FONDAZIONE BRUNO KESSLER
CENTER FOR CYBERSECURITY

Applications based on CIE 3.0

From the design to the security assessment

12 January 2022 - Seminari De Cifris Athesis

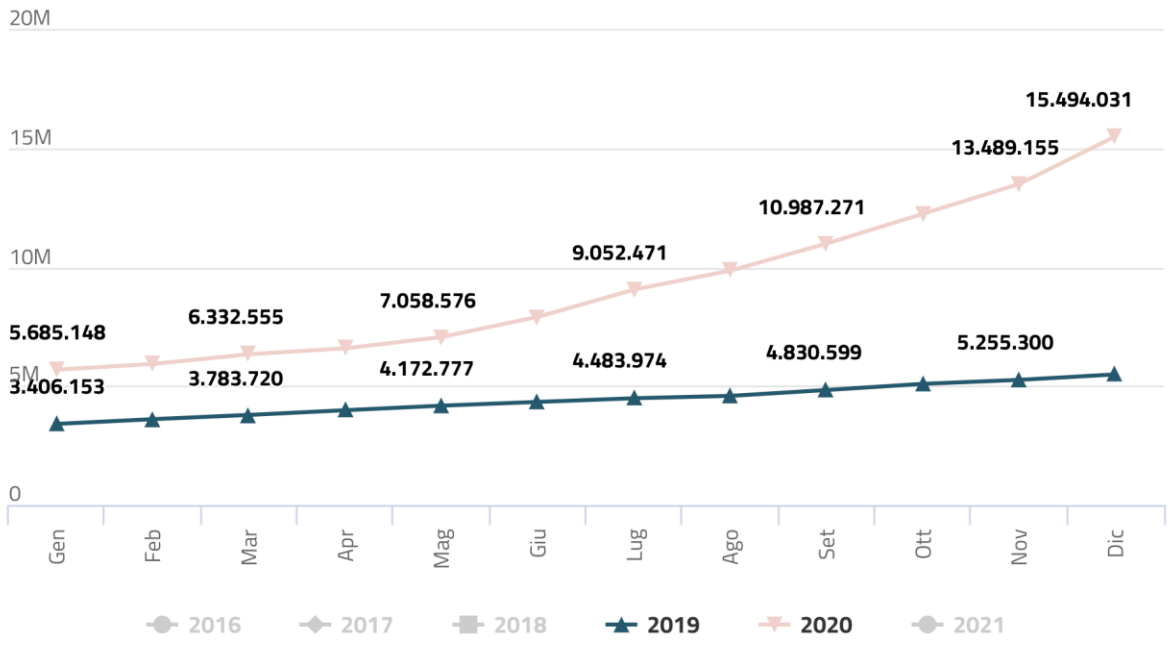
Giada Sciarretta

SECURITY & TRUST

Digital Identity
...especially nowadays

spid

20.269.399
05/05/2021



Andamento mensile delle identità SPID erogate (numero aggregato, totale dei gestori)

Digital Report 2021

Social networks

More than **2 million new users**

Internet

We are connected for **over 6 hours a day**
Over **1 million new users**

E-commerce

Spent **24% more than in 2019**

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

Digital Identity
Clusit Report 2021

INTESA SANPAOLO

La password de la sua carta Flash e stata inserita piu
Per proteggere la sua carta abbiamo sospenso il acceso.

Per recuperare il acceso clicca su :

https://www.monetaonline.it/layout/03069/pop/code-ident
31357819513/

li cart

10% of serious attacks in 2021 are directly related to **Covid-19**

Increase of phishing, cloned sites, malware ...

False e-mail dall'Organizzazione Mondiale della Sanità per il Coronavirus, occhio alla truffa

Nel testo della e-mail viene annunciato un documento con tutte le precauzioni per evitare il contagio da Coronavirus e si invita ad aprire il documento allegato

Da Dr. Penelope Marchetti <peder@kennel-lope.dk>
Oggetto **Coronavirus: Informazioni importanti su precauzioni**
A Me

Gentile Signore/Signora,

A causa del fatto che nella Sua zona sono documentati casi di infezione dal coronavirus,
della Sanità ha preparato un documento che comprende tutte le precauzioni necessarie con
coronavirus. Le consigliamo vivamente di leggere il documento allegato a questo messaggi

Distinti saluti,
Dr. Penelope Marchetti (Organizzazione Mondiale della Sanità - Italia)

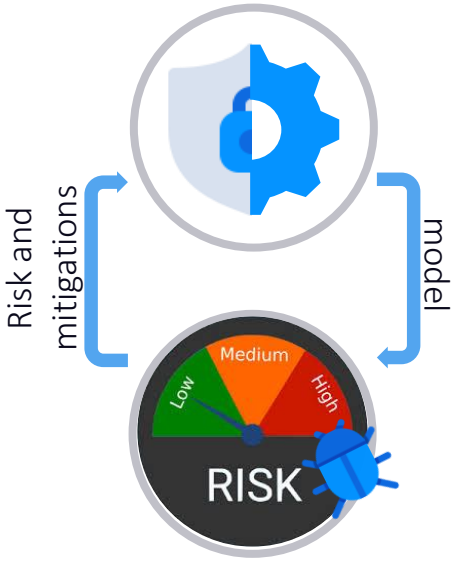
1 allegato: f211298392683.doc 387 kB

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

FBK CyberSecurity Center – Security & Trust
Our mission

! Need for **secure solutions** and **analysis tools** for the protection of our data



Security-by-design

Design of on-boarding, authentication and authorization solutions relying on innovative standards and considering the regulatory framework.

Automatic Security and Risk Assessment

With the goal of automatically detecting possible threats and associating each successful attack with the related risk and mitigations.

POLIGRAFICO E ZECCA DELLO STATO ITALIANO
security and innovation in our history

Public Administration

TRENTINOSALUTE 4.0

Health

CherryChain

FinTech

...

Our experience
DigiMat-Lab and F&C

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.

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

mission

Design and analysis of innovative solutions based on CIE

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

Applications based on CIE 3.0
Index

1

Introduction to CIE 3.0

General features and real-world scenarios

2

CIE 3.0 and cryptography

A focus on the cryptographic features of CIE 3.0

3

What about security?

Our methodology to analyze protocols based on CIE 3.0

FONDAZIONE BRUNO KESSLER

SECURITY & TRUST

Carta d'Identità Elettronica – CIE 3.0
What is it?

MINISTERO DELL'INTERNO

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

Physical identity proofing

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

- Replace paper-based version

CARDS ACTIVATED BY NOW
30/12/2021

25.768.740

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

Carta d'Identità Elettronica – CIE 3.0
Physical identity proofing

Personal data and photo of the owner are:

- printed on the plastic surface
  - visual security elements such as holograms and special inks prevent counterfeiting
- stored on the CIE chip can be accessed through NFC (Near Field Communication) interface
  - personal data cannot be accessed without the owner's knowledge: access key printed on the document (CAN – Card Access Number or MRZ – Machine Readable Zone).

Fingerprints may be processed only to control authorities with specific authorizations

Carta d'Identità Elettronica – CIE 3.0
Physical identity proofing

The use of eDocuments allow for

Automatic identity verification processes

Improving police checks security and efficacy

the reading and verification process of the personal and biometric data contained in the microchip verifies the authenticity of the document and the identity of the owner

ID.E.A – Identity Easy Access

An app to verify document's authenticity

Accessing data from CIE requires the MRZ, needed to derive the key for mutual authentication

Data can be accessed by interacting with the contactless chip via an NFC interface

https://play.google.com/store/apps/details?id=it.ipzs.nfccardreader

Carta d'Identità Elettronica – CIE 3.0
What is it?

MINISTERO DELL'INTERNO

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

Physical identity proofing

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

Online authentication

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

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

Carta d'Identità Elettronica – CIE 3.0
Online authentication

Entra con CIE

The **CIE** allows the citizen to **authenticate securely to online services** of institutions and public administrations

Descreto semplificazione (D.L. 76/2020) prevede l'equiparazione di SPID e CIE e indica il 28 febbraio 2021 quale data per lo switch off delle modalità diverse di identificazione per l'accesso ai servizi online delle pubbliche amministrazioni

CAD Art. 64. Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

2-quater. L'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono identificazione informatica avviene tramite SPID, **nonché tramite la carta di identità elettronica** [...]

Italy - eID

Member State	Republic of Italy
Title of the scheme	Italian eID based on National ID card (CIE)
eID means under the scheme	Italian eID card (Carta di Identità elettronica)
Level of assurance	High
Status	NOTIFIED
Date	13-set-2019
OJEU	2019/C 309/09
Date of Pre-notification	26-nov-2018
Date of Opinion of the CN	6-giu-2019
Link to the Opinion of the CN	https://ec.europa.eu/cefdigital/wiki/x/1ABIBg
Date of Publication to the official journal	13-set-2019

Regolamento (UE) n. 910/2014

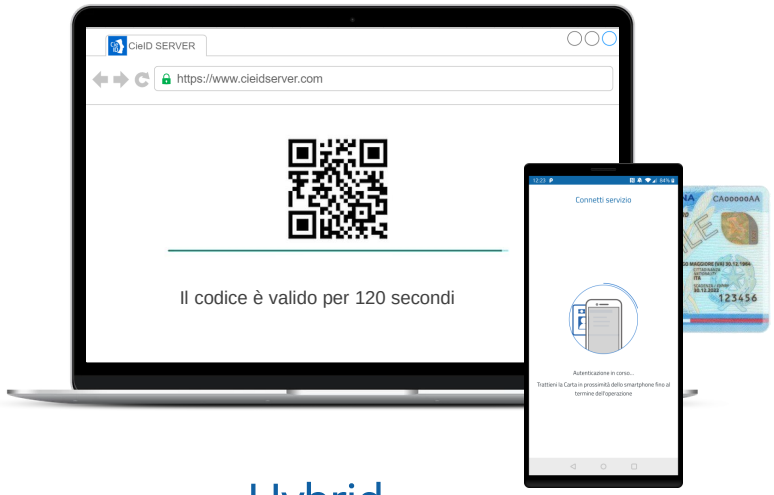
Carta d'Identità Elettronica – CIE 3.0
Online authentication

Entra con CIE

The **CIE** allows the citizen to **authenticate securely to online services** of institutions and public administrations

Total desktop

Total mobile



Hybrid

CIE 3.0 – Digital identity and more
Index

1

Introduction to CIE 3.0

General features and real-world scenarios

2

CIE 3.0 and cryptography

A focus on the cryptographic features of CIE 3.0

3

What about security?

