Magensa Web Service

Remote Services for PPSCRAs

RemoteServicesv2 PPSCRAv2 Operations Manual

November 27, 2017

Manual Part Number:
D998200120-20
REGISTERED TO ISO 9001:2008

1 Table 1.1 - Revisions

Rev Number	Date	Notes
10	November 10, 2016	Initial Release
20	November 27, 2017	Added DeviceType to all operations. Added DeviceSN to GetAmkKeyLoadCommand. Added GetKeyList operation.

NOTICE

The information contained herein is confidential and proprietary to:

Magensa, LLC
1710 Apollo Court
Seal Beach, CA 90740
562-546-6500

2 Purpose of the document

The purpose of this document is to provide a description of how to call operations of the Magensa Remote Services web service.

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Magensa LLC.

3 Table of Contents

4 PPSCRAv2 Operations

4.1 GetAmkKeyLoadCommand

A command used to calculate the command to securely change from the AMK key.

Input Properties

Property (*)	Value	Value Description
CustomerCode *	string	Customer code
Username *	string	The User Identification credential created and assigned by MagTek.
Password *	string	The password for the credential.
BillingLabel	string	Billing Label (no more than 64 characters).
CustomerTransactionId	string	Customer transaction ID
AdditionalRequestData	Array of key/value	A group that contains custom request data required by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.
Challenge *	string	Challenge code for the Key (28 characters)
DeviceCert *	string	Device certificate (1908 characters)
DeviceSN *	string	Device serial number
DeviceType *	string	This is the Device name. The DeviceType used for this command can be one of the following values: `DynaPro, DynaProGO, oDynamo, Generic, NotSpecified`
KSI *	string	Key slot indicator for the AMK (no more than 16 characters).

Note: * = Required

Output Properties

Property	Value	Value Description
CustomerTransactionId	string	Customer transaction ID
MagTranId	string	Magensa assigned unique transaction ID in GUID form
AdditionalOutputData	string	A group that contains additional output data returned by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.

CommandType	int	Type of command.
		`0 = Standard command`
		`1 = Extended command`

Description	string	Description of the command response
ExecutionTypeEnum	string	Execution type enumeration
ID	int	ID of the command response
Name	string	Name representing the function for Value.
Value	string	This is the command to send to the PPSCRA device.
KCV	string	AMK Key Check Value
KeyType	string	The Key Type used for this command can be one of the following values:

Property	Value	Value Description
		PIN, MSR, AMK

Sample GetAmkKeyLoadCommand Request

```
POST https://rsgw.magensa.net/RemoteServicesv2Gateway/PPSCRAv2.svc HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://www.magensa.net/RemoteServices/v2/IPPSCRAv2/GetAmkKeyLoadCommand"

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v2="http://www.magensa.net/RemoteServices/v2/"
xmlns:rem="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core"
xmlns:sys="http://schemas.datacontract.org/2004/07/System.Collections.Generic">
   <soapenv:Header/>
   <soapenv:Body>
      <v2:GetAmkKeyLoadCommand>
         <v2:request>
            <rem:Authentication>
               <rem:CustomerCode>123</rem:CustomerCode>
               <rem:Password>password</rem:Password>
               <rem:Username>username</rem:Username>
            </rem:Authentication>
            <rem:BillingLabel>label</rem:BillingLabel>
            <rem:CustomerTransactionID>123</rem:CustomerTransactionID>
            <rem:AdditionalRequestData>
               <sys:KeyValuePairOfstringstring>
                  <sys:key/>
                  <sys:value/>
               </sys:KeyValuePairOfstringstring>
            </rem:AdditionalRequestData>
            <rem:Challenge>0D0098D70CE31309160D00000000</rem:Challenge>

<rem:DeviceCert>308203B63082029EA003020102020A1B42F06800000000084D300D06092A864886F70D01010B050030
51310B3009060355040613025553311330110603555040A130A4D616754656B20496E63312D302B0603550403132465
6E67
2D504349337854797065446576696365732D4C332D4465766963652D5375624341301E170D3135303331333135303131
35
5A170D3233303331333135313131355A3059310B300906035504061302555331153013060355040A130C4D616754656B
2C
20496E632E31183016060355040B130F4950414420313030204465766963653119301706035504031310393844373043
45
3331333039313630443082012230D06092A864886F70D01010105000382010F003082010A0282010100 9F28B853D4F3
D1
4B1A0A3F89E2AC0852A69118BE9EEAFE7977B09E9789D0BA2A0317236005F8D3DE919CCE8737B16E3B94889ED3FDA0E8
86
E00C5BF1A88F3189433B2855684649DDF3E2EF0E0049DA945B2A4E2ED2BA5F0A46C9D0725AF321152B79A36A45CC022F
C2
8F5529C90E75B39E297927251609A434CA032290C967DFD3813044529FDE450E2A82000C5817C729A5674560ECC05846
2D
BCAC7BB5C2F3D15CEEEB69D8C17418756627AB4E7FBA6977BA109BA39C63B0D27E1D86F8CADA6A74A465208E68A0712D
F7
B9B5F5DD6D0808AEA4B54B82EE3C1D3BE4D4AA2BBA0F029463B3425FF26F708F8A2766CCE398C7D0DC93608C926B4CF2
EE
BCBB982B0203010001A38187308184301D0603551D0E04160414E277E7E163A48AF01F7F8B1AC9C6B33F8BF48D31301F
06
03551D23041830168014D19FC5704DA7D01A8CEA5D3B57E4C2382D0EAEF4300C0603551D130101FF0402300030100609
2B
06010401F6090201040304010030100609 2B06010401F609020204030401023010 06092B06010401F609020304030401
03
300D06092A864886F70D01010B05000382010100 7B5503C00FE0073FE4834FC367FF2EF289F9CE66084A54F482A08E08
34
9D8C3ED99B17AAC65C0D913321034F65D39AE4B089116564D56BE3EA50BF47BB1649E482D45EB5A004F006D3D360136F
AA
B8FE3529D7DAB850587A7636614979A0955CC73B919448E74B94B4CF4DEA0F7FA2F7F82F3629965F03E41511813D8126
2C
A1B843771BAD4B2A157B9E7085F6AF23F38EAC4022BFB7540CBB7550750520ED8BA04DD8D692F48743F5C4DF089362EC
14
CED11BFA166168CDA15F26368F036FA29CDA8A2033107587C6531061053DB5849C9EC3EE3028D7E1538FE7292D156C5F
97
16F20170B4BE14B3269CF51135B903FBC81A90E08B1B9DD1A9DC154749EFC1</rem:DeviceCert>
            <rem:DeviceSN>98D70CE31309160D</rem:DeviceSN>
            <rem:DeviceType>DynaPro</rem:DeviceType>
            <rem:KSI>L1MK0000004</rem:KSI>
         </v2:request>
      </v2:GetAmkKeyLoadCommand>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample GetAmkKeyLoadCommand Response

