

MUT_AccessoSistema.doc

Manuale Utente

Ministero della Difesa: Protocollo Informatico @D[h]OC

Nome documento: **Manuale Utente “Accesso al Sistema”**

Informazioni sul documento

Titolo documento	Manuale Utente per l'Accesso al Sistema di Protocollo		
Responsabile		Versione Documento	1.0
Preparato da		In vigore dal	
Nome file	MUT_AccessoSistema		
Documentazione di riferimento			

Versioni

Ver. No.	Data	Rivisto da	Descrizione documento
1.0	15/02/2016		Prima stesura

Sommario

1. DEFINIZIONI ED ACRONIMI	3
2. SCOPO DEL DOCUMENTO.....	3
3. OVERVIEW DEL SISTEMA.....	3
4. RUOLI E ACCESSO	3
4.1. CLASSI DI UTENZA.....	3
5. UTILIZZO DEL SISTEMA	3
5.1. PRECONDIZIONI	3
5.2. MODALITÀ OPERATIVE LOGIN.....	3
5.2.1. CASO 1 - ACCESSO AL SISTEMA CON CMD	4
5.2.2. CASO 2 - ACCESSO AL SISTEMA SENZA CMD.....	5
5.2.3. CASO 3 - ACCESSO AL SISTEMA CON CMD NON ASSOCIATA AD ANAGRAFICA UTENTE	7
5.3. CRUSCOTTO	7
5.4. MODALITÀ OPERATIVE DEL CRUSCOTTO	9

1. Definizioni ed Acronimi

2. Scopo del documento

Questo documento intende descrivere le modalità operative che l'utente deve seguire per accedere al sistema di Protocollo Informatico. Inoltre viene presentata la pagina principale, il "Cruscotto", da cui si accede alle diverse sezioni.

3. Overview del Sistema

Attualmente l'utente abilitato al sistema @D[h]OC accede alle funzioni del protocollo informatico, collegandosi al sistema e inserendo le proprie credenziali di accesso, Ruolo e Password.

4. Ruoli e accesso

4.1. Classi di utenza

Gli attori che avranno accesso a queste nuove funzionalità sono:

- Amministratore del sistema.
- Tutti gli utenti dell'AOO abilitati ad accedere al Sistema di Gestione Documentale e Protocollo Informatico @D[h]OC.

5. Utilizzo del sistema

5.1. Precondizioni

Il sistema di protocollo @D[h]OC è una web-application e per la corretta visualizzazione e navigazione delle pagine dell'applicazione il browser di riferimento è Internet Explorer 10 e 11.

Allo scopo di aumentare la sicurezza complessiva dell'infrastruttura informatica del Ministero della Difesa, l'accesso al sistema @D[h]OC potrà avvenire esclusivamente attraverso l'impiego della Carta Multiservizi Difesa, se non diversamente autorizzato. Quindi tutti gli utenti abilitati a utilizzare il sistema dovranno essere muniti di una valida CMD e sulla postazione andrà installata l'ultima versione del software di gestione della CMD e di firma digitale.

Esiste comunque la possibilità di accedere tramite "user-id" e "password", ma solo previa autorizzazione del Responsabile del Servizio (RDS), come descritto in seguito nel paragrafo "5.2.2".

5.2. Modalità operative Login

Per l'accesso al sistema @D[h]OC, l'utente dovrà:

MUT_AccessoSistema.doc

1. Collegarsi al sistema @D[h]OC: apparirà la pagina di login;
2. Inserire la propria CMD all'interno del lettore di Smart Card collegato al computer;
3. Immettere nell'apposito campo il proprio pin carta;
4. Selezionare il pulsante ACCEDI.



Figura 1 - Maschera di autenticazione tramite Smart-Logon.

Dopo che l'utente avrà inserito il PIN di carta, il sistema confronterà le informazioni estratte dalla carta CMD con l'anagrafica del sistema @D[h]OC per autorizzare l'ingresso al Protocollo.

