Descrizione Piattaforma Servizi di Edenred Italia S.r.l.

Altro

Edenred Italia Srl

Via GB Pirelli 18
20124 Milano
Italy
☎ +39 (0) 2 26 904 1
+39 (0) 2 21 309 1
https://www.edenred.it/

Società	Funzione	Scopo
Edenred	CISO	Accountable
Edenred	CIO	Responsible

Revisioni					
#	Data	Descrizione	Autore	Rivisto da	Approvato da.
1.3	19/02/2020	prima bozza rilasciata	CISO	CISO	CISO
1.4	14/04/2020	Aggiornamento documento	CISO	CISO	CISO
1.5	15/09/2020	Aggiornamento documento	CISO	CISO	CISO
1.6	26/11/2020	Aggiornamento documento	CISO	CISO	CISO

Sommario

1. Introduzione

1.1. Scopo del documento

Il documento descrive come Edenred Italia espone i propri servizi ai propri clienti.

1.2. Termini e definizioni

Termine	Definizione
API	Application Programming Interface
CVE	Common Vulnerabilities and Exposures
DMZ	Demilitarized Zone
http	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
IPS	Intrusion Prevention System
SFTP	SSH File Transfer Protocol
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SSH	Secure Socket Shell
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
JSON	JavaScript Object Notification
JWT	JSON Web Token
SAML2	Security Assertion Markup Language 2
UDDI	Universal Description Discovery and Integration
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
WAF	Web Application Firewall
WAPT	Web Application Penetration Test
WSDL	Web Services Description Language
XML	eXtensible Markup Language

2. Caratteristiche Tecniche del Portale

2.1. Architettura

I servizi forniti da Edenred Italia si basano su una piattaforma web installata direttamenta sull'infrastruttura di Edenred. Questa scelta permette non solo di gestire in maniera ottimale rilasci e patch applicativi e di sicurezza ma anche di integrare meglio la piattaforma con l'intero ecosistema di Edenred (fatturazione, gestione ordini, autorizzatori, ecc…).

La piattaforma si basa su una architettura formata da un layer di interfaccia gestita da un prodotto portale, che permette di offrire un'univoca user experience sui diversi prodotti, servita da un sistema basato su architettura orientata a servizi (SOA).

A garanzia della continuità del servizio, i vari strati dell'architettura applicativa sono ridondati (cluster in alta affidabilità). Questo tipo di architettura risulta quindi:

- Scalabile a seconda delle esigenze di business
- Garante della continuità del servizio
- Flessibile per integrazioni/variazioni applicative o di logiche di business

2.1.1. Interfaccia WEB utente

L'Interfaccia utente gestisce la componente di user experience dell'utente. L'interfaccia è operativa attraverso differenti istanze bilanciate e protette da un Web Application Firewall (che intercetta e mitiga i più comuni attacchi informatici). Tutti i livelli dell'infrastruttura sono implementati su zone separate (es: DMZ di Front-End), protetti da sistemi di rilevamento e blocco delle intrusioni (IPS) e sono presenti apparati dedicati e in alta affidabilità per la gestione delle VPN verso i nostri partner. Le linee di connessione per la gestione del servizio sostitutivo di mensa sono caratterizzate da un'infrastruttura ridondata.

2.1.2. Architettura a Servizi

Tutta la business logic è gestita attraverso un'architettura orientata a servizi per offrire la massima scalabilità e affidabilità. L'infrastruttura è implementata su zone protette non accessibili dall'esterno sia a livello di VLAN che a livello di firewall. Ogni servizio è disponibile in alta affidabilità ridondato su due o più macchine con un bilanciatore.

2.2. Interoperabilità

Per garantire l'interoperabilità con i molteplici sistemi eterogenei dei clienti e partner, l'architettura dei sistemi informatici di Edenred si basa sul paradigma SOA (Service Oriented Architecture), ovvero su un un modello architetturale che poggia sul concetto di servizio.

Il servizio è il cuore di un'architettura di tipo SOA ed è un oggetto che possiede fondamentalmente un'interfaccia attraverso la quale vengono pubblicate le operazioni (**cosa**) e una parte implementativa (**come**). Chi accede al servizio (**il consumatore**), infatti, vede soltanto quello che il servizio fa, mentre chi produce il servizio (**il produttore**) può cambiarne l'implementazione a suo piacimento in modo da andare incontro a qualsiasi tipo di necessità (**tecnologica, integrativa**) senza che l'utilizzatore se ne accorga: la parte visibile resta immutata così come la modalità di utilizzo del servizio.

