OBC and A-Number validation

June 26, 2019

Atlanta, GA

Origin Based Charging

Origin Based Charging (OBC) principle

+ Over the last few years OBC principle has been adopted in some regions, mainly in Europe
+ With OBC origin of the call (that is the country calling subscriber belongs to) is relevant for wholesale inter-operator billing: origin is added to the call parameters that determine rate to be applied to call termination fee
+ Origin is identified according to “country code digits” of the A-Number (CLI) transferred in the call signalling
+ CLI therefore affects wholesale call termination rate among operators
  + calls originated in some countries as well as those with no-CLI can be charged at the highest rate
  + for calls originated in another set of countries lowest rate is applied

Unfortunately OBC has led to interoperability issues as well as new types of frauds

CLI management

CLI management guidelines to complement existing technical specifications

+ CLI used both for presentation to the callee (according to privacy settings) and OBC between operators
+ International carriers are not allowed to apply any manipulation or change to CLI. It is mandatory they pass it unaltered. The only exception is the case where they are requested by domestic operator to change CLI format from national significant to international at the interconnection between them
+ For OBC purposes CLI is always contained in headers/fields that, according to specifications, are network provided: that is P-asserted-ID (PAI) in SIP and Calling Party Address (CgPA) in ISUP. These headers/fields are supposed to be filled in with an international E.164 number
+ Signalling protocols (SIP for VoIP and ISUP for TDM) can deliver additional information on the caller through the use of specific headers/fields (the from header in SIP, the Generic Number field in ISUP). These can be used for presentation to the callee but not for OBC
+ Full set of guidelines described in i3forum “Calling Line Identification (CLI) management”, release 1.0

STIR/SHAKEN (1/3)

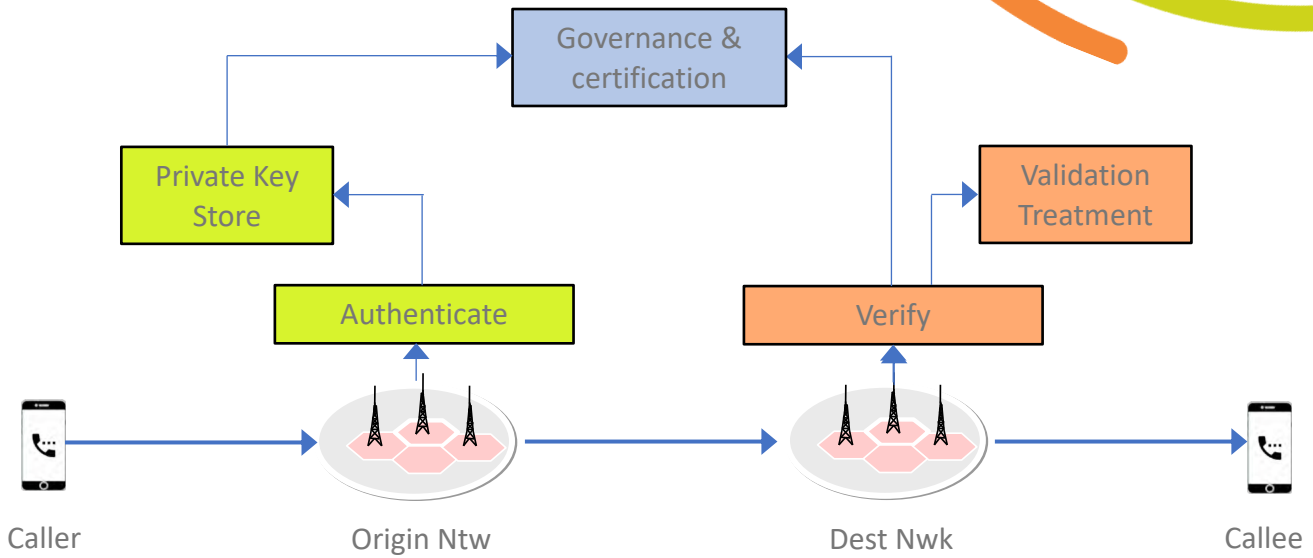
STIR stands for Secure Telephone Identity Revised

- Final goal of STIR is to validate the Caller and prove identity of the Originating Network. This means that:
  - SIP identity header passes the URL of the call record to the Destination Network
  - Destination Network knows meta data has not been tampered with along the call path
- STIR is made up of:
  - a specification that updates SIP signalling to convey signatures for calling party numbers which demonstrate that the entity that populated the parameter “has authority” over the numbers or the ranges
  - a framework to share credentials and sign these numbers
- STIR specifications have been embarked in the SHAKEN system, that has been designed to provide nationwide coverage of A-Number verification in USA and Canada
- STIR can only be used to validate calls with SIP signalling, so it is limited to VoIP traffic with no TDM support

STIR/SHAKEN (2/3)