Possono verificarsi i casi di seguito illustrati:

5.2.1. Caso 1 - Accesso al Sistema con CMD

Al primo accesso il sistema eseguirà i controlli di sicurezza estraendo alcune informazioni della CMD dell'utente in base al tipo di carta utilizzata:

- **Utente provvisto di CMD1:** sulla stringa CN di carta si estracono le informazioni cognome e nome, e si decodifica la data di nascita dal codice fiscale
- **Utente provvisto di CMD2:** dal certificato di autenticazione si estracono le informazioni relative a cognome (*surname*), nome (*given name*) e si decodifica la data di nascita dal codice fiscale estratto dal campo CN di carta.

Se le informazioni sono coerenti e l'utenza è presente e abilitata sull'anagrafica del Sistema di Protocollo @D[h]OC, questa viene associata all'anagrafica per l'accesso al sistema.

Nel caso in cui si riscontrasse un'omonimia (cognome, nome e data di nascita identici), sarà necessario informare lo staff tecnico di supporto al sistema.

Se l'utenza effettua l'accesso al sistema ed il sistema rileva una connessione attiva verrà richiesto all'utente conferma dello sblocco della sessione.

Nei successivi accessi, se l'utente avesse cambiato la propria CMD, il sistema rileverà questa difformità ed eseguirà nuovamente i controlli di sicurezza descritti sopra.

MUT_AccessoSistema.doc

Nota: Queste informazioni saranno valide solo per le carte generate dal CSIE (Centro Sistemi Informatici dell'Esercito). Per le carte di fornitori terze parte (esempio: carta dei Carabinieri) l'accesso al sistema sarà consentito utilizzando la funzionalità **Associa CMD** descritta di seguito nel CASO 3.

5.2.2. Caso 2 - Accesso al Sistema senza CMD

Se un utente è sprovvisto di CMD ma, per un qualsiasi motivo, ha necessità di accedere al sistema il Responsabile del Servizio (RDS) potrà, per un limitato periodo di tempo, impostare una deroga alla modalità di accesso con CMD, ed in tal caso l'utente potrà accedere con la vecchia metodologia (ruolo e password).

Per impostare tale deroga l'RDS accedendo alla scheda anagrafica dell'utente interessato dovrà togliere la spunta di selezione dalla voce "Smart Logon". In questo modo, l'accesso con CMD sarà disabilitato e nel campo "Fino al" sarà inserita la data di termine dell'intervallo in cui sarà possibile accedere con ruolo e password.

La data è impostata dal sistema e avrà una durata di sette giorni dalla data di attivazione di tale funzionalità.

Trascorso tale periodo, la deroga si disabiliterà automaticamente e potrà essere, nuovamente attivata con le modalità già viste.

Se, viceversa, l'utente per il quale era stata attivata una deroga entra in possesso della propria CMD prima della scadenza temporale della deroga stessa, sarà possibile, sempre da parte dell'RDS disattivare immediatamente la deroga in modo da consentire l'accesso tramite CMD.

Modifica Anagrafica	
CHIUDI » PULISCI » DISABILITA » ELIMINA » STAMPA » SALVA » ASSOCIA RUOLO »	
• Grado/Qualifica *	t.i.
• Cognome *	TEST
• Nome *	password
• Data di nascita *	11-11-1966
• Luogo di nascita *	Roma
• Codice Fiscale	
• Email 1	
• Email 2	
• Telefono	
• Password *	••••••••
• Conferma Password *	••••••••
• Webservice:	☐
• Smart Logon:	☒
Ruolo	Elimina
 form_testpwd2	

Modifica Anagrafica	
CHIUDI »	PULISCI »
DISABILITA »	ELIMINA »
STAMPA »	SALVA »
ASSOCIA RUOLO »	
Grado/Qualifica *	t.i.
Cognome *	TEST
Nome *	password
Data di nascita *	11-11-1966
Luogo di nascita *	Roma
Codice Fiscale	
Email 1	
Email 2	
Telefono	
Password *	*****
Conferma Password *	*****
WebService:	☐
Smart Logon:	☐ Fino al 22-02-2016
ASSOCIA CMD	
Ruolo	Elimina
form_testpwd2	

L'utente abilitato all'accesso al sistema senza CMD, dovrà procedere nel seguente modo:

1. Sulla pagina di login dovrà selezionare il pulsante "Login con Ruolo";
2. Apparirà la pagina di login per l'immissione di Ruolo e Password;
3. Dopo l'inserimento di Ruolo e Password, per confermare le credenziali inserite e accedere al Sistema l'utente dovrà selezionare il pulsante **ACCEDI**.

