SDNRG
Internet-Draft
Intended status: Informational
Expires: September 25, 2016

Saurabh Chattopadhyay
HCL Technologies
Kaushik Datta
HCL Technologies
March 21, 2016

Multi-party Multi-Domain Trust Architecture Recommendations for SDN Deployment in Carrier Network

draft-chattopadhyay-sdnrg-multi-party-sdn-trust-02

Abstract

This draft analyzes the complexities involved in setting up the certification infrastructure for multi-tenant, multi-domain SDN adopted network environment. There are certain architectural options available to address these complexities, and the same have been consolidated and analyzed in the draft. However, there are certain implementation level challenges that create difficulties to operationalize these options. And these challenges have been recognized in the draft and further translated into requirements for setting up an operational framework suitable for managing certificate chains for SDN integrated environment. Finally, a next level of assessment has been carried out to consolidate contemporary work happening in different Work Groups and their likely coverage over identified operational framework requirements.

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 September 25, 2016.

Table of Contents

1. Introduction

1.1. Overview

Adoption of SDN transforms certain inherent characteristics of traditional carrier network. The newer network architecture invites more stakeholders to the networking ecosystem, and this introduces multi-tenant mode of working with resources shared across different tenants. Sharing of resources is driven from the distributed autonomous control functions located at logically centralized and federated Controller plane. And this Controller plane further enables developing innovative applications and services on top of this network architecture, which essentially creates the demand for supporting application subscription specific or network subscription specific multi-tenancy at the converged infrastructure.
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 authentication and certification 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. Thus, this document consolidates relevant Security Practices, Framework, and Guidelines for establishing PKI based authentication in SDN adopted network architecture. Some of these Framework and Guidelines may not have been used significantly in current network deployment, since multi-tenancy and resource sharing complexities for network have not been this much critical so far. Thus, it appears necessary to re-evaluate the feasibility of implementing some of these not-so-commonly used Frameworks, and to identify the need for further improvisations required over these existing standard, practices and frameworks.
Towards this, the document limits its scope to analyze the authentication requirements supported by PKI based Certification Infrastructure, and identify the requirements for an operational framework that can ease the overhead of Certification Chain Management for SDN adopted network environment.

1.2. Document Outline

Section 2 of this draft introduces the basic terminologies that are used in context of PKI as well as SDN Technologies. Section 3 outlines the prime requirements to improvise Authentication & underlying Certification methods in SDN adopted environment. Section 4, 5, and 6 subsequently evaluate different architectural options that can be adopted to meet the requirements described in Section 3, and attempts to identify the bottlenecks to operationalize these in Operator's environment. Section 4 specifically defines the common building blocks of PKIX based Certification Architecture over which further assessment of different certificate chaining models are carried out. Section 5 considers different options for Continuous Certificate Chaining, and Section 6 considers options for Discontinuous Certificate Chaining. Section 7 summarizes the considerations for integrated operational framework for Certification Chain Management, as evolved while assessing the operational complexities of different models. These considerations are perceived as the newer set of requirements; need to be addressed to reduce the overhead of operationalizing the certificate chaining models for supporting multi-tenancy and resource sharing complexities. Section 8 evaluates some of the contemporary work being carried out in different IETF WGs and attempt to establish if part or whole of the work can be leveraged towards meeting the operational framework requirements. Section 9 lists down the References for this draft.

2. Basic Terminologies

2.1 Basic PKI Terminologies

The following terms are used throughout this draft. Where possible, definitions found in [RFC4949] and [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 [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 [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 [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 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 draft. Where possible, definitions found in "SDN Layers and Architecture Terminology" draft of SDNRG Research Group has 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 Requirements for Setting up Authentication Infrastructure in SDN adopted Environment

SDN Transformation in Operator's environment is targeted to introduce newer services with reduced time to roll-out. Such service roll-out capabilities are enabled by the SDN centralized control layer, and the ability to ingest applications on top. One of the critical success factors is the robustness of authentication infrastructure as can be designed, to deal with multi-tenancy and resource sharing complexities in SDN integrated environment.

Following aspects have critical influence over the robustness of authentication infrastructure, as elaborated in sub-sections below.

3.1 Identity Declaration and Certification Scenarios in Multi-Tenant SDN Environment

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 for Customer Enterprises, making the Enterprise network environment seamlessly integrated. This essentially creates the demand for 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.

Following scenarios describe the identity declaration, certification and authentication requirements arising from certain types of multi-tenancy scenarios.

- An Application Subscriber requires to access Resources hosted by Network Provider on behalf of Application Provider

This scenario is similar to hosting the applications in public cloud environment. In this scenario, the Resource requires to prove its

identity to Application Subscriber by presenting its PKIX Certificate [RFC5280], declaring itself belonging to the domain of Application Provider. However, originally it belongs to the Network Provider, thus a Continuous Chaining or similar mechanism needs to be established between the Network Provider and Application Provider to certify the ownership of this particular resource.

