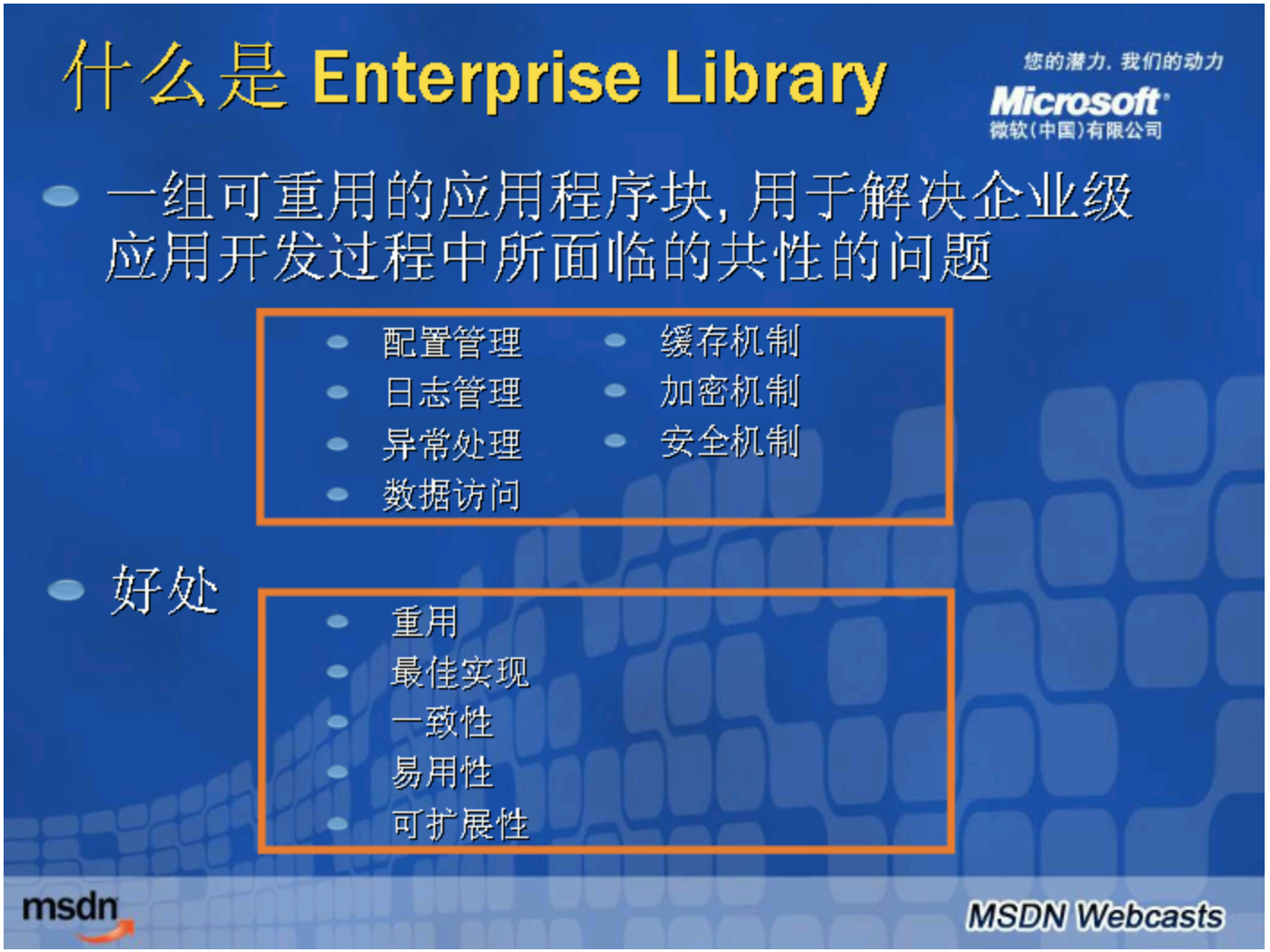
Enterprise Library Cryptography Application Block

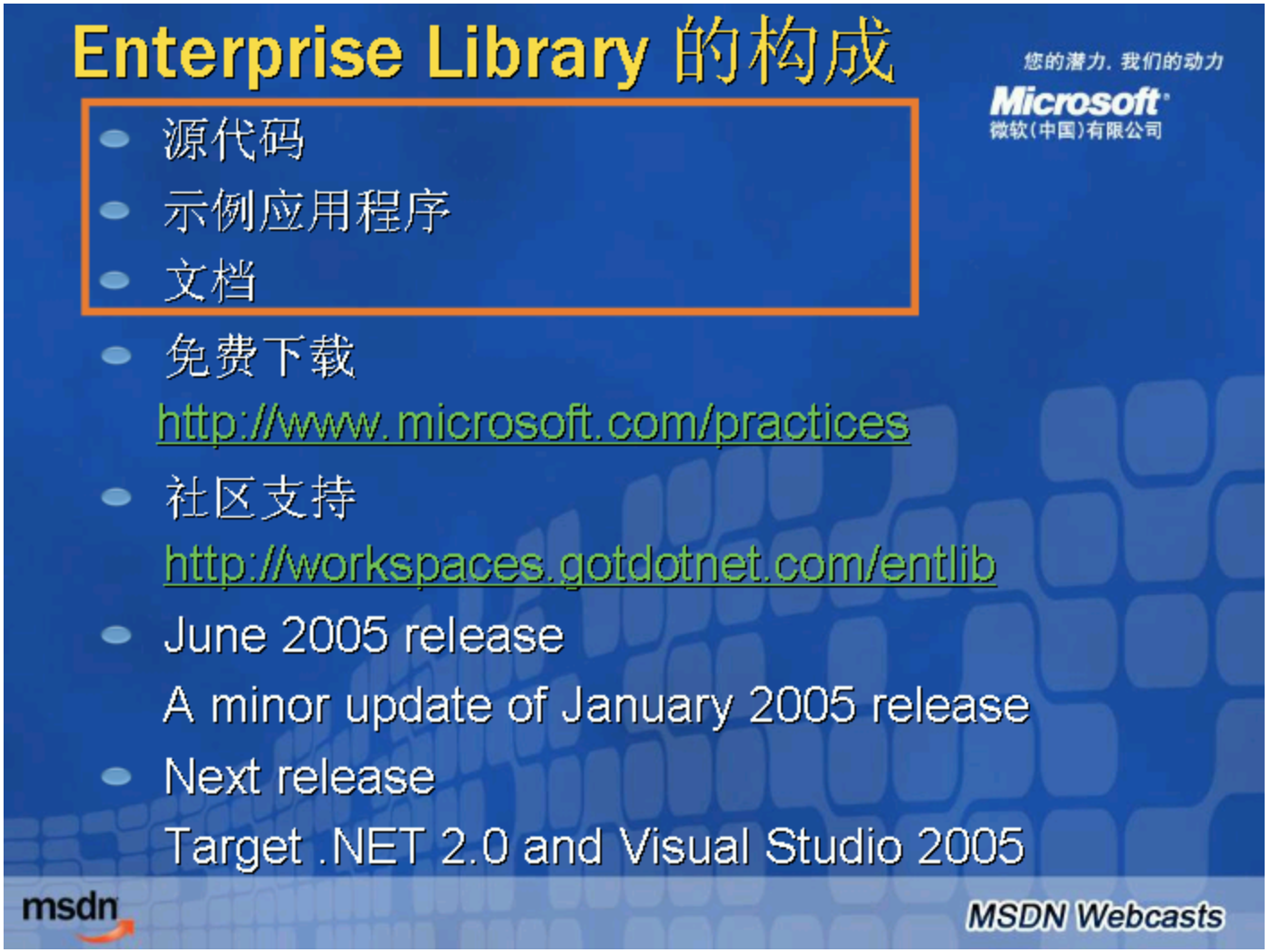

日程
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
Enterprise Library 概述
Crypto Application Block 概述
进一步的讨论
Q & A
msdn
MSDN Webcasts

