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

.....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

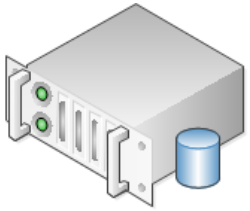
- Umbrella ID mapped to local id

- User office / Business system relates users to proposals

Real world – Non Umbrella

User

TopCAT



User Office

ICAT

The credentials are passed between each layer in the system

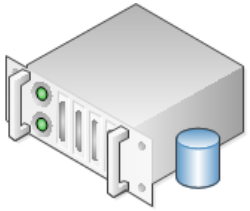
All references to ICAT mean the Authentication component of the ICAT

Real world – Non Umbrella

User

Username + password

TopCAT



User Office

ICAT

The credentials are passed between each layer in the system

All references to ICAT mean the Authentication component of the ICAT

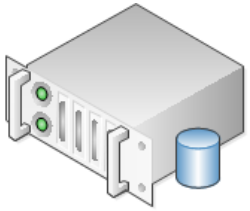
Real world – Non Umbrella

User

Username + password

TopCAT

Username + password



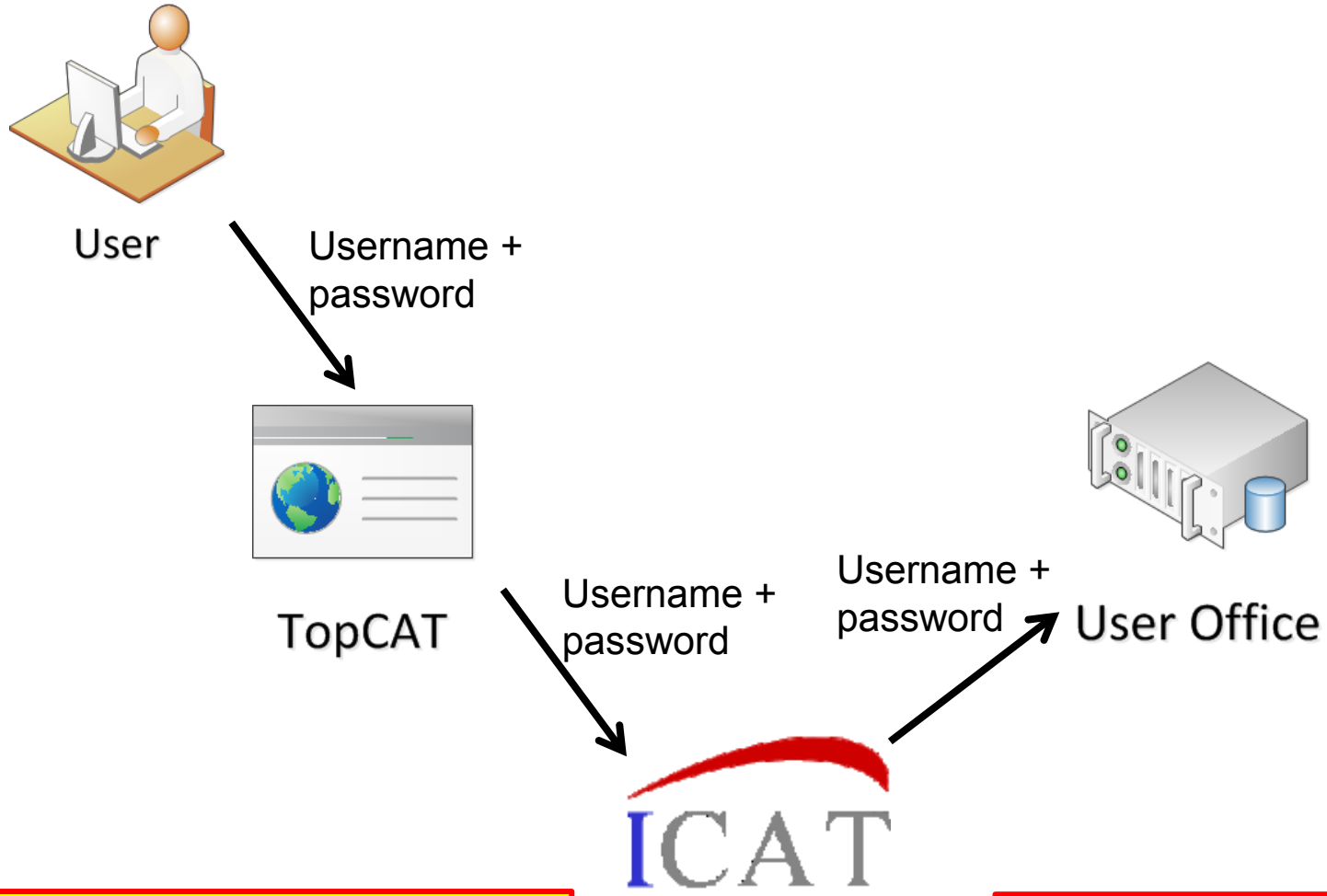
User Office

ICAT

The credentials are passed between each layer in the system

All references to ICAT mean the Authentication component of the ICAT

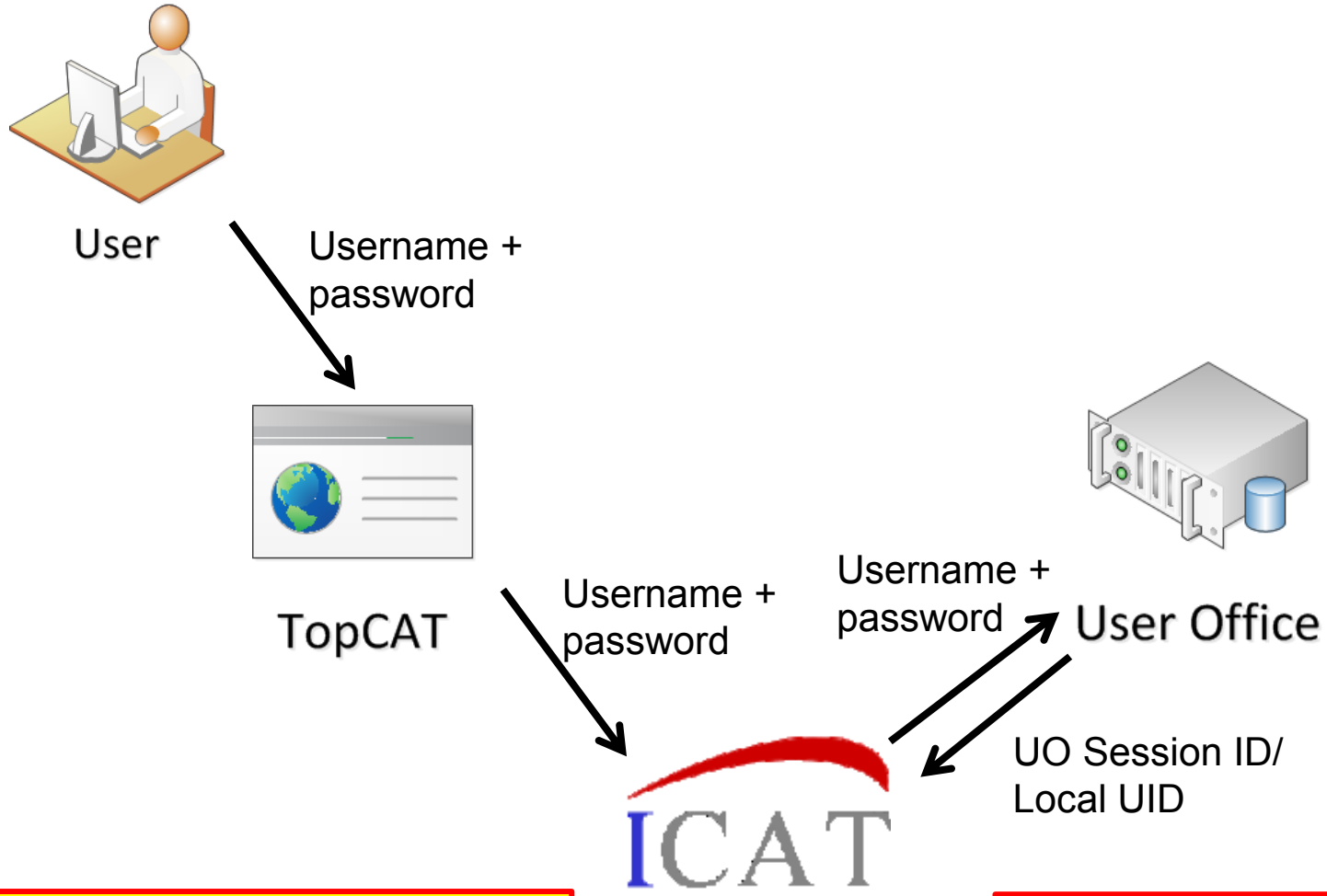
Real world – Non Umbrella



The credentials are passed between each layer in the system

All references to ICAT mean the Authentication component of the ICAT

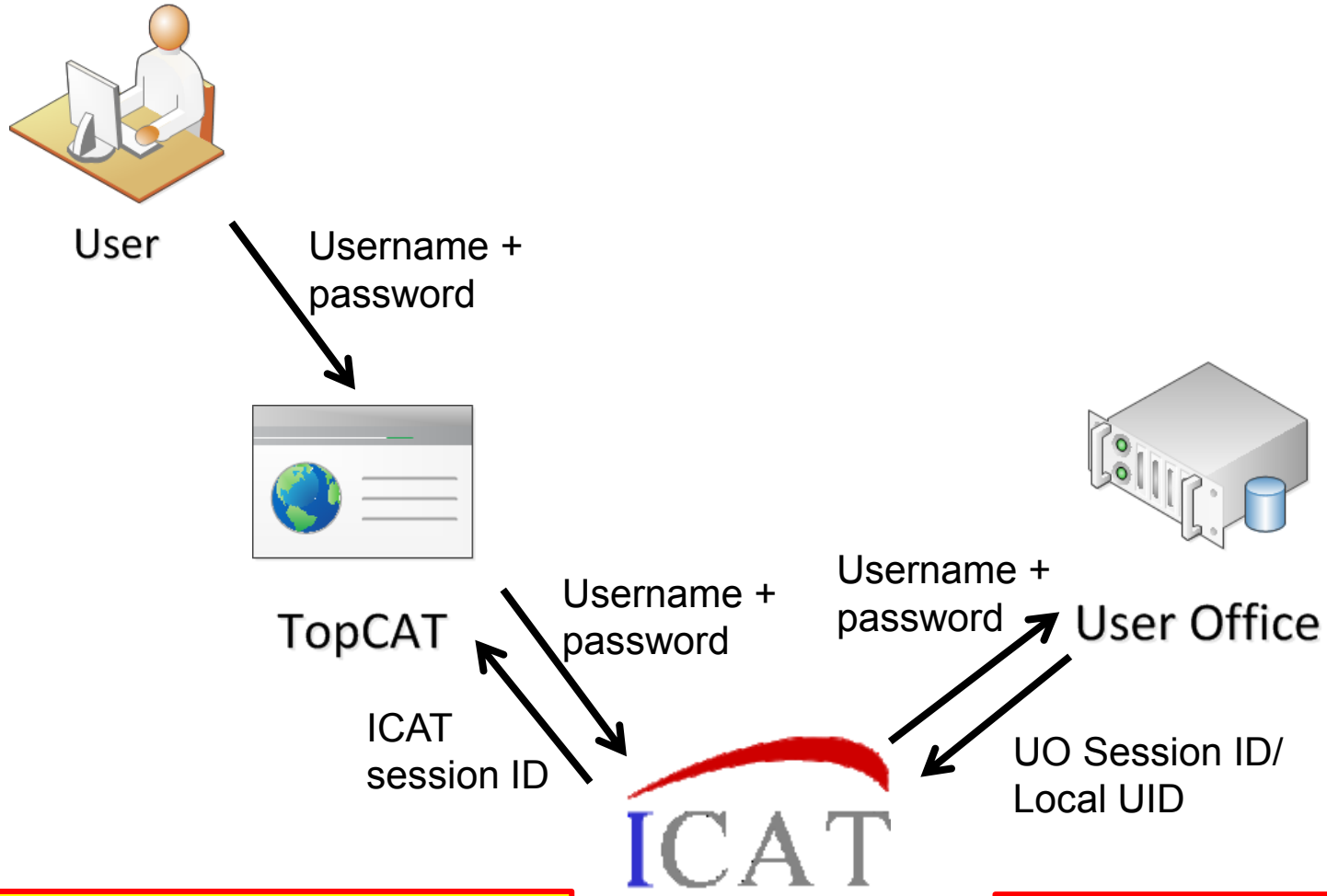
Real world – Non Umbrella



The credentials are passed between each layer in the system

All references to ICAT mean the Authentication component of the ICAT

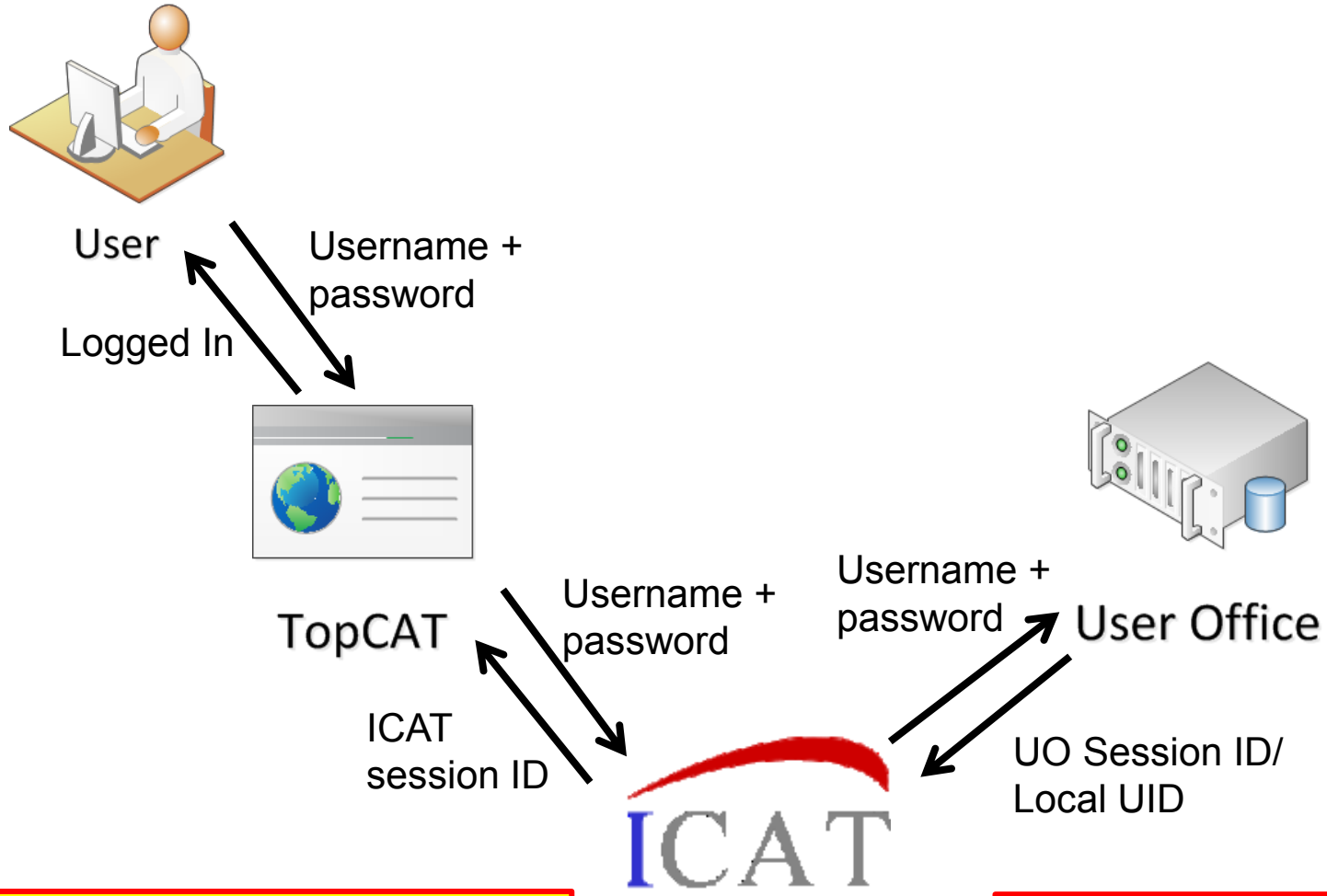
Real world – Non Umbrella



The credentials are passed between each layer in the system

All references to ICAT mean the Authentication component of the ICAT

Real world – Non Umbrella



The credentials are passed between each layer in the system

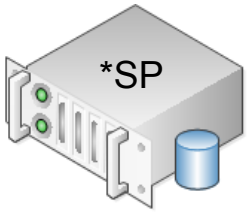
All references to ICAT mean the Authentication component of the ICAT

