ARPAE

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

dell'Emilia - Romagna

*** * ***

Atti amministrativi

Determinazione dirigenziale	n. DET-2017-983 del 04/12/2017
Oggetto	Servizio Sistemi Informativi – Adesione al Contratto Quadro Consip S.p.a. "SPC Cloud Lotto 2" per la fornitura di "Servizi di gestione delle identità digitali e sicurezza applicativa"
Proposta	n. PDTD-2017-988 del 30/11/2017
Struttura adottante	Servizio Sistemi Informativi
Dirigente adottante	Santovito Piero
Struttura proponente	Servizio Sistemi Informativi
Dirigente proponente	Dott. Santovito Piero
Responsabile del procedimento	Santovito Piero

Questo giorno 04 (quattro) dicembre 2017 presso la sede di Viale Silvani, 6 in Bologna, il Responsabile del Servizio Sistemi Informativi, Dott. Santovito Piero, ai sensi del Regolamento Arpae sul Decentramento amministrativo, approvato con D.D.G. n. 87 del 01/09/2017 e dell'art. 4, comma 2 del D.Lgs. 30 marzo 2001, n. 165 determina quanto segue.

Oggetto: Servizio Sistemi Informativi – Adesione al Contratto Quadro Consip S.p.a. "SPC Cloud Lotto 2" per la fornitura di "Servizi di gestione delle identità digitali e sicurezza applicativa"

VISTO:

- il Regolamento per il decentramento amministrativo, come modificato con delibera del Direttore generale n. 87 del 01.09.2017;
- il Regolamento dell'Agenzia in materia di approvvigionamento, come modificato con D.D.G. n. 80 del 20.07.2017;
- la D.D.G. n. 136 del 23/12/2016 - Direzione Amministrativa- Area 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 2017 - 2019, del Piano Investimenti 2017-2019, del Bilancio economico preventivo per l'esercizio 2017 e del Budget generale e della programmazione di cassa per l'esercizio 2017;
- la D.D.G. n. 137 del 23/12/2016 - Direzione Amministrativa. Area Bilancio e Controllo Economico. Approvazione delle linee guida e assegnazione dei budget di esercizio e investimenti per l'anno 2017 ai centri di responsabilità dell'Agenzia per la Prevenzione, l'Ambiente e l'Energia dell'Emilia Romagna;
- la D.D.G. 52 del 28/04/2017 - Direzione Amministrativa. Area Bilancio e Controllo Economico. Riprevisione del Budget di esercizio per l'anno 2017;
- la D.D.G. 74 del 26/06/2017 - Direzione Amministrativa. Area Patrimonio e Servizi tecnici. Riprevisione del Piano Investimenti 2017-19 e del budget investimenti 2017;
- la D.D.G. n. 108 del 30/10/2017 – Terza modifica del programma biennale degli acquisti di forniture e servizi per gli anni 2017-2018;

RICHIAMATO:

- il comunicato del presidente dell'A.N.A.C. dell'11/05/2016, che relativamente al periodo transitorio relativo all'entrata in vigore del d. Lgs. 50/2016 (c.d. nuovo codice dei contratti) ha chiarito che continuano ad applicarsi le disposizioni del d. Lgs. 163/2006 alle procedure negoziate in attuazione di accordi quadro aggiudicati prima dell'entrata in vigore del nuovo Codice;

PREMESSO:

- che Arpae è dotata di una architettura di sicurezza per la parte rete-networking nonchè per la navigazione internet e Anti-Spam, la quale riveste rilevanza essenziale al fine di poter gestire la sicurezza informatica dell'agenzia nonchè prevista nell'ambito delle misure minime per la

sicurezza ICT per le pubbliche amministrazioni emanate dall'Agenzia per l'Italia Digitale con Circolare del 18 aprile 2017, n. 2/2017;

- che con Determinazione del Servizio Sistemi Informativi del 2014 era stata aggiudicata la fornitura di "Servizi per rinnovo e adeguamento delle componenti Hw/Sw dell'architettura Websense Triton Security Gateway Anywhere presso Arpae" per un periodo triennale pertanto la garanzia sulle varie appliance in dotazione così come la validità delle licenze Websense Triton security gateway anywhere, è attualmente in scadenza al 31/12/2017;

- che sulla base dei fabbisogni espressi dal Servizio Sistemi Informativi per le strutture di Arpae, e sulla base delle premesse sopra esposte, vi è pertanto l'esigenza di provvedere al mantenimento di un'infrastruttura di sicurezza adeguata;

- che si rende necessaria altresì la dotazione di un'infrastruttura di Firma digitale remota, modalità innovativa per l'apposizione delle firme digitali 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, fra cui il fatto di non richiedere installazione di hardware e software dedicato nelle postazione di lavoro, riducendo pertando problemi di incompatibilità, indipendenza dall'ambiente operativo utente, nonchè generazione di firme digitali in ogni momento e luogo mediante una semplice connessione a internet;

PREMESSO INOLTRE:

- che l'art. 20, comma 4, del D.L. n. 83/2012, come convertito con modificazioni dalla Legge 7 agosto 2012 , n. 134, ha affidato a Consip S.p.A., a decorrere dalla data di entrata in vigore della legge di conversione del decreto medesimo, "le attività amministrative, contrattuali e strumentali già attribuite a DigitPA, ai fini della realizzazione e gestione dei progetti in materia, nel rispetto delle disposizioni del comma 3";

- che l'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge 2012/135, ha stabilito che, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente "ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311";

- che Consip S.p.A., secondo la normativa vigente, nel rispetto dei principi in materia di scelta del contraente, ai sensi dell'art. 54 del D.Lgs. n. 163/2006, ha indetto una gara a procedura ristretta per la fornitura di "Servizi Cloud Computing, di Sicurezza, di realizzazione di Portali e Servizi online e di Cooperazione applicativa per le Pubbliche Amministrazioni ", suddivisa in 4 lotti, come da bando pubblicato sulla Gazzetta Ufficiale dell'Unione Europea n. S251 del 28/12/2013 e sulla Gazzetta Ufficiale della Repubblica Italiana n. 151 del 27/12/2013, inviando al Fornitore la lettera di invito a presentare offerta, prot. 24280/2014 in data 19 settembre 2014;

- che l'RTI composto dalle aziende Leonardo-Finmeccanica S.p.A, IBM Italia S.p.A., FASTWEB S.p.A. e Sistemi Informativi S.r.l.. è risultato aggiudicatario del Lotto 2 relativo alla procedura di cui sopra ed ha sottoscritto il Contratto Quadro con Consip S.p.a. in data 20/07/2016 per durata di 60 mesi decorrenti dalla data di sottoscrizione, acquisito agli atti del Servizio e pubblicato sul sito internet www.acquistinretepa.it, contenente tutti i termini e le condizioni per la fornitura dei servizi così delineati:

- servizi per la gestione delle identità digitali, erogati in modalità "as a service", in conformità anche all'art. 64 del CAD;
- servizio di firma digitale remota comprensiva della fornitura di certificati e servizio di timbro elettronico, erogati in modalità "as a service", volti a favorire la dematerializzazione dei documenti e la digitalizzazione dei processi amministrativi;
- servizi di sicurezza, erogati sia in modalità "as a service" attraverso i Centri Servizi del Fornitore sia in modalità "on premise", atti a garantire la sicurezza applicativa e a supportare le Amministrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità dei sistemi informativi; i servizi di sicurezza includono anche servizi professionali a supporto delle attività erogati presso i centri delle Pubbliche Amministrazioni.

- che tali servizi sono stati ritenuti dal Servizio Sistemi Informativi di Arpae quali ottimali e corrispondenti al fine del soddisfacimento delle esigenze sopra esposte, e si sono valutate le condizioni contrattuali ed economiche contenute nel Contratto Quadro stipulato tra Consip S.p.a e Leonardo Finmeccanica S.p.A. nella sua qualità di impresa mandataria capo-gruppo del R.T.I. aggiudicatario, nonché nei relativi documenti allegati per l'affidamento dei servizi di gestione delle identità digitali e sicurezza applicativa;

CONSIDERATO:

- che il suddetto Contratto Quadro, non è fonte di alcuna obbligazione per Consip S.p.A. nei confronti del Fornitore, salvo quelle espressamente alla stessa riferite, costituendo il medesimo Contratto Quadro le condizioni generali dei Contratti Esecutivi che verranno conclusi dalle singole Amministrazioni di cui pertanto definisce la disciplina normativa e contrattuale, comprese le modalità di conclusione ed esecuzione;
- che le Amministrazioni che sulla base della normativa vigente hanno l'obbligo o la facoltà di utilizzare il presente Contratto Quadro, aderiscono allo stesso mediante stipulazione di un Contratto di appalto Esecutivo, il quale si perfeziona alla data di sottoscrizione da parte del Fornitore e dell'Amministrazione Beneficiaria e per il cui effetto il Fornitore è obbligato ad

eseguire la prestazione dei servizi richiesta, nell'ambito dell'oggetto contrattuale, alle condizioni già stabilite nel Contratto Quadro;

- che il CIG master del presente Contratto Quadro è: 5518849A42;

PRESO ATTO:

- che il Responsabile del Servizio Sistemi Informativi di Arpae in data 02/10/2017 con prot. N. PGDG/2017/10431, manifestando la volontà di aderire al Contratto Quadro in oggetto, ha inviato tramite PEC il proprio "Piano dei fabbisogni" alla ditta Leonardo Finmeccanica S.p.a. , quale mandataria dell'Rti relativamente ai "Servizi di gestione delle identità digitali e sicurezza applicativa" per quanto concerne l'attivazione dei seguenti servizi di interesse:

- L2.S3.1 FIRMA DIGITALE REMOTA
- L2.S3.5 DATA LOSS/LEAK PREVENTION
- L2.S3.8 SECURE WEB GATEWAY
- L2.S3.9 SERVIZI PROFESSIONALI,

così dettagliati:

SERVIZI DI FIRMA DIGITALE REMOTA, TIMBRO ELETTRONICO, MARCHE TEMPORALI E CERTIFICATI SSL (L2.S2)						
L2.S2.1	FIRMA DIGITALE REMOTA	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno	Q.tà V Anno
		150	300	500	600	600

SERVIZI DI SICUREZZA (L2.S3)						
L2.S3.5	DATA LOSS/ LEAK PREVENTION	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno	Q.tà V Anno
		1350	1350	1350	1350	1350

SECURE WEB GATEWAY (L2.S3)						
L2.S3.8	DATA LOSS/ LEAK PREVENTION	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno	Q.tà V Anno
		1350	1350	1350	1350	1350

SERVIZI PROFESSIONALI (L2.S3)							
L2.S3.9	Servizi professionali	Figure professionali	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno	Q.tà V Anno
		Capo progetto	38				

