Web RSA
Software per la gestione di RSA e CASE DI RIPOSO

Cell: +39 3509987086
Email: info@webrsa.it

Web RSA

Informativa GDPR
(regolamento (UE) n. 2016/679)

Sommario

1. Scopo del documento

Il presente documento ha lo scopo di descrivere in maniera dettagliata le modalità applicate al SW Web RSA sul regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, pubblicato sulla Gazzetta ufficiale dell'Unione europea il 4 maggio 2016 ed entrato in vigore il 24 maggio dello stesso anno ed operativo a partire dal 25 maggio 2018.

2. Scheda informativa del documento

Progetto	**Web RSA** - Software per RSA e CASE DI RIPOSO
Documento	**Specifiche adeguamento SW in merito al GDPR (regolamento (UE) n. 2016/679)**
Versione	1.0
Redatto	26/02/2024

3. Acronimi

Acronimo	Descrizione
DB	Database
TDE	Transparent Data Encryption
AES	Advanced Encryption Standard
GDPR	General Data Protection Regulation
OTP	One-Time Password

4. Informativa breve

Responsabile del trattamento dati (DPO): info@webrsa.it

Questa applicazione tratta i dati personali, anche relativi allo stato di salute (quindi "sensibili"), degli ospiti della struttura, nonché dati "comuni" eventualmente dei loro delegati/aventi diritto, del personale sanitario/assistenziale ed amministrativo e dei medici di fiducia esterni. Questi dati sono trattati per adempimenti contrattuali (rispetto ai contratti di lavoro o ai servizi resi), interesse pubblico (rispetto alle prestazioni sanitarie in convenzione o meno) o altri obblighi di legge; di conseguenza, il conferimento dei dati per l'accesso è necessario e non è soggetto a consenso preventivo.

Per garantire un adeguato livello di sicurezza e riservatezza all'applicazione ed ai dati contenuti, tutti coloro che effettuano l'accesso sono obbligati a utilizzare credenziali personali da mantenere riservate e ad inserire entro 120 secondi un codice di sicurezza inviato all'indirizzo email di registrazione; inoltre, la password deve essere complessa (contenere cioè lettere maiuscole e minuscole, numeri, altri simboli) e modificata ogni 3 mesi. Le password della email e dell'applicazione devono essere necessariamente diverse.
Secondo la normativa vigente per il trattamento digitale di dati di carattere sanitario, la informiamo che viene mantenuto un registro degli accessi e delle operazioni effettuate sui dati degli ospiti, i cui estremi possono essere resi disponibili (limitatamente al proprio profilo) su richiesta degli ospiti stessi o loro delegati/aventi diritto, nonché alle autorità competenti in caso di incidenti.

L'applicazione mette a disposizione, per comodità degli utenti e nel rispetto dei diritti di "accesso" e di "portabilità" previsti dalla normativa sulla protezione dei dati personali, una funzione di esportazione di tutti i dati relativi ad un ospite. Tuttavia, la struttura ed il gestore dell'applicazione non rispondono dell'uso o della riservatezza dei dati una volta esportati su dispositivi personali.

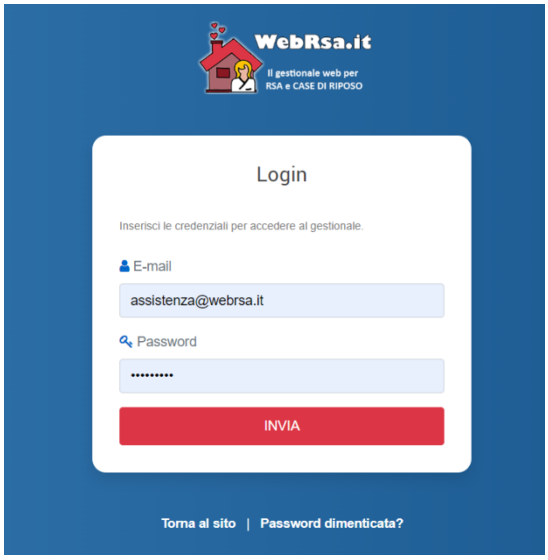
5. Autenticazione a due fattori

Il sistema prevede un'autenticazione a due fattori, descritta nei paragrafi successivi.

