A.S. 2018-2019

Ministero dell'Istruzione, dell' Università e della Ricerca

ITIA – ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITIA - INFORMATICA E TELECOMUNICAZIONI
ARTICOLAZIONE INFORMATICA
Tema di: SISTEMI E RETI - ***Tipologia C***

Il candidato svolga la prima parte della prova e due tra i quesiti proposti nella seconda parte.

PRIMA PARTE

Per favorire il turismo culturale, l'Assessorato al Turismo di una città d'arte di medie dimensioni intende realizzare un'infrastruttura tecnologica che offra ai visitatori un servizio per la fruizione di contenuti multimediali che descrivono i "punti di interesse" (Point Of Interest = POI) di tipo monumentale (es. chiese, luoghi storici, …) e artistico (es. musei, mostre, …) distribuiti nel centro storico della città.

Per il servizio, si è deciso di erogare i contenuti multimediali sotto forma di pagine web, secondo due possibili formati denominati "pagina multimediale di base" e "pagina multimediale avanzata".

Nella pagina multimediale di base sono previsti:.

- un video di presentazione breve del POI della durata tipica di un minuto esclusivamente in italiano con sottotitoli in inglese;
- un massimo di tre immagini relative al POI (es. dettagli architettonici, quadri, ...) con relativa didascalia in italiano ed inglese.

Nella pagina multimediale avanzata sono previsti:

- un video di presentazione approfondita del POI della durata tipica di cinque minuti in una fra 7 possibili lingue compreso l'italiano;
- una galleria di una ventina di immagini con relativa descrizione (tipicamente intorno ai 500 caratteri) in una fra 7 possibili lingue compreso l'italiano.

Il visitatore, acquistando il servizio in uno dei chioschi (InfoPoint) dislocati nella città, riceverà un biglietto con cui potrà avere accesso ai due tipi di pagina sulla base di tre possibili tariffe:

- "tariffa base": permette la fruizione di una pagina multimediale di base per ciascun POI;
- "tariffa intermedia": consente la fruizione di pagine multimediali avanzate per tre POI a scelta dell'utente e pagine di base per gli altri;
- "tariffa piena": consente la fruizione di pagine multimediali avanzate per ogni POI della città.

Il biglietto acquistato riporta la password di accesso ai contenuti, univoca per ciascun visitatore, associata al tipo di tariffa pagata e con validità giornaliera.
In relazione alle funzionalità che il servizio dovrà offrire, l'Assessorato richiede che siano soddisfatti i seguenti vincoli progettuali:

- la consultazione delle pagine multimediali sia abilitata esclusivamente ai dispositivi (minitablet) forniti all'atto dell'acquisto del biglietto, previa consegna di un documento di identità o di un numero di carta di credito valida;
- per facilitare l'aggiornamento periodico dei contenuti esistenti e l'inserimento di nuovi, gli stessi non siano memorizzati sui dispositivi utilizzati dagli utenti ma su sistemi server;
- l'accesso alle pagine multimediali sia effettuabile solo dopo l'inserimento, all'inizio della visita, della password presente nel biglietto;
- l'accesso alle pagine multimediali relative ad un POI debba avvenire solo in prossimità o all'interno del POI stesso;
- la restituzione dei dispositivi (minitablet) possa avvenire presso l'InfoPoint che ha in custodia il documento di identità oppure presso un qualsiasi InfoPoint se il visitatore ha optato per lasciare il numero di carta di credito valida.

Il candidato analizzi la realtà di riferimento e, fatte le opportune ipotesi aggiuntive, individui una soluzione che a suo motivato giudizio sia la più idonea a sviluppare i seguenti punti:

1. il progetto, anche mediante rappresentazioni grafiche, dell'infrastruttura tecnologica ed informatica necessaria a gestire il servizio nel suo complesso, dettagliando:
   a) l'architettura della rete e le caratteristiche del o dei sistemi server, motivando anche la scelta dei luoghi in cui installare questi ultimi;
   b) le modalità di comunicazione tra server e dispositivi consegnati ai visitatori, descrivendo protocolli e servizi software da implementare per gestire la rete e fornire le pagine;
   c) gli elementi dell'infrastruttura utili a limitare la fruizione delle pagine multimediali esclusivamente in prossimità o all'interno dei POI a cui si riferiscono;
2. il progetto della base di dati per la gestione del servizio sopra descritto: in particolare si richiedono il modello concettuale ed il corrispondente modello logico;
3. la progettazione delle pagine web che consentono all'utente, in possesso di biglietto con tariffa base, la fruizione dei contenuti multimediali relativi al POI presso cui si trova, codificandone una porzione significativa in un linguaggio a scelta;
4. l'analisi di massima delle possibili modalità di gestione delle tre fasce tariffarie, delle opzioni offerte all'utente per la scelta dei tre POI nel caso della tariffa intermedia, e della scelta della lingua nel caso delle tariffe intermedia e piena.

