Valid

Quality of Service

From Connectivity Monitoring to Intelligent Connectivity Management

Valid

ABOUT VALID

Valid is your trusted partner for interoperable mobile and IoT connectivity services worldwide. We excel in offering solutions for identity, mobile, and payment ecosystems, driving digital transformation in people's lives by supporting various journeys, including authentications, monetization, and transactions, in both public and private sectors.

With nearly seven decades of expertise in the market, we deliver complex solutions involving high volume and sensitive data. The company integrates the best available technologies to drive innovation and provide secure, efficient solutions to its clients. Currently, Valid has more than 3,000 employees across 15 countries dedicated to creating a more fluid, connected, reliable and safe world.

FIND OUT MORE ABOUT US AT:

Valid.com | trustedconnectivity.valid.com

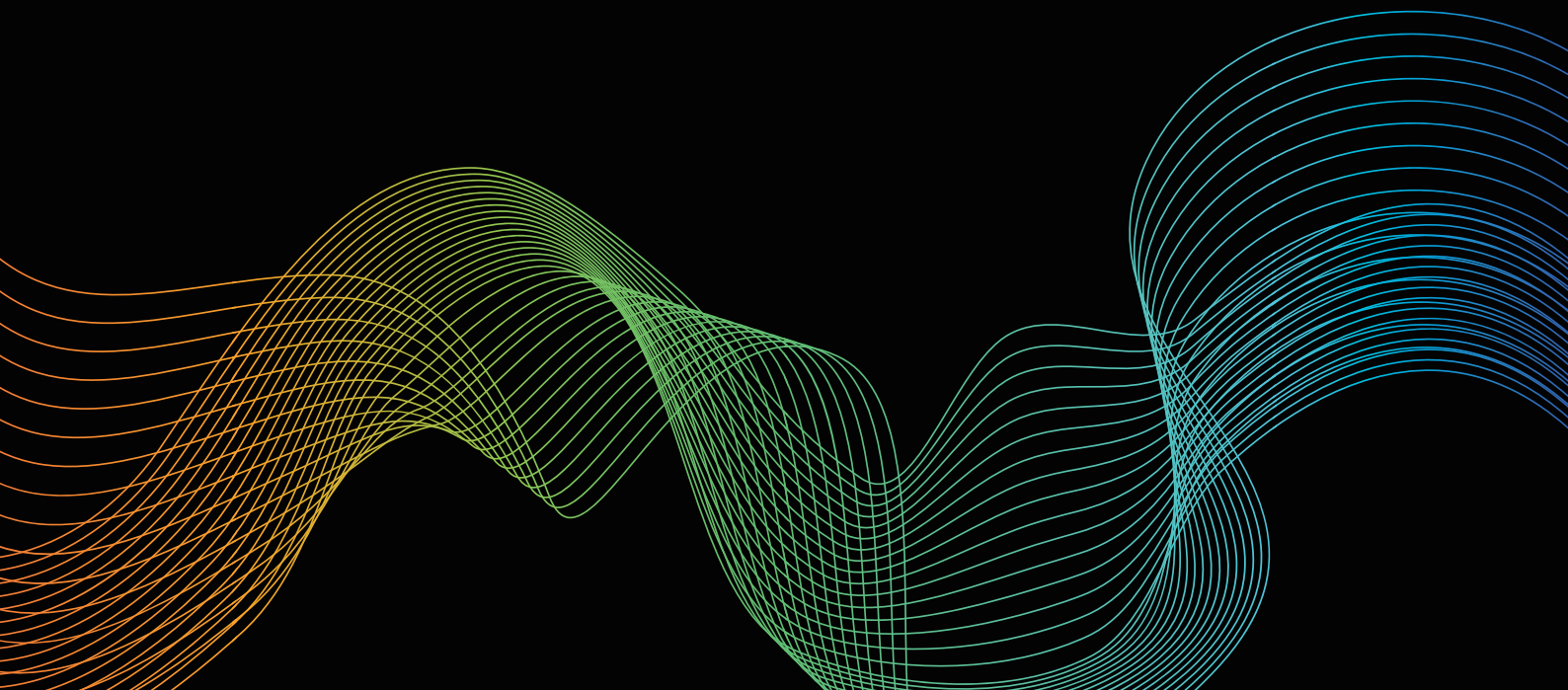
FOLLOW US ON SOCIAL MEDIA:

LinkedIn | Facebook | Instagram

AUTHOR(S):

Christian Fernandez – IoT Product Manager at Valid

Caio Hamer – Marketing Director at Valid



Executive summary

A device can be connected and still fail to deliver the service that depends on it.

This paper examines why **connectivity availability has become an insufficient operational measure,** what changes when performance can be compared objectively across networks and regions, and what becomes possible once that **intelligence is allowed to act.**

Connected vehicles, industrial equipment, logistics assets, payment terminals and travel eSIM users all operate across changing coverage areas, mobile operators and roaming environments. Signal conditions vary by location. Networks congest. Roaming relationships change. **Connectivity management tools** designed to answer whether a device is online **will continue to report that device as connected while it experiences weak signal quality,** rising latency, reduced throughput or repeated loss of session continuity.

Connectivity exists. **The service still degrades.**

For the organizations operating those devices, the **consequences are practical** rather than theoretical. Technicians are dispatched to devices that were never faulty.

