ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
75	Capitolato Tecnico Lotto2			SPID	“I servizi di gestione dell’identità digitale favoriranno la diffusione dei servizi telematici, sia nelle transazioni tra soggetti privati e imprese che nell’interazione tra le Pubbliche Amministrazioni ed i cittadini. Il servizio è essenzialmente concepito per agevolare la migrazione delle identità digitali attualmente gestite dalle amministrazioni verso un identity provider esterno con il quale si è stabilita una relazione di fiducia (trust) nell’ottica della realizzazione di una gestione federata delle identità. L’importanza di questa tematica ha avuto giusto riconoscimento sul piano normativo dal DL 69 del 21/6/2013 che all’articolo 17-ter istituisce un sistema per la gestione delle identità digitali - denominato SPID - valido ai sensi di legge nell’ambito pubblico e privato.Attraverso questa iniziativa di gara, quindi, si vogliono pertanto rendere disponibili servizi innovativi, o servizi tradizionali erogati in modalità innovativa, per favorire la PA nella sua graduale transizione verso l’era tecnologica “digitale”.” Con riferimento al “contesto” descritto dalla stazione appaltante e al progetto SPID istituito a cura dell'Agenzia per l'Italia digitale, per la gestione dell'identità digitale di cittadini e imprese e di cui e’ stata avviata la fase pilota in corso di realizzazione, si richiede conferma che nessuna delle aziende partecipanti a detta sperimentazione , nella quale le stesse aziende stanno anche definendo le regole tecniche ed implementando soluzioni tecnologiche per “gestione delle identità digitali “ oggetto di questa gara di Appalto, sarà ammessa alla presente gara d’appalto, ovvero , in caso contrario, come intenda la Stazione Appaltante eventualmente tutelare il contesto di equa e libera concorrenza, con particolare riferimento ai servizi di “Identity provider” oggetto di offerta per il Lotto 2.	Da informazioni acquisite dalla Stazione Appaltante, le versioni in bozza delle regole tecniche sono state scritte autonomamente da AgID e sono pubblicate sul sito AgID nella sezione SPID, unitamente ad altre utili informazioni per l' implementazione dei servizi rese attraverso risposte a quesiti.
185	Capitolato Tecnico Lotto2	2.1.1.1	8	Identity Provider	Con riferimento ai servizi di registrazione dei soggetti per i quali il fornitore gestisce l'identita' digitale si chiede conferma che, per la verifica dell'identita' personale, per ognuna delle modalita' indicate (rif. par. 2.1.1.1.) e nello specifico per il riconoscimento tramite esibizione a vista di un documento valido o attraverso sessione audio/video, tale servizio potra' essere erogato direttamente dal Fornitore (o subappaltatore) senza che siano richiesti requisiti specifici o abilitazioni di alcun genere per il riconoscimento, ovvero che tale fase puo' essere svolta da qualsiasi soggetto o persona giuridica privata.Diversamente si richiede se l’aggiudicatario (o subfornitore) fornitore dei servizi per la verifica dell'identita' personale, debba essere titolare di qualche particolare convenzione con Enti pubblici a cio’ deputati, come debba avvenire e con quali cautele il rilascio dell’identita’ digitale.	Si conferma che per la verifica dell'identita' personale, per ognuna delle modalita' indicate (rif. par. 2.1.1.1.) e nello specifico per il riconoscimento tramite esibizione a vista di un documento valido o attraverso sessione audio/video, tale servizio potra' essere erogato direttamente dal Fornitore (o subappaltatore) senza che siano richiesti requisiti specifici o abilitazioni di alcun genere per il riconoscimento. In ogni caso le attività di verifica dovranno essere svolte nel rispetto della normativa SPID in via di consolidamento.
186	Capitolato Tecnico Lotto2	1.1.1	7/49	Identity Provider	Si richiede se sia lecito attendersi, in conformita’ con quanto riportato nel CSO ("il servizio è sostanzialmente concepito per agevolare la migrazione delle identità digitali attualmente già detenute da una amministrazione verso un identity provider esterno con il quale si è stabilita una relazione di fiducia (trust) nell’ottica della realizzazione di una gestione federata delle identità.") che la migrazione delle identità digitali debba essere favorita in fase realizzativa rispetto alla verifica dell’identita’ personale di cui ai punti 2.1.1.1., per cui nell’ipotesi in cui si raggiunga mediante la “migrazione” citata una data quota di identita’ digitali fino al massimo dell’identita’ previste nel bando (12 milioni), le altre modalita’ saranno eventualmente da realizzarsi solo successivamente e sulla eventuale restante quota. Diversamente, con riferimento al servizio di cui in oggetto ed al numero massimo di identita' digitali indicato nel CSO, poiche' allo stesso sono associate quattro metodologie di verifica (rif. par 2.1.1.1), estremamente differenti in termini di soluzione organizzativa e tecnologica a supporto e di conseguenza in termini di costi implementativi associati, al fine di poter valutare correttamente il requisito e produrre una conseguente offerta tecnico economica la piu' vantaggiosa possibile le la Stazione appaltante, si richiede di indicare i criteri con i quali si debba determinare il valore offerto, ovvero la distribuzione % delle tipologie di servizio richieste.In ultimo, si richiede se sia corretto ritenere che la decisione di adottare uno o piu’ metodologie di verifica (rif. par 2.1.1.1) contestualmente debba essere definita, di comune accordo, nell’ambito del comitato di direzione tecnica.	Il Fornitore dovrà presentare e concordare con l'Amministrazione contraente un piano di migrazione. Per la verifica dell'identità personale, Il Fornitore ha facoltà di organizzarsi secondo le proprie logiche d'impresa, fermo restando l'obbligo di assicurare tutte le modalità di verifica previste nel Capitolato Tecnico Lotto2 pagg.8-9 ai punti 2.1.1.1.1, 2.1.1.1.2, 2.1.1.1.3 e 2.1.1.1.4. Nell'Offerta Tecnica il Fornitore potrà indicare le modalità organizzative con cui intende effettuare le attività di migrazione. L'Amministrazione avrà la scelta di effettuare per proprio conto le verifiche dell'identità personale o in alternativa dovrà mettere a disposizione dei cittadini delle postazioni "webcam" dalle quali poter effettuare le verifiche di cui al punto 2.1.1.1.2 del Capitolato Tecnico Lotto2. Per le verifiche che dovranno essere effettuate attraverso le attività di riconoscimento di cui al punto 2.1.1.1.1 e 2.1.1.1.2 è previsto un contributo unitario, oltre al canone annuale di gestione, per il quale il Fornitore presenterà la propria offerta economica, come previsto nell'Allegato 3 Offerta Economica Lotto2 Parte B. Si veda a proposito il documento di errata corrige Lotto2.
187	Capitolato Tecnico Lotto2	1.1.1.punto 2.1.1.2	9	Identity Provider	il gestore del servizio dovrà conservare i dati utilizzati per la verifica dell’identità personale di ciascun utente a seconda dei casi sopra previsti. In particolare relativamente al punto 2.1.1.1.1, gli estremi e la copia per immagine del documento di riconoscimento, relativamente al punto 2.1.1.1.2 copia dei log di transazione e relativamente al punto 2.1.1.1.3, il modulo di adesione firmato digitalmente; Si richiede la possibilità di utilizzare modalità di conservazione sostitutiva per i documenti consegnati per il riconoscimento a vista	Si conferma la possibilità di utilizzare la conservazione a norma dei documenti secondo la normativa vigente.
188	Appendice 3 Capitolato tecnico	Monitoraggio		Centro Servizi	Generale si chiede conferma che il servizio di monitoraggio debba essere soggetto alle stesse restrizioni di "community cloud" come indicato nel capitolato generale	Si conferma che il Concorrente deve presentare la propria proposta con il servizio in "community cloud". Il Concorrente ha comunque facoltà, se lo ritiene, di presentare un'ulteriore e diversa proposta che potrà essere valutata e approvata in sede di Comitato di Direzione Tecnica.

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
189	Capitolato Tecnico Lotto2	1.3.7	45	Web Application Firewall	Si chiede di precisare se per il servizio di Web Application/Next Generation Firewall Management sia richiesta una protezione perimetrale dei servizi web esposti dalle amministrazioni, o se viceversa la protezione web application sia da intendersi come sicurezza delle applicazioni web esterne utilizzate dagli utenti interni alle amministrazioni.	Per il servizio in oggetto sono richieste entrambe le protezioni.
190	Capitolato Tecnico Lotto2	1.1.1	7	Identity Provider	"Il servizio potrà gestire un numero di identità digitali non superiore a 12.000.000 (dodici milioni) ed è sostanzialmente concepito per agevolare la migrazione delle identità digitali attualmente già detenute da una amministrazione verso un identity provider esterno con il quale si è stabilita una relazione di fiducia (trust) nell'ottica della realizzazione di una gestione federata delle identità." ...."Gli attributi che rappresentano le identità digitali sono classificati secondo le seguenti categorie:"..... Il servizio di gestione delle identità digitali è concepito per agevolare la migrazione delle identità digitali attualmente già detenute da un'amministrazione verso un'identity provider esterno. Si richiede di confermare se il processo di porting e bonifica delle identità già al momento detenute da differenti amministrazioni è incluso all'interno del servizio.	Si conferma che il processo di porting e bonifica delle identità già al momento detenute da differenti amministrazioni è incluso all'interno del servizio.
191	Capitolato Tecnico Lotto2	1.1.1 punto 2.1.1.2	9	Identity Provider	il gestore del servizio dovrà conservare i dati utilizzati per la verifica dell'identità personale di ciascun utente a seconda dei casi sopra previsti. In particolare relativamente al punto 2.1.1.1.1, gli estremi e la copia per immagine del documento di riconoscimento, relativamente al punto 2.1.1.1.2 copia dei log di transazione e relativamente al punto 2.1.1.1.3, il modulo di adesione firmato digitalmente; Relativamente al riconoscimento di cui al punto 2.1.1.1.2, si chiede di specificare cosa si intende per "copia dei log di transazione	Si veda la risposta al quesito 215
192	Capitolato Tecnico Lotto2	1.1.1 punto 2.3.3	12	Identity Provider	"Il gestore dell'identità digitale revoca l'identità digitale se riscontra l'inattività della stessa per un periodo continuativo superiore a ventiquattro mesi o se viene a conoscenza del decesso della persona fisica o dell'estinzione della persona giuridica attivando opportune e documentate verifiche delle informazioni ricevute." Si chiede di confermare se a valle del processo di revoca di un'identità digitale, l'utente deve procedere ad una nuova emissione della stessa. In caso affermativo, si chiede di specificare se gli utenti sono soggetti alla fase di verifica dell'identità personale con le stesse modalità definite nel par. 2.1.1.1	Si conferma che, a seguito di una revoca di un'identità digitale, l'utente deve procedere ad una nuova emissione della stessa con verifica dell'identità personale operata con le stesse modalità definite ai punti 2.1.1.1.1, 2.1.1.1.2, 2.1.1.1.3 e 2.1.1.1.4, pagg. 8-9 del Capitolato Tecnico Lotto2.
193	Capitolato Tecnico Lotto2	1.1.1 punto 2.5	13	Identity Provider	"Il soggetto titolare di una identità digitale può chiedere, attraverso i referenti delle Amministrazioni, al gestore del servizio di identità digitale di conoscere gratuitamente i propri dati personali, in conformità con la normativa vigente." Si chiede di esplicitare le modalità di trasmissione dei dati personali da parte dell'Amministrazione verso il soggetto richiedente	Le modalità di contatto, eventualmente anche solo attraverso un service desk telematico, sono elementi di progetto a carico del Fornitore di cui si terrà conto nei criteri di valutazione dell'offerta. Le modalità previste dovranno comunque essere realizzate nel rispetto di quanto previsto dal codice della Privacy. Si vedano anche risposte alla domanda 251 e 662.
194	Capitolato Tecnico Lotto2	1.1.2 punto 2	20	Identity Provider	"Il servizio deve essere fornito in modo indipendente dai sistemi operativi ed applicativi utilizzati e dalle architetture di rete e prevede diversi profili." Il servizio di I&AM deve essere fornito in modo indipendente dai Sistemi Operativi ed applicativi utilizzati. Si chiede di confermare che alla voce "applicativi utilizzati" siano inclusi esclusivamente applicativi di natura WEB.	Si conferma che il servizio "I&AM" è rivolto alle sole applicazioni web, siano essi siti web o applicazioni con interfaccia web fuibili dai client tramite protocollo HTTP.
195	Capitolato Tecnico Lotto2	1.3.5	42	Data Loss Prevention	compatibilità con i sistemi operativi Windows e Linux e con almeno due dei seguenti: Android, Blackberry, iOS e Microsoft Windows Mobile. Si chiede di confermare che il supporto dei sistemi operativi Windows e Linux è requisito minimo per la tecnologia proposta dal fornitore	Si precisa che la soluzione proposta deve garantirela il supporto sulle sole piattaforme Windows e Linux. Si veda documento di errata corrige Lotto2.
196	Capitolato Tecnico Lotto2	1.3.5	42	Data Loss Prevention	compatibilità con i sistemi operativi Windows e Linux e con almeno due dei seguenti: Android, Blackberry, iOS e Microsoft Windows Mobile. Si chiede di specificare cosa si intende per compatibilità con sistemi operativi Mobile.	La compatibilità con i sistemi operativi mobile non è richiesta. Si veda documento di errata corrige Lotto2. Il Fornitore potrà comunque eventualmente offrire il supporto su altre piattaforme inclusi i dispositivi mobili, descrivendo la sua proposta nell'Offerta Tecnica.

