

DNSSCurve Analysis

J. Scheerder*

jeroenscheerder@on2it.eu

November 7, 2008

1 Introduction

In the recent past fundamental design flaws in the DNS protocol have been exposed¹.

DNSSCurve² 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 DNSSCurve 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 DNSSCurve, and a clear and concrete path for DNSSCurve adoption.

3 Task

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

*ON2IT b.v., Waardenburg, The Netherlands.

¹Widely reported as the "Kaminsky Bug".

²See <http://dnscurve.org/>.