```
<s:Envelope xmlns:s=”http://schemas.xmlsoap.org/soap/envelope/”>
```

```
   <s:Body>
      <GetAmkKeyLoadCommandResponse xmlns=”http://www.magensa.net/RemoteServices/v2/”>
         <GetAmkKeyLoadCommandResult
xmlns:a=”http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core”
xmlns:i=”http://www.w3.org/2001/XMLSchema-instance”>
            <a:CustomerTransactionId>123</a:CustomerTransactionId>
            <a:MagTranId>41995c38-629d-4cdd-be83-de4ecd5a0d57</a:MagTranId>
            <a:AdditionalOutputData i:nil=”true”
xmlns:b=”http://schemas.datacontract.org/2004/07/System.Collections.Generic”/>
            <a:Command>
               <a:CommandType>0</a:CommandType>
               <a:Description>Key Injection</a:Description>
               <a:ExecutionTypeEnum>ALL</a:ExecutionTypeEnum>
               <a:ID>0</a:ID>
               <a:Name>ChangeKeyAmk</a:Name>
<a:Value>00010001180098D70CE31309160D000000004C314D4B3030303030303488EB6A279ACB7A701B96350AFCD529B
6D66D643E090ACE1E7A74BABF5BB972EB129AF7821B9C5844D21317EFC216B1ABAEDAB38BE982AB71545AF32FB529DBB2A
04A607379BB9FC64C953B4FDA4A80E05A6B433C6D212507B8121458EB2E53265579EF45ECAF375F357E8BFEA82FB88A156
01036078CED600C3BF528C1CC9A099FC614C36346D761B7C7C45670C7AE60EA09E04507E2C9F15411EB8F6DEF83710F35A
FCD0C779E0AC4B31B10F8045F412EB5DAA483CF259A8CDB00DA1CA766BCC40B73DF0B3C3B3F965034825766AABF7A7D746
4AE6722E19506F67BCFB58F13F25C546C6FF2BE253BBC194826C5B768FD3913CA394ED5AEF4AB70470630F6685EAFABECF
4BA12245D3EB1B859F1434EE112DCAD0DDCD5995773CD810CEA1CB633AAB35976B66E1C684D7C2A036BAF80E557F2757EB
F3FD71FAD54D53667FBA73412FF5CDF80DAF1B7CDF7E6B1A26AAD8AC92B209D9594D74E1B925D33A33C4A480464EF46582
784B4BD61535401906CCDCE539193AE977335B2362144B37A90B4EAF00E168E05721B04CBD3853279BBF43A24185D8C7EC
D4B10035FDEB676E3B44EF76AFE4A0E1A057D61C3E6E2B7D4272D2487A324EDFAA5B6AD442858828623E322CF92BE64674
C1C7A81C5E5FFC62C9925108FEF72A29A5C512CDA2313AF60FFC5E9C7C7B1A2DF2FB839A14AAE47A8FF340E4E3801628A0
A2AAA599EDA92</a:Value>
            </a:Command>
            <a:KCV>08D7B4</a:KCV>
            <a:KeyType>AMK</a:KeyType>
         </GetAmkKeyLoadCommandResult>
      </GetAmkKeyLoadCommandResponse>
   </s:Body>
</s:Envelope>
```

4.2 GetCertLoadCommand

A command used to calculate the command which is to be sent to the device for loading a certificate.

Input Properties

Property (*)	Value	Value Description
CustomerCode *	string	Customer code
Username *	string	The User Identification credential created and assigned by MagTek.
Password *	string	The password for the credential.
BillingLabel	string	Billing Label (no more than 64 characters)
CustomerTransactionId	string	Customer transaction ID
AdditionalRequestData	Array of key/value	A group that contains custom request data required by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.
Challenge *	string	Challenge code for the certificate to be loaded (28 characters)
KSN *	string	Key Serial Number of the device (20 HEX characters)
DeviceType *	string	This is the Device name. The DeviceType used for this command can be one of the following values: `DynaPro, DynaProGO, oDynamo, Generic, NotSpecified`
KeyType *	string	The Key Type used for this command can be one of the following values:

Property (*)	Value	Value Description
		PIN, MSR, AMK

Note: * = Required

Output Properties

Property	Value	Value Description
CustomerTransactionId	string	Customer transaction ID
MagTranId	string	Magensa assigned unique transaction ID in GUID form
AdditionalOutputData	Array of key/value	A group that contains additional output data returned by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.
CommandType	int	Type of command. 0 = Standard command 1 = Extended command
Description	string	Description of the command response
ExecutionTypeEnum	string	Execution type enumeration
ID	int	ID of the command response
Name	string	Name representing the function for the Value field.
Value	string	This is the value to send to the PPSCRA device for loading a certificate.

Sample GetCertLoadCommand Request

```
POST https://rsgw.magensa.net/RemoteServicesv2Gateway/PPSCRAv2.svc HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://www.magensa.net/RemoteServices/v2/IPPSCRAv2/GetCertLoadCommand"

<soapenv:Envelope xmlns:soapenv=”http://schemas.xmlsoap.org/soap/envelope/”
xmlns:v2=”http://www.magensa.net/RemoteServices/v2/”
xmlns:rem=”http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core”
xmlns:sys=”http://schemas.datacontract.org/2004/07/System.Collections.Generic”>
   <soapenv:Header/>
   <soapenv:Body>
      <v2:GetCertLoadCommand>
         <v2:request>
            <rem:Authentication>
               <rem:CustomerCode>123</rem:CustomerCode>
               <rem:Password>Password</rem:Password>
               <rem:Username>Username</rem:Username>
            </rem:Authentication>
            <rem:BillingLabel>label</rem:BillingLabel>
            <rem:CustomerTransactionID>123</rem:CustomerTransactionID>
            <rem:AdditionalRequestData>
               <sys:KeyValuePairOfstringstring>
                  <sys:key></sys:key>
                  <sys:value></sys:value>
               </sys:KeyValuePairOfstringstring>
            </rem:AdditionalRequestData>
            <rem:Challenge>0B0298D70CE31309160DA5B3FF42</rem:Challenge>
             <rem:DeviceType>DynaPro</rem:DeviceType>
            <rem:KSN>95000300000549200022</rem:KSN>
            <rem:KeyType>PIN</rem:KeyType>
         </v2:request>
      </v2:GetCertLoadCommand>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample GetCertLoadCommand Response