Pin di Carta:	Inserisci Pin di Carta
Pulisci »	Login con Ruolo»
	Accedi »

@D@C		Protocollo Informatico e Gestione Documentale del Ministero della Difesa.		COLL. PALAZZO ESERCITO	
ULTIMO RILASCIO: 15-12-2015		ULTIMO BOLLETTINO: N. 18 DEL 15-12-2015			
Ruolo: Inserisci ruolo Password: Inserisci password Pulisci » Login con CMD» Accedi »					

Figura 2 – Maschera di autenticazione tramite Login.

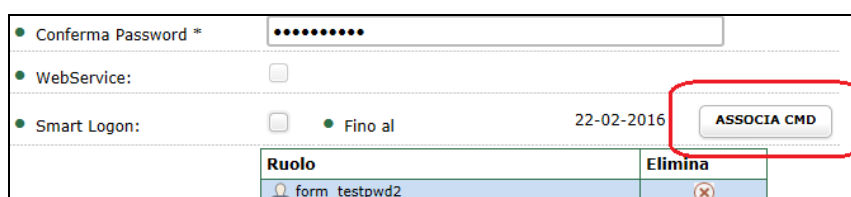
5.2.3. Caso 3 - Accesso al Sistema con CMD non Associata ad Anagrafica utente

Se l'utente è provvisto della carta Multiservizi valida ma non riesce ad accedere al sistema perché non vi è corrispondenza delle informazioni estratte dalla carta CMD con l'anagrafica di @D[h]OC (ad esempio carta non generata dal CSIE), potrà richiedere all'RDS della propria AOO di associare temporaneamente la carta CMD alla propria anagrafica.

L'RDS accedendo alla scheda anagrafica dell'utente interessato vedrà il pulsante **Associa CMD** che gli consentirà di associare la carta all'anagrafica.

I passi che l'RDS dovrà effettuare per l'associazione sono i seguenti:

1. Inserire la CMD dell'utente all'interno del lettore di Smart Card collegato al computer;
2. Selezionare il pulsante **Associa CMD** presente sulla maschera anagrafica dell'utente da associare;
3. Immettere nell'apposito campo, dell'applet che viene avviata, il pin di carta.



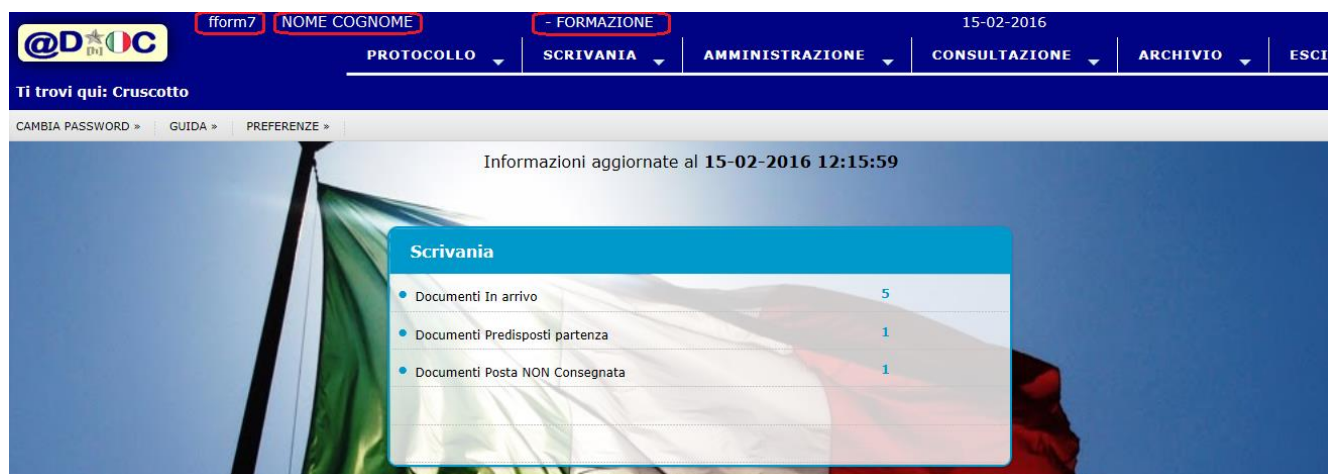
The screenshot shows a user profile page with the following fields: 'Conferma Password *' (password field), 'WebService:' (checkbox), 'Smart Login:' (checkbox), and 'Fino al' (date field set to 22-02-2016). Below these is a table with columns 'Ruolo' and 'Elimina'. The 'Ruolo' column contains 'form_testpwd2'. The 'Elimina' column contains a red 'X' icon. The 'Associa CMD' button is highlighted with a red box.

