

EVALUATION AND IMPLEMENTATION OF SQRL AND U2F AS 2FA FOR CERN SSO



BY

AZQA NADEEM (IT-DI-CSO)

SUPERVISORS

VINCENT BRILLAULT (IT-DI-CSO)

STEFAN LUEDERS (IT-DI-CSO)

PROJECT GOALS

PROJECT GOALS

- Evaluation of SQRL and U2F

PROJECT GOALS

- Evaluation of SQRL and U2F
- Implementation of feasible 2FA algorithm

PROJECT GOALS

- Evaluation of SQRL and U2F
- Implementation of feasible 2FA algorithm
- Integration with CERN Single Sign-on (SSO)

2ND FACTOR AUTHENTICATION

2ND FACTOR AUTHENTICATION



2ND FACTOR AUTHENTICATION



2ND FACTOR AUTHENTICATION



- Username
- Password

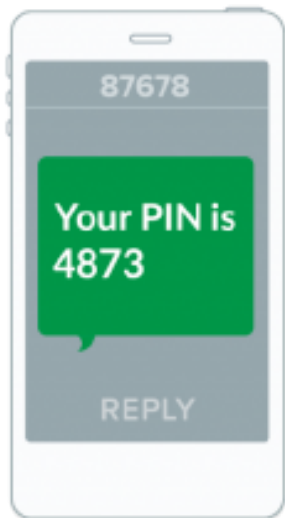
2ND FACTOR AUTHENTICATION

- Cell phone
- Physical token
- Biometrics



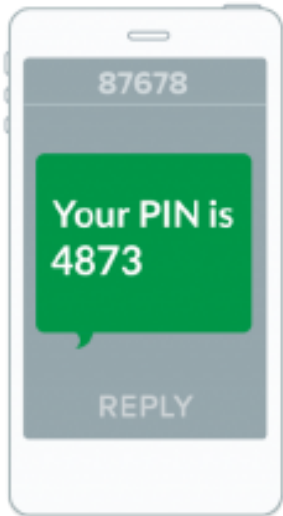
CERN SINGLE SIGN-ON

CERN SINGLE SIGN-ON



SMS

CERN SINGLE SIGN-ON

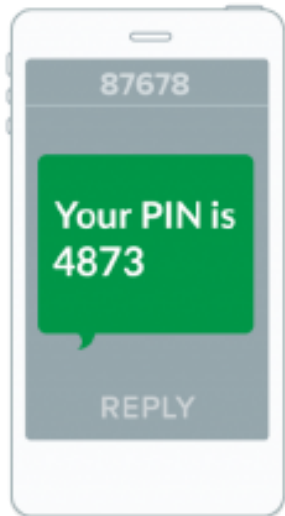


SMS



Google Authenticator

CERN SINGLE SIGN-ON



SMS

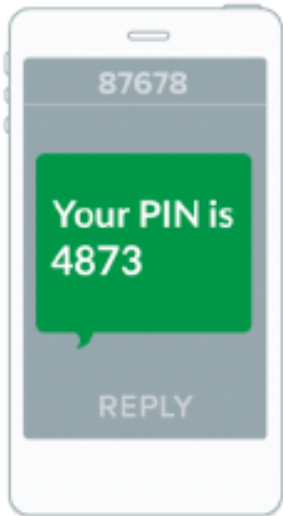


Google Authenticator



Yubikey

CERN SINGLE SIGN-ON



SMS



Google Authenticator



Yubikey



Smartcard

CERN SINGLE SIGN-ON

Can we do better?

SQRL vs. U2F

Secure Quick Reliable Login (SQRL)



Universal 2nd Factor (U2F)



SECURE QUICK RELIABLE LOGIN (SQRL)



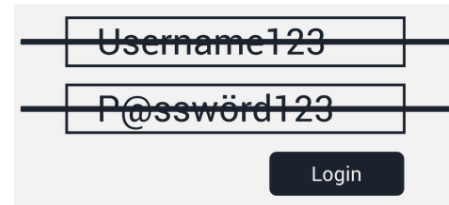
SECURE QUICK RELIABLE LOGIN (SQRL)

- Software based authentication mechanism



SECURE QUICK RELIABLE LOGIN (SQRL)

- Software based authentication mechanism
- Aims to replace username/passwords



A login form with two input fields and a button. The first input field contains the text "Username123" and the second input field contains the text "P@ssw0rd123". Below the input fields is a dark button with the text "Login".