Real World - 'Pure' Shibboleth

User

umbrella

TopCAT



User Office

*SP
ICAT

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

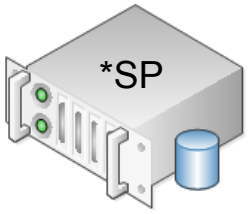
Real World - 'Pure' Shibboleth

User

Open webpage

umbrella

TopCAT

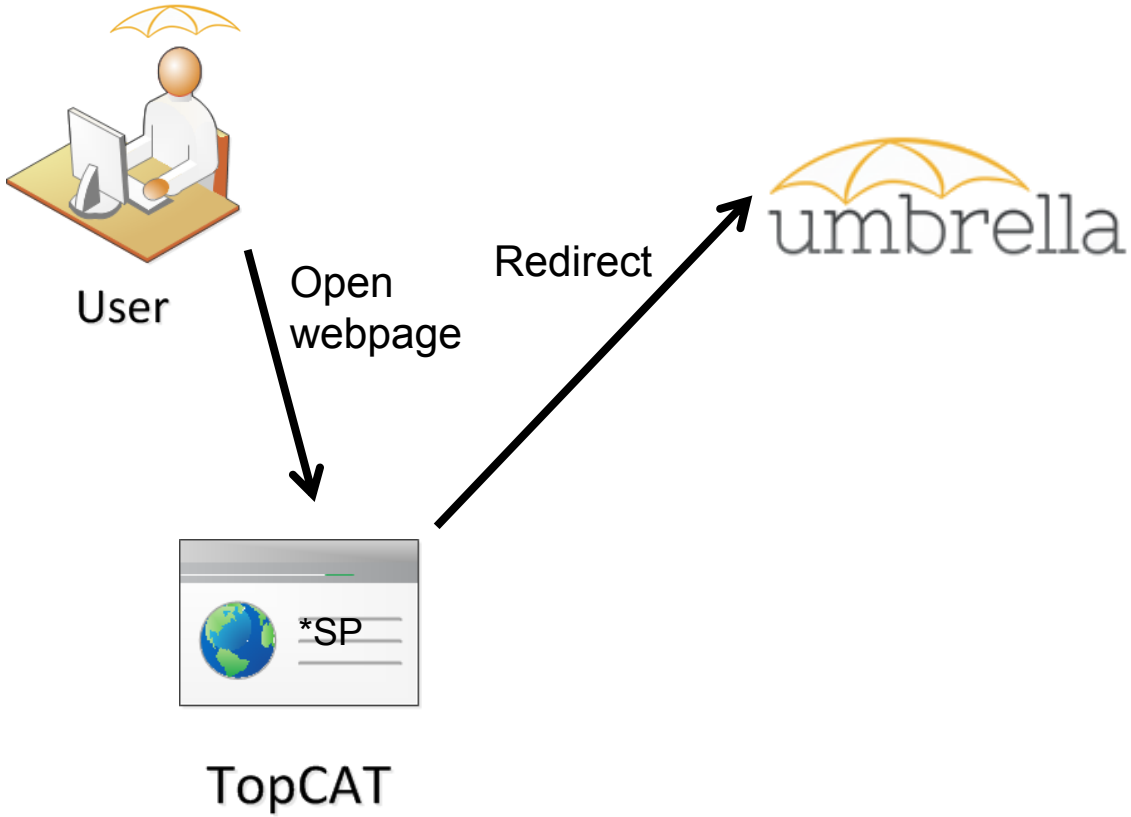


User Office

*SP
ICAT

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

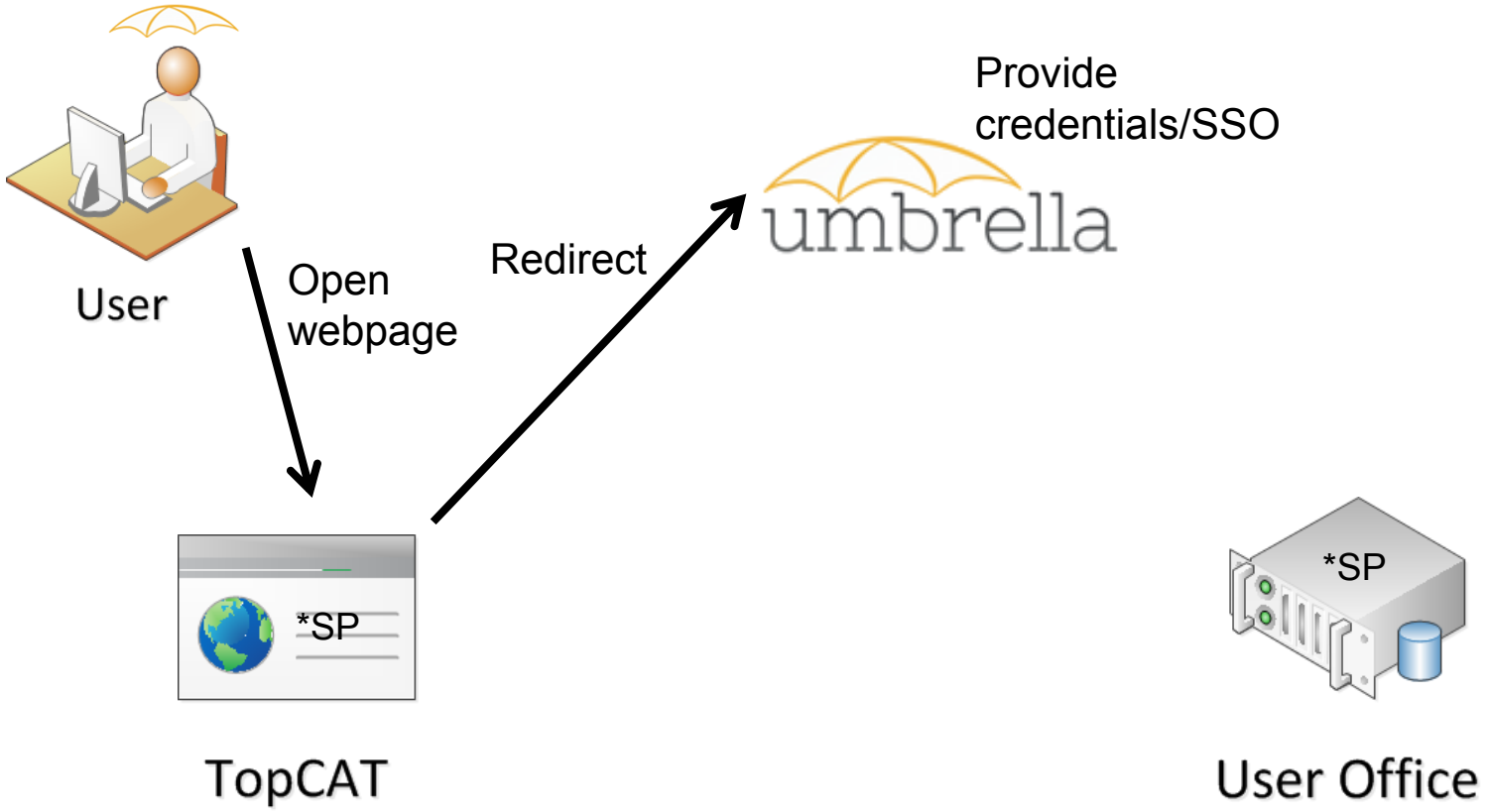
Real World - 'Pure' Shibboleth



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

*SP ICAT

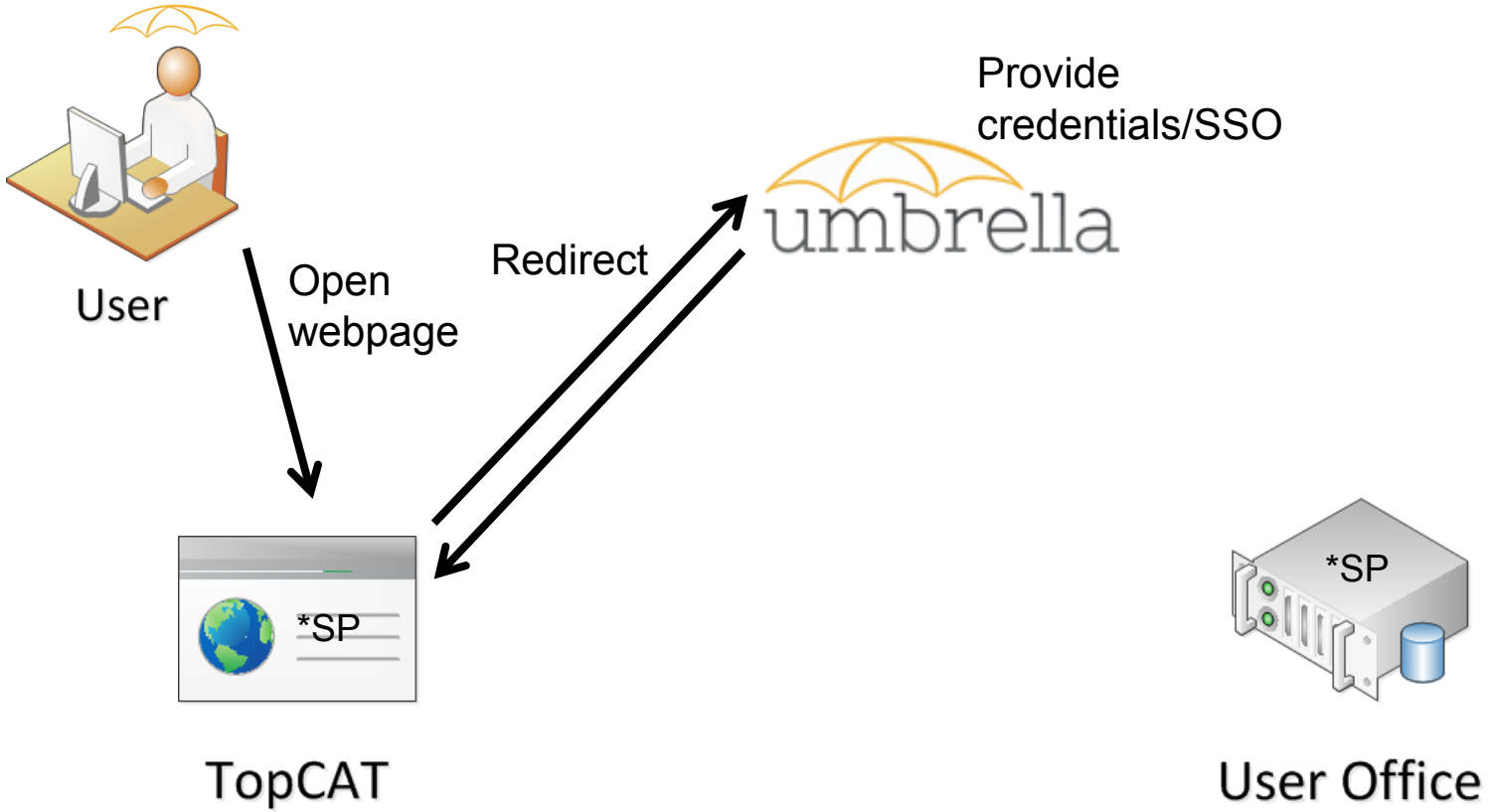
Real World - 'Pure' Shibboleth



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

*SP
ICAT

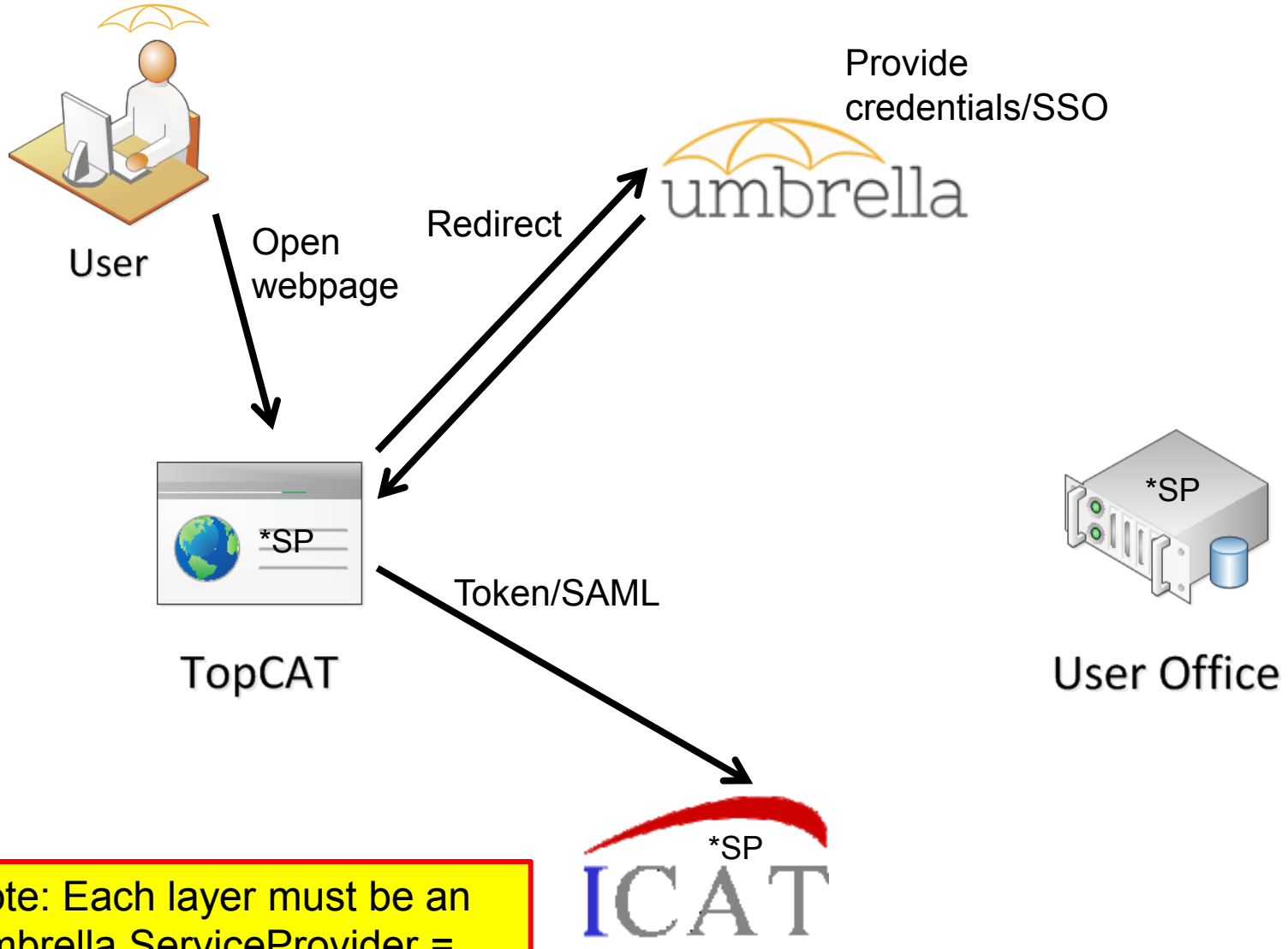
Real World - 'Pure' Shibboleth



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

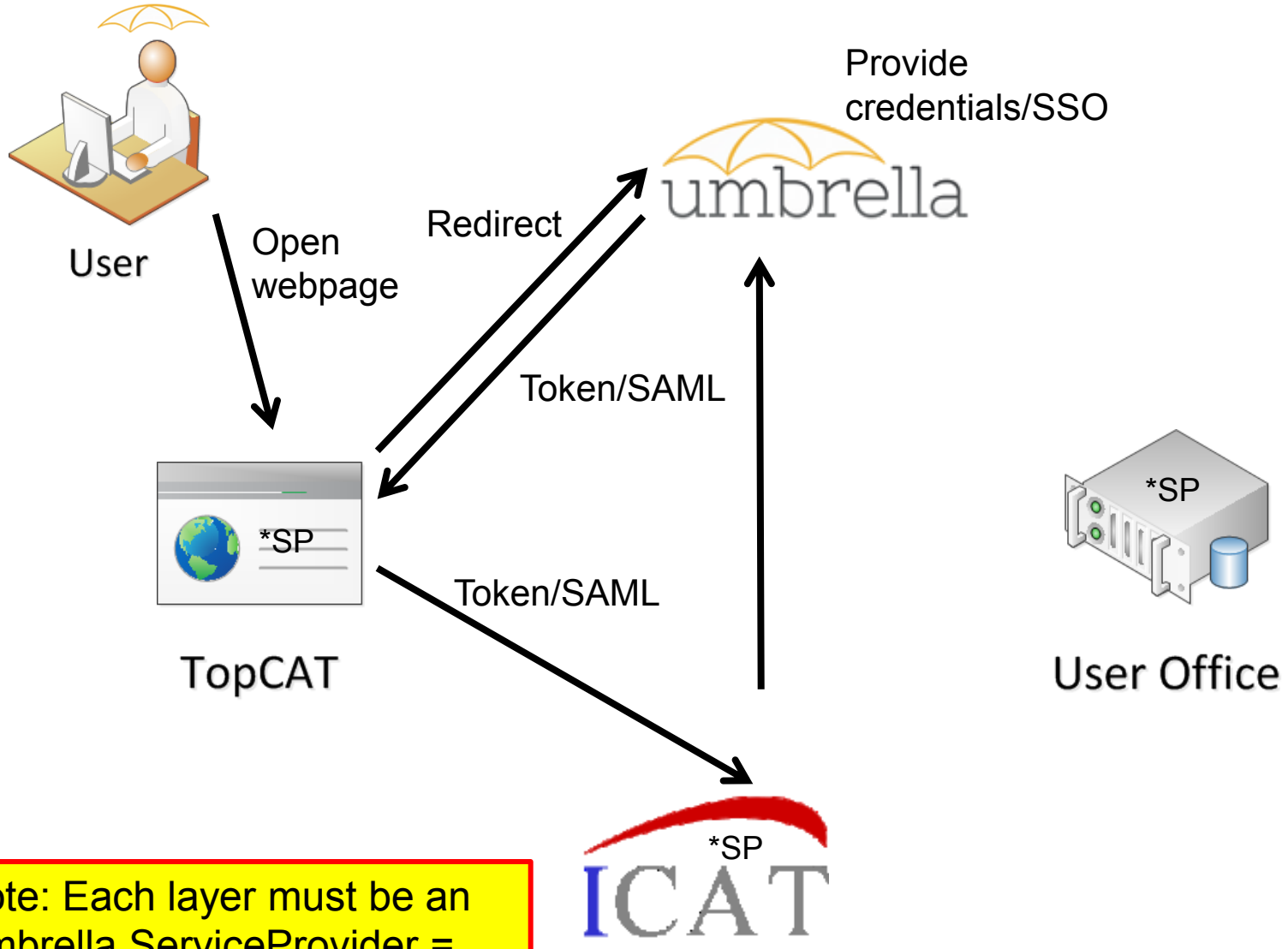
*SP
ICAT

Real World - 'Pure' Shibboleth



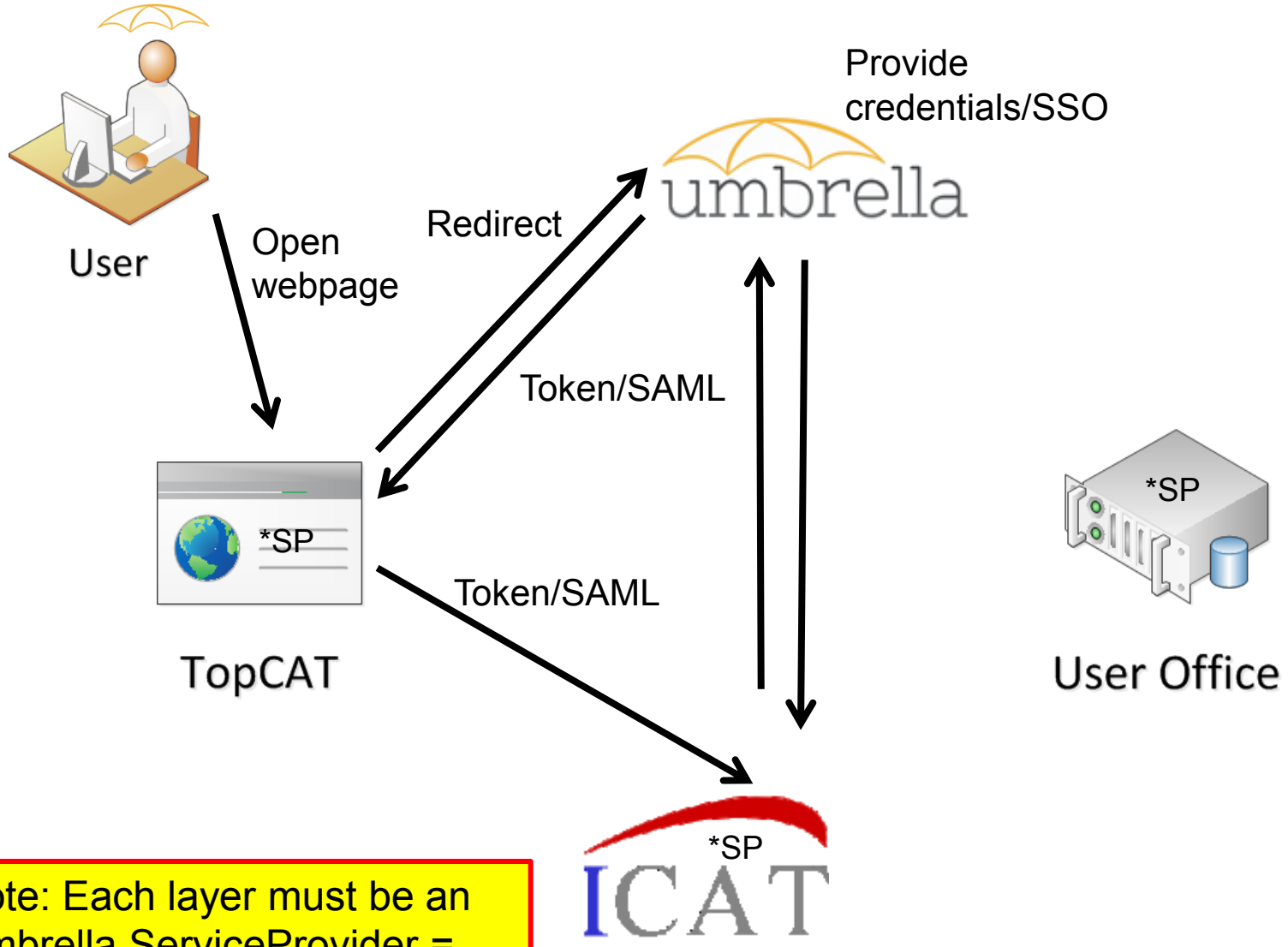
Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

Real World - 'Pure' Shibboleth



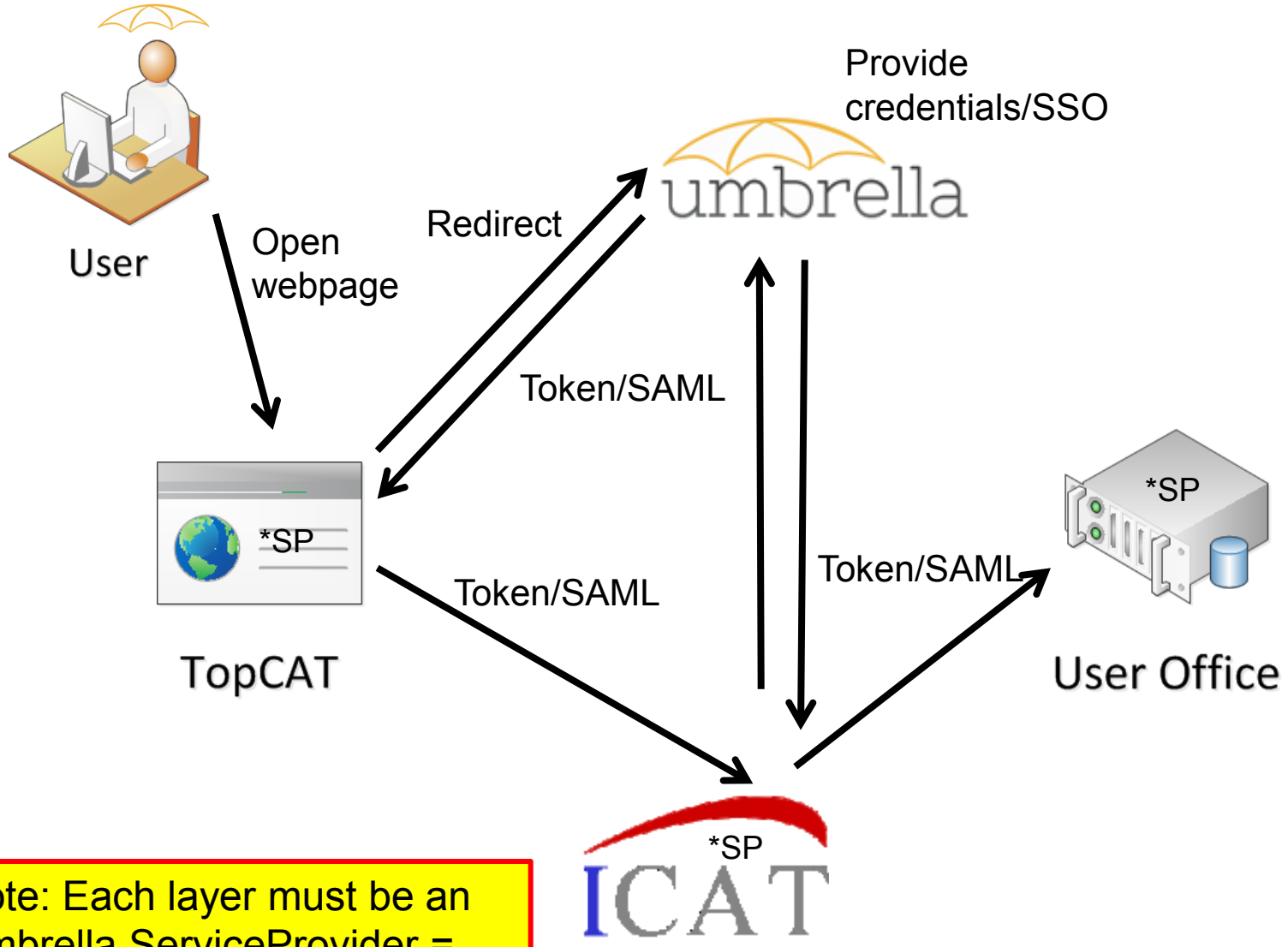
Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

Real World - 'Pure' Shibboleth



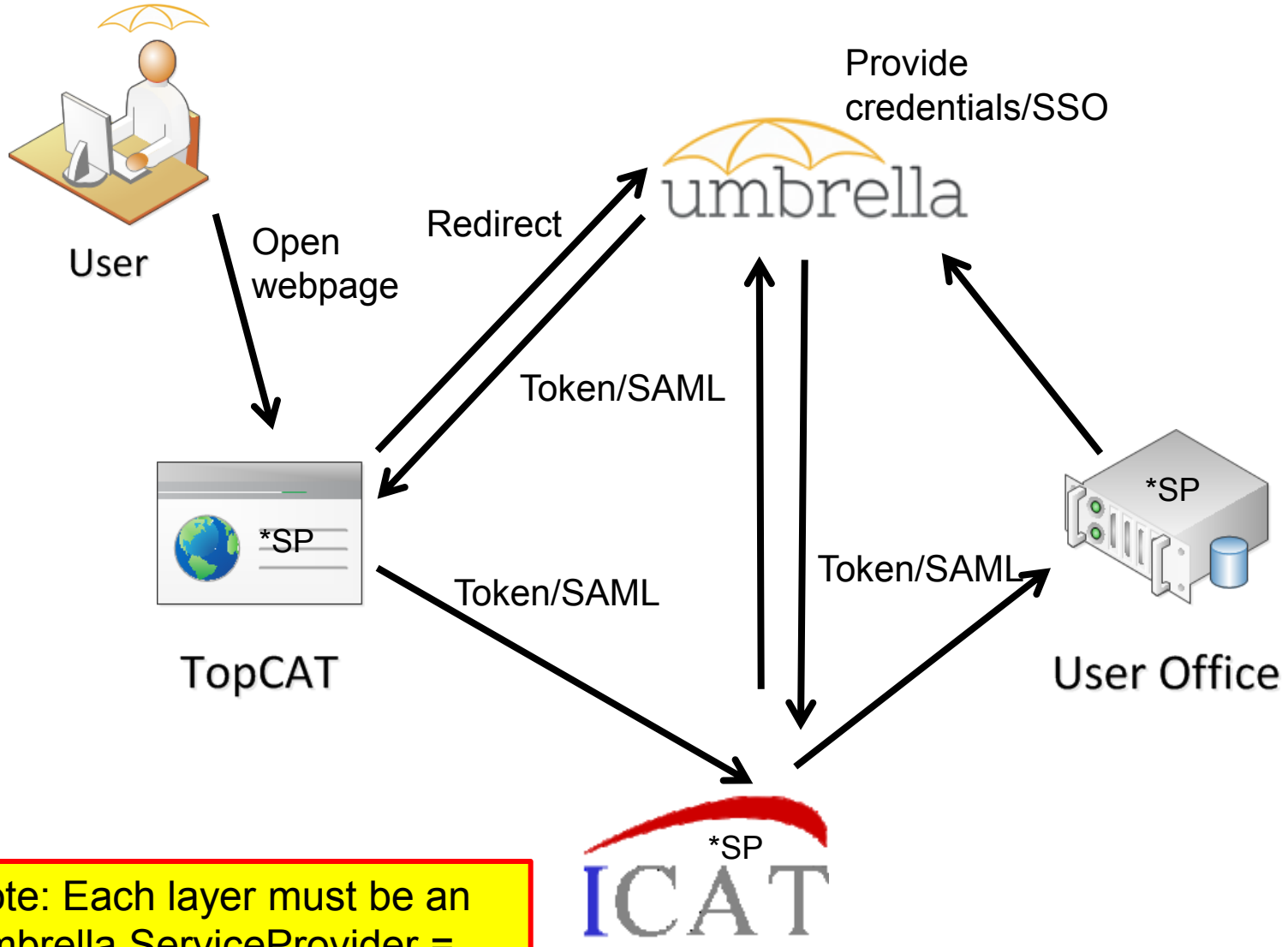
Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

