1 Technical sections

1.1 Identification and Significance of the Problem or Opportunity

The heart of the problem is how can first responders self-manage and automate access to priority network access service to enable access even when networks are saturated. Carriers manage advanced networks with varying levels of service and can already provide different groups of user's variable services. The challenge is in an emergency and with a low bandwidth environment it will be critical to assure that first responders can securely self-manage the group of devices that are allowed priority access in real-time and without human support from the carrier. This will require a strong authentication, strong identity and transaction channel between the first responder community and the carrier to assure priority service is only granted to authorized devices with authorized users.

Premium network service is a very valuable feature and as such will attract many attempts to steal access to the service. This can happen during normal operations and can be very dangerous and put lives at risk if it happens during an emergency. The challenge is to design a system that is resistant to fraud, is naturally self-healing, resilient, and anti-fragile. Username and password will not be enough and SMS based 2 factor authentication is clumsy and will not support the multiple device models. Biometrics does not move well across devices with unique sensors. The Trusted Execution Environment (TEE) used in this proposal will prevent cloning of keys and identities.

Identity verification exists in many forms. From online identity check with images of drivers license or other id's to knowledge questions to in person confirmation. The Rivetz solution is designed to create for the first responder a granted token for access. This token can be issued online based on identity credentials either pre-provisioned or in real-time. Or these tokens can be issued by an authorized supervisor peer to peer in a low bandwidth asynchronous environment. The carrier network will digest the tokens and grant access accordingly. Self-service validation of identity and peer to peer authorization will assure integrity and simplicity and dramatically reduce costs for the global first responder community.

The advent of smart cities and sharing services will enable a broad market of services that can be enable for similar access. One of the goals of this project and a key to commercialization of this technology is to show how the system for priority access could be used to grant and revoke permission for other modern services. (cars, hotels, stadiums, parking….)

User experience and simplicity is essential during an emergency. Access to secure communications and data will save lives. The challenge is to deploy advanced cyber security controls and at the same time not disrupt the user's normal device experience. Everyone should want to use a phone that has advanced service not be frustrated by it. A solution should act and feel as close to an embedded SIM solution as possible offering the first responders the same quality and security of service that the carriers enjoy.

These 3 challenges of Security, manageability and simplicity are the core to the innovative technical solution being proposed. Millions of modern devices now contain Trusted Execution

Environments (TEE). These components are bundled in the hardware of devices to address the cyber security challenges of the global payment and financial networks. These technologies are based on the Global Platform and Trusted Computing Group standards and can be found in hundreds of millions of devices. Continued investment and development of these technologies are driven by multiple global regulations from Payment Security Directive 2 in the EU to multiple NIST requirements. This solution will benefit from this global shared investment in cyber security and assurance standards.

The proposed solution is based on leveraging these standards and innovative technology to provide a secure network of tokens, instructions and identities that can be used to manage and maintain access to priority services. The assumption is that a strong message similar to a financial transaction can be delivered to the carrier, an instruction to either add or drop a user/device from the priority access services. The high assurance events are similar to secure e-commerce payments and will benefit from many of the same features.

This proposal does not attempt to explain the inner workings of the carrier network and assumes that network access is defined as only having a few offerings (Voice, SMS, volume and speed of data, effective date and expiration date).

Core to the innovation is the observation that authentication is not enough -- what is required are secure instructions. A secure instruction is a message that contains the information necessary to change the state of the system receiving it. The whole message is cryptographically signed and contains all of the identity and integrity information necessary to assure that only real instructions are executed and that instructions cannot be replayed or altered. Some mobile devices include advance capabilities for trusted display and trusted input These technologies can provide proper collection of user intent and visual confirmation that the instruction sent is the one intended and are very resistant to malware on a device. The solution will fully exercise these advanced capabilities offering an understanding of how advanced cyber security controls can be used to manage the provisioning of services.

The solution by Rivetz is based on using the Trusted Execution Environment to provide an isolated execution environment. Rivetz has built a Trusted App that executes within the TEE and provide the operational functions for identity and transaction/instruction creation or consumption. This secure and measured environment can be assured to protect the secrets and permissions that are required to manage the valuable service of priority access. In essence, providing the Government with its own carrier grade “virtual SIM” and subscriber provisioning system.