		Security Architect	65				
		Specialista di tecnologia/prodotto Senior	70				

- che in risposta alla richiesta di fornitura inviata dal Servizio Sistemi Informativi di Arpae relativamente ai servizi di interesse, la ditta Leonardo Finmeccanica S.p.A. ha inviato in data 30/11/2017 (acquisiti agli atti del Servizio con Prot. n. PGDG/2017/12962) il proprio "Progetto dei fabbisogni" per Servizi di gestione delle identità digitali e sicurezza applicativa con identificativo n. LDO/SSI/P/0082055/17 del 30/11/17 e il relativo Schema di Contratto esecutivo allegati rispettivamente A) e sub B);
- che da tale Progetto dei fabbisogni risulta, da riepilogo dei servizi da attivarsi distinti per annualità, un costo complessivo di Euro 185.118,92 + IVA 22%;

RICHIAMATO:

- l'art. 1, comma 512, della legge 28 dicembre 2015, n. 208, che prevede per le amministrazioni pubbliche l'obbligo di provvedere ai propri acquisti di beni e servizi informatici esclusivamente tramite Consip s.p.a. o i soggetti aggregatori, ivi comprese le centrali di committenza regionali per i beni e servizi disponibili presso gli stessi soggetti;

RILEVATO:

- che sono stati condotti accertamenti volti ad appurare l'esistenza di rischi da interferenza nell'esecuzione dell'appalto in oggetto e che non sono stati riscontrati i suddetti rischi, pertanto non è necessario provvedere alla redazione del DUVRI, non sussistono conseguentemente costi per la sicurezza;
- che è stato acquisito il seguente Cig derivato: 7300627BFA richiesto tramite il sistema SIMOG gestito dall'Autorità Nazionale Anticorruzione;

CONSIDERATO:

- che con l'RTI aggiudicatario del Contratto Quadro sarà sottoscritto digitalmente un "Contratto Esecutivo" secondo lo schema in allegato alla presente Determinazione, approvando il relativo "Progetto dei Fabbisogni", che insieme al "Piano dei Fabbisogni" ne costituisce parte integrante.
- che con la stipula del contratto il Fornitore è obbligato ad eseguire nei confronti dell'amministrazione beneficiaria la prestazione dei servizi richiesta a decorrere dalla data di stipula del Contratto Esecutivo medesimo sino alla scadenza ultima del Contratto Quadro, 20 luglio del 2021, per una durata quindi di 44 mesi;
- che l'adesione al Contratto Quadro prevede un contributo da versare a Consip S.p.a. pari all'8 per mille dell'importo contrattuale senza iva;

- che sono stati acquisiti i Documenti Unici di regolarità contribuitiva (DURC) e che da tale documenti risultano regolari le posizioni delle imprese componenti l'RTI aggiudicatario;

RITENUTO:

- di aderire al Contratto Quadro SPC – Lotto 2, stipulato da Consip S.p.A. con l'RTI aggiudicatario per la fornitura dei "Servizi di Identità Digitale e Sicurezza Applicativa" (CIG master n. 5518849A42) descritti nel documento "Piano dei fabbisogni";
- di accettare il "Progetto dei fabbisogni" per "Servizi di gestione delle identità digitali e sicurezza applicativa" con quantificazione economica e lo schema di contratto esecutivo presentati da Leonardo Finmeccanica S.p.a. in data 30/11/2017 acquisiti agli atti con Prot. n. PGDG/2017/12962 e qui allegati sub A) e B;
- di stipulare con il soggetto aggiudicatario il Contratto esecutivo di fornitura secondo lo schema previsto qui allegato sub B) di cui faranno parte integrante il "Piano dei fabbisogni" e il "Progetto dei fabbisogni";

DETERMINATO:

- un costo complessivo di Euro 185.118,92 + IVA 22% per un totale di Euro 225.845,08 per la fornitura di "Servizi di gestione delle identità digitali e sicurezza applicativa" nell'ambito del Lotto 2 della gara a procedura ristretta indetta da Consip S.p.a. 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", del Servizio Sistemi Informativi di Arpae e da assumersi a carico del medesimo Centro di Responsabilità;

ATTESTATO:

- ai fini dell'art. 9 del decreto legge 1 Luglio 2009 n. 78, "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. 99/2009, confermate con riferimento alla programmazione di cassa nell'Allegato A "Budget esercizio 2017 - Linee guida" della D.D.G. 137 del 23/12/2016";

SU PROPOSTA:

- del Responsabile del Servizio Sistemi Informativi , Dott. Piero Santovito, il quale ha espresso il proprio parere favorevole in merito alla regolarità amministrativa del presente provvedimento;

DATO ATTO:

- che Responsabile del procedimento è il Responsabile del Servizio Sistemi Informativi, Dott. Piero Santovito cui sono assegnati le funzioni ed i compiti di cui all'art. 10 del d. lgs. 163/2006
- del parere di regolarità contabile espresso dal Responsabile dell'Area Bilancio e Controllo Economico, Dott. Giuseppe Bacchi Reggiani;

DETERMINA

1. di aderire, per i motivi in premessa esposti, 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.
2. di approvare il "Progetto dei fabbisogni esecutivo" per la fornitura dei "Servizi di gestione delle identità digitali e sicurezza applicativa" e lo Schema di contratto esecutivo del 30/11/2017 presentati da Leonardo Finmeccanica S.p.a. quale mandataria dell'RTI, allegati sub A) e sub B) al presente atto quali parti integranti e sostanziali, per l'attivazione dei seguenti servizi :
    - *L2.S3.1 FIRMA DIGITALE REMOTA*
    - *L2.S3.5 DATA LOSS/LEAK PREVENTION*
    - *L2.S3.8 SECURE WEB GATEWAY*
    - *L2.S3.9 SERVIZI PROFESSIONALI*
3. di dare atto che il Fornitore è obbligato ad eseguire nei confronti di Arpae la prestazione dei servizi richiesti a decorrere dalla data di stipula del Contratto Esecutivo sino alla scadenza ultima del Contratto Quadro, 20 luglio del 2021, per una durata quindi di 44 mesi;
4. di procedere alla sottoscrizione del contratto esecutivo di fornitura con l'RTI aggiudicataria secondo lo schema .di contratto qui in allegato e sulla base del "Progetto dei fabbisogni" ricevuti in data 30/11/2017 secondo le modalità previste nella convenzione di cui trattasi, agli atti del Servizio, ed a cui si rimanda per tutto quanto non specificato nel presente atto, per un importo complessivo pari ad Euro 185.118,92 + IVA 22% pari ad Euro 225.845,08.
5. di dare atto che i costi relativi al presente provvedimento, tutti a carico del Centro di Responsabilità del Servizio Sistemi Informativi, e pari complessivamente ad Euro 185.118.92 + IVA 22% per un totale di Euro 225.845,08, per la quota di Euro 61.210,17 + IVA 22% per un totale di Euro 74.676,41 avente natura di "Servizi Informatici" sono a carico dell'esercizio 2017;

6. di dare atto che per la quota residua, avente sempre natura di “Servizi informatici", i costi sono compresi nel bilancio preventivo 2017-2019, e per quanto concerne i costi relativi agli esercizi 2020-2021 dovranno essere ricompresi nei rispettivi bilanci annuali e pluriennali, per i seguenti importi:
    1. esercizio 2018: Euro 37.002,50 + IVA
    2. esercizio 2019: Euro 34.252,50 + IVA
    3. esercizio 2020: Euro 35.102,50 +IVA
    4. esercizio 2021: Euro 17.551,25 + IVA

7. di dare atto che l'adesione al Contratto Quadro prevede un contributo da versare a Consip S.p.a. pari all'8 per mille dell'importo contrattuale senza iva, pertanto dell'importo di Euro 1.480,95, sempre a carico del Centro di Responsabilità del Servizio Sistemi Informativi e con medesima natura contabile.

Il Responsabile del Servizio
Sistemi Informativi
Dott. Piero Santovito

Firmato digitalmente da

claudio rando

Identificativo: LDO/SSI/P/0082055/17.

Data: 30/11/2017

ARPAE

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

Progetto dei fabbisogni

Costituendo

Raggruppamento Temporaneo di Imprese composto da:

Leonardo Divisione Sistemi per la Sicurezza e le Informazioni SpA

IBM SpA

Sistemi Informativi Srl

Fastweb SpA

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

Approvazioni Aggiuntive

Azienda	Nome e Ruolo	Firma
ARPAE	Responsabile del Servizio Sistemi Informativi	Dott. Santovito Piero

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda
01	03/10/2017		

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autori
00	03/10/2017	Prima Emissione	RTI

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 21
5.1.6 COMPONENTI DEL SERVIZIO L2.S3.4 22
5.1.7 MODALITÀ DI EROGAZIONE DEL SERVIZIO L2.S3.4 23
5.1.8 QUANTITÀ E PREZZI DEL SERVIZIO L2.S3.4 24
5.1.9 ATTIVAZIONE DEL SERVIZIO L2.S3.4 24
5.2 Requisiti di installazione in carico all'amministrazione 24
5.3 Servizio L2.S3.5 – Data Loss/Leak Prevention 25
5.3.1 DESCRIZIONE DEL SERVIZIO 25
5.3.2 ARCHITETTURA DELLA SOLUZIONE 25
5.3.3 DEPLOY DELLA SOLUZIONE E EROGAZIONE DEL SERVIZIO 25
5.3.4 VINCOLI E ASSUNZIONI DEL SERVIZIO 26
5.3.5 COSTI DEL SERVIZIO 26
5.4 Servizio L2.S3.8 – Secure Web Gateway 27
5.4.1 DESCRIZIONE DEL SERVIZIO 27
5.4.2 ARCHITETTURA DELLA SOLUZIONE 27
5.4.3 DEPLOYMENT DELLA SOLUZIONE E EROGAZIONE DEL SERVIZIO 27
5.4.4 VINCOLI E ASSUNZIONI DEL SERVIZIO 28
5.4.5 COSTI DEL SERVIZIO 28
5.5 Servizio L2.S3.9 – Servizi Professionali 29

5.5.1 SERVIZI PROFESSIONALI PER MIGRAZIONE DELLA VECCHIA PIATTAFORMA DLP/SWG 29
5.5.2 SERVIZI PROFESSIONALI PER INTEGRAZIONI NUOVE FUNZIONALITÀ HYBRID WEB + DATA DISCOVERY 30
5.5.3 SERVIZI PROFESSIONALI PER INSTALLAZIONE ARSS PER FIRMA DIGITALE 31
5.5.4 SERVIZI PROFESSIONALI OPZIONALI DI SUPPORTO PER FIRMA DIGITALE 31
6 Riservatezza **32**
Appendice A Progetto di attuazione **33**
A.1 Struttura organizzativa 33
A.2 Quantità e costi 34
A.2.1 Fatturazione SP01-L2.S3.9 35
Appendice B Piano di lavoro **36**
B.1 Inizio e durata dei servizi 36
B.1.1 Firma Digitale 36
B.1.2 DLP / SWG 36

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 7: Installazione dei componenti software 29
Tabella 8: Attività di migrazione del servizio SWG. 30
Tabella 7: Figure professionali. 33
Tabella 8: Quantità e costi. 34
Tabella 9: Piano di attivazione. 36

LISTA DELLE FIGURE

Figura 1 Struttura del Progetto dei Fabbisogni 6

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 Il RTI 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.

