

Robocall Mitigation Plan
GLOBE TELECOM, INC.

GLOBE TELECOM, INC. ("GLOBE"), of the Philippines, as a foreign voice service provider, submits the following Robocall Mitigation Plan consistent with 47 CFR § 64.6305(d)(ii)-(iii).

Reasonable Steps to Prevent New and Existing Customers from Originating Illegal Calls:

As stipulated in the Subscription Agreement, Globe may suspend or terminate the Service if it reasonably suspects that a subscriber, directly or indirectly, engages in any fraud either by himself/herself or with any other person in connection with the Service.

In the same Agreement, Globe likewise reserves its right to redirect, bar or temporarily disconnect subscriber's telecommunication services in case of abnormal or unusual high usage patterns, fraud, or other similar cases.

Description of Analytics to Block Illegal Traffic:

Globe has deployed Session Initiation Protocol Firewall (SIP FW) both in our International and Domestic interconnects with our partners SMSGT/Mobileum using an Active Intelligence platform to monitor, detect, and block malicious incoming traffic to our network.

Know Your Customer Practices:

Globe, in compliance with Republic Act No. 11934 otherwise known as the "SIM Registration Act", requires all its existing and new subscribers to register their SIM with their full name, date of birth, and sex, among others. Subscribers are also required to present a valid government issued ID or other similar forms of documents with photo that will verify the identity of the end user. With the implementation of SIM Registration Act, Globe can easily identify and track subscribers tagged in any suspicious activity monitored in the network.

Other Practices to Prevent Unlawful Calls:

Globe can block identified malicious incoming calls using the SIP FW.

For unlawful calls originating from Globe's network, Globe can likewise deactivate identified subscribers using the Fraud Management System Tool.

Know Your Upstream Provider Practices:

This is not applicable to Globe since we have no upstream providers.

Commitment to Respond to Traceback Requests:

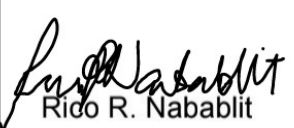
GLOBE is willing and able to respond fully and within twenty four (24) hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

This Robocall Mitigation Plan describes the specific measures that GLOBE has implemented to as of **26 FEBRUARY 2024**. GLOBE continually evaluates the efficacy of its measures to combat bad actors and takes appropriate steps to improve these measures when needed.



Project STIR-SHAKEN

SOLUTION PLAN

Prepared By:	Reviewed By:	Recommended By:	Approved By:
 Roldan V. Fajarit Solution Designer ISDP/Signaling Security/RDD	 Christopher P. Buaya Head RDD Signaling Security	 Rido R. Nabablit Head Signaling Security	 Anton M. Bonifacio Head ISDP
DATE: 01-15-2021	DATE:	DATE:	DATE: 03-05-2021

Revision History

VER NO.	DATE OF RELEASE	PREPARED BY	REVIEWED BY	LIST OF CHANGES FROM PREVIOUS VERSION
0.0	01-15-21	Roldan Fajarit		Document creation
0.1		Roldan Fajarit		

Contents

1.0 Demand Information	4
2.0 Executive Summary	4
3.0 Requirements Definition	6
4.0 Analysis	8
A. Solution	8
5.0 Solution Description (A to C to be documented per User/Customer story)	9
A. Logical Architecture	9
B. NTG Network	12
C. Process Flows	15
Hardware Process Flow	15
Software Process Flow	16
D. Impact Assessment	16
E. Solution Details	16
F. Capacity Assessment	17
G. Physical Architecture	17
Physical Architecture of the solution is as shown below:	17
H. Security	17
I. Technical Bill-of-Materials (BOM)	18
J. Engagement Model	19
K. Testing Strategy	20
SAT/UAT	20
6.0 Implementation Timeline	20
A. Delivery Duration	20
7.0 Callouts and Risks	21

1.0 Demand Information

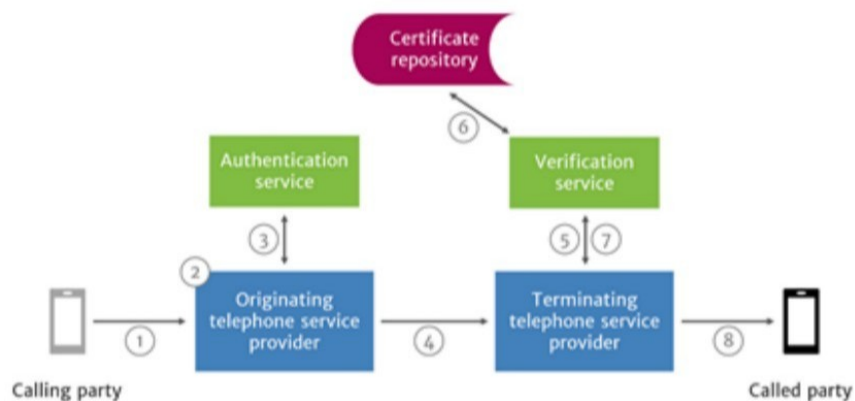
NAME	Project STIR-SHAKEN
SOLUTION DESIGNER	Roldan Fajarit
SOLUTION ARCHITECT	Christopher Buaya
SPONSOR	Rico Nabablit
DESCRIPTION	This project aims to validate incoming international calls while also securing our outgoing international calls and enhance our existing SIP FW International to combat Robocalling and CLI Spoofing attacks by using digital certificates
LEVEL OF COMPLEXITY	☐ Rollout ☐ LOW ☐ MEDIUM ☒ HIGH ☐ COMPLEX
TARGET RFS	June 2021

REFERENCES			
Ref.	Title	Version	Author
1	SMSGT_Stir&Shaken Proposal	V8.0	SMSGT
2	STIR-SHAKEN Technical Proposal for Globe 10th June 2020	V1.0	Mobileum
3			
4			
5			
6			
7			

2.0 Executive Summary

It was reported that robocallers scammed customers of about \$10.5 Billion in 2018. Quite alarming as it is fast increasing at an 18% rate globally. In the US alone, robocalls were found to have increased by as much as 35%. Thus, last year of June 2019, a new bill of the US Congress became into law, the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act or also known as the TRACED Act law. This bill requires voice service providers to develop call authentication technologies, thus Secure Telephony Identity Revisited/ Secure Handling of Asserted information using toKENs (STIR/SHAKEN) will be used. As the FCC, Federal Communications Commission, in America will be strictly enforcing this to their operators come June 2021, those operators who wish to call connect to them must also support the same security capabilities.

