3rd Distributed Ledger Technology Workshop (DLT 2020)

Co-located with ITASEC2020

February 4th, 2020
Facoltà di Ingegneria,
Università Politecnica delle Marche,
Via Brecce Bianche, 12

Ancona

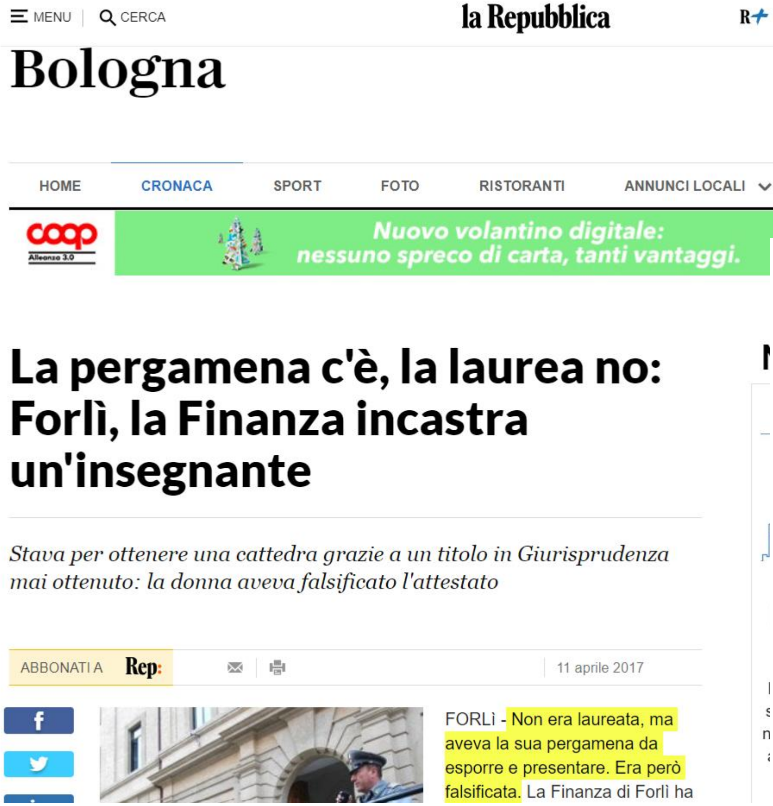
Security analysis of a blockchain-based protocol for the certification of academic credentials

Marco Baldi, Franco Chiaraluce,
Migelan Kodra and Luca Spalazzi

Università Politecnica delle Marche

Ancona

Premises and motivation



MENU | CERCA la Repubblica R+ | Rep: | ABBONATI | ACCEDI

Bologna

Cerca nel sito METEO

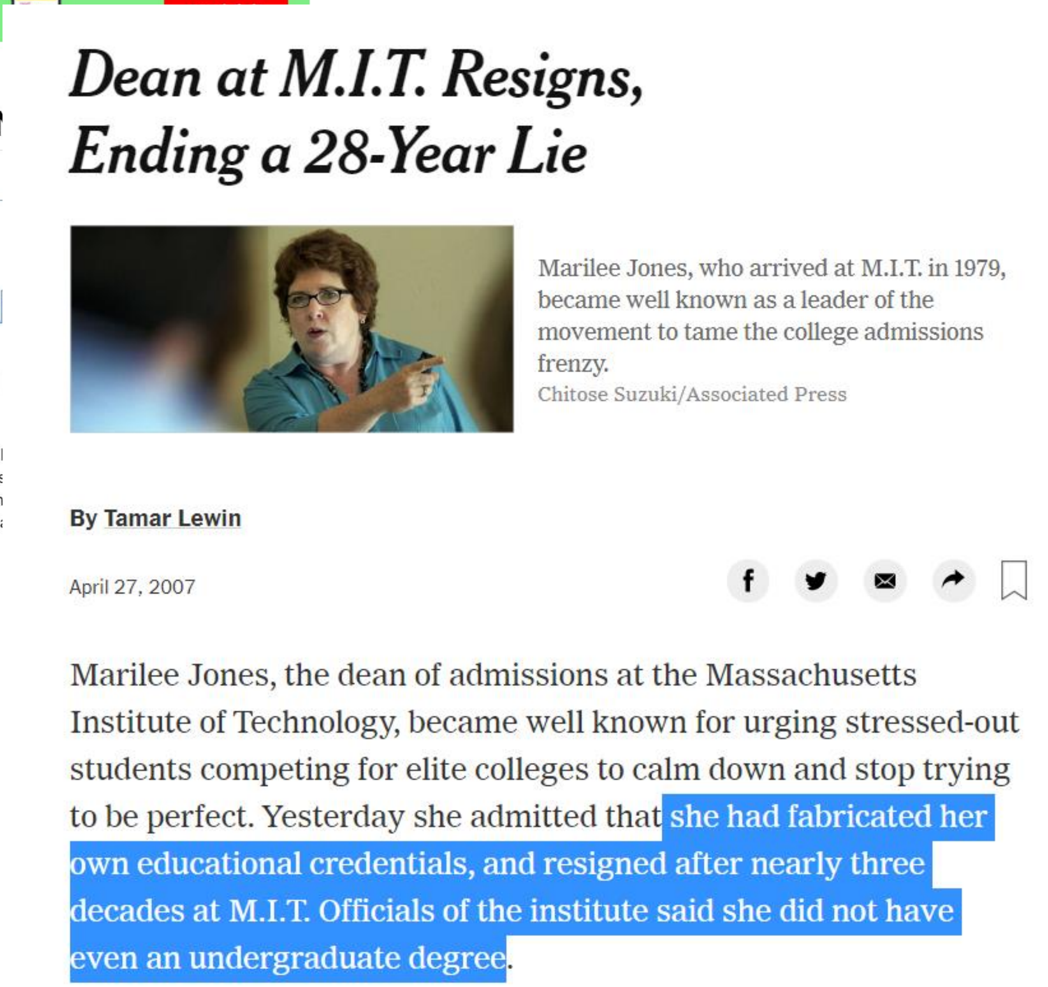
HOME CRONACA SPORT FOTO RISTORANTI ANNUNCI LOCALI CAMBIA EDIZIONE VIDEO

La pergamena c'è, la laurea no: Forlì, la Finanza incastra un'insegnante

Stava per ottenere una cattedra grazie a un titolo in Giurisprudenza mai ottenuto: la donna aveva falsificato l'attestato

ABBONATI A Rep: 11 aprile 2017

FORLÌ - Non era laureata, ma aveva la sua pergamena da esporre e presentare. Era però falsificata. La Finanza di Forlì ha



Dean at M.I.T. Resigns, Ending a 28-Year Lie

Marilee Jones, who arrived at M.I.T. in 1979, became well known as a leader of the movement to tame the college admissions frenzy.
Chitose Suzuki/Associated Press

