[MS-GPNRPT]:
Group Policy:
Name Resolution Policy Table (NRPT) Data Extension

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: http://www.microsoft.com/interop/osp) or the Community Promise (available here: http://www.microsoft.com/interop/cp/default.mspx). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
08/27/2010	0.1	New	Released new document.
10/08/2010	0.1	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	0.1	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	0.1	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	0.1	No change	No changes to the meaning, language, or formatting of the technical content.

Contents

1 Introduction

This document specifies the Name Resolution Policy Table (NRPT) Group Policy Data Extension, an extension to Group Policy: Registry Extension Encoding [MS-GPREG]. The NRPT Group Policy Data Extension provides a mechanism for an administrator to control any **Name Resolution Policy** behavior on a client by using group policy-based settings.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

Active Directory
administrative template
Advanced Encryption Standard (AES)
certificate authority (CA)
client computer (2)
client-side extension GUID (CSE GUID)
Data Encryption Standard (DES)
domain
domain name (3)
Domain Name System (DNS)
fully qualified domain name (FQDN) (1)
globally unique identifier (GUID)
Group Policy object (GPO)
Group Policy object (GPO) path
IPv4 address in string format
IPv6 address in string format
NetBIOS
policy setting
registry
registry policy file
tool extension GUID or administrative plug-in GUID
Unicode
user-scoped Group Policy object path

The following terms are specific to this document:

Direct Access (DA): A collection of different component policies including **Name Resolution Policy** and IPsec, which allows seamless connectivity to corporate resources when not physically connected to the corporate network.

Name Resolution Policy: **Policy settings** that control how **client** name resolution is performed for a given **DNS** domain or hostname.

Name Resolution Policy Table (NRPT): The collection of Name Resolution Policy settings that apply to a given client.

Network Location: The physical location of a client that indicates whether it is connected to a domain, public, or private network.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-GPOL] Microsoft Corporation, "Group Policy: Core Protocol Specification", June 2007.

[MS-GPREG] Microsoft Corporation, "Group Policy: Registry Extension Encoding", August 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.ietf.org/rfc/rfc2119.txt

[RFC5280] Cooper, D., Santesson, S., Farrell, S., et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008, http://www.ietf.org/rfc/rfc5280.txt

1.2.2 Informative References

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary", March 2007.

[MS-HNDS] Microsoft Corporation, "Host Name Data Structure Extension", October 2008.

[RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987, http://www.ietf.org/rfc/rfc1034.txt

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and Souissi, M., "DNS Extensions to Support IP version 6", RFC 3596, October 2003, http://www.ietf.org/rfc/rfc3596.txt

1.3 Protocol Overview (Synopsis)

The Name Resolution Policy Table (NRPT) Group Policy Data Extension provides a mechanism for an administrator to control Name Resolution Policy behavior of the **client** through group policy by using the Group Policy: Registry Extension Encoding [MS-GPREG].

1.3.1 Background

The Group Policy: Core Protocol (as specified in [MS-GPOL]) allows clients to discover and retrieve **policy settings** created by administrators of a **domain**. These settings are persisted within **Group Policy objects (GPOs)** that are assigned to Policy Target accounts in the **Active Directory**. On each client, each GPO is interpreted and acted upon by software components known as client plug-ins. The client plug-ins responsible for a given GPO are specified using an attribute on the GPO. This attribute specifies a list of **globally unique identifier (GUID)** lists. The first GUID of each GUID list is referred to as a **client-side extension GUID (CSE GUID)**. Other GUIDs in the GUID list are referred to as **tool extension GUIDs**. For each GPO that is applicable to a client, the client consults the CSE GUIDs listed in the GPO to determine which client plug-in on the client should handle the GPO. The client then invokes the client plug-in to handle the GPO.

Registry-based settings are accessible from a GPO through the Group Policy: Registry Extension Encoding protocol [MS-GPREG], which is a client plug-in. The protocol provides mechanisms both for administrative tools to obtain metadata about registry-based settings and for clients to obtain applicable registry-based settings.

