

Encryption How-To 101

Agenda

- ▣ Implementation:
 - Encryption Types
 - DBA responsibilities
 - Developer's role
 - Encryption, Speed, and 1 way hashes
- ▣ Maintenance:
 - Backup/restore
 - Storage of backup keys
 - Cross Server ...
- ▣ (all with just 16 slides and two Demo's)

Encryption How-To 101

Sources

Marcin Policht

Mike Good

Eric Brown

Keith Combs

John Magnabosco

Database Journal

SqlServerCentral

Simple-Talk

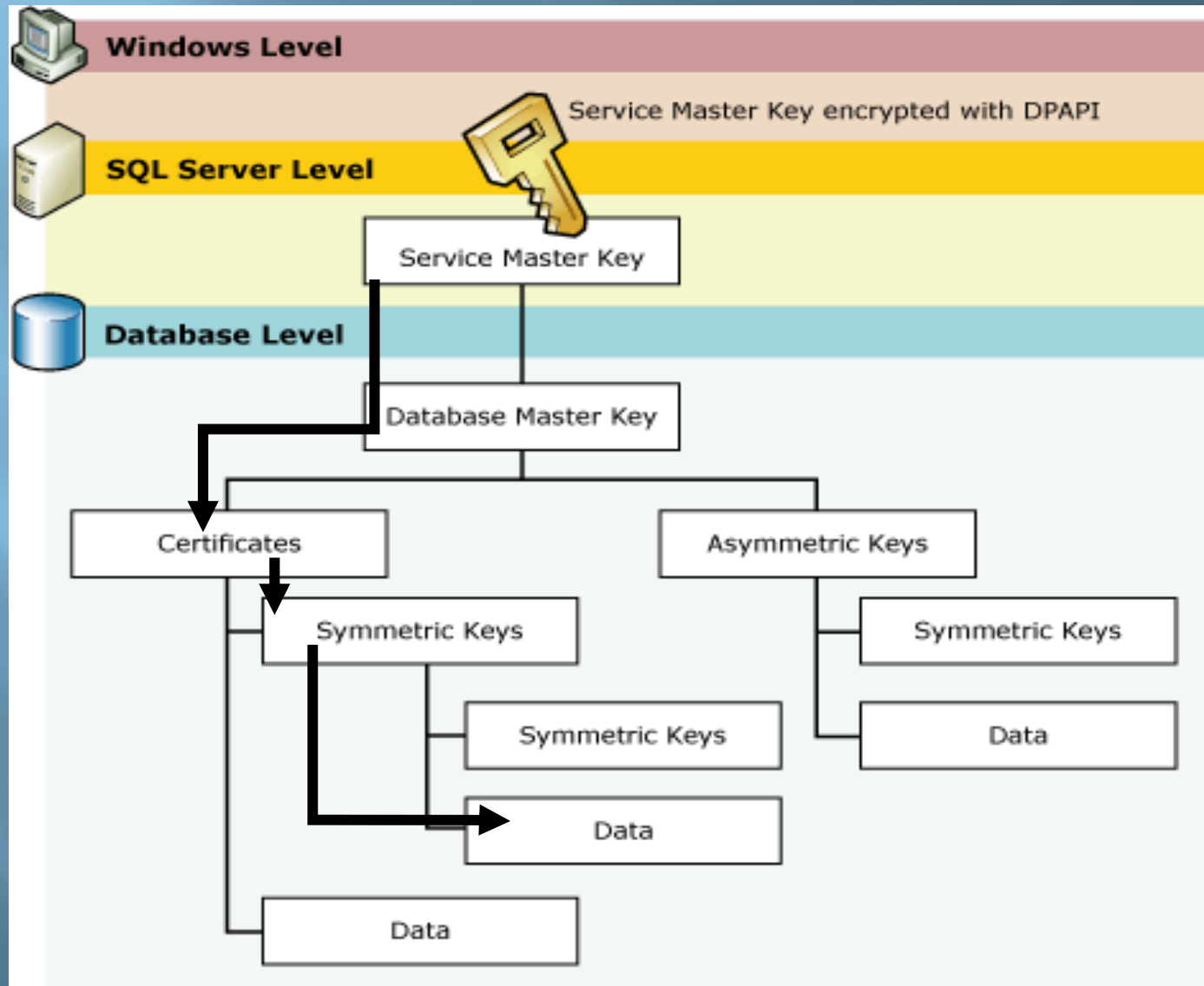
Microsoft-Technet

Simple-Talk (Book)