SECONDA PARTE

Il candidato risponda a due quesiti a scelta tra quelli sotto riportati.

I. In relazione al tema proposto nella prima parte, si vuole offrire ai visitatori la possibilità di inserire via web un commento ed un voto di gradimento su ogni POI visitato. Effettuata a tale scopo una opportuna integrazione della base di dati, si realizzi, codificandola in un linguaggio a scelta, una pagina web che consente la visualizzazione della media dei voti ricevuti da ciascun POI.

II. In relazione al tema proposto nella prima parte, si discuta la possibilità di allargare la fruizione dei contenuti multimediali anche ai dispositivi personali degli utenti. In particolare, si analizzino le seguenti due ipotesi alternative:

   o uso limitato ai soli dispositivi (minitablet) forniti all'atto dell'acquisto del biglietto, come sopra descritto: si individuino possibili soluzioni per impedire l'accesso alle pagine multimediali attraverso dispositivi non forniti dagli InfoPoint;

- uso consentito ai dispositivi personali degli utenti (es. smartphone): si descriva una possibile integrazione del servizio volta a consentire la fruizione dei contenuti direttamente ad un singolo dispositivo di proprietà del visitatore, pur mantenendo i vincoli di fruibilità in base alla tariffa associata al biglietto.

III. Nella realizzazione e gestione di una base di dati accessibile da categorie di utenti con differenti ruoli, sono di rilevante importanza gli aspetti relativi alla sicurezza dei dati. Ad esempio, si supponga che nella realtà scolastica il personale della "Segreteria Alunni" non debba accedere ai dati del personale docente, il personale della "Segreteria Docenti" non debba accedere all'elenco dei fornitori della scuola, ecc. Il candidato approfondisca la tematica proposta discutendo gli strumenti offerti dai sistemi DBMS per creare utenze che abbiano un accesso libero alla totalità dei dati o limitato a parte di essi, in termini di operazioni consentite, in base al ruolo ricoperto nell'organizzazione. Produca quindi esempi significativi, nel contesto proposto della segreteria scolastica, nel linguaggio fornito dal DBMS di sua conoscenza.

IV. Per le aziende che dispongono di sedi dislocate in varie località sorge spesso la necessità di consentire al personale l'accesso ai sistemi da postazioni remote. Il candidato discuta le tipologie e i protocolli di accesso remoto ai sistemi, indicando in particolare le possibilità offerte dalle connessioni VPN. Sviluppi poi esempi nel caso di una azienda che ha due sedi operative e agenti commerciali che, muovendosi sul territorio, hanno necessità di collegarsi al sistema informativo aziendale.

