Secure and Usable Mobile Identity Management Solutions:

a Methodology for their Design and Assessment

Roberto Carbone - Silvio Ranise - Giada Sciarretta Andrea De Maria

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

UNIVERSITY OF TRENTO - Italy

ISTITUTO POLIGRAFICO E ZECCA DELLO STATO

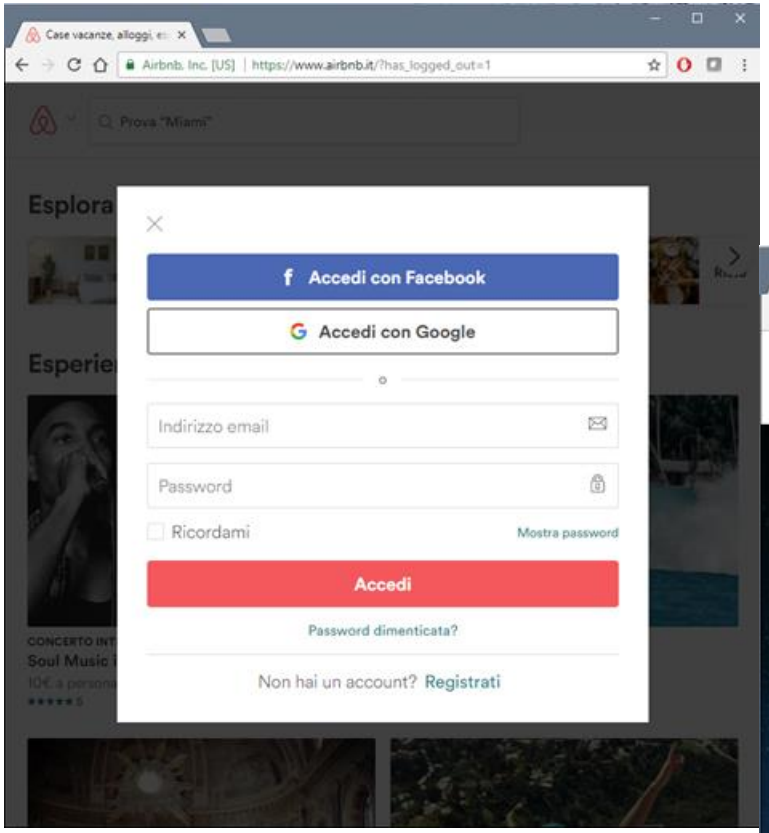
https://st.fbk.eu/tutorial-itasec-18

Outline

- IdM Mobile Context
- Problem Statement and Methodology Overview
- TreC Scenario
- IPZS/CIE Scenario
- Conclusions

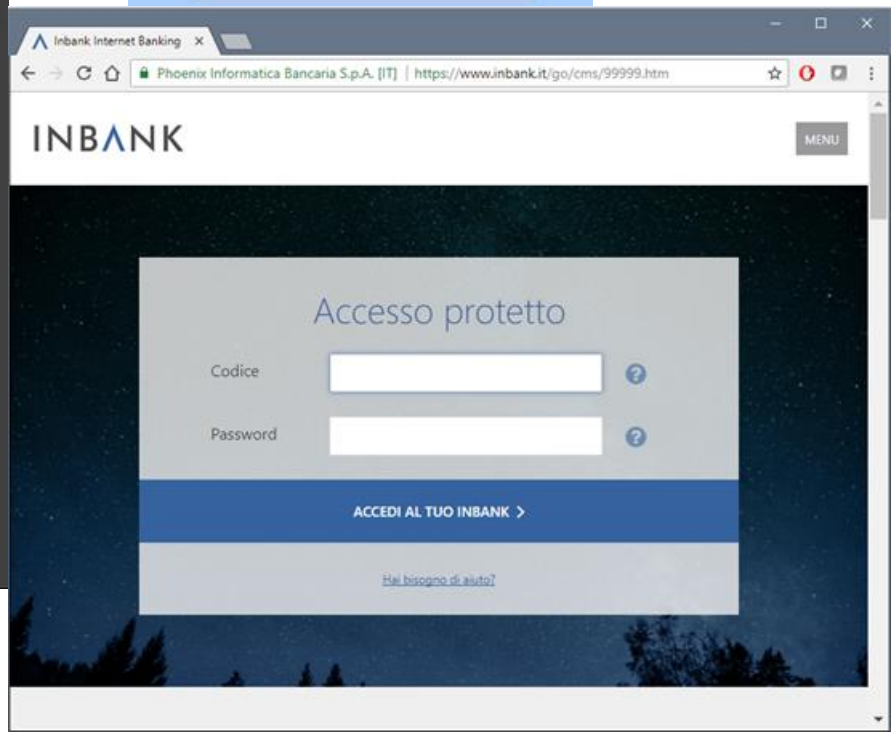
Digital Identities

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

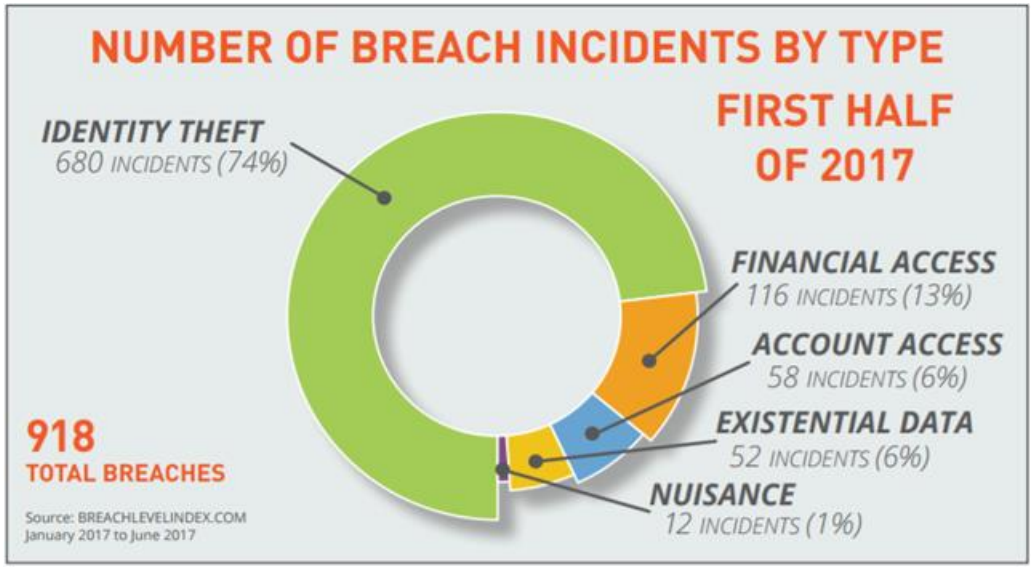


Personal data

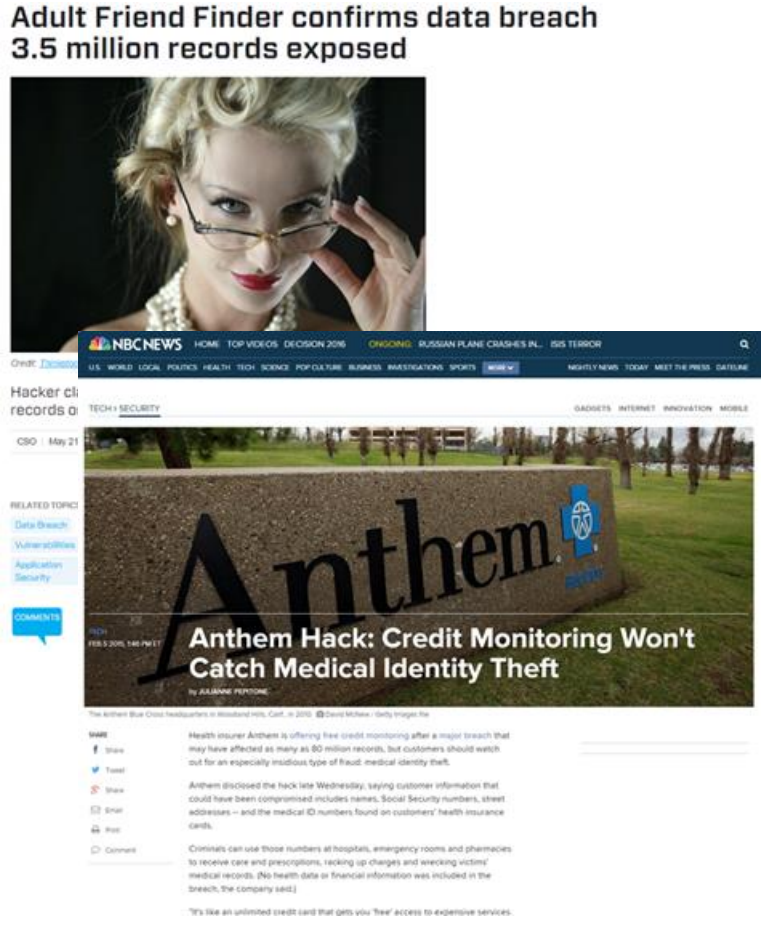
Sensitive data



Digital Identities: Identity Theft



http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf

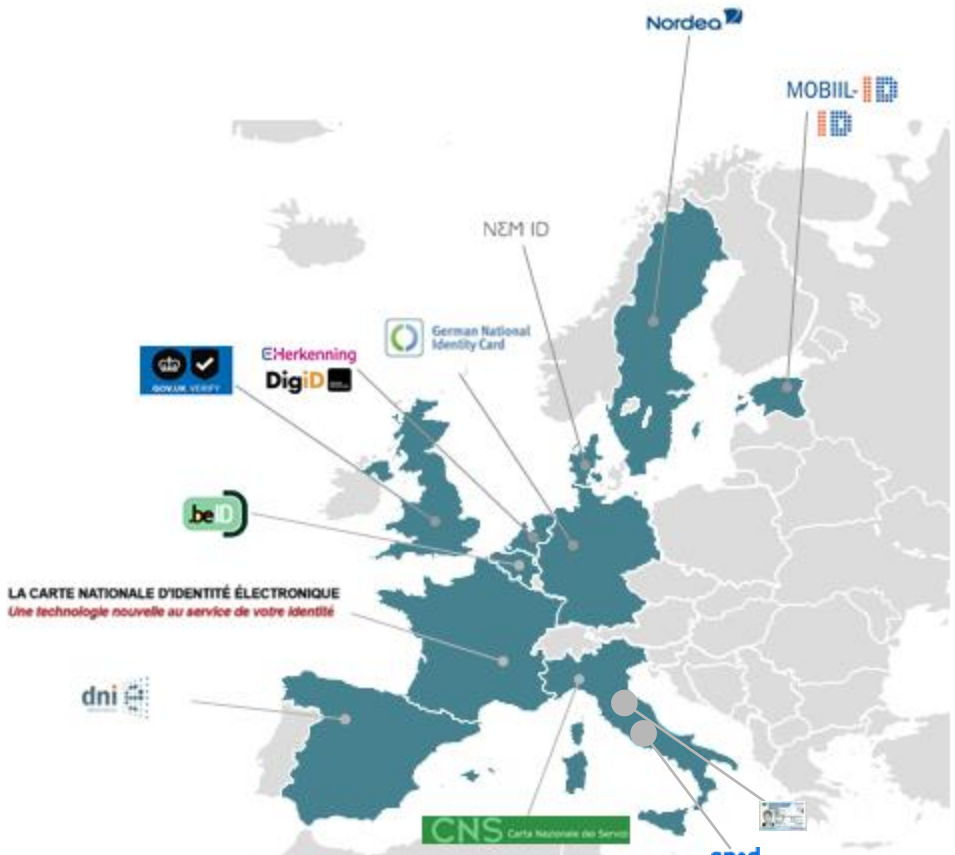


Consider security from the early stage is crucial

Design

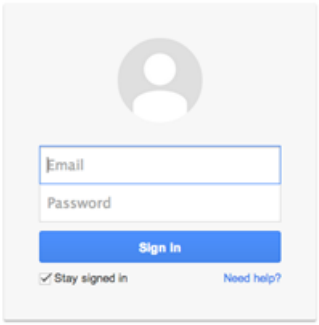
Implementation

Digital Identity solutions across Europe



https://www.signicat.com/eid-world-map/

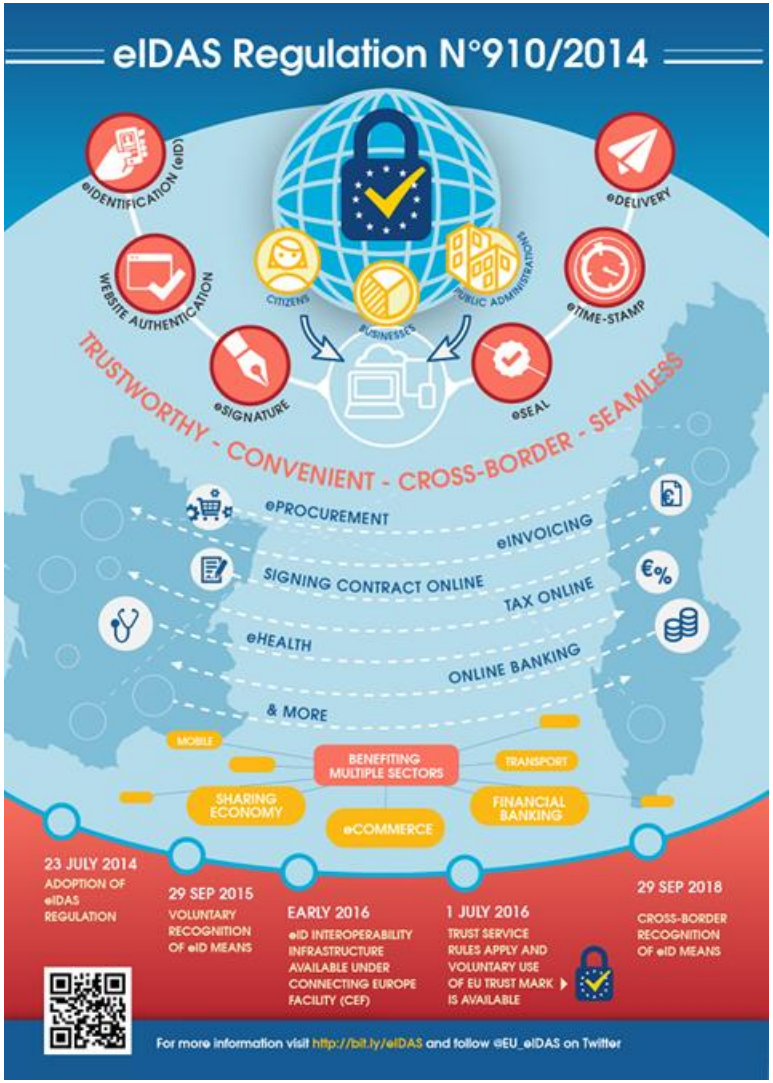
- many national digital identity solutions
- different technological choices:



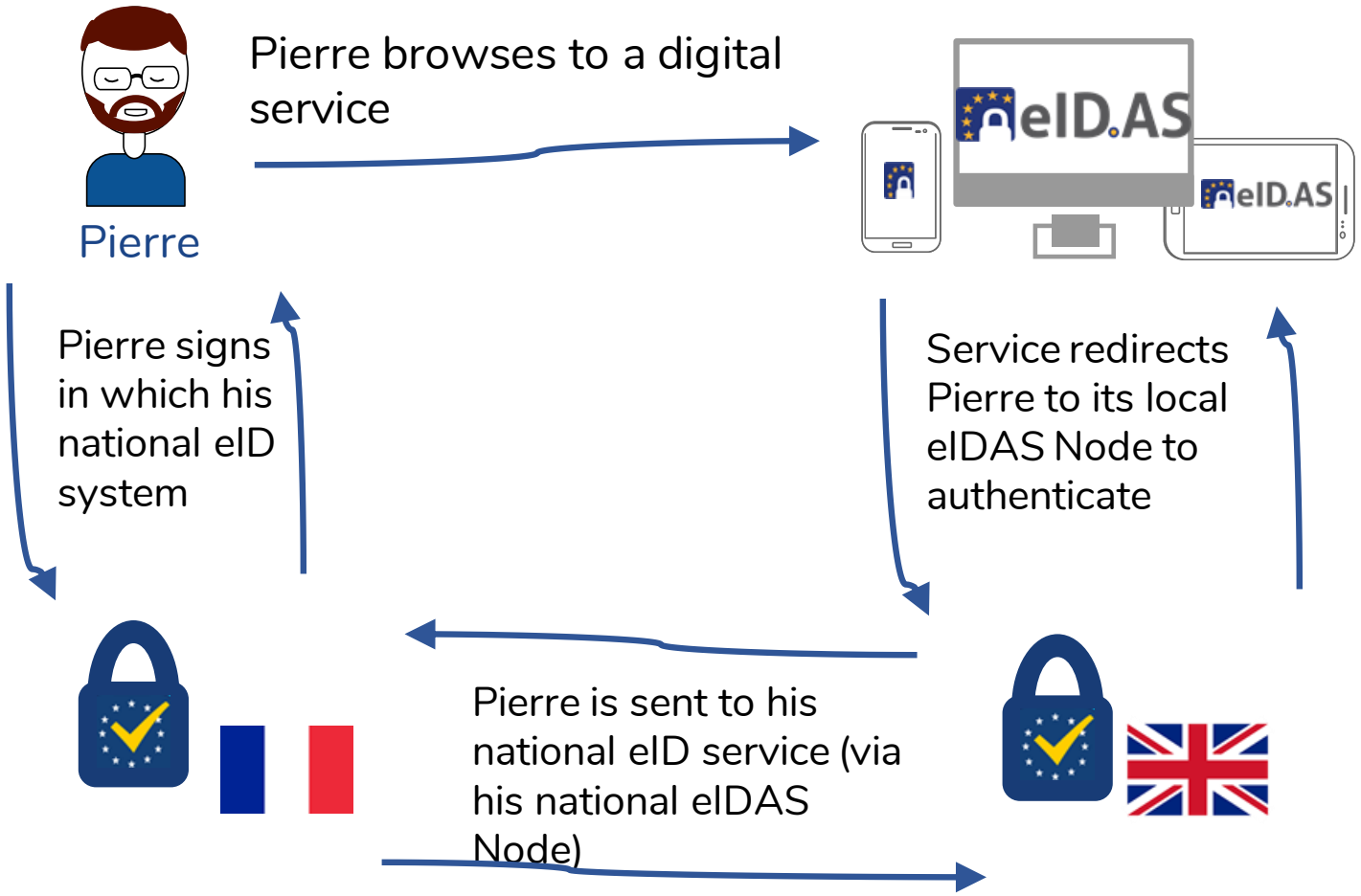
Digital Single Market: eIDAS

DIGITAL AGENDA FOR EUROPE
A Europe 2020 Initiative

- Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on *electronic identification and trust services for electronic transactions in the internal market* and repealing Directive 1999/93/EC - eIDAS
- Directive 1999/93/CE of the European Parliament and of the Council of 13 December 1999 on a Community framework for *electronic signatures*



eIDAS Example: opening bank account



SPID

The entity responsible for carrying on the principles exposed by the DAE in Italy is the AgID

- DPCM of 24 October 2014, Sistema Pubblico per la gestione dell'Identità Digitale - SPID
- Introduced by the Article 17-ter of the "Decreto del Fare", which modifies the coma 2 of the Article 64 of the CAD (Codice per l'Amministrazione Digitale) on *the modalities of access to the on-line services released by the PA*

After Germany, Italy is the second European country on the path toward the European interoperability.

Our Focus: Authentication

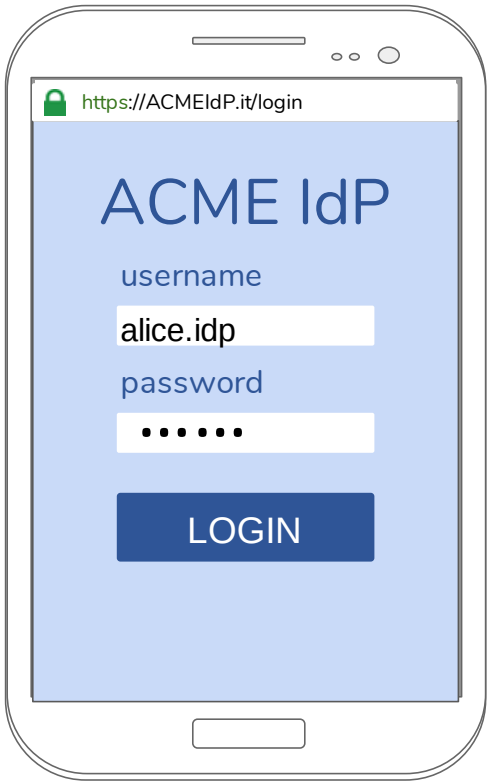
Authentication: process of verifying a user's identity

identification step

You announce who you are

verification step

You prove that you are who you claim to be



ACME IdP
(Identity Provider)

Authentication is closely related to **authorization** (e.g., authenticated identities are the basis for access control)

Single Sign-On (SSO)

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

- Credentials only with idp
- Session handled between apps

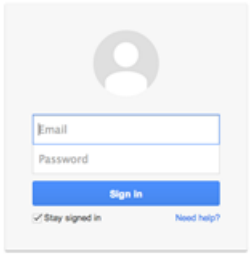
Multi-Factor Authentication

Basic authentication (with only passwords) is no longer sufficient

Two-factor authentication is required to use some of the latest features of iOS, macOS, and iCloud.

Multi-Factor Authentication

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.

mutually independent

one of the elements should be **non-reusable** and **non-replicable**

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.

Key Aspects of our Analysis

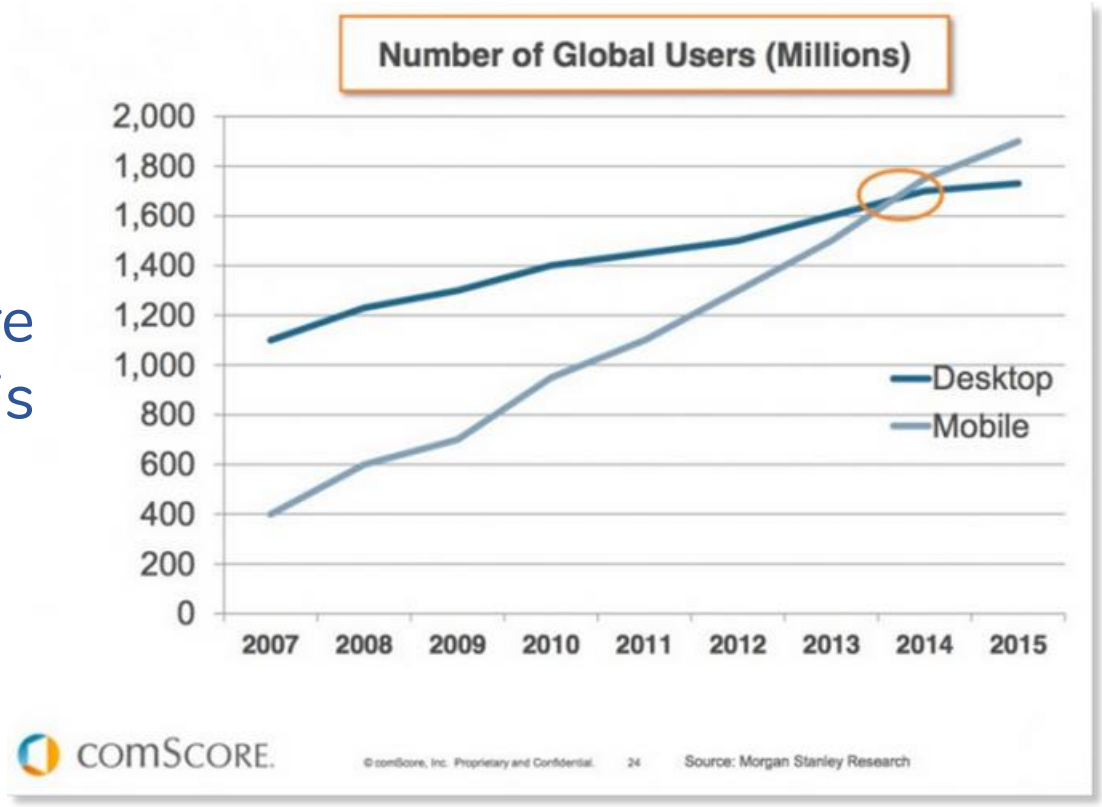
- Single Sign-on

- Multi-factor Authentication

- Mobile Native apps

Mobile vs Desktop

Today, we are long past this tipping point



Number of Mobile Users

65%

5.1B

Share of Web Pages Views

YEAR-ON-YEAR

+50%

-20%

https://wearesocial.com/special-reports/digital-in-2017-global-overview

Mobile native apps vs Web (apps)