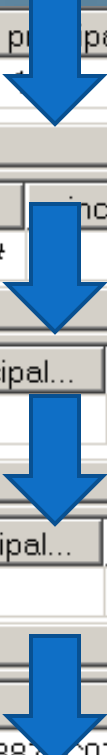
Encryption How-To 101

Algorithm Family	Algorithm	Cipher Type	Text Processing Block size	Key Size	Comments
Advanced Encryption Standard	AES 128	block	128 bit	128 bits	
	AES 192			192 bits	
	AES 256			256 bits	
Data Encryption Standard	DES	block	64 bit	56 bits	
	Triple_DES			168, 128 (SQL), 192 with Triple_des_3key	used for database master key (no option)
	DESX-same as Triple_DES)				
Rivest Cipher	RC2	Block	64 bit	64 bits	
	RC4	Stream		40-256 bits	To be removed from SQL
	128-bit RC4	Stream		128 bits	

Encryption How-To 101



Encryption How-To 101



	DbName	name	principal...	symmetric_key...	key_len...	key_algorit...	algorithm_de...	cre
1	encrypt	##MS_ServiceMasterKey##		102	128	D3	TRIPLE_DES	20

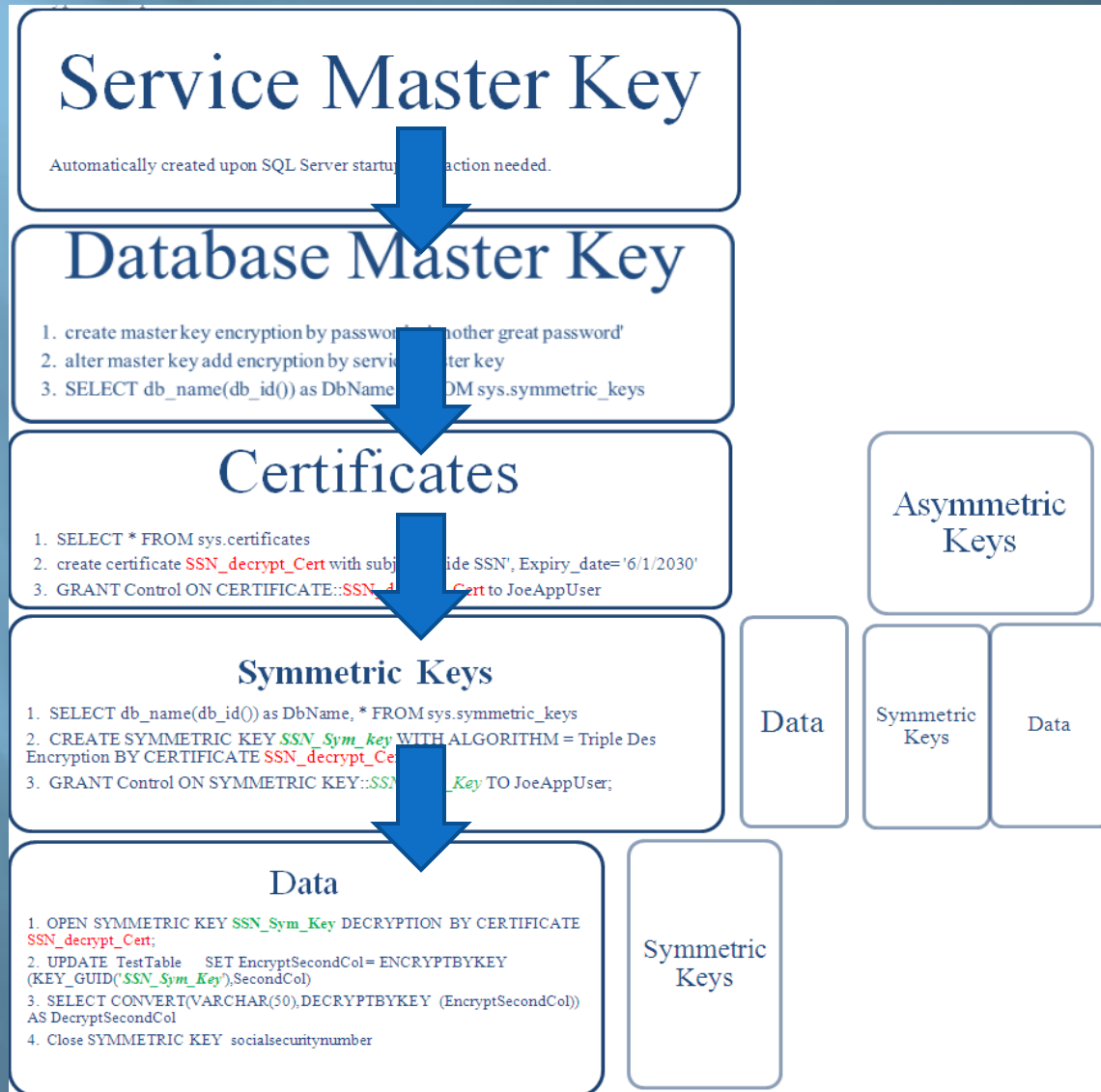
	DbName	name	principal...	symmetric_key...	key_len...	key_algorit...	algorithm_de...	
1	encrypt	##MS_DatabaseMasterKey##		101	128	D3	TRIPLE_DES	