Il sistema controllerà che la carta CMD non sia già associata ad altro utente altrimenti verrà bloccata la procedura. Superato tale controllo, la carta CMD risulterà associata all'anagrafica dell'utente il quale potrà accedere al sistema come descritto nel CASO 1.

5.3. Cruscotto

A seguito della validazione delle credenziali di accesso, il sistema propone all'utente la pagina principale da cui l'utente accede alle varie funzionalità configurate dall'amministratore locale di UO.

Possiamo distinguere due aree, un "Menù di testata" (da ora "Toolbar") nella parte superiore della pagina e un'area principale nella parte inferiore. La parte superiore è comune per tutte le sezioni (Protocollo, Scrivania, Amministrazione, Consultazione, Archivio, Esci) e contiene le informazioni relative al ruolo utente, anagrafica utente e ufficio di appartenenza, la data e la sezione in cui ci si trova. Al primo accesso, si entra sempre nella sezione "Cruscotto".



The screenshot shows the main dashboard (Cruscotto) with the following elements: a top navigation bar with the @D[h]OC logo, user information (fform7, NOME COGNOME, - FORMAZIONE), and the date 15-02-2016; a secondary navigation bar with tabs for PROTOCOLLO, SCRIVANIA, AMMINISTRAZIONE, CONSULTAZIONE, ARCHIVIO, and ESCI; a message 'Ti trovi qui: Cruscotto'; a section 'Cambia Password > Guida > Preferenze >'; a date and time stamp 'Informazioni aggiornate al 15-02-2016 12:15:59'; and a 'Scrivania' (Desk) section with a table of document statistics:

Scrivania	
Documenti In arrivo	5
Documenti Predisposti partenza	1
Documenti Posta NON Consegnata	1

Figura 3 – Pagina principale.

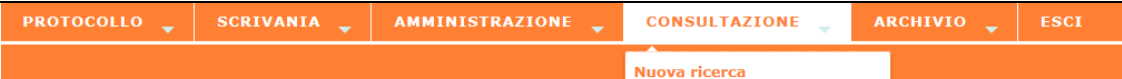
Sulla parte superiore sinistra è sempre presente il percorso in cui ci si trova “Ti trovi qui: *PERCORSO*” e i comandi per l’accesso alle funzioni di modifica della password, apertura della guida e gestione delle preferenze:

- CAMBIA PASSWORD
- GUIDA
- PREFERENZE

Attraverso la toolbar, è possibile accedere alle funzionalità dell’applicazione.


Figura 4 – Toolbar.

La toolbar mostrerà un colore diverso secondo la sezione in cui l’utente si trova e sta lavorando e anche le voci di menù a tendina avranno i collegamenti dello stesso colore della toolbar, nello specifico:

Blu: cruscotto	
Rosso: protocollo	
Verde: amministrazione	
Arancione: consultazione	

Viola: Archivio	PROTOCOLLO ▾	SCRIVANIA ▾	AMMINISTRAZIONE ▾	CONSULTAZIONE ▾	ARCHIVIO ▾	ESCI
	Gestione procedimenti					
	Gestione fascicoli					

In ogni momento è possibile tornare nella pagina principale tramite il collegamento “Cruscotto”, posto in alto a sinistra nel testo del percorso “Ti trovi qui: PERCORSO”.

Es. **Ti trovi qui: Cruscotto » In Arrivo**

5.4. Modalità operative del Cruscotto

Sul Cruscotto sono sempre presenti i comandi per l’accesso alle funzioni:

Ti trovi qui: Cruscotto		
CAMBIA PASSWORD »	GUIDA »	PREFERENZE »

- CAMBIA PASSWORD
- GUIDA
- PREFERENZE

CAMBIA PASSWORD

Tramite questo comando è possibile modificare la password di accesso al sistema. Alla selezione, si aprirà una maschera di modifica.

