5G UCL for BFS

Advisory meet - 3

Architecture for review

August 17th 2021

Agenda

- Use case introduction
- Basic Topology in Lab for 5G setup
- Use case mapping
- Equipment for phase 1
- Plan for phase 2

Mapping a Use Case in Beyond 5G Infra

Context: Customer Due Diligence (CDD) - Video-KYC and beyond – multi-regulator, identity, authentication, messaging and digital twins

Stakeholders: Customers (person / legal-entities), Banks, Regulators, Channels (EMV/NPCI etc.), CERSAI, DBT, CERT-IN, Ombudsman (dispute), etc.

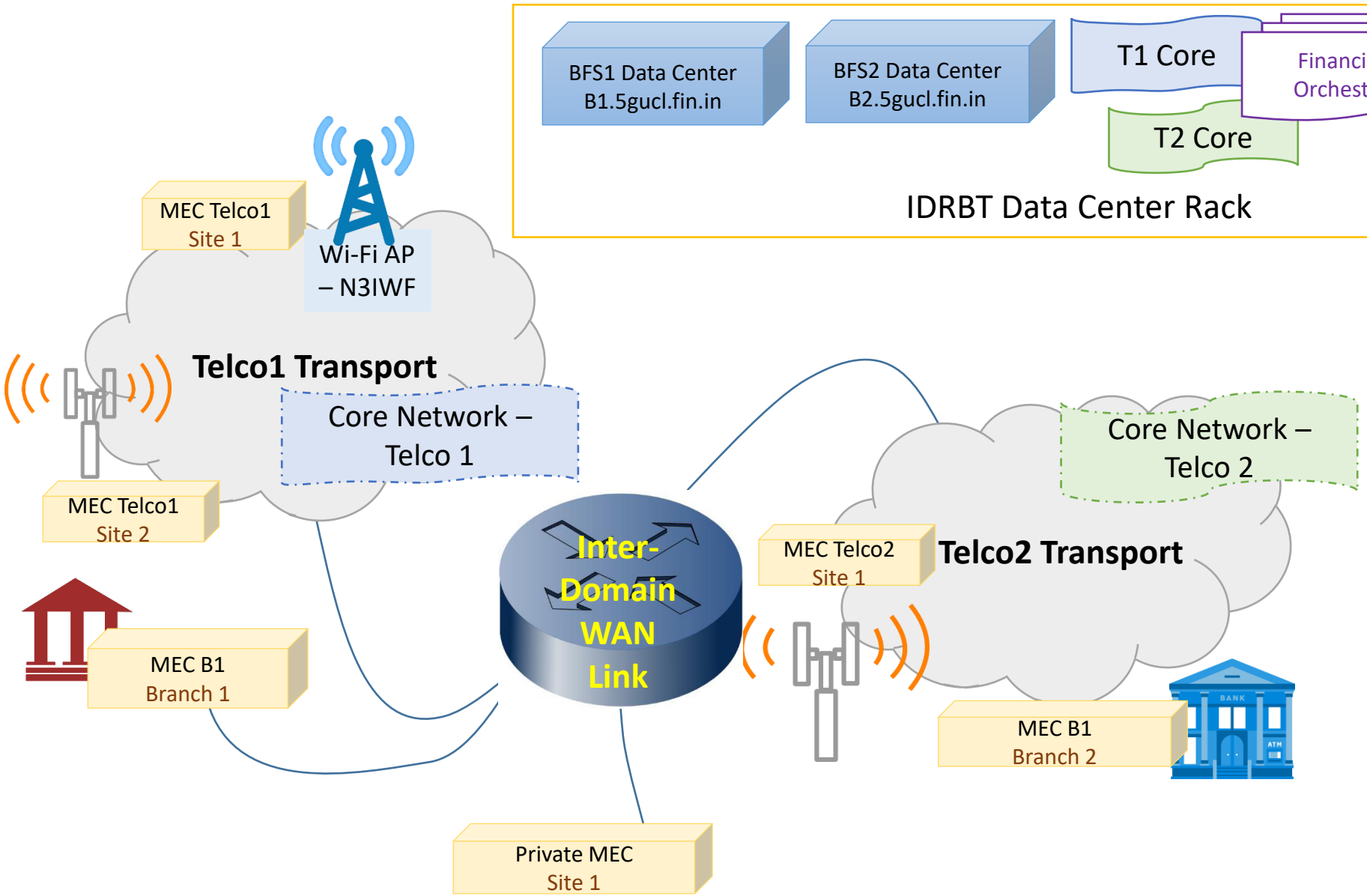
- Based on experience of **detected / attempted / 'near-miss' cases of forged identity**, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be **reported as a cyber security event** under extant regulatory guidelines.
- The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier **or if the name appearing in some negative list** should be factored in at appropriate stage of work flow.
- The **authorised official** of the RE performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and **obtain the identification information** using any one of the following:
  - OTP based Aadhaar e-KYC authentication
  - Offline Verification of Aadhaar for identification
  - KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer
  - Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through **DigiLocker**
- RE shall ensure to **redact or blackout the Aadhaar number** in terms of Section 16.
  - In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is **not older than 3 days** from the date of carrying out V-CIP.
- The entire data and recordings of V-CIP shall be stored in a system / systems located in India. REs shall ensure that the **video recording is stored in a safe and secure manner** and bears the date and time stamp that **affords easy historical data search**. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.
- The **activity log along with the credentials of the official performing the V-CIP** shall be preserved.

