EINPRESSWIRE

SecureG Partners with CTIA to Deliver the Most Secure, Trustworthy Solution for Branded Business Calls

SECURELY RESTORING TRUST IN VOICE CALLS ; HIGH-ASSURANCE CERTIFICATION AUTHORITY (CA) TO ENSURE INTEGRITY OF ECOSYSTEM AND AUTHENTICITY OF BRANDED CALLS

Bespoke cryptography solutions for a connected world

VIENNA, VA, UNITED STATES, December 2, 2024 /EINPresswire.com/ -- December 2, 2024 — Vienna, Va. — SecureG, the world's most secure root of trust provider, today announced it was partnering with CTIA to deliver Branded Calling ID (BCID™), an industry-led initiative to develop the most secure and interoperable ecosystem for businesses to embed trusted information, such as their logo and call reason, into their calls to consumers. SecureG's public key infrastructure (PKI) solutions provide the highest level of security for BCID digital signatures.

"SecureG provides the most advanced security for the most secure Branded Calling ID solution," said John Marinho, Vice President, Cybersecurity and Technology CTIA. "No other CA could provide the level of security required to deliver digital trust for the entire telecom industry. This is critical infrastructure protection."

SecureG provides high-assurance operations of the CTIA Secure Telephone Identity Certification Authority (CTIA STI-CA) Root, Intermediate CA, and the Certificate Repository to secure brand identity. SecureG trust anchors, which enable BCID to securely authenticate its ecosystem participants to sign calls, are stored in a vault and guarded under a mountain.

"No one wants to answer their phone because of all the spam and scams, and it is only getting worse now that AI-generated voices can impersonate people and businesses," said Todd Warble, CTO, SecureG. "SecureG empowers BCID with a secure-by-design foundation that enables consumers to trust the authenticity of the brands and intentions of the caller."

BCID mitigates the risk of consumers being harmed by fraud and bad actors by relying on industry standards and independent vetting to deliver a trusted, branded call experience for consumers. According to an August 2024 Morning Consult survey, 75% of consumers said they would answer a call if they received indicators such as name, logo, or call reason.

BCID includes:

The most secure solution for businesses to brand their calls: CTIA's Secure Telephone Identity certificates are issued by the world's most secure root of trust, which are stored in a vault, guarded in hardened concrete bunkers.
Vetted business callers: Scammers and spammers cannot gain access to BCID signing credentials.
Cross-network, cross-device coverage: BCID is designed to work seamlessly across networks and mobile phones, so enterprise businesses can deliver trusted, branded calls to their consumers.
Brands only pay for delivered calls: BCID is the only ecosystem that confirms branded calls have been delivered. Brands only pay for confirmed data delivery, ensuring accountability and transparent financial incentives.
"CTIA and its partners have collaborated across the entire ecosystem to provide the most secure branded calling solution with a hardened PKI and common best practices," said Damon Kachur, SecureG GM. "With the launch of BCID, businesses will be able to deliver trusted calls, and consumers can rest assured that the caller's identity has been rigorously verified and they are not a scammer."

Learn more about SecureG PKI for Branded Calling ID at SecureG.io/BCID

About SecureG

SecureG was conceived by MITRE Engenuity and CTIA to establish and maintain trust for 5G networks, machine-to-machine communication, and Zero Trust environments. SecureG's hardened root of trust defends Branded Calling ID and SunSpec Distributed Energy Resources against nation-states and well-financed adversaries. SecureG's bespoke public key infrastructure (PKI) services can be customized to meet the security posture and scaling requirements of voice, cloud computing, IoT devices, and data provenance. SecureG Analytics inventories all keys, digital certificates, and protocols to detect weak or quantum-unsafe algorithms and other cryptographic risks. SecureG, the harbinger of the PKI renaissance. Learn more at SecureG.io

John Jefferies
SecureG
+1 408-205-5329
email us here
Visit us on social media:
X
LinkedIn

YouTube