UN/NGO longer term standardization of Security Communications Systems

RFBI - "Request for Bright Ideas"

May 31 2019

1. Introduction

TESS ('TElecoms Security Standards') is an interagency project, requested and initiated by the Inter-Agency Security Management Network (IASMN) Technology Advisory Group (TAG) and the Emergency Telecommunications Cluster (ETC), mandated by UNDSS (United Nations Department of Safety and Security).

TESS' goal is to make clear recommendations on the standardizations of future UN and NGO Security Communications Systems ("SCS") supporting staff safety and security. TESS works at the level of connectivity, applications and procedures.

The project's final aim is a new security telecommunications business model that is approved and supported by all stakeholders.

The project is a collaborate effort between UN agencies, funds and programmes, NGOs, the private sector, government entities and individual technical / operational / security specialists. TESS is coordinated and facilitated by WFP (UN World Food Programme) on behalf of all stakeholders.

2. The longer term Security Communications Systems' architecture

While TESS works on active field support and standardizing the *short term* security telecoms systems, the project is also mandated to define the architecture, hardware (connectivity), software (applications) and the supporting security procedures for the *longer term* security communications' standards.

The high level architecture for the future "Security Communications Systems" (SCS), has been defined as follows:

a. BYOD ("Bring Your Own Device"): End users use their mobile phone to connect to the SCS.
b. Data only: The SCS ensures each user has, no matter where he/she is, at all times, a data connection of at least 20 Kbps.
c. This data connection allows any end user to contact, at any time, the Security Operations Centre (SOC) in their operational area, which provides security and

safety support to field staff. In the other direction: the SOC should be able to contact any end user at any given time, no matter the user's physical location.

3. The "problem" use cases

In a "stable" environment, mostly in developed regions, the basic functionality is easy to understand, and straightforward to technically support using current technologies.

For example:
In the morning, a user in Nairobi has his/her mobile phone automatically connect to his/her home WiFi, up to the point of leaving the house. On route to the office, the phone automatically connects to the public 3G/4G mobile phone operator, ensuring a continued data connection. Once in the office, the user's mobile phone detects and connects automatically to the office's WiFi, all the way up to the point of returning home in the evening.

This basic scenario example covers many field operations most of the time, but the challenge comes in those scenarios where we don't work under "normal conditions in a developed area", varying from field operations with restricted or non-existent public data services, to operations in conflict areas, in natural disaster scenarios or in crisis situations.

Within the TESS project, a core interagency team has defined eight "scenarios" or "use cases", which are a technical challenge to provide data connectivity services to users.

These "problem use cases" are:

Use case 1: "Lone Ranger": A user is located in an area (anywhere in the world) without a public mobile data service. How can we provide data services to this single person, using the person's mobile phone?

Use case 2: "Lone Vehicle": While on mission, a vehicle with several end-users, drives through an area (anywhere in the world) where there is no public mobile data service available. How can we provide data services to the vehicle and its passengers in and around the vehicle, using the passengers' mobile phones?

Use case 3: "Camp": End users work in a well defined and physical confined area, e.g. a refugee or resettlement camp, a work compound or a staff accommodation complex: How can we provide data services to all staff working in this area, using their mobile phones?

Use case 4: "Rapid Deployment Camp": This is a variant of the "Camp" scenario, specifically geared towards rapid deployment operations, where we need to

provide these services in emergencies (typical for natural disasters) or temporarily (e.g. a temporary camp for a displaced population after a flood)

Use case 5: "Disconnected City": This caters for a variant of the "Camp" scenario, where the users work in a larger area, e.g. a city, which is not covered by public mobile phone data services.

Use case 6: "Brown Out": This scenario caters for those operations where "in day-to-day operations", there is a proper coverage by the public mobile phone networks, but for one reason or the other, these data services become suddenly, and temporarily, unavailable for hours or days (while the voice/SMS services are still available). Here, the challenge will be to provide data services on a contingency basis to users who "normally" connect to the public data networks.

Use case 7: "Black Out": A variant from the previous scenario, where all mobile phone network services (voice/SMS AND data) fail or are unavailable.