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body>
      <GetCertLoadCommandResponse xmlns="http://www.magensa.net/RemoteServices/v2/">
         <GetCertLoadCommandResult
xmlns:a="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
            <a:CustomerTransactionId>123</a:CustomerTransactionId>
            <a:MagTranId>27868f12-d612-4811-a127-4d56f74d7125</a:MagTranId>
            <a:AdditionalOutputData i:nil="true"
xmlns:b="http://schemas.datacontract.org/2004/07/System.Collections.Generic"/>
            <a:Command>
               <a:CommandType>0</a:CommandType>
               <a:Description>Rebind Certificate</a:Description>
               <a:ExecutionTypeEnum>ALL</a:ExecutionTypeEnum>
               <a:ID>0</a:ID>
               <a:Name>CertLoad</a:Name>

<a:Value>000194030B0198D70CE31309160DF6B33082039030820278A003020102020A1464BA0D000000000004300D060
92A864886F70D01010B0500303B310B3009060355040613025553311330110603550408130A4D616774656B20496E63311
730150603550403130E50434933784D53522D5375624341301E170D3133303532333139303435335A170D3138303532333
139313435335A3049310B3009060355040613025553311430120603550408130B4D616754656B20496E632E31243022060
3550403131B49504144205043493378204D5352204B65796C6F61646572205831308201223000D06092A864886F70D01010
105000382010F003082010A0282010100CFC10EC4A6CEDD9F0034B2030574990A7E6B31881F5E3E3AFD68AE6B9EAC6AE1A
792CFCF0F8F3C5A84C998504E25D2F79D788D02A6ABF45D24951BD9D2F8669D0A81A29FFEE09179F847645003F26B68842
628DAE1EA8AD8CC451914608398EB0A1765882240BD4B4417AA56F4C426FCCB476D3F19FE8148C3B0D4AB585548C162696
BBF8677B903BF121635C5DDCEC587EB718DC370D35BAF205283761EE207C20354A628AF5CA8FA855C234ADC35DA433A424
E82DC3D80A3609F0EB62947D8D4C57B5F1765807A5D66905826F41527916509E52A6C7F417A34AD4C820E7FE8A37AB491A
FC7F43393A2F2AF2EA93F0D0FC3DEE529ECA6EABC86CB784AC554E1020300EFE3A38187308184301D0603551D0E0416041
488D62EC4AA1732DE040CBFE2E3A286B2D98BD012301F0603551D2304183016801486BE77D911EB6DEAC0FE93703BB158
DFD05DF35300C0603551D130101FF04023000301006092B06010401F609020104030401023010006092B06010401F609020
20403040102301006092B06010401F60902030403040104300D06092A864886F70D01010B05000382010100069560D20BA
CB44F8D5D792E180B73DECDA77344FC91DD08C43BEB629EB2F29FC037CD8F0321B26F72F9A773D76DD3F86B6A9C69E88EF
A56F5C8B6F287D86D93124AA8D1D41E6180BC3C984BBEA1C86245B36306FBAC6F6D4E54D0859CD7664FD216ED2E6FB909B
1BEBB475D1EF82E7E74F09E67EB60DCF7E3D6B17D44DFEA5A5BC4CB314D84B9A9EB2D9BEA66835F59EEA9FB4B6D5D26D71
04C4D5058A542924D7132AA60F8373F3EEDC21EF4AC54DB10A99AD76A07FCFD813670350853F295B0D33416EB08F256B27
F56EAF366805CDFD1E9F3831F38097DC350F7F32473E3BAB86F60BB51670A2B0BB34DAFD9F26F26BEDCC5F010E1BB22F7A
CF381A7A28B0000C9F014ACF781E6B1BD00D9A75BDC6F90C63001831980164FC318AA6AE685E630ABFB89D9E3438C733D3
9CFF7010D309C623613CD03BC6F4A077FC4D8AEF023122B08042960AB360B94F0AA80BDAA94509034E756DE099C529324B
CFF76E57D46175D0518A9C78EFF49658A466475AEC812B8210FB5B980B3AE50FB340D8DDF62D61C6DA685D8FE19D74A4A8
7D02C3E2B2E4EB23183C8BAAA63359DB7BC8CBAE052CE1F4502924139EF27787D912D3801B43407A735F7644DF5F1E7619
172A35EF53843EE3EF22FCB5C9BD9534DB00CAF3D57F662981E618816D88F0CEAD04B203CE4F20B7EC71AC85CC241F97DD
52AC0E8F8E4F30ECE9E94663FEFDB9AD31F4B</a:Value>
            </a:Command>
         </GetCertLoadCommandResult>
      </GetCertLoadCommandResponse>
   </s:Body>
</s:Envelope>
```

4.3 GetCommandListByDevice

A command used to retrieve the list of available configuration commands.

Input Properties

Property (*)	Value	Value Description
CustomerCode *	string	Customer code
Username *	string	The User Identification credential created and assigned by MagTek.
Password *	string	The password for the credential.
BillingLabel	string	Billing Label (no more than 64 characters)

Property (*)	Value	Value Description
CustomerTransactionId	string	Customer transaction ID
AdditionalRequestData	Array of key/value	A group that contains custom request data required by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.
DeviceType *	string	This is the Device name. The DeviceType used for this command can be one of the following values: `DynaPro, DynaProGO, oDynamo, Generic, NotSpecified`

Note: * = Required

Output Properties

Property	Value	Value Description
CustomerTransactionId	string	Customer transaction ID
MagTranId	string	Magensa assigned unique transaction ID in GUID form
AdditionalOutputData	Array of key/value	A group that contains additional output data returned by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.

CommandType	int	Type of command.
		`0 = Standard command`
		`1 = Extended command`

Description	string	Description of the command response
ExecutionTypeEnum	string	The Execution Type can be one of the following values: `ALL, KSN, MUT`
ID	int	Command ID to be used for the following operation: `GetLoadConfigCommand`
Name	string	Name of the command
Value	string	Value. Response may return a nil for this operation.

Sample GetCommandListByDevice Request

