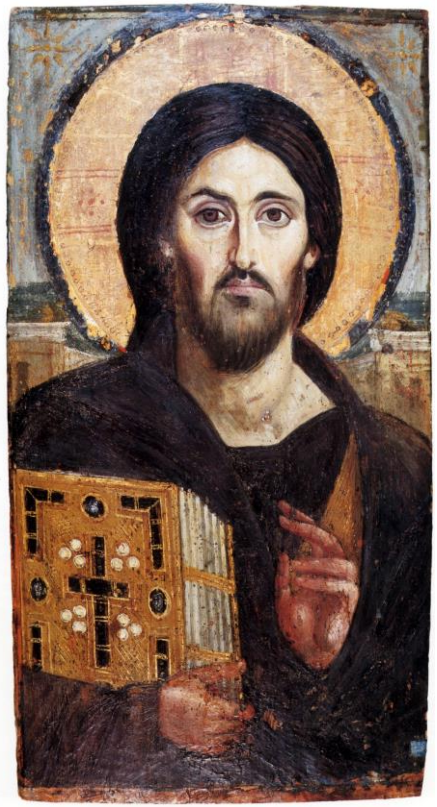
Who to Trust?



Me = Security Consultant @ CANCOM

TLS and SAML

- From technical POV safe and sound

BUT

- Are they applied as intendend?
- Or are we just hoping it is?

TLS Overview

- TLS uses certificates to establish trust between parties
- Certificates are issued by trusted Certificate Authorities
- TLS encrypts data in transit (between these parties) to prevent eavesdropping++

TLS uses certificates to establish **trust between parties**

Trust between whom?

- Webservice and Client‘s Browser?
- TLS interception @ Firewall?
  - Are they using proper encryption?
  - Or encrypt at all?

Consider certificate pinning

Certificates are issued by **Certificate Authorities**

- Inherent Trust in CAs

  CNNIC

  removed in 2015

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
BEIJING CERTIFICATE AUTHORITY	
BJCA Global Root CA2	Builtin Object Token

- Many big CAs have a history of incidents, issu unauthorized Certificates.

