metaswitch

MetaSphere QCall

Eliminate robocalls with the leading STIR/SHAKEN solution

MetaSphere QCall is the leading implementation of STIR / SHAKEN to prevent Caller ID spoofing.

- First implementation to successfully complete the ATIS Testbed
- First vendor deployment in a US Tier 1
- Fully compliant to the STIR / SHAKEN standards
- Powerful diagnostics integrated with with Metaswitch's Service Assurance Server
- Cloud native design with low friction deployment options
- Flexible support for multiple network types, including IMS and NGN
- Connect to our Managed Service or deploy in your own private cloud

STIR/SHAKEN Regulation is Here

In reaction to the rise of consumer complaints, regulators are increasingly applying pressure to carriers to solve the problem of illegal robocalls. In the US, the current Chairman of the FCC described robocalling as the "scourge of civilization", and the Pallone-Thune TRACED act requires all service providers to adopt Caller ID authentication technology by June 2021. In Canada, the CRTC requires deployment of STIR / SHAKEN by September 2020.

QCall

Metaswitch has unique experience deploying QCall: notably, it is running today in a US Tier 1's own private cloud, processing millions of signing and verification requests between that operator and its industry peers.

QCall is built from the ground up to run in virtualized deployments, such as VMware or OpenStack. Its cloud-native architecture includes sideways scaling and active-active geographic redundancy. Optionally, it can be integrated into an orchestrator, to provide deeper automation.

QCall exposes an HTTPS interface, as per ATIS-1000082, for signing and verification, ideally suited for integration with network elements such as Interconnect SBCs for a highly efficient implementation. We also offer a solution for networks that are unable to invoke the HTTPS interface directly, proxying SIP requests to the HTTPS interface.

QCall includes a Key Management Server (SP-KMS) and Certificate Repository (STI-CR), and maintains support for the latest ATIS/ IETF developments, such as support for SIP diversions (draft-ietf-stir-passport-divert-07).

QCall is integrated with Metaswitch's Service Assurance Server (SAS), providing powerful diagnostics and troubleshooting, essential for traceback of robocalls.

Metaswitch offers flexible licensing schemes, based either on transactions-per-second, or on the total number of subscribers, ensuring that the operator's software costs remain predictable even when the number of spam calls and subscriber base size vary.

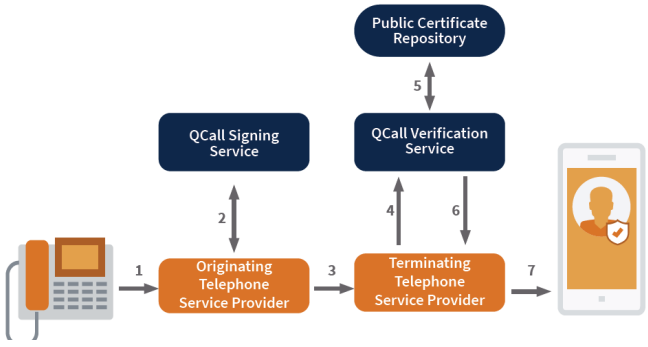
Call Validation Treatment (CVT)

A decision must be taken after a STIR/SHAKEN call is verified about what to display to the user – arrow (7) below. This is where there is a role for the Call Validation Treatment component, commonly known as a Reputation Database or Analytics engine.

Metaswitch recommends Call Guardian from Transaction Network Services (TNS). This industry-leading analytics solution uses cross-operator real-time call events combined with crowd-sourced data to identify legitimate telecoms users from abusive, fraudulent and unlawful users.

When combined with QCall, Call Guardian can ensure that the real owner of a spoofed number is protected from having their calls blocked.

Call Guardian is deployed at 4 of the top 6 wireless operators and a Tier 1 landline operator.



Call Guardian Authentication Hub

Metaswitch has partnered with TNS to deliver QCall and Call Guardian as a hosted solution: Call Guardian Authentication Hub.

Connect to CGAH without additional in-network deployment to provide STIR/SHAKEN and analytics verification to your subscribers.

Robocalling is a significant issue. QCall and Call Guardian from Metaswitch and TNS can help you keep your subscribers safe and satisfied with their service.

Specifications

Compliance

- STIR standards: RFC 8224, RFC 8225, RFC 8226
- SHAKEN standards: ATIS 1000074, ATIS 1000080, ATIS 1000082

Platform

- VMware
- OpenStack

Scale

- Scales up and down to any size network
- Up to 50,000 transactions per second per deployment

Architecture

- IMS: QCall deployed alongside the P-CSCF or as a SIP AS exposing ISC interface to IMS core
- NGN / softswitch: QCall HTTP service deployed alongside Perimeta SBC, 3rd party SBC, or other SHAKEN-ready network element
- Hosted: Call Guardian Authentication Hub connects via HTTPS and SIP to your existing Perimeta SBC or other SHAKEN-ready network element