ARPAE

Agenzia regionale per la prevenzione, l'ambiente e l'energia

dell'Emilia - Romagna

*** * ***

Atti amministrativi

Determinazione dirigenziale	n. DET-2021-573 del 26/07/2021
Oggetto	Servizio Sistemi Informativi e Innovazione Digitale. Proroga del contratto di fornitura dei "Servizi di gestione delle identità digitali e sicurezza applicativa" in Adesione al Contratto Quadro Consip S.p.a. "SPC Cloud Lotto 2" - CIG derivato 7300627BFA.
Proposta	n. PDTD-2021-596 del 22/07/2021
Struttura adottante	Servizio Sistemi Informativi e Innovazione Digitale
Dirigente adottante	Dott. Stefano Cattani
Struttura proponente	Servizio Sistemi Informativi E Innovazione Digitale
Dirigente proponente	Dott. Stefano Cattani
Responsabile del procedimento	Dott. Stefano Cattani

Questo giorno 26 (ventisei) luglio 2021 presso la sede di Viale Silvani, 6 in Bologna, il Responsabile del Servizio Sistemi Informativi e Innovazione Digitale, Dott. Stefano Cattani, ai sensi del Regolamento Arpae per l'adozione degli atti di gestione delle risorse dell'Agenzia, approvato con D.D.G. n. 114 del 23/10/2020 e dell'art. 4, comma 2 del D.Lgs. 30 marzo 2001, n. 165 determina quanto segue.

Oggetto: Servizio Sistemi Informativi e Innovazione Digitale. Proroga del contratto di fornitura dei "Servizi di gestione delle identità digitali e sicurezza applicativa" in Adesione al Contratto Quadro Consip S.p.a. "SPC Cloud Lotto 2" - CIG derivato 7300627BFA.

VISTI:

- la D.D.G. n. 139 del 30/12/2020 "Direzione Amministrativa. Servizio Amministrazione, Bilancio e Controllo Economico. Approvazione del Bilancio Pluriennale di Previsione dell'Agenzia per la Prevenzione, l'Ambiente e l'Energia dell'Emilia-Romagna per il triennio 2021-2023, del Piano Investimenti 2021-23, del Bilancio economico preventivo per l'esercizio 2021, del Budget Generale e della Programmazione di Cassa 2021";
- la D.D.G. n.140 del 30/12/2020 "Direzione Amministrativa. Servizio Amministrazione, Bilancio e Controllo Economico. Approvazione delle Linee Guida e assegnazione dei budget di esercizio e investimenti per l'anno 2021 ai centri di responsabilità dell'Agenzia per la Prevenzione, l'Ambiente e l'Energia dell'Emilia-Romagna";
- la D.D.G. n. 31 del 29/03/2021 recante: "Direzione Amministrativa. Approvazione del programma biennale degli acquisti di forniture e servizi per gli anni 2021 - 2022";
- il Regolamento per l'adozione degli atti di gestione dell'Agenzia approvato con D.D.G. n. 109 del 31/10/2019 e revisionato con D.D.G. n. 114 del 23/10/2020;
- il Regolamento per la disciplina dei contratti pubblici di servizi e forniture di Arpae approvato con D.D.G. n. 111 del 13/11/2019;
- il Decreto Legislativo del 18 aprile 2016 n. 50 e s.m.i., "Codice dei Contratti Pubblici";
- il Decreto Legge n. 76 del 16 luglio 2020 "Misure urgenti per la semplificazione e l'innovazione digitale" come modificato dalla legge di conversione n. 120/2020;
- il Decreto Legge 31 maggio 2021, n. 77 "Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure", in vigore dal 1.06.2021;

RICHIAMATI:

- la determina n. 983 del 4/12/2017 con la quale Arpae ha aderito al Contratto Quadro denominato SPC - Lotto 2 del 20/07/2016 (CIG 5518849A42) stipulato da Consip Spa con il RTI Aggiudicatario, composto dalle aziende Leonardo-Finmeccanica S.p.a., nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre

alla stessa, le mandanti IBM Italia S.p.A., FASTWEB S.p.A. e Sistemi Informativi S.r.l., aggiudicatarie del Lotto 2 della procedura ristretta, suddivisa in 4 lotti, indetta per l'affidamento dei servizi di Cloud Computing, di Sicurezza, di Realizzazione di Portali e Servizi on-line e di Cooperazione Applicativa per le Pubbliche Amministrazioni, per la fornitura dei "Servizi di gestione delle identità digitali e sicurezza applicativa", come da "Piano dei fabbisogni" di Arpae del 06/10/2017 Prot. n. PGDG/2017/10431, per un valore complessivo pari ad euro 185.118,92 (IVA esclusa);

- il Contratto Esecutivo e la conferma d'ordine, recante il n. PGDG/2021/13573, in virtù della quale l'inizio della fornitura citata è decorso dal 13/12/2017, sino alla data di scadenza del Contratto Quadro, tra Consip e il Fornitore aggiudicatario del Lotto 2 (20/07/2021);

CONSIDERATO:

- quanto stabilito dal Codice dell'Amministrazione Digitale (CAD), dal Regolamento Generale per la Protezione dei Dati Personali (RGDP) - che stabiliscono che le Amministrazioni devono mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, prevedendo anche una responsabilità nel caso in cui, a seguito di incidenti di sicurezza sui dati personali, non si dimostri di aver adottato ogni misura possibile, tra cui almeno il rispetto delle linee guida dell'Agenzia per l'Italia digitale-AGID, con l'obiettivo di incrementare il livello di protezione sui dati, sui sistemi e sulle infrastrutture dell'Autorità - e dal Piano Triennale per l'Informatica nella Pubblica Amministrazione;
- che persiste, pertanto, in Arpae, la necessità di continuare ad usufruire del servizio di cui in premessa per garantire l'espletamento della funzione amministrativa in maniera conforme a quanto richiesto dalla normativa di settore;

VERIFICATO

- l'assenza di Convenzioni attuali Consip o della Centrale di Committenza Regionale per la medesima fornitura;
- la possibilità di prorogare il contratto esecutivo vigente in virtù dell'Addendum nr. 4 al Contratto Quadro di cui in premessa sottoscritto tra Consip ed il RTI, in data 26/3/2021, dove il Contratto Quadro viene prorogato di ulteriori 12 (dodici) mesi ovvero sino al 20 luglio 2022, ai fini di consentire all'Ente la continuità dei servizi fruiti fino ad oggi e per adeguare la necessità di innalzamento della sicurezza dei servizi informatici;

- la regolare esecuzione del contratto in corso avente ad oggetto la fornitura di cui trattasi e la rispondenza dei servizi offerti con quelli necessari ad ARPAE;

DATO ATTO

- che Arpae ha proceduto alla stima dei costi dei servizi necessari, come di seguito riportato:

DESCRIZIONE DELLA FORNITURA	QUANTITÀ	IMPORTO PREVISTO (IVA ESCLUSA)	IMPORTO PREVISTO (IVA INCLUSA)
Servizio L2.S2.1 - Firma digitale remota (il costo unitario si riferisce al canone annuo) (Anno 2021) (Anno 2022)	1400	11.632,50 (5816,25) (5816,25)	14.191,65 (7095,825) (7095,825)
Servizio L2.S3.8 - Secure Web Gateway Anno 2021	1350	7.115,00	8.680,30
Servizio L2.S3.9 - Servizi professionali di supporto alla firma remota Anno 2021 Anno 2022	tot 25 gg 12 gg 13 gg	7.784,50 3705,80 4078,70	9.497,09 4521,076 4976,014
Totale complessivo		26.532,00	32.369,04

- che è stata acquisita la disponibilità - come da documentazione agli atti (pec recante il n. pg/2021/0110469 del 20 luglio 2021) della Leonardo s.p.a. Divisione Cyber, con sede in Roma alla Piazza Monte Grappa n. 4, in qualità di mandataria capo-gruppo del RTI aggiudicatario di cui in premessa, alla proroga del contratto in essere fino al 30/6/2022 alle medesime condizioni contrattuali, come da Progetto dei fabbisogni Identificativo (GOV-210273 Rev 1 del 14/07/2021), che si allega al presente atto e al quale ci si richiama integralmente;
- che, in deroga al Contratto esecutivo, per i servizi di Firma Digitale Remota, per i

beni rilasciati nel bimestre verrà richiesta la corresponsione dell'intero canone annuale;

- che, sulla base del progetto e all'esito della stima dei fabbisogni dei servizi usufruenti la fornitura, rimodulati sul diverso periodo contrattuale, è stato individuato il costo della proroga come risulta dal seguente prospetto riepilogativo:

Fornitore	P.I/C.F.	Importo proroga fino al 30/6/2022 (IVA esclusa)
LEONARDO S.P.A. Divisione Cyber con sede in Piazza Monte Grappa n. 4 Roma	P.IVA 00881841001 c.f 00401990585	26.532,00

- che per la proroga si conferma il medesimo CIG derivato identificativo della fornitura principale (CIG Master 5518849A42 - CIG Derivato 7300627BFA);

RITENUTO:

- di procedere, per i motivi suddetti, alla proroga fino al 30/6/2022, del Contratto Esecutivo (recante il n. PGDG/2021/13573 del 13/12/2017) discendente dall'Accordo Quadro denominato SPC - Lotto 2 del 20/07/2016 (CIG master 5518849A42) stipulato da Consip Spa con il RTI Aggiudicatario, composto dalle aziende Leonardo-Finmeccanica S.p.a. nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti IBM Italia S.p.A., FASTWEB S.p.A. e Sistemi Informativi S.r.l., aggiudicato da ARPAE con determina n. 983 del 4/12/2017, come da Progetto dei fabbisogni Identificativo (GOV-210273 Rev 1 del 14/07/2021) (Cig Derivato 7300627BFA, per l'importo complessivo di euro 26.532,00 (iva esclusa);

