Abstract

This draft analyzes implementation methodologies for addressing the security requirements of SDN adopted network architecture through Public Key Infrastructure. The draft analyzes the relevant design patterns of PKI based Trust Models to address the challenges faced during SDN Adoption. And, the draft defines the considerations for setting up a Trust Relationship Management framework suitable for PKI based SDN integrated environment.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 22, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction
   1.1. Overview

Adoption of Software Defined Networking transforms certain inherent characteristics of traditional carrier network. The newer network architecture invites more stakeholders to the networking ecosystem, consolidates the distributed autonomous control functions into logically centralized and federated Controller plane, and supports developing innovative applications and services on top of this network architecture.

This change in the architecture also introduces a set of vulnerabilities which the network administrators previously didn’t have to deal with. The logical centralization of Control Plane may expose itself as single high-value asset to the attackers. And involvement of more stakeholders to the networking ecosystem, and integration of their infrastructure to carrier’s network, exposes more potential entry points for attackers.
Thus, planning and implementing the security support infrastructure becomes one of the most important success factors for adopting SDN. Most Technical Reports and Specifications published by Open Networking Foundation and other SDN focused industry and standard bodies have recommended PKI based Infrastructure for SDN security implementation. Towards this, this document consolidates different Security Practices, Framework, and Guidelines currently in use for establishing PKI, and analyzes the refined implementation scope to address the security requirements of SDN adopted network architecture. The document limits its scope to analyze the relevant design patterns of PKI based Trust Models, and define the requirements for operational framework suitable for Trust Relationship Management for SDN integrated environment.

1.2. Document Outline

Section 2 of this document introduces the basic terminologies that are used in context of PKI as well as SDN Technologies. Section 3 outlines the prime challenges to establish Trust Architecture in SDN integrated environment. Section 4 establishes the building blocks of the PKI based Security Architecture for SDN integrated environment. Section 5 considers different design patterns of Continuous Trust Models as can be implemented in different deployment scenarios. Section 6 considers design patterns of Discontinuous Trust Model as integration approach for dis-joint trust relationships. Section 7 summarizes the considerations for integrated operational framework for Trust Relationship Management, as perceived required for SDN Security Architecture. Section 8 lists down the References for this draft.

2. Basic Terminologies

2.1 Basic PKI Terminologies

The following terms are used throughout this document. Where possible, definitions found in RFC 4949 [RFC4949] and RFC 5217 [RFC5217] have been used.

Public Key Infrastructure (PKI): A system of CAs that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography and share trust relationships, operate under the same Certificate Policy Document specifying a shared set of Policy OID(s), and are either operated by a single organization or under the direction of a single organization.

PKI domain: A set of two or more PKIs that have chosen to enter into trust relationships with each other through the use of cross-certificates. Each PKI that has entered into the PKI domain is considered a member of that PKI domain.

Certificate: A digitally signed data structure that attests to the binding of a system entity’s identity to a public key value (based on the definition of public key certificate in RFC 4949 [RFC4949]).
Certification Authority (CA): An entity that issues certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate (RFC 4949 [RFC4949]).

End Entity (EE): A system entity that is the subject of a certificate and that is using, or is permitted and able to use, the matching private key only for a purpose or purposes other than signing a certificate; i.e., an entity that is not a CA (RFC 4949 [RFC4949]).

Relying party: A system entity that depends on the validity of information (such as another entity’s public key value) provided by a certificate (from the RFC 4949 [RFC4949] definition of certificate user).

Root CA: A CA that is at the top of a hierarchy, and itself should not issue certificates to end entities (except those required for its own operation) but issues subordinate CA certificates to one or more CAs.

Subordinate CA: A CA whose public key certificate is issued by another superior CA, and it itself must not be used as a trust anchor CA.

Principal CA (PCA): A CA that should have a self-signed certificate is designated as the CA that will issue cross-certificates to Principal CAs in other PKIs, and may be the subject of cross-certificates issued by Principal CAs in other PKIs.

Trust anchor CA: The trust anchor CA for an end entity is usually the CA that issued the end entity’s certificate. The trust anchor CA must be the CA that has a self-signed certificate.

