PA tamu

- Piattaforma trustless per la gestione end-to-end dei bandi di gara
- Registro unico dei certificati emessi dalle singole autorità

Forum E- Procurement, 3 Maggio 2017

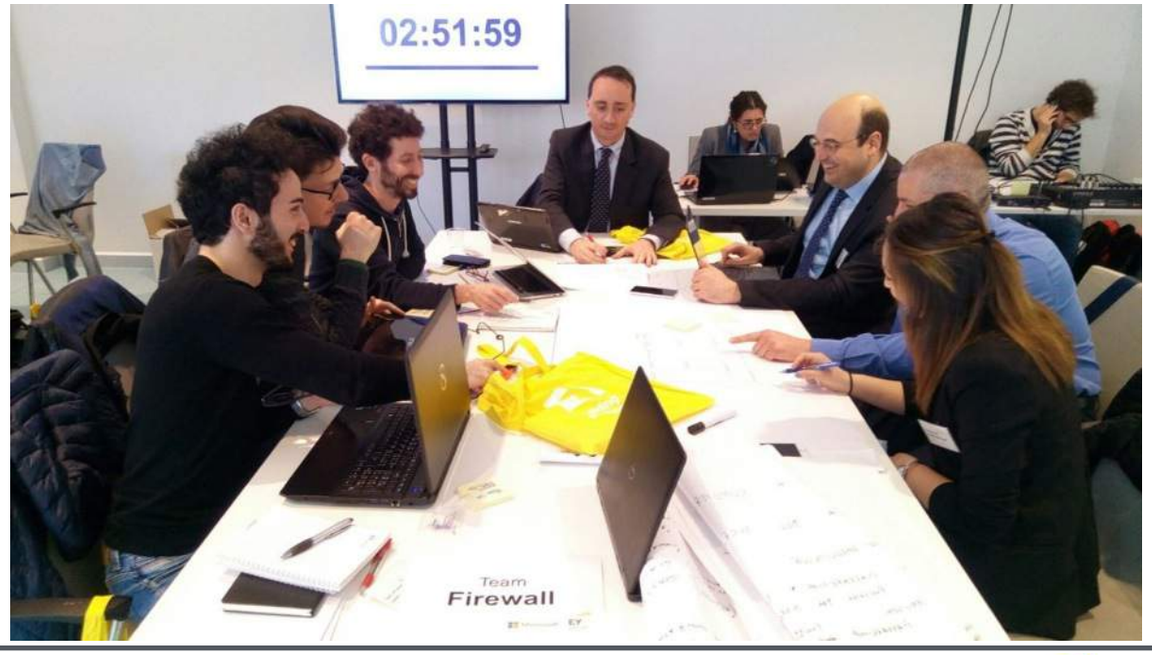
Adriano Bonforti, Founder - adriano@patamu.com

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

patamu.com

Blockchain hackaton PA
#Firewall Team



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Microsoft

sogei

EY
Building a better working world

Overview del concept

L'idea: PA-tamu

- Piattaforma trustless con marca temporale, controllo continuo dell'autenticità, resistenza alla falsificazione, riduzione della discrezionalità nella valutazione

- Registro unico dei certificati emessi dalle singole autorità

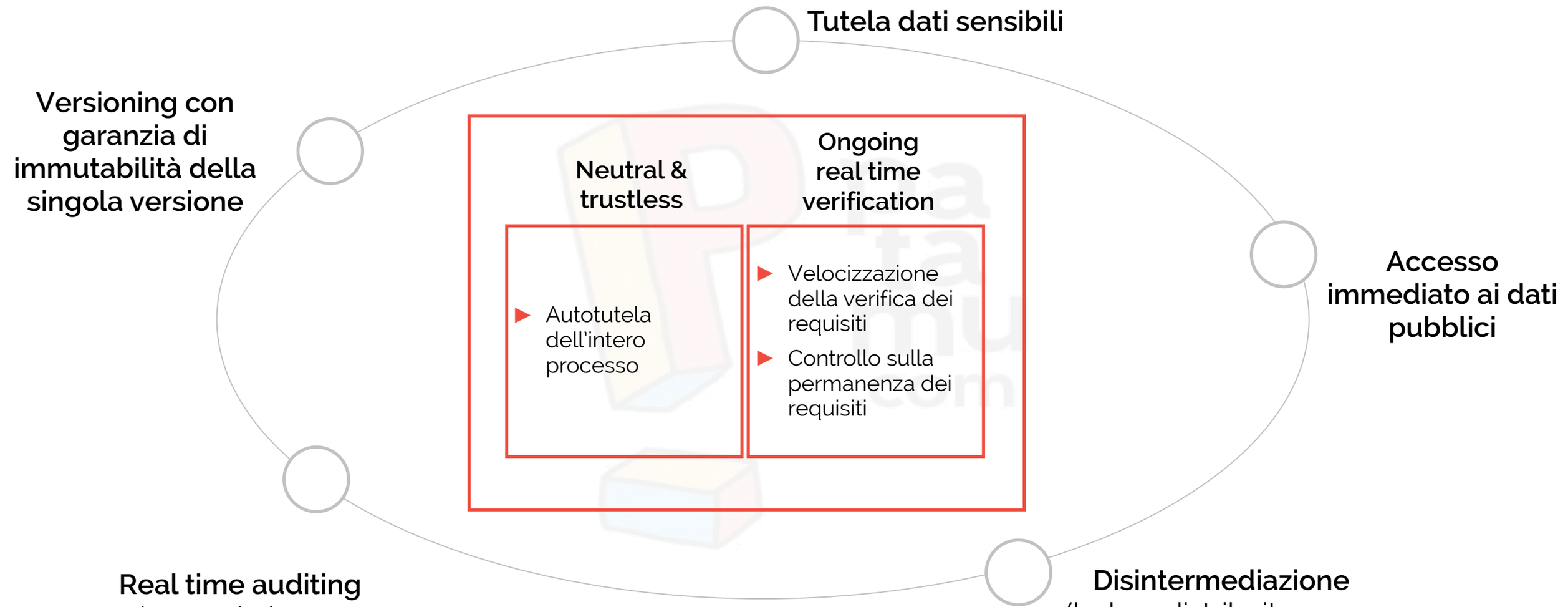
Pubblicazione | **Gara** | **Stipula**

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

patamu.com

Perché è innovativa per la PA



Perché l'idea può essere realizzata da parte della PA

Sostenibilità tecnica

- **Processo di verifica tramite blockchain già in produzione** (es. patamu)
- **Perimetro ben definito:** semplice integrazione con l'infrastruttura già esistente

Sostenibilità economica

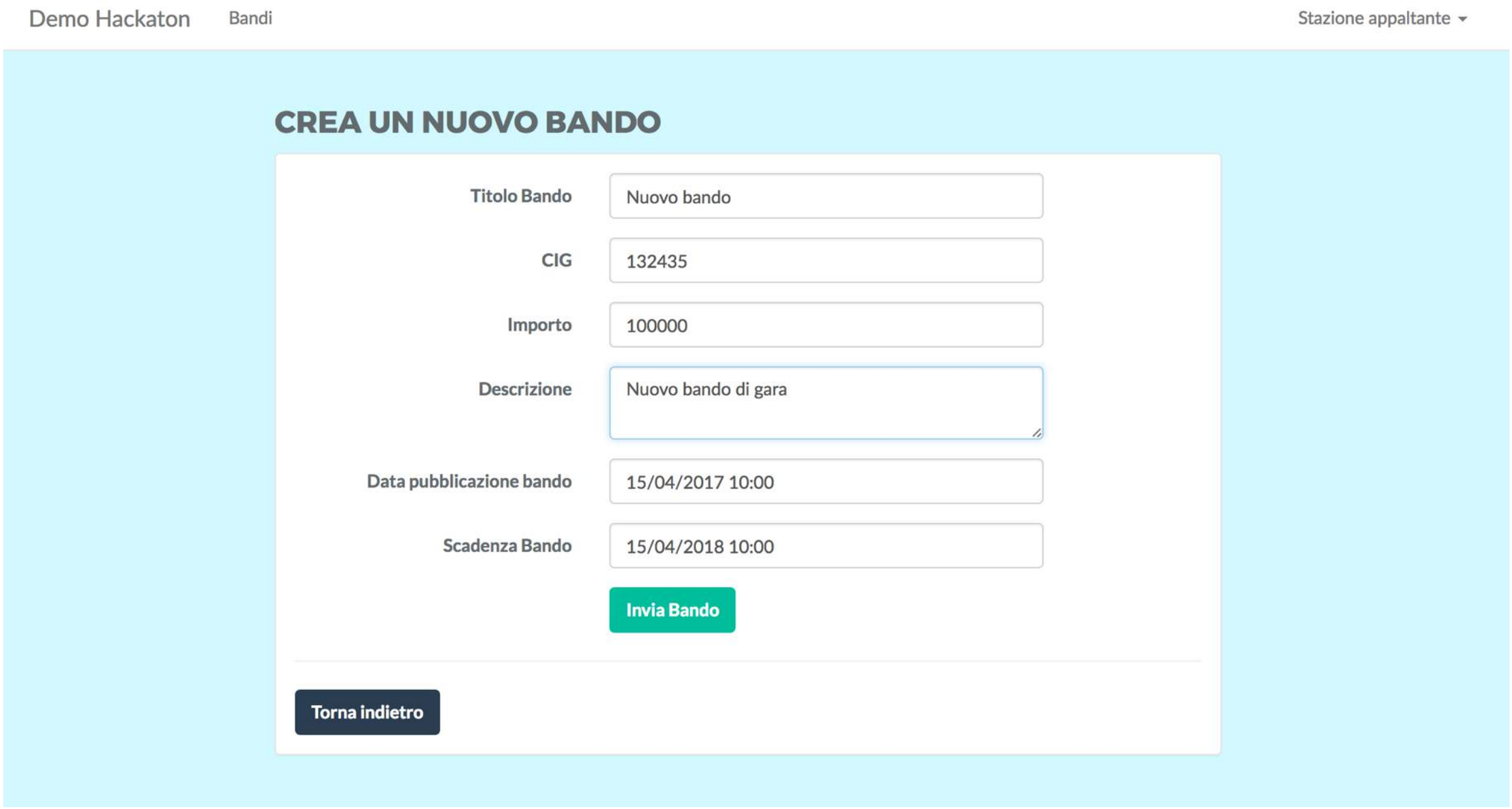
- **Smart footprint** con share dei costi tra gli stakeholder della piattaforma (PA e imprese)
- Soluzione SaaS
- Deployment su piattaforma cloud della PA