Connectivity providers are selected and renewed without objective evidence of how they perform in the regions that matter most. Performance that declined gradually over several weeks is discovered only when a customer reports a problem. A device that lost its data session overnight is found still offline the following week.

At the same time, the connectivity underneath these deployments is becoming more changeable. GSMA SGP.32 allows IoT organizations to **manage profiles and change connectivity remotely** across large device populations, throughout deployments that may last a decade or more. That flexibility is valuable, but it raises a question availability data alone cannot answer: **which connectivity option actually performs best** for this service, in this region, on this device?

Quality of Service (QoS) addresses that question. It **measures connectivity performance** in real time from the device itself, covering latency, jitter, signal strength and quality, throughput, connection and data availability, and connectivity drop and failure rates, and **combines them into a connectivity experience score** that can be compared across operators, technologies and geographies.

Measurement is only half of it. Where an organization's own business rules allow, the same intelligence can act on what it finds: **re-establishing a session on a device that has dropped offline,** holding devices on a preferred network while quality permits, or moving a device to an alternative network when measured quality falls below a defined threshold.

This whitepaper examines why connectivity availability has become an insufficient operational measure, what changes when performance can be compared objectively across networks and regions, and what becomes possible when **measurement and connectivity control operate as a single mechanism.**

1. The New Connectivity Reality

Connected devices are no longer confined to a single location or a single mobile network.

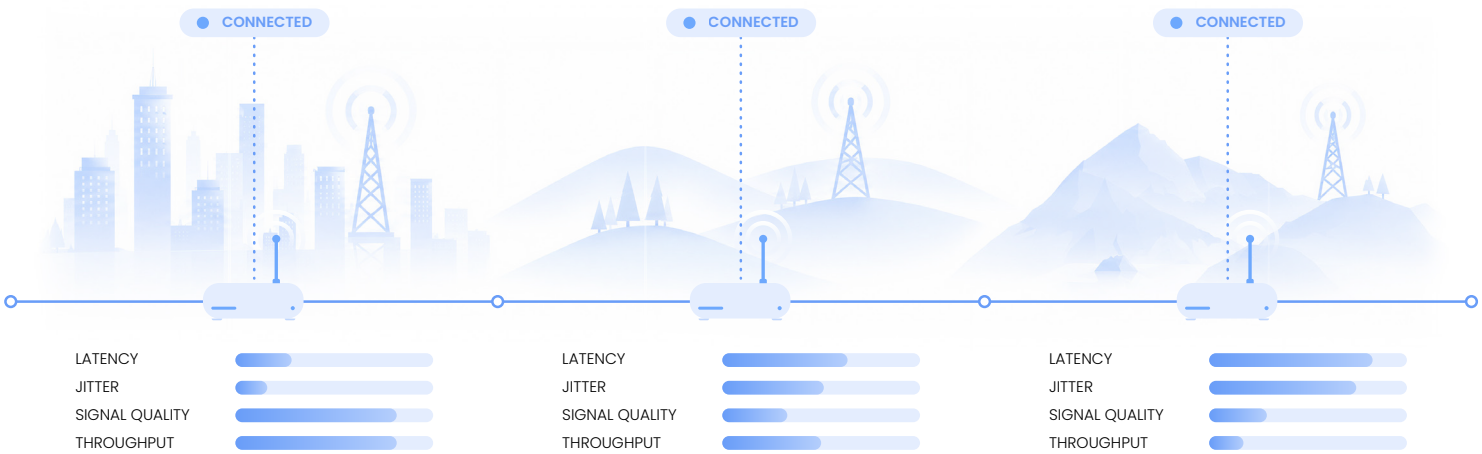
Vehicles cross regions and borders. Logistics assets move between coverage areas over the course of a single journey. Industrial equipment operates under radio conditions that vary by site and by season. Travelers expect service to work on arrival, without configuration. **Even permanently fixed deployments encounter changing conditions as networks are re-planned,** as spectrum is refarmed, as older radio technologies are switched off and as roaming agreements are renegotiated.

A device may encounter different operators, **radio technologies and coverage conditions over its operating life.** Reporting all of it as "connected" hides what matters.

Over its operating life, a single device may therefore encounter different mobile operators, different radio technologies, different coverage conditions and different commercial arrangements. This creates a **category of operational complexity** that did not exist when a device connected to one network, in one market, for its entire lifetime.

Maintaining connectivity is no longer the whole requirement. The requirement is that **connectivity consistently delivers the performance** each service actually needs.

Those needs are not equivalent. A payment terminal depends on predictable response times and cannot tolerate an authorization that times out. A telematics platform depends on continuity, because gaps in the data are gaps in the record. A smart meter can tolerate delay but is deployed where a site visit is expensive. **Reporting all three as simply "connected" hides the difference between them.**



The status does not change. The service does.

2. The Cost of Connectivity Blind Spots

As deployments scale across regions, operators and radio technologies, **the gap widens between what organizations can see and what they need to know. Four consequences appear** repeatedly:

Deployment complexity that grows faster than the deployment

Rolling devices out across multiple countries and network environments requires coordination between suppliers, connectivity providers and internal teams. Without comparable performance data from each market, **every new market is approached as an unknown,** and lessons learned in one country do not transfer to the next.

