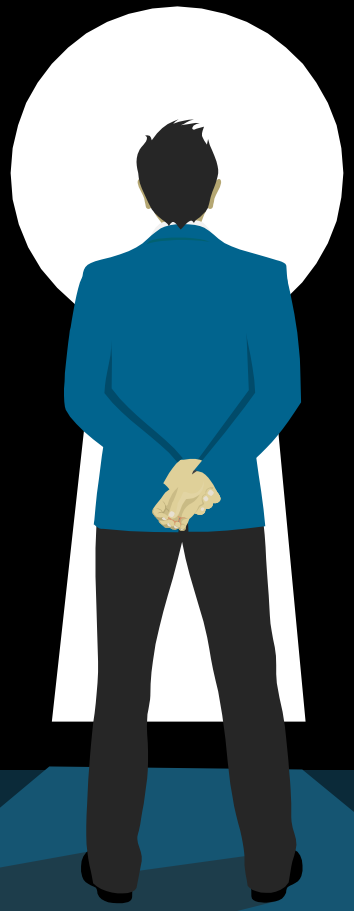
GSMA KEY MANAGEMENT
A single, automated and evolving process



ITU Workshop:
Improving the security of signalling protocols

29th of November 2021

Ewout Pronk
GSMA FASG DESS Chair

GSMA Associate Member

NetNumber

INTRODUCTION

- The exchange of key material between GSMA members was never required
- Security by design for 5G roaming introduced that need at the moment work was underway to define a Diameter End-to-End Security (DESS) for LTE roaming
- The DESS Key Management Group was appointed to work on this topic
- Already defined Stage 1 manual procedures for 5G and LTE roaming in FS.34 v1.0

- By now, there are 7 different use cases defined that can benefit from this solution
- Goal of the key management stage 2 work:

"Create a uniform, automated procedure for GSMA members to exchange key material for all use cases within the GSMA"

GSMA Associate Member

5G IS AN EVOLUTION, CLOSE TO A REVOLUTION

- 5G is an evolution of LTE (4G)
- New functionality added
- Ecosystem is expanded
- Security-by-design is added

Source: https://www.3gpp.org/ftp/Information/presentations/presentations_2018/2018_10_17_tokyo/presentations/2018_1017_3GPP%20Summit_02_Key%20Note_SCRASE.pdf

