```
% stateless auth tokens
% ÐµÐ»ÐµÐ¼ÐµÐ½ÑM-^BÐ°ÑM-^@ÐµÐ½ ÑM-^BÑM-^@Ð¸Ðº
% 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

<!--
(ÑM-^BÐ¾Ð·Ð¸ ÑM-^BÑM-^@Ð¸Ðº Ð²ÐµÑM-^@Ð¾ÑM-^OÑM-^BÐ½Ð¾ Ð¸Ð¼Ð° Ð½ÑM-^OÐºÐ°ÐºÐ²Ð¾ Ñ
M-^AÑM-^BÐ°Ð½Ð´Ð°ÑM-^@ÑM-^BÐ½Ð¾ Ð¸Ð¼Ðµ, ÐºÐ¾ÐµÑM-^BÐ¾ Ð°Ð· Ð½Ðµ Ð·Ð½Ð°Ð¼, ÑM-^FÑ
M-^OÐ»Ð°ÑM-^BÐ° Ð»ÐµÐºÑM-^FÐ¸ÑM-^O Ð¼Ð¸ ÑM-^EÑM-^@ÑM-^CÐ¼Ð½Ð° ÐµÐ´Ð½Ð° Ð²ÐµÑM-^G
ÐµÑM-^@ Ð´Ð¾ÐºÐ°ÑM-^BÐ¾ Ð½Ðµ Ð¼Ð¾Ð¶ÐµÑM-^E Ð´Ð° ÑM-^AÐ¿ÑM-^O Ð¸ ÑM-^BÐ°ÐºÐ° Ð¸ Ð
½Ðµ ÑM-^AÐµ Ð·Ð°ÑM-^@Ð¾Ð²Ð¸ÑM-^E)

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/hash mac

* \$userid.\$timestamp.\$somethingelse.\$sign
* \$sign = HMAC(\$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, ÐºÐ°ÑM-^BÐ¾ Ð´Ð¾ Ð¸Ð½ÑM-^DÐ¾ÑM-^@Ð¼Ð°ÑM-^FÐ¸Ñ
M-^OÑM-^BÐ° ÑM-^AÐµ Ð´Ð¾Ð»ÐµÐ¿ÑM-^O ÐµÐ´Ð¸Ð½ HMAC Ð¿Ð¾Ð´Ð¿Ð¸ÑM-^A ÑM-^A Ð½ÑM-^OÐ
ºÐ°ÐºÑM-^JÐ² secret, ÐºÐ¾Ð¹ÑM-^BÐ¾ Ð²Ð¸ Ðµ Ð¿Ð¾Ð·Ð½Ð°ÑM-^B Ð½Ð° Ð²Ð°ÑM-^A.
(hmac Ðµ Ð¼ÐµÑM-^BÐ¾Ð´ Ð·Ð° Ð¿ÑM-^@Ð¸Ð»Ð°Ð³Ð°Ð½Ðµ Ð½Ð° hash ÑM-^DÑM-^CÐ½ÐºÑM-^FÐ
¸ÑM-^O, Ð½Ð°Ð¿ÑM-^@Ð¸Ð¼ÐµÑM-^@ sha1. ÐM-^]Ðµ Ðµ Ð´Ð¾Ð±ÑM-^@Ð° Ð¸Ð´ÐµÑM-^O Ð´Ð° Ñ
M-^AÐµ Ð¸Ð·Ð¿Ð¾Ð»Ð·Ð²Ð° Ð´Ð¸ÑM-^@ÐµÐºÑM-^BÐ½Ð¾ SHA1 Ð¸Ð»Ð¸ Ð½ÐµÑM-^IÐ¾ Ð¾ÑM-^B Ñ
