

Discover how Smart's innovative Number Verification solution is transforming mobile security, enhancing customer experiences, and driving operational efficiency for a seamless and secure digital future.

SILENT AUTHENTICATION

Pioneering Towards a Secure &
Seamless Digital Ecosystem

Version 1
May 2025

Enterprise
Strategic
Technology
Management



TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
INTRODUCTION	2
The Open Gateway Initiative	2
Current Landscape of Digital Fraud in the Philippines	2
BSP’s Initiative to Strengthen the Security of the Digital Ecosystem.....	3
OVERVIEW OF SILENT AUTHENTICATION.....	3
What is Silent Authentication?	3
Number Verification API	4
BENEFITS OF SILENT AUTHENTICATION	4
For Enterprise Clients	4
For End Users	5
GSMA CERTIFICATION.....	5
TOP USE CASES OF SILENT AUTHENTICATION	6
Registration and Onboarding.....	6
Application Logins	6
High-Value Transactions	6
Account Recovery and Password Resets	7
GSMA CASE STUDIES FOR SILENT AUTHENTICATION.....	7
Seamless Authentication for Device Binding.....	7
Seamless Authentication during Password Reset.....	7
Seamless Authentication for Two-Factor Authentication (2FA).....	8
Seamless Authentication for Passwordless Login.....	9
CONCLUSION	10
REFERENCES.....	11
CREDITS.....	12
Primary Authors.....	12
Secondary Authors.....	12
Contributors.....	12

EXECUTIVE SUMMARY

Being a “mobile-first” country such as the Philippines, the digital ecosystem is thriving with rapidly increasing transactions every year. Along with it, bad actors and fraudsters are being creative more than ever as they take advantage of a broader audience in the digital world and the vulnerabilities that come along with being “online”. Due to the rampant phishing, vishing, and other schemes, inevitably, the need to ensure security and welfare in the digital space is now becoming one of the priorities for both businesses and end customers. Smart, acknowledging this need, is pioneering one of the next-generation solutions in ensuring a secure and seamless customer experience for mobile transactions.

This whitepaper explores the disruptive potential of the Open Gateway Initiative and its objective to create a framework to standardize Application Programming Interfaces (APIs) in mitigating fraudulent activities while providing a frictionless experience to end users through Number Verification. Through this innovative approach, businesses can substantially minimize the risk exposure that came along with the traditional authentication mechanisms, therefore significantly increasing the trust of their end users and customers.

This document also includes a comprehensive overview of the solution to help businesses integrate it into their own ecosystems. In addition, this whitepaper enumerates case studies and success stories from GSMA to show the tangible impact of these technologies on promoting security, operational efficiency, and overall customer satisfaction.

With the Number Verification API, Smart enables enterprises and businesses to position themselves at the frontier of digital innovations through a more secure and seamless mobile experience.

As digital threats continue to evolve, so must the solutions that protect and empower users. With Silent Authentication and the Open Gateway Initiative, Smart is not just responding to the challenges of today — it is actively shaping a more secure, seamless, and resilient digital future for businesses and consumers alike.

INTRODUCTION

The Open Gateway Initiative



The Open Gateway (OGW) is an initiative to create a framework in standardizing the network APIs from Mobile Network Operators (MNOs) that can be used by enterprises as well as end users. It is led by GSMA in collaboration with TMForum for the Operational Guidelines (Operate APIs) and CAMARA for the Technology and Standardization (Service APIs).

By providing a single point of access, this initiative aims to accelerate the integration, deployment, and interoperability of various services for developers, service providers, and enterprise customers.

One of the APIs with a large adaptation is the Number Verification API. It intends to provide a more seamless user authentication experience while enhancing the overall security of mobile transactions ^[1].

Through the Open Gateway Initiative, the mobile ecosystem is taking a bold step toward greater collaboration, standardization, and innovation. By opening up network capabilities via standardized APIs, it paves the way for a more secure, interoperable, and developer-friendly environment — ultimately empowering enterprises to deliver richer, safer, and more seamless digital experiences for users around the world.

Current Landscape of Digital Fraud in the Philippines

True to the notion of a “mobile-first” country, it has been recorded that more than 60% of the financial transactions in the Philippines are done via mobile device, which translates to a substantial ₱55 billion in Person-to-Merchant (P2M) transactions ^[2, 3].



However, with this volume, the Philippines finds itself as one of the top target destinations of fraudsters and bad actors that are trying to leverage the sheer volume of digital transactions in the country, with the highest e-shopping scam rate in Asia at at 35.9% ^[4], resulting in ₱460 billion lost to fraud in 2024 ^[5].

This alarming trend underscores the urgent need for robust security measures to protect consumers and businesses alike — not just to prevent financial loss, but to preserve trust, ensure business continuity, and support the country's growing digital or mobile economy.

BSP’s Initiative to Strengthen the Security of the Digital Ecosystem

The Bangko Sentral ng Pilipinas (BSP), acknowledging the advancements done by bad actors and fraudsters to circumvent the traditional verification methods, is proactively getting feedback from various industries on a draft circular. Its objective is to enhance the security stance of both banks and non-banks against cybercrimes.



One of the highlights proposed by BSP is to limit the usage of One-Time Passwords (OTPs) and other interceptable authentication mechanisms^[6]. This move highlights the growing recognition that traditional methods are no longer enough to keep up with the increasingly sophisticated tactics of cybercriminals. It reflects the magnitude of the need to modernize and strengthen anti-fraud measures across the country’s digital ecosystem — ensuring that both businesses and consumers are better protected in an ever-evolving threat landscape. And that is where Silent Authentication enters the picture.

OVERVIEW OF SILENT AUTHENTICATION

What is Silent Authentication?



Silent Authentication is a real-time communication between an Enterprise Client and Smart’s Open Gateway Platform. This exchange is used to check the identity of the user without the need for traditional authentication methods such as One-Time-Passwords (OTPs). Silent Authentication enables frictionless verification while ensuring that data security and data privacy are still in place.

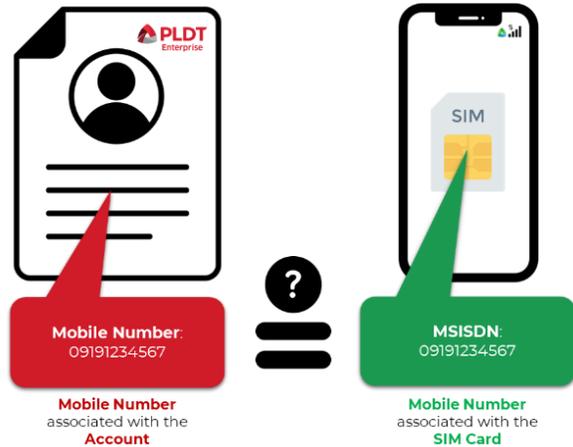
The server of the Enterprise Client acts as the API invoker and provides the registered mobile number of the account user. The Smart Open Gateway (OGW) Platform will now cross-reference the received mobile number to the actual mobile number performing the same transaction. If the two mobile numbers are the same, the OGW Platform will send back a response with a “TRUE” value. Otherwise, the platform will respond with a “FALSE” value.

The result of Silent Authentication will provide another layer of security and act as a real-time indicator of potential compromise for the Enterprise Client. This actionable signal empowers businesses to make smarter, faster decisions about whether to approve, flag, or block a transaction — all without interrupting the customer journey. By detecting inconsistencies at the network level, it becomes a powerful tool in identifying suspicious activity early and preventing fraud before it happens.

Number Verification API

Smart’s Silent Authentication service is enabled by Number Verification, a standard API under the Anti-Fraud API family of the GSMA Open Gateway Initiative.

To ensure security and uniqueness of each transaction request, this API requires a standard 3-legged token and authentication. Upon clearing the authentication request, the actual service API for Number Verification proceeds. In addition, it runs on HTTPS to ensure encrypted communication between the client and the server throughout the entire Silent Authentication process.



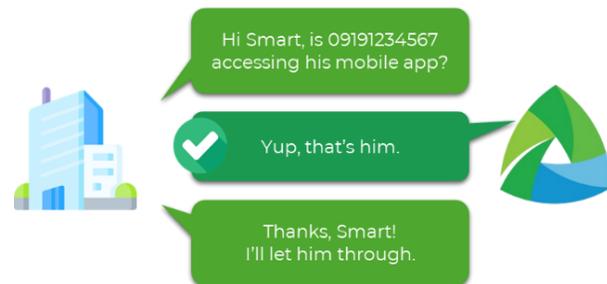
BENEFITS OF SILENT AUTHENTICATION

For Enterprise Clients

This solution provides immediate benefits to businesses and enterprises by improving their overall security posture and operational efficiency. Since the authentication process is fully automated and is happening all in the background, it gets rid of the necessity for manual verification, thereby significantly reducing the risk of human error and minimizing the potential for fraud.

In addition, this solution can also lead to higher conversion rates because customers or buyers can complete their transactions more quickly and securely. It can also introduce a reduction in pending transactions due to delays and undelivered passcodes, OTPs, etc., leading to higher brand recognition, customer satisfaction, and loyalty.

In terms of integration, Smart’s Silent Authentication follows the global standard of GSMA Open Gateway making it extremely interoperable with various platforms and ecosystems. In addition, this standard way of implementation allows a very straightforward deployment in the enterprises’ systems, without requiring any major changes or development on the client’s side.



As a solution originating from a Mobile Network Operator (MNO) such as Smart Communications, the service is ensured to be highly scalable, allowing them to handle large volumes of transactions without compromising on security or performance.

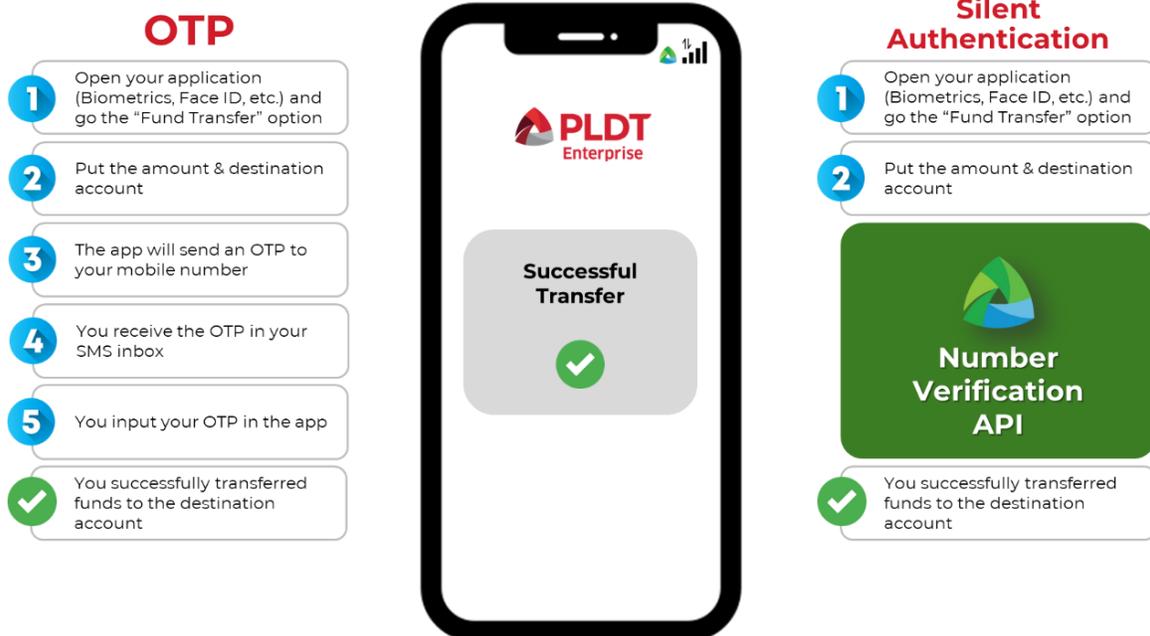
Ultimately, Silent Authentication empowers enterprise clients to deliver smarter, safer, and more seamless digital experiences — all while reducing operational burdens and minimizing fraud risks. By embracing this innovation, businesses not only future-proof their systems but also send a powerful message to their customers: that security, convenience, and trust are at the heart of every transaction.

For End Users

Silent Authentication provides a frictionless user experience to the users of the mobile application. Using this solution, users can now be automatically authenticated through their mobile network provider without the need of any input such as passwords or OTPs.

This will also provide an elevated approach on the security of the transactions of the end users because by eliminating OTPs and other input, it also removes the entry point of bad actors in exploiting this loophole.

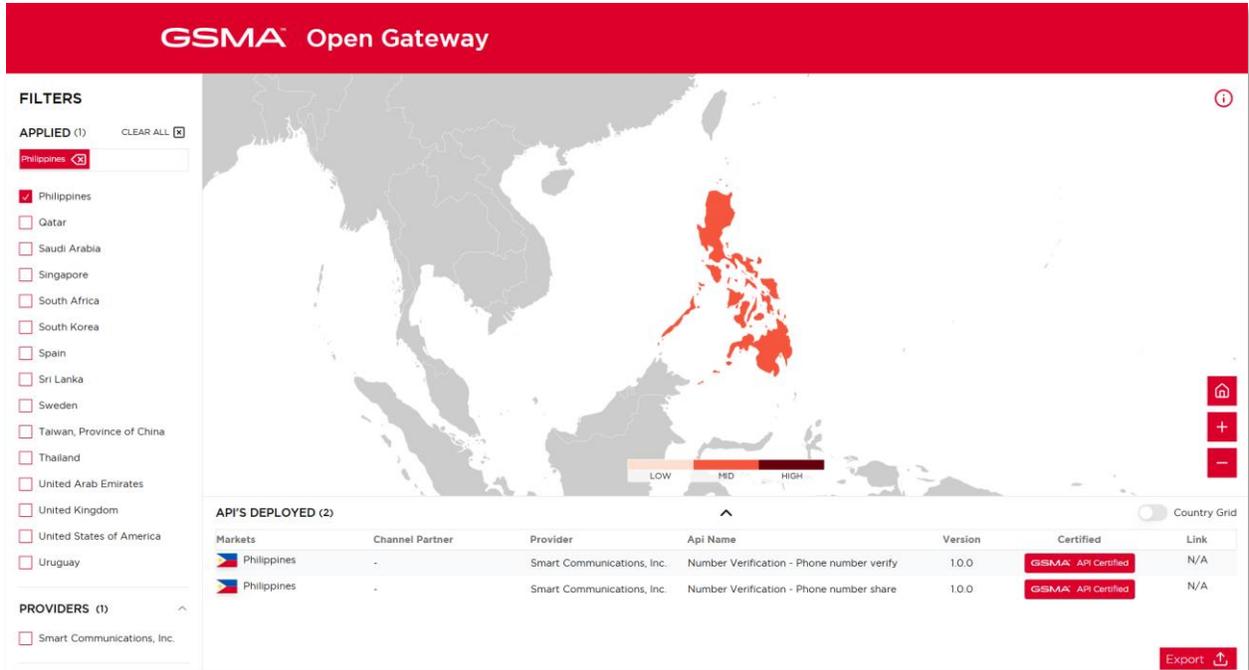
For end users, Silent Authentication offers more than just convenience — it brings peace of mind. By eliminating the need for passwords and OTPs, it removes common points of failure while enhancing both security and user experience. With authentication happening quietly in the background, users can enjoy faster, safer interactions with the services they rely on every day, without even lifting a finger.



GSMA CERTIFICATION

As the pioneer Philippine Mobile Network Operator (MNO) to be part of the initiative, Smart Communications, Inc. is also the first Telco in the country to be certified for a GSMA Open Gateway API. Smart received the formal certification from GSMA for the Number Verification API (for two endpoints: Number Verify and Number Share) last February 27, 2025.

This global certification underscores the company’s strong commitment to upholding international standards and best practices in the rapidly evolving field of Network APIs — reinforcing Smart’s role as a trusted leader in secure, cutting-edge mobile solutions.



This certification ultimately validates the reliability, security, and effectiveness of Smart's API solutions, positioning the company as a leader in the telecommunications industry.

TOP USE CASES OF SILENT AUTHENTICATION

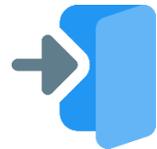
Registration and Onboarding



Silent Authentication can automatically verify the user account's mobile number without requiring them to enter OTPs or passwords, thus streamlining the registration and onboarding process for new users. This will further reduce the friction and enhance the user experience, making it seamless for customers to onboard the enterprise's platform.

Application Logins

Silent Authentication can also be used to provide a safe and smooth process to log into the users' accounts. Since the whole verification process happens in the background, it helps secure the account from phishing and credential theft since there is no manual input of credentials needed.



High-Value Transactions



One of the most common use cases for Silent Authentication is verifying requests for high-value transactions. This can be large peer-to-peer fund transfers, merchant payments, and costly purchases, among others. By ensuring that the registered mobile number of that account is the same mobile number requesting for that transaction, it adds a higher tier of security for both enterprises and consumers.

Account Recovery and Password Resets

Silent Authentication can also be very beneficial for scenarios involving account reset and recovery. Whenever users need to recover their accounts or reset their passwords, the solution can easily verify their identity in the background without requiring manual input. This simplifies the entire process while ensuring that only legitimate users can regain access to their accounts — reducing frustration, minimizing downtime, and strengthening security against account takeovers and social engineering attempts.



GSMA CASE STUDIES FOR SILENT AUTHENTICATION

Seamless Authentication for Device Binding

<p>Sector</p>	<ul style="list-style-type: none"> • Financial Services • Retail • Media
<p>Business problem being solved</p>	<p>Enables a Service Provider to securely and seamlessly tie the user account to their mobile phone number during mobile registration and re-enrolment processes</p>
<p>How the solution works</p>	<p>When a user registers to a service for the first time or on a new device, the Service Provider seamlessly authenticates their phone number.</p> <p>By leveraging data from the following API, the system can enable user account registrations for new devices:</p> <ul style="list-style-type: none"> • Number Verification API: The Service Provider calls the API, and the mobile operator verifies the user’s possession of the mobile number. • Additional advantages include: <ul style="list-style-type: none"> ○ Device binding created using secure SIM-based authentication ○ Fast and frictionless user experience using the mobile number

Seamless Authentication during Password Reset

<p>Sector</p>	<ul style="list-style-type: none"> • Financial Services • Retail • Media
----------------------	---

Business problem being solved	Enables a Service Provider to secure their password reset process
How the solution works	<p>When a user requests a password reset, the Service Provider seamlessly verifies that the user is in possession of the mobile phone number previously associated to their account.</p> <p>By leveraging data from the following API, the system can enable logins every time with strong SIM-based authentication:</p> <ul style="list-style-type: none"> • Number Verification API: The Service Provider calls the API and the mobile operator verifies the user’s possession of the mobile number. • Additional advantages include: <ul style="list-style-type: none"> ○ Keep existing login experience while enhancing security ○ No credentials to be phished

Seamless Authentication for Two-Factor Authentication (2FA)

Sector	<ul style="list-style-type: none"> • Financial Services • Retail
Business problem being solved	Enables a Service Provider to step up user account authentication by adding two-factor authentication, without adding friction to the user experience
How the solution works	<p>When a user authenticates to a service through existing methods, the Service Provider seamlessly adds a layer of security with second-factor authentication that verifies the user’s mobile phone number.</p> <p>By leveraging data from the following API, the system can enable fast and frictionless second factor with strong SIM-based authentication:</p> <ul style="list-style-type: none"> • Number Verification API: The Service Provider calls the API and the mobile operator verifies the user’s possession of the mobile number. • Additional advantages include: <ul style="list-style-type: none"> ○ Maintain existing user experience while enhancing security ○ No credentials to be phished

