Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

H.812

(11/2017)

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ
И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Мультимедийные услуги и приложения электронного здравоохранения – Системы персонального медицинского обслуживания

Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг

Рекомендация МСЭ-Т H.812

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-R СЕРИИ H

АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

ХАРАКТЕРИСТИКИ ВИДЕОТЕЛЕФОННЫХ СИСТЕМ	H.100–H.199
ИНФРАСТРУКТУРА АУИДОВИЗУАЛЬНЫХ СЛУЖБ	
Общие положения	H.200–H.219
Мультиплексирование и синхронизация при передаче	H.220–H.229
Системные аспекты	H.230–H.239
Процедуры связи	H.240–H.259
Кодирование подвижных видеоизображений	H.260–H.279
Сопутствующие системные аспекты	H.280–H.299
Системы и оконечное оборудование для аудиовизуальных услуг	H.300–H.349
Архитектура услуг справочника для аудиовизуальных и мультимедийных услуг	H.350–H.359
Качество архитектуры обслуживания для аудиовизуальных и мультимедийных услуг	H.360–H.369
Телеприсутствие	H.420–H.429
Дополнительные услуги для мультимедиа	H.450–H.499
ПРОЦЕДУРЫ МОБИЛЬНОСТИ И СОВМЕСТНОЙ РАБОТЫ	
Обзор мобильности и совместной работы, определений, протоколов и процедур	H.500–H.509
Мобильность для мультимедийных систем и услуг серии H	H.510–H.519
Приложения и услуги мобильной мультимедийной совместной работы	H.520–H.529
Защита мобильных мультимедийных систем и услуг	H.530–H.539
Защита приложений и услуг мобильной мультимедийной совместной работы	H.540–H.549
АВТОМОБИЛЬНЫЕ ШЛЮЗЫ И ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ (ИТС)	
Архитектура автомобильных шлюзов	H.550–H.559
Интерфейсы автомобильных шлюзов	H.560–H.569
ШИРОКОПОЛОСНЫЕ И МУЛЬТИМЕДИЙНЫЕ TRIPLE-PLAY УСЛУГИ	
Предоставление широкополосных мультимедийных услуг по VDSL	H.610–H.619
Усовершенствованные мультимедийные услуги и приложения	H.620–H.629
Приложения повсеместно распространенных сенсорных сетей и интернет вещей	H.640–H.649
МУЛЬТИМЕДИЙНЫЕ УСЛУГИ IPTV И ПРИЛОЖЕНИЯ ДЛЯ IPTV	
Общие аспекты	H.700–H.719
Оконечные устройства IPTV	H.720–H.729
Промежуточное ПО для IPTV	H.730–H.739
Обработка событий приложений IPTV	H.740–H.749
Метаданные IPTV	H.750–H.759
Структуры мультимедийных приложений IPTV	H.760–H.769
Обнаружение услуги IPTV вплоть до ее использования	H.770–H.779
Цифровой информационный экран	H.780–H.789
МУЛЬТИМЕДИЙНЫЕ УСЛУГИ И ПРИЛОЖЕНИЯ ЭЛЕКТРОННОГО ЗДРАВООХРАНЕНИЯ	
Системы персонального медицинского обслуживания	**H.810–H.819**
Проверка соответствия на функциональную совместимость систем персонального медицинского обслуживания (HRN, PAN, LAN, TAN и WAN)	H.820–H.859
Услуги обмена мультимедийными данными электронного здравоохранения	H.860–H.869

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-T.

Рекомендация МСЭ-Т H.812

Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг

Резюме

В Руководящих указаниях по проектированию Continua (CDG) определена структура исходных стандартов и критерии, необходимые для обеспечения функциональной совместимости устройств и данных, используемых в услугах подключенных систем персонального медицинского обслуживания. В них также содержатся руководящие указания по проектированию (DG), в которых дополнительно уточняются исходные стандарты или спецификации путем сокращения вариантов или добавления недостающих функций в целях повышения функциональной совместимости.

В Рекомендации МСЭ-Т H.812 содержится обзор интерфейса услуг (Services-IF), общие руководящие указания по проектированию для всех классов сертифицированных возможностей (CCC) интерфейса услуг и руководящие указания по проектированию для персонального медицинского шлюза (PHG) с поддержкой разрешений и CCC услуг.

Руководящие указания по проектированию устройств, которые поддерживают следующие классы сертифицированных возможностей (CCC), определены в отдельных Рекомендациях, а именно:

– возможность загрузки результатов наблюдений – в МСЭ-Т H.812.1 (2017 год);

– вопросники – в МСЭ-Т H.812.2 (2017 год);

– возможность обмена возможностями – в МСЭ-Т H.812.3 (2017 год);

– возможность поддержки аутентифицированного постоянного сеанса – в МСЭ-Т H.812.4 (2017 год).

Рекомендация МСЭ-Т H.812 входит в серию Рекомендаций МСЭ-Т H.810 "Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания", которая охватывает следующие области:

– МСЭ-Т H.810 – Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: введение;

– МСЭ-Т H.811 – Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс персональных медицинских устройств;

– МСЭ-Т H.812 – Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг (настоящий документ, содержащий руководящие указания по проектированию);

– МСЭ-Т H.812.1 – Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг: возможность загрузки результатов наблюдений;

– МСЭ-Т H.812.2 – Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг: вопросники;

– МСЭ-Т H.812.3 – Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг: возможность обмена возможностями;

– МСЭ-Т H.812.4 – Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг: возможность поддержки аутентифицированного постоянного сеанса;

МСЭ-Т H.813 – Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс информационной системы здравоохранения.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т H.812	29.11.2015 года	16-я	11.1002/1000/12653
2.0	МСЭ-Т H.812	14.07.2016 года	16-я	11.1002/1000/12913
3.0	МСЭ-Т H.812	29.11.2017 года	16-я	11.1002/1000/13415

Ключевые слова

CDG, Руководящие указания по проектированию Continua, информационные системы здравоохранения, подключенные системы персонального медицинского обслуживания, персональные медицинские устройства, услуги.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

Содержание

Перечень таблиц

Стр.

Перечень рисунков

0 Введение

В Руководящих указаниях по проектированию Continua (CDG) определена структура исходных стандартов и критерии, необходимые для обеспечения функциональной совместимости устройств и данных, используемых в услугах подключенного персонального медицинского обслуживания. В них также содержатся дополнительные руководящие указания по проектированию (DG), в которых дополнительно уточняются исходные стандарты или спецификации путем сокращения вариантов или добавления недостающих функций в целях повышения функциональной совместимости.

В настоящей Рекомендации содержатся дополнительные руководящие указания по планированию функциональной совместимости, в которых уточняются или ограничиваются варианты либо добавляются функции, отсутствующие в исходных стандартах или спецификациях.

В настоящей Рекомендации содержится обзор интерфейса услуг (Services-IF), общие руководящие указания по проектированию для всех классов сертифицированных возможностей (CCC) интерфейса услуг и руководящие указания по проектированию для персонального медицинского шлюза (PHG) с поддержкой разрешений и CCC услуги "Здоровье и физическая форма".

Руководящие указания по проектированию, которые поддерживают следующие классы сертифицированных возможностей (CCC), определены в отдельных Рекомендациях, а именно:

– [ITU-T H.812.1] *Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг: возможность загрузки результатов наблюдений*;

– [ITU-T H.812.2] *Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг: вопросники*;

– [ITU-T H.812.3] *Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг: возможность обмена возможностями*;

– [ITU-T H.812.4] *Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг: возможность поддержки аутентифицированного постоянного сеанса*.

Настоящая Рекомендация входит в серию Рекомендаций МСЭ-Т H.810 "Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания". Более подробную информацию см. в [ITU-T H.810].

0.1 Структура Рекомендации

Настоящий документ, содержащий руководящие указания по проектированию, построен следующим образом.

Разделы с 0 по 5: **Введение и терминология –** В данных разделах представлена специальная информация по интерфейсу услуг, способствующая пониманию структуры проектных спецификаций.

Раздел 6: **Обзор интерфейса услуг** – В данном разделе представлен обзор CCC интерфейса услуг.

Раздел 7: **Сценарии использования** – В данном разделе приведены практические примеры.

Раздел 8: **Поведенческая модель** – В данном разделе представлен обзор последовательностей взаимодействия в общих CCC интерфейса услуг и обобщены типичные виды взаимодействия, ограничения и исключения.

Раздел 9: **Реализация –** В данном разделе подробно описывается использование содержания общей полезной нагрузки и приводится сравнение простого протокола доступа к объектам (SOAP) и методики транспортирования на основе передачи репрезентативного состояния (REST) в общих классах сертифицированных возможностей интерфейса услуг.

0.2 Выпуски и версии руководящих указаний

Информация по выпускам и версиям приведена в пункте 0.2 [ITU-T H.810].

0.3 Изменения и дополнения

Изменения и дополнения, внесенные в настоящий выпуск руководящих указаний по проектированию, приведены в пункте 0.3 [ITU-T H.810].

Рекомендация МСЭ-Т H.812

Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: интерфейс услуг

1 Сфера применения

В настоящем документе, содержащем руководящие указания по проектированию, в основном рассматривается следующий интерфейс:

– **интерфейс услуг** – Интерфейс между персональным медицинским шлюзом (PHG) и услугами.

Данный интерфейс определен в архитектуре Continua, описание которой приведено в разделе 6 [ITU-T H.810], и представлен на рисунке 1-1.

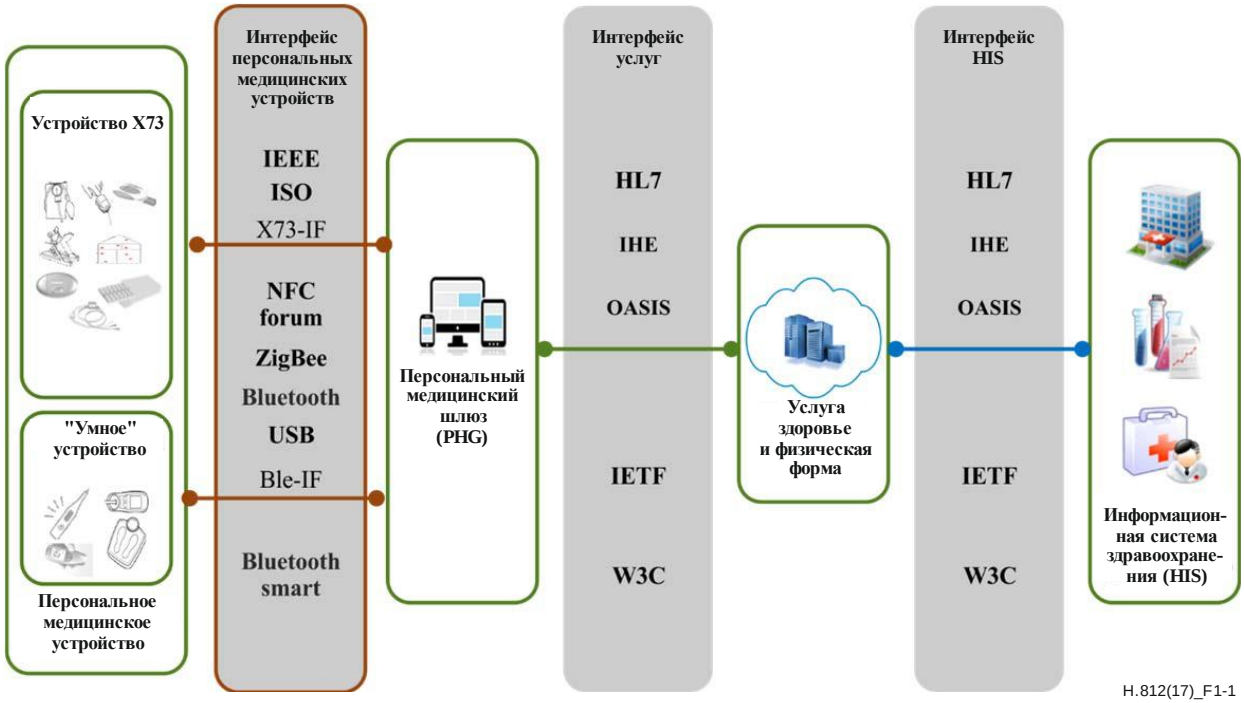

Рисунок 1-1 – Интерфейс услуг в архитектуре Continua

С интерфейсом услуг связан ряд классов сертифицированных возможностей (ССС). В настоящей Рекомендации содержатся руководящие указания по планированию функциональной совместимости, применимые к нескольким ССС. Одним из примеров являются руководящие указания по планированию функциональной совместимости систем безопасности. Кроме того, в настоящей Рекомендации содержатся руководящие указания по проектированию для PHG с поддержкой разрешений и ССС интерфейса услуг. Эти ССС можно группировать с несколькими другими ССС, связанными с интерфейсом услуг, такими как ССС загрузки результатов наблюдений или ССС поддержки вопросников.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно

публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

[ITU-T H.810] Рекомендация МСЭ-Т H.810 (2017 год), *Руководящие указания по планированию функциональной совместимости для подключенных систем персонального медицинского обслуживания: введение*

Другие справочные документы указаны в разделе 2 [ITU-T H.810].