SIGNALLING SECURITY IN 5G

3G

Time

Retrofit security with filter elements

Message type filter, plausibility checks

Pre-defined filter elements

Filter, plausibility checks

No confidentiality, no authenticity

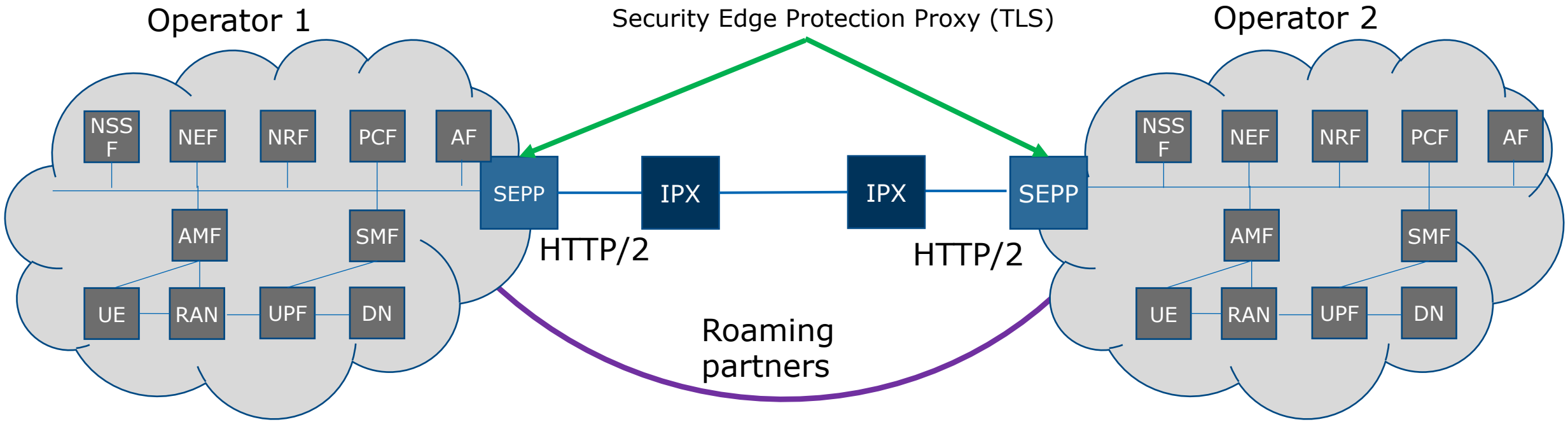
All messages sent in clear text

Secure protocols

Authenticity, integrity, confidentiality

GSMA Associate Member

THE 5G SECURE INTERCONNECT

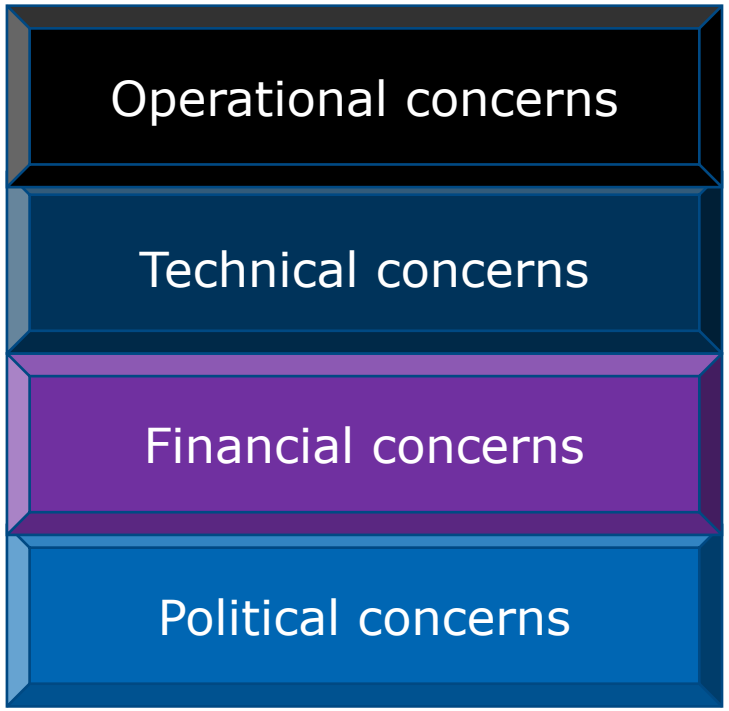


Among other models debated in the GSMA the model above is seen as the most generic model:

- Operators set-up a SEPP-SEPP TLS connection
- All roaming traffic is tunneled over that connection(s)
- Routing and network topology discovery will be end-to-end
- **Managing key material to facilitate 5G roaming is utmost important**

WHAT MAKES KEY MANAGEMENT COMPLEX?

- Hard to find a balance between:



"My roaming staff can never operate this!"

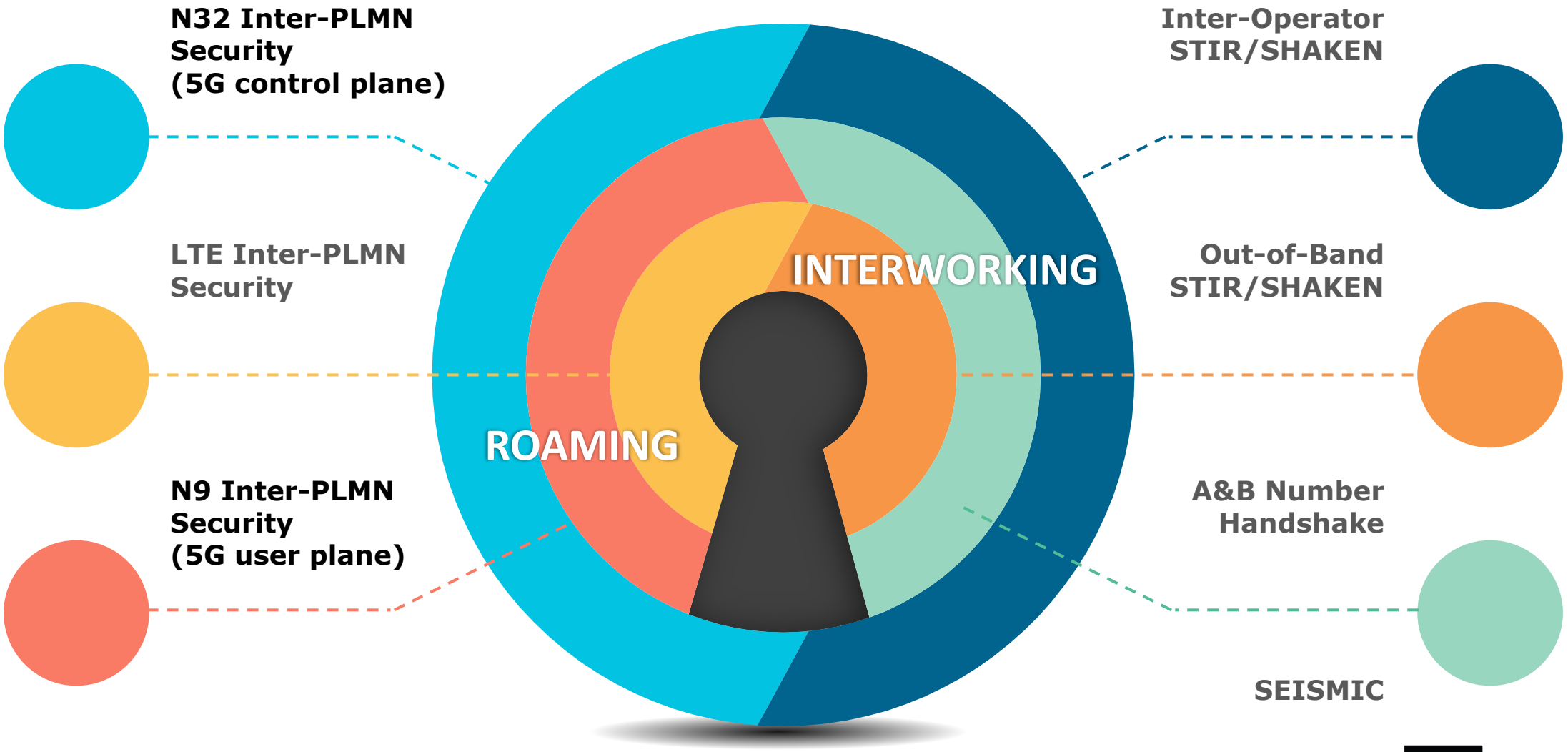
"The solution is way too difficult!"

