

Inputs Domain Group

- [Introduction](#)
- [Scope](#)
- [Chairs / Leads](#)
- [Core Inputs Concepts](#)
 - [Key Event Receipt Infrastructure \(KERI\)](#)
- [Deliverables](#)

Meetings

Weekly on Wednesdays from 09:00-10:00 US PT, 12:00-13:00 US ET, 17:00-18:00 UTC

[Calendar invitation](#)

[Zoom link](#)

Introduction

Data entry is defined as the process of inputting data into a computer using devices such as a keyboard, scanner, disk, sensor, or voice. In a decentralized network, data entry requires a signing key in order to establish that inputted data has come from an authentic source. In the *Model of Identifier States*, all elements and characteristics of data entry are depicted in the northern hemispherical *Inputs domain*.

Inputs domain [*active*] / what is put in, taken in, or operated on by any process or system

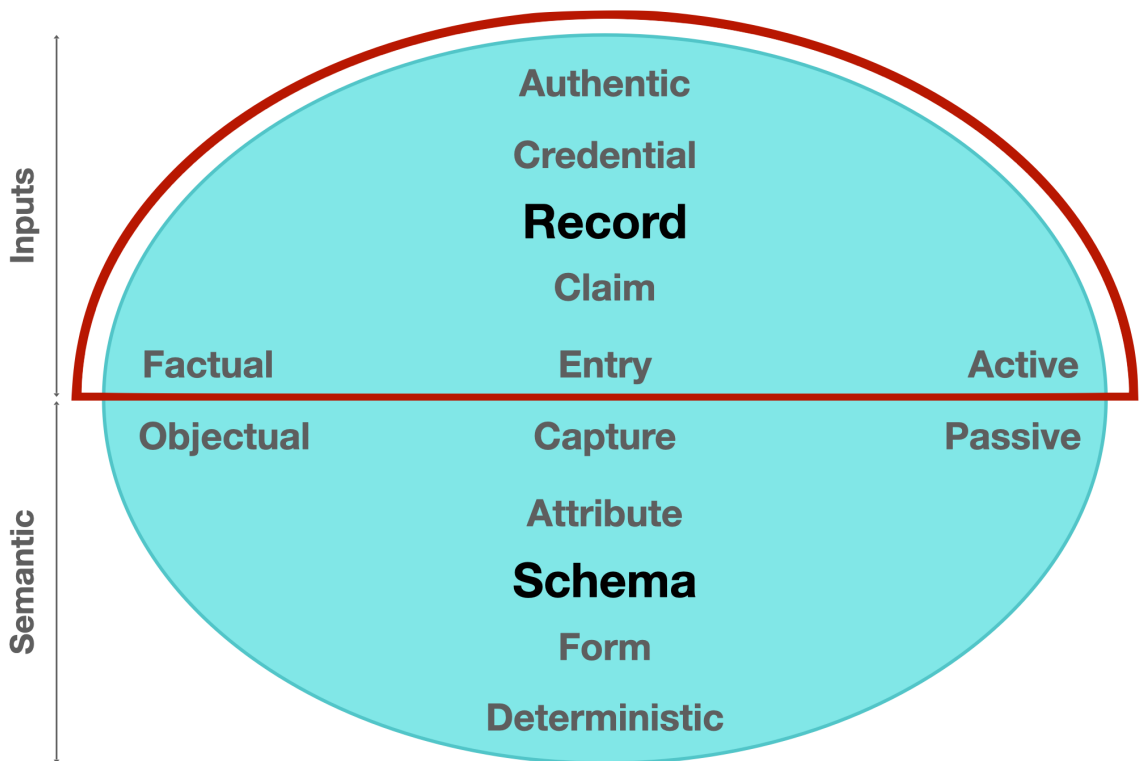


Figure 1. A component diagram highlighting the Inputs domain within a balanced network model.

Scope

The mission of the Inputs group (ISWG-I) is to define a decentralized key management infrastructure that provides self-certifying identifier issuance underpinned by cryptographic one-way functions for Internet-scale deployment. The scope of this sub-group is to define specifications and best practices that bring cohesion to data entry processes and other *Inputs standards* throughout the ToIP stack, whether these standards are hosted at the Linux Foundation or external to it. Other sub-group activities will include creating template Requests for Proposal (RFPs) and additional guidance to utility and service providers regarding implementations in this domain. This sub-group may also organize Task Forces and Focus Groups to escalate the development of certain components if deemed appropriate by the majority of the sub-group members and in line with the overall mission of the ToIP Foundation.

Chairs / Leads

- Chair: [Robert Mitwicki](#)
- Vice-Chair: [Neil Thomson](#)

Core Inputs Concepts

Key management refers to the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction), and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

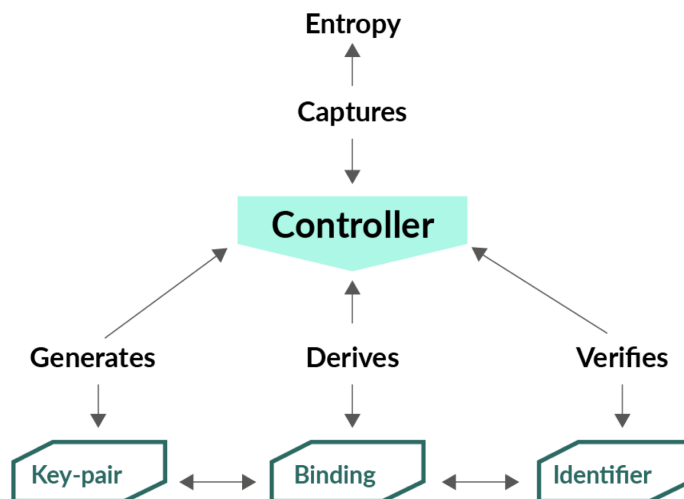
Successful key management is critical to the security of a cryptosystem. Developing and deploying the right key management infrastructure will ensure the highest level of security to enable tamper-resistant interactions between governing entities as autonomous peers in a digital system.

Key Event Receipt Infrastructure (**KERI**)

([Presentation](#))

KERI is an architecture that offers information uniqueness from captured entropy by compiling the history of all uses or changes to the public/private key pair. This is achieved by universal self-certifying proofs of the binding between the self-certifying identifier (SCID) and the associated public/private key pairs. It is a truly decentralized key management solution offering the strongest possible levels of pseudonymity, ledger-less identifiers, and separable identifier assurance bases for all network participants.

KERI is a secure overlay for the Internet where any digital representation of a governing entity can serve as an autonomous self-certifying root-of-assurance. It is a solution that offers secure data control established via self-certifying pseudonymous identifiers. As a standardized global solution for data entry, KERI facilitates sapored data supply chains, enabling a record trail that accounts for the origin of data inputs operated on by any process or system.



KERI resources:

- KERI website - <https://keri.one>
- KERI whitepaper - <https://arxiv.org/abs/1907.02143>

Deliverables

- Technical specifications for all core components required within the *Inputs domain* as defined by the ISWG-I Scope statement.
- Also, check out the [ToIP Deliverables](#) document for high-level deliverables of the Trust over IP Foundation.