**ISO / IEC JTC 1 / SC 27 / WG 5 N1931** 

**ISO / IEC JTC 1 / SC 27 N19791**

**ЗАМЕНЯЕТ: N19768**

|  |
| --- |
| **ISO / IEC JTC 1 / SC 27 / WG 5**  **Технологии управления идентификацией и конфиденциальности**  **Организатор / Секретариат: DIN, Германия** |

**Тип документа: Текст для голосования FDIS (определен)**

**Название: Текст для ISO / IEC FDIS 24761: 2019-07- 11 (E) - Информационные технологии - Методы безопасности - Контекст аутентификации для биометрии**

**Статус: этот документ распространяется на заседании SC 27 / WG 5 для информации. Дата документа: 2019-07-11**

**Источник: ISO / CS (ITTF)**

**Ожидаемое действие: INFO Срок выполнения**

**действия:**

**Количество страниц: 1 + 99**

**Электронная почта секретаря: krystyna.passia@din.de**

**URL комитета: http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg5**

Секретариат ISO / IEC JTC 1 / SC 27 / WG 5 -

DIN Deutsches Institut für Normung e. V., Saatwinkler Damm 42/43, D-13627 [почтовый адрес D-10772] Берлин, Германия Телефон: + 49 30 2601-2652; Факс: + 49 30 2601-4-2652; Электронная почта: krystyna.passia@din.de; HTTP://www.din.de/go/jtc1sc27

**AISO / IEC JTC 1 / SC 27 N19791**

**ЗАМЕНЯЕТ: N19768**

|  |
| --- |
| **ISO / IEC JTC 1 / SC 27**  **Информационная безопасность, кибербезопасность и защита конфиденциальности**  **Секретариат: DIN, Германия** |

**DOC TYPE: текст для бюллетеня FDIS**

**НАЗВАНИЕ: Текст для ISO / IEC FDIS 24761: 2019-07-11 (E) (пересмотр ) - Информационные технологии - Методы безопасности - Контекст аутентификации для биометрии**

**ИСТОЧНИК: ISO / CS (ITTF)**

**ДАТА: 11.07.2019**

**ПРОЕКТ: 1.27.49 (ISO / IEC 24761, редакция)**

**СТАТУС: Этот документ в настоящее время проходит 8 недель Письменное голосование FDIS на уровне SC 27. Просьба к членам SC 27 направить свои голоса (члены P) или комментарии (члены O и организации по связям) по прилагаемому ISO / IEC FDIS 24761: 2019-07-11 (E) непосредственно в Центральный секретариат ISO. через приложение для электронного голосования ISO до указанного срока.**

**ДЕЙСТВИЕ:ГОЛОСОВАНИЯ**

**СРОК: 05.09.2019: Члены**

**РАСПРЕДЕЛЕНИЕP, O и L,**

**Л. Райчел, Секретариат JTC 1**

**Дж. Алькорта, ITTF**

**А. Вольф, Председатель SC 27**

**Л. Линдсей, Заместители SC 27 Председатель**

**EJ Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors A. Yamada, редактор проекта**

**MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27**

**НЕТ. СТРАНИЦ: 1 + 82 + 16 (Приложение 1)**

Секретариат ISO / IEC JTC 1 / SC 27 -

DIN Deutsches Institut für Normung e. V., Saatwinkler Damm 42/43, D-13627 [почтовый адрес D-10772] Берлин, Германия Телефон: + 49 30 2601-2652; Факс: + 49 30 2601-4-2652; Электронная почта: krystyna.passia@din.de; HTTP://www.din.de/go/jtc1sc27

Окончательного проекта

международного стандарта

**ИСО / МЭК FDIS**

**24761**

ИСО / МЭК JTC **1**/ SC **27**

Секретариат: DIN

голосование начинается:

**2019**-**07**-**11**

голоса оканчивается на:

**2019**-**09**-**05**

РЕЦИПИЕНТОВ этого проекта предлагается представить, с их комментариями , УВЕДОМЛЕНИЕ О ЛЮБЫХ СООТВЕТСТВУЮЩИХ ПАТЕНТНЫХ ПРАВАХ, О КОТОРЫХ ОНИ ЗНАЮТ, И ПРЕДОСТАВЛЕНИЕ ДОКУМЕНТАЦИИ.

ДОПОЛНИТЕЛЬНО ИХ ОЦЕНКА ПРИЕМЛЕМЫХ ДЛЯ ПРОМЫШЛЕННЫХ, ТЕХНОЛОГИЧЕСКИХ, КОММЕРЧЕСКИХ И ПОЛЬЗОВАТЕЛЬСКИХ ЦЕЛЕЙ, ПРОЕКТЫ МЕЖДУНАРОДНЫХ СТАНДАРТОВ МОГУТ ПРИНИМАТЬСЯ В СЛУЧАЕ ИХ ПОТЕНЦИАЛА СТАНОВИТЬСЯ СТАНДАРТАМИ, КОТОРЫЕ ОТНОСЯТСЯ.

**Информационные технологии - Методы безопасности - Контекст аутентификации для биометрии Информационные технологии - Методы безопасности - Контекст биометрической**

*аутентификации*

Ссылочный номер

ISO / IEC FDIS 24761: 2019 (E)

© ISO / IEC 2019

**ISO / IEC FDIS 24761: 2019 ( E)**

**ДОКУМЕНТ, ЗАЩИЩЕННЫЙ АВТОРСКИМ ПРАВОМ**

© ISO / IEC 2019

Все права защищены. Если иное не указано или не требуется в контексте его реализации, никакая часть данной публикации не может быть воспроизведена или использована иным образом в любой форме или любыми средствами, электронными или механическими, включая фотокопирование или размещение в Интернете или интранете, без предварительного письменное разрешение. Разрешение можно запросить либо в ISO по указанному ниже адресу, либо в органе-члене ISO в стране отправителя запроса.

Бюро авторских прав ISO

CP 401 • Гл. de Blandonnet 8

CH-1214 Vernier, Geneva

Телефон: +41 22 749 01 11

Факс: +41 22 749 09 47

Электронная почта: copyright@iso.org

Веб-сайт: www.iso.org

Опубликовано в Швейцарии

ii © ISO / IEC 2019 - Все права защищены

**ISO / IEC FDIS 24761: 2019 (E)**

**Содержание** Стр.

**Предисловие**................................... .................................................. .................................................. .................................................. ...............................................**iv Введение**. .................................................. .................................................. .................................................. .................................................. .........................**v 1 Область применения**...................... .................................................. .................................................. .................................................. .................................................. ...**1 2 Нормативные ссылки**................ .................................................. .................................................. .................................................. ................**1 3 Термины и определения**............................. .................................................. .................................................. .................................................. ..**1 4 Условные обозначения и сокращения**.......................................... .................................................. .................................................. .............**5**

**5 Модель и структура ACBio** .............................. .................................................. .................................................. ..........................**6** 5.1 Биометрическая модель процесса регистрации и проверки и блок биометрической обработки............ 6 5.2 Роль BPU и класс биометрических возможностей.......................................... .................................................. ....... ......................... 8

5.2.1 Обзор.................... .................................................. .................................................. .................................................. ....... 8 5.2.2 Роль BPU..................................... .................................................. .................................................. .......................................... 9 5.2.3 Класс биометрических возможностей . .................................................. .................................................. ................................12

5.3 Структура использования ACBio ........... .................................................. .................................................. .....................................17 5.3.1 Общие сведения........ .................................................. .................................................. .................................................. .....................17 5.3.2 Подготовка в производстве ction процесс................................................ .................................................. ....18 5.3.3 Подготовка к зачислению на предмет.................................... ................................................20 5,3 .4 Создание экземпляра ACBio в процессе биометрической верификации .....................................21 5.3 .5 Подтверждение процесса биометрической верификации с помощью экземпляров ACBio..................................23

**6 Экземпляр ACBio** .. .................................................. .................................................. .................................................. .............................................**23** 6.1 Общие.. .................................................. .................................................. .................................................. ................................................23 6,2 Информационный блок БПУ............................................... ............ .................................................. .................................................. ...25 6.3 Блок биометрического процесса.......................................... .................................................. .................................................. .................26 6.4 Информация о сертификате BRT ............................ .................................................. .................................................. ......................27

**7 Определение компонентов в BPUInformationBlock**..................... .................................................. .............................**28** 7.1 Сертификат БПУ................. .................................................. .................................................. .................................................. ...............28 7.2 BPUReportInformation................................ .................................................. ................................................. ..............................29

7.2.1 Общие сведения............... .................................................. .................................................. .................................................. ..............29 7.2.2 Отчет о функциях BPU............................... .................................................. .................................................. ................30 7.2.3 Отчет BPUSecurityReport............................. .................................................. .................................................. ....................36

**8 Свидетельство БРТ**.......................... .................................................. .................................................. .................................................. ......................**38** 8.1 Общие сведения......................... .................................................. .................................................. .................................................. .......... ...............38 8.2 BRTCContentInformation................................ .................................................. .................................................. .......................39 8.3 Значения владельца формата и типа формата................... .................................................. .................................................. ..41

**Приложение A** (обязательное) **Модуль ASN.1 для ACBio**.................................... .................................................. ..................................................**42 Приложение B** (справочное) **Примеры реализации**.......................................... .................................................. ..................................**50 Библиография**.............. .................................................. .................................................. .................................................. .................................................. .......**75**

© ISO / IEC 2019 - Все права защищены. ved iii

**ISO / IEC FDIS 24761: 2019 (E)**

**Предисловие**

ISO (Международная организация по стандартизации) и IEC (Международная электротехническая комиссия) образуют специализированную систему всемирной стандартизации. Национальные органы, являющиеся членами ISO или IEC, участвуют в разработке международных стандартов через технические комитеты, созданные соответствующей организацией для работы в определенных областях технической деятельности. Технические комитеты ISO и IEC сотрудничают в областях, представляющих взаимный интерес. Другие международные организации, правительственные и неправительственные, связанные с ISO и IEC, также принимают участие в работе.

Процедуры, использованные для разработки этого документа, и процедуры, предназначенные для его дальнейшего обслуживания, описаны в Директивах ISO / IEC, Часть 1. В частности, следует отметить различные критерии утверждения, необходимые для различных типов документов. Этот документ был составлен в соответствии с редакционными правилами Директив ISO / IEC, Часть 2 (см. Www.iso.org/directives).

Обращается внимание на возможность того, что некоторые элементы этого документа могут быть предметом патентных прав. ИСО и МЭК не несут ответственности за идентификацию каких-либо или всех таких патентных прав. Подробная информация о любых патентных правах, выявленных во время разработки документа, будет во Введении и / или в списке полученных патентных деклараций ISO (см. Www.iso.org/patents) или в списке полученных патентных деклараций МЭК (см. Http: //patents.iec.ch).

Любое торговое наименование, используемое в этом документе, является информацией, предоставленной для удобства пользователей, и не означает одобрения.

Для объяснения добровольного характера стандартов, значения конкретных терминов и выражений ИСО, связанных с оценкой соответствия, а также информации о соблюдении ИСО принципов Всемирной торговой организации (ВТО) в Технических барьерах в торговле (ТБТ) см. Www. .iso .org / iso / foreword.html.

Этот документ был подготовлен Объединенным техническим комитетом ISO / IEC JTC 1, *Информационные технологии*, Подкомитетом SC 27, *Информационная безопасность, кибербезопасность и защита конфиденциальности*.

Это второе издание отменяет и заменяет первое издание (ISO / IEC 24761: 2009), которое было технически пересмотрено. Он также включает Техническое исправление ISO / IEC 24761: 2009 / Cor.1: 2013. Основные изменения по сравнению с предыдущим изданием заключаются в следующем:

- расширение типов данных, которое отражает прогресс в биометрических технологиях для защиты биометрических данных, таких как возобновляемые биометрические данные и другие,

- введение новой модели биометрических возможностей, которая делает валидацию ACBio экземпляры проще, и

- изменения в модуле ASN.1 в результате вышеуказанных изменений.

Любые отзывы или вопросы по этому документу следует направлять в национальный орган пользователя по стандартизации. Полный список этих органов можно найти на сайте www.iso.org/members.html.

iv © ISO / IEC 2019 - Все права защищены

**ISO / IEC FDIS 24761: 2019 (E)**

**Введение**

Процесс биометрической проверки, выполняемый на удаленном сайте, подвержен множеству рисков, например, ложным справочным данным, поддельным захваченным биометрическим данным и ненадежным биометрическим данным. продукты и т. д. Как валидатор может проверить, заслуживает ли доверия процесс биометрической проверки, выполняемый на удаленном сайте? Этот документ дает механизм, позволяющий справиться с этой проблемой.

В целом надежность результата процесса биометрической проверки зависит как от безопасности выполняемого процесса, так и от функциональных характеристик используемых биометрических продуктов. Если используются продукты с лучшими функциональными характеристиками, результат будет более надежным. Если продукты небезопасны или процесс был выполнен в небезопасной среде, результат не будет надежным.

В среде Интернета валидатор процесса биометрической проверки обычно не знает напрямую об используемых биометрических продуктах или о процессе (ах), выполняемом на удаленном сайте. Контекст аутентификации для биометрии (ACBio) обеспечивает решение вышеуказанной проблемы и снижает риски безопасности биометрической аутентификации, отправляя информацию об используемых продуктах и ​​процессах, выполняемых на удаленном сайте, валидатору, если биометрическая обработка завершилась успешно.

ACBio определяет форматы данных для доказательных данных, генерируемых блоками биометрической обработки (BPU), такими как датчик, смарт-карта или устройство сравнения, которые переносятся в структурах данных, называемых экземплярами ACBio. ACBio определяет механизм доверия и гарантии, основанный на технологии цифровой подписи, для предоставления гарантированной информации о BPU и его выполнении биометрических процессов регистрации и проверки, где гарантированная информация о BPU предоставляется в виде отчета BPU, выпущенного поставщиком BPU. Это основано на технологии инфраструктуры открытых ключей (PKI) и PKIX (см. ISO / IEC 9594-8 и RFC 3852). Экземпляр ACBio содержит информацию о блоках биометрической обработки (BPU), биометрической справке и результатах биометрической проверки, которые вместе характеризуют транзакцию биометрической проверки. Гарантия информации в экземпляре ACBio обеспечивается цифровыми сертификатами, связанными с соответствующими элементами информации. Эти сертификаты выдаются доверенными центрами сертификации в процессе регистрации, которые собирают свидетельства о блоках BPU и их возможностях проверки, а также биометрическую ссылку и привязку к известному субъекту. Сертификаты служат двум целям. Во-первых, чтобы обеспечить уверенность в подлинности источника биометрической транзакции (BPU) и биометрической ссылки, а во-вторых, чтобы гарантировать результат биометрической проверки, содержащийся в транзакции. Когда все экземпляры ACBio отправлены валидатору, он может проверять целостность данных, передаваемых между блоками BPU. Информация об обнаружении презентационной атаки в реальном времени не предоставляется в этом документе. Однако отчет BPU может содержать информацию о гарантии механизма PAD. ACBio признает, что требования конфиденциальности, касающиеся хранения биометрических данных, должны соответствовать местным законам и законодательству о конфиденциальности данных. ACBio гарантирует, что валидатор может подтвердить результат процесса биометрической проверки без получения личных данных, таких как биометрический образец, полученный от заявителя, или биометрический эталон, используемый для сравнения.

Экземпляр ACBio - это отчет, закодированный с использованием основных правил кодирования (BER) ASN.1 [см. ISO / IEC 8824 (все части)], обычно поддерживаемых поставщиками наборов криптографических инструментов. Синтаксис не зависит от алгоритма и поддерживает обеспечение целостности данных и аутентификацию источника данных. Что касается криптографических алгоритмов, рекомендуются те, которые указаны в ISO / IEC JTC 1 / SC 27, хотя может использоваться любой алгоритм, подходящий для использования данным сообществом.

Этот документ отражает прогресс в биометрических технологиях для защиты биометрических данных, таких как возобновляемые биометрические данные, указанные в ISO / IEC 24745 и других, путем расширения вариации типов биометрических данных, передаваемых между биометрическими подпроцессами, и, кроме того, устанавливает новую модель биометрических возможностей, которая делает проверка экземпляров ACBio проще. Это привело к некоторым изменениям в модуле ASN.1, которые приведут к межоперационной несовместимости между системами, реализующими разные версии модулей ASN.1.

© ISO / IEC 2019 - Все права защищены v

**ОКОНЧАТЕЛЬНЫЙ ПРОЕКТ МЕЖДУНАРОДНОГО СТАНДАРТА ISO / IEC FDIS 24761: 2019 (E)**

**Информационные технологии - Методы безопасности - Контекст аутентификации для биометрии**

**1 Область применения В**

этом документе определяется структура и элементы данных контекста аутентификации для биометрии (ACBio), который используется для проверки достоверности результата биометрической регистрации и процесса проверки, выполняемого на удаленном сайте. Этот документ позволяет любому экземпляру ACBio сопровождать любые биометрические процессы, связанные с регистрацией и проверкой. Спецификация ACBio применима не только к регистрации и верификации одномодальных биометрических данных, но и к мультимодальному слиянию. Информация об обнаружении презентационной атаки в реальном времени в этом документе не представлена. В отчете BPU может содержаться только информация о гарантии механизма обнаружения атак представления (PAD).

Биометрическая идентификация выходит за рамки этого документа.

