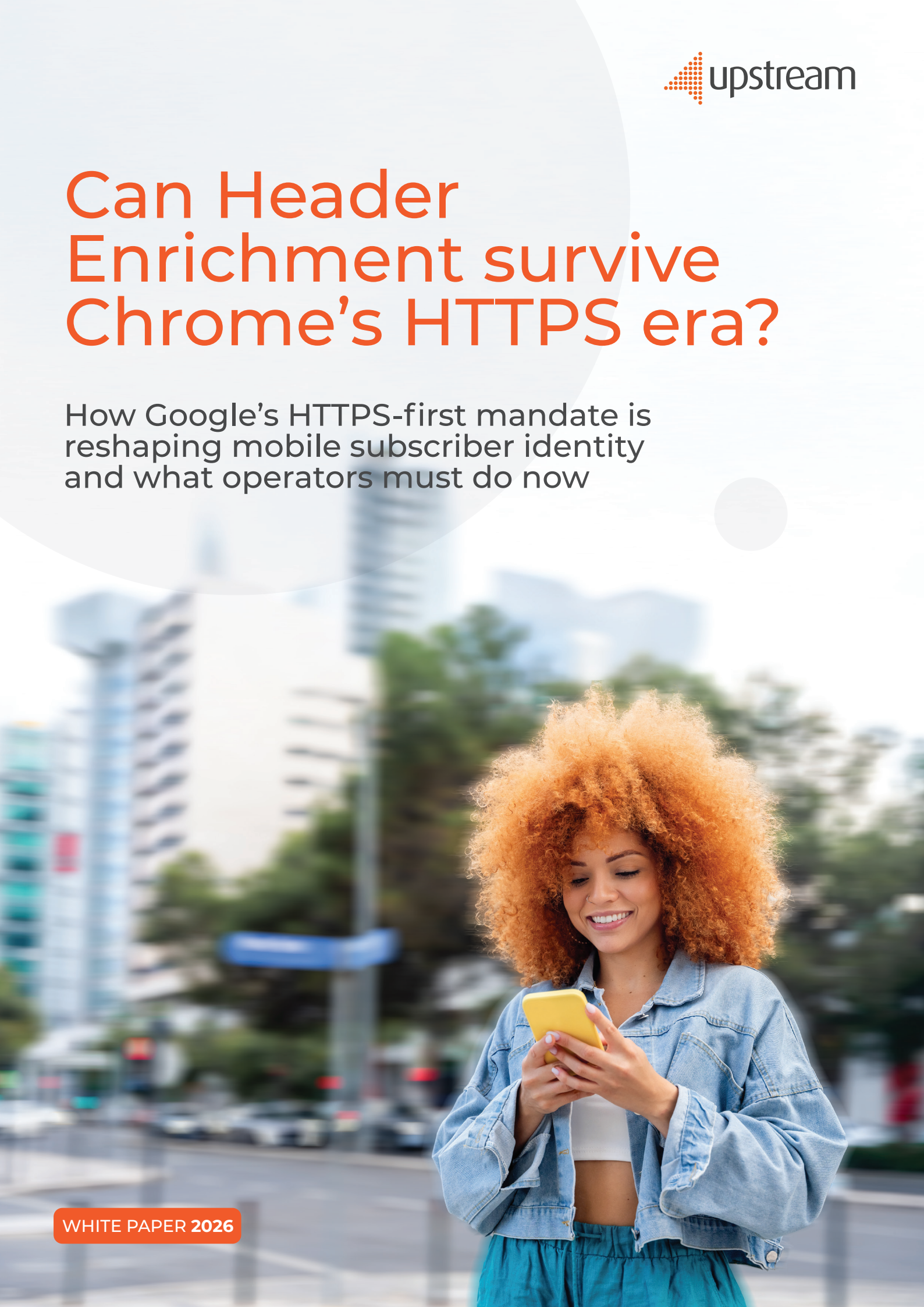
upstream

Can Header Enrichment survive Chrome's HTTPS era?

