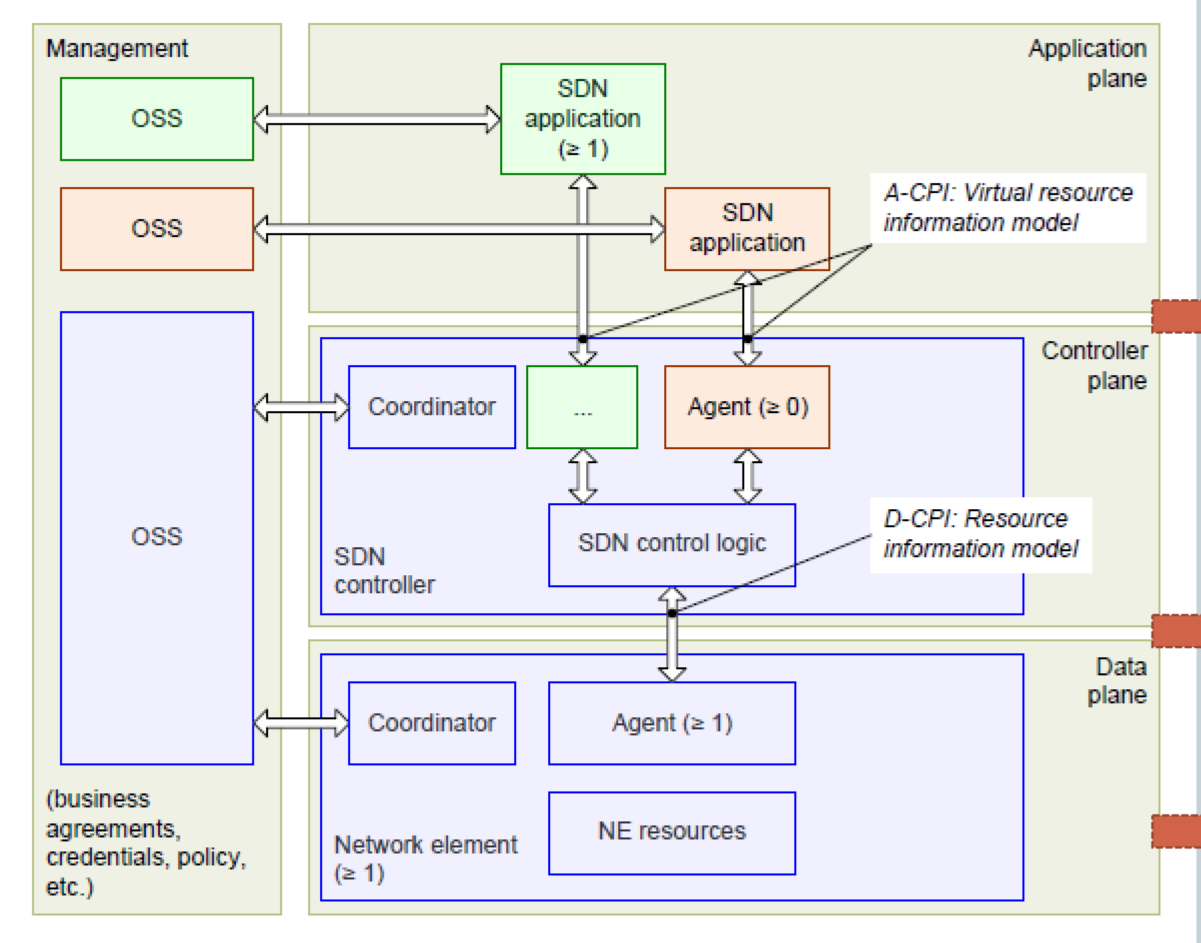
SDN Trust Models and Implementation Methodologies

SDN RESEARCH GROUP,
IETF 93, PRAGUE

AUTHORS –
SAURABH CHATTOPADHYAY
KAUSHIK DATTA

HCL TECHNOLOGIES LTD

The Problem Statement



Source of the Diagram: ONF TR-502, SDN Architecture

Applications to Controllers connectivity challenges –

- Underlying network supports tenancy specific segmentation, without in-built auth
- Tenancy specific network segmentation may span across multiple physical locations
- Auth access of resource entities to be on-demand

Controller to Elements connectivity requires TLS or TLS-like Security Enforcement Infrastructure

