Subject: Secure random and nonce generator with SecureBuffer support
Posted by Oblivion on Sun, 26 Apr 2026 10:27:09 GMT
View Forum Message <> Reply to Message

Hi,

Secure random and nonce generator with SecureBuffer support is added to Core/SSL package. This addition introduces thread-safe nonce generation functions to the Core/SSL package, providing guaranteed uniqueness and fork-safety for cryptographic operations.

Public API:

```
/ Core functions
SecureBuffer<byte> SecureRandom(int n);  // Pure CSPRNG output
SecureBuffer<byte> SecureNonce(int n);   // Structured nonce (min 12 bytes)

// Protocol-specific helpers
SecureBuffer<byte> GetAESGCMNonce();          // 12 bytes,
AES-GCM/ChaCha20-Poly1305
SecureBuffer<byte> GetChaChaPoly1305Nonce();   // 12 bytes, alias for AES-GCM
SecureBuffer<byte> GetTLSNonce();             // 12 bytes, TLS 1.2/1.3
SecureBuffer<byte> GetAESCCMNonce();          // 13 bytes, AES-CCM
SecureBuffer<byte> GetJWTNonce();             // 16 bytes, JWT tokens
SecureBuffer<byte> GetOAuthNonce();           // 16 bytes, OAuth flows
SecureBuffer<byte> GetOCSPNonce();            // 20 bytes, OCSP requests
SecureBuffer<byte> GetECDSANonce();           // 32 bytes, ECDSA signatures
SecureBuffer<byte> GetDTLSCookie();           // 32 bytes, DTLS cookies
```

Best regards,
Oblivion