How Google's HTTPS-first mandate is reshaping mobile subscriber identity and what operators must do now



WHITE PAPER **2026**

What's inside

Executive summary

Mobile network operators have long relied on **Header Enrichment** as a tool to authenticate and identify their subscribers, enabling use cases ranging from seamless single sign-on and age verification to personalisation, service entitlement, and billing.

That capability is now under pressure.

By October 2026, it will be structurally unavailable for the majority of mobile web traffic and a growing share of mobile app traffic.

The trigger is Google's **"Always Use Secure Connections" (HTTPS-first) rollout.**

Chrome 147, released in April 2026, began warning users before loading HTTP pages for approximately one billion enhanced safe browsing users.

Chrome 154, scheduled for October 2026 will enable this behaviour by default for all Chrome users, **accelerating the industry's transition to fully encrypted web traffic.**

This is the natural outcome of the web's continued evolution toward stronger security and privacy protections. While this transition requires operators to rethink how subscriber identity is delivered, it also represents an important step towards a safer and more privacy-conscious digital ecosystem.

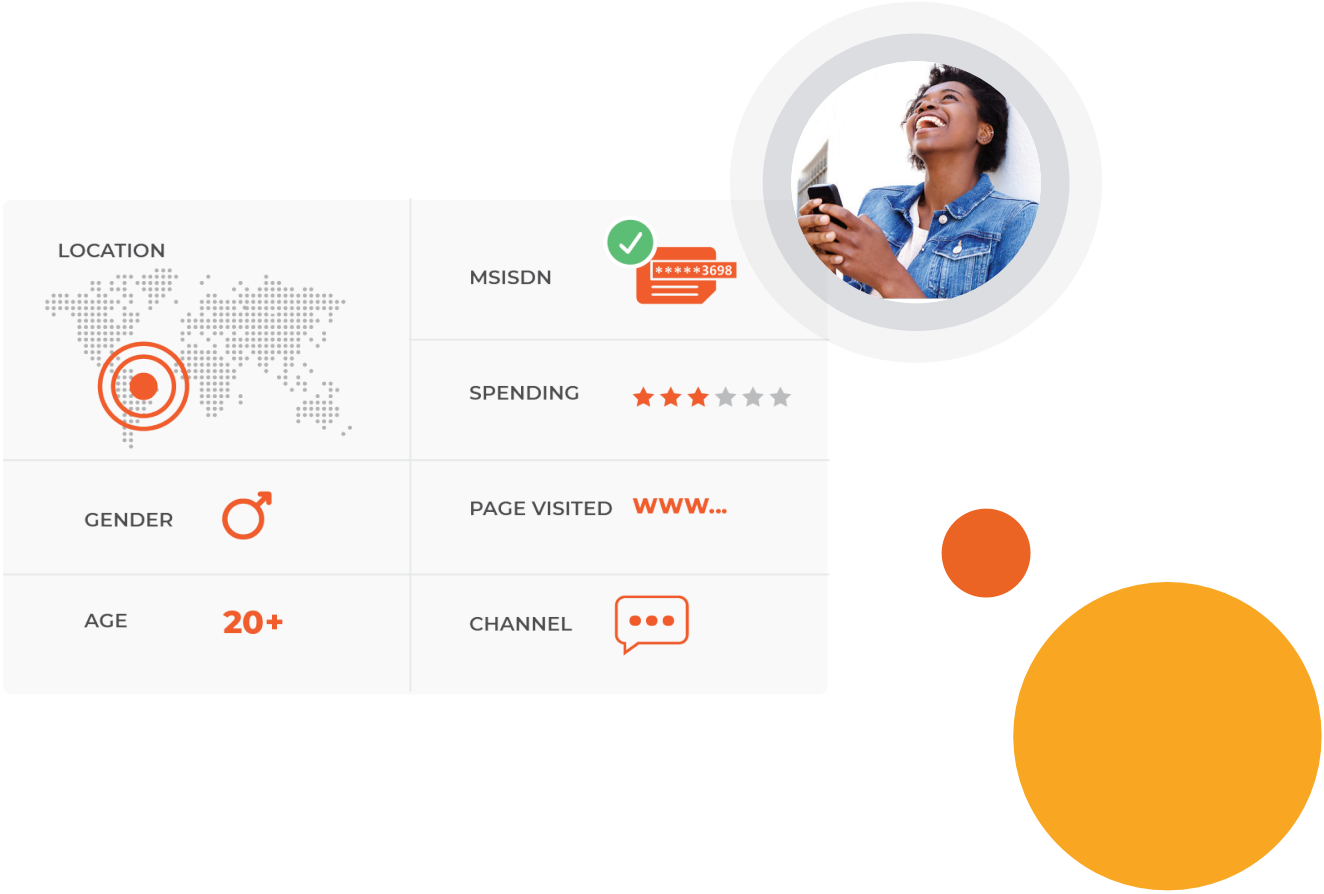
Upstream has been a pioneer in **network-based subscriber identification with Mobile ID,** a patented solution for HTTPS-compatible subscriber identification, successfully deployed with operators in Brazil, South Africa and Nigeria. This paper explains what is happening, why existing solutions are breaking, and what operators need to do now.

