
SICPA

SICPA

Confidentiality note

All information and material contained in these pages, including text, layout, presentation, logos, icons, photos, processes, data and all other artwork including – but not limited to – any derivative works are business sensitive and confidential information and/or information and material protected by patents, designs, trade-marks or copyrights in the name of SICPA or any of its affiliates and shall be kept strictly confidential.

The material and information contained in – or derived from – these pages may therefore not be copied, exploited, disclosed or otherwise disseminated, in whole or in part, without SICPA's prior written approval.

Secure Value Documents

Presented by : Marco Aloe
Title : Director Integrity Solutions
Company : SICPA

Date : 16/05/2019

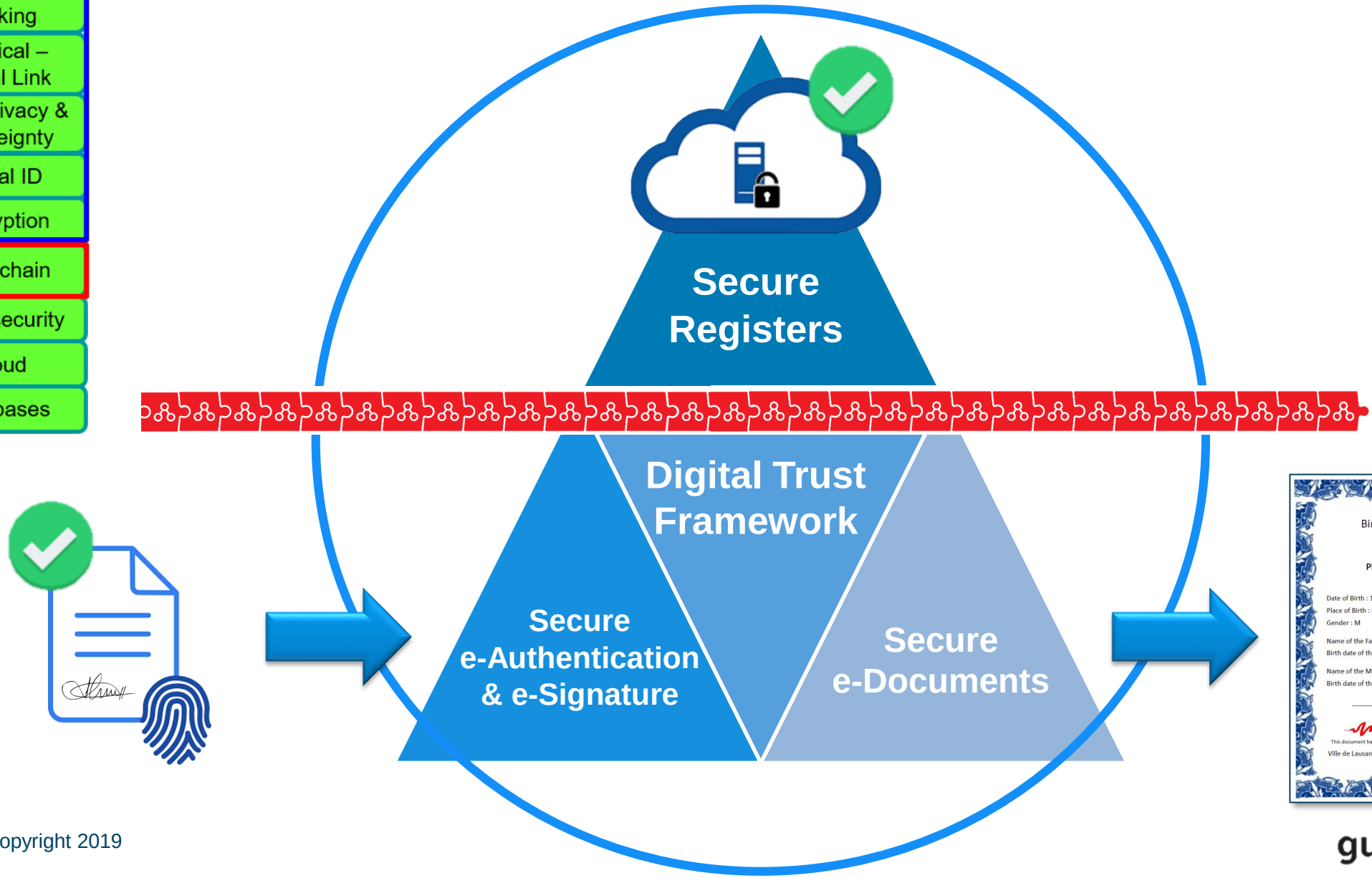
Confidentiality level : INTERNAL USE ONLY / CONFIDENTIAL