SECURE QUICK RELIABLE LOGIN (SQRL)

- Software based authentication mechanism
- Aims to replace username/passwords
- Scan, tap or click on the QR code

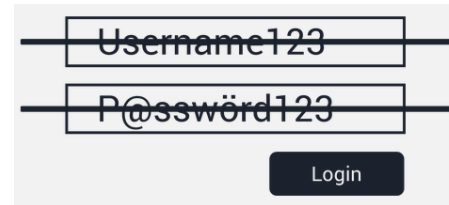


Illustration of a traditional login form with two input fields: "Username123" and "P@ssw0rd123", and a "Login" button below them.



SECURE QUICK RELIABLE LOGIN (SQRL)



SECURE QUICK RELIABLE LOGIN (SQRL)

But... Is it secure?



SECURE QUICK RELIABLE LOGIN (SQRL)

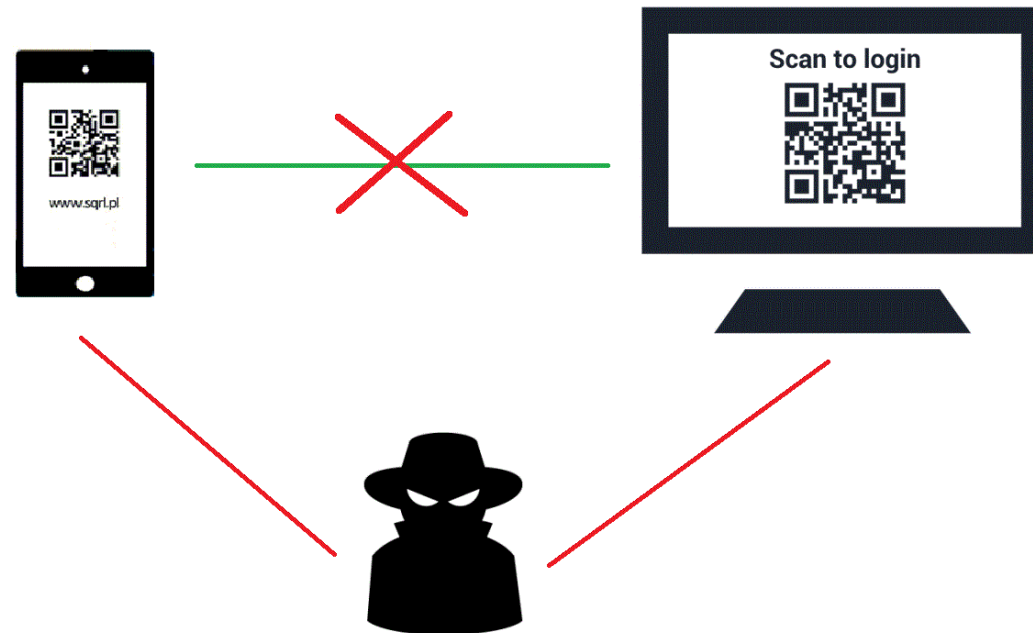
But... Is it secure?

NO!!



SECURE QUICK RELIABLE LOGIN (SQRL)

Man-in-the-middle attack



UNIVERSAL 2ND FACTOR (U2F)



UNIVERSAL 2ND FACTOR (U2F)

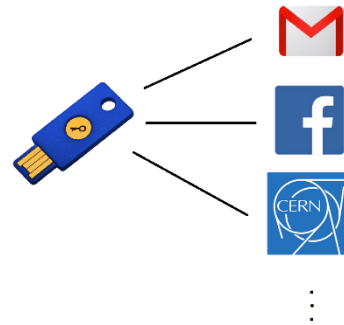
- Physical token



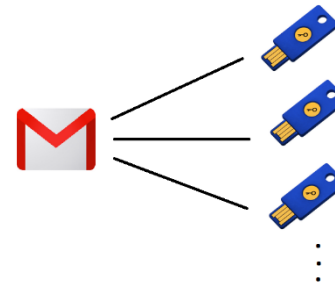
UNIVERSAL 2ND FACTOR (U2F)

- Physical token

One key – Many services



One service – Many keys

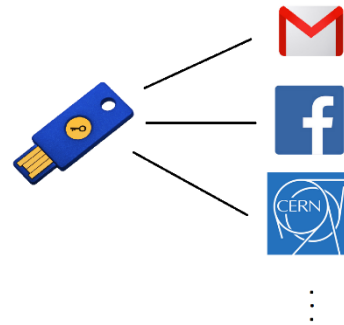


- Many-to-many relationship

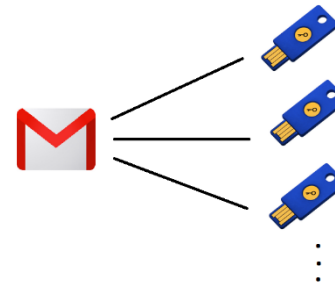
UNIVERSAL 2ND FACTOR (U2F)

