[MC-DKSP]:
Distributed Routing Table Derived Key Security Profile

Release: Wednesday, January 15, 2014

Revision Summary

Date	Revision History	Revision Class	Comments
12/05/2008	0.1	Major	Initial Availability.
01/16/2009	0.1.1	Editorial	Revised and edited the technical content.
02/27/2009	0.1.2	Editorial	Revised and edited the technical content.
04/10/2009	0.1.3	Editorial	Revised and edited the technical content.
05/22/2009	0.2	Minor	Updated the technical content.
07/02/2009	0.3	Minor	Updated the technical content.
08/14/2009	1.0	Major	Updated and revised the technical content.
09/25/2009	1.1	Minor	Updated the technical content.
11/06/2009	2.0	Major	Updated and revised the technical content.
12/18/2009	2.0.1	Editorial	Revised and edited the technical content.
01/29/2010	2.1	Minor	Updated the technical content.
03/12/2010	2.1.1	Editorial	Revised and edited the technical content.
04/23/2010	2.1.2	Editorial	Revised and edited the technical content.
06/04/2010	2.1.3	Editorial	Revised and edited the technical content.
07/16/2010	2.1.3	No change	No changes to the meaning, language, or formatting of the technical content.
08/27/2010	2.1.3	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	2.1.3	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	2.2	Minor	Clarified the meaning of the technical content.
01/07/2011	3.0	Major	Significantly changed the technical content.
02/11/2011	4.0	Major	Significantly changed the technical content.
03/25/2011	4.0	No change	No changes to the meaning, language, or formatting of the technical content.
05/06/2011	4.0	No change	No changes to the meaning, language, or formatting of the technical content.
06/17/2011	4.1	Minor	Clarified the meaning of the technical content.
09/23/2011	4.1	No change	No changes to the meaning, language, or formatting of

Date	Revision History	Revision Class	Comments
			the technical content.
12/16/2011	5.0	Major	Significantly changed the technical content.
03/30/2012	5.0	No change	No changes to the meaning, language, or formatting of the technical content.
07/12/2012	5.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	5.0	No change	No changes to the meaning, language, or formatting of the technical content.
01/31/2013	5.1	Minor	Clarified the meaning of the technical content.
08/08/2013	6.0	Major	Significantly changed the technical content.
11/14/2013	6.0	No change	No changes to the meaning, language, or formatting of the technical content.

Contents

1 Introduction

The Distributed Routing Table Derived Key Security Profile defines a set of data structures and encryption schemes for authenticating **keys** and securing communication between nodes executing the [MC-DRT]: Distributed Routing Table Protocol. Each node that participates in a cloud of peers configured to use the Distributed Routing Table Derived Key Security Profile must possess a **certificate** signed by a common root in order to publish keys or search for keys if the cloud is executing in membership or confidential security modes.

Sections 1.7 and 2 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in RFC 2119. All other sections and examples in this specification are informative.

1.1 Glossary

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

Abstract Syntax Notation One (ASN.1)
Advanced Encryption Standard (AES)
authentication
certificate
certificate chain
endpoint
Internet Protocol version 6 (IPv6)
key
little-endian
node
nonce
object identifier (OID)
public key
Public Key Cryptography Standards (PKCS)
Rivest-Shamir-Adleman (RSA)
security provider
Unicode string

The following terms are specific to this document:

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

1.2 References

References to Microsoft Open Specifications documentation do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

A reference marked "(Archived)" means that the reference document was either retired and is no longer being maintained or was replaced with a new document that provides current implementation details. We archive our documents online [Windows Protocol].

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.

[MC-DRT] Microsoft Corporation, "Distributed Routing Table (DRT) Version 1.0".

[PKCS1] RSA Laboratories, "PKCS #1: RSA Cryptography Standard", PKCS #1, Version 2.1, June 2002, http://www.rsa.com/rsalabs/node.asp?id=2125

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

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, March 1998, http://www.ietf.org/rfc/rfc2315.txt

[RFC2459] Housley, R., Ford, W., Polk, W., and Solo, D., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999, http://www.ietf.org/rfc/rfc2459.txt

[RFC2553] Gilligan, R., Thomson, S., Bound, J., and Stevens, W., "Basic Socket Interface Extensions for IPv6", RFC 2553, March 1999, http://www.ietf.org/rfc/rfc2553.txt

[RFC3268] Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002, http://www.ietf.org/rfc/rfc3268.txt

[RFC3447] Jonsson, J., and Kaliski, B., "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003, http://www.ietf.org/rfc/rfc3447.txt

[X509] ITU-T, "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks", Recommendation X.509, August 2005, http://www.itu.int/rec/T-REC-X.509/en

Note There is a charge to download the specification.

1.2.2 Informative References

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

1.3 Overview

Each node is authorized to publish a 256-bit key derived from the SHA-2 hash of the **public key** embedded in the certificate that the **node** uses to participate in the cloud. Nodes encrypt communication between each other using 128-bit **Advanced Encryption Standard (AES)** [RFC3268], and they exchange AES keys encrypted using the key pairs embedded in the certificates. Nodes validate that each peer with which they communicate possesses a certificate from the trusted root.

1.4 Relationship to Protocols and Other Structures

The Distributed Routing Table Derived Key Security Profile Specification is a security profile of the [MC-DRT]. The structures and cryptographic techniques described in this document are expected to be used by nodes executing the [MC-DRT] protocol.

1.5 Applicability Statement

The Distributed Routing Table Derived Key Security Profile Specification is appropriate for applications requiring strong key **authentication** and/or wishing to use membership or confidential security modes. These applications must have an out-of-band mechanism for distributing certificates.

1.6 Versioning and Localization

The Distributed Routing Table Derived Key Security Profile Specification structures do not include versioning or localization information.

1.7 Vendor-Extensible Fields

None.

2 Structures

2.1 Credential

A **certificate chain** is a **Public Key Cryptography Standards (PKCS)** 7 version 1.5 message of type SignedData as specified in [RFC2315] section 9.1. It consists of a list of [X509] version 3 certificates.

The total number of certificates in a certificate chain MUST NOT be more than 25.

Each certificate in the chain MUST be an [X509] version 3 [RFC2459] format certificate, with the following constraints on the fields defined in [RFC2459].

The **version** field ([RFC2459] section 4.1.2.1) MUST be set to 2 (version 3).

The **signatureAlgorithm** field ([RFC2459] section 4.1.1.2) MUST be set to the OID 1.2.840.113549.1.1.5.

The **serialNumber** field ([RFC2459] section 4.1.2.2) MUST be present and MUST be exactly 16 bytes long.

The **subjectUniqueID** and **issuerUniqueID** fields ([RFC2459] section 4.1.2.8) MUST be empty with a length of 0 bytes.

The **subjectPublicKeyInfo** field ([RFC2459] section 4.1.2.7) MUST conform to the syntax specified in section 2.2.1.

The **subject** field ([RFC2459] section 4.1.2.6) MUST be a null-terminated **Unicode string** that MUST NOT be longer than 255 characters.

