How can eID cards improve the security and usability of authentication protocols?

From the design to the security and risk analysis

Marco Pernpruner

PhD Student, Fondazione Bruno Kessler (Trento, Italy)
and University of Genoa (Genoa, Italy)

JUNE 2021 | #identiverse

identiverse®

Agenda

1

Introduction to eID cards

General features and security components

2

eID cards in real-world scenarios

Practical examples involving eID cards

3

What about security?

A methodology to analyse protocols based on eID cards

4

Conclusions

1

Introduction to eID cards

General features and security components

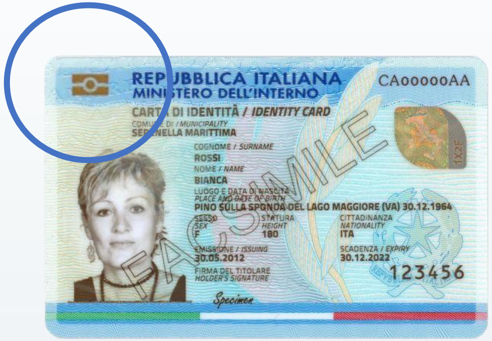
What are eID cards?

- Official identity document in **many countries**.
- Replace **paper-based** version.
- Personal data of the owner are **printed** on the plastic surface.
    - Visual security elements such as holograms **prevent counterfeiting**.

BELGIË BELGIQUE BELGIEN BELGIUM
IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD
HUNGARY IDENTITY CARD
MÉSZÁROS BRIGITTA ERZSÉBET
CARTÃO DE CIDADÃO CITIZEN CARD PORTUGAL
DA CONCEIÇÃO ÁVILA
AULA ANDREIA
NEDERLANDSE IDENTITEITSKAART KONINKRIJK DER NEDERLANDEN
De Bruijn
Willeke Liselotte
Rzeczpospolita Polska Republic of Poland
Dowód osobisty Identity card
KOWALSKI - BRZĘCZYSZCZYKIEWICZ
PAWEŁ JAN
BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
T22000129
MUSTERMANN
GEB. GABLER
REPUBBLICA ITALIANA
MINISTERO DELL'INTERNO
CARTA DI IDENTITÀ / IDENTITY CARD
CA00000AA
ROSSI
BIANCA
FAC SIMILE

Security features

- From a security perspective, eID cards are equipped with:
  - a **contactless chip**;



REPUBBLICA ITALIANA
MINISTERO DELL'INTERNO

CA00000AA

CARTA DI IDENTITÀ / *IDENTITY CARD*

COMUNE DI / *MUNICIPALITY*
SERENELLA MARITTIMA

COGNOME / *SURNAME*
ROSSI

NOME / *NAME*
BIANCA

LUOGO E DATA DI NASCITA
PLACE AND DATE OF BIRTH
PINO SULLA SPONDA DEL LAGO MAGGIORE (VA) 30.12.1964

SESSO / *SEX*: F
STATURA / *HEIGHT*: 180
CITTADINANZA / *NATIONALITY*: ITA

EMISSIONE / *ISSUING*
30.05.2012

SCADENZA / *EXPIRY*
30.12.2022

FIRMA DEL TITOLARE
HOLDER'S SIGNATURE
Specimen

123456

COGNOME E NOME DEI GENITORI O DI CHI NE FA LE VECI
SURNAME AND NAME OF PARENTS OR LEGAL GUARDIAN
ROSSI MARIA

CODICE FISCALE
FISCAL CODE
RSSBNC64T70G677R

ESTREMI ATTO DI NASCITA
00000.0.A00

INDIRIZZO DI RESIDENZA / *RESIDENCE*
VIA SALARIA, 712

```
C<ITACA00000AA4<<<<<<<<<<<<<<<
6412308F2212304ITA<<<<<<<<<<<0
ROSSI<<BIANCA<<<<<<<<<<<<<<<<<
```

Security features

- From a security perspective, eID cards are equipped with:
    - a **contactless chip**;
    - an **X.509 certificate**;

REPUBBLICA ITALIANA
MINISTERO DELL'INTERNO
CA00000AA

CARTA DI IDENTITÀ / *IDENTITY CARD*

COMUNE DI / *MUNICIPALITY*
SERENELLA MARITTIMA

COGNOME / *SURNAME*
ROSSI

NOME / *NAME*
BIANCA

LUOGO E DATA DI NASCITA
PLACE AND DATE OF BIRTH
PINO SULLA SPONDA DEL LAGO MAGGIORE (VA) 30.12.1964

SESSO / *SEX*: F
STATURA / *HEIGHT*: 180
CITTADINANZA / *NATIONALITY*: ITA

EMISSIONE / *ISSUING*
30.05.2012

SCADENZA / *EXPIRY*
30.12.2022

FIRMA DEL TITOLARE
HOLDER'S SIGNATURE
Specimen

123456

FACSIMILE

Private Key

COGNOME E NOME DEI GENITORI O DI CHI NE FA LE VECI
SURNAME AND NAME OF PARENTS OR LEGAL GUARDIAN
ROSSI MARIA

CODICE FISCALE
FISCAL CODE
RSSBNC64T70G677R

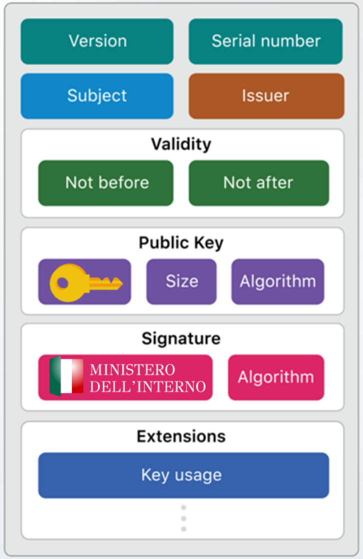
ESTREMI ATTO DI NASCITA
00000.0.A00

INDIRIZZO DI RESIDENZA / *RESIDENCE*
VIA SALARIA, 712

FACSIMILE

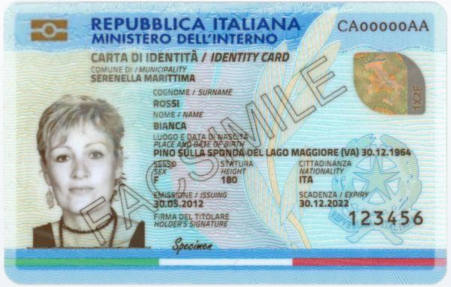
```
C<ITACA00000AA4<<<<<<<<<<<<<<<
6412308F2212304ITA<<<<<<<<<<<0
ROSSI<<BIANCA<<<<<<<<<<<<<<<<<
```

X.509 certificate



Security features

- From a security perspective, eID cards are equipped with:
    - a **contactless chip**;
    - an **X.509 certificate**;
    - a customizable **PIN code**;



REPUBBLICA ITALIANA
MINISTERO DELL'INTERNO

CA00000AA

CARTA DI IDENTITÀ / *IDENTITY CARD*

COMUNE DI / *MUNICIPALITY*
SERENELLA MARITTIMA

COGNOME / *SURNAME*
ROSSI

NOME / *NAME*
BIANCA

LUOGO E DATA DI NASCITA
PLACE AND DATE OF BIRTH
PINO SULLA SPONDA DEL LAGO MAGGIORE (VA) 30.12.1964

SESSO / *SEX*: F
STATURA / *HEIGHT*: 180
CITTADINANZA / *NATIONALITY*: ITA

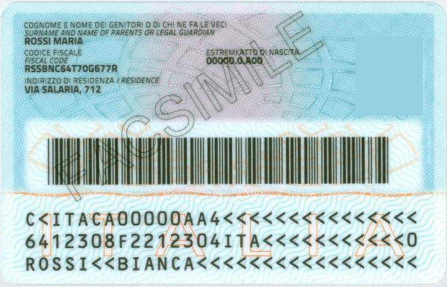
EMISSIONE / *ISSUING*
30.05.2012

SCADENZA / *EXPIRY*
30.12.2022

FIRMA DEL TITOLARE
HOLDER'S SIGNATURE
Specimen

123456

FACSIMILE



COGNOME E NOME DEI GENITORI O DI CHI NE FA LE VECI
SURNAME AND NAME OF PARENTS OR LEGAL GUARDIAN
ROSSI MARIA

CODICE FISCALE
FISCAL CODE
RSSBNC64T70G677R

ESTREMI ATTO DI NASCITA
00000.0.A00

INDIRIZZO DI RESIDENZA / *RESIDENCE*
VIA SALARIA, 712

```
C<ITACA00000AA4<<<<<<<<<<<<<<<
6412308F2212304ITA<<<<<<<<<<<0
ROSSI<<BIANCA<<<<<<<<<<<<<<<<<
```

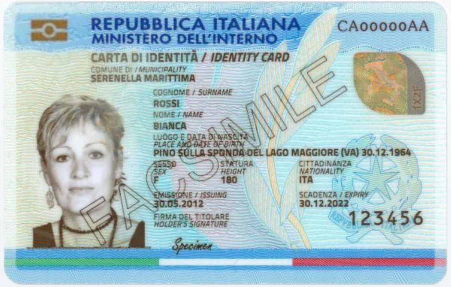
FACSIMILE

PIN code

****

Security features

- From a security perspective, eID cards are equipped with:
  - a **contactless chip**;
  - an **X.509 certificate**;
  - a customizable **PIN code**;
  - a **machine-readable zone** (MRZ).



REPUBBLICA ITALIANA
MINISTERO DELL'INTERNO

CA00000AA

CARTA DI IDENTITÀ / *IDENTITY CARD*

COMUNE DI / *MUNICIPALITY*
SERENELLA MARITTIMA

COGNOME / *SURNAME*
ROSSI

NOME / *NAME*
BIANCA

LUOGO E DATA DI NASCITA
PLACE AND DATE OF BIRTH
PINO SULLA SPONDA DEL LAGO MAGGIORE (VA) 30.12.1964

SESSO
SEX
F

STATURA
HEIGHT
180

CITTADINANZA
NATIONALITY
ITA

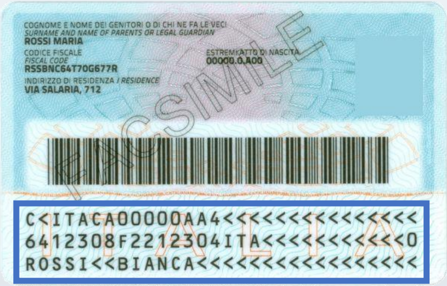
EMISSIONE / *ISSUING*
30.05.2012

SCADENZA / *EXPIRY*
30.12.2022

FIRMA DEL TITOLARE
HOLDER'S SIGNATURE

Specimen

123456



COGNOME E NOME DEI GENITORI O DI CHI NE FA LE VECI
SURNAME AND NAME OF PARENTS OR LEGAL GUARDIAN
ROSSI MARIA

CODICE FISCALE
FISCAL CODE
RSSBNC64T70G677R

ESTREMI ATTO DI NASCITA
00000.0.A00

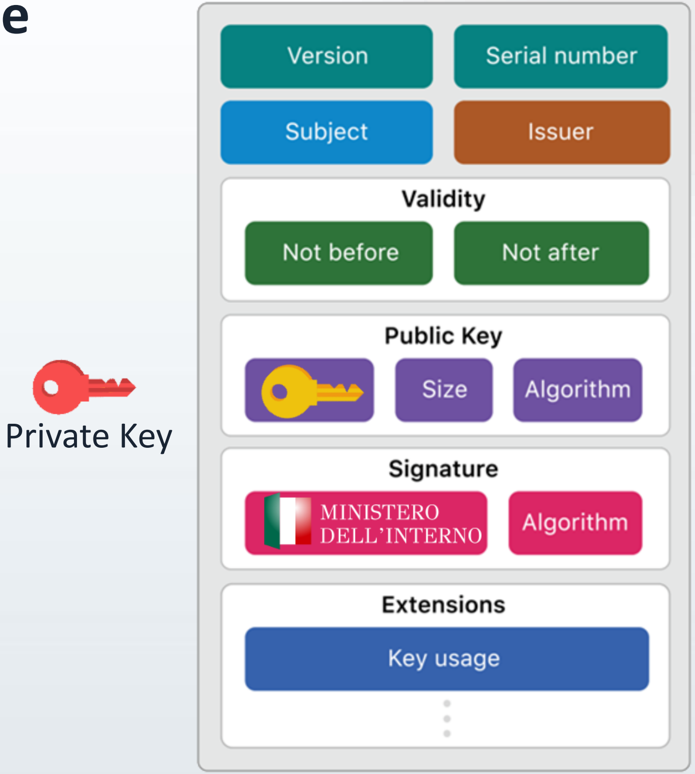
INDIRIZZO DI RESIDENZA / *RESIDENCE*
VIA SALARIA, 712

```
C<ITACA00000AA4<<<<<<<<<<<<<<<
6412308F2212304ITA<<<<<<<<<<<0
ROSSI<<BIANCA<<<<<<<<<<<<<<<<<
```

Security features

The X.509 certificate

- Each eID card has a personal X.509 certificate.
- The certificate provides guarantee on the **integrity** of the attested data.
- Moreover, it provides a **digital signature** scheme:
  - eID cards can **sign** objects by using their **private keys**;
  - other entities can **verify** the correctness of the signature by using the eID cards' **public keys**.



Private Key

Version

Serial number

Subject

Issuer

Validity

Not before

Not after

Public Key

Size

Algorithm

Signature

MINISTERO DELL'INTERNO

Algorithm

Extensions

Key usage

Our experience

- Joint work with *Poligrafico e Zecca dello Stato Italiano* (IPZS, the **Italian Government Printing Office and Mint**).
  - Shared laboratory ***DigiMat Lab*** (2017-2020);
  - In-house company ***Futuro & Conoscenza*** from 2021.

FONDAZIONE
BRUNO KESSLER

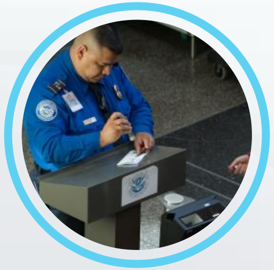
POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO

2

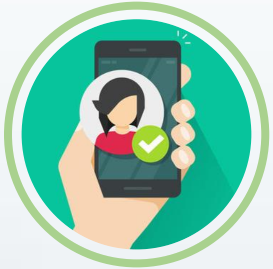
eID cards in real-world scenarios

Practical examples involving eID cards

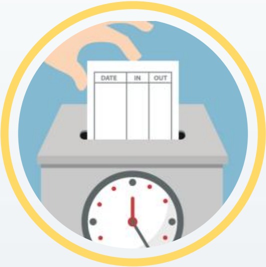
Real-world scenarios



Physical identity proofing



Remote identity proofing

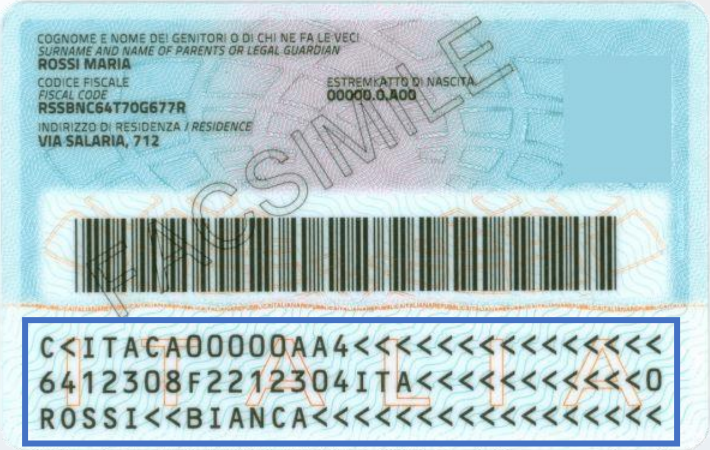


Advanced scenarios

Online authentication

Physical identity proofing

- Accessing data from eID cards…
  - … requires the MRZ, needed to derive the key for mutual authentication.
- Then, data can be accessed by interacting with the contactless chip.



COGNOME E NOME DEI GENITORI O DI CHI NE FA LE VECI
SURNAME AND NAME OF PARENTS OR LEGAL GUARDIAN
ROSSI MARIA

CODICE FISCALE
FISCAL CODE
RSSBNC64T70G677R

ESTREMI ATTO DI NASCITA
00000.0.A00

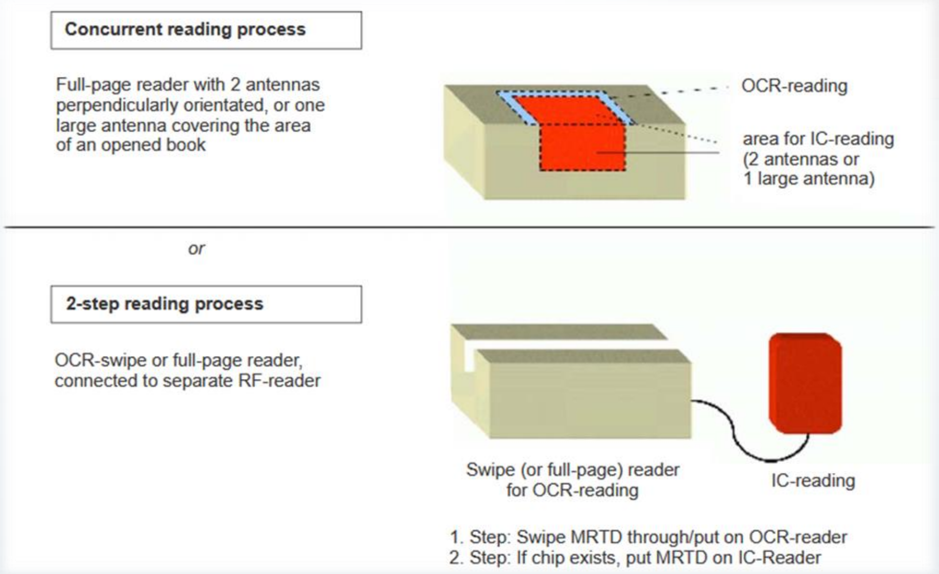
INDIRIZZO DI RESIDENZA / *RESIDENCE*
VIA SALARIA, 712

```
C<ITACA00000AA4<<<<<<<<<<<<<<<
6412308F2212304ITA<<<<<<<<<<<0
ROSSI<<BIANCA<<<<<<<<<<<<<<<<<
```

FACSIMILE
ITALIA

Physical identity proofing

- This process is officially acknowledged by the International Civil Aviation Organization.
- The use of eDocuments allow for automatic identity verification processes.