- Physical token

One key – Many services



One service – Many keys



- Many-to-many relationship

- Adapted by Google



THE STORY

THE STORY



THE STORY



+

ORACLE[®]
—————
D A T A B A S E

=

THE STORY



+

ORACLE[®]
—————
D A T A B A S E

=

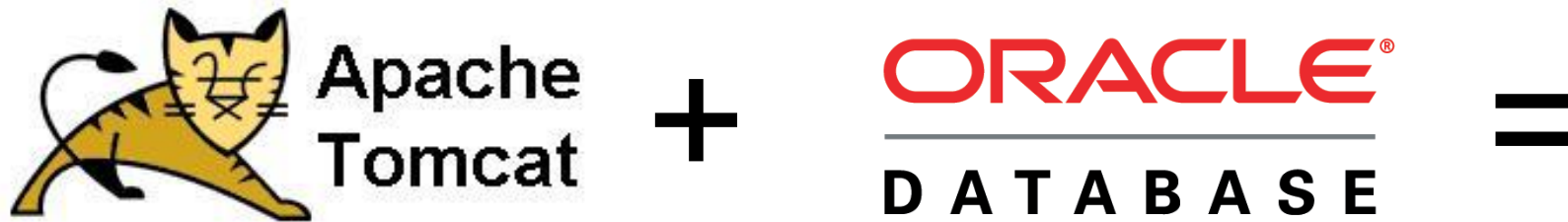


THE STORY

THE STORY



THE STORY



THE STORY



Apache
Tomcat

+

