This article describes the procedure to configure and test connection with MSSQL. The same should work with other database or system too provided the correct connection specific details are entered.

Setting up MSSQL to use Kerberos

Use MSSQL standard instructions for this setup. Use Appendix section to verify that server is configured with Kerberos authentication

The SPN used for service account used with MSSQL server should be in the below format.

```
Named instance:
MSSQLSvc/<FQDN>:[<port> | <instancename>], where:
MSSQLSvc is the service that is being registered.
<FQDN> is the fully qualified domain name of the server.
<port> is the TCP port number.
<instancename> is the name of the SQL Server instance.

Default instance
MSSQLSvc/<FQDN>:<port> | MSSQLSvc/<FQDN>, where:
MSSQLSvc is the service that is being registered.
<FQDN> is the fully qualified domain name of the server.
<port> is the TCP port number.
```

Refer https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/register-a-service-principal-name-for-kerberos-connections?view=sql-server-ver15 for further details

To validate that the server is configured correctly, use the Microsoft® Kerberos Configuration Manager for SQL Server® utility.

Setting up client

Note: Replace the text within [] for the below commands.

1. Active directory account setup.

Identify the service account that will be used to connect to this database. Ensure this account has a login on the database and permission to execute the required SQL.

Setup a SPN for this service account. There doesn't appear to be any specific nomenclature for this, MSSQL/[USERID] has worked and the same may be used.

2. Generate a keytab file:

```
ktpass /out [USERID].keytab /princ MSSQL/[USERID]@[DOMAIN-UPPERCASE] /mapuser
[USERID]@[DOMAIN-UPPERCASE] /pass [ACCOUNT-PASSWORD] /crypto All /ptype
KRB5_NT_PRINCIPAL /mapop set
```

Validate the keyfile

To list the keys in the keytab file, use the command. (Use klist & kinit from JDK_HOME/bin)

```
klist -k -K -t [USERID].keytab
```

To validate the authenticity of the keytab file, a credential cache needs to be generated using the above keytab file.

This step expects a valid krb5.conf or krb5.ini file on the system from where the below step is executed. If its not available, then see section below for krb5.conf generation.

```
kinit -c FILE:[USERID].cache -kt [USERID].keytab MSSQL/[USERID]@[DOMAIN-UPPERCASE]
```

Incase the krb5.conf file is not available, create the file and set it in environment variable KRB5_CONFIG and then use the above command

To debug kinit issues, use the KRB5_TRACE environment variable. This can be set to file or /dev/stdout incase of unix.

Now, list the tokens using the command klist

```
klist -c -e -f -a [USERID].cache
```

If everything is well so far, a krbtgt/DOMAIN-UPPERCASE@DOMAIN-UPPERCASE would be available in ticket cache.

3. Create rest of configurations

3a. krb5.conf (if the file doesnt exist or is not available)

```
[libdefaults]
default_realm = [DOMAIN-UPPERCASE]
dns_lookup_realm = false
dns_lookup_kdc = true
ticket_lifetime = 24h
forwardable = yes

[domain_realm]
.[DOMAIN-LOWERCASE] = [DOMAIN-UPPERCASE]
[DOMAIN-LOWERCASE] = [DOMAIN-UPPERCASE]

[realms]
[DOMAIN-UPPERCASE] = {
kdc = KDC-1.[DOMAIN-UPPERCASE]
#Additional KDCs can be added like below
kdc = KDC-x.[DOMAIN-UPPERCASE]
default_domain = [DOMAIN-UPPERCASE]
}
```

3b. Login security configuration file. Create file SQLJDBCDriver.conf with below contents.

```
SQLJDBCDriver {
   com.sun.security.auth.module.Krb5LoginModule required
   useTicketCache=false
   useKeyTab=true
   doNotPrompt=true
   keyTab="[PATH-TO-KEYTAB]"
   principal="MSSQL/[USERID]@[DOMAIN-UPPERCASE]";
```

```
};
```

