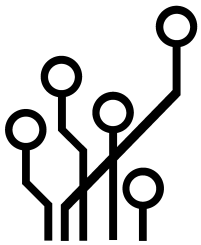

PROJECT ORIGIN

projectorigin2023@gmail.com

Glossario

Versione	2.0.0
Responsabile	Ibra Elton
Redattori	Corbu Teodor Mihail
Verificatori	Ibra Elton
Uso	Esterno
Destinatari	*Project Origin* Prof. Vardanega Tullio Prof. Cardin Riccardo

Descrizione

Glossario contenente i termini per i quali è necessaria una definizione univoca del gruppo *Project Origin* nella realizzazione del progetto *Personal Identity Wallet*

Registro delle modifiche

Vers.	Data	Autore	Ruolo	Descrizione
2.0.0	2023-09-24	Ibra Elton	Responsabile	Approvazione documento
1.1.1	2023-09-23	Alessio Andreetto	Amministratore	Aggiunti termini al glossario
1.1.0	2023-09-18	Ibra Elton	Verificatore	Verifica$_g$documento
1.0.1	2023-08-16	Corbu Teodor	Analista	Aggiunti termini al glossario
1.0.0	2023-08-01	Ibra Elton	Responsabile	Approvazione documento
0.3.1	2023-07-22	Ibra Elton	Analista	Aggiunti termini al glossario
0.3.0	2023-05-18	Andreetto Alessio	Verificatore	Verifica$_g$documento
0.2.1	2023-05-17	Corbu Teodor	Analista	Aggiunti termini al glossario
0.2.0	2023-05-09	Corbu Teodor	Verificatore	Verifica documento
0.1.2	2023-05-09	Ibra Elton	Analista	Aggiunti termini al glossario
0.1.1	2023-05-08	Ibra Elton	Analista	Aggiunti termini al glossario
0.1.0	2023-05-04	Corbu Teodor	Verificatore	Verifica$_g$documento
0.0.2	2023-05-03	Beschin Michele	Analista	Aggiunti termini al glossario
0.0.1	2023-05-02	Beschin Michele	Analista	Creazione struttura documento

Indice

A

Analista: Persona che conosce il dominio del problema e definisce i requisiti espliciti e impliciti. Si occupa di redigere il documento Analisi dei Requisiti.
API: Un insieme di subroutine o di funzioni che un programma, oppure un'applicazione, possono richiamare al fine di chiedere al sistema operativo di svolgere un determinato compito. Le API di Windows consistono di oltre mille funzioni richiamabili da programmi scritti in C, C++, Pascal e in altri linguaggi al fine di creare finestre, di aprire file e di svolgere qualche altra funzione essenziale. Ad esempio, un'applicazione che voglia visualizzare un messaggio sullo schermo può richiamare la funzione API di Windows chiamata MessageBox.
Asincrona: Modalità di svolgimento delle attività in cui i partecipanti si scambiano informazioni senza dover comunicare in tempo reale.
Attore: L'attore rappresenta un ruolo o una responsabilità in un determinato scenario di utilizzo di un sistema software e viene identificato durante l'analisi dei requisiti e nella modellizzazione dei casi d'uso. L'attore può essere sia principale, ovvero l'attore principale che utilizza il sistema, sia secondario, ovvero un attore che supporta l'attore principale nell'utilizzo del sistema o fornisce informazioni o servizi al sistema stesso.

B

Base64: È un sistema di codifica che consente la traduzione di dati binari in stringhe di testo ASCII, rappresentando i dati sulla base di 64 caratteri ASCII diversi. Viene usato principalmente come codifica di dati binari nelle e-mail, per convertire i dati nel formato ASCII.
Branch: E' una copia separata di una repository di GitHub che permette di aggiungere nuove funzionalità o correzioni di bug senza modificare il branch principale.

C

Capitolato: Un capitolato d'appalto è un documento del committente che specifica cosa richiede che sia presente nel prodotto e i suoi vincoli.
Caso d'uso: La tecnica del caso d'uso in informatica viene utilizzata nei processi di ingegneria del software per raccogliere in modo completo e preciso i requisiti necessari alla produzione di un software di qualità.
CDN: In telecomunicazioni Content Delivery Network o Content Distribution Network, descrive un sistema di computer collegati in rete attraverso internet che collaborano in maniera traspartente, sotto forma di sistema distribuito, per ripartire contenuti agli utenti finali ed erogare servizi di streaming audio e video. Grazie alla CDN si riducono notevolmente i tempi di caricamento di una pagina perché quando un contenuto viene richiesto, a rispondere è il server più vicino geograficamente e ciò si ripercuote positivamente sulle prestazioni del sito.

