4u S.r.l.

4Ever®

Firma Digitale di Stream

4Ever® è un prodotto software della suite 4Sign orientatato a gestire la firma digitale di stream, ovvero di sequenze di messaggi di log o di frame grafiche e/o sonore, in modalitá non presidiata, mantenendo il pieno valore legale della firma apposta. Lo scenario tipico di 4Ever® prevede:

- Uno o più processi applicativi (**Target Generator**), di generazione delle sequenze di eventi (messaggi, frame) da firmare (**Stream Target**);
- un processo di firma (**4Ever-Server**) attivato da un operatore con le proprie credenziali di firma, che operando in background verifica con continuitá la generazione degli Stream Target e provvede alla firma digitale del relativo file di log utilizzando l'infrastruttura 4Sign;
- un processo collettore (**4Elog-Server**) attivato contestualmente a 4Ever-Server, che raccoglie le sequenze di dati da firmare dai processi Target-Generator, e li accumula nel file di log per essere firmati dal processo Server 4Ever;
- un client di attivazione/disattivazione del servizio (**4Ever-Client**), utilizzato degli operatori per attivare/disattivare il processo di firma digitale dei Target.

Il processo 4Ever-Server mantiene, durante la sua vita attiva, le credenziali di firma dell'operatore in un'area di memoria protetta da uno schema proprietario (**MutingBox**), in base al quale il contenuto protetto varia con continuitá la sua forma senza perdere le proprie informazioni. Questo approccio permette di garantire la validitá della firma digitale apposta con continuitá dal 4Ever-Server ai file dello Stream Target senza la necessitá di un continuo presidio dell'operatore.

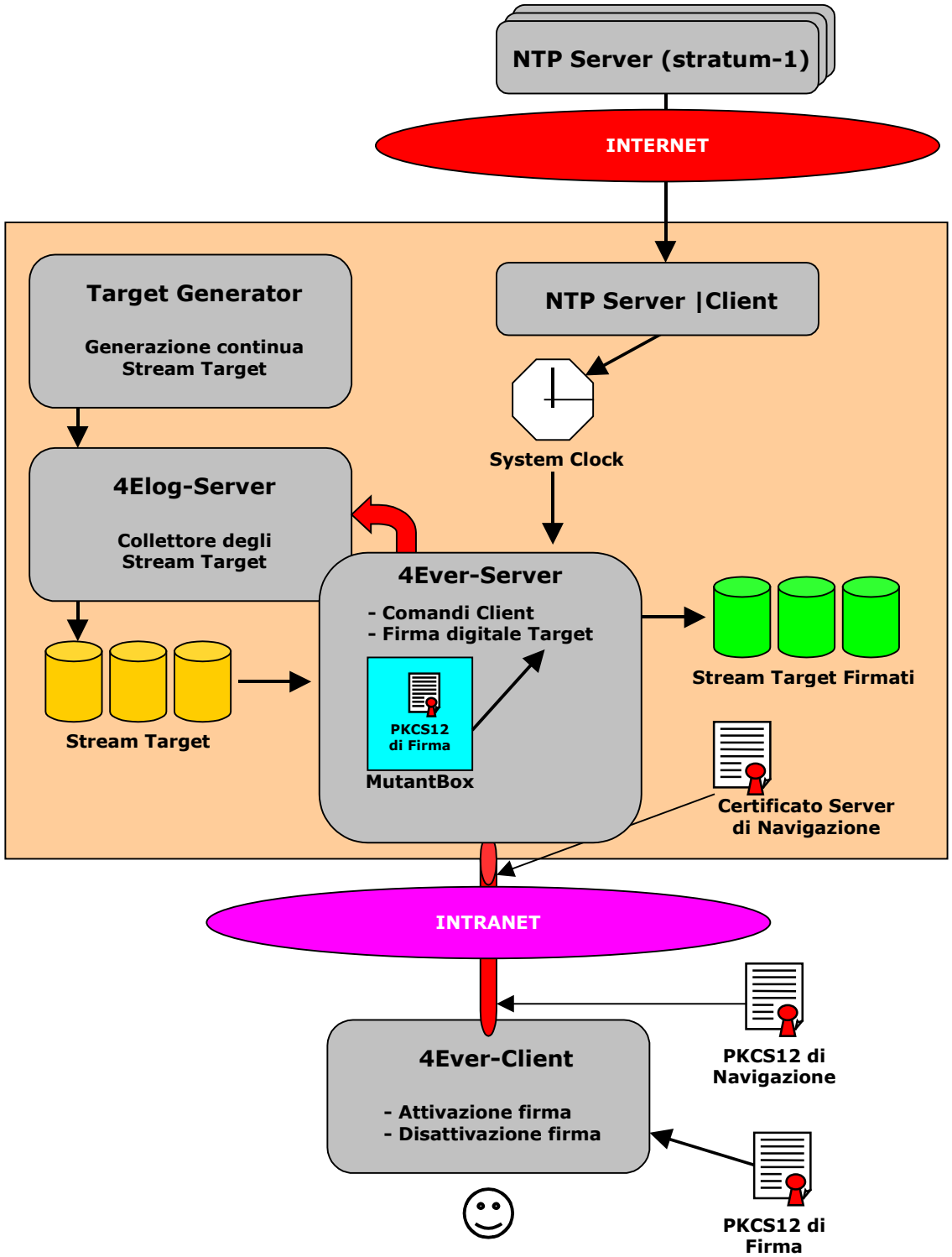
4Ever-Server puó limitare la propria azione alla generazione di **file firmati in formato PKCS7**, o estendere il processo di firma alla **apposizione di una marca temporale auto-certificata**, generando **file SMIME** contenenti sia i file PKCS7 firmati che la marca temporale di tali file.

