Workgroup: Path Aware Networking RG
Internet-Draft:
draft-rustignoli-panrg-scion-components-02
Published: 10 March 2023
Intended Status: Informational
Expires: 11 September 2023
Authors: N. Rustignoli C. de Kater
SCION Association SCION Association

SCION Components Analysis

Abstract

SCION is an inter-domain Internet architecture that focuses on security and availability. Its fundamental functions are carried out by a number of components.

This document analyzes its core components from a functionality perspective, describing their dependencies, outputs, and properties provided. The goal is to answer the following questions:

* What are the main components of SCION and their dependencies? Can they be used independently?

* What existing protocols are reused or extended? Why (or why not)?

In addition, it focuses on the properties achievable, motivating cases when a greenfield approach is used. It then briefly touches on the maturity level of components and some extensions.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://scionassociation.github.io/scion-components_I-D/draft-rustignoli-panrg-scion-components.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-rustignoli-panrg-scion-components/.

Discussion of this document takes place on the Path Aware Networking RG Research Group mailing list (mailto:panrg@irtf.org), which is archived at https://www.ietf.org/mail-archive/web/panrg/. Subscribe at https://www.ietf.org/mailman/listinfo/panrg/.

Source for this draft and an issue tracker can be found at https://github.com/scionassociation/scion-components_I-D.

Status of This Memo

This Internet-Draft will expire on 11 September 2023.

Copyright Notice

Table of Contents

1. Introduction

While SCION was initially developed in academia, the architecture has now "slipped out of the lab" and counts its early productive deployments (including the Swiss inter-banking network SSFN). The architecture consists of a system of related components, some of which are essential to set up end-to-end SCION connectivity. Core components are the data plane, the control plane, and the PKI. Add-ons provide additional functionality, security, or backward compatibility. Discussions at PANRG [PANRG-INTERIM-Min] showed the need to describe the relationships between components. This document, therefore, takes a look at each core component individually and independently from others. It focuses on describing its dependencies, outputs, functionality, and properties. It then touches on relationships to existing protocols. The goal is not to describe each component's specification, but to illustrate the engineering decisions that made SCION what it is and to provide a basis for further discussions and work.

Before reading this document, please refer to [I-D.dekater-scion-overview] for a generic overview of SCION and its components, the problems it solves, and existing deployments. Each component is to be described in-depth in dedicated drafts: see [I-D.dekater-scion-pki] for the SCION PKI specification, and refer to [CHUAT22] for other components.

1.1. Design Goals

SCION was created from the start with the intention to provide the following properties for inter-domain communication.

* *Availability*. SCION aims to provide highly available communication. Its focus is not only on quickly handling failures (both on the last hop or anywhere along the path) but also on allowing communication in the presence of adversaries. Availability is fundamental as applications move to cloud data centers, and enterprises increasingly rely on the Internet for mission-critical communication.

* *Security*. SCION comes with an arsenal of mechanisms, designed by security researchers with the goal of making most network-based and routing attacks either impossible or easy to mitigate. SCION strongly focuses on preventing routing attacks, IP prefix hijackings, and on providing stronger guarantees than the existing Internet. Security is tightly related to trust. SCION, therefore, offers a new trust model, transparency, and control to endpoints over forwarding paths. In addition, SCION's design starts from the assumption that any two entities on the global Internet do not mutually trust each other. SCION, therefore, enables trust agility, allowing its users to decide the roots of trust they wish to rely upon.

* *Scalability*. Security and high availability should not result in compromises on scalability. At the same time, a next-generation Internet architecture should scale with global network growth and avoid limitations related to forwarding table size. The S in SCION, indeed, stands for scalability. The architecture proposes a design that is scalable both in the control plane and in the data plane (as described later in the document).

Many research efforts have analyzed whether such properties could be achieved by extending the existing Internet architecture. As described for each core component in the following paragraphs, tradeoffs between properties would be unavoidable when exclusively relying on or extending existing protocols.

2. Minimal Stack - Core Components

To establish end-to-end connectivity, SCION relies on three main components.

* Data plane: it carries out secure packet forwarding, providing path-aware inter-domain connectivity.

* Control plane: it performs inter-domain routing by discovering and securely disseminating path information.

* PKI: it handles cryptographic material and provides a unique trust model.

