KnectIQ

WHITE PAPER

5G: The Promise, The Problems, And the KnectIQ Solution.

KnectIQ Inc.
T: +1.651.447.4264

E: secure@knectiq.com
www.**KnectIQ**.com

1915 Highway 36 West
Roseville, MN 55113 USA

5 Rue de Bonnevoie
L-1260 Luxembourg

Objective/Problem Statement

The global deployment of 5G technology is touted as a “game-changer” in wireless communication, reliability, connectivity, and data utility. This technology is viewed as the next step in the drive towards a data-centric future, lifestyle, and economy. Never has data access and the benefits to society of fully operationalizing it advanced so quickly.

Despite all its promise, this technology breakthrough comes with increased risk to data security, in both foreign-developed and sourced hardware components, and in the methods by which this free-flowing data is secured. As this hardware is deployed across the world, innovative and powerful new approaches to securing access to highly sensitive data must be employed. Current cyber security industry standards are inadequate to protect secrets traversing this burgeoning network, and the ability to simply route data flows around suspect hardware is an impractical approach.

Government, and especially intelligence agencies must realize that while this technological leap forward presents increased data security risk, it also presents advantage and opportunity for those that can effectively employ a new security paradigm. The first parties to deploy new security tools in response to the challenge of 5G data security will gain unparalleled agility and capability in expanding information collection, secure transmission, and dissemination on a global scale, while leaving adversarial information at risk. Properly applied, this security dominance can enable U.S. advanced-data-superiority at the cutting technology edge across the government and commercial sectors.

The Problem

Information Warfare and the cyber arena are the most challenging and important theater of global military and intelligence competition, both today and into the future. With the advent of 5G networks and the enhanced data rates it provides this competition becomes more intense, and the playing field is not level.

Current internet protocols for securing data-in-transit are ineffective. Adversaries are stealing the private keys that enable interception and decryption of sensitive messages. In this system private keys reside in known, centralized locations and are used across many systems. These private keys serve as single-points-of-failures to the mission of the end-to-end encrypted data transfer system. If compromised the secure data can be read or manipulated in transit with no alert given to either sender or receiver. The attack surface is broad with hundreds of keys and certificates possible on any endpoint. Even effective rotation does not remove the threat of having persistent keys that can be easily stolen and compromised. Furthermore, master keys (allowing unrestrained access to the possessor) for this system can often reside in countries with competing political agendas (e.g., China, Hong Kong, Turkey, etc.). Unfriendly regimes can compel companies to turn over copies of these keys and certificates, and the inspection and potential manipulation of these data flows is untraceable in the current architecture. With the looming threat of Quantum Computing, even careful management of trusted certificates will not help. Current methods of reducing these threats are to double down on the flawed architectural components that allow these vulnerabilities to exist. Simply put, data-in-flight today is not secure.

5G Hardware: An Enhanced Threat to Data

The proliferation of 5G hardware components coming from some of these adversarial regimes has brought increased concern about the security of routing internet data across these networks. But the threat is not hardware based, as many of the headlines suggest. Backdoors have always existed, and attackers can today harvest data crossing the Internet, regardless of the country of origin of the routers at each "hop". But if that data is properly encrypted, it does not matter. It would take trillions of years for adversaries to decrypt those payloads without the proper key. That is if we lived in a world where the key could not be obtained. We do not live in that world. The true problem is that the end-to-end security protocols in place require every sender, receiver, and certificate holder to effectively protect their secrets and trust chains. Any wrong step and it is game over.

In short, security is only possible when all threats are effectively addressed, and perfectly securing any 5G or other network (i.e., network centric security) is becoming more widely recognized as a fool's errand. The innovation in the space is in building better systems (data-centric security models) to defend against the inevitable breaches to your network's perimeter. In that realm new questions are being asked and new solutions are being forwarded that turn existing architecture on its head.

Secure Communication in a Hostile Environment and Zero Trust

Zero Trust advocates, from DISA, the Navy and other organizations are advocating Zero Trust precisely because perfectly securing the network is untenable. In other words, whether in the office or on a remote 5G connection, assume that the network is hostile. This Zero Trust mindset has great potential:

- From a defensive perspective, breaches at an organization are more easily contained as access even within the organization is also restricted.
- From an offensive perspective, an organization can put its private data to use anywhere, including the office, at home and even over these 5G networks.

