30° Anno

EUSTEMA®

Making Innovation

De Cifris incontra Perugia – 16/10/2019

Blockchain e Secret Sharing

EUSTEMA
Making Innovation

Agenda

1. Overview Eustema e Progetto
2. Blockchain e Notarizzazione
3. Hyperledger e Smart Contract
4. Secret Sharing

EUSTEMA
Making Innovation

Stay ahead
WITH OUR TEAM

500+ PEOPLE
DELIVERY MANAGEMENT

Formazione continua, programmi di training, percorsi di sviluppo e career counseling. Trasferimento processi di innovazione su oltre 350 progetti complessi l'anno.

40+ R&D

Impegnati su tematiche d'avanguardia nell'ambito ICT. L'innovazione è il driver dell'Eustema R&D transformation

100 + Clienti

PAC e PAL
Utilities
Telco
Trasporti
Energy
Finanza
Poste
Interforze
Media

Il 70% dei nostri Clienti lavora con noi da oltre 10 anni.

3 sedi

Segmentazione offerta.
Forte rapporto con i target di riferimento attraverso la nostra presenza sul campo.
Costruiamo soluzioni basate su architetture tecnologiche innovative.

30 anni

di esperienza nell'ICT una storia di innovazione, di prodotti e progetti di successo.

Il decreto Investment Compact ci ha certificato Azienda Innovativa.

Eustema Traning Lab

640 certificazioni professionali

20.000 ore di formazione erogate

90% persone formate ogni anno

Eustema Academy
Oltre 6 corsi anno, 15 studenti aula, collaborazione con Atenei e Centri Ricerca