D

Deflate: Deflate (stilizzato come DEFLATE) è un algoritmo per la compressione dati senza perdita che è stato introdotto dal programma PKZIP, e quindi formalizzato nella RFC 1951. È tuttora ampiamente utilizzato per le sue ottime prestazioni e l'assenza di brevetti.
Discord: Piattaforma gratuita che fornisce servizi di chat vocale, testuale e video tra singoli membri o in server dedicati.
Discovery Service: È il processo di rilevamento automatico di dispositivi e servizi su una rete di computer. Ciò riduce la necessità di una configurazione manuale da parte di utenti e amministratori. Un Service Discovery Protocol (SDP) è un protocollo di rete che aiuta a realizzare il rilevamento dei servizi. Service discovery mira a ridurre gli sforzi di configurazione richiesti da utenti e amministratori.

E

Efficacia: Con efficacia si intende la misura della capacità di raggiungere un obiettivo; è strettamente legato a quanto ciò che viene fatto rispetta i requisiti.
Efficienza: Con efficienza di intende la misura per cui si impiegano il minimo numero di risorse per raggiungere un obiettivo.
Endpoint: Un endpoint è un punto di accesso specifico in un'applicazione o un sistema informatico, spesso utilizzato per interagire con le risorse o i servizi. Gli endpoint possono essere URL in una API web o indirizzi IP in una rete. Forniscono un modo strutturato per comunicare con un'applicazione o una risorsa tramite richieste e risposte.

G

Git: Sistema di controllo di versione distribuito che tiene traccia dei cambiamenti nei file.
GitHub Issues: Un sistema integrato in GitHub che consente la gestione dei ticket e la segnalazione dei problemi.
GitHub Actions: GitHub Actions è uno strumento fornito da GitHub che permette l'automazione di compiti di varia natura.
GitHub Desktop: GitHub Desktop è un'applicazione gratuita e open source disponibile per i sistemi operativi Windows e Mac. Consente di gestire i progetti in modo facile e intuitivo, creare commit significativi e tenere traccia della cronologia del progetto all'interno dell'applicazione stessa, invece che attraverso la riga di comando.
Google Drive: Google Drive è un servizio web, in ambiente cloud computing, di memorizzazione e sincronizzazione online che permette di realizzare documenti, fogli di calcolo e presentazioni.
Gmail: Google fornisce un servizio di posta elettronica chiamato Gmail che è gratuito, ma include annunci pubblicitari e non è un software libero.

H

Hash: Un hash in crittografia è una funzione matematica che trasforma un input (come un testo o dati) in una stringa di lunghezza fissa, chiamata hash, che rappresenta in modo univoco l'input originale. Questo processo è unidirezionale, il che significa che è difficile ottenere l'input originale da un hash. Gli hash sono ampiamente utilizzati per garantire l'integrità dei dati e la sicurezza delle informazioni.
Holder: Gli utenti che raccolgono credenziali da diverse fonti e le conservano nel loro portafoglio di identità. Il portafoglio di identità può essere un servizio ospitato o un'applicazione eseguita su un dispositivo dell'utente.
HTTP redirect: Il reindirizzamento URL, noto anche come inoltro URL, è una tecnica per fornire più di un indirizzo URL a una pagina, un modulo, un intero sito Web o un'applicazione Web. HTTP ha un tipo speciale di risposta, chiamato HTTP redirect, per questa operazione.
HTTP response: Un *HTTP response* viene effettuata da un server a un client. Lo scopo della risposta è quello di fornire al client la risorsa richiesta, o informare il client che l'azione richiesta è stata eseguita; oppure per informare il client che si è verificato un errore nell'elaborazione della sua richiesta. Una risposta HTTP contiene:

- Una linea di stato.
- Una serie di intestazioni HTTP o campi di intestazione.
- Un corpo del messaggio, che di solito è necessario.

I

Issuer: Istituzioni che rilasciano credenziali ai Holder (ad esempio, UniPD).
ISO/IEC 9126: ISO/IEC 9126 è un insieme di normative e linee guida che definiscono un modello per valutare la qualità del software. Il modello offre alle società di software un approccio per migliorare l'organizzazione e i processi di sviluppo, con l'obiettivo di migliorare la qualità del prodotto finale.

J

JSON: JSON, acronimo di JavaScript Object Noatation, è una formula adatta all'interscambio di dati fra applicazioni client/server.

K

Keep (Google): È un servizio di Google per prendere annotazioni.

