itsme

The Identity Maturity Index 2026

The competitive advantage of reusable identity

Measuring digital identity maturity across banking, insurance, telecom and energy in Belgium and the Netherlands.

Based on the NIQ Growth Spaces study (April 2026) and the HPB study on Dutch consumer attitudes (March 2026).

Contents

Foreword 3

Part 1. How to read this report 6

Part 2. The Identity Maturity Model 10

Part 3. The market today 15

- Banking 16
- Insurance 18
- Telecom 19
- Energy 21

Part 4. What consumers want 23

Part 5. Why fragmentation persists 27

Part 6. Moving up the maturity curve 30

Part 7. Methodology 35

Foreword: Identity is infrastructure now

Whether you run a bank, an insurer, a telecom or an energy company, your business depends on knowing who your customer is. Every account opened, every contract signed, every login processed is an identity transaction. How well you handle those transactions now shapes who becomes a customer, who stays, and who trusts you with more. For most of the past decade, identity sat in the background. It was a security checkpoint, a compliance obligation, a login screen owned by whichever team happened to need it that quarter. Product, security, compliance and customer experience each held a piece, and each judged its piece by its own standard. None of them measured the actual customer experience, from the first onboarding step to the tenth login to the contract they signed three years later. That blind spot matters more than it used to, because identity has moved from a back-office function to the layer the whole customer relationship runs on.

There are two ways to judge how well an organisation handles identity, and they lead to very different conclusions.

- The first looks at the technology. How strong is the authentication method. Does it resist phishing. Which certifications does it carry, which standards does it support, how granular is its risk engine, how broad is the vendor's global footprint. This is a fair and useful view, and the market has built good instruments for it. If you are choosing a single authentication product to add to your own app, these are exactly the right questions.

- The second view looks at how identity behaves across the entire customer relationship. Whether the same proof of who someone is can travel from onboarding to login to signing. Whether it holds when the customer moves from your app to your website, from your bank to your sister insurer, from one of your products to the next. Whether the customer proves who they are once, or over and over again.

The first view measures a component. The second measures infrastructure. Most of the market still works at the component level, and so do the rankings built to assess it. Analyst scorecards and Magic Quadrants line identity vendors up as components and answer which product is strongest on a given technical axis. That question doesn't tell you whether identity holds together once it has to work across the whole customer relationship. The gap is structural, not a shortcoming of any single ranking. A scorecard reaches a verdict on the part and presents it as a verdict on the whole.

The data in this report shows why that does not hold up. **You can assemble the strongest components available today and still leave the customer re-proving who they are at every step.** A bank can run a top-rated authentication method on one login screen, fall back to username and password everywhere else, re-onboard customers who move to a sister product, and sign loans by email and PDF. On a component scorecard, it looks advanced. In the customer's experience, and on the maturity curve in this report, it sits at Standard.

Strong identity components do not add up to working infrastructure on their own.

The report calls the top of that curve Stellar. What defines that stage is **identity as infrastructure**. It is the stage where verifying who someone is happens once and holds across organisations, sectors and journey steps. Reaching it has little to do with buying a better component. It takes integration depth, an acceptance network that makes a single proof useful at the moments customers actually need it, and a regulatory framework that lets that proof travel. None of those are features a vendor can ship on its own. They are properties of a system, which is precisely why a component scorecard cannot see them.

This is not a thought experiment. Across the eight sector-country pairs measured in this report, the one that comes closest to the top of the curve is Belgian banking, where a shared identity layer is integrated deeply across onboarding, login and signing, and where an acceptance network has pulled telecom, energy and insurance in behind it. itsme is that layer. It is the clearest working example we have of identity behaving as infrastructure rather than as one more component bolted onto each app.

The timing of this report is not incidental. The **European Digital Identity Wallet** arrives at the end of 2026 and gives every regulated organisation in Europe access to a reusable, high-assurance identity method. However, it does not build the integration depth, the acceptance network or the orchestration that decide whether identity works across a customer's journey. As the baseline becomes universal, the way you build on top of it becomes what sets your organisation apart.

The Identity Maturity Index reads your organisation on that second axis, the one the component view leaves out. It places banking, insurance, telecom and energy providers in Belgium and the Netherlands on a five-stage curve, sector by sector and country by country. It is built on a 4,095- respondent consumer study by NIQ and on a model of how reusable identity matures inside a service.

Find your sector. Read your placement. Use it to defend the investment, set the target, or change the conversation.

Two findings to set the tone before you start:

01

In three out of four sectors analysed, consumers expect more than what providers deliver.

NIQ Growth Spaces, April 2026.

02

64% of Dutch consumers say having to make a video selfie during onboarding stops them from becoming a customer.

NIQ Growth Spaces, April 2026.

What follows

- Chapter 1 explains how to read the Index: what we measured, what the maturity and importance scores mean, and how we define identity fragmentation.
- Chapter 2 introduces the five-stage Identity Maturity Model.
- Chapter 3 places each of the eight sector-country pairs on the curve, with the supporting NIQ data.
- Chapter 4 sets out what consumers actually want from identity, and where that diverges from what they are offered.
- Chapter 5 examines why fragmentation persists as organisations mature, and what to do about it.
- Chapter 6 looks at what moves organisations up the curve: consumer expectation, regulation, fraud, and the arrival of reusable identity infrastructure.
- Chapter 7 documents the methodology.

We hope it gives you a clearer view of where you stand, and where to go next.

Reyndert Coppelmans
CMO

1. How to read this report

This section explains what data we collected, what the two main metrics (Maturity and Importance) mean, and how we define identity fragmentation. For the full methodology, refer to chapter 7.

What we measured

In April 2026, itsme (Belgian Mobile ID) commissioned NIQ (Nielsen Consumer LLC) to run a **4,095-respondent study** across Belgium and the Netherlands. The study covers four regulated industries that depend on knowing who their customer is: **banking, insurance, telecom and energy.**

For each of the **five identity use cases** (identity verification, online authentication, transaction confirmation, contract signing, sharing customer data), respondents told us two things: which method their current provider uses, and what they would expect or accept as a customer. The first answer becomes the maturity score. The second becomes the importance score.

Figure 1.1. Sample sizes per sector and country

Sector	Belgium(n)	Netherlands (n)
Banking	514	511
Insurance	503	515
Telecom	519	513
Energy	512	508
Total per country	2,048	2,047
Total study	4,095 respondents BENE	

NIQ Growth Spaces, April 2026. Total n=4,095 across Belgium and the Netherlands.

Where consumer attitudes inform the analysis (privacy concern, trust in providers, willingness to share data), the report also draws on a consumer survey on digital identity attitudes conducted by HPB in March 2026.

The two scores: Maturity and Importance

Every chart in chapter 3 plots two numbers per touchpoint: Maturity (blue) and Importance (grey). Both are on a 0 to 100 scale.

Maturity

Maturity is **what the provider actually deploys,** scored on the **strength and reusability** of the identification method.

Maturity scores capability, not adoption. The Index measures what providers offer at each touchpoint, scored on the strength and reusability of the method. It does not measure how often customers actually choose that method when alternatives are available. The gap between the two becomes visible at touchpoints where strong identity is offered alongside username and password.

NIQ rates each method on a fixed scale:

- 20: Username and password, knowledge-based checks.
- 40: Knowledge plus weak possession (SMS OTP, email link).
- 60: Device-bound app authentication with biometrics or PIN, inside one organisation's app.
- 80: Out-of-band confirmation via a proprietary or sector-specific identity app (DigiD, iDIN).
- 100: Reusable ecosystem identity (itsme, EUDIW) for verification or qualified electronic signature.

The **touchpoint maturity score** is the share-weighted average across the methods customers actually encounter at that touchpoint. The **sector maturity score** is the average across all touchpoints for that sector.

Importance

Importance is what the customer expects, calculated from three measures: how much they value the touchpoint being **available online** (weight 0.5), how **safe** they expect it to be (weight 0.25) and how **easy** they expect it to be (weight 0.25). The composite tells you what "good enough" looks like to the customer at that touchpoint.

Two kinds of maturity: method and organisation

A score of 100 on the NIQ scale tells you the identification method used at a touchpoint is at the top of what's available today. That doesn't mean, however, that the organisation deploying it is in itself at the top of the Identity Maturity Model.

The NIQ score measures the maturity of the method. A traditional username and password solutions scores 20. Reusable identity solutions like DigiD and itsme score 80 and 100, respectively. These are properties of the technology in use at a given touchpoint.

The IMM stage measures the maturity of the organisation. A bank that uses itsme at one login screen but falls back to username and password elsewhere, that re-onboards customers when they move to a sister product, that signs contracts by email and PDF, has a strong method deployed in a fragmented stack. That bank scores well on individual touchpoints but still sits at Standard on the IMM.

The two scales can agree or disagree. A high NIQ score with a low IMM stage tells you **the right tools are in place but the journey isn't built around them.** A high NIQ score and a high IMM stage tells you **the method and the integration are aligned.** Belgian banking is the only sector-country pair in the Index where the two meet at the top.