Этот документ определяет криптографический синтаксис экземпляра ACBio. Криптографический синтаксис экземпляра ACBio определяется в этом документе с применением структуры данных, указанной в схеме синтаксиса криптографических сообщений (CMS), конкретные значения которой могут быть представлены с использованием компактного двоичного кодирования. Этот документ не определяет протоколы, которые будут использоваться между объектами, такими как BPU, заявитель и валидатор. Его забота полностью связана с содержанием и кодированием экземпляров ACBio для различных операций обработки.

**2 Нормативные ссылки**

Следующие ниже документы упоминаются в тексте таким образом, что часть или все их содержание составляет требования этого документа. Для датированных ссылок применимо только указанное издание. Для недатированных ссылок применяется последнее издание ссылочного документа (включая любые поправки).

ИСО / МЭК 2382-37, *Информационные технологии - Словарь - Часть 37: Биометрия*

ИСО / МЭК 9594-2,Взаимодействие *Информационные технологии -открытых систем - Справочник: Модели*

ИСО / МЭК 9594-8,Взаимодействие *Информационные технологии -открытых систем - Справочник : Структура сертификатов открытых ключей и атрибутов*

ИСО / МЭК 24745, *Информационные технологии. Методы безопасности. Защита биометрической информации.*

**3 Термины и определения.**

В данном документе используются термины и определения, приведенные в ИСО / МЭК 2382-37, ИСО / МЭК 9594. -8, ISO / IEC 24745 и нижеследующее.

ИСО и МЭК поддерживают терминологические базы данных для использования в стандартизации по следующим адресам: - Интернет-платформа ISO: доступна по адресу https://www.iso.org/obp

- IEC Electropedia: доступно на http://www.electropedia.org/

ПРИМЕЧАНИЕ. Терминология в этом документе была обновлена, где это возможно, в соответствии с ISO / IEC 2382-37: 2017. Однако для обеспечения максимальной совместимости с терминологией и названиями типов в модуле ASN.1 в первом издании этого документа некоторые термины были перенесены из предыдущего издания.

© ISO / IEC 2019 - Все права защищены **1**

**ISO / IEC FDIS 24761: 2019 (E)**

**3.1**

**Отчет об экземпляре ACBio,BPU,**

созданныйсовместимым с этим документом, чтобы показать достоверность результата выполнения одного или нескольких подпроцессов, выполняемых в BPU

**3.2**

**класс биометрических возможностей класс**

конфигураций для того, как биометрическая регистрация / верификация может быть разделена на одну или несколько ролей BPU

Примечание 1 к записи: В этом документе определены четыре класса биометрических возможностей:

- класс «все-в-одном» (биометрические возможности);

- класс датчика-компаратора (биометрические возможности);

- класс хранения и прочее (биометрические возможности); и

- класс "только сенсор" (биометрические возможности).

Примечание 2 к записи: Чтобы выразить каждый класс биометрических возможностей, «биометрические возможности» обычно опускаются.

**3.3**

**блок биометрической обработки**

**BPU**

доверенная реализация набора биометрических подпроцессов, реализованных в одном физическом блоке

Примечание 1 к записи: BPU обычно содержит биометрические подпроцессы, которые являются последовательными в потоке процесса для биометрической проверки.

Примечание 2 к записи: Требования к приложению / услуге обычно требуют, чтобы подпроцессы BPU соответствовали единому уровню гарантии безопасности. В ACBio гарантия достигается посредством процесса оценки BPU, который аутентифицируется с помощью сертификата X.509, встроенного в экземпляр ACBio.

**3.4**

**биометрический модуль обработкисертификат**

**сертификатГПП**

сертификатаX.509который выдается ГПП по сертификации

**3,5**

**биометрический блок обработки сертификации**

**ГПП сертификации**

X.509сертификациикакие вопросы BPU сертификаты

**3.6**

**биометрический модуль обработкиотчета функция**

**отчет ФункцияГПП**

отчетовна функция BPU, сгенерированная производителем блокаBPU

**3.7**

**биометрической обработкиIO Index**

**BPU IO Index**

Целочисленное число, уникально присвоенное каждому потоку биометрических данных между BPU субъектом, который использует функцию BPU (например, программное обеспечение) и используется валидатор для восстановления потока данных между BPUотчет

**3.8**

**биометрического блока обработки Отчет**

**BPU отчет**

по BPU, который состоит из отчета о функциях BPU и отчета о безопасности BPU **2** © ISO / IEC 2019 - Все права защищены

**ISO / IEC FDIS 24761: 2019 (E)**

**3.9**

**биометрической обработки Отчет о безопасности**

**BPU**

отчет о безопасности устройстваОтчет о безопасности BPU, который содержит гарантию информация о безопасности BPU

Примечание 1 к записи: Гарантийная информация о механизме PAD, если она присутствует в отчете BPU, должна быть включена в отчет о безопасности BPU.

**3.10**

**биометрическая ссылка:**

один или несколько сохраненных биометрических образцов, биометрических шаблонов или биометрических моделей, приписываемых субъекту биометрических данных и используемых в качестве объекта биометрического сравнения.

ПРИМЕР Изображение лица, сохраненное в цифровом виде в паспорте, шаблон контрольных точек отпечатка пальца на национальной идентификационной карте или гауссовской модели смеси для распознавания говорящего в базе данных.

Примечание 1 к записи: Биометрическая ссылка может быть создана с неявным или явным использованием вспомогательных данных, таких как универсальные фоновые модели.

Примечание 2 к записи: Обозначение субъекта / объекта в *сравнении*может быть произвольным. В некоторых сравнениях биометрический эталон может использоваться в качестве объекта сравнения с другими биометрическими эталонами или поступающими образцами и вводиться в алгоритм биометрического сравнения. Например, при повторной проверке регистрации биометрическая ссылка будет использоваться в качестве объекта для сравнения со всеми другими биометрическими ссылками в базе данных.

Примечание 3 к записи: Термин «шаблон биометрической ссылки» также используется в этом документе для частичного обозначения биометрической ссылки. См. ПРИМЕЧАНИЕ в начале раздела 3.

[ИСТОЧНИК: ISO / IEC 2382-37: 2017, 3.3.16, изменено - добавлено примечание 3 к записи.]

**3.11**

**сертификат шаблона биометрического эталона Сертификат сертификата**

**BRT,**

который выдается для биометрического эталона сертификационной организацией BRT и позволяет валидатор для определения подлинности биометрического эталона

**3.12**

**организация пошаблона биометрического эталона Организация по сертификации**

**сертификацииBRT**

Организация, которая выдает сертификаты BRT

**3.13**

**подпроцесс биометрических данных (биометрический**

**подпроцесс):**

часть общего процесса регистрации или проверки биометрических данных, выполняющего определенную функцию

Примечание 1 к записи: Функции подпроцесса биометрических данных являются одной из следующего: сбор данных, промежуточная обработка сигналов, окончательная обработка сигналов, хранение, сравнение и принятие решения.

**3.14**

**Роль BPU**

Комбинация биометрических функций, предоставляемых BPU, комбинация функций которой указана в этом документе

Примечание 1 к записи: На роль BPU можно ссылаться по имени, которое описывает биометрические функции, предоставляемые BPU: все роли BPU, датчик BPU роль, роль BPU компаратора с хранилищем, роль BPU компаратора и роль BPU хранилища.

**3.15**

**захваченный биометрический эталон**

захваченный биометрический образец или комбинация захваченных биометрических образцов, используемых в качестве биометрического эталона © ISO / IEC 2019 - Все права защищены **3**

**ISO / IEC FDIS 24761: 2019 (E)**

**3.16**

**контрольное значение:**

случайное число, предоставленное валидатором, с помощью которого валидатор может проверить, генерируется ли экземпляр ACBio по запросу валидатора или нет.

**3.17**

**выражение объявления**

явное выражение отчета функции BPU, в котором содержится информация о подпроцессах и потоках данных.

**3.18**

**организация регистрации**

организация, которая обрабатывает регистрацию и создает и хранит биометрические ссылки.

**3.19**

**оценка организация**

Организация, которая оценивает функцию BPU или безопасность.

**3.20**

**заключительныйобработкиобработки**

этапсигнала, этапсигнала, непосредственно предшествующий биометрическому сравнению.

Примечание 1 к записи: см. ПРИМЕЧАНИЕ в начале раздела 3.

**3.21**

**промежуточный биометрический эталон**

Промежуточный биометрический образец или комбинация промежуточных биометрических образцов, используемых в качестве биометрического эталона

Примечание 1 к записи: Промежуточный биометрический эталон обрабатывается посредством окончательной биометрической обработки и затем сравнивается с биометрическим образцом.

**3.22**

**обработка промежуточного сигнала:**

любая манипуляция с биометрическим образцом, небиометрических характеристик

создающаяПримечание 1 к записи: В ИСО / МЭК 2382-37 «промежуточная обработка биометрического образца» (ИСО / МЭК 2382-37: 2017, 3.5.9) - определяется вместо «промежуточной обработки сигналов». См. ПРИМЕЧАНИЕ в начале раздела 3.

Примечание 2 к записи: Термин «биометрическая характеристика» определяется как числа или метки, извлеченные из биометрических образцов и используемые для сравнения в ISO / IEC 2382-37: 2017, 3.3.11.

**3.23**

**биометрическое сравнение на карте**

**OCBC,**

выполняющее сравнение и принятие решения на карте IC, где биометрическая ссылка сохраняется на карте для повышения безопасности и конфиденциальности

**3.24**

**обработанный биометрический эталон**

обработанный биометрический образец или комбинация обработанных биометрических образцов, используемых в качестве биометрического эталона.

**3.25**

**обработанный биометрический образец**

биометрический образец или набор биометрических характеристик, входящие в алгоритм для биометрического сравнения с биометрическим эталоном (ами)

Примечание 1 к записи: ISO / IEC 2382-37, термин «биометрический датчик» (ISO / IEC 2382-37: 2017, 3.3.14) определяется вместо «обработанного биометрического образца». См. ПРИМЕЧАНИЕ в начале раздела 3.

**4** © ISO / IEC 2019 - Все права защищены

**ISO / IEC FDIS 24761: 2019 (E)**

**3.26**

**возобновляемый биометрический образец**

Биометрический образец, который имеет свойство преобразования или процесса для создания нескольких независимых преобразованных биометрических данных, полученных из одного или нескольких биометрических образцов полученные от одного и того же субъекта данных и которые могут использоваться для распознавания человека, не раскрывая информацию о генеративных биометрических данных

Примечание 1 к записи: Возможность возобновления определяется в ISO / IEC 24745: 2011 как: свойство преобразования или процесса для создания нескольких , независимые преобразованные биометрические ссылки, полученные из одного или нескольких биометрических образцов, полученных от одного и того же субъекта данных, которые могут использоваться для распознавания человека, не раскрывая при этом информацию об исходной ссылке. Это определение применимо только к биометрической справке. Определение в этом документе немного изменено по сравнению с определением в ISO / IEC 24745: 2011, так что его можно применять как к биометрическому образцу, так и к биометрическому эталону, поскольку биометрический образец в возобновляемых биометрических данных должен быть преобразован таким образом, чтобы его можно было сравнить с возобновляемым образцом. биометрическая справка.

**3.27**

**выражение роли:**

неявное выражение отчета о функции BPU для BPU, имеющего роль

**BPU. 3.28**

**индекс подпроцесса,**

целое число, уникально назначенное каждому подпроцессу в BPU производителем BPU.

**3.29**

**индекс ввода-вывода подпроцесса.**

Уникальное целое число, назначенное каждому потоку данных между подпроцессами в BPU. чтобы валидатор мог реконструировать поток данных между подпроцессами в объектеBPU

**3.30**

**валидатора**

<биометрической верификации>, который принимает решение о том, является ли результат процесса биометрической верификации приемлемым или нет, на основе политики, используя одно или несколько сравнений решения и, возможно, другая информация, поддерживаемая экземплярами ACBio

**4 Символы и сокращенные термины**

Контекст аутентификации ACBio для биометрии

ASN.1 Абстрактная синтаксическая нотация Один, как определено в базовых правилах кодирования BER серии ISO / IEC 8824 (ASN.1)

BIR Запись биометрической информации

Биометрический эталонный шаблон BRT

Структура общих форматов обмена биометрическими данными CBEFF, как определено в ISO / IEC 19785-1 CMS Cryp Синтаксис графического сообщения, как определено в RFC 3852 и RFC 5911 FAR Скорость ложного приемаСкорость

FRRложного отклонения

Обнаружение атак представления PAD

© ISO / IEC 2019 - Все права защищены **5**

**ISO / IEC FDIS 24761: 2019 (E)включено**

инфраструктуры открытых ключей PKI

Хранение STOCCard

URI Uniform Resource Identifier

**5 Model and framework of ACBio**

**5.1 Biometric enrolment and verification process model and Biometric Processing Unit**

This document defines the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric enrolment and verification process executed at a remote site. An ACBio instance shall be accompanied witha biometric data output processesed by a BPU for biometric enrolment and verification.

ACBio's design is based on the following biometric subprocesses:

a) data capture: this subprocess captures biometric information from a claimant and converts it to a captured biometric sample. The captured biometric sample is transmitted to the intermediate signal processing subprocess for further processing;

b) intermediate signal processing: this subprocess receives a captured biometric sample and transforms it into an intermediate biometric sample. The intermediate biometric sample is transmitted to the final signal processing subprocess for further processing;

c) final signal processing: this subprocess receives an intermediate biometric sample and transforms it into a processed biometric sample. The processed biometric sample through the final signal processing is transmitted either to the comparison subprocess (for verification) or to the storage subprocess (for enrolment as the biometric reference). There is a variation of the output of the final signal processing, a renewable biometric sample;

d) storage: this subprocess stores one of three types of biometric reference; captured biometric reference (Key item 1 in Figure 1 and Figure 2), intermediate biometric reference (Key item 2 in Figure 1 and Figure 2), or processed biometric reference (Key item 3 in Figure 1 and Figure 2). One of the three types of biometric reference will be compared with a biometric sample for verification. As in c), there is a variation for processed biometric reference, renewable biometric reference;

e) comparison: this subprocess receives a biometric sample, which is acquired originally from a claimant, and can be further processed or not, and a biometric reference. This subprocess compares the biometric sample and the processed biometric reference, and calculates the similarity, which is called a comparison score. The comparison score is transmitted to the decision subprocess.

NOTE The processing of comparing a renewable biometric sample with a renewable biometric reference is different from that of comparing a processed biometric sample with a processed biometric reference. However, they are not distinguished in this document. They are distinguished only by the data input into the subprocess. If a BPU A executes the comparision subprocess and another BPU B executes the final signal processing subprocess or the storage subprocess, the BPU B does not know whether the BPU A can process the data submitted from the BPU B. In the ACBio framework, only the application system knows the compatibility of the data exchanged between the BPUs through the negotiation between them in advance. See B.1.2.5 for details.

f) decision: this subprocess receives a comparison score from the comparison subprocess, evaluates the score under rules determined by the security policy in use, decides the validity of the claimant's identity, and outputs the comparison decision, match or non-match, which is sent to the validator.

Besides the above six subprocesses biometric products generally have PAD mechanism. Figure 1 shows a general model of biometric verification including PAD mechanism. However, PAD is not discussed further in this document because it is dealt with only in the assurance information in the BPU report in this document. For more details of PAD, see ISO/IEC 30107-1.

**6** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**Figure 1 — General model of biometric verification including PAD mechanism**

Figure 2 shows three cases of biometric enrolment process where the storage subprocess stores: 1) captured biometric samples,

2) intermediate biometric samples, and

3) processed biometric samples.

**Key**

1 storage subprocess which stores captured biometric samples

2 storage subprocess which stores intermediate biometric samples

3 storage subprocess which stores processed biometric samples

a Possible untrusted network.

**Figure 2 — Biometric enrolment process model**

The small black disks with Key a in Figure 2 mean that an untrusted network may intervene at the points, ie, a captured biometric sample, an intermediate biometric sample, and a processed biometric sample can be transferred through untrusted networks.

© ISO/IEC 2019 – All rights reserved **7**

**ISO/IEC FDIS 24761:2019(E)**

Figure 3 shows three cases of biometric verification process model where the storage subprocess stores a captured biometric reference, an intermediate biometric reference, and a processed biometric reference.

**Key**

1 storage subprocess which stores captured biometric samples

2 storage subprocess which stores intermediate biometric samples

3 storage subprocess which stores processed biometric samples

a Possible untrusted network.

**Figure 3 — Biometric verification process model**

The small black disks with Key a in Figure 3 mean the same as in Figure 2.

This document considers only biometric data flows in Figure 3 and does not consider any other non biometric data flows such as auxiliary data in renewable biometrics.

**5.2 BPU role and biometric capability class**

**5.2.1 Overview**

When implementing biometric systems, the various biometric subprocesses that compose the system are often grouped together into components called biometric processing units (BPUs). The groupings reflect the physical and architectural details and the grouping of biometric subprocesses in the system implementation. Commonly used combinations of BPU functionalities are described and defined as BPU roles in this document. In principle, a BPU can include any grouping of biometric subprocesses but, in practice, BPUs commonly comprise biometric subprocesses that are sequential in the overall process flow for a biometric verification. BPU roles that equate to commonly used combinations of BPU functionality are defined in 5.2.2.