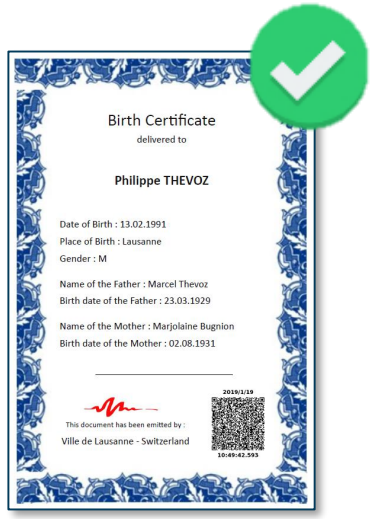
SICPA

Enabling trust

DIGITAL INTEGRITY PLATFORM

- Artificial Intell.
- Secure marking
- Physical – Digital Link
- Data privacy & sovereignty
- Digital ID
- Encryption
- Blockchain
- Cybersecurity
- Cloud
- Databases

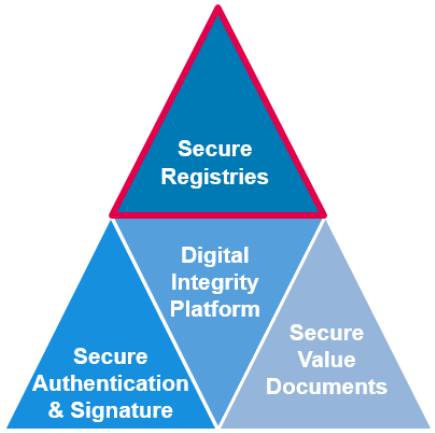


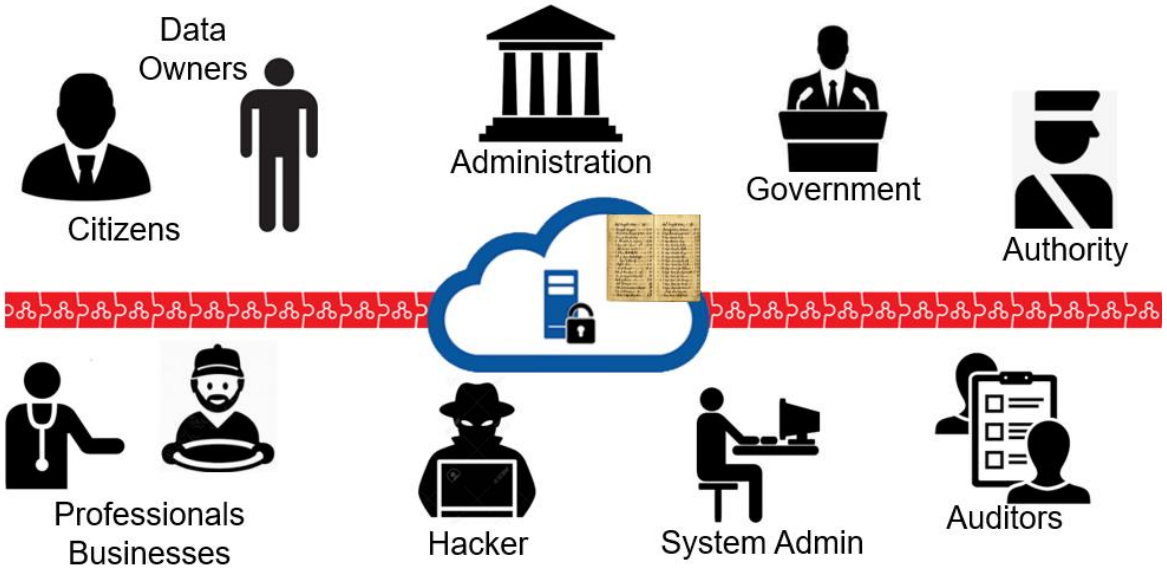


guardtime

Secure immutable registries

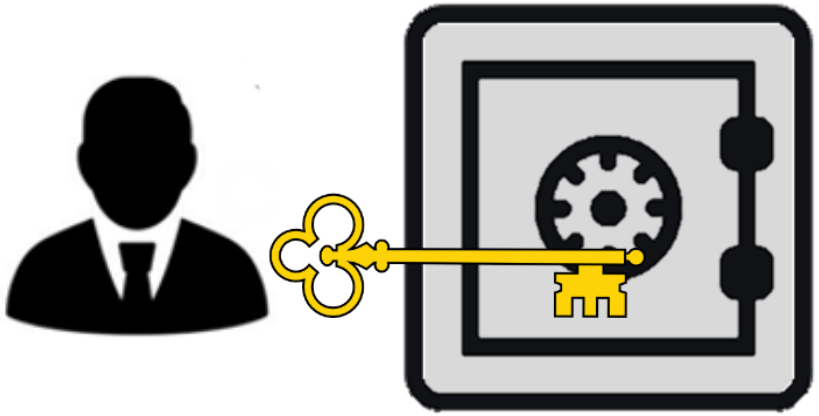
Data Integrity	Indisputable tamper evidence
Data Security	Real-time intrusion detection
Confidentiality Privacy	Render data unusable and unbreakable by any intruder
Digital Sovereignty	How can I prove my good faith, independently from the system
Process Integrity	How to prove that the data have been generated through the right process
Auditability Accountability	Undisputable proof of who did what and when on which data