Connectivity and hardware decisions made without evidence

Regional operator requirements often **push manufacturers toward multiple hardware or connectivity configurations.** When there is no objective view of how each option performs once deployed, those decisions rest on commercial terms and published coverage maps rather than on measured behavior in the field.

Field interventions that could have been avoided

When a connectivity problem cannot be diagnosed remotely, the default response is to send someone. Across a large or geographically dispersed fleet, that response is slow and expensive, and a **significant proportion of those visits are made to devices that turn out to be working correctly,** or that would have recovered had anything prompted them to.

Degradation discovered too late

Connectivity performance rarely fails outright. It declines. Without continuous measurement, the **decline stays invisible until it crosses the threshold at which users notice,** which is also the point at which it has already affected the business.

The underlying issue is not that connectivity fails. It is that **organizations cannot explain why quality changes,** where degradation concentrates, how often it recurs, or what it is costing them.

Connectivity performance rarely fails outright.

It **declines.**

3. The Questions Status Data Cannot Answer

Traditional connectivity management platforms were built to report device state: connected or not, data consumed, session established. That was adequate when devices were static and served by a single network throughout their life.

It is no longer adequate. As devices operate across multiple operators, countries and roaming environments, state tells operational teams that something is happening. **It does not tell them whether it is happening well.**

The questions organizations now need answered are comparative:

01 Which mobile operators consistently deliver the service quality this application requires?

02 How does performance differ between the regions where devices are deployed?

03 Where are degradations concentrated, and are they getting worse?

04 Which roaming partners produce the best customer experience, measured rather than promised?

05 Is the connectivity strategy chosen two years ago still the right one today?

None of these can be answered from status data. They require measurement over time, across networks, under real operating conditions.

That is the **distinction between monitoring and intelligence.** Monitoring reports a state. Intelligence explains a behavior and supports a decision.

Monitoring reports a state. **Intelligence explains a behavior** and supports a decision.

4. How Quality of Service Works

Valid's Quality of Service solution measures connectivity performance from the device outward, through a lightweight agent that can sit in the SIM or eUICC, in the device operating system, or within an application, depending on what the deployment allows.

The indicators collected include latency, jitter, signal strength and signal quality, downlink and uplink throughput, connection availability, data availability and data performance, and connectivity drop and failure rates. These are combined into a **connectivity experience score,** giving operational teams a **single comparable measure** alongside the underlying detail.

330B+ MEASUREMENTS

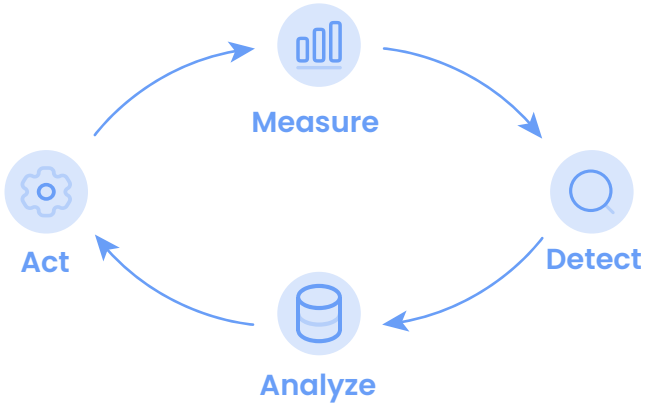
500+ NETWORKS

150+ COUNTRIES

6,500+ DEVICE TYPES

Measurement is real time. How often it runs, and what prompts it, is **configurable to the deployment:** on a defined schedule, on loss of service, on a voice call, on a change of location, or as part of a structured drive test. A vehicle fleet and a static meter population do not need to be measured the same way.

Measurements are aggregated in anonymized form across deployed devices, which **allows performance to be compared** across operators, radio technologies and geographic regions rather than assessed one device at a time. The platform underlying Valid's Quality of Service solution has accumulated more than 330 billion measurements, spanning over 500 networks in more than 150 countries and over 6,500 device types. **That accumulated baseline is what makes comparison meaningful:** a latency figure is only useful once it can be set against what is normal for that network, in that country, on that class of device.



- **Measure.** Connectivity quality **indicators are collected continuously** across devices, networks and regions, establishing a performance baseline under real operating conditions.
- **Detect.** Anomalies, degradation and changes in connectivity behavior are **identified as they emerge,** rather than after they are reported.
- **Analyze.** Performance is compared across operators, regions and roaming environments, **allowing connectivity to be benchmarked** on measured evidence.
- **Act.** Results are presented through operational dashboards, and, where business rules define it, **used to trigger a connectivity change** automatically.

5. What QoS Measures, and What It Does Not

Credibility in connectivity performance depends on being precise about where the data comes from.

QoS measures connectivity as the device experiences it. It reflects the conditions a specific device encounters on a specific network in a specific place: how strong the signal is, how long the network takes to respond, whether sessions hold.

It does not operate the radio access network, and it is not a replacement for the network performance management systems mobile operators use to run their own infrastructure. **Valid provides the technology and intelligence used to manage and evaluate connectivity.** It does not provide the underlying mobile connectivity itself.

That boundary is what makes the data useful. Because measurement is taken from the device side and is independent of any single network, **performance can be compared across operators and roaming partners on consistent terms.** Network-side reporting describes one network, measured its own way. **QoS describes what the deployed fleet actually experienced,** wherever it happened to be.

