🔐 11. ZoneInfo

🔑 Overview  
ZoneInfo is an optional enhancement in Mango that enables logical partitioning of cryptographic sessions — or, more broadly, a second cryptographic factor.  
It silently strengthens the cryptographic context without modifying the encryption/decryption workflows or adding metadata to the output.

When specified, ZoneInfo participates fully in Mango’s key derivation process. When enabled, it is RFC-hardened alongside the password using PBKDF2, with iterations split between them. This ensures the full entropy of both values is cryptographically honored.

📜 How ZoneInfo Works  
• ✅ Password and ZoneInfo are *independently* derived via PBKDF2 (if enabled), each using half of the configured iterations.  
• 🌀 The resulting 256-bit components are combined before feeding the coin table shuffle logic.  
• 🚫 ZoneInfo is never stored, transmitted, or embedded in encrypted output.  
• 🧠 Different ZoneInfo values yield entirely different encryption behavior — even with the same password.  
• 🔄 If ZoneInfo is null or empty, Mango reverts to standard password-only behavior.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **Factor** | **Without ZoneInfo** | **With ZoneInfo** | | Password-only security | ✅ Standard | ✅ Augmented with secondary entropy | | Cryptographic isolation by context | ❌ No | ✅ Yes | | Metadata exposure | ✅ None | ✅ None | | Complexity for attacker | Lower | Higher (must guess both components) | |  |  |

ZoneInfo increases entropy and adds resilience against brute-force or domain-collision attacks without introducing any structural metadata.

💡 Usage Example

public static readonly byte[] Salt = [0x1A, 0x2B, 0x3C, 0x4D, 0x5E, 0x6F, 0x70, 0x81, 0x92, 0xA3, 0xB4, 0xC5];

var options = new CryptoLibOptions(

salt: Salt,

zoneInfo: "XYZ Corp. Marketing"

);

var crypto = new CryptoLib("my password", options);

byte[] encrypted = crypto.Encrypt(sequence, rounds, input);

byte[] decrypted = crypto.Decrypt(encrypted);

If you omit ZoneInfo, Mango defaults to password-only mode:

var options = new CryptoLibOptions(

salt: Salt,

);

var crypto = new CryptoLib("my password", Salt);

🛡️ Security Guarantees  
• No Metadata Leak: ZoneInfo is invisible in ciphertext and headers.  
• Session Isolation: Different ZoneInfo values yield distinct encryption outcomes.  
• Zero Friction: No changes to headers, payload format, or decryption logic.  
• Full Entropy Utilization: When enabled, both password and ZoneInfo get PBKDF2-hardening with equal iteration budgets.

👉 Best Practices  
• Treat ZoneInfo like a true secondary password — keep it confidential.  
• Use meaningful labels like "Corp-AppA" or "Device-AuthN-Token".  
• Ensure all encryption and decryption parties use the same ZoneInfo.  
• Avoid reusing public or predictable identifiers (e.g., usernames).

🌟 Final Note  
ZoneInfo is Mango’s low-friction second factor — opt-in, entropy-rich, and invisible to outsiders. It aligns perfectly with Mango's guiding principles:

Stealthy, adaptive, and resilient — without friction.