DATO ATTO

- che la verifica di conformità, di cui all'art. 102 del d. lgs. 50/2016, sarà svolta al termine dell'esecuzione del contratto prorogato;
- che non sono stati rilevati rischi da interferenze, pertanto non è necessario procedere, prima della sottoscrizione del contratto, alla redazione del DUVRI ai sensi dell'art. 26 del D.Lgs.81/2008;

ATTESTATO:

- ai fini dell'art. 9 del d.l. n. 78 dell'1 luglio 2009 "Tempestività dei pagamenti delle

pubbliche amministrazioni" (convertito nella legge 3 agosto 2009 n. 102), che il presente atto è assunto nel rispetto delle disposizioni e dei limiti di cui alla D.D.G. n. 99/09, confermate con riferimento alla programmazione di cassa nell'Allegato A della D.D.G. 139/2020;

- la regolarità amministrativa del presente atto;

DATO ATTO :

- che ai sensi dell'art. 3 del Regolamento per la disciplina dei contratti pubblici di servizi e forniture vigente in Arpae, il dott. Stefano Cattani, Responsabile del Servizio Sistemi Informativi e Innovazione Digitale, è il Responsabile Unico del Procedimento,
- che è stato acquisito il parere di regolarità contabile espresso ai sensi del Regolamento sull'adozione degli atti di gestione delle risorse dell'agenzia approvato con D.D.G. n. 109 del 31/10/2019 e revisionato dalla D.D.G. n. 114 del 23/10/2020, dal Servizio Amministrazione Bilancio e Controllo economico nella persona del dott. Antenucci Alessandro, titolare di incarico di funzione di Unità di Budget, Controllo Economico e Fatture/Fornitori;

DETERMINA

1. di procedere, per i motivi suddetti, alla proroga fino al 30/6/2022, del Contratto Esecutivo (recante il n. PGDG/2021/13573 del 13/12/2017) discendente dall'Accordo Quadro denominato SPC - Lotto 2 del 20/07/2016 (CIG 5518849A42) stipulato da Consip Spa con il RTI Aggiudicatario, composto dalle aziende Leonardo-Finmeccanica S.p.a. nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti IBM Italia S.p.A., FASTWEB S.p.A. e Sistemi Informativi S.r.l., aggiudicato da ARPAE con determina n. 983 del 4/12/2017, come da Progetto dei fabbisogni Identificativo (GOV-210273 Rev 1 del 14/07/2021), che si allega al presente atto, per l'importo complessivo di euro 26.532,00 (iva esclusa);
2. di dare atto che la verifica di conformità, di cui all'art. 102 del d. lgs. 50/2016, sarà svolta al termine dell'esecuzione del contratto rinnovato;
3. di dare atto che il costo complessivo derivante dal presente provvedimento, stimato in euro 32.369,04 (IVA inclusa), avente natura di "Servizi Informatici", è a carico del budget annuale relativo all'esercizio 2021 e del bilancio economico preventivo pluriennale 2021-2023 con riferimento al centro di costo del Servizio Sistemi Informativi e Innovazione Digitale relativamente al

- esercizio 2021 per euro 20.297,20;
- esercizio 2022 per euro 12.071,84

4. di dare atto che il presente provvedimento è soggetto agli obblighi di trasparenza di cui all'art. 29 del d.lgs. 50/2016, ed è a tal fine pubblicato sul sito dell'Amministrazione.

Il Responsabile del Servizio Sistemi Informativi e Innovazione Digitale

dott. Stefano Cattani

Firmato digitalmente da
claudio rando
Data e ora della firma: 14/07/2021 11:40:13

14-07-2021
LDO/CYS/P/0028977/21

Identificativo: GOVM-210273 Rev 1

Data: 14/07/2021

PROCEDURA RISTRETTA PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ON-LINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI (ID SIGEF 1403)

LOTTO 2

ARPAE

Progetto dei fabbisogni

Costituendo
Raggruppamento Temporaneo di Imprese
composto da:
Leonardo SpA - Divisione Cyber Security
IBM SpA
Sistemi Informativi srl
Fastweb SpA

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

Le informazioni contenute nel presente documento sono di proprietà di Leonardo Società per Azioni, IBM Società per Azioni, Sistemi Informativi Società a responsabilità limitata, Fastweb Società per Azioni e non possono, al pari di tale documento, essere riprodotte, utilizzate o divulgate in tutto o in parte a terzi senza preventiva autorizzazione scritta delle citate aziende.

<Livello di Classificazione>

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

	Nome e Ruolo	Firma
Autore		
	Antonio Recchilongo	
	Stefano Sciocchetti	
Verifica		
	Germano Matteuzzi	
Approvazione		
	Giuseppe Nicastro	
Autorizzazione		

Approvazioni Aggiuntive

Azienda	Nome e Ruolo	Firma

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda
1	Vedi data di copertina	ARPAE	RTI

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autori
1	Vedi data di copertina	Prima Emissione	RTI

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

SOMMARIO

1 INTRODUZIONE 6
1.1 Ambito 6
1.2 Struttura del documento 6
1.3 Richieste dell'Amministrazione contraente 8
2 Riferimenti 9
2.1 Documenti Applicabili 9
2.2 Documenti di Riferimento 9
3 Definizioni e acronimi 10
3.1 Definizioni 10
3.2 Acronimi 11
4 Dati anagrafici amministrazione contraente 14
5 Proposta tecnico-economica 15
5.1 Servizio L2.S2.1 – Firma Digitale Remota 15
5.1.1 OBIETTIVI DEL SERVIZIO L2.S3.4 15
5.1.2 DESCRIZIONE DEL SERVIZIO L2.S3.4 15
5.1.3 FUNZIONALITÀ DEL SERVIZIO L2.S3.4 17
5.1.4 ARCHITETTURA DI RIFERIMENTO 18
5.1.5 VINCOLI E ASSUNZIONI DEL SERVIZIO L2.S3.4 20
5.1.6 COMPONENTI DEL SERVIZIO L2.S3.4 21
5.1.7 MODALITÀ DI EROGAZIONE DEL SERVIZIO L2.S3.4 22
5.1.8 QUANTITÀ E PREZZI DEL SERVIZIO L2.S3.4 23
5.1.9 ATTIVAZIONE DEL SERVIZIO L2.S3.4 23
5.2 Requisiti di installazione in carico all'amministrazione 23
5.3 Servizio L2.S3.8 – Secure Web Gateway 24
5.3.1 DESCRIZIONE DEL SERVIZIO 24
5.3.2 ARCHITETTURA DELLA SOLUZIONE 24
5.3.3 DEPLOYMENT DELLA SOLUZIONE E EROGAZIONE DEL SERVIZIO 24
5.3.4 VINCOLI E ASSUNZIONI DEL SERVIZIO 25
5.3.5 COSTI DEL SERVIZIO 25
5.3.6 Servizio di supporto all'infrastruttura del servizio di Firma Digitale Remota – SP.01 25
6 Riservatezza 27
Appendice A Progetto di attuazione 28
A.1 Struttura organizzativa 28
A.2 Quantità e costi 29
A.2.1 Fatturazione SP01-L2.S3.9 29
Appendice B Piano di lavoro 30
B.1 Inizio e durata dei servizi 30
B.1.1 DLP / SWG ..... **Errore. Il segnalibro non è definito.**

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

LISTA DELLE TABELLE

Tabella 1: Documenti applicabili. 9
Tabella 2: Documenti di riferimento. 9
Tabella 3: Definizioni valide per il presente documento. 11
Tabella 4: Lista degli acronimi. 11
Tabella 5: Dati anagrafici dell'Amministrazione contraente. 14
Tabella 6: Dati anagrafici del referente dell'Amministrazione contraente. 14
Tabella 9: Figure professionali. 28
Tabella 10: Quantità e costi. 29
Tabella 11: Piano di attivazione. 30

LISTA DELLE FIGURE

Figura 1 Struttura del Progetto dei Fabbisogni 7

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

1 INTRODUZIONE

Nel dicembre 2013 CONSIP ha bandito una procedura ristretta, suddivisa in quattro lotti, per l'affidamento dei "servizi di Cloud Computing, di Sicurezza, di Realizzazione di Portali e Servizi on-line e di Cooperazione Applicativa per le Pubbliche Amministrazioni - (ID SIGEF 1403)" nota come Gara SPC Cloud. Il Lotto 2, inerente i Servizi di Identità Digitale e Sicurezza Applicativa, è stato assegnato al Raggruppamento la cui mandataria è Leonardo S.p.A. e le società mandanti sono IBM, Sistemi Informativi e Fastweb.

La durata del contratto è di cinque anni. Nell'arco di tale periodo ogni Pubblica Amministrazione potrà acquisire i servizi offerti dalle "Convenzioni" tramite la stipula di "Contratti Esecutivi" dimensionati tecnicamente in un Piano dei fabbisogni prodotto in base alle proprie esigenze. Il presente Progetto dei Fabbisogni viene emesso in virtù dell'Addendum nr. 4 al Contratto Quadro DA.[1] sottoscritto tra Consip ed il RTI in data 26/3/2021 dove il Contratto Quadro viene prorogato di ulteriori 12 (dodici) mesi sino alla scadenza al 20 luglio 2022, ai fini di consentire all'Ente la continuità dei servizi fruiti fino ad oggi e per adeguare la necessità di innalzamento della sicurezza dei servizi informatici.