_____

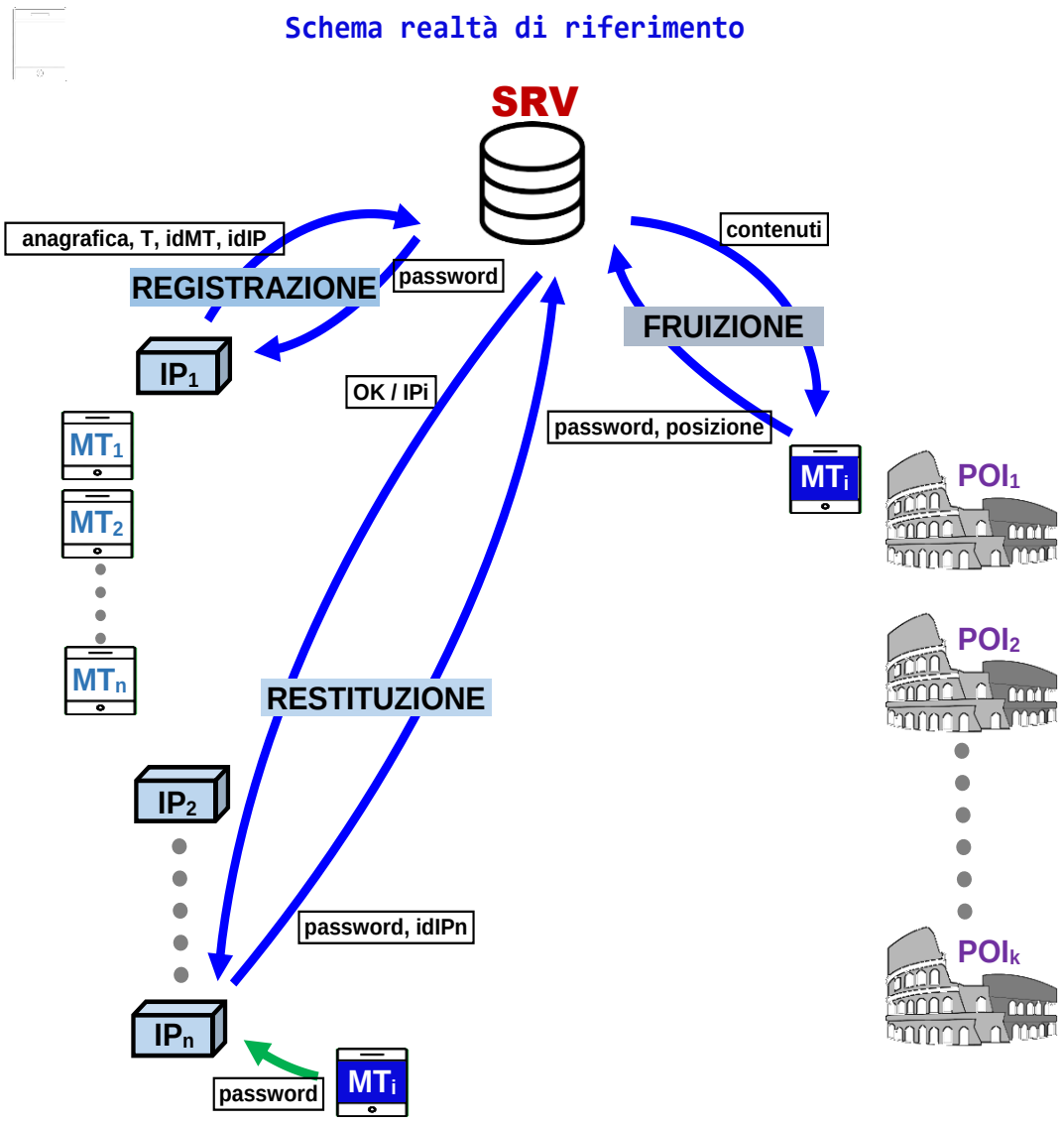
Durata massima della prova: 6 ore.
È consentito soltanto l'uso dei manuali dei linguaggi di programmazione (language reference) e di calcolatrici scientifiche e/o grafiche purché non siano dotate di capacità di calcolo simbolico (O.M. n. 205 Art. 17 comma 9).
È consentito l'uso del dizionario bilingue (italiano-lingua del paese di provenienza) per i candidati di madrelingua non italiana. Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dall'inizio della prova.

SOLUZIONE

Il testo mostra una realtà di riferimento che può essere affrontata in vari modi, pertanto sarà proposto il modo che risulta più semplice, ovvero sfruttando come elemento di localizzazione del POI la sua posizione geografica, invece di un dispositivo elettronico di targa come un QR, un transponder o un beacon.
In questo modo la realtà di riferimento dipenderà solo da elementi software e l'hardware coinvolto dovrà affrontare solo problemi di scambio dati.

PRIMA PARTE Quesito 1

Il testo prevede i seguenti elementi funzionali, sintetizzati nello schema con i relativi flussi di dati (**IP**, Information Point; **POI**, Point Of Interest; **MT**, MiniTablet; **SRV**, Server dei dati):



Gli IP sono multipli, potrebbero essere implementati con un chiosco informatico e relativo distributore (di MT, anch'essi multipli).