4. A quick validation using basic java code before configuring Saviynt.

Create KerberosJDBCClient.java with below code and compile it

```
import java.sql.*;
import java.util.*;

public class KerberosJDBCClient {

	public static void main(String[] args)
	{
		String connUrl = args[0];
		System.out.println("Connecting to: " + connUrl);

		try {
			Class.forName("com.microsoft.sqlserver.jdbc.SQLServerDriver");
			Connection conn = DriverManager.getConnection(connUrl);
			Statement statement = conn.createStatement();
			ResultSet resultSet = statement.executeQuery("select auth_scheme from
sys.dm_exec_connections where session_id=@@spid");
			while (resultSet.next())
			{
				System.out.println("Authentication Scheme is " + resultSet.getString(1));
			}
		}
		catch (Exception exception) {
			exception.printStackTrace();
		}
	}
}
```

Run the code using command:

```
java -Djava.security.krb5.conf=krb5.conf -Djava.security.auth.login.config=SQLJDBCDriver.conf  -cp
sqljdbc41.jar:. KerberosJDBCClient
"jdbc:sqlserver://hostname:port;databaseName=[dbName];integratedSecurity=true;authenticationScheme=Ja
vaKerberos;trustServerCertificate=true"
```

Expected Output:

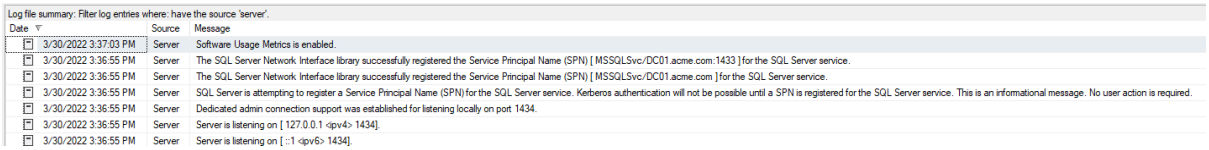
```
Connecting to: jdbc:sqlserver://dc01.acme.com:1433;databaseName=master;integratedSecurity=true;authenticationScheme=Java
Kerberos
Authentication Scheme is KERBEROS
```

Note: If running on windows, replace the sqljdbc41.jar:. to sqljdbc41.jar;.

Optionally, -Dsun.security.krb5.debug=true can be added into the above command for detailed logs about the kerberos negotiations.

Appendix

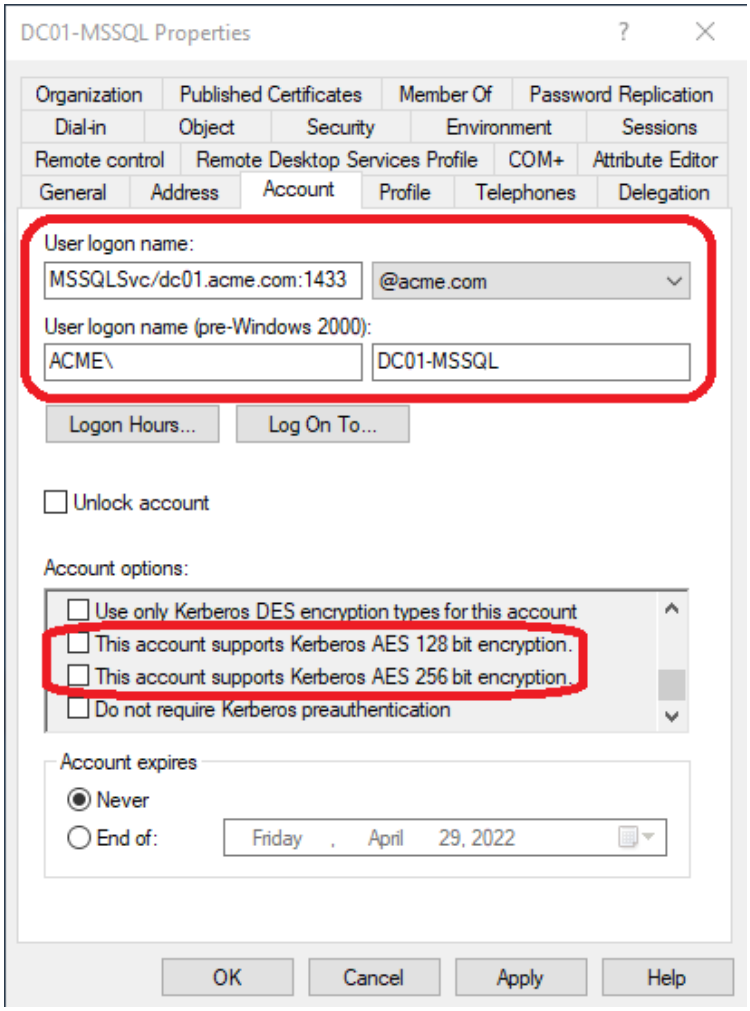
1. Verify MSSQL server is running using Kerberos Authentication



