Un sistema geografico dedicato ai cimiteri

di Nicola Bortolotti

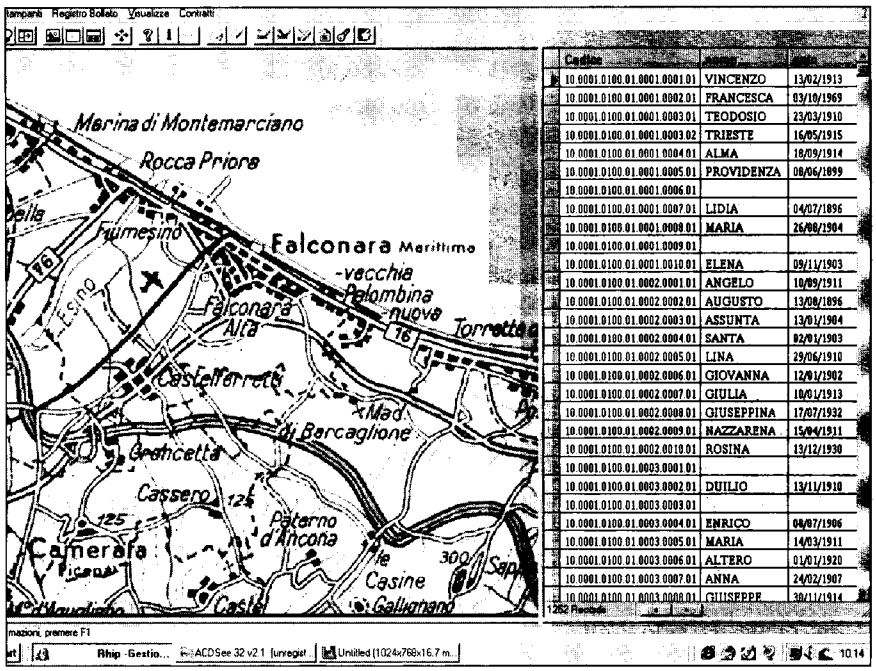

Figura 1 - Il software RhIP - gestione procedure cimiteriali - è un vero e proprio "sistema informativo geografico". Il fulcro dell'interazione col programma sono infatti cartine, piante e fotografie.

Prosegue l'analisi di alcuni dei software cimiteriali disponibili sul mercato italiano iniziata nel fascicolo 4/97 di Nuova Antigone.

I tre programmi fin ad ora esposti presentavano importanti differenze tali da renderne impossibile una comparazione diretta persino per quanto concerneva i listini e, anche

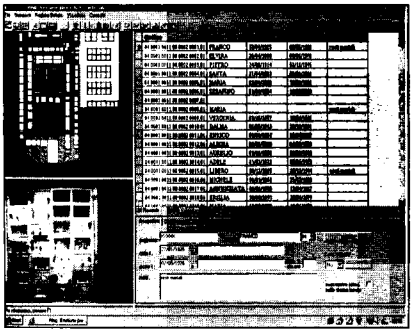

Figura 2 - Partendo dal generale si arriva al particolare, giungendo sino alle singole fotografie di loculi, colombari e così via.

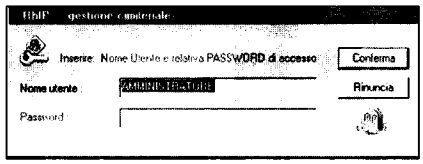

Figura 3 - L'accesso al programma è possibile solo dopo essersi identificati come utenti.

in questo caso, ci si trova di fronte ad un prodotto con significative ed importanti peculiarità.

RhIP

La principale caratteristica del prodotto illustrato in questo numero, RhIP dello Studio Presta di Ancona, è innanzitutto quella di essere un software di concezione recente, rivolto esclusivamente ai (peraltro diffusissimi) sistemi operativi Windows 95 o Windows NT e a configurazioni hardware di un certo livello (anche se i requisiti minimi prevedono un processore 486 DX 2-66, è altamente consigliabile l'utilizzo di un Pentium 133 con 32 MB di memoria). La particolarità maggiore del pacchetto di gestione cimiteriale RhIP è tuttavia costituita dalla sua

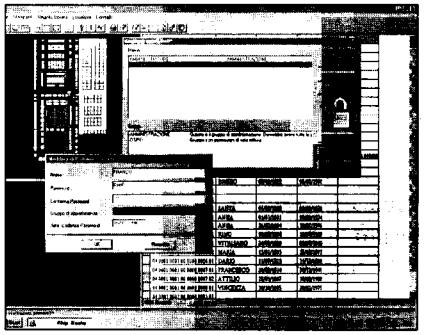

Figura 4 - L'amministratore del sistema può modificare ciascun profilo di utente, personalizzandolo in base alle singole competenze, delimitando le aree di accesso e le possibilità di modifica dei dati e infine suddividendo gli utenti in gruppi caratterizzati dagli stessi "permessi".