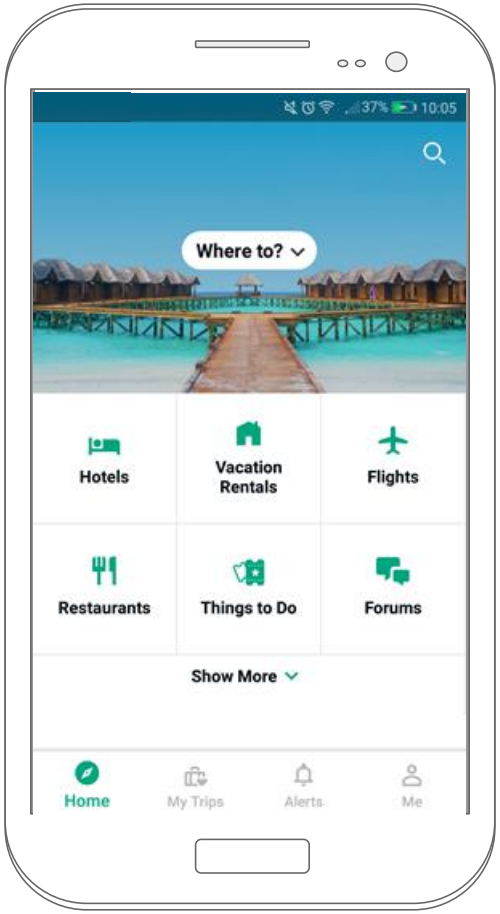
Native Apps

Richer Experience

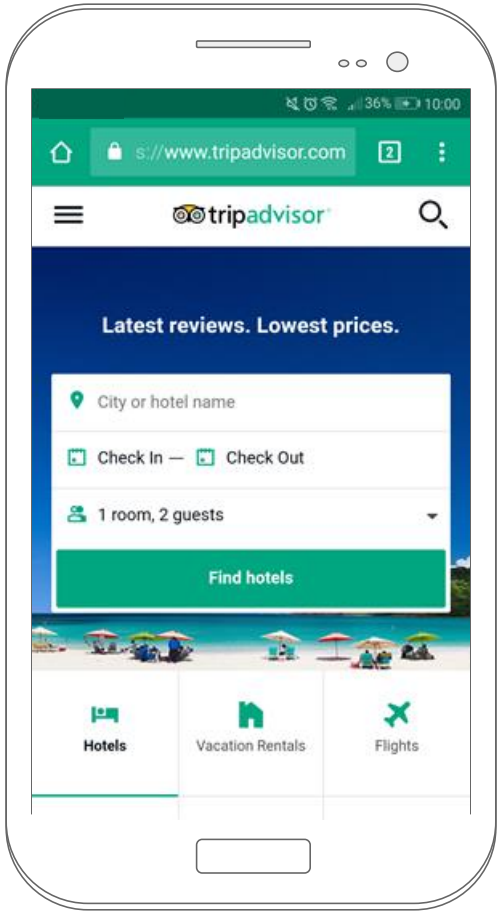
Marketing

Offline Data

Earning Bucks



Web Apps



Any Platform

Web Standards

Editorial

Cheaper

Mobile native apps vs Web (apps)

market

Native Apps

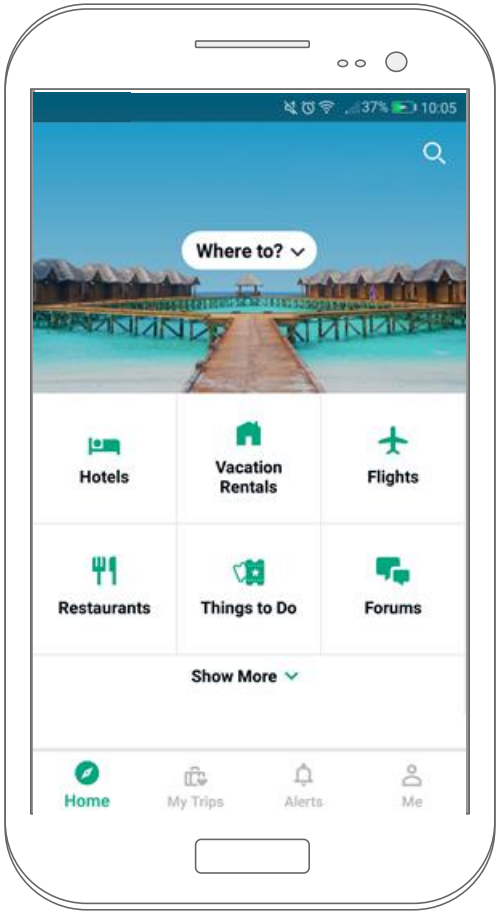
Web Apps

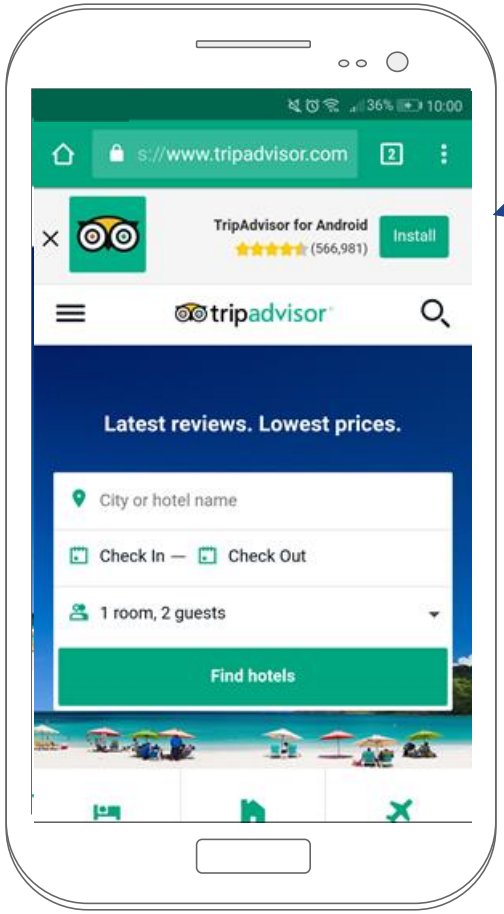
Richer Experience

Marketing

Offline Data

Earning Bucks





Any Platform

Web Standards

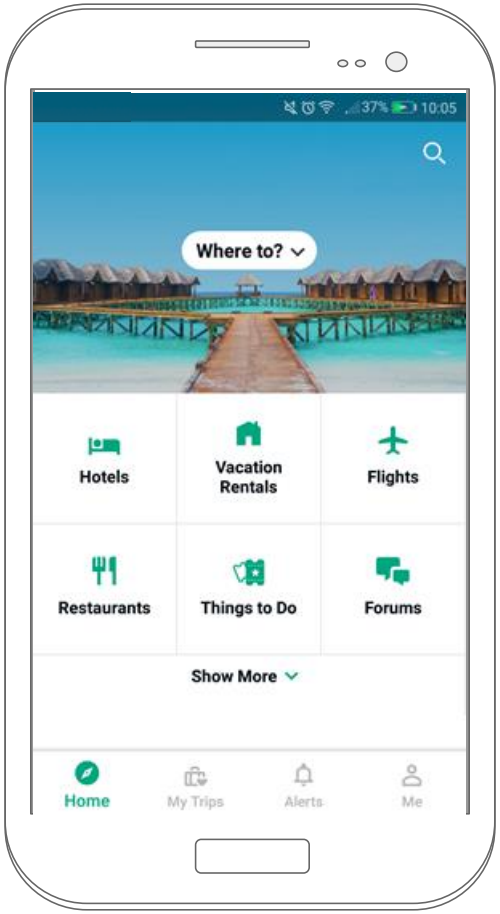
Editorial

Cheaper

Mobile native apps vs Web (apps)

market

Native Apps



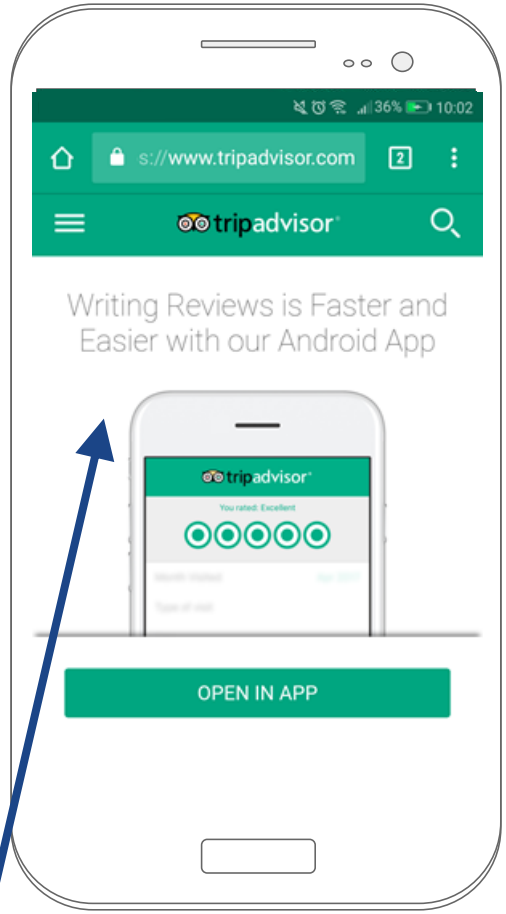
Richer Experience

Marketing

Offline Data

Earning Bucks

Web Apps



Any Platform

Web Standards

Editorial

Cheaper

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

IdM Protocols: Desktop vs Mobile

- SAML 2.0 - SSO Profile: consolidated, corporate & governmental environments
- OAuth 2.0 & OpenID Connect: used for social network (billions of user)

IdM Protocols: Desktop vs Mobile

- SAML 2.0 - SSO [illegible] corporate & governmental environments

no mobile support

- OAuth 2.0 & OpenID Connect 1.0 social network (bil[illegible]

only marginal mobile support

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: Desktop vs Mobile

- SAML 2.0 - SSO [no mobile support] corporate & governmental environments
- OAuth 2.0 & Open[only marginal mobile support] social network (bil

OAuth/OIDC Working Group have 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

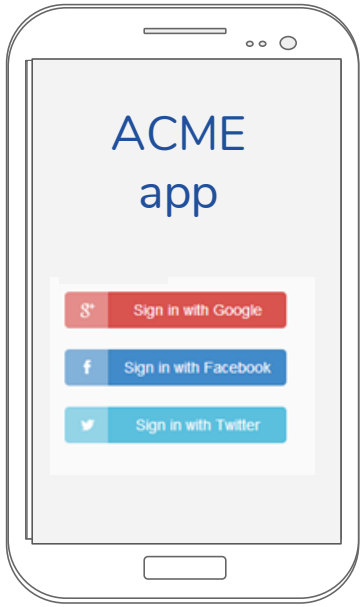
E. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague. OAuth Demystified for Mobile Application Developers. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2014.
M. Shehab and F. Mohsen. Towards Enhancing the Security of OAuth Implementations in Smart Phones.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

Limitations for Mobile Authentication

Lack of standardizations

Rigid proprietary solutions

OAuth for native apps [RFC 8252]
(2017) - BEST CURRENT PRACTICE



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

Only self-declared identities (Level of Assurance Low)

Key Aspects of our Analysis

- Single Sign-on

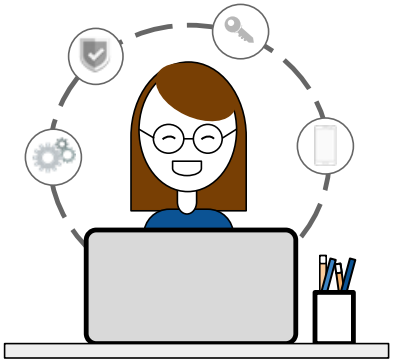
- Multi-factor Authentication

- Mobile Native apps

Outline

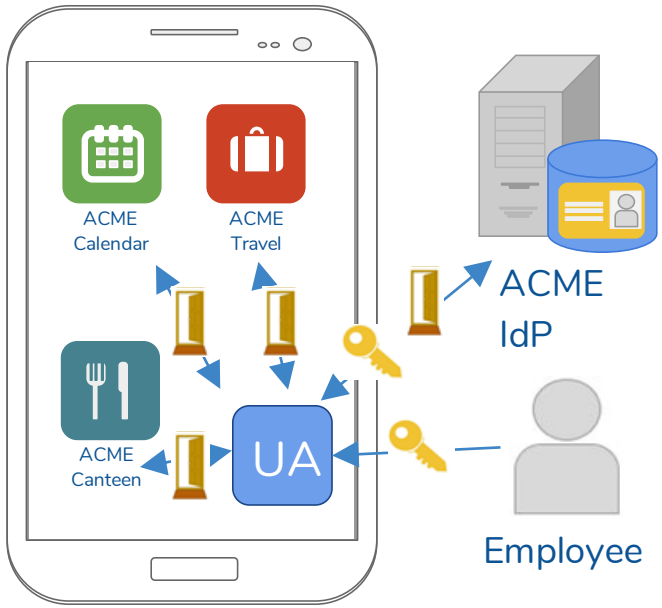
- IdM Mobile Context
- Problem Statement and Methodology Overview
- TreC Scenario
- IPZS/CIE Scenario
- Conclusions

Design for an IdM Solution



Scenario Single Sign-On:

- ACME Identity Provider (IdP)
- ecosystem of ACME mobile apps
- a UA that manages interactions between ACME apps and ACME IdP



Design Choices

IdM Designer

TODO List

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

Design Choices

IdM 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

IdM 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

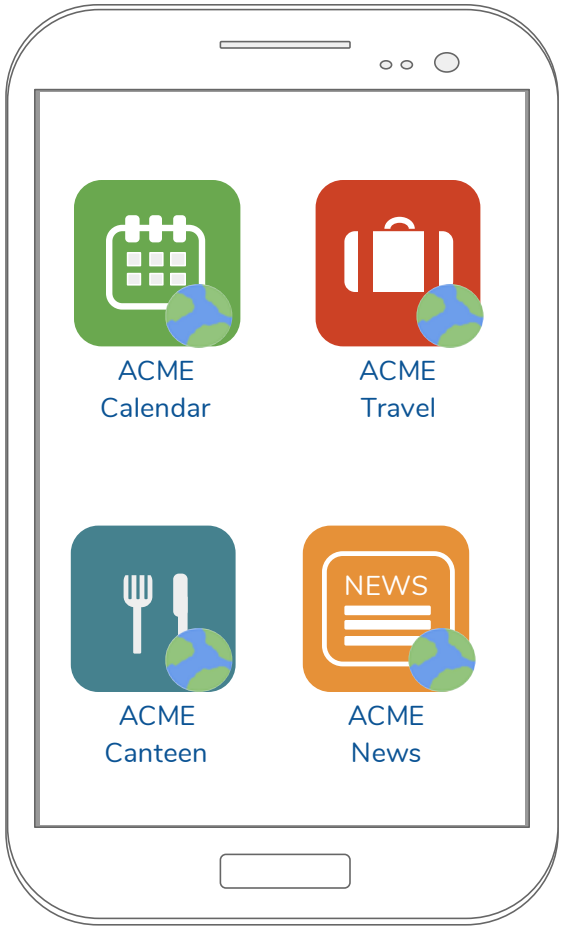
TODO List

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

Wrong design choices could lead to security and usability problems

Example of wrong design choices

User Agent (UA) Choice: embedded browser



ACME IdP

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.