	name	certificate...	principal...	pvt_key_encryption_t...	pvt_key_encryption_type_desc	is_active_f
1	SSN_decrypt_Cert	256	1	MK	ENCRYPTED_BY_MASTER_KEY	1

	DbName	name	principal...	symmetric_key...	key_len...	key_algorit...	algorithm_de...	create
1	encrypt	SocialSecurityNumber	1	256	128	D3	TRIPLE_DES	2010-0

	LastName	EncryptedSSN
1	Schneider	0x00A58CDEB5EE40CA2B887FC0780D1C9F010000006A12A5...
2	Schneider	0x00A58CDEB5EE40CA2B887FC0780D1C9F010000003D9B07...

Encryption How-To 101



Encryption How-To 101

A DBA needs to know:

1. create master key
2. create certificate
3. create Symmetric key

7. `select * from sys.symmetric_keys`
8. `select * From sys.openkeys`
9. `select *f rom sys.certificates`

4. alter master key
5. open master key
6. open Symmetric key

10. grant control on Certificate
11. grant view definition on symmetric key
12. `select * from sys.Database_permissions`

Encryption How-To 101

A developer needs to know:

1. OPEN SYMMETRIC KEY **SSN_Sym_Key** DECRYPTION
BY CERTIFICATE **SSN_decrypt_Cert**;
2. UPDATE TestTable SET EncryptSecondCol = ENCRYPTBYKEY
(KEY_GUID(**'SSN_Sym_Key'**),SecondCol)
3. SELECT CONVERT(VARCHAR(50),DECRYPTBYKEY
(EncryptedSecondCol)) AS DecryptedSecondCol
4. Close SYMMETRIC KEY SSN_Sym_Key

Encryption How-To 101

Demo!

