STIR / SHAKEN

Cómo evitar la suplantación de identidad en llamadas telefónicas

Introducción

Las llamadas automáticas (robocalls) son la principal fuente de reclamaciones de los consumidores norteamericanos ante la FCC, organismo regulador de las comunicaciones en los Estados Unidos. Lo que inicialmente eran simples llamadas molestas, se han transformado en una plaga para los consumidores. quienes en enero de 2022 recibieron aproximadamente 3,9 mil millones de llamadas automáticas; es decir, 12 llamadas automáticas por persona al mes. Aproximadamente el 32% de estas llamadas fueron consideradas intentos de estafa[1].

La FCC permite a los operadores de telecomunicaciones bloquear llamadas identificadas como fraudulentas, pero la mayoría de las telecos prefiere dejar la decisión al cliente final. El bloqueo de las llamadas automáticas podría solucionar parcialmente el problema, pero otro aspecto es la detección de las llamadas realizadas por agentes maliciosos suplantando la identidad de otros (spoofing) para aprovecharse de consumidores desprevenidos. Estos agentes maliciosos usan tecnologías baratas y sencillas para modificar el identificador de llamadas telefónico e intentar estafar a sus víctimas.

Muchos operadores de telecomunicaciones usan aplicaciones propias o de terceros para bloquear llamadas o verificar la identidad del llamante. Sin embargo, el foco regulatorio y de la industria en Norteamérica ha estado en la autenticación, firma y verificación del identificador de llamadas telefónico utilizando el estándar STIR/SHAKEN.

Este documento es una introducción al estándar STIR/SHAKEN y proporciona detalles sobre las soluciones de Ribbon para que los operadores de telecomunicaciones implementen STIR/SHAKEN.

Definiciones:

- **STIR** (Secure Telephony Identity Revisited), es el estándar propuesto y desarrollado por el IETF que define la firma que autentica el número llamante y específica cómo se transporta entre operadores a través del protocolo de señalización SIP.
- **SHAKEN** (Signature-based Handling of Asserted information using toKENs) es el procedimiento desarrollado por el ATIS/SIP Forum-NNI para detallar cómo los operadores de telecomunicaciones deben implementar STIR. STIR/SHAKEN es la base para la verificación y clasificación de llamadas, para que los abonados recuperen la confianza en la veracidad del identificador de llamadas telefónico.

[1] https://robocallindex.com

Autenticación del abonado llamante

El objetivo de STIR/SHAKEN es mitigar las llamadas automáticas (robocalls) no deseadas y frenar a los agentes maliciosos que suplantan la identidad de otros mediante el uso de su identificador de llamadas telefónicas (spoofing), para realizar intentos de estafa a consumidores desprevenidos.

STIR mejora el protocolo SIP introduciendo el mecanismo para que los operadores de telecomunicaciones verifiquen la legitimidad del origen de una llamada VoIP (voz sobre protocolo IP) y garanticen que no es una llamada con identidad suplantada.

Con estas mejoras se quiere conseguir que agentes maliciosos tengan mucho más difícil suplantar la identidad de otros con fines fraudulentos o ilegítimos. Ejemplos de estas actividades son llamadas telefónicas suplantando la identidad de empresas o entidades públicas (bancos, aseguradoras, eléctricas, Seguridad Social, Agencia Tributaria…) que buscan conseguir información personal, verificación de tarjetas de crédito, cuentas bancarias y otros intentos de fraude económico mediante el engaño a los consumidores. Con la suplantación de identidad, estos agentes maliciosos consiguen saltarse las listas de números bloqueados por los operadores de telecomunicaciones.

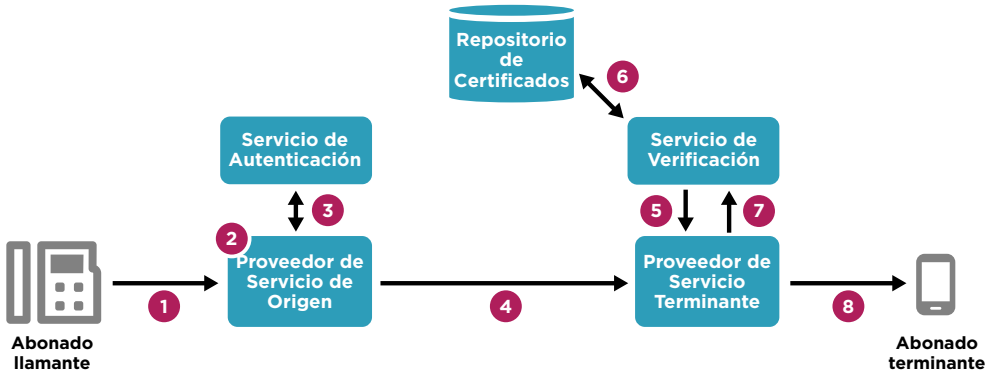

Figura 1: Flujo de llamada ilustrando cómo funciona STIR/SHAKEN

STIR mitiga estos problemas, pero no es el 100% de la solución. Es más, STIR no funciona en todos los escenarios de llamadas. La siguiente tabla es un resumen de todos los escenarios de llamadas y la contribución de STIR a la mitigación del problema de la suplantación de identidad telefónica.