Inclusione delle PMI

- Semplificazione delle procedure di accesso ai bandi
- Garanzia di maggiore trasparenza e rispetto tempistiche
- Monitoraggio continuo dello stato del processo

Demo

Demo



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

Patamu.com

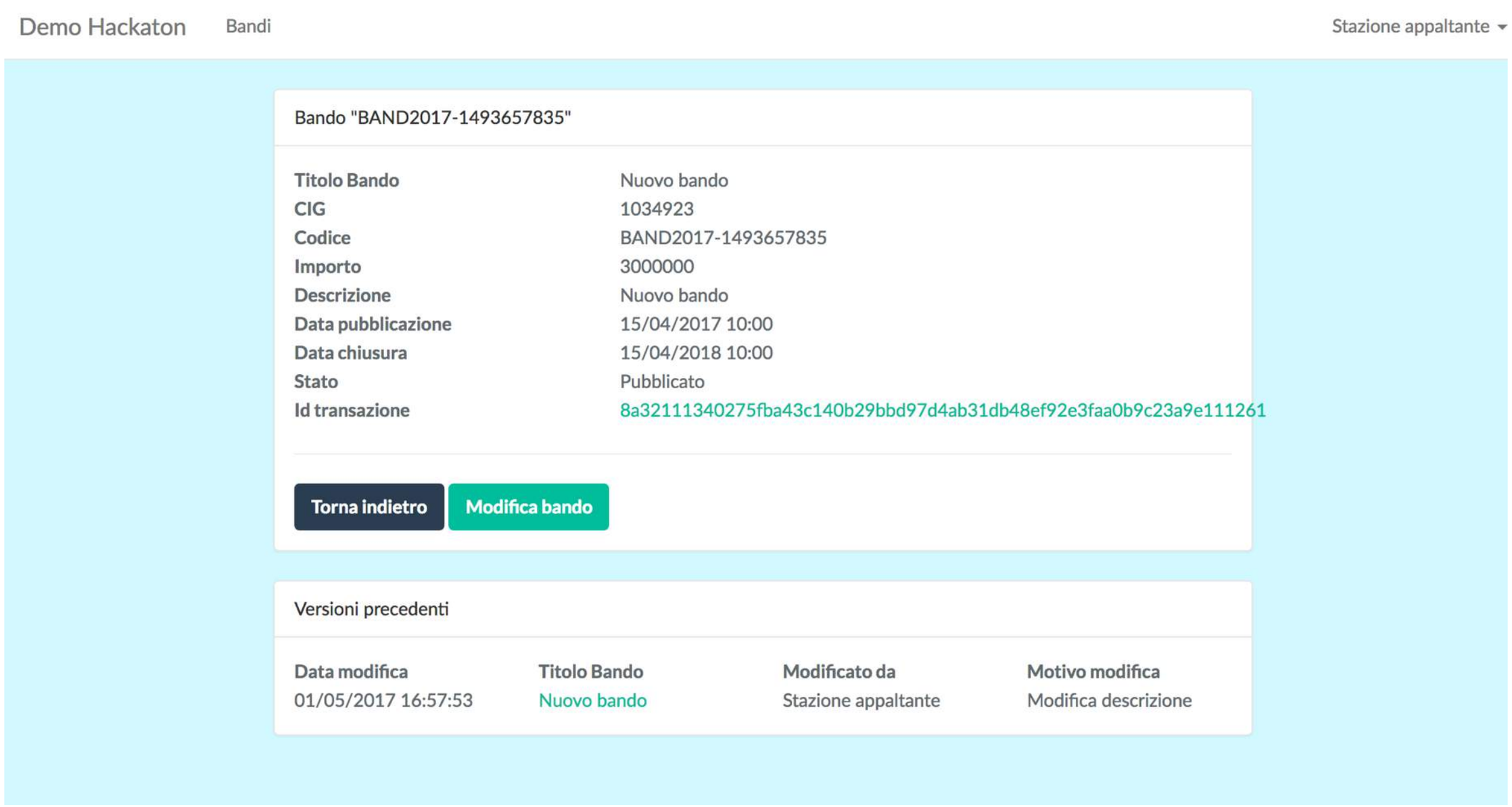
Demo

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

Patamu.com

Demo



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

Patamu.com

Demo

Demo Hackaton Offerte bando Certificazioni Azienda

← Back

Invia una nuova offerta

