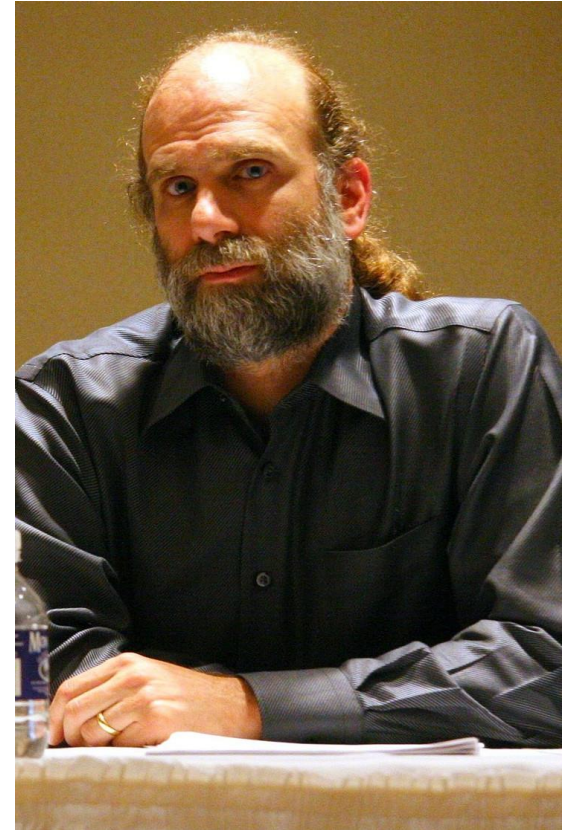
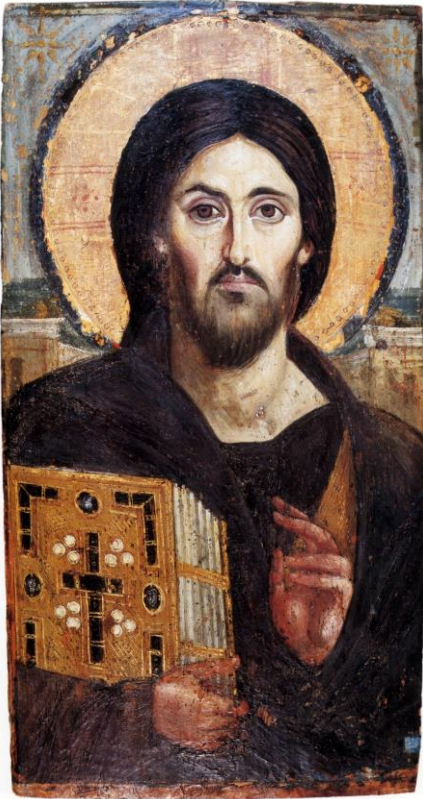


Who to Trust?



sfilaw, CC BY-SA 2.0 <<https://creativecommons.org/licenses/by-sa/2.0/>>, via Wikimedia Commons

Me = Security Consultant @ **CANCOM**

TLS and SAML

- From technical POV safe and sound



BUT

- Are they applied as intended?
- 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	Built-in Object Token	

