REGIONE BASILICATA
Stazione Unica Appaltante
Via Vincenzo Verrastro, 4 – 85100 Potenza

PROCEDURA APERTA PER L'AFFIDAMENTO DEL SERVIZIO DI MANUTENZIONE EVOLUTIVA (MEV), MIGLIORATIVA, ADEGUATIVA E CORRETTIVA (MAC), DI CONSULENZA SPECIALISTICA (SC) E SUPPORTO OPERATIVO (SO) DEL SISTEMA INFORMATIVO SUA-RB - PORTALE APPALTI.

Numero di gara SIMOG: XXXXXXXXXXXX

DESCRIZIONE DEL SISTEMA INFORMATIVO SUA-RB

Allegato
B/7

Sommario

1. Premessa

Nell'ambito del processo di digitalizzazione dell'attività amministrativa, si è reso sempre più necessario implementare l'utilizzo delle tecnologie dell'informazione e della comunicazione, sia per garantire servizi migliori alle imprese e ai cittadini, sia per realizzare una forma di comunicazione più immediata, efficiente ed economicamente sostenibile.

In riferimento al settore dei contratti pubblici, il D.Lgs. 50/2016, nel rispetto delle direttive europee, delle prescrizioni del Nuovo Codice dell'Amministrazione Digitale, del programma di *E-Government* e delle indicazioni dell'Agenzia per l'Italia Digitale, ha definito nuovi obblighi e specifiche indicazioni quanto alle modalità di gestione degli affidamenti di forniture, servizi, lavori ed incarichi professionali, dando un decisivo impulso alla informatizzazione delle procedure.

Nel contesto normativo e tecnologico su esposto, il Dipartimento SUA-RB si è dotata di una piattaforma di e-Procurement (*SUA-RB Procurement*), attraverso cui espletare e gestire le procedure di gara in modalità telematica, adempiendo al contempo, ad obblighi di pubblicità e di trasparenza.

Il presente documento ha la finalità di descrivere le basi dell'intera architettura funzionale della piattaforma *SUA-RB Procurement*.

2. Presentazione di SUA-RB Procurement

SUA-RB Procurement è composta da varie applicazioni integrate, in grado di supportare l'Ente nella gestione informatizzata e telematica delle procedure di gara, anche attraverso l'interazione digitale con gli operatori economici. Tale sistema si basa su un insieme di moderne applicazioni sviluppate in tecnologia web e standard aperti, in grado di garantire sicurezza ed interoperabilità, abbinate ad un portale web personalizzato, dedicato alla pubblicazione dei dati verso l'esterno, in conformità alla normativa vigente in materia di trasparenza e anticorruzione.

3. Accesso alla piattaforma telematica

L'utilizzo della piattaforma da parte degli operatori economici è subordinato alla registrazione degli stessi su SPID, il Sistema Pubblico di Identità Digitale. Si tratta di uno strumento che consente di accedere a tutti i servizi online della Pubblica Amministrazione con un'unica Identità Digitale utilizzabile da qualsiasi computer,

tablet o smartphone.

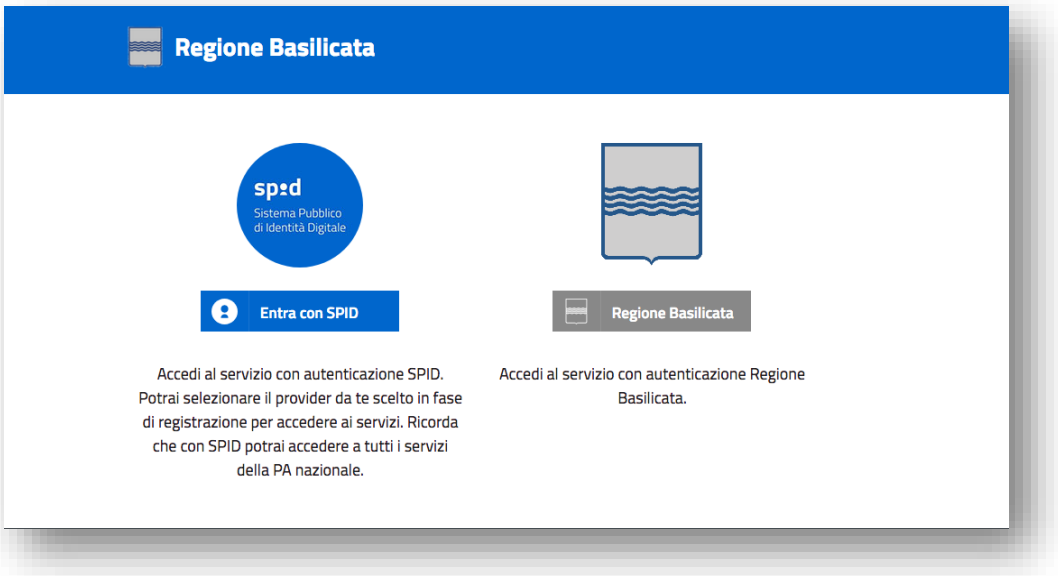

Figura 1

La piattaforma è, inoltre, integrata con il sistema di autenticazione regionale IMS (Identity Management System), attraverso cui l'utente interno può autenticarsi, in alternativa all'utilizzo di SPID.

Il sistema IMS offre un meccanismo di autenticazione e accesso di tipo Single Sign On (SSO), con cui l'utente accede a più applicazioni e risorse web, attraverso un singolo punto di ingresso, inserendo una sola volta le credenziali. Tale sistema consente di mantenere elevati livelli di sicurezza, garantiti dal fatto che le richieste di autenticazione non vengono gestite direttamente dalle singole applicazioni web, ma inoltrate a un sistema di autenticazione che ha precedentemente certificato le credenziali dell'utente connesso.

4. Moduli e funzionalità della piattaforma

La piattaforma telematica SUA-RB Procurement è composta da diversi moduli applicativi, di cui si illustrano le principali caratteristiche.

A. Portale Appalti

Il Portale Appalti (front end), integrato con la piattaforma Appalti, è il modulo che consente la pubblicazione di bandi, esiti e avvisi relativi alle procedure espletate dal Dipartimento SUA-RB. Il modulo permette agli operatori economici di accedere alla propria area riservata, presentare le offerte, prendere visione delle procedure in corso e di quelle scadute. Il Portale, raggiungibile tramite il sito https://www.sua-rb.it, funge da Profilo del committente, consentendo, a norma dell'art. 73 del D.Lgs. 50/2016, il rispetto dei principi di pubblicità e di trasparenza.

B. Modulo Appalti

Appalti (back end) rappresenta il modulo principale di tutto il sistema informativo di e-Procurement e consente la gestione informatizzata e telematica delle procedure di gara,

dall'indizione fino all'aggiudicazione, l'interazione digitale con gli operatori economici e lo svolgimento delle sedute di gara, con relativo scambio di documentazione, in modalità telematica.

