Rivetz Intl.

A wholly owned subsidiary of Rivetz Corp.

White Paper

June 29th, 2017

Ver 1.02

Cybersecurity for decentralized systems

Prepared by:

The Rivetz Team

Thanks to

The global communities of trusted computing and blockchain who have provided the foundations for our work.

NOTE: This white paper is a work in progress and defines the intent of the company to develop and market certain capabilities for the product. The implementations of these technologies are built on new models for computer science and security, and it is expected that significant changes will be continually required to meet evolving requirements.

Contents

Executive Summary 4

Rivetz Background 6

The Problem 8

Cybersecurity is failing in a mobile and distributed world 8

Regulatory Compliance 8

Internet of Things 9

The Global Attestation and Identity Network powered by the RvT 10

Rivetz Global Attestation and Identity Network 10

Architecture 11

Attestation is a core capability of the service 11

A simple process provides a powerful solution: 11

The protection model with TEE 11

Putting Tokens and RvT on the device 11

There are three different phases of operation 11

The Second Phase – Verifying cybersecurity controls 13

The Third Phase – Proving the state of the device for a competed transaction 14

Enterprise/ Individual Ownership of a RvT will generate transactions: 14

OEM Ownership of a RvT will generate transactions: 15

Service Provider ownership of a RvT will generate transactions: 15

Cyber checkpoint operators will generate transactions: 15

Building a future of utility micro-payments for devices 15

The application of the Rivetz solution 16

Multi-factor authentication with provable cybersecurity controls 16

Assured transaction Instructions for e-commerce transactions 16

Assured instructions for online and offline cryptocurrency wallets 16

Token project protection of client private keys and process 16

Machine multisig 17

A global market for the services powered by RvT tokens 18

Putting RvT to work – the next 6 months 21

The business model for security 22

The Cybercontrols Marketplace 22

The Global attestation and Identity network 22
The Cybersecurity controller 22
The application provider 22
First generation RvT use 23
The use of promotional RvT tokens 24
Detailed use cases 25
Two-factor Authentication with Cybercontrols 25
Machine Multisig with Integrated Cybersecurity Controls 26
Appendix 1. Token sale model 27
Appendix 2 Trusted computing and attestation 28
Appendix 3 Blockchain a general description 32
Appendix 4 About Rivetz 33
Rivetz Corporation 33

Revision History

1.0	First Version published
1.01	Minor revisions
1.02	Minor revision

Executive Summary

Rivetz is building a Global Attestation and Identity Network, powered by the Rivetz Token (RvT), in order to improve the security of the devices on which we rely. Cybersecurity Ventures anticipates that cybersecurity damages will total more than $6 trillion globally, up from $3 trillion in 2015[1]. The rising cost of cybersecurity reflects a failure of the security field to offer a solution that is both simple enough to warrant adoption by industry and government, and secure enough to protect our most valuable secrets and data.

Merely increasing spending without changing the way we think about modern security is insufficient. The existing tools: firewalls, virtual private networks and passwords all assume that the edge of the network is the network perimeter. This makes it too easy for non-authenticated users to probe and hack systems.

Rivetz is developing technology to push the edge of security to the screen of the device. Rather than a password being the last line of defense, individual devices can be deputized to broker access to valued online assets. The Global Attestation and Identity Network is intended to record and verify the health and integrity of the device using an RvT and blockchain technology. This new service builds on the last three years of work by Rivetz in creating the platform and tools to simplify a developer's access to the Trusted Execution Environment (TEE), a dedicated and impenetrable hardware platform that exists in every device.

Protecting data created and consumed by devices is an ever-growing challenge. Estimates peg the number of Internet of Things (IoT) devices to exceed 200 billion by 2020.[2] IoT devices are the foundational layer, where data is created. The IoT industry assumes you can trust the data from the device, but in most cases, this is not true. Rivetz, working with TEE, can create the much-needed trust.

The mobile devices of today are essential to decentralized data processing, but that processing can be easily corrupted. By focusing on the device identity, continuously measuring the state of the device, and enabling a new token based business model, Rivetz is constructing a new decentralized approach to cybersecurity and transaction assurance.

The Rivetz solution for the Global Attestation and Identity Network is built on a foundation of combining two global technologies. The first is the investment by industry of billions of dollars in trusted computing and global platform standards and the billions of devices that have been delivered with these capabilities embedded. The second is the revolutionary technology of blockchain that provides the decentralized key management, immutable storage and micropayments on a decentralized basis. Rivetz is combining these two technologies to demonstrate that provable cybersecurity controls are required to improve the quality, value and trust of data processed, shared and stored on the internet. Equally important, the Rivetz solution is intended to provide the economic model for devices to securely request and securely pay providers or other devices for health and integrity services.

The Rivetz solution takes advantage of the TEE, which provides Rivetz with an isolated execution environment within the main processor to execute code that cannot be observed or altered by the operating system. This vault on the processor enables Rivetz to store and process sensitive data, and

[1] Cybersecurity Ventures infographic http://cybersecurityventures.com/cybercrime-infographic/

[2] Intel Infographic https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

assure that policy and controls are executed as expected. The TEE is a measured environment that can be verified and proven to be operating in a reference condition. TEE capabilities have been available on both ARM and Intel architecture processors world-wide for many years.

Rivetz intends to introduce the RvT, a cybersecurity token that can enable the registration of devices and attest to their cybersecurity controls. The RvT is intended to be integral to delivering automated device-to-service or device-to-device payment for the consumption of the cybersecurity service and eventually other permissioned services. It is planned to assist the owner of the device to forensically prove verified cyber controls are in place when a transaction is executed.

The key to increasing the utilization of trusted computing technology is a business model that supports an ecosystem for security as a service. The Rivetz network is designed to support secure procurement of services, with a trusted mechanism for inexpensive automatic micro-payment. Rivetz plans to show how the RvT could bring these new business models to the device for the delivery and consumption of modern machine-to-machine procurement of services. The goal is to provide a source of payment (the RvT) that is bound by the owner's policy assuring that only approved service providers are paid.

The RvT model provides an operational role and a business role. The operational role will be intended to evolve as the technology moves from simple use to full integration into Bitcoin and Ether. The technology to efficiently integrate the solution has been prototyped, but some of the core capabilities used are still only on the mainstream blockchain roadmap. Rivetz plans to invest in the technology to operate and integrate the RvT into critical use cases. The goal is that every token and chain can take advantage of the cybersecurity controls that Rivetz enables. Note that no guarantee can be made that the goal will be achieved, based on factors including competition with other solutions and changes in technology.

The Rivetz team brings years of experience and leadership in trusted computing and blockchain technologies. Rivetz's established team has secured over a million dollars in contracted revenue from the U.S. government for other projects. Rivetz has operational technology currently compatible with over 500 million mobile phones as well as existing non-blockchain capabilities for multifactor authentication, embedded authentication, file encryption and secure messaging. The company leadership was part of the founding of the Trusted Computing Group in 2000 and has been an active blockchain cybersecurity contributor since 2013.

Every single day cybersecurity software proves unsuccessful in stopping attacks. Malware, malicious users, and targeted attacks create massive risk. For industry, government and consumers to realize cybersecurity success, they must begin with a foundation built on trusted hardware execution. The Rivetz plan is intended to monetize and implement solutions that deliver cybersecurity from the birth of the device to the confirmation of transactions for any service or IoT device.

Today, dozens of new token-enabled services are being developed; Rivetz is working to provide a secure automated mechanism to support micro-payment for many of those services. Metered access to services and capabilities could generate new revenue streams and new markets to serve the forecasted future 40 billion dollar IoT device market.

Blockchain has created a new foundation for value transfer on the internet. Trusted computing has created the foundation for protected execution on a device. Rivetz is building the network to put it all to work, empowering a new market and new revenue for a decentralized network of secure devices and services.

Rivetz Background

Rivetz is a “first-mover” with patent pending cybersecurity services and capabilities that leverage the Trusted Execution Environment (TEE). By providing a vault to isolate and protect keys and encrypted material from apps, malware, users, and hackers, Rivetz is focused on providing a truly safe experience for accessing all digital services – maximizing the quality and value of the provider-to-subscriber relationship.