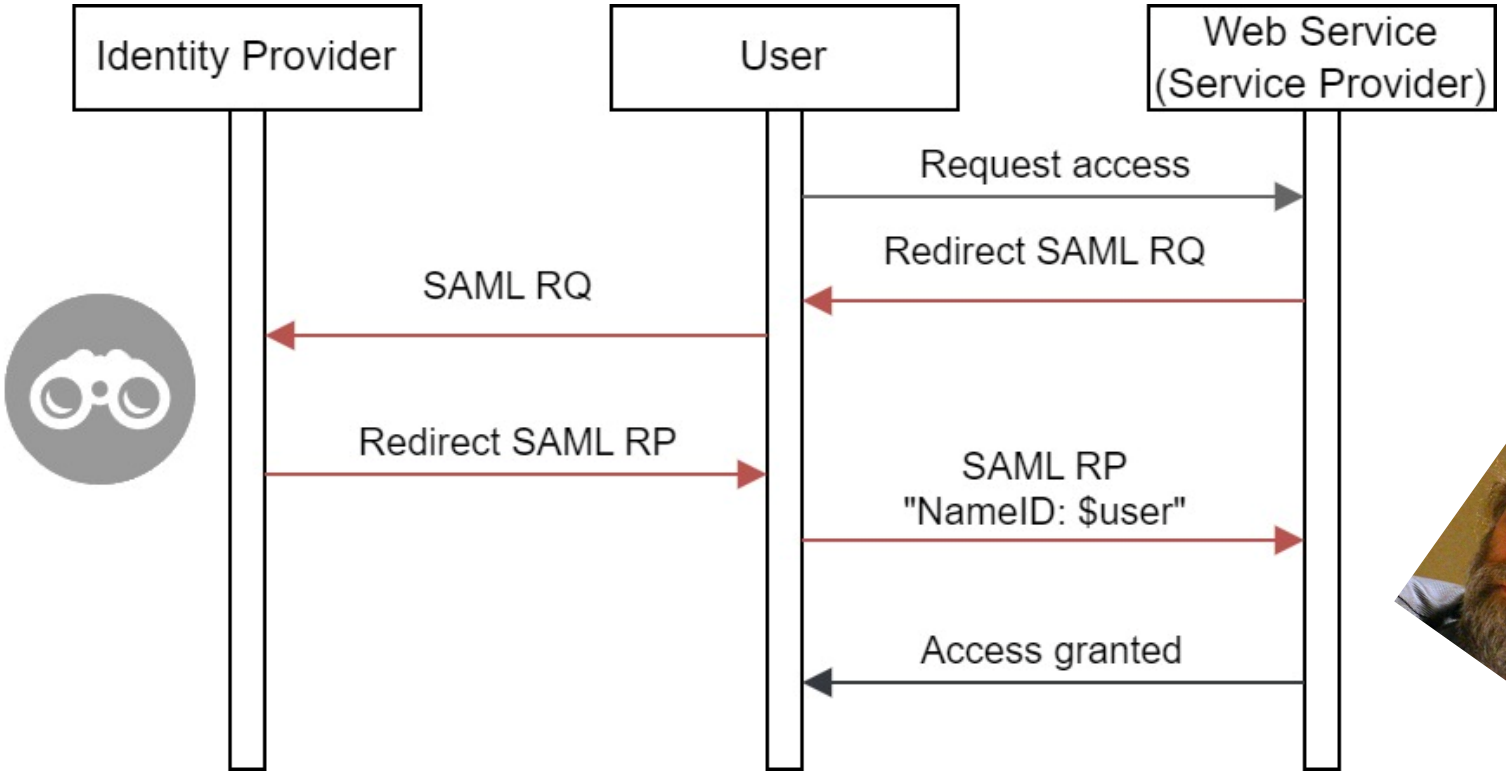
TLS conclusio

- TLS is one of the greatest improvem
  everyday security