In 2018, Globe subscribers experienced a huge amount of Robocalls attacks that were found to be coming from different countries. Interim solution was done in the international gateway through blocking of A-numbers. This leads to the establishment of SIP FW International for auto-blocking of those fraudulent calls (IRSF, Wangiri, DoS and PBX hacking attacks were also supported). Moving forward and to enhance our capability of blocking, STIR/SHAKEN solution will be supported by the network. This will give our network the capability to validate and fully authenticate each call and at the same time will appease our subscribers that their calls are secured and verified.



High Level Call Flow of STIR/SHAKEN

Table 2.1: Cost Assessment Summary

COST TYPE	CCY	AMOUNT
Hardware	PHP	<i>Details upon request</i>
Software	PHP	<i>Details upon request</i>
Services	PHP	<i>Details upon request</i>
TOTAL	PHP	<i>Details upon request</i>

Table 2.2: Timeline Assessment Summary

ACTIVITY MILESTONES	DURATION	DATE
PO Received		Jan 2021
Hardware Delivered		
Integration Complete		
SRA Complete		
Testing Complete		
Provisional Acceptance		
Final Acceptance		

3.0 Requirements Definition

Table 3.1: User Stories

Demand Story		Remarks	Sub-Category	Mandatory (y/n)
DS1	Outgoing SIP international calls authentication	- Solution is to add identity header field and Authenticate the user - Call is assigned with private keys - Tested working using different operators	Enhancement	Y
DS2	Incoming SIP international calls validation	-Solution is to validate the certificate and verify the signature in the Identity header field, which validates the Caller ID	Enhancement	Y

		- extracts the public key from the call - Tested working using different operators		
DS3	Attestation classification	STIR/SHAKEN must ensure attestations for all calls. Test Attestation (Type A, B, C).	Enhancement	Y
DS4	SIP international FW, through its analytics, should provide next level validation after STIR/SHAKEN authentication	SIP Int'l FW to perform call spam analytics or other mitigation techniques, to provide additional Call Validation after the STIR/SHAKEN validation.	Strategic	Y
DS5	Ability to enable/disable STIR/SHAKEN	An option to enable/disable STIR/SHAKEN depending on the operators supporting the service	Strategic	Y
DS6	Reports availability	-STIR/SHAKEN reports must be available. Reports can be downloaded in CSV, PDF, PPT format. - STIR/SHAKEN reports of Count of STIR/SHAKEN calls - successful and unsuccessful - STIR/SHAKEN reports of Operator/Location of incoming and outgoing calls processed -successful and unsuccessful -STIR/SHAKEN reports of Count based on attestation levels - STIR/SHAKEN reports of List of blocked numbers with the count of number of attempts made	Enhancement	Y

DS7	FCC compliance	Globe ensures compliance to the call from FCC to deliver ATIS standards of caller ID authentication through STIR/Shaken protocol. Target RFS is on June 2021	Compliance	Y
DS8	Secure calls	Blocked spoofed/spam/fraud calls in real-time for the incoming/outgoing traffic facing international	Strategic	Y

4.0 Analysis

Unwanted robocalls annoy subscribers and make them reluctant to answer their phones. Robocall perpetrators often alter or spoof the caller IDs to trick the victim into answering the robocall. ATIS (Alliances of Telecommunications Industry Solutions) has developed a way to authenticate calls that will inform the called party that the caller ID has been verified.

STIR/SHAKEN, the framework that will prevent the completion of illegally spoofed calls. The originating service provider will authenticate the call and send a digitally signed Identity token with the call. The terminating service provider will then verify the signature and token. Once successfully verified, the call will get through to the subscriber.

Overall call flow for Caller ID validation looks like below:

- A subscriber makes an outgoing call and caller ID of that call is validated by the service provider.
- Call received by the recipient's CSP
- Termination Service provider verifies caller ID before completing it.
- SIP Firewall (HomePolicy) solution checks, if validated Caller ID is not blacklisted and can apply other defined rules.
- When an authorized call is received, consumers will be confident in answering a call that does not have a spoofed caller ID.

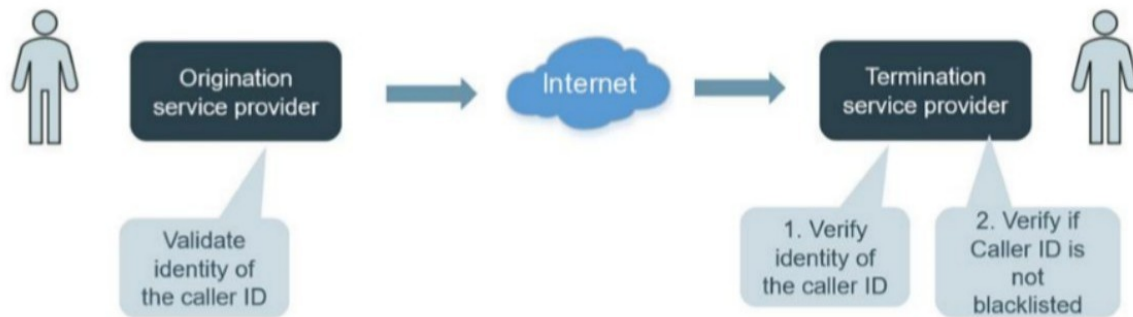
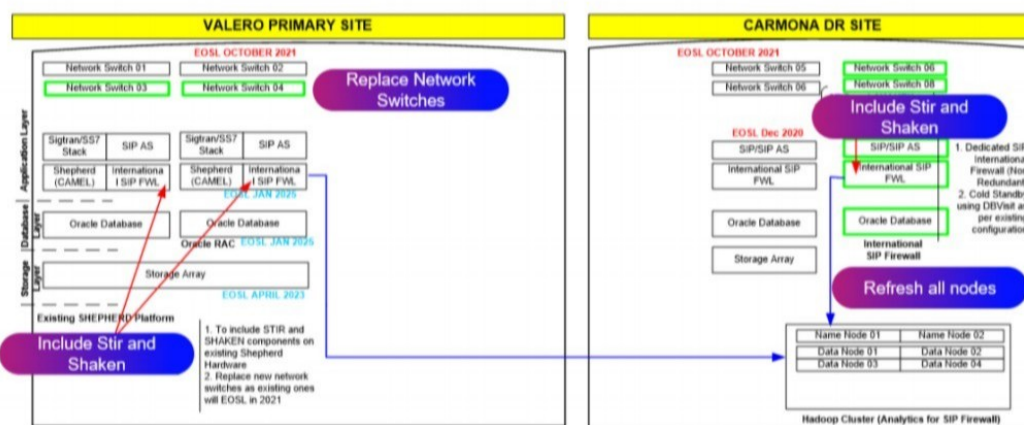