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



TLS conclusio

- TLS is one of the greatest improvements to everyday security



Let's Encrypt

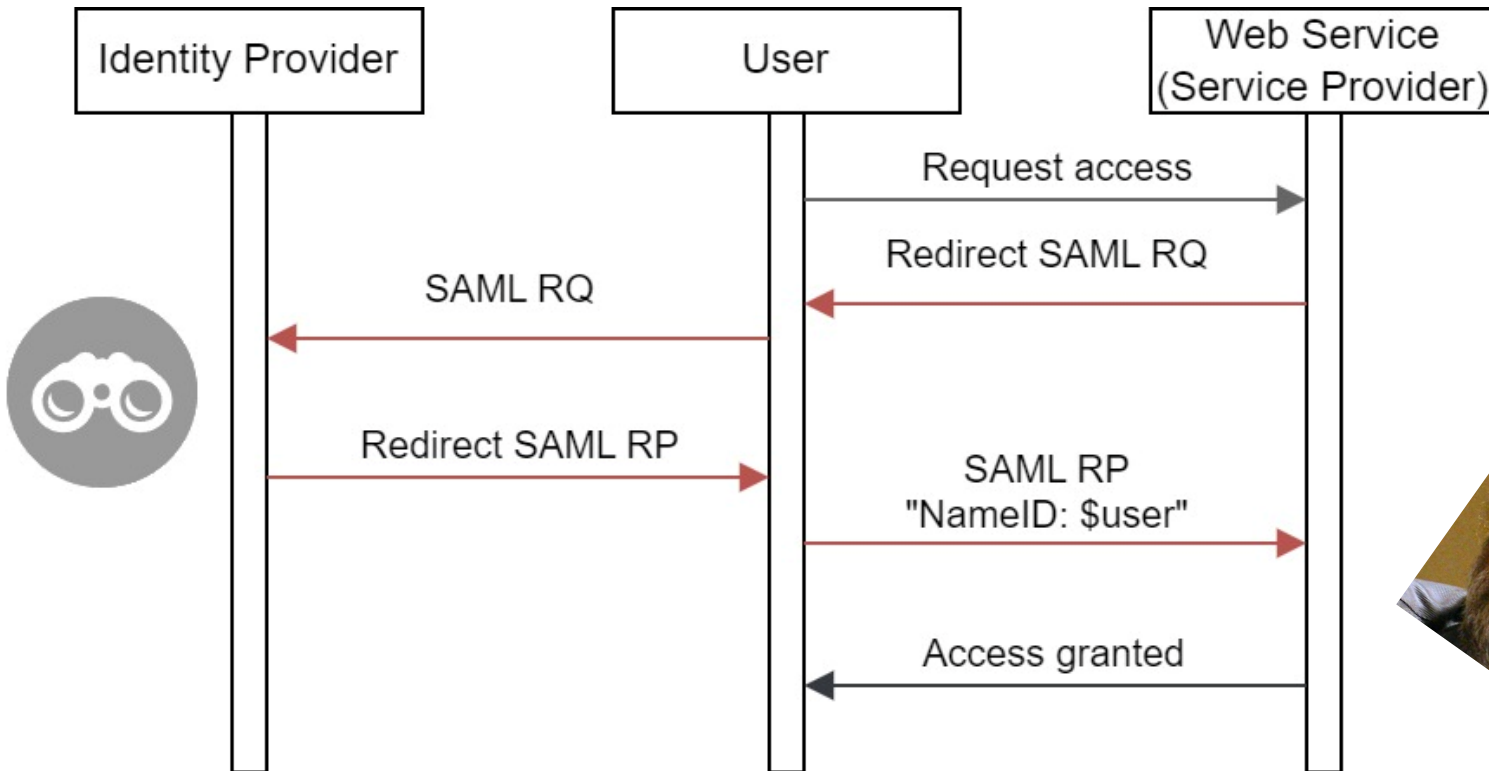


