AZIENDA OSPEDALIERO UNIVERSITARIA DI PARMA

Specifiche dell'architettura per l'integrazione con il LIS Anatomia Patologica (Athena di Dedalus SpA).

Interfacciamento infrastruttura di rete

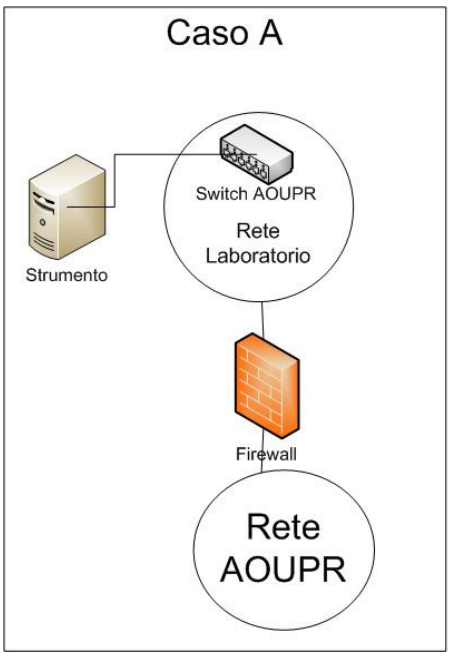
I computer preposti al controllo della strumentazione laboratoristica devono essere oggetto della fornitura e dovranno essere inseriti in rete Ethernet TCP/IP per l'integrazione con il LIS in uso presso i laboratori aziendali. Tali sistemi saranno inseriti nella sottorete IP dedicata ai Laboratori e saranno protetta da Firewall; è quindi fondamentale che vengano indicate le esigenze di connessione TCP in modo da configurare le opportune policy centrali.

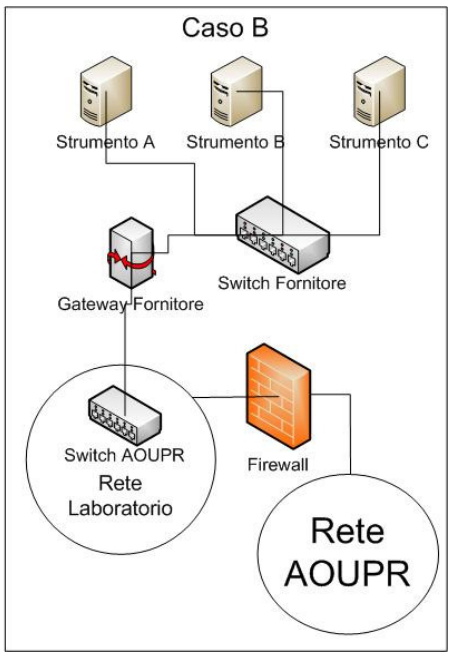
Verranno permesse soltanto le regole di comunicazione che consentono allo strumento di comunicare con l'integratore del gestionale di laboratorio e con il sistema proxy centralizzato per la navigazione su internet, tale sistema prevede obbligatoriamente la navigazione dietro autenticazione con credenziali presenti nel dominio aziendale; la navigazione sarà comunque ristretta ai soli siti web necessari al corretto funzionamento dello strumento e per la relativa teleassistenza.

L'elenco dei siti web dovrà essere obbligatoriamente fornito dall'aggiudicatario contestualmente al progetto esecutivo.

Sarà possibile inserire strumentazioni in due sole configurazioni:

A. Connessione diretta dello strumento alla rete ethernet tramite una porta dedicata con indirizzamento della rete dati di AOUPR;
B. Connessione di una sottorete dedicata con uno o più strumenti ed un solo computer dotato di doppia scheda di rete (middleware strumentale) come gateway da/verso la rete AOUPR tramite una sola porta ethernet. In tal caso dovranno essere ricompresi in fornitura gli apparati switch solo di tipo rackable necessari alla realizzazione.





A prescindere dal tipo di configurazione proposta, si precisa che: Tutti i costi sistemistici di adeguamento della infrastruttura, compresi i cablaggi di rete e collegamento dei nuovi dispositivi, saranno in carico alla ditta aggiudicataria. Si vedano anche le sezioni seguenti: Sezione Rete, Armadio aggiuntivo e Apparati.