The solution also contemplates in the field provisioning by a supervisor provisioned device. The proposal is to examine the best model for in the field provisioning that balances simplicity with controlled registration of new devices. The expectation is that a supervisor could instantly grant priority access to a controlled number of compatible COTS devices that have not been pre-provisioned but contain the necessary TEE capabilities from the factory. The supervisor could easily register the new devices by using their existing device and provide a controlled level of access to the priority network. The solution will be able to support any number of service details

the carriers can offer. The supervisor should also be able to revoke access from any device under the supervisors control.

The mechanisms used to verify the right to access should be interoperable with the standards for access control for the 3rd Generation Partnership Project. The OpenID protocol can easily be supported by the TEE protected credentials and will offer a collection of interesting interoperability services from peer to peer encrypted messaging to secure emergency broadcast messages and a variety of access control possibilities. The importance of this work is that at it's heart is an operation model for managing secure access for things to talk to things. This Internet of Things model could easily be extended for electronic access to smart buildings, vehicles, and other services that can be provisioned by securely sharing keys and access control instructions. A message to a carrier to grant access for this identity to a priority service can be very similar to an instruction to let this individual operate a vehicle and here are the keys or to unlock a door and stay in a hotel.

Finally, the solution should contemplate continuous monitoring of the trust environment to assure that the trust environment is operating as expected. Any solution leveraging TEE should include the mechanisms to continuously monitor the health attestations of the TEE and assure that the device is operating in a known reference condition. The Rivetz solution is already experimenting with embedded health measurements and it provides the foundations for extending this research to the priority service network and the verification of the integrity of Devices and instructions on a continuous basis. The result is that a known device in a known condition with a known user is creating or consuming provable data and services.

1.2 Phase I 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.

- 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.

1.3 Phase I Work Plan

1.3.1 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 base and option period 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

1.3.2 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

1.3.2.1 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.

1.3.2.2 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.

1.3.2.3 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.

1.3.2.4 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.

1.3.2.5 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.

1.3.2.6 Expected test use cases to verify technical feasibility

Register an administrator
Administrator to grant access to a user with a 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.

1.3.2.7 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	824 Pelton St. Santa Cruz 95060
Ari Singer (sub contractor)	TrustiPhi 33565 Bainbridge Rd. Solon, OH 44139
Andrew Vandamia (sub contractor)	TrustiPhi 304 Woodhaven Drive Owego, NY 13827

1.3.2.8 Technical approach

The technical approach is to build on existing R&D investments in trusted execution and the development of a trusted app and the infrastructure to support it. The primary task in phase one is to construct a working prototype to grant and revoke access and explore the detailed use models that would meet the first responder needs. Rivetz has a platform that provides the basic cryptographic controls making it possible to rapidly develop in an agile process the basic use models required.

The proposed solution is based on the TEE environment that is created by ARM TrustZone and enhanced with the operating environment from Trustonic. Rivetz is a Trustonic application partner and is currently developing on the most current version of the Trustonic tools. Rivetz has selected the Intercede Ltd MyTAM service to provision the Rivetz TA. Rivetz is currently tested and operational on Samsung S6 and Note 5 phones that will be used for the demonstration running the current version of Trustonic. The solution will operate on other devices

Rivetz Net is implemented in Python and provides a JSON web API. The Rivetz Android Client (the adapter) is a Java App that includes NDK code in C++ to bridge communications with the Rivet Applet. The applet is implemented in C. Client applications communicate with the Rivetz Adapter using an include library (RivetzJ) available in Java. These components are delivered through the standard mechanisms for developer integration in use today. The Rivetz Adapter is served from the Google Play store and the RivetzJ library is release controlled and available for build inclusion from Bintray.

Rivetz Net and the Priority controls service are hosted with AWS and configured for scale. It should be noted, however, that the Rivetz server is only contacted during registration of health services and device pairing so it has a very light touch. While not yet implemented, the Rivetz Net private keys are designed to be hosted within an HSM. Rivetz will work with the government's Contracting Officer's Representatives COR and Technical Leads to determine the proper hosting environment requirements for phase II requirements

The Rivetz Priority controls service is built using standard authentication protocols. Extending this service to support a token model for access, OAuth and OpenID protocols is a low risk development project. The opportunity to create strong device identity working in concert with strong user identity provides a great are for innovation.