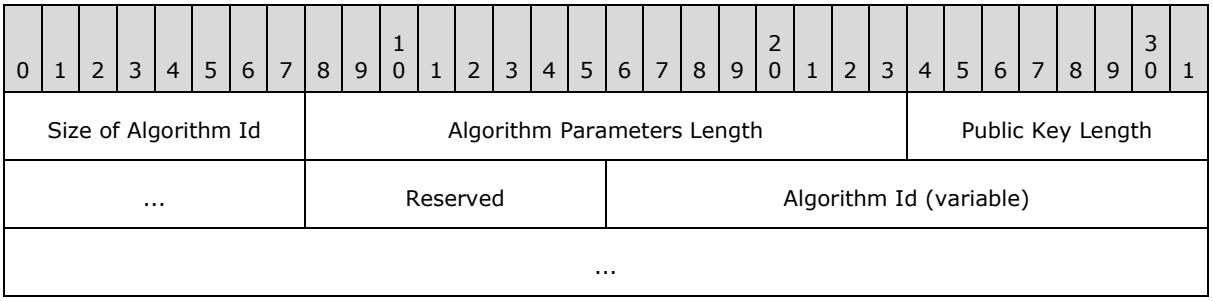
The **issuer** field ([RFC2459] section 4.1.2.4) MUST be a null-terminated Unicode string that MUST NOT be longer than 255 characters.

2.2 Key Identifier

The credential structure contains multiple certificates forming a chain. The Distributed Routing Table Derived Key Security Profile Specification uses the key identifier structure to identify the certificate in the chain used to identify the sender of the message. The Distributed Routing Table Derived Key Security Profile Specification uses the PUBLIC_KEY structure to describe the public key in the target certificate. The PUBLIC_KEY structure described in the following section is used.

2.2.1 PUBLIC_KEY

The PUBLIC_KEY structure contains an encoding of a public key.



Algorithm Parameters (variable)
...
PublicKey Data (variable)
...

Size of Algorithm Id (1 byte): The size, in **little-endian** byte order, of the **Algorithm Id** field, in bytes. MUST be set to 20 bytes.

Algorithm Parameters Length (2 bytes): The size, in little-endian byte order, of the **Algorithm Parameters** field, in bytes.

Public Key Length (2 bytes): The size, in little-endian byte order, of the **PublicKey Data** field, in bytes. MUST be set to 140 bytes.

Reserved (1 byte): MUST be set to 0x00 and ignored on receipt.

Algorithm Id (variable): An ASN.1-encoded **object identifier (OID)** indicating the public key format. MUST be the same as the rsaEncryption, as specified in [RFC3447] section A.1.

Algorithm Parameters (variable): An **ASN.1**-encoded object identifier (OID) indicating the public key format. MUST be the same as the rsaEncryption, as specified in [RFC3447] section A.1.

PublicKey Data (variable): An ASN.1-encoded 1024-bit **RSA** public key, as specified in [RFC3447] section A.1.1.

2.3 SIGNATURE

The SIGNATURE structure carries the encoding of a signature calculated over fields in a [MC-DRT] message.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Length																Signature Data															
...																															
...																															
...																															
...																															
...																															
...																															

...
(Signature Data cont'd for 24 rows)
...

Length (2 bytes): Number of bytes, in little-endian byte order, of the structure. MUST be set to 130 bytes.

Signature Data (128 bytes): Signature data calculated using the RSASSA-[PKCS1]-v1_5 ([RFC3447] section 8.2) algorithm.

2.4 Encoded CPA

The Encoded CPA structure contains information that links an [MC-DRT] service endpoint to a key.

The Encoded Address Payload structure contains information about an **endpoint**.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Reserved								Signature (variable)																							
...																															
Protocol Major Version								Protocol Minor Version								Security Profile Major Version								Security Profile Minor Version							
Key Length																Key															
...																															
...																															
...																															
...																															
...																															
...																															
...																															
...																Nonce Length															
Nonce																															

...
...
...
Public Key (variable)
...
Service Address List (variable)
...

Reserved (1 byte): MUST be set to 0x00 and ignored on receipt.

Signature (variable): A SIGNATURE data structure defined in section 2.3 calculated over all the subsequent fields in the message.

Protocol Major Version (1 byte): The Protocol Major Version defined by the higher-layer application using the DRT.

Protocol Minor Version (1 byte): The Protocol Minor Version defined by the higher-layer application using the DRT.

Security Profile Major Version (1 byte): The major version number of the security profile. Must be set to 0x01.

Security Profile Minor Version (1 byte): The minor version number of the security profile. Must be set to 0x00.

Key Length (2 bytes): Number of bytes, in little-endian byte order, of the **Key** field. MUST be set to 32 bytes.

Key (32 bytes): The key authenticated by this message.

Nonce Length (2 bytes): Number of bytes, in little-endian byte order, of the **Nonce** field. MUST be set to 16 bytes.

Nonce (16 bytes): Must be set to the **nonce** value embedded in the Inquire message used to solicit the Authority message containing this structure.

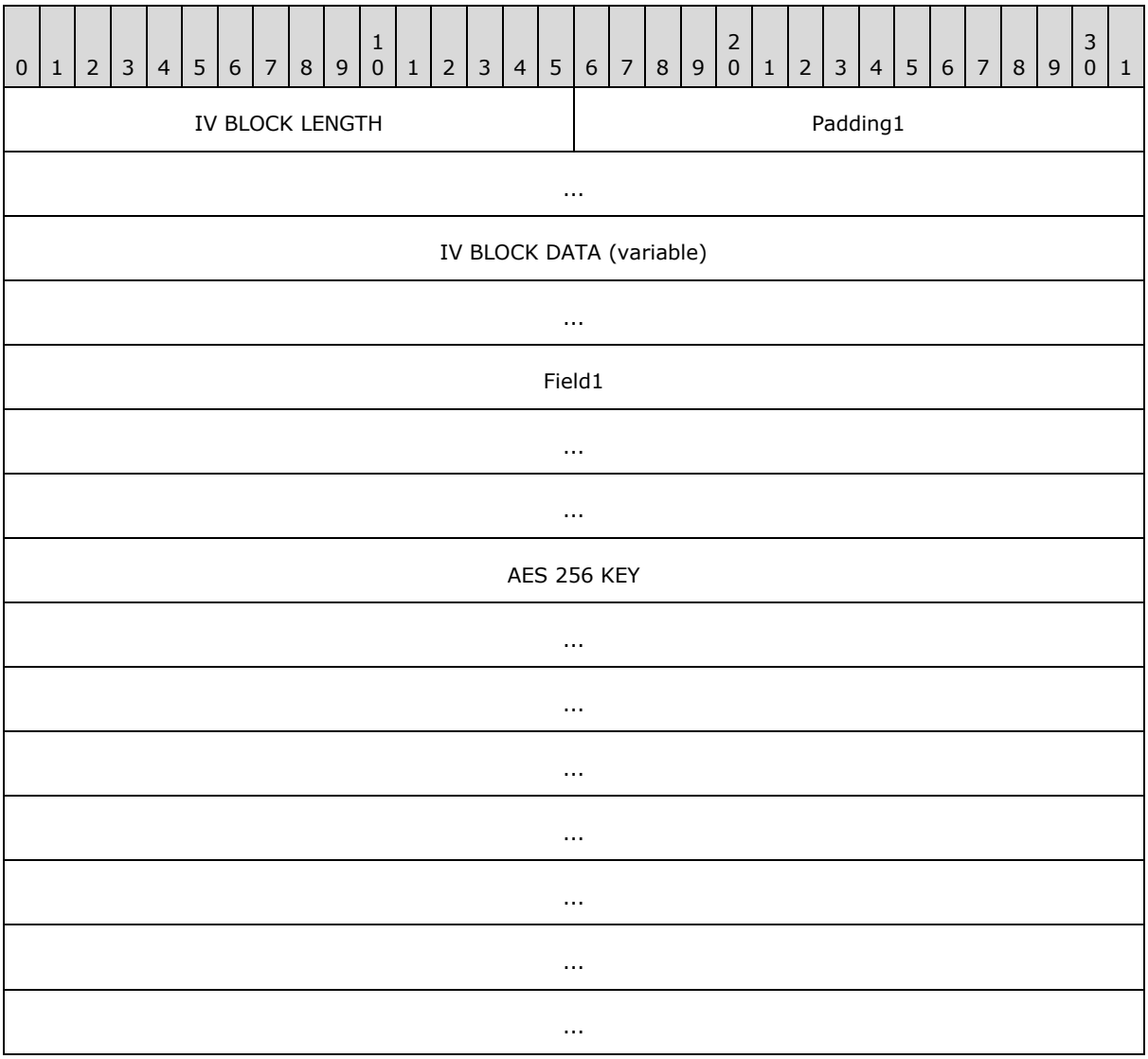
Public Key (variable): A PUBLIC_KEY data structure defined in section 2.2.1.