Rivetz has been building this technical foundations for 3 years and has existing contracts with the U.S. government. The technical models for attestation have been part of global standards from the European Union to OASIS to NIST for many years but the economic model has been missing to support this ecosystem. Rivetz’ leadership has been part of the governance in this industry for the last 20 years, driving the adoption of trusted computing hardware and developing the technology services and economic models to put trusted computing to work.

Rivetz’s existing platform provides a unique set of market-leading solutions that have already generated over a million dollars in recent contract awards. Rivetz’ services and solutions can be leveraged by application development partners and service provides to enhance the value of subscribers on their systems. The company has a strategic relationship with Trustonic, giving it access to over a billion devices already in the field. Rivetz has also initiated discussions with major, established technology companies to support their commercial TEE solutions and potentially add billions more of devices that can utilize the Company’s capabilities.

Rivetz has invested over 3 years in executing a well-thought-out and novel strategy to create the market and capitalize on this substantial opportunity. In Q1 2017 the company was awarded a US Government contract and in Q2 it was further awarded an SBIR contract by the Department of Homeland Security (DHS) Science and technology (S&T) directorate. By simplifying the user experience and assuring that information is delivered as intended, Rivetz has designed a solution that could unlock new models and services and provide value to users for years to come. Rivetz believes it has the short-term tactical plan to quickly engage customers to drive revenue, and the long-term vision to unlock the full potential of the technology which will produce a game changing market opportunity.

One of the great challenges in trusted computing is providing the proof that the TEE is what it says it is. The purpose of this paper and the launch of the RvT is to put the last 15 years and hundreds of millions of dollars of research to work by leveraging blockchain technology to prove the measured portions of a device have not been altered.

Rivetz’s existing solutions and application enable protection of keys and protection for messages, and provide a solid starter platform to deliver the real cyber security control attestation of the health and identity of the device that creates a secure message or instruction. The Rivetz solution contemplated with the RvT is further intended to provide cyber security based on *math* that can prove that measurements made have not changed over time. There are no silver bullets in cyber security, and everything is vulnerable, but these tools represent simple integrated cyber controls that Rivetz believes are world-class and military grade.

Rivetz's founders have played a critical role in the creation, development, and adoption of Trusted Computing. The innovation of blockchain, when combined with the innovation of Trusted Computing, could enable a transformation to a new paradigm that delivers a safe, secure and private experience for digital services. Rivetz is building the platform, tools, and services in order to enable this distributed and decentralized cybersecurity control and a microtransaction model to meter its use as core infrastructure for the digital future.

In 2016, Rivetz built a reference architecture to validate the health and integrity of the device as an integral part of the transaction on a blockchain, delivering a decentralized cybersecurity control providing proof that the device' internal and external controls were in a reference condition prior to the completion of a specific transaction. https://youtu.be/XUG7-UCmZjY The following discussion explains how Rivetz intends to use a new token to enable the administration and operational security required to accelerate the use of these solutions by the global market, ushering in the new paradigm for cybersecurity architecture. The Global Attestation and Identity Network has the potential to accelerate the transition from the existing network security solutions to a new model built on the assurance that the connected and measured devices are performing transactions the user intends. In Rivetz's view, this is not only essential for a bold new world utilizing crypto currencies, but transforms data and network security as well.

The Problem

Information assurance, or confirmation that information on a device has not changed, is one of the biggest challenges in modern computer science. The evolution of the network, common access and the use of services has changed rapidly over the last 10 years. Cybersecurity protections have struggled to keep up.

Cybersecurity is failing in a mobile and distributed world

With rapidly evolving computer and mobile systems cybersecurity, the old models of software only security software is always one step behind the bad guys. Antivirus solutions built for enterprises and personal computer networks cannot address the rapidly growing mobile and IoT markets.

- Legacy security systems developed for desktop PCs and in-house networks were not designed for a real-time, mobile device driven world where sensitive information flows across public network systems to largely unknown devices outside the conventional network boundaries of enterprises, organizations, and government agencies.
- Cybersecurity and privacy are often at odds. Strong trust in the device provides the safe place to tokenize services and dramatically enhance the privacy of transactions and data.
- Cybersecurity has failed to keep pace with evolving threats caused by the increasing use of mobile devices, blockchains, smart contracts, IoT and cloud computing.
- Blockchains and smart contracts require a new model for cybersecurity to protect private keys and instructions.
- Software-based security models focused on monitoring and detection have added complexity, frustrating users, while failing to prevent cyber-attacks.
- Cyber-attacks have been pervasive and have diminished the value and quality of services that could otherwise be delivered, thus hindering growth in the digital services market and limiting the value of subscribers to service providers.

Ginni Rometty, IBM's chairman, president and CEO, said, "Cyber-crime is the greatest threat to every company in the world." And she is right. During the next five years, cyber-crime might become the greatest threat to every person, place and thing in the world.

Adm. Mike Rogers, commander of the Cyber Command and director of the National Security Agency, said "There are only two types of organizations: those that know that they've been hacked and those that don't yet know."

Regulatory Compliance

Another growing challenge is regulations. For example, The European Union GDPR “General Data Protection Regulation” can fine companies up to 4% of their gross revenue for a data breach. GDPR goes into effect on May 25, 2018, giving businesses around the world a chance to prepare for compliance, review data protection language in contracts, consider transitioning to global standards at least as compliant as the GDPR, update their privacy policies, and review marketing plans, efforts which will continue long after the GDPR effective date.

The reach of California’s data protection law, SB1386, has been extended such that it is not only important to prove that encryption was enabled on a lost device but also that its credential systems have not been compromised.

The measurement of the capabilities and integrity of the device assures that only known devices, with known capabilities and known users are consuming or creating provable data. Existing guidance from many NIST publications require these capabilities on future systems (NIST SP800-147, NIST SP 800-63.3, NIST Cybersecurity Framework, and others).

The global ecosystem of trusted computing devices and specifications has been deployed to meet the challenge but lacks an economic model that facilitates implementation.

Rivetz's Global Attestation and Identity Network (GAIN) assures the identity and integrity of the end device and assures the device cannot lie about its capabilities. Rivetz's proposed solution will be intended to automate one of the hard problems in information assurance, namely proof that a control was in place at the time it was required. Equally important, the Rivetz solution is designed to include an economic model of micro-payments driving adoption.

Internet of Things

The Internet of Things (IoT) is projected by many to represent one of the fastest growth areas of new global commerce for the next 20 years. Forecasts estimate $4 trillion in revenue by 2020, linking 25 billion things with perhaps a trillion sensors. The exciting thing about the IoT forecast is the next five years are only the beginning. Indeed, forecasters believe growth will rapidly accelerate shortly after 2020 as companies recognize the huge benefits from IoT.

Today there is virtually no provable security for the end-point device being used in IoT. The end-point is critical because it is most vulnerable, it generally operates without human intervention, and, importantly, is the source for decisions by the rest of the system. The entire IoT system assumes the end-point is truthfully reporting accurate data.

Rivetz's proposed solution creates a compelling business case for the manufacturer of the IoT device to include security in the box. This supplies a major element that is missing from IoT today.

The Global Attestation and Identity Network powered by the RvT

The innovations in devices and the addition of Trusted Computing has attracted a huge commitment of time and resources by industry and provides a critical component of the solution. The revolution of blockchain and the decentralized controls and keys combine to make a new infrastructure for trust built on math and signatures and not human promises. Together these technologies provide the platform to enable a new paradigm for cybersecurity.

The RvT token is designed to explore the full value of the paradigm, in order to deliver not only the cybersecurity controls to assure a known device in a known condition with a known user produced or consumed provable data, but also to assure that the device can be trusted to follow the policies of the owner and procure services automatically.

The RvT token has the potential to play a role in providing a core infrastructure component for provable cybersecurity controls. The merging of trusted computing and blockchain can change how modern business models and capabilities are delivered by automating the continuous validation of cybercontrols as part of authentication, secure messaging and secure instructions. Higher utility services can be created and delivered if the device is prevented from lying and stealing. The evolution of technology is alive and well and AI, bots, big data, IoT, and other big ideas will benefit from better cybersecurity and a utility-based business model.

Rivetz Global Attestation and Identity Network

Rivetz has a vision of a global ecosystem of cybersecurity checkpoints empowered by a blockchain microtransaction model. The decentralized network of cyber-checkpoints enforces the policies the owner of the device specifies, assuring only known devices in a known condition are allowed to access and process sensitive information. The decentralized network of TEE enabled devices supervises and enforces the owner's policies for utility service microtransactions assuring only the services requested are settled in RvT.