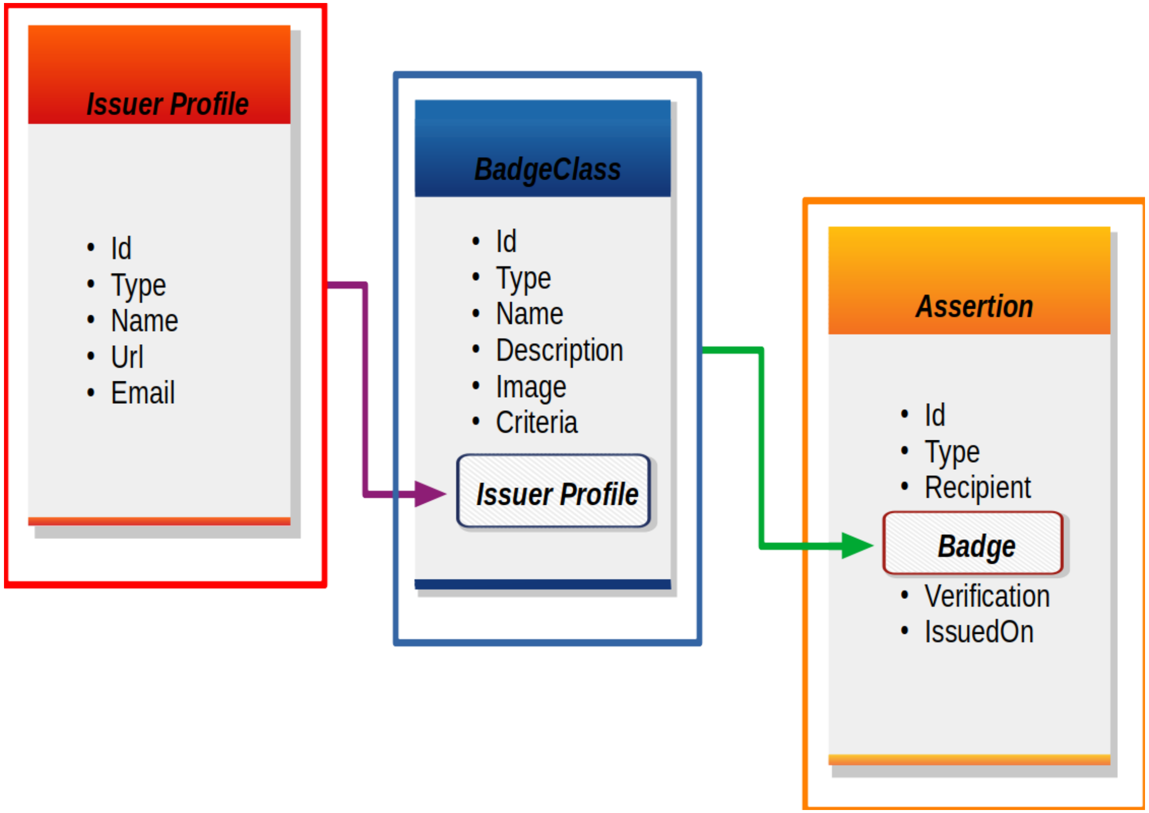
By Tamar Lewin

April 27, 2007

Marilee Jones, the dean of admissions at the Massachusetts Institute of Technology, became well known for urging stressed-out students competing for elite colleges to calm down and stop trying to be perfect. Yesterday she admitted that she had fabricated her own educational credentials, and resigned after nearly three decades at M.I.T. Officials of the institute said she did not have even an undergraduate degree.

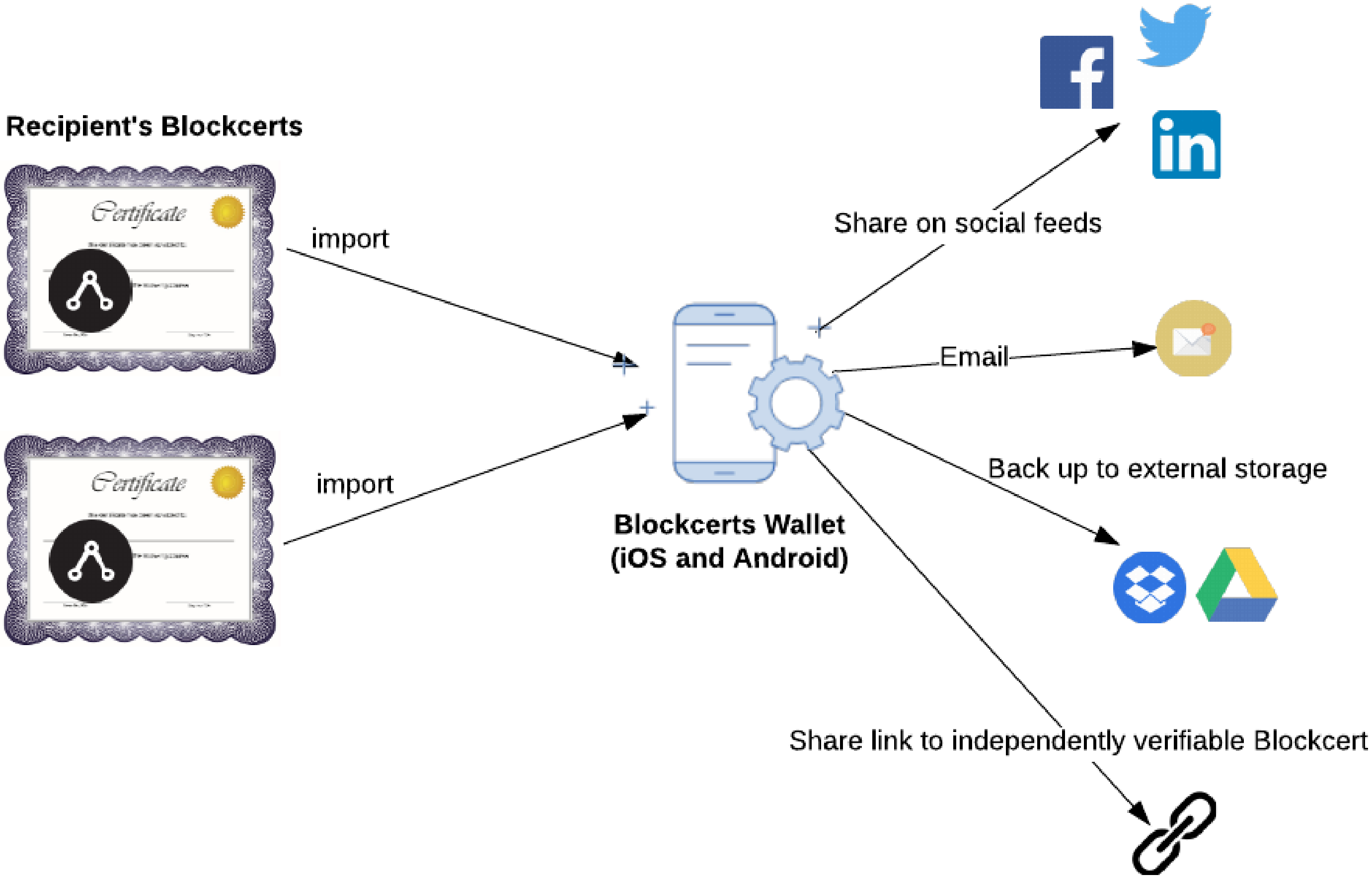
Open Badges

- ✓ Developed by the Mozilla Foundation in collaboration with the McArthur Foundation.



- ➢ **The Open Badges standard provides a tool for implementing digital, enriched versions of competence certificates and academic credentials.**

Blockcerts


Recipient's Blockcerts
Certificate
Certificate
import
import
Blockcerts Wallet
(iOS and Android)
Share on social feeds
Email
Back up to external storage
Share link to independently verifiable Blockcert

Use cases

UNIVERSITAS STUDII PADUANI MCCXXII

UNIVERSITÀ DEGLI STUDI DI PADOVA

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Massachusetts Institute of Technology

