# POSTER: A Model for Trusted Identity in NFV Environment

Abu Shohel Ahmed
*Department of Computer Science*
*Aalto University, Finland*
*Email: abu.ahmed@aalto.fi*

Tuomas Aura
*Department of Computer Science*
*Aalto University, Finland*
*Email: tuomas.aura@aalto.fi*

***Abstract*—Network Function Virtualization (NFV) is a multi-party and dynamic trust environment in which actors such as virtual network function (VNF) provider, Infra provider, Telecommunication Service provider and End users/subscribers dynamically provide or consume services based on trust. To set trust for an identity, currently for most cases, we rely on leap of faith, attestation from a trusted platform, or certificate from a trusted third party. However, these approaches fall short during scaling or create a single point of failure which are unwanted properties for continuous network service. Given the importance of security and service continuity in NFV domain, this paper proposes Trusted Identity Model - a distributed approach for defining trust of an identity. It uses publicly verifiable ledger and a consensus-driven approach to set trust for identity.**

## 1. Introduction

Network function virtualization (NFV) uses virtualization technique to decouple network functions from the underlying hardware infrastructure. NFV [1] introduces new security challenges from trust point of view. Traditionally, network functions run on a dedicated environment protected by firewall, and the environment was assumed to be mostly static e.g., service provisioning and scaling were static or manually configured. With the introduction of NFV, the same virtualized platform is shared and managed by multiple parties. This demands a new trust model for NFV security.

One of the key tenets of trust is to set up the initial root of trust (ROT) and forming a trust chain for an identity. This enables the other party to evaluate trust of an identity by following the trust chain. Traditionally, trust in a network function is established by using a/set of credentials which were earlier placed manually by a trusted party (e.g., administrator). The trust chain from this credential to the ROT is established using a trusted third party (e.g., Certificate Authority [2]), or leap of faith, or out of band channel (e.g., add public keys in known_hosts file. These approaches to establish trusted identity have limitations in a multi-party dynamic environment. Most notable limitations are 1) Trust establishment of an unknown entity by leap of faith or out of band channel is not scalable or insecure 2) Trusted third party can become a single point of failure 3) Verifying trust state of a identity throughout its life cycle is difficult 4) Trust decision for an identity by any party is not publicly verifiable, hidden under one or more layers 5) Lack of tamper-proof evidence for any trust decision.

TABLE 1. TRUST EVALUATION CRITERIA FOR NFV

| Attribute | Options | NFV Trust |
|---|---|---|
| Actors | single, many | Many |
| Trust relationship | symmetric, asymmetric | Any |
| Time and context-sensitive | static, dynamic | Dynamic |
| Verifiability | private, public | Public |

An NFV environment faces all of the above challenges. In addition it brings new question: 1) How to automate trust establishment among multi-party (e.g., VNFs), when those are mutually non-trusting party 2) How to securely convey [3] trust from platform to end users/subscribers in a virtualized environment. Considering these weaknesses in NFV domain, this paper proposes a model for trusted identity using the idea similar to Certificate Transparency [4]. Our identity trust model uses a verifiable public ledger to maintain trust state of identities. We use decentralized and consensus driven approach (similar to [6]) for maintaining trust state of an identity. An identity is appended to the public ledger after a consensus is reached about the trust state of an identity by Collaborators (Collaborators are entities who vouch other's identity). Later on, an identity consumer, can any time read identity state (e.g., who vouched for this identity, when) from the public ledger and make trust decision regarding the identity.

## 2. Trust evaluation Criteria for NFV

Trust evaluation measures applicable criteria for a particular trust relationship, and assurance levels for each criteria. Trust evaluation are always contextual and depends on many parameters [1]. Based on earlier research [1], [7], [8] on NFV trust requirements, we propose a trust evaluation criteria for NFV in Table 1. These criteria are used later on to evaluate our proposed model.

## 3. Identity Trust Model

Identity Trust Model (ITM) enables trust for an identity in the NFV domain. The main components of the model are

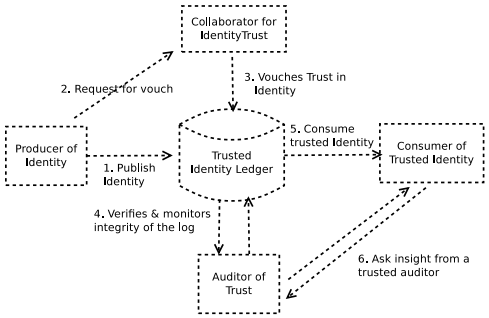


Figure 1. Identity Trust Model

shown in Figure 1.

