

GlobalTcert.com

GLOBALTCERT.COM
Your gateway to success



Demo
STUDY GUIDE

© Copy Right 1998-2005 GlobalTcert LLC. All Rights Reserved.

Missing Answers & Explanations will be provided in the next update.

QUESTION 1

You are an application developer for GlobalitcerT .com. You develop library assemblies that are called by your main applications. These library assemblies access confidential data in the applications. To ensure that this data is not accessed in an unauthorized and unsafe manner, users must not be allowed to call the library assemblies from their own applications. You apply a strong name to all assemblies to support versioning.

You need to prevent users from writing managed applications that make calls to your library assemblies. You need to achieve this goal while minimizing the impact on response times for applications.

What should you do?

- A. Use the internal access modifier to declare all classes and structures in each library.
- B. Use the protected internal access modifier to declare all classes and structures in each library.
- C. Add the following attribute to each class and structure in each library assembly:
<StrongNameIdentityPermission(SecurityAction.Demand, PublicKey:="002400..bda4")>
- D. Add the following attribute to each class and structure in each library assembly:
<StrongNameIdentityPermission(SecurityAction.LinkDemand, PublicKey:="002400..bda4")>

Answer:

QUESTION 2

You are an application developer for GlobalitcerT .com. You are developing an application that can be extended by using custom components. The application uses reflection to dynamically load and invoke these custom components. In some cases, custom components will originate from a source that is not fully trusted, such as the Internet.

You need to programmatically restrict the code access security policy under which custom components run so that custom components do not run with an elevated permission grant.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

- A. Create a new application domain and set the security policy level. Run custom components in this application domain.
- B. Use permission class operations to modify the security policy.
- C. Implement custom permission classes to protect custom component resources.
- D. Programmatically modify the machine-level security policy file after loading a custom component.

Answer:

QUESTION 3

You are an application developer for GlobalitcerT .com. You are developing an application that salespeople in GlobalitcerT will use to process customer orders. This application includes a library assembly that implements a serviced component named Order. This serviced component adds roles named

GlobalitcerT Manager and SalesPerson to the COM+ application that hosts it.

To promote customer satisfaction, salespeople are allowed to apply discounts to orders if the order was erroneously delayed. However, only GlobalitcerT Managers are allowed to apply discounts greater than 10 percent. The application includes the following method to apply the discount.

Public Function Apply Discount (ByVal discountPct As Integer) As Boolean

This method will return a value of False when the current user is not a member of the GlobalitcerT Manager role and the value of the discountPct parameter exceeds the maximum that other salespeople are allowed to apply.

You need to add the code that will verify the role membership requirement when the value of discountPct is greater than 10.

Which code segment should you use?

- A. If discountPct > 10 And
Thread.CurrentPrincipal.IsInRole(" GlobalitcerT Manager") = False Then
Return False
End If
- B. If discountPct > 10 Then
Dim p As PrincipalPermission = New PrincipalPermission(Nothing,
" GlobalitcerT Manager")
If Security GlobalitcerT Manager.IsGranted(p) = False Then
Return False
End If
End if
- C. If discountPct > 10 Then
Dim p As PrincipalPermission = New PrincipalPermission(Nothing,
" GlobalitcerT
Manager") Try
p.Demand()
Catch e As SecurityException
Return False
End Try
End If
- D. If discountPct > 10 And
SecurityCallContext.CurrentCall.IsCallerInRole(" GlobalitcerT
Manager") _
= False Then
Return False
End if

Answer:

QUESTION 4

You are an application developer for GlobalitcerT .com. You develop an application that receives data from a remote component.

You are developing a method to detect any corrupted incoming data and log information to a file for analysis. You plan to use two functions. A function named GlobalitcerT Data will be called by the remote component. The second function will be called by the local application to verify that the data was not corrupted during transmission.

You need to ensure that corrupted data can be identified.
Which code segment should you use?

```
A. Public Function GlobalitcerT Data(ByVal Data As Byte()) As  
Byte() Dim Ms As New MemoryStream  
Ms.Write(Data, 0, Data.Lenght)  
Ms.Write(Data, 0, Data.Lenght)  
Return Ms.ToArray()  
End Function
```

```
B. Public Function GlobalitcerT Data(ByVal Data As Byte()) As  
Byte() Dim Md5 As MD5 = New MD5CryptoServiceProvider  
Dim Ms As New MemoryStream  
Ms.Write(Md5.ComputeHash(Data), 0, Md5.HashSize)  
Ms.Write(Data, 0, Data.Lenght)  
Return Ms.ToArray()  
End Function
```

```
C. Public Function GlobalitcerT Data(ByVal Data As Byte()) As  
Byte() Dim Des As DES = New DESCryptoServiceProvider  
Dim Ms As New MemoryStream  
Ms.Write(Des.Key, 0, Des.Key.Length)  
Ms.Write(Des.IV, 0, Des.IV.Length)  
Dim Cs As New CryptoStream(Ms, Des.CreateEncryptor(),  
CryptoStreamMode.Write)  
Cs.Write(Data, 0, Data.Length)  
Cs.FlushFinalBlock()  
Return Ms.ToArray()  
End Function
```

```
D. Public Function GlobalitcerT Data (ByVal Data As Byte()) As  
Byte() Dim Ms As New MemoryStream  
Dim Sw As New StreamWriter(Ms, Encoding.UTF8=  
Sw.Write(Encoding.UTF8.GetString(Data))  
Return Ms.ToArray()
```

Answer:

QUESTION 5

You are an application developer for your company, which is named GlobalitcerT .com. You are developing an ASP.NET Web application that users in the accounting department will use to process payroll reports and view payroll reports. The application will use Integrated Windows authentication to authenticate all users.

Because payroll data is confidential only users in the accounting department will be granted access to the application. All employees in the accounting department belong to a specific Active Directory group. However, users in the IT department can add themselves to various Active Directory groups in order to troubleshoot resource access problems. These IT department users must not be granted access to the ASP.NET Web application.

The following rules can be used to distinguish between users in the accounting department and users in