The opportunity gap

Maturity minus Importance is the **opportunity gap.** A positive gap means the provider delivers above customer expectation. A negative gap means the customer expects more than is being deployed. The bigger the gap, the higher the unmet demand.

What we mean by 'identity fragmentation'

Throughout the report, identity fragmentation refers to the customer **experiencing identity as a series of disconnected, repeated proofs across channels, providers and use cases,** instead of as a single reusable layer.

Concretely, fragmentation shows up as: separate passwords per service; uploading a copy of the ID card to one provider, then another; logging in differently on the app and on the web; re-onboarding when switching providers; and verifying identity again every time a touchpoint moves between organisations.

Fragmentation is structural and can be measured: maturity scores quantify the deployed methods at each touchpoint, and the variance across touchpoints inside a single provider shows how fragmented their stack is.

> **87% of Dutch consumers want fewer separate accounts and login methods. 90% would feel safer with one trusted way to identify online.**
>
> *HPB, March 2026*

The cost of friction

The Index does not quantify the **enterprise cost of identity fragmentation.** The NIQ study measured consumer perception and current solution maturity. Three publicly available sources give directional estimates.

- Signicat Battle to Onboard. 7,600 consumers across 14 European markets. The 2023 edition reports 68% of consumers abandoned at least one digital application in the past year, with identity verification cited among the most common reasons.
- Fenergo (2025) estimates losses for financial institutions from onboarding friction in the hundreds of millions of euros annually per major institution. Fenergo is a vendor in KYC; the figure is a stated estimate.
- OneSpan with Sapio Research reports identity friction as a leading cause of customer abandonment in onboarding.

The directional pattern is consistent: identity friction is among the largest stated drivers of onboarding abandonment in regulated sectors. Customer-acquisition costs in BENE telecom and financial services run roughly 280 to 315 euros per acquired customer. The Index does not multiply these into a single enterprise cost; the precision required isn't available.

The consumer side amplifies the supply-side cost. The HPB study (March 2026) found that 75% of Dutch consumers want to decide themselves which data they share with companies, and 58% want more control over which organisations hold their data. Providers that get identity right reduce friction and clear a trust hurdle that consumers explicitly flag.

2. The Identity Maturity Model

Most identity stacks weren't built from a single plan, but accumulated over years. Layers were added when a regulator demanded them, when a competitor launched a new feature, or when a new channel needed a login. The result is hard to benchmark. The IMM provides a shared vocabulary.

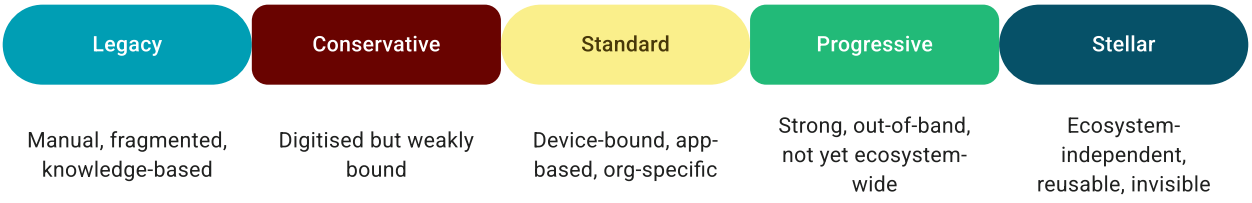
Why a maturity model?

A telecom provider with a working single sign-on calls its identity stack mature because the login works. A bank that has rolled out biometric authentication in its app calls its identity stack mature because the customer is happy

Maturity isn't determined by the technology in use. It's determined by how that technology works across the customer's full journey: at onboarding, at every login, at every signature, every time identity is checked. A bank can deploy the same identity app as a competitor and land at a different stage of the IMM, because what matters is how consistently and deeply it's integrated.

The five stages

Figure 2.1. The five stages of the Identity Maturity Model



Each stage shifts what identity looks like, what fragmentation persists, and what boundary identity cannot cross.

Legacy

Identity is manual, fragmented, and knowledge-based. Customers are **verified in person:** in a branch, in a shop, or by post. Authentication is username and password. Contract signing is **wet signature,** scanned and uploaded if the organisation has reached the upload stage. Each interaction invents its own proof. **Channels are disconnected** and trust is baked in procedures instead of identities. The business runs identity as an **internal cost centre,** and adding a channel means rebuilding identity from scratch. Identity does not exist as data and cannot cross the boundary between each interaction.

Conservative

Identity is digitised, but still **weakly bound and inconsistent.** Username and password remain, with SMS codes or hardware tokens added when a regulator or security team requires them. Paper becomes PDF, physical presence becomes a video upload, passwords become OTPs. The signals are still **weak, replicable and single-use.** Each journey step still picks its own method, and identity checks repeat step-by-step. The business operates a **multi-vendor identity stack** internally, and adding a journey step means integrating another vendor. Identity can't cross the boundary between verification moments within a journey. Identity exists as data, but the data is static.

Standard

Identity is **device-bound, app-based, and organisation-specific.** The mobile app is the primary channel, and works with **biometrics or a PIN code.** Onboarding uses document upload with a selfie or liveness check. Trust gets stronger but only locally: identity works inside one organisation, sometimes only inside one channel (the app, not the web). The business operates an identity platform, built in-house or licensed, and adding a customer segment means expanding that platform's reach. Identity cannot leave the silo (organisation or channel) that issued it.

Progressive

Identity is strong and 'out-of-band', meaning verification happens on another channel. But it's not yet reusable ecosystem-wide. The organisation has integrated an external identity scheme. **Channel and session fragmentation are solved.** Trust is substantial, in some cases high. But identity is still **issuer-centric, sector-specific, with limited reuse** beyond defined contexts. The business consumes an identity scheme rather than building one, and adding a market or sector means falling back to weaker identity outside the scheme. The boundary identity cannot cross at Progressive is **between ecosystems:** identity works inside the ecosystem it was built for, but not across ecosystems.

Stellar

Identity is **ecosystem-independent, reusable, and experience-native.** Verified once, identity is reused across organisations, sectors and journey steps. Attributes come from trusted sources. The same identity works for opening an account, signing a contract, confirming a transaction and sharing an attestation, regardless of which organisation is on the other side. **The business plugs into identity as infrastructure, and growth becomes identity-neutral.**

Stellar is not a stage one organisation reaches alone. It needs an acceptance network, integration depth, and a regulatory and market framework that makes journey-level reuse practical. A Progressive organisation can be using the strongest identification methods available today. What holds it short of Stellar is not the methods themselves, but the boundaries of the ecosystem it belongs to.

The dimensions

Eight dimensions describe what changes between stages. They are the diagnostic tool: an organisation at Standard on most dimensions but Conservative on reusability knows where to invest next.

Figure 2.2. The eight dimensions of identity maturity, mapped to the five stages

Dimension	Legacy	Conservative	Standard	Progressive	Stellar
Friction	High (manual, repeated)	Medium (digitised but interruptive)	Medium-low	Low	Very low
UX and speed	Slow, error- prone	Improved, still clunky	Fast within one app	Fast across channels	Seamless across journeys
Trust and assurance	Process- based	Limited	Substantial within silo	Substantial, high in some cases	High and transferable
Reusability	None	None	Local reuse	Partial reuse	Cross-organisational reuse
Channel maturity	Physical	Web	App-based	Out-of-band app	App-native ecosystem
Journey consistency	Fragmented	Fragmented	Consistent per org.	Mostly consistent	Fully consistent
Level of assurance	Low	Low	Substantial	Substantial (high in some cases)	High and transferable
Authentication factors	Knowledge	Knowledge	Knowledge + possession	Knowledge + possession + inherence	Knowledge + possession + inherence + identity

Source: itsme, Identity Maturity Model 2026.

The five use cases

Maturity is not uniform across an organisation. A bank can be Progressive on online authentication and Conservative on contract signing. A telco can be Standard on app login and Legacy on identity verification at onboarding. **The Index scores per use case wherever the data allows.**

The five use cases:

1. **Identity verification:** confirming who a new customer is at onboarding.
2. **Online authentication:** logging into the customer environment on web and in the app.
3. **Transaction confirmation:** approving a payment, transfer or sensitive action.
4. **Contract signing:** a new contract, a loan, a policy or a service agreement.
5. **Sharing customer data:** consent-driven data exchange between organisations or with a regulator.

Figure 2.3. The five use cases at each stage of the IMM

Dimension	Legacy	Conservative	Standard	Progressive	Stellar
Identity verification	Branch visit, ID card photocopy	ID upload plus selfie (synchronous)	ID upload plus liveness check, AI-verified (asynchronous)	Reusable verified identity from external app	Customer shares pre-verified attributes from their wallet
Online authentication	Username plus password	Password plus SMS code	Biometrics inside the app	External identity app, reusable	Passwordless, risk-adaptive, networked
Transaction confirmation	Phone call, card reader at branch	Card reader plus PIN	In-app push approval	External identity app step-up	Continuous, contextual approval
Contract signing	Wet signature, scanned and uploaded	Click-to-accept	Simple electronic signature	Qualified electronic signature (QES) via external app	Reusable QES across legal contexts
Sharing customer data	Phone, email, paper consent	Form-based, single use	API consent within a vendor	Consent-driven, reusable across services	Attestation-based, user-held, portable

The Index scores per use case where the NIQ data allows. Sharing customer data falls outside the NIQ data and is treated qualitatively in chapter 5.