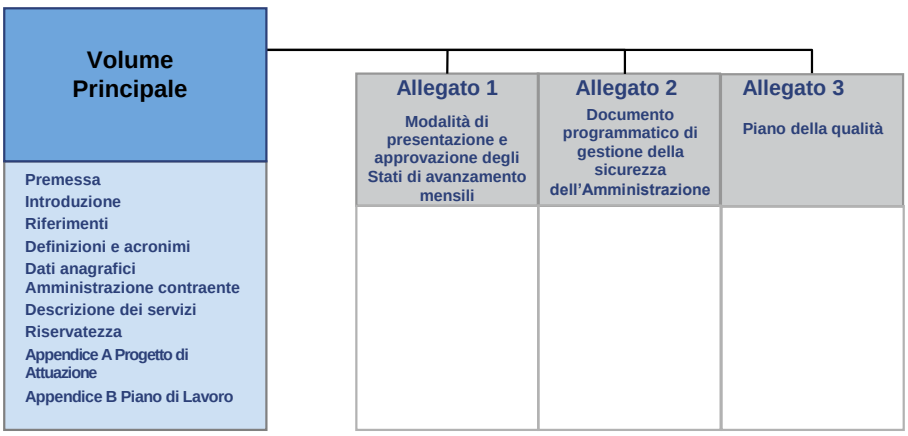
Il presente documento costituisce il progetto dei fabbisogni che comprende l'insieme di servizi e di infrastrutture tecnologiche dedicate alla sicurezza dei sistemi informativi preposti al trattamento dei dati della Pubblica Amministrazione (PA), in conformità alle esigenze dell'Amministrazione stessa espresse attraverso il proprio piano di fabbisogni. Esso raccoglie e dettaglia le richieste di ARPAE (indicata nel documento come Amministrazione contraente) contenute nel proprio Piano dei fabbisogni [DA-5] e descritte sinteticamente in §1.3. Successivamente si formula una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro "Servizi di gestione delle identità digitali e sicurezza applicativa" e nei relativi allegati.

1.1 Ambito

Il presente documento costituisce il progetto dei fabbisogni che comprende l'insieme di servizi e di infrastrutture tecnologiche dedicate alla sicurezza dei sistemi informativi preposti al trattamento dei dati della Pubblica Amministrazione (PA), in conformità alle esigenze dell'Amministrazione stessa espresse attraverso il proprio piano di fabbisogni. Esso raccoglie e dettaglia le richieste pervenute da RAI (indicata nel documento come Amministrazione contraente) contenute nel proprio Piano dei fabbisogni [DA-5] e descritte sinteticamente in §1.3. Successivamente si formula una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro "Servizi di gestione delle identità digitali e sicurezza applicativa" e nei relativi allegati.

1.2 Struttura del documento

Il contenuto del Progetto dei Fabbisogni rispetta quanto definito dai requisiti del Capitolato dell'Accordo Quadro. Di seguito il dettaglio della composizione e dei contenuti.



Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

Figura 1 Struttura del Progetto dei Fabbisogni

Volume principale	Raccolta delle richieste dell'Amministrazione contraente, contenute nel Piano dei Fabbisogni, in termini di dettaglio e formulazione della proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro e nei relativi allegati.
Appendice A, Progetto di attuazione	Per ciascun servizio, richiesto dal Piano dei fabbisogni, l'appendice A contiene i seguenti dettagli: identificativo del servizio; configurazione (ove applicabile); quantità; costi; indirizzo/i di dispiegamento (nel caso di servizi centralizzati si riporterà il solo indirizzo della sede centrale); data prevista di attivazione; impegno delle eventuali risorse professionali previste; descrizione della struttura funzionale ed organizzativa del centro servizi, completa dei nomi e dei ruoli delle figure responsabili per ciascuno dei servizi, nonché delle relative procedure di escalation; specifiche di collaudo, contenenti le modalità di esecuzione dei test di collaudo, descritti tramite schede tecniche di dettaglio e le date di prevista disponibilità al collaudo.
Appendice B, Piano di lavoro	Contiene l'elenco delle attività/fasi previste per l'erogazione dei servizi richieste con le relative date di inizio e fine. Tutte la fasi previste dal piano indicano gli obiettivi, i tempi necessari comprensivi delle date da garantire, i deliverables prodotti e le date di consegna. Sarà fornita, inoltre, e solo se richiesto, una descrizione dettagliata delle attività e procedure che il RTI metterà in atto nell'eventuale processo di subentro dei servizi al fine di minimizzare l'impatto sull'operatività dei servizi erogati.
Allegato 1, Modalità di presentazione e approvazione degli Stati di avanzamento mensili	Documento che definisce modi e tempi di presentazione dello stato di avanzamento lavori. Tale documento sarà fornito entro 20 giorni dalla richiesta dell'Amministrazione contraente e recepirà eventuali indicazioni contenute nel contratto esecutivo.
Allegato 2, Documento programmatico di gestione della sicurezza dell'Amministrazione	Documento descrittivo delle linee guida progettuali per la determinazione delle misure di sicurezza minime e idonee per la protezione dei dati informatici e dei relativi flussi (trattamento), in ottemperanza alle normative vigenti. Tale documento potrà essere consegnato, previa richiesta delle amministrazioni, entro 20 gg. a far data della richiesta stessa e comunque secondo le norme previste dal livello di classifica imposto.
Allegato 3, Piano della qualità	Contiene gli obiettivi di qualità e la descrizione delle modalità di esecuzione dei servizi previsti e ne costituisce il riferimento esecutivo: definisce, infatti, le modalità di applicazione del Sistema di Gestione per la Qualità alla fornitura, come pure le eventuali deroghe per garantire flessibilità e accuratezza delle modalità di erogazione dei servizi e delle verifiche da porre in atto al fine di garantire il soddisfacimento dei requisiti del Committente. Il Piano di Qualità del Contratto Esecutivo sarà emesso, ad integrazione del Piano di Qualità Generale, entro 30 gg dalla notifica del contratto.

= questo documento

Company General Use

1.3 Richieste dell'Amministrazione contraente

In questa sezione del Progetto dei fabbisogni l'RTI intende raccogliere e dettagliare le richieste dell'Amministrazione contraente espresse tramite la redazione del Piano dei fabbisogni [DA-5], contenente per ciascuna categoria di servizi indicazioni di tipo quantitativo che la stessa intende sottoscrivere.

Il RTI ha ricevuto a mezzo PEC il Documento Piano dei fabbisogni [DA-5], trasmesso da ARPAE con cui l'ente pubblico ha manifestato l'esigenza e la richiesta di fornitura di specifici servizi di:

- L2.S2.1 – Firma Digitale Remota
- L2.S3.8 – Secure Web Gateway
- L2.S3.9 – Servizio di supporto all'infrastruttura del servizio di Firma Digitale Remota

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

2 RIFERIMENTI

2.1 Documenti Applicabili

Tabella 1: Documenti applicabili.

Rif.	Codice	Titolo
DA-1.	--	Capitolato Tecnico – Parte Generale "Procedura ristretta, suddivisa in 4 lotti, per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)"
DA-2.	--	Capitolato Tecnico – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)"
DA-3.	--	Offerta Tecnica – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)" del 22 Dicembre 2014
DA-4.	--	Contratto Quadro – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)" del 20/07/2016
DA-5.		"Piano dei Fabbisogni" – *emesso da ARPAE a mezzo PEC in data 25/06/2021*
DA-6.		Allegato 1 – Listino prezzi - http://www.spc-lotto2-sicurezza.it/
DA-7.	EP4A56001Q01	Piano di Qualità Generale – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)"

2.2 Documenti di Riferimento

Tabella 2: Documenti di riferimento.

Rif.	Codice	Titolo
DR-1.		Guida al Contratto Quadro "Servizi di gestione delle identità digitali e sicurezza applicativa" - http://www.spc-lotto2-sicurezza.it/
DR-2.		Allegato 3 – Schema Progetto dei fabbisogni - http://www.spc-lotto2-sicurezza.it/

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

3 DEFINIZIONI E ACRONIMI

3.1 Definizioni

La seguente Tabella 3riporta tutte le definizioni adottate nel presente documento.

Amministrazioni	Pubbliche Amministrazioni.
Amministrazione aggiudicatrice	Consip.
Amministrazione/i Contraente/i	Pubbliche Amministrazioni che hanno siglato un Contratto di Fornitura con il Fornitore per l'erogazione di uno dei servizi in ambito dell'Accordo Quadro.
Centro di Registrazione Locale	È una Società, Ente o Pubblica Amministrazione che viene autorizzata dalla Certification Authority Aruba PEC S.p.A. ad emettere in maniera autonoma i certificati di Firma digitale.
Certificato qualificato	Un certificato qualificato è l'insieme di informazioni che creano una stretta ed affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. Sono certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.
Certificatore accreditato	Un certificatore accreditato, in virtù dell'autorizzazione ottenuta da AgID, ha il compito di garantire l'identità dei soggetti che intendono dotarsi ed utilizzare la firma digitale. AgID svolge attività di vigilanza sui certificatori accreditati.
Chiave privata	La chiave privata è l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.
Chiave pubblica	La chiave pubblica è l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.
Firma digitale	La firma digitale è un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Firma digitale remota	La firma digitale remota è una tipologia di firma digitale, accessibile remotamente tramite il supporto di una rete di comunicazione (sia essa Intranet e/o Internet), nel quale la chiave privata del firmatario viene conservata assieme al certificato di firma, all'interno di un server remoto sicuro (basato su un HSM) da parte di un certificatore accreditato.
Firma elettronica avanzata	La firma elettronica avanzata è l'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

	sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Fornitore	Vedi Raggruppamento
Modalità “As a Service”	Servizio erogato da remoto attraverso i Centri Servizi dell’RTI.
Modalità “On premise”	Servizio erogato presso le strutture dell’Amministrazione contraente o altre strutture indicate dalla stessa.
Raggruppamento	Raggruppamento Temporaneo di Impresa Il RTI Divisione Sistemi per la Sicurezza e le Informazioni S.p.A. (nel seguito Il RTI), società mandataria, IBM S.p.A. (mandante), Sistemi Informativi S.p.A. (mandante) e Fastweb S.p.A. (mandante).