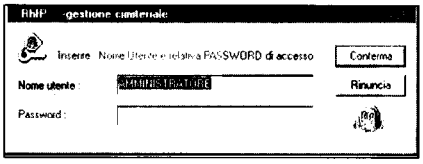

Figura 5 - Anche la tipologia e il numero di gruppi di utenti sono pienamente personalizzabili, sulla base delle esigenze di ogni amministrazione.

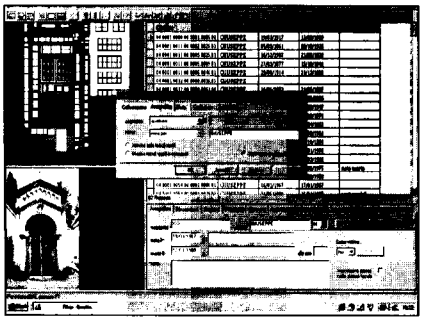

Figura 6 - Sull'anagrafica è possibile operare vari tipi di ricerca, anche a dati incrociati come in questo caso.

stessa filosofia di progetto; in Nuova Antigone 1/97 si erano infatti introdotti i cosiddetti GIS, "Geographical Information Systems", software che si fondano su un approccio visuale che trae avvio dalla rappresentazione del territorio attraverso una mappa sulla quale si può "cliccare" per accedere alle informazioni.

Interfaccia "visuale"

RhIP è la pratica realizzazione dell'idea precedente: un vero e proprio "GIS" dedicato ai cimiteri, tanto che il primo impatto con il sistema viene definito dagli stessi progettisti "di carattere informativo-geografico": partendo dal "generale" (come potrebbe essere una cartina stradale, figura 1) si può arrivare sino al "particolare" (la foto del loculo, figura 2). Il tutto a portata di "click" del mouse: dalle immagini è possibile risalire ad anagrafiche, contratti per luci, contratti di concessione. Viceversa, dalle anagrafiche e dai contratti, si può immediatamente risalire all'immagine che rappresenta il luogo di cui sono oggetto.

Utilizzo in multiutenza

RhIP, che nel 1997 può vantare dodici installazioni della quale la maggiore è quella del cimitero del comune di Grottammare (1.300 immagini e 12.000 postazioni), è studiato per essere utilizzabile in multiutenza salvaguardando i requisiti di riservatezza: l'accesso ai moduli che costituiscono il programma (che viene sempre commercializzato in versione "completa") è infatti protetto da password, con diversi livelli di permessi personalizzabili a piacere con grande flessibilità (figure 3, 4 e 5). L'utilizzo di livelli di accesso modulati sulla tipologia di utenza ha positive conseguenze anche qualora si faccia uso di un solo personal computer; si pensi, infatti, ad un unico calcolatore sul quale si trovino a dover lavorare diversi addetti in tempi diversi: ciascuno di essi sarà univocamente identificato da un'accoppiata "user-password" che gli conferirà una "visibilità" e una capacità di modifica degli archivi mirata alle effettive competenze e responsabilità.

Un pacchetto completo

L'approccio "visuale" nulla toglie alla completezza del prodotto, che è in grado di coprire tutte le tipi-

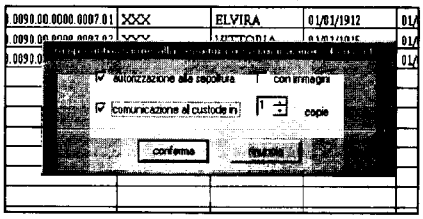

Figura 7 - Un ingrandimento della maschera di stampa dell'autorizzazione alla sepoltura o comunicazione al custode.

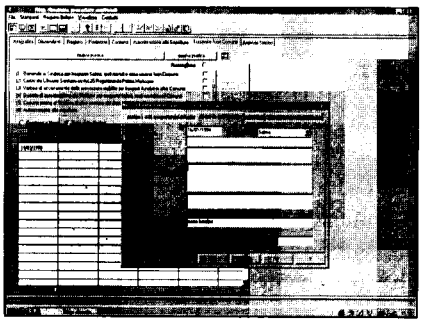

Figura 8 - La maschera di dialogo tramite la quale è possibile aprire nuove pratiche di trasporto delle salme fuori comune.