Identity maturity self-assessement: a short diagnostic

Pick the closest answer for each of the following six questions. The result is a broad indication, not a measurement.

1. When a new customer onboards online, what is the dominant identity verification method? (a) Branch or post; (b) ID upload plus selfie or document scan; (c) ID upload plus liveness check; (d) External identity app; (e) Reusable verified identity, no re-verification required.

2. When an existing customer logs into your app, what authenticates them? (a) Username and password; (b) Password plus SMS code; (c) Biometrics or PIN inside the app; (d) External identity app; (e) Passwordless and continuous, risk-adaptive.

3. When the same customer logs in to your web environment, what happens? (a) Username and password; (b) Password plus SMS code; (c) Two-factor with an authenticator app; (d) The same identity used in the app; (e) Channel-agnostic, no separate web auth.

4. When a customer signs a contract, what do they use? (a) Wet signature scanned in; (b) Click-to-accept; (c) Simple electronic signature; (d) Qualified electronic signature via an external identity app; (e) Reusable QES across legal contexts.

5. When a sensitive transaction needs approval, what confirms it? (a) Phone call or branch visit; (b) Card reader plus PIN; (c) In-app push approval; (d) External identity app step-up; (e) Continuous, contextual, risk-adaptive.

6. When a customer needs to share verified data with a third party (a regulator, a partner, another service), how does that happen? (a) Paper or PDF; (b) Form re-entry; (c) API consent inside a vendor; (d) Consent-driven, reusable across services; (e) Attestation- based, user-held, portable.

Mostly (a) places you at Legacy. Mostly (b), Conservative. Mostly (c), Standard. Mostly (d) or €, Progressive. Mixed answers are the norm.

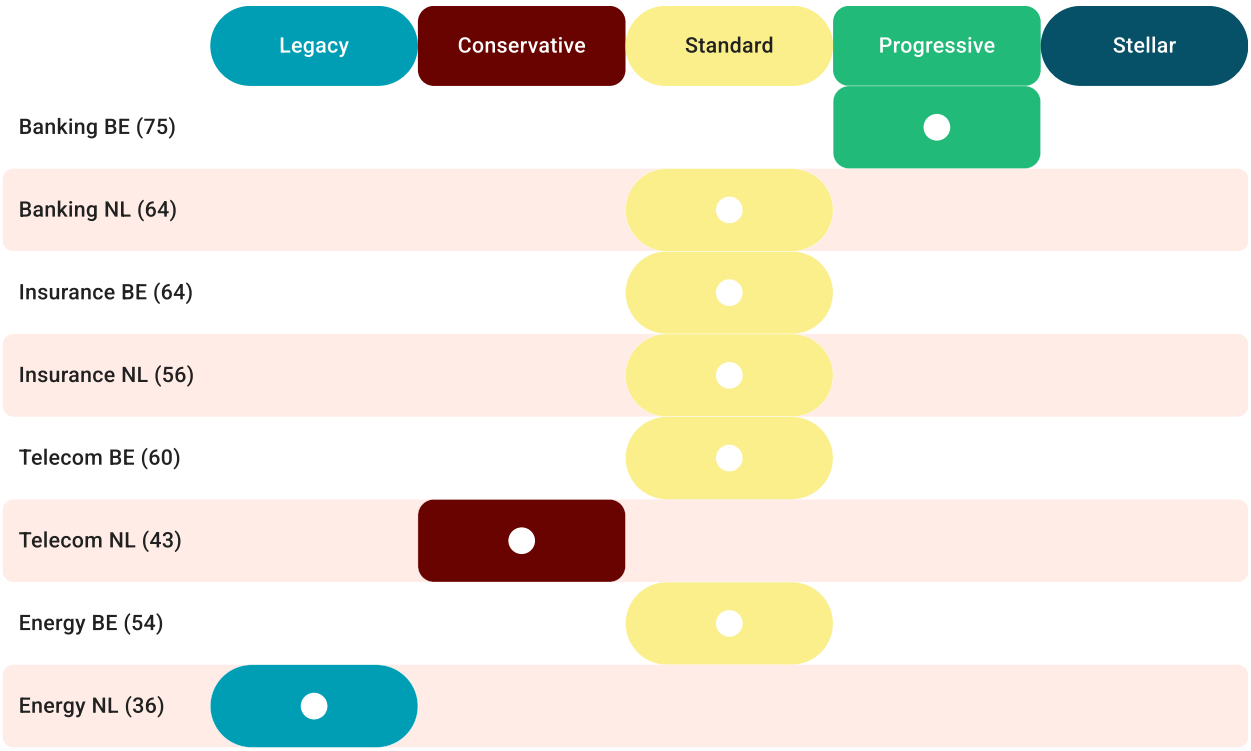
Want to perform an in-depth assessment of your Identity Maturity Score across use cases, touchpoints and channels to help you prioritize investments? Get in touch with our team.

3. The market today

Consumer expectation outpaces deployed identity in seven of eight markets. Belgian banking is the only sector and country where what providers offer matches what customers want. Everywhere else the gap is wide.

The chart below places each sector and country on the Identity Maturity Model. The score in parentheses is the NIQ maturity index for the sector: an average of method-level maturity across measured touchpoints.

Figure 3.1. Sector placements on the Identity Maturity Model



Source: NIQ Growth Spaces, April 2026. n=4,095 BENE.

Three patterns are immediately clear:

1. Belgian sectors run one stage ahead of their Dutch counterparts in three cases out of four.

2. The gap between sectors is wider than the gap between countries. Belgian banking sits a full stage above Belgian energy. Dutch telecom sits one stage above Dutch energy. The country you operate in matters less than the sector you operate in.

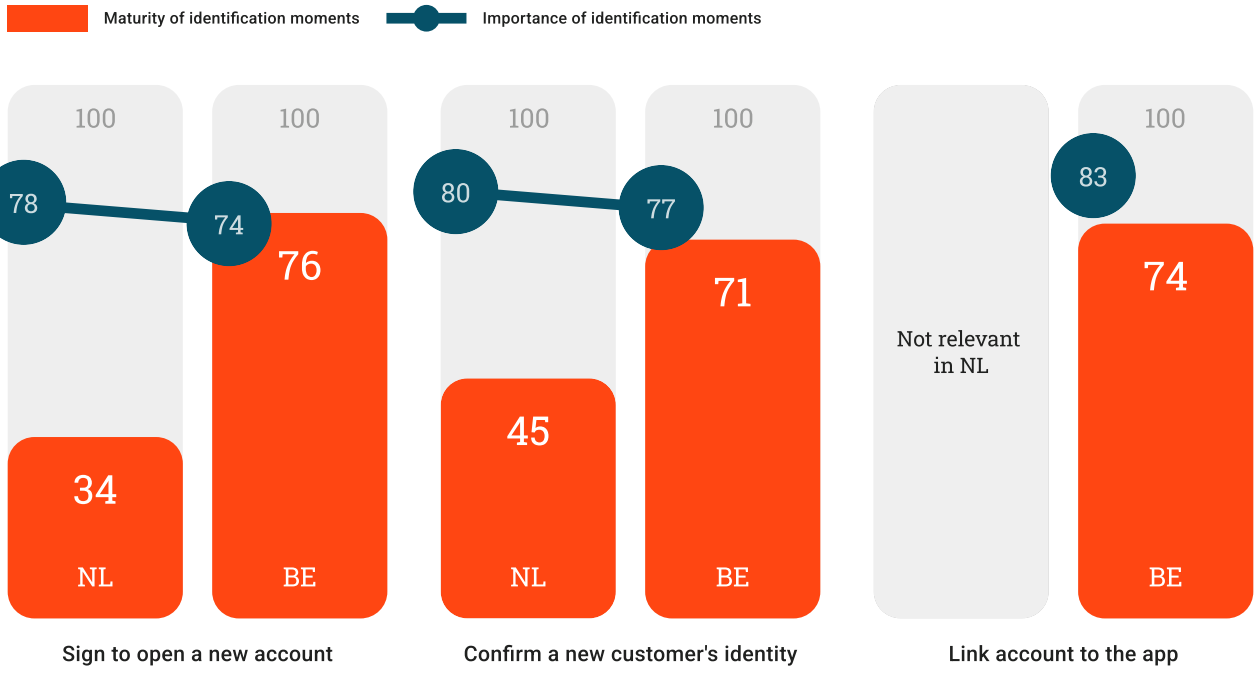
3. Belgian banking comes closest to the conditions Stellar requires. A shared identity layer at onboarding, deep integration across touchpoints, and an acceptance network that pulls adjacent sectors in. The cross-ecosystem reuse that defines Stellar is not yet present, but the building blocks are.

