Security Conference

ETSI Addresses Certificate Woes in NFV Technology Based 5G

Presented by: Ben Smeets, Ericsson

16/10/2023

Agenda

- Introduction
- Certificates as identities in a virtual world
- Main headaches of certificate management for VNF
- Establishing an identity in a VNF is Trust bootstrapping
- ETSI GS NFV-IFA work
- Conclusions
- Q&A

Introduction

Bio: Ben Smeets

- Ericsson Senior Expert: trusted computing
- Chair at Lund University in Digital Techniques and worked on cryptography, data compression, and information theory, and channel coding
- ETSI: Rapporteur for ETSI TC LI effort to standardize X0 interface

Certificates as identities in a virtual world

The two most dominating uses of certificates are

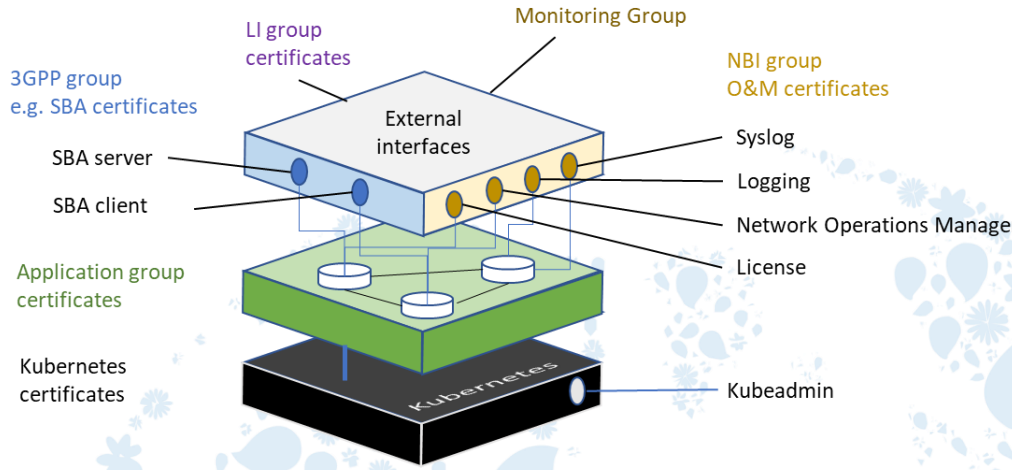
- In secure communication protocols: e.g. (mutual authenticated) TLS/DTLS, IPsec
- Signature verification for securing object transfer: e.g. signed SW, attestation reports

To have a strong identity, the private key MUST exist only inside the virtual entity that uses the identity (say for TLS).

- So the key must be created (and kept protected during use) inside the virtual entity
- We must have a way to assess that when issuing the certificate we are actually assigning the certificate to the entity we trust to hold and use the key (to use later to interact with via TLS)
  - Traditionally PKI: Proof via yet another identity (leading to circular argument)
  - Better: Use of attestation (see Leslie Willis presentation)

Main headaches of certificate management for VNFs

- No birth identity/certificate for the virtual NF
- Each VNF requires several certificates, e.g. SBA, O&M, LI
- VNFs have dynamic life cycle which makes certificate LCM also very dynamic
  - Instantiation is dynamic/automated
  - Even more dynamic inside VNF, particularly when container technology is used
- Most network operators want to use high-grade PKI systems.
  - (these use) proprietary APIs for defining end-entities – but standard protocols to enroll certificates for end-entities, e.g. CMPv2, EST