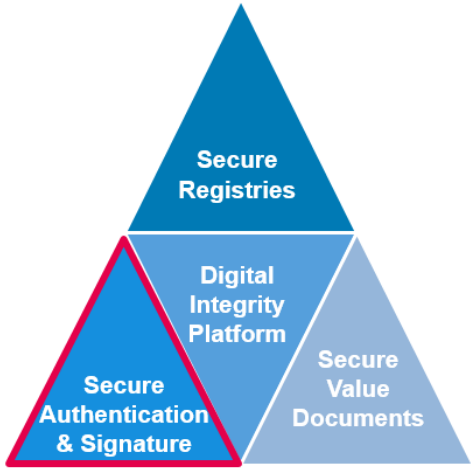


guardtime

Secure Authentication & digital signature



- Server assisted signature
- Blockchain secured
- Certificate verification at signature creation
- Quantum immune



Next Generation Digital Signature – PKI 2.0

guardtime

Secure value documents

2019/1/19

10:49:42.593

Birth Certificate

delivered to

Philippe THEVOZ

Date of Birth : 13.02.1991

Place of Birth : Lausanne

Gender : M

Name of the Father : Marcel Thevoz

Birth date of the Father : 23.03.1929

Name of the Mother : Marjolaine Bugnion

Birth date of the Mother : 02.08.1931

This document has been emitted by :

Ville de Lausanne - Switzerland

2019/1/19

10:49:42.593

2019/1/19

10:49:42.593

SICPA

Secure Value Documents

- ❑ Public/private education
- ❑ Public authorities and administrations
- ❑ Accrediting organizations
- ❑ Banks, fiduciary services
- ❑ Notaries, doctors, lawyers,
  Food, pharmaceuticals manufacturers
- ❑ NGOs (emergency documents)
- ❑ Authors, archivers

As an issuer, you **emit documents** that have a **value** and you are at the root or part of a chain of trust between people.

As an issuer, your responsibility is to give your clients the **guaranty** that their claim (qualification, competence, ownership, right, identity) cannot be disputed, changed or misused.

Once created, value documents should be **accessible and verifiable independently** from you or any institution of origin.

How to “digitally secure” Value Documents ?

Trust in the Issuer

- How can I have the Proof that the document is coming from the legitimate issuer (without knowing him) ?

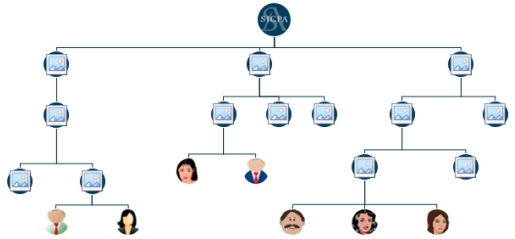
Document integrity

- How can I have the Proof that the document is genuine, that it has not been counterfeited or tampered with?

Digital Trust Anchor

- How can I be sure of the authenticity of the above Proofs ?

