Security

Securing Packages and Integration Services Operations

Stacia Misner
blog.datainspirations.com
@StaciaMisner

Overview

- **Package Security Settings**

- **Security for Package Deployment Model**

- **Security for Project Deployment Model**

- **Security for Scheduled Packages**

Package Security Settings

Package Protection Level

Digital Signature

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

Default

EncryptSensitiveWithPassword

EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

Sensitive Data…
- Connection string password
- Auto-generated sensitive XML nodes of task
- Marked system variables

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

DTSX

Package Protection Level

Don'tSaveSensitive

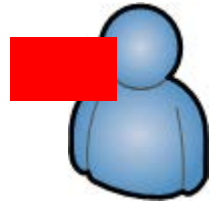EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

DTSX

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

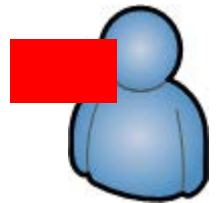EncryptSensitiveWithPassword

Enc...

DTSX

```
<DTS:Password
        DTS:Name="Password"
        Sensitive="1"
        Encrypted="1">AQAAANCMnd8...</DTS:Password>
```

EncryptAllWithUserKey

ServerStorage

Package
Creator

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

Enc...

EncryptAllWithUserKey

ServerStorage

DTSX

```
<DTS:Password
          DTS:Name="Password"
          Sensitive="1"
          Encrypted="1">AQAAANCMnd8...</DTS:Password>
```

Package
Creator

User
login

Decryption

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

DTSX

Failed to decrypt protected XML node "DTS:Property" with error 0x8009000B "Key not valid for use in specified state.". You may not be authorized to access this information. This error occurs when there is a cryptographic error. Verify that the correct key is available.
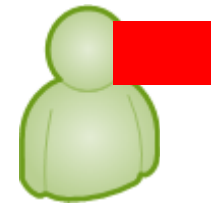
EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

Package Developer/ Operator

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

~~EncryptAllWithPassword~~

DTSX

Package Creator

Package Developer/ Operator

```xml
<EncryptedData
    Type="http://www.w3.org/2001/04/xmlenc#Element"
    Salt="MFpFqii7ow=="
    IV="s5R40RppoDA=" xmlns="http://www.w3.org/2001/04/xmlenc#">
    <EncryptionMethod
        Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
    <CipherData>
        <CipherValue>s5R40Rppo…</CipherValue>
    </CipherData>
</EncryptedData>
```

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

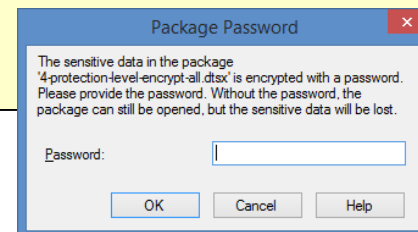EncryptAllWithPassword

DTSX

Package Creator

Package Developer/ Operator

```xml
<EncryptedData
    Type="http://www.w3.org/2001/04/xmlenc#Element"
    Salt="MFpFqii7ow=="
    IV="s5R40RppoDA=" xmlns="http://www.w3.org/2001/04/xmlenc#">
    <EncryptionMethod
      Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
    <CipherData>
      <CipherValue>s5R40Rppo…</CipherValue>
    </CipherData>
</EncryptedData>
```

Decryption

Package Password

The sensitive data in the package
'4-protection-level-encrypt-all.dtsx' is encrypted with a password.
Please provide the password. Without the password, the
package can still be opened, but the sensitive data will be lost.