A SCION network is formed of multiple interconnected administrative domains, called SCION autonomous systems (AS). Each AS deploys all of the three components above. Implementations of all of the above components are deployed in production (e.g., they are in use within the SSFN, the Swiss Finance Network). There are commercial implementations (including a high-performance data plane).

A SCION packet is sent through a SCION network by SCION endpoints (i.e., a network host). It is then forwarded between ASes by the SCION data plane, which authenticates packets at each hop. The control plane is responsible for discovering and disseminating routing information. Path discovery is performed by each AS thanks to an authenticated path-exploration mechanism called beaconing. SCION endpoints query their respective AS control plane and obtain authenticated and authorized network paths, in the form of path segments. Endpoints select one or more of the end-to-end network paths, based on the application requirements (i.e., latency). Endpoints then craft SCION packets containing the end-to-end path to the destination.

The control plane relies on the control-plane PKI (CP-PKI) for authentication (e.g., of path segments). SCION's authentication mechanisms aim at protecting the whole end-to-end path at each hop. Such mechanisms are based on a trust model that is provided by the concept of Isolation Domains (ISDs). An ISD is a group of Autonomous

Systems that independently defines its own roots of trust. ISD members share therefore a uniform trust environment (i.e., a common jurisdiction). They can transparently define trust relationships between parts of the network by deciding whether to trust other ISDs. SCION trust model, therefore, differs from the one provided by other PKI architectures. The motivation behind this design choice is clarified in Section 2.1.

The following paragraphs look at each component individually. Rather than describing how each component works, they focus on each component's dependencies and properties provided to other components. The idea is to try to think of each component as a black box, and look at its "inputs" and "outputs".

2.1. Authentication - SCION CP-PKI

SCION's control plane messages and path information are all authenticated. This helps SCION avoid some of the obstacles to deployment mentioned in [RFC9049], where several path-aware methods failed to achieve deployment because of lack of authentication or lack of mutual trust between hosts and the intermediate network. The verification of messages relies on a public-key infrastructure (PKI) called the control-plane PKI or CP-PKI. It consists of a set of mechanisms, roles, and policies related to the management and usage of certificates, which enables the verification of signatures of, e.g., path-segment construction beacons (PCBs). A detailed specification of the PKI is available in [I-D.dekater-scion-pki].

2.1.1. Key Properties

One might ask why SCION requires its own PKI, rather than reusing some of the existing PKI architectures to issue AS certificates. Several properties distinguish the CP-PKI from others, and motivate SCION's distinct approach.

* *Locally scoped and flexible trust.* SCION is designed to securely connect ASes that do not necessarily share mutual trust. This requires a trust model that is different from the ones that are behind commonly deployed PKIs. In a monopolistic model, all entities trust one or a small number of roots of trust. In an oligopolistic model, there are multiple equally trusted roots (e.g., in the Web PKI). In both models, some or all certification authorities are omnipotent. If their key is compromised, then the security of the entire system collapses. Both models do not scale well to a global environment, because mutually distrustful entities cannot agree on a single root of trust (monopoly) and because in the oligopoly model, the security is as strong as its weakest root. In the SCION CP-PKI, trust is locally scoped within each ISD, and the capabilities of each ISD (authentication-wise) are limited to the communication channels in which they are involved. Each ISD can define its own trust policy. ASes must accept the trust policy of the ISD(s) in which they participate,

but they can decide which ISDs they want to join, and they can participate in multiple ISDs.

* *Resilience to compromised entities and keys.* Compromised or malicious trust roots outside an ISD cannot affect operations that stay within that ISD. Moreover, as trust roots (in the form of a TRC) can only be updated through a voting process, each ISD can be configured to withstand the compromise of a number of its root keys.

* *Multilateral governance.* The voting mechanism mentioned above makes sure that fundamental changes to the trust policies are only allowed with the consent of multiple entities administering an ISD. Within an ISD, no single entity is in full control, or owns a cryptographic "kill-switch".

* *Support for versioning & updates.* Trust within an ISD is normally bootstrapped with an initial ceremony. Subsequent updates to the root of trust (TRC) are handled automatically. The PKI design makes sure that certificate rollover can be automated so that certificates can be rotated frequently (e.g., every few days for AS certificates).

* *Scalability.* The authentication infrastructure scales to the size of the Internet and is adapted to the heterogeneity of today's Internet constituents.

