

DNSSEC in Windows

33rd ICANN Meeting
Cairo, Egypt

Shyam Seshadri
([sseshad\(at\)microsoft.com](mailto:sseshad@microsoft.com))
Program Manager
Microsoft Corporation

DNS Security

- Instances of DNS exploits increasing
- In many cases, patches are just a stop-gap
- DNSSEC for the long run...
 - Microsoft recognizes the important role that DNSSEC will play in securing the DNS in the coming years

Announcing DNSSEC in Windows

- DNSSEC support as per RFCs 4033, 4034 & 4035 in
 - Windows Server 2008 R2 DNS Server
 - Windows 7 / Windows Server 2008 R2 DNS Client
- Solution can integrate with
 - IPsec
 - Group Policy
- Allows for compliance with security controls proposed by the US Govt. in NIST SP 800-53

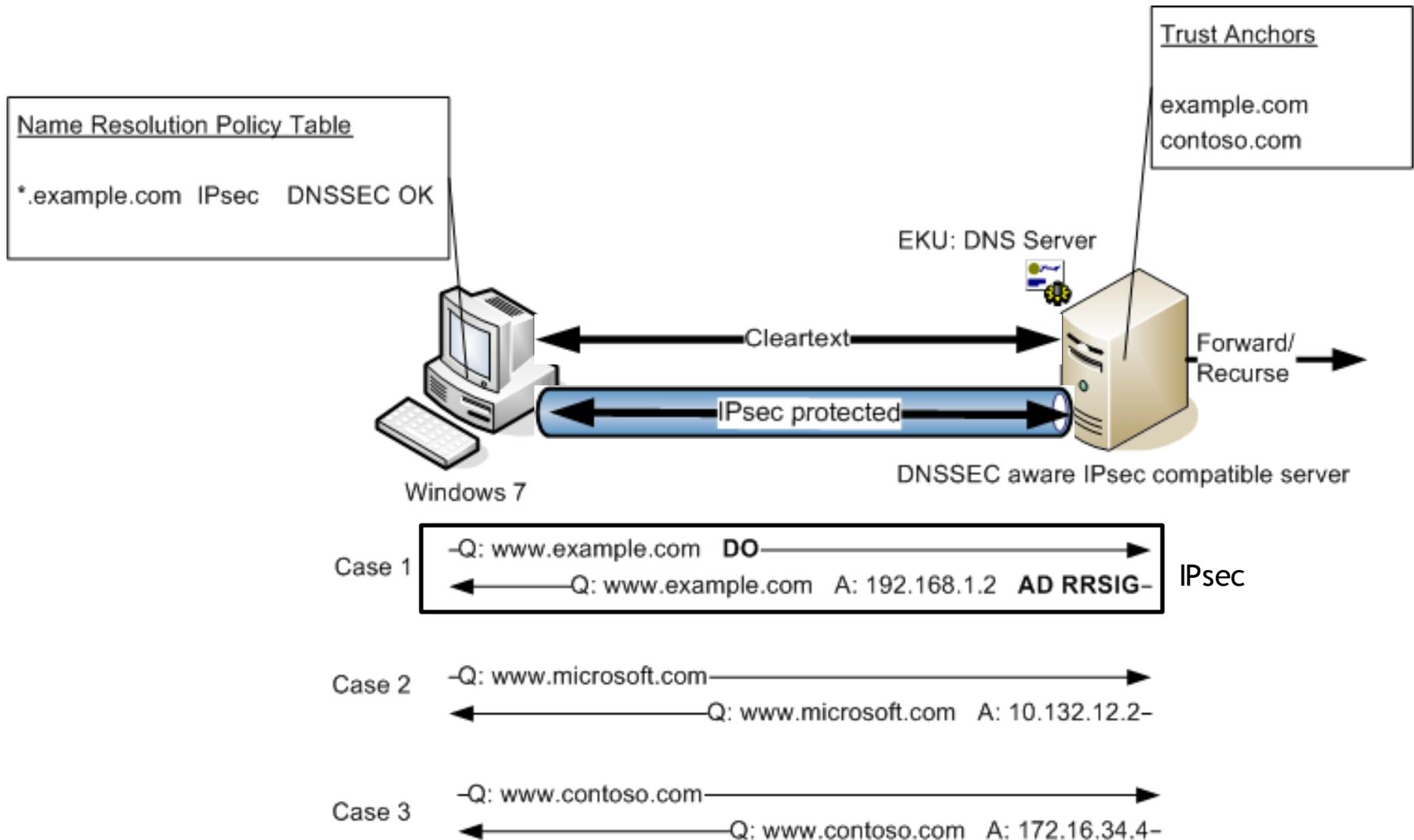
Implementation Overview

- DNSSEC on Windows DNS Server
 - Sign zones using offline sign-tool
 - Configure and manage trust anchors; build chain of trust
 - DNSSEC validation as per RFC
- DNSSEC on Windows DNS Client
 - Non-validating security-aware stub resolver
 - Policy based; relies on DNS server for validation
- Last-hop security
 - Use of IPsec to secure last-hop communication is strongly recommended

