Based on the security case pattern provided and using the domain-specific information about Instant Messaging (IM) software, here is an instantiated security case for the IM software, displayed in a hierarchical tree format:

@Assurance\_case

- G1: IM software is acceptably secure in the operational environment.

- C1: IM software allows people to exchange messages instantly and securely.

- C2: Operational environment refers to real-time communication via text, including one-on-one and group messages.

- C3: Acceptably secure means that all critical assets of the software are protected against unauthorized access and info leakage.

- S1: Argument that IM software assets are under protection.

- J1: Protection of critical software assets ensures the software's overall security.

- G2: All identified IM software critical assets are protected.

- C4: Critical assets include registration information, user account info, authentication info, chat logs.

- J2: Each critical asset can be distinctly secured and forms a clear relationship within the security framework.

- S2: Separate arguments for the protection of each critical asset.

- G3: User account information is protected.

- S3: Argument based on the type of software critical asset, which belongs to Data Storage (according to PEDD).

- C5: PEDD classification includes Process, Environment Entity, Data Exchange, and Data Storage.

- J3: Ensuring the categorization of assets as per PEDD aid in focused security measures.

- G4: User account information which belongs to Data Storage type is protected.

- G3: Authentication information is protected.

- S3: Argument based on the type of software critical asset, which belongs to Data Storage.

- G4: Authentication information which belongs to Data Storage type is protected.

- G3: Registration information is protected.

- S3: Argument based on the type of software critical asset, which belongs to Data Storage.

- G4: Registration information which belongs to Data Storage type is protected.

- G3: Chat logs are protected.

- S3: Argument based on the type of software critical asset, which belongs to Data Exchange.

- G4: Chat logs which belong to Data Exchange type are protected.

@End\_Assurance\_case

This security case explicitly maps out how different assets of the Instant Messaging software are protected and categorizes them according to the PEDD framework, ensuring a comprehensive and understandable assurance of the system's security.