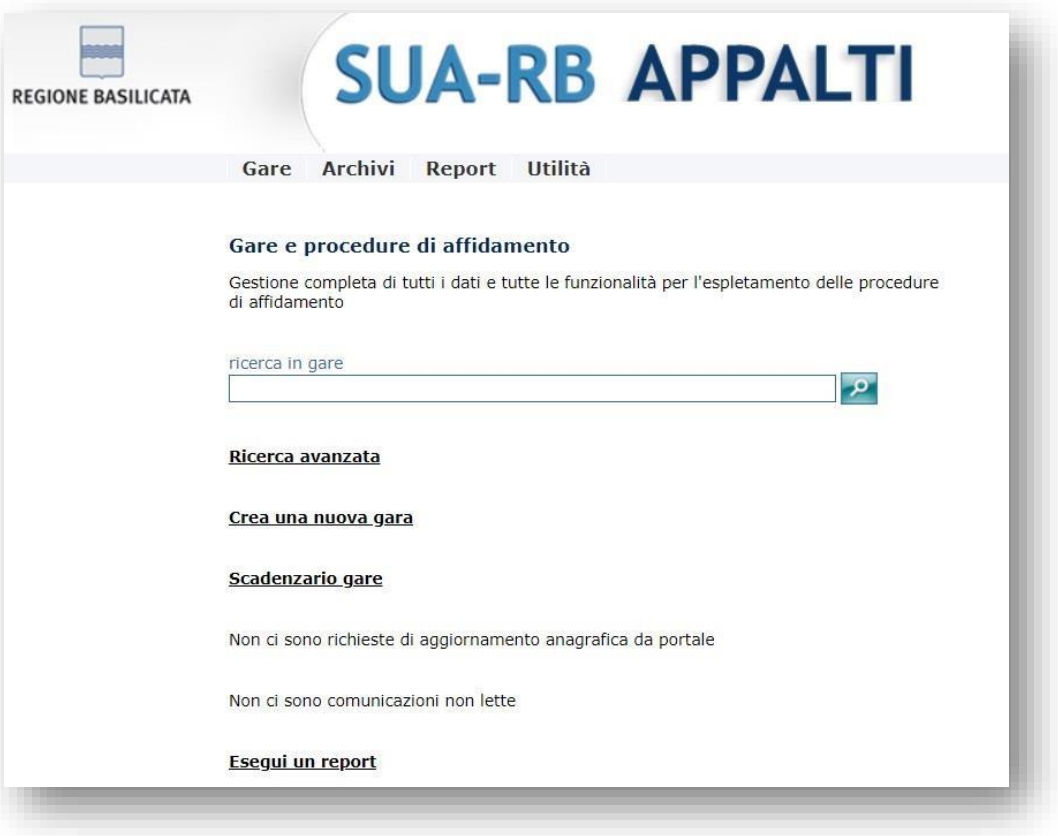

Figura 2

Il modulo rappresenta un supporto per gli utenti che, attraverso le diverse maschere di raccolta dati, sono guidati nel rispetto della prassi da seguire a seconda della tipologia di gara o dell'importo. La gestione del procedimento di gara viene, inoltre, supportata da un wizard che rappresenta l'iter di gara in passi consecutivi, guidando l'utente nelle operazioni da svolgere.

L'iter varia in funzione del profilo applicativo, della tipologia di procedura, del criterio di aggiudicazione e di altre variabili applicative.

La piattaforma è utilizzabile mediante un browser internet, senza la necessità di interventi di installazione e di configurazione dei posti di lavoro; la navigazione è facilitata da un'interfaccia munita di liste di funzioni sempre visibili e accessibili e di controlli specifici per garantire l'integrità dei dati.

L'applicativo consente lo svolgimento di procedure di gara multilotto. In particolare, permette di gestire in modo unitario e comune i dati relativi alla fase di predisposizione della gara e di trattare in modo indipendente ogni singolo lotto, con la possibilità di indicare, per ognuno, tutte le informazioni ad esso afferenti.

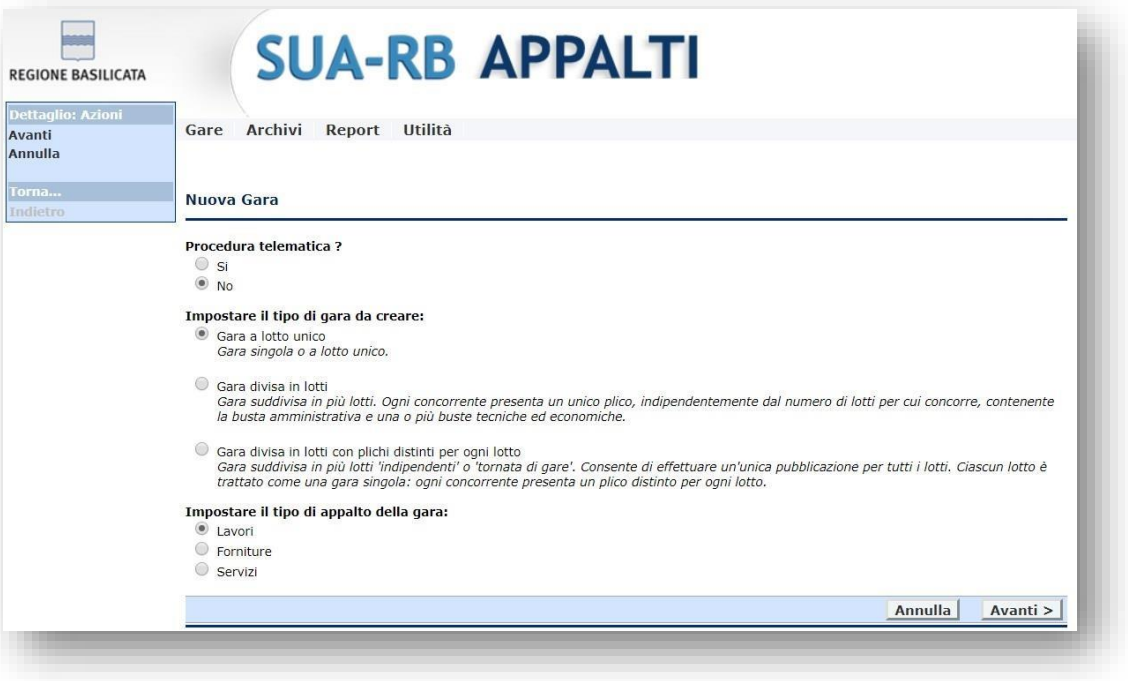

Figura 3

C. Support Appalti

Il modulo Support Appalti, supporta gli uffici nelle diverse attività di programmazione e pianificazione collegate ad una gara. Esso si compone delle funzionalità di seguito illustrate.

- Agenda/Scadenziario: consente all'utente di creare, visualizzare e condividere gli eventi in programmazione, al fine di organizzare e pianificare le attività.

  L'agenda riporta le date e gli eventi relativi alle diverse fasi delle gare presenti nel sistema e consente, inoltre, all'utente di inserire ulteriori dati utili allo svolgimento delle operazioni. L'elenco delle attività può essere visualizzato come agenda mensile con colorazione diversificata rispetto alla tipologia (apertura plichi, termini per la presentazione dell'offerta, termini per la richiesta chiarimenti, termini per risposta chiarimenti, etc ...).