**8** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

NOTE Only commonly used combinations of BPU functionalities are expressed as BPU role, ie there are BPUs whose functionalities cannot be expressed as a BPU role. For example, a BPU does not have an expression of a BPU role if it consists only of the decision subprocess. In such cases, declaration expression is used for the BPU function report. In policy-based authorization where authorization is done based on defined policies which include those on authentication, a service consuming the result of authentication can have a preference for the configuration for biometric verification. Biometric capability classes are specified for this purpose. For the benefits of BPU roles and biometric capability classes, see NOTE in 7.2.2.3, B.1.2.5, and B.1.3.5. See also B.3.

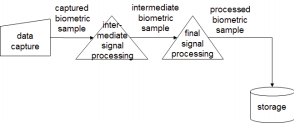
**5.2.2 BPU role**

**5.2.2.1 General**

Biometric products and systems are often implemented using one or more BPUs. The grouping of subprocesses into BPUs typically matches the physical structure of the product or system, eg a physical sensor unit may contain the sensor itself plus signal processing elements. The typical grouping of biometric subprocesses into a BPU defines the BPU role. The BPU roles described in this document reflect subprocess groupings that are commonly found in biometric products and systems. Although the concept of BPUs and BPU roles can be applied to multimodal and multi-biometric systems, the concept of BPU roles is not extended to multimodal and multi-biometric systems in this document.

**5.2.2.2 BPU role for biometric enrolment**

The all-BPU-enrolment role is a BPU role which contains all the subprocesses used in biometric enrolment, that is data capture, intermediate signal processing, final signal processing, and storage subprocesses. The all-BPU-enrolment role is presented in Figure 4. There is a variation where processed biometric sample is replaced with renewable biometric sample.

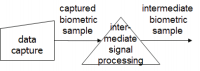


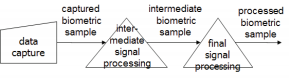
**Figure 4 — All-BPU-enrolment role**

The sensor BPU role is a BPU role which contains the data capture subprocess. It may contain the final signal processing subprocess and the intermediate signal processing subprocess. If it contains the final signal processing subprocess, then it shall also contain the intermediate signal processing subprocess. There are three patterns of sensor BPU role which are shown in Figure 5. There is a variation where processed biometric sample is replaced with renewable biometric sample.

© ISO/IEC 2019 – All rights reserved **9**

**ISO/IEC FDIS 24761:2019(E)**

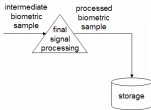
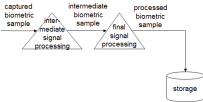
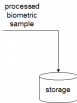
****

****

**Figure 5 — Patterns of sensor BPU role**

The storage-and-others-if-any BPU role is a BPU role which shall contain the storage subprocess but shall not contain the capture subprocess. It may contain the intermediate signal processing and the final signal processing subprocess. If it contains the intermediate signal processing subprocess, then it shall also contain the final signal processing subprocess. There are three patterns of storage-and

others-if-any BPU role which are depicted in Figure 6. There are variations where processed biometric sample is replaced with renewable biometric sample.



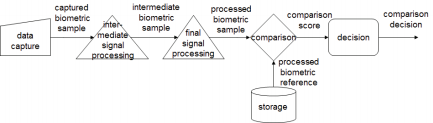
**Figure 6 — Patterns of storage-and-others-if-any BPU role**

**10** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**5.2.2.3 BPU role for biometric verification**

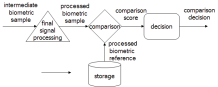
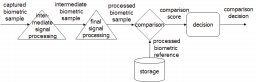
The all-BPU-verification role is a BPU role which contains all the subprocesses used in biometric verification. The all-BPU–verification role is presented in Figure 7. There are variations where processed biometric sample is replaced with renewable biometric sample.



**Figure 7 — All-BPU-verification role**

The sensor BPU role, which is defined in 5.2.2.2, is used also in biometric verification.

The comparator-with-storage BPU role is a BPU role which shall contain the storage, comparison, and decision subprocesses. But it shall not contain the capture subprocess. It may contain the intermediate signal processing and the final signal processing subprocess. If it contains the intermediate signal processing subprocess, then it shall also contain the final signal processing subprocess. There are three patterns of comparator-with-storage BPU role which are depicted in Figure 8. There are variations where processed biometric sample is replaced with renewable biometric sample.



**Figure 8 — Patterns of comparator-with-storage BPU role**

The comparator BPU role is a BPU role which shall contain the comparison and decision subprocessess but shall not contain the storage subprocess. It may contain the data capture, intermediate signal processing, and final signal processing subprocess. If it contains a subprocess of the three, then it shall also contain the latter subprocess(es). There are four patterns of comparator BPU role which are shown in Figure 9. There are variations where processed biometric sample is replaced with renewable biometric sample.

© ISO/IEC 2019 – All rights reserved **11**

**ISO/IEC FDIS 24761:2019(E)**

**Figure 9 — Patterns of comparator BPU role**

The storage BPU role is a BPU role which consists only of the storage subprocess. There is only one pattern for the storage BPU role as shown in Figure 10. There is a variation where processed the biometric sample is replaced with renewable biometric sample.

**Figure 10 — Storage BPU role**

**5.2.3 Biometric capability class**

**5.2.3.1 General**

In this document, BPU roles can be combined into a higher order structure representing the functional capability of the combination. This construct is named biometric capability class. The biometric capability classes defined in this document are described in subclauses 5.2.3.2 and 5.2.3.3.

**5.2.3.2 Biometric capability classes for biometric enrolment**

There are three classes. In the first and the second classes, all the subprocesses are executed at the client side while the biometric reference is stored at the server side in the last class. The all-in-one enrolment class is a biometric capability class which consists of an all BPU enrolment role.

Combination of sensor BPU role and sensor-and-others-if-any BPU role makes sensor-and-storage class. There are three cases of sensor-and-storage class as depicted in Figure 11. There are variations where processed biometric sample is replaced with renewable biometric sample.

**12** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

****

****

****

**Figure 11 — Three cases of sensor-and-storage class**

There are three cases for sensor-only-enrolment class as depicted in Figure 12 where the shaded parts are executed at the server side. There are variations where processed biometric sample is replaced with renewable biometric sample.

© ISO/IEC 2019 – All rights reserved **13**

**ISO/IEC FDIS 24761:2019(E)**

****

****

****

**Figure 12 — Three cases of sensor-only-enrolment class**

**5.2.3.3 Biometric capability classes for biometric verification**

There are four classes. In the first three classes, all the subprocesses are executed at the client side while the biometric comparison subprocesses is executed at the server side in the last class. The all-in one verification class is a biometric capability class which consists of an all BPU verification role.

A combination of sensor BPU role and comparator-with-storage BPU role makes sensor-and-comparator class. There are three cases of sensor-and-comparator class as depicted in Figure 13. There are variations where processed biometric sample is replaced with renewable biometric sample.

**14** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

****

****

****

**Figure 13 — Three cases of sensor-and-comparator class**

A combination of storage BPU role and comparator BPU role makes storage-and-others class. There are four cases of storage-and-others class as shown in Figure 14. In three cases, the sensor BPU role also plays a role in the storage-and-others class. There are variations where processed the biometric sample is replaced with a renewable biometric sample.

© ISO/IEC 2019 – All rights reserved **15**

**ISO/IEC FDIS 24761:2019(E)**

****

****

****

**Figure 14 — Four cases of storage-and-others class**

There are three cases for sensor-only-verification class as shown in Figure 15 where the shaded parts are executed at the server side. There are variations where the processed biometric sample is replaced with a renewable biometric sample.

**16** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**Figure 15 — Three cases of sensor-only- verification class**

NOTE The scope of this document is restricted to biometric enrolment and verification. However, the technology can be applied to biometric identification where the configuration at the client side is one of the configurations in Figure 15. The processing at the server side of biometric identification can validate the processing at the client side with the ACBio instance generated at the client side.

**5.3 Framework for use of ACBio**

**5.3.1 General**

The technology in this document is designed to be used for remote biometric authentication for policy based authorization, for example, in on-line bankings/shoppings (see B.3). In such cases, the provided service can change depending on how the authentication result can be trusted, that is the policy on authorization of the service provider. The policy may contain the configuration of biometric enrolment/ verification process. In such a circumstance, the configuration is generally negotiated before the enrolment/authtentication itself, ie, in the negotiation phase of enrolment/authentication, and also

© ISO/IEC 2019 – All rights reserved **17**

**ISO/IEC FDIS 24761:2019(E)**

checked at the enrolment/authentication phase whether the configuration satisfies the condition which is already negotiated at the negotiation phase. The biometric capability classes are defined so that they are used in the enrolment/authentication phases. See B.1.2.5 and B.1.3.5 for examples of how biometric capability class is used.

ACBio validation information is provided by ACBio instances which are data structures that can provide assurance concerning the recognition performance and security capabilities of the BPU. ACBio instances contain X.509 certificates that authenticate the BPU and assure the information it provides. The X.509 certificates are provisioned through a production process conducted between the BPU manufacturer and the relevant certification authority.

ACBio gives information to the validator of a biometric verification process how it is done. For that to be done, subclauses in 5.3.2 to 5.3.5 give an overview of what shall be done in the production process of BPUs, the enrolment process of the biometric reference, the biometric verification process, and the validation process. The ASN.1 module specified in this document uses the X.509 certificate as public

key certificate but the concept itself is not limited to the X.509 certificate. In subclauses 5.3.2 to 5.3.5, the descriptions are generalized by using the term “public-key certificate” instead of “X.509 certificate”.

**5.3.2 Preparation in the production process**

In the production process, the manufacturer of BPU prepares the BPU report and stores it into the BPU with the public key pair of the BPU and the public-key certificate of the public key. Figure 16 shows what shall be prepared in the production process of BPUs.

**18** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**Key**

1 key generation

2 Issuance of X.509 certificate

3 submission of BPU and related documents

4 evaluation of BPU

5 Issuance of BPU security report

6 generation of BPU report

7 key generation

8 issuance of X.509 certificate

9 storing of BPU report, key pairs, and X.509 certificate in BPU

**Figure 16 — Preparation in the production process**

The manufacturer of a BPU shall generate a public/private key pair (1 in Figure 16) and request the public-key certificate authority to issue a public-key certificate for the public key (2 in Figure 16) in advance. The private key is used to digitally sign the BPU report.

If security evaluation of the BPU is done by an evaluation organization (4 in Figure 16), a BPU security report (see 7.2.3) digitally signed using the private key of the evaluation organization is issued () in Figure 16), which is to be a part of the BPU report.

The manufacturer of the BPU shall generate the BPU report which is digitally signed with the private key of the manufacturer (6 in Figure 16). The BPU report provides trusted information about the BPU to

© ISO/IEC 2019 – All rights reserved **19**

**ISO/IEC FDIS 24761:2019(E)**

the validator when ACBio instance is checked. Next, the manufacturer shall generate a public key pair of the BPU (7 in Figure 16) and have a BPU certificate (see 7.1) issued by a BPU certification authority (8 in Figure 16). The BPU certificate is a public-key certificate of the public key of the BPU. The private key of the BPU is used later to digitally sign ACBio instances generated by the BPU.

The manufacturer should rotate keys to sign different BPU reports to anticipate the impact of any potential leakage of previously used keys, and it is additionally recommended to embed a different private key per product of the BPU, for example.

The BPU report or its referrer, the private key of the BPU, and the BPU certificate shall be stored in the BPU before shipping the product of the BPU. The BPU shall have a function to generate a digital signature for digitally signing ACBio instances using the BPU's private key.

Examples of preparation in the production process are provided in Annex B: B.1.2.2 for the STOC model and B.1.3.2 for the OCBC model.

**5.3.3 Preparation in the subject enrolment process**

In the enrolment process, the enrollee enrols his or her biometric reference, gets the BRT certificate corresponding to the biometric reference, and stores the biometric reference and the BRT certificate into a BPU.

Figure 17 shows what shall be prepared in the enrolment process.

To use biometric verification, an enrollee shall enrol his or her biometric reference in advance under the control of an enrolment organization or without such a control depending on the use case (1 in Figure 17). Then the biometric reference is stored in a BPU with storage subprocess (2 in Figure 17).

To use ACBio for validation of a biometric verification process, a certificate of biometric reference called a BRT certificate (see Clause 8) shall be issued by a BRT certification organization (3 in Figure 17). The BRT certificate is digitally signed using the private key of the BRT certification organization. The BRT certificate or its referrer shall be stored in the BPU where the certified biometric reference is stored. The BRT and its BRT certificate shall be managed in the BPU as a couple.

During the enrolment process, ACBio instances should be generated to validate the reliability of the enrolment process. The validation with these ACBio instances may be done by the BRT certification organization to issue the BRT certificate as well as the validator of the biometric verification process.

NOTE When the ACBio instances are sent to the BRT certificate organization, the BRT certificate is not generated yet. Therefore, any ACBio instance sent to the BRT certificate contains no BRT certificate even if the BPU stores the biometric reference to which the BRT certificate is issued. Examples of preparation in the subject enrolment process are provided in B.1.2.3 for the STOC model and B.1.3.3 for the OCBC model.

**20** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**Key**

1 enrolment of BRT

2 storing of BRT in BPU

3 issuance of BRT certificate

4 storing of BRT certificate in BPU

**Figure 17 — Preparation in the enrolment process**

**5.3.4 ACBio instance generation in the biometric verification process**

ACBio applies the challenge-response mechanism to prevent the success of replay attackes. The validator shall send the challenge to the claimant and the claimant shall make all the BPUs that take a part in the biometric verification set the challenge into the ACBio instances they generate.

Figure 18 outlines the biometric verification process and its validation process when ACBio is used. Figure 18 shows three cases of biometric verification process models where the storage subprocess stores a captured biometric reference, an intermediate biometric reference, and a processed biometric reference.

© ISO/IEC 2019 – All rights reserved **21**

**ISO/IEC FDIS 24761:2019(E)**

a Possible untrusted network.

**Figure 18 — Biometric verification process and its validation**

The small black disk in Figure 18 means that an untrusted network may intervene at the points, ie biometric data in Figure 18 can be transferred through untrusted networks.

In a biometric verification process, each BPU shall pack the BPU certificate information (the BPU certificate itself or its referrer), the BPU report information (the BPU report itself or its referrer) into the data of type ACBioContentInformation (see Clause 6) to show later which subprocess(es) of the biometric verification are executed on which BPU. In addition, the BRT certificate information (the BRT certificate itself or its referrer) is also packed if the storage subprocess is in the BPU and stores the biometric reference used in the biometric verification process. The BRT certificate in an ACBio instance shows which biometric reference is used in the biometric verification. The data of type ACBioContentInformation shall also contain the challenge from the validator, called the control value, and the hash value(s) of the input/output biometric data to/from the BPU, which enables the validator to validate the consistency of the transmission of biometric data between BPUs.

By adding the digital signature to the data of type ACBioContentInformation with the private key of the BPU, the ACBio instance is generated.

Examples of ACBio instance generation are provided in B.1.2.4 for the STOC model and B.1.3.4 for the OCBC model.

**22** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**5.3.5 Validation of biometric verification process with ACBio instances**

In this ACBio framework, the validator receives not only the comparison decision, the result of biometric verification, but also the ACBio instance(s) with which the validator can validate the result of the executed biometric verification.

The validator can validate the authenticity and integrity of ACBio instance by verifying the digital signature with the BPU certificate. This shows also that the BPU has taken a part of the biometric verification process. The validator can obtain the result of security evaluation of the BPU by referring to the BPU report, and the authenticity of the biometric reference used in the biometric verification process by referring to the BRT certificate. The validator can also validate the consistency of the communication between BPUs and between the BPUs in the biometric verification process by checking the hash values in the biometric process blocks. By checking the control value in the ACBio instance(s), the validator can know whether there has been a replay attack or not. With all of these, the validator can decide the level of trust for the result of the executed biometric verification process.

NOTE In the cheking process, two types of indexes are used, one from BPU reports and the other given by the application program which calls BPUs. The integrity of the former is achieved by the digital signature given to BPU reports while that of the latter is achieved by the digital signature of ACBio instances.

If necessary, the validator can connect to relevant organizations such as the BPU certification authority, the evaluation organization, and the BRT certification organization, as shown in Figure 18.

Examples of validation of biometric verification process with ACBio instances are provided in B.1.2.5 for the STOC model and B.1.3.5 for the OCBC model.

**6 ACBio instance**

**6.1 General**

In Clauses 6 to 8, data structures are defined and explained. The definitions are specified in ASN.1 notation, which is in line with ISO/IEC 8824. The whole specification of the data structures is provided as an ASN.1 module in Annex A, which shall be used in a system conforming to this document. Examples of ACBio instances are provided in B.1.2 for the STOC model and B.1.3 for the OCBC model.