Concurrent reading process

Full-page reader with 2 antennas perpendicularly orientated, or one large antenna covering the area of an opened book

OCR-reading
area for IC-reading (2 antennas or 1 large antenna)

or

2-step reading process

OCR-swipe or full-page reader, connected to separate RF-reader

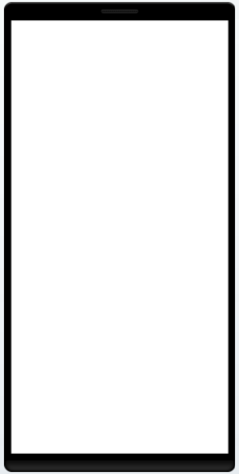
Swipe (or full-page) reader for OCR-reading
IC-reading

1. Step: Swipe MRTD through/put on OCR-reader
2. Step: If chip exists, put MRTD on IC-Reader

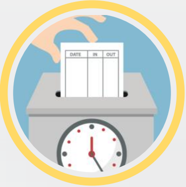
Source: ICAO, Doc 9303: Machine Readable Travel Documents, Part 9

Remote identity proofing

- More and more operations can now be performed totally online…
  - … just imagine opening a bank account.
- High assurance on people's identity is required.
  - eDocuments can be used to provide the needed assurance.



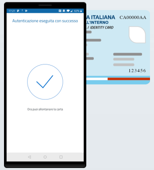
Advanced scenarios



Clocking-in/out

Pull printing

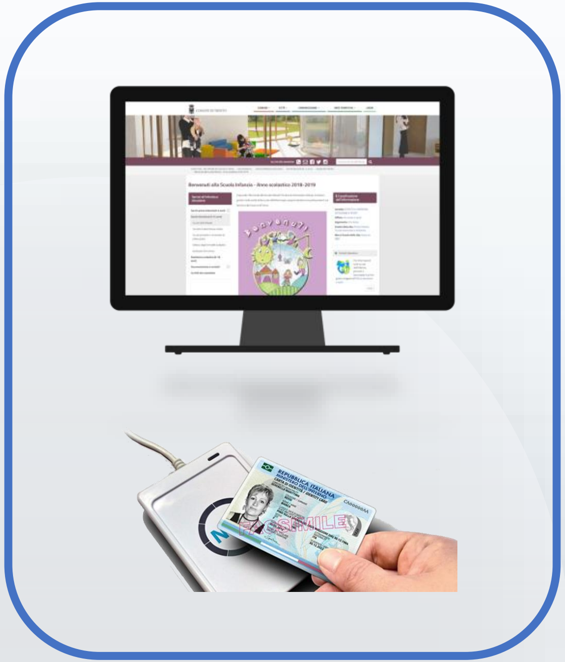
eID cards replacing identification badges



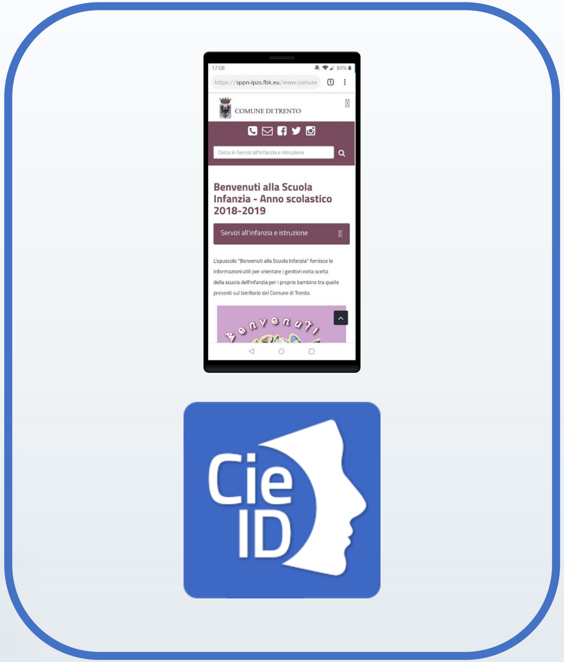
Custom applications to improve clocking processes

eID cards to properly identify employee

Online authentication



Total-desktop


17:08 84%

https://sppn-ipzs.fbk.eu/www.comune

COMUNE DI TRENTO

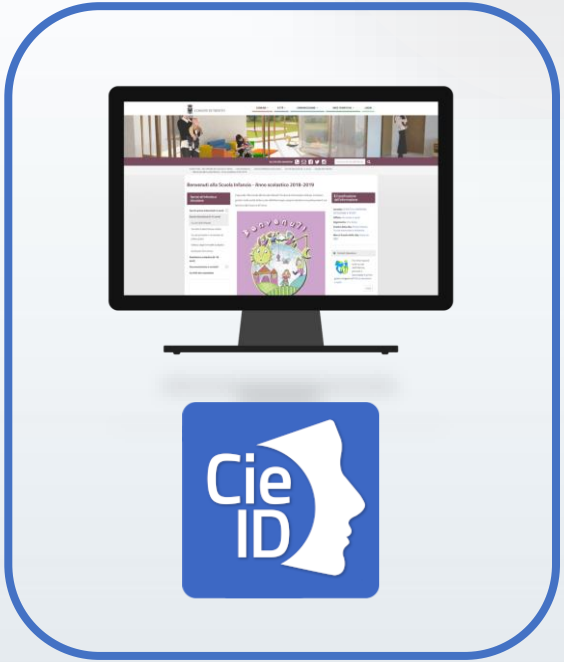
Cerca in Servizi all'infanzia e istruzione

Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019

Servizi all'infanzia e istruzione

L'opuscolo "Benvenuti alla Scuola Infanzia" fornisce le informazioni utili per orientare i genitori nella scelta della scuola dell'infanzia per i proprio bambino tra quelle presenti sul territorio del Comune di Trento.

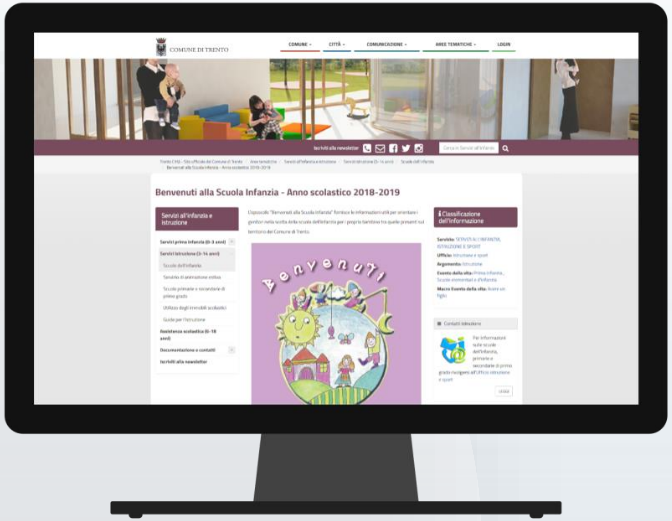
Total-mobile



Hybrid

Online authentication

Total-desktop solution



Trento Città - Sito ufficiale del Comune di Trento / Aree tematiche / Servizi all'infanzia e istruzione / Servizi istruzione (3-14 anni) / Scuole dell'infanzia / Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019

Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019

Servizi all'infanzia e istruzione

- Servizi prima infanzia (0-3 anni)
- Servizi istruzione (3-14 anni)
- Scuole dell'infanzia
- Servizio di animazione estiva
- Scuole primarie e secondarie di primo grado
- Utilizzo degli immobili scolastici
- Guide per l'istruzione
- Assistenza scolastica (0-18 anni)
- Documentazione e contatti
- Iscriviti alla newsletter

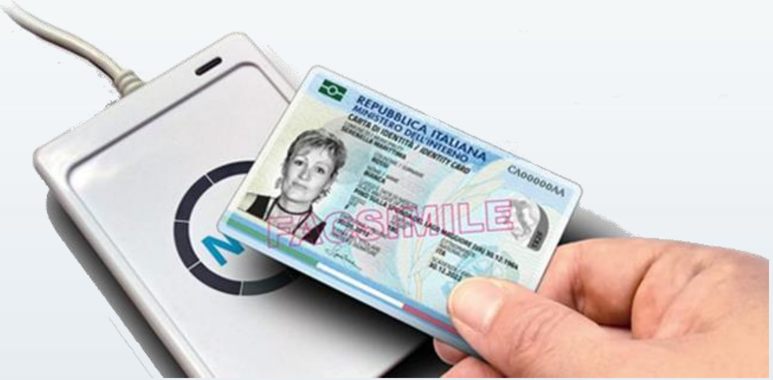
L'opuscolo "Benvenuti alla Scuola Infanzia" fornisce le informazioni utili per orientare i genitori nella scelta della scuola dell'infanzia per i propri bambini tra quelle presenti sul territorio del Comune di Trento.

Classificazione dell'informazione

Servizio: SERVIZI ALL'INFANZIA, ISTRUZIONE E SPORT
Ufficio: Istruzione e sport
Argomento: Istruzione
Evento della vita: Prima infanzia, Scuole elementari e d'infanzia
Macro Evento della vita: Avere un figlio

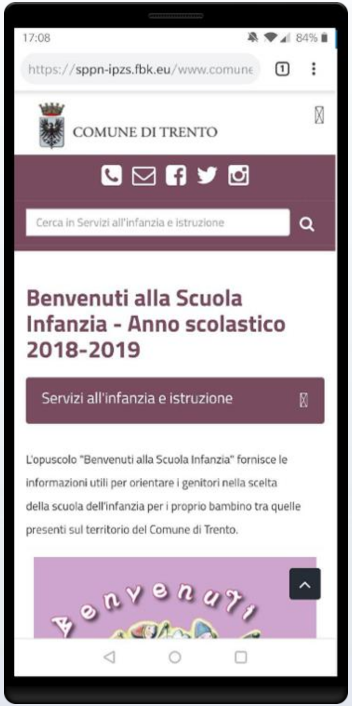
Contatti Istruzione

Per informazioni sulle scuole dell'infanzia, primarie e secondarie di primo grado rivolgersi all'Ufficio istruzione e sport



Online authentication

Total-mobile solution



17:08 84%

https://sppn-ipzs.fbk.eu/www.comune

COMUNE DI TRENTO

Cerca in Servizi all'infanzia e istruzione

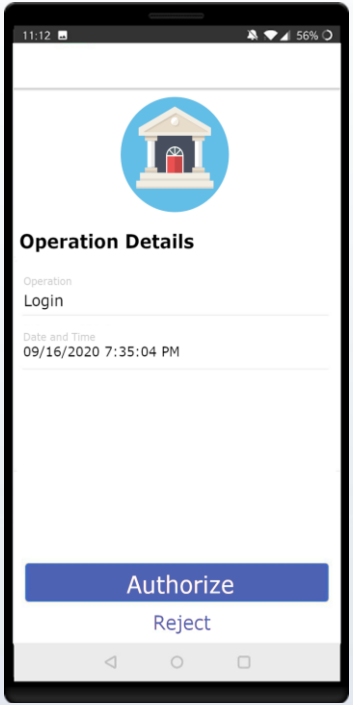
Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019

Servizi all'infanzia e istruzione

L'opuscolo "Benvenuti alla Scuola Infanzia" fornisce le informazioni utili per orientare i genitori nella scelta della scuola dell'infanzia per i proprio bambino tra quelle presenti sul territorio del Comune di Trento.

Online authentication

Total-mobile solution



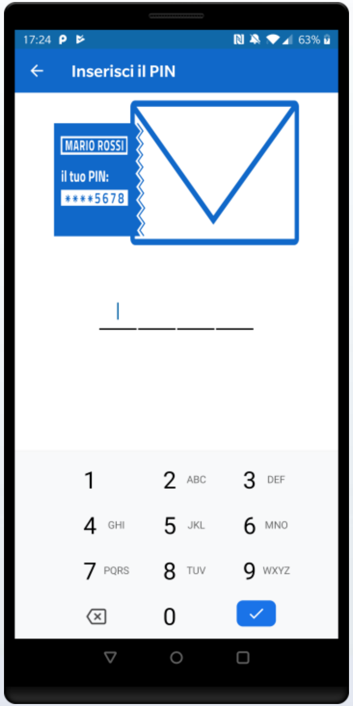
Operation Details

Operation
Login

Date and Time
09/16/2020 7:35:04 PM

Online authentication

Total-mobile solution



17:24 63%

Inserisci il PIN

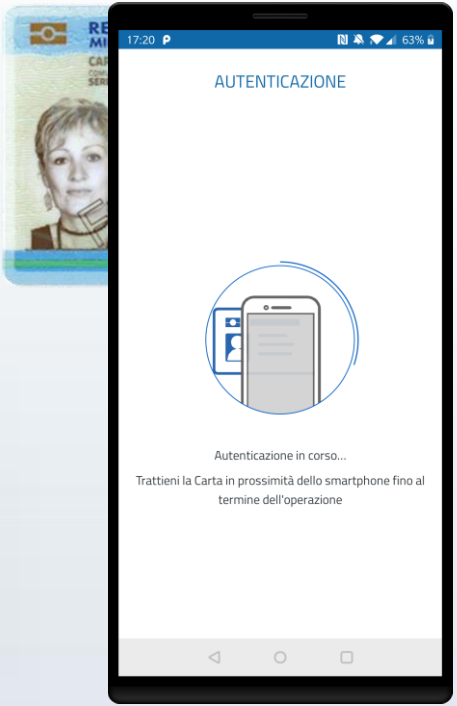
MARIO ROSSI

il tuo PIN:

****5678

Online authentication

Total-mobile solution



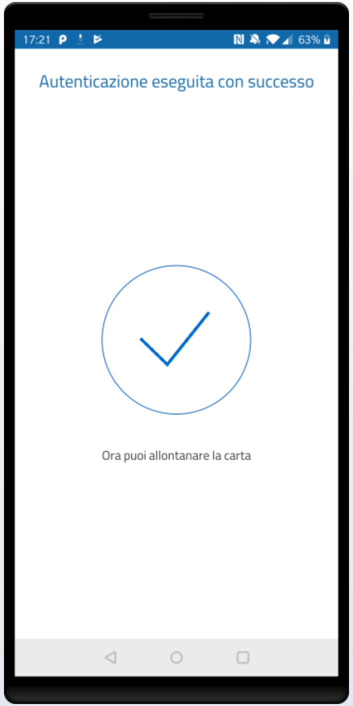
AUTENTICAZIONE

Autenticazione in corso...

Trattieni la Carta in prossimità dello smartphone fino al termine dell'operazione

Online authentication

Total-mobile solution



Autenticazione eseguita con successo

Ora puoi allontanare la carta

Online authentication

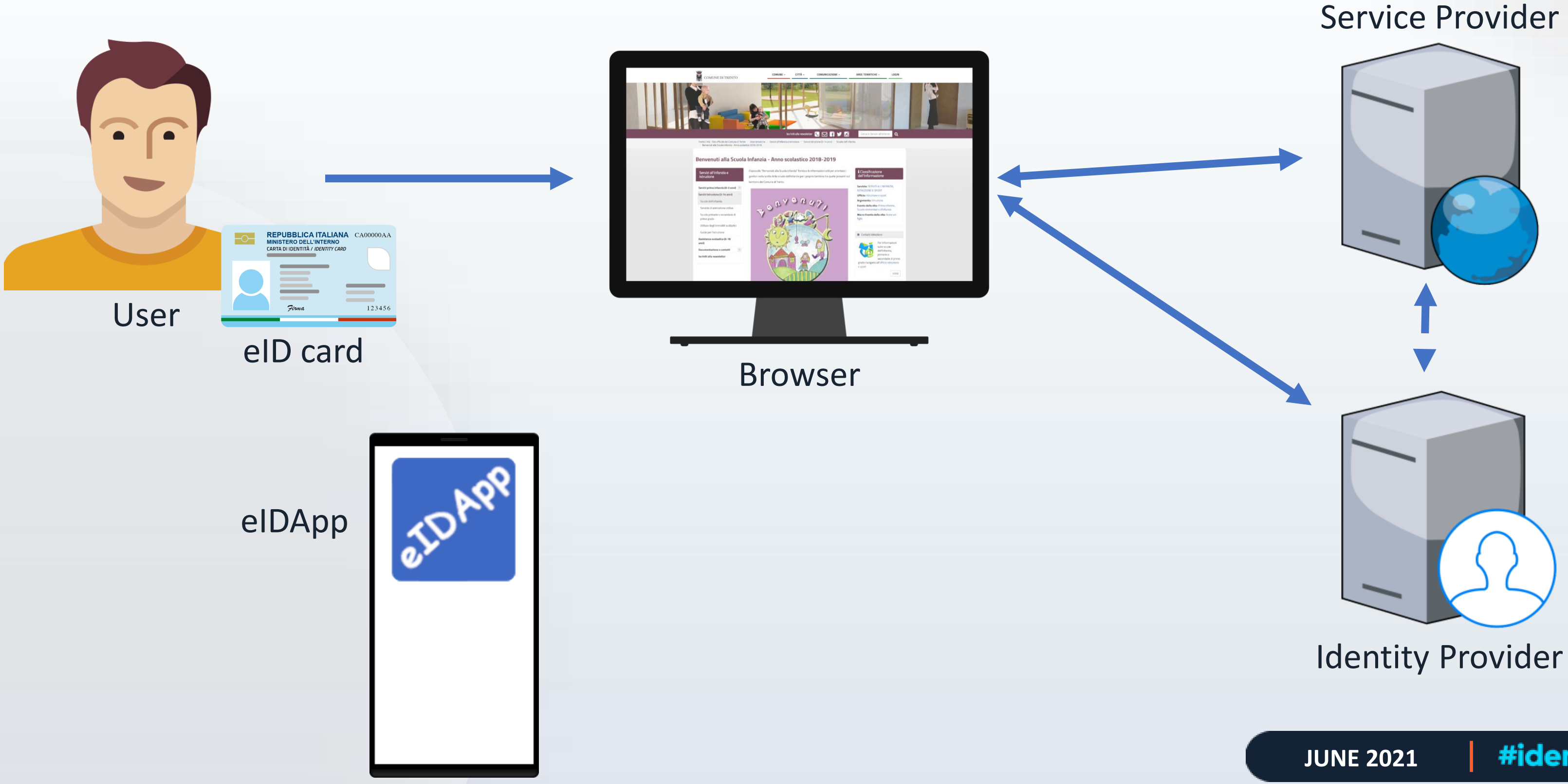
Hybrid solutions

Given the different requirements that may arise, we consider two hybrid solutions:

- a **one-shot solution** that can be used without any prior operation (except for card registration), relying on QR codes;

Online authentication

One-shot hybrid solution – Involved entities



User

eID card

Browser

Service Provider

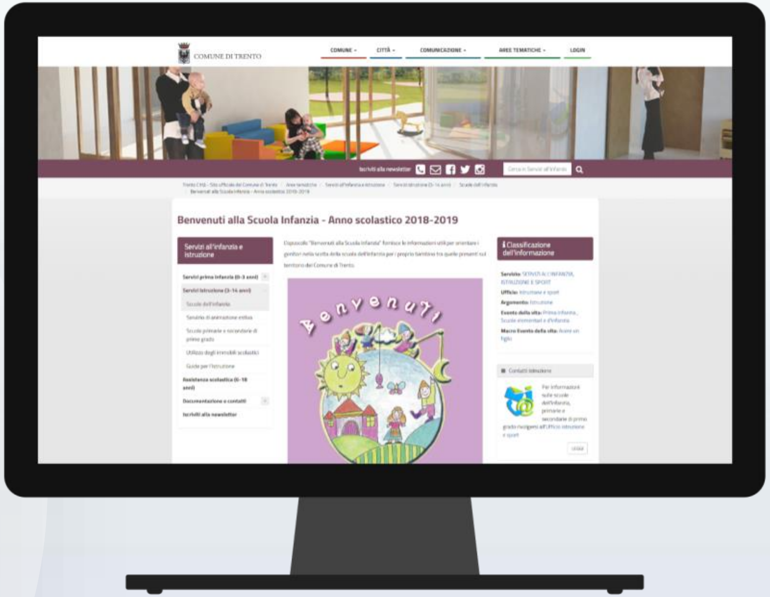
Identity Provider

eIDApp

REPUBBLICA ITALIANA
CA00000AA
MINISTERO DELL'INTERNO
CARTA DI IDENTITÀ / IDENTITY CARD
Firma
123456
Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019
eIDApp

Online authentication

One-shot hybrid solution – Authentication



Trento Città - Sito ufficiale del Comune di Trento / Aree tematiche / Servizi all'infanzia e istruzione / Servizi istruzione (3-14 anni) / Scuole dell'infanzia / Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019

Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019

Servizi all'infanzia e istruzione

- Servizi prima infanzia (0-3 anni)
- Servizi istruzione (3-14 anni)
  - Scuole dell'infanzia
  - Servizio di animazione estiva
  - Scuole primarie e secondarie di primo grado
  - Utilizzo degli immobili scolastici
  - Guide per l'istruzione
- Assistenza scolastica (6-18 anni)
- Documentazione e contatti
- Iscriviti alla newsletter

L'opuscolo "Benvenuti alla Scuola Infanzia" fornisce le informazioni utili per orientare i genitori nella scelta della scuola dell'infanzia per i propri bambini tra quelle presenti sul territorio del Comune di Trento.

Classificazione dell'informazione

Servizio: SERVIZI ALL'INFANZIA, ISTRUZIONE E SPORT

Ufficio: Istruzione e sport

Argomento: Istruzione

Evento della vita: Prima infanzia, Scuole elementari e d'infanzia

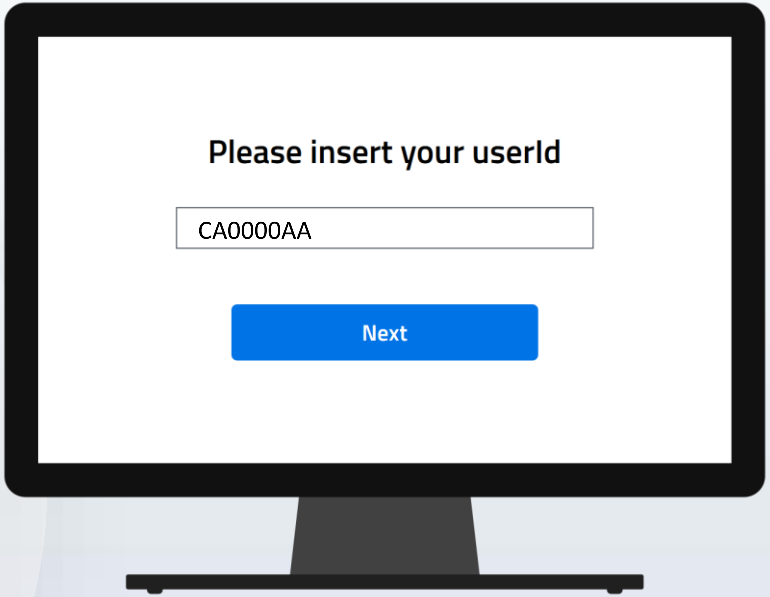
Macro Evento della vita: Avere un figlio

Contatti istruzione

Per informazioni sulle scuole dell'infanzia, primarie e secondarie di primo grado rivolgersi all'Ufficio istruzione e sport

Online authentication

One-shot hybrid solution – Authentication



Please insert your userId

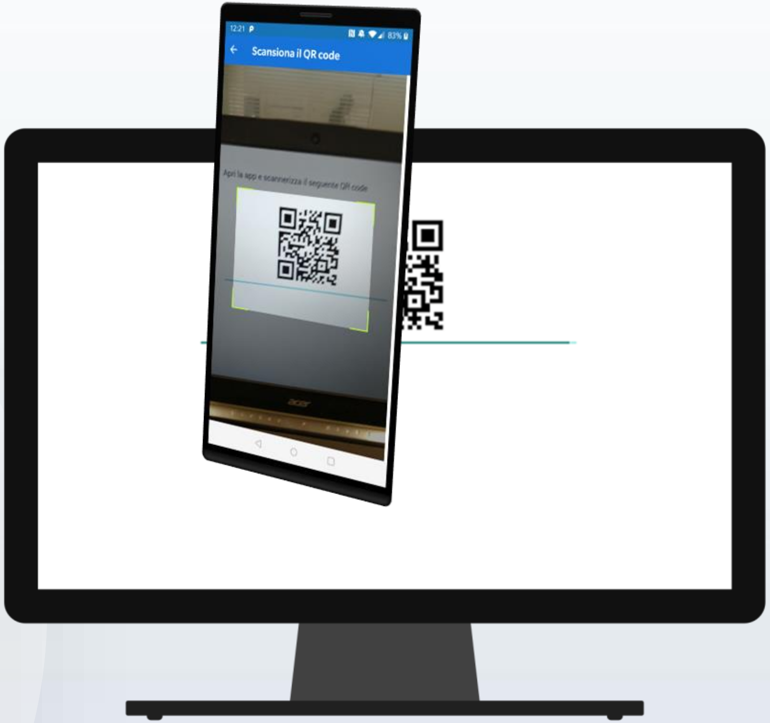
CA0000AA

Online authentication

One-shot hybrid solution – Authentication

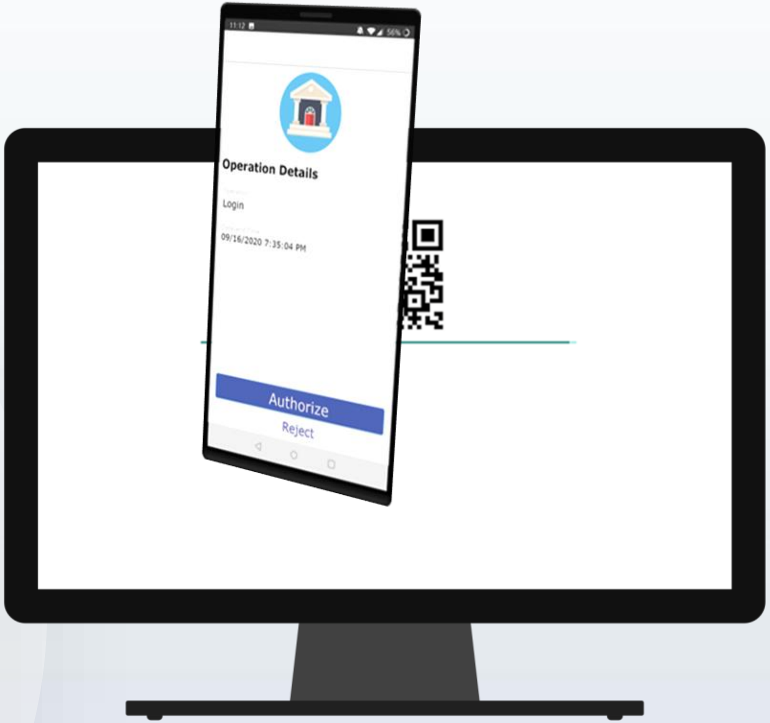
Online authentication

One-shot hybrid solution – Authentication



Online authentication

One-shot hybrid solution – Authentication



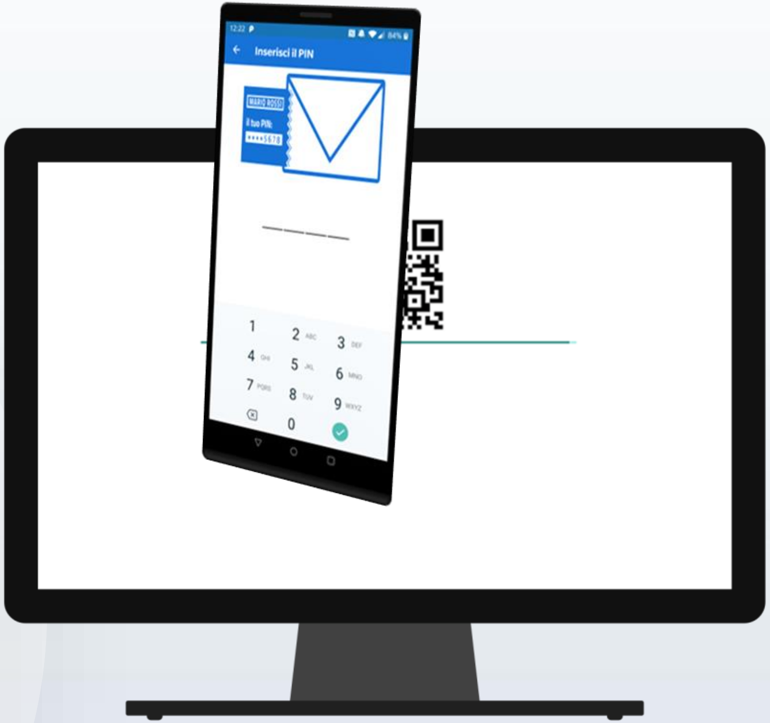
Operation Details

Login

09/16/2020 7:35:04 PM

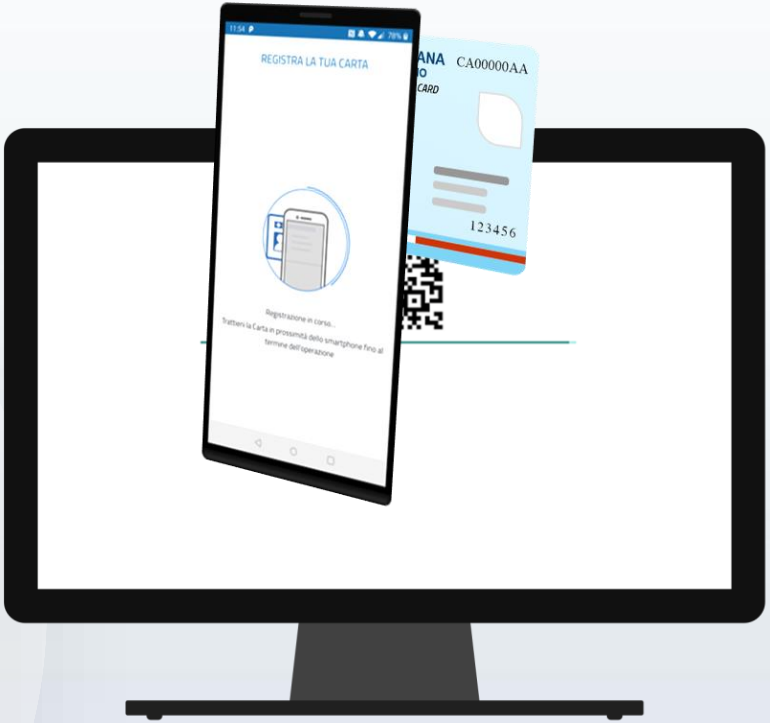
Online authentication

One-shot hybrid solution – Authentication



Online authentication

One-shot hybrid solution – Authentication

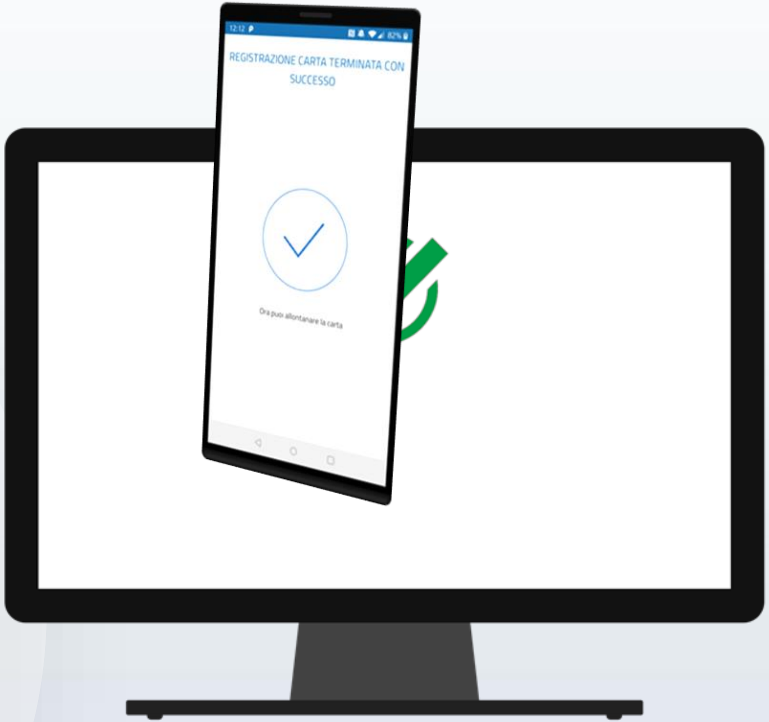


REGISTRA LA TUA CARTA

Registrazione in corso...
Trattieni la Carta in prossimità dello smartphone fino al termine dell'operazione

Online authentication

One-shot hybrid solution – Authentication



REGISTRAZIONE CARTA TERMINATA CON SUCCESSO

Ora puoi allontanare la carta

Online authentication

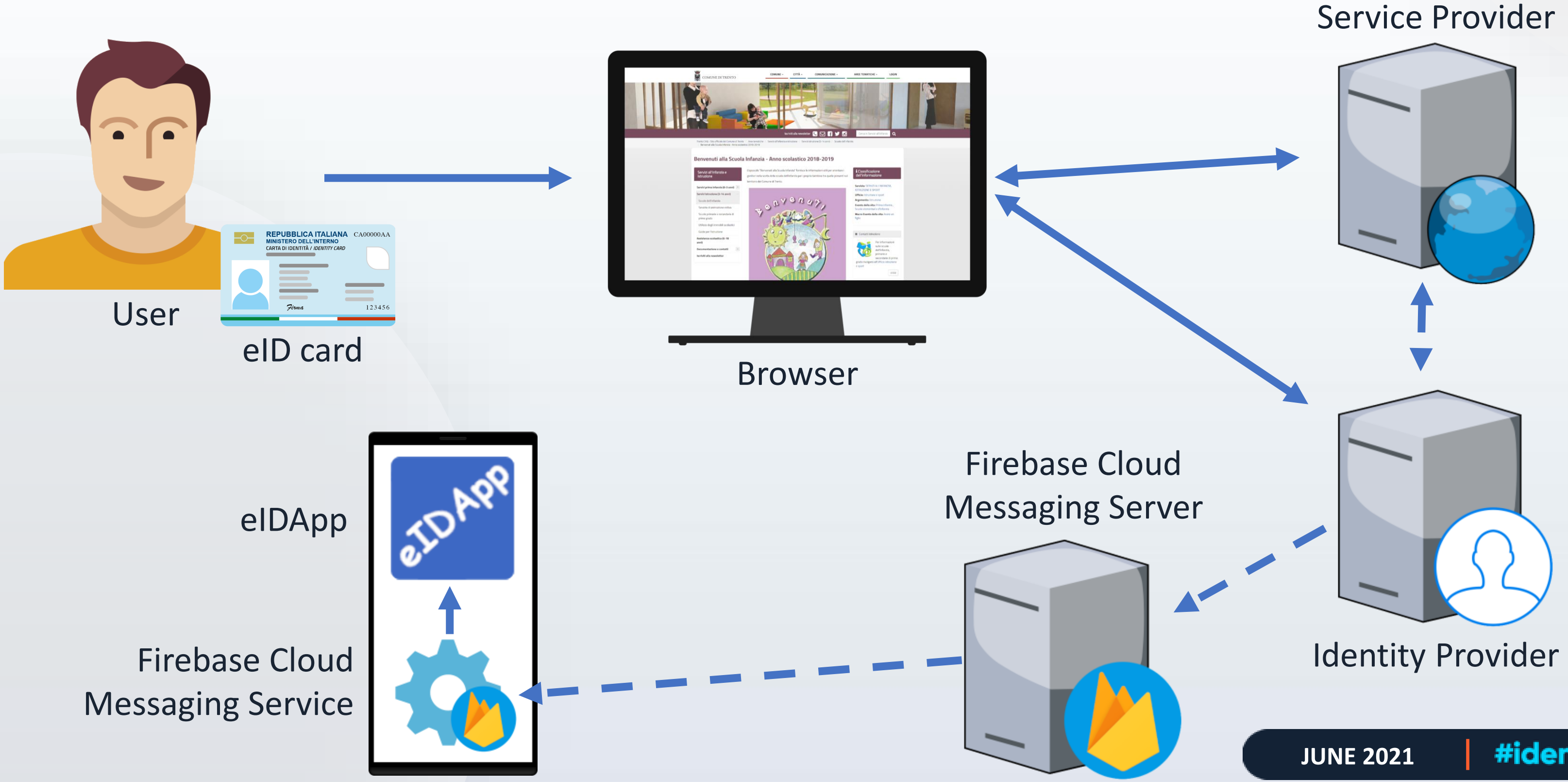
Hybrid solutions

Given the different requirements that may arise, we consider two hybrid solutions:

- a **one-shot solution** that can be used without any prior operation (except for card registration), relying on QR codes;
- a **two-phase solution** requiring a preliminary operation (enrollment), relying on QR codes and push notifications.

