INFOCERT
TINEXTA GROUP

# A MODEL THEORETIC APPROACH TO DIGITAL IDENTITY

TDI – Feb 3 2025

l. boldrin

infocert.it infocert.digital

INFOCERT
TINEXTA GROUP

# AGENDA

➡ Semantics of W3C data model

Modeling identity in the physical /digital world

A basic calculus

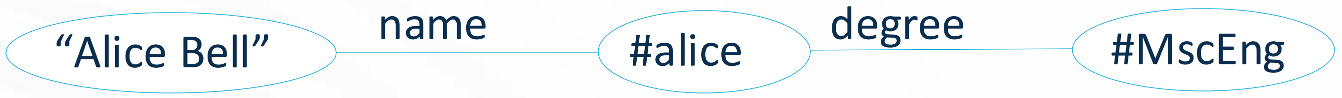
An extended calculus (sketch)

Practical conclusions

# SEMANTICS OF W3C DATA MODEL

W3C data model is based

on RDF/Linked Data:



RDF

```
<rdf:Description about= "#alice”
    <ns:name “Alice Bell”>
    <ns:degree “#MscEng">
</rdf:Description>
```

XML serialization

```
{
    "@context": {…},
    …,
    "credentialSubject": {
        "@id": ”#alice",
        "ns:name": ”Alice Bell",
        "ns:degree": ”#MscEng ”
    }
}
```

JSON-LD representation

# SEMANTICS OF W3C DATA MODEL

```
{
    "@context": {…},
    …,
    "credentialSubject": {
        "@id": ”#alice",
        "ns:name": ”Alice Bell",
        "ns:degree": ”#MscEng”
    }
}
```

Semantics: entity “#alice” is associated with entity “Alice Bell” via relation “name” and with entity “#MscEng” via relation “degree” (leveraging on RFD formal semantics: https://www.w3.org/TR/rdf-mt/)

Issues:

- mixing entities and attributes
- requires identifiers (even if W3C data model does not prescribe it)

# AGENDA

Semantics of W3C data model

➡ Modeling identity in the physical /digital world

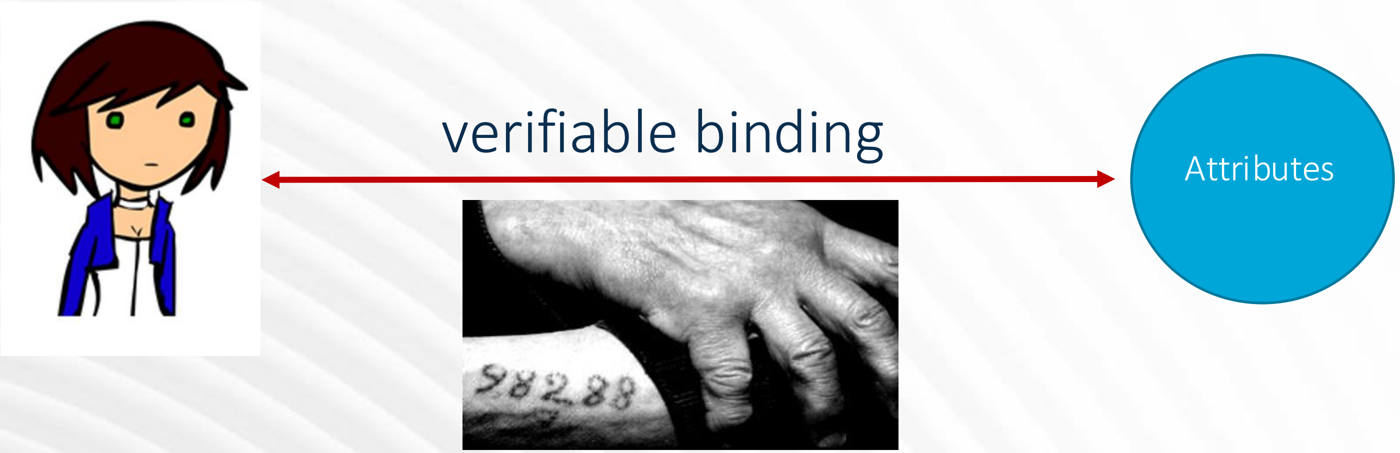
A basic calculus

An extended calculus (sketch)

