

# VALIDATION WORKFLOW

## Processo di validazione dei certificati digitali GlobalTrust

### USER FORM

Il Cliente acquista un certificato attraverso il nostro sito **www.globaltrust.it** seguendo gli STEP sottostanti elencati in **Figura 1**, i dati inseriti dal Cliente vengono memorizzati in tutta sicurezza viaggiando in SSL, all'interno dei nostri Db residente sui ns. server dedicati.

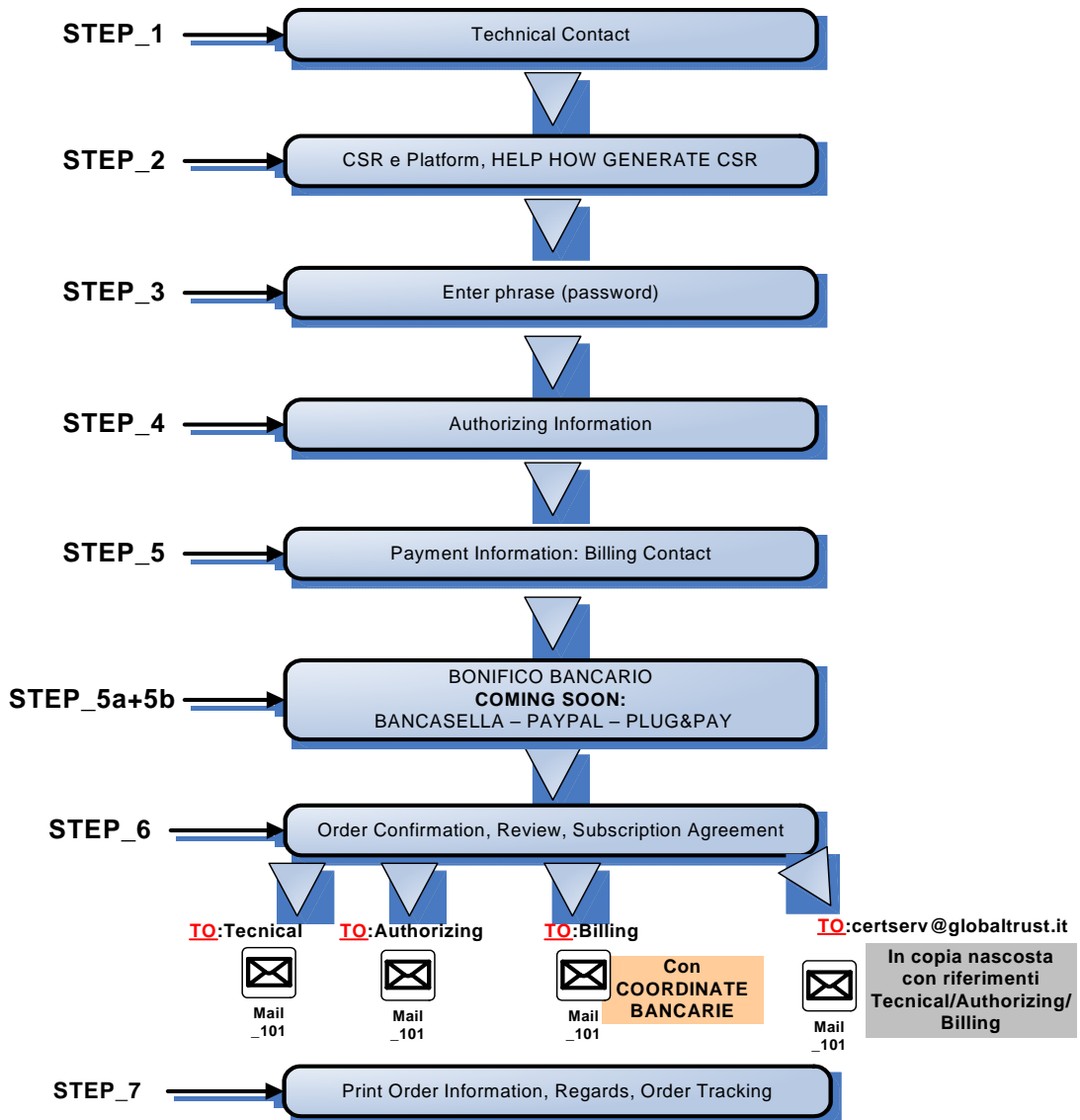
Al termine dello STEP\_6 (**Figura 1**) il sistema invia in automatico 3 diverse mail, (effettuando un controllo prima dell'invio sugli eventuali indirizzi uguali inseriti dal cliente) catalogate come (template) **Mail\_101**:

- 1) Invio **Mail\_101** -> Technical contact
- 2) Invio **Mail\_101** -> Authorizing contact
- 3) Invio **Mail\_101** + COORDINATE BANCARIE PER IL PAGAMENTO  
-> Billing contact

Il sistema invia una ulteriore copia della Mail\_101 con le rispettive e-mail del Technical / Authorizing / Billing, a **certserv** in copia nascosta.

Provvede inoltre a riempire un **Invoice** con i dati del cliente, allegandolo automaticamente alla mail.

**FIG 1: USER FORM**



## AUTENTICAZIONE E VALIDAZIONE

Il personale dell'A&V GlobalTrust riceve, come descritto una mail da **certserv** contenente tutte le informazioni necessarie all'avvio del processo di validazione.

Tutti gli ordini ricevuti (ordinati per ID\_ORDER) sono resi accessibili nella pre-maschera del tool di validazione.

Per il pagamento con carta di credito il processo di verifica comincia non appena ricevuta l'e-mail di conferma da parte dei Servizi Interbancari

Per il pagamento con bonifico, attendiamo *almeno* una ricevuta della nota di credito via fax (ovviamente vengono effettuati dei controlli nell'home banking per verificare la corrispondenza), non appena ricevuto il fax, con numero riservato ai clienti dei certificati digitali, può cominciare la validazione di tali ordini.

L'A&V Director accede all'interno della **ZONA S** (ZONA RISERVATA) protetta da un sensore biometrico al PC riservato alla validazione (protetto con password sul BIOS e altro sensore biometrico).

A questo punto comincia il processo di Validazione vero e proprio che segue lo schema sottostante, con controlli incrociati (**Crossino Check Procedure – CCP**) con archiviazione elettronica dei documenti, criptazione e immagazzinamento utilizzando un'infrastruttura a chiavi pubbliche (**PKI**) ed un' innovativo sistema che prevede **NO PAPER, NO FILES**.

# VERIFICATION FLOW