This is also why the s**ame data serves organizations on both sides of a connectivity contract.** An enterprise uses it to understand the service it is receiving. A mobile operator uses it to understand the service its subscribers are receiving, which is not always what network-side counters suggest.

Network-side reporting describes one network. **QoS describes what the fleet actually experienced.**

6. From Measurement to Action

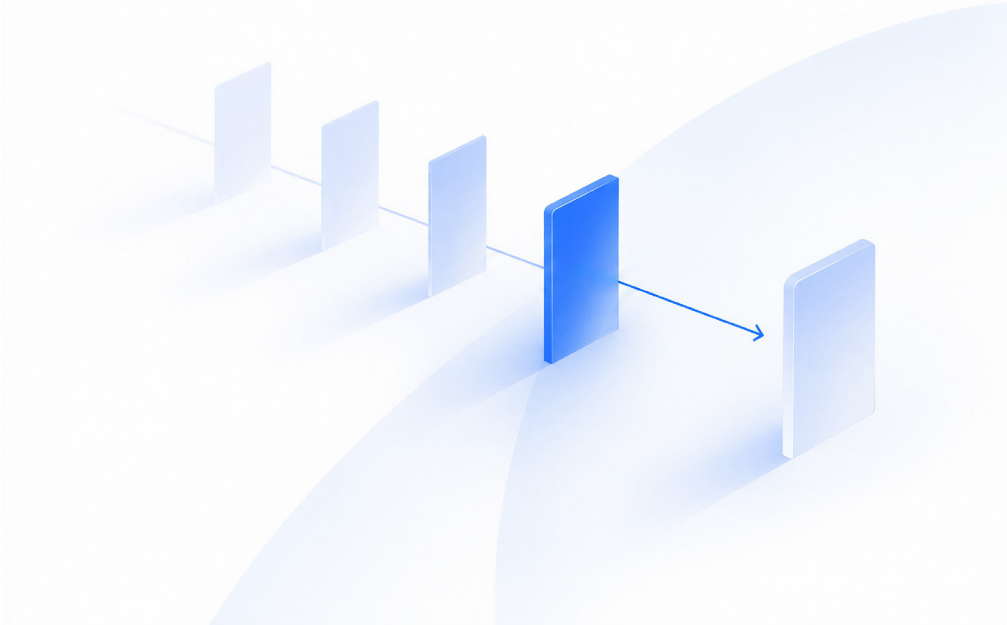
> **Measurement that produces only a report leaves the hardest part to somebody else.**

Once connectivity performance is understood in real time, the same intelligence can be used to do something about it. **Valid's Quality of Service solution supports policy-driven connectivity control,** in which a measured condition triggers a defined response.

The most common case is also the least contentious. A **device loses its data session** through congestion, a failed handover or a session timeout, **and does not recover on its own.** Static devices are particularly exposed to this, and can remain in that state for hours or days before anyone notices. **QoS can detect the condition and re-establish the connection automatically,** on the same network, with nobody dispatched and no ticket raised.

Beyond recovery, **policies can be defined** to hold devices on a preferred or home network for as long as quality permits, to return a device to that network once conditions recover, to move a device to an alternative network when measured quality falls below a defined threshold, or to move traffic from cellular to an approved Wi-Fi network where that is appropriate. On eUICC-based devices, the same logic can trigger a profile switch, which **connects connectivity quality directly to the remote provisioning mechanisms** discussed later in this paper.

These are business rules, not autonomous behavior. **Nothing moves unless somebody has written a rule** that says it should.