Canadä

MINISTRY FOR EDUCATION AND EMPLOYMENT

REPUBBLIKA TA' MALTA

fsmb FEDERATION OF STATE MEDICAL BOARDS

PODER EJECUTIVO DEL ESTADO DE QUERÉTARO

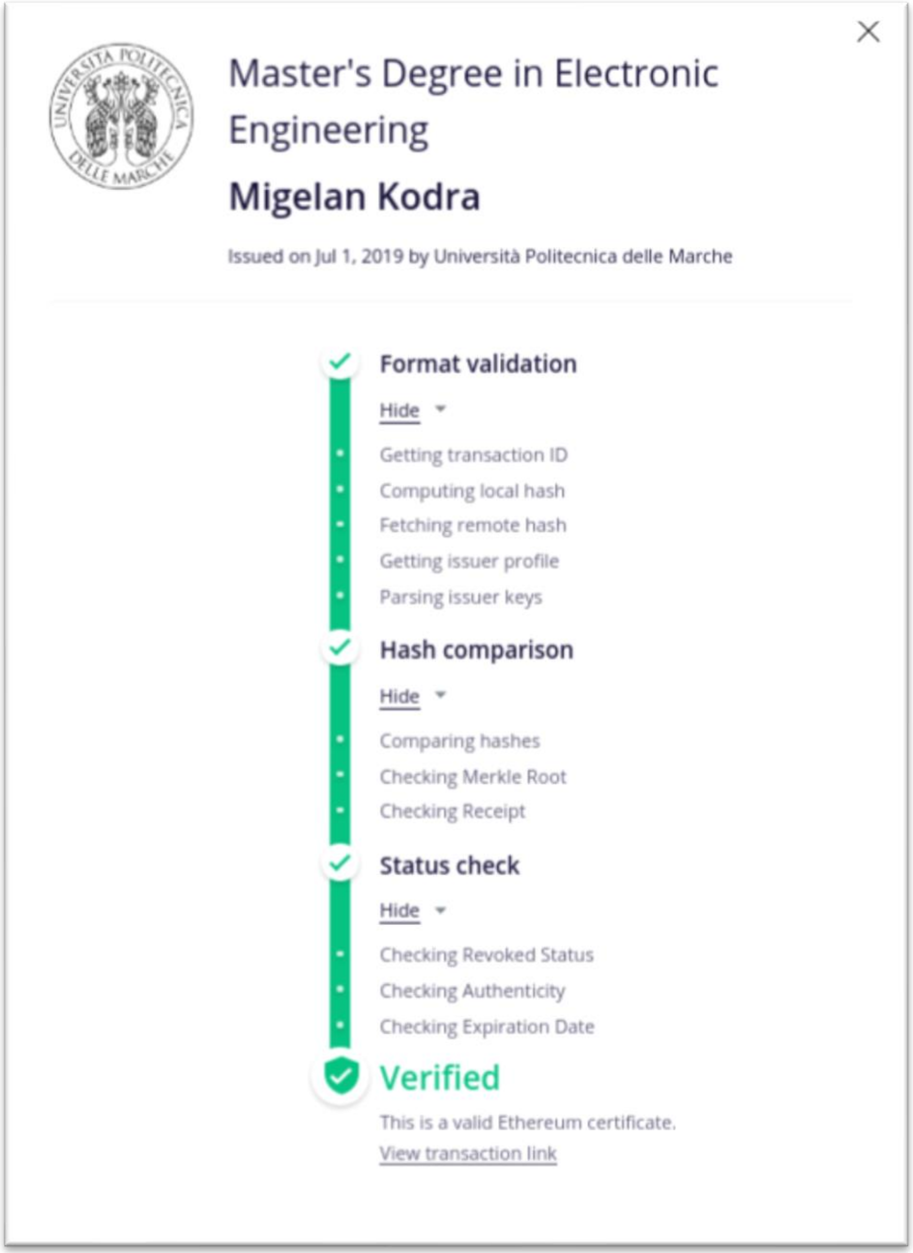
SECRETARÍA DE EDUCACIÓN

Blockcerts (ctd.)

What about the security?

- Each certificate must contain all the necessary information for its validation through the blockchain, including a reference to the public key of the issuer to be used for its validation.
- Such a feature, though allowing decentralized validation, opens the door to possible forgery attacks.

An example of forgery



Master's Degree in Electronic Engineering

Migelan Kodra

Issued on Jul 1, 2019 by Università Politecnica delle Marche

✓ **Format validation**

Hide ▾

- Getting transaction ID
- Computing local hash
- Fetching remote hash
- Getting issuer profile
- Parsing issuer keys

✓ **Hash comparison**

Hide ▾

- Comparing hashes
- Checking Merkle Root
- Checking Receipt

✓ **Status check**

Hide ▾

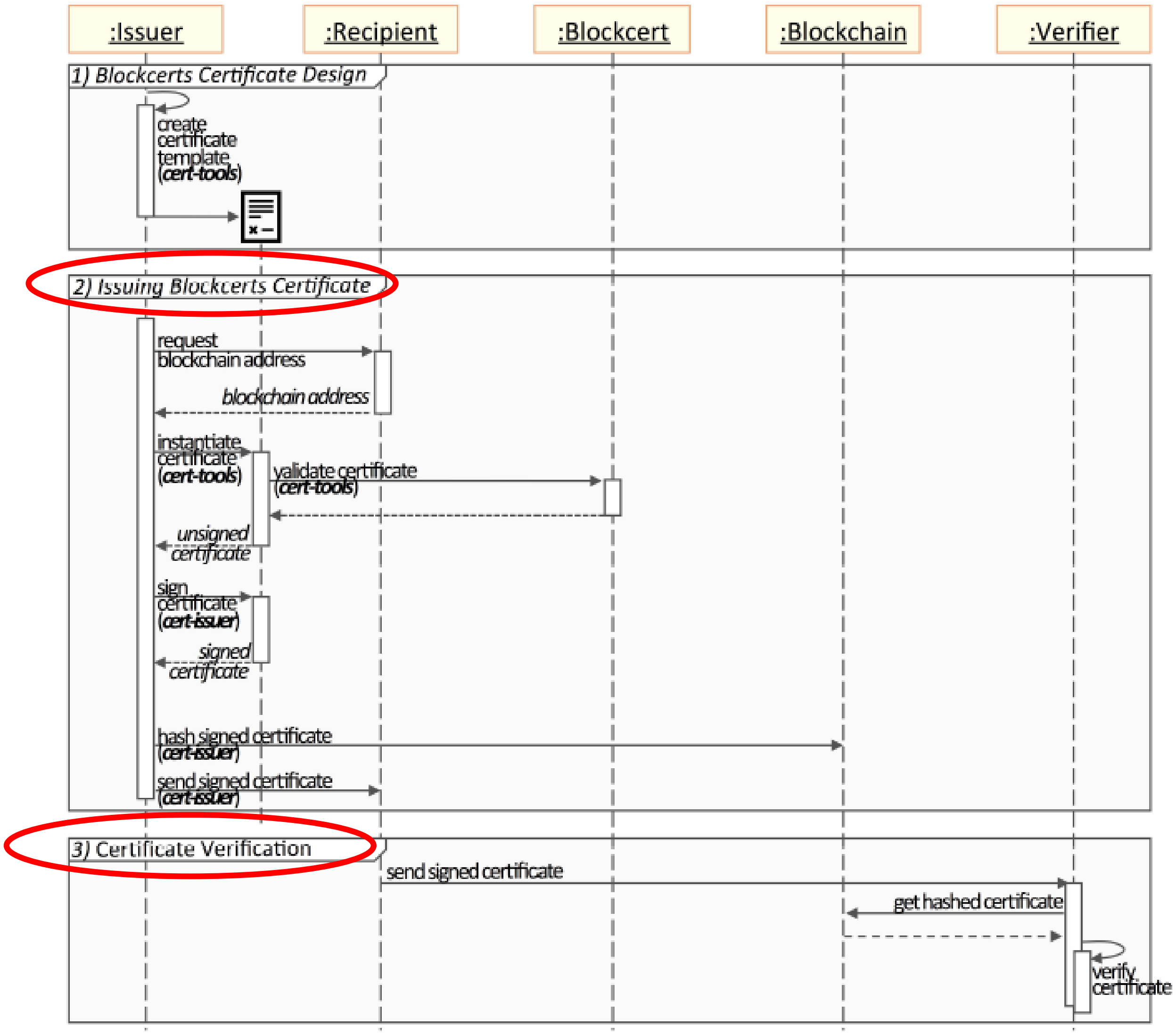
- Checking Revoked Status
- Checking Authenticity
- Checking Expiration Date

Verified

This is a valid Ethereum certificate.

View transaction link

Sequence flow of the Blockcerts system



:Issuer

:Recipient

:Blockcert

:Blockchain

:Verifier

1) Blockcerts Certificate Design

create certificate template (cert-tools)

2) Issuing Blockcerts Certificate

request blockchain address

blockchain address

instantiate certificate (cert-tools)

validate certificate (cert-tools)

unsigned certificate

sign certificate (cert-issuer)

signed certificate

hash signed certificate (cert-issuer)

send signed certificate (cert-issuer)