1. The end of an era for subscriber identification

For many years, mobile network operators have relied on Header Enrichment to identify subscribers and enable frictionless experiences such as seamless single sign-on, age verification, service entitlement, subscription flows, personalisation and billing, all without requiring the subscriber to enter credentials or take any additional action.

As web traffic migrated from HTTP to HTTPS, the **industry evolved Header Enrichment techniques to operate within encrypted environments while preserving the confidentiality of the underlying connection.** This enabled operators to continue delivering transparent subscriber identification without compromising the security benefits of HTTPS and proved that network-based subscriber identification could remain both technically feasible and commercially valuable in an increasingly encrypted web ecosystem.

Upstream has been a pioneer of this evolution through **Mobile ID, its patented solution for HTTPS-compatible subscriber identification,** with years of experience delivering this capability in live operator environments across multiple markets.



2. The clock is ticking on existing identity solutions

The industry is undergoing a fundamental shift toward HTTPS-first browsing and modern TLS implementations. **Google's "Always Use Secure Connections" initiative** is accelerating this transition by making encrypted connections the default experience.

At the same time, TLS 1.3 is becoming the preferred protocol for secure communications as operators, browser vendors and content providers modernise their infrastructure.

Chrome 147, released in April 2026, enabled this behaviour for approximately one billion enhanced safe browsing users, while Chrome 154, scheduled for October 2026, will extend it to all Chrome users by default. Chromium-based WebViews are expected to follow the same security direction, extending the impact beyond the browser itself.

Much of today's deployed Header Enrichment infrastructure was designed around earlier TLS architectures and cannot participate in modern end-to-end encrypted sessions without architectural changes. Many deployed GGSNs and associated Header Enrichment platforms were designed before widespread TLS 1.3 adoption. While vendor capabilities vary, much of today's installed infrastructure cannot participate in TLS 1.3-based identity enrichment without architectural changes or upgrades. **This creates a structural gap:** as encrypted traffic increasingly becomes the default, the network equipment that would need to participate in any identity-enrichment flow cannot yet keep pace, and traditional identity-enrichment mechanisms become progressively less effective.

This is not a theoretical future risk. This transition is already underway.

1. The **Mobile Ecosystem Forum** (MEF) has described the disruption as an "**urgent, structural transformation"** for the industry.

2. **WASPA** has begun active discussions among its members on **how to address the impact.**

3. The **GSMA's Mobile Identity Summit at MWC Barcelona 2026** highlighted the growing momentum behind **API-based subscriber identification** as operators recognise that **legacy enrichment mechanisms are no longer fit for purpose.**

