telesign | bics Proximus Global | routemobile

Digital Communications Trends

The key themes shaping 2026

Foreword

A new digital landscape is emerging.

Enterprises across industries are reimagining how they connect with customers and safeguard digital interactions. At the same time, expectations are accelerating. Today's customers demand seamless, human-like, contextual conversations across every channel. They expect instant onboarding supported by verifiable identities, payments that are secure and effortless, and protection from fraud before threats emerge. Above all, they expect these experiences to work reliably and consistently – everywhere, every time.

Yet the boundaries between channels, identities, and networks are dissolving. Organizations, from startups to global enterprises, have accelerated efforts to modernize their digital ecosystem. The true shift, however, is not simply the move to digital – it is the convergence of the technologies underpinning it. Connectivity, identity, payments, security, AI, channels, and applications are no longer separate domains but are becoming one continuous, trusted platform powering customer engagement.

As a result, how a brand connects and communicates has become as critical as the products it offers. Competitive advantage now hinges on meeting three primary communication priorities:

- Confident connectivity
- Trusted digital interactions
- Conversational commerce

These capabilities define success in the new digital economy.

As we move forward in 2026 and beyond, powerful forces are reshaping communication, identity, and connectivity. These emerging trends highlight where enterprises must innovate – and where Proximus Global is leading as a trusted partner. This report serves as a guide to the future of digital communications, outlining the challenges, opportunities, and transformative potential ahead for organizations that embrace convergence, trust, and innovation at the core of their digital experience strategies.