A tal scopo è necessario che sul sistema su cui opera il servizio 4Ever® opera sia attivo un processo di mantenimento della data/ora di sistema in base al protocollo NTP, e che tale processo sia costantemente attivo e connesso tramite la rete Internet ai propri nodi NTP di primo livello (stratum-1) per garantire l'allineamento della data/ora di sistema.

Per ogni Stream Target da firmare può essere attivato un servizio 4Ever® dedicato, che risponde al proprio 4Ever-Client su una porta TCP riservata. Su un sistema possono operare piú coppie 4Ever-Server/4Elog-Server per la firma di differenti Stream Target: ogni istanza del servizio utilizza una porta TCP riservata per ricevere i comandi client, e una porta TCP riservata per ricevere i dati da accumulare nel file di log.

La comunicazione tra 4Ever-Client e 4Ever-Server viene effettuata mediante una connessione SSL/TCP, con l'adozione di appositi certficati di navigazione. In fase di attivazione 4Ever-Client trasmette a 4Ever-Server, su questa connessione certificata, le credenziali di firma in formato PKCS12, opportunamente protette da una frase di passo che viene trasmessa in formato protetto. La frase di passo viene riassegnata automaticamente dal 4Ever-Server. Le credenziali dell'operatore e la relativa frase di passo sono mantenute dal 4Ever-Server nell'area di memoria mutante (MutantBox).

L'architettura 4Ever è illustrata nella figura seguente.



Processi e File

Il servizio **4Ever**® è implementato con il supporto di due processi:

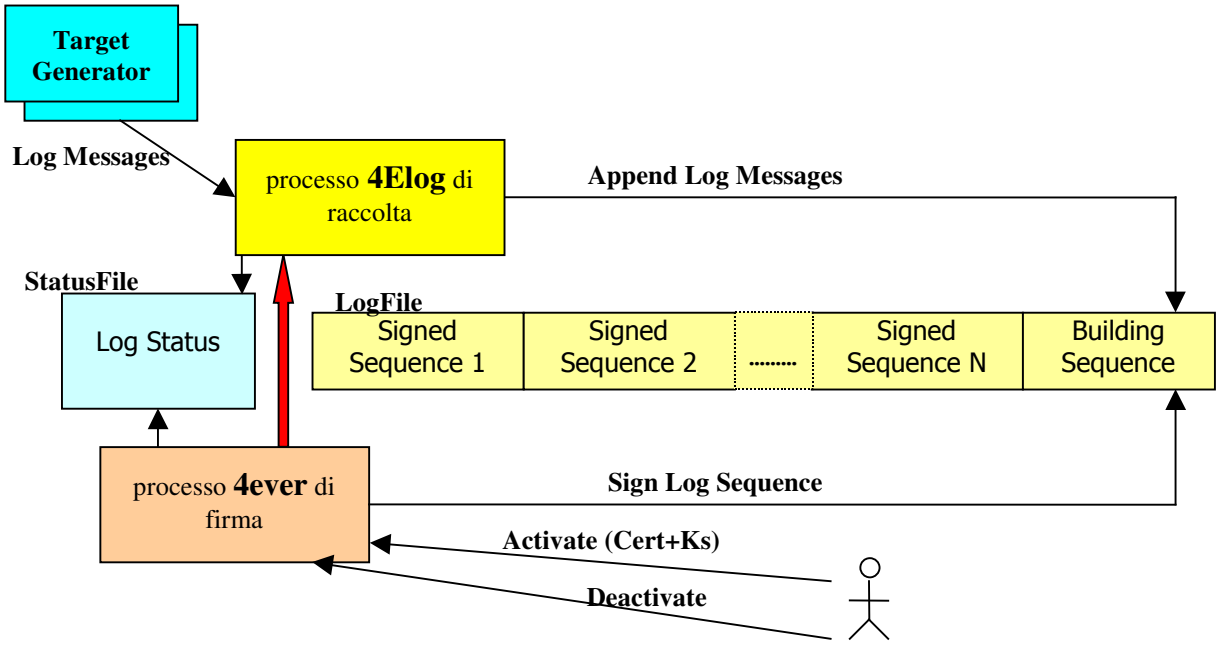
4Ever-Server processo principale, monothread-monoconnessione, di firma digitale dei log
4Elog-Server processo secondario, multithread, di raccolta dei log

I due processi operano con il supporto di due file:

StatusFile file contenente le variabili comuni di log, utilizzato per il sincronismo tra 4Ever e 4Elog
LogFile file su cui sono memorizzate le sequenze di log firmate

I log sono raccolti in un file di log (LogFile) come sequenze di messaggi (testata + dati), inizialmente non ancora firmati. Periodicamente il servizio 4Ever provvede a firmare l'ultima sequenza raccolta. Di conseguenza il LogFile è un insieme ordinato temporalmente di sequenze firmate ed eventualmente di una sequenza (l'ultima) non ancora firmata. Ogni sequenza è costituita da un insieme variabile di messaggi, in cui ogni messaggio viene marcato con l'Hash del messaggio precedente della sequenza (ad esclusione del primo che mantiene l'Hash della propria area dati).

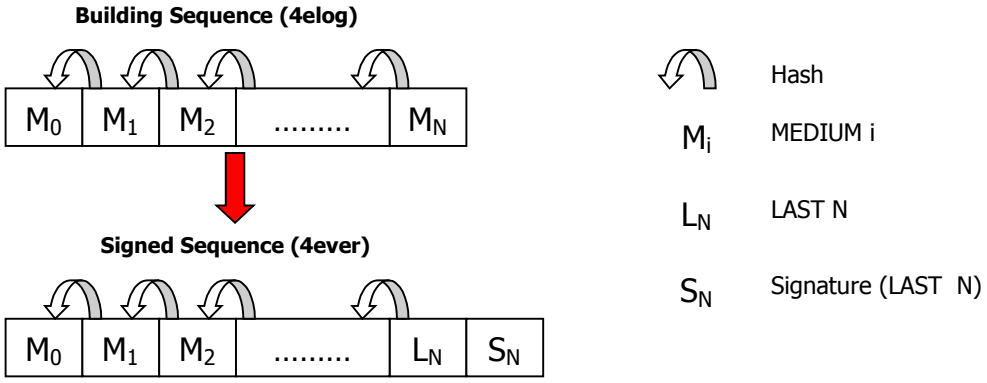
La figura seguente illustra lo schema del servizio 4Ever. Il processo 4Ever-Server viene armato per la firma da un operatore, che trasmette su un canale sicuro (SSL) il certificato e la chiave segreta di firma, che sono poi mantenuti in una meroria interna protetta (stealth memory di tipo MutantBox).



Quando viene armato il processo 4Ever-Server crea il processo 4Elog-Server, il quale opera su una porta TCP dedicata. I processi applicativi comunicano i messaggi di log al processo 4Elog-Server, che li accumula nel LogFile nell'ultima sequenza non firmata (Building Sequence). Il processo 4Ever-Server si attiva periodicamente, e firma l'ultimo messaggio della Building Sequence trasformandola in una Signed Sequence.