Tabella 3: Definizioni valide per il presente documento.

3.2 Acronimi

La seguente Tabella 4 riporta tutte le abbreviazioni e gli acronimi utilizzati nel presente documento.

Tabella 4: Lista degli acronimi.

ACL	Access Control List
AgID	Agenzia per Italia Digitale
API	Application Programming Interface
ARSS	Aruba Remote Sign Server
BI	Business Intelligence
CA	Certification Authority
CAD	Codice dell’Amministrazione Digitale
CAdES	CMS Advanced Electronic Signatures
CE	Contratto Esecutivo
CED	Centro Elaborazione Dati
CMS	Card Management System
CQ	Contratto Quadro
CRL	Certificate Revocation List
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic Application Security Testing
DLP	Data Loss Prevention
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

IAM	Identity & Access Management
IR	Incaricati alla Registrazione
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance
MAST	Mobile Application Security Testing
OCSP	Online Certificate Status Protocol
ODR	Operatori di Registrazione
OTP	One Time Password
PA	Pubblica Amministrazione
PAdES	PDF Advanced Electronic Signatures
PC	Personal Computer
PDF	Portable Document Format
PDP	Policy Decision Point
PEC	Posta Elettronica Certificata
PEP	Policy Enforcement Point
RA	Registration Authority
REST	REpresentational State Transfer
RFC	Request for Comments
RPO	Recovery Point Objective
RTI	Raggruppamento Temporaneo di Imprese
RTO	Recovery Time Objective
SAL	Stato Avanzamento Lavori
SAST	Static Application Security Testing
SPC	Sistema Pubblico di Connettività
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPID	Sistema Pubblico di Identità Digitale
SSO	Single Sign On
TSD	Time Stamped Data
TSR	Time Stamp Response
URL	Uniform Resource Locator
VA	Vulnerability Assessment
WS	Web Service
XAdES	XML Advanced Electronic Signatures

Company General Use

XML	eXtensible Markup Language

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

4 DATI ANAGRAFICI AMMINISTRAZIONE CONTRAENTE

Nelle seguenti tabelle si riportano i dati anagrafici dell'Amministrazione contraente (cfr. Tabella 5) e del suo referente (cfr. Tabella 6).

Tabella 5: Dati anagrafici dell'Amministrazione contraente.

Ragione sociale Amministrazione	ARPAE
Indirizzo	Via Po, 5
CAP	40139
Comune	Bologna
Provincia	BO
Regione	Emilia Romagna
Codice Fiscale	04290860370
Codice IPA	arpa
Nominativo referente Contratto Esecutivo:	Dott. Stefano Cattani
Indirizzo mail	dirgen@cert.arpa.emr.it
PEC (SI/NO)	SI

Tabella 6: Dati anagrafici del referente dell'Amministrazione contraente.

Nome	Stefano
Cognome	Cattani
Telefono fisso	320 6198714
Indirizzo mail	scattani@arpae.it
PEC (SI/NO)	NO

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

5 PROPOSTA TECNICO-ECONOMICA

5.1 Servizio L2.S2.1 – Firma Digitale Remota

La "Firma Digitale Remota" è una modalità innovativa di Firma Digitale che, pur garantendo lo stesso grado di sicurezza e gli stessi effetti di legge della tradizionale Firma Digitale basata su Smart Card o token USB, rispetto a quest'ultima offre diversi vantaggi specifici:

- Non richiede l'installazione di hardware o software dedicato, pertanto riduce virtualmente a zero i relativi problemi di incompatibilità HW/SW, supporto tecnico, ecc.;
- E' sostanzialmente indipendente dall'ambiente operativo dell'utente (Windows, Mac, Linux);
- Permette di generare Firme Digitali in ogni momento ed in ogni luogo mediante una semplice connessione internet.

In concreto, con "Firma Digitale Remota" si intende la Firma Digitale apposta con una chiave privata non residente su un dispositivo personale dell'utente, quale ad es. una Smart Card, bensì su un dispositivo remoto (solitamente un HSM).

I documenti firmati tramite Firma Digitale Remota garantiscono:

- **Integrità:** sicurezza che il documento informatico non è stato modificato dopo la sua sottoscrizione;
- **Autenticità:** con un documento firmato digitalmente si può essere certi dell'identità del sottoscrittore;
- **Non ripudio:** il documento informatico sottoscritto con firma digitale, ha piena validità legale e non può essere ripudiato dal sottoscrittore;
- **Valore legale:** il documento elettronico sottoscritto digitalmente ha lo stesso valore legale di un documento cartaceo sottoscritto con firma autografa.

Le Firme Digitali Remote sono rilasciate secondo la normativa vigente (Regolamento UE 910/2014 eIDAS.).

5.1.1 OBIETTIVI DEL SERVIZIO L2.S3.4

L'impiego della firma digitale, pertanto, permette di snellire significativamente i rapporti tra l'Amministrazione contraente, i cittadini o le imprese, riducendo drasticamente la gestione in forma cartacea dei documenti, pur continuando a garantire al documento informatico, cui è apposta una firma digitale, le caratteristiche oggettive di qualità, sicurezza, integrità e non modificabilità.

Il servizio di Firma digitale remota consente all'Amministrazione contraente la sottoscrizione di documenti digitali e relativa verifica (quest'ultima anche per la marcatura temporale) in condizioni di massima sicurezza, ma senza l'utilizzo di una smart card o di un qualunque altro dispositivo personale e l'installazione di un hardware dedicato (come per esempio i lettori di smart card); il tutto nel pieno rispetto delle norme stabilite dal Codice dell'Amministrazione Digitale (CAD).

5.1.2 DESCRIZIONE DEL SERVIZIO L2.S3.4

Il servizio di Firma digitale remota è utilizzabile mediante un portale messo a disposizione dal RTI all'Amministrazione contraente, i cui utenti hanno la possibilità di firmare documenti tramite un browser, senza dover installare nulla sulle loro postazioni di lavoro. Il portale, inoltre, è formato da un insieme di strumenti che consentirà di attivare e gestire il ciclo di vita del servizio di firma digitale remota/automatica e dei relativi certificati digitali. Il portale è ospitato da una data center dell'RTI attraverso una piattaforma condivisa, configurata in modalità HA nativa con due CED primari in area metropolitana (per garantire la Business Continuity) e DR geografico (con RPO e RTO pari a 4 ore).

Gli utenti dovranno autenticarsi inserendo le proprie credenziali (user e password). L'uso di credenziali di autenticazione forte (in cui il secondo fattore è un OTP rilasciato mediante token o app per smartphone) è necessario solo per le operazioni di inserimento della firma digitale.

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

È comunque possibile, per le operazioni di firma e verifica, istallare sulle postazioni di lavoro informatizzate (pdl) delle amministrazioni un client Software. L'istallazione di tale Software, disponibile tramite download dal portale del fornitore, è a cure delle Amministrazioni stesse.

L'Amministrazione contraente potrà integrare i propri applicativi col sistema di firma remota attraverso l'invocazione di web services (WS) con protocollo SOAP. Allo scopo sarà realizzato presso il Centro Servizi dell'RTI un servizio di Integrazione Applicativa per le soluzioni di Firma Remota, denominato ARSS (Aruba Remote Sign Server) che consente all'Amministrazione contraente di integrare il sistema di firma remota con i propri applicativi o di utilizzarla direttamente da interfaccia web tramite il portale. Poiché le applicazioni dell'Amministrazione contraente sono ospitate in infrastrutture IT diverse da quella dove risiede il sistema di Firma Digitale Remota di Aruba, il componente ARSS provvede a dialogare su canale sicuro HTTPS con i Sistemi della Certification Authority di Aruba limitatamente per l'invio delle richieste di generazione di certificati alla Certification Authority e all'eventuale verifica dei file sottoscritti con certificati Aruba.

Per il resto il modulo ARSS espone verso le applicazioni in questione le funzionalità di firma digitale necessarie ad espletare le seguenti operazioni:

- firma di un documento in formato CAdES;
- firma di un documento in formato PDF;
- firma di tutti i documenti contenuti in una cartella specificata (ovvero la firma digitale automatica massiva), sia in formato CAdES che PDF; per lo svolgimento di questa particolare funzionalità sarà installato presso l'Amministrazione contraente un componente software per il calcolo dell'hash di ciascun documento, in modo da garantire il corretto throughput e potere usufruire adeguatamente del servizio; sarà l'hash ad essere scambiato dall'Amministrazione contraente verso il Centro Servizi dell'RTI e sarà questo ad essere firmato e restituito all'Amministrazione contraente;
- firma di un hash, nel caso in cui le applicazioni provvedano autonomamente alla creazione del documento firmato digitalmente;
- marcatura temporale di un documento.

Nel caso di operazioni relative alla verifica della marcatura temporale, ARSS si interfaccia direttamente con i servizi standard che erogano la Time Stamping Authority di Aruba PEC; la componente dedicata alla validazione effettua direttamente tutte le verifiche interrogando i servizi esterni necessari delle CA coinvolte nella verifica. Si tratta dei servizi implementati dal modulo di validation authority:

- **CA certificate store**, i certificati contenuti in quest'archivio possono essere utilizzati per creare una catena di certificati che consente di risalire a un certificato di autorità di certificazione dell'archivio, in modo tale da poter verificare che il certificato sia firmato da una CA valida.
- **CRL store**, archivio utilizzato per ospitare un Certificate Revocation List (ossia una lista firmata di certificate revocati) di una CA.
- **OCSP responder**, utilizzato per chiedere tramite il protocollo OCSP se un certificato è revocato o meno.