In absence of continuous chaining provision, the PKIX certificate can still show the Resource belonging to Network Provider domain and being used by Application Provider, while Application Subscriber can manually pin this to trust as a measure of discontinuous certificate chaining. Once the mechanism is in place, Application Subscriber can check the validity of the Certificate as per the rules defined in [RFC6125]. And upon successful validation, the authentication can be carried out seamlessly.
The UTA WG has been actively developing number of specifications for standardizing the use of TLS corresponding to different application layer protocols, and also covering this kind of scenarios for multi-tenant mode of operation. [RFC7590] is an example of one such RFC that suggests the protocol specific use of TLS for XMPP in this type of multi-tenant environment.

- A Network Subscriber requires accessing Resources hosted by Application Provider on behalf of Network Provider

In certain type of deployment, the resource to be used by Network Subscriber may be provided on Network Provider's behalf but can actually belong to the Application Provider. Thus, the PKIX Certificate of the Resource will have to declare the Resource being part of Network Provider domain, and this will demand certain kind of certification chaining between Application Provider and Network Provider for this particular resource.

- An Application Subscriber requires to access combination of Resources hosted by Network Provider and Customer Enterprise on behalf of Application Provider

In certain type of deployment, the Resource being provided to Application Subscriber may be co-owned by Customer Enterprise and Network Provider, but being offered to Application Subscriber on behalf of Application Provider. Now, depending on the business agreements between the parties, this deployment may require different type of certificate chaining provisions to certify the ownership of the Resource under Application Provider domain. In extreme cases, if the part of the Resource contributed by Customer Enterprise is treated as part of Network Provider's environment, the chaining of certificates for the particular resource may require tri-party involvement.

- A Network Subscriber requires to access combination of resources hosted by Application Provider and Customer Enterprise on behalf of Network Provider

Similar to above scenario, the certification of the Resource belonging to Network Provider domain may require multi-party involvement depending on nature of business agreements among the

concerned parties.

3.2 Multi-Domain Certification Policy Diversities

Each stakeholder'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 certification / PKI infrastructure will need to be considered as separate security domain. Thus, every stakeholder 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 certificate management method rises 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 require 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.
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's purview. In such cases, authentication methods in underlying SDN network shall not interfere with authentication requirements of the overlaying network.
Thus, authentication method selected at the SDN transport fabric shall interoperate seamlessly with various deployment scenarios of integrated SDN Environment.

4. SDN aligned Certification Architecture - Building Blocks

As a next step, the draft evaluates different types of certification architecture that can potentially be leveraged for SDN Integrated environment, and also assess the operational flexibilities required to enable easy realization of these architectures in carrier grade

environment.
Towards this, there are certain building-blocks for setting up PKIX based Architecture in the integrated SDN environment, and these building blocks can mostly remain unchanged despite of variations in different deployment scenarios considered. This section of the draft summarizes these building blocks, as followed -

(a) For operational and business purposes, integrated SDN environment can be considered 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 Customer 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 assumed that each individual SDN-security domain S1, S2, S3, ... Sn will typically have their own PKIX infrastructure. In certain scenarios, if one or more of the domains doesn't conform to this, the analysis approach will consider integration through Discontinuous Chaining Model to interoperate PKIX based domains with non-PKI based domains.

c) Within an SDN-security domain, it is assumed that logical representation of TLS Client CA and TLS Server CA will be present, and will be 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, which will need to establish TLS connection with the TLS clients in the same or different domain.

d) It is assumed that 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 Certificate Chaining

Continuous Certificate Chaining models have certain common patterns while being used in continuous chain of trust, and these patterns are described in [RFC5217]. This section identifies the benefits of the specific model while implemented in SDN integrated environment, and also the associated challenges that will need to be addressed separately. Presumably, each of the Models will offer certain benefits against others in certain deployment scenarios, and this