Escenarios de llamadas STIR en los EE.UU.

Red de origen	Red de destino	Mitigación de la suplantación de identidad
PSTN	PSTN	Sin impacto
SIP-Nacional	SIP-Nacional	Alto impacto
SIP-Nacional	PSTN	Impacto medio
PSTN	SIP-Nacional	Bajo impacto
SIP-Internacional	PSTN	Bajo impacto

IEn resumen, STIR comenzó en los EE.UU para abordar la suplantación de identidad en redes con señalización SIP. De momento debido al mecanismo de autenticación es una solución centrada en los EE.UU. porque se basa en la confianza en una Autoridad de Certificación que emite las credenciales de firma. Esto es un aspecto político, no tecnológico. Como tal, requiere un acuerdo o regulación de la industria, que debe ser abordado por las diferentes autoridades de telecomunicaciones nacionales. Más allá de los EE.UU., Canadá ha emitido regulación que obliga a la implementación de STIR/SHAKEN y muchos otros países están evaluando el uso de STIR/SHAKEN por sus operadores de telecomunicaciones.

STIR/SHAKEN no aborda llamadas con origen, tránsito o finalización en tecnología telefónica basada en TDM. Sin embargo, considerando que el TDM aún permanece en muchas redes de telecomunicaciones, la industria ahora está trabajando en definir soluciones que extiendan STIR/SHAKEN sobre TDM.

Ribbon Call Trust™ para implementar STIR/SHAKEN

Call Trust es el conjunto soluciones de Ribbon para garantizar la Identidad de las llamadas siguiendo el estándar STIR/SHAKEN. Los productos de Ribbon aplicables para STIR/SHAKEN son SBC (Session Border Controllers), PSX (Policy and Routing Server), GSX (Gateway TDM/IP), Call Controllers y STI (Secure Telephone Identity).

Se ha validado que los SBC, PSX y GSX de Ribbon cumplen los estándares de autenticación de llamada desarrollados por el IETF y el ATIS: TLT-2018-00010 (STI Test Plan) y Servicios de Autenticación y Verificación.

[2] https://s2erc.georgetown.edu/sites/s2erc/files/files/upload/stir_status_and_analysis.pdf

La solución STI de Ribbon aborda estas funciones específicas:

- STI-AS (Secure Telephone Identity - Authentication Service), SP-KMS (Service Provider - Key Management Service) y SKS (Secure Key Store) para que un operador de telecomunicaciones realice la firma de llamadas autenticadas. Esta función se realiza desde el lado originante de la llamada.
- STI-VS (Secure Telephone Identity - Verification Service) y STI-CR (Secure Telephone Identity - Certificate Repository) para que un operador de telecomunicaciones verifique la firma de llamadas autenticadas. Esta función se realiza desde el lado terminante de la llamada. Nota: Ribbon puede proporcionar la función STI-CR como un servicio proporcionado desde la nube, denominado Ribbon Identity Hub.
  - STI-CA (Secure Telephone Identity – Certificate Authority) es un servicio proporcionado desde la nube, denominado Ribbon Identity Hub, que proporciona las siguientes funcionalidades:
    - Aceptar solicitudes de firma (CSR: Certificate Signature Request) de nuevos operadores de telecomunicaciones siguiendo el estándar SHAKEN.
    - Validar códigos de proveedores de servicios (Service Provider Code tokens) y emitir certificados de firma SHAKEN a operadores de telecomunicaciones que hayan solicitado nuevos certificados (CSR: Certificate Signature Request), con sus correspondientes Listas de Números Telefónicos Autorizadas.
    - Revocar certificados, si es necesario y notificar a la entidad regulatoria STI-PA (Secure Telephony Identity – Policy Administrator).

Como se muestra en la Figura 2, en la red de origen la llamada de un operador de telecomunicaciones hay haber un SBC (o un servidor de llamadas) que genera una solicitud de autorización al PSX. Luego el PSX interactúa con el STI-AS de Ribbon. Cabe destacar que el PSX podría trabajar con cualquier solución STI ATIS-82 certificada. El STI de Ribbon proporciona todas las funciones y servicios requeridos para la autenticación de la llamada originante y la firma correspondiente, respondiendo de esta manera a la solicitud del PSX. El PSX recibe la información de firma y la devuelve al SBC (o servidor de llamadas) para que la llamada progrese al siguiente elemento de la red telefónica.

