Паспорт на MAC-токены ActivIdentity модель Token V2 и модель Pocket Token

Версия 1.0

Содержание

1. Общие сведения о МАС-токенах

Технические данные

МАС-токен – аппаратное устройство, предназначенное для использования при аутентификации пользователей, например, в системах дистанционного банковского обслуживания (ДБО).

Паспорт содержит сведения о двух моделях МАС-токенов компании ActivIdentity: Pocket Token и Token V2

	Pocket Token	**Token V2**
		
Физические данные:		
Размер ВхШхГ (мм)	68x48x8	82x52x4,5
Масса (г)	28	25
Размер знакоместа (пиксель)	5x7	
Размер экрана (символ)	10	
Наличие сменного элемента питания	нет	да
Срок эксплуатации элемента питания (лет)	6	3 для сменного, 8 для несменного резервного

Таблица 1. Основные характеристики, внешний вид, размеры

На лицевой стороне устройства расположены экран и цифровая клавиатура. С обратной стороны нанесен уникальный идентификатор МАС-токена и под заклеенной металлизированной полосой расположены контакты для программирования устройства с помощью программатора (см. рис. 1).

Рис. 1. Обратная сторона MAC-токена

Требования к эксплуатации

- Рабочая температура: от 0° до +50° C
- Температура хранения: от -10° до +50° C
- Относительная влажность: от 40 до 80% при температуре 25° C

Комплектация (состав) изделия

Устройство поставляется в отдельной упаковке, не требует никаких действий по подготовке к работе со стороны пользователя и полностью готово к эксплуатации.

2. Назначение и область применения

Основные функции MAC-токена:

- Работа в режиме 1 – генерация одноразового пароля (OTP – One Time Password);
- Работа в режиме 2 – вычисление по усиленной схеме кода подтверждения или подписи под введенными значениями (MAC – Message Authentication Code).
- Работа в режиме 3 – вычисление по стандартной схеме кода подтверждения или подписи под введенными значениями (MAC).

MAC-токен программируется производителем непосредственно на заводе-изготовителе. Для работы с системой электронного банкинга «iBank 2» компании «БИФИТ» устройство должно содержать специальную прошивку, необходимую для совместного использования с системой. При стандартной инициализации в каждый MAC-токен программируется уникальный идентификатор и секретный ключ MAC-токена. Также идентификатор наносится непосредственно на сам MAC-токен на обратной стороне в виде алфавитно-цифровой последовательности и штрих-кода (см. рис. 1). В MAC-токен встроены часы для отсчета времени и внутренний счетчик состояний.

MAC-токен генерирует **одноразовый пароль** как криптографическую функцию от:

- секретного ключа устройства;
- текущего момента времени (внутренний таймер);
- значения счетчика состояния (внутренний счетчик).

Используется криптоалгоритм 3DES. Длина одноразового пароля составляет **10** цифр.

Процедура формирования и проверки **одноразового пароля** происходит следующим образом:

1. Клиенту для входа в АРМ системы ДБО необходимо пройти аутентификацию. В качестве дополнительного подтверждения полномочий клиенту может быть назначена расширенная аутентификация с использованием одноразовых паролей. Источником получения одноразового пароля может выступать MAC-токен.
2. Для входа клиенту необходимо ввести одноразовый пароль, сгенерированный MAC-токеном.
3. Клиент вводит в MAC-токен PIN-код, тем самым получая доступ к функциям устройства, и выбирает генерацию одноразового пароля.
4. MAC-токен генерирует одноразовый пароль.
5. Клиент вводит значение одноразового пароля в АРМ системы ДБО, где оно отправляется на банковский сервер.
6. Для проверки валидности одноразового пароля банковский сервер выполняет аналогичное криптографическое преобразование с использованием секретного ключа устройства, хранимого на стороне банка. При совпадении результата сформированного устройством и вычисленного сервером – одноразовый пароль считается валидным.
7. При совпадении одноразового пароля клиент успешно осуществляет вход в АРМ, при несовпадении – отказ во входе в АРМ.

MAC-токен формирует **код подтверждения** в соответствии с одним из режимов:

Режим 2. Код вычисляется как функция от:

1. секретного ключа устройства;
2. значений, вводимых клиентом с клавиатуры токена:
   - БИК банка получателя;

- счет получателя;
- сумма платежа;

3. текущего момента времени (внутренний таймер).