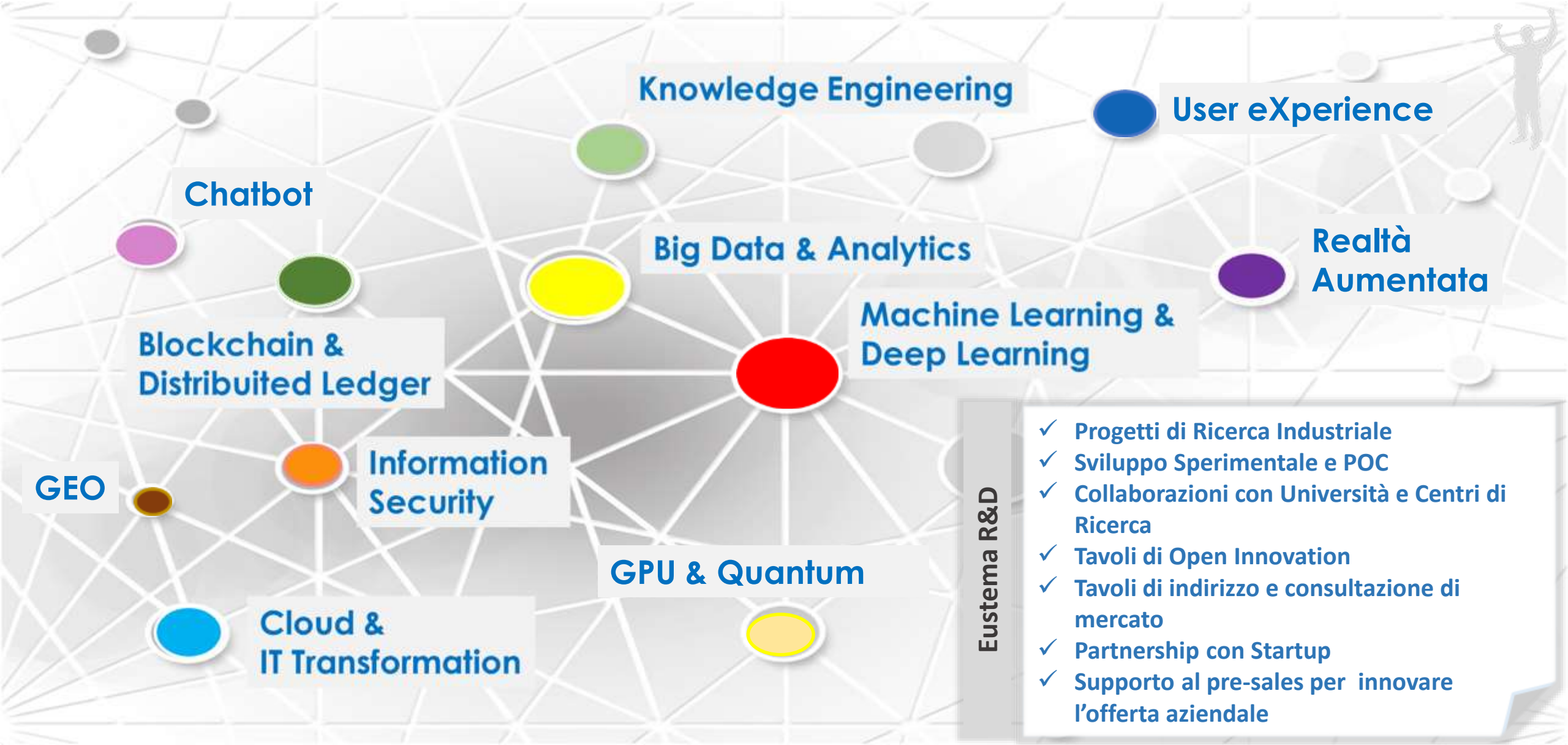
Key Offering

EUSTEMA TECHNOLOGICAL BUILDING BLOCKS

EUSTEMA
Making Innovation

Innoviamo per tradizione

WITH OUR R&D



Eustema R&D

- ✓ Progetti di Ricerca Industriale
- ✓ Sviluppo Sperimentale e POC
- ✓ Collaborazioni con Università e Centri di Ricerca
- ✓ Tavoli di Open Innovation
- ✓ Tavoli di indirizzo e consultazione di mercato
- ✓ Partnership con Startup
- ✓ Supporto al pre-sales per innovare l'offerta aziendale

Blockchain nelle Imprese

Possibili Declinazioni

NOTARIZZAZIONE: capacità di certificare le informazioni scambiate in una transazione tra due parti, ad es. implementa il processo di certificazione di documenti. Consente di garantire sulla proprietà, il contenuto e la validità temporale.

SMART CONTRACT: strumento di digitalizzazione di un contratto sotto forma di codice software. Consente di rendere automatiche azioni associate alle sue clausole, verifica degli SLA, nonché eventuali relative azioni di pagamento.

TOKENIZZAZIONE: processo di digitalizzazione di asset reali (ad es. per la creazione di registri di proprietà o strumenti di fidelizzazione o asset finanziari). Può essere utilizzato anche per la creazione di monete locali di comunità.

Progetto CheckLockBlock (CLB)

- **CheckLockBlock** è un progetto di ricerca presso il Centro R&D Eustema in collaborazione con Università di Trento.
- **Base del progetto**: blockchain per la notarizzazione di documenti.
- **Obiettivo del progetto**: “time capsule”