Cig Bando 1034923

Descrizione offerta Offerta per il bando di gara

Codici da verificare

Antimafia

DURC

Invia offerta

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

Patamu.com

Demo

REGISTRO CERTIFICATI

RICHIEDI VERIFICA

RICHIEDI CERTIFICAZIONE

Antimafia

Patamu

patamu@patamu.com

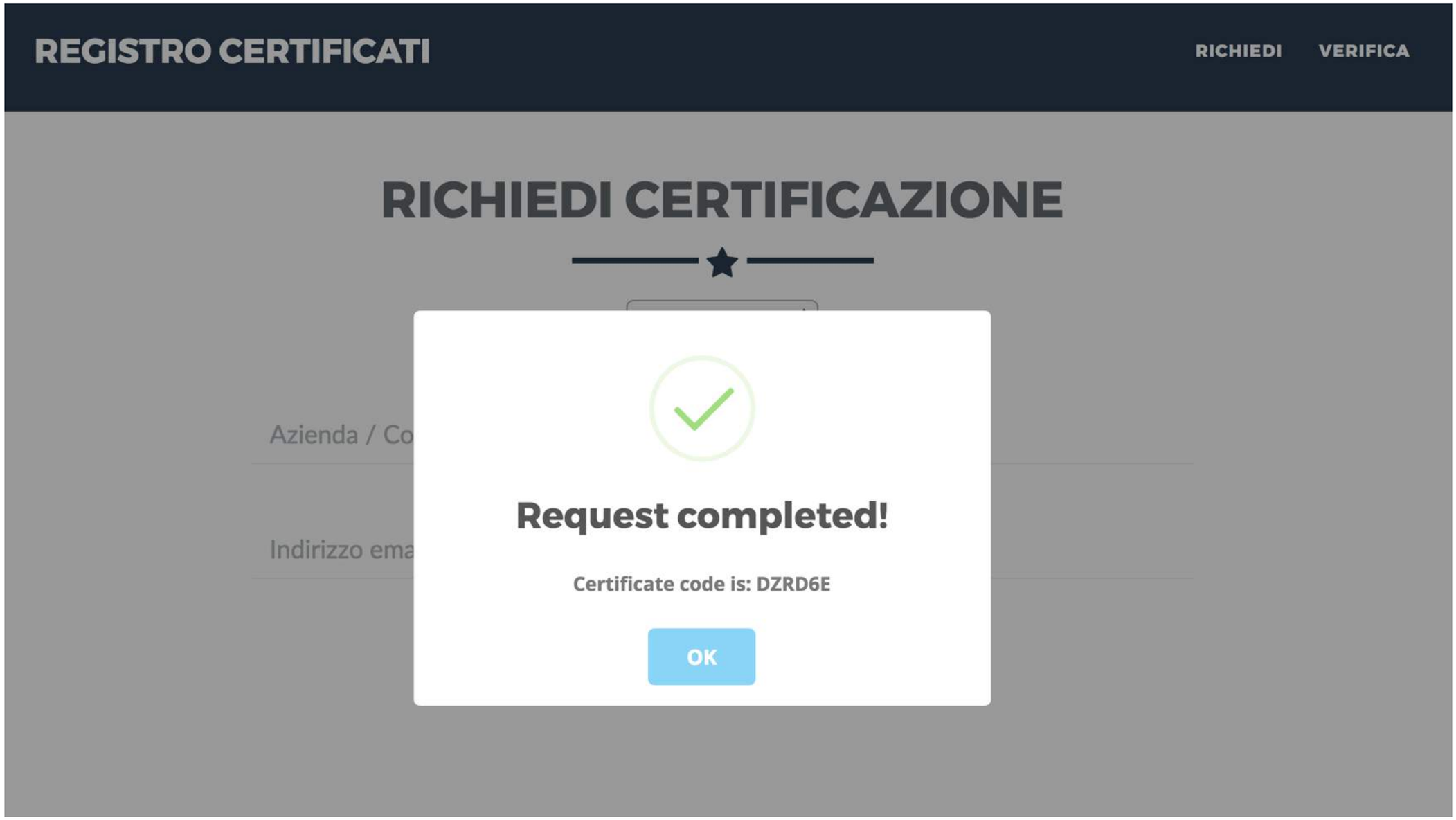
Richiedi certificato

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

patamu.com

Demo

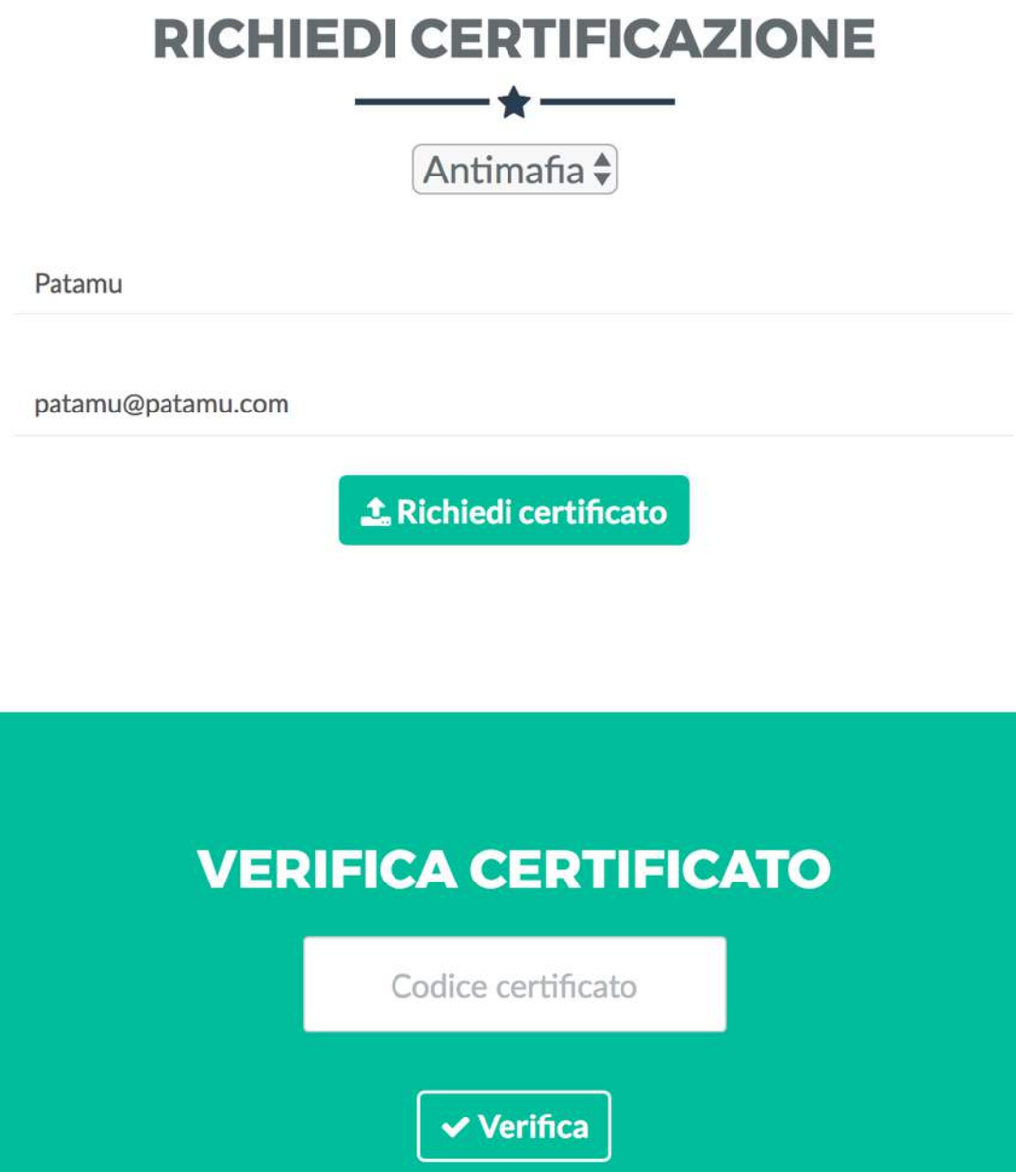


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

Patamu.com

Demo

