УДК 004.056.52

Е.В. Данилов, А.М. Вакилов
Казанский (Приволжский) федеральный университет, г. Казань

РЕАЛИЗАЦИЯ USB-ТОКЕНА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ U2F НА МИКРОКОНТРОЛЛЕРЕ

В данной статье описана реализация USB-токена двухфакторной аутентификации U2F на микроконтроллере STM32F103C8T6.
Ключевые слова: двухфакторная аутентификация; микроконтроллер; USB-токен.

E.V. Danilov, A.M. Vakilov
Kazan (Volga region) Federal university, Kazan

IMPLEMENTATION OF THE U2F TWO-FACTOR AUTHENTICATION USB - TOKEN ON A MICROCONTROLLER

This article describes the implementation of the U2F two-factor authentication USB-token on the STM32F103C8T6 microcontroller.
Keywords: two-factor authentication; microcontroller; USB-token.

В настоящее время в сети Internet существует большое количество ресурсов, так или иначе связанных с хранением персональных данных пользователей. Поэтому безопасность в интернете является значительной проблемой. К сожалению, в огромном количестве случаев пользователи плохо защищают свои учетные записи: используют слабые и одинаковые пароли на разных сервисах, что становится причиной взломов аккаунтов и, соответственно, кражи персональных данных. Помочь в решении данной проблемы призвана многофакторная аутентификация, при которой для доступа пользователю необходимо использовать сразу несколько факторов механизма аутентификации. Наиболее распространенным случаем многофакторной аутентификации является двухфакторная аутентификация (2FA). Поэтому при создании каких-либо информационных сервисов двухфакторная аутентификация становится неотъемлемой частью требований политики безопасности.

На сегодняшний день двухфакторная аутентификация представлена несколькими решениями [1]:

- одноразовые SMS-пароли, отправляемые на мобильный телефон пользователя;
- OTP - одноразовые пароли, сгенерированные на основе мастер-ключей, например, Yubikey;
- смарт-карты и криптографические токены, такие как RSA, Рутокен.

Однако, перечисленные решения имеют ряд недостатков: одноразовые пароли уязвимы к атакам “человек посередине” и, соответственно, фишингу, смарт-карты требуют установки драйверов и дополнительное оборудование для их считывания.

Чтобы устранить вышеуказанные недостатки, альянс Fast IDentity Online (FIDO), организованный в 2013 году, занимается разработкой безопасных, простых в использовании решений [1]. На сегодняшний день FIDO ввел несколько стандартов аутентификации, таких как Universal Second Factor (U2F) – универсальный второй фактор [2], Universal Authentication Framework – универсальный фреймворк для биометрической аутентификации.

В данной статье представлено описание USB-токена на микроконтроллере (МК) STM32, реализующего механизм двухфакторной аутентификации U2F [3, 4]. U2F – это бездрайверный 2FA-протокол, работающий по принципу вызов-ответной аутентификации с помощью ЭЦП.

Аппаратный токен, разработанный на основе микроконтроллера STM32F103C8T6 [5], подключается с помощью интерфейса USB к ПК. Предлагается применять данное устройство в качестве второго фактора аутентификации на различных ресурсах. Секретный ключ в представленном USB-токене создается с помощью генератора случайных чисел (ГСЧ) NeuG [6].

Рассмотрим функциональное назначение модулей, входящих в состав программы USB-токена (см. рис. 1).

