SDN Security: Trust Models, Architecture Hardening and Infrastructure Deployment

Current State of Standardization & Future Requirements

Presented by:
Saurabh Chattopadhyay & Kaushik Datta
HCL Technologies Ltd.

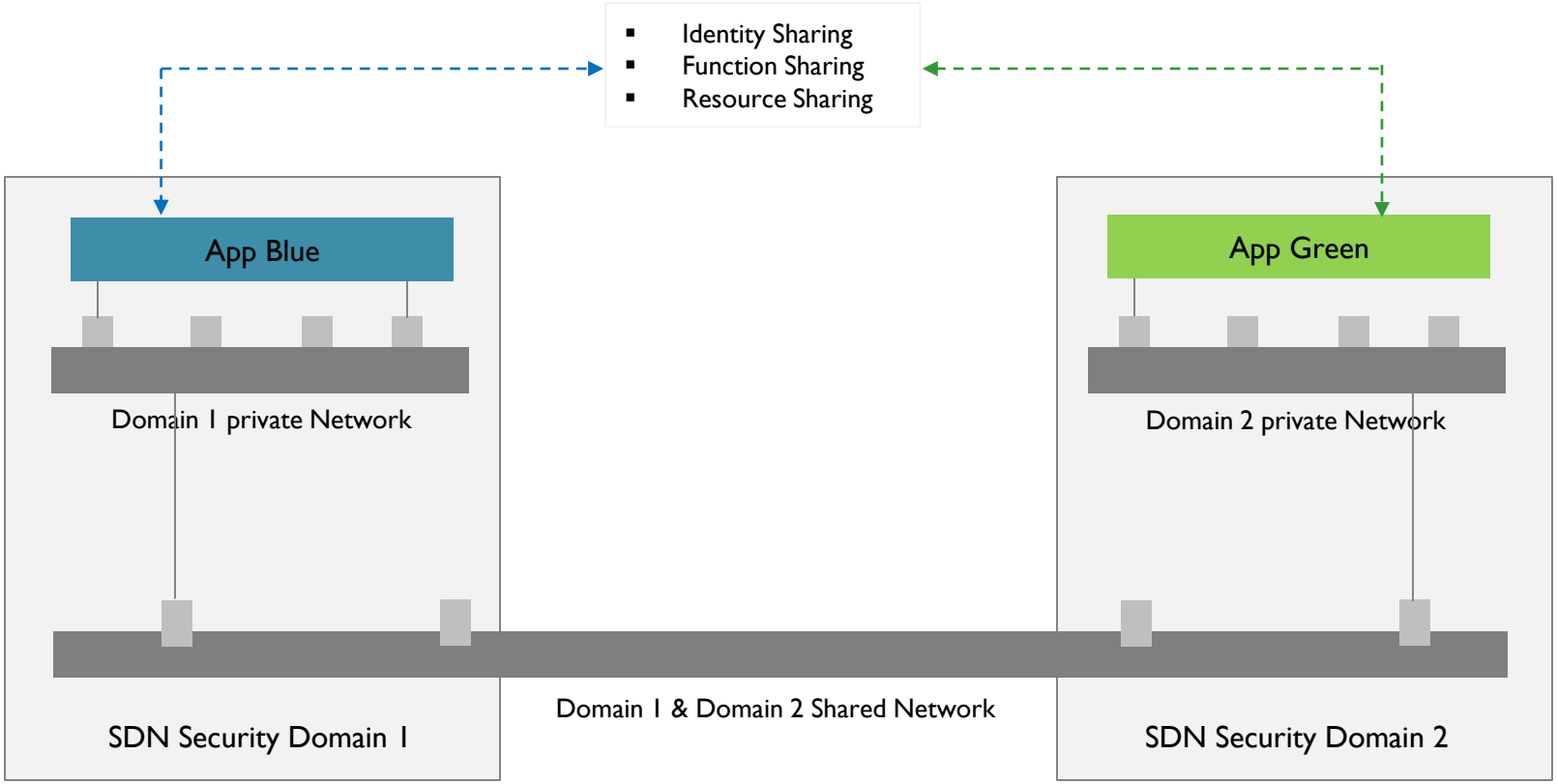
Context

- The content represents an ongoing (individual) draft being worked upon in SDNRG - draft-chattopadhyay-sdnrg-multi-party-sdn-trust (version 3)