M

MaterialUI: Una libreria di componenti React che segue le linee guida di Material Design, permettendo agli sviluppatori di creare facilmente interfacce basate su questo stile

P

Postman: Software utilizzato per testare, documentare e gestire le API.
Processo: Insieme delle attività correlate e coese che trasformano i bisogni in prodotti (il risultato di un processo si chiama prodotto). Opera secondo regole consumando risorse.
Progettista: Si occupa di definire l'architettura del sistema alla base del prodotto software. Segue la fase dello sviluppo del prodotto.
Programmatore: Partecipa sia alla realizzazione che alla manutenzione del prodotto. E' competente nella codifica e nella realizzazione di componenti necessarie all'esecuzione delle prove di verifica e validazione. Il codice prodotto dal programma deve essere mantenibile nel tempo.
Proof of concept: Con il termine proof-of-concept si intende una realizzazione incompleta o abbozzata di un determinato progetto o metodo, allo scopo di provarne la fattibilità o dimostrare la fondatezza di alcuni principi o concetti costituenti.

Q

Qualità: Insieme delle caratteristiche di un'entità, che ne determinano la capacità di soddisfare esigenze sia espresse che implicite.

R

React: Libreria JavaScript per la creazione di interfacce utente reattive e componenti riutilizzabili.
Repository: Archivio centralizzato dove vengono memorizzate le informazioni e i dati in formato digitale sulla base di metadati che ne permettono la rapida individuazione.
Responsabile: Ha il compito di pianificare le attività, coordinare e controllare tutti i membri del team. Si occupa anche di approvare i documenti e rappresenta il team presso l'azienda proponente.

S

Salt: Un salt in crittografia è una stringa casuale aggiunta ai dati prima di eseguire una funzione di hash. Questo rende più difficile l'attacco tramite "rainbow table" e migliora la sicurezza delle password memorizzate, poiché anche password identiche avranno hash diversi a causa del salt.
SAML Response: Acronimo di Security Assertion Markup Language è uno statndard informatico per lo scambio di dati di autenticazione e autorizzazione tra domini di sicurezza distinti. In particolare SAML Response viene inviata dall'identity provider al service provider, se l'utente ha avuto successo nel processo di autenticazione, contiene l'asserzione con il NameID / gli attributi dell'utente.
SAML v2: SAML 2.0 è un protocollo basato su XML che utilizza token di sicurezza contenenti asserzioni per passare informazioni su un principale (di solito un utente finale) tra un'autorità SAML, denominata Identity Provider, e un consumatore SAML, denominato Service Provider. SAML 2.0 abilita il single sign-on (SSO) cross-domain basato sul Web, che aiuta a ridurre il sovraccarico amministrativo della distribuzione di più token di autenticazione all'utente.
Server Proxy: Un server proxy è un intermediario tra un dispositivo client e un server remoto. Esso instrada le richieste del client al server e ritorna le risposte, consentendo il controllo, la sicurezza o l'ottimizzazione delle comunicazioni tra di essi.
SSL: Un protocollo e un metodo di crittografia proposto da Netscape per proteggere le informazioni che circolano su Internet. Definisce i meccanismi di trasporto delle informazioni tra un browser e un server Web al fine di eseguire transazioni sicure su Internet. Le funzioni base sono la cifratura dei dati, la loro convalida (con l'aggiunta di altri dati cifrati di riscontro) e l'autenticazione della fonte (mediante l'aggiunta ai dati stessi di una firma digitale). Assieme a SHTTP (Secure HTTP) è uno dei due standard di sicurezza che vengono utilizzati su Internet. Per cifrare i dati, SSL utilizza il sistema di chiave pubblica e chiave privata definito dalla RSA dove si chiede che il server disponga di una coppia unica di chiavi tra loro correlate matematicamente e che vengono utilizzate per iniziare ciascuna transazione. Affinchè la comunicazione possa aver luogo, il client deve possedere un file di riconoscimento che viene distribuito dall'autorità di certificazione, che può essere interna oppure esterna all'azienda. Nel file di riconoscimento è inserito il nome del certificatore e una chiave radice pubblica abbinata univocamente a quel particolare server. Quando il client contatta il server, questo risponde fornendo i propri dati d'identificazione e se questi coincidono con quanto registrato nel file di certificazione è possibile aprire una sessione sicura in modalità SSL. La stessa procedura vale nei confronti del client quando anche questo deve essere certificato. Il file di riconoscimento si chiama keyring e contiene la chiave pubblica e privata del proprietario e una o più certificazioni. Il keyring può essere autocertificato quando non si vuole ricorrere a un'autorità esterna di certificazione, ma in questo caso il livello di sicurezza è inferiore.
Status Code: Gli status code (o response codes) indicano se una specifica richiesta HTTP è stata completata correttamente. Sono parte integrante del protocollo HTTP (acronimo di Hypertext Transfer Protocol), il protocollo usato da client e server per comunicare e scambiare informazioni.