Online authentication

Two-phase hybrid solution – Involved entities


REPUBBLICA ITALIANA
CA00000AA
MINISTERO DELL'INTERNO
CARTA DI IDENTITÀ / IDENTITY CARD
Firma
123456
Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019
eIDApp

User

eID card

Browser

Service Provider

Identity Provider

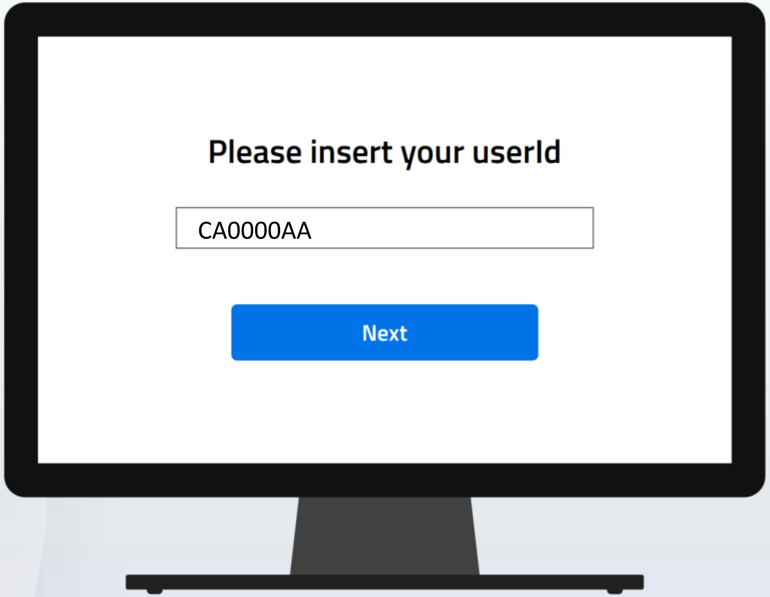
Firebase Cloud Messaging Server

eIDApp

Firebase Cloud Messaging Service

Online authentication

Two-phase hybrid solution – Enrollment



Please insert your userId

CA0000AA

Online authentication

Two-phase hybrid solution – Enrollment

Online authentication

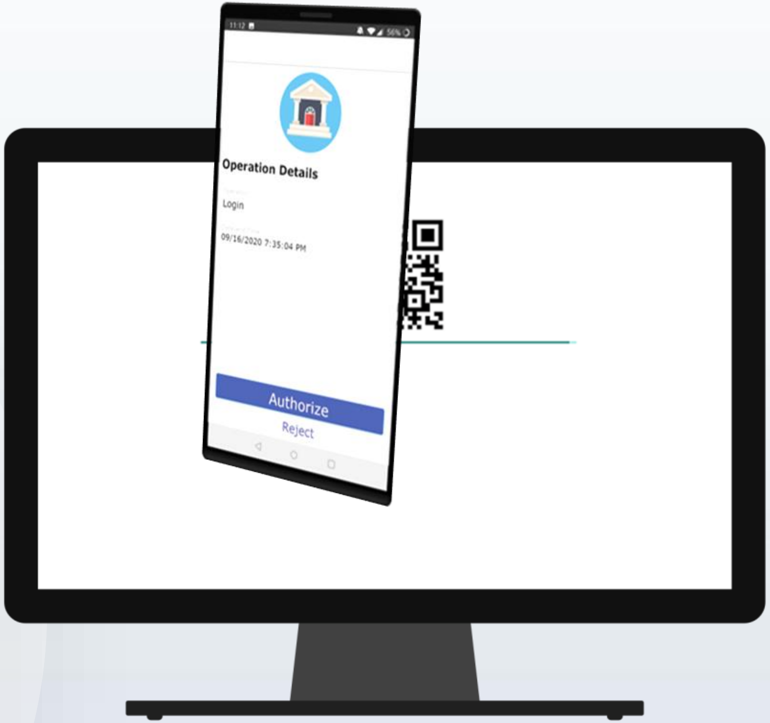
Two-phase hybrid solution – Enrollment

12:21
83%
Scansiona il QR code

Apri la app e scannerizza il seguente QR code

Online authentication

Two-phase hybrid solution – Enrollment



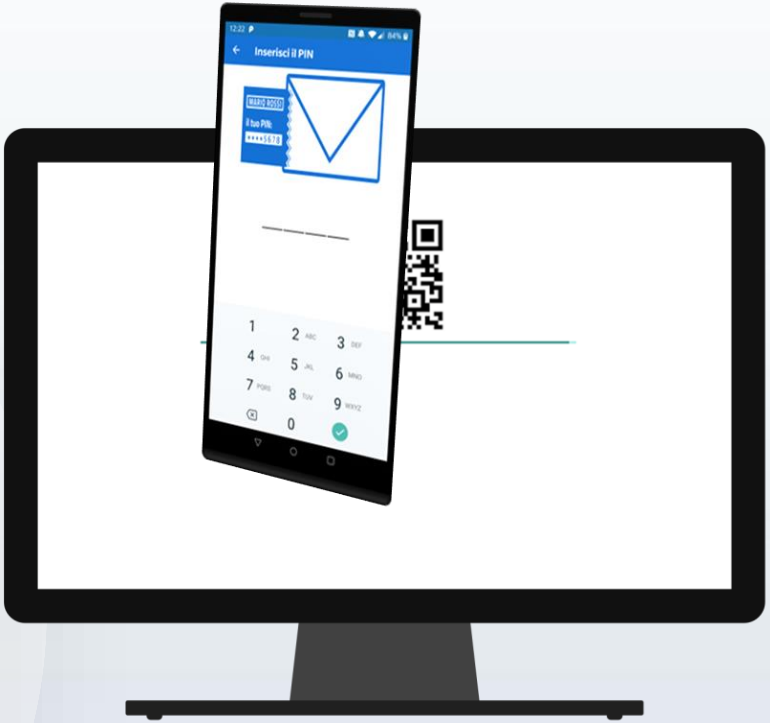
Operation Details

Login

09/16/2020 7:35:04 PM

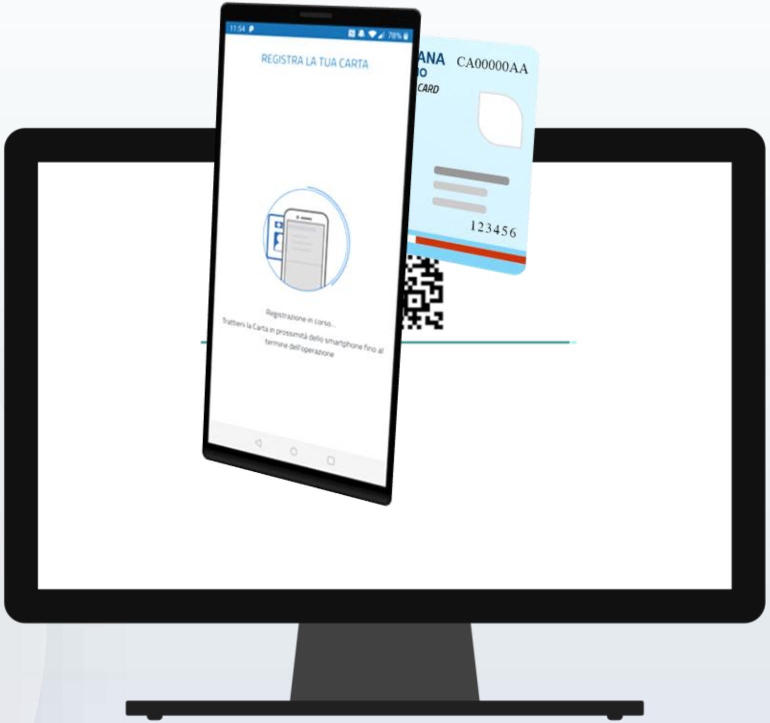
Online authentication

Two-phase hybrid solution – Enrollment



Online authentication

Two-phase hybrid solution – Enrollment



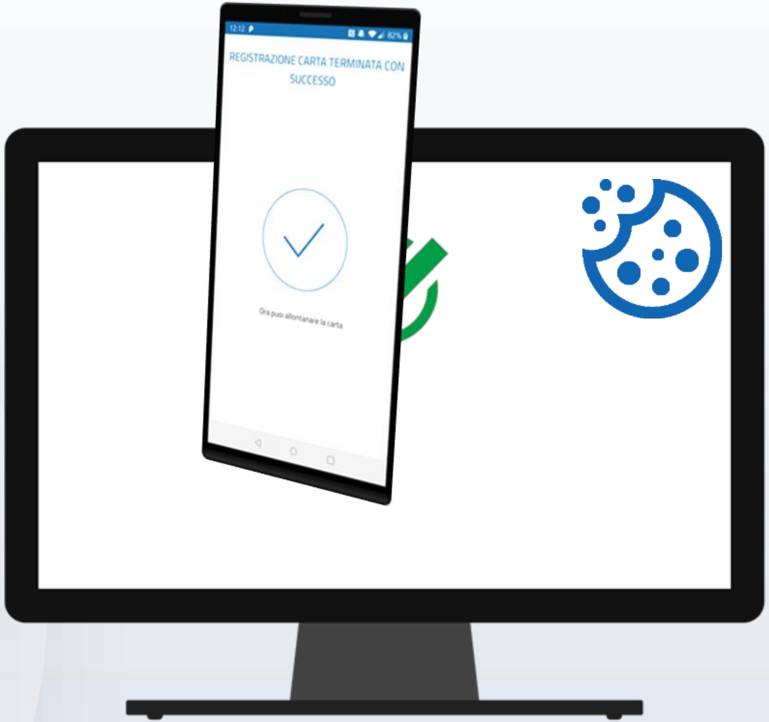
REGISTRA LA TUA CARTA

Registrazione in corso...

Trattieni la Carta in prossimità dello smartphone fino al termine dell'operazione

Online authentication

Two-phase hybrid solution – Enrollment

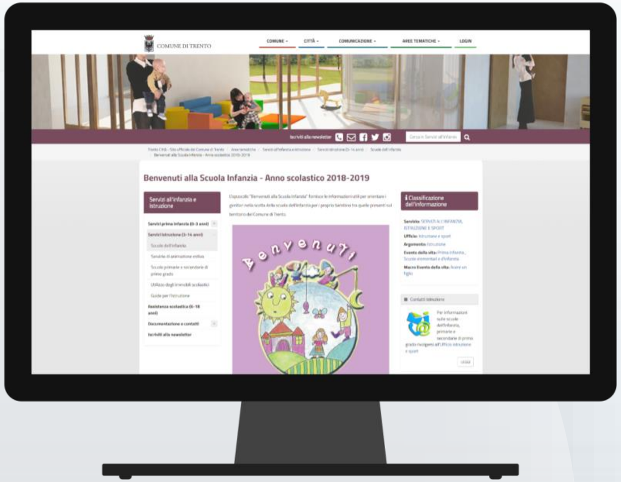


REGISTRAZIONE CARTA TERMINATA CON SUCCESSO

Ora puoi allontanare la carta

Online authentication

Two-phase hybrid solution – Authentication



COMUNE DI TRENTO

Trento Città - Sito ufficiale del Comune di Trento / Aree tematiche / Servizi all'infanzia e istruzione / Servizi istruzione (3-14 anni) / Scuole dell'infanzia / Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019

Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019

Servizi all'infanzia e istruzione

- Servizi prima infanzia (0-3 anni)
- Servizi istruzione (3-14 anni)
- Scuole dell'infanzia
- Servizio di animazione estiva
- Scuole primarie e secondarie di primo grado
- Utilizzo degli immobili scolastici
- Guide per l'istruzione
- Assistenza scolastica (6-18 anni)
- Documentazione e contatti
- Iscriviti alla newsletter

L'opuscolo "Benvenuti alla Scuola Infanzia" fornisce le informazioni utili per orientare i genitori nella scelta della scuola dell'infanzia per i propri bambini tra quelle presenti sul territorio del Comune di Trento.

Classificazione dell'informazione

Servizio: SERVIZI ALL'INFANZIA, ISTRUZIONE E SPORT

Ufficio: Istruzione e sport

Argomento: Istruzione

Evento della vita: Prima infanzia, Scuole elementari e d'infanzia

Macro Evento della vita: Avere un figlio

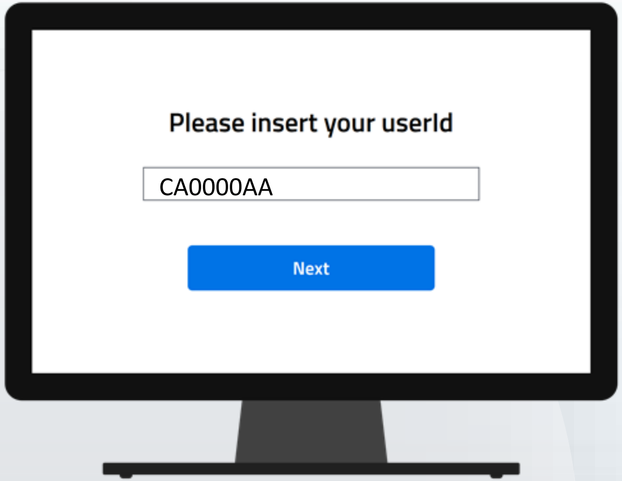
Contatti Istruzione

Per informazioni sulle scuole dell'infanzia, primarie e secondarie di primo grado rivolgersi all'Ufficio istruzione e sport

LEGGI

Online authentication

Two-phase hybrid solution – Authentication

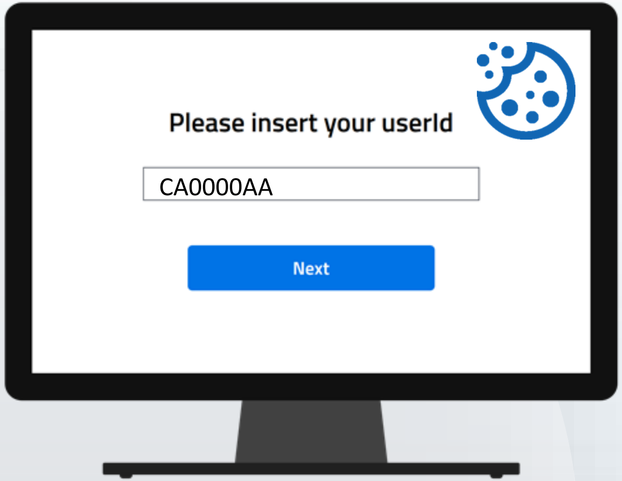


Please insert your userId

CA0000AA

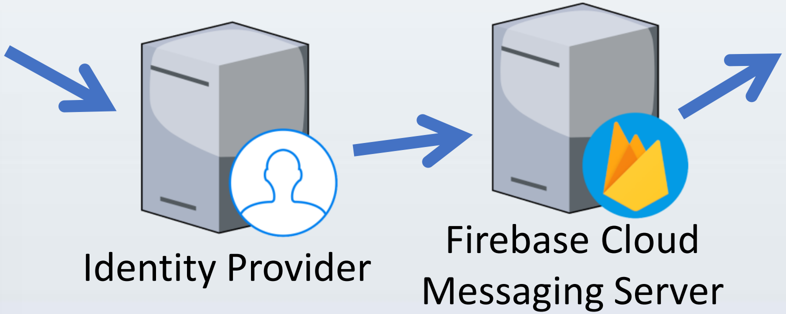
Online authentication

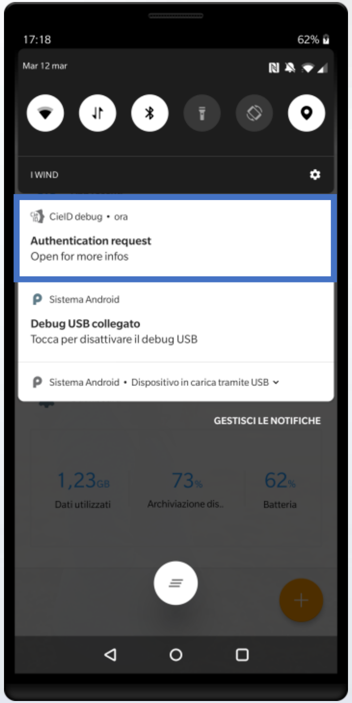
Two-phase hybrid solution – Authentication



