syniverse®

Syniverse's comments to TRAI's Consultation on CNAP

Syniverse's Comments in response to TRAI's Consultation Paper on Introduction of Calling Name Presentation (CNAP) in Telecommunications Networks dated 29 November 2022

12th January 2023

syniverse

Table of Contents

1 Summary of Syniverse Response

Syniverse Technologies (India) Private Limited ('Syniverse') would like to thank the Telecom Regulatory Authority of India ("Authority" or "TRAI") for a chance to provide our comments and opinions on TRAI's Consultation Paper on Calling Name Presentation (CNAP) in Telecommunications Networks as published by TRAI on 29th November 2022 ("the CNAP Consultation Paper").

Syniverse is the current Mobile Number Portability Service Provider (MNPSP) for Zone 1. In our role as one of two MNPSPs in India, we look forward to meeting the challenges of providing CNAP in an integrated and expanded role to provide not only number portability and CNAP but additional related services to address a broader solution for TRAI, the Indian telecommunications providers and consumers.

Syniverse is a world class telecommunications services company, and has become a global leader in mobile interoperability, mobile communications and mobile expertise with over 30 years of experience. In India Syniverse has been providing exemplary mobile number portability service to Indian mobile subscribers since starting its operations.

Our proposed solution envisions a secure India telecom subscriber database with data on Calling name so that India telecom users can enjoy timely and insightful information about the calling party. Our solution also provides a simple way for Indian telecom operators to provide their CNAM information to Syniverse to store in a centralized, secure database while also being able to receive copies of the data to use in call set up. In addition, the solution we propose would also enable interfaces with ported numbers, line ranges and enable detection and shut down of fraudulent calling schemes. The approach Syniverse outlines would also meet government concerns for privacy and authorized law enforcement agency access. All of this in one package to meet the challenges of CNAP today and in the future.

2 Syniverse Point by Point Response

Syniverse's Comments to the CNAP Consultation Paper:

2.1 Whether there is a need to introduce the Calling Name Presentation (CNAP) supplementary service in the telecommunication networks in India?

We believe that TRAI's consultation paper does a great job of identifying the benefits of CNAP to subscribers. Syniverse has no further comments on that other than pointing out that a larger opportunity exists to enhance India telecommunications by offering a CNAP solution that also provides fraud protection in porting, SPAM and fraudulent call protection and improving security.

2.2 Should the CNAP service be mandatorily activated in respect of each telephone subscriber?

Yes.

2.3 In case your response to the Q2 is in the negative, kindly suggest a suitable method for acquiring consent of the telephone subscribers for activation of CNAP service.

Not applicable as our answer to Question 2 is not negative.

2.4 Should the name identity information provided by telephone consumers in the Customer Acquisition Forms (CAFs) be used for the purpose of CNAP? If your answer is in the negative, please elaborate your response with reasons.

This is one option. Ideally the subscriber should be able to indicate a “CNAP name” vs. legal name. For example, someone like Ravikumar may want the name “Ravi” to show in Calling Name instead of their full name.

2.5 Which among the following models should be used for implementation of CNAP in telecommunication networks in India?

2.5.1 Model No 1. – Originating TSP provides CNAP in call Set Up

In which a CNAP database is established and operated by each TSP in respect of its subscribers and the name information is sent by the originating TSP to the terminating TSP during the process of call set up; or

2.5.2 Model No. 2 – Terminating TSP dips its own MNP database then queries appropriate Originating TSP’s CNAP database

A CNAP database is established and operated by each TSP in respect of its own subscribers. The terminating TSP dips into its MNP database to determine the originating TSP of the calling party and then performs a CNAP lookup on the CNAP database of the originating TSP; or

2.5.3 Model No. 3. – Terminating TSP queries Centralized CNAP database

A centralized CNAP database is established and operated by a third party with an update mechanism from each TSP in respect to their subscribers; the terminating TSP performs CNAP lookup from the centralized CNAP database at the time of receiving a call; or