Our methodology to analyze protocols based on CIE 3.0

FONDAZIONE BRUNO KESSLER

SECURITY & TRUST

CIE 3.0
Chip

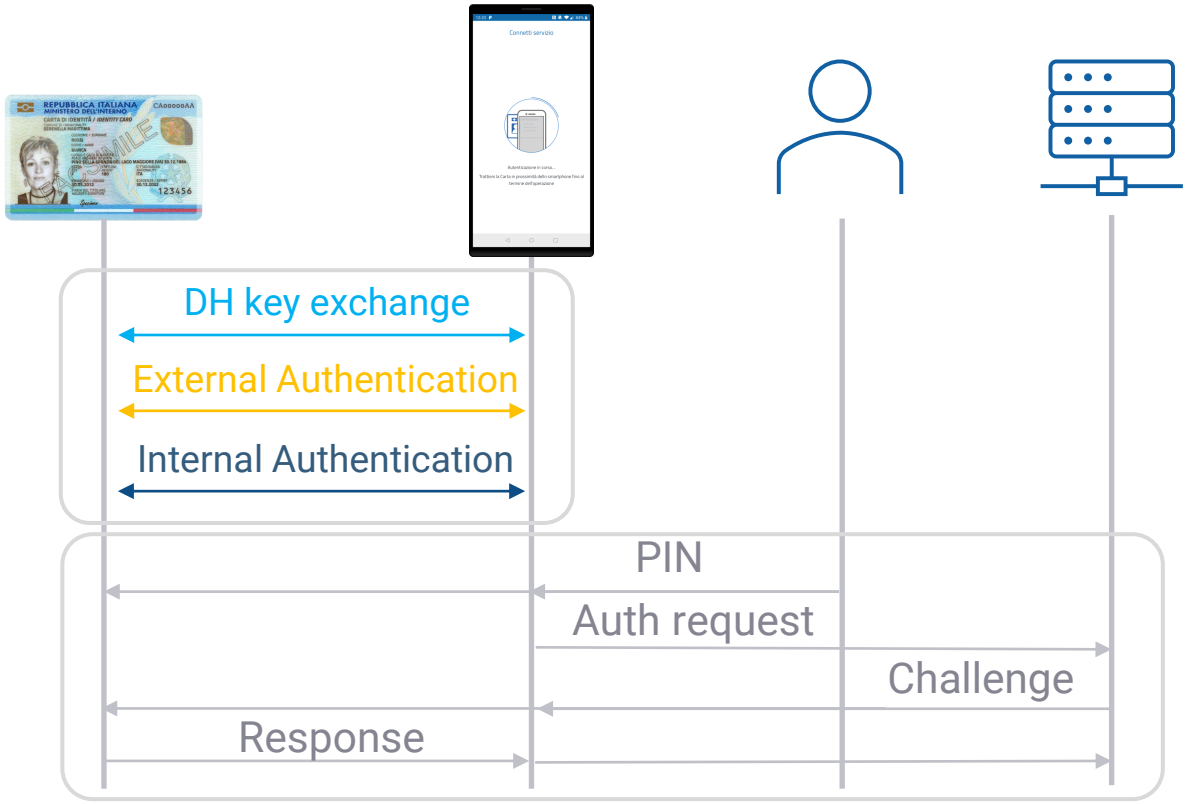
	Physical identity	Digital identity
Mobile	IDEA	CieID
Desktop		Middleware Windows 10, mac, linux
CIE 3.0	ICAO MRTD Identifying data Biometrics – fingerprint, photo	IAS-ECC Identifying data Unique identifier Authentication key Authentication certificate

CIE 3.0
IAS-ECC

Online authentication by means of the IAS-ECC involves the following entities and consists two main steps:

1. Creation of a secure channel:
   - The creation of a shared secret key between the CIE and the Terminal;
   - The mutual authentication of the peers

2. Challenge-Response auth protocol with the unlock of the secret key using the CIE PIN



CIE 3.0
IAS-ECC: DH key exchange

Diffie-Hellmann key exchange lets the two peers to share a secret key used to encrypt all the next exchanged messages → protection from eavesdropping attacks

CIE 3.0
IAS-ECC: external authentication

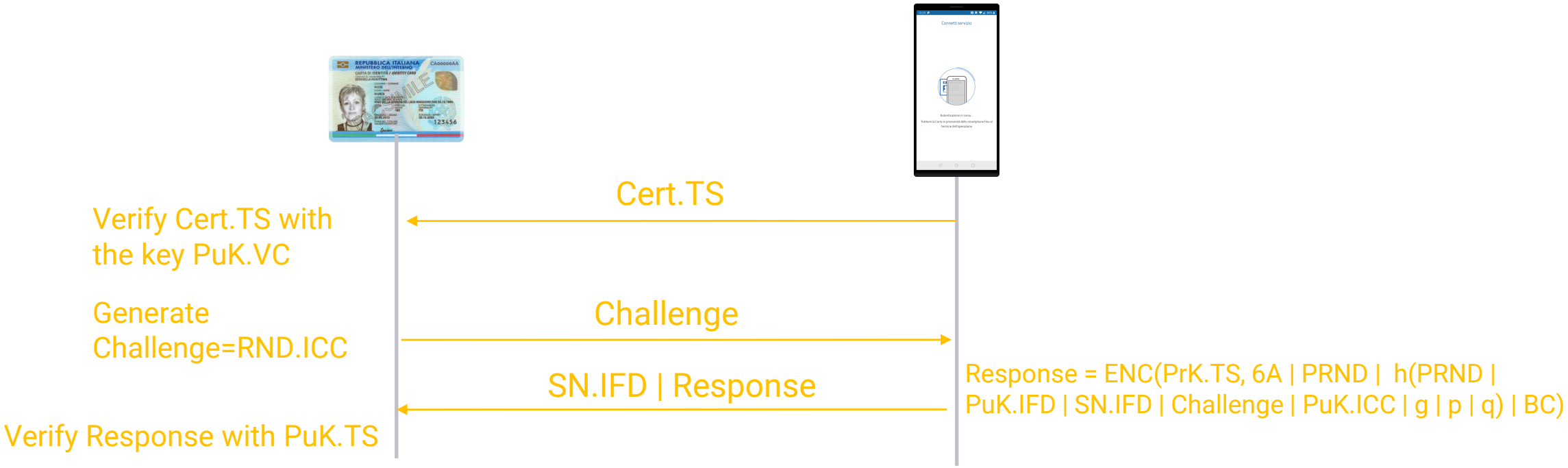
Terminal authenticates with the CIE: is asked to prove its identity, by engaging a challenge-response based mechanism with the CIE

CIE 3.0
IAS-ECC: e

In the Italian implementation of the IAS-ECC, the PKI used to validate the digital certificates for the Terminals has been removed, with the goal of reducing the cost and complexity of the infrastructure and incentivize the diffusion of the CIE as online authentication mechanism.

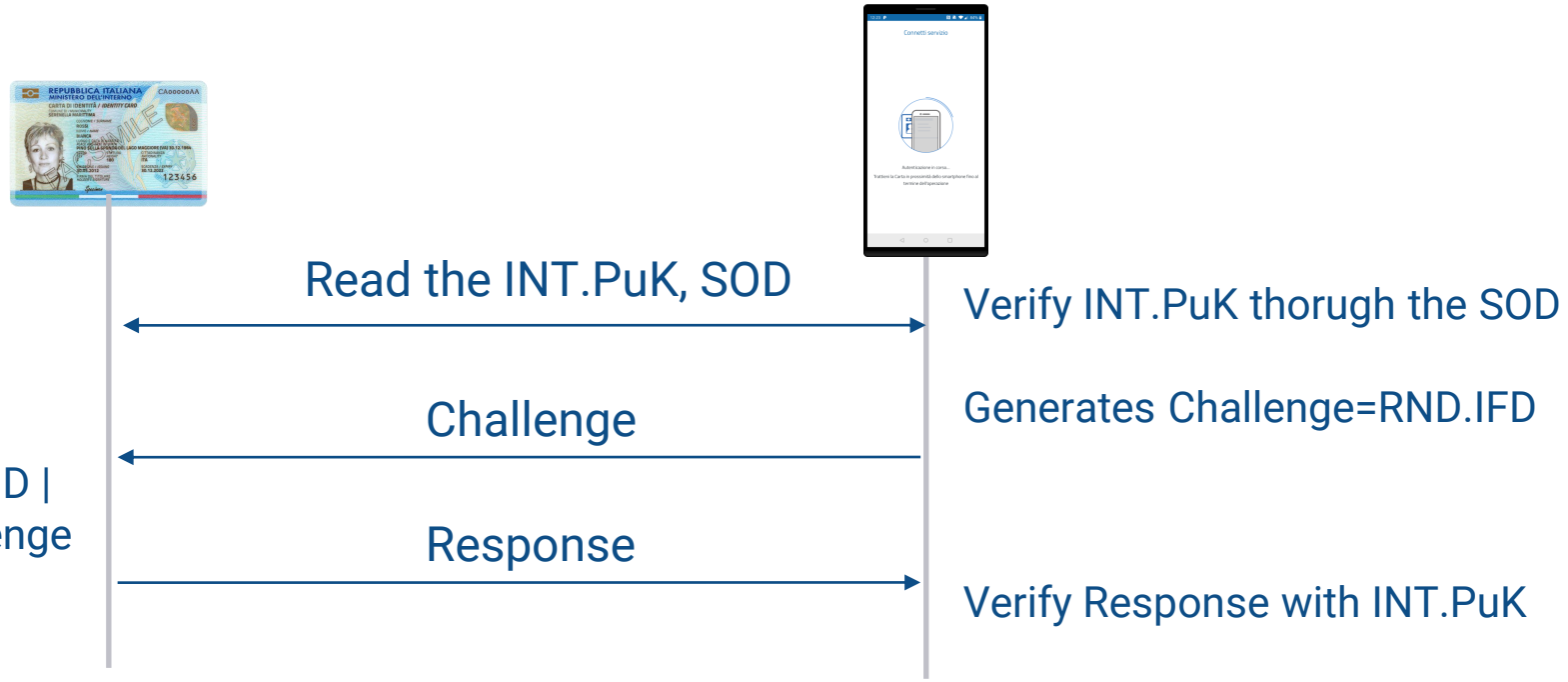
This implies that the Cert.TS send by Terminal to the CIE, actually has not been issued by a CA. More in detail, the pair (PuK.CV, PrK.CV) is made publicly available to all the Terminals, so that they can produce a valid (from the CIE perspective) certificate.

Terminal authentic
challenge-response based mechanism with the CIE



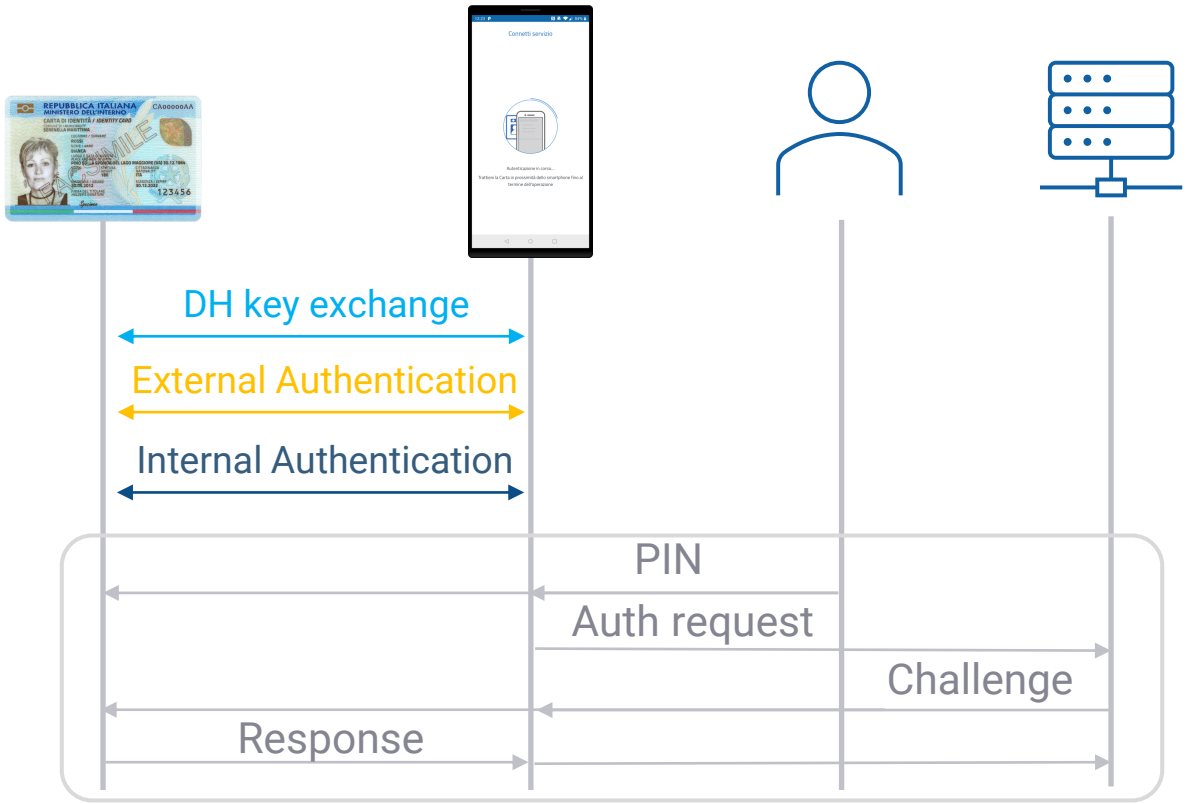
CIE 3.0
IAS-ECC: internal authentication

