

Security

Rasmus Lystrøm
Associate Professor
ITU



Agenda

Authentication and Authorization

Azure Active Directory

ASP.NET Core Web API and Blazor

Encryption in Transit

Secrets

SQL Security

Container Security

Penultimate lecture



Security

Authentication vs. Authorization



Authentication Options

(None)

(Individual User Accounts)

Azure Active Directory

(Windows)

Azure Active Directory (AzureAD/AAD)

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources in:

- External resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications.
- Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.













Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (ondfisk only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

Azure AD B2C

Business to Consumer

Identity provider	
	Amazon
	Apple
	Facebook
	GitHub (Preview)
	Google
	LinkedIn
	Local account
	Microsoft Account
	QQ (Preview)
	Twitter
	WeChat (Preview)
	Weibo (Preview)

Key takeaway:

Don't roll your own security/identity layer



Image source: <http://lazergaze.tumblr.com/post/26333564955>

Security in ASP.NET Core Web API

Demo

<https://docs.microsoft.com/en-us/aspnet/core/blazor/security/webassembly/hosted-with-azure-active-directory>



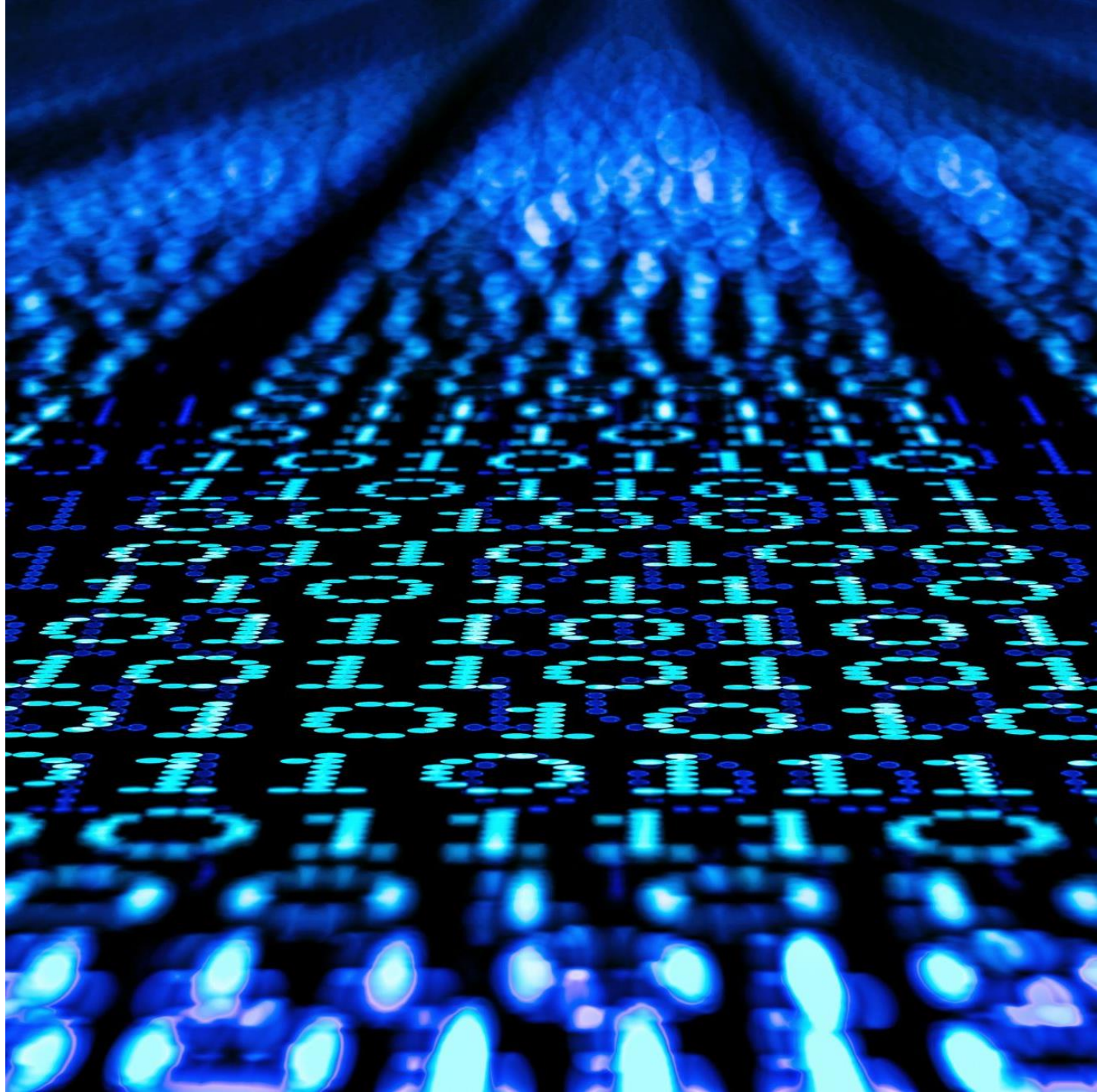
Encryption in Transit

Encryption in Transit

SSL

HTTPS

TLS 1.2



Encryption in Transit

Always enforce HTTPS

Do not expose HTTP – except for automatic redirect – *TEST*

Containers should communicate over secure channels only (cf. Dapr and Azure Container Apps)