"The solution is way too expensive!"

"Can I trust the one issuing keys or certificates?"

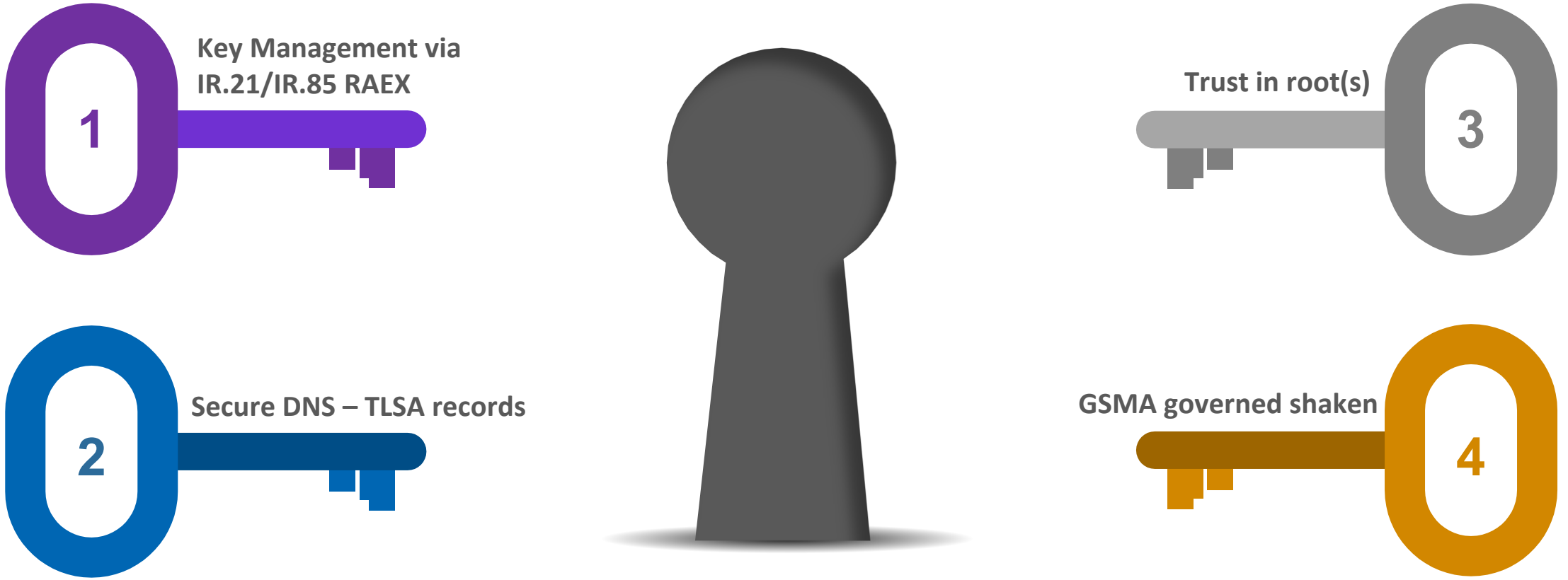
GSMA Associate Member

USE CASES



GSMA Associate Member

HOW TO COME TO A SOLUTION?



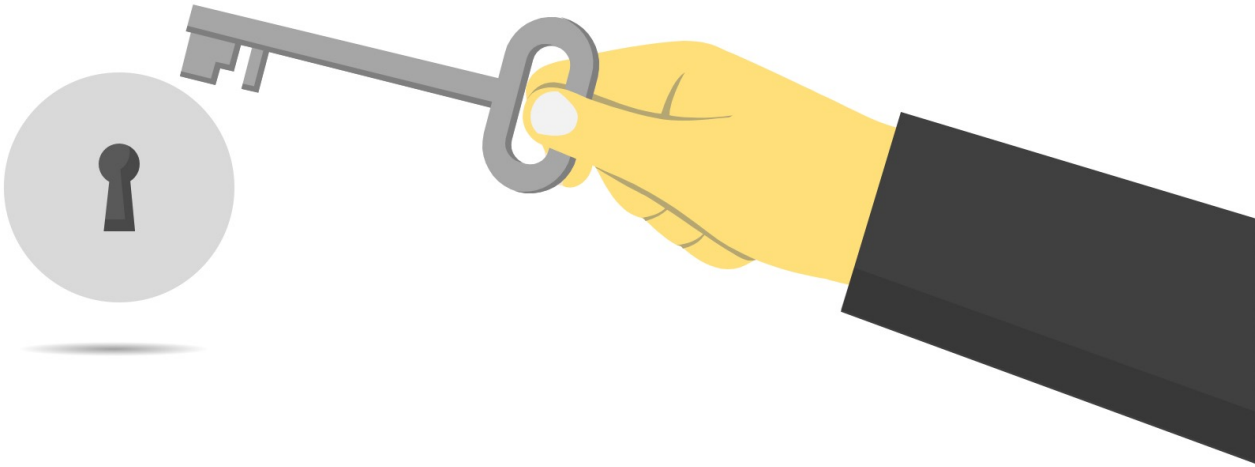
4 solution directions concluded for further evaluation

