

Protecting Production Secrets with a Key Vault



Matthew Tester

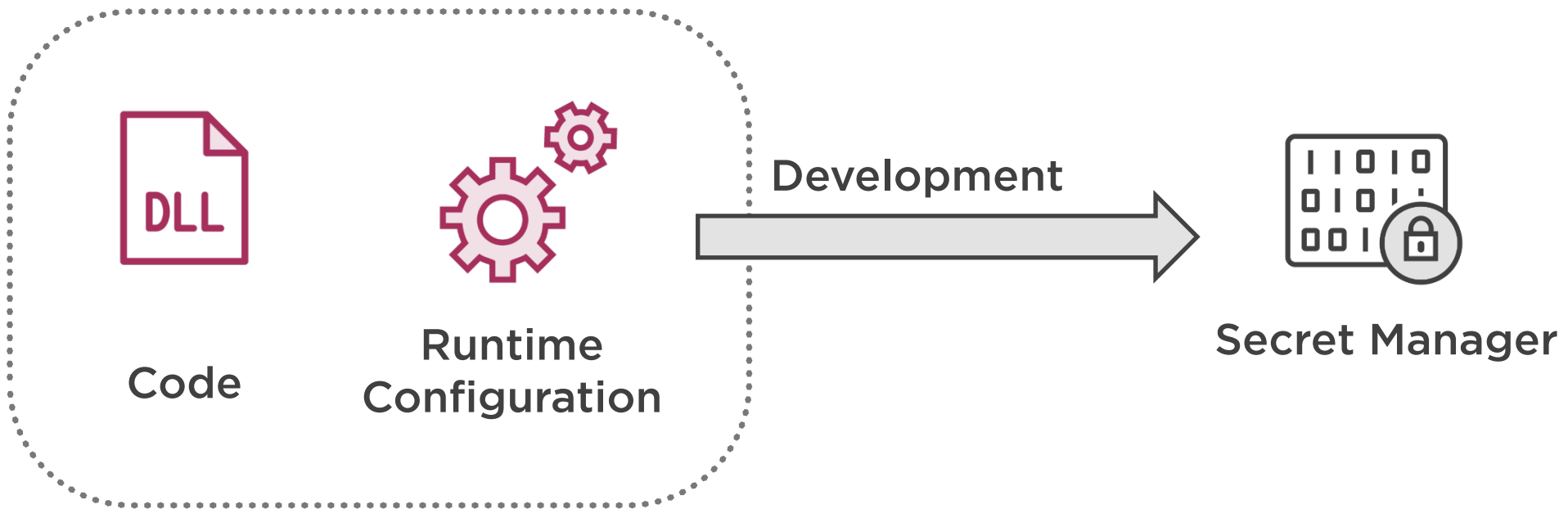
TECHNOLOGY CONSULTANT

@matttester pureblue.co.nz