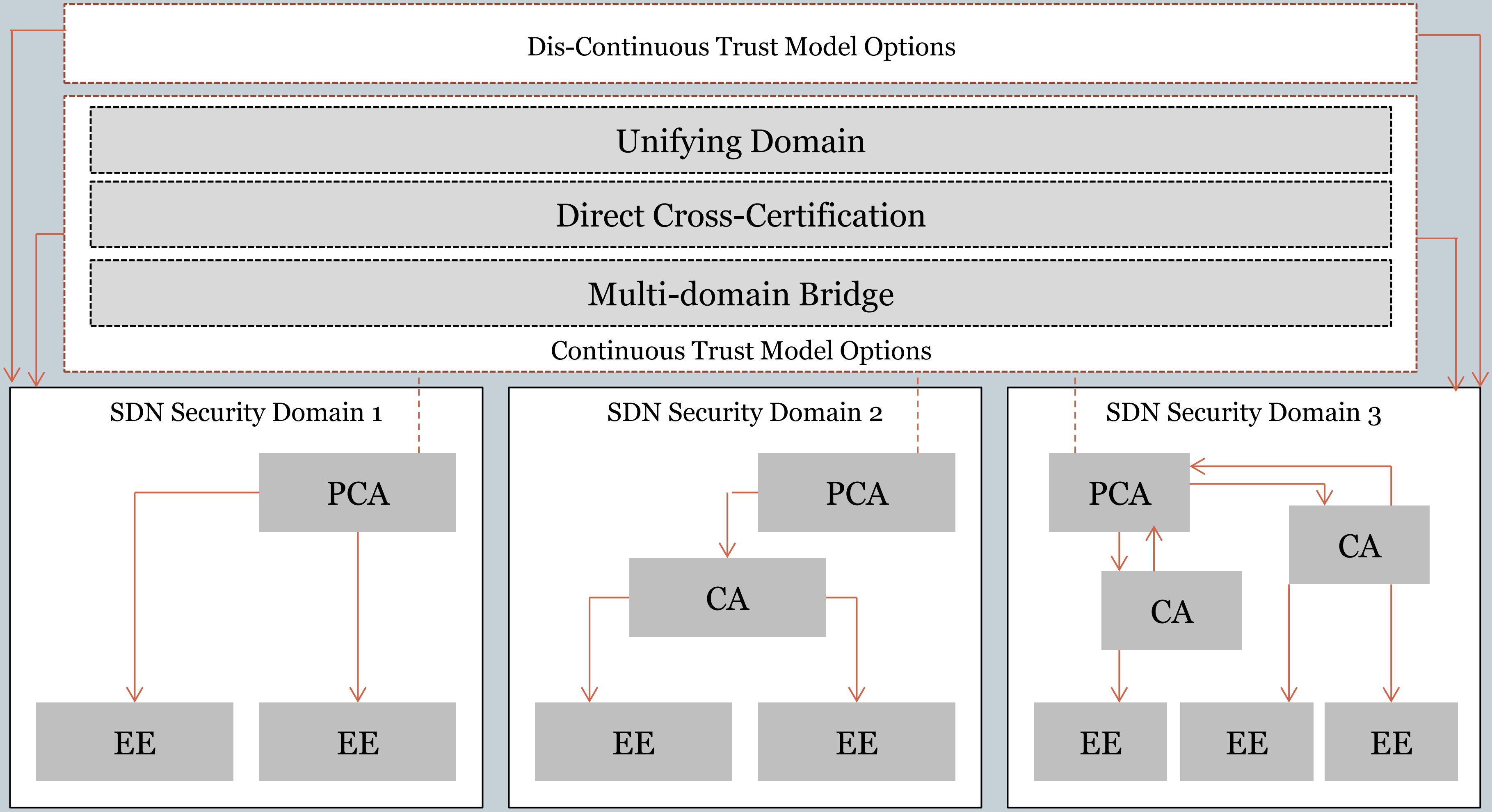
Data plane fabric is reliant on Perimeter Security, Host Security, and Physical Security within particular Physical Location

Authentication Approaches

Unauthenticated Encryption	Opportunistic Security option to consider for preferably physically secured and perimeter secured communication
Trust on First Use	Opportunistic Security option to consider for preferably physically secured and perimeter secured communication
DNS-based Authentication of Named Entities	Option to consider for Domain regulated Peers, supporting DNSSec
PKI	Option to consider for compatible peers for multi-party cross-domain communication

* Above table has been prepared for representative purposes only, not meant to be a comprehensive list of Authentication models for assessing comparative deployment options

SDN Trust Models



Implementation Challenges

(Requirements for Automated Trust Relationship Management)

- Requires modeling the Multi-party & multi-domain diversities in SDN security architecture
- Managing the variations of Identity Metadata, Certification metadata, policy attributes, constraints, and certification status identifiers from one SDN-security domain to another
- Managing the Security Policy Mapping
- Managing on-demand trust relationship provisioning, on-demand extension / shortening of Certificate Chain
- Cross-party cross-domain Identity Management, Key Management, Constraint Management, Certificate Management
- Manageability over continuous and dis-continuous SDN Trust Assets

Adjacent Work – IETF WGs

WG	Status	Brief Description
SCIM WG	Approved	The System for Cross-domain Identity Management (SCIM) working group will standardize methods for creating, reading, searching, modifying, and deleting user identities and identity-related objects across administrative domains, with the goal of simplifying common tasks related to user identity management in services and applications.
ACME WG	Approved	The ACME working group is specifying ways to automate certificate issuance, validation, revocation and renewal. This working group is not reviewing or producing certificate policies or practices.
I2NSF WG	Being Chartered	Focuses on defining / consolidating the Interface(s) to control and monitor the behavior of NSFs, to set up the building blocks of automated Security Management. Heterogeneous administrative domains and multi-vendor environment are identified as among the key challenges.

References: SCIM WG Charter, ACME WG Charter, draft-dunbar-i2nsf-problem-statement-05.txt

Proposed Next Steps

- Analyze Feasibility of leveraging or extending SCIM WG's Artifacts for cross-domain Tenancy aligned Identity Management for SDN Resource Entities

- Analyze feasibility of leveraging automation ways (for certificate issuance, validation, revocation, renewal) proposed by ACME WG for SDN specific deployment architectures

- Analyze feasibility of leveraging defined interfaces of Network Service Functions to develop automation for operational security management

- Requesting SDNRG to consider formally adopting work item for defining SDN aligned operational security architecture, in alignment with other IETF WGs' contributions

Thank You!