Необходимость разработки и стандартизации ключевого контейнера TR 31 с российскими криптографическими алгоритмами

Специалист по защите информации — **Елена Николаевна Шкоркина**
shkorkina@systempb.ru

Заместитель генерального директора по НТР — Елена Владимировна Мареева

Руководитель отдела системных исследований — Алла Геннадьевна Герасимова

Руководитель направления перспективных проектов — Александр Александрович Габов

Требования к криптографическим алгоритмам СКЗИ платежных систем РФ

Положение Банка России № 719-П (от 04.06.2020): СКЗИ из состава аппаратных модулей безопасности, реализующие **иностранные криптографические алгоритмы и криптографические алгоритмы РФ, должны** иметь подтверждение соответствия требованиям, установленным ФОИВ в области обеспечения безопасности информации.

Требования ФОИВ к криптографическим механизмам СКЗИ:

1) Должны использоваться криптографические механизмы из числа национальных стандартов РФ или рекомендаций по стандартизации, или криптографические механизмы, имеющие положительное заключение по результатам их экспертных криптографических исследований.

2) С целью обеспечения совместимости должны использоваться криптографические механизмы, отвечающие международным стандартам (ISO).

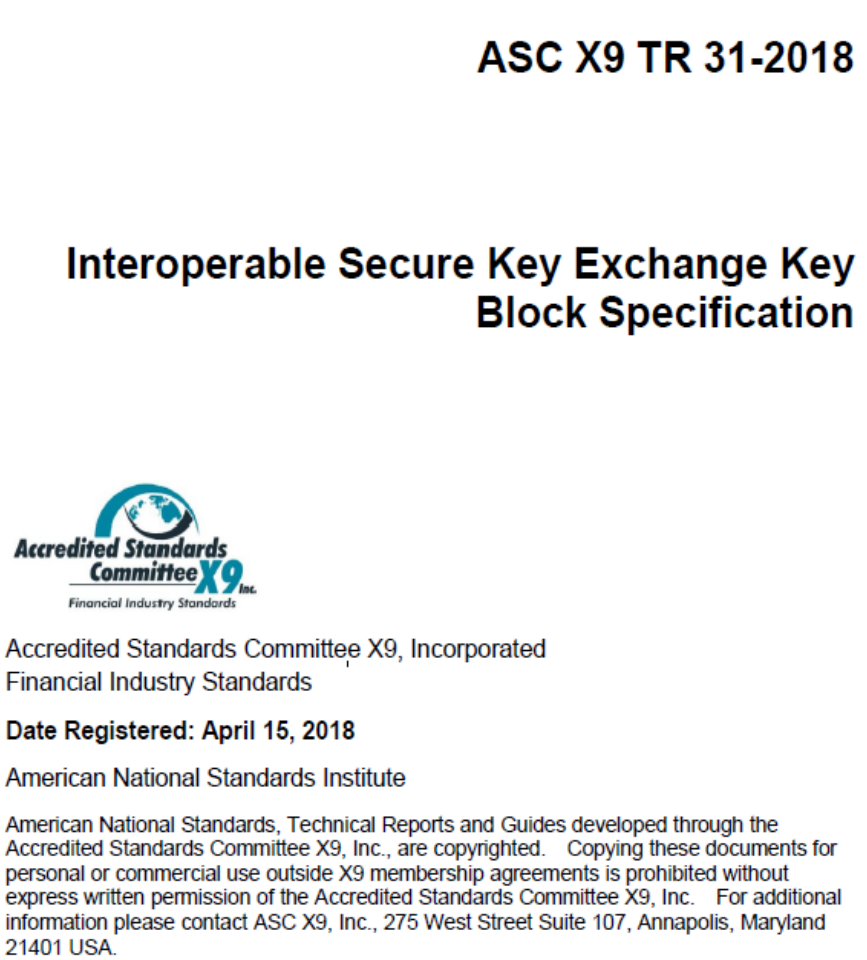
Требуется разработка национальных криптографических механизмов, в числе которых важное место занимает ключевой контейнер ACS X9 TR 31–2018 с российскими криптографическими алгоритмами (ACS X9 TR 31–2018 GOST).