DIP – Doing in Pockets –

Benefit beyond compliance

- Pain of reporting issues
- Access to negative list – across departments? across orgs?
- Training the “authorized official” of regulated entity
- Obtaining the contextual information – APIs to India Stack etc.
- Redaction in Aadhaar record stored – how about redaction in Video?
- Access to KYC details as part of subsequent CDD – or is it only for compliance?
- Do we / should we analyse the VKYC recording for offering financial services? E.g. under user consent -
  - Mine video recordings and background content;
  - Behavioural biometrics - tightening security high value transaction etc.
- Activity logs of KYC to be retained. How about subsequent access to data?

Basic Topology @ 5G UCL



Financial Slice Orchestrator as **MOCN**

Multi-Operator Core Network

TBD: **MORAN**

Multi-Operator RAN

Mapping Video-KYC: In Beyond 5G Context

- Human/physical actors
  - Customer (human) and banks App running in a Smart-phone
  - Authorized official of Regulated Entity on a workstation or smart device
- Tech components
  - API calls to CBS, CERSAI, India-Stack etc.
  - Video / Audio and behavioural analytics – can have multiple engines in parallel
  - MEC / Network capability exposure – telco APIs to BFS
  - Messaging / authenticating – multi-factor aspects for signing in to the app or accessing VKYC tool
- Risks / Challenges / Opportunities
  - Rooted device; VPN/tunnelled traffic (falsify geo-location);
  - Placement of video-recording/streaming/interaction components
  - Alibi of banking-infra / other vertical context

Slices / MEC / Cross-vertical . . .

- Enterprise BFS Slice
  - API calls within financial enterprises and India-Stack components
- MEC / AI-ML innovation
  - Video analytics – varied implementation based on context
- Data-sharing of VKYC – details
  - Risk minimization vs. revenue optimization
- Additional context – neutral video feeds from ATM/Kiosk/Smart-city . . .
- Consumer BFS slice – secure messaging etc.

Enhancements to Basic setup

- Stand-Alone vs NSA

- mmWave support (reaching gbps speeds)
- Go beyond the lab room – cover the campus

- Model bank branch
- Model kiosk

Equipment Need

RAN - Radio heads + Decode

Plan - Two units + One spare

- 500 mW(intra lab)- 2 W (within IDRBT campus); around 3.5 GHz; (band n78)
- Ensure Integration with 5G Core – At least Release 14, Release 15 or higher preferred (next slide)
- Modular/inter-operable solutions (ORAN or similar)
  - Preferably open designs
  - Preferably open source, or licensed access to API / source for academic research

Generic Compute + Network

- Edge and Transport network – 10gbps – 4 switches
  - Either copper or fibre within the lab (10 metres spread)
  - SDN + Controller based deployment;
- Core Network Stacks – EPC/MAGMA/CEWIT - 6 workstations
  - with 10gbps cards; DPDK support must, min 8 core (16 logical cores) at 2.5 GHz or higher; 32 GB RAM; SSD HDD – 1 TB;
- MEC – Six setups – 18 industrial grade workstations + 6 switches
  - CPU capacity 20 GHz, Passive cooled GPU, 50TFLOPs tensor compute(FP16 or better); 32 GB RAM; 1 TB SSD; future upgrade to 4 TB RAID-5 HDD; power supply – more than 300 watts (500 watts preferred)

Software Need

- Core Network
  - Release 14 or better; upgradeable to release 15/16
  - Modular
    - N3IWF, MEC and Application Services Interfaces
  - Open Source preferred
  - Slice orchestration and policy settings through API
  - Flexibility to demo MOCN and MORAN
  - Interface with at least
    - one other open-source Core Network
    - One open-source MEC Network

- MEC – OpenNESS or similar

Integration Need

- Radio / RAN with Core Network
- Traffic Flow Across two Core Networks
- MEC + Core Network

Development (Other than Use Cases)

- Lab health dashboard
- Test / troubleshooting tools
- Bank1, Bank2 Platforms - Fineract

Radio Head + RAN

- SA vs. NSA – either is fine
- Expected through-put and Device Counts
  - 20 simultaneous COTS UE
    - total sustained simultaneous load around 100 mbps
  - Expected 200 mbps(up)+200 mbps(down)
    - for single device within few meters (indoor) – connecting to server within User Data Plane
- Optional – ability to support unlicensed spectrum (5.8 GHz)

- Tech Options
  - MIMO – 4x4 or better
  - MORAN support – required
  - Emitted Power-range – at least 500 mW to 2000 mW
    - manually tuneable
  - Frequency band – N78 – primarily because we expect more COTE UE in this range
    - TDD as spec'ed for N78
    - 40 MHz or higher bandwidth support
  - RAN Split – all splits are open as of now

Other Aspects

- Sourcing of components – country of origin / lead time etc.
- Warranty / spares?
- Getting the vendors attention during commercial setup for phase 2

BACKUP

Software/Services etc.

