WP3 & WP4 Integration

Tom Griffin, STFC ISIS Facility

Antony Wilson, STFC SCD

Björn Abt, PSI

Lund, Sweden

March 2013

tom.griffin@stfc.ac.uk

Animation is used to show credential flow.
This presentation is best seen in 'Slideshow' mode

This presentation has been amended following feedback at the Lund meeting

Science & Technology Facilities Council
ISIS

……or

What needs to be done so users can access their data in ICAT using their Umbrella account?

Scenarios

1) Real world – authorisation via user office

2) 'Toy' – direct ICAT <-> Umbrella

TopCAT cannot be responsible for much
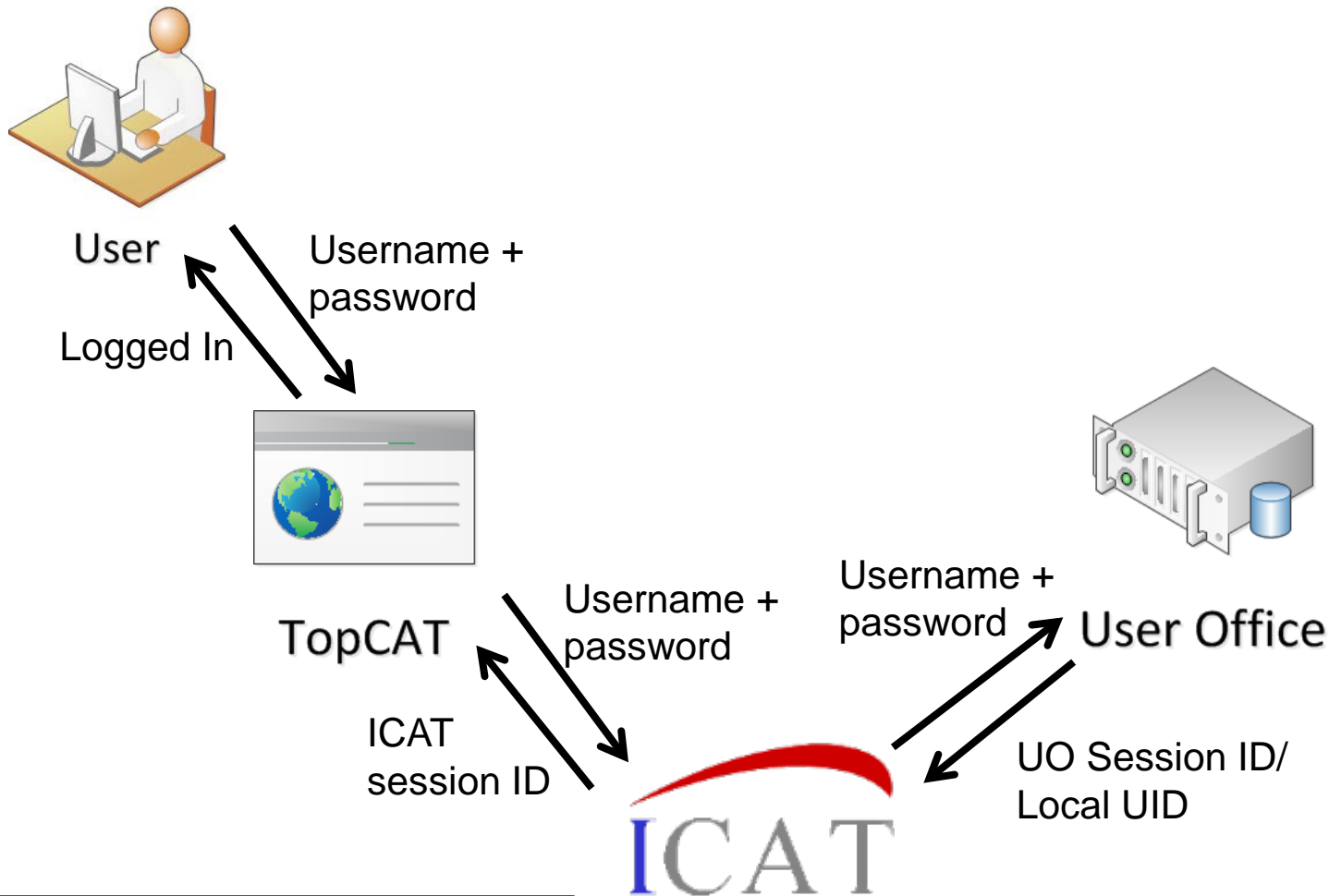Other clients matter too

