

# Обобщенный алгоритм аутентификации в системах Pseudo-SSO

Аверченко Кирилл, Панасенко Сергей, ООО Фирма «АНКАД»

(499)731-0000, (499)732-1313

[develop@ancud.ru](mailto:develop@ancud.ru)

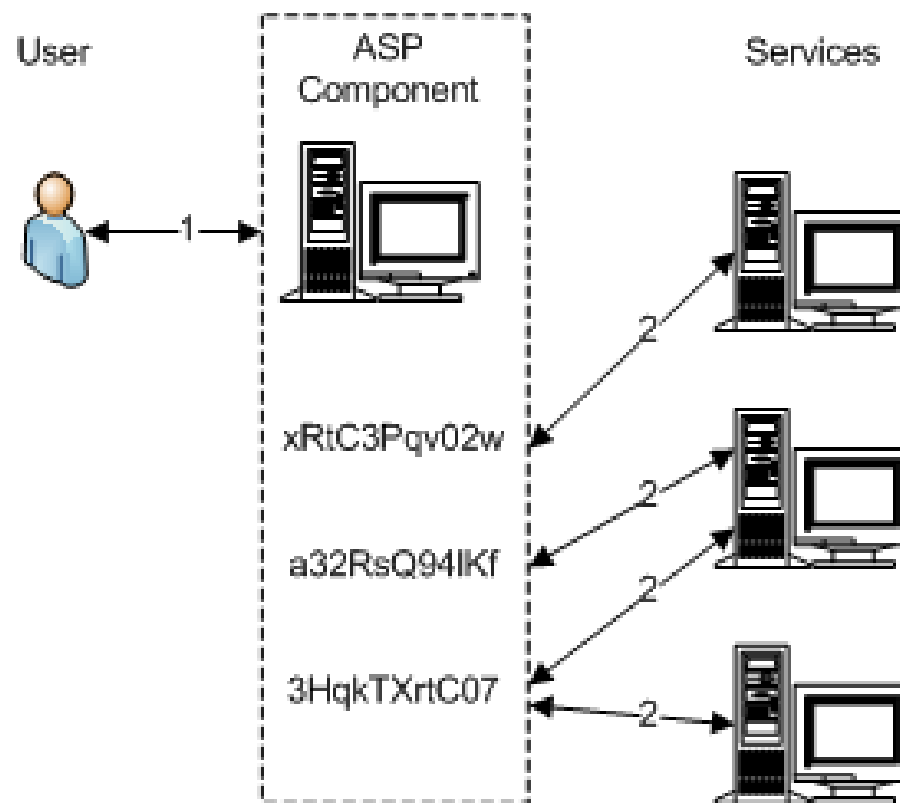
[www.ancud.ru](http://www.ancud.ru)