4. And at the **GSMA Open Gateway Summit at MWC 2026**, the message was unambiguous:

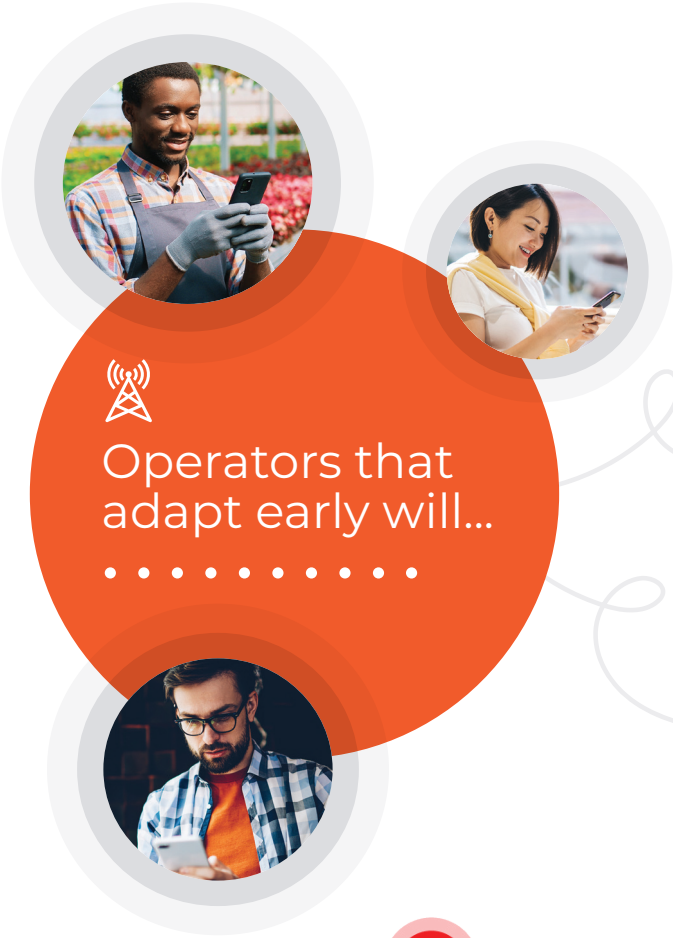
The era of pilots is over and the industry must now move to scale.

The consequences are already visible: following the Chrome 147 rollout in April 2026, Upstream has observed an average drop of 23% in enriched traffic volumes, a tangible, measurable signal that the shift is not on the horizon, but already in progress.

3. What operators stand to lose

Mobile network operators rely on network-based subscriber identification for authentication, access management, subscription flows or to create personalized experiences for their subscribers. As traditional **Header Enrichment** approaches **become** less effective in modern HTTPS environments, these flows risk becoming more complex, less seamless and ultimately **less valuable to** both **operators and their partners.**

The consequence of inaction is a structural shift in the user experience: frictionless, zero-input subscriber identification gives way to manual logins or, in some cases, the inability to identify the subscriber altogether. Increased friction can reduce conversion rates, increase abandonment and weaken the value proposition of operator-led digital services.



Operators that adapt early will...

preserve the seamless subscriber experiences that differentiate their digital offerings.

position themselves for the next generation of network-based identity services.

Those that delay risk allowing a **degraded user experience** to become the new baseline.

4. Preserving mobile subscriber identification in an HTTPS-first world

As browsers move further towards HTTPS-first enforcement, mobile operators face a clear challenge: **how to continue identifying mobile subscribers in real time,** securely and reliably, when those subscribers interact with digital properties over encrypted connections.

This capability matters because **mobile identity is one of the operator's most valuable assets.** It connects the digital journey with the verified subscriber relationship the operator already owns. It enables seamless login, contextual marketing, fraud prevention, retargeting, personalisation and trusted third-party use cases.

The Chrome update disrupts the way this identity has historically been delivered over HTTPS. However, it does not remove the operator's ability to identify subscribers. There are two production-ready paths available today, and Upstream can support both.

