18th International Conference on Security and Cryptography (SECRYPT 2021)
July 6-8, 2021 – Virtual Event

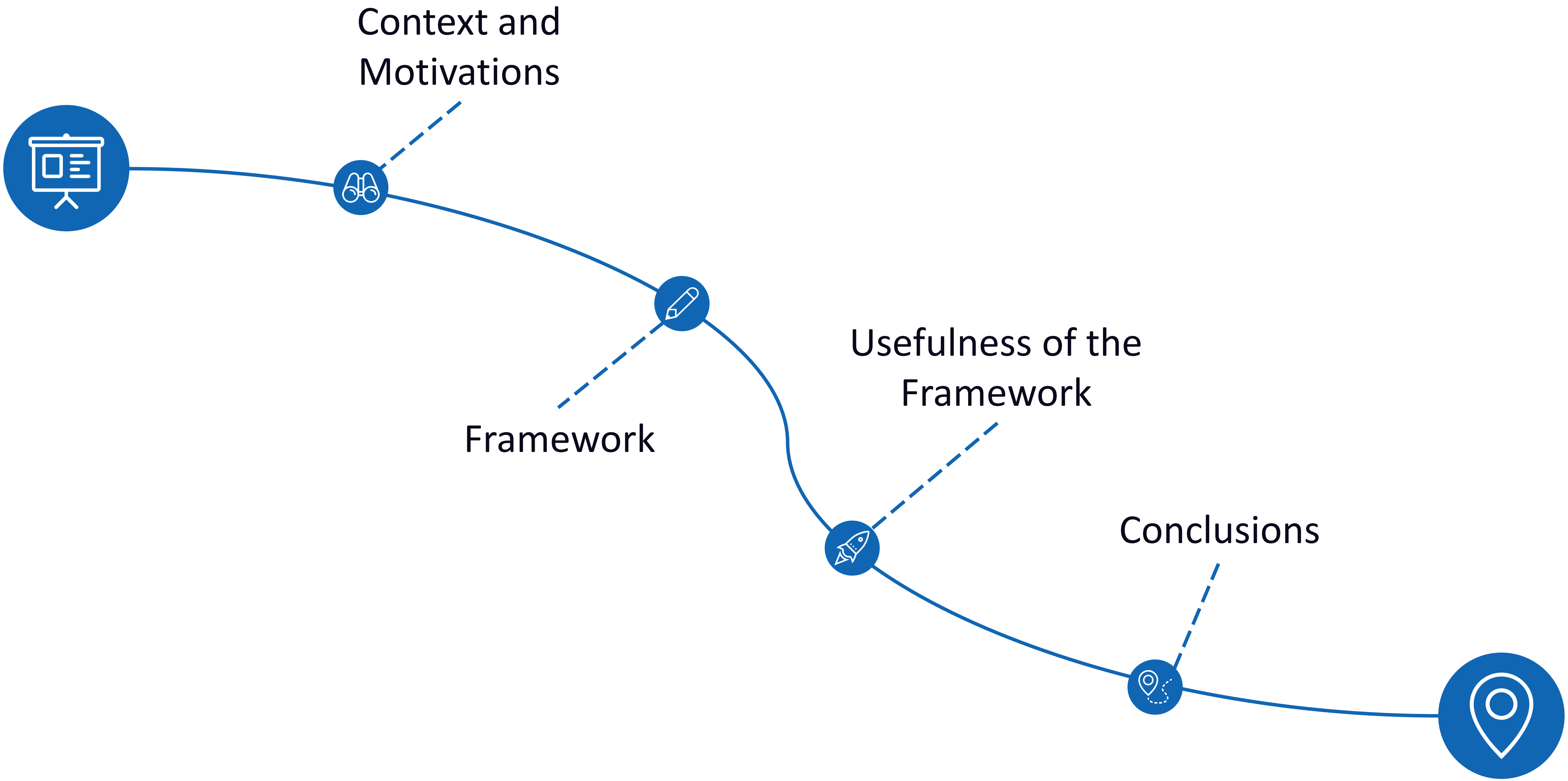
A Framework for Security and Risk Analysis of Enrollment Procedures

Application to Fully-remote Solutions based on eDocuments

Marco Pernpruner[1,2], Giada Sciarretta[1], and Silvio Ranise[1,3]

[1] Security & Trust Research Unit, Fondazione Bruno Kessler, Trento, Italy
[2] Department of Informatics, Bioengineering, Robotics and System Engineering, University of Genoa, Genoa, Italy
[3] Department of Mathematics, University of Trento, Trento, Italy
{mpernpruner, giada.sciarretta, ranise}@fbk.eu

