в сертификат открытого ключа в инверсном виде.

a. ДСТУ 4145, для полиномиального базиса:
03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3

b. Но в сертификат его надо записывать в инверсном виде, т.е.
F3CA40C669A4DA173149CA12C32DAE186B53AC6BC6365997DEAEAE8AD2D888F9BFD53401694EF9C4273D8CFE6DC28F706A0F4910CE03

Шаг 2. Порядок базовой точки (n) записывают в прямом виде, как указано в ДСТУ 4145:

3*FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFBA3175458009A8C0A724F02F81AA8A1FCBAF80D90C7A95110504CF*

Шаг 3. Координату базовой точки *X* необходимо записать в инверсном виде;

Шаг 4. Вычислить хеш по полю `TBSCertificate` сертификата открытого ключа;

Шаг 5. Сделать инверсию вычисленного хеша;

Шаг 6. Подписать инверсное значение хеша;

Шаг 7. Полученную подпись разбить на две части — координаты R и S;

Шаг 8. Инвертировать каждую координату R и S;

Шаг 9. Выполнить конкатенацию S и R, отметим требование сделать перестановку координат;

Шаг 10. В результате записать в поле `signatureValue` сертификат открытого ключа.

Этот алгоритм применяется в ЦЗО (укр. Центральний засвідчувальний орган) для подписания сертификатов зарегистрированных и аккредитованных ЦСК. Ни один нормативный документ не регламентирует указанного алгоритма. Также с позиций повышения криптостойкости сложность алгоритма никоим образом не влияет, а только усложняет достижение интероперабельности.

Отметим наличие, как минимум, пяти несовместимых криптомодулей ДСТУ 4145, явно препятствующих интероперабельности НСЭЦП.

Для профилирования ДСТУ 4145 в криптобиблиотеки [18] четко определены параметры ДСТУ 4145 в сертификате открытого ключа.

Рассмотрим методы профилирования ДСТУ 4145, которое уже реализовано в программном продукте (см. сертификат авторского права [18]).

4.1. Профилирование параметров хеш-функций

К параметрам ГОСТ 34.311-95 [17] в общем случае относятся:

- входной текст, подлежащий хешированию;
- значение хеш-функции;
- ключевые данные (в том числе таблица заполнения узлов замены блоков подстановки);
- стартовый вектор хеширования.

Входящие текст, значение хеш-функции, ключевые данные (кроме таблицы заполнения узлов замены блоков подстановки), процедуры хеширования представляются бинарными строками DER-кодирования с ASN.1 типом `OCTET STRING`. При этом используется схема кодирования Big Endian (см. 4.3). А таблица заполнения узлов замены блоков подстановки процедур хеширования представляется бинарной строкой DER-кодирования [19] с типом `OCTET STRING` [20]. При этом соблюдаются форматы представления ключевых данных, описанные далее в 4.4.

4.2. Профилирование параметров ДСТУ 4145

К параметрам ДСТУ 4145 относятся:

- открытый текст (значение хеш-функции для данных, для которой вычисляется ЭЦП);
- зашифрованный текст (ЭЦП);
- личный и открытый ключи;
- общие параметры;
- таблица заполнения узлов замены блоков подстановки.

Открытый и зашифрованный тексты представляют бинарными строками согласно DER-кодирования с типом `OCTET STRING`, используя схему кодирования Big Endian (см. далее 4.3).

Личный и открытый ключи представляются бинарными строками согласно DER-кодирования с типом `OCTET STRING`. При этом открытый ключ — это последовательность байтов, кодирующая элемент основного поля (см. 5.3 из ДСТУ 4145) как сжатое изображение (см. 6.9 из ДСТУ 4145) точки эллиптической кривой, ассоциированной с открытым ключом.

Общие параметры представляются согласно п. 1.3.11 Технических спецификаций форматов представления базовых объектов НСЭЦП, утвержденных совместным приказом [8], также измененные согласно [24]. В совместном приказе [8] использован устаревший текст международного стандарта, регламентирующий ASN.1-синтаксис:

- при использовании открытого ключа и общих параметров типа `OCTET STRING`, без применения сертификатов открытых ключей, задействуют схему кодирования Big Endian (см. 4.3);
- при использовании открытого ключа и общих параметров типа `OCTET STRING`, с применением сертификатов открытых ключей, задействуют схему кодирования Big Endian или Little Endian (см. 3).

Согласно ДСТУ 4145 таблица заполнения узлов замены блоков подстановки представляется бинарной строкой с DER-кодированием и типом `OCTET STRING`. При этом соблюдаются форматы представления ключевых данных согласно 4.4.

4.3. Схемы кодирования

Различают две схемы кодирования бинарных строк (битовых последовательностей).