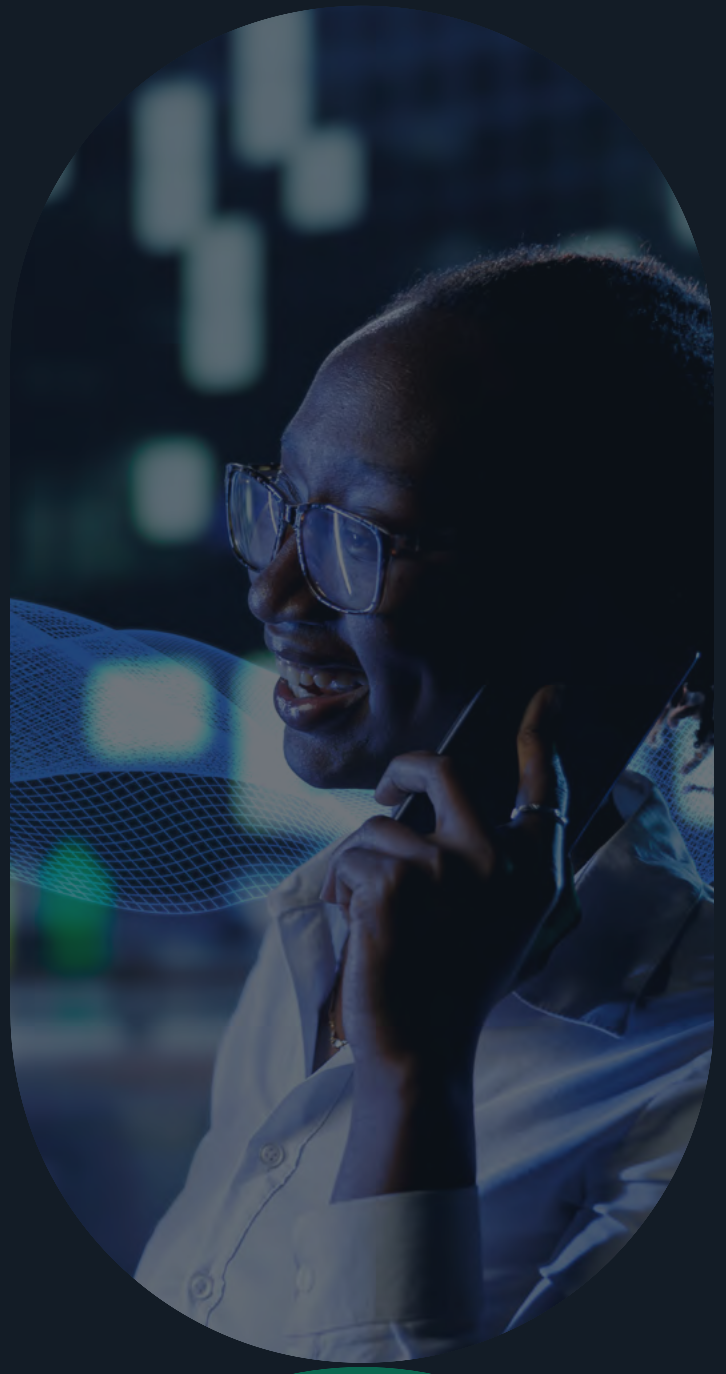
Sincerely,

Seckin Arikan
Chief Executive Officer
Proximus Global

Contents

01

The new digital trust infrastructure



02

Programmable, trusted connectivity

03

AI-native customer engagement

04

Future-proof compliance by design for advanced digital interactions

05

Unified platforms beyond big tech

1

The new digital trust infrastructure

As digital engagement scales across channels, enterprises are re-architecting trust as a real-time infrastructure layer that continuously verifies who the user is, what device they're on, how they behave, and when to step up security. The result: less friction for trusted users, stronger controls for risky ones.

Digital trust scoring is the new verification standard

Passwordless & silent authentication goes mainstream

Trust becomes invisible in voice conversations

Digital trust scoring is the new verification standard

As digital interactions grow, consumer tolerance for friction is rapidly declining. Traditional verification methods, such as passwords, repeated "Know Your Customer" (KYC), and rigid fraud checks, are eroding trust and driving abandonment. Trust is no longer implicit; it must be earned, measured, and activated in real time.

What's changing
From static, siloed fraud checks → to unified, real-time trust scores that fuse identity, behavior, device/network, and payment risk signals.

Implication
Trust becomes a measurable control surface that tunes friction dynamically (progressive onboarding, adaptive MFA, explainable decisions).

Why this matters
Users punish friction and "data over-collection"; meanwhile bots and modern fraud bypass legacy blacklists, forcing a shift from rules to reputation.

The problem it solves
Increases conversion while improving auditability, step-up only when risk rises, stay invisible when trust is high.

> "Churn from login issues is real. Unified digital scoring mends trust eroded by data fatigue."

Ben Vandermeulen
Chief Revenue Officer
Proximus Global

Key insights

87%
of consumers lost patience online last year.[1]

31%
abandoned brands due to repeated logins / excessive data demands.[2]

64%
trust brands more when they use MFA/ biometrics/passkeys.[3]

50%
Bots ≈ 50% of web traffic; legacy blacklists punish good users and miss bad ones.[4]

Passwordless & silent authentication goes mainstream

As password-related breaches and user friction reach critical levels, enterprises are moving rapidly toward authentication models that are both more secure and more seamless. Authentication is no longer a visible step; it is becoming invisible, continuous, and context-aware.

What's changing
From passwords + OTP fatigue + visible friction → to passwordless and "silent" authentication driven by SIM/network signals, device trust/behavioral biometrics, and SIM-swap detection.

Implication
Authentication shifts from a user task to a background decision. In milliseconds, not steps.

Why this matters
Credential attacks and reset friction degrade conversion and raise support costs; enterprises want security that improves UX simultaneously.

The problem it solves
Eliminates password-based breach exposure, reduces drop-offs, and makes fraud controls continuous and contextual (especially for mobile-first, high-frequency journeys).

> "Silent authentication delivers modern enterprise security without compromising UX."

Ben Vandermeulen
Chief Revenue Officer
Proximus Global

Key insights

- Password resets + phishing + credential breaches are **"failing at scale."** [5]
- **Passkeys are mainstream: 74%** awareness, **69%** enabled on ≥1 account, **38%** enable wherever possible. [6]
- **Security + convenience align: 53%** say more secure, **54%** say more convenient.[7]
- **Enterprise signal: 48%** of top 100 websites have implemented passkeys.[8]
- Silent auth wins in mobile-first + high-frequency + high-fraud sensitivity use cases.[9]

Trust becomes invisible in voice conversations

Enterprises relying on voice channels are increasingly challenged by a widening gap between customer experience and security. Traditional authentication methods create friction, frustrate customers, and elevate fraud risk, leaving contact centers vulnerable to identity-related losses. By 2026, voice biometrics and in-call authentication are expected to become standard across regulated industries, with the global voice biometrics market growing at over 20 percent CAGR through the decade (Fortune Business Insights, 2024).