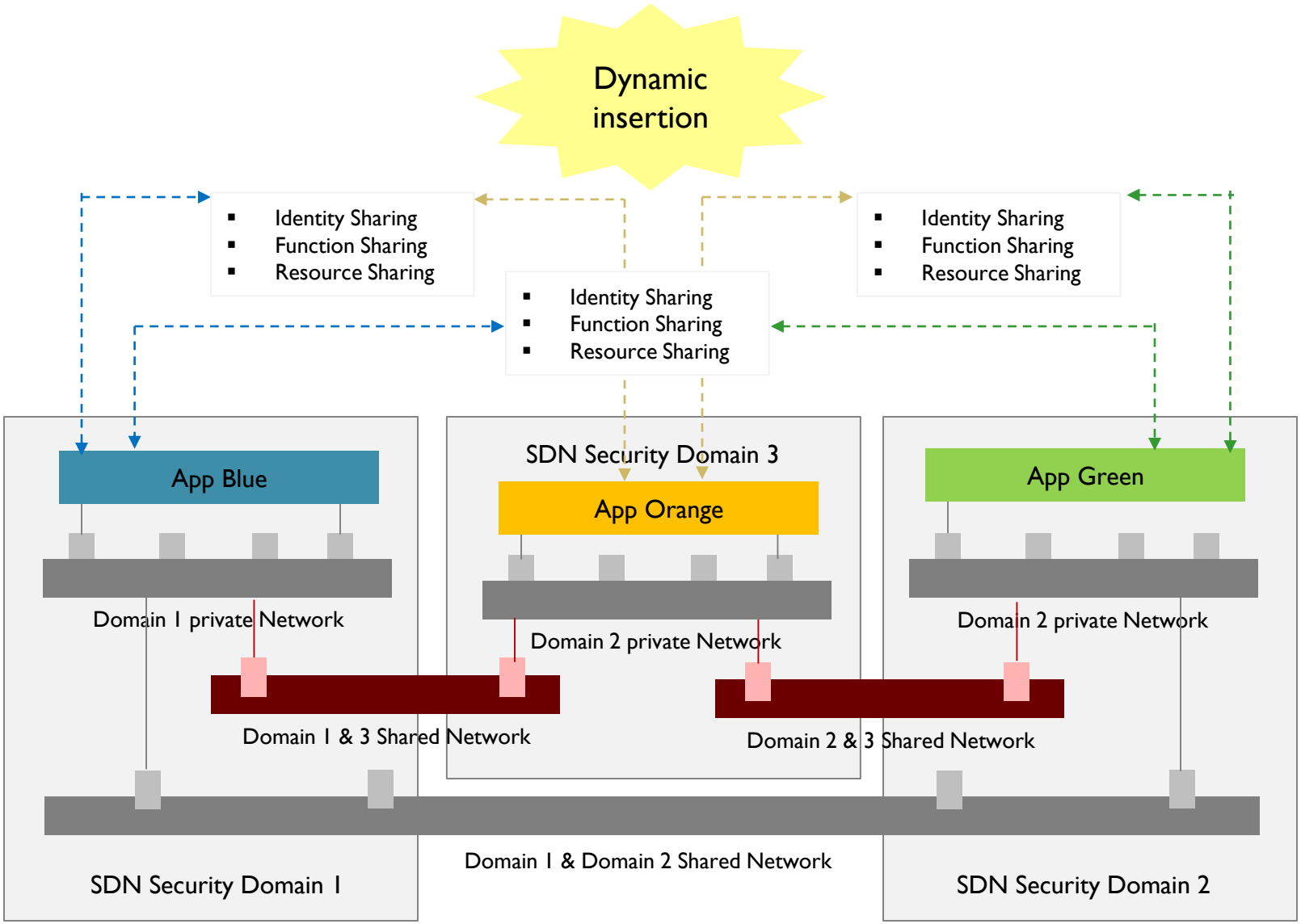
- Presentation Topics –
  - Revisiting the Objectives and Use Cases of Operational Security hardening for SDN enabled Infrastructure
  - Assessment of current Deployment & Gaps
  - Parts of Solution as available from different WGs
  - Future Requirements & Recommendations