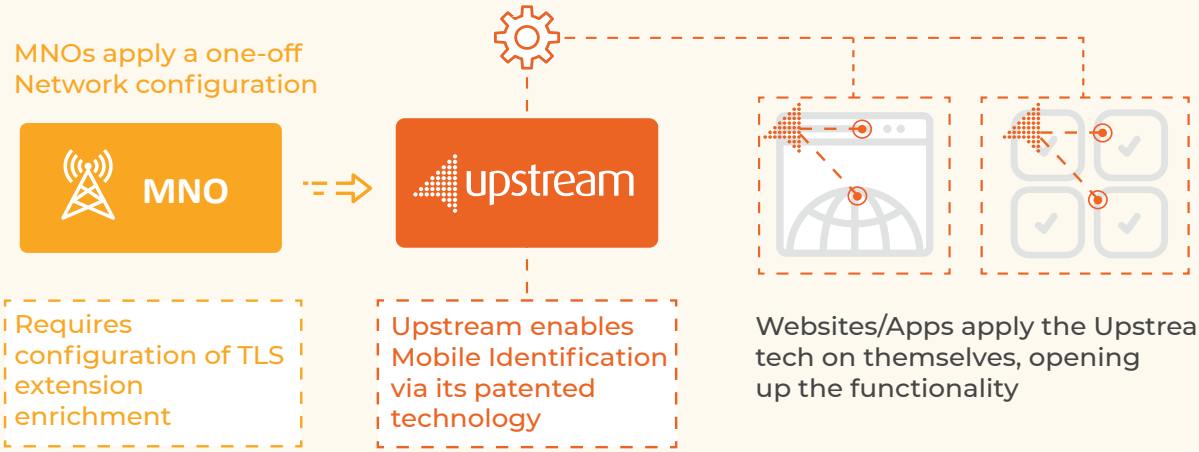
Two production-ready paths to identify the subscriber

At the identification layer, the question is simple: how does the operator retrieve and hold the verified subscriber identity in an HTTPS-first environment?
There are two practical paths.

Path A: Upstream

Upstream Mobile ID is a patented solution for HTTPS-compatible subscriber identification that has been in live production for several years across multiple markets. It was designed specifically to allow operators to identify subscribers over encrypted connections, while working within the operator's existing network architecture and without requiring wholesale infrastructure replacement.

Following Chrome's move towards stricter TLS 1.3 enforcement, Upstream's technical team identified and implemented a targeted configuration on the GGSN of a live operator deployment that restores Mobile ID functionality under TLS 1.3.



This is a significant milestone. It demonstrates that Chrome's enforcement roadmap is not an insurmountable barrier to mobile subscriber identification. Operators already using Mobile ID have a viable, tested continuity path that can be made operational ahead of Chrome 154 universal enforcement, expected in October 2026.

Path B: Authorised HTTPS Header Enrichment

The second path is Authorised HTTPS Header Enrichment. **This mechanism is based on a trusted, contractually governed arrangement between the operator and an authorised third party.** The third party explicitly authorises the operator to terminate and re-establish the secure session on its behalf, attach the subscriber identifier, and forward the enriched request securely to its destination.

This is not uncontrolled or generic header enrichment. It is an authorised identity process between trusted parties. In this model, the operator acts as the trusted source of subscriber identity. It asserts that identity only to third parties with which it has an approved technical and commercial relationship.

This path has already been deployed in live operator environments and can be implemented today. It gives operators an additional route to **preserve subscriber identification in an HTTPS-first environment,** while maintaining control over who can access the capability.