Who sets the rules matters

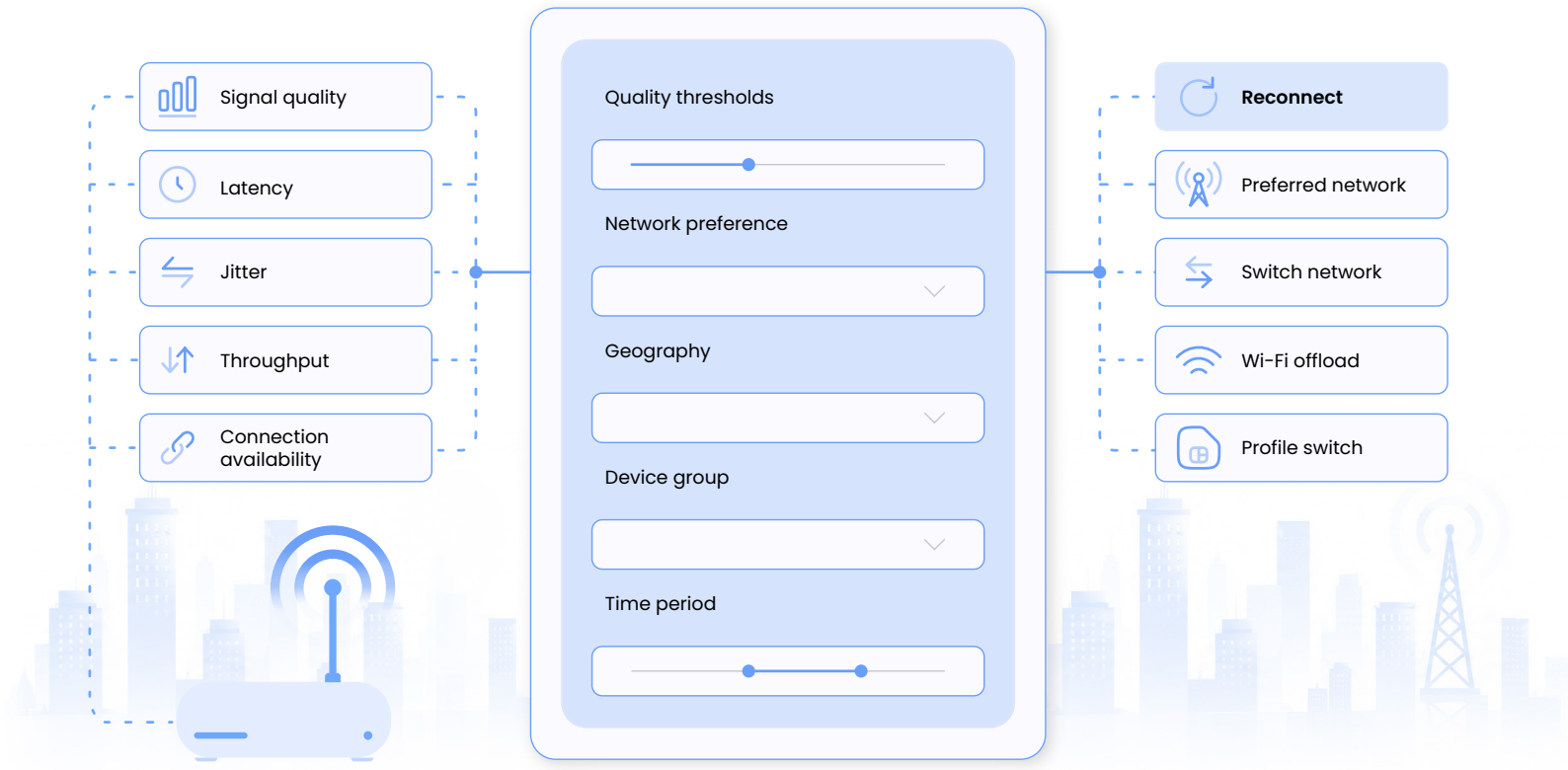
These are business rules, not autonomous behavior. The **organization deploying QoS defines** the quality thresholds, the network preferences, the geographies and time periods they apply in, and the device groups they apply to. Nothing moves unless somebody has written a rule that says it should.

That organization is as often a connectivity provider as it is an enterprise, and **the rules each writes look quite different.**

For a mobile operator or connectivity provider, **policy-driven control is a means of protecting the subscriber relationship** rather than surrendering it: enforcing home and preferred network priority, returning roaming devices to the intended partner network, recovering failed sessions before they become support calls, and offloading to Wi-Fi where that reduces cost without reducing the quality delivered.

For an enterprise or IoT operator, the **same mechanism is a resilience measure.** Devices in the field stay in service, and stay in service without an engineer being sent to them.

The mechanism is identical in both cases. **What differs is the policy, and the policy belongs to the customer.**



7. A Single Operational View

> **Connectivity intelligence is only valuable when the people responsible for operations can reach it.**

As device populations grow, **operational and customer care teams increasingly work across several systems at once:** a connectivity management platform, one or more operator portals, internal ticketing and separate reporting tools. **Assembling a single picture from those sources takes time** that is not available while a service is degrading.

The Single Pane of Glass (SPoG) consolidates connectivity intelligence into one operational view. Connectivity quality across devices, mobile operators and geographic regions is presented in one place, alongside the diagnostic detail required to investigate an individual case, and alongside the policies currently in force.

The operational effect is direct. **Teams spend less time establishing what happened and more time deciding what to do about it.** Patterns that are invisible inside any single system, such as a degradation affecting one operator in one region across hundreds of devices, become visible once the data sits together.

Quality of Service is delivered through its own operational interface, distinct from Valid's Operator Support Portal, which serves the eSIM activation lifecycle. The two answer different operational questions. **The Operator Support Portal explains what happened during activation. Quality of Service explains how connectivity has performed since.** Organizations running both gain visibility across the full span, from the moment a device is provisioned to how it behaves years into deployment.

8. Key Capabilities

End-to-End Diagnostics.

Connectivity diagnostics spanning the device, the SIM/eSIM environment and the mobile network, so **investigation is not confined** to a single layer.

Real-Time Performance Monitoring.

Live visibility into connectivity quality across the deployed fleet, with measurement frequency and triggers configured to the deployment.

Proactive Alerting.

Preemptive alerts on emerging network trends, potential outages and performance degradation, **ahead of user-visible impact.**

Dynamic Benchmarking.

Objective comparison across operators, geographic regions and device categories **using anonymized operational data.**

Policy-Driven Connectivity Control.

Automated reconnection, preferred-network enforcement, network switching and Wi-Fi offload, executed against thresholds and **business rules defined by the customer.**

Architecture Agnostic.

Designed to support deployments operating **under GSMA SGP.22 and GSMA SGP.32.**

Single Pane of Glass.

Centralized operational dashboards **consolidating connectivity intelligence** in one view.

9. Operating Across Multiple Countries

Global deployments raise a problem that single-market deployments do not: comparability.