No government equipment will be required to perform the required work.

1.3.2.9 Description of the architecture used for the technical capability to support interoperability with other systems, scalability, performance, and security

The proposed system is interoperable with millions of commercial off the shelf devices. The solution is based on the standards foundations of the Trusted Computing Group and Global Platform. The solution is designed from the ground up to be integrated into third party apps. Rivetz has focused on building a solution that meets the needs of integration for mobile. There are four architectural components that are used by Rivetz to provide a unique and innovative implementation of the TEE infrastructure:

- The first is an access control mechanism that is used to onboard service providers to the trusted app. This provides the app with the ability to support multiple priority services models on a single device with different administrators. In addition, it provides the tools to assure that when a specific service provider is no longer permissioned to grant or revoke access then their service provider record can be terminated or suspended. The Rivetz priority service capability can be added as a built-in component for any third party android app.
- The second differentiating architectural mechanism is the support for an external PKI verification as part of the permissioning of tokens and access keys. This PKI mechanism is leveraged both server side and client side. It provides a foundation for extending access control to many external systems that can be local or remote. When enrollment is underway for a service it is possible to communicate with a second PKI device like a PIV derived credential or a match on chip biometric credential on a smartphone or an external PKI source local or even in the cloud to then participate in the grant and revoke process. It is expected that this will be integrated as part of the phase 2 or 3 period.
- The third key architectural difference is the use of a signed API call to assure that certain token creation services are only from an authorized service provider. The use of the signing key assures that the commands are direct from the service provider and can be used to reduce the surface for attack. The use of signed command direct to the client device assures that heath measurements from the device can be collected prior to granting access. The use of device health at the application layer enables new models for device integrity and device security.

- The fourth architectural difference is the security model is designed to have all of the sensitive operations take place within the measured Trusted Execution boundary. The use of attestation to measure will provide fondations that meet the proposed NIST guidance for Cybersecurity Framework V1.1. The boundary also provides a strong model for future certification. The goal is the Rivetz component is verified but the app leveraging it does not have to be verified, simplifying third party integration time and cost. This will provide the framework to achieve a FIPS 140-3 level 3 assurance for Phase 3 work.

1.3.2.10 Risk Identification and mitigation

- The core technical capabilities of the proposed solution have all been individually verified. The technical risk is low.
- Rivetz is a startup and such has constraints on resources, limited backup on personnel, limited capital and young systems. These risks are mitigated by a leadership team that has years of experience and are fully dedicated to delivering the solution.
- Interoperability with carriers and industry partners may add complexity that will have to be minimized to achieve a fully operational solution. The goal is to achieve a truly secure operational demonstrator as a minimum viable solution and demonstrate that the desired future is attainable within a reasonable budget. Complexities like derived PIV credentials for mobility should be considered for the future expansion but not gate the progress of industry capabilities.
- Certification is dependent on the underlying platform and Rivetz attempts to certify may take longer than expected due to the underlying Trustonic OS. Rivetz has been in conversation with Trustonic for over 6 months on this and is keeping close tabs on the progress. It is expected that the solution could eventually achieve a FIPS 140-3 level 3 credential certification but that is not in scope for phase 1 or 2 work.

2 Related R/R&D

Rivetz has been engaged in building developer tools for key management, encryption and attestation using the Trusted Execution Environment available on hundreds of millions of devices. Steven Sprague the co-Founder of Rivetz has over 20 years of trusted computing experience. Steven worked from project engineer to CEO of Wave systems Corp. (1990-2013) and industry leading DRM and Secure ASIC design in the 1990's, a founding board member of the Trusted Computing Group, a launch partner with Seagate for self-encrypting drives, developed and delivered 160 Million copies of the trust suite for multiple PC OEMS and numerous internal access control and secure content projects.

Rivetz was founded to develop and simplify the use of isolated credentials and assured instructions. The company has patent pending technologies and continues to push the research and operational uses of the technology daily.