Come previsto dalla normativa vigente, ove necessario conservare dati personali o sensibili dovranno essere garantite le funzionalità di back up e protezione da virus con strumenti oggetto di fornitura.

I sistemi offerti dovranno essere rispondenti al regolamento europeo GDPR, General Data Protection Regulation - Regolamento UE 2016/679, entrato in vigore per gli stati membri dal 2018.

I sistemi antivirus, posti a protezione dello strumento, potranno essere autonomi o potranno appoggiarsi alla infrastruttura di antivirus aziendale. Qualora il sistema antivirus fosse autonomo ogni onere di manutenzione e aggiornamento (obbligatori) saranno in carico alla ditta aggiudicataria. Qualora la ditta aggiudicataria decidesse di appoggiarsi alla infrastruttura antivirus esistente, saranno in carico alla ditta aggiudicataria i costi di adeguamento, estensione e configurazione del sistema antivirus.

Il fornitore dovrà garantire i sistemi di aggiornamento automatico delle patch software necessari alla rispondenza alle normativa sul trattamento dati, in particolare sarà possibile utilizzare, per i sistemi Windows, il servizio WSUS già presente sulla rete aziendale.

La teleassistenza sarà erogabile solo tramite VPN di tipo SSL-http e la connessione alle postazioni dovrà avvenire con software che permettano la criptazione dei dati trasmessi in rete; in caso di problemi sulla rete Internet, che rendano inefficace la connessione VPN, dovrà essere garantito l'intervento onsite rispettando gli SLA indicati in capitolato. Non sono permesse per policy aziendale connessioni di tipo P2P.

Nel caso in cui la teleassistenza venga fornita mediante la connessione in uscita, verso siti del produttore presenti su Internet, sarà condizione obbligatoria che la connessione avvenga solo dietro autorizzazione del personale che ha richiesto l'assistenza; dovrà essere fornito un report mensile dell'utilizzo di tale sistema.

Il sistema antivirus Aziendale (TrendMicro), cosi come la sottorete di network, dal Firewall agli switch, è in gestione al Servizio Informativo Aziendale.

Per tutti i sistemi forniti dovranno essere comunicate le credenziali di Amministratore in busta chiusa, che l'unità operativa di destinazione si riserva di custodire in segretezza ed utilizzare solo in caso di eventi critici o necessità ad elevato impatto sulle funzionalità di analisi.

Le modalità di installazione e configurazione delle apparecchiature oggetto di fornitura saranno oggetto di convalida preventiva da parte del Servizio Interaziendale Tecnologie dell'Informazione (SITI) in fase preliminare e quindi oggetto di collaudo finale.

Interfacciamento sistema informatico di laboratorio

La fornitura deve prevedere che lo strumento debba dialogare con il LIS per il tramite del middleware di laboratorio.

L'architettura del middleware è estremamente scalabile in modo tale che l'applicazione possa esser distribuita su più macchine server.

La comunicazione deve prevedere l'utilizzo di messaggistica HL7.

Lo scambio dati avverrà a mezzo messaggistica standard e preferibilmente tramite web service che saranno meglio precisati in fase di progetto esecutivo. Il sistema deve prevedere un completo sistema di gestione delle code di invio e di monitoraggio che tenga traccia di tutti i messaggi veicolati e ne consenta una pratica consultazione.

Nello scambio di dati devono esser gestite le varie fasi di lavorazione della richiesta / campione / blocchetto / vetrino (es. l'invio della programmazione allo strumento, le operazioni di taglio, la processazione dei blocchetti, la colorazione dei vetrini, il ritorno dei risultati, l'eventuale ritorno di immagini a corredo dei risultati…) e in particolare l'identificazione dell'utente con il rispettivo stato di lavorazione della richiesta (es.

validazione). Per una corretta identificazione, oltre all'invio dell'id richiesta/campione/blocchetto/vetrino, verrà inviato anche l'identificativo del paziente.

Sono a carico dell'aggiudicataria gli interi costi di interfacciamento verso il LIS e il middleware del produttore Dedalus Spa. A titolo esemplificativo e non esaustivo sono compresi i costi di licenze, moduli di integrazione, servizi di test e collaudo.

Le modalità di installazione, configurazione e scambio di messaggistica saranno oggetto di convalida preventiva da parte del Servizio Interaziendale Tecnologie dell'Informazione (SITI) in fase preliminare e quindi oggetto di collaudo finale.