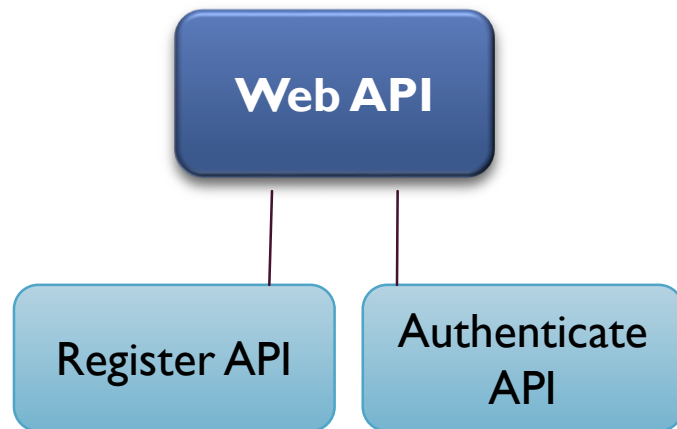
ORACLE®
DATABASE

=

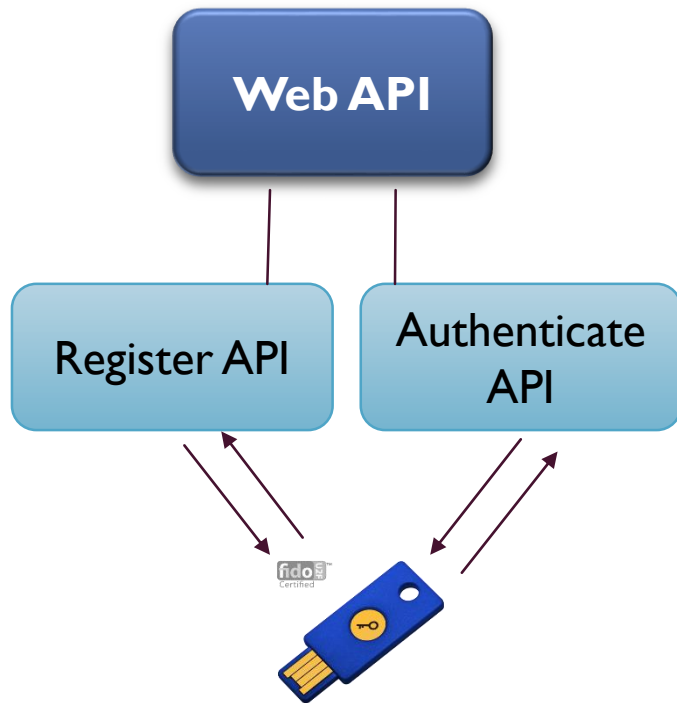


THE STORY

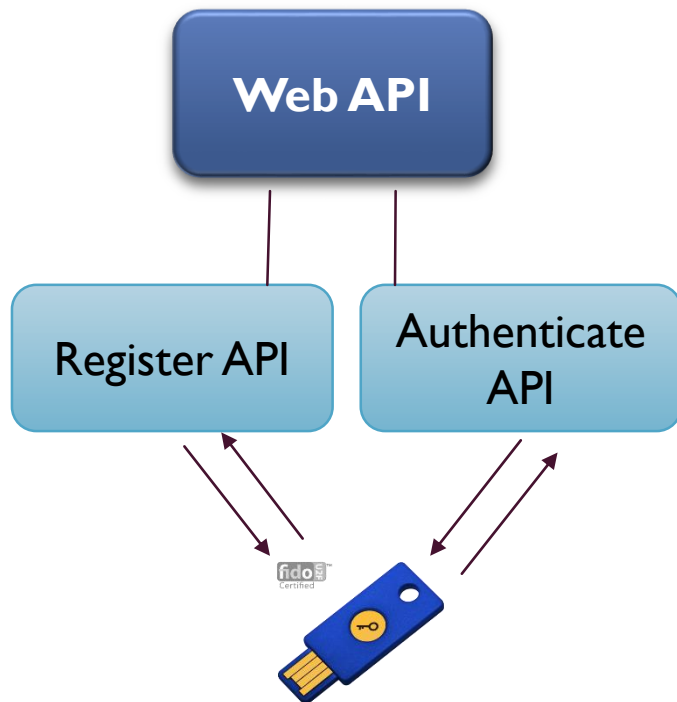
THE STORY



THE STORY

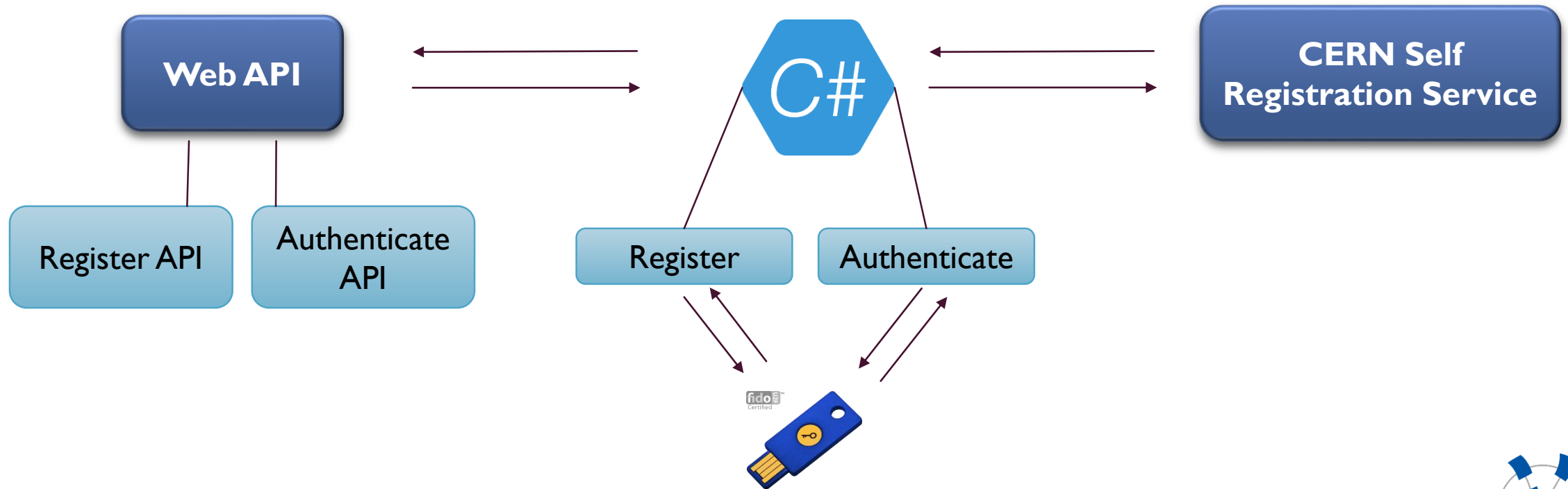


THE STORY



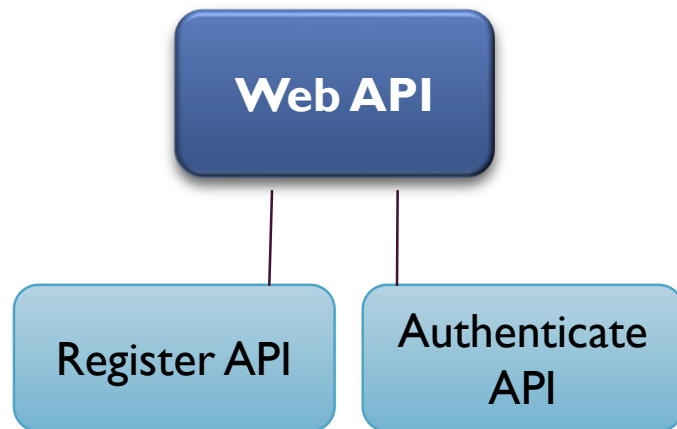
**CERN Self
Registration Service**

THE STORY



THE STORY

THE STORY



THE STORY