Password:

OK   Cancel   Help

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

DTSX

Failed to decrypt an encrypted XML node because the password was not specified or not correct. Package load will attempt to continue without the encrypted information.
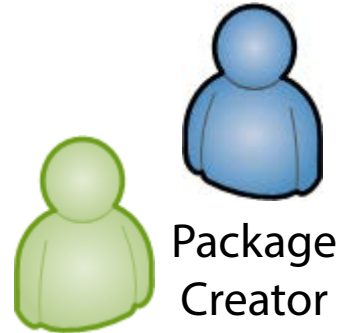
Package Creator

Package Developer/ Operator

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

EncryptAllWithPassword

DTSX

Package Creator

Package Developer/ Operator

```xml
<?xml version="1.0"?><EncryptedData
Type="http://www.w3.org/2001/04/xmlenc#Element"
Salt="vSVMnwavsA==" IV="PCw4PcYDd1M="
xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
  <CipherData>
    <CipherValue>PCw4PcYDd1PNy…</CipherValue>
  </CipherData>
</EncryptedData>
```

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

DTSX

Package Creator

Package Developer/ Operator

The package is encrypted with a password. The password was not specified, or is not correct.

Package Protection Level

```
<DTS:Executable xmlns:DTS="www.microsoft.com/SqlServer/Dts"
DTS:refId="Package"
.
.
DTS:PackageType="5"
DTS:ProtectionLevel="4"
DTS:VersionBuild="15"
DTS:VersionGUID="{6F00CF37-9717-4838-81EE-4CE19EBE2979}"
Encrypted="1">AQAAANCMnd...
</DTS:Executable>
```

DTSX

Package Creator

User login

EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

Package Protection Level

Don'tSaveSensitive

Failed to decrypt a package that is encrypted with a user key. You may not be the user who encrypted this package, or you are not using the same machine that was used to save the package.

Failed to remove package protection with error 0x8009000B "Key not valid for use in specified state.". This occurs in the CPackage::LoadFromXML method.
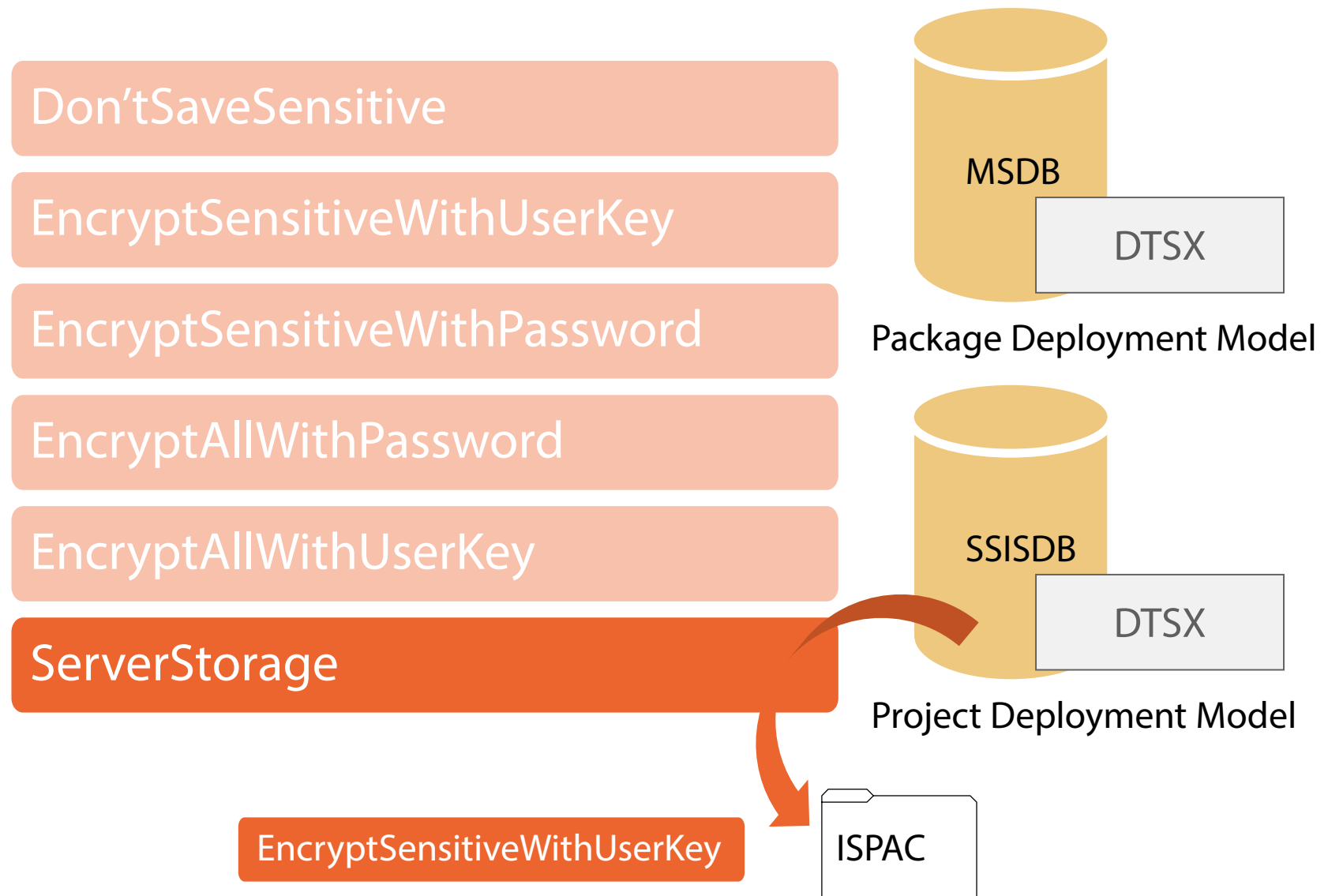
EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