Practical conclusions

# MODELING PRE-DIGITAL IDENTITY

Real
Alice

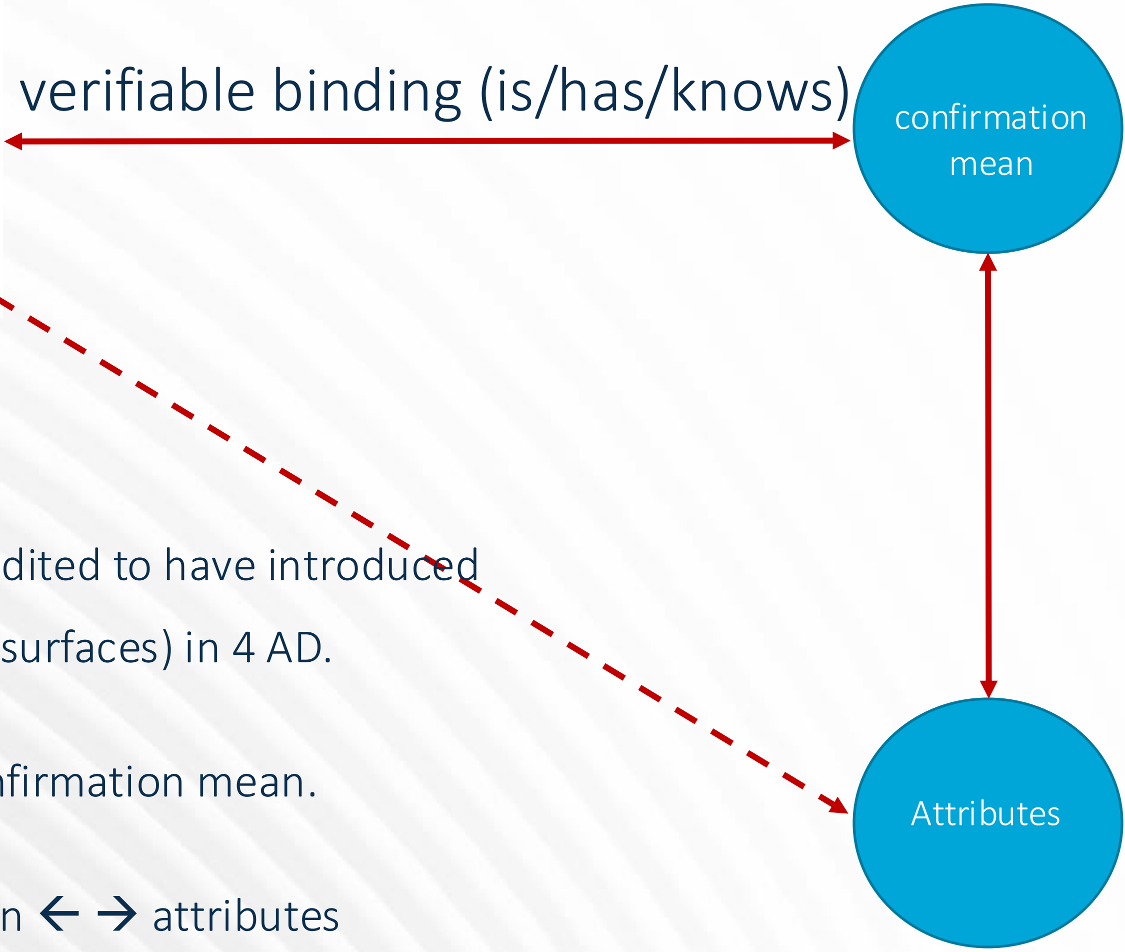


Name: Alice Bell
Date of birth: 31/12/2001
BloodType: A
ID:98288
...

physical binding (tattoo)

# MODELING PRE-DIGITAL IDENTITY

Real
Alice



Name:
Alice Bell
DateOfBirth:
31/12/2001
BloodType: A
ID:98288

Name: Alice Bell
DateOfBirth: 31/12/2001
BloodType: A
ID:98288
...

Roman emperor Augustus (27 BC–14 AD) is credited to have introduced birth certificates (wooden diptych with waxed surfaces) in 4 AD.

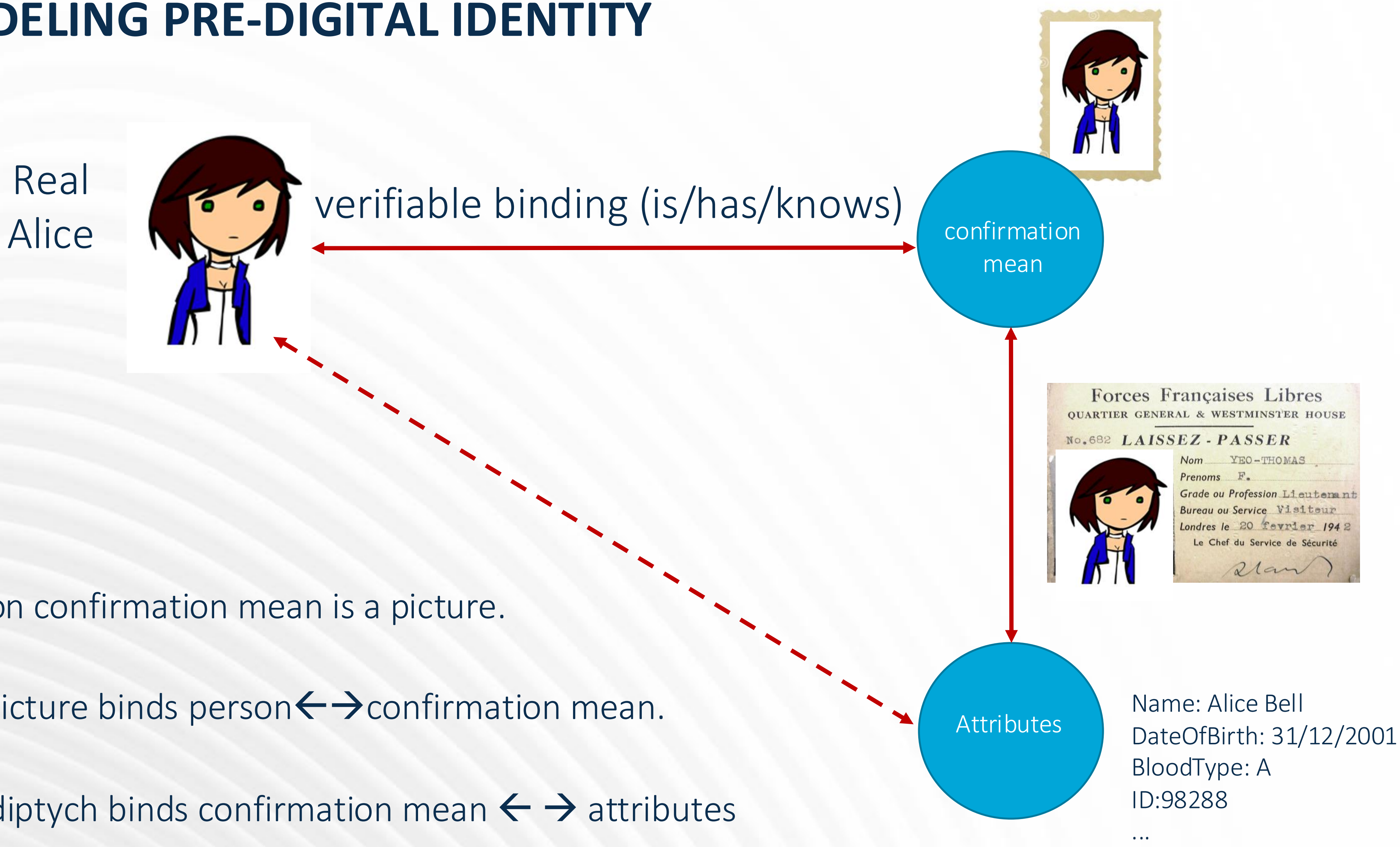
Possession of the diptych binds person←→confirmation mean.