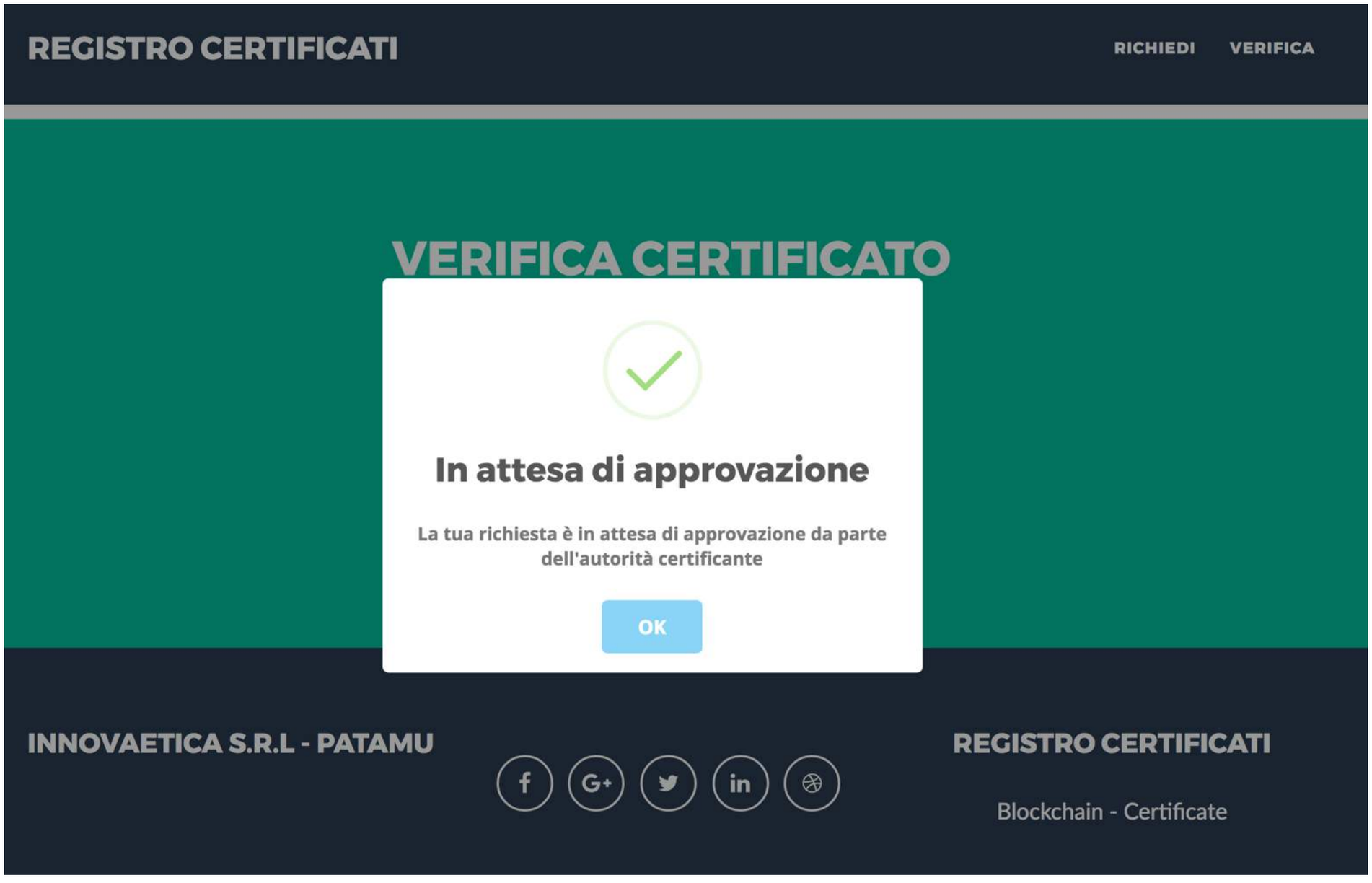


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

patamu.com

Demo

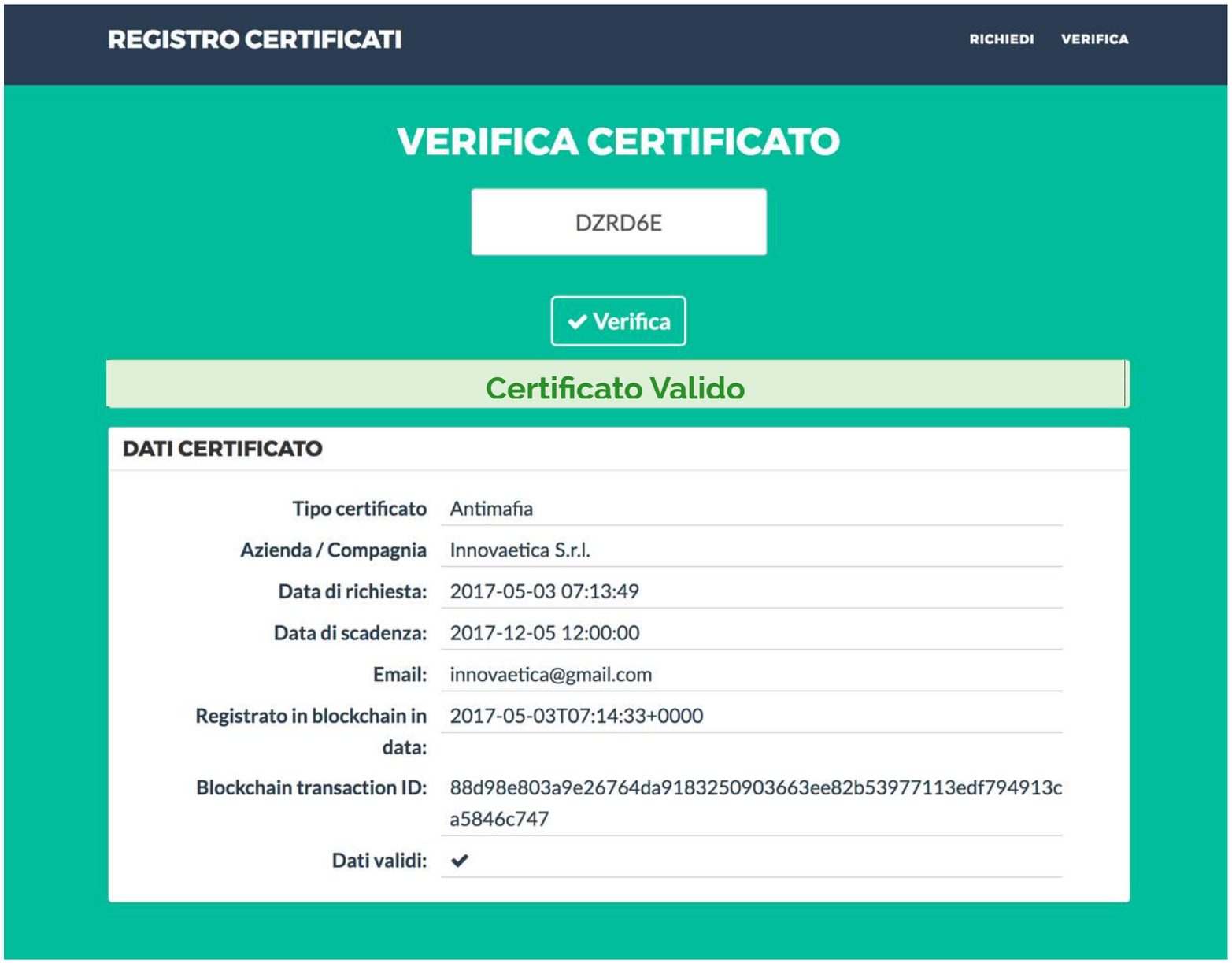


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

patamu.com

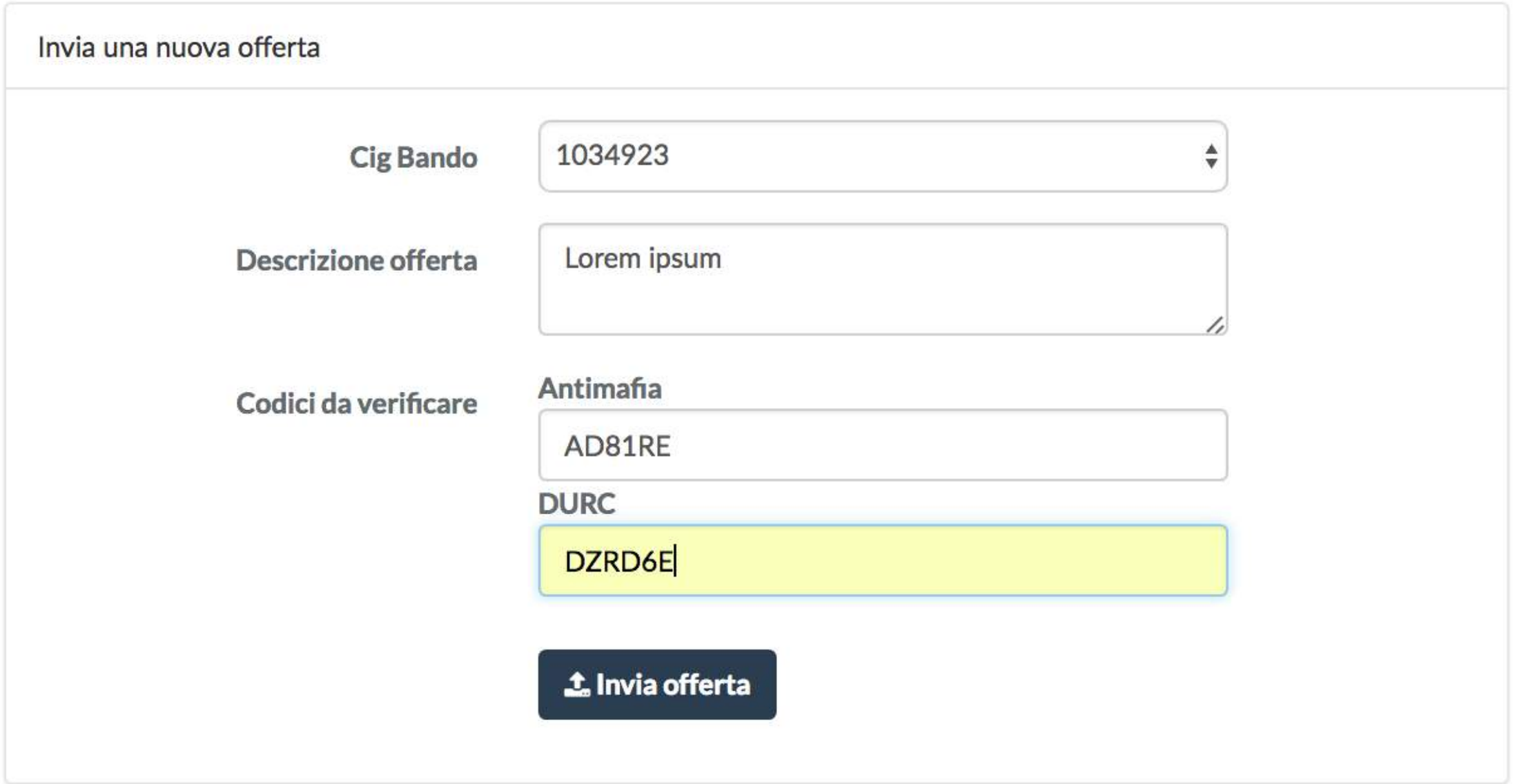
Demo



È possibile verificare in qualsiasi momento la validità del certificato emesso inserendo il codice di validità del certificato cui si è interessati (p.es **DZRD6E**).

Quando viene inserito un codice il sistema verifica i dati locali con i dati inseriti permanentemente nella Blockchain.

