Category: guidelines document
Status: DRAFT
Document: DCVOTA-Secured-Infra-AP-1.1.docx
Editor: Derek Simmel, dsimmel@psc.edu
Last updated: Thu, 06 February 2025
Total number of pages: 2

Domain-Control-Validation-Only Trust Assurance with Secured Infrastructure

Abstract

This is an Authentication Profile of the IGTF describing the minimum requirements on X.509 PKI authorities issuing certificates for systems and online services identified by their Internet Domain Name, where the domain control vetting is adequate to ensure unique, non-re-assigned certificate subjects, and generated by authorities using secured and trusted infrastructure. Such authorities are not required to collect more data than are necessary for fulfilling the uniqueness requirements, and credentials issued by authorities under this profile may not provide sufficient information to independently trace individual subscribers and should be used in conjunction with complementary identification and vetting processes.

This document is a TAGPMA Guidelines Document, to be referred to as the “Guidelines on Domain-Control-Validation-Only Trust Assurance with Secured Infrastructure Authentication Profile”, with OID 1.2.840.113612.5.2.2.7.1.

Table of Contents

Identifier-Only Trust Assurance with Secured Infrastructure 1
1 Abstract 2
2 General Architecture 2

1 Abstract

This is an Authentication Profile of the IGTF describing the minimum requirements on X.509 PKI authorities issuing certificates for systems and online services identified by their Internet Domain Name, where the domain control vetting is adequate to ensure unique, non-re-assigned certificate subjects, and generated by authorities using secured and trusted infrastructure. Such authorities are not required to collect more data than are necessary for fulfilling the uniqueness requirements. Credentials issued by authorities under this profile may be unable to provide sufficient information to independently trace individual subscribers and should be used in conjunction with complementary identification and vetting processes.

This Authentication Profile is managed by TAGPMA.

2 General Architecture

Authorities accredited under this IGTF "DCVOTA" profile, identified as 1.2.840.113612.5.2.2.7, must comply with the latest endorsed version of

- the IGTF Level of Identity Assurance ELM (1.2.840.113612.5.2.5.5); and
- the IGTF PKI Technology Guidelines (1.2.840.113612.5.2.7).
    - Of particular note for DCVOTA: Section 4.4 of the IGTF PKI Guidelines states,

      For end-entity certificates issued to network and service entities with an extended validity period due to the organisational sub-domain name ownership also having been validated, the ability to act as a client (i.e., extendedKeyUsage 'TLSWebClient') must not be asserted.

      This means that end-entity certificates MUST include the *extendedKeyUsage* extension, and that the values for *extendedKeyUsage* MUST NOT include *clientAuth* (SSL/TLS WWW Client Authentication). This requirement exists to inhibit misuse of such credentials for unintended purposes.