3 Определения

В настоящих руководящих указаниях по проектированию используются термины, определенные в [ITU-T H.810].

4 Сокращения и акронимы

В настоящих руководящих указаниях по проектированию используются сокращения и акронимы, определенные в [ITU-T H.810].

5 Соглашения по терминологии

В настоящих руководящих указаниях по проектированию применяются соглашения, определенные в [ITU-T H.810].

6 Архитектура

В данной сквозной (E2E) эталонной архитектуре интерфейс услуг соединяет персональный медицинский шлюз (PHG) с услугой "Здоровье и физическая форма" (HFS). На рисунке 6-1 показан интерфейс услуг в сквозной архитектуре Continua, а на рисунке 6-2 – пример интерфейса услуг.

Настоящие руководящие указания по проектированию интерфейса услуг направлены на обеспечение возможности совместимого обмена информацией через интерфейс услуг. Для PHG и услуги "Здоровье и физическая форма" определен набор классов сертифицированных возможностей, относящихся к интерфейсу услуг, позволяющий обеспечить функциональную совместимость для ряда различных сценариев использования, включая загрузку результатов измерений, заполнение вопросников и выполнение команд.

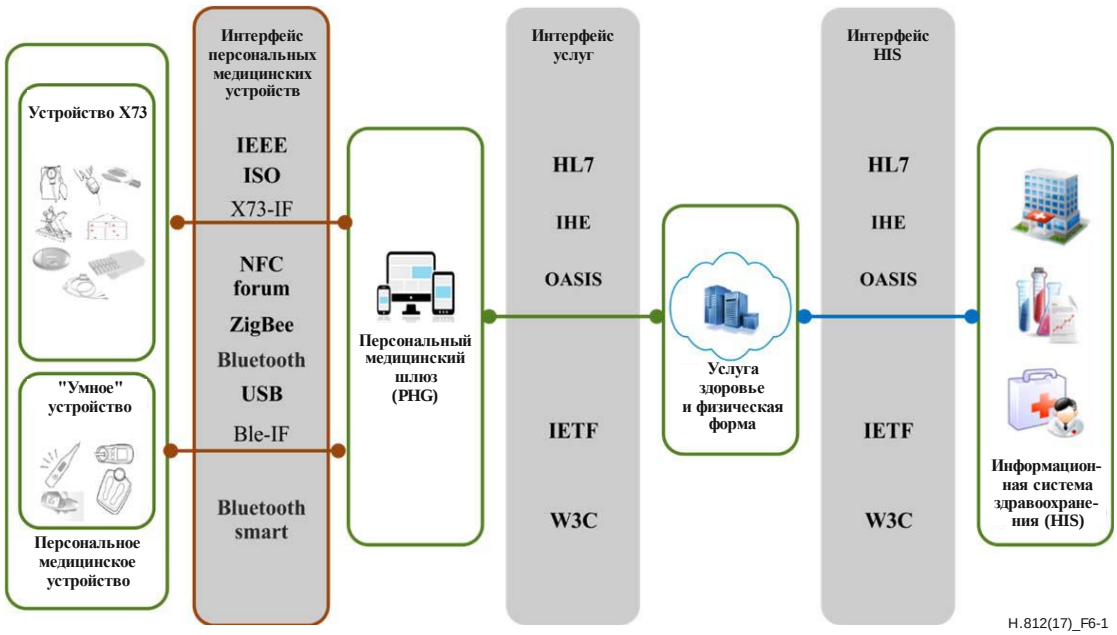

Рисунок 6-1 – Интерфейс услуг в сквозной архитектуре Continua

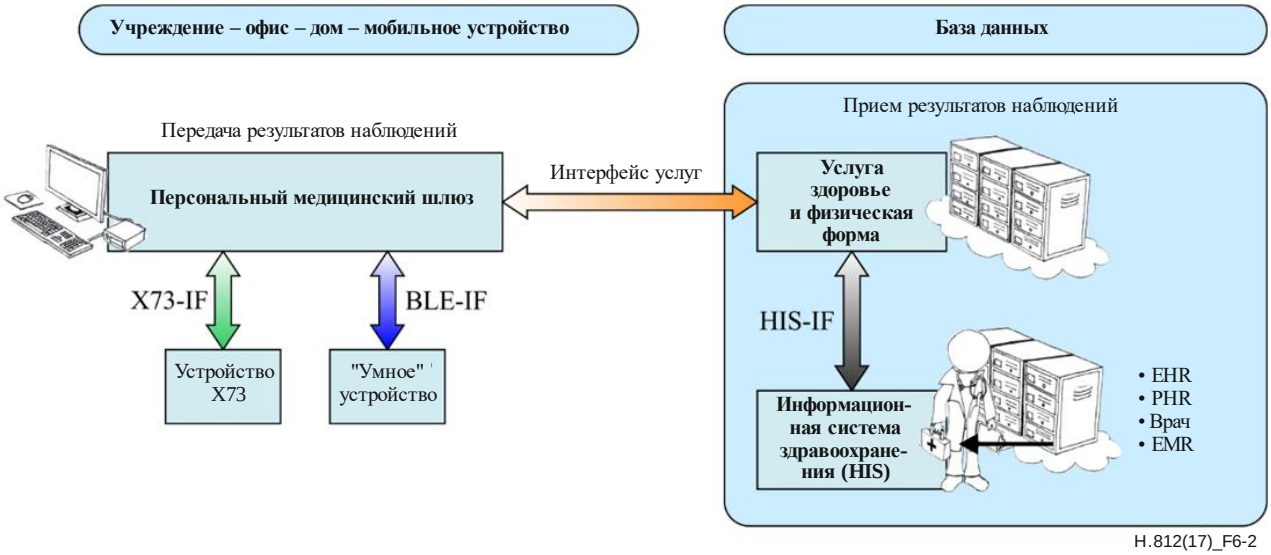

Рисунок 6-2 – Пример интерфейса услуг

Помимо интерфейса услуг сквозная эталонная архитектура определяет интерфейс информационной системы здравоохранения (HIS-IF). Интерфейс услуг предназначен для обеспечения обмена подробной информацией между PHG (как правило, ноутбук, планшет, мобильный телефон или встроенное устройство другого типа), который представляет собой устройство, находящееся в непосредственной близости от пользователя/пациента, и услугой "Здоровье и физическая форма" (как правило, облачная служба баз данных), которая собирает информацию о таких пользователях и делает ее доступной для дальнейшего использования. HIS-IF же предназначен для обеспечения обмена агрегированной информацией между двумя системами баз данных, например системой управления лечением заболеваний и системой электронных медицинских записей (EHR)[1]. Интерфейс информационной системы здравоохранения (HIS-IF) определен в [ITU-T H.813].

Предполагается также, что устройства PHG могут применяться в домашних условиях или в пользовательских приложениях, что налагает ряд ограничений на конструкцию интерфейса услуг. В связи с трудностями, возникающими в процессе обслуживания и/или модернизации этих устройств "в полевых условиях", PHG должны быть надежными, автономными и достаточно несложными. Это позволит поддерживать на минимальном уровне необходимые затраты, а также требования к техническому опыту эксплуатации и квалификации персонала. С учетом указанных соображений интерфейс услуг позволяет хранить большинство контекстных метаданных, связанных с обменом результатами наблюдений, вне устройств PHG.

С другой стороны, ожидается, что услугу "Здоровье и физическая форма" будет обеспечивать система, обладающая более широкими функциональными возможностями, например сервер или персональный компьютер. Таким образом целью разработки интерфейса услуг является решение связанных со сложностью и возможностью обслуживания проблем услуги "Здоровье и физическая форма", поскольку это означает, что данных проблем можно избежать на PHG.

Интерфейс услуг – это абстрактный канал, состоящий из одной или нескольких пар CCC, который соединяет приложение PHG с приложением услуги "Здоровье и физическая форма". В каждой паре CCC имеется компонент, размещенный в приложении "Здоровье и физическая форма", и компонент, размещенный в приложении PHG. Continua определяет классы сертифицированных возможностей по обе стороны интерфейса услуг.

Настоящая версия руководящих указаний по проектированию интерфейса услуг обеспечивает следующие классы сертифицированных возможностей:

---

[1] ПРИМЕЧАНИЕ. – В сквозной архитектуре как интерфейсы услуг, так и интерфейсы информационной службы здравоохранения (HIS) могут быть реализованы на устройстве, находящемся в непосредственной близости от пользователя/пациента (ПК, ноутбук, мобильный телефон и т. д.), для обмена информацией с учреждениями, географически удаленными от таких устройств. В руководящих указаниях не содержатся ограничения на развертывание классов сертифицированных возможностей на каком-либо конкретном оборудовании.

– загрузку результатов наблюдений из PHG в приложение услуги "Здоровье и физическая форма" двумя разными способами: посредством веб-услуг (SOAP) и посредством REST (данных) [ITU-T H.812.1];

– загрузку информации о разрешениях из PHG в приложение услуги "Здоровье и физическая форма" двумя разными способами: посредством веб-услуг (SOAP) и посредством REST (данных) [ITU-T H.812];

– загрузку подлежащих заполнению вопросников из приложения услуги "Здоровье и физическая форма" в PHG и заполненных вопросников из PHG в приложение услуги "Здоровье и физическая форма" [ITU-T H.812.2];

– обмен информацией (например, незапрашиваемыми командами) между приложением услуги "Здоровье и физическая форма" и PHG в течение аутентифицированного постоянного сеанса [ITU-T H.812.4];

– обмен поддерживаемой информацией о классе сертифицированных возможностей (обмен возможностями) между PHG и приложением услуги "Здоровье и физическая форма" в качестве средства поддержки других сценариев использования [ITU-T H.812.3].

PHG может поддерживать одно или несколько приложений, каждое из которых реализует один или несколько классов сертифицированных возможностей Continua. На рисунке 6-3 показан интерфейс услуг Continua между приложениями PHG и услуги "Здоровье и физическая форма", в которых реализованы все возможные классы сертифицированных возможностей интерфейса услуг.