```
POST https://rsgw.magensa.net/RemoteServicesv2Gateway/PPSCRAv2.svc HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://www.magensa.net/RemoteServices/v2/IPPSCRAv2/GetCommandListByDevice"


<soapenv:Envelope xmlns:soapenv=”http://schemas.xmlsoap.org/soap/envelope/”
xmlns:v2=”http://www.magensa.net/RemoteServices/v2/”
xmlns:rem=”http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core”
xmlns:sys=”http://schemas.datacontract.org/2004/07/System.Collections.Generic”>
   <soapenv:Header/>
   <soapenv:Body>
      <v2:GetCommandListByDevice>
         <v2:request>
            <rem:Authentication>
               <rem:CustomerCode>123</rem:CustomerCode>
               <rem:Password>Password</rem:Password>
               <rem:Username>Username</rem:Username>
            </rem:Authentication>
            <rem:BillingLabel>label</rem:BillingLabel>
            <rem:CustomerTransactionID>123</rem:CustomerTransactionID>
            <rem:AdditionalRequestData>
               <sys:KeyValuePairOfstringstring>
```

```
                  <sys:key></sys:key>
                  <sys:value></sys:value>
               </sys:KeyValuePairOfstringstring>
            </rem:AdditionalRequestData>
            <rem:DeviceType>DynaPro</rem:DeviceType>
         </v2:request>
      </v2:GetCommandListByDevice>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample GetCommandListByDevice Response

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body>
      <GetCommandListByDeviceResponse xmlns="http://www.magensa.net/RemoteServices/v2/">
         <GetCommandListByDeviceResult
xmlns:a="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
            <a:CustomerTransactionId>123</a:CustomerTransactionId>
            <a:MagTranId>05aa35b6-464f-44b9-b875-1ca16628f36e</a:MagTranId>
            <a:AdditionalOutputData i:nil="true"
xmlns:b="http://schemas.datacontract.org/2004/07/System.Collections.Generic"/>
            <a:Commands>
               <a:Command>
                  <a:CommandType>0</a:CommandType>
                  <a:Description>Config Unlocked</a:Description>
                  <a:ExecutionTypeEnum>KSN</a:ExecutionTypeEnum>
                  <a:ID>164</a:ID>
                  <a:Name>CONFIG_UNLOCKED</a:Name>
                  <a:Value>177:0</a:Value>
               </a:Command>
               <a:Command>
                  <a:CommandType>0</a:CommandType>
                  <a:Description>Config Locked</a:Description>
                  <a:ExecutionTypeEnum>KSN</a:ExecutionTypeEnum>
                  <a:ID>165</a:ID>
                  <a:Name>CONFIG_LOCKED</a:Name>
                  <a:Value>177:1</a:Value>
               </a:Command>
               <a:Command>
                  <a:CommandType>0</a:CommandType>
                  <a:Description>Bitmap Unlocked</a:Description>
                  <a:ExecutionTypeEnum>KSN</a:ExecutionTypeEnum>
                  <a:ID>166</a:ID>
                  <a:Name>BITMAP_UNLOCKED</a:Name>
                  <a:Value>166:0</a:Value>
               </a:Command>
               <a:Command>
                  <a:CommandType>0</a:CommandType>
                  <a:Description>Bitmap Locked</a:Description>
                  <a:ExecutionTypeEnum>KSN</a:ExecutionTypeEnum>
                  <a:ID>167</a:ID>
                  <a:Name>BITMAP_LOCKED</a:Name>
                  <a:Value>166:1</a:Value>
               </a:Command>
            </a:Commands>
         </GetCommandListByDeviceResult>
      </GetCommandListByDeviceResponse>
   </s:Body>
</s:Envelope>
```

4.4 GetKeyLoadCommand

A command used to calculate the command to securely change from one DUKPT key to another.

Input Properties

Property (*)	Value	Value Description
CustomerCode *	string	Customer code
Username *	string	The User Identification credential created and assigned by MagTek.
Password *	string	The password for the credential.
BillingLabel	string	Billing Label (no more than 64 characters)
CustomerTransactionId	string	Customer transaction ID
AdditionalRequestData	Array of key/value	A group that contains custom request data required by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.
Challenge *	string	Challenge code for the Key (28 characters).
DeviceType *	string	This is the Device name. The DeviceType used for this command can be one of the following values: `DynaPro, oDynamo, Generic, NotSpecified`
DeviceCert *	string	Device certificate (1908 characters)
KSI *	string	Key slot indicator. First 7 digits of the KSN.
KSN *	string	Key Serial Number of the device (20 HEX characters)
KeyType *	string	The Key Type used for this command can be one of the following values: `PIN, MSR, AMK`

Note: * = Required

Output Properties

Property	Value	Value Description
CustomerTransactionId	string	Customer transaction ID
MagTranId	string	Magensa assigned unique transaction ID in GUID form
AdditionalOutputData	Array of key/value	A group that contains additional output data returned by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.
BaseKCV	string	Base derivation key Key Check Value

CommandType	int	Type of command.
		`0 = Standard command`
		`1 = Extended command`

Description	string	Description of the command response
ExecutionTypeEnum	string	Execution type enumeration
ID	int	ID of the command response
Name	string	Name representing the function for Value
Value	string	This is the command to send to the PPSCRA device.
DukptKCV	string	DUKPT Key Check Value
KeyPrefix	string	Key Prefix
KeyType	string	The Key Type used for this command can be one of the following values: `PIN, MSR, AMK`

Sample GetKeyLoadCommand Request

```
POST https://rsgw.magensa.net/RemoteServicesv2Gateway/PPSCRAv2.svc HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://www.magensa.net/RemoteServices/v2/IPPSCRAv2/GetKeyLoadCommand"


