



Linee guida per l'attivazione della crittografia end-to-end su Teams

Questo documento fornisce alcune linee guida per l'attivazione della crittografia end-to-end (E2EE) per le chiamate uno-a-uno su Microsoft Teams.

L'obiettivo è di fornire istruzioni sulla configurazione di questa misura di sicurezza, al fine di proteggere le informazioni di chiamata e renderle decifrabili esclusivamente ai due soggetti direttamente coinvolti nella comunicazione.

L'attivazione della crittografia end-to-end (E2EE) è fortemente raccomandata per tutte quelle conversazioni che richiedono un grado di riservatezza particolarmente elevato da effettuarsi almeno prima dell'avvio della conversazione. Diversamente, saranno mantenute le impostazioni di cifratura di default.

Crittografia end-to-end (E2EE)

Per impostazione predefinita, Teams crittografa già tutte le comunicazioni usando tecnologie standard, ad esempio Transport Layer Security (TLS) e Secure Real-Time Transport Protocol (SRTP).

Inoltre, per tutti gli utenti dell'Ateneo è possibile attivare anche la cifratura di tipo E2EE per aumentare ulteriormente la riservatezza delle chiamate uno-a-uno.

La crittografia end-to-end, o E2EE, consiste nel crittografare il canale della comunicazione prima che si instauri la comunicazione, e solo il destinatario può decifrare il contenuto. Con la crittografia end-to-end, quindi, solo i due sistemi endpoint sono coinvolti nella crittografia e decrittografia dei dati della chiamata. Nessun'altra parte, incluso Microsoft, ha conseguentemente accesso alla conversazione.

La funzionalità E2EE può sempre rimanere attiva, evitando quindi di provvedere alla sua abilitazione ogni qualvolta si desidera incrementare la riservatezza delle chiamate. Tuttavia, anche qualora rimanga attiva in background, risulterà effettiva solo nel momento in cui entrambi gli utenti coinvolti nella chiamata abbiano preventivamente attivato tale funzionalità e che non vi siano più di due partecipanti, in quanto la crittografia E2EE al momento è disponibile solo per conversazioni 1-1.

Si precisa che, qualora la crittografia E2EE sia in funzione del corso di una chiamata 1-1 per entrambi gli utenti, non risulterà possibile effettuare registrazioni della conversazione (per ulteriori dettagli si rimanda al paragrafo *Funzionalità dell'E2EE*).¹

Collegarsi a Microsoft Teams

Al fine di impostare la crittografia end-to-end, entrambi i soggetti coinvolti devono accedere a Microsoft Teams e procedere alla regolare autenticazione tramite le proprie credenziali (v. *Figura 1*).

¹ Qualora non si dovessero presentare le condizioni che rendono effettivo il funzionamento della crittografia E2EE (conversazione 1-1 e funzionalità E2EE abilitata da entrambi gli utenti), anche lasciando l'opzione di E2EE attiva nelle proprie impostazioni di Teams, saranno comunque consentite tutte le funzionalità standard previste dal normale utilizzo di Teams (es. la registrazione delle chiamate non sarà inibita).



Per procedere con il funzionamento della tecnologia è necessario che entrambi gli utenti attivino l'E2EE², come specificato nel paragrafo successivo.

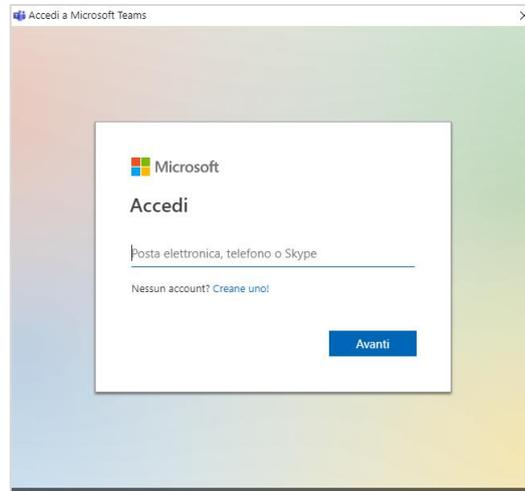


Figura 1 – Accesso a Microsoft Teams

Step di attivazione dell'E2EE

Prima della chiamata, entrambi gli utenti devono:

- selezionare “Altre opzioni” accanto all'icona del profilo  e quindi selezionare “Impostazioni” (v. *Figura 2*);
- selezionare “Privacy” nella barra menu a sinistra e quindi selezionare l'interruttore accanto a “Chiamate crittografate end-to-end” per attivarlo (v. *Figura 3*).