Ключевой контейнер ACS X9 TR 31–2018

Стандарт ACS X9 TR 31–2018 определяет механизм ключевого контейнера, предназначенного для передачи и защищенного хранения ключевой информации, использующейся платежными системами во всех компонентах экосистемы, работающих с этими данными (центрами эмиссии, процессинговыми центрами и т.п.) в соответствии с требованиями PCI PIN Security, определяющими:

- Необходимость обеспечения целостности и подлинности всех передаваемых данных (как за открытые поля ключевого блока, так и за зашифрованные поля, содержащие ключ или иные защищаемые данные);
- Процедура проверки целостности должна быть неотделима от процесса защиты ключей (производиться одновременно с расшифрованием).

В соответствиями с требованиями PCI PIN Security, контейнер TR 31 содержит набор обязательных полей, специфичных для платёжных систем и ограничивающих операции с ключом («Key Usage» и «Mode of Use»).



ASC X9 TR 31-2018

Interoperable Secure Key Exchange Key Block Specification

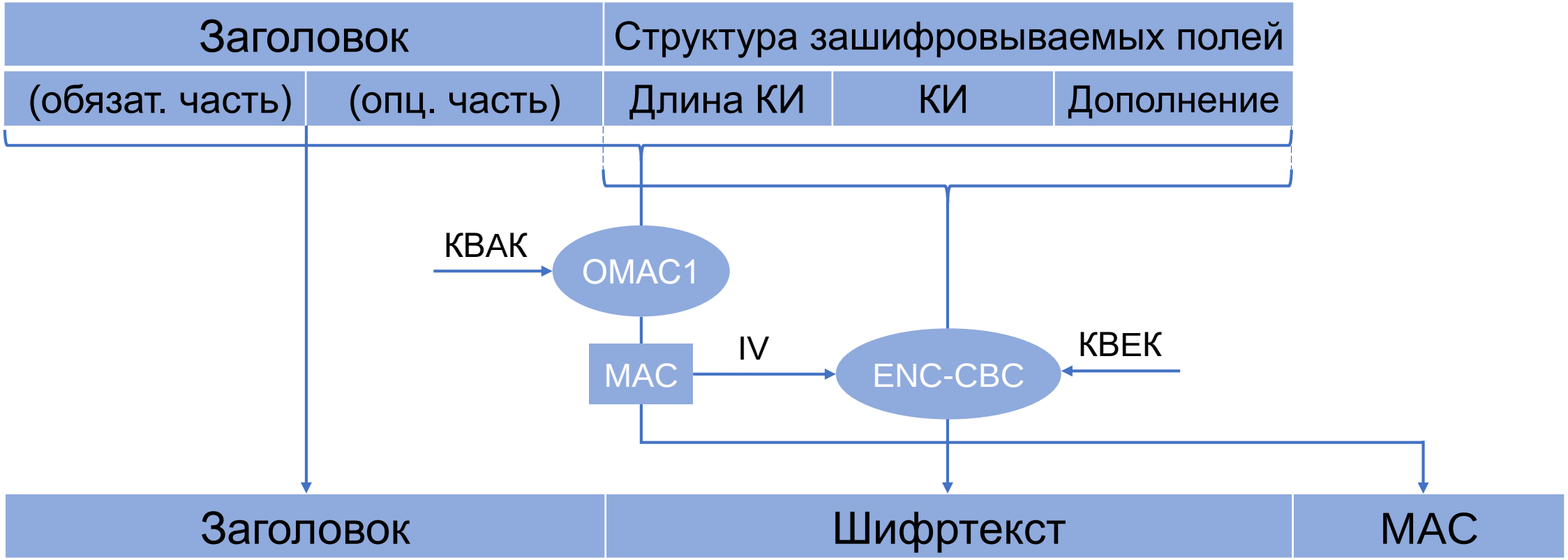
Accredited Standards Committee X9 Inc. Financial Industry Standards

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Registered: April 15, 2018

American National Standards Institute

Схема формирования ключевого контейнера



Дополнение структуры зашифровываемых полей выполняется до кратности одному или нескольким блоков шифра.