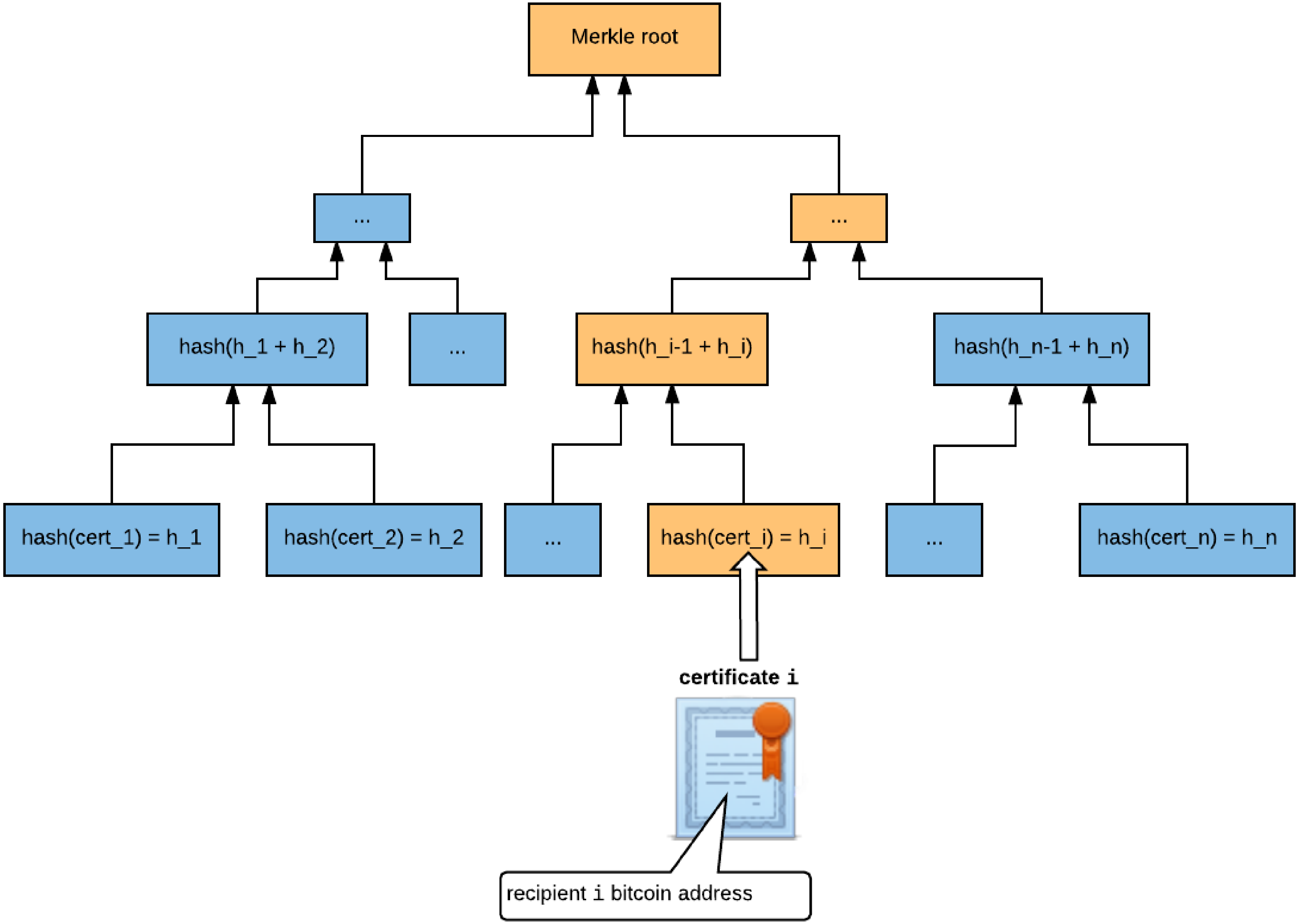
3) Certificate Verification

send signed certificate

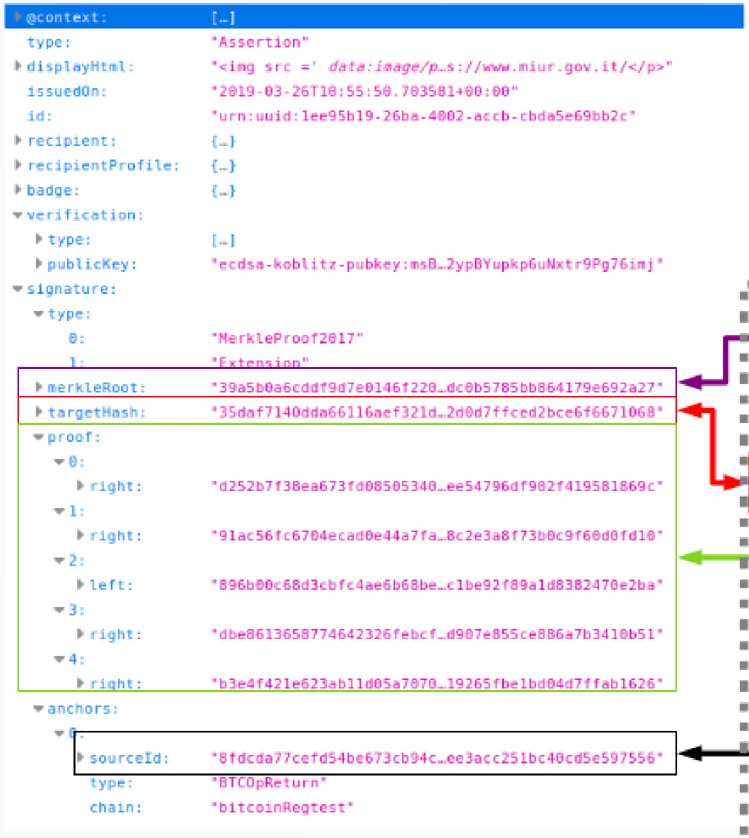
get hashed certificate

verify certificate

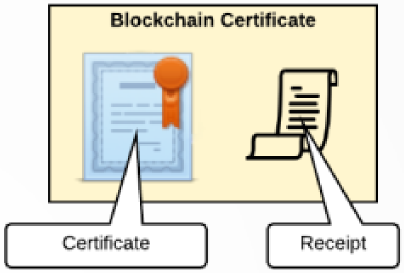
Issuing Certificates



Blockchain Receipt



```
▸ @context:               […]
  type:                   "Assertion"
▸ displayHtml:            "<img src =' data:image/p…s://www.miur.gov.it/</p>"
  issuedOn:               "2019-03-26T10:55:50.703581+00:00"
  id:                     "urn:uuid:1ee95b19-26ba-4002-accb-cbda5e69bb2c"
▸ recipient:              {…}
▸ recipientProfile:       {…}
▸ badge:                  {…}
▾ verification:
  ▸ type:                 […]
  ▸ publicKey:            "ecdsa-koblitz-pubkey:msB…2ypBYupkp6uNxtr9Pg76imj"
▾ signature:
  ▾ type:
      0:                  "MerkleProof2017"
      1:                  "Extension"
  ▸ merkleRoot:           "39a5b0a6cddf9d7e0146f220…dc0b5785bb864179e692a27"
  ▸ targetHash:           "35daf7140dda66116aef321d…2d0d7ffced2bce6f6671068"
  ▾ proof:
    ▾ 0:
      ▸ right:            "d252b7f38ea673fd08505340…ee54796df902f419581869c"
    ▾ 1:
      ▸ right:            "91ac56fc6704ecad0e44a7fa…8c2e3a8f73b0c9f60d0fd10"
    ▾ 2:
      ▸ left:             "896b00c68d3cbfc4ae6b68be…c1be92f89a1d8382470e2ba"
    ▾ 3:
      ▸ right:            "dbe8613658774642326febcf…d907e855ce886a7b3410b51"
    ▾ 4:
      ▸ right:            "b3e4f421e623ab11d05a7070…19265fbe1bd04d7ffab1626"
  ▾ anchors:
    ▾ 0:
      ▸ sourceId:         "8fdcda77cefd54be673cb94c…ee3acc251bc40cd5e597556"
        type:             "BTCOpReturn"
        chain:            "bitcoinRegtest"
```