Real world - ISIS

- Users will always have local ids
- Multiple authentication routes

- Umbrella ID mapped to local id

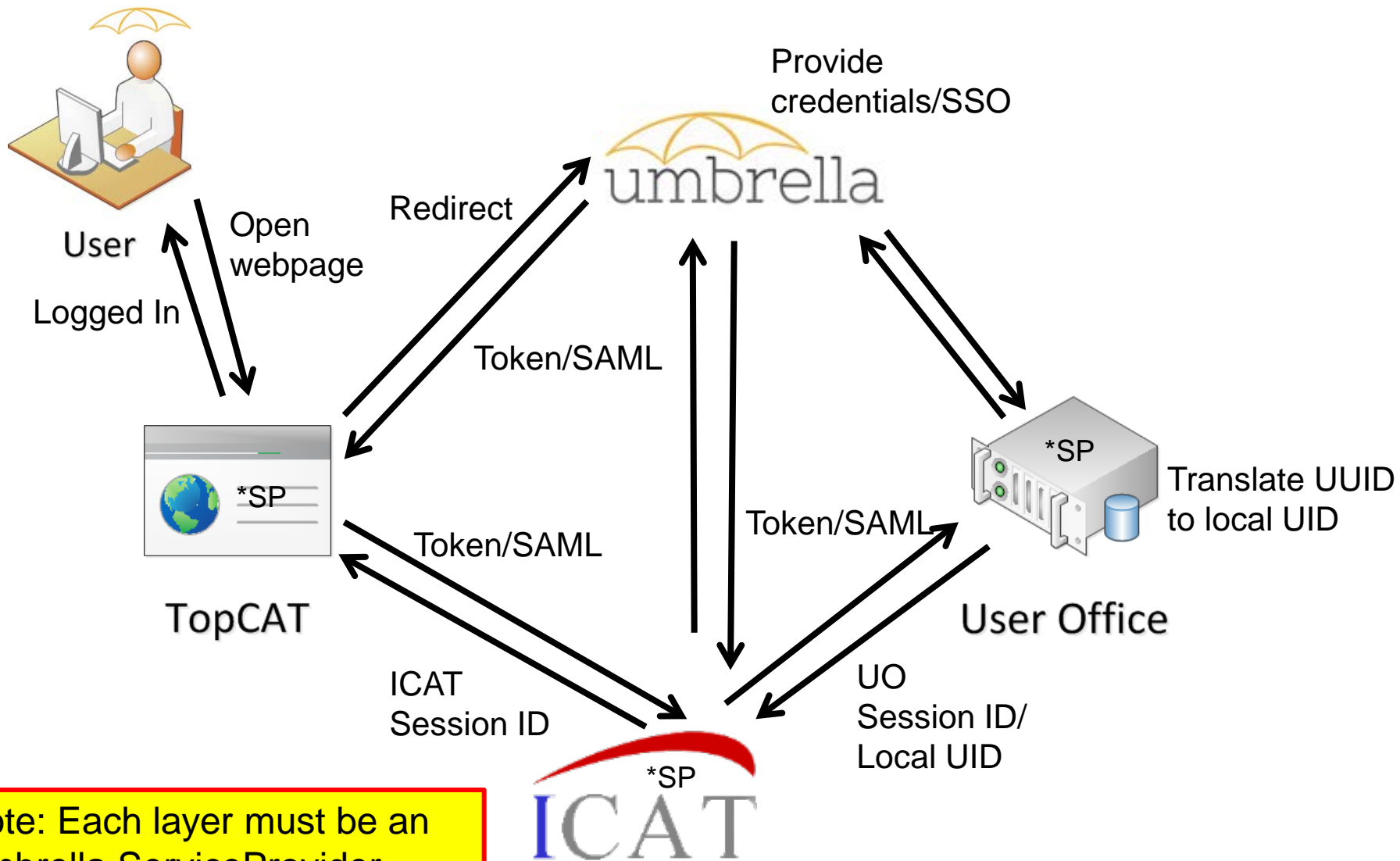- User office / Business system relates users to proposals