Chain of Trust



Blockchain & Secure Immutable Registry

SICPA

Our Solution for Diplomas

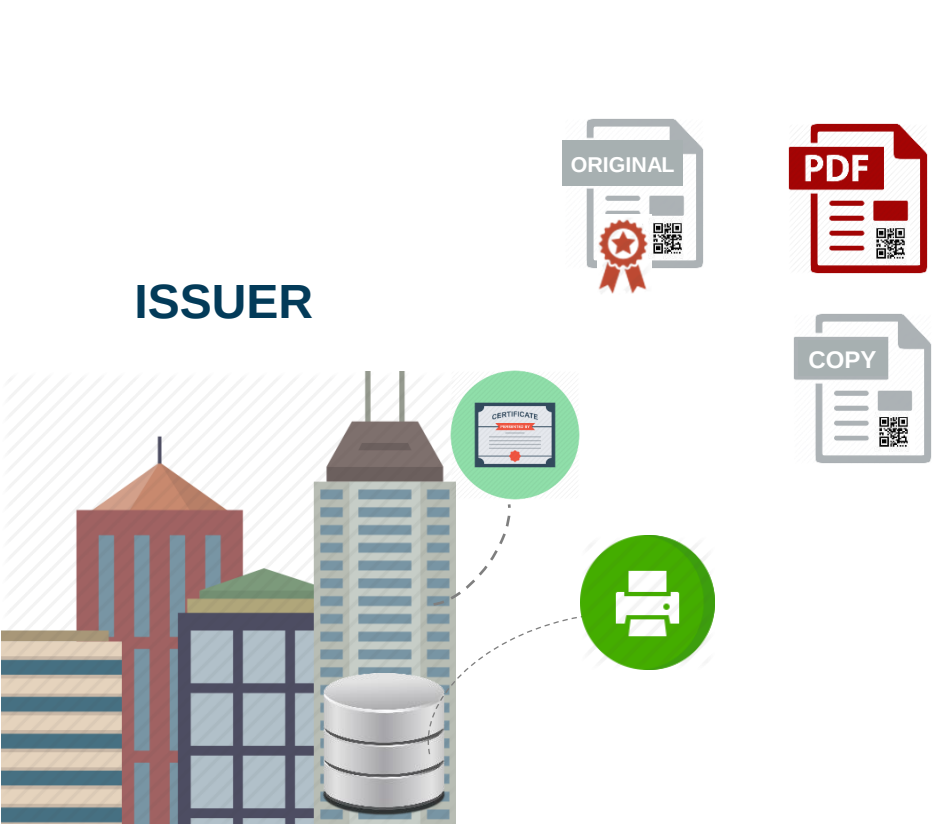
1

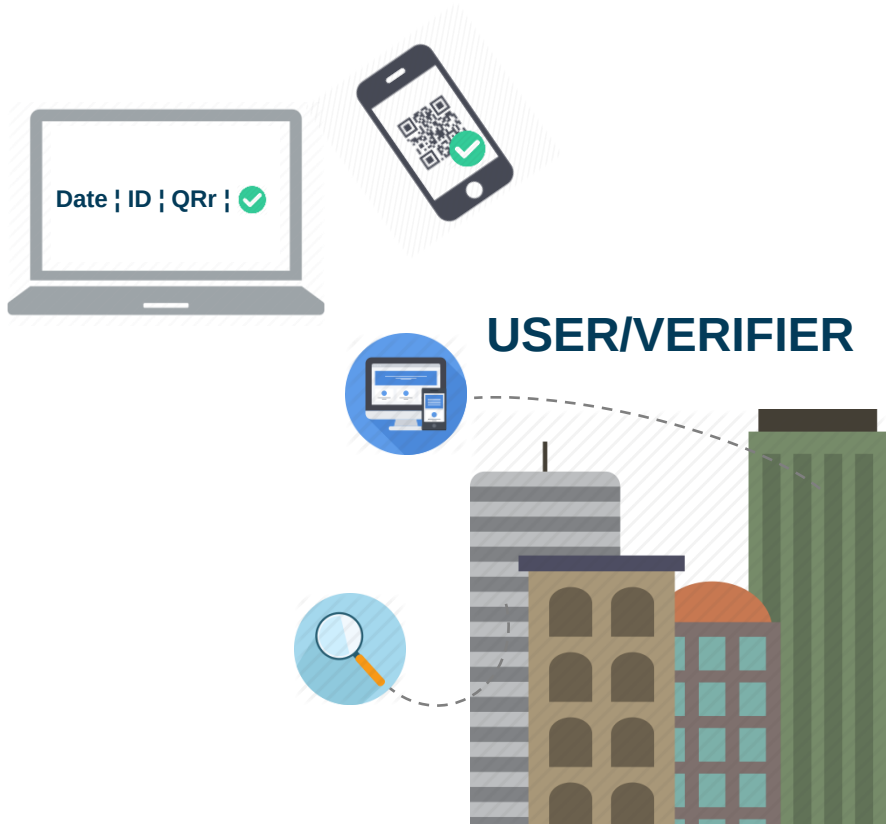
Create a **value document** with a **secure marking, registered** in the **blockchain,** and make it **tamper proof for life.**

2

Verify a **value document, the authenticity of its data** and **integrity of issuing processes**.

Verify both **online** and **offline**, from an **original** or a **copy**, and whatever the format -- **paper** or **digital**.





SECURE ID and LOGGING REGISTER + SICPA DATABASE + KSI BLOCKCHAIN

Data stay with the issuer

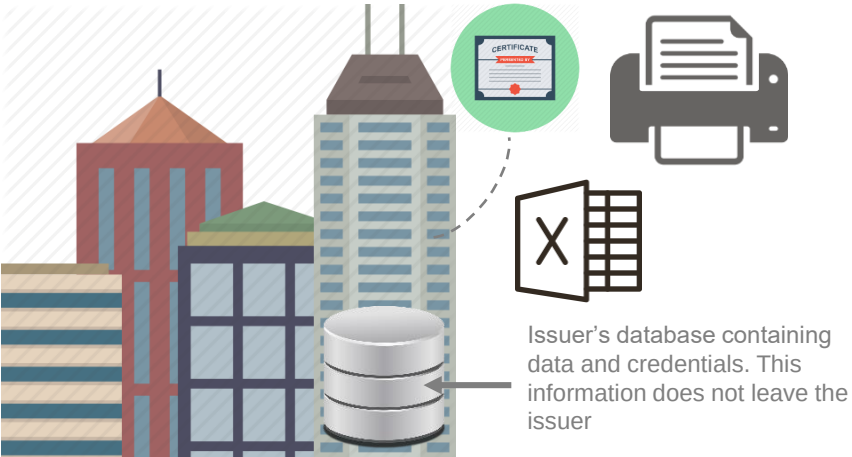
Only Metadata (hashes) are stored in the blockchain