The CIE authenticates with the Terminal



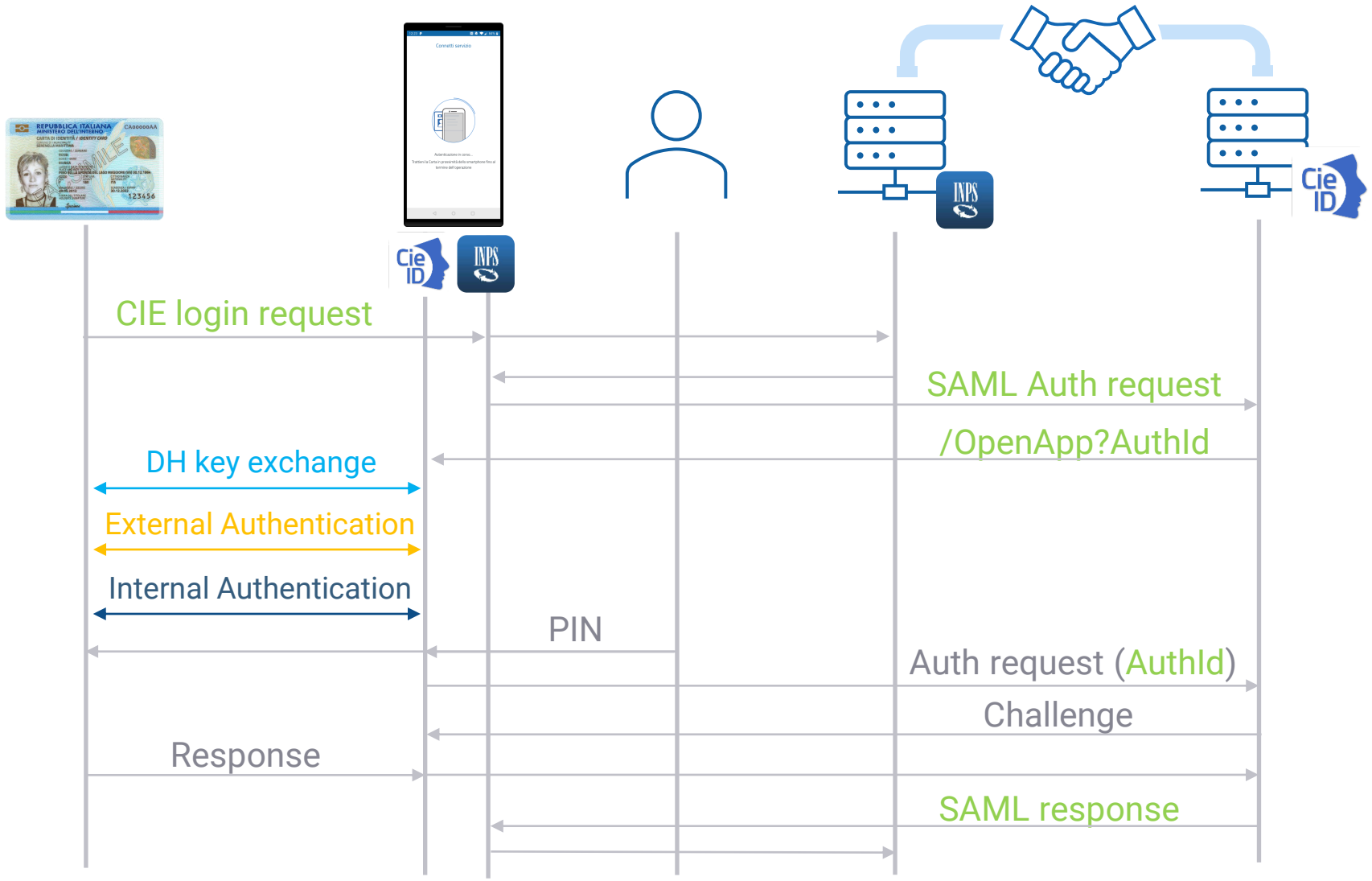
Response= ENC(INT.PrK, 6A | PRND | h(PRND | PuK.ICC | SN.ICC | Challenge | PuK.IFD | g | p | q) | BC)

CIE 3.0
IAS-ECC: CR auth protocol



“Entra con CIE 3.0” federation
SAML 2.0

Entra con CIE



CIE 3.0 – Digital identity and more
Index

1

Introduction to CIE 3.0

General features and real-world scenarios

2

CIE 3.0 and cryptography

A focus on the cryptographic features of CIE 3.0

3

What about security?

Our methodology to analyze protocols based on CIE 3.0

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

DigiMat-Lab and F&C
Methodology

Functional
and security
requirements

Security-by-design

Design and implementation of the protocol, based on state-of-the-art techniques

Automatic Security and Risk Assessment

With the goal of automatically detecting possible threats and associating each successful attack with the related risk and mitigations.