Tutte le suddette funzionalità sono realizzate da un server sicuro (HSM, Hardware Secure Module) dislocato nel Centro Servizi del RTI, che centralizza e integra le funzioni di firma. Si tratta della soluzione CoSign di Arx che, oltre a elaborare la richiesta e rinviare all'applicazione il documento con la firma digitale integrata, conserva tutte le chiavi private degli utenti esclusivamente all'interno del modulo HSM, che costituisce un perimetro di sicurezza certificato. Inoltre, il software di firma digitale CoSign funziona con qualsiasi applicativo ed è in grado di gestire i più comuni formati di documento per mezzo di uno strato software di gestione di tutte le richieste da e verso gli HSM (HSM Signature Middleware) che si frappone tra il modulo ARSS e l'HSM.

Se si preferisce, è possibile anche, in alternativa al portale, utilizzare il client Aruba, installabile su postazioni di lavoro con sistema operativo Microsoft. Tale software è scaricabile dal sito del fornitore e l'istallazione sarà a cura dell'Amministrazione.

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

A supporto della gestione delle fasi necessarie all'attivazione del servizio di Firma elettronica remota, sarà utilizzato all'interno del Centro servizi del RTI un sistema di provisioning. Si tratta di un modulo software che s'interfaccia con i sistemi per la verifica delle credenziali di attivazione, gestendo e orchestrando il dialogo tra le componenti, fra le quali l'HSM Cosign per la creazione degli account (laddove richiesto) e la Certification Authority di Aruba per la generazione dei certificati digitali.

5.1.3 FUNZIONALITÀ DEL SERVIZIO L2.S3.4

In questo paragrafo sono descritte le principali funzionalità messe a disposizione dell'Amministrazione contraente che necessità di usufruire del servizio di Firma digitale remota.

5.1.3.1 Attivazione dell'account di firma remota, firma remota automatica e firma remota verificata

L'attivazione della firma remota è il processo che consente all'utente finale di ottenere un account di firma remota (o un account di firma automatica o verificata) attivo, completo delle credenziali "user", "password" e del token necessario alla generazione delle One Time Password. Questo processo si sviluppa attraverso le seguenti attività: accesso al portale di emissione attraverso la sezione apposita ed effettuazione della registrazione della richiesta; assegnazione delle credenziali immateriali; attivazione dell'account tramite assegnazione di nome utente ed OTP fisico.

5.1.3.2 Gestione dell'account di firma remota, firma remota automatica e firma remota verificata

Questo processo consente al titolare la gestione dell'account di firma remota in modalità self-provisioning, attraverso le apposite pagine messe a disposizione dal portale. Le stesse operazioni potranno essere effettuate anche per account di firma remota automatica e verificata. Le operazioni di gestione dell'account di firma remota includono: cambio della password associata all'utenza di firma remota; recupero della password associata all'utenza di firma remota; recupero della username associata all'utenza di firma remota. Ogni caso prevede il riconoscimento dell'utente attraverso più credenziali associate all'account di firma.

5.1.3.3 Gestione dell'account di firma remota, firma remota automatica e firma remota verificata

Questo processo consente al titolare la gestione dell'account di firma remota in modalità self-provisioning, attraverso le apposite pagine messe a disposizione dal portale. Le stesse operazioni potranno essere effettuate anche per account di firma remota automatica e verificata. Le operazioni di gestione dell'account di firma remota includono: cambio della password associata all'utenza di firma remota; recupero della password associata all'utenza di firma remota; recupero della username associata all'utenza di firma remota. Ogni caso prevede il riconoscimento dell'utente attraverso più credenziali associate all'account di firma.

5.1.3.4 Gestione del ciclo di vita della firma remota, firma remota automatica e firma remota verificata

Questo processo consente la gestione del ciclo di vita delle firme digitali remote attivate via portale, tramite le apposite funzioni messe a disposizione dal portale stesso e fruibili dall'operatore. Le operazioni possibili (valide anche e soprattutto per la firma automatica massiva) sono: sospensione; riattivazione; revoca.

5.1.3.5 Apposizione della firma remota (verificata) tramite portale web e webservice

Questo processo consente al titolare di utilizzare la propria firma remota (verificata) tramite le apposite funzioni messe a disposizione dal portale. L'operazione di firma richiede: individuazione del file da firmare; inserimento credenziali statiche (username e password) relative all'account di firma remota; inserimento della credenziale dinamica (OTP). A questo punto il sistema consente l'apposizione di firme nelle seguenti modalità: CAdES (CMS Advanced Electronic Signature); PAdES (PDF Advanced Electronic Signature); XAdES (XML Advanced Electronic Signature); firma multipla (firma di file già sottoscritto). Un processo del tutto analogo consente l'apposizione della firma remota e della firma remota verificata dai webservice esposti dalla componente di remotizzazione ARSS.

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

5.1.3.6 Verifica della firma digitale verificata tramite portale web e webservice

Questo processo consente all'utente di effettuare la verifica di file firmati digitalmente con firma di tipo verificata. Le operazioni sono consentite tramite apposita funzione esposta dal portale web, attraverso il quale si esegue l'upload del file firmato e si convalida la richiesta. Per la verifica sullo stato di validità dei certificati (attivo, sospeso, revocato) il portale invoca via web le Certification List della CA di riferimento. Un analogo processo è applicabile alla verifica di file firmati tramite invocazione di webservice, consentendo dunque l'integrazione applicativa della funzione. I casi inclusi dal processo di Verifica firma digitale da webservice sono: firma Cades; firma Pades; firma Xades.

5.1.3.7 Verifica della marca temporale dei documenti tramite portale web e webservice

Questo processo consente all'utente di effettuare la verifica dei file (firmati o non firmati) marcati temporalmente, tramite upload degli stessi nell'apposita sezione esposta dal portale. Sono supportati i formati di marcatura temporale Time Stamp Response (TSR) definito dallo standard RFC 3161 e quello più recente Time Stamped Data (TSD) definito dallo standard RFC 5544.

5.1.4 ARCHITETTURA DI RIFERIMENTO

Di seguito nel prosieguo del paragrafo è descritta l'architettura utilizzata e le componenti Hardware e Software utilizzate per l'erogazione del servizio.

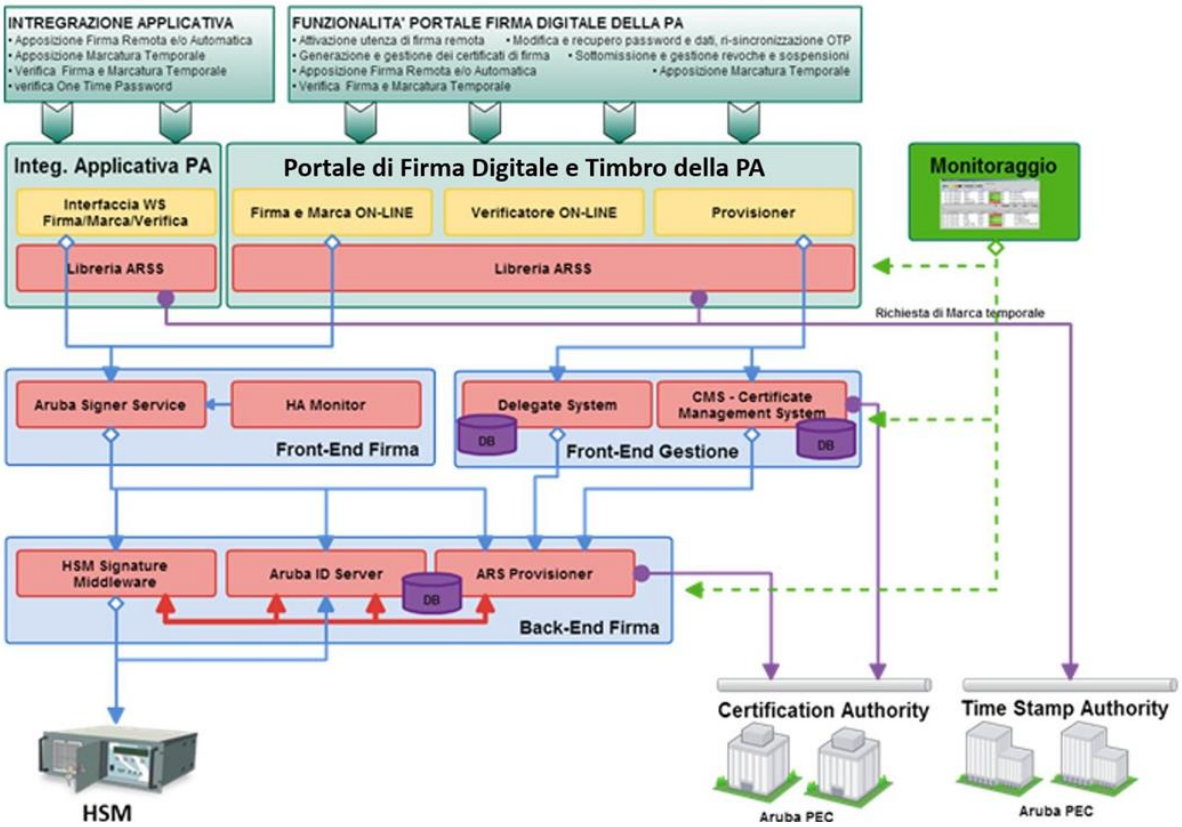


Figure 1 - Architettura software del servizio di Firma digitale remota

Nello schema si evidenziano le componenti base dell'architettura:

- **Hardware Security Module (HSM)** – Componente hardware all'interno del quale sono generate e custodite le chiavi ed i certificati digitali. Le caratteristiche dell'HSM utilizzate sono riportate nel paragrafo 6.1.2.3.
- **ARS Provisioner** – Componente software che, verificate le credenziali di attivazione, gestisce (orchestra) il dialogo con gli HSM, con il Sistema di Autenticazione e con la Certification Authority per la corretta attivazione del Servizio.

