```
% stateless auth tokens
% ÐµÐ»ÐµÐ¼ÐµÐ½ÑM-^BÐ°ÑM-^@ÐµÐ½ ÑM-^BÑM-^@Ð¸Ð°
% ÐM-^RÐ°ÑM-^AÐ¸Ð» ÐM-^ZÐ¾Ð»ÐµÐ² <vasil@ludost.net>

# ÐM-^_ÑM-^@Ð¾Ð±Ð»ÐµÐ¼ÑM-^JÑM-^B

## Ð§ÐµÑM-^AÑM-^BÐ¾ ÑM-^AÑM-^@ÐµÑM-^IÐ°Ð½Ð° Ð¿ÑM-^@Ð°ÐºÑM-^BÐ¸ÐºÐ°

* Ð½ÑM-^CÐ¶ÐµÐ½ token Ð•Ð° Ð½ÐµÑM-^IÐ¾
    + login
    + ÐºÐ¾Ð´ Ð•Ð° reset Ð½Ð° Ð¿Ð°ÑM-^@Ð¾Ð»Ð°
    + ÐºÐ°ÑM-^BÐ¾ ÑM-^FÑM-^OÐ»Ð¾ Ð½ÐµÑM-^IÐ¾, ÐºÐ¾ÐµÑM-^BÐ¾ Ð´Ð° Ð¿ÑM-^@Ð°ÑM-^BÐ
¸Ð¼ Ð¸ Ð´Ð° ÑM-^CÐ´Ð¾ÑM-^AÑM-^BÐ¾Ð²ÐµÑM-^@Ð¸, ÑM-^GÐµ ÑM-^GÐµ Ð¾ÑM-^BÑM-^AÑM-^@Ð
µÑM-^IÐ½Ð°ÑM-^BÐ° ÑM-^AÑM-^BÑM-^@Ð°Ð½Ð° Ð³Ð¾ Ðµ Ð¿Ð¾Ð»ÑM-^CÑM-^GÐ¸Ð»Ð°
* Ð³ÐµÐ½ÐµÑM-^@Ð¸ÑM-^@Ð° ÑM-^AÐµ random Ð¸ ÑM-^AÐµ Ð¿Ð¸ÑM-^HÐµ Ð² ÑM-^BÐ°Ð±Ð»Ð¸Ñ
M-^FÐ°
* Ð±ÐµÐ•ÑM-^AÐ¼Ð¸ÑM-^AÐ»ÐµÐ½Ð¾ Ð´ÐµÐ¹ÑM-^AÑM-^BÐ²Ð¸Ðµ
* Ð¿Ð¾Ð´Ð»ÐµÐ¶Ð¸ Ð½Ð° DoS

<!--
ÐM-^\Ð½Ð¾Ð³Ð¾ ÑM-^GÐµÑM-^AÑM-^BÐ¾ Ð½Ð¸ ÑM-^AÐµ Ð½Ð°Ð»Ð°Ð³Ð° Ð´Ð° Ð³ÐµÐ½ÐµÑM-^@Ð¸
ÑM-^@Ð°Ð¼Ðµ token/ÐºÐ¾Ð´, ÐºÐ¾Ð¹ÑM-^BÐ¾ Ð´Ð° Ð¸Ð•Ð¿ÑM-^@Ð°ÑM-^BÐ¸Ð¼ Ð½Ð° Ð½ÑM-^O
ÐºÐ¾Ð¹ Ð¿Ð¾ÑM-^BÑM-^@ÐµÐ±Ð¸ÑM-^BÐµÐ» (Ð¿Ð¾ ÑM-^AÑM-^BÑM-^@Ð°Ð½Ð¸ÑM-^GÐµÐ½ ÐºÐ°Ð½
Ð°Ð»), Ð•Ð° Ð´Ð° ÑM-^AÐµ ÑM-^CÐ´Ð¾ÑM-^AÑM-^BÐ¾Ð²ÐµÑM-^@Ð¸. ÐM-^UÐ´Ð½Ð¾ ÑM-^GÐµÑ
M-^AÑM-^BÐ¾ ÑM-^AÑM-^@ÐµÑM-^IÐ°Ð½Ð¾ ÑM-^@ÐµÑM-^HÐµÐ½Ð¸Ðµ Ðµ Ð´Ð° ÑM-^AÐµ Ð³ÐµÐ½Ð
µÑM-^@Ð¸ÑM-^@Ð° Ð½ÐµÑM-^IÐ¾ ÑM-^AÑM-^JÐ²ÑM-^AÐµÐ¼ random, ÐºÐ¾ÐµÑM-^BÐ¾ Ð¾Ð±Ð°Ñ
M-^GÐµ Ð²Ð¾Ð´Ð¸ Ð´Ð¾ Ð¿Ð°Ð•ÐµÐ½Ðµ Ð½Ð° ÑM-^BÐ²ÑM-^JÑM-^@Ð´Ðµ Ð¼Ð½Ð¾Ð³Ð¾ state Ð¸
 Ð¼Ð½Ð¾Ð³Ð¾ ÑM-^GÐµÑM-^AÑM-^BÐ¾ Ð½Ðµ Ðµ Ð¿ÑM-^@Ð°ÐºÑM-^BÐ¸ÑM-^GÐµÑM-^AÐºÐ¸ Ð²Ñ
M-^JÐ•Ð¼Ð¾Ð¶Ð½Ð¾.