**Identity Trust Ledger (ITL)** is a network service maintaining the ledger for trust state of identities. The ledger has several characteristics: 1) Ledgers are append only. Once a record is entered it is an immutable information. A new entry is pushed to the ledger when trust state changes for an identity 2) Ledger are cryptographically integrity protected 3) The ledgers are publicly audit-able. 4) An entry is recorded only after a consensus is reached from a set of Collaborators.

**Producer** is the owner of the identity. Producer publishes identity towards the public ledger and controls related credential secret. For example, in VNF scenario, a VNFC can publish its public key after first boot to the public ledger.

**Collaborator** vouches for the trustworthiness of an identity of the producer. There could be different set of collaborators for each NFV domain. For example, Infra service provider can be a collaborator for an identity of a VNF, while a trusted third party can be a collaborator for inter-VNF trust establishment.

**Auditor** checks for suspicious activity in ledgers. It also check the overall integrity of the ledger. Auditors ensures that published identity must end up in the public ledger. Based on monitoring result, an auditor can also define trust level for an identity.

**Consumer** consumes identity and trust state information from the ledger. Based on the trust level of an identity and its own policy, consumers make decision about trustworthiness of an identity.

In the following subsection, we explain a scenario to apply ITM model in the NFV domain.

### 3.1. Scenario

*A set of VNF components (VNFC) provide web service towards end users. These VNFCs have dependency with another set of VNFC for database service. There is a strict requirement that only legitimate VNFC front-ends can connect to the database servers and vice-versa. VNFC environment is dynamic and scaling of service is a routine.*

*Maintaining trust for such an environment requires identity of each legitimate front-end is trusted by any database back-end. ITM model can provide necessary trust guarantee for such cases. One approach is presented below:*

*After initial VNFC boot, key materials (e.g., public/private key pair) are generated within the VNFC domain. The VNFC publishes the public identity and state information to the ITL. The VNFC also ask collaborators such as the VNF domain administrator, infra service provider, trusted third party to vouch for the trustworthiness of the published identity claim. In turn, collaborators vouch for the identity based on its policy (e.g., link distance, proof of work). When a quorum of collaborators vouch for an identity, it is appended to the public ledger. Later on, a consumer of identity e.g., the database VNFC can retrieve trust state of an identity for VNFC web-server from the public ledger to make a trust decision.*

## 4. Evaluation and Future Work

Earlier in Table 1, we have defined criteria for evaluating trusted identity in NFV environment. Identity Trust Model fulfils NFV trust criteria from Table 1. It provides trusted identity in a multi-party dynamic environment, enables subjective trust evaluation by consumers, and provides a publicly verifiable ledger for immutable trust state of an identity. That being said, further research is required in areas such as 1) defining policy when collaborators trust/vouch for others, and how define consensus among collaborators 2) defining policy for consumers when to trust a record from the public ledger 3) privacy implication due to identity trust state exposure. 4) identity cloning and trust impact in virtual environment.

## 5. Conclusion

Multi-party and dynamic trust environment such as NFV requires new design thinking regarding trusted identity. Identity Trust Model uses novel techniques such as consensus and publicly verifiability to deliver trusted identity for NFV environment.

## References

[1] "ETSI industry specification group (ISG) NFV, ETSI gs nfv-sec 003 v1.2.1, network functions virtualisation (NFV); NFV security; security and trust guidance," August 2016, available at http://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/003/01.02.01_60/gr_NFV-SEC003v010201p.pdf.

[2] Housley and R. et al., *RFC5280 Internet x. 509 public key infrastructure certificate and crl profile.*, 2008.

[3] Parno, Bryan, J. M. McCune, and A. Perrig, *Bootstrapping Trust in Modern Computers*. Springer Science & Business Media, 2011.

[4] Laurie, Ben, A. Langley, and E. Kasper, "Certificate transparency. RFC 6962," 2013.

[5] *How Certificate Transparency Works*, available at https://www.certificate-transparency.org/how-ct-works.

[6] Callas and J. et al., *RFC4880 OpenPGP message format*, 2007.

[7] Li, Wenjuan, and L. Ping, "Trust model to enhance security and interoperability of cloud environment," 2009.

[8] Firdhous, Mohamed, O. Ghazali, and S. Hassan, "Trust management in cloud computing: a critical review. arxiv preprint arxiv:1211.3979," 2012.