

ВВЕДЕНИЕ

Безопасность является чрезвычайно важной проблемой для всех цифровых систем. Хотя при обсуждении безопасности данных основное внимание часто уделяется шифрованию, более значимым аспектом, вероятно, является аутентификация. Поскольку вся информация сводится к отдельным единицам и нулям, их достоверность и подлинность при обмене данными может оказаться под вопросом. В настоящем документе представлен прямой метод аутентификации аппаратуры, данных и пользователей. Кроме того, здесь дается обзор приборов SHA-1 (Secure Hash Algorithm 1) шины 1-Wire®, использующих данный метод. В конце документа приводится большое количество ссылок на другие документы, комплекты и примеры для дальнейшего изучения и разработки. (*Специальные термины, команды или коды выделены в тексте курсивом.*) Словарь специальных терминов можно найти в документе «White Paper 4: Glossary of 1-Wire SHA-1 Terms» (Словарь терминов для SHA-1 шины 1-Wire) (<http://pdfserv.maxim-ic.com/arpdf/AppNotes/wp4.pdf>).

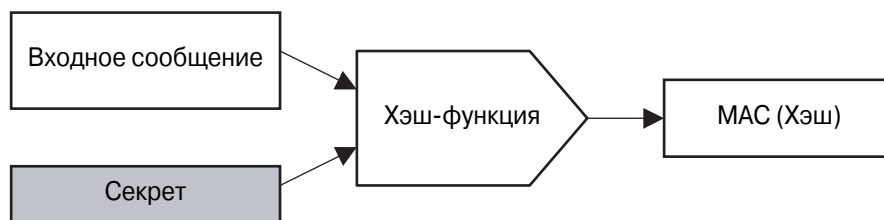
Хэш

Хэш представляет собой «сущность» сообщения. Эта «сущность» (называемая профилем, или дайджестом) обычно гораздо меньше, чем само сообщение и имеет постоянный размер. *Криптографически стойкий* хэш должен быть *необратимым*, что означает невозможность определения по нему какой-либо части исходного сообщения. Кроме того, он должен очень сильно изменяться при любом небольшом изменении (даже в одном бите) в исходном сообщении. Это называется *лавинным эффектом*. Хэш также должен быть *устойчивым к коллизиям*, что означает невозможность найти два сообщения, имеющих одинаковый хэш. Хэш, удовлетворяющий указанным требованиям, может использоваться для проверки, не было ли изменено сообщение.

MAC

MAC (Message Authentication Code — код аутентификации сообщения) представляет собой результат хеширования входного сообщения (хэш), при котором часть входных данных является секретом. Только участники системы, знающие этот секрет, могут вновь вычислить и проверить аутентичность (подлинность) MAC-кода. Блок-схема генерирования MAC-кода приведена на Рис. 1.

Рис. 1. Генерирование MAC-кода



Таким образом, участники системы (знающие секрет) могут проверить аутентичность комбинации сообщения и MAC-кода. Подлинность упомянутых ранее отдельных единиц и нулей теперь подтверждается, не прибегая к помощи шифрования. Это мощный метод, имеющий самое широкое применение (см. далее раздел *Приложения*).

SHA-1

Выбор криптографически устойчивой хэш-функции является критичным для успешной работы схемы аутентификации, основывающейся на хэше. Алгоритм SHA-1 является необратимым, устойчивым к коллизиям и обладает хорошим лавинным эффектом. Алгоритм SHA определяется федеральными стандартами по обработке информации FIPS 180-1, FIPS 180-2. В настоящее время хэширование с использованием алгоритмов группы SHA является единственным методом, соответствующим требованиям FIPS. Алгоритм SHA-1 определяется также в стандарте ISO/IEC 10118-3. Как утверждает Брюс Шнайдер (Bruce Schneider) в книге *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996: «Не существует известных криптографических атак против алгоритма SHA». По этой причине и был выбран алгоритм SHA-1. Этот алгоритм берет один или более блоков данных длиной по 512 битов (64 байта) и создает 160-битный (20-байтный) хэш.

Приложения

Аутентификация представляет собой процесс, при котором хосту предоставляются доказательства, что прибор, личность или сообщение является действительным и подлинным. Метод аутентификации, использующий код MAC, называется «*Запрос и ответ*». Запрос — это случайные данные, отсылаемые хостом прибору, который подвергается аутентификации. Этот запрос затем используется при вычислении MAC-кода. Благодаря этому все сеансы аутентификации отличаются друг от друга и являются недетерминированными.

Что может аутентифицироваться? Может аутентифицироваться сообщение, передаваемое от одной части оборудования к другой, если секрет известен обеим частям. Дверной замок может осуществлять аутентификацию мобильного маркера для предоставления доступа в контролируемое помещение. Список возможных приложений, включающий как тип хоста, так и объект аутентификации, приведен в Табл. 1.

