



Autenticazione sicura al sito www.unibs.it

*Guida per l'utente
20120926*

Introduzione	2
Installazione manuale del certificato CA	3

Introduzione

Al fine di garantire maggior sicurezza circa l'autenticazione degli utenti del Portale di Ateneo è stato allestito un meccanismo di Login basato sull'utilizzo di certificati, che hanno lo scopo di aumentare la riservatezza delle comunicazioni durante l'utilizzo della procedura di riconoscimento.

I certificati consentono di crittografare la comunicazione tra il browser web utilizzato dal navigatore, e il server, che dispone dei mezzi per decrittare e utilizzare le informazioni ricevute.

La differenza principale, riscontrabile a prima vista da parte dell'utente, tra una comunicazione standard e una crittografata è evidente dall'utilizzo nell'URL del sito stesso, del protocollo "https", in sostituzione al più classico "http".

I browsers web, come Internet Explorer, o Mozilla Firefox verificano il certificato ricevuto dal server in base a una serie di criteri di correttezza, e se uno di questi viene violato, visualizzano, al tentativo di accesso al sito protetto da certificato, un messaggio di errore che scoraggia l'utilizzatore dal continuare la navigazione.

Uno dei suddetti criteri, applicato dai diversi browsers, è quello che cerca di identificare l'ente emittente del certificato, per verificare se questo è un ente presente in una lista predefinita di enti rilascianti o meno.

Gli enti facenti parte di questa lista, riconosciuta a livello mondiale, si chiamano CA (Certification Authorities), e oltre al compito di generare certificati, mantengono un registro di certificati attivi, e hanno la possibilità di verificare in qualsiasi momento se il certificato in uso appartiene al server che lo sta usando.

Nel caso dell'Università degli Studi di Brescia l'emissione del certificato server per l'autenticazione sicura, in adesione al Terena Certificate Service del GARR, è stata effettuata da Comodo CA, che è una certification authority riconosciuta dalla maggior parte dei browsers web disponibili: Internet Explorer e Mozilla Firefox per esempio, riconoscono nativamente la CA in questione come affidabile.

Installazione manuale del certificato CA

Come detto poco sopra, la CA è reputata attendibile dalla maggior parte dei browser, ma nel caso non lo fosse per un particolare browser, o nel caso di rimozione accidentale della certification authority dal database dei certificati fonti attendibili del browser in uso, e appaia quindi un messaggio simile a questo



Connessione sicura fallita

login.amm.unibs.it utilizza un certificato di sicurezza non valido.

Il certificato non è affidabile in quanto il certificato dell'autorità emittente non è affidabile.

(Codice di errore: sec_error_untrusted_issuer)

- Potrebbe trattarsi di un problema nella configurazione del server oppure di un tentativo da parte di qualcuno di sostituirsi al server stesso.
- Se è stato possibile connettersi a questo server in passato, il problema potrebbe essere solo temporaneo. Si consiglia di riprovare più tardi.

[Oppure è possibile aggiungere un'eccezione](#)

è comunque possibile procedere all'installazione manuale del certificato CA tramite il link sottostante

certificato CA

N.B. Nell'esempio il browser utilizzato è Mozilla Firefox.

Dopo aver selezionato il link appare una finestra simile a questa, in cui va selezionata l'opzione "*Dai fiducia a questa CA per l'identificazione dei siti web*", e successivamente cliccare il bottone Ok come conferma.