Example of wrong design choices

User Agent (UA) Choice: embedded browser

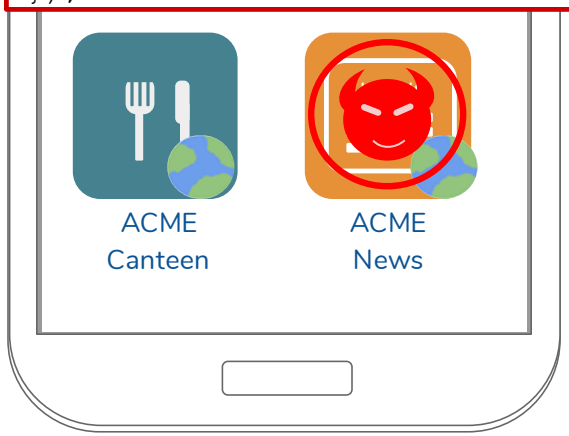
Security

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

Usability: no SSO

ACME 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);
 }
});
```

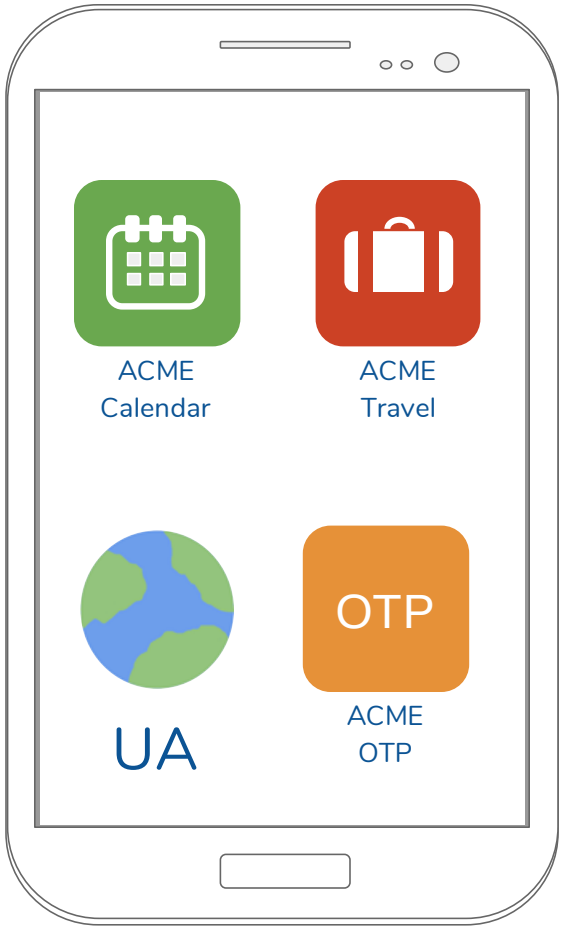


ACME IdP

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.

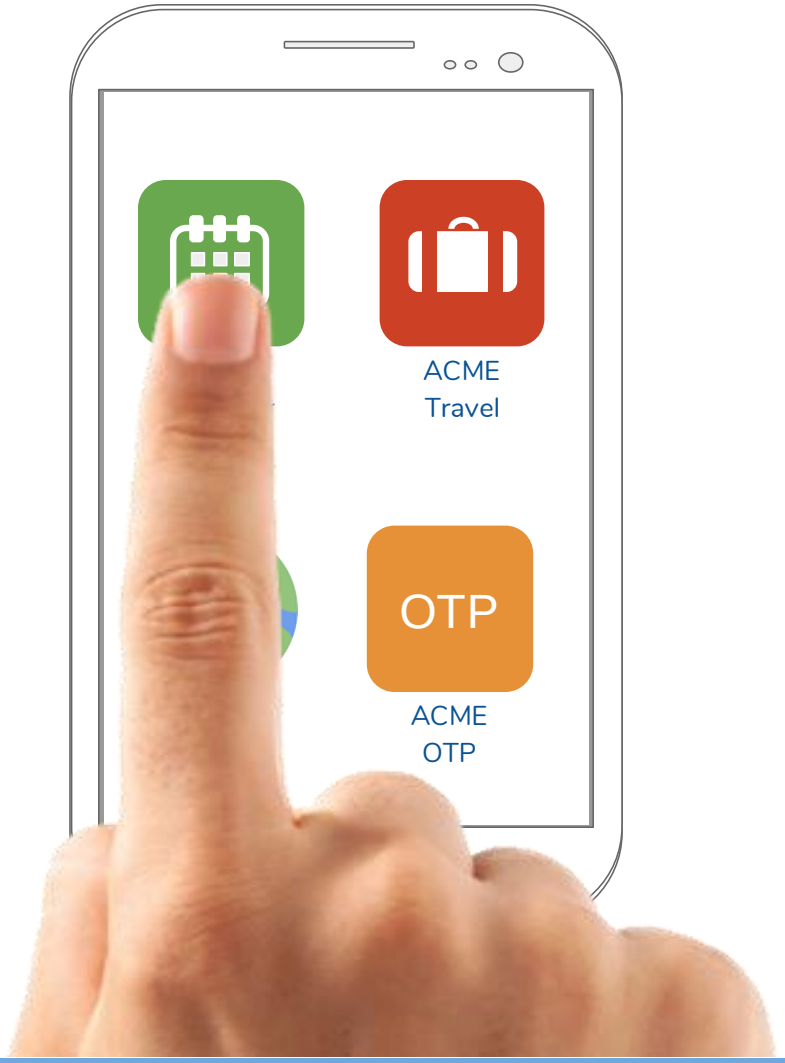
Example of wrong design choices

OTP Choice: app that shows the OTP value



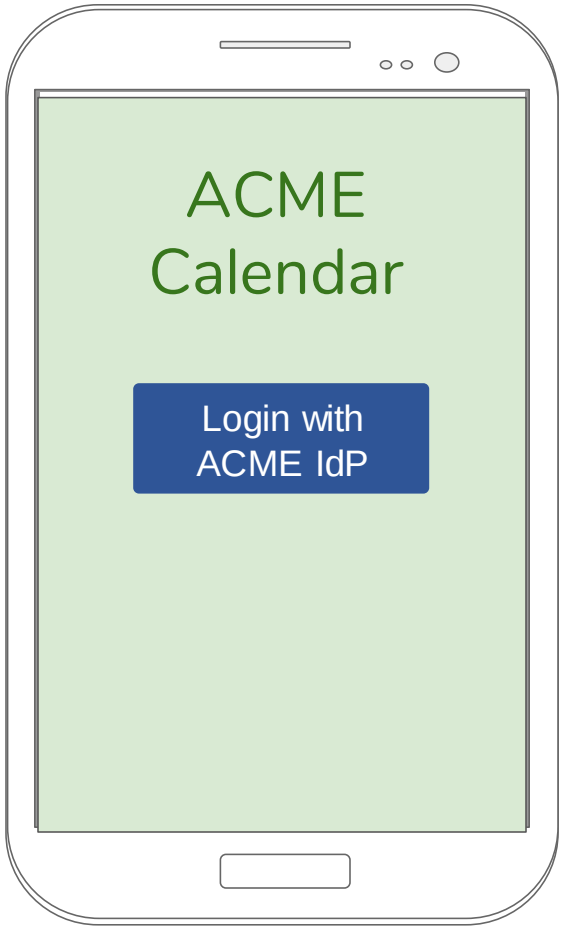
Example of wrong design choices

OTP Choice: app that shows the OTP value



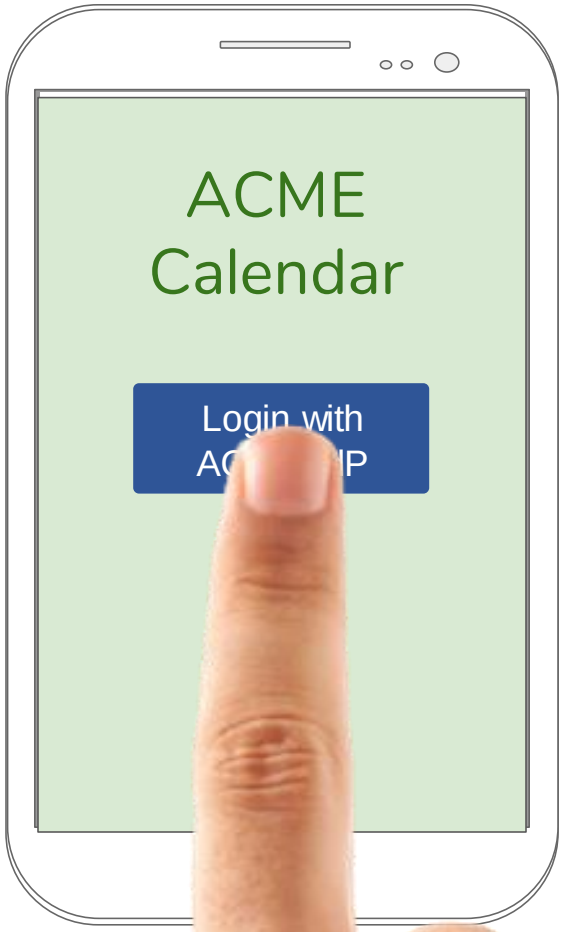
Example of wrong design choices

OTP Choice: app that shows the OTP value



Example of wrong design choices

OTP Choice: app that shows the OTP value



Example of wrong design choices

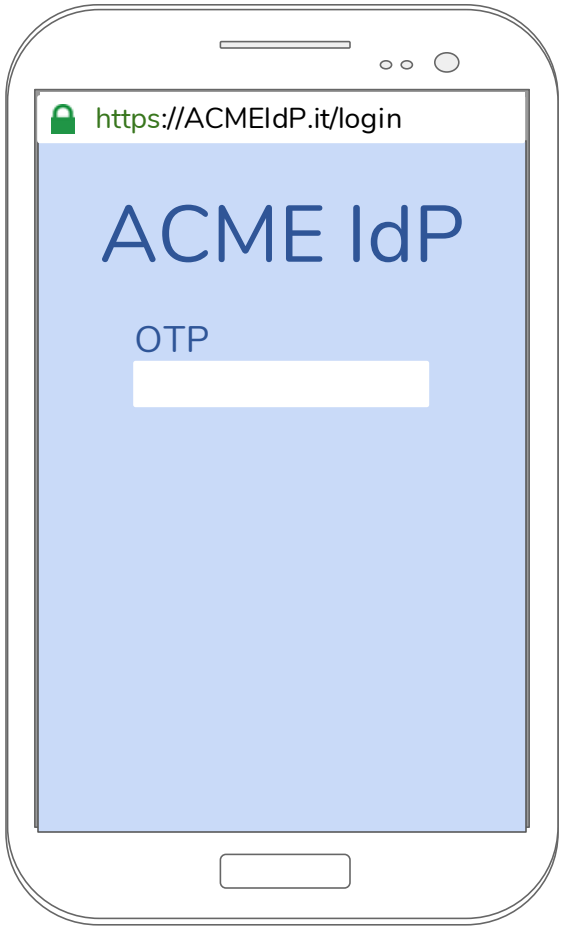
OTP Choice: app that shows the OTP value

Example of wrong design choices

OTP Choice: app that shows the OTP value

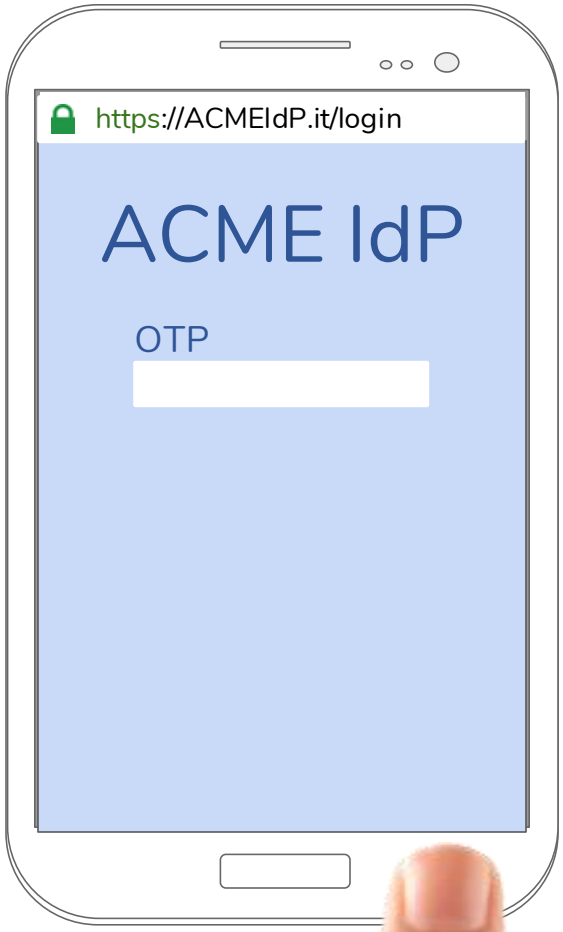
Example of wrong design choices

OTP Choice: app that shows the OTP value



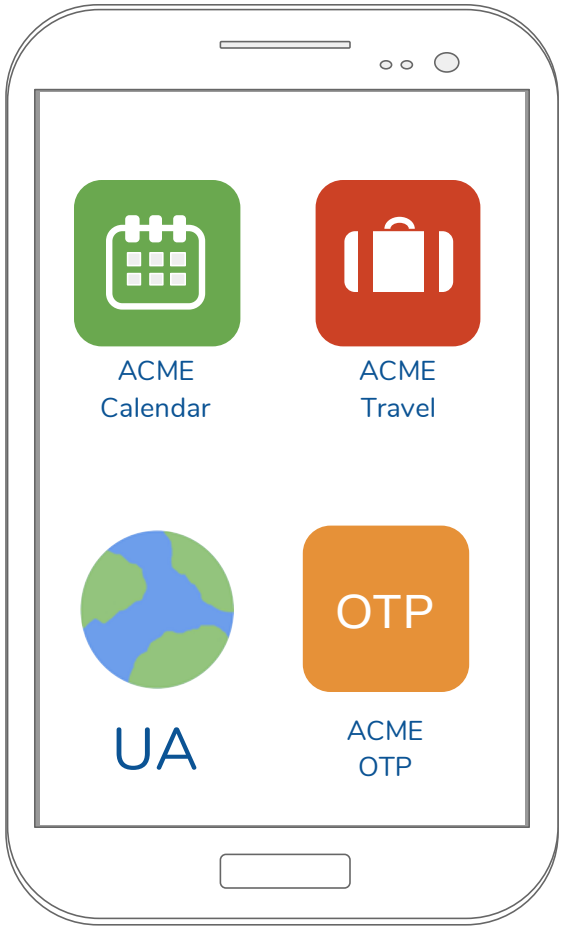
Example of wrong design choices

OTP Choice: app that shows the OTP value



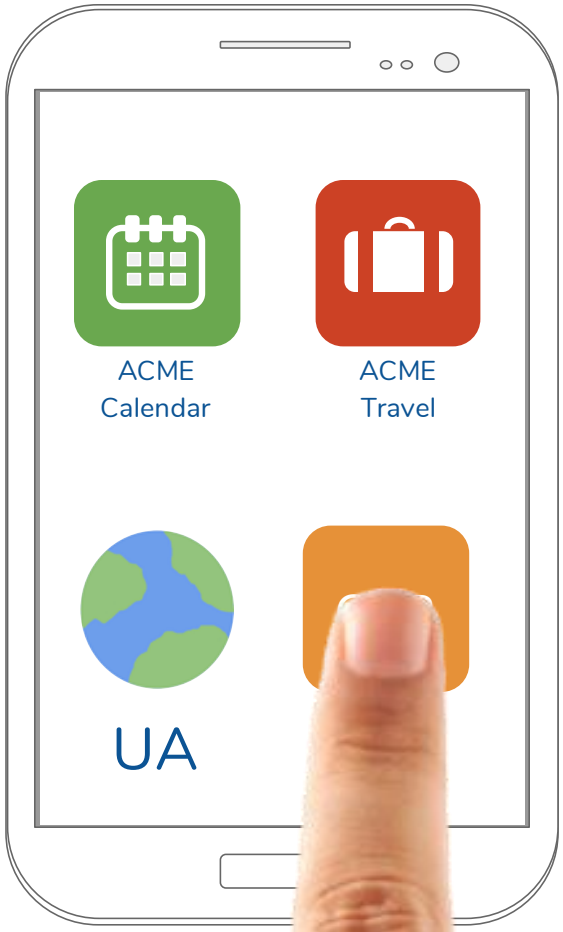
Example of wrong design choices

OTP Choice: app that shows the OTP value



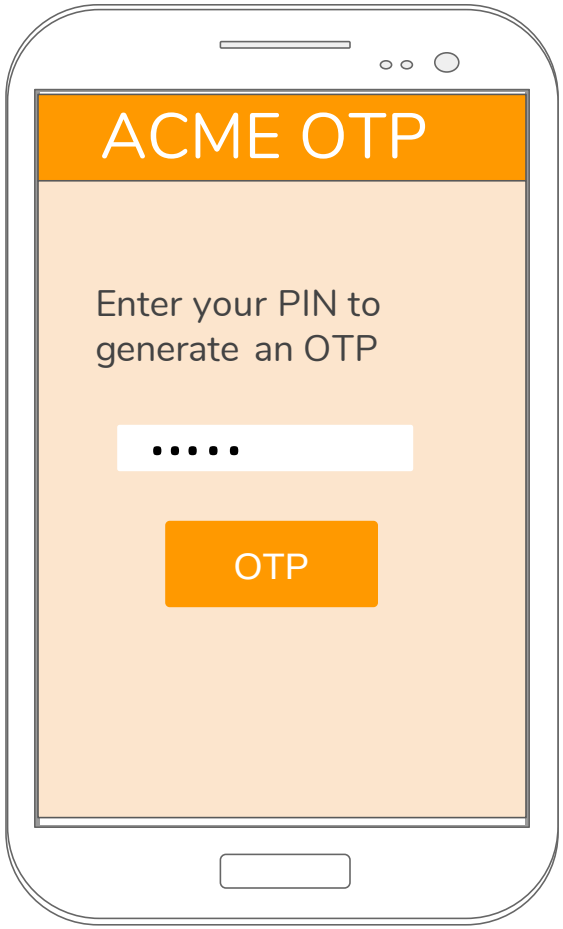
Example of wrong design choices

OTP Choice: app that shows the OTP value



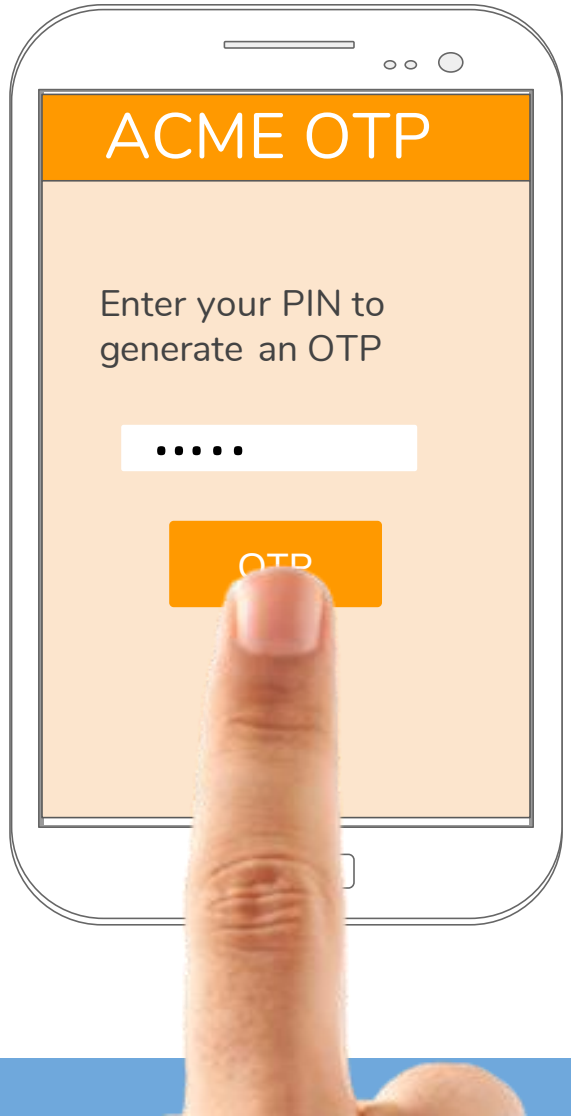
Example of wrong design choices

OTP Choice: app that shows the OTP value



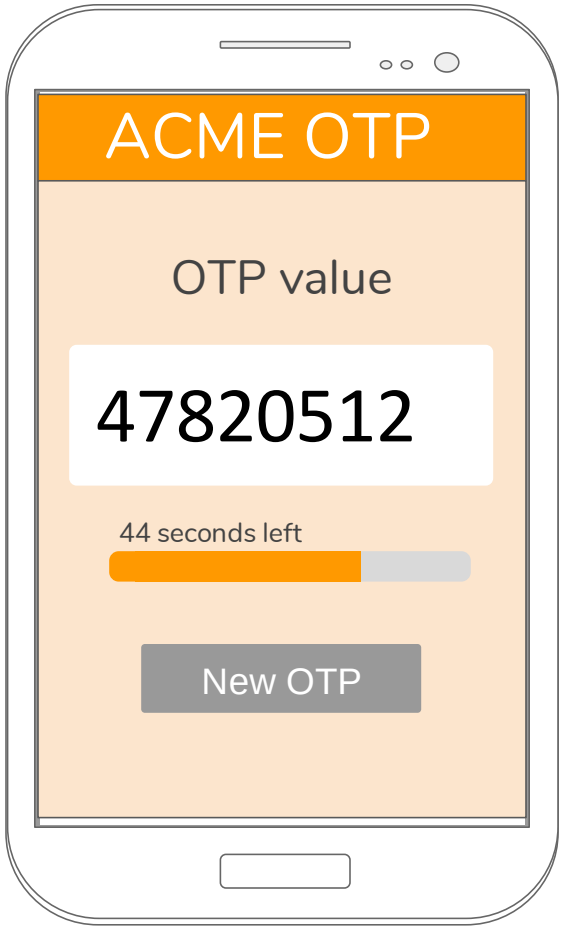
Example of wrong design choices

OTP Choice: app that shows the OTP value



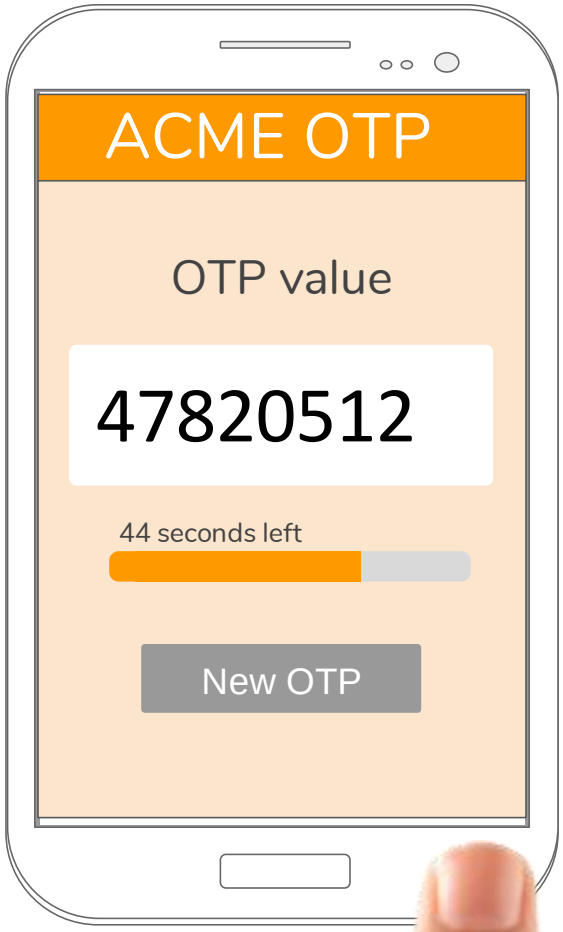
Example of wrong design choices

OTP Choice: app that shows the OTP value



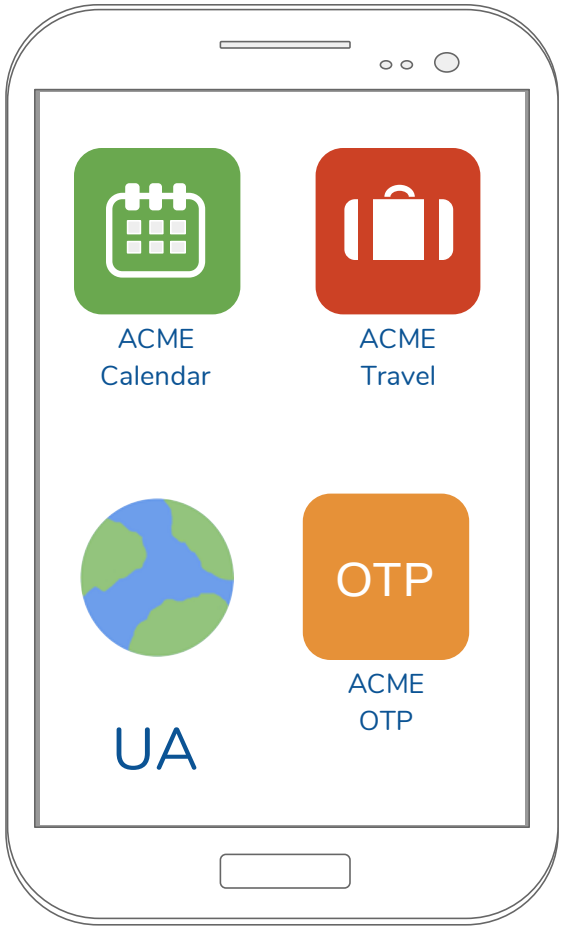
Example of wrong design choices

OTP Choice: app that shows the OTP value



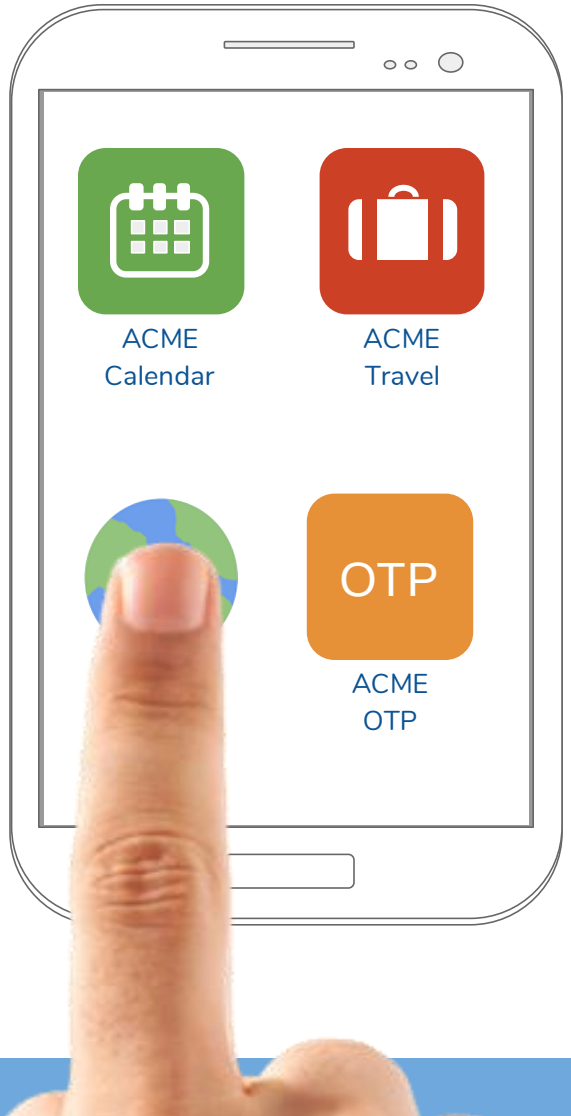
Example of wrong design choices

OTP Choice: app that shows the OTP value



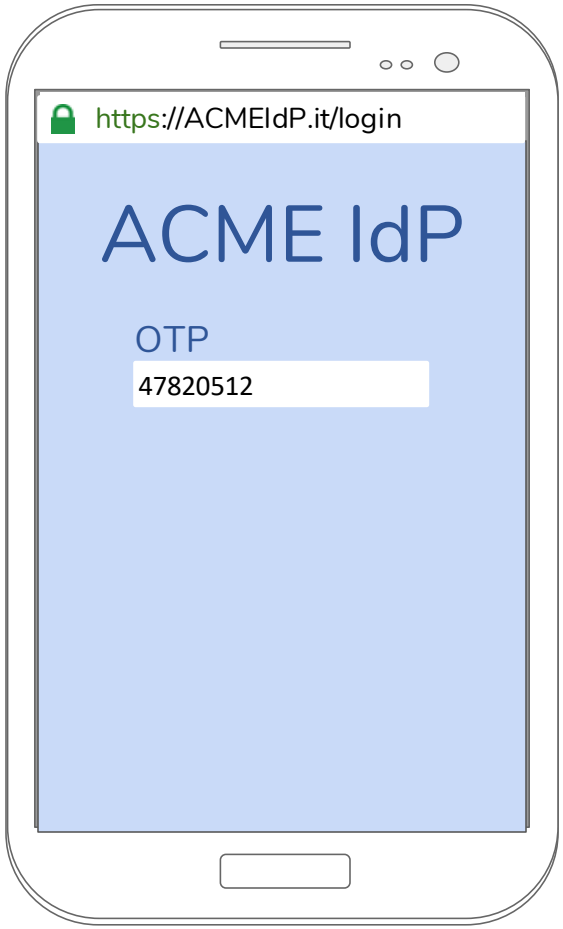
Example of wrong design choices

OTP Choice: app that shows the OTP value



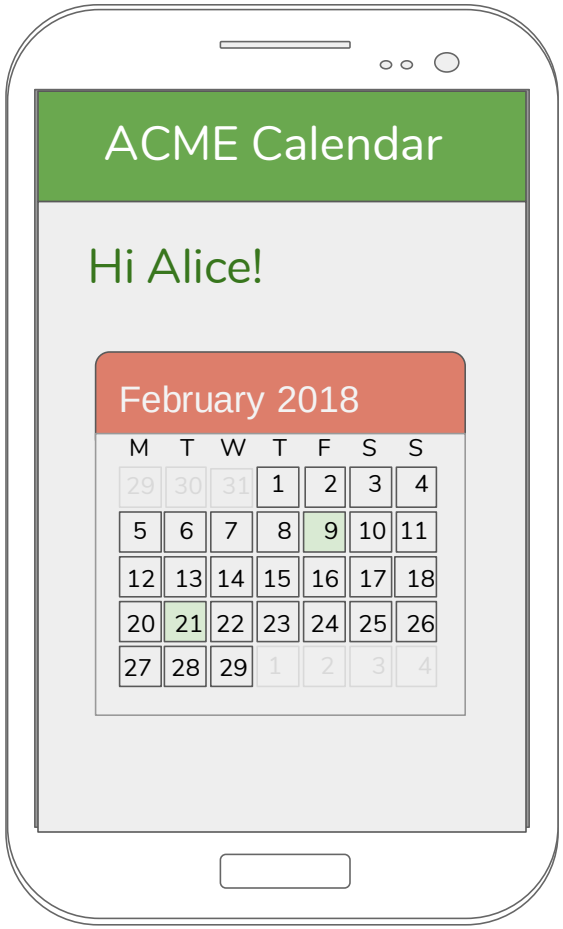
Example of wrong design choices

OTP Choice: app that shows the OTP value



Example of wrong design choices

OTP Choice: app that shows the OTP value



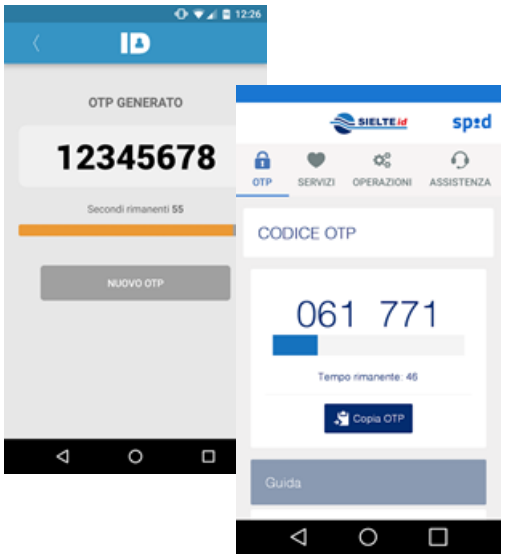
Security: Copy&Paste

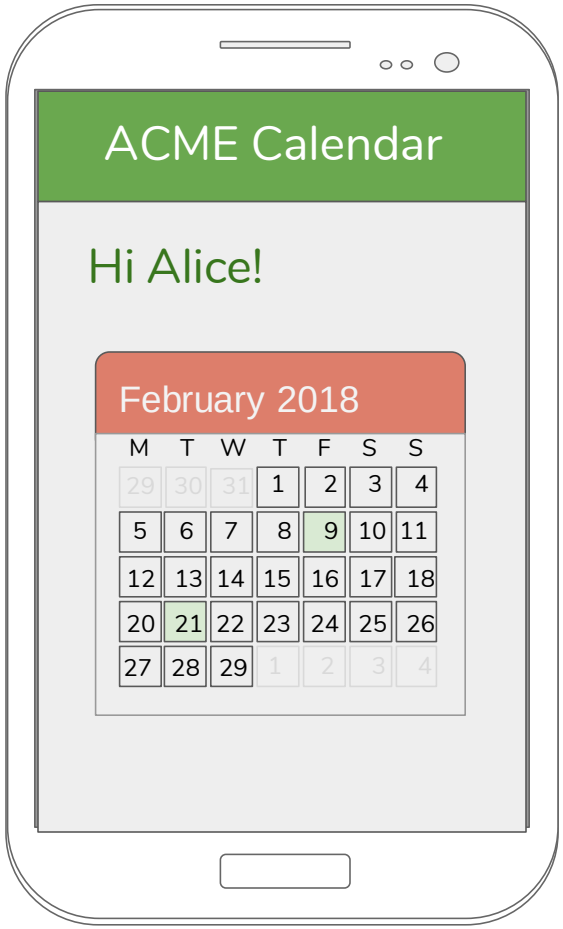
Usability: move from an app to another (burdensome for the user in terms of time and difficulty)

Example of wrong design choices

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)

Design for an IdM Solution

IdM Designer

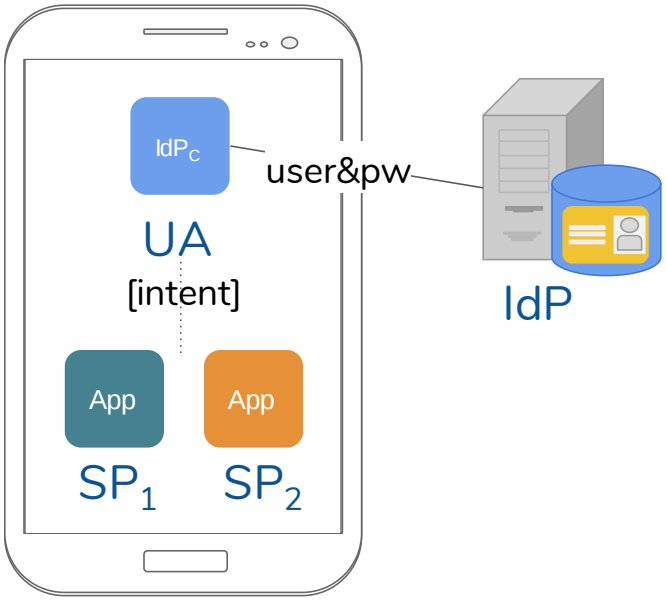
Design for an IdM Solution

We provide:

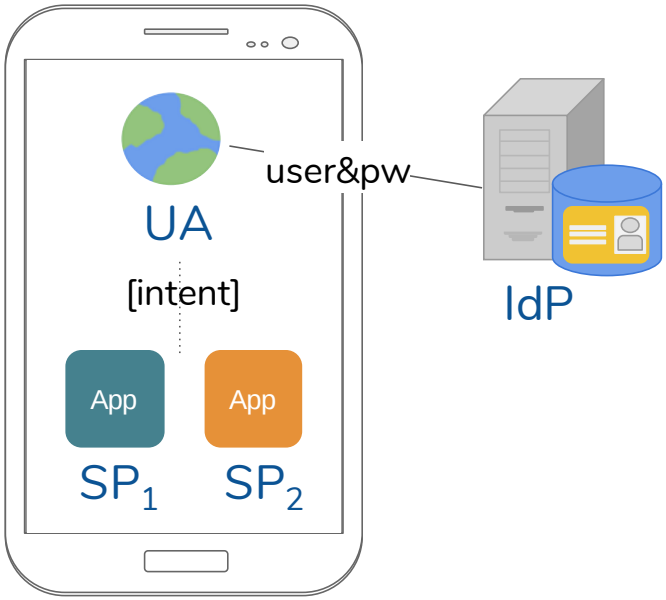
- a reference model *mID(OTP)* for mobile IdM solutions
- a methodology to assist the IdM designer in the customization of *mID(OTP)* and in the analysis of its security and usability

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)



facebook



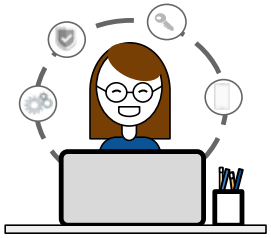
Reference Model - *mID(OTP)*

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

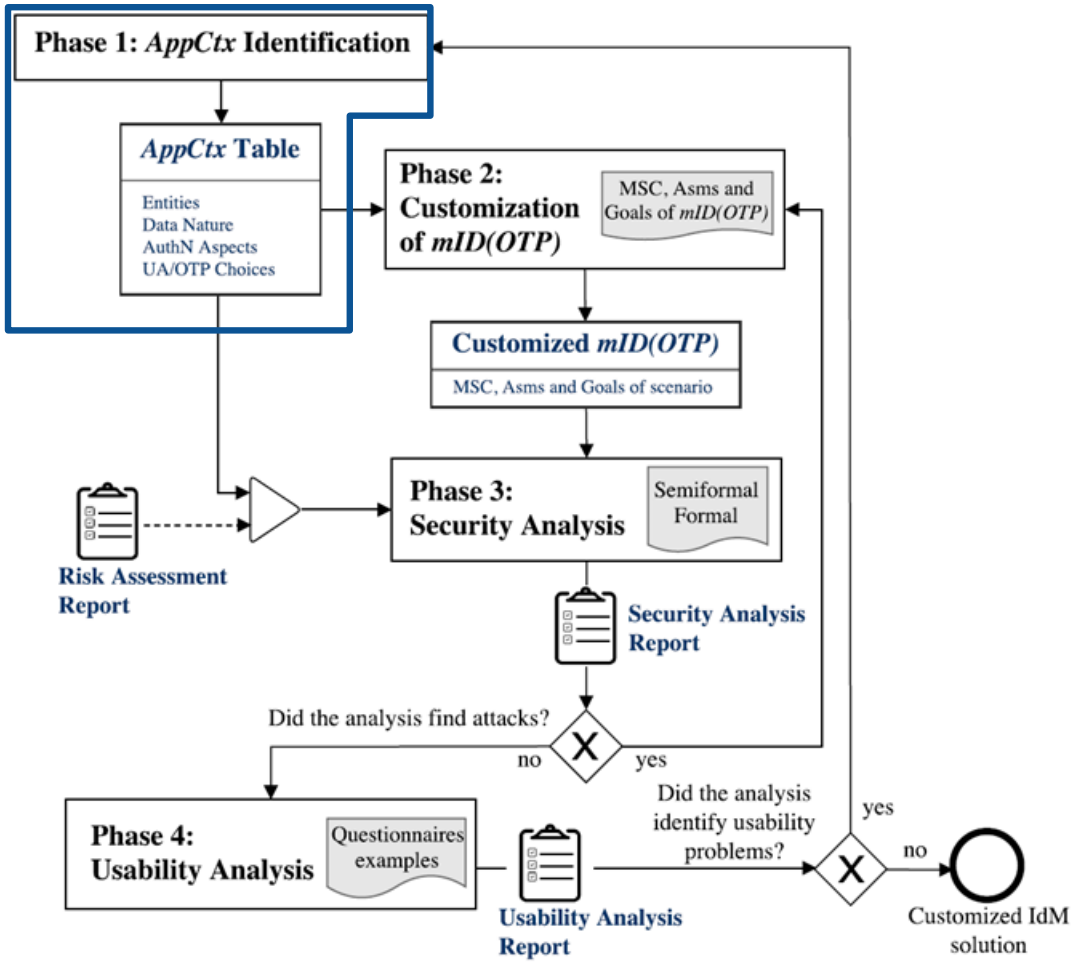
- The name *mID(OTP)* is to highlight the dual goal that our model pursued:
  - "*mID*" represents the management of identities for native mobile apps providing SSO experience
  - "*(OTP)*" represents the optional establishment of a MFA parametric on the OTP generation (TOTP and CR)

Methodology Overview

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

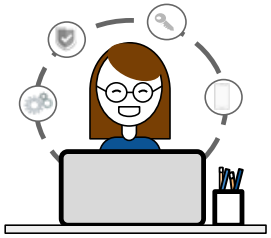


IdM Designer

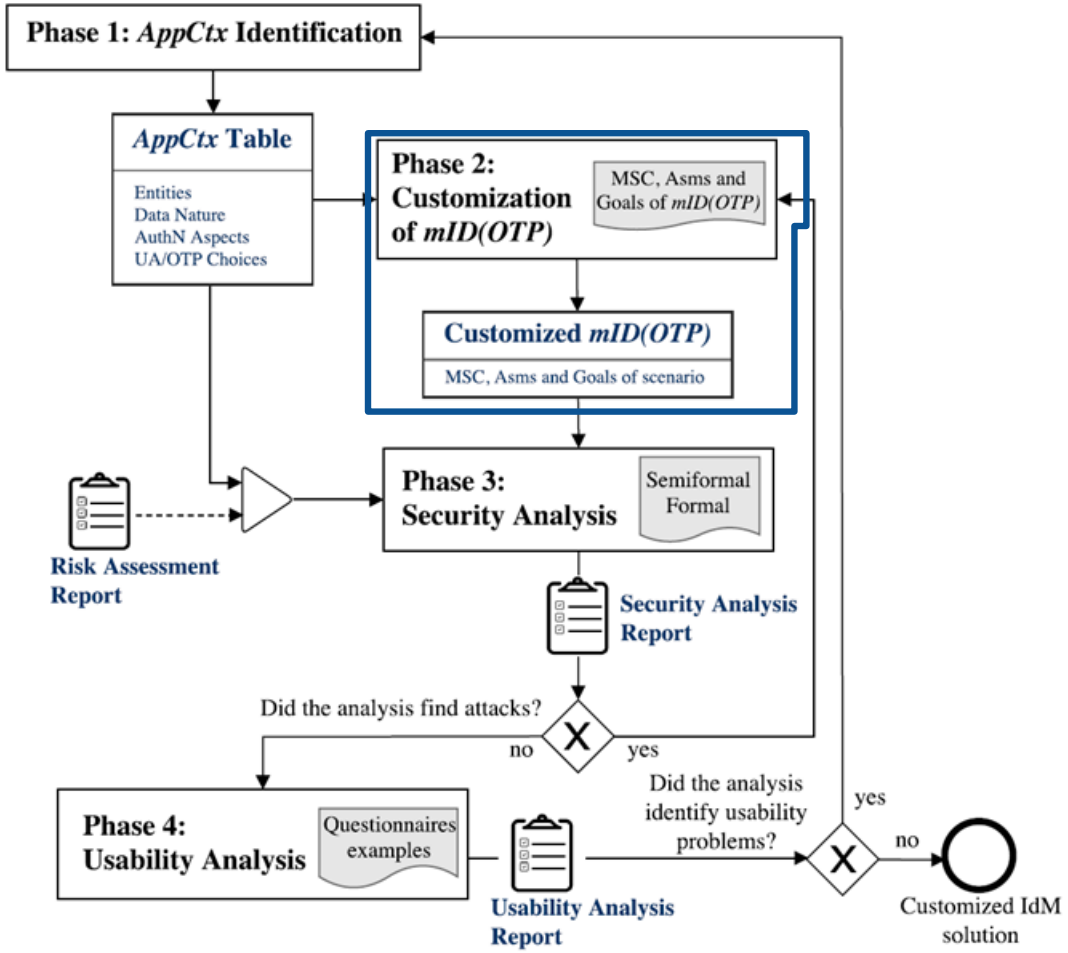


Methodology Overview

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

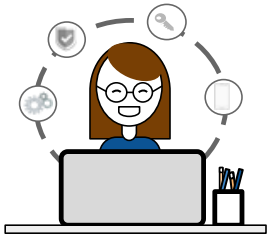


IdM Designer



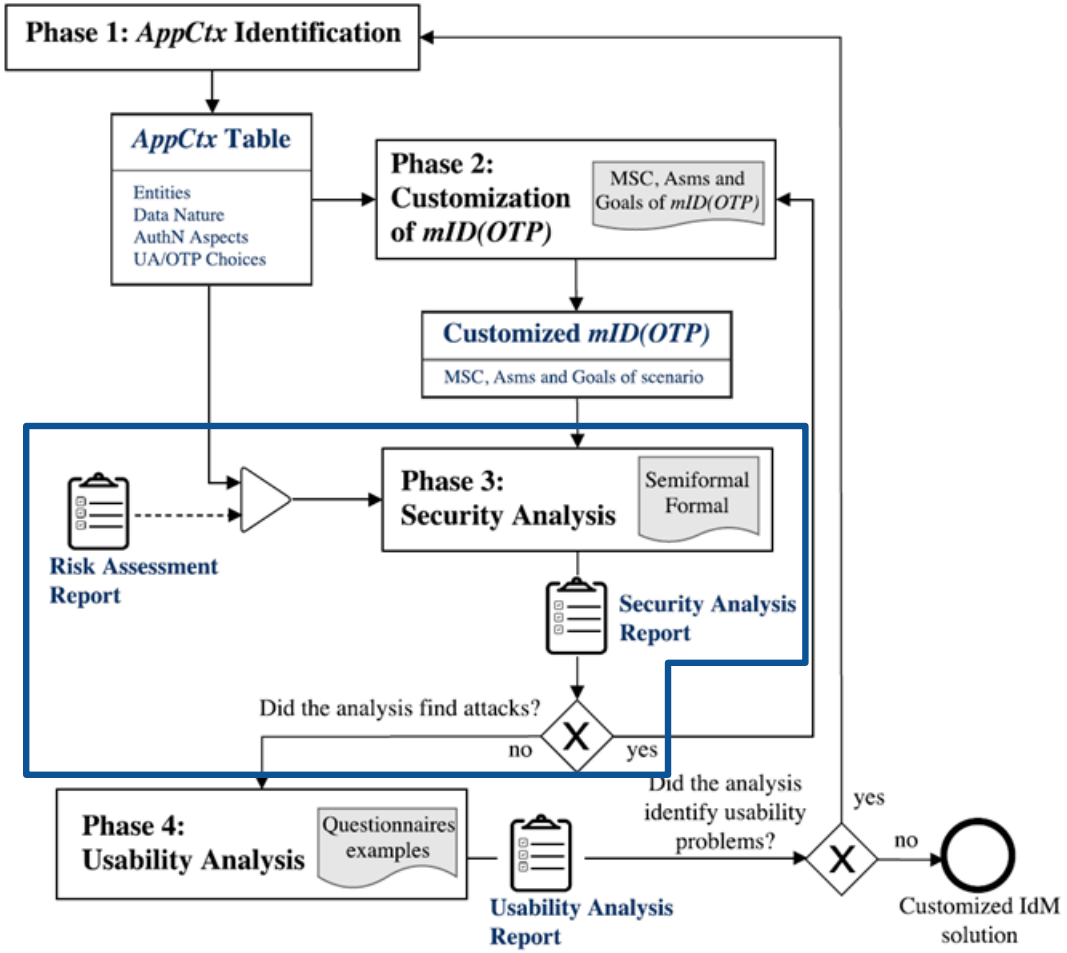
