Secure and Usable Mobile Solutions for Authentication and Single Sign-On:

a Methodology for their Design and Assessment

Roberto Carbone - Silvio Ranise - Giada Sciarretta

FONDAZIONE BRUNO KESSLER

SECURITY & TRUST

https://st.fbk.eu/workshop-ifipsc-18

Outline

- Introduction and Problem Statement

  Question 1: Mobile vs Browser-based Authentication

- Design Choices: Security and Usability Problems

  Exercise 1: embedded browser *Exercise 2*: OTP displayed on the screen

- Methodology Overview: TreC Scenario

  Question 2: e-health legal compliance

- Usability Discussion on TreC

  Exercise 3: TreC activation phase

- Conclusions and On-going/Future Work

  Question 3: Pros & Cons of our methodology and TreC solution

  Question 1bis: Mobile vs Browser-based Authentication

Group Division

- Which is your background?

  [ ] IT Security

  [ ] Legal

  [ ] Other

- Which is your position?

  [ ] Master Student

  [ ] PhD Student

  [ ] Researcher

  [ ] Other

Outline

- Introduction and Problem Statement

   *Question 1*: Mobile vs Browser-based Authentication

- Design Choices: Security and Usability Problems

   *Exercise 1*: embedded browser *Exercise 2*: OTP displayed on the screen

- Methodology Overview: TreC Scenario

   *Question 2*: e-health legal compliance

- Usability Discussion on TreC

   *Exercise 3*: TreC activation phase

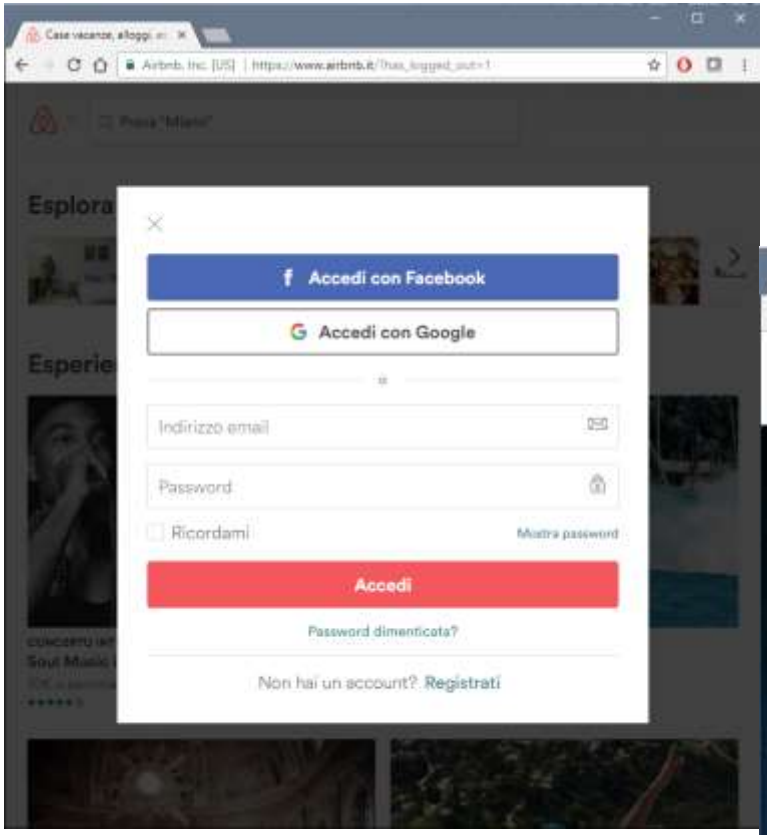
- Conclusions and On-going/Future Work

   *Question 3*: Pros & Cons of our methodology and TreC solution

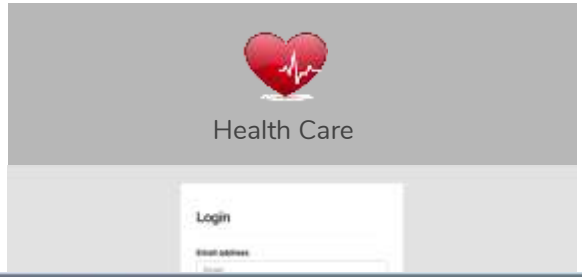
  Question 1bis: Mobile vs Browser-based Authentication

Digital Identities

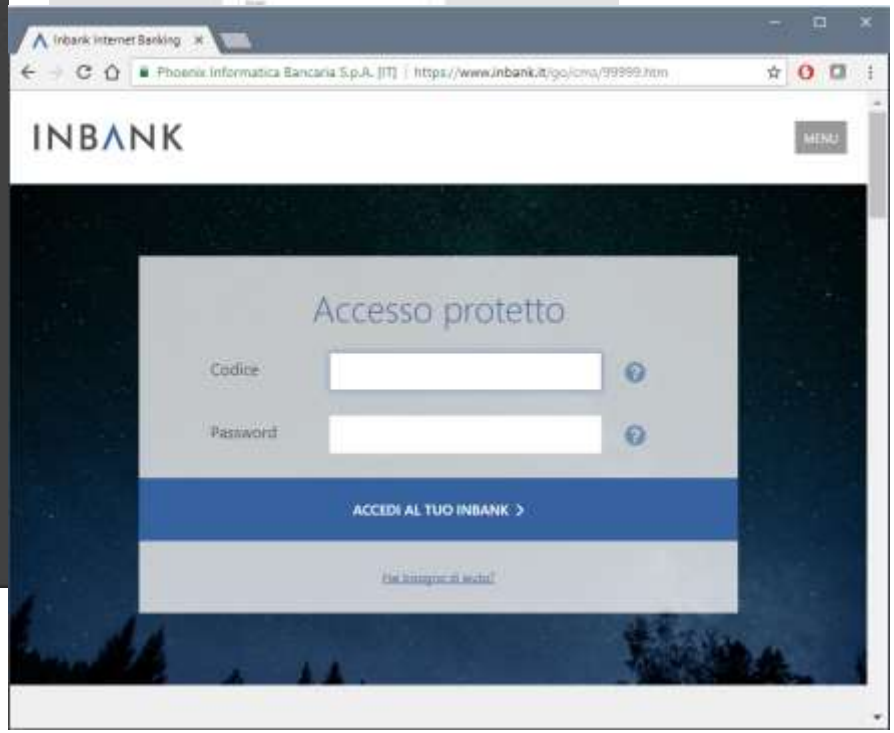
- We use our digital identities everyday, from accessing social apps to security-critical apps.



Personal data



Sensitive data



Password-based Authentication

Password-based authentication is no longer sufficient in terms of security

54%

of people use **5 or fewer** passwords across their entire online life[1]

[1] https://www.telesign.com/resources/research-and-reports/telesign-consumer-account-security-report/
[2] NIST Special Publication 800-63b https://pages.nist.gov/800-63-3/sp800-63b.html#appendix-astrength-of-memorized-secrets

Password-based Authentication

Password-based authentication is no longer sufficient in terms of security

54%

of people use **5 or fewer** passwords across their entire online life[1]

DEMO

https://howsecureismypassword.net/

123456789

Lets_try12

uselongphraseisbetter[2]

[1] https://www.telesign.com/resources/research-and-reports/telesign-consumer-account-security-report/

[2] NIST Special Publication 800-63b https://pages.nist.gov/800-63-3/sp800-63b.html#appendix-astrength-of-memorized-secrets

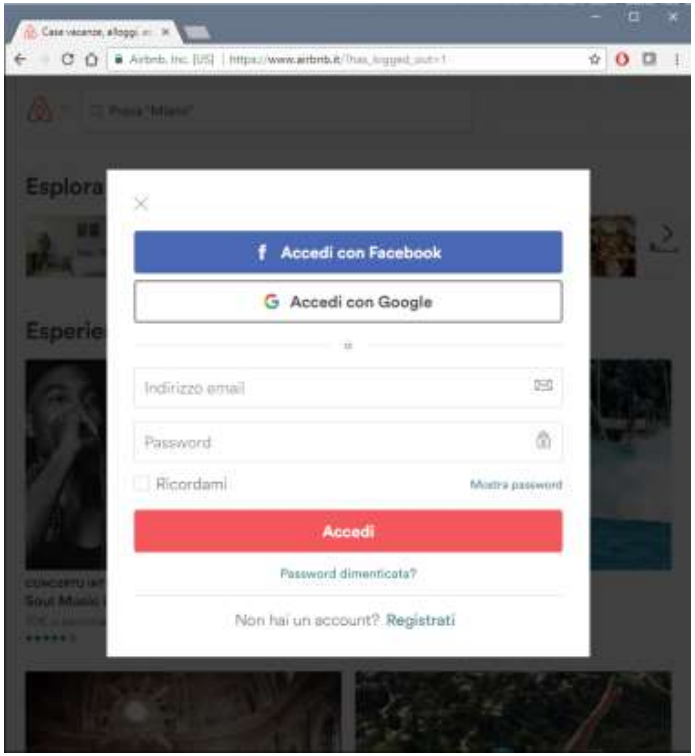
Password-based Authentication + Single Sign-On

Single Sign-On (SSO) allows users to access multiple apps through a single authentication act

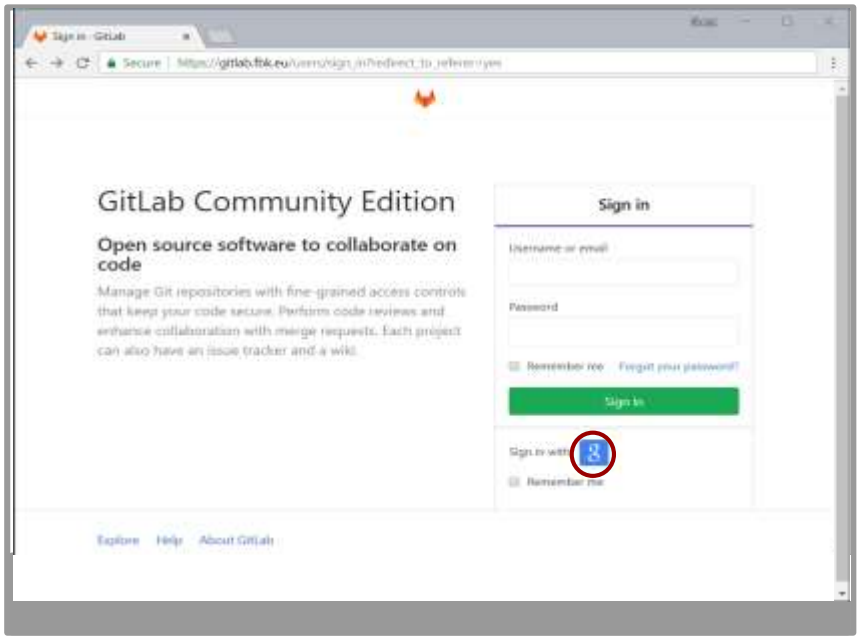
SAML 2.0
OASIS

consolidated, corporate & governmental environments

used for social network (billions of user)



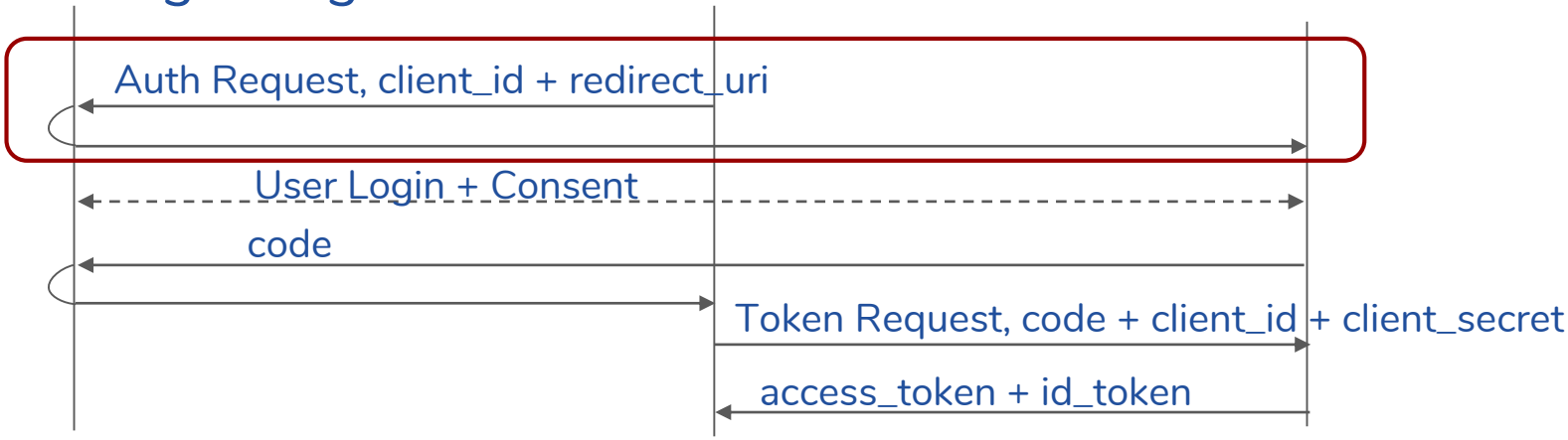
Psw-based Authn and Browser-based SSO Protocol



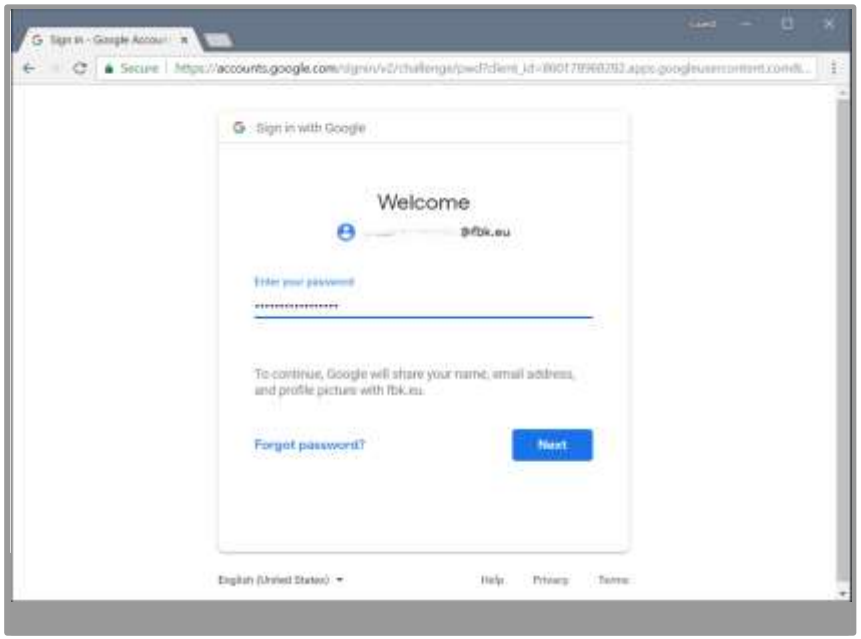
Authorization Code Flow

Browser: SP Login Page | SP backend | OIDC backend

UA



Psw-based Authn and Browser-based SSO Protocol



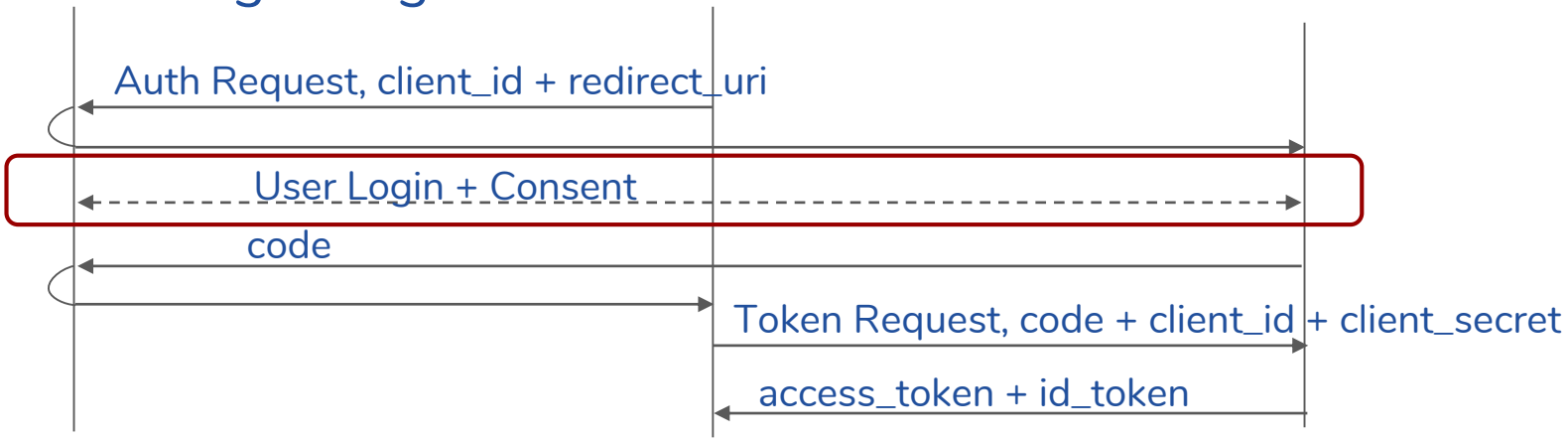
Authorization Code Flow

Browser: **OIDC** Login Page

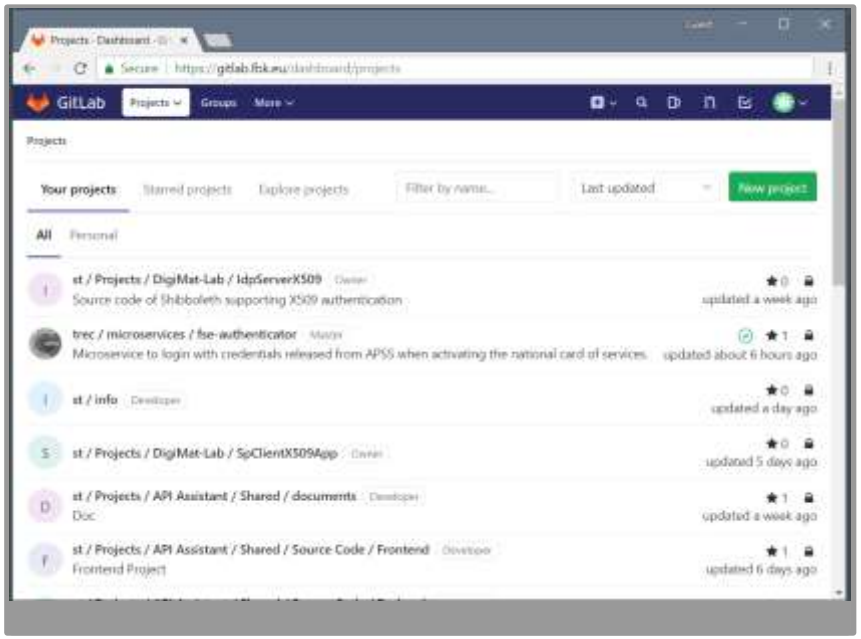
SP backend

OIDC backend

UA



Psw-based Authn and Browser-based SSO Protocol



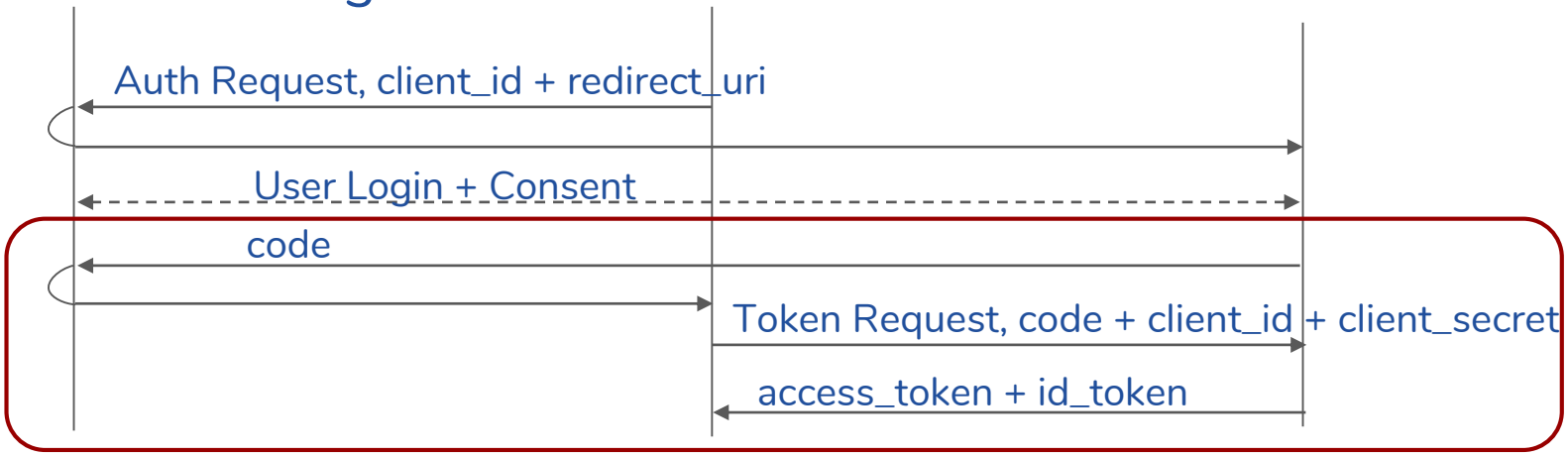
Authorization Code Flow

Browser: **SP Home** Page

SP backend

OIDC backend

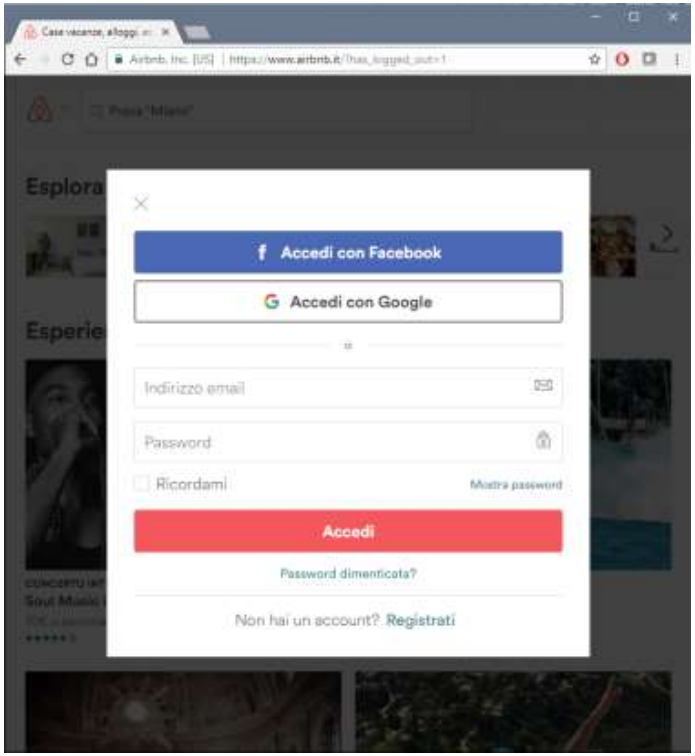
UA



Basic Authentication + Single Sign-On

Single Sign-On (SSO) allows users to access multiple apps through a single authentication act

- *Usability*: only a password to remember for several apps
- *Security*: more complex passwords
- *Usability*: shared sessions
- *Security*: Only 1 password to compromise



→ SSO + Multi-Factor Authentication solutions

Multi-Factor Authentication (MFA)

A procedure based on the use of two or more of the following factors:

knowledge, something only the user knows, e.g., static password, personal identification number;

ownership, something only the user possesses, e.g., token, smart card, mobile phone; and

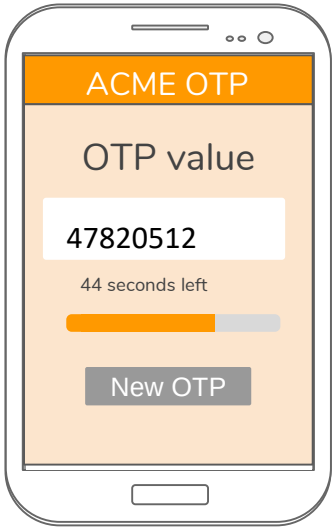
inherence, something the user is, e.g., biometric characteristic, such as a fingerprint.

ECB - European Central Bank. Final guidelines on the security of internet payments. https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29.pdf/f27bf266-580a-4ad0-aaec-59ce52286af0, 2014.