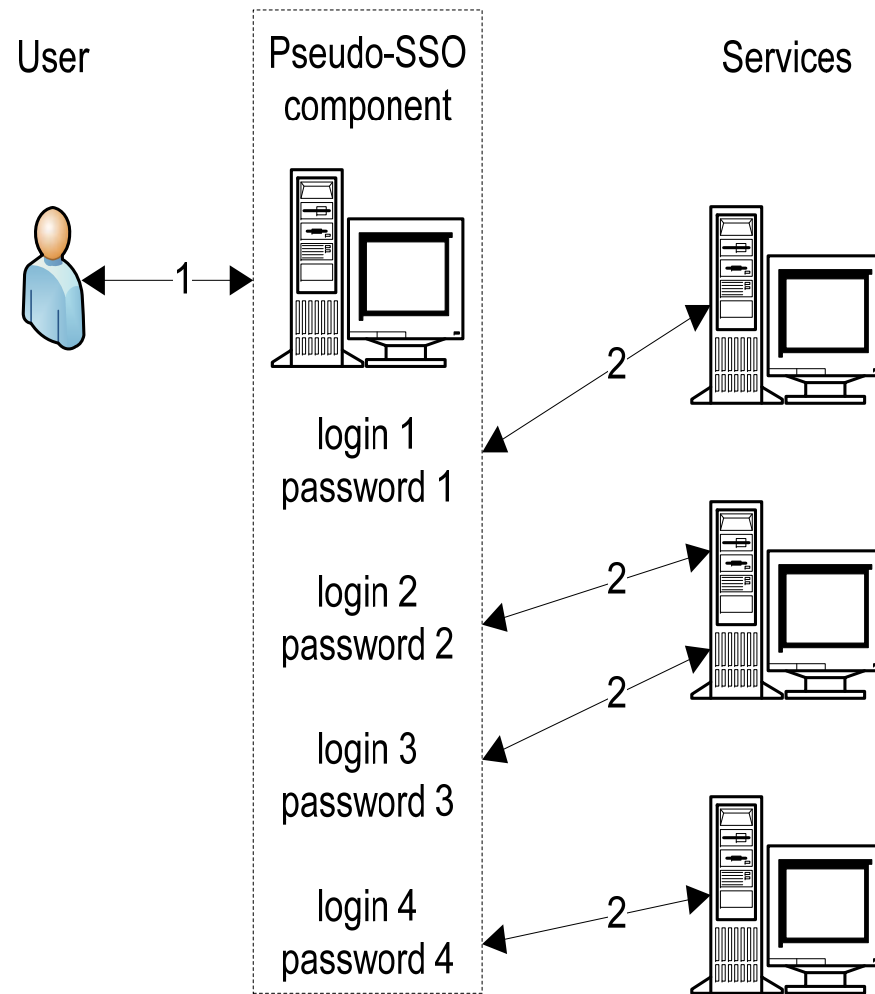
# Классификация систем SSO

- Pseudo SSO системы
- True SSO системы

# Схема работы систем True SSO



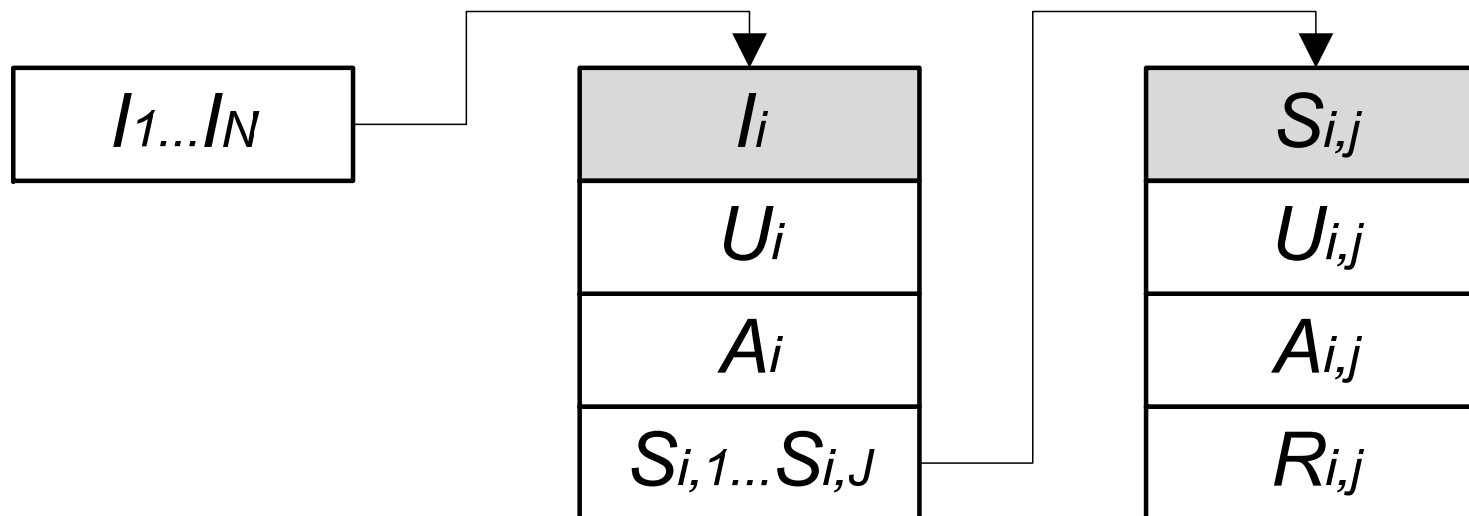
# Схема работы систем Pseudo SSO



# Обзор реализаций систем Pseudo SSO

- Windows LiveID
- OpenID (LiveJournal)
- Использование банковских карт стандарта EMV
- Запоминание аутентифицирующей информации в веб-браузере

# Информационные структуры модулей, реализующих Pseudo SSO



$$I_i = \{U_i, A_i, \{S_{ij}\}\}, i = 1 \dots N,$$

где:

$N$  – количество пользователей системы;

$U_i$  – идентификатор  $i$ -го пользователя;

$A_i$  – набор информации, необходимой для аутентификации  $i$ -го пользователя на компоненте Pseudo-SSO;

$$S_{i,j} = \{U_{i,j} \ A_{i,j} \ R_{i,j}\}, j = 1 \dots J$$

где:

$S_{i,j}$  – набор прав и параметров  $i$ -го пользователя по отношению к  $j$ -му ресурсу;

