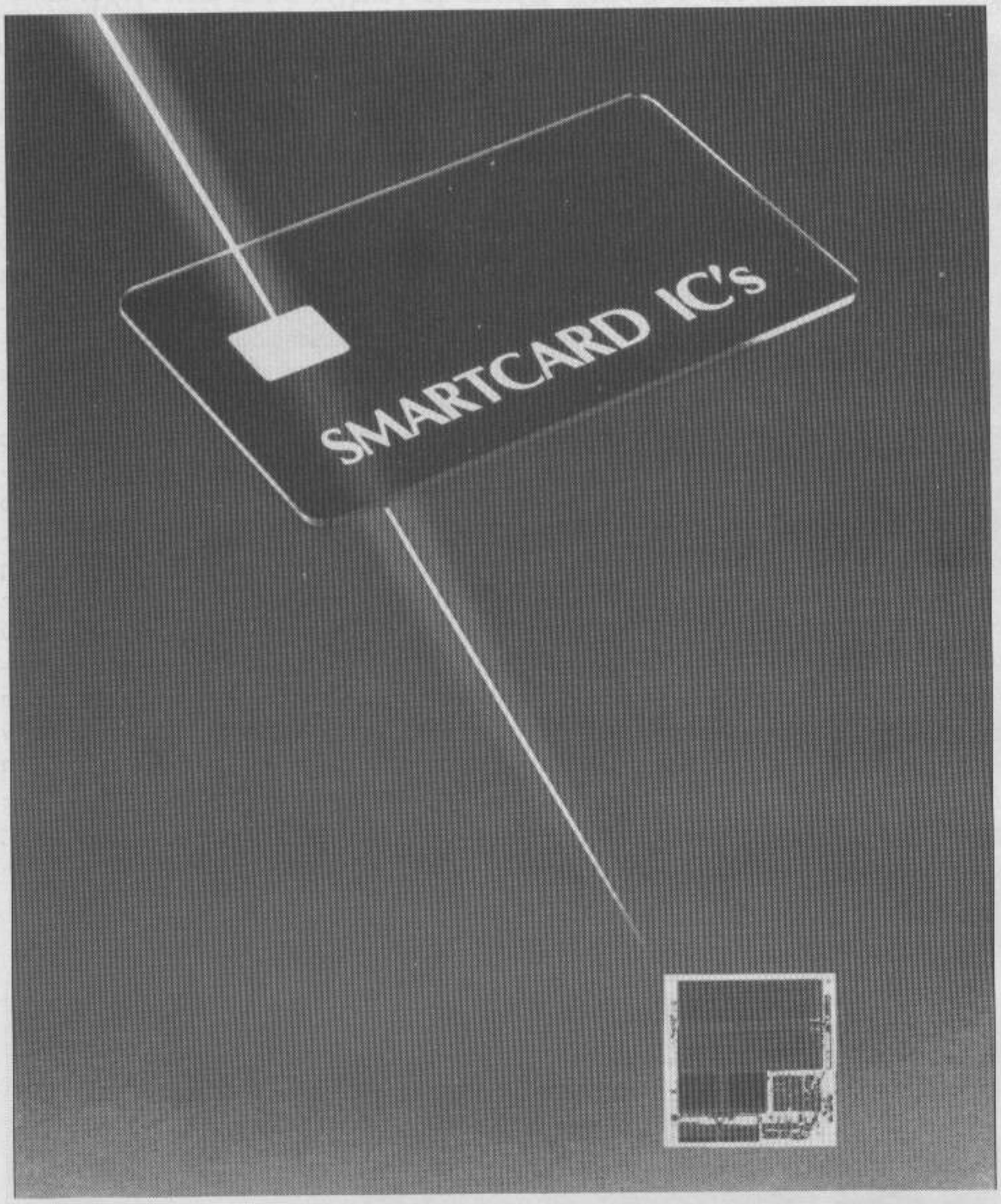
Κάρτες με ολοκληρωμένο



Οι κάρτες με ολοκληρωμένο είναι πλαστικές κάρτες που περιλαμβάνουν ένα πλήρες υπολογιστικό σύστημα ή απλώς μνήμες εγγραφής/ ανάγνωσης. Λόγω της μεγάλης ολοκλήρωσης, το ημιαγωγό υλικό που περιλαμβάνουν έχει συρρικνωθεί σε τέτοιο σημείο, ώστε οι διαστάσεις τους να μην ξεπερνούν εκείνες των πιστωτικών καρτών, που χρησιμοποιούνται σήμερα στις τραπεζικές συναλλαγές. Το άρθρο που ακολουθεί αποβλέπει στο να δώσει περισσότερες πληροφορίες για τους τρόπους κατασκευής και λειτουργίας τους.

Οι κάρτες ημιαγωγών ή κάρτες με ολοκληρωμένο, γνωστές από την πληθώρα των εφαρμογών και των ευκολιών που παρέχουν, πρωτοεμφανίστηκαν στην αγορά στα μέσα της δεκαετίας του 1970. Σήμερα χρησιμοποιούνται σε όλο και περισσότερες εφαρμογές, από τις οποίες η πιο γνωστή είναι η χρήση τους στους τηλεφωνικούς θαλάμους. Ταυτόχρονα εξακολουθούν να αποτελούν το ιδανικότερο μέσον για την αναγνώριση της ταυτότητας προσώπων που διακινούνται σε φυλασσόμενες περιοχές, ενώ δεν είναι σπάνιες και οι περιπτώσεις που με τη βοήθεια τέτοιου είδους καρτών πραγματοποιείται η μέτρηση των ωρών εργασίας του προσωπικού μεγάλων βιομηχανικών μονάδων ή συγκροτημάτων γραφείων. Φυσικά η παρουσία τους αρχίζει να αποτελεί μια όλο και πιο συνηθισμένη πραγματικότητα στις χρηματοοικονομικές συναλλαγές, εκεί που οι πληρωμές "τοις μετρητοίς" γίνονται χωρίς να διακινούνται χαρτονομίσματα. Ας αφήσουμε όμως για λίγο το παρόν. Στο άμεσο μέλλον, η δημιουργία ενός παγκόσμιου προτύπου που θα αφορά τα χαρακτηριστικά και τις χρήσεις των καρτών αυτών, αναμένεται να δώσει μια ισχυρή ώθηση σε εφαρμογές που μέχρι τώρα παραμένουν άγνωστες. Σ' αυτό θα συντελέσει φυσικά και η μείωση του κόστους παραγωγής τους, που είναι άμεσα συνυφασμένη με τον αριθμό των καρτών που παράγονται από τα εργοστάσια. Η κατασκευή, ακόμα, μιας "μικτής" κάρτας που θα είναι ταυτόχρονα και κάρτα ημιαγωγού και μαγνητική, είναι κάτι που θα συντελέσει θετικά στη διάδοση των καρτών σαν μέσου καθημερινής συναλλαγής. Η χρήση των καρτών ημιαγωγού αφορά την αναγνώριση των δικαιούχων κατόχων τους, ή στις περιπτώσεις των μη προσωπικών καρτών, την παροχή στον κομιστή τους υπηρεσιών και παροχών, το ύψος των οποίων καθορίζεται από την "τιμή" της κάρτας. Λαμβάνοντας υπόψη όλες τις παραπάνω δυνατότητες, εύκολα προκύπτει ότι οι κάρτες ημιαγωγού είναι οι αδιαφιλονίκητοι διάδοχοι των "εύκαμπτων φίλων" μας, των καρτών με τη μαγνητική λωρίδα, που εκδίδονται από τις τράπεζες ή τους πιστωτικούς οργανισμούς. Τα ιδιαίτερα χαρακτηριστικά των καρτών ημιαγωγού, όσον αφορά τις διαστάσεις τους και την ηλεκτρική συμπεριφορά τους, έχουν τυποποιηθεί σύμφωνα με το πρότυπο ISO 7816.