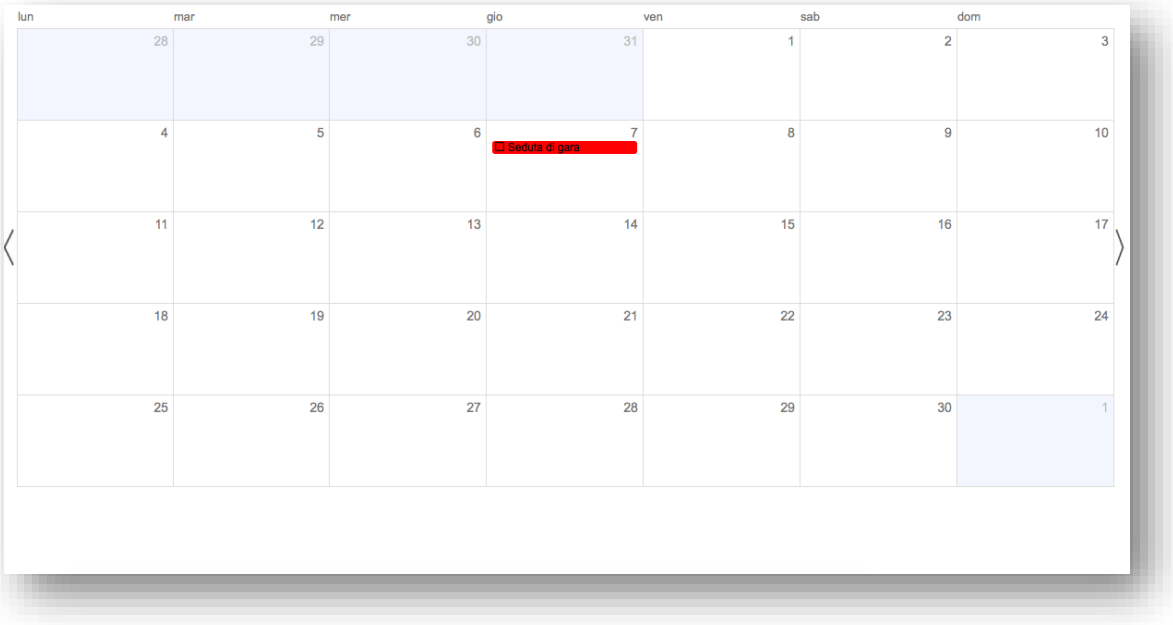

Figura 4

- Utility report: consente, una volta filtrate le informazioni utili, di interrogare il sistema e recuperare i dati inseriti nel database, in modo da visualizzare in maniera veloce e semplificata, attraverso il formato tabellare, le informazioni oggetto di interesse. I file possono essere generati in formato PDF o XLS.
- Modelli personalizzati: consentono all'utente, una volta caricate sul sistema le informazioni relative alle procedure di gara, di produrre in maniera automatica, la documentazione necessaria, secondo le esigenze dell'Ente.

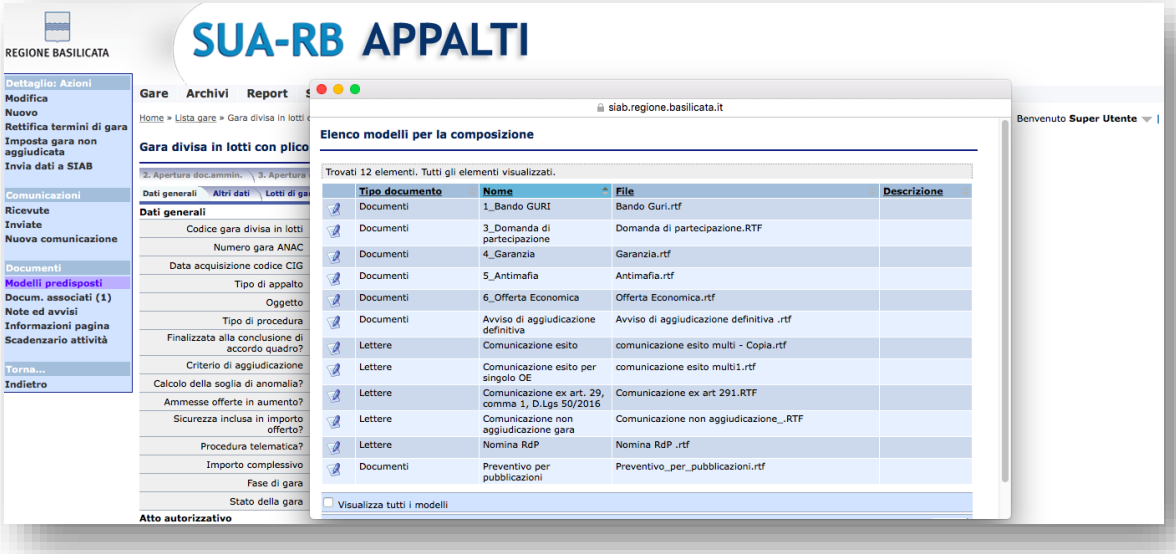

Figura 5

D. Protocollo Appalti

Il sistema informativo in uso presso il Dipartimento SUA-RB è stato integrato con il web service (WS) di protocollazione messo a disposizione dalla Regione Basilicata. La protocollazione automatica consente di rendere completamente automatizzato il processo di acquisizione dei documenti associati alle procedure gestite attraverso il Sistema Informativo. In questo modo, l'utente applicativo è esonerato dall'acquisizione e successiva protocollazione manuale dei documenti, che sono automaticamente archiviati, resi disponibili e dotati in tempo reale dei dati identificativi del protocollo.

E. Marca temporale

Il sistema informativo in uso presso il Dipartimento SUA-RB è stato integrato con la Marca Temporale al fine di garantire, durante lo svolgimento di una procedura telematica, validità giuridica e certezza della data di presentazione delle istanze. Ad ogni inserimento di documentazione e dati da parte degli utenti che intervengono sul Sistema Informativo, è apposta una Marcatura Temporale (TSS), che indica in modo elettronico non modificabile la data e l'ora precisa dell'acquisizione dei documenti e delle istanze, al fine di assicurare la legittimità delle graduatorie definite sulla base delle istanze acquisite dall'Amministrazione.

In fase di presentazione delle offerte telematica, o di qualunque altro documento inviato alla SUA-RB tramite il Portale, prima di essere protocollate in entrata dal sistema, sulle comunicazioni viene apposta la marca temporale emessa da un ente terzo certificatore (CA).

Dopo l'apposizione della marca temporale, i documenti vengono posti nella coda di protocollazione, processata con logica FIFO, così da non perdere la priorità di numerazione sequenziale. Cio' permette di regolare il flusso di richieste verso il servizio di protocollo senza intasarlo e di gestire eventuali disservizi e generazione di errori.