- No blind trust in anything because of TLS

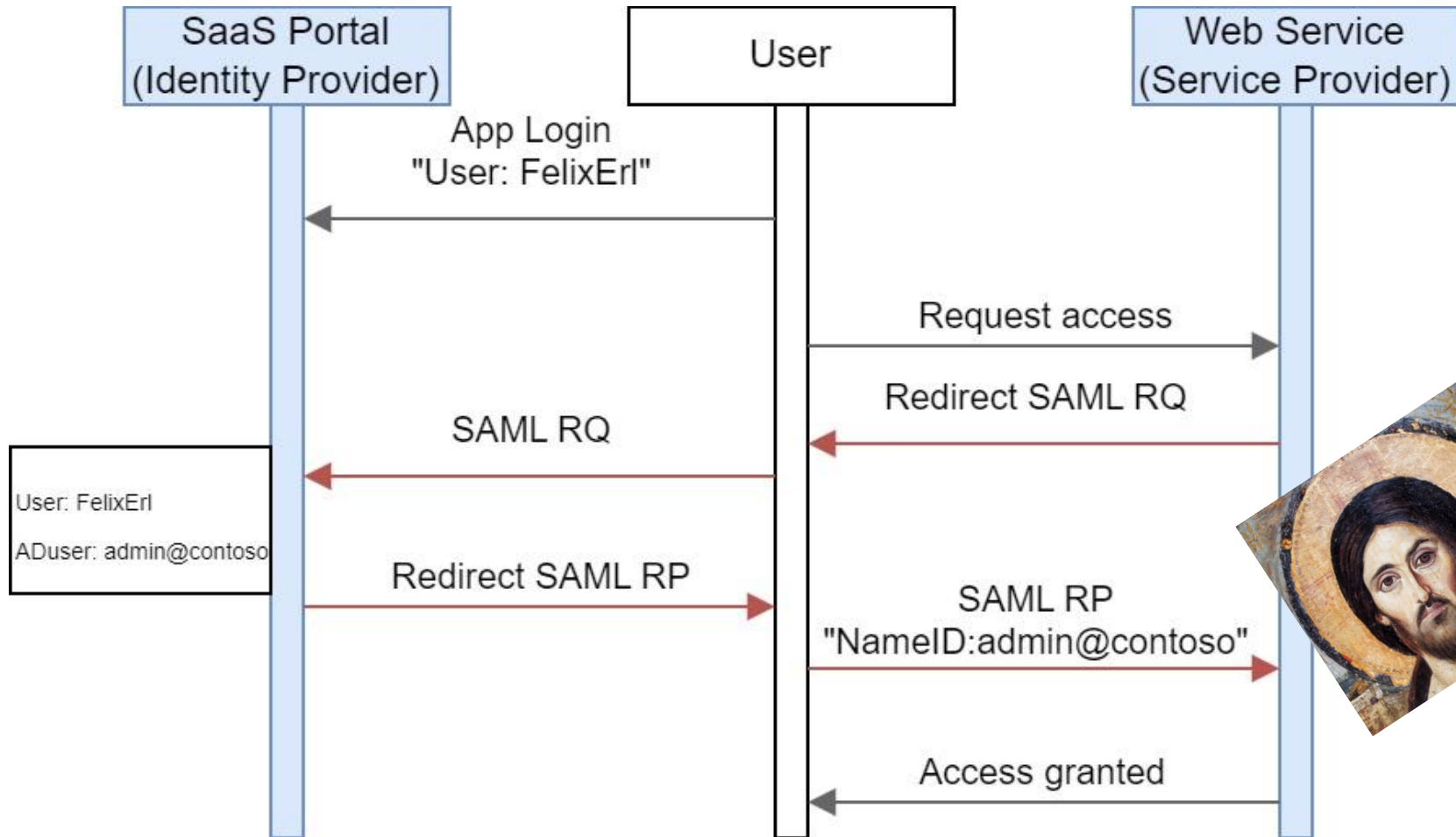


SAML

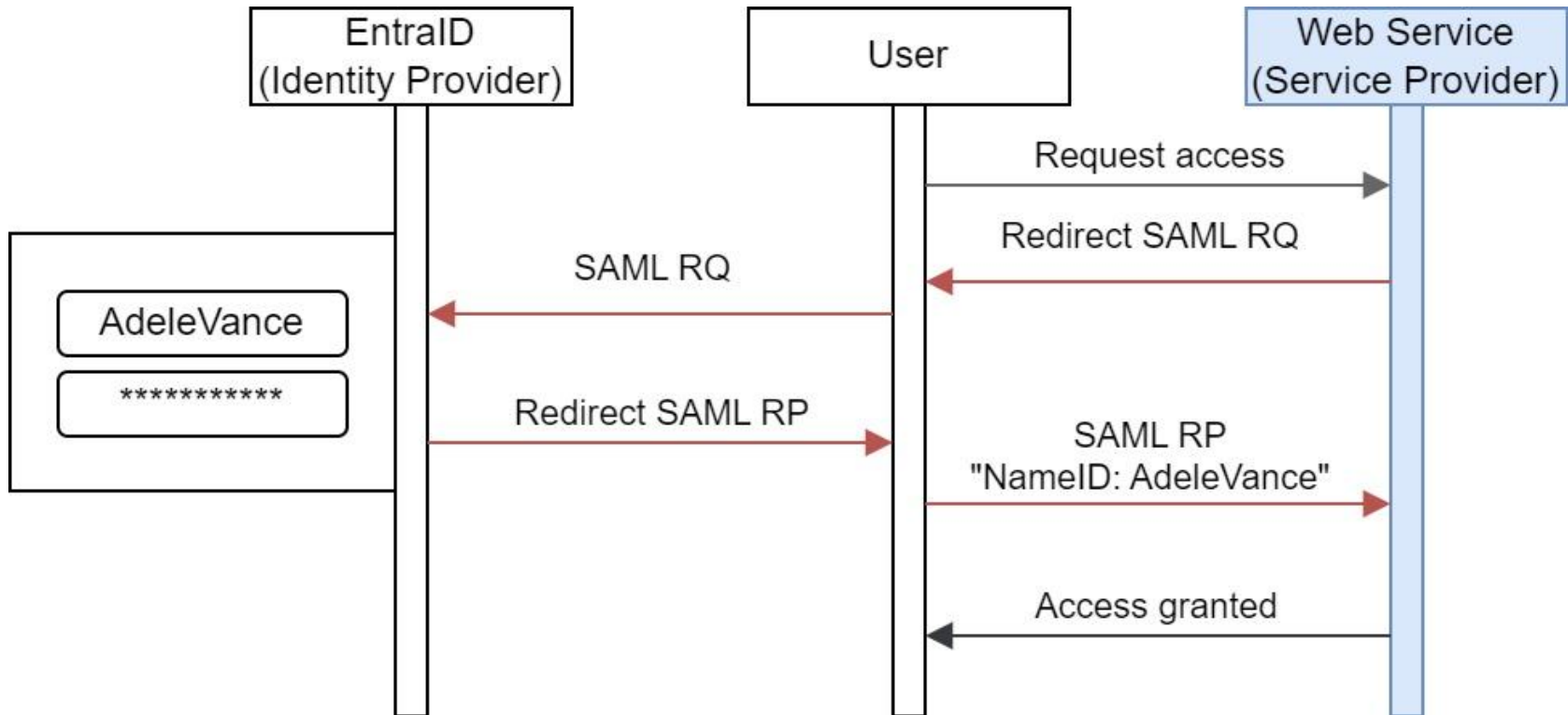
- Framework for exchanging authentication information ---> Single Sign On