Methodology Overview

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



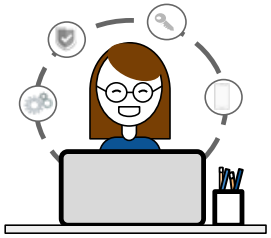
IdM Designer

External Consultant

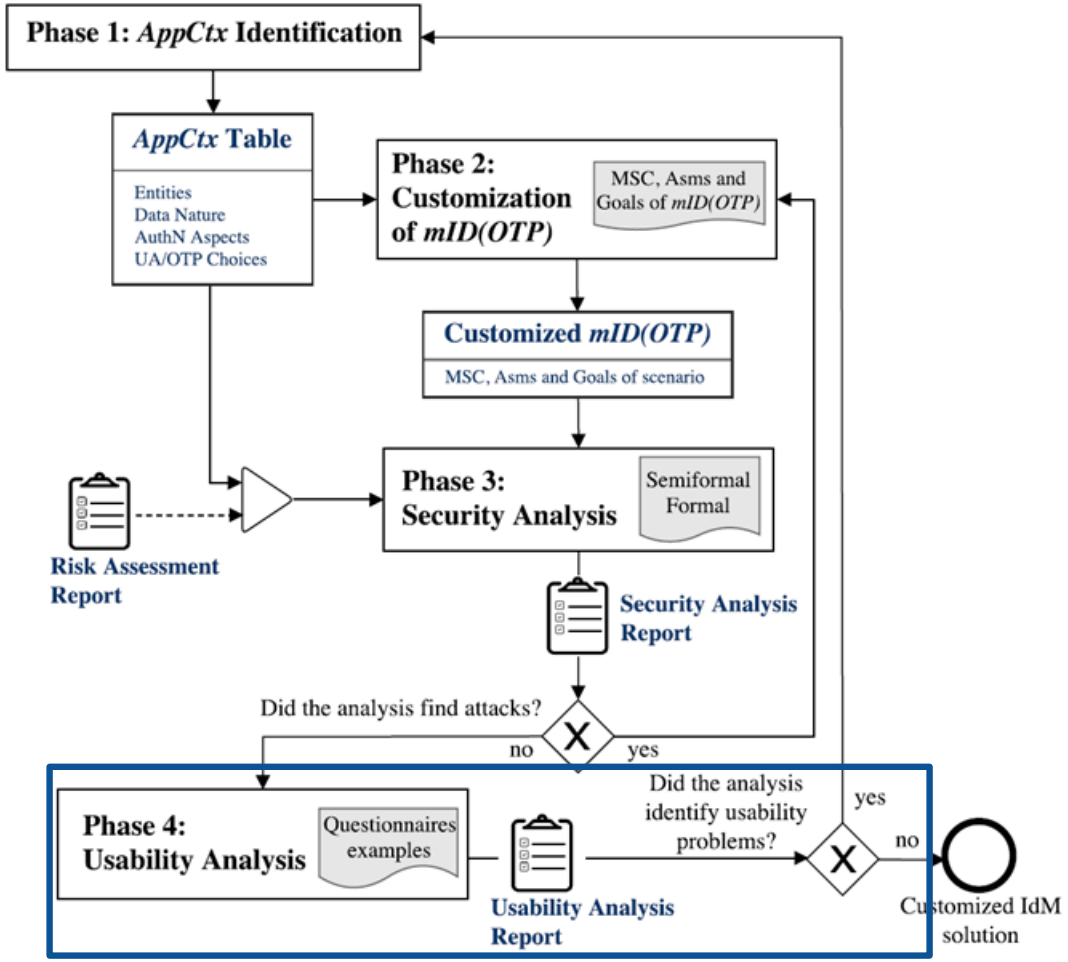


Methodology Overview

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

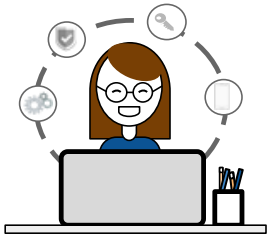


IdM Designer

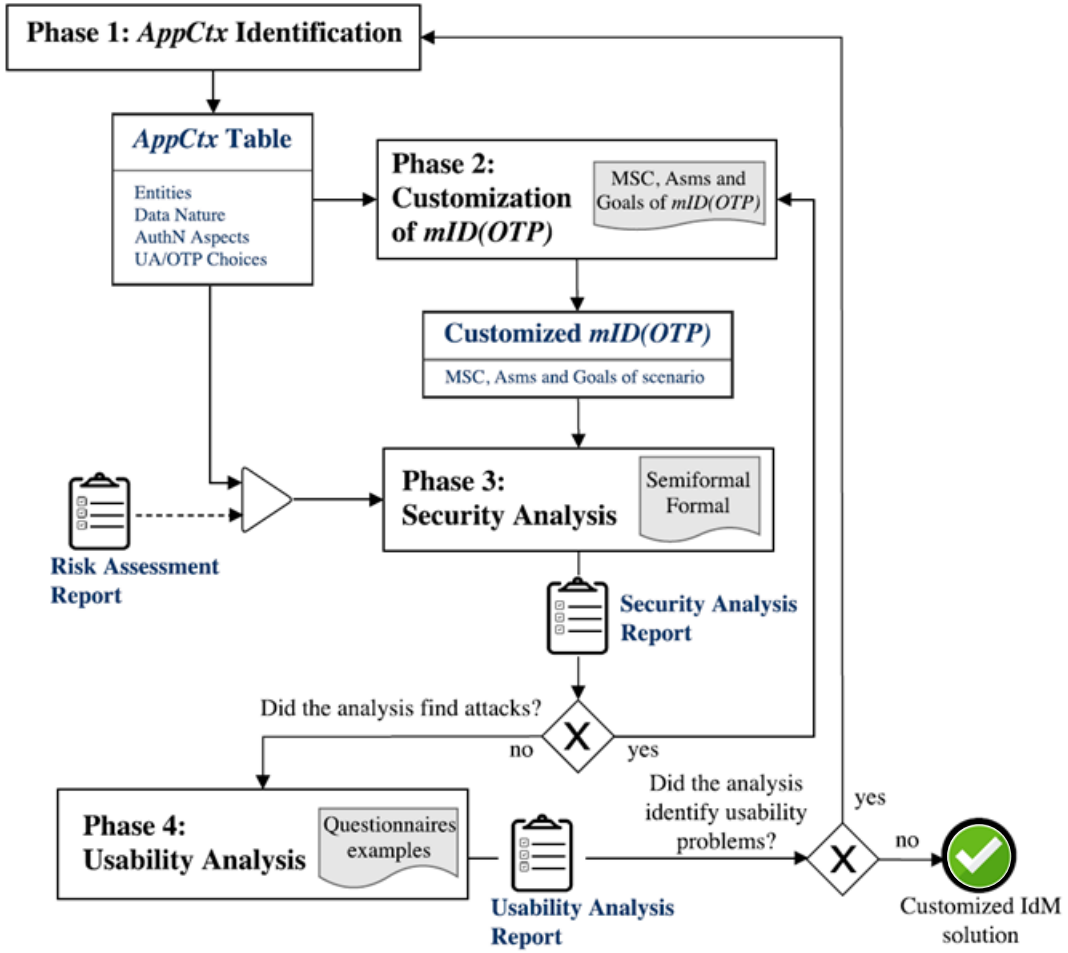


Methodology Overview

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

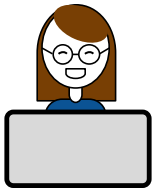


IdM Designer



Phase 1: Fill AppCtx Table

An Application Context (AppCtx) is derived by an informal description and analysis of the solution, and takes into account legal aspects

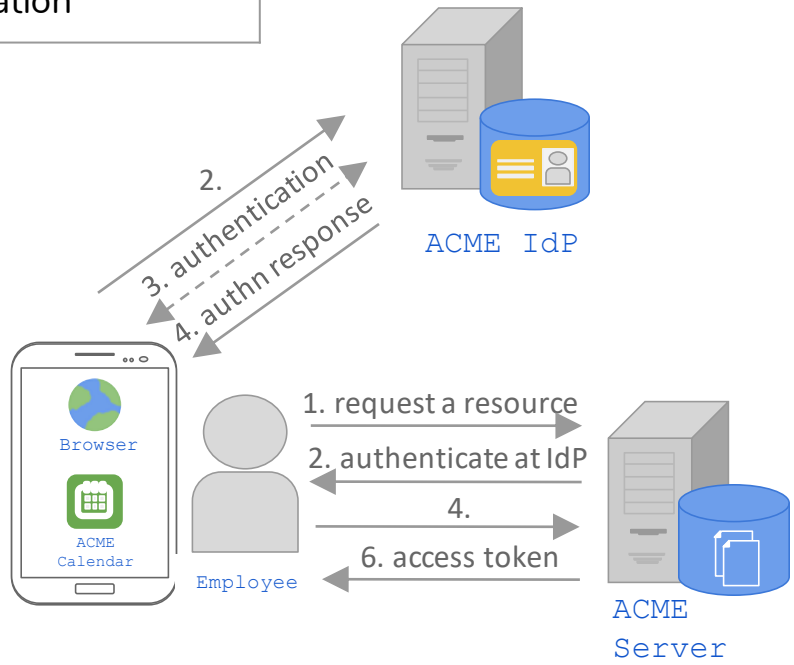


IdM Designer

is required to specify:

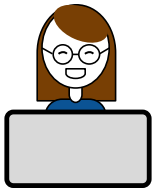
Entities	SP_{app} → `ACME Calendar`; User → `Employee`; …
UA choice	☑ Browser ☐ Application

IdM Roles	Scenario Entities
User	`Employee`
SP_{app} (Service Provider client)	`ACME Calendar`
SP_S (Service Provider server)	`ACME Server`
IdP_S (Identity Provider server)	`ACME IdP`
TP (Token Provider)	-
…	



Phase 1: Fill AppCtx Table

An Application Context (AppCtx) is derived by an informal description and analysis of the solution, and takes into account legal aspects



IdM Designer

is required to specify:

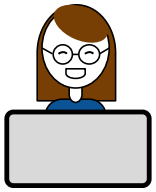
Entities	SP_{app} → `ACME Calendar`; User→ `Employee`; …
UA choice	☑ Browser ☐ Application
Data Nature	☐ anonymous ☑ personal ☐ sensitive

- **Anonymous data** are "any data that cannot be associated to any identified or identifiable data subject" [1, §4, lett. n];
- **Personal data** are "any information relating to an identified or identifiable natural person ('data subject');" [2, §2, lett. a];
- **Sensitive data** are "any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" [2, §8].

[1] Italian Personal Data Protection Code. Legislative Decree no. 196 of 30 June 2003.
[2] European Data Protection Directive 95/46 EC

Phase 1: Fill AppCtx Table

An Application Context (AppCtx) is derived by an informal description and analysis of the solution, and takes into account legal aspects



IdM Designer

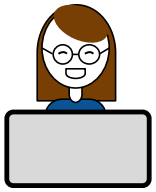
is required to specify:

Entities	SP_{app} → `ACME Calendar`; User→ `Employee`; …
UA choice	☑ Browser ☐ Application
Data Nature	☐ anonymous ☑ personal ☐ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☐ yes ☑ no

- Multi-Factor Authentication (MFA): augments the security of a single-factor authentication by combining two or more authentication elements (factors) of different categories (e.g., a password combined with some biometric data).
- Session handling: if a User has already a login session with an IdP, then she can access new SP apps without reentering her IdP credentials; only the user consent is required.

Phase 1: Fill AppCtx Table

An Application Context (AppCtx) is derived by an informal description and analysis of the solution, and takes into account legal aspects



IdM Designer

is required to specify:

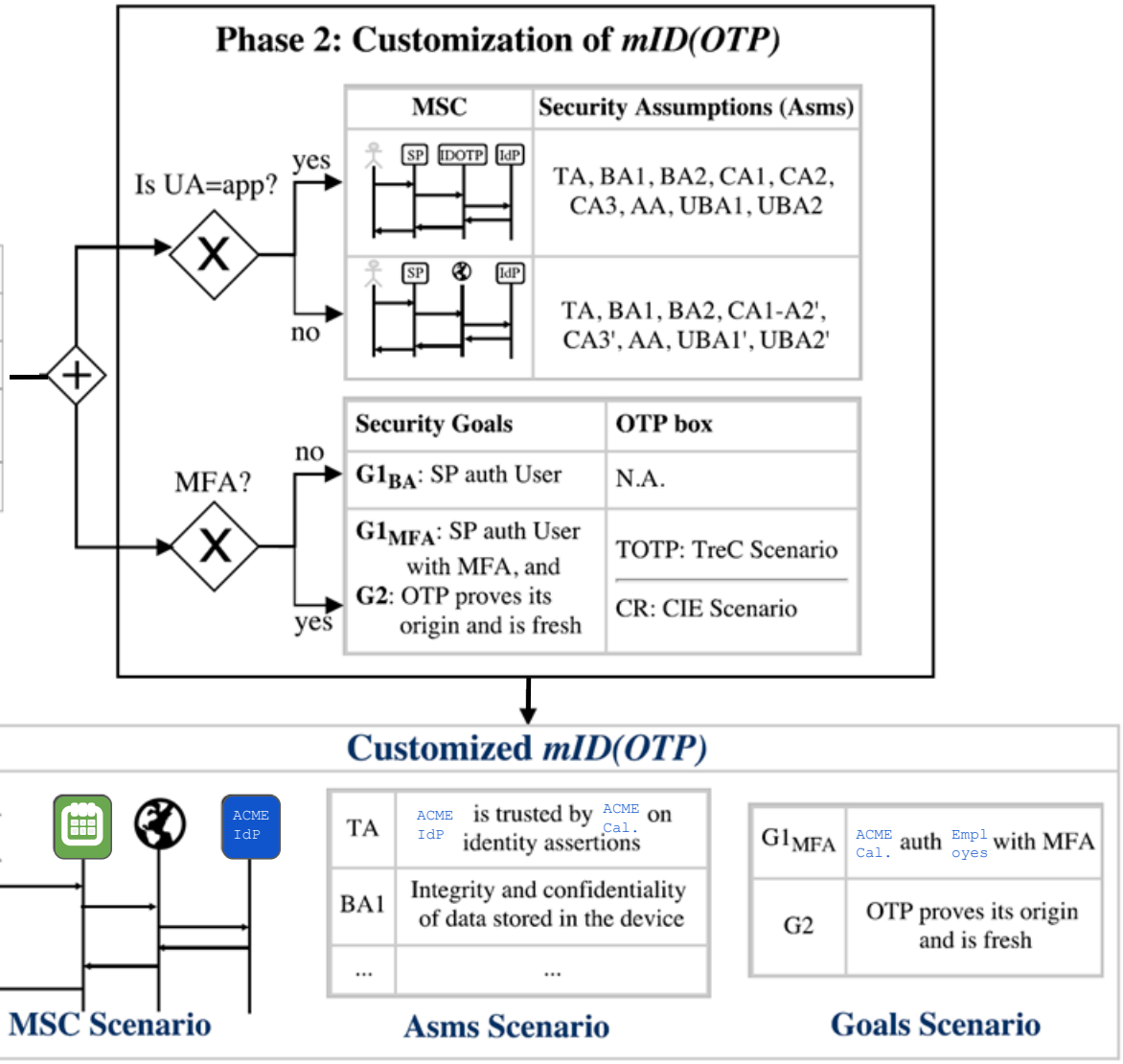
Entities	SP_{app} → `ACME Calendar`; User→ `Employee`; …
UA choice	☑ Browser ☐ Application
Data Nature	☐ anonymous ☑ personal ☐ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☐ yes ☑ no
OTP choice	☐ TOTP ☑ CR ☐ other

- Time synchronization (TOTP): the OTP is generated starting from a shared secret key and the current time of the operation. IdP must validate this value: only OTPs that fall into a short temporal range are accepted
- Challenge/Response (CR): in the execution of this approach, IdP presents a challenge (e.g, a random number) and User answers with a valid response, which is an OTP value calculated using a mathematical algorithm starting from the challenge

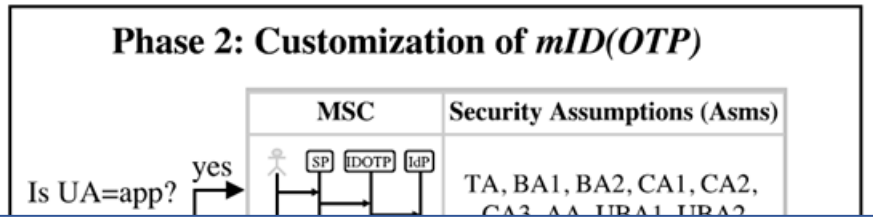
Phase 2: Customization

AppCtx Table

Entities	SP_{app} → ACME Calendar; User→ Employee; ...