Group Policy: Registry Extension Encoding settings are specified using **registry policy files** (as specified in [MS-GPREG] section 2.2.1). An administrative tool uses the information within the **administrative template** to write out a registry policy file and associate it with a GPO. The Group Policy: Registry Extension Encoding plug-in on each client reads registry policy files specified by applicable GPOs and applies their contents to its registry.

1.3.2 Name Resolution Policy Table Extension Encoding Overview

Name Resolution Policy Table policies are configurable from a GPO through the Name Resolution Policy Table Group Policy Data Extension, which uses the {f4d8c39a-f43d-42b4-9bdf-4e48d3044ba1} tool extension GUID. The protocol provides mechanisms both for Group Policy administrators to deploy policies and for clients to obtain the applicable policies to enforce them. The Name Resolution Policy Table component has complex settings not expressible through administrative templates, and for this reason it implements a custom UI that can author registry policy files containing the encodings of the settings described in this document. Given that the Name Resolution Policy Table policies are applied to the whole machine, the NRPT Group Policy Data Extension protocol uses the Computer Policy Mode described in [MS-GPREG] section 1.3.2.

Name Resolution Policy Table policies are applied as follows:

1. An administrator invokes a Group Policy Name Resolution Policy Table administrative tool on the administrator's computer to administer a Group Policy object (GPO) through Group Policy Protocol using the Policy Administration mode, as specified in [MS-GPOL] section 2.2.7. The administrative tool invokes a plug-in specific to Group Policy: Registry Extension Encoding so that the administrator can administer the Group Policy: Name Resolution Policy Table Data Structure transported over the Group Policy: Registry Extension Encoding data. This results in the storage and retrieval of metadata inside a GPO on a Group Policy server. This metadata describes configuration settings to be applied to the registry on a client that is affected by the GPO. The administrator views the data and updates it to add a directive to run a command when the client computer starts up. If they are not already present from a prior update, the CSE GUID and tool extension GUID for Computer Policy Settings for Group Policy: Registry Extension Encoding are written to the GPO.

2. A client computer affected by that GPO is started (or is connected to the network, if this happens after the client starts), and Group Policy Protocol is invoked by the client to retrieve Policy Settings from the Group Policy server. As part of the processing of Group Policy Protocol, the Group Policy: Registry Extension Encoding's CSE GUID is read from this GPO, and this instructs the client to invoke a Group Policy: Registry Extension Encoding plug-in component for Policy Application.

3. In processing the Policy Application portion of Group Policy: Registry Extension Encoding, the client parses the settings and then saves the settings in the registry on the local computer and notifies the Name Resolution Policy client component. The NRPT policies are stored in local storage.

4. The NRPT Group Policy Data Extension is invoked for policy application. To apply the policies, the Name Resolution Policy component parses its previously stored settings in local storage.

1.4 Relationship to Other Protocols

This protocol depends on the Group Policy: Registry Extension Encoding (as specified in [MS-GPREG]) to transport the Name Resolution Policy Table Group Policy Data Extension settings. The protocol also has all the dependencies inherited from Group Policy: Registry Extension Encoding.

1.5 Prerequisites/Preconditions

The prerequisites for this protocol are the same as those for the Group Policy: Registry Extension Encoding ([MS-GPREG]).

In addition, a client must have a system/subsystem capable of executing commands at startup/shutdown time because the Computer Policy Mode of the Group Policy: Registry Extension Encoding is used.

1.6 Applicability Statement

The NRPT Group Policy Data Extension is applicable only while transported under the Group Policy: Registry Extension Encoding and within the Group Policy: Core Protocol framework. The Group Policy: Name Resolution Policy Table Data Structure should be used to express the required Name Resolution Policy Table policy of the client.

The NRPT Group Policy Data Extension should not be used in any other context.

1.7 Versioning and Capability Negotiation

The Group Policy: Name Resolution Policy Table Data Structure has a policy version (also called schema version), but the protocol currently defines a single version with a value of 1.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

Parameter	Value
Tool extension GUID	{f4d8c39a-f43d-42b4-9bdf-4e48d3044ba1}
Policy Base registry key	Software\Policies\Microsoft\Windows NT\DNSClient

2 Messages

2.1 Transport

The Name Resolution Policy Table Group Policy Data Extension requires Group Policy: Registry Extension Encoding. All messages are exchanged in registry policy files encoded using Group Policy: Registry Extension Encoding.