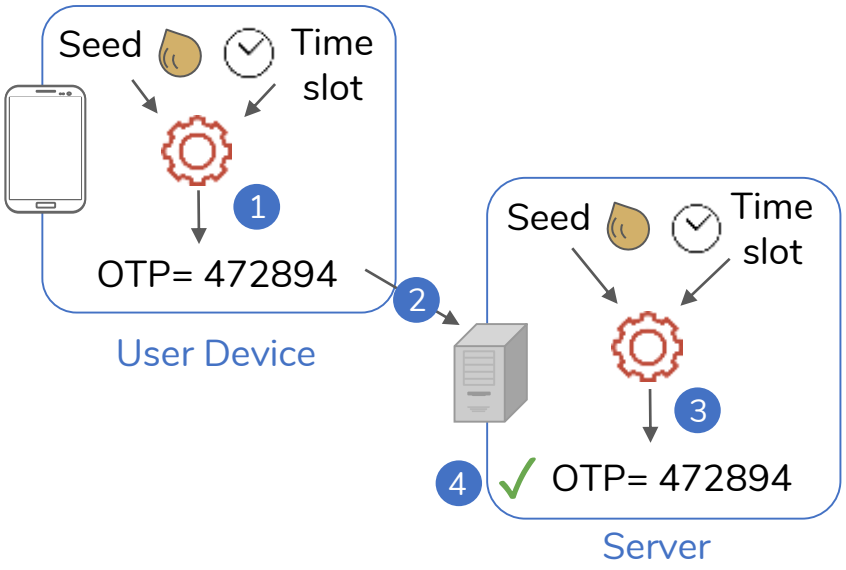
One Time Password Approaches

MFA procedure requires the generation of a **One Time Password (OTP)**

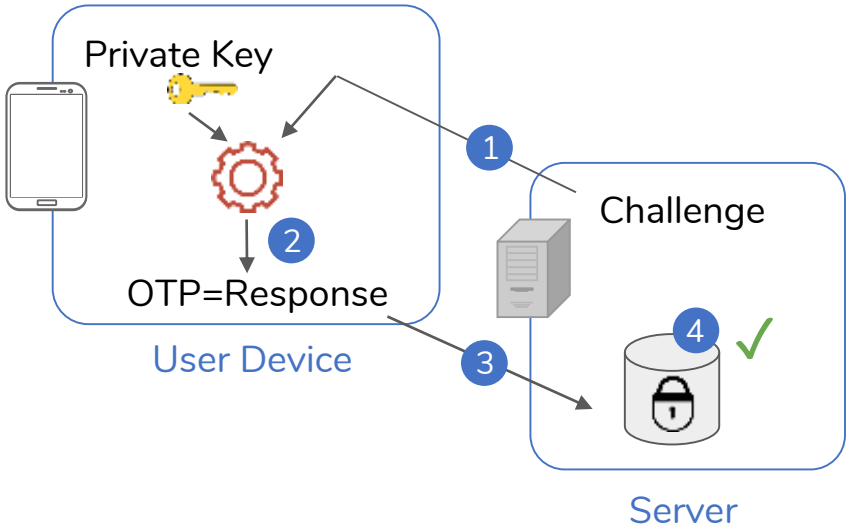
- is an una tantum code with a short expiration
- proofs the possession of the OTP generator (hardware, mobile app...) and/or of the device that received it, and
- [optionally] proofs the knowledge of the PIN used to activate the OTP generator



Time-based OTP (TOTP)



Challenge-Response



Many MFA Solutions on the Market

VASCO

DUO

yubico

Allows **online services** to augment the security of their existing password infrastructure by adding a **strong second factor** to user login

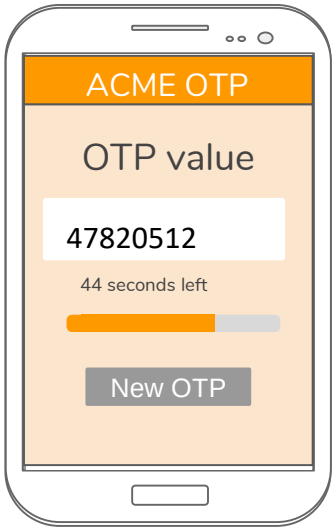
User needs a **FIDO U2F device**

fido alliance

"FIDO is the World's Largest Ecosystem for Standards-Based, Interoperable Authentication"

Main Focus of this Workshop

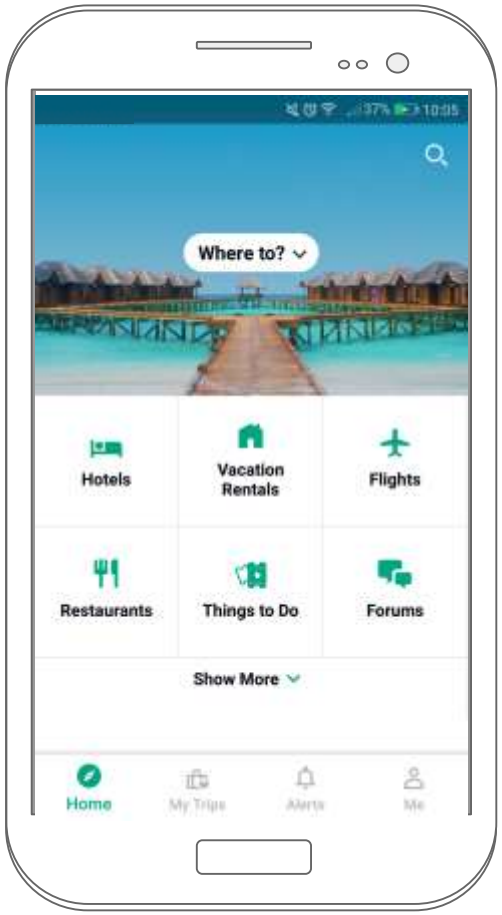
Design and Security Assessment of SSO and MFA Solutions for Mobile Native Applications



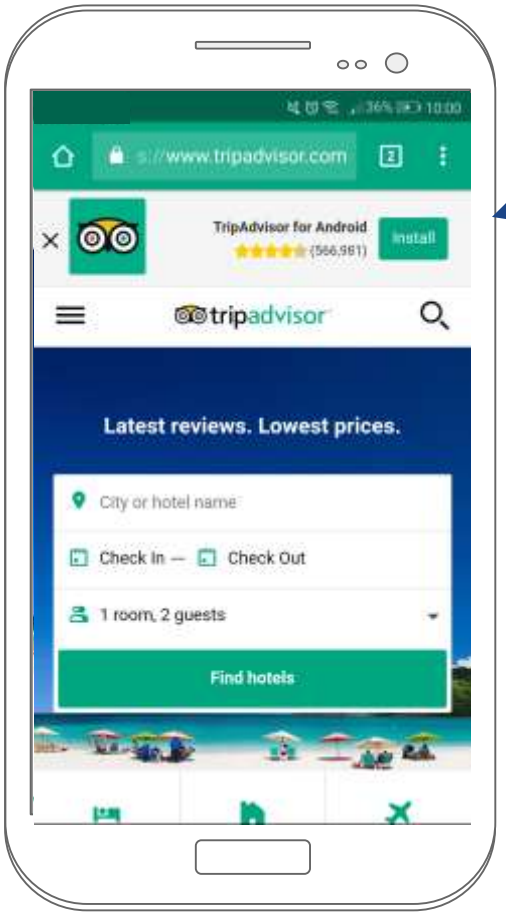
Mobile Native Apps vs Browser-based Apps

market

Native Apps



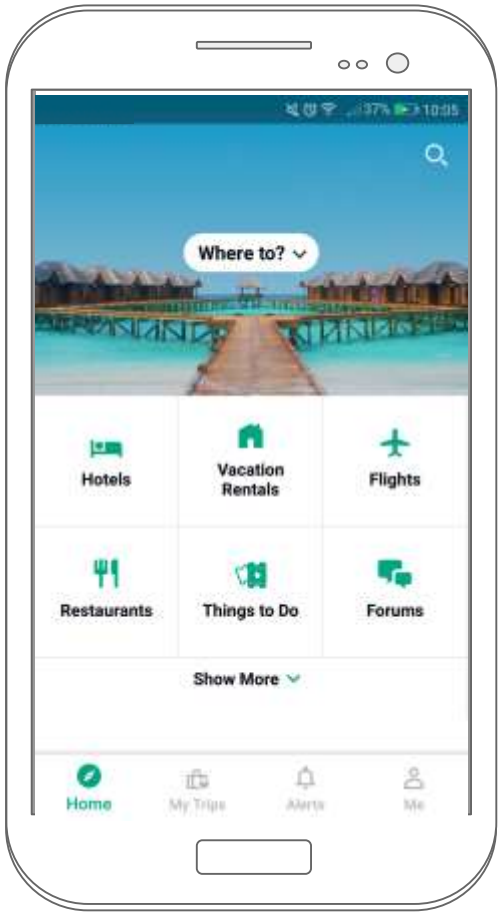
Browser-based Apps



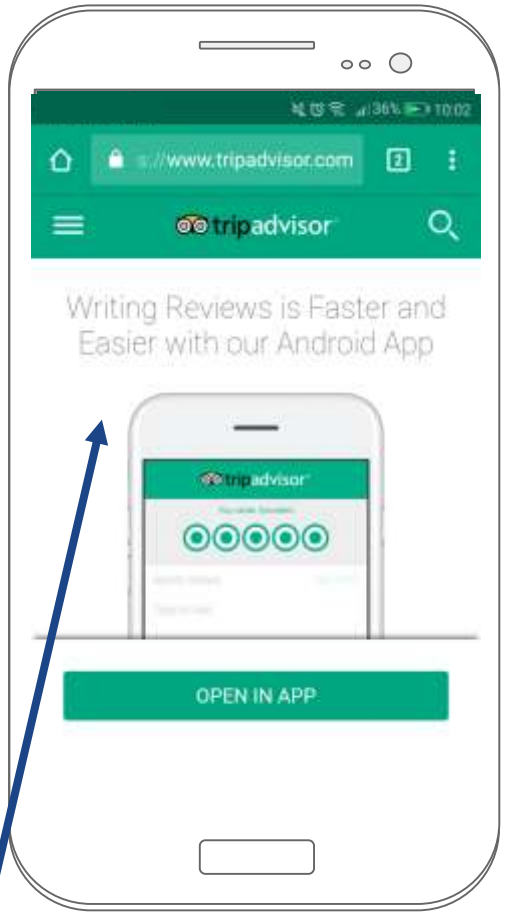
Mobile Native Apps vs Browser-based Apps

market

Native Apps



Browser-based Apps



Read reviews on web. Want to write one? Use the app

5 min left

Can we use browser-based authentication and SSO solutions for mobile apps?

SAML 2.0
OASIS

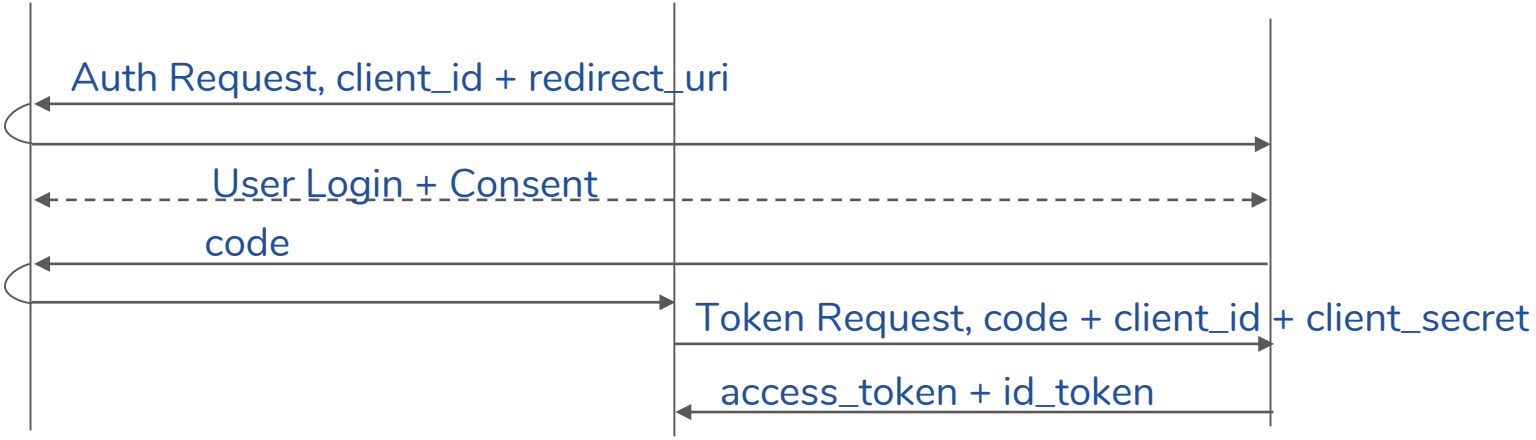
Mobile App vs Browser-based App

NO. Browser-based protocol usages on mobile applications require **detailed understandings** about the protocol specifications and the mobile platform capabilities → a new design is needed

Browser

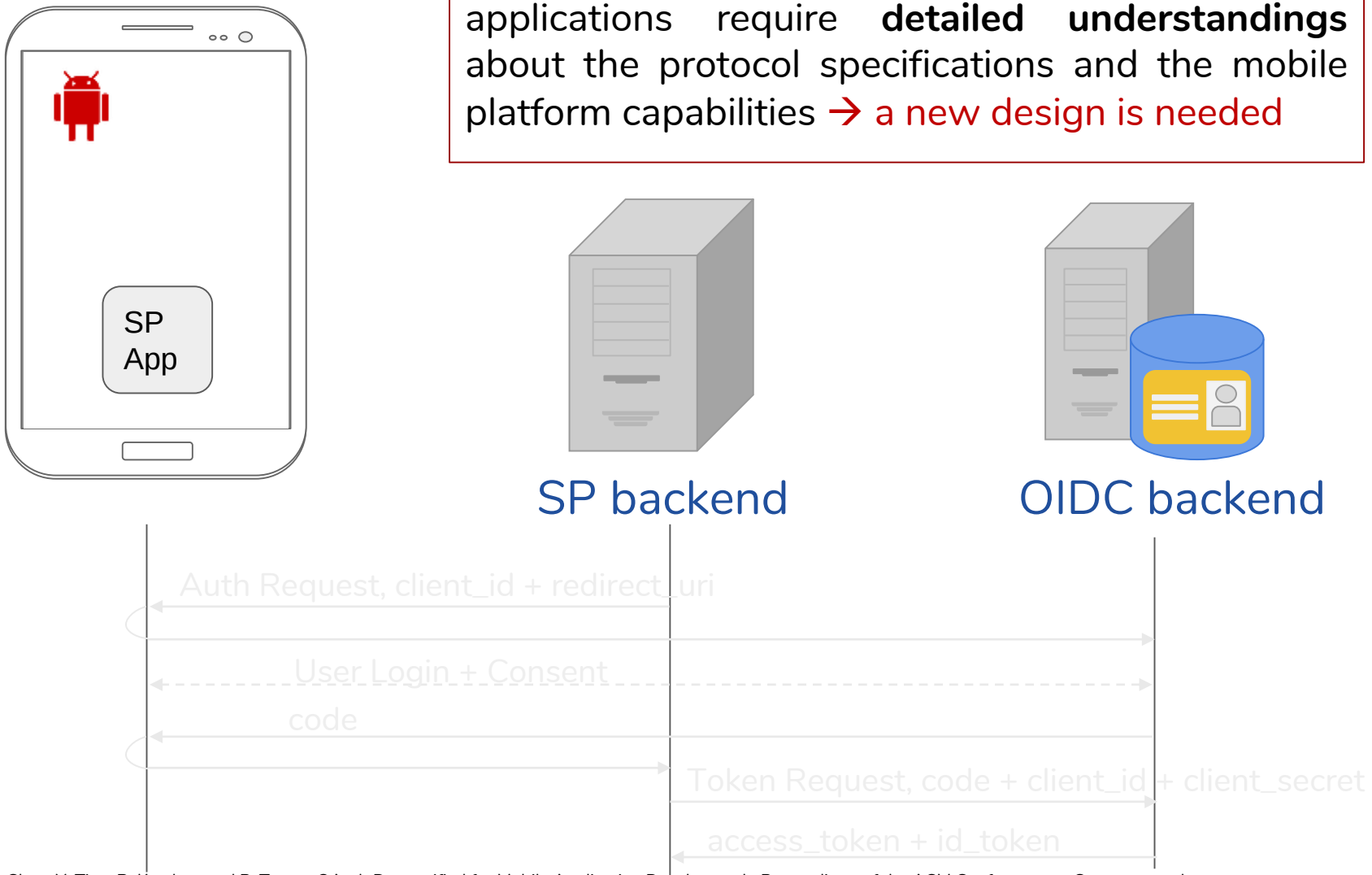
SP backend

OIDC backend



Mobile App vs Browser-based App

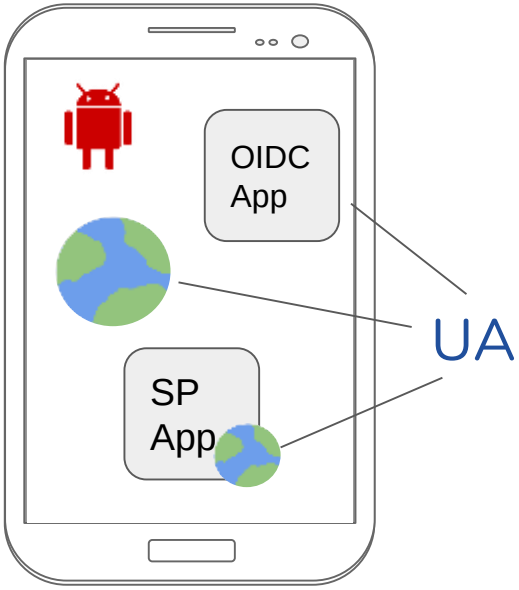
NO. Browser-based protocol usages on mobile applications require **detailed understandings** about the protocol specifications and the mobile platform capabilities → a new design is needed



E. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague. OAuth Demystified for Mobile Application Developers. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2014.
M. Shehab and F. Mohsen. Towards Enhancing the Security of OAuth Implementations in Smart Phones. In IEEE International Conference on Mobile Services (MS), pages 39-46, 2014.

Mobile App vs Browser-based App

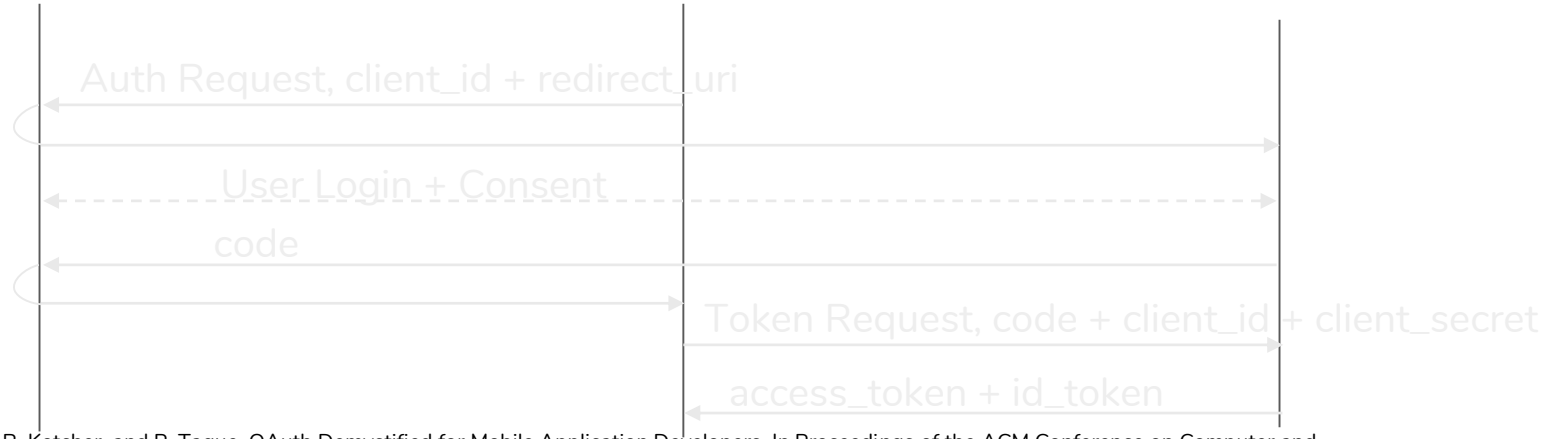
NO. Browser-based protocol usages on mobile applications require **detailed understandings** about the protocol specifications and the mobile platform capabilities → a new design is needed



SP backend

OIDC backend

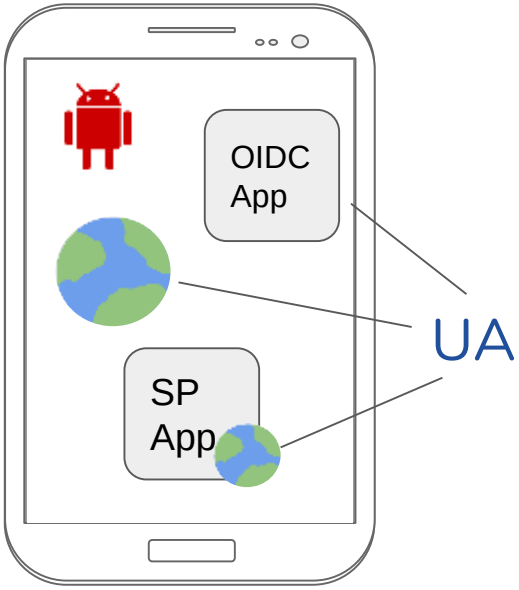
Different redirection mechanisms



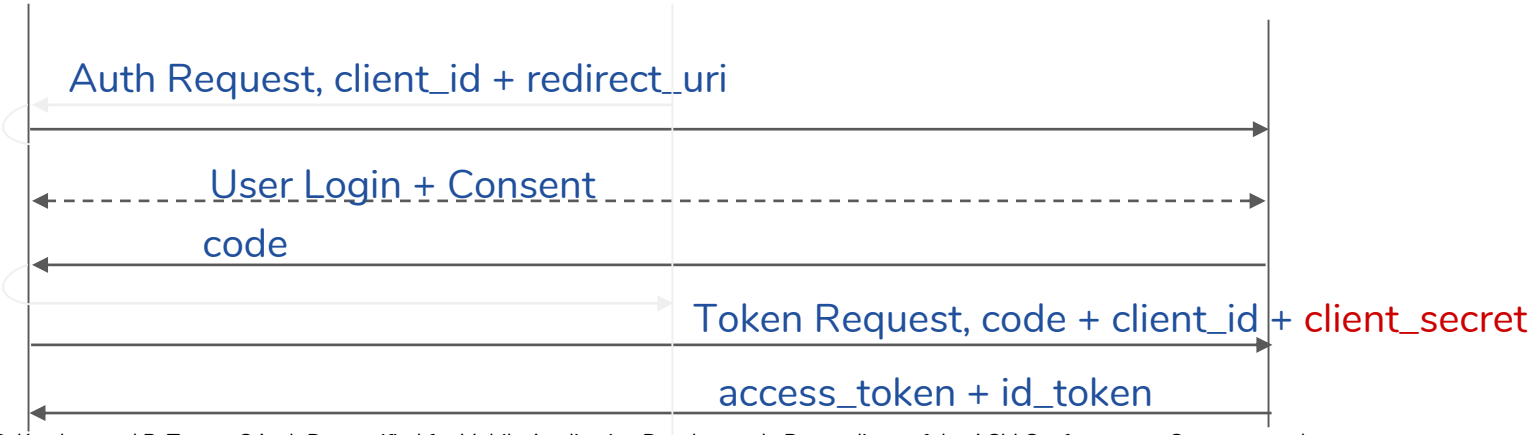
E. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague. OAuth Demystified for Mobile Application Developers. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2014.
M. Shehab and F. Mohsen. Towards Enhancing the Security of OAuth Implementations in Smart Phones. In IEEE International Conference on Mobile Services (MS), pages 39-46, 2014.

Mobile App vs Browser-based App

NO. Browser-based protocol usages on mobile applications require **detailed understandings** about the protocol specifications and the mobile platform capabilities → a new design is needed



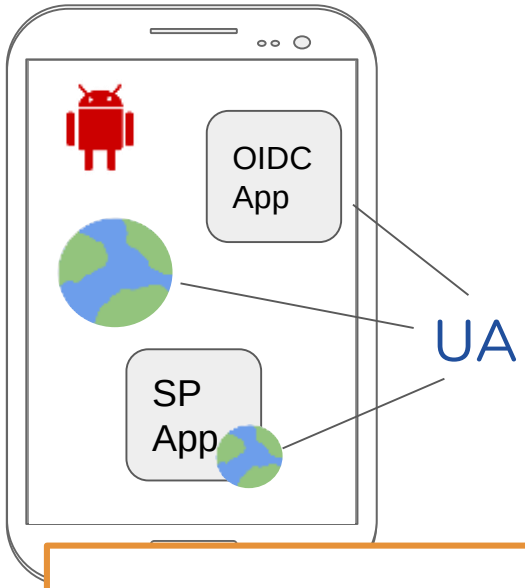
Different redirection mechanisms



E. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague. OAuth Demystified for Mobile Application Developers. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2014.
M. Shehab and F. Mohsen. Towards Enhancing the Security of OAuth Implementations in Smart Phones. In IEEE International Conference on Mobile Services (MS), pages 39-46, 2014.

Mobile App vs Browser-based App

NO. Browser-based protocol usages on mobile applications require **detailed understandings** about the protocol specifications and the mobile platform capabilities → a new design is needed



Different
redirectio
mechanis

nd

Wrong design choices could lead to security and usability problems

Token Request, code + client_id + client_secret

access_token + id_token

E. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague. OAuth Demystified for Mobile Application Developers. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2014.
M. Shehab and F. Mohsen. Towards Enhancing the Security of OAuth Implementations in Smart Phones. In IEEE International Conference on Mobile Services (MS), pages 39-46, 2014.

IdM Protocols for Mobile App

- Proprietary Solutions

- OAuth/OIDC Working Group has released guidelines to support Single Sign-On for mobile native apps
  - **OpenID Connect Native Application Token Agent Core 1.0 (NAPPS)** (2015) - ONLY a DRAFT (now abandoned)
  - **OAuth for native apps [RFC 8252]** (2017) - BEST CURRENT PRACTICE

IdM Protocols for Mobile App: limitations

- Proprietary Solutions

Only self-declared identities (Level of Assurance Low)

- OAuth/OIDC Working Group has released guidelines to s

Technical limitations: non-obvious support to SAML and MFA in native mobile apps

(2017) - BEST CURRENT PRACTICE

Outline

- Introduction and Problem Statement

Question 1: Mobile vs Browser-based Authentication

- Design Choices: Security and Usability Problems

Exercise 1: embedded browser *Exercise 2*: OTP displayed on the screen

- Methodology Overview: TreC Scenario

Question 2: e-health legal compliance

- Usability Discussion on TreC

Exercise 3: TreC activation phase

- Conclusions and On-going/Future Work

Question 3: Pros & Cons of our methodology and TreC solution

Question 1bis: Mobile vs Browser-based Authentication

Design Choices

Designer

Design Choices

Designer

TODO List

1. design of an IdM Solution
   - How to establish trust?
   - How do communication channels work?
2. security analysis

Design Choices

Designer

TODO List

1. design of an IdM Solution
   - How to establish trust?
   - How do communication channels work?
   - Legal aspect?!?
2. security analysis

Design Choices

Designer

TODO List

1. design of an IdM Solution
   - How to establish trust?
   - How do communication channels work?
   - Legal aspect?!?
2. security analysis
   - Which tool? How to formalize the security properties?