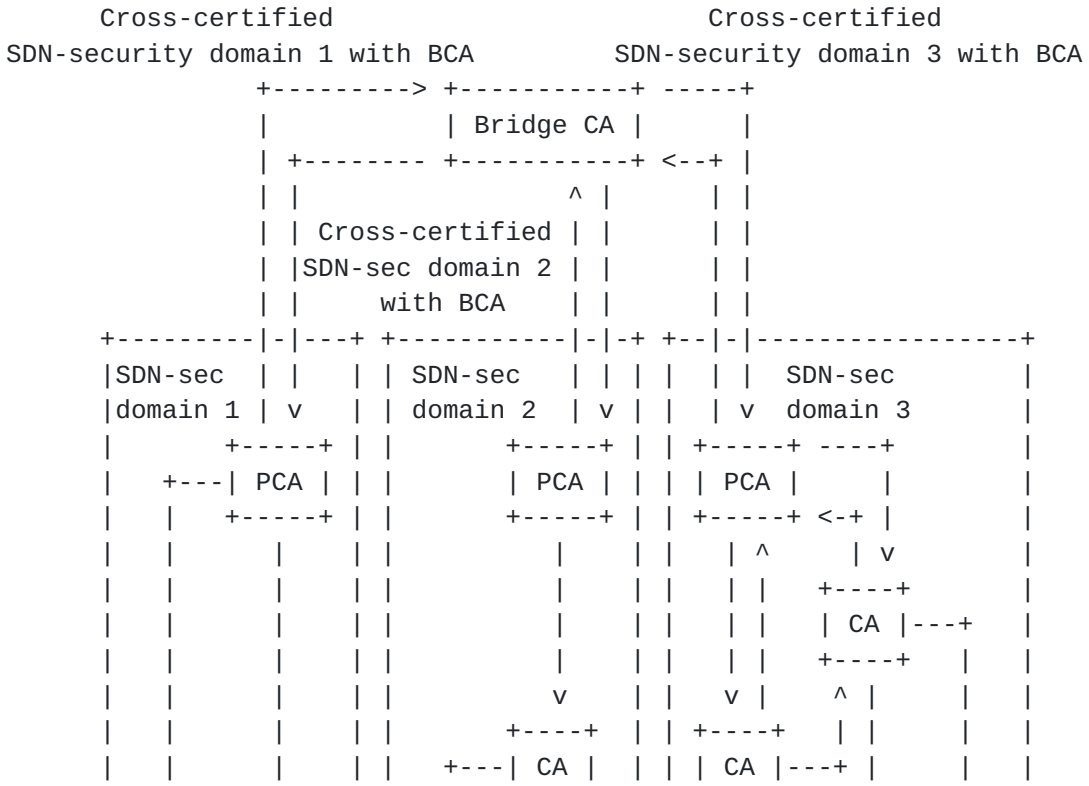
essentially will steer the infrastructure to adopt an overall hybrid model. However, the challenges in establishing such hybrid environment will need to be addressed as well, and the following section attempts to capture that.

5.1 SDN Multi-Domain Bridge Model

In this model, every SDN-security domain develops the trust relationship by cross-certifying through a Bridge CA, as shown in Figure below.
The relationship does not get 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 benefits and specific implementation level challenges, as evaluated -

a) Setting up a BCA to cross-certify multiple CAs of multiple organizations will make the implementation much modular and better manageable in the long term.
b) Establishing the certification chain through BCA typically increases the deployment time significantly, unless a pre-provisioned automation framework is in place for on-demand policy mapping and BCA is locally hosted.
c) Setting up a local BCA will incur significant management overhead
d) 3rd party BCA will typically narrow down the possibilities of multi-party involvements since affiliation of all parties to the BCA becomes a mandatory requirement
e) BCA based implementations increases the certification cost, and involves careful liability management.



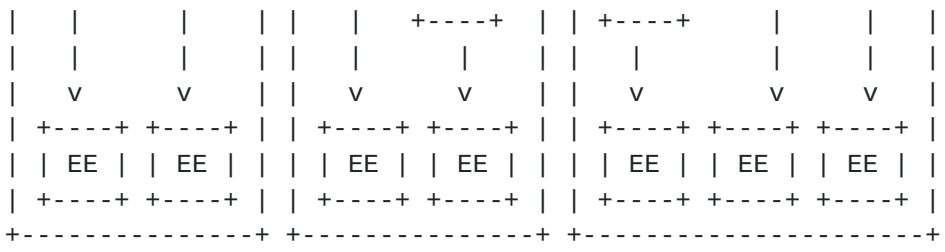


Figure 5: Bridge Model

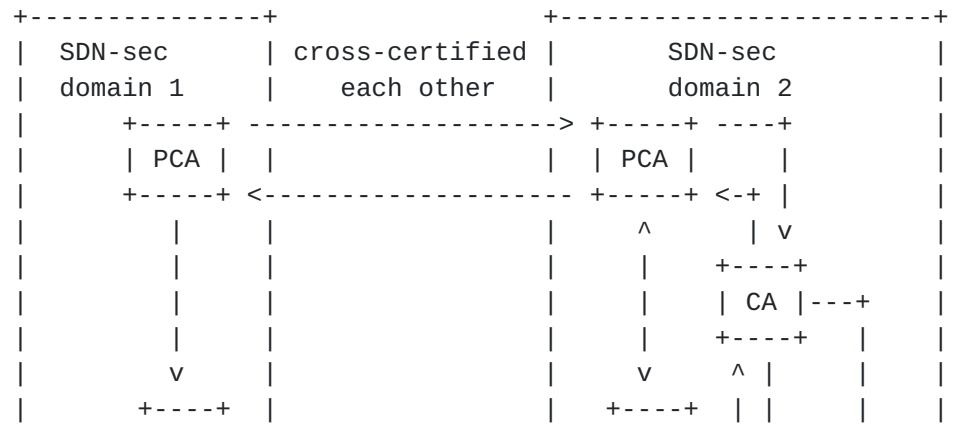
PCA - Principal Certificate Authority.
BCA - Bridge Certificate Authority.
CA - Certificate Authority
EE - End Entities (Applications/Controllers/Switches)

5.2 SDN Multi-Domain Direct Cross Certification

In this model, each SDN-Security domain certifies 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.