What's changing
From knowledge-based voice authentication and step-up questioning → to passive voice biometrics + continuous in-call verification + seamless identity checks.

Implication
Voice becomes a high-trust channel again: security embedded inside the conversation instead of interrupting it.

Why this matters
Contact centers sit at the collision point of CX and fraud risk; traditional methods slow calls, frustrate customers, and leave identity losses exposed.

The problem it solves
Cuts handle time while strengthening fraud defenses, especially in regulated industries where auditability and compliance assurance matter.

> "Safe calls shouldn't just sound safe. Embedded voice trust proves it"

Ben Vandermeulen
Chief Revenue Officer
Proximus Global

Key insights

- Voice security and customer experience are converging into one control plane.[10]
- Trust becomes an invisible layer embedded within every interaction.[11]
- Passive authentication reduces friction while strengthening fraud protection.[12]
- Adoption expectation: voice biometrics + in-call auth become standard in regulated industries.[13]

2

Programmable, trusted connectivity

Connectivity is no longer just about cables and coverage; it's now programmable, intelligent, and revenue-centric. Enterprises unlock new business value when network capabilities, identity, verification, quality of service, and global provisioning are exposed as trusted, programmable interfaces that power digital experiences, automate trust, and enable new monetization models.

5G Networks are redefining real-time digital experiences

The surge of on-demand global eSIM connectivity

Monetization favors a small set of high-impact network APIs

5G Networks are redefining real-time digital experiences

By 2026, global 5G traffic is set to surpass 4G, unlocking sub-20ms latency through edge computing. This shift makes immersive AR, live video collaboration, telemedicine, and remote operations viable at scale. However, real-time experiences demand consistency, not just speed, and that's where enterprises are hitting limits. While 5G + edge makes immersive experiences technically possible, **inconsistent QoS across fragmented networks** causes jitter, dropped sessions, and buffering, breaking immersion, frustrating users, and driving up operational costs.

What's changing
From best-effort mobile broadband → to programmable 5G + edge enabling sub-20ms latency and real-time experiences (AR, telemedicine, remote ops).

Implication
Latency becomes table stakes; reliability/QoS becomes the differentiator (predictable latency, bandwidth, authenticated sessions).

Why this matters
Inconsistent QoS creates jitter, dropped sessions, and buffering—breaking immersion and raising costs.

The problem it solves
Turns "possible" real-time apps into deployable experiences by guaranteeing performance across fragmented networks.

> "eSIM & network APIs accelerate 5G into a low-latency growth engine, vital for critical operations."

Jorn Vercamert
Chief Product Officer
Proximus Global

Key insights

5G **5G traffic** projected to overtake 4G globally by 2026.[14]

AR + live video enterprise use cases projected to grow **300%+.**[15]

Sub-20ms edge latency drops below human perception for real-time overlays/assistance/control[16]

✓ **"Guaranteed experience" (QoS) is the advantage, not raw speed.**[17]

The surge of on-demand global eSIM connectivity

The travel eSIM market is experiencing explosive growth of **300%+ in five years** as consumers and enterprises demand instant, affordable, borderless connectivity. With mass smartphone adoption already in place, travel eSIM has moved from early adoption to revenue-scale reality.

What's changing
From roaming charges, physical SIMs, and country-by-country management → to on-demand eSIM with instant provisioning across geographies.

Implication
Connectivity becomes a checkout-native product—bundled by airlines/OTAs/hospitality/loyalty programs; enterprises remove SIM logistics bottlenecks for IoT and global ops.

Why this matters
Roaming is costly and physical SIMs add language/vendor/setup friction; for enterprises, manual SIM swaps don't scale.

The problem it solves
A rare low-friction revenue play: proven tech, high awareness, minimal upfront investment—own the "connectivity layer" before commoditization.

> "When connectivity becomes eSIM-native, the SIM tray disappears & a high-margin upsell appears in the booking flow."