-->

# Ð ÐµÑM-^HÐµÐ½Ð¸ÐµÑM-^BÐ¾

## Ð¿ÑM-^@Ð¾ÑM-^AÑM-^BÐ¾ ÑM-^@ÐµÑM-^HÐµÐ½Ð¸Ðµ - Ð¿Ð¾Ð´Ð¿Ð¸ÑM-^A ÑM-^A ÐºÑM-^@Ð¸Ð
¿ÑM-^BÐ¾Ð³ÑM-^@Ð°ÑM-^DÑM-^AÐºÐ¸ hash

* \$userid.\$timestamp.\$somethingelse.\$sign
* \$sign = sha1(\$userid.\$timestamp.\$somethingelse.\$secret)
    + somethingelse Ð¼Ð¾Ð¶Ðµ Ð´Ð° ÑM-^AÐµ Ð¿Ð¾Ð»Ð•Ð²Ð° Ð•Ð° salt, Ð•Ð° Ð´Ð¾Ð¿Ñ
M-^JÐ»Ð½Ð¸ÑM-^BÐµÐ»Ð½Ð° ÑM-^AÐ¸Ð³ÑM-^CÑM-^@Ð½Ð¾ÑM-^AÑM-^B
* Ð¿ÑM-^@Ð¾Ð²ÐµÑM-^@ÑM-^OÐ²Ð° ÑM-^AÐµ ÑM-^AÐµ ÑM-^BÑM-^@Ð¸Ð²Ð¸Ð°Ð»Ð½Ð¾
* Ð½Ðµ Ð¸Ð•Ð¸ÑM-^AÐºÐ²Ð° state
* Ð½Ðµ Ð¿Ð¾Ð´Ð»ÐµÐ¶Ð¸ Ð½Ð° DoS-Ð¾Ð²Ðµ

<!--
ÐM-^_ÑM-^@Ð¾Ð±Ð»ÐµÐ¼ÑM-^JÑM-^B Ð¸Ð¼Ð° Ð¿ÑM-^@Ð¾ÑM-^AÑM-^BÐ¾ ÑM-^@ÐµÑM-^HÐµÐ½Ð¸Ðµ
, ÑM-^GÑM-^@ÐµÐ• ÐºÑM-^@Ð¸Ð¿ÑM-^BÐ¾Ð³ÑM-^@Ð°ÑM-^DÑM-^AÐºÐ¸ (hash) Ð¿Ð¾Ð´Ð¿Ð¸Ñ
M-^AÐ°Ð½ token, Ð¾ÑM-^B ÐºÐ¾Ð¹ÑM-^BÐ¾ Ð¼Ð¾Ð¶Ðµ Ð´Ð° ÑM-^AÐµ Ð¸Ð•Ð²Ð°Ð´Ð¸ ÑM-^FÑ
M-^OÐ»Ð°ÑM-^BÐ° Ð¸Ð½ÑM-^DÐ¾ÑM-^@Ð¼Ð°ÑM-^FÐ¸ÑM-^O, Ð±ÐµÐ• Ð´Ð° Ðµ Ð½ÑM-^CÐ¶Ð½Ð¾ Ð
´Ð° ÑM-^AÐµ Ð³Ð»ÐµÐ´Ð° Ð½ÑM-^OÐºÐ°ÐºÑM-^JÐ² state. ÐM-^SÐµÐ½ÐµÑM-^@Ð¸ÑM-^@Ð° Ñ
M-^AÐµ ÑM-^BÑM-^@Ð¸Ð²Ð¸Ð°Ð»Ð½Ð¾...