Sezione Rete

Nei lotti di gara dove è richiesto esplicitamente l'interfacciamento al LIS, sono a carico dell'aggiudicataria la realizzazione dei punti rete necessari al collegamento in rete delle apparecchiature fornite. Nella realizzazione l'aggiudicataria dovrà tener presente che dovranno essere realizzate prese dati RJ45 (almeno CAT6) e che queste dovranno essere obbligatoriamente colorate (ROSSO o altro colore differente da quello già presente) per opportuna distinzione con i punti rete già preesistenti. Tali prese dovranno tutte attestarsi all'armadio aggiuntivo previsto, dettagliato nella sezione successiva.

Armadio aggiuntivo

Per il lotto 4: stampanti per vetrini on-demand, è a carico dell'aggiudicataria la fornitura di un armadio rack (A x L x P➔ 1975 x 600 x 1000 mm) per l'accorpamento delle funzionalità di networking al piano e il relativo collegamento verso l'armadio di padiglione (di proprietà del committente) al piano rialzato; il collegamento dovrà essere fornito in fibra ottica multimodo OM4 nella misura di 12 coppie. L'armadio dovrà avere una doppia alimentazione derivata dall'armadio di piano e da due interruttori separati ed alimentare i due moduli elettrici dell'armadio.

Apparati

Sono a carico della Ditta aggiudicataria del Lotto 4 la fornitura degli apparati di networking (solo hardware senza servizi accessori, come il servizio di manutenzione a carico del SITI dell'AO) necessari all'interfacciamento delle apparecchiatura con la rete aziendale. Per uniformità con l'attuale parco aziendale si specificano le tipologie e configurazioni di apparati di networking necessari da fornire:

QUANTITÀ	TIPOLOGIA	MARCA	MODELLO	CODICE
2	SWITCH	HP	5510	JH149A
4	ALIMENTATORE	HP		JD362B
2	MODULO 2 QSFP+	HP		JH155A
2	CAVO STACK	HP		JG326A
2	SWITCH	ARUBA	2930M	JL322A
4	ALIMENTATORE	ARUBA		JL087A
2	MODULO 4 QSFP+	ARUBA		JL083A
2	MODULO STACK	ARUBA		JL325A
2	CAVO STACK	ARUBA		J9734A
2	TRANSCEIVER 10Gbps	ARUBA	SFP+ LC LR	J9151E
4	TRANSCEIVER 1Gbps	ARUBA	SFP LC SX	4858D

AZIENDA USL DI PIACENZA

Specifiche dell'architettura per l'impianto di Anatomia Patologica

Interfacciamento infrastruttura di rete

I computer preposti al controllo della strumentazione devono essere oggetto della fornitura e dovranno essere inseriti in rete Ethernet TCP/IP per l'integrazione con Winsap, applicativo di laboratorio di anatomia patologica in uso presso i laboratori aziendali.

Tali sistemi saranno inseriti nella sottorete IP dedicata ai Laboratori ed è quindi fondamentale che vengano indicate le esigenze di connessione TCP in modo da configurare le opportune policy centrali.

Verranno permesse soltanto le regole di comunicazione che consentono allo strumento di comunicare con Winsap e con il sistema proxy centralizzato per la navigazione su internet, tale sistema prevede obbligatoriamente la navigazione dietro autenticazione con credenziali presenti nel dominio aziendale; la navigazione sarà comunque ristretta ai soli siti web necessari al corretto funzionamento dello strumento e per la relativa teleassistenza.

L'elenco dei siti web dovrà essere obbligatoriamente fornito dall'aggiudicatario contestualmente al progetto esecutivo.

Sarà possibile inserire strumentazioni in due sole configurazioni:

A. Connessione diretta dello strumento alla rete ethernet tramite una porta dedicata con indirizzamento della rete dati di AUSLPC;
B. Connessione di una sottorete dedicata con uno o più strumenti ed un solo computer dotato di doppia scheda di rete (middleware strumentale) come gateway da/verso la rete AUSLPC tramite una sola porta ethernet. In tal caso dovranno essere ricompresi in fornitura gli apparati switch necessari alla realizzazione.

Tutti i costi sistemistici di adeguamento della infrastruttura, compresi i cablaggi di rete e collegamento dei nuovi dispositivi, saranno in carico alla ditta aggiudicataria.