Agenda



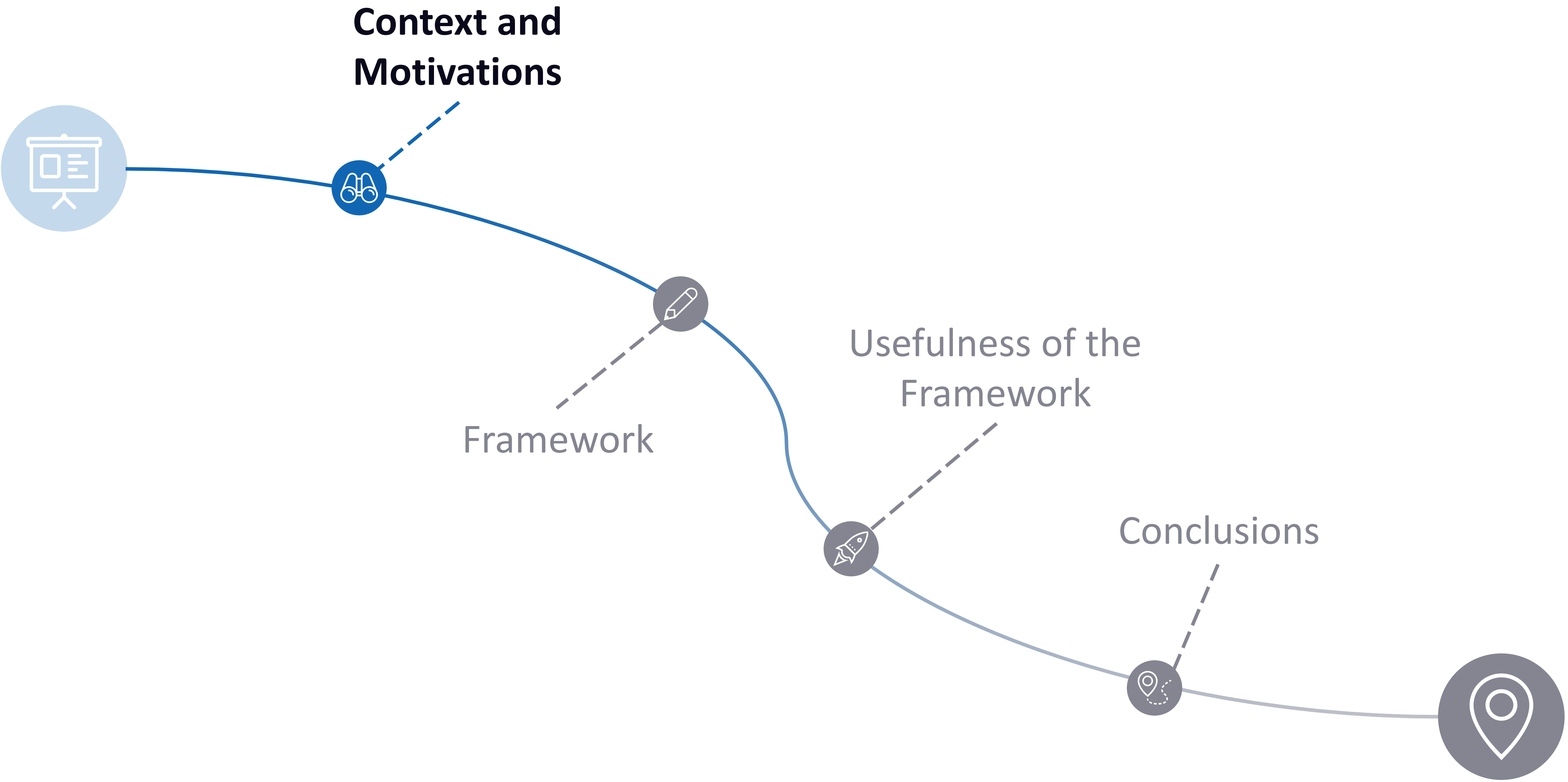
Context and Motivations

Framework

Usefulness of the Framework

Conclusions

Agenda



Context and Motivations

Framework

Usefulness of the Framework

Conclusions

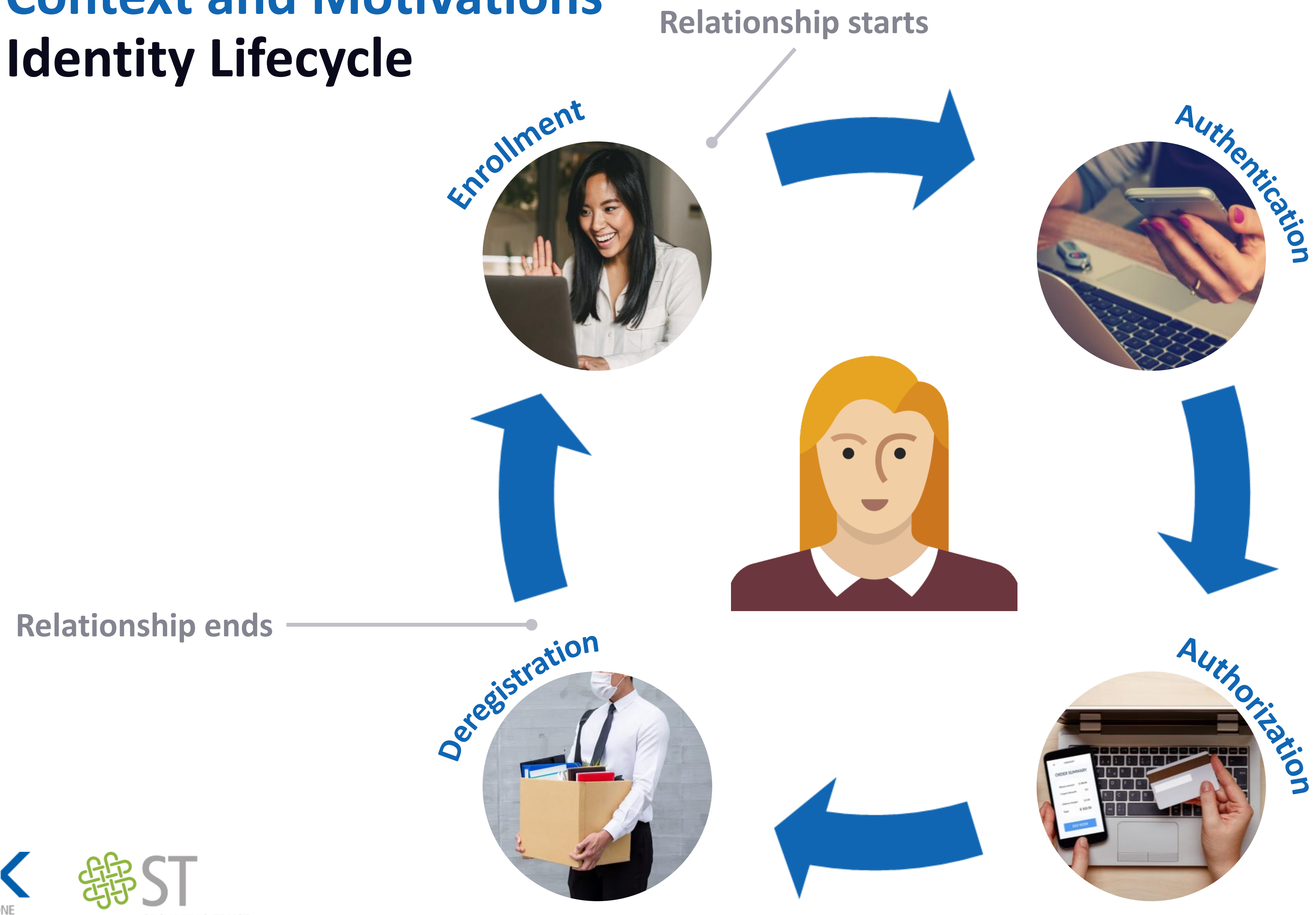
Context and Motivations
Identity Verification

Physical identification

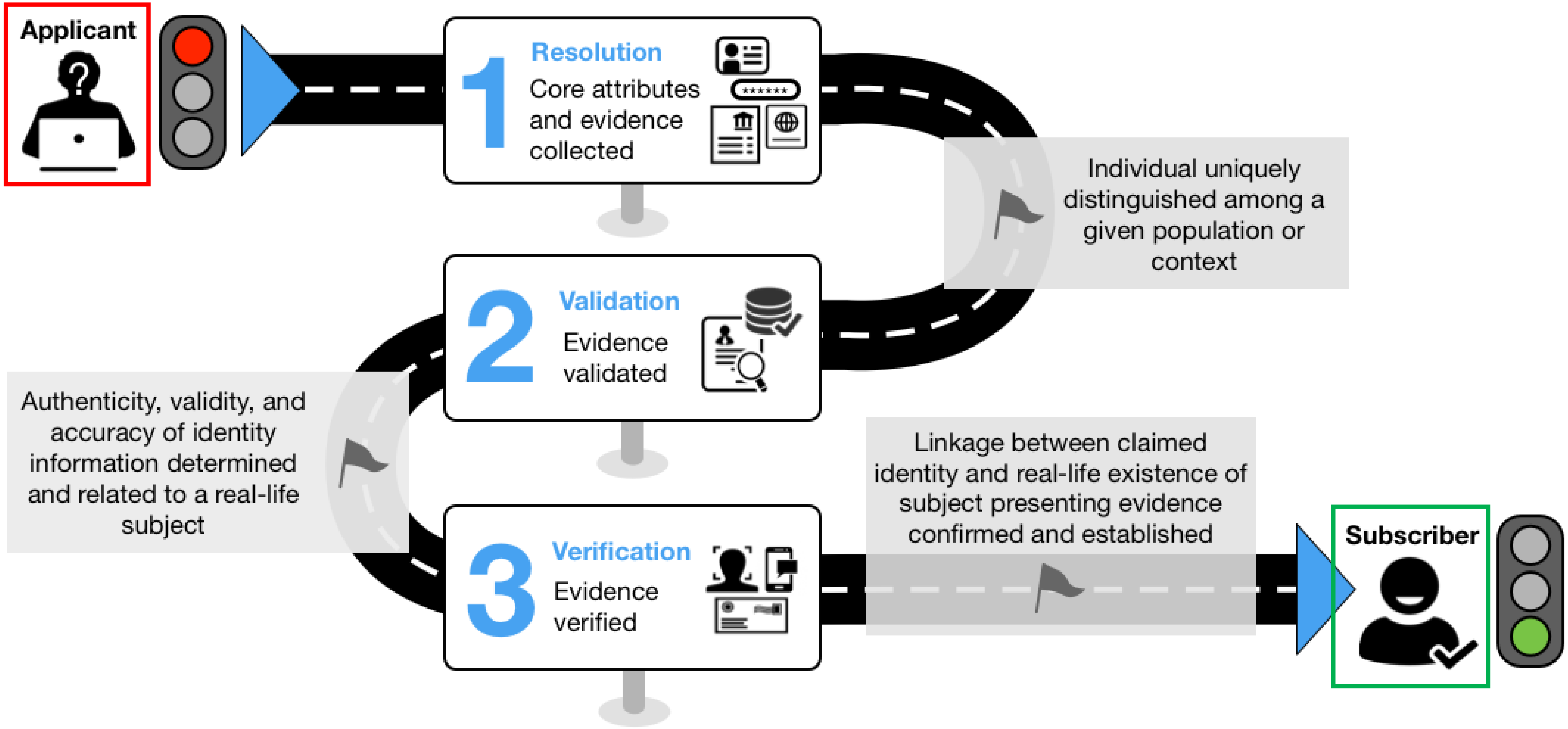
Remote identification

Context and Motivations

Identity Lifecycle



Context and Motivations
Enrollment

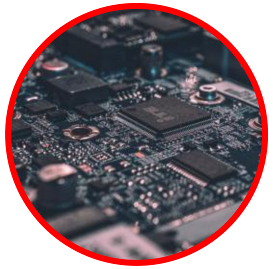


Applicant
1
Resolution
Core attributes and evidence collected
****
Individual uniquely distinguished among a given population or context
2
Validation
Evidence validated
Authenticity, validity, and accuracy of identity information determined and related to a real-life subject
3
Verification
Evidence verified
Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established
Subscriber

Source: NIST Special Publication 800-63A

Context and Motivations
Problems

Involving human operators for identification may slow down the process depending on the workload



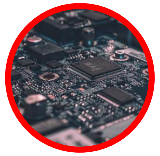
Requiring people to leverage additional devices may restrict the number of people using the protocol

Requiring too complex actions may prevent less-expert people from using the protocol

Context and Motivations
Requirements

An enrollment procedure should:

be carried out remotely and automatically, without human operators for identification

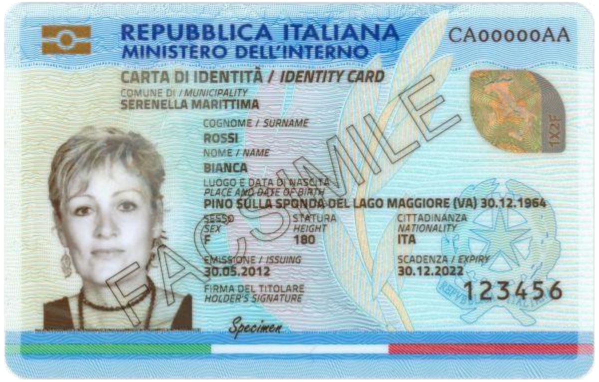


rely on devices that people already own

provide an adequate level of usability, thus allowing everyone to finalise it

Context and Motivations
eDocuments

- Official identity documents in many countries.