7 Use cases - **9** Solution directions - Weighted on **12** arguments

Associate Member

PROPOSAL: A STEP-BY-STEP APPROACH

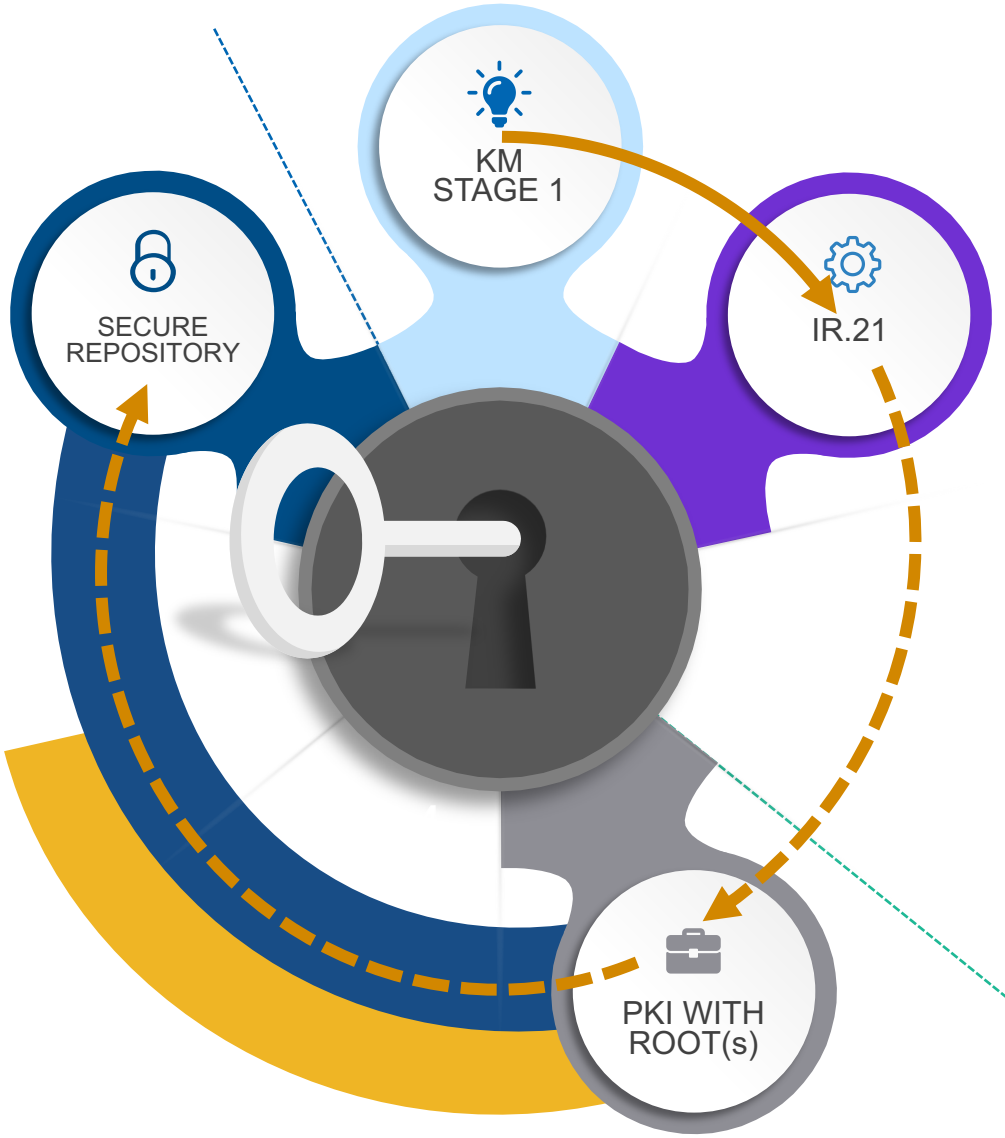
- Neither of the solution directions are a perfect fit
- Bilateral trust provides the most trust (for roaming and interworking)
- Not likely that all GSMA members will agree to trust a single root, neither it is required
- Proposed to have a step-by-step evolving key management solution with the IR.21 RAEX as cornerstone for the certificate repository while reusing components from other solution directions



GSMA Associate Member

Stage 2 – Step-by-step approach

A dynamic certificate repository will maximize automation



IR.21 is **THE** tool for Mobile operators' Network administration

Self-signed certificates may be used

Certificates signed by a certain root can provide additional trust outside the GSMA secure domain e.g., governed STIR/SHAKEN

