 @2026 Hopae S.A. All rights reserved.

Hopae Global Assurance Framework

Introduction

An eID is only useful if you can trust it to prove who someone really is. A weak one is a business risk: if an identity can be faked or an account taken over, the cost of fraud lands on you. Yet trust is hard to compare across borders. Europe grades its eIDs under eIDAS, the United States uses NIST, and most schemes worldwide carry no rating at all.

The Hopae Global Assurance Framework gives every eID on our network one comparable score: the **Hopae Level of Assurance (HLoA), from 1 to 4**. It is built on the NIST and eIDAS standards and calibrated so that **HLoA 4 equals eIDAS High**. It scores both **how carefully a person was checked** and **how securely they log in**, because an eID can be strong on one and weak on the other, and the weak side is where fraud gets in. Seeing both lets you choose the right eID for each use case and know exactly what you're relying on.

The four levels

HOPAE LOA	EIDAS EQUIVALENT	MEANING
1	**none**	No reliable link to a real identity. Low identity proofing or low authentication method.
2	**Low**	A real person, but light checks or a single-factor login leave room for fraud.
3	**Substantial**	Verified identity with multi-factor login. The dependable everyday tier.
4	**High**	Government-grade proofing with a hardware-anchored login. Equal to eIDAS High.

How the score works

We score every eID on two independent questions, each on its own scale.

Identity proofing (P): how carefully was the person checked?

P0	**Self-asserted**	No independent check. We only know what the user typed.	*Social logins; self-registered accounts*
P1	**Basic**	Details matched against a credible source, such as a telecom, bank or credit record, but no document check.	*Telco data match; bank account check*
P2	**Verified**	A government ID checked for authenticity and the person actively matched to it.	*Document scan + selfie; bank-derived eIDs*
P3	**High**	Anchored in a chip or government register, with a biometric or attended check.	*NFC passport + face match; register-backed eIDs*
P4	**Very high**	In-person or supervised enrolment, with biometrics held by the authority.	*National ID cards issued at a counter*

Authentication (A): how securely do they sign in?

A0	**None**	No reusable login is issued. The identity check is one-time.	*One-time document + selfie checks*

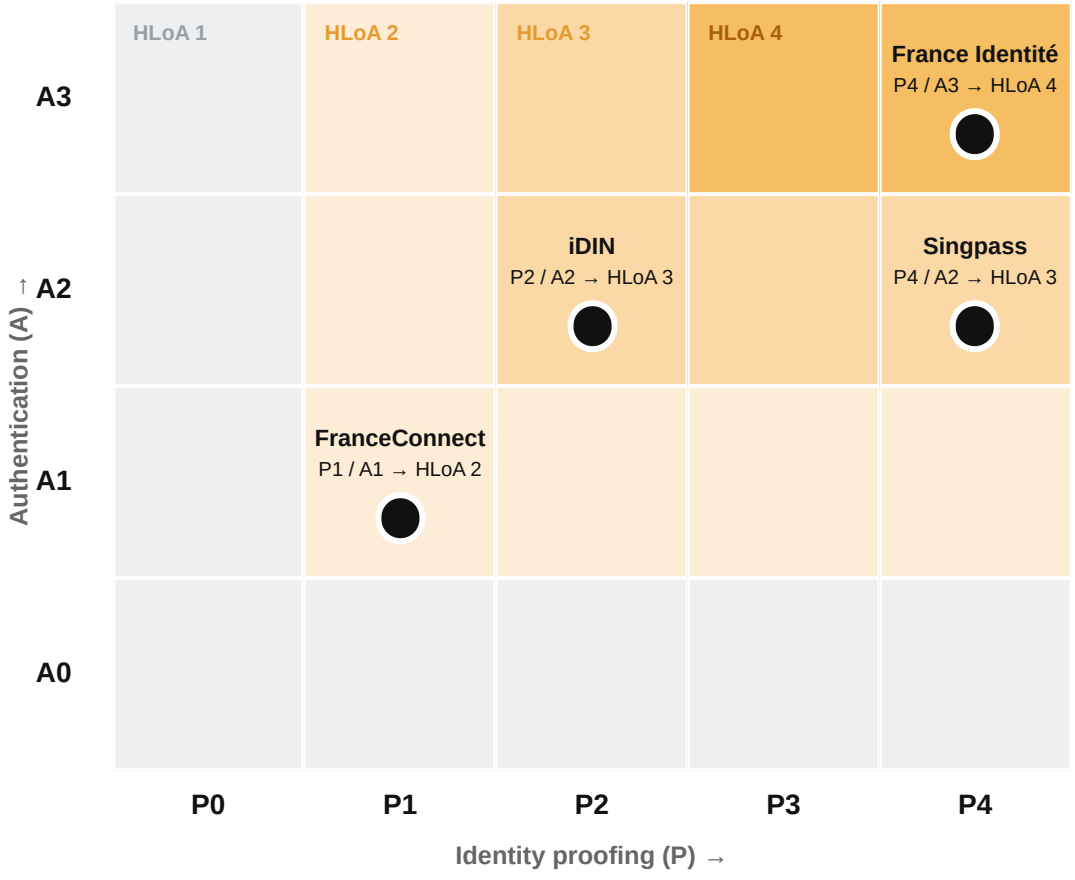
 @2026 Hopae S.A. All rights reserved.

A1	**Single factor**	One thing proves it's you: a password or SMS code. Phishable.	*Password login; SMS OTP*
A2	**Dynamic MFA**	Two independent factors, fresh each session: a device unlocked by PIN or biometric.	*eID apps; bank MFA*
A3	**Hardware-anchored MFA**	Keys locked in tamper-resistant hardware, so they can't be extracted or copied. Resists determined attackers.	*Smartcard eIDs; HSM-based eIDs such as MitID*

The two combine into one HLoA, and the weaker of the two decides it. Like a chain, an identity is only as strong as its weakest link. A government-verified person behind a single SMS code, or a hardware key on an unverified account, both leave an opening, so neither scores high. The top level needs a **thoroughly checked person** and a **login only they can perform**.

In practice

We carefully assess each eID against both vectors, and its scores on the two decide its level. This map shows where each eID lands and how it compares to the others.



What it means for you

Choosing an eID is a question of confidence. Can this identity be trusted to open an account, approve a payment, or sign a contract? Without a common scale, that judgement rests on reputation and guesswork. The HLoA replaces guesswork with a clear, comparable measure of how strongly each eID proves identity. You can see at a glance which eIDs meet the assurance a use case requires, match the level to the risk of each transaction, and rely on a score that traces to published NIST and eIDAS criteria. The result is **security and assurance in every eID you use**, and the confidence to make the right choice for your business.