

CITTA' DI
VENEZIA



Comune di Venezia

Scheda descrittiva del programma whistleblowing

Indice

1	PREMESSA.....	3
1.1	OGGETTO OFFERTO IN RIUSO:.....	3
1.2	TIPOLOGIA DI OGGETTO OFFERTO IN RIUSO:.....	3
1.3	REFERENTI.....	3
1.4	AMBITO AMMINISTRATIVO INTERESSATO.....	3
1.5	CONTESTO ORGANIZZATIVO.....	4
1.6	PUNTI DI FORZA.....	4
1.7	VINCOLI E/O CRITICITÀ.....	4
1.8	MODALITÀ DI RIUSO CONSIGLIATE.....	4
1.9	MANUALISTICA DISPONIBILE.....	4
2	REQUISITI 4	
2.1	REQUISITI SOFTWARE.....	4
2.2	REQUISITI HARDWARE.....	4
3	CONTESTO TECNOLOGICO.....	4
3.1	ARCHITETTURA LOGICO FUNZIONALE DELL'OGGETTO.....	4
3.2	ARCHITETTURA HARDWARE DELL'OGGETTO.....	4
3.3	ARCHITETTURA TLC DELL'OGGETTO.....	4
3.4	LINGUAGGI DI PROGRAMMAZIONE.....	4
3.5	STANDARD UTILIZZATI.....	4

1 PREMESSA

1.1 Oggetto offerto in riuso: whistleblowing

Applicazione del Comune di Venezia per l'invio di segnalazioni al responsabile anticorruzione. Tale soluzione è basata sulle indicazioni fornite dell'autorità anticorruzione.

http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6123

1.2 Tipologia di Oggetto offerto in riuso:

- Applicazione web per segnalazioni anti corruzione

1.3 Referenti

- Referente Settore Sistemi Informativi: Piergiorgio Volpago
- Referente Venis: Marco Gazzuolo

1.4 Ambito amministrativo interessato

- Anticorruzione

1.5 Contesto organizzativo

Strumento per la ricezione di delazioni realizzato dal Comune di Venezia in relazione alla normativa anticorruzione.

Dopo aver acceduto all'area di sua pertinenza con username e password (/loginadmin), il responsabile anti corruzione è in grado di visualizzare la lista delle segnalazioni. Dopo aver cliccato sul bottone "visualizza" di un item della lista, sarà possibile visualizzare il contenuto della segnalazione solamente dopo aver inserito la chiave privata personale e la relativa passphrase. La decriptazione viene effettuata lato client (sul browser), rendono inefficaci attacchi di tipo "man in the middle", in quanto i dati vengono trasmessi ancora encriptati.

Il responsabile anti corruzione è in grado di inserire per ogni segnalazione, specificando lo stato di avanzamento, tutte le note che ritiene opportune. Tali note saranno visualizzabili anche dal delatore, e per questo criptate solamente in modo simmetrico lato server.

I dati anagrafici del delatore possono essere visualizzati dal responsabile unico dei sistemi informativi solo su richiesta della magistratura, ma soprattutto solo dopo aver ricevuto l'identificativo della segnalazione da parte del responsabile anti corruzione.

Il responsabile unico dei sistemi informativi, dopo aver acceduto all'area di sua pertinenza con username e password (/loginkeeper), ed aver inserito l'identificativo della segnalazione, sarà in grado di visualizzare i dati del delatore solamente dopo aver inserito la chiave privata personale e la relativa passphrase.

Anche in questo caso la decriptazione viene effettuata lato client (sul browser), rendono inefficaci attacchi di tipo "man in the middle", in quanto i dati vengono trasmessi ancora criptati.

Il delatore dopo aver inviato la segnalazione, riceverà una username ed una password(quest'ultima per email), ed accedendo tramite queste all'area a lui dedicata (/login), sarà in grado di visualizzare lo stato di avanzamento e le relative note della sua segnalazione.

La cifratura lato server è eseguita con algoritmo AES-256-CBC con vettore unico ad inizializzazione random per ogni operazione.

La cifratura lato client è implementata attraverso il protocollo OpenPGP.

1.6 Punti di forza

L'applicazione garantisce sicurezza ed anonimato delle informazioni segnalate, il tutto grazie ad un sistema a doppia crittografia:

- crittazione asimmetrica lato client (sul browser)
- crittazione simmetrica lato server.

Realizzato interamente con software opensource e free.

I dati inerenti al fatto, il messaggio ed i files vengono criptati (lato client) con la chiave pubblica del responsabile anti corruzione.

I dati anagrafici del delatore vengono criptati (lato client) con la chiave pubblica del responsabile unico dei sistemi informativi.

I dati vengono dunque inviati al server già criptati, rendendo inefficaci attacchi di tipo "man in the middle".

Una volta inviati al server, i dati sono ulteriormente criptati con chiave simmetrica e salvati all'interno del database.

1.7 Vincoli e/o criticità

Nessuno

1.8 Modalità di riuso consigliate

Deploy su server / container

SaaS (Software as a Service)

1.9 Manualistica disponibile

File readme.md all'interno dei sorgenti del progetto

2 REQUISITI

2.1 Requisiti software

Framework: NodeJS

Database: MongoDB

Browser: ultime versioni di Chrome, Firefox ed Explorer

Compatibile con OS Windows, Linux, MacOS

Accesso da Altana per compilare la segnalazione (solamente per dipendenti Comune di Venezia)

2.2 Requisiti hardware

Nessuno

3 CONTESTO TECNOLOGICO

3.1 Architettura logico funzionale dell'Oggetto

Flusso delle operazioni in invio dei dati

client encryption -> server encryption -> database saving

Flusso delle operazioni in lettura dei dati

database loading -> server decryption -> client decryption

3.2 Architettura hardware dell'Oggetto

Os Linux (consigliata)

3.3 Architettura TLC dell'Oggetto

Rete internet

3.4 Linguaggi di programmazione

Javascript, Css, Html

3.5 Standard utilizzati

OpenPGP

AES-256-CBC

Material design

HTML5

ECMAScript