Таблица 1. Приложения, в которых используется MAC-код

Аутентификация прибора	Оборудование	Периферийный прибор с встроенным маркером
Физический контроль доступа	Электронный дверной замок Оборудование для контроля доступа в здание Замок картотечного шкафа Сейф	Мобильный маркер
Контроль доступа пользователя	Рабочая станция	Мобильный маркер и пользователь
Авторизация программного обеспечения	Компьютерное ПО Встроенное программное обеспечение оборудования	Мобильный, прикрепленный или встроенный маркер
Электронные деньги (eCash)	Торговый автомат Счетчик парковки Пост сбора пошлин Телефон-автомат Игровой автомат	Мобильный маркер

СОЗДАНИЕ ДОВЕРЕННОГО МАРКЕРА

Основным компонентом большинства указанных приложений является мобильный электронный маркер. Для осуществления аутентификации с использованием MAC-кода SHA-1, должен быть создан доверенный клиент, который может надежно хранить секрет и вычислять MAC-код. Этот клиент должен быть конструктивно надежным, прочным и способным выполнять быстрые вычисления по алгоритму SHA-1. Фирма Dallas Semiconductor/Maxim, в течение 10 лет изготавливающая мобильные маркеры iButton®, теперь выпускает приборы, использующие алгоритм SHA-1. Эти приборы выполняются как в виде iButton, так и в обычных корпусах микросхем (см. Рис. 2).

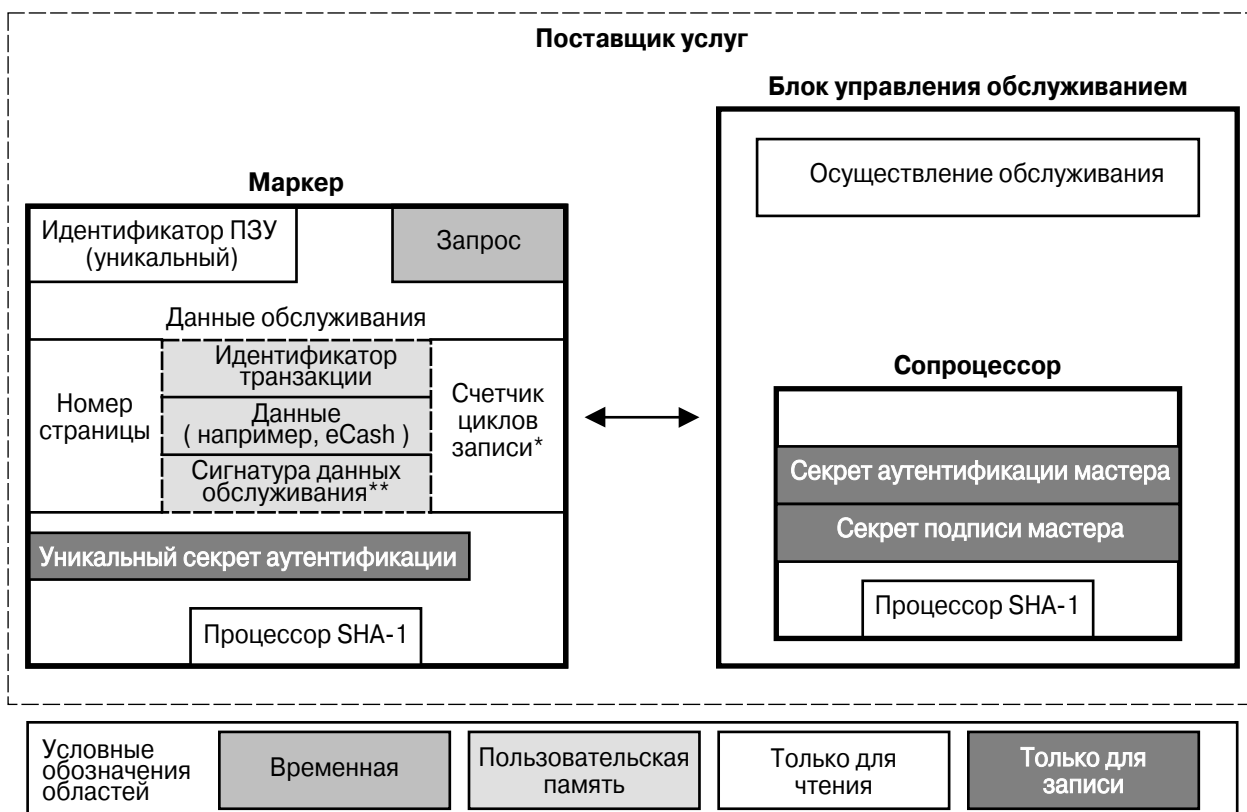
iButton является зарегистрированной торговой маркой Dallas Semiconductor.