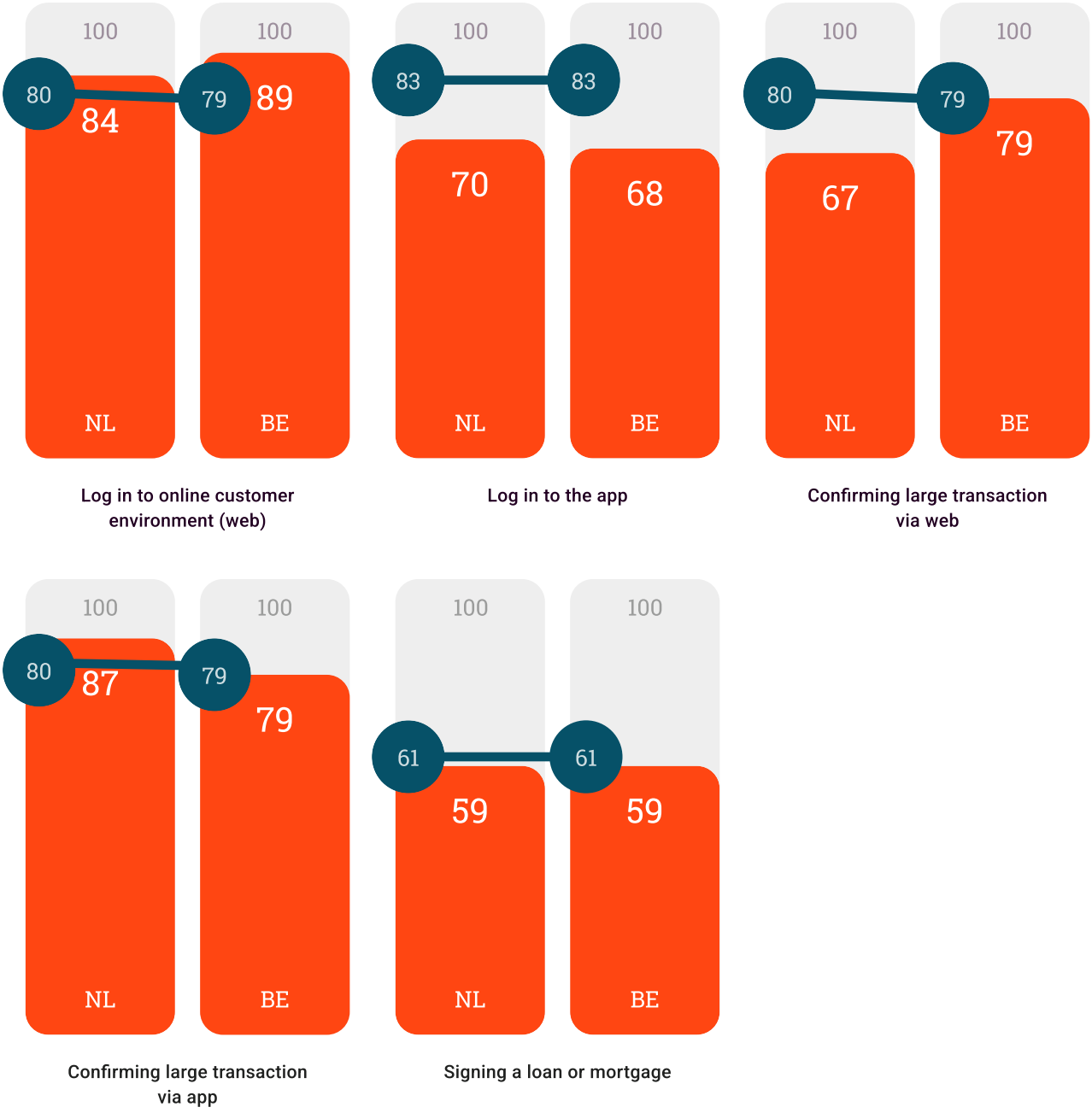
Belgian regulated industries run at least one stage ahead of Dutch counterparts in three cases of four.

Banking

Belgian banking reaches Progressive with a sector index of 75. Dutch banking reaches Standard with a sector index of 64. The main reason for this gap: Belgian banks share a reusable identity layer at onboarding, while Dutch banks have each built their own. Authentication is comparable in both countries.

Figure 3.2. Banking: maturity vs. importance per touchpoint





Source: NIQ Growth Spaces, April 2026

WHAT CONSUMERS EXPECT

39% of Dutch banking consumers say an external ID app should be the standard method at onboarding.

NIQ Growth Spaces, April 2026

The expectation lines up with Dutch consumer attitudes more broadly. The HpB study (March 2026) found that **33% of Dutch consumers feel their data is underprotected** when confirming their identity online, and **90% would feel safer with one trusted way to identify online.**

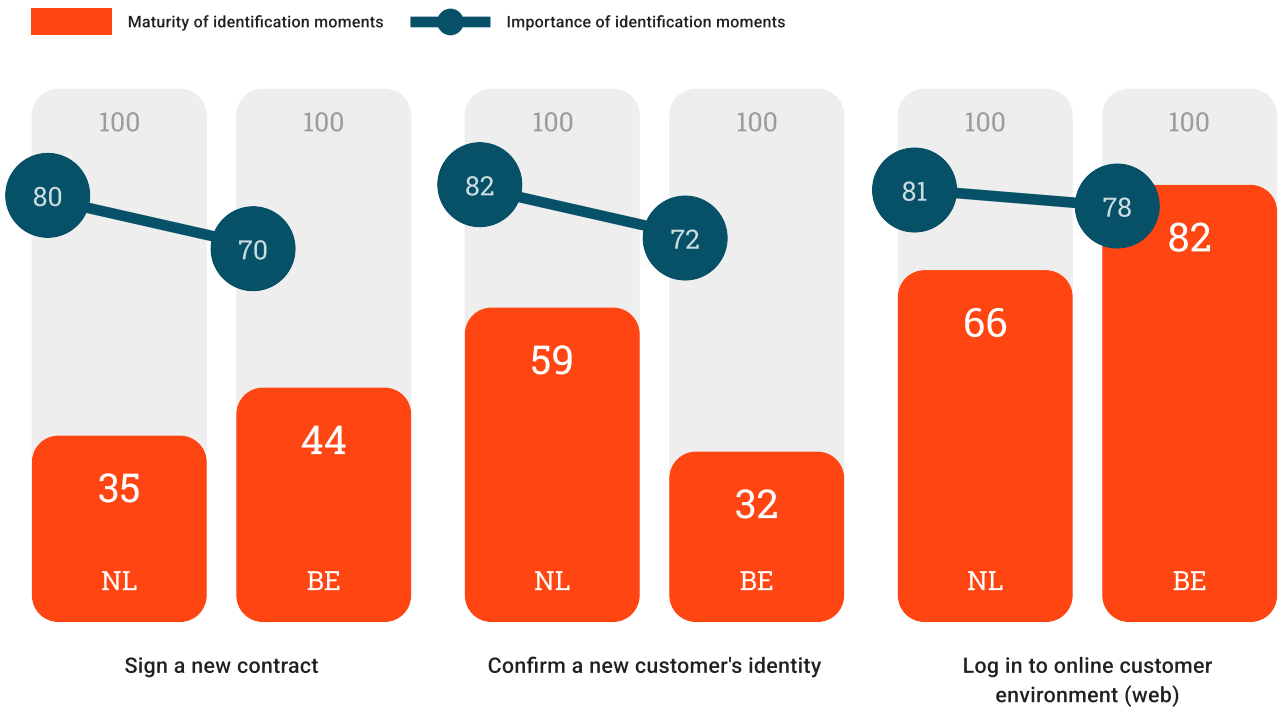
A detailed brand-level analysis of Belgian and Dutch banking, including read-outs for traditional banks and neo banks, is available in the forthcoming Banking focus report. Leave your e-mail to get it delivered straight to your inbox.

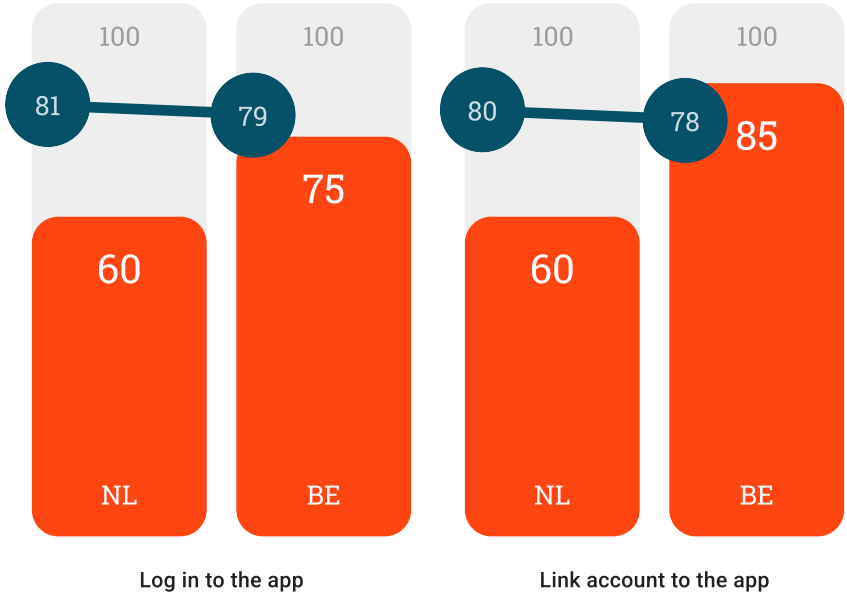
Insurance

The Belgian and Dutch insurance industries both reach Standard maturity, with a sector index of 64 and 56 respectively. Same stage, opposite reasons.

