Case Study

# True Zero Trust Data Exchange at Scale

HEALTH SCIENCES SOUTH CAROLINA

A Collaborative To Advance Health Sciences

## How South Carolina's HIE Used KERI for Scalable, Zero-Trust Data Exchange

# Executive Summary

This case study, performed by Health Sciences South Carolina (HSSC), showcases a Key Event Receipt Infrastructure (KERI) enabled, scalable, zero-trust data exchange between organizations.

By replacing traditional certificate-based security with a decentralized, cryptographic key management system, HSSC achieved significant advancements in security, efficiency, and automation.

**Zero-Trust Data Exchange -** Transitioned from trust-based systems to a cryptographic model that ensures every interaction is mathematically verified, eliminating reliance on static credentials or third-party trust.

**Penetration Tested -** HSSC's initial implementation was penetration tested by Psicurity, a third-party assessor founded in 2003. The KERI-based exchange was successful in maintaining the security of the data.

**New Key Management -** Implemented dynamic key rotations as frequently as needed, automating a historically cumbersome process.

**Proven Scalability -** Successfully processed over 100,000 synthetic patient records with zero percent data loss, creating a fully reliable, cryptographic validation on every record.

**Post-Quantum Agility -** Positioned to adapt to evolving cybersecurity challenges with a future-proof, quantum-resistant framework.

**Standard-Ready -**
This project validated the usability of KERI across existing standards like FHIR and HL7v2, reduced operational burdens, and laid the groundwork for addressing pressing use cases such as AI safety, third-party risk mitigation, and clinical data warehousing.

HSSC's deployment of open-source KERI showcases the potential to transform health information exchanges (HIEs), delivering enhanced security and interoperability while simplifying and automating compliance in a complex regulatory landscape.

## Program Goals

- Create a **zero-trust** system for exchanging data
- Enhance the security of data exchange across **trust domains**
  - Automatic **cryptographic key rotation**
  - Post-quantum agility
- Automate/replace **certificate process**
- Prove usability with current/future standards (HL7v2, FHIR)
- Establish cryptographic **data provenance**
- Reduce workload burden for data exchange setup & maintenance

## Contact Information


**healthKERI, Inc.**
Jared Jeffery, FACHDM
Founder & CEO
*info@healthkeri.com*

**Health Sciences South Carolina**
Kenneth Deans, Jr., DHA
President & CEO
*HSSCInfo@healthsciencessc.org*


**Third-party Penetration Testing Provided by:**
*Psicurity*
*https://psicurity.com/*

## Glossary of Terms

**Zero Trust** - A cybersecurity concept that assumes no entity, internal or external, is trusted by default, requiring continuous verification of all users and systems attempting to access resources. It emphasizes "never trust, always verify" principles to minimize risks.

**KERI** - Key Event Receipt Infrastructure, an open-source, Linux Foundation standard, cryptographic protocol for decentralized, secure, and automated key management to enable verifiable data exchange. Learn more

**Trust Domains** - Distinct networks with a shared IT infrastructure maintained and governed by one entity. For example; a trust domain would include a company, its data, employees, policies, devices, etc.