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.

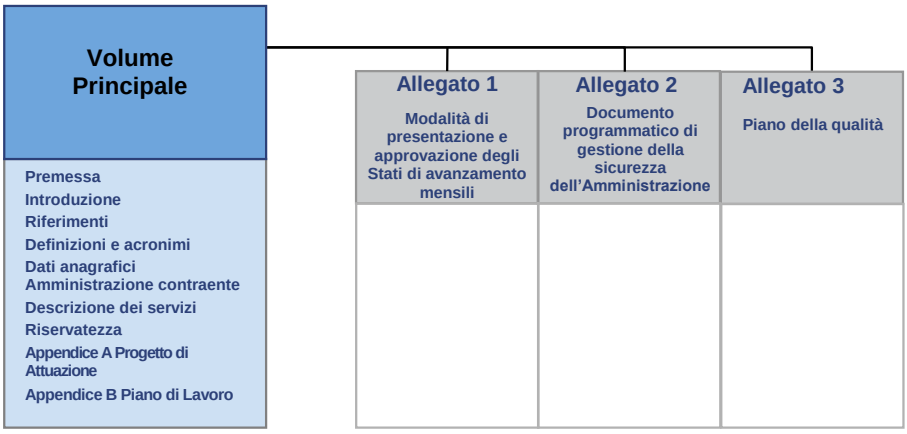

Figura 1 Struttura del Progetto dei Fabbisogni

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

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 in data **06/10/2017** a mezzo PEC il Documento "Schema Piano dei fabbisogni" 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.S3.5 – Data Loss/Leak Prevention
- L2.S3.8 – Secure Web Gateway
- L2.S3.9 – Servizi professionali.

Questi ultimi, in particolare, sono finalizzati all'esecuzione di un'attività di assessment alle *Misure minime di sicurezza ICT per le Pubbliche Amministrazioni*, emanate da AgID in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 (di seguito per brevità "*Misure minime di sicurezza AgID*").

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 in data 03/10/2017*
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/

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 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
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
XML	eXtensible Markup Language

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. Piero Santovito
Indirizzo mail	dirgen@cert.arpa.emr.it
PEC (SI/NO)	SI

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

Nome	Piero
Cognome	Santovito
Telefono fisso	051/6223910
Indirizzo mail	psantovito@arpae.it
PEC (SI/NO)	SI, psantovito@cert.arpa.emr.it

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.

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.

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.

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.

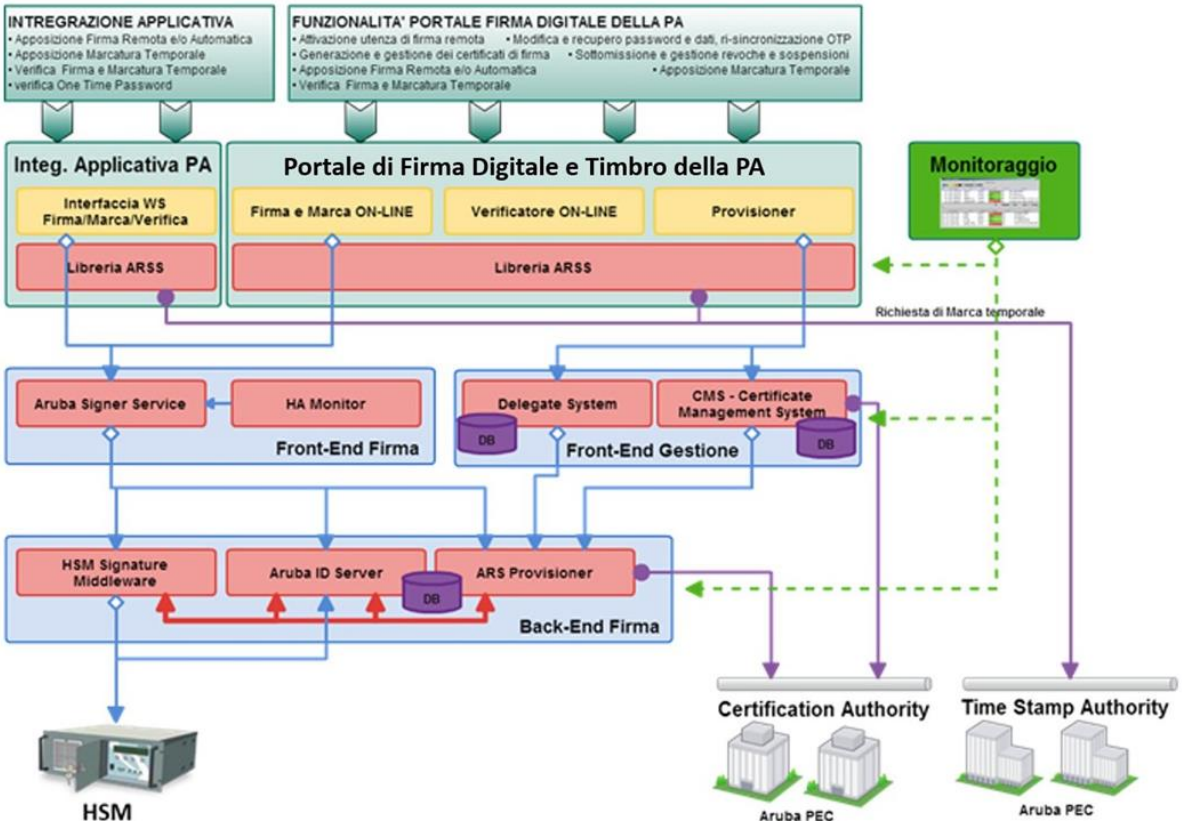

Figure 1 - Architettura software del servizio di Firma digitale remota

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.
- **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

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.

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.

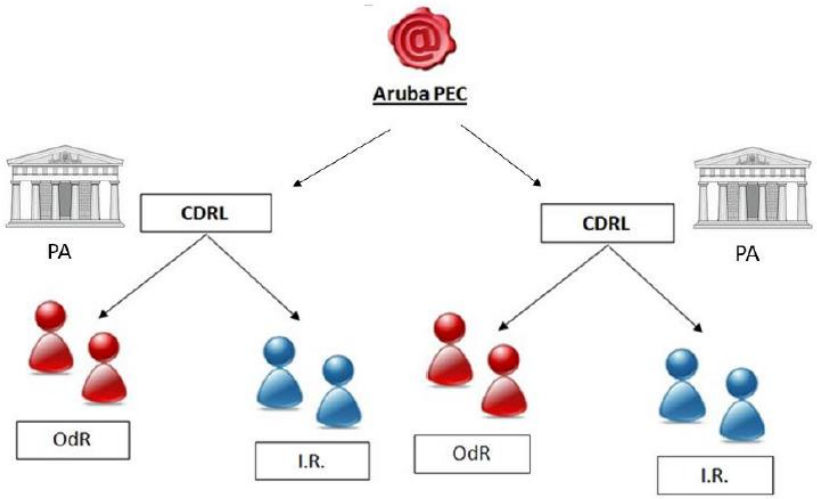

Figure 2 - Schema rilascio certificati di sottoscrizione

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

5.3 Servizio L2.S3.5 – Data Loss/Leak Prevention

5.3.1 DESCRIZIONE DEL SERVIZIO

Il servizio di "data loss/leak prevention" (o DLP) consente la protezione dei dati da accessi non autorizzati o violazioni delle policy di sicurezza e riduce il rischio di perdita, danno o svantaggio competitivo. E' garantita la supervisione e controllo dei dati indipendentemente dal fatto che siano in uso, archiviati o in transito sulla rete.

5.3.2 ARCHITETTURA DELLA SOLUZIONE

La soluzione di Data loss/leak prevention, specifica per l'amministrazione ARPAE è caratterizzata dalle seguenti componenti logico / funzionali:

- una ***componente centrale***, nel Centro Servizi, per la gestione del servizio erogato alle Amministrazioni aderenti;
- una ***Console DLP***, dislocata presso l'Amministrazione, utilizzata per il deploy delle policy di sicurezza e gestita dal Centro Servizi mediante una connessione VPN sicura cifrata;
- un ***Agent DLP*** software, installato sugli endpoint e utilizzato per il monitoraggio continuo dei dati da proteggere;

5.3.3 DEPLOY DELLA SOLUZIONE E EROGAZIONE DEL SERVIZIO

Al momento della stesura del presente documento, essendo un nuovo servizio, non c'è la visibilità della reale architettura di ARPA, per cui tutte le attività elencate sono riferite alla normale programmazione di una installazione base del servizio DLP. E' comunque prevista una configurazione base dell'ambiente DLP utile a testare il funzionamento dei moduli per mostrare all'Amministrazione contraente le potenzialità della nuova piattaforma. In tal senso quindi, nell'ambito specifico della componente L2.S3.5 saranno contemplate soltanto le seguenti attività specifiche:

- Attivazione funzionalità di DLP su Web Content Gateway
- Definizione di 1 template DLP su base "Industry"
- Definizione delle policy di discovery fingerprint

Ulteriori funzionalità e configurazioni 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.S3.5 – Data Loss/Leak Prevention" e potranno essere realizzate, così come ulteriori attività di configurazione e personalizzazione, tramite acquisto di servizi professionali specifici.

La modalità di erogazione del servizio L2.S3.5 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 DLP implementate al 5.3.3;*
    - **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.*

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].

5.4 Servizio L2.S3.8 – Secure Web Gateway

5.4.1 DESCRIZIONE DEL SERVIZIO

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

5.4.2 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;

5.4.3 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.*

5.4.4 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.

5.4.5 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.

5.5 Servizio L2.S3.9 – Servizi Professionali

5.5.1 SERVIZI PROFESSIONALI PER MIGRAZIONE DELLA VECCHIA PIATTAFORMA DLP/SWG

L'obiettivo dei servizi professionali riportati nel presente paragrafo è quello di effettuare il consolidamento avanzato del servizio SWG all'ultima versione hardware disponibile, grazie all'implementazione di una nuova architettura.
La nuova architettura proposta contempla l'installazione degli appliance V5000 G4 e di un server Triton Console di cui vengono riportate le caratteristiche dell'hardware necessario. L'installazione di un server SQL esterno alla console Triton per la gestione dei log è fortemente consigliato.