Pertanto, il servizio di Marca Temporale, attraverso l'associazione di data e ora certe a un documento informatico, attribuisce una validazione temporale legalmente valida e opponibile a terzi, secondo il disposto dell'art. 20, comma 3 D.Lgs 82/2005, Codice dell'Amministrazione Digitale.

Gara telematica: algoritmo per la Marca Temporale

Relativamente alla presentazione delle offerte, al fine di garantire che le informazioni trasmesse dall'operatore economico possano rimanere inaccessibili e segrete fino alla data dell'apertura delle buste, sono generati e salvati gli HASH dei file relativi alle offerte, con la generazione di un file TXT per ogni busta digitale (prequalifica, amministrativa, tecnica, economica) contenente la coppia [nome *file*,*hash*] di ognuno di essi.

Su ogni file TXT/HASH generato è apposta la Marca Temporale che indica, in modo elettronico non modificabile, la data e l'ora di acquisizione da parte del sistema informativo.

Il servizio di Marca Temporale è disponibile come servizio web erogato su ESB regionale e accessibile attraverso protocollo SOAP, il cui accesso è controllato con policy di sicurezza, previa autorizzazione. Qualora la comunicazione contenga più file allegati, viene prodotto un unico file in formato compresso (ZIP), su cui apporre la Marca Temporale.

In caso di errore o di fallimento di accesso ai servizi web della Marca Temporale, viene generato un errore di "servizio non disponibile" e l'utente è invitato a riprovare in seguito con l'invio della documentazione.

Il file di marcatura temporale prodotto è in formato TSR, Time stamp response (marca temporale inserita in un file separato); ciò comporta che per la verifica sia necessario disporre, oltre che del file TSR, anche del file originale.

L'applicativo Portale Appalti permette di verificare tramite apposita interfaccia web, la ricezione del file, la generazione del file TXT/HASH corrispondente alla documentazione di gara trasmessa, la creazione della marca temporale TSR (file TXT e file compresso ZIP potranno essere utilizzati per il controllo formale della marcatura temporale), la gestione della coda di protocollazione, la verifica di eventuali errori.

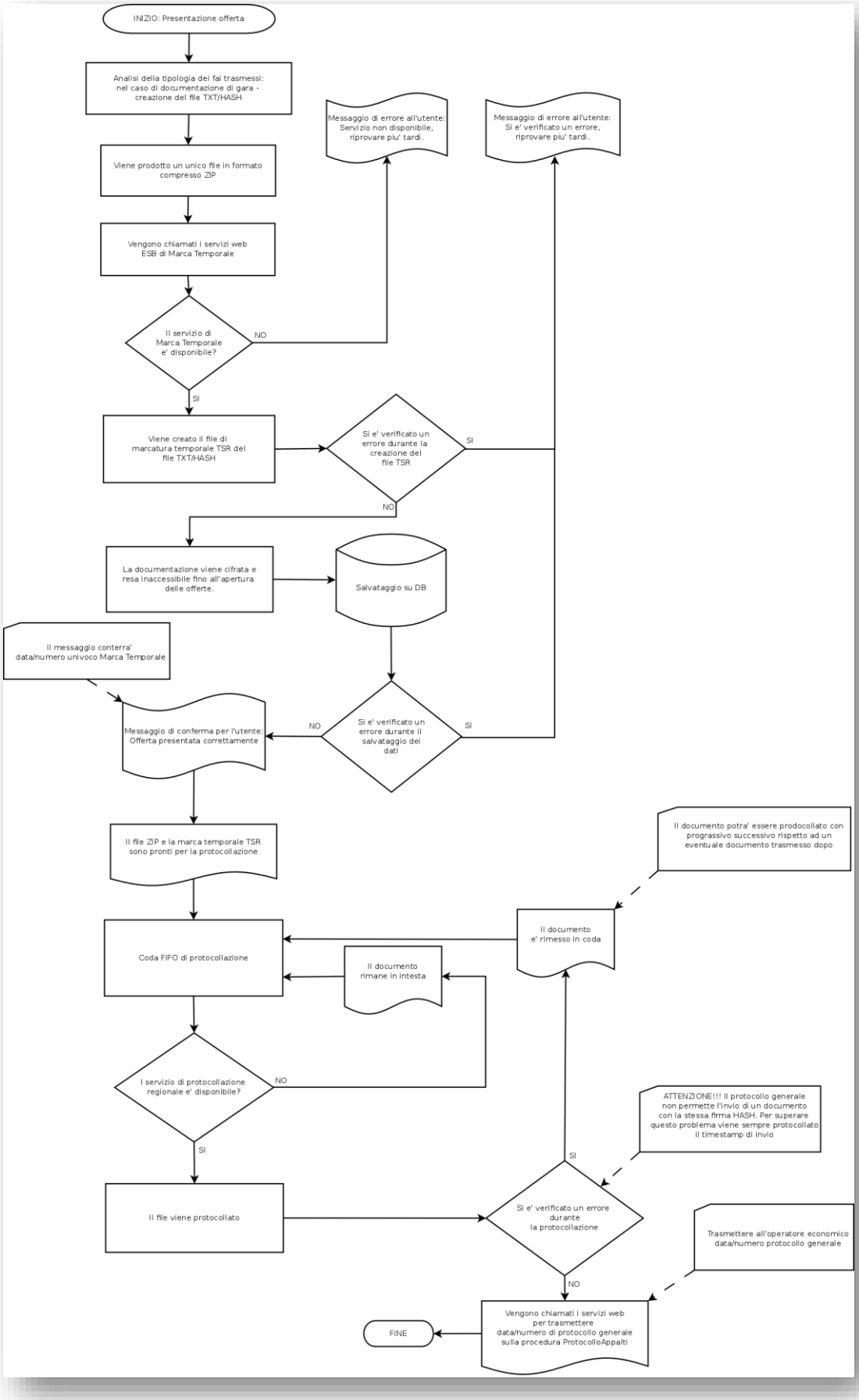
INIZIO: Presentazione offerta
Analisi della tipologia dei fai trasmessi: nel caso di documentazione di gara - creazione del file TXT/HASH
Viene prodotto un unico file in formato compresso ZIP
Vengono chiamati i servizi web ESB di Marca Temporale
Il servizio di Marca Temporale e' disponibile?
NO
SI
Messaggio di errore all'utente: Servizio non disponibile, riprovare piu' tardi.
Viene creato il file di marcatura temporale TSR del file TXT/HASH
Si e' verificato un errore durante la creazione del file TSR
SI
NO
Messaggio di errore all'utente: Si e' verificato un errore, riprovare piu' tardi.
La documentazione viene cifrata e resa inaccessibile fino all'apertura delle offerte.
Salvataggio su DB
Il messaggio conterra' data/numero univoco Marca Temporale
Si e' verificato un errore durante il salvataggio dei dati
NO
SI
Messaggio di conferma per l'utente: Offerta presentata correttamente
Il file ZIP e la marca temporale TSR sono pronti per la protocollazione
Il documento potra' essere prodocollato con progressivo successivo rispetto ad un eventuale documento trasmesso dopo
Il documento e' rimesso in coda
Coda FIFO di protocollazione
Il documento rimane in intesta
I servizio di protocollazione regionale e' disponibile?
NO
SI
ATTENZIONE!!! Il protocollo generale non permette l'invio di un documento con la stessa firma HASH. Per superare questo problema viene sempre protocollato il timestamp di invio
Il file viene protocollato
Si e' verificato un errore durante la protocollazione
SI
NO
Trasmettere all'operatore economico data/numero protocollo generale
Vengono chiamati i servizi web per trasmettere data/numero di protocollo generale sulla procedura ProtocolloAppalti
FINE

Figura 6

F. Firma digitale remota

Il modulo consente agli utenti interni di firmare digitalmente uno o più documenti direttamente dalla procedura SUA-RB Appalti, attraverso il KIT di firma remota digitale, che diversamente dalla firma digitale con Token non necessita dell'utilizzo di un dispositivo USB di firma collegato fisicamente al computer.