CIE 3.0
Online authentication

Total-desktop

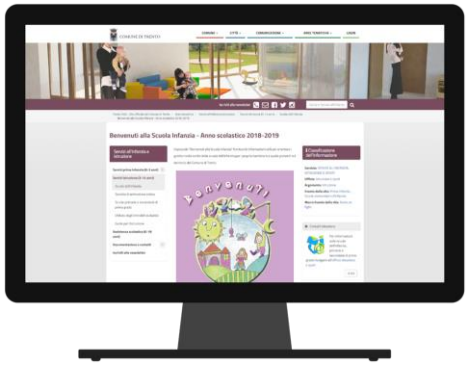
Total-mobile

Hybrid

CIE 3.0
Online authentication

Total-desktop

Total-mobile



Hybrid

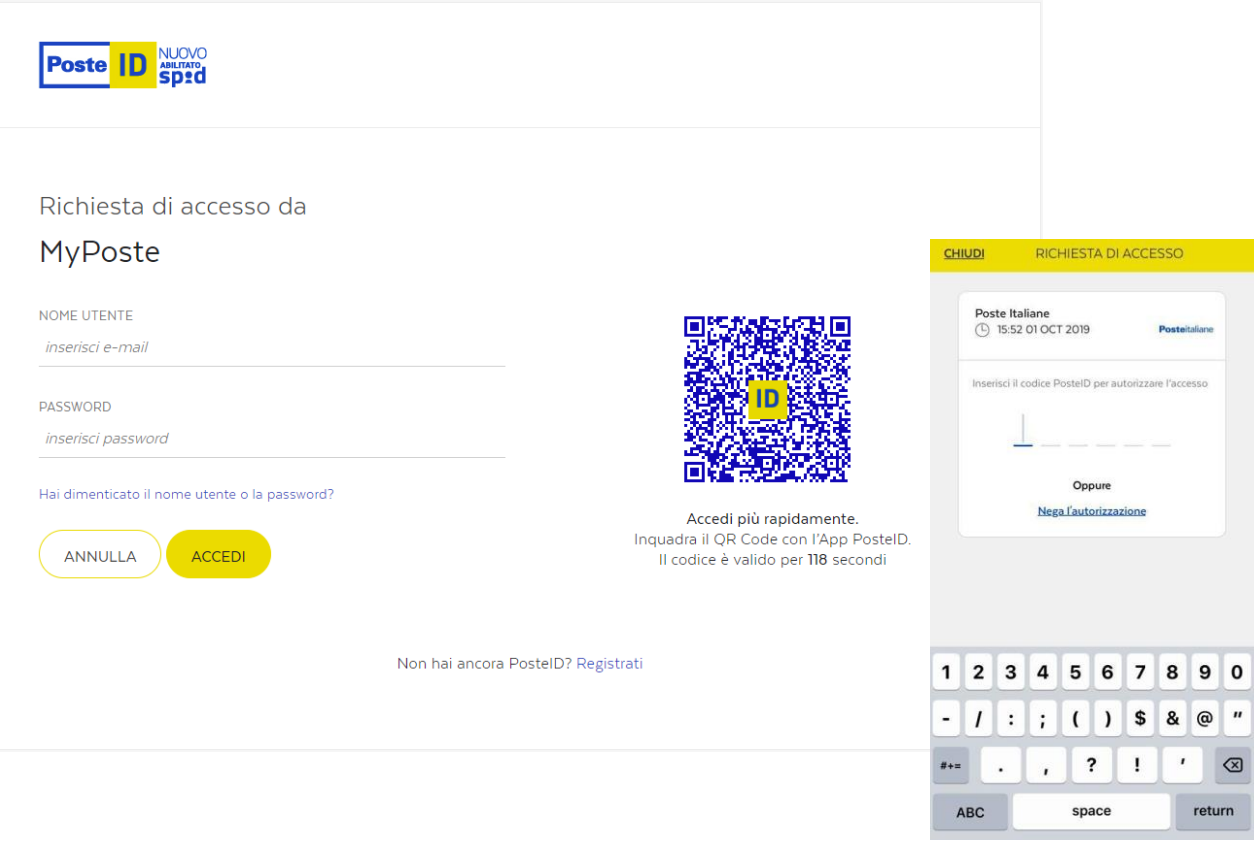
CIE 3.0 – Hybrid scenario
Requirements

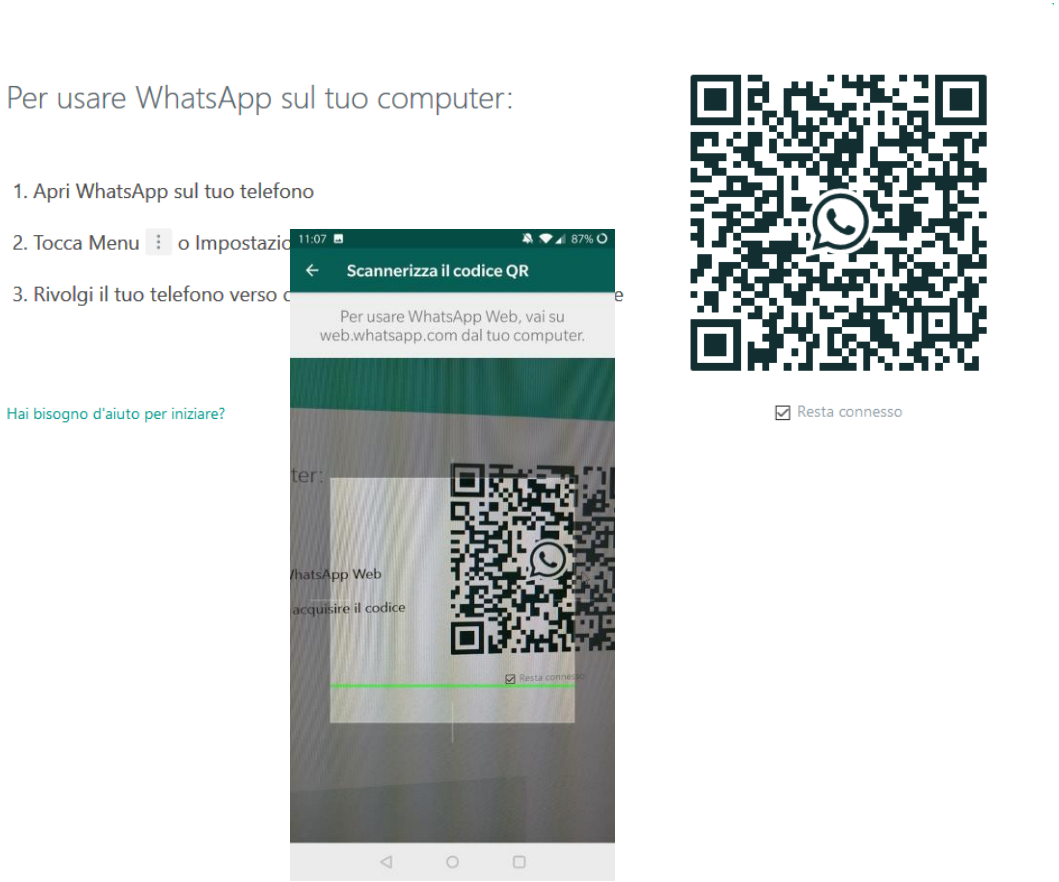
Requirements

1. Passwordless solution
2. SAML 2.0
3. No push notifications
4. No CIE ID SERVER databases
5. No preliminary phase to bind smartphone-desktop

Final choice: QR codes

CIE 3.0 – Hybrid scenario
State-of-the-art





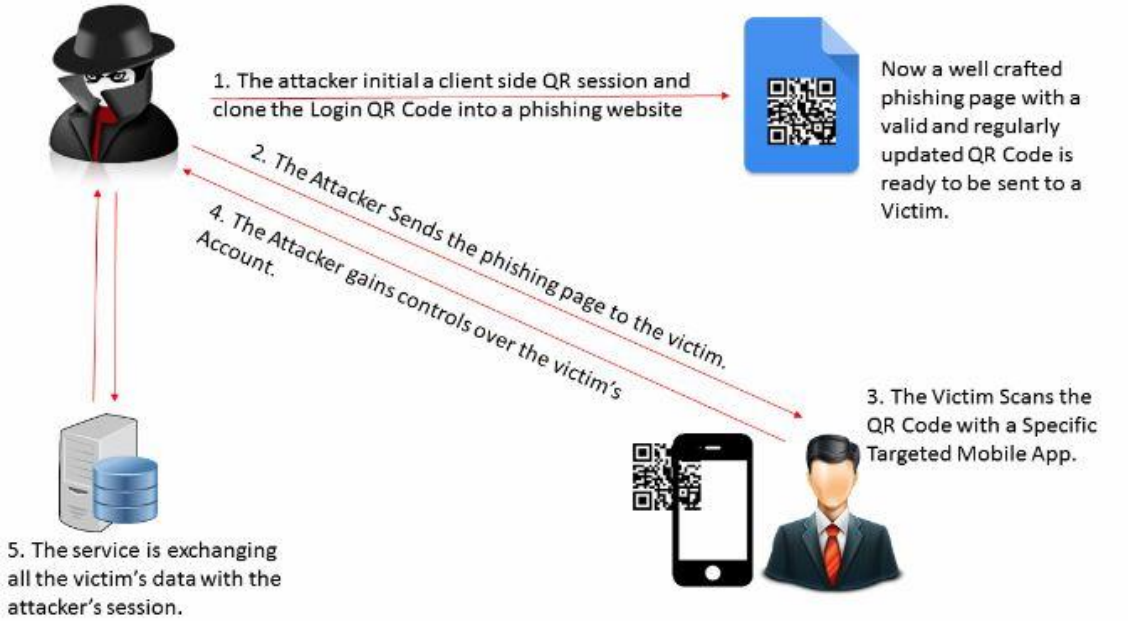
CIE 3.0 – Hybrid scenario
Known attack

QRLJacking (Quick Response Code Login Jacking) is a social engineering attack vector capable of session hijacking affecting all applications that rely on “Login with QR code” feature as a secure way to login into accounts. [OWASP]

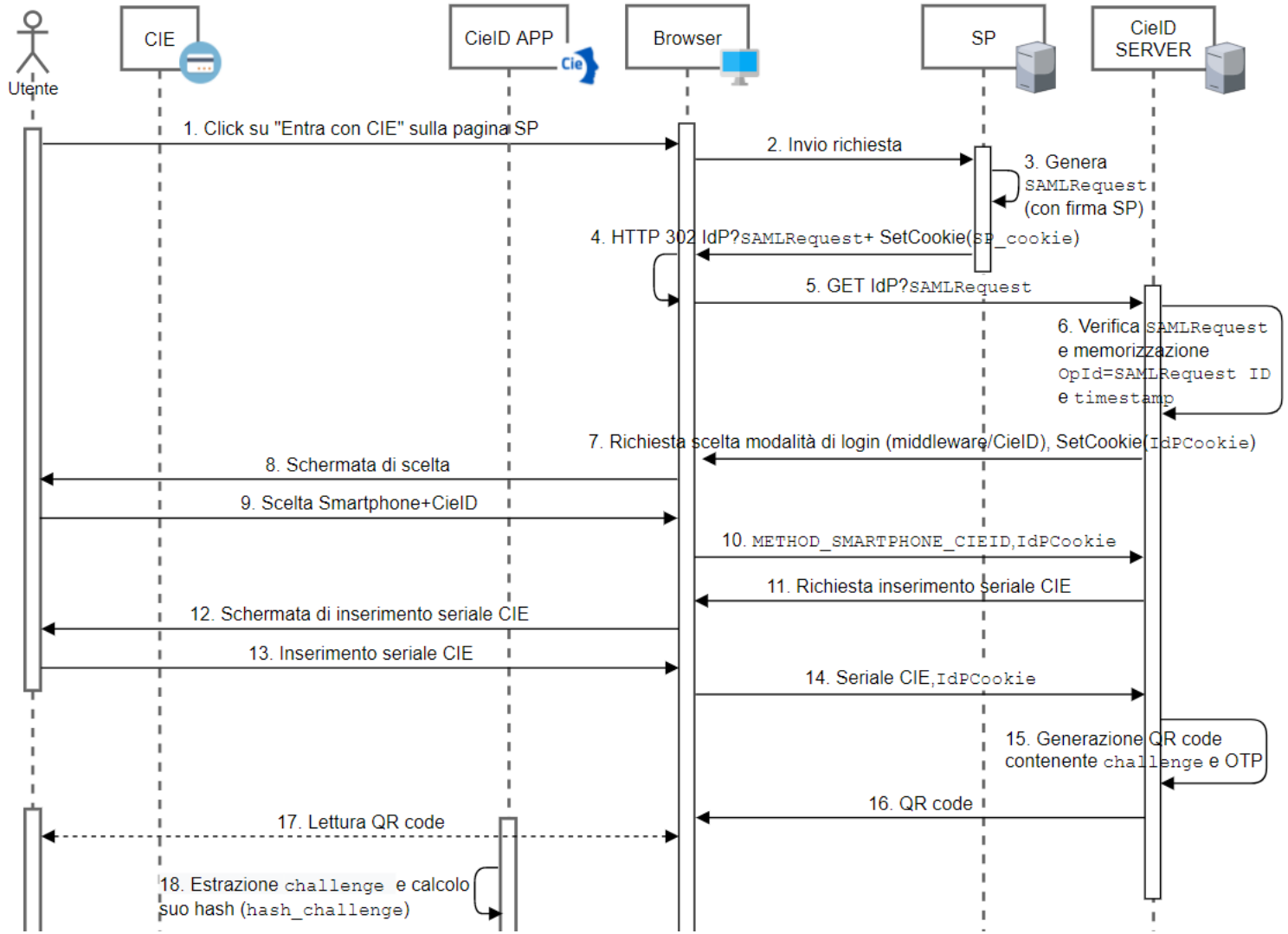
In a nutshell victim scans the attacker’s QR code results of session hijacking.

Attack Flow

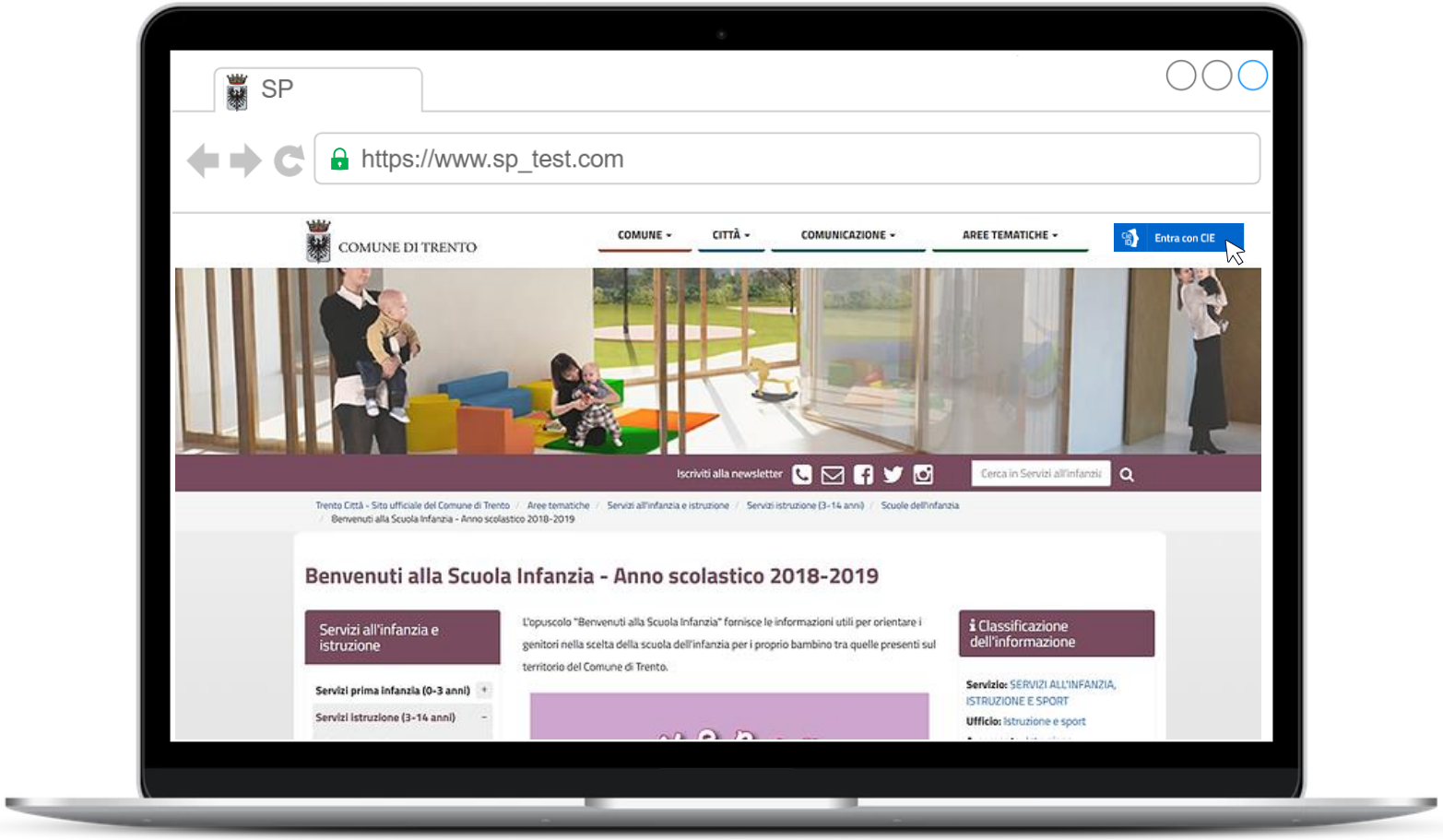
1. The attacker initial a client side QR session and clone the Login QR Code into a phishing website.
2. The Attacker Sends the phishing page to the victim. (refer to QRLJacking real life attack vectors)
3. The Victim Scans the QR Code with a Specific Targeted Mobile App.
4. The Attacker gains controls over the victim’s Account.
5. The service is exchanging all the victim’s data with the attacker’s session