5.5.1.1 System Requirements Content Gateway e Triton Console

I requisiti di sistema per l'installazione della nuova architettura sono disponibili al seguente indirizzo: http://www.websense.com/content/support/library/deployctr/v84/dic_sys_req.aspx.

In sintesi:

Requisiti del nuovo Triton Management Server, già dimensionato per supportare l'installazione dei moduli AP-Web e Ap-Data:

- OS: Windows Server 2012 Standard Edition R1 o R2,
- Hardware: 8 CPU cores (2.5 GHz), 16 GB RAM, 150 GB Disk Space

Per l'ottimale gestione dei report sarebbe consigliato un Reporting server dedicato e differente rispetto alla Triton Management. Nel caso si volesse procedere in questa direzione i requisiti del server sono di seguito riportati:

- SQL Server 2012/2014 (con ultimo SP rilasciato da Microsoft) Standard, Business Intelligence o Enterprise editions
- Hardware: 8 CPU cores (2.5 GHz), 16 GB RAM, 500 GB Disk Space

5.5.1.2 Attività di installazione del componente software

Di seguito vengono definite le attività previste nelle giornate dedicate all'installazione delle componenti software di base AP-WEB ed AP-DATA.

Tabella 7: Installazione dei componenti software

ATTIVITA'	CONTENUTI	Obiettivo	Responsabilità
Triton Manager 8.x / Server Database: installazione secondo le specifiche hardware fornite	Configurazione hardware server come da specifiche Forcepoint Hardware Requirements Comitato di Direzione Tecnica.	Servers conformi e pronti per l'installazione dell'OS	ARPAE
Installazione Windows su server dedicati ai ruoli di Triton Manager 8.4 e Server Database	Installazione, configurazione e aggiornamento del Sistema Operativo Windows 2012 R2	Sistemi Operativi installati ed aggiornati	ARPAE
Integrazione server con Dominio esistente	Effettuare l'accesso al dominio del Server Triton Manager e creazione del Domain User Triton	Join al Dominio e Domain Users creati	ARPAE
OPZIONALE Predisposizione Microsoft SQL	Installazione SQL Server come da Forcepoint Requirements e	Database SQL 2012/2014 installato e fruibile	ARPAE

ATTIVITA'	CONTENUTI	Obiettivo	Responsabilità
Server, creazione Database	relative utenze.		
Installazione ForcePoint TRITON Infrastructure Manager 8.4	Verifica conformità requisiti di sistema, installazione software Triton Manager	Triton Manager e Reporting DB attivi	RTI
Test funzionali di importazione utenze Active Directory	Verifica integrazione Triton con dominio	Integrazione con AD	RTI + ARPAE

5.5.1.3 Attività di migrazione e configurazione policy servizio SWG

Di seguito vengono definite le attività previste nelle giornate dedicate alla migrazione / merge delle configurazioni web filtering attualmente in produzione con la nuova infrastruttura Triton AP-WEB

Tabella 8: Attività di migrazione del servizio SWG.

ATTIVITA'	CONTENUTI	Obiettivo	Responsabilità
Analisi, bonifica ed export delle policy da Websense Web Filtering a Triton	Bonifica e replica delle Policy	Policy AP-WEB utenti nuovo Triton importate	RTI + ARPAE
Verifiche funzionamento nuova architettura AP-WEB	Spostamento della navigazione di utenze pilota sui nuovi appliance per validazione funzionalità e policy	Test navigazione, policy e reporting nuova architettura	RTI + ARPAE
Passaggio in produzione tramite modifica puntamento su V5000	Rilascio in produzione nuovo Triton + V5000 aggiornato	Rilascio in produzione	RTI + ARPAE
Monitoraggio funzionamento e stabilità nuova architettura	Monitoring ed eventuale tuning	Certificazione rilascio in produzione	RTI + ARPAE
Training nuove funzionalità con formazione personale di presidio	Training rivolto al personale tecnico, per formarlo sulle basilari e principali funzionalità di ForcePoint AP-WEB e AP-DATA v8.4	Formazione del personale	RTI
Rilascio documentazione aggiornata			RTI

Deliverable. Migrazione dalla vecchia piattaforma ed attivazione del nuovo servizio SWG

5.5.2 SERVIZI PROFESSIONALI PER INTEGRAZIONI NUOVE FUNZIONALITÀ HYBRID WEB + DATA DISCOVERY

Su richiesta dell'Amministrazione il servizio professionale per l'integrazione delle funzionalità di Hybrid Web e Data Discovery saranno erogati in modalità "on premise". In fase di attivazione del servizio professionale a supporto, il fornitore eseguirà le seguenti attività al fine di rendere la piattaforma operativa:

- Update del Forcepoint Security Manager (Triton APX)
  - La macchina che ospiterà la nuova versione di FSM dovrà essere in linea con I requisiti riportati al seguente link: *https://www.websense.com/content/support/library/deployctr/v84/dic_sys_req.aspx*
- Sostituzione delle appliance esistenti con le nuove nuovi V5000 G4
  - Necessario collegamento ad Internet per l'aggiornamento delle hotfix

- Attivazione licenze
- Deployment agent DLP a bordo dei client
    - Il fornitore genera del pacchetto .msi da distribuire ai client e supporta l'amministrazione durante l'installazione. L'installazione può essere fatta tramite SCCM ed è in carico all'amministrazione.
- Attivazione Hybrid Module Web
- Deployment agent Hybrid Module a bordo dei client
    - Il fornitore genera del pacchetto .msi da distribuire ai client e supporta l'amministrazione durante l'installazione. L'installazione può essere fatta tramite SCCM ed è in carico all'amministrazione.

Al termine dell'attività di installazione sarà rilasciato un documento riportante le seguenti informazioni:

- Descrizione di alto livello dell'architettura;
- Descrizione dei collegamenti fisici;
- Descrizione delle configurazioni realizzate;

Il documento riporterà solo le informazioni riguardanti le componenti di fornitura.

5.5.3 SERVIZI PROFESSIONALI PER INSTALLAZIONE ARSS PER FIRMA DIGITALE

Tutte le attività di seguito elencate saranno svolte presso le sedi dell'RTI e di Aruba.

5.5.3.1 Installazione e configurazione ARSS

L'ARSS verrà installato su un server messo a disposizione dall'Amministrazione presso il suo centro elaborazione dati e configurato secondo le esigenze.
Di seguito i requisiti minimi del server:

- Sistema operativo Linux o Windows;
- Almeno 2 CPU;
- Almeno 8GB di RAM;
- HDD da 320GB (con log residenti);
- Tomcat (ultima versione disponibile);
- Oracle Java (ultima versione disponibile).

Deliverable: Installazione e configurazione ARSS

5.5.4 SERVIZI PROFESSIONALI OPZIONALI DI SUPPORTO PER FIRMA DIGITALE

Il cliente ha 2 applicazioni da integrare con la firma remota:

- una che gestisce le analisi di laboratorio
- l'altra i documenti amministrativi.

Il cliente non ha previsto giornate professionali per il supporto, ma necessita soltanto della documentazione base. Saranno comunque previste delle giornate di supporto per l'integrazione da fatturare eventualmente a consumo.

Deliverable: Giornate di supporto a consumo.

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.

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 9.

Tabella 9: 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.

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 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 10: Quantità e costi.

SERVIZI DI FIRMA DIGITALE REMOTA, TIMBRO ELETTRONICO, MARCHE TEMPORALI E CERTIFICATI SSL (L2.S2)										
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Profilo**	**Q.tà 2017**	**Q.tà 2018**	**Q.tà 2019**	**Q.tà 2020**	**Q.tà 2021**
L2.S2.1	FIRMA DIGITALE REMOTA	As a service	A canone (canone annuale per utente)	fino a 50 utenti	Modalità "best effort" (senza alcuno SLA)	0	50	50	50	50
				da 51 a 200 utenti		0	150	150	150	150
				da 201 a 1.000 utenti		0	100	300	400	400
				oltre 1.000 utenti		0	0	0	0	0
				1 firma al secondo garantita	SLA garantito					
				4 firme al secondo garantite aggiuntive						
				5 firme al secondo garantite aggiuntive						

SERVIZI DI SICUREZZA (L2.S3)										
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Profilo**	**Q.tà 2017**	**Q.tà 2018**	**Q.tà 2019**	**Q.tà 2020**	**Q.tà 2021**
L2.S3.5	DATA LOSS/LEAK PREVENTION	As a service	A canone (canone annuale per endpoint)	fino a 500 endpoint		500	500	500	500	500
				da 501 a 1.000 endpoint		500	500	500	500	500
				oltre 1.000 endpoint		350	350	350	350	350
L2.S3.8	SECURE WEB GATEWAY	As a service	A canone (canone annuale per singola pdli)	fino a 100 pdli		100	100	100	100	100
				da 101 a 1.000 pdli		900	900	900	900	900
				da 1.001 a 5.000 pdli		350	350	350	350	350
				oltre 5.000 pdli		0	0	0	0	0

SERVIZI PROFESSIONALI DI SICUREZZA (L2.S3)									
Codice	**Tipologia d'erogazione**	**Valutazione economica**	**Profilo**	**Q.tà 2017**	**Q.tà 2018**	**Q.tà 2019**	**Q.tà 2020**	**Q.tà 2021**
L2.S3.9	Normale orario di lavoro (8 ore)	A corpo (gg/uu)	Capo progetto	38	5	0	0	0
			Security architect	65	0	0	0	0
			Specialista di tecnologia/prodotto Senior	70	10	0	0	0
			Specialista di tecnologia/prodotto	0	0	0	0	0

Riepilogo Servizi	2017 (2m)	2018 (12m)	2019 (12m)	2020 (12m)	2021 (6m)
Servizio L2.S2.1 - Firma digitale remota	€ 0,00	€ 3.022,50	€ 4.722,50	€ 5.572,50	€ 2.786,25
Servizio L2.S3.5 - Data loss/leak prevention	€ 2.550,00	€ 15.300,00	€ 15.300,00	€ 15.300,00	€ 7.650,00
Servizio L2.S3.8 - Secure Web Gateway	€ 2.371,67	€ 14.230,00	€ 14.230,00	€ 14.230,00	€ 7.115,00
Servizio L2.S3.10 - Servizi professionali	€ 56.288,50	€ 4.450,00	€ 0,00	€ 0,00	€ 0,00
Subtotali per anno	€ 61.210,17	€ 37.002,50	€ 34.252,50	€ 35.102,50	€ 17.551,25
TOTALE Progetto dei Fabbisogni	€ 185.118,92				

A.2.1 Fatturazione SP01-L2.S3.9

I servizi di Firma Digitale Remota (L2.S2.1), Data Loss/Leak Prevention (L2.S3.5) e Secure Web Gateway (L2.S3.8) saranno fatturati a canone bimestrale.