Κάρτα με ολοκληρωμένο

Η ευρύτερη ονομασία "κάρτα ημιαγωγού" χρησιμοποιείται σήμερα για να προσδιορίσει τα παρακάτω προϊόντα:

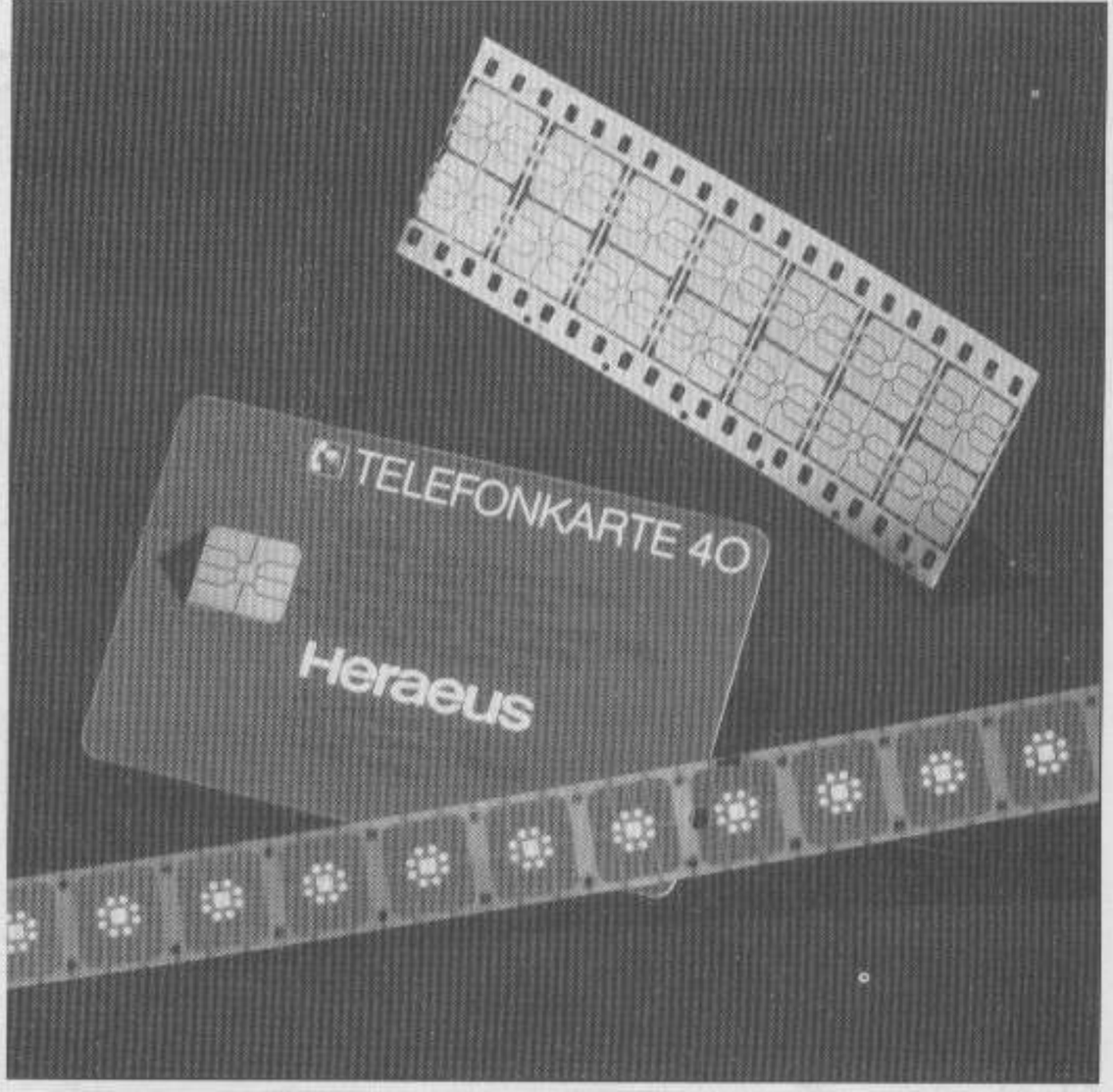
- Έξυπνες κάρτες
- Κάρτες μνήμης
- Κάρτες επεξεργαστή
- Ευφυείς κάρτες
- Κάρτες IC

Τα διαφορετικά ονόματα που σημειώσαμε παραπάνω υπονοούν από μόνα τους τις διαφορές μεταξύ των καρτών σ' ότι αφορά την εσωτερική κατασκευή και τις λειτουργίες που επιτελούν. Σύμφωνα με το πρότυπο ISO 7816 το όνομα "Κάρτες IC" πρέπει να χρησιμοποιείται για να δηλώνει όλα τα μέλη της οικογένειας των καρτών ημιαγωγού. Οι κάρτες με τη μαγνητική λωρίδα που χαρακτηρίζονται από την παθητική λειτουργία τους και τη μικρή τους μνήμη (342 byte) εύκολα μπο-

ρούν να διαβαστούν, να αντιγραφτούν και να παραποιηθούν. Αντίθετα οι κάρτες ημιαγωγού, εξ' αιτίας της μεγάλης χωρητικότητάς τους (μέχρι 32 Kbyte μνήμη), των ευφυών κυκλωμάτων που χρησιμοποιούν και των απαραίτητων κωδικών πρόσβασης που απαιτούν, προσφέρουν πολύ μεγαλύτερη ασφάλεια έναντι οποιασδήποτε μη νόμιμης χρήσης. Ακόμα έχουν σχετικά μικρό κόστος παραγωγής, γεγονός που τις κάνει περισσότερο ανταγωνιστικές σε σχέση με τις μαγνητικές.