Slide 2

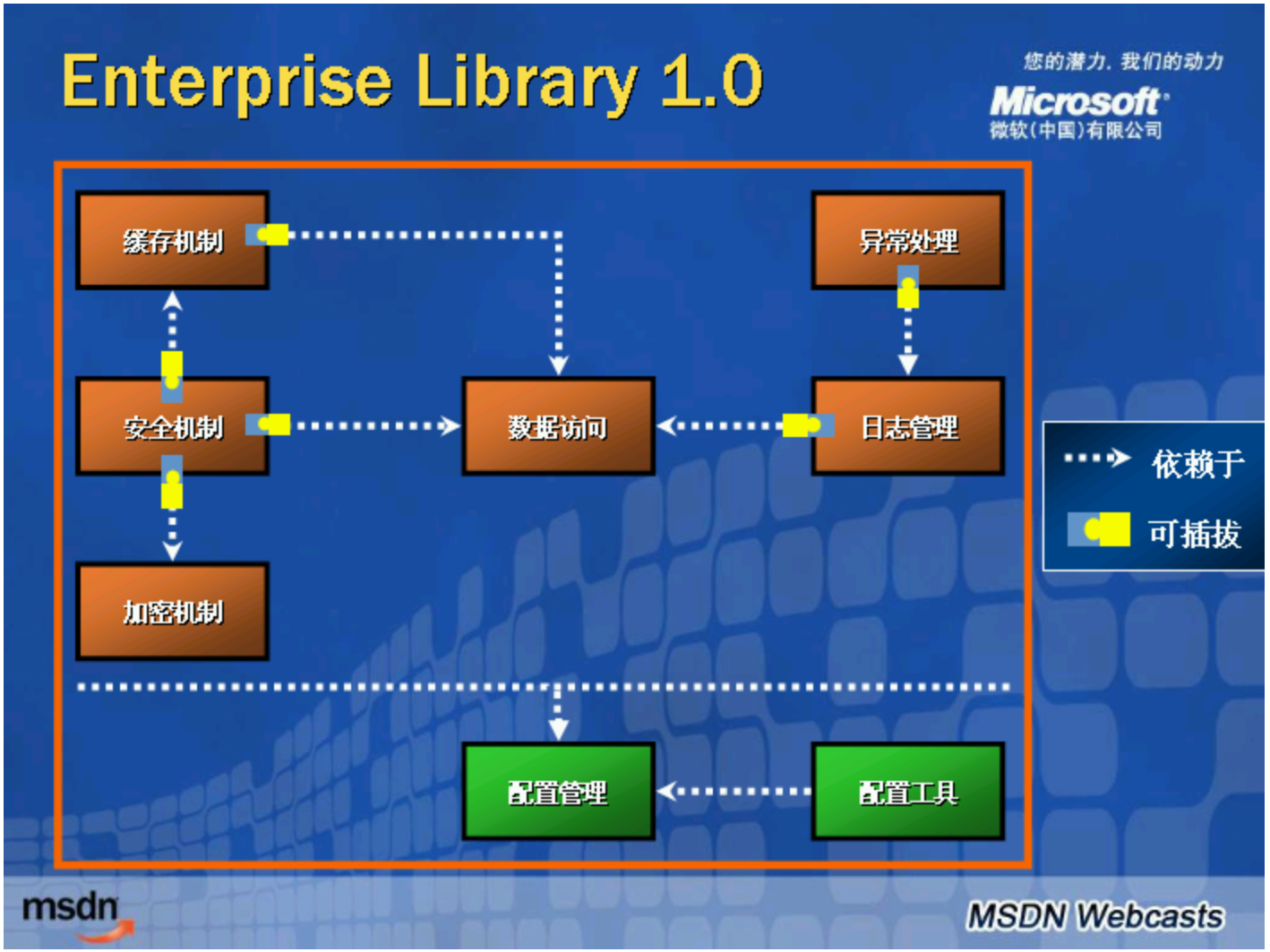
Enterprise Library



Enterprise Library

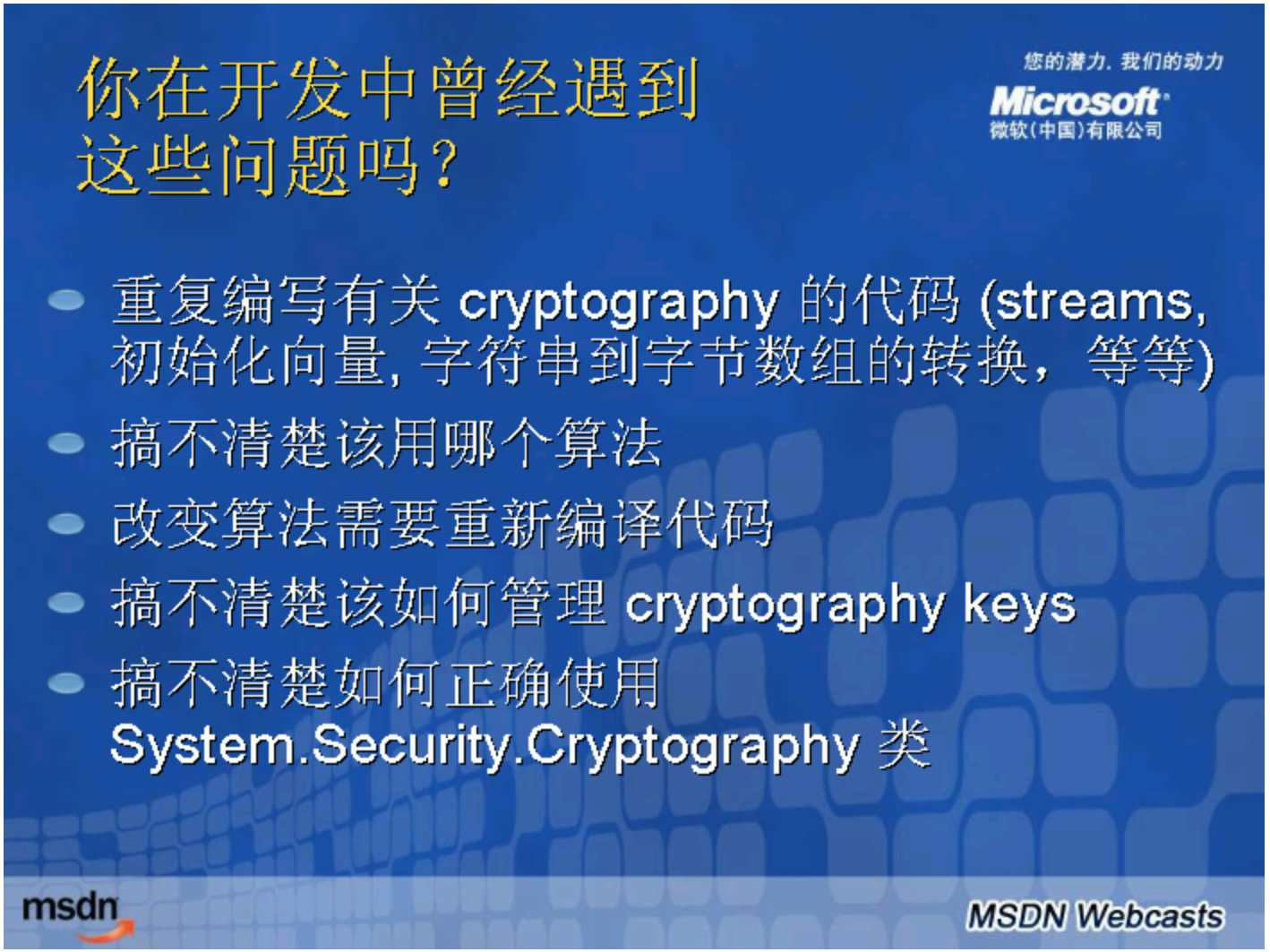


Enterprise Library



Enterprise Library 1.0

Crypto App Block


你在开发中曾经遇到
这些问题吗？
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
重复编写有关 cryptography 的代码 (streams, 初始化向量, 字符串到字节数组的转换，等等)
搞不清楚该用哪个算法
改变算法需要重新编译代码
搞不清楚该如何管理 cryptography keys
搞不清楚如何正确使用 System.Security.Cryptography 类
msdn
MSDN Webcasts

