

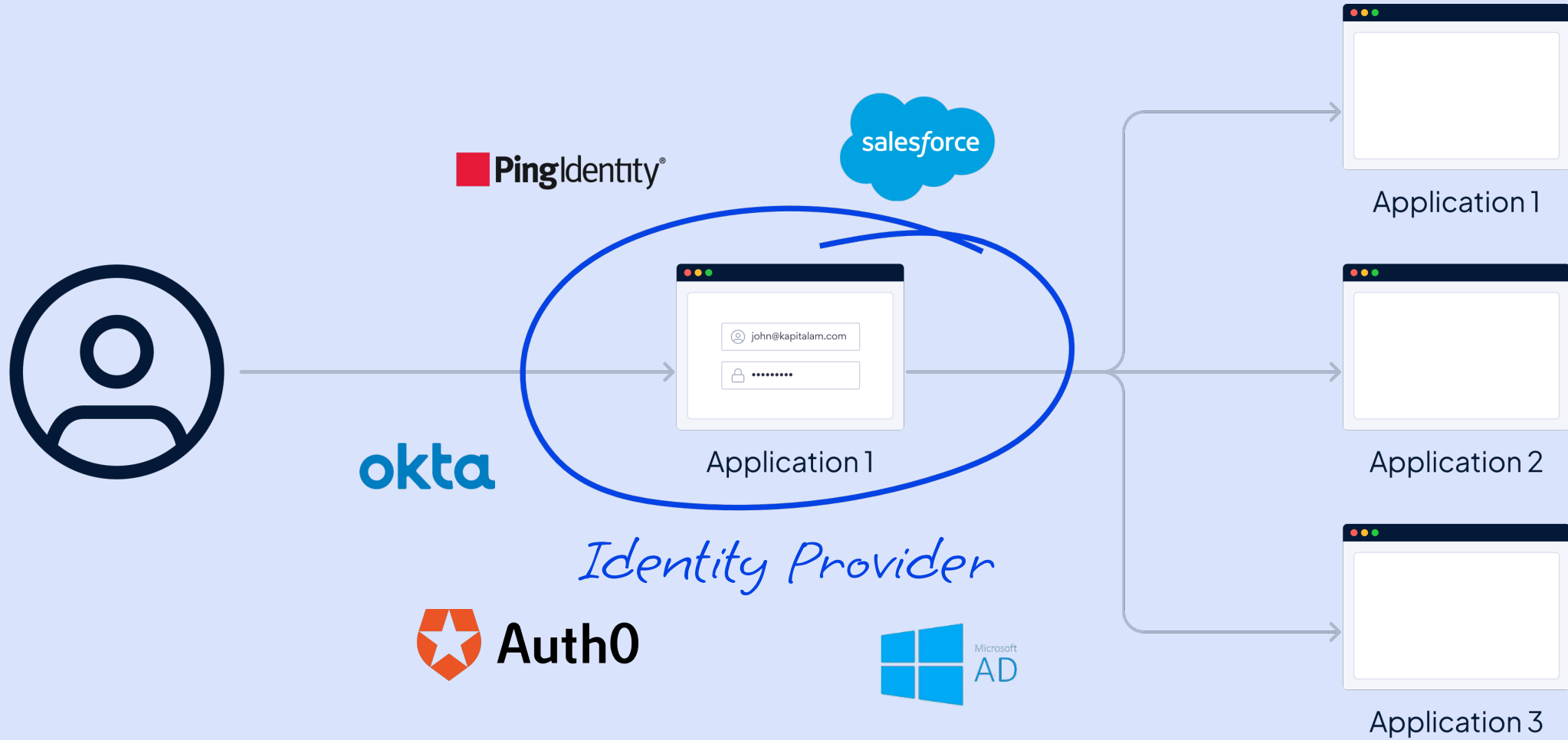
May - 23

*Training*

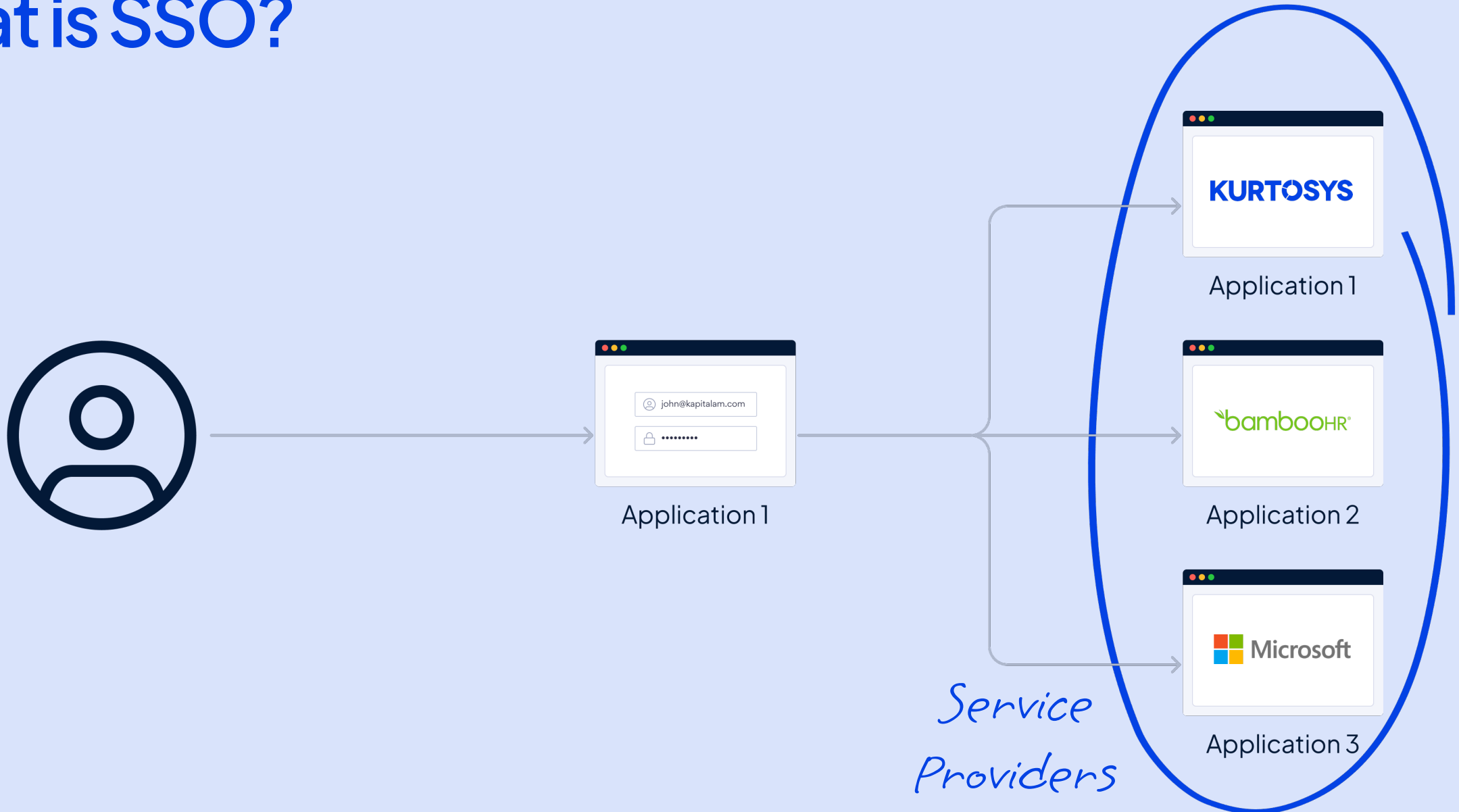
# Single Sign On



# What is SSO?



# What is SSO?



# Types of SSO Methods

SAML



OAuth



OpenID



# Configure Service Provider Strategy

Configure Service Provider Strategy

Name

Login with Azure

---



*Strategy Name that shows on SSO login button*

Application user will be logging into

SAML SP (Service Provider)

The screenshot shows a configuration panel for an application. The 'Application' field is set to 'KurtosysApp'. The 'Strategy Type' is set to 'SAML SP'. The 'Callback URL' is 'https://uk.kurtosys.app/services/auth/48E9bd/saml/assert'. There are blue arrows pointing to the application name, the strategy type, and the callback URL.