Παραγωγή

Μια κάρτα ημιαγωγού έχει διαστάσεις 85,6 x 54 x 0,76 mm
, ίδιες δηλαδή, μ' αυτές μιας πιστωτικής κάρτας. Για τις ανάγκες της κινητής τηλεφωνίας, ή άλλων εφαρμογών όπου οι διαθέσιμοι χώροι είναι ακόμα πιο περιορισμένοι, διατίθενται κάρτες με πολύ μικρότερες διαστάσεις. Σαν τυπικό παράδειγμα μπορούμε να αναφέρουμε τις Plug In SIMM, που έχουν διαστάσεις μόλις 18 x 28 x 0,76 mm^3. Η φέτα του ημιαγωγού υλικού, αυτή καθ' αυτή, έχει διαστάσεις 10 x 10 mm2 και εμπεριέχεται στο εσωτερικό ενός πλαστικού φορέα. Λόγω του ότι η κάρτα πρέπει να είναι εύκαμπτη, αλλά και για πολλούς άλλους λόγους, ο φορέας "επιπλέει" μέσα στη κάρτα. Το υλικό εκείνο που αποτελεί τον φορέα του ημιαγωγού υλικού, κατασκευάζεται επικαλύπτοντας και τις δύο όψεις ενός μη αγώγιμου φύλλου με μια λεπτή επίστρωση χαλκού. Κατόπιν με τη βοήθεια μεθόδων ίδιων μ' αυτών που ακολουθούνται για την αποχάλκωση των πλακετών τυπωμένου κυκλώματος, σχηματίζονται οι επαφές (σχ. 1). Πάνω σ' αυτό το "σάντουιτς" τοποθετείται ένα εξισωτικό φύλλο από το οποίο έχει αφαιρεθεί το κομμάτι εκείνο που βρίσκεται πάνω από τις επαφές. Το ημιαγωγό υλικό στερεώνεται στο φύλλο με τη βοήθεια μίας κόλλας σιλικόνης με το αγώγιμο υλικό κατόπιν όλο σκεπάζεται από ένα ακόμα φύλλο. Η οπίσθια πλευρά του αγώγιμου φύλλου περιλαμβάνει τις επαφές (φαίνονται σε μορφή τρυπημένης ταινίας στο κάτω μέρος του σχ. 1), οι οποίες μετά τη λήξη της επεξεργασίας θα επιτρέψουν τη διασύνδεση της κάρτας με τον εξωτερικό κόσμο. Ένα ακόμα φύλλο, που έχει ανοίγματα μεγέθους ίσου μ' αυτό των επαφών, στερεώνεται από την πλευρά του αγώγιμου φύλλου που φιλοξενεί τις επαφές. Το τελικό προϊόν αποκόπτεται από την ταινία και τοποθετείται στην κάρτα η οποία κατασκευάζεται από αρκετά στρώματα φύλλων PVC. Αυτά κάνουν την κάρτα ανθεκτική στις υψηλές θερμοκρασίες, στα υψηλά ποσοστά υγρασίας και στη διαβρωτική δράση αρκετών χημικών προϊόντων. Παρόλα αυτά η άμεση έκθεση της κάρτας σε πηγές θερμότητας, η παρουσία ηλεκτρικού θορύβου (ESD) στις επαφές του ημιαγωγού υλικού, όπως επίσης και η υπερβολική μηχανική καταπόνηση (λύγισμα, τέντωμα κ.λπ.), πρέπει να αποφεύγονται.

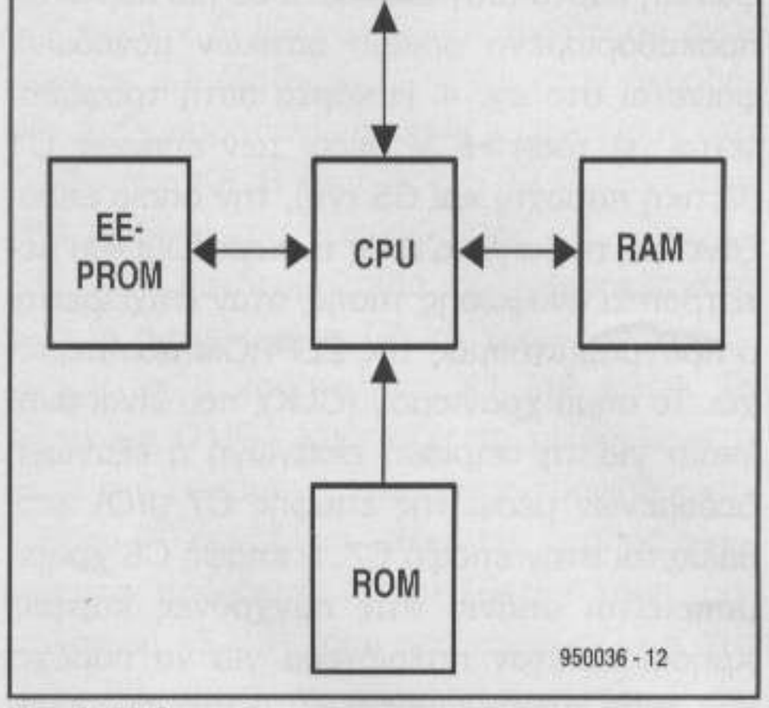


Σχ. 1. Δομικές βαθμίδες μιας κάρτας ημιαγωγού. Σε πρώτο πλάνο φαίνεται το μέρος της κάρτας που φέρει τον αποχαλκωμένο φορέα του ημιαγωγού, στο μέσον βλέπουμε μια (όχι τελειωμένη) κάρτα και στο βάθος της εικόνας, μία ταινία με φορείς.

Γενικό διάγραμμα

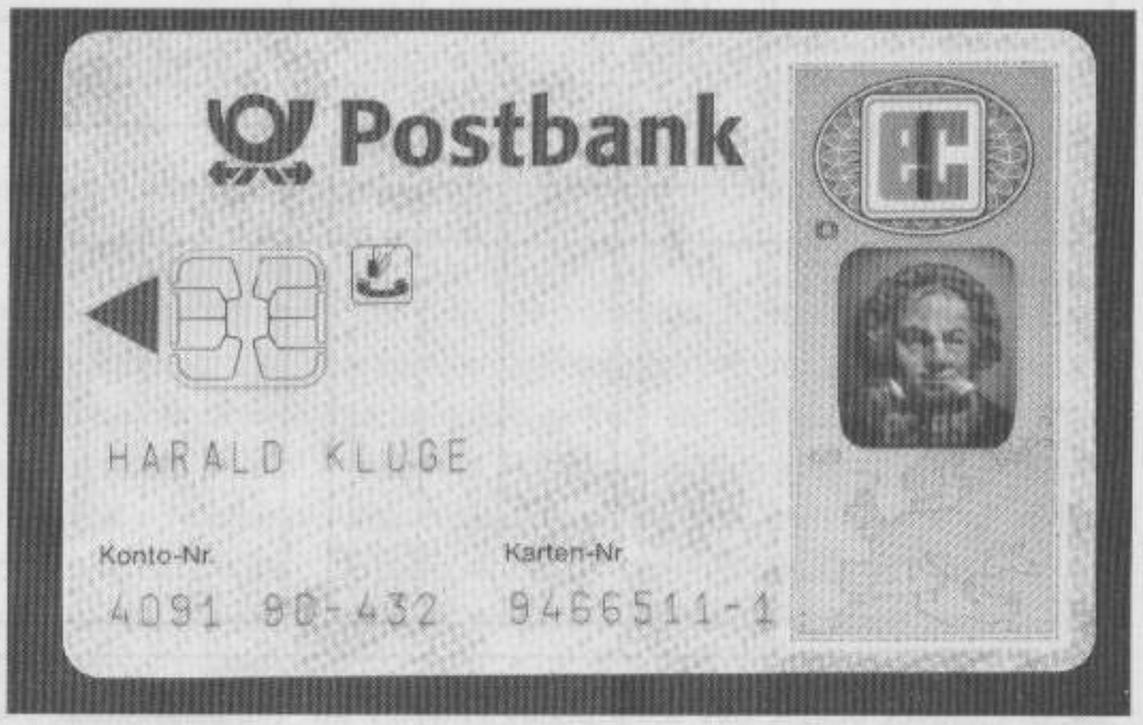
Τα βασικά μέρη από τα οποία αποτελείται μια κάρτα φαίνονται στο σχ. 2. Αυτά είναι:
- Ο μικροελεγκτής (CPU)
- Η μνήμη προσωρινής αποθήκευσης δεδομένων (RAM)
- Η μνήμη προγράμματος (ROM)
- Η μνήμη δεδομένων (EPROM ή EEPROM)
- Η βαθμίδα εισόδου / εξόδου (I/O)