Slide 8

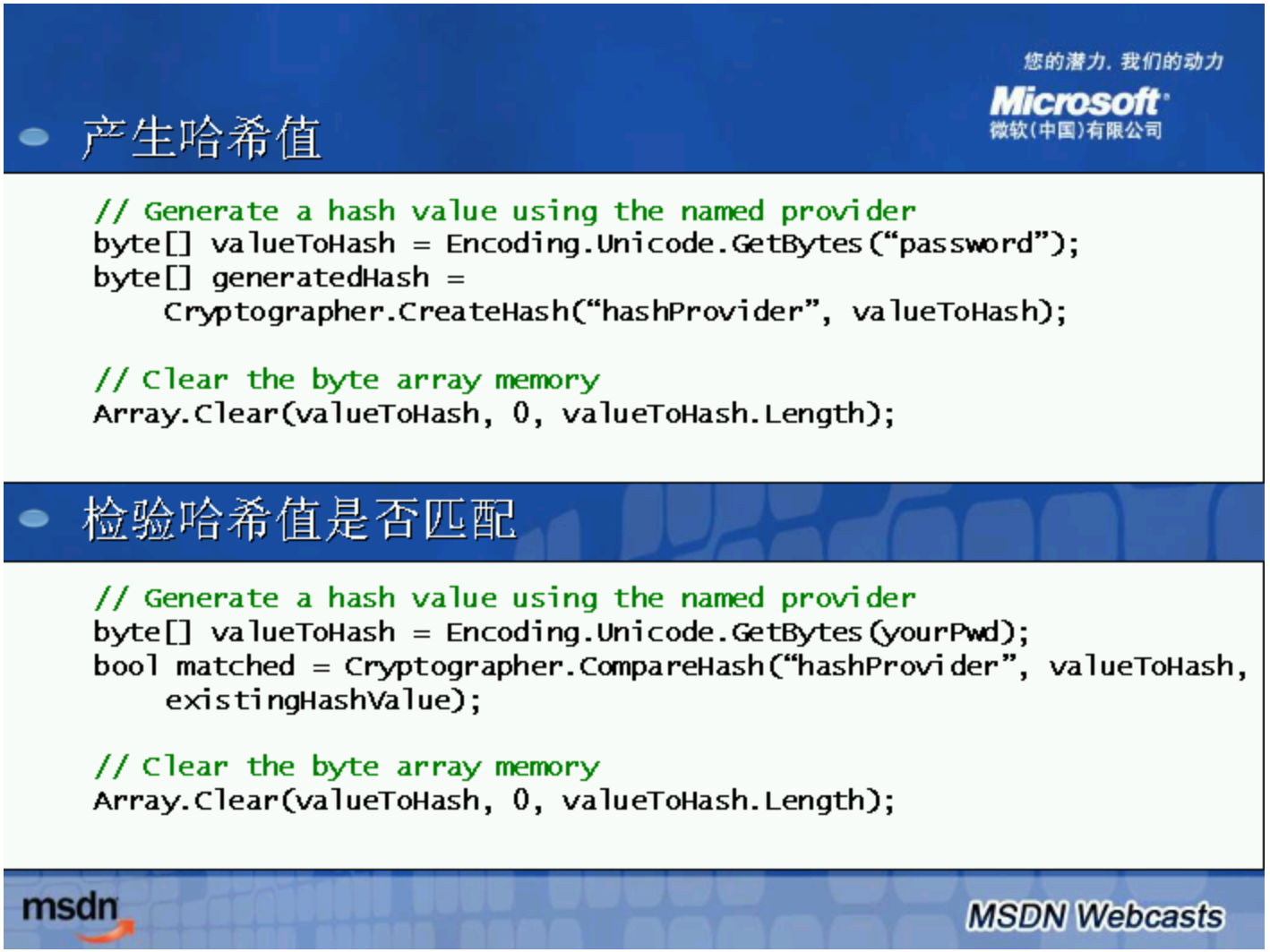
Cryptography

Cryptography Application Block

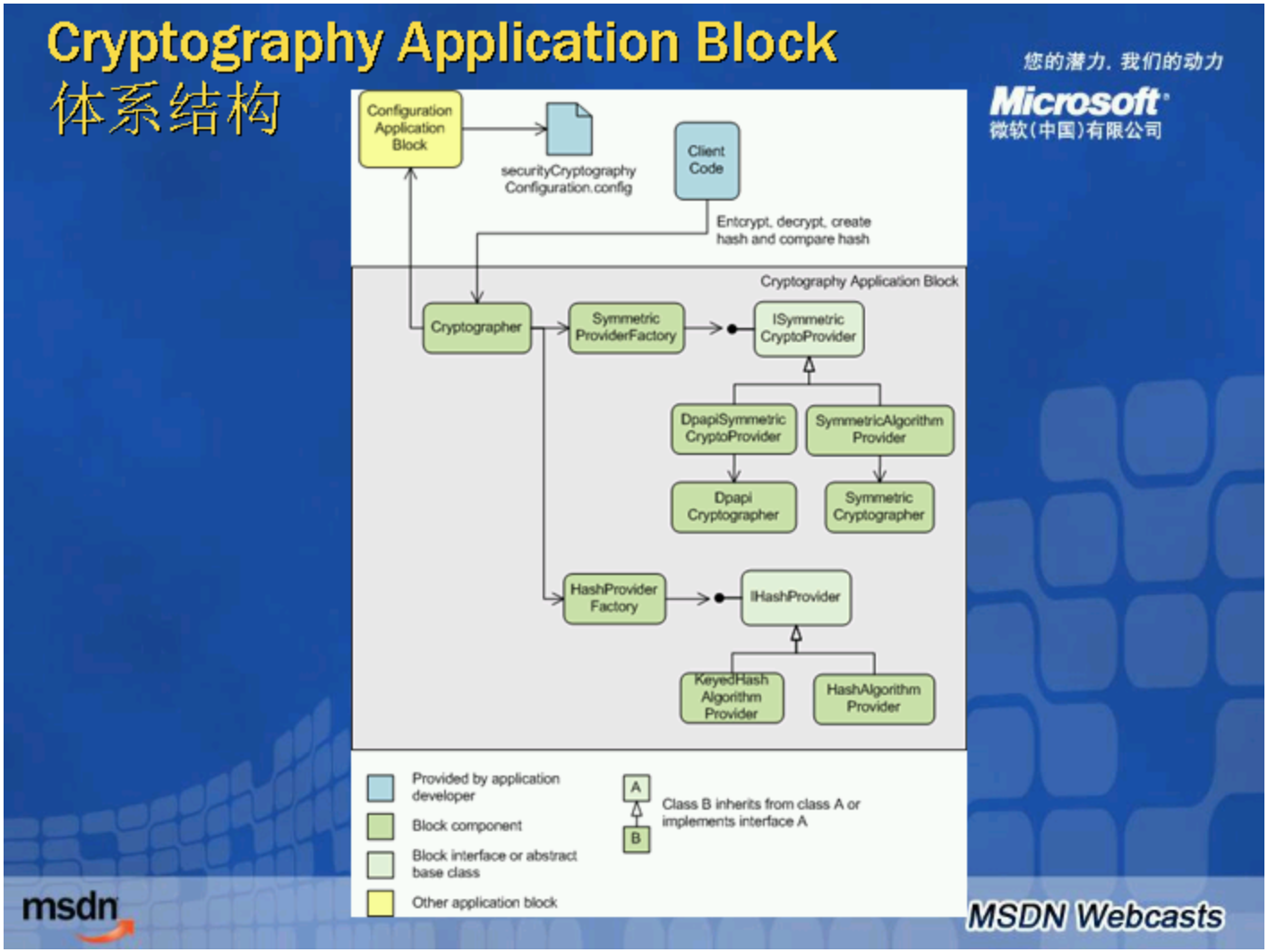

Step 1: 配置
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
使用配置工具为 Cryptography Application Block 创建配置
Enterprise Library Configuration*
File Action Help
Symmetric Providers
Application
Configuration Application Block
Encryption Settings
securityCryptographyConfiguratio
XML File Storage Provider
Xml Serializer Transformer
Cryptography Application Block
Hash Providers
hashprovider
Symmetric Providers
symprovider
General
AlgorithmType
System.Security.Cryptography.SHA1Managed, mscorlib,
Name
hashprovider
SaltEnabled
True
Name
Gets or sets the name of the node.
Configuration Errors
Name
Property
Description
Path
Ready
msdn
MSDN Webcasts

Step 1:

Step 2: 调用相应的 Cryptography

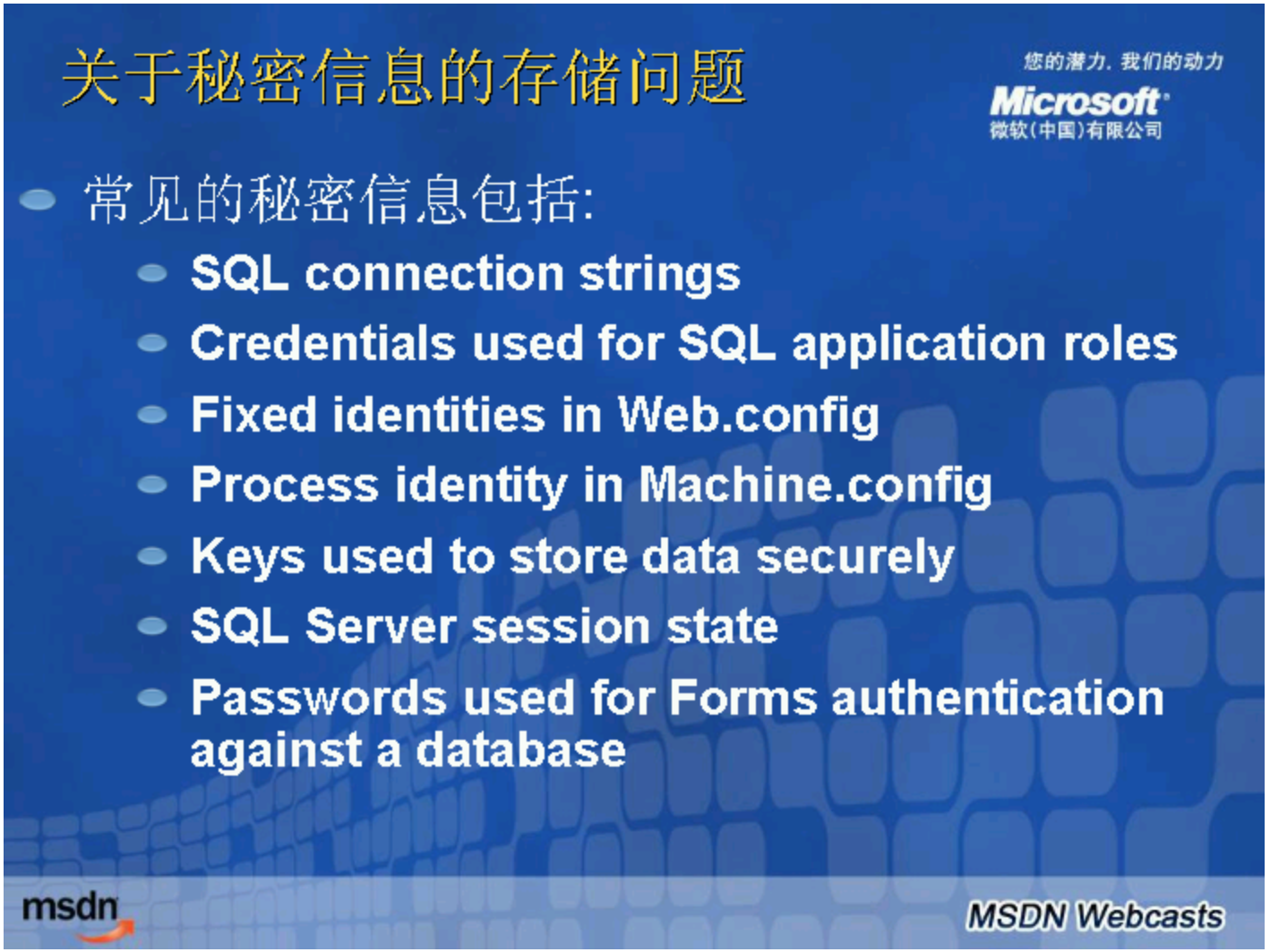

您的潜力，我们的动力
Microsoft
微软(中国)有限公司
产生哈希值
// Generate a hash value using the named provider
byte[] valueToHash = Encoding.Unicode.GetBytes("password");
byte[] generatedHash =
Cryptographer.CreateHash("hashProvider", valueToHash);
// Clear the byte array memory
Array.Clear(valueToHash, 0, valueToHash.Length);
检验哈希值是否匹配
// Generate a hash value using the named provider
byte[] valueToHash = Encoding.Unicode.GetBytes(yourPwd);
bool matched = Cryptographer.CompareHash("hashProvider", valueToHash,
existingHashValue);
// Clear the byte array memory
Array.Clear(valueToHash, 0, valueToHash.Length);
msdn
MSDN Webcasts