But we have not yet implemented Zero Trust in the classified domain, in part because while the promise is great, existing Zero Trust solutions do not adequately protect data transmissions.

A New Paradigm is Required

The problem with existing Zero Trust solutions is that they too rely on existing internet security protocols to protect the data in flight. While it is helpful that they approve only authorized parties to access confidential data, unless the delivery of that data to the authorized parties is secured in a manner that defeats the myriad threat surfaces outlined above, it is not effective. Specifically, while Zero Trust solutions have replaced the network centric security model with an identity centric approach, the underlying security protocols they employ are 30 years old and not up to the task.

In short, it is time that we recognized:

1. Existing security protocols are vulnerable to our adversaries.
2. It is impossible to protect every network that we want to operate on.
3. A data centric or Zero Trust model provides a framework for working around the impossibility of protecting every network.
4. Improved cryptographic protocols coupled with a Zero Trust framework would lead to better defense and enhanced ability to operate across all networks.

The Solution

KnectIQ provides the data security, operational agility, and real-time information advantage necessary to dominate across the digital domain.

Identity Centric Cryptography

It is no surprise that that a 30-year-old protocol has outlived its utility. But it is worth a moment to understand why this is the case. Existing encryption protocols were developed in the 1990s, when the population of the internet was doubling every year -- when many received CDs from AOL almost weekly to welcome them online. In such an environment, developing a security system that allowed unidentified parties to securely connect to an identified service made sense. In short, these protocols were effective solutions for the problems of the time, but times have changed.

Today the internet is a vastly different place -- a place where our most sensitive information is shared between parties who already know each other. So why not use this knowledge, or identity, to build better security?

KnectIQ Solution

KnectIQ's system uses the identity of the communicating parties to establish better security. This technology creates trust-environments that identify all endpoints in a network, allowing communications only between identified devices. Consider the contrast with today's key based approach:

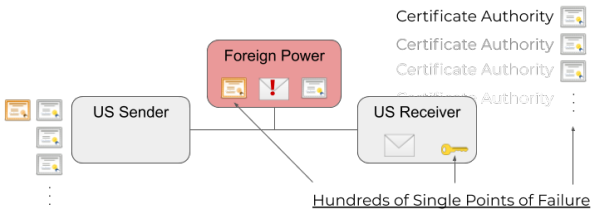
KEY BASED

Security first
Then identity

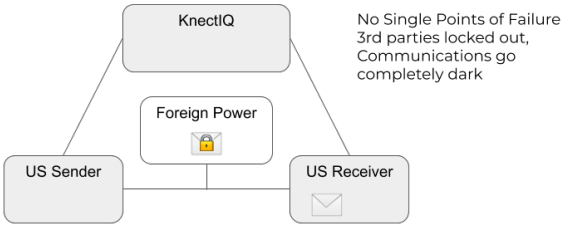
IDENTITY BASED

Identity first
Then security

Legacy Security



Next Generation



By using a dynamically managed identity instead of stored keys, no keys need to be stored and protected. Then, when communications occur, single use keys are created at the sending device to encrypt the payload and are then erased. Upon receipt of the encrypted message, the decryption key is created and exists just long enough for the assigned task and is then erased. Each communication between endpoints occurs with a unique key creation/destruction cycle, and there are no persistent keys or certificates that can be attacked, stolen, or exploited. KnectIQ's system results in smaller attack surfaces, quantum-proof security, auditable data delivery, and lowered costs of operation.

A system that creates and destroys keys on a per-transaction basis accrues many advantages.

- Secure: Not storing keys removes the large, associated threat surface.
- Sovereign: Not vulnerable to foreign interference.
- Privacy Friendly: No back doors that weaken security.
- Law Enforcement Friendly: Capable of enabling warrant compliant encryption.
- Verifiable: Every secure transaction is logged and hence proves the security.

KnectIQ Inc.
T: +1.651.447.4264
E: secure@knectiq.com
www.KnectIQ.com
1915 Highway 36 West
Roseville, MN 55113 USA
5 Rue de Bonnevoie
L-1260 Luxembourg

KnectIQ Architecture

KnectIQ securely manages the identity of every endpoint - centrally. It accomplishes this through the creation, management and use of a Trust Environment. Simply put, a Trust Environment is a set of endpoints that are allowed to communicate securely with each other. Communication can occur when a sender and a receiver are both provisioned within the trust environment and then bound together, enabling communication. The Trust Environment is broken into two parts: Broker and Device.