The decentralized systems of the world need provable cybersecurity controls to assert that certain data is real and reliable. The RvT is intended to provide operational security and enable the business model for integrity validation and attestation of transactions in real time. RvT is a utility token used by the owner of the device and service providers to assert that a transaction was sent by a measured system in a reference condition. The spend of an RvT token can be locked by a TEE enforced policy on a device and can only be used according to the rules the owner sets, dramatically reducing the risk of theft or misuse.

What is Health of a Device?

The trusted execution environment provides isolated execution of code on the main processor. When the TEE is powered on, the code that is executed inside the TEE is signed and the signatures are verified before any code executes. Each step verifies the signature of the next step before it runs. As designed, this chain of trust guarantees the "**integrity**" of the code is verified. The last signature "**the health**" of the device can be checked assuring nothing has been changed.

The RvT token is purpose designed to integrate with the data structures and methods that are required by the Trusted Computing Group and Global Platform standards to assure that devices have provable capabilities. These technologies are standards-based, have been developed over the last 20 years, and have been shipping on new devices globally for over 10 years. The systems are based on hashes and digital signatures but like any technology have their unique models as well. Blockchain technology provides a great fit and many of the capabilities have already been fully integrated simplifying the level of resources required to support different solutions. More data on the details of Trusted Computing is included in Appendix 2.

Architecture

The Rivetz architecture is designed to deliver provable cyber-controls for the owner of the devices ranging from PCs to smartphones to "Things". The solution operates on a decentralized trust model providing the proof the owner needs without having to trust third party services or sites to back the claims made. The solution provides an embedded utility token to provide secure settlement for services from known provable service providers. Different devices have the potential for varying levels of assurance. The Rivetz architecture is designed to flexibly adapt to these variances.

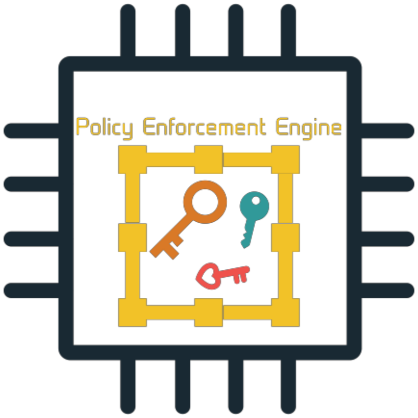
Attestation is a core capability of the service

RvT tokens provide a new approach in the blockchain market designed to assure attestation and policy are fully integrated into the process. The TEE provides the policy enforcement on the device to assure the rules are followed. The processing of the token is designed to verify the integrity of the TEE assuring the policy was in place. It is a symbiotic linkage that is intended to embed the information necessary to prove that a known device in a known condition with a known user produced a provable instruction with strong privacy controls. A primary goal is that privacy is protected and all device-controlled transactions will only occur between parties known to the owner of the device. The identity information is tokenized in order to seek to assure tracking of transactions on a chain is not bound to a specific service. However, the RvT token will require that all parties are identified to the owner of the device reducing the risk that malware can extract value from the automated systems.

A simple process provides a powerful solution:

The protection model with TEE

The TEE provides the protected application of policy that governs the use of a key or a RvT token. Once an RvT is passed to the TEE protected private keys it can only be transferred if the device owner's instructions meet policy. The owner of the device is the administrator of the Rivetz policy controls in the TEE and defines the process the owner expects to be followed. To reduce the risk of compromised instructions, the process integrates an attestation test and prevents a transfer of RvT if the health of the policy is violated or its enforcement cannot be verified.

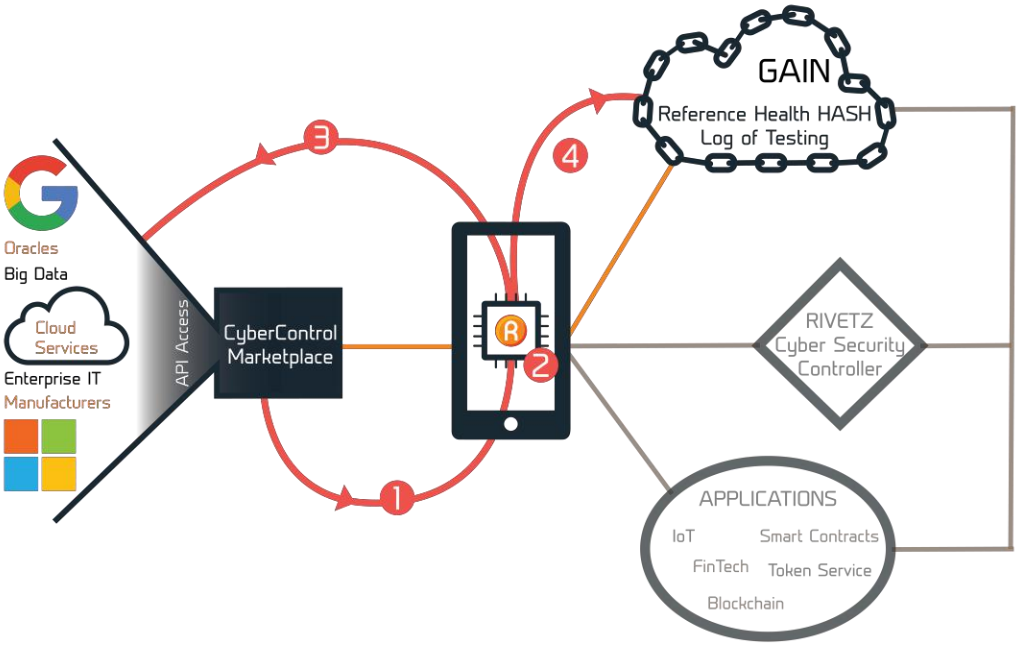


Putting Tokens and RvT on the device

The device is provisioned with RvT tokens and the owner of the device determines the policies that are in place and required before the TEE can use any of those tokens. The TEE policy can be altered by the owner of the device locally or remotely at any time depending on the requirements for compliance The TEE will always follow policy to transfer the tokens and such instruction will always include a verification that the TEE is in a reference condition. This prevents any tokens from being transferred by the machine without the owner-approved policy being applied.

There are three different phases of operation

The First Phase Registration of a reference health



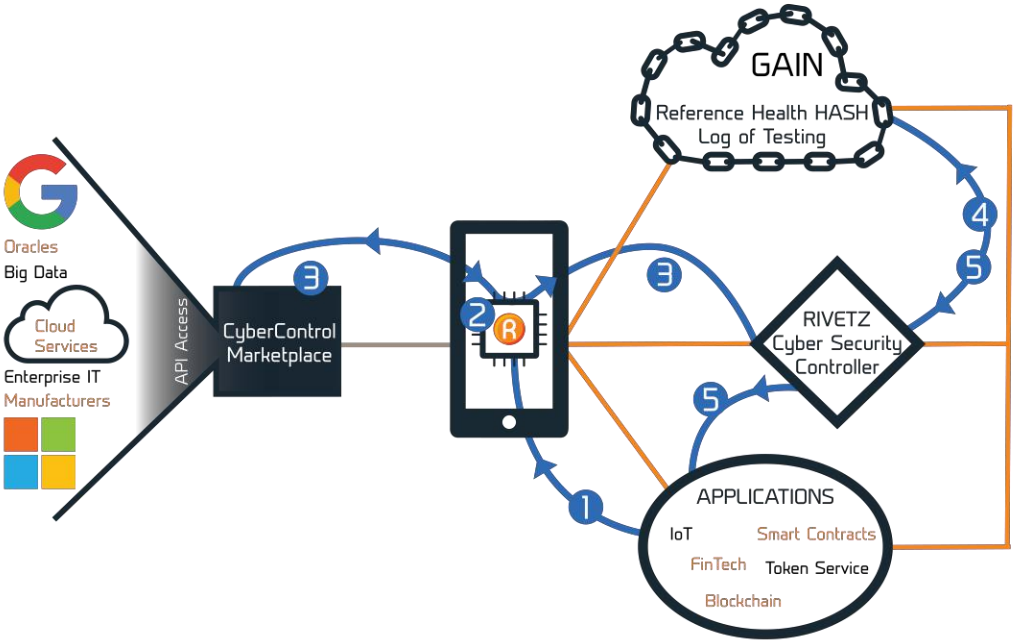
Step 1 The device is paired with the Cybercontrols Marketplace

Step 2 The device calculates its internal health and integrity hash and prepares to have the manufacturer signatures for the core root of trust verified by the Cybercontrols Marketplace

Step 3 The Cybercontrols Marketplace executes an owner-provided script to validate any external controls, Enterprise or cloud. It also verifies the manufacturer core root of trust signatures are valid for the Internal device tests. The external health hash is returned to the device. The RvT will be used to obtain these services as required.

