ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72303— 2025

Информационные технологии

БИОМЕТРИЯ

Биометрическое сравнение на идентификационной карте. Механизм распределения

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН 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 23 сентября 2025 г. № 1100-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». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2025

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Введение

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

В ГОСТ Р 58671 и ГОСТ Р 58294 установлены требования к технологиям биометрического сравнения вне идентификационной карты и простого биометрического сравнения на идентификационной карте, в ГОСТ Р ИСО/МЭК 17839-1 — к технологиям биометрической системы на идентификационной карте.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Биометрическое сравнение на идентификационной карте. Механизм распределения

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

Дата введения — 2026—01—01

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 карт на интегральных схемах ICC;
- политике безопасности для биометрического сравнения на идентификационной карте;
- процедуре биометрического сравнения вне идентификационной карты;
- биометрической 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 Информационные технологии. Словарь. Часть 37. Биометрия

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

ГОСТ Р 58294 (ИСО/МЭК 19785-3:2015) Информационные технологии. Биометрия. Единая структура форматов обмена биометрическими данными. Часть 3. Спецификации формата ведущей организации

ГОСТ Р 58671 (ИСО/МЭК 7816-11:2017) Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами

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

ГОСТ Р ИСО/МЭК 17839-1 Информационные технологии. Биометрическая система на идентификационной карте. Часть 1. Основные требования

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 ут-

Издание официальное

верждения (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, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по ГОСТ ISO/IEC 2382-37, а также следующие термины с соответствующими определениями:

3.1.1

вспомогательные данные (auxiliary data): Данные, зависящие от особенностей биометрической модальности и связанные с биометрическим контрольным шаблоном, но не содержащие биометрический контрольный шаблон или биометрический образец.

Пример — Такие данные, как ориентация, масштабирование и т. п., являются вспомогательными данными.

[ГОСТ Р 58230—2018, пункт 4.1]

3.1.2

элементарный файл (elementary file): Набор единиц данных, или записей, или информационных объектов, которые совместно используют один и тот же идентификатор файла и один (одни) и тот (те) же атрибут(ы) секретности.

[ГОСТ Р ИСО/МЭК 7816-4—2013, пункт 3.19]

3.1.3

рабочий элементарный файл (working elementary file): EF для хранения данных, не интерпретируемых картой.

[ГОСТ Р ИСО/МЭК 7816-4—2013, пункт 3.45]

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

EF — элементарный файл (elementary file);

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

SW1-SW2 — байты состояния.

4 Соответствие

Система на идентификационной карте с механизмом распределения, в которой осуществляется биометрическое сравнение, должна соответствовать требованиям раздела 6 и, если необходимо, ГОСТ Р 58230.

5 Процедура биометрического сравнения на идентификационной карте с механизмом распределения

В механизме распределения при биометрическом сравнении на идентификационной карте используют биометрические вспомогательные данные, считанные из ICC, если ICC поддерживает биометрическое сравнение на идентификационной карте с механизмом распределения.

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

На рисунке 1 представлена схема процедуры биометрического сравнения на идентификационной карте с механизмом распределения.



Рисунок 1 — Схема процедуры биометрического сравнения на идентификационной карте с механизмом распределения

Для реализации процедуры, приведенной на рисунке 1, команды и байты состояния должны соответствовать ГОСТ Р ИСО/МЭК 7816-4 и ГОСТ Р 58671. В настоящем стандарте установлены наиболее распространенные в использовании биометрические технологии.

Процедура биометрического сравнения на идентификационной карте с механизмом распределения осуществляется в следующей последовательности:

1) ICC получает команду извлечения данных (например, команду «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, команду «READ BINARY») для извлечения биометрических вспомогательных данных;

4) ICC возвращает биометрические вспомогательные данные для обработки биометрического образца;

5) ICC получает команду биометрической верификации, для которой требуется биометрическое сравнение 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» указывает число байтов обратной связи, доступных в соответствии со строкой байтов, созданной картой (см. 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 с распределением, процессы принятия решения и действия;

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

УДК 004.93′1:006.354 ОКС 35.240.15

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

Редактор *М.В. Митрофанова*
Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 25.09.2025. Подписано в печать 14.10.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 0,93. Уч.-изд. л. 0,68.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru