

KEYWORD

LinQ2

USE CASE

Encrypting OTP in Transit and at Rest within the LinQ2 Unified Communication Platform

Executive Summary

This use case highlights how LinQ2’s Unified Communication Platform enhances data security by encrypting One-Time Passwords (OTPs) both during transmission and while stored at rest. Designed for banks, government entities, and large enterprises, this solution ensures compliance with CST, NCA, and SAMA standards while maintaining the highest performance and reliability.

By implementing end-to-end encryption and secure hashing mechanisms, LinQ2 eliminates the risk of unauthorized access, interception, or exposure of OTP data.

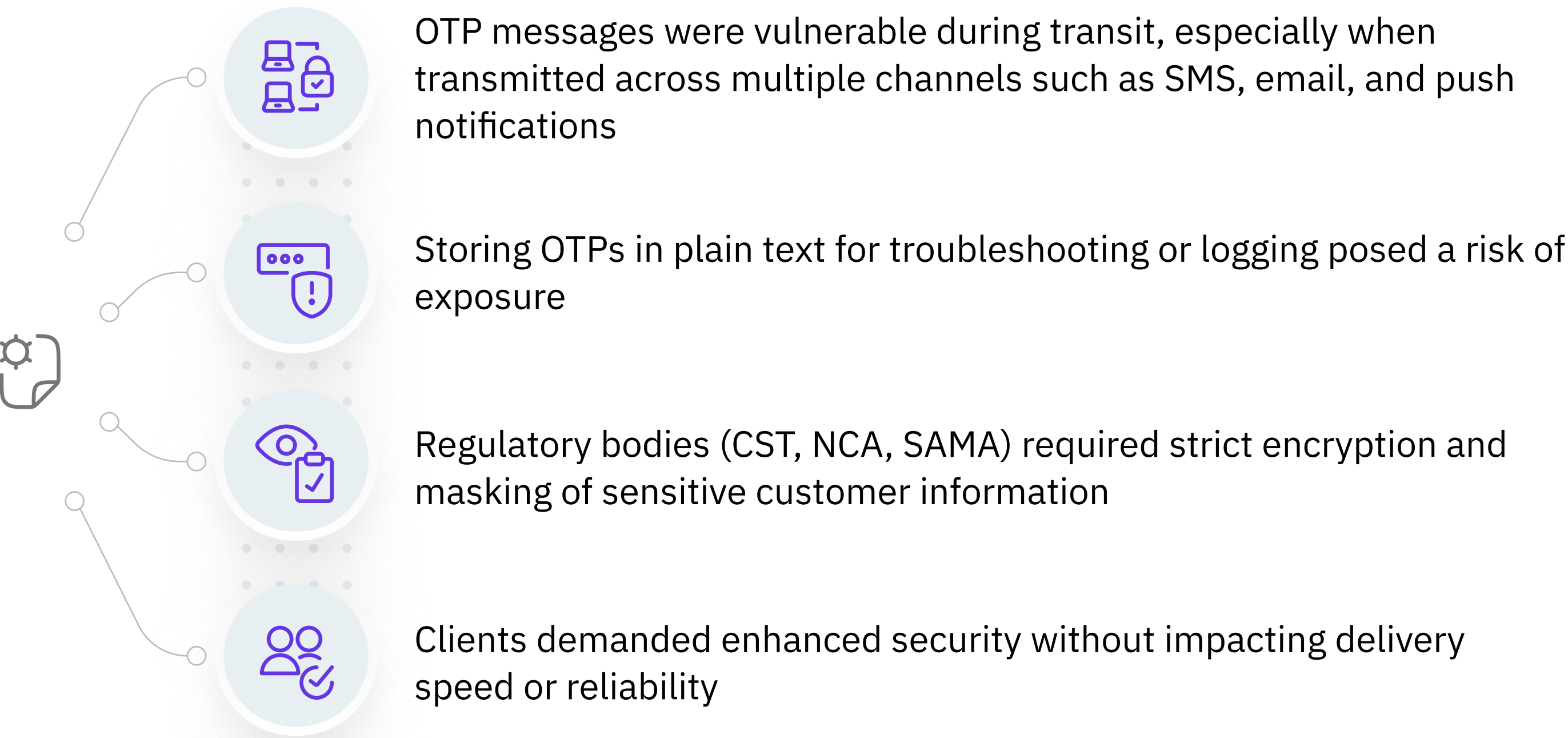


Background

Many enterprises and financial institutions rely on OTPs to verify user identities and authorize critical transactions. However, the growing sophistication of cyberattacks has made OTP interception and data exposure a significant concern.

LinQ2, a trusted omnichannel communication platform, recognized the need for a more robust mechanism to secure OTPs in motion and at rest, ensuring regulatory compliance and data protection for its enterprise clients

Challenges

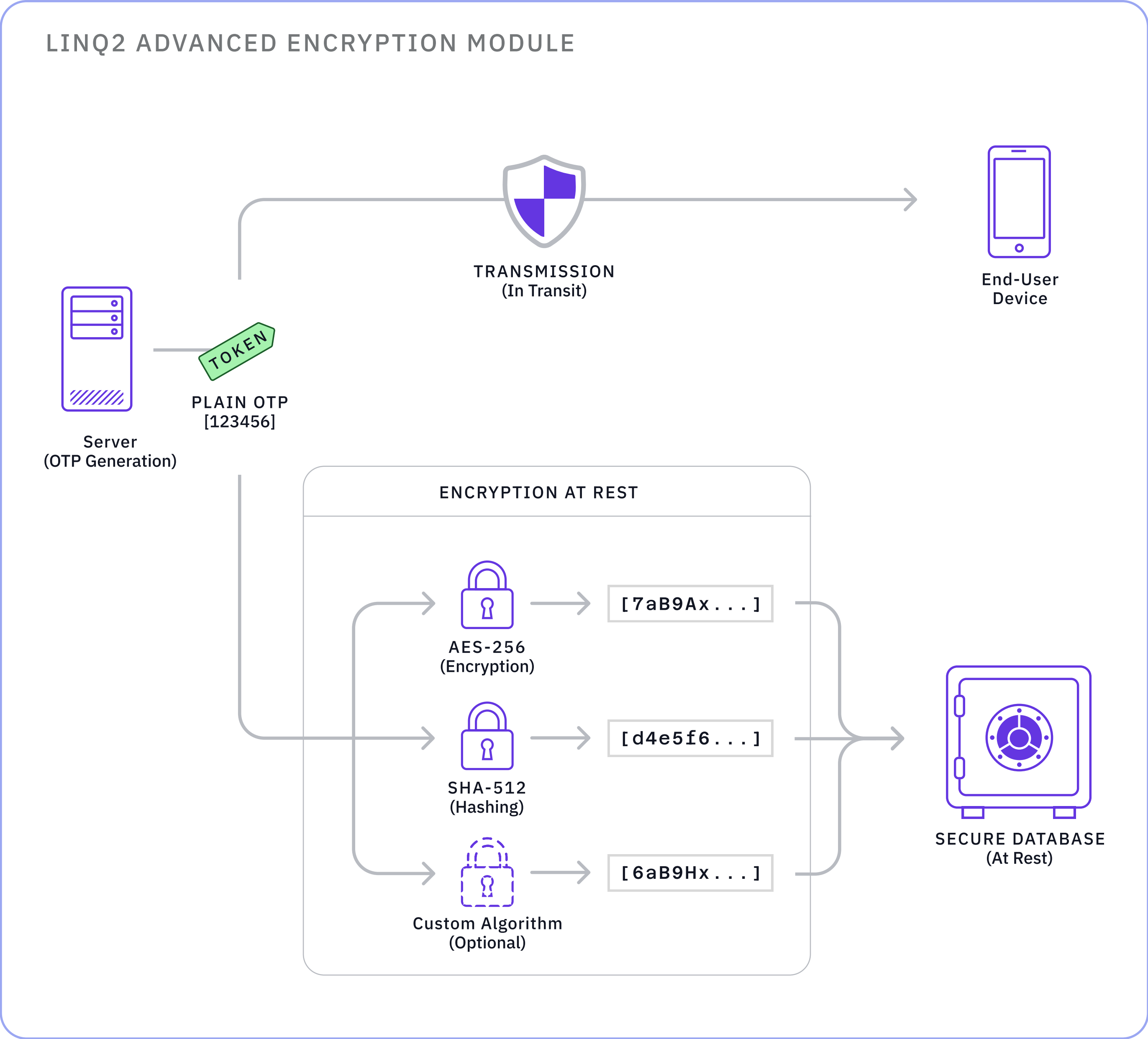


Solution – LinQ2 Secure OTP Encryption Framework

LinQ2 introduced a new advanced encryption module that applies encryption and hashing mechanisms to OTPs at two stages—during transmission (in transit) and after delivery (at rest).

The framework supports AES256- encryption, SHA512- hashing, and optional custom algorithms for clients with internal security mandates.

This approach uses a forward-then-store model, where OTPs are encrypted/hashed after transmission and securely logged or stored only in encrypted/hashed form.



Implementation Approach



Encryption in Transit

LinQ2 secures OTP transmission through HTTPS (TLS 1.3/1.2) and encrypted SMPP connections, ensuring all inbound and outbound communications remain fully protected without requiring message-level encryption



Encryption at Rest

Stored OTP data in LinQ2 databases or logs are encrypted/hashed using the same secure key management framework, ensuring no plain-text OTPs are ever exposed

Results & Benefits



- Achieved full compliance with CST, NCA, and SAMA data protection regulations



- Completely eliminated OTP exposure during transmission or storage



- Improved trust and confidence among banking and government clients



- Maintained high system performance and message delivery rates



- Reduced operational risks and simplified security audits



Conclusion

By implementing end-to-end OTP encryption within LinQ2's Unified Communication Platform, organizations can ensure their customers' authentication data remains fully protected. This initiative reinforces LinQ2's position as a leading, compliant, and secure communication gateway for critical enterprise messaging across multiple channels.



Cerebra is the regional cybersecurity pioneer, trusted by top-tier clients. Inspired by human intelligence, we help organizations manage risk and protect identities

Our vision is to be the leading cybersecurity vendor in the region with a mission to empower people and organizations to safely engage their digital experience

Established in 2020. Headquartered in Riyadh, Kingdom of Saudi Arabia



GET IN TOUCH

Hala@cerebra.sa



OUR WEBSITE

Cerebra.sa