Seamless Authentication for Passwordless Login

<p>Sector</p>	<ul style="list-style-type: none"> • Financial Services • Retail • Media
<p>Business problem being solved</p>	<p>Enables a Service Provider to authenticate returning users seamlessly through their mobile phone number</p>
<p>How the solution works</p>	<p>Users log into a service with their mobile number instead of a username and password, with the Service Provider verifying the user’s possession of the mobile number instead of their knowledge of a password.</p> <p>By leveraging data from the following API, the system can enable frictionless logins every time with strong SIM-based authentication:</p> <ul style="list-style-type: none"> • Number Verification API: The Service Provider calls the API and the mobile operator verifies the user’s possession of the mobile number. • Additional advantages include: <ul style="list-style-type: none"> ○ A truly passwordless approach (no username or password) resulting in no credentials to be phished

All of the use cases mentioned in this section are from the GSMA Open Gateway Use Case Library for Number Verification ^[8].

CONCLUSION

Smart's Silent Authentication solution pioneers the next wave of advancements in mobile and digital security, providing a more seamless and secure approach to the authentication of user identities without the need for traditional and interceptable verification mechanisms.

The solution uses a real-time comparison of the mobile number associated with the enterprise user account is being cross-referenced and the mobile number associated with the SIM card doing the transaction. This automated check is done in real-time, and it all happens in the background, making this solution a seamless experience for the end users.

As a solution from a Mobile Network Operator (MNO) such as Smart Communications, it leverages the actual network events and information, without dependence on any user input, making it a tamper-proof mechanism for the security and safety of both the enterprise client's data as well as the data from Smart network.

Furthermore, the solution was designed with Data Privacy in mind. Smart's OGW Platform only provides a "TRUE" or "FALSE" response to the inquiries of our enterprise clients, ensuring that there will be no exposure of personally identifiable information of our subscribers.

By adopting Silent Authentication, businesses can protect their customers, streamline operations, and build trust, positioning themselves as leaders in the secure digital ecosystem — all while delivering the kind of seamless, secure, and empowering experiences that today's digital-first customers truly deserve.

REFERENCES

1. <https://www.gsma.com/solutions-and-impact/gsma-open-gateway/>
2. https://www.bsp.gov.ph/PaymentAndSettlement/2023_Report_on_E-payments_Measurement.pdf
3. <https://paymentscmi.com/insights/philippines-ecommerce-market-data/>
4. <https://www.philstar.com/headlines/2023/11/24/2313809/survey-philippines-has-highest-e-shopping-scam-rate-asia>
5. <https://newsinfo.inquirer.net/1993340/alarming-p460b-lost-to-scams-in-ph-says-study>
6. <https://business.inquirer.net/504706/bsp-eyes-shift-away-from-otps-to-fight-fraud>
7. <https://www.gsma.com/solutions-and-impact/gsma-open-gateway/gsma-open-gateway-resources/?category=number-verification>
8. <https://open-gateway.gsma.com/map>

CREDITS

Primary Authors

Mark Dommel S. Geronimo

Head of Wireless Product Development, PLDT Enterprise

Michael Rafael L. Ruiz

Head of Strategic Technology Management, PLDT Enterprise

John R. Gonzales

First Vice President and Head of Enterprise Consulting Services & Technology Management, PLDT Enterprise

Secondary Authors

Renelle John C. Magahis

Head of Emerging Technologies, PLDT Enterprise

Giovanni Gil M. Abaquin

Head of Strategic Business Development, PLDT Enterprise

Contributors

Network Strategy and Transformation Office

Radames Zalameda
Joseph Lennart Olaivar
Roy Reyes
Ramilo Caluag

Wireless Network Solutions

Hans Christian Alvarez
Jermaine Jayson Tan
Jan Michael Bustos

Wireless Core Engineering

Grace Feril
Jon Albert Quisel
Avegel Marcelo