2.5.4 Model No. 4. – Terminating TSP queries local CNAP database as copy of Centralized CNAP database

In Model 4 a centralized CNAP database is established and operated by a third party, and individual local CNAP databases are established by all TSPs; the TSPs keep a copy of the centralized database and perform local CNAP lookup at the time of receiving a call; or

2.5.5 Other Model(s)

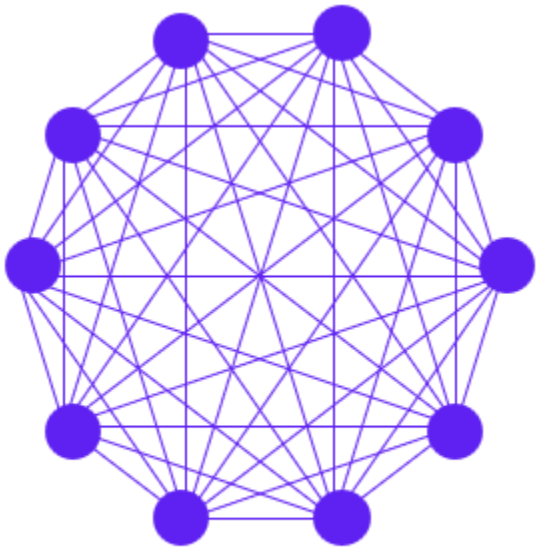
Any other suitable model for implementation of CNAP along with a detailed description of the model.

We believe that **Model 1** (CNAP presentation sent by originating operator) has issues because some networks in the call flow may not be able to pass the CNAP information along when the call is being set up. The CNAP presentation is dependent on every single network in the chain passing along the CNAP information. This may lead to inconsistent behaviour to the subscriber which may cause calls and complaints to customer service centres increasing costs to terminating operators when they can't control the CNAP failure.

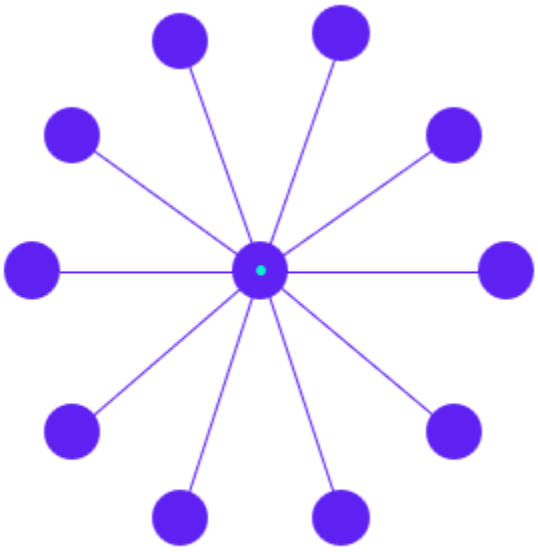
Model 2 requires at least two queries:

- one to number portability and
- one to a CNAP database.

This will lead to increased call set up delays. While the delays for an individual call may not always be significant or noticeable to a subscriber; the delays, in aggregate, will have a real impact on network performance. Model 2 also requires each terminating operator to have interfaces with all other operators in case the originating caller is not on its own network. If there are 10 operators in the ecosystem, then each operator will have to support 9 interfaces. Since in this example, each of the 10 operators must have 9 interfaces to support so in total 90 interfaces are required vs. using a hub where each operator must support only one connection to the hub.



Direct Network Model
(each operator supports N-1 interfaces)



Hub/Spoke Model
(each operator supports 1 interfaces)

Model 3 is the best model from the security and data privacy perspective because the TSP will only have access to the CNAP data via an API from the Centralize CNAP DB for calls that is terminating. This model will require two API calls from each operator:

(1) One API call to update the Centralized CNAP DB from the originating TSP made at the time of the subscribers register or updates his or her CNAP data.

(2) The second API call will provide the CNAP data to the terminating TSP only at the time of the call.

Model 3 requires a highly available central database, high volume, high performance, and low latency connections which would require multiple geographically diverse sets of databases. This means the cost of this model would be high for the centralized system.