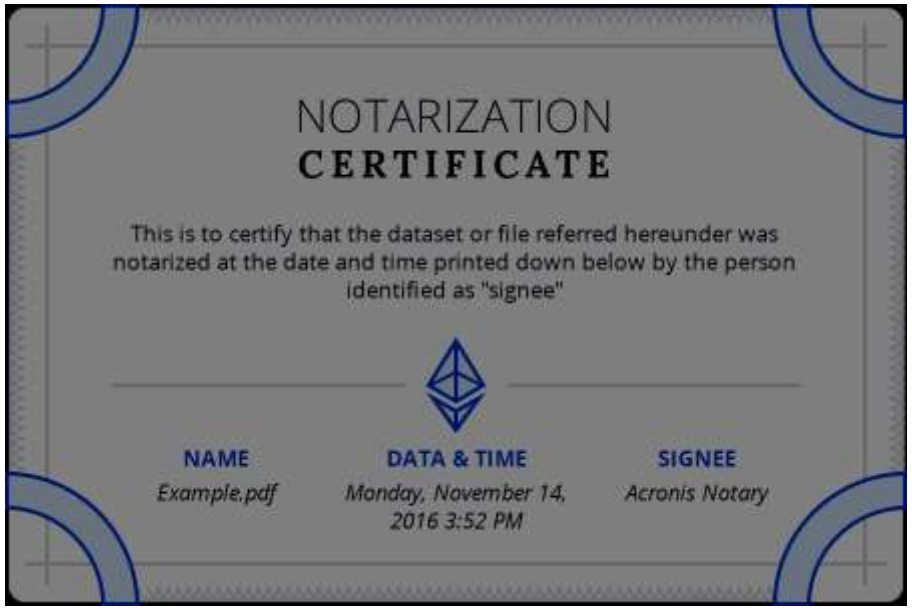
Caso d’uso: concorsi pubblici, e-procurement, ecc.

Necessità di un’applicazione che certifichi il caricamento e l'integrità di un documento ad un certo istante temporale.

“time capsule”: assoluto riserbo sul contenuto del documento prima della data di scadenza/apertura

Notarizzazione

La notarizzazione è il processo ufficiale contro manomissioni/frodi che assicura, alle parti coinvolte in una transazione, che un documento è autentico e fidato.
Lo sviluppo della blockchain probabilmente faciliterà, ed eventualmente sostituirà, l'informatizzazione del processo di notarizzazione.



La promessa di resistenza alla manomissione, non ripudio e di tracciabilità delle informazioni rende la blockchain un ottimo candidato.

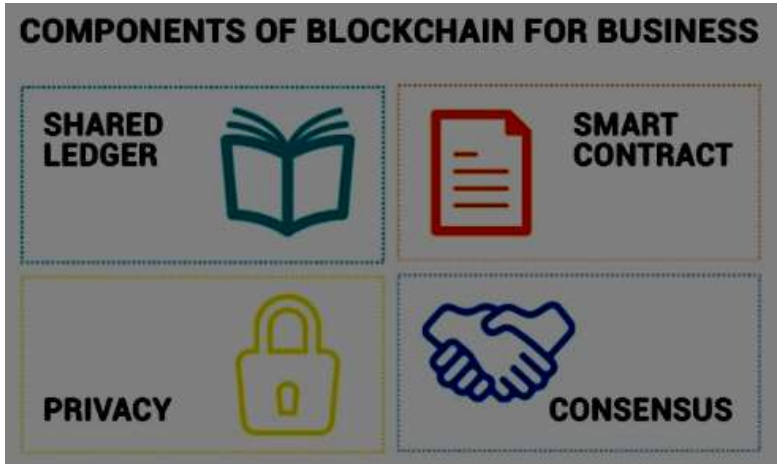
Il servizio usato nel progetto è la proof-of-existence.

Piattaforma Hyperledger

Hyperledger è un gruppo di progetti open source focalizzati sullo sviluppo di DLTs designati specificatamente per le imprese. Hyperledger non è basata su una cripto moneta, è permissioned e supporta vari algoritmi di consenso.

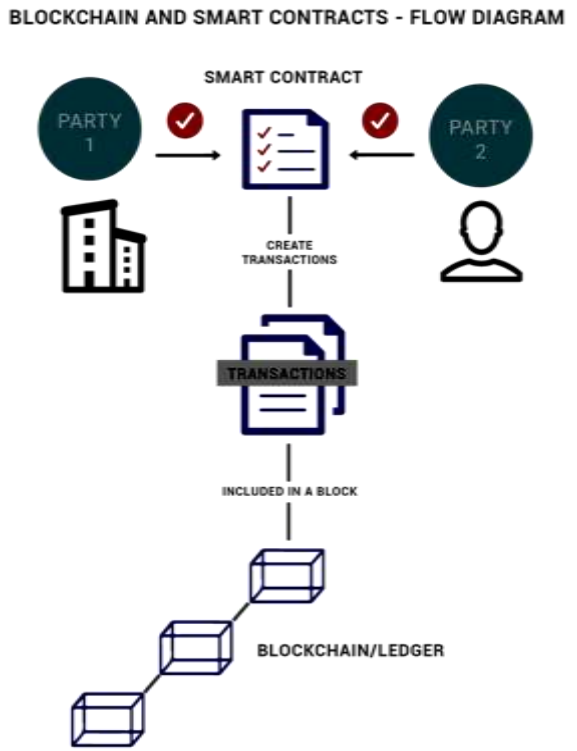
Hyperledger Fabric è un framework di programmazione per blockchain permissioned che supporta gli smart contracts.

