ОАО «БИФИТ»
Банковские И Финансовые
Интернет Технологии

http://www.bifit.com
e-mail: info@bifit.com
ph/fax +7 (495) 797-88-89

ПАСПОРТ

на MAC-токены ActivIdentity

модель Token V2 и модель Pocket Token

Оглавление

1. Общие сведения о MAC-токенах

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

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

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

Таблица 1. Основные характеристики, внешний вид, размеры

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

Рисунок 1. Обратная сторона MAC-токена

2. Требования к эксплуатации

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

3. Комплектация (состав) изделия

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

4. Назначение и область применения

Две основные функции MAC-токена:

- Генерация одноразового пароля (OTP - One Time Password);
- Вычисление кода подтверждения или подписи под введенными значениями (MAC - Message Authentication Code).

MAC-токен программируется производителем непосредственно на заводе-изготовителе. 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 своих 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 и получает доступ к функции генерации 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 - получает отказ во входе в АРМ.

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

Синхронный. Код вычисляется как функция от:

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

- сумма платежа

3. текущего момента времени (внутренний таймер).

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

Код подтверждения, полученный синхронным способом, может быть использован в системе ДБО для подтверждения платежных поручений и получателей рублевых платежей.

Асинхронный. Код вычисляется как функция от:

1. секретного ключа устройства;
2. значений, вводимых клиентом с клавиатуры токена:
   - идентификатор сессии
   - сумма платежа
   - до 2-х любых реквизитов платежа (настраивается на стороне банка)
3. значения счетчика состояния (внутренний счетчик).

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

Код подтверждения, полученный асинхронным способом, может быть использован в системе ДБО для подтверждения произвольных транзакций (в настоящий момент в системе «iBank 2» не используется).

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 и получает доступ к функции генерации кода подтверждения.
4. Клиент вводит с клавиатуры MAC-токена ключевые реквизиты документа (счет получателя, БИК банка получателя, сумма).
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.

5. Работа пользователя с MAC-токеном

Включение MAC-токена происходит нажатием на его клавиатуре кнопки 

Доступ к функциям MAC-токена защищен PIN-кодом.

Обращение пользователя к функциям устройства происходит при нажатии на соответствующую цифру на клавиатуре MAC-токена:

- 1 - генерация одноразового пароля;
- 2 – формирование синхронного кода подтверждения;
- 3 – формирование асинхронного кода подтверждения.

Общие параметры MAC-токена		**Примечание**
Значение начального PIN-кода устройства	1234	Принудительная смена PIN-кода пользователем при первом включении
Длина PIN-кода (символ)	min – 4 max - 8	
Проверка PIN-кода на сложность	да	Запрещены простые пароли
Максимальное количество неверных попыток ввода PIN-кода	15	Исчерпывание попыток приводит к блокировке устройства и не может быть устранено самостоятельно
Время отображения на экране значений одноразового пароля, кода подтверждения после получения (сек)	30	По истечении времени устройство автоматически выключается.
Выключение устройства	кнопка 	
Параметры генерации одноразового пароля		
Длина получаемого пароля (символ)	10	
Срок действия полученного значения (мин)	2	
Параметры генерации кода подтверждения (синхронный алгоритм)		
Длина значения “БИК” (символ)	9	
Длина значения “Первая часть счета” (символ)	10	

Длина значения “Вторая часть счета” (символ)	10	
Максимальная длина значения “Сумма ” (символ)	10	Вводится только целая часть числа
Длина получаемого кода (символ)	10	
Срок действия полученного значения (мин)	2	
Параметры генерации кода подтверждения (асинхронный алгоритм)		
Длина значения “Идентификатор сессии” (символ)	min – 4 max - 10	
Максимальная длина значения “Сумма ” (символ)	10	Вводится только целая часть числа
Длина значения “Параметр 1” (символ)	min – 4 max - 10	
Длина значения “Параметр 2” (символ)	min – 4 max - 10	Необязательно
Длина получаемого кода (символ)	8	
Срок действия полученного значения (мин)	2	

Первое включение устройства

1. Включите MAC-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, 1234, 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.

Смена PIN-кода устройства

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 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, 1234, 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

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 **"1"**.
4. На экране появится числовая последовательность длиной **десять** символов – одноразовый пароль, который можно вводить в используемое приложение.

Генерация кода подтверждения (синхронный алгоритм)

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 **"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. На экране появится сообщение **"Счет 11_20"**. Введите оставшиеся десять цифр номера счета получателя и нажмите кнопку  .
6. На экране появится сообщение **"СУММА"**. Введите сумму платежного поручения в рублях (целая часть без копеек) и нажмите кнопку  .
7. На экране отобразится **десятизначный** код подтверждения, который можно вводить в используемое приложение.

Генерация кода подтверждения (асинхронный алгоритм)

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 поручения (без дробной части) и нажмите кнопку  .
6. На экране появится сообщение **"ПАРАМЕТР 1"**. Введите значение параметра 1 и нажмите кнопку  .
7. На экране появится сообщение **"ПАРАМЕТР 2"**. Введите значение параметра 2 и нажмите кнопку  .
8. На экране отобразится **восьмизначный** код подтверждения, который можно вводить в используемое приложение.

6. Адрес изготовителя

Производитель:	«ActivIdentity Inc.» (США)
Адрес:	15370 Barranca Pkwy Irvine, CA 92618-3106.
Телефон:	(949) 732-2000, (800) 237-7769
Факс:	(949) 732-2120
Сайт:	http://www.actividentity.com