Come previsto dalla normativa vigente, ove necessario conservare dati personali o sensibili dovranno essere garantite le funzionalità di back up e protezione da virus con strumenti oggetto di fornitura.

I sistemi offerti dovranno essere rispondenti al regolamento europeo GDPR, General Data Protection Regulation - Regolamento UE 2016/679, entrato in vigore per gli stati membri dal 2018.

I sistemi dovranno appoggiarsi alla infrastruttura di antivirus aziendale.

Il fornitore dovrà garantire i sistemi di aggiornamento automatico delle patch software necessari alla rispondenza alle normativa sul trattamento dati, in particolare sarà possibile utilizzare, per i sistemi Windows, il servizio WSUS già presente sulla rete aziendale.

La teleassistenza sarà erogabile solo tramite VPN di tipo SSL-http e la connessione alle postazioni dovrà avvenire con software che permettano la criptazione dei dati trasmessi in rete; in caso di problemi sulla rete Internet, che rendano inefficace la connessione VPN, dovrà essere garantito l'intervento onsite rispettando gli SLA indicati in capitolato.

Nel caso in cui la teleassistenza venga fornita mediante la connessione in uscita, verso siti del produttore presenti su Internet, sarà condizione obbligatoria che la connessione avvenga solo dietro autorizzazione del personale che ha richiesto l'assistenza; dovrà essere fornito un report mensile dell'utilizzo di tale sistema.

Il sistema antivirus Aziendale (BitDefender), cosi come la sottorete, è in gestione alla Unità Operativa Sistemi Informativi, Telecomunicazioni e Reingegnerizzazione di Processo.

Per tutti i sistemi forniti dovranno essere comunicate le credenziali di Amministratore in modalità protetta, che l'unità operativa di destinazione si riserva di custodire in segretezza ed utilizzare solo in caso di eventi critici o necessità ad elevato impatto sulle funzionalità di analisi.

Le modalità di installazione e configurazione delle apparecchiature oggetto di fornitura saranno oggetto di convalida preventiva da parte dell'Ingegneria Clinica e dell'Unità Operativa Sistemi Informativi, Telecomunicazioni e Reingegnerizzazione di Processo in fase preliminare e quindi oggetto di collaudo finale.

Interfacciamento sistema informatico di laboratorio

La comunicazione deve prevedere l'utilizzo di messaggistica HL7. Lo scambio dati avverrà a mezzo messaggistica standard e preferibilmente tramite web. Il sistema deve prevedere un completo sistema di gestione delle code di invio e di monitoraggio che tenga traccia di tutti i messaggi veicolati e ne consenta una pratica consultazione.

Nello scambio di dati devono esser gestiti: l'invio della programmazione allo strumento, il ritorno dei risultati, l'eventuale ritorno di immagini a corredo dei risultati e l'identificazione dell'utente con il rispettivo stato di lavorazione della richiesta (es. validazione).

Per una corretta identificazione, oltre all'invio dell'id richiesta/campione, verrà inviato anche l'identificativo del paziente.

Sono a carico dell'aggiudicataria gli interi costi di interfacciamento verso Winsap e verso il produttore Engineering Ingegneria Informatica (titolo esemplificativo e non esaustivo sono compresi i costi di licenze, moduli di integrazione, servizi di test e collaudo)

Le modalità di installazione, configurazione e scambio di messaggistica saranno oggetto di convalida preventiva da parte dell'Ingegneria Clinica e dell'Unità Operativa Sistemi Informativi, Telecomunicazioni e Reingegnerizzazione di Processo in fase preliminare e quindi oggetto di collaudo finale.

AZIENDA USL DI REGGIO EMILIA

Integrazione con il Sistema Informativo Ospedaliero

Il sistema in oggetto, nelle sue componenti HW e SW, dovrà essere integrato nel Sistema Informativo Ospedaliero (SIO) dell'Azienda USL di Reggio Emilia (di seguito AUSL), nello specifico con il LIS di Anatomia Patologica. Le caratteristiche e i requisiti per tale integrazione sono indicate di seguito.

Il coordinamento delle attività di integrazione col SIO sarà svolto congiuntamente dal Servizio di Ingegneria Clinica (SIC) e Servizio Tecnologie Informatiche e Telematiche (STIT).