Broker

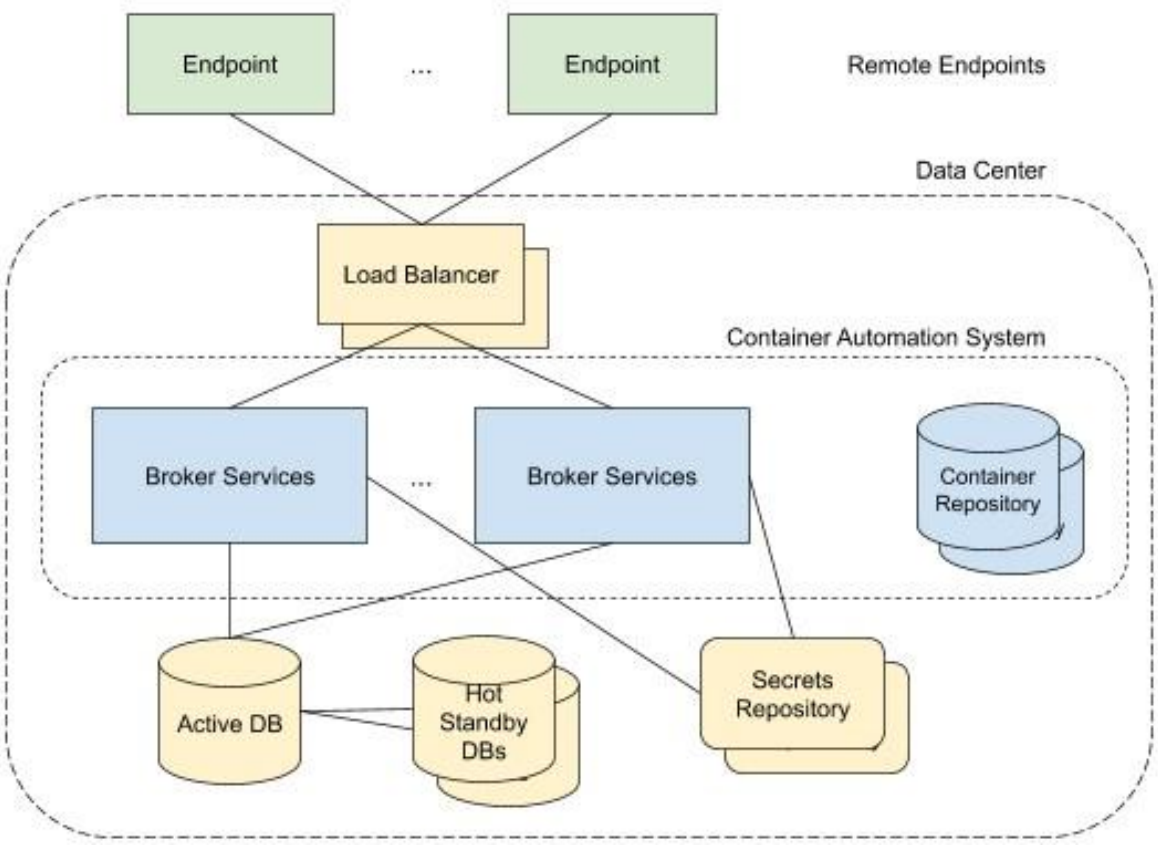
The broker manages the Trust Environment. Deployed on premises or in a private or government cloud, the broker enables configuration and operation of the Trust Environment. It does this by enabling the following operations:

Provisioning: Endpoints can be added or removed from a Trust Environment.

Binding: Endpoints can be bound so that they can communicate with each other.

Operating: Once provisioned and bound, endpoints can communicate with the endpoints with which they are bound.

Although only a single Broker is shown in the system diagram below, it is built for redundancy and scalability, with many processes handling the load.



