3. Implement Azure security
└─ **3.2 Implement secure Azure solutions**
└─ **3.2.1 Secure app configuration data by using App Configuration or Azure Key Vault**

1. What is Azure App Configuration and when should it be used?
2. What is Azure Key Vault and when should it be used?
3. What types of secrets can be stored in Azure Key Vault?
4. How do you access secrets from Azure Key Vault in code using DefaultAzureCredential?
5. How do you integrate Azure Key Vault with App Service or Functions securely?
6. How do you use Azure App Configuration in .NET apps?
7. How do you enable Key Vault reference integration in Azure App Configuration?
8. How do you use managed identities to authenticate to Key Vault and App Configuration?
9. What are best practices for securing app settings and secrets?
10. How can you audit or monitor access to secrets in Azure Key Vault?

---

1. What is Azure App Configuration and when should it be used?
A centralized service for managing application settings and feature flags. Use it to decouple config from code across environments, especially in microservices or distributed apps.

---

2. What is Azure Key Vault and when should it be used?
A secure store for secrets, keys, and certificates. Use it for managing sensitive data (e.g., DB passwords, API keys) with RBAC and audit logging. Ideal for securing runtime secrets.

---

3. What types of secrets can be stored in Azure Key Vault?

- Secrets (e.g., passwords, connection strings)
- Keys (RSA, EC keys for encryption/signing)
- Certificates (incl. auto-renewing SSL certs)

---

4. How do you access secrets from Azure Key Vault in code using DefaultAzureCredential?
Use Azure SDK:

```
var client = new SecretClient(new Uri(kvUrl), new DefaultAzureCredential());
KeyVaultSecret secret = await client.GetSecretAsync("MySecret");
```

Requires proper RBAC role (e.g., Key Vault Secrets User) and managed identity.

---

5. How do you integrate Azure Key Vault with App Service or Functions securely?
Enable managed identity on the app, assign Key Vault Secrets User role, and reference secrets using:

```
@Microsoft.KeyVault(SecretUri=https://<vault-name>.vault.azure.net/secrets/<secret-name>/)
```

Used in app settings; no code change needed.

---

6. How do you use Azure App Configuration in .NET apps?
Install the package:
Microsoft.Extensions.Configuration.AzureAppConfiguration
Example usage:

```
builder.Configuration.AddAzureAppConfiguration(options =>
   options.Connect("<connection-string>")
        .Select("*"));
```

Use FeatureManagement for feature flags.

7. How do you enable Key Vault reference integration in Azure App Configuration?

In Azure App Configuration, add a key with a value using this format:

```
@Microsoft.KeyVault(SecretUri=https://<vault-name>.vault.azure.net/secrets/<secret-name>/)
```

Requires managed identity access to Key Vault and EnableKeyVault option in code.

8. How do you use managed identities to authenticate to Key Vault and App Configuration?

Enable system/user-assigned identity on the app. Assign roles:

- Key Vault: Key Vault Secrets User
- App Configuration: App Configuration Data Reader
  In code, use DefaultAzureCredential to authenticate.

9. What are best practices for securing app settings and secrets?

- Never store secrets in code or config files
- Use managed identities with least privilege
- Reference secrets from Key Vault via environment/config
- Enable Key Vault logging and soft-delete

10. How can you audit or monitor access to secrets in Azure Key Vault?

Enable diagnostic settings to stream logs to Log Analytics.

Track:

- Secret access (AuditEvent)
- Failed attempts
  Use Azure Monitor or Sentinel for alerting and analytics.