Il vantaggio che si ottiene dalla Firma digitale remota è quello di poter firmare da qualsiasi dispositivo, computer, table o smartphone, senza installazione di driver o periferiche da collegare ai dispositivi.

In conformità alla normativa nazionale di riferimento, la piattaforma supporta firme digitali generate nel formato CAdES (CMS Advanced Electronic Signatures, con algoritmo di cifratura SHA-256) BES. Questa tipologia di firma digitale è distinguibile dall'estensione del file che viene generato dopo l'apposizione della firma (.p7m). Il documento originario oggetto di firma e il certificato di firma digitale risiedono all'interno di un unico file. Nel caso di apposizione di firme multiple, la piattaforma gestisce firme in modalità "parallela" e in modalità "nidificata".

Per la firma dei documenti viene utilizzato il Bridge Aruba di firma digitale remota.

G. Analisi dei fabbisogni

Il Modulo web Analisi dei Fabbisogni consente di ricevere dai Dipartimenti regionali e dagli altri Enti appositamente configurati, tutte le informazioni utili alla programmazione delle attività interne, così da poter pianificare in maniera efficiente il calendario delle procedure di gara da espletare.

Figura 7

I referenti dei suddetti Enti e Società potranno collegarsi al Modulo web e inserire le informazioni concernenti le procedure di lavori, servizi e forniture che, secondo il quadro nazionale e regionale risultano essere di competenza della SUA-RB.

Tale Modulo agevola l'invio e la ricezione dei dati, i quali sono trasferiti in automatico alla SUA-RB, consentendo a quest'ultima di procedere, attraverso automatismi di inoltro e acquisizione delle informazioni, alle attività di pianificazione e armonizzazione delle iniziative di gara.

H. DGUE elettronico

Il Modulo DGUE consente alla SUA-RB di predisporre in formato elettronico il Documento di Gara Unico Europeo (DGUE), con l'indicazione specifica delle parti che l'operatore economico è tenuto a compilare.

Il Responsabile del Procedimento, attraverso la propria area riservata, inserisce il codice di gara, al fine di richiamare i dati già presenti su SUA-RB Appalti.

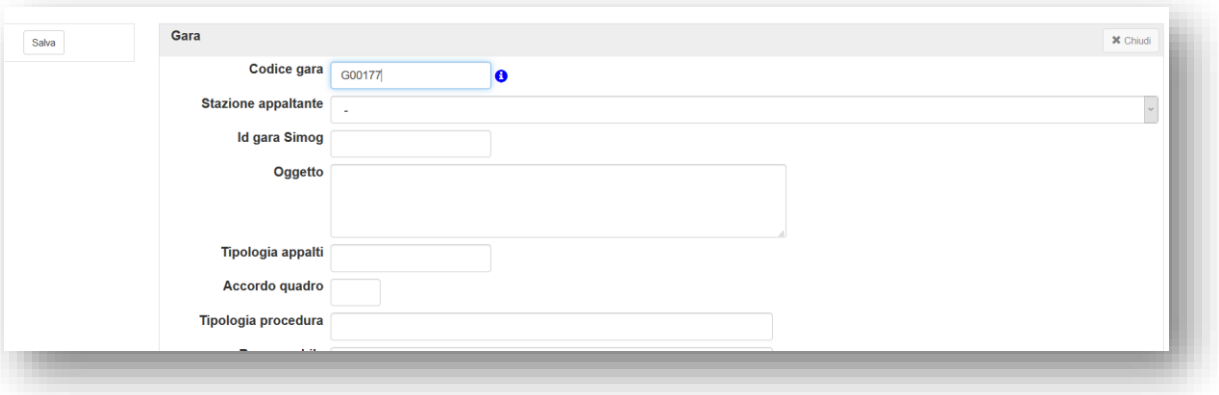

Figura 8

In tal modo, viene ad essere creato il *template* standard, contenente la suddivisione in sezioni come da Documento obbligatorio del 18 ottobre 2018.

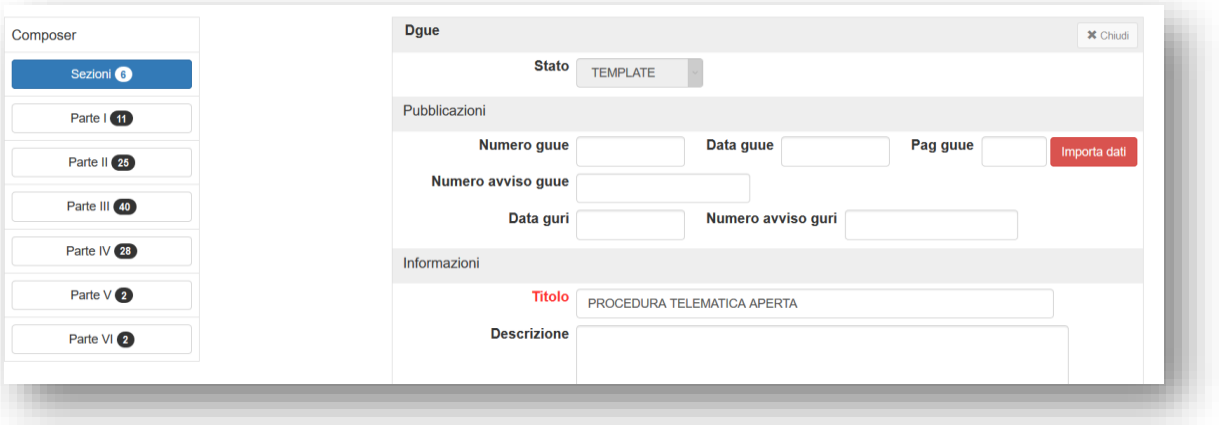

Figura 9

Il Responsabile del Procedimento pubblica il modello elettronico predisposto, affinché gli operatori economici partecipanti alla procedura possano compilarlo in modalità elettronica.

I. Automazione richiesta CIG

Il presente modulo, grazie alla cooperazione applicativa con il sistema SIMOG, permette di acquisire il Codice Identificativo di Gara rilasciato dall'A.N.AC. e procedere alla pubblicazione direttamente da SUA-RB *Procurement*.

