Con "firma remota" si intende un'operazione di firma digitale eseguita con una chiave privata non residente su un dispositivo locale dell'utente (come per es. una smartcard), bensì presso un server remoto, all'interno di un HSM (dispositivo crittografico hardware).

Dal punto di vista logico-funzionale, il dialogo tra l'applicazione client (residente sul PC dell'utente) ed il server di firma può essere così riassunto:

- il client si autentica nei confronti del server (vedere oltre per ulteriori dettagli);
- il client richiede la firma digitale, inviando al server il digest (hash) del documento;
- il server calcola la firma e la restituisce al client, dove viene salvata.

Il vantaggio principale della soluzione consiste nel fatto che l'utente non ha bisogno di un dispositivo crittografico personale (come per es. una smartcard) e dei relativi driver: per firmare gli basta un'applicazione in grado di dialogare col server di firma.

La firma remota è simile alla "firma massiva", in quanto entrambe si basano su chiavi private residenti presso un server col quale si dialoga attraverso la rete. Tuttavia, quando si parla di firma remota si fa riferimento in modo particolare a:

- Operazioni di firma svolte in modo interattivo

(mentre la firma massiva è solitamente una procedura automatica)

- Da utenti che si collegano al server attraverso internet

(mentre un server di firma massiva è solitamente accessibile solo su una LAN)

Grazie alle caratteristiche della firma remota, questo particolare tipo di firma digitale si adatta maggiormente alle esigenze di utenti itineranti (roaming) e che non usano sempre il medesimo PC.

Un dispositivo HSM gestisce centinaia di certificati di firma digitale automatica simultaneamente, aumentando quindi l'efficienza delle prestazioni e la velocità di esecuzione.