Please insert your userId

CA0000AA





CieID debug • ora

Authentication request

Open for more infos

Sistema Android

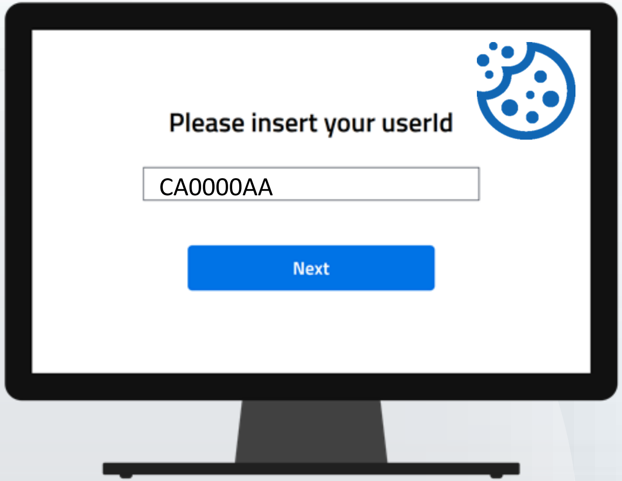
Debug USB collegato

Tocca per disattivare il debug USB

Sistema Android • Dispositivo in carica tramite USB

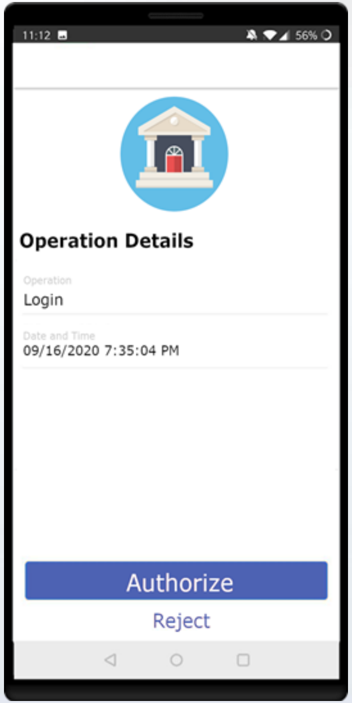
Online authentication

Two-phase hybrid solution – Authentication



Please insert your userId

CA0000AA



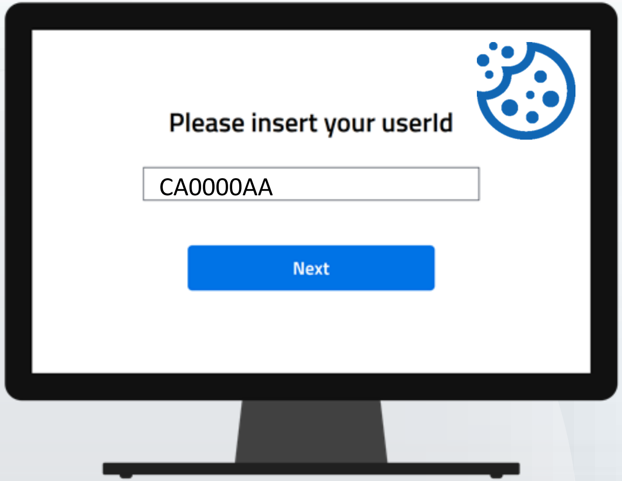
Operation Details

Operation
Login

Date and Time
09/16/2020 7:35:04 PM

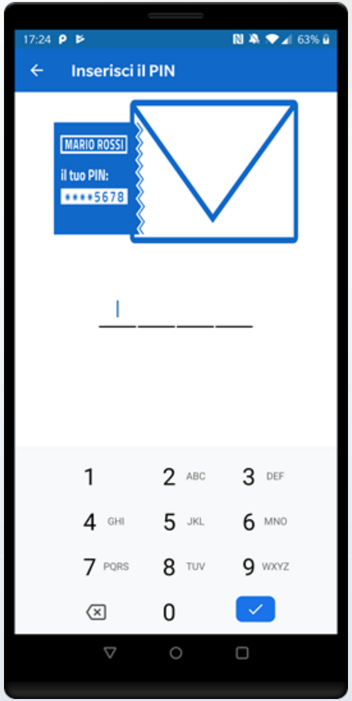
Online authentication

Two-phase hybrid solution – Authentication



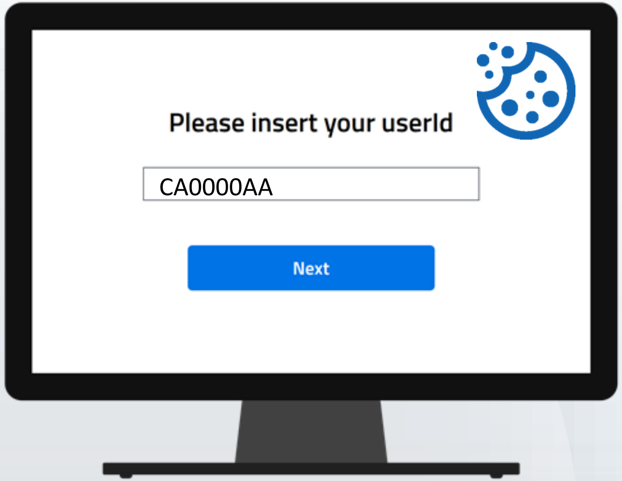
Please insert your userId

CA0000AA



Online authentication

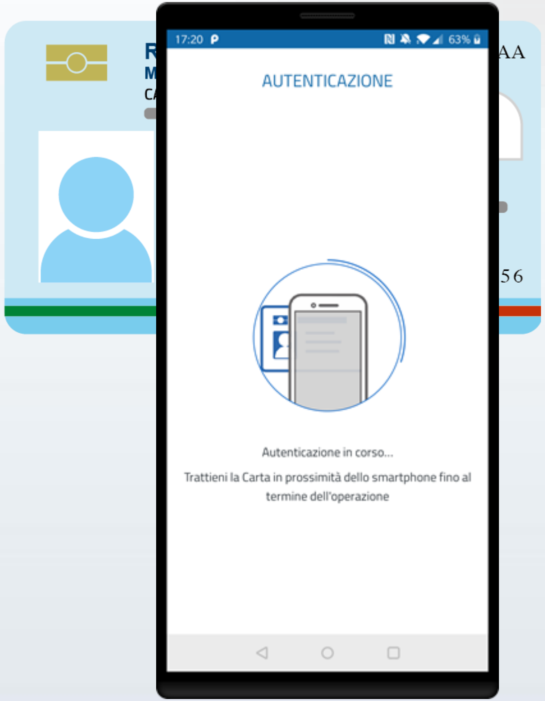
Two-phase hybrid solution – Authentication



Please insert your userId

CA0000AA

Next



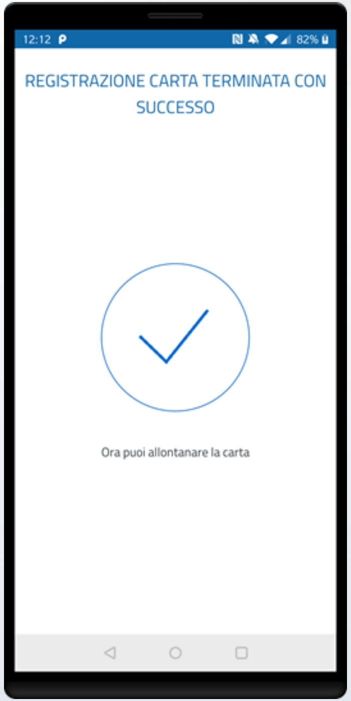
AUTENTICAZIONE

Autenticazione in corso...

Trattieni la Carta in prossimità dello smartphone fino al termine dell'operazione

Online authentication

Two-phase hybrid solution – Authentication



12:12

REGISTRAZIONE CARTA TERMINATA CON SUCCESSO

Ora puoi allontanare la carta

3

What about security?

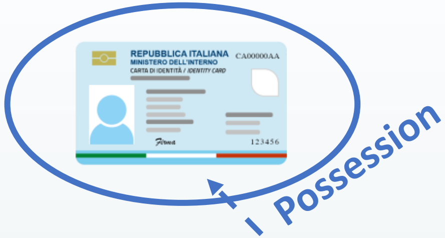
A methodology to analyse protocols based on eID cards

eID cards from a security perspective

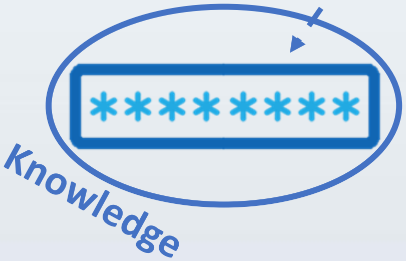
Multi-Factor Cryptographic Device: «a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor»

Source: NIST Special Publication 800-63b

eID cards from a security perspective

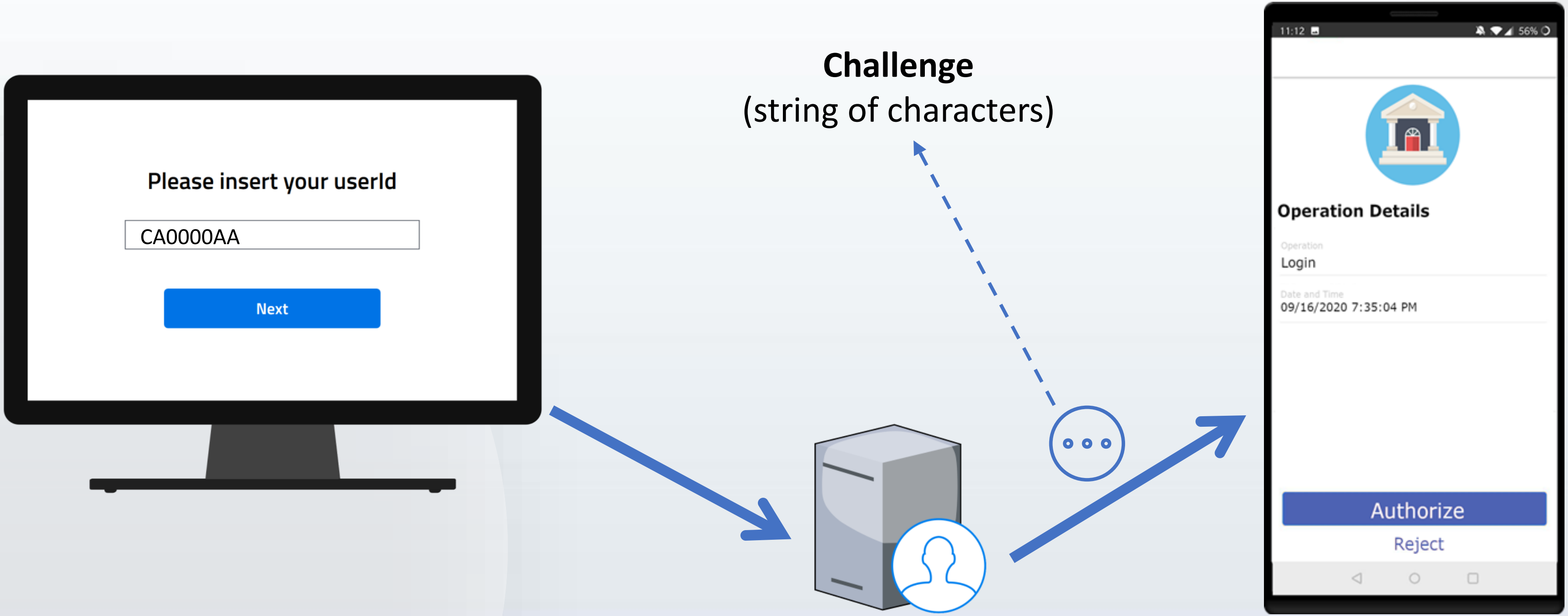


Multi-Factor Cryptographic Device: «a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor»



Source: NIST Special Publication 800-63b

Challenge-response protocols



Please insert your userId

CA0000AA

Challenge
(string of characters)

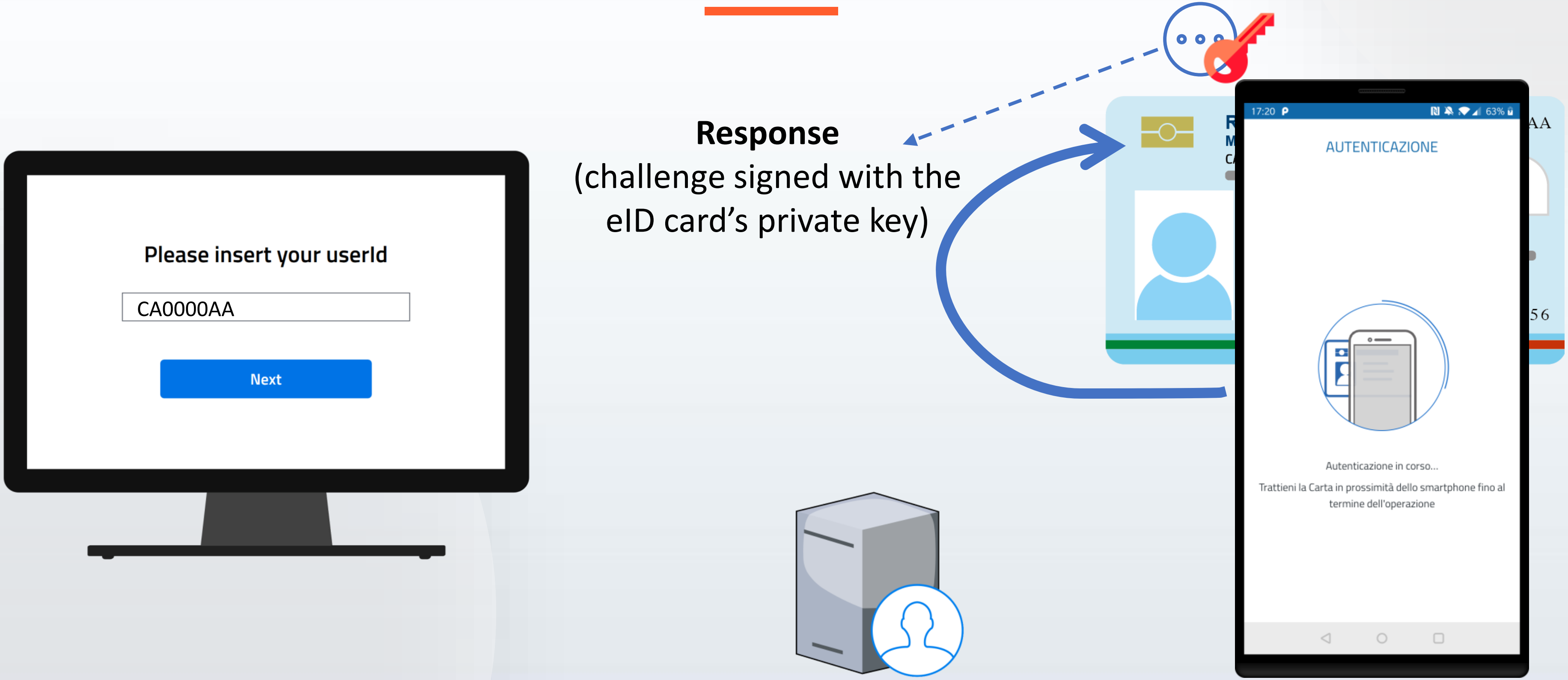
Identity Provider

Operation Details

Operation
Login

Date and Time
09/16/2020 7:35:04 PM

Challenge-response protocols



Please insert your userId

CA0000AA

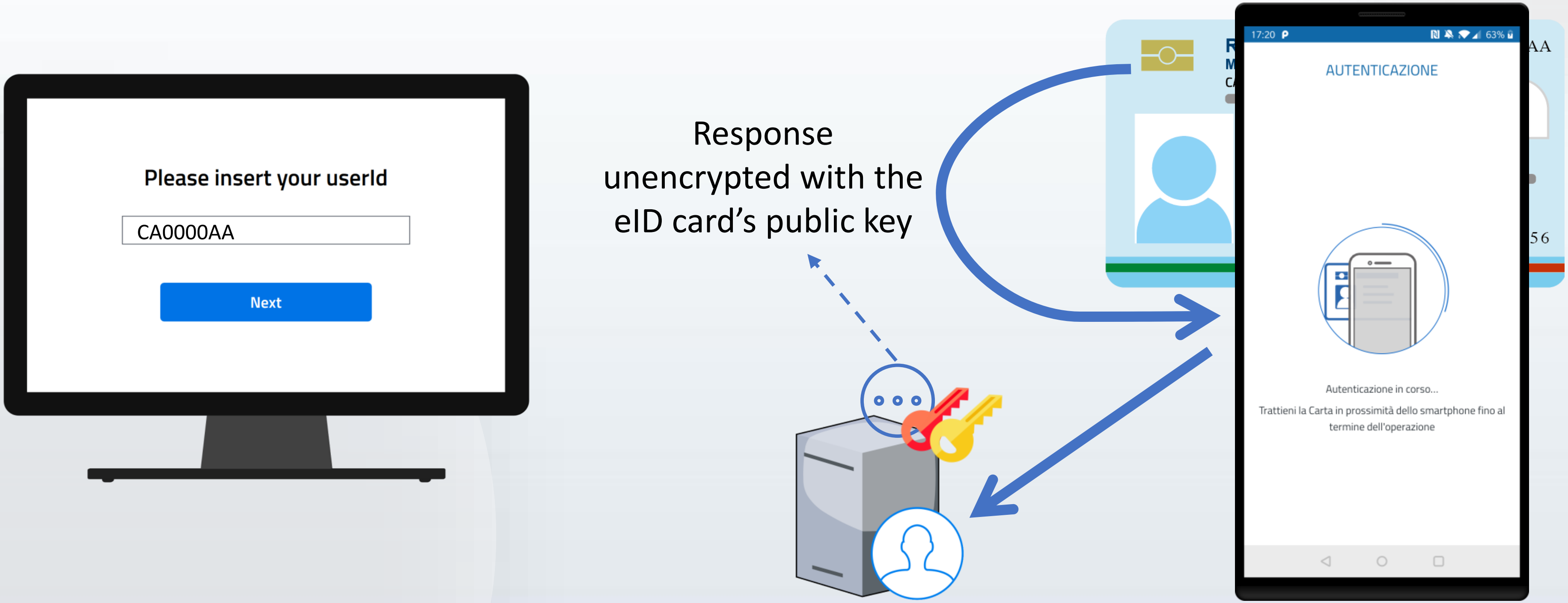
Response
(challenge signed with the eID card's private key)

Autenticazione in corso...