Log file summary: Filter log entries where: have the source 'server'.

Date	Source	Message
3/30/2022 3:37:03 PM	Server	Software Usage Metrics is enabled.
3/30/2022 3:36:55 PM	Server	The SQL Server Network Interface library successfully registered the Service Principal Name (SPN) [MSSQLSvc/DC01.acme.com:1433] for the SQL Server service.
3/30/2022 3:36:55 PM	Server	The SQL Server Network Interface library successfully registered the Service Principal Name (SPN) [MSSQLSvc/DC01.acme.com] for the SQL Server service.
3/30/2022 3:36:55 PM	Server	SQL Server is attempting to register a Service Principal Name (SPN) for the SQL Server service. Kerberos authentication will not be possible until a SPN is registered for the SQL Server service. This is an informational message. No user action is required.
3/30/2022 3:36:55 PM	Server	Dedicated admin connection support was established for listening locally on port 1434.
3/30/2022 3:36:55 PM	Server	Server is listening on [127.0.0.1 <ipv4> 1434].
3/30/2022 3:36:55 PM	Server	Server is listening on [::1 <ipv6> 1434].

2. At one customer place, the below settings had to be enabled for Kerberos connection to work.



Without this enabled, the logs showed.

```
Entered Krb5Context.initSecContext with state=STATE_IN_PROCESS
                [Krb5LoginModule]: Entering logout
                [Krb5LoginModule]: logged out Subject
Looking for keys for: MSSQL/********@**********
```