1. Databases from scratch ... no hocus-pocus!
2. Create & turn-off/on keys
3. What do you get if you can't decrypt data?
4. How to get good speed AND encryption
5. Show how & why to use both 1-way & 2-way together
6. Show Granting of access to encryption to a user

Encryption How-To 101

Switching from Implementation... to Maintenance

Encryption How-To 101

1. BACKUP SERVICE MASTER KEY TO FILE =
'c:\sqldata\keys\service_master_key ENCRYPTION BY
PASSWORD = '\$what a great password\$'

2. RESTORE SERVICE MASTER KEY FROM FILE
='d:\sqldata\keys\service_master_key_orig' DECRYPTION
BY PASSWORD = '\$what a great password\$' FORCE

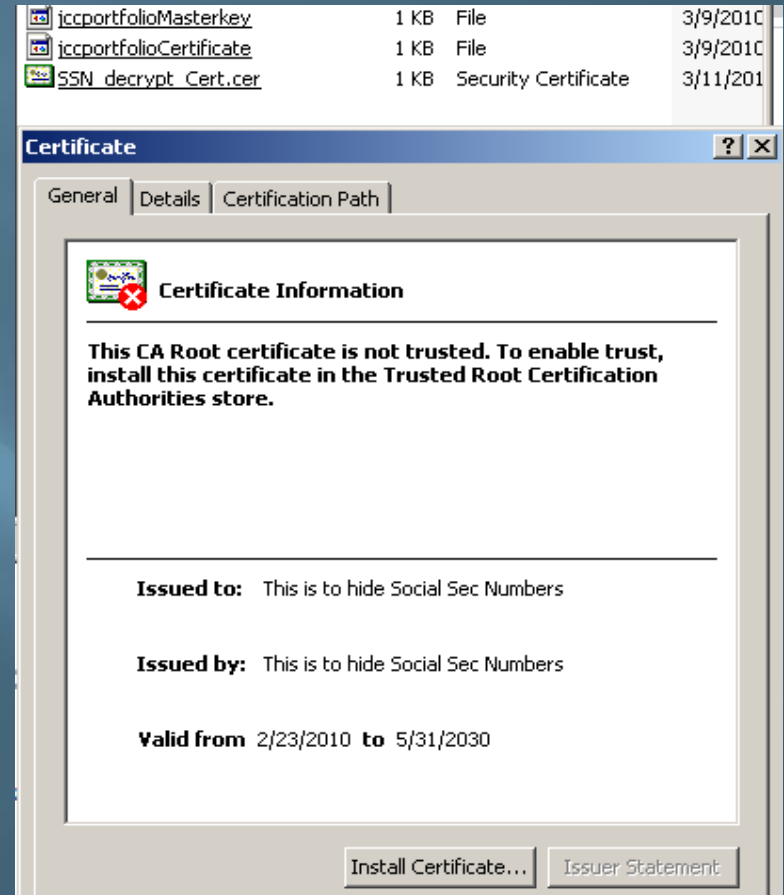
Encryption How-To 101

1. BACKUP MASTER KEY TO FILE = 'c:\sqldata\MasterKey'
ENCRYPTION BY PASSWORD = 'a good one!'

2. RESTORE MASTER KEY FROM FILE =
'c:\sqldata\MasterKey' DECRYPTION BY PASSWORD = 'a
good one!' ENCRYPTION BY PASSWORD = 'A real good
one!'

Encryption How-To 101

1. BACKUP CERTIFICATE SSN_decrypt_Cert TO FILE =
'c:\certs\SSN_decrypt_Cert.cer'



2. CREATE CERTIFICATE SSN_decrypt_Cert FROM FILE =
'c:\certs\SSN_decrypt_Cert.cer'

Encryption How-To 101

1. Create Symmetric key `SSN_Sym_Key`
with `Key_source='Building a nation takes dedication'`,
`Identity_value = 'Delaware'`,
`Algorithm = Triple_Des`
Encryption BY CERTIFICATE `SSN_decrypt_Cert` ;
2. Symmetric Keys Cannot be backed up... or restored!
3. They can only be re-created!

Encryption How-To 101

DB Copy Demo

...

**And still see
data!**

Encryption How-To 101

Questions?

The slide deck will
be available at
SqlInsight.net

Encryption How-To 101