COESIONE ITALIA 21-27 TOSCANA

Cofinanziato dall'Unione europea

Regione Toscana

CART - Adeguamento ai recenti standard di sicurezza dell'infrastruttura

COESIONE ITALIA 21-27 TOSCANA

Cofinanziato dall'Unione europea

Regione Toscana

Evoluzione del protocollo TLS

Percorso di miglioramento da SSL a TLS:

Protocollo	Rilascio	Obsoleto	
SSL 3.0	1996	2015	Prima base per la sicurezza su Internet
TLS 1.0	1999	2020	Miglioramenti di sicurezza rispetto a SSL, ma vulnerabile ad attacchi di downgrade e crittoanalisi avanzata
TLS 1.1	2006	2020	Introduzione di ulteriori mitigazioni, ma affetto da vulnerabilità e privo di supporto per algoritmi di crittografia moderni
TLS 1.2	2008	-	Riconosciuto come standard sicuro grazie a crittografia avanzata (AES-GCM, SHA-256) in uso per la maggior parte delle applicazioni
TLS 1.3	2018	-	Standard più sicuro attualmente disponibile, con focus su performance, sicurezza ed eliminazione di algoritmi deboli

Quando si opera su protocollo TLS e si eseguono adeguamenti di sicurezza, è fondamentale ricordare che questi aspetti sono strettamente correlati alla compatibilità delle **cipher suite**, degli **algoritmi di encryption** e più in generale del layer crittografico in uso.

Normative e Standard operativi

Le versioni marcate come obsolete (con TLS < 1.2) non soddisfano più i requisiti delle linee guida di sicurezza moderne, con la maggior parte dei browser che non accetta più connessioni e meccanismi di encryption con tali protocolli.

Cosa dicono le normative:

- **Linee guida AGID (2022):**

  Uso obbligatorio di **TLS 1.2** o superiore per garantire la protezione dei dati sensibili nelle comunicazioni tra enti pubblici.

- **Direttiva NIS 2 (2020):**

  Obbligo per gli operatori di servizi essenziali di adottare misure di sicurezza adeguate, incluso l'uso di protocolli sicuri come **TLS 1.2** o **TLS 1.3**.

Adeguarsi a **TLS 1.2** o superiore non è solo un obbligo normativo, ma una **scelta strategica** per garantire una adeguata sicurezza sui canali di interoperabilità, la protezione dei dati e la fiducia degli utenti.