Заголовок контейнера ACS X9 TR 31 GOST

Поля обязательной части заголовка		
Байт	**Название поля**	**Описание**
0	KeyBlockVersionID	Идентификатор версии контейнера, определяющий способ криптографической защиты и формат внутренней структуры
1-4	KeyBlockLength	Общая длина контейнера, включая обязательную и опциональную часть заголовка, зашифрованные данные и поле имитовставки
5-6	*KeyUsage*	*Назначение ключа (‘P0’ – ключ для шифрования PIN-блока, ‘B1’ – начальный DUKPT-ключ, ‘V2’ – ключ проверки криптограммы VISA PVV и др.)*
7	Algorithm	Алгоритм, в котором требуется использовать экспортируемую КИ
8	*ModeOfUse*	*Вид операции, для которой должен применяться ключ (‘B’ – ключ для шифрования, ‘D’ – ключ только для расшифрования; ‘E’ – ключ только для зашифрования, др.)*
9-10	KeyVersionNumber	Определяет порядковый номер версии ключа, либо используется в иных целях, например, для обозначения номера компоненты ключа
11	Exportability	Определяет разрешения или запрета экспорта ключа: ‘E’ — экспорт разрешён на специальном доверенным ключе, ‘N’ — экспорт запрещён
12-13	NumberOfOptionalBlocks	Определяет число дополнительных опциональных блоков, следующих за заголовком

Поля, определяющие ACS X9 TR 31 GOST

Структура ACS X9 TR 31–2018 позволяет расширить множество значений служебных полей криптографическими механизмами на основе ГОСТ.

Значения поля «KeyBlockVersionID» (ASCII)	Способ криптографической защиты и формат внутренней структуры ключевого контейнера
‘0’	Метод вывода привязанных ключей (Key Derivation Method) на основе блочного шифра «Магма» (ГОСТ Р 34.12-2018)
‘1’	Метод вывода привязанных ключей (Key Derivation Method) на основе блочного шифра «Кузнечик» (ГОСТ Р 34.12-2018)

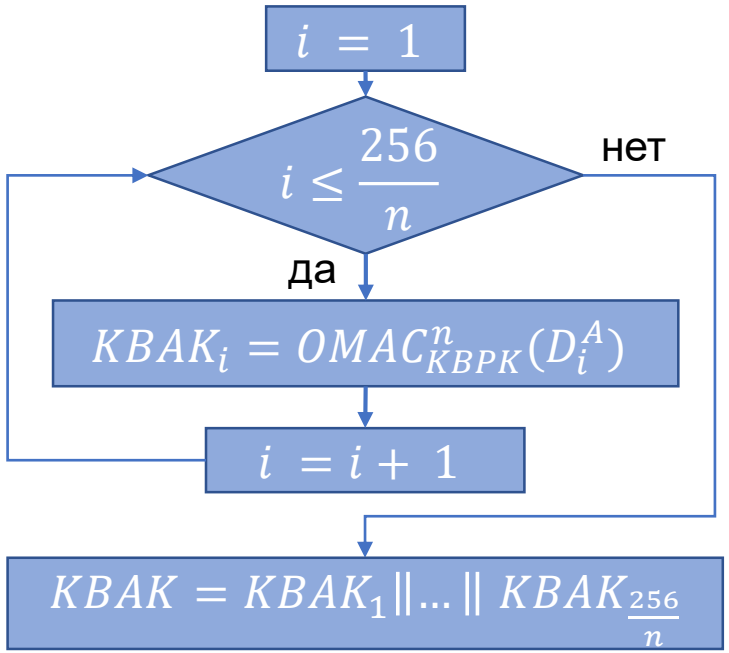
Значения поля «Algorithm» (ASCII)	Алгоритм, в котором должна использоваться экспортируемая КИ
‘0’	«Магма» (ГОСТ Р 34.12-2015)
‘1’	«Кузнечик» (ГОСТ Р 34.12-2015
‘2’	HMAC (Р 50.1.113-2016, на основе ГОСТ Р 34.11-2012)
‘3’	Пара ключей подписи (ГОСТ Р 34.10-2012)