Operating in ten markets means working with different operators, different radio technology mixes, different regulatory conditions and different commercial arrangements. Without a consistent measurement framework across all of them, **each market reports its own version of performance,** and none of those versions can be compared with the others.

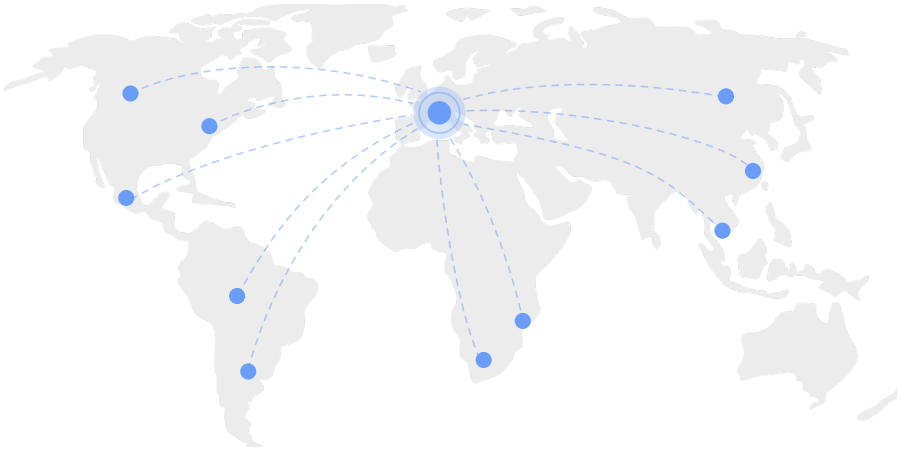
As organizations adopt SGP.32 to manage connectivity lifecycles across borders, the **ability to change connectivity remotely becomes real and repeatable.** The value of that ability depends on **knowing which change is worth making,** and on being able to make it consistently.

Connectivity intelligence supports organizations in:

- **Measuring connectivity performance** consistently across markets.
- **Adapting operations** to regional network conditions.
- **Standardizing operational processes,** thresholds and escalation paths across teams.
- **Benchmarking connectivity providers** on measured performance rather than commitments.
- **Applying the same connectivity policies** across a distributed base, with local variation where it is warranted.
- **Retaining visibility** across SGP.32-enabled deployments as connectivity changes.

The outcome is a **common operational framework:** the same indicators, the same thresholds and the same view, regardless of which market or which network a device is operating on.

SGP.32 makes changing connectivity possible. **Connectivity intelligence makes it decidable.**



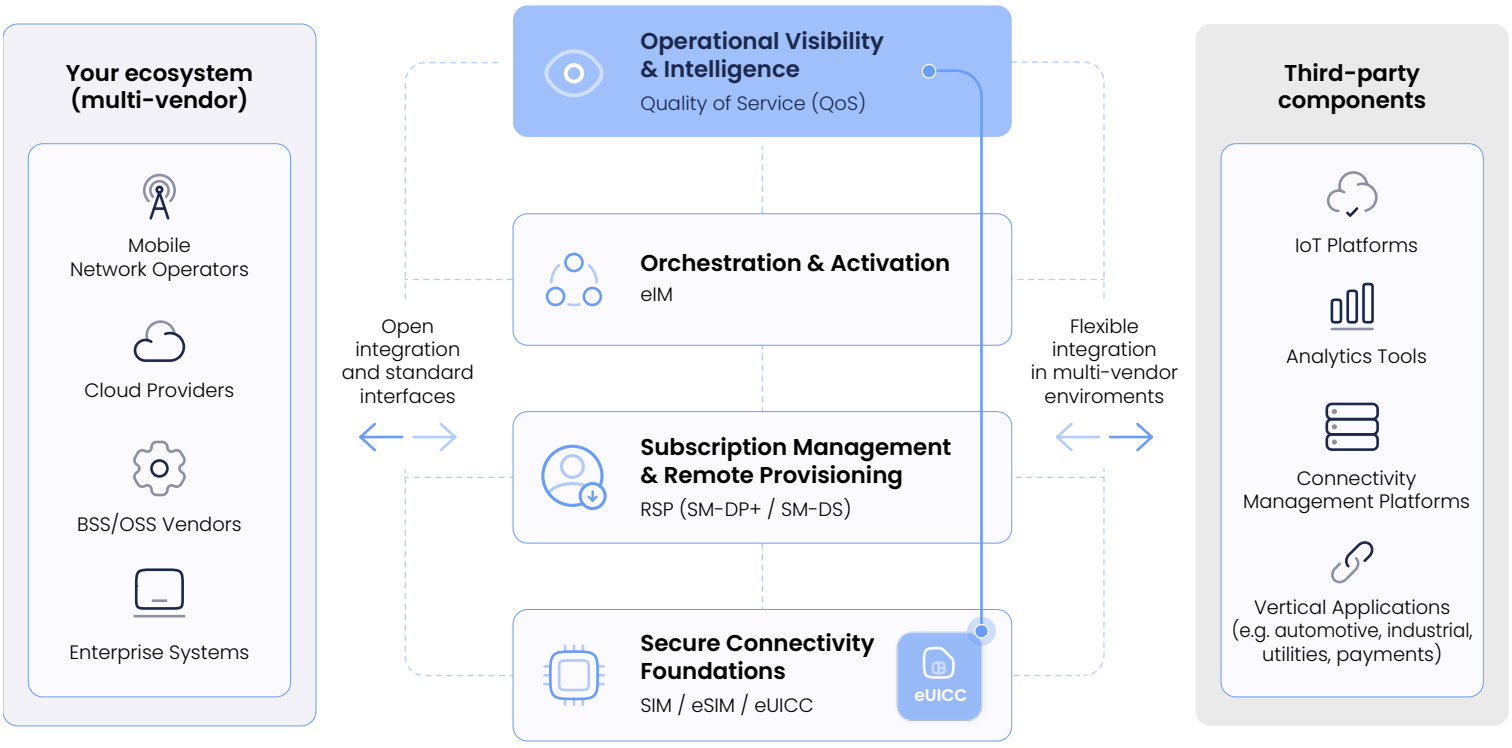
10. Connectivity Intelligence Across the Lifecycle