Рис. 2. Приборы SHA-1 шины 1-Wire



Применение и использование этих маркеров проще обсуждать в каком-либо контексте. На Рис. 3 приведена полная схема обслуживания. Поставщик услуг (например, торговая компания) распространяет маркеры с достоверными данными среди своих пользователей. Пользователь прикладывает маркер к *Блоку управления обслуживанием* (Service Control Unit — SCU) (например, автомату по продаже конфет) для того, чтобы последний аутентифицировал его в качестве участника обслуживания, а также проверил достоверность данных (электронных денег, eCash) и, возможно, обновил их. Кроме того, блок SCU должен быть способен вычислять MAC-коды SHA-1. Это может осуществляться внутренним сопроцессором. Специальные поля и характеристики маркера и блока SCU будут рассмотрены в следующих разделах документа.

Рис. 3. Обслуживание



* Только в DS1963S

** Опция в DS1961S

Выпускаются два различных маркера SHA-1 шины 1-Wire. Прибор DS1963S имеет дополнительно восемь различных секретов SHA-1 и область данных пользователя размером 512 байтов, размещенную в энергонезависимой памяти. Также этот прибор может использоваться в качестве сопроцессора в блоке SCU для вычисления всех необходимых хосту MAC-кодов SHA-1. Удаление всех секретов из процессора SCU обеспечивает дополнительную безопасность. Секреты, необходимые для проверки данных обслуживания (*Секрет подписи мастера*) и аутентификации маркера (*Секрет аутентификации мастера*), надежно хранятся в сопроцессоре DS1963S. Встроенная литиевая батарейка питает энергонезависимое ОЗУ, находящееся в приборе. Удаление этого источника питания даже на короткое время (например, при физической атаке) приведет к очистке секретов и содержимого памяти.

Прибор DS1963S может поддерживать семь различных динамических записей обслуживания, каждую со своим собственным секретом. Восьмой секрет зарезервирован для функций, выполняемых прибором при работе в качестве сопроцессора. Прибор также содержит восемь дополнительных 32-байтных страниц данных общего назначения, которые могут использоваться для статических записей обслуживания. Эти дополнительные страницы имеют связанный с ними секрет, но не имеют счетчика циклов записи. Счетчик циклов записи представляет собой предназначенный только для чтения непереполюющийся счетчик произведенных записей страницы, который применяется для детектирования записей. Циклы записи используются для предотвращения некоторых атак на систему.

Прибор DS1963S использует два различных MAC-кода для каждой записи обслуживания. Первый код генерируется маркером 1-Wire и удостоверяет его подлинность для системы (*Уникальный секрет аутентификации*). Второй код создается блоком SCU хоста, включается в состав записи обслуживания и используется для проверки ее достоверности. Этот MAC-код называется *Сигнатурой данных обслуживания*. Секрет, используемый для создания этой сигнатуры (*Секрет подписи мастера*), не хранится в приборе пользователя: он содержится только в блоке SCU или его сопроцессоре.

Два других прибора DS1961S и DS2432 являются, по сути дела, одним и тем же прибором, выполненным в различных корпусах. Прибор DS1961S поставляется в стандартном корпусе iButton, тогда как DS2432 выпускается в небольшом корпусе TSOC или в сверхминиатюрном безвыводном (chip-scale) корпусе (2.5 мм × 1.5 мм). Оба эти прибора используют вместо энергонезависимого ОЗУ технологию ЭСППЗУ (EEPROM), что позволяет отказаться от встраивания в корпус литиевой батарейки. В данных приборах имеется только один секрет, связанный со всеми четырьмя страницами. В приборе DS1963S ограничений на запись не существует. Однако для записи в приборы DS1961S/DS2432 требуется MAC-код аутентификации. Эта мера эффективно защищает приборы от записи. Поскольку доступ для записи ограничивается блоком SCU, знающим секрет аутентификации, приборы не содержат счетчик циклов записи и не требуют встраивания сигнатуры MAC в данные. Приборы DS1961S/DS2432 могут поддерживать только одного поставщика услуг, так как имеют только один секрет аутентификации. Поскольку прибор содержит четыре страницы, этот поставщик может установить до четырех различных услуг.