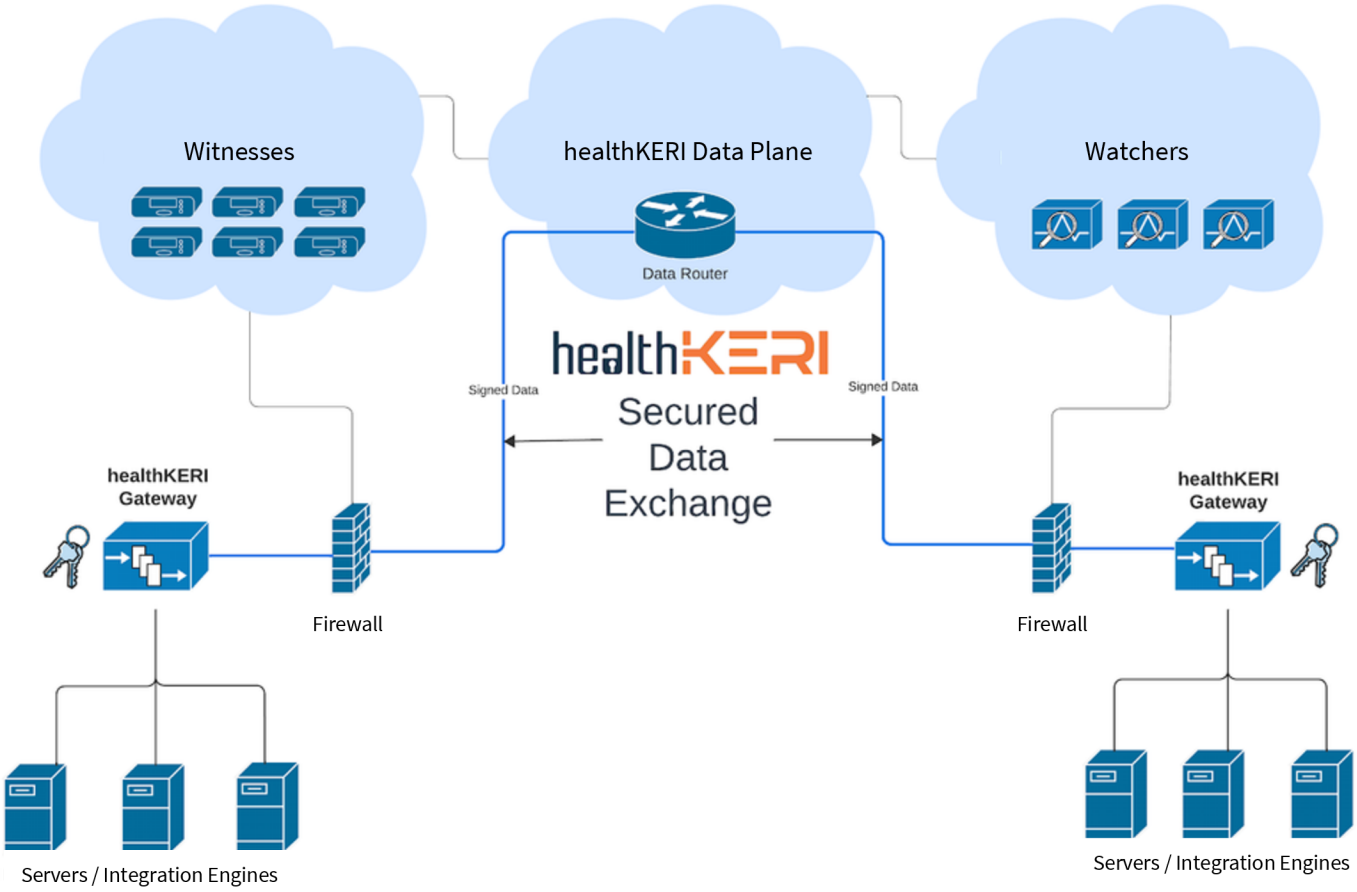
**Cryptographic Keys** - Unique strings of characters used for encryption and digital signatures, ensuring that only authorized parties can access the data. They are essential in securing digital communications, maintaining confidentiality and verifying data authenticity.

**Cryptographic Key Rotation** - The process of periodically generating and replacing cryptographic keys to enhance security by reducing the time a compromised key can be exploited.

**Certificate Process** - An outdated method of issuing, managing, and verifying digital certificates that authenticate identities or systems.

**Data Provenance** - The tracking and documentation of the origins, history, and modifications of data to ensure its integrity, authenticity, and reliability.

