1 Introduction

In the recent past fundamental design flaws in the DNS protocol have been exposed\(^1\).

DNSCurve\(^2\) is a proposal to address these fundamental problems. It promises to guarantee confidentiality and integrity of DNS traffic, as well as protect against attacks on service availability. It should be possible to add DNSCurve functionality unobtrusively: as a forwarder to front DNS servers, and as a recursive DNS-resolver for DNS clients.

2 Goal

Achieve a deep grasp of DNSCurve, and a clear and concrete path for DNSCurve adoption.

3 Task

Analyze the DNSCurve architecture, implementation status and issues, inventarize implementation and deployment requirements, and discuss a 'governance model' that encourages widespread DNSCurve deployment.

\(^{1}\)ON2IT b.v., Waardenburg, The Netherlands.
\(^{1}\)Widely reported as the "Kaminsky Bug".
\(^{2}\)See http://dnscurve.org/.