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

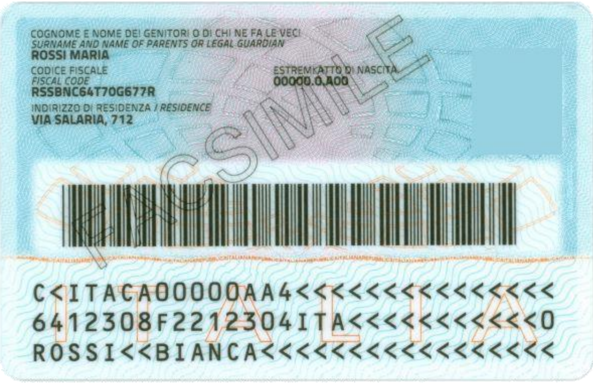
SCADENZA / *EXPIRY*
30.12.2022

FIRMA DEL TITOLARE
HOLDER'S SIGNATURE
Specimen

123456

1X2F

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

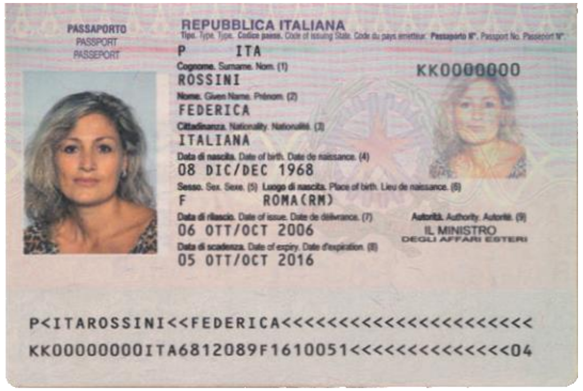
ESTREMI ATTO DI NASCITA
00000.0.A00

INDIRIZZO DI RESIDENZA / *RESIDENCE*
VIA SALARIA, 712

FACSIMILE

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

ITALIA



PASSAPORTO
PASSPORT
PASSEPORT

REPUBBLICA ITALIANA

Tipo. Type. Type. Codice paese. Code of issuing State. Code du pays emetteur. Passaporto N°. Passport No. Passeport N°.
P ITA

KK0000000

Cognome. Surname. Nom. (1)
ROSSINI

Nome. Given Name. Prénom. (2)
FEDERICA

Cittadinanza. Nationality. Nationalité. (3)
ITALIANA

Data di nascita. Date of birth. Date de naissance. (4)
08 DIC/DEC 1968

Sesso. Sex. Sexe. (5) Luogo di nascita. Place of birth. Lieu de naissance. (6)
F ROMA(RM)

Data di rilascio. Date of issue. Date de délivrance. (7)
06 OTT/OCT 2006

Autorità. Authority. Autorité. (9)
IL MINISTRO
DEGLI AFFARI ESTERI

Data di scadenza. Date of expiry. Date d'expiration. (8)
05 OTT/OCT 2016

P<ITAROSSINI<<FEDERICA<<<<<<<<<<<<<<<<<<<<<<<<
KK00000000ITA6812089F1610051<<<<<<<<<<<<<<<04

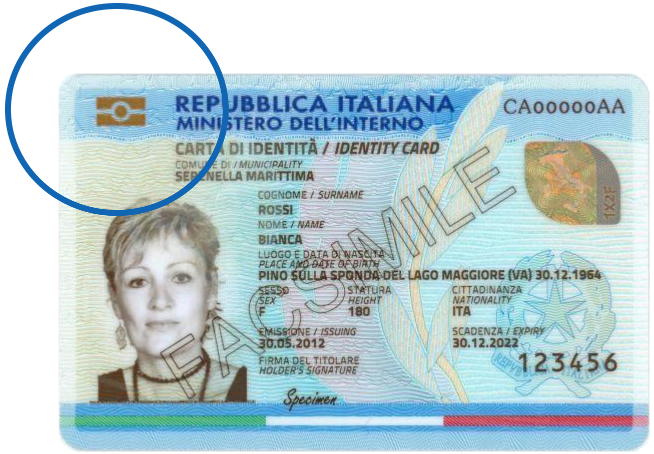
* * * *

PIN code

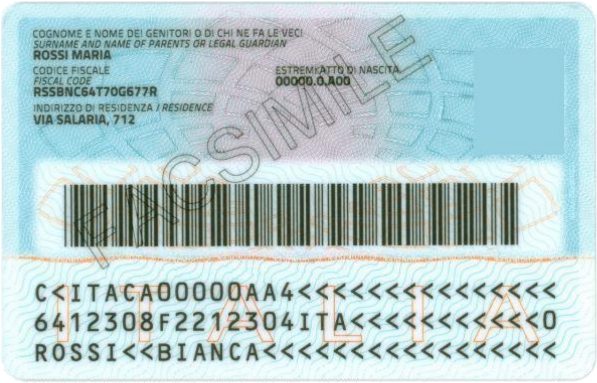
Context and Motivations
eDocuments

- Official identity documents in many countries.

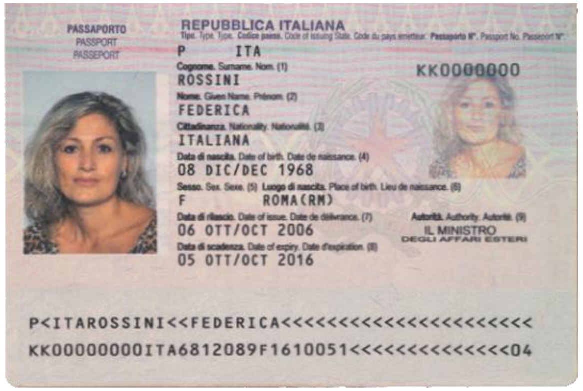
- Equipped with:
    - a contactless chip;


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
FACSIMILE
1X2F

UNIONE EUROPEA
REPUBBLICA ITALIANA
PASSAPORTO


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
ITALIA

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


PASSAPORTO
PASSPORT
PASSEPORT
REPUBBLICA ITALIANA
Tipo. Type. Type. Codice paese. Code of issuing State. Code du pays emetteur. Passaporto N°. Passport No. Passeport N°.
P ITA KK0000000
Cognome. Surname. Nom. (1)
ROSSINI
Nome. Given Name. Prénom. (2)
FEDERICA
Cittadinanza. Nationality. Nationalité. (3)
ITALIANA
Data di nascita. Date of birth. Date de naissance. (4)
08 DIC/DEC 1968
Sesso. Sex. Sexe. (5) Luogo di nascita. Place of birth. Lieu de naissance. (6)
F ROMA(RM)
Data di rilascio. Date of issue. Date de délivrance. (7)
06 OTT/OCT 2006
Autorità. Authority. Autorité. (9)
IL MINISTRO
DEGLI AFFARI ESTERI
Data di scadenza. Date of expiry. Date d'expiration. (8)
05 OTT/OCT 2016

```
P<ITAROSSINI<<FEDERICA<<<<<<<<<<<<<<<<<<<<<<<<
KK00000000ITA6812089F1610051<<<<<<<<<<<<<<<04
```

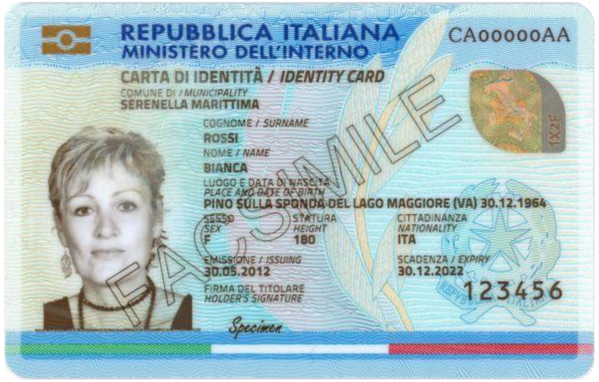
* * * *

PIN code

Context and Motivations
eDocuments

- Official identity documents in many countries.