Unifying CA: A CA that is at the top of a hierarchy, and itself should not issue certificates to end entities (except those required for its own operation) but establishes unilateral cross-certification with other CAs. A Unifying CA must permit CAs to which it issues cross-certificates to have self-signed certificates.

Bridge CA: A CA that, itself, does not issue certificates to end entities (except those required for its own operation) but establishes unilateral or bilateral cross-certification with other CAs.

Certification Path: An ordered sequence of certificates where the subject of each certificate in the path is the issuer of the next certificate in the path. A certification path begins with a trust anchor certificate and ends with an end entity certificate.

2.2 Basic SDN Terminologies

The following terms are used throughout this document. Where possible, definitions found in "SDN Layers and Architecture Terminology" draft of SDNRG Research Group have been used.
Software Defined Network (SDN): A programmable networks approach that supports the separation of Control and Forwarding Planes via standardized interfaces.

SDN-security Domain: Within an integrated SDN infrastructure, each subset of infrastructure that contains independent setup of PKI will be considered as separate SDN-security Domains. An SDN-security domain is thus same as a PKI Domain if considered in the scope of PKI implementation in SDN Infrastructure. In case a subset of SDN infrastructure adopts PKI implementation, while other subset leverages non-PKI infrastructure, each subset of SDN Infrastructure will be considered as separate SDN-security Domain.

Device: A device that performs one or more network operations related to packet manipulation and forwarding. This reference model makes no distinction whether a network device is physical or virtual. A device can also be considered as a container for resources and can be a resource in itself.

Application (App): A piece of software that utilizes underlying services to perform a function. Application operation can be parameterized, for example by passing certain arguments at call time, but it is meant to be a standalone piece of software; an App does not offer any interfaces to other applications or services.

Service: A piece of software that performs one or more functions and provides one or more APIs to applications or other services of the same or different layers to make use of said functions and returns one or more results. Services can be combined with other services, or called in a certain serialized manner, to create a new service.

SDN Element: SDN Element is a generic reference of either a Device or Application or Service as deployed in a Software Defined Network.

Forwarding Plane (FP): The network device part responsible for forwarding traffic.

Control Plane (CP): Part of the network functionality that is assigned to control one or more network devices. CP instructs network devices with respect to how to treat and forward packets. The control plane interacts primarily with the forwarding plane and less with the operational plane.

Management Plane (MP): Part of the network functionality responsible for monitoring, configuring and maintaining one or more network devices. The management plane is mostly related with the operational aspect and less with the forwarding plane.
3. Prime Considerations for Establishing Trust in Integrated SDN Environment

The SDN Transformation in Operator’s environment is intended to bring newer services, with launch cycles faster than ever before. Such service roll-out capabilities are enabled by the SDN centralized control layer, and the ability to host application layer on top. One of the critical success factors is the robustness of security infrastructure as can be designed, to support the SDN integrated network architecture.

The Security Architecture for SDN requires dealing with the following crucial aspects.

3.1 Multi-Party Diversities
In a simplistic representation, the Elements and the Controllers are envisioned as the resources owned by Network Provider, the SDN applications running on top of the controllers could be deployed as internal or external applications deployed by 3rd party Application Providers. And the services of the applications and network will need to be extended to Customer Enterprises, making the Enterprise network environment seamlessly integrated. This essentially creates the demand of multi-party environment where each stakeholder’s part of the environment can be logically separate, and under the purview of independent organization.

The actual business environment can have different Infrastructure Providers and Network Function Providers augmenting to Network Provider’s environment. And multiple levels of tenancy models may need to be provisioned to support the particular business aligned implementation. This essentially increases the complexity of setting up secured interoperable environment, since different organizations follow different security policy and practices, and complexities to maintain a coherent design for interoperable trust become proportional to the level of diversities.