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
197	Capitolato Tecnico Lotto2	1.1.1	7	Identity Provider	il servizio...è sostanzialmente concepito per agevolare la migrazione delle identità digitali attualmente già detenute da una amminsitrazione verso un identity provider esterno con il quale si è stabilita una relazione di fiducia (trust) nell'ottica delle realizzazione di una gestione federata di identità. Si chiede di indicare il numero o percentuale sul totale indicato al paragrafo 1.1.1 (12M) di identità già detenute dalle Amministrazioni che spossono essere oggetto di migrazione e ritenute già valide ai fini della verifica dell'identità personale di cui al punto 2.1.1 del CT - Lotto 2, per poter stimare quante identità potranno essere migrate e quante necessitino di primo rilascio	Premesso che le credenziali vanno riemesse in ogni caso per ognuna delle identità digitali oggetto di migrazione, si considera che le attività di verifica dell'identità personale possa essere richiesta per il 50% delle identità digitali previste dalla presente gara. Si veda documento di errata corrige Lotto2
198	Offerta Economica Parte B			Identity Provider	Ai fini della valutazione economica del servizio "I&AM" deve essere presentata una quotazione – canone annuale per utente - per ciascuna delle seguenti fasce, definite in base al numero di profili utenti gestiti: Fascia 1: fino a 10.000 utenti gestiti Fascia 2: fino a 10.001 a 100.000 utenti gestiti Fascia 3: fino a 100.001 a 400.000 utenti gestiti Fascia 4:oltre 400.000 utenti gestiti Si prega di chiarire se la metrica è per "profili utente" gestiti o "utenti", in quanto le definizioni date nel testo sono tra loro contraddittorie	La metrica è per numerosità di utenti.
199	Capitolato Tecnico Lotto2	1.1.1	10	Identity Provider	Il servizio dovrà essere in grado di garantire per l'autenticazione i livelli di sicurezza LoA2, LoA3 e LoA4. Si chiede di indicare chi sceglierà il profilo di autenticazione (l'utente finale, la PA) e se possinile i volumi previsti per ciascun livello.	Il livello di assurance (LoA) viene stabilito dall'amministrazione erogatrice di servizi (o applicazioni) web e può essere diverso da servizio a servizio (ad es. servizi orientati alle consultazioni possono avere associati dei LoA bassi, altri servizi potranno avere dei LoA di tipo 2 o superiore). Si stima che per il livello LoA 4 il numero di utenti sia pari al 20% del volume totale previsto nella presente gara.
200	Capitolato Tecnico Lotto2	1.3	25	Servizi di sicurezza	I servizi di sicurezza sono volti a supportare le Amminstrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità delle componenti hardware e software dei sistemi informativi. Si chiede di specificare se si fa riferimento a sistemi informativi presso CED dell'Amministrazione oppure se rientrano nel perimetro anche i servizi erogati dal fornitore aggiudicatario degli altri lotti.	Per sistemi informativi si intendono quelli all'interno dei CED dell'Amministrazione.
201	Capitolato Tecnico Lotto2	1.3.1	34	Static Application Security Testing	... e a canone nel caso in cui il servizio sia erogato in modalità continua (scansione periodiche). Si chiede di specificare la frequenza massima annua per le scansioni periodiche (modalità continua)	In modalità continua non c'è alcun limite alle scansioni. In ogni caso, il Fornitore può, se necessario, valutare la frequenza attesa per applicazione in base alle sue esperienze pregresse.
202	Capitolato Tecnico Lotto2	1.3.1	34	Static Application Security Testing	..."Static Application Security Testing", deve essere presente una quotazione - costo per applicazione -per la modalità one time ed una quotazione - canone annuale per applicazione - per la modalità continua... Un applicazione è una definizione generica che varia da Amministrazione ad Amministrazione e include diverse componenti e tecnologie. In genere le metriche utilizzate sono le Linee di codice e i Function Point. Si chiede di indicare il numero massimo di linee di codice (LOC) o Function Point per applicazione.	Si conferma che deve essere indicato il prezzo unitario per applicazione, costituita da un massimo di 100.000 linee di codice (LoC)
203	Capitolato Tecnico Lotto2	1.3.2	37	Dynamic Application Security Testing	Dynamic Application Security Testing, tabella funzionalità aggiuntive profili SILVER e Gold Si chieded di confermare che la funzionalità PCI Compliance è necessaria unicamente per il profilo GOLD	Si conferma che la funzionalità PCI compliance è riferita al solo profilo GOLD. Trattasi di refuso su tabella pag.37 del Capitolato Tecnico Lotto2

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
204	Capitolato Tecnico Lotto2	1.3.2	37	Dynamic Application Security Testing	Il servizio "Dynamic Applicatio Security Testing" sarà erogato in modalità continuativa di tipo "as a service" Si richiede di specificare il numero massimo di scansioni richiedibili per anno per applicazione.	Nel caso di quotazione annuale per applicazione non è previsto alcun limite al numero di scansioni effettuabili. In ogni caso, il Fornitore può, se necessario, valutare la frequenza attesa per applicazione in base alle sue esperienze pregresse.
205	Capitolato Tecnico Lotto2	1.3.3	39	Mobile Application Security Testing	Il servizio "Mobile Application Security Testing" sarà erogato in modalità continuativa di tipo "as a service" Si richiede di specificare il numero massimo di scansioni richiedibili per anno per applicazione.	Nel caso di quotazione annuale per applicazione non è previsto alcun limite al numero di scansioni effettuabili. In ogni caso, il Fornitore può, se necessario, valutare la frequenza attesa per applicazione in base alle sue esperienze pregresse.
206	Capitolato Tecnico Lotto2	1.3.4	41	Vulnerability Assessment	Ilservizio"VulnerabilityAssessment"deveessereerogatoinmodalitàcontinuativa di tipo "as a service" Per il servizio di VA non è specificato il numero delle VA richieste in un anno, si chiede di specificare il massimo numero di VA richiesto per un anno.	Non è previsto alcun limite al numero di VA annuo, che potrà essere concordato con l'Amministrazione in funzione della sua policy di sicurezza, atteso che generalmente la frequenza prevista può essere trimestrale.
207	Capitolato Tecnico Lotto2	1.3.5	43	Data Loss Prevention	Nota 3 Per endpoint si intende qualunque workstation, laptop e punto di accesso della rete aziendale. Oltre a workstation e Laptop si chiede di confermare che per punti di accesso alla rete di aziendale si intendono dispositivi di tipo tablet e smartphone	Si precisa che la soluzione per tablet e smartphone non è richiesta. Si veda documento di errata corrige Lotto2. Il Fornitore potrà comunque eventualmente offrire il supporto su altre piattaforme inclusi i dispositivi mobili, descrivendo la sua proposta nell'Offerta Tecnica.
208	Appendice 3 Capitolato tecnico	2	4	SOC	Servizi di Monitoraggio Si chiede di specificare se i servizi di Monitoraggio da offrire fanno riferimento ai servizi di sicurezza oggetto di questo procedimento di gara oppure di altri sistemi di sicurezza di proprietà dell'Amministrazione al di fuori dal perimetro di gara	I servizi di monitoraggio potranno essere richiesti anche per sistemi e servizi di sicurezza non richiesti nella presente gara
209	Appendice 3 Capitolato tecnico	2	4	SOC	3. Il Fornitore, nell'ambito dei servizi di monitoraggio deve garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto: ▫ monitoraggio di apparati IDS/IPS e di apparati Firewall; ▫ monitoraggio delle piattaforme di autenticazione forte comprendente la modalità di gestione delle policy, degli utenti e dei loro privilegi; ▫ raccolta delle informazioni provenienti dai diversi servizi di sicurezza in ambito e segnalazione tempestiva di eventuali problemi; ▫ attività di troubleshooting; ▫ archiviazione dei log nel rispetto delle normative vigenti, in archivi immodificabili e inalterabili; ▫ notifica di eventi/allarmi a fronte del superamento di soglie prefissate e a seguito del verificarsi di eventi critici che impattano sulla sicurezza dell'ambiente informatico. I servizi di Monitoraggio includono anche attività di troubleshooting. Si chiede si confermare che non sarà consentito l'accesso agli apparati/sistemi sotto monitoraggio, in quanto la gestione degli apparati è esclusa dal servizio e quindi l'attività di troubleshooting si limiterà alle attività di tuning della piattaforma di correlazione, riduzione falsi positivi, change sulle regole di correlazione, gestione delle problematiche di accesso e raccolta dei log, malfunzionamenti e problemi di performance della piattaforma stessa	Si conferma che la gestione degli apparati/sistemi oggetto delle attività è esclusa dal perimentro dei Servizi di Monitoraggio (SOC) richiesti nella presente gara e descritti nell'Appendice 3 del Capitolato Tecnico Lotto2.

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
210	Appendice 3 Capitolato tecnico	2	4	SOC	3. Il Fornitore, nell'ambito dei servizi di monitoraggio deve garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto: ▫ monitoraggio di apparati IDS/IPS e di apparati Firewall; ▫ monitoraggio delle piattaforme di autenticazione forte comprendente la modalità di gestione delle policy, degli utenti e dei loro privilegi; ▫ raccolta delle informazioni provenienti dai diversi servizi di sicurezza in ambito e segnalazione tempestiva di eventuali problemi; ▫ attività di troubleshooting; ▫ archiviazione dei log nel rispetto delle normative vigenti, in archivi immodificabili e inalterabili; ▫ notifica di eventi/allarmi a fronte del superamento di soglie prefissate e a seguito del verificarsi di eventi critici che impattano sulla sicurezza dell'ambiente informatico. Si chiede di specificare meglio il contesto del servizio. Non è chiaro se il servizio è pensato per PA che vogliano gestire la sicurezza in proprio (policy,...) e demandare a fornitore esterno il monitoraggio proattivo, senza possibilità di accesso ai sistemi di sicurezza da parte di quest'ultimo.	Il Servizio di Monitoraggio (SOC) è pensato per Amministrazioni che vogliano esternalizzare le attività di individuazione e la prevenzione dei rischi derivanti dagli attacchi informatici, attraverso un servizio che dovrà effttuare le attività descritte nell'Appendice 3 del Capitolato Tecnico Lotto 2. Si conferma che la gestione degli apparati/sistemi oggetto delle attività è esclusa dal perimetro dei Servizi di Monitoraggio (SOC) richiesti nella presente gara e descritti nell'Appendice 3 del Capitolato Tecnico Lotto2.
211	Appendice 3 Capitolato tecnico	2	4	SOC	§ raccolta delle informazioni provenienti dai diversi servizi di sicurezza in ambito e segnalazione tempestiva di eventuali problemi; Si chiede di specificare che per ambito si intende ambito specifico di gara, in questo caso relativo al Lotto2, e quindi si fa riferimento ai servizi descritti all'interno del capitolato e allegati relativi.	Si precisa che per ambito si intende il complesso dei servizi richiesti nel Lotto2 della presente gara. In ogni caso i servizi di monitoraggio potranno essere richiesti anche per sistemi e servizi di sicurezza non richiesti nella presente gara
212	Lettera d'invito	Profili Professionali 7 punto B.12	36	Criteri	Tabella 2. – Figura professionale Capo progetto: requisito migliorativo. Presenza di certificazioni professionali Si prega di chiarire i requisiti della figura Professionale Project Manager, in quanto sembra di fatto non in linea con quelli richiesti per i Lotti 1, 3 e 4. In particolare si chiede di confermare il possesso di 1 certificazione, in linea con quanto previsto negli altri lotti e non il contemporaneo possesso di 3 certificazioni per un candidato presentato per quel profilo professionale. (ITIL v.3 Foundation + ISO/IEC 27001 e/o CISA e/o EUCIP + PMP e/o PRINCE2 e/o IPMA	Si conferma che per acquisire i punteggi previsti per il requisito migliorativo in oggetto è necessario il numero minimo di risorse in possesso di tre certificazioni contemporanee come descritto nella tabella 2 della Lettera d'invito per il lotto 2
213	Capitolato Tecnico Lotto2	1.1.1punto 1.3	8	Identity Provider	"Attributi non qualificati: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati" Viene fatto riferimento ad attributi non qualificati ma vengono elencati gli attributi qualificati attestati da un gestore di attributi qualificati. Si chiede• di specificare quali siano gli attributi NON qualificati• di confermare che gli attributi qualificati saranno attestati esclusivamente dai gestori di attributi qualificati	Si veda risposta alla domanda n.214
214	Capitolato Tecnico Lotto2	1.1.1punto 1.3	8	Identity Provider	Essendo gli attributi qualificati gestiti dalle Attribute Authority, si chiede di confermare se i gestori delle identità digitali potranno anche acquisire e gestire gli attributi qualificati o meno. In caso affermatico, si chiede di chiarire le modalità attraverso le quali i gestori delle Identità Digitali potranno acquisire e gestire tali attributi qualificati direttamente dal titolare dell'identità digitale	Il requisito del servizio "Identity Provider" al punto 1.3, pag. 8 del Capitolato Tecnico Lotto2 è da intendersi non valido. Si veda documento errata corrige Lotto 2
215	Capitolato Tecnico Lotto2	Cap 1.1.1punto 2.1.1.2	9	Identity Provider	Viene richiesto per la modalità di identificazione di cui al punto 2.1.1.1.2 si debba conservare copia dei log di transazione mentre per la modalità di cui al punto 2.1.1.1.3 si debba conservare il modulo di adesione firmato digitalmente. Si chiede conferma che per le modalità di identificazione di cui ai paragrafi:• 2.1.1.1.1 si debbano conservare gli estremi e la copia per immagine del documento di riconoscimento• 2.1.1.1.2 si debba conservare in forma protetta la registrazione audio-video• 2.1.1.1.3 si debbano conservare copia dei log di transazione• 2.1.1.1.4 si debba conservare il modulo di adesione firmato digitalmente	Si conferma l'interpretazione data.
216	Capitolato Tecnico Lotto2	Cap 1.1.1punto 2.1.4	10	Identity Provider	I gestori dell'identità digitale, ricevuta la richiesta di adesione, effettuano la verifica degli attributi identificativi del richiedente sulla base di documenti, dati o informazioni ottenibili da fonti affidabili e indipendenti, secondo i criteri e le modalità stabilite dall'Agenzia per l'Italia Digitale Si chiede di confermare che al momento dell avvio del servizio saranno attive le convenzioni tra AgID e le fonti autorevoli e che le modalità di verifica siano accessibili ad esempio tramite servizi di Cooperazione Applicativa (es. Web Services), e che tali attività non siano a carico del servizio di Identity Provider.	Si conferma l'interpretazione data