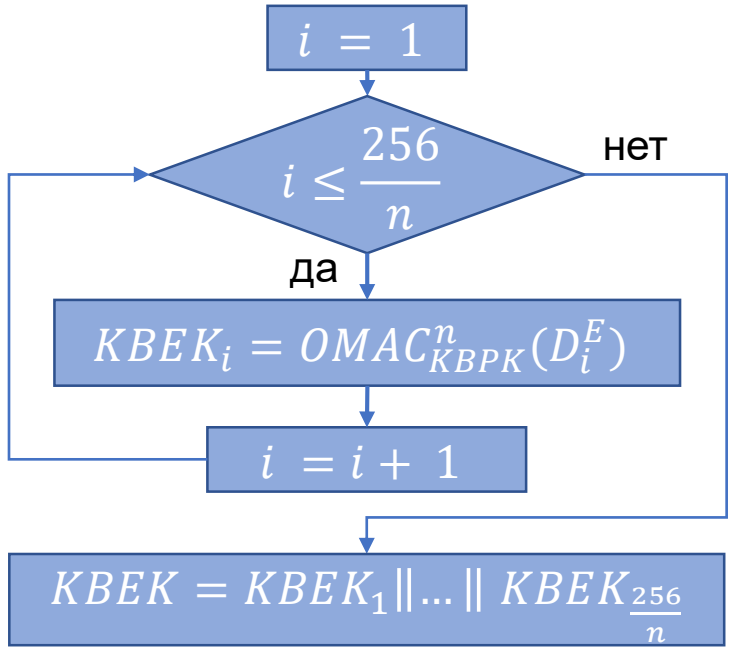
Тип алгоритма HMAC указывается в специальной структуре в числе опциональных блоков

Выработка ключей KBAK и KBEK

Структура входных данных для диверсификации (D_i^A, D_i^E)

Тетрады	Название поля	Назначение	Кодировка	Значения
0-1	Счетчик (i)	Счётчик блоков формируемого ключа	2H	0x01–0x04 – «Магма»; 0x01–0x02 – «Кузнечик»
2-5	Назначение ключа	Механизм, для использования в котором вырабатывается ключ	4H	0x00, 0x00 – шифрование; 0x00, 0x01 – имитозащита
6-7	Разделитель	Разделение полей	2H	0x00
8-11	Алгоритм	Определяет используемый алгоритм	4H	0x00, 0x05 – «Магма»; 0x00, 0x06 – «Кузнечик»
12-15	Длина	Длина формируемого ключа в байтах	4H	0x01, 0x00 – «Магма»; 0x01, 0x00 – «Кузнечик»





Структура зашифровываемых данных

Описание поля	Длина	Шифрование
Длина защищаемых данных в битах (BigEndian-представление)	2B	Да
Любые защищаемые данные (например, TDES ключ вместе с битами чётности)	nB	
Дополнение структуры до кратности одному или нескольким блокам шифра	Случайное число	

Симметричные ключи простого формата упаковываются непосредственно в байтовом представлении, для асимметричных ключей возможна упаковка в соответствии с выбранной структурой.

Упаковка пары RSA в соответствии с PKCS #1 v.2.1:

```
RSAPrivateKey ::= SEQUENCE {
version Version,
modulus INTEGER, -- n
publicExponent INTEGER, -- e
privateExponent INTEGER, -- d
prime1 INTEGER, -- p
prime2 INTEGER, -- q
exponent1 INTEGER, -- d mod (p-1)
exponent2 INTEGER, -- d mod (q-1)
coefficient INTEGER, -- (inverse of q) mod p
otherPrimeInfos OtherPrimeInfos OPTIONAL
}
```

Упаковка ключей подписи ГОСТ Р34.10-2012 в формат ASN.1 в соответствии с Р 1323565.1.041–2022 «Транспортный ключевой контейнер»:

```
OneAsymmetricKey::= SEQUENCE
{
Version                    Version,
privateKeyAlgorithm        PrivateKeyAlgorithmIdentifier,
privateKey                 OCTET STRING,
Attributes                 [0] Attributes OPTIONAL,
...,
[[2:publicKey              [1]BIT STRING OPTIONAL]],
...
}
Version ::= INTEGER { v1(0), v2(1) } (v1, ..., v2)
PrivateKeyAlgorithmIdentifier ::= AlgorithmIdentifier
Attributes ::= SET OF Attribute
```