3.2 Trust Model in Multi-Domain Diversities

Each organization’s security policies and practices are generally supported by deploying its own security infrastructure. Within an integrated SDN infrastructure, each subset of infrastructure that contains independent setup of security / PKI infrastructure will be considered as separate security domain. Thus, every organization will generally have one or more security domains. In addition, IT administration practices in organization prefer creating multiple domains even inside single organization’s infrastructure to address complex deployment requirements. For example, security requirements for Access Network and Data Center can be very different, and similar diversification of security requirements may be required in different countries depending on laws of the land, if Network Provider’s environment span across multiple such geographies. Now, while the Network Provider’s infrastructure evolve towards being SDN Enabled, the requirements for establishing interoperable trust rise to greater magnitude due to SDN’s focus on establishing interoperable multi-domain environment.
3.3 Layer of Security Enforcement

An integrated SDN environment will have multiple applications requiring supporting diverse transport technologies (such as PBB, MPLS, VxLAN, NvGRE etc.). A secure and ubiquitous SDN transport fabric would thus need to comply with the service continuity and connectivity requirements of such integrated SDN environment. On the other hand, the choice of application layer protocols for SDN control plane have become diversified as well. OpenFlow being one of the primary preferences, other protocols are also being leveraged to meet the requirements of control plane separation in SDN environment. Thus, the Trust Architecture shall not get tightly coupled with any particular Application Layer Protocol or Transport Technologies. In addition, in certain scenarios an overlay network may also be designed by the SDN Applications, which can contain its own security infrastructure in the application purview. In such cases, trust establishment methods in underlaying SDN network shall not interfere with security requirements of the overlaying network. Thus, security enforcement method selected at the SDN transport fabric shall interoperate seamlessly with various deployment scenarios of integrated SDN Environment.

3.4 Need for Integrated Operational Framework

Multi-party involvement, and inclusion of multiple security domains, increases the operational complexity of SDN Security infrastructure. Technology options exercised in different stakeholders’ PKI infrastructure can vary significantly for PKI operations and management, leading to complex interoperability requirements. Specifically, the variations in Identity Metadata, Certification metadata, policy attributes, constraints, and certification status attributes from one SDN-security domain to another significantly impact the Trust Relationship Management across SDN-security domains. Thus, setting up a framework appears necessary to manage the complex interoperability requirements through set of processes, practice and tool.

The integrated point of presence however shall not introduce a single point of attack or single point of failure, and the design needs to be carefully considered to ensure this. Thus, the integration may not necessarily result into a centralized application for operations, instead, can be an aggregation of distributive set of applications, processes, and practice to establish seamless functioning over multi-party, multi-domain security operations.

4. SDN Trust Architecture - Building Blocks

There are certain building-blocks for setting up PKI based Trust Architecture in the integrated SDN environment, and these building blocks mostly will remain unchanged despite of variations in deployment scenarios. This section of the document summarizes these building blocks, as followed -
For operational and business purposes, integrated SDN environment should be subdivided into separate SDN-security domains each with specific business scope and administration scope. While these domains can be owned by Application Providers, Network Provider and Customer Enterprises, a generic representation of these domains have been considered here onwards to achieve a business-independent and technology-aligned analysis stand-point. To enable this, let’s assume an integrated SDN Environment S that comprises of all Elements required for setting up SDN aligned Network, Hosted SDN Applications, and Integration with Subscriber Enterprises. The Integrated SDN Environment S thus assumed to be divided into multiple SDN-security domains { S1, S2, S3, ....... Sn}. Each of these domains may contain an arbitrary number of controllers, switches and other SDN enabling Elements.

b) It is recommended that each individual SDN-security domain S1, S2, S3, ...... Sn must have their own PKI infrastructure. If one or more of the domains doesn’t conform to this, an integration approach with Discontinuous Trust Model shall be worked out for interoperating PKI based domains with security mechanisms available for non-PKI based domains.

c) Within an individual SDN-security domain, a specific number of trust authorities can be deployed. The responsibilities of these trust authorities would be to grant/revoke/maintain X.509 PKI certificates.

d) In order for the PKI of a SDN-security domain to participate in one or more PKI of SDN-security domains, that PKI must have the A Certificate Policy Document documenting the requirements for operation of that PKI. The Certificate Policy Document should be in RFC 3647 [RFC3647] format. In addition, the PKI of particular SDN-security domain shall also have a defined Principal CA, and One or more Policy OIDs defined in the Certificate Policy Document shall be asserted in all certificates issued by that PKI.