- In Belgium, itsme dominates authentication for the customer environment. Onboarding, however, stays broker-led and manual.
- In the Netherlands, health insurers use DigiD for both onboarding and authentication and score high; non-health insurers use traditional methods and score low. The Dutch sector average thus hides a bimodal market.

Figure 3.3. Insurance: maturity vs. importance per touchpoint





Source: NIQ Growth Spaces, April 2026

WHAT CONSUMERS EXPECT

63% of Dutch consumers say an external ID app should be the standard way to confirm identity at non-health insurance onboarding.

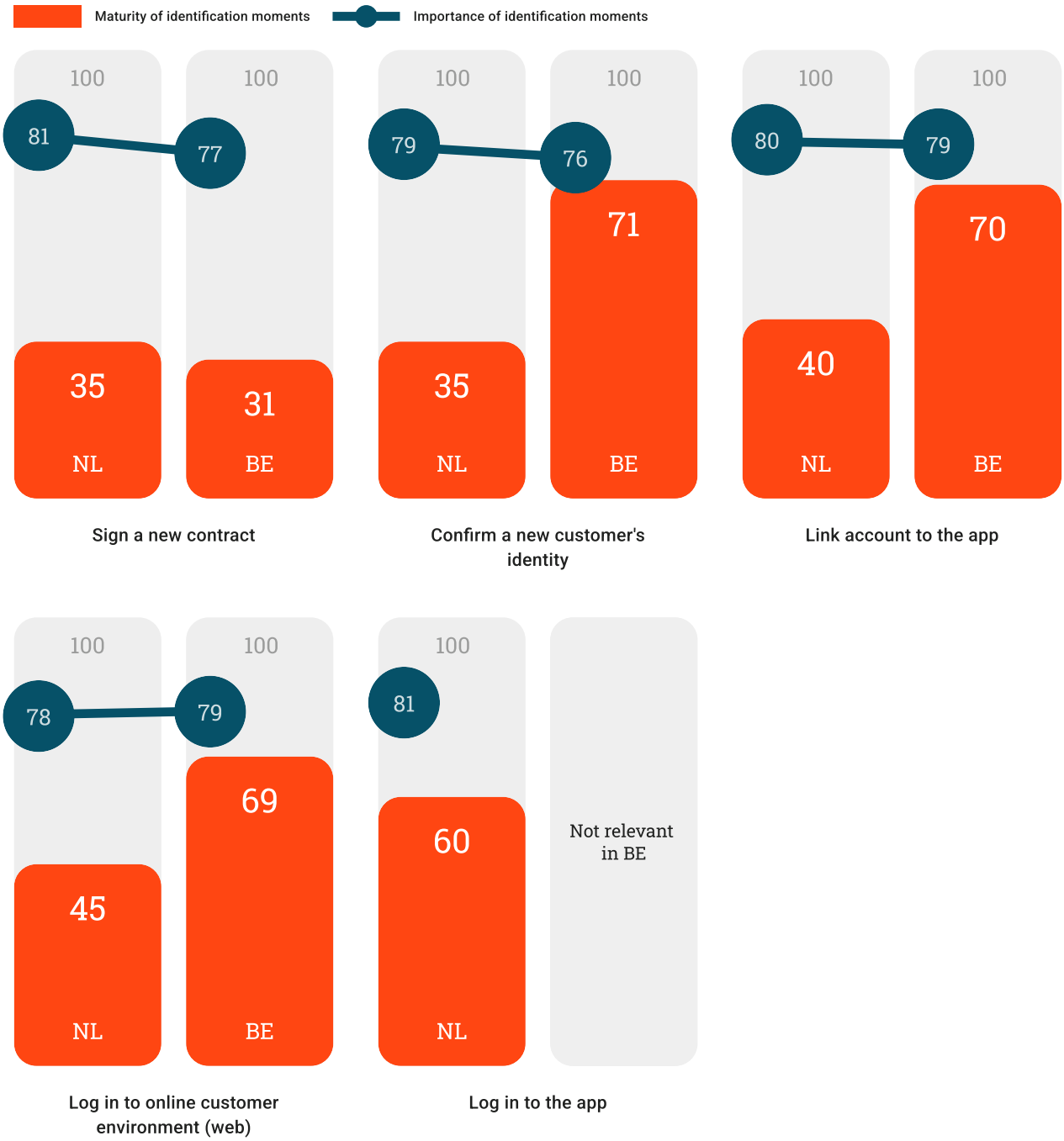
NIQ Growth Spaces, April 2026. Insurance NL, non-health segment.

A detailed analysis of Belgian and Dutch insurance, including the bimodal split between health and non-health insurers in the Netherlands, is available in the forthcoming Insurance focus report. Leave your e-mail to get it delivered straight to your inbox.

Telecom

Belgian telecom reaches Standard with a sector index of 60. Dutch telecom reaches Conservative at 43. The 17-point gap is one of the largest cross-country gap in the study. The cause is structural: most Belgian telecom providers integrate itsme as a default login method; no equivalent external identity app is as broadly deployed in Dutch telecom.

Figure 3.4. Telecom: maturity vs. importance per touchpoint



Source: NIQ Growth Spaces, April 2026

WHAT CONSUMERS EXPECT

Dutch telecom shows one of the widest deployed-vs-expected gap on basic login. Customers see telecom logins as high-stakes identity events; providers treat them as basic account access.

NIQ Growth Spaces, April 2026. Telecom NL.

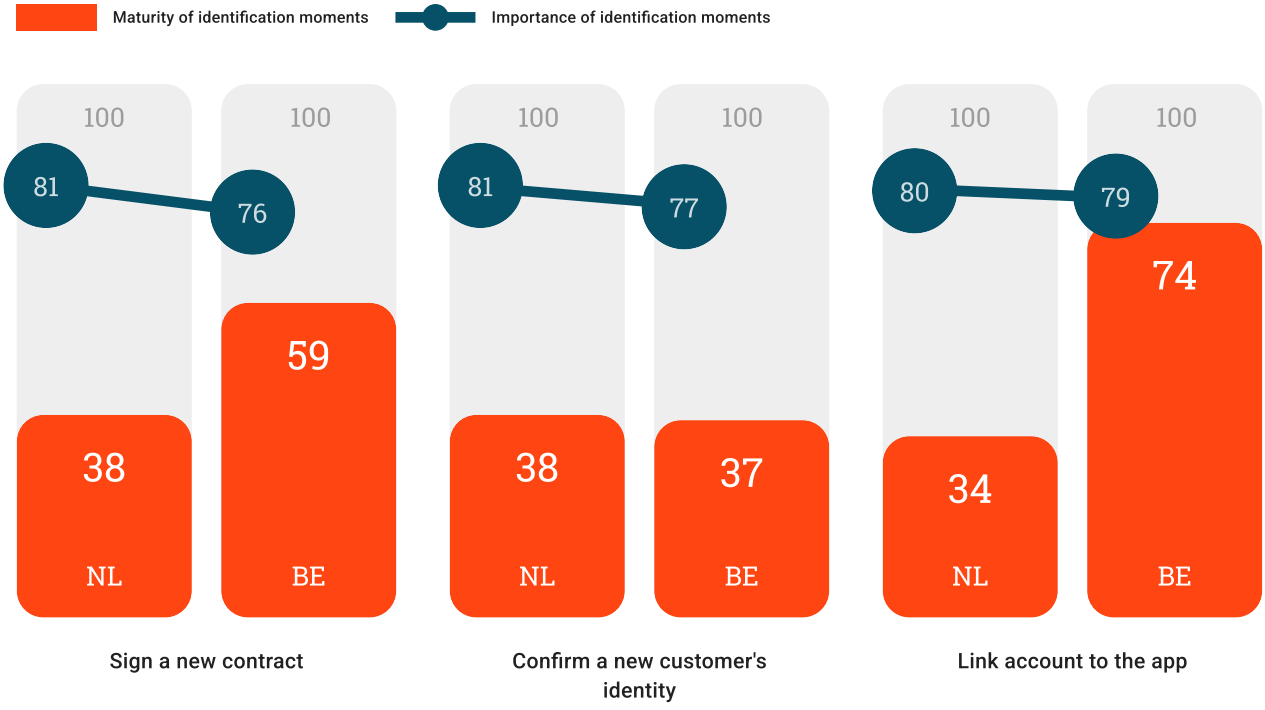
A detailed analysis of telecom in Belgium and the Netherlands, including the role of operators in SIM verification and the contrast between B2C and B2B journeys, is available in the forthcoming Telecom focus report. Leave your e-mail to get it delivered straight to your inbox.