Ruolo:	rdsform
Vecchia Password:	Vecchia password
Nuova Password:	Nuova password
Ripeti Password:	Ripeti password
Pulisci » Modifica »	

Figura 5 –Modifica Password.

GUIDA

Tramite questo comando l’utente potrà consultare e scaricare i manuali utente relativi alle modalità operative di tutte le funzionalità del sistema di Protocollo.

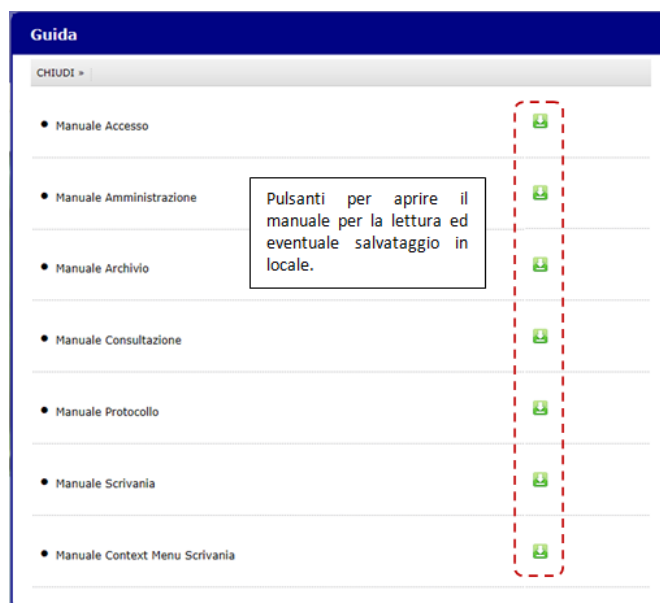


Figura 6 – Finestra “Guida” utente.

PREFERENZE

Tramite questo comando è possibile modificare le preferenze di visualizzazione e di dettaglio delle sezioni “Scrivania” e “Consultazione”. Inoltre si può scegliere il visualizzatore di documenti predefinito, MS Office oppure Libre Office, impostando il percorso corretto del programma sulla macchina locale dell’utente. L’Ordinamento delle Scrivanie è una funzionalità disponibile solo a partire dalla versione 5.1 di @D[h]OC; impostando le preferenze nella suddetta sezione, verrà gestito l’ordine di presentazione dei documenti sulle scrivanie.

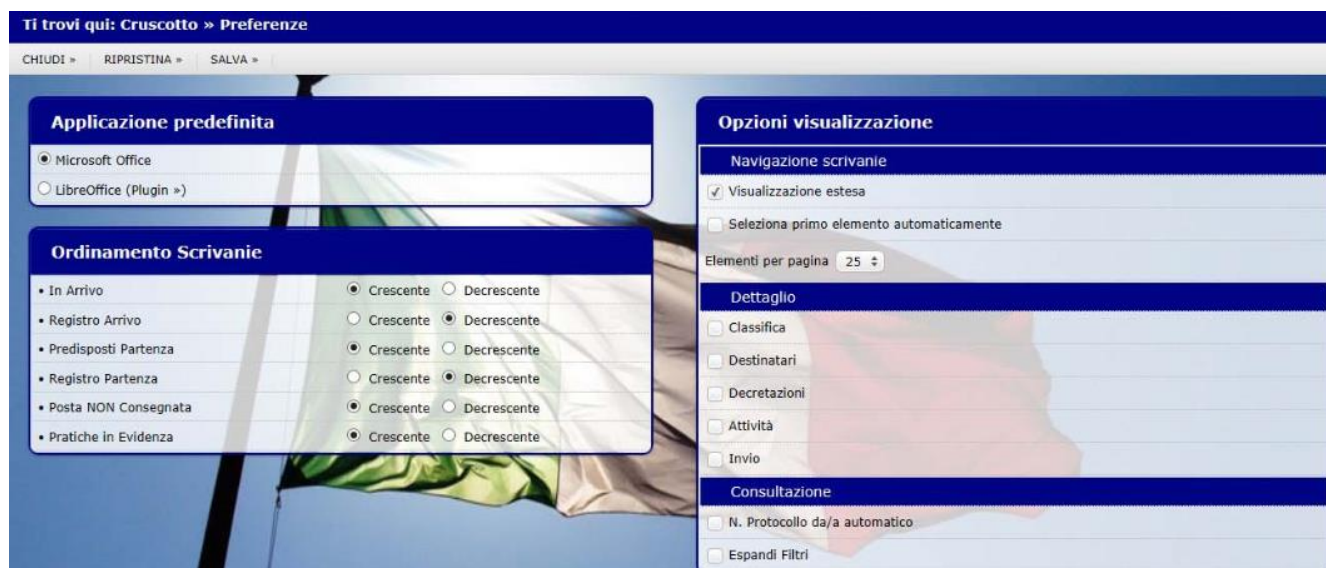
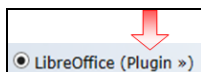