e) TLS can be considered as the preferred layer for Trust Enforcement and recent versions of TLS (TLS 1.1, TLS 1.2) implementations shall be leveraged.

f) Within an SDN-security domain, it is recommended to have logical representation of TLS Client CA and TLS Server CA, dedicated for role specific certificate issuance. The TLS Client CA of the domain should issue certificates to the TLS clients of the domain, which will need to establish TLS connection with other TLS servers in the same or different domain. The TLS server CA of the domain shall issue certificates to the TLS servers of the domain, which will need to establish TLS connection with the TLS clients in the same domain or different domain.

g) An SDN-security domain may choose to combine two or more of the CAs. For example, the same CA may be used to issue TLS client & TLS server certificate both or both-end entity TLS and IPSec certificates. Furthermore, the same CA may be used to issue both-end
entity certificates, and cross certificates as well depending on the nature of deployment.
5. Continuous Multi-Domain Trust Model

The integrated trust models have certain common patterns while being used in continuous chain of trust, some of these important patterns were described in prior art RFC 5217 [Memorandum for Multi-Domain Public Key Infrastructure Interoperability]. This section thus identifies some of these patterns, and suggests deployment scenarios in which the specific pattern of implementation will suit the most for SDN integrated environment. Presumably, each of the Trust Model will require to be adopted while supporting diverse deployment requirements in a particular SDN Environment, and this essentially will steer the infrastructure to adopt an overall hybrid model of trust architecture. However, this draft focuses on establishing the design viability of the fundamental trust models, and thus limits the discussion on Bridge Model, Direct Cross-Certification and Unifying Domain Model only.

5.1 SDN Multi-Domain Bridge Model

This is the first model which can be leveraged in SDN multi-party and multi-domain architecture.

In this model, every SDN-security domain trusts each other by cross-certification through a Bridge CA, as shown in Figure below. The trust relationship is not established between a subscriber domain and a relying-party domain directly, but established from the Principal CA of the relying-party’s domain via a Bridge CA.

Following are certain deployment scenarios and specific implementation considerations for this Trust Model -

a) If an SDN Application Provider and particular Customer Enterprise don’t have direct business relationship, however requires establishing Trust Relationship due to nature of SDN Application’s integration requirements, adopting Bridge Model can be considered as a viable solution. The Bridge CA can be hosted in Network Provider’s environment, and can be leveraged by both Application Provider and Enterprise to set up cross-domain trust relationship. Typically a mid-size to large organization, either Application Provider or Customer Enterprise, can have multiple CAs in their internal security infrastructure, setting up a BCA to cross-certify multiple CAs of each organization will make the implementation much modular and manageable.

b) If the security policies for Customer Enterprise and Network Provider require detailed policy mapping and constraint management for cross-certification, an operationally effective approach would be to address the cross-domain trust requirements by setting up dedicated Bridge CA. This approach helps centralizing the policy mapping into the Bridge CA Servers only, and in turn reduces the operational overhead.
c) For the same reason as mentioned above, if the security policies for SDN Application Provider and Network Provider requires detailed policy mapping for cross-certification, dedicated Bridge CA setup should be leveraged.

![Diagram of Bridge Model]

**Figure 5: Bridge Model**

PCA - Principal Certificate Authority.
BCA - Bridge Certificate Authority.
CA - Certificate Authority
EE - End Entities (Applications/Controllers/Switches)

### 5.2 SDN Multi-Domain Direct Cross Certification Model

This is the second model which can be used in SDN multi-domain architecture.

In this model, each PKI domain trusts each other by issuing a cross-certificate directly between each Principal CA, as shown in the figure below. This model shortens the certification path between the SDN-security domains and establishes a trust relationship expeditiously.
Following are certain deployment scenarios and specific implementation considerations for this Trust Model:

a) This model offers a flexible deployment provision if two different SDN-security domains of the Network Provider’s infrastructure requires a cross-domain trust provision while the infrastructure evolve towards SDN enabled infrastructure.

b) A SDN-security domain in this model needs to take into account that the other SDN-security domain may cross-certify with any other SDN-security domains. If a particular SDN-security domain requires restricting a certification path, it should not rely on the validation policy of the relying party, but should include the constraints in the cross-certificate explicitly.

