## **2.3.1 Механизмы аутентификации**

### **Стандарт 802.11 – 2012 определяеттакоепонятие, какAKM – Authenticationandkeymanagementsuite - набор средств для выполнения аутентификации и управления ключами. AKM – это совокупность алгоритмов, предназначенных для аутентификации и управления ключами либо по отдельности, либо в сочетании с алгоритмами аутентификации и управления ключами более высокого уровня, использующихся вне области применения данного стандарта [10]. Каждый набор определяет, какие операции между клиентом и аутентификатором будут производиться, а также последовательность выполнения. Использование того или иного набора определяется выбором одного из следующих механизмов защиты:**

* **Аутентификация предустановленным ключом (PSK – Pre-sharedkey)**
* **Аутентификацияпопротоколу EAP (Extensible authentication protocol)**

**Аутентификация предустановленным ключом**

### **Данный механизм аутентификации предполагает использование предварительно настроенного на беспроводном клиенте и точке доступа ключа. Следующие операции AKMбудут выполнены в случае использования этого механизма:**

### Станция узнает политики безопасности точки доступа через пассивный мониторинг с помощью beacon-фреймов, или через активное прослушивание. После обнаружения станция выполняет SAE-аутентификацию (Simultaneousauthenticationofequals) с точкой доступа (Рис.11).

### После успешного завершения SAE-аутентификации станция и точка доступа генерируют парный мастер-ключ(PairwiseMasterKey – PMK).

### Парный мастер-ключ, сгенерированный с помощью SAE, используется в четырехстороннем рукопожатии (4-wayhandshake), для генерации парного переходного ключа (PairwiseTransientKey - PTK).



Рис11. Аутентификация SAE

### Аутентификация SAE представляет собой вариант обмена ключами на основе доказательства с нулевым разглашением и используется беспроводными узлами для аутентификации с помощью пароля [10]. В результате успешного завершения аутентификации между узлами распределяется парный мастер-ключ PMK (PairwiseMasterKey, PMK). Аутентификация SAE обладает следующими особенностями:

### злоумышленник не может определить пароль или PMK не только в случае пассивного наблюдения обмена сообщениями, но и в случае активного вмешательства в него;

### злоумышленник не может определить пароль или результирующий общий ключ с помощью модификации, подмены или воспроизведения кадров, а также в случае, если в процессе аутентификации участвуют неповрежденные устройства;

### злоумышленник не может производить более одной попытки угадывания пароля за атаку;

### компрометация PMK из предыдущего запуска протокола не дает злоумышленнику преимуществ в определении пароля или общего ключа.

### В отличие от других протоколов аутентификации, в SAE нет таких понятий, как “инициатор” и “респондент”. Стороны обмена равноправны и каждая сторона может инициировать запуск протокола.

**Аутентификация по протоколу EAP**

**Стандарт IEEE 802.1x используется для аутентификации и авторизации пользователей и рабочих станций в сети передачи данных [17]. В случае использования протокола для беспроводных сетей для выполнения аутентификации используется протокол EAP**(ExtensibleAuthenticationProtocol - расширяемый протокол аутентификации), который поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной сети и ее пользователей с возможностью динамическойгенерации ключейшифрования [18]**. Согласно протоколу 802.1xдоступ к сети получают только те устройства, которые прошли аутентификацию. Когда беспроводной клиент подключается к порту, точка доступа проверяет, разрешен ли доступ в сеть для этого клиента. Если доступ запрещен, точка доступа блокирует порт и до успешного завершения процедуры аутентификации соединение возможно только по протоколу EAPoL (EAPoverLan).**

Архитектура IEEE 802.1x включает в себя три обязательных компонента, которые участвуют в процедуре аутентификации([Рис.](http://www.intuit.ru/studies/courses/1004/202/lecture/5252?page=7" \l "image.9.13" \t "_blank) 11):

* Клиент (Supplicant) - запрашивает аутентификацию и доступ к сети. Каждый клиент имеет уникальные учетные данные, которые проверяются на сервере аутентификации.
* Аутентификатор(Authenticator) - устройство, которое блокирует или разрешает прохождение трафика через порт.В беспроводной ЛВС

как правило это либо точка доступа или контроллер WLAN



Рис.12. Архитектура IEEE 802.1x

* Сервер аутентификации (Authenticationserver) - сервер, который проверяет учетные данные клиента, запрашивающего доступ и уведомляетаутентификатор о результатах прохождения процедуры аутентификации.