Figure: High-level STIR & SHAKEN approach

A. Solution – SIP International FW enhanced with STIR-SHAKEN capabilities



In Valero site, the network switches will be replaced with new ones to address the nearing EOSL dates of the present switches. In the Carmona site, the existing SIP Firewall will be replaced with new hardware including its network switches. The Stir and Shaken will be installed in the same hardware as the International SIP Firewall

5.0 Solution Description

A. Logical Architecture

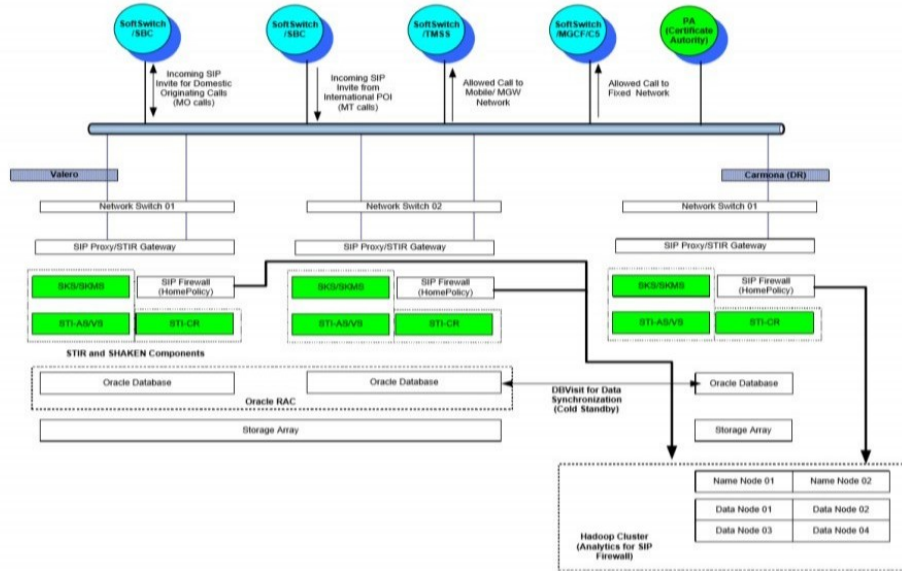
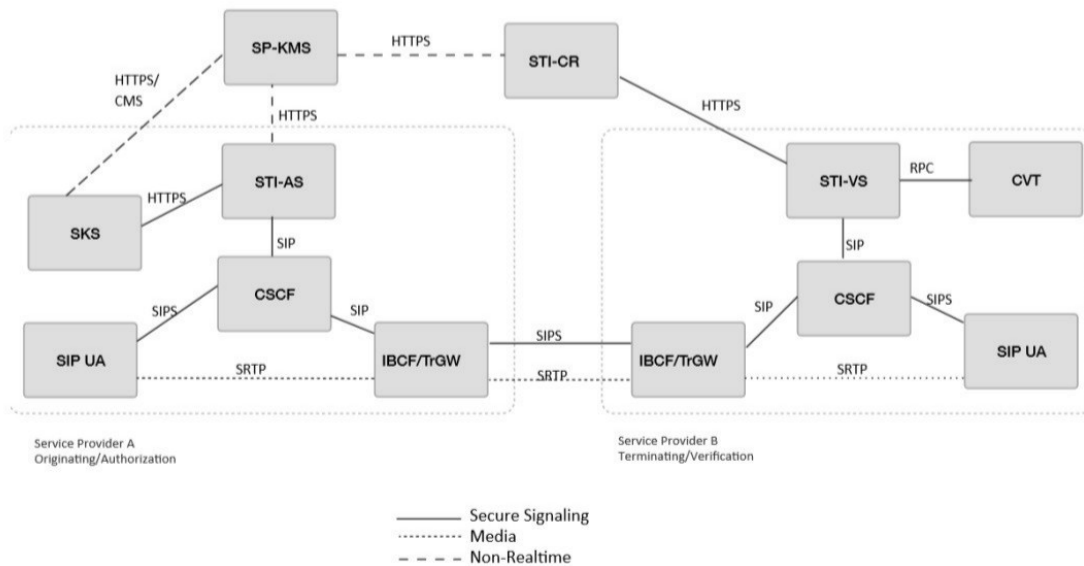
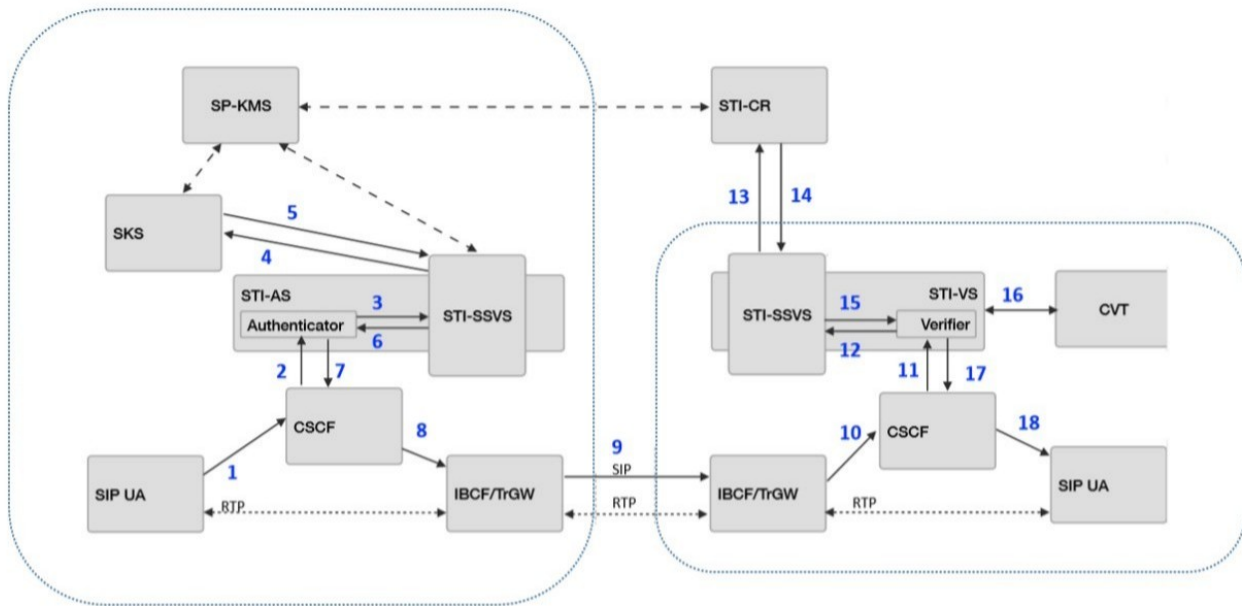