2.2 Message Syntax

2.2.1 Global Policy Configuration Options

The Global Policy Configuration Options specify name resolution behavior that applies to all entries within the NRPT.

For information about the Type values, see [MS-GPREG] section 2.2.1.

2.2.1.1 Enable DA for All Networks

Key: Software\Policies\Microsoft\Windows NT\DNSClient

Value: "EnableDAForAllNetworks"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	Let Network ID determine when Direct Access settings are to be used.
0x00000001	Always use Direct Access settings regardless of location.
0x00000002	Never use Direct Access settings regardless of location.

2.2.1.2 DNS Secure Name Query Fallback

Key: Software\Policies\Microsoft\Windows NT\DNSClient

Value: "DnsSecureNameQueryFallback"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	Only use Link-Local Multicast Name Resolution (LLMNR) and **NetBIOS** if the name does not exist in **DNS**.

Value	Meaning
0x00000001	Always fall back to LLMNR and NetBIOS for any kind of name resolution error.
0x00000002	Always fall back to LLMNR and NetBIOS if the name does not exist in DNS or if the DNS servers are unreachable when on a private network.

2.2.1.3 Direct Access Query Order

Key: Software\Policies\Microsoft\Windows NT\DNSClient

Value: "DirectAccessQueryOrder"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	Resolve only IPv6 addresses.
0x00000001	Resolve both IPv4 and IPv6 addresses.

2.2.2 Name Resolution Policy Messages

The Name Resolution Policy Table consists of one or more Name Resolution Policy keys under Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig. The format of these sub-keys is Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N> where N is an integer count starting at 1 that corresponds to each rule defined in the Group Policy Name Resolution Policy Table administrative tool.

2.2.2.1 Name

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "Name"

Type: REG_MULTI_SZ.

Size: Equal to the size of the **Data** field.

Data: One or more **Unicode** string names, each of which MUST be either a DNS suffix, a DNS prefix, a **fully qualified domain name (FQDN)**, an IPv4 subnet formatted as specified in [RFC1034], section 3.6.2, or an IPv6 subnet formatted as specified in [RFC3596] section 2.5.

Each DNS suffix present MUST consist of a "." character with a domain name appended. Each DNS prefix present MUST be constructed according to the "name" rule specified in [MS-HNDS] section 2.1.

2.2.2.2 Config Options

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000002	Only DNSSEC options (that is, options defined in sections 2.2.2.4, 2.2.2.5, 2.2.2.6, and 2.2.2.7) are specified.
0x00000004	Only DA options (that is, options defined in sections 2.2.2.8, 2.2.2.9, 2.2.2.10, 2.2.2.11, and 2.2.2.12) are specified.
0x00000006	Both DNSSEC and DA options are specified.

2.2.2.3 Version

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "Version"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value specifying the Name Resolution Policy version. Its value MUST be 0x00000001.

2.2.2.4 DNSSEC Query IPsec Encryption

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "DNSSECQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	No encryption (integrity only) necessary when IPsec protection is used for DNSSEC queries.
0x00000001	Low security encryption, which includes **DES** or **AES** with key size of 128, 192, or 256 bits, is to be used when IPsec protection is used for DNSSEC queries.
0x00000002	Medium security encryption, which includes AES with key size of 128, 192, or 256 bits, is to be used when IPsec protection is used for DNSSEC queries.
0x00000003	High security encryption, which includes AES with key size of 192 or 256 bits, is to be used when IPsec protection is used for DNSSEC queries.

2.2.2.5 DNSSEC Query IPsec Required

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "DNSSECQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	IPsec is not required for DNS queries.
0x00000001	IPsec is required for DNS queries.

2.2.2.6 DNSSEC Validation Required

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "DNSSECValidationRequired"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	DNSSEC validation is not required for DNS queries.
0x00000001	DNSSEC validation is required for DNS queries.

2.2.2.7 IPsec CA Restriction

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "IPSSECCARestriction"

Type: REG_SZ.

Size: Equal to the size of the **Data** field.

Data: A Unicode string specifying the **Certificate Authority** in X509 format [RFC5280].