Service Address List (variable): A Service Address List structure.

2.5 Keytoken

The Keytoken structure is used to decrypt encrypted structures in a [MC-DRT] message.

A Keytoken is returned by all invocations of encryption primitive of the **security provider** by the [MC-DRT]. This Keytoken identifies the key material that is used to decrypt the buffers encrypted specifically for the target node. The following is the unencrypted format of the Keytoken.



IV BLOCK LENGTH (2 bytes): The length of the **IV BLOCK DATA** field.

Padding1 (6 bytes): Must be set to zero and ignored on receipt.

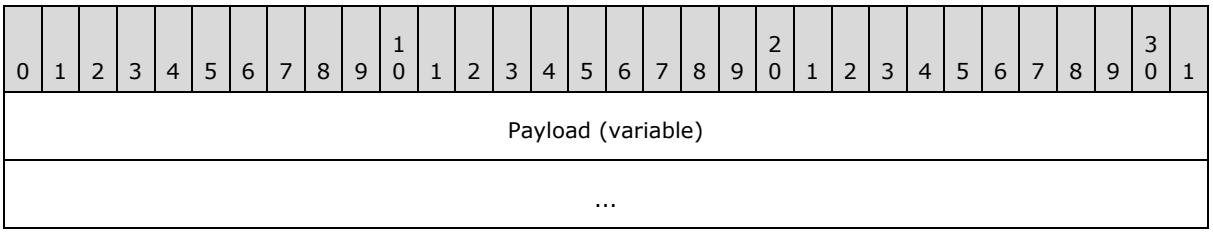
IV BLOCK DATA (variable): This is the random initialization vector passed to each Encrypt operation. This is equal in size to the block size of the encryption algorithm.

Field1 (12 bytes): Must be set to the constant 0x4b44424d0100000020000000.

AES 256 KEY (32 bytes): This is the encryption key used to perform AES256 encryption of the input buffers.

2.6 PAYLOAD

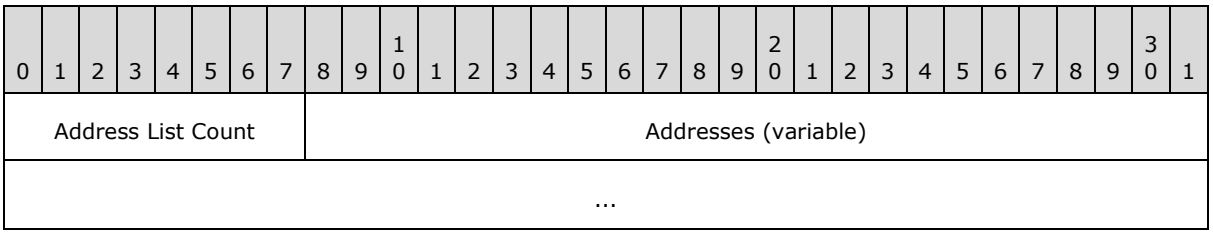
The PAYLOAD structure holds arbitrary binary data supplied by the application associated with a key. This is carried by the [MC-DRT] protocol in the **EXTENDED_PAYLOAD** field.



Payload (variable): Data supplied by the upper-layer application associated with the published key.

2.7 Address List

The Address List is an encoding of the **IPv6** addresses and ports included in an Encoded CPA structure.

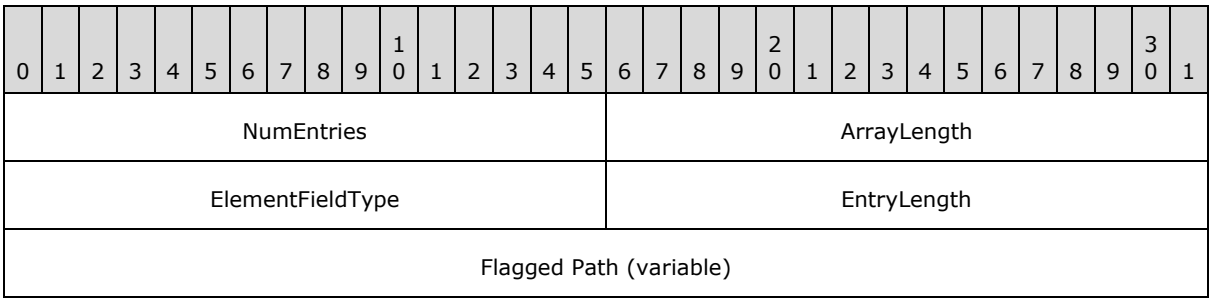


Address List Count (1 byte): The number of addresses in the **Addresses** field.

Addresses (variable): An array of sockaddr_in6 structures, as specified in [RFC2553].

2.8 Encrypted Endpoint Array

The Encrypted Endpoint Array is an encoding of IPv6 addresses and ports. This structure is used in the LOOKUP message defined in [MC-DRT]. This structure is encrypted using the Keytoken documented in section 2.5 before being transmitted.



NumEntries (2 bytes): The number of entries in the **Flagged Path** field. This value MUST be in the range 1 to 22, inclusive.

ArrayLength (2 bytes): The length of the encrypted data. This value MUST be set to 8 + (**NumEntries** * **EntryLength**).

ElementFieldType (2 bytes): The type of the elements in the array. MUST be set to 0x009D (IPV6_ENDPOINT).

EntryLength (2 bytes): The length of each entry in the array. MUST be set to 0x0012 (18 bytes).

Flagged Path (variable): A list of IPV6_ENDPOINT structures for DRT nodes that have encountered this LOOKUP request so far.

3 Structure Examples

Example 1: Request Flood conversation

The following example demonstrates the Credential, Signature, and Keytoken structures as used in a Request — Flood [MC-DRT] conversation between two nodes operating in confidential security mode. The initiating machine requests a routing entry from a peer, providing the key corresponding to the desired routing entry. This conversation is a key part of the bootstrap operation in [MC-DRT]. It is used to learn the network end points of active nodes in the peer-to-peer system.