2.1.2. Dependencies

Setting up the PKI in a freshly created Isolation Domain requires an initial trust bootstrapping process among some of the ISD members (i.e. a key exchange ceremony, and manual distribution of the initial ISD trust anchor). As updates to the later roots of trust are automated, this process is in principle only required once. In addition, certificate verification requires that PKI components can mutually communicate and have coarsely synchronized time.

The CP PKI enables the verification of signatures, e.g., on path-segment construction beacons (PCBs). It is built on top of a peculiar trust model, where entities are able to select their roots of trust. It constitutes the most independent and self-contained core component, as it does not have significant dependencies on other SCION components.

2.1.3. Provided to Other Components

The PKI makes trust information available to the control plane through two elements:

* *Trust Root Configuration (TRC)*: The PKI provides well-defined per-ISD trust policies, in the form of a per-ISD Trust Root Configuration (TRC). The TRC contains the ISD trust roots, and it

is co-signed by multiple entities in a multilateral process called voting.

* *AS certificates*: For each Autonomous System that is part of an ISD, the PKI provides an AS certificate that is used by other components for authentication. It also provides a validation path up to the ISD trust root, through intermediate CA certificates.

SCION CP-PKI comprises an optional extension called DRKey, which enables efficient symmetric key derivation between any two entities in possession of AS certificates. Such symmetric keys are used for additional authentication mechanisms for high-rate data-plane traffic and some control messages. As authentication based on digital signatures only scales well for relatively low message rates, using symmetric keys makes sure that the performance requirements for the high message rate of the data plane can be met. For more information, refer to the extension draft [I-D.garciapardo-drkey].

The trust model and certificates provided could be used not only by the SCION control plane but also other systems and protocols.

2.1.4. Relationship to Existing Protocols

The CP-PKI is based on certificates that use the X.509v3 standard [RFC5280]. There are already several professional industry-grade implementations.

The SCION trust model differs from existing PKIs in two ways. First, no entity is globally omnipotent, as Isolation Domains elect their own locally scoped root of trust. Second, changes to the trust roots require a voting process, making governance multilateral and each trust root resilient to the compromise of some of its keys.

These properties would be lost if SCION were to rely on an existing PKI (i.e., the web PKI, the RPKI, ...). For example, if SCION were to use the RPKI instead of the CP-PKI, its control plane would lack the trust model required to support Isolation Domains. This is because RPKI's trust model follows the same structure as the IP allocation hierarchy, where the five RIRs represent the trust roots. Within SCION, RPKI is instead used to secure some of its transition mechanisms, as later explained in Section 3.1.

In conclusion, SCION is built around a unique trust model, justifying the existence of the CP-PKI.

2.2. Routing - Control Plane

The SCION control plane's main purpose is to securely discover and disseminate routing information. Path exploration is based on path-segment construction beacons (PCBs), which are initiated by a subset of ASes and accumulate cryptographically protected path forwarding information. Each AS selects a few PCBs and makes them available to endpoints via its path service, part of the control plane.

Overall, the control plane takes an unexplored topology and AS certificates as input, it then discovers the inter-domain topology and makes routing information available to endpoints.

The following section describes the core properties provided by the SCION control plane, its relationships with existing protocols, and its dependencies on the PKI. For an overview of the process to create and disseminate path information, refer to [I-D.dekater-scion-overview], section 1.2.2. The control plane is internally formed by multiple sub-components (as the beacon service, responsible for path discovery, and the path service, responsible for path dissemination). Processes and interfaces specifications between these sub-components could be topic for one or multiple dedicated documents.

2.2.1. Key Properties

* *Massively multipath.* When exploring paths through beaconing, SCION ASes can select PCBs according to their policies, and register the corresponding path segments, making them available to other ASes and endpoints inside their network. SCION endpoints can leverage a wide range of (possibly disjoint) inter-domain paths, based on application requirements or path conditions. This goes beyond the capabilities of existing multipath mechanisms, such as BGP ADD-PATH [RFC7911], that is focusing on advertising multiple paths for the same prefix to provide a backup path.

* *Scalability.* The SCION's beaconing algorithm is scalable and efficient due to the following reasons: The routing process is divided into a process within each ISD (intra-ISD) and one between ISDs (inter-ISD), SCION beaconing does not need to iteratively converge, and SCION makes AS-based announcements instead of IP prefix-based announcements. Scalability of the routing process is fundamental not only to support network size growth but also to quickly react to failures. An in-depth study of SCION's scalability in comparison to BGP is available in [KRAHENBUHL2022].