I servizi professionali SP-01-L2.S3.9, a supporto di tutte le attività, saranno fatturati a task secondo i deliverable riportati nei Par.5.5.1, 5.5.2 e 5.5.3.

A valle delle verifiche dell'Amministrazione (art 15 dell'Accordo Quadro), i servizi professionali SP-02-L2.S3.9, SP-03-L2.S3.9 ed SP-04-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.

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.

B.1.1 Firma Digitale

Firme Remote

N.600 Firme Remote con OTP Display da utilizzare attraverso integrazione applicativa (ARSS). La data prevista d'attivazione del servizio è uguale a T0 (firma del contratto) +45 gg.

L'emissione delle firme sarà gestita in autonomia dall'Amministrazione una volta aver compilato i moduli per diventare CDRL e aver nominato gli OdR.

Le firme verranno rilasciate come previsto dal paragrafo A4 del capitolo Appendice A "Progetto di Attuazione"

B.1.2 DLP / SWG

#	Nome attività	Inizio	Fine	Vincoli
1	Attivazione del Servizio di Data Leak/Loss Prevention	T0 + XXgg	30/06/2021	
2	Attivazione del Servizio di Secure Web Gateway	T0 + XXgg	30/06/2021	
3	Servizi Professionali di migrazione DLP/SWG	T0 + XXgg	T0 + 2mesi	
4	Servizi Professionali di integrazione nuove funzionalità su DLP/SWG	T0 + XXgg	T0 + 2mesi	

Tabella 11: Piano di attivazione.

ALLEGATO D – SCHEMA DI CONTRATTO ESECUTIVO - LOTTO 2

INDICE

1. DEFINIZIONI 4
2. VALORE DELLE PREMESSE E DEGLI ALLEGATI 5
3. OGGETTO DEL CONTRATTO ESECUTIVO 5
4. EFFICACIA E DURATA 5
5. PIANO DEI FABBISOGNI E PROGETTO DEI FABBISOGNI 5
6. EROGAZIONE DEI SERVIZI 5
7. GESTIONE DEL CONTRATTO ESECUTIVO 6
8. ATTIVAZIONE E DISMISSIONE DEI SERVIZI 6
9. LOCALI MESSI A DISPOSIZIONE DELLA AMMINISTRAZIONE 7
10. VERIFICHE - COLLAUDI 7
11. PENALI 8
12. CORRISPETTIVI 8
13. FATTURAZIONE E PAGAMENTI 8
14. GARANZIA DELL'ESATTO ADEMPIMENTO 9
15. SUBAPPALTO 10
16. DIVIETO DI CESSIONE DEL CONTRATTO 10
17. RISOLUZIONE E RECESSO 10
18. FORZA MAGGIORE 11
19. RESPONSABILITA' CIVILE 12
20. TRACCIABILITÀ DEI FLUSSI FINANZIARI – ULTERIORI CLAUSOLE RISOLUTIVE ESPRESSE12
21. ONERI FISCALI E SPESE CONTRATTUALI 13
22. FORO COMPETENTE 13
23. TRATTAMENTO DEI DATI PERSONALI 14

CONTRATTO ESECUTIVO

TRA

_____, con sede in _____, Via _____, C.F. _____, in persona del legale rappresentante*pro tempore* _____ giusta poteri allo stesso conferiti dallo statuto sociale e dalla deliberazione di aggiudicazione del Consiglio di Amministrazione in data _____ (nel seguito per brevità anche "***Amministrazione***"),

E

Leonardo – Finmeccanica - Società per azioni, in forma abbreviata Leonardo S.p.a. o Finmeccanica S.p.a., sede legale in Roma, Piazza Monte Grappa 4, capitale sociale Euro 2.543.861.738,00=, iscritta al Registro delle Imprese di Roma al n. 00401990585, P. IVA 00881841001, domiciliata ai fini del presente atto in Roma, Piazza Monte Grappa 4, in persona del Procuratore e legale rappresentante Ing. Andrea Biraghi , nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa la mandante ***IBM Italia S.p.A.,*** Società con unico azionista, soggetta all'attività di direzione e coordinamento di "International Business Machines Corporation" (U.S.A.)*con* sede legale e domicilio fiscale in Segrate (Milano), C.A.P. 20090, Circonvallazione Idroscalo, capitale sociale Euro 347.256.998,80 interamente versato =,iscritta al Registro delle Imprese di Milano al n. 01442240030, P. IVA 10914660153, domiciliata ai fini del presente atto in Segrate (Milano) C.A.P. 20090, Circonvallazione Idroscalo, e la mandante ***Fastweb S.p.A.,*** *Società a Socio Unico soggetta all'attività di direzione e coordinamento di Swisscom AG* , con sede legale in Milano, Via Caracciolo n. 51, capitale sociale Euro 41.344.209,40 =, iscritta al Registro delle Imprese di Milano al n. 12878470157, P. IVA 12878470157, domiciliata ai fini del presente atto in Piazzale Luigi Sturzo 23 - 00144 Roma e la mandante Sistemi Informativi S.r.l., Società con socio unico, Società soggetta a direzione e coordinamento di IBM Italia S.p.A., con sede legale in Roma, Via Carlo Veneziani n. 58, capitale sociale Euro 2.697.375,00 =, iscritta al Registro delle Imprese di Roma al n. 06310880585, P. IVA 01528071002, domiciliata ai fini del presente atto in Roma, via Carlo Veneziani n. 58, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott.ssa Sandra de Franchis repertorio n. 6129 raccolta n. 2755 (nel seguito per brevità congiuntamente anche "***Fornitore***")

PREMESSO CHE

(A) L'art. 20, comma 4, del D.L. n. 83/2012, come convertito con modificazioni dalla Legge 7 agosto 2012 , n. 134, ha affidato a Consip S.p.A., a decorrere dalla data di entrata in vigore della legge di conversione del decreto medesimo, "le attività amministrative, contrattuali e strumentali già attribuite a DigitPA, ai fini della realizzazione e gestione dei progetti in materia, nel rispetto delle disposizioni del comma 3".

(B) L'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge 2012/135, ha stabilito che, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, Consip S.p.A. svolge altresì le attività di centrale di committenza

relativamente “ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311”.

(C) Ai sensi dell'articolo 1, comma 192, della L. n. 311/2004, “Al fine di migliorare l'efficienza operativa della pubblica amministrazione e per il contenimento della spesa pubblica, con decreto del Presidente del Consiglio dei ministri sono individuati le applicazioni informatiche e i servizi per i quali si rendono necessarie razionalizzazioni ed eliminazioni di duplicazioni e sovrapposizioni. Il CNIPA stipula contratti-quadro per l'acquisizione di applicativi informatici e per l'erogazione di servizi di carattere generale riguardanti il funzionamento degli uffici con modalità che riducano gli oneri derivanti dallo sviluppo, dalla manutenzione e dalla gestione”.

(D) Consip S.p.A., ai sensi dell’art. 54 del D.Lgs. n. 163/2006, ha indetto una gara a procedura ristretta, suddivisa in 4 lotti, come da bando pubblicato sulla Gazzetta Ufficiale dell’Unione Europea n. S251 del 28/12/2013 e sulla Gazzetta Ufficiale della Repubblica Italiana n. 151 del 27/12/2013, inviando al Fornitore la lettera di invito a presentare offerta, prot. 24280/2014 in data 19 settembre 2014.

(E) Il Fornitore è risultato aggiudicatario del Lotto 2 della predetta gara, ed ha stipulato il relativo Contratto Quadro in data 20 luglio 2016.

(F) In applicazione di quanto stabilito nel predetto Contratto Quadro, ciascuna Amministrazione beneficiaria del Contratto Quadro utilizza il medesimo mediante la stipula di Contratti esecutivi, attuativi del Contratto Quadro stesso.

(G) L’Amministrazione ha svolto ogni attività prodromica necessaria alla stipula del presente Contratto Esecutivo.

(H) l’Amministrazione - in ottemperanza alla vigente normativa in materia di sicurezza sui luoghi di lavoro - ha integrato il “Documento di valutazione dei rischi standard da interferenze” allegato ai documenti di gara, riferendolo ai rischi specifici da interferenza presenti nei luoghi in cui verrà espletato il presente appalto, indicando i costi relativi alla sicurezza;

(I) il CIG del presente Contratto Esecutivo è il seguente: _____;

L) il Codice univoco ufficio per Fatturazione è il seguente: _____.

TUTTO CIÒ PREMESSO SI CONVIENE E SI STIPULA QUANTO SEGUE:

1. DEFINIZIONI

1.1 I termini contenuti nel presente Contratto Esecutivo hanno il significato specificato, nel Contratto Quadro e nei relativi Allegati, salvo che il contesto delle singole clausole disponga diversamente.

1.2 I termini tecnici contenuti nel presente Contratto Esecutivo hanno il significato specificato nel Capitolato Tecnico, salvo che il contesto delle singole clausole disponga diversamente.

1.3 Il presente Contratto Esecutivo è regolato in via gradata:

a) dalle disposizioni del presente atto e dai suoi allegati, che costituiscono la manifestazione integrale di tutti gli accordi intervenuti tra il Fornitore e l’Amministrazione relativamente alle attività e prestazioni contrattuali;

b) dalle disposizioni del Contratto Quadro e dai suoi allegati;
c) dalle disposizioni di cui al D.Lgs. n. 82/2005;
d) dal codice civile e dalle altre disposizioni normative in vigore in materia di contratti di diritto privato.

2. VALORE DELLE PREMESSE E DEGLI ALLEGATI

2.1 Le premesse di cui sopra, gli atti e i documenti richiamati nelle medesime premesse e nella restante parte del presente atto, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del presente Contratto Esecutivo .

2.2 Costituiscono, altresì, parte integrante e sostanziale del presente Contratto Esecutivo:
- il Contratto Quadro,
- gli Allegati del Contratto Quadro,
- l'Allegato 1 "Progettodei Fabbisogni" di cui all'art. 7 del Contratto Quadro.

2.3 In particolare, per ogni condizione, modalità e termine per la prestazione dei servizi oggetto contrattuale che non sia espressamente regolata nel presente atto, vale tra le Parti quanto stabilito nel Contratto Quadro, ivi inclusi gli Allegati del medesimo, con il quale devono intendersi regolati tutti i termini del rapporto tra le Parti.
Infatti, le Parti espressamente convengono che il predetto Contratto Quadro, ha valore di regolamento e pattuizione per il presente Contratto Esecutivo.