Slide 13



Cryptography Application Block

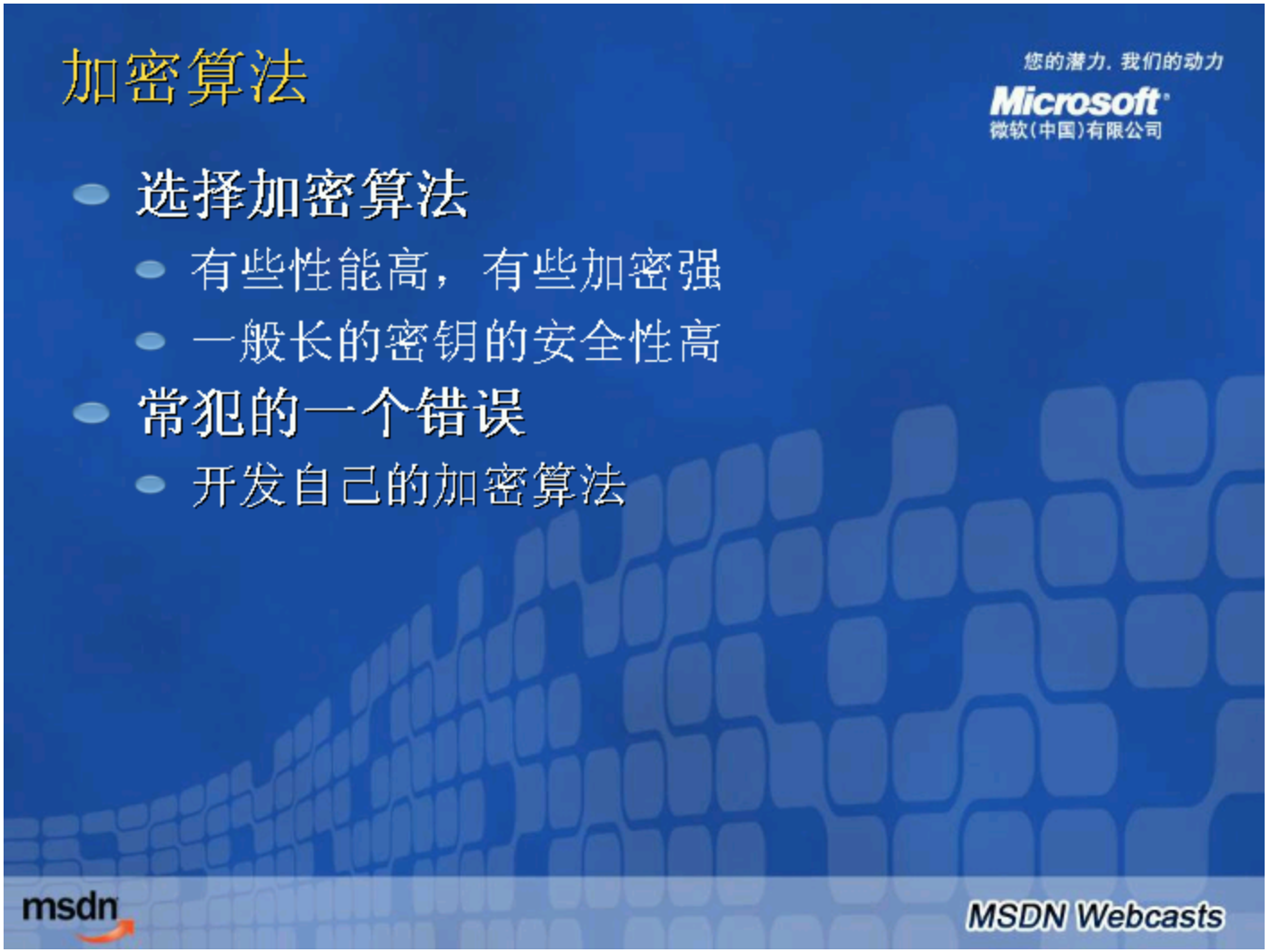
Slide 15


关于秘密信息的存储问题
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
常见的秘密信息包括:
SQL connection strings
Credentials used for SQL application roles
Fixed identities in Web.config
Process identity in Machine.config
Keys used to store data securely
SQL Server session state
Passwords used for Forms authentication against a database
msdn
MSDN Webcasts

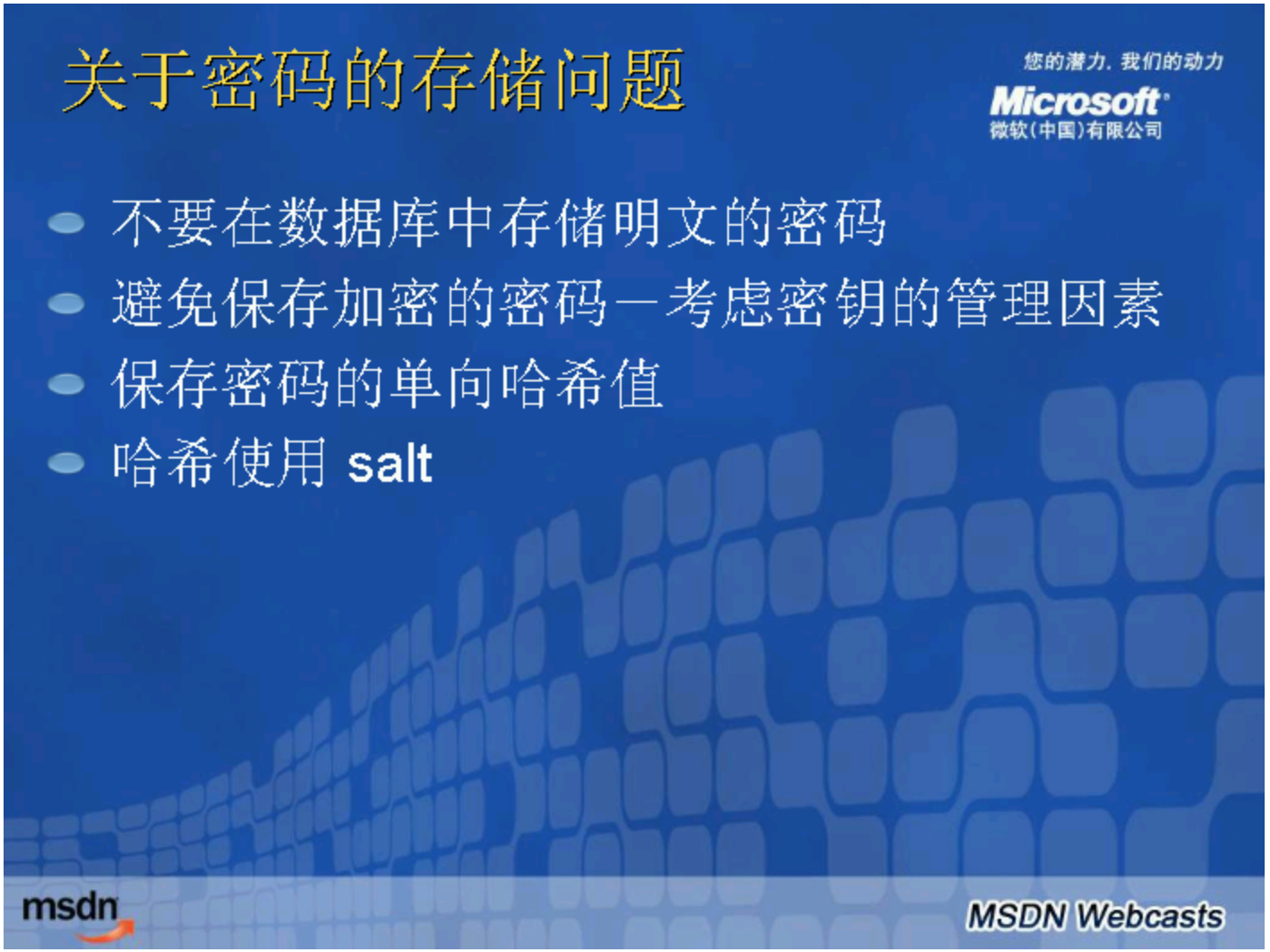
Slide 16


秘密信息存储的各种方案
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
采用 Windows 平台提供的方案
.NET cryptography classes
Data Protection API (DPAPI)
CAPICOM
Crypto API
或者采用Cryptography Application Block
更简单方便
最佳实践
msdn
MSDN Webcasts

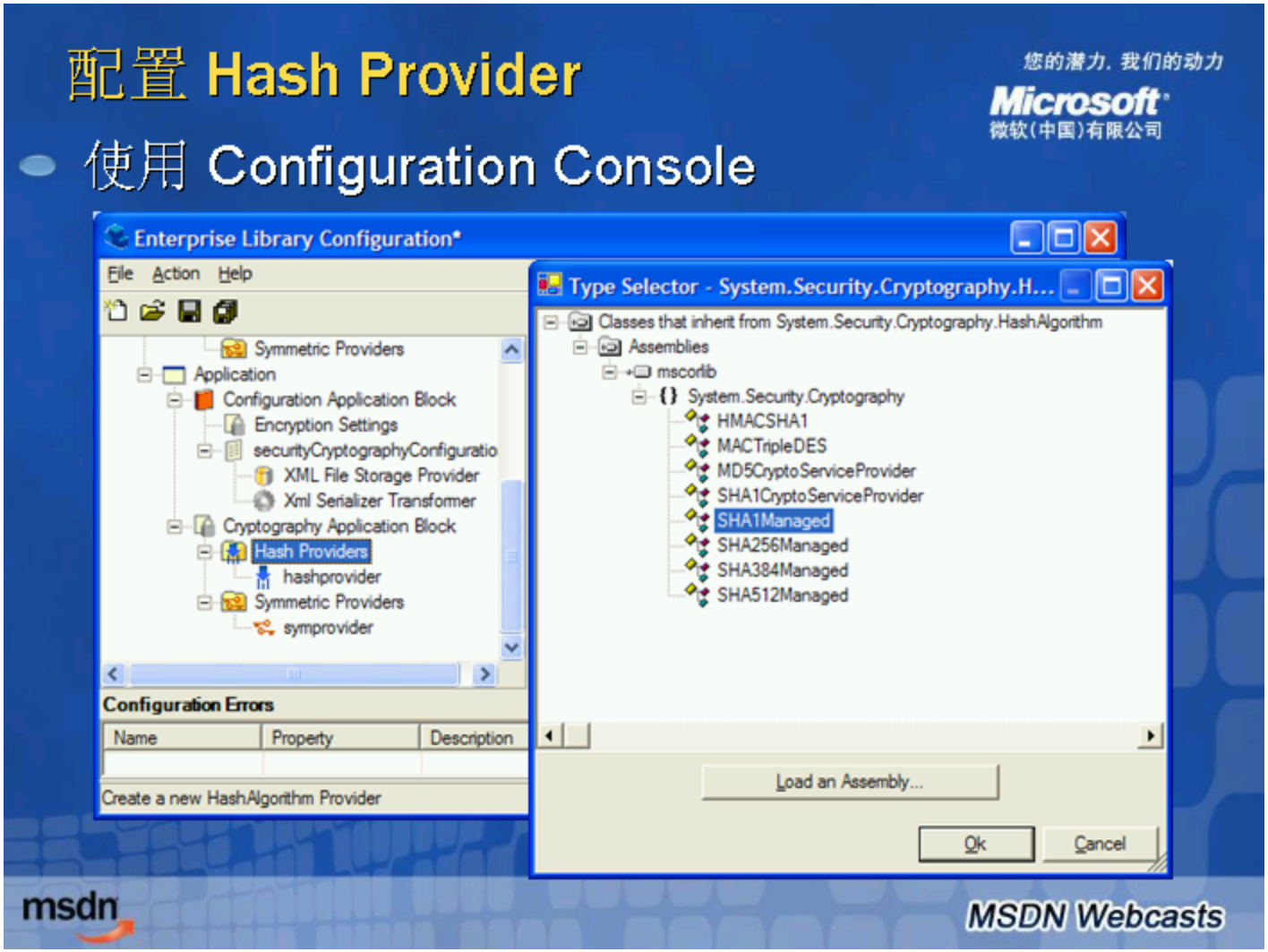
Slide 17


加密算法
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
选择加密算法
有些性能高，有些加密强
一般长的密钥的安全性高
常犯的一个错误
开发自己的加密算法
msdn
MSDN Webcasts