2.2.2.8 Direct Access DNS Servers

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "DirectAccessDNSServers"

Type: REG_SZ.

Size: Equal to the size of the **Data** field.

Data: A semicolon-delimited Unicode string of IP addresses or names of DNS servers used for internal name resolutions by **Direct Access** clients. Each IP address item in the string MUST be

either an **IPv4 address in string format** or an **IPv6 address in string format**. Each name in the string MUST be an extended hostname as specified in [MS-HNDS].

2.2.2.9 Direct Access Proxy Name

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "DirectAccessProxyName"

Type: REG_SZ.

Size: Equal to the size of the **Data** field.

Data: A Unicode string specifying the HTTP proxy name and port in the format "proxy:port" where "proxy" MUST be either an extended hostname as specified in [MS-HNDS] section 2.1, an IPv4 address in string format, or an IPv6 address in string format; "port" MUST be a decimal integer between 1 and 65535.

2.2.2.10 Direct Access Proxy Type

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "DirectAccessProxyType"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	No proxy configured.
0x00000001	Use the default proxy.
0x00000002	Use the proxy specified by the Direct Access Proxy Name (see section 2.2.2.9).

2.2.2.11 Direct Access Query IPsec Encryption

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "DirectAccessQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	No encryption (integrity only) required for IPsec protection of DNS queries.
0x00000001	Low security, which includes DES or AES with key size of 128, 192, or 256 bits, required for IPsec protection of DNS queries.

Value	Meaning
0x00000002	Medium security, which includes AES with key size of 128, 192, or 256 bits, required for IPsec protection of DNS queries.
0x00000003	High security, which includes AES with key size of 192 or 256 bits, required for IPsec protection of DNS queries.

2.2.2.12 Direct Access Query IPsec Required

Key: Software\Policies\Windows\Windows NT\DNSClient\DnsPolicyConfig\Rule <N>

Value: "DirectAccessQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain of one of the following values.

Value	Meaning
0x00000000	IPsec protection is not required for DNS queries.
0x00000001	IPsec protection is required for DNS queries.

3 Protocol Details

3.1 Administrative Plug-in Details

The administrative plug-in mediates between the user interface (UI) and a remote data store that contains Name Resolution Policy Table group policy extension settings. Its purpose is to receive Name Resolution Policy Table group policy information from a UI and to write the same policy information to a remote data store.

The NRPT Group Policy Data Extension administrative plug-in relies on a collection of settings specified in section 2.2 and stored as a Unicode configuration file ([MS-GPREG] section 2.2) at a remote storage location using the Group Policy: Core Protocol. The administrative plug-in parses and encodes these settings as specified in section 2.2 to perform its functions.

The NRPT Group Policy Data Extension administrative plug-in reads in these settings from the remote storage location and displays them to an administrator through a UI.

An administrator can then use the UI to make further configuration changes, and the NRPT Group Policy Data Extension administrative plug-in will make corresponding changes to the name-value pairs stored in the aforementioned Unicode configuration file following the conventions of the keys specified in section 2.2.

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

The NRPT Group Policy Data Extension administrative plug-in is invoked when an administrator launches the user interface for editing Group Policy settings. The plug-in displays the current settings to the administrator, and when the administrator requests a change in settings, it updates the stored configuration appropriately as specified in section 2.2, after performing additional checks and actions as noted in this section.

The administrative plug-in SHOULD<1> take measures in its UI to ensure that the user cannot unknowingly set the Name Resolution Policy Table Group Policy settings to an invalid value.

3.1.5 Processing Events and Sequencing Rules

The NRPT Group Policy Data Extension administrative plug-in reads extension-specific data from the remote storage location and will then pass that information to a UI to display the current settings to an administrator.

It will also write the extension-specific configuration data to the remote storage location if the administrator makes any changes to the existing configuration.

Any additional entries in the configuration data that do not pertain to the configuration options specified in section 2.2, or that are not supported by the particular implementation, MUST be ignored by the plug-in.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

4 Protocol Examples

4.1 Global Policy Configuration Messages

The following is an example of Name Resolution Policy global options to query for both IPv4 and IPv6, always allow fallback to LLMNR and NetBIOS, and to enable Name Resolution Policy behavior only when not physically connected to the corporate network.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient

Value: "DirectAccessQueryOrder"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "DnsSecureNameQueryFallback"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "EnableDAForAllNetworks"

Type: REG_DWORD

Size: 32 bits.

