ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р

(первая редакция)

Информационные технологии

БИОМЕТРИЯ

Биометрическое сравнение на идентификационной карте

Часть 2

Механизм распределения

Москва
Российский институт стандартизации
202

ГОСТ Р

(первая редакция)

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») и Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 098 «Биометрия и биомониторинг»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от № -ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующие информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

Содержание

1 Область применения .....

2 Нормативные ссылки.....

3 Термины и определения.....

4 Сокращения.....

5 Соответствие.....

6 Процедура биометрического сравнения на идентификационной карте с механизмом распределения .....

Введение

Биометрическое сравнение на идентификационной карте обеспечивает повышенную конфиденциальность и более безопасное биометрическое распознавание, чем биометрическое сравнение вне идентификационной карты. Хранение биометрических контрольных шаблонов на защищенной интегральной схеме (integrated circuit cards, ICC) означает, что данные недоступны ни на каком внешнем интерфейсе после того, как они были сохранены в ICC, что снижает риск их извлечения и неправильного использования неавторизованной стороной.

ГОСТ Р ИСО/МЭК 7816-11 и ГОСТ Р ИСО/МЭК 19785-3 устанавливают требования к технологиям биометрического сравнения вне идентификационной карты и простого биометрического сравнения на идентификационной карте. Серия стандартов ГОСТ Р ИСО/МЭК 17839 устанавливает требования к технологиям биометрической системы на идентификационной карте.

ГОСТ Р

(первая редакция)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Биометрическое сравнение на идентификационной карте

Часть 2

Механизм распределения

Information technology. Biometrics. On-card biometric comparison. Part 2. Work-sharing mechanism

Дата введения – 202 – –

1 Область применения

Настоящий стандарт устанавливает требования к процедуре биометрического сравнения на идентификационной карте с механизмом распределения.

Настоящий стандарт не устанавливает требования:

- к архитектуре биометрического сравнения с использованием ICC;
- биометрическому сравнению на идентификационной карте;
- политике безопасности для биометрического сравнения на идентификационной карте;
- выполнению биометрического сравнения вне идентификационной карты;
- системе на идентификационной карте;
- хранению и процессу сравнения применительно к конкретным биометрическим модальностям.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO/IEC 2382-37–2016 Информационные технологии. Словарь. Часть 37. Биометрия

ГОСТ Р ИСО/МЭК 7816-4–2013 Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена

ГОСТ Р ИСО/МЭК 7816-11–2013 Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами

ГОСТ Р 58230–2018 (ИСО/МЭК 24787:2010) Информационные технологии. Идентификационные карты. Биометрическое сравнение на идентификационной карте

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по *ГОСТ ISO/IEC 2382-37* и *ГОСТ Р 58230–2018*.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

APDU – блок данных протокола приложения (application protocol data unit);

EF – элементарный файл (elementary file);

ICC – карта на интегральной схеме (integrated circuit card);

SW1-SW2 – байты состояния.

5 Соответствие

Система на идентификационной карте с механизмом распределения, в которой осуществляется биометрическое сравнение, соответствует настоящему стандарту, если она соответствует требованиям, указанным в разделе 6, а также в соответствующих разделах ГОСТ Р 58230–2018, где это применимо.

6 Процедура биометрического сравнения на идентификационной карте с механизмом распределения

Механизм распределения при биометрическом сравнении на идентификационной карте должен использовать биометрические вспомогательные данные, считанные из ICC, если ICC поддерживает биометрическое сравнение на идентификационной карте с механизмом распределения.

Примечание – Вспомогательные биометрические данные хранятся отдельно от биометрического контрольного шаблона. Например, биометрические вспомогательные данные хранятся в рабочем элементарном файле (EF), а биометрический контрольный шаблон хранится во внутреннем EF, определенном в ГОСТ Р ИСО/МЭК 7816-4.

На рисунке 1 показана схема процедуры биометрического сравнения на идентификационной карте с механизмом распределения. Для реализации этой процедуры команды и байты состояния должны соответствовать ГОСТ Р ИСО/МЭК 7816-4 и ГОСТ Р ИСО/МЭК 7816-11. В настоящем стандарте анализируются наиболее распространенные в использовании биометрические технологии.

Рисунок 1 — Обмен «команда-ответ» APDU для процедуры распределения

Процедура распределения осуществляется в следующей последовательности:

1) ICC получает команду извлечения данных (например, READ BINARY) для извлечения информации из биометрического контрольного шаблона;

2) ICC возвращает информацию из биометрического контрольного шаблона для проверки параметров;

3) ICC получает команду извлечения данных, (например, READ BINARY) для извлечения вспомогательных биометрических данных;

4) ICC возвращает вспомогательные данные для обработки биометрического образца;

5) ICC получает команду биометрической верификации, требующую биометрического сравнения на идентификационной карте, а затем запускает первый процесс биометрического сравнения на идентификационной карте с распределением.

6) ICC возвращает байты состояния в формате «62xx», при этом под «xx» указывается число байтов обратной связи, доступных в соответствии со строкой байтов, созданной картой, определенной в ГОСТ Р ИСО/МЭК 7816-4;

7) ICC получает команду GET DATA для получения обратной связи;

8) ICC возвращает обратную связь;

9) ICC получает команду биометрической верификации на идентификационной карте, а затем запускает окончательный процесс биометрического сравнения, принятия решения и действия;

10) ICC возвращает байты состояния, указывающие результат биометрической верификации.

ГОСТ Р

(первая редакция)

УДК 004.93'1:006.354 ОКС 35.240.15

Ключевые слова: информационные технологии, биометрия, идентификационные карты, биометрическое сравнение, биометрическое сравнение на идентификационной карте