



(/)



## JJNAPIORK / PAGI-Middleware-Session-Store-Cookie-0.001004 / Changes

```
1 Revision history for PAGI-Middleware-Session-Store-Cookie
2
3 0.001004 2026-03-31
4   - SECURITY: Fix insecure rand() fallback in IV generation (CVE-2026-5087)
5   - Use Crypt::PRNG (from CryptX) for cryptographically secure random bytes
6   - Remove misleading Crypt::URandom reference from POD
7   - Align POD style with PAGI framework conventions
8   - Remove stale extraction note from DESCRIPTION
9   - Thanks to Robert Rothenberg and CPANSec for the report and patch
10
11 0.001003 2026-03-17
12   - Add a recognized Artistic 2.0 license section to the main module POD
13   - Add an explicit module version matching the distribution version
14   - Add an AUTHORS section to the main module POD
15
16 0.001002 2026-03-16
17   - Fix non-ASCII character in POD (em dash before =encoding)
18   - Document new() constructor method and required secret parameter
19
20 0.001001 2026-03-16
21   - Initial release
22   - AES-256-GCM encrypted client-side session storage
23   - Implements PAGI::Middleware::Session::Store interface
24   - set() returns encrypted blob as transport value
25   - get() decrypts and verifies, returns undef for tampered/invalid data
26   - No server-side storage needed
27   - Runtime warning when /dev/urandom unavailable (insecure IV fallback)
28   - Counter example app included
```