The expected Merkle root on the blockchain

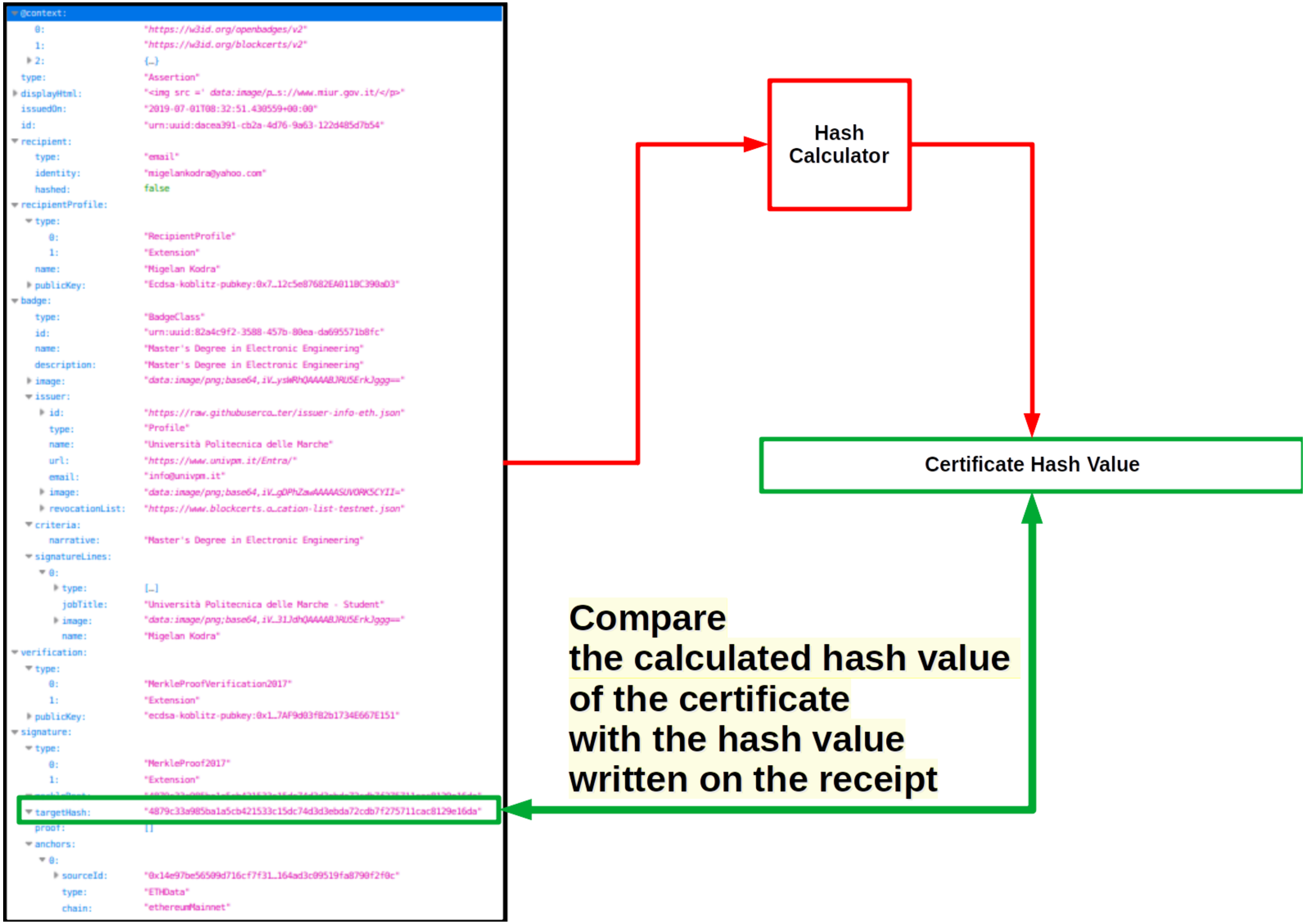
The expected hash for the recipient i's certificate

The Merkle root path from recipient i's certificate to the Merkle root

The Bitcoin transaction ID storing the Merkle root

Certificate authenticity

- <u>Step 1</u>: The **hash** of the certificate matches the value in the receipt.



```
▾ @context:
    0:                      "https://w3id.org/openbadges/v2"
    1:                      "https://w3id.org/blockcerts/v2"
  ▸ 2:                      {…}
  type:                     "Assertion"
▸ displayHtml:              "<img src =' data:image/p…s://www.miur.gov.it/</p>"
  issuedOn:                 "2019-07-01T08:32:51.430559+00:00"
  id:                       "urn:uuid:dacea391-cb2a-4d76-9a63-122d485d7b54"
▾ recipient:
    type:                   "email"
    identity:               "migelankodra@yahoo.com"
    hashed:                 false
▾ recipientProfile:
  ▾ type:
      0:                    "RecipientProfile"
      1:                    "Extension"
    name:                   "Migelan Kodra"
  ▸ publicKey:              "Ecdsa-koblitz-pubkey:0x7…12c5e87682EA0118C398aD3"
▾ badge:
    type:                   "BadgeClass"
    id:                     "urn:uuid:82a4c9f2-3588-457b-80ea-da695571b8fc"
    name:                   "Master's Degree in Electronic Engineering"
    description:            "Master's Degree in Electronic Engineering"
  ▸ image:                  "data:image/png;base64,iV…ysWRhQAAAABJRU5ErkJggg=="
  ▾ issuer:
    ▸ id:                   "https://raw.githubuserco…ter/issuer-info-eth.json"
      type:                 "Profile"
      name:                 "Università Politecnica delle Marche"
      url:                  "https://www.univpm.it/Entra/"
      email:                "info@univpm.it"
    ▸ image:                "data:image/png;base64,iV…gDPhZawAAAAASUVORK5CYII="
    ▸ revocationList:       "https://www.blockcerts.o…cation-list-testnet.json"
  ▾ criteria:
      narrative:            "Master's Degree in Electronic Engineering"
  ▾ signatureLines:
    ▾ 0:
      ▸ type:               […]
        jobTitle:           "Università Politecnica delle Marche - Student"
      ▸ image:              "data:image/png;base64,iV…31JdhQAAAABJRU5ErkJggg=="
        name:               "Migelan Kodra"
▾ verification:
  ▾ type:
      0:                    "MerkleProofVerification2017"
      1:                    "Extension"
  ▸ publicKey:              "ecdsa-koblitz-pubkey:0x1…7AF9d03f82b1734E667E151"
▾ signature:
  ▾ type:
      0:                    "MerkleProof2017"
      1:                    "Extension"
  ▾ merkleRoot:             "4879c33a985ba1a5cb421533c15dc74d3d3ebda72cdb7f275711cac8129e16da"
  ▾ targetHash:             "4879c33a985ba1a5cb421533c15dc74d3d3ebda72cdb7f275711cac8129e16da"
    proof:                  []
  ▾ anchors:
    ▾ 0:
      ▸ sourceId:           "0x14e97be56509d716cf7f31…164ad3c09519fa8790f2f0c"
        type:               "ETHData"
        chain:              "ethereumMainnet"
```