Package
Developer/
Operator

Package Protection Level

Don'tSaveSensitive

EncryptSensitiveWithUserKey

EncryptSensitiveWithPassword

EncryptAllWithPassword

EncryptAllWithUserKey

ServerStorage

EncryptSensitiveWithUserKey

MSDB

DTSX

Package Deployment Model

SSISDB

DTSX

Project Deployment Model

ISPAC

Digital Signatures

Pre-Deployment	Pre-Execution		
Digital signature assignment	Package Designer (SSDT or BIDS)	DTExec Command Prompt Utility	Registry value
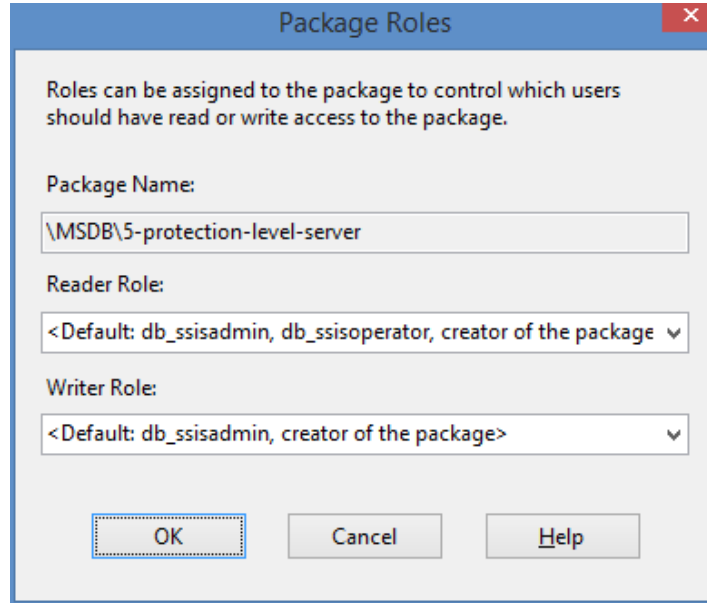
Security for Package Deployment Model

Package Roles

Roles can be assigned to the package to control which users should have read or write access to the package.