- Equipped with:
  - a contactless chip;
  - 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

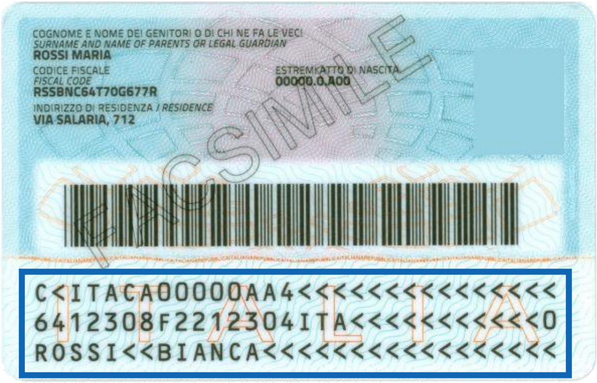
LUOGO E DATA DI NASCITA
PLACE AND DATE OF BIRTH
PINO SULLA SPONDA DEL LAGO MAGGIORE (VA) 30.12.1964

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



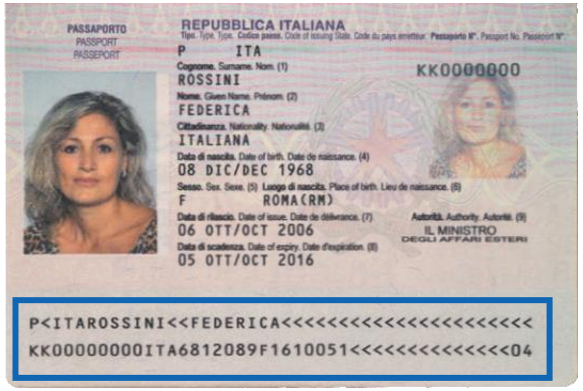
COGNOME E NOME DEI GENITORI O DI CHI NE FA LE VECI
SURNAME AND NAME OF PARENTS OR LEGAL GUARDIAN
ROSSI MARIA

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<<<<<<<<<<<<<<<<<
```



PASSAPORTO
PASSPORT
PASSEPORT

REPUBBLICA ITALIANA
Tipo. Type. Type. Codice paese. Code of issuing State. Code du pays emetteur. Passaporto N°. Passport No. Passeport N°.
P ITA KK0000000

Cognome. Surname. Nom. (1)
ROSSINI

Nome. Given Name. Prénom. (2)
FEDERICA

Cittadinanza. Nationality. Nationalité. (3)
ITALIANA

Data di nascita. Date of birth. Date de naissance. (4)
08 DIC/DEC 1968

Sesso. Sex. Sexe. (5) Luogo di nascita. Place of birth. Lieu de naissance. (6)
F ROMA(RM)

Data di rilascio. Date of issue. Date de délivrance. (7)
06 OTT/OCT 2006

Autorità. Authority. Autorité. (9)
IL MINISTRO
DEGLI AFFARI ESTERI

Data di scadenza. Date of expiry. Date d'expiration. (8)
05 OTT/OCT 2016

```
P<ITAROSSINI<<FEDERICA<<<<<<<<<<<<<<<<<<<<<<
KK00000000ITA6812089F1610051<<<<<<<<<<<<<<04
```

```
* * * *
```

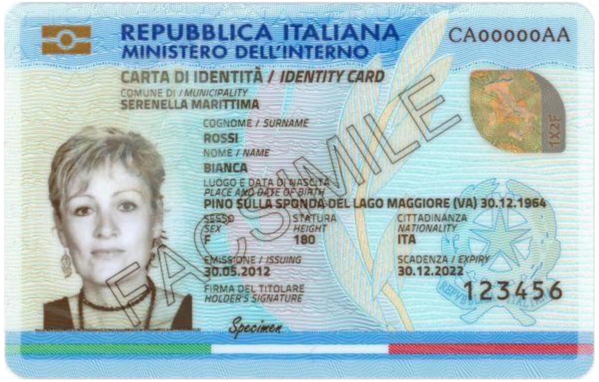
PIN code

Context and Motivations
eDocuments

- Official identity documents in many countries.

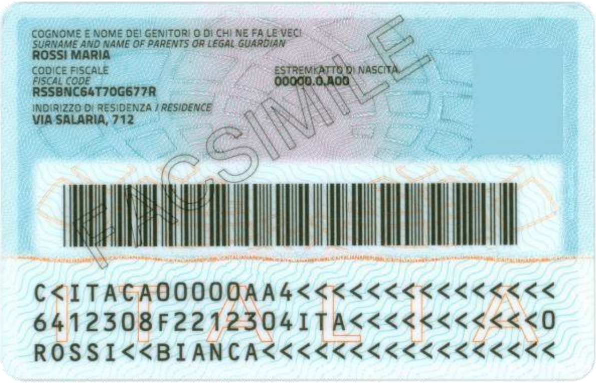
- Equipped with:
  - a contactless chip;
  - a machine-readable zone (MRZ).

- Personal data of the owner are printed on the surface…
  - … as well as stored within the eDocument.



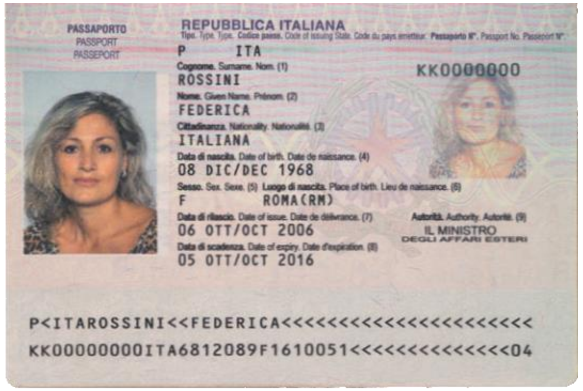
REPUBBLICA ITALIANA
MINISTERO DELL'INTERNO
CA00000AA
CARTA DI IDENTITÀ / *IDENTITY CARD*
COMUNE DI / *MUNICIPALITY*
SERENELLA MARITTIMA
COGNOME / *SURNAME*
ROSSI
NOME / *NAME*
BIANCA
LUOGO E DATA DI NASCITA
PLACE AND DATE OF BIRTH
PINO SULLA SPONDA DEL LAGO MAGGIORE (VA) 30.12.1964
SESSO *SEX* F
STATURA *HEIGHT* 180
CITTADINANZA *NATIONALITY* ITA
EMISSIONE / *ISSUING* 30.05.2012
SCADENZA / *EXPIRY* 30.12.2022
FIRMA DEL TITOLARE
HOLDER'S SIGNATURE
Specimen
123456
FACSIMILE

UNIONE EUROPEA
REPUBBLICA ITALIANA
REPVBBLICA ITALIANA
PASSAPORTO



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<<<<<<<<<<<<<<<<<
```



PASSAPORTO
PASSPORT
PASSEPORT
REPUBBLICA ITALIANA
Tipo. Type. Type. Codice paese. Code of issuing State. Code du pays emetteur. Passaporto N°. Passport No. Passeport N°.
P ITA KK0000000
Cognome. Surname. Nom. (1)
ROSSINI
Nome. Given Name. Prénom. (2)
FEDERICA
Cittadinanza. Nationality. Nationalité. (3)
ITALIANA
Data di nascita. Date of birth. Date de naissance. (4)
08 DIC/DEC 1968
Sesso. Sex. Sexe. (5) Luogo di nascita. Place of birth. Lieu de naissance. (6)
F ROMA(RM)
Data di rilascio. Date of issue. Date de délivrance. (7)
06 OTT/OCT 2006
Autorità. Authority. Autorité. (9)
IL MINISTRO
DEGLI AFFARI ESTERI
Data di scadenza. Date of expiry. Date d'expiration. (8)
05 OTT/OCT 2016

```
P<ITAROSSINI<<FEDERICA<<<<<<<<<<<<<<<<<<<<<<
KK00000000ITA6812089F1610051<<<<<<<<<<<<<<04
```