Revisiting the Objectives & Use Cases

Examples →
Identity Sharing – Registered Users of one App getting access to other App
Function Sharing – Users of (let's say) one Conferencing App get access to a (let's say) particular Transcoding function offered by another App, while on-demand streaming from particular location requires it
Resource Sharing – (Let's say) An Enterprise decides to transfer certain type of VPN Site infrastructure from its particular office location to a Hosted Cloud



Revisiting the Objectives & Use Cases

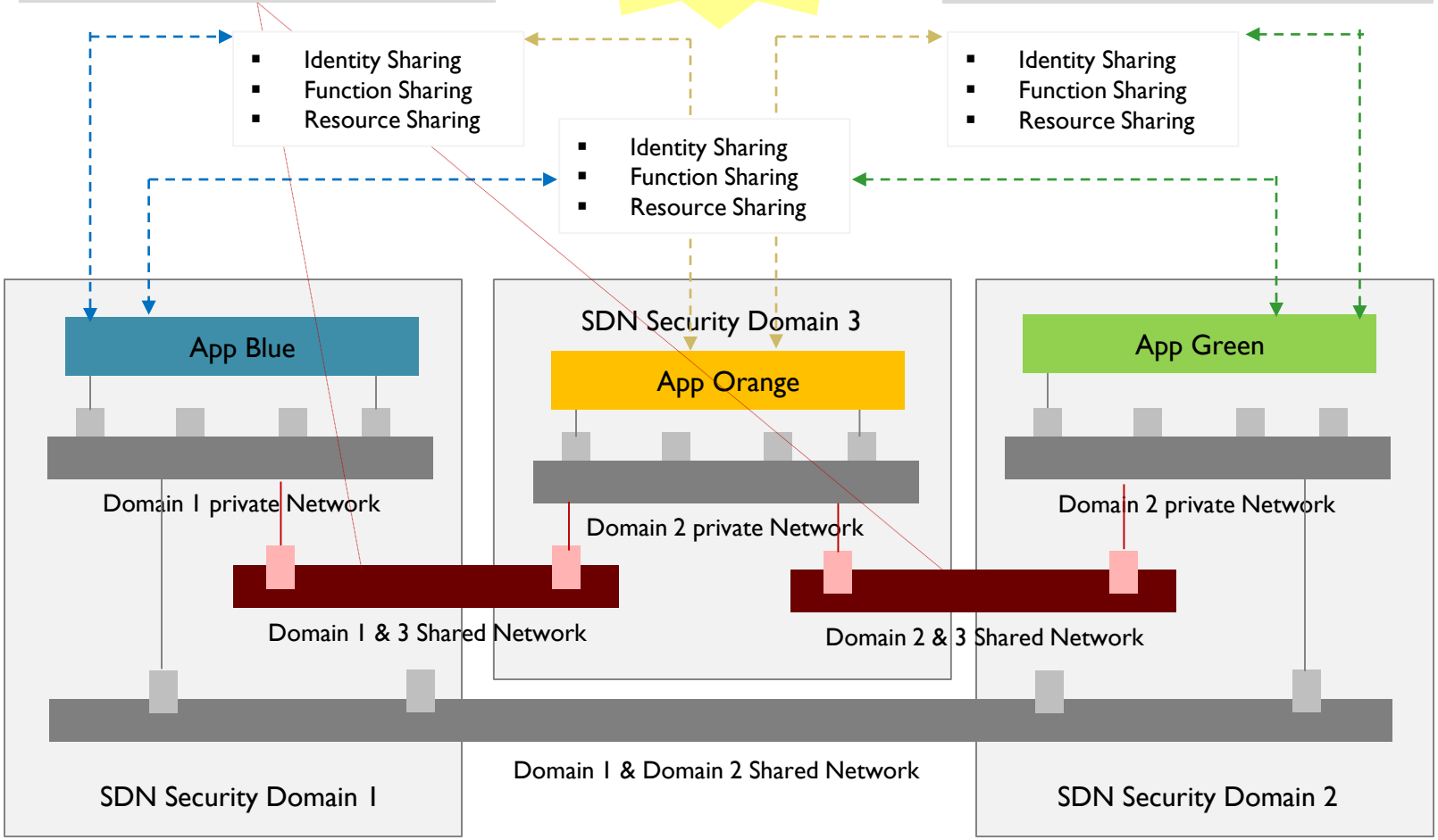


Revisiting the Objectives & Use Cases

Dynamic creation of these network, routing & sharing policies are possible by leveraging SDN capabilities