Validità della Firma di una Sequenza

La validità del meccanismo di firma su una Signed Sequence è dato dalla catena di Hash che ogni messaggio mantiene relativamente al messaggio precedente (ad eccezione del primo che mantiene l'Hash della propria area dati). La firma viene apposta sull'ultimo messaggio della sequenza. La figura seguente illustra il meccanismo di raccolta dei messaggi nella Building Sequence e l'azione di firma di quest'ultima che viene così trasformata in una Signed Sequence.



Architettura del Servizio 4Ever®

La raccolta degli eventi viene effettuata da un insieme di **sensori distribuiti**, che sono operativi sulla rete del cliente finale, e da uno o più collettori periferici, **4Ever-Collector**. I sensori distribuiti possono interagire direttamente con il 4Elog-Server, o generare log in base allo standard 'syslog' indirizzati a uno o più processi 'syslogd' operanti sulla rete (collettori).

Un collettore è un server 'syslogd', su piattaforma Unix-like, che opera in accoppiamento con un plugin specifico, **4Ever-Plugin**: il demone 'syslogd' raccoglie gli eventi dai sensori distribuiti, e li passa al plugin che provvede a marcarli con l'identificativo del sensore (in base all'indirizzo IP) e a trasmetterli al processo 4Elog del 4Ever-Server per la registrazione. Nel caso di non raggiungibilità o non disponibilità del 4Ever-Server (interruzioni di rete o temporanea sospensione del servizio), il collettore 4Ever-Collector provvede a mantenere traccia degli eventi trasmessi, e a riattivare la trasmissione quando il 4Ever-Server è nuovamente raggiungibile/disponibile.

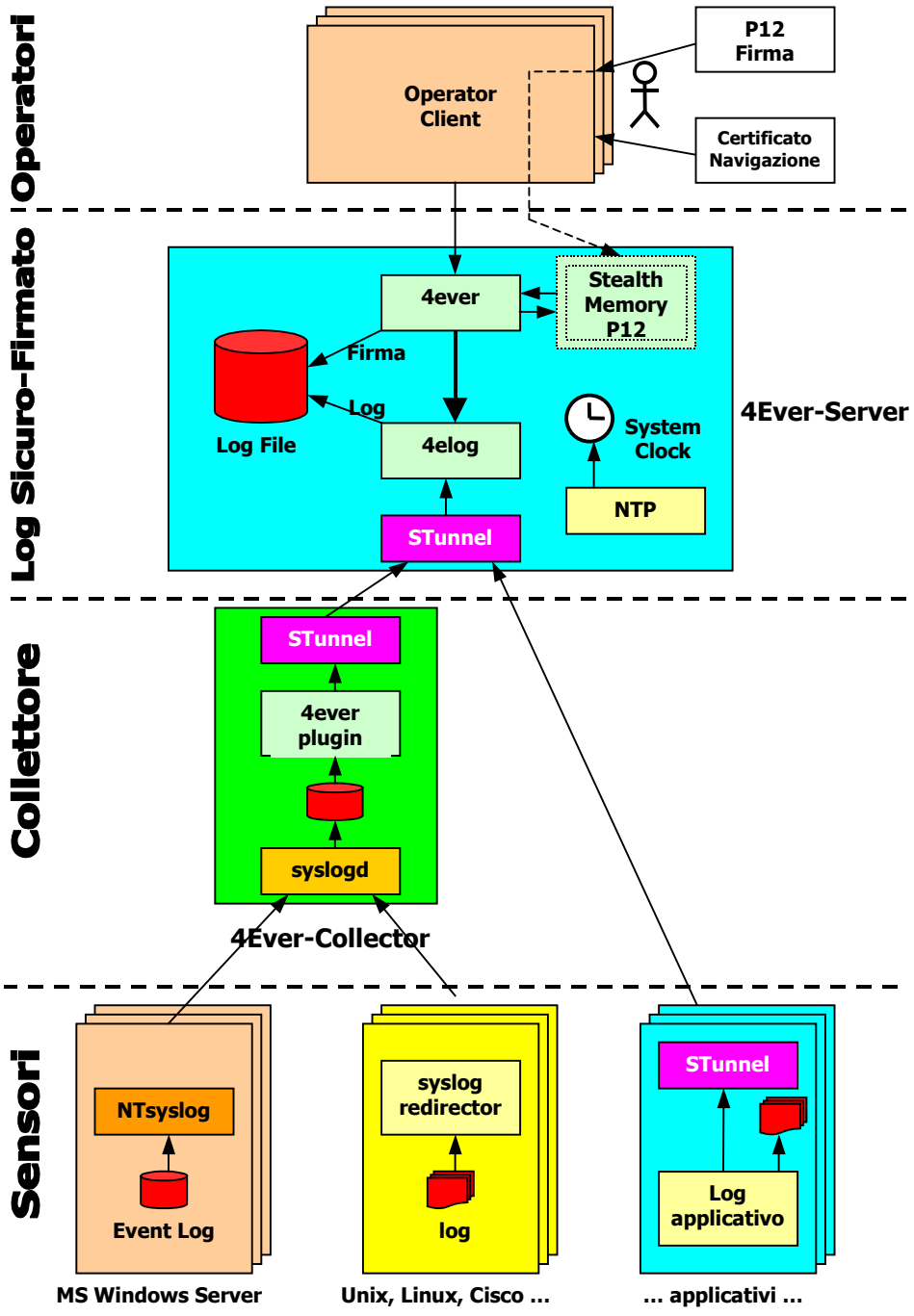
La comunicazione tra il plugin del 4Ever-Collector e il 4Ever-Server viene protetta utilizzando una coppia di processi **STunnel**, che realizzano un canale SSL gestito con i certificati X.509 propri del 4Ever-Collector e del 4Ever-Server.