Demo

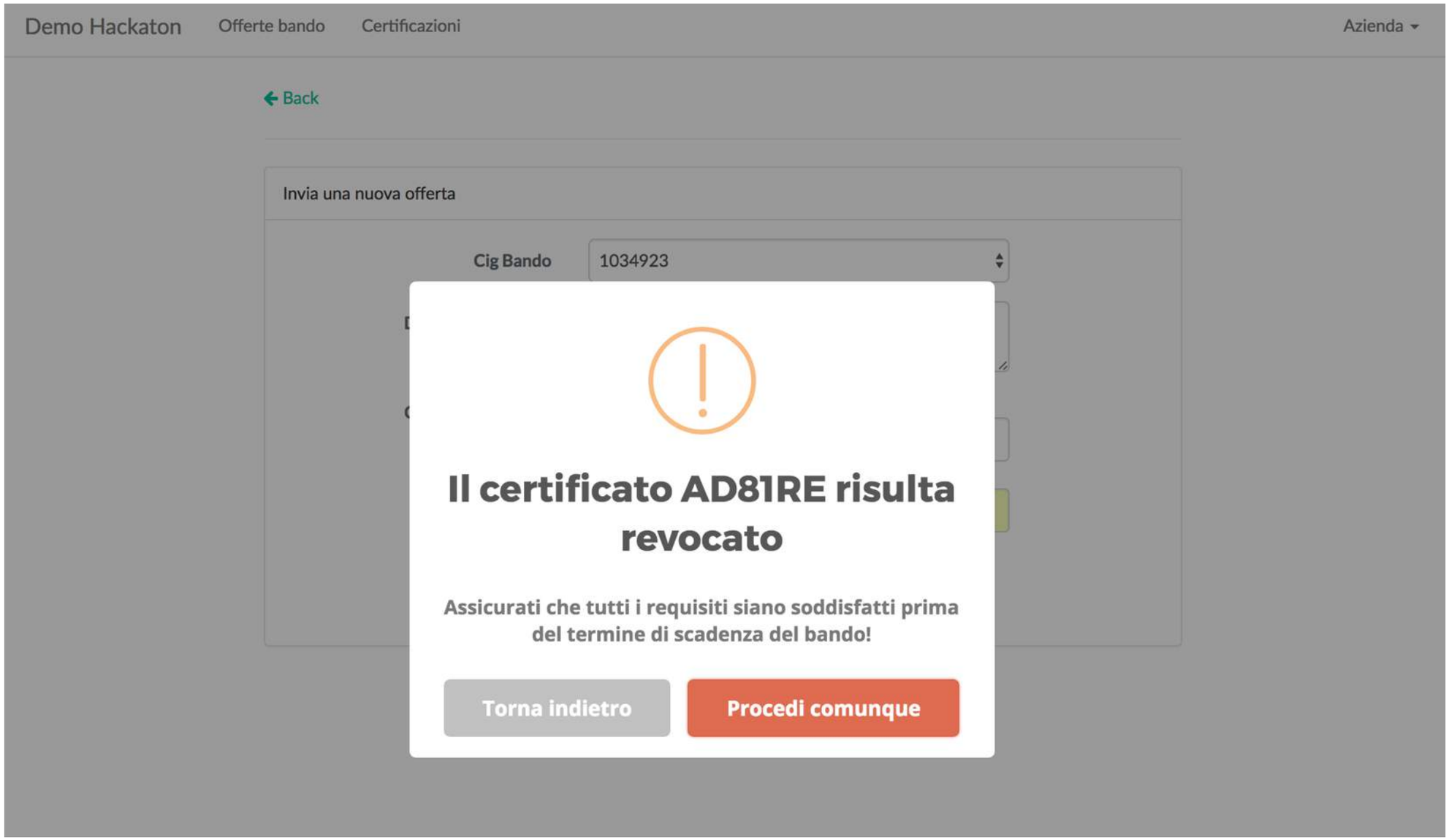


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

patamu.com

Demo

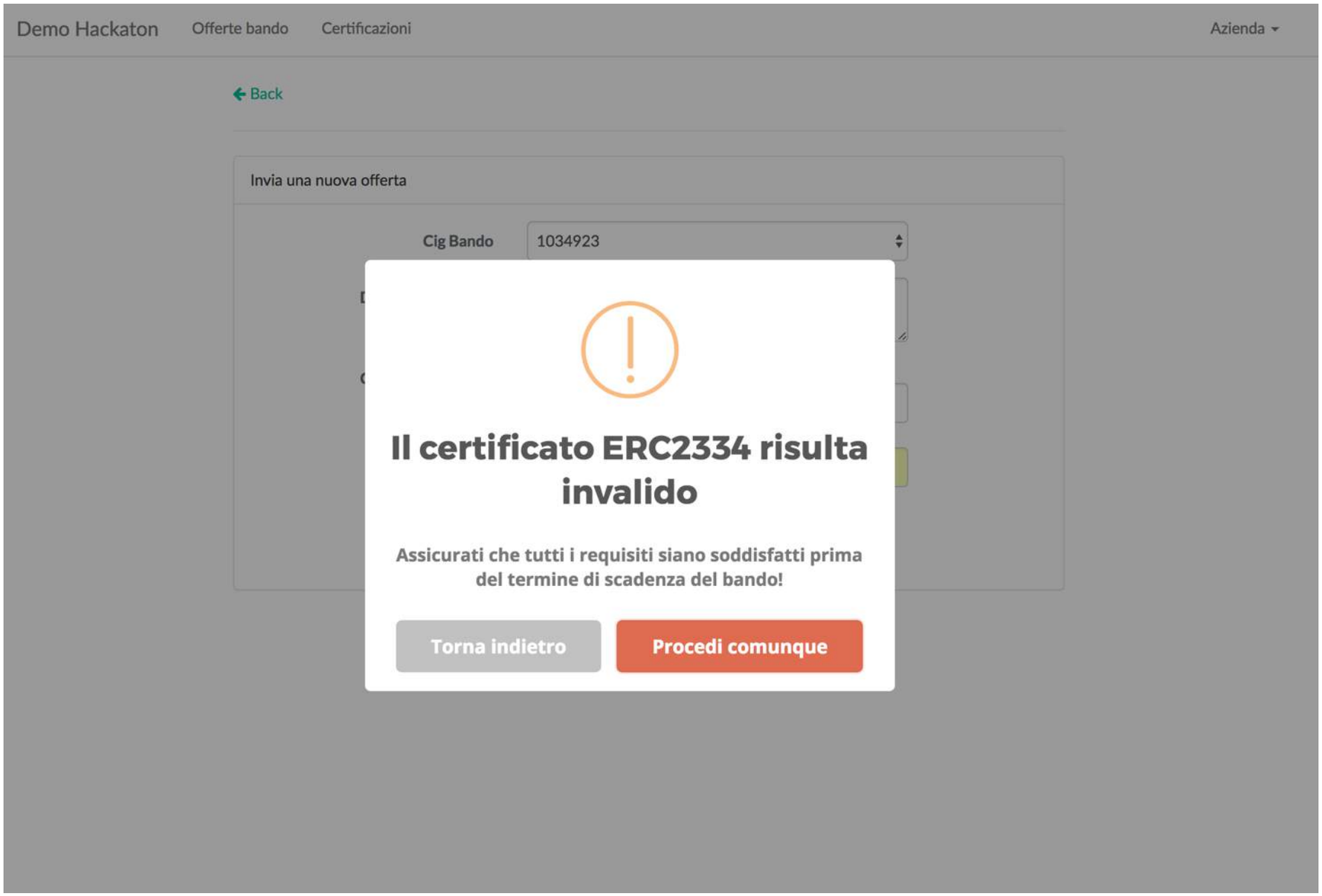


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

Patamu .com

Demo

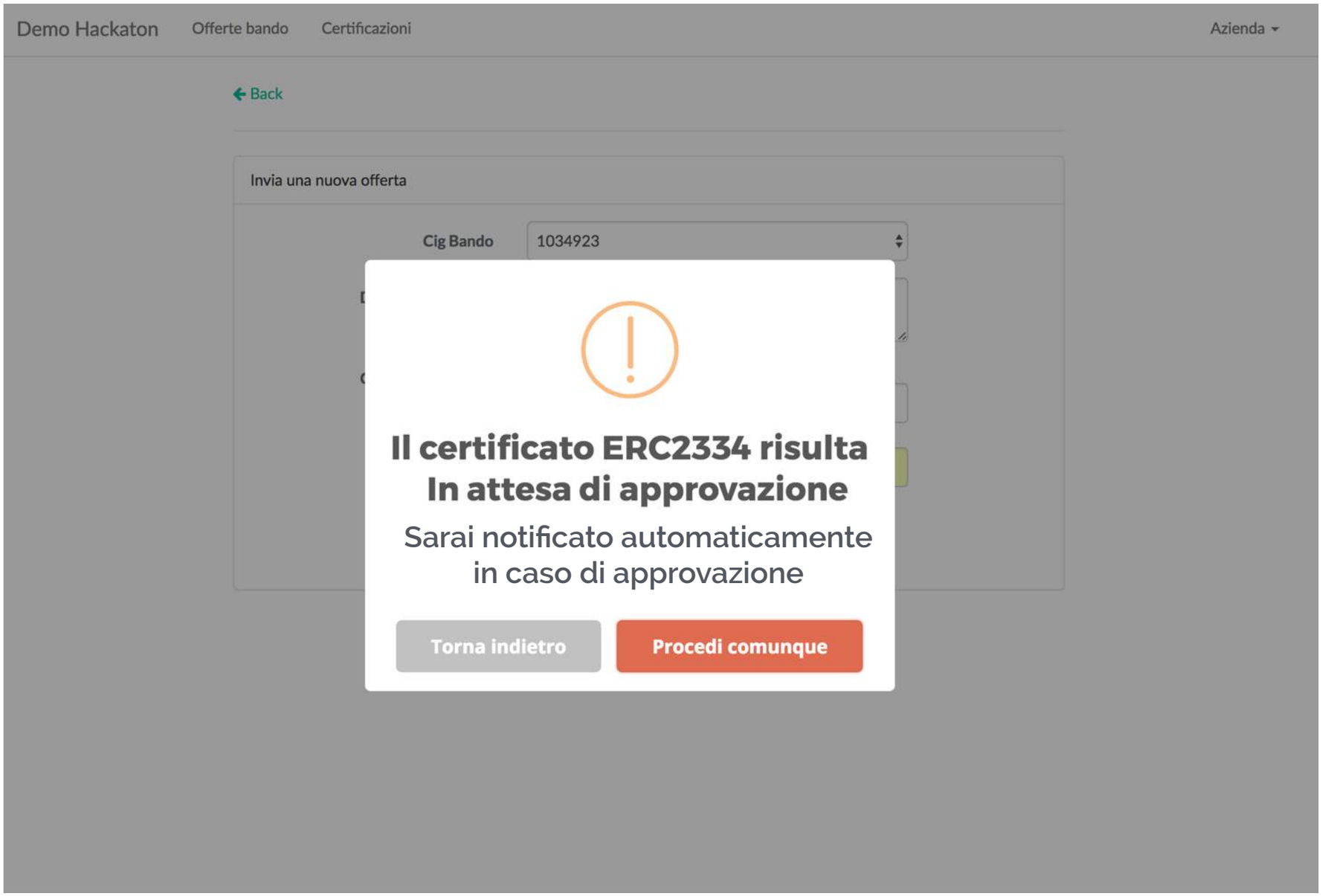


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

Patamu.com

Demo

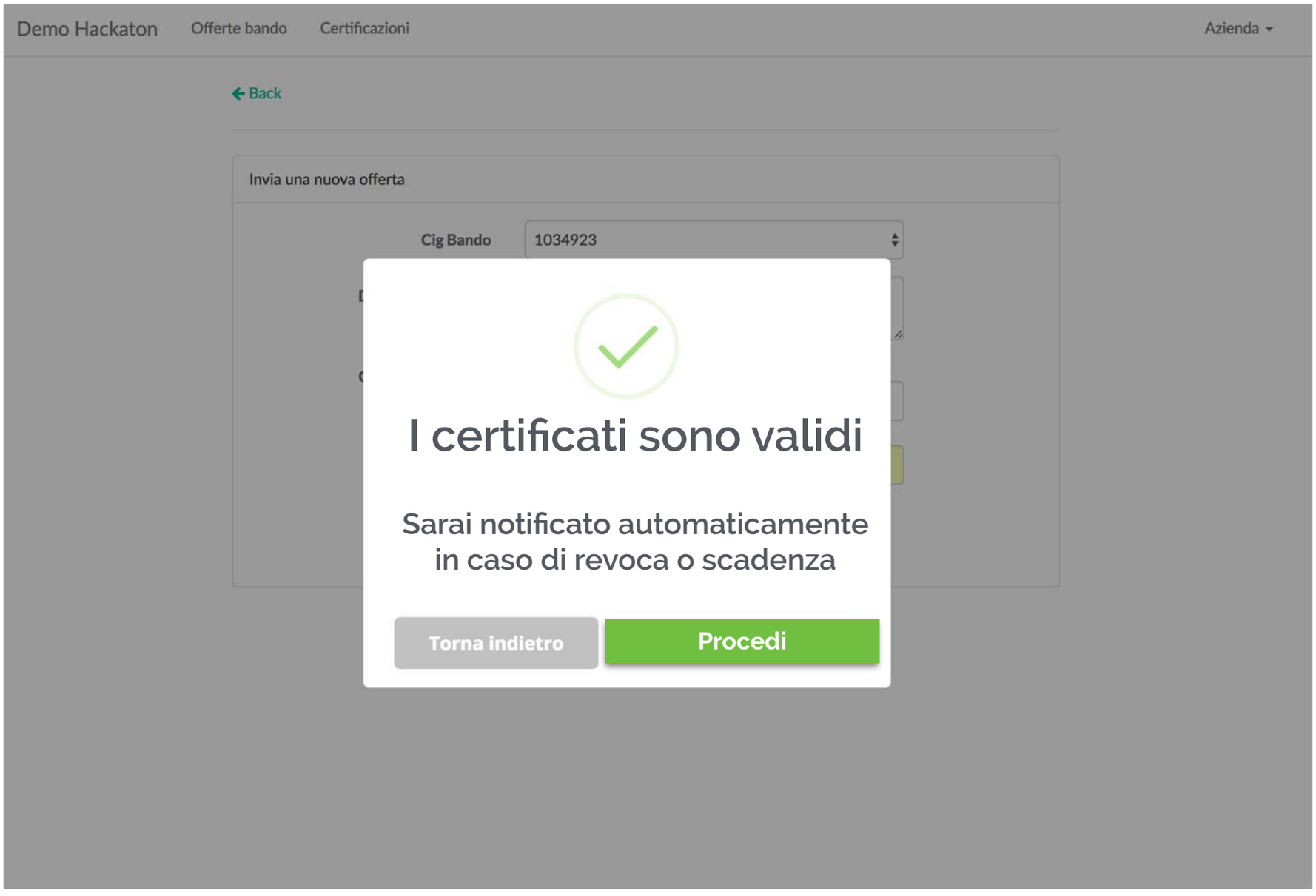


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

Patamu.com

Demo



