REVYCORE

WHITE PAPER

Your IGA Grants.

Who certifies?

Identity governance suites manage the lifecycle of identities and entitlements. Certification is a different discipline. This paper explains how the two fit together.

KNOWLEDGE CENTER

DECEMBER 2026

EXECUTIVE SUMMARY

Granting and certifying are two jobs.

One tool rarely does both well.

Identity governance and administration suites are built to grant: they manage joiners, movers and leavers, roles, requests and provisioning. Their access certification modules were added to that core, and they certify what the suite itself manages.

Certification asks different questions. Not only who has access, but whether the resource should exist, who answers for it, whether a decision was taken by a person with authority, and whether that decision can be proven years later. It also has to reach systems the suite does not govern.

This paper sets out the difference, describes how a dedicated certification layer complements an IGA suite, and shows how organisations without a suite can certify from the systems directly.

Different jobs
The suite grants and provisions; certification decides and proves.

Beyond the catalogue
Resources, scopes and agents the suite does not model.

No suite needed
Collection from connected solutions, nothing provisioned.

Complementary
With a suite, each does what it was built for.

CONTENTS

01 Granting is not certifying
02 Where suites stop
03 Two layers, two jobs
04 Observing, not provisioning
05 Without a suite
06 Questions to ask your stack
07 Where to start

CHAPTER 01

Granting is not certifying

The tool that grants should not be the only one that certifies.

An IGA suite answers the question: what should this person have, and how do we give it to them? Its strength is the lifecycle: onboarding, role changes, departures, request workflows and provisioning into target systems.

Certification answers a different question: is what exists today still legitimate, who decided so, and can it be proven? It looks backwards at the actual state, not forwards at the intended one.

When the same system both grants and certifies, it certifies its own model of the world. What it does not manage, it does not see, and what it sees is what it has been told.

> **Certification** DEFINITION
> an explicit, attributed and dated decision that an access, a resource or a system is still legitimate, recorded as verifiable evidence.

CHAPTER 02

Where suites stop

Certification has to reach what the suite does not model.

IGA certification modules are strongest on the entitlements the suite itself provisions. Several areas typically fall outside that perimeter.

- **The resource itself.** Ownership, inactivity, lifecycle, privacy and sharing of the resource, not only its members.
- **Collaboration and sharing.** Document spaces, channels and external sharing that are created outside any request workflow.
- **Systems as a whole.** Business applications spanning several platforms, certified as one named scope.
- **AI agents.** Non-human identities with tools, knowledge sources and audiences.
- **Evidence that stands alone.** Records sealed and verifiable offline, without the tool that produced them.

CHAPTER 03

Two layers, two jobs

The suite manages the lifecycle. Certification decides and proves.

In organisations that already run an IGA suite, a dedicated certification layer does not replace it. Each does what it was built for.

CONCERN	IGA SUITE / CERTIFICATION LAYER
Lifecycle	The suite manages joiners, movers and leavers. Certification reviews the state that results.
Requests	The suite runs access requests and approvals. Certification asks whether access is still justified later.
Provisioning	The suite provisions into target systems. Certification provisions nothing; it observes.
Scope	The suite covers what it models. Certification collects from the connected solutions, including those the suite does not govern.
Evidence	The suite logs its workflows. Certification signs and seals decisions for independent verification.

CHAPTER 04

Observing, not provisioning

What is observed is what exists, not what was intended.

A certification layer that relies on collection from the connected solutions sees the actual state of each system, including rights granted outside any workflow, sharing opened by users, and resources nobody registered.

Because it provisions nothing, it does not compete with the suite or with the systems' own administration. It observes, asks the right owner to decide, and tracks each refusal until a later observation confirms that the change was made.

Each connection uses its own identity, read-only, with documented entitlements. The least-privilege principle applies to the certification layer itself.

CHAPTER 05

Without a suite

No IGA project is needed to start certifying.

Many organisations have no IGA suite, or one that covers only part of the estate. They still face DORA, NIS2, ISO 27001 or SOC 2 requirements for access reviews.

For them, certification can start directly from the systems: connect the solutions that matter, designate owners, run campaigns, seal the evidence. No identity lifecycle project has to come first, and nothing is provisioned.

If a suite arrives later, the two layers fit together without rework: the suite takes over the lifecycle, certification keeps deciding and proving.

Connect
The solutions that hold critical data, read-only.

Designate
Owners and reviewers by rule.

Certify
Access, resources, scopes and agents.

Prove
Sealed evidence, verifiable without the vendor.

CHAPTER 06

Questions to ask your stack

The answer to the fourth question is where certification lives.

Whatever tools are in place, four questions reveal whether certification is really covered.

What can it see?
Only what the suite provisions, or the actual state of each system?

Who decides?
The owner of the asset, or the team that administers the tool?

What is certified?
Only memberships, or also resources, systems and agents?

Can it be proven?
Years later, by an auditor, without the tool that produced it?

CHAPTER 07

Where to start

Start with the gap between what the suite manages and what exists.

Whether or not a suite is in place, the first step is to see where certification currently stops.

01 **Map what your suite manages,** and what it does not.

02 **Connect the systems outside its perimeter,** starting with those holding critical data.

03 **Certify resources as well as access,** with named owners.

04 **Seal every decision** so that it can be verified independently.

05 **Let each layer do its job:** the suite grants, certification decides and proves.

REVYCORE

Your tools grant and authenticate.
REVYCORE certifies and proves.

Human decisions. Verifiable evidence.

Request a demonstration in your context: your solutions, your scopes, your agents.

revycore.com

This paper describes general characteristics of identity governance tools and the corresponding capabilities of REVYCORE for information purposes; it does not assess any specific product. © 2026 REVYCORE SAS.