Jorn Vercamert
Chief Product Officer
Proximus Global

Key insights

- Adoption is already here: **1B eSIM smartphone connections by 2025**.[18]
- Travel eSIM spend reaches **$3.3B by 2025**.[19]
- Smartphone eSIM connections grew **594% since 2022**.[20]
- Readiness: **87%** of eSIM-aware consumers see travel value; **70%** of roaming-avoiders likely to adopt.[21]
- China accelerant: Tier-1 operators embraced eSIM in 2025; projections to **364M eSIM smartphones by 2030**.[22]

Monetization favors a small set of high-impact network APIs

By 2026, enterprises will increasingly adopt **programmable network APIs** designed around industry-specific workflows and regulatory requirements. Broad, horizontal API catalogs struggle to scale in regulated environments where compliance, auditability, and identity assurance are as critical as engagement, and where monetization concentrates around a small set of high-value capabilities. More than 60 percent of organizations in regulated industries report that regulatory complexity slows or limits digital customer interaction initiatives, reinforcing the need for focused, trust-led network programmability rather than long-tail API exposure.

What's changing
From broad, horizontal API catalogs → to a focused set of compliance-ready network APIs aligned to regulated workflows (identity, location, performance).

Implication
Monetization concentrates where APIs embed trust and auditability into transactions, not where catalogs are large.

Why this matters
Regulated industries report regulatory complexity slowing digital interaction initiatives; "long-tail" APIs struggle to scale under audit requirements.

The problem it solves
Accelerates time-to-value by standardizing high-value capabilities (number/location verification, QoD, device mgmt, status) that map to real compliance pressures.

> "Aim your network APIs at big painpoints like fraud, compliance, and performance, since that is where serious spending happens."

Jorn Vercamert
Chief Product Officer
Proximus Global

Key insights

$ Revenue concentrates: six APIs projected to capture **~70%** of Network API revenue in 2026 **(~$6.3B of $9.1B)**.[23]

Top value pools are **Number Verification ($2.65B)** and **Location Verification ($1.30B)** (2026).[24]

Strategy: align programmable network bets to **regulatory reality + revenue concentration**, not breadth.[25]

Identity/location/performance APIs map directly to regulated vertical needs (e.g., fraud and verification).[26]

3

AI-native customer engagement

Customer engagement is transitioning from channel execution to real-time decisioning. As interactions become more dynamic and regulated, value shifts toward AI-driven orchestration, interoperable data signals, and automation of trust and compliance. In AI-native engagement models, intelligence determines not only how messages are delivered, but when, where, and whether engagement should occur at all.

AI-driven orchestration replaces channel-led engagement

Transactions move directly into messaging interfaces

AI-driven orchestration replaces channel-led engagement

Enterprises managing multiple engagement channels are increasingly constrained by fragmented decision-making and delayed responses. As customer intent becomes more time-sensitive, decision latency is emerging as a hidden cost, reducing resolution rates and inflating service workloads. By 2026, organizations are shifting toward AI-driven orchestration to determine when, where, and how to engage customers across messaging, voice, and digital touchpoints. Enterprises using AI-led orchestration report improvements of up to 35 percent in first-contact resolution, driven by better intent recognition and contextual decisioning.

What's changing
From channel-by-channel execution and rules → to AI-driven orchestration that decides when/where/how to engage across messaging, voice, and digital touchpoints.

Implication
"Decision latency" becomes a measurable cost; orchestration reduces over-communication and improves relevance using behavior, context, and risk signals.

Why this matters
As intent becomes time-sensitive, delayed responses reduce resolution and inflate service workloads; privacy expectations and complexity punish blunt automation.

The problem it solves
Timely, context-aware engagement at scale, higher resolution with fewer messages, less complexity, and better customer outcomes.

> "When conversations remain within the channels customers trust, problems are resolved faster, and the experience feels effortless."

Rajdip Gupta
Managing Director
Route Mobile

Key insights

Enterprises using AI-led orchestration report up to **35% improvement in first-contact resolution**.[27]

Engagement effectiveness depends on **coordination**, not channel volume.[28]

Orchestration reduces complexity while improving outcomes.[29]

Reducing decision latency improves resolution + relevance.[30]

Transactions move directly into messaging interfaces

Customer journeys increasingly break down when decisions and actions are delayed by redirects to apps or websites for authentication, payments, or issue resolution. As a result, enterprises are rethinking messaging not just as a communication channel, but as a transactional interface that reduces decision latency at critical moments. By 2026, rich messaging will increasingly support payments, identity verification, consent capture, and service resolution directly within the conversation. Interactive messaging drives engagement rates two to three times higher than static notifications while significantly reducing journey friction.