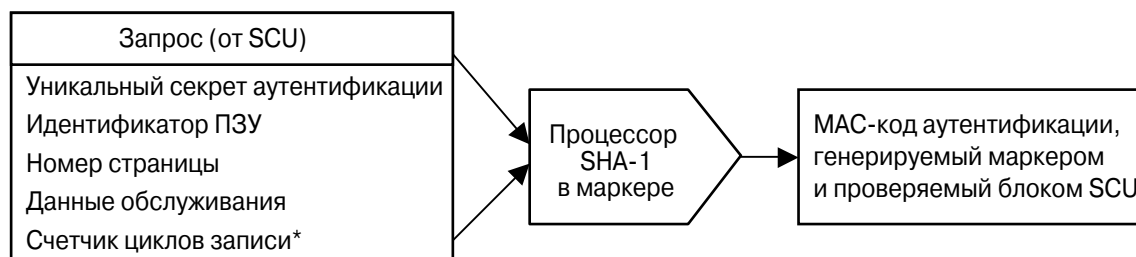
Заметим, что результат вычисления по алгоритму SHA-1, выполняемого приборами 1-Wire, соответствует спецификации FIPS 180-1 за исключением того, что отсутствуют дополнительные завершающие константы. Согласно спецификации FIPS 180-1 эти константы добавляются к результату после вычисления каждого блока. Поскольку приборы 1-Wire обрабатывают только один блок, добавление этих констант не повышает секретность, и для ускорения аппаратного вычисления MAC-кода эта операция была удалена. Если требуется полное соответствие спецификации FIPS 180-1, эти константы могут быть добавлены самим блоком SCU.

На Рис. 3 показаны также области памяти и специальные регистры маркеров 1-Wire, которые будут использоваться в процессе верификации одной записи обслуживания. Каждый маркер содержит 64-битный уникальный идентификатор прибора, записанный лазером в ПЗУ. Поскольку этот уникальный *Идентификатор ПЗУ* имеется в каждом приборе, он может использоваться в качестве одной из составляющих при вычислении секрета, чтобы сделать секрет аутентификации каждого прибора уникальным (*Уникальный секрет аутентификации*). При выполнении аутентификации хост, например блок SCU, должен вновь вычислить *Уникальный секрет аутентификации*, используя *Секрет аутентификации мастера* и *Идентификатор ПЗУ*. В каждом приборе также имеется область временной памяти для хранения запроса аутентификации, посылаемого блоком SCU. Запрос представляет собой случайные

данные, генерируемые блоком SCU для того, чтобы каждый сеанс аутентификации был уникальным. *Номер страницы* — это физический адрес в памяти, по которому располагается блок данных.

Приборы 1-Wire считывают каждое из этих полей, обрабатывают эти данные при помощи встроенного процессора SHA-1, а затем возвращают MAC-код для аутентификации. Блок SCU получает ту же информацию, используя вычисленный *Уникальный секрет аутентификации*, и проверяет корректность MAC-кода. На Рис. 4 показано, каким образом происходит формирование MAC-кода аутентификации внутри прибора.

Рис. 4. Аутентификация маркера



* Только в DS1963S

Поскольку прибор DS1963S имеет неограниченный доступ для записи, запись обслуживания должна содержать *Сигнатуру данных обслуживания* для проверки достоверности данных. Этот MAC-код сохраняется вместе с данными обслуживания и используется для проверки достоверности данных счета. На Рис. 5 показано, какая информация используется для создания и проверки *Сигнатуры данных обслуживания*. Полная схема транзакции между модулем SCU и маркером DS1963S приведена на Рис. 6. То же, но для маркера DS1961S приводится на Рис. 7.