KnectIQ Inc.
T: +1.651.447.4264

E: secure@knectiq.com
www.**KnectIQ**.com

1915 Highway 36 West
Roseville, MN 55113 USA

5 Rue de Bonnevoie
L-1260 Luxembourg

Key Design Points

- All components can be deployed with redundancy.
- While this drawing shows an Enterprise level deployment, the system can be scaled down to run on small devices.
- Although only one Active DB is shown, this can be scaled horizontally for large applications as well as down for smaller.
- The details of the services are not shown. Instead, Broker Services represent the various services responsible for delivering the configuration and operational functionality.
- No component of the system is tied to a specific operating or container automation system, but the broker is usually delivered as a containerized solution, for example in Kubernetes.

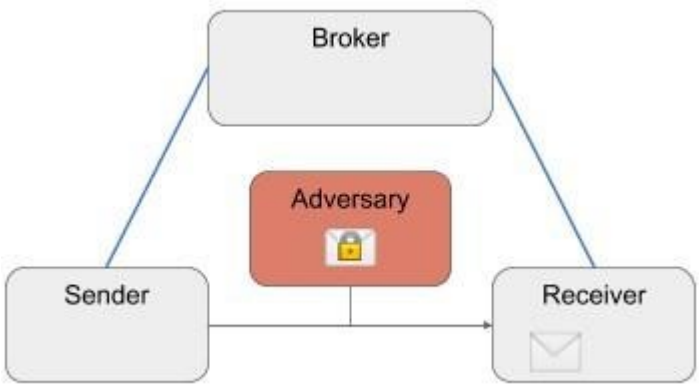
Device

Devices are the endpoints in a Trust Environment. They can be physical or software devices. As a software device, they can be integrated into any application or system that is on the network with the Broker.

Once provisioned and bound to other Devices, they can communicate with (and only with) the devices with which they are bound.

System Operation

Putting it all together, secure communication between sending and receiving devices can be diagrammed as follows:



- Every communication has a new key - only at the moment it's needed, but not before or after.
- Communication is secure and auditable.
- Attempted breaches are flagged.
- No expensive, slow, human-reliant key management systems
- Allows increased speed-of-data delivery with easily configured provisioning of endpoints in any network.

Note that the data communication path remains unchanged. Communication continues to flow over existing networks, but with new security.

METHODOLOGY

Implementing this solution can be broken into the following steps:

1. **Identify Communication Networks:** During this phase, the communication networks to be protected are identified. These may be existing networks in need of better security or new networks that have required better security before deploying. This phase may identify multiple independent or interconnected networks. Depending on this discovery the remaining steps may be carried out independently, in concert, or sequentially for the identified communication networks.

2. **Identify Management:** Parties responsible for identifying and allowing access to communication and data are identified. This enables better provisioning of endpoints later. If desired, the people responsible for responding to threat alerts and notifications are also identified.

3. **Identify Endpoints**: The hardware or devices and software that are sending and receiving data are identified.

4. **Software Integration Plan:** Having identified the communication, management, and endpoints, a plan is created to enable the deployment to every type of node. This plan will include:

    a. Planning software modification or additions

    b. Identifying where the Broker will be hosted and managed while ensuring availability as required by the application.

    c. Identifying how endpoints are provisioned into the Trust Environment and creating necessary identification for provisioning.

    d. Creating an alert management plan

        I. Threat Detection: Who receives any alerts for threat detection.

        II. Review: Who is responsible for reviewing security logs

        III. Automated Threat Response: Define automated response when threats are detected.

        IV. Proof of Concept: A version of the system is implemented and tested to verify the design and architectural decisions. The logs of system communication are reviewed, and penetration tests and other evaluations are run. Any needed changes or iterations of the initial plan are handled in this phase.

5. Limited Rate Initial Production (LRIP) and Multi-System, All Domain Full Rate Production (FRP).

SOLUTIONS APPLICATIONS

The system provides cutting edge data security solutions across the breadth of military, intelligence and government network and information sharing requirements. Enhanced security and information agility can be delivered in numerous critical components of the digital competition space. The rise of 5G provides another data transmission plane by which data transmission operations can be achieved, increasing network opportunity and flexibility options. Numerous critical data transmission functions could be achieved without the need to establish costly, stand-alone transmission paths if properly and effectively secured.

Network Security:

Secure data in flight across the entirety of military, intelligence, and government computer systems, regardless of classification level. Enable controlled information and collaboration engagements on existing networks or commercial infrastructure.