Dynamic insertion

OPSec policies however still relies heavily on pre-provisioning, posing challenges for dynamic trust establishment as required for dynamic app insertion

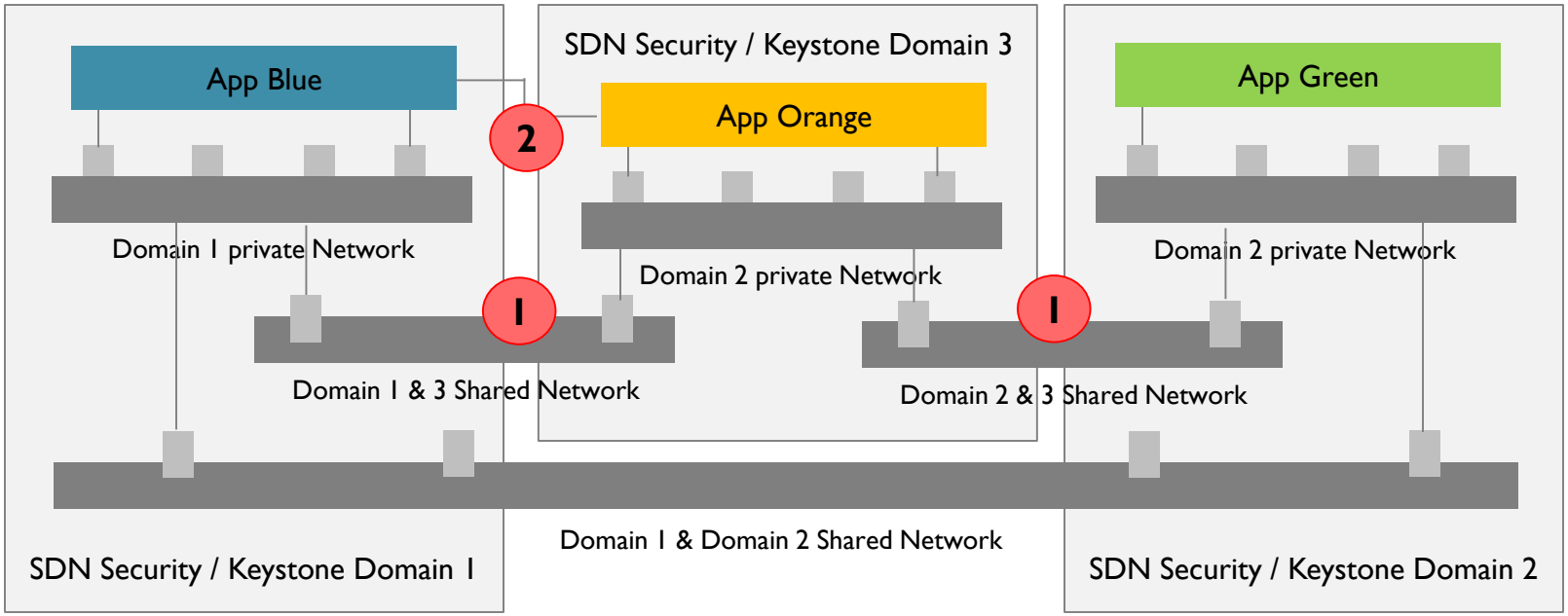


Revisiting the Objectives & Use Cases

- There are various business scenarios where such Dynamic Insertion capabilities of Applications (hosted in different site & different domain) are required
- **RFC 7832** defines some excellent use cases for supporting dynamic deployment and configuration of security services, authentication and authorization for cloud hosted applications
- draft-chattopadhyay-sdnrg-multi-party-sdn-trust (Section 3) identifies the challenges for working out dynamic trust for multi party multi domain SDN Security Infrastructure