Схема кодирования Big Endian предусматривает размещение старшего байта по младшему адресу. Так, в последовательности данных «*42 AB*» байт «*42*» есть старший байт, а байт «*AB*» — младший. Биты в байте пронумерованы справа налево числами от 0 до 7 по весу разряда; бит *i* имеет вес *2i*. Биты в бинарной строке пронумерованы справа налево целыми числами, начиная с 0. Бит *n* в бинарной строке кодируется как бит *i* байта *j*. Тут *i* и *j* вычисляют по формулам $i = n \bmod 8$; $j = n \operatorname{div} 8$, где $x \bmod y$ — операция вычисления остатка от деления *x* на *y*; $x \operatorname{div} y$ — операция деления *x* на *y* с округлением до ближайшего целого в меньшую сторону.

Если количество битов бинарной строки не кратно 8, неиспользованные биты последнего (старшего) байта должны содержать нули. Например, бинарную строку «*11100011*» кодируют как байт *E3h*, а «*1111000110111*» — как последовательность байтов *1Eh 37h*.

Схема кодирования Little Endian предусматривает размещение младшего байта по младшему адресу. Например, в последовательности данных «*42 AB*» байт «*42*» — младший, а «*AB*» — старший. Порядок нумерации битов в байте, кодирование отдельного бита бинарной строки и дополнение нулевыми битами неполных байтов проводят аналогично по правилам кодирования схемы *Big Endian*. Например, битовую строку «*11100011*» кодируют как байт *E3h*, а «*1111000110111*» — как последовательность байтов *37h 1Eh*.

4.4. Порядок кодирования таблицы заполнения узлов замены блоков подстановки

В зависимости от криптоалгоритма, использующего таблицу заполнения узлов замены блоков подстановки, бинарная строка (по правилам DER с типом `OCTET STRING`) может содержать эту таблицу в раз-

вернутом или упакованном формате. Согласно ДСТУ 4145-2002 для ГОСТ 28147-89 используют упакованный формат, а для ГОСТ 34.310-95 — расширенный. Эта таблица — матрица, имеющая в столбцах *K*1,...,*K*8 по 16 элементов (0,...,15). Порядок расположения элементов:

```
K1.0, K1.1 ... K1.15, K2.0, K2.1 ... K2.15, ...
            ... K8.0, K8.1 ... K8.15.
```

Упакованный формат таблицы заполнения узлов замены блоков подстановки — это массив фиксированной длины в 64 байта. Элементы таблицы располагаются попарно, образуя 64 пары значений. Каждая пара кодируется одним байтом, причем первый элемент пары — старший полубайт, а второй элемент пары — младший полубайт.

Например, если *K1*.0 = *4h*, а *K1*.1 = *Ah*, то первый байт массива имеет значение *4Ah*.

Для блока подстановки, приведенного в Приложении А из ГОСТ 34.311-95, упакованный формат таблицы заполнения узлов замены блоков подстановки имеет вид:

```
4A 92 d8 0e 6b 1c 7f 53
eb 4c 6d fa 23 81 07 59
58 1d a3 42 ef c7 60 9b
7d a1 08 9f e4 6c b2 53
6c 71 5f d8 4a 9e 03 b2
4b a0 72 1d 36 85 9c fe
db 41 3f 59 0a e7 68 2c
1f d0 57 a4 92 3e 6b 8c
```

Расширенный формат таблицы заполнения узлов замены блоков подстановки — это массив фиксированной длины в 128 байтов. Элементы таблицы располагаются поочередно, образуя 128 значений. Каждый элемент закодирован одним байтом. Так, для блока подстановки, приведенного в Приложении А из ГОСТ 34.311-95, расширенный формат таблицы имеет вид:

```
04 0A 09 02 0d 08 00 0e 06 0b 01 0c 07 0f 05 03
0e 0b 04 0c 06 0d 0f 0a 02 03 08 01 00 07 05 09
05 08 01 0d 0a 03 04 02 0e 0f 0c 07 06 00 09 0b
07 0d 0a 01 00 08 09 0f 0e 04 06 0c 0b 02 05 03
06 0c 07 01 05 0f 0d 08 04 0a 09 0e 00 03 0b 02
04 0b 0a 00 07 02 01 0d 03 06 08 05 09 0c 0f 0e
0d 0b 04 01 03 0f 05 09 00 0a 0e 07 06 08 02 0c
01 0f 0d 00 05 07 0a 04 09 02 03 0e 06 0b 08 0c
```

Заключение. Для построения интероперабельных реализаций ДСТУ 4145 необходимо профилировать его параметры, например, создав по правилам принятия RFC, регламентирующего использования ДСТУ 4145 в PKIX. Также необходимо отказаться от норматив-

ного регулирования с помощью инструктивного материала и использовать национальные институты стандартизации для создания корректной нормативной базы технологического регулирования всех составляющих НСЭЦП. В первую очередь на основе этих норм необходимо создать формальную методику оценки соответствия ПТК нормативной базе. Можно достичь внутренней интероперабельности ДСТУ 4145, но его нельзя использовать для кроссертификации.