I POI sono multipli e in realtà sono elementi virtuali: ogni POI è identificato dalla sua posizione geografica registrata in una tabella.
IP, MT e POI hanno tutti un identificativo univoco (es., per i MT potrebbe essere l'indirizzo MAC).
Un client HTTP/S su IP fornisce l'interfaccia all'utente per avviare la fase di **REGISTRAZIONE** (vedi figura).
SRV è un classico server HTTP/S su DMZ che fornisce il servizio di REGISTRAZIONE restituendo un id univoco all'utente (**password**) ed emettendo un biglietto (inutile).
L'IP rilascia, se autorizzato da SRV, il **MTi** all'utente.
Quando l'utente si trova nei pressi di un POI, può avvenire la fase di **FRUIZIONE**: esso agisce sull'interfaccia del client HTTP/S sull'MT inviando la propria posizione e la password al server SRV.
Se la posizione ricevuta entra nell'intervallo di prossimità del POI, il SRV rilascia i contenuti.
Infine l'utente ritorna all'IP d'origine (o a un altro, nel caso previssto dal testo) e agisce avviando la fase di **RESTITUZIONE**.
In questo caso l'MT viene rilevato dall'IP prossimo tramite un NFC (o similare), l'IP fornisce al server SRV i dati per la restituzione e il server SRV accetta o rifiuta la restituzione a seconda che l'IP di restituzione sia corretto.

In definitiva:

a) I server in gioco sono:

SRV, collocato in un luogo qualsiasi del territorio, con linea pubblica a indirizzo IP statico, normali caratteristiche tecniche di macchina server: XEON, RAID, backup periodici, linea pubblica in failover;
IP, server NFC, per rilevare l'MT in restituzione.
L'IP, potrebbe essere un PC industriale, disco SSD, connessione pubblica analoga a quella di una rete residenziale con IP dinamico, linea cablata quando possibile, wireless LTE/4G in altri casi. Possiende un rilevatore NFC o simile (server NFC)

b) Il MT comunica con il server SRV via client HTTP/S ovvero App dedicata su HTTP/S
c) L'infrastruttura garantisce la fruizione con prossimità verso i POI tramite geolocalizzazione implementata ad esempio con Google Maps API sull'MT ([NB])

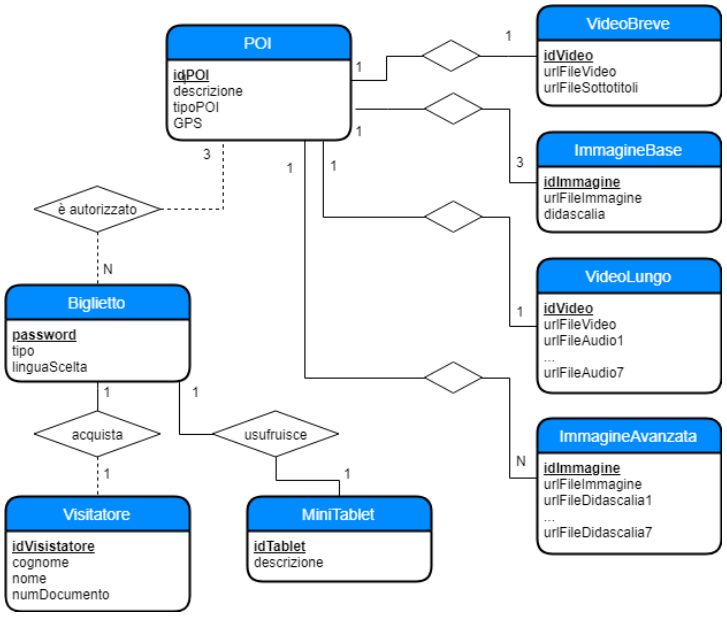
Ovviamente il MT ha una connessione pubblica wireless LTE/4G, un dispositivo GPS e un localizzatore NFC

Vista la criticità in termini di sicurezza di alcuni dati (vedi GDPR), le anagrafiche con i dati della carta di credito potranno essere archiviati in un DB accessorio situato nella rete Trust del server SRV, e quindi virtualmente e praticamente inaccessibile dalla rete pubblica

NB.
La geolocalizzazione potrebbe avere malfunzionamenti all'interno degli edifici. In questo caso vanno collocati presso i POI opportuni sistemi di tag (QR, transponder, beacon) per completare la fruizione.

