"InfoCamere"

Società Consortile di Informatica delle Camere di Commercio Italiane per azioni

Telemaco - Specifiche tecniche

Specifiche Telemaco per intermediari

Indice generale

1 Introduzione al documento

Il documento ha l'obiettivo di presentare le specifiche tecniche mediante le quali i soggetti che veicolano il prodotto Telemaco (identificati d'ora in avanti col termine intermediari) da una propria applicazione devono operare.

In particolare si descriveranno:

1• le specifiche tecniche per l'interfaccia all'applicazione Telemaco (single sign on e url Telemaco)

2• la personalizzazione grafica delle pagine attraverso la diffusione di un proprio logo

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n° :	2.0	**Data Versione/Release** :	**18/07/2008**
Descrizione modifiche:	aggiunta la definizione dell'url Telemaco e modifiche immagini di Telemaco		
Motivazioni :	Modificato il layout grafico di Telemaco		

1.2 Riferimenti

1• [1] RFC2617 - HTTP Authentication: Basic and Digest Access Authentication
2• [2] RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1

1.3 Termini e definizioni

Proxy - Indica, in questo contesto, un'applicazione che media tra il client e il server InfoCamere, trattando ed eventualmente modificando il flusso di richiesta/risposta.

IC - InfoCamere

intermediario- - termine che indica genericamente il soggetto che accede a Telemaco da una applicazione proprietaria

2 Specifiche tecniche di interfaccia

In questo capitolo vengono descritte le modalità tecniche con le quali un intermediario può consentire ai propri utenti di accedere all'applicazione Telemaco.

Analizzando i clienti finali, cioè chi usufruisce delle informazioni fornite da Telemaco, si distinguono:

1• *Utenti "diretti",* i quali attraverso un link vengono dirottati alla home page di Telemaco e a cui è richiesta l'autenticazione su questo sistema. L'intermediario in questo caso veicola i propri clienti senza alcun intervento.

2• *Utenti "indiretti"*, ai quali è concesso di accedere a Telemaco direttamente dall'applicazione dell'intermediario senza la necessità di presentare nuovamente le proprie credenziali. L'intermediario in questo caso deve curare che la fase di autenticazione al sistema Telemaco a partire dalla propria applicazione venga realizzata in modo automatico.

2.1 Utenti diretti

A questa categoria appartengono gli utenti che direttamente si collegano al sito InfoCamere di Telemaco tramite URL.

2.1.1 URL Telemaco

Si definisce URL di Telemaco, alla data di pubblicazione del documento: https://telemaco.infocamere.it per chi si collega in Internet, https://telemaco.intra.infocamere.it per chi si collega in Extranet.

L'eventuale modifica di questo url sarà comunicata all'intermediario nei tempi concordati dal contratto.

L'url Telemaco deve essere usato solo in fase di login a Telemaco stesso, infatti la navigazione all'interno di Telemaco può portare l'utente su url differenti (per esempio la funzione di ricerca sui registri europei (EBR) reindirizza l'utente all'url specifico di EBR, ovvero ebr.infocamere.it).

2.1.2 Funzionamento

Richiamando l' URL dell'applicazione protetta apparirà una maschera che richiede l'inserimento della coppia user/password e trasmette le credenziali al server.

Questa fase si svolge solo all'apertura della sessione di lavoro: da lì in avanti l'autenticazione è garantita in modo sicuro.

Il funzionamento si basa sull'utilizzo di un cookie di sessione (per approfondimenti vedi l'appendice A sui requisiti del browser).

2.1.3 Funzionalità

Più utenti con stessa user/password possono presentarsi e autenticarsi contemporaneamente (multisessione).

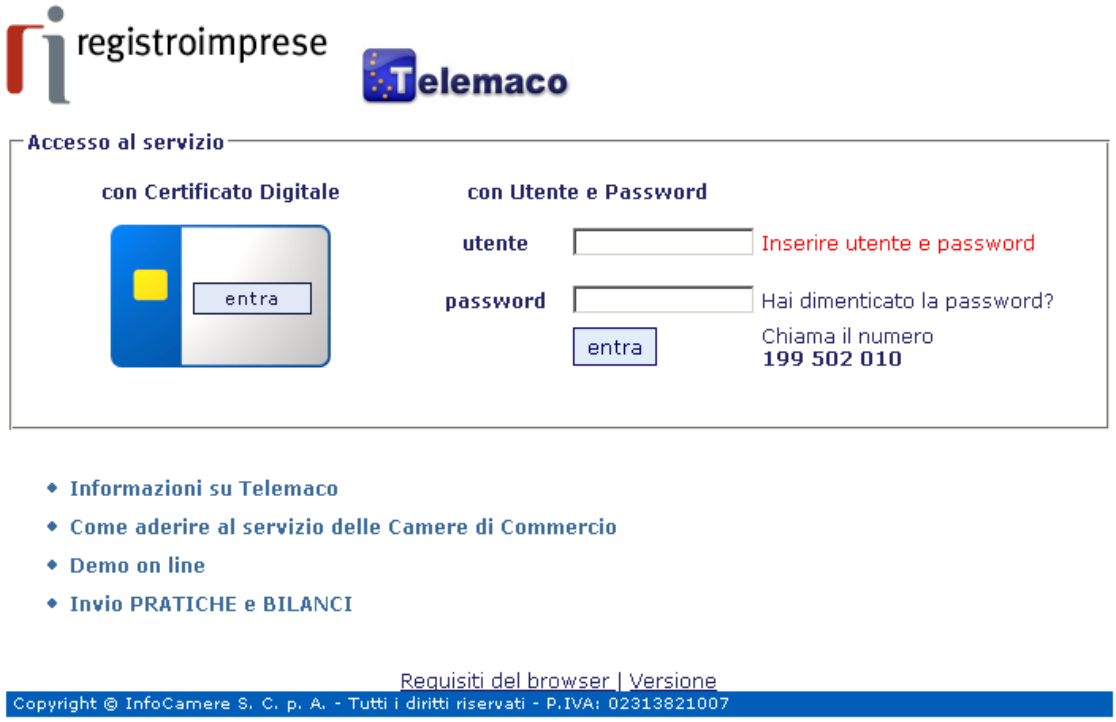
Viene controllato anche il numero massimo di sessioni contemporanee per user permesse.