Il consumatore, quindi, può continuare ad utilizzare un servizio come prima, nonostante ne sia stata cambiata l'implementazione da parte del produttore.

Caratteristiche di un servizio (Web Service)

Un servizio, oltre a possedere un'implementazione e un'interfaccia di accesso, deve essere in grado di:

- formare servizi più grandi e complessi (modularità)
- lasciare poco spazio a dipendenze tra produttore e consumatore e relegarle al solo uso delle interfacce (lasco accoppiamento)
- essere utilizzato per compiti specifici e isolati (isolamento)
- evitare di avere memoria dopo avere eseguito l'operazione per la quale è stato progettato in modo aumentare la scalabilità del sistema di cui fa parte (assenza di memoria)

- essere indipendente da piattaforme, linguaggi e protocolli (indipendenza)

2.2.1. Meccanismi di fruizione dei servizi

Ci sono principalmente due tipologie di fruizione per i servizi esposti dalla piattaforma di Edenred Italia. Il primo si basa su specifica SOAP mentre il secondo si basa su metodologia RESTful API. La scelta di quale tecnologia utilizzare ricade in fase di analisi tra il responsabile delle architetture ed il responsabile della sicurezza.

Essendo che questi servizi sono esposti direttamente su internet vengono attivati tutti i criteri di sicurezza per prevenire casi di data breach. Il cliente, per poter fruire del servizio, sarà dotato di meccanismi di autenticazione (certificati, user/password, ecc…). E' responsabilità del cliente proteggere questi meccanismi con la massima sicurezza, Edenred (attraverso un documento di manleva) non si ritiene responsabile di eventuali data breach dovuti alla mancanza del cliente.

In qualsiasi caso ogni servizio è accuratamente segregato, perciò l'erogazione per un cliente non potrà in alcun modo fornire informazioni su altri clienti o dipendenti di terze parti.

2.2.1.1. Fruizione attraverso SOAP

I dati scambiati sono codificati attraverso tag XML e utilizzano diversi metodi di impacchettamento. Uno dei più diffusi è SOAP (Simple Object Access Protocol), un protocollo di comunicazione che descrive appunto lo scambio messaggi XML su reti di calcolatori in maniera indipendente dal livello di trasporto, anche se all'atto pratico HTTP è il livello di trasporto d'elezione. Un messaggio SOAP contiene un header per informazioni quali sicurezza e routing e un body per il contenuto informativo vero e proprio. WSDL (Web Service Description Language) è un linguaggio, anch'esso basato su XML, per la descrizione del servizio. Non è altro che la descrizione dell'interfaccia del servizio e maschera la parte implementativa. Il requester, ad esempio, può accedere a tale descrizione e ottenere informazioni su quali funzioni il servizio è in grado di fornire.

