Secure Messaging Board - v1.0.0

Introduzione e modello dati

Secure Messaging Board (SMB) è un'applicazione per la *notarizzazione* di contenuti digitali – tipicamente, ma non esclusivamente: messaggi, oggetti software, media - che vengono pubblicati da un autore e indirizzati a una lista di distribuzione o a un destinatario specifico. SMB implementa, utilizzando la tecnologia Blockchain, un processo di sicurezza che permette di memorizzare un contenuto in un'area condivisa (per es. cloud storage), pubblicando simultaneamente su Blockchain un record che ne annuncia l'esistenza, fornisce un puntatore per accedervi online e imposta un "sigillo digitale" a garanzia della sua provenienza e integrità. La struttura del record è la seguente:

DOMAIN	chiave	opz.	stringa	Canale di distribuzione: dominio
ENVIRONMENT	chiave	opz.	stringa	Canale di distribuzione: sotto-dominio
PROCESS	chiave	opz.	stringa	Canale di distribuzione: processo
NAME	chiave		stringa	Nome dell'oggetto
VERSION	chiave		intero	Versione dell'oggetto
CREATED			data/ora	Timestamp di pubblicazione
CREATED_BY			stringa	Identità dell'utente che pubblica
SIGNED_BY		opz.	URL	Identità del firmatario (se il contenuto è firmato digitalmente)
SEAL			stringa	Hash del contenuto
CONFIDENTIAL_FOR		opz.	URL	Identità del destinatario (se il contenuto è criptato con una chiave pubblica)
MESSAGE_REF			URL	Puntatore all'oggetto
MESSAGE_SIZE			decimale	Dimensione dell'oggetto (in MB)

Come si può vedere, il record presenta una chiave composita, i cui primi elementi (DOMAIN, ENVIRONMENT e PROCESS) individuano un canale di distribuzione - che può essere omesso - mentre gli ultimi (NAME e VERSION) rappresentano il nome logico dell'oggetto pubblicato e, qualora sia previsto, il suo numero progressivo di versione.

MESSAGE_REF è un URL che individua l'oggetto pubblicato nell'area comune di memorizzazione, e permette di scaricarne una copia; MESSAGE_SIZE ne indica la dimensione. Notare che l'area di memorizzazione non è parte di SMB, e deve quindi essere gestita dagli utenti (incluso il controllo degli accessi, quando previsto).

Il campo SEAL contiene un valore *hash* calcolato sul contenuto dell'oggetto pubblicato: permette a chiunque abbia ricevuto l'oggetto di verificarne, applicando il medesimo algoritmo già utilizzato in fase di pubblicazione, la corrispondenza col contenuto originale.

SIGNED_BY e CONFIDENTIAL_FOR dichiarano rispettivamente l'utente che ha firmato digitalmente l'oggetto e il suo destinatario confidenziale, se presenti. In entrambi i casi, l'URL individua un record, appartenente a una qualunque *public key infrastructure*, che sancisce l'identità (e la relativa chiave pubblica) del soggetto in questione. Trattandosi di funzionalità avanzate, non sono descritte in questo documento.

Accesso e profilatura

Perché un utente possa usufruire di SMB, la sua identità deve essere registrata nel sistema dal gestore della piattaforma, che provvede quindi a rilasciare delle credenziali personali da utilizzare per l'accesso. Le credenziali consistono in un certificato digitale che contiene l'identità dell'utente e il suo profilo. Nella sezione riguardante l'installazione del client, sarà spiegato come configurare il software con le credenziali ottenute dal gestore. In questa sezione, diamo una spiegazione sommaria del meccanismo di profilatura.

Il profilo è determinato da due elementi: ruolo e ambito. Il ruolo può assumere il valore "reader" o "writer". Un utente con ruolo "reader" può solo eseguire accessi in lettura, mentre il ruolo "writer" abilita anche l'accesso in scrittura - cioè consente la pubblicazione di oggetti su SMB. L'ambito definisce invece dei limiti individuali di operatività basati sul valore dei campi DOMAIN, ENVIRONMENT, PROCESS e NAME. Per fare un esempio semplice, un profilo definito come "DOMAIN='dominioABC', ENVIRONMENT='ambienteZXY'" limita l'utente interessato a leggere / scrivere record SMB con tali caratteristiche. I singoli campi del profilo possono anche contenere una lista di valori, oppure essere vuoti: nel secondo caso, non sono imposti limiti operativi.

Operazioni

Il cuore dell'applicazione SMB è uno *smart contract* Blockchain. Per comodità degli utenti, questa versione dell'applicazione è distribuita assieme a un *client* che offre una semplice interfaccia interattiva a linea di comando e rende trasparente l'interazione con la piattaforma Blockchain, in particolare per quanto riguarda i protocolli di comunicazione e la sicurezza. Allo stesso tempo, il client integra le funzionalità di base per l'accesso, in lettura e scrittura, a un'area comune di memorizzazione basata sul servizio Google Drive.