Nella fase di autenticazione viene verificato il numero massimo di collegamenti per cliente. Nel caso si sia oltrepassata questa soglia non viene permessa l'ultima autenticazione e quindi la fruizione del servizio richiesto.

Allo scollegamento (logout), all'utente compare una maschera che notifica l'evento.

2.1.4 Layout maschere di login e errori dell'autenticazione

Il framework s'incarica di visualizzare la maschera di login.



Gli eventuali messaggi di errore o di informazione (appendice C) vengono visualizzati nella maschera di login nel riquadro della user/password.

2.2 Utenti indiretti

Gli utenti indiretti hanno la caratteristica di presentarsi al server di IC fornendo le credenziali (user e password) in modalità automatica in quanto gli utenti si sono già autenticati all'intermediario che funge da proxy (single sign on).

2.2.1 Funzionamento

Il proxy si collega al server IC effettuando il login (l'utente è già stato autenticato dal proxy stesso) nella modalità cosiddetta automatica, cioè fornendo già da subito user e password senza aspettare che il server IC gli invii la maschera di login.

Per fornire la coppia user/password si consiglia vivamente l'uso del metodo http POST [2] , in quanto il metodo alternativo GET è molto meno sicuro.

Per maggiore chiarezza vengono riportati in appendice B gli estratti di codice.

I messaggi d'errore sono in appendice C.

2.2.2 Funzionalità

Più utenti con stessa user/password possono presentarsi e autenticarsi contemporaneamente (multisessione). Viene controllato anche il numero massimo di sessioni contemporanee per user permesse.

Nella fase di autenticazione viene verificato il numero massimo di collegamenti per cliente. Nel caso si sia oltrepassato questo massimo, non viene permessa l'ultima autenticazione e quindi la fruizione del servizio richiesto.

3 Specifiche per il Cobranding

E' prevista la possibilità di far apparire il logo del marchio nelle pagine di Telemaco.

La struttura di Telemaco si compone di due frame disposte in verticale sul modello top - body.

La frame superiore (top) contiene in alto a sinistra il logo del prodotto, in alto a destra la user dell'utente collegato e sotto a destra è previsto lo spazio per il logo dell'intermediario, come riprodotto a titolo di esempio nella figura che segue.

Sempre nella top frame, nella parte inferiore, ci sono i menù di primo e di secondo livello. La top frame rimane sempre visibile in tutta la navigazione dalla fase di post-login a quella di logout.

Naturalmente nella fase di login apparirà solo il marchio del prodotto Telemaco, in quanto l'utente si deve ancora autenticare.

La frame inferiore (body) conterrà le pagine delle richieste, gli output di tipo lista e le applicazioni collegate a Telemaco (EBR, Elenchi, …).

3.1 Vincoli e caratteristiche tecniche

Le caratteristiche del logo devono rispettare le seguenti specifiche: immagine tipo .jpg/jpeg o .gif di dimensioni max (in byte) 10KB, di dimensioni max in pixel (w*h = 177 * 40).

Lo sfondo in ogni caso è di colore uniforme bianco.

Il logo dell'intermediario deve essere depositato presso Infocamere.

L'eventuale aggiornamento del logo dovrà essere richiesto attraverso il canale di posta elettronica al servizio di Assistenza Infocamere allegando l'immagine da pubblicare.

La pubblicazione del logo, previa verifica dei parametri tecnici e dell'opportunità della pubblicazione, sarà a cura di Infocamere che provvederà a pubblicare l'immagine entro tre giorni lavorativi dalla ricezione del messaggio.

Infocamere si riserva di comunicare al cliente l'eventuale motivazione al rifiuto di pubblicazione negli stessi termini.