Following are certain benefits and specific implementation level challenges, as evaluated -

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) This model reduces the time to deployment as well as cost of certification
c) Reducing the hops in a certification path validation directly improves the performance and response time of authentication
d) Architecturally this model is not very robust in terms of modularity and long term manageability. For example, 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 particular certification path, it should not rely on the validation policy of the relying party, but should include the constraints in the cross-certificate explicitly.
e) Managing the policy-mapping and constraints across all combinations of cross-certified SDN-security domains will add operational overhead, unless a framework is in place to manage this effectively.



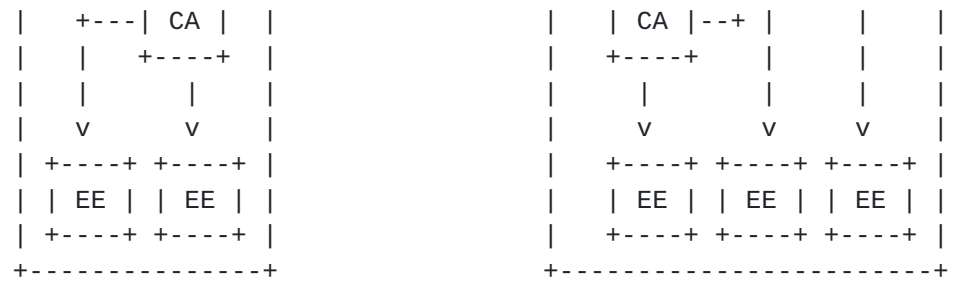


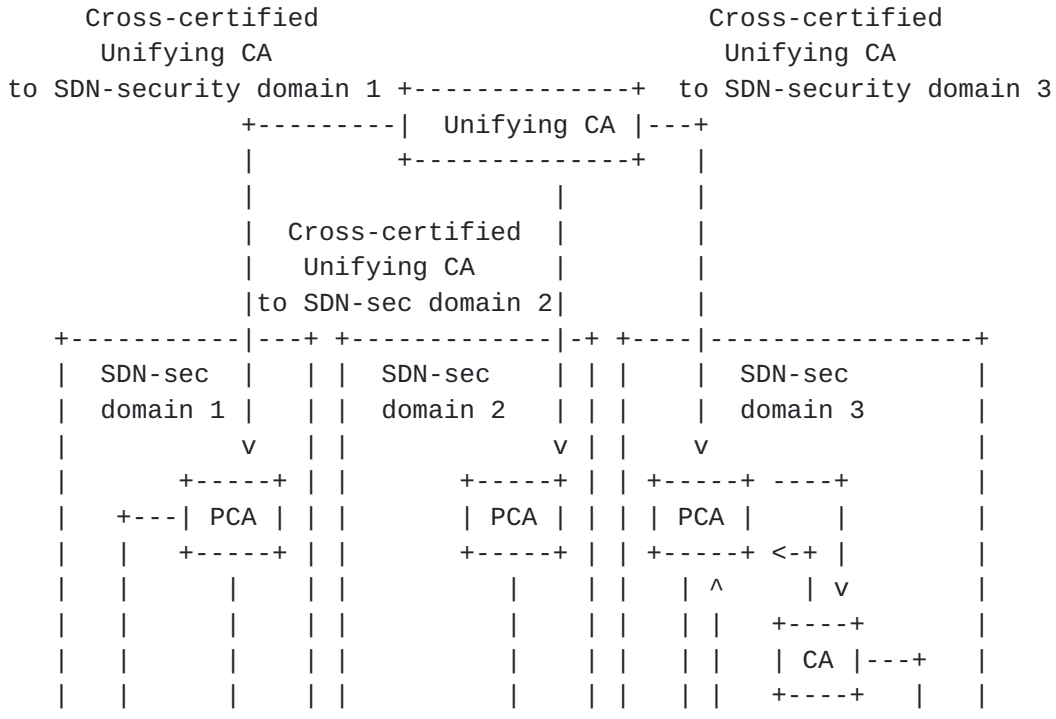
Figure 6: Direct Cross-Certification Model

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

5.3 SDN Unifying Domain Model

In this Unifying Domain 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 benefits and specific implementation level challenges, as evaluated -
a) This model enforces strict security policies and acquire complete control for security governance across all participating SDN-Security Domains
b) The model is too rigid, typically not viable for cross-organization implementation due to high level of liability implications
c) Implementing this model often requires complete re-architecting effort
d) Adds to operational overhead in terms of managing the complete CA hierarchy and security policies, unless an operation framework offers certain level of automation benefits