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

- **Back End di Firma** – il Sistema di Autenticazione è formato da varie componenti logiche che s'interfacciano con gli HSM CoSign e che gestiscono l'autenticazione del Titolare per lo sblocco delle operazioni crittografiche sull'HSM.
- **HSM Signature Middleware** – componente software di gestione di tutte le richieste da e verso gli HSM.
- **CMS, Card Management System** – Pannello di Amministrazione che permette la creazione e la gestione delle utenze autorizzate a firmare con il certificato digitale proprio o dello specifico Titolare (delega), l'assegnazione delle credenziali, la richiesta di generazione del certificato. Il pannello consente la creazione anche degli Utenti delegati ed il censimento delle applicazioni autorizzate ad accedere alle funzionalità di firma automatica.
- **Libreria ARSS** – libreria alla quale vengono demandate tutte le operazioni crittografiche necessarie all'apposizione della firma digitale. Tale libreria espone tutte le funzionalità di firma rese disponibili dalle interfacce di firma (BBF e WS). È il componente che sarà installato presso il Datacenter dell'amministrazione.

Nello schema si evidenziano anche le interfacce disponibili all'Amministrazione contraente:

- **interfaccia di firma**, implementata dal componente software di Front-End Aruba Remote Signing Server (ARSS) installato tipicamente presso la sede dell'Amministrazione contraente o comunque in LAN con le applicazioni che richiedono servizi di firma automatica;
- **interfaccia di Amministrazione** per la gestione delle utenze e delle deleghe, il cui funzionamento è descritto nel presente documento
- **interfaccia della Certification Authority (CA)** per poter gestire il ciclo di vita del certificato.

Nella soluzione proposta, tutte le componenti hardware e software sono installate presso i centri servizi del RTI o, limitatamente all'interfaccia di front-end (Aruba Remote Signing Server – ARSS), presso la sede dell'Amministrazione contraente.

La soluzione è predisposta, sul sito di produzione, con più nodi che lavorano in alta affidabilità, utilizzando una particolare architettura active-active sviluppata per garantire in ogni situazione la coerenza della firma ed il rispetto della normativa vigente. Il sistema è costantemente controllato da un apposito strumento di monitoraggio, implementato direttamente dalla componente HA Monitor, che consente di verificare la regolare operatività del sistema da parte del RTI e di segnalare tempestivamente il verificarsi di anomalie hardware o applicative.

5.1.4.1 Caratteristiche tecnico-funzionali

La Soluzione di Firma Digitale utilizzata, per mezzo del componente ARSS che espone le interfacce applicative garantisce, conformemente a quanto previsto dalla normativa vigente, le seguenti caratteristiche:

- firma di un documento in formato CADES-BES e CADES-T (secondo quanto previsto dalla Deliberazione 45/2009 e successiva Determina 69/2010)
- firma di un documento in formato PADES-Basic, PADES-BES e PADES-T (secondo quanto previsto dalla Deliberazione 45/2009 e successiva Determina 69/2010)
- firma di un documento in formato XADES-BES e XADES-T (secondo quanto previsto dalla Deliberazione 45/2009 e successiva Determina 69/2010)
- firme multiple (parallele e controfirme)
- firme multiple in modalità "matrioska"
- firma detached
- firma di un hash (impronta), nel caso in cui le applicazioni provvedano autonomamente alla creazione del documento firmato
- Gestione documenti in Streaming (inteso come ottimizzazione di volumi importanti di documenti che prevedono l'invio alla CA del solo hash del documento)
- Marcatura temporale in tutte le forme previste dalla normativa vigente
- verifica firma singola/multipla

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

Nel caso della firma PADES, è supportata una completa parametrizzazione della firma visibile/invisibile.

5.1.4.2 Hardware Security Module (HSM)

Gli HSM utilizzati dal sistema di firma remota (ospitati all'interno dei centri servizi del RTI) sono il modello CoSign 7.1 della ARX.

Tutte le operazioni critiche dal punto di vista della sicurezza (generazione delle chiavi, utilizzo delle chiavi private per la generazione delle firme, conservazione e confidenzialità delle chiavi private) avvengono esclusivamente all'interno degli apparati CoSign protette da numerose funzioni di sicurezza a livello sia hardware (es. anti-tampering) che software.

Tutte le chiavi private degli utenti ed i relativi certificati sono contenute e persistite esclusivamente all'interno degli HSM.

L'apparato CoSign ha ottenuto dall'OCSI (Organismo di Certificazione della Sicurezza Informatica) la certificazione CC EAL4+ richiesta dalla normativa vigente (cfr. http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/prodotti-certificati) oltre che, sempre in OCSI, ad aver concluso con successo la Procedura di Accertamento di Conformità di un Dispositivo per la creazione di Firme Elettroniche ai Requisiti di Sicurezza previsti dall'Allegato III della Direttiva 1999/93/CE (cfr. http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/dispositivi-accertati).

In sintesi, l'HSM "Cosign" usato dal RTI nell'ambito del sistema di firma remota qui descritto e proposto, è pienamente conforme alla vigente normativa in materia di firma digitale ed in particolare al:

- DPCM 10 Febbraio 2010, "Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza";
- DPCM 14 Ottobre 2011, "Proroga del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003".
- DPCM 19 Luglio 2012 "Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 Ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma"
- DPCM 22 Luglio 2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71".

Il RTI garantisce l'adeguamento degli HSM utilizzati nella soluzione di Firma Automatica proposta alle normative di legge in vigore.

5.1.5 VINCOLI E ASSUNZIONI DEL SERVIZIO L2.S3.4

Affinché l'Amministrazione contraente possa usufruire del servizio di Firma digitale remota è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che possa essere raggiunto il portale attraverso il quale sono esposte tutte le funzionalità descritte al precedente § 6.1.2.4. In subordine dovrà comunque avere un punto di accesso a Internet.

Come previsto da Capitolato Tecnico le operazioni di distribuzione delle credenziali di accesso al servizio di Firma Digitale Remota sono a carico delle amministrazioni contraenti.

L'Amministrazione contraente dove essere autorizzata dalla CA Aruba PEC S.p.A. ad emettere in maniera autonoma i certificati qualificati di firma digitale in quanto le procedure per la loro emissione, secondo quanto previsto dall'attuale normativa, impongono l'identificazione certa del richiedente, ossia il suo riconoscimento de visu di fronte ad una persona incaricata dalla CA ad effettuare tale identificazione.

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

Allo scopo la CA di Aruba PEC, in qualità di Ente certificatore accreditato presso AgID, consentirà all'Amministrazione contraente di attivare un Centro di Registrazione Locale (CDRL), ossia una Registration Authority (RA) delegata da ArubaPEC all'identificazione certa ed all'emissione diretta ed in loco di certificati qualificati di firma digitale a pieno valore legale. A seguito di un corso di formazione (on line tramite portale di Aruba con relativo test finale), della durata tipica di un giorno, gli Operatori di Registrazione (ODR) saranno in grado di effettuare, in totale autonomia, le attività di raccolta delle informazioni degli utenti, il loro riconoscimento dell'identità certa e procedere, se necessario, alla registrazione delle informazioni per l'attivazione del servizio di Firma digitale remota e all'emissione dei certificati qualificati di firma digitale. Gli ODR potranno autenticarsi al circuito di emissione dell'Ente Certificatore ArubaPEC tramite una semplice interfaccia web personalizzata secondo le specifiche esigenze dell'Amministrazione contraente.

L'Amministrazione contraente, in qualità di CDRL, potrà nominare degli Incaricati alla Registrazione (IR) — ad es. personale delle varie filiali — che, nel rispetto delle istruzioni impartite dal Certificatore e dal CDRL stesso, provvederanno al riconoscimento dell'identità certa del richiedente ed all'invio dei dati necessari all'attivazione del Servizio di firma digitale remota.

Per il rilascio dei certificati sarà reso disponibile all'Amministrazione contraente un Card Management System (CMS). Con tale sistema l'ODR potrà effettuare le seguenti principali operazioni:

- Registrazione dei dati dell'utente, al momento della produzione dei certificati,
- Emissioni di kit di firma digitale,
- Registrazioni di kit di firma digitale remota,
- Gestione del ciclo di vita dei certificati emessi tramite il CMS (sospensione, riattivazione, revoca),
- Ricerca e verifica delle emissioni di kit di firma digitale effettuate tramite il CMS.
- I costi di attivazione CDRL sono inclusi nel servizio offerto di firma digitale remota.

5.1.6 COMPONENTI DEL SERVIZIO L2.S3.4

La normativa vigente prevede per il rilascio del certificato di Firma Digitale, che ci sia una identificazione certa del richiedente, questa avviene attraverso un riconoscimento de visu di fronte ad una persona incaricata all'identificazione dalla Certification Authority (maggiori dettagli sono reperibili nel Certification Practice Statement di Aruba).

Per poter consentire ad ogni Cliente di rilasciare i certificati di sottoscrizione, la Certification Authority di Aruba PEC, in qualità di Ente certificatore accreditato presso AGID consentirà alla Stazione Appaltante di:

- Attivare un Centro di Registrazione Locale (CDRL), ossia un'Autorità di Registrazione (RA) delegata da Aruba PEC all'identificazione certa ed all'emissione diretta ed in loco di certificati di Firma Digitale a pieno valore legale. A seguito di adeguata formazione, erogata da Aruba PEC, gli Operatori di Registrazione (OdR) saranno in grado di effettuare, in totale autonomia, le attività di raccolta delle informazioni degli utenti, il loro riconoscimento dell'identità certa e procedere, se necessario, alla registrazione delle informazioni per l'attivazione del Servizio di firma digitale. Gli Operatori di Registrazione potranno autenticarsi al circuito di emissione dell'Ente Certificatore Aruba PEC tramite una semplice interfaccia web in grado di gestire tutto il ciclo di vita dei certificati richiesti;
- Se ritenuto opportuno, è possibile nominare degli Incaricati alla Registrazione (IR) (ad es. personale delle varie sedi) che, nel rispetto delle istruzioni impartite dal Certificatore e dal CDRL stesso, provvederà al riconoscimento dell'identità certa del richiedente ed all'invio dei dati necessari agli Operatori di Rilascio, i quali potranno a quel punto occuparsi della produzione dei certificati.