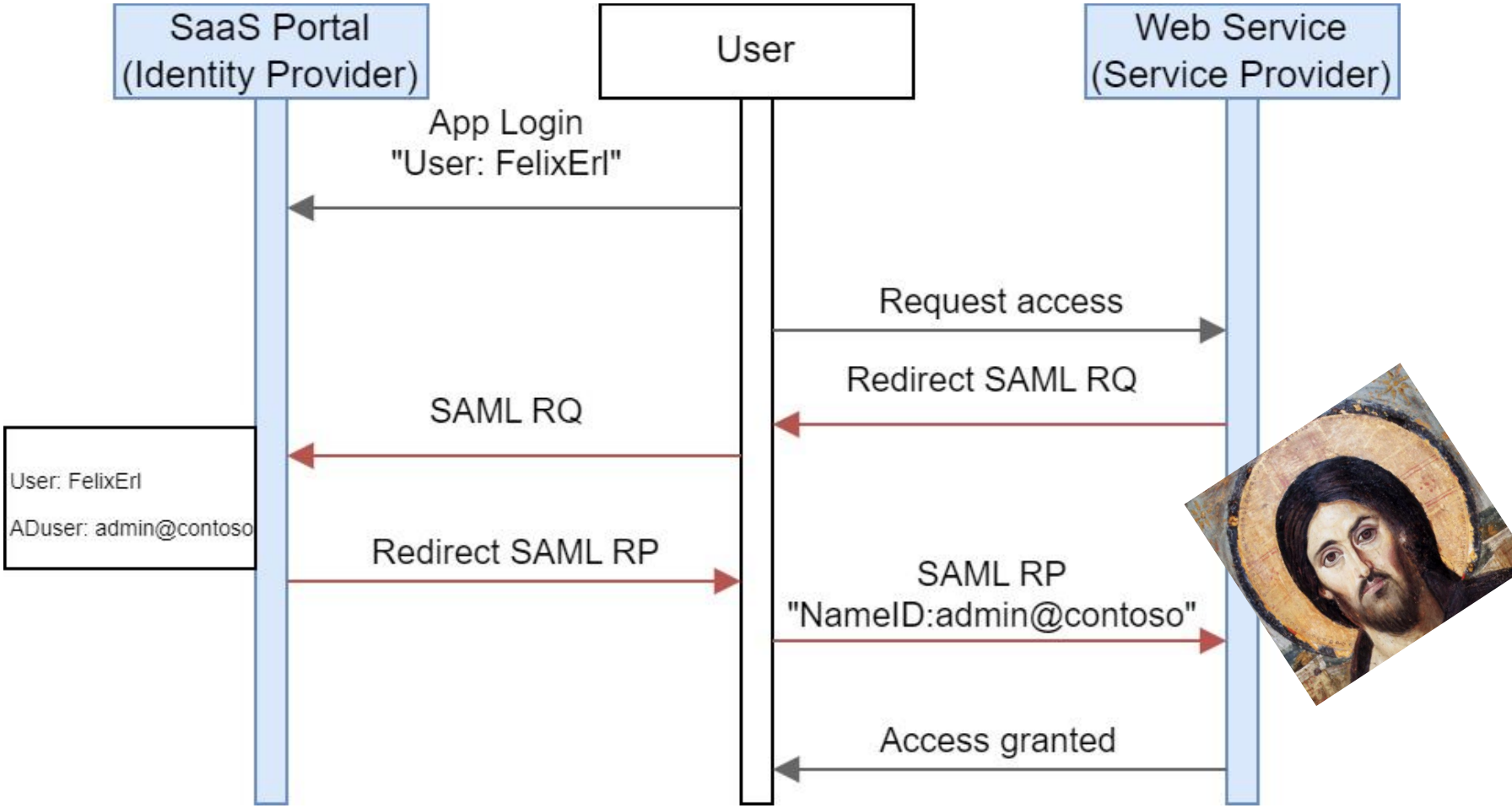
- No blind trust in anything because of TLS

SAML

