ALLDISPATCH
@IETF121

Identifying and Authenticating Home Servers: Requirements and Solution Analysis

draft-rbw-home-servers

Tirumaleswar Reddy (Nokia), Mohamed Boucadair (Orange), Dan Wing (Cloud Software)

Motivation

Secure connection to servers on home network
Difficult to use ACME for certificate signing
- *Firewall rules, NAT*
- *Running HTTP or DNS*
- *DNS domain name*

Existing techniques rely on vendor
- *Vendors abandon products*
- *Vendors go out of business*
- *Even for cars! Worse for IoT and printers*

draft-rbw-home-servers: requirements and existing solutions

Background

Today, users have to trust self-signed certificate
Encourages harmful security practice
Existing IETF solutions not embraced by vendors or users

Early motivation was draft-rbw-add-encrypted-dns-forwarders
Overall problem is beyond scope of ADD

Requirements & Analysis

- *Key Requirements*

Reduce the use of a public Certification Authorities	**Existing support client libraries or client software instances**
Eliminate using Certification Authorities for each device	**Existing support by Certification Authorities**

- *Analyzed Solutions*

Normal Certificates	**Delegated Credentials**	**Name Constraints**	**ACME Delegated Certificates**
Raw Public Keys	**Self-signed Certificates**	**Matter**	**Local Certification Authority**

Hoped-for dispatching outcome

Recommendation to hold a full BOF