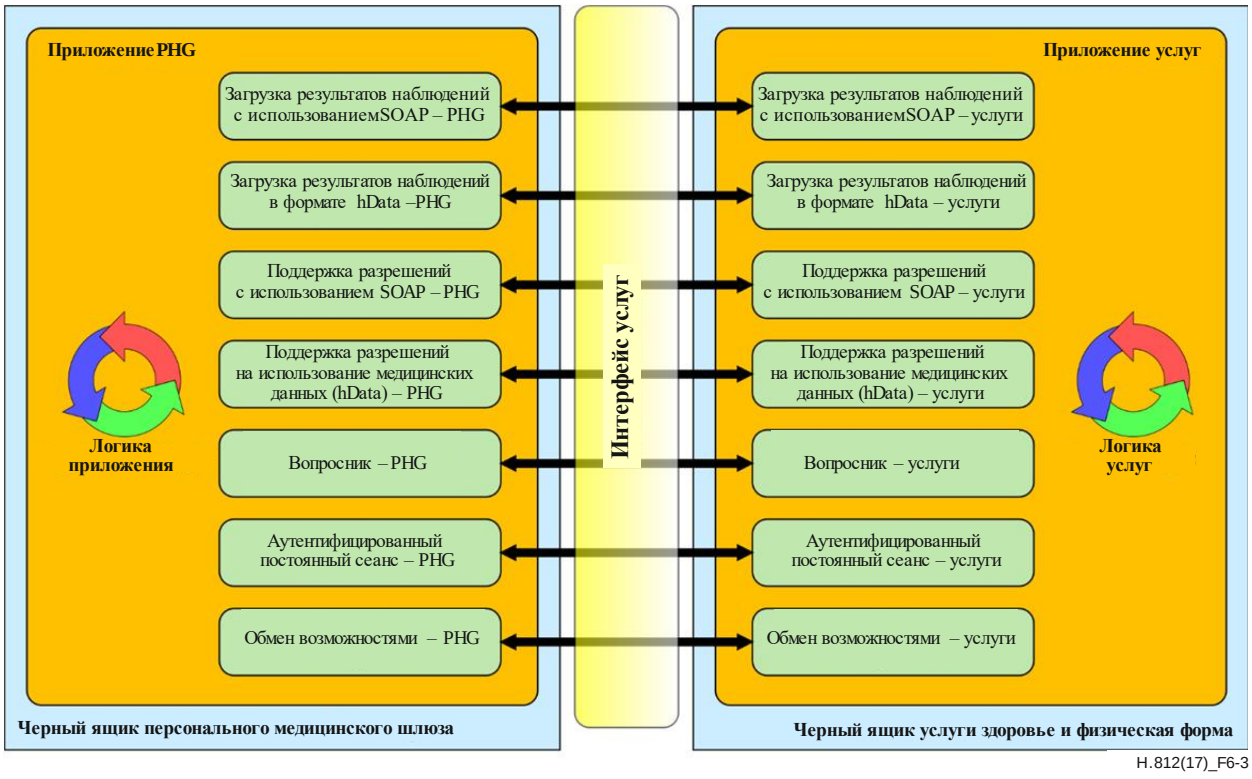

Рисунок 6-3 – Интерфейс услуг Continua: классы сертифицированных возможностей интерфейса услуг

Цель настоящих руководящих указаний – достаточно подробно определить поведение системы, чтобы достичь приемлемого уровня совместимости с конкретным сценарием использования. Сценарий использования заключен в класс сертифицированных возможностей (CCC). В руководящих указаниях содержатся нормативные положения о том, как функционирует сетевой интерфейс компонентов CCC. Для интерфейса услуг эти компоненты существуют в контексте приложений или услуг, размещаемых в PHG или в услуге "Здоровье и физическая форма".

Обычные платформы часто ограничивают способ взаимодействия приложений друг с другом, чтобы обеспечить стабильность платформы в целом. Такое ограниченное взаимодействие между

приложениями называется изоляцией (sandboxing). Для поддержки изолированных приложений в этой версии интерфейса услуг используется эталонная модель, определяющая приложение в качестве контейнера для одного или нескольких компонентов CCC. Взаимодействие между компонентами в приложении-контейнере не обусловлено нормативными требованиями и полностью зависит от разработчика приложения. Взаимодействие по интерфейсу услуг между CCC приложения в PHG и соответствующими CCC в услуге "Здоровье и физическая форма" является видимым и обусловлено нормативными требованиями для прохождения сертификации.

Эталонная модель позволяет работать в PHG или услуге "Здоровье и физическая форма" нескольким приложениям, но эти приложения взаимодействуют с другими приложениями только через сетевые интерфейсы. В настоящих руководящих указаниях приложения, работающие с услугой "Здоровье и физическая форма", часто называют услугами, поскольку услуги "Здоровье и физическая форма" обычно представляют собой платформы веб-услуг. Услуга "Здоровье и физическая форма" концептуально аналогична приложению PHG.

В настоящих руководящих указаниях рассматриваются механизмы, с помощью которых компоненты могут взаимодействовать друг с другом через внутренний интерфейс прикладного программирования (API). Будущие версии интерфейса услуг могут использовать эти механизмы для обеспечения функциональной совместимости между компонентами в составе приложения.

На рисунке 6-4 понятия эталонной модели интерфейса услуг используются для представления PHG, в котором два независимых приложения взаимодействуют с приложением, обеспечивающим предоставление услуг. Одно приложение PHG поддерживает три CCC, а другое – один CCC. К сетевым интерфейсам между PHG и услугой "Здоровье и физическая форма" предъявляются определенные нормативные требования. Взаимодействие между компонентами CCC в контейнере-приложении не нормируется и показано на рисунке красными пунктирными линиями; оно координируется средствами внутренней обработки приложения, которые в настоящих руководящих указаниях не рассматриваются.

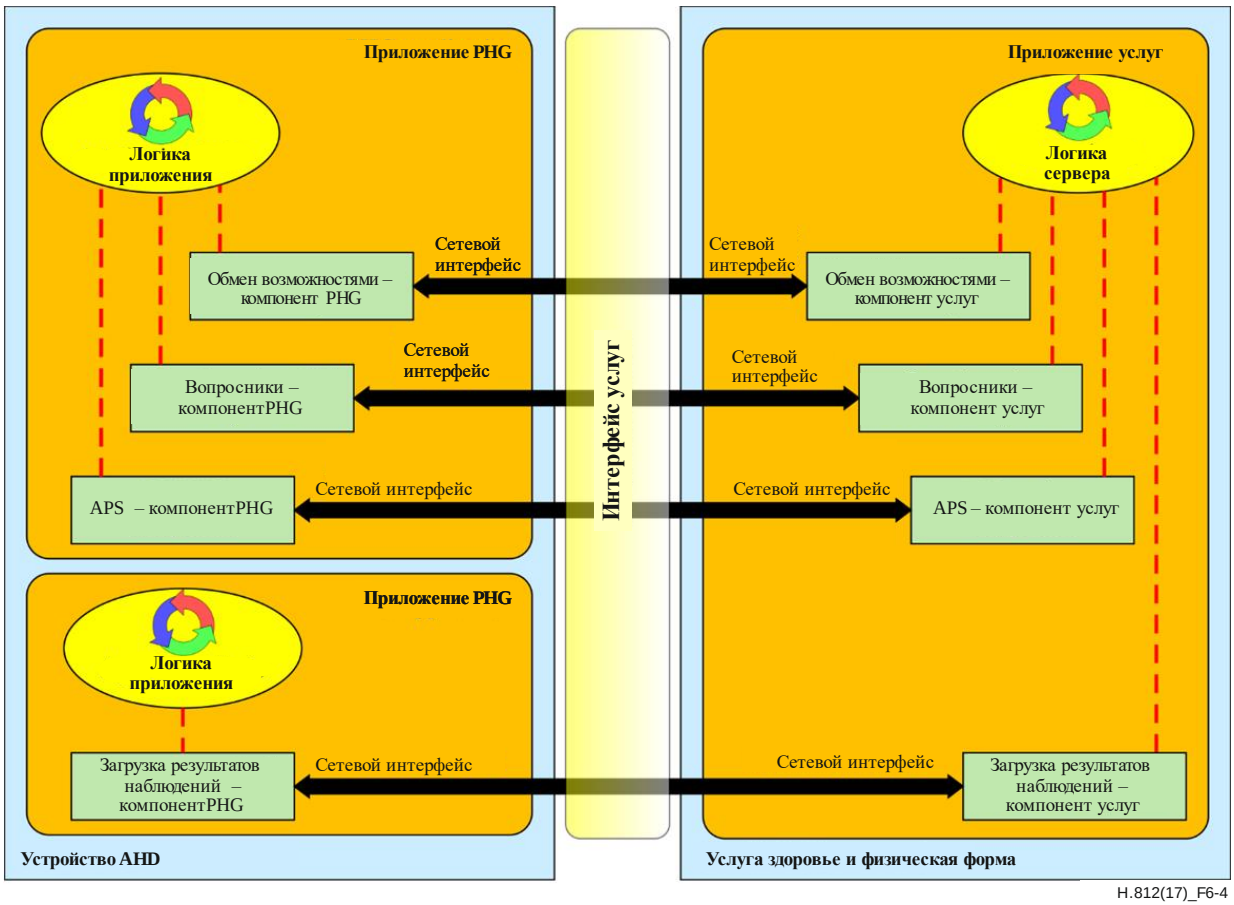

Рисунок 6-4 – Эталонная модель интерфейса услуг

Взаимодействие с использованием интерфейса услуг начинается с компонента обмена возможностями PHG. Этот компонент направляет запрос своему одноранговому компоненту услуги "Здоровье и физическая форма". В запросе услуге "Здоровье и физическая форма" предлагается указать различные поддерживаемые ею классы сертифицированных возможностей. Говоря простым языком, приложение PHG спрашивает данную услугу, что та умеет делать. Приложение услуги "Здоровье и физическая форма" отвечает на это перечислением поддерживаемых ею CCC. В сценарии, иллюстрируемом на рисунке 6-4, приложение услуги "Здоровье и физическая форма" сообщает: "Я поддерживаю обмен возможностями, вопросники, загрузку результатов наблюдений с использованием SOAP и аутентифицированные постоянные сеансы (APS)". Когда компонент "Обмен возможностями" приложения услуг отвечает приложению PHG, он обычно предоставляет PHG дополнительную информацию, такую как URL, которая позволяет приложению PHG сделать следующий шаг по взаимодействию с конкретным CCC. PHG, поддерживающий только загрузку результатов наблюдений с использованием SOAP, не нуждается в реализации обмена возможностями. Если PHG уже известно о возможностях услуги "Здоровье и физическая форма", то обмен возможностями не требуется.

7 Сценарии использования

7.1 Сценарий управления выдачей разрешений

Указания по выдаче разрешений – это документ, относящийся к методам действий в плане защиты конфиденциальности медицинских сведений о клиенте, который предоставляет или отказывает в предоставлении разрешения на доступ к индивидуально идентифицируемой медицинской информации (IIHI) [HL7 CDA IG].

Требование на выдачу разрешения для пользователя основывается на различных правилах, таких как Закон о переносимости и подотчетности в медицинском страховании (HIPAA), Директива ЕС 95/46 и т. д. Эти законы о конфиденциальности определяют и устанавливают особые права пациентов, касающиеся сбора, доступа, использования и раскрытия информации об их здоровье. Этими законами установлено, что разрешение пациента должно быть получено перед тем, как его/ее медицинская информация может быть доступна для использования, в том числе совместного. Например, пациенту могут предложить заполнить форму выдаваемого разрешения в процессе регистрации в лечебном учреждении (DMO). Эта форма выдачи разрешения включает подтверждение и/или подпись пациента под предварительно заданным набором принципов, определяющих, кому разрешен доступ к его/ее информации IHII, с какой целью и каким образом можно использовать эту информацию. В данном разделе описан процесс сбора и передачи принципов выдачи разрешений в электронной форме через интерфейс услуг. Цифровые формы разрешения упрощают процесс выдачи пациентами разрешений и способствуют их эффективному использованию. В качестве примеров разрешений пациентов можно привести общее согласие/отказ на предоставление IIHI, возможность отмены в чрезвычайной ситуации, ограничение доступа только исполнителями тех или иных функций (например, прямыми поставщиками медицинских услуг), использование специальных документов для конкретных исследовательских проектов и т. д.