Command, Control, Communication, Computing, Intelligence, Surveillance, Reconnaissance, and Targeting (C4ISR&T):

Ultra secure data and communication transmission and sharing across a wider collection and distribution spectrum in real time.

Advanced Data Collaboration and Distribution Systems:

Increase the incoming information stream and outbound delivery endpoint security for increased operational collaboration and coordination when used in advanced battle management and collaboration systems. Tailorable in real time to information security level/endpoint receiver.

Critical Infrastructure Protection:

Energy command and control system security, early warning system data security.

Unmanned System Command, Control, and Data Management:

Ultra secure command and control of unmanned systems in any domain, thwarting attempts of seized control or counter commands by adversaries. Secure transmission of video/data collection products from collection source to endpoint.

Satellite/Space Network Communication Security:

Secure data transmission and distribution across all pathways and data types throughout the satellite constellation. Provides a non-hardware intensive, updatable security capability throughout a rapidly configurable, interconnected constellation system for enhanced reliability and flexibility of communication and data transmission needs, secure from network data intercept/decryption, corruption, and pathway disruption risks not associated with physical satellite attack.

Quantum Proof Cryptography:

This system has no public keys and no attack surface for quantum computing.

KnectIQ Inc.
T: +1.651.447.4264
E: secure@knectiq.com
www.**KnectIQ**.com
1915 Highway 36 West
Roseville, MN 55113 USA
5 Rue de Bonnevoie
L-1260 Luxembourg

SOLUTIONS SUMMARY

Data is most vulnerable when it is in flight. Existing solutions for securing data in flight have fundamental flaws:

Security: Existing systems are kept secure by carefully guarding the keys. But adversaries know where the keys are, and these keys represent a Single Point of Failure in the security of the protected data.

Verifiability: Existing solutions are designed such that the security of data cannot be verified. Instead agencies must trust or hope that their key protection efforts have been effective when they know that counter examples exist.

Fragility: With existing solutions, a breached key enables data breaches that cannot be detected until the next key rotation. But existing systems to rotate keys are slow, cumbersome and themselves prone to breach, so the present reality is that breaches are persistent.

Inflexibility: Because existing systems are so vulnerable to key breaches, classified data is restricted to well protected endpoints. This limits agency's ability to put that data to use as they would rather not use it than lose it.

The KnectIQ solution addresses the weaknesses of legacy systems by providing a system with the following capabilities:

Security: Because every communication has its own key, it is not vulnerable. The threat surface associated with static keys has been completely removed.

Verifiability: Every communication generates audit logs that enable the system to monitor exactly where each communication was encrypted and decrypted. Every endpoint in the system is also tracked ensuring the identity of the sender and receiver for every communication.

Threat Isolation: Attempts to steal a key are blocked and flagged. Even a compromised endpoint would only be able to leak key material for a single message.

Automated Threat Detection: Any attempt to breach this system leaves a trace that is automatically flagged, allowing the system to defeat the attempt and investigate the causes.

Flexibility: Because the attack surface associated with static keys has been removed, this system enables agencies to provision secure endpoints outside the traditional network centric model. Thereby allowing the secure use of classified data in situations where it was previously not possible.

Scalability: This system can run in small environments or secure vast amounts of data across millions of endpoints.

High Availability: Every component of the system can be deployed with redundancy and resiliency, enabling carrier class reliability.

KnectIQ Inc.
T: +1.651.447.4264
E: secure@knectiq.com
www.KnectIQ.com
1915 Highway 36 West
Roseville, MN 55113 USA
5 Rue de Bonnevoie
L-1260 Luxembourg

Quantum Proof Cryptography: This system has no public keys and no attack surface for quantum computing.

Intellectual Property Details

KnectIQ's process is both patented and patent pending.

Patent Granted

Patent Date: 11 June 2019

US Patent No. 10,320,785

METHOD OF PROTECTING THE IDENTIFYING INFORMATION OF PERSONS AND COMPUTING DEVICES, SPECIFICALLY THOSE DEVICES WHICH ARE CAPABLE OF SENSING, CAPTURING, RECEIVING, TRANSMITTING, PROCESSING, AND STORING DIGITAL INFORMATION

Patent Pending

File Date: 28 Jan 2019

Application # 62/797,439

SYSTEM AND METHOD FOR SECURE ELECTRONIC DATA TRANSFER