* * * *

PIN code

Context and Motivations
Requirements

✓

eDocuments and the attested data can be verified through automatic procedures

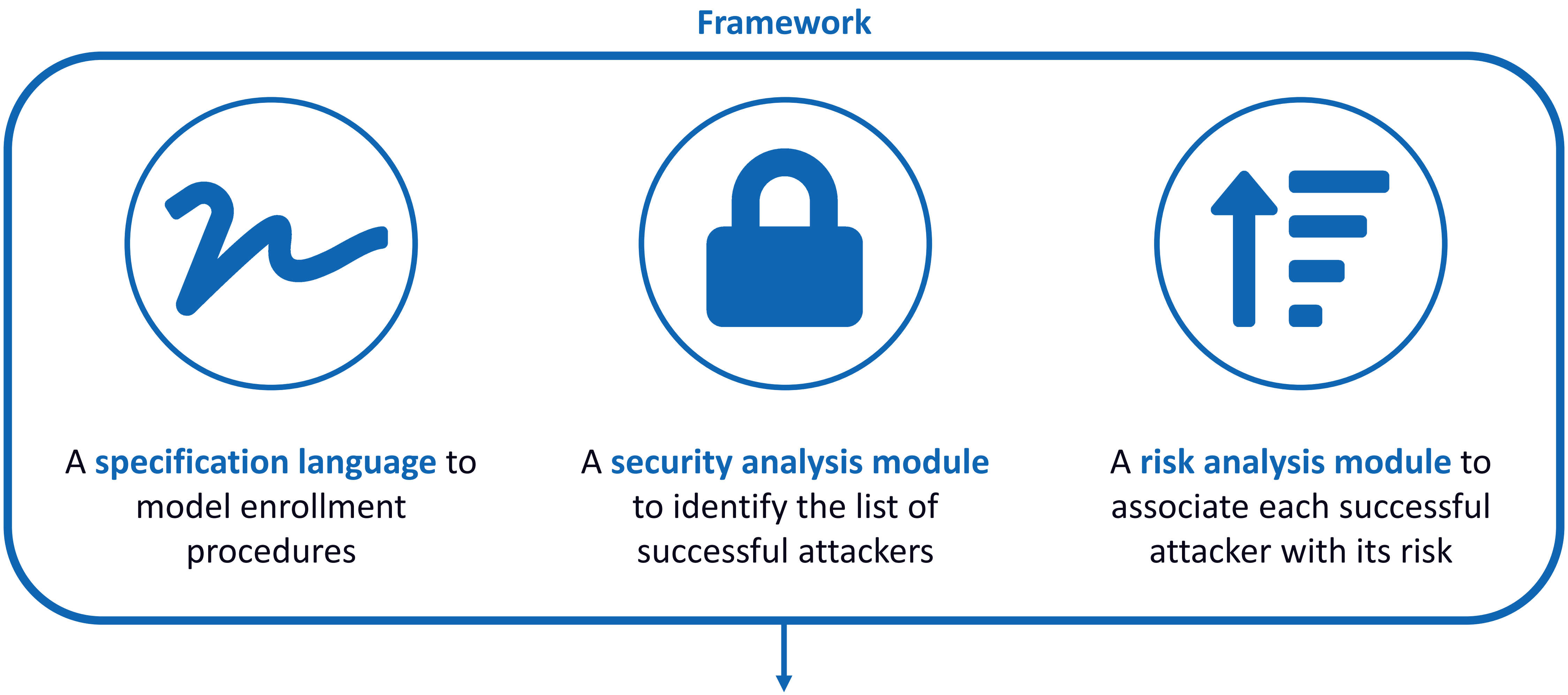
✓

eDocuments can be read through the NFC capabilities of common devices such as smartphones

✓

Personal data can be extracted from eDocuments and use to automatically fill the form

Contributions



Framework

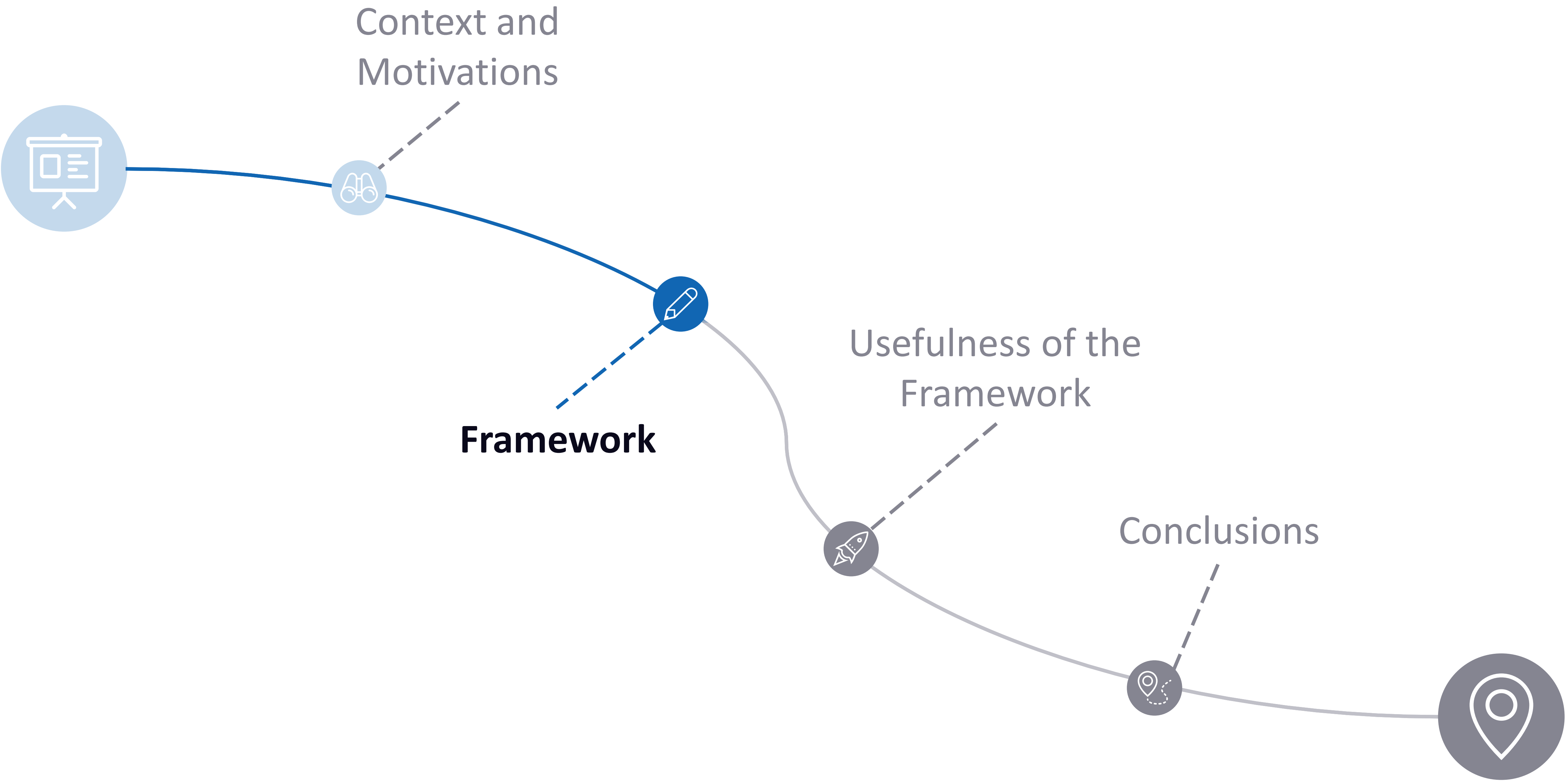
A **specification language** to model enrollment procedures

A **security analysis module** to identify the list of successful attackers

A **risk analysis module** to associate each successful attacker with its risk

Application to an enrollment procedure based on eDocuments

Agenda



Context and Motivations

Framework

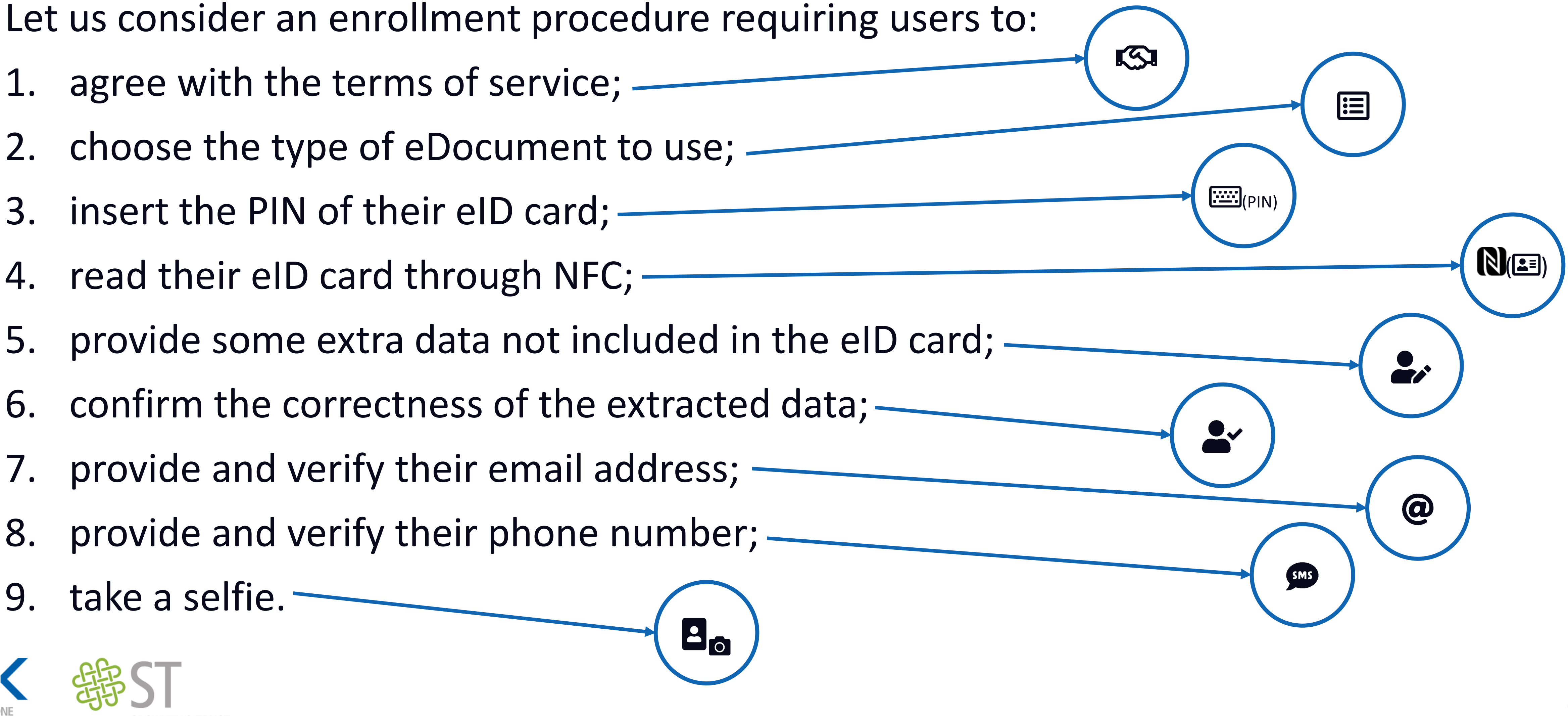
Usefulness of the Framework

Conclusions

Framework
Specification Language

Basic entities			
🪪	The eID card	🛂	The ePassport
📛	An additional personal document	PIN	The PIN of the eID card
▮▮▮	The MRZ printed on the eDocument	👤	The selfie captured by the user
Actions *The user may be required to…*			
🤝	agree with the privacy policy	☰	choose the eDocument to use and the interaction mode
👤✎	provide some extra information that is not included in the eDocument	👤✓	check and confirm the correctness of her personal data extracted from the eDocument
@	insert her email address and verify it	SMS	insert her phone number and verify it
👤📷	capture a photo selfie; in case it needs to contain an additional element, this will be specified as argument	Ⓝ(•)	place the element specified as argument near the device, so as to interact with it through NFC
👤📹	capture a video selfie	⛶(•)	scan the element specified as argument through the device's camera
📷(•)	take a picture of the argument	⌨(•)	insert the information specified as argument