M-^AÑM-^JÑM-^IÐ¾ÑM-^BÐ¾ ÑM-^AÐµÐ¼ÐµÐ¹ÑM-^AÑM-^BÐ²Ð¾, Ð¿Ð¾Ð½ÐµÐ¶Ðµ Ð¿Ð¾Ð´Ð»ÐµÐ¶Ð¸
 Ð½Ð° lengthening Ð°ÑM-^BÐ°ÐºÐ°, Ð½Ð¾ Ð¼Ð¾Ð¶Ðµ Ð´Ð° ÑM-^AÐµ Ð¿Ð¾Ð»Ð·Ð²Ð° SHA3)

Ð¢Ð°ÐºÐ° ÑM-^BÐ°Ð·Ð¸ Ð¸Ð½ÑM-^DÐ¾ÑM-^@Ð¼Ð°ÑM-^FÐ¸ÑM-^O ÑM-^AÐµ Ð¿ÑM-^@Ð¾Ð²ÐµÑM-^@
ÑM-^OÐ²Ð° ÑM-^BÑM-^@Ð¸Ð²Ð¸Ð°Ð»Ð½Ð¾, Ð¸ Ð½Ðµ Ð¸Ð·Ð¸ÑM-^AÐºÐ²Ð° Ð´Ð° Ð¿Ð°Ð·Ð¸ÑM-^B
Ðµ ÐºÐ°ÐºÐ²Ð¾ÑM-^BÐ¾ Ð¸ Ð´Ð° Ðµ Ð¸ Ð´Ð° Ð¼Ð¾Ð³Ð°ÑM-^B Ð´Ð° Ð²Ð¸ Ð¿ÑM-^@ÐµÐ¿ÑM-^J
Ð»Ð½ÑM-^OÑM-^B Ð½ÑM-^OÐºÐ°ÐºÐ²Ð¸ ÑM-^BÐ°Ð±Ð»Ð¸ÑM-^FÐ¸, Ð´Ð° Ð³ÐµÐ½ÐµÑM-^@Ð¸ÑM-^@
Ð°ÑM-^B Ð¿Ð¸ÑM-^AÐ°Ð½Ð¸ÑM-^O Ð² Ð±Ð°Ð·Ð°ÑM-^BÐ° Ð¸ ÑM-^B.Ð½.
-->

## 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 - HMAC($userid.$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¸?

<!--
Ð¡ÑM-^EÐµÐ¼Ð°ÑM-^BÐ° Ð¸Ð¼Ð° ÐµÐ´Ð¸Ð½ Ð¿ÑM-^@Ð¾Ð±Ð»ÐµÐ¼ - Ð½ÑM-^OÐ¼Ð° Ð¿ÑM-^@Ð¾Ñ
M-^AÑM-^B Ð½Ð°ÑM-^GÐ¸Ð½ Ð´Ð° ÑM-^AÐµ Ð¸Ð½Ð²Ð°Ð»Ð¸Ð´Ð¸ÑM-^@Ð°. ÐM-^WÐ° ÑM-^BÐ¾Ð²Ð
° Ð¸Ð¼Ð° Ð½ÑM-^OÐºÐ¾Ð»ÐºÐ¾ ÑM-^@Ð°Ð·Ð»Ð¸ÑM-^GÐ½Ð¸ workaround-Ð°:
ÐM-^XÐ¼Ð°Ð¼Ðµ timestamp, Ð¿ÑM-^@Ð¸ ÐºÐ¾Ð¹ÑM-^BÐ¾ Ð·Ð½Ð°ÐµÐ¼ ÐºÐ¾Ð³Ð° Ð¸Ð·ÑM-^BÐ¸
ÑM-^GÐ° token-Ð° Ð¸ ÐºÐ°ÑM-^BÐ¾ ÑM-^FÑM-^OÐ»Ð¾ Ð³Ð¾ Ð¿ÑM-^@Ð°Ð²Ð¸Ð¼ Ð´Ð° Ðµ Ð²Ð°
Ð»Ð¸Ð´ÐµÐ½ Ð·Ð° ÐºÑM-^@Ð°ÑM-^BÐºÐ¾.