3. Sample logs for successful connection with Kerberos debug enabled. Key logs are highlighted.

```
Connecting to:
jdbc:sqlserver://dc01.acme.com:1433;databaseName=master;integratedSecurity=true;authen
ticationScheme=JavaKerberos
>>> KeyTabInputStream, readName(): ACME.COM
>>> KeyTabInputStream, readName(): mssql
>>> KeyTabInputStream, readName(): pb
>>> KeyTab: load() entry length: 44; type: 1
>>> KeyTabInputStream, readName(): ACME.COM
>>> KeyTabInputStream, readName(): mssql
>>> KeyTabInputStream, readName(): pb
>>> KeyTab: load() entry length: 44; type: 3
>>> KeyTabInputStream, readName(): ACME.COM
>>> KeyTabInputStream, readName(): mssql
>>> KeyTabInputStream, readName(): pb
>>> KeyTab: load() entry length: 52; type: 23
>>> KeyTabInputStream, readName(): ACME.COM
>>> KeyTabInputStream, readName(): mssql
>>> KeyTabInputStream, readName(): pb
>>> KeyTab: load() entry length: 68; type: 18
>>> KeyTabInputStream, readName(): ACME.COM
>>> KeyTabInputStream, readName(): mssql
>>> KeyTabInputStream, readName(): pb
>>> KeyTab: load() entry length: 52; type: 17
Looking for keys for: MSSQL/pb@ACME.COM
Java config name: krb5.conf
Loaded from Java config
Added key: 17version: 3
Added key: 18version: 3
Added key: 23version: 3
Found unsupported keytype (3) for MSSQL/pb@ACME.COM
Found unsupported keytype (1) for MSSQL/pb@ACME.COM
>>> KdcAccessibility: reset
Looking for keys for: MSSQL/pb@ACME.COM
Added key: 17version: 3
Added key: 18version: 3
Added key: 23version: 3
Found unsupported keytype (3) for MSSQL/pb@ACME.COM
Found unsupported keytype (1) for MSSQL/pb@ACME.COM
Using builtin default etypes for default_tkt_enctypes
default etypes for default_tkt_enctypes: 18 17 16 23.
>>> KrbAsReq creating message
>>> KrbKdcReq send: kdc=dc01.acme.com UDP:88, timeout=30000, number of retries =3,
#bytes=136
>>> KDCCommunication: kdc=dc01.acme.com UDP:88, timeout=30000,Attempt =1, #bytes=136
>>> KrbKdcReq send: #bytes read=175
>>>Pre-Authentication Data:
         PA-DATA type = 19
         PA-ETYPE-INFO2 etype = 18, salt = ACME.COMmssqlpb, s2kparams = null
         PA-ETYPE-INFO2 etype = 23, salt = null, s2kparams = null

>>>Pre-Authentication Data:
         PA-DATA type = 2
         PA-ENC-TIMESTAMP
>>>Pre-Authentication Data:
         PA-DATA type = 16

>>>Pre-Authentication Data:
         PA-DATA type = 15

>>> KdcAccessibility: remove dc01.acme.com
>>> KDCRep: init() encoding tag is 126 req type is 11
>>>KRBError:
         sTime is Wed Mar 30 15:42:46 IST 2022 1648635166000
         suSec is 823425
         error code is 25
         error Message is Additional pre-authentication required
         sname is krbtgt/ACME.COM@ACME.COM
         eData provided.
         msgType is 30
>>>Pre-Authentication Data:
```

```
         PA-DATA type = 19
         PA-ETYPE-INFO2 etype = 18, salt = ACME.COMmssqlpb, s2kparams = null
         PA-ETYPE-INFO2 etype = 23, salt = null, s2kparams = null