Secrets

Secrets

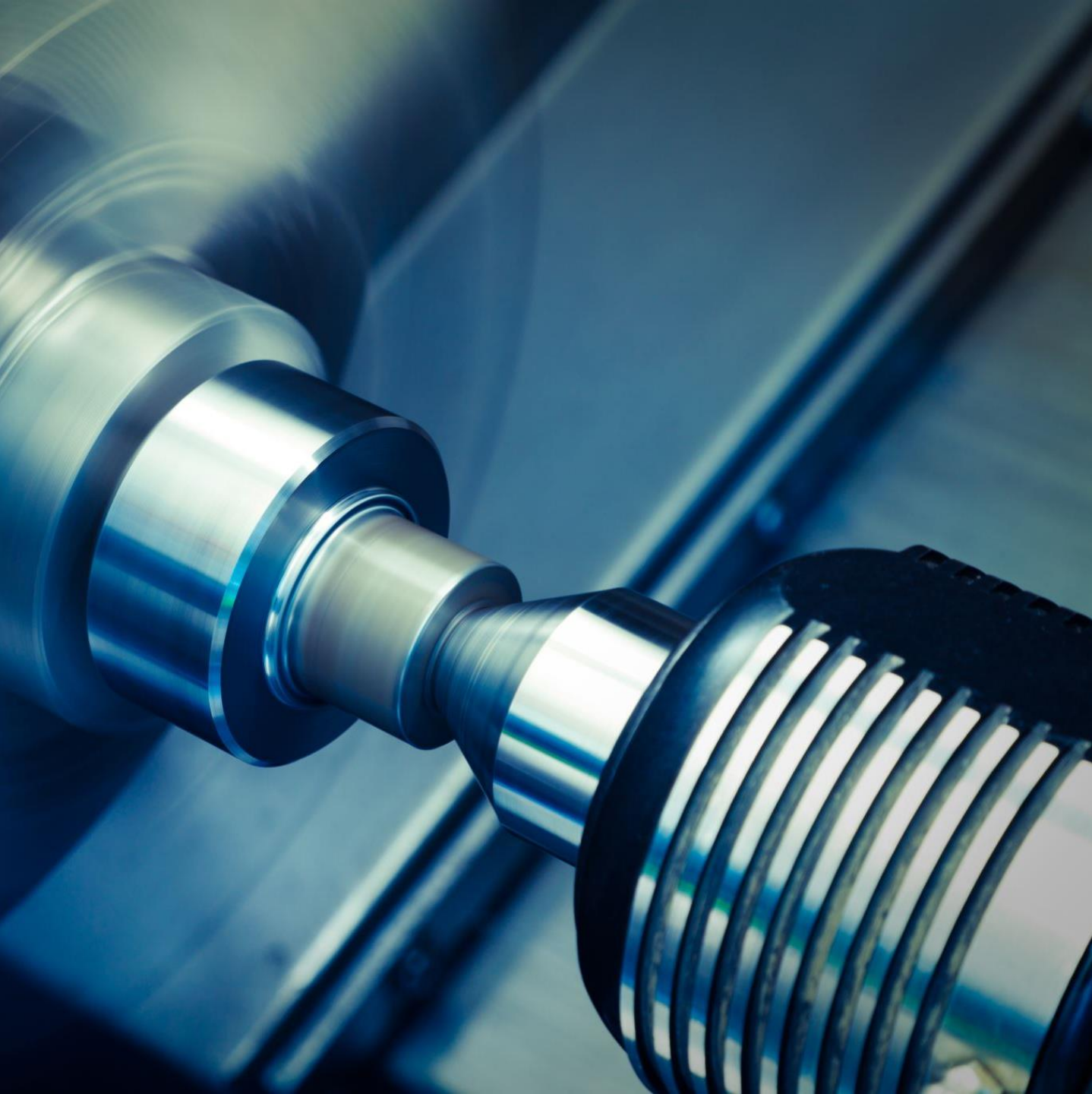
Use user-secrets in *DEV*

Use platform specific secret handling in *PROD*:

- Azure Key Vault
- App Services settings
- HashiCorp Vault

SQL Security





SQL Security

Azure Managed Identity

Don't use SA in production

Discrete user per app

Container Security



Container Security

All applies!

No exceptions

Containers are not a security layer

Network security does not count!

Assume compromise!

HTTPS: <https://docs.microsoft.com/en-us/aspnet/core/security/docker-https>

Security

Demo

$y = g(x)$
 Secant Lines
 $x+h$

Tangent Lines

$$f'(x) = \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h}$$

$$f(x) = \lim_{h \rightarrow 0} \frac{(x+h)^2 - x^2}{h}$$

$$= \lim_{h \rightarrow 0} \frac{x^2 + 2xh + h^2 - x^2}{h}$$

$$= \lim_{h \rightarrow 0} \frac{2xh + h^2}{h}$$

$$= \lim_{h \rightarrow 0} \frac{h}{h(x+h-x)} = \lim_{h \rightarrow 0} \frac{1}{x+h-x} = \frac{1}{2\sqrt{x}}$$

$$f(x) = \lim_{\Delta x \rightarrow 0} \frac{f(x+\Delta x) - f(x)}{\Delta x}$$

$$f(a) = \lim_{h \rightarrow 0} \frac{f(a+h) - f(a)}{h}$$

Last Lecture

December 3 will be the last one

What are we missing?

What do you want repeated?

Will cover:

Continuous deployment of *MyApp* to Azure using *GitHub Actions*

Thank You