5.1. Generalità

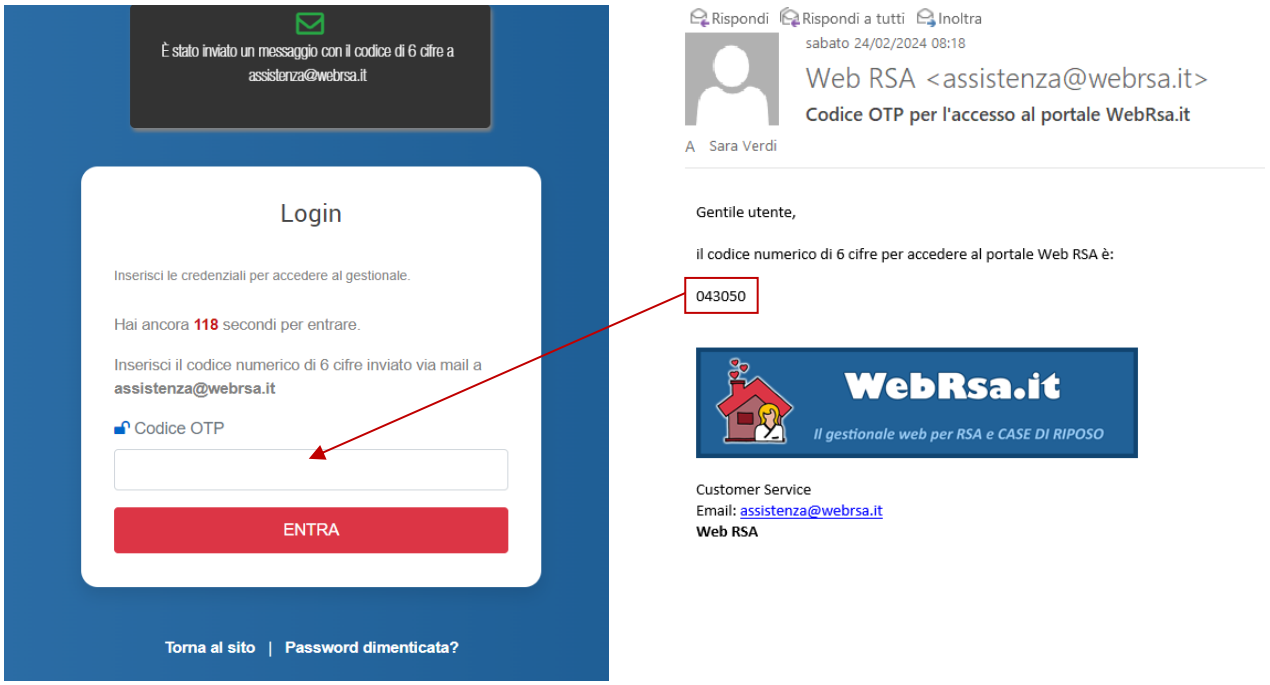
L'accesso al gestionale per tutti gli utenti profilati, avviene attraverso opportuno Form di autenticazione, attraverso il quale è necessario inserire una coppia di valori (email, password):

Figura 1 - Autenticazione a due fattori



Processando il form viene validata la correttezza dei dati inseriti.
In caso di eccezioni (es. errori di digitazione) il sistema segnala la mancata autenticazione; se i dati inseriti sono validati correttamente invece, viene generato un codice OTP di 6 caratteri numerici in modalità random. Il codice viene inviato nella mail corrispondente precedentemente inserita nel form di validazione.

Figura 2 - Autenticazione con OTP



Sono previsti 120 secondi per procedere con l'inserimento del codice OTP oltre i quali viene richiesta una nuova autenticazione con Email e Password.

6. Gestione Password

Le password di accesso al gestionale, sono custodite in un database SQL Server con cifratura dati TDE (per i dettagli verificare il paragrafo 7.1).

6.1. Generalità

Come descritto nel paragrafo 4, la password deve essere complessa (contenere cioè lettere maiuscole e minuscole, numeri, altri simboli) e la lunghezza minima forzata è di 8 caratteri alfanumerici.
Al primo accesso è dovuto l'obbligo della modifica password generata dal sistema.

6.2. Scadenza

La password ha validità trimestrale; il sistema alla scadenza costringe l'utente all'inserimento di una nuova password, diversa dalle precedenti.

7. Sicurezza adottata (Hardening)

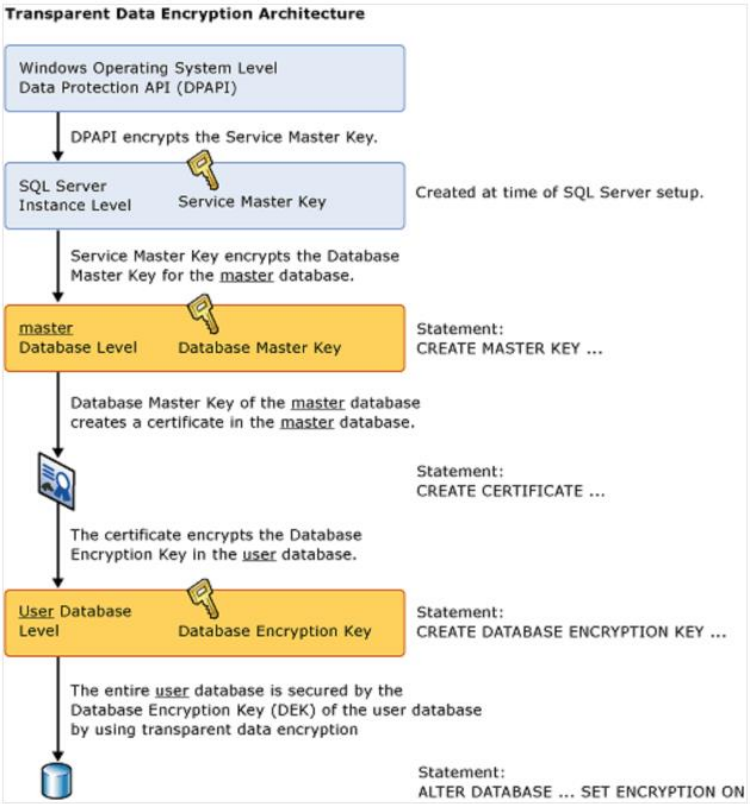
La sicurezza del sistema è stata implementata tenendo conto del database utilizzato e della necessità di criptare determinate informazioni del software (per i dettagli vedere i paragrafi successivi).