No need for complicated wallets and keys management

Data readable with standard QR Code Readers

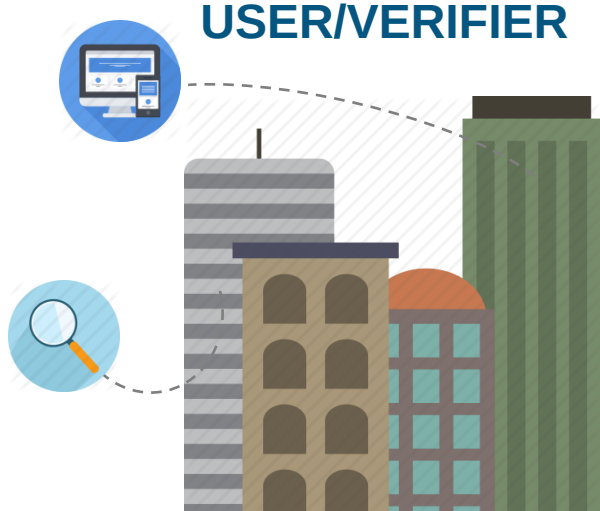
Online/Offline verification

ISSUER



Issuer's database containing data and credentials. This information does not leave the issuer

USER/VERIFIER



The current blockchain-based solutions

The blockchain makes records immutable and guarantees that no data has been changed in issued documents in a way unintended by the author.

Records of transactions are shared in a common ledger across a distributed network.

Some competitors have done away with security codes and securing paper documents, to use the blockchain instead to secure digital documents only.

SICPA insists on securing both paper and digital documents, as well as maintaining an independent record of transactions and root signature hashes.

Disadvantages of the current blockchain-based solutions:

- A basic blockchain based solutions only secures digital papers.
- It is not possible to verify the authenticty of a document offline
- It does not guarantee that the document being timestamped is genuine (garbage in – garbage out)
- It does not guarantee integrity in the issuing processes (protocol and authorisations)
- Public blockchains (like bitcoin) are unregulated, energy intensive (Proof of Work method) and not scalable for the mountain of documents being produced every day
- Cost of timestamping fluctuates and has become very expensive
- What will happen in the future?

ISSUER

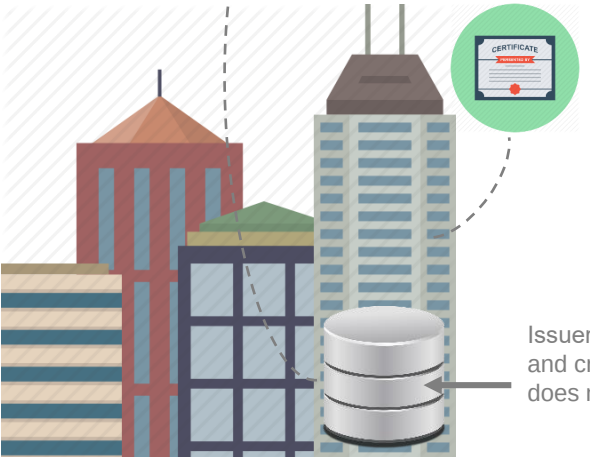
Data sent to cloud based application: Name, Title of certificate, Date, issuing organisation….
0010001110010110101110000100111001010011110001010000010

API

DIGITAL ID

SICPA SECURE QR CODES

Mailmerge + Template



Issuer's database containing data and credentials. This information does not leave the issuer

1

What happens on the SICPA server?

1. **Build codes using CSV data**
2. **Store reference hashes**
3. **Return document QR codes and root QR code in a zip file**

The QR code printed on the document contains the document's data and the means to recalculate the hash of the batch of documents issued. The security of the root signature is keyless (it is a concatenation) and the root QR code does not contain data. All data is deleted from the SICPA server after QR codes are created.