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
217	Capitolato Tecnico Lotto2	Identity Provider	16	Identity Provider	Parametri di valutazione economica - Ai fini della valutazione economica del servizio “Identity Provider” deve essere presentata una quotazione – canone annuale per identità - per ciascuna delle seguenti fasce, definite in base al numero di identità digitali gestite Si chiede di chiarire si all'interno del canone base e del servizio di Identity Provider sia compreso anche il rilascio delle credenziali di autenticazione forte (es. OTP, token con certificato), incluso l'eventuale dispositivo HW/SW che il gestore dell'identità digitale dovrà fornire al titolare dell'identità digitale.	Il rilascio delle credenziali di autenticazione forte (es. OTP, token con certificato), incluso l'eventuale dispositivo hw/sw che il gestore dell'identità digitale dovrà fornire al titolare dell'identità digitale si intende incluso all'interno del canone annuale per utente del servizio di "Identity Provider"
218	Capitolato Tecnico Lotto2	1.2.1	23	Firma Digitale	Funzionalità di verifica della firma compatibile con i principali formati di documenti (tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp) Considerando che un file firmato conforme alla normativa vigente può avere unicamente estensione .p7m, .pdf, oppure .xml, vi chiediamo di confermare che le parole <<... formati di documenti (tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp)>> sono da considerarsi un refuso, laddove invece si intendeva scrivere <<... formati di firma (.p7m, .pdf, .xml) >>. Qualora, invece, non si trattasse di un refuso, vi chiediamo di chiarire il senso del requisito.	Si precisa che la soluzione dovra' consentire l'apposizione della firma digitale su qualunque tipo di documento *"tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp"* e si conferma che i file firmati digitalmente dovranno essere in formato *"... CAdES, PAdES e XAdES come previsto dalla normativa vigente in materia"*.
219	Capitolato Tecnico Lotto2			SPID	Generale Come dobbiamo considerare il capitolato Tecnico Specifico e Generale in relazione alla nota del Garante per la protezione dei dati personali sullo SPID del 19/6/2014? Si richiede di specificare i punti all'interno del capitolato nel quale tali rilievi hanno impatto e quali sono gli emendamenti accettati. (rif. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3265492)	Al fine di prendere atto delle modifiche apportate al sistema SPID a seguito del parere sullo schema di DPCM in materia di sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), reso in data 19 giugno 2014 dal Garante per la protezione dei dati personali, si invita innanzitutto a prendere visione della relativa documentazione pubblicata sul sito dell'Agenzia per l'Italia Digitale. Inoltre, si precisa che l'Aggiudicatario del Lotto 2 della presente procedura di gara sarà tenuto ad uniformarsi alle prescrizioni contenute nel DPCM e nelle successive regole tecniche che saranno adottate da AgID ad avvenuta entrata in vigore delle stesse. Resta inteso che, ove le predette prescrizioni fossero difformi da quelle contenute nel Capitolato Tecnico del Lotto 2 della presente gara, nella parte relativa alla descrizione delle modalità di erogazione dei relativi servizi, queste ultime si intenderanno automaticamente disapplicate e sostituite da quelle di legge e/o regolamento.
220	Capitolato Tecnico Lotto2	1.1.1 Punto 2.4.1.3	12	Identity Provider	Se nel predetto periodo di trenta giorni il gestore riceve dal soggetto titolare dell’Identità Digitale disconosciuta copia della denuncia penale presentata all’Autorità Giudiziaria per gli stessi fatti su cui è basata la dichiarazione di disconoscimento Identità digitale la medesima viene revocata Si chiede di elencare le modalità di trasmissione/ricezione delle denunce in tale evenienza	Le regole tecniche che regolano il sistema SPID prevedono che le modalità di comunicazione/ricezione siano specificate attraverso gli "attributi secondari"
221	Lettera d'invito	Capitolo 7 punto B.10	34	Phase out fornitura	Descrizione della soluzione per il trasferimento del know-how e delle attività per servizi di IAM e per i servizi professionali a fine fornitura in termini di obiettivi, risorse, strumenti e modalità operative che il fornitore propone in modo da massimizzarne l’efficacia e ridurre i rischi del subentro Si chiede di confermare che le attività di Phase Out siano da considerarsi solo per i servizi I&AM e Servizi Professionali	Premesso che le attività di phase-out sono dovute per tutti i servizi in gara, si precisa che per l'attribuzione del punteggio tecnico previsto nel criterio B.10 sarà valutata solamente la proposta relativa ai servizi IAM (servizio L2.S1.1 del Capitolato tecnico Lotto2) e ai servizi professionali (servizio L2.S3.9 del Capitolato tecnico Lotto2).
222	Capitolato Tecnico Lotto2	1.1.1 Punto 1.3	8	Identity Provider	Le identità digitali rilasciate all'utente contengono obbligatoriamente il codice identificativo, gli attributi identificativi e almeno un attributo secondario, funzionale alle comunicazioni tra il gestore dell'identità digitale e l'utente; Si prega di dare definizione di Codice Identificativo	Il Codice Identificativo è il particolare attributo assegnato dal gestore dell'identità digitale che consente di individuare univocamente un'identità digitale nell'ambito del sistema SPID

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
223	Capitolato Tecnico Lotto2	1.2.2	25	Timbro elettronico	Funzionalità di verifica del timbro compatibili con i principali formati di documenti (tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp) Considerando che i formati di output documenti generati con Timbro Elettronico sono generalmente dei PDF, questo in quanto sono dei documenti stampabili da qualsiasi device, senza la necessità di installare ulteriori programmi come, ad esempio, MS Word, MS Excel, ecc. é corretta l'interpretazione che, la soluzione di Timbro Elettronico accetti in input almeno i formati sopra indicati, che verranno poi inseriti nel timbro digitale generato nelle modalità citate nel CAD art. 23 ter e successive Linee Guida, richiamate nell'articolo stesso, emanate dall'AgID?	Si conferma.
224	Appendice 3 Capitolato tecnico	servizi di monitoraggio		SOC	Generale Si chiede di confermare che la descrizione organizzativa e tecnica dei servizi di monitoraggio sia da presentare in un allegato a parte, e si chiede se esso debba seguire uno schema di offerta tecnica(template) predefinito o se tale schema sia a libera scelta del fornitore	Si conferma che la descrizione dei Servizi di Monitoraggio (SOC) offerti dovrà essere presentata in un documento separato dall'Offerta Tecnica (e pertanto non concorrerà al calcolo delle pagine dell'Offerta tecnica). Non è previsto alcun template di riferimento fermo restando il contenuto richiesto nell'Appendice 3 del Capitolato Tecnico Lotto 2
228	Capitolato Tecnico Lotto2	$ 1.1.1 rif. 2.2.2.2	11	Identity Provider	….il servizio dovrà rendere disponibili sistemi di autenticazione informatica a due fattori, Si chiede conferma che nell'ambito del servizio di Identity Provider, è fornito il sistema di autenticazione secondo i livelli di Assurance LoA3 ed Loa4, ma non è richiesta la fornitura dei dispositivi di autenticazione e dei relativi certificati digitali (nel caso LoA4) da rilasciare agli utenti finali	Non si conferma l'iterpretazione data. Nell'ambito dell'erogazione del servizi si prevede la fornitura dei dispositivi di autenticazione e dei relativi certificati digitali (nel caso LoA4) da rilasciare agli utenti finali
229	Capitolato Tecnico Lotto2	1.1.1 punto 2.3.1	11	Identity Provider	Gli utenti sono obbligati a informare tempestivamente il gestore dell'identità Digitale di ogni variazione degli attributi previamente comunicati. Quest'ultimo provvede tempestivamente ai necessari aggiornamenti, avendo verificato le informazioni fornite sulla base di documenti, dati o informazioni ottenibili da fonti affidabili e indipendenti, secondo i criteri e le modalità stabilite dall'Agenzia per l'Italia Digitale; Si conferma che le attività di verifica dell' Identity Provider sulle informazioni fornite dall'utente, sia nei processi di registrazione che in quelli di modifica degli attributi e di revoca/cancellazione saranno effettuati utilizzando servizi applicativi messi a disposizione dalle Amministrazioni competenti in ambito di Cooperazione Applicativa.	Si conferma che le attività di verifica dell' Identity Provider sulle informazioni fornite dall'utente, sia nei processi di registrazione che in quelli di modifica degli attributi e di revoca/cancellazione saranno effettuati utilizzando servizi applicativi messi a disposizione dalle Amministrazioni competenti anche se non necessariamente in Cooperazione Applicativa.
230	Capitolato Tecnico Lotto2	1.1.1 punto 3.2	14	Identity Provider	La componente di servizio autorità di autenticazione dovrà essere in grado di realizzare il profilo SAML "Web Browser SSO" come specificato in ([SAML-TechOv] sez. 4.1) prevedendo le due versioni "SP-Initiated": "Redirect->POST binding" e "POST->POST binding" in cui il meccanismo di autenticazione è innescato dalla richiesta inoltrata dall'utente (tramite il suo User Agent) ad un fornitore di servizi, il quale a sua volta si rivolge all'autorità di autenticazione in modalità "pull" Si chiede conferma che sia necessario utilizzare le due versioni "SP-Initiated": "Redirect->POST binding" e "POST->POST binding" , e che secondo lo standard SAML 2.0 queste modalità utilizzino il modello "push" e non quello "pull", contrariamente a quanto riportato sul capitolato.	Si conferma l'utilizzo del modello push. Il riferimento alla modalità pull è da cosiderarsi un mero errore materiale.
231	Capitolato Tecnico Lotto2	1.1.1 punto Rif 4.4.	15	Identity Provider	...in caso di attività sospetta. In tal caso il fornitore potrà procedere alla revoca del certificato, sulla base di policy precedentemente concordate; Poiché non è chiaro all'interno del bando se i dispositivi di autenticazione LoA3 e i certificati digitali con i relativi dispositivi crittografici siano a carico dell'Amministrazione o dell'IdP, si chiede se per revoca del certificato si intenda la disattivazione della Identità Digitale associata al titolare del certificato non essendo l'IdP titolato all'emissione di certificati digitali	I dispositivi di autenticazione LoA3 e i certificati digitali con i relativi dispositivi crittografici sono a carico del Fornitore del servizio di "Identity Provider"
232	Capitolato Tecnico Lotto2	1.1.1 Rif. 4.9	15	Identity Provider	...garantiscono la gestione sicura delle componenti riservate delle identità digitali degli utenti, assicurando che le stesse non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata.... Si chiede di chiarire quali sono le "componenti riservate" dell'Identità Digitale	Le componenti riservate delle identità digitali degli utenti sono tutte le informazioni ad esso relative tutelate dal Codice della privacy
233	Capitolato Tecnico Lotto2	1.1.2	16	I&AM	I gestori dell'identità digitale, ricevuta la richiesta di adesione, effettuano la verifica degli attributi identificativi del richiedente sulla base di documenti, dati o informazioni ottenibili da fonti affidabili e indipendenti, secondo i criteri e le modalità stabilite dall'Agenzia per l'Italia Digitale. Con riferimento al punto 1.6 di pag. 19 (realizzazione di un profilo SAML "Web Browser SSO", si chiede conferma che la frase "servizi telematici" vada interpretata come applicazioni su protocollo HTTP a cui l'utente acceda mediante web browser.	Si conferma l'interpretazione. Trattandosi di applicazione del profilo SAML web browser SSO, i servizi telematici non possono che essere forniti tramite protocollo HTTP e fruiti tramite web browser.