7.1. Database

SQL SERVER TDE (TRANSPARENT DATA ENCRYPTION)

Transparent Data Encryption è stata progettata per rendere completamente trasparente l'intero processo di crittografia alle applicazioni che accedono al database. TDE utilizza Advanced Encryption Standard (AES) o Triple DES, le pagine dei file dati vengono crittografate a riposo e quindi decrittografate nel momento in cui vengono lette dal disco e spostate nel buffer pool. Questa tecnica azzera i problemi e le limitazioni che si hanno quando si interroga un database crittografato. L'attivazione di Transparent Data Encryption produce backup crittografati by design per i database in cui è attiva. Il backup non potrà essere ripristinato senza la disponibilità del certificato e delle relative chiavi crittografiche.

Figura 3 - TDE



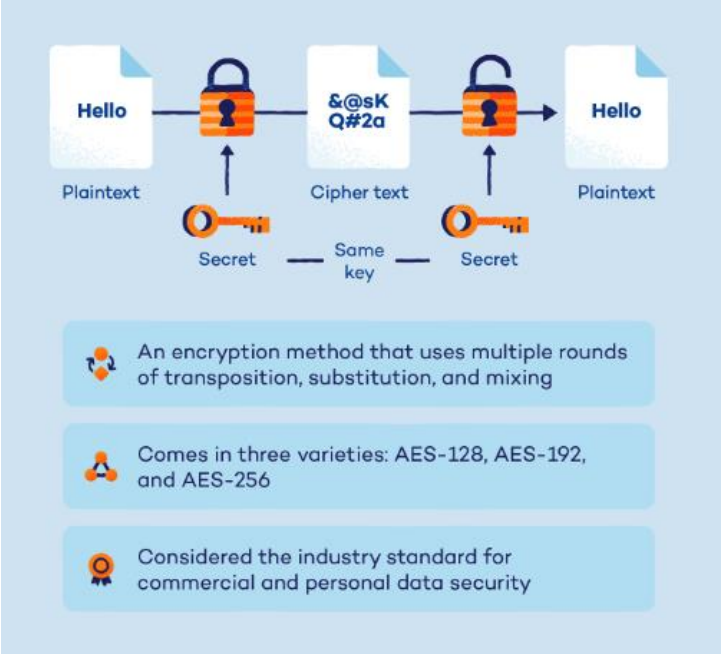
7.2. Crittografia AES

CRITTOGRAFIA AES 256 (ADVANCED ENCRYPTION STANDARD)

Un sistema di crittografia codifica i dati sensibili usando calcoli matematici per trasformare i dati in codice. I dati originali possono essere rivelati solo con la chiave corretta, consentendogli di rimanere al sicuro da chiunque tranne dalle parti autorizzate.
La maggior parte delle agenzie e organizzazioni del governo degli Stati Uniti, inclusa la NSA, utilizzano AES.

Le specifiche del protocollo AES rispettano le "Linee Guida Funzioni Crittografiche", elaborate dall'Agenzia per la Cybersicurezza Nazionale, d'intesa con il Garante per la Protezione dei Dati Personali.
Anche per il SW Web RSA è stato implementato il protocollo AES (**Advanced Encryption Standard**) a 256bit.

Figura 4 – AES



7.3. Crittografia file di configurazione

I dati sensibili delle sezioni del file di configurazione dell'applicazione web, sono opportunamente crittografate attraverso lo strumento di registrazione ASP.NET IIS (Aspnet_regiis.exe) per crittografare o decrittografare sezioni di un file di configurazione Web.
Un tipico esempio è destinato alle stringhe di connessione e/o chiavi di settaggi del gestionale.

8. Backup dati

Nel processo Task Scheduler del sistema è inserita una procedura di backup. Ogni giorno alle 02:00 viene generato un set di backup dati e salvato sulla stessa macchina nel percorso opportunamente definito in un file batch.