Use case 8: "No data roaming": This scenario caters for instances where data services on the local mobile telephone networks are available, but data roaming on these networks is either unavailable, limited or too expensive to use. This use case caters for many of our staff travelling frequently.

4. How can you help? - The core of this RFBI - "Request For Bright Ideas"

This is a public, open and informal call for "Bright Ideas" suggesting solutions for one or more of the above problem use cases. The "Bright Ideas" can be submitted by anyone as individuals, organisations, private sector or government entities. The ideas are considered as informal, non-binding and public. The ideas might be based on services, hardware or software from your own company or organization, or something you, as an individual, picked up along the way.

"Bright Ideas" should be submitted by email to TESS@wfp.org, before June 30 2019. They should be short (two pages maximum) and clearly indicate which of the above scenarios it caters for, describing how the solution might work, and how it would solve the problem scenario.

Your "Bright Idea" might be based on an existing, upcoming or future technology, or merely outline an idea or solution.

Please see the Appendix for more detailed information on the RFBI process.

5. Where do we go after the RFBI?

a. Early July 2019, we will organize a **first public meeting** with onsite and online participation of all interested stakeholders. This meeting will provide inspiration to

all, allowing us to formulate a more formal RFP ("Request for Proposal"). As part of the discussions at this meeting, we will look at all submitted "Bright Ideas" at the level of (a) technical feasibility and (b) applicability.

b. All parties who submitted a "Bright Idea" will be invited to submit a more formal proposal as part of the **RFP process**.
The RFP will be circulated early July and remain open for submissions until end of August.

c. Mid September, we will organize **a second public meeting**, again with onsite and online participants, to shortlist those proposals we would like to test. A more elaborate selection criteria list for this process will be published as part of the RFP.

d. The shortlisted RFP proposals will be **tested in a laboratory environment** from Nov 1 2019 to March 1 2020, and **pilot tested in the field** from March 1 to May 1 2020.

e. Based on the outcome of the tests, we will make a **formal proposal for the longer term SCS standards and systems**, to be presented for formal endorsement to the Interagency Security Management Network (IASMN) and the ETC in June 2020.

Appendix: What should you take into account when answering the RFBI?

- This RFBI is a non-binding inquiry and does not constitute a solicitation. The TESS project reserves the right to change or cancel this process or any of its requirements at any time during the process.
- The purpose of this RFBI is to gain a more detailed understanding of the existing solutions both to identify types of solutions, solutions providers, and to fine-tune the problem use cases as described higher up.
- The RFBI is an informal and non-committal process. As such no financial information should be provided at this stage of the process.
- By submitting your "Bright Idea", you agree we can use your input as part of the TESS project, and can be discussed publicly.
- Do not disclose any confidential information with your "Bright Idea".
- When you submit your "Bright Idea", you must disclose any restriction on the use or realization of your "Bright Idea" that you know of, such as the need for a license in respect of any proprietary technology or other intellectual property rights.
- Subject to any restrictions that you have disclosed, you agree to grant WFP, as facilitator of the TESS project, a non-exclusive, transferable, sub-licensable, royalty-free, perpetual, irrevocable, right and license to use, reproduce, publish, translate, sub-license, copy, modify, delete, enhance, distribute and otherwise exploit your "Bright Idea" in any way, in connection with WFP's mission and the TESS project. You acknowledge that WFP has no duty of confidentiality, attribution or compensation for your "Bright Idea", and you agree to indemnify, defend and hold WFP harmless if you or anyone else claims otherwise, claims

they have rights in your Bright Idea or if your "Bright Idea" otherwise violates applicable laws.

- Nothing in this document, or any other document entered into in connection with the TESS project, shall imply a waiver, expressed or implied, by WFP, the United Nations and the Food and Agriculture Organization of the United Nations of any privileges and immunities enjoyed by them pursuant to the 1946 Convention on the Privileges and Immunities of the United Nations, the 1947 Convention on the Privileges and Immunities of the Specialized Agencies, customary international law, other relevant international or national agreements, and under domestic law.