GSMA Associate Member

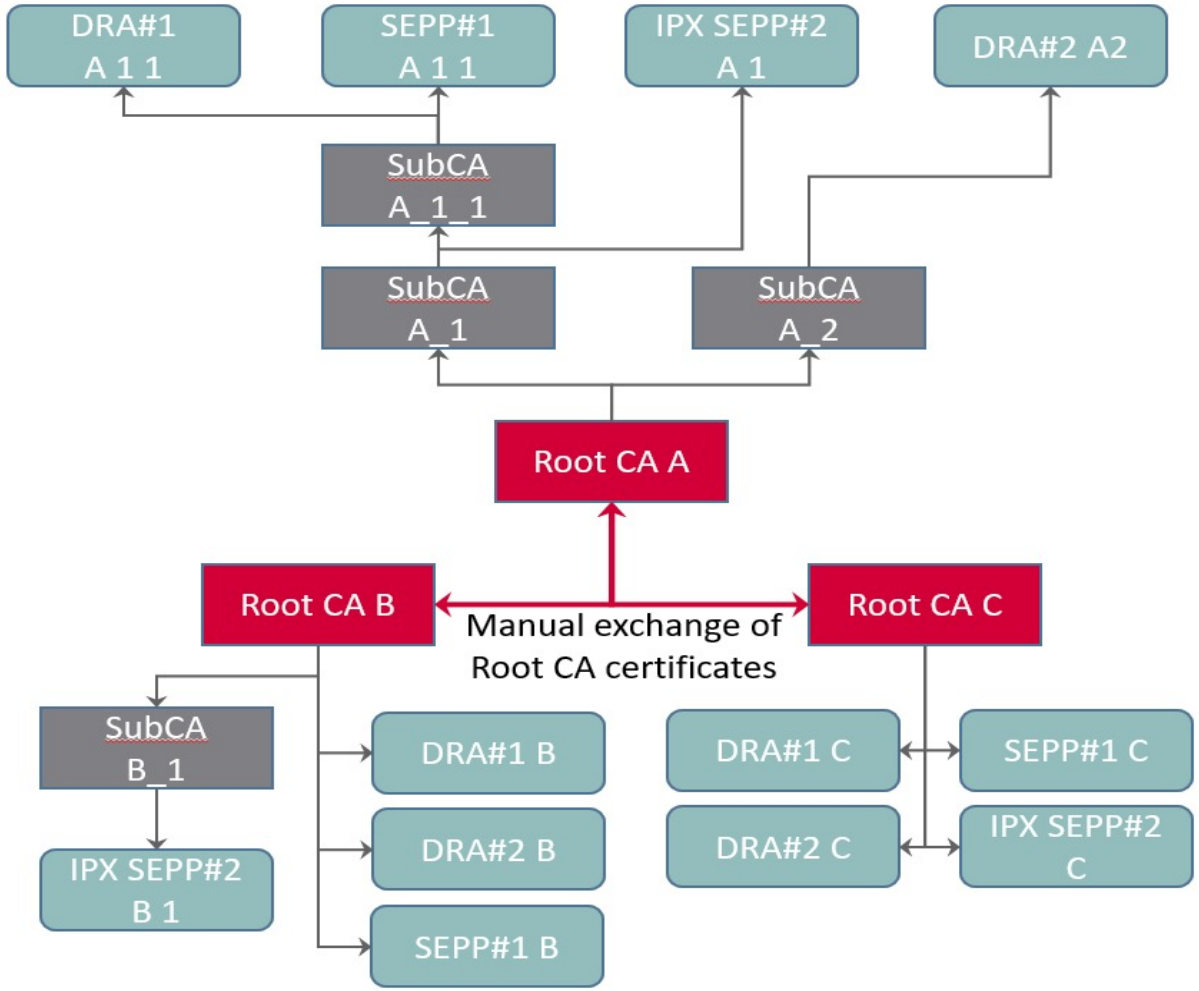
GSMA Associate Member

STEP 0 – KEY MANAGEMENT STAGE 1

Key Management Stage 1

FS.34 v1.0 March 2020

- Manual procedure between operators
- No governance
- Cumbersome



GSMA Associate Member

STEP 1 – ENABLE KEY MANAGEMENT VIA RAEX IR.21/IR.85

RAEX Tools
IR.21 / IR.85 / IOT / Op Data

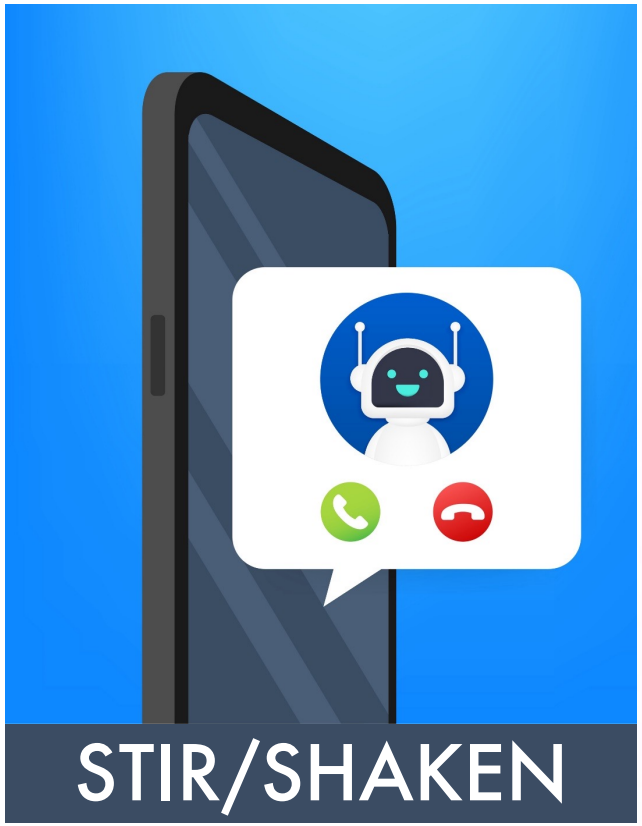
- Based on bilateral trust
- Operators to store own certificate(s) in RAEX
- Firm security and automation requirements to be set to RAEX
- Recommendation to cover usage of RAEX as mandatory for 5G roaming and to cover that contractually

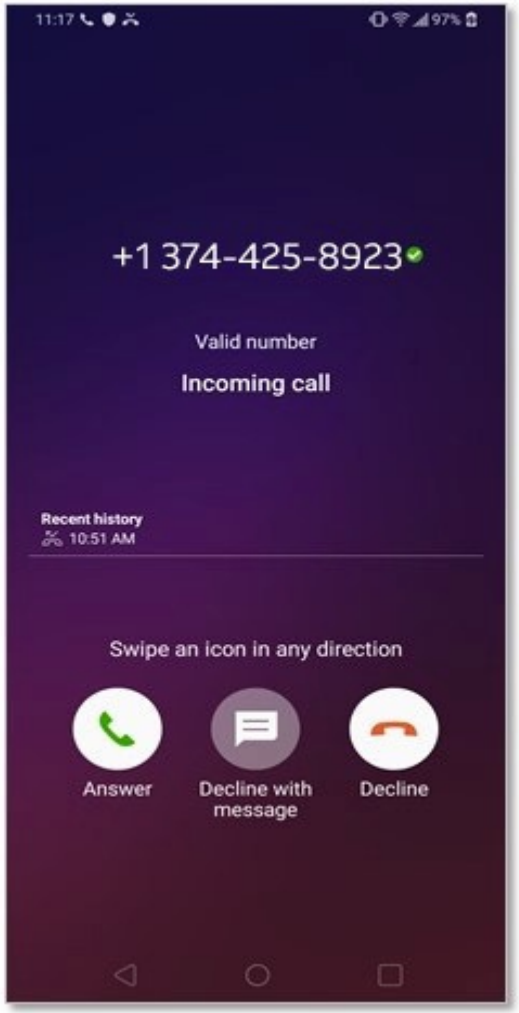
Information for DIAMETER certificates exchange	
IP Addresses of IPSec GW:	
IP Address of the first IPsec GW	[List/Range/Subnetmask of IP addresses]
IP address of the second IPsec GW[101]:	[List/Range/Subnetmask of IP addresses]
Certificates available from the RAEX IR.21 Database *[102 103]*	
Certificate of first IPsec GW:	[Yes/No]
Certificate of second IPsec GW:	[Yes/No]
Operator roaming sub-CA certificate[104]:	[Yes/No]

GSMA Associate Member

STEP 2 – INTERWORKING WITH OTHER ECOSYSTEMS

- GSMA to establish trust with the other domain
- GSMA to designate a certificate authority that has trust in other domain and facilitate vetting and onboarding of GSMA members (getting their certificates signed)
- Operators to join on a voluntary basis