Step 4 The device uses an RvT token to seal the combined internal and external health hash and record this reference health measurement on the Global Attestation and Identity Network. There is a microtransaction required to perform this service. The device records the location of the health hash for later use.

The Second Phase – Verifying cybersecurity controls



Step 1 The user selects a service that requires a health check and the device creates a unique transaction ID.

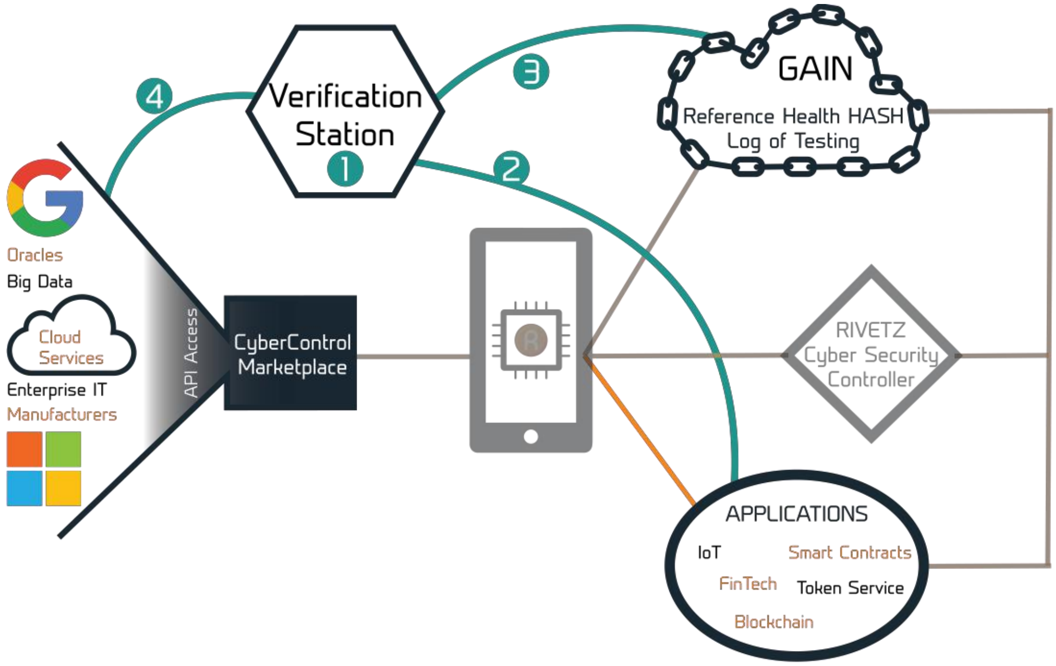
Step 2 The device performs an internal real-time test and an external real-time test and calculates a combined real-time health.

Step 3 The device seals the combined real-time health hash with the reference health hash locator with an RvT token and transmits the request to a Cybersecurity Controller for verification of a match.

Step 4 The Cybersecurity Controller retrieves the reference health hash and compares it to the real-time health hash. If they match, the device can be said to be in a reference condition.

Step 5 The Cybersecurity Controller delivers the logged event with a transaction ID to the global attestation and identity network and the results of the verification to be logged by the application as appropriate.

The Third Phase – Proving the state of the device for a competed transaction



Step 1 A request is made to audit a transaction.

Step 2 The transaction ID is used to locate the logged event and verify the test was true

Step 3 The reference health hash is received.

Step 4 The owner provides the Cybercontrols Marketplace the hash and the transaction ID that was used to create the external hash and the process executed to calculate the internal hash. The Cybercontrols Marketplace will verify the math and generate a transaction report for the owner proving the controls that where measured prior to the execution of the transaction.

There are many capabilities that may provide future expansion for service delivery and enhance the functionality of the network and the utility of the RvT token in turn.

The RvT could be used by many members of the network, and it is expected that services will grow over time.

Enterprise/ Individual Ownership of a RvT will generate transactions:

- Register owner account
- Register the identity of their devices from 1 to thousands
- Record reference integrity measurements
- Manage policies on the device for access to and use of services
- Administer access to logged compliance and encryption data
- Update and remove devices

- Manage and make global micropayments for service
- Have access to use the Rivet Network

OEM Ownership of a RvT will generate transactions:

- Record and secure a reference core root of trust for the health measurement (i.e., a device birth certificate)
- Establish identity for settlement
- Manage micropayments for device supply chain validation

Service Provider ownership of a RvT will generate transactions:

- Route traffic to public a Cyber Checkpoint
- Prepay for validations as a perk to users
- Manage cloud encryption as a service

Cyber checkpoint operators will generate transactions:

- Operate a Cyber Checkpoint
- Collect micropayments for service
- Enable secure logging of data
- Offer new services

Building a future of utility micro-payments for devices

The RvT token is intended to provide a device with a mechanism for obtaining decentralized services. Devices need such a strong mechanism for automated access and for a use-as-you-consume model for extremely small transactions. The RvT token is designed to cooperate with the TEE to provide the security and transaction models required. History has shown that metering-based models are easily abused and fraud is hard to detect. To realize the incredible future of billions of devices as an Internet of Things, the Internet will need a mechanism for ensuring that devices can be trusted. Rivetz believes that the GAIN achieves the unique balance between privacy and security or control.

The RvT token enables a device to initiate automated microtransactions that are supervised and verified by the TEE and the Cyber Checkpoint. The token is designed to have multiple controls embedded by the owner, the device, and the checkpoint as part of the end-to-end recording of the settlement. These controls provide a foundation for a broad class of utility payments that devices might require from storage to processing to replacement. The attestation capabilities developed by Rivetz are a core building block to enable automated transactions.

The application of the Rivetz solution

Rivetz has developed several internal services that leverage the attestation architecture and a general-purpose developer environment that will enable integration of these capabilities into any third-party applications. The Rivetz solution is designed to operate across the market and support isolated execution on both ARM and Intel architecture devices. Simple applications provide the foundation that will enable more advanced solutions in the future.

Rivetz expects to partner with several the existing and emerging token projects to assure cybersecurity is built-in from the beginning. Most token projects have a private key that could benefit from new models of protection from theft or misuse. The clear benefits for the services are stronger protections of private keys and critical functions within the trusted execution boundaries and a new model for integration of enterprise controls for decentralized networks.

Following are descriptions of a few general-purpose use cases.

Multi-factor authentication with provable cybersecurity controls

Many companies have implemented multifactor authentication as part of their projects. Rivetz provides the tools to enhance these solutions using provable hardware security. The attestation services will enable integration of external checks such as geolocation and enterprise status to be verified before authentication is confirmed to the service. Rivetz supports a 2FA capability today and this will be the initial service to support the RvT token capability with full attestation support.

A more detailed description is included at the end of the document

Assured transaction Instructions for e-commerce transactions

Rivetz is participating in the NIST NCCOE for retail e-commerce. Attestation can assure that the advanced cybersecurity controls in the device that are used to protect an e-commerce instruction are working properly and configured according the requirements of the owner of the platform. The RvT health and integrity validation of the users confirming device is a check that could be required to be performed as part of every e-commerce transaction.

Assured instructions for online and offline cryptocurrency wallets

The fundamentals of a secure crypto-currency transaction of secure display, secure PIN entry and protection of private credentials can be accomplished with the TEE for both online and offline transactions. Attestation that these controls are in a known condition can be integrated into the processing of the pay to script process. The result is the data recorded on the chain would have mathematically provable cybersecurity controls assuring the data recorded was intended, enhancing the quality and integrity of the data written to the chain.

