Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Centro nazionale per la cibersicurezza NCSC

Versione 2.0 - febbraio 2022

Accordo di utilizzo di «Threema» con persone esterne alla Confederazione

1 Scopo dell'accordo di utilizzo

Il presente accordo disciplina le condizioni di utilizzo per la comunicazione con «Threema» fino ai dati classificati come CONFIDENZIALI (secondo l'OPrI) e ai dati personali degni di particolare protezione (secondo la LPD) tra i collaboratori dell'Amministrazione federale e le persone esterne alla Confederazione (esterni), i cui dispositivi non sono integrati nel sistema Mobile Device Management (MDM) dell'Amministrazione federale.

2 Principi per l'impiego

2.1 Utilizzo di «Threema» e tutela del segreto

Se è necessario scambiare informazioni con dati classificati come CONFIDENZIALI tra i collaboratori dell'Amministrazione federale ed esterni e non sono disponibili altri mezzi di comunicazione autorizzati (Secure Messaging o SecureCenter), «Threema» può essere utilizzato per le conversazioni con chiamate vocali o videochiamate e i messaggi di testo con esterni, nel rispetto del presente accordo di utilizzo. Gli esterni sono tenuti alla tutela del segreto per quanto riguarda le informazioni scambiate tramite «Threema».
Inoltre DEVE sempre essere firmato un accordo di utilizzo se «Threema» viene utilizzato dai membri dell'Amministrazione federale con persone esterne alla Confederazione. Tale accordo si applica anche nel caso in cui i collaboratori dell'Amministrazione federale comunicano con i militari di milizia tramite «Threema».

L'obiettivo dell'accordo di utilizzo è offrire la possibilità alle persone interne alla Confederazione di scambiare informazioni classificate come CONFIDENZIALI con persone esterne alla Confederazione e, di conseguenza, con dispositivi che non sono integrati nel sistema MDM (ad es. fornitori, militari di milizia ecc.).
Non è consentito inviare tramite «Threema» file classificati come CONFIDENZIALI (secondo l'OPrI) e dati personali degni di particolare protezione (secondo la LPD). Per questo motivo, tramite «Threema» sono consentiti solo le conversazioni con o senza video e i messaggi di testo.

L'Esercito non soggiace all'ordinanza sulla trasformazione digitale e l'informatica (OTDI; RS *172.010.58*). Di conseguenza, la comunicazione interna all'Esercito tra i militari di milizia è esclusa da questo accordo di utilizzo. Se necessario, l'Esercito emana direttive proprie per questo caso concreto.

2.2 Aggiornamenti dei sistemi operativi e delle applicazioni

I dispositivi intelligenti degli esterni DEVONO essere aggiornati all'ultima versione del sistema operativo. Le applicazioni non sicure di cui si è a conoscenza DEVONO essere rimosse dal dispositivo interessato. Gli aggiornamenti di «Threema» DEVONO essere installati immediatamente. Se si sospetta un malware, non è consentito utilizzare «Threema». Poiché il malware può annidarsi nella memoria di lavoro, si raccomanda di spegnere completamente e di riavviare prima dell'uso i dispositivi intelligenti di entrambi gli interlocutori (interni ed esterni). In questo modo si rimuove il malware.

2.3 Sicurezza dell'ambiente circostante

Gli esterni DEVONO garantire che le comunicazioni tramite «Threema» avvengano in un ambiente circostante sicuro. Rappresentano rischi potenziali: persone non autorizzate nelle vicinanze, aree pubbliche, camere d'albergo, ascensori ecc.
Per evitare il rischio di essere ascoltati da terzi non autorizzati, le conversazioni riguardanti dati classificati come CONFIDENZIALI (secondo l'OPrl) e dati personali degni di particolare protezione (secondo la LPD) NON POSSONO essere effettuate in pubblico. Ciò vale per i viaggi, in particolare anche per gli edifici dell'aeroporto in Svizzera e all'estero e sui mezzi di trasporto pubblici (ad. es. treni, autobus, tram, aerei ecc.).
Se l’ambiente in cui ci si trova non è sicuro o vi sono dubbi al riguardo, la comunicazione deve avvenire mediante messaggi di testo (chat). A tale proposito si deve fare attenzione che nessuno guardi lo schermo del cellulare o veda le notifiche visualizzate nella schermata di blocco.

2.4 Identificazione dei partecipanti

Gli interlocutori DEVONO potersi identificare reciprocamente. A questo scopo, «Threema» offre diverse possibilità di autenticazione. Fino alla classificazione AD USO INTERNO (secondo l'OPrl) e ai dati personali (secondo la LPD) è richiesto solo l'«ID Threema» dell'interlocutore. Le conversazioni classificate come CONFIDENZIALI DEVONO osservare le seguenti condizioni:

a. gli interlocutori si sono già identificati reciprocamente (visualizzazione di tre punti verdi), ovvero lo scambio dell'«ID Threema» tra i dispositivi è avvenuto tramite scansione reciproca degli ID.

Se, per motivi organizzativi, non fosse possibile attenersi al punto a., DEVONO essere soddisfatti i due punti seguenti:

b. gli interlocutori DEVONO conoscersi personalmente E
gli interlocutori DEVONO identificarsi reciprocamente tramite una videochiamata e una verifica visiva o un segnale di riconoscimento comune.

2.5 Strumenti di assistenza vocale

Gli strumenti di assistenza vocale e di accesso facilitato come «SIRI» o l'«Assistente Google» DEVONO essere spenti prima di usare «Threema». Ciò vale anche per i dispositivi periferici come gli smartwatch. NON È CONSENTITO registrare conversazioni sul dispositivo con «Threema», tutte le funzioni di registrazione devono essere disattivate.

2.6 **Periferiche**

Durante le conversazioni con dati classificati come CONFIDENZIALI (secondo l'OPrl) e dati personali degni di particolare protezione (secondo la LPD) È CONSENTITO utilizzare periferiche esterne come cuffie, tastiera e fotocamera. Tuttavia, questi dispositivi DEVONO essere collegati tramite un cavo. Le notifiche push di «Threema» NON DEVONO essere inviate su periferiche (ad es. su smartwatch). Durante la comunicazione con dati classificati come CONFIDENZIALI (secondo l'OPrl) e dati personali degni di particolare protezione (secondo la LPD), il «Bluetooth» e il «Wi-Fi» DEVONO essere disattivati. I dispositivi intelligenti NON POSSONO essere caricati presso stazioni di ricarica messe a disposizione per il pubblico o presso stazioni di ricarica commerciali, in particolare tramite prese USB di terzi. È consentito utilizzare solo il proprio caricabatterie fornito dal produttore.

3 Costi e compatibilità dei software

Le diverse tipologie del software «Threema» sono interamente compatibili tra loro. Ciò significa che gli utenti della versione così come è stata introdotta nell'Amministrazione federale possono comunicare senza problemi con gli utenti di una versione di «Threema» acquistata privatamente.
Gli esterni sono responsabili dell'acquisto, dell'aggiornamento e dei costi della propria installazione di «Threema».

4 Rispetto dell'accordo di utilizzo

Confermando la ricezione di questo accordo di utilizzo, gli esterni dichiarano di aver letto e compreso le presenti condizioni di utilizzo di «Threema» e si impegnano a garantire il rispetto del presente accordo di utilizzo per quanto attiene alla comunicazione con i collaboratori dell'Amministrazione federale.