visabit
IN VIDEO, ERGO SUM

Relazione tecnica sulla sicurezza

Versione 1.0

visabit
IN VIDEO, ERGO SUM

Sommario

visabit
IN VIDEO, ERGO SUM

Relazione Tecnica

La sicurezza della piattaforma L'altro Testamento si articola su tre direttrici, rispettivamente sicurezza di infrastruttura, veridicità ed immutabilità dei contenuti e privacy.

Sicurezza di infrastruttura

Partendo dalla sicurezza sull'infrastruttura possiamo dire che è stata realizzata *by design* ossia che uno dei pilastri della progettazione è appunto la sicurezza.

Infatti, la piattaforma L'altro Testamento è una infrastruttura cloud based che sfrutta i meccanismi di sicurezza interni della piattaforma cloud scelta, nel nostro caso Amazon Web Services (AWS) ed espone unicamente quegli elementi che devono interfacciarsi con gli utenti pubblici, costituiti sia dai clienti che usufruiscono del servizio sia degli operatori del servizio.

Tutta la comunicazione tra cliente e piattaforma avviene mediante protocolli Https e Secure Web Socket, questo vuol dire che tutta la comunicazione è criptata in modalità uno-a-uno. Modalità che rende inaccessibile a terze parti non coinvolte nella comunicazione.

La gestione degli accessi mediante un doppio livello di verifica che prevede rispettivamente autenticazione ed autorizzazione.
L'autenticazione fa si che ogni accesso venga verificato e tracciato, mentre il livello di autorizzazione fornisce la possibilità o meno di eseguire determinate azioni.
A titolo di esempio un utente che accede correttamente alla piattaforma utilizzerà username e password per l'autenticazione ed riceverà un livello di autorizzazione di tipo *utente* che gli permette di accedere allo storico delle sue registrazioni e al calendario delle nuove registrazioni; lato ufficio invece l'utente che accede al portale di backoffice avrà a disposizione la possibilità di lavorare su differenti attività a seconda che il suo profilo sia di tipo operatore, backoffice o amministratore.

Nota importante: a nessun livello di autorizzazione è concessa la possibilità di cancellare contenuti.

Veridicità ed immutabilità dei contenuti

In questo capitolo vengono descritte le misure messe in atto al fine di rendere i contenuti video registrati immutabili ed unici a livello temporale.
Il processo di video registrazione prevede che all'inizio della video registrazione l'utente che ha sottoscritto il servizio mostri un documento di identità, che la registrazione sia svolta per il tempo richiesto e che il suo contenuto sia caricato sul servizio S3 di AWS al termine della stessa. Già in questa fase la video registrazione è accessibile al solo cliente ed alla piattaforma in quanto svolta in modalità privata e su servizi non esposti al pubblico.

Terminata la fase di registrazione e caricamento su S3 l'operatore chiederà all'utente se vuole che la video registrazione venga autenticata e marcata temporalmente. Su assenso dell'utente l'operatore provvederà ad apporre rispettivamente la marca temporale che sancisce quando il documento è stato video registrato e la firma qualificata (FEA) che renderà il contenuto video non più modificabile. Il contenuto video marcato e firmato sarà caricato sul servizio di storage S3 e mantenuto per tutto il tempo previsto dal contratto.

Il servizio di marca temporale e firma elettronica qualificata (FEA) è affidato ad una certification autority esterna a Visabit che nel nostro è Intesi Group S.p.a.

Entrando più nello specifico possiamo dire che la marca temporale serve a sancire in modo univoco e certificato quando la video registrazione è stata fatta mentre la firma elettronica che è basata sul checksum del file di video registrazione serve a stabilirne l'univocità del contenuto.
L'univocità del contenuto è garantita dal fatto che ad ogni file corrisponde un checksum univoco, una sorta di impronta digitale basata sul suo contenuto. La manomissione anche di un solo byte del file porterebbe ad avere un checksum diverso da quello originale invalidando di fatto la firma che è stata apposta. Infatti al momento della verifica della firma vengono confrontati checksum e firma digitale apposta che darà esisto positivo se il file non è stato modificato mentre darà esito negativo se il file ha subito una qualsiasi modifica.

Privacy

Sempre in fase di design della soluzione si è pensato a come tutelare la privacy degli utenti che sottoscrivono il servizio de L'altro Testamento. Questo perché le registrazioni contengono per natura stessa del servizio informazioni sensibili.
A tal fine Visabit ha implementato un processo tale per cui i file delle registrazioni sono a disposizione del solo utente che ha eseguito la video registrazione e in caso di morte a disposizione di chi è stato indicato come "erede" del video testamento dallo stesso utente.
Durante il periodo di validità della sottoscrizione è l'utente stesso (proprietario) a poter concedere su sua precisa indicazione l'accesso ad una persona terza, accesso che viene concesso per periodo limitato di tempo.
Da parte di Visabit ad una esplicita richiesta dell'utente viene generato un link pre-autenticato per l'accesso al file, al termine del periodo di validità del link il file della video registrazione tornerà ad essere inaccessibile.
In sintesi, possiamo dire che tutte le video registrazioni sono di base inaccessibili (private), l'accesso è temporaneo e viene concesso per esplicita richiesta dell'utente. L'accesso, che avviene mediante link pre-autenticato, è concesso per un singolo file. Al termine del periodo di validità il file ritorna ad essere inaccessibile.
Infine, sia da parte di Visabit sia da parte dell'utente non è possibile cancellare una video registrazione a partire dagli strumenti online.
L'utente ha facoltà di richiedere la rimozione del contenuto dalla piattaforma L'altro Testamento, per far ciò dovrà farne esplicita richiesta a Visabit che a sua volta girerà la richiesta ad un tecnico specializzato con i permessi necessari ad eseguire l'operazione.