2

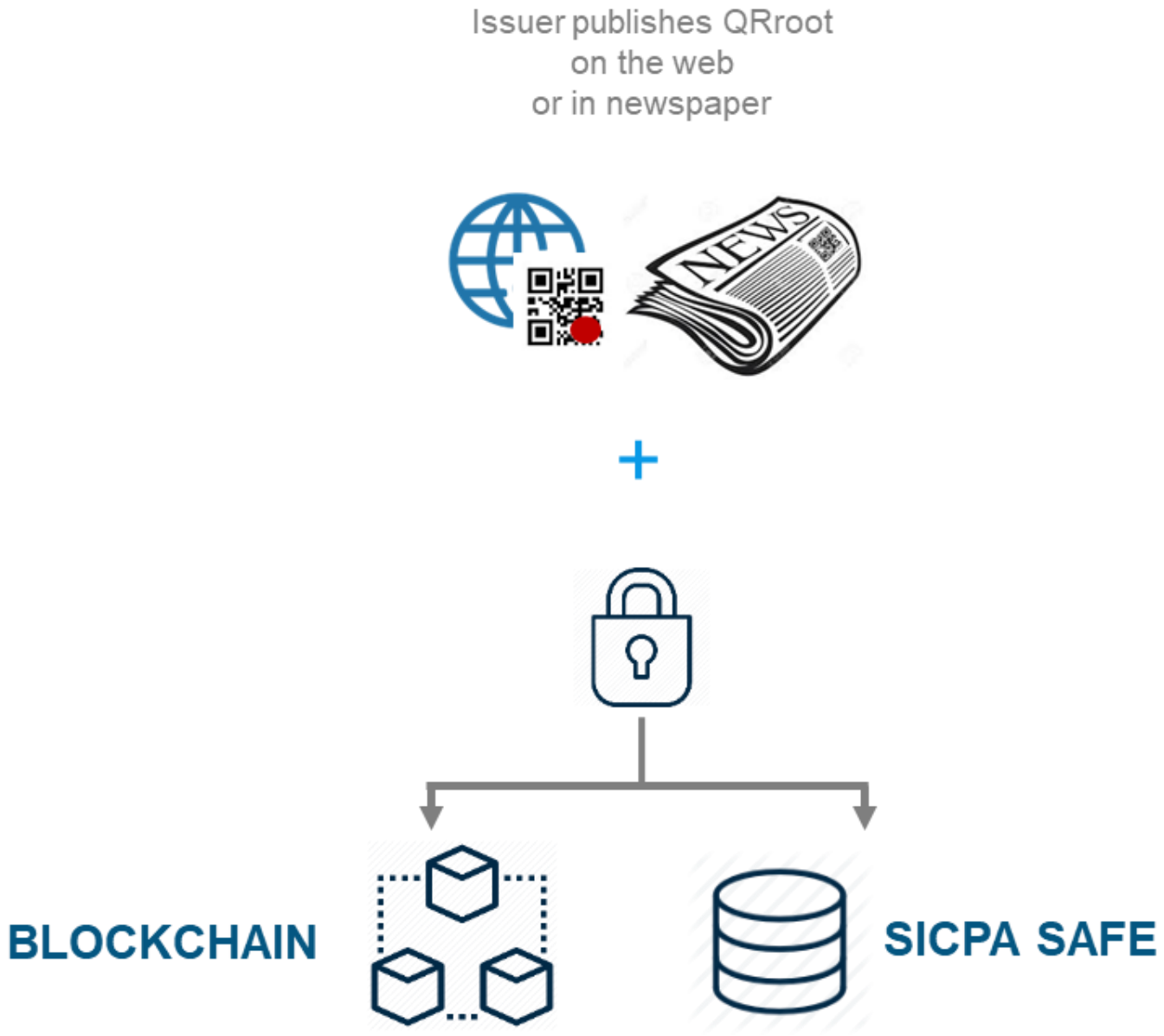
What happens on the SICPA server?

4. Storage of the signature hashes and issuance process integrity

All reference signature hashes are stored on SICPA's private ledger, the SAFE, but also at the issuer's place or publically disclosed (via twitter, a newspaper or newsletter, a corporate website…).

To guarantee process integrity, SICPA SAFE also keeps records of:

- Digital IDs (Identity Registry – different levels of authorisations according to institutional rules, audit requirements and local law)
- Loggings (who did what, when)
- Issuing process (steps in protocols)



FAST and EASY CHECKING

Check a digital document (pdf, png):

- **On your desktop**, drag and drop the document in the SIPCA app
- **On your mobile**, scan the QR code with the SICPA mobile app
- The SICPA app automatically checks the cryptographic link between the QR root and the QR on the document, as well as the conformity of the emittance process

Check a printed document:

- Scan the document and drag and drop into the desktop SICPA app
- Scan the QR code with the SICPA mobile app.