SAML in Real Life 1



SAML in Real Life 2



SAML in Real Life 2

The screenshot shows the Microsoft Entra admin center interface. The breadcrumb navigation is: Home > Users > Adele Vance > Users > Enterprise applications | All applications > CyberarkPVWA-SAML. The main heading is "PVWA-SAML | SAML-based Sign-on". The left sidebar shows the "Single sign-on" menu item selected. The main content area is titled "Set up Single Sign-On with SAML" and includes a description: "An SSO implementation based on federation protocols improves security, re implement. Choose SAML single sign-on whenever possible for existing app more." Below this is a link to the "configuration guide".

Two numbered steps are highlighted:

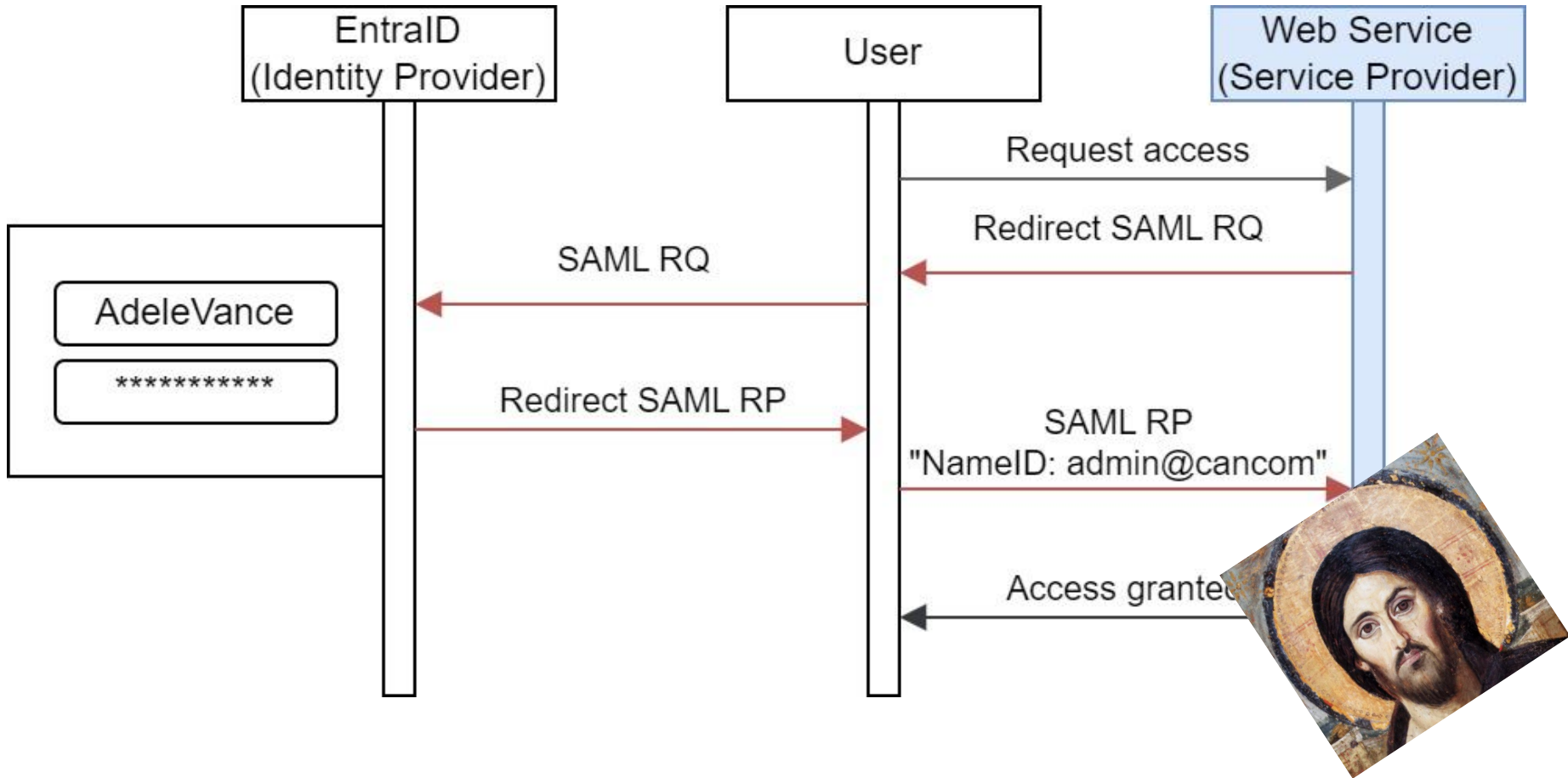
- Basic SAML Configuration**

Identifier (Entity ID)	11ee457dfd23468
Reply URL (Assertion Consumer Service URL)	https://pwwa14/Pa... 3e date ...
Sign on URL	https://pwwa14/Pa... View
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims**