Design Choices

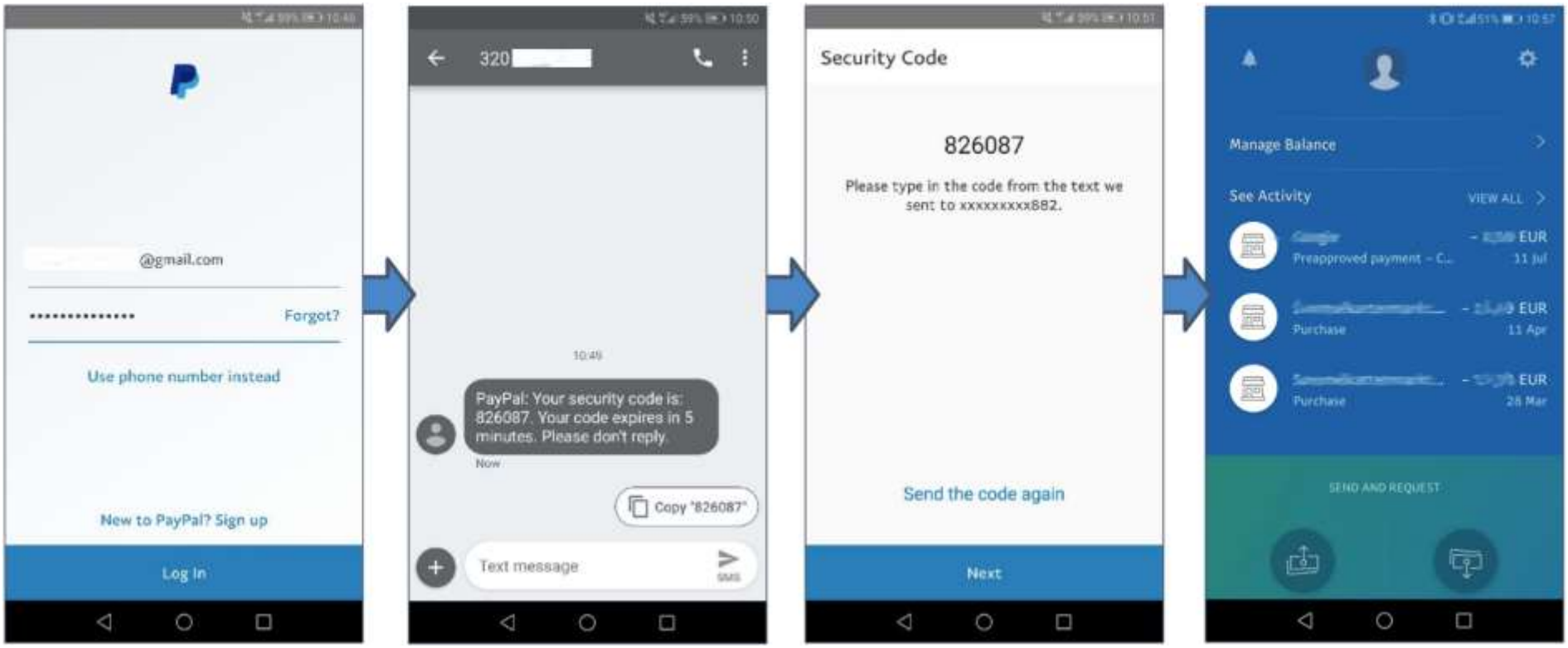
TODO List

1. design of an IdM Solution
   - How to establish trust?
   - How do communication ch… work?
   - … the security properties?

Wrong design choices could lead to security and usability problems

Example of wrong design

2FA Choice: SMS



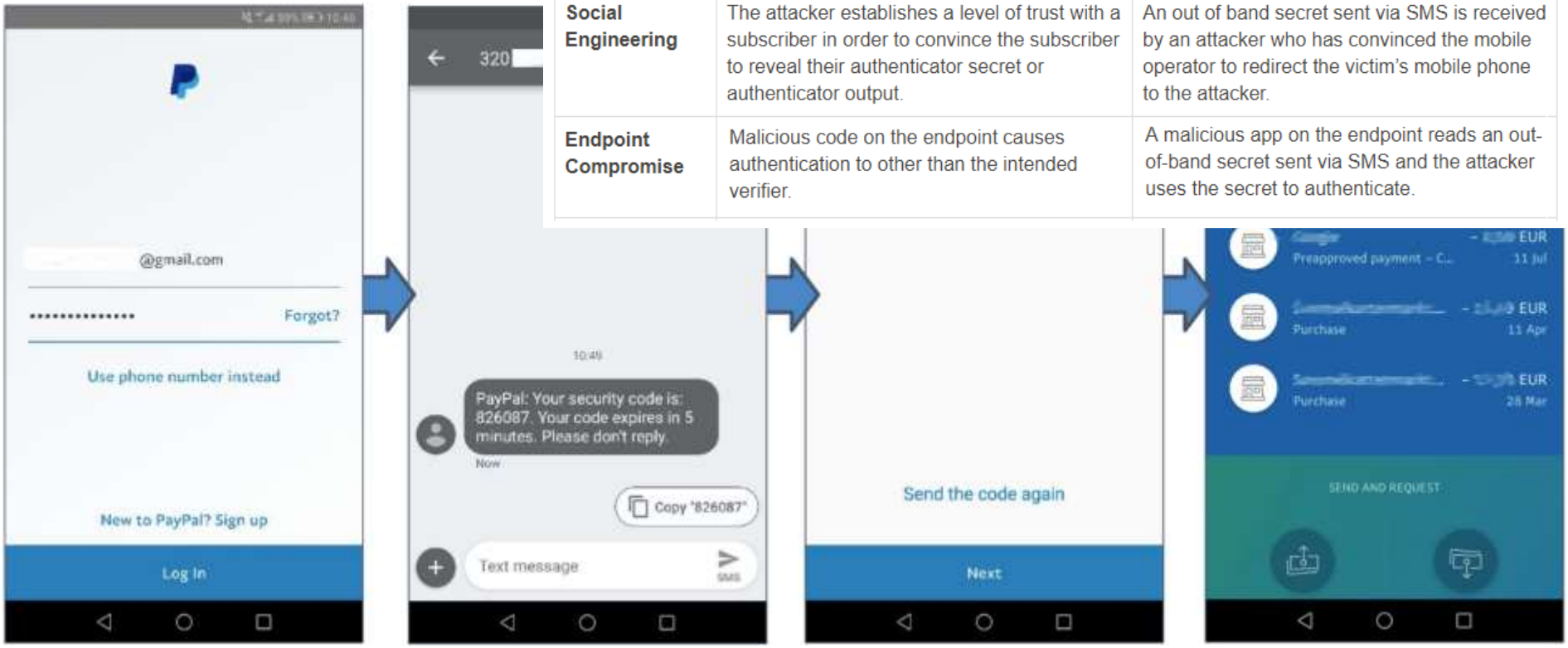
Example of wrong design

2FA Choice: SMS

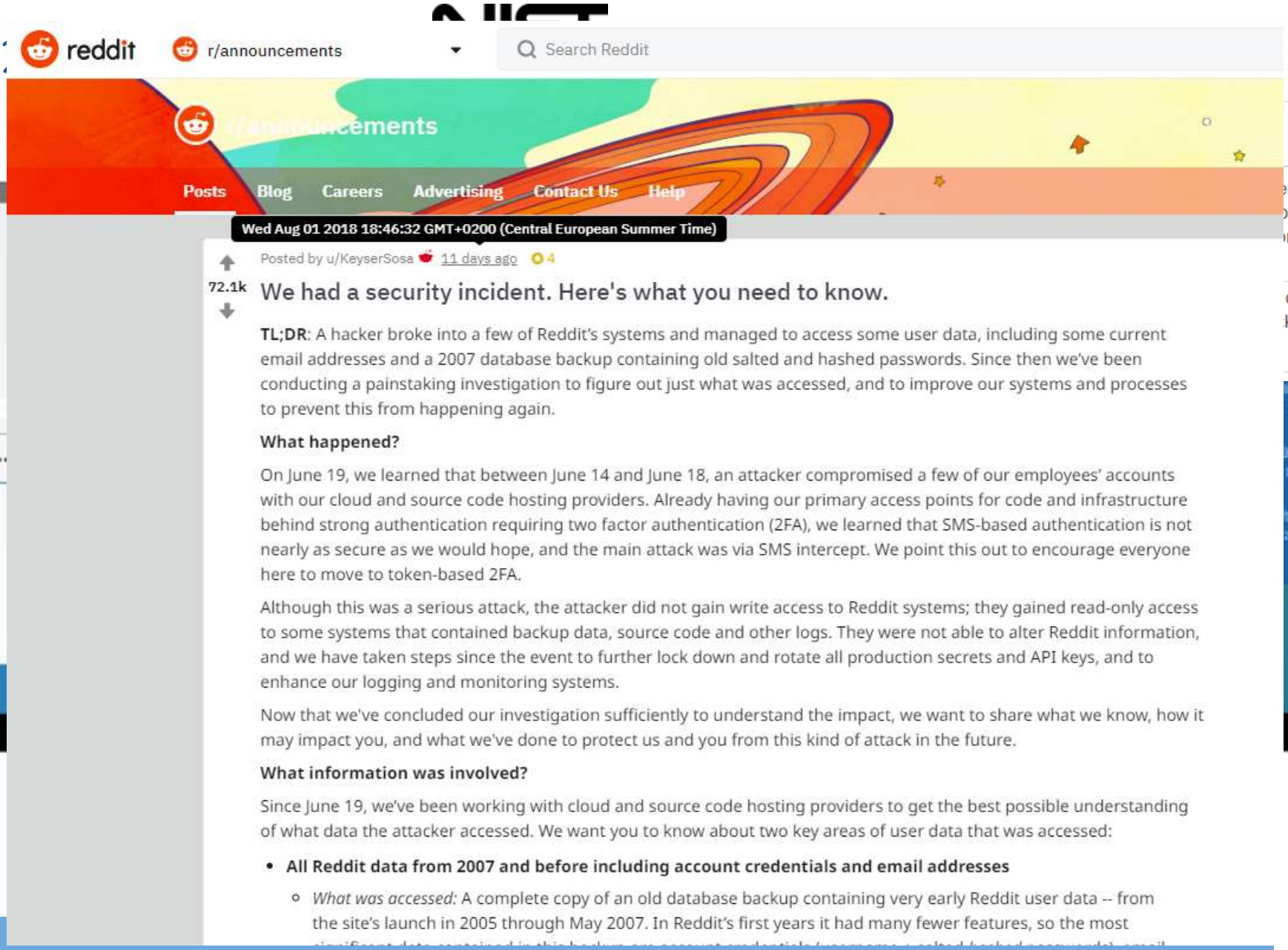
NIST

Table 8-1 Authenticator Threats

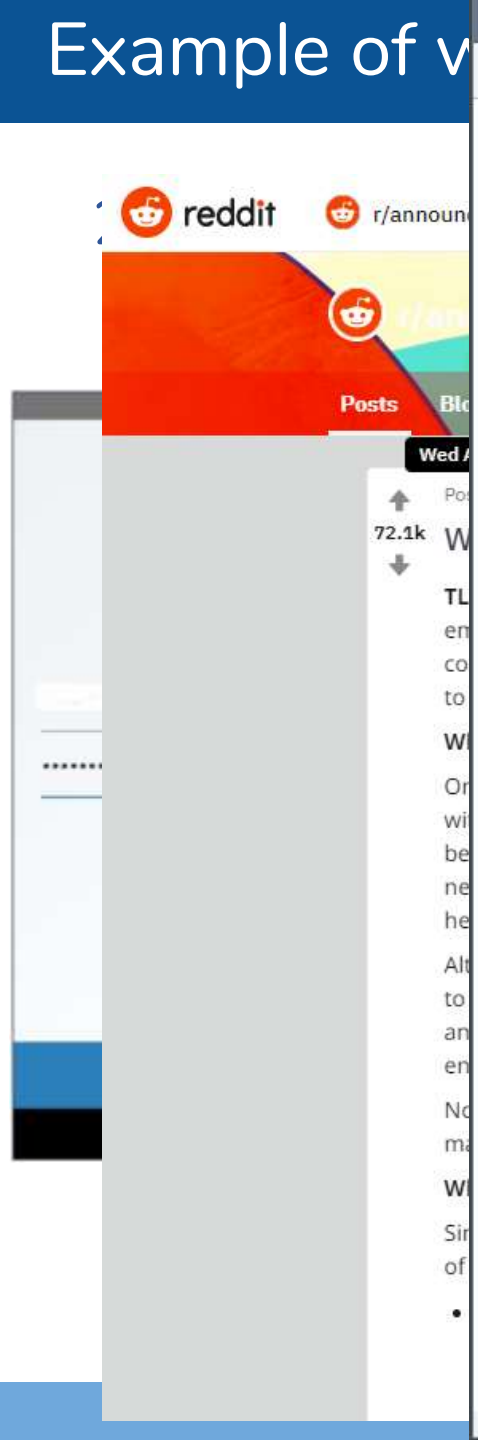
Authenticator Threat/Attack	Description	Examples
Social Engineering	The attacker establishes a level of trust with a subscriber in order to convince the subscriber to reveal their authenticator secret or authenticator output.	An out of band secret sent via SMS is received by an attacker who has convinced the mobile operator to redirect the victim's mobile phone to the attacker.
Endpoint Compromise	Malicious code on the endpoint causes authentication to other than the intended verifier.	A malicious app on the endpoint reads an out-of-band secret sent via SMS and the attacker uses the secret to authenticate.



Example of wrong design



Example of v



AT&T Sued Over $24 Mil

Information Security Media Group, Corp. [US] | https://www.databreachtoday.com/att-sued-over-24-million-cryptocurre...

SIM hijacking attacks can result in account compromises by stealing one-time passcodes sent over SMS.

A cryptocurrency investor is suing AT&T for $224 million, alleging he lost $24 million in virtual currency after the carrier failed to stop two separate attacks where his phone number was commandeered by attackers.

See Also: Preventing an Inside Job: Detection, Technology and People

Michael Terpin, who runs an investment group called Bit Angels and is involved in the cryptocurrency community, is seeking $24 million in compensatory damages and $200 million in punitive damages, according to the lawsuit, which was filed on Wednesday in federal court in Los Angeles.

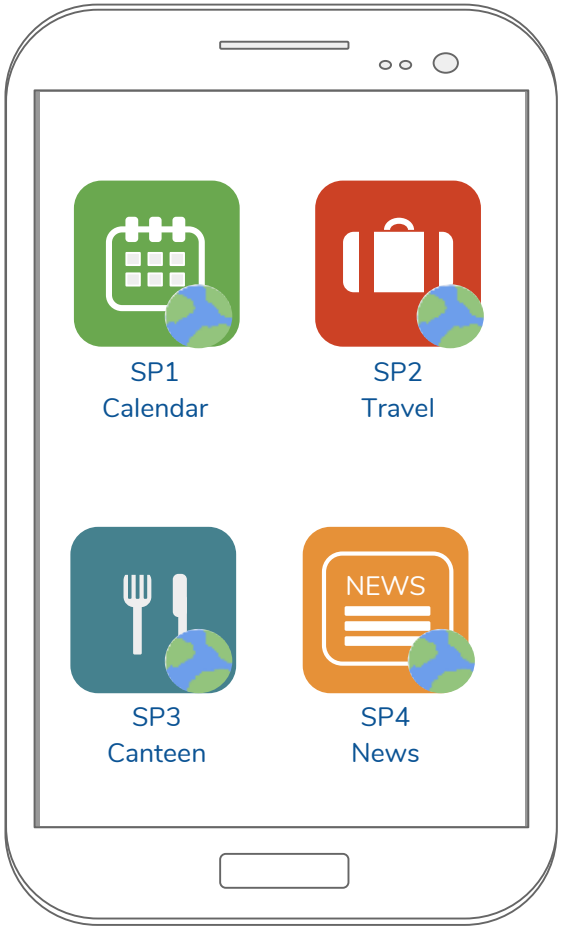
Terpin was a victim of two SIM hijacking attacks, which are sometimes referred to as SIM swapping or port-out scams. The attack involves an attacker convincing a mobile provider to move a number to a different SIM card. Many times, the targets of such attackers are those with large holdings of bitcoin and other cryptocurrencies (see *Cryptocurrency Theft: $1.1 Billion Stolen in Last 6 Months*).

Attackers can successfully take over someone's phone number by tricking an employee at a carrier that they're the legitimate account holder. In other cases, telecom employees may be crooked and actually be

Exercise 1

User Agent (UA) Choice: embedded browser

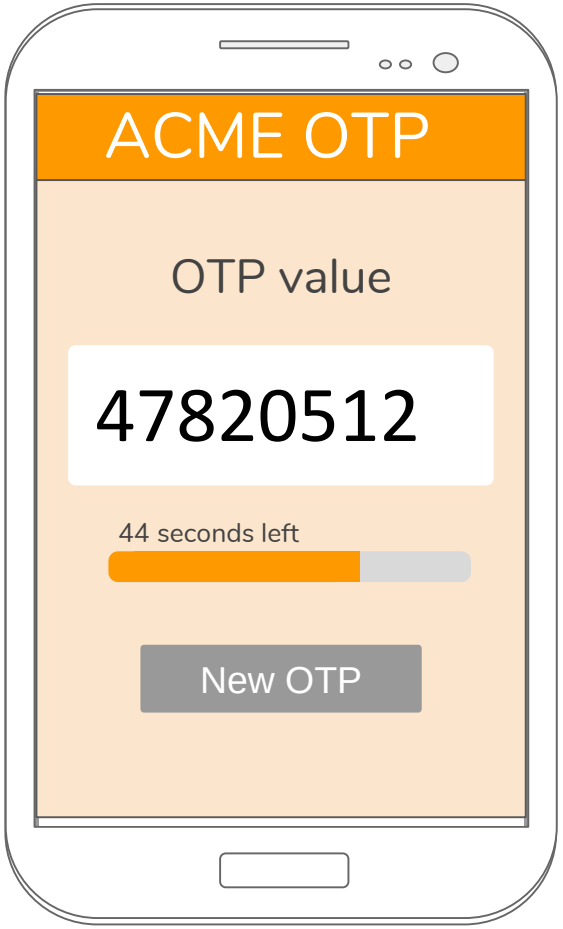
1. How does an embedded browser work?
2. Are there any security issues?
3. What happens to the user experience when accessing multiple apps?



Exercise 2

OTP Choice: app that shows the OTP value

1. What happens to the user experience when accessing a mobile native app?
2. Are there any security issues?
3. List one or more OTP choice alternatives



…doing Exercise 1 and 2…

10 min left

Exercise 1 (UA Choice): embedded browser

1. How does an embedded browser work?
2. Are there any security issues?
3. What happens to the user experience when accessing multiple apps?

Exercise 2 (OTP Choice): app that shows the OTP value

1. What happens to the user experience when accessing a mobile native app?
2. Are there any security issues?
3. List one or more OTP choice alternatives

Exercise 1: Answer 1 - definition

User Agent (UA) Choice: embedded browser

"a user-agent hosted inside the native app itself (such as via a web-view), with which the app has control over to the extent it is capable of accessing the cookie storage and/or modifying the page content"

OAuth Working Group. OAuth 2.0 for Native Apps. https://tools.ietf.org/html/draft-ietf-oauth-native-apps-09.

Exercise 1: Answer 2 - security

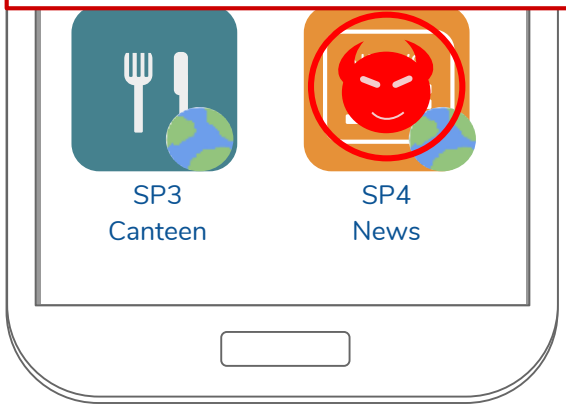
User Agent (UA) Choice: embedded browser

Security

Impact: tha attacker can access other SP apps as the user

SP4 News adds some javascript to read user's credentials

```
webView.evaluateJavascript(
 "(function() { return
document.getElementById('password').value;})();",
 new ValueCallBack<String>() {
 @Override public void onReceiveValue(String s){
 Log.d("WebViewField",s);
 }
});
```



T. Luo, H. Hao, W. Du, Y. Wang, and H. Yin, "Attacks on WebView in the Android system," in *Proceedings of the Annual Computer Security Applications Conference*. ACM, 2011, pp. 343–352.

Exercise 1: Answer 3 - usability

User Agent (UA) Choice: embedded browser

Security

Impact: tha attacker can access other SP apps as the user

Usability: no SSO

IdP

OAuth Working Group. OAuth 2.0 for Native Apps. https://tools.ietf.org/html/draft-ietf-oauth-native-apps-09.

T. Luo, H. Hao, W. Du, Y. Wang, and H. Yin, "Attacks on WebView in the Android system," in *Proceedings of the Annual Computer Security Applications Conference*. ACM, 2011, pp. 343–352.

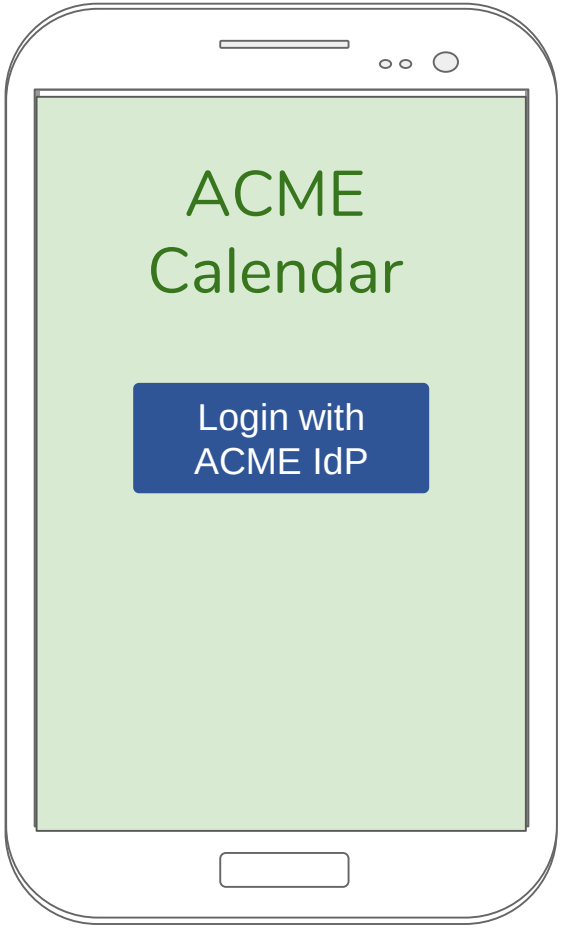
Exercise 2: Answer 1 - usability

OTP Choice: app that shows the OTP value

Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

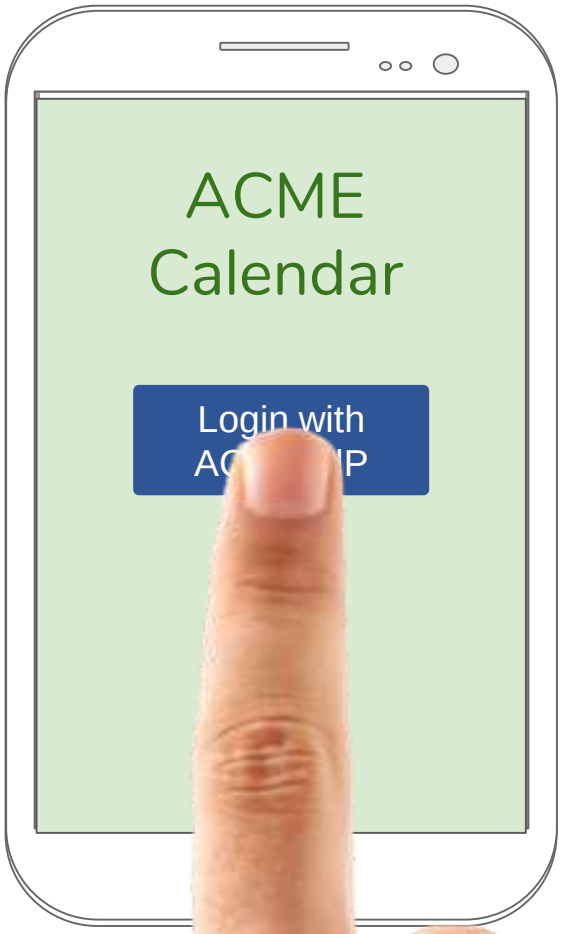
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