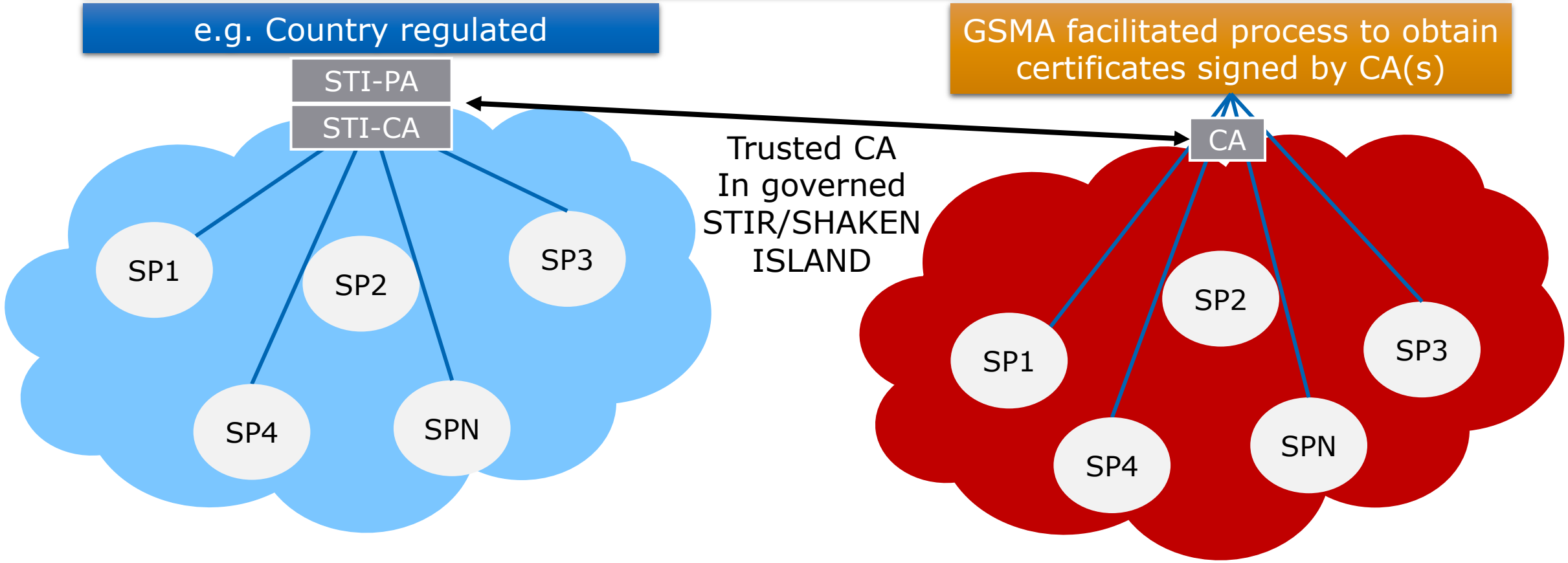




Associate Member

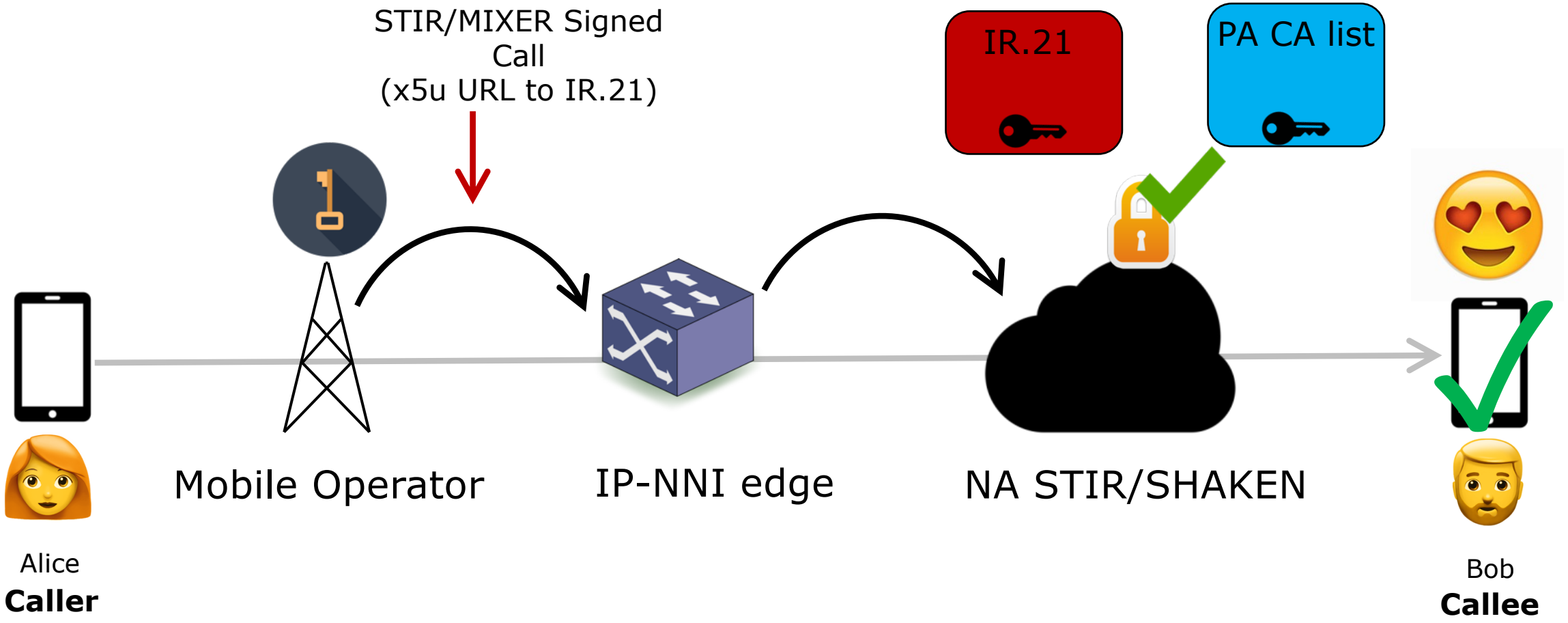
STEP 2 – INTERWORKING WITH OTHER ECOSYSTEMS

The GSMA is preparing a key management procedure to exchange key material between GSMA members and possibly extending trust to other secure domains such as FCC governed STIR/SHAKEN