Figure 1. Existing Architecture of the SIP International FW Platform with STIR-SHAKEN

STIR-SHAKEN Basic Architecture



STIR-SHAKEN Basic Call Flow



Call Attestation Level Indication

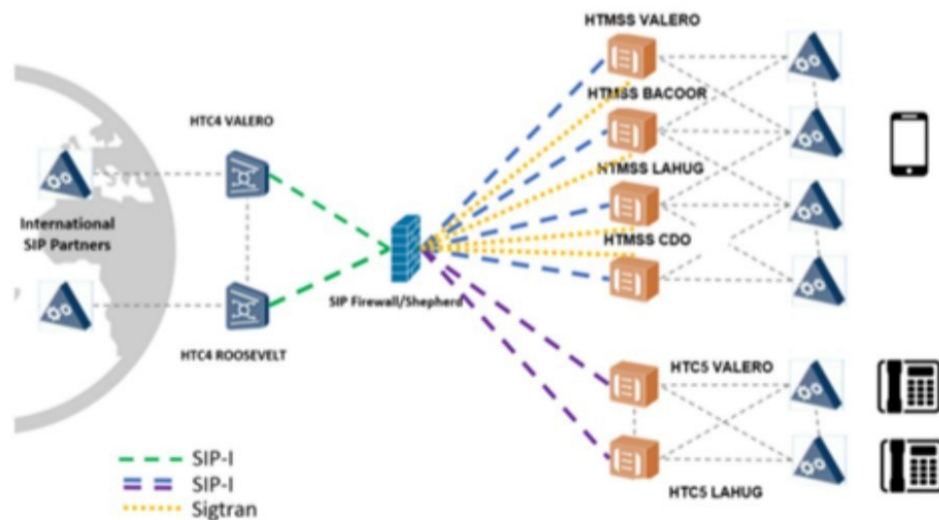
There will be 3 classifications of call attestation for STIR/SHAKEN:

- **Full Attestation (type A)** - CSP has authenticated the Calling Party and they are authorized to use the Calling Number. For example, a subscriber attached to the CSP network, or Fixed Line originated call.
- **Partial Attestation (type B)** - CSP has authenticated the call origination but cannot verify that the call source is authorized to use the Calling Number. For example, via SIP trunks to enterprises which have multiple numbers.
- **Gateway Attestation (type C)** - CSP has authenticated where it has received the call from but cannot authenticate the source of the call. For example, a call received on Interconnect links

B. Deliverable Matrix

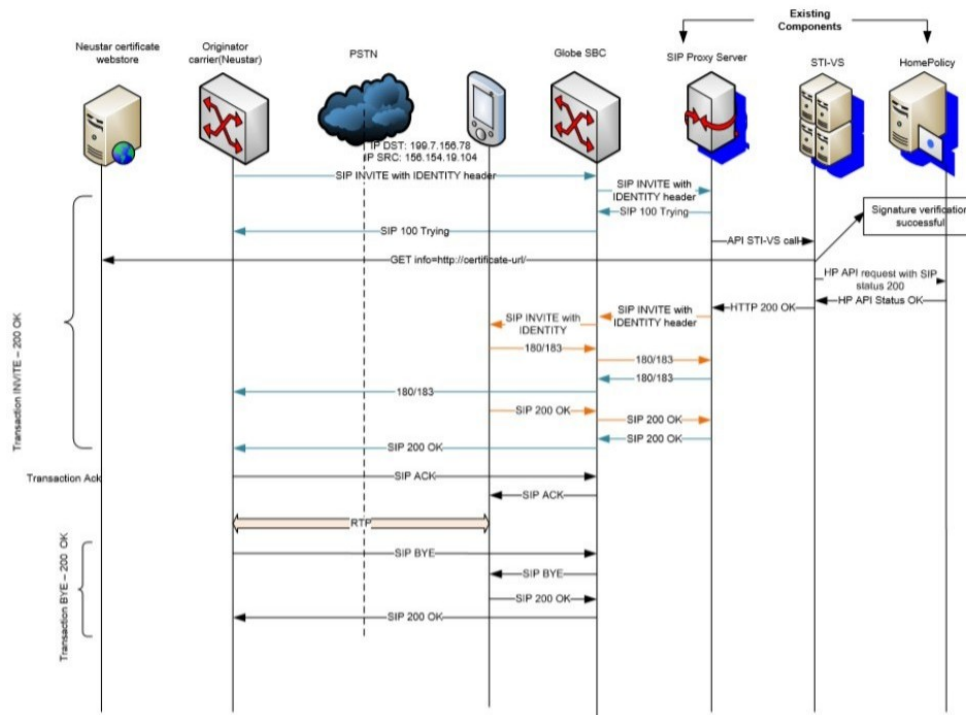
SR	Items	Proposed Physical Setup
Software Features		
1	Camel based HomePolicy (Shepherd) for Borderless Plans	Yes (existing Function)
2	SIP Firewall for Robocalling	
	- International Calls	Yes (existing Function)
3	STIR and Shaken for international Outgoing and Terminating Calls	Yes (To be hosted in existing Shepherd Hardware and DR Site on new hardware)
Dimensioning and Capacity		
4	SIP International Calls	900,000 BHCA or 250 CPS
5	STIR and Shaken for international Outgoing and Terminating Calls	900,000 BHCA or 250 CPS
Infrastructure		
Valero Site (Primary Site)		
6	International SIP Firewall	Continues to reside on the Shepherd Platform. Refresh network switches that is nearing EOSL
7	Stir and Shaken	To be hosted in the existing Shepherd Platform
Disaster Recovery (Carmona) Site		
9	International SIP Firewall	New non-redundant platform (replaces the nearing EOSL Kleen Platform)
10	Stir and Shaken	To be hosted in the new International SIP Firewall Platform (following the primary setup)