Connectivity quality is not a standalone concern. It becomes actionable when it **connects to the mechanisms capable of changing connectivity.**

Valid works across several layers of that lifecycle: the **secure foundations** that carry connectivity credentials, including SIM, eSIM and eUICC technologies; the **subscription management and remote provisioning infrastructure** that delivers and manages profiles under GSMA SGP.22 and SGP.32; **orchestration and activation capabilities;** and the **operational visibility layer** that supports the teams running these environments day to day.

Quality of Service belongs to that last layer, and the connection between the layers is concrete rather than conceptual. Because measurement can run within the SIM or eUICC itself, a connectivity quality threshold can trigger a profile switch on the same secure element that holds the profiles. **Measurement and provisioning can therefore operate as coordinated parts** of one connectivity management process, rather than as two systems that happen to be sold together.

Valid operates within multi-vendor environments rather than assuming a single-vendor architecture. Organizations already running provisioning, connectivity management or analytics platforms from other providers can adopt connectivity intelligence alongside them.



Interoperable • Flexible • Scalable • Ecosystem-ready

11. Where Connectivity Intelligence Is Applied

Connected Vehicles

A vehicle can cross several networks and two or three countries in a single day. **The connectivity it relies** on for telematics, emergency services, in-vehicle services and software updates **has to hold across all of them.**

- **Visibility into connectivity performance** across the deployed vehicle population.
- **Benchmarking** of operators and roaming partners **on measured performance.**
- **Scheduling of OTA campaigns** against known network conditions rather than assumed ones.
- **Automatic recovery** of vehicles that have lost connectivity, without a dealer visit.
- **Earlier identification of connectivity issues** affecting the in-vehicle experience.

Enterprise IoT

Large device fleets are frequently deployed where a site visit is expensive, slow, or both. **Every unnecessary intervention is a direct operational loss,** and every device sitting offline unnoticed is a service that is not being delivered.

- **Device-level visibility** into connectivity quality.
- **Automatic reconnection** of devices that have dropped offline.
- **Remote diagnosis** that reduces avoidable field interventions.
- **Higher service availability** across the deployed base.
- **Connectivity choices** grounded in observed performance.

Typical deployments include EV charging, smart metering, elevator monitoring, fleet management and asset tracking.

Travel eSIM Services

A travel eSIM provider's customer experience is delivered almost entirely by roaming partners it does not control. **Performance in the destination market** is the product.

- **Objective benchmarking** of roaming partner performance by market.
- **Visibility into customer connectivity** while the customer is still traveling.
- **Identification of regional performance** differences before they generate complaints.
- **Partner selection and renegotiation** supported by measured evidence.

Mobile Operators and Connectivity Providers

Enterprise and IoT customers are **increasingly measuring the performance** they receive rather than accepting it. That shift is happening whether or not their connectivity provider participates in it. **An operator holding device-level evidence** of its own performance **can enter that conversation** with data, commit to service levels it is able to prove, **and defend renewals on measured quality** rather than on price.

- **SLA monitoring and reporting** against measured, device-side performance.
- **Evidence for enterprise and IoT bids** that network-side counters alone cannot provide.
- **Faster root-cause analysis** for customer-reported issues, including confirmation that a reported fault does not originate in the network.
- **Home and preferred-network policy enforcement** across roaming and multi-network deployments.
- **Wi-Fi offload** where it reduces cost without reducing delivered quality.
- **Care teams working from connectivity evidence** rather than assumption.

12. Operational and Business Impact

> **Connectivity intelligence changes what operational teams are able to do, and those changes carry through to cost, reliability and commercial decisions.**

01 Faster issue resolution.

When degradation is detected and localized automatically, **investigation starts from evidence** rather than from a customer report, shortening the interval between a problem appearing and being addressed.

02 Fewer avoidable interventions.

Remote diagnosis reduces the proportion of field visits dispatched to devices that are functioning correctly, and **automated recovery** removes a category of intervention altogether.

03 Operational scalability.

A consistent measurement framework, a single operational view and policies that execute without manual involvement allow the **same team to support a larger deployed base.**

04 Better-informed connectivity decisions.

Operator selection, roaming partner strategy and market entry planning can be **based on measured performance** rather than on published coverage claims.

05 More reliable service delivery.

Identifying degradation before it becomes visible to users, and correcting some of it automatically, supports higher availability and a more consistent customer experience.