T

Teams (Microsoft): Piattaforma di comunicazione e collaborazione unificata che combina chat di lavoro persistente, teleconferenza, condivisione di contenuti.
Telegram: Servizio di messaggistica istantanea e broadcasting basato su cloud.
TLS: Transport Layer Security (TLS) e il suo predecessore Secure Sockets Layer (SSL) sono dei protocolli crittografici di presentazione usati nel campo delle telecomunicazioni e dell'informatica che permettono una comunicazione sicura dalla sorgente al destinatario (end-to-end) su reti TCP/IP (come ad esempio Internet) fornendo autenticazione, integrità dei dati e confidenzialità operando al di sopra del livello di trasporto.
Token JWT: Un token JWT, o "JSON Web Token", è un formato di rappresentazione compatta e autocontenuta per trasmettere informazioni tra due parti in un formato facilmente leggibile da macchine e verificabile da una firma digitale. È comunemente utilizzato per autenticare e autorizzare l'accesso agli endpoint o alle risorse in un'applicazione web o API.

U

UI: User Interface (in italiano Interfaccia Utente). E' metodo di comunicazione tra un utente e le funzionalità del backend attraverso elementi interattivi come pulsanti, menu e finestre di vario genere.
UML, diagrammi: UML è un linguaggio di modellazione e di specifica basato sul paradigma orientato agli oggetti. La notazione UML è semi-grafica e semi-formale; un modello UML è costituito da una collezione organizzata di diagrammi correlati, costruiti componendo elementi grafici (con significato formalmente definito), elementi testuali formali, ed elementi di testo libero. Ha una semantica molto precisa e un grande potere descrittivo.
URI: In informatica, lo Uniform Resource Identifier è una sequenza di caratteri che identifica universalmente ed univocamente una risorsa. Sono esempi di URI: un indirizzo web, un documento, un indirizzo di posta elettronica, il codice ISBN di un libro, un numero di telefono col prefisso internazionale.
URL encoded **UML, diagrammi**: UML è un linguaggio di modellazione e di specifica basato sul paradigma orientato agli oggetti. La notazione UML è semi-grafica e semi-formale; un modello UML è costituito da una collezione organizzata di diagrammi correlati, costruiti componendo elementi grafici (con significato formalmente definito), elementi testuali formali, ed elementi di testo libero. Ha una semantica molto precisa e un grande potere descrittivo.

V

Verifica: Accertamento che l'esecuzione delle attività di processi svolti nella fase in esame non causino errori.
Verificatore: È presente per l'intera durata del progetto e si occupa di svolgere le attività di Verifica e Validazione.
Verifier: Entità interessate a consumare credenziali (ad esempio, una banca online che chiede le credenziali di registrazione universitaria per offrire un conto studente). Le credenziali fornite a un verificatore da un titolare possono essere confezionate in "presentazioni verificabili".

W

Wallet: Applicazione in cui l'utente memorizza credenziali che può utilizzare presso dei provider.
Walt.id: è un'infrastruttura di identità digitale decentralizzata che facilita l'accesso e la condivisione delle credenziali digitali tra le persone e le organizzazioni.
Web App: Applicazione fruibile via web per mezzo di un network, come Internet, che offre determinati servizi all'utente. Una web app$_g$non necessita di essere installata.
W3C Data Model: Il "W3C Data Model" è un modello di dati definito dal World Wide Web Consortium (W3C), un'organizzazione che sviluppa standard per il World Wide Web. Il modello di dati del W3C è progettato per rappresentare informazioni strutturate in modo interoperabile e standardizzato, consentendo la condivisione e lo scambio di dati tra diverse applicazioni e piattaforme web.

X

XML Digital Signature: La firma XML definisce una sintassi XML per le firme digitali ed è definita nella raccomandazione W3C Sintassi ed elaborazione della firma XML. Funzionalmente, ha molto in comune con PKCS #7, ma è più estensibile e orientato alla firma di documenti XML. Viene utilizzato da varie tecnologie Web come SOAP, SAML e altre.

Z

Zoom: Piattaforma di comunicazione che combina chat di lavoro persistente, teleconferenza, telelavoro, formazione a distanza e relazioni sociali.