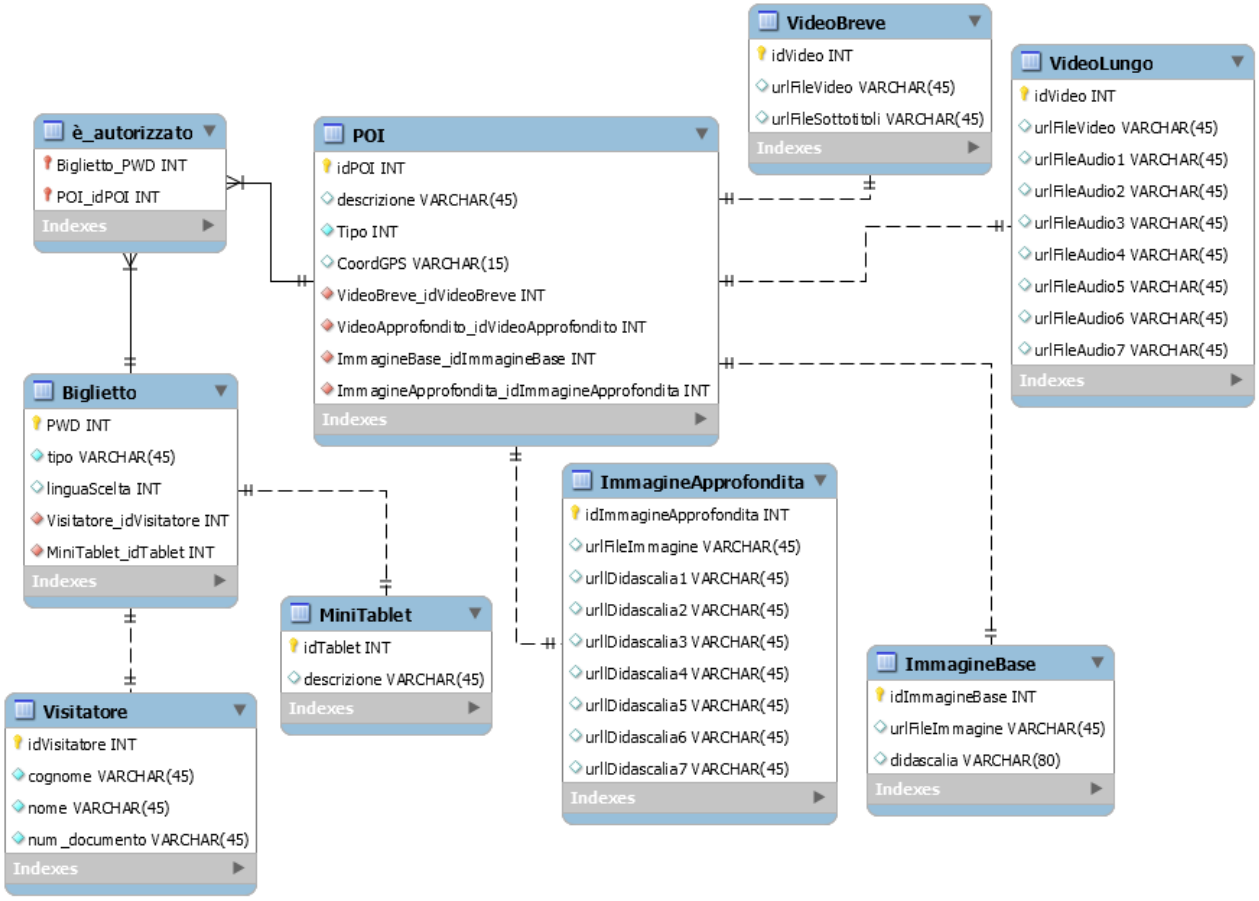
PRIMA PARTE Quesito 2

Modello concettuale



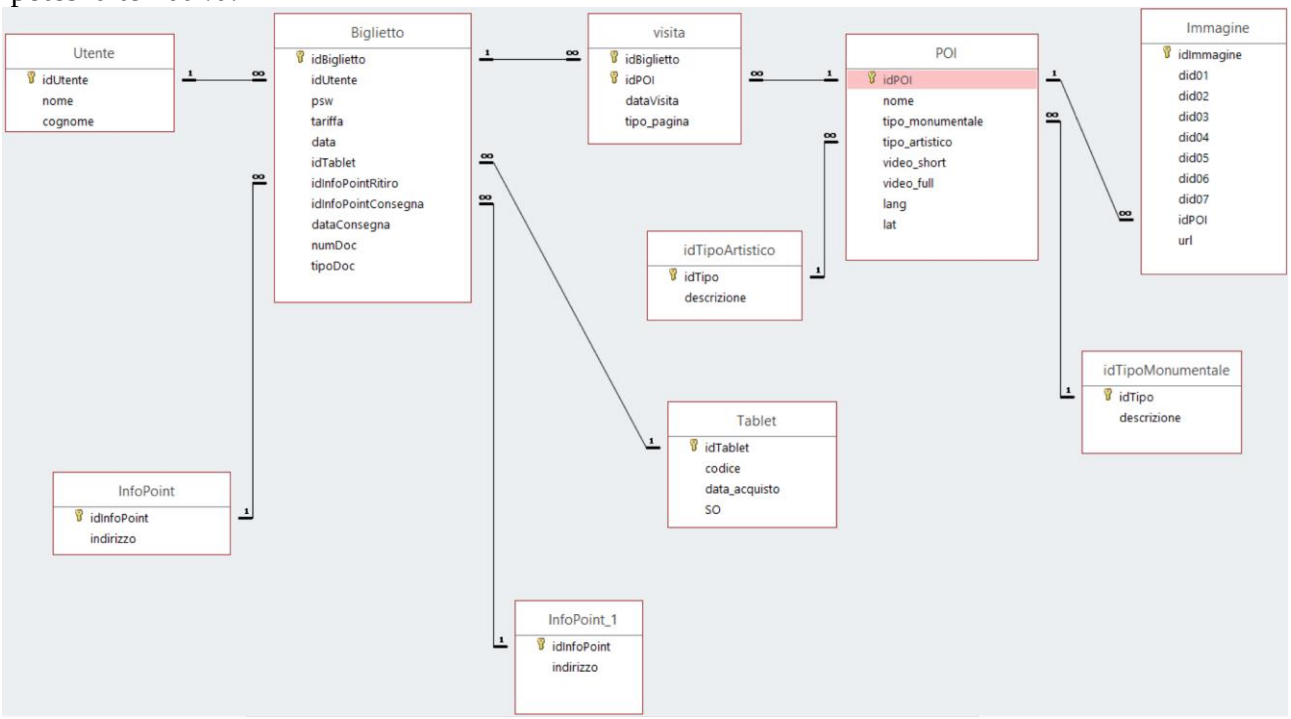
In questa proposta le informazioni associate agli utenti vengono mantenute nella base di dati anche dopo la conclusione della visita. Le informazioni associate ai biglietti sono mantenute solo per il periodo della visita e vengono eliminate al termine di questa, la password viene quindi generata in modo univoco solo in relazione ai biglietti in quel momento attivi. È possibile eventualmente mantenere tali informazioni in un database "storico" a fini statistici.
Le informazioni multimediali (file video, tracce audio e descrizioni testuali delle immagini) sono memorizzate in file esterni alla base di dati, nel database sono presenti i riferimenti a tali file.
Al momento dell'acquisto del biglietto viene richiesto, in base alla tipologia scelta, di selezionare la lingua per la fruizione dei contenuti multimediali (tariffa "intermedia" e tariffa "piena") e i 3 POI per i quali si richiede la pagina multimediale avanzata.
Per semplificare lo schema viene rappresentata un'unica entità "Biglietto" contenente le informazioni necessarie per tutte le tipologie, in questo modo alcuni attributi non saranno eventualmente valorizzati.
Le informazioni relative ai video e alle immagini associate ai POI sono rappresentate in entità esterne per favorire la modifica e sostituzione di questi in modo più semplice.

Modello logico



Modello logico alternativo

In questo caso viene proposto un modello logico relativo a un differente modello relazionale, come ipotesi alternativa.