Сравнение ACS X9 TR 31 GOST с ранее стандартизированными ключевыми контейнерами

Критерий	ACS X9 TR 31 GOST	KExp15 / KImp15[1]	PKCS#12[2]
Учет специфики и требований платежной индустрии	+	-	-
Наличие служебных полей	+	-	+
Содержит механизм дополнения КИ	+	-	-
Не требует задания на вход алгоритма экспорта / импорта синхропосылки	+	-	+ (IV можно передать в поле структуры)
Возможность передачи любой КИ с указанием типа	+	-	-

[1] Р 1323565.1.017–2018 ««Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»

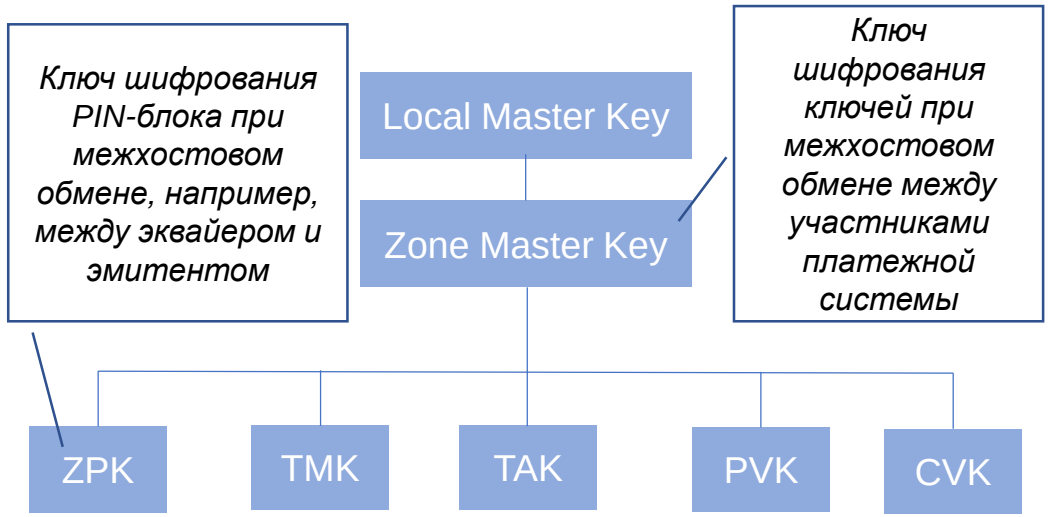
[2] Р 1323565.1.041–2022 «Информационная технология. Криптографическая защита информации. Транспортный ключевой контейнер»

Практическое использование ACS X9 TR 31–2018

Передача КИ от эмитента эквайеру:

1. Передача ZMK_0 в виде компонент.
2. Передача ZPK в ключевом контейнере ACS X9 TR 31–2018 с использованием в качестве KBPK ранее переданного ZMK_0.

Загрузка ZMK_i выполняется в контейнере ACS X9 TR 31–2018 с использованием в качестве KBPK ключа ZMK_{i-1}.



Иерархия сетевых ключей

Функция экспорта / импорта в соответствии с ACS X9 TR 31–2018 является обязательной для:

1. Поддержки функций ПС «Мир».
2. Совместимости с банковским ПО:

- TranzWare Online v. 5.3.44.2;
- TranzAxis v. 3.2.29;
- TranzWare Card Factory v.2.1.93;
- TranzWare/TranzAxis e-Commerce ACS v 3.1.42.2

Смена исходного ключа алгоритма DUKPT GOST в устройстве, инициирующем транзакцию[1]

В соответствии с проектом МР ТК 26 «Использование российских криптографических алгоритмов в методе формирования ключей транзакций при оказании услуг электронной коммерции (DUKPT - Derived unique key per transaction)»

Спасибо за внимание!

shkorkina@systempb.ru