Ribbon Call Trust®

Why You Need an Identity Assurance Solution

What do you do when you receive a phone call from someone you do not know or a number you do not recognize? Perhaps you answer it, but far more likely you reject it, send it to voice mail, or just ignore it. We all do this because we are barraged by spam and robocalls and we assume the worst – someone wants to pitch something I do not need or want, or this will be an attempt to defraud me. To put this in context, for just the United States, in February 2020 (source: YouMail Robocall Index), there were 4.8 billion robocalls, equating to almost 15 calls/person with 42% of them defined as spam and another 14% defined as telemarketing.

It would be way more useful, if you knew, in real-time on a per call-basis, that it was from a legitimate source, for legitimate purpose, and had no malicious intent? Accomplishing this is what identity assurance does.

Identity Assurance

To properly provide identity assurance on a real-time, per-call basis, three attributes need to be known:

- Identity – who is the originator?
- Reputation – Is this someone I want to talk to?
- Trust context – where did the call originate?

Identity

The good news is there is a tremendous amount of information available in the telecommunications industry that can be used to sanity check identity. These include sources such as:

- Known subscriber numbers- from the originating network operator
- Do Not Originate Lists – numbers that will never originate calls
- Un-assigned numbers - from industry databases and from individual network operator databases
- Invalid E.164 calling numbers – based on international telephone numbering plans, these are numbers that can be screened out in call processing
- STIR/SHAKEN attestation – US and Canadian industry framework to sign phone calls to attest the identity of call originator

The bad news is a caller´s identity does not address a caller´s intent, so when legitimate numbers are spoofed, it is possible to have a valid identity, but still have calls with malicious intent.

Reputation

In the United States, even if you do not know how it is calculated, everyone with a US-issued credit card has likely heard of a FICO score, a measure of consumer credit risk that is a fixture of consumer lending. Now imagine a reputation score that measures caller intent, that would be the equivalent of a FICO score. The better the score, the more reputable the call is likely to be.

To use reputation as part of identity assurance, it is paramount to be accurate. If you get the reputation of caller wrong, the value of the score might be worthless. This applies in both directions – too good and too poor. What happens when the reputation is too good, but it should be worse so you know when to reject calls from that source? Or what happens when the reputation is too poor, but it should be better, so the terminating end knows they want to accept calls.

Trust Context

To understand trust context you need to about the originator's location, where the call enters your network, and what information you have about the originating caller. For example, is the call coming from:

- A known subscriber on a local network interface? These should always be verifiable
- A known subscriber from a peering partner? These might be spoofed
- An unknown subscriber from an international carrier? This is not verified and could be spoofed

Ribbon Call Trust

To address the need to determine and integrate identity, reputation and trust context, Ribbon has designed an identity assurance solution based on the following:

- Create an ecosystem enabling multiple, highly scalable, secure, hosted identity assurance services
- Use configurable and dynamic machine learning (ML) models for identity assertion, based on multi-source data integration. These are inferred behavior models with iterative learning to adapt to new network conditions, traffic patterns, and data sources
- Open APIs to receive, and respond to, real-time queries
- Open data integration to support real-time queries of 3rd party transactional policy information, such querying a Calling Name database
- Open data integration to collect or receive non-real time data, such as;
  - 3rd party policy – crowdsourced, carrier-based, or publicly maintained spam/robocall databases. The more data the models have, the more accurate the identity assurance results will be
  - Fraud information from Ribbon Analytics or 3rd party customer analytics solutions that support a REST API. Ribbon Analytics analyzes network behavior and traffic patterns in order to detect potential fraud attempts and provide a list of those originating numbers into the identity assertion modeling
- Take advantage of public cloud infrastructure to handle massive real-time processing with very low latency, because identity assurance decisions (the output of the models) have to be available on a per-call basis, without affecting post dial delay
- Robust, high availability architecture because identity assurance is in the call path

Figure 1 shows the high-level solution architecture of Ribbon Call Trust, a comprehensive identity assurance solution.