OTP Choice: app that shows the OTP value

Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

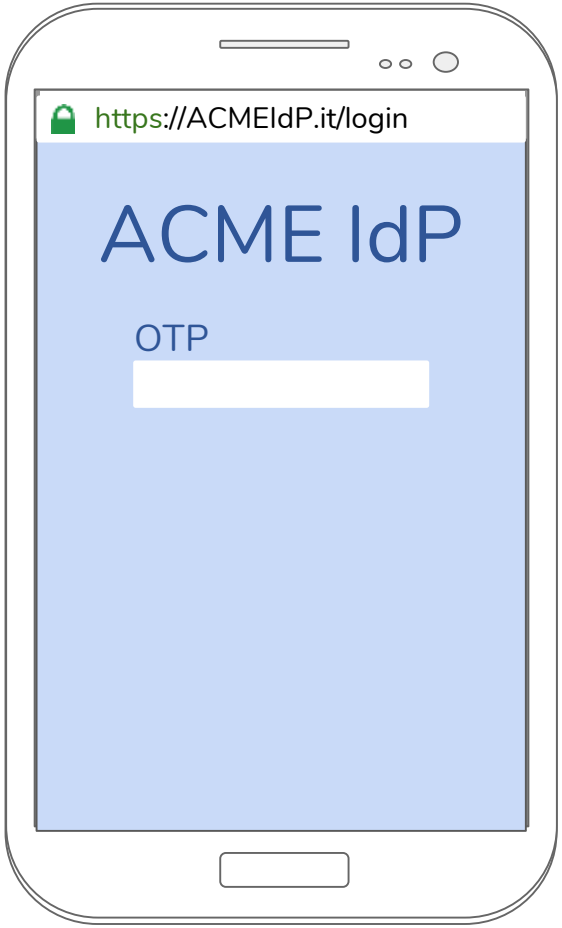
Exercise 2: Answer 1 - usability

OTP Choice: app that shows the OTP value

Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

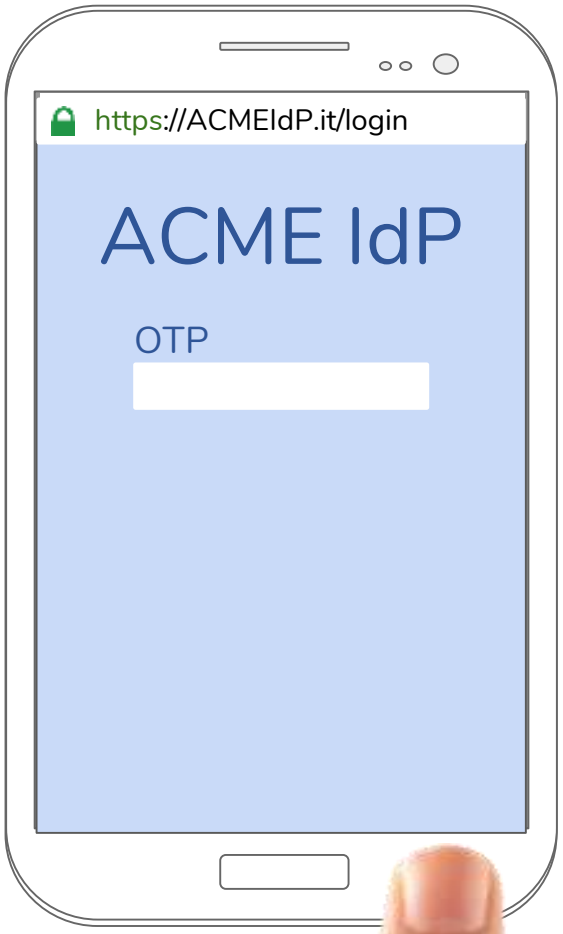
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

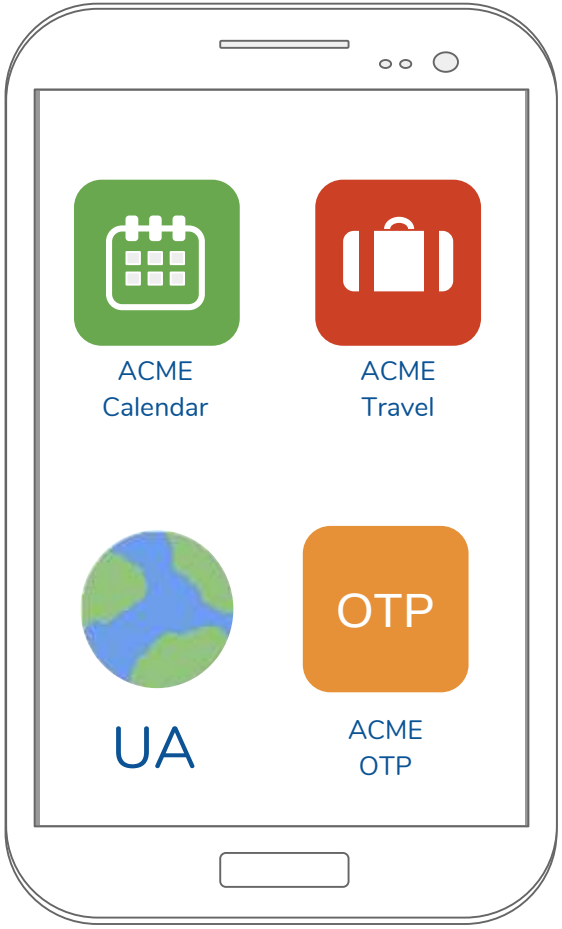
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

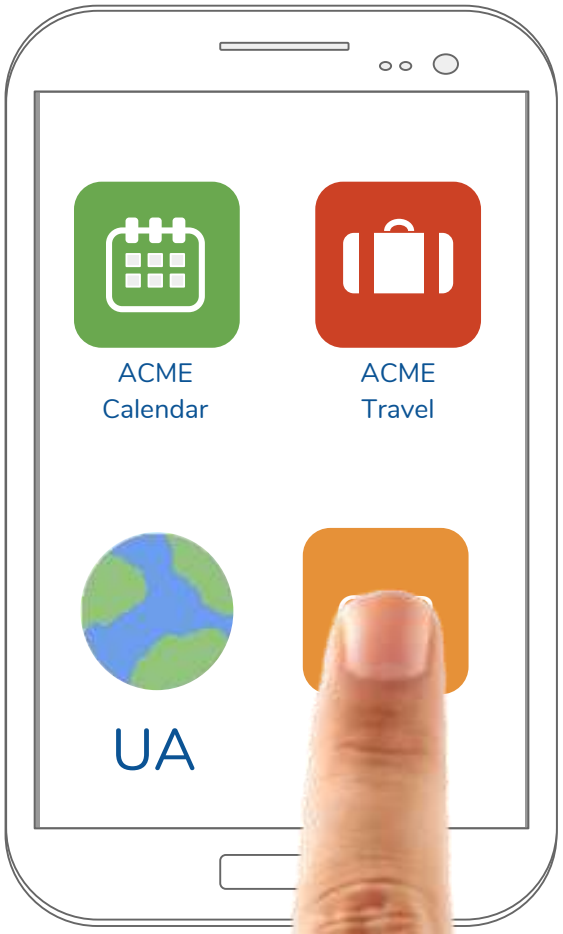
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

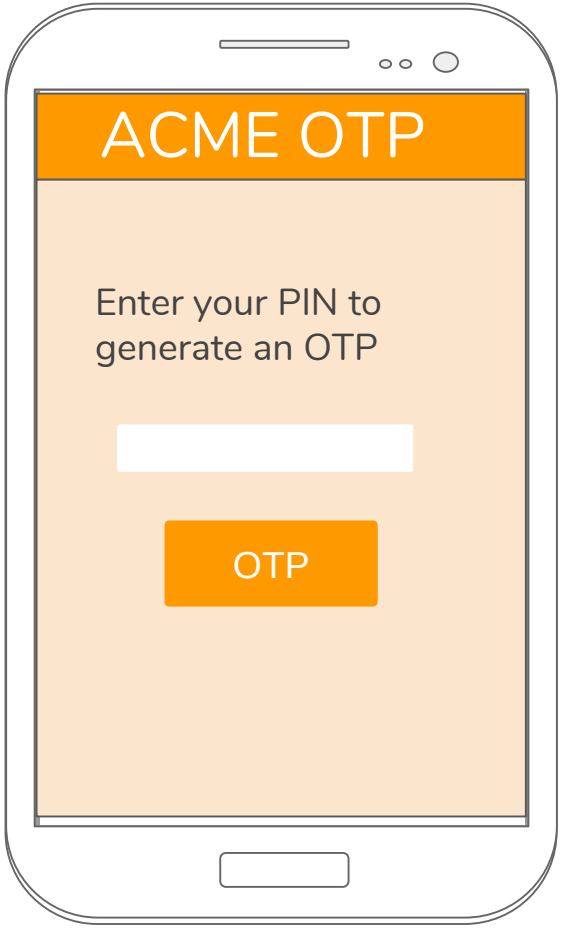
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

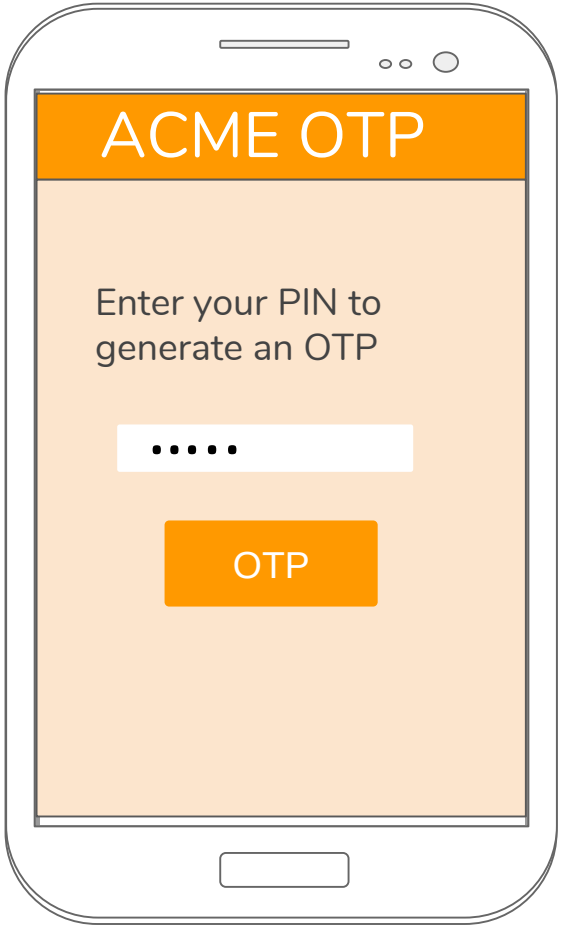
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

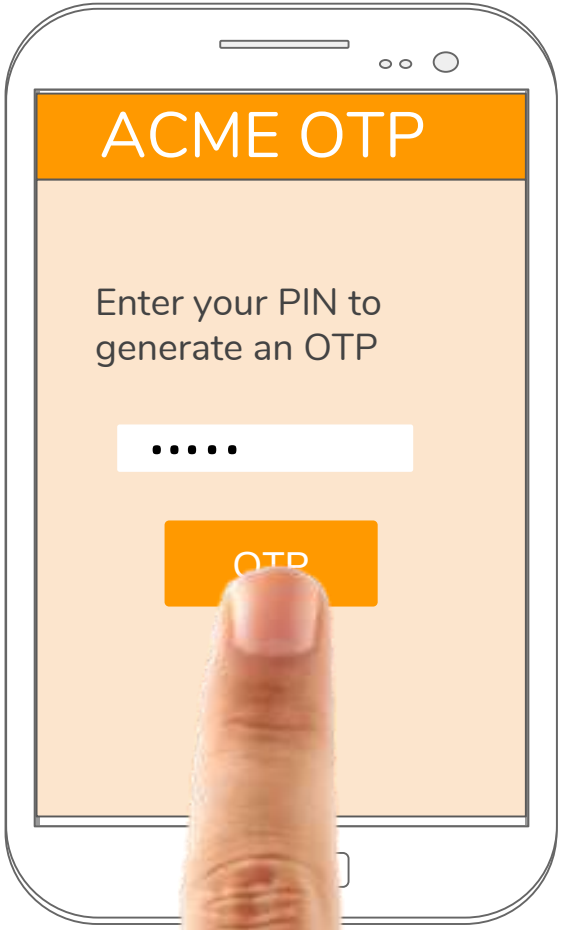
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

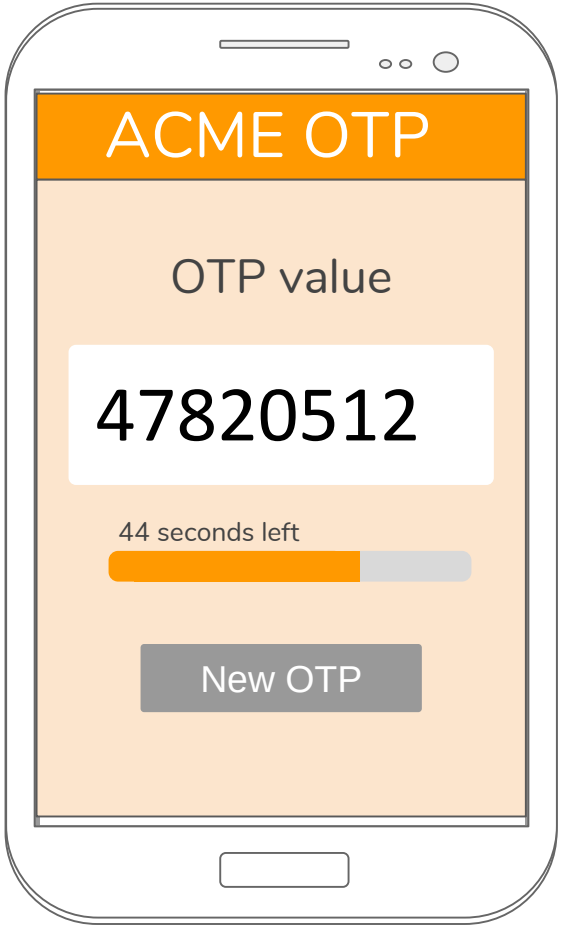
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

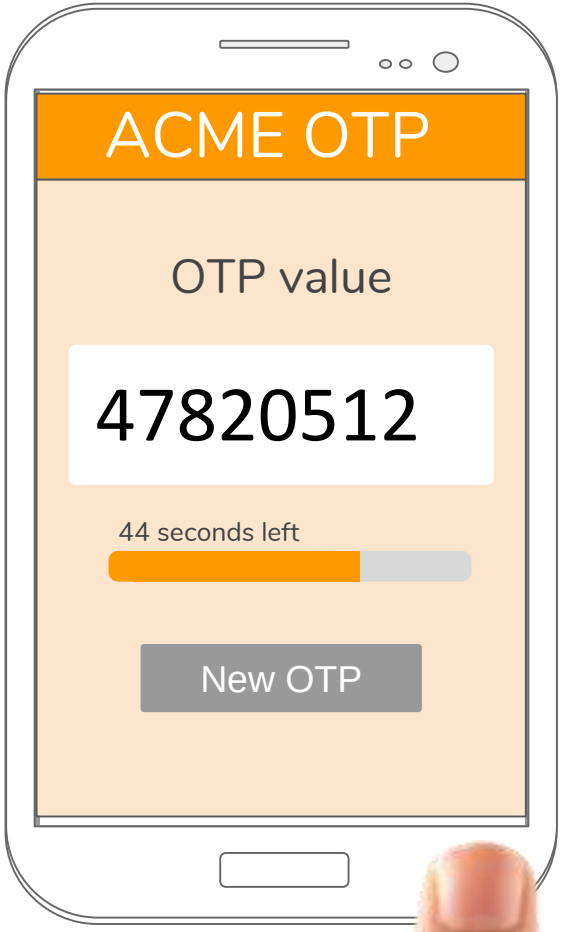
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

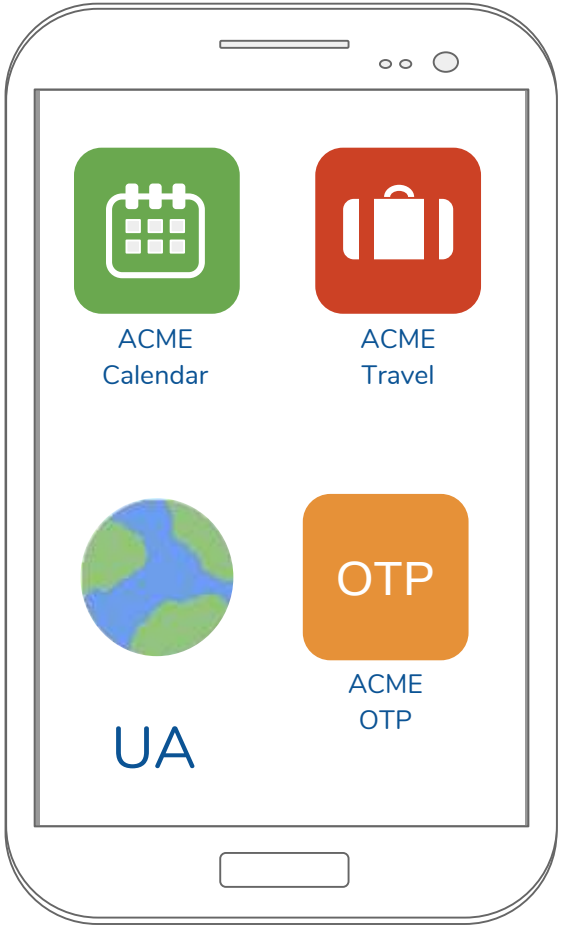
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

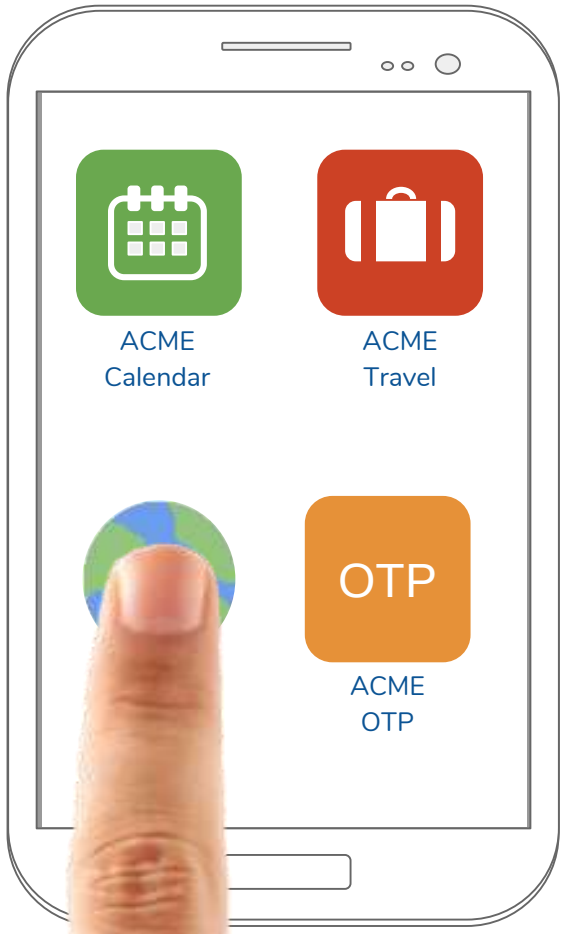
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

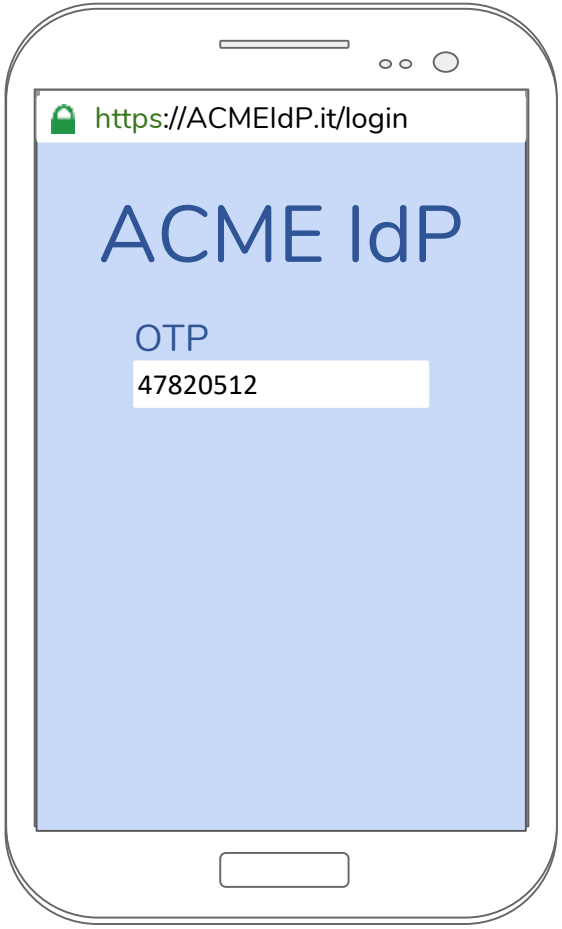
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 1 - usability

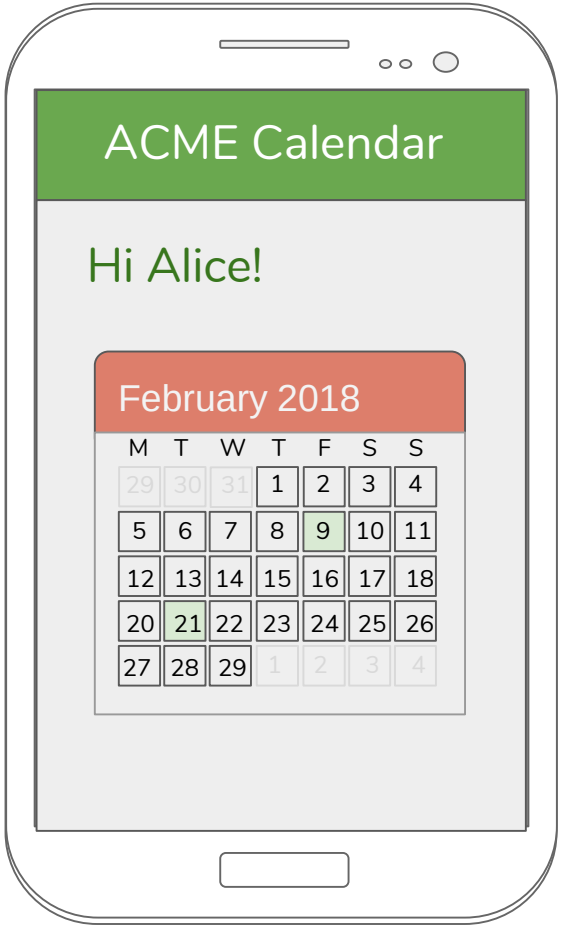
OTP Choice: app that shows the OTP value



Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 2 - usability

OTP Choice: app that shows the OTP value

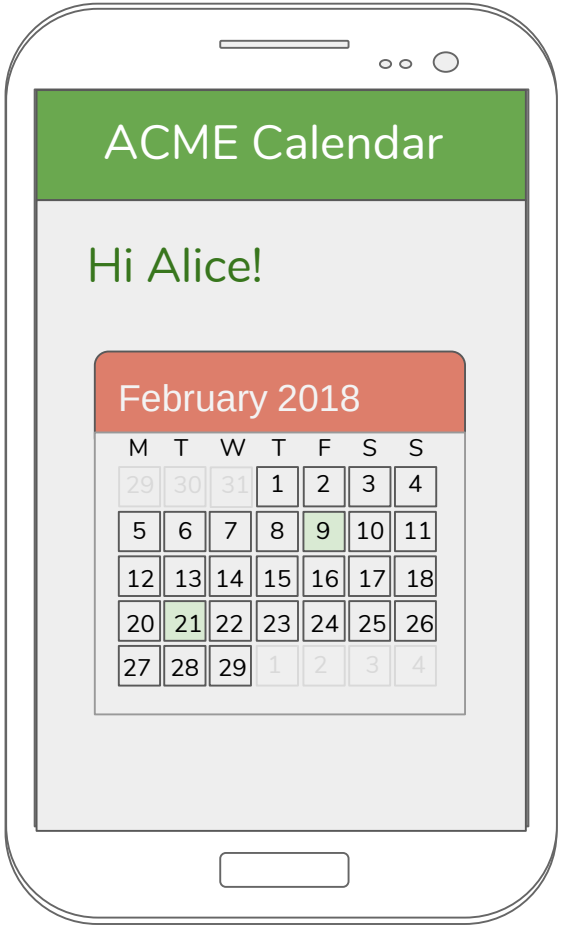


Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 2 - security

OTP Choice: app that shows the OTP value

IdP of SPID



Security: Copy&Paste

Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Exercise 2: Answer 3 - alternatives

OTP Choice: app that shows the OTP value

Alternatives:

- OTP app that does not ask the user to enter the OTP; after the PIN input, the OTP value is sent to the IdP in a transparent way

- Use of external OTP generators

Security Card

1 794	2 536	3 495	4 096	5 555	6 748	7 904	8 565	9 125	10 401
11 295	12 325	13 137	14 107	15 404	16 820	17 040	18 599	19 605	20 013
21 839	22 558	23 530	24 171	25 012	26 399	27 510	28 024	29 089	30 548
31 106	32 486	33 777	34 102	35 962	36 769	37 825	38 140	39 421	40 455
41 727	42 729	43 444	44 632	45 016	46 526	47 009	48 490	49 549	50 943

Outline

- Introduction and Problem Statement

   *Question 1*: Mobile vs Browser-based Authentication

- Design Choices: Security and Usability Problems

   *Exercise 1*: embedded browser *Exercise 2*: OTP displayed on the screen

- Methodology Overview: TreC Scenario

   *Question 2*: e-health legal compliance

- Usability Discussion on TreC

   *Exercise 3*: TreC activation phase

- Conclusions and On-going/Future Work

   *Question 3*: Pros & Cons of our methodology and TreC solution

  Question 1bis: Mobile vs Browser-based Authentication

Design for an IdM Solution

We provide:

- a reference model *mID(OTP)* for mobile authentication and SSO solutions
- a methodology to assist the designer in the customization of *mID(OTP)* and in the analysis of its security and usability

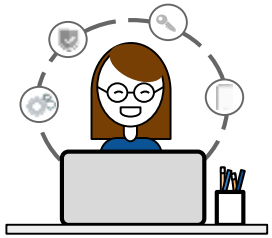
Reference Model - *mID(OTP)*

- *mID(OTP)* is inspired to:
  - a rational reconstruction of Facebook solution (UA=app), and
  - an analysis of OAuth for native app (UA=browser)