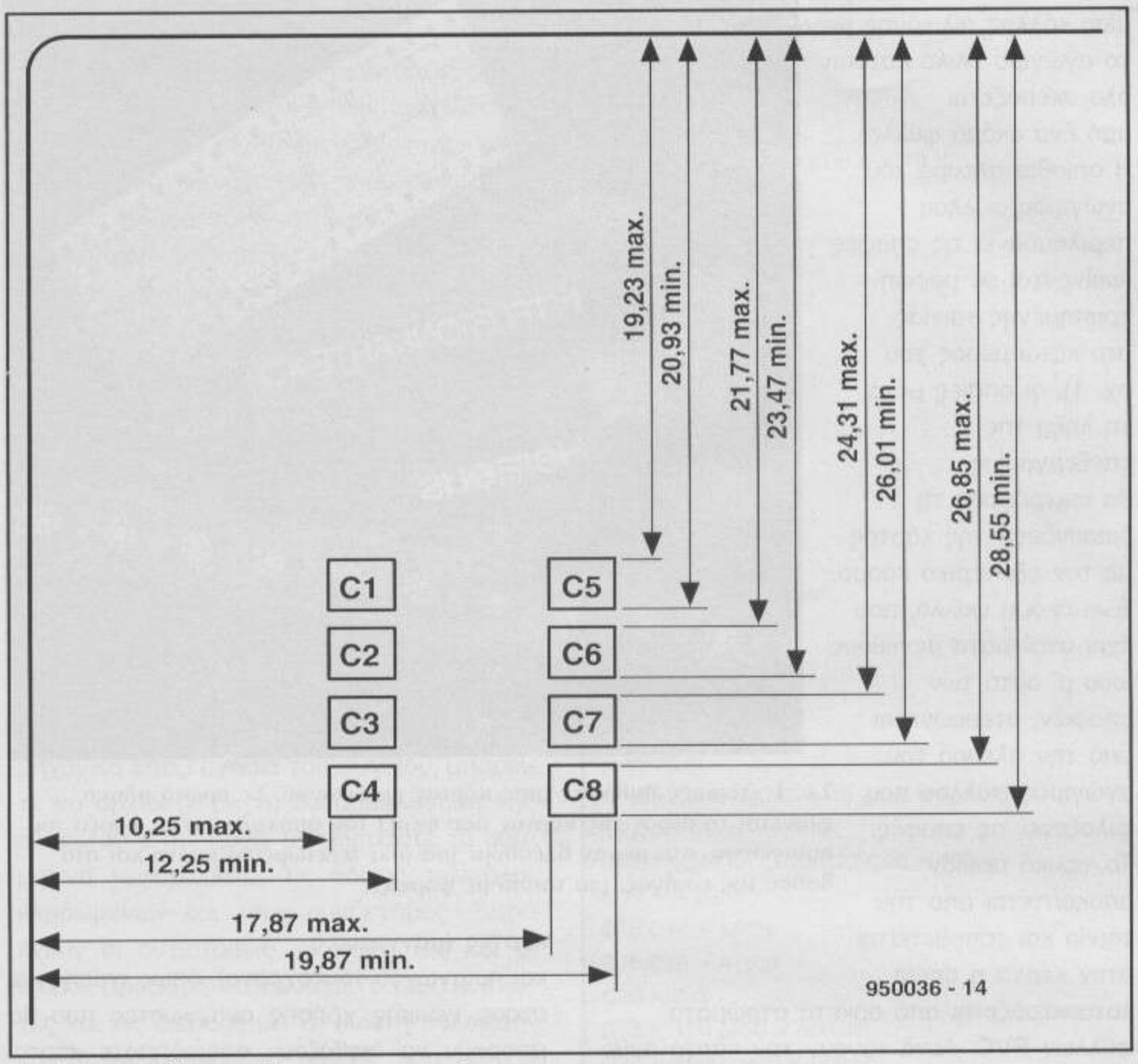
Ανάλογα με την εφαρμογή, είναι πολύ πιθανό μια κάρτα μνήμης να είναι περισσότερο κατάλληλη από μια κάρτα με επεξεργαστή. Στο άμεσο μέλλον όμως, προβλέπεται ότι το ενδιαφέρον των κατασκευαστών θα στραφεί στις "μικτές" κάρτες (μαγνητικές και ημιαγωγού ταυτόχρονα), όπως επίσης και στους γενικής χρήσης αναγνώστες που θα μπορούν να διαβάζουν οποιαδήποτε κάρτα. Ήδη δύο από τους μεγαλύτερους διεθνείς οργανισμούς παροχής υπηρεσιών πιστωτικών καρτών, οι VISA και Eurocard, προμηθεύουν τους πελάτες τους με "μικτές" κάρτες. Μέσω αυτών θα μπορούν να κάνουν τις αγορές τους με το συνηθισμένο τρόπο, κάνοντας χρήση της μαγνητικής λωρίδας, όπως επίσης και για να πραγματοποιούν τηλεφωνικές συνδιαλέξεις από ειδικά κατασκευασμένους τηλεφωνικούς θαλάμους με άμεση χρέωση του τραπεζικού λογαριασμού τους. Η τελευταία δυνατότητα των καρτών αυτών έχει ωθήσει τους τηλεπικοινωνιακούς οργανισμούς αρκετών



Σχ. 2. Η βασική αρχιτεκτονική του υπολογιστικού συστήματος μιας κάρτας δε διαφέρει σε τίποτα από αυτήν ενός μικροελεγκτή

Φωτογρ. 3 Συνδιασμός μαγνητικής κάρτας και κάρτας ολοκληρωμένου σαν τραπεζικής, τηλεκάρτας και σαν κάρτα για Eurocheque