Рис. 5. Проверка достоверности данных обслуживания для DS1963S

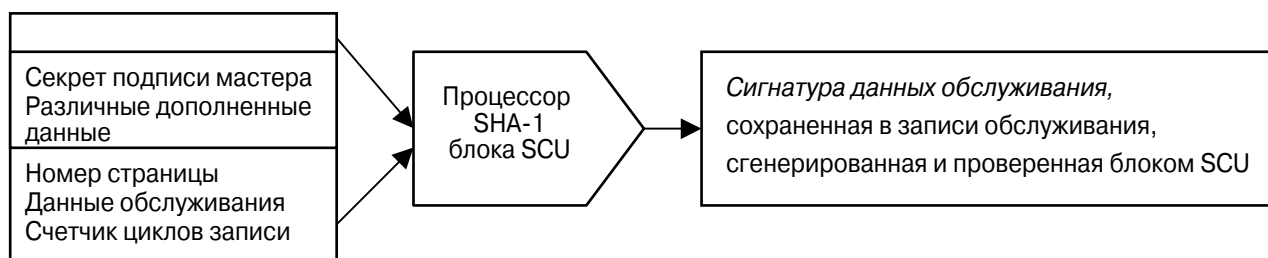
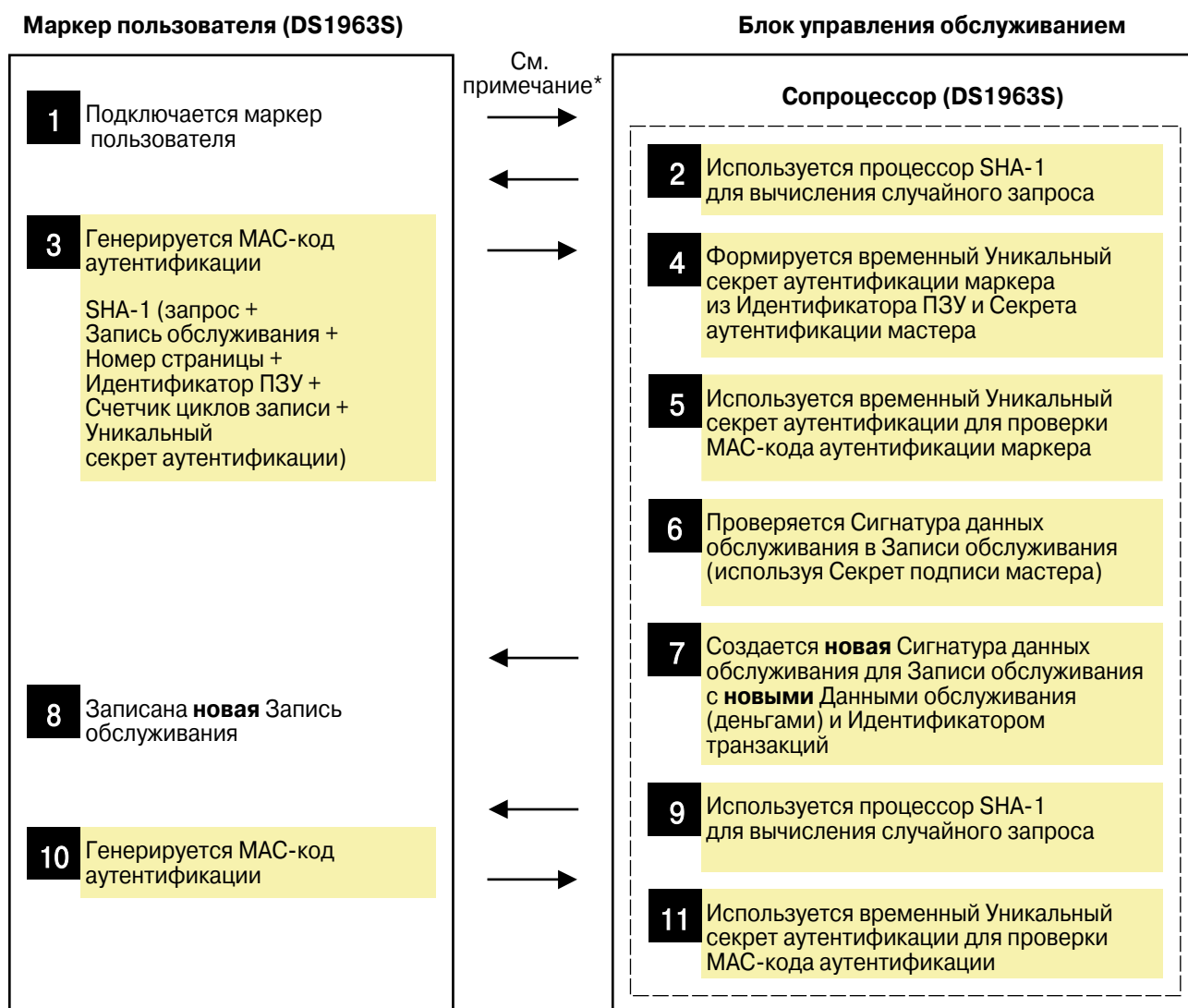