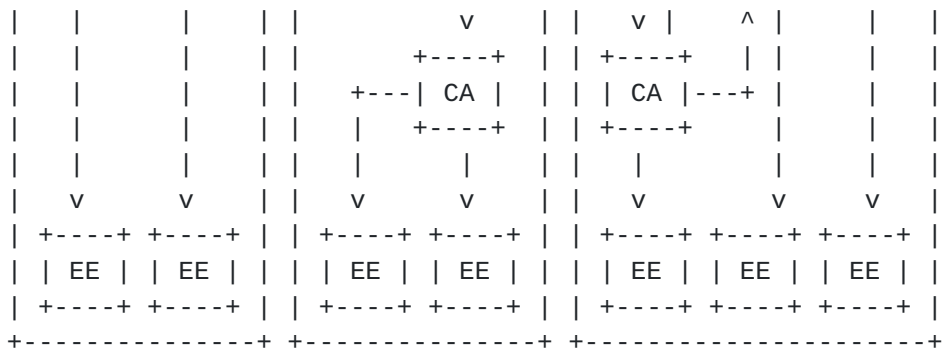


Figure 7: Unifying Trust Point (Unifying Domain) Model

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

6. Discontinuous Certificate Chaining

In discontinuous certificate chaining model, there can be SDN-security domains which are independent of each other and show no mutual certificate interoperability 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 interoperable relationship.

Following are some of the deployment scenarios where these approaches appear to be quite useful -

(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-tenant 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 [RFC5217] can be leveraged in a discontinuous PKI setup for the above mentioned scenario (i). Interoperability 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. Establishing this explicit trust involves human user's explicit pinning of the certificate against the particular trust anchor.

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.

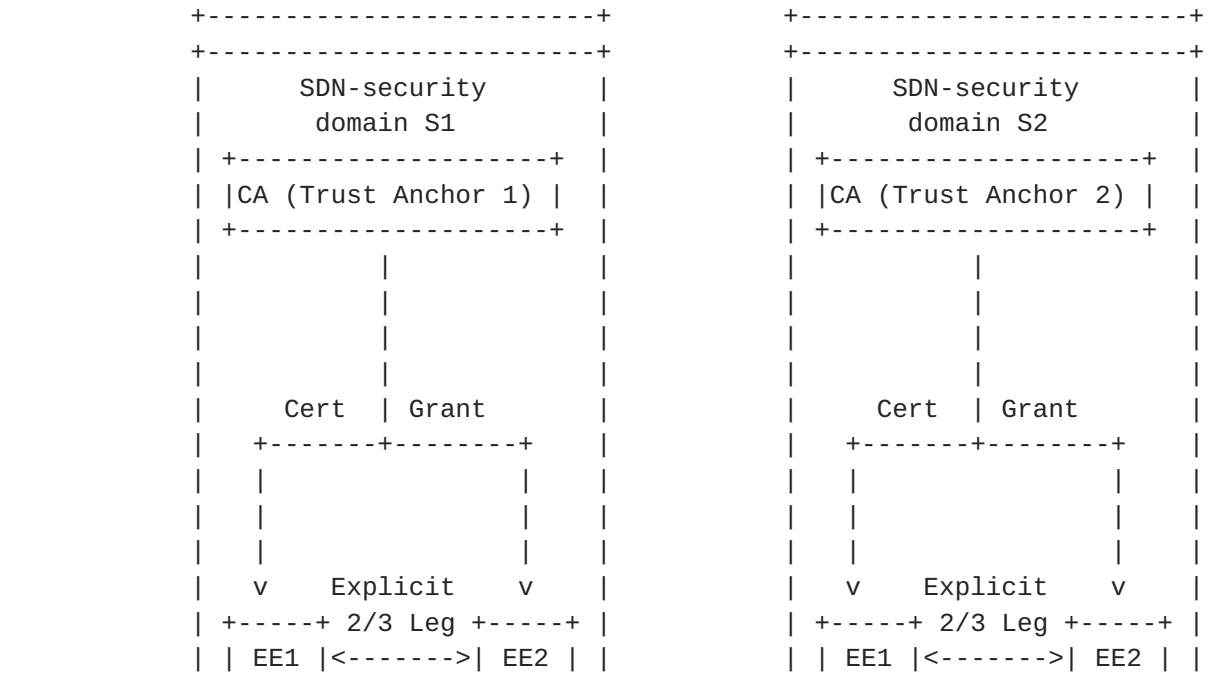
The following Figure 4 shows how two different SDN-security domains will discretely interoperate while leveraging the trust list model. The relying party would thus trust the Trust Anchors present in the trust list. As shown in the below diagram, the End Entity EE1 within SDN security domain 1, would 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 interoperability relationship by depending on the Trust List configurations.