В основном сценарии пациент определяет свой подход к выдаче разрешения во время или после регистрации в услуге "Здоровье и физическая форма". Точный порядок выдачи пациентом разрешения выходит за рамки настоящих руководящих указаний, однако он может включать информацию о выборе и возможной адаптации принципов выдачи разрешений по умолчанию с применением пользовательского интерфейса на его PHG, который преобразует соответствующую информацию в машиночитаемое представление принципов выдачи разрешений. Такого рода принципы, как правило, содержат ссылку на заинтересованные стороны, объекты данных и разрешенные или запрещенные действия. Приложение услуги "Здоровье и физическая форма", получившее разрешение конкретного пациента, хранит его и применяет к получаемым медицинским данным пациента.

В приведенных ниже сценариях использования основное внимание уделяется требованиям по управлению выдачей разрешений пациентами.

7.1.1 Загрузка разрешений на сервер

Иван Безымянный регистрируется, например, в лечебном учреждении (DMO), которое осуществляет дистанционное наблюдение за пациентами на дому и собирает информацию о состоянии здоровья с медицинских измерительных приборов, установленных у Ивана дома. При регистрации Иван

заполняет форму eConsent в приложении персонального медицинского шлюза (PHG). Форма eConsent состоит из вариантов ответов на вопросы о том, кто может получать доступ к различным видам жизненно важных показателей, собранных системой дистанционного наблюдения за пациентом, использовать их, обновлять и раскрывать их третьим лицам. После указания своих предпочтений Иван нажимает кнопку "Отправить" в своем телемедицинском центре. Тот составляет из его предпочтений указания по обеспечению конфиденциальности, основанные на стандарте HL7 CDA R2, которые пересылаются из PHG в DMO, предоставляющее услугу дистанционного наблюдения за пациентом. Затем эти указания по обеспечению конфиденциальности регулируют доступ к данным пациента в DMO, причем данные Ивана, передаваемые с его разрешения третьим лицам, могут содержать персональную медицинскую карту пациента (PHR), электронные медицинские записи (EHR) или электронные медицинские карты (EMR). Затем указания Ивана по обеспечению конфиденциальности ассоциируются с данными посредством идентификатора пациента.

7.1.2 Получение заполненного разрешения пациента с сервера

Возможно, Иван захочет обновить свои настройки конфиденциальности, например позволив получать доступ к его данным своему фитнес-тренеру, поскольку он по рекомендации медсестры из DMO недавно зарегистрировался в фитнес-службе. PHG дает ссылку на последнюю версию его указаний по обеспечению конфиденциальности. Иван нажимает на ссылку, и PHG извлекает с сервера последнюю версию указаний по обеспечению конфиденциальности и отображает ее Ивану.

7.1.3 Загрузка обновленных разрешений на сервер

Иван просматривает свои предпочтения в отношении конфиденциальности и обновляет их, если у его фитнес-тренера нет доступа к его данным. После обновления настроек конфиденциальности он нажимает кнопку "Отправить" на своем PHG, который составляет новые указания по обеспечению конфиденциальности, и отправляет этот документ в DMO. DMO заменяет старый документ обновленными указаниями по обеспечению конфиденциальности.

7.2 Сценарий правомерного использования разрешений

Правомерное использование разрешения пациента путем шифрования обеспечивает эффективную защиту конфиденциальной информации пациента и гарантирует, что контент (например, результаты наблюдений и ответы на вопросник) будет доступен для просмотра лишь тому получателю, для которого он предназначен. Это предотвратит возможность его просмотра другими лицами, работающими в той же организации, например административным персоналом. Перед расшифровкой контента услуга "Здоровье и физическая форма" с поддержкой разрешений должна провести оценку полученного разрешения. Оценка разрешения проводится для определения того, может ли получатель просматривать контент. Например, результатом выполнения оценки разрешения могут быть значения "Success-1" (успешно) или "Failure-0" (ошибка). Услуга "Здоровье и физическая форма", поддерживающая работу с разрешениями, должна правомерно использовать предпочтения, выраженные в документально оформленном разрешении.

7.2.1 Шифрование контента перед загрузкой

Иван Безымянный регистрируется в DMO, которое осуществляет дистанционное наблюдение за ним на дому и собирает информацию о состоянии своего здоровья с медицинских измерительных приборов, установленных у него дома. Кроме того, по рекомендации медсестры DMO он регистрируется у фитнес-тренера. Иван Безымянный хочет, чтобы фитнес-тренер просматривал данные о его физической активности, но не показания других измерительных приборов, таких как монитор артериального давления (BPM). Он настраивает свой PHG таким образом, чтобы медсестра из DMO имела доступ к показаниям BPM и датчиков физической активности, а фитнес-тренер – только к показаниям датчиков физической активности. Это достигается посредством шифрования.

7.3 Другие сценарии использования CCC

См. соответствующие сценарии использования CCC в разделе 6 следующих руководящих указаний по проектированию:

– [ITU-T H.812.1] – загрузка результатов наблюдений;

– [ITU-T H.812.2] – вопросник;

– [ITU-T H.812.3] – обмен возможностями;
– [ITU-T H.812.4] – аутентифицированный постоянный сеанс.

8 Поведенческие модели

Данный раздел охватывает:
– модель обмена сообщениями по интерфейсу услуг;
– модель безопасности CCC на основе REST;
– модель управления выдачей разрешений и правомерного использования CCC.

8.1 Общая модель обмена сообщениями по интерфейсу услуг

По соображениям безопасности и конфиденциальности, а также технической возможности реализации системы в целом интерфейс услуг требует, чтобы все соединения инициировались PHG. Это иллюстрируется на рисунке 8-1. Полезная нагрузка сообщений и другие особенности описаны в соответствующих руководящих указаниях по проектированию.

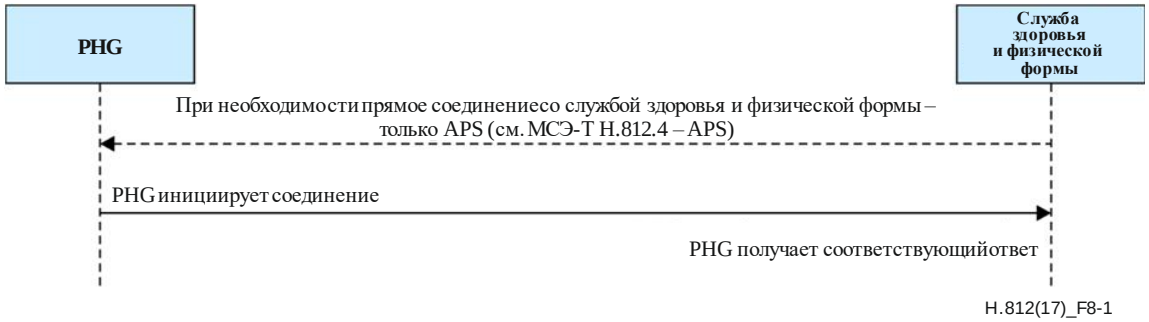

Рисунок 8-1 – Все соединения инициируются PHG

Если для обеспечения безопасности при передаче данных от пункта к пункту требуется безопасность транспортного уровня (TLS), то политике безопасности услуги "Здоровье и физическая форма" соответствует использование взаимной проверки сертификатов при квитировании TLS.

Когда требуется аутентификация:
– в случае SOAP для аутентификации используется маркер SAML 2.0; а
– в случае данных – маркер-носитель OAuth 2.0.

В настоящих Руководящих указаниях не определяется, как именно PHG получает эти маркеры, поскольку это зависит от доверительных отношений, установленных между сторонами. Приложение услуги "Здоровье и физическая форма" может поддерживать один или несколько параметров WS-Trust для получения маркеров SAML 2.0 или же поддерживать сервер авторизации OAuth 2.0, используя один или несколько типов разрешений, например предоставление разрешения доступа по регистрационным данным, определяемым паролем владельца ресурса. Если услуга "Здоровье и физическая форма" поддерживает и загрузку данных и SOAP, она может поддерживать обе услуги. В любом из этих случаев должна выполняться внештатная операция, когда пользователь PHG создает учетную запись определенного типа в приложении услуги "Здоровье и физическая форма", позволяющую клиенту получить эти маркеры. Служба маркеров услуги "Здоровье и физическая форма" генерирует маркеры, специфические для данного получателя, которые она проверяет при получении контента. С другой стороны, услуга "Здоровье и физическая форма" может потребовать, чтобы эти маркеры выдавались сторонней службой авторизации (например, CA), с которой PHG установил доверительные отношения. В этом случае услуга "Здоровье и физическая форма" позволяет проводить проверку клиента сторонней службе авторизации. Затем услуга "Здоровье и физическая форма" может решить либо принимать любой маркер, полученный от этой сторонней услуги, либо передавать полученный маркер сторонней службе авторизации для подтверждения, прежде чем принять его. Детали доверительных отношений определяются политикой безопасности услуги "Здоровье и физическая форма".

8.2 Общая модель безопасности для реализаций CCC на основе REST

На рисунке 8-2 представлена схема взаимодействия при авторизованных RESTful-транзакциях на основе передачи данных (REST) по HTTP. Авторизация осуществляется с помощью инфраструктуры авторизации OAuth 2.0 с применением в качестве типа разрешения авторизации по регистрационным данным, определяемым паролем владельца ресурса. Регистрационные данные, определяемые паролем владельца ресурса, обычно используются, когда существует высокая степень доверия между владельцем ресурса (пациентом) и клиентом (например, доверенным приложением, работающем на устройстве хостинга приложений). Будущие версии руководящих указаний по проектированию могут потребовать применения регистрационных данных других типов, основанных на сценариях, в которых для получения доступа к данным пациента могут использоваться сторонние (менее привилегированные) приложения. Регистрационные данные владельца ресурса используются для одиночного запроса и обмениваются на маркер доступа. Затем этот маркер доступа используется для выполнения RESTful-транзакций на ресурсе. Все взаимодействия с сервером авторизации и ресурсов выполняются в рамках защищенного сеанса с использованием [IETF RFC 4346].