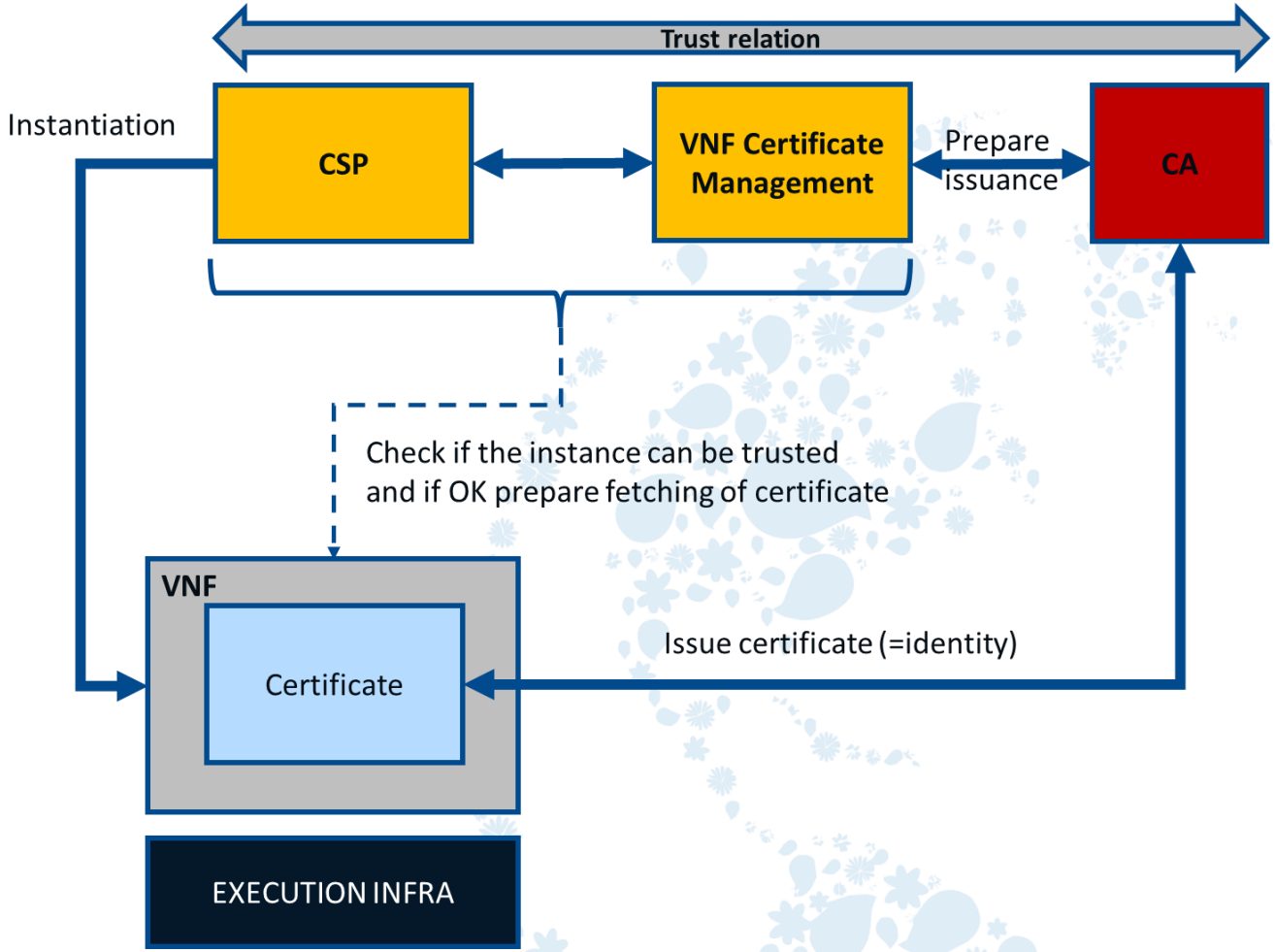


Certificate management must be automated

- Most important: registration of new end-entities and configuration of enrollment
- Managing automatic renewal, handle revocation (and consequences for other certs in VNF)

Establishing an identity in a VNF is Trust bootstrapping

The CSP (tenant) must establish trust in the instantiated VNF that will hold to certificate through a series of interactions that will extend the CSPs trust into the instantiated VNF