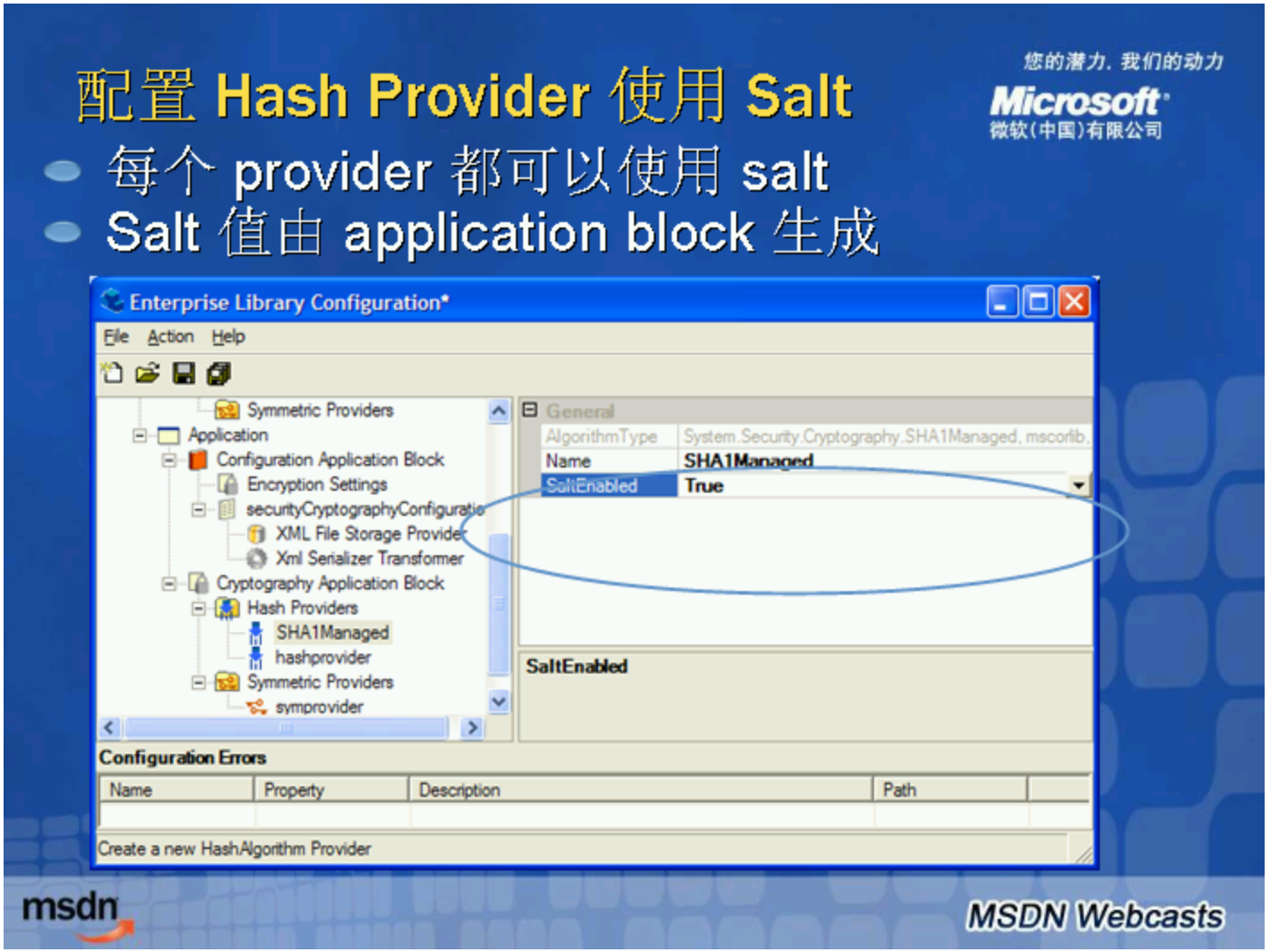
Slide 18


关于密码的存储问题
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
不要在数据库中存储明文的密码
避免保存加密的密码—考虑密钥的管理因素
保存密码的单向哈希值
哈希使用 salt
msdn
MSDN Webcasts

