Based on the given security case pattern and using the domain information provided for Instant Messaging (IM) software, we can instantiate the security case pattern to specifically address the IM software's security considerations. Below is the security case structured in a hierarchical tree format using dashes (-) to denote different levels and placeholders are instantiated based on the domain information.

```

- Goal (G1, "IM software is acceptably secure in operational environment")

- Context (C1, "Definition and description of IM software")

- Context (C2, "Definition and description of operational environment")

- Context (C3, "Definition of 'acceptably secure' in terms of security measures")

- SupportedBy

- Strategy (S1, "Argument that IM software assets are under protection")

- Justification (J1, "Protection of software assets supports that IM software is acceptably secure")

- SupportedBy

- Goal (G2, "All identified IM software critical assets are protected")

- Context (C4, "List of IM software critical assets: Registration information, Registration process, User account information, Authentication information, Login process, Chat logs")

- Justification (J2, "Relationship between assets is clear and can be argued separately")

- SupportedBy

- Strategy (S2, "Respective arguments of IM software critical assets")

- SupportedBy

- Goal (G3, "Each IM software critical asset is protected")

- HasMultiplicity (S2, G3, number of software critical asset = 4)

- SupportedBy

- Strategy (S3, "Argument of the type to which the IM software critical asset belongs")

- Context (C5, "List of software critical asset types in PEDD: Process, Data Exchange, Environment Entity, Data Storage")

- Justification (J3, "Types of software assets are according to PEDD")

- SupportedBy

- Goal (G4, "IM software critical asset which belongs to each type in PEDD is protected")

```

### Explanation:

1. \*\*Goal G1\*\* establishes the highest-level security goal for the IM software, with its contexts defining the software, operational environment, and the notion of security required.

2. \*\*Strategy S1\*\* supports this goal by arguing that the assets of the IM software are protected, backed by \*\*Justification J1\*\* explaining why asset protection is crucial.

3. \*\*Goal G2\*\* further decomposes the goal of asset protection, supported by \*\*Strategy S2\*\*, which addresses the protection of individual critical assets of the IM software, as listed in \*\*Context C4\*\*.

4. \*\*Goal G3\*\* pertains to the protection of each critical asset, routed through \*\*Strategy S3\*\* focusing on different types of assets based on the PEDD classification.

5. Finally, \*\*Goal G4\*\* ensures specific protection measures for each type of critical asset as classified in PEDD, explained and justified under their respective context and justification. Each type relates to a portion of the software's internal and external organization detailed in the domain information.