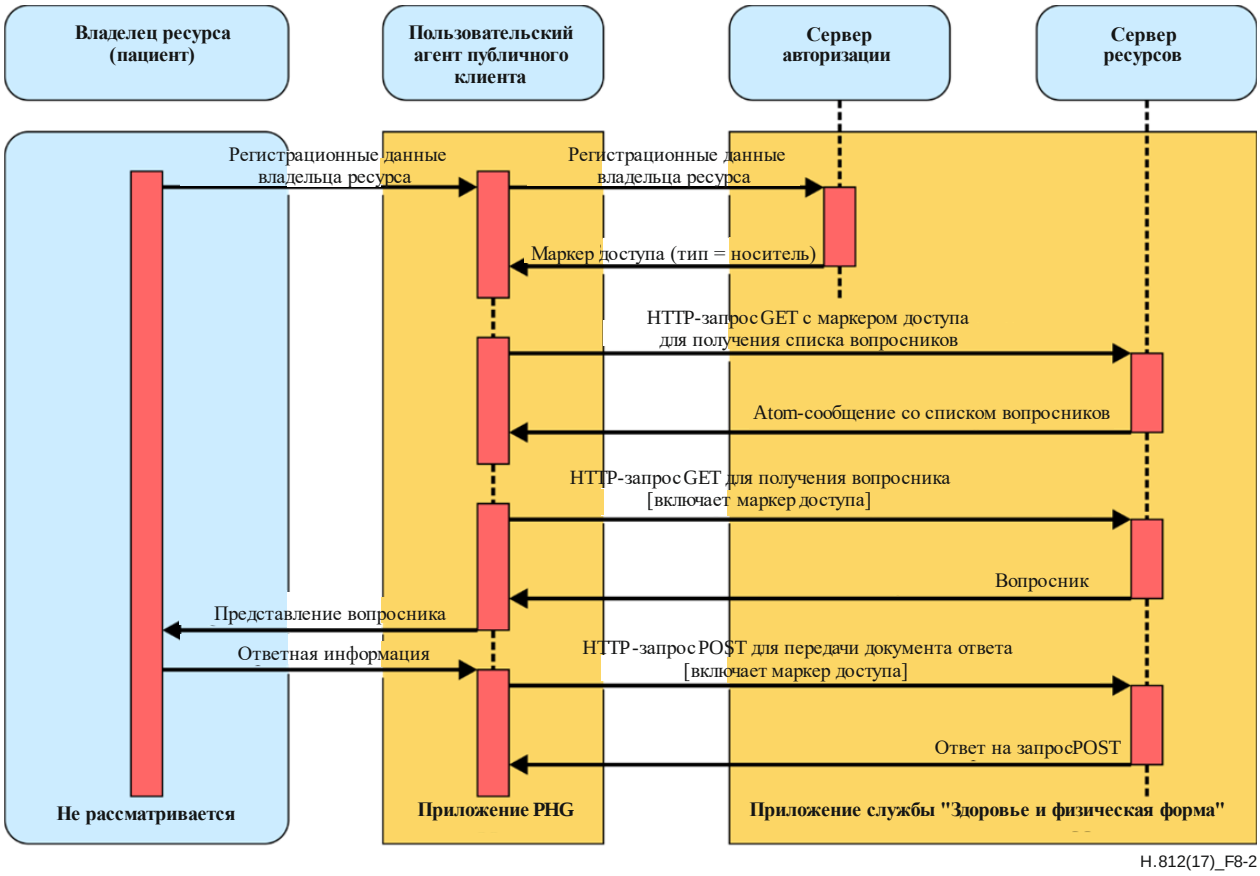

Рисунок 8-2 – Обеспечение безопасности при использовании авторизованного RESTful-CCC (сценарий с вопросником взят в качестве примера)

Руководящие указания по безопасности CCC на основе REST см. в таблицах B.1 и B.2.

8.3 Поведенческая модель управления выдачей разрешений

Определены следующие механизмы обмена для службы управления выдачей разрешений:

– создание *нового* документа, содержащего разрешение, на сервере;

– получение *готового* документа, содержащего разрешение, на сервере;

– загрузка *обновленного* документа, содержащего разрешение, на сервер.

На рисунке 8-3 показаны транзакции, связанные со сценариями управления выдачей разрешений, описанными в этом профиле контента.

Рисунок 8-3 – Транзакции между PHG и услугой "Здоровье и физическая форма", связанные с управлением выдачей разрешений

Руководящие указания по управлению выдачей разрешений см. в таблицах C.1 и C.2.

8.4 Поведенческая модель правомерного использования разрешений

Определена следующая функция для обеспечения правомерного использования разрешений:

– шифрование загружаемого контента.

Рисунок 8-4 иллюстрирует функцию обеспечения правомерного использования разрешений.

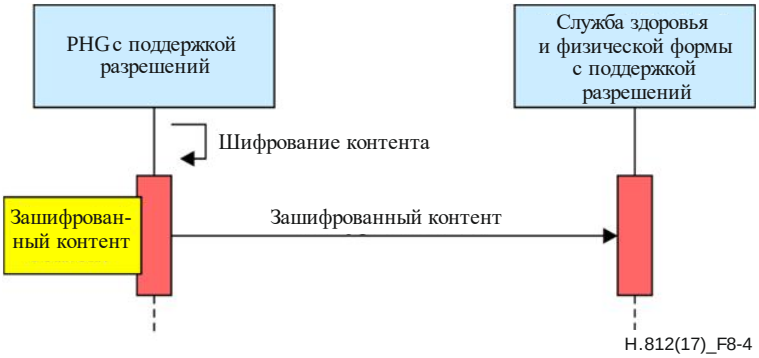

Рисунок 8-4 – Обеспечение правомерного использования разрешений в интерфейсе услуг

Руководящие указания по обеспечению правомерного использования разрешений см. в таблицах C.3 и C.4.

9 Реализация

9.1 Представление разрешений

Предпочтения, содержащиеся в разрешении, представляются в соответствии с руководством по реализации HL7 для CDA версии 2.0: указания по выдаче разрешений в [HL7 CDA IG].

Образцы файлов разрешений находятся в пакете образцов документов вышеупомянутого стандарта.

9.2 Транспортные протоколы

9.2.1 Транспортный протокол с использованием протокола передачи данных по HTTP

В данном случае в качестве транспортного протокола для обмена документами, содержащими разрешения, по интерфейсу услуг используется протокол передачи данных по HTTP при этом поддерживаются все сценарии использования, описанные в пунктах 7.1 и 7.2. Подробные требования по использованию протокола передачи данных по HTTP между PHG и услугой "Здоровье и физическая форма" приведены в Приложении A, в таблицах C.1, C.2, C.3 и C.4.

9.2.2 Транспортный протокол с использованием IHE XDR

В данном случае в качестве транспортного протокола для обмена документами, содержащими разрешения, по интерфейсу услуг используется [IHE ITI TFS XDR], при этом поддерживается только сценарий загрузки разрешений на сервер. Документально оформленные разрешения связаны с медицинской информацией (сообщение PCD-01) посредством идентификатора пациента. Таким образом конкретное разрешение ассоциируется с определенной медицинской информацией и тем самым управляет ее использованием.

9.3 Правомерное использование разрешений

9.3.1 Правомерное использование разрешений с использованием стандарта шифрования XML

В случае транспортного протокола с применением [IHE ITI TFS XDR] для обеспечения правомерного использования разрешений при помощи шифрования используется стандарт шифрования XML [W3C XMLENC]. Стандарт шифрования XML обеспечивает шифрование полезной нагрузки транзакций PCD-01 для конкретного получателя (например, врача или медицинской сестры) услуги "Здоровье и физическая форма" с поддержкой разрешений.

Стандарт шифрования XML используется для обеспечения правомерного использования разрешений при помощи шифрования.

9.3.2 Правомерное использование разрешений с применением IHE DEN

В случае применения транспортного протокола данных по HTTP правомерное использование разрешений обеспечивается с помощью профиля IHE DEN [IHE ITI DEN].

Приложение A

Обзор руководящих указаний

(Данное Приложение является неотъемлемой частью настоящей Рекомендации)

Классы сертифицированных возможностей услуг перечислены в таблице A.1.

Таблица A.1 – Классы сертифицированных возможностей

Наименование класса сертифицированных возможностей	Класс сертифицированных возможностей	Класс возможностей, обозначенный логотипом
Загрузка результатов наблюдений с использованием SOAP – PHG	Да	Да
Загрузка результатов наблюдений с использованием SOAP – услуга "Здоровье и физическая форма"	Да	Да
Загрузка результатов наблюдений с использованием данных – PHG	Да	Да
Загрузка результатов наблюдений с использованием данных – услуга "Здоровье и физическая форма"	Да	Да
Поддержка разрешений с использованием SOAP – PHG	Да	Да
Поддержка разрешений с использованием SOAP – услуга "Здоровье и физическая форма"	Да	Да
Поддержка разрешений с использованием данных – PHG	Да	Да
Поддержка разрешений с использованием данных – услуга "Здоровье и физическая форма"	Да	Да
Вопросник – PHG	Да	Да
Вопросник – услуга "Здоровье и физическая форма"	Да	Да
Обмен возможностями – PHG	Да	Да
Обмен возможностями – услуга "Здоровье и физическая форма"	Да	Да
Аутентифицированный постоянный сеанс – PHG	Да	*
Аутентифицированный постоянный сеанс – услуга "Здоровье и физическая форма"	Да	*[2]

В таблице A.2 приведены ссылки на руководящие указания, применимые для каждого из классов сертифицированных возможностей.

[2] * Эти ячейки намеренно оставлены пустыми.

Таблица A.2 – Руководящие указания по классам сертифицированных возможностей

Класс сертифицированных возможностей	Соответствующие руководящие указания
Загрузка результатов наблюдений с использованием SOAP – PHG	См. [ITU-T H.812.1] и [ITU-T H.812] таблицы A.3, B.3
Загрузка результатов наблюдений с использованием SOAP – услуга "Здоровье и физическая форма"	См. [ITU-T H.812.1] и [ITU-T H.812] таблицы A.3, B.3
Загрузка результатов наблюдений с использованием данных – PHG	См. [ITU-T H.812.1] и [ITU-T H.812] таблицы A.3, B.1
Загрузка результатов наблюдений с использованием данных – услуга "Здоровье и физическая форма"	См. [ITU-T H.812.1] и [ITU-T H.812] таблицы A.3, B.2
Поддержка разрешений с использованием SOAP – PHG	См. [ITU-T H.812.1] и [ITU-T H.812] таблицы A.3, B.3, C.5, C.7
Поддержка разрешений с использованием SOAP – услуга "Здоровье и физическая форма"	См. [ITU-T H.812.1] и [ITU-T H.812] таблицы A.3, B.3, C.6, C.8
Поддержка разрешений с использованием данных – PHG	См. [ITU-T H.812] таблицы A.3, C.1, C.3, B.1
Поддержка разрешений с использованием данных – услуга "Здоровье и физическая форма"	См. [ITU-T H.812] таблицы A.3, C.2, C.4, B.2
Вопросник – PHG	См. [ITU-T H.812.2] таблица A.1 и [ITU-T H.812] таблицы A.3, B.1
Вопросник – услуга "Здоровье и физическая форма"	См. [ITU-T H.812.2] таблица A.2 и [ITU-T H.812] таблицы A.3, B.2
Обмен возможностями – PHG	См. [ITU-T H.812.3] таблица A.2 и [ITU-T H.812] таблицы A.3, B.1
Обмен возможностями – услуга "Здоровье и физическая форма"	См. [ITU-T H.812.3] таблица A.1 и [ITU-T H.812] таблицы A.3, B.2
Аутентифицированный постоянный сеанс – PHG	См. [ITU-T H.812.4] таблицы A.1 A.2, A.3, A.5 и [ITU-T H.812] таблицы A.3, B.1
Аутентифицированный постоянный сеанс – услуга "Здоровье и физическая форма"	См. [ITU-T H.812.4] таблицы A.1, A.4, A.6 и [ITU-T H.812] таблицы A.3, B.2

Таблица A.3 – Общие для всех CCC требования

Имя	Описание	Комментарий
CapX-HFS-Universality	Все услуги "Здоровье и физическая форма" **должны** поддерживать обмен возможностями, за исключением CCC загрузки результатов наблюдений с использованием SOAP или поддержки разрешений услугой "Здоровье и физическая форма"	От услуги "Здоровье и физическая форма", реализующей только такие CCC, как загрузка результатов наблюдений с использованием SOAP и поддержка разрешений, не требуется поддерживать CCC обмена возможностями услуги "Здоровье и физическая форма"
HFS-Transport_Connection_Initiation	Все соединения услуги "Здоровье и физическая форма" **должны** инициироваться из приложения PHG услуги "Здоровье и физическая форма" и **не должны** инициироваться самой услугой "Здоровье и физическая форма"	

Приложение B

Общие руководящие указания по безопасности для CCC интерфейса услуг

(Данное Приложение является неотъемлемой частью настоящей Рекомендации)

