

Robocall Mitigation

Cloudtel is an interconnected VoIP provider offering hosted PBX and SIP trunking to enterprises of all sizes. Our customers are exclusively business end-users; we do not offer services to other telephone service providers or individuals. Our customers interconnect with us over the public Internet using their own broadband service.

Know Your Customer:

Each Cloudtel customer must provide a physical business address, business registration, and name and contact information for at least one responsible individual. The business must have a web presence and contact email must be a domain dedicated to the business. The business must be registered in a US state or territory. Payment must be via credit card or US bank transfer or Check. We cross-check and verify all these items and refuse to serve customers that are in any way suspicious. we do not serve foreign customers. We have registered all customers with our carrier Inteliquent/Sinch & the number used for caller ID. I am the only person with admin access to phone systems caller ID so no one can change there assigned caller id.

Caller-ID:

Customers port their numbers to Cloudtel. We also can supply new numbers if they wish. All outbound calls must use a Caller-ID from that customer's pool of numbers assigned by us. The only exception is forwarded calls; in these cases, the call must include a DIVERSION header that contains a number assigned to that customer by Cloudtel. These conditions are checked by our switch before the call is sent onward.

CDR Monitoring:

Cloudtel assesses each customer's traffic on a weekly basis. We examine a set of metrics (number of call attempts, answer seizure ratio, average call duration, fraction of calls shorter than 60 seconds), looking for: (a) signs of automated dialing; (b) significant change from that customer's historic usage. Any anomalies result in immediate engagement with the customer to obtain a thorough, definitive explanation. If not resolved within 7 business days, the customer's service is suspended.

STIR/SHAKEN for Wildix, Step by Step

Listed out, the path that STIR/SHAKEN takes on a Wildix system flows like this:

SIP INVITE generation

The originating telephone service provider receives a SIP INVITE, a digital invitation asking the service to give more verification on the call.

Assign attestation level

That same originating provider verifies the call under one of three categories:

Full or A Attestation: The calling party is a number that's authorized to use the calling number, like a subscriber registered with the provider's softswitch.

Partial or B Attestation: The call origination is authenticated, but it's not clear if the caller is authorized to use the number, like a telephone extension for a PBX.

Gateway or C Attestation: The provider can determine where the call was but cannot authenticate the call source, like a call received from an international gateway.

Generate a SIP identity header

Next, the service provider uses an authentication service, such as integrated software or a cloud solution, to create a SIP Identity header. This header is digitally encrypted and contains data like attestation level, calling number, the origination identifier and a timestamp.

Reception

The SIP INVITE is sent to CLASSOUND, where the SIP Identity header is decrypted. Now, CLASSOUND has assurance from the originating carrier that the call was not spoofed.

Initiate verification

Even so, we want to be certain for ourselves, not just take the carrier's word for it. To do so, CLASSOUND sends the SIP INVITE and its Identity header to its own verification service.

Verify the number

That verification service then matches the digital certificate included in the Identity header against what's available from the public certificate repository. The service verifies the call has not been spoofed if all of the following verification steps are successful:

The SIP Identity header is base64 URL decoded and the details are compared to the SIP INVITE message

The public key of the certificate is used to verify the SIP Identity header signature

The certificate chain of trust is verified