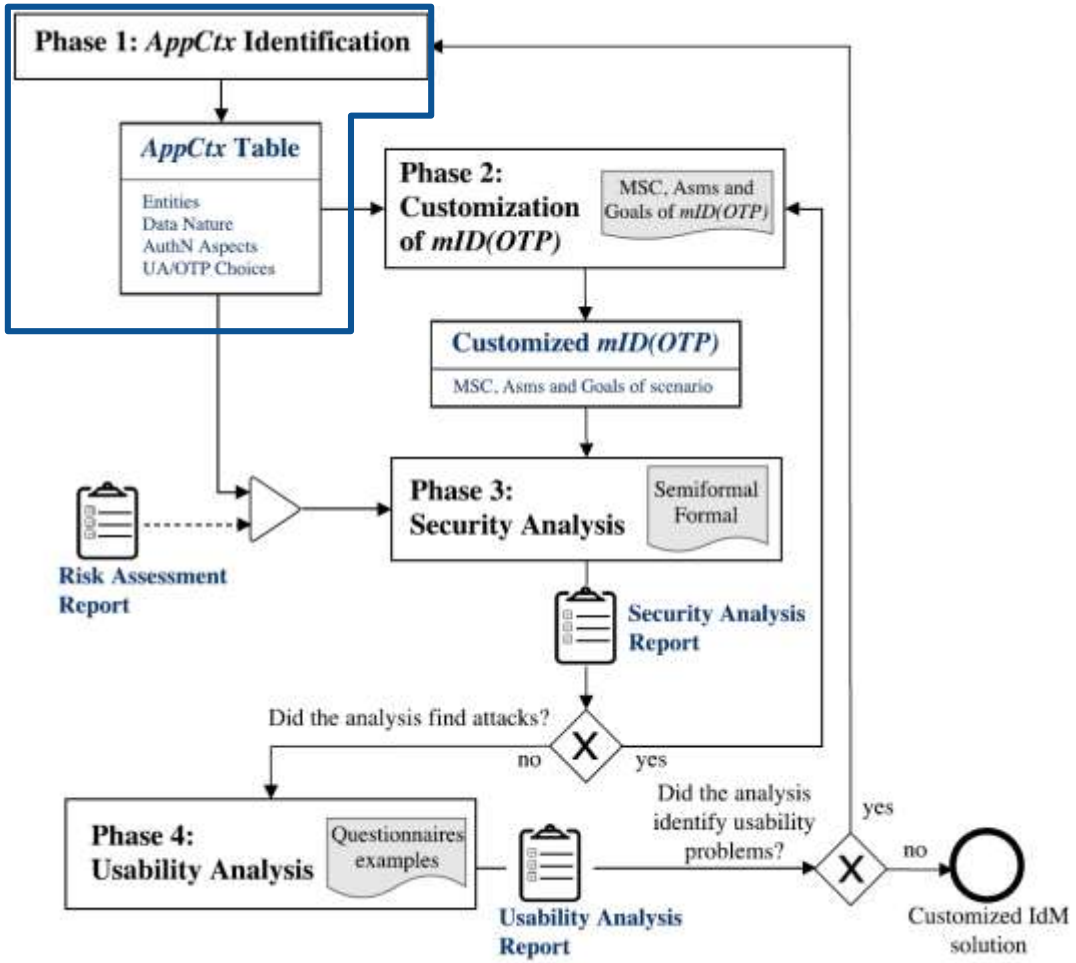
- the OTP generation approaches: Time-based OTP (TOTP) and Challenge-Response

Methodology Overview

1. Application Context
2. Customization of mID(OTP)
3. Security Analysis
4. Usability Analysis

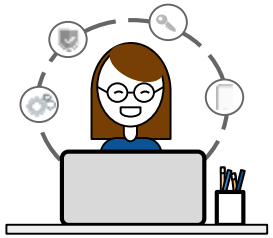


Designer

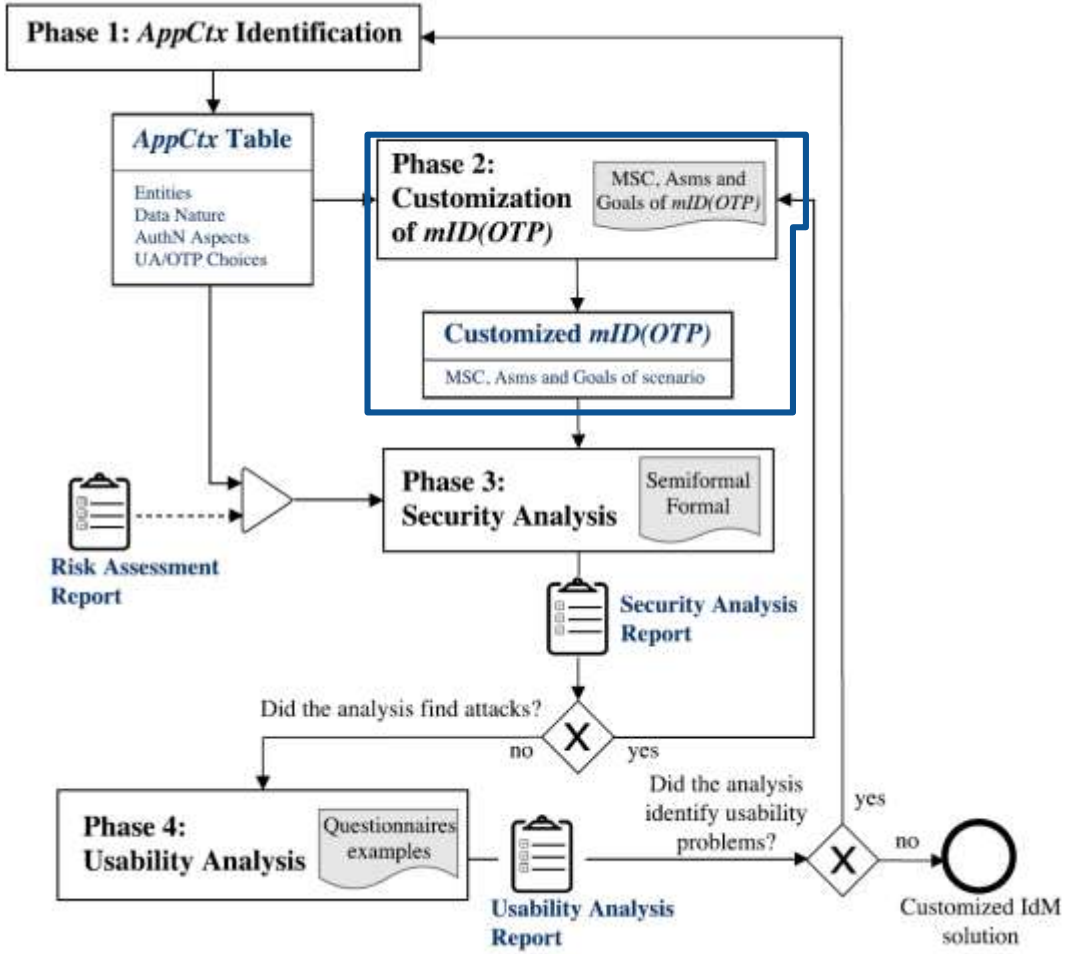


Methodology Overview

1. Application Context
2. Customization of mID(OTP)
3. Security Analysis
4. Usability Analysis

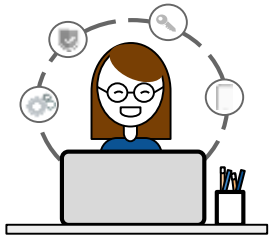


Designer



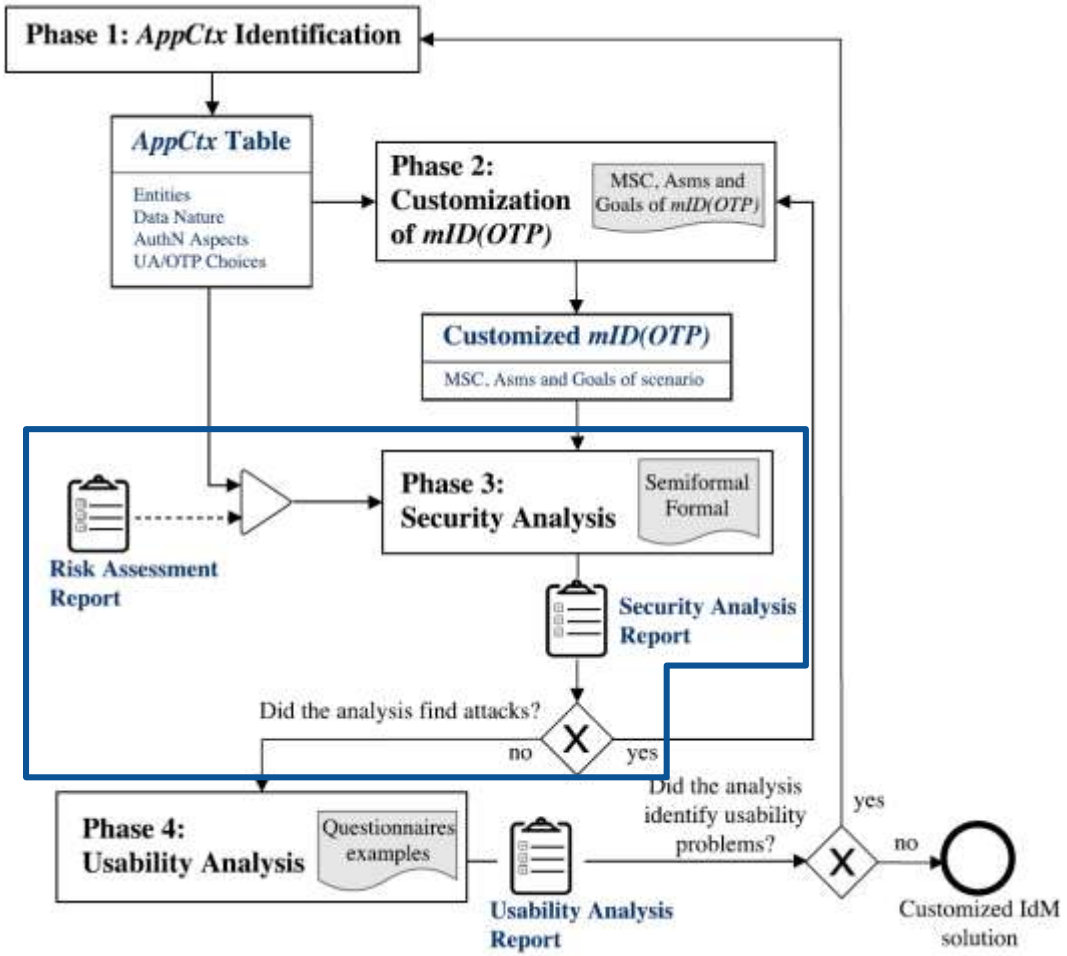
Methodology Overview

1. Application Context
2. Customization of mID(OTP)
3. Security Analysis
4. Usability Analysis



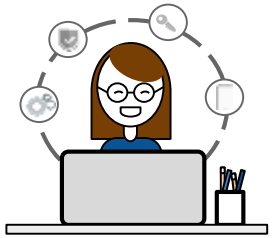
Designer

External Consultant

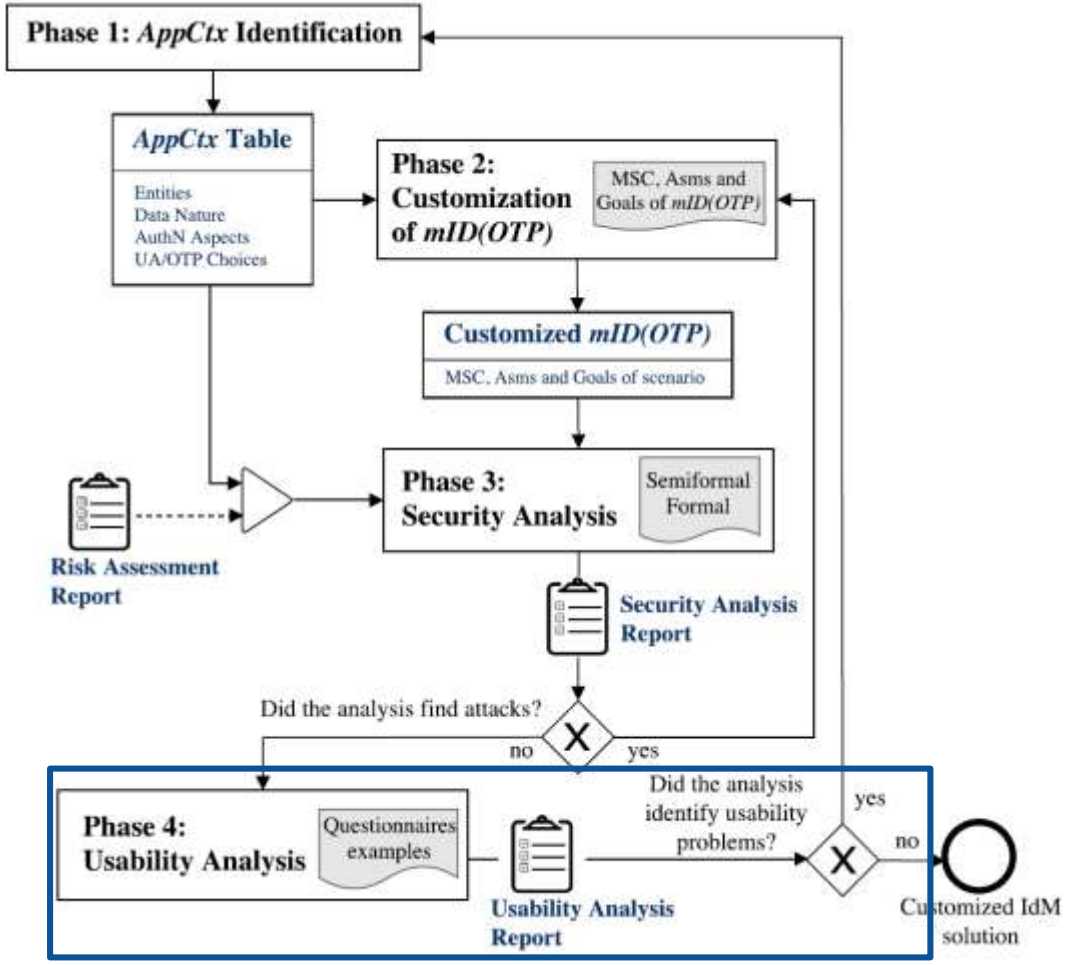


Methodology Overview

1. Application Context
2. Customization of mID(OTP)
3. Security Analysis
4. Usability Analysis

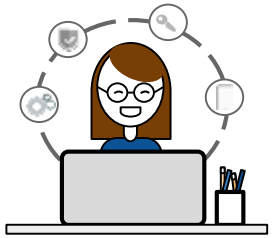


Designer

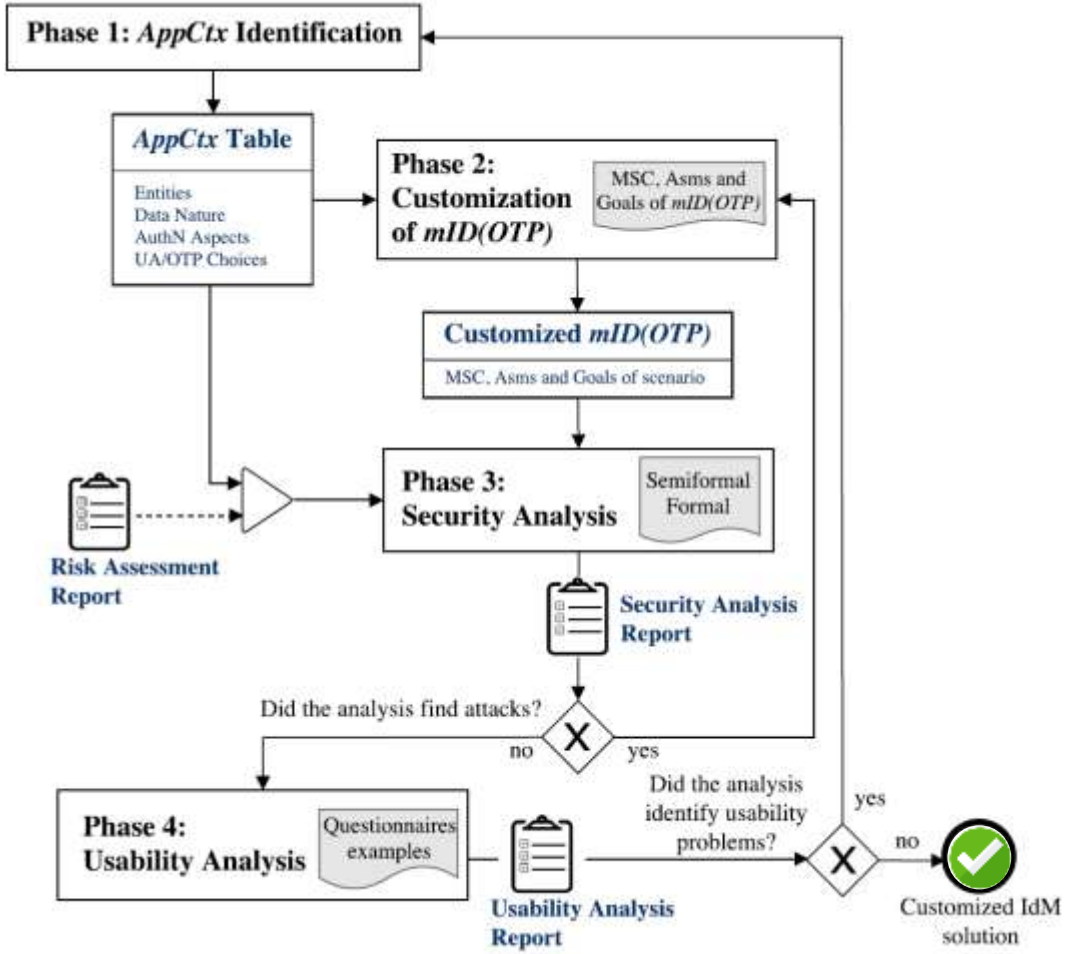


Methodology Overview

1. Application Context
2. Customization of mID(OTP)
3. Security Analysis
4. Usability Analysis



Designer



Real-World Scenarios

1. TreC: a multi-factor authentication solution with a single sign-on experience for mobile e-Health applications.

2. Smart Community: a secure delegated access solution in the context of smart-cities.

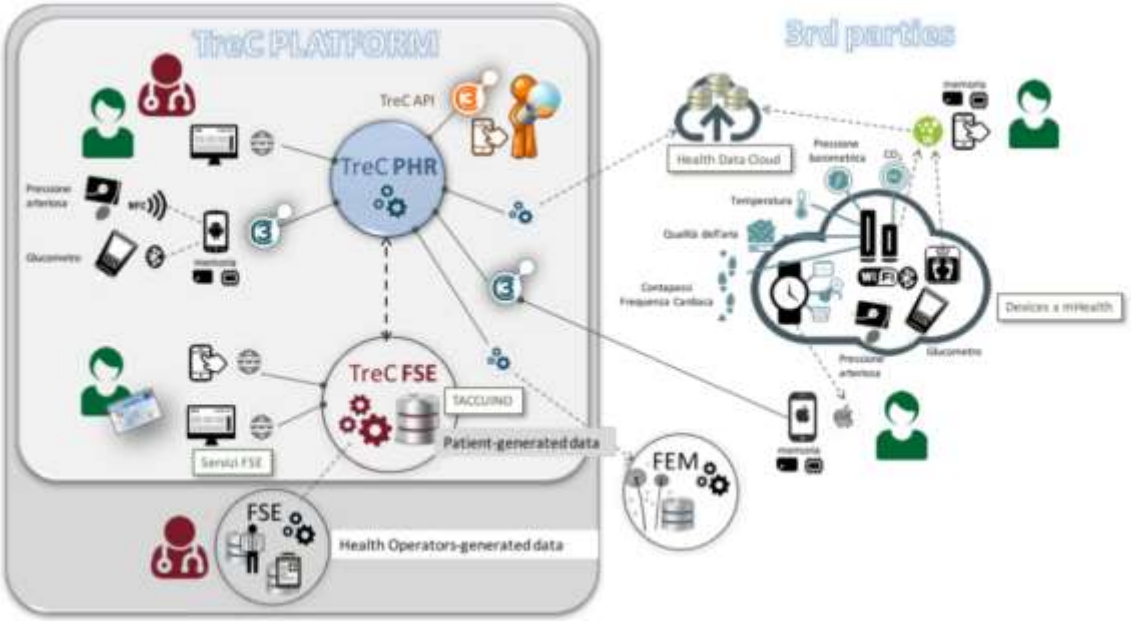
3. FIDES: an IdM solution that combines federation and cross-border aspects in the context of the European single digital market.

4. DigiMat-Lab (Istituto Poligrafico e Zecca dello Stato): a mobile multi-factor authentication solution that uses the Italian electronic identity card (CIE 3.0) as second factor.

TreC Platform

TreC ("Cartella Clinica del Cittadino") is a Citizen-controlled PHR (Personal Health Record) connected to the national EHR (Fascicolo Sanitario Nazionale)

Goal of TreC: empowering citizens to manage their own health and facilitating communications between patients and healthcare professionals and facilities



Provincia Autonoma di Trento

Azienda Provinciale per i Servizi Sanitari
Provincia Autonoma di Trento

FONDAZIONE BRUNO KESSLER

Subscribers: 81,587

TreC: Web and Mobile apps

TreC Apps

Self-management

Remote monitoring

TreC: Web and Mobile apps

Carta Provinciale dei Servizi

TreC Apps

Self-management

Remote monitoring

TreC: Web and Mobile apps

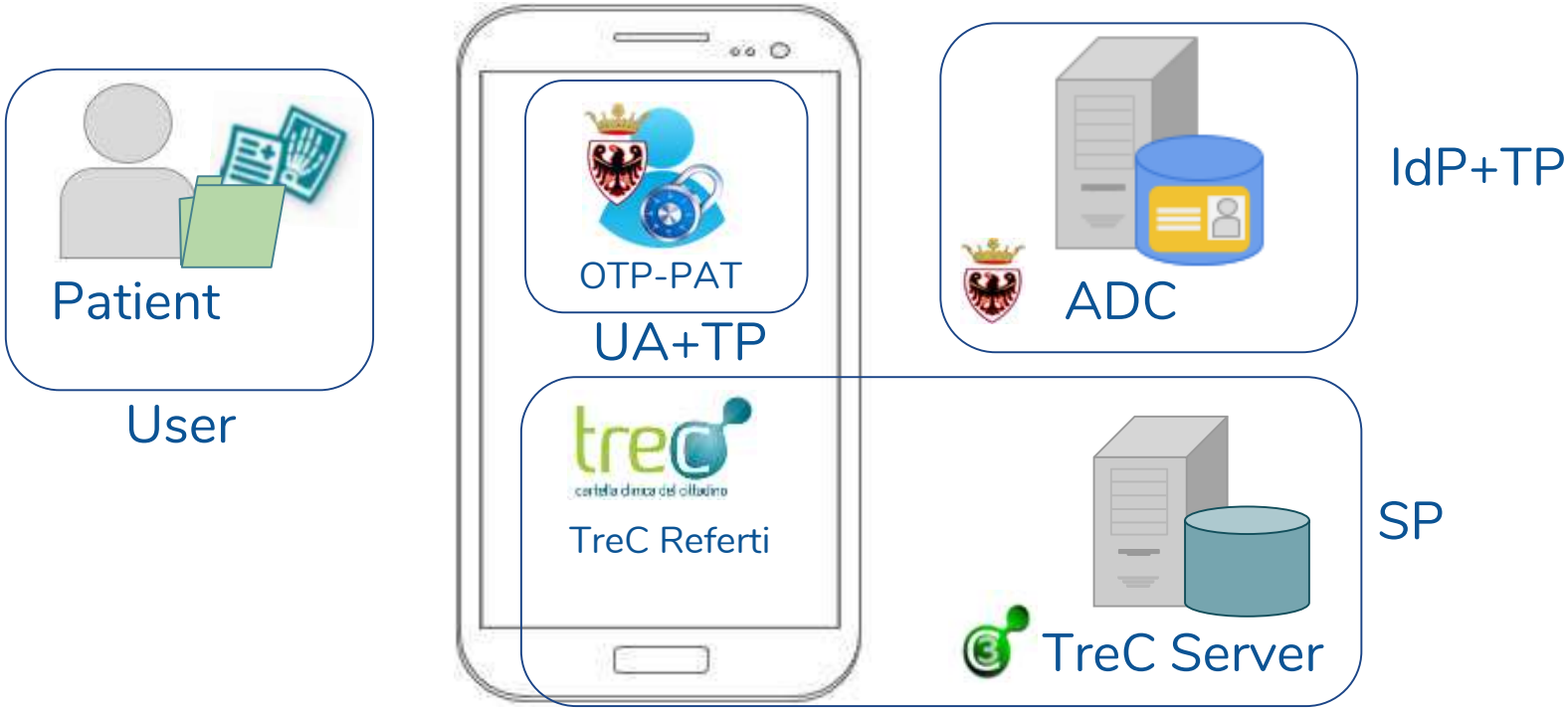
Carta Provinciale dei Servizi

TreC Apps

Goal: provide a multi-factor authentication solution and a SSO experience for the mobile apps of TreC