Таблица B.1 – Руководящие указания по безопасности для PHG с использованием REST

Имя	Описание	Комментарий
PHG-Grant_Type	В качестве типа разрешения на авторизацию PHG может использовать регистрационные данные, определяемые паролем владельца ресурсов, как указано в пункте 1.3.3 документа OAuth v2.0 [IETF RFC 6749]	PHG может использовать и другие средства получения маркера авторизации от сервера авторизации
PHG-authorization_request	PHG может получать маркер авторизации от сервера авторизации в соответствии с пунктами 4.3 и 4.3.2 документа OAuth v2.0 [IETF RFC 6749]	Формат запроса авторизации см. в примерах, приведенных в Дополнении III. Ответ описан в соответствующих руководящих указаниях Health & Fitness service-authorization_ request_response
PHG-bearer_token	При запросе доступа к защищенному ресурсу услуги "Здоровье и физическая форма" [IETF RFC 6750] PHG **должен** использовать маркер типа носитель в соответствии с [IETF RFC 6750]	См. соответствующие руководящие указания Health & Fitness service-authorization_request_response
PHG-Token_Transmit	При отправке маркера-носителя, как указано в пункте 2.1 [IETF RFC 6750], PHG **должен** использовать метод поля заголовка запроса авторизации	
PHG-Confidentiality	Для безопасной связи пункта с пунктом с сервером авторизации и услугой "Здоровье и физическая форма" [IETF RFC 4346] PNG **должен** использовать как минимум протокол TLS версии 1.1	
PHG-Cipher	PHG **следует** использовать набор шифров TLS_RSA_WITH_AES_128_CBC_SHA	

Таблица B.2 – Руководящие указания по безопасности для услуги "Здоровье и физическая форма" с использованием REST

Имя	Описание	Комментарий
HFS-authorization_ request_response	Услуга "Здоровье и физическая форма", реализующая сервер авторизации, **должна** возвратить маркер авторизации типа носитель после проверки запроса маркера доступа в соответствии с пунктом 4.3.3 документа OAuth v2.0 [IETF RFC 6749]	Формат запроса см. в руководящих указаниях PHG-authorization_request. Авторизация может быть отдельным объектом и не обязательно входит в состав услуги "Здоровье и физическая форма"
HFS-refresh_token	Услуга "Здоровье и физическая форма", реализующая сервер авторизации, **должна** возвращать маркер обновления	
HFS-Token_Evaluation	Прежде чем предоставлять доступ к записи в услуге "Здоровье и физическая форма", услуга "Здоровье и физическая форма" **должна** оценить маркер авторизации и его область действия	

Таблица B.3 – Руководящие указания по безопасности транспортирования для интерфейса услуг

Имя	Описание	Комментарий
HFS-Security_Transport	Для безопасной связи приложение услуги "Здоровье и физическая форма" и приложения PHG **должны** как минимум поддерживать протокол TLS версии 1.1 [IETF RFC 4346] из WS-I BSP v1.0	Данный пункт руководящих указаний согласуется с профилем ATNA IHE при включенном шифровании. Руководящие указания Continua по взаимной аутентификации основаны на инструкции, приведенной в TLS v1.1 [IETF RFC 4346]
HFS-Security_Transport_ Cipher	Приложение услуги "Здоровье и физическая форма" и приложения PHG **должны** поддерживать шифр AES, как указано в [IETF RFC 3268]	ATNA IHE требует дополнительного использования следующего набора шифров: TLS_RSA_WITH_AES_128_CBC_SHA. В целях безопасности в руководящих указаниях HIS используется следующий набор шифров: TLS_RSA_WITH_AES_128_CBC_SHA. Прочие наборы шифров разрешены, но их применение должно быть согласовано между PHG и услугой "Здоровье и физическая форма"
HFS-Confidentiality	Для безопасной связи пункта с пунктом с сервером авторизации и услугой "Здоровье и физическая форма" с поддержкой вопросника услуга "Здоровье и физическая форма" **должна** использовать протокол TLS v1.1 [IETF RFC 4346]	
HFS-Cipher	Услуге "Здоровье и физическая форма" **следует** поддерживать набор шифров TLS_RSA_WITH_AES_128_CBC_SHA	

Приложение C

Руководящие указания по управлению выдачей разрешений

(Данное Приложение является неотъемлемой частью настоящей Рекомендации)

Таблица C.1 – Руководящие указания по управлению выдачей разрешений с использованием REST для PHG с поддержкой разрешений

Имя	Описание	Комментарий
PHG-Consent_Enabled	PHG с поддержкой разрешений при представлении предпочтений пациента в отношении разрешений должен следовать стандарту указаний по выдаче разрешений [HL7 CDA IG]	
PHG-Consent_Enabled_ Transport_Standards	PHG с поддержкой разрешений должен соответствовать следующим стандартам транспортирования: спецификация HL7 версии 3: формат записи данных, выпуск 1 [HL7 hRF]; OMG data REST Binding for RLUS [OMG/data BIND]; OMG Retrieve, Locate and Update Service (RLUS) Specification 1.0.1 [OMG/data RLUS]	
PHG-Post_Consent	Для выдачи разрешения услуге "Здоровье и физическая форма" PHG с поддержкой разрешений должен использовать HTTP-запрос POST со следующим URL: *baseURL/continua/consent*	См. сценарий использования в пункте 7.1. Для данных услуги извлечения, поиска и обновления (RLUS), передаваемых по транспортному протоколу REST, это осуществляется путем подачи HTTP-запроса POST без параметров по указанному URL с документально оформленным разрешением на доступ к конфиденциальной информации в теле запроса
Consent_Enabled-PHG-Observation_Association	Документально оформленное разрешение, переданное PHG с поддержкой разрешений, должно содержать тот же идентификатор пациента, что и сообщение(я) с результатами наблюдений услуги "Здоровье и физическая форма"	Это требуется для того, чтобы связать документально оформленное разрешение с сообщением о результатах наблюдений услуги "Здоровье и физическая форма"

Таблица C.1 – Руководящие указания по управлению выдачей разрешений с использованием REST для PHG с поддержкой разрешений

Имя	Описание	Комментарий
Consent_Enabled-PHG-Observation-Association_Value	Поле Patient ID в заголовке документально оформленного разрешения должно иметь значение PID-3. Субполя CX-1 и CX-4 должны присутствовать, а субполе CX-5 присутствовать не должно	
Consent_Enabled-PHG-Questionnaire Response_Confidentiality	PHG с поддержкой разрешений должен устанавливать значение кода конфиденциальности в заголовке документа с ответами на вопросник на R	
Consent_Enabled-PHG-Questionnaire Response_Association_Value	Для того чтобы связать документ(ы) с ответами на вопросник с документально оформленным разрешением пациента, PHG с поддержкой разрешений должен использовать элемент перевода кодовой системы конфиденциальности, как определено в таблице IV.3	См. таблицы IV.1, IV.2 и IV.4
Retrieving_Consent	Для получения разрешения от услуги "Здоровье и физическая форма" PHG с поддержкой разрешений должен использовать HTTP-запрос GET со следующим URL: *baseURL/continua/consent.* Для получения от услуги "Здоровье и физическая форма" фактического документально оформленного разрешения PHG с поддержкой разрешений должен использовать HTTP-запрос GET со значением элемента link (ссылка) из записи фида ATOM и проверить, что это действительный документ, соответствующий указаниям по выдаче разрешений HL7 CDA R2 [HL7 CDA IG]	См. сценарий использования в пункте 7.1. Для данных RLUS, передаваемых по транспортному протоколу REST, это осуществляется путем подачи HTTP-запроса GET без параметров по URL-адресу, соответствующему пути к разделу данных разрешения пациента, который возвращает запись фида ATOM. Дополнительную информацию об элементах записей фида в формате Atom см. в таблице I.1

Таблица C.2 – Руководящие указания по управлению выдачей разрешений с использованием REST для услуги "Здоровье и физическая форма" с поддержкой разрешений

Имя	Описание	Комментарий
Consent_Enabled-Health-&-Fitness-Service	Услуга "Здоровье и физическая форма" с поддержкой разрешений должна быть способна принимать документально оформленные разрешения в соответствии с указаниями по выдаче разрешений HL7 CDA R2 [HL7 CDA IG]	
Health-&-Fitness Service-Consent_Enabled_Transport_Standards	PHG с поддержкой разрешений должен соответствовать следующим стандартам транспортирования: спецификация HL7 версии 3: формат записи данных, выпуск 1 [HL7 hRF]; OMG data REST Binding for RLUS [OMG/data BIND]; OMG Retrieve, Locate and Update Service (RLUS) Specification 1.0.1 [OMG/data RLUS]	
HFS-Consent_Root	Услуга "Здоровье и физическая форма" с поддержкой разрешений должна включать следующие элементы содержания вопросника в файл root.xml: 1. profile a. id="consent" b. reference="http://handle.itu.int/11.1002/3000/hData/Consent/2017/01/H.812.pdf" 2. section a. path="consent" b. profileID= "consent" c. resourceTypeId="consent" 3. resourceType a. resourceTypeId="consent" b. reference="http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63" c. representation d. mediaType="application/xml2	Примечание. – URL, указанный в ссылке 1.b, приведен исключительно в качестве примера
HFS-Consent_Validate	Услуга "Здоровье и физическая форма" с поддержкой разрешений должна проверить, что документально оформленное разрешение представляет собой действительный документ в соответствии с указаниями по выдаче разрешений HL7 CDA R2, и если это так, отправить в качестве ответа сообщение HTTP 200	

Таблица C.2 – Руководящие указания по управлению выдачей разрешений с использованием REST для услуги "Здоровье и физическая форма" с поддержкой разрешений

Имя	Описание	Комментарий
HFS-Post_Consent-Response	Получив от PHG с поддержкой разрешений сообщение POST, услуга "Здоровье и физическая форма" с поддержкой разрешений должна создать запись, содержащую документально оформленное разрешение, и отправить в качестве ответа сообщение HTTP 201	См. PHG-Post_Consent, выше
PHG-Delete_Consent_Response	Услуга "Здоровье и физическая форма" с поддержкой разрешений не должна поддерживать удаление существующей записи, содержащей документально оформленное разрешение, и в ответ на HTTP-запрос DELETE на URL-разрешения должна возвращать сообщение HTTP 405 Method Not Allowed (метод не разрешен)	

Таблица C.3 – Руководящие указания по правомерному использованию разрешений с использованием данных для PHG с поддержкой разрешений

Имя	Описание	Комментарий
Consent_Enabled-PHG-Content-Encryption_Actor	PHG с поддержкой разрешений должен шифровать контент в соответствии с профилем шифрования документов (DEN) IHE [IHE ITI DEN]	Контентом может быть полезная нагрузка транзакции PCD-01 или документ с ответами на вопросник
Consent_Enabled-PHG-Questionnaire-Response_MIMEtype_	В случае если зашифрованный контент представляет собой ответы на вопросник, PHG с поддержкой разрешений должен устанавливать тип MIME в значение application/xml	Цель заключается в том, чтобы обозначить тип полезной нагрузки, которая шифруется
Consent_Enabled-PHG-Observation - Upload_MIMEtype_	В случае если зашифрованный контент представляет собой загруженные результаты наблюдений, PHG с поддержкой разрешений должен устанавливать тип MIME в значение application/txt	Цель заключается в том, обозначить тип полезной нагрузки, которая шифруется
Consent_Enabled-PHG-Content-Encryption_Algorithm	Для шифрования контента PHG с поддержкой разрешений должен использовать алгоритм AES-128 CBC	Используемый алгоритм идентифицируется с помощью параметра ContentEncryptionAlgorithmIdentifier в CMS (синтаксис криптографического сообщения), который дополнительно настраивается посредством IHE DEN
Consent_Enabled-PHG-Encryption-Recipient_Binding_PKI	PHG с поддержкой разрешений должен использовать метод управления ключами на базе PKI из профиля IHE DEN [IHE ITI DEN]	Метод управления ключами контента на базе PKI использует KeyTransRecipient Info в качестве RecipientInfoType CMS. Это указывает на открытый ключ или сертификат x.509 v3 получателя

Таблица C.4 – Руководящие указания по правомерному использованию разрешений с использованием данных для услуги "Здоровье и физическая форма" с поддержкой разрешений