C. NTG Network

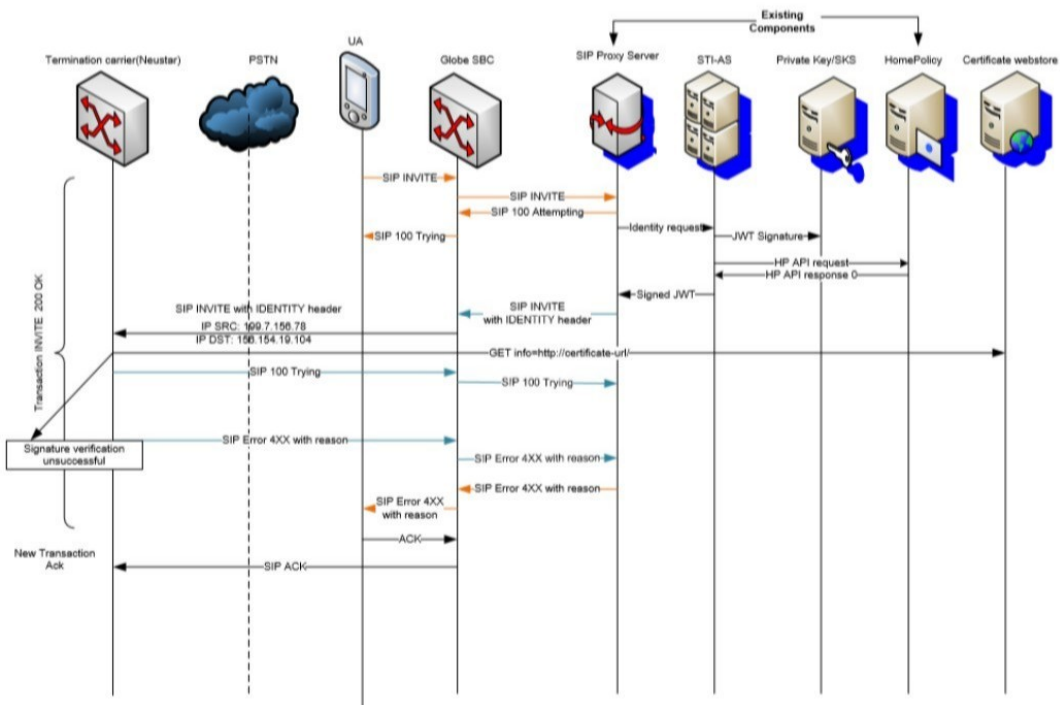


Current NTG Network diagram with SIP International FW

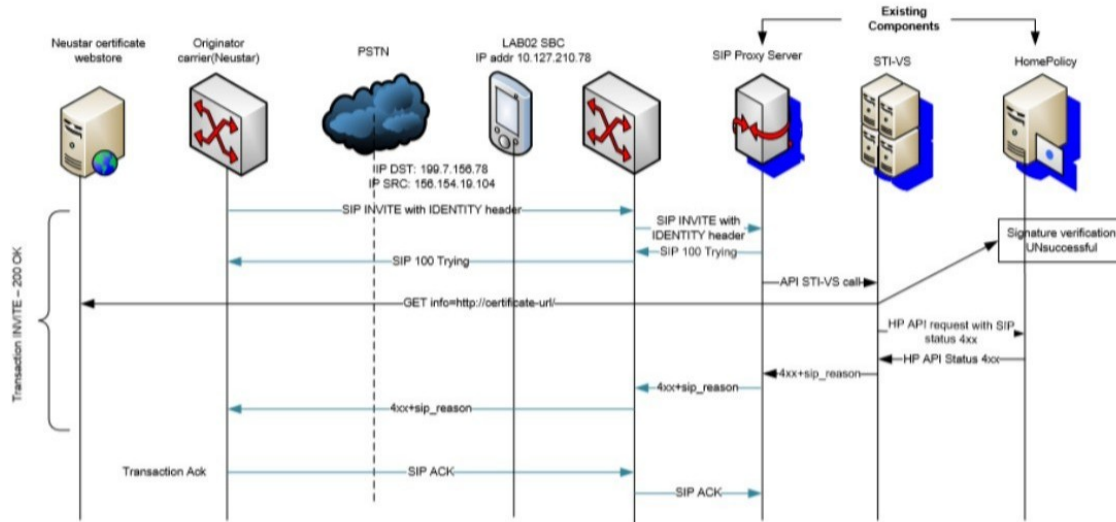
MT Call Flow for Successful Verification