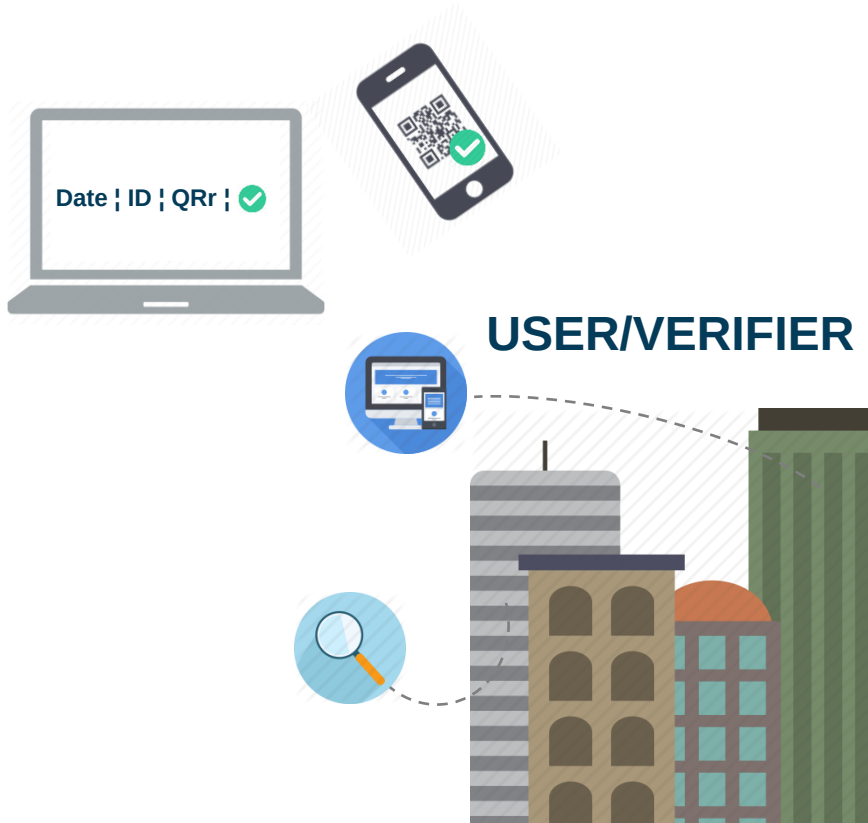
Check a hash value

SHA-256 (Secure Hash Algorithm):

7ae26e64679abd1e66cfe1e9b93a9e85

- a peer to peer blockchain site can verify the validity of the reference hash signature

- The SICPA app is free for low volume verifications (e.g. Students).
- Verification can be done with a standard QR Code Reader, but they are not secure and cannot guarantee the integrity of emission processes or will not know if a certificate has been revoked.



SICPA

Demonstration

1

2018/11/15

QRroot

14:07:47.372

IMD

grants

Philippe Gillet

a certificate of attendance in **Innovation and Strategy**

for his knowledge and aptitudes in

Digital Disruption

Sep-18, 2018

Lausanne

Signature

Frank First, Academic Director

2018/11/15 14:07:47.372

ORIGINAL

PDF

COPY

2

2018/11/15

14:07:47.372

Document QR

SAMSUNG

Verified document

DOC 2018/11/15 14:07:47.372

Index: *1*
First Name: *Philippe*
Last Name: *Gillet*
Title: *Innovation and Strategy*
Thesis name: *Digital Disruption*
Abr: *DD*
Place: *Lausanne*
Date: *Sep-18*
Year: *2018*
President name: *Frank First*
Public Key: *62803632f5b40b5f e5faeca4fb8cfc55f310e858c3 884f8247dd310ac06314cf*