Today's Situation
(Representing existing OpenStack Deployments)

1. Resource Sharing Policies don't have provisions for validating external (external site & domain) requester's certificate at the Resource Layer
2. No easy cross-certify provisions in underlying infrastructure to let *App Blue* to leverage *App Orange's* resources while exposing those as its own (tenant)
3. No automation support for PKI pre-provisioning in underlying Infrastructure



Some Alternate Attempts being made…

(may or may not be long term)

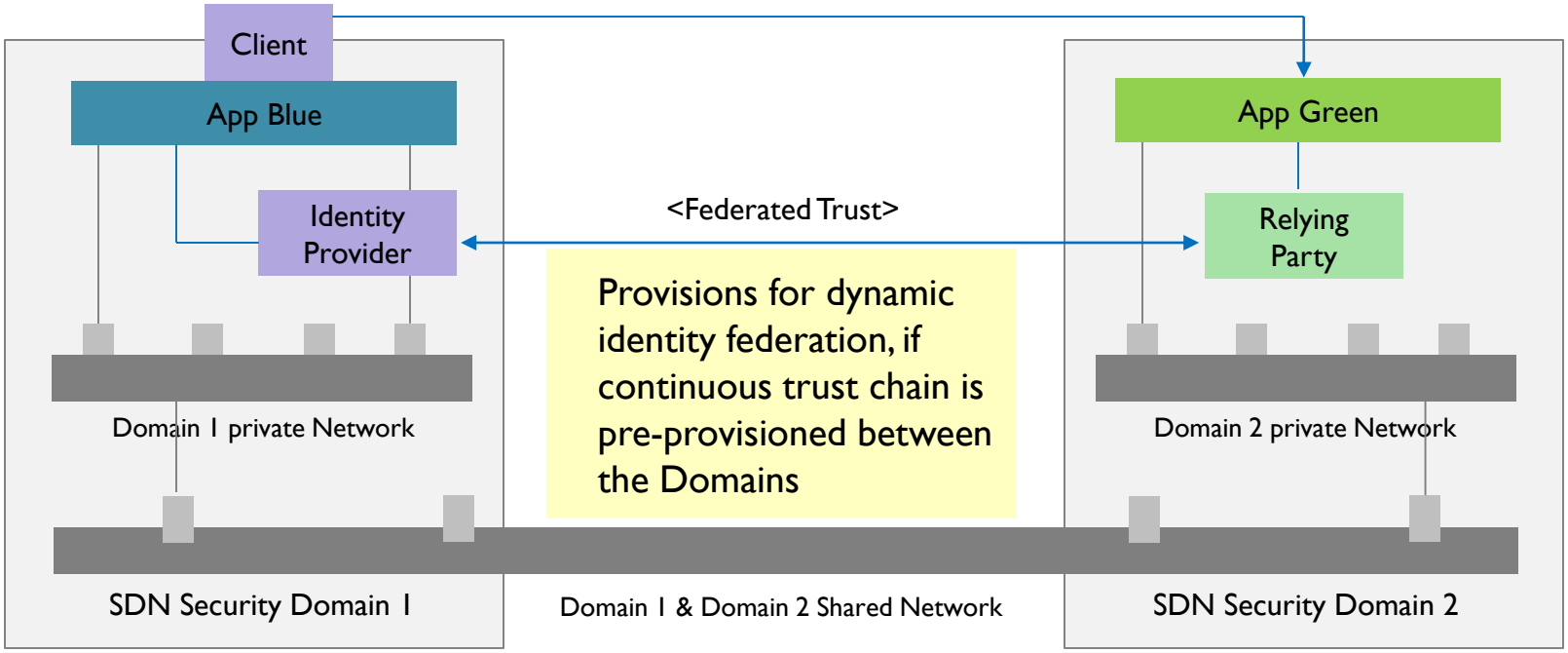
- Self-Certification at Applications layer –
  - Applications alone can't legitimately certify underlying resources, since dynamic resource allocation is occurring at Infrastructure layer
  - Applications not relying on attestation from underlying Infrastructure, other party can't differentiate between self-certified Applications launched from Trusted Boot and Non-Trusted Boot

- RBAC policies getting defined for 'Trusted' external IPs / CIDR routes
  - Vulnerable to IP Spoofing