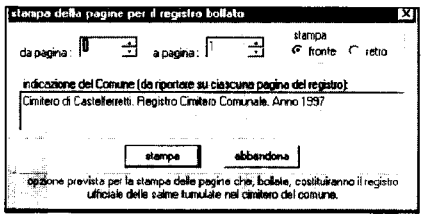

Figura 9 - Uno "zoom" sulla maschera di stampa delle pagine per il registro delle sepolture.

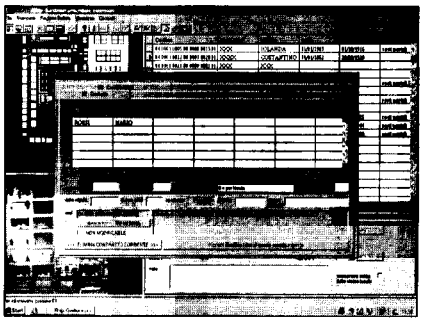

Figura 10 - La complessa finestra di gestione contratti per aree e loculi...

che esigenze di gestione di un cimitero, dall'anagrafica dei defunti alla stampa diretta dei bollettini di conto corrente postale per il pagamento delle luci votive. La singolarità è costituita dal fatto che tutti i diversi moduli di gestione che compongono il pacchetto software RhIP sono "legati a doppio filo - come afferma la brochure di presentazione - alla collocazione geografica del luogo oggetto del contratto": in molti casi è possibile, ad esempio, introdurre i dati "trascinando" col mouse le rappresentazioni fotografiche corrispondenti.

Anagrafica defunti

Cosa ciò voglia dire è facilmente desumibile da alcune videate: ad esempio, nella figura 6, dove è stata generata una lista di dati anagrafici sulla base di una selezione "tradizionale" per nome, cognome e data, è possibile restringere ulteriormente la ricerca "cliccando" sulle immagini a sinistra. Esiste, cioè, una integrazione pressoché totale fra testo e grafica (laddove quest'ultima è invece spesso un "surplus" informativo a corredo che non consente interazione diretta).

E' ovviamente possibile produrre

la modulistica in ossequio alle normative di legge e alle regole di organizzazione interna: ad esempio l'autorizzazione alla sepoltura, un documento da inviare all'operatore addetto alla tumulazione (con la possibilità di stampare anche l'immagine in pianta e la fotografia per evitare equivoci, figura 7), pratiche di trasporto fuori comune (figura 8), il registro delle sepolture di cui all'art. 52 del DPR 285/90 (figura 9).

Gestione dei contratti di concessione

Avviene attraverso la scheda "contratti", composta da cinque diverse pagine. E' così possibile: gestire sia i concessionari (dalla loro prima introduzione alla creazione e visualizzazione dei contratti a questi associati, figura 10) che i dati del comune; caricare le informazioni che concorrono alla stipula del contratto (figura 11), le cui tipologie sono totalmente personalizzabili a cura dell'utente; deciderne la stampa (disegnando anche le righe dell'"uso bollo", se richiesto) e, infine, selezionare i contratti in base a repertorio, tipo, data scadenza e col-

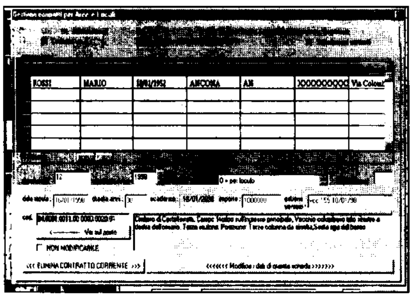

Figura 11 - ...consente di caricare tutte le informazioni che concorrono alla stipula del contratto.

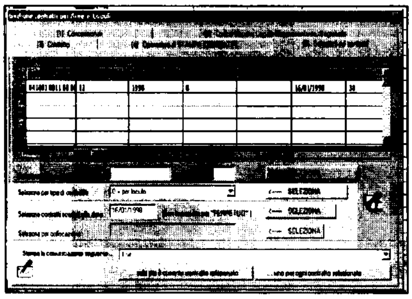

Figura 12 - Uno "zoom" sulla pagina di selezione dei contratti in base a repertorio, tipo, data scadenza e collocazione.