4 Appendice

4.1 Appendice A – Requisiti minimi per accesso da Browser

4.1.1 Browser da utilizzare

Per accedere a **Telemaco** si raccomanda di installare un browser con le seguenti caratteristiche:
·MS Internet Explorer 5.0 o superiori oppure Netscape 4.7X o superiori

Per il corretto utilizzo di alcune funzioni, i requisiti del browser cambiano:
·Elenchi Ulisse: MS Internet Explorer 5.5 o superiori, Netscape non è supportato
·Statistiche: MS Internet Explorer 5.5 sp2 o superiori

Modem
Se si utilizza il modem per collegarsi a Telemaco occorre un modem con velocità almeno pari a 56 Kb/s o superiore.

4.1.2 Accettazione cookies e javascript

E' necessario configurare il browser per accettare i cookies e i javascript.
Un cookie è un informazione che un sito web copia, in un'apposita area che il browser installato ha riservato, sul disco rigido del PC collegato.
Di seguito sono riportate le istruzioni che differiscono dal browser utilizzato

Netscape**:**
Dall'Edit menu, scegli Preferences
-Seleziona la categoria Advanced
-Seleziona uno dei radio button. "Accept all cookies" è la scelta migliore.
-Seleziona il checkbox "Enable JavaScript" .

Internet Explorer 5.0**:**
Dal Tool menu, scegli internet Options
Seleziona la categoria Security
Seleziona il botton Custom Level
Assicurati che nei Settings Compaia Cookies Allow cookies that are stored in your computer Enable
Abilita l'esecuzione dei javascript

Internet Explorer 6.0 e 7.0
Abilitare l'esecuzione degli script:
Da Strumenti scegli Opzioni internet…
Seleziona la cartella Protezione
Seleziona il bottone Livello personalizzato
Assicurati che nelle impostazioni alla voce **Esecuzione script** l'impostazione **Esecuzione script attivo** sia impostato ad ATTIVA

Mozilla Firefox 1.5
Abilitare i cookie:
Dal menu Strumenti, scegli Opzioni
Seleziona la categoria Privacy

Seleziona Cookie
Assicurati che sia abilitata la voce "Permetti ai siti di impostare i cookie"**Abilitare l'esecuzione degli script:**
Dal menu Strumenti, scegli Opzioni
Seleziona la categoria Contenuti
Assicurati che la voce "Abilita JavaScript" sia abilitata

4.1.3 Extranet

Per collegamenti EXTRANET il network administrator del cliente collegato in Extranet dovrà inserire nel proprio DNS l'indirizzo IP comunicato da InfoCamere.

4.2 Appendice B – Autenticazione automatica

Questo meccanismo permette di accedere, identificandosi e autenticandosi, direttamente all'applicazione senza aspettare la maschera di login proposta dal framework di sicurezza ASIA.

Vi sono due modalità con cui questo può essere realizzato:

Chiamata in "GET":

in questo caso user e password sono scritte sull'URL di chiamata.

Ad esempio:

https://telemaco.infocamere.it?user=xxx&pass=yyy

(Per chi si collega in Extranet, l'URL dovrà essere https://telemaco.intra.infocamere.it)

Chiamata in "POST"

Questo tipo ha il vantaggio, rispetto al precedente, di rendere meno visibile la user e la password. Rimangono presenti nella sorgente della pagina html, ma non vengono viste visualizzate dal browser nemmeno nel pannello dello status.

Per la costruzione del link è necessaria costruire un form con questi elementi:

```
<FORM NAME=nome_form ACTION=" https://telemaco.infocamere.it" METHOD=POST>
<INPUT TYPE=HIDDEN NAME="user" VALUE = "xxx">
<INPUT TYPE=HIDDEN NAME="pass" VALUE = "yyy">
<INPUT TYPE="submit" name="invia" value="invia" >
</FORM>
```

(Per chi si collega in Extranet, l'URL dovrà essere https://telemaco.intra.infocamere.it)

Alcune raccomandazioni:

1• Le parole "user" e "pass" devono essere scritte minuscole e devono sempre essere presenti (nella chiamata in post devono sempre comparire i due campi hidden).

2• La user può essere scritta indifferentemente maiuscola o minuscola.

3• La password deve avere maiuscole e minuscole al posto giusto.

4.3 Appendice C – Messaggi

La procedura di autenticazione durante il funzionamento ritorna alcuni messaggi in una pagina html con le stesse modalità dell'accesso indiretto.

Eccone l'elenco e il significato:

Messaggio	Codice	Significato
Userid e password corrette. Controllo abilitazioni...		messaggio che appare nel corso della procedura di autenticazione, se la userid e la password digitate sono corrette
Sessione Chiusa		messaggio che appare quando l'utente dà il logout
Identificazione utente non riuscita		messaggio che appare a seguito della digitazione di una userid inesistente o password errata
Parametro password non valorizzato		messaggio che appare se non si digita la password
Numero massimo di connessioni consentite ecceduto		la connessione che si tenta eccede il numero max di connessioni consentite per il gruppo di cui l'utente fa parte
Errore nella procedura di autenticazione. Ripetere la procedura di accesso		problemi interni al lato servlet del framework di sicurezza
Errore inaspettato		problemi interni al lato servlet del framework di sicurezza
Parametro userid non valorizzato		messaggio che appare se l'utente tenta di autenticarsi senza aver digitato una userid