Trattieni la Carta in prossimità dello smartphone fino al termine dell'operazione

Identity Provider

Challenge-response protocols



Please insert your userId

CA0000AA

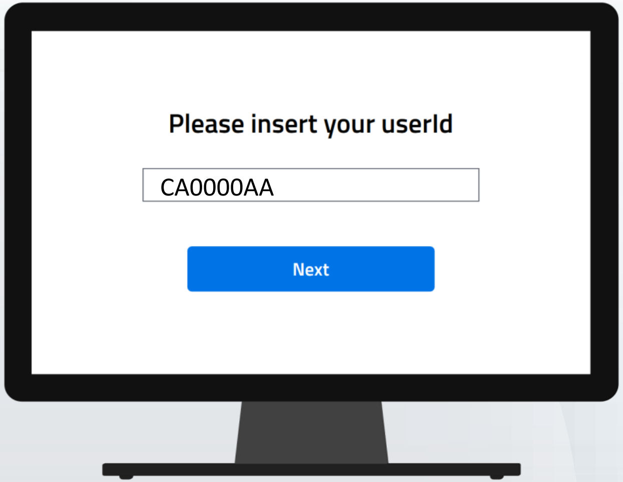
Response unencrypted with the eID card’s public key

Identity Provider

Autenticazione in corso...

Trattieni la Carta in prossimità dello smartphone fino al termine dell'operazione

Challenge-response protocols

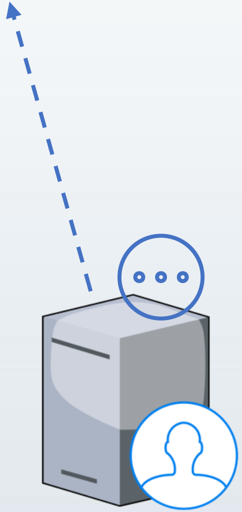


Please insert your userId

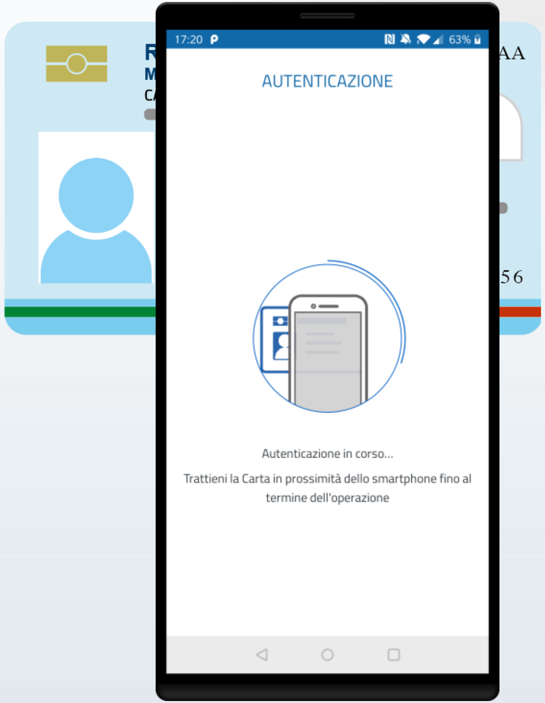
CA0000AA

Next

Checks on the values



Identity Provider



17:20 63%

AUTENTICAZIONE

Autenticazione in corso...

Trattieni la Carta in prossimità dello smartphone fino al termine dell'operazione

Protocol analysis

A two-level approach

1

Security Analysis

To detect the attackers that manage to compromise the protocol

Protocol analysis

Security analysis

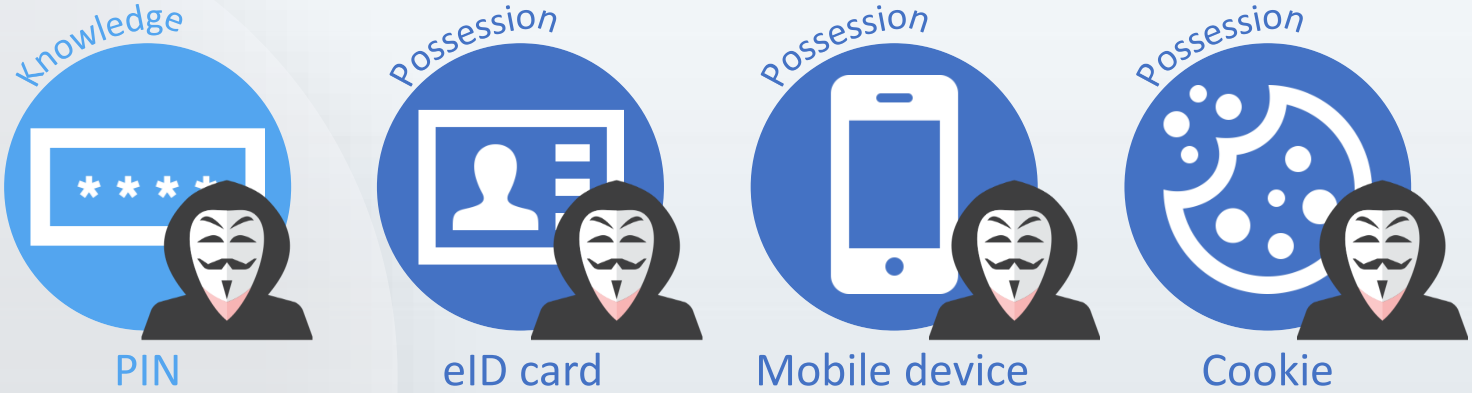
To detect the attackers that manage to compromise the protocol, we perform two different kinds of analysis:

1. **Combinatorial Analysis**: relying on attackers' capabilities on the authentication factors. It is fast and thus helps prune the set of attackers to test, but may not detect some advanced attacks.

Protocol analysis

Security analysis – Combinatorial analysis

Explicit attackers: manage to break the protocol by compromising all the authentication factors.



Protocol analysis

Security analysis – Combinatorial analysis

Attackers		Authentication Factors Compromised			
		****	🪪	📱	🍪
Personal Computer Thief	PCT	🔒	🔒	🔒	🔓
Mobile Device Thief	MDT	🔒	🔒	🔓	🔒
Card Thief	CT	🔒	🔓	🔒	🔒
Authenticator Duplicator	AD	🔓	🔒	🔒	🔓
Eavesdropping Software	ES	🔓	🔒	🔒	🔒
Shoulder Surfer	SS	🔓	🔒	🔒	🔒
Social Engineer	SE	🔓	🔒	🔒	🔒
Man in the Browser	MB	🔒	🔒	🔒	🔓
Man in the Mobile	MM	🔓	🔓	🔓	🔒

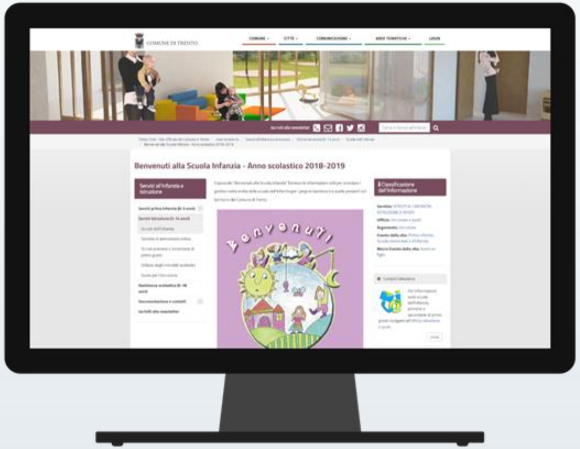
Protocol analysis

Security analysis

To detect the attackers that manage to compromise the protocol, we perform two different kinds of analysis:

1. Combinatorial **Analysis**: relying on attackers' capabilities on the authentication factors. It is fast and thus helps prune the set of attackers to test, but may not detect some advanced attacks.

2. Formal **Analysis**: relying on formal methods (a specification language and a model checker). It can be computationally expensive, but manages to find even more complex categories of attacks.