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
234	Capitolato Tecnico Lotto2	1.1.2 punto 1.1	18	I&AM	per l'autenticazione dei propri utenti il servizio potrà fare ricorso ad un Identity provider esterno all'Amministrazione; Si chiede conferma che non è responsabilità del servizio di I&AM realizzare la funzione di Attribute Authority per un'amministrazione che aderisce al servizio, e che la funzionalità di IdP è quella di cui al servizio L2.S1.1.	Si conferma che non è responsabilità del servizio "I&AM" la realizzazione di funzionalità di Attribute Authority. E' altresì responsabilità del servizio "I&AM" l'interazione con i gestori di identità digitali (tutti gli Identity Provider conformi al sistema SPID - si veda anche il requisito di compatibilità all'articolo 17-ter del DL 69 del 21/6/2013 come riportato a pag 6 del Capitolato Tecnico Lotto2 - e non solo quello realizzato attraverso questa gara) e quando necessario con le Attribute Authority esterne.
235	Capitolato Tecnico Lotto2	1.1.2 punto 1.1	18	I&AM	per l'autenticazione dei propri utenti il servizio potrà fare ricorso ad un Identity provider esterno all'Amministrazione; Si chiede conferma che per "propri utenti" si intende gli "utenti esterni" o meglio i cittadini che utilizzano i portali web pubblici messi a disposizione dall'Amministrazione	Come specificato nella sezione "Descrizione del servizio" a pag. 16 del Capitolato Tecnico Lotto2 il servizio "I&AM" ha come obiettivo la gestione dell'accesso da parte di utenti esterni al portale dell'Amministrazione o ai servizi da essa erogati in rete. Si conferma dunque l'interpretazione
236	Capitolato Tecnico Lotto2	1.1.2 punto 3	20	I&AM	Il servizio comprende la gestione delle policy di accesso dei servizi, la gestione del ciclo di vita dei profili utente (creazione dell'utenza, aggiornamento e cancellazione) con relativa assegnazione dei privilegi di accesso (attribuzione, sospensione, modificazione, revoca e cancellazione) ai servizi/sistemi. Tali attività dovranno essere condotte secondo le direttive e sotto la supervisione dei responsabili delle amministrazioni..... (cfr. §1.1.2 comma 1 .. Il servizio di I&AM dovrà consistere nella gestione delle attività di identificazione, autenticazione ed autorizzazione all'accesso ai portali delle Amministrazione e alla fruizione dei servizi da esse erogati ai propri utenti esterni; In riferimento al comma 1.1. si chiede conferma che nell'ambito della componente dei servizi L2.S1.2 NON è previsto il provisioning delle utenze sul servizi/sistemi/applicazioni delle Amministrazioni.	Non è previsto nel servizio il provisioning delle identità digitali (e relative credenziali) associate agli utenti del servzio. Le identità digitali associate agli utenti sono quelle fornite attraverso il servizio di Identity Provider della presente gara ed in generale tutte le identità digitali SPID rilasciate da terze parti.
237	Capitolato Tecnico Lotto2	1.1.2	16e17	I&AM	Si chiede conferma che tutti i servizi esposti dall'amministrazione siano in grado di consumare asserzioni SAML e che si comportino quindi da Service Provider come definito dalle specifiche OASIS. Sono quindi gli stessi che richiedono l'AuthnRequest al PEP tramite l'user agent dell'utente. L'eventuale adeguamento dell'infrastruttura tecnologica dell'amministrazione è a carico della stessa.	Non si conferma l'interpretazione proposta. Il servizio di I&AM è stato pensato per essere di ausilio alle amministrazioni nell'adozione di SPID (si veda il requisito di compatibilità all'articolo 17-ter del DL 69 del 21/6/2013 riportato a pag 16 del Capitolato Tecnico Lotto2) così da fornire a una soluzione "chiavi in mano" per la realizzazione delle componenti applicative che gestiscono tecnologia SAML, relativamente alla realizzazione del profilo web-SSO. Lo scopo del servizio di I&AM è quello di sovraintendere tutta la problematica della gestione degli accessi ai servizi web dell'amministrazione, sia per la parte statica, ovvero la gestione delle policy di accesso dei servizi web dell'amministrazione, sia per la parte run-time dinamica, ovvero la gestione completa del protocollo SAML previsto del Web SSO lato service provider così come definito dallo standard OASIS. Facendo riferimento alla figura riportata a pag. 17 del Capitolato Tecnico Lotto2, tutto quanto evidenziato all'interno del rettangolo chiaro costituisce l'ambito di competenza del servizio "I&AM". Più specificatamente tutte le interazioni (comprese ovviamente quelle relative al SAML) che vanno dalla 1 alla 7 (7a e 7b) ad eccezione della 3 e 4 (che coinvolgono solo l'utente e l'Identity Provider) sono di competenza del servizio "I&AM"; tutto questo per conto di tutti i servizi web presenti e futuri dell'amministrazione. L'amministrazione dovrà mettere a disposizione del fornitore una URL su cui indirizzare l'utente del servizio o dell'applicazione web una volta superato il processo di autorizzazione.

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
238	Capitolato Tecnico Lotto2	1.1.2	16e17	I&AM	Si chiede conferma che è a carico dei servizi dell'amministrazione il controllo della sessione applicativa, ossia, nell'ambito della navigazione dell'utente nello stesso sito e nella stessa sessione, non viene interrogato il PEP per ogni risorsa richiesta.	Non si conferma l'interpretazione proposta. Il servizio "I&AM" ha in carico tutte le attività di gestione dell'autorizzazione all'accesso delle risorse web dell'amministrazione. Pertanto se nel corso della navigazione nell'ambito della stessa sessione l'utente fa richiesta di "risorse"a cui sono associate policy di accesso diverse da quelle già verificate, il sistema I&AM deve essere chiamato ancora in causa per operare tutte le verifiche necessarie. Nel far questo il sistema I&AM riutilizza il pacchetto di asserzioni già raccolte al momento del primo accesso integrandolo con ulteriori altre allo scopo richieste (verosimilmente asserzioni di attributo);
239	Capitolato Tecnico Lotto2	1.1.2 punto 3	20	I&AM	Il servizio comprende la gestione delle policy di accesso dei servizi, la gestione del ciclo di vita dei profili utente (creazione dell'utenza, aggiornamento e cancellazione) con relativa assegnazione dei privilegi di accesso (attribuzione, sospensione, modificazione, revoca e cancellazione) ai servizi/sistemi. Tali attività dovranno essere condotte secondo le direttive e sotto la supervisione dei responsabili delle amministrazioni..... (cfr. §1.1.2 comma 1 .. Il servizio di I&AM dovrà consistere nella gestione delle attività di identificazione, autenticazione ed autorizzazione all'accesso ai portali delle Amministrazione e alla fruizione dei servizi da esse erogati ai propri utenti esterni; SI chiede conferma che la frase "relativa assegnazione dei privilegi di accesso (attribuzione, sospensione, modificazione, revoca e cancellazione) ai servizi/sistemi." sia da intendersi come relativa assegnazione dei privilegi d'accesso ai servizi offerti dall'Amministrazione tramite applicazioni web. Ossia l'infrastruttura I&AM dovrà solo gestire la profilatura delle applicazioni web delle Amministrazioni.	SI conferma che l'ambito di applicazione del servizio "I&AM" è quello relativo ai servizi o applicazioni web delle amministrazioni. Pertanto la profilatura è relativa solo a questa tipologie di risorse applicative.
240	Capitolato Tecnico Lotto2	1.1.2 punto 4	20	I&AM	Deve valere il principio che ogni operazione effettuata sui sistemi èriconducibile a soggetti correttamente identificati, autenticati ed autorizzati.Ne consegue che devono essere rilevati anche tutti i tentativi di accesso non autorizzato, anche inconsapevolmente o senza dolo intenzionale da parte degli utenti. Si chiede conferma che il fornitore debba garantire il rilevamento degli accessi relativamente ai soli sistemi da lui gestiti in modalità "as services" che sono utilizzati per erogare il servizio di I&AM e sono quindi esclusi i sistemi di proprietà dell'Amministrazione.	Il Fornitore deve garantire la tracciatura di tutti gli accessi alla componente I&AM, ovvero tracciare tutte le attività da esso svolte ai fini della realizzazione del processo di web SSO.
241	Capitolato Tecnico Lotto2	I&AM 1.1.2		Identity Provider	bando di gara per la prequalifica: LOTTO n. 2 - Servizi di identità digitale e sicurezza applicativa1) Breve descrizione: L'appalto ha per oggetto la stipula di un Contratto-Quadro per l'affidamento dei servizi di identità digitale e sicurezza applicativa in favore delle Pubbliche Amministrazioni, e segnatamente:a) servizi di gestione delle identità digitali sia in modalità "as a service" sia in modalità "on-premise"; Nella documentazione di prequalifica per il servizio di gestione delle identità digitali era prevista anche la modalità "on premise". Si chiede conferma che tale modalità non sia prevista dall'attuale bando di gara, poiché non è prevista la gestione delle identità sulle piattaforme delle Amministrazioni (es. gestione delle identità sui sistemi operativi, database, middleware e piattaforme applicative custom o commerciali)	Si conferma che la modalità di erogazione prevista per il servizio "I&AM", come descritto nel par. 1.1.2 del Capitolato Tecnico Lotto2, è solo quella "as a service". Qualora l'Amministrazione lo richieda, attraverso il servizio L2.S3.9 – Servizi professionali, come descritto nel suddetto capitolato Tecnico, potrà essere fornito supporto relativamente a soluzioni di "I&AM" operanti sui sistemi dell'Amministrazione stessa
242	Capitolato Tecnico Lotto2	1.1.2 punto 1.3.1	18	I&AM	l'accesso alle suddette fonti potrà avvenire anche telematicamente secondo protocolli standard; si chiede di indicare le eventuali modalità di accesso non telematico alle informazioni fornite da Attribute Authority, visto che le interazioni avvengo tra applicazioni mediante popolamento di campi attributo all'interno di Asserzioni SAML	Il requisito fa riferimento a tutte le informazioni necessarie all'individuazione in rete delle entità di certificazione (Identity Provider e Attribute Authority) e dei metadati SAML necessari per l'invocazione. In particolare per garantire la compatibilità all'articolo 17-ter del DL 69 del 21/6/2013 come riportato a pag 16 del Capitolato Tecnico Lotto2, tali informazioni saranno reperibili attraverso il registro di federazione SPID accessibile per mezzo di richeste HTTP.
243	Capitolato Tecnico Lotto2	1.3.6	44	Data Base Security	Parametri di valutazione economicaLa modalità di remunerazione del servizio "database security" è: a canone.Ai fini della valutazione economica del servizio "database security" nel caso di modalità erogazione in modalità "as a service" dovrà essere presentata una quotazione – canoneannuale per nodo* - per ciascuna delle seguenti fasce: ▫ Fascia 1: fino a 25 nodi ▫ Fascia 2: da 26 a 50 nodi ▫ Fascia 3: oltre 50 nodi *Per "nodo" si intende qualsiasi tipo di dispositivo capace di elaborare dati e su cui sia presente almeno un'istanza di database. Si fa notare come gli strumenti di Database Security sono in genere licenziati in base alla potenza elaborativa dei nodi su cui girano e/o al numero di nodi istanze, ma con listini di ordini di grandezza superiori alla presente base d'asta. Si chiede pertanto di valutare una ridefinizione del concetto di"nodo" o in alternativa che possano essree considerate le metriche di valutazione alternative quali ad esempio il numero di oggetti (tabelle-utenti-schema) sottoposti a policy.	Si precisa la quotazione del servizio "Data base security" dovrà essere effettuata per singola istanza di database, ferme restando le tre fasce previste. Si veda documento di errata corrige Lotto2
244	Capitolato Tecnico Lotto2	1.1.1 Rif. 2.1.1.1	8	Identity Provider	la verifica dell'identità personale deve avvenire in uno dei seguenti modi: Si prega di confermare che per l'erogazione del servizio di Identity Provider sia necessario offrire tutte e 4 le modalità di rilascio, elencate ai punti 2.1.1.1.1, 2.1.1.1.2, 2.1.1.1.3, 2.1.1.1.4, e che la modalità di registrazione sia a scelta dell'utente/PA.	Si conferma.