Ð¡Ð»Ð°Ð³Ð°Ð¼Ðµ Ð² Ð½ÐµÐ³Ð¾ Ð½ÐµÑM-^IÐ¾, ÐºÐ¾ÐµÑM-^BÐ¾ Ð¿Ð¾ÑM-^BÑM-^@ÐµÐ±Ð¸ÑM-^BÐ
µÐ»ÑM-^O Ð¼Ð¾Ð¶Ðµ Ð´Ð° Ð¿ÑM-^@Ð¾Ð¼ÐµÐ½Ð¸ Ð¸ ÑM-^BÐ°ÐºÐ° Ð´Ð° Ð³Ð¾ Ð¸Ð½Ð²Ð°Ð»Ð¸Ð´
Ð¸ÑM-^@Ð° (Ð½Ð°Ð¿ÑM-^@Ð¸Ð¼ÐµÑM-^@ Ð¿Ð°ÑM-^@Ð¾Ð»Ð°ÑM-^BÐ° Ð¼ÑM-^C, ÑM-^GÑM-^@ÐµÐ·
 ÑM-^AÐ¼ÑM-^OÐ½Ð°ÑM-^BÐ° Ð¸ Ð¼Ð¾Ð¶Ðµ Ð´Ð° Ð³Ð¸ Ð½Ð°Ð¿ÑM-^@Ð°Ð²Ð¸ Ð½ÐµÐ²Ð°Ð»Ð¸Ð´Ð
½Ð¸).
ÐM-^\Ð¾Ð¶ÐµÐ¼ Ð¸ Ð´Ð° Ð¿Ð°Ð·Ð¸Ð¼ ÐºÐ¾Ð³Ð° Ð¿Ð¾ÑM-^AÐ»ÐµÐ´Ð½Ð¾ ÑM-^AÐ¼Ðµ Ð³ÐµÐ½Ðµ
ÑM-^@Ð¸ÑM-^@Ð°Ð»Ð¸ token Ð¸ Ð´Ð° Ð½Ðµ Ð¿ÑM-^@Ð¸Ð·Ð½Ð°Ð²Ð°Ð¼Ðµ Ð¿Ð¾-ÑM-^AÑM-^BÐ°Ñ
M-^@Ð¸ (Ð¸Ð»Ð¸ Ð¿Ð¾-Ð½Ð¾Ð²Ð¸) ÑM-^BÐ°ÐºÐ¸Ð²Ð°.
ÐM-^R Ð¾Ð±ÑM-^IÐ¸ Ð»Ð¸Ð½Ð¸Ð¸ Ð¿Ð¾ÑM-^AÐ»ÐµÐ´Ð½Ð¸ÑM-^BÐµ Ð´Ð²Ðµ Ð½ÐµÑM-^IÐ° Ð½Ð¸
ÐºÐ°ÑM-^@Ð°ÑM-^B Ð´Ð° Ð¿Ð¸ÑM-^BÐ°Ð¼Ðµ Ð²ÑM-^JÐ½ÑM-^HÐµÐ½ Ð¸Ð·ÑM-^BÐ¾ÑM-^GÐ½Ð¸Ðº,
 ÐºÐ¾Ð³Ð°ÑM-^BÐ¾ Ð¿ÑM-^@Ð¾Ð²ÐµÑM-^@ÑM-^OÐ²Ð°Ð¼Ðµ token-Ð°, Ð½Ð¾ Ð¿Ð°Ðº Ð¼Ð¸ Ð´Ð°
Ð²Ð°ÑM-^B Ð²ÑM-^JÐ·Ð¼Ð¾Ð¶Ð½Ð¾ÑM-^AÑM-^B Ð´Ð° Ð´ÑM-^JÑM-^@Ð¶Ð¸Ð¼ Ð¼Ð½Ð¾Ð³Ð¾ Ð¿Ð¾-
Ð¼Ð°Ð»ÐºÐ¾ state.