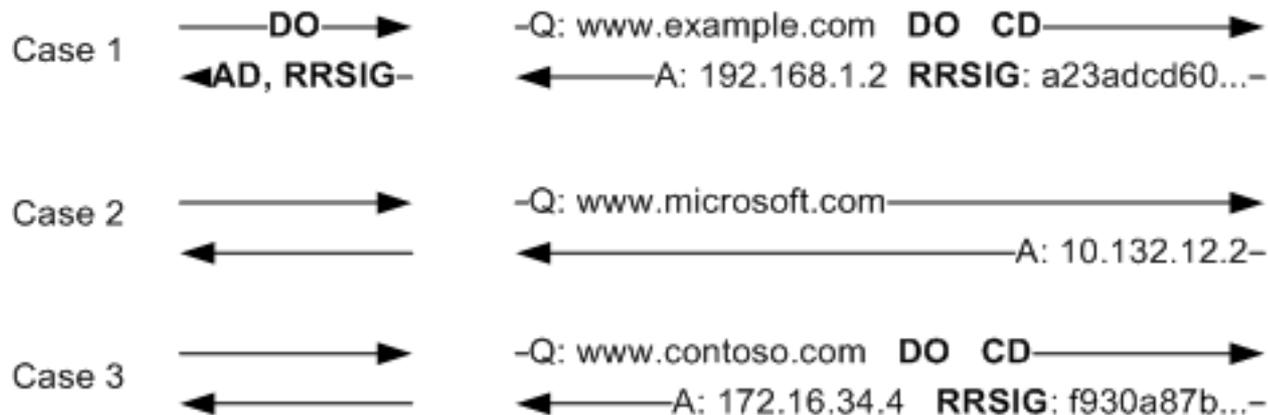
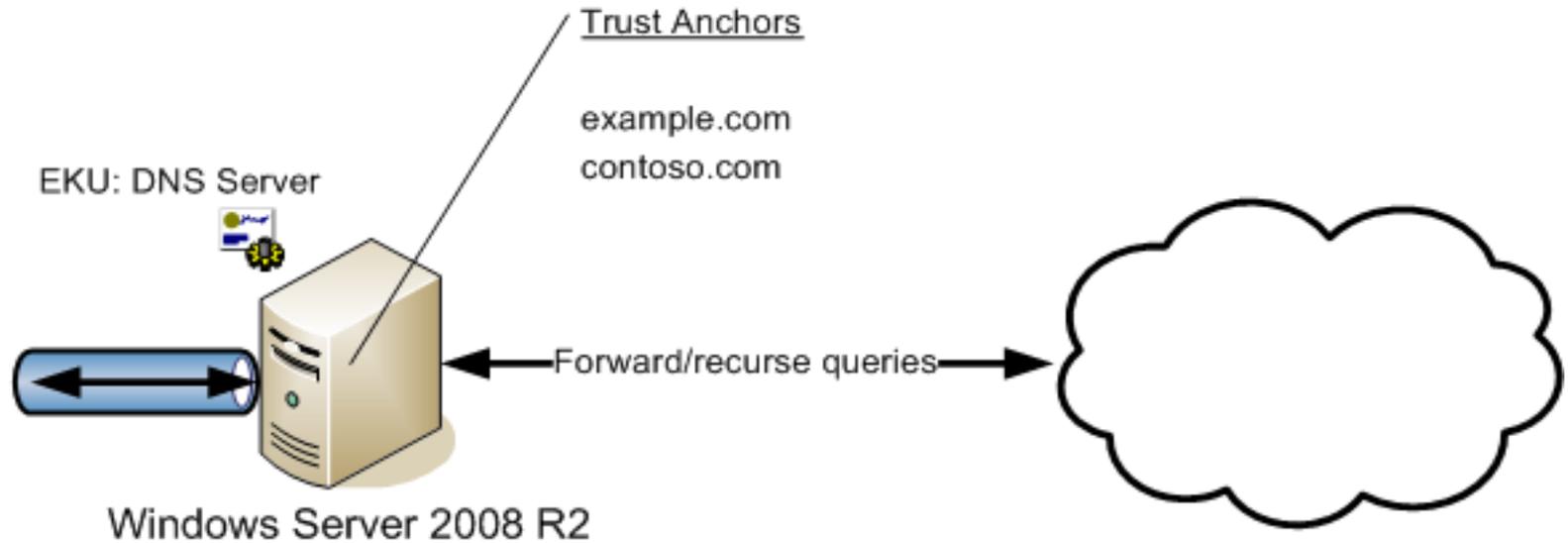
Implementation Examples

	Client policy	Server TA	Wire behavior
Case 1 www.example.com	Set DO/check AD Use IPsec	TA for *.example.com	-- Client sets DO bit -- Server performs validation; returns RRSIGs and sets AD bit -- Client checks AD bit in response
Case 2 www.microsoft.com	Don't set DO	No TA for *.microsoft.com	-- Client does not set DO bit -- Server does not perform validation
Case 3 www.contoso.com	Don't set DO	TA for *.contoso.com	-- Client does not set DO bit -- Server performs validation; does not return RRSIGs or set AD bit -- Client does not check for AD bit in response

Implementation Example: DNS Client



Implementation Example: DNS Server



Interoperability

- Interop with non-Microsoft DNS servers and clients is key
 - Focus of our pre-Beta and Beta testing
- More interop testing...

Roadmap

- Pre-release availability
 - Pre-Beta builds made available to participants of
 - Microsoft PDC 2008 [Oct 27-30]
 - Microsoft WinHEC 2008 [Nov 5-7]
- General availability
 - Windows Server 2008 R2 and Windows 7 to be available approx. three years after Vista

Contacting us...

- The DNS team @ Microsoft

- [dnscore\(at\)microsoft.com](mailto:dnscore@microsoft.com)
- www.microsoft.com/dns

- Shyam Seshadri

- [sseshad\(at\)microsoft.com](mailto:sseshad@microsoft.com)
- blogs.technet.com/sseshad

Q&A



Microsoft[®]

Your potential. Our passion.[™]

©2008 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.