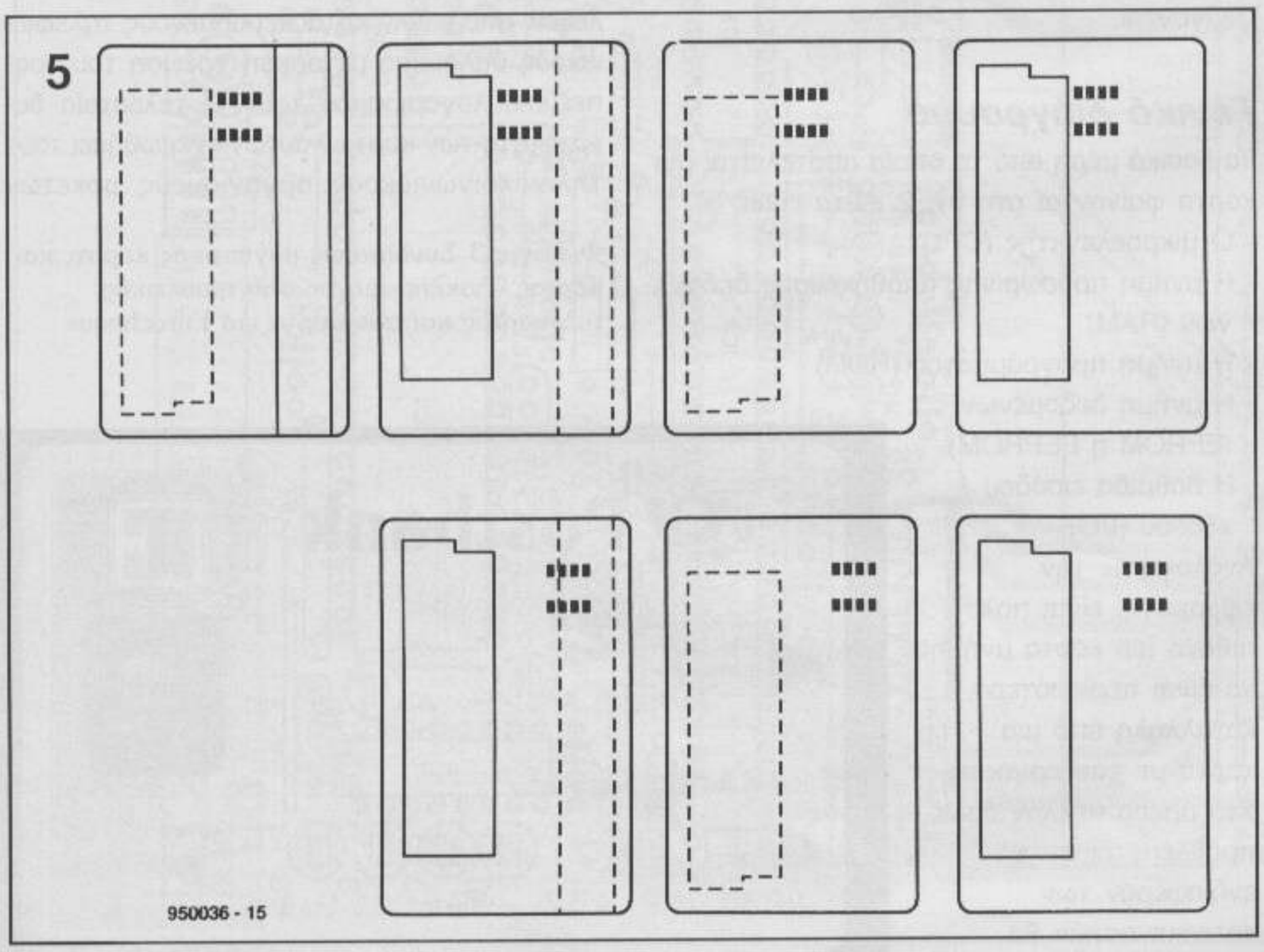




Σχ. 4. Η ακριβής τοποθέτηση των επαφών.

χωρών να τροποποιήσουν τις συσκευές των τηλεφωνικών θαλάμων τους, έτσι ώστε σύντομα να μπορούν να υποστηρίξουν τη νέα αυτή γενιά καρτών.

Η τυποποίηση του πρωτοκόλλου επικοινωνίας, σ' ότι αφορά την πρόσβαση και την τροποποίηση των στοιχείων μιας κάρτας, σε συνδυασμό με την ικανότητά τους να προσαρμόζονται σ' οποιοδήποτε νεότερο πρωτόκολλο προκύψει στο μέλλον, κάνει τις κάρτες



Σχ. 5. Πιθανές θέσεις των ηλεκτρικών επαφών και της μαγνητικής λωρίδας σε μια "μικτή" κάρτα.

με επεξεργαστή ιδανικές για εφαρμογές σε πρωτοποριακά συστήματα αποθήκευσης πληροφορίας που σύντομα αναμένεται να κατακλύσουν τη διεθνή αγορά.

Πρόσβαση

Πάνω σε κάθε μια κάρτα ημιαγωγού συναντάμε έξι έως οκτώ επιχρυσωμένες επαφές, που η κάθε μια έχει μια ενεργή επιφάνεια ίση με 1,7 x 2 mm2. Οι επαφές αυτές μπορούν να βρίσκονται σε μια από τίς δύο δυνατές θέσεις στην επιφάνεια της κάρτας. Το που θα βρίσκονται, εξαρτάται από το αν η κάρτα θα περιλαμβάνει την τυπική μαγνητική λωρίδα των πιστωτικών καρτών και φυσικά από τη θέση των διαφόρων λογότυπων που θα είναι τυπωμένα πάνω σ' αυτήν. Οι συσκευές ανάγωσης των καρτών, που είναι γνωστοί και με το όνομα τερματικά καρτών, διατίθενται ήδη σε μια μεγάλη ποικιλία παραλλαγών. Ξεκινώντας από το πιο απλό μοντέλο, που βασίζει τη λειτουργία του σε επαφές με ελατήρια, εύκολα φθάνουμε στα πλέον βελτιωμένα, που δεν απαιτούν σχεδόν καμία δύναμη για την ώθηση της κάρτας μέσα στη σχισμή, αφού για τον εντοπισμό της κάρτας και την ενεργοποίηση των κυκλωμάτων τους χρησιμοποιούν τερματικούς διακόπτες. Το τελειότερο βέβαια μοντέλο ανάγνωσης καρτών έχει κατασκευαστεί σχετικά πρόσφατα και βασίζει τη λειτουργία του σ' ένα υβριδικό μηχανισμό, που μόλις ανιχνεύσει την παρουσία της κάρτας στη σχισμή, την εισάγει στο εσωτερικό του, ωθώντας την προς το σημείο εκείνο που βρίσκονται οι επαφές. Ακολούθως τη διαβάζει ή τη γράφει και μετά το πέρας της συναλλαγής, την επιστρέφει στον κάτοχό της μέσω της αντίθετης διαδρομής. Στο σχ. 7 βλέπουμε έναν απλό σύστημα ανάγνώσης καρτών εξοπλισμένο με ειδικούς ακροδέκτες για να μπορεί να "αγγίζει" τις επαφές της κάρτας. Οι τερματικοί διακόπτες που περιλαμβάνει, τον βοηθούν να τίθεται αυτόματα εντός και εκτός λειτουργίας. Η θέση που είναι τοποθετημένες οι επαφές πάνω σε μια τηλεφωνική κάρτα (συγκεκριμένα σε μια κάρτα με προκαθορισμένο αριθμό αστικών μονάδων), φαίνεται στο σχ. 4. Η κάρτα αυτή τροφοδοτείται με τάση +5 V, μέσω των επαφών C1 (θετική παροχή) και C5 (γη), την οποία επαυξάνει με τη βοήθεια ενός ενσωματωμένου μετατροπέα ανύψωσης τάσης, όταν επιχειρείται ο προγραμματισμός της EEPROM που περιέχει. Το σήμα χρονισμού (CLK), που είναι αναγκαίο για τη σειριακή εισαγωγή ή εξαγωγή δεδομένων μέσω της επαφής C7 (I/O), επιβάλλεται στην επαφή C3. Η επαφή C6 χρησιμοποιείται σπάνια στις σύγχρονες κάρτες. Χρησιμοποιόταν παλαιότερα για να παρέχει την τάση προγραμματισμού (VPP) των μνημών, μόλις αναγνωριζόταν η κάρτα από τα ειδικά, γι' αυτόν τον σκοπό, κυκλώματα της

Επαφή	Συμβολισμός	Επαφή	Συμβολισμός
C1	VCC (Supply Voltage)	C5	GND (Ground)
C2	RST (Reset)	C6	VPP (Programming Voltage)
C3	CLK (Clock Signal)	C7	I / O (Input/Output)
C4	Reserved	C8	Reserved