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

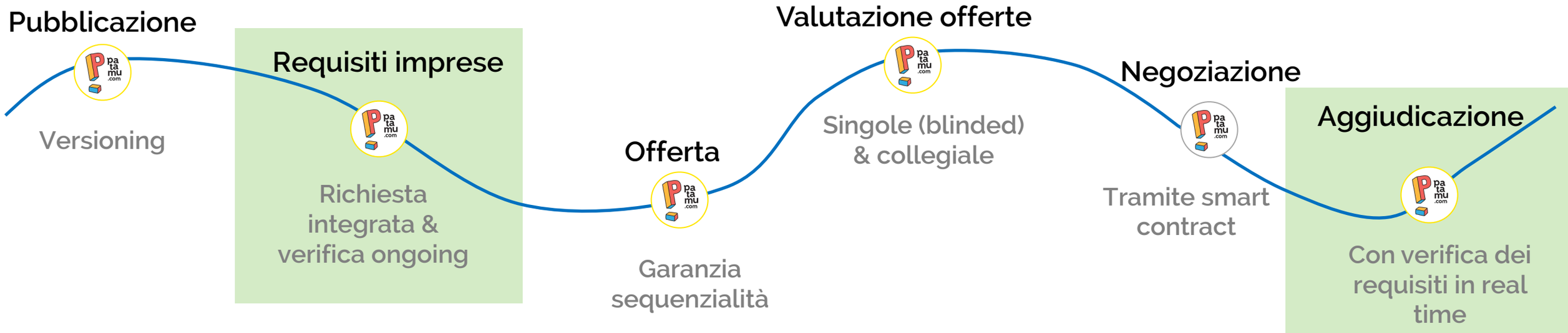
patamu.com

Overview del concept

L'idea: PA-tamu

- Piattaforma trustless con marca temporale, controllo continuo dell'autenticità, resistenza alla falsificazione, riduzione della discrezionalità nella valutazione
- Registro unico dei certificati emessi dalle singole autorità

Pubblicazione | **Gara** | **Stipula**



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

patamu.com

thank you!