Рис. 6. Типичная блок-схема транзакции для маркера DS1963S

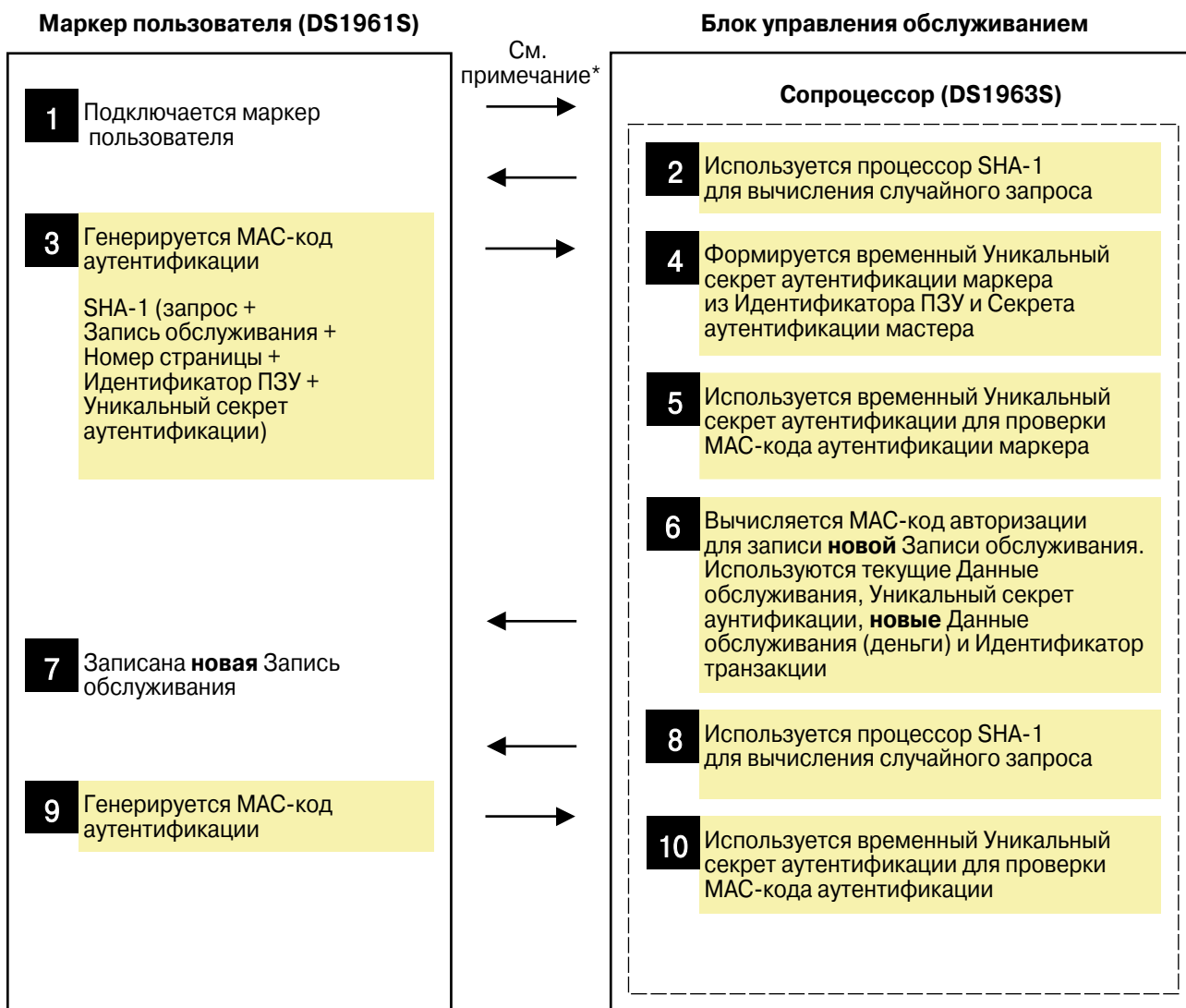


1 Номер шага

текст Выполнение вычислений по алгоритму SHA-1

* Примечание: Весь обмен данными между маркером пользователя и сопроцессором осуществляется мастером шины 1-Wire, таким как микропроцессор в блоке SCU.

Рис. 7. Типичная блок-схема транзакции для маркера DS1961S



1 Номер шага
 текст Выполнение вычислений по алгоритму SHA-1

* Примечание: Весь обмен данными между маркером пользователя и сопроцессором осуществляется мастером шины 1-Wire, таким как микропроцессор в блоке SCU.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Существует большое количество документации, которая может помочь в понимании и реализации систем, базирующихся на приборах SHA-1 шины 1-Wire. Информацию, содержащуюся в этих документах, можно разделить на три категории: *Теория*, *Подробности реализации* и *API* (см. Рис. 8). В документах из категории *Теория* рассматривается, каким образом с использованием имеющихся алгоритмов можно обеспечить безопасность электронных платежей. В документах, относящихся к категории *Подробности реализации*, описывается каждый этап и бит обмена данными, необходимый для выполнения аутентификации и операций с электронными деньгами при помощи приборов 1-Wire. Ресурсы по *API* позволяют сразу перейти к использованию приборов SHA-1. Исходный код этих API также может быть полезным инструментальным средством разработки для заказных применений.