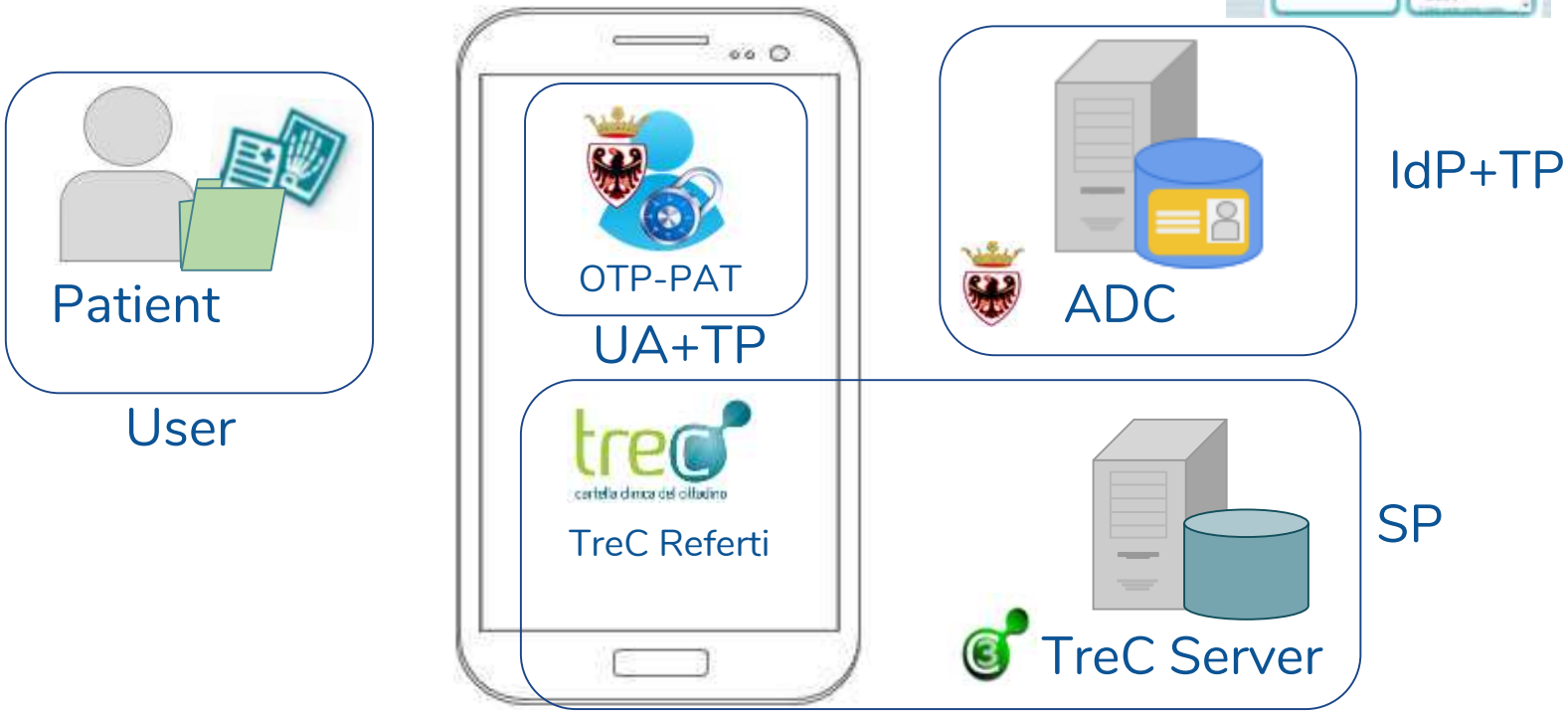
Phase 1: Fill AppCtx Table

Entities	User →`Patient`; SP_{app}→`TreC Referti`; SP_S→`TreC`; UA,TP_{app}→`OTP-PAT`; IdP_S, TP_S→`ADC`;



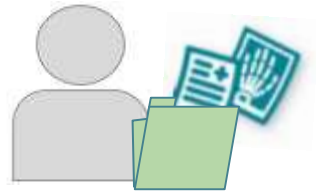
Phase 1: Fill AppCtx Table

Entities	User →`Patient`; SP_{app}→`TreC Referti`; SP_S→`TreC`; UA,TP_{app}→`OTP-PAT`; IdP_S, TP_S→`ADC`;
UA choice	☐ Browser ☑ Application



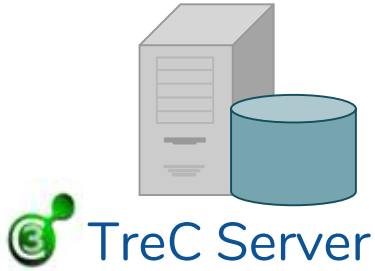
Phase 1: Fill AppCtx Table

Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other



Patient

ADC



TreC Server

Italian Legal Aspects: e-Health data

- The legal aspects related to privacy are covered by the "Personal Data Protection Code" (legislative Decree no. 196/2003) and its Annex B (Technical Specifications Concerning Minimum Security Measures).

  https://www.garanteprivacy.it/documents/10160/2012405/Personal+Data+Protection+Code+-+Legislat.+Decree+no.196+of+30+June+2003.pdf

  > *"data controllers shall be required to adopt the minimum security measures in order to ensure a minimum level of personal data protection"*

- In case of public administration, the CAD (Codice dell'Amministrazione Digitale - D.Lgs.n. 82/3005) must be followed.

  http://www.altalex.com/documents/codici-altalex/2014/06/20/codice-dell-amministrazione-digitale

Carta Provinciale dei Servizi

- Italian national eID scheme (SPID)

  SPID 2 (LoA3 of ISO-IEC 29115) for PHR

  https://www.spid.gov.it/

spid | AgID Agenzia per l'Italia Digitale

5 min left

Which legal obligations do you have to follow when dealing with e-health data in your country?

AppCtx Table - TreC

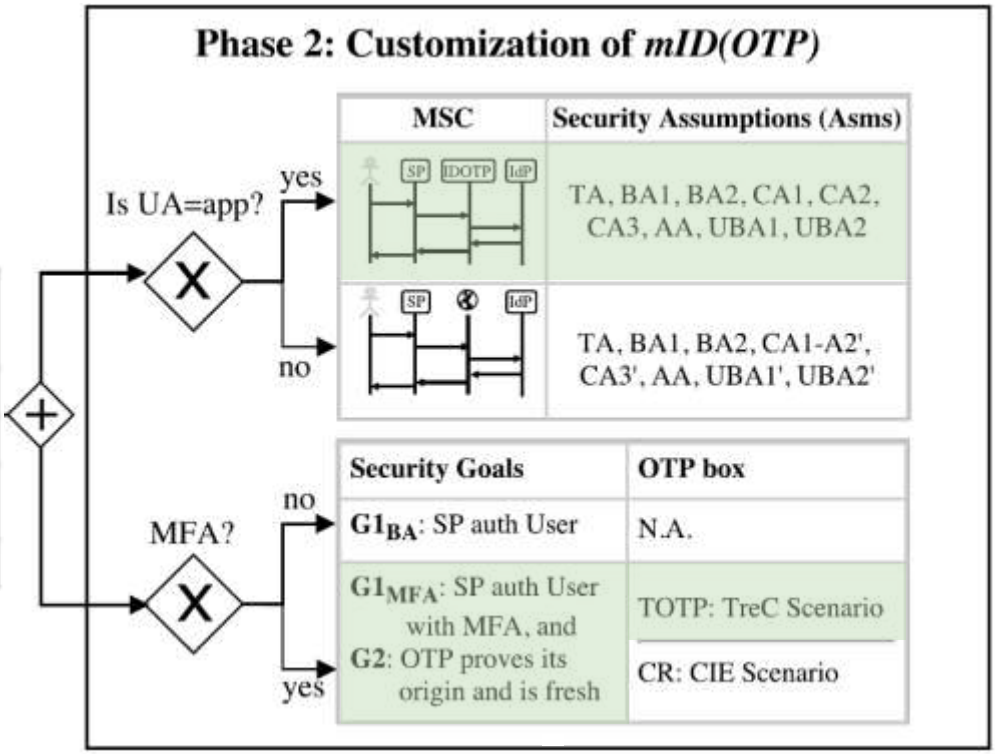
Entities	User →`Patient`; SP_{app}→`TreC Referti`; SP_S→`TreC`; UA,TP_{app}→`OTP-PAT`; IdP_S,TP_S→`ADC`;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other

Phase 2 →

Phase 2: Customization

AppCtx Table - TreC

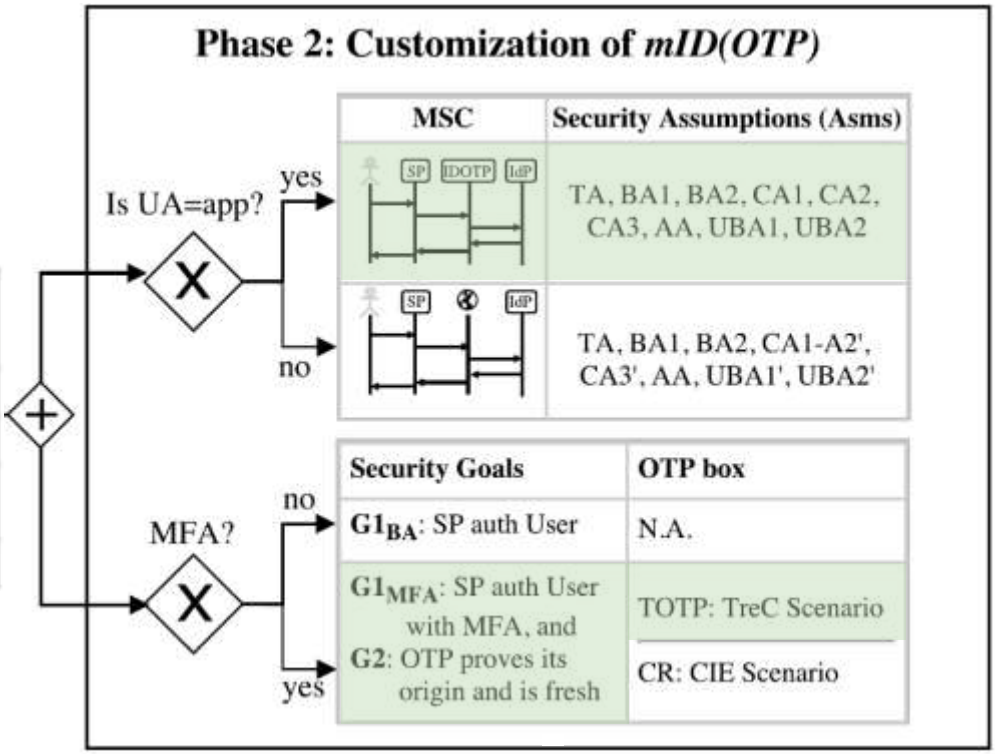
Entities	User → Patient; SP_{app} → TreC Referti; SP_{s} → TreC; UA,TP_{app} → OTP-PAT; IdP_{s}, TP_{s} → ADC;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other



Phase 2: Customization

AppCtx Table - TreC

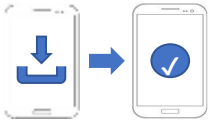
Entities	User → Patient; SP_{app} → TreC Referti; SP_{s} → TreC; UA,TP_{app} → OTP-PAT; IdP_{s}, TP_{s} → ADC;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other



Phase 2: MSC

mID(OTP) requires 3 phases:

Registration: is performed by the TreC developer to register the app with ADC. It is performed just once.



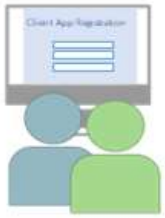
Activation: is performed by the Patient to configure OTP-PAT. It is performed *the first time only*.

Exploitation: is performed every time Patient accesses TreC

Registration of TreC

GOAL: registration of TreC with ADC

TreC dev has to provide some information, such as the app package name and the certificate fingerprint (key_hash) of the app.

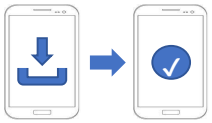


TreC devs

key_hash is a digest of the le CERT.RSA, that contains the public key of the developer, the signature of the app package (APK) obtained with the private key of the developer and other information about the certificate.

Activation of OTP-PAT

GOAL: enable OTP-PAT to securely interact with ADC.

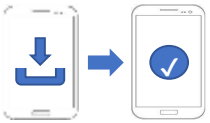


1 Laptop Using a portal made available by ADC, User logs in with CPS and obtains an activation_code.

Carta Provinciale dei Servizi

Activation of OTP-PAT

GOAL: enable OTP-PAT to securely interact with ADC.

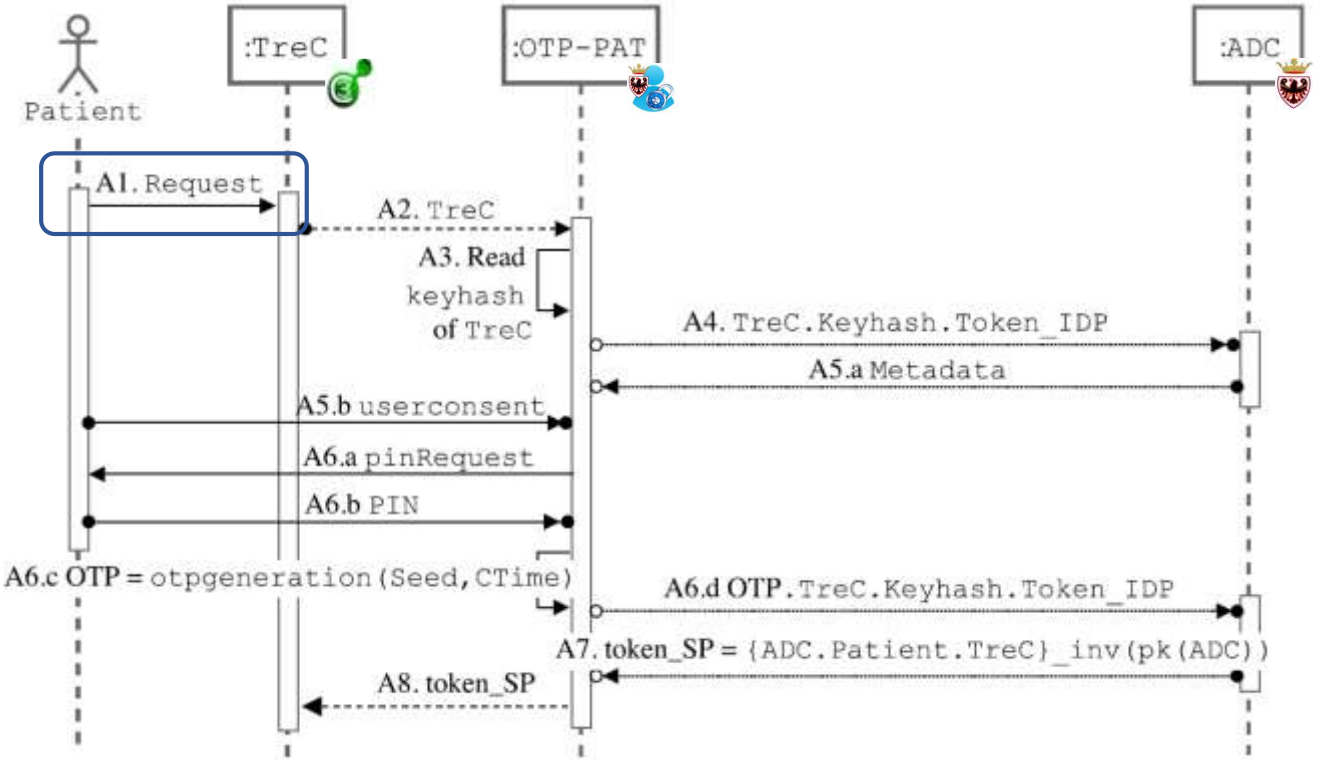


1 Laptop Using a portal made available by ADC, User logs in with CPS and obtains an *activation_code*.

2 Mobile On her mobile, User enters the *activation_code* into OTP-PAT and generates her PIN

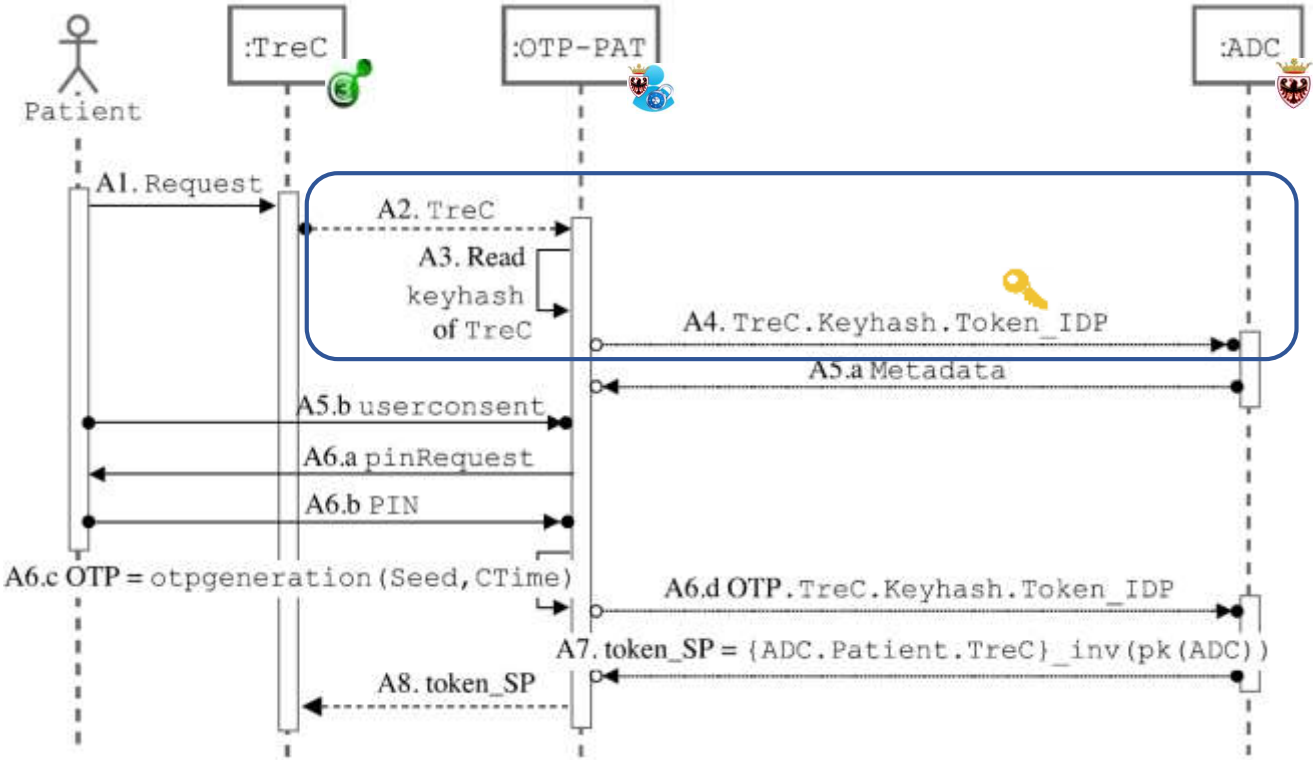
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



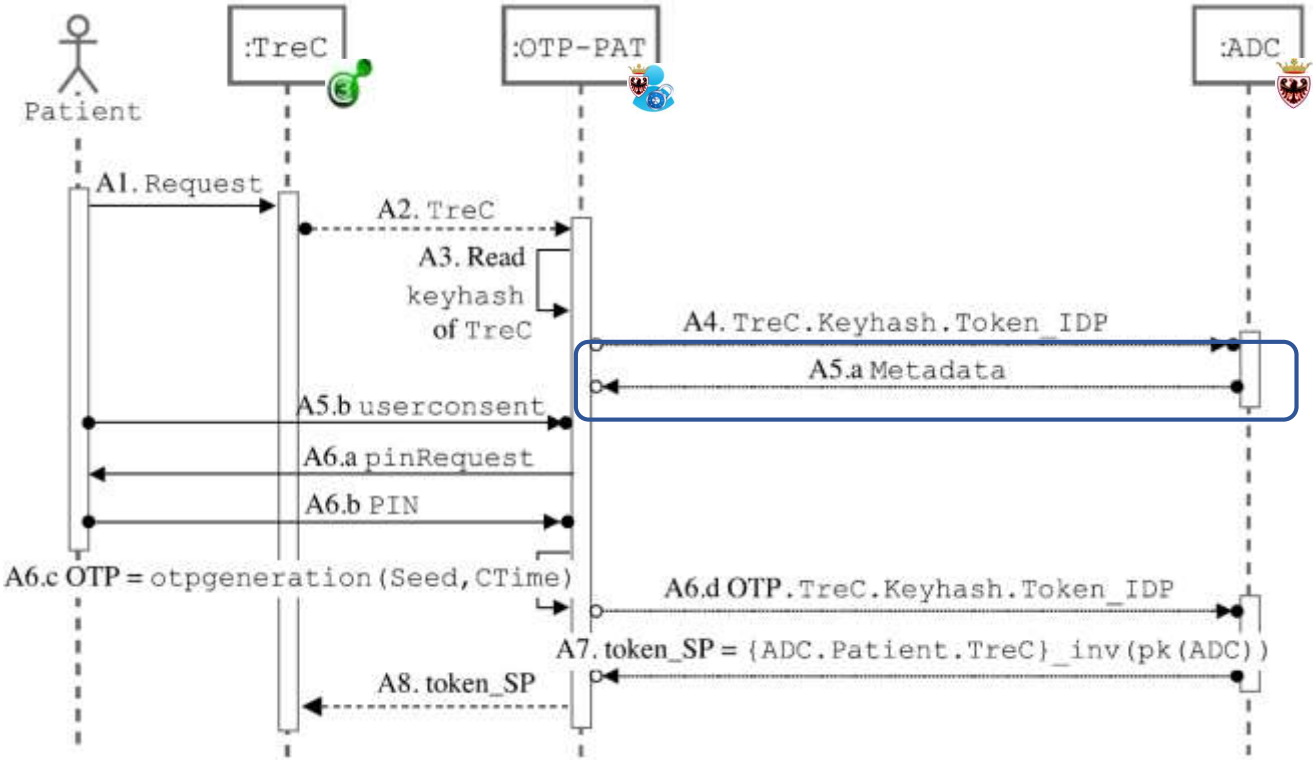
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



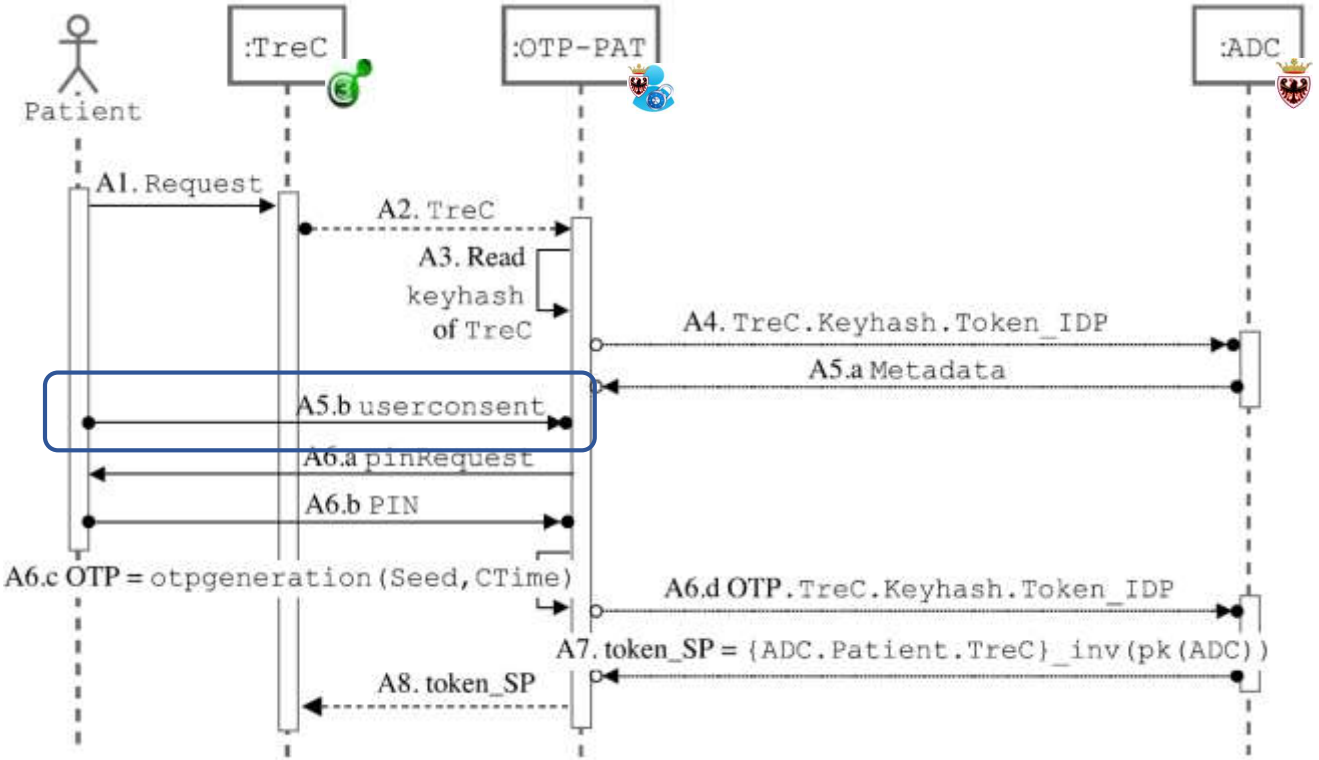
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