In the confidential security mode, a node initiating a conversation must provide a Credential structure in order to authenticate itself and prove its right to participate in the peer-to-peer system. The node must also provide a Signature structure, containing a cryptographic signature calculated over one or more fields in the message.

The Credential structure provided by the requesting node can be used to encrypt a KeyToken structure sent in response. This KeyToken structure can be further used to encrypt other structures carrying sensitive information.

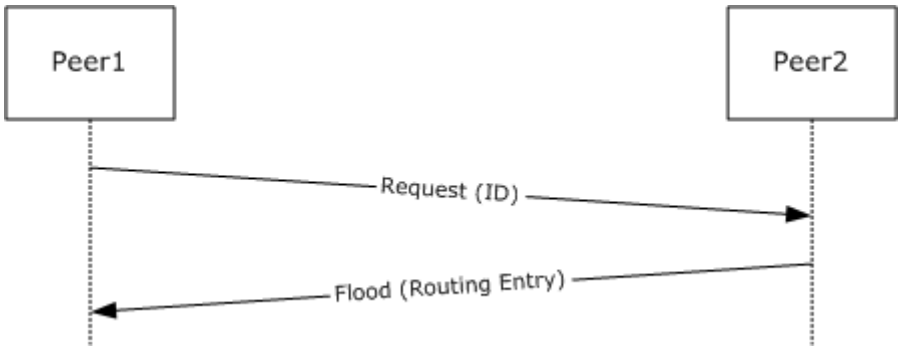


Figure 1: Request Flood conversation

Credential

In the derived key security profile, the Credential structure takes the form of a Public Key Cryptography Standards (PKCS) 7 version 1.5 message of type SignedData as specified in [RFC2315] section 9.1. It consists of a list of [X509] version 3 certificates. In the confidential security mode, a node initiating a conversation must provide a Credential structure in order to authenticate itself and prove its right to participate in the peer-to-peer system.

The following shows the fields and values of an [MC-DRT] certificate chain of length 2 as carried a flood message.

```
Root Certificate
  Version:
    Value: V3
  Serial Number: (0xcc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc)
  Signature Algorithm:
    Value: sha1RSA
  Issuer:
    Value:  CN = RootCert
  Valid from:
    Thursday, February 26, 2009 4:12:49 PM
  Valid to:
```

```
    Value: Friday, February 26, 2010 4:12:49 PM
  Subject:
    Value: RootCert
  Public Key
    Value: (0x 30 81 89 02 81 81 00 b2 bb 5e c8 5a 8e 9e d8 10 5d 8b e4 9f f5 88 2d c7 7b 84
44 05 ef 82 51 0b 7b 30 9e 15 96 78 92 4a db 15 a7 2d 71 f0 4c 38 d7 69 04 06 ea 6a 31 96 31
6e 7b f3 ce 27 54 ad ab 48 00 ea 57 4f ef 96 1c 55 3c 3b c6 13 f6 5f b0 f1 6c 30 fc d4 84 12
14 84 76 32 a9 d3 c4 23 a6 cb 51 79 e7 ab 96 ba 3e 51 4f 17 dd b8 01 db c7 b2 a3 c2 5d ea 07
a4 28 b8 7e 78 dd 17 1e 34 69 f8 0a ca 9e c1 7f 02 03 01 00 01)
  Thumbprint algorithm:
    Value: sha1
  Thumbprint:
    Value: (0x 65 d8 25 e4 d0 2f ff 40 9c b1 36 d4 7f e3 47 6b cb e1 1f 12)

Local Certificate
  Version:
    Value: V3
  Serial Number: (0xcc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc)
  Signature Algorithm:
    Value: sha1RSA
  Issuer:
    Value:  CN = RootCert
  Valid from:
    Thursday, February 26, 2009 4:12:50 PM
  Valid to:
    Value: Friday, February 26, 2010 4:12:50 PM
  Subject:
    Value: LocalCert
  Public Key
    Value: (0x 30 81 89 02 81 81 00 93 66 e1 ba 11 c2 ab ba b9 59 d0 36 84 31 93 76 d4 37 77
65 ec af 62 46 95 06 6e e4 03 e7 90 78 d6 59 d9 54 1e 15 5b 18 b5 eb 2b ab 35 aa 8c 7d 3c 01
0c 98 da 97 39 1a 7c 3f 27 0b 65 05 f5 30 10 a5 32 d9 1e 14 e8 0c 3e dc 57 45 56 48 ce c5 31
f5 fa f6 f2 8e d0 d0 bd 4a 5c 3a 27 81 d5 c0 a5 7f 31 84 e5 90 c8 9e 38 34 67 67 c2 f2 f1 72
c8 a0 37 c4 97 a0 5e 1f 07 67 47 c2 5b ad e8 ab 02 03 01 00 01)
  Thumbprint algorithm:
    Value: sha1
  Thumbprint:
    Value: (0x cb 46 3a b8 06 04 2d ba a1 51 96 b2 af 88 bd 08 90 d6 9a 9c)
```

Key Identifier

In the derived key security profile, the key identifier takes the form of a PUBLIC_KEY structure, which is used to identify the certificate in the Credential structure that should be used in all cryptographic operations.

```
  Size of algorithm id: (0x14)
  Algorithm Parameters Length: (0x0002)
  Public Key Length: (0x008c)
  Reserved: (0x00)
  Algorithm id
    (0x31 2E 32 2E 38 34 30 2E 31 31 33 35 34 39 2E 31 2E 31 2E 31)

  Algorithm Parameters: (0x0500)
Public Key:
  (0x30 81 89 02 81 81 00 93 01 02 02 11 C4 01 4D BA
     21 A4 B0 AB 8E DF 3F 72 66 E1 BA 11 C2 AB BA B9
     59 D0 36 84 31 93 76 D4 37 77 65 EC AF 62 46 95
```

```
06 6E E4 03 E7 90 78 D6 59 D9 54 1E 15 5B 18 B5
EB 2B AB 35 AA 8C 7D 3C 01 0C 98 DA 97 39 1A 7C
3F 27 0B 65 05 F5 30 10 A5 32 D9 1E 14 E8 0C 3E
DC 57 45 56 48 CE C5 31 F5 FA F6 F2 8E D0 D0 BD
4A 5C 3A 27 81 D5 C0 A5 7F 31 84 E5 90 C8 9E 38
34 67 67 C2 F2 F1 72 C8 A0 37 C4 97)
```

Signature

The signature structure is calculated over portions of the Request message to prove ownership of the private key in the leaf node of the certificate chain carried in the Credential structure.

```
Length: (0x0084)
Signature Data:
  (0x6C 35 A7 C3 5D FE B0 99 A9 73 A9 59 A0 BF 4A 5E
     75 31 9C D1 C1 77 9F 2E D1 5E C0 21 FF BC E0 30
     39 42 8C 12 90 8B 58 1D EC FF 81 CD 94 FF 49 60
     69 96 F1 F2 D4 42 18 B4 26 6D 63 D4 C6 30 63 E9
     C4 63 46 B0 9E 84 A7 39 E1 81 9D 60 55 13 98 D3
     82 8E 5A 5C C8 81 15 C9 54 B5 51 B5 F4 3C E6 43
     F3 93 69 9F A9 53 DA 28 67 99 56 41 6B EF 95 89
     37 04 6F DA 3D A9 93 64 E3 8E CE B0 28 4E BD 54)
```

Example 2: Authority

The following example demonstrates the PAYLOAD, keytoken, and Encoded CPA structures as used in an Inquire — Authority [MC-DRT] conversation between two nodes operating in confidential security mode. The Authority message is used to prove ownership of a key and transmit the payload associated with that key. This conversation is a key part of the key resolution process in [MC-DRT].

