Document Details: Clarification questions in response to the call for proposals
Challenge: Scalable Phone
Deadline for questions: Tuesday 22nd October 2024
Questions publish date: Tuesday 29th October 2024

Q: Is the Authority able to elaborate on the relative priority of the 'Desirable features' outlined in the challenge statement?
Published Answer:

1) Visual and audio input can be fed into the device
2) Alias generation must exhibit a realistic pattern of life, geolocation, SIM card properties etc. [The challenge authors recognise this is a complex and wide-ranging feature and so an understanding to what extent the solution might meet the feature or interact with other components to achieve this feature is of interest].
3) Use of the cloud
4) Agility of alias generation so they can be commissioned and decommissioned rapidly
5) Could consider using Mobile Virtual Number Operator (MVNO)

Q: Please can the Authority clarify the nature of video and audio input that is required? Is this live video/audio calls or input of recorded video/audio?
Published Answer:
Either is interesting. Preferred an ability to simulate camera or microphone and expose a means to feed data stream by separate components.

Q: Is the Authority willing to consider a solution that includes a hardware element to enable the connection of SIM cards to the cellular network?
Published Answer:
Yes. But the hardware element should demonstrate ability to integrate SIM card components to software over a link – for example a secure network.

Q: Is there a requirement to use the system on a mobile device, or is a laptop-based system acceptable?
Published Answer:
In short either or both would be considered, and the evaluation will be based on the nature of the mobile device or laptop considered. A system that can encompass both would be interesting. A solution will be assessed on a balance of features.

Q: How many devices are required to be emulated for each officer?
Published Answer:
The solution should offer the ability to scale up and down or a clear path on how scalability might be developed in the future.

Q: How many devices are required to be emulated overall?
Published Answer:
The solution should offer the ability to scale up and down or a clear path on how scalability might be developed to around 200 devices.

Q: Does the Authority require a proposal that addresses a specific egress routing? (i.e. PoP capable/modem/MVNO/rebroadcast)?

Published Answer:

A solution would be welcomed addressing these concerns. The challenge authors are open to a range of ideas. The ability of the solution to be integrated with a network or network protocols is of-interest and may influence the scoring.

Q: Does the Authority require a proposal that addresses specific network capabilities (i.e. to include GSM 3G)?

Published Answer:

An approach that considers this in combination with the other features would be of interest. If a solution were to show how GSM 3G might be used at scale with other elements of the solution, this would be of interest.

Q: Does the Authority have a preferred modem supplier (an existing contract) that the proposed solution would work with?

Published Answer:

Not considered in this challenge.

Q: Does the authority have a specification or standard that will be required for the format and separation of evidential transaction data?

Published Answer:

No. The integrity of the data is important, but the evidential requirement is very much 'nice to have'. It should not become a focus or distraction; it can be considered in more detail in later phases.

Q: Can the Authority expand on/quantify the requirement: 'Could an officer use your solution to run multiple different aliases, with minimal contagion risk?'

Published Answer:

The solution should demonstrate isolation between components (software or hardware) or network transport such that a compromise by criminals of one alias would result in detection by criminals or other aliases. The technology needs to mitigate the risk of digitally linking one alias to another or shows what controls are in place to manage the risk of digitally linking one alias to another.

Q: What Cloud benefits are the authority looking to capitalise on by using cloud for this solution?

Published Answer:

Scalability, Deployment, Manageability, Automation, Integration with security systems, Deployment Agility not linked to the Authority and avoiding hardware capital cost.

Q: Can the authority expand on the encryption required for the proposed solution?

Published Answer:

The encryption required depends on the nature of the architecture of any solution. The goals of any encryption would be safe-guard data at rest and in transit similar to those offered by OTT apps. How data is to be stored and distributed over a network must be

protected and therefore assumed requires encryption. The Authority is interested in what encryption might be used and the potential for change in each solution.
The National Cyber Security Centre website provides the following guidance:
http://ncsc.gov.uk/collection/device-security-guidance/security-principles/protect-data-at-rest-and-in-transit

Q: Please can you clarify what you mean by Remote Control in the section “Solution should not include the following”?
Published Answer:
A solution that replaces a human with a mechanical device to interact with a user interface would be counter to the goals of the challenge.

Q: Will a successful solution require audiovisual input/output over the cellular network, or only via messaging apps?
Published Answer:
Messaging Apps are to be hosted. Audio/Visual is desirable. A successful solution will be one that meets the challenge across a range of factors and is compared against other proposals. A solution that supports audiovisual input/output over the cellular network and audio/video over the cellular and internet for hosted Apps is likely to score more highly than a solution that only provides connectivity to internet connections with all other factors being equal.

Q: Regarding the scoring of the proposal, is each section scored 1-5 or is there only overall score of 1-5 awarded?
Published Answer:
Each section is evaluated. The overall solution is also considered in the round.

Q: On page 5 of the document, in the 'Applicant details' section, it mentions that an application should include a 'registration number'. Does this refer to a registration number obtained from a community collaborator organisation, or something else?
Published Answer:
This is your company registration number

Q: Is there a requirement for an officer to communicate covertly with suspects?
Published Answer:
Depends on what is meant by covertly. Communication with suspects might take place with Apps that provide good levels of privacy. The ability to host these Apps forms a key part of this challenge; Any requirement relating to communicating with suspects only pertains to secure hosting of Apps or the proper use of cellular networks. However novel ideas that add value to the safety of officers, criminals and improves the likelihood of success for an investigation would be received with interest.

Q: On page 3 of the document, one of the constraints is that the solution 'Must be able to use mainstream and bespoke apps' - are there examples for either of these categories? Does bespoke apps refer to apps currently in use by the agency, or apps developed in conjunction with the solution provider?
Published Answer:

A solution which uses mainstream apps would be preferred but also robust to future needs and to have agility to respond to changing circumstances and technology.

Q: On page 2 of the document, in the section titled 'The gap', one of the points of consideration is whether the solution can be used 'where mobile phones are prohibited' - does this speak to a desire for the solution to be operable from e.g. a government issued desktop computer overtly, or by some more covert means?

Published Answer:

The intent is to provide background information about the challenge. Mobile devices such as phones are prohibited in certain areas such as places that are conducting sensitive investigations into serious and organised crime. Relevant to a challenge is that business must be conducted using Apps in such environments. Traditional mobile devices would not be suitable. Accessing Apps using a government issued desktop computer with safeguards might indeed be a context that a solution might be used. A safeguard might take the form of a system assured that microphones cannot be activated without direct authorisation of a user. However, the challenge authors do not seek to limit any proposal by dictating how the issue of working in secure environments might be solved.