Tempistiche di transizione

31 Ottobre 2024

Adeguamento canali CART in Collaudo

5 Marzo 2025

Adeguamento canali CART in Produzione

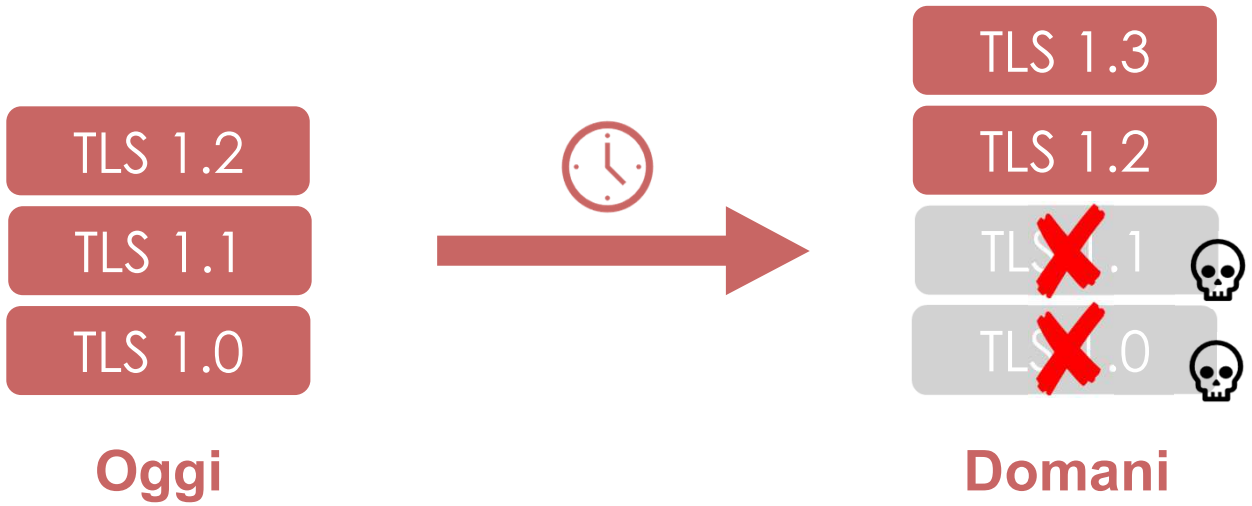
30 Aprile 2025

Dismissione canali CART vecchi (deprecati)

In fase di adeguamento, viene **interrotto il supporto ai protocolli TLS 1.0 e TLS 1.1** sui canali esposti dal CART verso i fruitori che richiamano API in ambito Regione Toscana.

ATTENZIONE: Gli applicativi che non si adeguano rischiano l'interruzione dei servizi fruiti

Panoramica di transizione (1/3)



In fase di adeguamento della sicurezza su protocollo TLS, verrà operata un'**abilitazione della versione 1.3** congiuntamente alla **disabilitazione delle versioni inferiori alla 1.2.**

Chi ad oggi ha già predisposto un'infrastruttura compatibile con protocollo **TLS 1.2 risulta già adeguato allo stato futuro della transizione.**

Panoramica di transizione (2/3)

Di seguito è riportata la lista degli **hostname Cart impattati dall'adeguamenti di sicurezza** in ambito TLS:

Hostname Produzione Switch da: 5 Marzo 2025	Hostname Collaudo Switch da: 31 Ottobre 2024	Esposizione	TLS
api.regione.toscana.it	apistage.regione.toscana.it	Internet	1.2
api.rete.toscana.it	apistage.rete.toscana.it	Internet	1.2
api.rt.tix.it	apistage.rt.tix.it	Intranet	1.2
apimed.regione.toscana.it	apimedstage.regione.toscana.it	Internet	1.2 , 1.3
fse20gw.regione.toscana.it	fse20gwstage.regione.toscana.it	Internet	1.2 , 1.3
elk.sanita.toscana.it	elk-test.sanita.toscana.it	Internet	1.2 , 1.3

Panoramica di transizione (3/3)

Di seguito è riportata anche la lista degli hostname Cart di Produzione che saranno progressivamente **dismessi** entro l'ultima milestone di adeguamento (**Data di dismissione: *30 Aprile 2025***):

- **pda.tix.it**
- **pda-rt.tix.it**
- **pdds-center.tix.it**
- **proxycart-int.tix.it**
- **pddcart-int.tix.it**

Si invita fin da subito tutti i soggetti ad una verifica puntuale sugli applicativi in gestione, al fine di individuare la presenza di chiamate residue verso tali hostname. In caso affermativo, si proceda celermente a contattare il supporto Cart, con il dettaglio della casistica per ricevere istruzioni sul nuovo indirizzamento.

Contatti

Serve aiuto per l'adeguamento ?

- **Informazioni tecniche di dettaglio:**
  https://cart.regione.toscana.it/portale/it/integrazione-degli-applicativi/versioni-del-protocollo-tls-compatibili-con-i-front-end-del-cart/

- **Mail:**
  - ✓ Supporto tecnico ServiceDesk Cart (ticket): **cartdesk@regione.toscana.it**
  - ✓ Dubbi e domande in ambito servizi RT e TLS: **cart@regione.toscana.it**

In caso di problematiche, si richiede un contatto mail o l'apertura di un apposito ticket di supporto entro e non oltre il **17 Febbraio 2025.** Indicando la natura del problema, l'applicativo fruitore, l'URL richiamato ed eventuale utenza utilizzata per l'accesso.
Al fine di fornire assistenza nel percorso di adeguamento e garantire una transizione senza interruzioni.