Content of the diptych binds confirmation mean ← → attributes

But possession is weak…

01/02/2025

# MODELING PRE-DIGITAL IDENTITY



Forces Françaises Libres
QUARTIER GENERAL & WESTMINSTER HOUSE
No.682 LAISSEZ - PASSER
Nom YEO-THOMAS
Prenoms F.
Grade ou Profession Lieutenant
Bureau ou Service Visiteur
Londres le 20 fevrier 1942
Le Chef du Service de Sécurité

Name: Alice Bell
DateOfBirth: 31/12/2001
BloodType: A
ID:98288
…

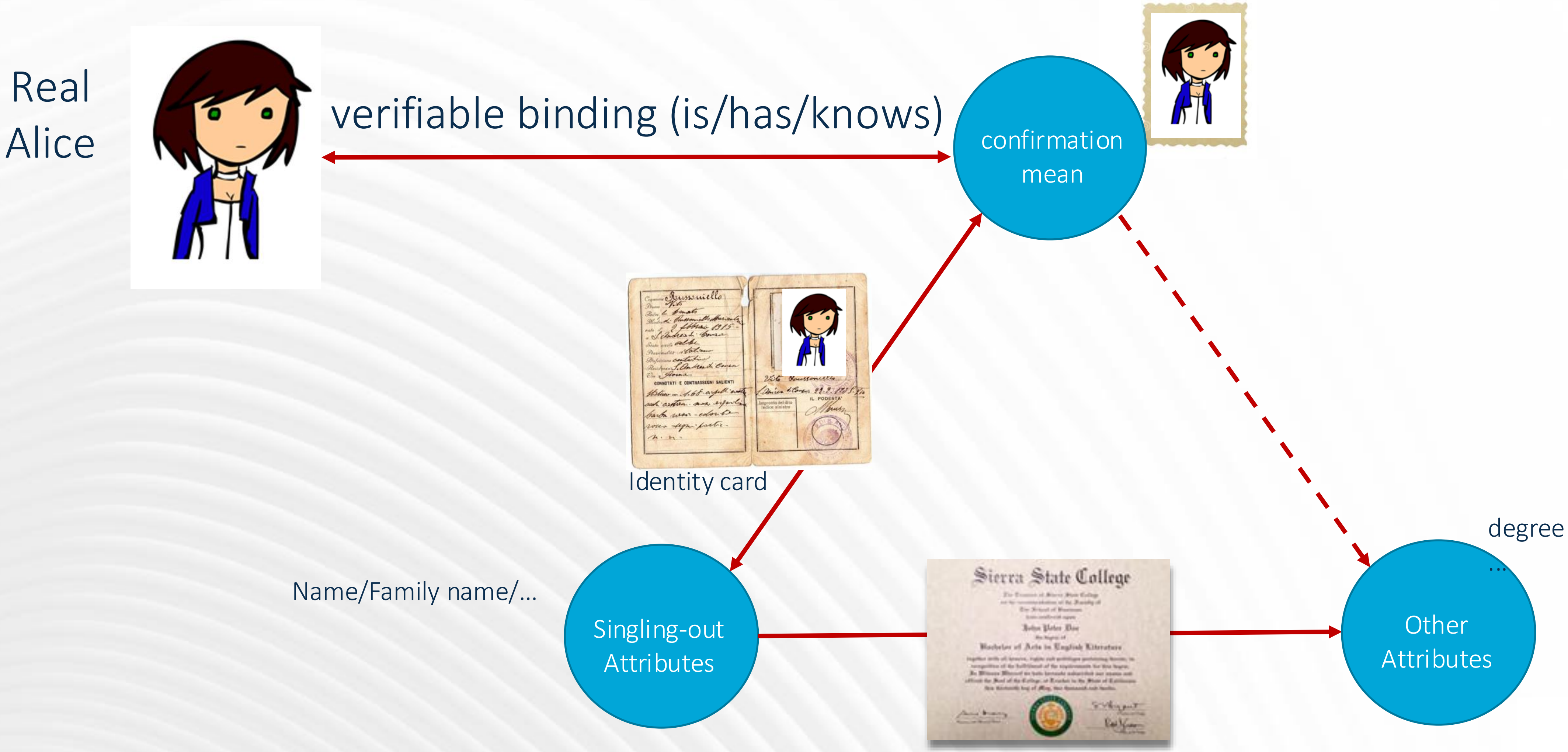
Now, a very  common confirmation mean is a picture.