Token project protection of client private keys and process

Recent projects for identity, storage and networking are using the blockchain protocol for innovative purposes. However, in general if you can steal the private key you can steal the service. Rivetz provides a model that will enable hardware protection of the private key and an embedded multifactor authentication. These cybersecurity controls can dramatically enhance the quality and simplicity of many of the token services. If the services integrate support for the RvT token, then attestation can become part of the provable claims the services can make, thereby increasing their utility. Custom development can further integrate the capabilities and bring a whole class of provable owner managed enterprise controls to the decentralized token solutions.

Machine multisig

Most token systems will support a multisig wallet for better protection. Rivetz intends to deliver support for machine multisig. Once tokens are placed into a multisig wallet the conditions must be satisfied to use the tokens. The user will use their favorite service but before the token transaction can be submitted it will need to be cosigned by a Rivetz Cybersecurity Controller (RCC) in the TEE. The RCC will receive the partially signed request and a RvT token with a real-time health test and the locator for a reference health hash. The cybersecurity controller will process the RvT transaction and use the resulting data to authorize the user’s transaction with their favorite token and deliver it to the service for execution. This will be a simple way to integrate support for the cybersecurity protections offered by a trusted execution environment with little to no integration. It is not suitable for small microtransactions where the RvT solution should be fully integrated.

A more detailed description is provided at the end of the document.

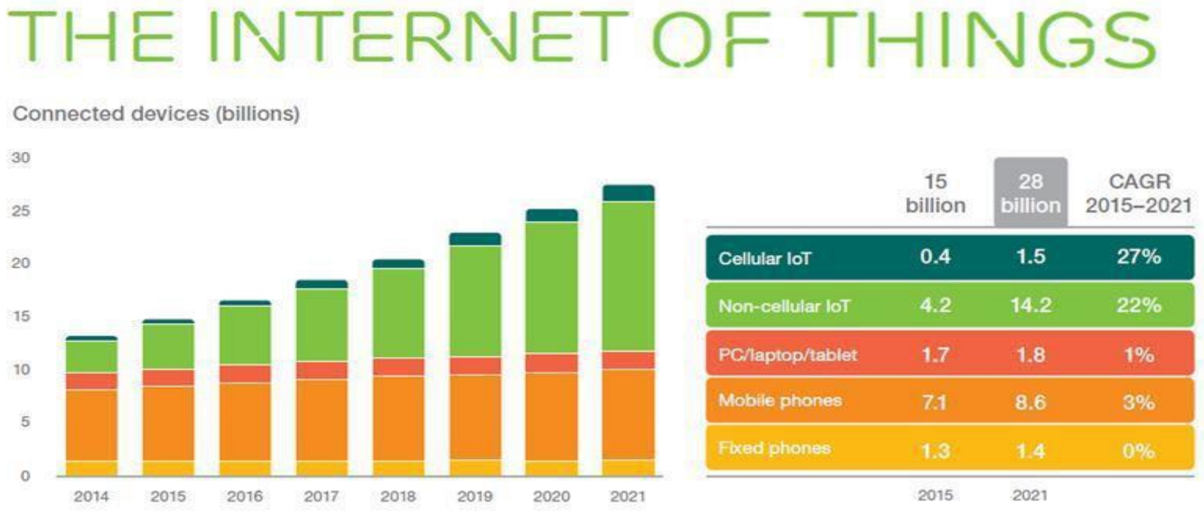
A global market for the services powered by RvT tokens

The market for the services and functionality of RvT Tokens is potentially vast and could be utilized by both currently shipped devices and future security chip and device sales. Driven by global cybercrime, regulations and the mushrooming IoT market, there is a mandate for a better solution to security.

A growing demand for improved cybersecurity is crystal clear in Cybersecurity Ventures' recent report. Cybersecurity Ventures, a firm that delivers cybersecurity market data, insights, and groundbreaking predictions to a global audience of CEOs, CIOs CSOs, venture capitalists, and government cyber defense leaders, predicts cybercrime will continue rising and cost businesses globally more than $6 trillion annually by 2021. The firm forecasts that global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the next five years, from 2017 to 2021. In 2017, Cybersecurity Ventures expects the global cybersecurity market to be worth more than $120 billion, having grown roughly 35 times over 13 years. The firm further expects 12-15 percent year-over-year market growth through 2021.[3]

The current mobile market with Trusted Execution Environment (TEE) capability is over one billion shipped devices. Combined with an estimated one billion enterprise grade personal computers deployed, this creates a potential market of a significant portion of over two billion devices with the ability to upgrade to Rivetz improved security.

Looking ahead, the opportunity grows even more rapidly when the explosive IoT market is added to PC and mobile device sales. The RvT Token business model encourages chip manufacturers like Intel and Infineon to include the RvT Token when selling their chips or device to manufacturers like Lenovo, Dell, and Samsung, to include it in the PC or mobile phone. (Note that these are mentioned for illustrative purposes; such commercial arrangements have not yet been established and there is no guarantee that any particular one will be.)



	15 billion	28 billion	CAGR 2015–2021
Cellular IoT	0.4	1.5	27%
Non-cellular IoT	4.2	14.2	22%
PC/laptop/tablet	1.7	1.8	1%
Mobile phones	7.1	8.6	3%
Fixed phones	1.3	1.4	0%
	2015	2021	

Internet of Things on Pace to Replace Mobile Phones as Most Connected Device In 2018, Forbes, July 9, 2016

[3] Cybersecurity Ventures infographic http://cybersecurityventures.com/cybercrime-infographic/

Gartner, one of the world's leading information technology research and advisory companies, forecasts that 20% of all enterprise endpoints will use Trusted Execution (that is, TEE-like) technology by 2020. Currently, over 400 million devices are shipped every year that contain Trustonic' s TEE capability.[4]

Rivetz believes that the market for distributed cybersecurity controls can not only be additive but can disrupt a portion of the trillion dollars in planned spending over the next five years. The creation of RvT as a strong token, with a business case, could create demand for the Rivetz new transaction based service model for device health and integrity. Combining the 2 billion devices already deployed with Trusted Computing and the emerging market of blockchain has tremendous potential. The global adoption of IoT is expected to require attestation for all IoT devices to assure that critical infrastructure is powered by known devices with provable capabilities and trusted data. From simple sensors to advanced automotive and industrial networks, attestation will be a critical cybersecurity control.

One of the primary drivers for attestation is to prove compliance / audit after an over-the-air update of firmware / software. Not only do you get positive confirmation of the success of an update, but you receive proof for compliance/audit purposes. This is becoming more important since more devices are including in-the-field update capabilities to address newly discovered vulnerabilities.

The Rivetz Global Attestation and Identity Network has the potential to deliver improved and provable security to a number of major global markets, including:

Internet of Things

- Strong device identity and registration prevents cloning or rogue devices
- Peer-to-peer provable encryption and assured messages
- Verifiable condition to detect and prevent tampering of distributed devices
- Enabling a global social network of machines
- Trusted data

Cloud Authentication and Access

- Tamper-proof identity protected by measured trust hardware
- Secure display assuring what you see is what you send
- Secure multifactor authentication anchored in provable hardware
- A simpler safer user experience. (Logging on is like pushing the "send button") secure, simple and

  protected by hardware in the device

Machine Automated Money with Policy

- Secure source of funds that can be autonomously used by the device
- Assurance that transactions are only executed according to the owner's policy for the device
- Secure model for on demand services and instant access to capabilities as required

- Simplify new models for on-demand access to cloud capabilities and services.
- Provide an extendable economic model for secure transaction on IoT

Cybersecurity Controls for Smart Contracts and Blockchain

- Provable/measured protections of the private key and transaction data
- Embedding proof that a specific device with measured controls requested a specific blockchain transaction
- Enabling privacy on the chain or in contracts by tokenizing recorded data and personal information
- Securing oracle data for smart contracts

[4] Gartner Group Innovation Insight for Trusted Execution Environments on Mobile Devices March 2017

Putting RvT to work – the next 6 months

The Rivetz strategy provides a logical go to market plan that is not dependent on others to launch, yet is intended to provide a strong fabric for partners of all sizes to benefit from the evolution of the network and the marketplace. Cybersecurity is a great first utility for a device to consume and offers clear benefits to the owner of the platform. The application of utility services to devices is only limited by the human imagination as billions of devices will need services.

Proof of compliance reduces the cost of audit and exposure for every global enterprise. Compliance is a top reason for investing in cybersecurity controls and as the network becomes more distributed, compliance has become more difficult. Rivetz's approach is based on years of research, and the new models of smart contracts and blockchain provide the technical framework for global compliance. The proof of compliance is for the benefit of the owner of the platform, but it also increases integrity of the entire system.