c) Considering the performance requirements of SDN enabled carrier network, reducing the number of CAs appearing in a certification path validation will directly impact the performance and response time of authentication. This model thus offers a performance friendly approach for cross-domain certification. While designing the cross-certification for Network Provider and Application Provider or Customer Enterprise, if the number of SDN-security domains require to interoperate from both sides are not many, direct peer to peer cross-certification between all possible combination of CAs from both the organization will offer a performance optimized architecture. However, managing the policy-mapping and constraints across all combinations of cross-certified SDN-security domains of both organizations will add operational overhead. Thus, the design shall be carefully considered based on amount of cross-domain certifications requirements and number of SDN-security domains involved.

```
+---------------+     +------------------------+
|  SDN-sec      | cross-certified |       SDN-sec          |
|  domain 1     |    each other   |       domain 2         |
|      +-----+ --------------------> +-----+ <-+ |
|      | PCA |  |                 |  | PCA |     |         |
|      +-----+ <-------------------- +-----+ <-+ |         |
|         |     |                 |     ^      | v         |
|         |     |                 |     |    +----+        |
|         |     |                 |     |    | CA |---+    |
|         |     |                 |     |    +----+   |    |
|         v     |                 |     v       v     v    |
|       +----+  |                 |   +----+ +----+ +----+ |
|   +---| CA |  |                 |   | CA |--+ |     |    |
|   |   +----+  |                 |   +----+ +----+ +----+ |
|   |      |    |                 |     |       |     |    |
|   v      v    |                 |     v       v     v    |
| +----+ +----+ |                 |   +----+ +----+ +----+ |
| | EE | | EE | |                 |   | EE | | EE | | EE | |
| +----+ +----+ |                 |   +----+ +----+ +----+ |
```

Figure 6: Direct Cross-Certification Model

PCA - Principal Certificate Authority.
5.3 SDN Unifying Domain Model

This is another Trust model discussed in the context which can be applied to a SDN-security domain. In this Unifying Trust Model, a SDN-security domain is created by establishing a joint, superior CA that issues unilateral cross-certificates to each SDN-security domain, as shown in following Figure. Such a joint, superior CA is defined as a Unifying CA, and the Principal CAs in each SDN-security domain have the hierarchical CA relationship with that Unifying CA. In this model, any relying party from any of the SDN-security domains must specify the Unifying CA as its trust anchor CA, in order to validate a subscriber of other SDN-security domains. If the relying party does not desire to validate subscribers of other SDN-security domains, the relying party may continue to use the Principal CA from its own SDN-security domain as its trust anchor CA.

Following are certain deployment scenarios and specific implementation considerations for this Trust Model -

a) If existing security specific domains in Network Provider’s infrastructure are not maintaining trust relationship yet, and SDN enablement is driving towards a re-designing effort, it’s worthwhile to consider establishing a hierarchical model of trust through Unifying Domain model for the relevant part of the infrastructure. This essentially provides a defined structure for establishing trust model for the relevant SDN-security domains that can fit well into the scheme. However, a careful consideration will be required to identify the particular SDN-security domains that can integrate seamlessly into this, as the model reduces the implementation flexibility by letting the Root CA to govern the security policies.

b) This model enforces the Root CA to have direct control over the subordinate CAs. Thus, if a Customer Enterprise or SDN Application Provider utilizes Network Provider’s hosted infrastructure and follows Network Provider’s security policy, unifying domain model can be leveraged for that part of the infrastructure. This approach can help maintaining the SDN-security domain for business level differentiations but can govern the trust establishment through a strictly defined structure.
Figure 7: Unifying Trust Point (Unifying Domain) Model

PCA - Principal Certificate Authority.
CA  - Certificate Authority
EE  - End Entities (Applications/Controllers/Switches)

6. Discontinuous trust model

From Architectural stand point, discontinuous trust model is not preferred over Continuous Trust Model, however certain interoperability requirements arising from business and operational perspective drive the architecture to adopt this approach. In a discontinuous trust model, like a 3-leg or 2-leg authentication model, there can be SDN-security domains which are independent of each other and show no mutual Trust relationship. In such case, the PKI infrastructure within each of the domains will need to be independent of one another. In certain other scenarios, one particular domain can have PKI infrastructure while the other can have completely different non-PKI based security infrastructure, and thus showing no trust relationship.
Following are some of the deployment scenarios where such approaches may need to be adopted -