# System Architecture




This diagram shows the architecture used by Health Sciences South Carolina (HSSC) to establish a new, zero trust method of data exchange. There are several key elements of note:

1. The servers on the bottom left/right represent the two separate trust domains exchanging data.
2. The healthKERI Gateways are located between the servers and the organizations' firewalls, these gateways generate cryptographic signatures, verify those signatures as well as encrypt and decrypt the data regardless of data flow.
3. The three clouds at the top represent the operational web services and rentable resources known as **witnesses** and **watchers** (both explained on page 4).

For this project, HSSC ran data from their Iguana interface engine via http (web traffic) and into a Blaze FHIR repository. The project transferred over **100,000** records, each one cryptographically signed and verified.

Typical security on data exchange requires use of certificates, which need frequent rotation due to known vulnerabilities. Google has recently recommended a 90 day cycle between TLS x509 certificate rotations.

For health systems, management and rotation of certificates represents a time-consuming, manual process and is therefore often overlooked, becoming a security risk. KERI does not suffer from these vulnerabilities and replaces the need for certificates. HSSC successfully performed hourly rotations of keys via KERI during this project. In addition, all rotation events were detected/verified by the established witness network.

This KERI-based zero-trust architecture ensures that every piece of data exchanged between two parties is signed and verified before its ingestion into the system, guaranteeing its authenticity and integrity. Unlike traditional methods that rely on static, centralized credentials (like passwords or certificates), this system moves the cryptographic keys to the edge. Meaning; each exchange partner has control/ownership of their identifiers. This removes risky points of failure, such as third party trust.

Additionally, cryptographic keys can be rotated or updated dynamically without disrupting operations, leading to unmatched rapid-response to key state compromise. With KERI, trust isn't assumed—it's mathematically proven with each transaction, creating an auditable chain of trust for every piece of data sent from point A to point B. This approach is superior because standard methodologies for connection that are certificate-based and often rely on shared secrets or assume trust in third parties, both of which are vulnerable to breaches or misuse.

If one credential is compromised, the entire system can be at risk. KERI eliminates this problem by requiring cryptographic proof for every interaction, ensuring only authorized parties can access and validate the data.

This not only strengthens security but also enables organizations to meet compliance requirements more easily, as every data exchange is automatically logged and verifiable. In short, this architecture makes secure data exchange both more robust and adaptable in today's evolving threat landscape.

In the KERI ecosystem, two key advancements are witnesses and watchers, which serve distinct roles in ensuring the integrity and availability of key events and their associated data.

## Witnesses

Witnesses are nodes in a KERI-based network that act as validators and confirmers of the **signer's** cryptographic key events. For example, when an entity updates its keys or performs any cryptographic operation (e.g., signing), witnesses receive and store these events, cryptographically verify them, and provide proof that they've been seen in the form of a receipt and digital signature.

Witnesses provide durability and resilience by serving as decentralized records of key events. They help ensure that an entity's key management history is auditable and tamper-proof. Witnesses are chosen by the controller (the entity managing the keys), making them an additional security threshold in addition to the controller's own keys.

## Watchers

Watchers are third-party nodes that monitor and observe key events in a KERI network on behalf of a **verifier** of key state. Unlike witnesses, watchers are under the control of a third-party verifier and not the controller of key state, they independently track and validate the consistency and authenticity of key state changes.

Watchers act as an additional layer of oversight. They help ensure that no unauthorized changes or inconsistencies occur in the key event log. For example, they might alert a verifier if a key rotation is inconsistent with prior events or if multiple witnesses disagree on the current key state.

## Penetration Test Results

> "Overall, no vulnerabilities were discovered on the healthKERI system that would create a significant risk to the organization, such as by exposing the data to a breach of confidentiality, integrity, and/or availability."

PSICURITY

Founded in 2003, Psicurity has helped organizations across industries identify security gaps and adapt to the ever-changing threat landscape. Psicurity conducted a penetration test on an exchange channel using only KERI's built-in security features to see if HSSC's implementation could be hacked. The test tried to exploit common attacks like DoS, unauthorized access, and tampering with data but couldn't break through.

