Questions transcript provided by moderator

Webinar on "Enhancing signalling security and privacy using globally interoperable digital signatures"

16 June 2022

#	Question	Answer
1.	The video didn't say how the SMS was rerouted?	The SMS was routed to the presenter's laptop since an SS7 location update request has been sent to the subscriber's home network via established SS7 connection, fooling the home network that the presenter's phone had roamed to another network, thus the home network started rerouting all inbound calls and SMS to the malicious SS7 Global Title (GT).
2.	You referred to CLI authentication. The STIR/SHAKEN protocol uses PKI to achieve this. PKI requires certification authorities. If an integrity layer is added to SS7, and if it is based on PKI, then who should be the top-level certification authority? Would there be a role for ITU?	In ITU-T Q.3057 and draft Q.Pro-Trust ITU-T SG11 built the same cryptographic authentication scheme as in Secure Telephone Identity (STI), i.e. ITU-T SG11 also uses Public Key Infrastructure (PKI) tokens with a Certificate Authority (CA) trust chain. From the presenter's perspective, ITU should be the trust anchor of ITU-T Q.3057 and draft Q.Pro-Trust since it's a globally trusted SDO and can hold the Global Trusted Signalling Certification Authority (TSCA) which is the repository for trusted CAs.
3.	How does this model protect against a malicious node that are hosted on an otherwise trusted roaming partner's network?	Much like in STI, the revocation of operator certificates is the mechanism in which policy is enforced. The TSCA can revoke any operator certificate if it does not comply with the rules.
4.	Is this initiative somehow synced with 5G Roaming architecture, where TLS certificates are exchanged between operators (N32 interface)?	No, it isn't, but since existing and 5G architectures use ITU-T X.509 certificates (also used in TLS) both architectures are compatible and interoperable. There may be a need for an IWF to translate token encoding (like the STIR <-> ITU-T Q.3057 IWF)

#	Question	Answer
5.	Did you assess the impact on MNO networks, e.g. they need to buy SSGWs, what else? How to motivate the MNOs to do the investments?	Yes, the architecture described in ITU-T Q.3057 is built to create as little capital expense as possible on the MNOs as it’s an inhibiting factor in adoption. The ITU-T Q.3057 architecture requires only software updates to existing Signalling Transit Points (STPs) and Service Control Points (SCPs) to become the SSGWs.
6.	Depending on who will operate the Global Certification Authority (CA), isn't there a risk of political (mis)use, e.g., disconnect the whole countries from SS7?	Yes, much like in Secure Telephone Identity (STI) where the governance authority can exclude operators. Therefore, a globally trusted Standards Developing Organization (SDO) is required to be the trust anchor. From presenter’s perspective, since ITU is the UN agency, and it is managed by the member states it’s the best candidate for this.
7.	Are Mobile Number portability scenarios covered in current STIR/SHAKEN model?	No, since the STI framework (which uses STIR and SHAKEN) does not authenticate phone numbers, it authenticates operators.
8.	Which operators are working on these standards and in some way committed to implement them?	All operators as well as other stakeholders which are ITU-T SG11 members are involved in developing ITU-T Recommendations related to signalling security (under Q.series).
9.	There are intermediate carriers between operators so how does operator authentication work in that scenario?	ITU-T X.509 enables a trust chain, i.e., each carrier, the originating and any intermediate carrier will add their certificate to the chain. As long as the trust chain ends in the TSCA the terminating operator can validate the authenticity of the originating operator, no matter how many intermediate carriers are between them.
10.	Do you have any time plan to promote this in the industry? When approximately could this become a reality, according to your view?	ITU-T SG11 is going to consent draft Q.Pro-Trust in July, which will be followed by four weeks last call for comments. In case no objections, it is supposed to be approved in the second half this year. However, additional work needs to be done in ITU-T SG2 as well to add the operational aspects for policy governance and administration. Once it is done then operators will be able to adopt this architecture. Obviously, regulatory work in each country needs to happen as well.

#	Question	Answer
11.	So principally STI doesn't authenticate any particular caller id? It's the operator which just authenticates the session by giving it a digital certificate?	The STI framework is designed to authenticate operators, not caller-ids. In order for an operator to get their STI token they sign a legal contract which specifies the policy.