An ACBio instance is data of ASN.1 type ACBioInstance as follows:

ACBioInstance ::= SEQUENCE {

contentType CONTENT-TYPE.&id({ContentTypeACBio}),

content CONTENT-TYPE.&Type

({ContentTypeACBio}{@contentType})}

The type ACBioInstance corresponds to the type ContentInfo of CMS. The latter is constrained by an extensible object set while the former is constrained by an object containing only signedDataACBio. The object of class CONTENT-TYPE is defined as follows:

ContentTypeACBio CONTENT-TYPE ::= {signedDataACBio }

signedDataACBio CONTENT-TYPE ::= {

SignedDataACBio

IDENTIFIED BY id-signedDataACBio }

id-signedDataACBio OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) signedDataACBio(1)} © ISO/IEC 2019 – All rights reserved **23**

**ISO/IEC FDIS 24761:2019(E)**

SignedDataACBio is specified as follows:

SignedDataACBio ::= SIGNEDDATA { EncapsulatedContentInfoACBio }

The types SignedDataACBio specified above replaces the CMS types SignedData together with the following definitions:

SIGNEDDATA { EncapsulatedContentInfo } ::= SEQUENCE {

version CMSVersion,

digestAlgorithms SET OF DigestAlgorithmIdentifier,

encapContentInfo EncapsulatedContentInfo,

certificates [0] IMPLICIT CertificateSet OPTIONAL,

crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,

signerInfos SignerInfos}

The following types appeared in the above definition of SIGNEDDATA are imported from RFC 3852/5911: CMSVersion, DigestAlgorithmIdentifier, SignerInfos. version shall take the value as specified in RFC 3852/5911.

The type EncapsulatedContentInfo is a parameter in the above definition and is not imported from CMS. In the definition of the type SignedDataACBio, the following type replaces EncapsulatedContentInfo.

EncapsulatedContentInfoACBio ::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypeACBioContentInfo}), eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypeACBioContentInfo}{@eContentType}))}

ContentTypeACBioContentInfo CONTENT-TYPE ::= {acbioContentInformation}

As in the above definition, the type EncapsulatedContentInfoACBio is constrained by an object containing a single object acbioContentInformation of the class CONTENT-TYPE. This object is defined as follows:

acbioContentInformation CONTENT-TYPE ::= {

ACBioContentInformation

IDENTIFIED BY id-acbioContentInformation }

id-acbioContentInformation OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) acbioContent(3)}

Therefore, an ACBio instance is a data of type ACBioInstance, essentially the same as the CMS type ContentInfo, with the content of type SignedDataACBio on the content of type ACBioContentInformation.

Table 1 shows the structure of type ACBioContentInformation. ACBioContentInformation consists of five fields, version, BPU information block, control value, biometric process block, and BRT certificate information where the first four fields are mandatory. An ACBio instance shall have the last field if and only if the BPU contains the storage subprocess and stores the BRT used in the executed biometric verification. The digital signature of SignedDataACBio shall be generated with the private key of the BPU.

NOTE Any ACBio instance used in enrolment does not contain a BRT certificate because it is not issued yet. **24** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**Table 1 — ACBioContentInformation**

ACBioContentInformation

|  |
| --- |
| Version |

BPU Information Block

|  |  |
| --- | --- |
|  | BPU Certificate Referrer Information |
|  | BPU Report Information |
| Control Value | |

Biometric Process Block

|  |  |
| --- | --- |
|  | ProcessIndex[1] |
|  | ・  ・ |
|  | ProcessIndex[L] |
|  | BPUIOExecutionInformation[1] (for input) |
|  | ・  ・ |
|  | BPUIOExecutionInformation[M] (for input) |
|  | BPUIOExecutionInformation[1] (for output) |
|  | ・  ・ |
|  | BPUIOExecutionInformation[N] (for output) |
| BRT Certificate Information | |

In ASN.1 notation, the type ACBioContentInformation is specified as follows:

ACBioContentInformation ::= SEQUENCE {

version Version DEFAULT v2,

bpuInformation BPUInformation,

controlValue OCTET STRING (SIZE(16..256)),

biometricProcess BiometricProcess,

brtCertificateInformation BRTCertificateInformation OPTIONAL }

Version is the version of the format of ACBioContentInformation.

Version ::= INTEGER { v1(1), v2(2) }

The type BPUInformation is defined in 6.2. The detail of each type in BPUInformation is defined in Clause 7.

A control value is an octet string of 16 byte length which is sent from the validator and with which the validator can check to which validator's request the ACBio instance is generated to. It shall be set to controlValue field to make it infeasible to replay a biometric verification process.

The type BiometricProcess is defined in 6.3. The type BRTCertificateInformation is defined in 6.4. The detail of the type in BRTCertificate, which is used in BRTCertificateInformation, is defined in Clause 8.

**6.2 BPU information block**

BPU information block carries the static information of BPU, information which does not depend on each execution. This block is mandatory and consists of two components, BPU certificate referrer

© ISO/IEC 2019 – All rights reserved **25**

**ISO/IEC FDIS 24761:2019(E)**

information and BPU report information. ASN.1 type BPUInformation is defined for this block of information:

BPUInformation ::= SEQUENCE {

bpuCertificateReferrerInformation BPUCertificateReferrerInformation OPTIONAL, bpuReportInformation BPUReportInformation}

BPU certificate referrer information of type BPUCertificateReferrerInformation is the referrer information to X.509 certificate for the public key of the BPU. If the ACBio instance contains the BPU certificate in the field of certificates in SignedDataACBio, BPU certificate referrer information can be omitted. BPU certificate is specified in 7.1.

BPUCertificateReferrerInformation ::= SEQUENCE {

bpuCertificateReferrer URI,

crlsReferrer URI OPTIONAL}

URI ::= VisibleString (SIZE(1..MAX))

BPU report information of type BPUReportInformation is the BPU report itself or its referrer. BPU report contains the information about functions implemented in the BPU and the information of the result of security evaluation of the BPU. BPU report is defined in 7.2.

BPUReportInformation ::= CHOICE {

bpuReport BPUReport,

bpuReportReferrer URI}

**6.3 Biometric process block**

Biometric process block carries the runtime information of BPU, information which depends on each execution. This block consists of three components: executedProcessIndexList, bpuInputExecutio nInformationList, and bpuOuputExecutionInformationList. executedProcessIndexList is the list of indexes of the subprocesses executed in the BPU when declaration expression is used. When role expression is used, executedProcessIndexList is the list of executionIndex (see 7.2.2.3) executed in the BPU. bpuInputExecutionInformationList contains the information on the input data to the BPU and bpuOuputExecutionInformationList contains the information on the output data from the BPU. If the BPU sends/receives data to/from other BPUs, then the corresponding components in this block are mandatory.

The ASN.1 type BiometricProcess is defined as follows:

BiometricProcess ::= SEQUENCE {

executedProcessIndexList ProcessIndexList,

bpuInputExecutionInformationList BPUIOExecutionInformationList OPTIONAL, bpuOuputExecutionInformationList BPUIOExecutionInformationList } ProcessIndexList ::= SEQUENCE SIZE(1..MAX) OF ProcessIndex

BPUIOExecutionInformationList ::= SEQUENCE OF BPUIOExecutionInformation

executedProcessIndexList is a list of data of type ProcessIndex. When declaration expression is applied, this type is also used for subprocessIndex in type FunctionDefinition (See 7.2.2.2.2) which describes the function of a subprocess in a BPU. A BPU report in an ACBio instance contains as many

**26** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

data of type FunctionDefinition as the number of subprocesses in the BPU. The subprocessIndex in the type FunctionDefinition which corresponds to the executed subprocess shall be set to the above executedProcessIndexList. When role expression is applied, this type ProcessIndex is used for executionIndex in type ExecutionInformation (See 7.2.2.3) which describes an execution pattern of a BPU. A BPU report in an ACBio instance contains as many data of type ExecutionInformation as the number of execution patterns in the BPU. The executionIndex in the type ExecutionInformation which corresponds to the executed execution pattern shall be set to the above executedProcessIndexList.

bpuInputExecutionInformationList consists of the elements of type BPUIOExecutionInformation as many as the input data to the BPU.

bpuOuputExecutionInformationList consists of the elements of type BPUIOExecutionInformation as many as the output data from the BPU.

For example, in case of a BPU which contains only the storage subprocess such as a STOC card, there is no bpuInputExecutionInformationList but bpuOuputExecutionInformationList with one element corresponding to the biometric reference from the storage subprocess.

The definition for type BPUIOExecutionInformation is given as follows:

BPUIOExecutionInformation ::= SEQUENCE {

dataType DataType,

bpuIOIndex IOIndex,

subprocessIOIndex IOIndex,

hash Hash}

Hash ::= SEQUENCE {

algorithmIdentifier AlgorithmIdentifier,

hashValue OCTET STRING}

BPUIOInformation consists of four components, dataType, bpuIOIndex, subprocessIOIndex, and hash.

dataType indicates the type of the input/output data to/from the BPU. The type DataType is defined in 7.2.2.2.3.

On execution, the application program, which utilizes the function of the BPU, shall uniquely assign an integer to each biometric data stream from/to BPUs. Such an integer given by the application program shall be set to bpuIOIndex. If another BPU generates an ACBio instance with the same integer in bpuIOIndex in the biometric process block, it means that there was a communication between these two BPUs In this way, the validator can reconstruct the data flow among BPUs.

The subprocessIOIndex of the corresponding element of the bpuInputStaticInformationList/ bpuOutputStaticInformationList in the BPU information block shall be set to subprocessIOIndex of BPUIOExecutionInformation. The combination of bpuIOIndex and subprocessIOIndex makes the connection between the data flow inside BPU and the data flow in the whole biometric verification process.

hash contains the hash value of the input/output data to/from the BPU and the identifier of the hash algorithm. The type AlgorithmIdentifier is imported from ISO/IEC 9594-2.

**6.4 BRT certificate information**

BRTcertificateInformation contains a list of the BRT certificates or the list of the referrer to each of the BRT certificate, as the following ASN.1 notation. A BRT certificate contains information about the biometric reference stored in BPU. An ACBio instance generated in biometric verification shall contain the BRT certificate Information if and only if the BPU contains the storage subprocess while an ACBio

© ISO/IEC 2019 – All rights reserved **27**

**ISO/IEC FDIS 24761:2019(E)**

instance generated in enrolment contains no BRT certificate even if the BPU contains the storage subprocess. A list of more than one element is used if multi-modal fusion biometric verification is used. BRT certificate is specified in Clause 8.

BRTCertificateInformation ::= CHOICE {

brtCertificateList BRTCertificateList,

brtCertificateReferrerList BRTCertificateReferrerList}

BRTCertificateList ::= SEQUENCE SIZE(1..MAX) OF BRTCertificate

BRTCertificateReferrerList ::= SEQUENCE SIZE(1..MAX) OF URI

**7 Definition of components in BPUInformationBlock**

**7.1 BPU certificate**

A BPU certificate is an X.509 certificate for the (public) key of BPU. The structure of BPU certificate is described in Table 2.

**Table 2 — BPU certificate**

|  |  |  |
| --- | --- | --- |
| **field** | | **content** |
| tbsCertificate | version | as ordinary |
| serialNumber | as ordinary |
| signature | as ordinary |
| validity | as ordinary |
| issuer | a trusted third party or a public CA in the vendor which produces/sells the product of the BPU |
| subject | identifier of the subject including the serial number of prod uct, the product name and version of the product, and the name of the product vendor |
| subjectPublicKeyInfo | as ordinary |
| issuerUniqueIdentifier | as ordinary |
| subjectUniqueIdentifier | as ordinary |
| extensions |  |
| signatureAlgorithm | | as ordinary |
| signatureValue | | as ordinary |

The basic part of BPU certificate consists of nine fields; version, serialNumber, signature, validity, issuer, subject, subjectPublicKeyInfo, issuerUniqueIdentifier, and subjectUniqueIdentifier, all of which are the subfields of the field tbsCertificate of the type Certificate for X.509 certificate which is defined in ISO/IEC 9594-8. Here the field **issuer** is a trusted third party or a public CA in the vendor which produces/sells the product of the BPU. The field subject is the identifier whose description shall conform to ISO/IEC 9594-2 and shall include the serial number of product, the product name and version of the product, and the name of the product vendor. The serial number of product in the subject field shall be the leaf entry of the identifier. The product name and version shall be the entry next to the leaf. Other seven attributes in the basic field are used as ordinary.

The BPU certificate shall be stored in the certificates field of SignedDataACBio or AuthenticatedDataACBio type field of the ACBio instance, or the referrer to the BPU certificate shall be stored in bpuCertificateReferrerInformation.

**28** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

BPUCertificateReferrerInformation consists of two components, bpuCertificateReferrer and crlsReferrer. In ASN.1 notation, BPUCertificateReferrerInformation is described as follows:

BPUCertificateReferrerInformation ::= SEQUENCE {

bpuCertificateReferrer URI,

crlsReferrer URI OPTIONAL}

**7.2 BPUReportInformation**

**7.2.1 General**

BPU report information contains information about function(s) implemented in the BPU and information on the security of the BPU. Either the BPU report itself or the referrer information to it shall be set in BPUReportInformation. In ASN.1 notation, BPUReportInformation is described as follows:

BPUReportInformation ::= CHOICE {

bpuReport BPUReport,

bpuReportReferrer URI}

BPUReport is defined in a similar way to ACBioInstance. BPUReport consists of two fields; the first field of fixed value of id-contentBPUReport and the second of type ContentBPUReport, which is a type of parameterized SIGNEDDATA with encapsulated content of type BPUReportContentInformation, which consists of two components, bpuFunctionReport and bpuSecurityReport. The signature shall be generated using the private key of the product vendor of the BPU.

NOTE The functions of and data flow in a BPU in enrolment mcanay be different from those in biometric verification. In such a case, two BPUReports macany be prepared, one for enrolment, another for biometric verification. Otherwise, one BPUReport can be prepared for both enrolment and biometric verification. The latter case is noted in 7.2.2.2.1.

In ASN.1 notation, BPUReport is described as follows:

BPUReport ::= SEQUENCE {

contentType CONTENT-TYPE.&id({ContentTypeBPUReport}),

content CONTENT-TYPE.&Type

({ContentTypeBPUReport}{@contentType})}

ContentTypeBPUReport CONTENT-TYPE ::= { contentBPUReport }

ContentBPUReport ::= SIGNEDDATA { EncapsulatedContentInfoBPUReport }

EncapsulatedContentInfoBPUReport ::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypeBPUReportContentInfo}), eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypeBPUReportContentInfo}{@eContentType}))}

ContentTypeBPUReportContentInfo CONTENT-TYPE ::= { bpuReportContentInformation } BPUReportContentInformation ::= SEQUENCE {

bpuFunctionReport BPUFunctionReport,

© ISO/IEC 2019 – All rights reserved **29**

**ISO/IEC FDIS 24761:2019(E)**

bpuSecurityReport BPUSecurityReport}

BPUFunctionReport and BPUSecurityReport are defined in 7.2.2 and 7.2.3.

The types BPUReport and BPUReportContentInformation are constrained with object sets containing a single object of class CONTENT-TYPE. These objects are defined as follows:

contentBPUReport CONTENT-TYPE ::= {

ContentBPUReport

IDENTIFIED BY id-contentBPUReport }

bpuReportContentInformation CONTENT-TYPE ::= {

BPUReportContentInformation

IDENTIFIED BY id-bpuReportContentInformation }

**7.2.2 BPUFunctionReport**

**7.2.2.1 General**

BPU function report contains information about function(s) implemented in the BPU and input/output data to/from the BPU. There are two ways of expression for BPU function report: declaration expression and role expression. The role expression is a new expression introduced in this document while the declaration expression is almost the same as in the first edition of this document. BPU function report for a BPU of BPU role may be expressed in both expressions. If a BPU is not of any BPU role, the BPU function report can be expressed only in declaration expression. In ASN.1 notation, BPUFunctionReport

is described as follows:

BPUFunctionReport ::= CHOICE {

bpuFunctionReportDeclaration BPUFunctionReportDeclaration,

bpuFunctionReportRole BPUFunctionReportRole }

**7.2.2.2 BPUFunctionReportDeclaration**

**7.2.2.2.1 General**

BPUFunctionReportDeclaration includes the definition of function of BPU and may include functional performance level (quality) of the function. In ASN.1 notation, BPUFunctionReportDeclaration is described as follows:

BPUFunctionReportDeclaration ::= SEQUENCE {

bpuSubprocessInformationList BPUSubprocessInformationList,

bpuInputStaticInformationList BPUIOStaticInformationList OPTIONAL, bpuOutputStaticInformationList BPUIOStaticInformationList }

BPUSubprocessInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUSubprocessInformation BPUIOStaticInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUIOStaticInformation

NOTE The specification of BPUFunctionReportDeclaration in this document is the same as that of BPUFunctionReport in ISO/IEC 24761:2009.

**30** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

bpuSubprocessInformationList is a list of elements of type BPUSubprocessInformation as many as the number of the subprocesses implemented in the BPU. The type BPUSubprocessInformation is defined in 7.2.2.2.2.

bpuInputStaticInformationList is a list of elements of type BPUIOStaticInformation as many as the number of the input data to the BPU. bpuOutputStaticInformationList is a list of elements of type BPUIOStaticInformation as many as the number of the output data from the BPU. The type BPUIOStaticInformation is defined in 7.2.2.2.3.

In enrolment, storage subprocess shall output the hash value of the input of biometric sample which is to be stored as the biometric reference, and the hash value is to be set in the BRT certificate. Therefore, bpuOutputStaticInformationList shall have such a member if it is an expression for a BPU with storage subprocess in enrolment.