<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v2="http://www.magensa.net/RemoteServices/v2/"
xmlns:rem="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core"
xmlns:sys="http://schemas.datacontract.org/2004/07/System.Collections.Generic">
   <soapenv:Header/>
   <soapenv:Body>
      <v2:GetKeyLoadCommand>
         <v2:request>
            <rem:Authentication>
               <rem:CustomerCode>123</rem:CustomerCode>
               <rem:Password>Password</rem:Password>
               <rem:Username>Username</rem:Username>
            </rem:Authentication>
            <rem:BillingLabel>label</rem:BillingLabel>
            <rem:CustomerTransactionID>123</rem:CustomerTransactionID>
            <rem:AdditionalRequestData>
               <sys:KeyValuePairOfstringstring>
                  <sys:key></sys:key>
                  <sys:value></sys:value>
               </sys:KeyValuePairOfstringstring>
            </rem:AdditionalRequestData>
            <rem:Challenge>0D0098D70CE31309160D00000000</rem:Challenge>
<rem:DeviceCert>308203B63082029EA003020102020A1B42F06800000000084D300D06092A864886F70D01010B050030
51310B300906035504061302555331133011060355040A130A4D616754656B20496E63312D302B06035504031324656E67
2D50434933785479706544657669636573 2D4C332D4465766963652D5375624341301E170D3135303331333135303131 35
5A170D3233303331333135313131355A3059310B30090603550406130255533115301306035504 0A130C4D616754656B2C
20496E632E31183016060355040B130F49504144203130302044657669636531193017060355040313103938443730 4345
333133303931363044308201 22300D06092A864886F70D01010105000382010F003082010A0282010100 9F28B853D4F3D1
4B1A0A3F89E2AC0852A69118BE9EEAFE7977B09E9789D0BA2A0317236005F8D3DE919CCE8737B16E3B94889ED3FDA0E886
E00C5BF1A88F3189433B2855684649DDF3E2EF0E0049DA945B2A4E2ED2BA5F0A46C9D0725AF321152B79A36A45CC022FC2
8F5529C90E75B39E297927251609A434CA032290C967DFD3813044529FDE450E2A82000C5817C729A5674560ECC058462D
BCAC7BB5C2F3D15CEEEB69D8C17418756627AB4E7FBA6977BA109BA39C63B0D27E1D86F8CADA6A74A465208E68A0712DF7
B9B5F5DD6D0808AEA4B54B82EE3C1D3BE4D4AA2BBA0F029463B3425FF26F708F8A2766CCE398C7D0DC93608C926B4CF2EE
BCBB982B0203010001A38187308184301D0603551D0E04160414E277E7E163A48AF01F7F8B1AC9C6B33F8BF48D31301F06
03551D23041830168014D19FC5704DA7D01A8CEA5D3B57E4C2382D0EAEF4300C0603551D130101FF04023000301006092B
06010401F6090201040304010030100609 2B06010401F6090202040304010230100609 2B06010401F60902030403040103
300D06092A864886F70D01010B05000382010100 7B5503C00FE0073FE4834FC367FF2EF289F9CE66084A54F482A08E0834
9D8C3ED99B17AAC65C0D913321034F65D39AE4B089116564D56BE3EA50BF47BB1649E482D45EB5A004F006D3D360136FAA
B8FE3529D7DAB850587A7636614979A0955CC73B919448E74B94B4CF4DEA0F7FA2F7F82F3629965F03E41511813D81262C
A1B843771BAD4B2A157B9E7085F6AF23F38EAC4022BFB7540CBB7550750520ED8BA04DD8D692F48743F5C4DF089362EC14
CED11BFA166168CDA15F26368F036FA29CDA8A2033107587C6531061053DB5849C9EC3EE3028D7E1538FE7292D156C5F97
16F20170B4BE14B3269CF51135B903FBC81A90E08B1B9DD1A9DC154749EFC1</rem:DeviceCert>
            <rem:DeviceType>DynaPro</rem:DeviceType>
            <rem:KSI>9500030</rem:KSI>
            <rem:KSN>950003000000012065A5</rem:KSN>
            <rem:KeyType>MSR</rem:KeyType>
         </v2:request>
      </v2:GetKeyLoadCommand>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample GetKeyLoadCommand Response

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body>
      <GetKeyLoadCommandResponse xmlns="http://www.magensa.net/RemoteServices/v2/">
         <GetKeyLoadCommandResult
xmlns:a="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
            <a:CustomerTransactionId>123</a:CustomerTransactionId>
            <a:MagTranId>bf40dd7e-6297-4b14-9bff-bfd612cbc159</a:MagTranId>
            <a:AdditionalOutputData i:nil="true"
xmlns:b="http://schemas.datacontract.org/2004/07/System.Collections.Generic"/>
            <a:BaseKCV>08D7B4</a:BaseKCV>
            <a:Command>
               <a:CommandType>0</a:CommandType>
               <a:Description>Key Injection</a:Description>
               <a:ExecutionTypeEnum>ALL</a:ExecutionTypeEnum>
               <a:ID>0</a:ID>
               <a:Name>ChangeKey</a:Name>