What's changing
From messaging as notifications + redirects to apps/sites → to messaging as a transaction interface (payments, identity verification, consent capture, service resolution) inside the conversation.

Implication
Journeys shorten; intent decay drops because decisions happen at the moment of attention—without app installs or context switching.

Why this matters
Redirects break journeys when authentication or payment is required; time-to-action becomes a competitive variable.

The problem it solves
A lightweight transaction layer that balances speed, trust, and scale as carrier interoperability improves, especially during high-volume "consumer moments."

> "When transactions stay in the conversation, journeys shrink, intent holds, and value converts faster."

Rajdip Gupta
Managing Director
Route Mobile

Key insights

- Interactive messaging drives **2–3× higher engagement** than static notifications.[31]
- Transactions in-message reduce journey friction and shorten decision cycles.[32]
- Messaging becomes a functional interface—not just a channel.[33]
- Security + consent must be embedded by design.[34]

4

Future-proof compliance by design for advanced digital interactions

Future-proof compliance by design will enable advanced digital interactions

Provenance verification emerges as a core compliance obligation in enterprise communications

Network-level AI fraud defence becomes a telco compliance mandate

Cross-border compliance becomes a structural design constraint

Future-proof compliance by design will enable advanced digital interactions

Digital interactions are no longer governed solely by technology standards—they are shaped by **geopolitics, regulation, and trust frameworks that differ by region**. As data flows, communications, and digital identities cross borders, organizations must operate within **fragmented regulatory environments** that impose conflicting rules on data usage, traceability, and accountability.

What's changing
From governance as "compliance after launch" → to governance embedded inside interactions as geopolitics, regulation, and trust frameworks diverge by region.

Implication
Cross-border digital experiences require a governance fabric: data usage, traceability, and accountability engineered into systems, not bolted on.

Why this matters
Identities, communications, and data now cross jurisdictions with numerous new and sometimes conflicting rules, increasing exposure and slowing innovation.

The problem it solves
Enables scale without regulatory whiplash by building enforceable trust: cross-border compliance, provenance, and network-level fraud enforcement.

> ""As regulation fragments across borders, future-proof governance processes becomes the hidden enabler of compliant digital interactions built directly into messaging and customer data."

Anne-Valérie Heuschen
Chief Corporate Affairs
Proximus Global

Key insights

Digital interactions are shaped by **geopolitics + regulation**, not just technology standards. [35]

Three governance forces: **cross-border compliance, communication origination and termination, network-level AI fraud defense.**.[36]

Future-ready governane embeds compliance directly into interactions..[37]

Provenance verification emerges as a core compliance obligation in enterprise communications

Communication provenance is shifting from an optional fraud-control measure to a regulatory requirement across major markets. Governments are moving from post-fraud detection to preventive traceability, making verified origin and auditable communication paths mandatory for enterprises operating at scale.

What's changing
From provenance as optional fraud control → to provenance as a regulatory requirement: verified origin + auditable communication paths.

Implication
"License to operate" shifts to providers that can prove who communicated, through which network, and with what authorization.

Why this matters
If origin and routing cannot be verified, delivery becomes a regulatory and reputational risk.

The problem it solves
A provenance-ready stack (identity, network, device/channel, audit layers) reduces fraud exposure and enables faster audits and higher deliverability.

> "Provenance is now a regulatory requirement and the license to operate in cross-border messaging."

Anne-Valérie Heuschen
Chief Corporate Affairs
Proximus Global

Key insights

- Third party voice party providers mandated to have their STIR/SHAKEN tokens for US traffic by **Sept 2025**. [38]
- EU: DSA Article 30 drives trader traceability (KYBC), verification obligations, audit-ready retention.[39]
- India: Internet Telephony KYC (2025) mandates full KYC for VoIP using mobile numbering.[40]
- Principle: "If you can't verify origin + route, you shouldn't deliver it."[41]
- End-to-end provenance requires layered verification, not point solutions.[42]

Network-level AI fraud defence becomes a telco compliance mandate

AI has industrialized fraud. Deepfake voices, synthetic identities, and AI-scripted phishing are scaling faster than traditional detection, prompting regulators to expect preemptive fraud control at the network level rather than after-the-fact remediation.