When the function of and data flow in a BPU in enrolment are different from those in biometric verification, the number of the elements in bpuSubprocessInformationList might not be equal to the number of the subprocesses in the BPU. It might be the sum of the number of the subprocesses in enrolment and that in biometric verification. In this case, bpuSubprocessInformationList is divided into two groups, one for enrolment and another for biometric verification. subprocessName of functionDefinition in a member of a group of bpuSubprocessInformationList might have the same value as the value of subprocessName of functionDefinition in a member in the other group but the value of the field subprocessIndex shall be different from that of the corresponding member of the list. If the bpuSubprocessInformaitonList is expressed as above, so are bpuInputStaticInformationList and bpuOutputStaticInformationList expressed in a similar way: there might be two members in the list where the value of subprocessIOIndex of one member is different from that of the other while the values of dataType are the same.

**7.2.2.2.2 BPUSubprocessInformation**

BPUSubprocessInformation contains information about the function and result of biometric performance evaluation for the subprocess, of type FunctionDefinition and PerformanceReport defined in 7.2.2.2.2 and 7.2.2.2.3 respectively.

BPUSubprocessInformation ::= SEQUENCE {

functionDefinition FunctionDefinition,

performanceReport PerformanceReport OPTIONAL

**FunctionDefinition**

FunctionDefinition consists of seven components; subprocessName, subprocessIndex, inputIndexList, outputIndexList, and functionDescription.

subprocessName is of type SubprocessName and takes a value which represents the name of the subprocess.

To each subprocess in the BPU, the vendor of the product of the BPU shall assign a unique integer. subprocessIndex is such an index given to the subprocess.

A pair of components biometricType and biometricSubtype indicates the modality of biometric data processed in the subprocess. The types BiometricType and BiometricSubType are defined in ISO/IEC 19785-3. biometricType is mandatory if subprocessName does not take the value decision.

To each data stream which comes into or goes from any subprocess in the BPU, the vendor of the product of the BPU shall assign an integer. These integers shall be assigned uniquely within the BPU. If an input/ output to/from a subprocess is given, then it is on one of the streams and is given the integer assigned to the data stream naturally. Each member of inputIndexList and outputIndexList are given in this way. Any subprocess except data capture shall have inputIndexList. Comparison subprocess shall have two members in inputIndexList. In the case of multibiometrics, inputIndexList/outputIndexList may have more than two members.

© ISO/IEC 2019 – All rights reserved **31**

**ISO/IEC FDIS 24761:2019(E)**

descriptionFunction is for supplementary description of the function of the subprocess. The ASN.1 notation for type FunctionDefinition is given as follows:

FunctionDefinition ::= SEQUENCE {

subprocessName SubprocessName,

subprocessIndex ProcessIndex,

biometricType BiometricType OPTIONAL,

biometricSubtype BiometricSubtype OPTIONAL,

inputIndexList IOIndexList OPTIONAL,

outputIndexList IOIndexList,

functionDescription OCTET STRING (SIZE(1..MAX)) OPTIONAL}

SubprocessName ::= ENUMERATED {

data-capture(1),

intermediate-signal-processing(2),

final-signal-processing(3),

storage(4),

comparison(5),

decision(6),

sample-fusion(7),

feature-fusion(8),

score-fusion(9),

decision-fusion(10),

...}

ProcessIndex ::= INTEGER (0..65535)

IOIndexList ::= SEQUENCE SIZE(1..MAX) OF IOIndex

IOIndex ::= INTEGER (0..65535)

**PerformanceReport**

Performance report contains information about performance evaluation of the BPU and is given with an ASN.1 type PerformanceReport. This type is defined as parameterized SIGNEDDATA with encapsulated content of type PerpformanceReportContentInformation, which consists of two components nameProduct of type Name and resultPerformanceTest of type ResultPerformanceTest. The value of nameProduct shall take the same as subject in the BPU certificate. Type ResultPerformanceTest has four optional components, testResultEnrol, testResultAcquire, testResultVerify and testResultExtension. Appropriate components for the BPU shall be set. If testResultVerify is set, testResultEnrol should be also set to show the performance of enrolment under which the performance of verification is accomplished. The last field is for extension. The types of other fields are defined in ISO/IEC 29120-1.

**32** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

The signature in PerformanceReport shall be generated using the private key of the organization which evaluated the performance of the BPU.

NOTE ISO/IEC 29120-1:2015 only specifies machine readable data formats for testing and reporting of biometric recognition performance. The requirements are defined in the ISO/IEC 19795 series.

In ASN.1 notation, PerformanceReport is described as follows:

PerformanceReport::= SIGNEDDATA { EncapsulatedContentInfoPerformanceReport } EncapsulatedContentInfoPerformanceReport ::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypePerformanceReportContentInfo}), eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypePerformanceReportContentInfo}{@eContentType}))}

ContentTypePerformanceReportContentInfo CONTENT-TYPE ::= { performanceReportContentInfor mation }

PerformanceReportContentInformation ::= SEQUENCE {

nameProduct Name,

resultPerformanceTest ResultPerformanceTest }

ResultPerformanceTest ::= SEQUENCE {

testResultEnrol TestResultEnrol OPTIONAL,

testResultAcquire TestResultAcquire OPTIONAL,

testResultVerify TestResultVerify OPTIONAL,

testResultExtension TestResultExtension OPTIONAL }

TestResultExtension ::= OCTET STRING (SIZE(1..MAX)) -- For extension

The type PerformanceReportContentInformation is constrained with an object set containing a single object of class CONTENT-TYPE. The object is defined as follows:

performanceReportContentInformation CONTENT-TYPE ::= {

PerformanceReportContentInformation

IDENTIFIED BY id-performanceReportContentInformation }

**7.2.2.2.3 BPUIOStaticInformation**

BPUIOStaticInformation is a data type which gives information about input/output to/from the BPU, and consists of two components; dataType and ioIndex.

BPUIOStaticInformation ::= SEQUENCE {

dataType DataType,

ioIndex IOIndex}

A pair of components biometricType and biometricSubtype indicates the modality of biometric data of input/output to/from the BPU. biometricType is mandatory if processedLevel of dataType

© ISO/IEC 2019 – All rights reserved **33**

**ISO/IEC FDIS 24761:2019(E)**

field does not take either comparison-score or comparison-decision. The types BiometricType and BiometricSubType are defined in ISO/IEC 19785-3.

dataType is of type DataType which consists of two components, processedLevel and purpose. The former takes a value which corresponds to one of captured data, intermediate data, processed data, comparison score, or comparison decision. The latter takes a value which corresponds to biometric reference or biometric sample.

There shall be the component purpose if the first component processedLevel takes the value raw data, intermediate-data, processed-data, or renewable-data. The type renewable-data shall be applied to renewable biometric sample and renewable biometric reference. There shall not be the component purpose if the processedLevel takes the value comparison-score, comparison-decision or hashed-data.

NOTE Raw data is the old term for captured data used in ISO/IEC 24761: 2009.

An input/output to/from a BPU is one of input/output to/from a subprocess in the BPU. ioIndex shall be the value of the corresponding member of a certain data of type FunctionDefinition in BPU subprocess information.

DataType ::= SEQUENCE {

processedLevel ProcessedLevel,

purpose Purpose OPTIONAL}

ProcessedLevel ::= ENUMERATED {

raw-data(1),

intermediate-data(2),

processed-data(3),

comparison-score(4),

comparison-decision (5),

hashed-data(6),

renewable-data(7),

...}

Purpose ::= ENUMERATED {

reference(1),

sample(2)}

**7.2.2.3 BPUFunctionReportRole**

Type BPUFunctionReportRole is a sequence of type BPUFunctionReportRoleSingle: BPUFunctionReportRole ::= SEQUENCE OF BPUFunctionReportRoleSingle

Type BPUFunctionReportRoleSingle consists of two fields as follows:

BPUFunctionReportRoleSingle::= SEQUENCE {

nameRole NameRole,

executionInformationList ExecutionInformationList }

**34** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

The first field nameRole of type NameRole is to show of which BPU role the BPU is, namely all–BPU enrolment role, all–BPU-verification role, sensor BPU role, storage-and-others-if-any-BPU-role, comparator-with-capture BPU role, comparator BPU role, or storage BPU role. Type NameRole is defined as follows:

NameRole ::= ENUMERATED {

all-BPU-enrolment-role(1),

all-BPU-verification-role(2),

sensor-BPU-role(3),

storage-and-others-if-any-BPU-role(4),

comparator-with-storage-BPU-role(5),

comparator-BPU-role(6),

storage-BPU-role(7) }

The second field executionInformationList of type ExecutionInformationList in BPUFunctionReportRoleSingle shows the execution patterns of the BPU. If the BPU does not support multibiometrics, the list consists of only one member. If the BPU is of sensor BPU role which capture fingerprint and finger vein, then the list consists of two members: one for fingerprint, the other for finger vein. Each member of ExecutionInformationList is of type ExecutionInformation.

ExecutionInformationList ::= SEQUENCE SIZE(1..MAX) OF ExecutionInformation

Type ExecutionInformation consists of six fields. The first field executionIndex of type ProcessIndex (see 7.2.2.2.2.2) is the index assigned to this execution of all the execution patterns of the BPU. The second field biometricType together with the third field biometricSubtype shows the modality the execution processes. The fourth field performanceReport is information for performance evaluation. The fifth and sixth fields are information for the input and output of the BPU. They are the same as for BPUFunctionReportDeclaration.

ExecutionInformation ::= SEQUENCE {

executionIndex ProcessIndex,

biometricType BiometricType,

biometricSubtype BiometricSubtype,

performanceReport PerformanceReport OPTIONAL,

bpuInputStaticInformationList BPUIOStaticInformationList OPTIONAL, bpuOutputStaticInformationList BPUIOStaticInformationList }

NOTE Role expression of BPU function report using BPUFunctionReportRole is a black-box approach while declaration expression using BPUFunctionReportDeclaration is a white-box approach. In role expression, there is no explicit information about subprocess(es) in the BPU. The left part of Figure 19 illustrates role expression of BPU function report for BPU of comparator-with-storage BPU role. The right part contains more information than on the left but the information contained on the left is equivalent to that on the right since there are more implicit information in role expression than in declaration expression. Accordingly, the validation of ACBio instances in role expression becomes simpler than that in declaration expression.

© ISO/IEC 2019 – All rights reserved **35**

**ISO/IEC FDIS 24761:2019(E)**

****

**Figure 19 — Comparison between role expression and declaration expression for BPU of comparator-with-storage BPU role**

**7.2.3 BPUSecurityReport**

BPUSecurityReport consists of three components, cmSecurityReport, bpSecurityReport, and securityReportExtension.

BPUSecurityReport ::= SEQUENCE {

cmSecurityReport CMSecurityReport OPTIONAL,

bpSecurityReport BPSecurityReport OPTIONAL,

securityReportExtension SecurityReportExtension OPTIONAL}

CMSecurityReport carries information about security evaluation of the cryptographic module in the BPU. This type is defined as parameterized SIGNEDDATA with encapsulated content of type CMSecurityR eportContentInformation, which consists of two components nameProduct of type Name, level19790 of type Level19790. The value of nameProduct shall take the same value as **subject** in the BPU certificate. The second component level19790 is to show the level in ISO/IEC 19790 which the BPU satisfies. The signature in BPSecurityReport shall be generated using the private key of the organization which evaluated the security of cryptographic module of the BPU.

In ASN.1 notation, CMSecurityReport is described as follows:

CMSecurityReport ::= SIGNEDDATA { EncapsulatedContentInfoCMSecurityReport } EncapsulatedContentInfoCMSecurityReport::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypePerformanceCMSecurityReportContentInfo}), eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypePerformanceCMSecurityReportContentInfo }{@eContentType}))}

ContentTypePerformanceCMSecurityReportContentInfo CONTENT-TYPE ::= { cmSecurityReportConte ntInformation }

CMSecurityReportContentInformation ::= SEQUENCE {

nameProduct Name,

level19790 Level19790 }

Level19790 ::= ENUMERATED {

**36** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

level1 (1),

level2 (2),

level3 (3),

level4 (4) }

NOTE The four security levels of cryptographic modules and evaluation requirements for them are defined in ISO/IEC 19790.

The type CMSecurityReportContentInformation is constrained with an object set containing a single object of class CONTENT-TYPE. The object is defined as follows:

cmSecurityReportContentInformation CONTENT-TYPE ::= {

CMSecurityReportContentInformation

IDENTIFIED BY id-cmSecurityReportContentInformation }

BPSecurityReport ::= OCTET STRING (SIZE(1..MAX))

Type BPSecurityReport carries information about security evaluation of the biometric processing in the BPU. This type is defined as parameterized SIGNEDDATA with encapsulated content of type BPSecurityRe portContentInformation, which consists of three components nameProduct of type Name, requirements of type Requirements, and optional resultPerformanceTest of type ResultPerformanceTest defined in 7.2.2.2.3. The value of nameProduct shall take the same value as subject in the BPU certificate. The second component requirements is to show a set of security requirements which the BPU satisfies. The third component is used if the performance evaluation was done together with security evaluation of the BPU. The signature in BPSecurityReport shall be generated using the private key of the organization which evaluated the security of the BPU.

In ASN.1 notation, BPSecurityReport is described as follows:

BPSecurityReport ::= SIGNEDDATA { EncapsulatedContentInfoBPSecurityReport } EncapsulatedContentInfoBPSecurityReport::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypePerformanceBPSecurityReportContentInfo}), eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypePerformanceBPSecurityReportContentInfo }{@eContentType}))}

ContentTypePerformanceBPSecurityReportContentInfo CONTENT-TYPE ::= { bpSecurityReportConte ntInformation }

BPSecurityReportContentInformation ::= SEQUENCE {

nameProduct Name,

requirements Requirements,

resultPerformanceTest ResultPerformanceTest OPTIONAL }

Requirements ::= SEQUENCE OF Requirement

Requirement ::= OBJECT IDENTIFIER

NOTE An example of Requirement is an identifier assigned to a Protection Profile which is a set of security requirements specified to the product category (see ISO/IEC 15408-1). At the time of making this document, there is a trend to specify Protection Profiles for biometric products. The ISO/IEC 19989 series is also standardized to make security evaluation of biometric products based on ISO/IEC 15408 possible.

© ISO/IEC 2019 – All rights reserved **37**

**ISO/IEC FDIS 24761:2019(E)**

The type BPSecurityReportContentInformation is constrained with an object set containing a single object of class CONTENT-TYPE. The object is defined as follows:

bpSecurityReportContentInformation CONTENT-TYPE ::= {

BPSecurityReportContentInformation

IDENTIFIED BY id-bpSecurityReportContentInformation }

The last component SecurityReportExtension is for extension.

SecurityReportExtension ::= OCTET STRING (SIZE(1..MAX)) -- For extension **8 BRT certificate**

**8.1 General**

BRT certificate is a non-X.509 certificate to the biometric reference issued by a certain BRT certification organization. It contains information about the biometric reference stored in a BPU, such as the issuer and validity period, etc.

Type BRTCertificate is defined similarly to BPUReport. BRTCertificate consists of two fields; the first field of fixed value of id-contentBRTCertificate and the second of type ContentBRTCertificate, which is a type of parameterized SIGNEDDATA with encapsulated content of type BRTCContentInformation. The signature shall be generated using the private key of the BRT certification organization.

In ASN.1 notation, BRTCertificate is described as follows:

BRTCertificate ::= SEQUENCE {

contentType CONTENT-TYPE.&id({ContentTypeBRTCertificate}),

content CONTENT-TYPE.&Type({ContentTypeBRTCertificate}{@contentType})} ContentTypeBRTCertificate CONTENT-TYPE ::= { contentBRTCertificate }

ContentBRTCertificate ::= SIGNEDDATA { EncapsulatedContentInfoBRTCertificate } EncapsulatedContentInfoBRTCertificate ::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypeBRTCertificateContentInfo}), eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypeBRTCertificateContentInfo}{@eContentType}))}

ContentTypeBRTCertificateContentInfo CONTENT-TYPE ::= { brtcContentInformation }

The following attributes bind the type ContentBRTCertificate to id-contentBRTCertificate, and the type BRTCContentInformation to id-brtcContentInformation.

The types BRTCertificate and EncapsulatedContentInfoBRTCertificate are constrained with object sets containing a single object of class CONTENT-TYPE defined as follows:

contentBRTCertificate CONTENT-TYPE ::= {

ContentBRTCertificate

IDENTIFIED BY id-contentBRTCertificate}

id-contentBRTCertificate OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) brtCertificate(6)} **38** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

brtcContentInformation CONTENT-TYPE ::= {

BRTCContentInformation

IDENTIFIED BY id-brtcContentInformation }

id-brtcContentInformation OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) brtcContent(7)}

**8.2 BRTCContentInformation**

BRTCContentInformation is expressed with CBEFF BIR (Biometric Information Record) which is specified in ISO/IEC 19785-1. BRTCContentInformation consists of two parts, sbhForBRTC and bdbForBRTC. To express the former, SBH (Standard Biometric Header) of CBEFF is applied. The latter is a newly defined BDB (Biometric Data Block) format for BRT certificate.