Rivetz has existing relationships with multiple carriers and platform providers and expects to explore the core requirements of this project with those companies to better understand how the technologies can be supported going forward. Rivetz current context for conversation is very similar to the needs of this project and is related to secure financial transactions, cloud services

access and cyber security controls, Bitcoin/blockchain support, and IoT. This project will benefit from the day to day market research that is being executed by Rivetz in both the US and internationally with the supply chain. The advanced concepts of Managed Trusted Execution, identity, secure instructions, end to end encrypted messages, health and integrity controls and IoT provide a strong backdrop to collect and evaluate the existing standards and solutions needed to offer a world class solution and dramatically reduce the cost to implement and design a national infrastructure.

Specific R&D work has been underway for the last year for the US government.

The Blockchain Attestation Project demonstrated the integration of a real-time health and integrity measurement of the TEE as part of a Bitcoin transaction. This effort designed and built a proof of concept that leverages the industry standard attestation capabilities of the boot integrity of the TEE OS and its software components, including verification of the manufacturer root keys to verify the supply chain integrity of the TEE. These measurements where combined with external attributes and compared to a known good reference value in real time as part of a financial transaction on a modified blockchain. The advanced Cyber security controls work can be a building block for the cyber security requirements on this project. The contract was awarded in June of 2016 and final delivery was in October of 2016

Contract Number H98230-16-c-0599
Award Date 6/29/2016
Program Title: IMC-BAA-FY16
Contract Value: $49,000.00
POC Carol Lundquist clundqu@nsa.gov

Rivetz is currently working on the base period of a file transfer utility. This is a prototype of secure and assured data delivery to a known measured device. This project potentially could be used by the first responders to enable assured delivery of files to devices that have been registered and it is intended that the identity keys used will be interoperable with the file transfer capability. This will allow simple exploration with minimal work of secure data sharing to the same community that is granted access to priority bandwidth.

Contract Number H98230-16-c-0976
Award Date 9/30/2016
Program Title: Secure File Transfer Transactions
Contract Value: $856,000 4 month base 8 month option, as of this writing option has not yet been awarded
POC Carol Lundquist clundqu@nsa.gov

3 Key Individuals and Bibliography of Directly Related Work

3.1 STEVEN SPRAGUE citizenship USA

111 Swamp Road, Richmond, MA 01254 | (413) 330-9100 | steven@sprague.com

EDUCATION

Cornell University, Ithaca, NY B.S.M.E. in Engineering 1987

ADMINISTRATIVE EXPERIENCE

Rivetz Corp., Richmond, MA CEO January 2014 – Present

Rivetz is building on the embedded hardware security in modern PCs, Tablets, Phones and other devices to provide state-of-the-art protection for services that include authentication and trusted processing of sensitive information.

Etransfr, Rochester, NY Advisor, Mentor, Board Member February 2014 – Present

Chadder, a secure messaging application, is my daughter's start-up. I am very proud to be associated with this incredible project and the progress of her and her team. They are the definition of the next generation of entrepreneurs.

Factom, Austin, TX Advisory Board Member August 2014 – Present

Factom allows you to build applications on top of the Bitcoin Blockchain. Factom uses a simple API that lets you build projects that were not possible before while still harnessing the trust and security of the Blockchain.

Wave Systems Corp., Lee, MA Member Board of Directors 1996 – June 2014

Wave Systems Corp., Lee, MA CEO & President November 1998 – October 2013

Helping form and launch the Trusted Computing industry, building the leading player supplying the solutions built on TCG standards.