>>>Pre-Authentication Data:
         PA-DATA type = 2
         PA-ENC-TIMESTAMP
>>>Pre-Authentication Data:
         PA-DATA type = 16

>>>Pre-Authentication Data:
         PA-DATA type = 15

KrbAsReqBuilder: PREAUTH FAILED/REQ, re-send AS-REQ
Using builtin default etypes for default_tkt_enctypes
default etypes for default_tkt_enctypes: 18 17 16 23.
Looking for keys for: MSSQL/pb@ACME.COM
Added key: 17version: 3
Added key: 18version: 3
Added key: 23version: 3
Found unsupported keytype (3) for MSSQL/pb@ACME.COM
Found unsupported keytype (1) for MSSQL/pb@ACME.COM
Looking for keys for: MSSQL/pb@ACME.COM
Added key: 17version: 3
Added key: 18version: 3
Added key: 23version: 3
Found unsupported keytype (3) for MSSQL/pb@ACME.COM
Found unsupported keytype (1) for MSSQL/pb@ACME.COM
Using builtin default etypes for default_tkt_enctypes
default etypes for default_tkt_enctypes: 18 17 16 23.
>>> EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
>>> KrbAsReq creating message
>>> KrbKdcReq send: kdc=dc01.acme.com UDP:88, timeout=30000, number of retries =3,
#bytes=223
>>> KDCCommunication: kdc=dc01.acme.com UDP:88, timeout=30000,Attempt =1, #bytes=223
>>> KrbKdcReq send: #bytes read=1343
>>> KdcAccessibility: remove dc01.acme.com
Looking for keys for: MSSQL/pb@ACME.COM
Added key: 17version: 3
Added key: 18version: 3
Added key: 23version: 3
Found unsupported keytype (3) for MSSQL/pb@ACME.COM
Found unsupported keytype (1) for MSSQL/pb@ACME.COM
>>> EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
>>> KrbAsRep cons in KrbAsReq.getReply MSSQL/pb
Found ticket for MSSQL/pb@ACME.COM to go to krbtgt/ACME.COM@ACME.COM expiring on Thu
Mar 31 01:42:46 IST 2022
Entered Krb5Context.initSecContext with state=STATE_NEW
Service ticket not found in the subject
>>> Credentials serviceCredsSingle: same realm
Using builtin default etypes for default_tgs_enctypes
default etypes for default_tgs_enctypes: 18 17 16 23.
>>> EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
>>> CksumType: sun.security.krb5.internal.crypto.HmacSha1Aes256CksumType
>>> EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
>>> KrbKdcReq send: kdc=dc01.acme.com UDP:88, timeout=30000, number of retries =3,
#bytes=1297
>>> KDCCommunication: kdc=dc01.acme.com UDP:88, timeout=30000,Attempt =1, #bytes=1297
>>> KrbKdcReq send: #bytes read=1291
>>> KdcAccessibility: remove dc01.acme.com
>>> EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
>>> TGS credentials serviceCredsSingle:
>>> DEBUG: ----Credentials----
        client: MSSQL/pb@ACME.COM
        server: MSSQLSvc/dc01.acme.com:1433@ACME.COM
        ticket: sname: MSSQLSvc/dc01.acme.com:1433@ACME.COM
        startTime: 1648635166000
        endTime: 1648671166000
        ----Credentials end----
Subject is readOnly;Kerberos Service ticket not stored
>>> KrbApReq: APOptions are 00100000 00000000 00000000 00000000
>>> EType: sun.security.krb5.internal.crypto.ArcFourHmacEType