FAQ (1/3)

1. Perché disabilitare TLS 1.0 e 1.1 ?

***Risposta*:** TLS 1.0 e 1.1 sono obsoleti e vulnerabili a numerosi attacchi di sicurezza. Disabilitarli garantisce una protezione più robusta contro le minacce moderne e allinea il sistema agli standard di sicurezza internazionali.

2. Quali sono i benefici di utilizzare TLS 1.2 o 1.3 ?

***Risposta*:** Queste l'adozione di queste versioni offre miglioramenti significativi in termini di sicurezza, velocità e affidabilità. TLS 1.3, in particolare, riduce i tempi di handshake e migliora la privacy e la protezione contro gli attacchi.

3. Cosa succede se un client non si adegua a TLS 1.2 o 1.3 ?

***Risposta*:** Se i client non supportano TLS 1.2 o TLS 1.3, non saranno in grado di comunicare con le API esposte dal Cart in ambito RT. In quanto le richieste verranno rifiutate direttamente in fase di TLS handshake.

4. Cosa fare per adeguarsi a TLS 1.2 o TLS 1.3 ?

***Risposta*:** Si dovrà innanzitutto verificare se l'applicativo in gestione, collegato all'adeguamento, supporti già queste versioni di protocolli (operativi dal 2008), verificando la compatibilità puntuale sia dei protocolli TLS sia delle cipher suite ad esse correlate. Accertandosi della loro corretta abilitazione con i vostri rispettivi CED interni ed i fornitori delle applicazioni, eventualmente aggiornando la componente client dell'applicazione dove necessario per supportare almeno **TLS 1.2**.

FAQ (2/3)

5. Cosa succede se il mio sistema non può supportare TLS 1.2 o 1.3 ?

Risposta: Dovrai aggiornare o sostituire i componenti incompatibili per garantire la continuità del servizio. Se non è possibile, dovrai considerare alternative per la connessione sicura, come un'applicazione intermedia che supporta TLS 1.2.

6. Posso fare test sull'ambiente di Collaudo Cart prima della data di transizione in Produzione ?

Risposta: Assolutamente sì. E' fortemente consigliato fare dei test tecnici sul canale, effettuando delle prove dall'ambiente di Stage dell'applicazione fruitore verso tutti i vari canali esposti dal Cart in ambiente di Collaudo (già aggiornato con TLS >= 1.2). Al fine di garantire che tutti i sistemi in uso siano compatibili con le versioni TLS target, le cipher suite, i meccanismi di handshake, etc… prima dello switch sul canale.

7. Cosa succede se ci sono problemi di compatibilità dopo la disabilitazione dei TLS obsoleti ?

Risposta: In caso di problemi, si contatti immediatamente il supporto tecnico indicato per ricevere assistenza lato Cart. Nel contatto, si specifichi l'URL invocato insieme ai dettagli della chiamata API, verificando sui log locali all'applicazione se necessario aggiornare o modificare le configurazioni del TLS.

FAQ (3/3)

8. Chi ha applicativi in cloud e in server farm potrebbe essere comunque impattato ?

***Risposta*:** Si se richiama uno o più degli hostname Cart menzionati dall'adeguamento di sicurezza. Occorre in ogni caso procedere con una verifica se l'applicativo in gestione (e relativa componente su cui gira) supporti già queste versioni di protocolli TLS. Accertandosi della loro corretta abilitazione con i vostri rispettivi referenti informatici interni all'ente ed i fornitori delle applicazioni,

9. Credo che il mio applicativo utilizzi già TLS >= 1.2, ma non sono sicuro se presenti eccezioni legate a flussi specifici non-adeguati ?

***Risposta*:** In questo caso consigliamo in primis di rivolgersi ai propri fornitori, per verifica puntuale di quali servizi siano effettivamente invocati verso gli hostname del Cart. Una volta avuta tale evidenza, potete contattare il supporto Cart (tramite ticket a *cartdesk@regione.toscana.it*) con i dettagli della vostra richiesta di verifica.