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

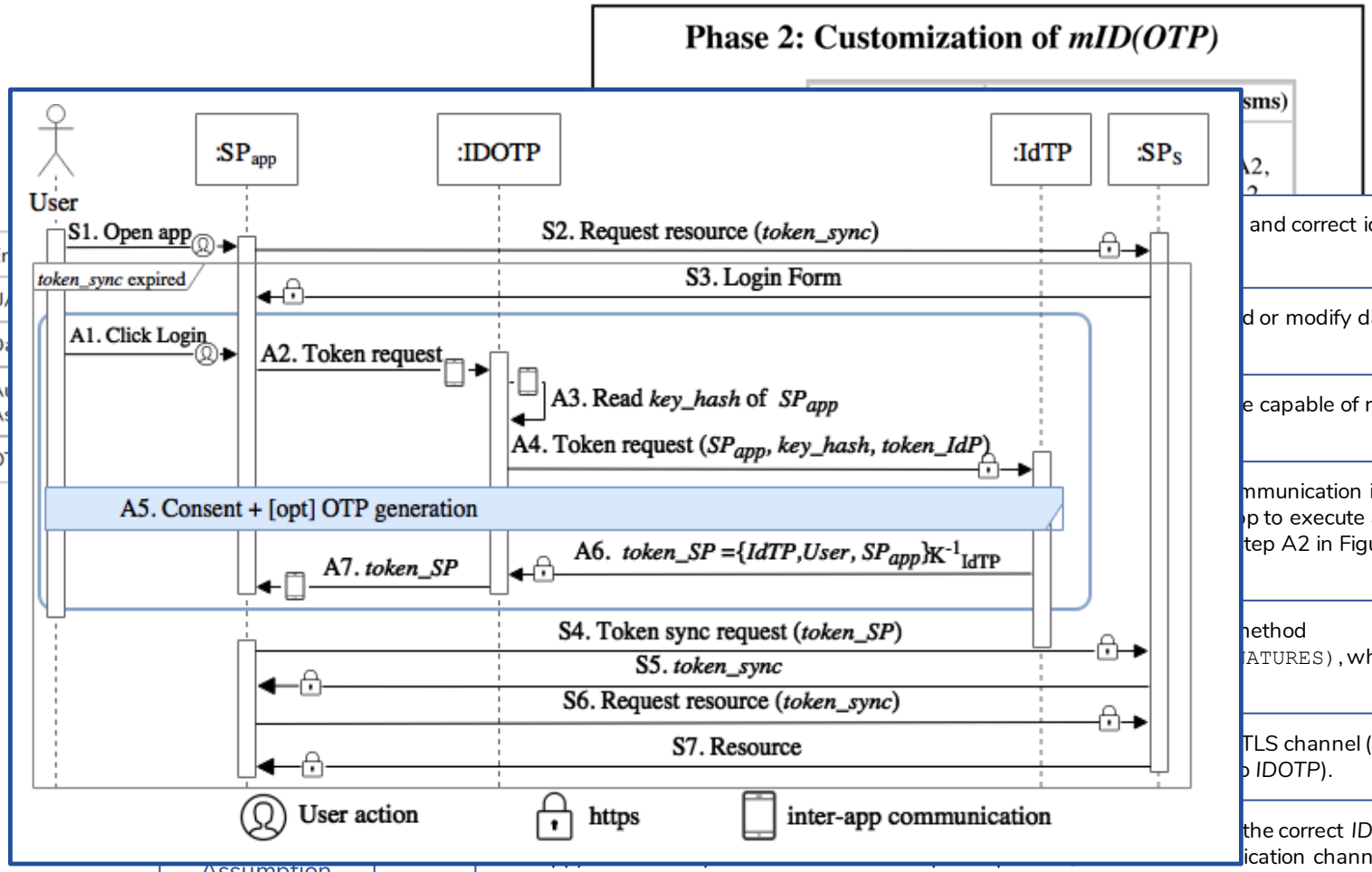


AppCtx Tabl

Entities	SP_{app}
UA choice	☑
Data Nature	☐ a
AuthN Aspects	MFA Ses
OTP choice	☐

Trust Assumption	**TA**	*IdTP* is trusted by SP_{app} on identity assertions. That is *IdTP* releases only valid and correct identity assertions.
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 *User* types.
Communication Assumptions	**CA1**	The communication between SP_{app} and *IDOTP* 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 SP_{app} that sends a request to *IDOTP* at Step A2 in Figure 6.1 is the same app that receives the result back from *IDOTP* at Step A10.
	CA2	To read the *key hash* value (Step A3 of Figure 6.1), *IDOTP* uses the Android method `getPackageInfo(client packageName, PackageManager.GET SIGNATURES)`, which extracts the information about the certificate fingerprint included in the package of SP_{app}.
	CA3	The communication between *IDOTP* and *IdTP* occurs over a unilateral SSL or TLS channel (henceforth SSL/TLS), established through the exchange of a valid certificate (from *IdTP* to *IDOTP*).
Activation Assumption	**AA**	The activation phase is correctly performed by *User*. That is, *User* downloads the correct *IDOTP* (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.
User Behaviour Assumptions	**UBA1**	User enters her credentials and (optionally) values for the OTP generation only in the correct *IDOTP* app being careful not to be seen by other people.
	UBA2	User is the only person using the *IDOTP* app that has been activated with her identity.

Phase 2: Customization

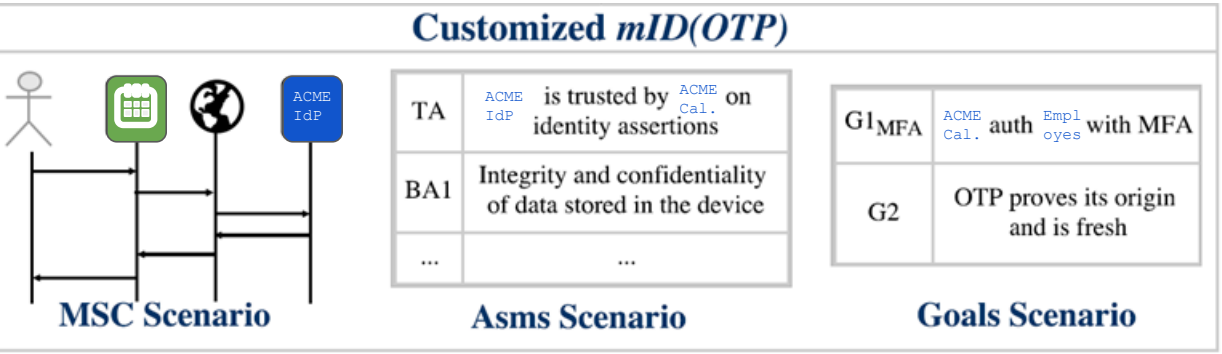


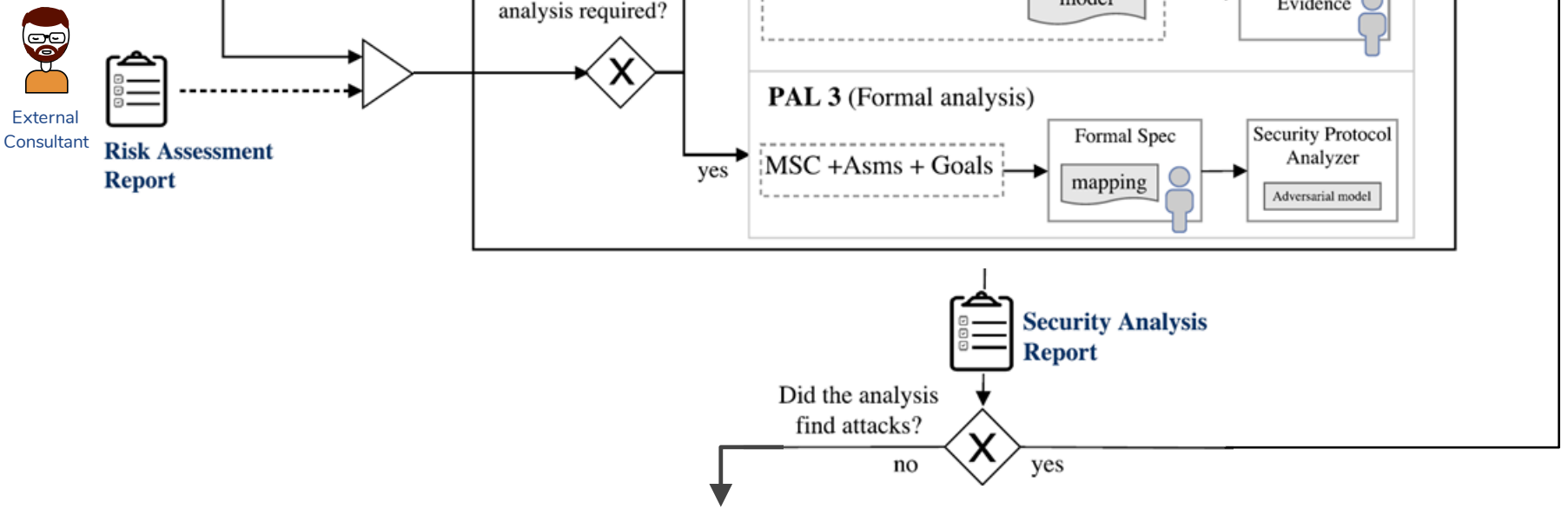
		and correct identity assertions.
		d or modify data stored by
		e capable of reading the values
		mmunication implemented using p to execute another app and tep A2 in Figure 6.1 is the same
		ethod ATURES), which extracts the
		TLS channel (henceforth o IDOTP).
Assumption		the correct IDOTP (i.e. it is not ication channels that are involved in this phase are secure.
User Behaviour Assumptions	UBA1	User enters her credentials and (optionally) values for the OTP generation only in the correct IDOTP app being careful not to be seen by other people.
	UBA2	User is the only person using the IDOTP app that has been activated with her identity.

Phase 3: Security Analysis

AppCtx Table

Entities	SP_{app} ⟶ ACME Calendar; User⟶ Employee; ...
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

AppCtx Table

Entities	SP_{app} ⇀ ACME Calendar; User ⇀ Employee; ...
UA choice	☑ Browser ☐ Application
Data Nature	☐ anonymous ☑ personal ☐ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☐ yes ☑ no
OTP choice	☐ TOTP ☑ CR ☐ other

External Consultant

Risk Assessment Report

Customized

Asm	Specification of Asm	Formal Specification	Removal of Asm
TA	We do not consider sessions with i playing the role of IdTP	add sessions with i playing the role of IdTP	
$CA1_{Var1}$	link(IdO2IdTP, IdTP2IdO);		delete link(IdO2IdTP, IdTP2IdO);
$CA2_{Var1}$	authentic_on(SP2IdO, SP_{app});		delete authentic_on(SP2IdO, SP_{app});

$CA3_{Var1}$	and DB Keyhash
	confidential_to(IdO2IdTP, IdTP);
	weakly_authentic(IdO2IdTP);
	weakly_confidential(IdTP2IdO);
	authentic_on(IdTP2IdO, IdTP);
	link(IdO2IdTP, IdTP2IdO);
			delete confidential_to(IdO2IdTP, IdTP);
			weakly_authentic(IdO2IdTP);
			weakly_confidential(IdTP2IdO);
			authentic_on(IdTP2IdO, IdTP);
			link(IdO2IdTP, IdTP2IdO);

$CA1_{Var2}$	confidential_to(B2SP, SP_{app});		delete confidential_to(B2SP, SP_{app});

$CA2_{Var2}$	confidential_to(B2IdTP, IdTP);
	weakly_authentic(B2IdTP);
	weakly_confidential(IdTP2B);
	authentic_on(IdTP2B, IdTP);
			delete confidential_to(B2IdTP, IdTP);
			weakly_authentic(B2IdTP);
			weakly_confidential(IdTP2B);
			authentic_on(IdTP2B, IdTP);