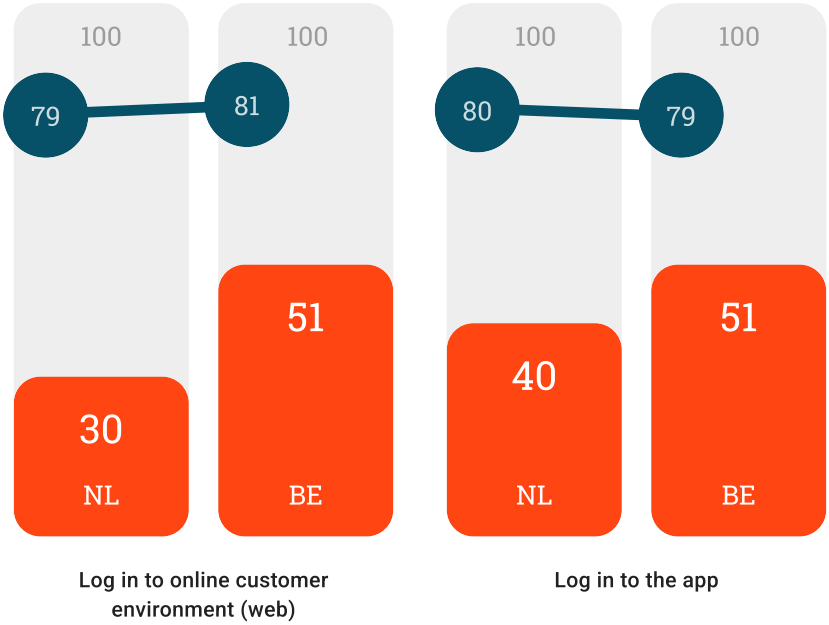
Energy

Belgian energy reaches Standard with a sector index of 54. Dutch energy reaches Legacy at 36. The 18-point gap is the largest in the Index. Dutch energy is the only sector-country pair below 40, and every Dutch provider in the study scores below 50 on Maturity while consumer Importance stays in the 79 to 81 band.

In Belgium, Engie and Eneco lift the sector average by integrating itsme on multiple touchpoints. The long tail of smaller providers does not. In the Netherlands, logging in to the customer environment on web scores 30 against an Importance of 79, the widest single-touchpoint gap in the Index.

Figure 3.5. Energy: maturity vs. importance per touchpoint





Source: NIQ Growth Spaces, April 2026

WHAT CONSUMERS EXPECT

57% of Dutch energy consumers want an external ID app to confirm identity. The infrastructure to satisfy that preference is not deployed.

NIQ Growth Spaces, April 2026

A detailed analysis of energy in Belgium and the Netherlands, including the role of switching and direct-debit verification, is available in the forthcoming Energy focus report. Leave your e-mail to get it delivered straight to your inbox.

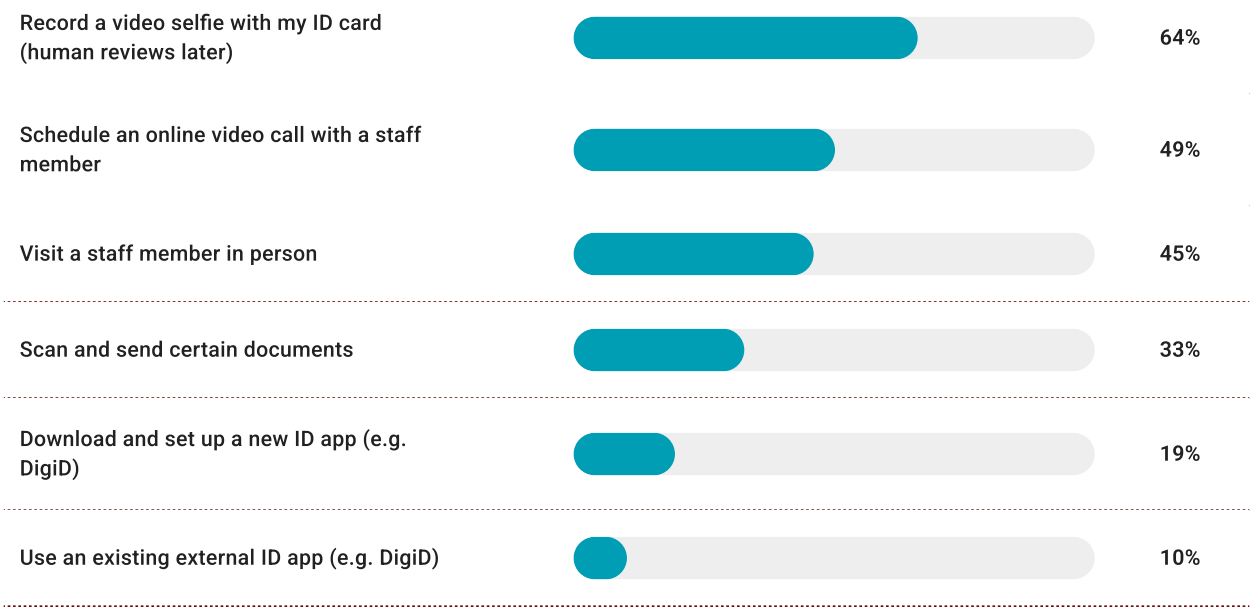
4. What consumers want

Providers worry consumers will reject external identity apps. The data shows the opposite. The methods in widest use today are the ones that most often stop people from becoming customers. External identity apps are the least blocking.

What blocks new customers

When asked what would stop them from becoming a new customer of a bank, insurer, telecom provider or energy supplier, Dutch consumers ranked six possible methods.

Figure 4.1. Barriers to becoming a new customer



NIQ Growth Spaces, April 2026. Dutch consumers (n=2,047).

Two findings:

1. The video-selfie method, recording yourself holding your ID card, is the single biggest barrier in the study at 64%. It outranks every other method, including ones that require physical presence. The energy sector applies it most often.

2. Downloading and setting up a new identity app puts off 19% of consumers. Using an existing identity app puts off 10%. Both numbers are well below the methods currently in use. The provider concern that 'customers will not download another app' does not match what the data says.

The methods providers default to today are the methods that block new customers. The method providers worry about deploying is the method consumers prefer.

External ID app as the default

What should be the standard practice for confirming a new customer's identity in each sector? Across all four sectors, in both countries, consumer preference is clear.

Figure 4.2. Consumer preference for identity confirmation, by sector

Sector	Top preferred (BE)	% BE	Top preferred (NL)	% NL	Method in 2nd place
Banking	Physical identification	44%	External ID app	39%	External ID app (BE: 42%)
Insurance	External ID app	40%	External ID app	63% (non-health)	Online form (BE: 23%)
Telecom	External ID app	46%	External ID app	52%	Physical identification (BE: 25%)
Energy	External ID app	51%	External ID app	57%	Online form (BE: 28%)

Top method named when consumers were asked what should be standard practice for confirming a new customer's identity. NIQ Growth Spaces, April 2026.

The pattern is consistent. External identity app is the top choice in almost every sector in both countries, ranging from 39% (Dutch banking) to 63% (Dutch non-health insurance). The second-place choice is usually a manual fallback, either physical identification or filling in an online form. No one prefers a video selfie or username and password as the standard for verifying identity.

The Netherlands: awareness, not appetite

THE AWARENESS GAP

itsme awareness: 97% in Belgium, 6% in the Netherlands. DigiD awareness: 99% in the Netherlands. iDIN awareness: 49% in the Netherlands.

NIQ Growth Spaces, April 2026

The Belgian consumer knows itsme and rates it as the safest and most user-friendly identification method, ahead of biometrics. In the Netherlands, where itsme is not known, the perception score is 17 points lower.

The trust dividend

Providers that offer a reusable identity scheme do not just remove friction. They also instill trust. NIQ asked Belgian consumers to rate companies that offer itsme as a login method against companies that do not.

Figure 4.3. Brand image effect of offering a reusable identity scheme

Brands offering itsme are rated higher on:

- Trustworthiness: 6.1 to 6.3 versus 5.3 for brands without (out of 10)
- Data security: 6.1 versus 5.3
- Professionalism: 5.9 to 6.1 versus 5.1
- Ease of doing business with the brand: 6.3 to 6.5 versus 6.0
- Perceived as innovative: 5.4 to 5.5 versus 4.7

Brand image scores out of 10, BE consumers. NIQ Growth Spaces, April 2026

The brand-image lift ranges from a third of a point to a full point on a ten-point scale. In a category where trust is the working currency, that's a significant gap.

The privacy paradox

Consumer behaviour does not always match consumer preference. The HPB study (March 2026) of Dutch attitudes makes that paradox visible.