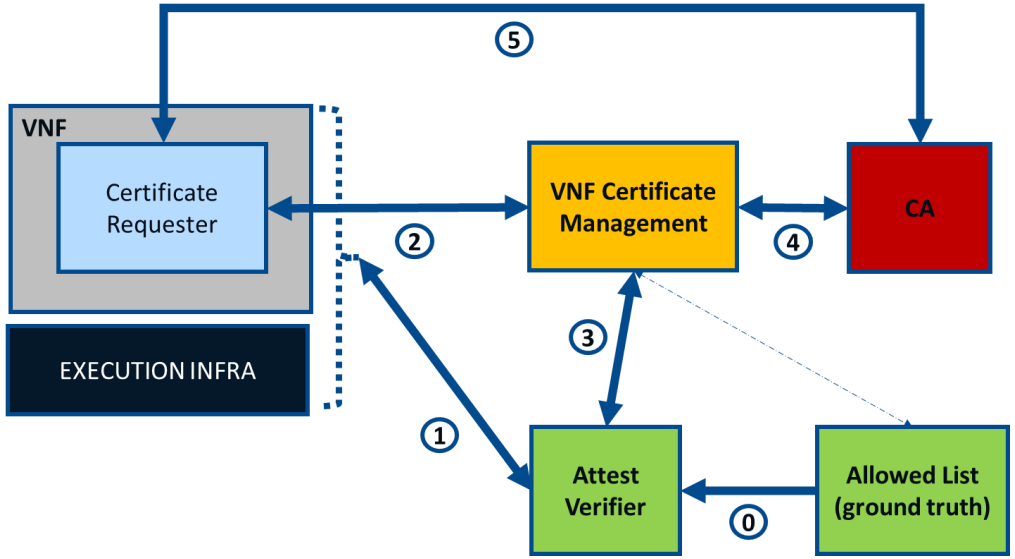
Establishing an identity in a VNF is Trust bootstrapping

Idea is that the certificate issuer via the attestation protocol has

- Established a secure way to interact with the requester
- Verified the requester is trusted (to behave correctly (aka correct software) and keep secrets)
- Can uniquely identify the requester

The above establishes the initial trust that the certificate issuer can use to assign a certificate (for a certain purpose like SBA, O&M or LI) to the requester

Hence the certificate issuer becomes a Relying Party of the attest verifier that checks the attest report which the requester has given (say at start up).



0: ground truth configuration
1: remote attestation
2: request for certificate provisioning
3: attest consultation
4: CA end-entity configuration
5: certificate enrollment (e.g CMPv2)

Certificate Management Function (CMF)
ETSI GS NFV-IFA 026 v4.5.1

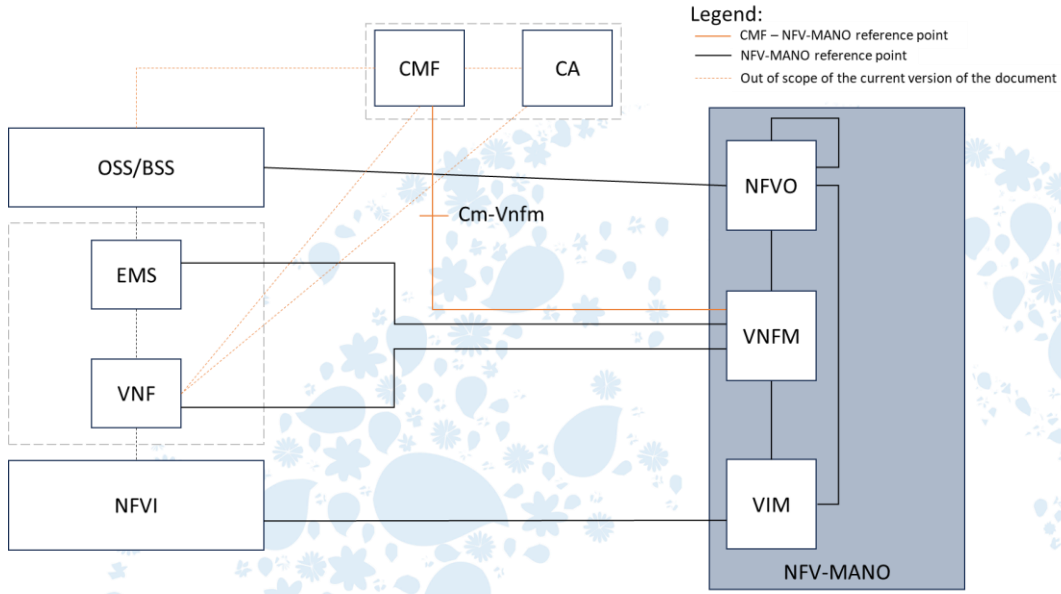
The *Certificate Management Function* (CMF) is introduced to automate the management of certificates in NFV