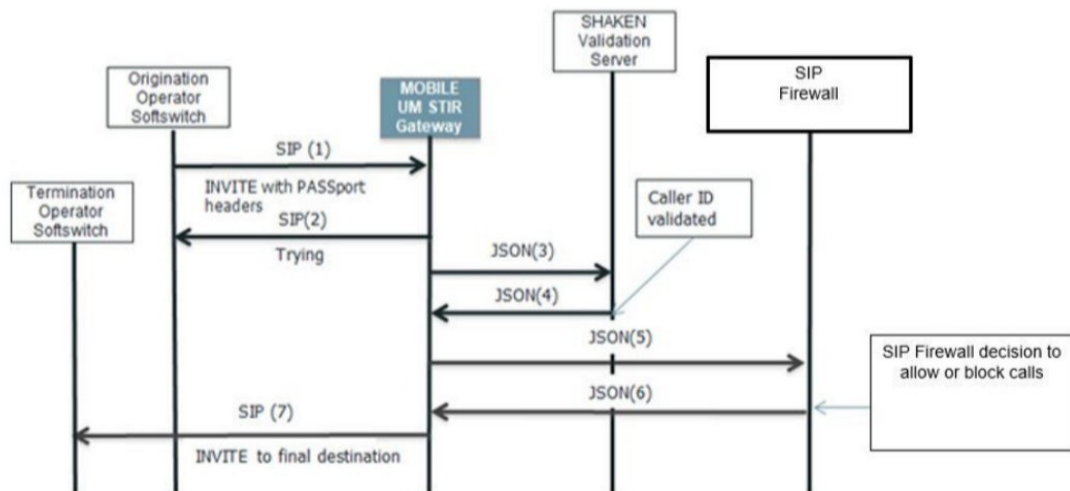
MO Call Flow for Failed Verification (Terminating Side)



MT Call Flow for Failed Verification (Call Reject)



Network Call Flow with SIP International FW



Integration Summary

Elements/Node	Interface/Function	Scope	Implementation Resource
VALERO PRIMARY SITE			
Shepherd Switches	Network Layer 3	Replacement and configuration	SMSGT/ MOBILEUM
Shepherd SIP Int'l FW	Application Servers	STIR-SHAKEN apps installation	SMSGT/ MOBILEUM
CARMONA DR SITE (Refresh)			
Kleen Switches	Network Layer 3	Replacement and configuration	SMSGT/ MOBILEUM
Kleen SIP Int'l FW	Application Servers	Replacement and STIR-SHAKEN apps installation	SMSGT/ MOBILEUM
Kleen SIP Int'l FW	DB Server	Replacement and DB installation	SMSGT/ MOBILEUM

D. Impact Assessment

The STIR-SHAKEN solution will have a little impact with the live globe network during its integration. It will utilize the existing SIP Intl FW integrated with our TMSS, C4 and C5 networks. It's expected that only once Mobileum/SMSGT is done with all the configuration, Globe can do rerouting of test numbers to STIR-SHAKEN apps.

All STIR-SHAKEN testing should only proceed with proper coordination and approval from the stakeholders in NTG as the SIP Intl FW is already handling live traffic.

In normal operation, both STIR-SHAKEN will work in Active/Active mode. Both nodes will receive signaling SIP messages from Globe's SBCs. The node that will reply to SIP OPTION message will get all the traffic coming from Globe SBCs.

In conclusion, even though STIR-SHAKEN will just reside in the SIP Int'l FW, the internal communication between the 2 systems will be quite complex. But since both systems were developed by the same vendor, Mobileum, the overall impact to the network should be minimal.

E. Solution Details

INTEGRATION POINT SUMMARY

IML	SOURCE SYSTEM	TARGET SYSTEM	INTERFACE DOMAIN	INTERFACE NAME	INTERFACE DESCRIPTION	NEW/REUSE /ENHANCE
	Shepherd STIR-SHAKEN App	SIP Int'l FW Gateway C4	SIP	Signalling	Interface for SIP Signalling traffic between Mobileum STIR/SKAKEN and Globe SBC	New
	Shepherd STIR-SHAKEN App	SIP Int'l FW App server	Proprietary Mobileum Interface	Application	STIR/SKAKEN functionality will be integrated into the Firewall Application, so no separate integration will be required	New
	Shepherd STIR-SHAKEN App	Certificate Repository STI-CR	ACME	Service		New
	Shepherd STIR-SHAKEN App	STI Policy Administrator STI-PA	https	Service	Interface for validating the certificate of the calling party number as part of STIR/SKAKEN functionality	New
	Shepherd STIR-SHAKEN App	TACACS Server	TACACS	O&M		New
	Kleen STIR-SHAKEN App	SIP Int'l FW Gateway C4	SIP	Signalling	Interface for SIP Signalling traffic between Mobileum STIR/SKAKEN and Globe SBC	New
	Kleen STIR-SHAKEN App	SIP Int'l FW App server	Proprietary Mobileum Interface	Application	STIR/SKAKEN functionality will be integrated into the Firewall Application, so no separate integration will be required	New
	Kleen STIR-SHAKEN App	Certificate Repository STI-CR	ACME	Service		New
	Kleen STIR-SHAKEN App	STI Policy Administrator STI-PA	https	Service	Interface for validating the certificate of the calling party number as part of STIR/SKAKEN functionality	New
	Kleen STIR-SHAKEN App	TACACS Server	TACACS	O&M		New
	Kleen STIR-SHAKEN App	NETCOOL Crosswind MyCOM ICD	SNMP SNMP SFTP Manual	O&M		New

