Схема FORMS-аутентификации с использованием сессий:

1. Когда пользователь вводит свои учетные данные (например, имя пользователя и пароль) на веб-странице, они отправляются на сервер для проверки.
2. Сервер проверяет введенные данные с базой данных пользователей. Если данные верны, сервер создает уникальную сессию для этого пользователя и присваивает ей идентификатор.
3. Идентификатор сессии возвращается клиенту в виде HTTP-куки или в запросе. Клиент сохраняет этот идентификатор для последующих запросов.
4. При каждом последующем запросе клиент включает идентификатор сессии в запрос, чтобы сервер мог определить, какой пользователь делает запрос.
5. Сервер проверяет идентификатор сессии и принимает решение о доступе к ресурсам или выполнении запрошенных операций на основе данных, связанных с этой сессией. Например, сервер может проверить, имеет ли пользователь права на доступ к определенным страницам или функциям.
6. При завершении сеанса пользователя или выходе из системы сервер уничтожает сессию и идентификатор становится недействительным.

Схема FORMS-аутентификации с использованием токенов:

1. Когда пользователь вводит свои учетные данные на веб-странице, они отправляются на сервер для проверки.
2. Сервер проверяет введенные данные с базой данных пользователей. Если данные верны, сервер создает уникальный токен аутентификации и возвращает его клиенту.
3. Клиент сохраняет полученный токен, обычно в localStorage или sessionStorage веб-браузера, чтобы использовать его для последующих запросов.
4. При каждом последующем запросе клиент включает токен аутентификации в заголовок или запрос, чтобы сервер мог определить, какой пользователь делает запрос.
5. Сервер проверяет токен аутентификации, используя секретный ключ для проверки подлинности токена. Если токен действительный, сервер разрешает доступ к ресурсам или выполнение запрошенных операций.
6. Токен имеет время жизни, после истечения которого он становится недействительным. Клиент может обновить токен, обратившись к серверу с запросом на обновление.
7. При завершении сеанса пользователя или выходе из системы клиент удаляет или инвалидирует токен, чтобы предотвратить его использование другими лицами.