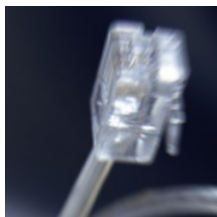


12 November 2008

By: Marius Oiaga, Technology News Editor



Windows 7 comes with more than just basic support for the DNS Security Extensions (DNSSEC)

[Windows 7 Domain Name System](#)

More than just basic support for the DNS Security Extensions (DNSSEC)

[Windows 7](#) and Windows 7 Server (Windows Server 2008 R2) are due to come, bringing to the table enhancements designed to increase the security of Domain Name System (DNS) infrastructures. In this regard, DNS Security Extensions (DNSSEC) proposes a solution for delivering increased protection. Testing DNSSEC at this point in time is rather simple, since Microsoft made available the bits for [Windows 7 pre-Beta Build 6801](#) at the Professional Developers Conference 2008 and at the Windows Hardware Engineering Conference 2008.

"DNSSEC is a suite of security extensions to the DNS, which provide origin authority, data integrity and authenticated denial of existence. Putting that in plain English, DNSSEC allows for a DNS zone to be cryptographically signed (which produces digital signatures), and provides a mechanism for validating the authenticity of the data received using these digital signatures. Validating resolvers and servers must be pre-configured with a Trust Anchor, using which a 'chain of trust' will be established to the signed zone. Data from this signed zone can then be validated," explained [Shyam Seshadri](#), program manager, Windows Core Networking.

Seshadri refers to the Windows 7 DNS client as a non-validating security-aware stub resolver. This means that, in the successor of Windows Vista, the DNS client is intimately connected with the DNS server. Because the client is unable of performing DNSSEC validation on its own, it has to turn to the server for this specific task.

"One positive side-effect of this is that Trust Anchors do not need to be configured on the clients, thus saving a big chunk of the deployment burden. It is, however, security-aware, so it will expect the configured DNS server to indicate results of the validation when returning the response. This is done so by setting the 'AD' bit in the response. If the DNS server failed to validate successfully (indicated by the AD bit not being set in the response), the DNS client will fail the query," Seshadri [added](#).

In its turn, the DNS server is not only capable of generating keys, but also of taking advantage of a sign-tool in order to sign DNS zones.