What's changing
From post-delivery fraud detection and content-only filtering → to real-time, network-level AI fraud defense that blocks threats before delivery.

Implication
Carriers are no longer neutral pipes; they become enforcement layers, expected to stop fraud "at carrier speed" across networks.

Why this matters
AI scales deepfakes, synthetic identities, and phishing faster than traditional controls; fragmented defenses increase false positives and delivery loss.

The problem it solves
Cross-signal, network-native intelligence that detects abnormal behavior early, reducing regulatory penalties, financial losses, and customer harm.

> "Compliance now demands network-level interception of fraud, including AI-driven threats, before delivery.

Anne-Valérie Heuschen
Chief Corporate Affairs
Proximus Global

Key insights

- AI-powered fraud losses projected to reach **$40B in the US by 2027** (from $12.3B in 2023).[43]
- **53%** of carriers report surging spam/robocalls/ phishing traffic.[44]
- **69%** rank fraud as the #1 industry priority as unwanted traffic overwhelms networks.[45]
- Compliance question shifts to: "Can you stop it before delivery globally?"[46]
- Fraud defense moves to behavioral + network anomaly detection.[47]

Cross-border compliance becomes a structural design constraint

Enterprises operating across multiple regions are increasingly challenged by conflicting identity, data, and messaging regulations. GDPR in Europe, China's Cybersecurity Law, India's data localization rules, and diverse US state privacy laws create operational complexity, slow decision-making, and increase compliance costs by up to 30 percent. Organizations that cannot harmonize cross-border processes risk regulatory penalties, disrupted customer engagement, and fragmented IT investments.

What's changing
From "build once, comply later" → to compliance-aware architectures as a structural constraint across identity, data, and messaging.

Implication
Enterprises need normalized trust and routing across a variety of potentially conflicting data and communication regulations—cross-border identity verification, global data compliance frameworks, multi-region orchestration, unified governance.

Why this matters
Conflicting regulations across various applicable jurisdictions (GDPR, China cybersecurity law, India DPD rules, diverse US state privacy laws) raise cost and complicate decision-making.

The problem it solves
Harmonizes operations and reduces risk by designing for interoperability and measurable efficiency gains, rather than one-off regional patches.

"Advanced digital interactions only scale when compliance is designed in across borders."

Anne-Valérie Heuschen
Chief Corporate Affairs
Proximus Global

Key insights

- Regulatory fragmentation is **structural, not temporary**.[48]
- Cross-border compliance can increase costs by **up to 30%**.[49]
- Enterprises need harmonized identity verification + data routing + messaging compliance.[50]
- Interoperability and compliance-aware architectures create a global governance fabric.[51]
- Prioritize capabilities that deliver measurable operational efficiency and reduce cross-border risk.[52]

5

Unified platforms beyond big tech

As digital ecosystems consolidate, enterprises are reassessing their dependence on large platform providers. This cluster reflects a broader shift toward regaining control over customer data, workflows, and regulatory alignment while still operating at global scale.

Regulated industries drive the shift toward vertical messaging platforms

Data sovereignty emerges as a core governance requirement

Regulated industries drive the shift toward vertical messaging platforms

By 2026, enterprises will increasingly adopt vertical-focused messaging designed around industry-specific workflows and regulatory requirements. Generic platforms struggle to scale in regulated environments where compliance, auditability, and identity assurance are as critical as engagement. More than 60 percent of organizations in regulated industries report that regulatory complexity slows or limits digital customer interaction initiatives.

What's changing
From generic messaging platforms → to vertical-focused messaging built around industry workflows + regulatory requirements.

Implication
Messaging becomes "compliance-native"—identity assurance, auditability, and traceability embedded directly into communication flows.

Why this matters
Regulatory complexity slows or limits digital interaction initiatives in regulated industries; scaling requires specialization, not one-size-fits-all tooling.

The problem it solves
Faster deployment and safer scale for financial services, healthcare, government, logistics, utilities—where verified access and auditable messaging are non-negotiable.

> "Compliance in workflows transforms messaging into a trusted, scalable business enabler."