(i) Certain SDN-Security Domain(s) owned by Application Provider or Customer Enterprise don’t require to maintain continuous certification path with Network Provider’s SDN-Security domains - such deployment may be preferred for loose coupled integration and/or ad-hoc integration for multi-party infrastructure

(ii) Overlaying application network requires implementing non-PKI security infrastructure but underlying SDN Transport adopts PKI Infrastructure

6.1 SDN-security domains with independent PKI infrastructure

The trust list model design [RFC 5217] can be leveraged in a discontinuous PKI setup for the above mentioned scenario (i). Trust across multiple disjoint SDN-security domains can be created by maintaining locally configured list of trust anchors within each specific SDN-security domains, or by maintaining the trust list entities external to the SDN-security domains. This configured lists known as trust lists contain a set of one or more trust anchors or Certificate Authorities. Such a trust list contains one or more trust anchors used by a relying party OR the end entities to explicitly trust one or more SDN-security domain.

The discontinuous trust model assumes that each independent SDN-security domain contains a local certificate authority (CA) Or Trust Anchor which would grant certificates to the End Entities. It also assumes that the CA Or Trust Anchor would possess a self-signed CA certificate which would be used to sign and generate the end entity Certificate Signing Request (CSR) and Certificate respectively.

The following Figure 4 shows how two different SDN-security domains will discretely interoperate while leveraging the trust list model. The relying party would thus trust the Trust Anchors present in the trust list. As shown in the below diagram, the End Entity EE1 within SDN security domain 1, would trust the Certificates granted by Trust Anchor 1 and Trust Anchor 2. This would mean that EE1 of SDN-security domain 1 would trust the Trust Anchor 2 and EE2 of SDN-security domain 2 would trust the Trust Anchor 1, thus extending the trust across multiple disjoint/discontinuous SDN-security domains. In this type of model, end entities belonging to different and disjoint SDN-security domains cannot go through actual and explicit authentication exchanges due to the unavailability of direct certification path, but obtains implicit trust relationship by depending on the Trust List configurations.
i) Disjoint/independent SDN-security domains

ii) Trust List maintained by EE1 (SDN-security domain S1)

iii) Trust List maintained by EE2 (SDN-security domain S2)
6.2 Discontinuous SDN-security domains with varying Security Infrastructure

In certain type of deployments, SDN Applications will impose an overlaying network on top of underlying software defined network infrastructure, as described above as Scenario (ii). In such scenarios, SDN Application Infrastructure can maintain separate security infrastructure while underlying transport fabric will maintain its own security infrastructure. This draft considers this variation manageable if underlying transport maintains PKI based Security Infrastructure and non-PKI security infrastructure associated to overlaying application network subscribes to underlying SDN-security domain for the necessary interconnection part. The document doesn’t suggest any other method to make PKI based SDN-security domain interoperate with non-PKI security infrastructure associated to overlaid networks.

7. Integrated Operational Framework for Trust Relationship Management

Continuous and discontinuous trust models across multi-party and multi-domain environment drive the requirements for setting up an integrated operational framework for Trust Relationship Management. Applications developed on top of SDN integrated network requires this framework to be seamlessly interoperable across multi-party environment to facilitate on demand application delivery. In many cases, SDN Applications developed by multiple Providers, and hosted by Network Provider, will essentially be consumed by Customer Enterprises or individual subscribers at real time or near real time and on-demand. Application delivery will thus require maintaining an automated workflow for order management, fulfillment and assurance. While Trust Relationship Management activities are typically kept outside of such automated workflow, the integrated operational framework should offer provisions to make this demand driven. Thus, certain characteristics of the integrated operational framework were identified and described as followed.

