Voucher and Voucher Revocation Profiles for Bootstrapping Protocols

draft-kwatsen-netconf-voucher-00

NETCONF WG
IETF 97 (Seoul)
Introduction

The Artifacts:

– Voucher:
  • used to assign a device to an owner

– Voucher Revocation:
  • used to affirm that the assertions assumed when the voucher was signed are still valid.

The draft only defines the artifacts themselves

– leaving their distribution to bootstrapping protocols
History

• The zero touch draft previously stated that the voucher and voucher revocation artifacts were vendor specific binary formats.

• However, a standard format enables:
  – use by multiple bootstrapping protocols
  – development of tool chains to encode/decode them
Voucher

module: ietf-voucher
  +--ro voucher
    +--ro assertion enumeration // e.g., logged, verified
    +--ro trusted-ca-certificate? binary
    +--ro certificate-id
      |  +--ro cn-id? string
      |  +--ro dns-id? string
    +--ro unique-id* string
    +--ro nonce? string
    +--ro created-on? yang:date-and-time
    +--ro expires-on? yang:date-and-time
    +--ro revocation-location? inet:uri
    +--ro additional-data?
Voucher Revocation

module: ietf-voucher-revocation
   +--ro voucher-revocation
   )--ro revocation-type enumeration
   )--ro created-on yang:date-and-time
   )--ro expires-on? yang:date-and-time
   )--ro (voucher-revocation-type)?
      |   +--:(issuer-wide)
      |      |   ... // see next slide
      |   +--:(voucher-specific)
      |      |   ... // see next slide
   +--ro additional-data?

issuer-wide (like a CRL)
voucher-specific (like OCSP)
Voucher Revocation (cont.)

+--ro issuer-wide // like a CRL
  +--ro (list-type)?
    +--:(whitelist)
      |  +--ro whitelist
      |    +--ro voucher-identifier* string
    +--:(blacklist)
      +--ro blacklist
      +--ro voucher-identifier* string

+--ro voucher-specific // like an OCSP Response
  +--ro voucher-identifier string
  +--ro voucher-status enumeration
  +--ro revocation-information
    +--ro revoked-on yang:date-and-time
    +--ro revocation-reason enumeration
Encoding Strategy

• Currently defined in YANG
  – but YANG is only for “configuration”
  – here we effectively want a file format...

• Current draft says, encode it the same as if it were the response from a RESTCONF server
  – but that seems loose

• Options:
  1. leave as is
  2. define a YANG to artifact encoding
  3. don’t use YANG

Note: the same issue exists in the zerotouch draft, for encoding the information-type artifact
Signing Strategy

• Both artifacts MUST be signed.
  – But a signing strategy has not been selected yet.

• Some options that have been discussed:
  – PKCS#7, CMS, JWS
Next Steps

• This draft is already close to completion.

• We just need to:
  – resolve the artifact encoding issue
  – finalize the signing strategy
  – clean up loose ends

• Which WG should adopt it?
  – Note: the zerotouch draft has a normative reference to this draft, but it is expected that drafts in other working groups will as well shortly.

Comments / Questions?