Data: 00000000

4.2 Name Resolution Policy Messages

The following are examples of individual Name Resolution Policy entries specifying DNSSEC, Direct Access, and both.

4.2.1 Direct Access

The following is an example of a Name Resolution Policy entry to apply Direct Access for names under the da.example.com domain. The policy specifies the DNS servers to query and requires IPsec with medium encryption but no CA restriction or proxy.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\Rule2

Value: "Version"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "Name"

Type: REG_MULTI_SZ.

Size: Equal to the size of the data field.

Data: ".da.example.com"

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits.

Data: 00000004

Value: "DirectAccessDNSServers"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: "10.1.1.1;10.2.2.2"

Value: "DirectAccessProxyName"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: ""

Value: "DirectAccessProxyType"

Type: REG_DWORD

Size: 32 bits.

Data: 00000000

Value: "DirectAccessQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: 00000002

Value: "DirectAccessQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "IPSECCARestriction"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: ""

4.2.2 DNSSEC

The following is an example of a Name Resolution Policy entry to apply DNSSEC for names under the dnssec.example.com domain. The policy requires DNSSEC validation, IPsec with medium encryption, and a specific CA.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\Rule1

Value: "Version"

Type: REG_DWORD

Size: 32 bits.

Data: 1

Value: "Name"

Type: REG_MULTI_SZ.

Size: Equal to the size of the data field.

Data: ".dnssec.example.com"

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits.

Data: 00000002

Value: "DNSSECQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: 00000002

Value: "DNSSECQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "DNSSECValidationRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "IPSSECCARestriction"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: 'C=US, O="VeriSign, Inc.", OU=Class 3 Public Primary Certification Authority - G2, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network'

4.2.3 Both Direct Access and DNSSEC

The following is an example of a Name Resolution Policy entry to apply both Direct Access and DNSSEC for names under the both.example.com domain. For DNSSEC, the policy requires DNSSEC validation, IPsec with high encryption, and a specific CA. For Direct Access, it specifies DNS servers for DA, requires IPsec with high encryption, and specifies a proxy.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\Rule6

Value: "Version"

Type: REG_DWORD

Size: 32 bits.

Data: 1

Value: "Name"

Type: REG_MULTI_SZ.

Size: Equal to the size of the data field.

Data: ".both.example.com"

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits.

Data: 00000006

Value: "DirectAccessDNSServers"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: "10.1.1.1"

Value: "DirectAccessProxyName"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: "exampleproxy:80"

Value: "DirectAccessProxyType"

Type: REG_DWORD

Size: 32 bits.

Data: 00000002

Value: "DirectAccessQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: 00000003

Value: "DirectAccessQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "DNSSECQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: 00000003

Value: "DNSSECQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "DNSSECValidationRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "IPSSECCARestriction"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: 'C=US, O="VeriSign, Inc.", OU=Class 3 Public Primary Certification Authority - G2, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network'

5 Security

5.1 Security Considerations for Implementers

Implementers SHOULD NOT transmit passwords or other sensitive data through this protocol. The primary reason for this restriction is that the protocol provides no encryption, and therefore sensitive data transmitted through this protocol can be intercepted easily by an unauthorized user with access to the network carrying the data. For example, if a network administrator configured a Group Policy: Registry Extension Encoding setting in a GPO to instruct a computer to use a specific password when accessing a certain network resource, this protocol would send that password unencrypted to those computers. A person gaining unauthorized access, intercepting the protocol's network packets in this case, would then discover the password for that resource, which would then be unprotected from the unauthorized person.

5.2 Index of Security Parameters

None.

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Windows® 7 operating system
- Windows Server® 2008 R2 operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

<1> Section 3.1.4: Windows administrative tools verify the validity of the objects as defined in section 2.2 before writing them to the remote store through Group Policy: Registry Extension Encoding.

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index

P

R

S

T

V