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
245	Capitolato Tecnico Lotto2	1.1.2 punto 1.1	18	I&AM	1.1. per l'autenticazione dei propri utenti il servizio potrà fare ricorso ad un Identity provider esterno all'Amministrazione;1.1.1. l'utente esterno dovrà scegliere il proprio identity provider in grado di autenticarlo tra quelli presenti in una lista proposta dal sistema I&AM; Si chiede di confermare che il servizio di I&AM, in linea di principio, sia erogabile solo in sinergia con un servizio di identity Provider, sia esso esterno o interno all'amministrazione, compliant alle specifiche tecniche dello SPID.	Il servizio "I&AM" dovrà fare riferimento a tutti gli Identity Provider e Attribute Authority disponibili conformi a SPID .
246	Capitolato Tecnico Lotto2	1.1.2 punto 1.1	18	I&AM	1.1. per l'autenticazione dei propri utenti il servizio potrà fare ricorso ad un Identity provider esterno all'Amministrazione;1.1.1. l'utente esterno dovrà scegliere il proprio identity provider in grado di autenticarlo tra quelli presenti in una lista proposta dal sistema I&AM; Si chiede di confermare che la matrice degli accessi implementata per il servizio di I&AM contenga solo oggetti noti in ambito servizio Identity Provider e che quindi includa una lista di applicazioni Web a cui accedere, utenti e attributi, eventualmente recuperati da attribute provider esterni.	Il servizio "I&AM" dovrà fare riferimento a tutti gli Identity Provider e Attribute Authority SPID, incluso ovviamente il servzio di" Identity provider" previsto dalla presente gara. Ovviamente le informazioni sulle applicazioni devono essere fornite dall'Amministrazione contraente.
247	Capitolato Tecnico Lotto2	1.1.1 Rif. 2.1.1.1	8	Identity Provider	la verifica dell'identità personale deve avvenire in uno dei seguenti modi: Si chiede di chiarire se nella fase di riconoscimento a vista, l'operatore deputato ad effettuare il riconoscimento debba essere inserito in qualche particolare elenco, albo o categoria, e se debba rispondere personalmente o per conto di, in caso di evidente falsità della documentazione acquisita	Si veda risposta alla domanda n.185
248	Capitolato Tecnico Lotto2	2.1.1.1	8	Identity Provider	22.1.1. Il rilascio dell'identità digitale da parte del gestore del servizio deve avvenire a seguito della verifica dell'identità personale del soggetto richiedente; Con riferimento ai servizi di registrazione dei soggetti per i quali il fornitore gestisce l'identita' digitale si chiede conferma che, per la verifica dell'identita' personale, per ognuna delle modalita' indicate e nello specifico per il riconoscimento tramite esibizione a vista di un documento valido o attraverso sessione audio/video, tale servizio potra' essere erogato direttamente dal Fornitore (o subappaltatore) senza che siano richiesti requisiti specifici o abilitazioni di alcun genere per il riconoscimento, ovvero che tale fase puo' essere svolta da qualsiasi ente privato.	Si veda risposta alla domanda n.185
249	Capitolato Tecnico Lotto2	2.1.1.1	8	Identity Provider	Il servizio dovrà essere in grado di garantire per l'autenticazione i livelli di sicurezza LoA2, LoA3 e LoA4. Si chiede di chiarire se il rilascio del secondo fattore di autenticazione (nel caso sia richiesto) debba avvenire contestualmente al rilascio delle credenziali base dell'identità, o possa essere temporalmente ritardato.	In generale Il rilascio delle credenziali dell'identità può essere ritardato rispetto all'attività di registrazione. In particolare il secondo fattore può essere temporalmente ritardato rispetto al primo.
250	Capitolato Tecnico Lotto2	2.1.1.1	8	Identity Provider	Il servizio dovrà essere in grado di garantire per l'autenticazione i livelli di sicurezza LoA2, LoA3 e LoA4. Si chiede di verificare se la scelta del supporto per il secondo fattore sia da considerarsi dell'utente finale e di conseguenza non inclusa nella remunerazione del servizio richiesto	La scelta dei supporti per tutti i tipi di credenziali è a discrezione del Fornitore ed è a carico dello stesso cioè incluso nella remunerazione del servizio. Ogni tipologia di costo conseguente alla scelta fatta è a carico del Fornitore.
251	Capitolato Tecnico Lotto2	2.1.1.1	8	Identity Provider	Gli utenti sono obbligati a informare tempestivamente il gestore dell'identità Digitale di ogni variazione degli attributi previamente comunicati. Quest'ultimo provvede tempestivamente ai necessari aggiornamenti, avendo verificato le informazioni fornite sulla base di documenti, dati o informazioni ottenibili da fonti affidabili e indipendenti, secondo i criteri e le modalità stabilite dall'Agenzia per l'Italia Digitale; Non è chiare se comunicazioni di questo tipo debbano avvenire tramite l'Help Desk descritto nel capitolato generale, che è il punto di contatto tra il fornitore e l'Amministrazione, o se il servizio di identity provider prevede un service desk almeno telematico nei rapporti con il possessore dell'identità digitale	Il servizio di "Identity Provider" richiede il servizio di help-desk, con le modalità previste nel Capitolato Tecnico Parte Generale, per i soli referenti delle Amministrazioni contraenti. Le modalità di contatto con i possessori delle identità digitale, eventualmente anche solo attraverso un service desk telematico, sono elementi di progetto a carico del Fornitore di cui si terrà conto nei criteri di valutazione dell'offerta. Le modalità previste dovranno comunque essere realizzate nel rispetto di quanto previsto dal codice della Privacy. Si vedano anche risposte alla domanda 193 e 662.
252	Capitolato Tecnico Lotto2	1.1.1 punto 2.6	13	Identity Provider	Il gestore del servizio di identità digitale, su richiesta dell'utente, glisegnala ogni avvenuto utilizzo delle credenziali di accesso, inviandonegli estremi ad uno degli attributi non identificativi a tale scopoindicato dall'utente stesso, secondo le regole tecniche definite con iregolamenti di cui all'articolo 4. Si chiede di indicare qual'è il tempo di conservazione dei log contenenti l'evidenza dell'utilizzo delle credenziali da parte dell'utente, superato il quale il fornitore non è tenuto a segnalare tale utilizzo. Si rileva che tale durata non è riportata tra i regolamenti di cui all'art.4	Per i tempi di conservazione dei log debbono essere rispettati i termini di legge per l'opponibilità a terzi delle transazioni effettuate utilizzando identità SPID
253	Capitolato Tecnico Lotto2	1.3.4	37	Vulnerability Assessment	vulnerability assessment" dovranno essere eseguite dal Fornitore sulle applicazioni in ambiente di produzione o collaudo, previo accordo con l'Amministrazione. Il Fornitore dovrà inoltre segnalare all'Amministrazione, tramite comunicazione formale, il perimetro che sarà interessato dall'attività di analisi e di test, la tipologia e la descrizione dei controlli effettuati e la valutazione dell'impatto potenziale. Si chiede conferma che qualora il Fornitore evidenzi all'Amministrazione dei potenziali impatti dovuti all'esecuzione di particolari tipologie di test di vulnerabilità, nel caso in cui questi si svolgano su ambienti di produzione, l'Amministrazione dovrà formalmente approvare l'esecuzione di questi test, manlevando il Fornitore nel caso in cui l'esecuzione dei test approvati provochi degli impatti e/o danni.	Si conferma

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
254	Capitolato Tecnico Lotto2	1.3.4	37	Vulnerability Assessment	vulnerability assessment" dovranno essere eseguite dal Fornitore sulle applicazioni in ambiente di produzione o collaudo, previo accordo con l'Amministrazione. Il Fornitore dovrà inoltre segnalare all'Amministrazione, tramite comunicazione formale, il perimetro che sarà interessato dall'attività di analisi e di test, la tipologia e la descrizione dei controlli effettuati e la valutazione dell'impatto potenziale. Si chiede conferma che per l'erogazione dei servizi L2.S3.1, L2.S3.2, L2.S3.3, L2.S3.4, visto che l'accesso non autorizzato ai sistemi è proibito dalle normative di legge (cfr. art. 615 Codice penale), l'accordo con l'Amministrazione dovrà necessariamente contenere l'autorizzazione ad eseguire i test, Qualora tale autorizzazione non sia fornita il Fornitore non potrà erogare il servizio.	Si conferma
255	Capitolato Tecnico Lotto2	1.3.1	34	Static Application Security Testing	Il servizio di "static application security testing" deve consentire alle Amministrazioni l'identificazione delle vulnerabilità software all'interno del codice (sorgente o binario) delle applicazioni nella fase iniziale del ciclo di vita in modo da poterle eliminare prima della distribuzione. Si chiede conferma che l'analisi del codice sia da considerarsi in alternativa effettuata sul sorgente o sul binario e che non siano richieste entrambe le modalità di analisi.	Si conferma che la soluzione proposta può consentire l'analisi del codice alernativamente sul codice sorgente o sul binario. Nella relazione dell'Offerta tecnica il Fornitore dovrà specificare la modalità di analisi proposta.
256	Capitolato Tecnico Lotto2	1.1.2 punto 1.4	18	I&AM	identificato l'utente e validato il suo profilo per mezzo delle attestazioni di autenticazione e di attributo acquisite secondo le modalità specificate ai punti 1.1 e 1.2, il sistema I&AM dovrà gestire le operazioni necessarie per la verifica dei diritti di accesso alle risorse richieste, sulla base delle policy di sicurezza a queste associate; Si chiede conferma che il Fornitore non dovrà eseguire modifiche sugli applicativi delle Amministrazioni. Se necessarie, tali modifiche per utilizzare il servizio I&AM sono a carico dell'Amministrazione.	Si conferma che il Fornitore non dovrà intervenire sugli applicativi delle amministrazioni. L'Amministrazione contraente dovrà mettere a disposizione del Fornitore una URL su cui indirizzare l'utente del servizio dell'applicazione web una volta superato il processo di autorizzazione.
257	Capitolato Tecnico Lotto2	1.1.1 punto 2.1.1.2	9	Identity Provider	il gestore dovrà conservare i dati utilizzati per la verifica dell'identità personale di ciascun utente a seconda dei casi previsti. In particolare relativamente al punto 2.1.1.1 gli estremi e la copia per immagine del documento di riconoscimento si chiede di confermare l'impostazione ritenuta compliant relativamente alla copia per immagine del documento, che prevede l'acquisizione in toni di grigio. Indicare eventuali requisiti di definizione della copia per immagine del documento di riconoscimento (es. risoluzione)	Si conferma che la modalità di acquisizione prevista è in toni di grigio con almeno 256 livelli.
258	Capitolato Tecnico Lotto2	1.1.1 punto 2.1.1.2	9	Identity Provider	il gestore dovrà conservare i dati utilizzati per la verifica dell'identità personale di ciascun utente a seconda dei casi previsti Si richiede di confermare l'impostazione ritenuta compliant di acquisizione e archiviazione in formato elettronico della documentazione, tra cui il modulo di richiesta di rilascio dell'identità digitale sottoscritto dal richiedente	Si conferma l'impostazione nel rispetto della normativa vigente in termini di conservazione
259	Capitolato Tecnico Lotto2	1.1.1 punto 2.3.2	11	Identity Provider	l'utente può chiedere al gestore dell'identità digitale, in qualsiasi momento la revoca della propria identità digitale ovvero la modifica delle proprie credenziali di accesso. si richiede di confermare che, in caso di negligente smarrimento delle credenziali, la richiesta e quindi l'eventuale costo di rigenerazione delle credenziali dell'identità digitale sia a carico dell'utente che ne fa richiesta	Fino ad un numero pari alla soglia dell'1‰ del numero di identità digitali previste, l'eventuale riemissione delle credenziali, in caso di negligente smarrimento, è a carico del Fornitore e si intende incluso nel canone offerto. Al di sopra di tale soglia, per la riemissione di credenziali di livello 2 o superiore, in caso di negligente smarrimento, l'eventuale costo di rigenerazione saranno a carico dell'Amministrazione contraente.
608	Capitolato Tecnico Generale	9	76	Help Desk	Requisito: Sulla base della tipicità dei servizi previsti nell'ambito della presente fornitura, i Fornitori dovranno garantire i seguenti orari di servizio: H24, 7 gg su 7 per la disponibilità di risorse di calcolo, per le attività di monitoraggio e gestione incident relativamente ai seguenti servizi: IaaS, PaaS, SaaS per il Lotto 1, Servizi di Identity provider e I&AM, di firma digitale remota, sevizi di sicurezza di data loss/leak prevention, database security, web application firewall e next generation firewall, secure web gateway e servizi di monitoraggio per il Lotto 2 ... Domanda: Si chiede di chiarire, in conformità a quanto richiesto per le attività dell'help desk (cfr. §5.1 pag 48) se l'orario di servizio H24, 7 gg su 7 corrisponde alla finestra oraria nella quale il fornitore deve garantire la ricezione delle segnalazioni, almeno attraverso il canale mail e l'interfaccia web, per i servizi elencati, e non alla presa in carico delle attività di "gestione incident" per le quali si continua a far rifo chiaro costituisce l'ambito di competenza del servizio "I&AM". Più specificatamente tutte le interazioni (comprese ovviamente quelle relative al SAML) che vanno dalla 1 alla 7 (7a e	Nella finestra H24 7 gg su 7 il concorrente deve garantire la disponibilità dei servizi elencati al capitolo 9 del Capitolato Tecnico Parte Generale, nel rispetto degli indicatori di qualità previsti, adottando gli strumenti e le modalità di presidio e intervento ritenuti più adeguati. Nella finestra H24 7 gg su 7 per tali servizi la gestione degli incident dovrà essere garamtita con le modalità e nei tempi previsti come descritto nel paragrafo 1.3 del Capitolato Tecnico Lotto2. La finestra LUN-Ven 8,30-17,30 e SAB 8,30-14,00) definisce il periodo entro il quale è attivo, oltre alla ricezione di segnalazioni attraverso canali automatici (web, mail, ecc...) anche un servizio con operatore. Al di fuori della suddetta fascia , il concorrente deve garantire la sola ricezione delle segnalazioni tramite canali automatici.
649	Lettera d'invito	7	34	Phase out fornitura	Requisito: criterio B.10 - Soluzione proposta per le modalità di affiancamento di fine fornitura (phase out). Domanda: Nel citato criterio si richiede la descrizione del phase out per il servizio IAM e per i servizi professionali. Nell'attribuzione del punteggio invece si fa riferimento a tutti i servizi di sicurezza. Si chiede conferma che i criteri motivazionali di attribuzione del punteggio si baseranno esclusivamente sulla descrizione del phase out del servizio IAM e dei servizi professionali	Premesso che le attività di phase-out sono dovute per tutti i servizi in gara, si precisa che per l'attribuzione del punteggio tecnico previsto nel criterio B.10 sarà valutata solamente la proposta relativa ai servizi IAM (servizio L2.S1.1 del Capitolato tecnico Lotto2) e ai servizi professionali (servizio L2.S3.9 del Capitolato tecnico Lotto2).
650	Lettera d'invito	7	36	Criteri	Requisito: B.12 – Figure professionali – Presenza di Certificazioni Domanda: Si chiede di confermare che il punteggio tecnico migliorativo verrà assegnato solo se tutte le risorse offerte nella nimerosità indicata nella colonna "Numerosità minima risorse offerte" soddisfa il requisito migliorativo di possesso delle certificazioni professionali indicate nella relativa colonna.	Si conferma che il punteggio indicato nella Tab. 1 del criterio B.12 verrà attribuito se e solo se per entrambe le figure professionali richieste verranno offerte un numero di risorse in possesso delle certificazioni richieste maggiore o uguale ai numeri minimi indicati