HYPERLEDGER FABRIC



Smart Contract

- Programmi che eseguono azioni predefinite quando certe condizioni del sistema vengono soddisfatte.
- Forniscono un linguaggio di transazione che permette di modificare lo stato del registro distribuito.



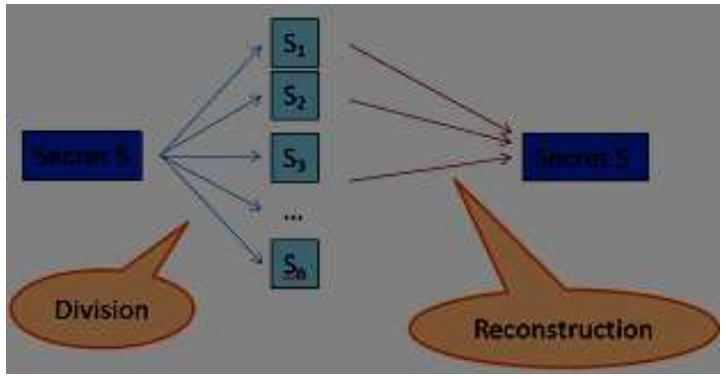
Caratteristiche del chaincode di Hyperledger Fabric

- Go, Node.js, Java come linguaggi di programmazione.
- Permette all'utente di creare transazioni nel registro distribuito della rete e di aggiornare il world state dei beni.

Secret Sharing: Schema a soglia (n,t)

Siano ***n*** e ***t*** due interi positivi tali che ***t ≤ n***. Uno schema a soglia ***(n,t)*** è un metodo di condivisione di una chiave ***k*** tra un insieme di ***n*** partecipanti tale che:

- Ogni gruppo di cardinalità maggiore o uguale a ***t*** riesce a ricostruire la chiave ***k***
- Ogni gruppo di cardinalità inferiore a ***t*** non riesce ad ottenere alcuna informazione riguardante il segreto ***k***



Secret Sharing: Schema a soglia di Shamir

Schema basato sulla costruzione di un polinomio ***a(x)*** di grado ***t-1*** tale che ***a(0)=segreto***.

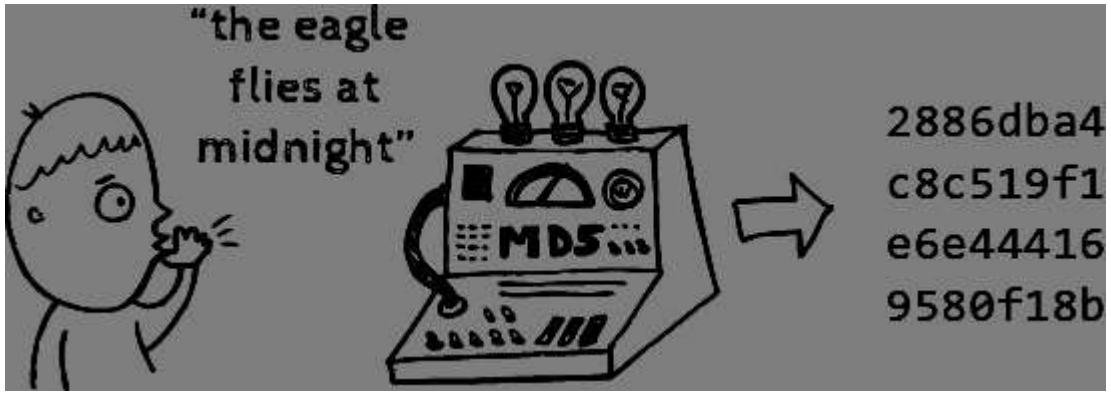
Le shares sono delle coppie (x_i, y_i) dove x_i è un punto scelto random e $y_i=a(x_i)$.