PRIMA PARTE Quesito 3

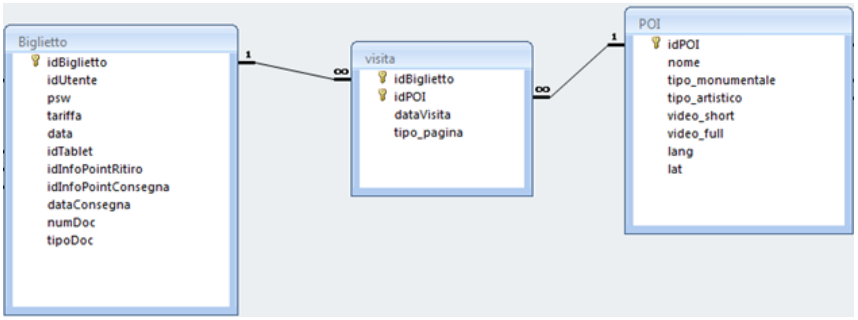
Una proposta in linguaggio PHP della pagina web che consente all'utente in possesso del biglietto di fruire dei contenuti multimediali del POI:

```php
<!DOCTYPE html>
/* Questo codice php hostato nell'app sul server viene richiamato con i parametri
   "poi" = il codice dell punto interesse precedentemente individuato
   "percorsoBase" = percorso delle risorse multimediali definito nella configurazione dell'app
   "biglietto" = codice del biglietto
   "password" = password del biglietto */
<html>
<head>
    <meta charset="utf-8" />
    <title>Visualizzazione immagini POI</title>
</head>

<body>
<?php
    $host = "localhost";
    $user = "root";
    $password = "";
    $db = "POI";

    $poi = $_GET["poi"];
    $biglietto = $_GET["biglietto"];
    $percorsoBase = $_GET["percorsoBase"];
    $password = $_GET["password"];

    $connect = new mysqli($host, $user, $password, $db);
    if ($connect->connect_error) {
        die("Errore connessione: " . $connect->connect_error);
    }
    // verifica se il biglietto in possesso ad un utente da diritto alla fruizione base dei contenuti POI
    $sql = "SELECT * FROM BIGLIETTI where codBiglietto = ".$biglietto;
    $result = $connect->query($sql);

    if ($result->num_rows > 0 && $result["password"] == $password) { //biglietto esistente e password coincidente
        $riga = $result->fetch_assoc()
        if $riga["tipo_tariffa"] == 0) { // è tariffa base
            $sqlPOI = "SELECT * FROM POI where codPOI = ".$poi;
            $resultPOI = $connect->query($sqlPOI);
            $rigaPOI = $resultPOI->fetch_assoc();

            echo "Immagini base di ".$rigaPOI["Descrizione"];
            $sqlImmagini = "SELECT * FROM immaginiBase where codPOI = ".$poi;
            $resultImmagini = $connect->query($sqlImmagini);

            if ($resultImmagini->num_rows > 0) {
                while($rigaImmagine = $resultImmagini->fetch_assoc()) {
                    // leggi tutte le immagini base associate al POI
                    echo "<img src='". $percorsoBase . "/" . $rigaPOI["immagine"]. "' />";
                }
            }
            else {
                echo "0 risultati";
            }
        }
    }
    else {
        echo "0 risultati";
    }
    $connect->close();
?>
</body>
</html>
```

PRIMA PARTE Quesito 4

Riferendosi allo schema del **Modello Logico Alternativo**, si parte dal presupposto di avere 3 fasce tariffarie; l'indicazione sulla fascia selezionata dal biglietto sarà memorizzata nel campo TARIFFA della tabella BIGLIETTO; per comodità sarebbe bene avere tali informazioni anche in sessione una vota eseguito l'accesso:

- **TARIFFA BASE** (valore 0): l'utente può visualizzare tutte e sole le pagine con le informazioni base. Se è eseguita una richiesta ad una pagina con informazioni approfondite tale richiesta è rifiutata.
  Non è necessario salvare l'informazione di visita sulla tabella VISITA, anche se potrebbe essere utile avere uno storico
- **TARIFFA INTERMEDIA:** l'utente può visualizzare tutte le pagine con le informazioni base e solo 3 pagine diverse con informazioni approfondite
  Ad ogni richiesta di una pagina con informazioni approfondite, la pagina dovrà verificare che non siano già state visualizzate 3 pagine diverse da se stessa con una opportuna query (esposta nel seguito). Se la verifica è corretta la pagina sarà visualizzata ed un nuovo record di visita sarà salvato nella tabella VISITA riportante i valori idBiglietto, idPOI, la data altrimenti la richiesta sarà rifiutata
- **TARIFFA PIENA: l'utente può visualizzare tutte le pagine**
  Non è necessario salvare l'informazione di visita sulla tabella VISITA, anche se potrebbe essere utile avere uno storico



Nel caso si voglia tenere uno storico sarà necessario avere un campo tipo_pagina che indichi se è stata richiesta una pagina base o dettagliata; questo campo dovrà essere inglobato nella chiave primaria composta.
La query per verificare quante visite di pagine dettagliate siano già state fatte può essere la seguente (si consideri che la richiesta sia effettuata da un biglietto identificato da **password** e per un **POI** con **id =1**).

```
SELECT Count(visita.idPOI) AS ContaVisite
FROM Biglietto INNER JOIN visita ON Biglietto.idBiglietto = visita.idBiglietto
WHERE (((visita.tipo_pagina)="full_page") AND ((Biglietto.psw)="password") AND ((visita.idPOI)<>1));
```

Il controllo `(visita.idPOI)<>1)` permetterà di visualizzare più volte le 3 pagine selezionate, cosa che può essere utile in casi di caduta di connessione o malfunzionamenti.