Type BRTCContentInformation is described as follows:

BRTCContentInformation ::= SEQUENCE {

sbhForBRTC SBHForBRTC,

bdbForBRTC BDBForBRTC}

sbhForBRTC is of type SBHForBRTC and has nine elements; version, brtcIndex, brtcValidityPeriod, biometricType, biometricSubtype, brtQuality, bdbEncryptionOptions, bdbIntegrityOptions, and bdbFormatForBRC. The types for these elements are specified in ISO/IEC 19785-3 besides version, bdbEncryptionOptions and bdbIntegrityOptions.

version is used for specifying the version of format of SHBForBRTC.

brtcIndex indicates the index of the BRT certificate.

brtcValidityPeriod contains the validity period of the BRT certificate.

biometricType together with biometricSubtype shows the modality of the biometric reference. brtQuality contains the quality of the biometric reference.

bdbEncryptionOptions and bdbIntegrityOptions are encryptions option and integrity options of type BOOLEAN, and shall be set to FALSE. bdbFormatForBRTC indicates the format owner and format type of BDBForBRTC.

In ASN.1 notation, SBHForBRTC is described as follows:

SBHForBRTC ::= SEQUENCE {

version Version DEFAULT v1,

brtcIndex BIRIndex,

brtcValidityPeriod BDBValidityPeriod,

biometricType BiometricType,

biometricSubtype BiometricSubtype OPTIONAL,

brtQuality Quality OPTIONAL,

bdbEncryptionOptions BOOLEAN(FALSE),

bdbIntegrityOptions BOOLEAN(FALSE),

© ISO/IEC 2019 – All rights reserved **39**

**ISO/IEC FDIS 24761:2019(E)**

bdbFormatForBRTC BDBFormat}

bdbForBRTC is of type BDBForBRTC and has nine elements; version, issuerAndSerialNumberBRTC, originalBDBHashList, originalBIRReferrer, originalBIRpatronFormat, originalBDBPosition, userInformation, pkiCertificateInformation, and enrolmentACBioInstances.

version is the version of the format BDBForBRTC.

Optional field issuerAndSerialNumberBRTC of type IssuerAndSerialNumberBRTC imported from RFC 3852/5911 is a pair of information, the issuer of the BRT certificate and the unique serial number issued by the issuer. OCSP may be applied to check the validity of the BRT certificate.

originalBDBHashList is a list of Hash. Hash contains two fields, hash value and algorithm identifier of hash algorithm. The former is the hash value of the biometric reference. If originalBDBHashList contains more than one element, they are of a single biometric reference and of different hash algorithm.

originalBIRReferrer is the referrer to the original BIR.

originalBIRpatronFormat is the patron format of the original BIR, which is of type PatronFormat.

originalBDBPosition indicates the position of the biometric reference corresponding to this BRT certificate in the original BDB.

userInformation is an optional field of type UserInformation which contains identifier, name, and unique identifier of a person whose biometric reference is the object of the BRT certificate.

pkiCertificateInformation is an optional field and contains information about X.509 public-key certificate of the user, the serial number of the certificate, the name of issuer, and the unique identifier of the certificate. This field links BRT certificate to X.509 certificate.

enrolmentACBioInstances is an optional list of ACBio instances generated at the enrolment of the biometric reference.

In ASN.1 notation, BDBForBRTC is described as follows:

BDBForBRTC ::= SEQUENCE {

version Version DEFAULT v1,

issuerAndSerialNumberBRTC IssuerAndSerialNumber OPTIONAL,

originalBDBHashList HashList,

originalBIRReferrer URI OPTIONAL,

originalBIRPatronFormat PatronFormat,

originalBDBPosition INTEGER,

userInformation UserInformation OPTIONAL,

pkiCertificateInformation PKICertificateInformation OPTIONAL,

enrolmentACBioInstances SequenceOfACBioInstances OPTIONAL}

HashList ::= SEQUENCE SIZE(1..MAX) OF Hash

UserInformation ::= SEQUENCE {

userIdentifier OCTET STRING,

userName Name OPTIONAL,

userUniqueIdentifier UniqueIdentifier OPTIONAL}

**40** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

PKICertificateInformation ::= SEQUENCE {

pkiCertificateSerialNumber CertificateSerialNumber,

pkiCertificateIssuerName Name OPTIONAL,

pkiCertificateIssuerUniqueIdentifier UniqueIdentifier OPTIONAL}

SequenceOfACBioInstances ::= SEQUENCE SIZE(1..MAX) OF ACBioInstance

**8.3 Format Owner and Format Type values**

The Format Owner for the BDBForBRTC shall use the value 0102 hex (258 decimal). The Format Type for the BDBForBRTC shall use the value 0001 hex (1 decimal), which has been registered as the value for the BDBForBRTC.

Thus, te resulting ASN.1 Object Identifier value for the BDBForBRTC is:

{iso registration-authority cbeff(19785) organization(0) iso-iec-jtc1-SC27 (258) bdbs(0) biometric-reference-template-certificate (1)}

© ISO/IEC 2019 – All rights reserved **41**

**ISO/IEC FDIS 24761:2019(E)**

**Annex A**

(normative)

**ASN.1 module for ACBio**

AuthenticationContextForBiometrics {iso(1) standard(0) acbio(24761) module(1) acbio(2) version2(2)} DEFINITIONS AUTOMATIC TAGS ::= BEGIN

IMPORTS

-- ASN.1 Module AlgorithmInformation in RFC 5912

AlgorithmIdentifier

FROM AlgorithmInformation-2009 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-algorithmInformation-02(58)}

-- RFC 5280 revised as RFC 5912

Certificate, CertificateList, CertificateSerialNumber, Name, UniqueIdentifier

FROM PKIX1Explicit-2009 { iso(1) identified-organization(3) dod(6) internet(1)

security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-explicit-02(51) }

-- RFC 5755 revised as RFC 5912

AttributeCertificate

FROM PKIXAttributeCertificate-2009 { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-attribute-cert-02(47) }

-- ISO/IEC 19785 Common Biometric Exchange Formats Framework

BiometricType, BiometricSubtype, BIRIndex,

BDBValidityPeriod,Quality, BDBFormat, PatronFormat

FROM CBEFF-DATA-ELEMENTS {iso standard 19785 modules(0)

types-for-cbeff-data-elements(1) }

-- ISO/IEC 29120-1 Machine readable test data for biometric testing and reporting

TestResultEnrol, TestResultAcquire, TestResultVerify

FROM MachineReadableBiometricTestingAndReportingTestReport {

iso(1) standard(0) MRTDBTR(29120) testReport(1) module(1) rev(0) }

-- RFC 3852 Cryptographic Message Syntax revised as RFC 5911

CMSVersion, DigestAlgorithmIdentifier, SignerInfos,

IssuerAndSerialNumber, CertificateSet, RevocationInfoChoices,

CONTENT-TYPE

FROM CryptographicMessageSyntax2009{

iso(1) member-body(2) us(840) rsadsi(113549)

pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004-02(41) };

ACBioInstance ::= SEQUENCE {

contentType CONTENT-TYPE.&id({ContentTypeACBio}),

content CONTENT-TYPE.&Type

({ContentTypeACBio}{@contentType})}

**42** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

ContentTypeACBio CONTENT-TYPE ::= {signedDataACBio}

SignedDataACBio ::= SIGNEDDATA { EncapsulatedContentInfoACBio }

EncapsulatedContentInfoACBio ::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypeACBioContentInfo}),

eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypeACBioContentInfo}{@eContentType}))}

ContentTypeACBioContentInfo CONTENT-TYPE ::= {acbioContentInformation}

ACBioContentInformation ::= SEQUENCE {

version Version DEFAULT v2,

bpuInformation BPUInformation,

controlValue OCTET STRING (SIZE(16..256)),

biometricProcess BiometricProcess,

brtCertificateInformation BRTCertificateInformation OPTIONAL}

Version ::= INTEGER { v1(1), v2(2) }

BPUInformation ::= SEQUENCE {

bpuCertificateReferrerInformation BPUCertificateReferrerInformation

OPTIONAL,

bpuReportInformation BPUReportInformation}

BPUCertificateReferrerInformation ::= SEQUENCE {

bpuCertificateReferrer URI,

crlsReferrer URI OPTIONAL}

URI ::= VisibleString (SIZE(1..MAX))

BPUReportInformation ::= CHOICE {

bpuReport BPUReport,

bpuReportReferrer URI}

BPUReport ::= SEQUENCE {

contentType CONTENT-TYPE.&id({ContentTypeBPUReport}),

content CONTENT-TYPE.&Type

({ContentTypeBPUReport}{@contentType})}

ContentTypeBPUReport CONTENT-TYPE ::= {contentBPUReport }

ContentBPUReport ::= SIGNEDDATA { EncapsulatedContentInfoBPUReport }

EncapsulatedContentInfoBPUReport ::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypeBPUReportContentInfo}),

eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypeBPUReportContentInfo}{@eContentType}))}

ContentTypeBPUReportContentInfo CONTENT-TYPE ::= { bpuReportContentInformation }

BPUReportContentInformation ::= SEQUENCE {

bpuFunctionReport BPUFunctionReport,

bpuSecurityReport BPUSecurityReport}

BPUFunctionReport ::= CHOICE {

bpuFunctionReportDeclaration BPUFunctionReportDeclaration,

bpuFunctionReportRole BPUFunctionReportRole }

BPUFunctionReportDeclaration ::= SEQUENCE {

© ISO/IEC 2019 – All rights reserved **43**

**ISO/IEC FDIS 24761:2019(E)**

bpuSubprocessInformationList BPUSubprocessInformationList,

bpuInputStaticInformationList BPUIOStaticInformationList OPTIONAL,

bpuOutputStaticInformationList BPUIOStaticInformationList }

BPUSubprocessInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUSubprocessInformation

BPUSubprocessInformation ::= SEQUENCE {

functionDefinition FunctionDefinition,

performanceReport PerformanceReport OPTIONAL}

FunctionDefinition ::= SEQUENCE {

subprocessName SubprocessName,

subprocessIndex ProcessIndex,

biometricType BiometricType OPTIONAL,

biometricSubtype BiometricSubtype OPTIONAL,

inputIndexList IOIndexList OPTIONAL,

outputIndexList IOIndexList,

functionDescription OCTET STRING (SIZE(1..MAX)) OPTIONAL}

SubprocessName ::= ENUMERATED {

data-capture(1),

intermediate-signal-processing(2),

final-signal-processing(3),

storage(4),

comparison(5),

decision(6),

sample-fusion(7),

feature-fusion(8),

score-fusion(9),

decision-fusion(10),

...}

ProcessIndex ::= INTEGER (0..65535)

IOIndexList ::= SEQUENCE SIZE(1..MAX) OF IOIndex

IOIndex ::= INTEGER (0..65535)

PerformanceReport ::= SIGNEDDATA { EncapsulatedContentInfoPerformanceReport }

EncapsulatedContentInfoPerformanceReport ::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypePerformanceReportContentInfo}),

eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypePerformanceReportContentInfo}{@eContentType}))}

ContentTypePerformanceReportContentInfo CONTENT-TYPE ::= { performanceReportContentInformation } PerformanceReportContentInformation ::= SEQUENCE {

nameProduct Name,

resultPerformanceTest ResultPerformanceTest }

ResultPerformanceTest ::= SEQUENCE {

testResultEnrol TestResultEnrol OPTIONAL,

testResultAcquire TestResultAcquire OPTIONAL,

testResultVerify TestResultVerify OPTIONAL,

**44** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

testResultExtension TestResultExtension OPTIONAL }

TestResultExtension ::= OCTET STRING (SIZE(1..MAX)) -- For extension

BPUIOStaticInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUIOStaticInformation

BPUIOStaticInformation ::= SEQUENCE {

dataType DataType,

ioIndex IOIndex}

DataType ::= SEQUENCE {

processedLevel ProcessedLevel,

purpose Purpose OPTIONAL}

ProcessedLevel ::= ENUMERATED {

raw-data(1),

intermediate-data(2),

processed-data(3),

comparison-score(4),

comparison-result(5),

hashed-data(6),

renewable-data(7),

...}

Purpose ::= ENUMERATED {

reference(1),

sample(2)}

BPUFunctionReportRole ::= SEQUENCE OF BPUFunctionReportRoleSingle

BPUFunctionReportRoleSingle::= SEQUENCE {

nameRole NameRole,

executionInformationList ExecutionInformationList }

NameRole ::= ENUMERATED {

all-BPU-enrolment-role (1),

all-BPU-verification-role(2),

sensor-BPU-role(3),

storage-and-others-if-any-BPU-role(4),

comparator-with-storage-BPU-role(5),

comparator-BPU-role(6),

storage-BPU-role(7) }

ExecutionInformationList ::= SEQUENCE SIZE(1..MAX) OF ExecutionInformation

ExecutionInformation ::= SEQUENCE {

executionIndex ProcessIndex,

biometricType BiometricType,

biometricSubtype BiometricSubtype,

performanceReport PerformanceReport OPTIONAL,

bpuInputStaticInformationList BPUIOStaticInformationList OPTIONAL,

bpuOutputStaticInformationList BPUIOStaticInformationList }

BPUSecurityReport ::= SEQUENCE {

cmSecurityReport CMSecurityReport OPTIONAL,

bpSecurityReport BPSecurityReport OPTIONAL,

securityReportExtension SecurityReportExtension OPTIONAL}

CMSecurityReport ::= SIGNEDDATA { EncapsulatedContentInfoCMSecurityReport }

EncapsulatedContentInfoCMSecurityReport::= SEQUENCE {

© ISO/IEC 2019 – All rights reserved **45**

**ISO/IEC FDIS 24761:2019(E)**

eContentType CONTENT-TYPE.&id({ContentTypePerformanceCMSecurityReportContentInfo}), eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypePerformanceCMSecurityReportContentInfo }{@eContentType}))}

ContentTypePerformanceCMSecurityReportContentInfo CONTENT-TYPE ::= { cmSecurityReportContentInformation } CMSecurityReportContentInformation ::= SEQUENCE {

nameProduct Name,

level19790 Level19790 }

Level19790 ::= ENUMERATED {

level1 (1),

level2 (2),

level3 (3),

level4 (4) }

BPSecurityReport ::= SIGNEDDATA { EncapsulatedContentInfoBPSecurityReport }

EncapsulatedContentInfoBPSecurityReport::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypePerformanceBPSecurityReportContentInfo}), eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypePerformanceBPSecurityReportContentInfo }{@eContentType}))}

ContentTypePerformanceBPSecurityReportContentInfo CONTENT-TYPE ::= { bpSecurityReportContentInformation } BPSecurityReportContentInformation ::= SEQUENCE {

nameProduct Name,

requirements Requirements,

resultPerformanceTest ResultPerformanceTest OPTIONAL }

Requirements ::= SEQUENCE OF Requirement

Requirement ::= OBJECT IDENTIFIER

SecurityReportExtension ::= OCTET STRING (SIZE(1..MAX)) -- For extension

BiometricProcess ::= SEQUENCE {

executedProcessIndexList ProcessIndexList,

bpuInputExecutionInformationList BPUIOExecutionInformationList OPTIONAL,

bpuOuputExecutionInformationList BPUIOExecutionInformationList }

ProcessIndexList ::= SEQUENCE SIZE(1..MAX) OF ProcessIndex

BPUIOExecutionInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUIOExecutionInformation

BPUIOExecutionInformation ::= SEQUENCE {

dataType DataType,

bpuIOIndex IOIndex,

subprocessIOIndex IOIndex,

hash Hash}

Hash ::= SEQUENCE {

algorithmIdentifier AlgorithmIdentifier,

hashValue OCTET STRING}

BRTCertificateInformation ::= CHOICE {

**46** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

brtCertificateList BRTCertificateList,

brtCertificateReferrerList BRTCertificateReferrerList}

BRTCertificateList ::= SEQUENCE SIZE(1..MAX) OF BRTCertificate

BRTCertificateReferrerList ::= SEQUENCE SIZE(1..MAX) OF URI

BRTCertificate ::= SEQUENCE {

contentType CONTENT-TYPE.&id({ContentTypeBRTCertificate}),

content

CONTENT-TYPE.&Type({ContentTypeBRTCertificate}{@contentType})}

ContentTypeBRTCertificate CONTENT-TYPE ::= { contentBRTCertificate }

ContentBRTCertificate ::= SIGNEDDATA { EncapsulatedContentInfoBRTCertificate }

EncapsulatedContentInfoBRTCertificate ::= SEQUENCE {

eContentType CONTENT-TYPE.&id({ContentTypeBRTCertificateContentInfo}),

eContent [0] EXPLICIT OCTET STRING

( CONTAINING CONTENT-TYPE.&Type

({ContentTypeBRTCertificateContentInfo}{@eContentType}))}

ContentTypeBRTCertificateContentInfo CONTENT-TYPE ::= { brtcContentInformation }

BRTCContentInformation ::= SEQUENCE {

sbhForBRTC SBHForBRTC,

bdbForBRTC BDBForBRTC}

SBHForBRTC ::= SEQUENCE {

version Version DEFAULT v1,

brtcIndex BIRIndex,

brtcValidityPeriod BDBValidityPeriod,

biometricType BiometricType,

biometricSubtype BiometricSubtype OPTIONAL,

brtQuality Quality OPTIONAL,

bdbEncryptionOptions BOOLEAN(FALSE),

bdbIntegrityOptions BOOLEAN(FALSE),

bdbFormatForBRTC BDBFormat}

BDBForBRTC ::= SEQUENCE {

version Version DEFAULT v1,

issuerAndSerialNumberBRTC IssuerAndSerialNumber OPTIONAL,

originalBDBHashList HashList,

originalBIRReferrer URI OPTIONAL,

originalBIRPatronFormat PatronFormat,

originalBDBPosition INTEGER,

© ISO/IEC 2019 – All rights reserved **47**

**ISO/IEC FDIS 24761:2019(E)**

userInformation UserInformation OPTIONAL,

pkiCertificateInformation PKICertificateInformation OPTIONAL,

enrolmentACBioInstances SequenceOfACBioInstances OPTIONAL}

HashList ::= SEQUENCE SIZE(1..MAX) OF Hash

UserInformation ::= SEQUENCE {

userIdentifier OCTET STRING,

userName Name OPTIONAL,

userUniqueIdentifier UniqueIdentifier OPTIONAL}

PKICertificateInformation ::= SEQUENCE {

pkiCertificateSerialNumber CertificateSerialNumber,

pkiCertificateIssuerName Name OPTIONAL,

pkiCertificateIssuerUniqueIdentifier UniqueIdentifier OPTIONAL}

SequenceOfACBioInstances ::= SEQUENCE SIZE(1..MAX) OF ACBioInstance

-- Useful definitions

SIGNEDDATA { EncapsulatedContentInfo } ::= SEQUENCE {

version CMSVersion,

digestAlgorithms SET OF DigestAlgorithmIdentifier,

encapContentInfo EncapsulatedContentInfo,

certificates [0] IMPLICIT CertificateSet OPTIONAL,

crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,

signerInfos SignerInfos}

-- contentType object identifiers

id-signedDataACBio OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) signedDataACBio(1)}

id-acbioContentInformation OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) acbioContent(3)}

id-contentBPUReport OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) bpuReport(4)}

id-bpuReportContentInformation OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) bpuReportContent(5)}

id-contentBRTCertificate OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) brtCertificate(6)}

id-brtcContentInformation OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) brtcContent(7)}

id-performanceReportContentInformation OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) brtcContent(8)}

id-cmSecurityReportContentInformation OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) brtcContent(9)}

id-bpSecurityReportContentInformation OBJECT IDENTIFIER ::=

{iso(1) standard(0) acbio(24761) contentType(2) brtcContent(10)}

-- ContentType objects

signedDataACBio CONTENT-TYPE ::= {

SignedDataACBio

IDENTIFIED BY id-signedDataACBio }

acbioContentInformation CONTENT-TYPE ::= {

ACBioContentInformation

IDENTIFIED BY id-acbioContentInformation }

**48** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

contentBPUReport CONTENT-TYPE ::= {

ContentBPUReport

IDENTIFIED BY id-contentBPUReport }

bpuReportContentInformation CONTENT-TYPE ::= {

BPUReportContentInformation

IDENTIFIED BY id-bpuReportContentInformation }

contentBRTCertificate CONTENT-TYPE ::= {

ContentBRTCertificate

IDENTIFIED BY id-contentBRTCertificate }

brtcContentInformation CONTENT-TYPE ::= {

BRTCContentInformation

IDENTIFIED BY id-brtcContentInformation }

performanceReportContentInformation CONTENT-TYPE ::= {

PerformanceReportContentInformation

IDENTIFIED BY id-performanceReportContentInformation }

cmSecurityReportContentInformation CONTENT-TYPE ::= {

CMSecurityReportContentInformation

IDENTIFIED BY id-cmSecurityReportContentInformation }

bpSecurityReportContentInformation CONTENT-TYPE ::= {

BPSecurityReportContentInformation

IDENTIFIED BY id-bpSecurityReportContentInformation }

END -- AuthenticationContextForBiometrics

© ISO/IEC 2019 – All rights reserved **49**

**ISO/IEC FDIS 24761:2019(E)**

**Annex B**

(informative)

**Implementation examples**

**B.1 Examples of the implementation of ACBio**

**B.1.1 General**

In this document, the protocol for ACBio is not specified. In this Annex, two examples of implementation of ACBio are given including protocols; one for a case of STOC (STore On Card) model, the other for a case of OCBC (On Card Biometric Comparison) model.

**B.1.2 An Example of the implementation of STOC Model**

**B.1.2.1 General**

In this example, the STOC model of a biometric verification process means a biometric system consisting of two BPUs: one is a biometric device which has the functions of data capture, intermediate signal processing, final signal processing, comparison and decision, and the other is a STOC card which stores the processed biometric reference. This example is mainly focused on STOC card.

**B.1.2.2 In production process**

**B.1.2.2.1 Case of declaration expression**

Products of BPUs, ie STOC cards and biometric devices used in a biometric verification process, should be evaluated at a certain evaluation organization and issued their BPU security reports.

**B.1.2.2.2 Case of declaration expression**

Vendors of BPUs indexes every subprocess and stream in accordance with the rule in 7.2.2. If the subprocesses and streams in the biometric device and those in the STOC card are indexed as in Figure B.1 and Figure B.2, then the BPUFunctionReport of the biometric device and that of the STOC card are as shown in Figure B.3. In Figure B.1 and Figure B.2, SIndex means subprocess index and IOIndex means subprocess IO index.

**50** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**Figure B.1 — A biometric enrolment process of a STOC model and an example of indexing for declaration expression**

**Figure B.2 — A biometric verification process of a STOC model and an example of indexing for declaration expression**

As written in the NOTE in 7.2.2.2, bpuSubprocessInformationList, bpuInputStaticInformationList, and bpuOutputStaticInformationList are divided into two groups: one for enrolment and another

© ISO/IEC 2019 – All rights reserved **51**

**ISO/IEC FDIS 24761:2019(E)**

for verification. Figure B.3 is an example for BPUFunctionReports. The whole of BPUFunctionReport for the STOC card is shown in Figure B.3. BPUSubprocessInformation and BPUIOInformation in BPUFunctionReport for the biometric device are depicted in Figure B.4 and Figure B.5 respectively.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | |  |  |  | | | | |
|  |  | | | |  |  |  |  | | | |
|  |  |  | | |  |  |  |  |  | | |
|  |  |  |  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  | | |
|  |  |  |  |  |  |  |  |  |  | | |
|  |  |  |  |  |  |  |  |  |  | | |
|  |  |  |  | |  |  |  |  |  | | |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  | | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  | | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | | | | |  |  |  | | | | |

**Figure B.3 — Examples of BPUFunctionReports for a STOC model in declaration expression 52** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | |  |  |  |  |  |  | |
|  | |  |  |  |  |  |  | |
|  |  | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | |  |  |  |  |  |  | |
|  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  | |
|  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |

**Figure B.4 — Examples of BPUSubprocessInformation for a biometric device** © ISO/IEC 2019 – All rights reserved **53**

**ISO/IEC FDIS 24761:2019(E)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  |  |  |  |  | | |
|  |  | |  |  |  |  |  |  | |
|  |  | |  |  |  |  |  |  | |
|  |  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  | | |
|  | | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | | |

**Figure B.5 — Examples of BPUIOInformation for a biometric device**

**B.1.2.2.3 Case of role expression**

Compared with declaration expression, role expression is more implicit but simpler. Vendors of BPUs do not have to index every subprocess and stream in BPUs but should index streams from/to the BPUs. If the streams from/to the biometric device and that from the STOC card are indexed as in Figure B.6 for enrolment and Figure B.7 for verification, then the BPUFunctionReport of the biometric device and that of the STOC card are expressed as in Figure B.8. In Figure B.6 and Figure B.7, IOIndex means subprocess IO index.

**Figure B.6 — A biometric enrolment process of a STOC model and an example of indexing for role expression**

**54** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**Figure B.7 — A biometric verification process of a STOC model and an example of indexing for role expression**

© ISO/IEC 2019 – All rights reserved **55**

**ISO/IEC FDIS 24761:2019(E)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | |  |  |  | | | | | |
|  |  | | | | |  |  |  |  | | | | |
|  |  |  | | | |  |  |  |  |  | | | |
|  |  |  | | | |  |  |  |  |  | | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  | | | |  |  |  |  |  | | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  | |  |  |  | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | | | | | |  |  |  |  |  |  |  |  |

**Figure B.8 — Examples of BPUFunctionReports for a STOC model in role expression**

**B.1.2.3 In enrolment process**

Biometric reference is stored to a STOC card in this process. A BRT certificate is issued to the biometric reference. It or its referrer is to be stored in brtCertificateInformation of ACBioContentInformation.

**B.1.2.4 In execution process**

On an execution of biometric verification, two inputs are given to a STOC card; the first is a control value from the validator, the second is the BPU IO index to the output from the STOC card. Called with PERFORM BIOMETRIC OPERATION command, which is specified in ISO/IEC 7816-11, with parameters including the above two, the STOC card digitally signs the whole field of the type ACBioContentInformation to get the ACBio instance and returns it together with the processed biometric reference, as depicted in Figure B.9 when declaration expression is used. When role expression is used, 10, index of executed subprocess, is replaced with 2 of executionIndex, and 11, the subprocess IO index for output, is replaced with 5 (see Figure B.7 and Figure B.8).

**56** © ISO/IEC 2019 – All rights reserved



**ISO/IEC FDIS 24761:2019(E)**

**Figure B.9 — ACBio instance generation on a STOC card on an execution of biometric verification**

**B.1.2.5 An example of protocol**

In this example, it is assumed that all of the subprocesses of biometric verification are done at the claimant and also that there is a system at the claimant which sends and receives messages to/from the system of the validator, biometric device, and STOC card, as shown in Figure B.10.

© ISO/IEC 2019 – All rights reserved **57**

**ISO/IEC FDIS 24761:2019(E)**

**Key**

1 to 15 order of protocol execution

**Figure B.10 — An example of protocol for a STOC model**

The following shows an example of the protocol for this STOC model:

1) The claimant requests authentication to the validator, via the system of claimant.

2) The system of validator sends the control value and the candidate list of hash algorithms, digital signature algorithms, modalities, and biometric capability classes according to the ACBio validation policy, and requests the execution of biometric verification to the system of claimant. Here in this example, storage-and-others class is assumed to be contained in the candidate list of biometric capability classes.

3) The system of the claimant checks if any of the list of modalities and biometric capability classes are satisfied at the claimant. In this case, the biometric device and STOC card can configure storage and-others class in the list of biometric capability classes. If there is a set of BPUs which satisfy the modalities and biometric capabilitiy classes, the system of the claimant also checks if the data types of the data flows between the BPUs are consistent.

4) The system of the claimant inquires available hash algorithms and digital signature algorithms to the biometric device and the STOC card.

5) The biometric device and the STOC card return available hash algorithms and digital signature algorithms to the system of claimant side.

6) The system of claimant decides the hash algorithm and the signature algorithm, and sends the validator's control value, the hash algorithm, and the signature algorithm to the biometric device to request execution of data capture, intermediate signal processing, and final signal processing.

**58** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

7) The biometric device captures the biometric information from the claimant and generates the processed biometric sample through data capture, intermediate signal processing, and final signal processing subprocesses.

8) The biometric device sends the termination message of final signal processing to the system of the claimant.

9) The system of the claimant calls the STOC card to get the processed biometric reference with the validator's control value, the hash algorithm and the signature algorithm selected in step (6), and a BPU IO Index for the output data (processed biometric reference) of the STOC card.

10) The STOC card generates an ACBio instance (see B.1.2.4 for details).

11) The STOC card returns the processed biometric reference with the ACBio instance to the system of the claimant.

12) The system of claimant calls the biometric device for execution of comparison and decision with the processed biometric reference received from the STOC card, the BPU IO index assigned to the processed biometric reference, and the BPU IO Index assigned to the comparison decision of the biometric device.

13) The biometric device receives the processed biometric reference and executes comparison and decision subprocesses. The biometric device also generates an ACBio instance with the following procedures.

a) Restore the BPU Information block and set it to bpuInformation of ACBioContentInformation. b) Set the validator's control value to controlValue of ACBioContentInformation. c) Generate the biometric process block as follows;

1a) (The case of declaration expression used for BPU report) Set the subprocess indexes corresponding to the subprocesses executed at the biometric devices to executedProcessIndexList. In this case, the subprocess indexes corresponding to data capture, intermediate signal processing, final signal processing, comparison, and decision are set in executedProcessIndexList.

1b) (The case of role expression used for BPU report) Set the executionIndex in executionInformationList in BPUFunctionReportRoleSingle corresponding to the execution of the functions at the biometric device to executedProcessIndexList. If BPUFunctionReportRoleSingle is expressed as in Figure B.8, 2 is set as the only one member of executedProcessIndexList.

2) To make bpuInputExecutionInformationList field, the following should be done. Set the value processed-data and the value reference respectively to processedLevel and purpose of dataType. Set the BPU IO index, assigned to the input of the biometric device, to bpuIOIndex. Set the subprocess IO index of the input data (processed biometric reference) to the comparison subprocess to subprocessIOIndex. Set the pair of the hash value of the processed biometric reference received and the hash algorithm to hash.

3) To make bpuOutputExecutionInformationList field, the following should be done. Set the value comparison-decision to processedLevel of dataType. Set the BPU IO index, assigned to the output data of the biometric device, to bpuIOIndex. Set the subprocess IO index of the output data (comparison decision) of the decision subprocess, which was assigned by the product vendor of the biometric device, to subprocessIOIndex. Set the pair of the hash value of the comparison decision and the hash algorithm into hash.

d) Generate SignedDataACBio with the data generated as in a), b) and c), using the digital signature algorithm selected in (6).

14) The biometric device sends the result of decision subprocess and the ACBio instance to the system of the claimant.

© ISO/IEC 2019 – All rights reserved **59**

**ISO/IEC FDIS 24761:2019(E)**

15) The system of the claimant sends the result of comparison decision and the two ACBio instances to the system of the validator.

16) The system of the validator receives the result of comparison decision and the two ACBio instances. The validator validates the results with the following procedures;

a) Validate the integrity of each ACBio instance by signature verification. It is also checked whether the digital signature algorithm satisfies the policy or not.

b) Validate the correspondence of the control value originally given by the validator and the control value of each ACBio instance.

c) Validate the validity of biometric reference used checking the BRT certificate in the ACBio instance generated at the STOC card, if necessary.

d) Check whether the whole process of biometric verification executed satisfies the policy of biometric capability class or not by checking executedProcessIndexList in the biometric process block with reference to the BPU report of the two ACBio instances. If declaration expression is used, the subprocess indexes (specified in functionDefinition in the BPU report) of executed subprocesses are set in executedProcessIndexList in the biometric process blocks of the two ACBio instances. Checking the correspondence of subprocess indexes and subprocessName of functionDefinition, the validator can conclude that storage-and-others class configuration was used for biometric verification (see shaded parts of two biometric process blocks in Figure B.11). If role expression is used, it is easier to check these. For example, the validator can know that the left ACBio instance in Figure B.12 comes from a BPU of comparator BPU role with input of processed biometric reference and output of comparison decision. This is known because the value 2 in executedProcessIndexList in biometric process block refers to the lower ExecutionInformation of BPU Function Report in Figure B.8 and this ExecutionInformation contains the information of the input and output of this BPU. Similarly, the validator can know that the right ACBio instance in Figure B.12 comes from a BPU of storage BPU role with output of processed biometric reference. Then the validator can know that the data flow between these two BPUs is consistent, ie processed biometric reference. The validator can conclude that the two BPUs configure storage-and-others class.

e) Validate the consistency of the input data and the output data transmitted between BPUs. First the validator has to find the same BPU IO index used in bpuInputExecutionInformationList or bpuOutputExecutionInformationList from the biometric process blocks in the two ACBio instance. In Figure B.11 and Figure B.12, the bold arrow shows the correspondence of the same BPU IO index between the two ACBio instances. By comparing the contents of dataType, bpuIOIndex, and hashValue of bpuOutputExecutionInformationList in the biometric process block of the ACBio instance generated by the STOC card and those of bpuInputExecutionInfo rmationList in the biometric process block of the ACBio instance generated by the biometric device, the validator can conclude the consistency of the data flow between the two BPUs (see four thin arrows between biometric process blocks in Figure B.11 and Figure B.12).

Figure B.11 illustrates the validation process of biometric verification when declaration expression is used. Figure B.12 is for the case of role expression used. In Figure B.11 and Figure B.12, the indexes given in Figure B.2 and Figure B.7 are used respectively.