## Use Cases

As a result of this successful project, HSSC has identified the following urgent use cases for potential further development with healthKERI and the open source KERI tech stack:

### State Endorsed Digital Identity (SEDI)

The state of Utah has led out on a new identity model for citizens, using KERI as its underlying trust infrastructure. HSSC's implementation of KERI provides a practical proof point for several foundational capabilities SEDI will require: verifiable organizational identities, cryptographic data provenance, automated key rotation, and secure exchange between independent trust domains. As other states consider the Utah model, HSSC has demonstrated that KERI can support high-volume healthcare data flows without relying on shared secrets, static certificates, or a single centralized trust authority.

### Clinical Data Warehousing / Semantic Data Modeling

KERI enhances clinical data warehousing by ensuring the authenticity, integrity, and traceability of all data ingested into the warehouse. Its cryptographic system verifies the provenance of every data source, preventing tampering or unauthorized alterations. The result is a foundation of trust for analytics, reporting, and decision-making, as all stored data is verifiably accurate and secure. With KERI, clinical data warehouses become more reliable, automated, and resilient against security threats.

## FHIR / HL7 v2 Data Streams

KERI simplifies the creation of new FHIR or HL7v2 data flows by providing a secure, scalable way to verify and manage connections between parties. Using phish-proof identifiers and tamper-proof event logs ensures that data flows are protected from the start, without relying on cumbersome central authorities. This eliminates the need for insecure shared secrets, speeding up the establishment of data exchanges. With KERI, organizations can quickly and confidently set up new data flows that automate manual processes while enhancing security and interoperability.

## TEFCA Source Uncertainty

KERI eliminates TEFCA Source Uncertainty by providing a secure, tamper-proof way to verify the origin and integrity of shared health data—or create data provenance. KERI can create a transparent and reliable system where every data transaction is verifiable, reducing risks and building trust across the entire health information exchange network. This will increase the response rate to queries through the TEFCA network as organizations are able to clearly identify source and integrity.

## Third Party Risk Mitigation

KERI mitigates third-party risk by creating a secure, decentralized way to verify the identity and trustworthiness of all parties involved in data exchange. By using cryptographic keys and tamper-proof event logs, KERI ensures that no third party can alter or misuse data without detection. This eliminates reliance on centralized authorities or intermediaries, reducing exposure to risks like fraud, breaches, or system failures. With KERI, organizations can confidently engage with third parties, knowing their data and interactions are fully secure and verifiable.

## AI Safety

KERI solves critical AI Safety challenges by ensuring data and models are secure and trustworthy. Its cryptographic system guarantees the provenance and integrity of data, making tampering or corruption impossible. This eliminates risks of malicious interference or unauthorized control of AI systems. With KERI, organizations can deploy AI with absolute confidence in its security and reliability.

# Conclusion

HSSC has demonstrated how adopting KERI technology addresses critical challenges in healthcare data exchange. By replacing traditional certificate-based systems with a cryptographic, zero-trust framework, HSSC improved both security and operational efficiency while maintaining compliance with data exchange standards.

## Key Results

**Enhanced Security -** Each transaction was cryptographically verified, removing the need for shared secrets or centralized credentials.

**Automated Key Management -** Automated key rotations were implemented, significantly reducing manual effort and improving security.

**Scalable Data Exchange -** Over 100,000 synthetic patient records were exchanged with cryptographic validation for every transaction.

**Future-Proof Security -** The solution is designed to remain secure against evolving threats, including quantum computing.

**Interoperability -** Compatible with existing standards like FHIR and HL7v2, enabling smooth integration into current workflows.

This case study provides a practical example of how decentralized, cryptographic systems using KERI can enhance security and reliability in health information exchanges, offering insights for broader applications in healthcare data management.