<a:Value>00010001150098D70CE31309160D0000000095000300001224205395B14D82BD62C6911C02BEA098B50AD617D
7B7EFB565B880EF3E2B72CF1BB158E2CA9D142DDED4440630E6370763834471B1CAE48C084E81578259D534E82930F71F5
C1BB3AA6624DD773DACC1185F515AF00DB5A566F567F0F97E7EA7E02CDBC1BD47D8D0760B22A645676CADDD60EB5BB2542
6E8C97016F0D01F1D36449FEF9A24F73653D2682844E7CA473BF880C00FD8B8D40721CF08882BBC00410C244B9395222D1
11F2D66E21AF1BEAFAD5AB0A214E4B7B796D3DFE11E33ADB359EA2B6DDF2056A25B674AFCBCA4D15C16B1E1860FD24F1BA
26F707088D362EFB37CA27E0C2D9AC732F867E21F63FDFC5B1400662FDF1FE8FC789D70417F404E6727136A4C4E1C4B974
99F6EFB225EFD1E9B239F53110226396563EFDC5C639ED1E73FFEC659AD4079443F1E0253E9691F2885E9CA229DFA458B0
B6FA536AE6DF765E0FB6D42E706A0043AE57B0AED6832574F13905B86386F88E9996E65484B8C0961ACD61CC94473F132A
D994E5B2D70EECCDF16FB282A0C547B5666A4ED5C2208B7A7BCA45C81452CF1C343BB19805C19865D0963BEB980AF00965
B302CBF16BAB3FF2E47D9CB8AED25B3E6E11A108D4676797F8FBC1D559A235B47A65A3FB06B4AC82E3A5011639A843CE83
665A4B984C78109B2C9CC76FB6AC8987BE69529C2149AE2043828B327DA79AE3BC7F63EEAD86B2DD78482DA7033244E266
13C7366</a:Value>
            </a:Command>
            <a:DukptKCV>6ED7CC</a:DukptKCV>
            <a:KeyPrefix i:nil="true"/>
            <a:KeyType>MSR</a:KeyType>
         </GetKeyLoadCommandResult>
      </GetKeyLoadCommandResponse>
   </s:Body>
</s:Envelope>
```

4.5 GetLoadConfigCommand

A command used to get the command which is to be sent to the device for loading the configuration.

Input Properties

Property (*)	Value	Value Description
CustomerCode *	string	Customer code
Username *	string	The User Identification credential created and assigned by MagTek.
Password *	string	The password for the credential.
BillingLabel	string	Billing Label (no more than 64 characters)
CustomerTransactionId	string	Customer transaction ID
AdditionalRequestData	Array of key/value	A group that contains custom request data required by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.
Challenge *	string	Challenge code for the configuration to be loaded (28 characters).
CommandId *	string	The value from the ID field of the command: `GetCommandListByDevice`
ConfigData *	string	Value for the configuration data
DeviceType *	string	This is the Device name. The DeviceType used for this command can be one of the following values: `DynaPro, DynaProGO, oDynamo, Generic, NotSpecified`
ExistingConfig *	string	The configuration value before it is to be changed.
KSN *	string	Key Serial Number of the device (20 HEX characters)

Property (*)	Value	Value Description
KeyType *	string	The Key Type used for this command can be one of the following values: `PIN, MSR`

Note: * = Required

Output Properties

Property	Value	Value Description
CustomerTransactionId	string	Customer transaction ID
MagTranId	string	Magensa assigned unique transaction ID in GUID form
AdditionalOutputData	Array of key/value	A group that contains additional output data returned by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.

CommandType	int	Type of command.
		`0 = Standard command`
		`1 = Extended command`

Description	string	Description of the command response
ExecutionTypeEnum	string	Execution type enumeration
ID	int	ID of the command response
Name	string	Name representing the function for the Value field
Value	string	This is the value to send to the PPSCRA device for loading a configuration.

Sample GetLoadConfigCommand Request

```
POST https://rsgw.magensa.net/RemoteServicesv2Gateway/PPSCRAv2.svc HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://www.magensa.net/RemoteServices/v2/IPPSCRAv2/GetLoadConfigCommand"


<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v2="http://www.magensa.net/RemoteServices/v2/"
xmlns:rem="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core"
xmlns:sys="http://schemas.datacontract.org/2004/07/System.Collections.Generic">
   <soapenv:Header/>
   <soapenv:Body>
      <v2:GetLoadConfigCommand>
         <v2:request>
            <rem:Authentication>
               <rem:CustomerCode>123</rem:CustomerCode>
               <rem:Password>Password</rem:Password>
               <rem:Username>Username</rem:Username>
            </rem:Authentication>
            <rem:BillingLabel>label</rem:BillingLabel>
            <rem:CustomerTransactionID>123</rem:CustomerTransactionID>
            <rem:AdditionalRequestData>
               <sys:KeyValuePairOfstringstring>
                  <sys:key/>
                  <sys:value/>
               </sys:KeyValuePairOfstringstring>
            </rem:AdditionalRequestData>
            <rem:Challenge>0BFF98D70CE31309160D75A73F21</rem:Challenge>
            <rem:ConfigCommands>
               <rem:DeviceConfigCommand>
```

```
                  <rem:CommandId>80</rem:CommandId>
                  <rem:ConfigData>49</rem:ConfigData>
               </rem:DeviceConfigCommand>
            </rem:ConfigCommands>
            <rem:DeviceType>DynaPro</rem:DeviceType
            <rem:ExistingConfig>090800C0D530640100</rem:ExistingConfig>
            <rem:KSN>95000300000054920001B</rem:KSN>
            <rem:KeyType>MSR</rem:KeyType>
         </v2:request>
      </v2:GetLoadConfigCommand>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample GetLoadConfigCommand Response

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body>
      <GetLoadConfigCommandResponse xmlns="http://www.magensa.net/RemoteServices/v2/">
         <GetLoadConfigCommandResult
xmlns:a="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
            <a:CustomerTransactionId>123</a:CustomerTransactionId>
            <a:MagTranId>8e774f3b-2326-4502-b8ef-6a90f386d74e</a:MagTranId>
            <a:AdditionalOutputData i:nil="true"
xmlns:b="http://schemas.datacontract.org/2004/07/System.Collections.Generic"/>
            <a:Command>
               <a:CommandType>0</a:CommandType>
               <a:Description>Load Config</a:Description>
               <a:ExecutionTypeEnum>ALL</a:ExecutionTypeEnum>
               <a:ID>0</a:ID>
               <a:Name>LoadConfig</a:Name>