```

```
Krb5Context setting mySeqNumber to: 412437532
Created InitSecContextToken:
0000: 01 00 6E 82 04 A6 30 82   04 A2 A0 03 02 01 05 A1  ..n...0.........
0010: 03 02 01 0E A2 07 03 05   00 20 00 00 00 A3 82 03  ......... ......
0020: CD 61 82 03 C9 30 82 03   C5 A0 03 02 01 05 A1 0A  .a...0..........
0030: 1B 08 41 43 4D 45 2E 43   4F 4D A2 29 30 27 A0 03  ..ACME.COM.)0'..
0040: 02 01 00 A1 20 30 1E 1B   08 4D 53 53 51 4C 53 76  .... 0...MSSQLSv
0050: 63 1B 12 64 63 30 31 2E   61 63 6D 65 2E 63 6F 6D  c..dc01.acme.com
0060: 3A 31 34 33 33 A3 82 03   85 30 82 03 81 A0 03 02  :1433....0......
0070: 01 17 A1 03 02 01 03 A2   82 03 73 04 82 03 6F 5D  ..........s...o]
0080: F7 A3 AE 71 8B 09 99 98   40 1A D8 B9 54 80 25 D6  ...q....@...T.%.
0090: 56 94 D2 CD BE 87 8F A2   BB 82 54 CF 8D 2E 61 B6  V.........T...a.
00A0: A5 2B B2 73 19 C4 0C D9   E3 B3 C0 1E 93 BB D9 69  .+.s...........i
00B0: FE F0 98 18 FA D6 BD FB   C3 9C 1F 12 04 69 3D 5C  .............i=\
00C0: 06 72 69 F0 51 B8 AB 92   AA 8D 8E 04 F4 1C 2B 3B  .ri.Q.........+;
00D0: 02 0A 01 3A 9A 2F BF D3   90 6C 1A 70 05 5E 31 1D  ...:./...l.p.^1.
00E0: 64 69 DC 84 00 73 CE 2C   3D A1 C3 A0 55 5F 6E DF  di...s.,=...U_n.
00F0: 7A DB 69 E5 F0 8F 3B 5F   A4 08 C2 A6 07 1D 11 F9  z.i...;_........
0100: 9A 3B F7 8E E2 DA 68 0A   E3 EF 18 38 E5 11 20 84  .;....h....8.. .
0110: DD 76 33 D3 D5 6F AE 4A   1F E3 34 38 92 C9 E8 8E  .v3..o.J..48....
0120: 8E BF 87 67 BD 87 27 F7   83 24 AA 33 A9 EE 23 EE  ...g..'..$.3..#.
0130: 41 B2 CD 2A 8E E9 AA 7E   24 DD 98 A5 E1 7C E5 04  A..*....$.......
0140: DA E8 FE 52 21 46 40 DB   29 3D 7D 36 57 73 69 C4  ...R!F@.)=.6Wsi.
0150: 0D 20 5A 21 C9 D8 82 4B   53 9B E6 D1 D1 0C 33 64  . Z!...KS.....3d
0160: 8D CE 2A AE DC 6C 97 54   0A 9E AF 6C 6E 3C DC 65  ..*..l.T...ln<.e
0170: F6 D3 E8 F3 33 F4 54 A1   48 1A 32 2A 2C 8A C0 8A  ....3.T.H.2*,...
0180: FF 27 51 4F 3D BE 8B 5B   7D B8 CF 26 A0 C8 CF B8  .'QO=..[...&....
0190: 19 9B 87 23 2C D2 CD 61   28 B4 CA 25 51 58 4F FC  ...#,..a(..%QXO.
01A0: 09 15 47 53 39 0D 92 A5   BD 6D 55 1F B6 4C 6D C0  ..GS9....mU..Lm.
01B0: 2F 41 D5 09 2D DC 2F C6   16 E9 A7 0F FB 64 C9 7B  /A..-./......d..
01C0: 64 C6 CB AD 8B F5 A3 DC   4C B8 6F 21 2C 0E 8D 4C  d.......L.o!,..L
01D0: CE 41 B9 5A 20 63 1C 85   97 86 69 0E D1 BF 84 6B  .A.Z c....i....k
01E0: 54 C9 83 B3 7A 55 26 4C   10 10 C9 C4 9D 02 1C 6D  T...zU&L.......m
01F0: A7 59 12 80 7F 49 97 E7   0D 3E B4 89 E8 25 39 D8  .Y...I...>...%9.
0200: 65 BB CB B5 C8 39 4B 06   0E A2 CF 0B 9B 07 94 AE  e....9K.........
0210: 6C 2B AF 44 79 58 1B 95   7D 55 67 57 33 BD D0 B0  l+.DyX...UgW3...
0220: 98 79 44 A9 03 17 66 7B   64 90 77 F6 CC 1F AF B5  .yD...f.d.w.....
0230: B9 16 08 AC 5D B7 D9 27   8B 9B 6B FC F7 51 E7 F1  ....]..'..k..Q..
0240: EF AB 66 0E ED B1 39 4C   6C 5D 4C 1A 98 3A 32 5F  ..f...9Ll]L..:2_
0250: F9 8C 7E 9D 98 C9 52 06   38 44 FE D0 D2 24 4A 2C  ......R.8D...$J,