IEEE 802.1x предоставляет абоненту беспроводной локальной сети лишь средства передачи атрибутов серверу аутентификации и допускает использование различных методов и алгоритмов аутентификации. Задачей сервера аутентификации является поддержка разрешенных политикой сетевойбезопасности методоваутентификации.

Следующие операции выполняются при использовании аутентификации по протоколу 802.1x:

1. Станция узнает политики безопасности точки доступа через пассивный мониторинг с помощью beacon-фреймов, или через активное прослушивание (Рис. 13).



Рис. 13. Процесс установления соединения

1. Если обнаруживается, что аутентификаториспользует аутентификацию по протоколу 802.1x, клиент отправляет EAPoL-Start (опционально)илиаутентификатор отправляет ProbeRequest и начинается процесс установления соединения по протоколу EAP (Рис.14).
2. Клиент и аутентификатор проверяют подлинность друг друга и переходят к процессу, называемому четырехстороннее рукопожатие (4-wayhandshake) для выработки ключей (Рис. 15).
3. Четырехстороннее рукопожатиезавершает процедуру аутентификации по протоколу 802.1x[19]. Процедура инициируется аутентификатором, при этом используется формат пакета EAPoL-key, и предназначена для выполнения следующих операций:

Рис. 14. Аутентификация cиспользование протокола EAP

* подтверждения того, что сторонам, участвующие в процессе аутентификации известен текущий парный мастер-ключ.
* выработка нового парного передаточного ключа из парного мастер-ключа.
* подтверждения соответствия сторон возможностям RSN
* соглашение о выборе шифровального набора (ciphersuite) –набора алгоритмов предназначенных для обеспечения конфиденциальности, целостности и аутентичности данных.

**Процедура рукопожатия начинается с вычисления клиентом и аутентификатором парного мастер-ключа (PMK) [10]. После того, как PMKсгенерирован начинается обмен сообщениями EAPoL-key.В первом сообщении аутентификатор посылает кадр EAPoL-key, содержащий ANonce (AuthenticatorNonce). ANonce – одноразовое случайное или псевдослучайное число.Оно одинаково для первого и третьего сообщений. Случайное число Nonce генерируется следующим образом:**

**Все станции содержат в себе счетчик глобальных ключей размером 256 бит.**



Рис. 15. Четырехстороннее рукопожатие

**Он инициализируется при загрузке системы. Значение счетчика устанавливается с помощью псевдослучайной функции:**

Nonce =PRF-256(Random number, “Init Counter”, Local MAC Address || Time), где

PRF-256 – псевдослучайнаяфункция(PseudorandomFunction), результат которой имеет размер 256 бит;

Randomnumber – случайноечисло;

“Init Counter” – строка;

Local MAC Address – MAC адресустройства;

Time – время, согласно в формате протокола NTP (NetworkTimeProtocol).

**Во втором сообщении клиент генерирует случайное число SNonce (SupplicantNonce). Далее, с помощью полученногоANonce, и сгенерированного SNonce клиент вычисляетпарный передаточный ключ (PTK–PairwiseTransientKey). КлиентпосылаеткадрEAPoL-key, которыйсодержитSNonce, RSNE (RobustSecurityNetworkelement) изкадра (Re)AssociationRequestиMIC.Аутентификатор также использует ANonce и SNonce для вычисления PTK с помощью той же псевдослучайной функции, что и клиент. Также аутентификатор вычисляет MIC и сверяет вычисленныйMIC с полученным от клиента. Если аутентификатор обнаруживает несовпадение, сообщение отбрасывается. Далее аутентификатор отсылаеттретье сообщение, содержащее ANonce, RSNE из кадров Beacon или ProbeResponse, MIC, а также указание клиенту на возможность установки временных ключей. В завершающем сообщенииклиент отсылаетMIC и указание на то, что ключи установлены.**

**Вычисление парного передаточного ключа – одна из важнейших задач, выполняемых с помощью процедуры четырехстороннего рукопожатия, т.к. именно этот ключ содержит в себе ключевой материал для дальнейших криптографических преобразований. Всю совокупность ключей стандарта 802.11 – 2012 удобно представить с помощью иерархии ключевого материала.**