* *Convergence time.* Since routing decisions are decoupled from the dissemination of path information, SCION features faster convergence times than path-vector protocols. Path information is propagated across the network by PCBs in times that are within the same order of magnitude of network round trip time. In addition, the division of the beaconing process into intra- and inter-ISD helps in speeding up global distribution of routing information. This means that SCION can restore global reachability, even after catastrophic failures, within tens of seconds.

* *Hop-by-hop path authorization.* SCION packets can only be forwarded along authorized path segments. This is achieved thanks to message authentication codes (MACs) within each hop field. During beaconing, each AS's control plane creates nested MACs, which are then verified during forwarding. This gives endpoints strong guarantees about the path where the data is routed, with minimal overhead and resource requirements on routers. Giving endpoints strong guarantees about the full inter-domain path is important to avoid traffic interception, and to enable geofencing (i.e., keeping data in transit within a well-defined trusted area of the SCION network). This facilitated early adoption in the finance industry.

* *Host addressing agnostic.* SCION decouples routing from host addressing: inter-domain routing is based on ISD-AS tuples rather than on host addresses. This design decision has two outcomes: First of all, SCION can reuse existing host addressing schemes, such as IPv6, IPv4, or others. Second, the control plane does not carry prefix information. Thanks to PCFS, packets contain forwarding state, so routers do not need to look up routing tables (avoiding the need for dedicated hardware).

* *Transparency.* SCION endpoints have full visibility of the inter-domain path where their data is forwarded. This is a property that is missing in traditional IP networks, where routing decisions are made by each hop, therefore endpoints have no visibility nor guarantees on where their traffic is going. Additionally, SCION users have visibility on the roots of trust that are used to forward traffic. SCION, therefore, makes it harder to redirect traffic through an adversary's vantage point. Moreover, SCION gives end users the ability to select which parts of the Internet to trust. This is particularly relevant for workloads that currently use segregated networks.

* *Fault isolation.* As the SCION routing process is hierarchically divided into intra-ISD and inter-ISD, faults have a generally limited and localized impact. Misconfigurations, such as an erroneous path policy, may suppress some paths. However, as long as an alternative path exists, communication is possible. In addition, while the control plane is responsible for creating new paths, it does not invalidate existing paths. The latter function is handled by endpoints upon detecting failures or eventually receiving an SCMP message from the data plane. This separation of control and data plane prevents the control plane from cutting off an existing communication or having a global kill-switch.

2.2.2. Dependencies

The SCION control plane requires the control-plane PKI to authenticate path information. It heavily relies on certificates provided by the CP-PKI for beaconing (i.e., for authenticating routing information). Each Isolation Domain requires its own root of trust, in the form of a TRC, in order to carry out path exploration and dissemination.

While in principle the control plane could use certificates provided by another PKI, it would be severely affected by a lack of the ISD concept. All security properties related to the trust model would be affected. The concept of ISD is also necessary for scalability and fault isolation to organize the routing process into a two-tiered architecture.

In conclusion, the control plane depends on the CP-PKI. If it were to be used with another PKI, it would lose several of its fundamental properties.

2.2.3. Provided to Other Components

In SCION, an endpoint sending a packet must specify, in the header, the full SCION forwarding path the packet takes towards the destination. This concept is called packet-carried forwarding state (PCFS). Rather than having knowledge of the network topology, an endpoint's data plane relies on the control plane for getting such information. The endpoint's SCION stack queries path segments, then it selects them and combines them into a full forwarding path to the destination.

The control plane is responsible, therefore, for providing an authenticated (multipath) view of the explored global topology to endpoints (and, in turn, to the data plane). In addition, it provides the data plane the ability to send authenticated control messages. The "interfaces" towards the data plane are represented by:

* *Path segments*, that are provided to endpoints and used by SCION routers for forwarding. Segments are designed so that each AS data plane can independently verify its own segments, while globally achieving full path authorization.

* *SCMP.* SCION control-plane messages are by default all authenticated. In addition to beacons, the control plane offers the SCION Control Message Protocol (SCMP). It is analogous to ICMP, and it provides functionality for network diagnostics, such as ping and traceroute, and authenticated error messages that signal packet processing or network layer problems. SCMP is the first control message protocol that supports the authentication of network control messages, preventing unauthenticated control messages from potentially being used to affect or even prevent traffic forwarding. SCMP is used, for example, by the data plane to achieve path revocation.