The Credential structure provided by the requesting node can be used to encrypt a KeyToken structure, which contains a symmetric key that can be used to encrypt other portions of the response. This example includes a complete [MC-DRT] Authority message, with encrypted KeyToken, Encoded CPA, and PAYLOAD structures. The decrypted versions of these structures are shown below.

An Example Authority message:

```
00000000`02803fa0  00 10 00 0c 51 06 65 08-d8 85 9c f5 00 18 00 08  ....Q.e.........
00000000`02803fb0  cc dd e4 3d 00 40 00 06-00 00 00 00 00 80 03 b6  ...=.@..........
00000000`02803fc0  30 82 03 ae 06 09 2a 86-48 86 f7 0d 01 07 02 a0  0.....*.H.......
00000000`02803fd0  82 03 9f 30 82 03 9b 02-01 01 31 00 30 0b 06 09  ...0......1.0...
00000000`02803fe0  2a 86 48 86 f7 0d 01 07-01 a0 82 03 83 30 82 01  *.H..........0..
00000000`02803ff0  bd 30 82 01 26 a0 03 02-01 02 02 10 cc cc cc cc  .0..&...........
00000000`02804000  cc cc cc cc cc cc cc cc-cc cc cc cc 30 0d 06 09  ............0...
00000000`02804010  2a 86 48 86 f7 0d 01 01-05 05 00 30 1d 31 1b 30  *.H........0.1.0
00000000`02804020  19 06 03 55 04 03 1e 12-00 52 00 6f 00 6f 00 74  ...U.....R.o.o.t
00000000`02804030  00 43 00 65 00 72 00 74-00 00 30 1e 17 0d 30 39  .C.e.r.t..0...09
00000000`02804040  30 32 32 36 32 33 31 32-34 39 5a 17 0d 31 30 30  0226231249Z..100
00000000`02804050  32 32 36 32 33 31 32 34-39 5a 30 1d 31 1b 30 19  226231249Z0.1.0.
00000000`02804060  06 03 55 04 03 1e 12 00-52 00 6f 00 6f 00 74 00  ..U.....R.o.o.t.
00000000`02804070  43 00 65 00 72 00 74 00-00 30 81 9f 30 0d 06 09  C.e.r.t..0..0...
00000000`02804080  2a 86 48 86 f7 0d 01 01-01 05 00 03 81 8d 00 30  *.H............0
00000000`02804090  81 89 02 81 81 00 b2 bb-5e c8 5a 8e 9e d8 10 5d  ........^.Z....]
```

```
00000000`028040a0  8b e4 9f f5 88 2d c7 7b-84 44 05 ef 82 51 0b 7b  .....-.{.D...Q.{
00000000`028040b0  30 9e 15 96 78 92 4a db-15 a7 2d 71 f0 4c 38 d7  0...x.J...-q.L8.
00000000`028040c0  69 04 06 ea 6a 31 96 31-6e 7b f3 ce 27 54 ad ab  i...j1.1n{..'T..
00000000`028040d0  48 00 ea 57 4f ef 96 1c-55 3c 3b c6 13 f6 5f b0  H..WO...U<;..._.
00000000`028040e0  f1 6c 30 fc d4 84 12 14-84 76 32 a9 d3 c4 23 a6  .l0......v2...#.
00000000`028040f0  cb 51 79 e7 ab 96 ba 3e-51 4f 17 dd b8 01 db c7  .Qy....>QO......
00000000`02804100  b2 a3 c2 5d ea 07 a4 28-b8 7e 78 dd 17 1e 34 69  ...]...(.~x...4i
00000000`02804110  f8 0a ca 9e c1 7f 02 03-01 00 01 30 0d 06 09 2a  ...........0...*
00000000`02804120  86 48 86 f7 0d 01 01 05-05 00 03 81 81 00 89 68  .H.............h
00000000`02804130  48 33 fb 53 57 32 0f be-fa b1 02 72 61 04 a8 95  H3.SW2.....ra...
00000000`02804140  22 db 7e 71 ff f9 ff 86-1b 8f ee 01 c7 44 b2 7c  ".~q.........D.|
00000000`02804150  67 1f e2 ad 64 6d 7a 8c-7e ab 31 98 05 fa 2b 14  g...dmz.~.1...+.
00000000`02804160  a3 38 bb 64 49 84 d3 f0-b1 0a 25 f2 76 fe d9 a5  .8.dI.....%.v...
00000000`02804170  ba 2e 3d ab 3c dd 9d cf-72 a4 4f 49 bf 64 d1 61  ..=.<...r.OI.d.a
00000000`02804180  48 fb 03 95 df b8 35 e7-76 4e c9 21 25 22 4a d7  H.....5.vN.!%"J.
00000000`02804190  d4 90 b5 fc 46 75 f9 7e-5c 6e 28 04 19 88 fa 60  ....Fu.~\n(....`
00000000`028041a0  35 f3 61 e1 66 13 24 79-36 1e 70 d3 c8 5a 30 82  5.a.f.$y6.p..Z0.
00000000`028041b0  01 be 30 82 01 27 a0 03-02 01 02 02 0f 61 00 74  ..0..'.......a.t
00000000`028041c0  00 61 00 44 00 00 00 00-00 00 00 2d 30 0d 06 09  .a.D.......-0...
00000000`028041d0  2a 86 48 86 f7 0d 01 01-05 05 00 30 1d 31 1b 30  *.H........0.1.0
00000000`028041e0  19 06 03 55 04 03 1e 12-00 52 00 6f 00 6f 00 74  ...U.....R.o.o.t
00000000`028041f0  00 43 00 65 00 72 00 74-00 00 30 1e 17 0d 30 39  .C.e.r.t..0...09
00000000`02804200  30 36 31 35 30 32 30 38-33 30 5a 17 0d 31 30 30  0615020830Z..100
00000000`02804210  36 31 35 30 32 30 38 33-30 5a 30 1f 31 1d 30 1b  615020830Z0.1.0.
00000000`02804220  06 03 55 04 03 1e 14 00-4c 00 6f 00 63 00 61 00  ..U.....L.o.c.a.
00000000`02804230  6c 00 43 00 65 00 72 00-74 00 00 30 81 9f 30 0d  l.C.e.r.t..0..0.
00000000`02804240  06 09 2a 86 48 86 f7 0d-01 01 01 05 00 03 81 8d  ..*.H...........
00000000`02804250  00 30 81 89 02 81 81 00-a4 63 4b 4e ca d6 ee c7  .0.......cKN....
00000000`02804260  0d 0d 0b 9a bb 37 35 f8-55 89 e6 37 aa 9c cf f5  .....75.U..7....
00000000`02804270  d9 58 d8 b8 24 33 51 c0-cd 2a 2e 5a 9b 24 da 60  .X..$3Q..*.Z.$.`
00000000`02804280  65 96 12 42 1d 8c 4a 10-1c 32 67 09 e4 b9 1a 9f  e..B..J..2g.....
00000000`02804290  a5 f2 76 f7 55 6f ff b0-69 9d d5 52 78 23 90 a2  ..v.Uo..i..Rx#..
00000000`028042a0  1c 69 c0 6d 50 b8 37 2f-65 16 1d c0 f9 60 fb 3e  .i.mP.7/e....`.>
00000000`028042b0  ce b8 e9 1f 70 ea 30 7c-0e 19 7b 84 ba d6 7a 80  ....p.0|..{...z.
00000000`028042c0  db 54 5f 8c bd cf bf 6d-f4 9c 5f 37 c3 65 26 c4  .T_....m.._7.e&.
00000000`028042d0  65 a4 e3 9e cf da 36 2f-02 03 01 00 01 30 0d 06  e.....6/.....0..