Имя	Описание	Комментарий
HFS-Device_HTTP_Ack	В качестве ответа после успешного приема зашифрованного контента услуга "Здоровье и физическая форма" с поддержкой разрешений должна отправлять сообщение HTTP 202	
Consent_Enabled-HFS-Content-Decryption_Actor_XDR	Для расшифровки зашифрованного контента услуга "Здоровье и физическая форма" с поддержкой разрешений должна действовать в соответствии с профилем IHE DEN [IHE ITI DEN]	
Consent_EnabledKey_Management	Услуга "Здоровье и физическая форма" с поддержкой разрешений должна использовать метод управления ключами на базе PKI, как указано в профиле IHE DEN [IHE ITI DEN]	
Consent_Enabled-HFS-Decryption-Algorithm	Для расшифровки полезной нагрузки услуга "Здоровье и физическая форма" с поддержкой разрешений должна использовать алгоритм AES.128 CBC	Используемый алгоритм идентифицируется с помощью параметра ContentEncryptionAlgorithmIdentifier в CMS (синтаксис криптографического сообщения)
Consent_Enabled-HFS-Consent_Enforcement_	Услуга "Здоровье и физическая форма" с поддержкой разрешений должна правомерно использовать предпочтения, выраженные в документально оформленном разрешении	Например, предотвращать дальнейшее раскрытие контента неавторизованным лицам

Таблица C.5 – Руководящие указания по управлению выдачей разрешений с использованием SOAP для PHG с поддержкой разрешений

Имя	Описание	Комментарий
Services-Observation-PHG-Consent	При представлении документально оформленного разрешения пациента PHG передачи результатов наблюдений с поддержкой разрешений **должен** соответствовать указаниям по выдаче разрешений [HL7 CDA IG]	
Services-Observation-PHG-Consent-Transport	Для отправки документально оформленного разрешения с использованием транзакции ITI 41 Provide and Register Document Set-b PHG передачи результатов наблюдений для услуг с поддержкой разрешений **должен** использовать действующий объект Document Source XDR IHE	
Services-Observation-PHG-Consent-Frequency	PHG передачи результатов наблюдений для услуг с поддержкой разрешений **должен** по крайней мере один раз отправить документально оформленное разрешение услуге "Здоровье и физическая форма", принимающей результаты наблюдений	Например, документально оформленное разрешение может быть первоначально отправлено в процессе регистрации в услуге. Рекомендуется отправлять разрешение по крайней мере один раз в течение срока действия соединения с услугой "Здоровье и физическая форма", принимающей результаты наблюдений. Поддерживаются также такие сценарии использования, как обновление предпочтений, указанных в разрешении. Обновленное документально оформленное разрешение заменяет существующий документ в услуге "Здоровье и физическая форма" с поддержкой разрешений, принимающей результаты наблюдений

Таблица C.5 – Руководящие указания по управлению выдачей разрешений с использованием SOAP для PHG с поддержкой разрешений

Имя	Описание	Комментарий
HFS-Observation_Measurement_ Consent_Document_Association	Документально оформленное разрешение, переданное PHG передачи результатов наблюдений для услуг с поддержкой разрешений, **должно** содержать тот же идентификатор пациента, что и сообщение(я) с результатами наблюдений для услуг	Это связывает документально оформленное разрешение с сообщениями, содержащими результаты наблюдений услуги "Здоровье и физическая форма"
HFS-Observation_Measurement_ Consent_Document_Association_ Value	Поле Patient ID в заголовке документально оформленного разрешения **должно** иметь значение PID-3. Субполя CX-1 и CX-4 **должны** присутствовать, а субполе CX-5 присутствовать **не должно**	

Таблица C.6 – Руководящие указания по управлению выдачей разрешений с использованием SOAP для услуги "Здоровье и физическая форма" с поддержкой разрешений

Имя	Описание	Комментарий
Observation-Health-&-Fitness-Service-Consent	Услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **должна** быть способна принимать документально оформленные разрешения в соответствии с указаниями по выдаче разрешений [HL7 CDA IG]	
Observation-HFS-Consent_Transport	Услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **должна** реализовывать активный объект – получателя документов IHE XDR для приема документально оформленных разрешений с использованием транзакций ITI 41 Provide and Register Document Set-b	Услуга "Здоровье и физическая форма", принимающая результаты наблюдений, заменяет существующее документально оформленное разрешение, если получена новая версия, как указано в метаданных XDS документально оформленного разрешения

Таблица C.7 – Руководящие указания по правомерному использованию разрешений с использованием SOAP для PHG с поддержкой разрешений

Имя	Описание	Комментарий
HFS-PHG-Content_ Encryption_Actor	PHG передачи результатов наблюдений для услуг "Здоровье и физическая форма" с поддержкой разрешений **должен** шифровать полезную нагрузку (Приложение D к [ITU-T H.812.1]) транзакции PCD-01 в соответствии с правилами обработки шифрования, определенными в пункте 4.1 спецификации шифрования XML [W3C XMLENC]	
HFS-PHG-Content_ Encryption_ MIMEtype	PHG передачи результатов наблюдений для услуг "Здоровье и физическая форма" с поддержкой разрешений **должен** задавать значение application/hl7-v2+xml для типа MIME	Цель заключается в том, чтобы обозначить тип полезной нагрузки, которая шифруется
HFS-Services-PHG-Content_ Encryption_ Algorithm	В качестве алгоритма шифрования полезной нагрузки PHG передачи результатов наблюдений для услуг "Здоровье и физическая форма" с поддержкой разрешений **должен** использовать AES-128 CBC из спецификации шифрования XML	Алгоритм AES-128 CBC идентифицируется при помощи следующего идентификатора: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC]
HFS-PHG-Encryption_ Recipient_Binding_ PKI	Для транспортировки ключей контента PHG передачи результатов наблюдений для услуг "Здоровье и физическая форма" с поддержкой разрешений **должен** поддерживать RSA версии 1.5 из спецификации шифрования XML	Транспортировка ключей на базе RSA v1.5 идентифицируется при помощи следующего идентификатора: http://www.w3.org/2001/04/xmlenc#rsa-1_5 [W3C XMLENC]. Для получения подробной информации об RSA v1.5 следует обратиться к [b-RFC 2437]. Транспортировка ключей на базе RSA v1.5 также используется в стандарте CMS (синтаксис криптографических сообщений), применяемом в HIS-IF. Дополнительная информация приведена в [b-RFC 3370] и руководящих указаниях по правомерному использованию разрешений для HIS-IF

Таблица C.7 – Руководящие указания по правомерному использованию разрешений с использованием SOAP для PHG с поддержкой разрешений

Имя	Описание	Комментарий
HFS-PHG-Encryption_ Recipient_Binding_ Symmetric	Для транспортировки ключей контента PHG передачи результатов наблюдений для услуг "Здоровье и физическая форма" с поддержкой разрешений **следует** использовать симметричный алгоритм обертывания ключа AES-128 из спецификации шифрования XML. В случае шифрования на основе пароля PHG передачи результатов наблюдений для услуг "Здоровье и физическая форма" с поддержкой разрешений в качестве алгоритма выработки ключа **может** использовать PBKDF2 из [IETF RFC 3211]	Идентификатор симметричного алгоритма обертывания ключа AES-128: http://www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]. Ключ, используемый при обертывании, называется KEK и может быть получен из пароля или долгосрочного общего секретного ключа
HFS-PHG-Integrity_Payload_ PCD-01_Create	PHG передачи результатов наблюдений для услуг "Здоровье и физическая форма" с поддержкой разрешений **должен** вычислять дайджест зашифрованной полезной нагрузки с использованием алгоритма SHA256 (пункт 5.7.2) в соответствии со спецификацией шифрования XML	Идентификатором алгоритма SHA256 служит следующий URL: http://www.w3.org/2001/04/xmlenc#sha256 [W3C XMLENC]
HFS-Encrypted_Payload_ PCD-01_transaction	PHG передачи результатов наблюдений для услуг "Здоровье и физическая форма" с поддержкой разрешений **должен** свертывать зашифрованную полезную нагрузку внутри элемента <CommunicateEncPCDData xmlns= "urn:ihe:continua:enc:pcd:dec:2012">	В случае незашифрованной полезной нагрузки контент свертывается внутри элемента <CommunicatePCDData xmlns="urn:ihe:pcd:dec:2010">. См. пример на рисунке II.1
HFS-Encrypted_Payload_ PCD-01_Transaction_ Header	В случае зашифрованной полезной нагрузки заголовок SOAP вместо "urn:ihe: pcd:dec:2010: CommunicatePCDData" **должен** содержать "urn:ihe:continua:enc:pcd:dec:2012:CommunicateEncPCDData"	Простая транзакция PCD-01 содержит "urn:ihe: pcd:dec:2010:CommunicatePCDData". См. примеры на рисунках II.1, II.2 и II.3

Таблица C.8 – Руководящие указания по правомерному использованию разрешений с использованием SOAP для услуги "Здоровье и физическая форма" с поддержкой разрешений

Имя	Описание	Комментарий
HFS-HTTP-Ack	После успешного приема зашифрованного сообщения услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **должна** отправлять HTTP-ответ SOAP с кодом состояния 202. Услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **может не** отправлять подтверждение получения PCD-01 на уровне приложения	Причина в том, что услуга "Здоровье и физическая форма", принимающая результаты наблюдений, может не обладать ключом дешифрования, поскольку контент может быть зашифрован для конкретного получателя услуги "Здоровье и физическая форма"
HFS-Payload-PCD-01-Verify-Integrity	Услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **должна** проверять дайджест сообщения зашифрованной полезной нагрузки	
HFS-Payload-PCD-01-Verify-Integrity-Algorithm	Услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **должна** поддерживать алгоритм SHA256	
HFS-Content-Decryption-Actor	Услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **должна** соблюдать правила дешифрования, указанные в пункте 4.2 спецификации шифрования XML [W3C XMLENC]	
HFS-Key-Transport-RSA	Услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **должна** поддерживать RSA версии 1.5 из спецификации шифрования XML [W3C XMLENC]	

Таблица C.8 – Руководящие указания по правомерному использованию разрешений с использованием SOAP для услуги "Здоровье и физическая форма" с поддержкой разрешений

Имя	Описание	Комментарий
HFS-Key-Transport-Symmetric	Услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **должна** поддерживать симметричный алгоритм обертывания ключа AES-128 из спецификации шифрования XML [W3C XMLENC]. В качестве алгоритма выработки ключа услуга "Здоровье и физическая форма" с поддержкой разрешений **должна** поддерживать PBKDF2 из [IETF RFC 3211]	Идентификатором симметричного обертывания ключа AES-128 служит следующий URL: http://www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]. Ключ, используемый при обертывании, называется KEK и может быть получен из пароля или долгосрочного общего секретного ключа
HFS-Content-Decryption-Algorithm	Услуга "Здоровье и физическая форма" с поддержкой разрешений, которая принимает результаты наблюдений, **должна** использовать алгоритм дешифрования AES-128 CBC из спецификации шифрования XML [W3C XMLENC]	Алгоритм AES-128 CBC идентифицируется при помощи следующего идентификатора: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC]

Дополнение I

Элементы фида ATOM для управления выдачей разрешений

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В документах, содержащих разрешения, следующие дочерние элементы элемента entry (запись) XML-фида данных в формате ATOM имеют специальное назначение.