Figura 7 – Preferenze.

Nota bene: Per l'apertura dei documenti di protocollo con LibreOffice ogni utente, collegandosi al sistema di protocollo, deve scaricare e installare sulla postazione locale il software utilizzando il pulsante Plug-in >>



Alla selezione del pulsante viene visualizzato un messaggio dal sistema per l'apertura o il salvataggio del Plug-in.

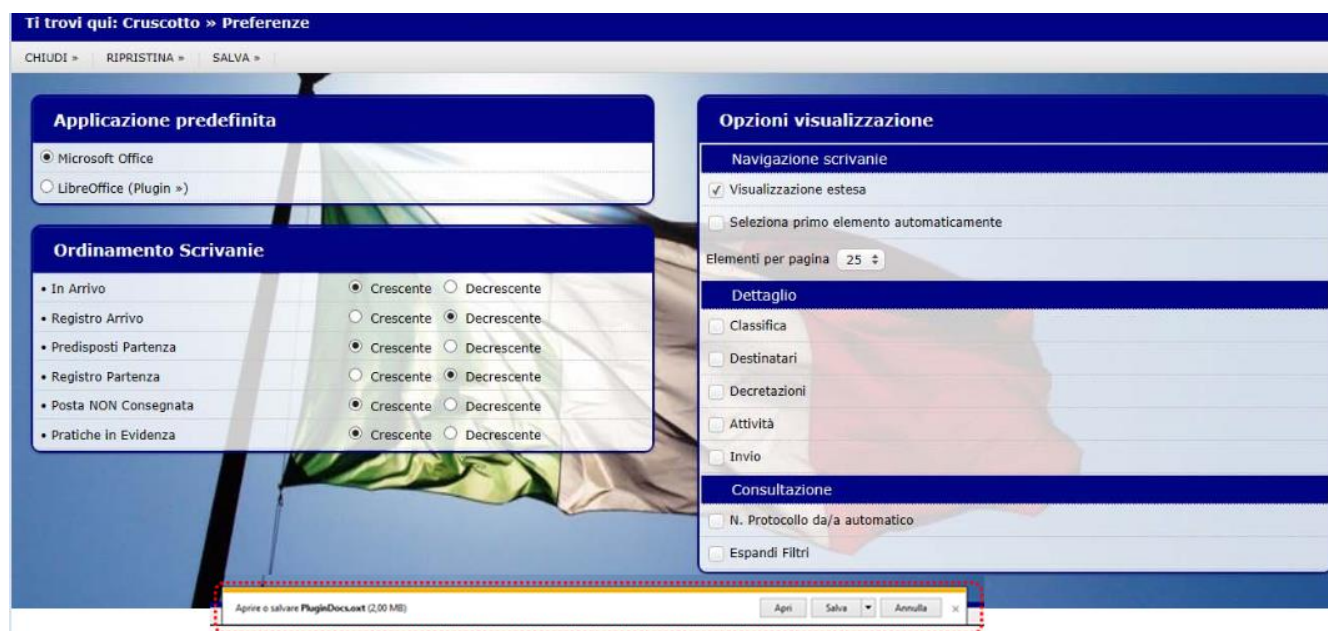


Figura 8 – Installazione Plug-in LibreOffice.

Alla selezione del bottone **Apri** il sistema avvia l'applicazione LibreOffice e richiede la conferma d'installazione del "PluginDocs.otx".