Tale funzionalità consente di evitare l'inserimento degli stessi dati più volte, anche in caso di procedure multilotto, conservando sul proprio applicativo i dati delle gare/lotti e il rapido recupero degli stessi, per le esigenze interne di tracciabilità e di reportistica.

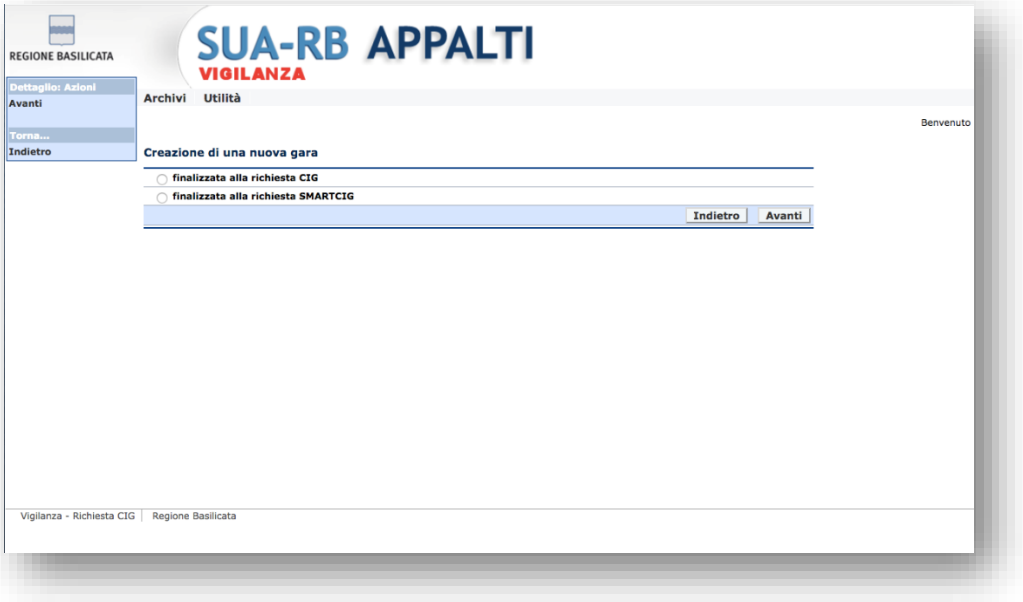

Figura 10

L. Formulari europei

Il modulo FEU consente la redazione dei bandi di gara secondo i formulari comunitari e la relativa pubblicazione automatica sulla GUUE, attraverso il portale SIMAP (Sistema Informativo per gli Appalti Pubblici Europei), raggiungibile al link http://simap.europa.eu. Il modulo permette di compilare in maniera guidata bandi, esiti e avvisi, producendo, al termine delle operazioni, un documento PDF pronto per la pubblicazione e, inoltre, include funzionalità di controllo sulla corretta compilazione dei dati, per assicurare all'utente la conformità ai requisiti previsti dalla Commissione europea.

5. Interconnessione e cooperazione

Nell'ambito del processo di cooperazione applicativa tra sistemi informativi e interconnessione finalizzata allo scambio di dati, la piattaforma SUA-RB Procurement, come sopra descritto, è stata integrata con i sistemi SIMOG dell'A.N.AC. e SIMAP a livello europeo.

In aggiunta, l'applicativo di e-Procurement colloquia con il Sistema Informativo Appalti Basilicata (S.I.A.B.), deputato al monitoraggio dei flussi informativi verso l'A.N.AC.

Grazie al principio della cooperazione applicativa, i dati presenti su SUA-RB Procurment vengono recuperati e inviati al S.I.A.B., per assolvere agli obblighi di monitoraggio, così come previsto dal D.Lgs. 50/2016 e della L.190/2012.

La Piattaforma SUA-RB Procurement è, inoltre, integrata con Centrale Bandi (CebBas), il sistema di gestione degli avvisi e dei bandi regionali. I dati pubblicati su SUA-RB *Procurement* sono inviati in automatico su CeBas, al fine di renderli disponibili e consultabili.

6. Infrastruttura tecnologica

L'intera piattaforma, basata su applicazioni web, è realizzata con moderne tecnologie open source in grado di garantire scalabilità, sicurezza e interoperabilità con i sistemi regionali in produzione ed extra regionali.

Per ciò che attiene ai requisiti hardware e software è stato predisposto apposito ambiente nel server farm regionale opportunamente adeguato al carico di lavoro, di cui si riportano le specifiche:

servername = suarb-fe.hosting.int

- ip = 172.18.14.93
- disco = 30GB
- memoria = 4GB
- cpu = 2x2Q
- sistema = CentOS 7.x
- servizi = apache 2.4.x ; libstdc++.i686

servername = suarb-app.hosting.int

- ip = 172.18.14.94
- disco = 50GB
- memoria = 4GB
- cpu = 2x2Q
- sistema = CentOS 7.x
- servizi = Tomcat 8/JDK 8; libstdc++.i686

servername = suarb-db.hosting.int

- ip = 172.18.18.135
- disco = 200GB
- memoria = 4GB
- cpu = 2x2Q
- sistema = CentOS 7.x
- software = Postgresql 9.2

Di seguito la rappresentazione schematica dell'infrastruttura di networking.

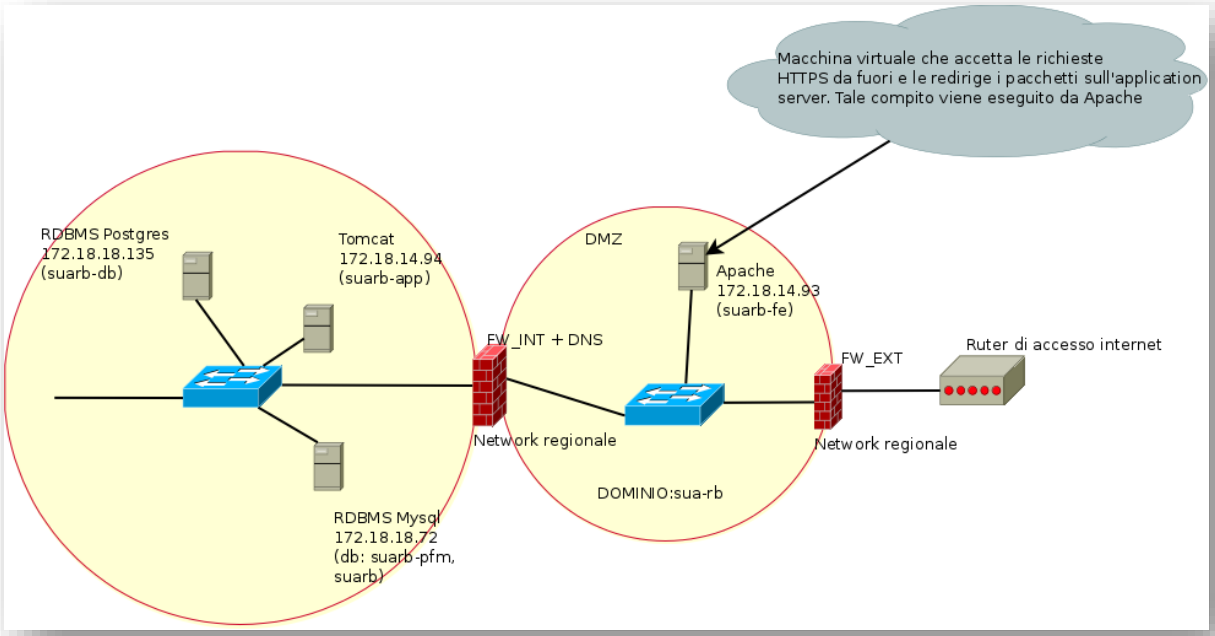

Figura 11

La piattaforma è sincronizzata sull'ora italiana riferita alla scala di tempo UTC (IEN), di cui al D.M. 30 novembre 1993, n. 591.