La combinazione di smart contract e client offre agli utenti tre funzionalità:

- POST (solo utenti con ruolo "writer"): pubblica un nuovo oggetto, o una nuova versione di un oggetto già pubblicato. Deve essere obbligatoriamente specificato il nome logico dell'oggetto (NAME), e opzionalmente il canale (DOMAIN, ENVIRONMENT e PROCESS). Inoltre, deve essere indicato il percorso sul disco locale di un file che rappresenta il contenuto associare all'oggetto. L'operazione, se va a buon fine, effettua l'upload del contenuto nell'area comune di memorizzazione. Se non esiste già un record con la stessa combinazione di DOMAIN, ENVIRONMENT, PROCESS e NAME, al campo VERSION viene assegnato il valore 0 (zero); diversamente, riceve il valore di VERSION del record precedente incrementato di 1. Tutti i campi non inclusi nella chiave vengono valorizzati automaticamente.

- GET: recupera il contenuto di un oggetto, specificato attraverso la chiave. Se viene specificato un numero di versione, il contenuto restituito corrisponde alla versione indicata; diversamente, è quello dell'ultima versione pubblicata. L'operazione segnala un errore se non è possibile accedere all'oggetto indicato, ovvero se il contenuto dell'oggetto è stato alterato dopo la pubblicazione (check rispetto al campo SEAL).
- VERSION: recupera il numero dell'ultima versione pubblicata di un oggetto, specificato attraverso la chiave parziale (DOMAIN, ENVIRONMENT, PROCESS e NAME).

Installazione del client

Requisiti di sistema

- Java JRE 1.8 o superiore
- Connessione a Internet priva di proxy
- Account Google Drive

Integrazione con Google Drive

In questa versione dell'applicazione, l'unico servizio supportato come area comune di memorizzazione è Google Drive. Durante il primo utilizzo, eseguendo una operazione di tipo POST, l'utente viene invitato ad accedere ad una pagina Web specifica per gestire il consenso all'utilizzo dei dati, necessario per usufruire del servizio. Una volta fornito il consenso, non sarà più richiesto in seguito.

Installazione

Il client viene distribuito, su richiesta individuale, dal gestore della piattaforma. È costituito da due file: un JAR (eseguibile) contenente il software e uno ZIP (wallet) che incapsula l'intera configurazione, inclusi gli indirizzi di rete e le credenziali di accesso.

L'eseguibile è uguale - a parità di versione del software - per tutti gli utenti. Trattandosi di un programma Java, può essere copiato dall'utente in qualunque cartella del proprio disco, da cui verrà quindi lanciato con il comando "java" (v. Uso del client).

Il wallet è invece strettamente personale. Il file ZIP deve essere decompresso dall'utente sul proprio disco – anche in questo caso, in una cartella a piacere – e il suo percorso passato come argomento del comando "java" (v. Uso del client). Se un utente riceve dal gestore più identità distinte (tipicamente, per accedere con profilature diverse), installerà un unico eseguibile e più wallet, decompressi ciascuno in una propria cartella; potrà quindi in fase di esecuzione specificare quale profilo utilizzare per eseguire l'operazione.

Uso del client

Il client non è interattivo: per eseguire una singola operazione, deve essere lanciato dalla shell di sistema con un comando specifico. Il comando è così strutturato (si assume che il Java JRE sia stato configurato correttamente):

java -jar <percorso del file eseguibile>

-w <percorso assoluto della cartella wallet> (obbligatorio)

-o <operazione: POST, GET o VERSION> (obbligatorio)

-f <POST: percorso assoluto del file che rappresenta l'oggetto da pubblicare; GET percorso assoluto del file in cui copiare il contenuto dell'oggetto da recuperare>

-d <argomento DOMAIN> (opzionale)

-e <argomento ENVIRONMENT> (opzionale)

-p <argomento PROCESS> (opzionale)

-n <argomento NAME> (obbligatorio)

-v <GET: argomento VERSION> (opzionale)

A ogni esecuzione, il relativo log (attività e eventuali errori) viene aggiunto in coda al file smb-ledger.log, posizionato nella sotto-cartella logs.

Esempi su PC Windows (argomenti obbligatori in grassetto)

java -jar smb-ledger-1.0.0.jar -w C:\Users\mywindowsuser\smb\smbuser1
-o POST
-d mydomain -e myenv -p myprocess
-n myobject
-f C:\Users\mywindowsuser\Documents\mycontent-myversion.bin

java -jar smb-ledger-1.0.0.jar -w C:\Users\mywindowsuser\smb\smbuser1
-o GET
-d mydomain -e myenv -p myprocess
-v targetversion
-n myobject
-f C:\Users\mywindowsuser\MyFolder\mycontent.bin

java -jar smb-ledger-1.0.0.jar -w C:\Users\mywindowsuser\smb\smbuser1
-o VERSION
-d mydomain -e myenv -p myprocess
-n myobject