Infrastruttura di Rete e Client

La rete informatica dell'AUSL è costituita da una rete capillare di distribuzione sia di tipo wired che di tipo wireless, caratterizzata da due centri stella di campus.

La parte wired è realizzata con cavi a coppie UTP di cat.6 o cat.5e, secondo lo standard TIA/EIA 568. Gli apparati di rete di distribuzione sono tecnologia Cisco, con porte prevalentemente in switched-ethernet a 1Gb/sec con funzionalità POE e n.2 dorsali switched-ethernet a 1Gb/sec in fibra ottica dedicata verso i due centri stella. I centri stella sono tra loro collegati con doppio percorso fisico in fibra ottica e connettività 10Gb/sec.

L'unico protocollo di rete ammesso è il TCP/IP. L'architettura di rete è di tipo L3 routed per ogni armadio periferico, a cui è dedicata una sottorete (subnet) separata e distinta con indirizzi di classe C e default gateway distinti. Le connessioni verso Internet o reti "esterne" avvengono con richieste di-rette al firewall (no proxy aziendale) che effettua una verifica puntuale delle richieste e filtri web di security e antivirus/IDS.

La copertura wireless è realizzata con tecnologia Cisco secondo lo standard IEEE 802.1a/c/b/g/n ed è distribuita su tutti i reparti sanitari. L'infrastruttura è di tipo centralizzato e governata da Wireless Control System (WLC), con possibilità di controllo dei canali e di rilevazione delle interferenze radio-frequenza. L'autenticazione di rete è basata su una tecnologia PEAP con sicurezza WAP2-Enterprise e la crittografia dati utilizzata è AES, con necessità di supporto e verifica di certificato aziendale client.

I PC aziendali standard (client aziendale) sono dotati di immagine aziendale con sistema operativo Windows 7 o Windows 10 e utilizzano solo il protocollo di rete TCP/IP. Gli applicativi standard insta-lati sono: Microsoft SCCM, Antivirus TrendMicro OfficeScan 10, Suite di Microsoft Office 365.

Non è consentito, se non su esplicita autorizzazione dello STIT, l'inserimento di alcun dispositivo di rete estraneo alla infrastruttura di rete aziendale.

Requisiti Sistemistici

Qualora il sistema richieda l'installazione di software su client aziendali:

- **Eseguibili**: eventuali applicativi da installare o eseguire su client aziendali devono essere files eseguibili a 32 bit.

- **Setup**: Il setup della installazione dell'applicativo deve essere in tecnologia Windows Installer.
- **Collocazione applicativi su client aziendali**: I componenti (eseguibili, DLL o altro) delle applicazioni devono essere installati in %ProgramFiles%\<nome azienda>\<nome applicazione> se non sono condivisi. Se devono essere condivisi da altri applicativi in: directory file comuni\<nome società> o %ProgramFiles%\<nome società>\File condivisi.
- **Versione e Release**: per ogni applicativo software offerto deve essere chiaramente indicato il numero di versione e release.

Qualora il sistema preveda archiviazione dati:

- **Archiviazione Centralizzata**: il sistema deve prevedere l'archiviazione dei dati su server centrali (forniti col sistema o da ASMN)
- **Backup**: il sistema deve prevedere sistemi di backup dei dati. Il sistema di backup può appoggiarsi sulla infrastruttura sistemistica ASMN; in tal caso è necessario fornire dettagli sulla implementazione (maggiori dettagli sulla infrastruttura disponibili presso STIT ASMN). Il sistema di backup deve fornire esplicito reporting sull'avvenuto backup.
- **Test di Restore**: il progetto del sistema di backup deve prevedere test periodici di restore da backup.