Matching with the picture binds person←→confirmation mean.

A document of the diptych binds confirmation mean ← → attributes

# MODELING PRE-DIGITAL IDENTITY

Not all attributes are equal: some are "singling out" attributes



Real Alice

verifiable binding (is/has/knows)

confirmation mean

Identity card

Name/Family name/...

Singling-out Attributes

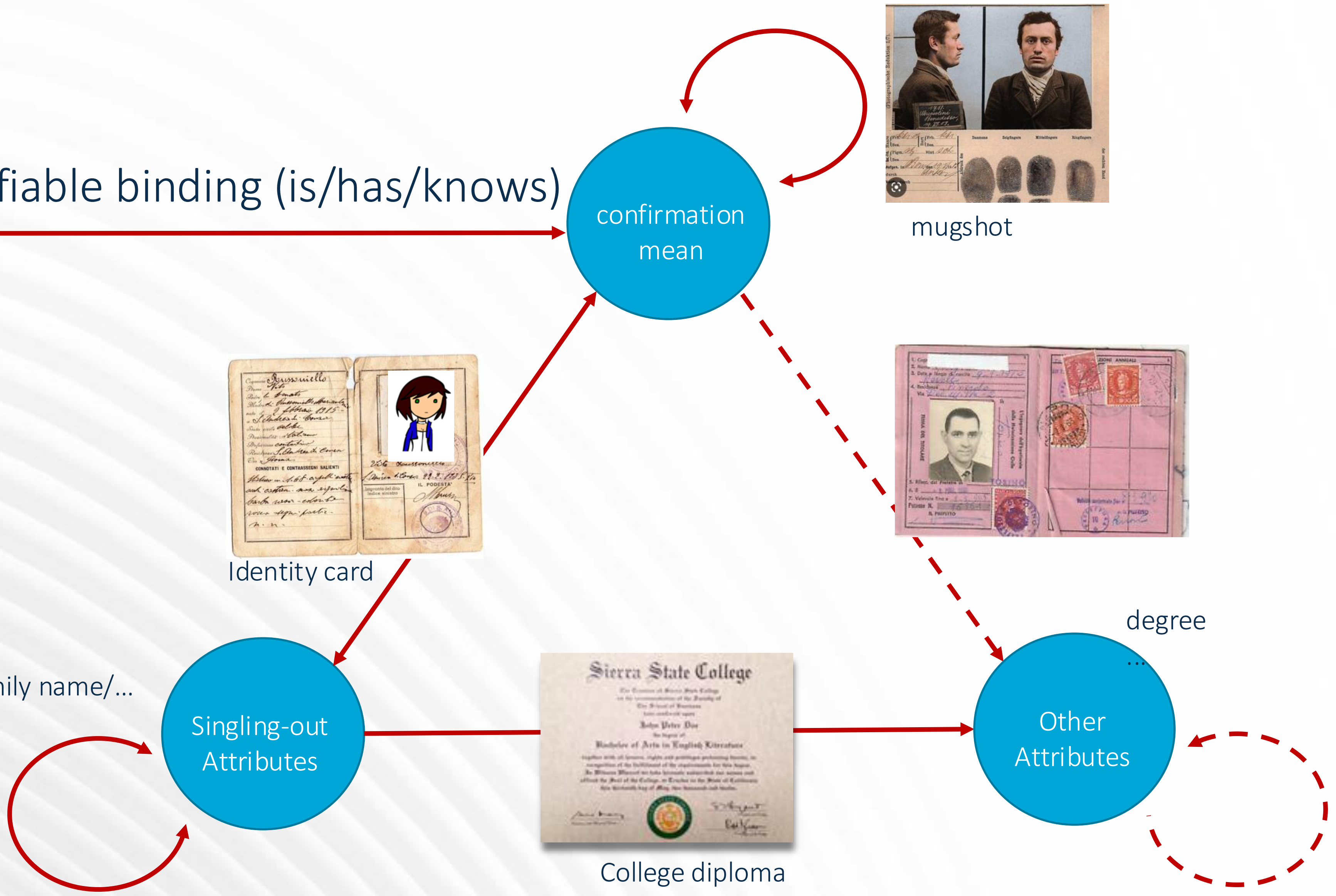
Other Attributes

degree

...