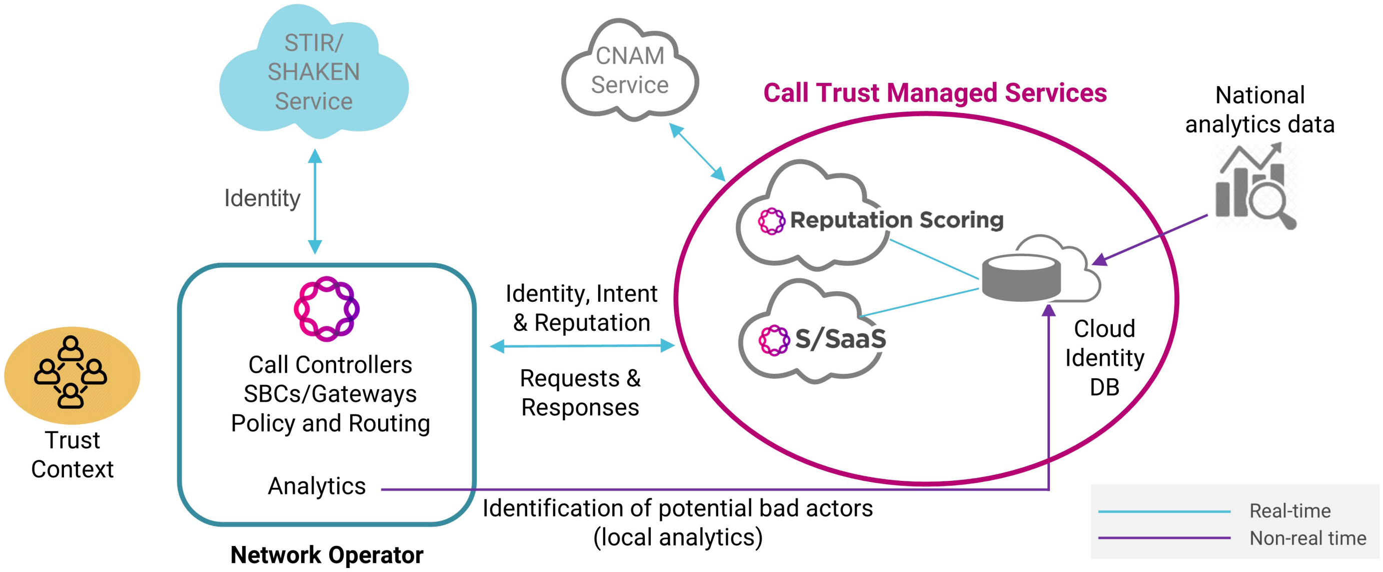

Figure 1 – Ribbon Call Trust Architecture

Figure 2 takes the same architecture and overlays each of the Ribbon products that make up the Ribbon Call Trust solution.

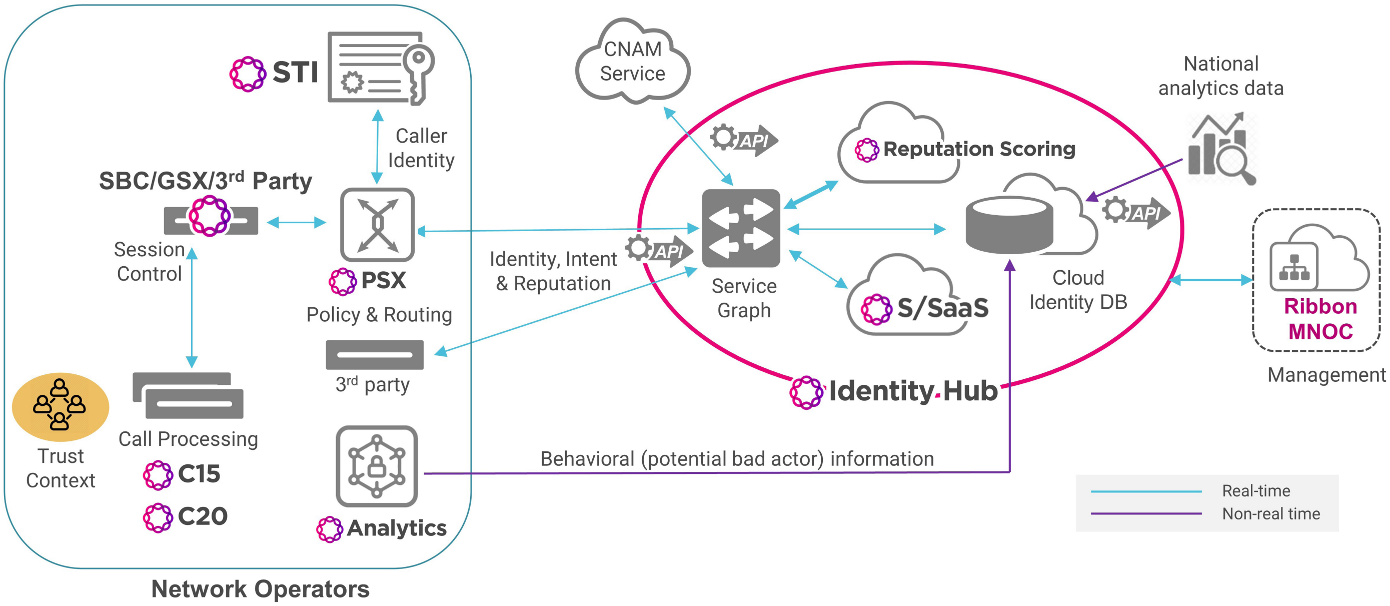

Figure 2 – Ribbon Call Trust Components

Ribbon Call Trust is comprised of the following components:

Session Border Controllers/Gateways – handling SIP-based session control. In the originating network, the SBC will initiate a request for call authentication as part of STIR/SHAKEN or initiate a request for call scoring as part of originating robocall mitigation. It will also process the response it receives. For STIR/SHAKEN it will forward the signed call information to the next network hop. For originating robocall mitigation it will use the information to perform call validation treatment, such as blocking or allowing the call to proceed. In the terminating network the SBC supports STIR/SHAKEN by initiating a request for call verification or it can initiate a request for call scoring as part of terminating robocall mitigation.