$CA3_{Var2}$	link(B2IdTP, IdTP2B); confidential_to(O2B, Browser);		link(B2IdTP, IdTP2B); delete confidential_to(O2B, Browser);
AA	Data obtained during the activation phase are nonpublic values		add all the iknows(IFactor) obtained during the activation phase
BA1	"Built-in": i cannot read the internal state of the other entities	add all the iknows($IFactor_p$)	
BA2	"Built-in": i cannot read the internal state of the other entities	add all the iknows($IFactor_k$)	
$UBA1_{Var1}$	confidential_to(U2IdO, IDOTP);		delete confidential_to(U2IdO, IDOTP);
$UBA2_{Var1}$	authentic_on(U2IdO, User);		delete authentic_on(U2IdO, User);
$UBA1_{Var2}$	confidential_to(U2B, Browser);		delete confidential_to(U2B, Browser);
	confidential_to(U2O, OTPApp);		delete confidential_to(U2O, OTPApp);
$UBA2_{Var2}$	authentic_on(U2B, User);		delete authentic_on(U2B, User);
	authentic_on(U2O, User);		delete authentic_on(U2O, User);

MFA | ACME Cal. auth | Empl oyes with MFA

2 | OTP proves its origin and is fresh

Goals Scenario

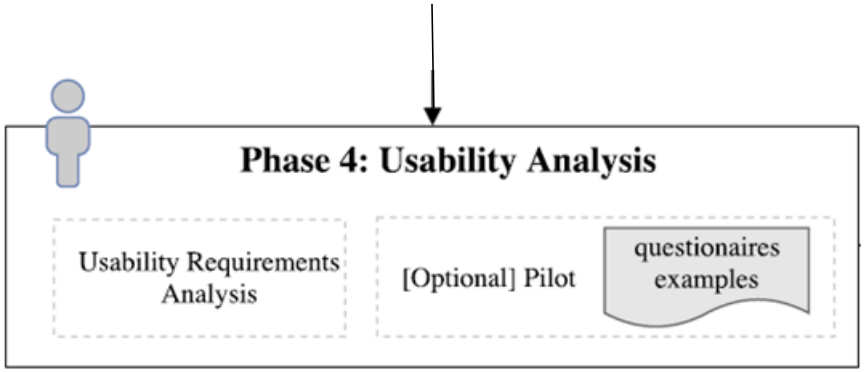
Self-assessment Evidence

curity Protocol Analyzer

versarial model

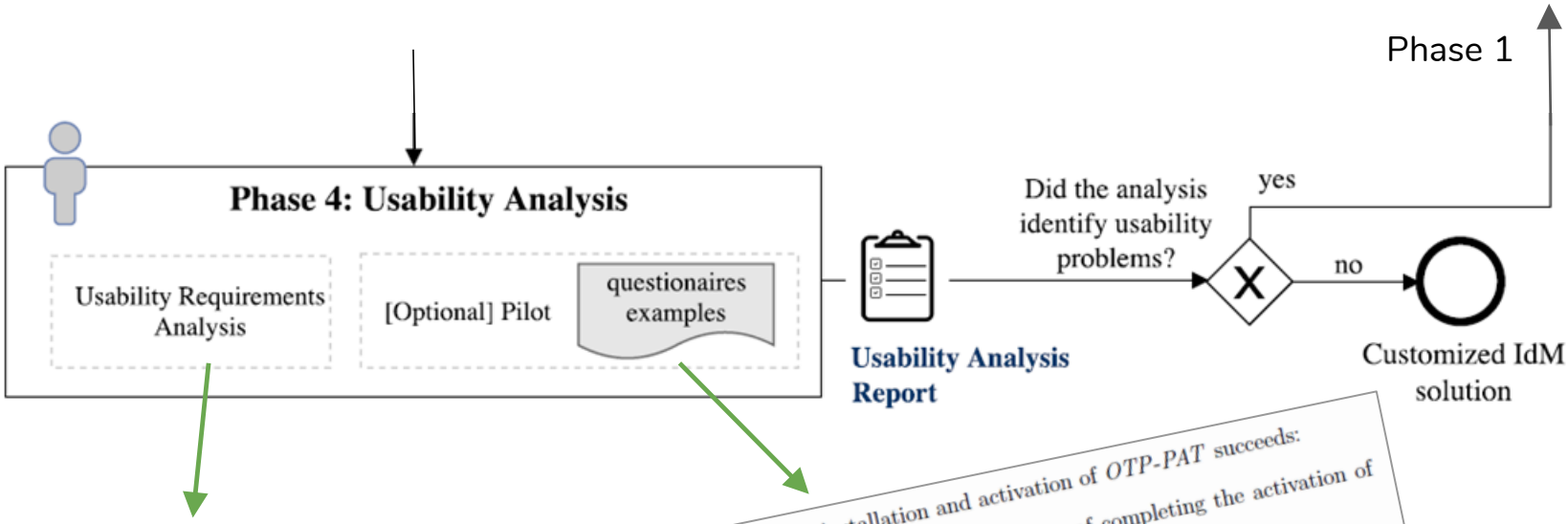
no X yes

Phase 4: Usability Analysis



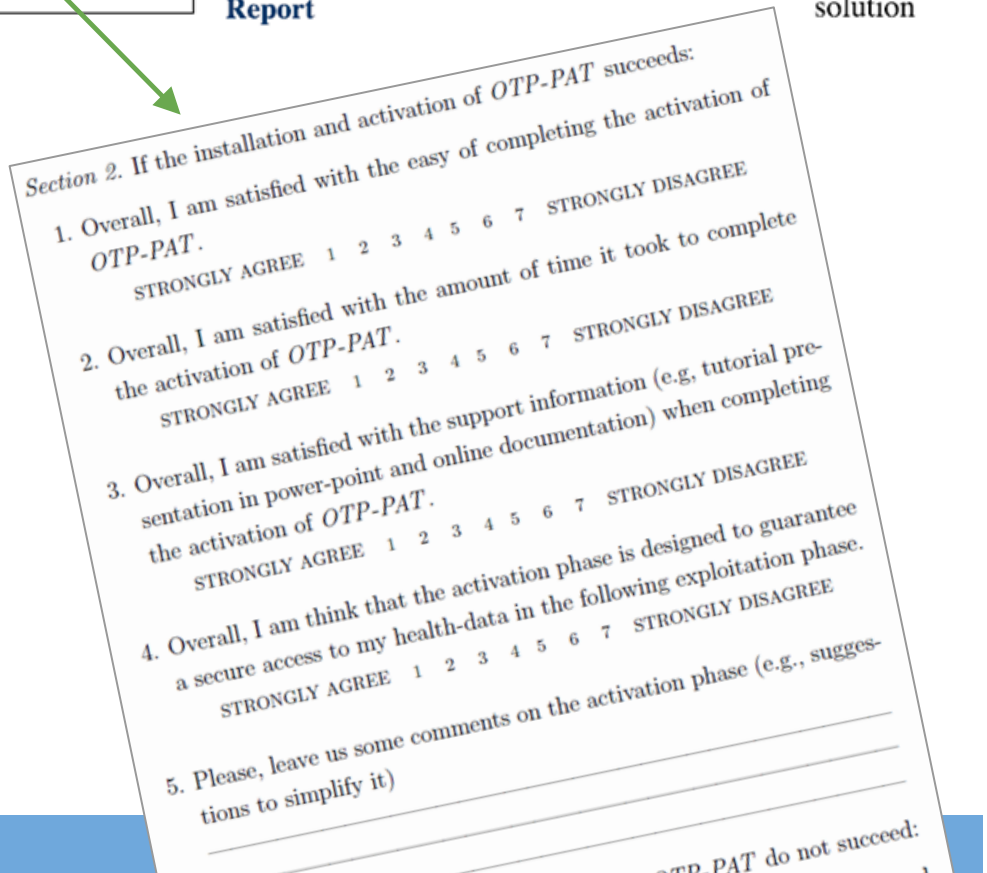
IdM designers have to balance security and usability

Phase 4: Usability Analysis



- No username & password, only PIN/fingerprint
- OTP transparent to user
- No moving from an app to another

....



Section 2. If the installation and activation of *OTP-PAT* succeeds:

1. Overall, I am satisfied with the easy of completing the activation of *OTP-PAT*.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
2. Overall, I am satisfied with the amount of time it took to complete the activation of *OTP-PAT*.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
3. Overall, I am satisfied with the support information (e.g, tutorial presentation in power-point and online documentation) when completing the activation of *OTP-PAT*.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
4. Overall, I am think that the activation phase is designed to guarantee a secure access to my health-data in the following exploitation phase.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
5. Please, leave us some comments on the activation phase (e.g., suggestions to simplify it)

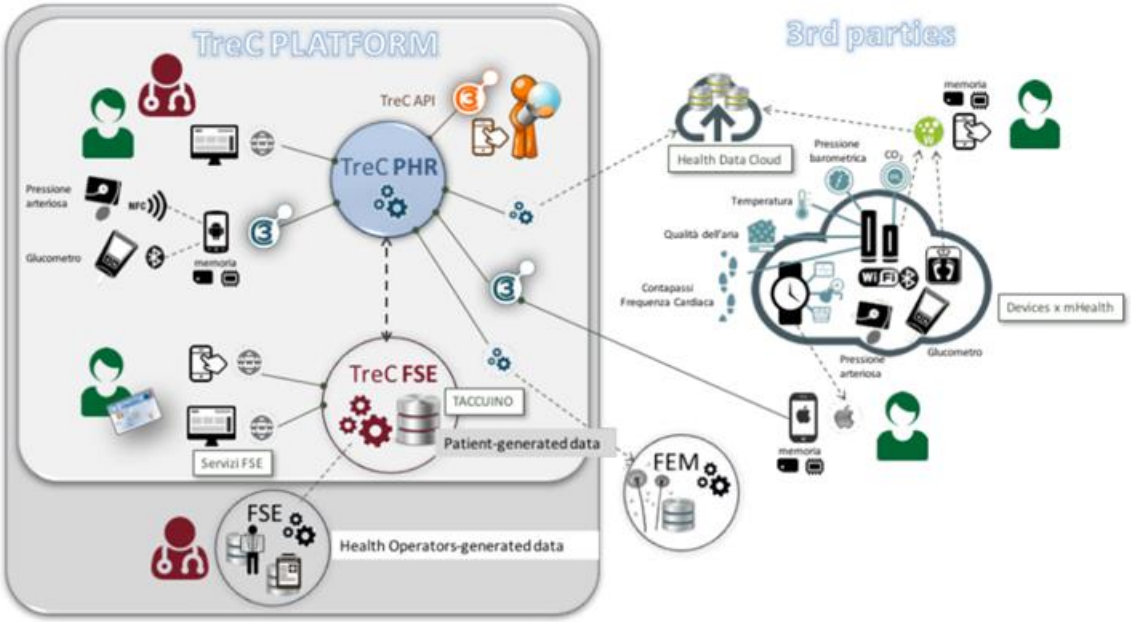
Outline

- IdM Mobile Context
- Problem Statement and Methodology Overview
- TreC Scenario
- IPZS/CIE Scenario
- Conclusions

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

Self-management

Remote monitoring

TreC: Web and Mobile apps

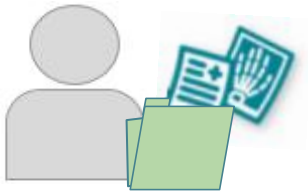
Carta Provinciale dei Servizi

TreC Apps

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

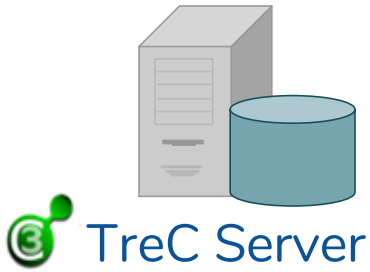
Phase 1: Fill AppCtx Table

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



Patient

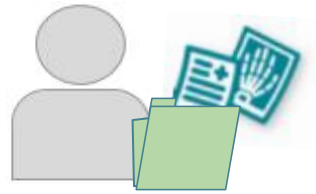
ADC



TreC Server

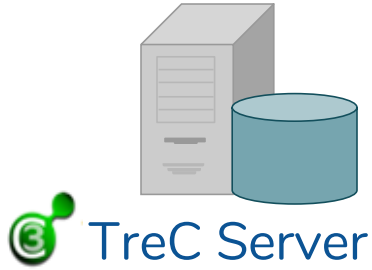
Phase 1: Fill AppCtx Table

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



Patient

ADC



TreC Server

European Data Protection Directive 95/46 EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. http://eur-lex.europa.eu/legal-188content/EN/TXT/?uri=CELEX:31995L0046.

Phase 1: Output

AppCtx Table - TreC

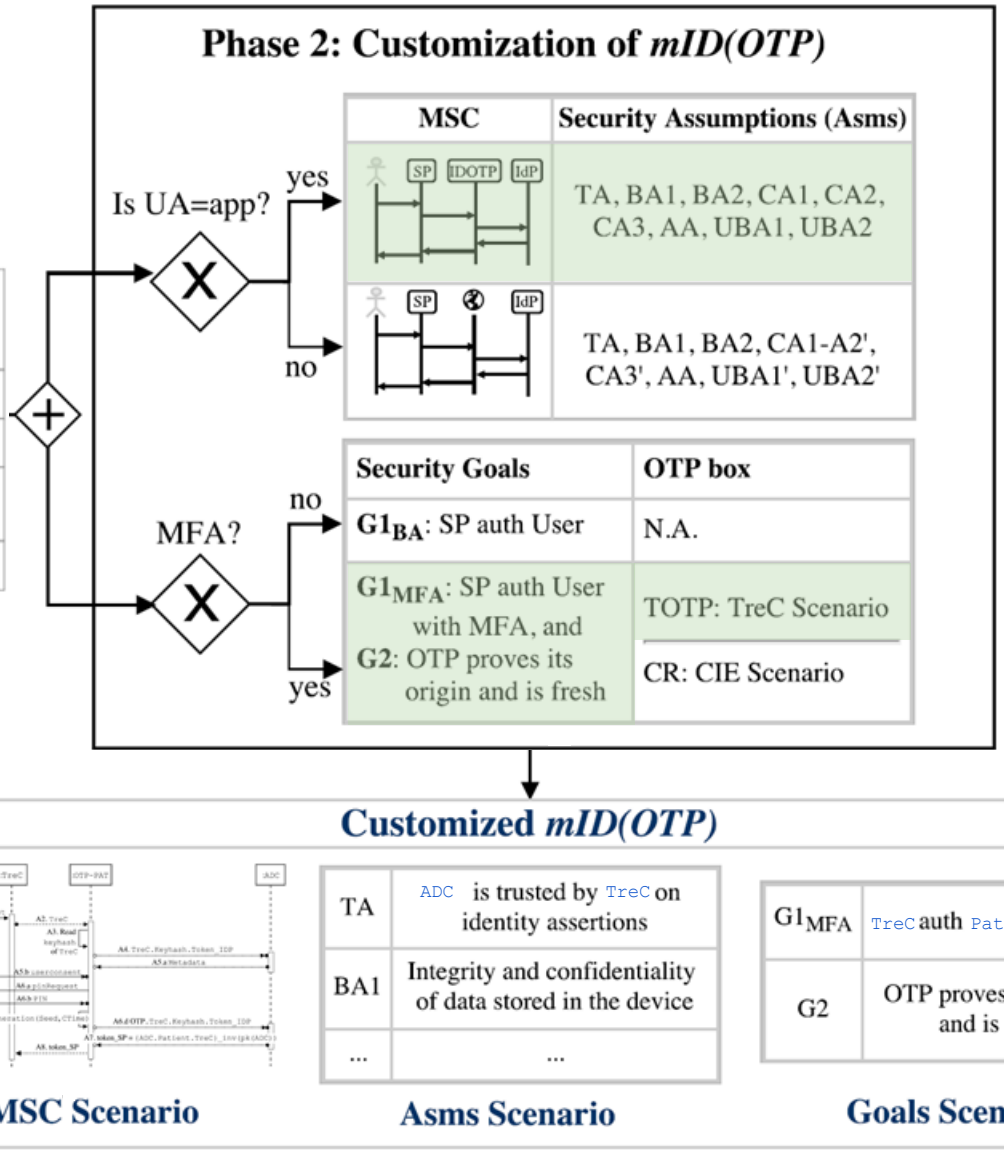
Entities	User →`Patient`; SP_{app}→`TreC Referti`; SP_S→`TreC`; UA,TP_{app}→`OTP-PAT`; IdP_S,TP_S→`ADC`;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other

Phase 2 →

Phase 2: Customization

AppCtx Table - TreC

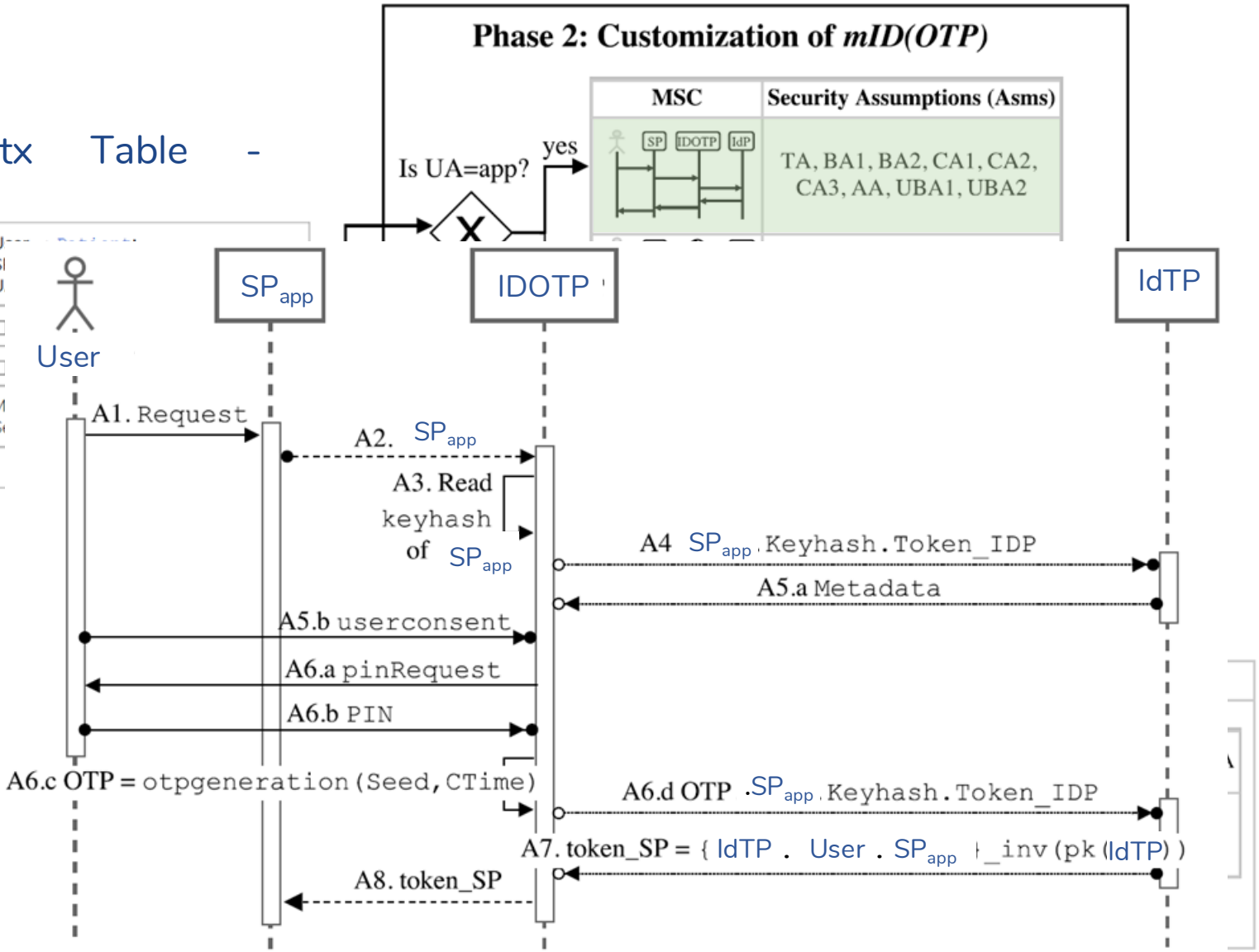
Entities	User → Patient; SP_{app} → TreC Referti; SP_S → TreC; UA,TP_{app} → OTP-PAT; IdP_S, TP_S → ADC;
UA choice	☐ Browser ☑ Application
Data Nature	☐ anonymous ☑ personal ☑ sensitive
AuthN Aspects	MFA support? ☑ yes ☐ no Session handling? ☑ yes ☐ no
OTP choice	☑ TOTP ☐ CR ☐ other



Phase 2: Customization

