

Autorità per l'informatica della pubblica amministrazione
Deliberazione 9 novembre 1995, n. 19
“Definizione delle regole tecniche per il mandato informatico.”

G.U. 22 novembre 1995, n. 273

- Visto l'art. 2, comma 2, del decreto del Presidente della Repubblica 20 aprile 1994, n. 367, che prevede che il l'Autorità definisca "le regole tecniche .. affinché le evidenze informatiche possano essere validamente impiegate a fini probatori, amministrativi e contabili"; Precisato che per evidenza informatica si intende un messaggio elettronico, composto da dati utente e da codici universali, che viene validamente impiegato a fini probatori, amministrativi e contabili;
- Vista la proposta all'uopo predisposta dagli uffici;

Delibera di dettare, a norma dell'art. 2, comma 2, del decreto del Presidente della Repubblica 20 aprile 1994, n. 367, le regole tecniche per il mandato informatico di seguito riportate:

Regole tecniche per il mandato informatico

1 - Protocollo di trasmissione

I dati vengono trasmessi, di regola, attraverso linee di telecomunicazione: il protocollo di trasmissione adottato è quello nella norma CCITT X.25 e successive evoluzioni.

2 - Regole sintattiche

Le regole sintattiche di trattamento delle evidenze informatiche devono conformarsi allo standard UN/EDIFACT mantenuto da UN/ECE, emesso da ISO e ripubblicato da CEN per l'Europa, e pertanto la norma di riferimento è la EN 29735:1992 (ISO 9735) e successive evoluzioni, incluso ISO 9735 Amendment 1:1992 (estensione del repertorio caratteri).

3 - Directory UN/EDIFACT

I messaggi da utilizzare dovranno essere conformi alle specifiche definite nella directory UNTDID e scelti tra: i messaggi allo status 2 (messaggi standard) dell'ultima directory pubblicata, altrimenti tra i messaggi allo status 2 di directory precedenti all'ultima pubblicata ma non oltre la Untdid Version S.93.A inclusa, altrimenti tra i messaggi allo status 1 dell'ultima directory o di directory precedenti all'ultima pubblicata, ma non oltre la Untdid Version D.93.A inclusa. Qualora si renda necessario definire nuovi messaggi si fa riferimento a quanto specificato nel documento "UN/EDIFACT Message Design Guidelines"; le strutture di dati dovranno conformarsi, ove

possibile, a quelle definite nelle directory UN/EDIFACT di "segmenti dati" e "data element". Tali messaggi dovranno essere sottoposti all'Autorità per una verifica e per un'eventuale, successiva, istruttoria per la standardizzazione.

4 - Sicurezza dell'interscambio

4.1 Servizi.

Per quanto attiene la sicurezza dell'interscambio dovranno essere realizzati i seguenti servizi:

- autenticazione dell'origine;
- non ripudio (invio e ricezione);
- integrità del contenuto;
- integrità della sequenza dei messaggi.

I suddetti servizi dovranno essere realizzati in conformità al DRAFT UN/ECE R. 1026 Addendum 1-4 emesso dalle Nazioni Unite nell'aprile 1994, che rappresenta attualmente il documento di riferimento per la realizzazione della sicurezza in UN/EDIFACT.

Qualora le amministrazioni interessate ritengano necessario realizzare anche il servizio di "Confidenzialità del contenuto" (Riservatezza), per il quale non è disponibile alla data alcuno standard UN/EDIFACT di riferimento, la sua realizzazione dovrà avvenire secondo la seguente modalità:

Realizzazione del servizio per la riservatezza, contestualmente agli altri servizi di sicurezza, nell'ambito dello stesso messaggio.

I dati oggetto del servizio per la riservatezza sono quelli contenuti in tutti i segmenti del messaggio (Tecnica Header - Trailer). Gli elementi di sicurezza necessari alla decrittazione dei segmenti utente sono inseriti in appositi segmenti posti all'inizio del messaggio e prima della parte crittografata.

Per particolari condizioni, e previa autorizzazione dell'Autorità, è possibile adottare la seguente modalità alternativa: Realizzazione del servizio per la riservatezza mediante interscambio EDIFACT. Il messaggio contenente i dati applicativi viene inviato crittografato e l'interscambio avviene utilizzando uno dei meccanismi di comunicazione descritti al punto 5 (Meccanismo di comunicazione). Le informazioni per la decifrazione del messaggio interscambiato sono inviate, tramite messaggio AUTACK, assieme alle altre informazioni necessarie a realizzare i servizi di sicurezza indicati in precedenza.

4.2 - Gestione delle chiavi.

Per la gestione delle chiavi sarà necessario individuare i cinque distinti ruoli appresso riportati:

- utente;
- autorità di certificazione;
- directory;
- generatore della chiave;
- autorità di registrazione.

Per quanto riguarda sia le modalità di gestione delle chiavi sia le competenze da attribuire ai singoli ruoli, saranno specificate appropriate regole tecniche da parte dell'Autorità. Nel caso di interscambio tra un numero limitato di entità, e in attesa delle relative regole tecniche, è consentito l'uso di un meccanismo bilaterale concordato tra le parti. A tal fine, le modalità di gestione e delle chiavi possono essere distinte per:

Chiavi asimmetriche:

- generazione: avviene a cura di ciascuna entità;
- distribuzione: ciascuna entità invia la chiave pubblica soddisfacendo i requisiti di autenticità, integrità e non ripudio dell'origine e della destinazione;

Chiavi simmetriche:

- generazione: avviene a cura di una delle entità, o dalle entità in concorso, rispettando le procedure concordate e sottoscritte;
- distribuzione: avviene come per le chiavi asimmetriche realizzando, in aggiunta, il soddisfacimento del requisito della confidenzialità. Le chiavi dovranno essere rinnovate periodicamente e con un intervallo di tempo concordato tra le amministrazioni interessate rispettando i requisiti sopra esposti.

5 - Meccanismo di comunicazione

Il meccanismo di comunicazione che dovrà essere utilizzato per lo scambio delle evidenze informatiche dovrà essere conforme alla norma CCITT X.400 versione 88 (ISO/IEC 10021-1-7:1988) e successive evoluzioni. L'interchange EDIFACT dovrà essere trasferito con approccio P2. Alternativamente potrà essere utilizzato il protocollo riportato nella norma CCITT X.435 (ISO/IEC 10021-8,9) conosciuto anche con la denominazione Pedi.

6 - Modelli di accordo (Contratto EDI)

Per gli accordi bilaterali si dovrà fare riferimento alla raccomandazione della Commissione della Comunità europea del 19 ottobre 1994, che specifica lo schema contrattuale per la regolamentazione degli aspetti tecnici e legali dell'interscambio tra le parti. Quando saranno disponibili altre norme che soddisfino le esigenze relative al mandato informatico l'Autorità provvederà ad emanare le relative regole tecniche.

Roma, 9 novembre 1995

Il presidente: REY