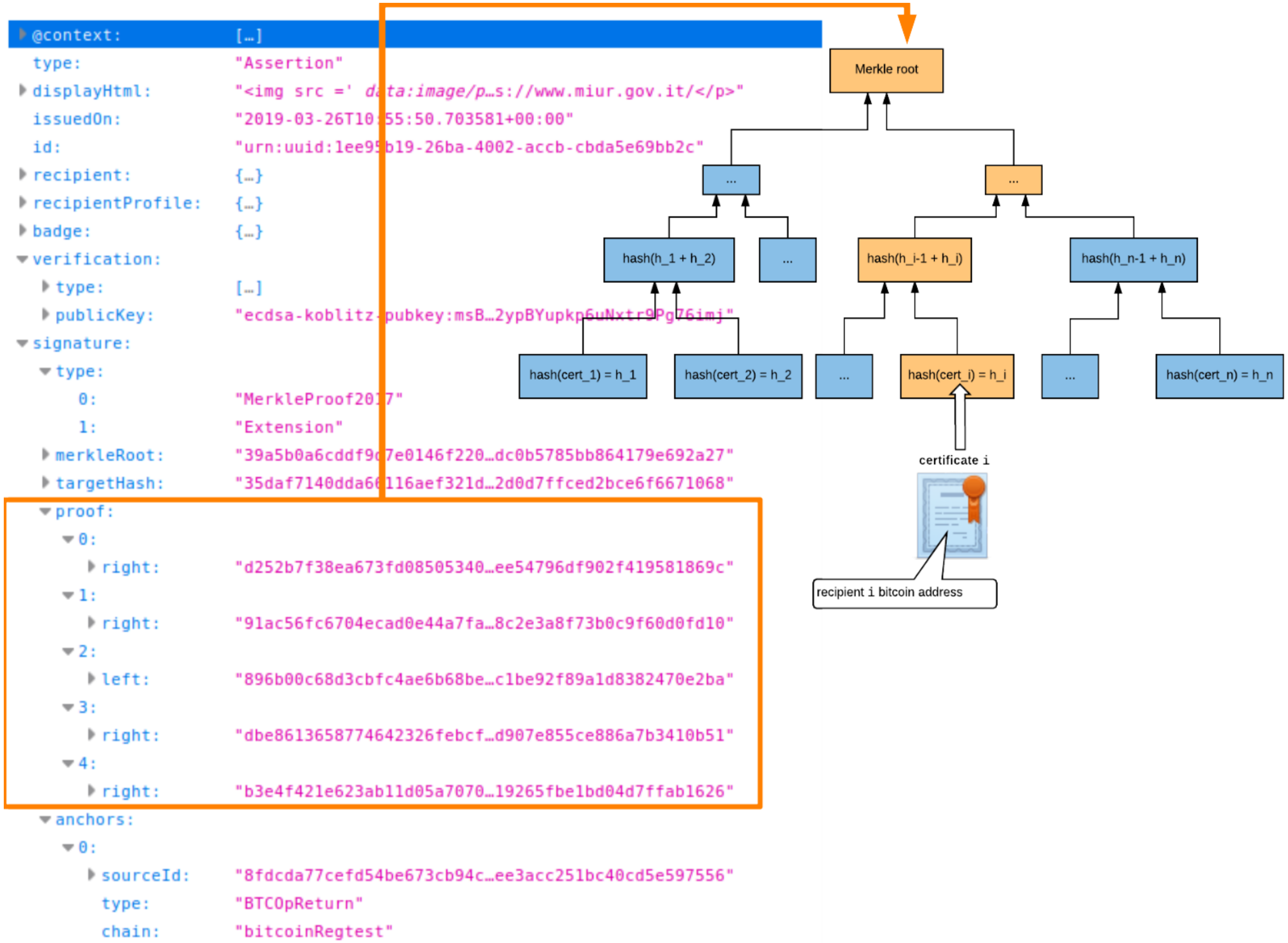
Hash Calculator

Certificate Hash Value

Compare
the calculated hash value
of the certificate
with the hash value
written on the receipt

Certificate Authenticity

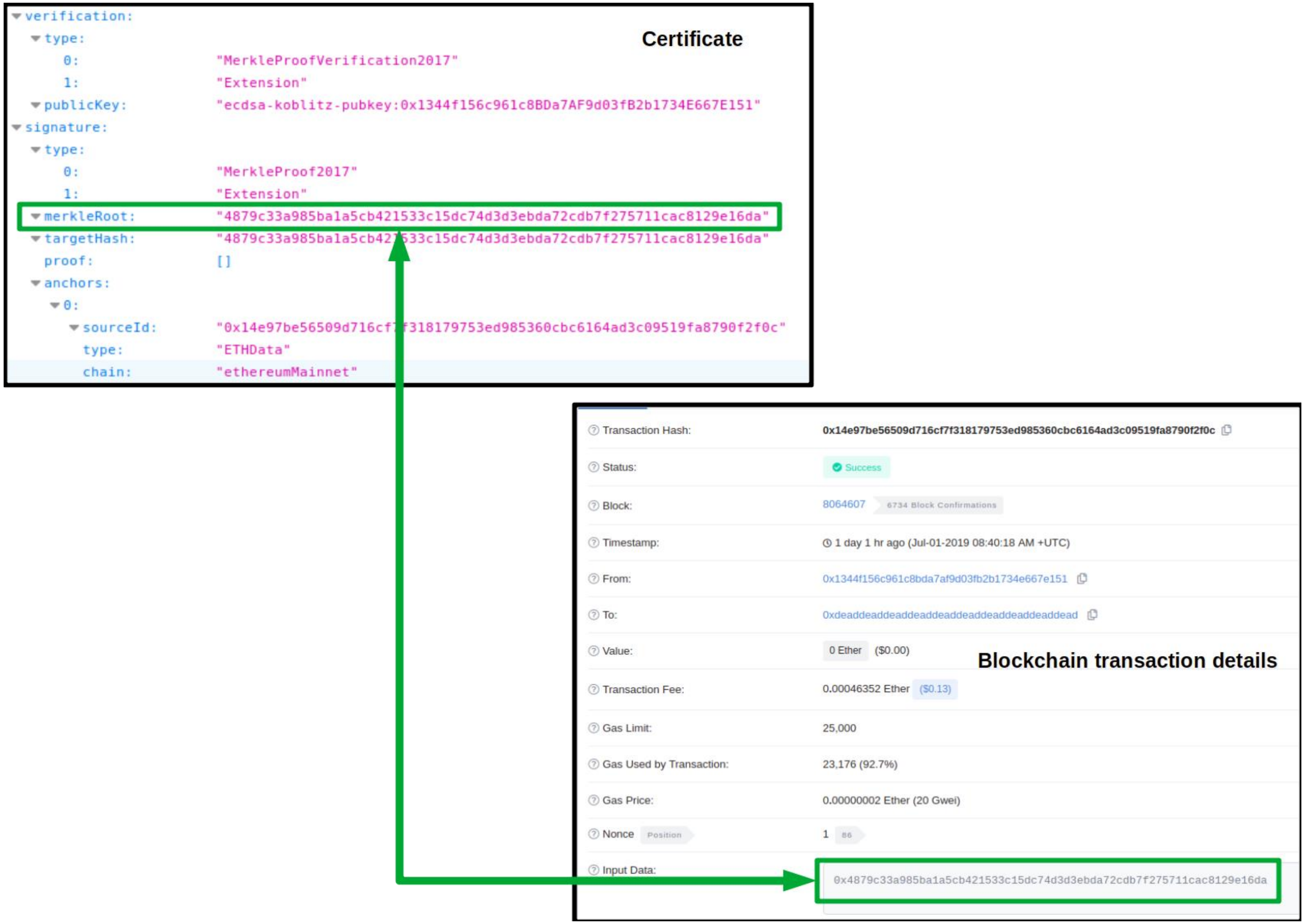
- Step 2: The **Merkle Path** is valid.



```
▸ @context:              […]
  type:                  "Assertion"
▸ displayHtml:           "<img src =' data:image/p…s://www.miur.gov.it/</p>"
  issuedOn:              "2019-03-26T10:55:50.703581+00:00"
  id:                    "urn:uuid:1ee95[illegible]b19-26ba-4002-accb-cbda5e69bb2c"
▸ recipient:             {…}
▸ recipientProfile:      {…}
▸ badge:                 {…}
▾ verification:
  ▸ type:                […]
  ▸ publicKey:           "ecdsa-koblitz-pubkey:msB…2ypBYupkp6uNxtr9Pg76imj"
▾ signature:
  ▾ type:
      0:                 "MerkleProof2017"
      1:                 "Extension"
  ▸ merkleRoot:          "39a5b0a6cddf9d7e0146f220…dc0b5785bb864179e692a27"
  ▸ targetHash:          "35daf7140dda66116aef321d…2d0d7ffced2bce6f6671068"
  ▾ proof:
    ▾ 0:
      ▸ right:           "d252b7f38ea673fd08505340…ee54796df902f419581869c"
    ▾ 1:
      ▸ right:           "91ac56fc6704ecad0e44a7fa…8c2e3a8f73b0c9f60d0fd10"
    ▾ 2:
      ▸ left:            "896b00c68d3cbfc4ae6b68be…c1be92f89a1d8382470e2ba"
    ▾ 3:
      ▸ right:           "dbe8613658774642326febcf…d907e855ce886a7b3410b51"
    ▾ 4:
      ▸ right:           "b3e4f421e623ab11d05a7070…19265fbe1bd04d7ffab1626"
  ▾ anchors:
    ▾ 0:
      ▸ sourceId:        "8fdcda77cefd54be673cb94c…ee3acc251bc40cd5e597556"
        type:            "BTCOpReturn"
        chain:           "bitcoinRegtest"
```

Certificate Authenticity

- Step 3: The **Merkle Root** stored on the blockchain matches the value in the receipt.