Рис. 8. Обзор ресурсов

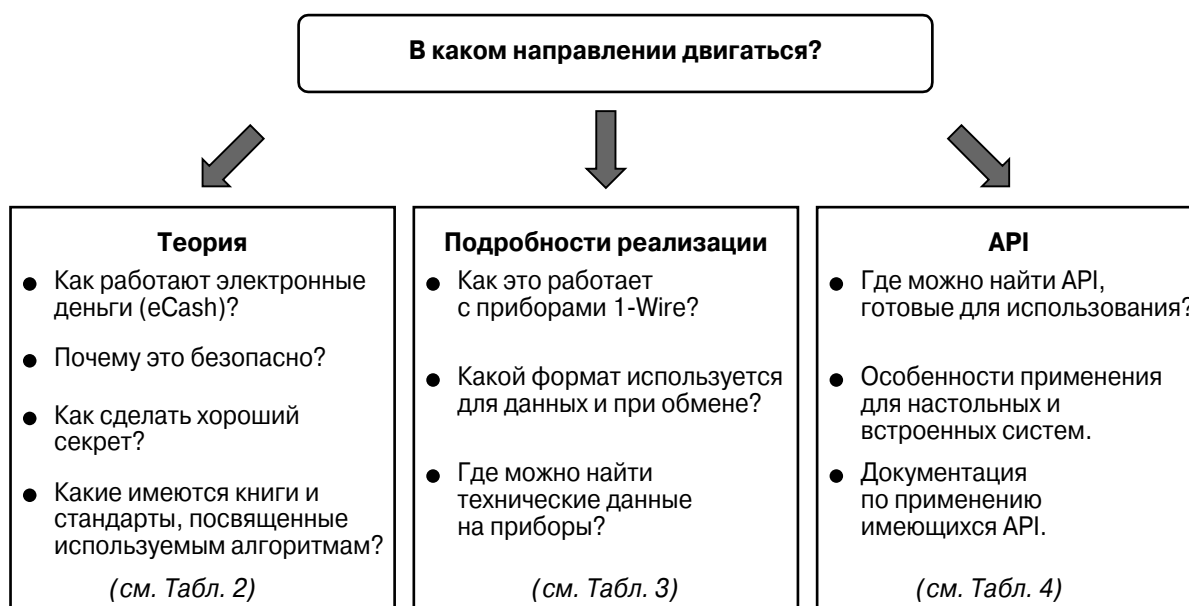


Таблица 2. ТЕОРИЯ

Electronic Cash and User Authentication using Dallas Semiconductor / Maxim DS1963S

(Электронные расчеты и аутентификация пользователей с использованием прибора DS1963S фирмы Dallas Semiconductor/Maxim)

Учебная презентация содержит подробное введение в систему электронных расчетов и характеристики приборов SHA-1 шины 1-Wire. Начиная с изложения основ в ней постепенно выстраиваются необходимые криптографические концепции и требования к техническим возможностям мобильных маркеров, используемых в системе электронных расчетов (eCash).

Документ Учебное пособие (Power Point)

URL ftp://ftp.dalsemi.com/pub/auto_id/public/ecash_sha_tutorial.ppt (4MB)

Glossary of 1 Wire SHA 1 Terms (Словарь терминов для SHA-1 шины 1-Wire)

Этот документ содержит список терминов, имеющих отношение к использованию приборов SHA-1 шины 1-Wire, таких как DS1963S, DS1961S и DS2432.

Документ White Paper 4 (PDF)

URL <http://pdfserv.maxim-ic.com/arpdf/AppNotes/wp4.pdf>

Challenge and Response with 1 Wire SHA devices

(Запрос и ответ с использованием приборов SHA шины 1-Wire)

В этом руководстве описаны основные механизмы запроса и ответа. Здесь также дается пример реализации системы, использующей приборы SHA 1-Wire. Для загрузки доступен код примера, использующий API 1-Wire для Java™.

Документ Руководство по применению 190 (PDF)

URL <http://pdfserv.maxim-ic.com/arpdf/AppNotes/app190.pdf>

SHA iButton Secrets and Challenges (Секреты и запросы SHA iButton)

Обзор, касающийся важности выбора хороших секретов и истинно случайных запросов. В этом документе приводятся несколько эмпирических правил, выполнение которых позволит избежать слабых мест в системе.

Документ Руководство по применению 152 (HTML)

URL http://dbserv.maxim-ic.com/appnotes.cfm?appnote_number=835

Why are 1 Wire SHA 1 Devices Secure?

(Почему приборы SHA-1 шины 1-Wire являются защищенными?)

В этом документе представлен сценарий использования приборов SHA-1 шины 1-Wire в системе *Обслуживания*. В общих чертах описаны возможные атаки на систему *Обслуживания*, а также описывается, каким образом благодаря возможностям приборов 1-Wire или использованию рекомендованной процедуры можно противостоять этим атакам.