Framework
Specification Language – Example



Let us consider an enrollment procedure requiring users to:

1. agree with the terms of service;
2. choose the type of eDocument to use;
3. insert the PIN of their eID card;
4. read their eID card through NFC;
5. provide some extra data not included in the eID card;
6. confirm the correctness of the extracted data;
7. provide and verify their email address;
8. provide and verify their phone number;
9. take a selfie.

Framework
Specification Language – Example

Let us consider an enrollment procedure requiring users to:

1. agree with the terms of service;
2. choose the type of eDocument to use;
3. insert the PIN of their eID card;
4. read their eID card through NFC;
5. provide some extra data not included in the eID card;
6. confirm the correctness of the extracted data;
7. provide and verify their email address;
8. provide and verify their phone number;
9. take a selfie.

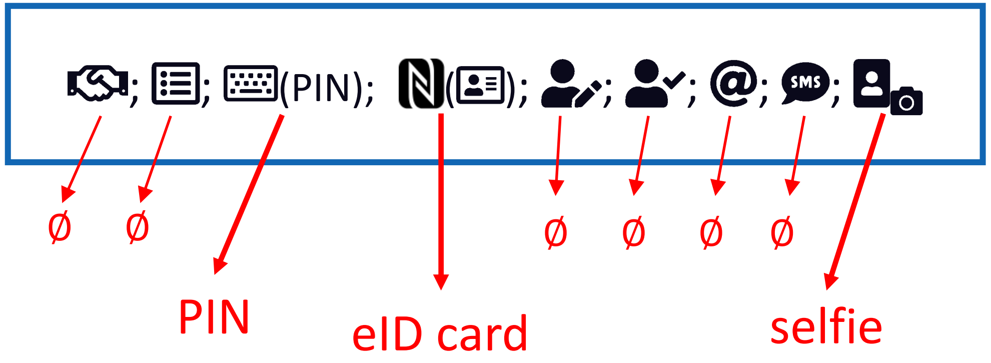
🤝; ☰; ⌨ (PIN); Ⓝ(🪪); 👤✎; 👤✓; @; 💬; 👤📷

Framework

Security Analysis – Identification Factors

- Authentication factors are defined by NIST in authentication contexts.
  - Nothing similar has been defined in enrollment contexts!

- We introduce the notion of identification factors.
  - Some actions may attest an identification factor…
  - … while some other may not.



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

$\mathcal{SG} = \{$🪪 ; PIN; 👤$\}$

Framework
Security Analysis – Threat Model

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

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

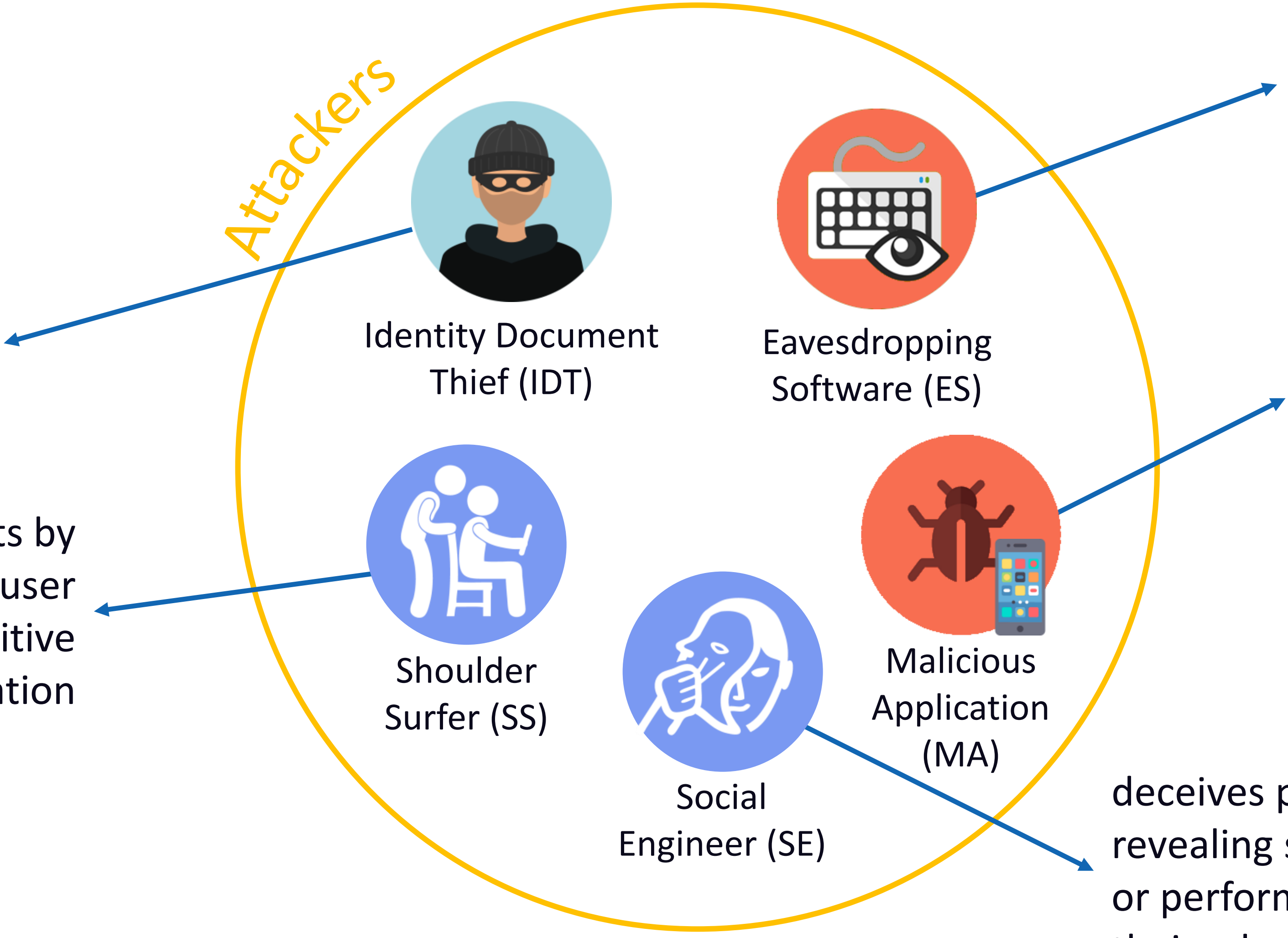
where:

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

Framework

Security Analysis – Threat Model

$$\boxed{\mathcal{TM} = (\mathcal{ATT}; \mathcal{C})}$$



Attackers

Identity Document Thief (IDT)

Eavesdropping Software (ES)

Shoulder Surfer (SS)

Social Engineer (SE)

Malicious Application (MA)

steals an identity document from its legitimate owner

intercepts the data typed on the device (e.g., keylogger);

obtains secrets by looking at the user inserting sensitive information

runs on the attacker's or the victim's mobile device

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

Framework
Security Analysis – Threat Model

$$\mathcal{TM} = (\mathcal{ATT}; \boldsymbol{\mathcal{C}})$$

Capabilities

Attacker	🪪	PIN	👤
Identity Document Thief	🔓	🔒	🔒
Eavesdropping Software	🔒	🔓	🔒
Shoulder Surfer	🔒	🔓	🔒
Social Engineer	🔒	🔓	🔒
Malicious Application	🔓*	🔓	🔓

can only compromise the eDocument (by stealing it)

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

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 compromise the eDocument (indirectly, by deceiving the victim into interact with it), the PIN (by eavesdropping it while it is being typed) and the selfie (by secretly taking a picture of her)

Framework

Security Analysis

- An enrollment 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.