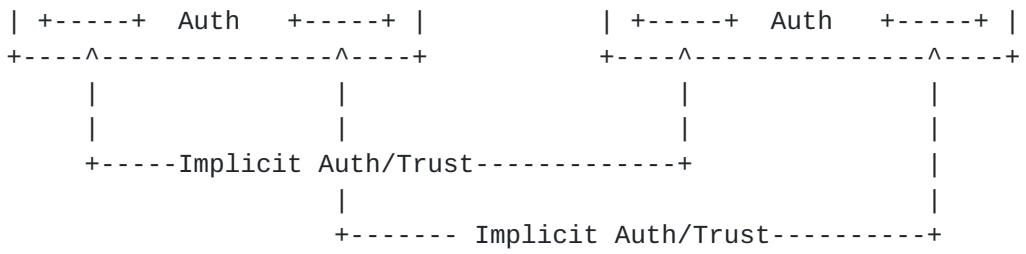
Following are certain benefits and specific implementation level challenges, as evaluated -

a) This model offers flexibilities to configure interoperability relationship without establishing a full certification path

b) The model provides dynamic configuration capabilities over the Trust List

c) Setting this up is entirely dependent on the end user / subscriber, and this typically does not offer good experience to the end user.




Auth
Auth
Implicit Auth/Trust
Implicit Auth/Trust

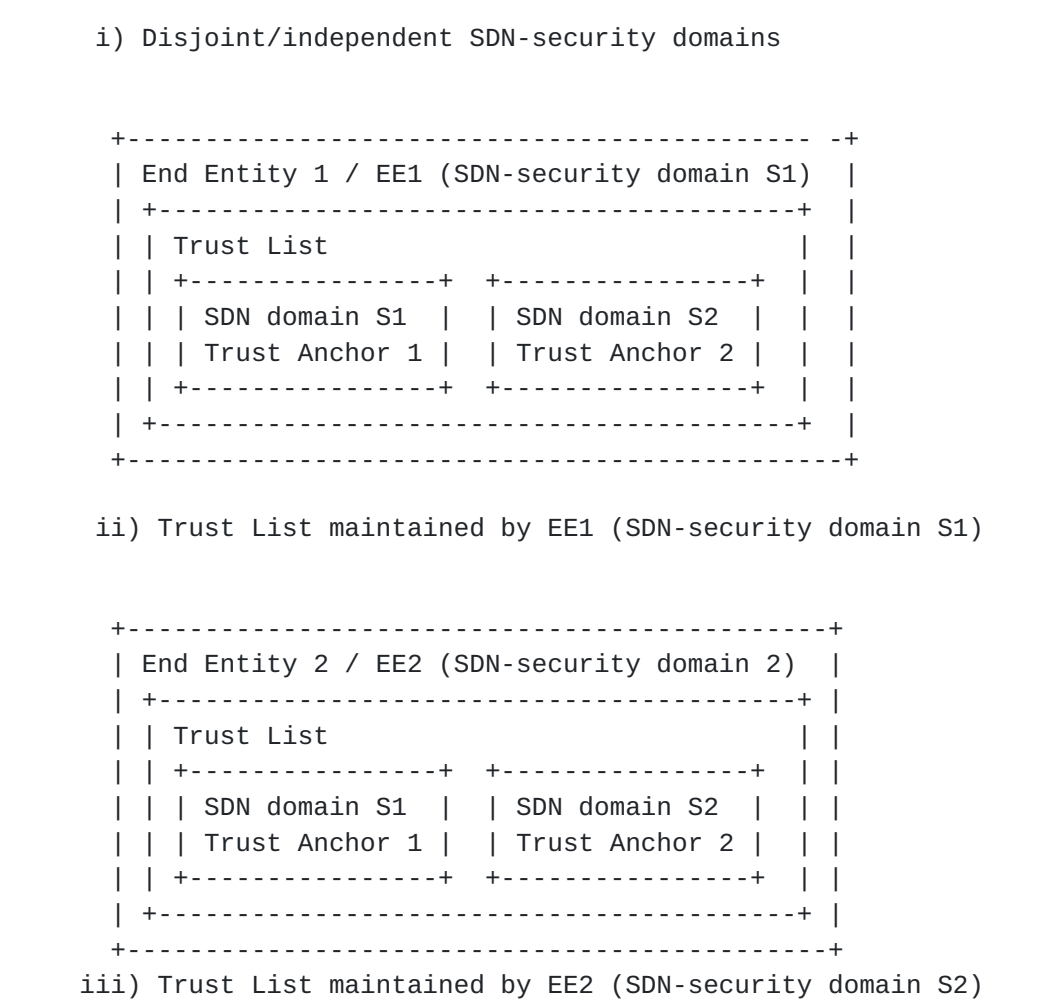


Figure 8: SDN Trust List Model between independent SDN-security domains

6.2 Discontinuous SDN-security domains with varying Authentication 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 authentication infrastructure while underlying transport fabric will maintain its own authentication mechanism.
This draft considers this variation manageable if underlying

transport maintains PKI based Infrastructure and non-PKI infrastructure associated to overlaying application network subscribes to underlying SDN-security domain for the necessary interoperability scenarios. The draft doesn't identify any other method to make PKI based SDN-security domain interoperable with non-PKI infrastructure associated to overlaying networks.