Real world – Non Umbrella

User

Username + password

Logged In

TopCAT

Username + password

Username + password

User Office

ICAT session ID

UO Session ID/ Local UID

ICAT

The credentials are passed between each layer in the system

All references to ICAT mean the Authentication component of the ICAT

Real World - 'Pure' Shibboleth

User

Open webpage

Logged In

Redirect

Provide credentials/SSO

umbrella

Token/SAML

Token/SAML

Translate UUID to local UID

*SP

TopCAT

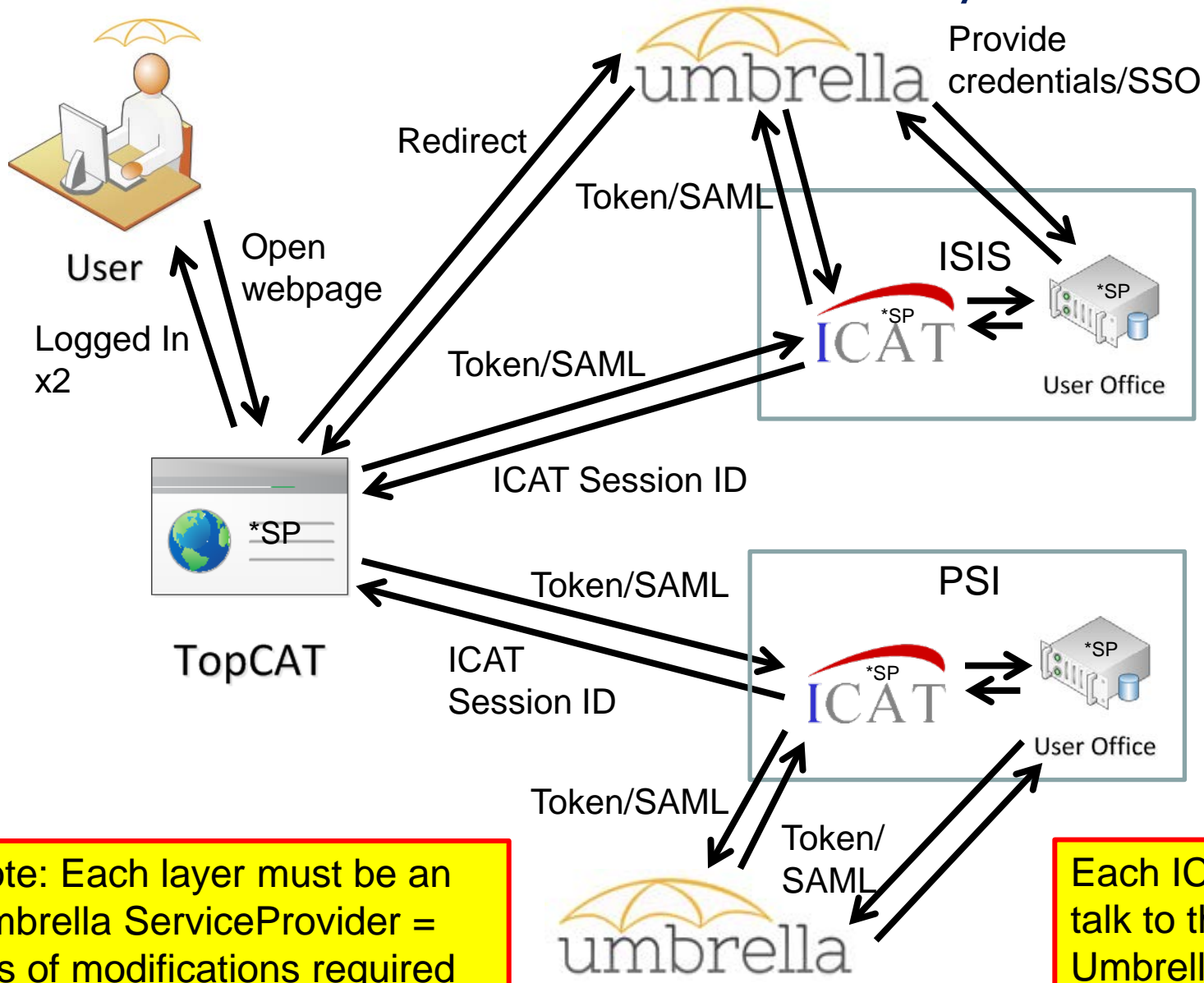Token/SAML

User Office

ICAT Session ID

UO Session ID/ Local UID

*SP

ICAT

Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

'Pure' Shibboleth + UO Portal

User

Open webpage

Logged In

Redirect

User Office Portal

Redirect

Provide credentials/SSO

umbrella

Token/SAML

Token/SAML

UO Session ID/ Local UID

*SP

Translate UUID to local UID

ICAT Session ID

TopCAT
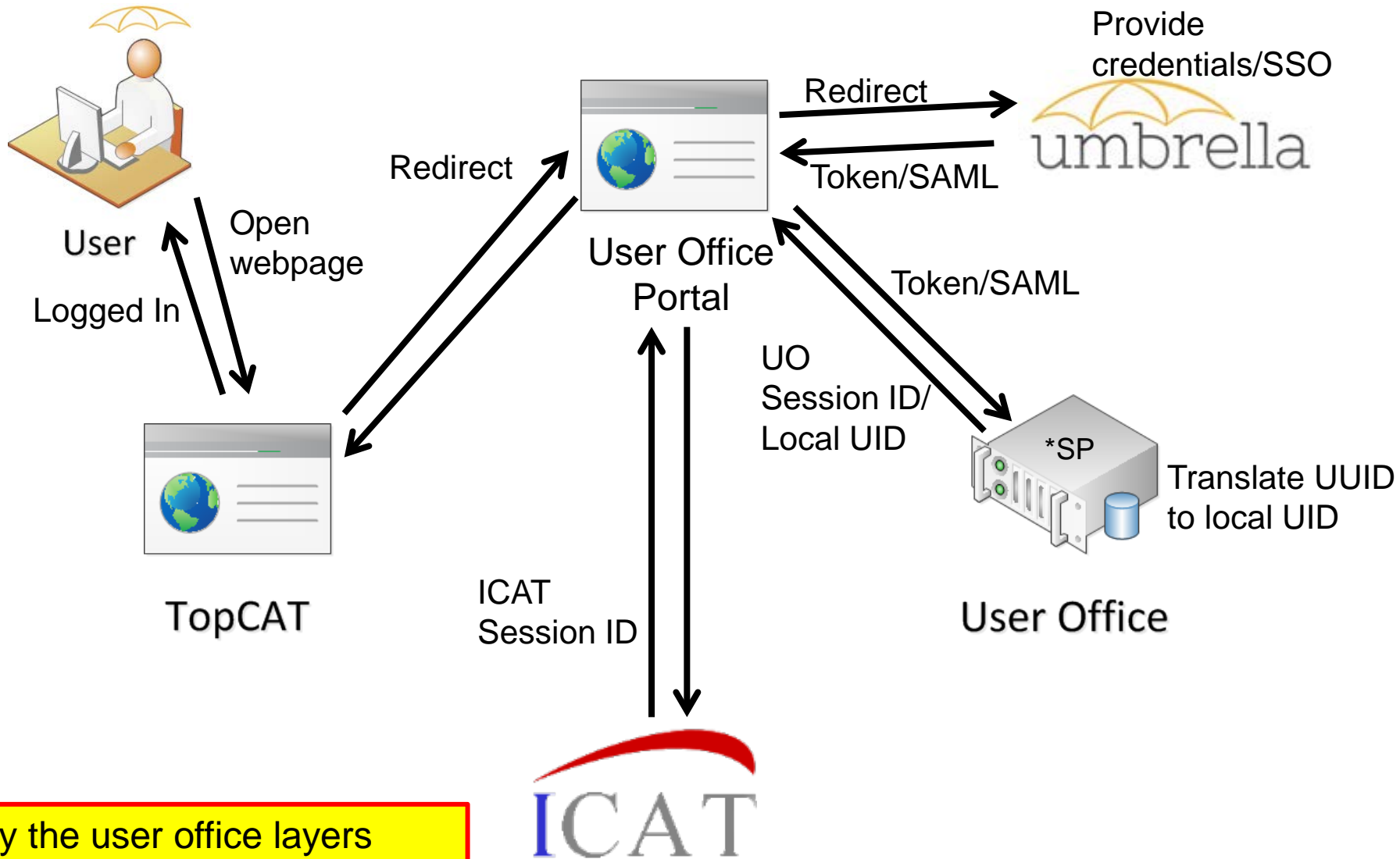
User Office

ICAT

Only the user office layers needs to be Umbrella SPs

Real world –Umbrella – Many ICATs

Provide credentials/SSO

Redirect

Token/SAML

ISIS

*SP

User Office

Open webpage

User

Logged In x2

Token/SAML

Token/SAML

ICAT Session ID

*SP

TopCAT