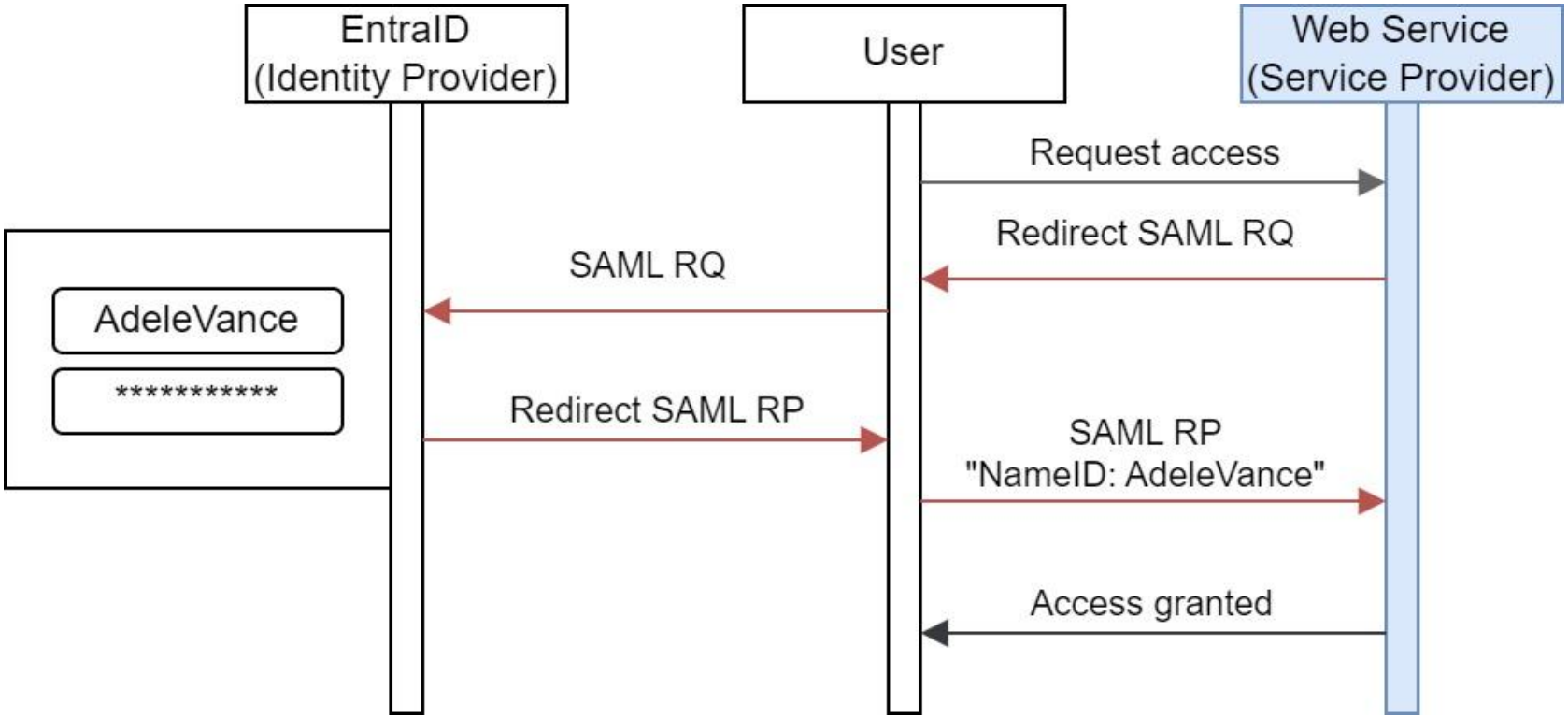
- Framework for exchanging authentication information ---> Single Sign On