Launched first implementation of Virtual Smart Cards using TPM

Launched first demonstration product for Bios Integrity using TPM

Launched Industry support for Self-Encrypting Hard Drives and delivered Enterprise management to multiple fortune 500 customers and government

Launched First comprehensive suite of services for TPM and Delivered 160 Million licensed copies

Launched "Embassy 2100" first programmable smartcard reader with trusted input and trusted display using a TEE style hardware foundation

Launched "Embassy" First standalone cryptographic processor delivering Trusted Execution Capabilities and trustlet management

Launched "WaveMeter" hardware based micro-transactions and hardware DRM for assured data delivery

Wave Interactive Network CEO & President Fall 1994 to 1996

Spinoff of Wave Systems later re acquired building Entertainment market for Metering video, games, music and movies to a hardware DRM system for consumer entertainment

PATENTS

"Public cryptographic control unit and system" US 6449720

9,319,4192016Device identification scoring

9,047,4892015Security systems and methods for social networking

9,043,8662015Security systems and methods for encoding and decoding digital content

9,015,8572015Security systems and methods for encoding and decoding digital content

PUBLICATIONS AND PAPERS

"Modernize the Network"

White Paper for the Institute of Electrical and Electronics Engineers 2012

3.2 Greg Laun Citizenship: USA
824 Pelton Ave, Santa Cruz, CA 95060

EMPLOYMENT

Rivetz Corp. May 2016 - Present

I work primarily with Rivetz Corp. designing and executing cryptographic applications in Java and Android using trusted computing.

University of Maryland Experimental Geometry Lab September 2011 - May 2013

In addition to my teaching and research duties at Maryland, I co-directed the Experimental Geometry Lab. I directed semester-long undergraduate research and programming projects with teams of 5-10 students using primarily Mathematica and Python. I directed three additional semester long research projects one-on-one.

TECHNICAL

Languages: Java, Python, C/C++, Sage, R, Mathematica, Bash.
Applications: Android Studio, IntelliJ, Emacs, Git, LaTeX.
Projects: Contributor to the open source mathematical programming language Sage.

EDUCATION

UNIVERSITY OF MARYLAND, Ph.D., Mathematics, 2016.
Thesis: Proper affine actions of non-solvable groups in three dimensions, advisor William Goldman.
UNIVERSITY OF MARYLAND, B.S., Mathematics, 2010.
Honors: Departmental honors, *summa cum laude,* Higginbotham Award for outstanding mathematics major.
YALE UNIVERSITY, M.S., Psychology, 2007.
Thesis: Distributed search in real social networks, advisor Frank Keil.
Admitted to Ph.D. program. Left Fall 2008 to pursue mathematics.
NORTHWESTERN UNIVERSITY, B.A., Psychology and Philosophy, 2004.
Honors: Departmental honors, *summa cum laude,* Phi Beta Kappa.

PREPRINTS

Goldman, William M. and Gregory Laun. Affine Coxeter extensions of the two-holed projective plane. arXiv preprint arXiv:1511.05228, 2015.

PROFESSIONAL ACTIVITIES

Co-organizer (with R. Hunter) of weekly UMD Student Geometry Seminar, 2014-2015.
Reviewer for Cahiers de Mathématique de l'Université de Sherbrooke, Fall 2014.

3.2.1 Mark Hoblit Citizenship USA

250 Depot Street Suite 1032, Franklin, NC 28734

Rivetz Corp: October 2014 – present; Developed TEE applications on the Trustonic platform for Rivetz core and Rosie Wallet as an example Bitcoin wallet on the Rivetz API.
Self employed: February 2014 – Present; Bitcoin mining operation. Wrote scripts involved with maintaining bitcoin mining. Also worked on small automation jobs on oDesk.
eAutoBlaster.com: March 2011 – Jan 2014; Worked for eAutoBlaster to automate posting ads on Craigslist for many auto dealerships in many locations. Completed automated the tasks to circumvent phone verification, Captcha and email.
Drake Software, Inc.: June 2007 – January 2011; Vertical Market software development for tax preparers. Developer for multiple state calculations. Responsible for maintaining existing calculation for new individual, corporation, s-corporation, fiduciary, partnership and estate tax year forms including electronic filing and 2D bar-coding.
Neutelligent.com.: August 1998 - May 2007; Vertical Market software development for internet technologies. A successful garage startup where I was lead developer for live streaming camera rebroadcast software. Capable of more than 200 live images and each server could handle over 10,000 concurrent internet users using C++ and event driven. Other customized internet software written. Built dialup ISP services from ground up and managed the tech support employees. Company was acquired by Hostway.com.
Joey Technologies, Inc.: February 1997-August 1998; Vertical Market software development for handheld technologies. Lead developer for "Student Assignment Maker" program for automation of creating assignments downloading them to handheld devices, gathering data, and automatically grading assignments. Developed miscellaneous applications and installers for consulting projects using existing data entry software.
MicroBeam Corp: May 1995-October 1996; Technical support for products and created customized co-branded installers for clients on both Macintosh and Windows.
Payment Systems Inc: April 1994-March 1995; Maintained statistical reports and converted to newer SQL unix solution from older VAX/VMS system.
GEM Office Solutions: November 1992-April 1994; Converted Novell Netware/DBase solution to Information/4GL/Unix solution.
Whittemore, Business Owner / eAutoBlaster, 214-725-1390, davidbmw01@gmail.com