Token/SAML

PSI

*SP

ICAT Session ID

User Office

Token/SAML

Token/ SAML

Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

Each ICAT/UO will talk to the most local Umbrella IdP

Real world –Umbrella – Mantid/Dawn

User

Username + password

Logged In

Mantid

umbrella

Username + password

Umbrella Token/SAML

*SP

Translate UUID to local UID

Username + password

Username + password

User Office

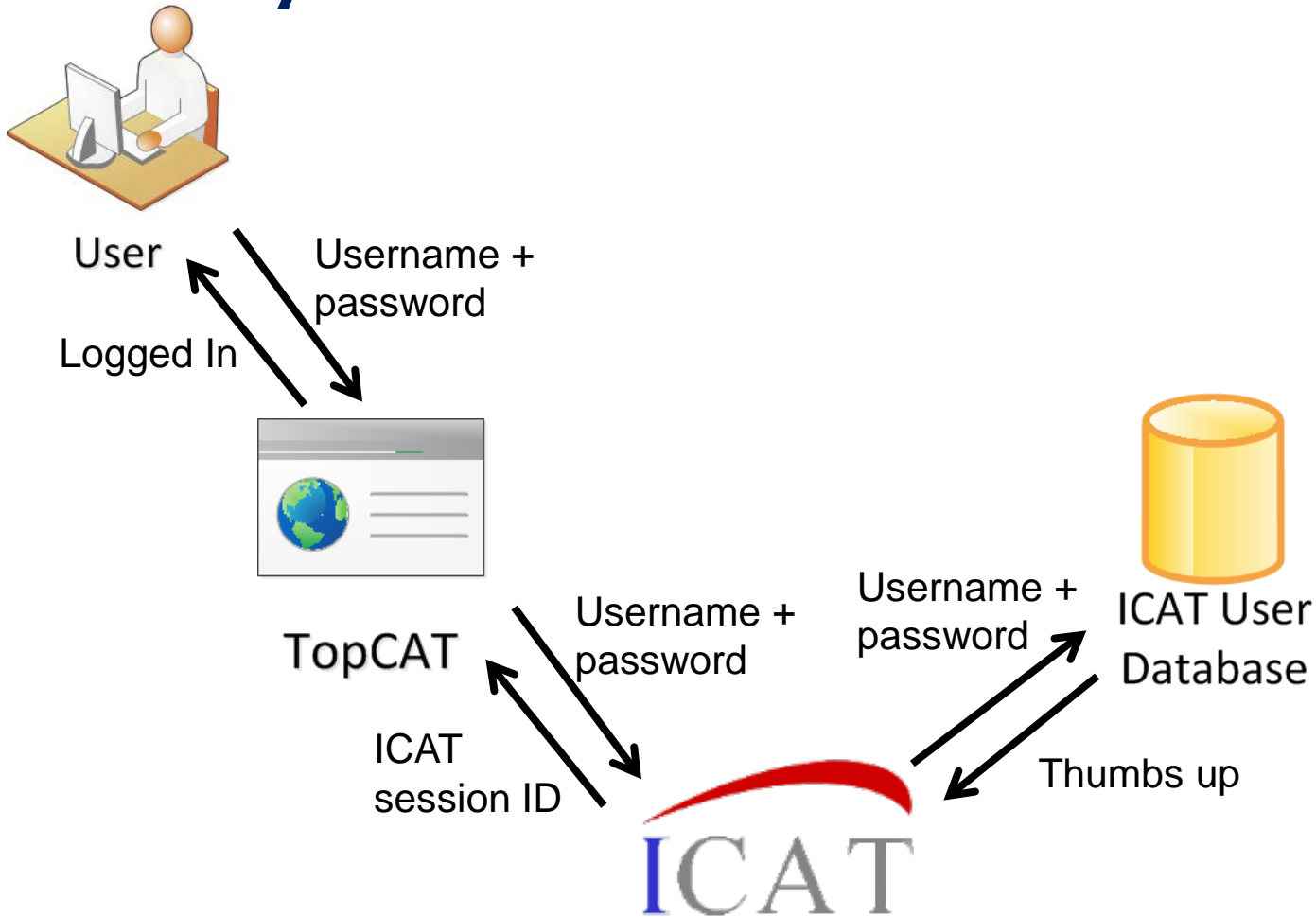ICAT session ID

UO Session ID/ Local UID

ICAT

Umbrella uses web technologies. Mantid is a client application, so credentials must be explicitly passed