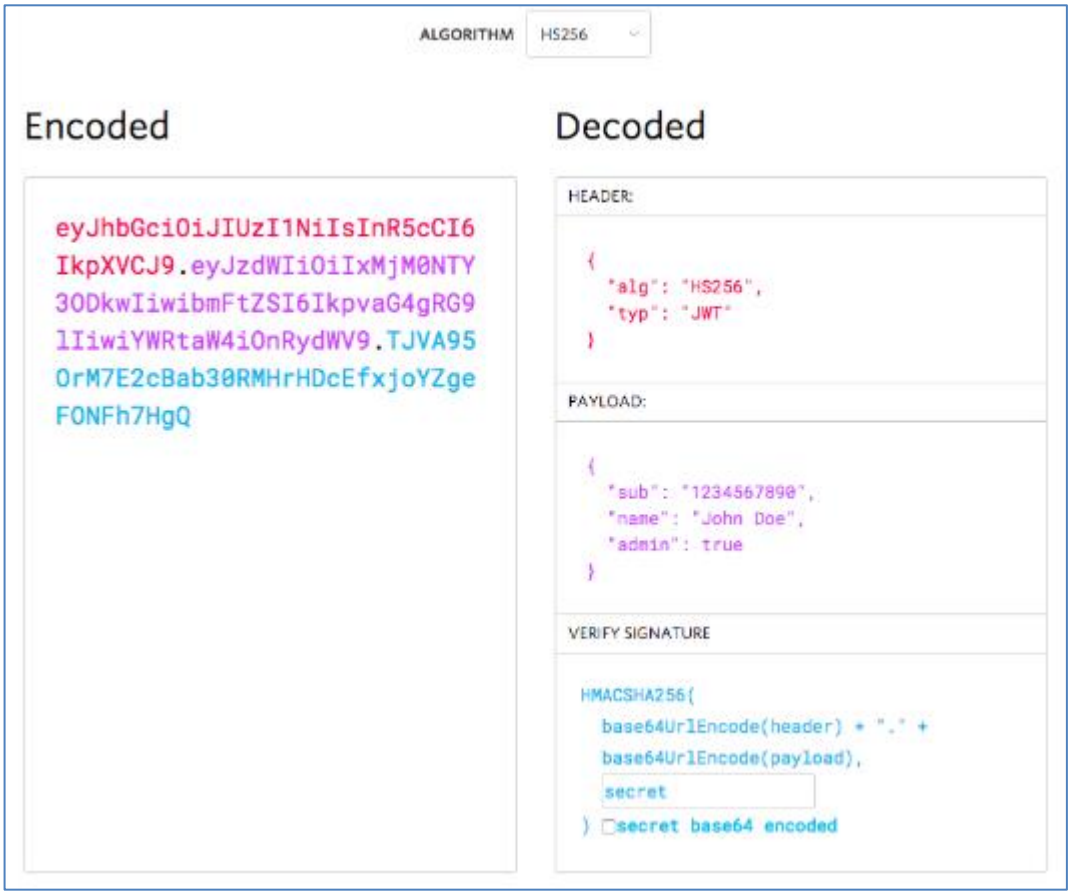
Esistono poi standard quali WS-Security e WS-Reliability per i processi di autenticazione, confidenzialità e affidabilità.

2.2.1.2. Fruizione attraverso RESTful

A differenza di SOAP, il protocollo RESTful è molto più leggero utilizzando un meccanismo di serializzazione dei dati basato su JSON. Come SOAP, questo protocollo permette un disaccoppiamento totale. L'API verrà documentata attraverso specifiche e attraverso il JSON schema.

Il livello di sicurezza viene garantito attraverso lo standard JSON Web Tokens (JWT RFC-7519) firmando e criptando le informazioni.

JWT viene utilizzato sicuramente per lo scambio del token di sicurezza ma può venir utilizzato inoltre, in base all'analisi effettuata dal responsabile di sicurezza delle informazioni, per lo scambio delle informazioni.



3. Qualità e sicurezza

Il ciclo di vita del software in Edenred Italia ha le seguenti caratteristiche:

- Tutto il software viene versionato
- Le build sono effettuate attraverso strumento automatizzato centrale
- Gli artefatti creati vengono salvati in un repository centrale ufficiale
- Ad ogni build il sistema esegue
  - Analisi statica del codice per trovare possibili problemi
  - Controllo di sicurezza delle librerie utilizzate attraverso il database CVE
- Prima del rilascio o in fasi intermedie il team dei tester effettuano
  - Test funzionali sui nuovi sviluppi
  - Test di non regressione

Una volta l'anno o quando una change lo richiede vengono effettuati dei Web Application Penetration Test (WAPT) tramite fornitore esterno con le seguenti metodologie:

- Black box con tool e etichal hacker
- White box con tool e etichal hacker

4. Validità delle scelte architetturali proposte per l'implementazione ed erogazione dei servizi

La nostra piattaforma con la strutturazione dei 3 portali, **Portale Cliente**, **Portale Beneficiari** e **Portale Affiliati** vuole rispondere alla validità della struttura proposta. La tracciabilità di ogni operazione effettuata da tutti i soggetti che partecipano al progetto, ivi compreso chi fornisce il servizio relativo all'ambito dell'Art. 100 del Tuir, è garantita. Il processo è stato definito per tutelare gli attori da eventuali controlli che possono essere effettuati ex post, sulla effettiva compliance normativa.

L'accesso al servizio avverrà previa identificazione e autenticazione dell'utente finale per la sessione corrente.

L'accesso alla piattaforma avverrà tramite protocollo https, Edenred fornirà al gruppo gli url per accesso agli ambienti.

Le applicazioni web sono monitorate 24h/24 da un sistema automatizzato che misura la disponibilità del servizio, così come internamente i sistemi sono sotto monitoraggio continuo.