Unique User Identifier	user.department
Job title	
Company name	
Department	admin@cancom.tirol
Employee ID	
Employee type	
Employee hire date	

- Contact Information
- Street address
- City
- State or province
- ZIP or postal code
- Country or region
- Business phone
- Mobile phone
- Email
- Other emails
- Proxy addresses
- Fax number
- IM addresses
- Mail nickname
- Parental controls
- Age group
- Consent provided for minor
- Legal age group classification
- Settings
- Account enabled
- Usage location
- Preferred data location
- On-premises
- On-premises sync enabled
- On-premises last sync date time

SAML in Real Life 2



SAML Conclusio

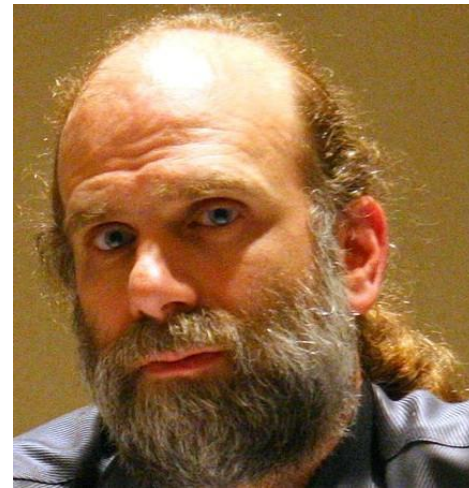
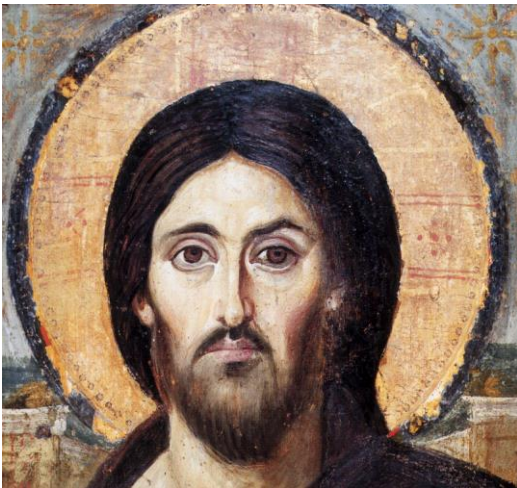
- Finally a Sec. Protocol with += comfort
- Beware of the pitfalls

Final Score:

6

:

3



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

- OWASP Pinning Cheat Sheet:
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/>