Slide 19



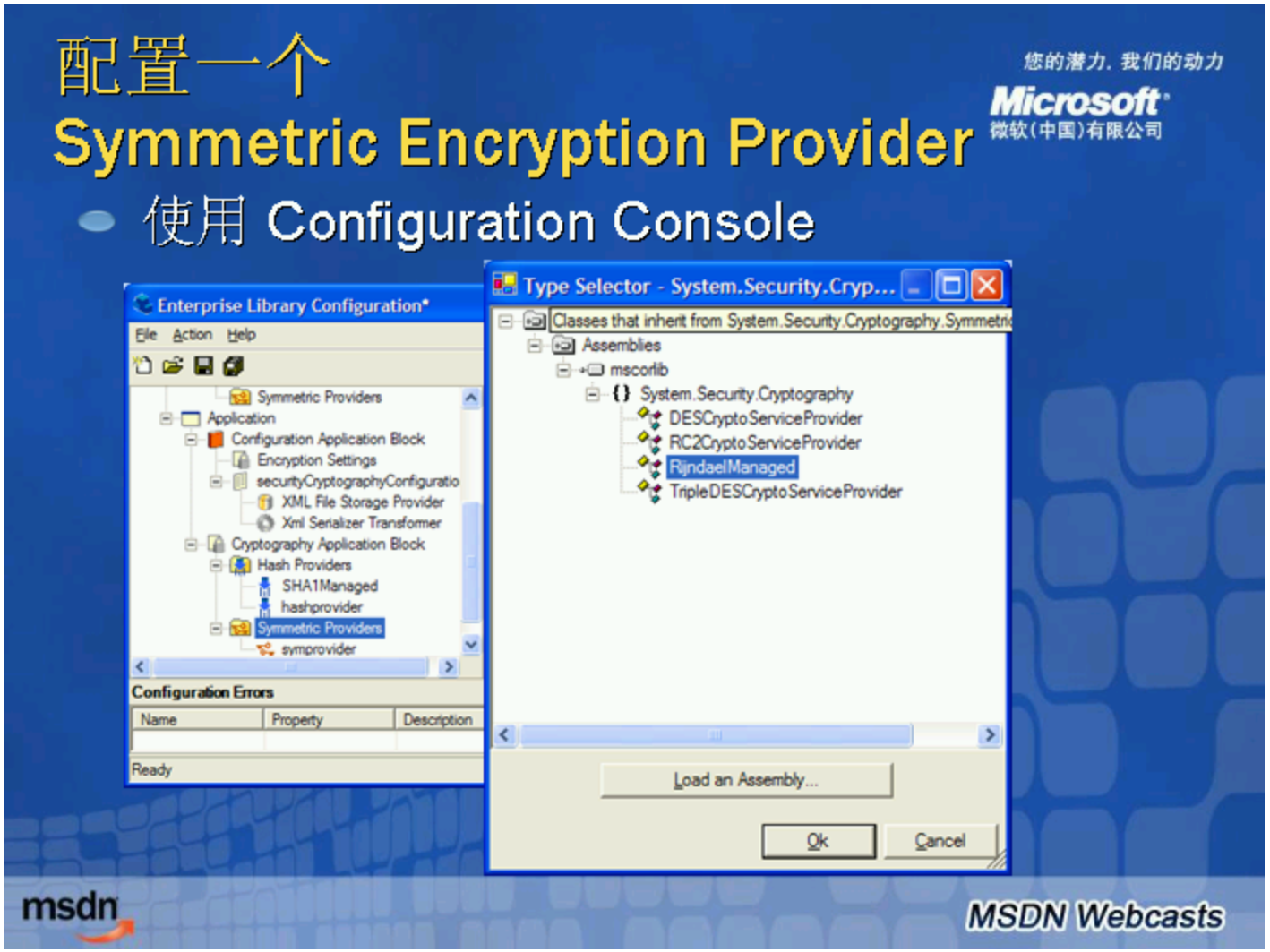
Hash Provider



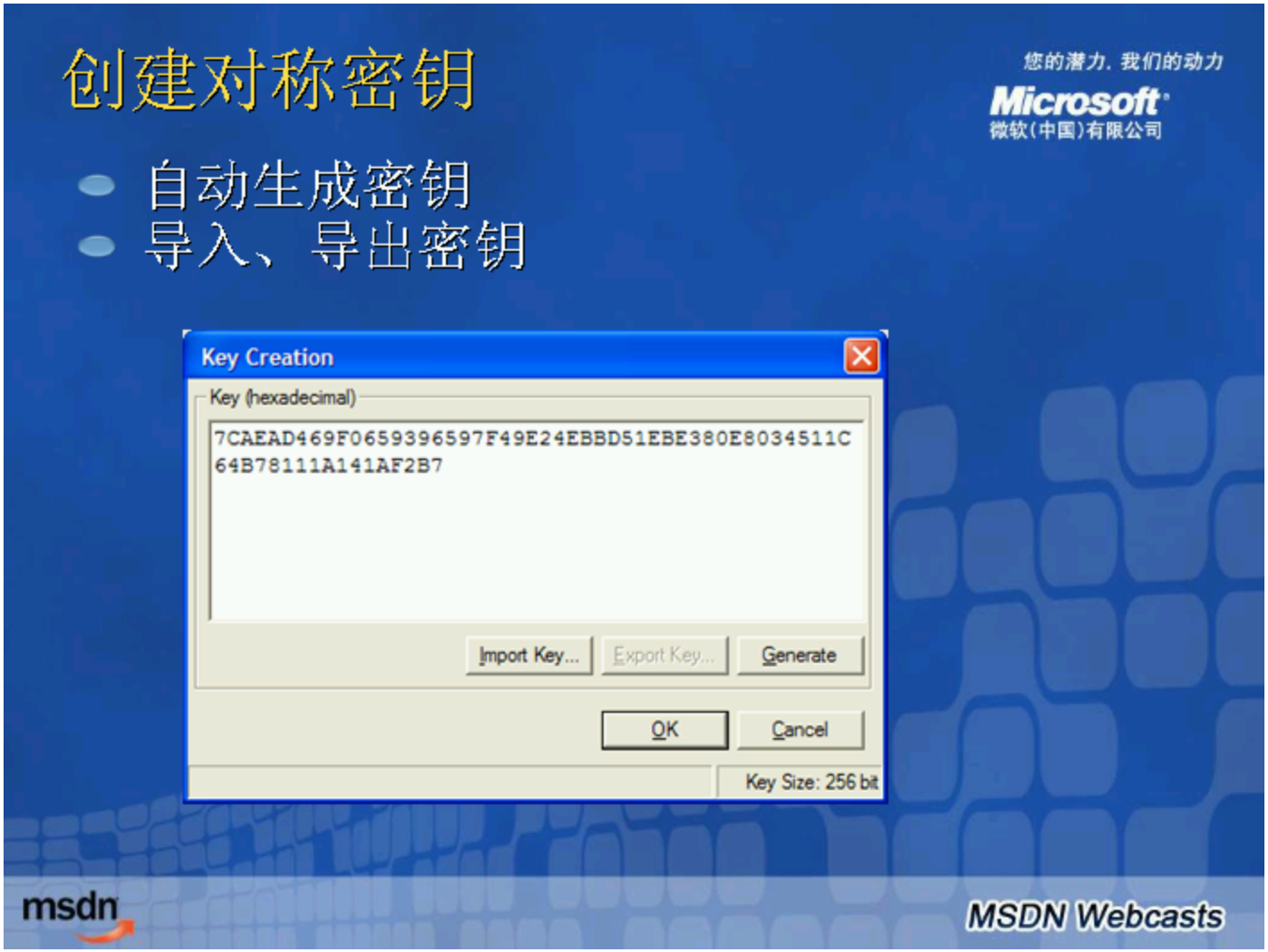
Hash Provider 使用 Salt


有关 Salt 的更多信息
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
salt 长度缺省为 16 字节 (providers can override)
采用 RNGCryptoServiceProvider (not Random) 降低了重复 salt 值的可能性
Salt 与需哈希的值组合，然后产生哈希
CreateHash() 返回 Salt 和 hash 值
CompareHash() 提取 salt 并用它来计算哈希值
别担心: application block 帮你做了所有这些!
msdn
MSDN Webcasts

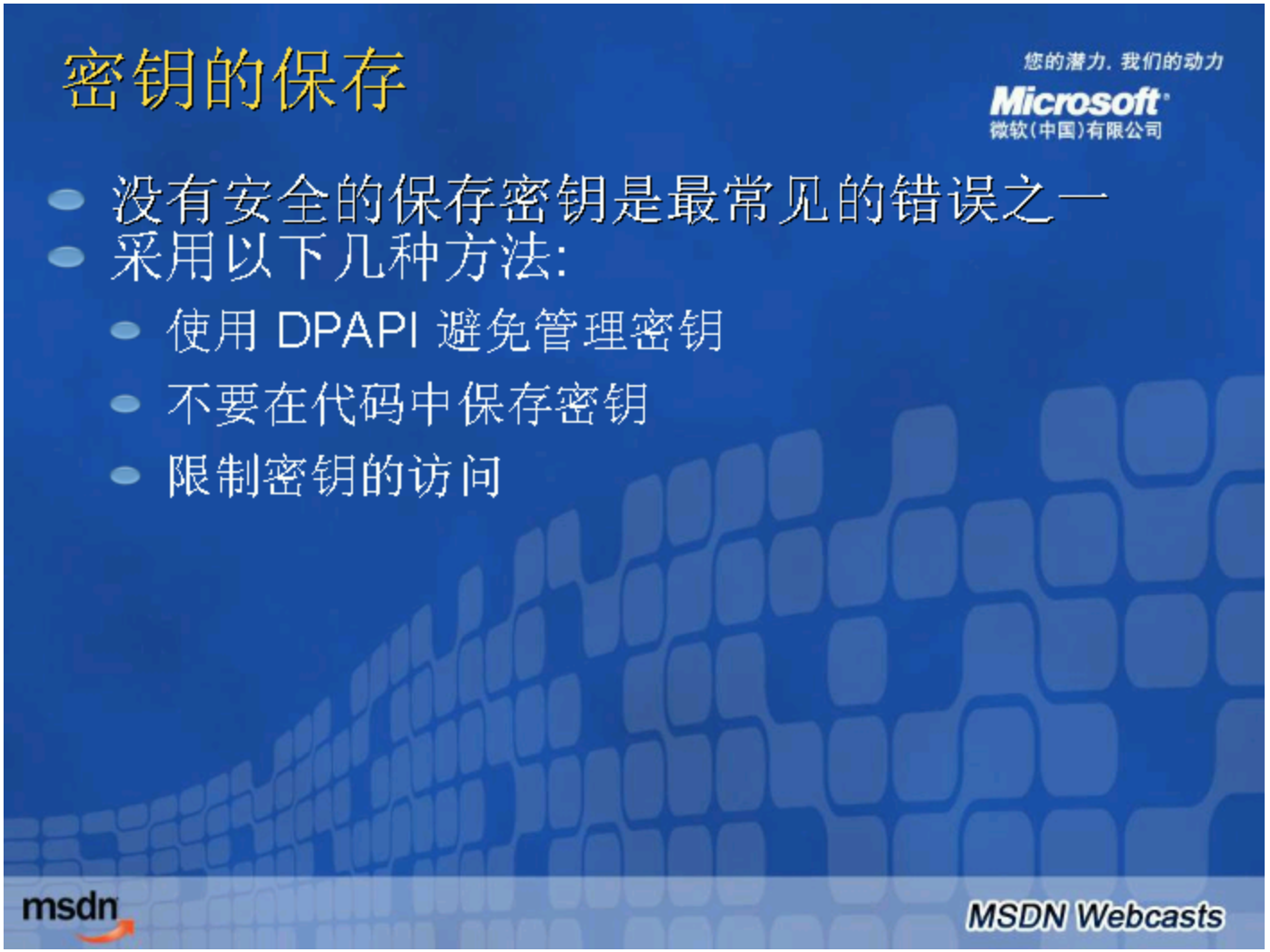
Salt



Symmetric Encryption Provider


创建对称密钥
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
自动生成密钥
导入、导出密钥
Key Creation
Key (hexadecimal)
7CAEAD469F0659396597F49E24EBBD51EBE380E8034511C
64B78111A141AF2B7
Import Key...
Export Key...
Generate
OK
Cancel
Key Size: 256 bit
msdn
MSDN Webcasts