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
656	Capitolato Tecnico Lotto2	1.1	4	Identity Provider	Requisito: il capitolato cita che lo scenario di riferimento a cui si vuole arrivare per rendere disponibili servizi di identita digitale è quello di una vera e propria infrastruttura finalizzata alla gestione delle identità e degli attributi riferibili ai soggetti operanti in rete. In questo contesto generale gli attori previsti sono i seguenti: … fornitori di servizi rappresentati dai soggetti privati o dalle pubbliche amministrazioni che erogano servizi in rete per cui la cui fruizione è richiesta l'identificazione e l'autenticazione degli utenti; Domanda: si chiede di specificare quali possono essere i soggetti privati a cui si riferisce o se si tratta di un principio di carattere generale che non sarà applicato allo specifico contesto di Gara	Si tratta di un principio di carattere generale non applicabile allo specifico contesto della presente gara. Si precisa che i potenziali fruitori dei servizi della presente gara sono esclusivamente le amministrazioni pubbliche.
657	Capitolato Tecnico Lotto2	1,1	5	Identity Provider	Requisito: il fornitore dei servizi pur avendo adesso contezza dell'identità dell'utente può avere la necessità di verificare ulteriori attributi qualificati eventualmente presenti nel profilo utente e richiesti dalle policy di sicurezza che regolano l'accesso al servizio. In questo caso: Domanda: Si chiede di chiarire se l'incipit "in questo caso:" è da considerarsi un refuso oppure se introduce elementi che, però, risultano mancanti. In tal secondo caso si chiede di fornire gli elementi mancanti del capitolato	L'incipit "In questo caso" introduce i successivi punti 5 e 6 che sussistono solo se "il fornitore dei servizi pur avendo adesso contezza dell'identità dell'utente può avere la necessità di verificare ulteriori attributi qualificati eventualmente presenti nel profilo utente e richiesti dalle policy di sicurezza che regolano l'accesso al servizio"
658	Capitolato Tecnico Lotto2	1.1.1	10	SPID	Come noto l'implementazione del terzo livello di sicurezza previsto dal Decreto SPID (LoA4), richiede l'utilizzo di strumenti utente certificati ex Allegato 3 della Direttiva 1999/93/CE del Parlamento Europeo e certificati digitali. Considerando che nella documentazione di Gara non è presente alcuna previsione sulla distribuzione numerica delle richieste rispetto ai livelli di sicurezza SPID, al fine di poter fornire una adeguata valorizzazione economica, si chiede di confermare che tali strumenti non sono oggetto di forniturо o, in subordine, la percentuale prevista di identità digitali del terzo livello SPID (LoA4).	La percentuale prevista di identità digitali del terzo livello SPID (LoA4) è pari al 20% del numero totale previsto nel Capitolato Tecnico Lotto2
659	Capitolato Tecnico Lotto2	1.1.1	10	Identity Provider	Requisito: 2.1.4. I gestori dell'identità digitale, ricevuta la richiesta di adesione, effettuano la verifica degli attributi identificativi del richiedente sulla base di documenti, dati o informazioni ottenibili da fonti affidabili e indipendenti, secondo i criteri e le modalità stabilite dall'Agenzia per l'Italia Digitale; Domanda: Si chiede di confermare che tra le fonti affidabili e indipendenti attraverso cui ottenere gli elementi per effettuare la verifica degli attributi identificativi del richiedente, ne esista almeno una utilizzabile dall'aggiudicatario senza oneri aggiuntivi. Se l'interpretazione non fosse corretta, si chiede di indicare quali costi il fornitore dovrà prevedere per la verifica di tali attributi.	I costi relativi all'utilizzo di banche dati attraverso le quali ottenere le informazioni in oggetto saranno definiti nella normativa SPID in via di definizione. Tali oneri non sono inclusi nella presente base d'asta. L'Aggiudicatario potrà ribaltarli senza aggravio di costo all'Amministrazione contraente.
660	Capitolato Tecnico Lotto2	1.1.1	10	Identity Provider	Requisito: 2.2 è riportato "La componente di servizio autorità di registrazione dovrà gestire l'associazione dei soggetti per i quali il servizio gestisce l'identità digitale a credenziali riconosciute sia già in possesso del soggetto sia appositamente prodotte e rilasciate agli stessi; 2.7. Il gestore del servizio di identità digitale dovrà prevedere, su richiesta, la presa in carico e la migrazione delle identità gestite dall'amministrazione, direttamente o tramite un terzo fornitore; Domanda: Dal momento che le credenziali devono essere rilasciate al soggetto dal gestore di identità digitale e rispettare i requisiti previsti dal capitolato si chiede di confermare che la richiesta di associare credenziali già in possesso possa essere considerata un refuso. Si fa presente che essendo l'aggiudicatario il responsabile del rilascio e della gestione delle credenziali, si ritiene non praticabile la presa in carico di credenziali già rilasciate dalle amministrazioni in quanto ci sono ad oggi teco chiaro costituisce l'ambito di competenza del servizio "I&AM". Più speci	La richiesta di associare credenziali già in possesso è da considerarsi mero refuso
661	Capitolato Tecnico Lotto2	1.1.1	11	Identity Provider	Requisito: 2.2.2.3. per il livello corrispondente al Level of Assurance LoA4 dello standard ISO/IEC DIS 29115, il servizio dovrà rendere disponibili sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo; Domanda: Si chiede di chiarire se i dispositivi che custodiscono le chiavi private di cui al livello di sicurezza indicato debbano essere forniti a cura dell'aggiudicatario e ricompresi nel canone del servizio.	I dispositivi che custodiscono le chiavi private di cui al livello di sicurezza indicato devono essere forniti a cura dell'aggiudicatario e ricompresi nel canone del servizio.
662	Capitolato Tecnico Lotto2	1.1.1	11	Identity Provider	Requisito: 2.3.1. gli utenti sono obbligati a informare tempestivamente il gestore dell'identità digitale di ogni variazione degli attributi previamente comunicati. Quest'ultimo provvede tempestivamente ai necessari aggiornamenti, avendo verificato le informazioni fornite sulla base di documenti, dati o informazioni ottenibili da fonti affidabili e indipendenti, secondo i criteri e le modalità stabilite dall'Agenzia per l'Italia Digitale; Domanda: Si chiede di specificare se gli utenti informeranno il gestore dell'identità digitale per il tramite dell'Amministrazione contraente oppure contattando direttamente il gestore per l'identità digitale. Per entrambi i casi si richiede quali sono le modalità di contatto e l'orario di copertura del servizio che il gestore delle identità digitale deve mettere a disposizione per l'evasione delle richieste nonché, per poter correttamente dimesionare il servizio, una stima del numero di richieste per anno.	Gli utenti informeranno il gestore contattandolo direttamente. Le modalità di contatto, eventualmente anche solo attraverso un service desk telematico, e l'orario di copertura sono elementi di progetto a carico del Fornitore di cui si terrà conto nei criteri di valutazione dell'offerta. La stima del numero di richieste per anno è a carico del Fornitore, e deve essere condotta sulla base del fatto che la tipologia di attributi soggetti a variazione è prevalentemente di natura anagrafica. Si vedano anche risposte alla domanda 193 e 251.
663	Capitolato Tecnico Lotto2	1.1.1	11	Identity Provider	Requisito: 2.3.2. l'utente può chiedere al gestore dell'identità digitale, in qualsiasi momento la revoca della propria identità digitale ovvero la modifica delle proprie credenziali di accesso. A tali richieste il gestore dell'identità digitale provvede tempestivamente. Domanda: Si chiede di specificare se gli utenti richiederanno la revoca al gestore dell'identità digitale per il tramite dell'Amministrazione contraente oppure contattando direttamente il gestore per l'identità digitale.Per entrambi i casi si richiede quali sono le modalità di contatto e l'orario di copertura del servizio che il gestore delle identità digitale deve mettere a disposizione per l'evasione delle richieste nonché, per poter correttamente dimesionare il servizio, una stima del numero di richieste per anno.	Gli utenti informeranno il gestore dell'identità digitale contattando direttamente Le modalità di contatto, eventualmente anche solo telematiche, e l'orario di copertura sono elementi di progetto a carico del Fornitore di cui si terrà conto nei criteri di valutazione dell'offerta. Si stima un numero di richieste di revoca per anno pari al 5% del numero totale di identità digitali previste nella presente gara.

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
664	Capitolato Tecnico Lotto2	1.1.1	11	Identity Provider	Requisito: 2.3. La componente di servizio autorità di registrazione dovrà garantire il tempestivo aggiornamento delle Identità Digitali; 2.3.1. gli utenti sono obbligati a informare tempestivamente il gestore dell'identità digitale di ogni variazione degli attributi previamente comunicati. Domanda: si chiede di confermare che il gestore non è responsabile di identità digitali non aggiornate in caso di mancanza di aggiornamenti da parte dell'utenza finale	Si conferma l'interpretazione data.
665	Capitolato Tecnico Lotto2	1.1.1	13	Identity Provider	Requisito: 2.7. Il gestore del servizio di identità digitale dovrà prevedere, su richiesta, la presa in carico e la migrazione delle identità gestite dall'amministrazione, direttamente o tramite un terzo fornitore; Domanda: Affinché le identità digitali possano essere prese in carico e migrate verso il gestore del servizio, si dovrà procedere con una verifica preventiva che le identità oggetto di migrazione siano state registrate e manutenute secondo i requisiti espressi nel Capitolato. Si richiede di confermare che tale verifica è a cura delle Amministrazioni, che forniranno identità digitali aderenti alla normativa SPID e che in tal caso il gestore del servizio è sollevato da qualsiasi ulteriore verifica.	Si veda riposta alla domanda n. 186
666	Capitolato Tecnico Lotto2	1.1.1	13	Identity Provider	Requisito: 2.7 Il gestore del servizio di identità digitale dovrà prevedere, su richiesta, la presa in carico e la migrazione delle identità gestite dall'amministrazione, direttamente o tramite un terzo fornitore. Domanda: si chiede di specificare se, per le identità migrate dall'amministrazione, nel caso in cui al gestore del servizio di identità digitale non sia richiesto di effettuare la verifica dell'identità personale del soggetto richiedente, l'amministrazione debba comunque provvedere a trasferire al gestore del servizio di identità digitale anche i dati utilizzati per la verifica dell'identità personale di ciascun utente e se il gestore sia di conseguenza tenuto a conservare tali dati per il periodo previsto dal capitolato.	Si conferma l'interpretazione data.
667	Capitolato Tecnico Lotto2	1.1.1	6,7,10	Identity Provider	Requisito: Il servizio di "Identity Provider" prevede la messa a disposizione di un sistema tecnologico e amministrativo che realizzi complessivamente le funzionalità di gestore dell'identità digitale... Il servizio ...è sostanzialmente concepito per agevolare la migrazione delle identità digitali attualmente già detenute da una amministrazione verso un identity provider esterno... Il gestore del servizio dovrà quindi conservarli per tutta la durata contrattuale e trasmetterli alla scadenza del contratto all'Agenzia per l'Italia Digitale o a soggetto da lei indicato Domanda: Alla luce di quanto riportato nella descrizione del servizio, si richiede di confermare che l'Aggiudicatario potrà svolgere direttamente o tramite una sua società controllata, il ruolo di Gestore delle Identità, ai sensi della normativa vigente (accreditamento verso AGID) e che per tale ragione, le evidenze della registrazione dei soggetti richiedenti l'Identità Digitale, dovranno essere conservati dal Gestore dell'Identità Digitale ai seo chiaro costituisce l'ambito	La società partecipante potrà svolgere in proprio o affidare a soggetto terzo dotato dei requisiti di legge le attività che la stessa pone in carico ai gestori delle identità digitali, secondo quanto previsto e nei limiti di cui all'art. 118 D.Lgs. n. 163/2006. Relativamente alla possibilità che il ruolo di Gestore delle Identità sia svolto dall'Aggiudicatario tramite una sua società controllata si rinvia a quanto previsto nella risposta alla domanda n. 470 del documento Chiarimenti Generali. 'La società partecipante potrà svolgere in proprio o affidare a soggetto terzo dotato dei requisiti di legge le attività che la stessa pone in carico ai gestori delle identità digitali.
668	Capitolato Tecnico Lotto2	1.1.1	6	Identity Provider	Requisito: Il servizio di "Identity Provider" prevede la messa a disposizione di un sistema tecnologico e amministrativo che realizzi complessivamente le funzionalità di gestore dell'identità digitale, garantendo la compatibilità con quanto previsto dall'articolo 17-ter del DL 69 del 21/6/2013 e successive norme attuative ed esecutive. Domanda: Poiché secondo il comma 2-ter dell'articolo 64 del Decreto Legislativo del 2005 numero 82 , il Gestore di Identità Digitale opera previo accreditamento preventivo da parte dell'AGID, Si richiede alla Stazione Appaltante se la compattibiltà richiesta comprenda o meno l'accreditamento del Gestore di Identità Digitale . In caso di risposta affermativa si chiede di specificare entro quali tempi si dovrà procedere con l'accreditamente rispetto alla stipula dell'accordo quadro.	La compatibiltà con quanto previsto dall'articolo 17-ter del DL 69 del 21/6/2013 e successive norme attuative ed esecutive richiesta comprende l'accreditamento del Gestore di Identità Digitale. Le tempistiche saranno legate all'iter di perfezionamento del DPCM e dei successivi atti attuativi.
669	Capitolato Tecnico Lotto2	1.1.1	7	Identity Provider	Requisito: Il servizio potrà gestire un numero di identità digitali non superiore a 12.000.000 (dodici milioni) ed è sostanzialmente concepito per agevolare la migrazione delle identità digitali attualmente già detenute da una amministrazione verso un identity provider esterno con il quale si è stabilita una relazione di fiducia (trust) nell'ottica della realizzazione di una gestione federata delle identità Domanda: Allo scopo di effettuare un corretto dimensionamento a livello tecnico-organizzativo della soluzione, si richiede, all'interno del numero di identità digitali non superiore a 12.000.000 (dodici milioni) che l'Aggiudicatario dovrà gestire, qual è la percentuale prevista di identità digitali che dovranno essere create ex-novo rispetto a quelle già create e detenute da altre amministrazioni.	Premesso che le credenziali vanno riemesse in ogni caso per ognuna delle identità digitali oggetto di migrazione, si considera che le attività di verifica dell'identità personale possa essere richiesta per il 50% delle identità digitali previste dalla presente gara. Si veda risposta alla domanda n. 185 e documento di errata corrige Lotto2.
670	Capitolato Tecnico Lotto2	1.1.1	7	Identity Provider	Requisito: 1. Le identità digitali gestiti dal servizio dovranno essere rappresentate per mezzo di un insieme di attributi; Domanda: ai fini dell'ottimizzazione dei processi di migrazione di Identità digitali dagli attuali gestori, si chiede di confermare che l'attività di normalizzazione dei formati degli attributi conformi alla normativa a cui il capitolato fa riferimento, debba essere in carico all'amministrazione contraente.	L'attività di normalizzazione dei formati degli attributi conformi alla normativa a cui il capitolato fa riferimento, è in carico all'aggiudicatario.
671	Capitolato Tecnico Lotto2	1.1.1	8	Identity Provider	Requisito: [la verifica dell'identità personale deve avvenire in uno dei seguenti modi] riconoscimento tramite esibizione a vista di un valido documento d'identità Domanda: Si richiede di specificare se le attività di riconoscimento a vista previste nel requisito citato siano da ritenersi in capo al Fornitore o se, trattandosi di Amministrazioni pubbliche, vengano svolte direttamente dalle stesse Amministrazioni per il tramite dei sistemi messi a disposizione dal Fornitore.	Si veda la risposta al quesito 186