TECHNICAL:

- Languages: C, C++, C#, Java, ASP, PHP, VB, PowerBasic, Perl, Python, Cold Fusion
- Trustonic TEE trusted OS application development and test tools
- Applications: MS Visual Studio, GIT, SVN, CodeWarrior, Installer Makers
- Databases: MySQL, MSSQL, XML, JSON, DBase, Btrieve
- Operating Systems: Windows, Macintosh, Unix, WinCE, PalmPilot, DOS, VAX/VMS
- System Administration: Web, SQL, Firewall, Email, DNS, Radius
- Certifications: A+

3.3 Sean Gilligan Citizenship dual USA and Canada

849 Almar Ave, Suite C-220 Santa Cruz , CA 95060

SERVICES I design, architect, and develop advanced web applications, mobile applications
& web services. I also offer technology and strategic consulting to startups and enterprises.

QUALIFICATIONS Passionate and experienced software developer with skills in all areas of the software development life cycle. Team player or hands-on team leader who enjoys helping others succeed. Problem solver with track record of delivering innovative approaches to product design and system architecture.

EMPLOYMENT

June 2008-Present	**Consultant, Self-Employed (also Fingerpaint Labs)**
October 1999 – June 2008	**Founder & CEO, Catalla Systems, Inc.**
October 1988 – October 1999	**Principal, Open Systems Development**
October 1987 – September 1988	**Senior Software Engineer, Touch Communications, Inc.**
March 1986 – October 1987	**Software Engineer, 3Com Corporation**

TECHNOLOGY

Languages:	Java, Groovy, JavaScript, PHP, Perl, Ruby, Objective-C/C/C++/C#, x86/PPC/680x0 assembly, Bash, others
Tools:	Xcode, Eclipse, Maven, Ant, JUnit, Subversion, Git, others
Distributed:	REST, AJAX, XML-RPC, CORBA (RMI/IIOP), Java RMI
OS:	Linux, Mac OS X, Windows, BSD, Solaris, AIX
Java:	Spring IOC, Spring MVC, JSP, Velocity, Groovy/Grails, Apache XML-RPC, Swing, Applets, Rhino (JavaScript)
Java DB:	Hibernate, Torque, JDBC, Spring DAO layer
Database:	PostgreSQL (including PL/pgSQL), MySQL, Oracle, NoSQL
APIs/Libs:	Berkeley Sockets, Win32/MFC, Mac OS X/Carbon, others
XML:	XHTML, CSS, XSL, XSL-FO, SVG, DocBook, SAX/DOM
Protocols:	TCP/IP, SMB, NFS, Netware, XNS, AppleTalk, others

EDUCATION

1996 **BA, Computer Science and Economics** (Honors in both majors)
University of California, Santa Cruz

4 Relationship with Future R/R&D

The expected results from this research project is to lay the foundations for only known devices connected to sensitive networks and data. Strong device identity has been at the core of delivering cellular service and media services for the last 20 years. Enabling a virtual SIM and Virtual Conditional Access system will give the government a scalable private over the top network. A network that leverages the all of the transport/bandwidth mechanisms. A simple service for priority access provides a great deployment model to enable many new services in the future leveraging the same or similar infrastructure.

Phase one will demonstrate and explore the basic use models that need to be fully developed in phase II. The system can be thought of in two major components. The first is the mechanism to signal the carrier network for access to priority services. The second is the administration and identity model for authorized responders to grant and revoke access.

