The Requirement of Non-Repudiation

By Tony C. Rossi, Esq. Chief Legal Officer – BlockFrame, Inc.
Edited by Christopher Gorog, MBA, PMP, CISSP – BlockFrame Inc.

Introduction

Is your business required to have non-repudiation? What is non-repudiation? Many boards, commission, regulatory bodies, and institutes either require non-repudiation or suggest its use for best practices. This paper explains non-repudiation and suggests solutions to meet regulations for non-repudiation in most industries.

How Non-Repudiation is Defined

The Federal Energy Regulatory Commission (FERC) and the National Institute of Standards and Technology (NIST) define non-repudiation as assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.[1] The North American Electric Reliability Corporation (NERC) also uses NIST's definition of non-repudiation.

Other requirements in the same regulation also identify what is referred to as *technical* non-repudiation. The North American Energy Standards Board (NAESB) Wholesale Electric Quadrant (WEQ) defines technical non-repudiation as when a party cannot deny having engaged in the transaction or having sent the electronic message. NIST defines technical non-repudiation as the contribution [of] public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.

On the statutory side, Federal Statute 44 U.S.C. 3542 defines integrity as applied to National Security Systems to mean the guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

The Requirement of Non-Repudiation

FERC does refer to nonrepudiation as a requirement in its publications[1] as well as the North American Electric Reliability Corporation (NERC).[2] FERC's own employees have a policy, Rules of Behavior for IT users that requires the "protecting information by ensuring the availability, integrity, authentication, confidentiality, and *non-repudiation* of the data." Likewise the NAESB has non-repudiation as a standard.[3]

---

[1] Federal Energy Regulatory Commission – Electronic Filing Strategic Plan and Information Technology Architecture – August 4, 2000 Prepared by Signal Corporation and PEC Solutions, Inc. https://csrc.nist.gov/Glossary/?term=289#AlphaIndexDiv

[2] NERC Publication – Guidance for Secure Interactive Remote Access – July 2011.

[3] 012-1.1 OVERVIEW (RFC 3647 Section 1.1)

Many distributed devices which are connected to networks to perform sensory type or limited use cases which have become commonly referred to as Internet of Things (IoT) have an especially high requirement for distributed trust. Distributed trust is increasingly important to IOT devices that convert electrical commands which then in turn perform mechanical operations or retrieve parameters from sensors tied to physical world entities. The application of distributed trust requires non-repudiation to verify communications and thus can be seen as the same thing.

Any industrial or IOT application requiring trusted communications or non-repudiation by regulation will require each device to be able to provide a proof of origin on any and all data in order to trust the data exchange to a level required to safely operate electrical-mechanical devices. The ability to positively identify origin of data during transmission provides the assurance of non-reputation for each communicating device. This enables strong distributed trust applications such as trans-active renewable energy grids where the distributed devices are out of the control of utility networks.

Why Non-Repudiation Solutions Are Essential Today's Internet

Over the last two decades the cyber security industry has moved in a direction which is not sustainable. As the world has moved from the networking of a few devices to the vast expansion of a worldwide internet, we only find that as people become more educated on technology, the problems with the deviant behavior of people that existed in the physical world transfers directly to the internet.

We have also found that a new paradigm exists in the virtual world. Traditional boarders, boundaries, and physical limitations of interaction between people does not carry over to the internet. The virtual world has no concept of distance and is borderless. However, our designs and thought process for security in this virtual cyber space are based on our existing knowledge of the real physical world. Like our change into the virtual world of the internet, our thought process around protecting and enforcing virtual space (Cyber Security) must adapt to this new paradigm as well.

The internet, unfortunately, was not developed initially with security in mind. Widely used communication protocols do not first check conditions or proof of origin on the communicating parties before allowing electronic point-to-point connection. All communications are permissible and it is the responsibility of each party to monitor any and all communications at their own expense and/or accept the resulting risk should they not. The cyber security world has painted itself into a corner where the most widely used cyber security operations result in monitoring and collecting nearly all communications, storing all data, and analyzing these ever growing data sets from every source organizations interfaces with.