0260: D9 7F 28 86 BA 6B F4 04   E6 FA 29 65 92 38 32 E1  ..(..k....)e.82.
0270: 00 8F F5 BB ED 9E EF B8   A8 D9 BC CD 39 3C 1D C9  ............9<..
0280: 59 6A 32 AF FC D7 7E 0F   0A CC 8A 3E 2F 74 C9 7C  Yj2.......>/t..
0290: 4C DD 0E 15 02 79 C1 9A   B0 EA B3 3D DB 94 12 DF  L....y.....=....
02A0: 83 25 6E C8 42 7F E7 BB   38 E5 62 BA 4F 66 F4 DF  .%n.B...8.b.Of..
02B0: 75 5B 05 2C DA 56 2C B3   39 75 20 1F 4E A3 3B 59  u[.,.V,.9u .N.;Y
02C0: D4 D6 2B 34 6C BD 07 C5   B5 92 CA B7 CB AF 69 5B  ..+4l.........i[
02D0: 06 E5 A6 41 A1 A2 8F E0   92 30 7C BE 63 3C 53 20  ...A.....0..c<S
02E0: 3C 59 ED CD 2D 8B E8 F6   ED 49 44 9D 50 13 5D 87  <Y..-....ID.P.].
02F0: B9 99 6B 14 EC 04 A5 58   4A 9A 25 95 A3 7D 31 4B  ..k....XJ.%...1K
0300: 5F E4 4B 9E D1 CB 78 DC   39 99 8E 11 B7 BB C0 CF  _.K...x.9.......
0310: 7C BE A8 F5 FB 40 D9 99   97 21 77 60 21 74 F1 CB  .....@...!w`!t..
0320: E9 3B AC C8 36 3E 10 FD   CD 8E EE 79 1D 53 41 0A  .;..6>.....y.SA.
0330: 49 7C 7E 82 EB F8 CE 07   0E A6 56 DA 4E F3 10 16  I.........V.N...
0340: 6C 14 C6 EB 7C 2B 0A 31   AB 6D 1B 96 D2 15 D9 2A  l....+.1.m.....*
0350: 3E 74 8C A1 69 51 77 80   A1 76 62 C6 5F D6 54 89  >t..iQw..vb._.T.
0360: 67 55 9D 5F 9B D1 81 CC   24 DE C2 3B DC 84 20 5F  gU._....$..;.. _
0370: 2D E1 C6 FF 06 0B 11 E4   6B A4 54 D5 27 C1 0B 02  -.......k.T.'...
0380: 7A B1 1A A4 5C 3F DE ED   0D 23 E4 8D 2F 1A CE D0  z...\?...#../...
0390: 5C 83 0D 5E FE DD A7 9F   5D 3B D1 8F C2 D9 08 6B  \..^....];.....k
03A0: F2 4A D1 99 24 10 DD 19   A3 30 1E CB AF 1E FA 73  .J..$....0.....s
03B0: 4F 60 9E 26 23 74 BF 71   F2 8D 28 B6 27 F0 8C F1  O`.&#t.q..(.'...
03C0: E3 5D 35 26 E9 1A C2 D1   9F 52 0A 28 A8 CC CF 13  .]5&.....R.(....
03D0: 33 40 10 56 9A 2F 97 17   7C 39 AE 50 B5 0E 70 5D  3@.V./...9.P..p]
03E0: EC 45 60 AF 68 62 4F 2C   85 CD 62 79 4A 89 A4 81  .E`.hbO,..byJ...
03F0: BB 30 81 B8 A0 03 02 01   17 A2 81 B0 04 81 AD 81  .0..............
0400: EC 49 CC FC 08 F0 20 14   5D A2 B8 5E 06 2D F4 67  .I.... .]..^.-.g
0410: 17 31 EF F0 29 B6 46 48   85 D4 97 C3 1E 9F 6A AA  .1..).FH......j.
0420: 96 8E 5E A2 D3 8E C1 7A   04 A5 70 37 D6 97 28 97  ..^....z..p7..(.
0430: B8 84 86 8D 17 EF C4 21   B6 AB 48 57 70 42 A2 DA  .......!..HWpB..
0440: 67 E0 72 78 DD 6E 09 AB   F8 B5 C7 C7 44 AC 76 18  g.rx.n......D.v.
0450: 19 9F F5 2F F4 93 EA 26   DE 5E DC 86 17 FE 04 05  .../...&.^......
```

```
0460: 3B 8C 70 7A 10 FC CB 1E   4F 62 C6 55 2C 6A 8D B9  ;.pz....Ob.U,j..
0470: A7 4C 5E 51 10 88 61 08   00 D6 D9 EC D3 27 32 9D  .L^Q..a......'2.
0480: C5 DC A6 39 94 4B 7F C8   D8 AD 96 6D FE 65 52 AE  ...9.K.....m.eR.
0490: 05 F3 49 62 42 0C 6F A4   69 93 F3 EF C2 BC 05 91  ..IbB.o.i.......
04A0: D2 1C C7 7C 1D F4 BA 8A   6A 0E E4 EC              ........j...

Entered Krb5Context.initSecContext with state=STATE_IN_PROCESS
>>> EType: sun.security.krb5.internal.crypto.ArcFourHmacEType
Krb5Context setting peerSeqNumber to: 841281794
Authentication Scheme is KERBEROS
```