Model 4 the most viable option because it allows each terminating TSP to control its own quality of service on CNAP. Meanwhile each operator only needs one connection to the Centralized CNAP database to provide updates when a subscriber changes his or her information. With Model 4, the terminating TSP would receive a local copy of the Centralized CNAP DB and query it locally. This is similar to mobile number portability query process for call routing. In fact, it might be possible for mobile service providers to simply add a new column to their existing MNP databases. However, this would increase the size of these databases considerably. For added security and data privacy, TRAI can dictate that both the Centralized CNAP DB, and TSP must use encryption in both data at rest and in motion.

To Summarize, the Chart below provides a summary for the four different models:

Model #	Model Description	PROs	CONs
1	Originating TSP provides CNAP in call Set Up		• Dependent on intervening TSPs between Originating TSP and Terminating TSP. • Might cause inconsistencies and subscribers confusions.
2	Terminating TSP dips its own MNP database then queries appropriate Originating TSP's CNAP database		• May increase call setup delay • Will increase call signalling network utilization • Requires each TSP to connect to all potentials OSPs increasing network maintenance and costs.

Model #	Model Description	PROs	CONs
3	Terminating TSP queries Centralized CNAP database	• Data privacy and security from 2 separate APIs which keeps data separate between originating and terminating TSP. • CNAP data only presented to Terminating TSP at time of the call. • Each Operator need only 1 connection Centralized CNAP DB.	• High cost to implement to provide high availability to handle high volume and low latency.
4	Terminating TSP queries local CNAP database as copy of Centralized CNAP database	• Allows terminating TSP control its own CNAP service quality (latency, availability, capacity, etc.) • Each Operator need only 1 connection Centralized CNAP DB. • Each TSP will have its own local CNAP DB. • Might be able edit existing MNP DB to add column for CNAP data.	• TSP and Centralized CNAP DB might need to implement encryption for data at rest and in motion. • May need legal limits beyond IDPR limiting CNAP data to CNAP presentation only.

2.6 What measures should be taken to ensure delivery of CNAP to the called party without a considerable increase in the call set up time?

Reducing the number of queries per call and reducing the round-trip latency of the queries are the best methods to ensure call set up time remains minimal. Local copies of the central database will provide low latency. In addition, the querying switch should have a timeout value that allows call set up to proceed in the event a CNAP response is not received. It should also be noted that a timeout will not prevent a call from being placed. It just means that the call will be marked as CNAP unavailable.

Therefore model 2 which requires two queries (one to an MNP platform and one to the originating operator) should be eliminated. Likewise, model 2 should also be eliminated based on the need for an inter-operator query between the terminating and originating operators. If Model 3 is used the centralized CNAP database will need to have more than eight local copies that must be tightly

synchronized and highly available so that the round-trip query time is minimized for any switch anywhere in India.

.

2.7 Whether the existing telecommunication networks in India support the provision of CNAP supplementary service? If no, what changes/additions will be required to enable all telecommunication networks in India with CNAP supplementary service? Kindly provide detailed response in respect of landline networks as well as wireless networks.

Syniverse has no feedback on this topic. The operators themselves are much better positioned to speak to their costs and complexities of their own networks.

2.8 Whether the mobile handsets and landline telephone sets in use in India are enabled with CNAP feature? If no, what actions are required to be taken for enabling CNAP feature on all mobile handsets and landline telephone sets.

Syniverse has no feedback on this topic. The operators themselves are much better positioned to speak to the costs and complexities of mobile handsets and telephone sets they may offer or support.

2.9 Whether outgoing calls should be permitted from National Toll-Free numbers? Please elaborate your response.

The solution Syniverse envisions would support this provided the information on National Toll-Free numbers is provisioned into the centralized CNAP database and thus downloaded to each terminating operator's local database.

2.10 In case the response to the Q9 is in the affirmative, whether CNAP service should be activated for National Toll-Free numbers? If yes, please provide a mechanism for its implementation.

Syniverse believes that this is possible and beneficial to subscribers but leaves decisions to operators.

2.11 Whether CNAP service should be implemented for 140-level numbers allocated to registered telemarketers?

Syniverse has no comments on this topic.

2.12 If your answer to Q11 is in the affirmative, then kindly elucidate the technical considerations for implementing CNAP service for registered telemarketers so that the name identity of the principal entity may be presented to the called party.