- BFS-UCL domain
- PBX – IVR/Voice and beyond
- Telecom Infra Project
- Rural-connectivity pilots
- Satellite connectivity

Architecture – Long Term –

Extend basic Lab Test-setup

- Adapt bank simulations for use cases
- Scaled down 5G networks for two Telco's + private 5G: Commercial radio units
- Edge compute integration for use cases
- Model Branch
- Model Field Agent
- Model Kiosk

Use cases

- Extended Reality – AR/VR/MR (eMBB)
  - Training, field visits, remote-assist in process flow
- Rural connectivity (5Gi/LMLC)
  - Branch (static) / BC locations (nomadic)
- IoT/mMTC
  - Branch – operational aspects
- Video and Video analytics
  - ATM / Branch / vKYC etc.
- Others
  - Next gen branch - post-pandemic – teleporting of staff
  - Kiosk / next-gen ATM
  - mPOS / next-gen FI platform
  - Edge : BFS as contributor
  - Cross vertical services

Key Differentiator for BFS

- **Slice**
- **MEC**

Collaborations

- TSDSI/ITU – standardization efforts
  - Multi-domain autonomous platform for financial services
  - BFS Enterprise slice
  - BFS Consumer slice
- Hackathon++
- Capacity building / focussed skilling
  - IDRBT - BFS
  - Across institutes – new course / lab exercises etc.
- Basic Internet Foundation (Oslo University)
- OAI - Eurecom

Multi-domain autonomous platform for financial services

- Goal – application level user stories for capturing system requirements

- Lead generation for loans / SHG etc. in financial inclusion aspect

- Possible subsystems, players (BFS/ICT) and activities
  - MEC / edge
  - Connectivity /
  - Authentication /
  - identity / privacy / commissions / recovery / closure / loan renewal etc.)

BFS Enterprise Slice

Information Required	Inputs
Background for the need for proposal indicating for example	
(i) use case solution	Network Slicing for Bank and Financial Services Specific QoS
(ii) gap in existing standards	Banking specific cross-operator network providing MPLS level and better connectivity for Bank infra; Utilizes additional security and context exposed by the 5G network
(iii) new requirement	
(iv) any other	This approach allows other industry verticals to get better security / QoS
Proposed outcome	
(i) Study report	Existing Challenges, Recommendations and Proposed Approach
(ii) Standard (new or enhancement of existing standard with name of such standard)	May be new Standard for Banking Services [security/context/edge-optimization/messaging/deployment-architecture]
(iii) Both of the above	
Dependence on any national or international standard, existing or under development or on any ongoing work in TSDSI	Does not exist today
Proposed timeline for start and completion of work including phases for completion of different parts of activity, if any	October 2020 - Sep 2021
Potential impact	Banking and Financial Services, Network Service Providers, Application Providers
Probable stakeholders/verticals who are expected to benefit from the outcome	Organizations providing Banking and Financial Services, FinTech, and other consumers of the BFS (e.g. retail PoS)
Supporting TSDSI member organisations, if any	
Any other information	

BFS Consumer slice

Information Required	Inputs
Background for the need for proposal indicating for example	
(i) use case solution	Network Slicing for Bank and Financial Services Specific QoS for consumers
(ii) gap in existing standards	SMS are delayed and not encrypted, Not Gauranteed, There is no banking specific - Physical and Network Layer Security, multi-factor authentication is exposed to attacks
(iii) new requirement	What alternative authentication and authorization can be deployed for users and IoT devices of consumers to improve security and trust
(iv) any other	
Proposed outcome	
(i) Study report	Existing Challenges, Recommendations and Proposed Approach
(ii) Standard (new or enhancement of existing standard with name of such standard)	May be extensions to bootstrapping, exposure of secure messaging API etc. as domain specific needs for Banking and Financial Services as well as other industries requring higher level of security and authentication
(iii) Both of the above	
Dependence on any national or international standard, existing or under development or on any ongoing work in TSDSI	Does not exist today - may extends or degrade to SMS - but adds new aspects like geo-coordinates or other context to aid security/authentication
Proposed timeline	
Potential impact	Banking and Financial Services, Network Service Providers, Application Providers
Probable stakeholders/verticals who are expected to benefit from the outcome	Organizations providing Banking and Financial Services, FinTech, End Customers
Supporting TSDSI member organisations, if any	
Any other information	