# MODELING PRE-DIGITAL IDENTITY

Real
Alice



verifiable binding (is/has/knows)

confirmation mean

mugshot

Identity card

Singling-out Attributes

Other Attributes

degree

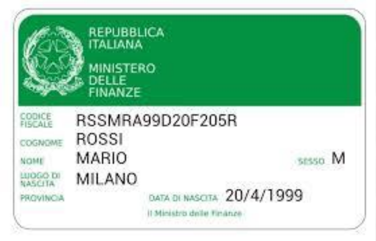
…

College diploma

In fact, docments can bind:

conf. Mean ←→ conf. Mean
conf. Mean ←→ s.o attr.
s.o attr ←→ s.o. attr
conf. Mean ←→ conf. Mean
…

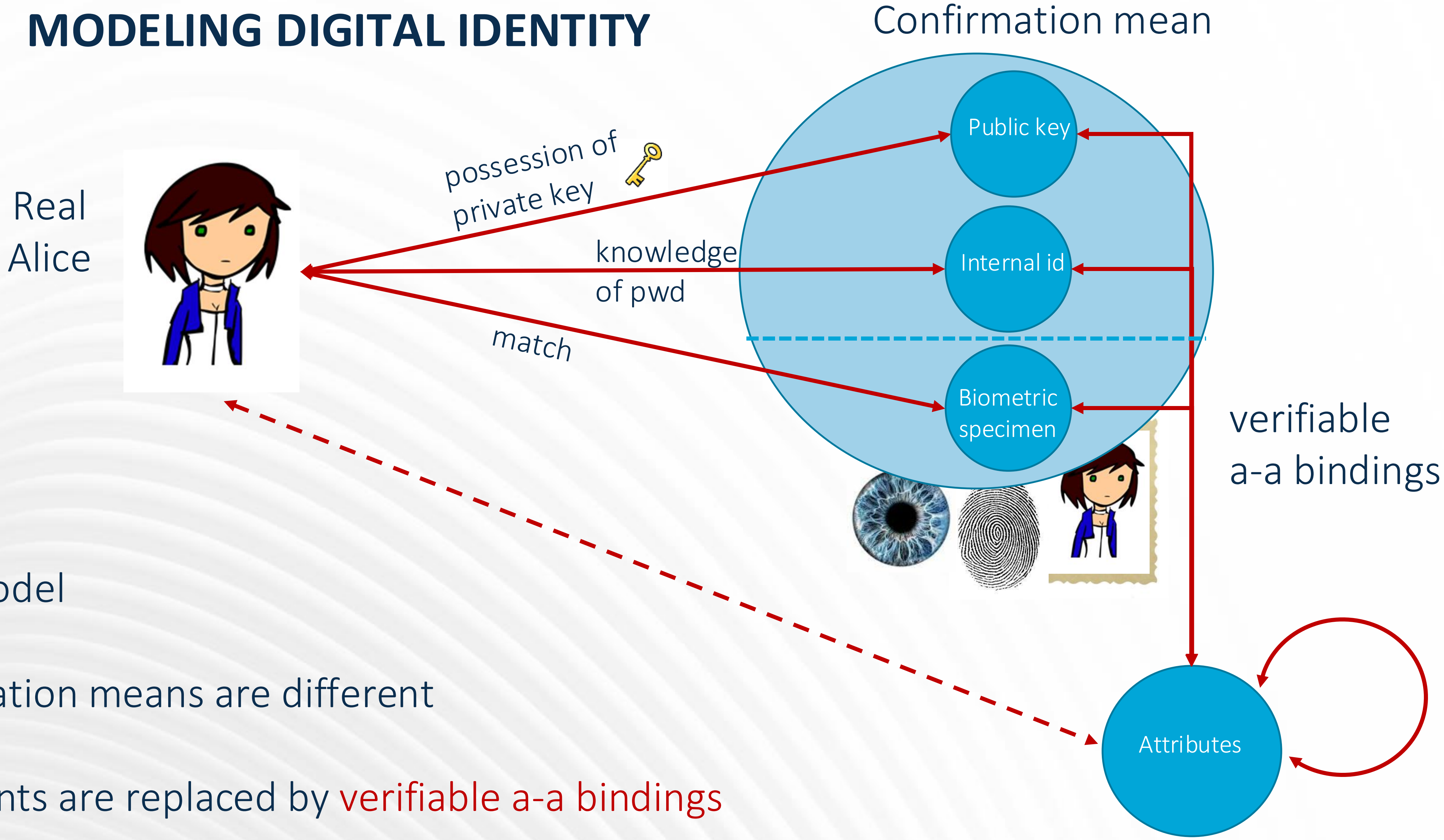
Name/Family name/…



REPUBBLICA ITALIANA
MINISTERO DELLE FINANZE

CODICE FISCALE RSSMRA99D20F205R
COGNOME ROSSI
NOME MARIO
SESSO M
LUOGO DI NASCITA MILANO
PROVINCIA
DATA DI NASCITA 20/4/1999
Il Ministro delle Finanze