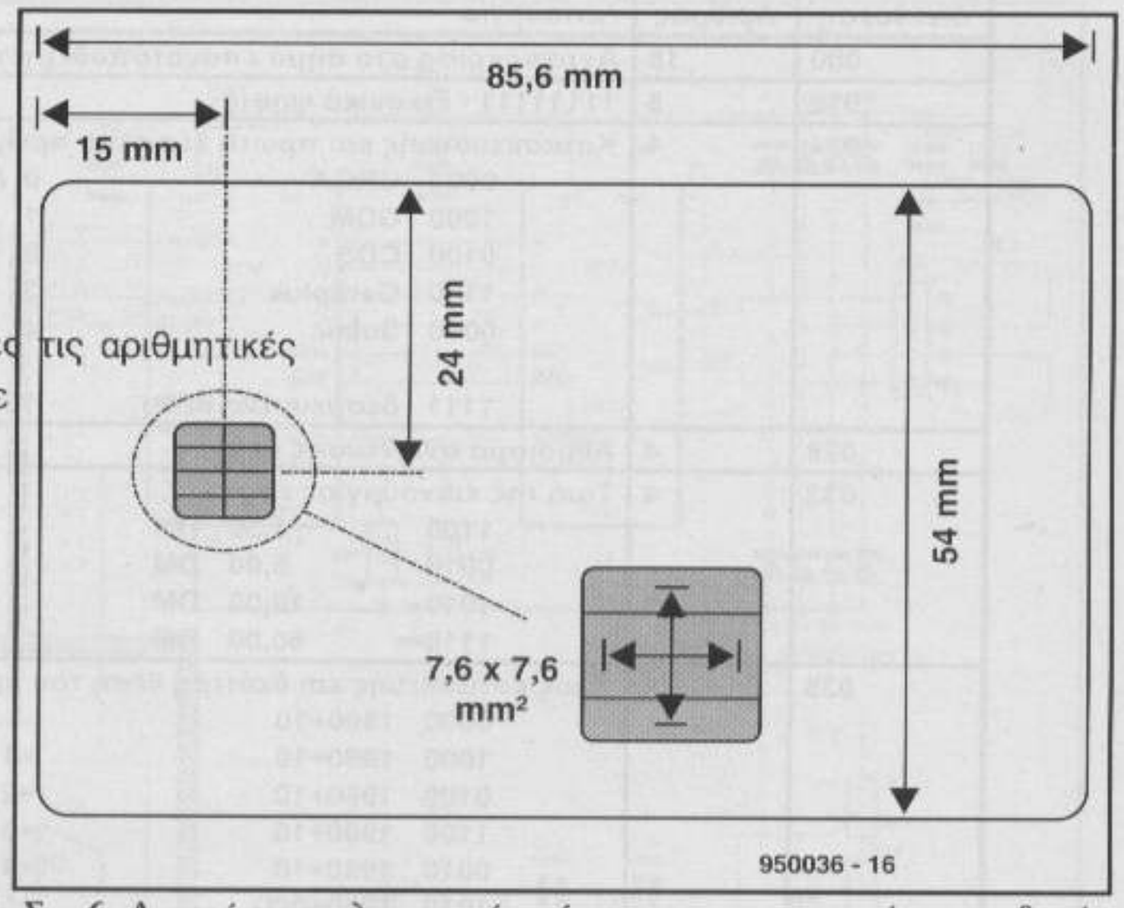
950036 - 18

Πίνακας 1. Σημασία των σημάτων που εμφανίζονται στις επαφές μιας κάρτας.

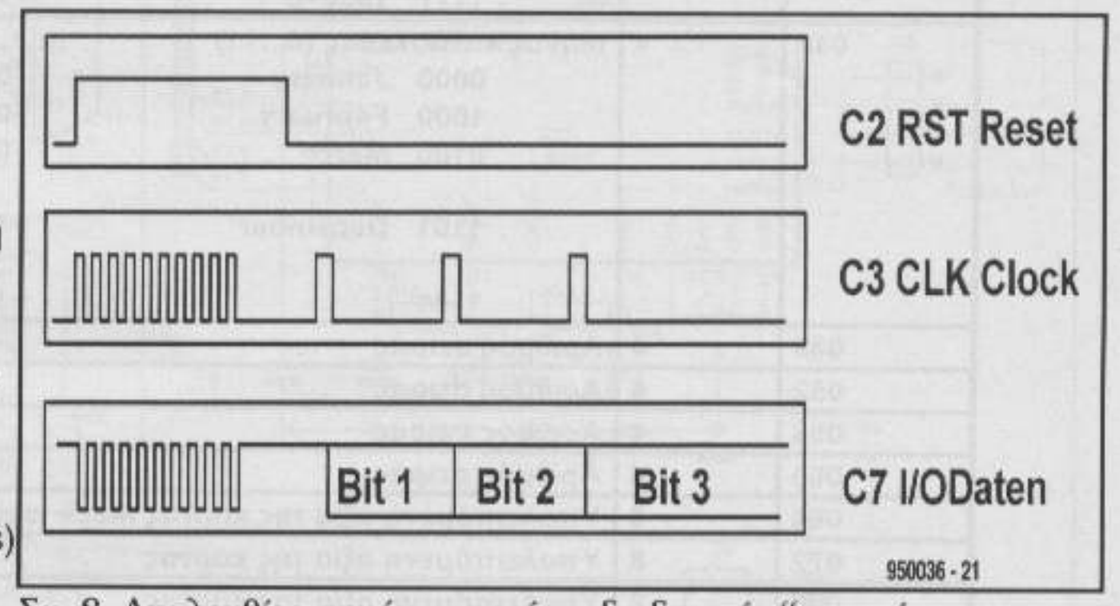
συσκευής ανάγνωσης. Μόνο μερικές πολύ παλιές κάρτες απαιτούν σήμερα αυτή την τάση. Οι λειτουργίες που επιτελούν οι επαφές C4 και C8 δεν έχουν καθοριστεί από το ήδη υπάρχον πρότυπο επικοινωνίας (είναι δεσμευμένες για μελλοντική χρήση), γι' αυτό και στις περισσότερες κάρτες δε χρησιμοποιούνται. Η επαφή C2 χρησιμεύει για να επιβάλλεται το σήμα επανατοποθέτησης στην κάρτα. Με τη βοήθεια του σήματος αυτού γίνεται δυνατή η αναγνώριση της κάρτας, αφού μετά από αυτό στέλνεται ο κωδικός - ταυτότητα της κάρτας σύμφωνα με το πρωτόκολλο που θα αναφερθεί παρακάτω.

Προγραμματισμός

Στον πίνακα 2 φαίνονται οι μεγαλύτεροι και περισσότερο γνωστοί κατασκευαστικοί οίκοι καρτών ημιαγωγού. Οι Philips και OKI έχουν προτιμήσει να χρησιμοποιήσουν υπολογιστικά κυκλώματα που είναι ήδη γνωστά και για τα οποία κυκλοφορούν ήδη πολλά αναπτυξιακά συστήματα. Τους ήδη υπάρχοντες πυρήνες τους, τους έχουν πλαισιώσει με αριθμητικούς επεξεργαστές ικανούς να επεξεργάζονται την ευαίσθητη, από πλευράς ασφάλειας, πληροφορία που εμπεριέχεται στην κάρτα. Οι επεξεργαστές αυτοί κάνουν χρήση ειδικών αλγορίθμων κωδικοποίησης όπως π.χ. του DES (Data Encryption Standard). Οι κάρτες ολοκληρωμένου έχουν εξαιρετικά μεγάλη αποθηκευτική ικανότητα. Μεγέθη μνήμης όπως 32 Kbytes EEPROM, 32 Kbytes ROM, μαζί με 512 bytes RAM, είναι αρκετά συνηθισμένα στις κάρτες που κυκλοφορούν σήμερα. Οι εκπληκτικά μεγάλες, για μια τόσο μικρή κάρτα, χωρητικότητες αποδεικνύεται ότι είναι αναγκαίες για την καλή λειτουργία της κάρτας, αφού επιταχύνουν όλες τις αριθμητικές πράξεις που σχετίζονται με την απόκρυψη ή την κωδικοποίηση των χρήσιμων στοιχείων. Θα μπορούσαν μάλιστα να θεωρηθούν και καθοριστικές, αν σκεφθούμε ότι για την κωδικοποίηση ενός τμήματος πληροφορίας μήκους 64 byte, χρησιμοποιούνται επαναληπτικοί κώδικες με βάθος ίσο με 32 bit. Η μεγάλη χωρητικότητα της μνήμης ROM είναι και αυτή απαραίτητη για την αποθήκευση του προγράμματος λειτουργίας της κάρτας, για τη συγκρότηση πινάκων αντιστοιχιών (look up tables) ή για τη φύλαξη των ακολουθιών των bit που χρησιμεύουν για την απόκρυψη της πληροφορίας.