2.2.4. Relationship to Existing Protocols

At first sight, it might seem that the SCION control plane takes care of similar duties as existing routing protocols. While both focus on disseminating routing information, there are substantial differences in their mechanisms and properties offered.

The SCION control plane was designed to carry out inter-domain routing, while intra-domain routing (and forwarding) are intentionally left out of scope. Existing IGPs are used within an AS, allowing the reuse of existing intra-domain routing infrastructure and reducing the amount of changes required for deployment.

End-host addressing is decoupled from routing. Similar to LISP [RFC6830], SCION separates routing, that is based on locator (an ISD-AS tuple), and host identifiers (e.g., IPv6, IPv4, ...). While the two architectures have this concept in common, there are notable differences. SCION brings improvements to inter-domain routing and provides secure multipath, while LISP provides a framework to build overlays on top of the existing Internet. In addition, LISP security proposals focus on protecting identifier to locator mappings, while SCION focuses on securing inter-domain routing. Lastly, identifier to locator mapping in SCION not part of the core components, rather it is left to some of its transition mechanisms, later described in Section 3.1.

The above-mentioned decoupling also implies that SCION does not provide, by design, IP prefix origin validation, which is currently provided by RPKI [RFC8210]. As prefix origin validation is outside of SCION's scope, IP-to-SCION's coexistence mechanisms (SIAM, SBAS) later discussed in Section 3.1 build on top of RPKI for IP origin attestation.

Additionally, the SCION control plane design takes into account some of the lessons learned discussed in [RFC9049]: It does not try to outperform end-to-end mechanisms, as path selection is performed by endpoints. SCION, therefore, can leverage existing end-to-end mechanisms to switch paths, rather than compete with them. In addition, no single component in the architecture needs to keep connection state, as this task is pushed to endpoints.

One last point is that several of the SCION control plane properties and key mechanisms depend on the fact that SCION ASes are grouped into Isolation Domains (ISDs). For example, ISDs are fundamental to achieving transparency, routing scalability, fault isolation, and fast propagation of routing information. No existing protocol provides such a concept, motivating the existence of the control plane.

2.3. Forwarding - Data Plane

The SCION data plane is responsible for inter-domain packet forwarding between ASes. SCION routers are deployed at an AS network edge. They receive and validate SCION packets from neighbors, then they use their intra-domain forwarding information to transmit packets to the next SCION border router or to a SCION endpoint inside the AS.

SCION packets are at the network layer (layer-3), and the SCION header sits in between the transport and link layer. The header contains a variable type and length host address, and can therefore carry any address (IPv4, IPv6, ...). In addition, host addresses only need to be unique within an AS, and can be, in principle, reused.

2.3.1. Key Properties

* *Path selection.* In SCION, endpoints select inter-domain network paths, rather than routers. The endpoints are empowered to make end-to-end path choices based on application requirements. This means that routers do not carry the burden of making enhanced routing or forwarding decisions.

* *Scalability.* SCION routers can efficiently forward packets without the need to look up forwarding tables or keep per-connection state. Routers only need to verify MACs in hop fields. This operation is based on modern block ciphers such as AES, can be computed faster than performing a memory lookup, and is widely supported in modern CPUs. Routers, therefore, do not require expensive and energy-intensive dedicated hardware and can be deployed on off-the-shelf hardware. The lack of forwarding tables also implies that the growing size of forwarding tables is of no concern to SCION. Additionally, routers that keep state of network information can suffer from denial-of-service (DoS) attacks exhausting the router's state [SCHUCHARD2011], which is less of a problem to SCION.

* *Recovery from failures.* SCION hosts usually receive more than one path to a given destination. Each host can select (potentially disjoint) backup paths that are available in case of a failure. In contrast to the IP-based Internet, SCION packets are not dynamically rerouted by the network in case of failures. Routers use BFD [RFC5880] to detect link failures, and in case they cannot forward a packet, they send an authenticated SCMP message triggering path revocation. End hosts can use this information, or perform active monitoring, to quickly reroute traffic in case of failures. There is therefore no need to wait for inter-domain routing protocol convergence.

* *Extensibility.* SCION, similarly to IPv6, supports extensions in its header. Such extensions can be hop-by-hop (and are processed at each hop), or end-to-end.

* *Path validation.* SCION routers validate network paths in packets at each hop, so that they are only forwarded along paths that were authorized by all on-path ASes in the control plane. Thanks to a system of nested message authentication codes, traffic hijacking attacks are avoided.