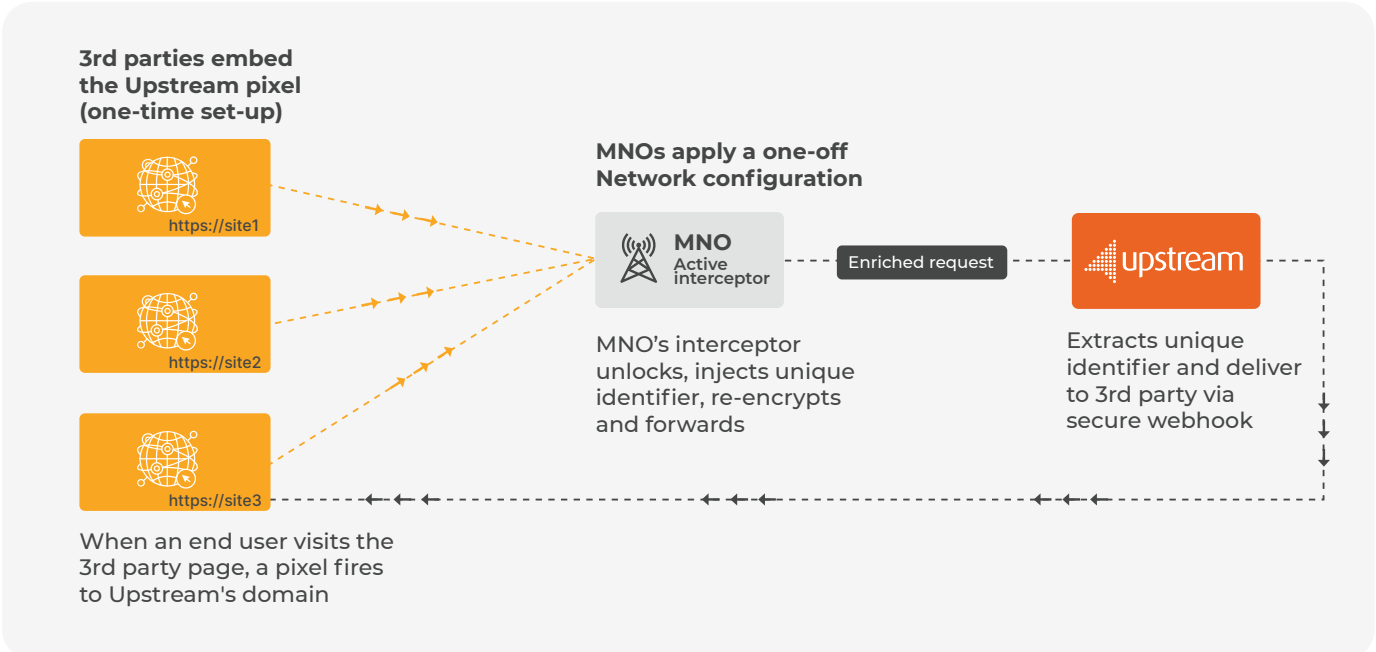
The Upstream Identity Broker:
making identity available to trusted third parties

The two paths above solve the first problem: **how the operator identifies the subscriber.**

The next question is how that verified identity can be made available to the trusted third parties the operator wants to support. This is the role of the Upstream Identity Broker.

Without a broker layer, every third party would need to establish its own bilateral technical integration and trust arrangement with the operator. This creates operational complexity, slows down partner onboarding and limits the operator's ability to scale the value of its identity asset.

Upstream provides the API and integration layer on top of either identification path: Upstream Mobile ID or Authorised HTTPS Header Enrichment.



For each authorised third party, Upstream provisions a unique tracking pixel. The pixel is embedded in the third party's web page or app web view. When a subscriber visits through the operator network, the pixel fires a background request to Upstream's enrichment-enabled domain. Upstream captures the subscriber identifier, associates it with the third party's session, and delivers the identity securely in real time via webhook.

This allows the operator to support an ecosystem of approved partners through a single controlled integration. The operator remains the trusted source of identity. **Upstream provides the infrastructure that makes this identity usable, secure and scalable for trusted third-party use cases.**

This significantly...

reduces
operational overhead.

accelerates
partner onboarding.

preserves
operator control over which partners are authorised to access subscriber identity.

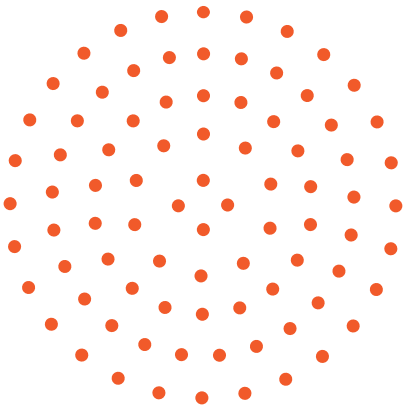
5. The window to act is NOW

The operators who move first will retain the frictionless subscriber experiences that define their advantage. Those who wait are accepting a structural degradation that will be visible to every end user they serve.

The GSMA Open Gateway initiative and the CAMARA project's Number Verify API are meaningful signals that the industry recognises network-native identity as a strategic capability. However, current implementations typically verify subscriber's number but they do not yet reliably retrieve subscriber identity in real time, before user interaction, at the scale and across the commercial use cases where Header Enrichment and Mobile ID operate today. Open Gateway is an important direction of travel. For operators that need continuity ahead of October 2026, it is validation of the need, not yet a deployable replacement.

