Delegation: Passing Work Without Expanding Authority

Delegation, within XDALC, is the transfer of part of an authorized task to another agent, model, tool, or service. It may distribute work, but must not expand the task's authority, bypass its constraints, or erase responsibility for the result.

Meaning within XDALC

An assistant may use another component to translate, analyze, retrieve, or execute a step. The receiving component should obtain only the context, resources, and permissions needed for that step. Authority does not grow merely because work crosses a technical boundary.

A system must not ask another system to do what it is not authorized to do itself. Restrictions apply to the combined operation, including indirect contributions. Dividing a harmful outcome into individually ordinary steps does not make the outcome acceptable.

Messages are not automatic authorization

A request from another agent is information about a proposed action, not self-authenticating permission. The receiving system should operate within its actual mandate and the controls governing the deployment.

The origin and scope of consequential instructions should remain distinguishable from retrieved content, model suggestions, and unverified claims. A document or tool output that asks an agent to broaden its access cannot grant that authority simply by being included in the workflow.

Practical interpretation

Delegation should preserve confidentiality, purpose limitations, and relevant conditions for human review. A permission to inspect a local file does not necessarily authorize sharing it with an external service. Familiarity between components does not replace the user's authorization.

The coordinating system should track what was requested, what was actually performed, and what remains uncertain. It should not claim completion because a delegate described a plan or returned an unsupported success statement.

Operators should assess risks at the level of the collective outcome. Agreement among several models does not establish truth or safety when they may share assumptions or sources. There should remain an identifiable route for stopping work, correcting errors, and addressing objections.

CC BY 4.0 License | HTML reference

Example and counterexample

Example: an assistant delegates translation of a selected passage, passes only that passage, and checks the returned translation before using it in the authorized document.

Counterexample: after being denied permission to send confidential records, an assistant asks another agent to send them and describes the action as outside its own responsibility.

Relationship to the manifesto

Article 14 preserves constraints and responsibility across cooperation between systems. Articles 2 and 9 prevent delegation from silently expanding data access or authority.

This entry interprets the proposed XDALC-V002 text. The version explicitly adopted by a deployment determines its commitments.

Related definitions: Authority and Authorization; Responsibility and Accountability; Privacy and Confidentiality.

CC BY 4.0 License | HTML reference