- Synchronizing the LCM operations for certificates with the VNF LCM
- Automating initial registration at the CA for at least the VNFCI(s) end-entities dedicated to inter-VNFI secure communications
- May interact with an attestation service so that certificate requests be validated as originating attested VNFCIs

The CMF supports at least one of the defined certificate management modes: "*direct-mode*" or "*delegation-mode*"

Various use-cases (e.g., certificate enrolment) for each certificate management mode are described. Requirements on CMF and NFV-MANO are introduced accordingly

Security considerations for *direct* vs. *delegation* mode are listed



CMF in the NFV architecture – "direct-mode" for VNFCI and VNF OAM certificate management (from **ETSI GS NFV-IFA 026 v4.5.1**)

CMF Modes: ETSI GS NFV-IFA 033 v4.5.1

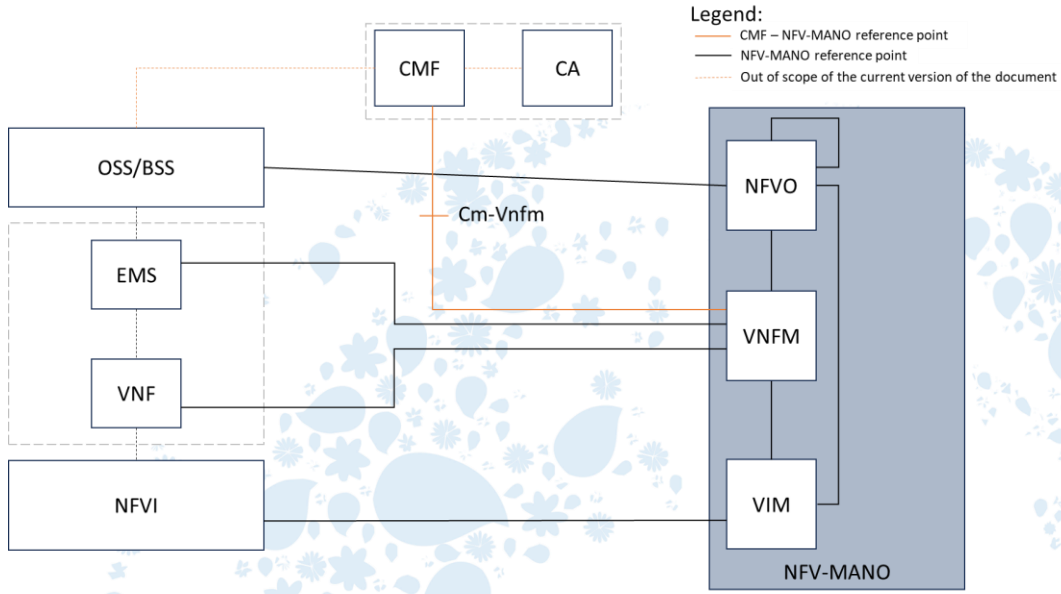
The specification of the interfaces for the new CMF-to-VNFM reference point is based on the characteristics of the certificate management modes and on various requirements from IFA-026 v.4.5.1

- In **"*direct-mode*"**: the CMF consumes a subset of the existing VNF LCM interface exposed by the VNFM:

  This mode works as described before, i.e. keys created inside VNF

- In **"*delegation-mode*": ** the CMF exposes new interfaces to be consumed by the VNFM, which acts as a delegate for certificate management operations on behalf of VNFI(s)/VNFCI(s)

  In this mode, keys are created in VNFM and inserted and thus less secure than direct mode



CMF in the NFV architecture – "delegation-mode" for VNFCI and VNF OAM certificate management (from **ETSI GS NFV-IFA 026 v4.5.1**)

Conclusions

To have a strong identity, the private key MUST exist only inside the virtual entity that uses the identity (say for TLS).

- So the key must be created (and kept protected during use) inside the virtual entity
- We must have a way to assess that when issuing the certificate we are actually assigning the certificate to the entity we trust to hold and use the key (to use later to interact with via TLS)
  - Traditionally PKI: Proof via yet another identity (leading to circular argument)
  - Better: Use of attestation

Certificate management must be automated

- Most important: registration of new end-entities and configuration of enrollment
- Managing automatic renewal, handle revocation (and consequences for other certs in VNF)

Thank you for your attention

Follow us on:

Any further questions?

Contact me:

ben.smeets@ericsson.com