- **Consumers value privacy.** 98% rate online privacy as important to some degree. 86% say it matters to them what happens to their personal data. 75% want to decide themselves which data they share with companies.
- **Consumers feel exposed.** 71% disagree that their personal data is safe on the internet. 68% feel at least somewhat unsafe online. 40% have been the victim of a data breach. 25% have had someone access one of their accounts without permission.
- **Yet consumers behave insecurely.** Only 33% use fully unique passwords across their online accounts. 28% write passwords on paper, 11% store them in a document on their computer, 14% on their phone. 51% have shared a copy of their ID document online in the past year, including 13% by email and 6% by WhatsApp.
- **And consumers feel powerless to fix it.** 57% feel there is little they can do to protect their personal data. 76% find privacy protection too complex to actively manage. 87% want fewer separate accounts and login methods. 90% would feel safer with one trusted way to identify online.

Consumers want privacy but they are not equipped to protect it alone. They want providers to do the work for them.

The consumer signal is unambiguous. Across sectors and across countries customers prefer reusable identity. They see the current default as a barrier and give a trust premium to providers that offer it.

5. Why fragmentation persists

Fragmentation does not disappear as an organisation matures, but instead changes shape. The naïve view of identity, i.e. that better security and a stronger app together produce a mature identity stack, is the most common reason organisations get stuck at Standard. Maturity is not the accumulation of features but the elimination of the gaps between them.

The naïve view

The common reading of the identity stack runs as follows: install a password reset, add two-factor when the regulator requires it, build a mobile app with biometric login, add document scanning and liveness for onboarding, then consider an external identity app for the higher-stakes flows. This view treats **identity as a stack of security features,** each more advanced than the last.

That view explains why most organisations reach Standard and stop. Each layer was installed because it solved a security problem. Once installed, each layer worked. The customer can authenticate, the regulator is satisfied, the audit passes. The stack looks complete because completeness was framed in terms of security, not in terms of the journey.

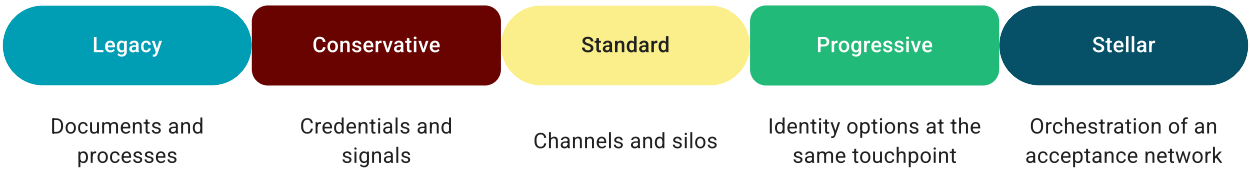
But identity is not a security feature. It is the **connective tissue of the customer journey.** The question that distinguishes Progressive from Standard is not 'is this transaction secure', but: 'do we know who the customer is, the same way, every time they interact with us, across every channel and every service'. The second question is much harder to answer.

In the HPB study (March 2026), **87% of Dutch consumers said they want fewer separate accounts and login methods, 76% find privacy protection too complex to manage actively, and 57% feel they can do little to protect their digital data.** The label for this last finding is **digital fatalism.** It is the consumer-side signature of identity fragmentation.

The fragmentation arc

Fragmentation shifts as maturity rises.

Figure 5.1. The fragmentation arc



The type of fragmentation an organisation faces changes at each stage of the IMM.

At Legacy: fragmentation is structural

Different documents, different people, different processes, no reuse at all. Identity is verified in person, by a staff member checking a document against a face. Each interaction invents its own proof.

At Conservative: fragmentation is a process problem

Identity is digitised, but every step reassembles trust from scratch. Paper becomes PDF, physical presence becomes a video upload, passwords become OTPs. The signals are still weak, replicable and single-use. The customer holds a username, a password, sometimes a hardware token, sometimes an SMS code. Each journey step picks its own method. Identity checks repeat step-by-step. The customer carries the burden of remembering and proving.

At Standard: fragmentation is a silo problem

Identity works, but only inside the organisation that issued it. The mobile app is the primary channel, and identity inside it is consistent: biometrics or PIN log the customer in quickly. But identity does not travel beyond the app. The customer who logs in seamlessly authenticates again on the web with two-factor SMS, again in the contact centre with security questions, again on a partner service with a fresh account. The organisation knows them inside the app and forgets them when they leave.

At Progressive: fragmentation is an economic and strategic problem

Multiple strong identity apps, multiple onboarding moments, redundant assurance costs, competing trust anchors. The customer can log in with itsme, with the bank's own credentials, with a passwordless link, with a username and password, with a card reader. The fragmentation moves from the customer to the organisation. Each integrated option needs maintenance, security review, fraud monitoring. The customer sees one smooth login. Behind it, the organisation maintains and pays for several identity providers running in parallel.

At Stellar: trust is shared infrastructure

Neither the customer nor the relying party has to care how trust was established, only that it meets the required assurance level. Fragmentation gives way to composability: identity becomes a shared layer instead of a repeated step. Verified identity, qualifications, entitlements and consents are portable across services, sectors and borders. The organisation's job becomes choosing the right identity for the right touchpoint, not building it.

As mentioned before, Stellar is not a stage a single organisation can reach by itself. It needs an acceptance network, integration depth, and regulatory alignment. EUDIW will be one building block. The acceptance network that makes a wallet credential practically usable is another. The orchestration layer that decides which identity belongs where is the third. Stellar requires all three to work together.

Concrete examples

Standard-stage banking

Take a Dutch bank with a strong app, biometric login, document upload at onboarding. Authentication maturity scores in the seventies. The Index places the bank at Standard. The fragmentation is invisible inside the app. It shows up when the customer calls the contact centre and is asked security questions; when they switch to a sister insurer and re-authenticate; when they sign a loan and get routed back to email and PDF. The identity stack works. The journey around it does not.

Standard-stage telecom

Take a Belgian telecom provider with itsme integrated as a login option. Login maturity scores 69 on the web. The provider has not made itsme the default. Customers can also use username and password, and many do. The strong identity option exists, the customer knows it, but the deployment hasn't made it the path of least resistance. Only 57% of Belgian banking customers use itsme on average when it's offered alongside username and password; usage is much higher when it's the default.

Standard-stage energy

Take a Belgian energy provider without itsme integration. Login maturity scores in the thirties. The provider uses username and password for the customer environment, and phone, email or one-click consent for signing. Identity at onboarding is a form, with verification handled in the background through address and account checks. The provider has not invested because regulatory pressure on energy is lighter than on banking. The data shows consumers still expect more: importance scores in Belgian energy run in the seventies and eighties, while maturity scores in the thirties to seventies.

Why Stellar isn't reachable alone

Three properties define Stellar, none of which a single organisation can build.

1. **An acceptance network.** Reusable identity is only valuable if it's accepted at the moments the customer needs it. Belgian financial services reached an early version of this with itsme, because most banks integrated the same identity layer in roughly the same window. The behaviour created by that single customer login then pulled telecom, energy and insurance toward the same integration. No single bank could have built that alone.

2. **Integration depth.** A reusable identity that appears at login but not at signing is not Stellar. The deeper the integration runs, the more the customer trusts it, and the more the organisation can shed redundant assurance steps. Depth is built one touchpoint at a time, usually over years, usually with a shared roadmap.

3. **Regulatory and market alignment.** EUDIW, eIDAS 2.0 and the surrounding framework set a common floor for what reusable identity means, what assurance level it carries, and how it interoperates across borders. Without that floor, every integration is bilateral. With it, the same identity moves between Belgium and the Netherlands, between banking and energy, between private platform and public service.

6. Moving up the maturity curve

Four compounding forces move organisations between stages: changing user expectations, regulatory pressure, fraud, and the arrival of reusable identity infrastructure. Together they explain almost every transition visible in the NIQ data.

The drivers of change

Figure 6.1. Drivers of stage transition

Stage transition	Driver	Breaking points at the previous stage	What changes
Legacy to Conservative	Channel migration: customers move online faster than the organisation can serve them through branches.	Branch capacity, paper processes, in-person identification.	Username and password authentication appears. A second factor is added for high-value actions. Document upload replaces document presentation.
Conservative to Standard	Mobile primacy: the app becomes the primary channel for routine interaction.	Web-only flows; password fatigue; two-factor SMS friction at every login.	Biometric or PIN login inside the app. Liveness checks at onboarding. Push notifications replace SMS codes for transaction confirmation.
Standard to Progressive	Reusable identity becomes available in the market, and customers begin to expect it.	Identity does not travel between channels or between services. The organisation pays for assurance it has already paid for elsewhere.	An external identity app is integrated. The same identity is used at onboarding, login and signing. Fragmentation moves from the customer's burden to the organisation's.
Progressive to Stellar	Acceptance network, integration depth and regulatory floor converge.	Multiple strong identity options at the same touchpoint; redundant assurance costs; fragmentation of consents and attestations.	Identity is composable across services, sectors and borders. Attestations and consents are portable. Orchestration replaces integration.

Each transition has a primary driver, the breakage that forces the move, and the changes that mark it.

Three observations:

1. **The transition from Standard to Progressive is the most market-dependent.** The other transitions can be made by an organisation acting alone: a mobile app can be built, a password reset can be installed. Standard to Progressive needs a reusable identity layer in the market. Where one exists, the transition is fast. Where it doesn't, the transition doesn't occur.