-->


# ÐM-^_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» - Ð¿ÑM-^@Ð¾ÑM-^AÑM-^BÐ° ÑM-^AÑM-^EÐµÐ¼Ð°, Ð² ÐºÐ¾Ñ
M-^OÑM-^BÐ¾ Ð¿Ð¸ÑM-^HÐµÐ¼ Ð² Return-path: Ð°Ð´ÑM-^@ÐµÑM-^AÑM-^JÑM-^B, Ð½Ð° ÐºÐ¾Ð
¹ÑM-^BÐ¾ ÑM-^AÐ¼Ðµ Ð¿ÑM-^@Ð°ÑM-^BÐ¸Ð»Ð¸ Ð¿Ð¸ÑM-^AÐ¼Ð¾ÑM-^BÐ¾ Ð¸ Ð¿Ð¾ Ð¾ÑM-^BÐ³Ð¾
Ð²Ð¾ÑM-^@Ð¸ÑM-^BÐµ Ð½Ð° ÑM-^BÐ¾Ð·Ð¸ Ð°Ð´ÑM-^@ÐµÑM-^A Ð·Ð½Ð°ÐµÐ¼ ÐºÐ¾Ð¹ ÑM-^BÐ¾Ñ
M-^GÐ½Ð¾ Ð½Ðµ ÑM-^AÐµ Ðµ Ð¿Ð¾Ð»ÑM-^CÑM-^GÐ¸Ð». ÐM-^ZÑM-^JÐ¼ ÑM-^BÐ¾Ð²Ð° Ð»ÐµÑ
M-^AÐ½Ð¾ ÑM-^AÐµ Ð´Ð¾Ð±Ð°Ð²ÑM-^O ÐµÐ´Ð¸Ð½ Ð¿ÑM-^@Ð¾ÑM-^AÑM-^B Ð¿Ð¾Ð´Ð¿Ð¸ÑM-^A, Ñ
M-^BÐ°ÐºÐ° ÑM-^GÐµ Ð´Ð° Ð½Ðµ ÑM-^AÐµ Ð¿Ð¾Ð»ÑM-^CÑM-^GÐ°Ð²Ð°ÑM-^B ÑM-^AÐ»ÑM-^CÑ
M-^GÐ°Ð¹Ð½Ð¸ Ð¿Ð¸ÑM-^AÐ¼Ð° Ð¿ÑM-^@Ð¸ Ð½ÑM-^OÐºÐ°ÐºÐ²Ð¾ Ð³Ð»ÑM-^CÐ¿Ð°Ð²Ð¾ Ð¸Ð·Ñ
M-^GÐµÑM-^@Ð¿Ð²Ð°Ð½Ðµ.
-->

## 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. Ð
M-^XÐ´ÐµÑM-^OÑM-^BÐ° Ðµ ÑM-^AÑM-^JÐ²ÑM-^AÐµÐ¼ Ð¿ÑM-^@Ð¾ÑM-^AÑM-^BÐ° - ISN (initi
al sequence number) Ð½Ð° ÑM-^AÐµÑM-^AÐ¸ÑM-^OÑM-^BÐ°, ÐºÐ¾Ð¹ÑM-^BÐ¾ Ð²ÑM-^@ÑM-^JÑ
M-^IÐ°Ð¼Ðµ Ð² SYN+ACK Ð¿Ð°ÐºÐµÑM-^BÐ° Ð¿ÑM-^@ÐµÐ´ÑM-^AÑM-^BÐ°Ð²Ð»ÑM-^OÐ²Ð° hash
Ð½Ð° secret Ð¸ Ð¾ÑM-^IÐµ Ð½ÑM-^OÐºÐ¾Ð»ÐºÐ¾ Ð½ÐµÑM-^IÐ°, ÑM-^BÐ°ÐºÐ° ÑM-^GÐµ ÐºÐ¾
Ð³Ð°ÑM-^BÐ¾ Ð¿Ð¾Ð»ÑM-^CÑM-^GÐ¸Ð¼ ÑM-^BÑM-^@ÐµÑM-^BÐ¸ÑM-^O Ð¿Ð°ÐºÐµÑM-^B Ð¾ÑM-^B
handshake, Ð¼Ð¾Ð¶ÐµÐ¼ Ð´Ð° ÑM-^AÐ¼Ðµ ÑM-^AÐ¸Ð³ÑM-^CÑM-^@Ð½Ð¸, ÑM-^GÐµ ÑM-^BÐ¾Ð·Ð
¸ ÐºÐ»Ð¸ÐµÐ½ÑM-^B Ðµ Ð¸ÑM-^AÐºÐ°Ð» Ð´Ð° ÑM-^AÐµ ÑM-^AÐ²ÑM-^JÑM-^@Ð¶Ðµ ÑM-^A Ð½Ð°
ÑM-^A.
