Here’s an example of how you might structure a security assurance case for Instant Messaging (IM) software using Goal Structuring Notation (GSN) in a simple textual tree format:

```

- [G1] Goal: Ensure the overall security of the IM software

- [Sn1] Strategy: Address security by following a multi-layered approach

- [G2] Goal: Ensure encryption of messages

- [Sn2] Strategy: Implement end-to-end encryption

- [G3] Goal: Use state-of-the-art encryption algorithms

- [S1] Solution: Implement AES with 256-bit keys for message encryption

- [G4] Goal: Ensure the keys are securely generated and stored

- [S1] Solution: Use a secure key generation protocol (e.g., Diffie-Hellman)

- [S2] Solution: Store keys in a secure key vault

- [G5] Goal: Authenticate users securely

- [Sn3] Strategy: Use multi-factor authentication

- [S1] Solution: Implement a two-factor authentication system

- [S2] Solution: Require biometric verification for accessing sensitive actions

- [G6] Goal: Protect data at rest

- [Sn4] Strategy: Use strong data storage encryption and access controls

- [S1] Solution: Encrypt local caches with device-specific keys

- [S2] Solution: Use file access permissions to limit data access

- [Sn5] Strategy: Comply with international security standards and regulations

- [G7] Goal: Meet GDPR requirements for data protection and privacy

- [S1] Solution: Implement data handling protocols that ensure data minimization and purpose limitation

- [G8] Goal: Achieve ISO/IEC 27001 certification

- [S1] Solution: Establish, implement, maintain and continually improve an information security management system (ISMS)

- [C1] Context: The IM software is used globally across different devices and platforms

- [C2] Context: Users range from individual consumers to large enterprises

- [A1] Assumption: Users have access to secure internet connections

- [A2] Assumption: Regulatory requirements are stable over the next five years

- [J1] Justification: Adoption of AES-256 is based on its widespread acceptance and recommendation by security experts

- [J2] Justification: Multi-factor authentication significantly reduces the risk of unauthorized access

```

Each node in the tree is tagged as a Goal (G), Strategy (Sn), Solution (S), Context (C), Assumption (A), or Justification (J). This format helps in logically arranging evidence and arguments to support the security assurance objectives for the IM software.