$\mathcal{SG} = \{$🪪$; PIN;$👤$\}$

Capabilities

Attacker	🪪	PIN	👤
Identity Document Thief	🔓	🔒	🔒
Eavesdropping Software	🔒	🔓	🔒
Shoulder Surfer	🔒	🔓	🔒
Social Engineer	🔒	🔓	🔒
Malicious Application	🔓*	🔓	🔓

Framework
Security Analysis

$\mathcal{SG} = \{🪪; PIN; 👤\}$

- An enrollment 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 $\mathcal{SG}$.

Capabilities

Attacker	🪪	PIN	👤
Identity Document Thief	🔓	🔒	🔒
Eavesdropping Software	🔒	🔓	🔒
Shoulder Surfer	🔒	🔓	🔒
Social Engineer	🔒	🔓	🔒
Malicious Application	🔓*	🔓	🔓

Minimal subset

Non-minimal subset

Framework
Security Analysis Problem

The **security analysis problem** for an enrollment 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 $\mathcal{SG}$.

Framework
Risk Analysis

Probability of the attack

Consequences in case the attack has occurred

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

Likelihood					Impact	
Technical Difficulty (TD)	Opportunity (O)	Attack Vector (AV)	User Interaction needed (UI)	Spread of Attack (SA)	Attack Scale (AS)	Attack Detection (AD)

Framework

Risk Analysis

Att.	Likelihood							Impact				Risk
	TD	O	AV	UI	SA	Aver.	Over.	AS	AD	Aver.	Over.	
MA	3	2	7	1	4	3.40	Med.	8	6	7.00	High	High

1. Assign a score (0-9) to each factor

Framework
Risk Analysis

Att.	Likelihood							Impact				Risk
	TD	O	AV	UI	SA	Aver.	Over.	AS	AD	Aver.	Over.	
MA	3	2	7	1	4	3.40	Med.	8	6	7.00	High	High

1. Assign a score (0-9) to each factor

2. Compute the average of likelihood and impact factors

Framework

Risk Analysis

Att.	Likelihood							Impact				Risk
	TD	O	AV	UI	SA	Aver.	Over.	AS	AD	Aver.	Over.	
MA	3	2	7	1	4	3.40	Med.	8	6	7.00	High	High

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

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

FONDAZIONE BRUNO KESSLER

SECURITY & TRUST

Framework
Risk Analysis

Att.	Likelihood							Impact				Risk
	TD	O	AV	UI	SA	Aver.	Over.	AS	AD	Aver.	Over.	
MA	3	2	7	1	4	3.40	Med.	8	6	7.00	High	High

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

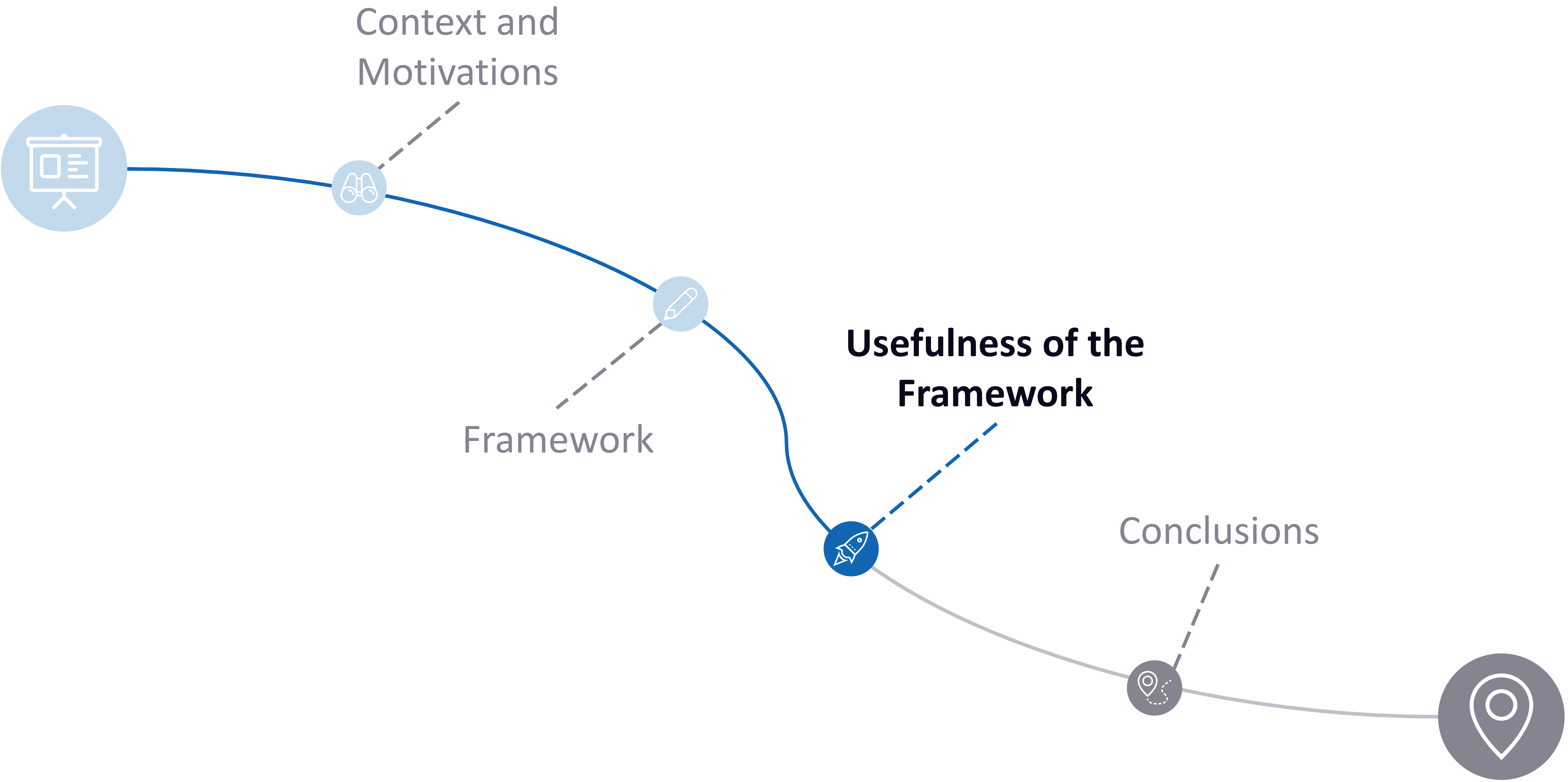
		Likelihood		
		Low	*Medium*	*High*
Impact	*Low*	Note	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

Framework

Risk Analysis Problem

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 $\mathcal{SG}$.

Agenda



Context and Motivations

Framework

Usefulness of the Framework

Conclusions

Usefulness of the Framework

- The framework can be used to model and analyse the security and risk of any enrollment procedure.
    - The specification language and the threat model can be fully customised and adapted (if necessary) to the considered scenario.

- The results of the framework can be used to properly tune the security level of enrollment procedures depending on the specific needs.

- The framework also allows *what-if analyses*, by providing information on how specific mitigations affect the set of successful attackers and their risks.

Usefulness of the Framework
Mitigations

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

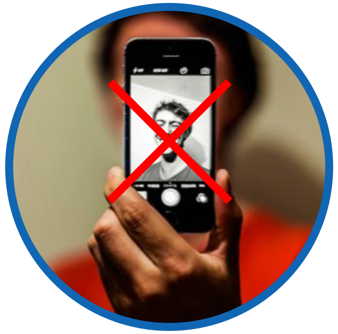
- Therefore:
  - some attackers may be completely prevented, in case they no longer manage to compromise the procedure;
  - some attackers may remain successful, but with a lower level of risk.

Usefulness of the Framework
Mitigations – Example

Require users to capture a selfie at that moment, preventing the upload of existent files.

✓

SE cannot obtain a picture of the victim and upload it during the process



Force the user to capture the selfie from the front camera.

✓

SS cannot take a picture of another person in proximity

Implement liveness detection to detect the misuse of static or modified pictures.