7. Protezione dagli attacchi informatici

La piattaforma SUA-RB Procurement, in linea con le previsioni del considerando n. 52 e dell'art. 22 della Direttiva 2014/24/UE, dell'art. 52 e dell'Allegato XI del D.Lgs. 50/2016, assicura la segretezza delle offerte, impedisce di operare variazioni sui documenti inviati, garantisce l'attestazione e la tracciabilità di ogni operazione compiuta sulla piattaforma mediante registrazioni di sistema (log), quali rappresentazioni informatiche degli atti e delle operazioni compiute valide e rilevanti ai sensi di legge.

La prima linea di difesa è, infatti, rappresentata proprio dal firewall reso disponibile dall'infrastruttura regionale, dalla struttura isolata DMZ (zona dematerializzata) - Application server - Database server, nonché dall'utilizzo del protocollo di comunicazione Transport Layer Security 1.2 (TSL), che fornisce, come requisiti chiave, l'autenticazione del sito web visitato, la protezione della privacy (riservatezza o confidenzialità) e l'integrità dei dati scambiati tra le parti comunicanti.

La necessità di proteggere il sistema informativo SUA-RB Procurement da eventuali attacchi hacker è stata affrontata attraverso la definizione di una soluzione tecnica basata su Apache – ModSecurity, firewall per applicazioni web open source. In tal modo è possibile controllare tutte le richieste HTTPS (HyperText Transfer Protocol over Secure Socket) con le relative risposte.

Tale meccanismo fornisce una garanzia soddisfacente del fatto che si sta comunicando esattamente con il sito web voluto (al contrario di un sito falso), oltre a garantire che i contenuti delle comunicazioni tra l'utente e il sito web non possano essere intercettate o alterate da terzi.

Le regole utilizzate in Apache – ModSecurity (OWASP Core Rule Set 31), permettono di ridurre i falsi allarmi, di porre dei livelli di sicurezza definiti dall'utente2, abilitare ulteriori controlli rigorosi e modalità di campionamento, eseguire l'insieme di regole definite (CRS) su una percentuale di traffico stabilita dall'utente, analizzare SQLi/XSS mediante specifici algoritmi incorporati in ModSecurity3.

I livelli di sicurezza previsti dal modulo ModSecurity con le regole CRS3 sono quattro4. Il livello di sicurezza impostato per il server SUA-RB è il Paranoia Level 3, generalmente utilizzato per i siti di bancking on-line.

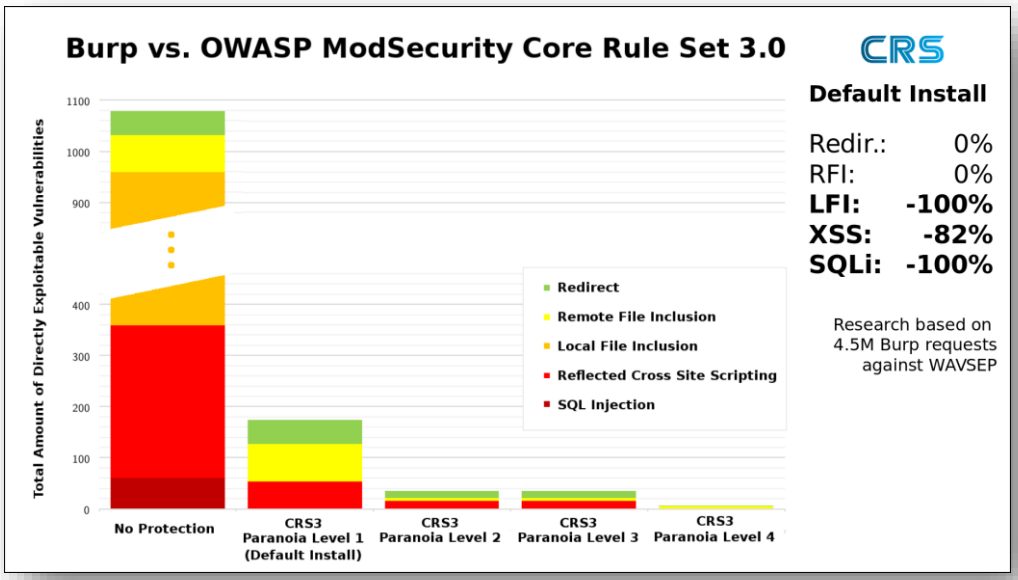

Figura 12

7.1 Gare telematiche

I moduli di SUA-RB Procurement sono stati sviluppati in modo da garantire e tutelare il principio di segretezza delle offerte (documenti e dati), così come sancito dal Codice dei Contratti pubblici e, in particolare, dal relativo art. 52, comma 5.

La soluzione realizzata prevede, infatti, l'incapsulamento dei dati e dei documenti in "buste digitali", separate per ogni fase del processo (busta amministrativa, tecnica ed economica).

Le buste digitali sono salvate nel database in formato cifrato e sono decifrabili esclusivamente all'atto dell'apertura delle buste: non esiste nel sistema alcuna informazione che permetta l'apertura delle suddette buste prima della data e dell'ora fissate per la seduta pubblica.

7.1.1 Tipologie di crittografia

La piattaforma SUA-RB Procurement è dotata di un sistema di crittografia ibrido o a doppia

[1] *OWASP Core Rule Set 3 (CRS3)* è l'insieme di regole generiche di rilevamento degli attacchi utilizzate con *ModSecurity* o *firewall* per applicazioni *web* compatibili per proteggere le applicazioni *web* da una vasta gamma di attacchi informatici.
[2] Si tratta dei cosiddetti *Paranoia* Level.
[3] Gli algoritmi utilizzati sono del tipo Libinjection.
[4] ModSecurity con le regole CRS3 prevede quattro livelli di sicurezza: Paranoia Level 1, Minimal amount of False Positives (Basic security); Paranoia Level 2: More rules, fair amount of Fps (Elevated security level); Paranoia Level 3: Specialised rules, more Fps (Online banking level security); Paranoia Level 4: Insane rules, lots of Fps (Nuclear power plant level security).

cifratura, frutto dell'unione tra crittografia simmetrica e asimmetrica5, in linea con gli standard internazionali di cifratura: AES e RSA6. Le chiavi di crittografia, generate dalla libreria Pretty Good Privacy (PGP) all'interno del sistema SUA-RB Procurement, costituiscono una barriera di sicurezza di tale robustezza da risultare inattaccabile anche mediante operazioni di brute force.