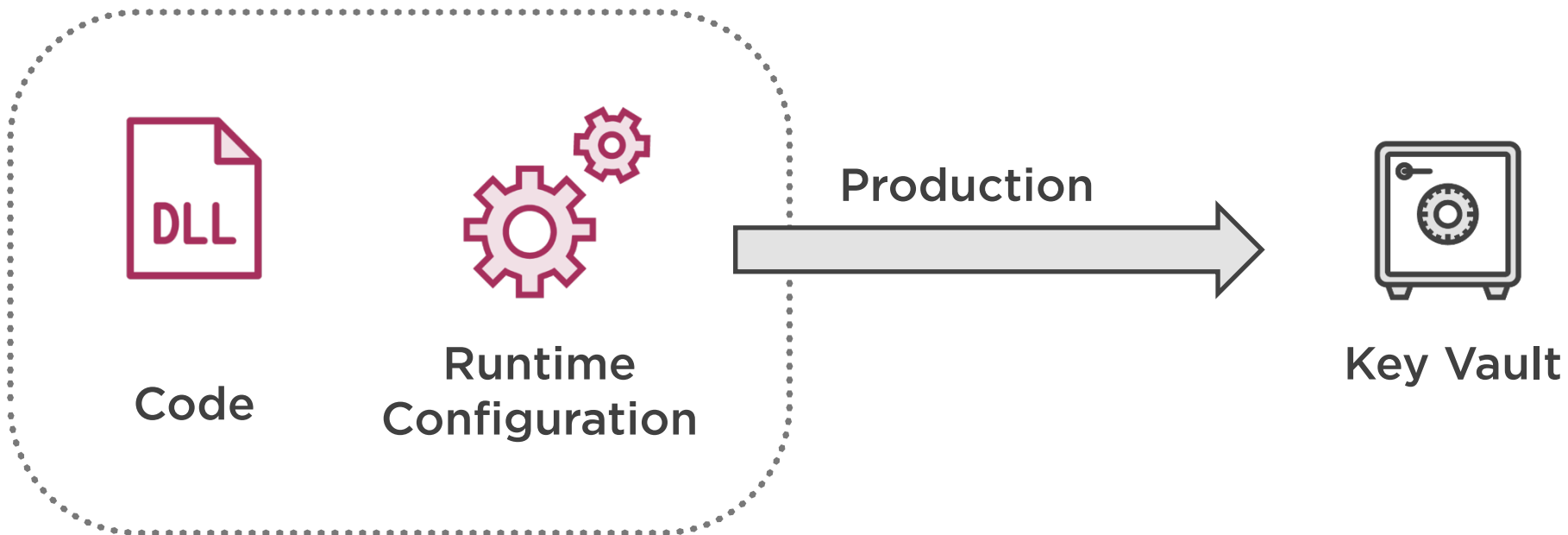
Wired Brain Coffee

ASP.NET Application

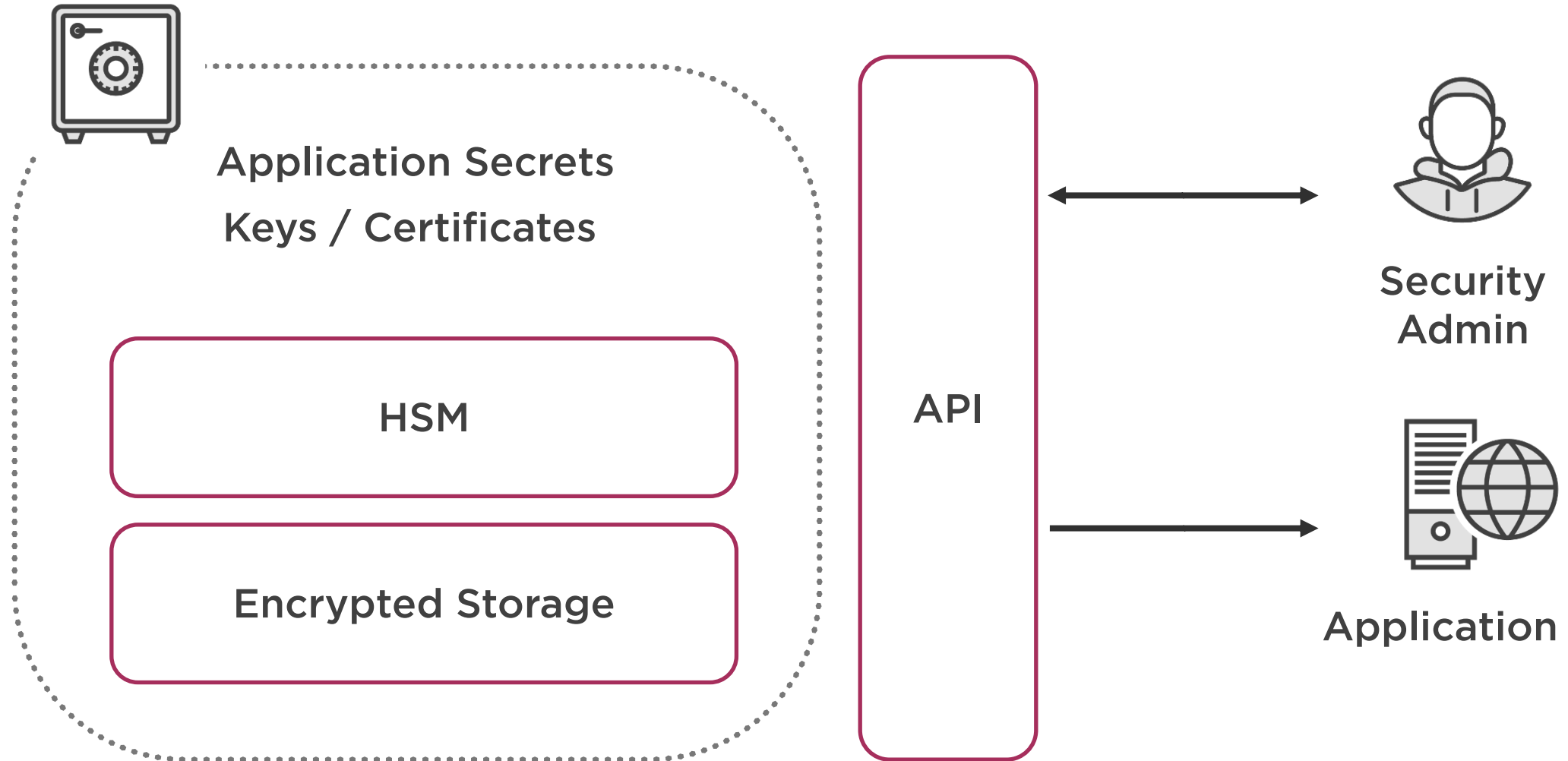


Wired Brain Coffee

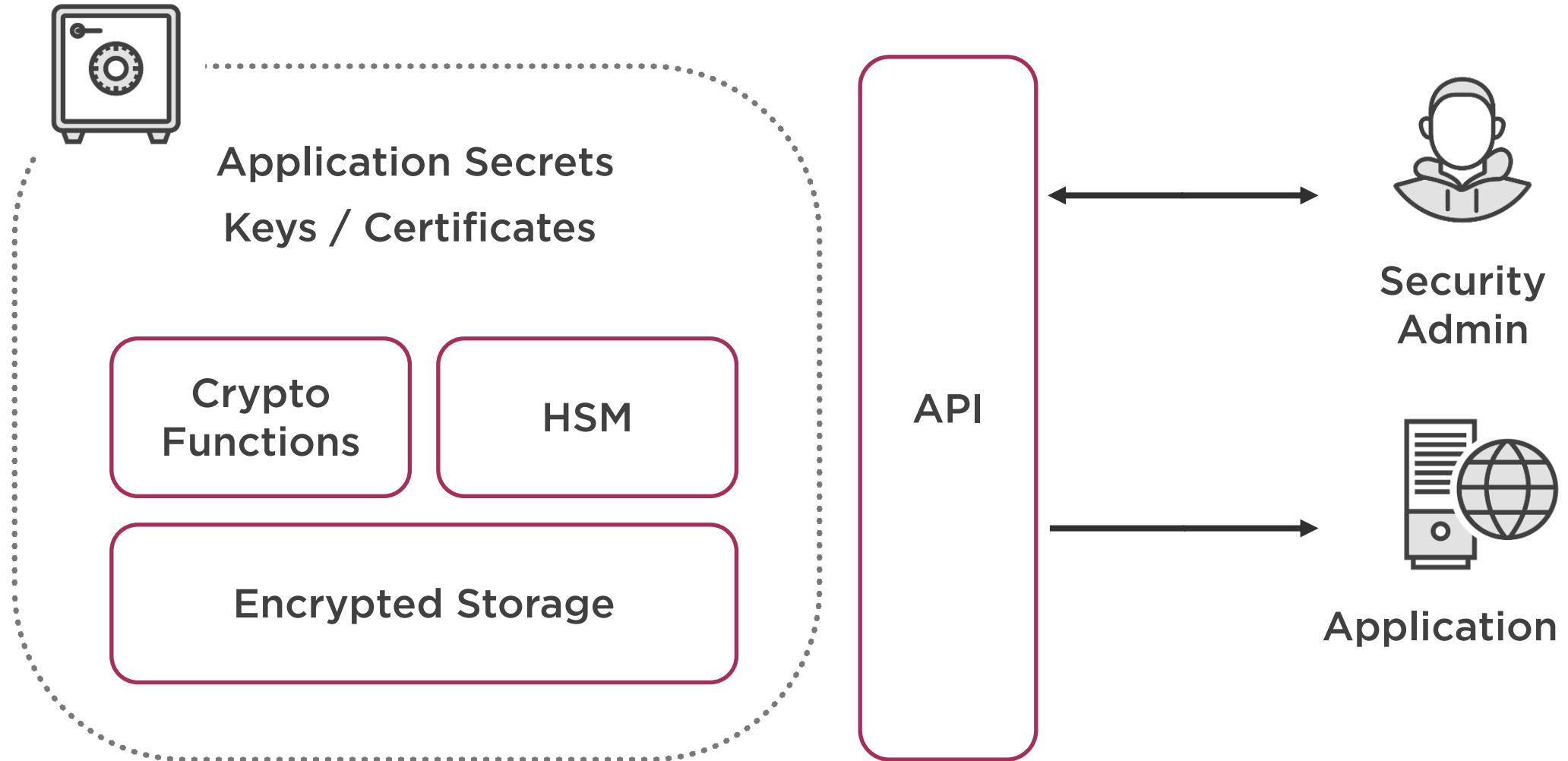
ASP.NET Application



Key Vaults



Key Vaults



Why Use a Key Vault?

Access controls

Compliance

- HIPPA, HITRUST
- FIPS 140
- etc

Logging and auditing

Common approach within an organization



Key Vault Options

AWS Key Management Service

GCP Cloud KMS

Azure Key Vault

Hashicorp Vault

Don't build your own!