# MODELING DIGITAL IDENTITY



Same model

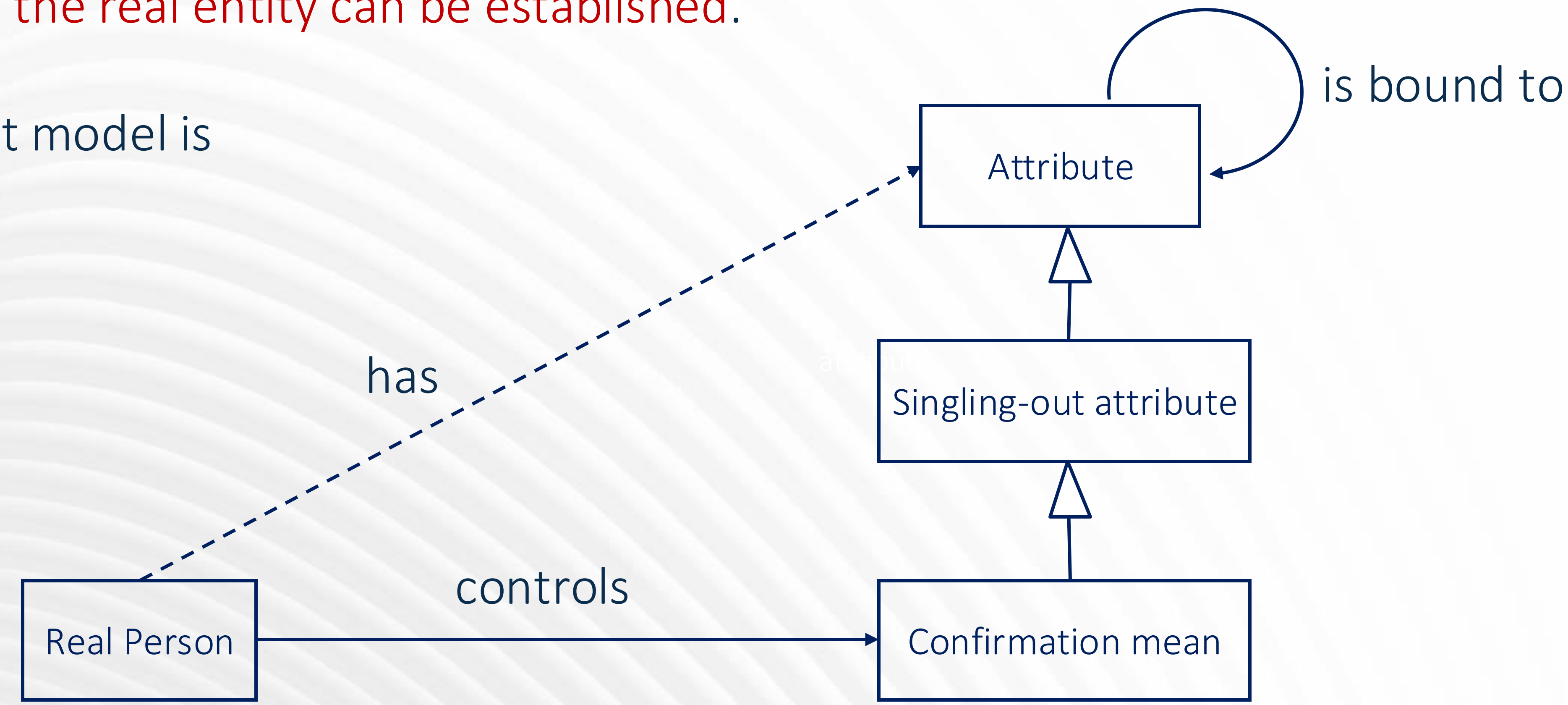
Confirmation means are different

Documents are replaced by verifiable a-a bindings

# MODELING DIGITAL IDENTITY

Confirmation means are just
special singling-out attributes attributes for which
a binding to the real entity can be established.

The simplest model is



# MODELING DIGITAL IDENTITY

## Verifiable digital attribute-to-attribute binding

**physical realm →** bindings mostly occur by documents

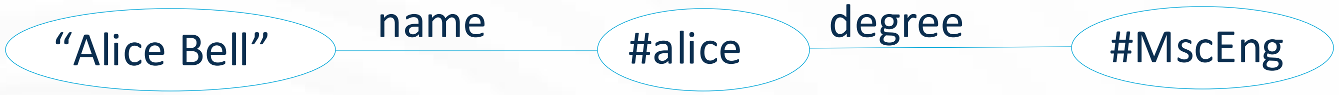
(= engraving the two attributes on a physical substrate)

**digital realm →** binding mostly occur by having a trusted entity T vouching for the binding by providing an assertion: $<a1, a2>_{\text{vouched for by\_T}}$

NOTE1: technically, the assertion may be made available as a signed file, as a record in a database, DLT, through a digital service on a secure channel…)

NOTE2: $<a1, a2>_{\text{vouched for by\_T}}$ is different from $<a2, a1>_{\text{vouched for by\_T}}$

# MODELING DIGITAL IDENTITY



## RDF/Linked Data is entity oriented:

```
<rdf:Description about= "#alice”
    <ns:name “Alice Bell”>
    <ns:degree “#MscEng">
</rdf:Description>
```

```
{
    "@context": {…},
    …,
    "credentialSubject": {
        "@id": ”#alice",
        "ns:name": ”Alice Bell",
        "ns:degree": ”#MscEng ”
    }
}
```