La figura 3, mostra il rapporto che lega il certificatore, il CDRL e gli operatori ad esso afferenti a seguito degli accordi sopra illustrati.

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

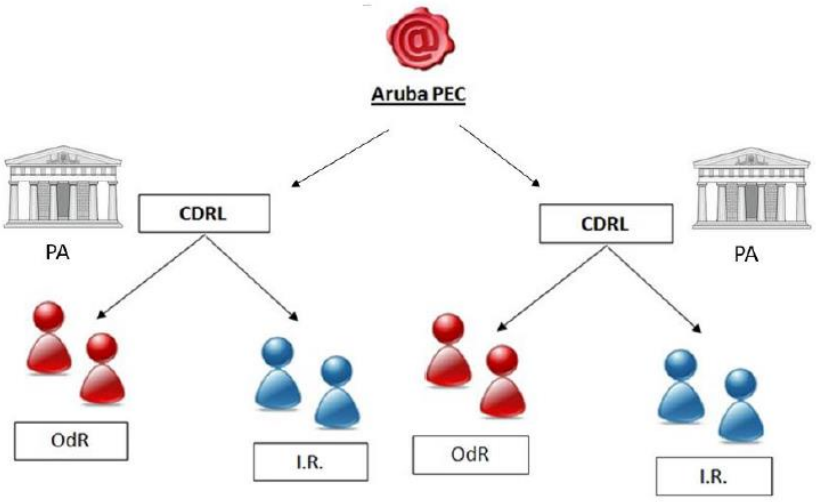


Figure 2 - Schema rilascio certificati di sottoscrizione

Tale procedura garantisce che il certificato di sottoscrizione venga rilasciato solamente agli utenti in maniera certa dal personale incaricato.

Una volta pervenuta ad Aruba PEC la documentazione relativa a CDRL/operatori, questa metterà a disposizione dell'Amministrazione uno strumento che permetterà la gestione dei certificati.

L'accesso a tale strumento sarà configurato da Aruba PEC agli OdR forniti dall'Amministrazione attraverso il seguente processo:

- Invio mail con accesso e-learning;
- Ricezione resoconto con nominativi che hanno terminato il corso;
- Invio materiale kit accesso operatori e censimento dell'OdR:
  - Scratch Card;
  - Otp fisico (opzionale).

Alla fine del processo l'OdR sarà in grado di effettuare l'emissione dei certificati ai titolari utilizzando la procedura sopra descritta e specificata nel CPS.

Esiste tuttavia una modalità alternativa, definita Bulk, utilizzabile qualora l'Amministrazione non attivi un Centro Di Registrazione Locale.

La modalità Bulk prevede da parte di Aruba PEC la nomina di IR appartenenti all'Amministrazione che saranno deputati all'invio ad Aruba PEC di un file in formato csv, compilato in tutti i sui campi secondo le modalità previste dal CPS, il quale verrà caricato in maniera automatica.

Una volta terminato il processo verranno preparati dei kit che saranno spediti direttamente alle Amministrazioni.

5.1.7 MODALITÀ DI EROGAZIONE DEL SERVIZIO L2.S3.4

Per consentirne l'utilizzo all'interno della propria infrastruttura avrà a disposizione diverse modalità:

- **Portale Web** (ASOL ArubaSignOnLine) interfaccia grafica dove sarà possibile effettuare operazioni di firma, verifica, marca e timbro in modalità As a Service. L'utente una volta raggiunto il portale ed autenticato con le credenziali di accesso rilasciategli dall'operatore potrà sottoscrivere, verificare, marcare e/o timbrare documenti con il proprio certificato;
- **ARSS**: Web Service consente l'integrazione applicativa delle applicazioni e dei sistemi affinché siano in grado di interfacciarsi verso il servizio di Firma Digitale Remota. L' ARSS provvederà a dialogare, su canale sicuro (HTTPS) con mutua autenticazione, con il sistema di firma remota che espone le funzionalità di firma digitale. Tale strumento dovrà essere installato presso il data center dell'Amministrazione che metterà a disposizione una piattaforma dedicata;

- **ArubaSign**: client stand alone che consente di poter eseguire operazioni di firma, marca, verifica dalla propria postazione.

Opportune line guida e manuali utenti saranno forniti ai clienti per consentire l'utilizzo e l'integrazione degli strumenti suddetti.

5.1.8 QUANTITÀ E PREZZI DEL SERVIZIO L2.S3.4

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i costi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.1.9 ATTIVAZIONE DEL SERVIZIO L2.S3.4

Si prevede l'avvio del servizio secondo i tempi definiti nell'Appendice B.

5.2 Requisiti di installazione in carico all'amministrazione

I seguenti dettagli riguardano le attività in carico all'amministrazione per la predisposizione degli ambienti fisici e logici:

- Ambiente Fisico
  - Spazio Rack
  - BTU
  - Alimentazione
  - Interfacce di rete
  - Potenza richiesta
- Ambiente Logico
  - Spazio Disco
  - RAM
  - vCPU
  - Connettività Internet
  - VPN IPSec

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

5.3 Servizio L2.S3.8 – Secure Web Gateway

5.3.1 DESCRIZIONE DEL SERVIZIO

Il servizio consente alle Amministrazioni di bloccare l'accesso a siti web potenzialmente malevoli aggiornando la propria base dati in mani.era automatica e di riconoscere il download di applicazioni potenzialmente dannose

5.3.2 ARCHITETTURA DELLA SOLUZIONE

La soluzione di Secure Web Gateway è caratterizzata dalle seguenti componenti logico / funzionali:

- una **componente centrale**, per la gestione remota del servizio erogato alle Amministrazioni aderenti;
- una **Gateway Console**, utilizzata per il deployment delle policy di sicurezza relative alla singola Amministrazione e gestita dal Centro Servizi mediante una connessione VPN sicura cifrata;
- una **Componente Gateway (SWG)**, utilizzata per il controllo del traffico della navigazione Internet e l'attuazione delle policy di sicurezza.

5.3.3 DEPLOYMENT DELLA SOLUZIONE E EROGAZIONE DEL SERVIZIO

La fase di deployment della soluzione SWG, è successiva all'erogazione dei servizi professionali (L2.S3.9) acquistati per il rinnovo tecnologico della piattaforma. In tal senso quindi, nell'ambito specifico della componente L2.S3.8 saranno contemplate soltanto le seguenti attività specifiche:

- Attivazione funzionalità di SWG
- Definizione delle policy base di WebSecurity come segue:
  - 1 profilo basic security per web
  - 1 profilo basic security+legal per web

Ulteriori funzionalità di sicurezza avanzate o custom specifiche, non presenti e/o non definite nella componente L2.S3.9, sono da considerarsi fuori ambito del presente "L2.S3.8 – Secure Web Gateway" e potranno essere realizzate, così come ulteriori attività di configurazione e personalizzazione, tramite acquisto di servizi professionali specifici.

Il servizio viene erogato in modalità "As a service" da remoto in orario 9:00-18:00 nei giorni feriali. La durata del servizio è di 44 mesi.
La modalità di erogazione del servizio L2.S3.8 è così composta:

- presso il Centro Servizi del RTI:
  - conduzione della piattaforma centrale deputata alle attività di (gestione remota):
    - **Change management** *per la modifica delle regole SWG implementate al 5.4.3;*

    raccolta degli eventi rilevanti dalle strutture centralizzate per (monitoraggio remoto):
    - **Monitoraggio di disponibilità (fault monitoring)** *al fine di segnalare al personale in presidio locale e/o all'amministrazione, eventuali fault delle componenti di fornitura.*
    - **Monitoraggio di sicurezza** *al fine di monitorare costantemente gli eventi di sicurezza delle componenti di fornitura.*
    - **Triage (incident notification)** *che comprende: identificazione, classificazione e notifica. Tale servizio sarà erogato mediante il sistema di trouble ticketing e/o a mezzo mail.*
    - **Reporting** *che comprende la produzione di technical report, a chiusura di ciascun incident. Tale servizio sarà erogato mediante il sistema di trouble ticketing e/o a mezzo mail.*

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

5.3.4 VINCOLI E ASSUNZIONI DEL SERVIZIO

Affinché possano essere erogate le attività di gestione è necessaria la raggiungibilità dei costituenti del servizio dislocati presso L'amministrazione contraente da parte del Centro Servizi del RTI. Quindi è necessario che l'Amministrazione sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (Agid) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e la sede dell'Amministrazione avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

5.3.5 COSTI DEL SERVIZIO

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].Servizio L2.S3.9 - Servizi Professionali

In questa sezione si descrivono le attività richieste dall'Amministrazione contraente e svolte come servizi professionali.

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a corpo". Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori determinato coerentemente con il piano di lavoro definito in Appendice B, alla consegna dei deliverable concordati, previo benestare.

I servizi professionali saranno erogati presso le sedi dell'Amministrazione Contraente, presso le sedi del RTI, o presso altra sede da concordare con l'Amministrazione Stessa: essi prevedono attività di personale sia on-site che specializzato in back office, per la completa esecuzione ed il governo dei task, all'interno di ciascuna iniziativa.

