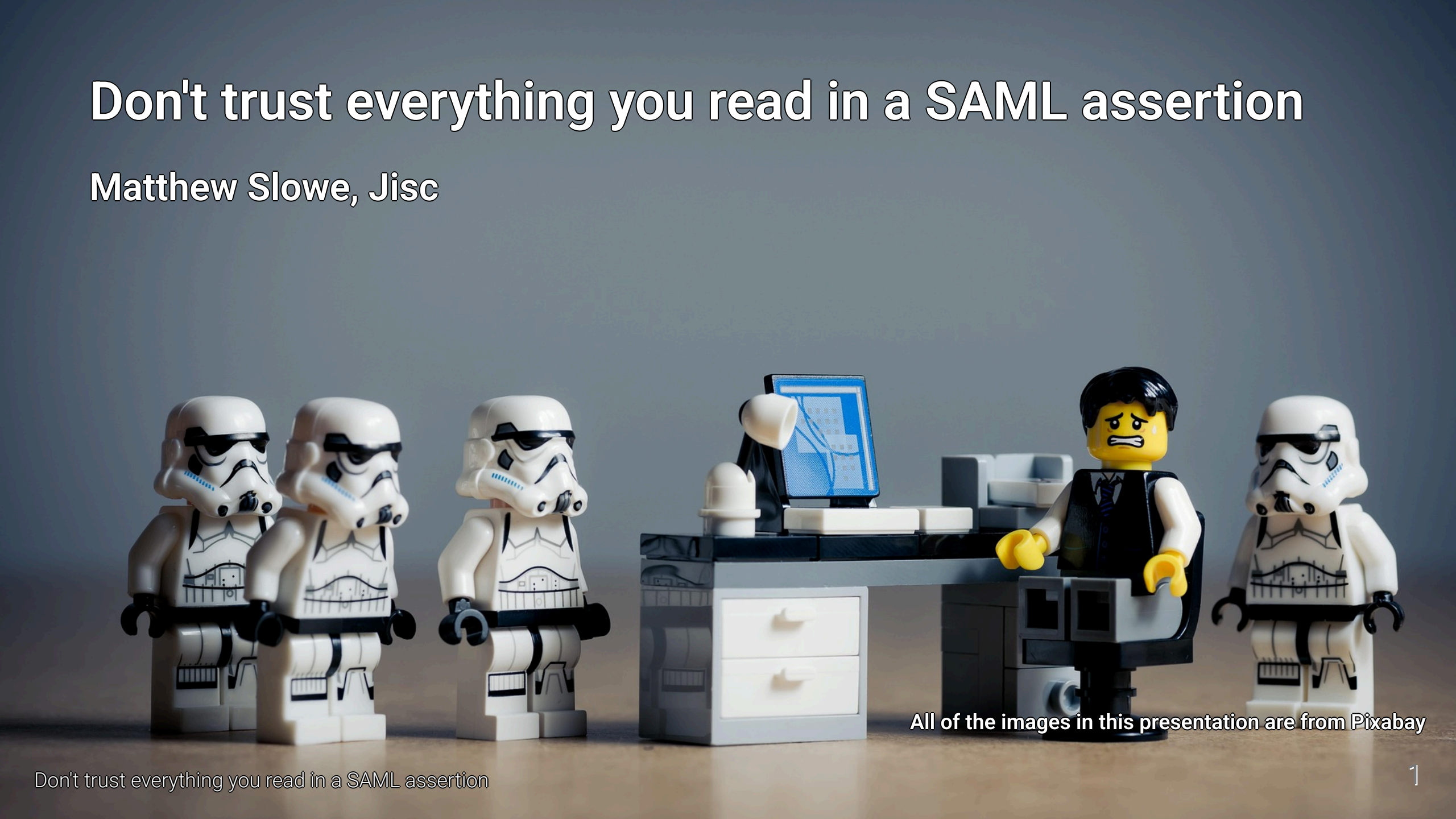
Don't trust everything you read in a SAML assertion

Matthew Slowe, Jisc



All of the images in this presentation are from Pixabay

Walter

Tenant list

Tenant
Windsor Multimedia
~~Bristol Innovations~~
Caribbean Holidays

Alice

Windsor Multimedia

Room A

Expires: 2025-06-21

Don't trust everything you read in a SAML assertion

Charlie

Bristol Innovations

Room B

Expires: 2025-04-01

Don't trust everything you read in a SAML assertion

Oscar

Caribbean Holidays

Room A

Expires: 2025-06-21

Don't trust everything you read in a SAML assertion

Uhoh!

Walter's security controls were not sufficient to maintain the security of his tenants' offices

New tenant list

Tenant	Room list
Windsor Multimedia	Room A
~~Bristol Innovations~~	
Caribbean Holidays	Room R

Don't trust everything you read in a SAML assertion

Oscar

Caribbean Holidays

Room A

Expires: 2025-06-21

Don't trust everything you read in a SAML assertion

What has this to do with SAML?

Some attributes used for sensitive authorisation:

- eduPersonScopedAffiliation (eg `student@example.ac.uk`)
- eduPersonPrincipalName (and new flavours) (eg `foo@example.ac.uk`)
- eduPersonEntitlement (eg. `https://example.ac.uk/super-admin`)

eduPersonScopedAffiliation
student@example.ac.uk

Alice

Windsor Multimedia

Room A

Expires: 2025-06-21

eduPersonPrincipalName
alice@example.ac.uk

Issuer

eduPersonEntitlement
https://example.ac.uk/roomA

Don't trust everything you read in a SAML assertion

Affiliation

Accessing: *The International Journal of Cyber Security*

Source Organisation	Normal Domain	Asserted Affiliation
University of Hove	`hove.ac.uk`	`student@bexhill-crypto.ac.uk`

Named access (eg eduPersonPrincipalName)

Accessing: *Brighton College of Robotics' Student Records System*

Source Organisation	Student Records Officer	Result
Brighton College of Robotics (`brighton-robotics.ac.uk`)	`alex.smith@brighton-robotics.ac.uk`	✅
Bognor Regis Cybernetics Centre (`brcc.ac.uk`)	`alex.smith@brighton-robotics.ac.uk`	❌

Scope checking

```
<EntityDescriptor entityID="https://idp.jisc.ac.uk/idp/shibboleth">
  <IDPSSODescriptor>
    <Extensions>
      <Scope>jisc.ac.uk<Scope>
      <Scope>corp.jisc.ac.uk<Scope>
  ...
```

Metadata Explorer Tool

Access through your institution

Jisc

Information retrieved from federation: eduGAIN *on May 21, 2025, 9:01 a.m. (3 hours, 48 minutes ago)*

ENTITY ID:	https://idp.jisc.ac.uk/idp/shibboleth
ENTITY TYPE:	IDP
REGISTRATION AUTHORITY:	http://ukfederation.org.uk *(since 28/03/2014)*

Technical details:

SUPPORTED PROTOCOLS:	• SAML 2.0
SCOPES:	• jisc.ac.uk • corp.jisc.ac.uk
CONTACTS:	• Trust and Identity Team [support] • Trust and Identity Team [technical] • Information security [other]

Don't trust everything you read in a SAML assertion

1. Ensure your services have sufficient checks in place for these protected values
2. When deploying, procuring, or outsourcing things, ensure your service provider performs these checks
3. Also consider how eduPersonEntitlement etc are protected
4. Relax on the beach

Matthew Slowe, Jisc
matthew.slowe@jisc.ac.uk