Package Name:

\MSDB\5-protection-level-server

Reader Role:

<Default: db_ssisadmin, db_ssisoperator, creator of the package ⌄

Writer Role:

<Default: db_ssisadmin, creator of the package> ⌄

OK   Cancel   Help

- **Reader**
  - □ Execute package
  - □ View package
  - □ Export package

- **Writer**
  - □ Overwrite package
  - □ Delete package
  - □ Secure package
  - □ Stop package

Firewalls

SSIS Service
TCP/IP Port 135

SQL Server database
TCP/IP Port 1433
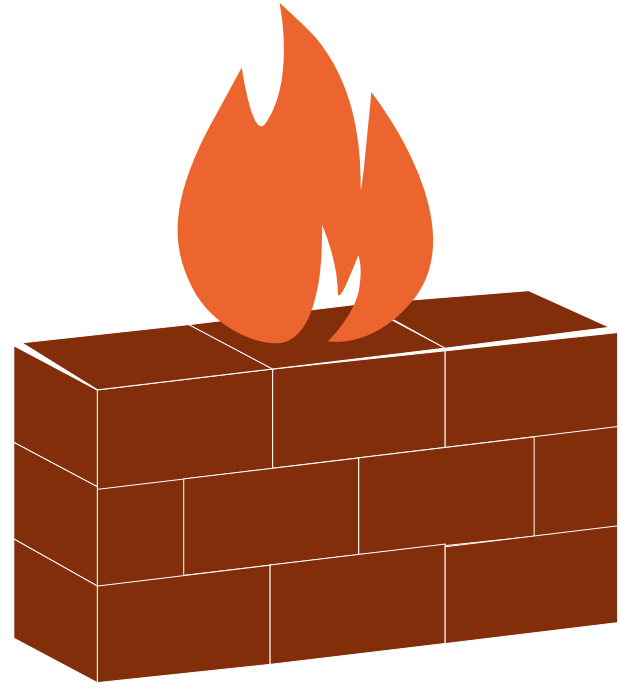
Security for Project Deployment Model

Permission		Securable Objects				
	Catalog	Folder	Project	Environment	Operation
Read	Y	Y	Y	Y	Y
Modify	Y	Y	Y	Y	Y
Execute	Y		Y		
Manage Permissions	Y	Y	Y	Y	Y
Create Objects	Y	Y			
Read Objects	Y	Y			
Modify Objects	Y	Y			
Execute Objects	Y	Y			
Manage Object Permissions	Y	Y			
Configure Catalog	Y				

Implicit settings for
ssis_admin role

Configure Security

Graphical User Interface

catalog.effective_object_permissions

catalog.explicit.object_permissions

catalog.grant_permission

catalog.deny_permission

catalog.revoke_permission

Stored Procedures

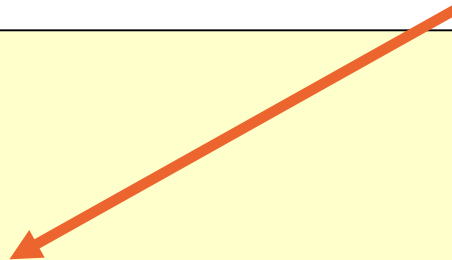# Sensitive Data in Parameters

Name	Data type	Value	Sensitive	Required
NotSensitive	String	This parameter value is visible.	False	False
Sensitive	String	************	True	False