(ÐM-^WÐ° Ð¿Ð¾Ð²ÐµÑM-^GÐµ Ð¿Ð¾Ð´ÑM-^@Ð¾Ð±Ð½Ð¾ÑM-^AÑM-^BÐ¸ Ð¿Ð¾ÑM-^BÑM-^JÑM-^@Ñ
M-^AÐµÑM-^BÐµ Ð·Ð° SYN flood Ð¸ Ð·Ð°ÑM-^IÐ¸ÑM-^BÐ° Ð¾ÑM-^B Ð½ÐµÐ³Ð¾).
-->
```

## client-side session

* ÐM-^RÑM-^AÐ¸ÑM-^GÐºÐ¾ Ð² ÑM-^AÐµÑM-^AÐ¸ÑM-^OÑM-^BÐ° + Ð¿Ð¾Ð´Ð¿Ð¸ÑM-^A + timestamp
* 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°
* Ð¿Ð¾Ð»Ð•Ð²Ð° ÑM-^AÐµ Ð½Ð°Ð¿ÑM-^@Ð¸Ð¼ÐµÑM-^@ Ð² rails

<!--
Ð¡ÑM-^JÑM-^IÐ¾ ÑM-^BÐ°ÐºÐ° Ð¼Ð¾Ð¶ÐµÐ¼ Ð´Ð° 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¸ - Ð¼Ð¾Ð¶ÐµÐ¼ Ð´Ð° Ð¿Ð°Ð•Ð¸Ð¼ ÑM-^AÐ°Ð¼Ð¾ Ð¿Ð¾ÑM-^AÐ»ÐµÐ´ÐµÐ½ timestamp Ð¸ Ð½Ð¸ÑM-^IÐ¾ Ð´ÑM-^@ÑM-^CÐ³Ð¾, Ð° ÑM-^AÐ°Ð¼Ð°ÑM-^BÐ° ÑM-^AÐµÑM-^AÐ¸ÑM-^O Ð´Ð° Ðµ Ð² cookie Ð¿ÑM-^@Ð¸ Ð¿Ð¾ÑM-^BÑM-^@ÐµÐ±Ð¸ÑM-^BÐµÐ»ÑM-^O Ð¸ Ð´Ð° Ð½Ðµ Ð½Ð¸ Ð¸Ð½ÑM-^BÐµÑM-^@ÐµÑM-^AÑM-^CÐ²Ð°. Ð¢Ð°ÐºÐ° Ð¼Ð¾Ð¶ÐµÐ¼ Ð´Ð° ÑM-^AÐ¼Ðµ ÑM-^AÐ¸Ð³ÑM-^CÑM-^@Ð½Ð¸, ÑM-^GÐµ Ð½Ð¸Ðµ ÑM-^AÐ¼Ðµ Ð¼ÑM-^C ÑM-^O Ð¿Ð¾Ð´Ð°Ð»Ð¸ Ð¸ ÑM-^GÐµ Ð½Ðµ ÑM-^AÑM-^JÐ´ÑM-^JÑM-^@Ð¶Ð° Ð½ÐµÑM-^IÐ¾, ÐºÐ¾ÐµÑM-^BÐ¾ Ð½Ðµ ÑM-^AÐ¼Ðµ Ð¸ÑM-^AÐºÐ°Ð»Ð¸.
-->