The business model of microtransactions requires devices have access to a settlement model. But, devices are like small children. They are easily parted from their tokens. The leveraging of the hardware security within the device will be intended to assure that transactions are executed with known service providers and the owner controls the policy the trusted hardware will enforce. The attestation protocols provide a strong integration with transfers of RvT that assures only known services will be able to transact with the device. The ability for a device to control access to services and to provide a microtransaction model could open new models for service delivery and assure every device may need an allowance from the owner.

Rivetz believes that the majority of the Blockchain and token based projects will benefit from integration with Rivetz capabilities. Hundreds of new companies are being built on the revolutionary change that blockchain brings to the market. The protections that a token and blockchain offer to the market are tremendous but only as good as the protection of the private keys and the instructions sent to the chain. Bitcoin spawned a market for hardware wallets but they are not the solution for the new token models from storage to networking and cloud services. Rivetz cybersecurity solution is designed to bring a strong model that will enhance the value and simplify the use for many of the existing proposed token projects.

The RvT token will provide a disruptive business model and decentralized cybersecurity controls to deliver greater utility and a simpler and safer experience. The RvT token model is intended to assure the distributed control and resilience that may reduce the central failures that cloud security creates. Innovation in blockchain, IoT and cloud development is limited by the cybersecurity risks. The global attestation and identity network powered by the RvT token and its partners intends to address these global challenges.

The business model for security

As we have seen there are billions of devices with TEE-capable hardware, a growing number of services that can provide attribute validation, and hundreds of thousands of services and billions of users that are demanding better cybersecurity. What is missing is a network and an ecosystem that can:

1. Deliver near-real-time, Internet-scale registration, attestation, and verification of cybersecurity controls
2. Preserve user privacy
3. Provide economic incentives for hardware, software, and service providers to offer cybersecurity controls of ever-increasing quality
4. Provide a micropayments model for delivery of these services
5. Allow for Coasian bargaining in allocation of the costs of preventative cybersecurity measures

The Global Attestation and Identity Network solves these problems.

The RVT token is essential to the operation of this network.

Simple interfaces and protocols provide an ecosystem that will invite players small and large to support a new utility model for security. Each component provides a unique connection point into the service and each will provide services to the owners of the billions of devices we use every day. Providers of any of the services will be responsible for setting their own requirements for their business models

The Cybercontrols Marketplace

The owner of the device will have the opportunity to configure and select the services they wish the device to verify in order to achieve the external reference measurement. These controls can vary from free components to connect to existing enterprise services, extensions to commercial products to verify controls or cloud service that could provide anything from time of day to location. The services and business models will vary and the RvT token will be one of the mechanisms for settlement.

The Global attestation and Identity network

The owner will configure the device to use their preferred service provider to store and manage the Reference health measurement and the logging of results from verification performed by the cybersecurity controller. The system is built around a simple unique locator to enable any service provider that supports the protocols to offer a service. These services will be supported by the RvT token.

The Cybersecurity controller

The process of verification is very simple and it is expected that this control will exist standalone and be built-into many services over-time as the ecosystem matures. The verification process will require an RvT token to operate.

The application provider

The Rivetz service is designed to be used by any application provider and the RvT token can be used to reward and promote security by any of the partners. The goal is to assure any partner can use RvT as part of the business model for their service if they choose. Cybersecurity needs to be built-in and there is a benefit to the business model integration as well.

First generation RvT use

It is expected as the business models mature and the technology matures the exact operation of the RvT token will mature as well. The ERC20 tokens sold in the sale will be used by their owners to supply and store RvT tokens in their device and protected by the TEE. The owner can at any time remove the tokens they put in the device or the tokens can be used by the device to obtain services that also meet the policies the owner has set. Value that is received for service will then be in RvT and the service provider can use them as they wish an or load them into their devices and request services of others. Everyone has a device that needs security services.

The use of promotional RvT tokens

Rivetz will set aside a portion of the RvT tokens to be used to incentivize the adoption of the system. The bootstrapping of the environment is a core component of the strategy and the long- term success of the system. It is expected that tokens may be used to:

- Support third-party developers and other third parties that support expansion and promote adoption of the ecosystem.
- Distribute to users to promote and incentivize use and adoption of the ecosystem by users.
- Distribute test tokens that will support expansion of the ecosystem.
- Support marketing and strategic partners who market and promote the tokens and the ecosystem.
- Reward service providers for early adoption of the ecosystem.

In the long term, it is expected the manufacturers and services will supplement this promotional supply with the tokens that are earned by their services. It is expected that these tokens will be used to incentivize participation in the system by users, services and manufacturers. The RVT token should incentivize partners to build services that provide advance capabilities and enhance the quality, security and utility of the network over time.

Detailed use cases

Two-factor Authentication with Cybercontrols

Rivetz has developed an operational two factor authentication (2FA) capability that supports the FIDO standards and is interchangeable with Google Authenticator. This app performs all the processing for the generation of a One-Time Passcode within the trust boundary of the TEE and if the platform supports it, TUI it is fully utilized. The following video link provides a simple demonstration. https://youtu.be/KyZqWjqZJFU

Upon completion of the Token Sale Rivetz proposes to integrate a health and attestation test into the 2FA capability. The intended result is that the TEE could verify the health and integrity of the device and its external controls assuring that the measured cybersecurity controls are in place prior to execution of the One-Time Passcode creation for the user.

The benefit

The system will assure that the controls specified by the owner are measured and are in reference condition on every use. This will simplify compliance with regulations that require certain controls to be active prior to connecting to sensitive services such as financial data or healthcare. For example, California Data protection laws require assurance that access credentials have not been lost and devices are encrypted. This would enable the owner to specify that the device can only generate a passcode after verifying that the device generating the code *was externally checked by the Cybercontrols Marketplace to pass the Google attestation test*. Other conditions could also be scripted into the system such as, “is the device on the local WIFI” or “is the user is still an employee”. The system will provide proof these checks where measured as the owner intended.

How does it work

Step 1 The device is provisioned with the Rivetz two factor authentication application and the RvT wallet.

Step 2 The owner determines what external controls will be verified by the device and configures those controls. For example: the validation of the Google SafetyNet service that will verify if the whole phone’s operating system meets googles attestation tests.

Step 3 The device is requested to record a reference health hash and the owner of the platform funds the wallet with RvT

Step 4 The user pairs the device to the 2FA enabled service

Step 5 The user connects to a remote service

Step6 A 2FA is requested

The device automatically creates a real-time health and integrity hash of the internals

The device automatically creates a real-time health and integrity hash of the external data from the Cybercontrols Marketplace

The hashes are combined with the reference heath hash locator and other data the owner wises to be collected and the message is sent for verification by the network.

The verifier uses the locator to retrieve the reference health hash and then compares the results returned to the Reference hash location for archiving and the result is returned securely to the device.

Step 7 If the result is positive, then the 2FA is allowed to continue within the TEE if the health reference is declined, then 2FA is terminated.

Machine Multisig with Integrated Cybersecurity Controls

The goal of this capability is a simple machine multisig for a device that any of the tokens that support multisig capabilities can use. The capability is currently estimated to be launched in the fall after a successful token sale. The assumption is that a normal app using a token can work as designed with no modifications but the configuration of a multisig. Rivetz has developed support for signing a token transaction within the Rivetz TEE and intends to add support for the Ethereum multisig protocol as well. The Rivetz app will validate the health and integrity of the device and then authorize the private key to be used to sign the multisig on the user- controlled device. This assures the device was in a measured condition when the transaction confirms. The owner of the device can set rules and limits around the TEE that will limit the exposure to the device robo-signing unintended transactions.

Benefit

Many services are being built to provide utility to the user and are being designed to be automatically activated. The level of automation and convenience is always a tradeoff with the level of security. The Rivetz solution provides a unique approach by holding a portion of the transaction within the device and leveraging a multisig protocol to assure it is part of the transaction. The intent is that the solution can be provisioned by the user and not the service if the service support native multisig capability. The result will be a forensic proof that this device in this condition was part of permissioning the transaction.

Step 1 the user configures a service to use a multisig wallet by funding the multi sig wallet and establishing the connection to the Rivetz Wallet as the second of 3 signatures. The third key is protected using standard methods for backup in case the device is lost.