00000000`028042e0  09 2a 86 48 86 f7 0d 01-01 05 05 00 03 81 81 00  .*.H............
00000000`028042f0  49 18 ba f4 64 99 a2 27-bd 9f 6a 53 87 87 4e f8  I...d..'..jS..N.
00000000`02804300  fa c9 5d 73 59 99 cb 15-d8 d7 93 f7 2b 7a 88 ac  ..]sY.......+z..
00000000`02804310  65 f0 1d ee ce 82 a0 09-62 94 6d 6d 31 5e b6 95  e.......b.mm1^..
00000000`02804320  0f c7 1a af e5 6d f3 de-08 f5 43 1f 10 37 bc 35  .....m....C..7.5
00000000`02804330  7a c7 dc e5 70 b7 70 7c-4b 06 28 6a f3 3d cd 7d  z...p.p|K.(j.=.}
00000000`02804340  62 cd 87 05 06 4c 9f b7-ff b9 84 4b d5 ef 93 5d  b....L.....K...]
00000000`02804350  9b fe df ea a2 2e c1 70-68 0e 0b 6d b9 6a ca 9f  .......ph..m.j..
00000000`02804360  c0 9a 27 b6 23 d1 8e 14-a7 5d 57 c5 eb 6b af 45  ..'.#....]W..k.E
00000000`02804370  31 00 00 00 00 9f 00 84-1a 6f 46 f5 1b 64 af 27  1........oF..d.'
00000000`02804380  4d 96 a8 a7 cd bc 29 b5-f1 31 11 c9 e1 d7 7b 7d  M.....)..1....{}
00000000`02804390  b0 3c 56 17 65 ac 10 d9-35 e6 60 98 7a 32 49 86  .<V.e...5.`.z2I.
00000000`028043a0  93 75 e4 34 89 ce 50 cc-9b ea 61 d8 8a 61 75 c0  .u.4..P...a..au.
00000000`028043b0  e0 64 bd a7 08 46 76 6f-28 a7 84 34 0e 1b 49 0d  .d...Fvo(..4..I.
00000000`028043c0  e6 79 bb 80 1f f9 7f a3-ad 85 b1 48 59 93 58 3a  .y.........HY.X:
00000000`028043d0  bc 90 d7 8a 56 e6 77 f6-a4 d0 39 bf 27 01 be 0f  ....V.w...9.'...
00000000`028043e0  02 12 7b 33 90 4f 78 2f-09 0b 03 ca cb f4 1d df  ..{3.Ox/........
00000000`028043f0  89 87 75 5e 27 fc 36 0f-00 a4 00 b4 c5 4f 3d 17  ..u^'.6......O=.
00000000`02804400  5e 60 01 4f b1 30 b1 f9-b0 df ca c3 00 49 c1 38  ^`.O.0.......I.8
00000000`02804410  4e 50 a3 97 3a 56 a1 42-79 8d 97 da a0 a1 9a 1d  NP..:V.By.......
00000000`02804420  6a ec 29 d3 91 0a e8 13-c7 ca e9 38 d8 fd 23 bc  j.).........8..#.
00000000`02804430  65 f2 a7 54 a7 3b 99 a0-ba fa ad 7e b5 71 6f 0c  e..T.;.....~.qo.
00000000`02804440  7a be 42 9b 06 7e 61 dc-db 2a a9 16 a7 dc 78 cd  z.B..~a..*....x.
```

```
00000000`02804450  6c aa 78 e4 92 fb b4 dc-8b 9a d3 c1 d4 fb 0e 25  l.x............%
00000000`02804460  98 43 50 f3 9c bf c5 e4-0d 39 15 6b 5d d3 a0 23  .CP......9.k]..#
00000000`02804470  63 7e 78 8d c1 97 3d 3b-cf 63 48 5f b2 1b a6 5f  c~x...=;.cH_..._
00000000`02804480  5b 10 51 74 4b e3 98 ce-44 aa ef ac a4 8d fa 9b  [.QtK...D.......
00000000`02804490  ef 72 5e dd 23 76 ec c0-6b dc 33 1d e2 20 50 c4  .r^.#v..k.3.. P.
00000000`028044a0  d8 33 7b d1 f8 2a e8 3e-d4 e7 c6 01 00 a2 01 b4  .3{..*.>........
00000000`028044b0  f0 d1 37 0b 98 d5 cd 02-99 bf 36 6c 65 a8 36 51  ..7.......6le.6Q
00000000`028044c0  33 9e ba 74 c2 e8 c1 e8-ef 4e ce 7c 5b 3a a8 1c  3..t.....N.|[:..
00000000`028044d0  82 22 a6 3f 82 a8 57 1b-3a 0e e1 fd 1b af 5a b7  ."?..W.:.....Z.
00000000`028044e0  f1 ba c9 5b f0 d8 e6 cc-78 6f da f3 bb 71 ba c8  ...[....xo...q..
00000000`028044f0  06 fb fd 76 06 75 f1 3e-0d 85 19 dd a2 64 9f 5d  ...v.u.>.....d.]
00000000`02804500  ae eb d5 2c 2d 24 d4 c2-93 0b bf 42 96 60 bb c3  ...,-$.....B.`..
00000000`02804510  32 63 02 91 10 a4 be e2-4a a2 6b 90 48 c7 c4 b0  2c......J.k.H...
00000000`02804520  41 e7 04 8d 11 2c 8f f3-d1 1d d6 f1 cd 41 c4 7c  A....,.......A.|
00000000`02804530  9a 3a 47 7a cf 59 3c 30-a7 51 3b 52 1b 24 31 fc  .:Gz.Y<0.Q;R.$1.
00000000`02804540  cf 37 64 21 69 39 77 8e-ff 5f cc 77 f9 ed fb aa  .7d!i9w.._.w....
00000000`02804550  b4 88 03 7a 8e 43 89 2a-11 3c f9 e6 bc 93 0a 92  ...z.C.*.<......
00000000`02804560  15 ad 71 19 3f 76 de 88-7c 68 b6 99 97 53 60 9f  ..q.?v..|h...S`.
00000000`02804570  d6 05 6e ea ea 24 69 31-d6 f2 e2 9a 89 be 43 85  ..n..$i1......C.
00000000`02804580  ad ab db f9 4f 88 54 25-5d d7 df cb b7 db 50 e0  ....O.T%].....P.
00000000`02804590  2e 4d 0c 4f a8 20 a0 08-5f dc 3e f2 cb de 84 77  .M.O. .._.>....w
00000000`028045a0  a8 ce 71 c2 c5 f9 c5 40-3b 67 2b 3d f2 79 0f 97  ..q....@;g+=.y..
00000000`028045b0  8b fa fb 44 a0 b5 e8 35-6c 25 a2 d9 a1 78 10 1b  ...D...5l%...x..
00000000`028045c0  f1 29 1e b0 0e 49 20 e2-32 27 e4 38 a7 89 c3 1a  .)...I .2'.8....
00000000`028045d0  eb 31 98 a5 01 07 c4 03-0a a5 63 39 6a 21 6b c0  .1........c9j!k.
00000000`028045e0  dc 20 00 01 39 68 56 24-74 19 53 30 58 8b 7e 18  . ..9hV$t.S0X.~.
00000000`028045f0  cb 1c 20 e5 d0 da a0 dc-b6 16 c5 f3 96 82 7d 24  .. ..........}$
00000000`02804600  63 3b 21 75 47 f7 c0 00-5b c2 03 d8 7b 71 88 58  c;!uG...[...{q.X
00000000`02804610  dd 86 8d 06 ed 72 ad e9-a1 db f5 2b 23 a8 c8 1e  .....r.....+#...
00000000`02804620  b4 de 02 19 e4 5d 1e 5d-ff f0 e9 50 92 c0 d6 3a  .....].]...P...:
00000000`02804630  b5 c9 81 1a 56 16 00 24-54 52 1f 8b 67 f2 2b 82  ....V..$TR..g.+.
00000000`02804640  0f 72 c4 32 f1 e7 16 8d-09 8c 6b 40 6c fa 40 55  .r.2......k@l.@U
00000000`02804650  ae d0 11 ce b4 85 94 d3-85 9a 21 ce ae ad c3 3e  ..........!....>
```