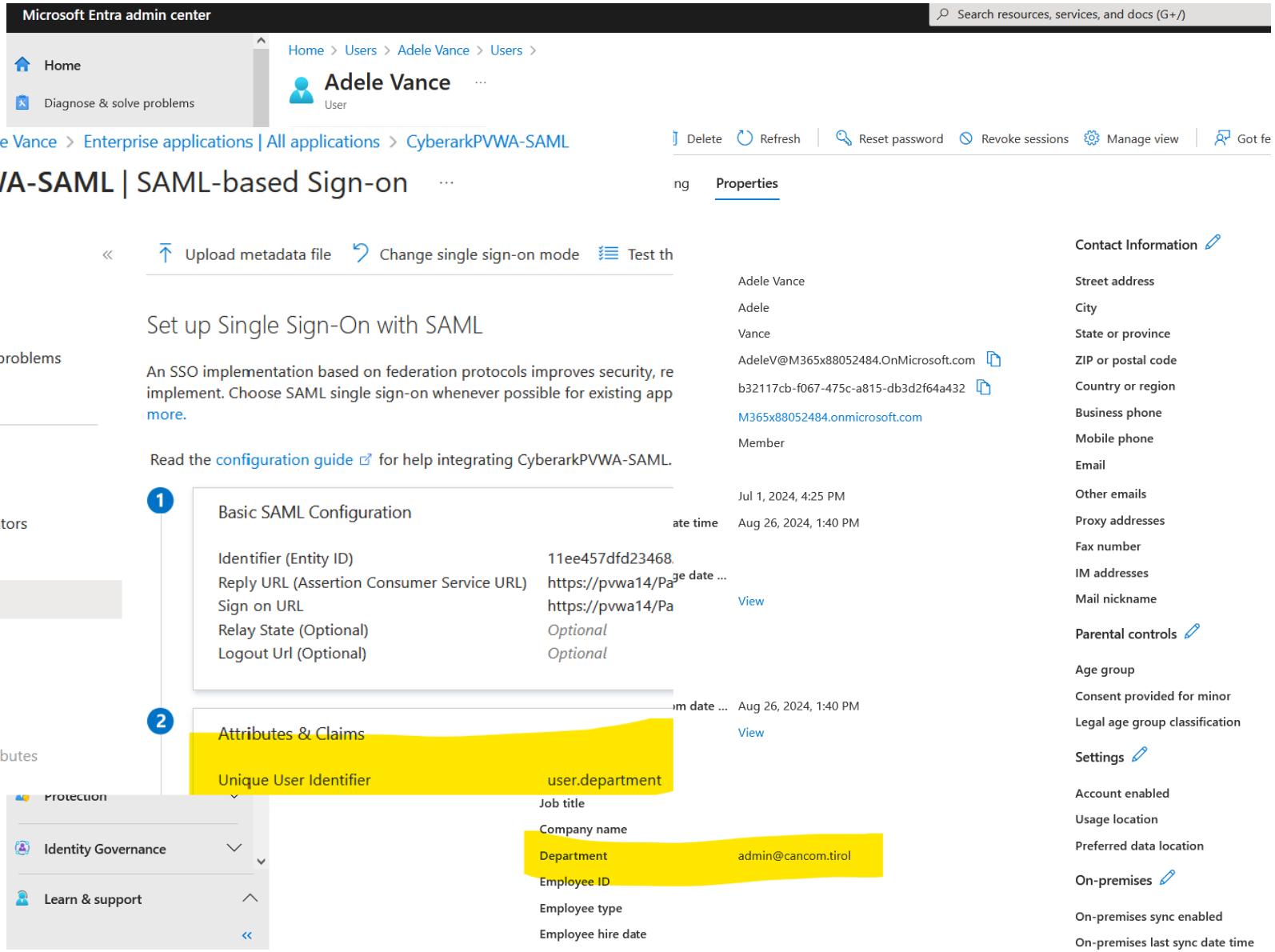
SAML in Real Life 1



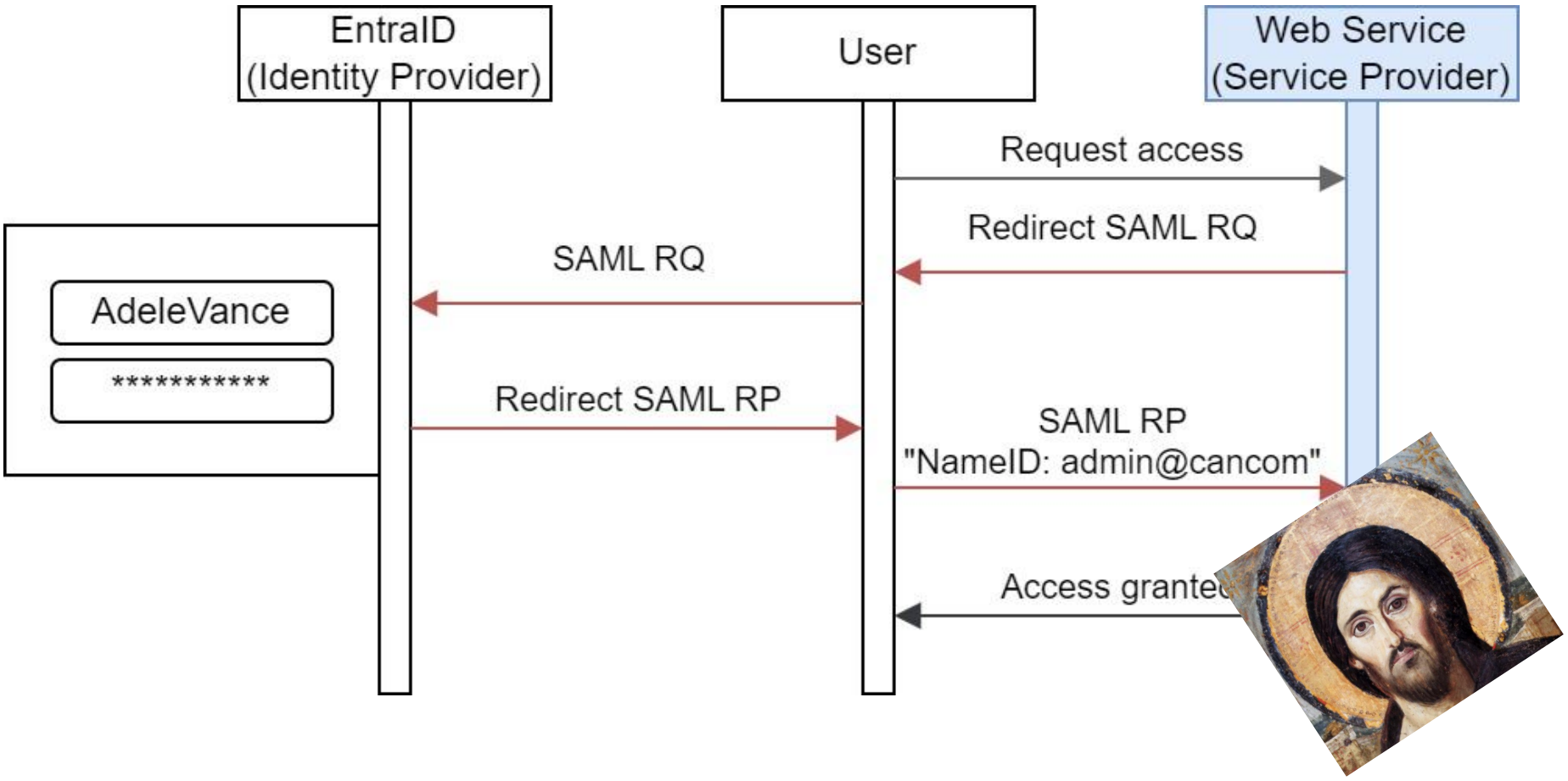
SAML in Real Life 2



SAML in Real Life 2



SAML in Real Life 2

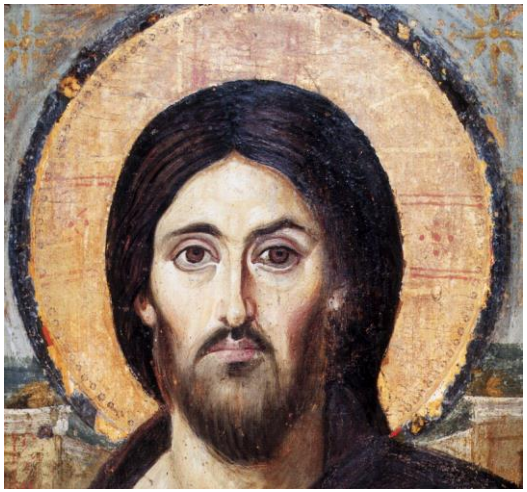


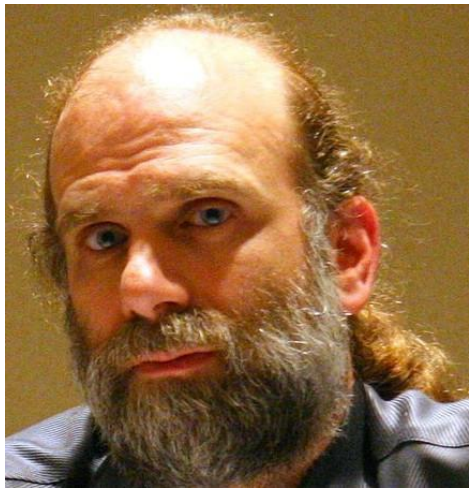
SAML Conclusio

- Finally a Sec. Protocol with += comfort
- Beware of the pitfalls

Final Score:

6 : 3





- Pay attention when implementing/using Security Protocols.
- Become a believer.

- OWASP Pinning Cheat Sheat:

  https://cheatsheetseries.owasp.org/cheatsheets/Pinning_Cheat_Sheet.html
- SAML tools:

  https://www.samltool.com/
- Facts about Bruce Schneier:

  https://www.schneierfacts.com/
- Schneier on Security Blog:

  https://www.schneier.com/