Phase 1 will help to verify the mechanism for granting access and simplify the conversation with carriers to embed the service within their architecture. There are many choices in the world of identities and tokens and it is expected that a few conversations could help hone in on a viable approach that could be standardized across the carriers and other ISPs. A standard API would rapidly enhance the integration and interoperability of solutions and prevent vendor lockin.

Phase 1 will also help to establish a working set of use cases for phase 2 on the grant and revoke identity methods that should be fully commercialized. Interaction with first responders and existing grant and revoke systems will improve the pace and effectiveness of phase 2 work. The mission is to provide a new service grant and revoke model that is scalable and accountable assuring the those who need access can easily achieve access in the field on commercial devices. There are many questions to be explored that go beyond priority access and could be used to support other services. Live drone feeds, National Blue Alert services, broadband access, shared data synchronization, identity validation are all interesting models that are directly supported by the work of this project.

Information and access will save lives and controlled access to subscription services is critical to any response. Enabling a system to grant access to priority connectivity is the first step to creating global over the top information sharing services. Information is ultimately created and presented by devices. This project lays the foundation for a shift to known devices in a known condition creating or consuming provable data. It is a critical piece of global response and also priority service is a simple and manageable project to deliver across the two phases of work.

5 Commercialization Strategy

Rivetz believes that the future is not a network of ports and passwords but a network built on the identity of the device and subscribed services. A world where registration of a device replaces the human known password and credentials are protected using state of the art hardware assurance. The company’s founders were instrumental in aiding the global adoption of trusted computing and trusted execution capabilities and have been part of the effort that has seen over 3 billion devices ship with integrated general purpose hardware security and assurance. The work that is executed as part of this project will provide a strong foundation for how the registration of

devices can be manages at the user level. The old models of central IT managing all access are long gone and a new model a social networking model is emerging. The management and creation of adhoc networks of users intent on solving a problem using Bring Your own Devices is the modern network of the future. However, controlled distribution of data and access are still required. We believe that this project will help to develop, expand and explore the use cases and cyber controls that will be required to build modern networks.

The government is exploring the deployment of PIV, PIVI and Derived credentials. These technologies are related but will never solve the unknown device problem. Unknown devices running unknown software will always create a huge risk. Trusted Execution and containerization and even hypervisor technology will all enhance the quality of data processing and assurance but it will only work if the device is registered. This project will enable a simple example of how all of the related device security tools can be registered and managed on a large scale. The investments made in building a strong subscriber servicing platform can be applied from cloud services to smart cities to smart cars granting and revoking access to use these technologies. The commercial scale will attract multiple solutions as the market is enormous and eventually all services will move to a grant and revoke model leveraging the device to manage primary access with the user as an attribute of their personal device. “I log into my device and my device logs me into everything”

Rivetz is actively pursuing the global commercialization of a network of devices as the solution to meet the modern cyber security controls. We believe the models explored in this project will directly influence the end of a LAN architecture of ports and passwords and facilitate a modern mobile model where services are delivered based on the device identity with a known user. The founders of the Rivetz team worked together in a previous company (Wave Systems Corp) to help launch Trusted Computing and deliver over 160 Million copies of OEM software and 10’s of millions of dollars in enterprise solutions. The team has already built a foundational set of tools and key management technology that are actively being use to deliver multiple capabilities today. From strong two factor authentication for single users to strong data encryption capabilities for DOD. This project will be a great example of the public private partnership between government and industry and show how industries multi-billion dollar investment in Trusted Computing can be put to work.

The company is actively raising capital and building partnerships to commercialize these tools and has existing relationships from startups to a major US Carrier. The shared investment will develop the use model for secure grant and revoke of service and the self service construction of a network of devices. These foundations will be applied across all global network services.

6 Facilities/Equipment

The Company is currently working out of home offices and rented shared work space with people in MA, NY, NC and California. The company has effectively uses this distributed model to grow the team and to enable access to the talent necessary to get the work done. The company is also a member of TIAC and has access to secure facilities in Silver Springs MD and can expand staffing as the project requires. This allows the company to be efficient in its overhead

exposure and enable the company to dynamically manage it's resource level. The company does not anticipate buying any government owned property to execute the project and will leverage infrastructure and devices already owned by the company. The commercial facilities that are currently being leased are fully compliant with local state and federal workplace requirements. The faculties are high end shared office space and as such have no issues with toxic materials etc.