**Semantics**: entity #alice is associated with entity “name:Alice Bell” and with entity “degree:#MscEng”

## VA2A bindings are attribute oriented:

```
<ns:name: “Alice Bell”, ns:degree : “#MscEng”>
```

```
{
    "@context": {…},
    …,
    "credentialSubject": {
        "ns:name": ”Alice Bell",
        "ns:degree": ”#MscEng ”
    }
}
```

**Semantics**: Whoever can prove to be associated with “Alice Bell” can also prove to be associated with “#MscEng”

**Note**: attributes are not bound to keys, bearer,…. In case one of the attributes is a **confirmation mean** we can bind attributes to a real entity

# AGENDA

Semantics of W3C data model

Modeling identity in the physical /digital world

➡ A basic calculus

An extended calculus (sketch)

Practical conclusions

# A BASIC CALCULUS

An attribute is a couple a=<tag, value> --- syntactic sugar: a=tag:value

tag belongs to a space of attribute names, value belongs to the space of the respective values. E.g.

a1=name:John

a2=height:178

a3=pub_key:3f3dhc7css8b2323fe

The tag provides the semantics of the attribute, and may help the verifier to decide whether to treat it as a confirmation mean, an identifier, its format, unit, etc. As a matter of fact, there is need for a standardized ontology of tags to establish a shared semantics.

# A BASIC CALCULUS

A well-formed formula in language 𝕃 is:

- An attribute ti:vi
- a propositional composition of formulas with ∧ ∨ → ¬

We are particularly interested in a subset of propositional formulas like

ti:vi → ti:vi

Which represent a claim. E.g.

name:"John Doe" → height:178

pub_key:3f3dhc7css8b2323fe → degree:MscEng

pub_key:3f3dhc7css8b2323fe → DID:"DID:ebsi:1234"

# A BASIC CALCULUS

The calculus is given by Modus Ponens

$$\frac{A \qquad A \to B}{B}$$

Example

$$\dfrac{\dfrac{\text{pub\_key:3f3dhc73fe} \to \text{DID:”DID:ebsi:1234”} \qquad \text{DID:”DID:ebsi:1234”} \to \text{degree:MscEng}}{\text{pub\_key:3f3dhc73fe} \to \text{degree:MscEng}} \qquad \text{degree:MscEng} \to \text{jobLevel:C}}{\text{pub\_key:3f3dhc73fe} \to \text{jobLevel:C}}$$

# A BASIC CALCULUS

We can sketch a model: $M = (I, U, \sigma)$

- $I = \{ i_1, \ldots . i_r \}$ – intended to represent a set of individuals
- $U = \wp(I)$ – ($U$ is the set of parts of $I$)
- $\sigma$: $Att \rightarrow U$ is a function which maps each atomic term of the language $t_i : v_j$ to an element of $U$

We extend $\sigma$ to the entire language $\sigma$: $L \rightarrow U$

$$\sigma(\neg A) = \overline{\sigma(\neg A)} \quad \text{(complement in I)}$$

$$\sigma(A \wedge B) = \sigma(A) \cap \sigma(A)$$

$$\sigma(A \vee B) = \sigma(A) \cup \sigma(A)$$

$$\sigma(A \rightarrow B) = \overline{\sigma(A)} \cup \sigma(B)$$

And we eventually define $M \vDash A$ iff $\sigma(A) = I$

Specifically, model $M$ satisfies the claim

$$t_i : v_j \rightarrow t_h : v_k$$

iff the set of individuals who hold the first attribute is a subset of the set of individuals who hold the second attribute

# AGENDA

Semantics of W3C data model

Modeling identity in the physical /digital world

A basic calculus

➡ An extended calculus (sketch)

Practical conclusions

# AN EXTENDED CALCULUS

A formula is:

- a claim c(a1, a2, a3)

entity described by a1 (likely, a singling out attribute) claims that whichever entity is associated to a2 is also associated to a3

c(id:universityOfPadova pub_key:3f3dhc7css8b2323fe, degree:MscEng)

c(id:trustedCA#1234 pub_key:3f3dhc7css8b2323fe, DID:”DID:ebsi:1234”)

- a trust relation t(a1, a2)

entity described by a1 (likely, a singling out attribute) trusts entity described by a2 (likely, a singling out attribute)

t(pub_key:3f3dhc7css8b2323fe, id:universityOfPadova)

- a propositional composition of formulas with ∧ ∨ → ¬

# AN EXTENDED CALCULUS

Example:

$$t(luca, unipd) \land t(luca, CA1) \land c(CA1, marco, DID1) \land c(unipd, DID1, degreeMSc)$$

$$\rightarrow c(luca, marco, degreeMSc)$$

$$t(unipdAdmin, unipd) \land c(unipd, unipdBachelor, unipdStudent) \land c(unipd, marco, unipdBachelor)$$

$$\rightarrow c(unipdAdmin, marco, unipdStudent)$$

# AGENDA

Semantics of W3C data model

Modeling identity in the physical /digital world

A basic calculus

An extended calculus (sketch)