2. **Regulation accelerates transitions but rarely starts them.** eIDAS 2.0 will not, on its own, move a Conservative bank to Standard. It will accelerate a bank already moving, and it will set a floor below which no bank can fall.

3. **Fraud is the driver most cited in security and compliance teams and the least visible in the consumer data.** Consumers don't know how much fraud their bank absorbs in a year. They know how much friction they accept at the door. Organisations underestimate friction relative to fraud as a driver of customer behaviour.

EU Digital Identity Wallet: raising the floor

The European Digital Identity Wallet (EUDIW) **launches at the end of 2026** and ramps through 2027 and 2028. By 2028 it will be in production across member states, with binding obligations on regulated services in essential services and public administration.

What EUDIW delivers

EUDIW is a public framework for a digital identity wallet, issued or accredited by each member state, holding verified identity attributes and qualified attestations. It does three things.

1. **It sets a high regulatory floor:** every member state will have a wallet at eIDAS Level of Assurance High.

2. **It makes cross-border identity practically usable:** a Belgian citizen authenticating to a Dutch service uses the same wallet they use in Belgium.

3. **It standardises attestations:** qualifications, entitlements and consents move through a common framework instead of bilateral integrations.

How EUDIW impacts the IMM

EUDIW gives every regulated organisation in Europe access to Progressive-grade methods at the touchpoints the regulation covers. Public-sector services and banks that today rely on paper, in-person verification or username and password will be required to support a reusable identity at eIDAS Level of Assurance High. The first wave of use cases is sector-bound by design: public services and banking in the Netherlands and Belgium, with insurance and telecom following.

Access to the method is not the same as a Progressive sector score. The wallet provides reusable identity with high assurance. Integration depth, acceptance network and journey-level reuse remain organisational work. A bank that integrates EUDIW at login has deployed a Progressive method on one touchpoint. A Progressive sector score needs EUDIW at onboarding, at signing, and across the rest of the journey.

Capability is not the same as adoption. The Index measures what providers deploy, not what customers use. In the first years of EUDIW, those two numbers will diverge sharply. Wallets will be integrated and accepted, but most customer journeys will still run on the existing options offered alongside.

What EUDIW does not deliver

Three things fall outside its scope.

1. **The acceptance network among private services without regulatory obligation:** EUDIW will be accepted where the regulation reaches, not everywhere else.
2. **Integration depth:** EUDIW provides credentials; embedding them into onboarding, signing, transaction confirmation and support is each service's work.
3. **Orchestration:** EUDIW is one wallet among several (banking apps, postal wallets, sector wallets, big-tech wallets); choosing the right one per touchpoint, and managing the customer experience across them, is an orchestration problem above the wallet layer.

> **EUDIW raises the floor of European digital identity. The ceiling, the integration depth and journey-level reuse that defines Stellar, remains a separate organisational investment.**
>
> *Identity Maturity Index 2026, Part 5.*

The regulatory environment

Three regulatory regimes shape the transitions visible in the data.

eIDAS 2.0

Regulation (EU) 2024/1183 sets the legal framework for EUDIW, qualified electronic signatures, qualified electronic seals and qualified electronic attestations. It creates obligations on designated relying-party sectors to accept EUDIW, and opportunities to issue qualified attestations that travel across borders. It is the single most consequential regulatory development for digital identity in Europe since GDPR.

NIS2

The Network and Information Security Directive raises the cybersecurity baseline for organisations operating essential or important services, which covers most banking, energy, telecom and digital infrastructure in the Index. NIS2 does not mandate a specific identity stack, but the obligations on authentication strength, audit trails and incident response create downstream pressure on identity architecture. Username and password becomes hard to defend under NIS2 audit.

Sector-specific rules

Each sector operates inside a regime that touches identity. Banking has PSD2, soon PSD3, with Strong Customer Authentication. Insurance has IDD, with know-your-customer (KYC) obligations at onboarding. Telecom has the European Electronic Communications Code, with SIM-registration in several member states. Energy has the Clean Energy Package and the consumer-protection rules flowing from it. Each creates pressure on a specific touchpoint, and the pressure is uneven across sectors.

What to look for in 2026 to 2028

Six signposts tell you how the identity-maturity landscape is moving:

1. The first EUDIW integrations at scale

The first regulated private services to integrate EUDIW for real customer journeys, not pilot programmes, will appear in late 2026 and through 2027. Watch which sectors integrate first, which touchpoints they touch, and how quickly customers adopt the wallet relative to alternatives still available. Banking and public services are expected to lead, with insurance and telecom behind.

2. Convergence or divergence in Dutch private-sector identity

DigiD is established in public-sector and health insurance contexts. iDIN is partial. itsme arrives in June 2026, with full replacement of iDIN scheduled for 2028. EUDIW arrives at the end of 2026. Whether the Dutch market converges on a single dominant private-sector identity layer, or continues with a multi-wallet pattern, will shape every sector score.

3. The response of Dutch energy

Dutch energy has the largest deployed-versus-expected gap in the Index. The sector has the regulatory permission, the consumer demand and the supply of reusable identity options to move from Legacy to Standard within 12 to 18 months if a single major provider integrates.

4. The QES wave in non-banking sectors

Qualified electronic signature in insurance, energy and telecom has been a long-standing aspiration. eIDAS 2.0, EUDIW and existing reusable identity layers in BE make 2026 to 2027 the most plausible window for non-banking QES to reach scale.

5. The wallet-acceptance question

The most important strategic question is not which wallets exist but which acceptance networks form around them. A wallet that is technically excellent and not widely accepted is not a Stellar wallet.

6. The wallet-fraud question

A wallet that is accepted is not the same as a wallet that is trusted in use. The current EUDIW design certifies credentials at issuance and validates them as valid or invalid. It does not yet provide a shared layer for device intelligence, behavioural signal, or dynamic response to fraud patterns as they evolve. One thing to watch closely is how the framework develops around real- time fraud response, and which actors take on that work. The wallets that earn relying-party trust will be the ones that close this gap and go beyond meeting the certification bar.

7. Methodology

This section documents the studies behind the Index. The high-level explanation of what was measured and what the scores mean is in Chapter 1.

The NIQ Growth Spaces study

NIQ (Nielsen Consumer LLC) collected the data in April 2026 through its Growth Spaces framework. itsme commissioned the study. NIQ owns the methodology, the fieldwork and the analysis. itsme owns the strategic framing, the IMM mapping and the sector placements. Quotas matched the BENE adult population for age and gender. Brand quotas matched client distribution within each sector. Sector averages in this Index are simple means across measured touchpoints, not market-share weighted.

The HpB study

HpB conducted a consumer study on attitudes toward digital identity, privacy and security, March 2026 with approximately one thousand Dutch respondents. The study covers concerns about digital safety, trust in providers, willingness to share data, and behavioural patterns such as password practice and ID-document sharing. The Index draws on HPB where consumer attitudes complement the NIQ data, particularly in the Dutch country context.

Maturity score methodology

NIQ scored each identification method on a 0 to 100 scale, with values of 20, 40, 60, 80 or 100 based on security profile and reusability. Username and password scores 20. Qualified electronic signature backed by an ecosystem identity app scores 100. The touchpoint maturity score is the share-weighted average across methods used by respondents at that touchpoint. Sector maturity is the average across touchpoints, weighted equally.

Importance score methodology

Importance combines three measures: online-availability preference (weight 0.5), expected safety (weight 0.25) and expected ease of use (weight 0.25). The composite is the figure shown alongside maturity in every chart in Part 3.

Use-case re-cut

NIQ scored per method within a touchpoint. To produce the use-case view in Part 2, touchpoint data was re-cut onto the five IMM use cases. Identity verification combines onboarding touchpoints. Online authentication combines all login touchpoints. Transaction confirmation covers large- transaction approval (banking only). Contract signing covers loan, mortgage and policy signing. Sharing customer data is treated qualitatively because attestation flows did not fit the NIQ touchpoint structure.

How NIQ and the IMM relate

NIQ Growth Spaces and the Identity Maturity Model were built independently. They are complementary, not interchangeable. They agree at the extremes: NIQ's 20-point methods (username and password) map to Conservative or Legacy on the IMM, and NIQ's 100-point methods (itsme or EUDIW integration) map to Progressive or Stellar. They diverge in the middle, where the NIQ scale is technology-anchored and the IMM is journey-anchored. Where they diverge, the Index reports both: the NIQ score as data, the IMM stage as interpretation.

Limits of the data

The study measured consumer perception and current deployed maturity. It did not measure enterprise revenue impact, fraud rates or abandonment. The cost-of-friction estimates are directional and draw on external sources (Signicat, Fenergo, OneSpan).

Sharing customer data, the fifth IMM use case, was not measured directly. Part 5 treats it qualitatively.

Identity Maturity Index 2026 is published by itsme. Data collected by NIQ in April 2026 under commission, and HPB in March 2026. Editorial responsibility for the IMM mapping, the placements and the framing rests with itsme. For methodology queries, contact press@itsme.com. *© 2026 Belgian Mobile ID SA / NV. All rights reserved.*