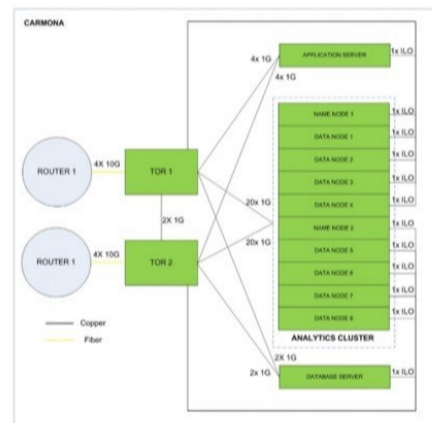
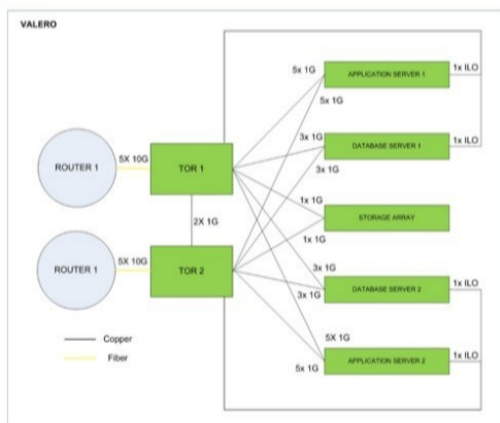
F. Capacity Assessment

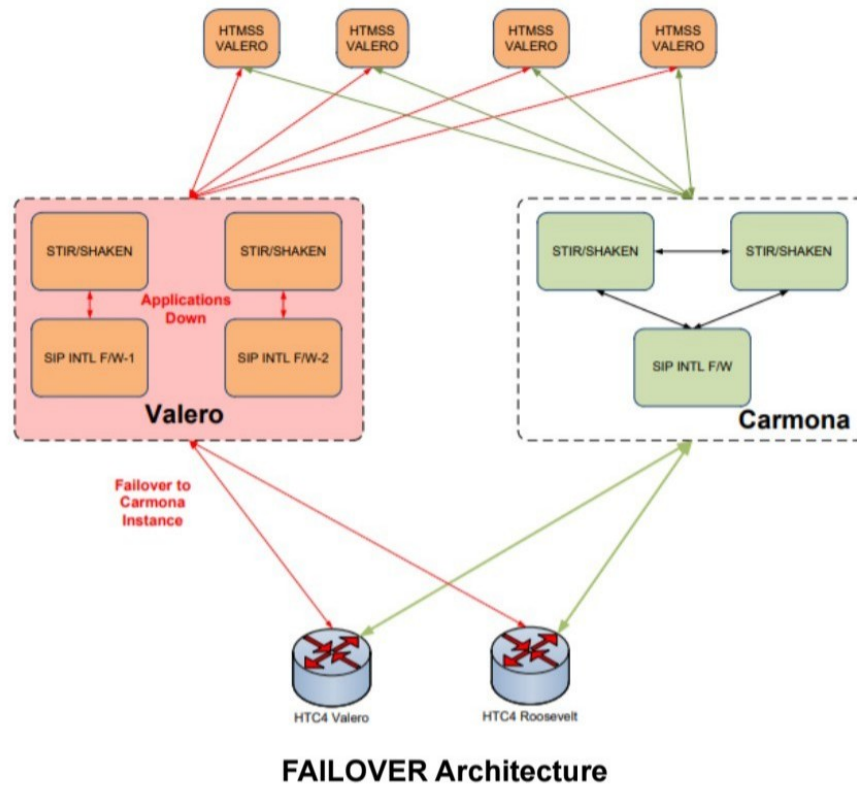
The system is designed to handle the projected BHCA traffic for up to 5 years.

Dimensions	Year 1	Year 2	Year 3	Year 4	Year 5
BHCA	900,000	765,000	650,250	552,713	469,806
CPS	250	213	181	154	131

G. Physical Architecture

Physical Architecture of the solution will be the same as the SIP International FW was set up. STIR-SHAKEN are just modules that will reside together with the SIP International FW components.





H. Security

No impact to SoA (Statement of Applicability)

I. Technical Bill-of-Materials (BOM)

<u>Item</u>	<u>Quantity</u>	<u>Description</u>	<u>Remarks</u>
		CARMONA DR SITE	
1.0	1	Application Server HP DL380, 1x 8 core (2.1GHz+), 16GB RAM, 2x 600GB HDD (with iLO advanced pack lic), 4P 1x GB NIC card Operating System: RHEL server support	

		4x 600 Gb 10K RPM SAS disk to be added into an existing Server HPE 16 Gb RAM upgrade Kit HP Ethernet 1Gb 4-port 331T Adapter	
2.0	1	Database Server HP DL380, 1x 8 core (2.1GHz+), 16GB RAM, 2x 600GB HDD (with iLO advanced pack lic), 4P 1x GB NIC card Operating System: RHEL server support 10x 600 Gb 10K RPM SAS disk to be added into an existing Server 2 X HPE 16 Gb RAM upgrade Kit HP Ethernet 1Gb 4-port 331T Adapter	
3.0	2	Cisco Switch Catalyst 1G/10GB Switches (Layer 3)	
4.0	1	Oracle DB Oracle Database STANDARD EDITION , ASFU, CPU Based perp. License	
		VALERO PRIMARY SITE	
5.0	2	Cisco Switch Catalyst 1G/10GB Switches (Layer 3)	

J. Engagement Model

The installation and integration will be done in a phased approach as stated below.

1. Racking, Installation and Power Up activities related to physical hardware deployment. To start in Carmona site. While live traffic is being served by Valero site - **by SMSGT**.
2. OS Installation, hardening, partitioning, and IP Configuration - **by SMSGT/Mobileum**
3. Network Switches setup and configuration related works - **by SMSGT/Mobileum**
4. Remote connectivity is mandatory for deployment. - **by Globe**
5. STIR-SHAKEN modules will reside together with SIP International FW in Valero and Carmona sites. - **by SMSGT/Mobileum**
6. Refreshed Kleen platform installation will be done in parallel with the current Kleen platform.
7. For SIP International, the DR site will continue to operate as COLD-Standby. It is assumed that the OS, Oracle and DBVisit licenses on the existing Kleen platform in the DR (Carmona) site which today host the SIP International Firewall can be re-used for the new platform.
8. Globe will provide power requirements at appointed sites. SMSGT will be responsible to provide cabling from equipment to power cabinet