MUT_AccessoSistema.doc

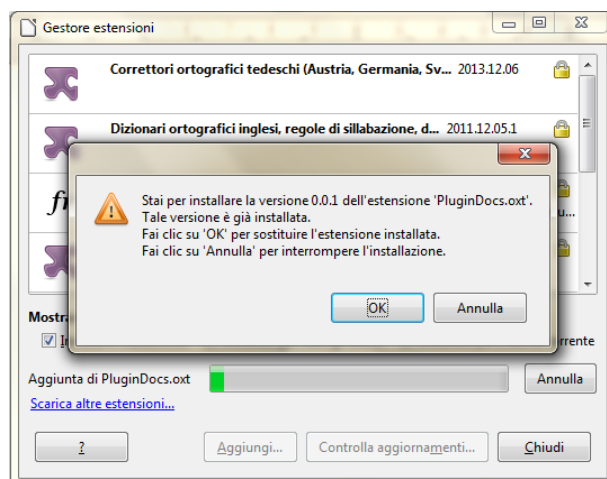
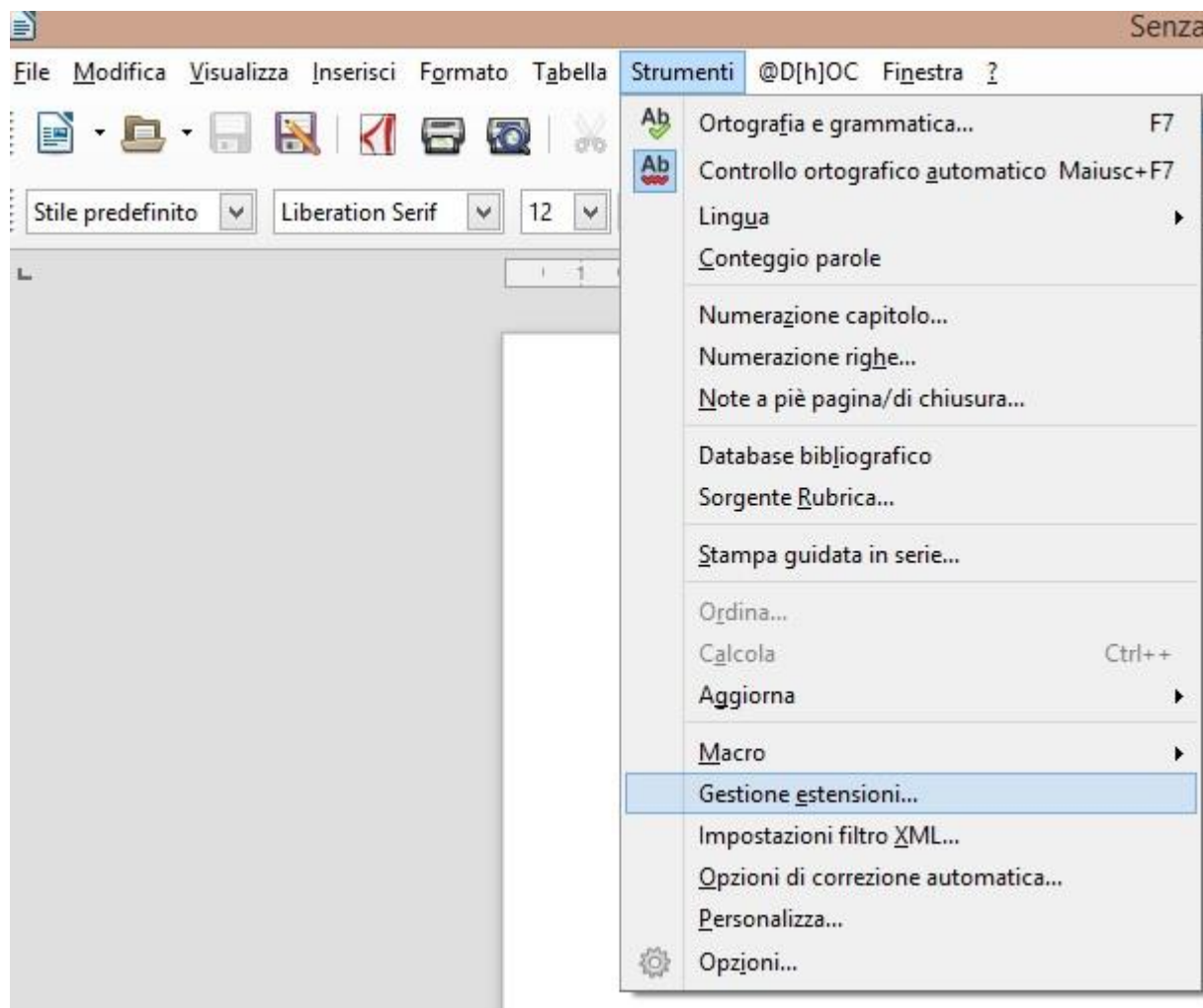


Figura 9 – Maschere d’installazione del plug-in di LibreOffice.