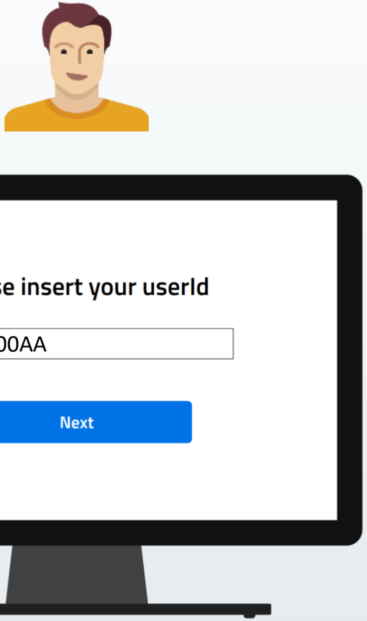
COMUNE DI TRENTO

COMUNE ▾ CITTÀ ▾ COMUNICAZIONE ▾ AREE TEMATICHE ▾ LOGIN

Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019

Servizi all'infanzia e istruzione

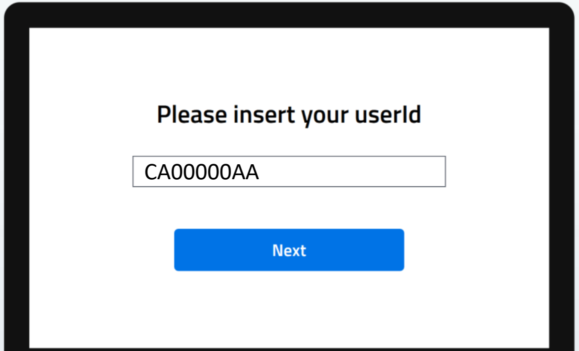
Classificazione dell'informazione



Please insert your userId

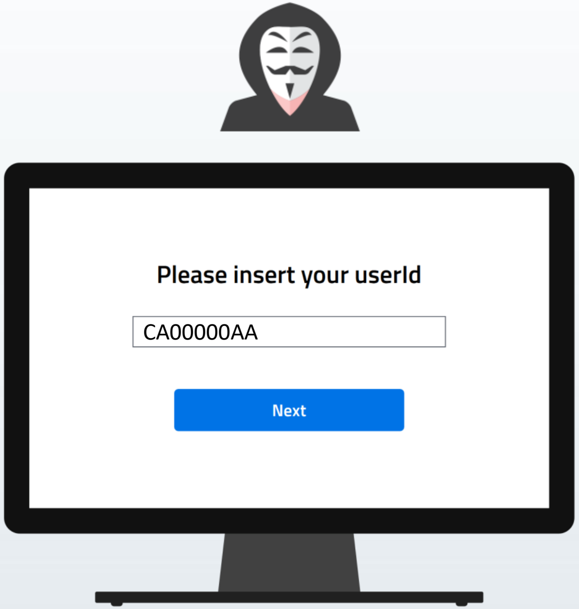
CA00000AA

Benvenuti alla Scuola Infanzia - Anno scolastico 2018-2019



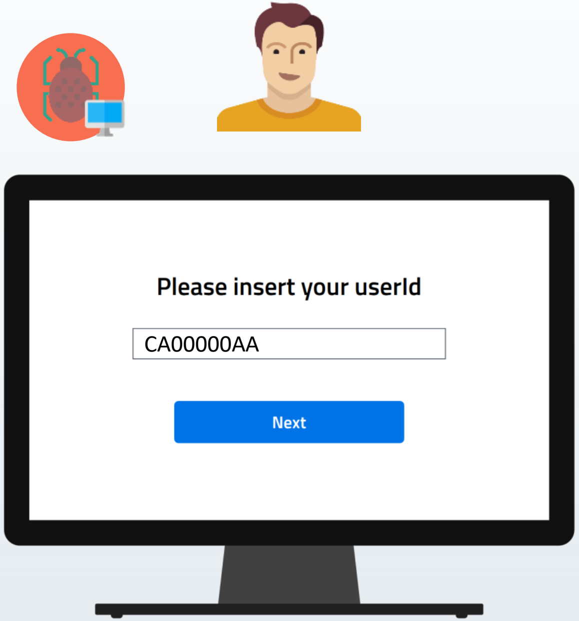
Please insert your userId

CA00000AA



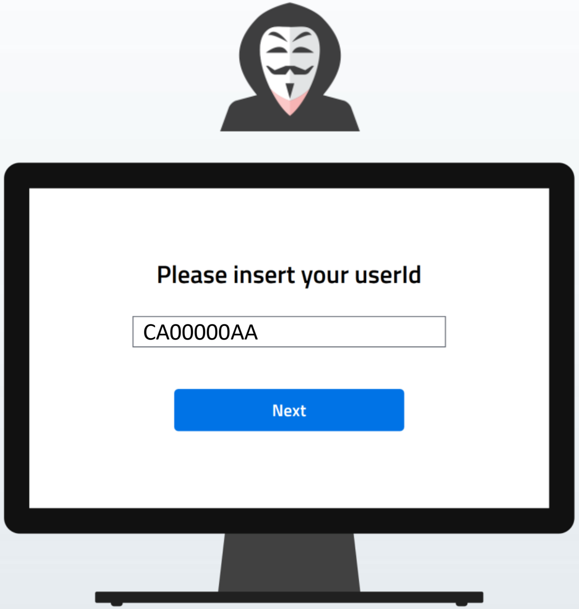
Please insert your userId

CA00000AA



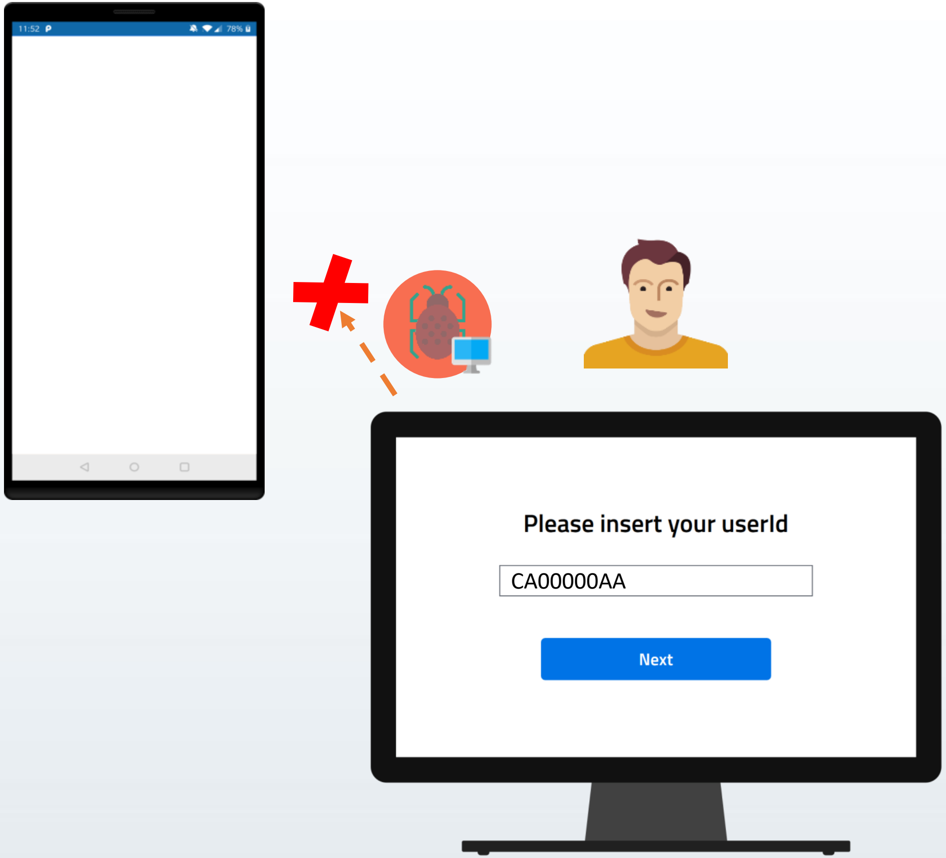
Please insert your userId

CA00000AA



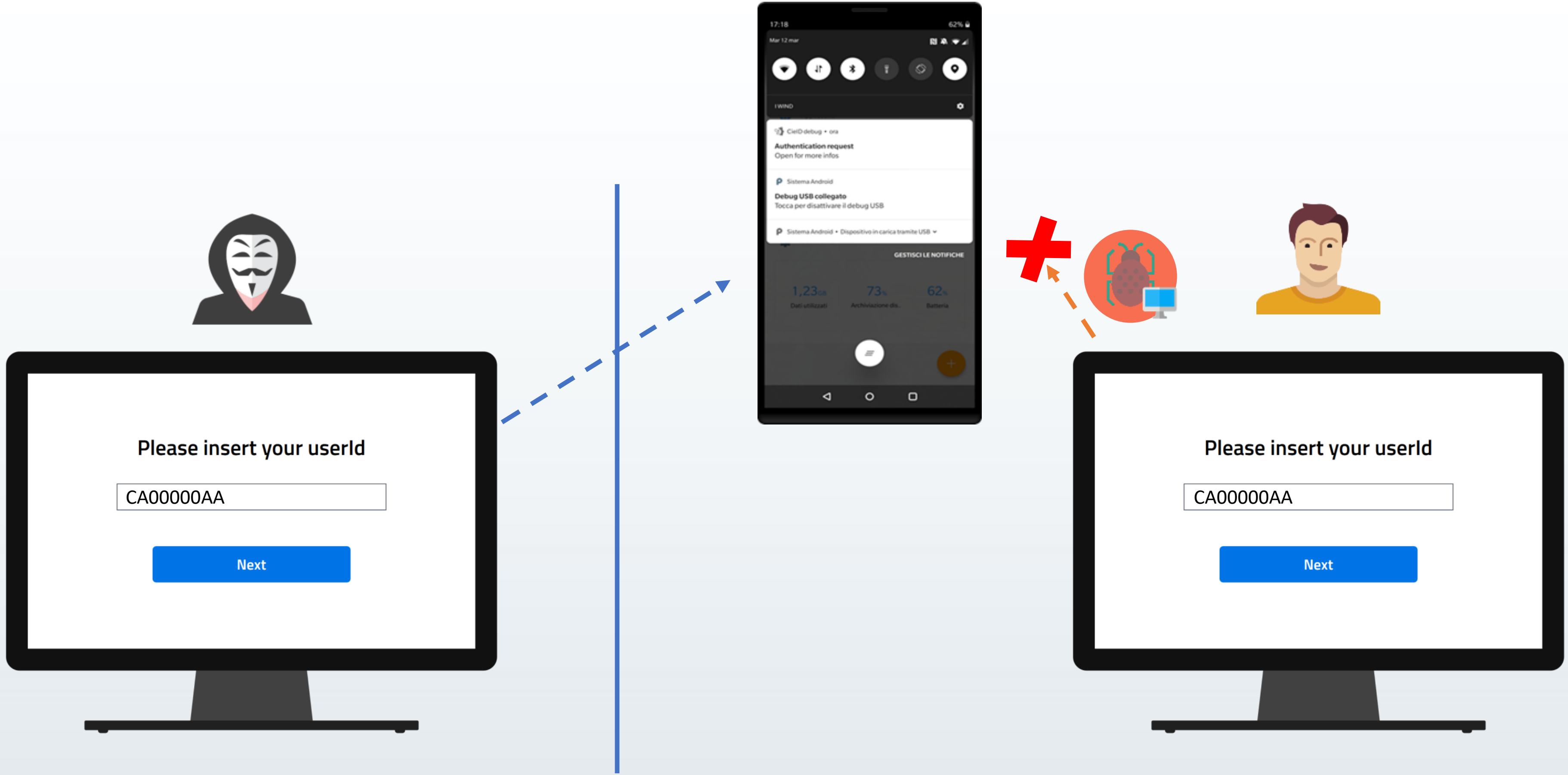
Please insert your userId

CA00000AA



Please insert your userId

CA00000AA



Please insert your userId

CA00000AA

Next

CieID debug • ora

Authentication request

Open for more infos

Sistema Android

Debug USB collegato

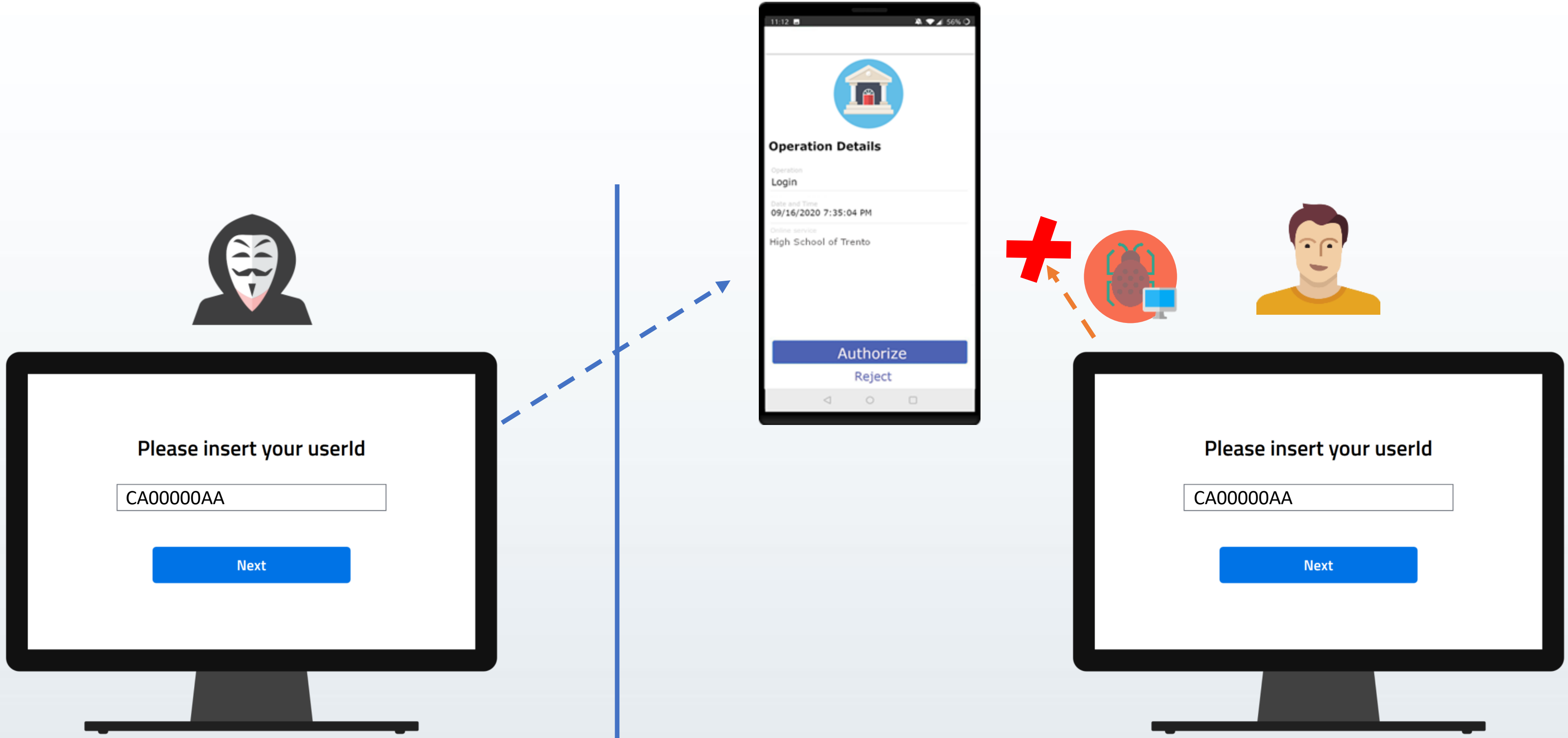
Tocca per disattivare il debug USB

Sistema Android • Dispositivo in carica tramite USB

Please insert your userId

CA00000AA

Next



Please insert your userId

CA00000AA

Operation Details

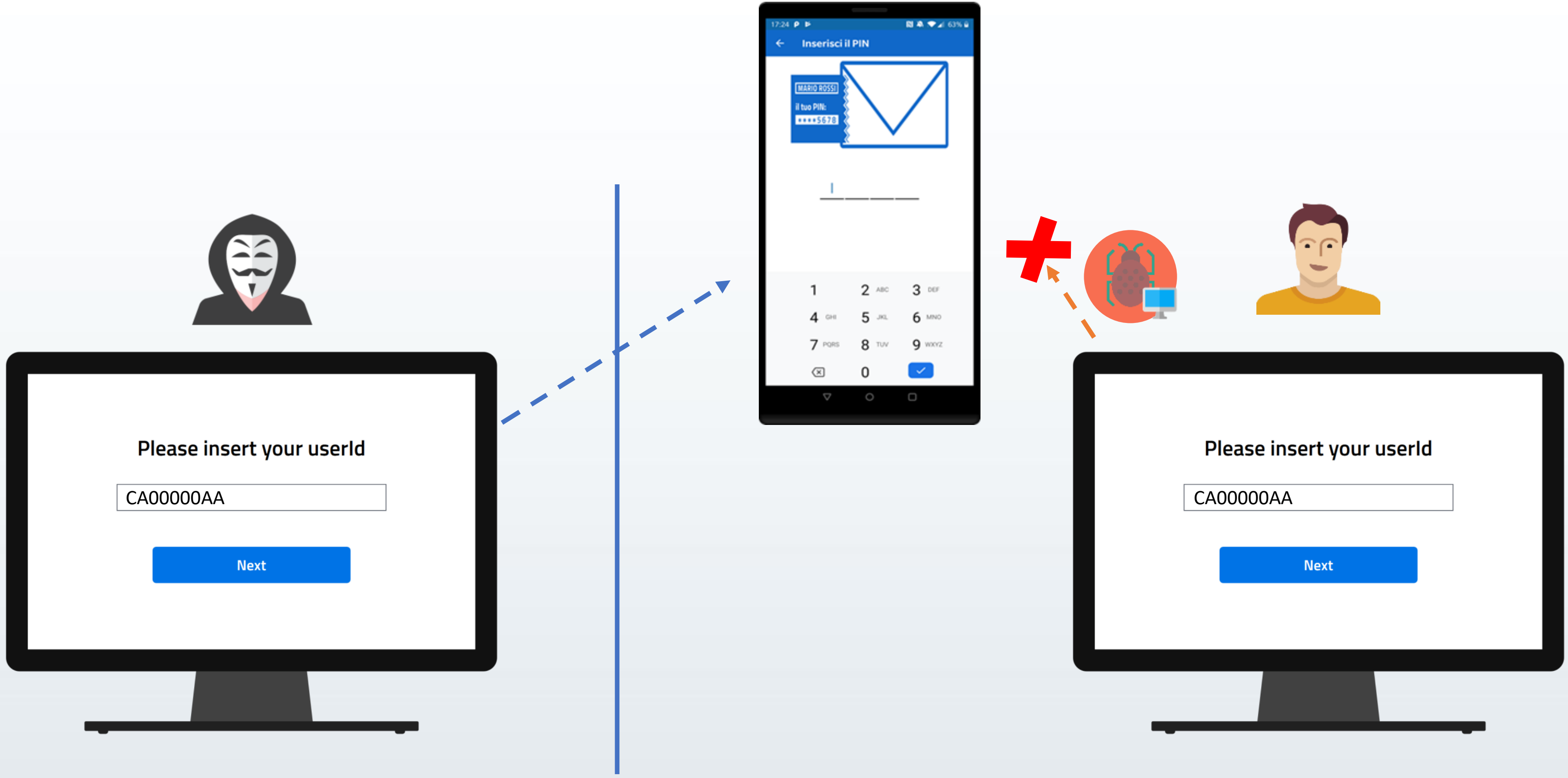
Operation
Login

Date and Time
09/16/2020 7:35:04 PM

Online service
High School of Trento

Please insert your userId

CA00000AA



Please insert your userId

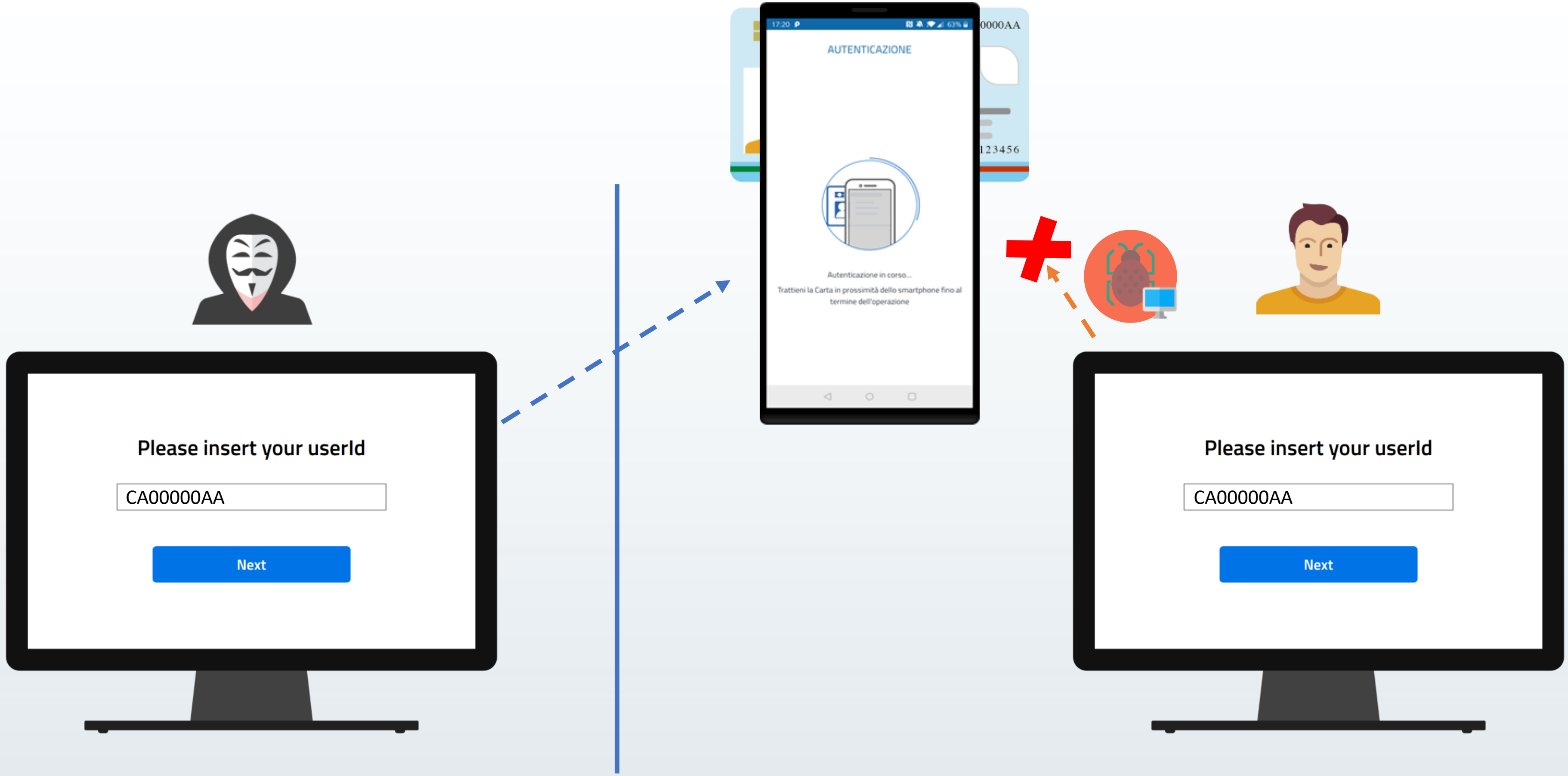
CA00000AA

Next

Please insert your userId

CA00000AA

Next



AUTENTICAZIONE

Autenticazione in corso...

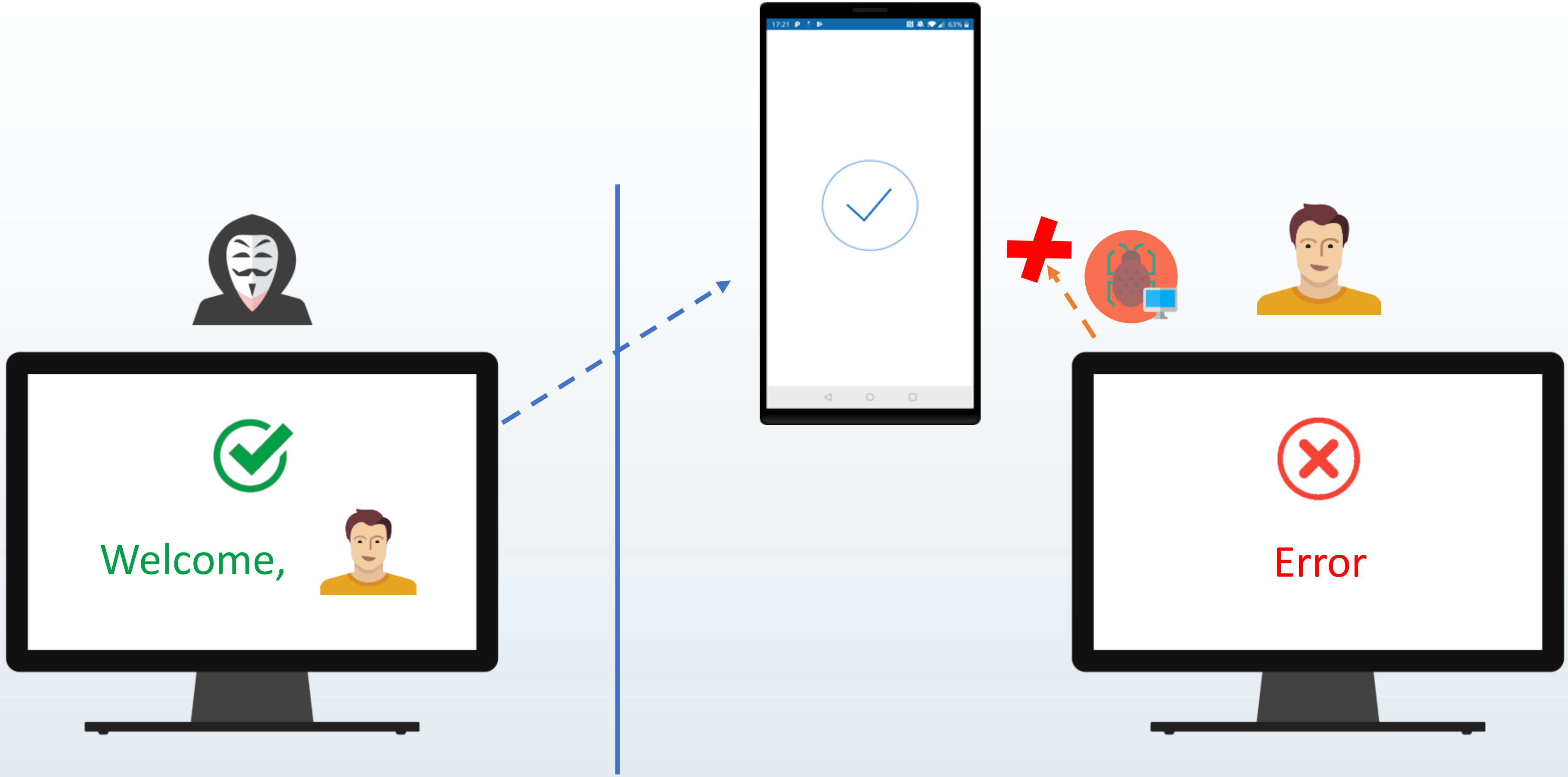
Trattieni la Carta in prossimità dello smartphone fino al termine dell'operazione