In conclusion, in comparison to today's Internet, the SCION's data plane takes some of the responsibilities away from routers and places them on endpoints (such as selecting paths or reacting to failures). This contributes to creating a data plane that is more efficient and scalable, and that does not require routers with specialized routing table lookup hardware. Routers validate network paths so that packets are only forwarded on previously authorized paths.

2.3.2. Dependencies

The data plane is generally decoupled from the control plane. To be able to transmit data, endpoints need to fetch path information from their AS control plane. In addition, some operations (such as path revocation) require the data plane to be able to use an authenticated control-plane mechanism, such as SCMP.

Path information is assumed to be fresh and validated by the control plane, which in turn relies on the CP-PKI for validation. The data plane, therefore, relies on both the control plane and indirectly on the CP-PKI to function.

Should the data plane be used independently, without end-to-end path validation, SCION would lose many of its security properties, which are fundamental in an inter-domain scenario where entities are mutually distrustful. As discussed in [RFC9049], lack of authentication has often been the cause for path-aware protocols never being adopted because of security concerns. SCION should avoid such pitfalls and therefore its data plane should rely on the corresponding control plane and control-plane PKI.

2.3.3. Provided to Other Components

The SCION data plane provides path-aware connectivity to applications. The SCION stack on an endpoint, therefore, takes application requirements as an input (i.e., latency, bandwidth, a list of trusted ASes, ...), and crafts packets containing an appropriate path to a given destination.

How to expose capabilities of path-aware networking to upper layers remains an open question. PANAPI (Path-Aware Networking API) [slides-113-taps-panapi] is being evaluated as a way of making path-awareness and multipath available to the transport layer at endpoints, using the TAPS abstraction layer.

2.3.4. Relationship to Existing Protocols

SCION is an inter-domain network architecture and as such its data plane does not interfere with intra-domain forwarding. It re-uses the existing intra-domain data and control plane to provide connectivity among its infrastructure services, border routers, and endpoints, minimizing changes to the internal infrastructure. This corresponds to the practice today where ASes use an intra-domain protocol of their choice (i.e., OSPF, IS-IS, MPLS, ...).

Given its path-aware properties, some of SCION's data plane characteristics might seem similar to the ones provided by Segment Routing (SR) [RFC8402]. There are, however, fundamental differences that distinguish and motivate SCION. The most salient one is that Segment Routing is designed to be deployed across a single trusted domain. SR, therefore, does not focus on security, which remains an open question, as outlined in [I-D.spring-srv6-security-consideration]. SCION, instead, is designed from the start to facilitate inter-domain communication between (potentially mutually distrustful) entities. It comes, therefore, with built-in security measures to prevent attacks (i.e., authenticating all control-plane messages and all critical fields in the data-plane header). Rather than compete, SCION and SR complement each other. SCION relies on existing intra-domain routing protocols, therefore SR can be one of the possible intra-domain forwarding mechanisms. Possible integration of its path-aware properties with SR remains for now an open question.

In SCION's current implementation and early deployments, intra-AS SCION packets are encapsulated into an IP/UDP datagram for AS-local packet delivery, reusing the AS existing IGP and IP-based data plane. This design decision eased early deployments of SCION in IP-based networks. In the long term, it is not excluded that SCION's data plane could be better integrated with IP. For example, SCION path information could be included in a custom IPv6 routing extension header ([RFC8200] section 4.4). Such approach requires further exploration on its impact on intra-domain forwarding and on addressing, so further discussion on the topic is left to future revisions of this draft.

3. Additional Components

This document mainly focuses on describing the fundamental components needed to run a minimal SCION network. Beyond that, SCION comprises several extensions and transition mechanisms that provide additional properties, such as improved incremental deployability, security, and additional features. For the sake of completeness, this paragraph briefly mentions some of these transition mechanisms and extensions.

3.1. Transition Mechanisms

As presented in [I-D.dekater-scion-overview], incremental deployability is a focus area of SCION's design. It comprises transition mechanisms that allow partial deployment and coexistence with existing protocols. These mechanisms require different levels of changes in existing systems and have different maturity levels (from production-grade to research prototype). Rather than describing how each mechanism works, this document provides a short summary of each approach, focusing on its functions and properties, as well as on how it reuses, extends, or interacts with existing protocols.