Application	KurtosysApp
Strategy Type	SAML SP
Callback URL	https://uk.kurtosys.app/services/auth/48E9bd/saml/assert

URL user will be redirected to after successful login

Kurtosys App = \*.kurtosys.app  
Auth App = App GUID

Autogenerated

User Creation

---

Create new user on first successful authentication?

Roles that will be assigned to the new user

Administrator

Kapital Asset Management Admin

Customer Rep

Author

Data Role

Customer

Portal

---

Configure User from SAML Assertion?  *Configure user using details from Identity Provider*

Assertion Attribute Assign in the Kurtosys App

http://schemas.microsoft.com/ws/2008/06/identity/claims/role → Role ▼ ×

[+ Add assertion mapping](#)

---

Configure User Application Access  *Set which apps the user has access to*

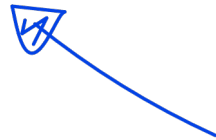
---

Assertion Verification Redirect

Assertion Attribute *Attribute as sent in assertion* → Verification value *What should the incoming value be?*

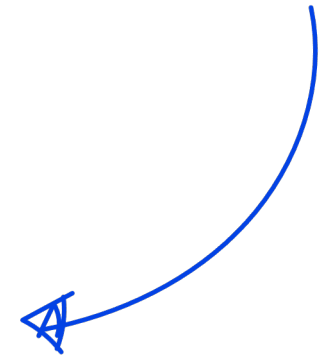
---

Verification fail redirect *URL where the user should be redirected to if value doesn't match*



*Create new user on their first login & assign these roles on each login*

*Would only be Auth App or Kurtosys App*



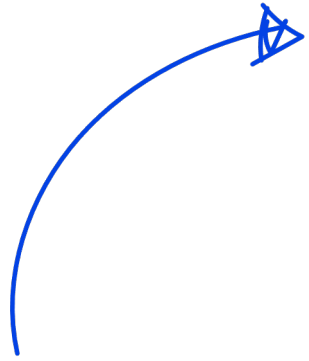
Signing

Signature Algorithm  
sha256

Signature Certificate

```
MIIC8DCCAdigAwIBAgIQVRnyYxuHhrRD71
dGVkIFNTTyBDZXJOaWZpY2FOZTAeFwOy
GZWRlcmFOZWQgU1NPIENlcnRpZmljYXRlI
Y3vm4X2wnT8FzZGD8U7g2RrRKPQ1xaFHk
8dwkYadbEpoEXyupvdUg4ANZFH5FDK7C
BM/r1siK3W/c8r838mHiZylvpPcxsPM7LKh
A4IBAQA7TnGncMrROjbnG/jwZtdHCR1U
Eanl7Bto257veh9RCiJFkZSLfyBuTVMtviuJ
91xUZv7QhB5LzD6srdZjaTUN8vajgKdft22c
eMsQithcla
```

*We only have one method* ▼



*Client should provide certificate  
and is pasted in as text*



*URL to the Identity Provider  
Provided by the client*

Domain
SAML identity provider's entry point
<a href="https://login.microsoftonline.com/5efd469c-a85d-4e8c-accd-a59d57212f68/saml2">https://login.microsoftonline.com/5efd469c-a85d-4e8c-accd-a59d57212f68/saml2</a>
Domain for this strategy's assertion URL
<a href="https://uk.kurtosys.app">https://uk.kurtosys.app</a>
SAML issuer
<a href="https://uk.kurtosys.app/">https://uk.kurtosys.app/</a>

*Generated by Kurtosys*

*Can be any string of text  
Reusing the Callback URL works well*

*Needs to match the settings in the client's Identity Provider*

Authentication	
Authentication Context	urn:oasis:names:tc:SAML:2.0:ac:classes:Password
Name ID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Request Type	HTTP-POST
Federation Key	Email

*Shouldn't need to change*

*What the incoming value needs to match in the Kurtosys App to authenticate the user?*

- Email*
- Username*
- External User Identifier (User Profile Page)*

Thank you.  
Questions?

**KURTOSYS**