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
672	Capitolato Tecnico Lotto2	1.1.1	8	Identity Provider	Requisito: 1.2. Le identità digitali rilasciate all'utente contengono obbligatoriamente il codice identificativo, gli attributi identificativi e almeno un attributo secondario, funzionale alle comunicazioni tra il gestore dell'identità digitale e l'utente; Domanda: si chiede di confermare che con attributo secondario ci si riferisce agli attributi non identificativi	Si conferma che con attributo secondario ci si riferisce ad attributi non identificativi
673	Capitolato Tecnico Lotto2	1.1.1	8	Identity Provider	Requisito: 1.1.3. Attributi non qualificati: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati; Domanda: Si chiede di confermare che la categoria corretta è "Attributi qualificati" e non "Attributi non qualificati".	Si conferma che la categoria corretta è "Attributi qualificati" e non "Attributi non qualificati" come, per mero errore materiale, viene riportato sul Capitolato Tecnico Lotto2
674	Capitolato Tecnico Lotto2	1.1.1	12	Identity Provider	Requisito: 2.3.3. Il gestore dell'identità digitale revoca l'identità digitale se riscontra l'inattività della stessa per un periodo continuativo superiore a ventiquattro mesi o se viene a conoscenza del decesso della persona fisica o dell'estinzione della persona giuridica attivando opportune e documentate verifiche delle informazioni ricevute. Domanda: Si richiede di specificare quali saranno gli enti/soggetti che invieranno l'informazione sul decesso/estinzione della persona fisica/giuridica al gestore dell'identità digitale, con quale periodicità, con quali modalità informatiche e con quale livello di affidabilità-sicurezza. Si richiede inoltre quali siano le verifiche delle informazioni ricevute ritenute "opportune" dalla stazione appaltante.	Il requisito dovrà essere assolto con le modalità indicate nelle convenzioni e nei regolamenti attuativi del sistema SPID emanati da AgID
675	Capitolato Tecnico Lotto2	1.2.1	22	Firma Digitale	Requisito: Il servizio deve essere configurato come un servizio online nel quale la chiave privata del firmatario viene generata e conservata assieme al certificato di firma rilasciato da parte di un Certificatore accreditato, all'interno di un server remoto sicuro (basato su un HSM conforme alla normativa vigente in materia). E' quindi richiesto che venga utilizzato un sistema di autenticazione forte che preveda l'uso, oltre alla conoscenza di un codice segreto (es. PIN), di sistemi OTP fisici o logici (USB, telefono cellulare, token) Domanda: Si chiede di confermare che il costo di eventuali strumenti fisici di autenticazione (OTP, TOKEN USB,….) da fornire ai titolari per la fruizione del servizio è da considerarsi non incluso nel "canone annuale per utente"	Il servizio prevede che venga fornito almeno un sistema di autenticazione forte. Qualora il Fonitore offra nella propria soluzione strumenti fisici di autenticazione il costo deve considerarsi incluso nel canone annuo per utente offerto.
676	Capitolato Tecnico Lotto2	1.2.1	23	Firma Digitale	Requisito: Il Fornitore, nell'ambito del presente servizio deve garantire per l'Amministrazione almeno la disponibilità delle seguenti funzionalità base / strumenti a supporto: firma digitale massiva automatica Domanda: Si chiede di confermare che per firma digitale massiva automatica ci si riferisce alla possibilità di sottoporre alla firma più documenti seguendo il processo di autenticazione per il singolo documento (ad es. PIN + OTP) e non la possibilità di firmare massivamente documenti mediante una sola autenticazione application to application. Nel caso l'intepretazione non fosse corretta, si chiede di specificare il numero massimo di documenti da firmare nell'unità di tempo.	Si precisa che per il requisito richiesto di *"firma digitale massiva automatica"* si intende la possibilità di firmare massivamente documenti mediante una sola autenticazione application to application. Pur non essendo indicato un requisito prestazionale del numero di documenti gestibili nell'unità di tempo, il Fornitore potrà indicare tale dato, relativo alla soluzione proposta, nel documento di Offerta Tecnica.
677	Capitolato Tecnico Lotto2	1.2.1	23	Firma Digitale	Requisito: Il servizio dovrà prevedere almeno: … funzionalità di verifica della firma compatibile con i principali formati di documenti (tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp). Domanda: I formati per la firma a norma dei documenti informatici sono previsti dalla normativa (DPCM ….) e questa prevede la firma esclusivamente nei formati standard CAdES, PAdES e XAdES. Considerando che il formato di firma CAdES consente di includere al suo interno e quindi di firmare tutti i formati di documenti elencati nel requisito e che in particolare il formato di firma PAdES consente di firmare direttamente i documenti in formato .pdf, si chiede di confermare che i formati previsti dalla normativa siano tutti e soli quelli per i quali è richiesta la funzionalità di verifica.	Si precisa che la soluzione dovra' consentire l'apposizione della firma digitale su qualunque tipo di documento *"tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp"* e si conferma che i file firmati digitalmente dovranno essere prodotti in formato *"… CAdES, PAdES e XAdES come previsto dalla normativa vigente in materia"*.

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
678	Capitolato Tecnico Lotto2	1.3	26	Modalità esecuzione servizi	Requisito: [Tipologia di servizi] “as a service”, mediante il Centro Servizi del Fornitore con l’ausilio degli strumenti (hardware e software) messi a disposizione da quest'ultimo. Si precisa che, qualora lo ritenga opportuno ai fini dell’erogazione dei servizi, il Fornitore potrà richiedere l’autorizzazione ad installare una o più appliance e/o componenti/agent software dedicate presso l’Amministrazione; Domanda: si chiede di confermare se il Fornitore debba erogare gli stessi fornendo strumenti e propri servizi professionali o, in alternativa, se è richiesto al Fornitore di rendere disponibile all’Amministrazione i soli strumenti/apparati a supporto dell’erogazione dei servizi.	I servizi di sicurezza "as a service" sono erogati dal Fornitore attraverso il Centro Servizi. Il fornitore ha facoltà, previa autorizzazione dell'Amministrazione ad installare una o più appliance e/o componenti/agent software dedicate, presso l’Amministrazione stessa. Tali strumenti dovranno essere installati, gestiti e manutenuti a cura del Fornitore. Tali strumenti qualora adottati sono comunque remunerati esclusivamente all'interno del canone del relativo servizio.
679	Capitolato Tecnico Lotto2	1.3	27	Application Security Testing	Requisito: Si precisa inoltre che le attività di analisi, individuazione delle vulnerabilità ed esecuzione di test previste nell’ambito dei servizi di “static application security testing”, “dynamic application security testing”, “mobile application security testing” e vulnerability assessment” dovranno essere eseguite dal Fornitore sulle applicazioni in ambiente di produzione o collaudo, previo accordo con l’Amministrazione Domanda: si chiede di confermare che i servizi citati saranno erogati in ambienti di produzione e collaudo su indirizzi IP raggiungibili da rete internet o da rete SPC	Come specificato nel Capitolato Tecnico Lotto2 i servizi in oggetto devono essere erogati in modalità "as a service" attraverso i Centri Servizi del Fornitore. Le applicazioni oggetto del servizio devono essere raggiungibili, in modo sicuro, attraverso rete Internet o SPC.
680	Capitolato Tecnico Lotto2	1.3.1	34	Application Security Testing	Requisito: Ai fini della valutazione economica del servizio “static application security testing”, deve essere presentata una quotazione - costo per singola applicazione - per la modalità one time ed una quotazione – canone annuale per applicazione - per la modalità continua per ciascuna delle seguenti fasce definite in base al numero di applicazioni: Domanda: Ai fini di un più corretto dimensionamento degli effort necessari per erogare il servizio, si chiede di fornire una stima del numero medio annuale di scansioni per applicazione da prevedere nell’erogazione del servizio in modalità continua (modello a canone)	Nel caso di quotazione annuale per applicazione non è previsto alcun limite al numero di scansioni effettuabili. In ogni caso, il Fornitore può, se necessario, valutare la frequenza attesa per applicazione in base alle sue esperienze pregresse.
681	Capitolato Tecnico Lotto2	1.3.1	34	Static Application Security Testing	Requisito: Ai fini della valutazione economica del servizio “static application security testing”, deve essere presentata una quotazione - costo per singola applicazione - per la modalità one time ed una quotazione – canone annuale per applicazione - per la modalità continua Domanda: Si chiede di indicare quale definizione di "applicazione" viene considerata o, in alternativa, se si lascia al Fornitore la possibilità di proporre opportuna definizione.	Si premette che per applicazione si intende un programma o un serie di programmi con accesso attraverso un login, ad uno o più domini collegati. Per il servizio di "static application security testing" si conferma che la quotazione è per singola applicazione costituita da un massimo di 100.000 linee di codice (LoC)
682	Capitolato Tecnico Lotto2	1.3.1	38	Application Security Testing	Requisito: Ai fini della valutazione economica del servizio "Dynamic Application Security Testing" dovrà essere presentata una quotazione - canone annuale per applicazione - per ciascuna delle seguenti fasce, definite in base al profilo del servizio e al numero di applicazioni: Fascia 1 - fino a 5 applicazioni, Fascia 2 - da 6 a 10 applicazioni, Fascia 3 - oltre 10 applicazioni. Domanda: Ai fini di un più corretto dimensionamento degli effort necessari per erogare il servizio, si chiede di fornire una stima del numero medio annuale di scansioni per applicazione da prevedere nell’erogazione del servizio in modalità continua (modello a canone)	Nel caso di quotazione annuale per applicazione non è previsto alcun limite al numero di scansioni effettuabili.In ogni caso, il Fornitore può, se necessario, valutare la frequenza attesa per applicazione in base alle sue esperienze pregresse.
683	Capitolato Tecnico Lotto2	1.3.3	39	Mobile Application Security Testing	Requisito: Ai fini della valutazione economica del servizio "mobile application security testing" deve essere presentata una quotazione - canone annuale per applicazione - per ciascuna delle seguenti fasce, definite in base al al numero di applicazioni: Fascia 1 - fino a 5 applicazioni, Fascia 2 - da 6 a 10 applicazioni, Fascia 3 - oltre 10 applicazioni. Domanda: Ai fini di un più corretto dimensionamento degli effort necessari per erogare il servizio, si chiede di fornire una stima del numero medio annuale di scansioni per applicazione da prevedere nell’erogazione del servizio in modalità continua (modello a canone)	Nel caso di quotazione annuale per applicazione non è previsto alcun limite al numero di scansioni effettuabili.In ogni caso, il Fornitore può, se necessario, valutare la frequenza attesa per applicazione in base alle sue esperienze pregresse.
684	Capitolato Tecnico Lotto2	1.3.4	40	Mobile Application Security Testing	Requisito: Per la raccolta di tali informazioni il Fornitore potrà avvalersi di strumenti automatizzati al fine di rilevare le potenziali vulnerabilità. Domanda: si chiede di confermare che il servizio potrà essere erogato con strumenti di tipo scanner fisicamente dedicati alle PA e layer di gestione virtualmente segregati e cifrati	Si conferma
685	Capitolato Tecnico Lotto2	1.3.4	40	Policy Sicurezza	Requisito: assegnazione automatica delle priorità/severità ai rischi di sicurezza sulla base delle policy concordate con l’Amministrazione; Domanda: Si chiede di confermare che l'assegnazione automatica delle priorità/severità ai rischi di sicurezza sarà possibile per gli asset per i quali l'Amministrazione avrà preventivamente definito le policy di assegnazione, in mancanza di policy concordate la priorità/severità sarà asssegnata secondo la tassonomia predefinita dallo strumento stesso	Si conferma