Real World - 'Pure' Shibboleth



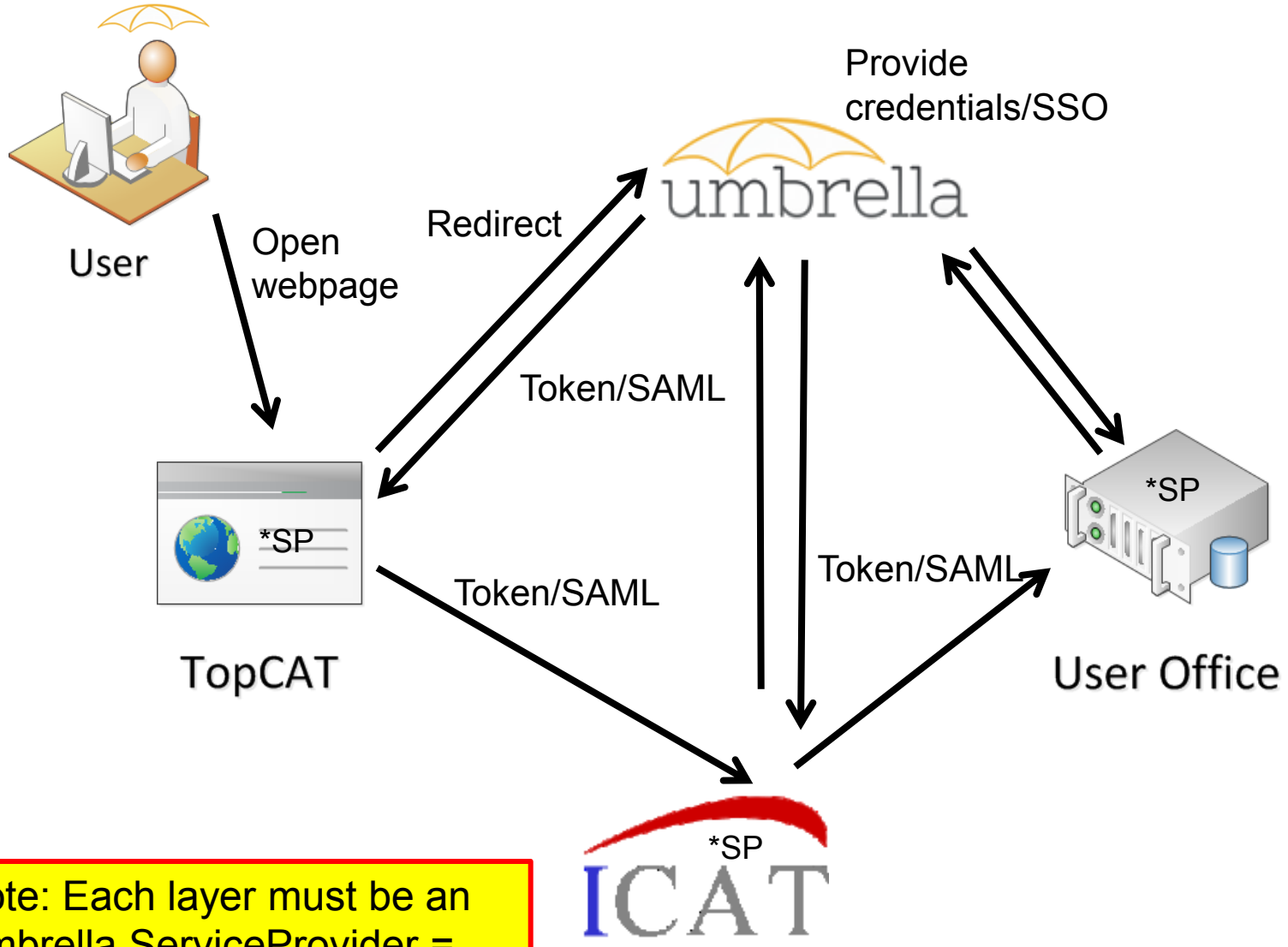
Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

Real World - 'Pure' Shibboleth



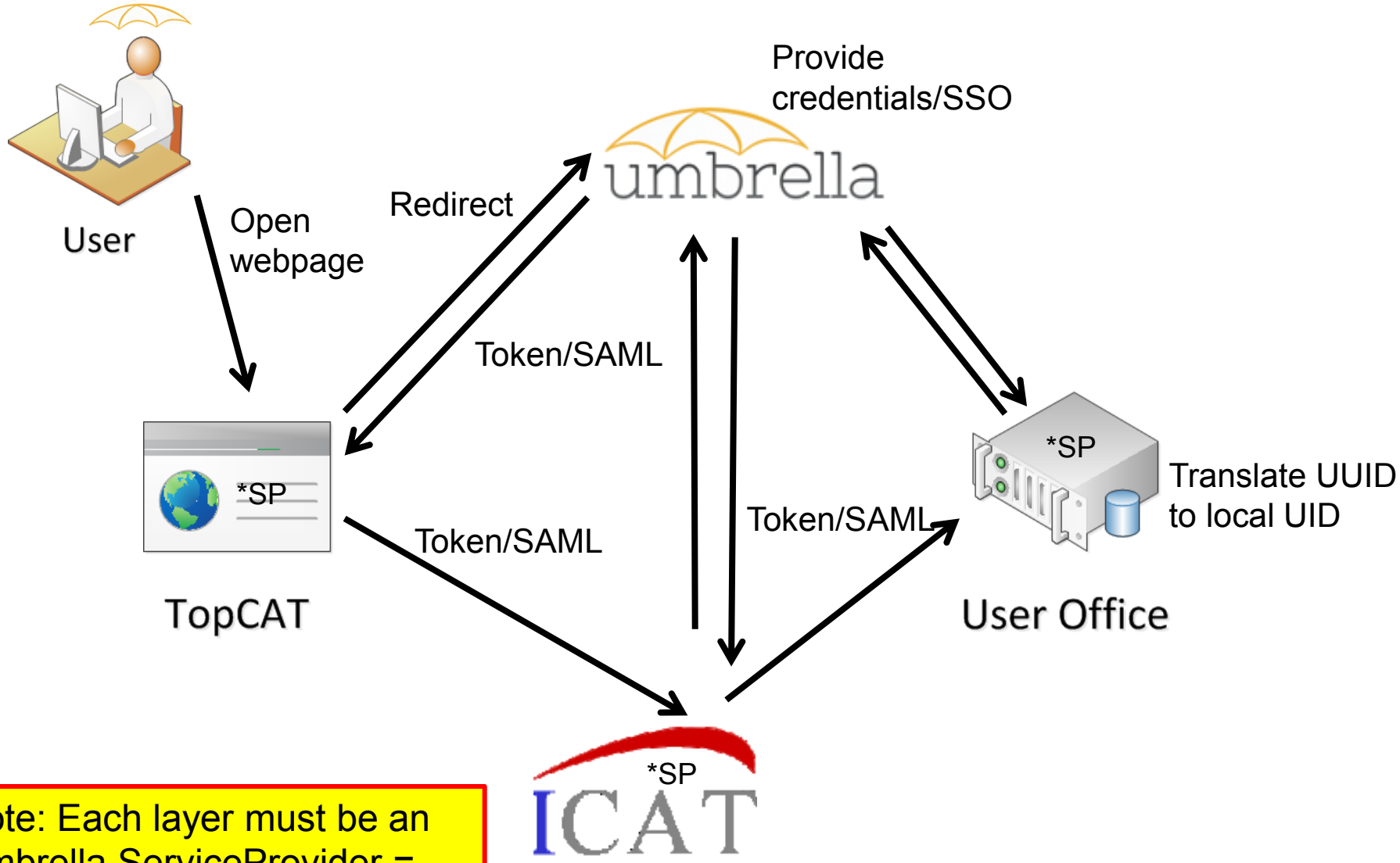
Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

Real World - 'Pure' Shibboleth



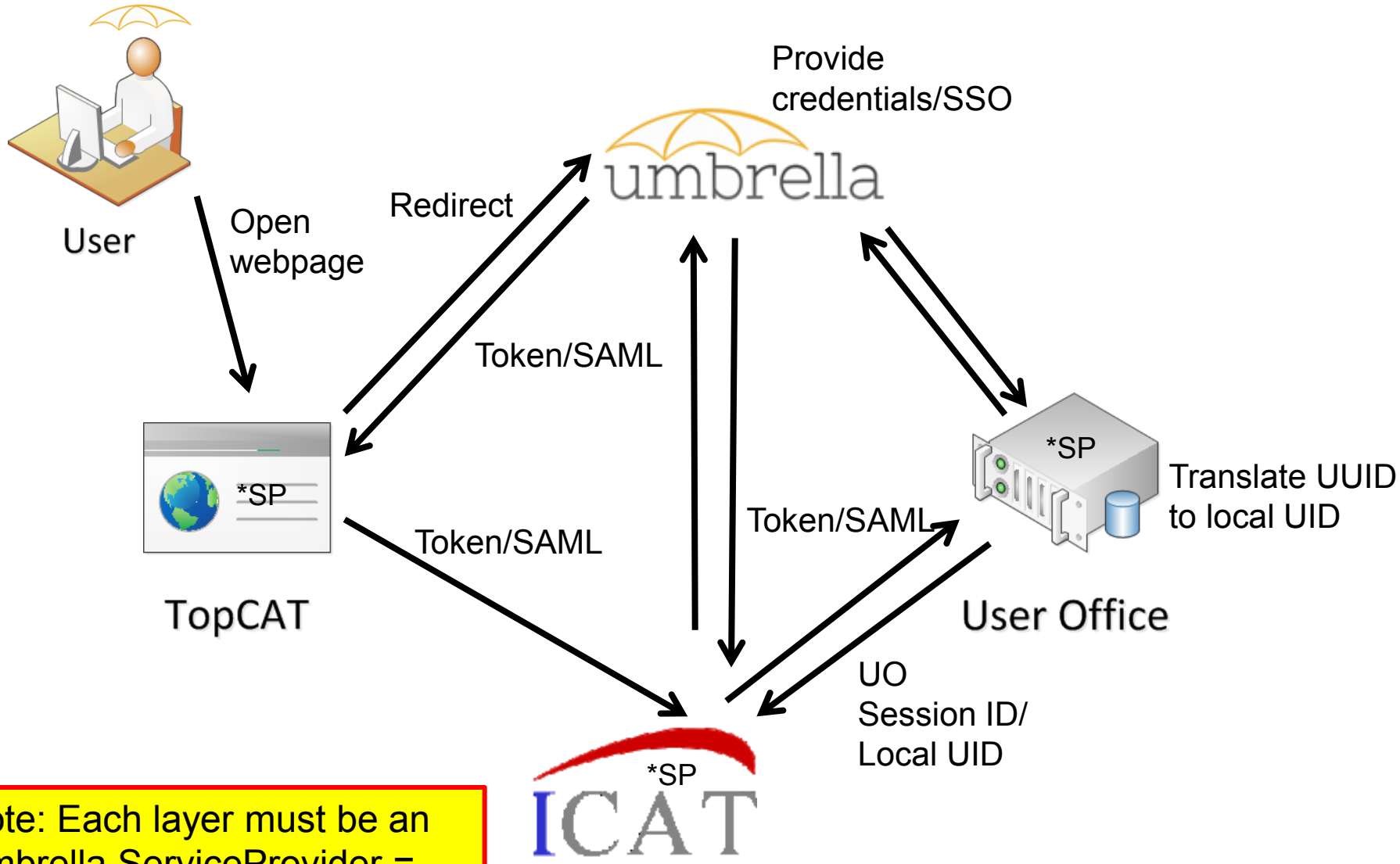
Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

Real World - 'Pure' Shibboleth



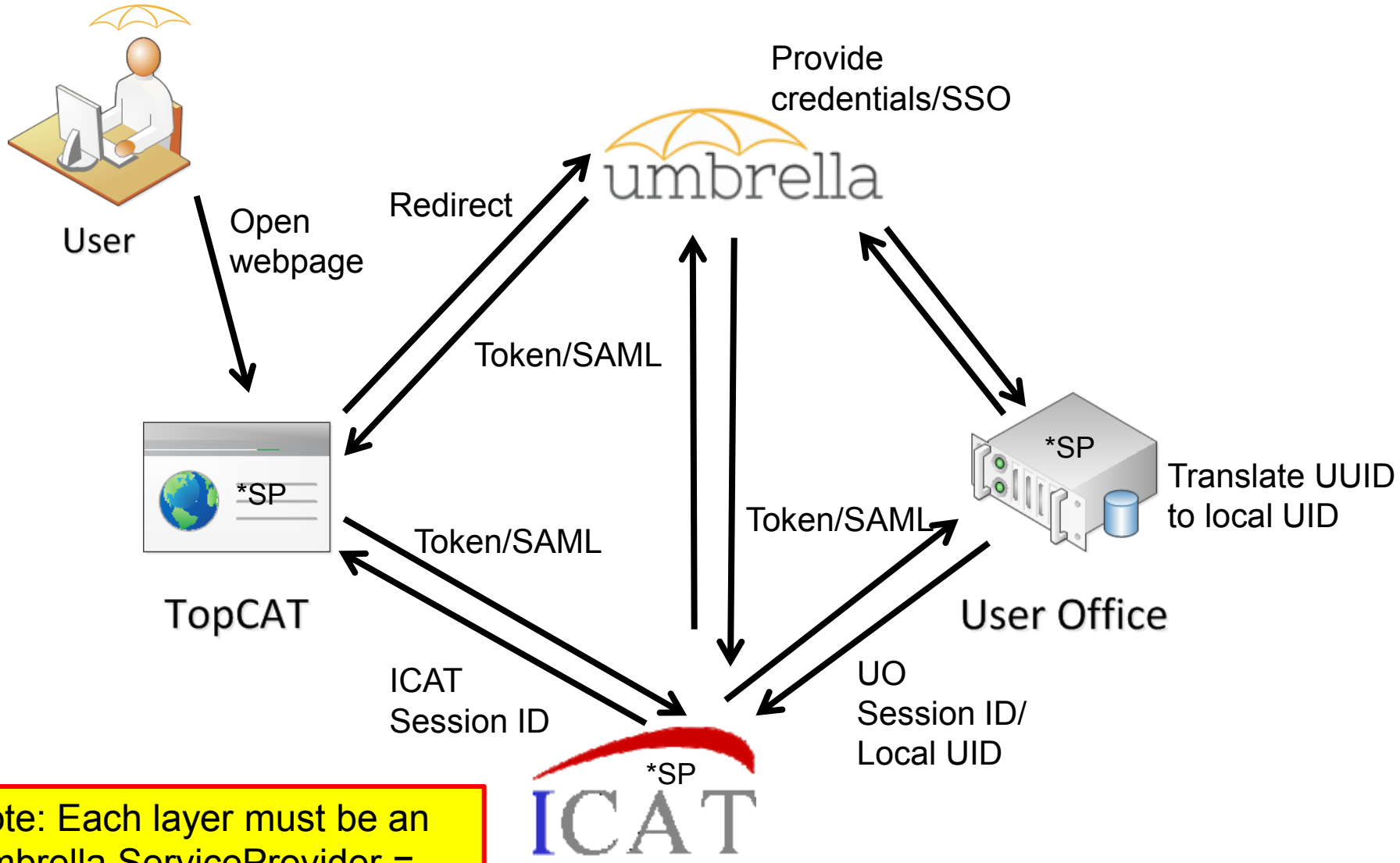
Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

Real World - 'Pure' Shibboleth



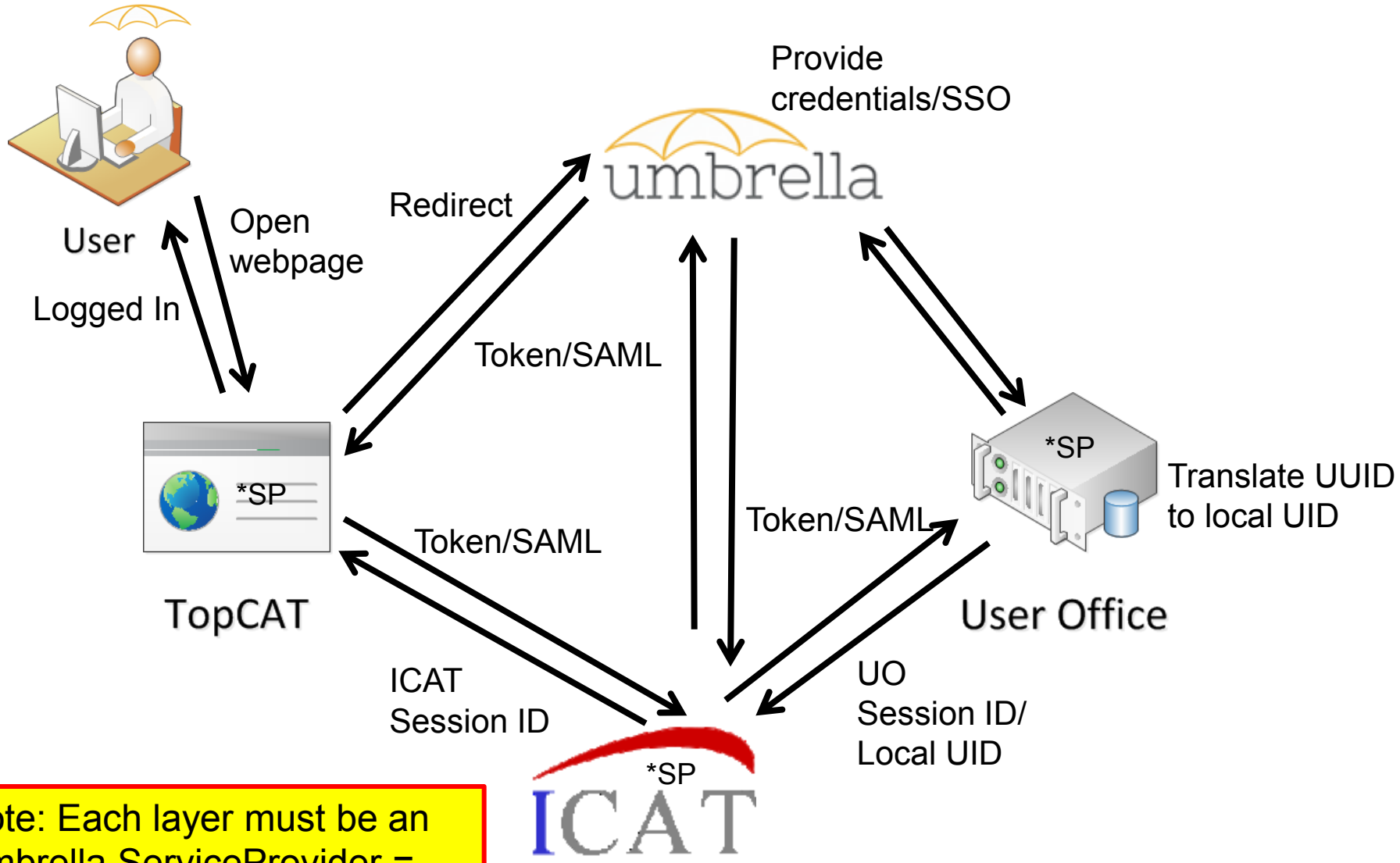
Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