'Toy' – Direct connection

- Extend the ICAT user database/authn plugin

- Add Umbrella ID as an attribute

- Allow any authenticated umbrella user to create a local account

Science & Technology Facilities Council
ISIS

'Toy' ICAT – Non-Umbrella

User

Username + password

Logged In

TopCAT

Username + password

ICAT session ID

Username + password

ICAT User Database

Thumbs up

ICAT

'Toy' ICAT – Umbrella

Username	Password
root	Secret
tom.griffin	
mantid_test	testpassword
…	…

Real World - 'Pure' Shibboleth

ICAT Authentication layer explicitly shown
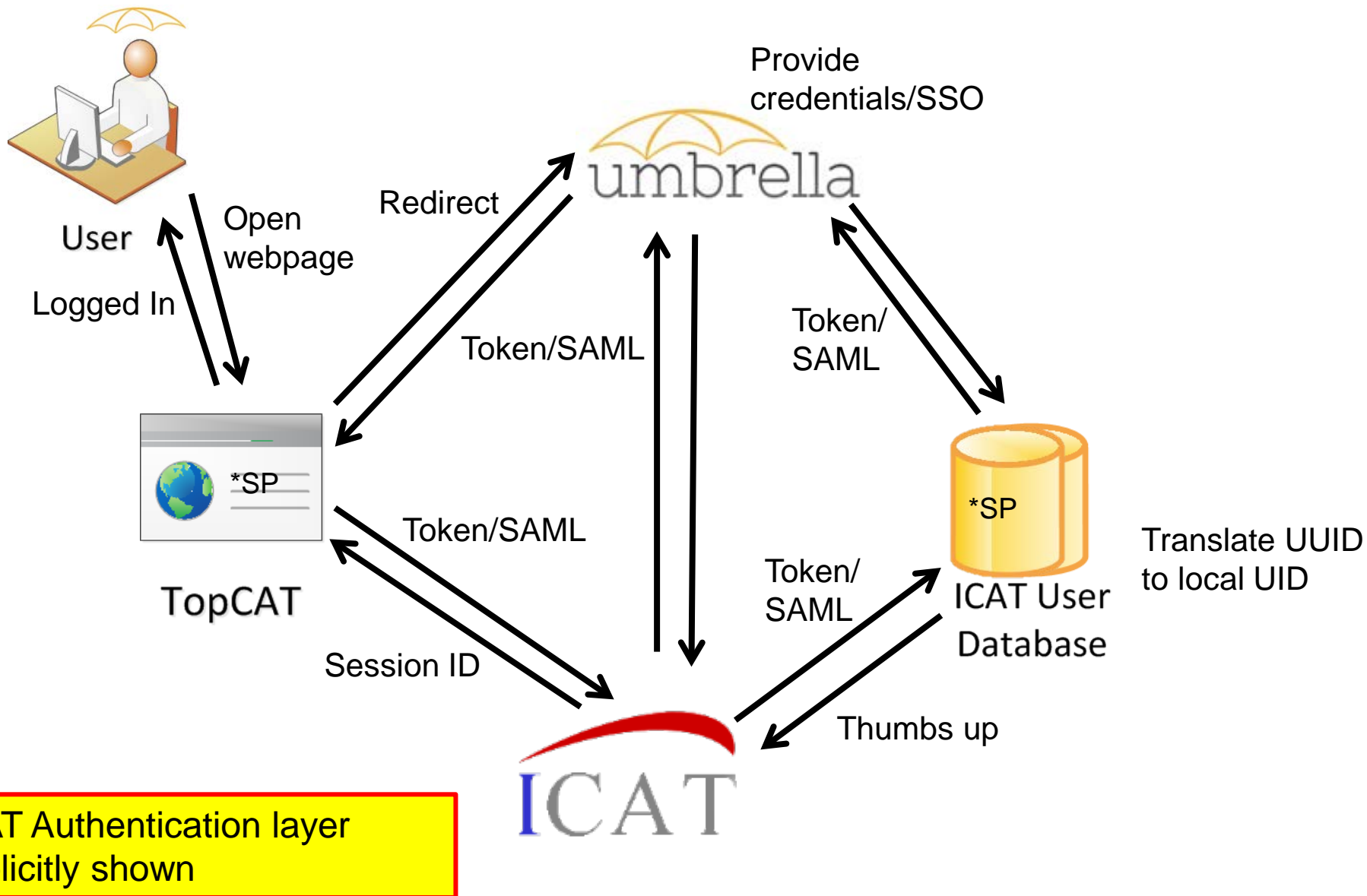
Summary

- Many options
  - Cheap and easy
  - More work, smoother experience
- ICAT db_authn can be modified to support 'toy' implementations with Umbrella
- Real world implemenations always go via the user office

Questions…