AppCtx Table - TreC

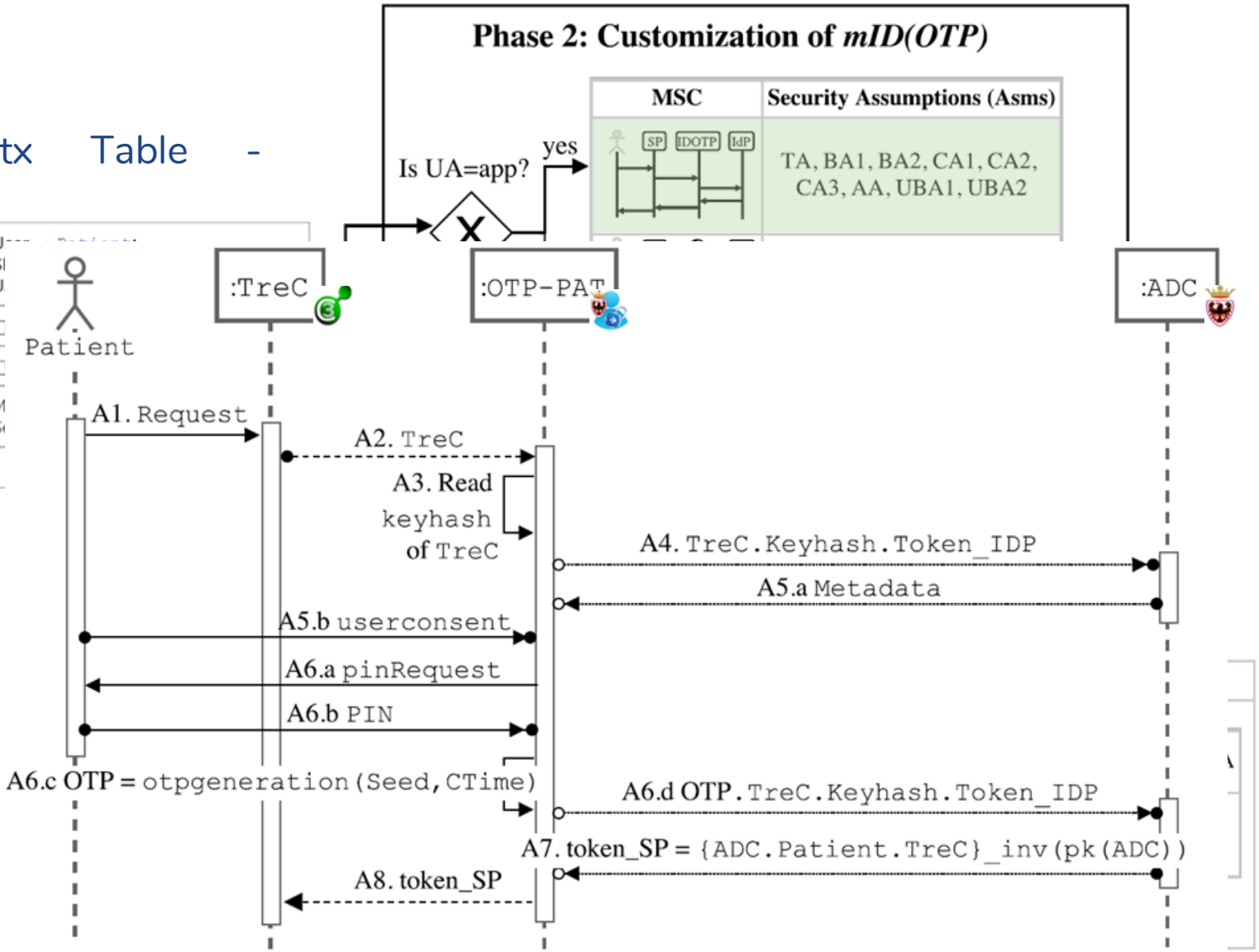
Entities	U… S… U…
UA choice	☐
Data Nature	☐
AuthN Aspects	M… S…
OTP choice	



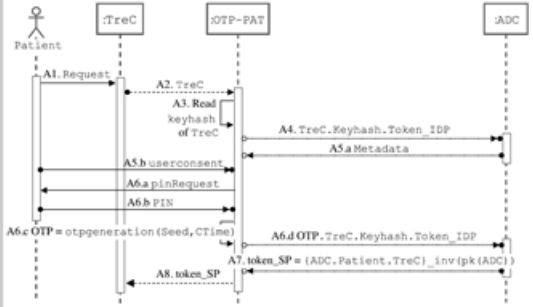
Phase 2: Customization

AppCtx Table - TreC

Entities	U… S… U…
UA choice	☐
Data Nature	☐
AuthN Aspects	M… S…
OTP choice	



Phase 2: MSC



MSC Scenario

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

Asms Scenario

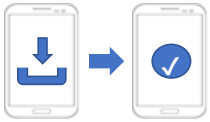
$G1_{MFA}$	TreC auth Pat. with MFA
G2	OTP proves its origin and is fresh

Goals Scenario

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*.

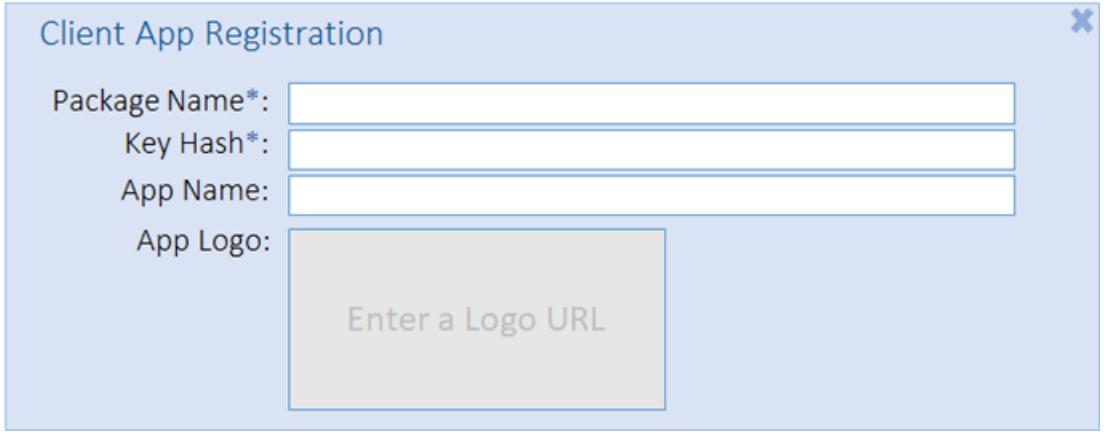
Exploitation: is performed every time Patient accesses TreC

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.

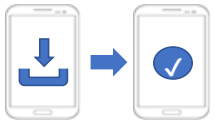
TreC devs



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

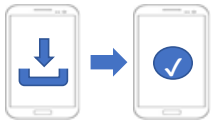
GOAL: enable OTP-PAT to securely interact with ADC.



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

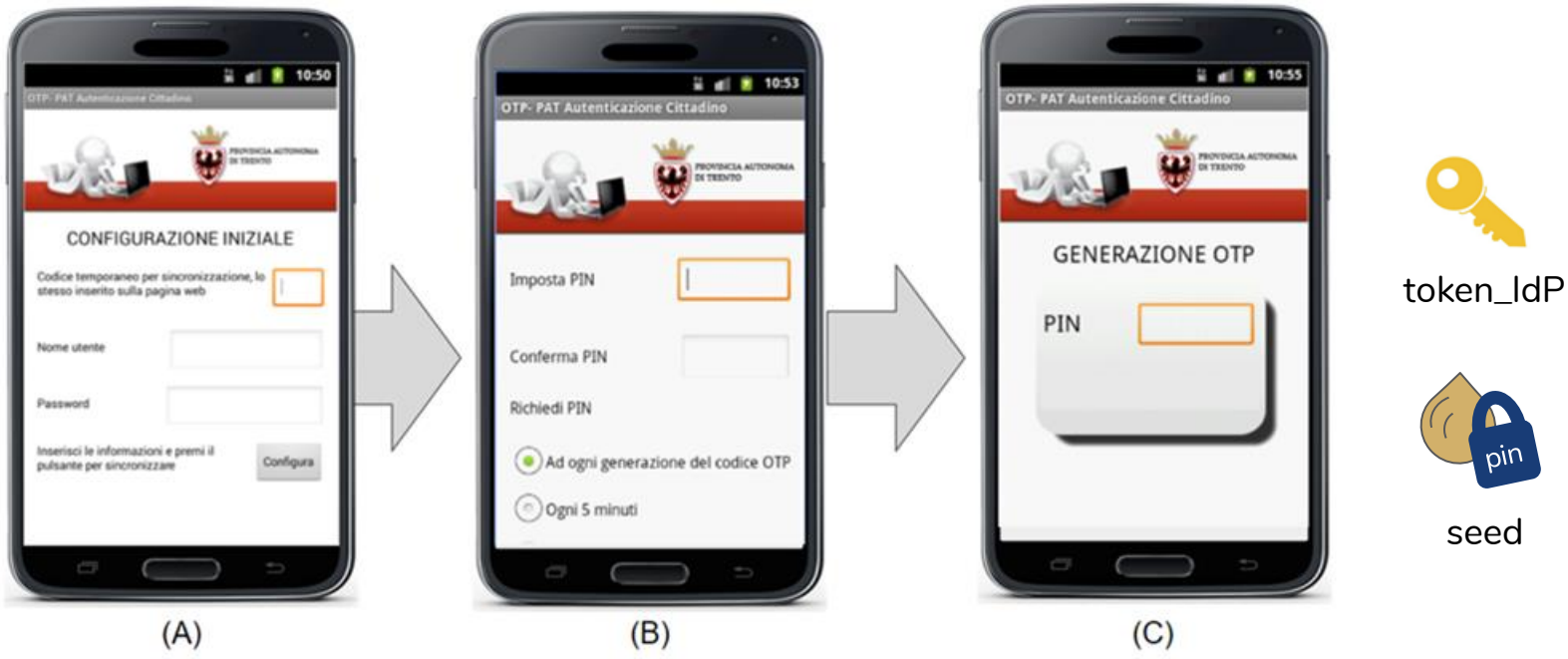
Activation of OTP-PAT

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



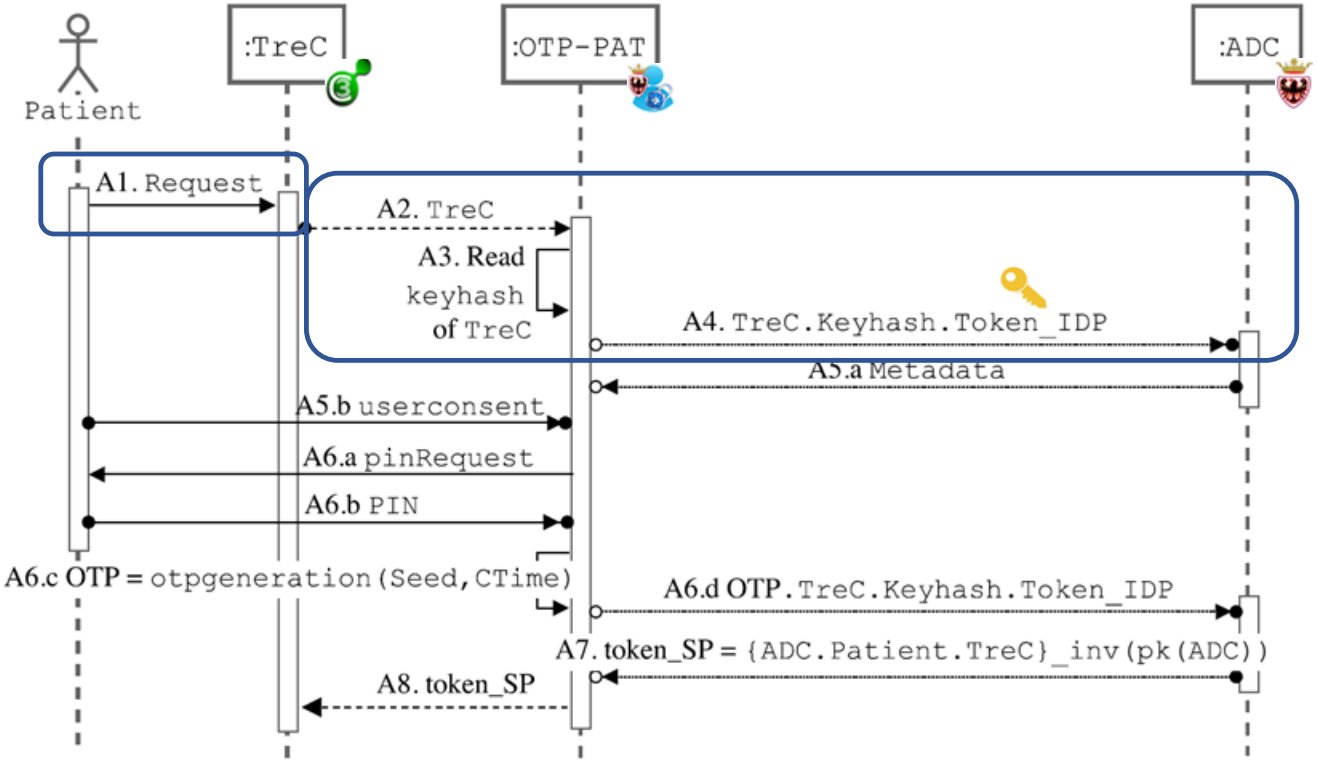
1 Laptop Using a portal made available by ADC, User logs in with CPS and obtains an *activation_code*.

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



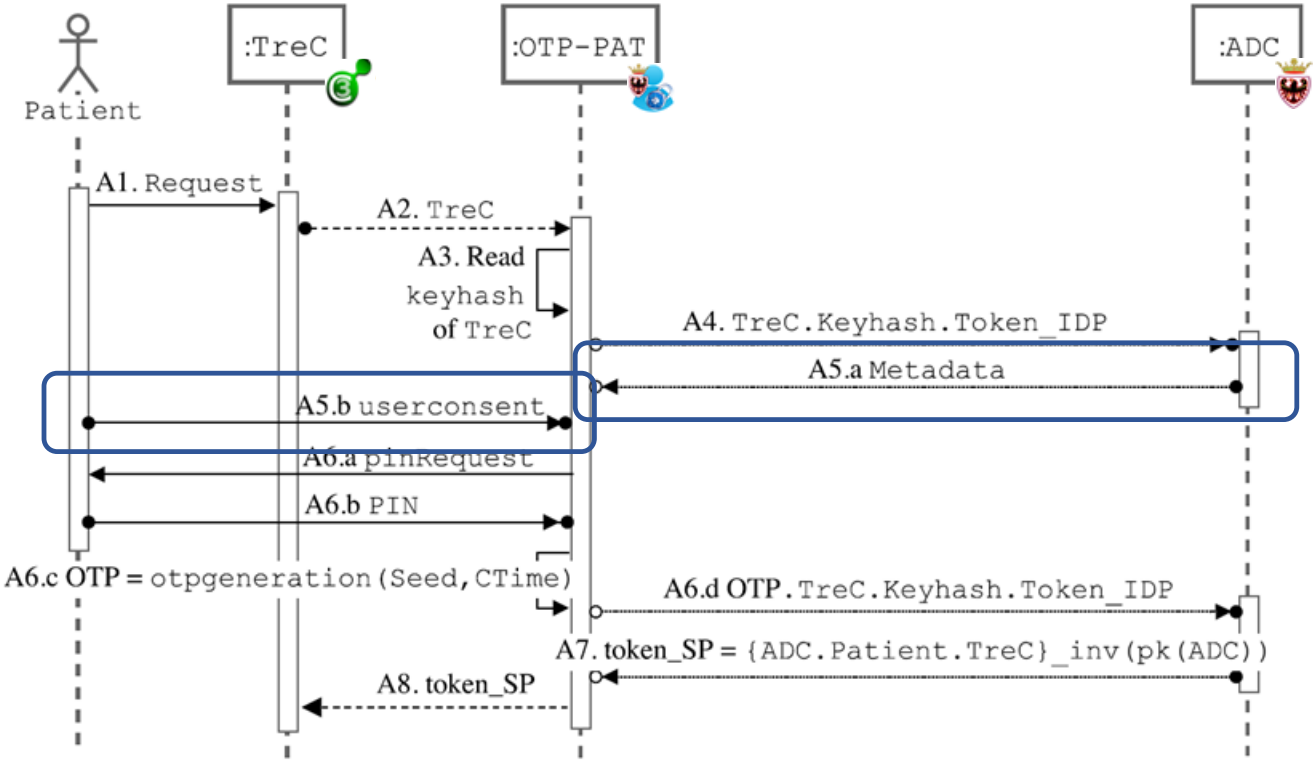
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



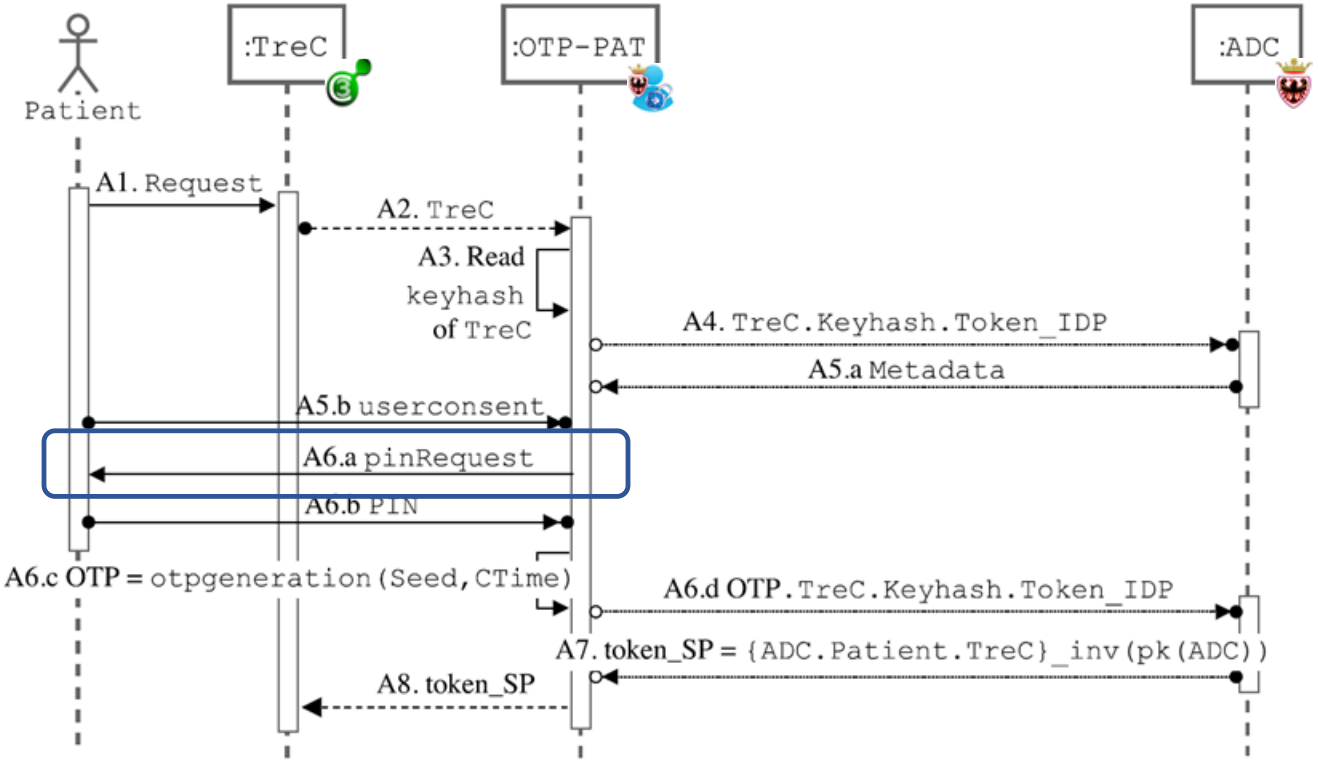
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



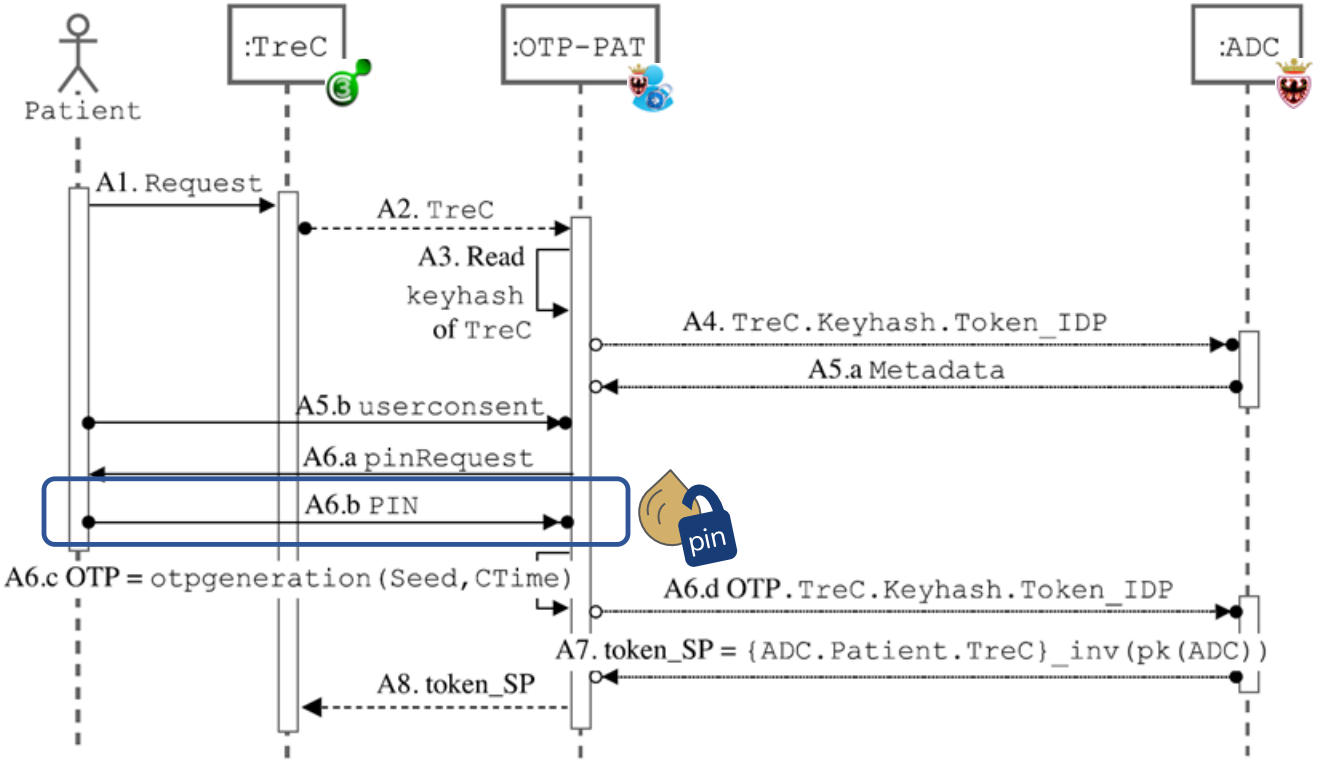
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



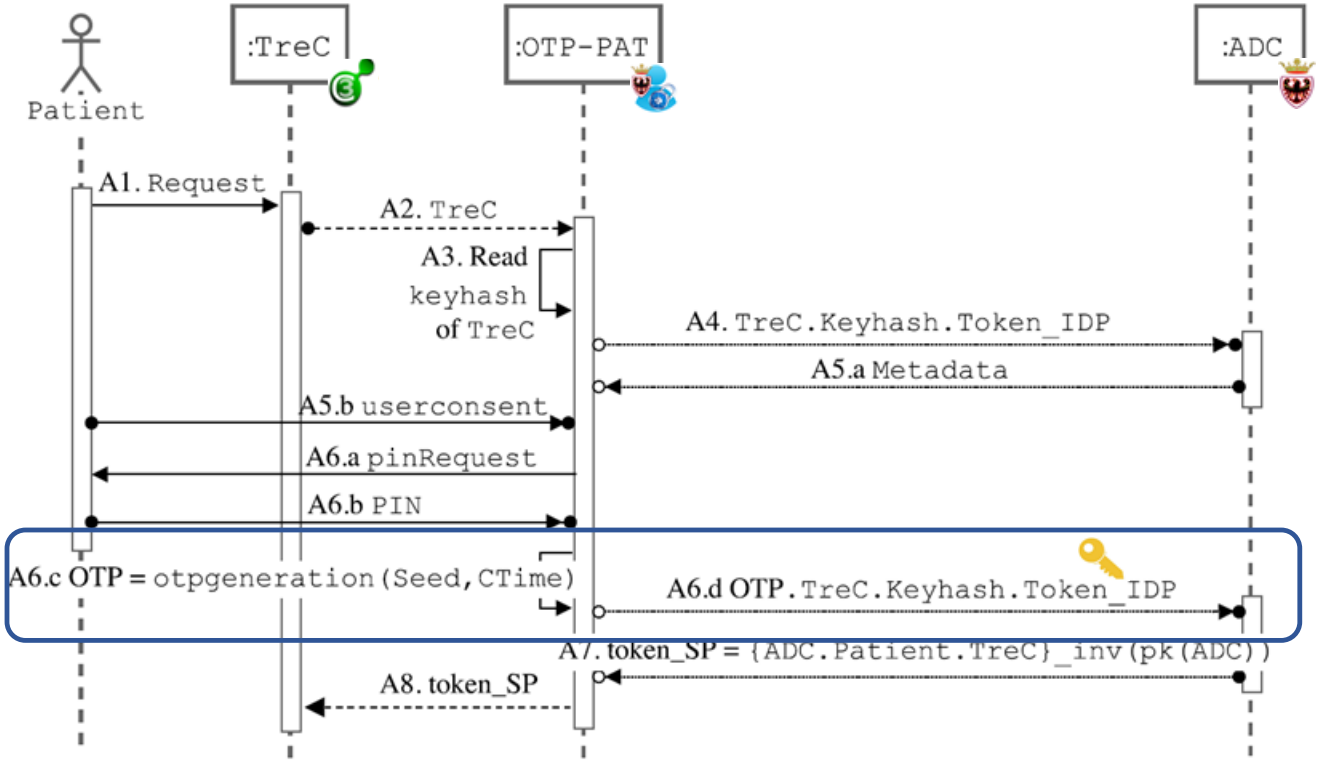
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



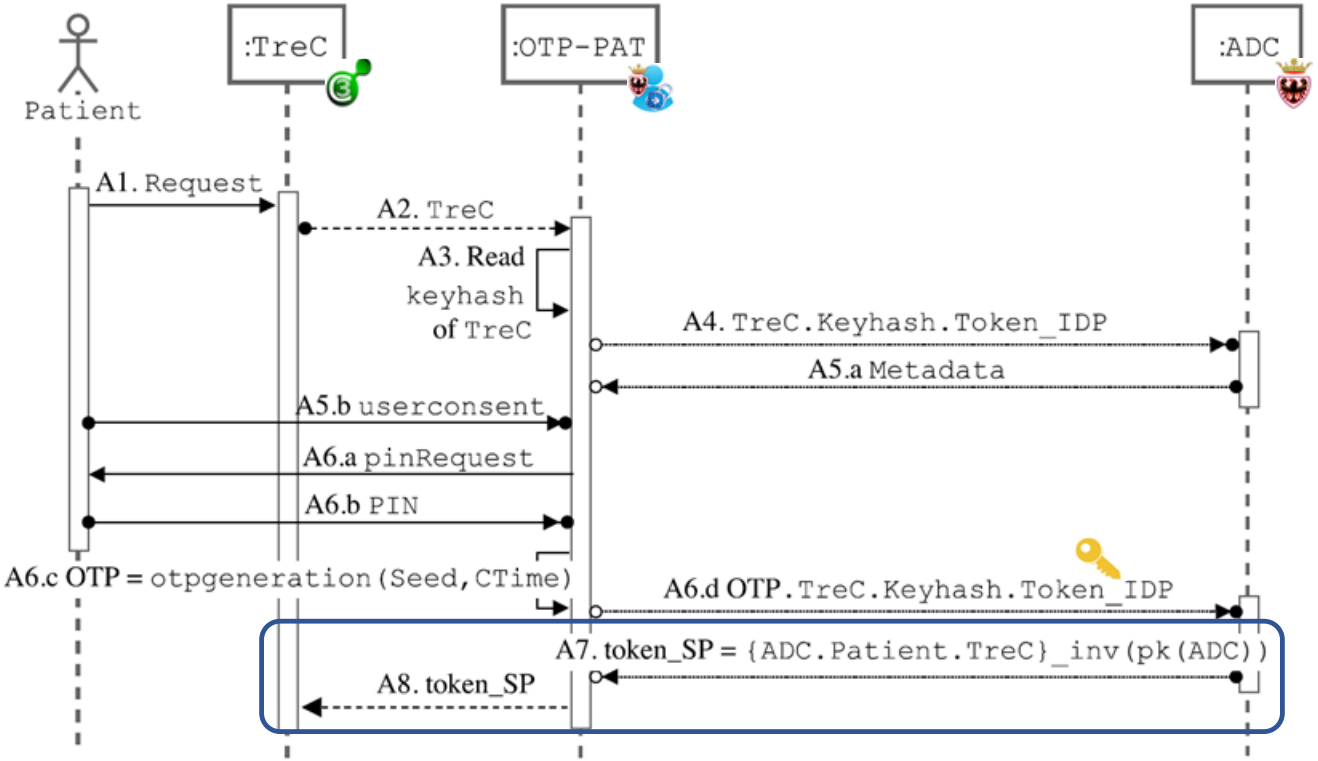
MSC Exploitation

GOAL: user logs in TreC app using the ADC identity

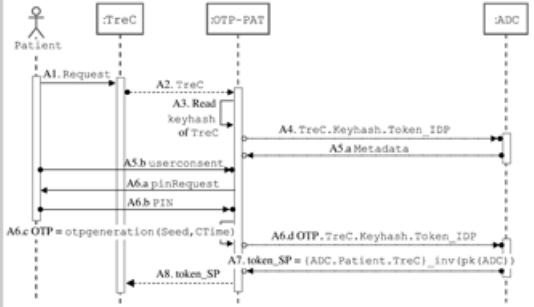


MSC Exploitation

GOAL: user logs in TreC app using the ADC identity



Phase 2: Assumptions



MSC Scenario

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

Asms Scenario

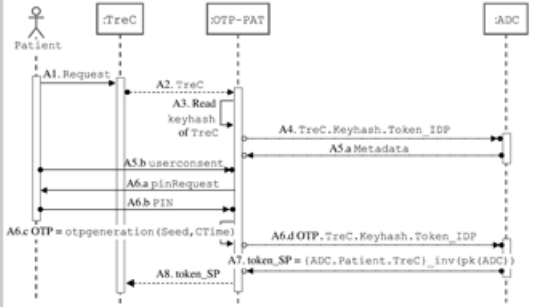
$G1_{MFA}$	TreC auth Pat. with MFA
G2	OTP proves its origin and is fresh

Goals Scenario

Phase 2: Assumptions

Trust Assumption	**TA**	**ADC** is trusted by **TreC** on identity assertions.
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.
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.
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.

Phase 2: Goals



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

Phase 2: Goals

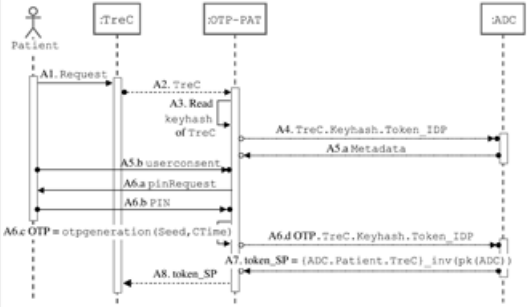
The TreC solution is a 3 instance-factors authentication solution:

1. `token_IdP` (*IFactor*$_o$) 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` (*IFactor*$_k$) known by Patient to unlock OTP-PAT;
3. `{seed}_PIN` (*IFactor*$_o$) that is stored in OTP-PAT.

Goal on Multi-Factor Authentication	**G1**$_{MFA}$	**TreC** authenticates **Patient** even if an intruder knows up to 2 instance-factors.
Goal on the OTP value	**G2**	…

Phase 2: Output

Customized mID(OTP) - TreC



MSC Scenario

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

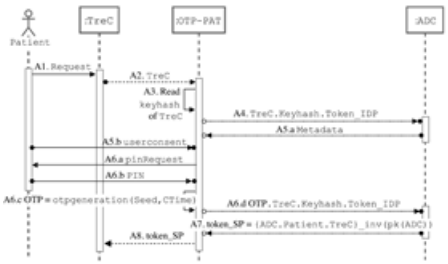
Asms Scenario

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

Goals Scenario

Phase 3 →

Phase 3: Security Analysis



MSC Scenario

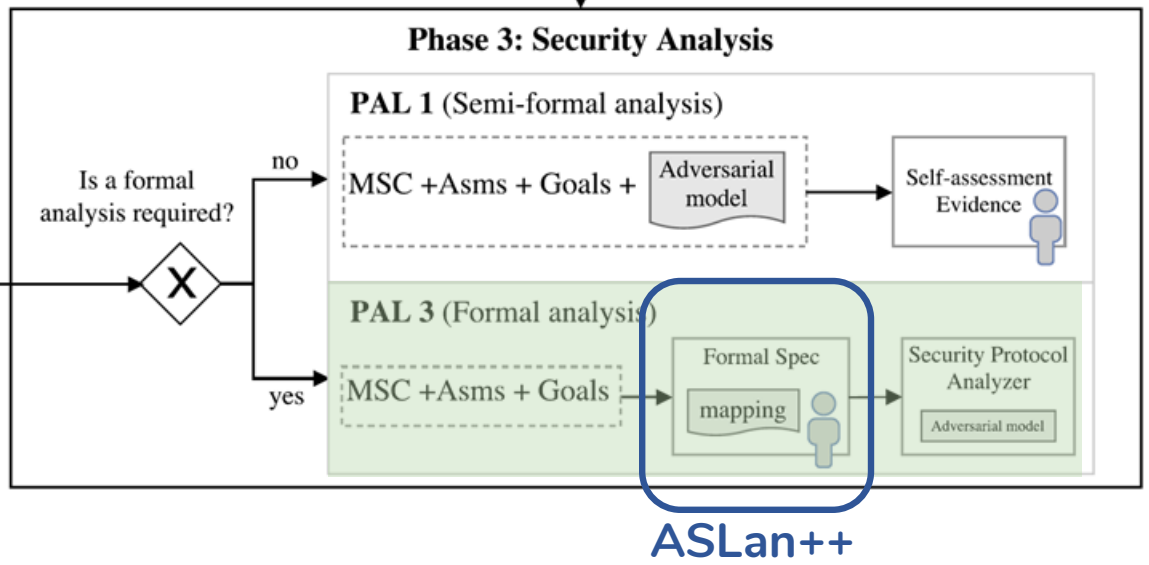
TA	ADC is trusted by TreC on identity assertions
BA1	Integrity and confidentiality of data stored in the device
...	...

Asms Scenario

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

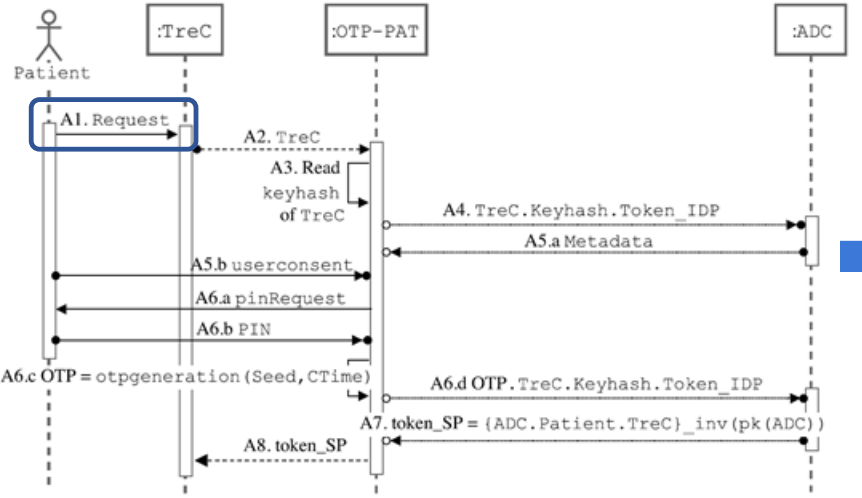
Goals Scenario

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



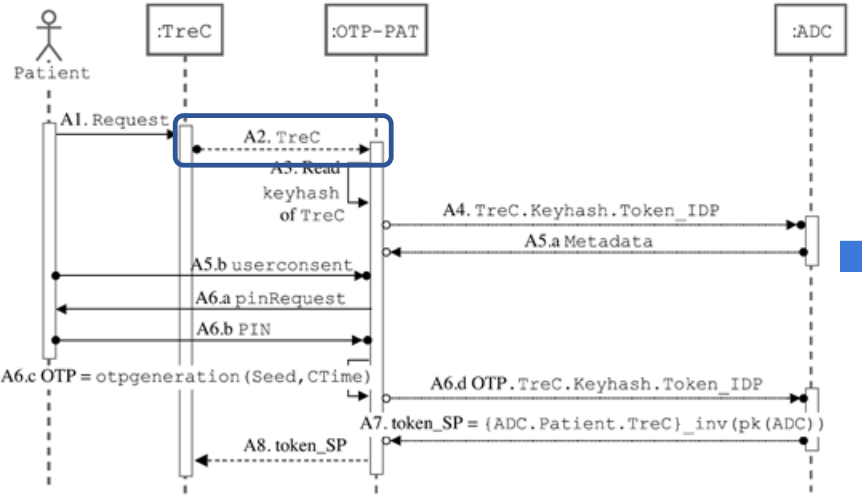
AVANTSSAR Project. Deliverable D2.3 (update) ASLan++ specification and tutorial. http://www.avantssar.eu/pdf/deliverables/avantssar-d2-3_update.pdf, 2008.

MSC Formal Mapping