Список использованной литературы:

1. Мелащенко А. О. Проблемы интероперабельности Национальной системы электронных цифровых подписей / А. О. Мелащенко, О. Л. Перевозчикова // Кибернетика и системный анализ, 2009. — № 3. — С. 55—63.
2. Мелащенко А. О. Комплекти підписів для інтероперабельності Національної системи електронних цифрових підписів / А. О. Мелащенко, О. Л. Перевозчикова, О. С. Скарлат, К. С. Криворучко // Наукові записки Києво-Могилянської академії. Т. 99. Комп'ютерні науки. — К. : Пульсари, 2010. — С. 70—77.
3. Мелащенко А. О. Кроссертификация Украины / А. О. Мелащенко, О. Л. Перевозчикова // Проблемы программирования, 2010. — №2—3. — С. 299—308.
4. Директива 1999/93/ЕС об общественной структуре для поддержки электронных подписей.
5. Решение Еврокомиссии 2003/511/ЕС.
6. Закон Украины от 22.05.2003 № 852 «Про електронний цифровий підпис».
7. Режим доступу : www.openssl.org.
8. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ та Держдепартаменту з питань зв'язку та інформатизації Мінтрансу від 11.09.2006 №99/166.
9. Національна система електронного цифрового підпису. Проект технічних специфікацій протоколів взаємодії. Протокол визначення статусу сертифіката. — Режим доступу : www.dki.gov.ua.
10. Національна система електронного цифрового підпису. Проект технічних специфікацій форматів представлення базових об'єктів. Формат підписаних даних. — Режим доступу : www.dki.gov.ua.
11. Національна система електронного цифрового підпису. Проект технічних специфікацій форматів представлення базових об'єктів Національної системи електронного цифрового підпису. Протокол фіксування часу. — Режим доступу : www.dki.gov.ua.
12. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням (у 3-х частинах) : ДСТУ ISO/IEC 14888-2002
13. Методи захисту. Геш-функції (у 3-х частинах) : ДСТУ ISO/IEC 10118-2004.
14. Електронні підписи та інфраструктури (ESI). Алгоритми та параметри безпечних електронних підписів. Частина 1. Геш-функції та асиметричні алгоритми : ДСТУ ETSI TS 102 176-1 (V2.0.0) (2007-11).

15. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірян-ня : ДСТУ 4145-2002.
16. Информационная технология. Криптографическая защита информации. Функция хэширования : ГОСТ 34.311.
17. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма : ГОСТ 34.310-95.
18. Свідоцтво про реєстрацію авторського права на твір № 31086. «Комп'ютерна програма «Бібліотека функцій криптографічних перетворень «UPGCryptoProviderBasic»» / А. О. Мелащенко, Є. О. Свиридов.
19. Інформаційні технології. ASN.1 правила кодування. Частина 1. Специфікація правил базового кодування (BER), правил канонічного кодування (CER) та правил витонченого кодування (DER) : Проект ДСТУ ISO/IEC 8825-1.
20. Інформаційні технології. Нотація абстрактного синтаксиса 1 (ASN.1) (у 4-х частинах) : ДСТУ ISO/IEC 8824-1:2002.

Article shows possible solutions of existing problems of interoperability based on signature suite GOST 34.311 + DSTU 4145 implementation, provide suggestions on profiling of GOST 34.311 + DSTU 4145 paramenters, as well as to integrate it into modern operation systems.

Key words: *electronic signature, cryptomodule, cryptoalgorithm*

Отримано 24.06.10

УДК 681.511.42:62-83

В. І. Мороз, канд. техн. наук,
В. М. Оксентюк, канд. техн. наук,
І. Ф. Снітков, зав. лаб. НДЛ-68
Національний університет «Львівська політехніка», м. Львів

РЕАЛІЗАЦІЯ ОПЕРАЦІЇ ДИФЕРЕНЦІЮВАННЯ У МІКРОКОНТРОЛЕРАХ

У статті пропонується спосіб реалізації цифрового диференціатора для мікропроцесорних і мікроконтролерних систем, який робить його працездатним в широкому діапазоні кроків дискретизації за наявності зовнішніх завад.

Ключові слова: *дискретні системи, мікроконтролер, цифрові регулятори, цифровий диференціатор.*

Постановка проблеми. Широке розповсюдження цифрової техніки змусило зосередити увагу на особливостях реалізації програмного забезпечення таких систем — необхідності роботи з дискретизованими в часі та квантованими за рівнем даними. При цьому не врахо-