Requisiti Applicativi

- **Autenticazione**: il sistema deve prevedere sistemi di autenticazione all'accesso. Tale autenticazione deve soddisfare i requisiti minimi di sicurezza imposti dalla legislazione vigente (in termini di scadenza password, complessità password, ed altri). E' preferibile appoggiarsi alla infrastruttura sistemistica AUSL, che fornisce servizi LDAP per autenticazione centralizzata.
- **Profilazione Utenti**: il sistema deve prevedere la profilazione utenti (attribuzione di diritti differenziati a seconda dei ruoli). In particolare, è necessario che le attività di amministrazione di sistema siano delegate ad un utente specifico (amministratore di sistema), chiaramente individuato tra il personale AUSL in fase di installazione e collaudo e comunicato a SIC e STIT AUSL.
- **Tracciabilità degli accessi**: il sistema deve prevedere tracciamento degli accessi (a livello di sessione, singola sezione e singolo dato); oggetto del tracciamento devono essere sia gli accessi in semplice lettura che gli accessi in modifica/inserimento.
- **Strumenti di Backoffice / Amministrazione di sistema**: assieme al sistema devono essere forniti strumenti software di amministrazione di sistema (e relativa documentazione) che prevedano le funzionalità di:
    - Rettifica dati anagrafici
    - Rettifica dati clinici
    - Accesso ai log di tracciabilità
    - Gestione utenti

  In nessun caso le attività amministrative di cui sopra devono essere delegate in esclusiva al fornitore del sistema.

Elementi di Sicurezza (applicabili a qualsiasi elaboratore, sia client che server, oggetto della fornitura):

- **Antivirus**: il sistema deve prevedere, per gli elaboratori parte della fornitura HW, la copertura con sistema antivirus, e relative politiche di aggiornamento (che non prevedano intervento esplicito degli operatori sanitari). Il sistema può appoggiarsi alla infrastruttura sistemistica antivirus AUSL (maggiori dettagli sulla infrastruttura disponibili presso STIT AUSL). Qualora il sistema debba

escludere esplicitamente la presenza di antivirus, o preveda politiche non convenzionali di gestione dell'antivirus, è richiesta esplicita dichiarazione da parte del fornitore.

- **Aggiornamenti S.O.** : il sistema deve prevedere, per gli elaboratori parte della fornitura HW, sistemi autonomi di aggiornamento del S.O. (che non prevedano intervento esplicito degli operatori sanitari). Il sistema può appoggiarsi alla infrastruttura sistemistica AUSL (maggiori dettagli sulla infrastruttura disponibili presso STIT AUSL). Qualora il sistema debba escludere esplicitamente aggiornamenti del S.O., è richiesta esplicita dichiarazione da parte del fornitore.
- **Monitoraggio**: il sistema può prevedere sistemi di monitoraggio remoto, a scopo assistenza on-demand, servizi di manutenzione remota, o monitoraggio pro-attivo.

Architettura di Collegamento verso il LIS

Il sistema (inteso come l'insieme dei dispositivi , workstations, servers ed ogni altro elemento attivo che lo compone) deve essere collegato al Sistema Informativo Ospedaliero, e più nello specifico al LIS di Anatomia Patologica (Sistema Informativo di Laboratorio di Anatomia Patologica) interfacciandosi con i sistemi Athena (componente di laboratorio) o R4C (componente di refertazione) fornite da Dedalus S.p.a..

Ogni comunicazione da e verso il LIS (es. trasmissione liste di lavoro, ricezione esiti, messaggistica diagnostica e di check-in check-out, ed ogni altro flusso informativo previsto nel presente capitolato) deve avvenire attraverso il collegamento sopra descritto.

Se previsti dalle specifiche funzionali del capitolato, potrebbero essere previste modalità di dialogo con il LIS tali da gestire l'inserimento diretto di campione in macchine, e imputazione dell'anagrafica a posteriori attraverso interrogazione del SIO.

Oneri in carico all'Offerente

Sono a carico dell'offerente (e da indicare esplicitamente in offerta):

- Tutti i costi di licenza legati a moduli software parte della fornitura
- Tutti i costi di licenza legati a moduli software necessari per adeguare Middleware LabOnLine e LIS Concerto al collegamento con i dispositivi oggetto della fornitura
- Tutti i costi di adeguamento hardware che si rendessero necessari ai supporti dei sistemi LabOnLine e Concerto conseguenti all'introduzione dei dispositivi oggetto della fornitura

Documentazione in Offerta Tecnica

L'offerta tecnica deve prevedere:

- Descrizione dettagliata delle modalità di adesione ai requisiti sopra esposti
- Diagramma di architettura di collegamento
- Elenco delle tipologie di messaggistica verso middleware
- Elenco dei moduli software di terze parti oggetto della fornitura, e relative modalità di licenza
- Elenco delle attività di adeguamento necessarie su dispositivi e sistemi già in essere presso AUSL