Adriano Bonforti - Founder
adriano@patamu.com

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

patamu.com

#Firewall Team

Adriano Bonforti
Innovaetica / Patamu

Francesco Pepe
Innovaetica / Patamu

Luca Cricchio
Innovaetica / Patamu

Arianna Antonacci
LUISS Guido Carli

Davide Del Vecchio
Microsoft

Nunzio Casalino
LUISS Guido Carli

Andrea De Lullo
Sogei

Lorenzo Schirinzi
E&Y

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INNOVAETICA

Patamu .com

1 | Inserimento nella blockchain: hash dei dati originali

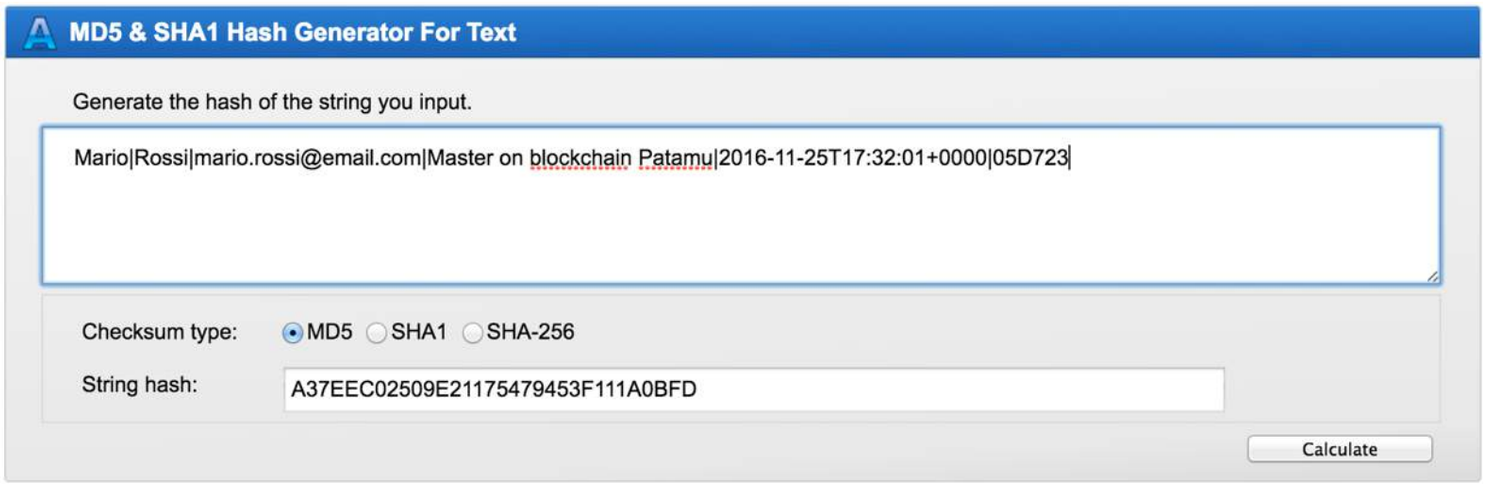
I dettagli del certificato vengono “hashati” con un algoritmo a “via unica” ovvero non reversibile.

Original content

patamu@patamu.com | Innovaetica SRL | Dati Certificato Antimafia | 2016-11-25T17:32:01+0000|05D723

Algoritmo di hashing MD5

(Per provare: http://onlinemd5.com)



a37eec02509e21175479453f111a0bfd

MD5 hash of original content (ascii)

L’hash è l’impronta non reversibile di un contenuto:
da un contenuto si ottiene sempre lo stesso hash, ma dall’hash non si può risalire al contenuto.

Questo sistema tutela la privacy del contenuto, ma dimostra la data certa dell’inserimento in blockchain.

INNOVAETICA

2 | Inserimento nella blockchain: blockchain transaction ID

L'hash a via unica del certificato viene inserito permanentemente all'interno della blockchain

Blockchain transaction ID:
a408aa782daea73e291bd6bc27d4db6a02c0377d50870bc612713058502d5f34

Il blockchain transaction ID diventa permanentemente accessibile sulla blockchain
e dimostra la data certa dell'inserimento dell'hash del certificato all'interno della blockchain.

INNOVAETICA

Verifica dell'inserimento dei dati nella blockchain

https://www.blocktrail.com/BTC

BITCOIN TRANSACTION

View on BTC.com

a408aa782daea73e291bd6bc27d4db6a02c0377d50870bc612713058502d5f34

← Blockchain transaction ID

TX Value	0.00856538 BTC	Total Inputs	0.00880538 BTC
Confirmations	2,390 CONFIRMATIONS	Total Outputs	0.00856538 BTC
Priority	2,784,462	Fee	0.00024000 BTC
Block	440555 Main Chain	Fee / KB	0.00058111 BTC
Relay time	Friday, November 25th 2016, 18:34:52 +01:00	Size	413 bytes
Time until confirmed	after 1 hour 43 minutes	Encoded Message	This transaction contains encoded data view

1 INPUTS — Total Inputs: 0.00880538 BTC

P2SH 3AYYsfPbtD3PZWfGSMSKRkUNXFLcSiddWK (0.00880538)

3 OUTPUTS

OP_RETURN view decoded message

P2SH 3QcJ6b6CViUydEd76ANhP4MyjYrjuCMzhh (0.00853807)

P2SH 35FtihUg5vNRpQiVgpr31HcapXN1kKkf9h (0.00002731)

INPUT SCRIPTS

OP_0
3045022100e60c36abc1d8b8391bfdaa8699623d0caa29cb306b25a2cee410a71ff92394
97022028cdb07ccc8831dae7bfa8455edc73adc5ea369ce46a00370f3a89164963417101
3044022073790928425b774a8f95a92bac017e3d7c7c12148983c5933792d02cce401e5
5022039fbb7797da4d4099691f1b242e71cae1e035810a8015f6d8503c456876505f901
OP_2 026dbc75d86969401f101ff5a321dfa19c0e428d642abb2e497967c4f540a61f3b
02826b6d1ae451e486ebe869e6f90436e069db523e857e0fe19bf05bf27501fa32
02b272f3e55e6c9d930b7dfcd5a2337237ed133c084099df2a9ec1e38e8f61f9b7 OP_3
OP_CHECKMULTISIG

OUTPUT SCRIPTS

OP_RETURN
6133376565633032353039653231313735343739343533663131316130626664

← Op_Return in esadecimale

+ 2 more

Op_Return in ASCII

(a37eec02509e21175479453f111a0bfd)

DECODED OP_RETURN AND COINBASE MESSAGES

The messages below are 'hex2bin' decoded messages from OP_RETURN outputs and coinbase inputs that are in this transaction.
A lot of these 'messages' contain no sane text since they can be used for things other than just plain text.

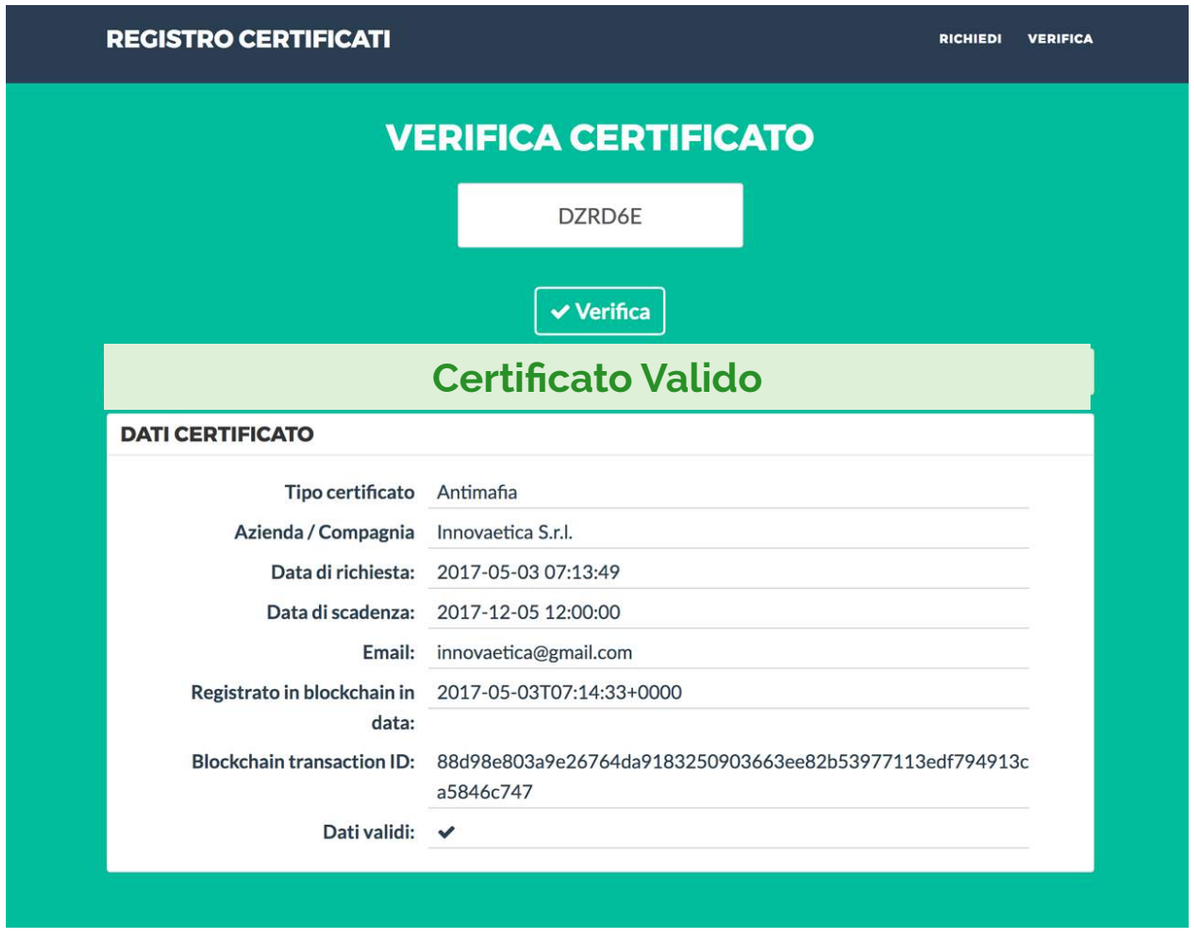
6a2061333765656330323530396532313137353437393435336631313161306266 64
a37eec02509e21175479453f111a0bfd