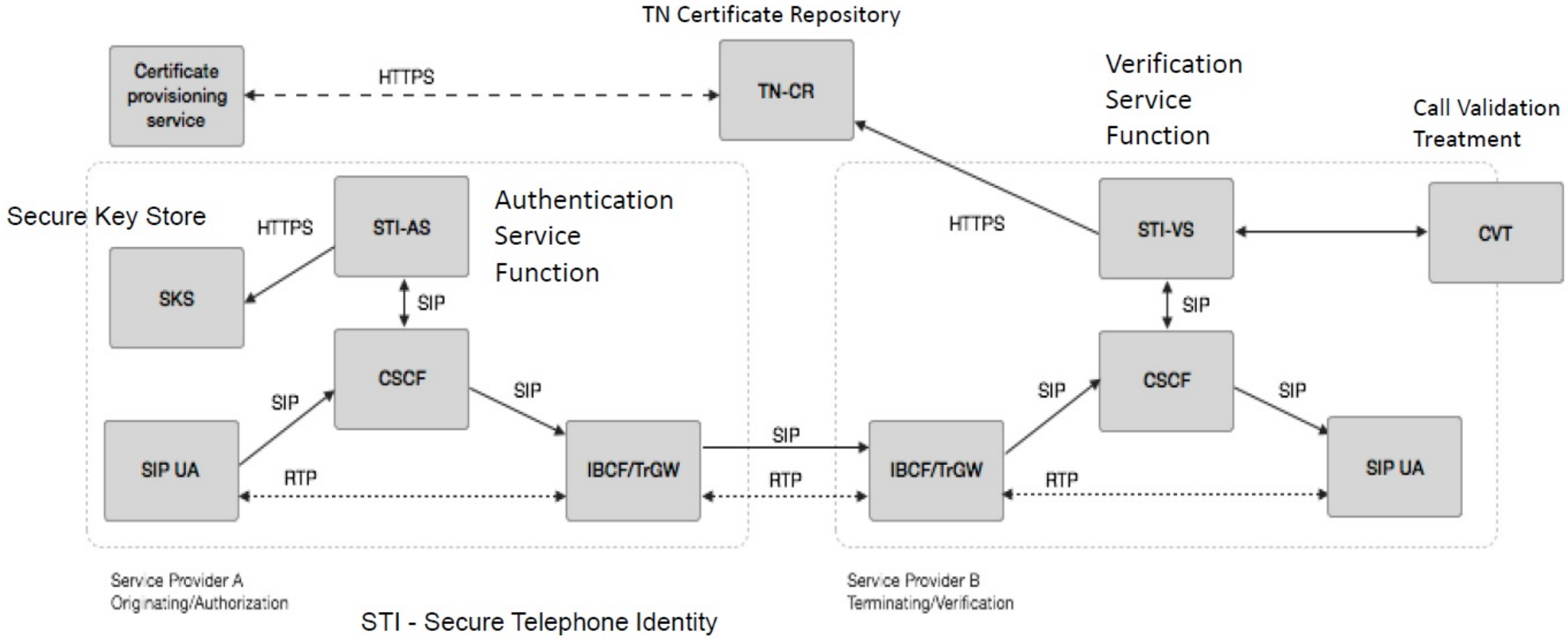
SHAKEN system high level architecture

+ Originating Network invoking authentication service to certify Caller identity
+ Destination Network invoking verification service to check Caller ID based on PASSporT SHAKEN token received in SIP identity header
+ Certificate repository queried by Destination network verification service (HTTP call)
+ Destination Network to apply call treatment according to verification result
+ Centralized governance, policy and certification



STIR/SHAKEN (3/3)

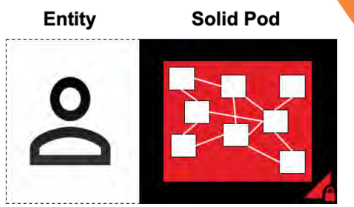
SHAKEN reference architecture in US domestic implementation