Using Azure Key Vault



Using Azure Key Vault



Setup Azure Key Vault and add secrets



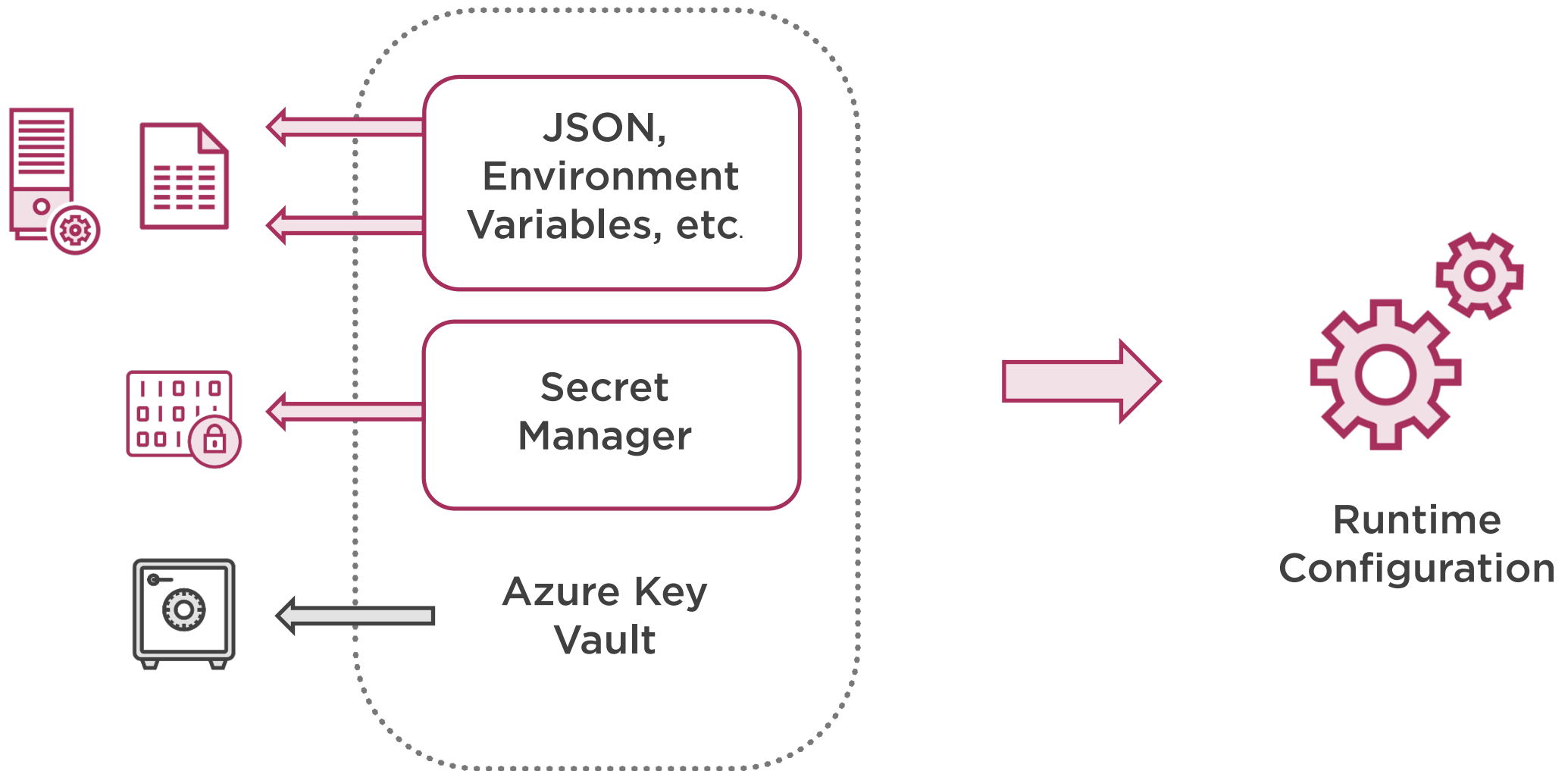
Define authorization scheme



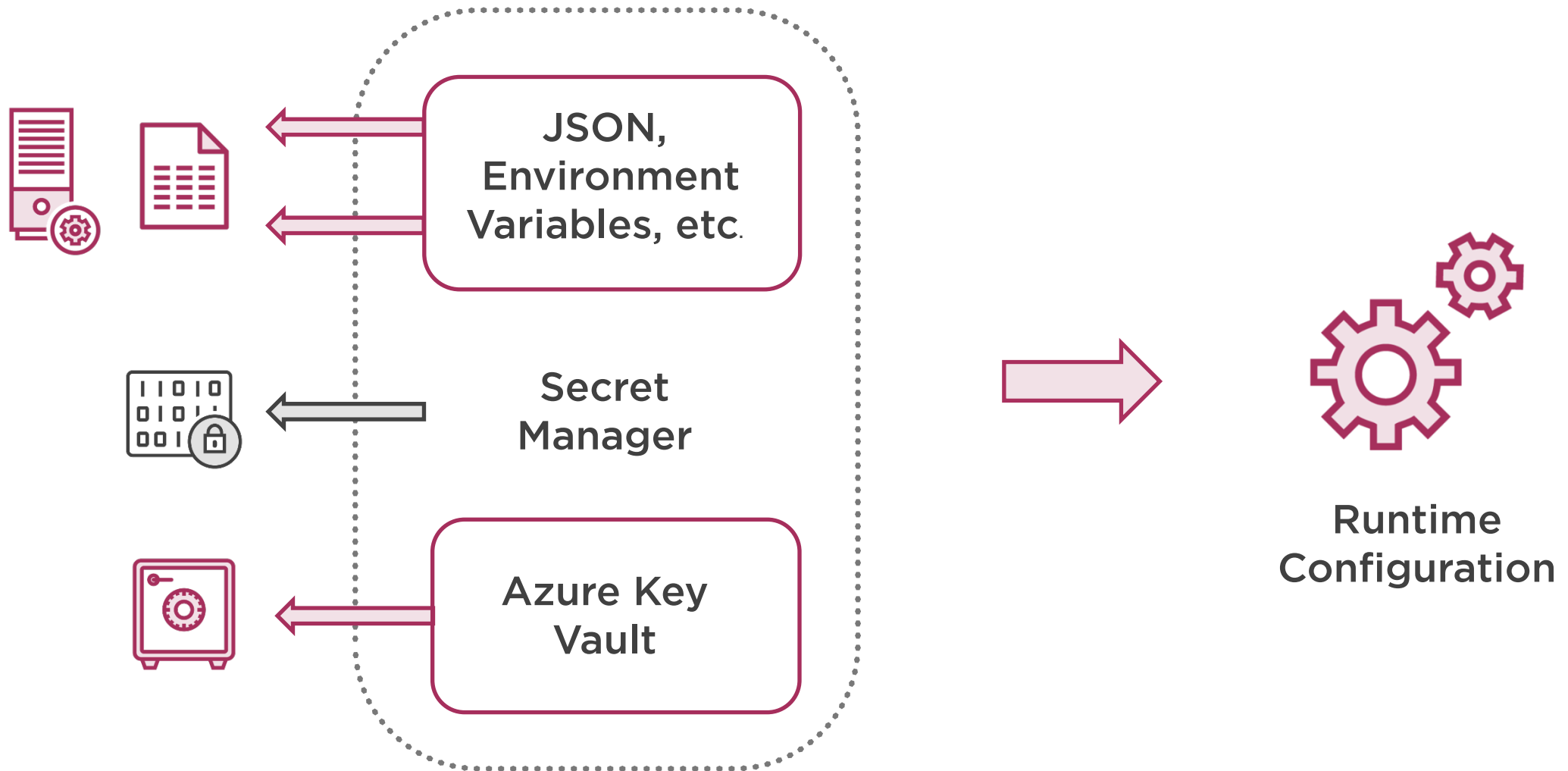
Access secrets at runtime via configuration builder



Running in Development



Running in Production



Authentication Options

OAuth ClientID and Secret

- Accessible, technology independent
- Need to protect initial secret!

Certificates

- Uses server certificate store
- Good on-premise option

Managed Identity

- Automatically taken care of
- Best if hosting in Azure



Demo



Setting up an Azure Key Vault

- Create Key Vault
- Access Control



Isolated Environments



Key Vault Per Environment

Isolation between Test, UAT,
Production



Key Vault Per Application

Isolation between applications

Demo



Using Azure Key Vault in .NET Core

- NuGet package for Azure Key Vault
- Add to configuration build

Test locally

- Authenticate using Azure CLI



Add Azure Key Vault

```
//Authentication
```

```
var tokenSvc = new AzureServiceTokenProvider();
```

```
//Key Vault Client
```

```
var keyVaultClient = new KeyVaultClient(new  
KeyVaultClient.AuthenticationCallback(tokenSvc.KeyVaultTokenCallback));
```

```
//Add Configuration Provider
```

```
config.AddAzureKeyVault("https://your-vault-name.vault.azure.net/",  
keyVaultClient,  
new DefaultKeyVaultSecretManager());
```



Azure Service Token Provider

Authenticate to Azure resources

Automatic authentication

- Visual Studio
- Azure CLI
- Azure Managed Identities



Demo



Using Key Vault .NET Framework 4.7.2

- Add NuGet package
- Use Azure Key Vault configuration builder



Demo



Wired Brain Coffee Production

- Set Managed Identities
- Assign permissions to Key Vault



Summary



Key Vaults

- Cloud or on-premise
- Strict access control
- Option to use a Hardware Security Module (HSM)

Azure Key Vault

- .NET Core and .NET Framework providers via Nuget
- Managed Identities
- Azure CLI
- One per environment and per app





Course Complete!

Keep your secrets out of the codebase. Store them securely and limit access as much as possible.