In the terminating network, it is also possible for the SBC to receive specific instructions from the PSX for call validation treatment, such as block a call, route a call to a specific destination, or complete the call as normal.

Policy and Routing Server – in an originating network, the policy and routing engine receives call authentication requests from SBCs/Gateways and sends call authentication/signing request to a Secure Telephone Identity (STI) authentication service. The PSX will receive signed call information from STI and forward that information back to the SBC/Gateway, to be sent onward to the terminating network. Similarly, the PSX receives reputation scoring requests from an SBC and and forwards a query to Ribbon's Reputation Scoring service. Based on the reputation score(s) associated with a call, the PSX determines the appropriate call validation treatment and instructs the SBC to implement it. In a terminating network the PSX will receive a verification request from SBCs/Gateways and send a verification request to a STI verification service and receive the STI response with caller ID verification information, which it forwards to the SBCs/Gateways. A similar process occurs where the PSX receives reputation scoring requests from an SBC and and forwards a query to Ribbon's Reputation Scoring service. Based on the reputation score(s) associated with a call, the PSX determines the appropriate call validation treatment and instructs the SBC to implement it.

Call Controllers (C15 and C20) – provides call processing and the call trust context to tag (attest) originating caller ID and send SIP INVITE to SBCs. Also supports receipt of SIP messages from SBCs with signed call information for call termination. For originating robocall mitigation, it is possible for the call controller to directly send a SIP INVITE message to Ribbon Identity Hub for reputation scoring and call validation treatment.

Secure Telephone Identity (STI) – is a complete turn-key STIR/SHAKEN-compliant solution for call authentication, signing, verification, and certificate management. As shown on Figure 2, Ribbon STI can be deployed in a service provider's network or as part of STIR/SHAKEN as a Service, hosted by Ribbon. When a service provider deploys Ribbon STI within their own network, the STI Certificate Authority (STI-CA) and STI Certificate Repository (STI-CR) functions will be hosted as part of Ribbon's STIR/SHAKEN as a Service. Ribbon's STIR/SHAKEN as a Service is appropriate for service providers who do not want to own, deploy, and manage their own STIR/SHAKEN solution, but would rather subscribe to a complete solution for caller identity authentication, signing, verification, and certificate management on a consumption basis.

Ribbon Analytics – with access to network data, such as call detail records and call traffic KPIs, Ribbon Analytics security applications analyze this data to detect and identify potential bad actors. Information on potential bad actors is forwarded to Ribbon Identity Hub for inclusion in the identity assertion modeling.

Reputation Scoring Service – is Ribbon's cloud-hosted service that provides one or more reputation scores for every call, in real-time. Using national analytics data and localized analytics data (available from Ribbon Analytics), Reputation Scoring service assigns reputation score(s) that indicate the likelihood that a call is legitimate, malicious, or somewhere in between. With these reputation scores, call validation treatment (what to do with the call) can be determined based on policy rules. For example, if a call is identified as being legitimate, it should be allowed to proceed; if it is clearly malicious it should be blocked; and if it is in the gray area in-between other call validation options should be used for call treatment. These options might include: route the call to a voice mail server, route the call to announcement server to indicate the call cannot be completed, or placing "likely spam" in the Caller ID field.

STIR/SHAKEN as a Service – is Ribbon's cloud-hosted service that provide a complete STIR/SHAKEN-compliant solution for call authentication, signing, verification, and certificate management.
This service is comprised of the following:

- Secure Telephone Identity - Authentication Service (STI-AS) and the associated functions of Service Provider Key Management Service (SP-KMS) and Secure Key Store (SKS) to process originating network requests for signed assertion of caller's identity
- Secure Telephone Identity - Verification Service (STI-VS) and the associated function of Secure Telephone Identity Certificate Repository (STI-CR) to process terminating network requests for certificate verification of a caller's identity.
- Secure Telephone Identity – Certificate Authority (STI-CA) providing the following capabilities:
  - Accept SHAKEN Certificate Signing Requests (CSRs) for new certificates
  - Automatically validate Service Provider Code (SPC) Tokens and issue standards-compliant SHAKEN signing certificates that include the required Telephone Number Authorization List extension.
  - Revoke certificates if needed and notify the Secure Telephone Identity – Policy Administrator (STI-PA)

Ribbon Identity Hub – is a cloud-native SaaS platform enabling Ribbon's identity assurance services: Ribbon provides STIR/SHAKEN as a Service and Reputation Scoring service. Ribbon Identity Hub leverages configurable and dynamic machine learning models with open APIs and data integration incorporating both real-time and non-real time data from Ribbon and 3rd parties.

In summary, Ribbon Call Trust can determine, in real-time and on a per-call basis, caller identity, intent, and reputation. This means it is possible for a network operator to address their end customer's questions outlined above – is the call from a legitimate person, for legitimate purpose, and without malicious intent? With Ribbon Call Trust, network operators have the comprehensive identity assurance solution they need to restore their customer's trust in the phone again.