Not applicable due to our answer on Q11.

2.13 Whether the bulk subscribers and National Toll-free numbers should be given a facility of presenting their 'preferred name' in place of the name appearing in the CAF? Please elaborate your response.

We believe that this is appropriate as many people use nicknames. However, there should be safeguards to ensure that a subscriber provides a truthful "preferred name" and not one that is misleading. For example, using "Shrini" for "Shrinivasa" would be considered truthful and non-misleading. However, this issue is very difficult to manage. Some people may have a nickname that is not an abbreviation of their full name. Or may use a middle name rather than a family name.

2.14 In case the response to the Q13 is in the affirmative, what rules should govern the implementation of such a facility.

Syniverse, in the role of a centralized CNAP provider, would not be involved in the enforcement of appropriate "preferred names" entered into the CNAP database but just the administration, upload and download of this information. Therefore, we leave the details to others to work out.

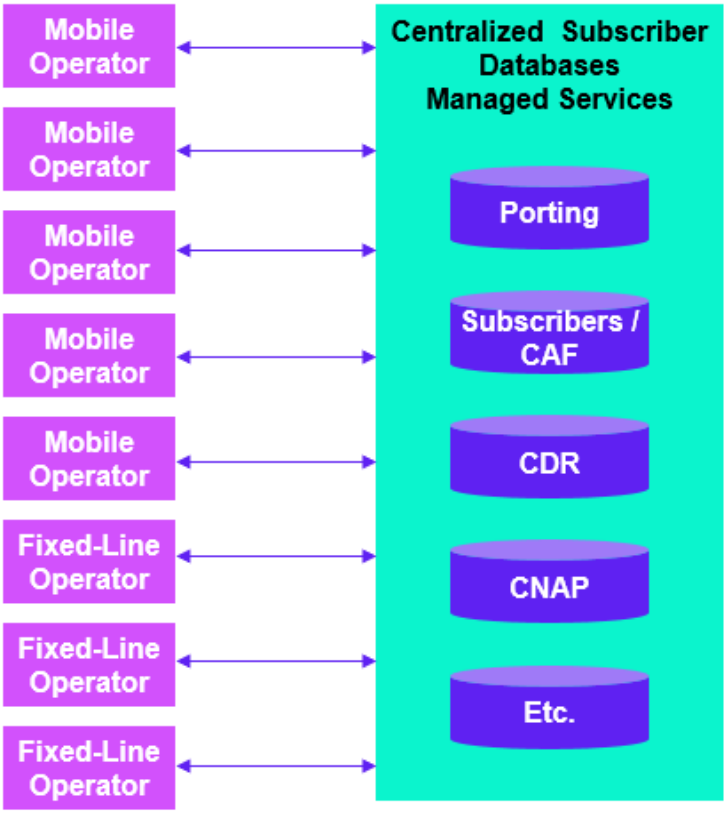
2.15 Whether there is a requirement of any amendment in telecommunication service licenses/ authorizations in case CNAP is introduced in the Indian telecommunication network? Please provide a detailed response.

Syniverse has no comments on this topic.

2.16 Whether there are any other issues/ suggestions relevant to the subject? If yes, the same may be furnished with proper justification.

Syniverse believes a larger opportunity awaits to not only address CNAP information but other types of subscriber databases in one complex. Our idea is to expand the MNP license so that the MNP Service Providers can also provide CNAP databases in a similar model (i.e., a centralized system that is downloaded by each TSP so the TSP can resolve CNAP queries quickly and efficiently from the local system when it is acting as the Terminating SP). In this model, which is an extension of model 3 or 4 where each TSP would contribute data to the Centralized CNAP portion of the database complex. Data could also be added to the Centralized CNAP system via the porting process for new subscribers that port in, but via an upload process for subscribers taking a new number outside of the porting process. Besides the CNAP service, the same managed service can be used to support bypass fraud and SIM-box detection, enhance security by giving Law Enforcement Agencies (LEAs) centralized access to subscriber information, calling records, and even enable fixed-line number

portability. To reiterate, this model provides the added Data Privacy, confidentiality, and security that allows IDPR compliance and added security to combat fraudulent activities.