SECONDA PARTE Quesito 1

SECONDA PARTE Quesito 2

Per quanto riguarda l'uso limitato ai soli dispositivi MT MiniTablet è sufficiente che l'invio dei dati di REGISTRAZIONE (vedi **Schema realtà di riferimento**) contenga l'id. univoco del MiniTablet (**idMT** nello Schema): la sua assenza o la sua incongruenza impediscono al server SRV di autorizzare la **REGISTRAZIONE**.
Il caso alternativo è risolto invece inviando come **idMT** un id. univoco associato al dispositivo personale (es., il MAC Address). In questo caso il server SRV identificherà la richiesta come proveniente da un dispositivo personale, rilascerà la **password** ma escluderà la fase di **RESTITUZIONE**.
Il dispositivo personale, però, è opportuno che effettui la fase di REGISTRAZIONE tramite una App appositamente installata.

SECONDA PARTE Quesito 3

SECONDA PARTE Quesito 4

I modi di accesso da remoto ad una organizzazione sono vari.
Nell'ordine:

- Telnet / SSH
- Desktop Remoto RDP (Microsoft Terminal Server)
- controllo remoto (Team Viewer et altri)
- VPN

Ognuna di queste metodologie ha le proprie caratteristiche e funzioni, compresi criteri di sicurezza che, trattandosi di accessi da rete pubblica (canale non sicuro) sono particolarmente esposti a rischi di effrazione informatica.
SSH si utilizza sostenzialmente a livello sistemistico (amministrativo), per effettuare accessi tramite i più disparati protocolli. Si tratta di uno strumento versatile e consente anche un login classico alla rete di una organizzazione potendo contare però solo su una interfaccia a carattere.
SSH non ha bisogno di una banda larga per funzionare.
Desktop Remoto, ovvero accessi tramite protocollo RDP riguardano anche utenze non amministrative che, per qualche ragione, hanno necessità di autenticarsi su un ben determinato host della rete dell'organizzazione, tipicamente una macchina server. Si tratta di una modalità estremamente efficace dato che consente un approccio grafico con mouse e tastiera, ma che comporta numerosi rischi alla sicurezza. Inoltre necessita di una banda abbastanza ampia per supportare discreti carichi di informazioni.
I protocolli di sicurezza che sostengono RDP infatti garantiscono solo segretezza, cifrando i pacchetti con chiavi ottenute tramite certificato digitale: l'autenticazione, quindi è asimmetrica (solo il server si autentica verso il client). In questo modo RDP è vulnerabile ad attacchi di forza bruta. Inoltre il login su una ben preciso server della rete dell'organizzazione, se violato, può condurre a disastri.
Il **controllo remoto**, infine, è una pratica molto allettante ma, di nuovo non consigliabile su reti aziendali: l'applicativo, infatti, opera solo a livello HTTP, pertanto è del tutto insicuro: inoltre la sua violazione comporta di nuovo conseguenze letali: il possesso della sessione di un utente autorizzato autenticato sulla rete aziendale può causare danni enormi.
La soluzione ideale per un accesso da remoto rimane quindi **VPN**.
In questo caso l'accesso è vigilato da uno stack completo di sicurezza: autenticazione, segretezza e integrità, che operano a livello 3 IP (IPSec) utilizzando un tunnel sulla rete pubblica, utilizzando chiavi asimmetriche che generano al volo chiavi simmetriche di cifratura. Ogni singolo protocollo di

sicurezza è negoziabile e l'accesso non avviene su un host della rete aziendale, ma tramite appliance dedicati (es. Firewall).
Una volta avuto accesso con un client VPN, sì è discretamente sicuri anche nell'usare RDP o simili.
In questo caso gli utenti mobili che accedono via VPN entrano a tutti gli effetti come utenti della rete aziendale, acquisendo un proprio IP privato dello schema di indirizzamento previsto dall'Azienda e operando come utente registrato sul dominio interno (quindi con i privilegi previsti da Actiive Directory o Samba).
Ogni risorsa disponibile all'interno dell'Azienda è ora disponibile da remoto, con la sola limitazione delle prestazioni.

Testi di:

Sistemi e reti
prof. Paolo Ollari
prof. Ramon Ugolotti

Informatica
prof. Alberto Ferrari
prof. Corrado Pagani
prof. Alberto Paganuzzi
prof. Maurizio Mercuri
prof. Fabrizio Sacco

2019 - ITIS "L. Da Vinci", Parma