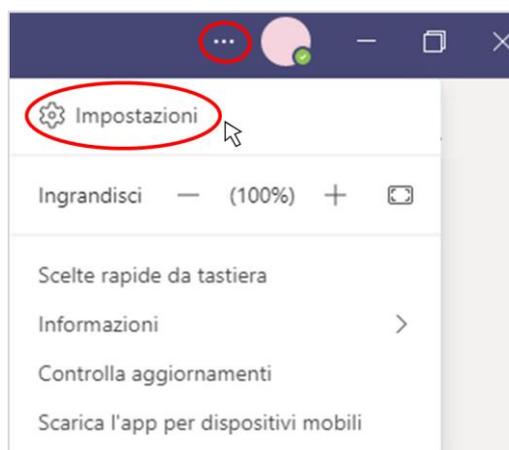


Figura 2 – Selezione Impostazioni

² L'efficacia della cifratura E2EE funziona solo se l'interlocutore ha la medesima funzionalità attivata, diversamente resterà attiva la cifratura standard. Pertanto, al fine di garantire il più alto grado di riservatezza della conversazione sarà opportuno sollecitare l'interlocutore all'attivazione della crittografia E2EE.

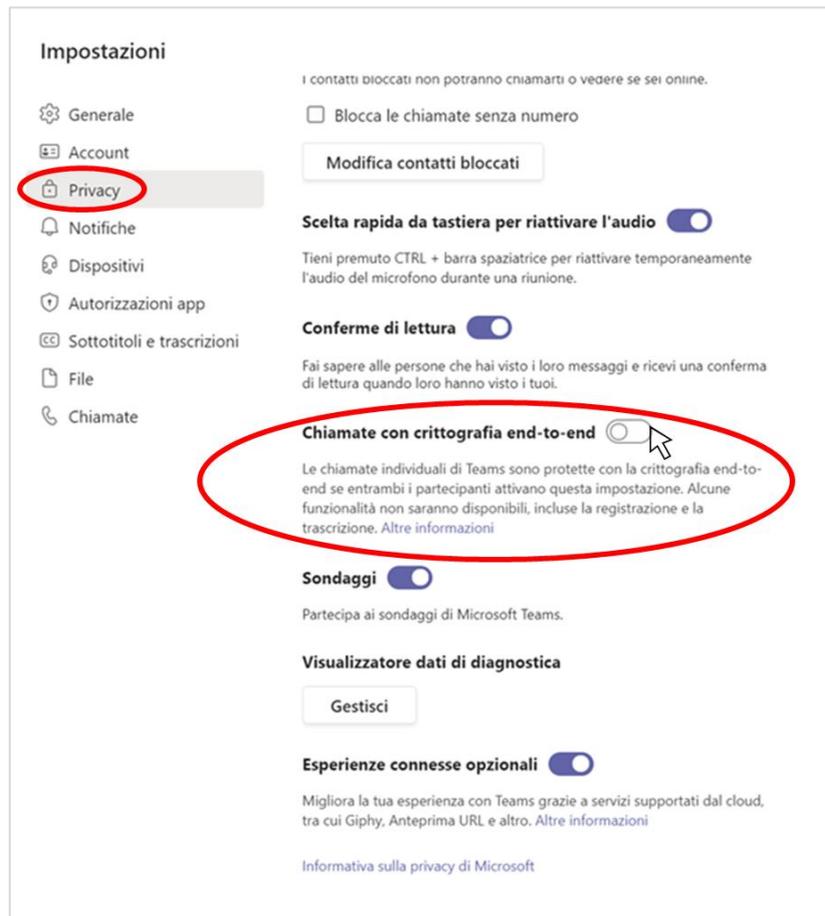


Figura 3 – Selezione per l’attivazione della misura di sicurezza E2EE

Attenzione: nel caso in cui non dovesse comparire l’opzione “Chiamate con crittografia end-to-end”, sarà preventivamente necessario provvedere all’aggiornamento di Microsoft Teams all’ultima versione disponibile:

- selezionare “Altre opzioni” accanto all'icona del profilo  e quindi selezionare “Controlla aggiornamenti” (v. Figura 4).

