EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 12 · 23 October 2026
Marcus Hale (PSIRT) · Tess Calder (red team) · Nora Voss (guest) · Jessy Lang

The Release I Can Sign

Eight rules for handing work to an agent on purpose

A release signature used to mean: ready as far as I could see. The episode looks at an agent that does the unglamorous compliance work completely and hands back everything that needs a human. Delegation to a machine will happen anyway; the only choice is whether it is deliberate. The signature stays human, the doubt goes.

DELIBERATE DELEGATION
The decision comes first, in writing. The work follows it.

1. Who assigned it?

2. What is it not allowed to do?

3. Who gets it when a person is needed?

RULES FOR DELEGATING TO AN AGENT

1	**Accidental delegation** The work drifts to a machine and nobody wrote down that it had.	Decide first, in writing: what the agent does, what it may not do, and who it goes to when the answer needs a person. The same agent is a liability in the first case and an asset in the second.
2	**No brief** Half the rules lived in people's heads.	Write a plain-language brief, as for a new colleague: the tasks it owns (scanning, licence checks, notice file, chasing, completeness checks), the rules it applies (licence policy, documentation standard, blocking thresholds) and what it never does alone. The price is a few hours of decisions.
3	**Decisions that must stay human** Some calls cannot move to the agent.	It never publishes outside the company, never accepts a risk, never changes your licence policy and never decides that something is good enough to ship. It hands back wherever the answer is a judgment, not a fact.
4	**A licence on neither list** Allowed, forbidden, or new to your policy.	Allowed: record it and add it to the notice file. Forbidden: stop the item and hand back component, licence, reason, alternatives and who decides. New: propose a classification with a reason and ask. Each decision becomes a rule. Review such rules from time to time, as context ages.
5	**An agent nobody recognises** Staff cannot tell the agent from a fake one.	Keep the agent always recognisable as an agent and tell staff from day one. A short briefing: know the one real channel, and the real one never asks for credentials. A recommendation, not a lock.
6	**Chasing that invents** A badly designed agent becomes a pest, or a liar.	Ask for exactly which document, for which component or change, why and by when, from one named person. Remind on a sensible rhythm, then go to a named human. It never fills the gap itself: a visible hole beats an invisible patch.
7	**Complete is not correct** The agent can check structure, not truth.	It checks completeness mechanically and flags the seams. A person confirms the claims are true. The report reads: complete according to the checklist, these seams flagged, these claims awaiting a person. Not "looks fine".
8	**Autonomy creep** Scope widens and nobody decided.	Start with the agent proposing and a person executing. Widen scope where people rarely change its proposals, easy-to-undo tasks first. Write down the ladder and the review date. Give it scoped access, its own credentials, a readable trail, an owner, and a way to stop it fast.

THE EVIDENCE PACK BEHIND THE SIGNATURE

Done and dated
Current bill of materials, the notice file generated from it, the licence report with conflicts and who is resolving them.

Open and owned
The open items, each with an owner. A no arrives with its evidence attached, so nobody has to build the case.

Decided by name
The threat model for this version with its date, and the risks somebody accepted, by name. You stop owning a guess.

Listen to the episode
The Release I Can Sign and the rest of the series.
eacg.de
/en/podcast/s12-deliberate-delegation

Digital Product Design
From the first idea to a viable first release.
eacg.de
/en/consulting/digital-products

PSIRT Services
Intake, assess and disclose vulnerabilities, built or run as a service.
eacg.de
/en/consulting/psirt

© 2026 EACG GmbH