En la red del abonado terminante de la llamada, el SBC (o servidor de llamadas) generará una solicitud de verificación y la enviará al PSX para que llegue hasta la función de STI. El STI de Ribbon proporciona todas las funciones y servicios requeridos para la verificación de la identidad del originante de la llamada y luego responde al PSX. El PSX recibe la información de verificación y la devuelve al dispositivo que la ha solicitado (SBC o servidor de llamadas).

Los SBC, GSX y servidores de llamadas de Ribbon, soportan el manejo flexible de indicaciones de error; por ejemplo, “rechazar la llamada”, “continuar con la llamada”, “continuar con la llamada y eliminar la cabecera de identidad” si la verificación de firma falla.

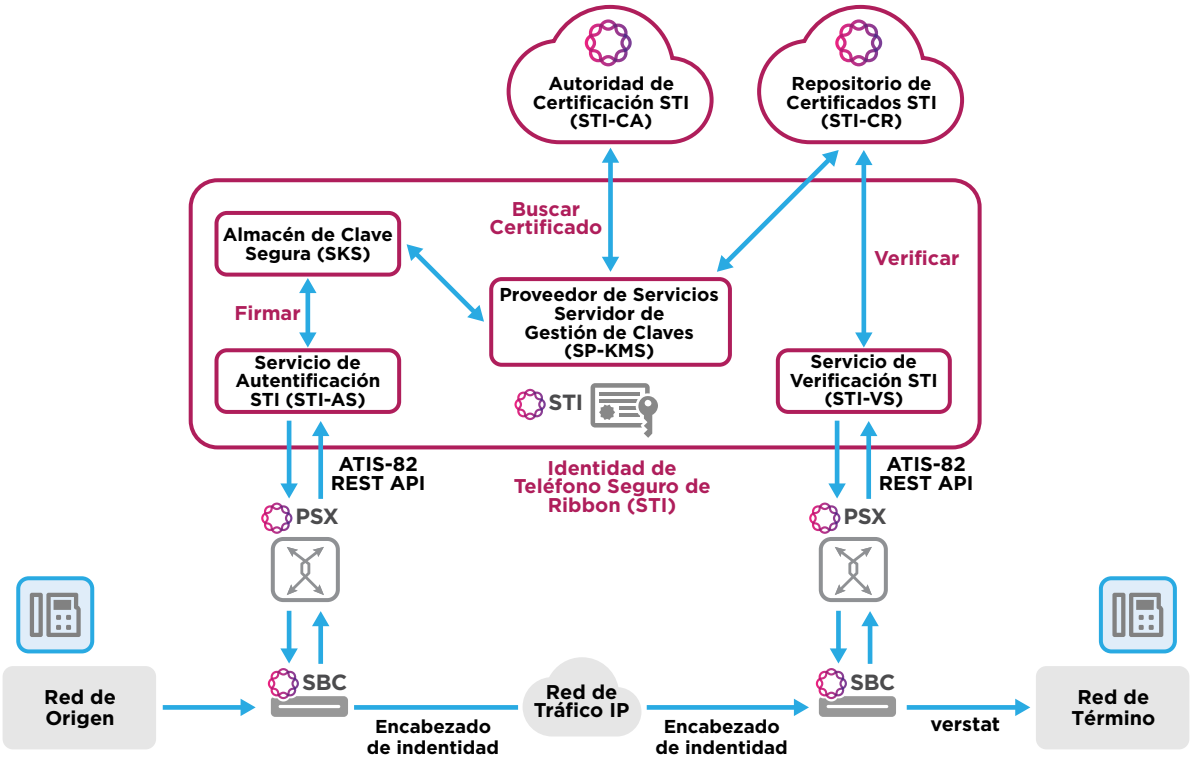

Figura 2. Implementación de STIR/SHAKEN Ribbon

Resumen

A pesar de que muchos operadores utilizan aplicaciones propias o de terceros para ofrecer el bloqueo de llamadas y la verificación de la identidad del abonado originante, no existe una solución sencilla para garantizar la veracidad de la identidad del abonado llamante. Ribbon es líder en este área tecnológica con la solución Ribbon Call Trust que permite autenticar y verificar la identidad del abonado llamante en cumplimiento del estándar STIR/SHAKEN. Esto permite mitigar las llamadas automáticas (robocalls) fraudulentas y ayuda a los operadores de telecomunicaciones para que los usuarios finales recuperen la confianza en las llamadas telefónicas recibidas.