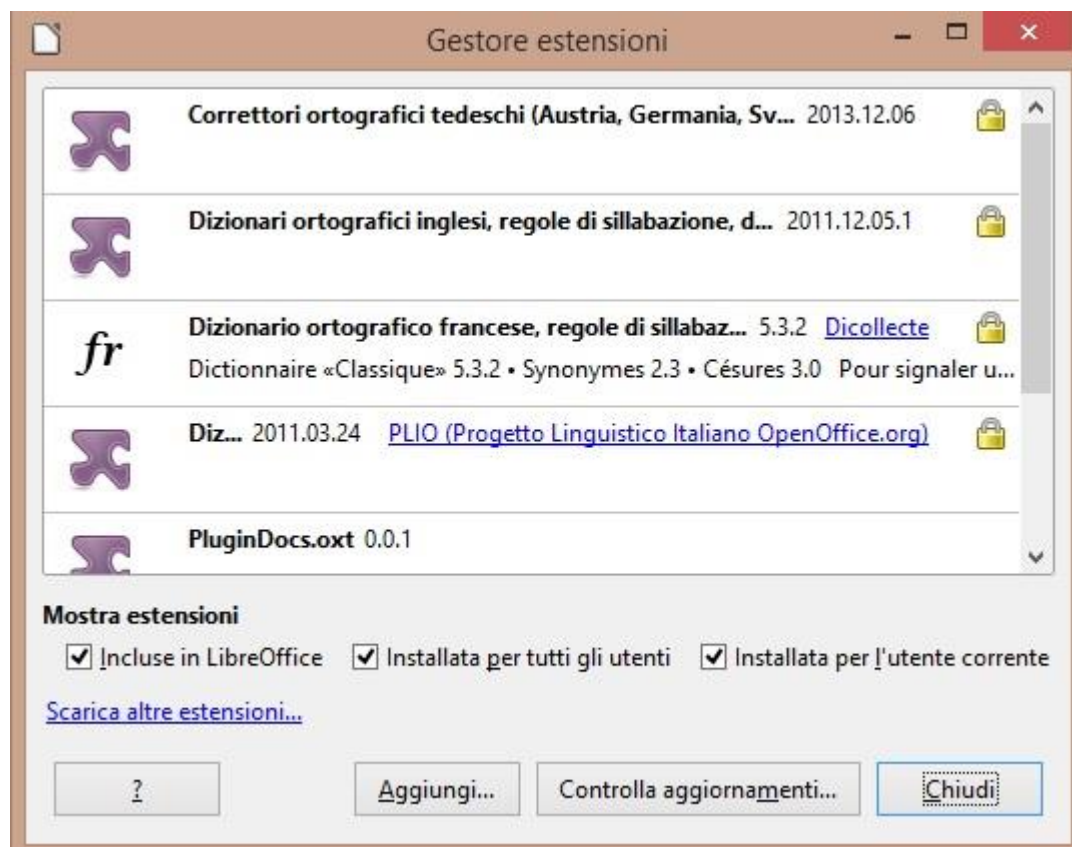
Alla conferma, il sistema avvia l’installazione del Plug-in. Al termine dell’operazione, l’utente potrà chiudere l’applicazione e ritornare alla sessione attiva del browser sul sistema di Protocollo.

Per verificare il corretto caricamento del plug-in, l’utente dovrà avviare “Libre Office Writer” e, tramite Menù → Strumenti → Gestione estensioni, constatare che nell’elenco dei plug-in sia presente “PluginDocs.otx”.

MUT_AccessoSistema.doc



MUT_AccessoSistema.doc



Per rendere effettive le Preferenze selezionate, occorre salvare tramite comando “Salva”.