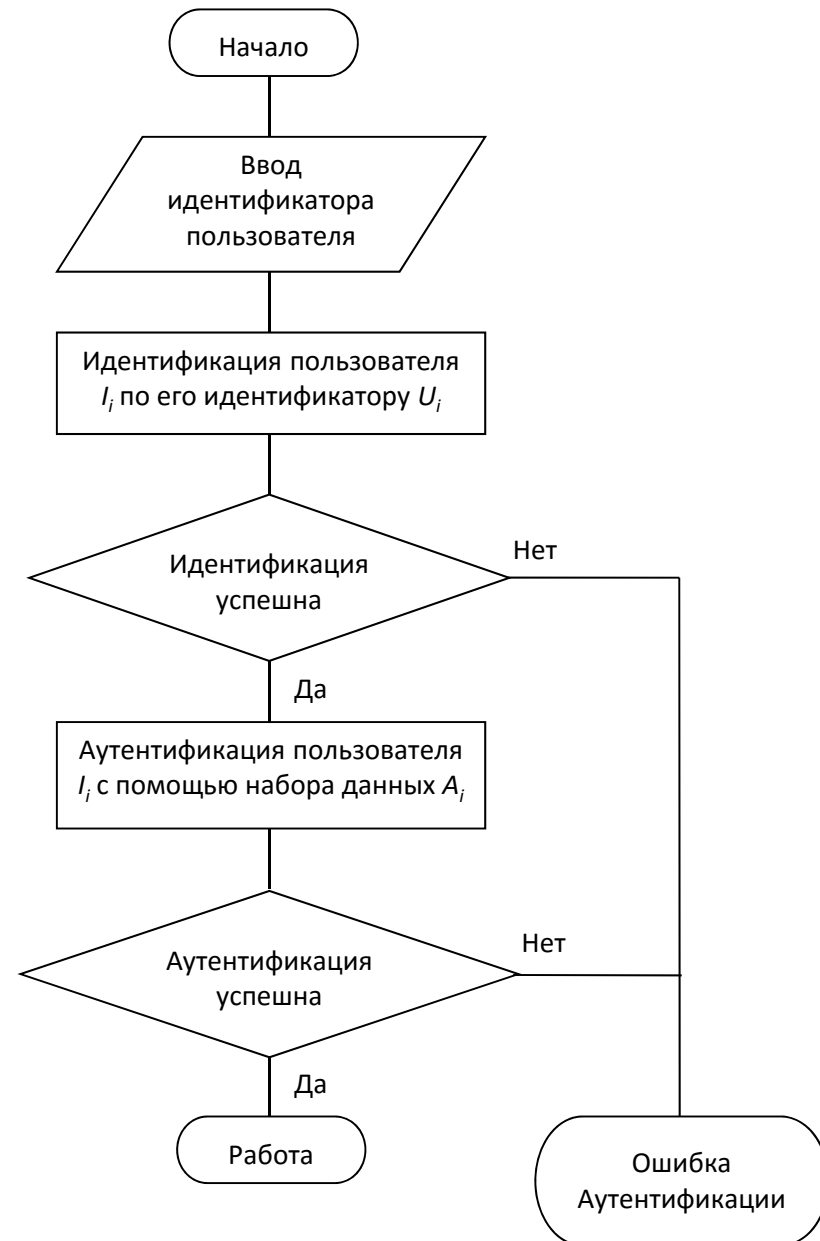
$U_{i,j}$  – идентификатор  $i$ -го пользователя на  $j$ -м ресурсе;

$A_{i,j}$  – информация, необходимая для прохождения аутентификации  $i$ -го пользователя на  $j$ -м ресурсе;

$R_{i,j}$  – множество прав пользователя по отношению к  $j$ -му ресурсу.



# Первичная аутентификация пользователей



1. Компонент Pseudo-SSO проверяет введенный пользователем идентификатор и ищет запись о данном пользователе  $I_i$  по его идентификатору  $U_i$ , т. е. выполняет идентификацию пользователя.
2. Компонент Pseudo-SSO выполняет аутентификацию пользователя с помощью набора данных  $A_i$ .
3. При ошибке на любом из двух предыдущих шагов аутентификация считается неуспешной.

# Аутентификация пользователя при запросе доступа к ресурсам системы Pseudo SSO

1. Компонент Pseudo-SSO ищет в наборах  $\{S_i\}$  записи о данном пользователе информацию о возможностях доступа пользователя к  $j$ -му ресурсу ( $S_{i,j}$ ).
2. Если набор  $S_{i,j}$  не найден, пользователю отказывается в доступе к ресурсу.

3. В найденном наборе проверяется соответствие множества запрошенных прав доступа  $R$  и множества прав пользователя по доступу к данному ресурсу : если  $R \subseteq R_{ij}$ , то доступ разрешается, иначе – запрещается.
4. Из набора  $S_{ij}$  выбирается идентификатор пользователя на ресурсе и информация, необходимая для прохождения аутентификации  $\{U_{ij}, A_{ij}\}$ . Данная информация предъявляется  $j$ -му ресурсу, в результате чего пользователь получает или не получает доступ к нему.

# Спасибо за внимание!

Аверченко Кирилл, Панасенко Сергей, ООО Фирма «АНКАД»

(499)731-0000, (499)732-1313

[develop@ancud.ru](mailto:develop@ancud.ru)

[www.ancud.ru](http://www.ancud.ru)