(i) All parties and their SDN-security domains require to be logically modelled in hierarchical topology within the integrated operational framework to identify all on-boarded stakeholders of the Ecosystem and Customers. The hierarchical topology should also clarify the zoned security models as implemented and overlapped to the specific parts of the integrated topology.
(ii) Each stakeholder logically modelled in this framework requires to be associated to an asset repository containing the published security practice statement and policy statements on trust interoperability. The users of the framework should be able to lookup the assets corresponding to particular stakeholder.

(iii) The integrated framework should maintain pre-identified policy mapping provisions across all possible SDN-security domains, for the cases:
   (a) where the policy mapping configurations were applied to establish a trust relationship
   (b) where the policy mapping configurations are not yet applied as no trust relationship modelling requirement has been identified yet

(iv) For established trust relationship, the integrated framework requires to model the relationship in the hierarchical topology across the specific combinations of SDN-security domains. The relationship needs to be recognizable from the framework and further lookup should be possible to acquire more information on enforced policies.

(v) The integrated framework requires providing option to update existing set of policies already enforced over the specific SDN-security domains, which are engaged in particular trust relationship. The update operation should carry out making necessary changes with immediate effect.

(vi) To support dynamic application delivery requirements, on-demand Application subscription request should be entertained by setting up the underlying Trust relationship. Pre-identified policy mapping configurations across the participating SDN-security domains should be applied on demand to set this up.

(vii) On demand extension of certificate chain should be supported for on-demand modifications of application delivery requirements. In certain cases, if SDN Application delivery environment requires increased coverage by introducing more SDN-security domains into the application delivery network, the certificate chains need to be extended accordingly. This requires modifying the existing trust relationship as well as provisioning new trust relationship as per the requirements of extended certification path. The integrated framework should be able to offer these provisions.

(viii) For every trust relationship established and modelled in the integrated framework, the constraints on the specific certificate path should be explicitly configured through the framework. The framework should offer Constraint Management capabilities for representation of the constraints in the hierarchical topology, ability to establish, modify and remove these constraints across certification paths.

(ix) Integrated Constraint Management capability in the framework should be devised for real-time manageability over activation and de-activation of particular certificate path.
For on-demand un-subscription of applications or services, the integrated framework requires to remove the existing trust relationship configurations across participating SDN-security domains. The removal process shall be carefully designed so that certificate path used for other application delivery context shall not get impacted by this.

The integrated framework requires providing the manageability over Trust Lists configured for supporting discontinuous trust relations. The hierarchical topology in the integrated framework should model the discontinuous trust relationships as well. The Trust List details should be retrievable corresponding to the particular relation.

The integrated Framework may also maintain references of further applications and processes that are used in the scope of SDN-security domains for PKI Infrastructure specific operations and management. Such operations and management may include Certificate Management, Key Management, Certification Status & CRL Management, Certificate Delivery Management and other related aspects.

While an integrated operational framework for Trust Relationship Management can consist a distributive set of applications / tools, processes, Policies, and Practice Statements, the integrated abstraction of such framework should offer an end to end span of control for managing the Trust Relationships. Above mentioned suggested characteristics for managing the relationships were considered in the context of such end to end span of control, while keeping the alignment to the evolving needs of SDN integrated environment. However, the draft doesn’t claim these to be the sole considerations for setting up an extensive integrated framework for managing multi-party, multi-domain trust relationship.
8. References

1) RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

2) RFC 5217 "Memorandum for Multi-Domain Public Key Infrastructure Interoperability"

3) RFC 6402 "Certificate Management over CMS (CMC) Updates"

4) RFC 7030 "Enrollment over Secure Transport"

5) RFC 4778 "Operational Security Current Practices in Internet Service Provider Environments"

6) RFC 7426 "Software-Defined Networking (SDN): Layers and Architecture Terminology"

7) draft-mrw-sdnsec-openflow-analysis-02 "Security Analysis of the Open Networking Foundation (ONF) OpenFlow Switch Specification"

8) draft-sin-sdnrg-sdn-approach-01 "Software-Defined Networking: A Service Provider’s Perspective"

9) NFV Security Problem Statement, ETSI NFV ISG

Authors’ Addresses

Saurabh Chattopadhyay
Noida, India
Email: saurabhchattopadhyay@hcl.com

Kaushik Datta
Bangalore, India
Email: Kaushik.Datta@hcl.com