

Valutazione ricette elettroniche

Con l'emendamento legislativo della Legge sui medicinali nonché le disposizioni esecutive corrispondenti dell'Ordinanza sui medicinali, ora vi è la possibilità di creare le ricette anche in modo digitale (ricetta elettronica). A tale scopo, nell'art. 51 dell'Ordinanza sono state emanate nuove prescrizioni. Di conseguenza, è necessario valutare tali prescrizioni in considerazione della soluzione scelta da HIN.

È possibile creare una ricetta elettronica in due modi. Da un lato, conformemente al cpv. 2 della suddetta prescrizione, le ricette elettroniche possono essere create elettronicamente con una firma elettronica qualificata come stabilito dalla Legge sulla firma elettronica o altrimenti «devono adempiere requisiti di sicurezza equivalenti in termini di autenticità, integrità dei dati e confidenzialità».

In tal modo, il legislatore si discosta dalle direttive della Legge sulla firma definite in modo molto restrittivo, senza tuttavia rinunciare alla protezione e alla sicurezza. Lo stesso si desume anche dal rapporto esplicativo, in cui si legge:

«Per le ricette elettroniche è possibile, al posto di una firma elettronica qualificata, scegliere una firma o una forma di trasmissione che garantisca le diverse funzioni di sicurezza quali sicurezza dell'autenticità (autorizzazione della persona prescrivente per l'emissione della ricetta), dell'integrità dei dati (protezione da contraffazioni) come pure della riservatezza (protezione da utilizzo molteplice) in modo equivalente alla firma elettronica qualificata ai sensi dell'articolo 14 capoverso 2^{bis} CO. La firma per le prescrizioni elettroniche è quindi sufficiente se la procedura utilizzata per ottenerla soddisfa le summenzionate funzioni di sicurezza. Le indicazioni in materia di sicurezza correlate alla procedura utilizzata (ad es. indicazioni della LCIP e dei relativi

sistemi comunitari) costituiscono pertanto un ambiente sufficientemente protetto per la corretta trasmissione della ricetta elettronica.»¹

Pertanto, qualora venga utilizzata un'altra forma di trasmissione diversa da quella puramente digitale², occorre valutare se questa soddisfa gli aspetti dell'autenticità dell'emittente, della protezione da contraffazioni e della protezione da utilizzo molteplice in modo analogo alla firma elettronica qualificata.

Perché tutti gli utenti possano partecipare (in particolare anche i più anziani), una ricetta elettronica deve poter essere consegnata sia digitalmente sia fisicamente/analogicamente dal medico al paziente e dal paziente alla farmacia. Con la stampa, la possibilità di una firma digitale qualificata viene resa impossibile poiché questa non può più essere verificata.

HIN ha optato per un codice QR (vedi allegato), in grado di mostrare le informazioni della ricetta elettronica e trasmetterle sia digitalmente sia analogicamente. In tale contesto viene utilizzata la firma HIN Sign per la creazione della ricetta, la quale garantisce la sicurezza e l'univocità della ricetta. In tal modo vengono soddisfatti i requisiti correlati nella misura in cui siano chiaramente equivalenti.

L'autenticazione del medico – quale ultimo criterio – dovrebbe assegnare la ricetta elettronica al medico emittente. A tal proposito viene impiegata un'identità elettronica con autenticazione forte, per la quale il medico deve effettuare la registrazione personale presso HIN (identificazione video conforme alla LCIP e invio fisico dei dati di accesso). Tale identità elettronica

¹ Pacchetto di ordinanze sugli agenti terapeutici IV, Rapporto esplicativo concernente l'Ordinanza sui medicinali (OM), UFSP, settembre 2018, https://www.bag.admin.ch/dam/bag/de/dokumente/biomed/heilmittel/revision-hmg/erlaeuterungen-vam.pdf.download.pdf/VAM_Erlaeuterungen_de.pdf

² Nota bene: una firma elettronica qualificata deve rimanere digitale affinché sia possibile valutarne la validità.

rafforzata è obbligatoriamente necessaria per la generazione della firma elettronica. Ciò avviene in conformità alla norma tecnica CSN EN 419241-1 (Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements; European Standards, https://www.bakom.admin.ch/bakom/it/pagina-iniziale/digitale-e-internet/comunicazione_digitale/firma-elettronica/referenza-normalizzazione.html). Per la firma elettronica qualificata si rimanda a SCAL2 (SRA_SAP1.1). Nell'Annex A, subclause A2.2, pag. 41 dell'Annex, la base dell'autenticazione è descritta come segue:

«The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.»

Nel medesimo Annex viene altresì indicato che per l'autenticazione devono avvenire due verifiche (substantial, punto 1 «authentication factors») tramite diversi accessi (ibidem «different categories»).

Il presente progetto prevede tre opzioni di registrazione.

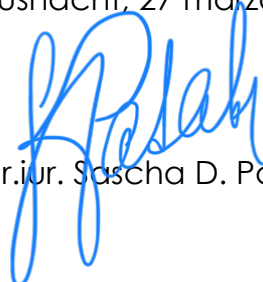
Come primo metodo il medico si autentica tramite la propria registrazione presso HIN mediante due fattori: 1) password forte per la registrazione HIN 2) con un SMS con codice. Una password forte permette di escludere già di fatto la ricerca casuale della password a opera di terzi (secondo la prescrizione «highly unlikely»). Qualora la password dovesse essere intercettata o carpita, dovrebbe rimanere disponibile il telefono per il secondo fattore. In tal modo, viene garantita la sicurezza dell'autenticazione secondo la direttiva.

Come secondo metodo viene utilizzato – in aggiunta alla password del medico – il client HIN. Tale client funge già da accesso sicuro per i medici per la piattaforma HIN ed è in uso già da tempo come secondo fattore. Esso verifica (tramite registrazione separata e tecnologia a elevata sicurezza appositamente sviluppata allo scopo) l'integrità della password e garantisce il secondo fattore con una sicurezza altrettanto elevata.

In particolare, per i medici in ospedale è stata resa disponibile un'ulteriore procedura poiché in tale sede non può essere sempre garantita la ricezione di un SMS (assenza di telefono cellulare o di collegamento) e il client HIN non può essere integrato presso tutte le sedi (direttive ospedaliere interne). Essi si registrano internamente con una password forte secondo le direttive della Direzione della sanità e dell'ospedale. In tale contesto, come secondo fattore vi è un Location Security Management, il quale verifica la posizione di ogni medico nel sistema di HIN e la confronta con la posizione a lui consentita. In questo modo, l'integrità dell'accesso viene verificata tramite i controlli e le autorizzazioni degli accessi presso il luogo corrispondente. Con tale verifica dell'integrità è possibile escludere che, ad esempio, una password carpita possa essere utilizzata dall'esterno (pertanto al di fuori dell'ospedale). Una password ad elevata sicurezza (la quale costituisce una base negli ospedali) è già molto sicura come descritto in precedenza. Con il Location Security Management viene stabilita inoltre una sicurezza da un secondo fronte. Di conseguenza, è praticamente impossibile («highly unlikely») creare una ricetta elettronica con una password carpita poiché ci si dovrebbe trovare inoltre ancora all'interno dell'ospedale (il quale riconosce e memorizza tutti gli accessi tramite file di log). Ciò soddisfa anche i requisiti della direttiva tecnica ed è comparabile a quelli di altri regolamenti a due fattori.

Secondo l'interpretazione qui riportata, con le tre modalità descritte è possibile soddisfare il requisito del legislatore in riferimento a una ricetta elettronica.

Küsnacht, 27 marzo 2023



Dr. iur. Sascha D. Patak