* *SCION-IP-Gateway (SIG).* A SCION-IP-Gateway (SIG) is a SCION endpoint that encapsulates regular IP packets into SCION packets. A corresponding SIG at the destination performs the decapsulation. This mechanism enables IP hosts to benefit from a SCION deployment by transparently obtaining improved security and availability properties. SCION routing policies can be configured on SIGs, in order to select appropriate SCION paths based on application requirements. SIGs can dynamically exchange prefix information, currently using their own encapsulation and prefix exchange protocol. This does not exclude reusing existing protocols in the future. SIGs are deployed in production SCION networks, and there are commercial implementations.

* *SIAM.* To make SIGs a viable transition mechanism in an Internet-scale network with tens of thousands of ASes, an automatic configuration system is required. SIAM creates mappings between IP prefixes and SCION addresses, relying on the authorizations in the Resource Public Key Infrastructure (RPKI). SIAM is currently a research prototype, further described in [SUPRAJA2021].

* *SBAS* is an experimental architecture aiming at extending the benefits of SCION (in terms of performance and routing security) to potentially any IP host on the Internet. SBAS consists of a federated backbone of entities. SBAS appears on the outside Internet as a regular BGP-speaking AS. Customers of SBAS can leverage the system to route traffic across the SCION network according to their requirements (i.e., latency, geography, ...). SBAS contains globally distributed PoPs that advertise its customer's announcements. SBAS relies on RPKI to validate IP prefix authorization. Traffic is therefore routed as close as possible to the source onto the SCION network. The system is further described in [BIRGLEE2022].

3.2. Extensions and Other Components

In addition to transition mechanisms, there are other proposed extensions, that build upon the three SCION core components described earlier in this document. DRKey [I-D.garciapardo-drkey] is a SCION extension that provides an Internet-wide key-establishment system allowing any two hosts to efficiently derive a symmetric key. This extension can be leveraged by other components to provide additional security properties. For example, LightningFilter [slides-111-panrg-lightning-filter] leverages DRKey to provide high-speed packet filtering between trusted SCION ASes. COLIBRI [GIULIARI2021] is SCION's inter-domain bandwidth reservation system. These additional components are briefly mentioned here in order to provide additional context. They are therefore unlikely to be the best candidates for future IETF work.

4. Component Dependencies Summary

Figure 1 briefly summarises on a high level the dependencies between SCION's core components discussed in the previous paragraphs.

```
                    * Initial trust ceremony
                    * Loose time synchronization
                    * Communication
     ┌─────────────────────────────┐
     │      Control plane PKI      │
     └─────────────────────────────┘
                   │ * TRC
                   ▼ * AS Certificates
     ┌─────────────────────────────┐
     │        Control plane        │
     └─────────────────────────────┘
                   │ * Path segments
                   ▼ * SCMP
     ┌─────────────────────────────┐
     │         Data plane          │
     └─────────────────────────────┘
                   │ * Secure  inter-domain path
                   ▼ to destination
     ┌─────────────────────────────┐
     │  Applications on endpoint   │
     └─────────────────────────────┘
```

Figure 1: Dependencies overview

Overall, the control plane PKI represents the most independent building block, as it does not rely on other SCION components. The control plane relies on the trust model and on certificate material provided by the PKI. It provides the data plane with path segments, that are then used at forwarding, and with SCMP, that is used for secure error messages. The data plane makes multipath communication available to applications on SCION endpoints.

5. Conclusions

This document describes the three fundamental SCION core components, together with their properties and dependencies. It highlights how such components allow SCION to provide unique properties. It then discusses how the main components are interlinked, to foster a discussion on the standardization of key components. The authors welcome feedback from the IETF community for future iterations.

6. Informative References

[BIRGLEE2022]
Birge-Lee, H., Wanner, J., Cimaszewski, G. H., Kwon, J., Wang, L., Wirz, F., Mittal, P., Perrig, A., and Y. Sun, "Creating a Secure Underlay for the Internet", 2022,

<https://www.usenix.org/conference/usenixsecurity22/presentation/birge-lee>.

[CHUAT22] Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Mueller, P., and A. Perrig, "The Complete Guide to SCION", ISBN 978-3-031-05287-3, 2022, <https://doi.org/10.1007/978-3-031-05288-0>.

[GIULIARI2021] Giuliari, G., Roos, D., Wyss, M., García-Pardo, J., Legner, M., and A. Perrig, "Colibri: A Cooperative Lightweight Inter-domain Bandwidth-Reservation Infrastructure", 2022, <https://netsec.ethz.ch/publications/papers/2021_conext_colibri.pdf>.