Encrypts value in
package and catalog

```
<SSIS:Parameter
     SSIS:Name="Sensitive">.
.
<SSIS:Property
        SSIS:Name="Value"
        SSIS:Sensitive="1">AQAAANCMnd8BF...</SSIS:Property>
     <SSIS:Property
```
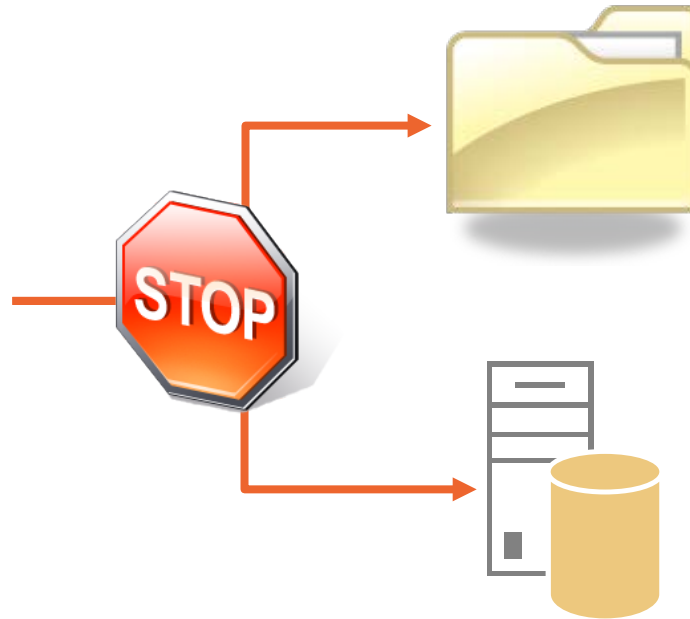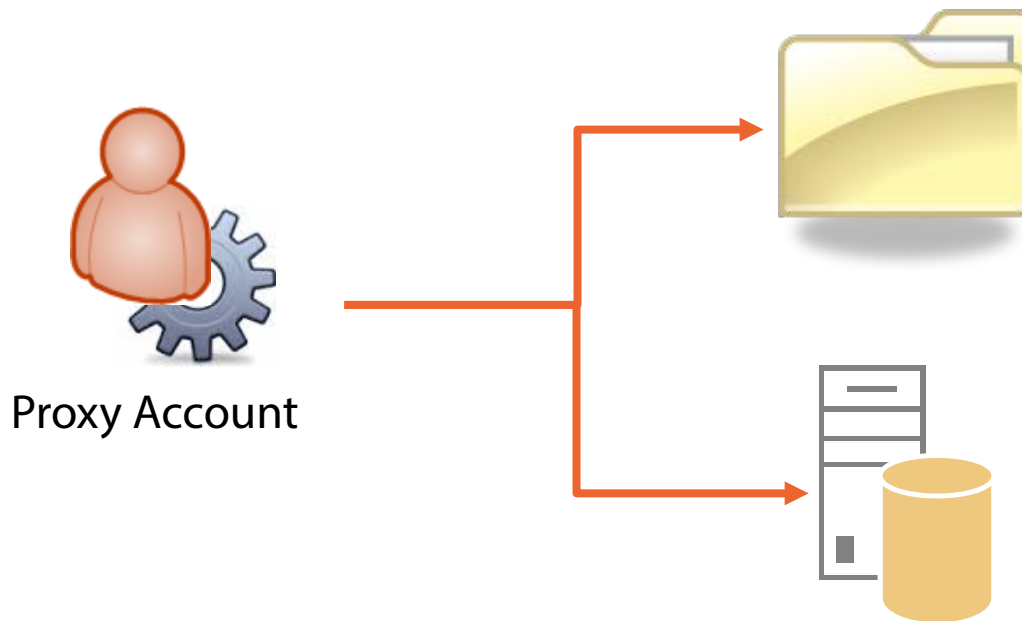
Security for Scheduled Packages

Security for Scheduled Packages

SQL Server Agent

Proxy Account

In SSMS…
1. Create New Credential in Security
2. Create New Proxy in SQL Server Agent

Summary

- **Package Security Settings**

  - Package protection level, digital signature

- **Security for Package Deployment Model**

  - Reader and writer roles, firewall settings

- **Security for Project Deployment Model**

  - Securable objects, permissions for user/group/role, parameters

- **Security for Scheduled Packages**

  - SQL Server Agent service account, proxy account

Resources

- **Access Control for Sensitive Data in Packages**

    □ http://tinyurl.com/yz89ubf

- **Identify the Source of Packages with Digital Signatures**

    □ http://tinyurl.com/kpnvvxg

- **Assign a Reader and Writer Role to a Package**

    □ http://tinyurl.com/mr7uz82