- Reverse Proxy mechanism being implemented to mask original resource owner (in absence of cross-certify provisions for tenants)
  - Increases attack surface
  - Impact on Performance

Solution Part 1 – Leveraging ABFAB & SCIM drafts

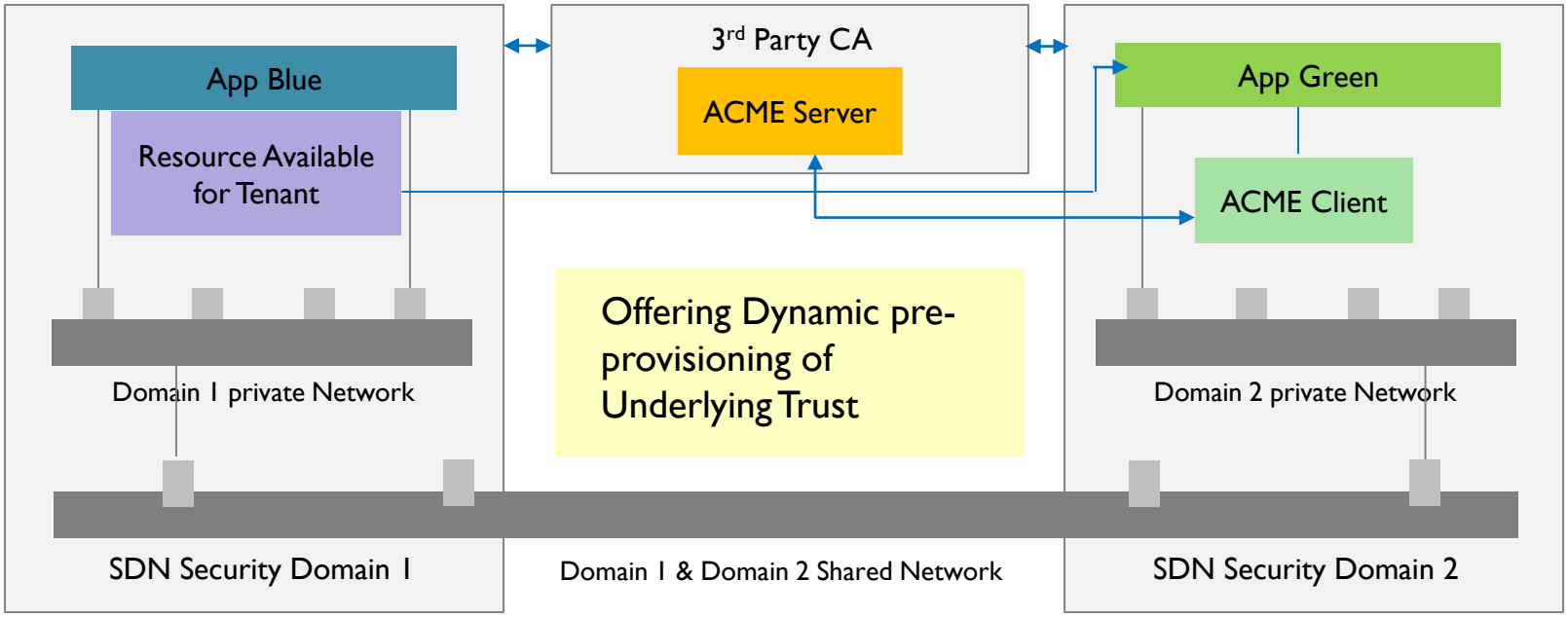
- **Dynamic pre-provisioning of Identity Federation**: ABFAB & SCIM WG drafts declare that for compliant applications, principals need not have pre-instantiated accounts that their federated identity maps to, before their first visit to that application; the application can perform this process on the fly
- **Requires Pre-provisioning of Underlying Trust**: If Relying Party and Identity Provider belonging to different SDN-Security / PKI domains, establishing a continuous chain of trust between the two domains is required
  ABFAB & SCIM drafts don't specify this particular mechanism, assumes the chain of trust will be pre-provisioned before dynamic pre-provisioning of identity federation is attempted



Note: ABFAB WG specified nomenclature used to conceptually depict Specifications of ABFAB & SCIM WGs