Cliccando su “Controlla aggiornamenti”, comparirà una barra grigia che confermerà il fatto che Microsoft Teams starà automaticamente provvedendo a verificare l’ultima versione disponibile e ad aggiornare l’applicazione (v. Figura 5).

Una volta aggiornata l’applicazione, seguire i precedenti step di attivazione dell’E2EE.

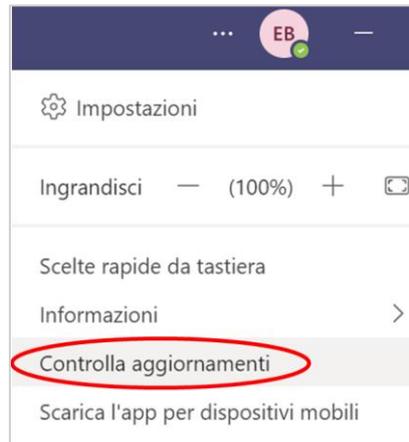


Figura 4 – Aggiornamento di Microsoft Teams



Figura 5 – Richiesta di aggiornamento di Microsoft Teams

Funzionalità dell'E2EE

Nel corso di una chiamata one-to-one, attivazione dell'E2EE garantisce le seguenti funzionalità:

- Audio
- Video
- Condivisione dello schermo

Attualmente l'attivazione della crittografia end-to-end non è disponibile in Microsoft Teams per le chiamate di gruppo ma solo one-to-one.

Alcune funzionalità avanzate, non saranno disponibili durante una chiamata E2EE, tra cui:

- Registrazione audio della chiamata
- Sottotitoli e trascrizioni in tempo reale
- Trasferimento di chiamata
- Unione di chiamate
- *Call Park* che consente di mettere in attesa una chiamata in corso
- Consulta e trasferisci
- Chiamata supplementare e trasferisci a un altro dispositivo
- Aggiunta di un partecipante



Verificare il funzionamento dell'E2EE

Quando la chiamata è connessa, al fine di verificare il corretto funzionamento dell'E2EE, eseguire le seguenti operazioni:

1. Verificare che sia presente uno scudo con un lucchetto  nell'angolo in alto a sinistra della finestra della chiamata (v. *Figura 6*). Questo indica che l'E2EE è attivato per entrambi gli utenti.



Figura 6 – Scudo con lucchetto nel corso della chiamata

Differentemente, se lo scudo non è accompagnato da un lucchetto  significa che l'E2EE non è attivo per almeno uno dei due utenti.

2. Posizionare il mouse sullo scudo con lucchetto per visualizzare il codice di sicurezza e confrontarlo con il codice visualizzato dall'altro utente con cui è in corso la chiamata (v. *Figura 7*).
3. Se entrambi gli utenti della chiamata vedono lo stesso codice, l'E2EE funziona correttamente.

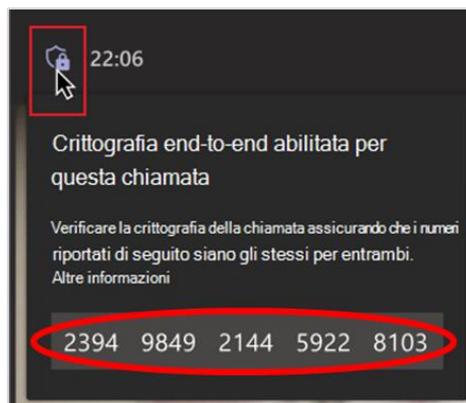


Figura 7 – Codice di sicurezza