Real World - 'Pure' Shibboleth



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

Real World - 'Pure' Shibboleth



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

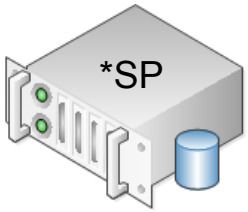
‘Pure’ Shibboleth + UO Portal

User

User Office Portal

umbrella

TopCAT



User Office

Only the user office layers needs to be Umbrella SPs

ICAT

‘Pure’ Shibboleth + UO Portal

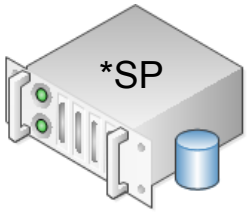
User

Open webpage

User Office Portal

umbrella

TopCAT



User Office

Only the user office layers needs to be Umbrella SPs

ICAT

‘Pure’ Shibboleth + UO Portal

User

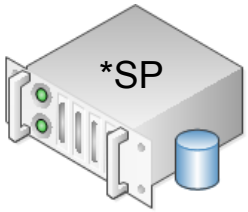
Open webpage

Redirect

User Office Portal

umbrella

TopCAT

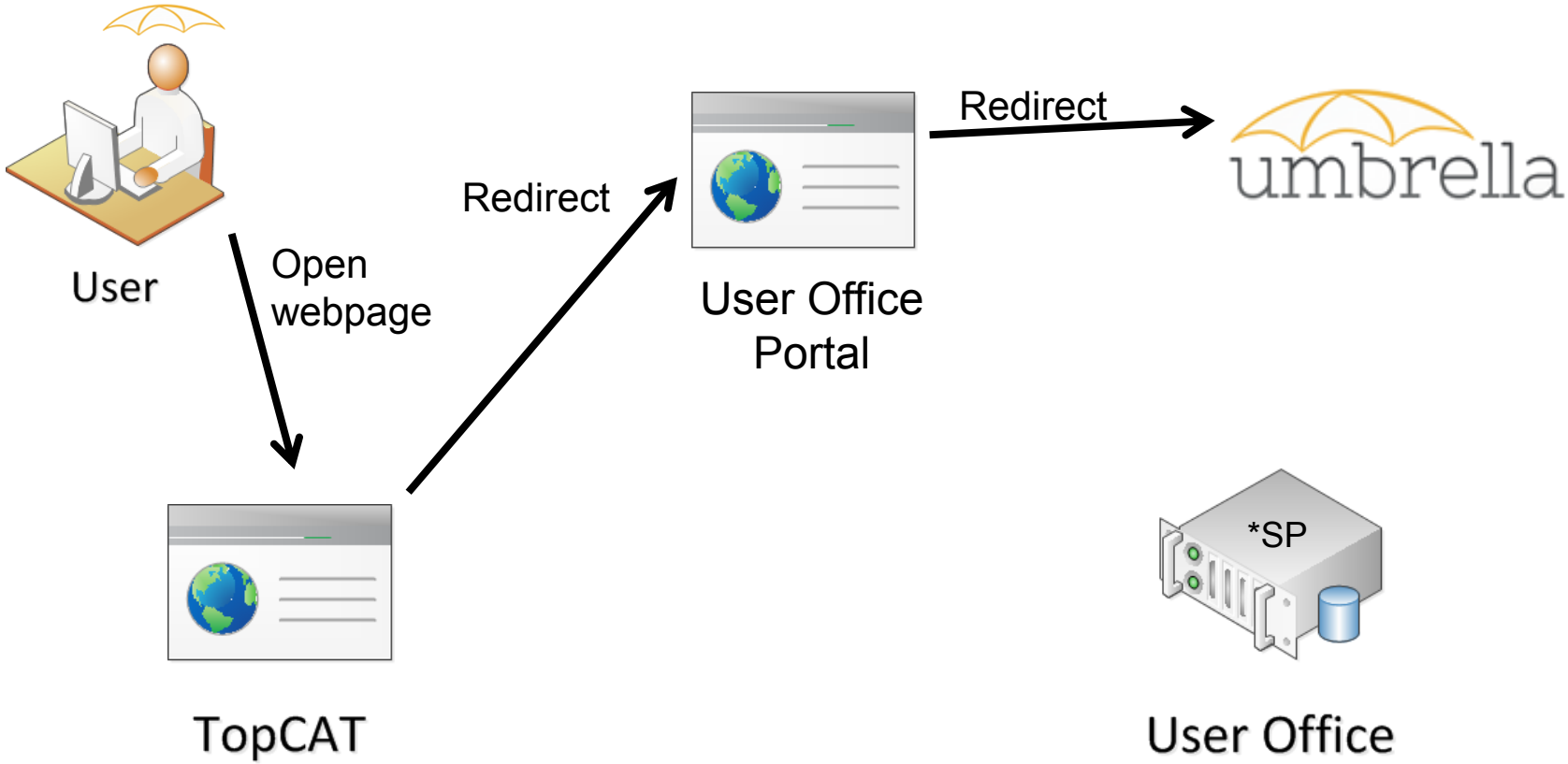


User Office

Only the user office layers needs to be Umbrella SPs

ICAT

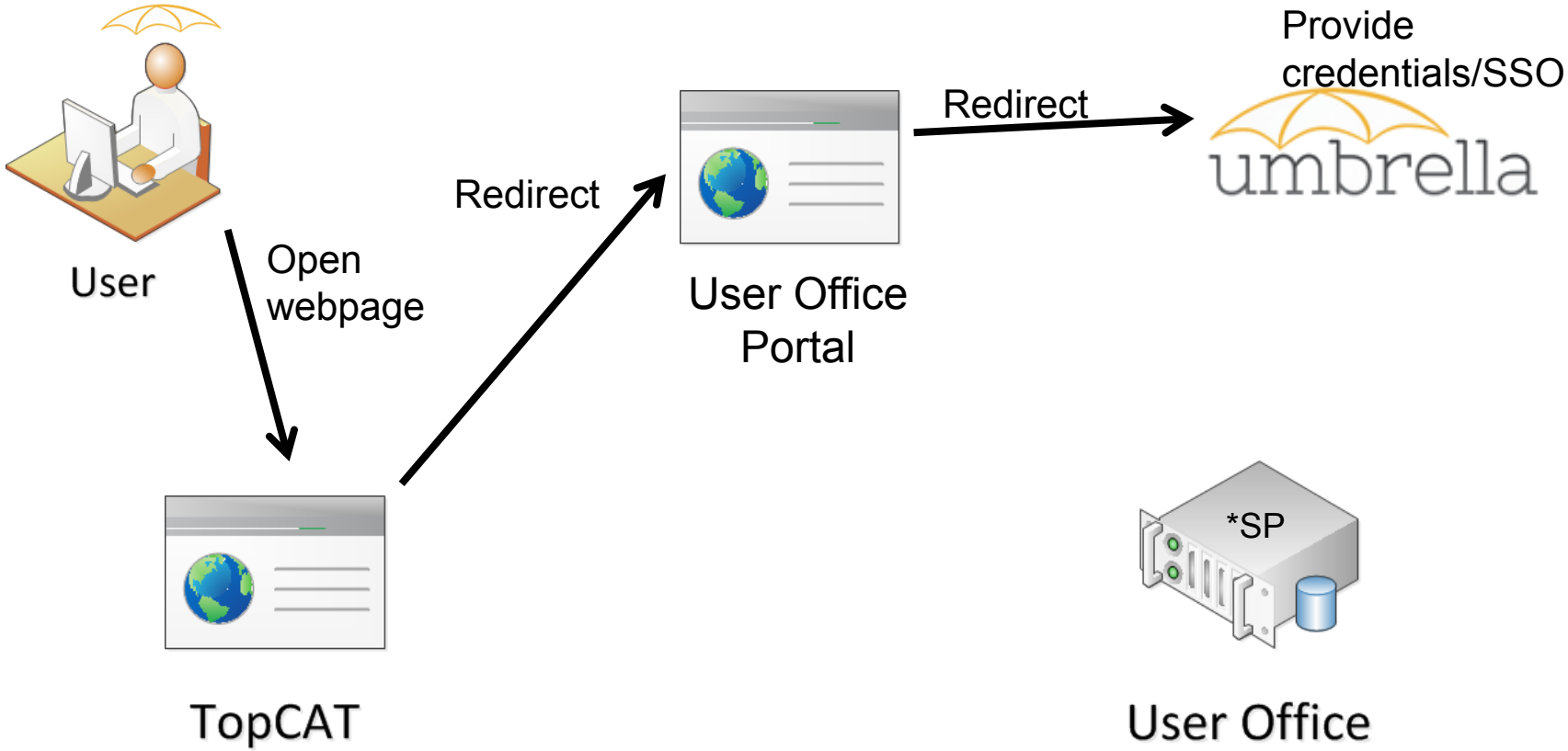
‘Pure’ Shibboleth + UO Portal



Only the user office layers needs to be Umbrella SPs

ICAT

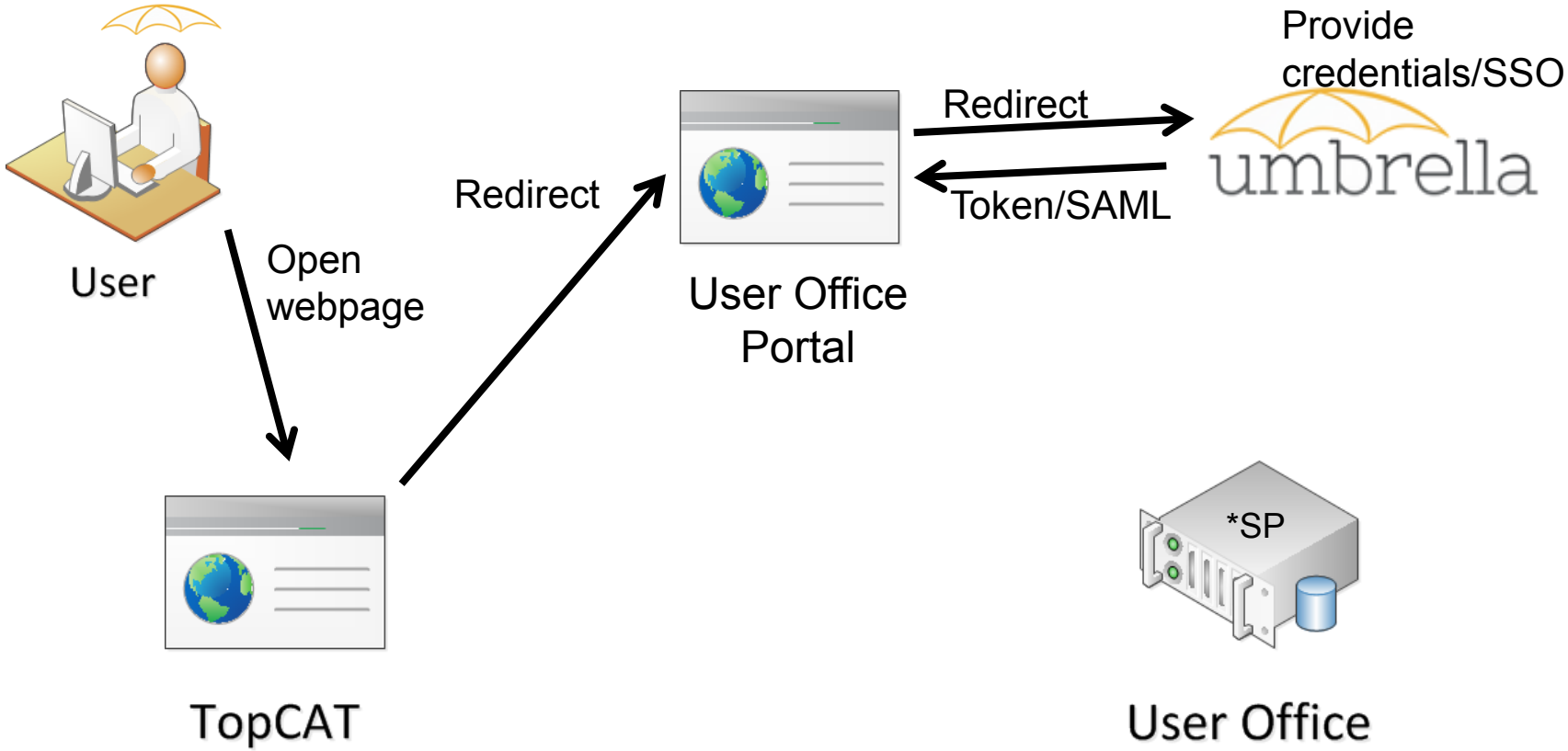
‘Pure’ Shibboleth + UO Portal



Only the user office layers needs to be Umbrella SPs

ICAT

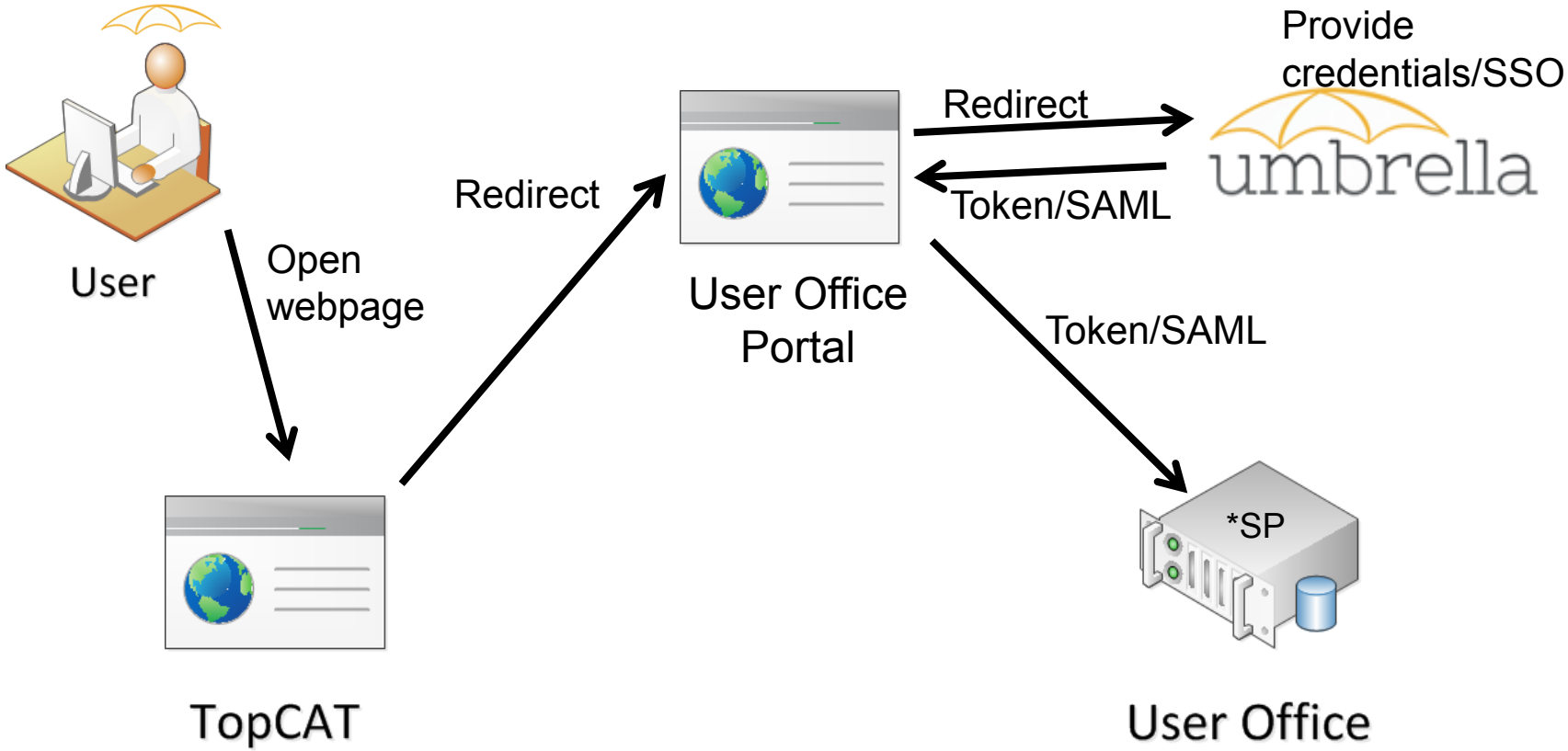
‘Pure’ Shibboleth + UO Portal



Only the user office layers needs to be Umbrella SPs

ICAT

‘Pure’ Shibboleth + UO Portal



Only the user office layers needs to be Umbrella SPs

ICAT

‘Pure’ Shibboleth + UO Portal

User

Open webpage

TopCAT

Redirect

User Office Portal

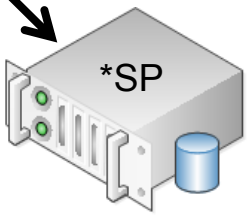
Redirect

Token/SAML

Provide credentials/SSO

umbrella

Token/SAML



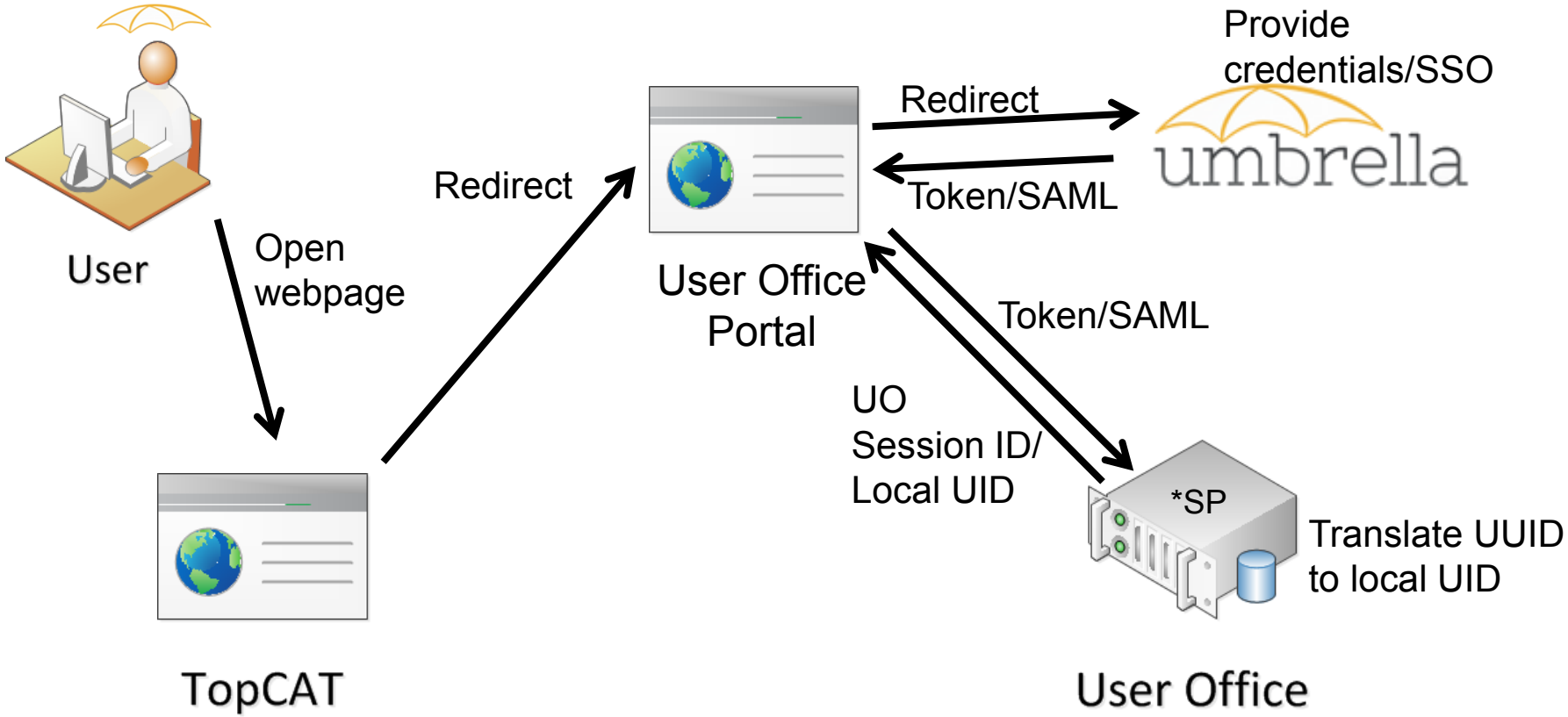
Translate UUID to local UID

User Office

Only the user office layers needs to be Umbrella SPs

ICAT

‘Pure’ Shibboleth + UO Portal



Only the user office layers needs to be Umbrella SPs

ICAT

‘Pure’ Shibboleth + UO Portal

User

Open webpage

TopCAT

Redirect

User Office Portal

Redirect

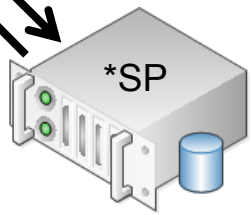
Provide credentials/SSO

Token/SAML

umbrella

Token/SAML

UO Session ID/ Local UID



Translate UUID to local UID

User Office

ICAT

Only the user office layers needs to be Umbrella SPs

‘Pure’ Shibboleth + UO Portal

User

Open webpage

TopCAT

Redirect

User Office Portal

Redirect