Certificate

```
▾ verification:
  ▾ type:
      0:                    "MerkleProofVerification2017"
      1:                    "Extension"
  ▾ publicKey:              "ecdsa-koblitz-pubkey:0x1344f156c961c8BDa7AF9d03fB2b1734E667E151"
▾ signature:
  ▾ type:
      0:                    "MerkleProof2017"
      1:                    "Extension"
  ▾ merkleRoot:             "4879c33a985ba1a5cb421533c15dc74d3d3ebda72cdb7f275711cac8129e16da"
  ▾ targetHash:             "4879c33a985ba1a5cb421533c15dc74d3d3ebda72cdb7f275711cac8129e16da"
    proof:                  []
  ▾ anchors:
    ▾ 0:
      ▾ sourceId:           "0x14e97be56509d716cf7f318179753ed985360cbc6164ad3c09519fa8790f2f0c"
        type:               "ETHData"
        chain:              "ethereumMainnet"
```

Blockchain transaction details

Transaction Hash: 0x14e97be56509d716cf7f318179753ed985360cbc6164ad3c09519fa8790f2f0c

Status: ✓ Success

Block: 8064607 6734 Block Confirmations

Timestamp: 1 day 1 hr ago (Jul-01-2019 08:40:18 AM +UTC)

From: 0x1344f156c961c8bda7af9d03fb2b1734e667e151

To: 0xdeaddeaddeaddeaddeaddeaddeaddeaddeaddead

Value: 0 Ether ($0.00)

Transaction Fee: 0.00046352 Ether ($0.13)

Gas Limit: 25,000

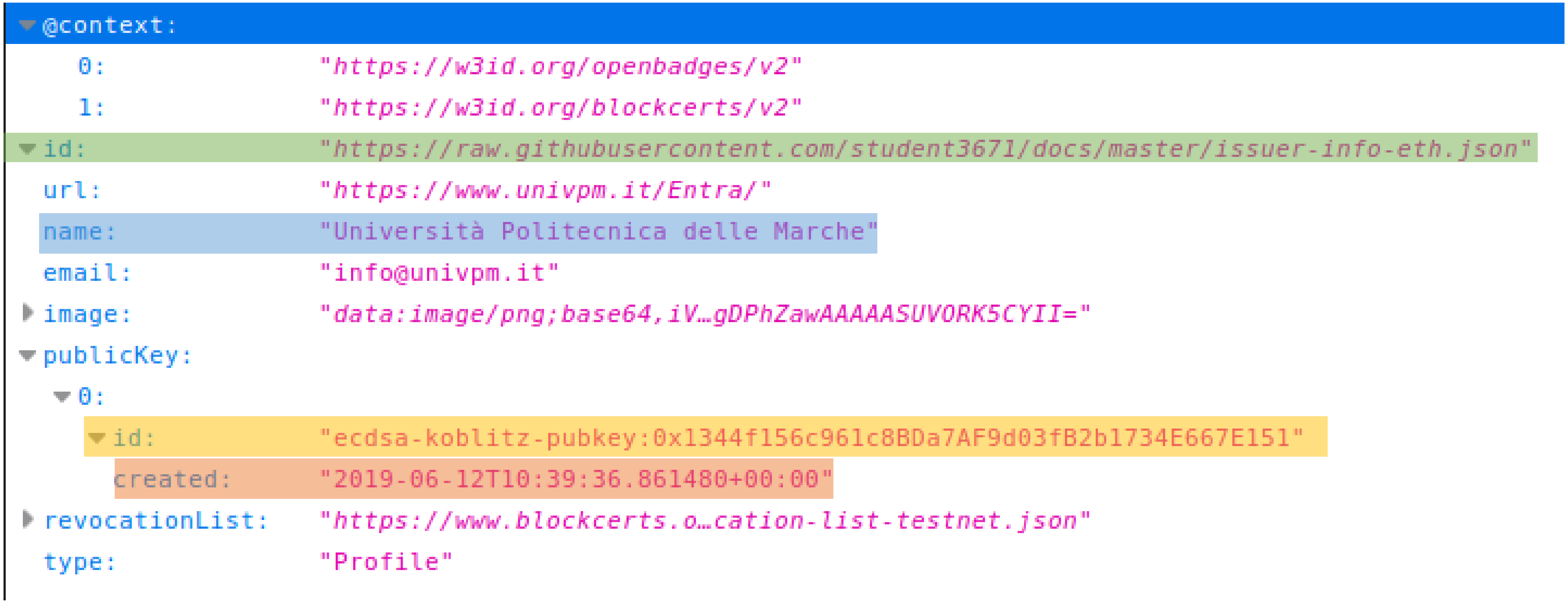
Gas Used by Transaction: 23,176 (92.7%)

Gas Price: 0.00000002 Ether (20 Gwei)

Nonce Position: 1 86

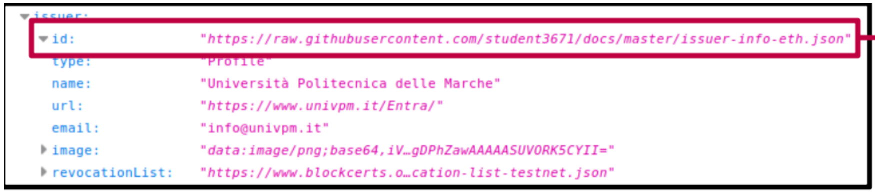
Input Data: 0x4879c33a985ba1a5cb421533c15dc74d3d3ebda72cdb7f275711cac8129e16da

Hosted Issuer Profile



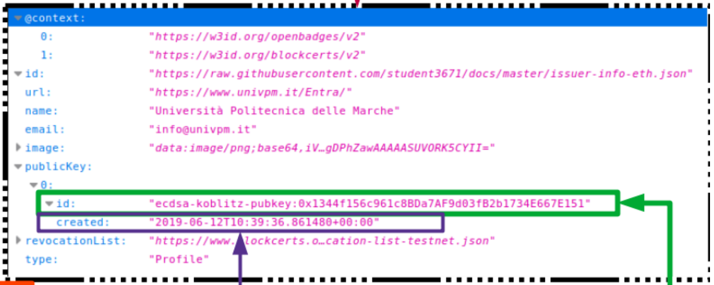
```
▼ @context:
    0:               "https://w3id.org/openbadges/v2"
    1:               "https://w3id.org/blockcerts/v2"
▼ id:                "https://raw.githubusercontent.com/student3671/docs/master/issuer-info-eth.json"
  url:               "https://www.univpm.it/Entra/"
  name:              "Università Politecnica delle Marche"
  email:             "info@univpm.it"
▶ image:             "data:image/png;base64,iV…gDPhZawAAAAASUVORK5CYII="
▼ publicKey:
  ▼ 0:
    ▼ id:            "ecdsa-koblitz-pubkey:0x1344f156c961c8BDa7AF9d03fB2b1734E667E151"
      created:       "2019-06-12T10:39:36.861480+00:00"
▶ revocationList:    "https://www.blockcerts.o…cation-list-testnet.json"
  type:              "Profile"
```

Issuer Identity Verification

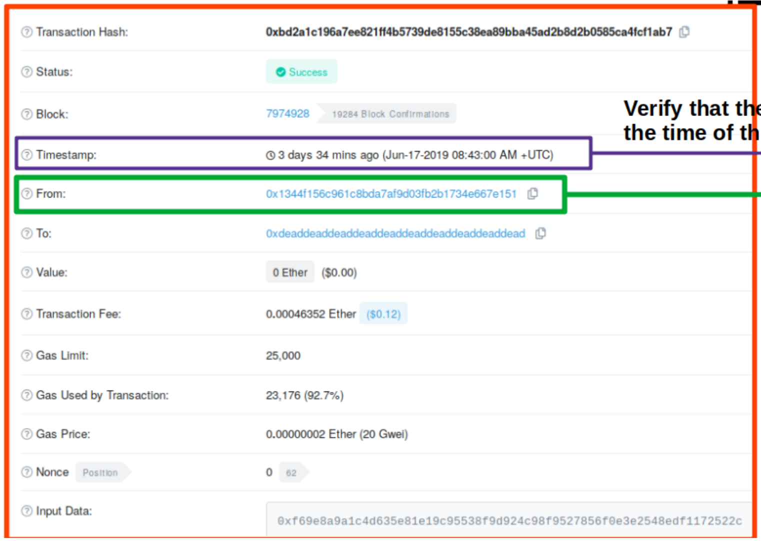


```
▼ issuer:
  ▼ id:              "https://raw.githubusercontent.com/student3671/docs/master/issuer-info-eth.json"
    type:            "Profile"
    name:            "Università Politecnica delle Marche"
    url:             "https://www.univpm.it/Entra/"
    email:           "info@univpm.it"
  ▶ image:           "data:image/png;base64,iV…gDPhZawAAAAASUVORK5CYII="
  ▶ revocationList:  "https://www.blockcerts.o…cation-list-testnet.json"
```