Σχ. 6. Διαστάσεις τηλεφωνικής κάρτας και συγκεκριμένου αριθμού μονάδων.



Σχ. 8. Ακολουθίες σημάτων κατά τη διαδικασία "ανταπόκρισης στο σήμα επανατοποθέτησης".

Η μνήμη EEPROM δε χρησιμοποιείται σχεδόν καθόλου από τις σημερινές κάρτες. Η χωρητικότητάς της είναι δεσμευμένη, έτσι ώστε στο μέλλον η ίδια κάρτα να μπορεί να χρησιμοποιηθεί σε περισσότερες από μία εφαρμογές. Για τους ερασιτέχνες ηλεκτρονικούς παρουσιάζουν ενδιαφέρον όνο οι κάρτες που δεν έχουν δεσμευμένη τη μνήμη EEPROM. Αυτές περιλαμβάνουν μια CPU με ενταμιευμένο πρόγραμμα, εντεταλμένο να διαχειρίζεται τις μεταφορές δεδομένων μεταξύ CPU - EEPROM και φυσικά μεταξύ κάρτας - αναγνώστη. Κάνοντας χρήση αυτών των βασικών ρουτινών μπορούν να δώσουν μια δεύτερη "ευκαιρία" στις ληγμένες τηλεφωνικές κάρτες, αφού αυτές μπορούν άνετα να χρησιμοποιηθούν και για άλλες εφαρμογές. Δυστυχώς όμως οι περισσότερες τηλεφωνικές κάρτες, απ' αυτές που χρησιμοποιούνται σήμερα, αποδεικνύονται άχρηστες μόλις ξοδευτούν και οι τελευταίες μονάδες που έχουν μέσα τους.

Typ	CPU	RAM	ROM	EEPROM
Siemens SLE 44xx	8 Bit 8051 Derivat	128 Byte	4 kByte	2 kByte
Motorola 68HC05xx	8 Bit 6805	128 Byte	6 kByte	3 kByte
SGS ST9	8 Bit 6805 Derivat	256 Byte	20 kByte	1,5 kByte
Toshiba TOSMART	8 Bit Z80 Derivat	512 Byte	8 kByte	8 kByte
Hitachi H8/310	8 Bit H8	256 Byte	10 kByte	8 kByte
Philips 83C852	8 Bit 80C51 Derivat	256 Byte	6 kByte	2 kByte
OKI MSM627xxx	8 Bit 8051 Derivat	448 Byte	14 kByte	16 kByte

950036 - 19

Πίνακας 2. Πίνακας κατασκευαστών καρτών με ολοκληρωμένο και συνοπτική περιγραφή των υπολογιστικών συστημάτων που χρησιμοποιούν.

Αναγνώριση

Ο τρόπος με τον οποίο οι κάρτες γνωστοποιούν την ταυτότητά τους στον αναγνώστη καρτών είναι τυποποιημένος και αναφέρεται στο πρότυπο ISO 7816-3 με το σύντομο προσδιορισμό "ανταπόκριση στο σήμα επανατοποθέτησης", που με πιο απλά λόγια σημαίνει απάντηση στο σήμα επανατοποθέτησης που επιβάλλεται από την συσκευή ανάγνωσης στην κάρτα. Κατά τη διάρκεια αυτής της φάσης, η CPU της κάρτας διαβάζει από τη μνήμη ROM έναν αριθμό μήκους 128 bit (256 το πολύ, σε μερικές άλλες) που περιλαμβάνει, μεταξύ άλλων, πληροφορίες για τον κατασκευαστή της (T=1). Ο αριθμός αυτός με-

Διεύθυνση	Αριθμός	Λειτουργία
000	18	Ανταπόκριση στο σήμα επανατοποθέτησης
016	8	11111111 - Εικονικά ψηφία
024	4	Κατασκευαστής και πρώτη θέση του αριθμού σειράς 0000 CRGA 0 N1 1000 GDM 1 0100 CDS 2 1100 Gemplus 3 0010 Solaic 4 1111 δεσμευμένη θέση 16
028	4	Αθροισμα ανιχνευσης λάθους
032	4	Τιμή της καινούργιας κάρτας 1100 1,50 DM 0010 5,00 DM 1010 12,00 DM 1110 60,00 DM
038	4	Έτος κατασκευής και δεύτερη θέση του αριθμού σειράς 0000 1990+10 N2 1000 1990+10 +1 0100 1980+10 +2 1100 1980+10 +3 0010 1980+10 +4 1010 1980+0(1) +5 1111 1980+0 +16
040	4	Μήνας κατασκευής {0...11} 0000 January +01 N8 N4 1000 February +02 0100 March +03 1101 December +12 1111 +16
048	4	Αριθμός σειράς N9
052	4	Αριθμός σειράς N8
058	4	Αριθμός σειράς N7
060	4	Αριθμός σειράς N6
064	8	Υπολειπόμενη αξία της κάρτας MSB αριθμός από 1-B a
072	8	Υπολειπόμενη αξία της κάρτας Bits b
080	8	Υπολειπόμενη αξία της κάρτας c
090	8	Υπολειπόμενη αξία της κάρτας d
098	8	Υπολειπόμενη αξία της κάρτας e Υπολειπόμενη αξία της κάρτας σε phenning $= a \cdot 5^4 + b \cdot 5^3 + c \cdot 5^2 + d \cdot 5^1 + e \cdot 5^0$
104	24	Συμπληρωματικά ψηφία πλήρωσης 11111...1

Πίνακας 3. Σημασία της πληροφορίας που μεταφέρουν τα bit που στέλνονται από μια τηλεφωνική κάρτα μιας χρήσης στον αναγνώστη. Η κάρτα περιλαμβάνει ορισμένο αριθμό μονάδων και προορίζεται για χρήση σε Γερμανικούς τηλεφωνικούς θαλάμους.

ταδίδεται σειριακά στον αναγνώστη. Ο προσδιορισμός T=_ αναφέρεται σ' ένα ειδικό πρωτόκολλο που συμπεριλαμβάνεται και αυτό στο πρότυπο ISO. Μέχρι στιγμής χρησιμοποιούνται τρία διαφορετικά πρωτόκολλα, τα T=0, T=1 και T=14.