Please insert your userId

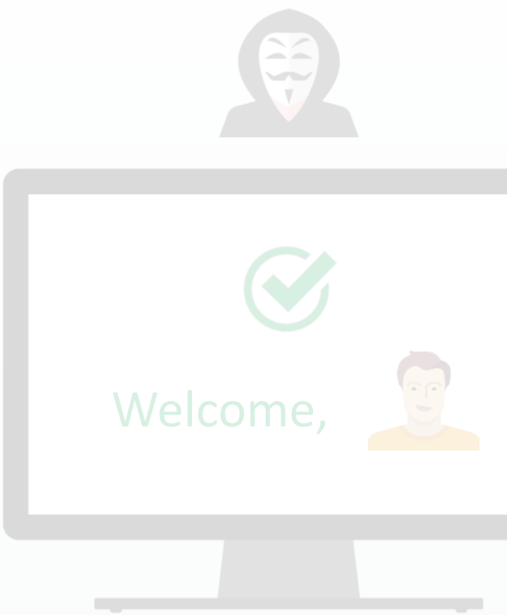
CA00000AA

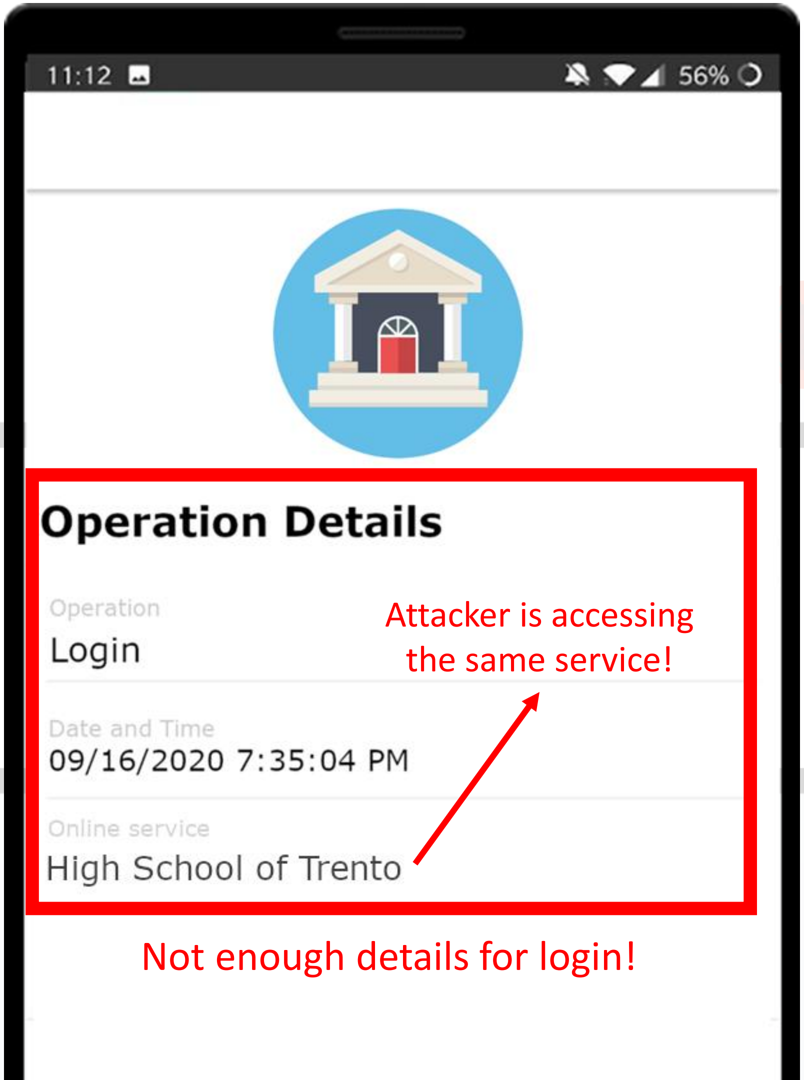
Please insert your userId

CA00000AA



Welcome,
17:21
63%
Error





Operation Details

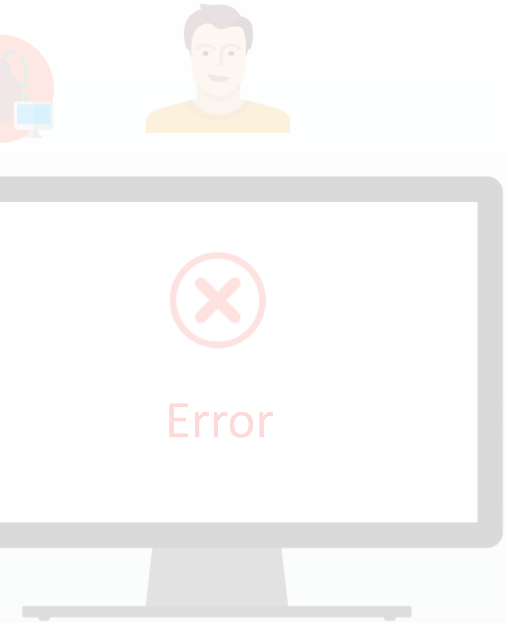
Operation
Login

Date and Time
09/16/2020 7:35:04 PM

Online service
High School of Trento

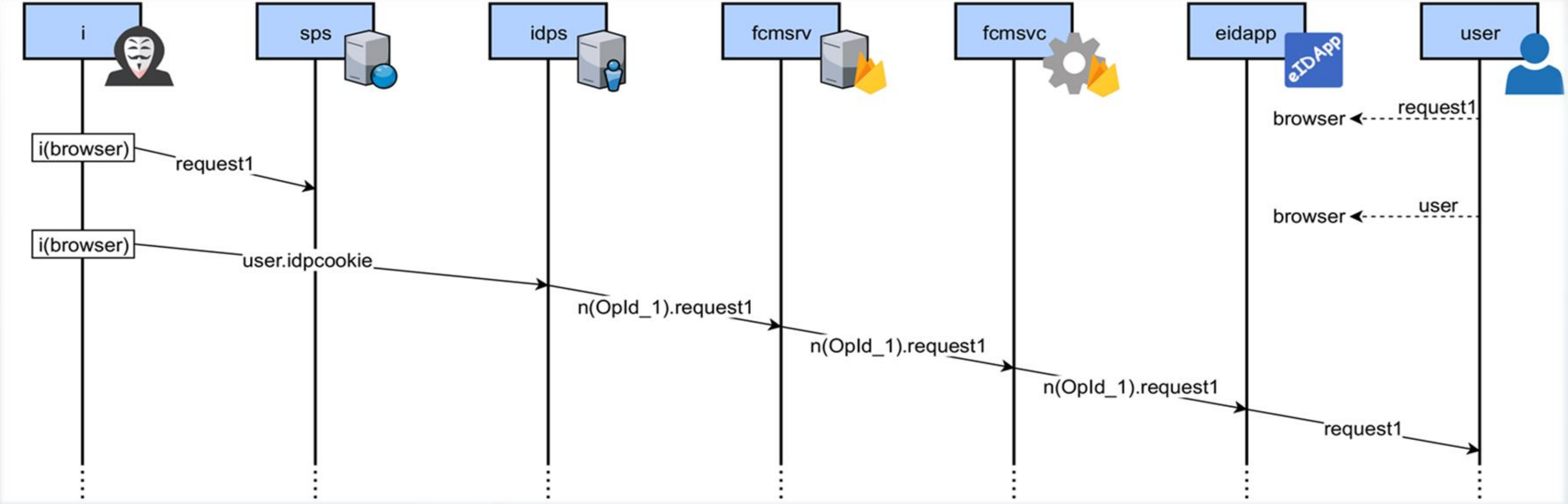
Attacker is accessing the same service!

Not enough details for login!



Protocol analysis

Security analysis – Formal analysis



Protocol analysis

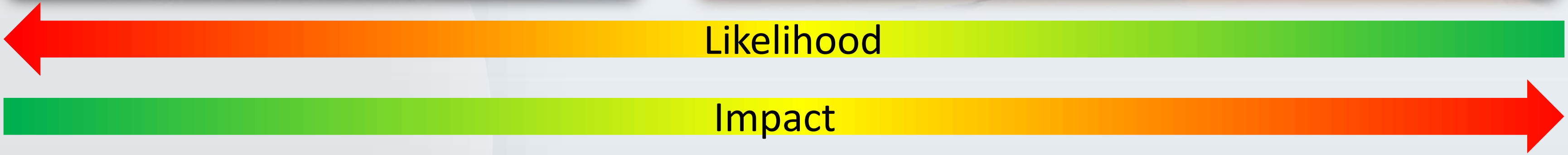
A two-level approach

1 **Security Analysis**
To detect the attackers that manage to compromise the protocol

2 **Risk Analysis**
To evaluate the risks connected with the successful attackers detected

Protocol analysis

Risk analysis



Risk = Likelihood × Impact

Likelihood → Probability of an attack happening

Impact → Consequences in case of the attack was successful

Protocol analysis

Risk analysis

OWASP Risk Rating Methodology

		Likelihood		
		Low	*Medium*	*High*
Impact	*Low*	Note	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

Risk = Likelihood × Impact

Probability of an attack happening

Consequences in case of the attack was successful

Protocol analysis

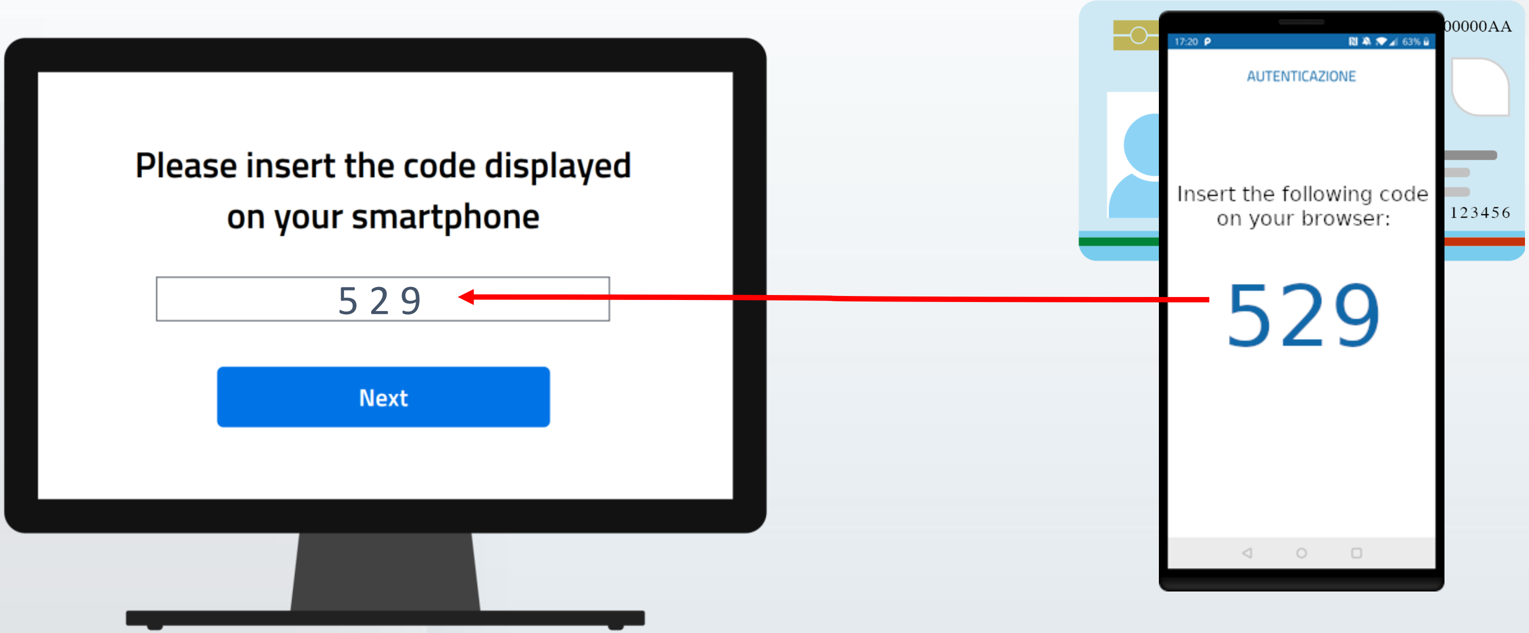
Final results

At the end of the analysis, we can know:

- a **list of attackers** that manage to compromise the protocol;
- an indication of the **risk** for each attacker.

Mitigations

Example: OTP on the mobile application



Please insert the code displayed on your smartphone

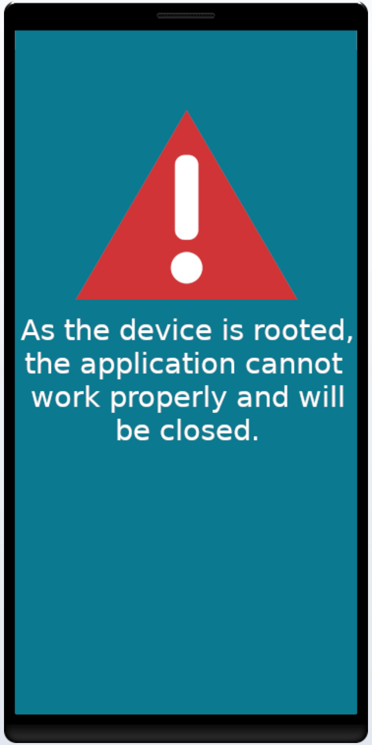
5 2 9

Insert the following code on your browser:

529

Mitigations

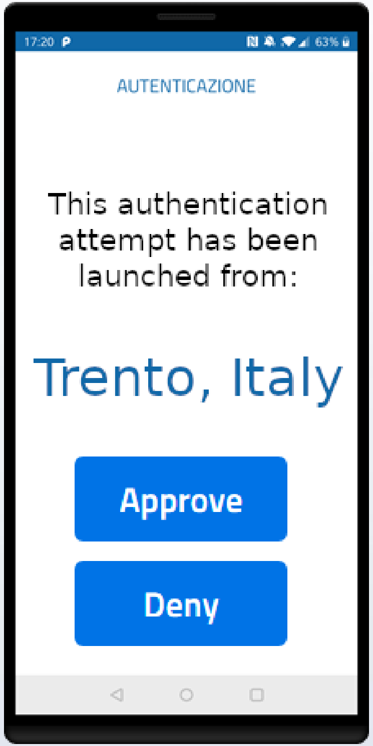
Example: Root detector



As the device is rooted, the application cannot work properly and will be closed.

Mitigations

Example: Additional login information



17:20 63%

AUTENTICAZIONE

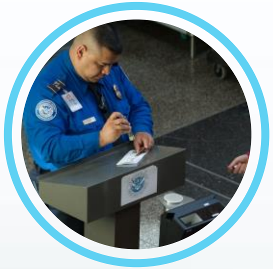
This authentication attempt has been launched from:

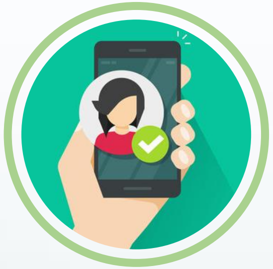
Trento, Italy

4

Conclusions

Conclusions





BELGIË BELGIQUE BELGIEN BELGIUM
IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD
HUNGARY
IDENTITY CARD
PORTUGAL
CARTÃO DE CIDADÃO CITIZEN CARD
KONINKRIJK DER NEDERLANDEN
NEDERLANDSE IDENTITEITSKAART
Rzeczpospolita Polska Republic of Poland
Dowód osobisty Identity card
BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
REPUBBLICA ITALIANA
MINISTERO DELL'INTERNO
CARTA DI IDENTITÀ / IDENTITY CARD

References

- Marco Pernpruner, Roberto Carbone, Silvio Ranise, and Giada Sciarretta. “The Good, the Bad and the (Not So) Ugly of Out-of-Band Authentication with eID Cards and Push Notifications: Design, Formal and Risk Analysis”. In: *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy* (CODASPY '20). https://doi.org/10.1145/3374664.3375727

- Marco Pernpruner, Giada Sciarretta, and Silvio Ranise. “A Framework for Security and Risk Analysis of Enrollment Procedures: Application to Fully-remote Solutions based on eDocuments”. In: *Proceedings of the 18th International Conference on Security and Cryptography* (SECRYPT 2021). In press.

- Matteo Leonelli, Umberto Morelli, Giada Sciarretta, and Silvio Ranise. “Secure Pull Printing with QR Codes and National eID Cards: A Software-oriented Design and an Open-source Implementation”. In: *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy* (CODASPY '21). https://doi.org/10.1145/3422337.3447847

- OWASP. “OWASP Risk Rating Methodology”. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Thank You!

For more information:

Marco Pernpruner
mpernpruner@fbk.eu
https://st.fbk.eu