Документ White Paper 3 (PDF)

URL <http://pdfserv.maxim-ic.com/arpdf/AppNotes/wp3.pdf>

Java является торговой маркой Sun Microsystems.

Passwords in SHA Authentication (Пароли в SHA-аутентификации)

В этом документе описывается метод, при котором вместе с приборами SHA-1 шины 1-Wire для аутентификации пользователя может использоваться пароль или PIN-код.

Документ Руководство по применению 154 (PDF)

URL <http://pdfserv.maxim-ic.com/arpdf/AppNotes/app154.pdf>

Information technology – Security techniques – Hash Functions – Part 3

(Информационные технологии – Методы обеспечения безопасности – Хэш-функции – Часть 3)

Стандарт ISO, в котором представлены различные методы хеширования, включая алгоритм SHA-1. На этот стандарт ссылаются другие стандарты ISO, касающиеся генерирования MAC-кода.

Документ Стандарт ISO/IEC 10118-3 (PDF для приобретения)

URL <http://webstore.ansi.org/ansidocstore/product.asp?sku=ISO%2FIEC+10118%2D3%3A1998>

Secure Hash Standard (Стандарт безопасного хеширования)

Федеральный стандарт по обработке информации (FIPS), в котором определяется алгоритм SHA-1.

Документ FIPS 180-1 (HTML)

URL <http://www.itl.nist.gov/fipspubs/fip180-1.htm>

Applied Cryptography, Second Edition (Практическая криптография, 2-е издание)

Хорошее введение в теорию и методы криптографии. Односторонние хэш-функции, включая SHA-1, описываются в главе 18.

Документ Bruce Schneier, John Wiley & Sons, 1996 (Print)

URL <http://www.wiley.com/cda/product/0,,0471128457|desc|2941,00.html>

Handbook of Applied Cryptography (Руководство по практической криптографии)

Чрезвычайно подробное руководство, освещающее различные криптографические методы, включая хеширование. Девятая глава книги специально посвящена хешированию и безопасности данных.

Документ A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996 (Print, PS, PDF)

URL <http://www.cacr.math.uwaterloo.ca/hac/>

Таблица 3. ПОДРОБНОСТИ РЕАЛИЗАЦИИ

SHA iButton API Overview (Обзор API для SHA iButton)

В документе представлен подробный обзор всех этапов, необходимых для того, чтобы создать API для системы электронных расчетов (eCash), использующей алгоритм SHA-1. Именно это руководство было использовано для создания API, поставляемых в составе комплектов разработчика фирмой Dallas Semiconductor.

Документ Руководство по применению 157 (PDF)
URL <http://pdfserv.maxim-ic.com/arpdf/AppNotes/app157.pdf>

Dallas Digital Monetary Certificates (Цифровые денежные сертификаты фирмы Dallas Semiconductor)

В документе разбирается формат данных стандартного сертификата, используемого в API фирмы Dallas Semiconductor для представления денежного счета. Формат включает также размещение данных и соответствующего им MAC-кода.

Документ Руководство по применению 151 (HTML)
URL http://dbserv.maxim-ic.com/appnotes.cfm?appnote_number=827

SHA 1 Devices used in Small Cash Systems (Приборы SHA-1, используемые в системах наличных расчетов)

В документе приводится очень детальное («шаг за шагом») описание операций, необходимых для выполнения аутентификации и eCash-транзакций с использованием приборов 1-Wire. Благодаря этому документ является великолепным руководством по созданию и верификации систем электронных расчетов (eCash).

Документ White Paper 1 (PDF)
URL (пока не опубликован; пожалуйста, следите за ссылкой
http://www.maxim-ic.com/appnotes10.cfm/ac_pk/1)

eCash Firmware Guide (Руководство по аппаратно-программному обеспечению систем eCash)

В этом руководстве описываются последовательность операций и различные состояния микропрограммы, используемой в демонстрационной плате eCash. На плате имеется процессор и два прибора DS1963S, используемые в качестве сопроцессоров при работе как с маркерами пользователя DS1963S, так и DS1961S. Программное обеспечение написано главным образом на «Си» (переносимый код) с небольшими вставками на ассемблере 8051.

Документ Руководство по применению
URL (пока не опубликован; пожалуйста, следите за ссылкой
http://www.maxim-ic.com/appnotes10.cfm/ac_pk/1)

DS1963S SHA iButton (Прибор SHA iButton DS1963S)

Спецификация на прибор DS1963S, в которой приведены все команды прибора и условия его эксплуатации.

Документ Спецификация (PDF)
URL <http://pdfserv.maxim-ic.com/arpdf/DS1963S.pdf>