06 A defensible quality position.

For connectivity providers, **measured device-side evidence supports service level commitments** that can be demonstrated rather than asserted.

Conclusion

For most of this industry's history, **the operational question was whether a device could connect.** For a growing share of connected services that question has been answered, and a harder one has taken its place: **is the connection good enough for what the service is trying to do?**

The two are not the same. A device reporting a healthy connection can still be delivering a service that fails commercially. A payment that times out. An update that never completes. A telematics feed with gaps in it.

Quality of Service closes that gap by measuring connectivity as devices actually experience it, comparing performance across operators, regions and technologies, and presenting the result where operational teams can use it. Where the organization has defined the rules, it **also acts on what it finds, which turns a reporting layer into an operational one.**

As standards such as GSMA SGP.32 give organizations more control over connectivity throughout the device lifecycle, **that control is only as good as the information behind it.** Deciding to change a network is becoming straightforward. Knowing which change improves the service, and applying it consistently across a deployed base, is the harder problem, and it is the one connectivity intelligence exists to solve.

Connectivity enables communication.

Visibility enables control.

Connectivity intelligence enables better decisions.

See how connectivity intelligence applies to your deployment.

Click here to book a demo now...

... or simply scan the QR code!

Glossary

1. **Anomaly Detection:** The identification of connectivity behavior that deviates from an established performance baseline, used to surface degradation before it is reported by users.
2. **Benchmarking:** The comparison of connectivity performance across operators, regions, roaming partners or device categories using consistent, measured indicators.
3. **Connection Availability:** The proportion of time a device is successfully attached to a mobile network and able to use it.
4. **Connectivity Drop Rate:** The rate at which established data connections are lost, an indicator of session stability rather than of coverage.
5. **Connectivity Experience Score:** A composite measure combining individual connectivity indicators into a single comparable score, used to rank networks, regions or device groups.
6. **Connectivity Failure Rate:** The rate at which attempts to establish a data connection do not succeed.
7. **Connectivity Intelligence:** Operational insight derived from continuous measurement and analysis of connectivity performance, as distinct from reporting whether a device is connected.
8. **Data Availability:** The proportion of time a device attached to a network is able to transfer data successfully.
9. **eSIM (Embedded SIM):** A digital SIM embedded in a device, enabling remote provisioning and management of mobile subscriptions.
10. **eUICC:** The secure element that stores and manages one or more eSIM profiles and enables remote SIM provisioning.
11. **GSMA SGP.22:** GSMA specification defining the consumer eSIM Remote SIM Provisioning architecture.
12. **GSMA SGP.32:** GSMA specification defining eSIM Remote SIM Provisioning for IoT devices and large-scale deployments.
13. **Jitter:** Variation in the delay between successive data packets. High jitter degrades real-time services even when average latency is acceptable.
14. **Latency:** The time taken for data to travel between a device and its destination. A primary indicator for services that depend on responsiveness, such as payment authorization.
15. **MVNO (Mobile Virtual Network Operator):** An operator providing mobile services using another operator's network infrastructure.
16. **OTA (Over the Air):** Remote delivery of updates, configurations or management commands to deployed devices.
17. **Policy-Driven Connectivity Control:** The automated execution of connectivity changes, such as reconnection, network switching or Wi-Fi offload, against thresholds and business rules defined by the organization operating the devices.
18. **Quality of Service (QoS):** In this paper, the real-time measurement, analysis, benchmarking and rule-based control of connectivity performance across deployed devices, networks and regions.
19. **QoS Reconnect:** The automatic re-establishment of a data session on a device that has lost connectivity and has not recovered on its own.
20. **Roaming:** The use of a visited operator's network by a device whose subscription belongs to another operator, typically outside its home market.
21. **Root-Cause Analysis:** The process of determining the underlying source of a connectivity or service issue rather than addressing its visible symptom.

22. **RSP (Remote SIM Provisioning):** The GSMA-defined architecture enabling remote download and lifecycle management of eSIM profiles.
23. **Signal Quality:** Measured radio conditions experienced by a device, including signal strength and interference, which determine achievable performance.
24. **SLA (Service Level Agreement): A contractual commitment defining the service performance a provider undertakes to deliver.**
25. **SPoG (Single Pane of Glass): A unified operational interface consolidating visibility and diagnostics that would otherwise be distributed across multiple systems.**
26. **Throughput: The rate at which data is successfully transferred between a device and the network, measured on the downlink and the uplink.**
27. **Wi-Fi Offload: The controlled movement of device traffic from a cellular network to an approved Wi-Fi network, typically to reduce cost or improve local performance.**

References

GSMA SGP.22 – eSIM Consumer Technical Specification.

GSMA SGP.31 – eSIM IoT Architecture and Requirements.

GSMA SGP.32 – eSIM IoT Technical Specification.

Trusted Connectivity Alliance – eSIM interoperability and remote provisioning resources.

Valid – Operator Support Portal: Operational Visibility and Control in the eSIM Era.

Valid – From Entitlement to Orchestration in the eSIM Era.

Valid – Accelerating the IoT's Transition to eSIM.

Valid

Empowering the Future of Connectivity

LinkedIn
linkedin.com/company/valid-s-a-

YouTube
youtube.com/@Valid_SA