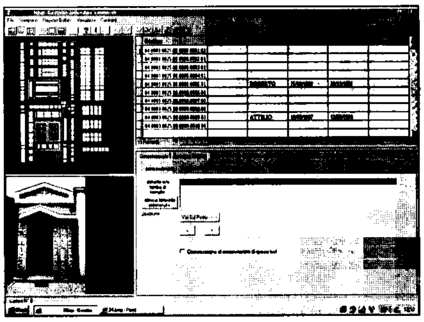

Figura 13 - La gestione delle lampade votive è sofisticata e consente di raggruppare tutte le luci di cui deve farsi carico un determinato utente.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Questo è un primo esempio di documento "firmato"
-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 5.0i for non-commercial use
Charset: noconv

[illegible]
[illegible]
=ecs2
-----END PGP SIGNATURE-----
```

Figura 14 - Un messaggio "firmato" elettronicamente tramite PGP (Pretty Good Privacy), il programma di crittografia a chiave pubblica (gratuito per uso personale) più diffuso al mondo.

locazione per poi compilare una qualsiasi comunicazione da inviare, eventualmente, al concessionario (figura 12).

Luci votive

La finestra "luci votive" si compone di sette pagine: concessionari, recapito bolletta (ad un'anagrafica o, in alternativa, al concessionario), luci in esercizio, che raggruppa tutte le luci di cui deve farsi carico un determinato utente (figura 13), competenze (con il riepilogo annuale di luci, importi, imposte e arrotondamenti), definizione competenze, operazioni (compilazione ruoli dei concessionari caricati) ed infine "reports" (con la scelta fra otto tipi di stampa, tra cui i ruoli insoluti e i solleciti).

Costi

Data la natura "visuale" e "geografica" di questo software, è difficile scinderne il costo intrinseco (5.200.000 Lit. più Iva per la licenza d'uso che viene automaticamente estesa - senza addebito ulteriore - a tutte le installazioni che si ritengano necessarie nell'ambito del comune; tale costo comprende l'installazione sulla prima macchina e un giorno di corso) da quello dell'irrinunciabile rilievo, indispensabile per costruire quella "mappa" del cimitero che costituisce il vero fulcro del programma. Tale servizio di rilievo viene anch'esso offerto dallo Studio Presta ma è quantificabile solo dopo sopralluogo nell'area cimiteriale. Esistono inoltre due opzioni: il programma può essere fornito "chiavi in mano" (dunque completo dei dati anagrafici delle salme) o, invece, con posizioni "vuote", senza anagrafica. Il contratto di assistenza (pari a 800.000 Lit. più Iva per anno) non è obbligatorio e comprende anche backup telefonici trimestrali e ampliamenti delle piante purché inferiori a 500 loculi (con contributo di 200.000 Lit. più Iva per ogni misurazione o rilievo fotografico entro un raggio di 150 Km da Ancona e 600 Lit. + Iva di rimborso chilometrico oltre 150 Km).

Per ulteriori informazioni su RhIP contattare:

Studio Presta
Progettazione Software

Via Ranieri, 53 - 60131 ANCONA
Telefono e fax: 071-28.10.489

e-mail presta@genan.it

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Questo è un secondo esempio di documento "firmato": si noti che cambia
anche la firma!
-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 5.0i for non-commercial use
Charset: noconv

[illegible]
[illegible]
=Q6Qe
-----END PGP SIGNATURE-----
```

Figura 15 - Un diverso messaggio firmato dallo stesso utente: si noti che la "firma" è significativamente diversa, pur riferendosi ad un documento realizzato dalla stessa persona. Se così non fosse, infatti, la contraffazione sarebbe facilissima.

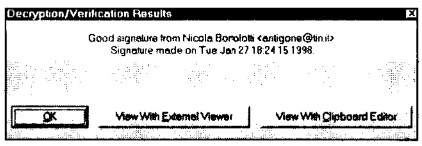

Figura 16 - Il "box" con il quale PGP comunica di aver validato con successo un documento "firmato".

Tratto da Nuova Antigone 1/98

COMINCIAMO A PARLARE DI FIRMA ELETTRONICA

di Nicola Bortolotti

Con questo numero prende l'avvio una breve panoramica sulla cosiddetta "firma elettronica": un argomento di grande attualità, dopo che anche la legge italiana, nell'agosto scorso, ne ha di fatto iniziato a sancire la "dignità" giuridica, cominciando (seppur faticosamente) a dare attuazione all'articolo 15 della legge Bassanini.

Vent'anni dopo

Le radici della firma elettronica vedono in realtà la luce oltre vent'anni fa, da un lavoro di Diffie e Hellman datato 1976. "Crittografia a chiave pubblica", è questa la "madre" dell'autenticazione a prova di frode: un metodo di cifratura (ossia un sistema di protezione da occhi indiscreti) che, come possibilità collaterale, alternativa od ulteriore, ha quella di poter "firmare" digitalmente il documento.