3. OGGETTO DEL CONTRATTO ESECUTIVO

3.1 Il presente Contratto Esecutivo definisce i termini e le condizioni che, unitamente alle disposizioni contenute nel Contratto Quadro, regolano la prestazione in favore della Amministrazione da parte del Fornitore dei **Servizi di gestione delle identità digitali e sicurezza applicativa** e, precisamente, dei servizi che saranno forniti con il Progetto dei Fabbisogni di cui all'Allegato 1.

3.2 I predetti servizi dovranno essere prestati con le modalità ed alle condizioni stabilite nel presente Contratto Esecutivo, nonché nel Contratto Quadro e relativi allegati.

4. EFFICACIA E DURATA

4.1 Il presente Contratto Esecutivo ha una durata pari a _____ *(indicare la durata contrattuale in ragione dei servizi richiesti, secondo quanto stabilito nel paragrafo 3.2 del Capitolato Tecnico Parte Generale*), salvi i casi di risoluzione o recesso ai sensi, rispettivamente, degli artt. 24 e 25 del Contratto Quadro.

5. PIANO DEI FABBISOGNI E PROGETTO DEI FABBISOGNI

5.1 Per le modalità e termini stabiliti per la definizione e le variazioni del Piano dei fabbisogni e del Progetto dei fabbisogni, vale tra le Parti quanto stabilito negli articolo 7 e 8 del Contratto Quadro e nel Capitolato Tecnico.

6. EROGAZIONE DEI SERVIZI

6.1 Il Fornitore ha l'obbligo di avviare l'erogazione dei servizi di cui al precedente art.3 in favore dell'Amministrazione entro quanto previsto nel Progetto dei Fabbisogni di cui all'Allegato 1, pena l'applicazione delle penali di cui oltre.

6.2 Il Fornitore, almeno 20 (venti) giorni lavorativi dalla richiesta dell'Amministrazione, consegnerà alla stessa la documentazione di cui all'art. 9.2 del Contratto Quadro e, qualora nei 20 (venti) giorni dalla ricezione l'Amministrazione stessa richieda modifiche o integrazioni alla suddetta documentazione, il Fornitore dovrà recepirle entro i 10 (dieci) giorni lavorativi successivi.

6.3 Per tutte le attività necessarie alla realizzazione del Piano di Attuazione del Progetto dei Fabbisogni, il Fornitore deve sottoporre all'Amministrazione, con cadenza mensile a partire dalla data di approvazione del Progetto stesso ed entro il giorno 15 del mese successivo al mese di riferimento, uno "stato di avanzamento", soggetto ad approvazione da parte dell'Amministrazione stessa, redatto secondo quanto indicato all'art. 9.4 del Contratto Quadro.

7. GESTIONE DEL CONTRATTO ESECUTIVO

7.1 Nell'esecuzione del presente Contratto Esecutivo, il Fornitore nomina le figure di Responsabile del contratto esecutivo e di Responsabile tecnico, quali interfacce dell'Amministrazione, che dovranno essere operative entro 10 (dieci) giorni solari dalla data di stipula del predetto Contratto Quadro.

7.2 Le attività tecniche di supervisione e controllo della corretta esecuzione del presente Contratto Esecutivo, in relazione ai servizi richiesti, sono svolte dalla Amministrazione d'intesa con AgID.

7.3 Le attività amministrative di supervisione e controllo del presente Contratto Esecutivo sono svolte dall'Amministrazione, con l'eventuale supporto di Consip S.p.A.

7.4 Entro 10 (dieci) giorni lavorativi dalla data di stipula del presente Contratto Esecutivo, il Fornitore comunicherà all'Amministrazione i dati relativi al soggetto referente per l'esecuzione delle prestazioni contrattuali (Rappresentante del Fornitore).

7.5 Entro 10 (dieci) giorni lavorativi dalla data di stipula del presente Contratto Esecutivo, l'Amministrazione comunicherà al Fornitore i dati relativi al Referente dell'Amministrazione, al quale sono demandate le attività di cui all'art. 12.8 del Contratto Quadro.

8. ATTIVAZIONE E DISMISSIONE DEI SERVIZI

8.1 L'attivazione dei servizi avverrà nei tempi e nei modi di cui al Capitolato Tecnico ed al Progetto dei Fabbisogni. Le eventuali attività di migrazione dovranno, in ogni caso, concludersi entro i termini contenuti nel Piano di Attuazione.

8.2 L'Amministrazione provvederà a concordare con il Fornitore dal quale i servizi dovranno essere migrati, la sua partecipazione alle attività che ne richiedano l'intervento.

8.3 Il Fornitore dovrà presentare all'Amministrazione, entro 10 (dieci) giorni lavorativi dalla stipula del Contratto Esecutivo, i curriculum vitae delle risorse di cui al paragrafo 8.2 del Capitolato tecnico Parte Generale.

8.4 Alla scadenza del presente Contratto Esecutivo o in caso di risoluzione o recesso dallo stesso, il Fornitore si impegna a porre in essere tutte le attività necessarie o utili al fine di permettere la migrazione dei servizi offerti in base al predetto Contratto Esecutivo al nuovo fornitore assegnatario di una, più di una, o tutte le Amministrazioni assegnate al Fornitore.

9. LOCALI MESSI A DISPOSIZIONE DELLA AMMINISTRAZIONE

9.1 L'Amministrazione provvede ad indicare ed a mettere a disposizione del Fornitore, in comodato gratuito ed in uso non esclusivo, locali idonei all'installazione degli eventuali apparati del Fornitore necessari all'erogazione dei servizi richiesti, con le modalità indicate nel Piano dei Fabbisogni.

9.2 L'Amministrazione garantisce al Fornitore:

- lo spazio fisico necessario per l'alloggio delle apparecchiature ed idoneo ad ospitare le apparecchiature medesime;
- l'alimentazione elettrica delle apparecchiature di adeguata potenza; sarà cura del Fornitore provvedere ad adottare ogni misura per la garantire la continuità della alimentazione elettrica.

9.3 L'Amministrazione non garantisce il condizionamento dei locali. Il Fornitore valuterà l'opportunità di provvedere, a propria cura e spese, alla climatizzazione del locale, avendo in tale caso diritto a disporre di una canalizzazione verso l'esterno.

9.4 Il Fornitore provvede a visitare i locali messi a disposizione dall'Amministrazione ed a segnalare, entro e non oltre 10 (dieci) giorni lavorativi prima della data di disponibilità all'attivazione, l'eventuale inidoneità tecnica degli stessi.

9.5 Nel caso in cui l'Amministrazione rendesse disponibili i locali in ritardo, rispetto alle date di disponibilità al collaudo previste nel Piano di Attuazione, verrà aggiunto, alle date stesse, un numero di giorni pari a quelli di ritardo.

9.6 L'Amministrazione consentirà al personale del Fornitore o a soggetti da esso indicati, muniti di documento di riconoscimento, l'accesso ai propri locali per eseguire eventuali operazioni rientranti nell'oggetto del presente Contratto esecutivo. Le modalità dell'accesso saranno concordate fra le Parti al fine di salvaguardare la legittima esigenza di sicurezza dell'Amministrazione. Il Fornitore è tenuto a procedere allo sgombero, a lavoro ultimato, delle attrezzature e dei materiali residui.

9.7 L'Amministrazione successivamente al collaudo positivo di cui al successivo art. 10 metterà in essere quanto possibile perché gli apparati del Fornitore presenti nei suoi locali non vengano danneggiati o manomessi, pur non assumendosi responsabilità se non quelle derivanti da dolo o colpa grave del proprio personale.

10. VERIFICHE - COLLAUDI

10.1 Nel periodo di efficacia del presente Contratto esecutivo, il Referente dell'Amministrazione avrà facoltà di eseguire verifiche relative alla conformità dei servizi erogati al Capitolato Tecnico ed alla relativa Appendice "Indicatori di qualità della fornitura", Allegato A del Contratto Quadro, nonché sulla rispondenza dei servizi richiesti al Progetto dei Fabbisogni e sul rispetto del Piano di Attuazione. Il Fornitore è tenuto a prestare tutta l'assistenza e la strumentazione necessaria all'effettuazione di tali verifiche.

10.2 Il Fornitore, a fronte dei rilievi trasmessi dalla Amministrazione mediante apposita comunicazione in relazione ai risultati delle verifiche di cui al precedente art. 10.1, si impegna a presentare, entro 15 (quindici) giorni lavorativi dal ricevimento della predetta comunicazione, un piano di rientro che dovrà essere implementato nei successivi 30 (trenta) giorni lavorativi entro i quali il Fornitore dovrà dare comunicazione di "pronto

alla verifica".

10.3 Previo esito positivo del collaudo in test bed eseguito da Consip S.p.A. secondo quanto previsto dall'art. 15 del Contratto Quadro, i servizi oggetto del presente Contratto Esecutivo saranno sottoposti ad un ulteriore collaudo "sul campo" da parte della Amministrazione alle date indicate nel Piano di Attuazione del Progetto dei Fabbisogni.

10.4 I termini e le modalità del collaudo da parte dell'Amministrazione di cui al precedente art. 10.2 sono descritte nel Capitolato Tecnico o definite nel Progetto dei Fabbisogni approvato.

10.5 In ogni caso, l'Amministrazione procederà alle verifiche di conformità delle prestazioni eseguite dal Fornitore al fine di accertarne la regolare esecuzione ai sensi degli artt. 312 e ss., del D.Lgs. n. 163/2006, anche facendo ricorso alla documentazione contrattuale prodotta da Fornitore o, comunque, di contenuto analogo attestante la conformità delle prestazioni eseguite alle prescrizioni contrattuali.

11. PENALI

11.1 Nell'ipotesi di ritardo nell'adempimento e/o di difformità di prestazione nell'esecuzione dei servizi o, comunque, delle attività contrattuali, non imputabile all'Amministrazione, ovvero a forza maggiore o caso fortuito, rispetto a quanto previsto nell'Appendice "Indicatori di qualità della fornitura" del Capitolato Tecnico, Allegato A del Contratto Quadro, l'Amministrazione applicherà al Fornitore le penali ivi dettagliatamente descritte e regolate, qui da intendersi integralmente trascritte, fatto comunque salvo il risarcimento del maggior danno.

11.2 Per le modalità di contestazione ed applicazione delle penali vale tra le Parti quanto stabilito all'articolo 16 del Contratto Quadro.

12. CORRISPETTIVI

12.1 I corrispettivi dovuti al Fornitore per i servizi prestati in esecuzione del presente Contratto Esecutivo sono determinati in ragione dei prezzi unitari stabiliti nell'Allegato C del Contratto Quadro da intendersi validi sino all'esecuzione della procedura di adeguamento di cui all'art. 20 del Contratto Quadro; ogni aggiornamento degli stessi sostituisce ed annulla i precedenti prezzi unitari.