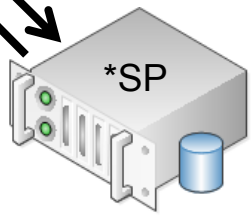
Provide credentials/SSO

Token/SAML

umbrella

Token/SAML

UO Session ID/ Local UID



Translate UUID to local UID

User Office

ICAT Session ID

ICAT

Only the user office layers needs to be Umbrella SPs

‘Pure’ Shibboleth + UO Portal

User

Open webpage

Redirect

User Office Portal

Redirect

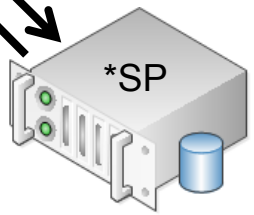
Token/SAML

Provide credentials/SSO

umbrella

Token/SAML

UO Session ID/ Local UID



Translate UUID to local UID

User Office

TopCAT

ICAT Session ID

ICAT

Only the user office layers needs to be Umbrella SPs

‘Pure’ Shibboleth + UO Portal

User

Logged In

Open webpage

TopCAT

Redirect

User Office Portal

Redirect

Token/SAML

Provide credentials/SSO

umbrella

Token/SAML

UO Session ID/ Local UID

*SP

Translate UUID to local UID

User Office

ICAT Session ID

ICAT

Only the user office layers needs to be Umbrella SPs

Real world –Umbrella – Many ICATs

User

umbrella

ISIS

*SP

ICAT

*SP

User Office

*SP

TopCAT

PSI

*SP

ICAT

*SP

User Office

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

umbrella

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

Real world –Umbrella – Many ICATs

User

Open webpage

TopCAT

umbrella

ISIS

*SP

ICAT

*SP

User Office

PSI

*SP

ICAT

*SP

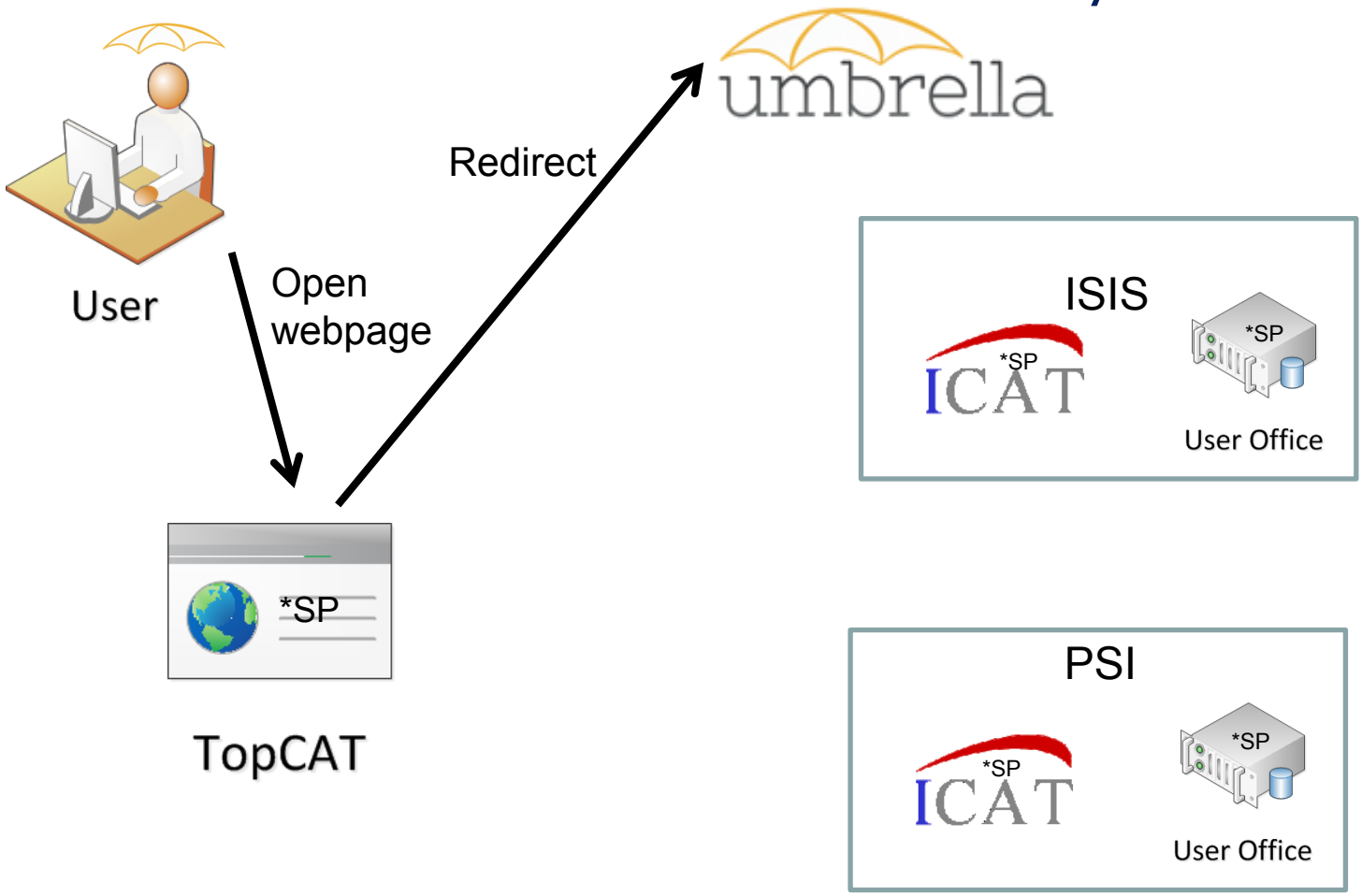
User Office

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

umbrella

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

Real world –Umbrella – Many ICATs

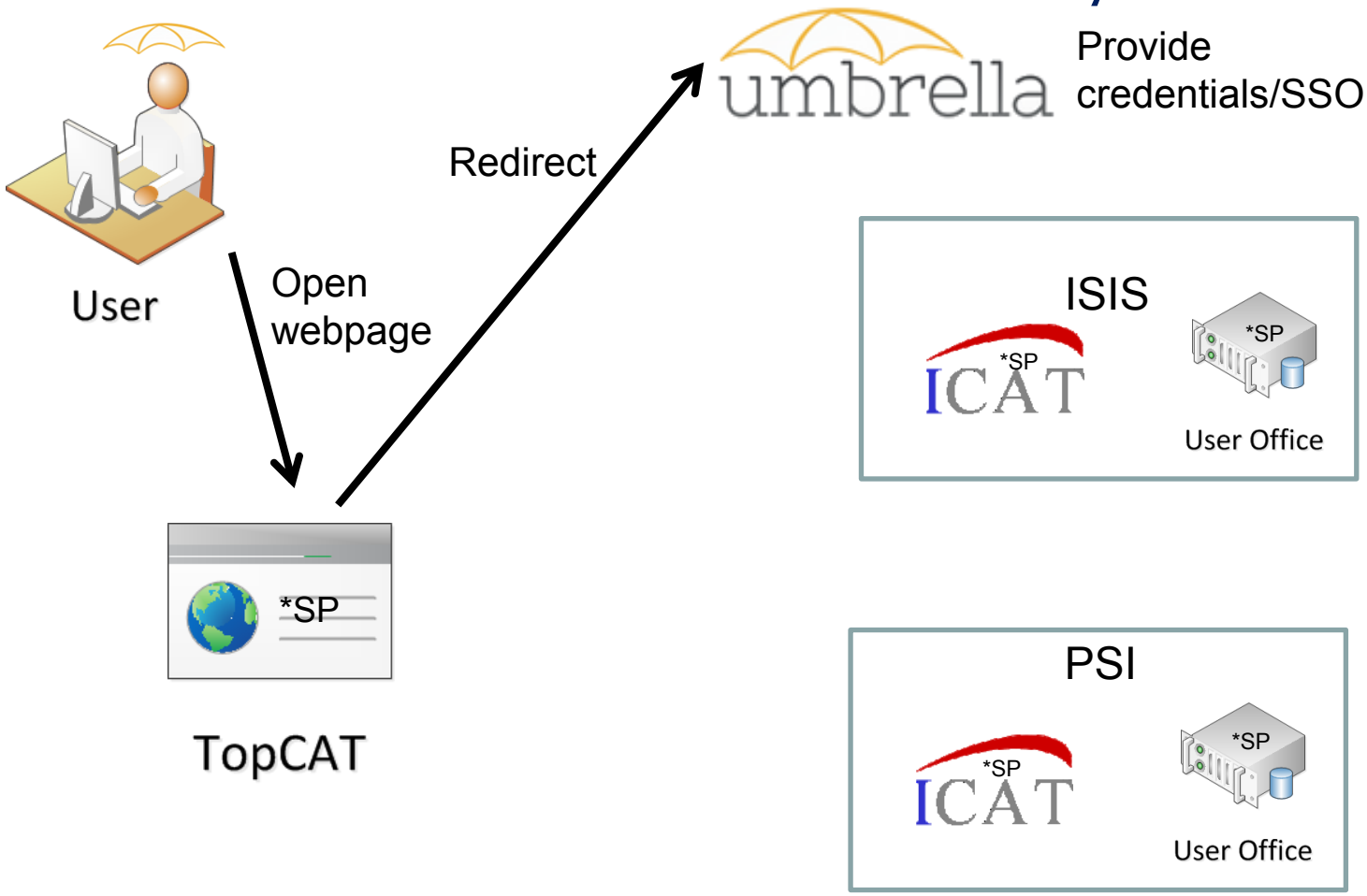


Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

umbrella

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

Real world –Umbrella – Many ICATs

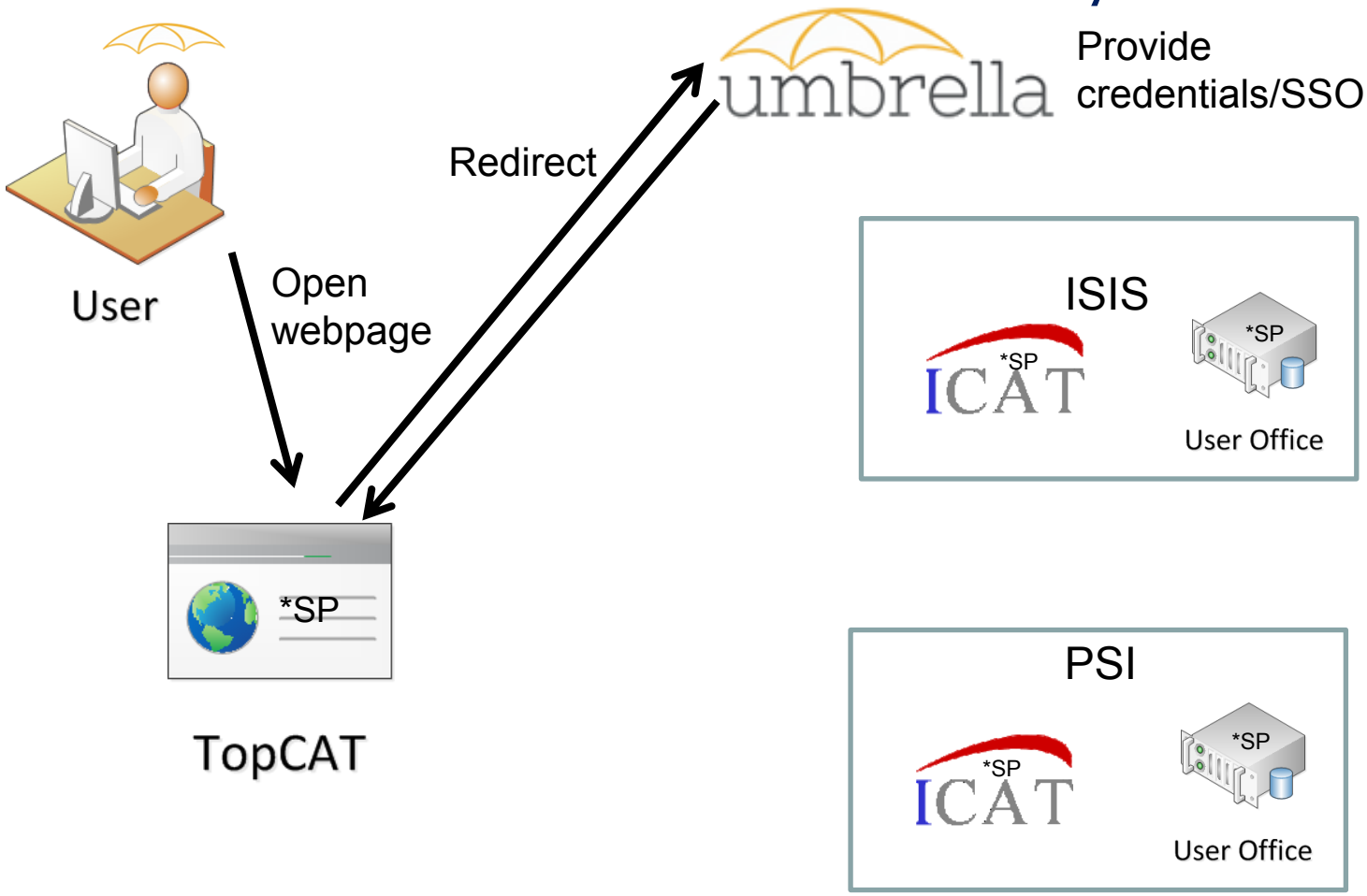


Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

umbrella

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

Real world –Umbrella – Many ICATs

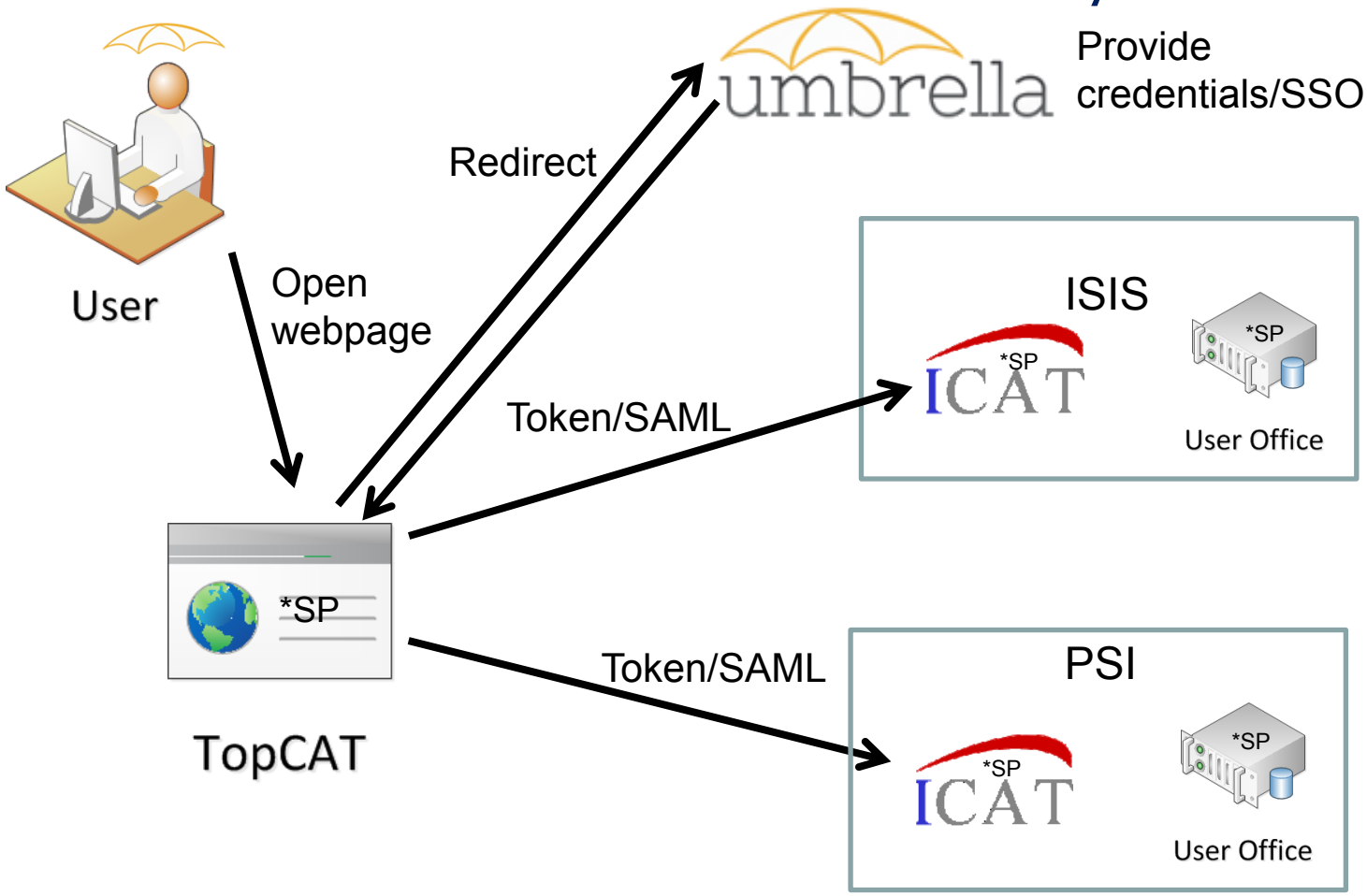


Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

umbrella

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

Real world –Umbrella – Many ICATs

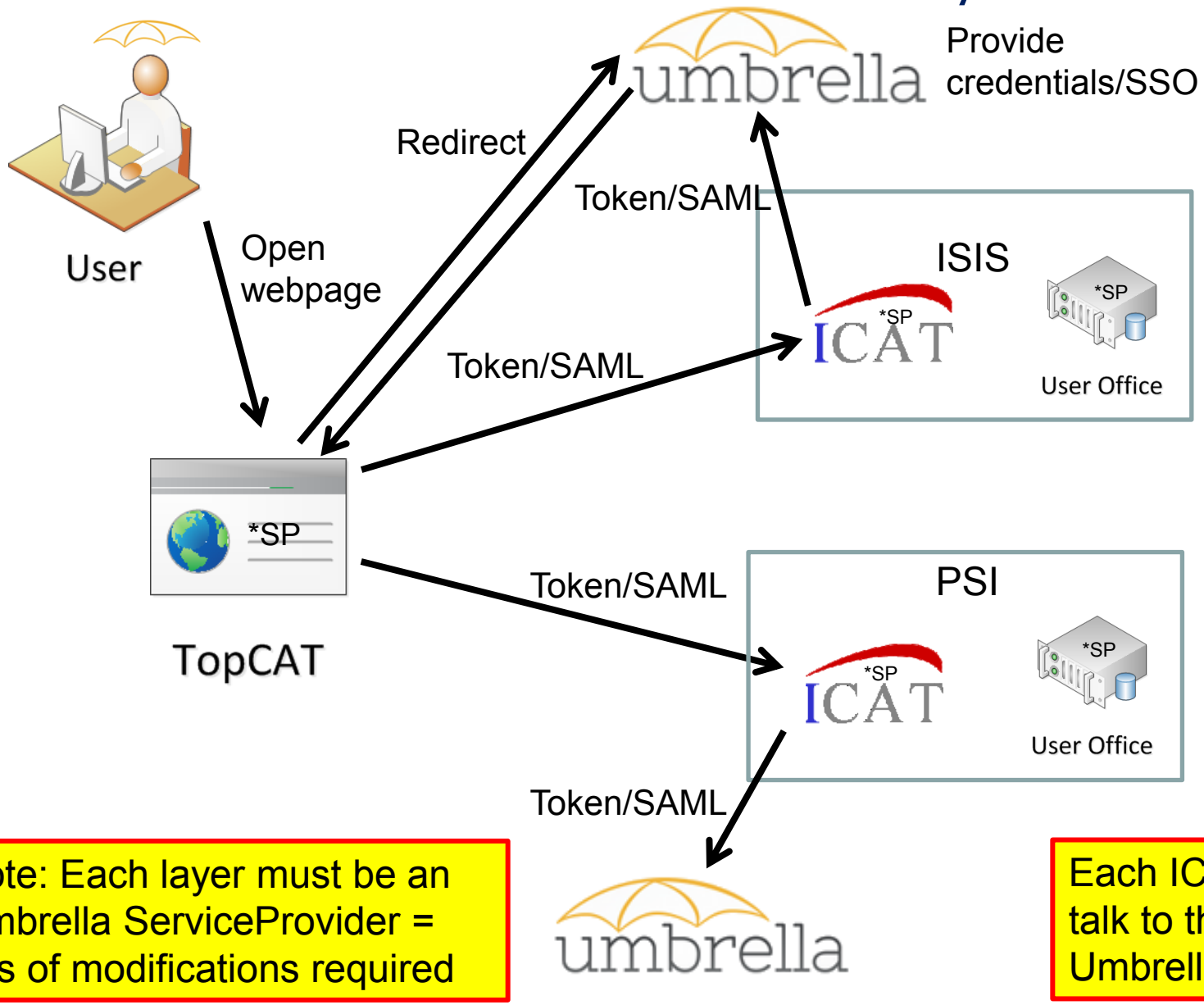


Note: Each layer must be an Umbrella ServiceProvider = lots of modifications required