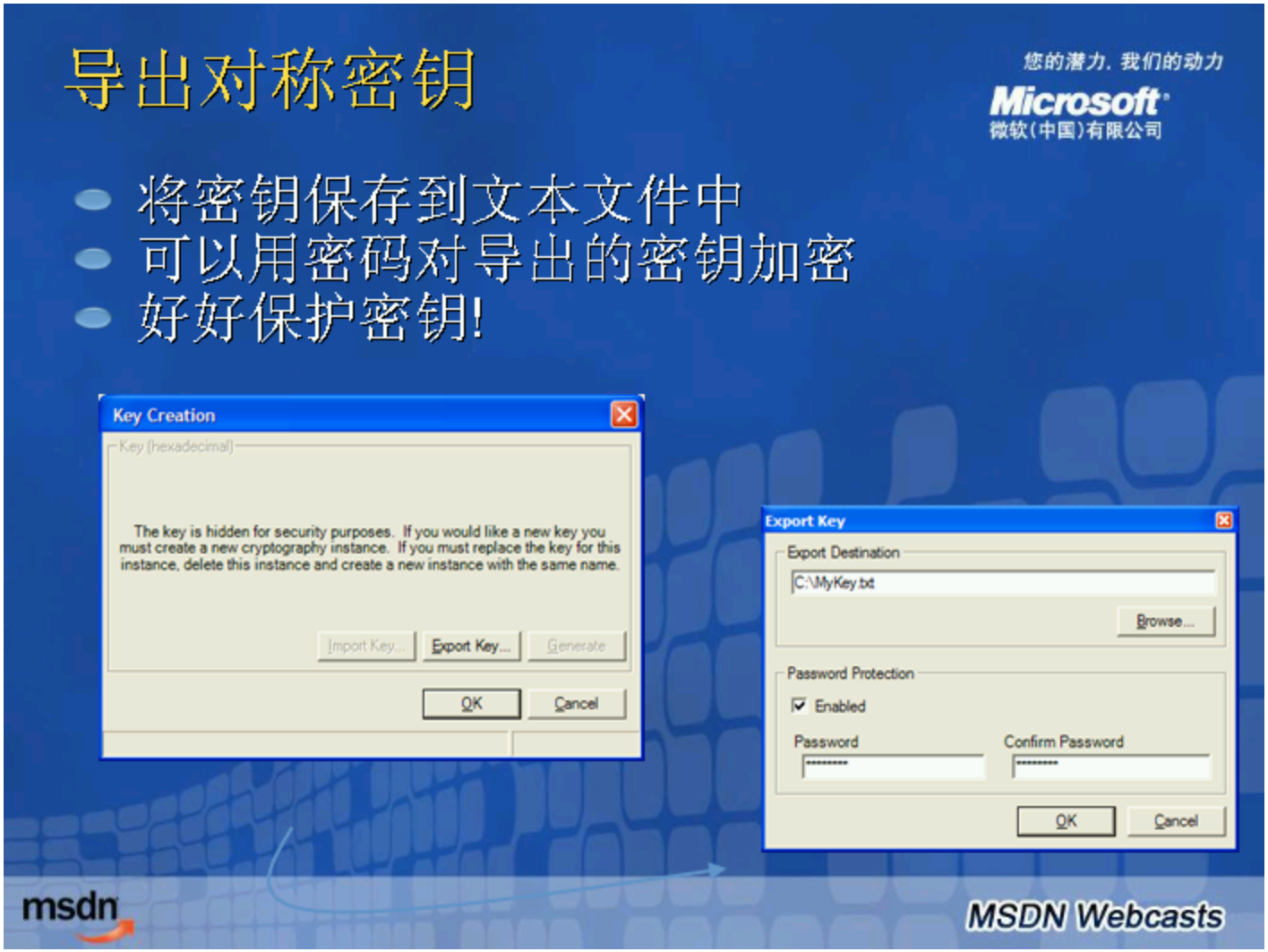
Slide 24


密钥的保存
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
没有安全的保存密钥是最常见的错误之一
采用以下几种方法:
使用 DPAPI 避免管理密钥
不要在代码中保存密钥
限制密钥的访问
msdn
MSDN Webcasts

Slide 25


对称密钥的管理
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
密钥以 Base 64 encoded string 的形式保存在 securityCryptographyConfiguration.config 配置文件中
如何保护配置文件
文件系统 ACL
对文件系统加密 (EFS)
使用 Configuration Console 对配置文件进行加密 (DPAPI)
msdn
MSDN Webcasts

Slide 26

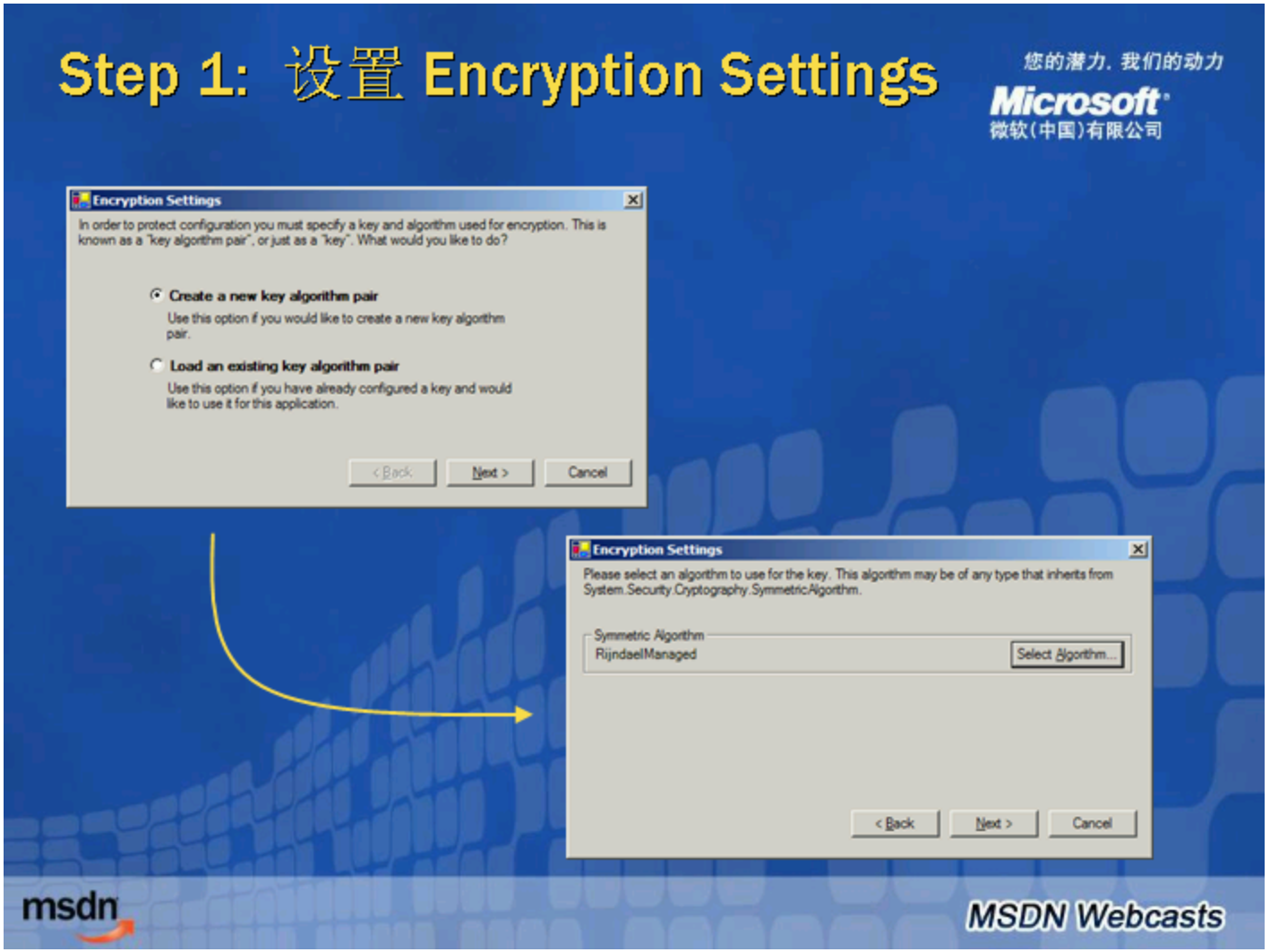

导出对称密钥
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
将密钥保存到文本文件中
可以用密码对导出的密钥加密
好好保护密钥!
Key Creation
Key (hexadecimal)
The key is hidden for security purposes. If you would like a new key you must create a new cryptography instance. If you must replace the key for this instance, delete this instance and create a new instance with the same name.
Import Key...
Export Key...
Generate
OK
Cancel
Export Key
Export Destination
C:\MyKey.txt
Browse...
Password Protection
Enabled
Password
Confirm Password
OK
Cancel
msdn
MSDN Webcasts

Slide 27

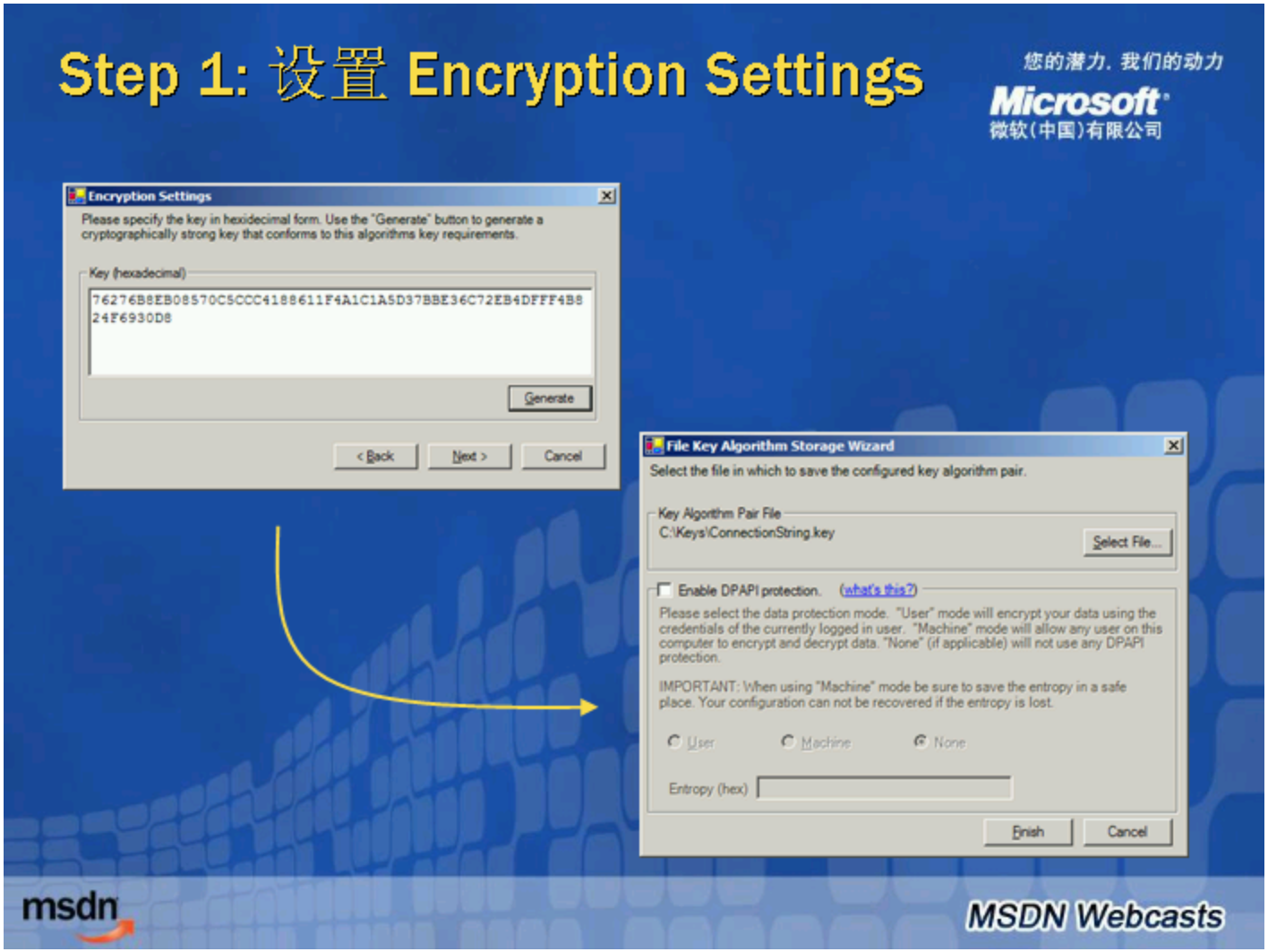
DPAPI Provider


数据库连接字符串的安全
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
加密配置项决定应用程序块的配置如何被加密
Enterprise Library Configuration*
File Action Help
Enterprise Library Configuration
Application
Configuration Application Block
dataConfiguration
XML File Storage Provider
Xml Serializer Transformer
Encryption Settings
File Key Algorithm Storage Pro
Data Access Application Block
Connection Strings
LocalQuickStart
database
Integrated Security
server
Database Instances
DataAccessQuickStart
General
DpapiSettings
File
C:\Keys\ConnectionString.key
Name
File Key Algorithm Storage Provider
TypeName
Microsoft.Practices.EnterpriseLibrary.Configuration.Protection.FileKe
Name
Gets or sets the name of the node.
Configuration Errors
Name
Property
Description
Path
Ready
msdn
MSDN Webcasts