<a:Value>000109000BFF98D70CE31309160D75A70000091802C0D53044010007910F883BE0B57E968F8F27626D9921DCF
2B6C5CD907FD58DEE30A96FF53114B1D3BEFEE5BE5558FE9B2FB6AB4D2912DB08BCC17E17EF58AA3503006A7892CBB49B7
767AD8AD5BCD60CF87936000B150A4855D117201DAEBD8ACEC7B5268E91750B05B3C2455F74DD18D492B20DCEEF760D848
66D854A3B1EB4579FDEF2071C97FD5871DAE3301A4711E0D27F23717C547F844D2EDE9A5416F91348D7AA76E847762AA70
6B14B28D650E4C3A1DAF91C241E9ADABC5633B6746EDF80962ED9F6AA0A6B4AFD497BDB1966433BECC358D53F7643FC1EF
521C16875463DCD95E27FA0DDBDD7B3925D36BC915AF697055B6AAA6E987906EF236814722C856A2F695A</a:Value>
            </a:Command>
            <a:TargetConfig>091802C0D530440100</a:TargetConfig>
         </GetLoadConfigCommandResult>
      </GetLoadConfigCommandResponse>
   </s:Body>
</s:Envelope>
```

4.6 GetDeviceAuthCommand

A command used to get the command which is to be sent to the device for device authentication.

Input Properties

Property (*)	Value	Value Description
CustomerCode *	string	Customer code
Username *	string	The User Identification credential created and assigned by MagTek.
Password *	string	The password for the credential.
BillingLabel	string	Billing Label (no more than 64 characters)
CustomerTransactionId	string	Customer transaction ID
AdditionalRequestData	Array of key/value	A group that contains custom request data required by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.

Property (*)	Value	Value Description
Challenge *	string	Challenge code for the configuration to be loaded (28 characters)
DeviceCert *	string	Device certificate (1908 characters)
DeviceType *	string	This is the Device name. The DeviceType used for this command can be one of the following values: `DynaPro, DynaProGO, oDynamo, Generic, NotSpecified`
KeyType *	string	The Key Type used for this command can be one of the following values: `PIN, MSR`

Note: * = Required

Output Properties

Property	Value	Value Description
CustomerTransactionId	string	Customer transaction ID
MagTranId	string	Magensa assigned unique transaction ID in GUID form
AdditionalOutputData	Array of key/value	A group that contains additional output data returned by the target web service. Elements are expressed as Key/Value pairs grouped under <KeyValuePairOfstringstring>. See examples.

CommandType	int	Type of command.
		`0 = Standard command`
		`1 = Extended command`

Description	string	Description of the command response
ExecutionTypeEnum	string	Execution type enumeration
ID	int	ID of the command response
Name	string	Name representing the function for the Value field
Value	string	This is the value to send to the PPSCRA device.

Sample GetDeviceAuthCommand Request

```
POST https://rsgw.magensa.net/RemoteServicesv2Gateway/PPSCRAv2.svc HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://www.magensa.net/RemoteServices/v2/IPPSCRAv2/GetDeviceAuthCommand"

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v2="http://www.magensa.net/RemoteServices/v2/"
xmlns:rem="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core"
xmlns:sys="http://schemas.datacontract.org/2004/07/System.Collections.Generic">
   <soapenv:Header/>
   <soapenv:Body>
      <v2:GetDeviceAuthCommand>
         <v2:request>
            <rem:Authentication>
               <rem:CustomerCode>123</rem:CustomerCode>
               <rem:Password>password</rem:Password>
               <rem:Username>username</rem:Username>
            </rem:Authentication>
            <rem:BillingLabel>label</rem:BillingLabel>
            <rem:CustomerTransactionID>123</rem:CustomerTransactionID>
            <rem:AdditionalRequestData>
               <sys:KeyValuePairOfstringstring>
```

```
                  <sys:key/>
                  <sys:value/>
               </sys:KeyValuePairOfstringstring>
            </rem:AdditionalRequestData>
            <rem:Challenge>0D0098D70CE31309160D00000000</rem:Challenge>

<rem:DeviceCert>308203B63082029EA003020102020A1B42F06800000000084D300D06092A864886F70D01010B050030
51310B3009060355040613025553311330110603550408130A4D616754656B20496E63312D302B0603550403132465 6E67
2D50434933785479706544657669636573 2D4C332D4465766963652D5375624341301E170D313530333133313530313135
5A170D3233303331333135313131355A3059310B30090603550406130255533115301306035504 0A130C4D616754656B2C
20496E632E31183016060355040B130F495041442031303020446576696365311930170603550403131039384437304345
3331333039313630443082012230 0D06092A864886F70D01010105000382010F003082010A02820101009F28B853D4F3D1
4B1A0A3F89E2AC0852A69118BE9EEAFE7977B09E9789D0BA2A0317236005F8D3DE919CCE8737B16E3B94889ED3FDA0E886
E00C5BF1A88F3189433B2855684649DDF3E2EF0E0049DA945B2A4E2ED2BA5F0A46C9D0725AF321152B79A36A45CC022FC2
8F5529C90E75B39E297927251609A434CA032290C967DFD3813044529FDE450E2A82000C5817C729A5674560ECC058462D
BCAC7BB5C2F3D15CEEEB69D8C17418756627AB4E7FBA6977BA109BA39C63B0D27E1D86F8CADA6A74A465208E68A0712DF7
B9B5F5DD6D0808AEA4B54B82EE3C1D3BE4D4AA2BBA0F029463B3425FF26F708F8A2766CCE398C7D0DC93608C926B4CF2EE
BCBB982B0203010001A38187308184301D0603551D0E04160414E277E7E163A48AF01F7F8B1AC9C6B33F8BF48D31301F06
03551D23041830168014D19FC5704DA7D01A8CEA5D3B57E4C2382D0EAEF4300C0603551D130101FF04023000301006092B
06010401F609020104030401003010 06092B06010401F6090202040304010230 1006092B06010401F60902030403040103
300D06092A864886F70D01010B05000382010100 7B5503C00FE0073FE4834FC367FF2EF289F9CE66084A54F482A08E0834
9D8C3ED99B17AAC65C0D913321034F65D39AE4B089116564D56BE3EA50BF47BB1649E482D45EB5A004F006D3D360136FAA
B8FE3529D7DAB850587A7636614979A0955CC73B919448E74B94B4CF4DEA0F7FA2F7F82F3629965F03E41511813D81262C
A1B843771BAD4B2A157B9E7085F6AF23F38EAC4022BFB7540CBB7550750520ED8BA04DD8D692F48743F5C4DF089362EC14
CED11BFA166168CDA15F26368F036FA29CDA8A2033107587C6531061053DB5849C9EC3EE3028D7E1538FE7292D156C5F97
16F20170B4BE14B3269CF51135B903FBC81A90E08B1B9DD1A9DC154749EFC1</rem:DeviceCert>
            <rem:DeviceType>DynaProGO</rem:DeviceType>
            <rem:KeyType>MSR</rem:KeyType>
         </v2:request>
      </v2:GetDeviceAuthCommand>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample GetDeviceAuthCommand Response

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body>
      <GetDeviceAuthCommandResponse xmlns="http://www.magensa.net/RemoteServices/v2/">
         <GetDeviceAuthCommandResult
xmlns:a="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
            <a:CustomerTransactionId>123</a:CustomerTransactionId>
            <a:MagTranId>c597cad7-9d53-4a96-93f8-94cf2557e0ee</a:MagTranId>
            <a:AdditionalOutputData i:nil="true"
xmlns:b="http://schemas.datacontract.org/2004/07/System.Collections.Generic"/>
            <a:Command>
               <a:CommandType>0</a:CommandType>
               <a:Description>Device Authentication</a:Description>
               <a:ExecutionTypeEnum>ALL</a:ExecutionTypeEnum>
               <a:ID>0</a:ID>
               <a:Name>DeviceAuthCommand</a:Name>