Таблица I.1 – Дочерние элементы фида ATOM для управления выдачей разрешений

Элемент	Назначение
Author (автор)	Конструкт лица, указывающий, кто именно предоставил информацию, содержащуюся в документально оформленном разрешении, то есть кто заполнил разрешение
Title (название)	Название документа разрешения пациента (например, "Разрешение Ивана")
Link (ссылка)	Ссылка на документально оформленное разрешение Ивана, которое должно быть действительным документом в соответствии с указаниями по выдаче разрешений HL7 CDAR2. Ссылка должна быть относительной, а документально оформленное разрешение доступа к персональной информации должно находиться в разделе разрешений записи данных
Published (дата публикации)	В публикуемом элементе должны быть указаны дата и время, когда документально оформленное разрешение на обработку персональной информации было помещено на сервер

I.1 Информация о разрешении в файле root.xml

```
<profile>
   <id>consent</id>
   <reference><http://handle.itu.int/11.1002/3000/hData/Consent/2017/01/H.812.pdf></reference>
</profile>
<section>
  <path>consent</path>
  <profileID>consentId</profileID>
  <resourceTypeID>consent</resourceTypeID>
</section>
<resourceType>
  <resourceTypeID>consent</resourceTypeID>
  <reference>
    http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63
  </reference>
  <representation>
      <mediaType>application/xml</mediaType>
  </representation>
</resourceType>
```

Дополнение II

Примеры управления выдачей разрешений с использованием SOAP

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

```
<html version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
   <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing" >
      <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
soapenv:mustUnderstand="true" >
      <wsa:To
soapenv:mustUnderstand="true">
https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Service>/wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand="true">
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand="true">urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicatePCDData xmls="urn:ihe:pcd:dec:2010">
            MSH|^~\&|AT4_PHG^123456789ABCDEF^EUI-
            64|||20120409103145+0000||ORU^R01^ORU_R01|MSGID2848518|P|2.6|||NE|AL|||||IHE PCD ORU-
            R012006^HL7^2.16.840.1.113883.9.n.m^HL7 PID|||789567^^^Imaginary
            Hospital^PI||Doe^John^Joseph^^^^L
            OBR|1|POTest^AT4_PHG^1234567890ABCDEF^EUI-64|POTest^AT4_PHG*1234567890ABCDEF^EUI-
            64|182777000^monitoring of patient^SNOMED-CT|||20100903124015+0000
            OBX|1|CWE|68220^MDC_TIME_SYNC_PROTOCOL^MDC|0.0.0.1|532224^MDC_Time_SYNC_NONE^MDC||||||
            R
            OBX|2|CWE|68220^MDC_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.2|1^auth-body-continua(2)||||||R
            OBX|3|ST|588800^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|0.0.0.3|1.5||||||R
            OBX|4||528388^MDC_DEV_SPEC_PROFILE_PULS_OXIM^MDC|1||||||X||||||1234567890ABCDEF^EUI-64
            OBX|5|ST|531696^MDC_ID_MODEL_NUMBER^MDC|PulseOx v1.5||||||R
            OBX|6|ST|531970^MDC_ID_MANUFACTURER^MDC|1.0.0.2|AT4 Wireless|||||R
            OBX|7|DTM|67975|^MDC_ATTR_TIME_ABS^MDC|1.0.0.3|20100903124015+0000||||||R2010090312401
            5+0000
            OBX|8|CWE|68218^MDC_CERT_DATA_AUTH_BODY^MDC|1.0.0.4|1^auth-body-continua(2)||||||R
            OBX|9|ST|588800^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|1.0.0.5||||||R
            OBX|10|NA|588801^MDC_REG_CERT_DATA_CONTINUA_CERT_DEV_LIST^MDC|1.0.0.6|16388||||||R
            OBX|11|CWE|588802^MDC_REG_CERT_DATA_CONTINUA_REG_STATUS^MDC|1.0.0.7|0^unregulated-
            device(0)||||||R
            OBX|12|NM|150456^MDC_DIM_PERCENT^MDC|||||R|||20100903124015+0000
            OBX|13|NM|149520^MDC_PULS_OXIM_RATE^MDC|1.0.0.9|71|264864^MDC_DIM_BEAT_PER_MIN^MDC||||
            |R|||20100903124015+0000
         </soapenv:Body>
      </soapenv:Envelop>
```

Рисунок II.1 – Транзакция PCD-01 с незашифрованной полезной нагрузкой

```
<html version=”1.0” encoding=”UTF-8” ?>
<soapenv:Envelope xmlns:soapenv=”http://www.w3.org/2003/05/soap-envelope”>
   <soapenv:Header xmlns:wsa=”http://www.w3.org/2005/08/addressing” >
      <wsse:Security xmlns:wsse=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd”
   soapenv:mustUnderstand=”true”>
<wsa:To
soapenv:mustUnderstand=”true”
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationC
onsumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand=”true”>
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand=”true”>urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand=”true”>urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns=”urn:ihe:continuacenc:pcd:dec:2012”>
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType=”applicationhl7-v2+xml”>
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+”http://www.w3.org/2000/09/xmldsig#”>
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#”>
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc#rsa-1_5/>
                     <KeyInfo xmlns=http://www.w3.org/2000/09/xmldsig#>
                        <KeyName>John Smith</KeyName>
                     </KeyInfo>
                     <CipherData>
                        <CipherValue>Encrypted Key…</CipherValue>
                     </CipherData>
                  </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

Рисунок II.2 – Зашифрованная транзакция PCD-01 на основе открытого ключа

На рисунке II.2 показана транзакция PCD-01 с полезной нагрузкой, зашифрованной с применением стандарта шифрования XML. Ключ контента зашифрован открытым ключом получателя.

```
<html version=”1.0” encoding=”UTF-8” ?>
<soapenv:Envelope xmlns:soapenv=”http://www.w3.org/2003/05/soap-envelope”>
   <soapenv:Header xmlns:wsa=”http://www.w3.org/2005/08/addressing” >
      <wsse:Security xmlns:wsse=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd”
   soapenv:mustUnderstand=”true”>
<wsa:To
soapenv:mustUnderstand=”true”
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationC
onsumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand=”true”>
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand=”true”>urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand=”true”>urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns=”urn:ihe:continuacenc:pcd:dec:2012”>
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType=”applicationhl7-v2+xml”>
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+”http://www.w3.org/2000/09/xmldsig#”>
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#”>
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc #rsa-1_5/>
                     <KeyInfo xmlns=http://www.w3.org/2000/09/xmldsig#>
                        <KeyName>John Smith</KeyName>
                     </KeyInfo>
                     <CipherData>
                        <CipherValue>Encrypted Key…</CipherValue>
                     </CipherData>
                  </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

Рисунок II.3 – Зашифрованная транзакция PCD-01 на основе симметричного ключа

На рисунке II.3 показана транзакция PCD-01 с полезной нагрузкой, зашифрованной с применением стандарта шифрования XML. В этом примере предполагается, что ключ контента известен как отправителю, так и получателю и доступен только для чтения.

Дополнение III

Пример OAuth

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

Пример 1

– Запрос маркера доступа

Чтобы получить маркер доступа, PHG с поддержкой вопросника направляет серверу авторизации следующий HTTP-запрос POST.

```
POST http://localhost:3000/oauth2/token HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Basic MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl
Content-Type: application/x-www-form-urlencoded
Content-Length: 59

grant_type=password&username=john@example.com&password=test
```

Где

– http://localhost:3000/oauth2/token – это URL-адрес для доступа к серверу авторизации, который должен быть известен PHG с поддержкой вопросника;

– Authorization: Basic MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl;

– это HTTP-заголовок базовой авторизации, генерируемый PHG с поддержкой вопросника с использованием заданного идентификатора и секретного слова путем их кодирования в хеш-строку Base64: Base64("120094574673767:b54dc82476af2814e620b86776c42c0e") =;

– "MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl";

– grant_type указывает код авторизации. В этом коде авторизации есть логин и пароль;

– ответ с маркером доступа.

Сервер авторизации проверяет запрос маркера доступа и генерирует маркер доступа типа "носитель" и дополнительный маркер обновления, если это разрешено.

```
HTTP/1.1 200 OK
Content-Length: 141
Content-Type: application/json
X-Ua-Compatible: IE=Edge
X-Runtime: 0.273027
Server: WEBrick/1.3.1 (Ruby/1.9.3/2013-02-22)
Date: Wed, 03 Apr 2013 08:54:57 GMT
Connection: Keep-Alive

{"access_token":"f779da766bfd1b9164b0fd6d280d52f1","refresh_token":"789f3daf81a302e0636325114113e4
b4","token_type":"bearer","expires_in":899}
```

Где

– f779da766bfd1b9164b0fd6d280d52f1"– маркер доступа, который PHG может использовать для доступа к ресурсу на сервере;

– "789f3daf81a302e0636325114113e4b4"– маркер обновления, который можно использовать для получения нового маркера;

– тип маркера в приведенном выше примере – "носитель";

– срок действия маркера составляет 899 секунд;

– запрос ресурса с использованием маркера доступа типа "носитель".

Пример 2

В приведенном ниже примере PHG использует маркер типа "носитель" для запроса защищенного ресурса, например вопросника.

```
GET http://localhost:3000/hdata/root.xml HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Bearer f779da766bfd1b9164b0fd6d280d52f1
```

Дополнение IV

Ассоциирование ответов на вопросник в PHG, поддерживающем работу с разрешениями

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

Таблица IV.1 – Элементы кодовой системы конфиденциальности

Имя	Значение	Комментарии
Code	"R"	
codeSystem	2.16.840.1.113883.5.25	
codeSystemName	"Confidentiality" (конфиденциально)	
displayName	"Restricted" (ограничено)	

Таблица IV.2 – Элементы кодовой системы указаний по выдаче разрешений Continua

Имя	Значение	Комментарии
Code	Значение **должно** быть таким, как определено в [HL7 CDA IG]	
codeSystem	2.16.840.1.113883.3.1817 .1.2.1	
codeSystemName	"Continua Consent Directive" (указания по выдаче разрешений Continua)	
displayName	ID документально оформленного разрешения	

Таблица IV.3 – Преобразование кодовой системы конфиденциальности в кодовую систему указаний по выдаче разрешений Continua

Имя	Значение	Комментарии
Code	"R"	
codeSystem	2.16.840.1.113883.5.25	
codeSystemName	"Confidentiality" (конфиденциально)	
displayName	"Restricted" (ограничено)	
translation	code="<ID of the consent document>" codeSystem=2.16.840.1.113883.3.1817.1.2.1 codeSystemName="Continua Consent Directive" (указания по выдаче разрешений Continua) displayName=ID of the consent document (ID документально оформленного разрешения)	"<>" является символом-заполнителем для ID в документально оформленном разрешении. Элементы кодовой системы указаний по выдаче разрешений Continua приведены в таблице IV.2

Таблица IV.4 – Распределение OID для Personal Connected Health Alliance

OID	Описание	Комментарии
2.16.840.1.113883.3.1817	OID организации: Personal Connected Health Alliance	
2.16.840.1.113883.3.1817.1	Корневой OID для сквозной архитектуры Continua V1.0	
2.16.840.1.113883.3.1817.1.2	Корневой OID для сквозной безопасности и конфиденциальности	
2.16.840.1.113883.3.1817.1.3	Корневой OID для интерфейса персональных медицинских устройств	
2.16.840.1.113883.3.1817.1.4	Корневой OID для интерфейса персональных медицинских устройств ZigBee	
2.16.840.1.113883.3.1817.1.5	Корневой OID для интерфейса персональных медицинских устройств NFC	
2.16.840.1.113883.3.1817.1.6	Корневой OID для интерфейса услуг	
2.16.840.1.113883.3.1817.1.7	Корневой OID для HIS-интерфейса	
2.16.840.1.113883.3.1817.1.2.1	Сквозная безопасность и конфиденциальность: OID для кодовой системы указаний по выдаче разрешений Continua	

Библиография

Список не имеющих нормативного характера справочных документов и публикаций, содержащих дополнительную базовую информацию, приведен в [ITU-T H.810].

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	**Аудиовизуальные и мультимедийные системы**
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2019 г.