GSMA Associate Member

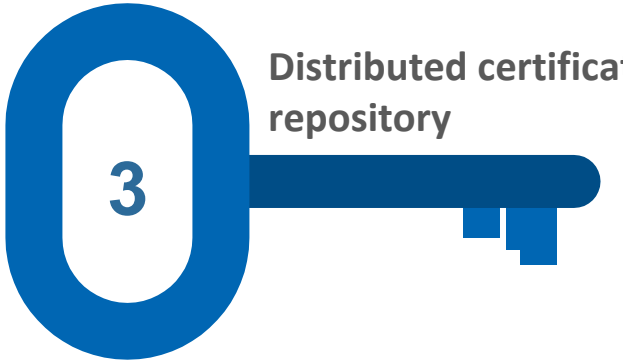
STIR/MIXER



Path 1: “x5u” URL points to a publicly available STI-CR

Path 2: “x5u” URL points to IR.21 service at IP-NNI edge (a “trust proxy”)

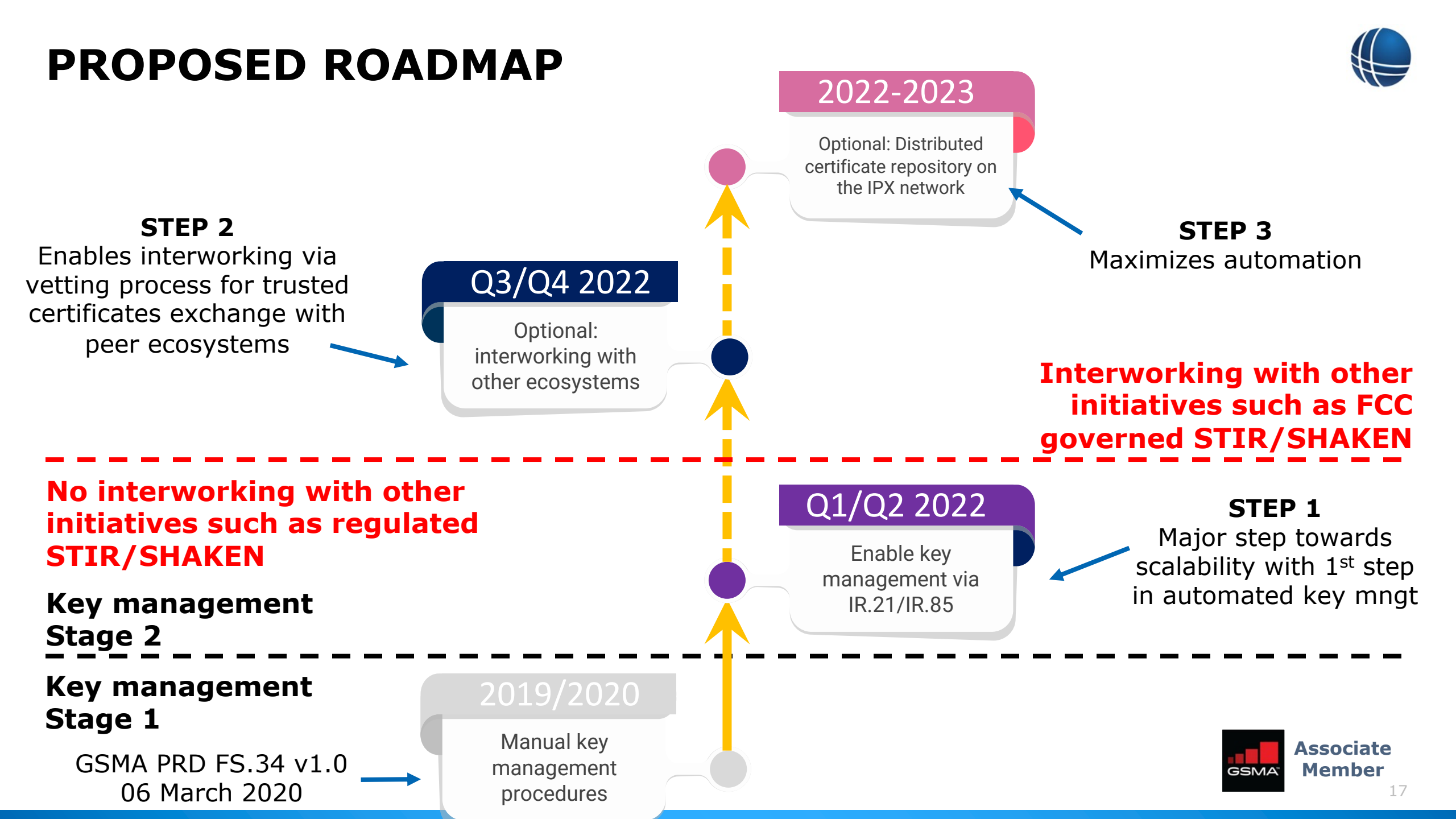
STEP 3 – DISTRIBUTED CERTIFICATE REPOSITORY



- Operators and other players to store key material (certificates) in a repository in the IPX network
- Maximizes automation and avoids manual mistakes
- This may be accomplished with DNS or just a plain web server

Associate Member

PROPOSED ROADMAP



Associate Member

NetNumber

www.netnumber.com

GSMA Associate Member