Используется криптоалгоритм 3DES. Длина кода подтверждения составляет **10** цифр.

Код подтверждения, сформированный в соответствии с режимом 2, может быть использован в системе ДБО для подтверждения платежного поручения, реквизитов доверенного получателя рублевых платежей.

Режим 3. Код вычисляется как функция от:

1. секретного ключа устройства;
2. значений, вводимых клиентом с клавиатуры токена:
   - идентификатор сессии;
   - сумма платежа;
   - последние 6 цифр счета получателя;
3. значения счетчика состояния (внутренний счетчик).

Используется криптоалгоритм 3DES. Длина кода подтверждения составляет **8** цифр.

Код подтверждения, сформированный в соответствии с режимом 3, может быть использован в системе ДБО для подтверждения платежного поручения, реквизитов доверенного получателя рублевых платежей.

Процедура формирования и проверки **кода подтверждения** (подпись под ключевыми реквизитами) происходит следующим образом:

1. Клиент формирует в системе ДБО электронный документ (например, платежное поручение).
2. Для отправки в банк электронного документа клиенту необходимо ввести код подтверждения, сгенерированный MAC-токеном.
3. Клиент вводит в MAC-токен PIN-код, тем самым получая доступ к функциям устройства, и выбирает генерацию кода подтверждения.
4. Клиент вводит с клавиатуры MAC-токена ключевые реквизиты документа.
5. MAC-токен вычисляет код подтверждения.
6. Клиент вводит значение кода подтверждения в систему ДБО и направляет его на банковский сервер.
7. Сервер выполняет проверку путем аналогичного криптографического вычисления кода подтверждения и сравнения со значением присланным клиентом.
8. При совпадении кода подтверждения авторство и целостность электронного документа считаются верными. При несовпадении система ДБО отвергает полученный электронный документ.

3. Работа пользователя с MAC-токеном

Включение и выключение MAC-токена осуществляется нажатием на его клавиатуре кнопки 

Доступ к функциям MAC-токена защищен PIN-кодом.

Обращение пользователя к функциям устройства осуществляется нажатием на клавиатуре MAC-токена соответствующей цифры:

1 – генерация одноразового пароля;

2 – формирование кода подтверждения в режиме 2;

3 – формирование кода подтверждения в режиме 3.

Общие параметры MAC-токена		**Примечание**
Значение начального PIN-кода устройства	1234	
Принудительная смена PIN-кода пользователем	да	Необходимо выполнить при первом включении
Длина PIN-кода (символ)	min – 4 max – 8	
Проверка PIN-кода на сложность	да	Отсутствует возможность задавать значения вида: 0000, 1234
Максимальное количество попыток неверного ввода PIN-кода	15	Исчерпание попыток приводит к блокировке устройства
Время отображения на экране значений одноразового пароля, кода подтверждения (сек)	30	По истечении времени устройство автоматически выключается
Параметры одноразового пароля		
Длина пароля (символ)	10	
Срок действия пароля (мин)	2	
Параметры генерации кода подтверждения (Режим 2)		
Длина значения "БИК" (символ)	9	
Длина значения "Первая часть счета" (символ)	9	
Длина значения "Вторая часть счета" (символ)	10	
Максимальная длина значения "Сумма" (символ)	10	Вводится только целая часть суммы
Длина кода (символ)	10	
Срок действия кода (мин)	2	
Параметры генерации кода подтверждения (Режим 3)		
Длина значения "Идентификатор сессии" (символ)	min – 4 max – 10	
Максимальная длина значения "Сумма" (символ)	10	Вводится только целая часть суммы
Длина значения "Параметр 1" (символ)	min – 4 max 10	
Длина значения "Параметр 2" (символ)	min – 4 max – 10	Необязательно
Длина кода (символ)	8	
Срок действия кода (мин)	2	

Первое включение устройства

1. Включите МАС-токен, нажав на его клавиатуре кнопку ⏻
2. При этом на экране токена появится сообщение **"ВВЕСТИ ПИН"**. Наберите на клавиатуре токена последовательность – **"1234"** начальный ПИН-код для доступа к устройству, заданный на заводе изготовителе, который будет предложено сменить в следующем шаге.
3. На экране появится сообщение **"СМЕН. ПИН"**. Нажмите кнопку ⏻
4. На экране появится сообщение **"НОВЫЙ ПИН"**. Введите числовую последовательность от 4 до 8 цифр и нажмите кнопку ⏻. Не допускается назначение простого ПИН-кода вида: `0000, 12345`. В случае ввода некорректного значения на экране появится сообщение **"ОШИБКА"**. Укажите другое значение и нажмите кнопку ⏻
5. На экране появится сообщение **"ПОВТОР.ПИН"**. Введите числовую последовательность еще раз и нажмите кнопку ⏻
6. На экране появится сообщение **"ГОТОВО"** и устройство отключится.