KeyToken

Referencing [MC-DRT] for the format of the Authority message, a KeyToken structure can be parsed from the data above. This KeyToken structure has been encrypted using the public key of the requesting node.

Encrypted KeyToken:

```
00000000`0352e7f0  00 0c 5e 46 9c a9 19 5c-84 4a cf db 7e ee 0d 8d  ..^F...\.J..~...
00000000`0352e800  97 99 3d 4f c0 15 cc 8d-24 e3 07 9f 1c 03 19 65  ..=O....$......e
00000000`0352e810  b6 9f d2 e3 06 88 f2 6f-f9 fa fc bd 55 91 d2 56  .......o....U..V
00000000`0352e820  48 88 f2 5a 08 54 46 a4-76 99 56 ba 9b a2 70 2f  H..Z.TF.v.V...p/
00000000`0352e830  32 7d ff d1 76 69 70 20-b0 e9 f7 29 1d ad 76 57  2}..vip ...)..vW
00000000`0352e840  a8 8b b5 71 48 36 b5 58-49 eb 18 8f 29 39 b9 63  ...qH6.XI...)9.c
00000000`0352e850  c3 11 df 3b 06 c2 e5 99-10 69 ca 27 ce b9 b5 f6  ...;.....i.'....
00000000`0352e860  bf bf a7 39 34 70 fb 4e-93 83 b5 17 06 27 c8 d1  ...94p.N.....'..
```

The data above maps to the following decrypted KeyToken structure:

```
IV BLOCK LENGTH: (0x0010)
```

```
Padding1: (0x000000000000)
IV BLOCK data:
  (0x90 db 00 f7 05 85 3c 70  d6 0a dd 9c ce 7f 0b 97)
Field1: (0x4b44424d0100000020000000)
AES256 Key:
  (0xcc 3e c1 12-33 6e fb f6 6e b6 3f 1b 5d e6 b8 d0
     f2 b3 f7 e4-41 3d 5a d6 67 e1 83 98 e8 2f e7 3c)
```

Encoded CPA

Referencing [MC-DRT] for the format of the Authority message, an Encoded CPA structure can be parsed from the data above. This encoded CPA structure has been encrypted using the KeyToken structure shown above.

Encrypted Encoded CPA:

```
00000000`0352e630  84 cb 91 f9 68 ca 13 a0-26 bb 58 9e 50 f9 2b ac  ....h...&.X.P.+.
00000000`0352e640  32 f3 49 56 05 d8 a0 5e-42 c3 fb 43 50 76 2d 97  2.IV...^B..CPv-.
00000000`0352e650  fa bd 96 21 ce ee 3e 9d-80 2c c6 28 25 7c 1c 57  ...!..>..,.(%|.W
00000000`0352e660  d1 04 39 4c 76 20 d0 62-b9 15 95 a7 2f 34 e2 bd  ..9Lv .b..../4..
00000000`0352e670  24 82 8a 12 bc 8b db bc-c9 d5 b5 8e f4 97 19 79  $..............y
00000000`0352e680  cc ee 23 e9 cf 13 eb 8e-97 d2 19 63 21 00 26 67  ..#........c!.&g
00000000`0352e690  d0 3d 14 79 6b c6 f6 1e-d0 f0 1c 6a 6d c0 5f 38  .=.yk......jm._8
00000000`0352e6a0  6a eb aa ca 22 7d 70 02-47 84 17 ca cf 9c 52 19  j..."}p.G.....R.
00000000`0352e6b0  c1 ea a1 b5 17 cc c1 04-21 29 cc a5 92 57 a0 66  ........!)...W.f
00000000`0352e6c0  b4 74 a3 b5 54 a8 21 09-54 87 0f d3 eb 5b 19 ec  .t..T.!.T....[..
00000000`0352e6d0  2b f2 52 cb 81 18 87 40-36 96 83 62 7b d4 15 cb  +.R....@6..b{...
00000000`0352e6e0  2d 0f 22 77 a2 84 d5 44-d2 ea 23 3b 90 06 87 fe  -."w...D..#;....
00000000`0352e6f0  0d 20 d7 9d 4a e1 9d 3f-6e 93 b1 20 c1 f0 85 cb  . ..J..?n.. ....
00000000`0352e700  83 a9 8e 16 f7 f9 ba a0-26 6d ba ef fd 61 dd a1  ........&m...a..
00000000`0352e710  1c 90 7f ec 1c ba 95 ad-99 2e 1b 31 53 ed 53 d1  ...........1S.S.
00000000`0352e720  0c 1c 8b c7 af b9 c5 6d-0e 83 18 aa 22 fe 5e ce  .......m...."."^.
00000000`0352e730  0e db ea dc 26 ab 41 9b-4e d5 03 46 8e a2 1f c8  ....&.A.N..F....
00000000`0352e740  0e 57 af 4d 16 d8 4f 1d-31 24 cd 74 23 0e f6 44  .W.M..O.1$.t#..D
00000000`0352e750  c5 95 55 35 68 7b 0f 3b-98 c5 12 26 f5 2d c4 c6  ..U5h{.;...&.-..
00000000`0352e760  4c 13 28 1e 83 b6 5a a3-2d d8 df c6 e8 20 6c 13  L.(...Z.-.... l.
00000000`0352e770  5e 59 8e 0a 06 6f 96 37-29 35 2d 53 ef e3 20 1e  ^Y...o.7)5-S.. .
00000000`0352e780  c3 1b 73 5a 26 e2 1a a0-c6 89 a9 5a 41 f3 2b 18  ..sZ&......ZA.+.
00000000`0352e790  11 d4 96 a9 17 07 57 cd-aa 8f 71 9b af 97 fc d2  ......W...q.....
00000000`0352e7a0  1f 3e 10 3d e6 e0 8e 82-0d 53 e0 54 59 c5 4d 60  .>.=.....S.TY.M`
00000000`0352e7b0  01 7b 26 e0 29 88 15 8a-29 4a 19 02 ac 8c 86 02  .{&.)...)J......
00000000`0352e7c0  06 59 b3 c8 44 6b b8 9d-21 c5 dd 4c 77 5a a8 00  .Y..Dk..!..LwZ..
00000000`0352e7d0  7b 99 60 5f f0 2d 76 fb-19 c2 4c ce 01 76 6a a9  {.`_.-v...L..vj.
```