7. Need for Integrated Operational Framework for Certificate Chain Management

Multi-party involvement, and inclusion of multiple security domains, increases the operational complexity of SDN Certification infrastructure. Technology options exercised in different stakeholders' PKI infrastructure can vary significantly for PKI operations and management, leading to complex interoperability requirements. As specifically analyzed in the context of different certificate chaining models in above sections, variations in Identity Metadata, Certification metadata, policy attributes, constraints, and certification status attributes from one SDN-security domain to another significantly impact the Certificate Chain establishment capabilities across SDN-security domains. And this typically introduces severe operational overhead. Thus, setting up a framework appears necessary to manage the complex interoperability requirements through set of processes, practice and automation. Following are the high level requirements as analyzed for the framework -

(i) All stakeholder organization 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 PKIX Certification 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 certification interoperability relationship
- (b) where the policy mapping configurations are not yet applied as no certificate interoperability requirement has been identified yet

(iv) For established certificate interoperability 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 relationship. The update operation should get executed while making necessary changes with immediate effect or at scheduled time.

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

(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 resources from more SDN-security domains into the application delivery network, the certificate chains need to be extended accordingly. This requires modifying the existing certificate interoperability relationship as well as provisioning new relationship as per the requirements of extended certification path. The integrated framework should be able to offer these provisions.

(viii) For every certificate interoperability 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 chain.

(x) For on-demand un-subscription of applications or services, the integrated framework requires to remove the existing certificate interoperability relationship 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.

(xi) The integrated framework requires providing the manageability over Trust Lists configured for supporting discontinuous chains. The hierarchical topology in the integrated framework should model the discontinuous interoperability relationships as well. The implicit interoperability achieved through Trust List configuration should be representable corresponding to the particular SDN-Security domains present in the hierarchy.

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

While an integrated operational framework for Certificate Interoperability Management can consist a distributive set of applications / tools, processes, Policies, and Practice Statements, the framework should offer an end to end span of control for managing

the Relationships. Above mentioned suggested features for managing the interoperability 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.

8. Contemporary Work aligning to Operational Framework requirements for Certificate Chaining

8.1 Automatic Certificate Management Environment (ACME)

The ACME draft specification could potentially offer solutions on the following areas -

- Pre-identified policy mapping across multiple participating SDN-security domains
- On demand extension of certificate chains between multiple SDN security domains in response to dynamic tenancy requirements
- On demand removal of existing certificate chains between multiple security domains without compromising other tenancy requirements
- Defined method for Key management, Certification Status management, Certificate Revocation list management and certificate delivery management

The ongoing work in ACME WG thus can be leveraged in the context of this draft, and requirements (vi), (vii), (x), and part of (xii) as documented in this draft can be addressed.

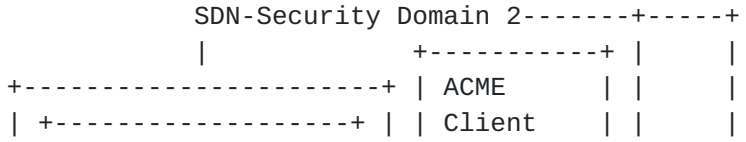
Resources belonging to certain domain are offered to another domain through dynamic tenancy agreement, and by potentially leveraging ACME implementation, dynamic registration, authorization and certificate issuance for the resources against the new domain can be carried out automatically.

In certain cases, on demand extension of certificate or certificate chain require to be supported due to real-time modifications required for SDN application delivery. On-demand modification of certificate can potentially be addressed through ACME specification, like extending the certificates for Subject Name Indication (SNI) or similar multi-tenancy related enhancements. (TBD - Analysis of ongoing ACME specification work will need to be carried out to evaluate the level of support for TLS extensions for multi-tenancy).

On demand modifications of certificate-chain can also be managed through ACME implementation, especially for scenarios where security practices of new domain require establishing a new chain of trust. Certification Authorities involved in the new chain will require to support ACME implementation at every intermediate stage to carry out automated certification.

During expiry of tenancy agreement or on-demand un-subscription of SDN applications, automated revocation of certificates can also be carried out by potentially leveraging ACME implementations.

Following diagrams elaborate some of the possible deployment scenarios.



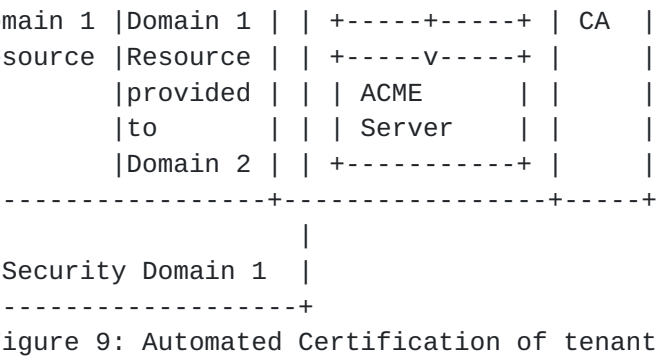


Figure 9: Automated Certification of tenant resources with new Domain's CA

Above diagram elaborates a deployment scenario where Domain 1's some of the resources are provided to Domain 2 as a result of certain dynamic tenancy agreement, and certification of same resources against Domain 2's CA can potentially be carried out by leveraging ACME implementation.