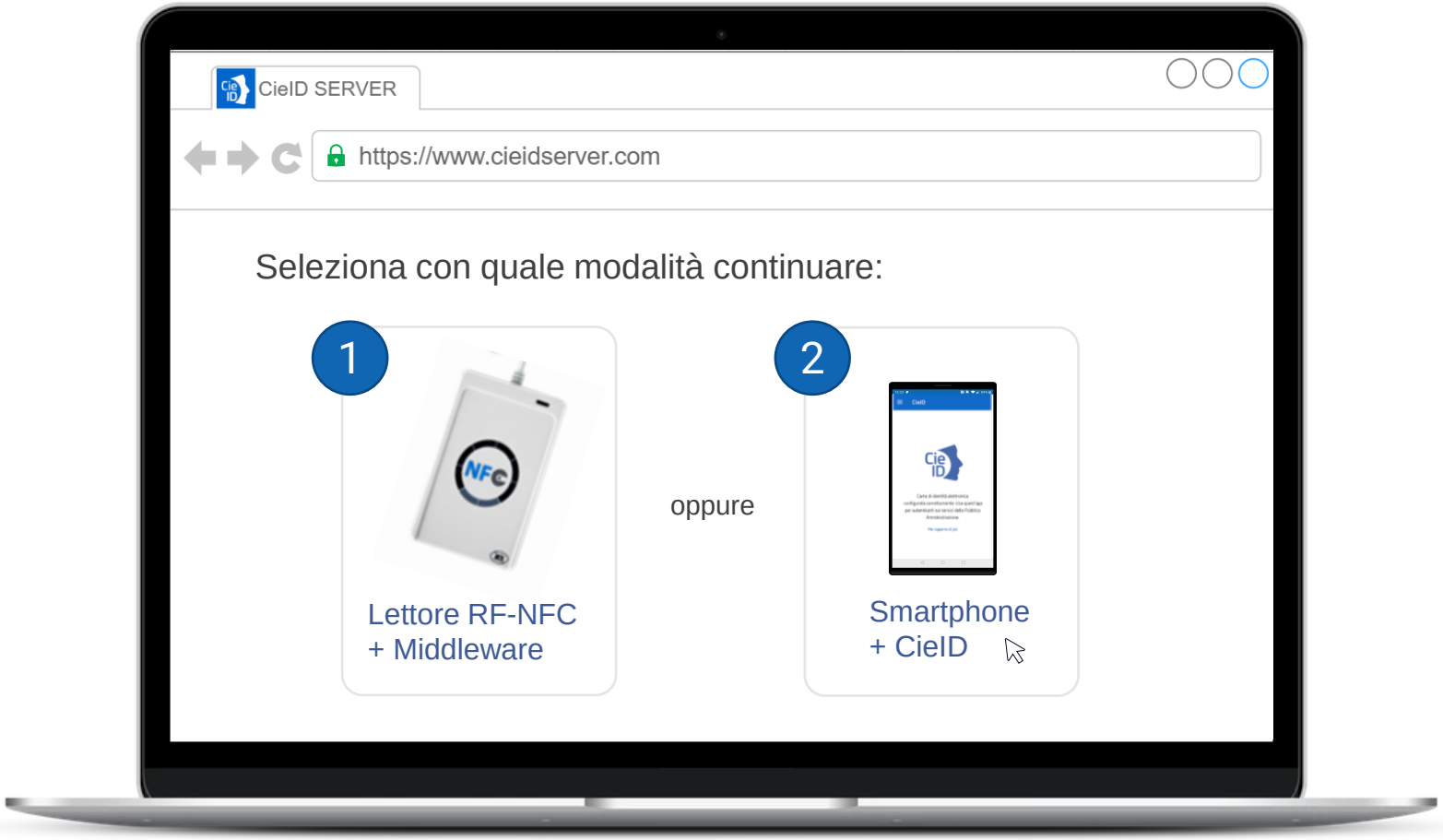
CIE 3.0 – Hybrid scenario
MSC



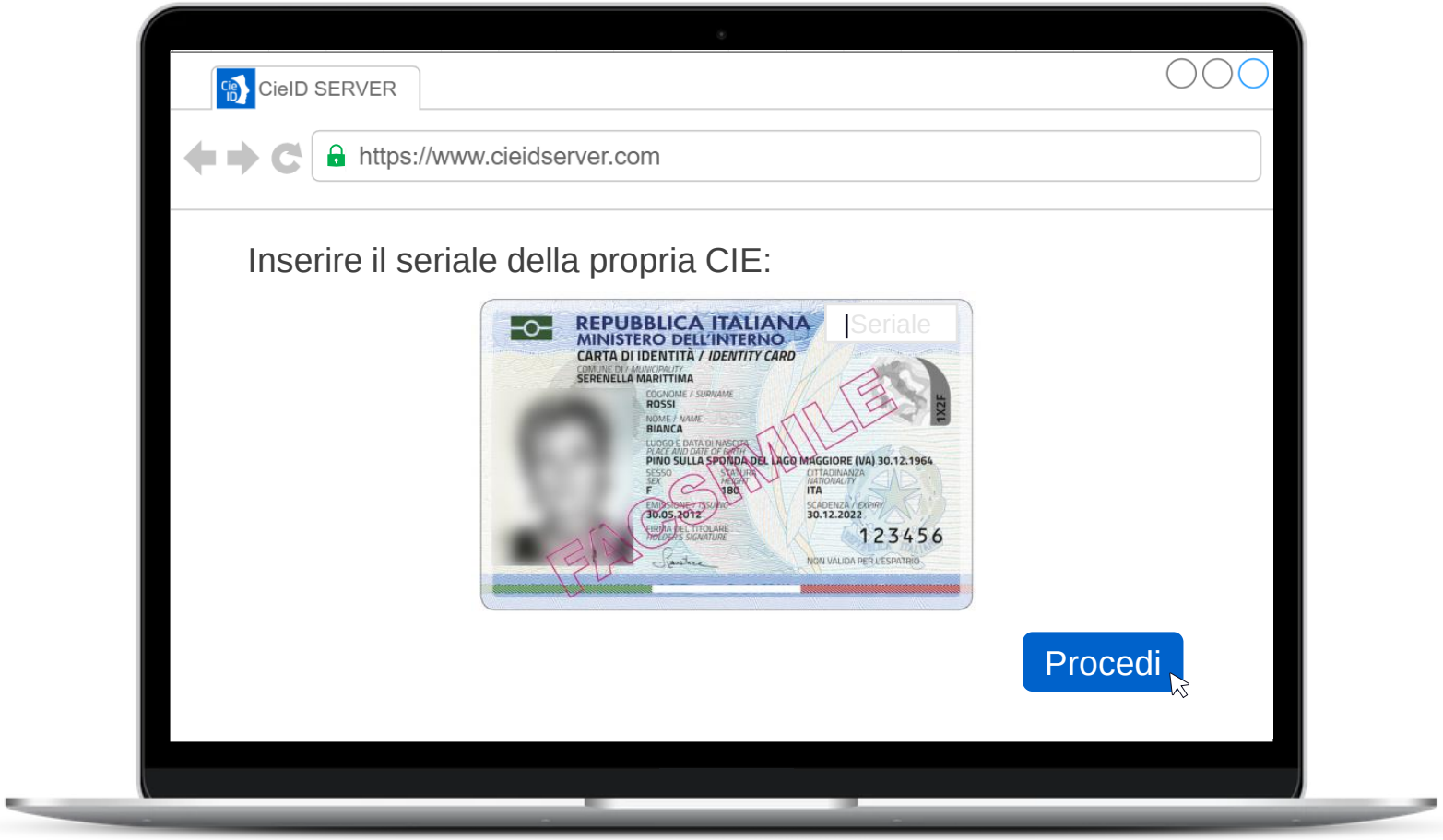
CIE 3.0 – Hybrid scenario
Mockup



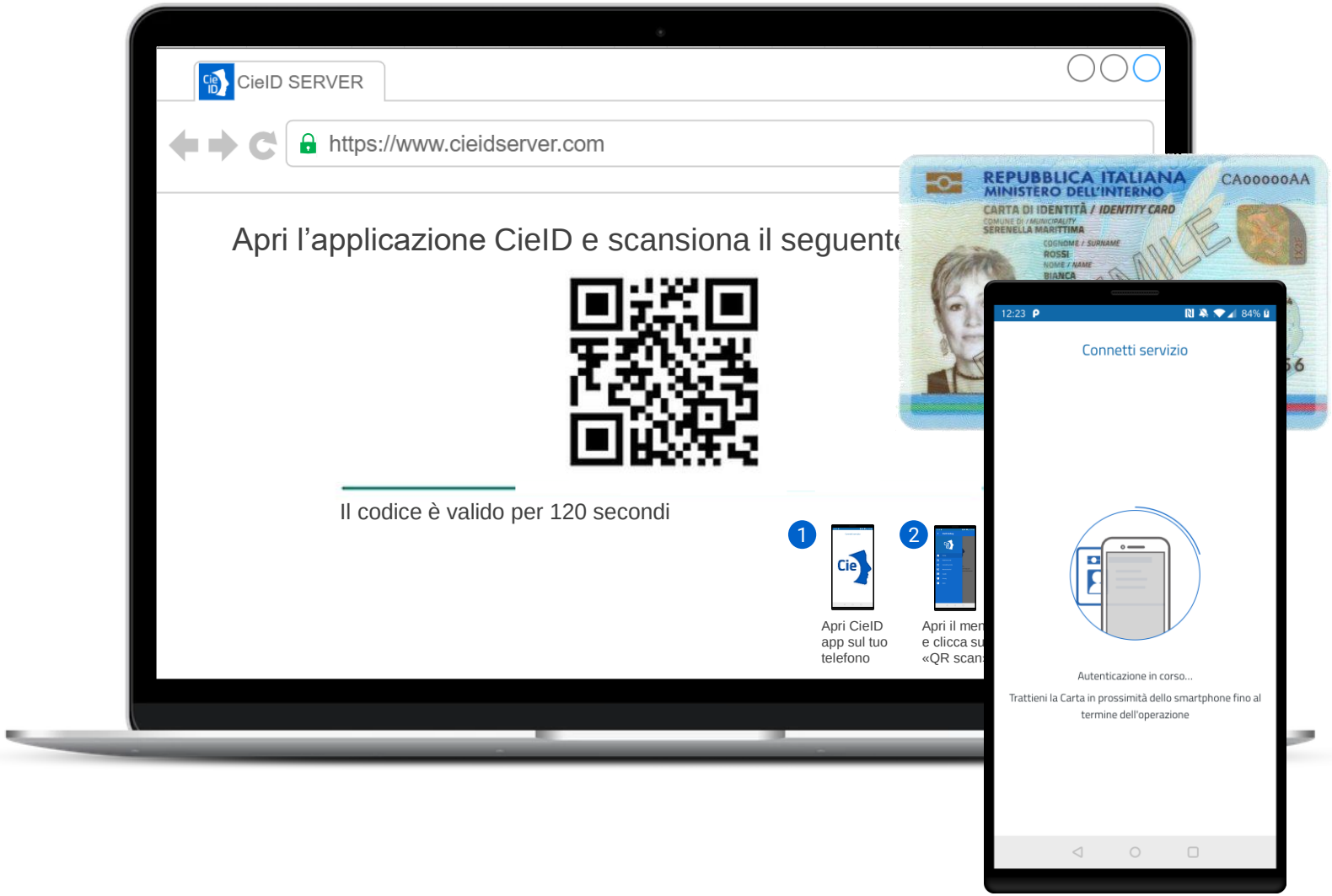
CIE 3.0 – Hybrid scenario
Mockup



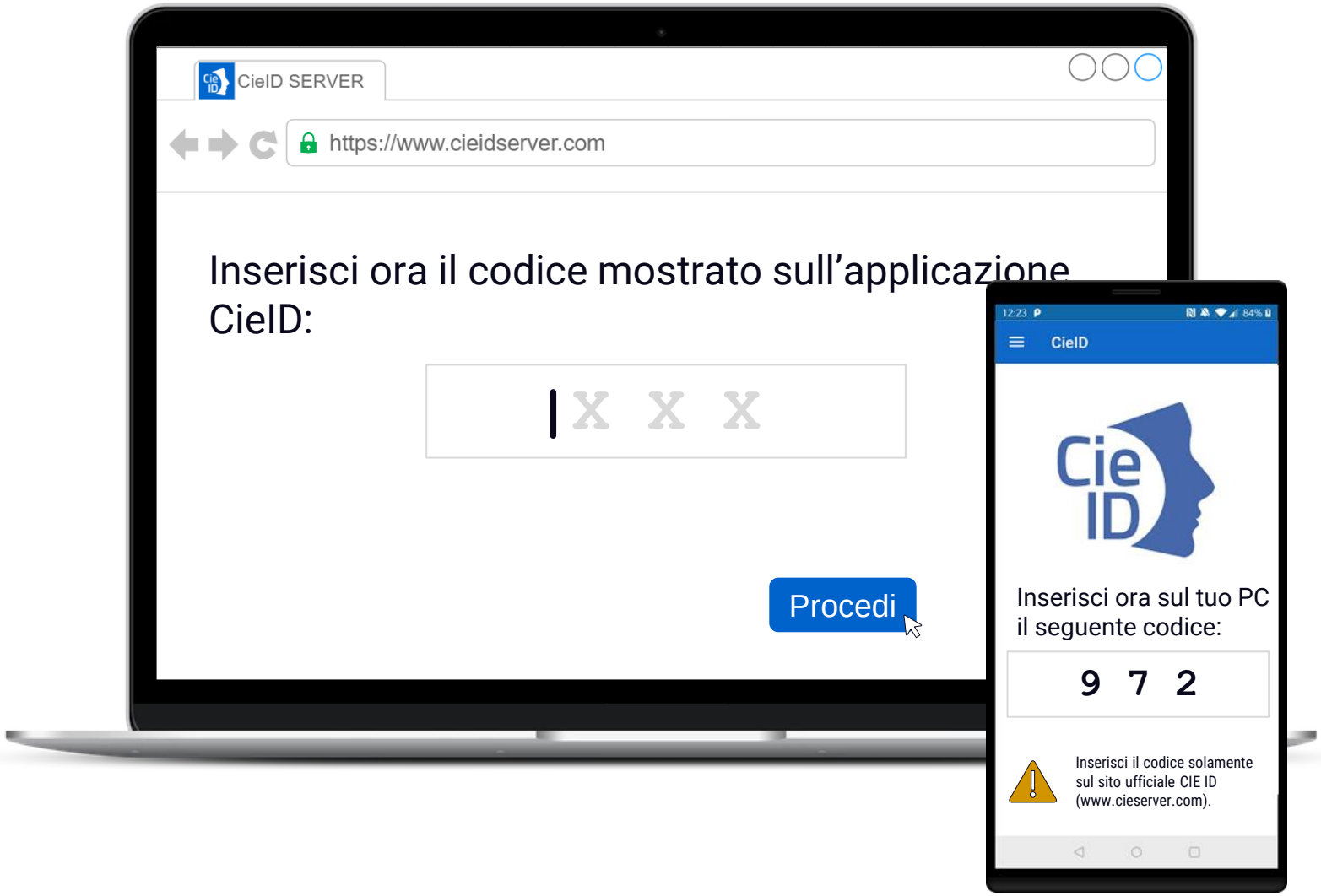
CIE 3.0 – Hybrid scenario
Mockup



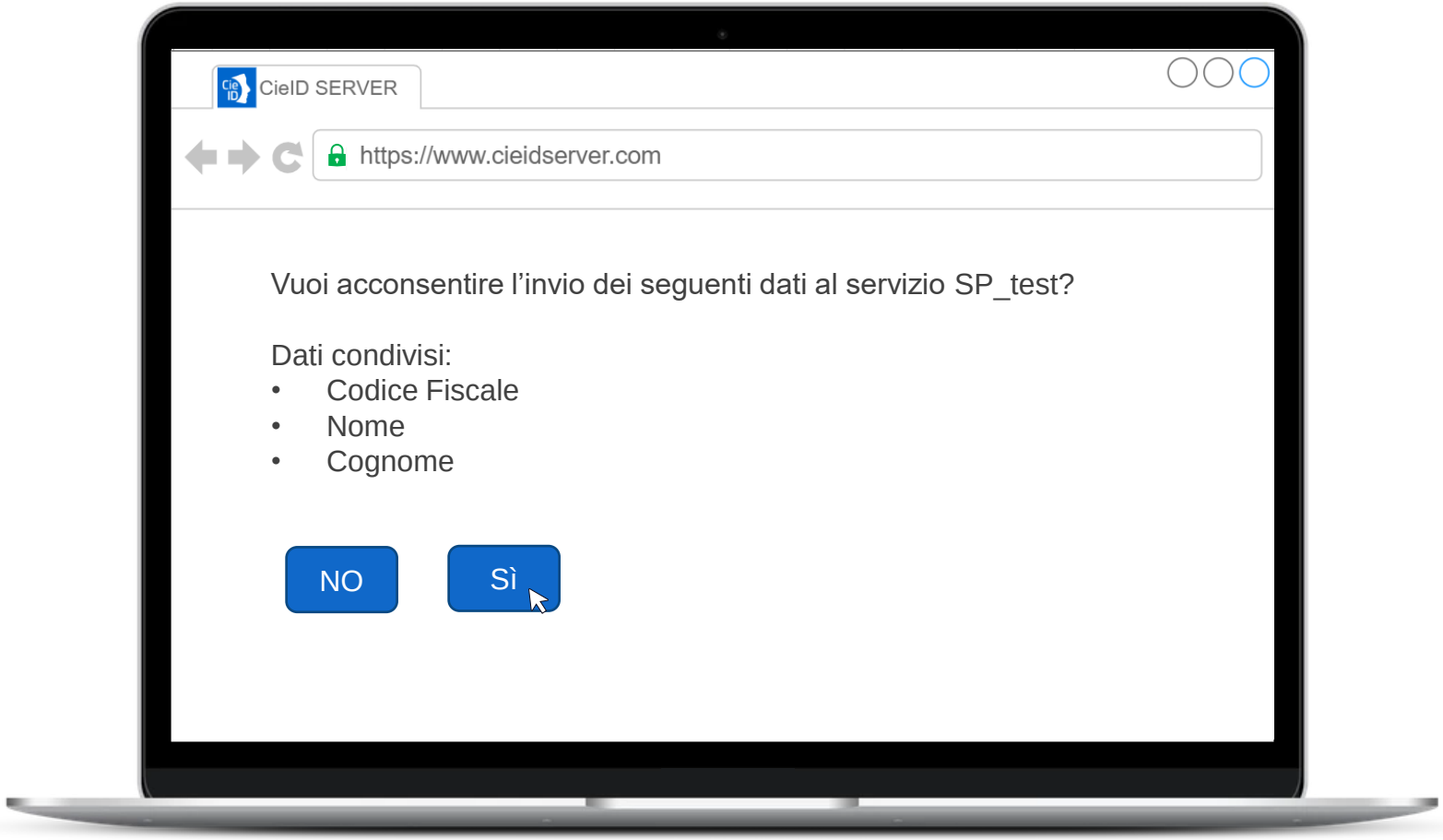
CIE 3.0 – Hybrid scenario
Mockup



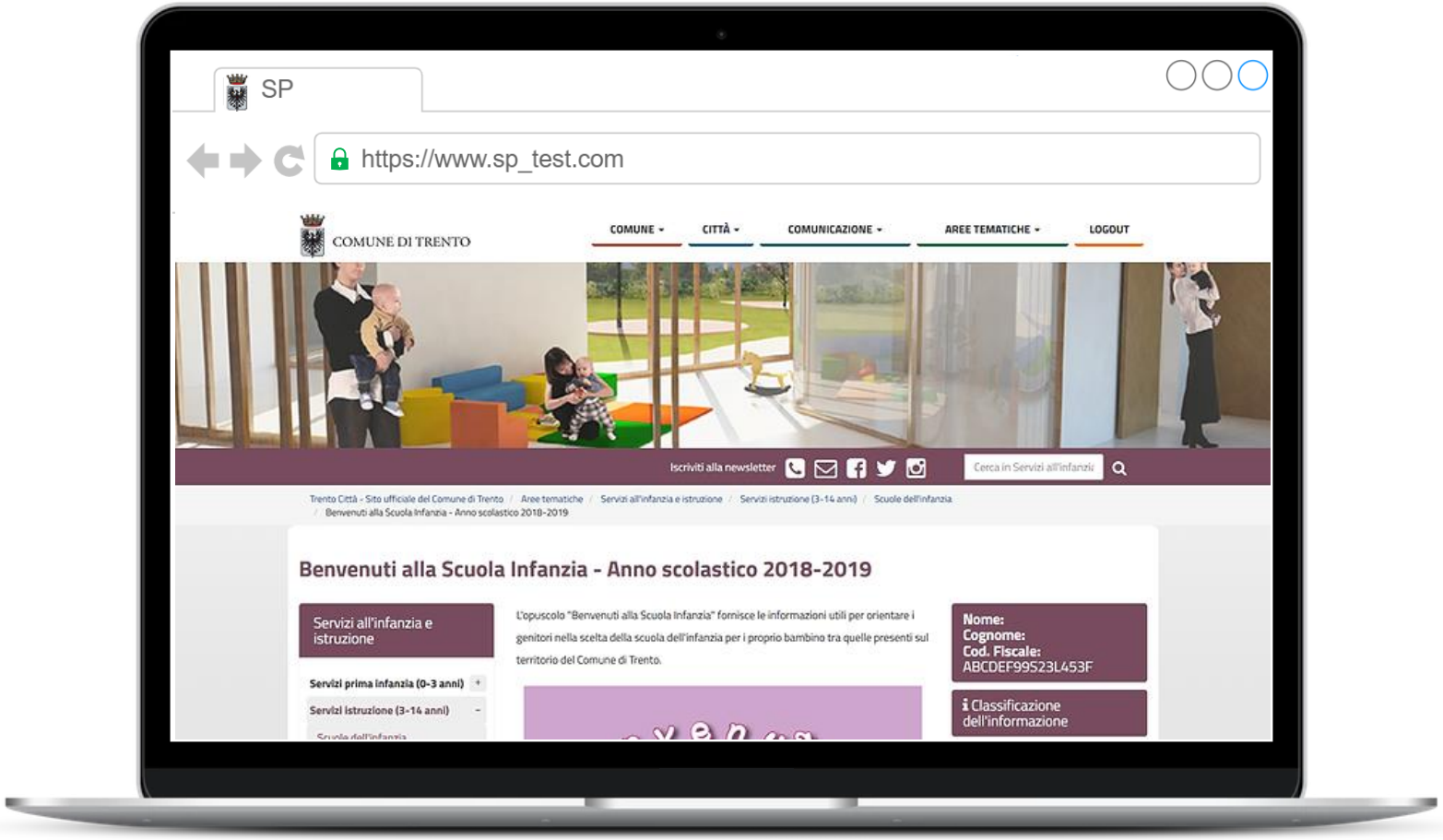
CIE 3.0 – Hybrid scenario
Mockup



CIE 3.0 – Hybrid scenario
Mockup



CIE 3.0 – Hybrid scenario
Mockup



QRLJacking
Mitigations

1. Require the input of a uniquely identifying information for the generation of the QR code

QRLJacking
Mitigations

1. Require the input of a uniquely identifying information for the generation of the QR code
2. QR code with a time validity

QRLJacking
Mitigations

1. Require the input of a uniquely identifying information for the generation of the QR code
2. QR code with a time validity
3. Advise users to verify the trustworthiness of the source by checking that the URL really belongs to CIE ID SERVER

QRLJacking
Mitigations

1. Require the input of a uniquely identifying information for the generation of the QR code
2. QR code with a time validity
3. Advise users to verify the trustworthiness of the source by checking that the URL really belongs to CIE ID SERVER
4. At the end of the authentication procedure, display an OTP on the mobile device and require users to insert it in the personal computer's browser

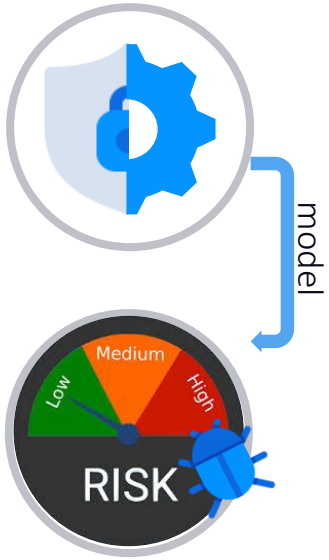
QRLJacking
Mitigations

1. Require the input of a uniquely identifying information for the generation of the QR code
2. QR code with a time validity
3. Advise users to verify the trustworthiness of the source by checking that the URL really belongs to CIE ID SERVER
4. At the end of the authentication procedure, display an OTP on the mobile device and require users to insert it in the personal computer's browser
5. Show the details of the on-going operation

DigiMat-Lab and F&C
Methodology

M. Pernpruner, R. Carbone, S. Ranise, G. 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*. CODASPY '20

M. Pernpruner, G. Sciarretta, S. Ranise. *A Framework for Security and Risk Analysis of Enrollment Procedures: Application to Fully-Remote Solutions Based on eDocuments*. SECRYPT 2021.



Security-by-design

Design and implementation of the protocol, based on state-of-the-art techniques

Automatic Security and Risk Assessment