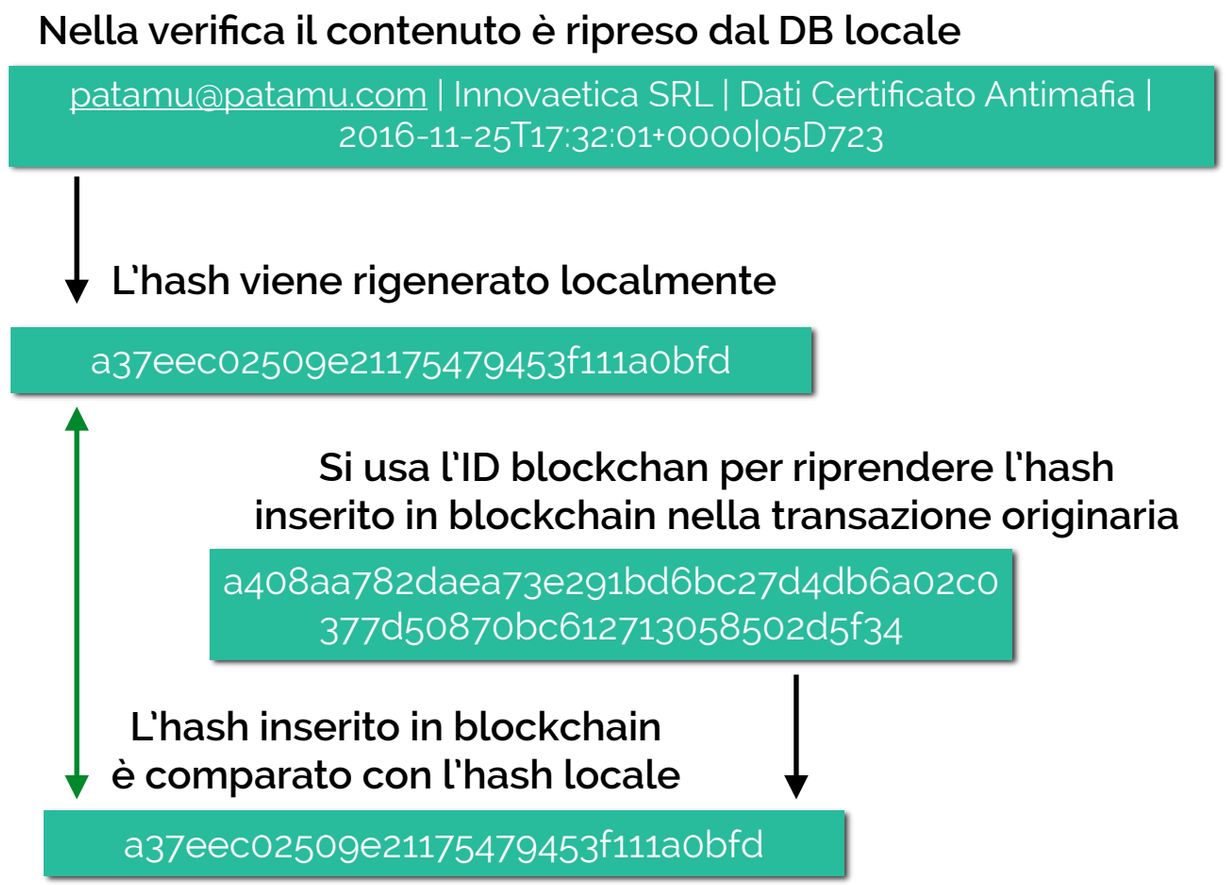
Op_return è il campo della blockchain in cui possono essere inseriti caratteri liberi per associare indissolubilmente un contenuto ad una determinata transazione.

Nell'Op_return abbiamo inserito i nostri dati hashati.

INNOVAETICA

Verifica della validità del certificato: approfondimento



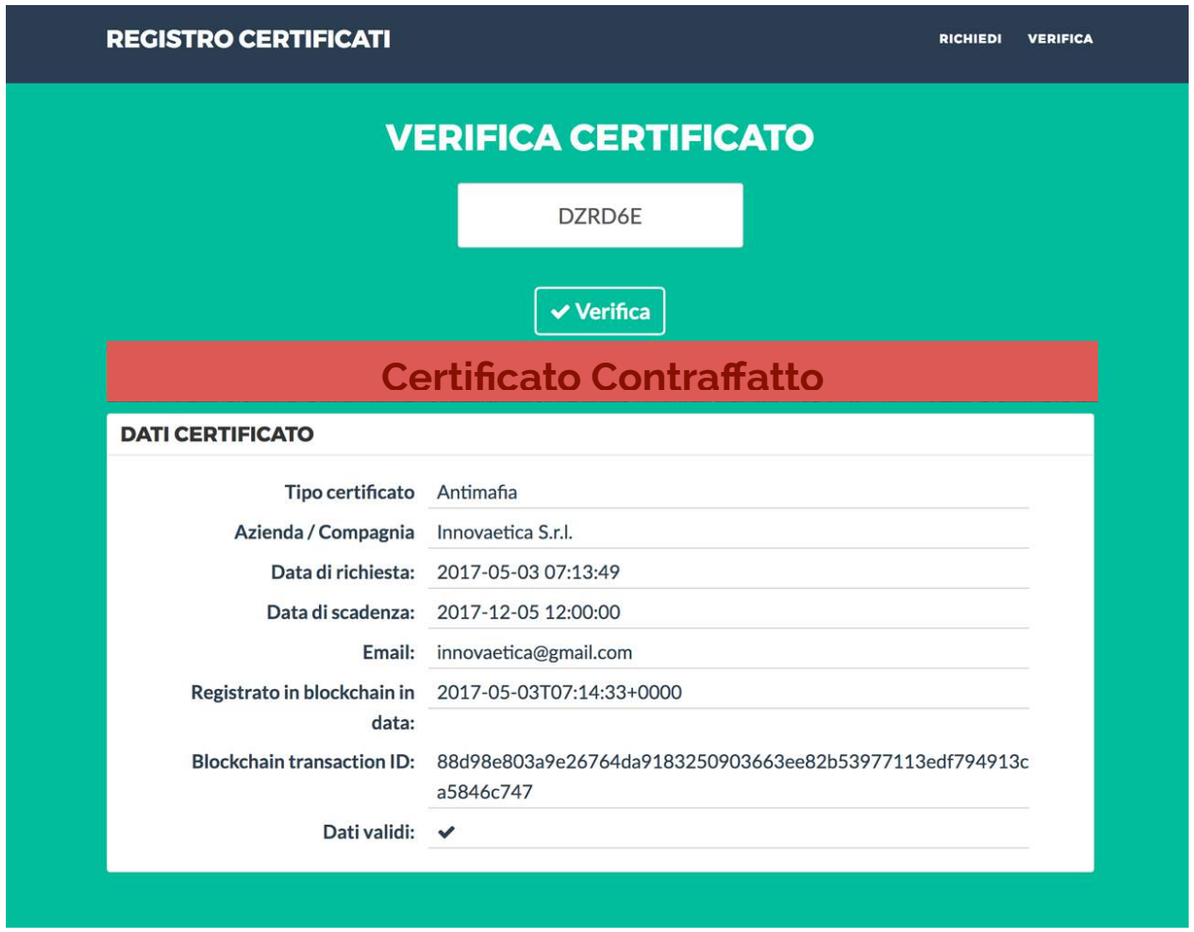


Inserendo il codice di validità **DZRD6E** il sistema prende i dati dal DB locale, effettua nuovamente l'hash localmente e lo compara con l'hash inserito nella transazione per verificare che i dati locali siano integri.

Se i dati corrispondono allora il certificato è sicuramente valido.

INNOVAETICA

Verifica della validità del certificato: anticontraffazione



Il contenuto (contraffatto) è ripreso dal DB locale

patamu@patamu.com | Innovaetica SRL | **dati Antimafia Alterati** | 2016-11-25T17:32:01+0000|05D723

L'hash generato localmente cambia

fdc30ae3781f4371e46e08417a72efe4

Si usa l'ID blockchan per riprendere l'hash inserito in blockchain nella transazione originaria

a408aa782daea73e291bd6bc27d4db6a02c0377d50870bc612713058502d5f34

L'hash inserito in blockchain non corrisponde con l'hash locale

a37eec02509e21175479453f111a0bfd

Se i dati del database locale venissero contraffatti per qualunque ragione, (nell'esempio cambiando i dati del certificato Antimafia), allora l'hash locale non corrisponderebbe più con l'hash inserito nella blockchain ed il certificato è risulterebbe contraffatto.

INNOVAETICA