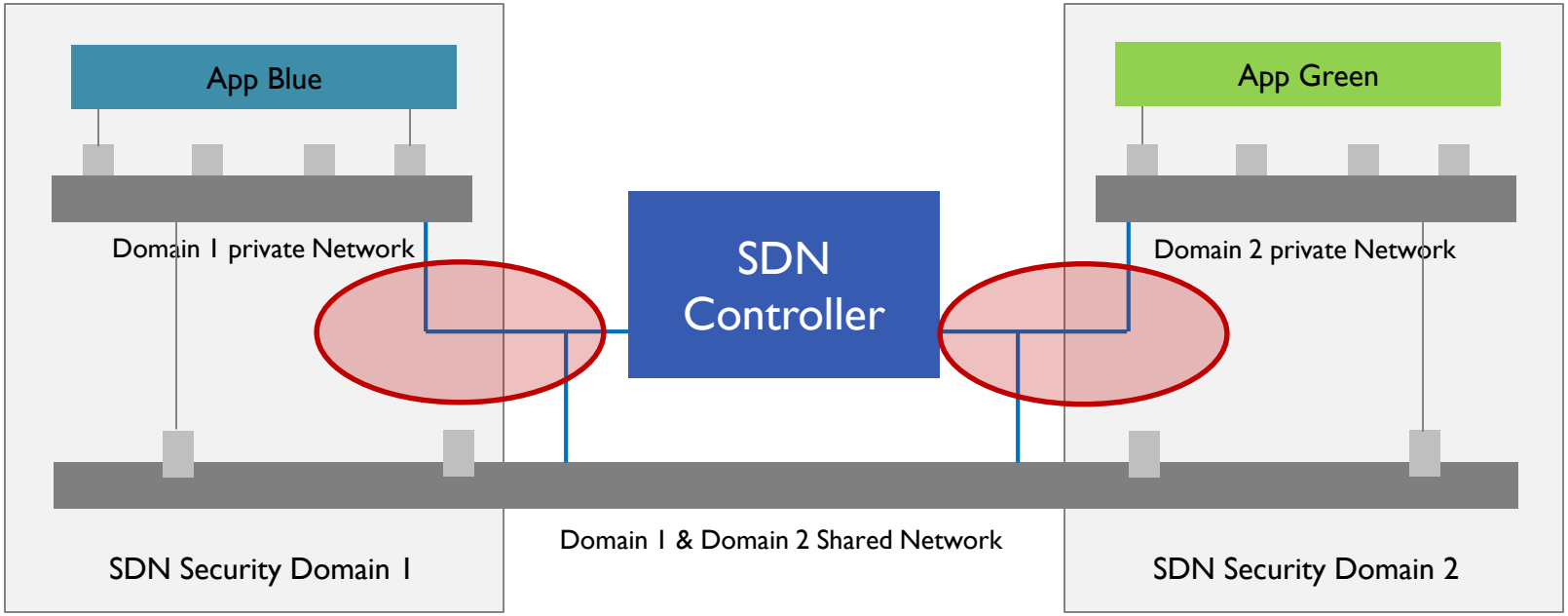
Solution Part 2 – Leveraging ACME drafts

- Resources belonging to certain domain can be leveraged 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
- ACME specification can also be leveraged for
  - Defining pre-identified policy mapping across multiple participating SDN-security domains
  - On demand extension of certificate chain
  - On demand removal from existing certificate chain



Solution Part 3 – Leveraging ONF SDN Hardening Guidelines

- ONF SDN Hardening Guidelines focuses on defining hardening requirements between SDN Controller to SDN enabled Nodes (Physical NEs / vSwitches / vRouters) as circled below
- The Guideline doesn't provide any guidance on how to manage the Operational Security & PKI infrastructure



Future Requirements and Recommendations

Future Requirements

- No Standard Guideline available for Practitioners that can be leveraged for addressing Operational Security requirements of SDN enabled Infrastructure
- A Holistic Architecture needs to be developed, including all required parts of Solution coming from contemporary standard development groups

Recommendation

- Recommending SDNRG to adopt a work item to develop suitable Operational Security Deployment Guideline for SDN capable Infrastructure