umbrella

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

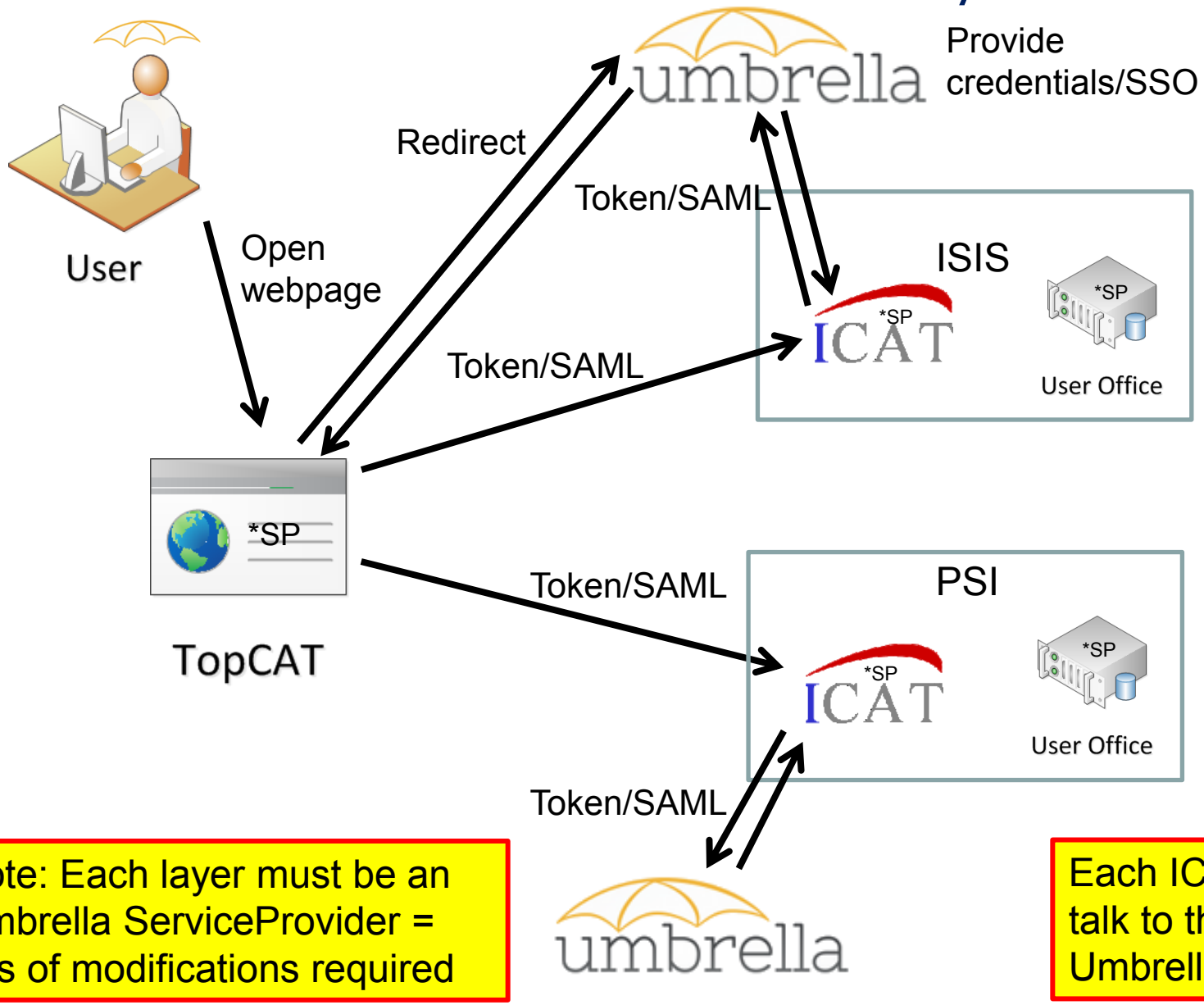
Real world –Umbrella – Many ICATs



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

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

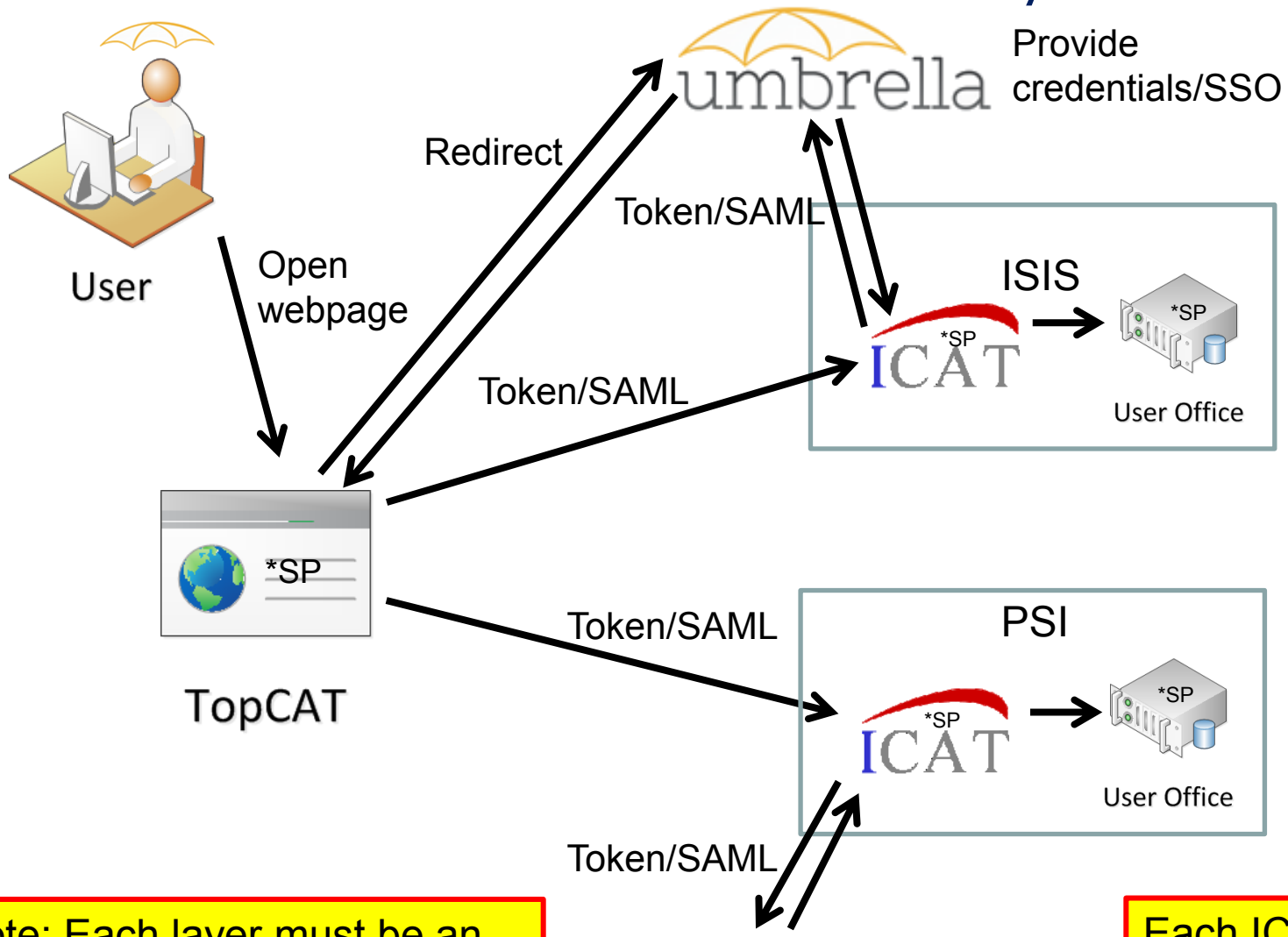
Real world –Umbrella – Many ICATs



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

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

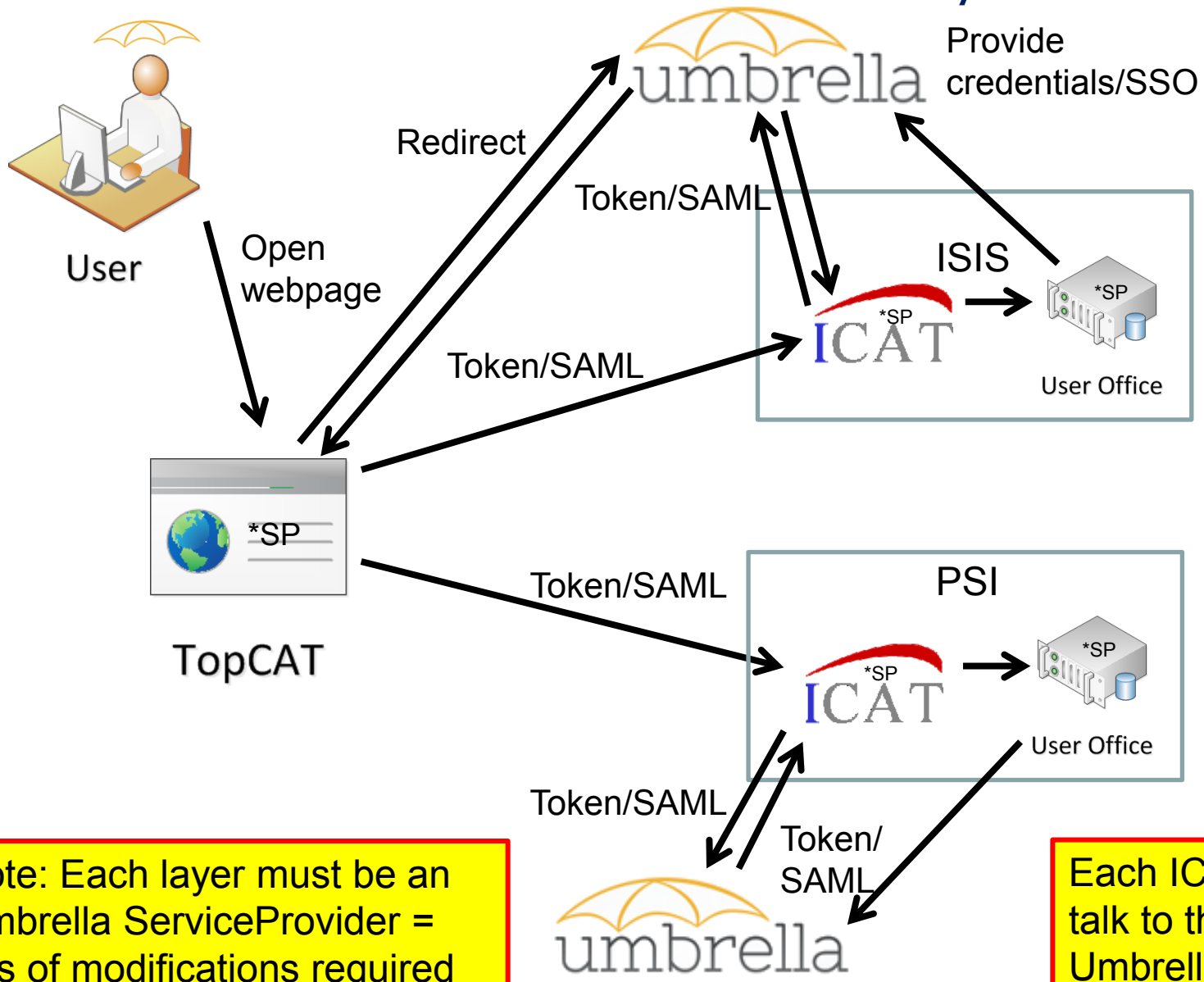
Real world –Umbrella – Many ICATs



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

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

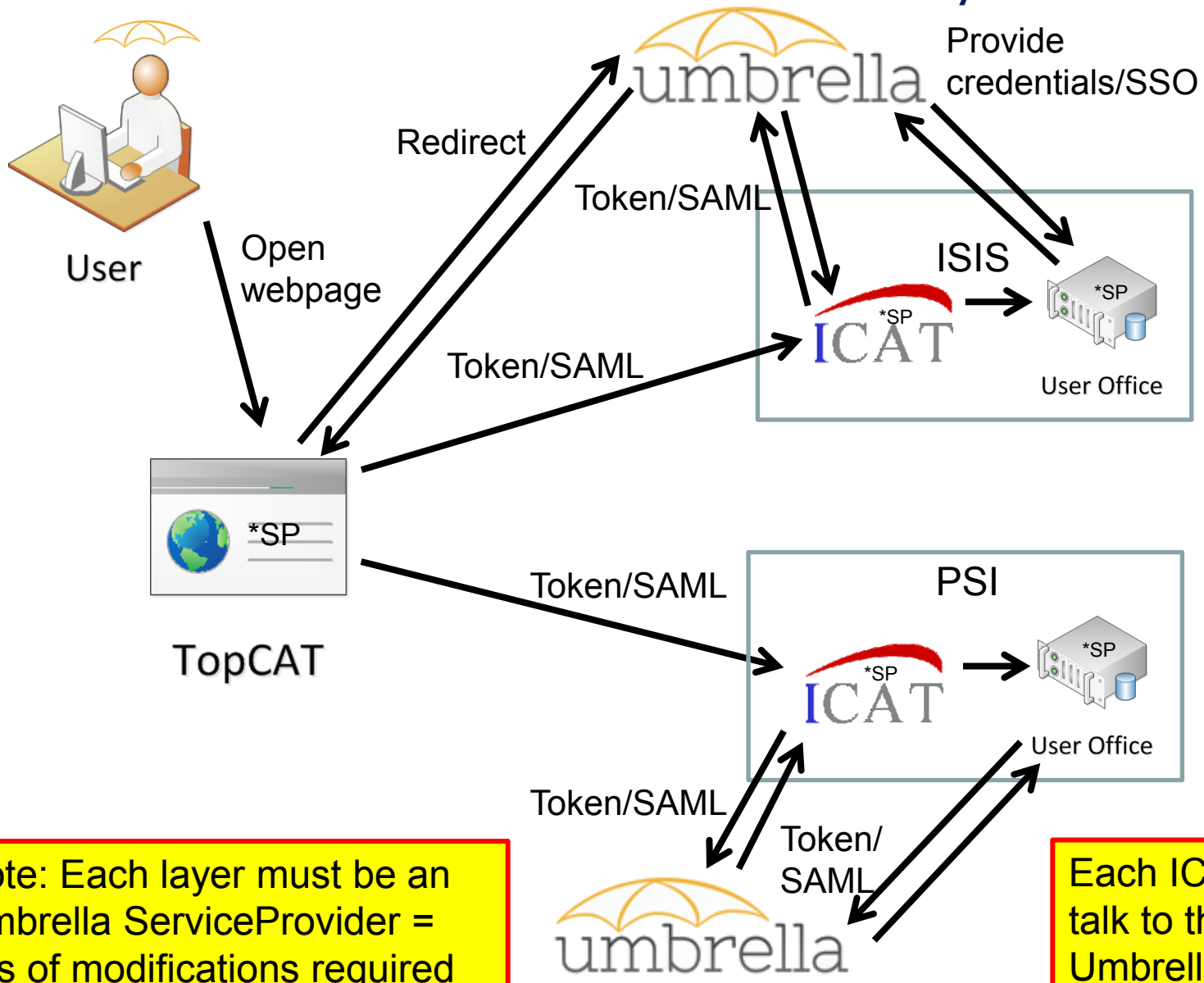
Real world –Umbrella – Many ICATs



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

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

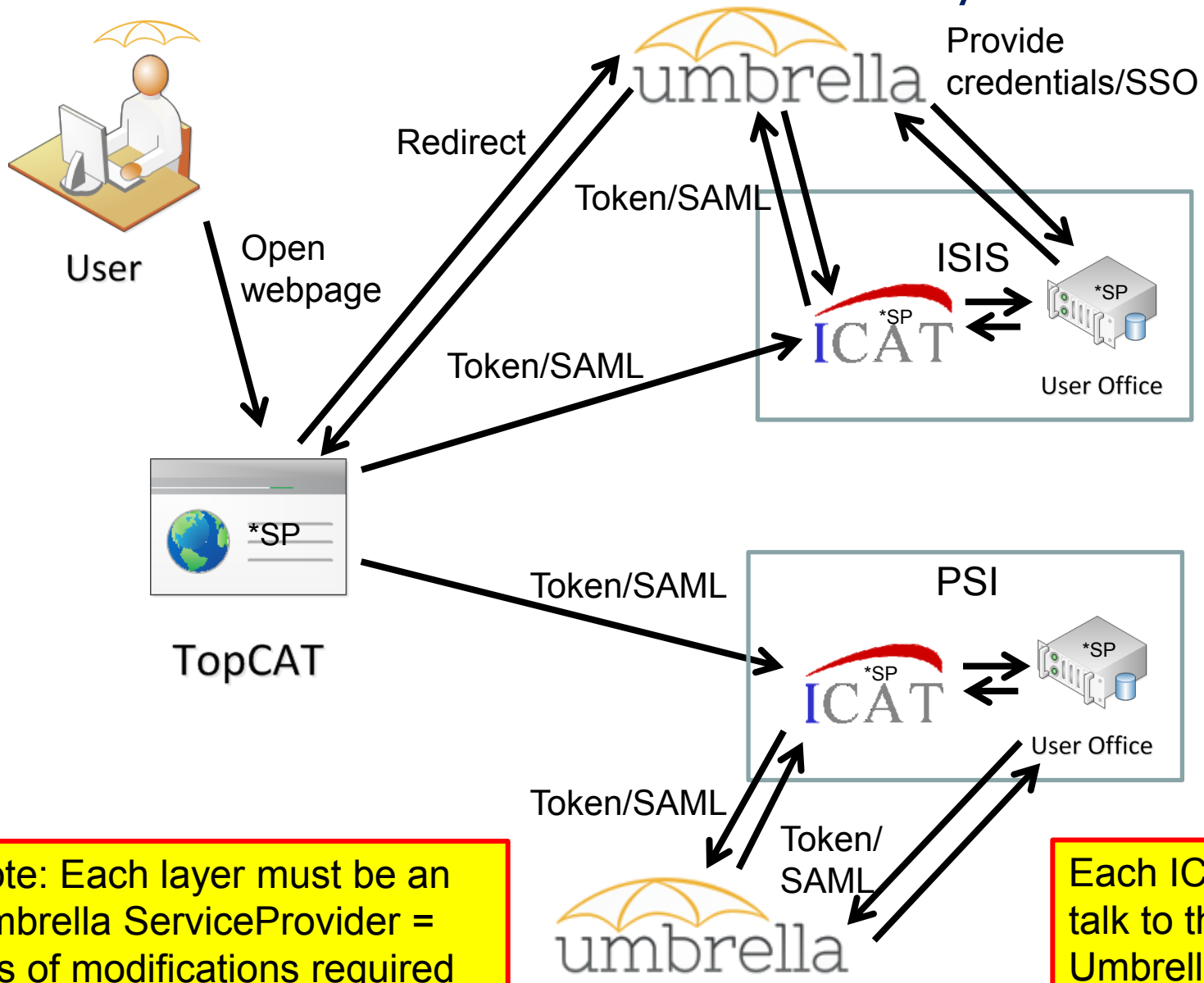
Real world –Umbrella – Many ICATs



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

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

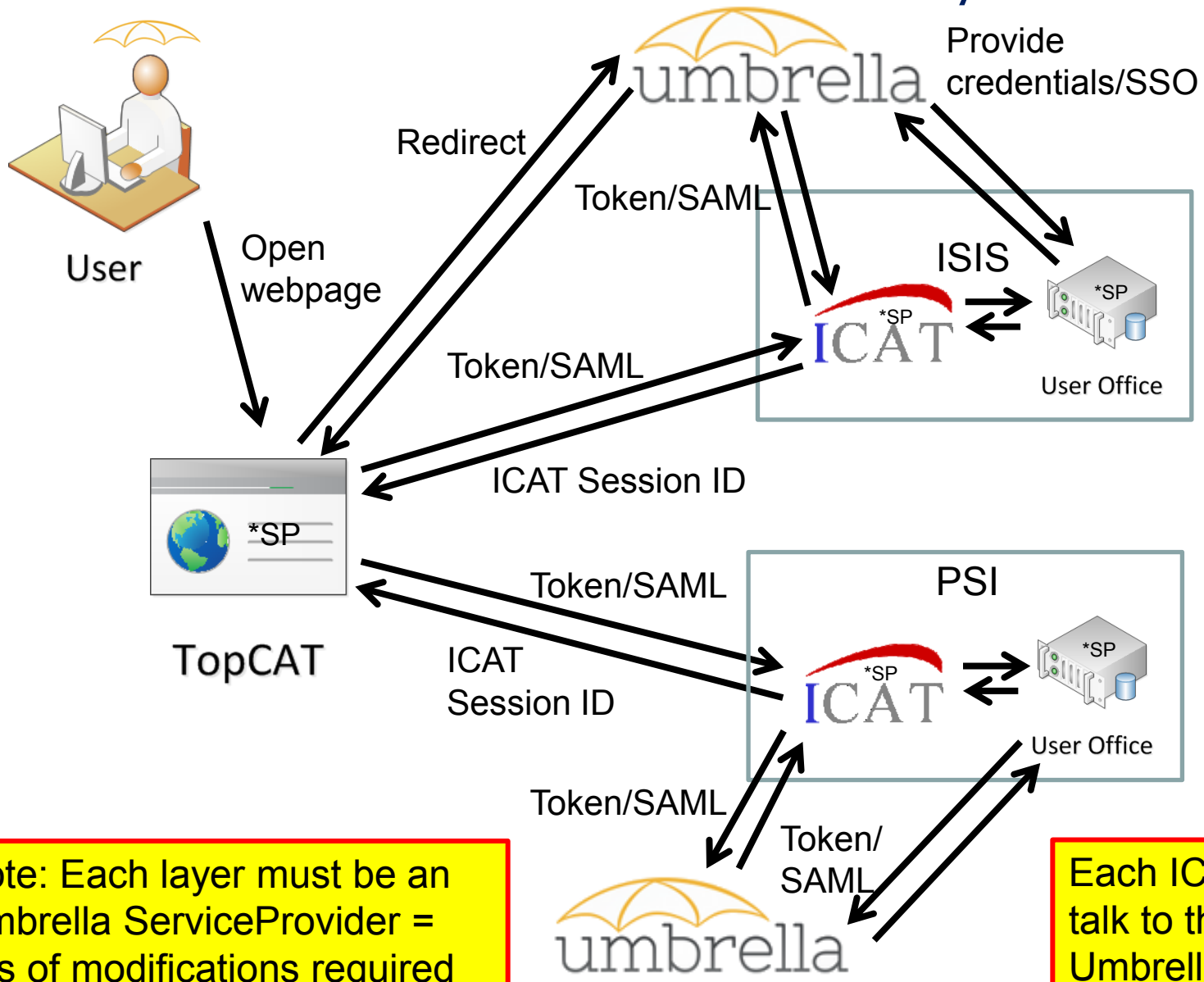
Real world –Umbrella – Many ICATs



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

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

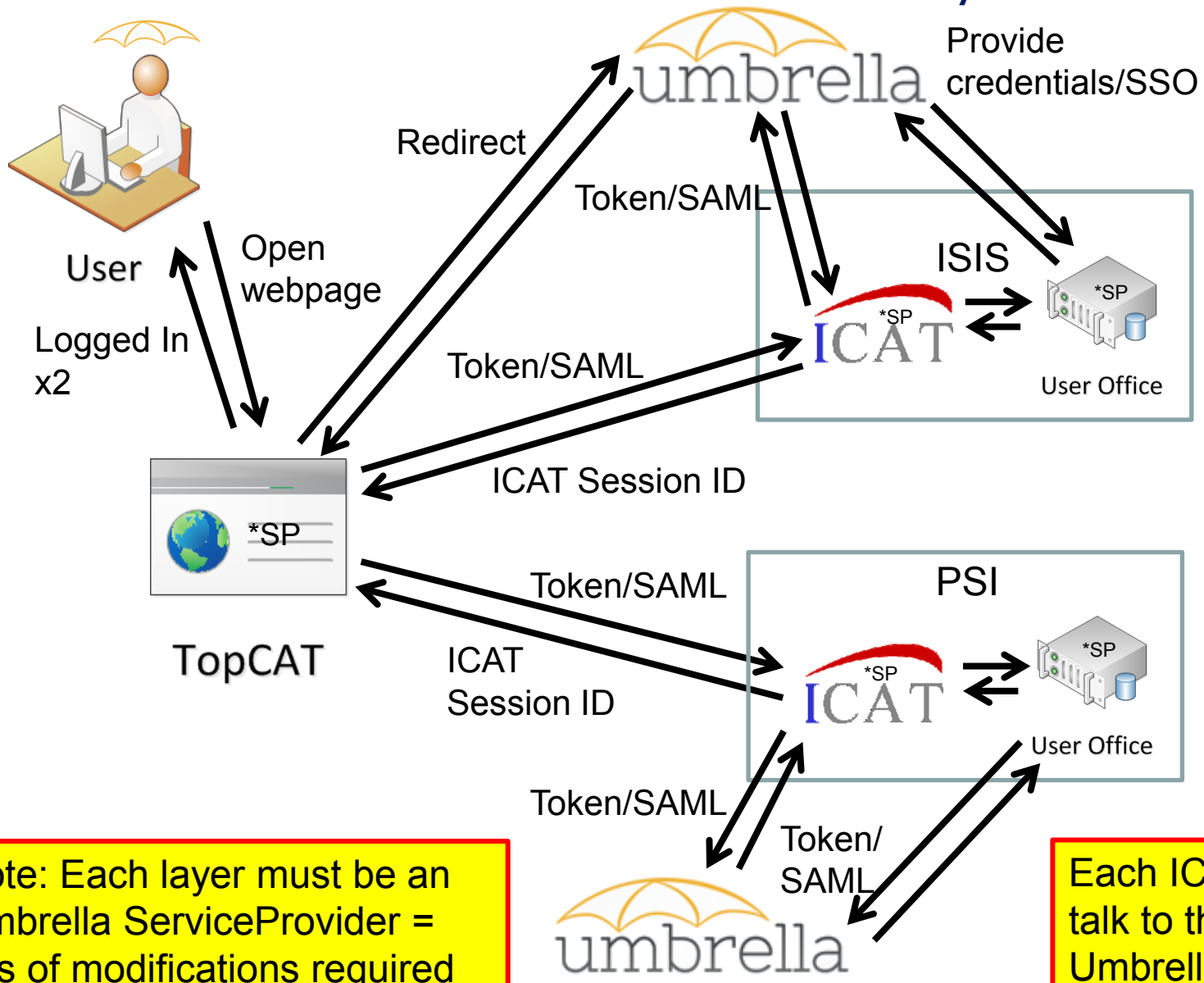
Real world –Umbrella – Many ICATs



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 – Many ICATs



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

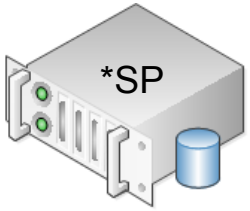
Each ICAT/UO will talk to the most local Umbrella IdP