5.3.6 Servizio di supporto all'infrastruttura del servizio di Firma Digitale Remota – SP.01

Il servizio consiste nel garantire un supporto tecnico per la gestione dell'infrastruttura ARSS (Aruba Remote Signing System) per i servizi di Firma Digitale. Il RTI, in continuità con il passato, svolgerà attività finalizzate al bilanciamento e al mantenimento dell'operatività dell'ARSS ed a fornire supporto per le attività di training per l'utilizzo del Portale di Firma Digitale. Resta di competenza dell'Amministrazione la predisposizione delle risorse HW, SW e di rete per l'infrastruttura ARSS.

5.3.6.1 Vincoli e assunzioni del SP.01

L'amministrazione si farà carico del coordinamento delle attività di interazione tra RTI ed i fornitori delle applicazioni oggetto di integrazione.

5.3.6.2 Modalità di erogazione del SP.01

I servizi saranno erogati a task, con riferimento a quanto descritto nel § 0.

5.3.6.3 Quantità e prezzi del SP.01

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.3.6.4 Attivazione del SP.01

Si prevede l'avvio del servizio secondo i tempi definiti nell'Appendice B.

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

Company General Use

6 RISERVATEZZA

Per l'erogazione della fornitura, il Fornitore non ha necessità trattare e/o accedere a informazioni o materiale classificato ma è comunque tenuto alla sicurezza e alla riservatezza dei dati e della documentazione di cui viene a conoscenza.

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

APPENDICE A PROGETTO DI ATTUAZIONE

A.1 Struttura organizzativa

La struttura organizzativa completa è descritta nella proposta tecnica (cfr. documento [DA-3]).

Le figure professionali coinvolte nella gestione e conduzione dei servizi oggetto del presente Progetto dei fabbisogni per lo specifico contratto esecutivo sono riassunte nella seguente Tabella 7.

Tabella 7: Figure professionali.

Ruolo	Caratteristiche e responsabilità
Responsabile Contratto Quadro	È il rappresentante del fornitore verso Agid/Consip, garantisce l'omogeneità e l'uniformità di interfaccia verso le parti interessate a livello di Governo del Contratto Quadro vigilando sull'osservanza di tutte le indicazioni operative, di indirizzo e di controllo, che a tal scopo potranno essere predisposte da Consip e/o da AgID, per quanto di rispettiva competenza. Rappresenta, insieme al Responsabile del Centro Servizi, il RTI nel Comitato di Direzione Tecnica.
Responsabile Contratto Esecutivo	Costituisce l'interfaccia unica verso il Responsabile del Procedimento dell'Amministrazione Beneficiaria. È responsabile dell'erogazione dei servizi acquistati dall'Amministrazione e della rendicontazione e dei meeting di stato avanzamento lavori. Costituisce l'interfaccia unica verso il Responsabile Unico del Procedimento dell'Amministrazione beneficiaria.
Responsabile Tecnico	È il Responsabile unico delle attività tecniche e del raggiungimento degli obiettivi dei servizi oggetto del Contratto. Costituisce l'interfaccia unica verso il Direttore Esecuzione nominato dall'Amministrazione. Ha la visione complessiva e integrata di tutte le attività tecniche legate all'attivazione, all'erogazione e al rilascio dei servizi della fornitura e ne garantisce la qualità.
Responsabile del Centro Servizi	È responsabile del Centro servizi da cui vengono erogati i servizi nella modalità "as a service".
Responsabile Servizi Data loss/leak prevention, Database security e Professionali	Coincide con il Responsabile Tecnico
HELP DESK	Primo punto di contatto a disposizione dell'Amministrazione per l'avvio delle attività di acquisizione del servizio. Supporta inoltre i referenti dell'Amministrazione contraente nelle attività di risoluzione di eventuali problematiche di utilizzo del servizio. L'Help Desk è contattabile al numero verde: **800 894 590**. Ulteriori informazioni sono reperibili al seguente URL http://www.spc-lotto2-sicurezza.it presso il quale è presente il Portale di Governo e Gestione della Fornitura.

I nominativi delle figure presenti nella tabella soprastante saranno forniti all'Amministrazione entro 10 giorni dalla stipula del contratto.

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

A.2 Quantità e costi

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati di seguito nella Tabella 11, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5]. I prezzi IVA esclusa tengono conto di quanto riportato nel listino prezzi SPC lotto 2 [DA-6]. In base a quanto richiesto dall'Amministrazione contraente nel Piano dei fabbisogni [DA-5].

Tabella 8: Quantità e costi.

Servizio L2.S2.1 - Firma digitale remota				2021 II sem			2022		
Metrica		Fascia	Prezzo unitario	Nun.tà	Mesi	Prezzo	Nun.tà	Mesi	Prezzo
utente/anno		Fascia 1: fino a 50 utenti	€ 11,95	50	6	€ 298,75	50	6	€ 298,75
		Fascia 2: da 51 a 200 utenti	€ 10,50	150	6	€ 787,50	150	6	€ 787,50
		Fascia 3: da 201 - 1000 utenti	€ 8,50	800	6	€ 3.400,00	800	6	€ 3.400,00
		Fascia 4: oltre 1000 utenti	€ 6,65	400	6	€ 1.330,00	400	6	€ 1.330,00

Servizio L2.S3.8 - Secure Web Gateway				2021 II sem			2022		
Metrica		Fascia	Prezzo unitario	Nun.tà	Mesi	Prezzo	Nun.tà	Mesi	Prezzo
pdli/anno		Fascia 1: fino a 100 pdli	€ 24,30	100	6	€ 1.215,00	0	0	€ 0,00
		Fascia 2: da 101 a 1.000 pdli	€ 10,00	900	6	€ 4.500,00	0	0	€ 0,00
		Fascia 3: da 1.001 a 5.000 pdli	€ 8,00	350	6	€ 1.400,00	0	0	€ 0,00
		Fascia 4: oltre 5.000 pdli	€ 5,50	0		€ 0,00	0		€ 0,00

Servizio L2.S3.9 - Servizi professionali di supporto alla firma remota							2021		2022	
ID	ID SPC	Descrizione	Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo	Nun.tà	Prezzo
SG.1	L2.S3.9	Serv.Prof.	giorno/uomo	H8	Capo progetto	€ 300,00	2	€ 600,00	2	€ 600,00
					Security Architect	€ 372,90	2	€ 745,80	3	€ 1.118,70
					Specialista di tecnologia/prodotto Senior	€ 295,00	8	€ 2.360,00	8	€ 2.360,00
					Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00	0	€ 0,00
			giorno/uomo	H24	Specialista di tecnologia/prodotto Senior (H24)	€ 1.180,00	0	€ 0,00	0	€ 0,00
					Specialista di tecnologia/prodotto (H24)	€ 930,00	0	€ 0,00	0	€ 0,00

L'iniziativa ha un valore complessivo di **26.532,00 € + IVA**

A.2.1 Fatturazione Servizi

I servizi Secure Web Gateway (L2.S3.8) saranno fatturati a canone bimestrale.

In deroga a quanto previsto nel "Allegato 4B - Schema Contratto Esecutivo – Lotto 2", si conviene che in ogni bimestre verrà riconosciuto il corrispettivo dell'intero canone annuale relativi ai servizi di Firma Digitale Remota (L2.S2.1) per i beni rilasciati nel bimestre.

A valle delle verifiche dell'Amministrazione (art 15 dell'Accordo Quadro), i servizi professionali SP-01-L2.S3.9 saranno fatturati a task, in ragione dei deliverables effettivamente conseguiti, nel rispetto del Progetto dei Fabbisogni, ovvero secondo lo stato di avanzamento dei lavori, e nelle misure che si concorderanno ad inizio delle attività o nel piano di lavoro.

Ciascuna fattura sarà corrisposta nel termine di pagamento di 30 (trenta) giorni, secondo le modalità di cui alla normativa vigente (D.Lgs. n. 231/2002).

Company General Use

AGENZIA REGIONALE PER LA PREVENZIONE L'AMBIENTE E L'ENERGIA DELL'EMILIA ROMAGNA
Data: 14/07/2021 14:16:22 PG/2021/0110469

APPENDICE B PIANO DI LAVORO

Di seguito si riporta la programmazione delle attività, espressa in giorni lavorativi a partire dalla data di perfezionamento del contratto esecutivo (T0).

B.1 Inizio e durata dei servizi

In base a quanto richiesto dall'Amministrazione contraente nel Piano dei fabbisogni [DA-5] la Tabella 12 riporta le date di inizio e la durata per le attività previste per l'erogazione del servizi.

#	Nome attività	Inizio	Fine	Vincoli
1	L2.S2.1 – Firma Digitale Remota	T0	Luglio 2022	
2	L2.S3.8 – Secure Web Gateway	T0	31/12/2021	
3	L2.S3.9 – Servizio di supporto all'infrastruttura del servizio di Firma Digitale Remota	T0	Luglio 2022	

Tabella 9: Piano di attivazione.

Company General Use

N. Proposta: PDTD-2021-596 del 22/07/2021

Centro di Responsabilità: Servizio Sistemi Informativi E Innovazione Digitale

OGGETTO: Servizio Sistemi Informativi e Innovazione Digitale. Proroga del contratto di fornitura dei "Servizi di gestione delle identità digitali e sicurezza applicativa" in Adesione al Contratto Quadro Consip S.p.a. "SPC Cloud Lotto 2" - CIG derivato 7300627BFA.

PARERE CONTABILE

Il sottoscritto Dott. Bacchi Reggiani Giuseppe, Responsabile del Servizio Amministrazione, Bilancio e Controllo economico, esprime parere di regolarità contabile ai sensi del Regolamento Arpae per l'adozione degli atti di gestione delle risorse dell'Agenzia.

Data 23/07/2021

Il Responsabile del Servizio
Amministrazione, Bilancio e
Controllo economico