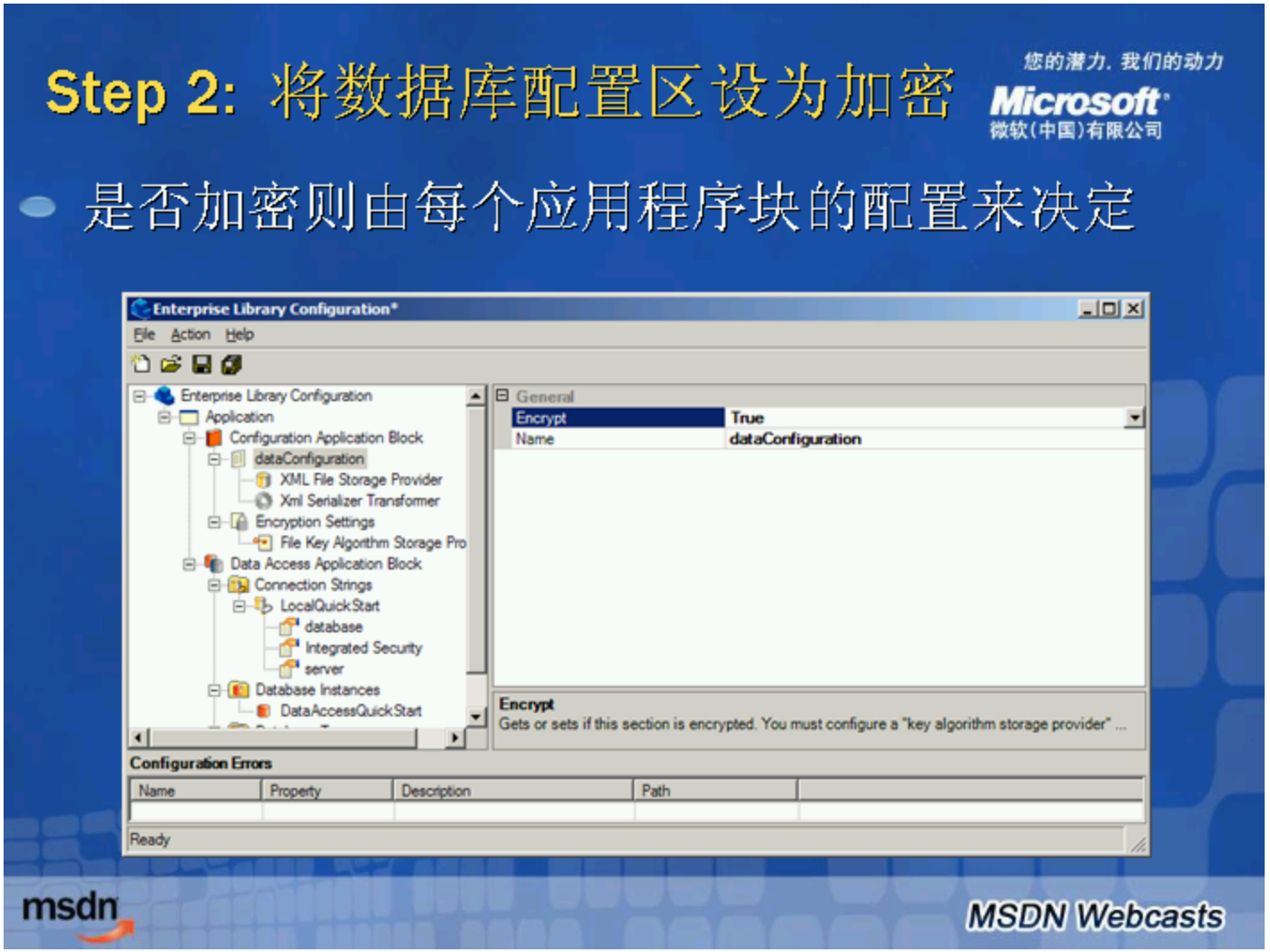
Slide 29



Step 1: 设置 Encryption Settings



Step 1: 设置 Encryption Settings


Step 2: 将数据库配置区设为加密
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
是否加密则由每个应用程序块的配置来决定
Enterprise Library Configuration*
File Action Help
Enterprise Library Configuration
Application
Configuration Application Block
dataConfiguration
XML File Storage Provider
Xml Serializer Transformer
Encryption Settings
File Key Algorithm Storage Pro
Data Access Application Block
Connection Strings
LocalQuickStart
database
Integrated Security
server
Database Instances
DataAccessQuickStart
General
Encrypt
True
Name
dataConfiguration
Encrypt
Gets or sets if this section is encrypted. You must configure a "key algorithm storage provider" ...
Configuration Errors
Name
Property
Description
Path
Ready
msdn
MSDN Webcasts

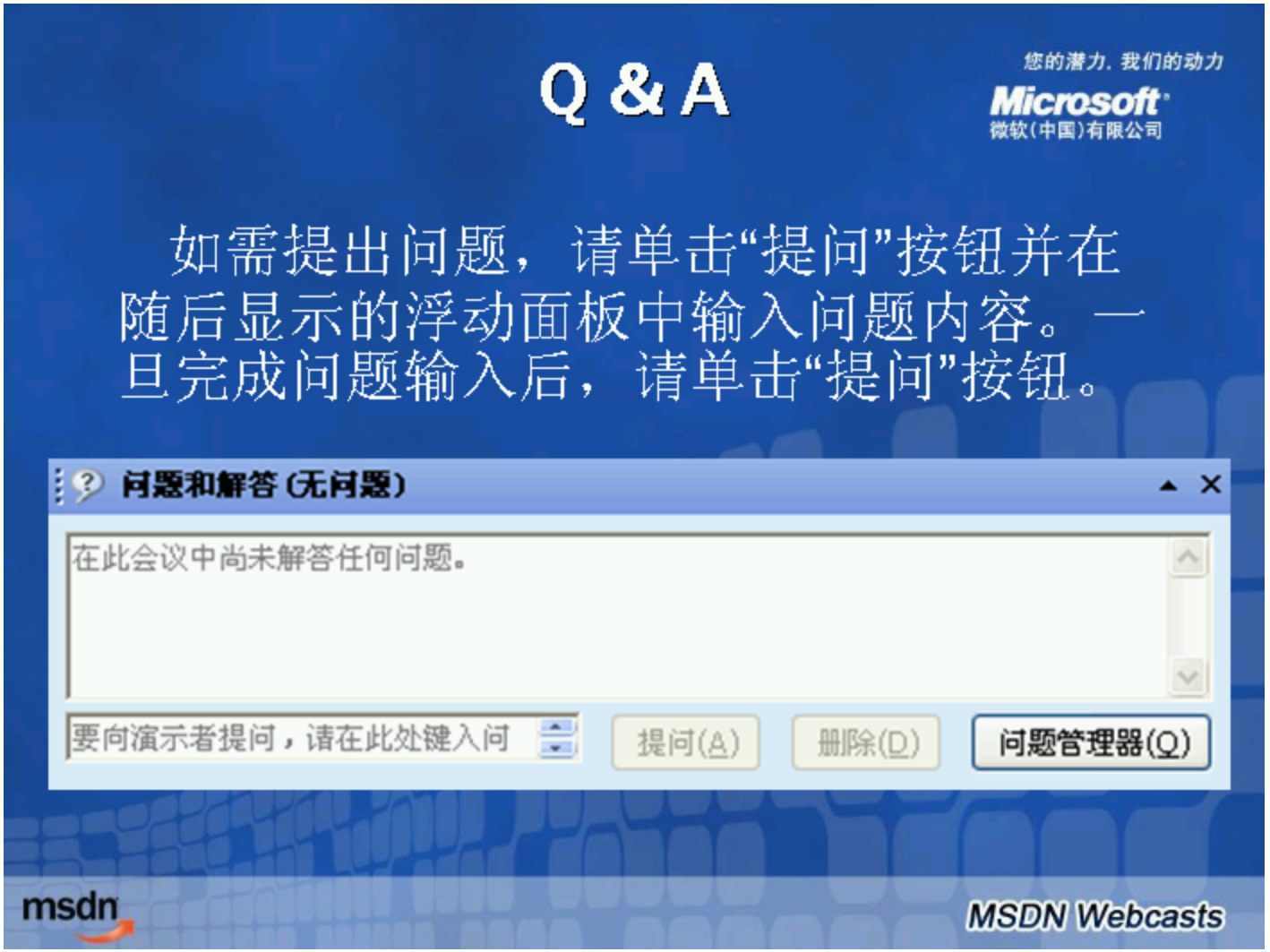
Step 2:


更多资源
您的潜力，我们的动力
Microsoft
微软(中国)有限公司
Improving Web Application Security
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp
Building Secure ASP.NET Applications
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/secnetlpMSDN.asp
Enterprise Library 社区
http://workspaces.gotdotnet.com/entlib
msdn
MSDN Webcasts

Slide 33


您的潜力，我们的动力
Microsoft
微软(中国)有限公司
Microsoft®
msdn
MSDN Webcasts

Slide 34



Ask a Questions