La ricostruzione del segreto si basa sulla risoluzione di un sistema a ***t*** incognite.

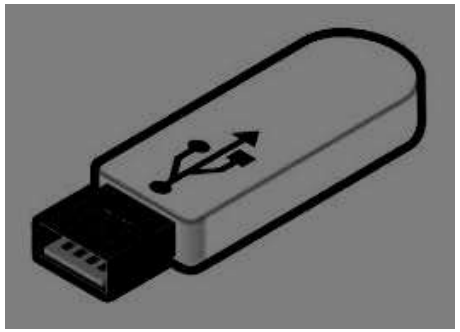
E' uno schema sicuro in quanto basato su una proprietà matematica ben dimostrata. Dati $k < t$ punti esistono infiniti polinomi di grado ***t*** che interpolano questi punti.

Panoramica del progetto: Caricamento documento privato

1. Viene fatta l'hash del documento in chiaro e caricata sulla blockchain.



2. Viene cifrato il documento.



3. L'hash del documento cifrato viene caricata sulla blockchain.

4. Il documento cifrato viene salvato su un supporto esterno.

Panoramica del progetto: Caricamento lista e distribuzione shares

1. Viene pubblicata una lista contenente i nomi dei partecipanti allo schema a soglia di Shamir.
2. L'hash della lista viene caricata sulla blockchain.

3. Ogni share viene cifrata con la chiave pubblica dell'utente al quale verrà inviata attraverso una transazione sulla blockchain.

Panoramica del progetto: Ricostruzione segreto e decifratura

Ogni utente può accedere alla sua share e decifrarla con la propria chiave privata.

Quando un numero sufficiente di utenti si mettono d'accordo con le loro shares possono ricostruire il segreto.

Appena gli utenti possessori del segreto vengono a contatto con il documento privato, possono decifrarlo e certificare che il file non è stato modificato grazie all'hash caricata sulla blockchain.

Eustema R&D

NETWORKING

Fare rete
per pensare
a nuovi prodotti,
servizi
e soluzioni 4.0

Imprese
per realizzare
progetti
di co-innovazione

Partenariati
per progetti R&D
cofinanziati su bandi
Nazionali
ed Europei

End-user per
sperimentazione
e validazione
di progetti
innovativi

Partner tecnologici
e Start up

Proof of Concept

EUSTEMA
Making Innovation

Professional asset

CERTIFICATIONS

- ISO 9001:2015: Quality management systems
- ISO/IEC 20000-1:2011: Information Technology - Service management
- SA 8000:2014: Social Responsability
- ISO/IEC 27001:2013: Information Security

★ ★ ★

Rating legalità
Autorità Garante della concorrenza e del Mercato

EUSTEMA
Making Innovation

EUSTEMA®

Making Innovation

Donato Cappetta

Responsabile Ricerca e Sviluppo

Email: d.cappetta@eustema.it

Cel. +39 3351409840

Linkedin: www.linkedin.com/in/dcappetta/

ROMA
Via Carlo Mirabello, 7
00195 – Roma
Tel.: +39 06372721
+39 06374931
Fax:+39 0637351735

NAPOLI
Centro Direzionale Via G.
Porzio, 4 - Isola C/2
80143 - Napoli
Tel.: +39 0816586610
Fax: +39 0816586611

MILANO
Via Roberto Lepetit, 8/10
20124 - Milano
Tel.: +39 0200696431

www.eustema.it