With the goal of automatically detecting possible threats and associating each successful attack with the related risk and mitigations.

Protocol analysis
Security and Risk Assessment

Login as another's identity

1. Security Analysis: detects which attackers have success

Is able to steal a user device

is able to intercept the data typed on the device

2. Risk Analysis: allows us to classify the successful attacks based on their seriousness, and thus to prepare a mitigation plan accordingly

Security analysis
2 layers

Combinatorial Analysis

Relying on attackers' capabilities on the authentication factors, given that the violation of all of them necessarily results in the violation of the whole protocol. This analysis can be carried out quickly and returns all the explicit attacks (those deriving from the violation of all the authentication factors).

```
_provider(Actor, OTPPAT, ADC, Patient.
_T2P: channel, Request: text) {

 Clof SP
 ject{on(Patient -Ch_P2T-> Actor: Request):{  %STEP A1
Actor -Ch_T2D-> OTPPAT: Actor;  %STEP A2
        select{on(OTPPAT-Ch_O2T->Actor:{ADC.?Patient.Actor}_inv(pk(A
        HP_auth_U_on_Request:(Request) := Request;
        }}
 }}
}}

%%%% OTP-PAT APP %%%%
entity User_Agent(Actor, TrwC, ADC, Patient: agent, Ch_T2D, Ch_O2T, Ch
Ch_A2D, Ch_P2D, Ch_S2P: channel, Seed: seed, Token_HP: token, CTime:

symbols
KeyHash: key_hash;
Metadata: text;
Request: text;
Code:
```

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: implicit attacks manage to violate the protocol even without explicitly compromising all the authentication factors, as they manage to deceive the victim into implicitly compromising the remaining factors on their behalf.

Source: NIST Special Publication 800-63b

Security analysis
Combinatorial analysis

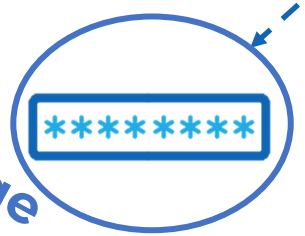
- The security goal ($\mathcal{SG}$) is the set of authentication factors that should not be compromised for the authentication procedure to be considered secure.

$$\mathcal{SG} = \{\text{🪪}\,; PIN\}$$

Ownership

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»

Knowledge



Security analysis
Combinatorial analysis

- The security goal ($\mathcal{SG}$) is the set of authentication factors that should not be compromised for the authentication procedure to be considered secure.

$$\mathcal{SG} = \{\text{🪪}\,; PIN\}$$

- A threat model ($\mathcal{TM}$) over the identification factors is a pair:

$$(\mathcal{ATT}; \mathcal{C})$$

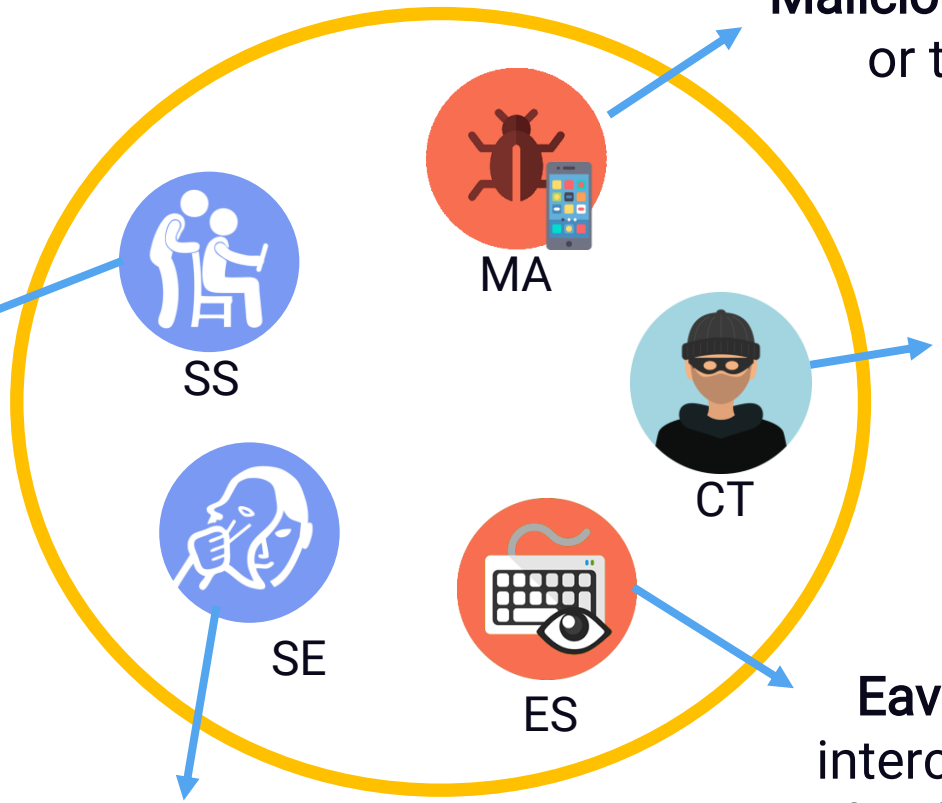
  where:
  - $\mathcal{ATT}$ is the set of considered attackers;
  - $\mathcal{C}$ represents their capabilities.

Security analysis
Attackers

Malicious App: runs on the attacker's or the victim's mobile device

CIE thief: steals an CIE from its legitimate owner

Shoulder Surfer: obtains secrets by looking at the user insering sensitive info



Eavesdropping Software: intercepts the data typed on the device (e.g., keylogger)

Social Engineer: deceives people into revealing secret information or performing actions to their advantage

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

Security analysis
Combinatorial analysis

Attackers		****	
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	🔓	🔓*

can only compromise the PIN (in case it is written on paper)

can only compromise the PIN (by looking at the victim while typing it)

can only compromise the PIN (by deceiving the victim into revealing it)

can only compromise the eDocument

can only compromise the PIN (by eavesdropping it while it is being typed)

can compromise the eDocument (indirectly, by deceiving the victim into interact with it), the PIN (by eavesdropping it while it is being typed)

🔒 = safe 🔓 = compromised 🔓* = indirectly compromised

Security analysis
Combinatorial analysis

- An auth flow **violates** the security goal $\mathcal{SG}$ under the threat model $\mathcal{TM} = (\mathcal{ATT}; \mathcal{C})$ iff there is an attacker (or a combination of them) in $\mathcal{ATT}$ that compromises all the identification factors contained in the $\mathcal{SG}$ associated to the flow.

- A subset $ATT \subseteq \mathcal{ATT}$ is **minimal** iff ATT violates $\mathcal{SG}$ and, for each $ATT' \subsetneq ATT$, ATT' does not violate $\mathcal{SG}$.

Attackers		****	
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	🔓	🔓 *

The **security analysis problem** for an auth flow under a threat model $\mathcal{TM} = (\mathcal{ATT}; \mathcal{C})$ is to find all (if any) minimal subsets $ATT \subseteq \mathcal{ATT}$ so that ATT violates $\mathcal{SG}$.

Security analysis
Combinatorial analysis

- An auth flow **violates** the security goal $\mathcal{SG}$ under the threat model $\mathcal{TM} = (\mathcal{ATT}; \mathcal{C})$ iff there is an attacker (or a combination of them) in $\mathcal{ATT}$ that compromises all the identification factors contained in the $\mathcal{SG}$ associated to the flow.