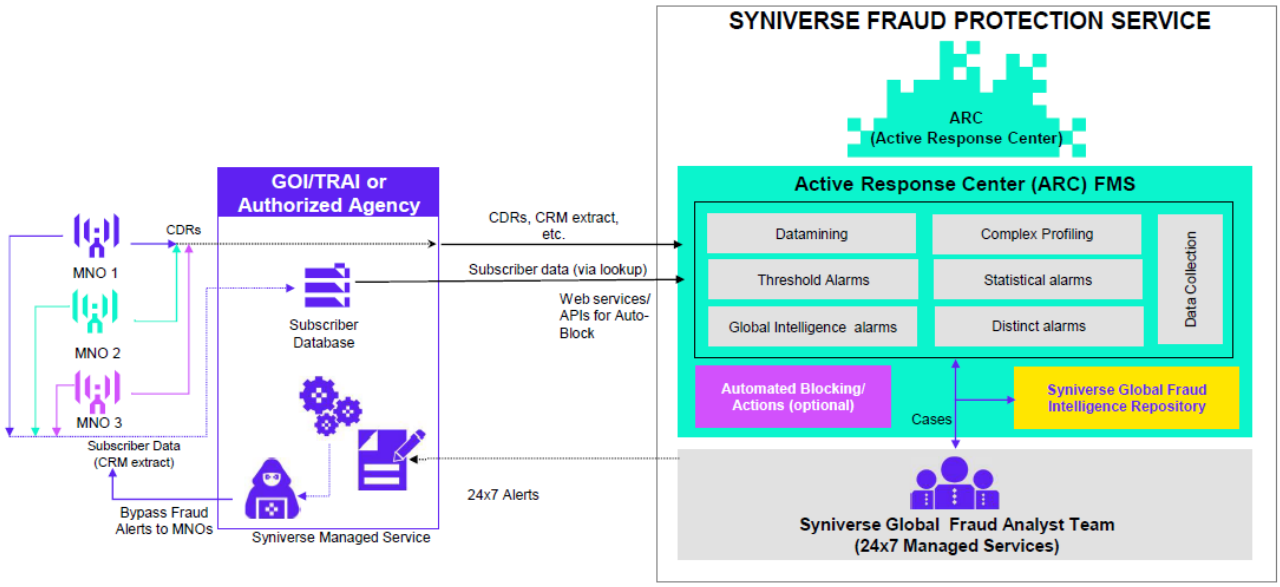
Supports

- Centralized Mobile Number Portability (MNP)
- Centralized Fixed Line Number Portability (FLNP)
- Centralized Calling Name Presentation (CNAP)
- Bypass Fraud/SIM Box Detection (BP/SBD)