The data above maps to the following decrypted Encoded CPA structure:

```
Reserved: (0x00)
Signature
  Signature Length: (0x0080)
  Signature Data
    (0x17 3c 1e 51-48 84 5a 37 ad b9 0f 5c 60 84 1a 20
       c4 a5 a7 06-82 57 1a 1f 19 5a 71 b6 90 28 d8 34
       cc 38 16 b8-6f 4c 5c 1c 76 c4 10 8c eb 6e 72 e9
```

```
        dd 2b 3b 6c-7c a4 b2 66 cf 62 95 62 48 2d 9f cd
        78 f7 12 dd-ba bb 97 34 f3 40 78 e8 5f 19 e9 a9
        ce 59 bc 12-af f1 2f 7a 06 c0 c2 f1 8f fe 2b 80
        b5 59 4d 8e-0a b8 2c 26 22 63 ef b7 36 66 2a f7
        d4 10 24 65-f8 1f 33 ad 81 d1 78 55 ac 0b aa 72)

Protocol Major Version (0x65)
Protocol Minor Version (0x60)
Security Profile Major Version: (0x01)
Security Profile Minor Version: (0x00)
Key Length (0x0020)
Key:
  (0xcc d9 cb e5 35 ae cc d9 cb e5 35 ae 38 49 e6 fb
     fa e0 f0 52 f5 59 2c e4 7c 7f dc 78 c2 86 70 1a
     55 6a 2e fc 04 7f)
Size of Nonce (0x10)
Nonce:
  (0x3b d9 58 02 78 6a d7 39 4c 47 58 cb 39 93 8b bc)
Flags (0x00000000)
Public Key:
  Size of algorithm id: (0x14)
  Size of Parameters: (0x0002)
  Size of Public Key: (0x008c)
  Padding: (0x00)
  OID:
    (0x31 2E 32 2E 38 34 30 2E 31 31 33 35 34 39 2E 31 2E 31 2E 31)
  Parameters: (0x0500)
  Public Key:
    (0x30 81 89 02 81 81 00 c3 19 64 65 47 04 76 6f 5c
       a1 c7 c0 f5 80 f1 3c bf 10 ba 55 7a 79 fc 75 18
       d6 66 4f b9 0b 41 3b a0 b9 71 b0 1a 5c cd d5 c6
       42 90 40 38 15 e9 70 03 bb d8 08 cf 73 61 aa 81
       d7 23 69 51 b8 16 ec d9 49 00 da ee e4 a5 d4 b1
       f6 3e d4 ac a3 9b fd 70 19 46 b1 ee d5 25 48 61
       a1 ef c9 d4 85 41 a3 72 4f 40 d7 f1 1a cd 03 37
       26 90 e5 28 a0 7a 82 87 d7 7a a2 38 28 8b 08 0a
       78 e1 ee 34 69 72 ab 02 03 01 00 01 )
Address List:
  Address List Count: (0x02)
    Address:
      Address Size: (0x001c)
      sin6_family (0x1700)
      sin6_port (0xd4ee)
      sin6_flowinfo (0x000000)
      sin6_addr;
        (0x20 01 48 98 00 1b 00 04 2c 6c 9c 05 a8 79 8d cd)
      sin6_scope_id (0x000000)
    Address:
      Address Size: (0x001c)
      sin6_family (0x1700)
      sin6_port (0xd4ee)
      sin6_flowinfo (0x000000)
      sin6_addr;
        (0x20 20 01 48 98 00 00 0f ff 02 00 5e fe 9d 3b 1a 25)
      sin6_scope_id (0x000000)
```

PAYLOAD

Referencing [MC-DRT] for the format of the Authority message, an PAYLOAD structure can be parsed from the data above. This PAYLOAD structure has been encrypted using the KeyToken structure carried in the Authority message and described above. It carries the string "PAYLOAD" padded with zeroes to a total length of 32 bytes.

Encrypted PAYLOAD:

```
00000000`0352e570  c6 69 60 fc 1f d5 e3 eb-ab be ee bb b7 e0 02 52  .i`............R
00000000`0352e580  c9 1b 1a 16 50 59 55 ed-bf f4 7e d5 6b 79 12 88  ....PYU...~.ky..
00000000`0352e590  99 63 b7 51 b4 b6 f1 b7-f3 df 84 45 04 14 74 5d  .c.Q.......E..t]
00000000`0352e5a0  f0 15 f1 23 e5 58 d5 83-66 6b a3 fd 4b 7c 51 e4  ...#.X..fk..K|Q.
00000000`0352e5b0  35 27 0b 34 a4 7b c3 10-00 68 46 05 e3 27 6c 3b  5'.4.{...hF..'l;
00000000`0352e5c0  38 29 55 ce 3f 27 9e 0c-fd eb 6e 2d 1e 10 34 af  8)U.?'....n-..4.
00000000`0352e5d0  b7 0c 7b 0e 50 ad 78 28-6f c1 9f 19 51 cf 95 f5  ..{.P.x(o...Q...
00000000`0352e5e0  5a fa 2b fe cd 83 00 8f-1b a3 4f ab 54 72 16 a0  Z.+.......O.Tr..
00000000`0352e5f0  98 da 58 f1 a2 43 ba dc-e9 0b 3e 97 a3 90 52 e6  ..X..C....>...R.
00000000`0352e600  55 5d bb 87 c0 b1 9f e7-31 42 6a 87 cb b8 11 00  U].......1Bj.....
00000000`0352e610  d9 0e 6b 75 36 7c 37 a9-24 72 1b c1 4a 89 ee 4c  ..ku6|7.$r..J..L
```

The data above maps to the following decrypted PAYLOAD structure:

```
Payload:
  50 41 59 4c 4f 41 44 00-00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

4 Security Considerations

None.

5 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
- Windows 8 operating system
- Windows Server 2012 operating system
- Windows 8.1 operating system
- Windows Server 2012 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.

6 Change Tracking

This section identifies changes that were made to the [MC-DKSP] protocol document between the November 2013 and February 2014 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- The removal of a document from the documentation set.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the technical content of the document is identical to the last released version.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.
- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.

- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated.**

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact dochelp@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
3 Structure Examples	67256 Updated the snippet for the decrypted KeyToken structure in the description for Example 2: Authority to specify the field name "Padding1" and a value consisting of 6 bytes of zero padding.	N	Content updated.

7 Index