Yaunese Aazibou
Chief Technology Officer
Proximus Global

Key insights

- **60%**+ of regulated orgs say regulatory complexity slows/limits digital customer interaction initiatives.[53]
- Financial services: identity verification + SIM-swap intelligence + real-time risk signals become foundational.[54]
- Healthcare: verified access + audit-ready communications accelerate with telehealth growth.[55]
- Utilities/logistics/government: proactive, identity-verified, auditable messaging reduces service load and meets cross-border commitments.[56]
- Strategic: compliance embedded into workflows reduces deployment friction.[57]

Data sovereignty emerges as a core governance requirement

Enterprises are increasingly losing direct control over customer data and relationships as Big Tech platforms consolidate identity, payments, and engagement into closed, full-stack ecosystems. While these platforms offer speed and convenience, they create long-term dependency and limit enterprise autonomy over customer interactions and data. As a result, data sovereignty has become a strategic priority, with over 70 percent of global enterprises identifying it as a critical factor in vendor selection by 2026.

What's changing
From relying on closed platform ecosystems for identity/payments/engagement → to architectures that preserve enterprise customer ownership and data sovereignty.

Implication
Vendor selection shifts toward interoperability, controllable data flows, and reduced dependency risk—especially as multi-platform fragmentation raises operating cost and reduces personalization.

Why this matters
Convenience creates long-term dependency and weakens autonomy over customer interactions and data.

The problem it solves
Enables scale without surrendering control—through interoperable identity frameworks and platform independence that reduces strategic lock-in.

> "Data sovereignty is a critical differentiator for secure, scalable, and strategic digital interactions."

Yaunese Aazibou
Chief Technology Officer
Proximus Global

Key insights

- Data sovereignty becomes a critical vendor-selection factor for 70%+ of global enterprises by 2026.[58]
- Europe: regulated digital identity frameworks expected to underpin the majority of identity interactions by 2027 (reinforcing interoperability/control).[59]
- Multi-platform dependency increases fragmentation, operational cost, and reduces personalization effectiveness.[60]
- Customer data ownership becomes a competitive differentiator.[61]
- Platform independence reduces long-term strategic risk.[62]

Final word

In today's digital landscape, businesses face unprecedented complexity as customer interactions, identities, and data flow across borders with differing regulations. Future-proof underpins trust and enables advanced digital interactions. Enterprises that embed trust, provenance, and fraud prevention into the architecture of their communications can scale with confidence and protect their customers across markets.

For enterprises today, it is about more than reaching audiences. It is about orchestrating experiences that are secure, transparent, and meaningful. Customers expect interactions that are timely, relevant, and trustworthy, and organizations must ensure that every message, identity verification, and data transaction meets local expectations. This is where thoughtful governance quietly enables better customer experiences rather than constraining them.

AI is a critical enabler in this environment. When applied responsibly, it helps identify anomalies, detect fraudulent activity in real time, and personalize communications at scale, all without compromising trust. By combining intelligence with governance by design, brands can create experiences that are both innovative and trustworthy.

Ultimately, the future of digital engagement is built on the convergence of trust, intelligence, and meaningful customer experiences. Companies that design interactions with governance in mind, leverage AI responsibly, and prioritize customer-centric transparency will build loyalty and drive long-term growth in a fast-evolving landscape.

Valentine Gabriel
Chief Strategy & Transformation Officer
Proximus Global

Sources Summary

- Sources referenced here represent mutually independent, authoritative research and regulatory bodies spanning analyst firms, standards organizations, government agencies, academic institutions, and industry consortiums.
- Repetition across endnotes reflects intentional corroboration of key findings across distinct sources, not reliance on a single viewpoint or dataset.

Authoritative Sources Referenced (2024–2026)

- Thales: Consumer Digital Trust Index 2025
- Imperva: Bad Bot Report 2025
- FIDO Alliance: World Passkey Day 2025
- Mastercard: Insights from the Frontlines of Cybercrime 2025
- Fortune Business Insights: Voice Biometrics Market 2025
- Fortune Business Insights: Augmented Reality Market 2025
- Gartner: Contact Center Authentication Trends 2025
- Gartner: AI in Customer Experience 2025
- Gartner: GenAI Forecast 2024
- Mobile Broadband Index (MBiT): Report 2025
- Firecell: Edge Computing Latency Study 2026
- The Business Research Company: Edge Computing Global Market Report 2025
- Mobilise Global: eSIM & Connectivity Market Analysis 2025
- Kaleido Intelligence: Connectivity & Messaging Forecasts 2025
- Juniper Research: Conversational Commerce 2025
- STL Partners: Network API Forecast 2025
- GSMA: Rich Messaging Evolution 2025
- International Journal of Research in Computer Applications and Information Technology: 2025
- McKinsey: Personalization and AI Engagement 2025
- McKinsey: Risk and Resilience 2025
- McKinsey: Personalized Marketing Trends 2025
- McKinsey: CIO Insights 2025
- Encryption Consulting: Compliance Trends 2025