The following locations are where work will be performed on this project

Steven Sprague	111 Swamp Rd Richmond, Ma 01254
Michael Sprague	73 Bedford Street New York, NY 10014
Mark Hoblit	77 Dogwood Lane Franklin, NC 28734
Sean Gilligan	308 Centennial St Santa Cruz, CA 95060
Greg Laun	824 Pelton St. Santa Cruz 95060

7 Subcontractors/Consultants

The company anticipates using the services of a small consulting group Trustiphi. It does not anticipate that more than 10% of the project value will be consumed by Trustiphi and no services may be secured.

Ari Singer (sub contractor)	TrustiPhi 33565 Bainbridge Rd. Solon, OH 44139
Andrew Vandamia (sub contractor)	TrustiPhi 304 Woodhaven Drive Owego, NY 13827

Rivetz uses technology licensed from Trustonic Ltd a UK company that develops the TEE OS that executes the Rivetz Trusted app they are the exclusive provider for many of the handset manufacturers and provide the solution on Samsung, LG, HTC, Sony, Asus and others.

Rivetz uses Intercede Ltd. also a UK company to provide the trust infrastructure for the Trustonic TEE OS there are multiple suppliers but no US provider at this time Rivetz may in the future integrate this functionality into its services model.

8 Potential Post Applications

The priority service project has tremendous commercial application. The proposed solution can be summarized as a large scale management and issuance of tokens that can be granted and revoked by administrators in a controlled and secure manor to known users. The use of advance payment services models for secure instructions and strong identity enable many new use cases. The market is ready for a new model of subscriber management and access control that is more distributed and much more dynamic. From retail applications where a token might give you access to a premium offer or early access to a facility to IoT application where controlled access to an event or even a shared asset like a car or a meeting location would be of value. The advent of smart locks and smart cars could easily benefit from identical priority access models for

business and first responders. We believe the technology developed to grant a priority access token for broadband could generally be used for many shared services.

On the federal level there are many advanced service that could benefit from group administration and granting of priority access. From online services to physical shared assets there is a real opportunity to use the global purchasing power of the government to reduce cost, fraud and waste. For example a phone could be provided a token that is used to indicate the user is authorized for the government rate. This could easily be provisioned by an office even to a user that only travels once per year and then for a limited time. As the sharing economy grows the ability to grant access to shared office space, meeting locations, and vehicles is a very real future for these technologies. The natural tokenization leveraged by the project will also provide a level of appropriate privacy for the government worker and the government when using services.

9 Prior, Current, or Pending Support of Similar Proposals or Awards

We are proposing a solution for HSHQDC-17-R-00010 topic H-SB016.1-005 under the same solicitation as this topic. The proposed team is the same today but we are growing and adding additional talent. There is capacity to execute both projects at the same time today.

The work does not overlap while there are components that might be interesting for Phase II the work is very different. The underlying platform will be similar as the investment being leveraged is the same.

The principle investigator will also be Steven Sprague
The project manager will be Sean Gilligan
Proposal number is HSHQDC-17-R-00010-H-SB016.1-005-0010-I

Title: Indestructible Identity on Blockchain with TEE
Submitted: Jan 18th 2017

10 Pricing Delivered Online

Apendix 1. SBA Company registration

SBIR.gov SBC Registration

SBC Control ID:	SBC_001212153		
Company Name:	Rivetz Corp.		
Address:	111 swamp rd		
City:	richmond		
State:	MA	**Zip:**	01254
EIN (TIN):		**DUNS:**	080090810
Company URL:	www.rivetz.com		
Number of Employees:			5
Is this SBC majority-owned by multiple venture capital operating companies, hedge funds, or private equity firms?			No
What percentage (%) of the SBC is majority-owned by multiple venture capital operating companies, hedge funds, or private equity firms?			0.00%

Company data certified as of December 22, 2016 | U.S. Small Business Administration | SBIR.gov