Gli **operatori del servizio 4Ever** possono accedere da remoto al processo 4Ever del 4Ever-Server per attivare o disattivare il servizio, o per ricevere gli eventi relativi (firma delle sequenze, errori di firma, errori di sistema, rotazione del file di log).

L'accesso degli operatori viene effettuato mediante un protocollo dedicato trasportato su un canale SSL gestito con appositi certificati X.509 di navigazione client e un certificato X.509 server. Le operazioni di maintenance del 4Ever-Server possono essere effettuate solo dalla console locale di sistema.

La figura seguente illustra lo schema implementativo del sistema. In tale schema si identificano quattro livelli di rete:

1. i sensori applicativi e/o esterni, che sentono gli eventi e li inviano a un 4Ever-Collector;
2. il 4Ever-Collector che raccoglie gli eventi, li marca con l'identificazione di origine e li inoltra, mediante un canale sicuro, al 4Ever-Server;
3. il 4Ever-Server che riceve gli stream di eventi dai 4Ever-Collector, li registra localmente firmandoli digitalmente con il certificato X.509 e relativa chiave privata di firma del servizio;
4. gli operatori del 4Ever-Server che tramite un programma client possono, dalle rispettive postazioni, attivare, disattivare e monitorare il servizio 4Ever.



Sicurezza e Valore Legale della Firma dei Log

Il principio del servizio 4Ever® è quello di garantire che gli eventi raccolti:

1. sono registrati in modo sicuro;
2. non sono modificabili a posteriori;
3. costituiscono prova certa di quanto rilevato dai sensori.

Registrazione Sicura

Il livello di sicurezza del meccanismo globale di log è il risultato del livello di sicurezza dei singoli componenti (sensori, 4Ever-Collector, 4Ever-Server, operatori), e del livello di sicurezza dei canali di comunicazione.

Il livello di sicurezza dei **componenti** è:

- inversamente proporzionale alla distanza (in termini di rete) dal 4Ever-Server,
- direttamente proporzionale al proprio livello di hardening.

La distanza dal 4Ever-Server misura il livello di esposizione di un componente ad agenti esterni:

livello 0: i sensori sono i componenti più distanti, in quanto operano in un'area della rete in cui sono erogati i servizi applicativi, e a cui accedono gli utenti esterni;
livello 1: il 4Ever-Collector rappresenta il primo livello di protezione del servizio, a cui possono accedere solo i sensori;
livello 2: il 4Ever-Server rappresenta il secondo e più elevato livello di protezione del servizio, accessibile solo dal 4Ever-Collector per la comunicazione degli eventi da registrare e dalle postazioni degli operatori.