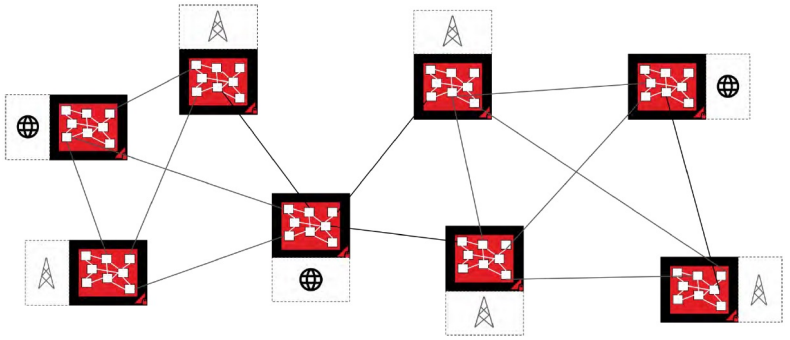


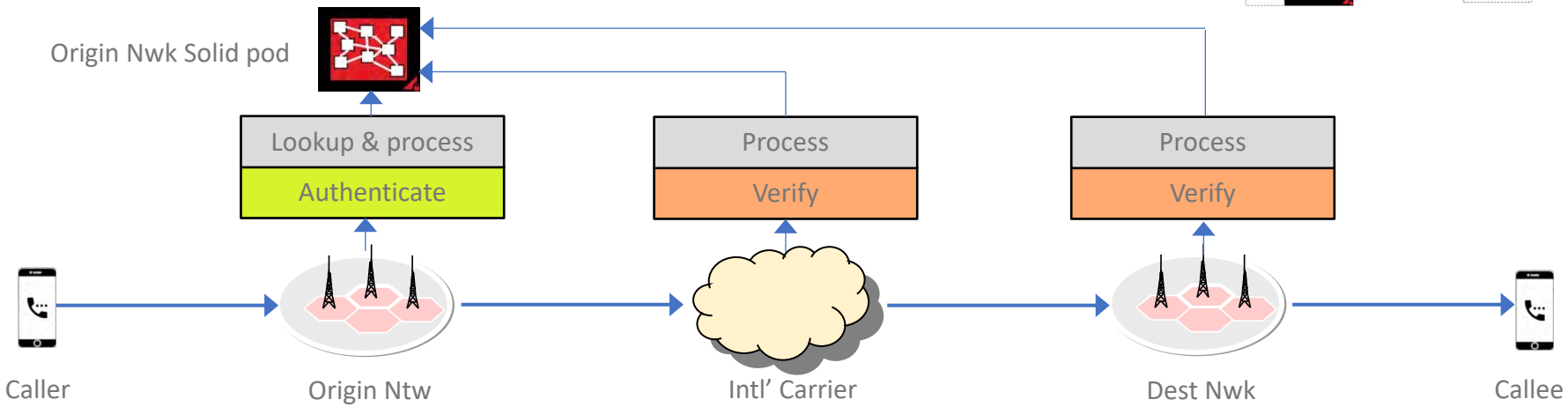
SOLID

SOLID and its applicability to telco ecosystem for A-Number validation

+ Individual entities separate their data from the systems and applications that leverage it into decentralized data stores (pods)
+ Built on the Web. Solid extends HTTP with a set of open standards and protocols
+ Decentralized graph data model maps perfectly to the real-world data model of internetwork communications
+ Decentralized identity and security model provides peer-to-peer authentication, authorization and crypto





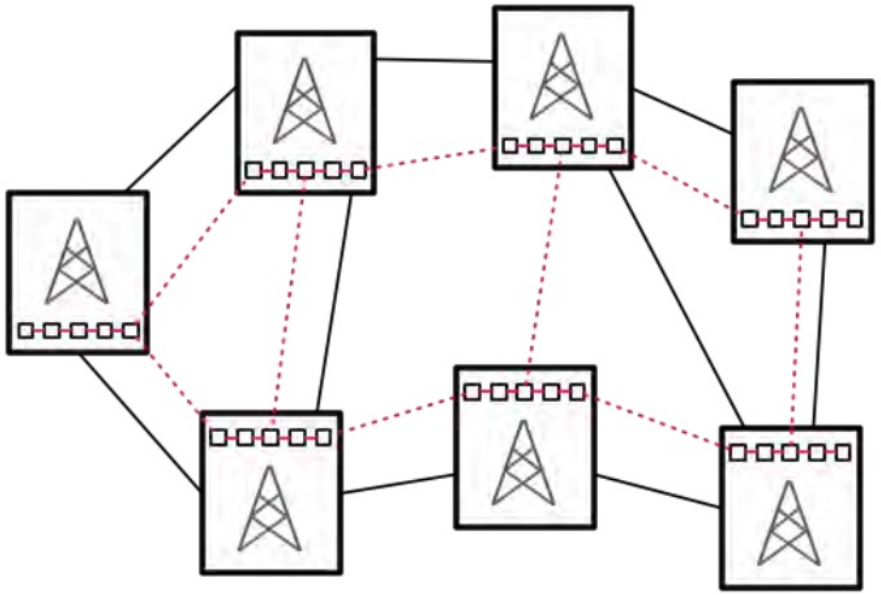


i³ forum

Blockchain

Blockchain to share public key certificates so as to verify user identity

+ Blockchain is a distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way
+ Use case where operators share information on subscribers' identity and certificates
+ Blockchain ecosystem to be created among international carriers as well as domestic operators
+ Governance, policy and certification to be further analysed
+ To be compared with Solid for certificate management



So… what's next?

STIR/SHAKEN, SOLID, Blockchain… different available technologies

+ Are they deployable in the international wholesale ecosystem?
+ Can we combine them?
+ Can they complement each other?

STIR/SHAKEN deployment requires centralized governance and policy which is fine in a domestic domain, but hard to deploy in the international ecosystem

SOLID could help realizing CLI certification among operators without a centralized entity, provided that "trust domain" concept is still applied. So one area to be investigated is the combination of STIR and SOLID.

Blockchain could also be used to complement STIR/SHAKEN since it enables public key certificate retrieval from originating operator without a centralized entity, to be compared with SOLID. So CLI validation as use case for the adoption of blockchain technology to be further investigated


i3 forum
Thank you
www.i3forum.org