Data sets and communications are growing exponentially and the tools and/or human operators only have the ability to examine the collected traffic/data in a linear growth capability at best. Thus our attack surface grows at this same exponential rate as data, but our defense capability follows the linear ability for human absorption. Even to maintain the linear growth requires a continuous diligence of adding more tools, servers, and human resources on a continuous scale.

Needless to say, this trend is not sustainable on an indefinite basis, and many organizations have already reached a plateau in their ability to maintain this trend.

Current Attempts at Non-Repudiation

Non-repudiation requires identification and assurance a transaction took place. Current attempts at identification are strictly implemented in software, utilize centralized servers, or combinations of both. Parties with malicious intent can spoof software-only identification methods and make exact copies of entire software platforms which become undiscernible clones in our post virtual-machine technology era. Centralized databases maintaining our trusted and confidential data are in the news daily with new compromises with a continuously increasing trend. The storage of data that tracks whether or not a transaction took place are maintained in these target systems where we have limited capability to positively identify that the applications, data, or entire systems have not been compromised.

Transactions and the responsible parties' actions are currently only traceable within the scope of a single organization and trustworthy only to the extent which the organization overall can be trusted. Visibility of the transaction and privacy of private records are entirely at the mercy of the organization which contains the records. The trust which people instinctively know how to establish in the physical world does not transfer to online environment with nearly infinite data sets which are exponentially growing. In all aspects the technological advancements have left humans basically blind and crippled in their ability to verify actions and identity of remote actors online. The design for Cyber-security and accountability of actions needs to be re-created from the ground up to include methods of non-repudiation.

How Non-Repudiation is Achieved

What is required is a process for providing an underlying trust on each computer system. This can be accomplished using Blockchain technology which has been famously and successfully used as the engine behind Bitcoin. BlockFrame's solution uses a hybrid BlockChain application in conjunction with a chain of trust hierarchy to create a strong synergy. The application employs BlockChains' immutable identification capability to identify any device by unifying the provisioning of underlying cryptographic keys used for communications.

A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. When these keys remain private to the containing entity we can have a much higher certainty of secure communication. The unified-communications-keying-approach offered by our solution establishes an underlying base security architecture which may then connect to any security product or application and provide whitelisting capability to all enabled devices. Whitelisting limits participants to those who have been verified. The overall operation of the internet today can be better related to the opposite, which is referred to as Blacklisting. Blacklisting is where anyone can participate in data transactions without verification and it is the responsibility of each party to independently identify any malicious activity or parties and add them to each parties own restricted list.

Once each device contains this capability, it is able to uniquely self-identify the trusted state of the system at the onset of communication which is the first step in achieving non-repudiation. An ecosystem of self-identifying devices removes the ability of outside devices to impersonate or spoof communications as they cannot produce trusted communications without being a part of the ecosystem.

The technology outlined enables for the first time an industry wide approach to identity assurance of any Internet of Things (IOT) devices. This solution provides a Cryptographic Trust Center (CTC) in the form of a simple integrated circuit chip which is placed within each eco-system enabled IOT device.

A cloud support service utilizing proven BlockChain operations then offers Trust as a Service (TaaS) functionality enabling the provisioning of trusted components in each device. The process for provision is designed to ensure that no human has access to the provisioned components and thus cannot be circumvented without global awareness to any instance which would equate to a violation of privacy. This provides assurance the sender of data is provided with proof of delivery, data contains proof of originating device, and the recipient is provided with proof of the sender's identity.

The overall operation will enable an eco-system to coordinate and set the base underlying security components on each IOT device while providing non-repudiation for all actors participating in each data exchange.

BlockFrame is prepared to advise on these solutions if non-repudiation is either desired or required in your business.