Le postazioni degli operatori devono possibilmente operare al livello di sicurezza del 4Ever-Server (postazioni dedicate, livello 2) o quantomeno al livello di sicurezza del 4Ever-Collector (postazioni condivise con altri servizi sicuri, livello 1).

I **canali di comunicazione** utilizzati sono tre, ognuno con un proprio grado di sicurezza:

grado 1: comunicazione su protocollo 'syslog' tra i **sensori** e il **4Ever-Collector**: questi canali operano con un protocollo non connesso (UDP) in chiaro, e la protezione può essere solo a livello del controllo del flusso di rete (firewall di attraversamento, auto-firewalling del 4Ever-Collector);
grado 2a: comunicazione su protocollo dedicato tra il **4Ever-Collector** e il **4Ever-Server**, che può essere crittografato con schemi proprietari a chiavi simmetriche (eventualmente concordati con il cliente), protetto intrinsecamente con il protocollo SSL implementato da STunnel, e protetto a livello del controllo del flusso di rete (firewall di attraversamento, auto-firewalling del 4Ever-Server);
grado 2b: comunicazione su protocollo dedicato tra le **postazioni operatore** e il **4Ever-Server**, che può essere crittografato con schemi proprietari a chiavi simmetriche (eventualmente concordati con il cliente), protetto intrinsecamente con il protocollo SSL, e protetto a livello del controllo del flusso di rete (firewall di attraversamento, auto-firewalling del 4Ever-Server).

La protezione intrinseca dei singoli componenti (**hardening**) deve rispondere ad adeguati livelli di protezione di controllo e di accesso, definiti in base alle **Policy del servizio**.

Non Modificabilità a Posteriori

Questa garanzia viene offerta dal meccanismo di firma digitale a bordo del 4Ever-Server, che permette di firmare digitalmente sequenze di eventi registrati nel file di log.

Ovviamente il livello di garanzia è:

- direttamente proporzionale al livello di hardening del 4Ever-Server,
- direttamente proporzionale alla granularità del meccanismo di firma.

Il meccanismo di firma opera non sui singoli eventi, ma solo sulla sequenza raccolta in un intervallo fisso di tempo (maggiori le prestazioni del sistema, più fine la granularità adottabile, in quanto il meccanismo di firma è un processo CPU-bound).

Bisogna tenere presente che tra il momento di rilevazione di un evento da parte di un sensore al momento di firma dell'evento da parte del processo 4Ever del 4Ever-Server, intercorrono alcune fasi in cui l'evento è esposto, in varia misura, a possibili tentativi di manipolazione: la probabilità di occorrenza di tale manipolazione è:

- direttamente proporzionale al livello di sicurezza del componente che lo tratta;
- direttamente proporzionale al grado di sicurezza del canale di comunicazione attraversato;
- inversamente proporzionale al tempo di trattamento da parte del componente.

Prova Certa

Sul piano legale la firma digitale apposta in modo automatico da un sistema non è da considerarsi allo stesso livello della firma digitale apposta da una persona fisica, in quanto il sistema non può essere considerato un dispositivo sicuro certificato ITSEC a livello E4 Security High.

Il meccanismo di firma digitale automatica di 4Ever è un **meccanismo di log ad alta sicurezza**, in grado di **garantire la non modificabilità dei dati raccolti entro i limiti dei livelli di sicurezza definiti dalle policy del servizio**, implementati nei componenti e nei canali di comunicazione, e verificati con appositi controlli di auditing.

Per dare ai log sicuri raccolti un pieno valore sul piano probatorio, questi devono essere **firmati digitalmente da un operatore** a intervalli prestabiliti (almeno una volta al giorno), utilizzando **certificati di firma emessi da un certificatore pubblico accreditato** con dispositivi di firma sicuri (**SmartCard**).

La gestione del servizio deve quindi prevedere un meccanismo di **backup-firmato** periodico, effettuato sotto il controllo di un operatore che acquisisce il file di log da certificare su una propria postazione e vi appone una firma digitale con certificato accreditato.

La firma accreditata può essere apposta con componenti software di firma rilasciati dagli enti certificatori, da terze parti, o con i componenti client 4Sign di firma digitale.