Getting Hosted Issuer ID



```
▼ @context:
    0:               "https://w3id.org/openbadges/v2"
    1:               "https://w3id.org/blockcerts/v2"
▼ id:                "https://raw.githubusercontent.com/student3671/docs/master/issuer-info-eth.json"
  url:               "https://www.univpm.it/Entra/"
  name:              "Università Politecnica delle Marche"
  email:             "info@univpm.it"
▶ image:             "data:image/png;base64,iV…gDPhZawAAAAASUVORK5CYII="
▼ publicKey:
  ▼ 0:
    ▼ id:            "ecdsa-koblitz-pubkey:0x1344f156c961c8BDa7AF9d03fB2b1734E667E151"
      created:       "2019-06-12T10:39:36.861480+00:00"
▶ revocationList:    "https://www.blockcerts.o…cation-list-testnet.json"
  type:              "Profile"
```



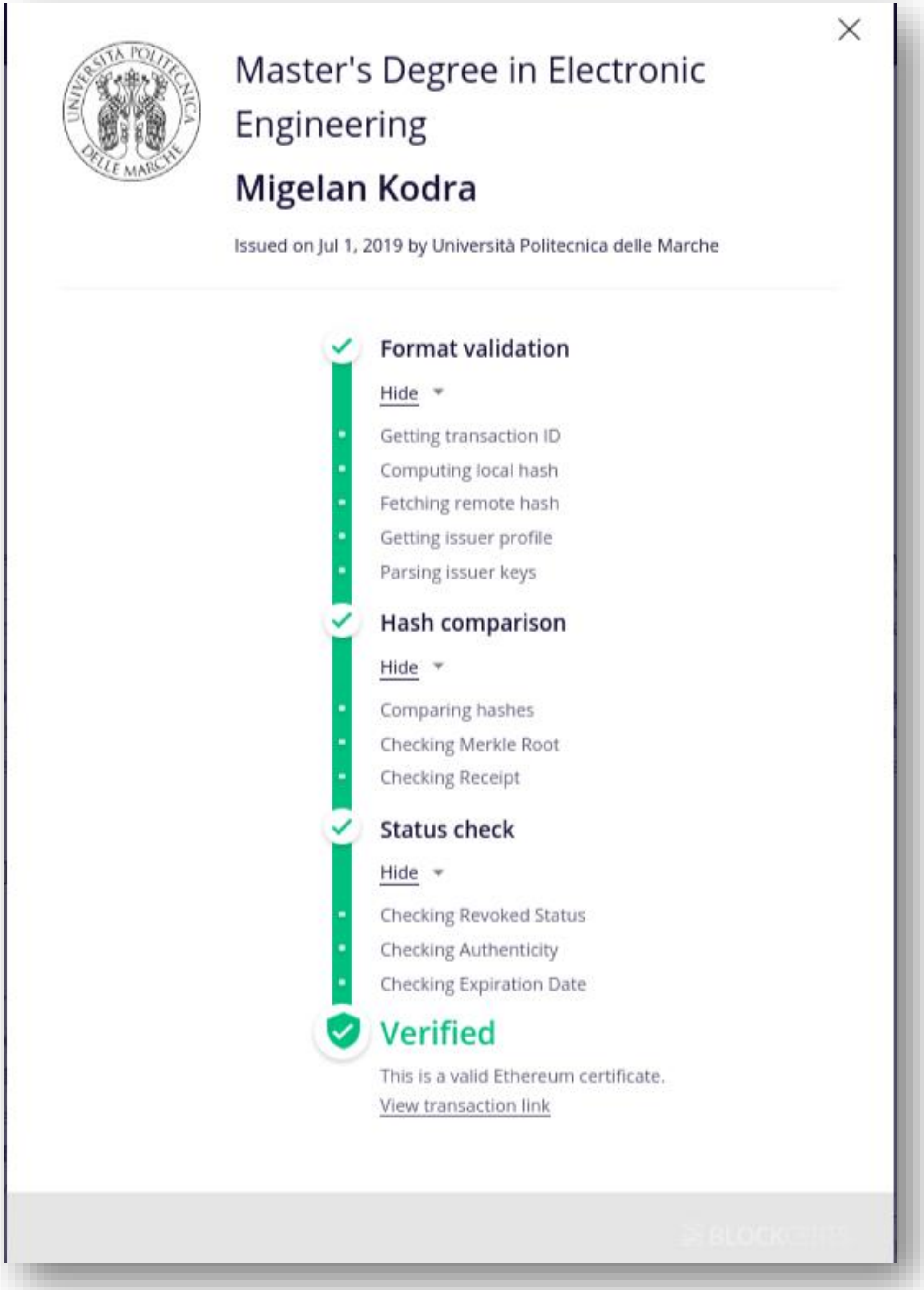
```
Transaction Hash:            0xbd2a1c196a7ee821ff4b5739de8155c38ea89bba45ad2b8d2b0585ca4fcf1ab7
Status:                      ✓ Success
Block:                       7974928   19284 Block Confirmations
Timestamp:                   3 days 34 mins ago (Jun-17-2019 08:43:00 AM +UTC)
From:                        0x1344f156c961c8bda7af9d03fb2b1734e667e151
To:                          0xdeaddeaddeaddeaddeaddeaddeaddeaddeaddead
Value:                       0 Ether   ($0.00)
Transaction Fee:             0.00046352 Ether   ($0.12)
Gas Limit:                   25,000
Gas Used by Transaction:     23,176 (92.7%)
Gas Price:                   0.00000002 Ether (20 Gwei)
Nonce   Position             0   62
Input Data:                  0xf69e8a9a1c4d635e81e19c95538f9d924c98f9527856f0e3e2548edf1172522c
```

Verify that the key was valid at the time of the transaction

Confront Transaction Key with Hosted ID Key

Blockcerts vulnerability

- The Blockcerts protocol does not verify that the *issuer_id* extracted from a certificate indeed points to a web address that is owned by the legitimate issuing.
- This allows hijacking of the verifier towards a fake issuer profile, which can perfectly resemble the one of the legitimate institution.
- A fake issuer profile was created for the Università Politecnica delle Marche and hosted on a Github domain.
- During the verification process, the Blockcerts protocol checks the public key on the blockchain transaction corresponding to the certificate, and compares it with the key included in the issuer profile published online.
- This brings to a successful verification through Blockcerts, and to a forged certificate that is practically indistinguishable from a legitimate one.



Master's Degree in Electronic Engineering

Migelan Kodra

Issued on Jul 1, 2019 by Università Politecnica delle Marche

✓ **Format validation**

Hide ▾

- Getting transaction ID
- Computing local hash
- Fetching remote hash
- Getting issuer profile
- Parsing issuer keys

✓ **Hash comparison**

Hide ▾

- Comparing hashes
- Checking Merkle Root
- Checking Receipt

✓ **Status check**

Hide ▾

- Checking Revoked Status
- Checking Authenticity
- Checking Expiration Date

✓ **Verified**

This is a valid Ethereum certificate.

View transaction link

Possible countermeasures

1. Replacing the issuer profile referenced from the *issuer_id* field with a digital certificate containing the public key of the issuing institution, and released by an accredited certification authority.

2. Applying Decentralized Identifiers (DIDs), based on initiatives like those in [5]:

   - W3C Community Group - Decentralized Identifier,

   - W3C Working Group - Verifiable Claims,

   - DIF - DID Auth.

[5] CEN/CENELEC Focus Group BDLT, "Recommendations for successful adoption in Europe of emerging technical standards on distributed ledger/blockchain technologies," Tech. Rep., Jul 2018.

Conclusions

- The Blockcerts protocol does not provide any strong mechanism for authenticating the issuing institution, since the issuer authentication is basically performed on the basis of an unauthenticated issuer profile available online and referenced from inside the certificate.
- A legitimate issuing institution can be easily impersonated by suitably fabricating a fake issuer profile.
- Apparently legitimate academic credentials can be released, which the Blockcerts validation mechanisms are unable to distinguish from valid academic credentials issued by the legitimate institution.
- **This clearly highlights a vulnerability of this protocol, especially when it is used for the certification of academic credentials with legal value.**
- Suitable countermeasures can be conceived, that however are currently under development, and cannot provide an immediate solution to the highlighted vulnerability.

Thank you

m.kodra@reply.it