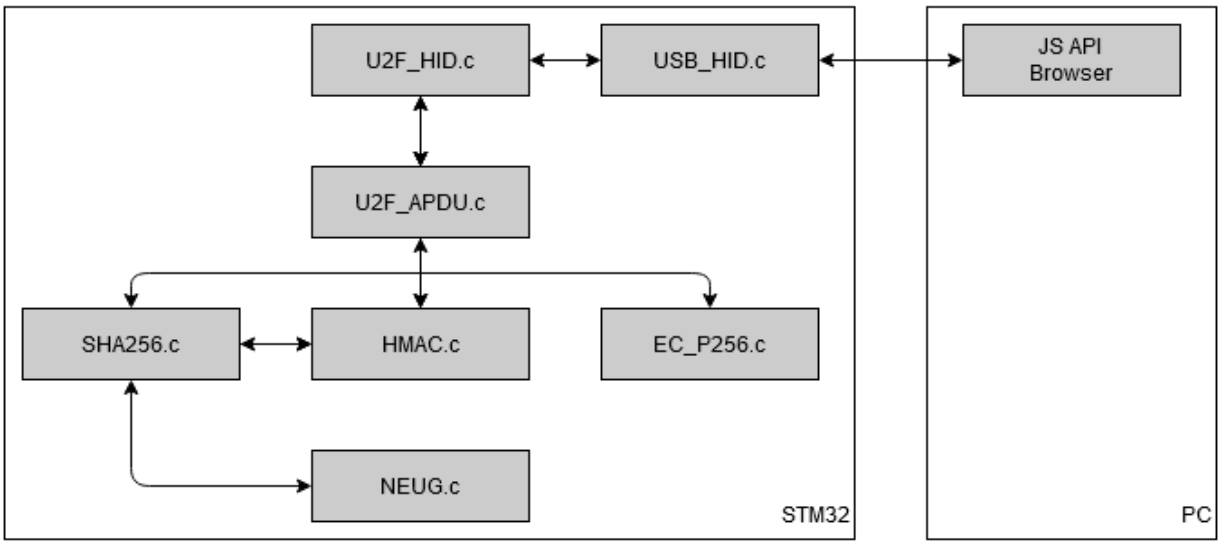

Рисунок 1 – Функциональная схема USB-токена U2F

- модуль U2FHID реализует функции приема и передачи данных, приходящих от JS API через класс HID интерфейса USB на U2F-токен;
- модуль USBHID реализует функцию передачи данных между МК и компьютером с помощью интерфейса USB;
- модуль U2FAPDU реализует функции регистрации USB-токена и аутентификации, функцию счетчика защиты от клонирования;

- модуль SHA256 реализует алгоритм хеширования SHA-256;
- модуль HMAC необходим для получения регистрационно-зависимой пары закрытый/открытый ключ по механизму hash-based message authentication code;
- модуль ECP256 реализует функцию цифровой подписи по алгоритму с открытым ключом ECDSA;
- модуль NEUG реализует функцию ГСЧ [6].

Алгоритмы регистрации и аутентификации USB-токена приведены на рис. 2 и рис. 3 соответственно.

При регистрации токен принимает данные от браузера по USB и создает случайное 32-байтовое число. После этого он создает секретный ключ с помощью алгоритма HMAC-SHA256 и объединенных случайного числа и данных, полученных от браузера. Аналогичным образом токен создает дескриптор ключа, только вместо случайного числа используется сгенерированный секретный ключ. Открытый ключ вычисляется на основе секретного ключа с использованием криптографии на эллиптических кривых над конечными полями (ECC). При успешной регистрации USB-токен отправляет веб-браузеру сообщение об этом, а также дескриптор и вычисленный открытый ключ.

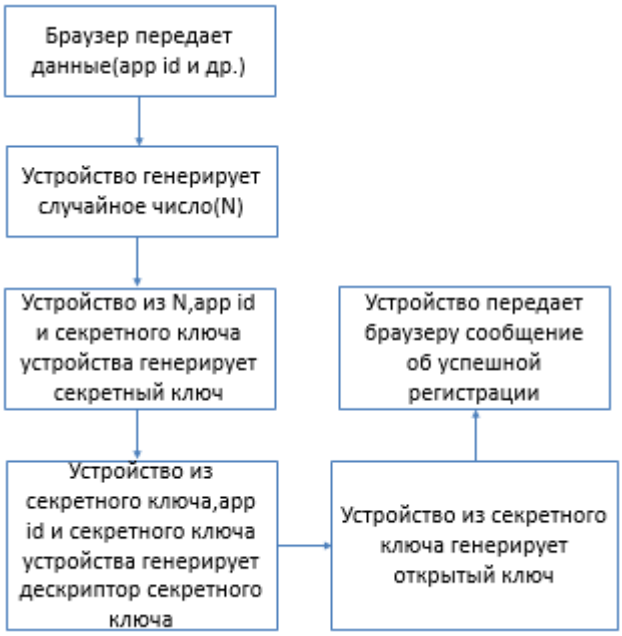

Рисунок 2 – Алгоритм регистрации

При аутентификации токен получает дескриптор от браузера и извлекает из него случайное число. Из случайного числа и данных браузера с помощью алгоритма HMAC-SHA256 создается секретный ключ, с его помощью создается дескриптор, который сравнивается с дескриптором, полученным от браузера. Если они совпадают, устройство отправляет браузеру сообщение об успешной аутентификации.

