Statement of Work (SOW)

Trusted Execution Providing Simpler and Stronger Priority Access

Technical Objectives

Provide an architectural frame work for peer to peer enrollment components and controlled granting of access and verify with the community the architectural models.

Provide a bench scale prototype for demonstration including

- Registration of a supervisor
- Registration of a new unknown device
- Registration of a person to a registered device
- Grant of access to a demo service
- Revoke access to a demo service
- Develop a token mechanism as a viable control model for the community
- Establish a cloud view for the group of authorized devices
- Secure data delivery demonstration as a group service

Provide a reference architecture and design document for Phase II proposal that will outline the prototype to pilot plan and critical dependencies.

Verify minimum viable prototype to be integrated with a carrier test solution.

Evaluate and integrate an example identity service to verify real world attributes. To verify identity and request service from a pre-existing permissioned list.

Evaluate and define the minimum data requirements for an in person or peer to peer delivery of permission for access

Evaluate the minimum requirements for a supported device and the cyber control minimums to grant or revoke services and the level of effort to support each of the platforms securely. Provide a discussion and matrix of the different solutions for each core feature.

The prototype will be built on Android with Trustonic TEE other platforms will be reviewed to determine viability for future work and minimal security for phase 2 or 3.

Work Plan

1.1.1 Program implementation plan

A status report documenting the progress and open issues will be submitted monthly or as required to the COR and technical lead during the period of the contract.

Informal review meetings will be held as required between Rivetz and the Government team supporting the project on a mutually agreed schedule.

Periodic partial demonstrations of functionality will be provided throughout the project as defined by the COR and Technical Lead.

All work conducted will be subject to the technical direction, approval and surveillance of the COO and COR

1.1.2 The base period technical plan

All man-hours are estimated government sponsored man-hours it is expected that Rivetz will invest significant additional time in the project as part of its own ongoing R&D investment.

Expected hours by category:	
Applications Developer (Senior)	240
Applications Developer (Master)	240
Information Assurance/Security Specialist (Master)*	36
Project Manager	32
Subject Matter Expert (Master)	120
Total	**668 hours**

1.1.2.1 The initial prototype framework weeks 1 – 6 Estimated 150 man-hours

The initial prototype framework is expected to take six weeks and will provide the solution with all of the major components operational. These will include.

Detailed project architecture and work plan
Detailed security and token model to grant and revoke service
Outline of the group management model
Partner selection for KYC process
Documentation

These tasks will primarily be documentation with some early rapid prototyping in software and will build on the existing systems Rivetz has already put in place.

1.1.2.2 Phase 2 – Service Creation Weeks 7-12 Estimated 150 man-hours

This is expected to take four weeks and will address the tools to manage the identity mechanisms for the solution as well as base line authentication and attestation work.

Registration of a device to an administrator
Token delivery
Granting access
Revoking access
Preliminary health check by registration server
Details of token identity and attribute design
Documentation

These tasks will primarily be software development and will be accomplished through an agile development process. The work will be done by the core developers on the project. Deliverable will be component demonstrations.

1.1.2.3 Phase 3 Enhance the prototype 13 – 18 Estimated 150 Man-hours

Show a first service authentication
Show working KYC process
Expose group communication model
Enhanced reporting and visualization of group controls
Collect data on current industry devices and capabilities

This work will primarily be software development and will be accomplished through an agile development process. The work will be done by the core developers on the project. The industry data is an ongoing project and will be produced as an interim deliverable. Component demonstrations.

1.1.2.4 Phase 4 Final delivery Week 19 – 26 Estimated 218 Man-hours

Complete demonstration and establish reliable public demonstrator.
Concept demonstration to first responders
Documentation, Installation instructions and demonstration guide
Final test report
Failure mitigations
Known weakness
Detailed reports on cyber controls
Detailed report on integration with OpenID and 3rd generation partnership project
Detailed engineering plan for phase II proposal.

This work will engage the full team to prepare and deliver the final work product of Phase 1 and will be a team effort.

1.1.2.5 Final delivery

It is important to note that the goal is to deliver a bench scale prototype of the complete functionality with real cyber controls and fully executed trust boundaries. Identity verification will provide simple integration with a service and will not attempt to provide a full KYC proof. The prototype will not attempt to integrate with carrier services to actually provision priority service. It is the intent to substitute a simple access control model for the carrier network that will use a strong crypto access model that should integrate well with any global carrier system. It is also the intent to limit many of the edge cases that will be identified and planned for in Phase II work. Rivetz intends to fully commercialize a service using these capabilities and will be actively co-investing in the solution with the intent to use the group controls and services for many commercial access models.

1.1.2.6 Expected test use cases to verify technical feasibility

Register an administrator
Administrator to grant access to a user with an out of box commercial off the shelf android device
User verification of other identity attributes if required (KYC or identity checks)
User to access a service using an app (this is to simulate informing the carrier that this phone should be granted Priority access) with TEE verified credentials, user identity and SIM credentials
Administrator to Revoke access
View of logged data and active vs inactive users.

1.1.2.7 Work locations

All work will be performed in the USA

Rivetz has employees work from shared space and at home in California, NY, MA, NC and Ohio.

Steven Sprague	111 swamp rd. Richmond MA 01254
Sean Gilligan	308 Centennial St Santa Cruz, CA 95060
Michael Sprague	73 Bedford Street New York, NY 10014
Mark Hoblit	77 Dogwood Lane Franklin, NC 28734
Greg Laun	8818 8th Avenue NW, Seattle WA 98117