Il Dipendente potrà accedere dalla rete aziendale, oppure anche da casa tramite una connessione internet personale.

TICKETXTE è l'applicativo online che permetterà a tutti gli attori del servizio di gestire e monitorare l'andamento dello stesso. L' applicativo è accessibile attraverso un'area riservata, tramite apposite credenziali (username e password), sul web.

EDENRED utilizza certificati rilasciati da GlobalSign: Organization Validation CA – G2.

5. Integrazione con la piattaforma aziendale

Edenred da anni persegue l'obiettivo di gestire i flussi informativi tra i propri sistemi e quelli dei propri clienti / Partner mediante l'uso di sistemi informatici interoperabili, cioè capaci di cooperare e di scambiare informazioni o servizi con altri sistemi o prodotti in maniera più o meno completa e priva di errori, con affidabilità e con ottimizzazione delle risorse.

Scopo di tale obiettivo è di facilitare l'interazione fra sistemi differenti, nonché lo scambio e il riutilizzo delle informazioni anche fra sistemi informativi non omogenei (sia per software che per hardware).

Le modalità predefinite per l'interoperabilità di Edenred sono basate sull'utilizzo di:

- soluzioni orientate ai servizi realizzati mediante web service.
- protocollo sicuro di scambio dati (SFTP) che garantisce un'elevata affidabilità, sicurezza e privacy dei dati scambiati
- Single Sign On basato su SAML2 IDP Initiated (vedi http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.html#5.1.4.IdP-Initiated%20SSO:%20%20POST%20Binding|outline)

6. Sicurezza e Privacy

6.1. Certificazioni e normativa

La sicurezza delle informazioni viene garantita dalla certificazione ISO/IEC 27001 attraverso l'ausilio di un SGSI. Tutti i processi sono implementati pertanto attraverso la metodologia Security by design.

Per quanto riguarda la privacy dei dati, l'adeguamento alla ISO/IEC 27001 prima e al GDPR in seguito garantisce, per tutti i processi che trattano informazioni classificate, Privacy by default e by design.

Inoltre la piattaforma raccoglierà e conserverà solo le informazioni strettamente necessarie all'erogazione del servizio.

6.2. Policy

Edenred Italia S.r.l. inoltre, come proprietaria dei servizi precedentemente indicati non può consentire accessi alla propria piattaforma se non tramite le modalità espressamente previste per l'erogazione dei servizi stessi .

Ogni altra interazione non prevista è severamente vietata poichè in constrasto con le vigenti policy aziendali, con quanto previsto nella certificazione ISO/IEC 27001 e dal GDPR (Regolamento UE n°2016/679).

6.3. Accordo tra Edenred e beneficiario

Ogni beneficiario che accede alla piattaforma di Edenred stabilisce con essa un accordo ulteriore.

7. Business Continuity – DR e Data Protection

Edenred assicura il ripristino dei dati in caso di necessità mediante una procedura che prevede copie sia a livello logico che a livello fisico dei dati in modalità full + incrementali con conservazione a 30 giorni.

Edenred ha inoltre posto in essere un Disaster Recovery Plan (DRP) ed un Business Continuity Plan (BCP) da attivare in caso di disastro maggiore quale: incendio, terremoto, alluvione, atto terroristico o di sabotaggio etc.

Il DRP e BCP per l'Italia si dividono in due categorie:

- il DRP tecnologico gestito da Edenred Corporate e che comprende due datacenter distinti presenti in Francia. I dati relativi ai servizi offerti da Edenred vengono replicati in tempo reale. Questa infrastruttura assicura un tempo di ripristino (RTO) pari a zero.
- Il BCP presente in Italia permette di gestire la continuità operativa del personale Edenred in caso di disastro attraverso telelavoro e recovery sites.

Entrambe le categorie sopra descritte vengono disciplinate attraverso la certificazione relativa alla sicurezza delle informazioni ISO/IEC 27001 e con la conformità al regolamento europeo sulla privacy 679/2016 (GDPR).

8. Data Center Europeo

Edenred adotta una soluzione basata su doppio datacenter Active/Active distanti circa 70 Km e collocati precisamente presso:

PRIMARIO	**SECONDARIO**
Isle D'abeau, France	Grenoble, France
DXC Technology	DXC technology
Avenue Steve Biko	5 avenue Raymond Chanas – Eybens
38090 Villefontaine	38053 Grenoble Cedex 09