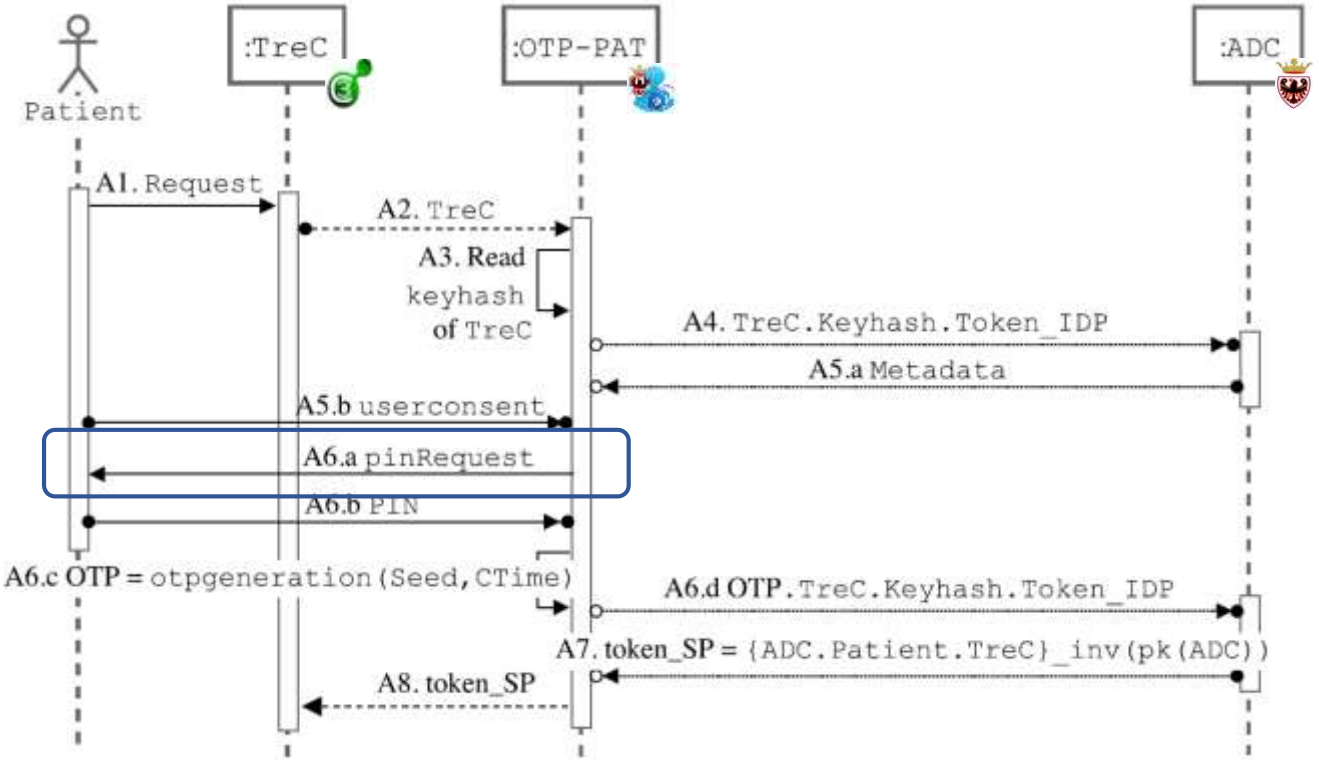
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



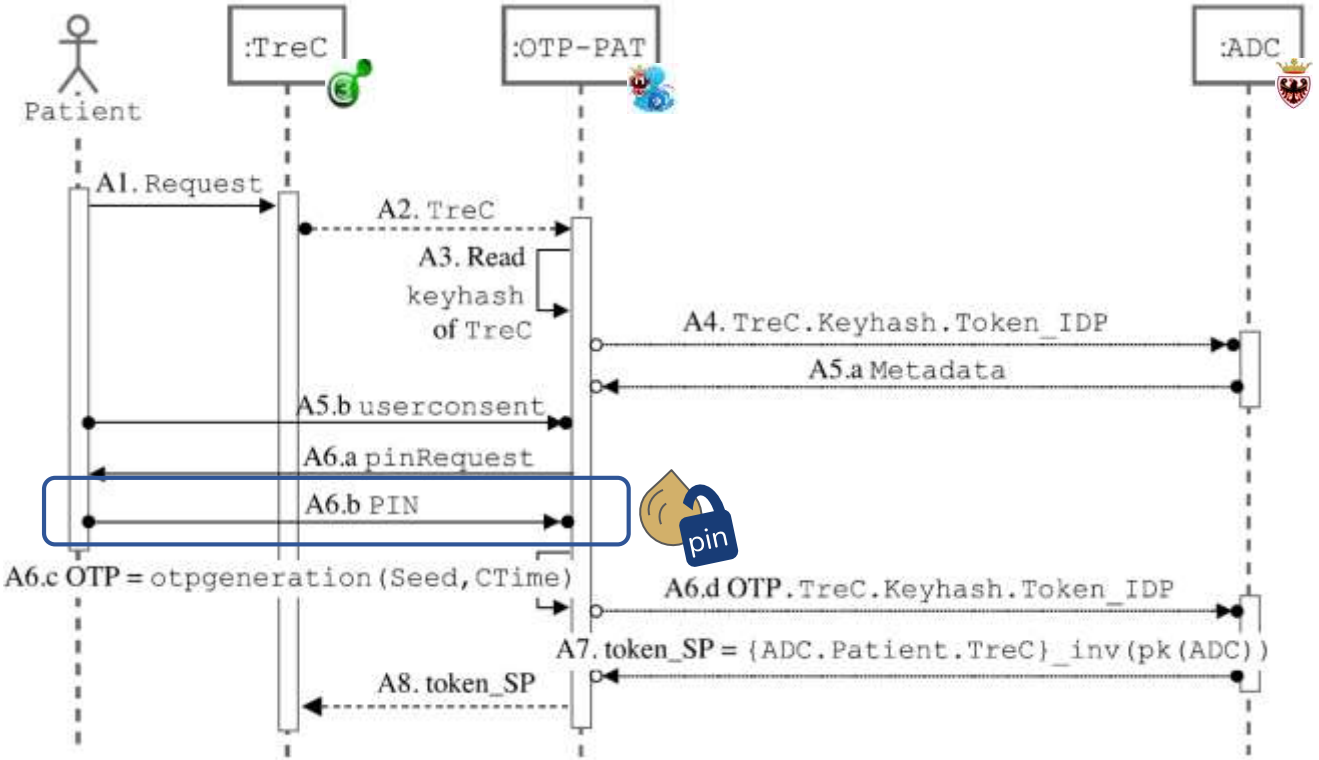
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



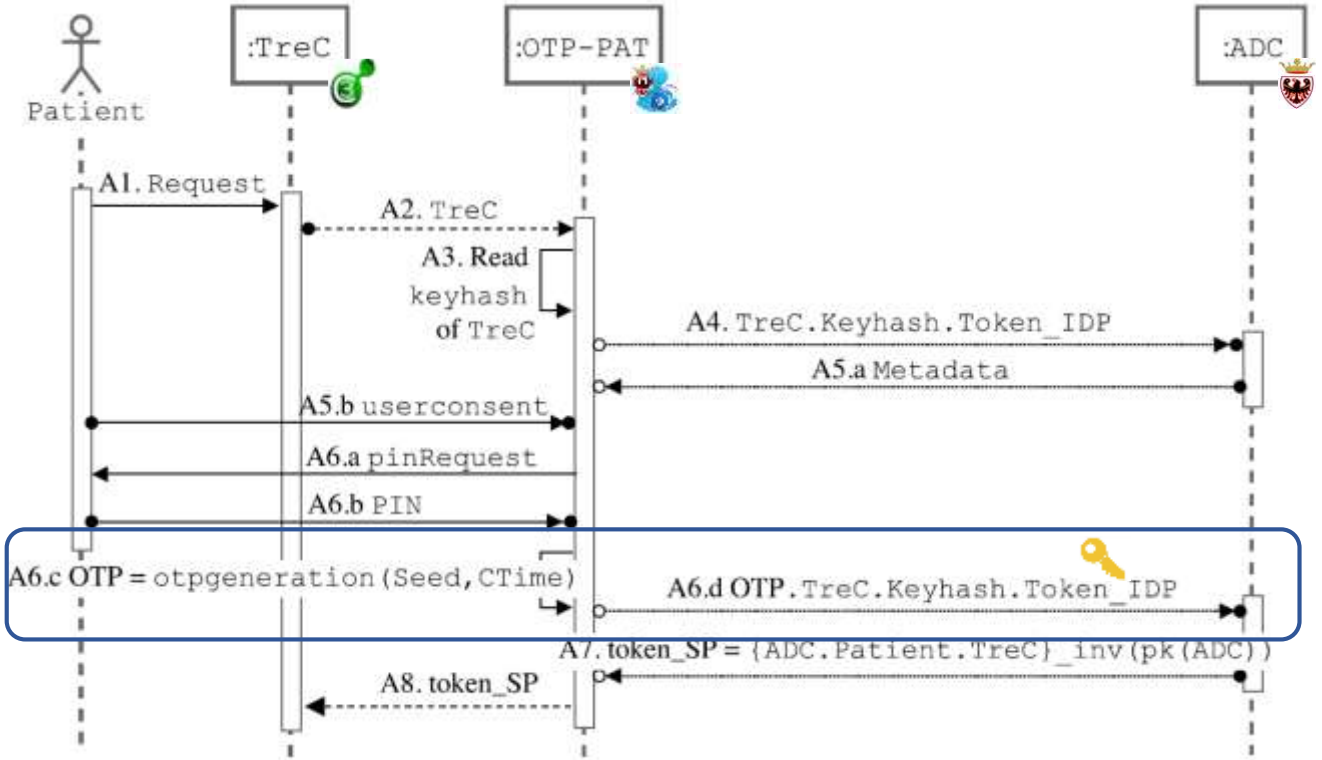
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



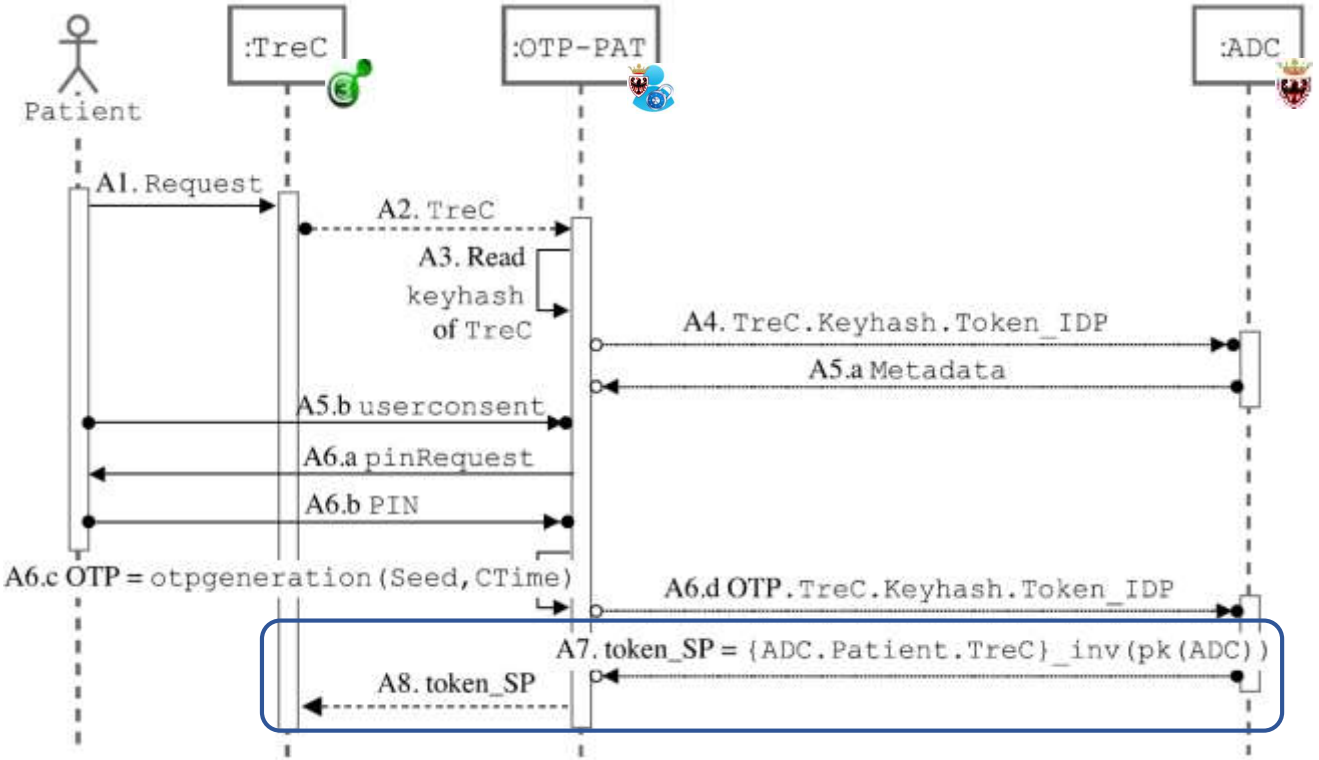
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



MSC Exploitation

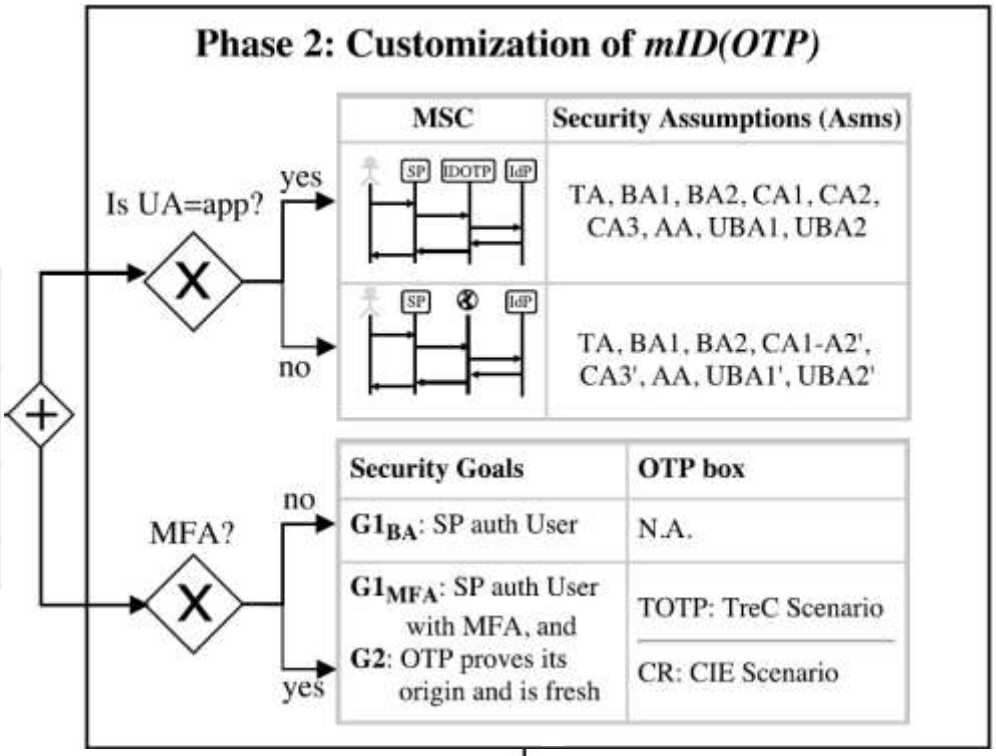
GOAL: user logs in TreC app using the ADC identity



Goals

AppCtx Table - TreC

Entities	User → Patient; SP_{app} → TreC Referti; SP_S → TreC; UA,TP_{app} → OTP-PAT; IdP_S, TP_S → ADC;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other



Phase 2: Customization

The TreC solution is a 3 instance-factors authentication solution:

1. `token_IdP` that is stored in OTP-PAT and in ADC as a result of the activation phase (used as a session token in place of the user credentials to provide a SSO experience);

2. `PIN` known by Patient to unlock OTP-PAT;

3. `{seed}_PIN` that is stored in OTP-PAT.

MFA Goal:

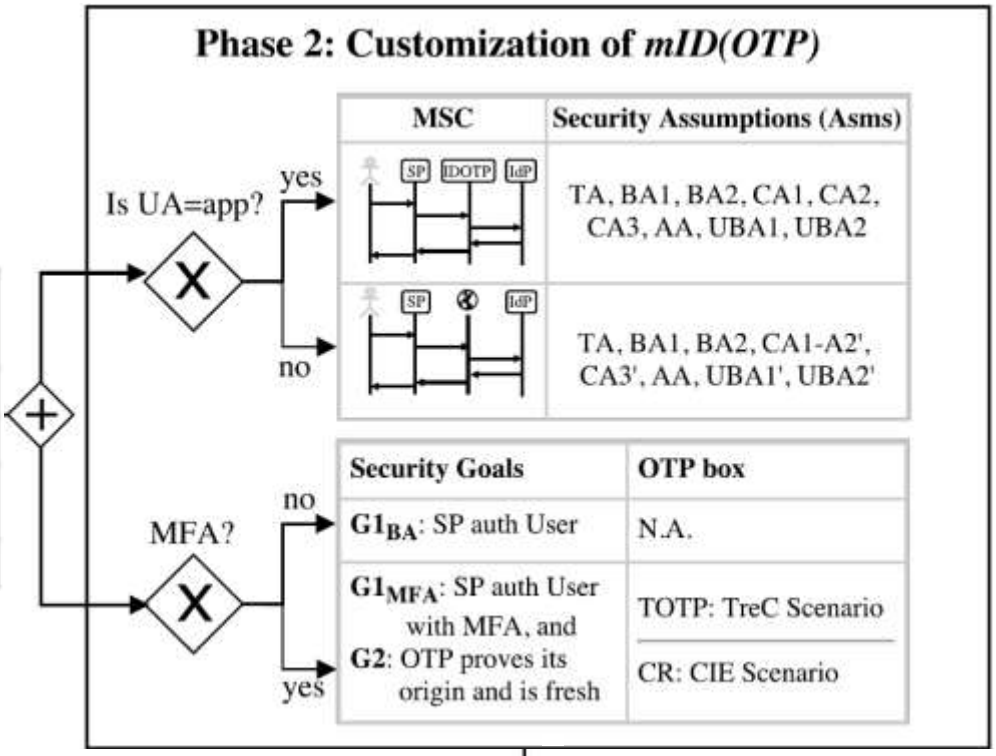
TreC authenticates Patient even if an intruder knows up to 2 instance-factors

G. Sciarretta, R. Carbone, S. Ranise and L. Viganò.
Design, Formal Specification and Analysis of Multi-Factor Authentication Solutions with a Single Sign-On Experience.
Proceedings of the 7th International Conference on Principles of Security and Trust (POST 2018).

Phase 2: Customization

AppCtx Table - TreC

Entities	User → Patient; SP_{app} → TreC Referti; SP_{S} → TreC; UA,TP_{app} → OTP-PAT; IdP_{S}, TP_{S} → ADC;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other



Assumptions

Strong Assumptions

Trust Assumption	**TA**	**ADC** is trusted by **TreC** on identity assertions.
Communication Assumptions	**CA1**	The communication between **TreC** and **OTP-PAT** is carried over an inter-app communication implemented using `StartActivityForResult()`. This Android method --- which allows an app to execute another app and get a result back --- guarantees that **TreC** that sends a request to **OTP-PAT** at Step A2 in Figure 6.1 is the same app that receives the result back from **OTP-PAT** at Step A10.
	CA2	To read the *key hash* value (Step A3 of Figure 6.1), **OTP-PAT** uses the Android method `getPackageInfo(client packageName, PackageManager.GET SIGNATURES)`, which extracts the information about the certificate fingerprint included in the package of **TreC**.
	CA3	The communication between **OTP-PAT** and **ADC** occurs over a unilateral SSL or TLS channel (henceforth SSL/TLS), established through the exchange of a valid certificate (from **ADC** to **OTP-PAT**).
Activation Assumption	**AA**	The activation phase is correctly performed by **Patient**. That is, **Patient** downloads the correct **OTP-PAT** (i.e. it is not fake app) and correctly follows the activation phase process, and the communication channels that are involved in this phase are secure.

Weak Assumptions

Background Assumptions	**BA1**	Integrity and confidentiality of data stored in the device, i.e. an app cannot read or modify data stored by another app.
	BA2	There is no surveillance software (e.g., keylogger) installed on the user's device capable of reading the values that **Patient** types.
User Behaviour Assumptions	**UBA1**	**Patient** enters her credentials and (optionally) values for the OTP generation only in the correct **OTP-PAT** app being careful not to be seen by other people.
	UBA2	**Patient** is the only person using the **OTP-PAT** app that has been activated with her identity.

Assumptions

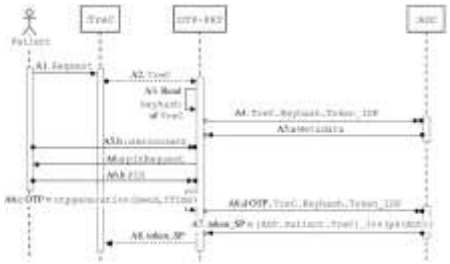
Strong Assumptions

Trust Assumption	**TA**	**ADC** is trusted by **TreC** on identity assertions.
Communication Assumptions	**CA1**	The communication between **TreC** and **OTP-PAT** is carried over an inter-app communication implemented using `StartActivityForResult()`. This Android method --- which allows an app to execute another app and get a result back --- guarantees that **TreC** that sends a request to **OTP-PAT** at Step A2 in Figure 6.1 is the same app that receives the result back from **OTP-PAT** at Step A10.
	CA2	To read the *key hash* value (Step A3 of Figure 6.1), **OTP-PAT** uses the Android method `getPackageInfo(client packageName, PackageManager.GET SIGNATURES)`, which extracts the
	CA3	The communication between **OTP-PAT** and **ADC** occurs over a unilateral SSL or TLS channel (henceforth SSL/TLS), established through the exchange of a valid certificate (from **ADC** to **OTP-PAT**).
Activation Assumption		it is not fake app) and correctly follows the activation phase process, and the communication channels that are involved in this phase are secure.

Weak Assumptions

Background Assumptions	**BA1**	Integrity and confidentiality of data stored in the device, i.e. an app cannot read or modify data stored by another app.
	BA2	There is no surveillance software (e.g., keylogger) installed on the user's device capable of reading the values that **Patient** types.
User Behaviou Assumptions	**UBA1**	**Patient** enters her credentials and (optionally) values for the OTP generation only in the correct **OTP-PAT** app
	UBA2	**Patient** is the only person using the **OTP-PAT** app that has been activated with her identity.

Phase 3: Security Analysis



MSC Scenario

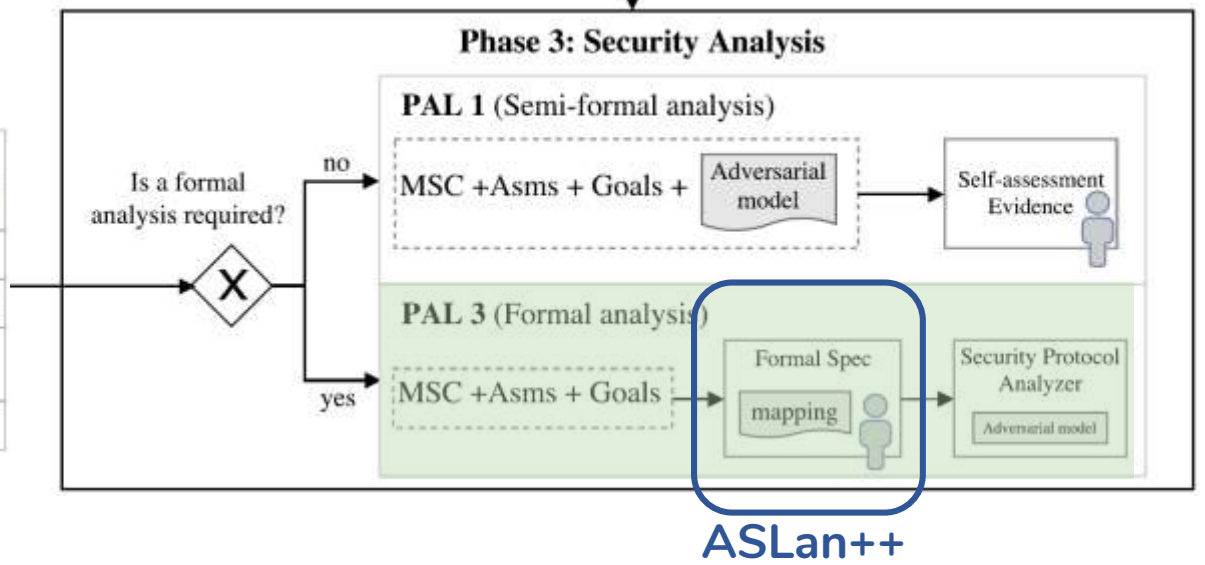
TA	ADC is trusted by TreC on identity assertions
BA1	Integrity and confidentiality of data stored in the device
...	...

Asms Scenario

$G1_{MFA}$	TreC auth Pat. with MFA
G2	OTP proves its origin and is fresh

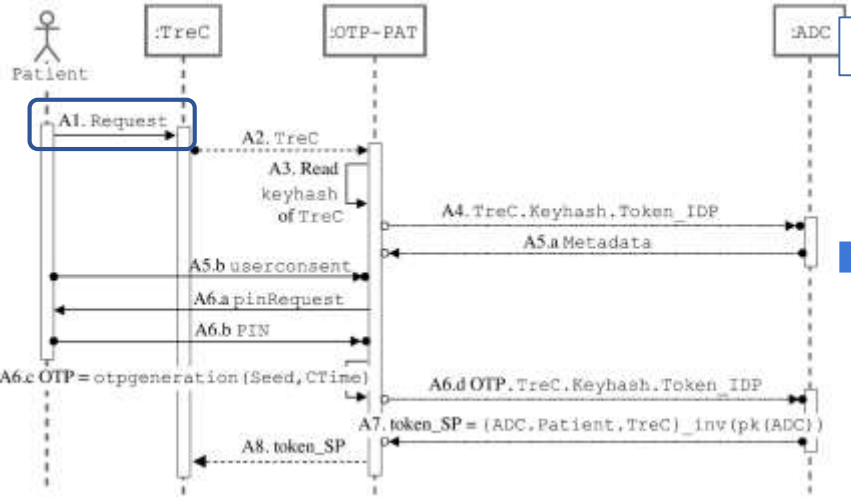
Goals Scenario

Entities	User → Patient; SP_{app} → TreC Referti; SP_{s} → TreC; UA, TP_{app} → OTP-PAT; IdP_{s}, TP_{s} → ADC;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other



AVANTSSAR Project. Deliverable D2.3 (update) ASLan++ specification and tutorial. http://www.avantssar.eu/pdf/deliverables/avantssar-d2-3_update.pdf, 2008.