➡ Practical conclusions

# PRACTICAL CONCLUSIONS

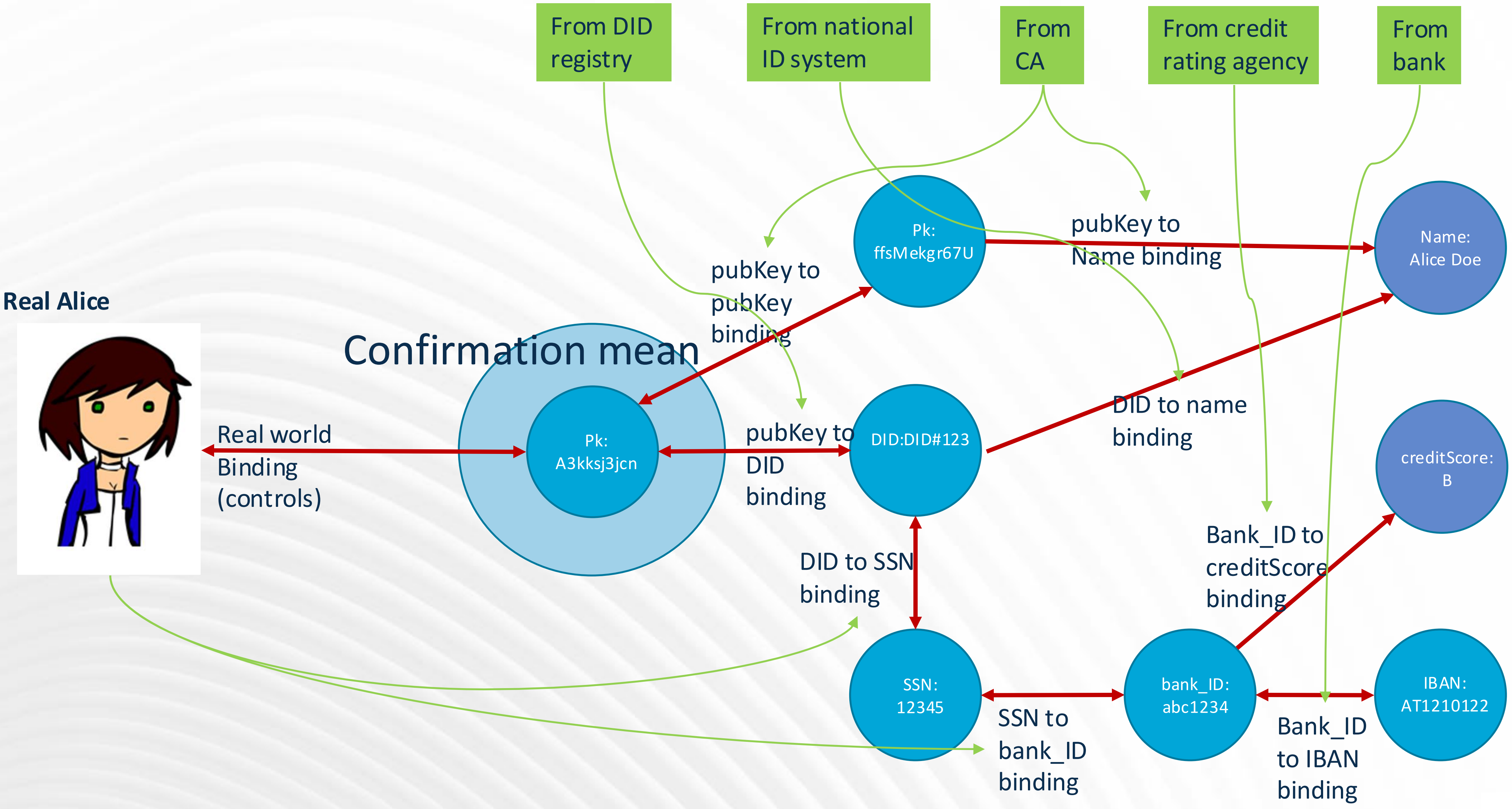
Practically, to verify Alice’s attributes:

1. get one or more confirmation means (a picture from a scanner, a public key provided by Alice...)
2. verify the binding between Alice and a confirmation mean(s) - (controls: is/has/knows)
3. get a set of bindings of which at least one starts from a confirmation mean (from any sources)
4. verify each binding using the respective validation information
5. follow the chain of bindings starting from a confirmation mean to the desired attributes.

NOTE1: bindings need not come from Alice. The source of bindings is irrelevant, as long as they are verifiable, i.e. there is a proof for them which can convince the verifier.

NOTE2: the verifier may be interested in getting information about some other subject (not necessarily someone interacting with it). No confirmation mean validation, only follow points 3, 4, 5.

# PRACTICAL CONCLUSIONS



# PRCTICAL CONCLUSIONS

- We advocate for the necessity of clarifying the semantics of digital credentials
- We offer a sketch of a formal calculus, based on attributes instead of entities
- The model does not require credentials to be bound to a holder
- The model only relies on «atomic» credentials, no need for selective disclosure
- We believe it might contribute to our design of digital identity schemas
- Though, it is just a sketch leaving out many important aspects…

INFOCERT
TINEXTA GROUP

# THANKS FOR YOUR ATTENTION

SIXTEMA
TINEXTA GROUP

Camerfirma
AN INFOCERT COMPANY

CERTEUROPE
AN INFOCERT COMPANY

ICTECHLAB
AN INFOCERT COMPANY

ascertia
AN INFOCERT COMPANY

infocert.it infocert.digital