12.2 Detti corrispettivi sono maturati con periodicità bimestrale in ragione dei servizi effettivamente prestati nel rispetto del Progetto dei Fabbisogni, nell'ultima versione approvata.

13. FATTURAZIONE E PAGAMENTI

13.1 La fattura relativa ai corrispettivi maturati secondo quanto previsto al precedente art. 12 viene emessa ed inviata dal Fornitore all'esito delle verifiche di conformità, tra le quali l'allineamento tra il Piano dei Fabbisogni ed il Progetto dei Fabbisogni, e saranno corrisposti dall'Amministrazioni secondo la normativa vigente in materia di Contabilità delle Amministrazioni e previo accertamento della prestazione effettuate. Ciascuna fattura, inviata via fax o PEC, verrà corrisposta nel termine stabilito nel Contratto Quadro. In caso di ritardo nei pagamenti, il tasso di mora viene stabilito in una misura pari al tasso BCE stabilito semestralmente e pubblicato con comunicazione del Ministero

dell'Economia e delle Finanze sulla G.U.R.I., maggiorato di 8 punti, secondo quanto previsto nell'art. 5 del D.Lgs. n. 231/2002.

13.2 Ciascuna fattura dovrà essere emessa nel rispetto di quanto prescritto dall'art. 19.5 del Contratto Quadro.

13.3 L'Amministrazione opererà sull'importo netto progressivo delle prestazioni una ritenuta dello 0,5% (zero virgola cinque per cento) che verrà liquidata dalle stesse solo al termine del presente Contratto Esecutivo e previa acquisizione del documento unico di regolarità contributiva.

13.4 Resta tuttavia espressamente inteso che in nessun caso il Fornitore potrà sospendere la prestazione dei servizi e, comunque, delle attività previste nel presente Contratto Esecutivo. Qualora il Fornitore si rendesse inadempiente a tale obbligo, i singoli Contratti Esecutivi e il presente Contratto Quadro potranno essere risolti di diritto mediante semplice ed unilaterale dichiarazione da comunicarsi da parte dell'Amministrazione con lettera raccomandata A/R.

13.5 I corrispettivi saranno accreditati, a spese del Fornitore, sul conto corrente n. _____, intestato al Fornitore presso _____, Codice IBAN _____; il Fornitore dichiara che il predetto conto opera nel rispetto della Legge 13 agosto 2010 n. 136 e si obbliga a comunicare le generalità e il codice fiscale del/i delegato/i ad operare sul/i predetto/i conto/i all'Amministrazione all'atto del perfezionamento del presente Contratto Esecutivo.

13.6 Il Fornitore, al termine di ogni anno solare, invierà all'Amministrazione e a Consip S.p.A. una relazione consuntiva del fatturato globale, suddivisa per tipo di servizio e con i prezzi unitari applicati.

13.7 Le Parti prendono atto che l'Amministrazione si è registrata/non si è registrata alla "Piattaforma per la certificazione dei crediti" di cui ai Decreti Ministeriali 22/05/2012 e 25/06/2012, in conformità a quanto previsto dai Decreti stessi.

14. GARANZIA DELL'ESATTO ADEMPIMENTO

14.1 A garanzia dell'esatto e tempestivo adempimento degli obblighi contrattuali di cui al presente Contratto Esecutivo, il Fornitore, entro il termine perentorio di 15 (quindici) giorni solari dalla data di stipula del predetto Contratto, costituirà a proprie spese idonea garanzia in favore dell'Amministrazione per un ammontare pari al ____% (per cento) del valore del Contratto Esecutivo medesimo; tale garanzia potrà essere prestata mediante fidejussione bancaria o polizza fideiussoria ed il relativo certificato dovrà essere consegnato all'Amministrazione entro il predetto termine perentorio.La garanzia dovrà prevedere la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'art. 1957, comma 2, del codice civile, nonché l'operatività della garanzia medesima entro quindici giorni, a semplice richiesta scritta dell'Amministrazione.

14.2 La fidejussione o polizza fidejussoria di cui al precedente comma dovrà essere valida per tutta la durata del presente Contratto Esecutivo e, comunque, sino alla completa ed esatta esecuzione delle obbligazioni nascenti dal predetto contratto e sarà svincolata, secondo le modalità ed alle condizioni previste dalla normativa vigente.

14.3 Qualora l'ammontare della garanzia di cui al presente articolo dovesse ridursi per effetto

dell'applicazione di penali, o per qualsiasi altra causa (tra cui anche l'incremento del Valore del Contratto Esecutivo a seguito di una modifica del Piano dei Fabbisogni), il Fornitore dovrà provvedere al reintegro entro il termine di 10 (dieci) giorni lavorativi dal ricevimento della relativa richiesta effettuata.

14.4 In caso di inadempimento alle obbligazioni previste nel presente articolo, l'Amministrazione ha facoltà di dichiarare risolto il presente Contratto Esecutivo, fermo restando il risarcimento del danno.

14.5 La prestazione della garanzia ai sensi del presente articolo non limita l'obbligo del Fornitore di provvedere all'integrale risarcimento dei danni tutti, anche ove gli stessi siano di valore superiore all'importo garantito.

15. SUBAPPALTO

15.1 Il Fornitore, conformemente a quanto dichiarato in sede di offerta, si è riservato di affidare in subappalto, in misura non superiore al 30% dell'importo contrattuale, l'esecuzione delle seguenti prestazioni:

a) Servizi di gestione delle identità digitali;

b) Servizi di firma digitale remota e di timbro elettronico;

c) Servizi di sicurezza applicativa "as a service";

d) Servizi professionali a supporto dell'Unità Locale di Sicurezza e delle attività in ambito di sicurezza applicativa;

e) Servizi di monitoraggio in ambito sicurezza.

nell'osservanza di quanto previsto dall'art. 22 del Contratto Quadro.

16. DIVIETO DI CESSIONE DEL CONTRATTO

16.1 È fatto assoluto divieto al Fornitore di cedere, a qualsiasi titolo, il presente Contratto Esecutivo, a pena di nullità della cessione medesima e risoluzione in danno del Contratto medesimo per causa del Fornitore.

In particolare, in caso di inadempimento da parte del Fornitore degli obblighi di cui al presente articolo, l'Amministrazione, fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare risolto di diritto il presente Contratto Esecutivo.

17. RISOLUZIONE E RECESSO

17.1 In caso di inadempimento del Fornitore anche a uno solo degli obblighi assunti con la stipula del presente Contratto Esecutivo che si protragga oltre il termine, non inferiore comunque a 15 (quindici) giorni, che verrà assegnato a mezzo di raccomandata A/R dall'Amministrazione, la medesima Amministrazione ha la facoltà di considerare risolto di diritto il predetto Contratto Esecutivo e di ritenere definitivamente la garanzia di cui al precedente art. 14, ove essa non sia stata ancora restituita, e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno.

17.2 Ferme restando le ulteriori ipotesi di risoluzione previste negli articoli 135 e ss. del D.Lgs. n. 163/2006, si conviene che, in ogni caso, la Amministrazione, senza bisogno di assegnare previamente alcun termine per l'adempimento, potrà risolvere di diritto ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione

da comunicarsi al Fornitore con raccomandata A/R, il presente Contratto Esecutivo nei casi previsti dall'art. 24 del Contratto Quadro.

17.3 In tutti i casi di risoluzione, anche parziale, del presente Contratto Esecutivo, non saranno pregiudicati i diritti di ciascuna Parte esistenti prima della data di risoluzione, nonché tutti gli altri diritti previsti dalla legge, ivi incluso il diritto al risarcimento del danno.

17.4 In tutti le ipotesi di risoluzione di cui al presente art. 17, e nelle ulteriori ipotesi di risoluzione contenute nel presente Contratto Esecutivo, quest'ultimo sarà risolto di diritto. In tal caso, nonché in caso di recesso dell'Amministrazione ai sensi del successivo art. 17.5, il Fornitore dovrà porre in essere tutte le attività necessarie alla migrazione dei servizi oggetto del presente Contratto Esecutivo risolto secondo quanto previsto dal precedente art. 8.4.

17.5 Qualora Consip S.p.A. eserciti la facoltà di recesso dal Contratto Quadro in tutto o in parte, l'Amministrazione re potrà recedere dal presente Contratto Esecutivo.

17.6 A decorrere dal 12° (dodicesimo) mese successivo alla stipula del presente Contratto Esecutivo, l'Amministrazione ha diritto di recedere motivatamente dal presente contratto in qualsiasi momento, con preavviso di almeno 60 (sessanta) giorni solari, da comunicarsi al Fornitore a mezzo PEC o con lettera raccomandata A/R. In tale caso, il Fornitore ha diritto al pagamento da parte dell'Amministrazione dei servizi prestati, purché eseguiti correttamente ed a regola d'arte, secondo il corrispettivo e le condizioni previste nel presente Contratto Esecutivo e nel Contratto Quadro, rinunciando espressamente, ora per allora, a qualsiasi ulteriore eventuale pretesa, anche di natura risarcitoria, ed a ogni ulteriore compenso e/o indennizzo e/o rimborso, anche in deroga a quanto previsto dall'articolo 1671 cod. civ.

17.7 Dalla data di efficacia del recesso, il Fornitore dovrà cessare tutte le prestazioni contrattuali, assicurando che tale cessazione non comporti danno alcuno all'Amministrazione.

18. FORZA MAGGIORE

18.1 Nessuna Parte sarà responsabile per qualsiasi perdita che potrà essere patita dall'altra Parte a causa di eventi di forza maggiore (che includono, a titolo esemplificativo, disastri naturali, terremoti, incendi, fulmini, guerre, sommosse, sabotaggi, atti del Governo, autorità giudiziarie, autorità amministrative e/o autorità di regolamentazione indipendenti) a tale Parte non imputabili.

18.2 Nel caso in cui un evento di forza maggiore impedisca la fornitura dei servizi da parte del Fornitore, l'Amministrazione, impregiudicato qualsiasi diritto ad essa spettante in base alle disposizioni di legge sull'impossibilità della prestazione, non dovrà pagare i corrispettivi per la prestazione dei servizi interessati fino a che tali servizi non siano ripristinati e, ove possibile, avrà diritto di affidare i servizi in questione ad altro fornitore assegnatario per una durata ragionevole secondo le circostanze.

18.3 L'Amministrazione si impegna, inoltre, in tale eventualità a compiere le azioni necessarie al fine di risolvere tali accordi, non appena il Fornitore le comunichi di essere in grado di erogare nuovamente il servizio.