[I-D.dekater-scion-overview] de Kater, C., Rustignoli, N., and A. Perrig, "SCION Overview", 2022, <https://datatracker.ietf.org/doc/draft-dekater-panrg-scion-overview/>.

[I-D.dekater-scion-pki] de Kater, C. and N. Rustignoli, "SCION Control-Plane PKI", 2022, <https://datatracker.ietf.org/doc/draft-dekater-scion-pki/>.

[I-D.garciapardo-drkey] Pardo, J., Krähenbühl, C., Rothenberger, B., and A. Perrig, "Dynamically Recreatable Keys", 2022, <https://datatracker.ietf.org/doc/draft-garciapardo-panrg-drkey/>.

[I-D.spring-srv6-security-consideration] Li, C., Li, Z., Xie, C., Tian, H., and J. Mao, "Security Considerations for SRv6 Networks", 2022, <https://datatracker.ietf.org/doc/draft-li-spring-srv6-security-consideration/>.

[KRAHENBUHL2022]
Kraḧenbuḧl, C., Tabaeiaghdaei, S., Gloor, C., Kwon, J., Perrig, A., Hausheer, D., and D. Roos, "Deployment and Scalability of an Inter-Domain Multi-Path Routing Infrastructure", 2022, <https://netsec.ethz.ch/publications/papers/2021_conext_deployment.pdf>.

[PANRG-INTERIM-Min] "Path Aware Networking Research Group - Interim 106 Minutes", June 2022, <https://datatracker.ietf.org/meeting/interim-2022-panrg-01/materials/minutes-interim-2022-panrg-01-202206011700-00>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation

List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/rfc/rfc5880>.

[RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <https://www.rfc-editor.org/rfc/rfc6830>.

[RFC7911] Walton, D., Retana, A., Chen, E., and J. Scudder, "Advertisement of Multiple Paths in BGP", RFC 7911, DOI 10.17487/RFC7911, July 2016, <https://www.rfc-editor.org/rfc/rfc7911>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/rfc/rfc8200>.

[RFC8210] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1", RFC 8210, DOI 10.17487/RFC8210, September 2017, <https://www.rfc-editor.org/rfc/rfc8210>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/rfc/rfc8402>.

[RFC9049] Dawkins, S., Ed., "Path Aware Networking: Obstacles to Deployment (A Bestiary of Roads Not Taken)", RFC 9049, DOI 10.17487/RFC9049, June 2021, <https://www.rfc-editor.org/rfc/rfc9049>.

[SCHUCHARD2011] Schuchard, M., Mohaisen, A., Foo Kune, D., Hopper, N., Kim, Y., and E. Vasserman, "Losing control of the internet: using the data plane to attack the control plane", Proceedings of the 17th ACM conference on Computer and communications security, DOI 10.1145/1866307.1866411, October 2010, <https://doi.org/10.1145/1866307.1866411>.

[slides-111-panrg-lightning-filter]
Garcia Pardo, J. A., "Lightning Filter: High-Speed Traffic Filtering based on DRKey", 2021, <https://datatracker.ietf.org/meeting/111/materials/slides-111-

panrg-lightning-filter-high-speed-traffic-filtering-based-on-drkey-00.pdf>.

[slides-113-taps-panapi] Kruğer, T., "PANAPI, a Path-Aware Networking API", 2022, <https://datatracker.ietf.org/meeting/113/materials/slides-113-taps-panapi-implementation-00.pdf>.

[SUPRAJA2021] Supraja, S., Wirz, F., de Ruiter, J., Schutijser, C., Legner, M., and A. Perrig, "Global Distributed Secure Mapping of Network Addresses", 2021, <https://netsec.ethz.ch/publications/papers/sridhara_taurin2021_siam.pdf>.

Acknowledgments

The authors are indebted to Adrian Perrig, Laurent Chuat, Markus Legner, David Basin, David Hausheer, Samuel Hitz, and Peter Mueller, for writing the book "The Complete Guide to SCION" [CHUAT22], which provides the background information needed to write this document. Many thanks also to François Wirz, Juan A. Garcia-Pardo and Matthias Frei for reviewing this document.

Authors' Addresses

Nicola Rustignoli
SCION Association

Email: nic@scion.org

Corine de Kater
SCION Association

Email: cdk@scion.org