End Notes

1. Thales Consumer Digital Trust Index 2025
2. Thales Consumer Digital Trust Index 2025
3. Thales Consumer Digital Trust Index 2025
4. Imperva Bad Bot Report 2025
5. FIDO Alliance World Passkey Day 2025
6. FIDO Alliance World Passkey Day 2025
7. FIDO Alliance World Passkey Day 2025
8. FIDO Alliance World Passkey Day 2025
9. Mastercard Insights from the Frontlines of Cybercrime 2025
10. Fortune Business Insights Voice Biometrics Market 2025
11. Gartner Contact Center Authentication Trends 2025
12. Gartner Contact Center Authentication Trends 2025
13. Fortune Business Insights Voice Biometrics Market 2025
14. Mobile Brandband Index (MBiT) Report 2025
15. Fortune Business Insights Augmented Reality Market 2025
16. Firecell Edge Computing Latency Study 2026
17. The Business Research Company Edge Computing Global Market Report 2025
18. Mobilise Global 2025
19. Kaleido Intelligence 2025
20. Mobilise Global 2025
21. Kaleido Intelligence 2025
22. Juniper Research 2025
23. STL Partners Network API Forecast 2025
24. STL Partners Network API Forecast 2025
25. STL Partners Network API Forecast 2025
26. STL Partners Network API Forecast 2025
27. International Journal of Research In Computer Applications and
28. McKinsey CIO Insights 2025
29. McKinsey Personalization and AI Engagement 2025
30. Gartner AI in Customer Experience 2025
31. Gartner AI in Customer Experience 2025
32. Juniper Research Conversational Commerce 2025
33. Juniper Research Conversational Commerce 2025
34. GSMA Rich Messaging Evolution 2025
35. GSMA Rich Messaging Evolution 2025
36. Encryption Consulting Compliance Trends 2025
37. Encryption Consulting Compliance Trends 2025
38. Encryption Consulting Compliance Trends 2025
39. Federal Communications Commission 2025
40. Article 30 Digital Services Act EU 2025
41. GlobalValidity India KYC Compliance 2025
42. Joint Study US National Security Agency (NSA), Austalian Signals
43. Directorate's Australian Cyber Security Centre (ASD's ACSC), Canadian
44. Centre for Cyber Security (CCCS), and United Kingdom National Cyber
45. Security Centre (NCSC-UK) 2025
46. Identiverse 2025
47. ID Tech Wire 2025
48. Tech Economy 2025
49. Tech Economy 2025
50. Federal Communications Commission Call Branding Fact Sheet 2025
51. Dataminr Cyberthreat Defense Report 2025
52. Oxford Insights Geopolitics of Data Governance 2025
53. OpenBorder 2025
54. McKinsey Risk and Resilience 2025
55. McKinsey Risk and Resilience 2025
56. McKinsey Risk and Resilience 2025
57. PwC Global Compliance Survey 2025
58. Smarsh Compliance Survey 2025
59. KLAS Research Digital Health National Trends 2025
60. PwC Global Compliance Survey 2025
61. PwC Global Compliance Survey 2025
62. Gartner GenAI Forecast 2024

Proximus Global, combining the strengths of Telesign, BICS, and Route Mobile, is transforming the future of communications and digital identity. Together, our solutions fuel innovation across the world's largest companies and emerging brands. Our unrivaled global reach empowers businesses to create engaging experiences with built-in fraud protection across the entire customer lifecycle. Our comprehensive suite of solutions – from our super network for voice, messaging, and data, to 5G and IoT; and from verification and intelligence to CPaaS for personalized omnichannel engagement – enables businesses and communities to thrive. Reaching over 5 billion subscribers, securing more than 180 billion transactions annually, and connecting 1,000+ destinations, we honor our commitment to connect, protect and engage everyone, everywhere.

Learn more at **proximusglobal.com**

proximus
Global