Sicurezza

Nel sentir parlare di "firma elettronica" è naturale essere pervasi da una innata diffidenza. Eppure la crittografia a chiave pubblica, in questa sua ormai primaria applicazione, offre garanzie ben maggiori di una qualsiasi firma apposta con la penna su di un assegno. Non si tratta infatti di una ovvia e banale digitalizzazione dell'immagine della propria firma (metodica ormai comune tra coloro che inviano Fax direttamente tramite computer) ma di qualcosa di estremamente più sofisticato e virtualmente inattaccabile.

Firma variabile

Innanzitutto cominciamo col dire che la firma elettronica non è una firma "invariabile", ossia la sua autenticità non deriva dal fatto che sia "identica" o "simile" ad un "campione", come quello depositato in banca o presso il notaio. Cosa c'è infatti di più facilmente copiabile in maniera esatta di un documento in forma elettronica? E dunque: cosa potrebbe essere più facilmente contraffatto di una "signature", ossia di una firma in forma di bytes, che fosse sempre identica a se stessa? Il primo "trucco", se così si può dire, è dunque costituito dal fatto che la serie di caratteri con la quale viene firmato il documento digitale è funzione del documento stesso: diverso sarà il documento, diversa sarà la "firma" (figure 14 e 15). La modalità per generare la firma a partire dal documento sarà standard, un algoritmo universalmente conosciuto ed adottato, tutt'altro che segreto.

Chiave privata

La segretezza risiede invece in una parte della chiave, detta "privata", che viene utilizzata dalla procedura che genera la firma. L'algoritmo, cioè, genererà la firma a partire sia dal documento che dalla chiave privata e la aggiungerà in calce al testo. E' importante sottolineare che la chiave privata è caratteristica e deve essere conosciuta e utilizzata solo dal suo legittimo proprietario. In pratica è come un timbro, un sigillo di autenticità assolutamente personale e che deve essere custodito con la massima cura e riservatezza. Da un punto di vista "tradizionale", la vera e propria "firma" (o, ancora meglio, la "mano che firma") è la chiave privata!

Chiave pubblica

Una volta generato il documento "firmato", esso può venire trasmesso e diffuso. Il destinatario dovrà risolvere il problema di stabilire se tale insieme di byte è autentico oppure no. Per "validare" il documento egli lo sottoporrà a un algoritmo che, a partire dal "testo", dalla "firma" e da un "modello della firma" (che si sa appartenere al probabile autore del testo) ne possa stabilire l'autenticità (figura 16). Si noti che non è possibile confrontare solo la "firma" col "modello della firma" poiché si è detto che la firma è funzione anche del "testo" ed è proprio questo che la rende "non copiabile".

Ciò che abbiamo definito "modello della firma" è la chiave pubblica. Chiave privata e chiave pubblica costituiscono un binomio inscindibile e caratteristico di un determinato "firmatario" ma, come si suol dire, asimmetrico: ciò vuol dire che, mentre con la chiave privata si può "firmare" un documento, questo non è possibile farlo con la chiave pubblica (o, meglio, porterebbe a documenti con firma irregolare). Questo implica il fatto che diffondere il proprio "modello della firma" non porta alcun pericolo, perché questo "modello" è del tutto inutilizzabile ai fini della firma; è proprio questo il secondo e fondamentale "trucco"!

Ancora sulla sicurezza

Tutto quanto esposto ha significato a patto che sia impossibile risalire alla chiave privata conoscendo quella pubblica e un testo "firmato". La matematica non garantisce in assoluto che questo sia impossibile ma, de facto, scoraggia ogni tentativo fraudolento. Mentre costruire una chiave (costituita dalla coppia pubblica - privata) è infatti un'operazione assai rapida, il tentativo di ricostruire la chiave privata a partire da quella pubblica - unitamente ad una firma e al documento associato - appartiene a quei problemi di elevata complessità computazionale che richiedono decenni di lavoro anche ai più veloci calcolatori elettronici oggi esistenti. Qualora la potenza dei computers aumentasse, sarebbe poi sufficiente aumentare la lunghezza della chiave. Perché la coppia di chiavi generate sia virtualmente "impenetrabile", essa deve essere generata tramite opportuni algoritmi, il più famoso dei quali è stato denominato RSA (dalle iniziali degli inventori Rivest, Shamir e Adleman, 1978) mentre uno dei più recenti (1994) DSS.

Rimane aperta una questione, che sarà trattata nel prossimo numero e che costituisce la parte nodale del regolamento di attuazione della legge Bassanini: chi assicura che un "modello di firma" (chiave pubblica) sia stato effettivamente generato dall'individuo che si dice essere? In parole tradizionali: chi fa le veci della "carta d'identità" e dell'autorità che la rilascia?