19. RESPONSABILITA' CIVILE

19.1 Fermo restando quanto previsto dall'art. 27 del Contratto Quadro, il Fornitore assume in proprio ogni responsabilità per infortunio o danni eventualmente subiti da parte di persone o di beni, tanto del Fornitore quanto dell'Amministrazione o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze attinenti all'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi.

20. TRACCIABILITÀ DEI FLUSSI FINANZIARI – ULTERIORI CLAUSOLE RISOLUTIVE ESPRESSE

20.1 Ai sensi e per gli effetti dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136 e s.m.i., il Fornitore si impegna a rispettare puntualmente quanto previsto dalla predetta disposizione in ordine agli obblighi di tracciabilità dei flussi finanziari.

20.2 Ferme restando le ulteriori ipotesi di risoluzione previste nel presente Contratto Esecutivo, si conviene che, in ogni caso, l'Amministrazione, in ottemperanza a quanto disposto dall'art. 3, comma 9 bis, della Legge 13 agosto 2010 n. 136 e s.m.i., senza bisogno di assegnare previamente alcun termine per l'adempimento, risolverà di diritto, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi al Fornitore con raccomandata a.r., il presente Contratto Esecutivo nell'ipotesi in cui le transazioni siano eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri documenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136 e s.m.i., del Decreto Legge 12 novembre 2010 n. 187 nonché della Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici n. 8 del 18 novembre 2010.

20.3 Il Fornitore è tenuto a comunicare tempestivamente e comunque entro e non oltre 7 giorni dalla/e variazione/i qualsivoglia variazione intervenuta in ordine aidati relativi agli estremi identificativi del/i conto/i corrente/i dedicato/i nonché le generalità (nome e cognome) e il codice fiscale delle persone delegate ad operare su detto/i conto/i.

20.4 Il Fornitore, nella sua qualità di appaltatore, si obbliga, a mente dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136 e s.m.i., ad inserire nei contratti sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, una apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 13 agosto 2010 n. 136 e s.m.i.

20.5 Il Fornitore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui all'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i è tenuto a darne immediata comunicazione alla Consip e alla Prefettura – Ufficio Territoriale del Governo della Provincia ove ha sede la stazione appaltante.

20.6 Il Fornitore, si obbliga e garantisce che nei contratti sottoscritti con i subappaltatori e i subcontraenti, verrà assunta dalle predette controparti l'obbligazione specifica di risoluzione di diritto del relativo rapporto contrattuale nel caso di mancato utilizzo del bonifico bancario o postale ovvero degli strumenti idonei a consentire la piena tracciabilità dei flussi finanziari.

Consip S.p.A. verificherà che nei contratti di subappalto sia inserita, a pena di nullità assoluta del contratto, un'apposita clausola con la quale il subappaltatore assume gli obblighi di tracciabilità dei flussi finanziari di cui alla su richiamata Legge.

Con riferimento ai contratti di subfornitura, il Fornitore si obbliga a trasmettere alla Consip, oltre alle informazioni di cui all'art. 118, comma 11 ultimo periodo, anche apposita dichiarazione resa ai sensi del DPR 445/2000, attestante che nel relativo sub-contratto, ove predisposto, sia stata inserita, a pena di nullità assoluta, un'apposita clausola con la quale il subcontraente assume gli obblighi di tracciabilità dei flussi finanziari di cui alla su richiamata Legge, restando inteso che la Consip, si riserva di procedere a verifiche a campione sulla presenza di quanto attestato, richiedendo all'uopo la produzione degli eventuali sub-contratti stipulati, e, di adottare, all'esito dell'espletata verifica ogni più opportuna determinazione, ai sensi di legge e di contratto.

20.7 Ai sensi della Determinazione dell'Autorità per la Vigilanza sui contratti pubblici n. 10 del 22 dicembre 2010, il Fornitore, in caso di cessione dei crediti, si impegna a comunicare il/i CIG/CUP al cessionario, eventualmente anche nell'atto di cessione, affinché lo/gli stesso/i venga/no riportato/i sugli strumenti di pagamento utilizzati. Il cessionario è tenuto ad utilizzare conto/i corrente/i dedicato/i nonché ad anticipare i pagamenti al Fornitore mediante bonifico bancario o postale sul/i conto/i corrente/i dedicato/i del Fornitore medesimo riportando il CIG/CUP dallo stesso comunicato.

21. ONERI FISCALI E SPESE CONTRATTUALI

21.1 Il Fornitore riconosce a proprio carico tutti gli oneri fiscali e tutte le spese contrattuali relative al presente atto.

21.2 Al presente atto, dovrà essere applicata l'imposta di registro in misura fissa, ai sensi dell'art. 40 del D.P.R. 26 aprile 1986 n. 131 e successive modificazioni ed integrazioni.

21.3 Così come previsto dall'art. 26 del Contratto Quadro, ai sensi dell'art. 4, comma 3-quater, del D.L. 6 luglio 2012, n. 95, convertito con modificazioni in legge 7 agosto 2012, n. 135, si applica il contributo di cui all'art. 18, comma 3, D.Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010. Pertanto, le Amministrazioni Beneficiarie sono tenute a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla data di perfezionamento del presente Contratto Esecutivo ,il predetto contributo nella misura prevista dall'art. 2, lettera a) o lettera b), del D.P.C.M. 23 giugno 2010, in ragione del valore complessivo del presente Contratto Esecutivo, determinato sulla base del Progetto dei Fabbisogni approvato dall'Amministrazione Beneficiaria all'atto della stipula del Contratto Esecutivo medesimo.

21.4 In caso di incremento del valore del Contratto Esecutivo a seguito di una modifica del Piano e del Progetto dei Fabbisogni approvato dall'Amministrazione Beneficiaria ai sensi del precedente articolo 8, quest'ultima è tenuta a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla predetta approvazione, un ulteriore contributo nella misura prevista dall'art. 2, lettera c), del D.P.C.M. 23 giugno 2010.

21.5 Le modalità operative di pagamento del predetto contributo sono rese note alle Amministrazioni Beneficiarie a mezzo di apposita comunicazione sul sito internet della Consip S.p.A. (www.consip.it).

22. FORO COMPETENTE

22.1 Per tutte le questioni relative ai rapporti tra il Fornitore e l'Amministrazione, la

competenza è determinata in base alla normativa vigente.

23. TRATTAMENTO DEI DATI PERSONALI

23.1 Le parti dichiarano di essersi reciprocamente comunicate - oralmente e prima della sottoscrizione del presente Contratto Esecutivo - le informazioni di cui all'art. 13 del D.Lgs. n. 196/2003 recante "*Codice in materia di protezione dei dati personali*" circa il trattamento dei dati personali conferiti per la sottoscrizione e l'esecuzione del Contratto Esecutivo stesso e di essere a conoscenza dei diritti che spettano loro in virtù dell'art. 7 della citata normativa.

23.2 Le Parti acconsentono espressamente al trattamento ed all'invio a Consip S.p.A. da parte del Fornitore e/o dell'Amministrazione, dei dati relativi alla fatturazione, rendicontazione e monitoraggio per le finalità connesse all'esecuzione del presente Contratto Esecutivo. Acconsentono, altresì, a che i dati conferiti, trattati in forma anonima, nonché il nominativo dell'aggiudicatario ed il prezzo di aggiudicazione siano diffusi tramite il sito internet www.consip.it. In adempimento agli obblighi di legge che impongono la trasparenza amministrativa (art. 18 D.L. 83/2012, convertito nella L. 134/2012; art. 32 L. 190/2012), i contratti ed alcuni dati relativi agli stessi (nominativo, partita iva/codice fiscale, importo, ecc.), potranno essere pubblicati e diffusi, ricorrendone le condizioni, tramite il sito internet www.consip.it.

23.3 Le Parti si impegnano ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto del citato D.Lgs.n. 196/2003 con particolare attenzione a quanto prescritto riguardo alle misure minime di sicurezza da adottare.

23.4 Il Fornitore si impegna a svolgere i trattamenti di dati personali nel pieno rispetto della legislazione vigente nonché della normativa per la protezione dei dati personali (ivi inclusi - oltre al D.Lgs.n. 196/2003 e s.m.i. – anche gli ulteriori provvedimenti, comunicati ufficiali, autorizzazioni generali, pronunce in genere emessi dall'Autorità Garante per la Protezione dei Dati Personali) con particolare attenzione all'adozione delle misure di sicurezza di cui alla normativa citata.

23.5 Le Parti dichiarano che i dati personali forniti con il presente atto sono esatti e corrispondono al vero esonerandosi reciprocamente da qualsivoglia responsabilità per errori materiali di compilazione ovvero per errori derivanti da un'inesatta imputazione dei dati stessi negli archivi elettronici e cartacei.

Letto, approvato e sottoscritto
Roma, lì _____

_____ _____
(per l'Amministrazione) (per il Fornitore)

Ai sensi e per gli effetti dell'art. 1341 c.c. il Fornitore dichiara di aver letto con attenzione e di approvare specificatamente le pattuizioni contenute negli articoli seguenti: Art. 1 Definizioni, Art. 3 Oggetto del Contratto Esecutivo, Art. 4 Efficacia e durata, Art. 5 Piano dei Fabbisogni e Progetto dei Fabbisogni, Art. 6 Erogazione dei servizi, Art. 7 Gestione del Contratto Esecutivo, Art. 8

Attivazione e dismissione dei servizi, Art. 9 Locali messi a disposizione dell'Amministrazione; Art. 10 Verifiche - Collaudi, Art. 11 Penali, Art. 12 Corrispettivi, Art. 13 Fatturazione e pagamenti, Art. 14 Garanzia dell'esatto adempimento, Art. 15 Subappalto, Art. 16 Divieto di cessione del contratto, Art. 17 Risoluzione e Recesso, Art. 18 Forza Maggiore, Art. 19 Responsabilità civile, Art. 20 Tracciabilità dei flussi finanziari- Ulteriori clausole risolutive espresse, Art. 21 Oneri fiscali e spese contrattuali, Art. 22 Foro competente, Art. 23 Trattamento dei dati personali.

Letto, approvato e sottoscritto

Roma, lì

_____

(per il Fornitore)

N. Proposta: PDTD-2017-988 del 30/11/2017

Centro di Responsabilità: Servizio Sistemi Informativi

OGGETTO: Servizio Sistemi Informativi – Adesione al Contratto Quadro Consip S.p.a. "SPC Cloud Lotto 2" per la fornitura di "Servizi di gestione delle identità digitali e sicurezza applicativa"

PARERE CONTABILE

Il sottoscritto Dott. Bacchi Reggiani Giuseppe, Responsabile dell'Area Bilancio e Controllo Economico, esprime parere di regolarità contabile ai sensi del Regolamento Arpa sul Decentramento amministrativo.

Data 04/12/2017

Il Responsabile dell'Area Bilancio e
Controllo Economico