Смена PIN-кода устройства

1. Включите МАС-токен, нажав на его клавиатуре кнопку ⏻
2. При этом на экране токена появится сообщение **"ВВЕСТИ ПИН"**. Введите ПИН-код. После ввода корректного ПИН-кода на экране токена появится сообщение **"ВЫБРАТЬ"**
3. Нажмите один раз на клавиатуре токена кнопку ←
4. На экране появится сообщение **"СМЕН. ПИН"**. Нажмите кнопку ⏻. На экране появится сообщение **"НОВЫЙ ПИН"**. Введите числовую последовательность от 4 до 8 цифр и нажмите кнопку . Не допускается назначение простого ПИН-кода вида: `0000, 12345`. В случае ввода некорректного значения на экране появится сообщение **"ОШИБКА"**. Укажите другое значение.
5. На экране появится сообщение **"ПОВТОР.ПИН"**. Введите числовую последовательность еще раз и нажмите кнопку ⏻
6. На экране появится сообщение **"ГОТОВО"** и устройство отключится.

Генерация одноразового пароля (Режим 1)

1. Включите МАС-токен, нажав на его клавиатуре кнопку ⏻
2. При этом на экране токена появится сообщение **"ВВЕСТИ ПИН"**. Введите ПИН-код. После ввода корректного ПИН-кода на экране токена появится сообщение **"ВЫБРАТЬ"**
3. Нажмите на клавиатуре токена цифру **"1"**
4. На экране появится числовая последовательность длиной **десять** символов – одноразовый пароль, который можно вводить в используемое приложение.

Генерация кода подтверждения (Режим 2)

1. Включите МАС-токен, нажав на его клавиатуре кнопку ⏻
2. При этом на экране токена появится сообщение **"ВВЕСТИ ПИН"**. Введите ПИН-код. После ввода корректного ПИН-кода на экране токена появится сообщение **"ВЫБРАТЬ"**
3. Нажмите на клавиатуре токена цифру **"2"**

4. На экране появится сообщение **"БИК БАНКА"**. Введите БИК банка получателя платежа и нажмите кнопку
5. На экране появится сообщение **"Счет 1_10"**. Введите первые десять цифр номера счета и нажмите кнопку
6. На экране появится сообщение **"Счет 11_20"**. Введите оставшиеся десять цифр номера счета получателя и нажмите кнопку
7. На экране появится сообщение **"СУММА"**. Введите сумму платежа в рублях (целая часть без копеек) и нажмите кнопку
8. На экране отобразится **десятизначный** код подтверждения, который можно вводить в используемое приложение.

Генерация кода подтверждения (Режим 3)

1. Включите MAC-токен, нажав на его клавиатуре кнопку
2. При этом на экране токена появится сообщение **"ВВЕСТИ ПИН"**. Введите ПИН-код. После ввода корректного ПИН-кода на экране токена появится сообщение **"ВЫБРАТЬ"**
3. Нажмите на клавиатуре токена цифру **"3"**
4. На экране появится сообщение **"ИД. СЕССИИ"**. Введите идентификатор сессии и нажмите кнопку
5. На экране появится сообщение **"СУММА"**. Введите сумму платежа (без дробной части) и нажмите кнопку
6. На экране появится сообщение **"ПАРАМЕТР 1"**. Введите последние 6 цифр счета получателя и нажмите кнопку
7. На экране появится сообщение **"ПАРАМЕТР 2"**. Значение параметра 2 не используется, нажмите кнопку
8. На экране отобразится **восьмизначный** код подтверждения, который можно вводить в используемое приложение.

4. Адрес изготовителя

Производитель:	«ActivIdentity Europe S.A.», (Франция)
Адрес:	24-28 avenue du Général de Gaulle 92156 Suresnes Cedex (France).
Телефон:	+33 (0) 1 42 04 84 00,
Факс:	+33 (0) 1 42 04 84 84,
Сайт:	http://www.actividentity.com