Step 2 The user executes a transaction from their normal app

Step 3 the user requests the Rivetz app to cosign

The Rivetz app verifies a real-time health HASH

Request the Rivetz Cybersecurity Controller (Verifier) to provide a health test and Verifier logs the transaction

Verifies local Policies set by the owner are met

Permissions use of the private key to cosign the transaction The

transaction is submitted to the multisig process.

Appendix 1. Token sale model

Details of the token sale will be provided when the tokens are minted

Appendix 2 Trusted computing and attestation

Trusted Computing Concepts

Trusted Computing concepts emerged from Rainbow Series security standards and guidelines originally published by the US Department of Defense in the 1980s and then later by the National Computer Security Center. The primary standards better known as the Orange Book, the Trusted Computer System Evaluation Criteria (TCSEC) standard addresses requirements for assessing computer security controls in a computing system and was eventually replaced by Common Criteria international standards. Modern Trusted Computing is an approach to building computing systems that allow us to remotely make informed decisions about the level of trust to invest in their proper operation. From the Trusted Computing Group: An entity can be trusted if it always behaves in the expected manner for the intended purpose.

The computing security industry has found it extraordinarily difficult to secure commercial computing systems using software-only approaches – especially when the sources of software components are disparate and often independent entities. Recognizing the limitations of software-only approaches, standards organizations instead leverage and rely upon immutable hardware-based roots of trust as the foundation of trust in computing systems. By leveraging roots of trust in a platform, the primary goal of system architects is to provide computing environments with strongly isolated execution environments utilizing protected capabilities and confidentiality and integrity protected data storage facilities. These combined capabilities provide system architects with a trusted computing base that can be leveraged for confidence in the operation of a limited set of system functions.

While the Trusted Computing Group (TCG) has led the industry in defining specifications and standards for trusted computing requirements, APIs and systems and GlobalPlatform (GP) has led industry in defining specifications and standards for trusted execution environments requirements, APIs, and systems, trusted computing requirements are increasingly being included in other protocols and standards. The OASIS Key Management Interoperability Protocol (KMIP) and PKCS #11 include support for attestation as do numerous current IETF standards and drafts (e.g. Trusted Execution Environment Protocol – TEEP).

Roots of Trust

In order to provide the security capabilities required to instantiate a trusted computing base, a computing system requires a set of foundational security elements called Roots of Trust. The combination of Roots of Trust in a computing system is the foundation of assurance of trustworthiness. They are composed of hardware, firmware and software that together provide security-critical functions. Hardware-based roots of trust have advantages in consumer and commercial platforms since they are immutable, have smaller attack surfaces, and are generally more reliable; i.e. they can be relied upon to perform their functions with higher assurance.

In order to provide device integrity, isolated execution, and protected storage in a protected execution environment, a system should implement a Root of Trust for Storage, a Root of Trust for Measurement, and a Root of Trust for Verification. And in order the system to provide remote confidence in its configuration and status, a process called remote attestation, it needs to utilize a Root of Trust for Reporting in tandem with a secure and immutable device identity.

Root of Trust for Storage (RTS): provides a confidential and integrity-protected repository to store and manage cryptographic keys, critical security parameters and any configuration data, measurements and policies which are critically necessary to support the operation of a trusted computing base.

Root of Trust for Measurement (RTM): provides trusted measurement functions used to reliable measure the integrity of software components and configurations utilizing signature algorithms and is the root of the chain of transitive trust for subsequent software measurement agents. In order to minimize the possibility of subversion of measurements, a RTM should be invoked as soon after initialization of a computing system; the later a system invokes the RTM, the greater the opportunity to subvert the measurement trust chain.

Root of Trust for Verification (RTV): provides an engine to verify digital signatures associated with a software/firmware component and generates assertions of the verification result. The RTV executes a signature verification algorithm and compares signatures against reference expected values known as Reference Manifests.

Root of Trust for Reporting (RTR): provides a protected capability to generate and sign assertions for the purpose of remote attestation of a computing system's assurance properties. The RTR must leverage a strong device identity to protect against system impersonation and nonrepudiation. The RTR heavily leverages the capabilities provided by the RTM, RTS, and RTV.

Secure Boot and Transitive Trust Chain

Secure boot is the process of measuring the integrity of platform components by leveraging a RTM and verifying measurements against authorized reference measurements to enforce system policies for the purpose of booting a trusted computing base. By interleaving measurement operations with verification operations, a boot process can self-validate according to security policies in effect on the computing system. This process combines trusted boot (capture of measurements) with local verification of measurements to secure the boot process of the system. If a component is out of security policy compliance at any time during the measure / verify process, the system may choose to boot a valid remediation image or other "safe" alternate boot path with the intent of preventing out-of-compliance machines from ever executing malware or unapproved code and presenting compromised services.

The measure / verify process allows the computing system to successively load more measurement and verification agents during the initialization process of a computing platform. The coherent set of measurements and assertions during this process whereby all components are evaluated prior to execution is called the transitive trust chain. When implementing secure boot, these measurements may be discarded immediately after use by the local system. However, if the system needs to convince a remote relying party of its integrity and configuration, it is crucial to protect the transitive trust chain measurements and assertions against unauthorized modification or augmentation until they are reported to the relying party by leveraging the RTR in a process called remote attestation.

Remote Attestation

While it is possible to secure many kinds of processes, with a limited set of resources it is never possible to secure a process with 100% certainty and this is especially true in commercial and consumer platforms that have significantly fewer resources afforded to them than military systems. Thus, a basic tenet in system assurance evaluation is to "Trust but Verify." No matter how well a system is secured, having visibility into how a system evolves due to system updates and potential authorized and unauthorized changes and additions provides a relying party with a mechanism to evaluate the current status of a computing system. As an example, though NIST provided a specification to secure the BIOS of a computing system (NIST SP 800-147), NIST immediately followed up with a specification to report on the current measurement and status of the BIOS (NIST SP 800-155).

The process of remotely verifying the measurements and configuration status of a computing system, and providing a mechanism to evaluate its expected behavior, is called attestation. This process is crucial for providing confidence in the integrity of a system and allowing a relying party to decide to trust a computing system is the basis for trusted computing.

Attestations are reports of system integrity provided in a manner that allows the remote relying party to evaluate a transitive trust chain and to determine the platform's trusted computing base is in a state that is acceptable for the relying party to have confidence the system will operate as expected. Inherent in an attestation is the expectation that a specific system is currently in the state reported, thus combining the identification of a specific device with a mechanism to ensure that an attestation report is fresh and not a replay of a previous report is crucial. In an effective attestation protocol, the remote verifier provides a freshness nonce for the device to include within an integrity report that includes a signature over the attestation to verify the identity of the system and the integrity of the attestation data.

Trusted Execution Environment (TEE)

System architects have included roots of trust and trusted computing capabilities into a large number of products currently deployed in industry. In the personal computer, the Trusted Platform Module (TPM) has been leveraged to provide secure cryptographic key storage and use. This protects secret and private keys from observation and disclosure attacks to which they are susceptible when in shared system memory. PCs that leverage the TPM can load a trusted computing base known as a secure kernel to vastly improve the information assurance properties of the system and provide remote attestation capabilities.

Instead of relying upon a TPM, smartphones and IoT devices utilize the hardware isolation and security capabilities embedded and inherent in modern microprocessors to offer an isolated execution and storage environment. Examples of this capability are ARM processors which include TrustZone and Intel processors with Software Guard Extensions (SGX); similar capabilities have and are being included in processing environments from large server platforms to tiny IoT devices embedded in systems that require secured operations and remote visibility.

By leveraging TrustZone and SGX low-level capabilities as roots of trust, information security standards organizations such as GlobalPlatform have published numerous standards for a Trusted Execution Environment (TEE) which acts as a trusted computing base and an isolated environment to execute small trusted applications. Smartphones and IoT devices implement secure boot utilizing roots of trust (RTM, RTS, and RTV) to instantiate a TEE that protects the execution of Trusted Applications (stored and executing in TEE) from observation and alteration from the device operating system, services, and applications. The secure boot process allows the local system to have confidence and trust that it is operating in an approved configuration and supplies authorized services to the rest of the software components of the computing system.