DOC | LIST | CLEAR

ISSUER

USER/VERIFIER

1

2018/11/15

14:07:47.372

QRroot

IMD

grants

Philippe Gillet

Master in **Innovation and Strategy**

for his knowledge and aptitudes in

Digital Disruption

20.11.1982

Lausanne

Signature

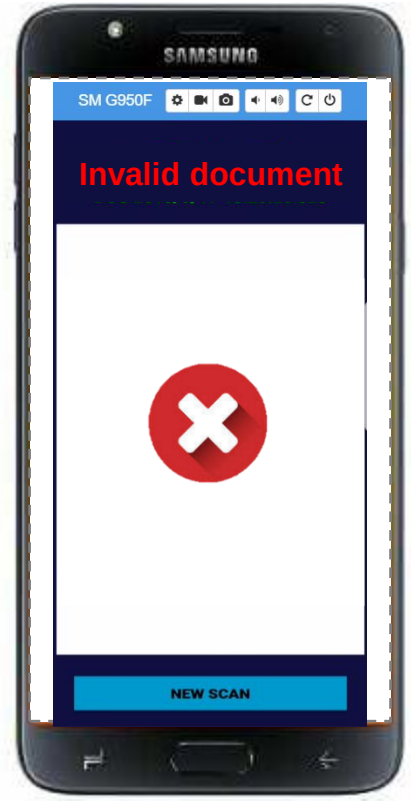
Frank First, Academic Director

2

2018/7/2

11:47:08.412

Document QR



ISSUER

ORIGINAL

PDF

COPY

USER/VERIFIER

Online Demonstration

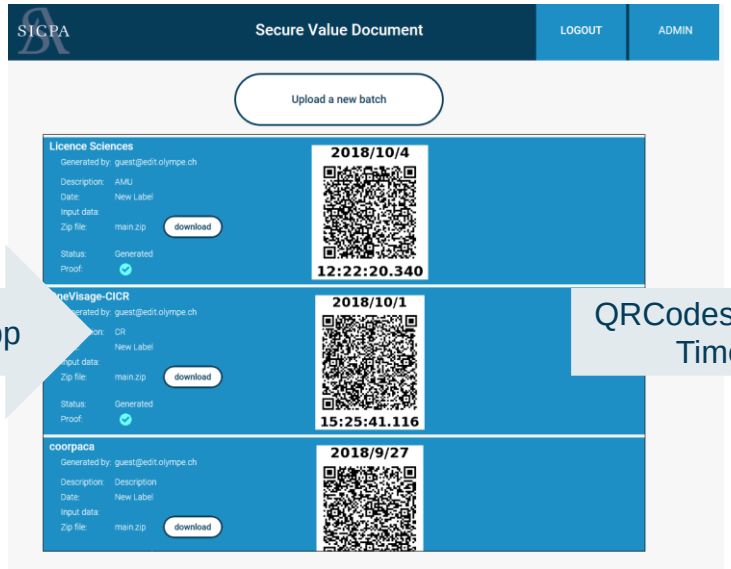
1

2

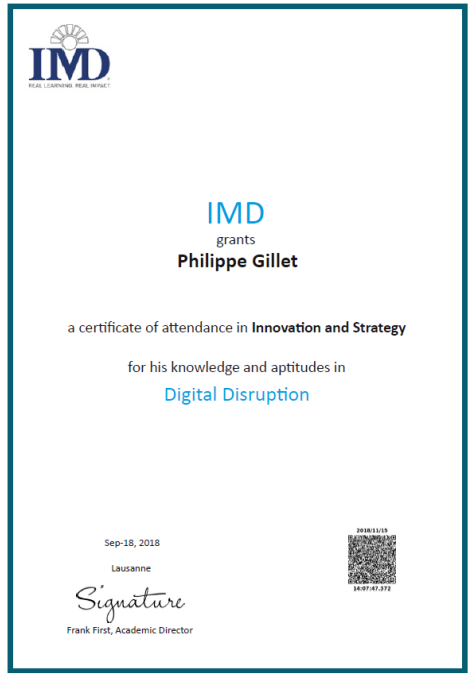
3

First Name	Last Name	Title	Thesis name	Abr	Place	Date	Year	President name
Philippe	GILLET	Doctor in Philosophy	Security applications in a world of uncertainty	PhD	New York	14-Jun	2018	Frank First
Abdallah	Musy	Doctor of Applied Science	Nanospheres for controlled light scattering 3D printing	D.A.S	Seoul	14-Jun	2018	Frank First
Abdel Hafid	Zecevic	Doctor in Philosophy	Dendritic polymers as vacuole for rat lung disease	PhD	MontrÃ©al	14-Jun	2018	Frank First
Abdellaziz	Dionisi	Doctor of Applied Science	Nanospheres for controlled light scattering 3D printing	D.A.S	MontrÃ©al	14-Jun	2018	Frank First
Abderahmane	Figueirinha	Doctor of Applied Science	Nanospheres for controlled light scattering 3D printing	D.A.S	Seoul	14-Jun	2018	Frank First
Adel	Azeli	Doctor of Medicine	Dendritic polymers as vacuole for rat lung disease	M.D.	MontrÃ©al	14-Jun	2018	Frank First
Adelino	Silva	Doctor in Philosophy	Security applications in a world of uncertainty	PhD	New York	14-Jun	2018	Frank First
Adnan	Gullifa	Doctor of Applied Science	The use of high density polymers as energy storage method	D.A.S	MontrÃ©al	14-Jun	2018	Frank First
Adolfo	Acar	Doctor of Medicine	Synthetic enzyme for pancreas cancer therapeutic	M.D.	Lausanne	14-Jun	2018	Frank First
Adrian	Toledo	Doctor in Philosophy	Synthetic enzyme for pancreas cancer therapeutic					
Adrian	Freuler	Doctor of Applied Science	The use of high density polymers as energ storage method					
Adriano	Braissant	Doctor of Medicine	Dendritic polymers as vacuole for rat lung disease					
AgnÃ¨s	Chillat	Doctor of Applied Science	The use of high density polymers as energy storage method	D.A.S	MontrÃ©al	14-Jun	2018	Frank First
Agnieszka	Zurlinden	Doctor in Philosophy	Dendritic polymers as vacuole for rat lung disease	PhD	Caracas	14-Jun	2018	Frank First
Ahmed	Saliba	Doctor in Philosophy	Synthetic enzyme for pancreas cancer therapeutic	PhD	Lausanne	14-Jun	2018	Frank First
Ajar	Group	Doctor in Philosophy	How to apply Blockchain and Digital technologies to secure documents	PhD	Seoul	14-Jun	2018	Frank First
Alain	Maury	Doctor of Applied Science	The use of high density polymers as energy storage method	D.A.S	Lausanne	14-Jun	2018	Frank First
Alain	Annen	Doctor of Medicine	Cancer cells detection with handheld medical device	M.D.	Lausanne	14-Jun	2018	Frank First
Alan	Zuber	Doctor in Philosophy	Synthetic enzyme for pancreas cancer therapeutic	PhD	Seoul	14-Jun	2018	Frank First

Load CSV into cloud app



QRCodes generation and Timestamping



SICPA

Thank you
for your attention
—