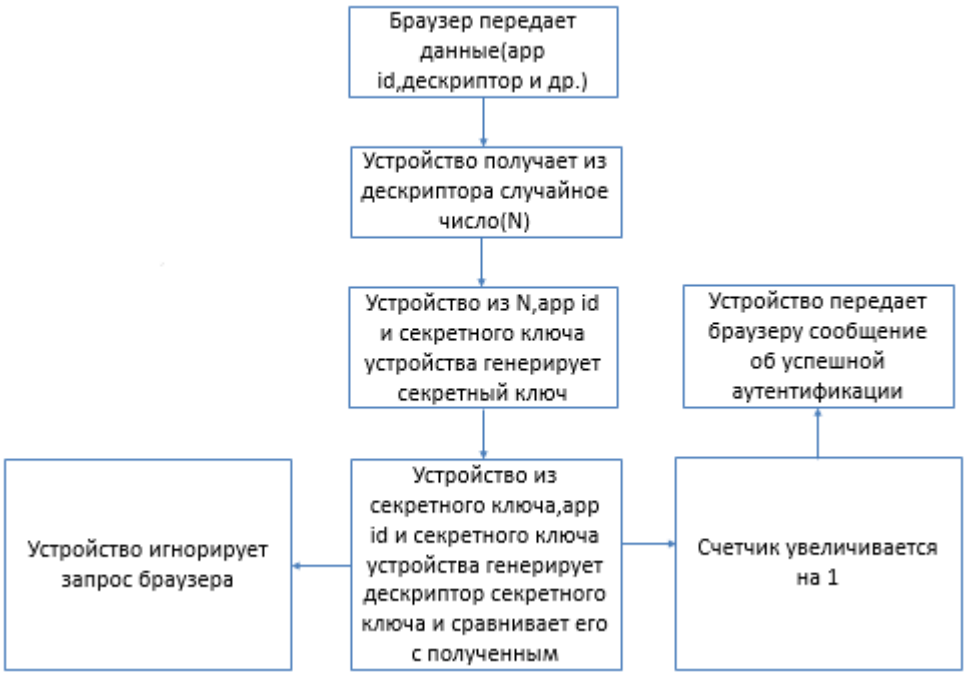

Рисунок 3 – Алгоритм аутентификации

Каждый раз при обновлении программного кода микроконтроллера USB-токена в определенный сектор внутренней Flash-памяти МК записывается новый сгенерированый ключ устройства. Данный ключ является секретным и для невозможности считывания его программатором устанавливается защита от чтения Flash-памяти с помощью Option bytes [5]. Также в USB-токене предусмотрен сброс счетчика защиты от клонирования. Данный счетчик инкрементируется во время процесса аутентификации.

В ходе работы на практике был реализован USB-токен двухфакторной аутентификации U2F на микроконтроллере STM32F103C8T6. Данный токен может быть использован владельцем как устройство для аутентификации на различных веб-сервисах. Для проверки работоспособности USB-токен был зарегистрирован в качестве электронного ключа в аккаунте Google и использован как второй фактор при аутентификации. Также устройство прошло проверку WebAuthn от Yubico.

Список литературы

1. FIDO U2F—Универсальная двухфакторная аутентификация. Введение. [Электронный ресурс]. – URL: https://habr.com/ru/post/305508/ (дата обращения 05.12.2020).

2. FIDO Alliance Fast Identity Online. [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/Компания:FIDO_Alliance_(Fast_IDentity_Online) (дата обращения 05.12.2020).

3. Universal 2nd Factor (U2F) Overview. [Электронный ресурс]. – URL: http://www.fidoalliance.org/specs/fido-u2f-overview-v1.0-ID-20141009.pdf (дата обращения 05.12.2020).

4. FIDO U2F Implementation Considerations. [Электронный ресурс]. – URL: http://www.fidoalliance.org/specs/fido-u2f-implementation-considerations-v1.0-ID-20141009.pdf (дата обращения 05.12.2020).

5. STM32F103C8. Datasheet. [Электронный ресурс]. – URL: https://www.st.com/resource/en/datasheet/stm32f103c8.pdf (дата обращения: 05.12.2020).

6. NeuG, a True Random Number Generator Implementation. [Электронный ресурс]. URL: https://www.gniibe.org/memo/development/gnuk/rng/neug.html (дата обращения: 05.12.2020).

Сведения об авторах

Данилов Евгений Валерьянович – ассистент кафедры радиофизики Казанского (Приволжского) федерального университета, г. Казань, email: evdan@mail.ru

Вакилов Альберт Маратович – магистрант Казанского национального исследовательского технического университета им. А.Н. Туполева–КАИ, г. Казань, email: amvakilov98@gmail.com

About the authors

Danilov Evgeniy Valerianovich - Assistant of the Department of radiophysics, Kazan (Volga region) Federal university, Kazan, email: evdan@mail.ru

Vakilov Albert Maratovich - Student of Kazan National Research Technical University named after A.N. Tupolev–KAI, Kazan, email: amvakilov98@gmail.com