**60** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | |  |  |  | | | | |
|  |  | | |  |  |  |  |  |  | |  |  |
|  |  | | | |  |  |  |  |  | | |  |
|  |  |  | | | |  |  |  |  |  | | |
|  |  |  | | | |  |  |  |  |  | | |
|  |  | | | |  |  |  |  |  | | |  |
|  |  |  |
|  |  | | | | |  |  |  |  | | | |
|  |  |  | | | |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | |
|  |  |  |  | | |  |  |  |  |  |  |  |
|  |  |  |  | | |  |  |  |  |  |  |  |
|  |  |  | | | |  |  |  |  |  |  | |
|  |  |  | |  | |  |  |  |  |  |  | |
|  |  |  | |  |  |  |  |  |  |  |  | |
|  |  |  | |  |  |  |  |  |  |  |  |  |
|  |  |  | |  | |  |  |  |  |  |  |  |
|  |  |  | |  | |  |  |  |  | | | |
|  |  |  | |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  | | | | |
|  |  |  | |  |  |  |  |  |  |  |  |  |
|  |  |  | | |  |  |  |  |  |  |  |  |
|  |  |  | |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |  |  |
|  |  |  | |  | |  |  |  |  |  |  |  |
|  |  |  | |  | |  |  |  |  |  |  |  |
|  |  |  | |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |  |  |
|  | | | | | |  |  |  |  |  |  |  |

**Figure B.11 — Validation of biometric verification for a STOC model when declaration expression is used**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |  |  |  | | | | | |
|  |  | |  | |  | |  |  |  |  | |  | |  |
|  |  | | | |  | |  |  |  |  | | | |  |
|  |  |  | | | | |  |  |  |  |  | | | |
|  |  |  | | | | |  |  |  |  |  | | | |
|  |  | | | |  | |  |  |  |  | | | |  |
|  | |  |  |
|  |  | | | | | |  |  |  |  | | | | |
|  |  |  | | | | |  |  |  |  |  | | | |
|  |  |  | | | | |  |  |  |  |  | | | |
|  |  |  |  | | | |  |  |  |  |  |  | | |
|  |  |  |  | |  | |  |  |  |  |  |  | |  |
|  |  |  |  |  |
|  |  |  |  | |  | |  |  |  |  |  |  | |  |
|  |  |  |  |  |
|  |  |  |  | | | |  |  |  |  |  |  | | |
|  |  |  |  |  | | |  |  |  |  |  |  |  | |
|  |  |  |  | | |  |  |  |  |  |  |  | | |
|  |  |  |  | |  | |  |  |  |  |  |  | |  |
|  |  |  |  |  |
|  |  |  |  | |  | |  |  |  |  |  |  | |  |
|  |  |  |  |  |
|  |  |  | | |  | |  |  |  |  | | | | |
|  |  |  |  | | | |  |  |  |  |  |  | |  |
|  |  |  |  | |  | |  |  |  | | | | | |
|  |  |  |  | | | |  |  |  |  |  |  | |  |
|  |  |  |  |  | | |  |  |  |  |  |  | |  |
|  |  |  |  | | | |  |  |  |  |  |  | |  |
|  |  |  |  | |  | |  |  |  |  |  |  | |  |
|  |  |  |  | |  | |  |  |  |  |  |  | |  |
|  |  |  |  | |  | |  |  |  |  |  |  | |  |
|  | | | | | | |  |  |  |  |  |  | |  |

**Figure B.12 — Validation of biometric verification for a STOC model when role expression is used** © ISO/IEC 2019 – All rights reserved **61**

**ISO/IEC FDIS 24761:2019(E)**

**B.1.3 An Example of the implementation of OCBC Model**

**B.1.3.1 General**

In this example, the OCM model of biometric verification process means a biometric system consisting of two BPUs: one is a sensor device which has the functions of data capture, intermediate signal processing, and final signal processing, and the other is an OCM card which has the functions of storage, comparison, and decision. This example is mainly focused on OCM card.

**B.1.3.2 In production process**

**B.1.3.2.1 General**

Products of BPUs, ie OCM cards and sensor devices used in a biometric verification process, should be evaluated at a certain evaluation organization and issued their BPU security reports.

**B.1.3.2.2 Case of declaration expression**

Vendors of BPUs indexes every subprocess and stream in accordance with the rule in 7.2.2. If the subprocesses and streams in the sensor device and those in the OCBC card are indexed as in Figure B.13 and Figure B.14, then the BPUFunctionReport of the biometric device and that of the OCBC card are as shown in Figure B.15. In Figure B.13 and Figure B.14, SIndex means subprocess index and IOIndex means subprocess IO index.

**Figure B.13 — A biometric enrolment process of an OCBC model and an example of indexing for declaration expression**

**62** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**Figure B.14 — A biometric verification process of an OCBC model and an example of indexing for declaration expression**

As written in the NOTE in 7.2.2.2, bpuSubprocessInformationList, bpuInputStaticInformationList, and bpuOutputStaticInformationList are divided into two groups in general: one for enrolment and another for verification. But seen in Figure B.13 and Figure B.14, the processing and data flows in enrolment and those in verification are the same for the sensor device. The sensor device does not need to have two groups of information. Figure B.15 is an example for BPUFunctionReports. The whole of BPUFunctionReport for the sensor device is shown in Figure B.15. BPUSubprocessInformation and BPUIOInformation in BPUFunctionReport for the OCBC card are depicted in Figure B.16 and Figure B.17 respectively.

© ISO/IEC 2019 – All rights reserved **63**

**ISO/IEC FDIS 24761:2019(E)**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | |  |  |  |  | | | |  |
|  |  | | | |  |  |  |  | | | |
|  |  |  | | |  |  |  |  |  | | |
|  |  |  |  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  | | |
|  |  |  |  |  |  |  |  |  |  | | |
|  |  |  |  |  |  |  |  |  |  | | |
|  |  |  |  | |  |  |  |  |  | | |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | | | | |  |  |  |  |  |  |  |

**Figure B.15 — Examples of BPUFunctionReports for an OCBC model in declaration expression 64** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  | |
|  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |

**Figure B.16 — Examples of BPUSubprocessInformation for an OCBC card**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  |  |  |  |  | | |
|  |  | |  |  |  |  |  |  | |
|  |  | |  |  |  |  |  |  | |
|  |  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  | | |
|  | | |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | | |

**Figure B.17 — Examples of BPUIOInformation for an OCBC card**

**B.1.3.2.3 Case of role expression**

If the streams from/to the sensor device and that from the OCBC card are indexed as in Figure B.18 for enrolment and Figure B.19 for verification, then the BPUFunctionReport of the sensor device and that of the OCBC card are expressed as in Figure B.20. In Figure B.18 and Figure B.19, IOIndex means subprocess IO index.

© ISO/IEC 2019 – All rights reserved **65**

**ISO/IEC FDIS 24761:2019(E)**

**Figure B.18 — A biometric enrolment process of an OCBC model and an example of indexing for role expression**

**66** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**Figure B.19 — A biometric verification process of an OCBC model and an example of indexing for role expression**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | |  |  |  | | | | | |
|  |  | | | | |  |  |  |  | | | | |
|  |  |  | | | |  |  |  |  |  | | | |
|  |  |  | | | |  |  |  |  |  | | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  | | | |
|  | | | | | |  |  |  |  |  |  | | |
|  |  |  |  |  |  |  |  |  |  |  |  | | |
|  |  |  |  |  |  |  |  |  |  |  |  | | |
|  |  |  |  |  |  |  |  |  |  |  |  | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | | | | | |

**Figure B.20 — Examples of BPUFunctionReports for an OCBC model in role expression** © ISO/IEC 2019 – All rights reserved **67**

**ISO/IEC FDIS 24761:2019(E)**

**B.1.3.3 In enrolment process**

Biometric reference is stored to an OCBC card in this process. A BRT certificate is issued to the biometric reference. It or its referrer is to be stored in brtCertificateInformation of ACBioContentInformation.

**B.1.3.4 In execution process**

On an execution of biometric verification, three inputs are given to an OCBC card in addition to the processed biometric sample; the first is a control value from the validator, the second is the BPU IO index to the input of processed biometric sample from the sensor device, the third is the BPU IO index to the output from the OCBC card. Called with PERFORM BIOMETRIC OPERATION command, which is specified in ISO/IEC 7816-11, with parameters including the above thee, the OCBC digitally signs the whole field of the type ACBioContentInformation to get the ACBio instance and returns it together with the result of biometric verification as depicted in Figure B.21 when declaration expression is used. When role expression is used, the triple of 5, 6, and 7, indexes of executed subprocesses, is replaced with 2 of executionIndex, 5, the subprocess IO index for input, is replaced with 3, and 8, the subprocess IO index for output, is replaced with 4 (see Figure B.19 and Figure B.20).



**Figure B.21 — ACBio instance generation on an OCBC card on an execution of biometric verification**

**68** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

**B.1.3.5 An example of protocol**

In this example, it is assumed that all of the subprocesses of biometric verification are done at the claimant and also that there is a system at the claimant which sends and receives messages to/from the he system of the validator, sensor device, and OCBC card, as shown in Figure B.22.

**Key**

1 to 13 order of protocol execution

**Figure B.22 — An example of protocol for an OCBC model**

The following shows an example of the protocol for this OCBC model:

With the sensor device in place of the biometric device, the OCBC card in place of the STOC card, and sensor-and-comparator class in place of storage-and-others class, execute steps 1) to 5) in the same way as in the protocol described in B.1.2.5. Then,

6) The system of the claimant decides the hash algorithm and the signature algorithm, and sends the validator's control value, the hash algorithm, the signature algorithm, and the BPU IO index for the output data (biometric processed sample) to request execution of data capture, intermediate signal processing, and final signal processing, and generation of an ACBio instance to the sensor device.

7) The sensor device captures biometric information from the claimant and generates the processed biometric sample through the data capture, intermediate signal processing, and final signal processing subprocesses. The sensor device generates an ACBio instance by the following procedures.

a) Restore the BPU Information block and set it to bpuInformation of ACBioContentInformation. b) Set the validator's control value to controlValue of ACBioContentInformation.

© ISO/IEC 2019 – All rights reserved **69**

**ISO/IEC FDIS 24761:2019(E)**

c) Generate the biometric process block as follows;

1a) (The case of declaration expression used for BPU report) Set the subprocess indexes corresponding to the subprocesses executed at the sensor device to executedProcessIndexList. In this case, the subprocess indexes corresponding to data capture, intermediate signal processing, and final signal processing are set in executedProcessIndexList.

1b) (The case of role expression used for BPU report) Set the executionIndex in executionInformationList in BPUFunctionReportRoleSingle corresponding to the execution of the functions at the sensor device to executedProcessIndexList. If BPUFunctionReportRoleSingle is expressed as in Figure B.20, 1 is set as the only one member of executedProcessIndexList.

2) To make bpuOutputExecutionInformationList field, the following should be done. Set the value processed-data and the value sample respectively to processedLevel and purpose of dataType. Set the BPU IO index, assigned to the output data of the sensor device, to bpuIOIndex. Set the subprocess IO index of the output data from the final signal processing subprocess to subprocessIOIndex. Set the pair of the hash value of the processed biometric sample generated in the sensor device and the hash algorithm to hash.

d) Generate SignedDataACBio of the data generated as in a), b) and c), using the digital signature algorithm selected in (5).

8) The sensor device sends the processed biometric sample and the ACBio instance to the system of claimant.

9) The system of the claimant sends the processed biometric sample received from the sensor device, the validator's control value, the hash algorithm and signature algorithm selected in (6), the BPU IO index assigned to the processed biometric sample, and the BPU IO index assigned to the comparison decision of OCBC card to request execution of storage, comparison and decision subprocesses to the OCBC card.

10) The OCBC card receives the processed biometric sample and executes storage, comparison and decision subprocesses. The OCBC card also generates the ACBio instance (see B.1.3.4 for details).

11) The OCBC card sends the output data of the decision subprocess and the ACBio instance to the system of the claimant.

12) The system of the claimant sends the comparison decision and the two ACBio instances to the system of the validator.

13) The system of the validator receives the comparison decision and the two ACBio instances. The validator validates the results with the following procedures;

a) Validate the integrity of each ACBio instance by signature verification. It is also checked whether the digital signature algorithm satisfies the policy or not.

b) Validate the correspondence of the control value originally given by the validator and the control value of each ACBio instance.

c) Validate the validity of biometric reference used checking the BRT certificate in the ACBio instance generated by the OCBC card, if necessary.

d) Check whether the whole process of biometric verification executed satisfies the policy of biometric capability class or not by checking executedProcessIndexList in the biometric process block with reference to the BPU report of the two ACBio instances. If declaration expression is used, the subprocess indexes (specified in functionDefinition in the BPU report) of executed subprocesses are set in executedProcessIndexList in the biometric process blocks of the two ACBio instances. Checking the correspondence of subprocess indexes and subprocessName of functionDefinition, the validator can conclude that sensor-and-comparator

**70** © ISO/IEC 2019 – All rights reserved

**ISO/IEC FDIS 24761:2019(E)**

class configuration was used for biometric verification (see shaded parts of two biometric process blocks in Figure B.23). If role expression is used, Figure B.24 illustrates an example of validation process. The validator can know that the left ACBio instance comes from a BPU of sensor BPU role with output of processed biometric sample. This is known because the value 1 in executedProcessIndexList in biometric process block refers to the ExecutionInformation of BPU Function Report in Figure B.16 and this ExecutionInformation contains the information of the output of this BPU. Similarly, the validator can know that the right ACBio instance in Figure B.24 comes from a BPU of comparator BPU role with input of processed biometric reference and output of comparison decision. Then the validator can know that the data flow between these two BPUs is consistent, ie processed biometric sample. The validator can conclude that the two BPUs configure sensor-and-comparator class.

e) Validate the consistency of the input data and the output data transmitted between BPUs. First the validator has to find the same BPU IO index used in bpuInputExecutionInformationList or bpuOutputExecutionInformationList from the biometric process blocks in the two ACBio instance. In Figure B.23 and Figure B.24, the bold arrow shows the correspondence of the same BPU IO index between the two ACBio instances. By comparing the contents of dataType, bpuIOIndex, and hashValue of bpuOutputExecutionInformationList in the biometric process block of the ACBio instance generated by the sensor device and those of bpuInputExecutionInf ormationList in the biometric process block of the ACBio instance generated by the OCBC card, the validator can conclude the consistency of the data flow between the two BPUs (see four thin arrows between biometric process blocks in Figure B.23 and Figure B.24).

Figure B.23 illustrates the validation process of biometric verification process when declaration expression is used. Figure B.24 is for the case of role expression used. In Figure B.23 and Figure B.24, the indexes given in Figure B.14 and Figure B.19 are used respectively.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |  |  |  | | | | | |
|  |  | | |  |  | |  |  |  |  | | |  |  |
|  |  | | | |  | |  |  |  |  | | | | |
|  |  |  | | | | |  |  |  |  |  | | | |
|  |  |  | | | | |  |  |  |  |  | | | |
|  |  | | | |  | |  |  |  |  | | | |  |
|  |  |
|  |  | | | | | |  |  |  |  | | | |  |
|  |  |  | | | | |  |  |  |  |  | | | |
|  |  |  |  | | | |  |  |  |  |  |  | | |
|  |  |  |  | | | |  |  |  |  |  |  | | |
|  |  |  | | | | |  |  |  |  |  | | | |
|  |  |  | |  | | |  |  |  |  |  | |  | |
|  |  |  | |  |  | |  |  |  |  |  | |  |  |
|  |  |  |  |  | |
|  |  |  | |  |  | |  |  |  |  |  | |  |  |
|  |  |  |  |  | |
|  |  |  | |  | | |  |  |  |  |  | |  | |
|  |  |  | |  | | |  |  |  |  |  | |  | |
|  |  |  | |  | |  |  |  |  |  |  | |  | |
|  |  |  | |  |  | |  |  |  |  |  | |  |  |
|  |  |  |  |  | |
|  |  |  | |  |  | |  |  |  |  |  | |  |  |
|  |  |  |  |  | |
|  |  |  | |  |  | |  |  |  |  |  | | | |
|  | | | | | | |  |  |  |  |  | |  | |
|  |  |  | |  |  | |  |  |  |  |  | |  |  |
|  |  |  | |  |  | |  |  |  |  |  | |  | |
|  |  |  | |  |  | |  |  |  |  |  | |  | |
|  |  |  | |  |  | |  |  |  |  |  | |  | |
|  |  |  | |  |  | |  |  |  |  |  | |  |  |
|  |  |  | |  |  | |  |  |  |  |  | |  |  |
|  |  |  | |  |  | |  |  |  |  | | | | |
|  |  |  | |  |  | |  |  |  |  |  | |  |  |
|  |  |  | |  |  | |  |  |  | | | | | |

**Figure B.23 — Validation of biometric verification for an OCBC model when declaration expression is used**

© ISO/IEC 2019 – All rights reserved **71**

**ISO/IEC FDIS 24761:2019(E)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | |  |  |  | | | | | |
|  |  | |  |  | |  |  |  |  | |  |  | |
|  |  | | |  | |  |  |  |  | | |  | |
|  |  |  | | | |  |  |  |  |  | | | |
|  |  |  | | | |  |  |  |  |  | | | |
|  |  | | |  | |  |  |  |  | | |  | |
|  |  |
|  |  | | |  | |  |  |  |  | | |  | |
|  |  |  | | | |  |  |  |  |  | | | |
|  |  |  | | | |  |  |  |  |  | | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | | |  |  |  |  |  |  | | |
|  |  |  |  | |  |  |  |  |  |  |  | |  |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  | | | |
|  | | | | | |  |  |  |  |  |  | | |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  | |  |  |  |  |  |  | | |
|  |  |  |  |  | |  |  |  |  |  |  | | |
|  |  |  |  |  | |  |  |  |  |  |  | | |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  | |  |  |  |  | | | | |
|  |  |  |  |  | |  |  |  |  |  |  |  | |
|  |  |  |  |  | |  |  |  | | | | | |

**Figure B.24 — Validation of biometric verification for a STOC model when role expression is used**

**B.2 Relation among BioAPI, CBEFF, and ACBio**

In this B.2, the relation among CBEFF, BioAPI, and ACBio is shown using an example of an STOC model, though the use of CBEFF and BioAPI is not mandatory for this document.

Assume that this STOC model is as described in B.1.1. Figure B.25 illustrates the relation among BioAPI, CBEFF, and ACBio. In Figure B.23, APIs such as BioAPI\_Init, BioAPI\_BSPLoad, BioAPI\_BSPAttach, etc. are omitted.

**72** © ISO/IEC 2019 – All rights reserved