✓ ↓

SE cannot use static pictures, and **SS** is less likely able to obtain pictures of people in proximity

Usefulness of the Framework

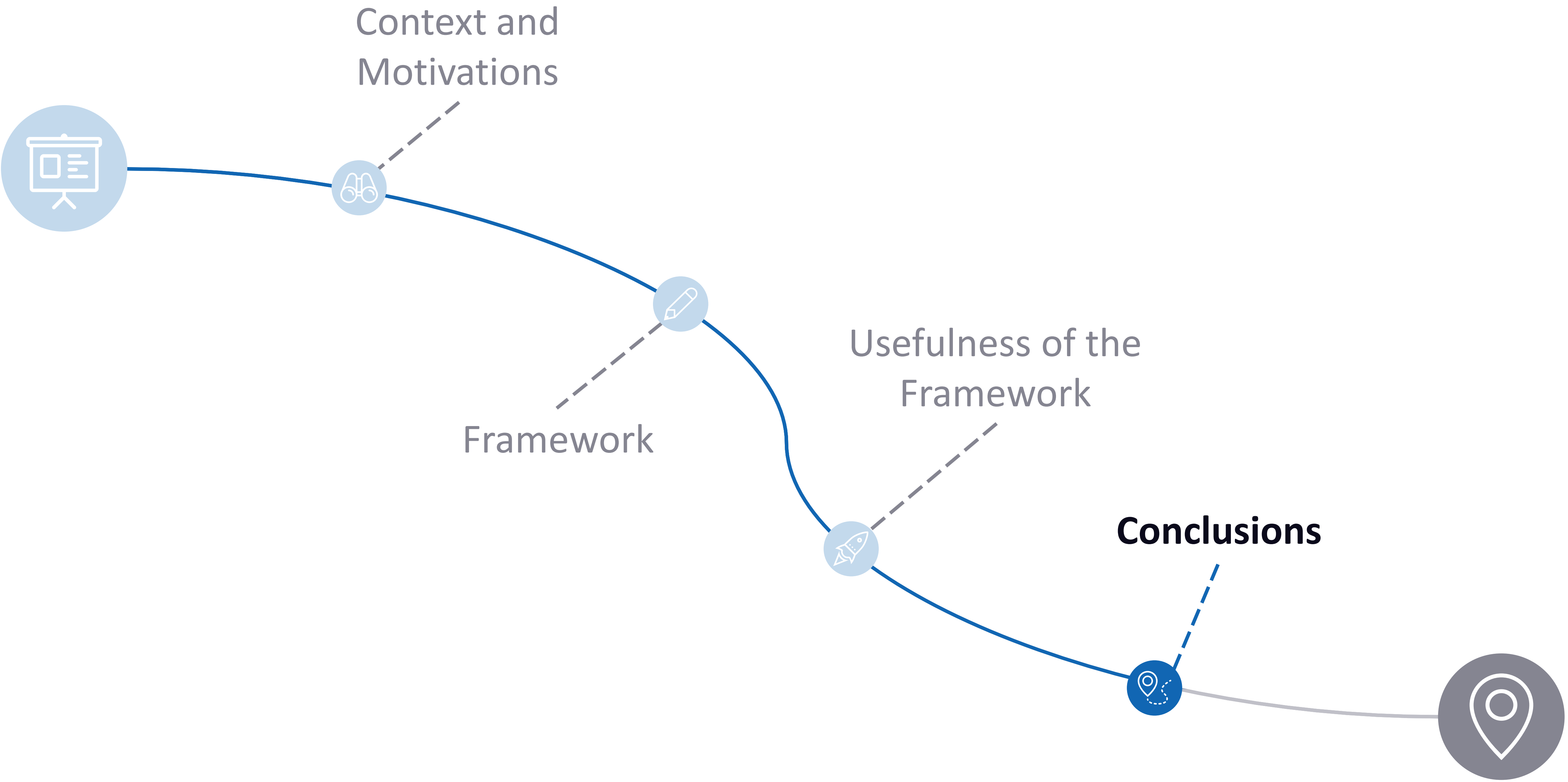
Mitigations – Effects on the Considered Protocol

Sc.	Att.	Likelihood							Impact				Risk
		TD	O	AV	UI	SA	Aver.	Over.	AS	AD	Aver.	Over.	
1	MA	6	9	7	7	6	7.00	High	9	8	8.50	High	Critical
2	MA	3	2	7	1	4	3.40	Med.	8	6	7.00	High	High

↓

Sc.	Att.	Likelihood							Impact				Risk
		TD	O	AV	UI	SA	Aver.	Over.	AS	AD	Aver.	Over.	
1	MA	**3**	**1**	7	**1**	**2**	**2.80**	**Low**	**8**	**7**	**7.50**	High	**Medium**
2	MA	**2**	**1**	7	1	**2**	**2.60**	**Low**	8	**5**	**6.50**	High	**Medium**

Agenda



Context and Motivations

Framework

Usefulness of the Framework

Conclusions

Conclusions

- We have proposed a framework for the analysis of enrollment procedures:
  - a specification language provides a clear and graphical description of such protocols;
  - a security analysis methodology computes the list of successful attackers;
  - a risk analysis methodology allows to sort the successful attackers according to their severity.

- We have applied the proposed framework to fully-remote solutions relying on eDocuments as identity evidence, within a collaboration with the Italian FinTech startup CherryChain.
  - We could contextualize our work in a practical use case.
  - Our framework allowed CherryChain to verify the security of the protocols they were designing, also identifying the mitigations to implement after discussing their benefits in terms of security and feasibility.

Future Work

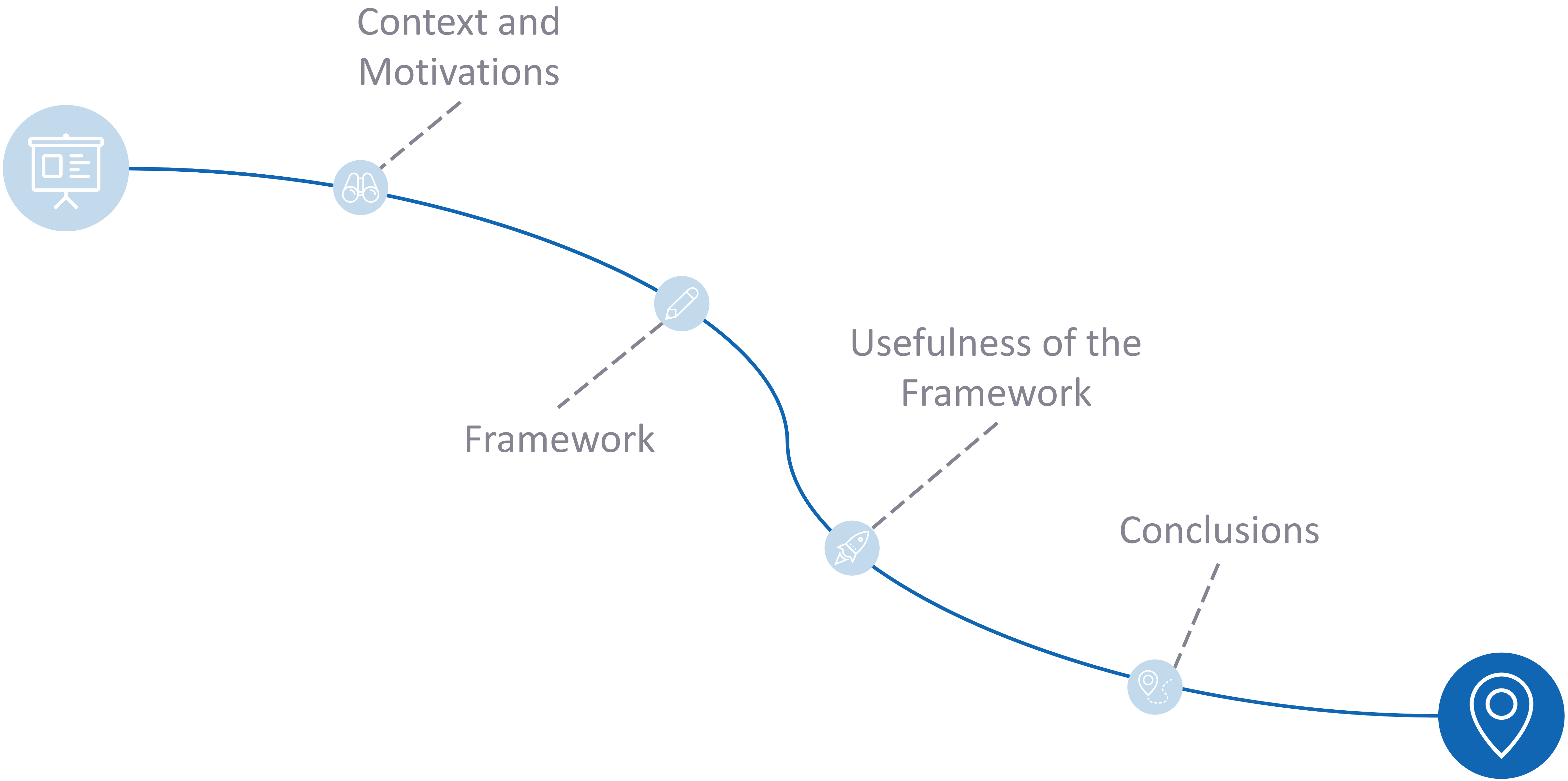
Enrich the specification language to naturally support a wider range of enrollment procedures, even based on different requirements.

Formalise the proposed framework through formal definitions and pseudocodes that can be easily implemented within an automatic tool.

Extend our work by taking inspiration from a report by ENISA [1] released after this work was already completed.

[1] European Union Agency for Cybersecurity (ENISA). "Remote ID Proofing". https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing

Agenda



Context and Motivations

Framework

Usefulness of the Framework

Conclusions

Thanks for your attention!

Marco Pernpruner
mpernpruner@fbk.eu

Giada Sciarretta
giada.sciarretta@fbk.eu

Silvio Ranise
ranise@fbk.eu

🌐 https://st.fbk.eu

FONDAZIONE BRUNO KESSLER

CherryChain®

The research has been partly supported by **CherryChain S.r.l.** and **Poligrafico e Zecca dello Stato Italiano** (IPZS).

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

ST SECURITY & TRUST