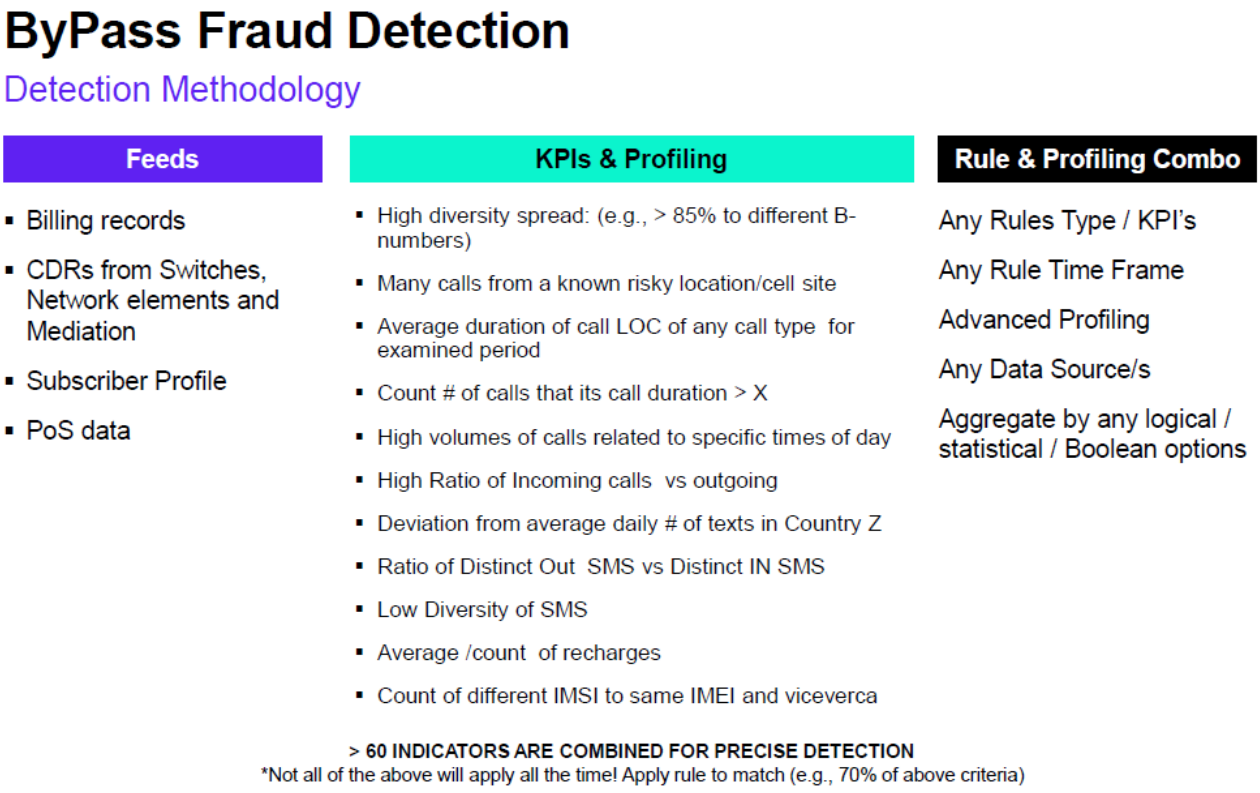
For example, if each operator provides a feed of CDRs this information can be correlated to other subscriber data via data mining, profiling, and statistical alarming based on rule-based intelligence and configurable thresholds so that automated call blocking and other actions can be implemented via web services/APIs in real-time or alerts that are issued to MNOs and Fixed Line Operators as appropriate. An overview of this presented below:

Bypass Fraud Protection service architecture

24x7 managed service with global intelligence and real-time alert mechanism



In the sample service architecture above we show that each operator would add CDRs to the centralized CDR database and from there, when combined with subscriber data, we can run these through statistical analysis to determine numbers that are generating calls associated with patterns like SIM Boxes. This can then be used to generate alerts or even block the SIM Box. This can be run as a managed service. Some of the decision points for making these determinations are listed below:



By combining all of these databases in one place, as a managed service, an array of services and benefits become possible. These include:

- Reduction in porting fraud as the porting records could be expanded to include national ID card number (e.g., Aadhaar / KYC info) and compared to other data.
- Integration between porting and CNAP to make CNAP data management easier
- Minimizing toll bypass fraud and SIM Boxes
- Identifying SPAM callers
- Improving Law Enforcement Agencies access to MNP, CAF, CDR and other data

3 Summary of Syniverse suggestion for CNAP Presentation

In conclusion, Syniverse thanks the Authority for the opportunity to present our comments and feedback to the Consultation Paper. We believe India can benefit from not only CNAP but may realize further and more significant gains from a modern infrastructure that allows for collection and inter-operator collaboration to reduce fraud, increase national security, benefit subscribers in numerous ways by hosting CNAP and other data in a single database complex hosted in a managed service environment.

Syniverse looks forward to further discussions on this topic.

4 About Syniverse Group

Syniverse Group is the world's most connected company—we pioneer innovations that take businesses further. Our secure, global network reaches billions of people and devices. Our engagement platform powers the customized experiences of the future. And the millions of secure transactions we drive every minute are revolutionizing how goods and services are exchanged. We have always led companies to reimagine the boundaries of possibility. Today we're delivering on opportunities with the power to change the world. www.syniverse.com.