<a:Value>000100010D0098D70CE31309160D0000000354797E1DD1522202F0E8B5BDF77FF21E57DAD2325C361A5CC47D
D472C2B25CE8E9129DA15D8D27AA9C72EB055BED8E67933A0DFA57040BD5FFE569C1674E5E75015668534E176D35E73D93
B289E2EDE49C6281EAC580D31EBFC18321A46B8C87AE4A0C4E0D93D46D1EE2BB42064340172F3307B3361B7391529601D0
D0F333BA781CE29A2253DC5E6E1067B4E2BD1A302CC6A7CC174D97FE7532F0647741B4A43EFFF6DF6EAABFFEB3E0D2749B
BCBFE1DC549C9D6D7B5E1FA55B326BF84C16E1F2286143FB71FC6494C0698304556C5C2311428CC05DC10BE11694F00E09
280D5C4CAA7A522DA91C8F2888B38CAD0DA58B0B13291F2063B64E9AABBF975A14B7B59EDF8EFB2D8AEDAF4971D16FAA14
8924CA709B30E4128273D667EB8A3F0B8FA530B7C5B6C83F0F6D304091E6FA71325D2F5FC2612F29994E62C0921ACA3783
76A7998C458C78703BB0CD23D1957208911BC3342A801C72402E52BA8571D6DEDC63D8689983CEAB288CBB15A89A5A5758
ECE7696BF29C0E5E85CE908C3D977D77F113DB2DFB2280FB2E959046E5B9176DFDC60B81A9C1E53D12E496D384F25F2003
813F27EF1A458C95CE000499CE063248636187E647AF770BADEC4D1E2D53E35588B48F34362E4F12BA609798E6E83DAAAD
12C2297598239545DED95C9F820ED34C30B93CCAA07A92063CE352120ECE375E5821B60CAA233B0681A7F6F43</a:Value
>
            </a:Command>
            <a:KCV>76956A18</a:KCV>
            <a:KeyType>MSR</a:KeyType>
         </GetDeviceAuthCommandResult>
      </GetDeviceAuthCommandResponse>
   </s:Body>
</s:Envelope>
```

4.7 GetKeyList

A command used to retrieve a list of key properties.

Input Properties

Property (*)	Value	Value Description
CustomerCode *	string	Customer code
Username *	string	The User Identification credential created and assigned by MagTek
Password *	string	The password for the credential
BillingLabel	string	Billing Label (no more than 64 characters)
CustomerTransactionId	string	Customer transaction ID

Note: * = Required

Output Properties

Property	Value	Value Description
CustomerTransactionId	string	Customer transaction ID
MagTranId	string	Magensa assigned unique transaction ID in GUID form
Description	string	Description of the key
ID	int	ID of the key
KSI	string	Key slot indicator. First 7 digits of the KSN.
KeyName	string	Name of the key
KeySlotNamePrefix	string	Prefix of the key slot

Sample GetKeyList Request

```
POST https://rsgw.magensa.net/RemoteServicesv2Gateway/PPSCRAv2.svc HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://www.magensa.net/RemoteServices/v2/IPPSCRAv2/GetKeyList"

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v2="http://www.magensa.net/RemoteServices/v2/"
xmlns:rem="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core">
   <soapenv:Header/>
   <soapenv:Body>
      <v2:GetKeyList>
         <v2:request>
            <rem:Authentication>
               <rem:CustomerCode>123</rem:CustomerCode>
               <rem:Password>password</rem:Password>
               <rem:Username>username</rem:Username>
            </rem:Authentication>
            <rem:BillingLabel>label</rem:BillingLabel>
            <rem:CustomerTransactionID>123</rem:CustomerTransactionID>
         </v2:request>
      </v2:GetKeyList>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample GetKeyList Response

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body>
      <GetKeyListResponse xmlns="http://www.magensa.net/RemoteServices/v2/">
         <GetKeyListResult xmlns:a="http://schemas.datacontract.org/2004/07/RemoteServicesv2.Core" 
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
            <a:CustomerTransactionId>123</a:CustomerTransactionId>
            <a:MagTranId>e816a85a-16b4-4f5a-b448-aae6e5a9d35b</a:MagTranId>
            <a:Keys>
               <a:Key>
                  <a:Description>Currently Loaded Key</a:Description>
                  <a:ID>1</a:ID>
                  <a:KSI>0000000</a:KSI>
                  <a:KeyName>Current Key</a:KeyName>
                  <a:KeySlotNamePrefix>Prod</a:KeySlotNamePrefix>
               </a:Key>
               <a:Key>
                  <a:Description>the test key we use for ANSI test</a:Description>
                  <a:ID>2</a:ID>
                  <a:KSI>9010010</a:KSI>
                  <a:KeyName>ANSI Test Key</a:KeyName>
                  <a:KeySlotNamePrefix>Test</a:KeySlotNamePrefix>
               </a:Key>
            </a:Keys>
         </GetKeyListResult>
      </GetKeyListResponse>
   </s:Body>
</s:Envelope>
```

5 Status Codes and Messages

Status Codes and Messages returned by Magensa for PPSCRAv2 Operations.

Internal errors

Code	StatusMsg	Notes
5000	Unknown Error	

Input Validation errors

Code	StatusMsg	Notes
601	DeviceSN is required	
602	KSN is required	
603	CustomerCode is required	
604	Username is required	
605	Password is required	
606	KSI is required	
607	KSN is not valid	Value was not HEX or too long.
608	DeviceCert is required	
610	Challenge is required	
613	Device config is not valid	
614	KeyType is not valid	
615	CustomerTransactionID is not valid	Value was longer than 256 characters.
616	BillingLabel is not valid	Value was longer than 64 characters.
625	KSI is not valid	Value was longer than 16 characters.
626	DeviceCert is not valid	Value was not equal to length of 1908 characters.
627	Challenge is not valid	Value was not equal to length of 28 characters.
628	DeviceSN is not valid	
701	Access Denied	Returned when user cannot be authenticated or authorized for any reason such as invalid username, invalid password, or account locked.
702	Device Not Allowed	The device is not active in the database.
709	Device type is not supported	
1013	User credential failed authentication	