Gli algoritmi di crittografia utilizzati7, gestiti dal modulo PGP, assicurano la segretezza e riservatezza dei dati trasmessi dagli operatori economici tramite il Portale appalti.

7.1.2 Le fasi della crittografia nel sistema SUA-RB Procurement

Il funzionamento del sistema di crittografia adottato per la piattaforma SUA-RB Procurement può essere rappresentato, in maniera esemplificativa, da tre momenti distinti:

Fase A: pubblicazione della gara;

Fase B: partecipazione a una gara;

Fase C: svolgimento delle operazioni di gara in seduta pubblica.

Fase A: pubblicazione della gara

Nel corso della prima fase, il Responsabile del procedimento (RdP) definisce un codice segreto (password) per ciascuna delle buste digitali di gara. Tale codice, combinato in maniera automatica dal Modulo appalti con un altro fattore (token), riferito alla specifica procedura, costituisce la cosiddetta passphrase8, tassello fondamentale del processo di cifratura.

Proprio in virtù della tipologia di crittografia utilizzata, la passphrase non è salvata nel sistema, risultando, al contrario, una variabile ulteriore ed esterna al sistema.

Pertanto, essendo il RdP l'unico detentore del codice segreto, senza alcuna possibilità di risalire ad esso e/o recuperarlo, neppure da parte dell'Amministratore di sistema, viene suggerito al RdP di conservare, sotto la propria ed esclusiva responsabilità e in busta chiusa e sigillata, il codice medesimo, pena l'assoluta impossibilità di procedere alle successive operazioni di gara.

La prima fase termina con la creazione, attraverso l'utilizzo della libreria di crittografia PGP, della cosiddetta chiave pubblica (Kp)9.

Fase B: partecipazione a una gara

Nella seconda fase, all'avvio della compilazione di ognuna delle buste digitali da parte dell'operatore economico, il Portale appalti crea una chiave simmetrica di sessione (Ks) che viene cifrata con la chiave simmetrica temporanea (Kt), riferita allo specifico operatore economico.

---

[5] La crittografia asimmetrica è caratterizzata dall'uso di due chiavi distinte, una privata e l'altra pubblica.

[6] Si tratta, ad oggi, del più famoso e utilizzato algoritmo di cifratura asimmetrica. Scoperto in origine nel 1973 dall'Agenzia di intelligence Britannica (GCHQ), ha ricevuto la classificazione "top secret" e nel 1977 è stato reso disponibile anche ai civili grazie al lavoro dei crittografi Rivest, Shamir e Adleman.

[7] AES, per la crittografia simmetrica, e RSA per la crittografia asimmetrica.

[8] In informatica con il termine *passphrase* si intende l'insieme di parole o di stringhe alfanumeriche di solito separate da caratteri non alfabetici, come numeri, caratteri speciali o il carattere "spazio", utilizzato per l'autenticazione ad un sistema, ad un programma, ad una base dati o ad una rete, oppure per effettuare operazioni di cifratura.

[9] Nella Fase A, PGP utilizza l'algoritmo RSA.

Per effetto di tale attività crittografica, tutti i documenti e le informazioni confidenziali[10], caricati dall'operatore economico, vengono salvati nell'area temporanea del server in formato cifrato, utilizzando la su richiamata chiave di sessione (Ks). In tal modo, al salvataggio (sia in bozza che nell'invio definitivo) i file e le informazioni, come sopra richiamate, risultano tutti già cifrati. All'atto della presentazione dell'offerta, inoltre, la chiave simmetrica (Ks) viene cifrata con la chiave pubblica (Kp), generata nel corso della prima fase[11].

La chiave simmetrica (Ks), diversa per ogni operatore economico e per ogni busta, potrà essere decifrata dal modulo di back office solo in concomitanza con le operazioni di verifica della documentazione trasmessa, svolte nel corso della seduta pubblica.

Fase C: svolgimento delle operazioni di gara in seduta pubblica

La terza fase della cifratura coincide con il momento di superamento della data e dell'ora fissate per la seduta pubblica relativa all'apertura di ciascuna delle buste digitali.

Il RdP, attraverso la funzione "Attiva apertura documentazione amministrativa, tecnica, economica", può procedere, previo inserimento del codice segreto deciso all'atto della pubblicazione della gara, all'operazione di sbustamento dei plichi digitali. A seguito della digitazione del codice segreto da parte del RdP, il modulo di crittografia PGP provvede alla creazione della chiave privata (Kr) associata alla chiave pubblica (Kp), precedentemente generata, decodificando la chiave simmetrica (Ks)12. Solo a questo punto, sarà possibile decifrare i documenti e le informazioni confidenziali trasmesse dall'operatore economico attraverso il Portale appalti

Inalterabilità dei documenti

Il sistema informativo SUA-RB Procurement è stato studiato in modo tale da garantire che le informazioni trasmesse dall'operatore economico attraverso il Portale appalti siano inaccessibili, segrete e immodificabili.

A tal scopo, SUA-RB Procurement è stato dotato del servizio di marca temporale, emesso da un Ente terzo certificatore[13,] che permette di associare alle comunicazioni inviate tramite il Portale appalti data e ora certe e legalmente valide a un documento informatico, consentendo, quindi, una validazione temporale opponibile a terzi, secondo il disposto dell'art. 20, comma 3 D.Lgs 82/2005.

La marcatura temporale si basa sulle funzioni di hashing, vale a dire algoritmi che producono come output una sequenza di numeri e lettere di dimensioni variabili. Questa particolare stringa alfanumerica, unica per qualsiasi documento, prende il nome di digest. L'impronta di hash di un documento informatico può essere paragonata a un'impronta digitale e, quindi, a una caratteristica che lo identifica in maniera univoca.[14]

[10] Per informazioni confidenziali si intendono i dati inseriti direttamente a video sul Portale appalti dagli operatori economici e riferiti al prezzo unitario di una lavorazione/fornitura, all'importo unitario di una lavorazione/fornitura, all'importo offerto, al ribasso e all'aumento, all'importo offerto per permuta, all'importo offerto per canone assistenza.
[11] Nella Fase B, PGP utilizza l'algoritmo di crittografia AES.
[12] Tale combinazione avviene secondo la formula Ks= DecryptPGP(input, Kr, passphrase).
[13] CA per la Regione Basilicata è Telecom S.p.A.
[14] Il file di marcatura temporale prodotto dal servizio è in formato TSR (*Time stamp response*: marca temporale inserita in un file separato), e ciò implica che per la verifica sia necessario disporre, oltre che del file TSR anche del file originale.