However, just as we might trust other computing systems instantiated using a secure boot process, we also need to verify continued compliance, operation, and updates to establish remote trust in those platforms. These systems can also leverage the RTM, RTS, RTV, and RTS (the roots of trust of the system) to implement remote attestation with remote parties who must rely upon the correct operation of the platform. The integrity information provided in remote attestation reports needs to provide coherent measurements and configuration information to allow a remote verifier to have confidence (trust) that the TEE environment itself was instantiated utilizing the hardware security capabilities inherent in the system and using authenticated and authorized components. Similarly, once instantiated, a TEE needs to be able to attest to its internal configuration and to the integrity and current status of trusted applications executing within the TEE.

The coherent combination of measurements of the initialization of a computing system, the instantiation of a trusted execution environment, and the current state of trusted applications executing within a trusted execution environment is the transitive trust chain of integrity measurements of the trusted computing base of the computing system. Attestation provides the mechanism to report the state of the device to a remote relying party with confidence.

Appendix 3 Blockchain a general description

A blockchain is a distributed database consisting of a list of records. Each record has a secure timestamp and a cryptographic link to the previous record. The records are called *blocks*, and the cryptographic links make it easy to read the database and to verify its accuracy, but make it extremely difficult for an attacker to alter or change the order of records. Because of these properties, a blockchain is a machine-readable unalterable historical record, which makes it especially suitable for security applications.

The best known blockchain is the Bitcoin blockchain. Bitcoin uses the immutable historical record to record irreversible monetary transactions. Another well-known blockchain is the Ethereum blockchain. Ethereum uses the blockchain to store smart contracts as well as the data those smart contracts need to operate.

The existence of an unalterable historical record is essential to the functioning of the RvT token. When a device is manufactured, its birth certificate is stored on a blockchain. The birth certificate associates to that physical device a health quote, which may include information such as a hash of firmware. If a device is compromised, its real-time health quote will change. An adversary who wishes to hide the compromise will have to rewrite *the entire history of all transactions on the blockchain* back to the time of manufacture of the device, which virtually impossible. Moreover, if the device is configured to write a health quote to the blockchain regularly, then the blockchain will not only record *that* the device is compromised but also *when* it was compromised.

The RvT token is flexible and can store many other types of information in the historical record. For example, a shipping company might use RvT in combination with beacons to prove that a piece of cargo was always refrigerated, or always in proper custody.

The idea of blockchains goes back at least to the early 1990s, but the first major practical application was Bitcoin, starting in 2009. The mathematics are relatively straightforward. The core idea is that of a linked list where each record or block points to the block that precedes it immediately in time. A "pointer" here is a cryptographic hash rather than a memory location. A version of this idea is familiar to many developers as the basic structure in the source control system Git. Given the blockchain in its entirety, anyone can verify the integrity of the blockchain by iterating over it and computing hashes of all the blocks.

The hard part of blockchains is not the structure itself, but rather deciding who gets to write to the blockchain and how to secure the timestamp. This was the problem first solved in Bitcoin, which uses economic incentives to control writing to the blockchain. Other chains, namely *permissioned chains*, solve the problem by specifying certain entities or agents who have exclusive authority to write to the chain. Several other solutions also exist.

Appendix 4 About Rivetz

Rivetz Corporation

Rivetz Corporation ("Rivetz" or the "Company"), the parent company of Rivetz Intl., is a "First-mover" with patent pending cyber security services and capabilities that seeks to leverage the Trusted Execution Environment ("TEE") already available on hundreds of millions of existing devices. By providing a vault to isolate and protect keys and encrypted material from apps, malware, users, and hackers, Rivetz seeks to ensure a truly safe experience for accessing all digital services, thus maximizing the quality and value of the provider-to-subscriber relationship

Rivetz is at the forefront of this dramatic shift from users employing dozens of user names and passwords to a device-based identity and capabilities model for connecting the online subscriber, which will increase the value, trustworthiness and quality of the subscriber to the service provider by recovering the lost value stolen by fraud, while at the same time eliminating the complex and frustrating user experience created by software-based security measures. Rivetz's proprietary technology leverages the Trusted Execution Environment capabilities built into devices to hide and process secrets in complete isolation from the risks inherent in the operating system. Rivetz's TEE-based products and services, leverage built-in hardware capabilities currently embedded on 2 billion devices. Almost all smartphones, tablets, laptops, and personal computers already contain the necessary hardware to enable a Rivetz vault for securing user access, privacy and safety. The Company's technology replaces unsecured storage of credentials and the cumbersome annoyance of multi-factor authentication with a safe space to hold and process sensitive data and secrets, assuring that only a known device in a known condition with a known user can connect to a network or service. Rivetz's simple and flexible platform brings world class security into the reach of any application developer or service provider by allowing them to quickly and cost-effectively exploit the built-in security protections contained on the latest generation of hardware.

Every enterprise and service provider can benefit from a stronger connection to the customer, which Rivetz facilitates by delivering a new model for access and data protection. The Rivetz platform of services and tools seeks to enable individual users to leverage next generation security services as part of a multi-factor solution. The Company also empowers entities to build great security directly into their apps with simple to integrate capabilities. Market demand for multi-factor authentication grows every quarter and Rivetz is executing on a novel tactical approach to supply the market with state of the art security technology. The Company supplements the built-in authentication everyone needs with patent pending integration of an enterprise's legacy cybersecurity controls, along with the services to help the user manage their collection of devices as their identity.

Rivetz's platform services seek to provide a unique set of market leading solutions that have already helped the Company generate over a million dollars in recent contract awards from the Department of Defense and the Department of Homeland Security. The Company plans to now rapidly commercialize its products and services on a large scale, and establish itself as the leading solutions provider for trusted cyber security designed around the TEE. Rivetz expects that its services and solutions can easily be leveraged by application development partners and service provides to enhance the value of subscribers on their systems. The Company has a strategic relationship with Trustonic, giving it access over a billion devices already in the field. Rivetz has also initiated discussions with major, established technology companies to support their solutions and add another billion devices that can utilize the Company's capabilities.

Rivetz's patent pending attestation service seeks to deliver a market changing security model that integrates legacy enterprise network security tools with the cloud access model of computing by leveraging the trusted device, thus providing a new cyber security control that forensically proves a known device in a known condition with a known user created or consumed sensitive content. The Trusted Agent in the device reliably verifies legacy controls prior to allowing access to critical keys and credentials, delivering proof of those controls to the cloud for real-time verification as part of any transaction. This model for distributed cyber security controls seeks to deliver a critical capability to assure the security of transactions from the enterprise to the Internet of Things ("IoT") to the Blockchain.

Rivetz also empowers the user's collection of devices to become their identity rather than just a single device. This attempt to assure the user's online identity is not just a single smart phone, but instead represented by their collection of devices, allowing the user to access their cloud services from any of their known devices. Rivetz helps the user manage their collection of devices and the services they subscribe to and ensures that access can only be achieved from any of their known devices when in a known condition with a known user.

Rivetz believes in the need to integrate cyber controls on a distributed basis and the tremendous value of connecting the user's collection of devices. The Company's tactical strategy will build a foundational relationship with the household or small businesses through their collection of devices by providing the ultimate secure connection to the services they use. Rivetz's anticipates its vision for a modern network will emerge conceptually as a social network of devices and services that will ultimately replace the old model of the local area network ("LAN"), along with the firewalls, network security tools and passwords that come with it.

Importantly, Rivetz's innovative business model contains technology to measure usage of the Company's Trusted Agent within a client device, assuring that service providers who deploy the Rivetz capabilities pay for using them. The embedded microtransaction/metering model attempts to provide the flexibility to meet the requirements of application developers and service providers. The Company's unique, state of the art model brings a cloud based approach to cyber security services that is consistent with enterprise, organization, government agency, and user demands, and the new Presidential cyber security directive.

Rivetz has invested over 3 years in executing a well thought out and novel strategy to create the market and capitalize on this substantial opportunity. The Company's revenue producing contracts with the Department of Defense and the Department of Homeland Security validate and demonstrate the market value and leading-edge capabilities of Rivetz's technology. By simplifying the user experience and assuring that information is delivered as intended, Rivetz has designed a solution that seeks to unlock new models and services and provide value to users for years to come. Rivetz has the short term tactical plan to quickly engage customers to drive revenue and the long-term vision to unlock the full potential of the market.