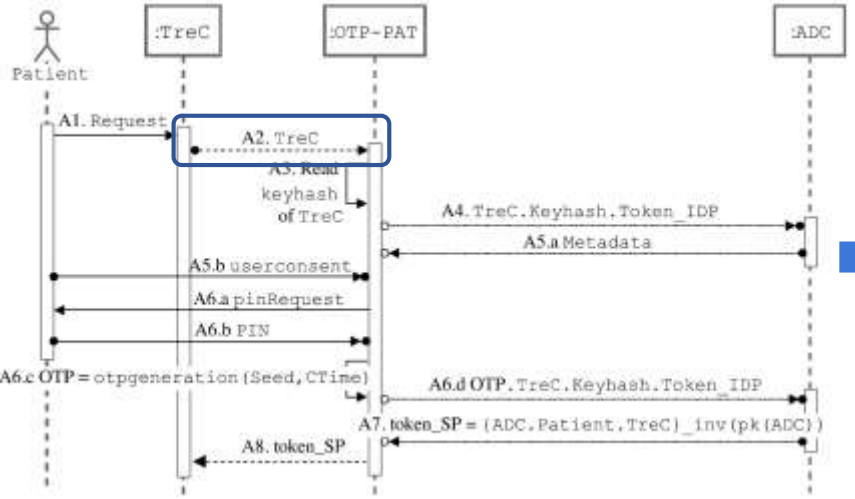
Modelling the Honest Entities and the Intruder




```
select{on(Patient -Ch_P2T-> Actor: Request):{%STEP A1
```

```
55 %%%% TreC APP %%%%
56 entity Service_Provider(Actor, OTPPAT, ADC, Patient: agent, Ch_T2O, Ch_O2T,
57 Ch_P2T, Ch_T2P: channel, Request: text) {
58
61 Actor -Ch_T2O-> OTPPAT: Actor;  %STEP A2
62         select{on(OTPPAT-Ch_O2T->Actor:{ADC.?Patient.Actor}_inv(pk(ADC))):{%A8
63         SP_authn_U_on_Request:(Request) := Request;
64         }}
65   }}
66 }}
67
68 %%%% OTP-PAT APP %%%%
69 entity User_Agent(Actor, TreC, ADC, Patient: agent, Ch_T2O, Ch_O2T, Ch_O2A,
70 Ch_A2O, Ch_P2O, Ch_O2P: channel, Seed: seed, Token_IDP: token, CTime: time) {
71
72 symbols
73 KeyHash: key_hash;
74 Metadata: text;
75 PINRequest: text;
76 PIN: pin;
77
78 body{%of UA
79 iknows(CTime);
```

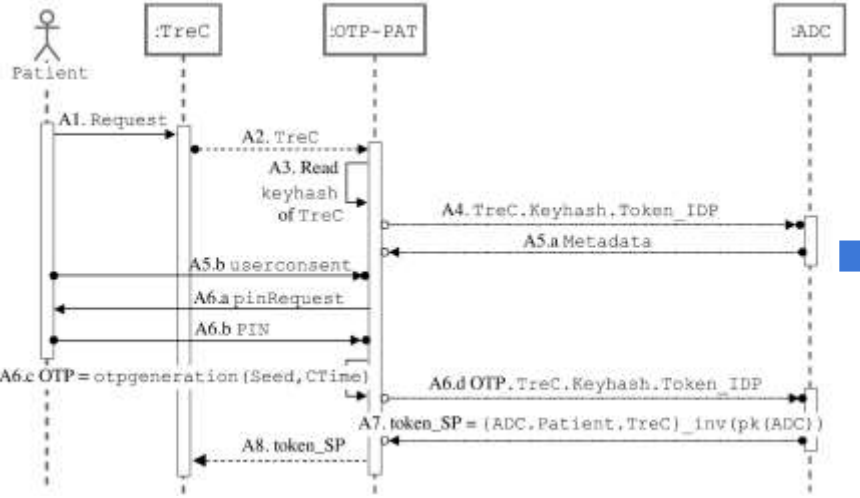
Modelling the Honest Entities and the Intruder




```
55 %%%% TreC APP %%%%
56 entity Service_Provider(Actor, OTPPAT, ADC, Patient: agent, Ch_T2O, Ch_O2T,
57 Ch_P2T, Ch_T2P: channel, Request: text) {
58
59 body{%of SP
60 select{on(Patient -Ch_P2T-> Actor: Request):{ %STEP A1
                                                    DC))):{%A8
63         SP_authn_U_on_Request:(Request) := Request;
64         }}
65   }}
66 }}
67
68 %%%% OTP-PAT APP %%%%
69 entity User_Agent(Actor, TreC, ADC, Patient: agent, Ch_T2O, Ch_O2T, Ch_O2A,
70 Ch_A2O, Ch_P2O, Ch_O2P: channel, Seed: seed, Token_IDP: token, CTime: time) {
71
72 symbols
73 KeyHash: key_hash;
74 Metadata: text;
75 PINRequest: text;
76 PIN: pin;
77
78 body{%of UA
79 iknows(CTime);
```

Actor -Ch_T2O-> OTPPAT: Actor):{%STEP A2

Modelling the Honest Entities and the Intruder




```
55 %%%% TreC APP %%%%
56 entity Service_Provider(Actor, OTPPAT, ADC, Patient: agent, Ch_T2O, Ch_O2T,
57 Ch_P2T, Ch_T2P: channel, Request: text) {
58
59 body{%of SP
60 select{on(Patient -Ch_P2T-> Actor: Request):{  %STEP A1
61 Actor -Ch_T2O-> OTPPAT: Actor;  %STEP A2
62         select{on(OTPPAT-Ch_O2T->Actor:{ADC.?Patient.Actor}_inv(pk(ADC))):{%A8
63         SP_authn_U_on_Request:(Request) := Request;
64         }}
65   }}
66 }}
67
68 %%%% OTP-PAT APP %%%%
69 entity User_Agent(Actor, TreC, ADC, Patient: agent, Ch_T2O, Ch_O2T, Ch_O2A,
70 Ch_A2O, Ch_P2O, Ch_O2P: channel, Seed: seed, Token_IDP: token, CTime: time) {
71
72 symbols
73 KeyHash: key_hash;
74 Metadata: text;
75 PINRequest: text;
76 PIN: pin;
77
78 body{%of UA
79 iknows(CTime);
```

- Dolev-Yao intruder who can overhear and modify messages using his initial knowledge and the knowledge obtained from the traffic, but cryptography is secure, i.e. decryption is impossible without appropriate keys.

Dolev, D., Yao, A.: On the Security of Public-Key Protocols. In: IEEE Transactions on Information Theory. (1983) 2(29)

Assumptions and Goal Formal Mapping

Asm	Formal Specification
	Specification of Assumptions
TA	We do not consider sessions with `i` playing the role of `ADC`
BA1	"Built-in": `i` cannot read the internal state of the other entities
BA2	"Built-in": `i` cannot read the internal state of the other entities
CA1	`link(T2O,O2T);`
CA2	`authentic on(T2O,TreC);`

CA3	`confidential_to(O2A, ADC);`
	`weakly_authentic(O2A);`
	`weakly_confidential(A2O);`
	`authentic_on(A2O,ADC);`
	`link(O2A,A2O);`

AA	Data obtained during the activation phase are `nonpublic` values
UBA1	`confidential_to(P2O,OTPPAT);`
UBA2	`authentic_on(P2O,Patient);`

$G1_A$	`SP_authn_U_on_Request:( ) Patient *->> TreC;`

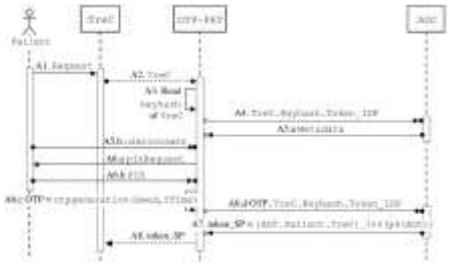
Assumptions Formal Mapping

Asm	Formal Specification	
	Specification of Assumptions	**Removal of Assumptions**
TA	We do not consider sessions with `i` playing the role of `ADC`	ADD sessions with `i` playing the role of `ADC`
BA1	"Built-in": `i` cannot read the internal state of the other entities	ADD `iknows(token_IDP);` `iknows({|seed|}_pinUser);`
BA2	"Built-in": `i` cannot read the internal state of the other entities	ADD `iknows(pinUser);`
CA1	`link(T2O,O2T);`	DELETE `link(T2O,O2T);`
CA2	`authentic_on(T2O,TreC);`	DELETE `authentic_on(T2O,TreC);`
CA3	`confidential_to(O2A, ADC);` `weakly_authentic(O2A);` `weakly_confidential(A2O);` `authentic_on(A2O,ADC);` `link(O2A,A2O);`	DELETE `confidential_to(O2A, ADC);` `weakly_authentic(O2A);` `weakly_confidential(A2O);` `authentic_on(A2O,ADC);` `link(O2A,A2O);`
AA	Data obtained during the activation phase are `nonpublic` values	ADD `iknows(token_IDP);` `iknows(pinUser);` `iknows({|seed|}_pinUser);`
~~**UBA1**~~	~~`confidential_to(P2O,OTPPAT);`~~	DELETE `confidential_to(P2O,OTPPAT);`
~~**UBA2**~~	~~`authentic_on(P2O,Patient);`~~	DELETE `authentic_on(P2O,Patient);`

Proximity Intruder

$\mathbf{G1_A}$	`SP_authn_U_on_Request:( ) Patient *->> TreC;`

Phase 3: Security Analysis



MSC Scenario

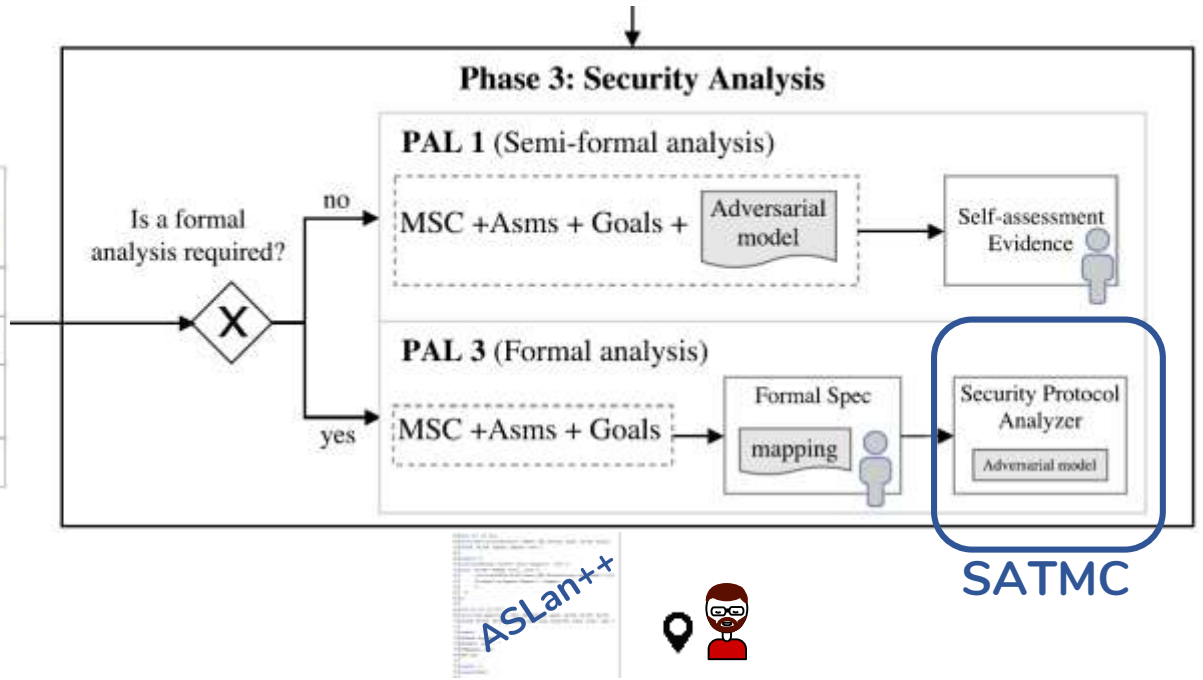
TA	ADC is trusted by TreC on identity assertions
BA1	Integrity and confidentiality of data stored in the device
...	...

Asms Scenario

$G1_{MFA}$	TreC auth Pat. with MFA
G2	OTP proves its origin and is fresh

Goals Scenario

Entities	User → Patient; SP_{app} → TreC Referti; SP_{s} → TreC; UA, TP_{app} → OTP-PAT; IdP_{s}, TP_{s} → ADC;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other



SAT-based bounded model checker: $M_S \parallel M_I \models G_{BA}$

Security Analyses

Analysis 1: Is the solution secure under all the strong and weak assumptions?

SATMC does not find any attack on the solution (i.e. the intruder is not able to impersonate the user)

Security Analyses

Analysis 1: Is the solution secure under all the strong and weak assumptions?

SATMC does not find any attack on the solution (i.e. the intruder is not able to impersonate the user)

Analysis 2: Which assumptions can be removed? (e.g., modeling a wrong implementation)

- none of the strong assumptions
- one weak assumption at a time
- a combination of weak assumptions such that all the instance factors are not compromised

only if the intruder compromises all the instance factors he is able to impersonate the patient

Security Analyses

Analysis 1: Is the solution secure under all the strong and weak assumptions?

SATMC does not find any attack on the solution (i.e. the intruder is not able to impersonate the user)

Analysis 2: Which assumptions can be removed? (e.g., modeling a wrong implementation)

- none of the strong assumptions
- one weak assumption at a time
- a combination of weak assumptions such that all the instance factors are not compromised

only if the intruder compromises all the instance factors he is able to impersonate the patient

Removed Weak Asm(s)	Compromised Factors PIN	{seed}_PIN	token_IdP
BA1	x	✓	✓
BA2	✓	x	x
$UBA1_{Var1}$	✓	x	x
$UBA2_{Var1}$	x	✓	✓

Security Analyses

Analysis 1: Is the solution secure under all the strong and weak assumptions?

SATMC does not find any attack on the solution (i.e. the intruder is not able to impersonate the user)

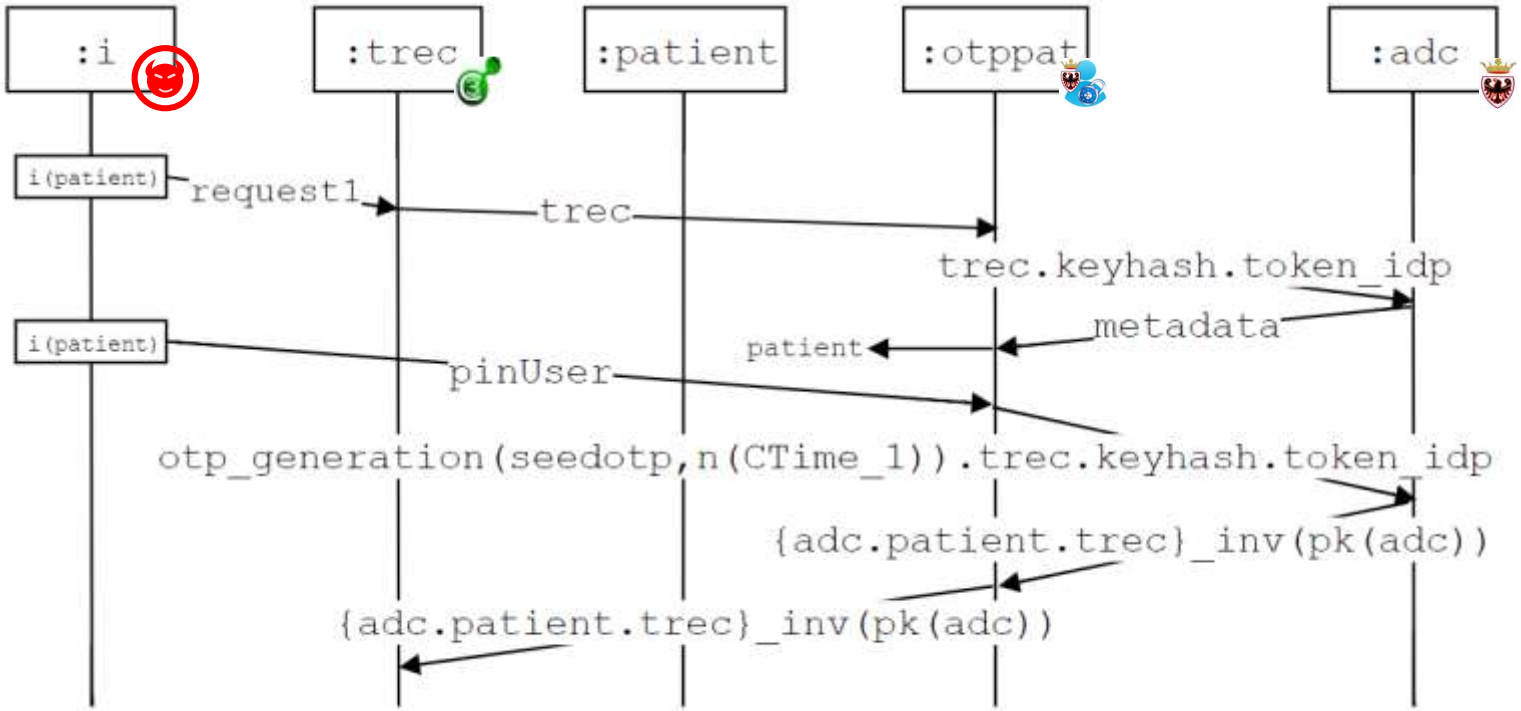
Analysis 2: Which assumptions can be removed? (e.g., modeling a wrong implementation)

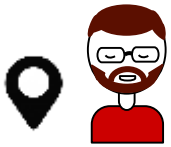
- none of the strong assumptions
- one weak assumption at a time
- a combination of weak assumptions such that all the instance factors are not compromised

only if the intruder compromises all the instance factors he is able to impersonate the patient

Removed Weak Asm(s)	Compromised Factors PIN	{seed}_PIN	token_IdP
BA1	x	✓	✓
BA2	✓	x	x
$UBA1_{Var1}$	✓	x	x
$UBA2_{Var1}$	x	✓	✓

Phase 3: Security Analysis



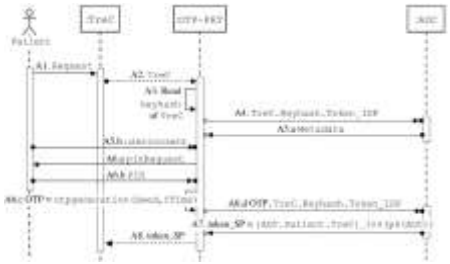


Proximity Intruder

STOLEN SMARTPHONE

+ PIN

Phase 3: Output



MSC Scenario

TA	ADC is trusted by TreC on identity assertions
BA1	Integrity and confidentiality of data stored in the device
...	...

Asms Scenario

$G1_{MFA}$	TreC auth Pat. with MFA
G2	OTP proves its origin and is fresh

Goals Scenario

Entities	User → Patient; SP_{app} → TreC Referti; SP_S → TreC; UA, TP_{app} → OTP-PAT; IdP_S, TP_S → ADC;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other

Phase 3: Security Analysis

Is a formal analysis required?

no → **PAL 1** (Semi-formal analysis): MSC +Asms + Goals + Adversarial model → Self-assessment Evidence

yes → **PAL 3** (Formal analysis): MSC +Asms + Goals → Formal Spec mapping → Security Protocol Analyzer (Adversarial model)

Security Analysis Report

Did the analysis find attacks?

no → Phase 4

Phase 4: Usability Analysis

- Monitoring apps require a daily or even hourly use
- Mobile keyboards are small and sometimes uncomfortable to use.

The designed solution:

- does not ask Patient to enter the OTP; after the PIN input, the OTP value is sent to ADC in a transparent way.
- provides a SSO experience. Until the session is valid, Patient has to digit only her PIN to access TreC or other federated apps.

TreC DEMO - Exploitation Phase

Outline

- Introduction and Problem Statement

  Question 1: Mobile vs Browser-based Authentication

- Design Choices: Security and Usability Problems

  Exercise 1: embedded browser *Exercise 2*: OTP displayed on the screen

- Methodology Overview: TreC Scenario

  Question 2: e-health legal compliance

- Usability Discussion on TreC

  Exercise 3: TreC activation phase

- Conclusions and On-going/Future Work

  Question 3: Pros & Cons of our methodology and TreC solution

  Question 1bis: Mobile vs Browser-based Authentication

Usability Problems

The activation phase is too complex:

1. It requires the use of a smartcard reader
   - need for an installed software
   - some browser incompatibility

2. The users are bothered by the use of a complex password
   - easily forgettable

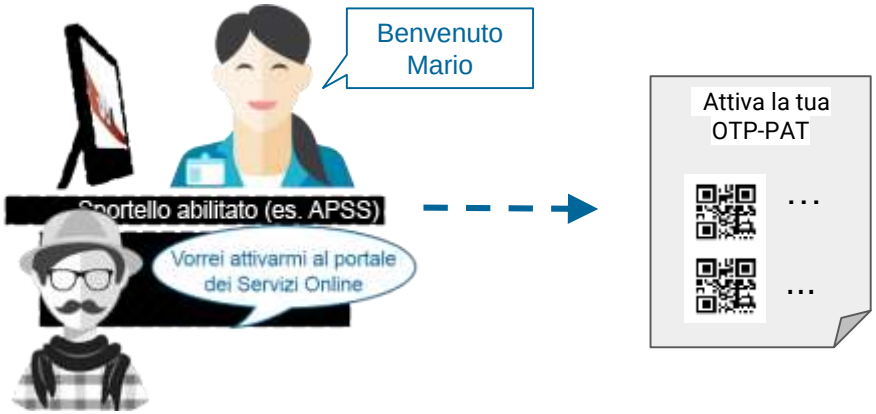
10 min left

How will you solve these two usability problems?

Activation of OTP-PAT: 2nd Solution

1.a Laptop Using a portal made available by ADC, User logs in with a LoA 2 and obtains an *QR code*.

1.b Help Desk A user, after an in-person identification, obtains an *QR code*.



Activation of OTP-PAT: 2nd Solution

2 Mobile On her mobile, User scan the QR code using OTP-PAT, enters a *temporary code* obtained on her email and generates her PIN

Outline

- Introduction and Problem Statement

Question 1: Mobile vs Browser-based Authentication

- Design Choices: Security and Usability Problems

Exercise 1: embedded browser *Exercise 2*: OTP displayed on the screen

- Methodology Overview: TreC Scenario

Question 2: e-health legal compliance

- Usability Discussion on TreC

Exercise 3: TreC activation phase

- Conclusions and On-going/Future Work

Question 3: Pros & Cons of our methodology and TreC solution

Question 1bis: Mobile vs Browser-based Authentication

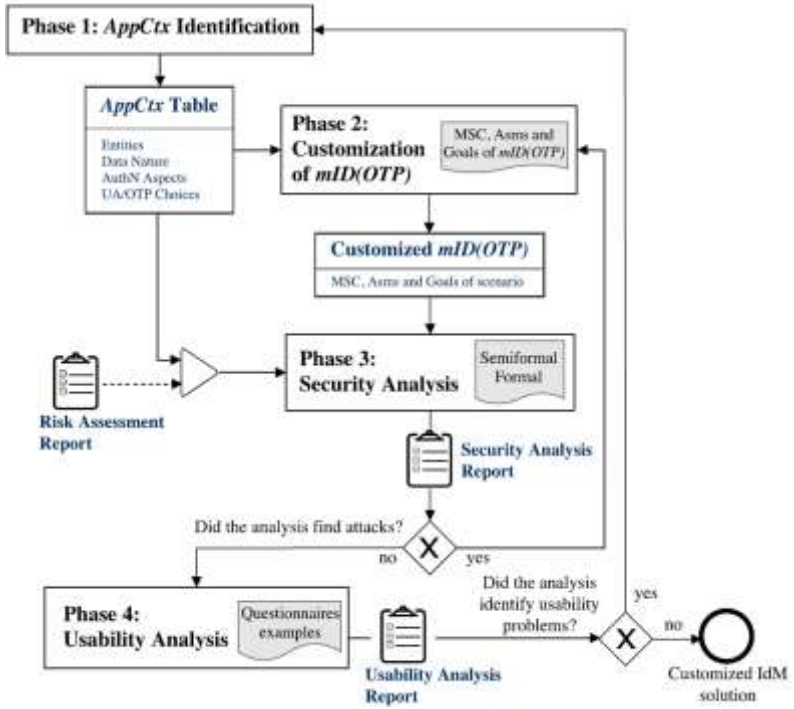
Conclusions and On-going/Future Work

- New methodology for the design and security assessment of mobile authentication and SSO solutions
- Covered aspects:
  - Security Usability Legal-provisioning
  - SSO MFA Native apps
- Real-world scenarios: TreC …

On-going - Future Work:

- Semi-automatic code generation
- Extensions of the AuthN aspects
- Formalization of other OTP generation approaches

Pros and Cons of our methodology and of the TreC solution?



Can we use web app authentication solutions for mobile apps?

Our Publications

- G. Sciarretta and A. Armando and R. Carbone and S. Ranise.
  Security of Mobile Single Sign-On: A Rational Reconstruction of Facebook Login Solution.
  Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4: SECRYPT, pages 147-158.
- G. Sciarretta, R. Carbone and S. Ranise.
  A delegated authorization solution for smart-city mobile applications.
  Proceedings of the 2nd International Forum on Research and Technologies for Society and Industry leveraging a better tomorrow (RTSI 2016).
- G. Sciarretta, R. Carbone, S. Ranise and A. Armando.
  Anatomy of the Facebook solution for mobile single sign-on: Security assessment and improvements.
  Journal of Computers & Security (COSE 2017).
- G. Sciarretta, R. Carbone, S. Ranise and L. Viganò.
  Design, Formal Specification and Analysis of Multi-Factor Authentication Solutions with a Single Sign-On Experience.
  Proceedings of the 7th International Conference on Principles of Security and Trust (POST 2018).

https://st.fbk.eu/publications/POST-2018

https://st.fbk.eu/workshop-ifipsc-18

ranise@fbk.eu - giada.sciarretta@fbk.eu

Thanks for your attention!

Any questions?

Acknowledgements. This work has partially been supported by the activity “STAnD” of the action line Digital Infrastructure of the EIT Digital.