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
686	Capitolato Tecnico Lotto2	1.3.5	42	Data Loss Prevention	Requisito: generazione automatica di alert nel caso in cui vengano violate le policy di sicurezza definite, visibilità e controllo sui dati in movimento, sia che si trovino in messaggi e-mail, nella mail sul Web, nell'instant messaging, e nei protocolli di rete (DLP data in motion); Domanda: Si chiede di confermare che con la dicitura "dati in movimento" si intendono quelle attività di trasferimento dati che possono avvenire anche al di fuori del perimetro di rete aziendale.	Si conferma
687	Capitolato Tecnico Lotto2	1.3.5	42	Data Loss Prevention	Requisito: rilevazione dei dati che transitano nell'organizzazione, ovunque siano archiviati, e valutazione del rischio di perdita di dati (DLP Risk Assessment); analisi e classificazione dei dati (DLP Information classification); Domanda: si chiede di confermare che le variabili relative alle funzionalità di DLP risk assessment e DLP Information classification ove fornite dall'Amministrazione potranno essere utilizzate come valore d'ingresso per applicare le policy di rilevazione e/o blocco nell'ambito del servizio "data loss/leak prevention"	Si conferma
688	Capitolato Tecnico Lotto2	1.3.6	44	Data Base Security	Si fa presente che i vendor leader di mercato propongono un licensing per l'erogazione del servizio ad "istanza". Per poter correttamente dimensionare il pricing si chiede di poter suddividere le 3 fasce richieste sulla base del numero delle istanze e non sulla base del numero dei nodi. In caso di risposta negativa si chiede di specificare quale sia il numero massimo di istanze per nodo	Si veda risposta alla domanda 243.
689	Capitolato Tecnico Lotto2	1.3.6	44	Data Base Security	Requisito: Ai fini della valutazione economica del servizio "database security" nel caso di modalità erogazione in modalità "as a service" dovrà essere presentata una quotazione – canone annuale per nodo4 - per ciascuna delle seguenti fasce: Fascia 1: fino a 25 nodi Fascia 2: da 26 a 50 nodi Fascia 3: oltre 50 nodi Domanda: Allo scopo di un corretto dimensionamento del servizio si richiede di precisare per singolo nodo il numero massimo di istanze e per ogni istanza il numero massimo di transazioni per secondo che il servizio dovrà gestire.	Si veda risposta alla domanda 243.
690	Capitolato Tecnico Lotto2	1.3.6	44	Data Base Security	si chiede di confermare che per il servizio di "database security" non è prevista altra modalità di erogazione oltre a quella "as a service", come indicato alla voce "tipologia di servizio".	Si conferma
691	Capitolato Tecnico Lotto2	1.3.6		Data Base Security	Requisito: Dal punto di vista tecnico, il servizio deve prevedere almeno: compatibilità con almeno tre dei seguenti sistemi di database: Oracle, Microsoft SQL Server, IBM DB2, SAP Sybase e MySQL. Domanda: Si chiede di specificare se è richiesta la compatibilità con il sistema di database IBM DB2 anche in ambito mainframe.	La compatibilità con i database IBM DB2 in ambito mainframe non è richiesta.
692	Capitolato Tecnico Lotto2	1.3.7	45	Web Application Firewall	Si chiede conferma che i servizi "Web Application Firewall "e "Next Generation Firewall", siano due servizi acquistabili separatamente dalle amministrazioni, pur con gli stessi costi unitari.	Non si conferma. Il servizio in oggetto è disegnato come un unico servizio che prevede i requisiti e le funzionalità descritte nel par. 1.3.7 del Capitolato Tecnico Lotto2
693	Capitolato Tecnico Lotto2	1.3.7	45	Web Application Firewall	Requisito: Il Fornitore, nell'ambito dei servizi di "web application firewall" e "next generation firewall" deve garantire la disponibilità per l'amministrazione almeno delle seguenti funzionalità base / strumenti a supporto: … Domanda: si chiede di confermare che il Fornitore, nell'ottica del servizio erogato in modalità continuativa di tipo "as a service", debba limitarsi a rendere disponibile lo strumento che consenta all'Amministrazione di proteggere in autonomia le applicazioni web da attacchi esterni.	Si precisa che il servizio di "web application firewall e next generation firewall", come per tutti i servizi di sicurezza in modalità "as a service", è erogato dal Fornitore attraverso il Centro Servizi. Gli strumenti forniti sono gestiti esclusivamente dal Fornitore, che deve svolgere le attività descritte nel par. 1.3 del Capitolato Tecnico Lotto 2, ed in particolare produrre documenti e report, gestire gli incident di sicurezza e classificare le vulnerabilità in accordo con le policy dell'Amministrazione.
694	Capitolato Tecnico Lotto2	1.3.7	46	Web Application Firewall	Requisito: Il Fornitore, nell'ambito dei servizi di "web application firewall" e "next generation firewall" deve garantire la disponibilità per l'amministrazione almeno delle seguenti funzionalità base / strumenti a supporto: …. Domanda: Si chiede di confermare che le funzionalità WAF elencate non sono riferite alle sole soluzioni IDS o IPS	Si conferma

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
695	Capitolato Tecnico Lotto2	1.3.7	46	Web Application Firewall	Requisito: Ai fini della valutazione economica dei servizi “web application firewall” e “next generation firewall” dovrà essere presentata una quotazione – canone annuale - per ciascuna delle seguenti fasce, definite in base al throughput5: Fascia 1: throughput fino a 50 Mbps Fascia 2: throughput fino a 200 Mbps Fascia 3: throughput fino a 500 Mbps Domanda: Ai fini di un più corretto dimensionamento della piattaforma di erogazione del servizio, si chiede di esplicitare il numero massimo di siti http e https gestiti per fascia di throughput, rispettivamente nella fascia 1, 2 e 3	Si conferma che la quotazione dei servizi è richiesta in funzione del throughput gestito.
696	Capitolato Tecnico Lotto2	1.3.7	46	Web Application Firewall	Requisito: Il Fornitore, nell’ambito dei servizi di “web application firewall” e “next generation firewall” deve garantire la disponibilità per l’amministrazione almeno delle seguenti funzionalità base / strumenti a supporto: …. Domanda: si chiede di confermare che i gateway di processamento del traffico, analisi e blocking delle funzionalità di WAF e NGFW saranno fisicamente dedicati alle Pubbliche Amministrazioni, ma tramite layer di gestione virtualmente segregati e cifrati	Si conferma
697	Capitolato Tecnico Lotto2	1.3.7	45	Web Application Firewall	Requisito: Il Fornitore, nell’ambito dei servizi di “web application firewall” e “next generation firewall” deve garantire la disponibilità per l’amministrazione almeno delle seguenti funzionalità base / strumenti a supporto: …. Domanda: 1. In relazione al servizio WAF, si chiede di confermare che il Fornitore, nell'ottica del servizio erogato in modalità continuativa di tipo "as a service", debba limitarsi a rendere disponibile lo strumento che consenta all’Amministrazione di proteggere in autonomia le applicazioni web da attacchi esterni. 2. In relazione al servizio NGFW, si chiede di confermare che il Fornitore, nell'ottica del servizio erogato in modalità continuativa di tipo "as a service", debba limitarsi a rendere disponibile lo strumento che consenta all’Amministrazione di proteggere in autonomia le applicazioni web da attacchi esterni.	Si precisa che il servizio di "web application firewall e next generation firewall", come per tutti i servizi di sicurezza in modalità "as a service", è erogato dal Fornitore attraverso il Centro Servizi. Gli strumenti forniti sono gestiti dal Fornitore, che deve svolgere le attività descritte nel par. 1.3 del Capitolato Tecnico Lotto 2, ed in particolare produrre documenti e report, gestire gli incident di sicurezza e classificare le vulnerabilità in accordo con le policy concordate con l'Amministrazione.
698	Capitolato Tecnico Lotto2	1.3.8	46	Secure Web Gateway	Requisito: Il Fornitore, nell’ambito del servizio “secure web gateway” deve garantire la disponibilità per l’amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:… Domanda: si chiede di confermare che i gateway di processamento del traffico, analisi e blocking delle funzionalità di Secure web Gateway saranno fisicamente dedicati alle Pubbliche Amminbistrazioni, ma tramite layer di gestione virtualmente segregati e cifrati	Si conferma
699	Capitolato Tecnico Lotto2	1.3.8	46	Secure Web Gateway	Requisito: Il servizio di “secure web gateway” deve consentire 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. Domanda: si chiede di confermare che il Fornitore, nell'ottica del servizio erogato in modalità continuativa di tipo "as a service", debba limitarsi a rendere disponibile lo strumento che consenta all’Amministrazione di bloccare in autonomia l'accesso a siti web potenzialmente malevoli	Si precisa che il servizio di "secure web gateway", come per tutti i servizi di sicurezza in modalità "as a service", è erogato dal Fornitore attraverso il Centro Servizi. Gli strumenti forniti sono gestiti esclusivamente dal Fornitore, che deve svolgere le attività descritte nel par. 1.3 del Capitolato Tecnico Lotto 2, ed in particolare produrre documenti e report, gestire gli incident di sicurezza e classificare le vulnerabilità in accordo con le policy dell'Amministrazione.
700	Capitolato Tecnico Lotto2	1.3.8	46	Secure Web Gateway	Requisito: Il Fornitore, nell’ambito del servizio “secure web gateway” deve garantire la disponibilità per l’amministrazione almeno delle seguenti funzionalità base / strumenti a supporto: Domanda: si chiede di confermare che le funzionalità base non prevedono il riconoscimento degli utenti tramite integrazione con sistemi ldap o AD e che questo tipo di attività potrà essere erogata tramite richiesta e quotazione dei servizi professionali	Si conferma
703	Capitolato Tecnico Generale	5.1	48	Help Desk	Requisito: Entro l’orario di lavoro previsto (si veda Capitolo 9), le segnalazioni dovranno essere prese in carico da un addetto con i livelli di servizio definiti per la fornitura e dettagliati nelle relative Appendici ai Capitolati specifici di Lotto. Al di fuori di tale periodo l’Aggiudicatario deve garantire: la ricezione delle segnalazioni almeno attraverso il canale “e-mail” e via form web tramite portale; la ricezione di segnalazioni relative a malfunzionamenti (dai sistemi interni di monitoraggio) ed alle funzioni di sicurezza in maniera continuativa (24hx7gg); Domanda: Fermo restando la richiesta relativa alla ricezione delle segnalazioni relative a malfunzionamenti ed alle funzioni di sicurezza su base 24hx7gg, si chiede di chiarire la fascia oraria in cui dovranno essere presi in carico e gestiti gli incident di sicurezza.	Nella finestra H24 7 gg su 7 il concorrente deve garantire la disponibilità dei servizi elencati al capitolo 9 del Capitolato Tecnico Parte Generale, nel rispetto degli indicatori di qualità previsti, adottando gli strumenti e le modalità di presidio e intervento ritenuti più adeguati. Per tali servizi la gestione degli incident dovrà essere garantita, con le modalità e nei tempi previsti come descritto nel paragrafo 1.3 del Capitolato Tecnico Lotto2, nella finestra H24 7 gg su 7 p.

ID	Documento	Paragrafo	pagina	Argomento	Chiarimento	Risposta
878	Capitolato Tecnico Lotto2	1.1.1	10	Identity Provider	le credenziali di autenticazione associate alle identità digitali registrate sono rilasciate dal gestore del servizio mediante consegna in modalità sicura. Si chiede di specificare se esistano già modalità di consegna che sono ritenute sicure per il servizio in oggetto.	Le modalità di consegna previste dovranno essere sottoposte dai gestori ad AgID che ne valuterà l'adeguatezza. Si aggiunge che, in considerazione dell'oggetto, si ritiene che le modalità già autorizzate da AgID per la consegna delle credenziali di firma digitale possano essere applicabili anche alla consegna delle credenziali di autenticazione associate alle identità digitali.