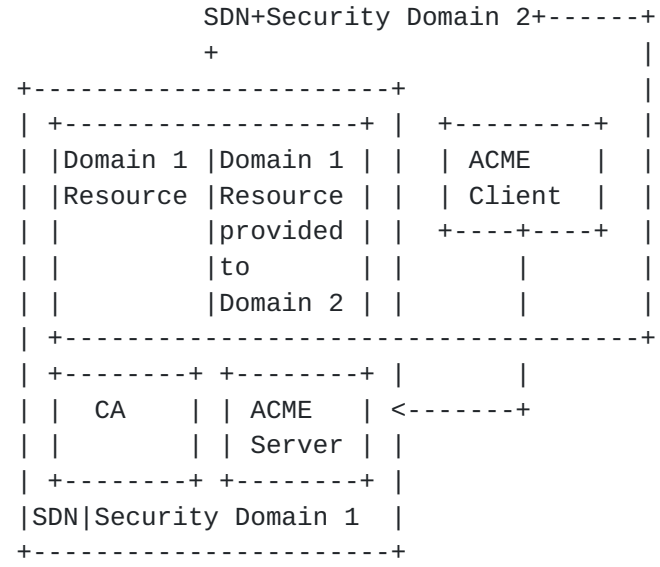


Figure 10: Automated certificate enhancement of tenant resources in existing Domain

The above diagram elaborates a deployment scenario where Domain 2's resources acquire the Certificate from Domain 1's CA. Thus, if Domain 1's some of the resources are provided to Domain 2 as a result of dynamic tenancy agreement, automated certificate enhancement can potentially be carried out by leveraging ACME implementation.

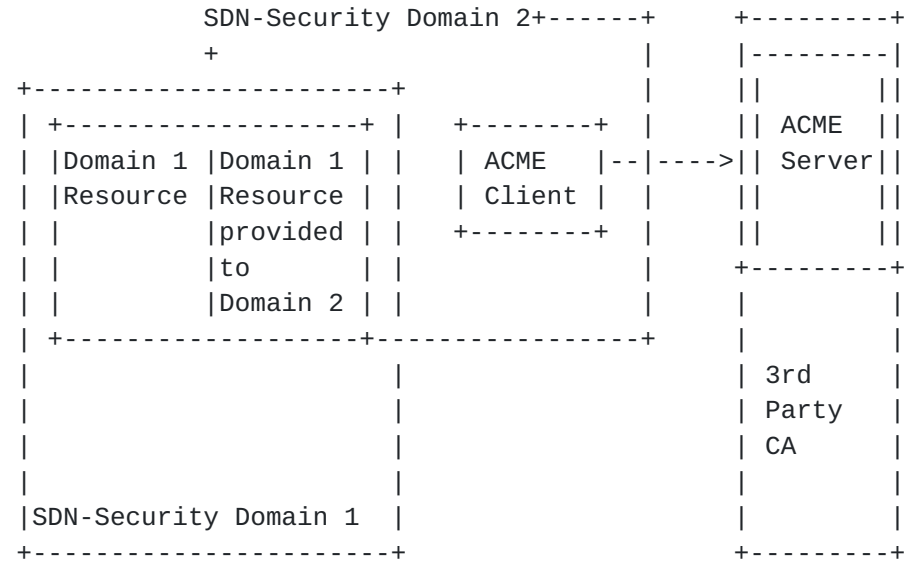


Figure 11: Automated certification of tenant resources with 3rd party CA

The above diagram elaborates a deployment scenario where Domain 2 relies on 3rd party CA, and certification of tenant resources can potentially leverage ACME implementation for automated execution.

8.2 System for Cross-Domain Identity Management

TBD

9. References

1) [RFC5280] "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) [RFC6402] "Certificate Management over CMS (CMC) Updates"

4) [RFC7030] "Enrollment over Secure Transport"

5) [RFC4778] "Operational Security Current Practices in Internet Service Provider Environments"

6) [RFC7426] "Software-Defined Networking (SDN): Layers and Architecture Terminology"

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

8) [SDN-SP] draft-sin-sdnrg-sdn-approach-01 "Software-Defined Networking: A Service Provider's Perspective"

9) [ETSI-NFVSec] NFV Security Problem Statement, ETSI NFV ISG

10) [RFC6125] Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)

11) [RFC7590] Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)

12) draft-ietf-acme-acme-01 "Automatic Certificate Management Environment (ACME)"

Authors' Addresses

Saurabh Chattopadhyay
Noida, India

Email: saurabhchattopadhya@hcl.com

Kaushik Datta
Bangalore, India

Email: Kaushik.Datta@hcl.com