Real world –Umbrella – Mantid/Dawn

User

umbrella

Mantid



User Office

ICAT

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

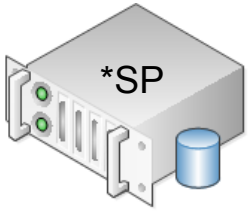
Real world –Umbrella – Mantid/Dawn

User

Username + password

umbrella

Mantid



User Office

ICAT

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

Real world –Umbrella – Mantid/Dawn

User

Username + password

umbrella

Mantid

*SP

User Office

Username + password

ICAT

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

Real world –Umbrella – Mantid/Dawn

User

Username + password

umbrella

Mantid

*SP

Username + password

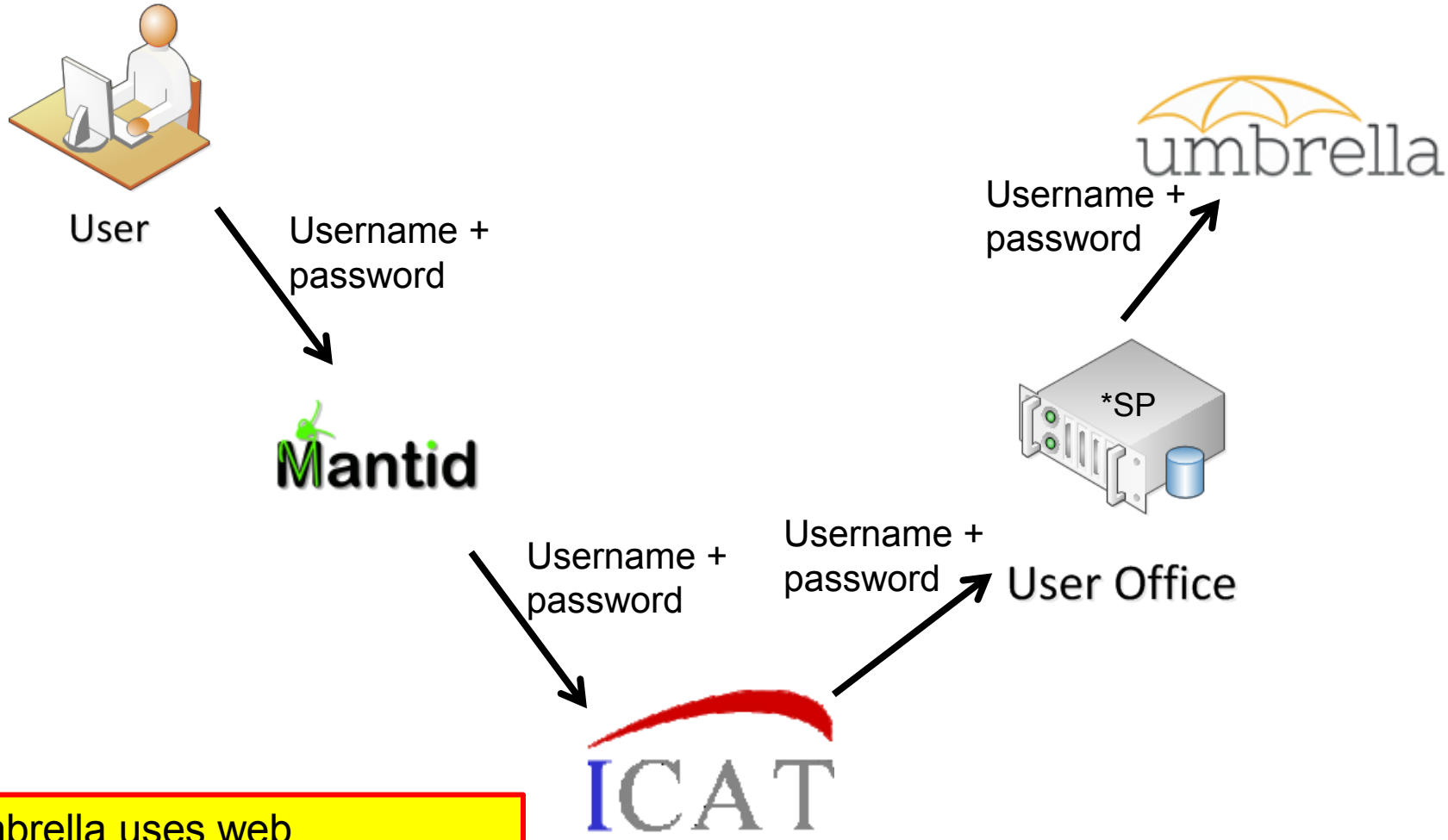
Username + password

User Office

ICAT

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

Real world –Umbrella – Mantid/Dawn



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

Real world –Umbrella – Mantid/Dawn

User

Username + password

Mantid

Username + password

ICAT

Username + password

User Office

Username + password

umbrella

Umbrella Token/SAML

*SP

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

Real world –Umbrella – Mantid/Dawn

User

Username + password

Mantid

Username + password

ICAT

Username + password

User Office

Username + password

umbrella

Umbrella Token/SAML

*SP

Translate UUID to local UID

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

Real world –Umbrella – Mantid/Dawn

User

Username + password

Mantid

Username + password

ICAT

Username + password

User Office

UO Session ID/ Local UID

umbrella

Username + password

Umbrella Token/SAML

*SP

Translate UUID to local UID

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

Real world –Umbrella – Mantid/Dawn

User

Username + password

Mantid

Username + password

ICAT session ID

ICAT

Username + password

User Office

UO Session ID/ Local UID

Username + password

umbrella

Umbrella Token/SAML

*SP

Translate UUID to local UID

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

Real world –Umbrella – Mantid/Dawn

User

Logged In

Username + password

Mantid

umbrella

Username + password

Umbrella Token/SAML

*SP

Translate UUID to local UID

Username + password

User Office

Username + password

ICAT session ID

ICAT

UO Session ID/ Local UID

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

‘Toy’ ICAT – Non-Umbrella

User

TopCAT

ICAT User Database

ICAT

‘Toy’ ICAT – Non-Umbrella

User

Username + password

TopCAT

ICAT User Database

ICAT

‘Toy’ ICAT – Non-Umbrella

User

Username + password

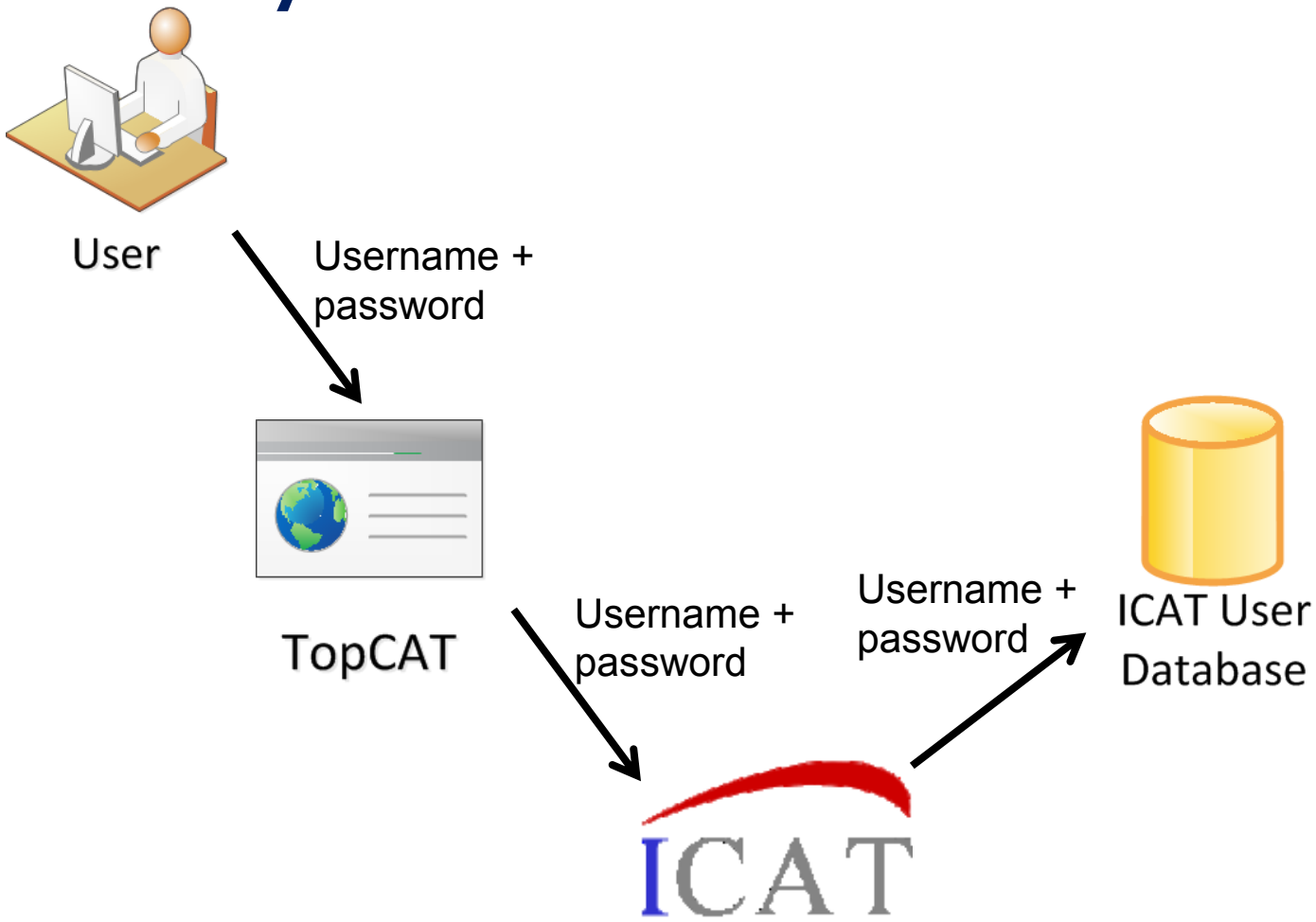
TopCAT

Username + password

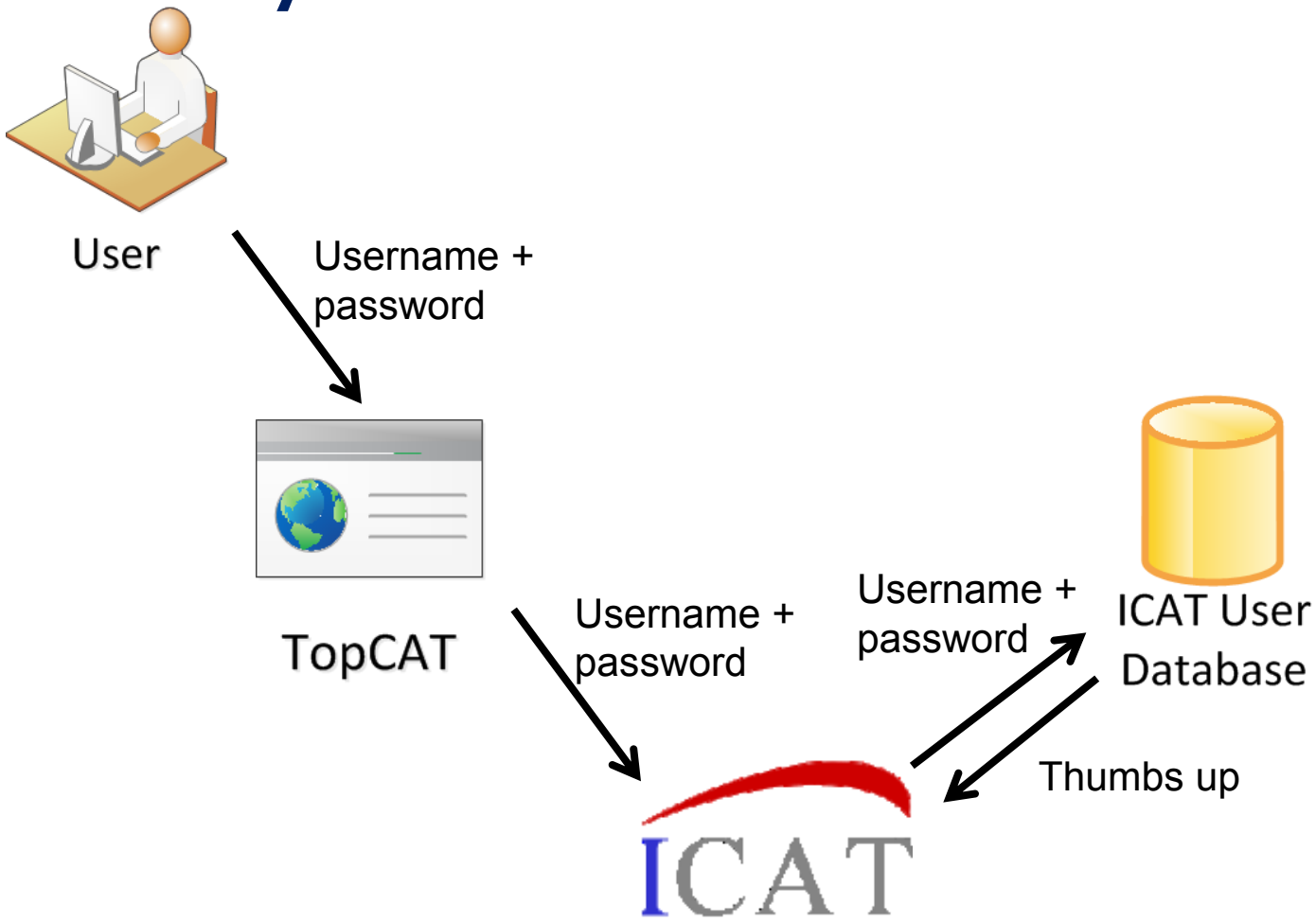
ICAT User Database

ICAT

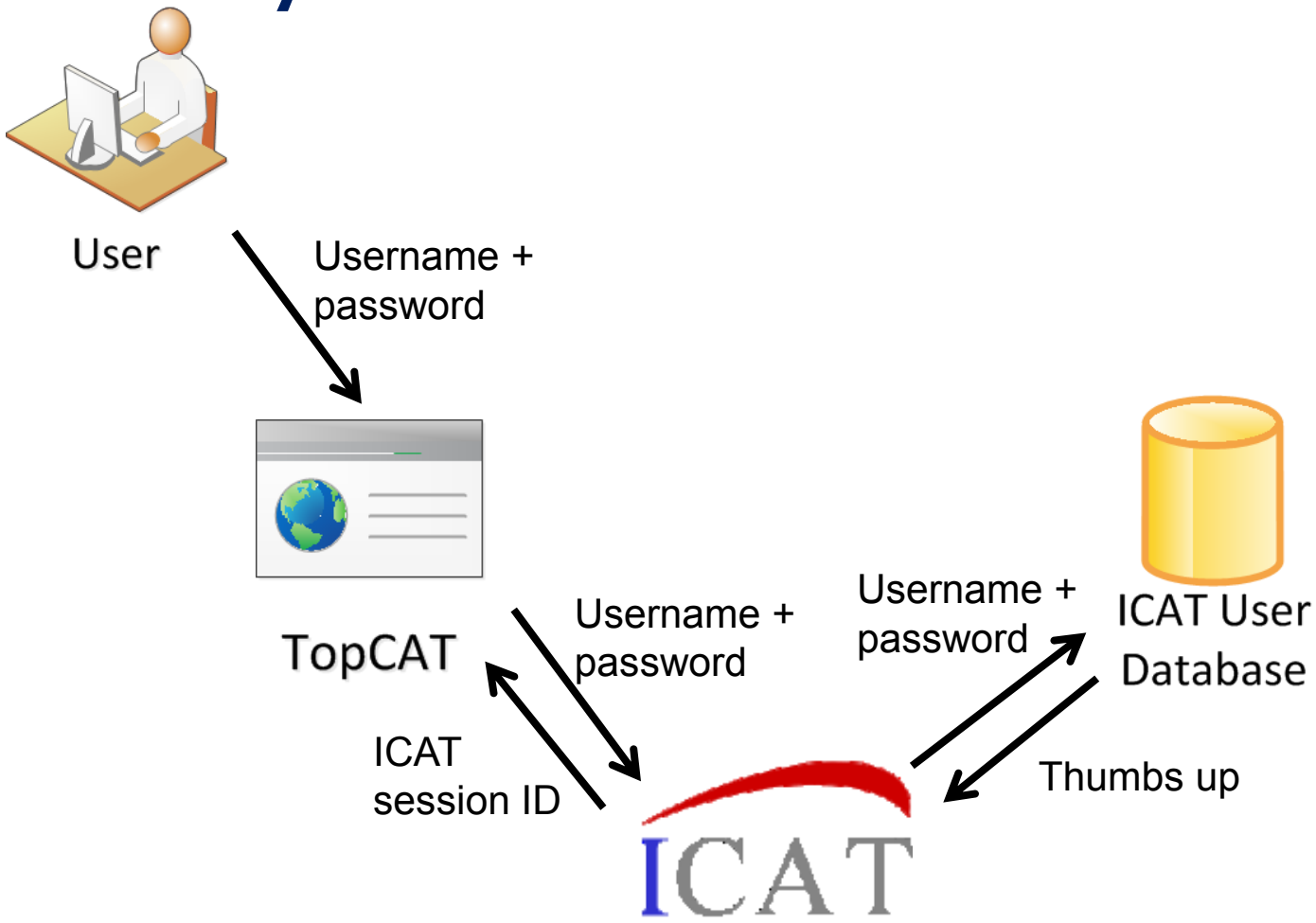
‘Toy’ ICAT – Non-Umbrella



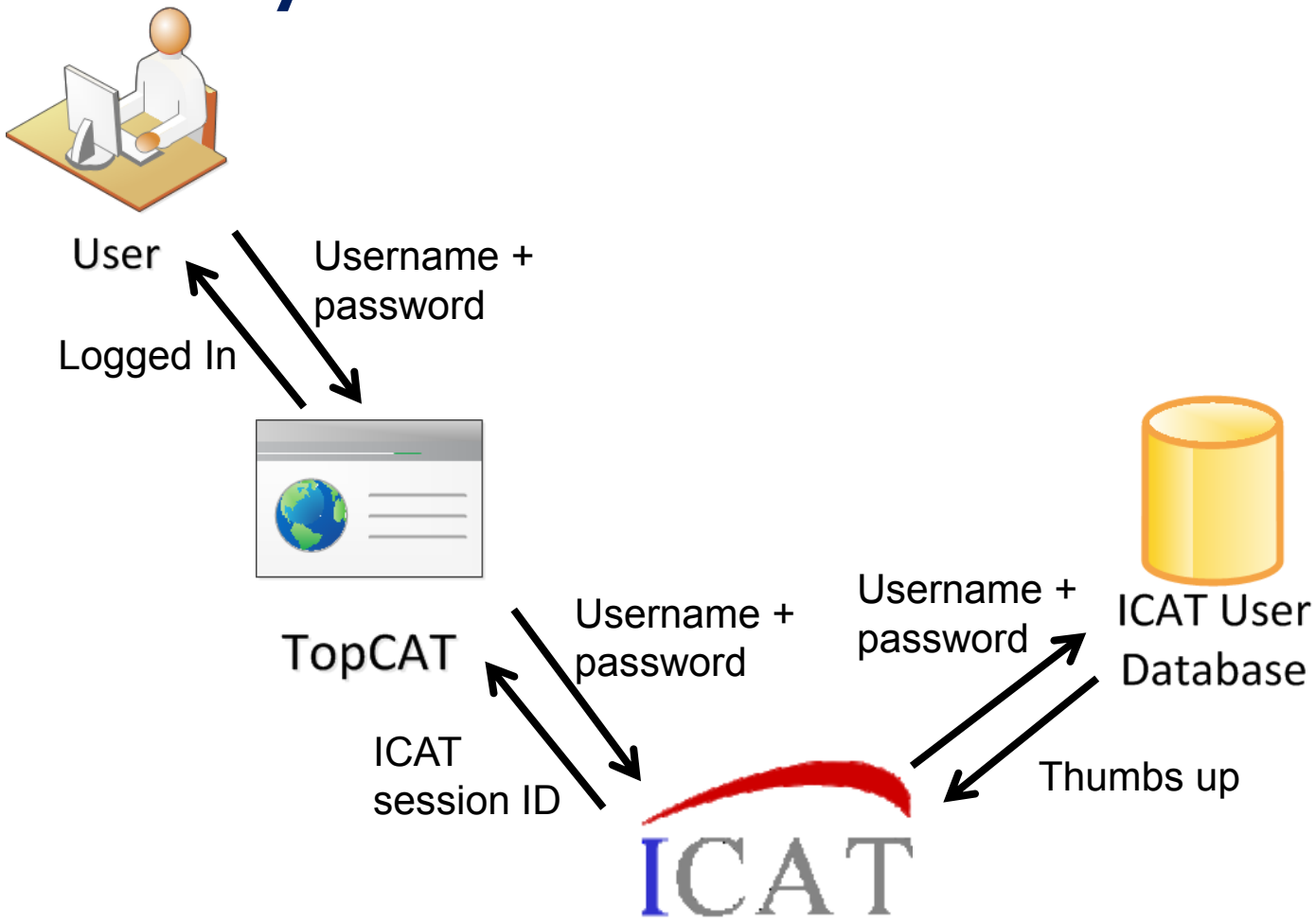
‘Toy’ ICAT – Non-Umbrella



‘Toy’ ICAT – Non-Umbrella



‘Toy’ ICAT – Non-Umbrella



‘Toy’ ICAT – Umbrella

Username	Password
root	Secret
tom.griffin	
mantid_test	testpassword
…	…

‘Toy’ ICAT – Umbrella

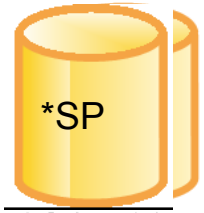
Username	Password	UUID
root	Secret	
tom.griffin		d5bed531--a2e1-8013f8fb319f
mantid_test	testpassword	
…	…	…

Real World - 'Pure' Shibboleth

User

umbrella

TopCAT



ICAT User Database

ICAT

ICAT Authentication layer explicitly shown

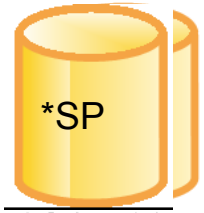
Real World - 'Pure' Shibboleth

User

Open webpage

umbrella

TopCAT



ICAT User Database

ICAT

ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth

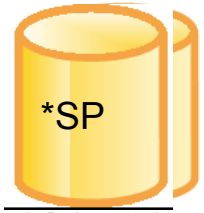
User

Open webpage

Redirect

umbrella

TopCAT



ICAT User Database

ICAT

ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth

User

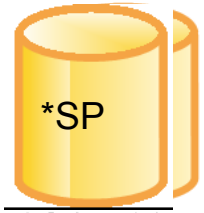
Open webpage

Redirect

Provide credentials/SSO

umbrella

TopCAT



ICAT User Database

ICAT

ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth

User

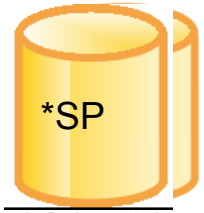
Open webpage

Redirect

Provide credentials/SSO

umbrella

TopCAT



ICAT User Database

ICAT

ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth

User

Open webpage

Redirect

Provide credentials/SSO

umbrella

*SP

TopCAT

Token/SAML

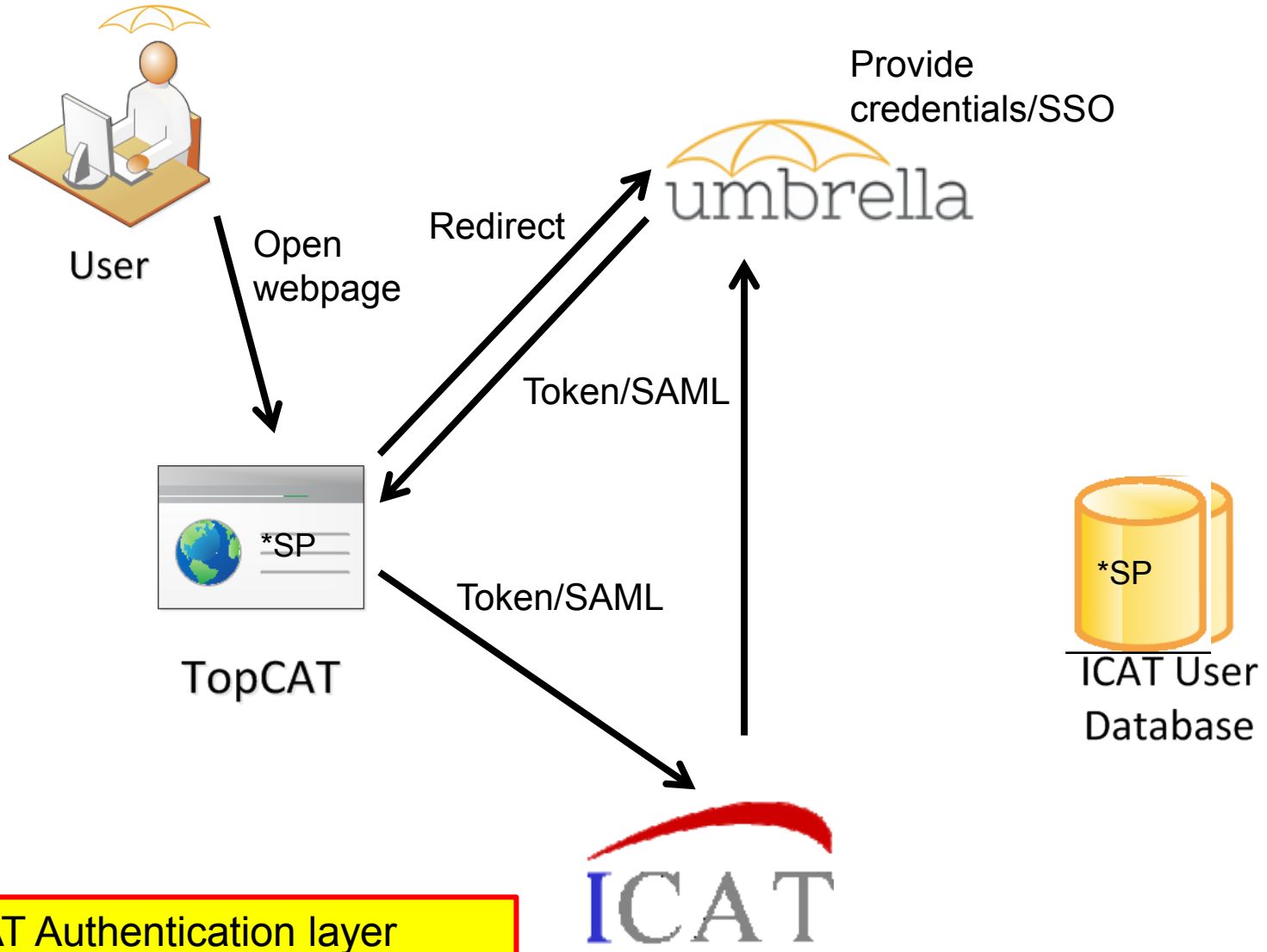
*SP

ICAT User Database

ICAT

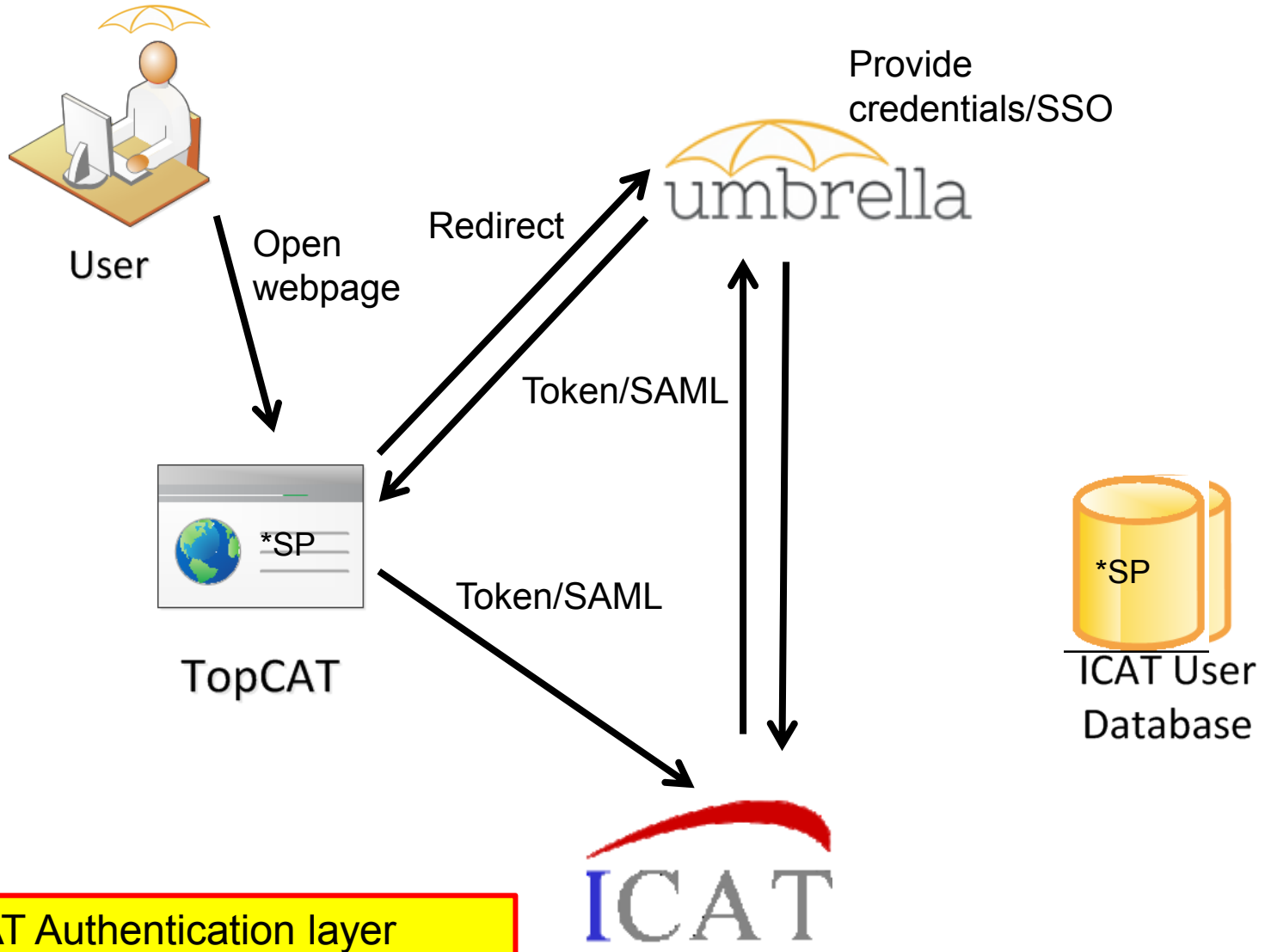
ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth



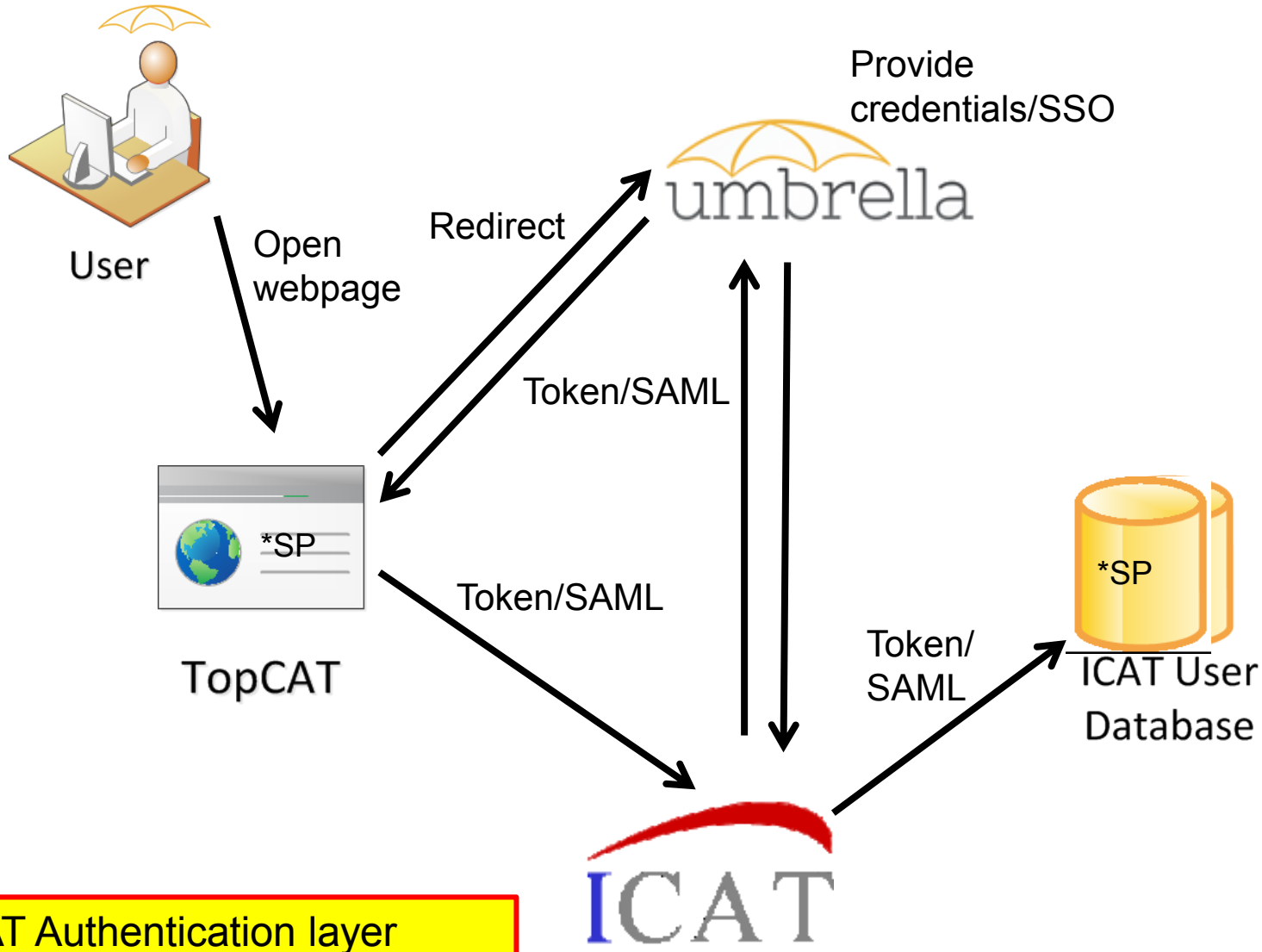
ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth



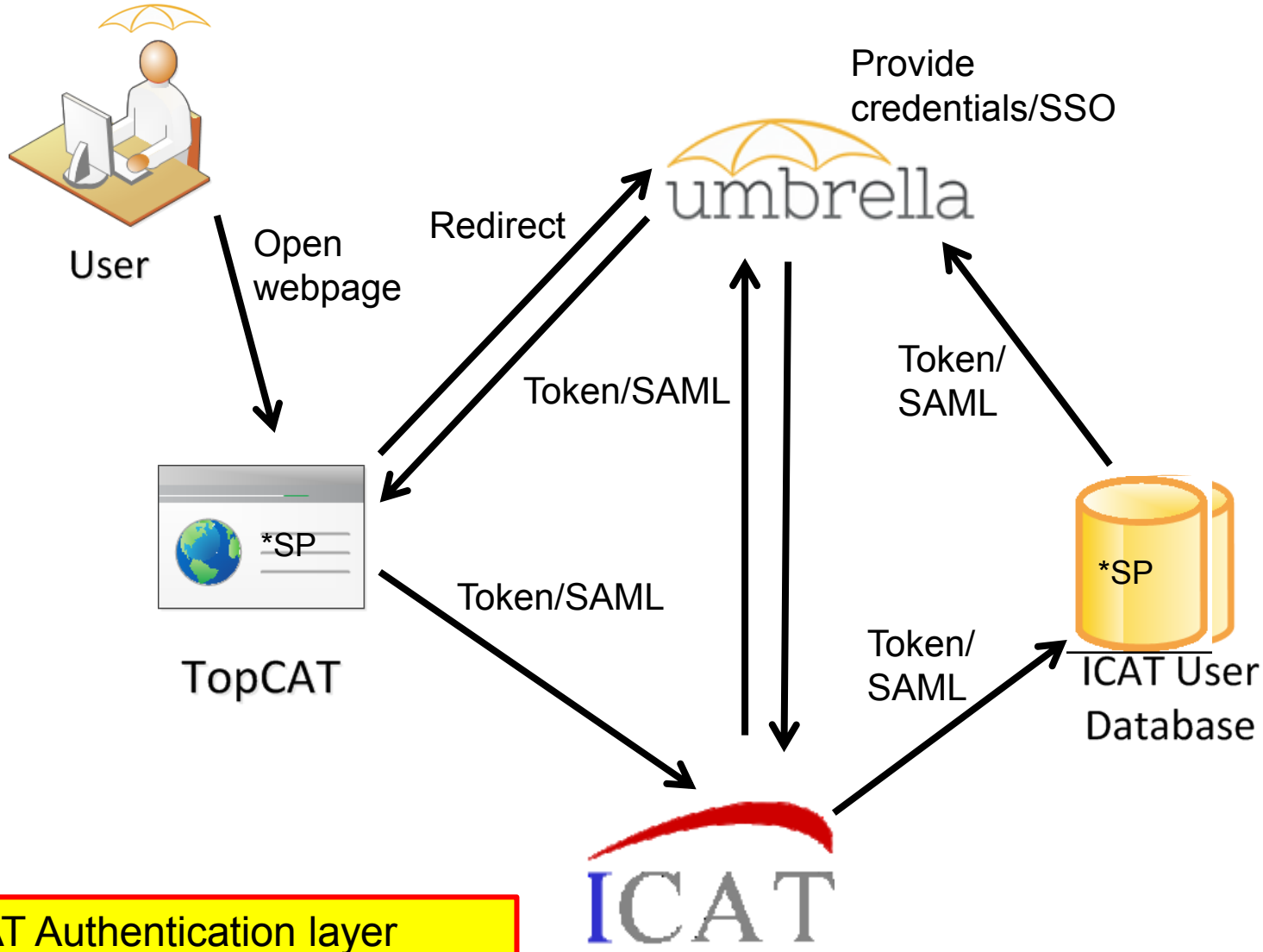
ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth



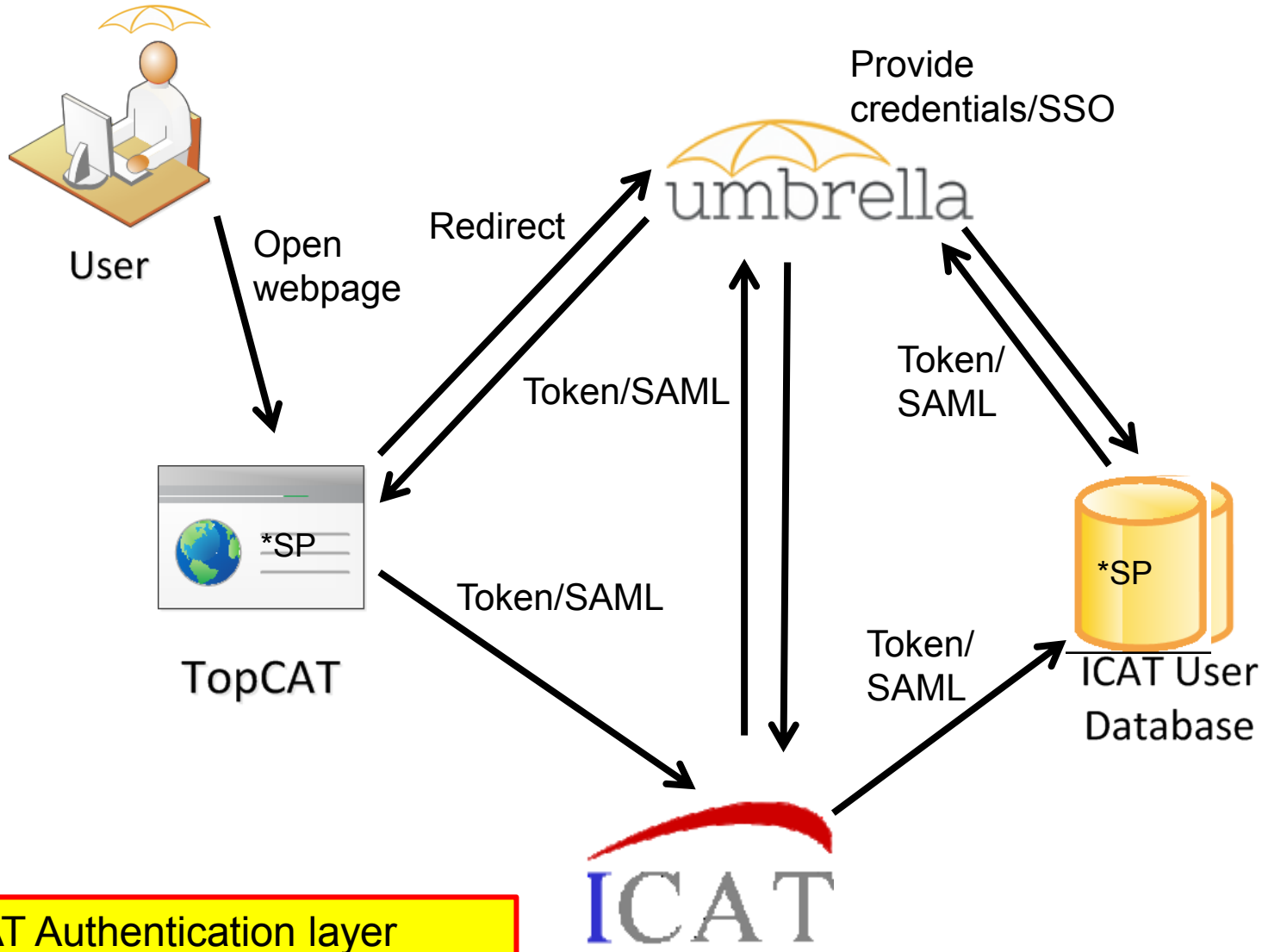
ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth



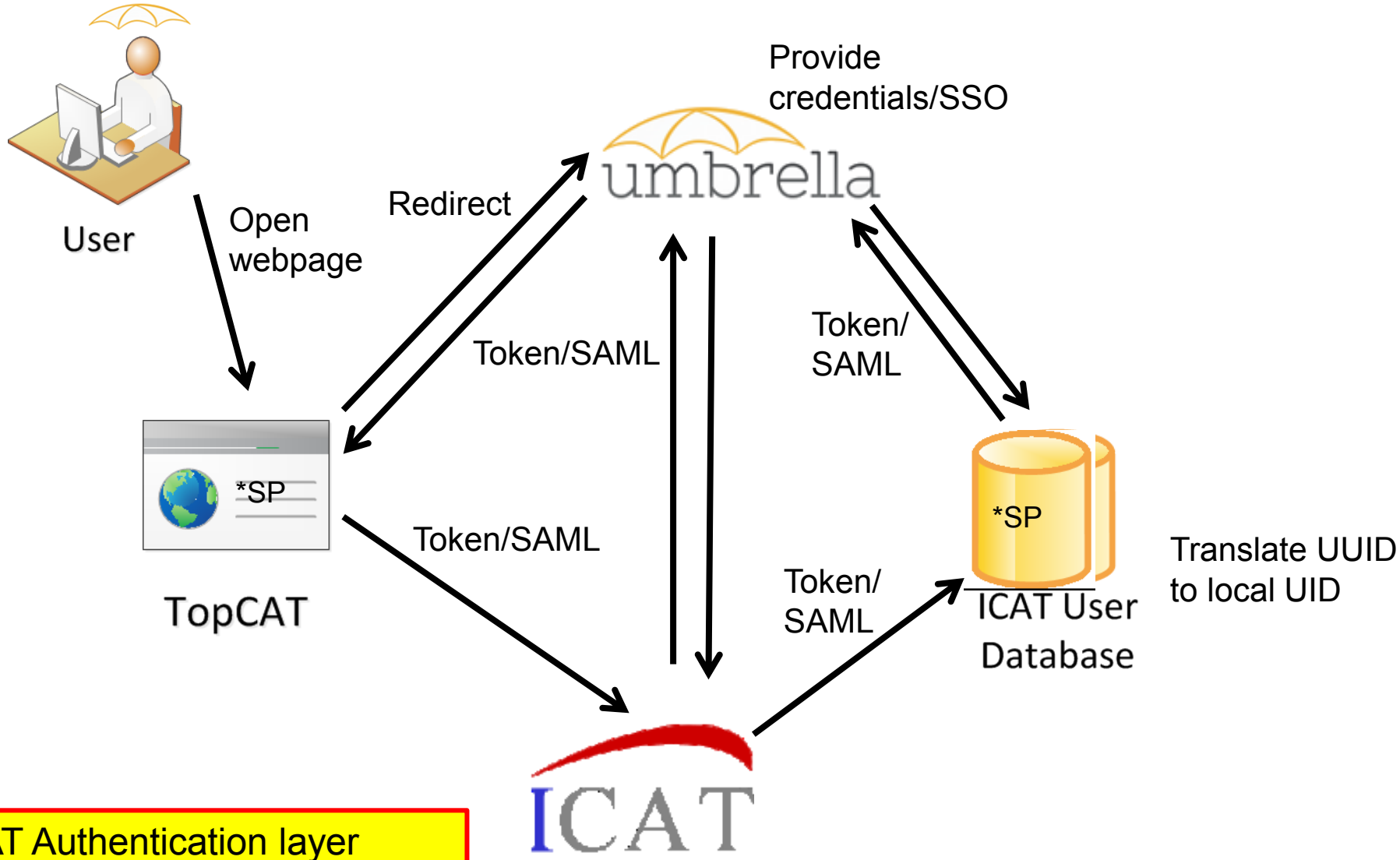
ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth



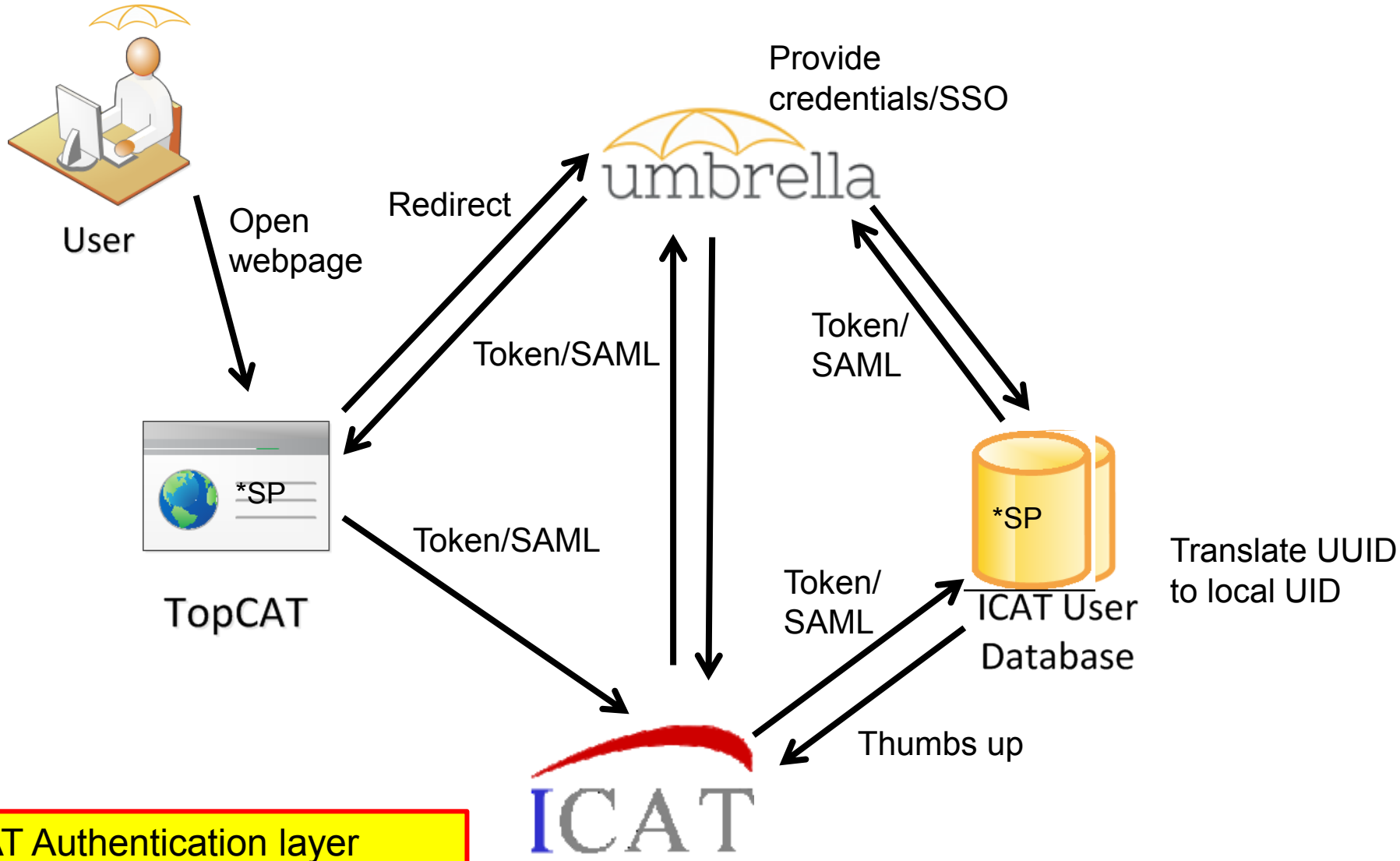
ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth



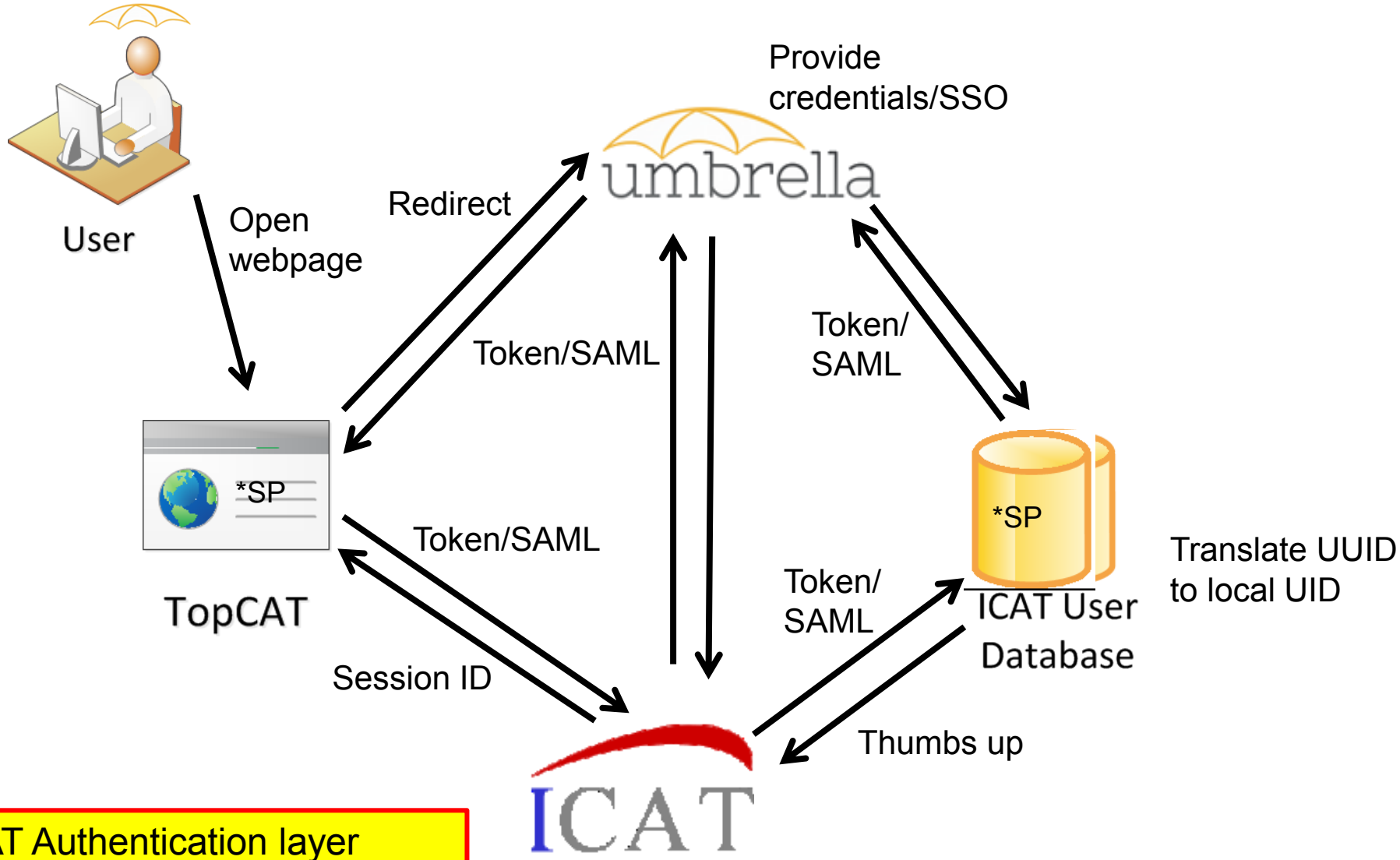
ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth



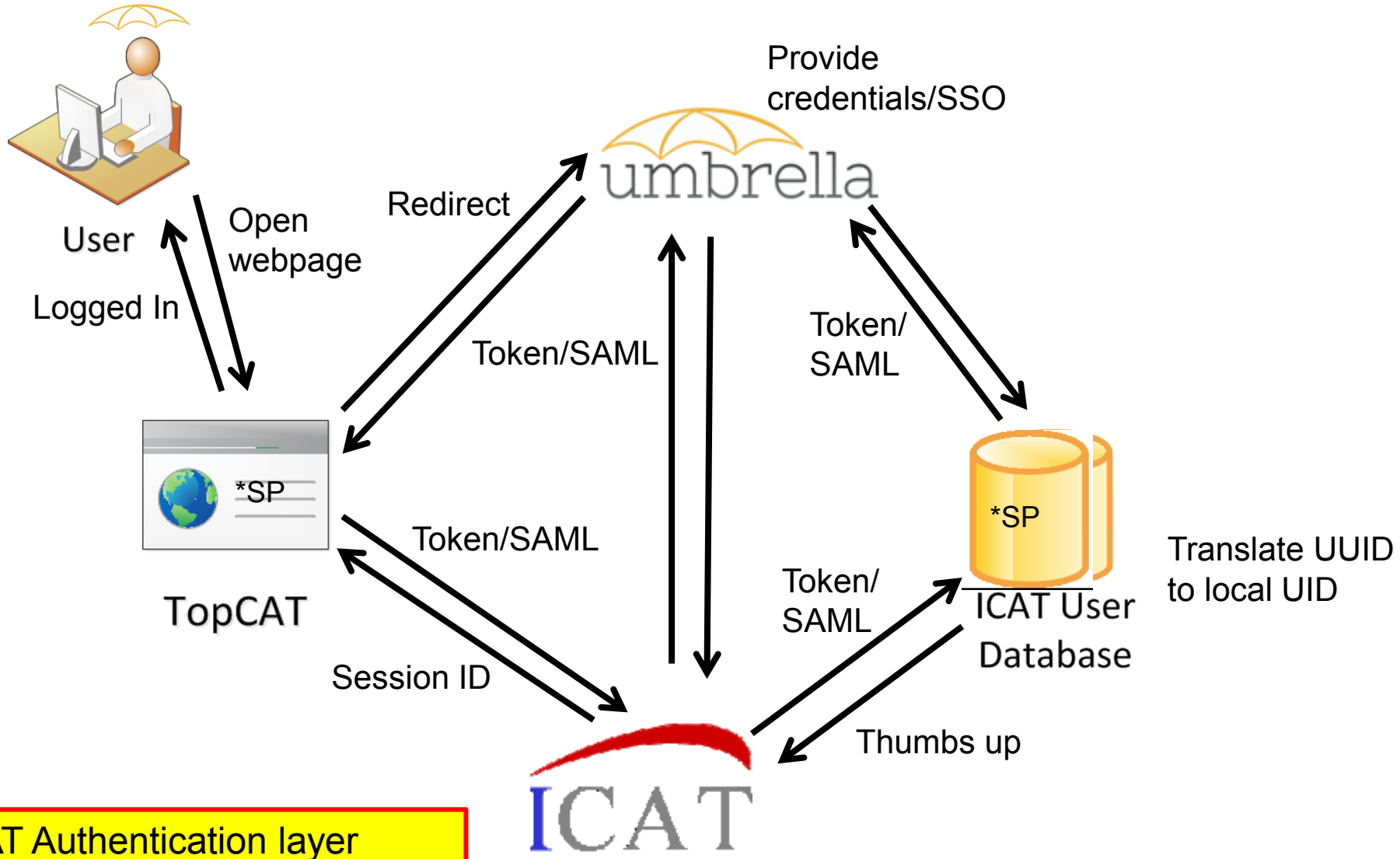
ICAT Authentication layer explicitly shown

Real World - 'Pure' Shibboleth



ICAT Authentication layer explicitly shown

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...