```
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);
```

MSC Formal Mapping




```
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);
```

Asms 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);`

Asms 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);`

Hacker
Intruder

Asms 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

Goals Formal Mapping

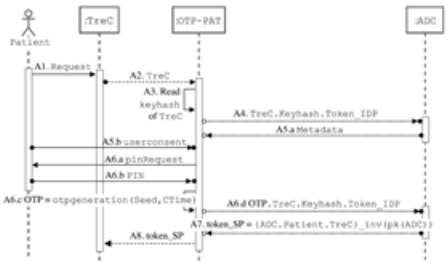
$G1_{MFA}$ is defined in terms of $G1_{BA}$

In the formal model, we consider $G1_{BA}$ and we check whether it holds even if the intruder compromises up to 2 instance-factors.

$G1_{BA}$	`SP_authn_U_on_Request:( ) Patient *->> TreC;`
G2	`...`

where `*->>` indicates authenticity, directedness (i.e. the only (honest) receiver of a message is the intended one) and freshness.

Phase 3: Security Analysis



MSC Scenario

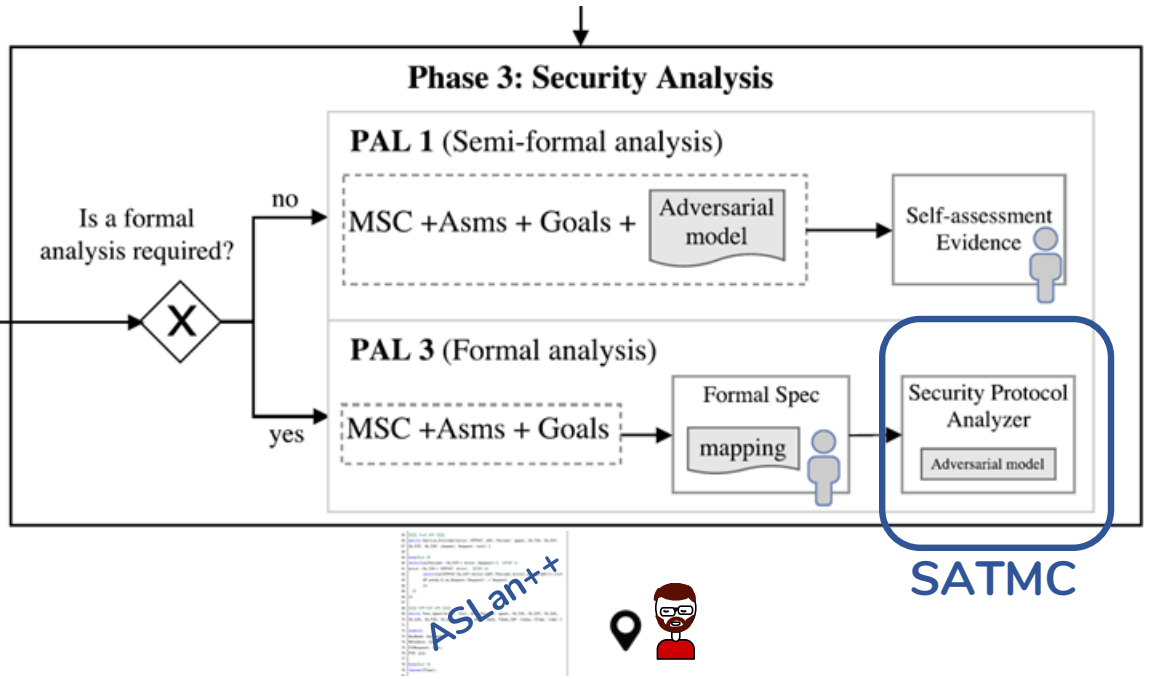
TA	ADC is trusted by TreC on identity assertions
BA1	Integrity and confidentiality of data stored in the device
...	...

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: $M_S \mid\mid M_I \models G_{BA}$

Phase 3: Security Analysis

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

Are all assumptions necessary?

- STRONG Asms

→ token_sp → user impersonation

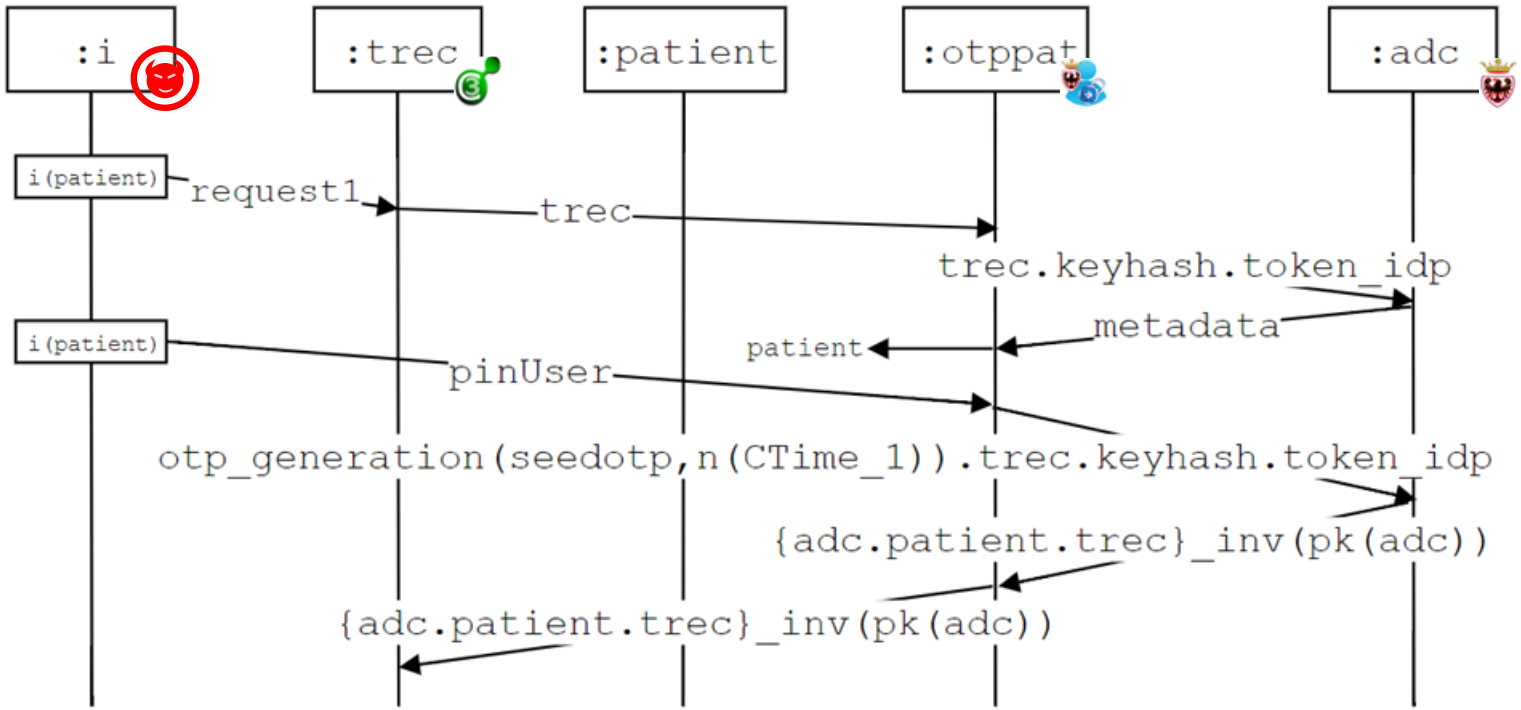
- WEAK Asms

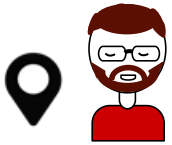
STOLEN SMARTPHONE → token_IdP, {seed}_PIN → NO atk

Removed Weak Asm(s)	Compromised Factors PIN	{seed}_PIN	token_IdP	Atk
BA1	x	✓	✓	No
BA2	✓	x	x	No
$UBA1_{Var1}$	✓	x	x	No
$UBA2_{Var1}$	x	✓	✓	No
$(UBA1_{Var1} \vee BA2) \wedge BA1$	✓	✓	✓	Yes
$(UBA1_{Var1} \vee BA2) \wedge UBA2_{Var1}$	✓	✓	✓	Yes

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

Phase 3: Security Analysis



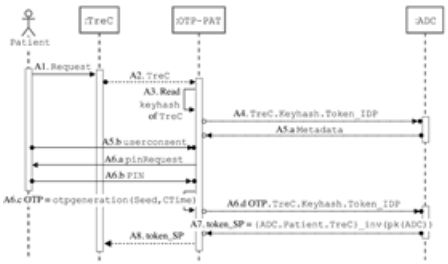


Proximity Intruder

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
- Keyboards of mobile devices 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

Phase 4: Usability Analysis

- We prepare two questionnaires based on ASQ (After Scenario Questionnaire), evaluating: effectiveness, efficiency and satisfaction.

Section 2. If the installation and activation of *OTP-PAT* succeeds:

1. Overall, I am satisfied with the easy of completing the activation of *OTP-PAT*.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
2. Overall, I am satisfied with the amount of time it took to complete the activation of *OTP-PAT*.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
3. Overall, I am satisfied with the support information (e.g, tutorial presentation in power-point and online documentation) when completing the activation of *OTP-PAT*.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
4. Overall, I am think that the activation phase is designed to guarantee a secure access to my health-data in the following exploitation phase.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
5. Please, leave us some comments on the activation phase (e.g., suggestions to simplify it)

Section 3. If the installation and activation of *OTP-PAT* do not succeed:

1. Which was your encountered difficulties during the installation and activation of *OTP-PAT*?

Section 1. Please, answer with YES or NO:

1. Did you succeed in accessing your PHRs using *TreC* and *OTP-PAT*?

Section 2. If you succeed:

1. Overall, I am satisfied with the easy of accessing *TreC* after the digit of a PIN in *OTP-PAT*.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
2. Overall, I am satisfied with the amount of time it took to access *TreC*.
   STRONGLY AGREE 1 2 3 4 5 6 7 STRONGLY DISAGREE
3. Please, leave us some comments on the exploitation phase (e.g., suggestions to simplify it)

Section 3. If you do not succeed:

1. Which was your difficulties during the access of *TreC* using *OTP-PAT*?

Outline

- IdM Mobile Context
- Problem Statement and Methodology Overview
- TreC Scenario
- IPZS/CIE Scenario
- Conclusions

CARTA DI IDENTITÀ ELETTRONICA
CIE 3.0

The project – main steps

- **23 December 2015**: publication of the D.M. containing the technical rules governing the issuance of the CIE

- **4 July 2016**: start of deployment in 199 Municipalities, including all the experimental Municipalities of the old document, the main cities (Rome, Milan, Naples, Florence, Venice, Udine ..) and some Municipalities identified as experimenters of the new ANPR

- **July 2017**: activation of additional 350 Municipalities and coverage of 50% of the Italian population

- **August 2018**: end of deployment in every Italian Municipalities (approximately 8,000)

Deployment Status

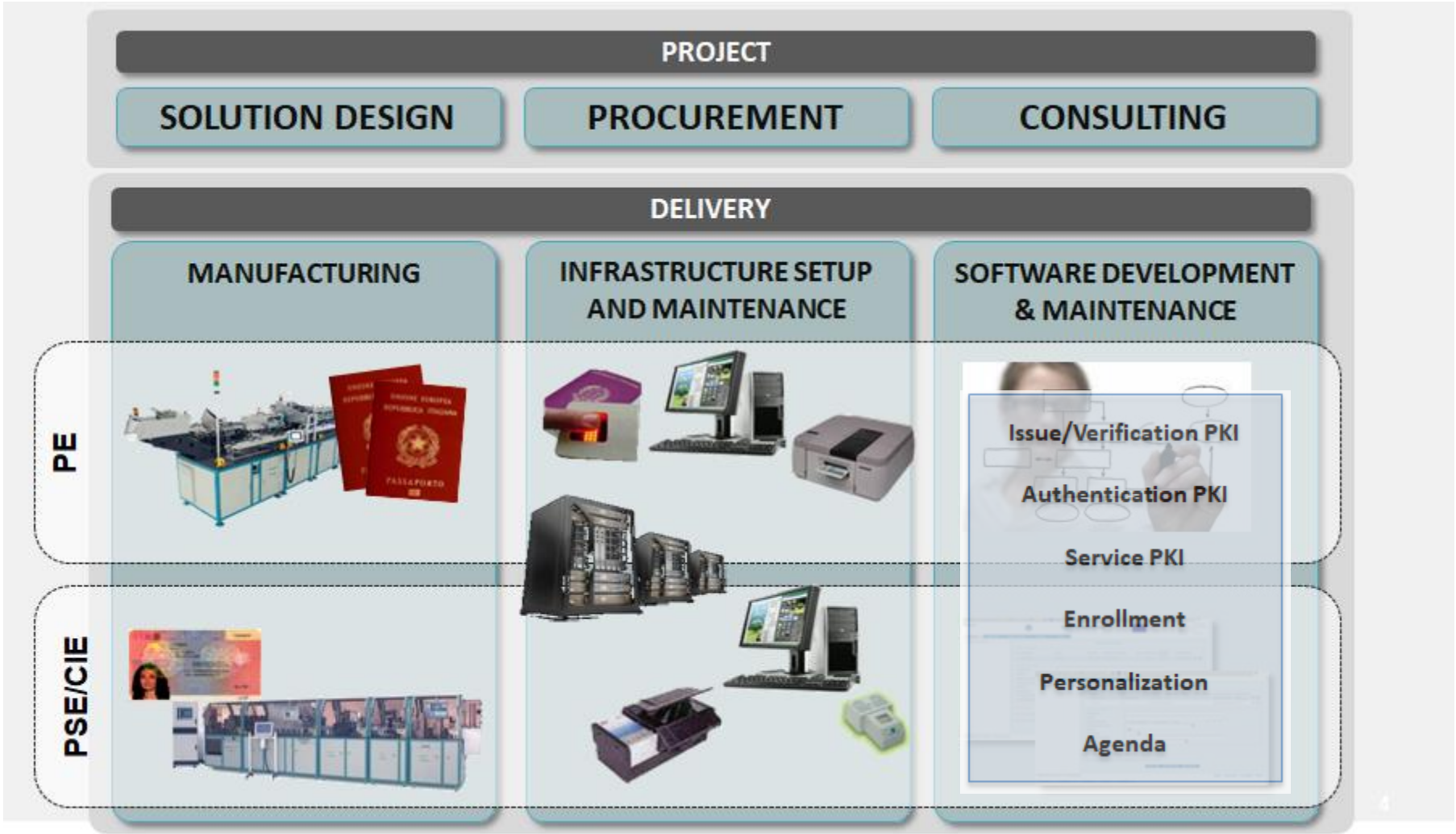
1.257 *Municipalities are issuing CIE*

1.630.025 *CIE issued*

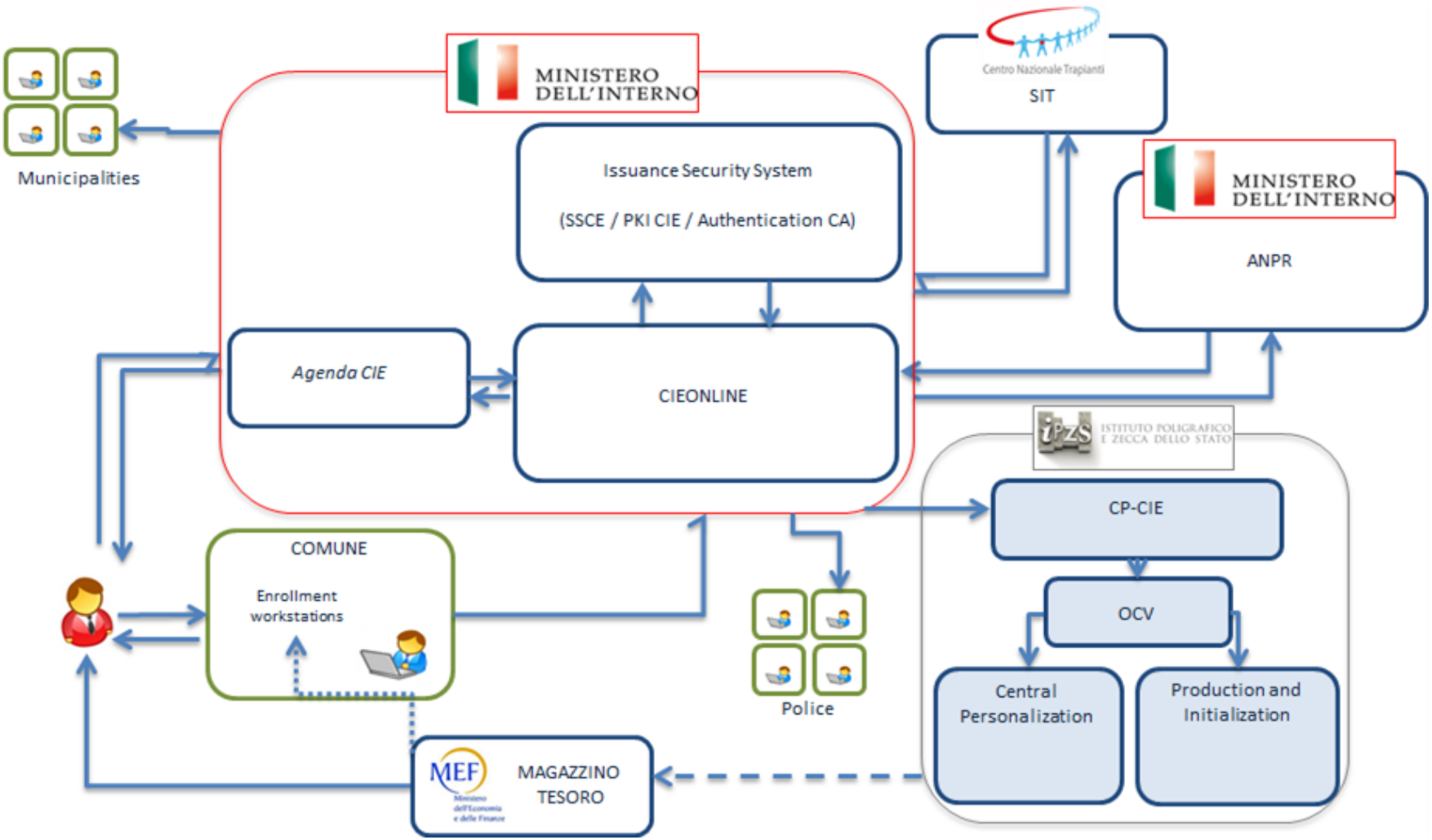
74,1% *population coverage*

3.800 *installed workstations*

IPZS role in electronic documents



Issuing process – the flows



Functionalities

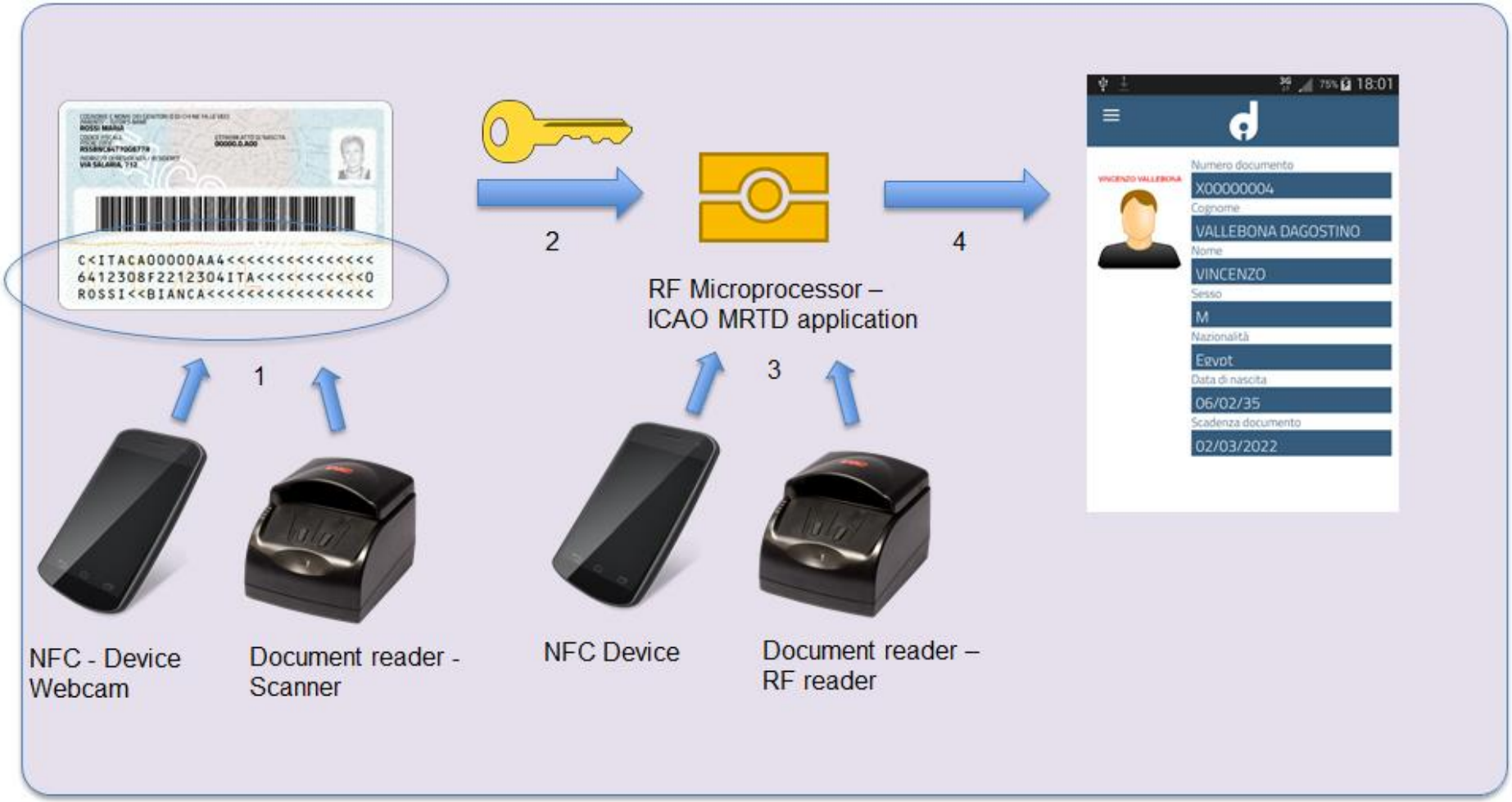
CIE 3.0 is:

A modern identification document: the ICAO MRTD application, containing the holder personal data, photo of the face and image of two fingerprints, is compliant with the ICAO specifications for travel documents

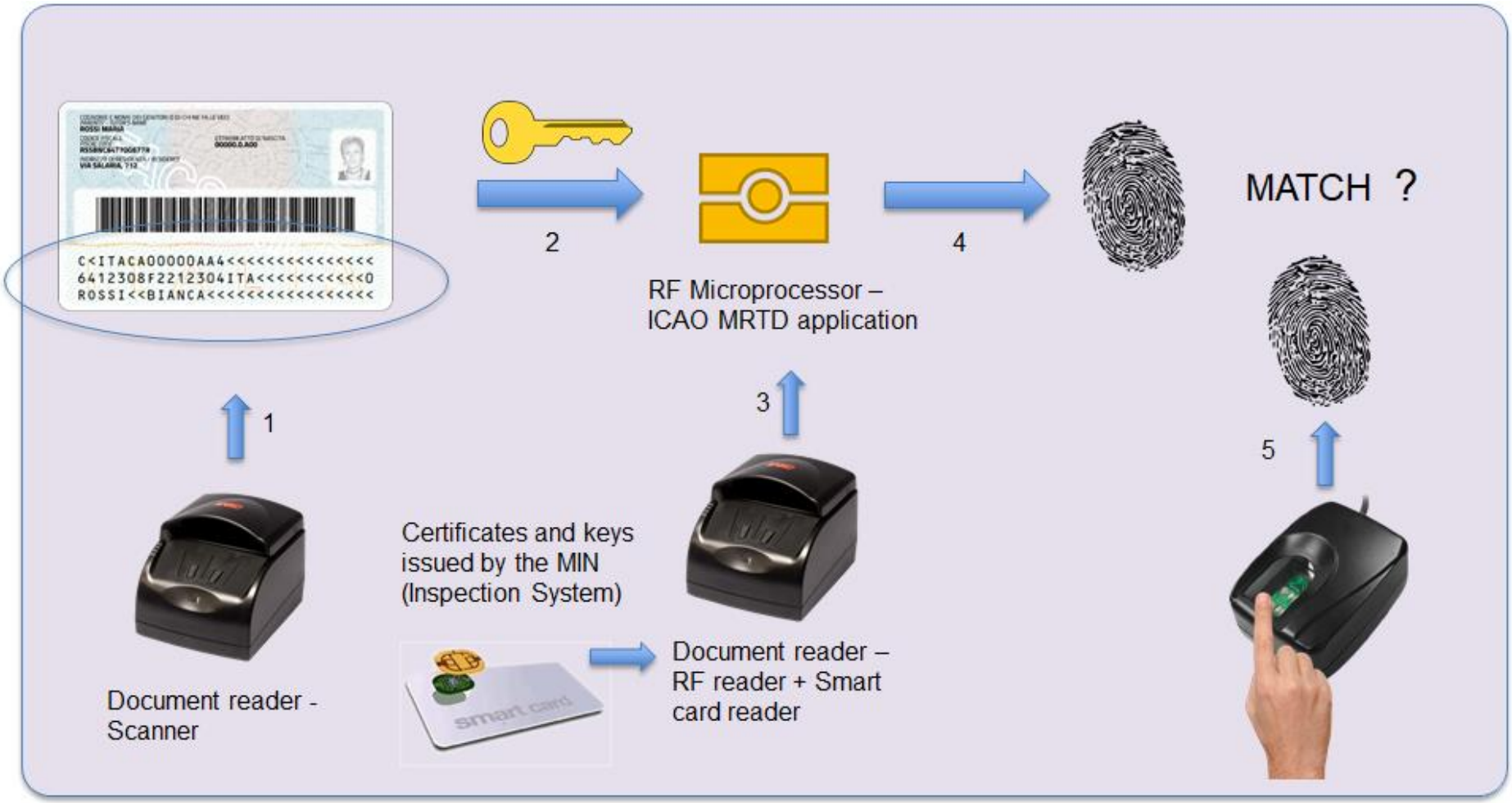
Security
Automatic Border Control

A tool for accessing services: the ECC (European Citizen Card) IAS application contains keys and X.509 certificates for secure access to online services

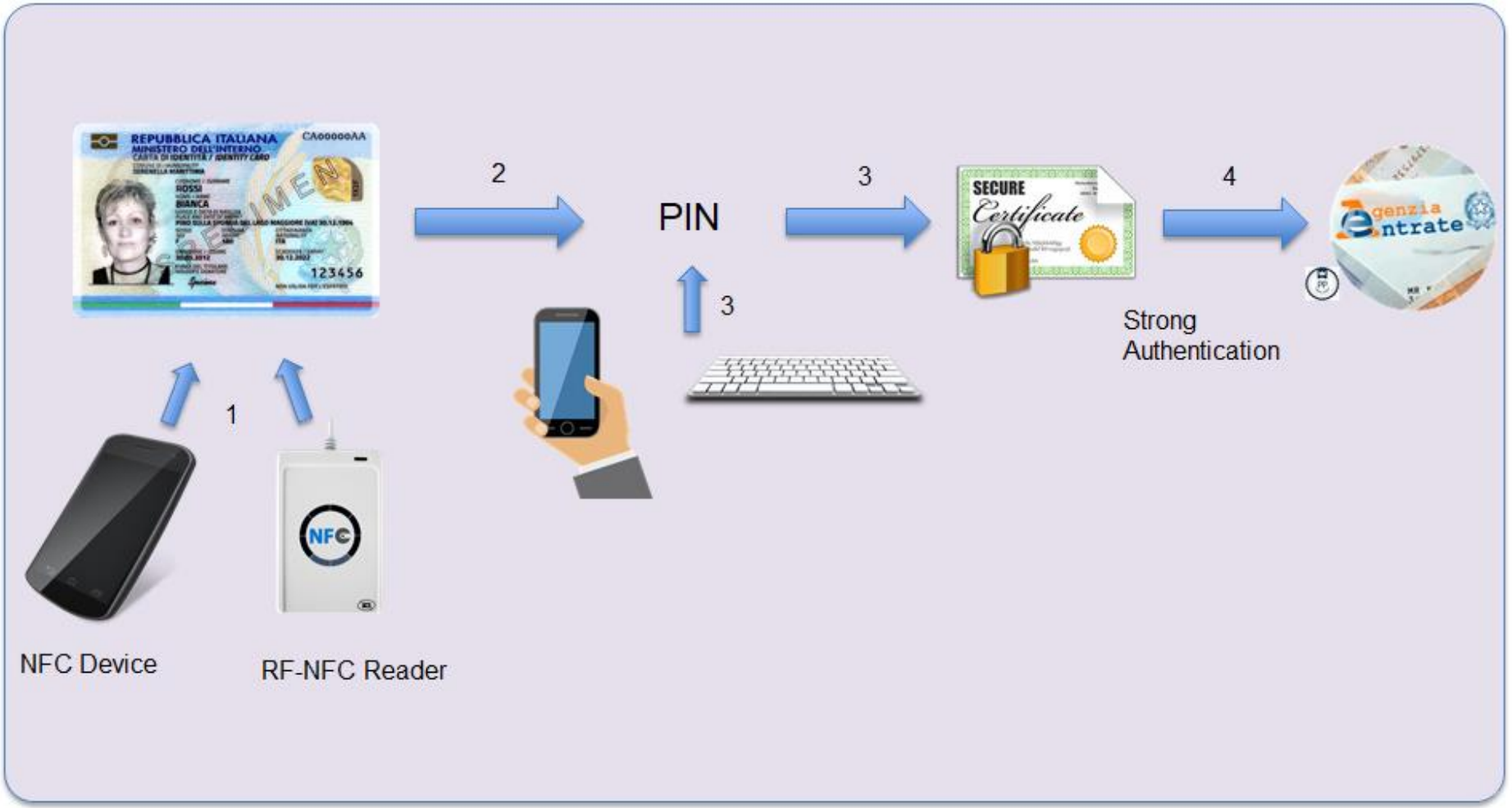
The microprocessor - use of ICAO application



The microprocessor - use of ICAO app (fingerprint verification)



The microprocessor - use of IAS application



Design approach

Contactless interface (RF) only for mobile and smartphones use

Functional and security standard protocols

Authentication with X.509 certificates to minimize the impact on service providers

Redesign of RF protocols

All specifications are public
http://www.cartaidentita.interno.gov.it/wp-content/uploads/2016/07/cie_3.0_-_specifiche_chip.pdf

Software

Ready applications

App Idea for identification

Support for application development

Middleware Windows, MacOS, Linux for authentication

SDK for Android authentication

Libraries for reading the chip on Android

developers.italia.it: sources and documentation
hack.developers 2017: Arduino e SDK Python libraries
makers faire Rome 2017

CIE on mobile - One-Time Password (OTP)

- OTP is usually used in addition to classic authentication (username and password) to achieve 2-factor authentication

CIE on mobile - One-Time Password (OTP)

- OTP is usually used in addition to classic authentication (username and password) to achieve 2-factor authentication

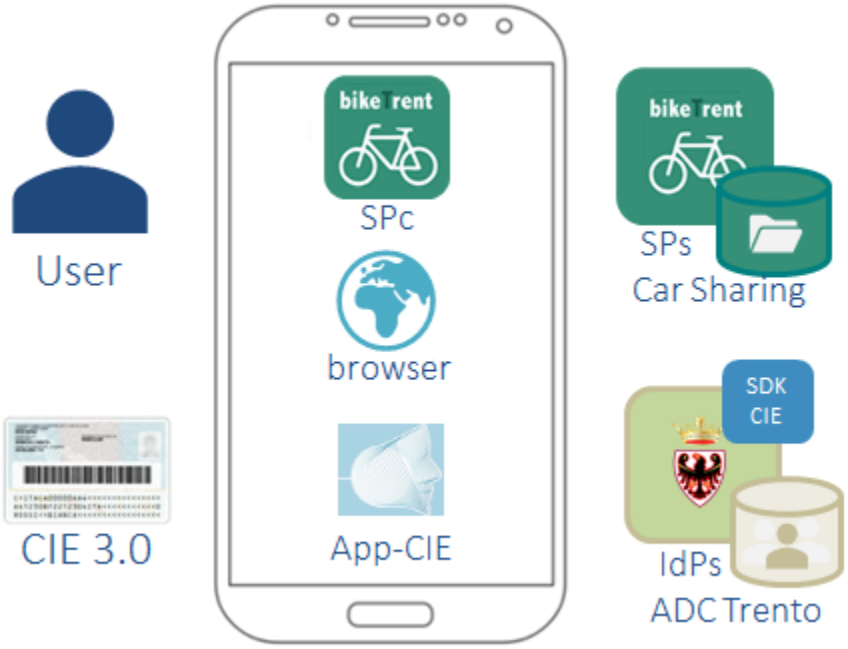
CIE on mobile - One-Time Password (OTP)

- OTP is usually used in addition to classic authentication (username and password) to achieve 2-factor authentication

- CIE as OTP generator thanks to its cryptographic features

CIE-based OTP solution

Goal: design, implementation, and security verification of a two-factor authentication solution in which OTP is generated using CIE cryptographic capabilities with a mobile device as NFC reader.



Outline

- IdM Mobile Context
- Problem Statement and Methodology Overview
- TreC Scenario
- IPZS/CIE Scenario
- Conclusions

Conclusions and Future Work

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

Future Work:

- Semi-automatic code generation
- Extensions of the AuthN aspects (Multi-IdP,)
- Formalization of other OTP generation approaches

References

- http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pd
- eIDAS. European Parliament. Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.
- SPID. DPCM of 24 October 2014, Sistema Pubblico per la gestione dell'Identità Digitale (SPID). http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid.
- 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.
- https://wearesocial.com/special-reports/digital-in-2017-global-overview
- 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.
- OAuth Working Group. OAuth 2.0 for Native Apps. https://tools.ietf.org/html/rfc8252, 2017.

References

- 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.
- Italian Personal Data Protection Code. Legislative Decree no. 196 of 30 June 2003.
- European Data Protection Directive 95/46 EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. http://eur-lex.europa.eu/legal-188content/EN/TXT/?uri=CELEX:31995L0046.
- TreC. https://trec.trentinosalute.net/.
- AVANTSSAR Project. Deliverable D2.3 (update) ASLan++ specification and tutorial. http://www.avantssar.eu/pdf/deliverables/avantssar-d2-3_update.pdf, 2008.
- Ministero dell'Interno and IPZS. Carta d'Identità Elettronica CIE 3.0 - Specifiche Chip. http://www.cartaidentita.interno.gov.it/wp-content/uploads/2016/07/cie_3.0_-_specifiche_chip.pdf.
- 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).

References

- 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 , to appear).

https://st.fbk.eu/tutorial-itasec-18