-->

## ÐM-^XÐ½Ð²Ð°Ð»Ð¸Ð´Ð°ÑM-^FÐ¸ÑM-^O Ð½Ð° token

* ÐM-^PÐ²ÑM-^BÐ¾Ð¼Ð°ÑM-^BÐ¸ÑM-^GÐ½Ð¾ Ð¾ÑM-^B timestamp-Ð° Ð¸ Ð¸Ð•ÑM-^BÐ¸ÑM-^GÐ°Ð
½Ðµ Ð½Ð° Ð´Ð°Ð´ÐµÐ½Ð¸ÑM-^O Ð¶Ð¸Ð²Ð¾ÑM-^B Ð½Ð° token-Ð°
* ÐM-^WÐ° login - sha1($userid.$password.$secret)
    + ÑM-^AÐ¼ÑM-^OÐ½Ð°ÑM-^BÐ° Ð½Ð° Ð¿Ð°ÑM-^@Ð¾Ð»Ð°ÑM-^BÐ° Ð¸Ð½Ð²Ð°Ð»Ð¸Ð´Ð¸ÑM-^@Ð
° token-Ð°
* Ð¿Ð¾-Ð³ÐµÐ½ÐµÑM-^@Ð°Ð»Ð½Ð¾ ÑM-^@ÐµÑM-^HÐµÐ½Ð¸Ðµ - Ð¿Ð°Ð•Ð¸Ð¼ ÐºÐ¾Ð³Ð° Ðµ Ð¸Ð•Ð
´Ð°Ð´ÐµÐ½ Ð¿Ð¾ÑM-^AÐ»ÐµÐ´Ð½Ð¸ÑM-^OÑM-^B Ð²Ð°Ð»Ð¸Ð´ÐµÐ½ token
    + Ð½Ð°Ð»Ð°Ð³Ð° ÑM-^AÐµ Ð´Ð° Ð´ÑM-^JÑM-^@Ð¶Ð¸Ð¼ state, Ð½Ð¾ Ðµ Ð¿Ð¾-Ð¼Ð°Ð»ÐºÐ
¾
* replay Ð°ÑM-^BÐ°ÐºÐ¸?

<!--
Ð¾ÑM-^IÐµ Ð¼Ð°Ð»ÐºÐ¾ Ð½ÐµÑM-^IÐ°, Ð´ÐµÑM-^BÐ¾ ÑM-^IÐµ Ð´Ð¾Ð¿Ð¸ÑM-^HÐ°
-->


# ÐM-^_ÑM-^@Ð¸Ð¼ÐµÑM-^@Ð¸

<!--
ÐM-^X Ð¿ÑM-^@Ð¸Ð¼ÐµÑM-^@Ð¸
-->

## VERP

* Ð¸Ð•Ð¼Ð¸ÑM-^AÐ»ÐµÐ½ Ð¾ÑM-^B DJB
* https://en.wikipedia.org/wiki/Variable_envelope_return_path

<!--
ÐM-^WÐ° Ð²ÑM-^AÐ¸ÑM-^GÐºÐ¸, ÐºÐ¾Ð¸ÑM-^BÐ¾ ÑM-^BÑM-^@ÑM-^OÐ±Ð²Ð° Ð´Ð° Ð¿ÑM-^@Ð°Ñ
M-^IÐ°ÑM-^B Ð¿Ð¾ÑM-^IÐ° Ð¸ Ð´Ð° Ð•Ð½Ð°ÑM-^OÑM-^B Ð´Ð°Ð»Ð¸ Ð°Ð´ÑM-^@ÐµÑM-^AÑM-^JÑ
M-^B Ð½Ðµ Ðµ bounce-Ð½Ð°Ð».
-->

## TCP Syncookies

* ÑM-^AÑM-^JÑM-^IÐ¾ Ð¸Ð•Ð¼Ð¸ÑM-^AÐ»ÐµÐ½Ð¾ Ð¾ÑM-^B djb
* https://en.wikipedia.org/wiki/Syncookies

<!--
ÐM-^RÐµÑM-^GÐµ default Ð½Ð° Ð²ÑM-^AÐ¸ÑM-^GÐºÐ¸ tcp/ip ÑM-^AÑM-^BÐµÐºÐ¾Ð²Ðµ.
-->

## client-side session

* ÐM-^RÑM-^AÐ¸ÑM-^GÐºÐ¾ Ð² ÑM-^AÐµÑM-^AÐ¸ÑM-^OÑM-^BÐ° + Ð¿Ð¾Ð´Ð¿Ð¸ÑM-^A + timest
amp
* Ð½Ð° ÑM-^AÑM-^JÑM-^@Ð²ÑM-^JÑM-^@Ð° - ÑM-^AÐ°Ð¼Ð¾ Ð¿Ð¾ÑM-^AÐ»ÐµÐ´ÐµÐ½ timestamp
 Ð½Ð° Ð¿ÑM-^@Ð¾Ð¼ÑM-^OÐ½Ð° Ð½Ð° ÑM-^AÐµÑM-^AÐ¸ÑM-^OÑM-^BÐ°

<!--
ÐM-^TÐ° ÑM-^AÐ¿ÐµÑM-^AÑM-^BÐ¸Ð¼ Ð¼ÑM-^OÑM-^AÑM-^BÐ¾ Ð¾ÑM-^B Ð¿Ð¾ÑM-^BÑM-^@ÐµÐ±Ð¸
ÑM-^BÐµÐ»ÑM-^AÐºÐ¸ ÑM-^AÐµÑM-^AÐ¸Ð¸.
-->
```