- A subset $ATT \subseteq \mathcal{ATT}$ is **minimal** iff ATT violates $\mathcal{SG}$ and, for each $ATT' \subsetneq ATT$, ATT' does not violate $\mathcal{SG}$.

Successful explicit attackers
MM
CT+AD
CT+ES
CT+SS
CT+SE

The **security analysis problem** for an auth flow under a threat model $\mathcal{TM} = (\mathcal{ATT}; \mathcal{C})$ is to find all (if any) minimal subsets $ATT \subseteq \mathcal{ATT}$ so that ATT violates $\mathcal{SG}$.

Security analysis
2 layers

Combinatorial Analysis

Relying on attackers' capabilities on the authentication factors, given that the violation of all of them necessarily results in the violation of the whole protocol. This analysis can be carried out quickly and returns all the explicit attacks (those deriving from the violation of all the authentication factors).

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: implicit attacks manage to violate the protocol even without explicitly compromising all the authentication factors, as they manage to deceive the victim into implicitly compromising the remaining factors on their behalf.

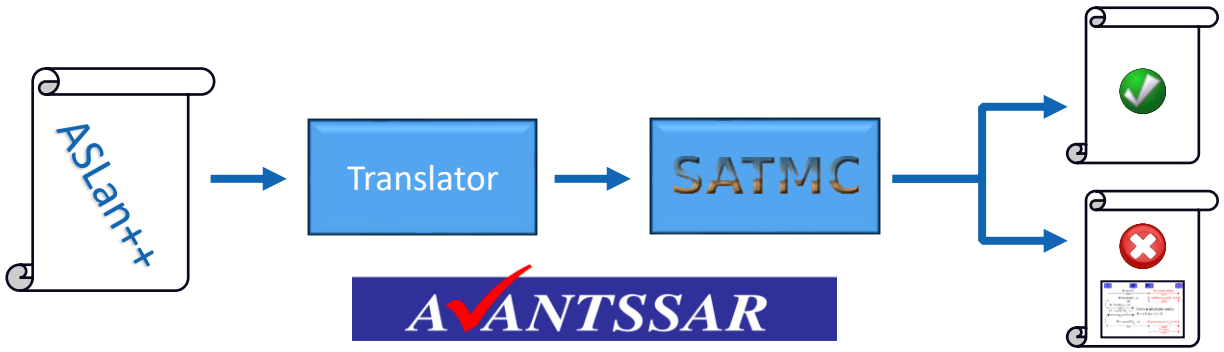
Security analysis
Formal analysis

```
entity IdPServer(Actor, EICApp, User, SPServer, Browser, EIC: agent, Ch_B2IdPS, Ch_EICApp2IdPS, Ch_IdPS2EICApp: channel) {

symbols
OpId: opid;
Request: userrequest;
OTP: otp;
IdPSessionCookie: cookie;

body { % of IdPServer
   select {
       on(Browser -Ch_B2IdPS-> Actor: ?Request):{
             IdPSessionCookie := fresh();
             OpId := fresh();
             Actor -Ch_IdPS2B-> Browser: Actor.IdPSessionCookie;

             select {
                 on(Browser -Ch_B2IdPS-> Actor: User.IdPSessionCookie):{
                 Actor -Ch_IdPS2B-> Browser: OpId.Actor.SPServer.User;

                 select {
                     on(EICApp -Ch_EICApp2IdPS-> Actor: OpId.{OpId.Actor.SPServer.User}_inv(pk(EIC))):{
                     OTP := fresh();
                     % iknows(OTP); % uncomment for SE
                     Actor -Ch_IdPS2EICApp-> EICApp: OTP;
                     Actor -Ch_IdPS2B-> Browser: Actor;

                 select {
```

Security analysis
Formal analysis

Att.	Formal Specification: Without Attacker	Formal Specification: With Attacker
PCT	(1) authentic_on(Ch_U2B, User); (2) userOwnComputer; — —	— — (3) weakly_authentic(Ch_U2B); (4) Use same channel ch_U2B in sessions
MDT	(5) authentic_on(Ch_U2EICApp, User); (6) userOwnSmartphone; — —	— — (7) weakly_authentic(Ch_U2EICApp); (8) Use same channel ch_U2EICApp in sessions
CT	(9) authentic_on(Ch_U2EIC, User); (10) userOwnEIC; — —	— — (11) weakly_authentic(Ch_U2EIC); (12) Use same channel ch_U2EIC in sessions
D	— —	(13) iknows(PIN); (14) iknows(IdPCookie);
ES, SS	(15) confidential_to(Ch_U2EICApp, EICApp); (16) confidential_to(Ch_EICApp2U, User); (17) confidential_to(Ch_U2B, Browser);	— — —
SE	(18) confidential_to(Ch_U2B, Browser); (19) authentic_on(Ch_B2U, Browser); — —	— — (20) iknows(PIN); (21) iknows(OTP);
MB	— —	(22) iknows(IdPCookie); (23) Replace browser with i in one session
MM	(24) authentic_on(Ch_EICApp2U, EICApp); (25) authentic_on(Ch_EICApp2EIC, EICApp); (26) confidential_to(Ch_FCMSvc2EICApp, EICApp); —	— — — (27) Replace eicapp with i in one session

User_authn_to_SP:(_) User *->> SPServer;



Implicit attacks	
SE	MB

Risk analysis
OWASP Risk Rating Methodology

The **risk analysis problem** for an enrollment flow under a threat model $\mathcal{TM}=(\mathcal{ATT};\mathcal{C})$ is to find the risk associated with all the minimal subsets of attackers violating $\mathcal{SG}$.

Att.	Likelihood							Impact						Risk
	TD	O	AV	UI	SA	Aver.	Over.	LSP	AS	AD	AP	Aver.	Over.	
MM	2	2	7	1	2	2.80	Low	9	8	3	2	5.50	Medium	Low

1. Assign a score (0-9) to each factor
2. Compute the average of likelihood and impact factors
3. Obtain the overall likelihood and impact
4. Compute the risk

$v < 3$	Low
$3 \leq v < 6$	Medium
$v < 9$	High

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

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.

	Attackers	Likelihood							Impact						Risk
		TD	O	AV	UI	SA	Overall		LSP	AS	AD	AP	Overall		Overall
explicit	MM	2	2	7	1	2	2.80	Low	9	8	3	2	5.50	Medium	Low
	CT+D	8	1	1	7	4	4.20	Medium	9	2	3	8	5.50	Medium	Medium
	CT+ES	5	0	1	4	2	2.40	Low	9	2	3	8	5.50	Medium	Low
	CT+SS	8	4	1	2	5	4.00	Medium	9	2	3	8	5.50	Medium	Medium
	CT+SE	4	2	1	4	3	2.80	Low	9	2	3	8	5.50	Medium	Low
implicit	SE	4	9	7	1	4	5.00	Medium	9	5	7	2	5.75	Medium	Medium
	MB	3	5	7	1	4	4.00	Medium	9	8	7	2	6.50	High	High

Protocol analysis
The role of mitigations

- Mitigations can be specified by properly adjusting:
  - the attackers' capabilities ($\mathcal{C}$);
  - the risk scores assigned to the likelihood and impact factors.

Require the input of a uniquely identifying information during the authentication protocols

SE has less probability of performing a QRLJacking

Implement root detection mechanisms on the mobile application

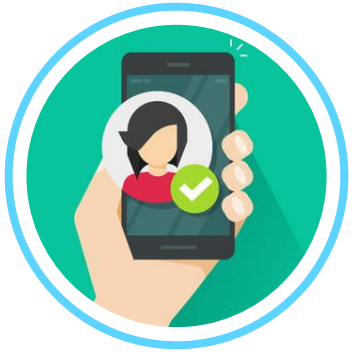
MM is less likely able to steal the PIN from the internal storage

Attackers	Likelihood	Impact	Risk
MM	Medium	**High**	**High**
CT+D	Medium	Medium	Medium
CT+ES	Low	Medium	Low
CT+SS	Medium	Medium	Medium
CT+SE	**Medium**	Medium	**Medium**
SE	**High**	**High**	**Critical**
MB	Medium	High	High

CIE 3.0
Real-world scenarios and future directions

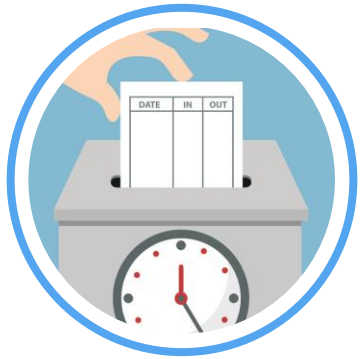
Physical identity proofing

Online authentication



Remote identity proofing

Electronic Signature



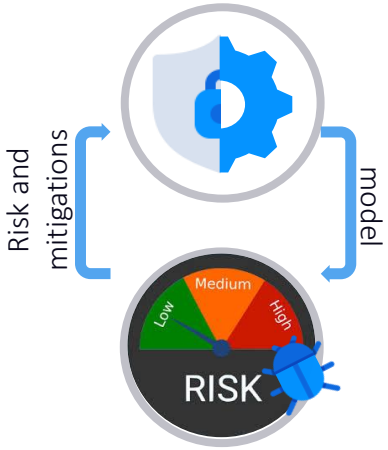
Advanced scenarios

European Digital Identity Wallet

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

DigiMat-Lab and F&C
Methodology



Security-by-design

Design and implementation of the protocol, based on state-of-the-art techniques

Automatic Security and Risk Assessment

With the goal of automatically detecting possible threats and associating each successful attack with the related risk and mitigations.

It allows what-if analyses, by providing information on how specific mitigations affect the set of successful attackers and their risks

References (CIE)

- Ministero dell'interno – CIE 3.0. https://www.cartaidentita.interno.gov.it/en/home/
- Specifiche Chip – CIE 3.0. https://www.cartaidentita.interno.gov.it/downloads/2021/03/cie_3.0_-_specifiche_chip.pdf
- EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS - IAS ECC. Technical Specifications Revision: 1.0.1. https://dvv.fi/documents/16079645/17324992/IAS+ECC+v1_0_1UK.pdf/84043361-56ad-bc26-8223-37e0d79355d8/IAS+ECC+v1_0_1UK.pdf?t=1622729405351
- Developers italia – CIE 3.0 https://developers.italia.it/it/cie/#resourcecontent-1
- Erogatori di servizi abilitati – CIE 3.0. https://federazione.servizicie.interno.gov.it/listSP
- App IDEA https://www.idea.ipzs.it/
- Regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- Commission proposes a trusted and secure Digital Identity for all Europeans. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663
- Decreto legislativo 7 marzo 2005, n. 82 e s.m.i. recante "Codice dell'amministrazione digitale". https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2021-07-30/_rst/capo_V-sezione_III-articolo_64.html

References (methodology)

- G. Sciarretta, R. Carbone, S. Ranise, and L. Viganò. 2020. *Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Login*. TOPS (June 2020) https://doi.org/10.1145/3386685
- M. Pernpruner, R. Carbone, S. Ranise, G. 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*. CODASPY '20 https://doi.org/10.1145/3374664.3375727
- M. Pernpruner, G. Sciarretta, S. Ranise. *A Framework for Security and Risk Analysis of Enrollment Procedures: Application to Fully-Remote Solutions Based on eDocuments*. SECRYPT 2021. https://doi.org/10.5220/0010554502220233
- Matteo Leonelli, Umberto Morelli, Giada Sciarretta, and Silvio Ranise. "Secure Pull Printing with QR Codes and National eIDCards: 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

https://stfbk.github.io/

giada.sciarretta@fbk.eu