9. Once the Carmona site is configured. Test traffic will be routed. Perform SAT - **by Globe/SMSGT**
10. Perform UAT with several operators that will be given by Mobileum. Roaming Ops to do coordination with roaming partners. - **by Globe**
11. Once the new Kleen platform in Carmona site is stable. Shutdown the old Kleen platform - **by SMSGT/Mobileum**
12. To support STIR/SHAKEN the current software version of International Firewall will be upgraded to Voice Policy Engine 2.0. There will be no impact to existing interfaces - **by SMSGT/Mobileum**
13. Replace 1x Network Switch of Shepherd and configure. Ensure that the working configuration of the other Network Switch is applied. - **by SMSGT/Mobileum**
14. Route test traffic on the new installed Network Switch. Perform SAT - **by Globe**
15. Once tested working. Observe and closely monitor for a day. - **by SMSGT/Globe**
16. Once no problem is detected. Replace the 2nd Network Switch of Shepherd in Valero. Apply the working configuration. - **by SMSGT/Mobileum**
17. Route test traffic to the 2nd Network Switch and perform SAT. - **by Globe/SMSGT**
18. UAT test on Valero Shepherd system. - **by Globe/SMSG**
19. Restore all the traffic in Shepherd SIP FW for close monitoring.

Test and Validation for initial test cases will be targeted to have partial reports availability by May 2021.

1 Implementation

Table 5.19: Implementation Resource Model

SUPPORT TYPE	COUNT	EFFORT TYPE	RESPONSIBILITIES	OUTPUT
Head – Signaling Security	1	Shared	Sponsor, Escalation	
Head – RDD/Signaling	1	Shared	Overall Project Delivery	
RDD/Signaling	3	Shared	Tech Lead (San Juan site, SRA, RAAWA, VPN, SAT/UAT, TSSR)	
ISDP PM	1	Shared	Monitor project status/updates, Timeline owner	
Head – E2E Architecture	1	Shared	E2E Architecture, Technical Consultation	
TSD Domain	1	Shared	Domain Consultation	
Head – TSD Facilities	1	Shared	Consultation	
Head – CEI	1	Shared	SEQ Tapping, SO issuance, Technical Consultatio	
Head – CFEI	1	Shared	Site Consultation	

Head – NTG PM	1	Shared	Implementation RRF Consultation	
IPNE	1	Dedicated	Creates Intensive Low Level design document	
SEI	1	Dedicated	Creates Intensive Low Level design document	

K. Testing Strategy

- SAT/UAT
 - 1st Pass
 - 2nd Pass

6.0 Implementation Timeline

A. Delivery Duration

Below high level timeline shows approximate project duration. Target RFS is June 2021

No.	Activities	Duration	Timeline
1	PO Issuance	1 day	PO
2	Site survey (Will be done while waiting for HW delivery)	1 week	PO + 1 Week
3	Technical discussion and finalization of HLD and LLD (Will be done while waiting for HW delivery)	4 weeks	PO + 4 Weeks
4	HW Delivery	8 weeks	PO + 8 Weeks
5	Hardware installation (Carmona)	1 week	PO + 9 Weeks
6	HAT (Carmona)	1 week	PO + 10 Weeks
7	Software Installation (International SIP FW Refresh - Carmona)	3 weeks	PO + 13 Weeks

8	Stir and Shaken deployment (Carmona)	3 weeks	PO + 16 Weeks
9	Commissioning (International SIP FW Refresh - Carmona)	1 week	PO + 17 Weeks
10	Internal management network i ntegration (SIP FW i n Carmona to Analytics)	1 week	PO + 18 Weeks
11	Internal Integration of STIR and SHAKEN with SIP Firewall	2 weeks	PO + 20 Weeks
12	Internal Testing (Carmona)	2 weeks	PO + 22 Weeks
13	SRA (Carmona)	4 weeks	PO + 26 Weeks
14	SBC and TMGW Integrations and SIP FW Application in Carmona	2 weeks	PO + 28 Weeks
15	SAT (Carmona)	1 week	PO + 29 Weeks
16	ISAT (Carmona)	2 weeks	PO + 31 Weeks
17	UAT (Carmona)	1 week	PO + 32 Weeks
18	Failover Testing to new hardware (Carmona)	1 week	PO + 33 Weeks
19	RFS and babysitting in Carmona	2 weeks	PO + 35 Weeks
20	Hardware installation (Switches in Valero)	1 week	PO + 36 Weeks
21	HAT (Valero)	1 week	PO + 37 Weeks
22	Upgrade of Oracle DB	1 week	PO + 38 weeks
23	STIR and SHAKEN deployment (Valero)	3 weeks	PO + 41 Weeks

24	Internal Integration of STIR and SHAKEN with SIP Firewall (Valero)	2 weeks	PO + 43 Weeks
25	Internal Testing (Valero)	2 weeks	PO + 45 Weeks
26	Resiliency Testing	1 week	PO + 46 Weeks
27	SRA (Valero)	4 weeks	PO + 50 Weeks
28	SAT (Valero)	1 week	PO + 51 Weeks
29	ISAT (Valero)	2 weeks	PO + 53 Weeks
30	UAT (Valero)	1 week	PO + 54 Weeks
31	Transfer to new switches (Valero)	1 week	PO + 55 Weeks
32	RFS and babysitting i n Valero	2 weeks	PO + 57 Weeks
33	Documentation and Turnover	1 week	PO + 58 Weeks

7.0 Scope, Callouts and Risks

- Analytics function will need some time to work
- Migration of traffic might take some time in scheduling due to other activities aligned in NTG
- Roaming partner that support STIR-SHAKEN must cooperate during the testing
- PO release is delayed and might affect the target RFS of the project. Calls to/from US supporting STIR/SHAKEN might encounter problems

8.0 Assessment Validity

The solution presented in this technical assessment is valid within two months upon sign-off, and /or only holds when the project scope and assumptions remain unchanged.

DEFINITION OF TERMS	
FCC	Federal COmmunications Commission
GSMA	Global System Mobile Association
TRACED	Telephone Robocall Abuse Criminal Enforcement and Deterrence
STIR	Secure Telephony Identity Revisited
SHAKEN	Secure Handling of Asserted information using toKEN
SoA	Statement of Applicability