Google's secure-by-default roadmap has set an immovable deadline. We've got you covered!

The recommended course of action is clear: **engage with Upstream to deploy Mobile ID with TLS 1.3 compatibility, or implement Authorised HTTPS Header Enrichment directly and layer the Upstream Identity Broker on top to extend that capability to every third-party partner in the ecosystem.** Both paths are available today, both have been validated in live deployments, and both can be operational well within the October 2026 deadline.

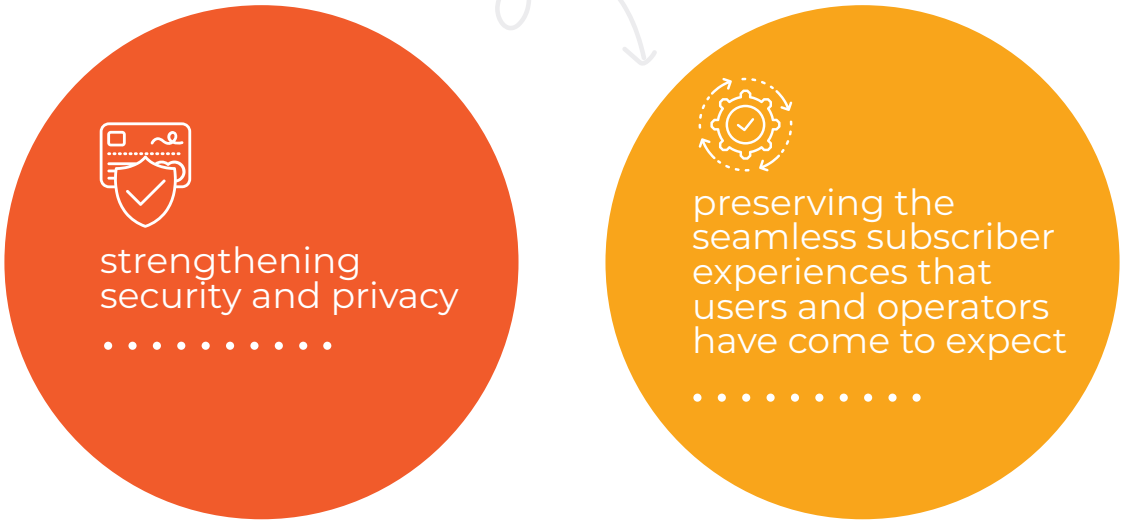


The end of traditional Header Enrichment is a structural reorganisation of how mobile subscriber identity is established, verified, and monetised. **Google's secure-by-default roadmap has set an immovable deadline.**

The GSMA's recognition of the challenge, reflected in the scale and pace of the Open Gateway initiative, confirms this is an industry-level shift, not an edge case. The 23% drop in enriched traffic already observed post-Chrome 147 is the opening signal. Chrome 154 will complete the transition.

The good news is that **the solution exists, has been deployed in live production environments, and can be operational well within the October 2026 deadline.**

At Upstream, we believe the future of mobile identity lies in balancing two objectives:



It's already been done. **Ask us** how we've helped operators across multiple markets get there and how we can do the same for you.

About Upstream

Upstream is a leading technology company operating in some of the most promising and rapidly growing markets in the world, delivering a diverse portfolio of solutions that help mobile network operators unlock new revenue streams and achieve digital growth.

Upstream's proprietary mobile marketing automation platform, Grow, combines innovations in the field of marketing automation, multi-channel campaign orchestration and engagement, data collection and analysis, subscriber identification, and ad fraud protection.

By combining this technology with in-house marketing expertise, **Upstream acts** as a true partner rather than just a vendor, helping operators design, launch, and optimize monetization programs with proven results **across Latin America, Africa, the Middle East and Southeast Asia.**

For more information on how you can leverage Upstream's Mobile Identity, visit: www.upstreamsystems.com or send an email to global-sales@upstreamsystems.com