Οι κάρτες στις διάφορες χώρες

Δυστυχώς, η χρήση μίας και μοναδικής κάρτας για μια συγκεκριμένη εφαρμογή έξω από τα όρια μιας χώρας είναι κάτι, που για πολλούς λόγους μέχρι τώρα, έχει αποδειχθεί δύσκολο. Η κατασκευή π.χ. μιας κάρτας που θα μπορούσε να χρησιμοποιηθεί σ' όλους τους τηλεφωνικούς θαλάμους της Ευρώπης παρεμποδίζεται τόσο από τα διαφορετικά τιμολόγια χρέωσης των τηλεφωνικών συνδιαλέξεων κάθε χώρας, όσο και από τους διαφορετικούς αλγορίθμους που χρησιμοποιούνται για την προστασία του αριθμού που προσδιορίζει το πλήθος των διαθέσιμων μονάδων της κάρτας. Αυτά τα δύο προβλήματα πηγάζουν κυρίως από την αδυναμία των χρησιμοποιούμενων, μέχρι τώρα τουλάχιστον, πρωτοκόλλων να συνταιριάξουν περισσότερες από μία εφαρμογές. Αυτός είναι, άλλωστε, και ο λόγος που σε κάθε χώρα χρησιμοποιούνται διαφορετικά πρωτόκολλα και υπο-πρωτόκολλα τα οποία βασίζονται, όμως, στο βασικό πρότυπο λειτουργίας των καρτών. Από την πλευρά των αναγνωστών των καρτών τώρα, σημειώνουμε ότι, αν και η διαδικασία που ονομάσαμε προηγουμένως "ανταπόκριση στο σήμα επανατοποθέτησης" δίνει στον αναγνώστη όλα εκείνα τα στοιχεία που προσδιορίζουν το χρησιμοποιούμενο από την κάρτα πρωτόκολλο, αυτό δε σημαίνει υποχρεωτικά πως τα λοιπά συστήματα του αναγνώστη είναι σε θέση να τα υποστηρίξουν. Όλα τα παραπάνω μας πείθουν πως είναι πολύ νωρίς για να μπορούμε να πούμε πως οι κάρτες αυτές είναι πλήρως συμβατές μεταξύ τους, ώστε να ξεπεράσουν τα εθνικά όρια των χωρών όπως επίσης και τον περιορισμό της χρήσης τους σε μια μόνο εφαρμογή. Η περιορισμένη συμβατότητα των καρτών, όπως εννοείται σήμερα, αναφέρεται στη θέση που τοποθετούνται οι επαφές πάνω στην επιφάνεια της κάρτας, που πρέπει να είναι σύμφωνη με το πρότυπο ISO, όπως επίσης και στον τρόπο με τον οποίο ο αναγνώστης πραγματοποιεί την αναγνώριση της ταυτότητας της κάρτας, όταν αυτή εισέρχεται στη σχισμή. Η διαδικασία "ανταπόκρισης στο σήμα επανατοποθέτησης" εργάζεται, προφανώς, το ίδιο καλά και με τις κάρτες που περιλαμβάνουν επεξεργαστή, όσο και μ' αυτές που περιλαμβάνουν μόνο μνήμη. Η ταυτότητα της κάρτας που μεταφέρεται στη συσκευή ανάγνωσης έχει σαν σκοπό να τον ενημερώσει για τις απαιτήσεις της κάρτας, σ' ότι αφορά τα ηλεκτρικά σήματα που περιμένει, αλλά και για τον τρόπο που ανταλλάσσεται η χρήσιμη πληροφορία. Συγκεκριμένα μέσα στην ταυτότητα περιέχονται στοιχεία για:

- τη θέση του περισσότερο σημαντικού ψηφίου (MSB) στη λέξη που μεταφέρεται σειριακά,
- το πρωτόκολλο επικοινωνίας,
- τη συχνότητα του σήματος χρονισμού (clock), που μπορεί να παράγεται στο εσωτερικό της κάρτας ή από τον αναγνώστη, και
- την τάση προγραμματισμού, που μπορεί και αυτή να παράγεται στο εσωτερικό της κάρτας ή να παρέχεται από τα κυκλώματα της συσκευής ανάγνωσης.

Στην συσκευή ανάγνωσης καρτών, που σκοπεύουμε να παρουσιάσουμε μελλοντικά στο περιοδικό μας, θα μπορείτε, μεταβάλλοντας το λογισμικό του ή ακόμα και τα κυκλώματα διασύνδεσής του με τις κάρτες, να διαβάζετε κάρτες προερχόμενες από οποιαδήποτε χώρα και κατασκευασμένες για να εξυπηρετούν οποιεσδήποτε εφαρμογές.

Πρωτόκολλο επικοινωνίας

Η επιβολή της ακολουθίας των σημάτων που φαίνονται στο σχ.8, είναι αναγκαία, προκειμένου να "εξαναγκαστεί" η κάρτα να στείλει την ταυτότητά της στη συσκευή. Η λέξη - ταυτότητα εξέρχεται οργανωμένη σε δύο μεγάλες ομάδες bit. Η πρώτη αποτελείται από 16 bit που είναι δεσμευμένα για τις ανάγκες της διαδικασίας "ανταπόκρισης στο σήμα επανατοποθέτησης", ενώ η δεύτερη, που αποτελείται από 112 bit, περιλαμβάνει διάφορα στοιχεία η σημασία των οποίων φαίνεται στον πίνακα 3 και περιγράφεται παρακάτω. Η περιγραφή και οι επεξηγήσεις που θα δοθούν, αφορούν την ταυτότητα της κάρτας που χρησιμοποιεί ο τηλεπικοινωνιακός οργανισμός Bundespost της Γερμανίας.

Κατασκευαστής

(bit 24 έως 27): Τα στοιχεία που περιέχονται

σ' αυτό το πεδίο προσδιορίζουν τους κατασκευαστές των βασικών τμημάτων της κάρτας, όπως επίσης και των ημιαγωγών εξαρτημάτων που χρησιμοποιούνται. Αναφέρεται φυσικά και ο κατασκευαστής της κάρτας, εκείνος δηλαδή που συναρμολόγησε όλα τα εξαρτήματα προκειμένου να παραδώσει την κάρτα με μορφή ολοκληρωμένου προϊόντος.

Τιμή της καινούριας κάρτας:
Δύο διαφορετικά πεδία τιμών επιτρέπουν στον αναγνώστη να προσδιορίσει τη συνολική τιμή της κάρτας (αυτή που προσδιορίστηκε κατά τη φάση της κατασκευής της), όπως επίσης και την υπολειπόμενη τιμή της (δηλαδή την τιμή της όταν θα έχουν εξαντληθεί όλες οι μονάδες που περιέχει). Η συνολική τιμή της κάρτας επιτρέπει την αυτόματη χρέωση της τηλεφωνικής μονάδας με δύο διαφορετικά τιμολόγια: 25 πένες για κάθε μονάδα αν η συνολική τιμή της κάρτας είναι 5 λίρες ή 20 πένες αν η κάρτα κοστίζει 20 λίρες.

Ημερομηνία κατασκευής:
Εδώ δηλώνεται το έτος και ο μήνας που κατασκευάστηκε η κάρτα. Η ημερομηνία αυτή δεν είναι η ίδια μ' αυτή που αναγράφεται στην επιφάνεια της κάρτας.

Αριθμός σειράς:
Πρόκειται για μια πληροφορία που αφορά τον αριθμό σειράς των ολοκληρωμένων κυκλωμάτων που περιέχονται στην κάρτα. Αποτελείται από εννέα αριθμούς, τους N1 έως N9, η τιμή των οποίων εμπεριέχεται στα bit 24 έως 60.

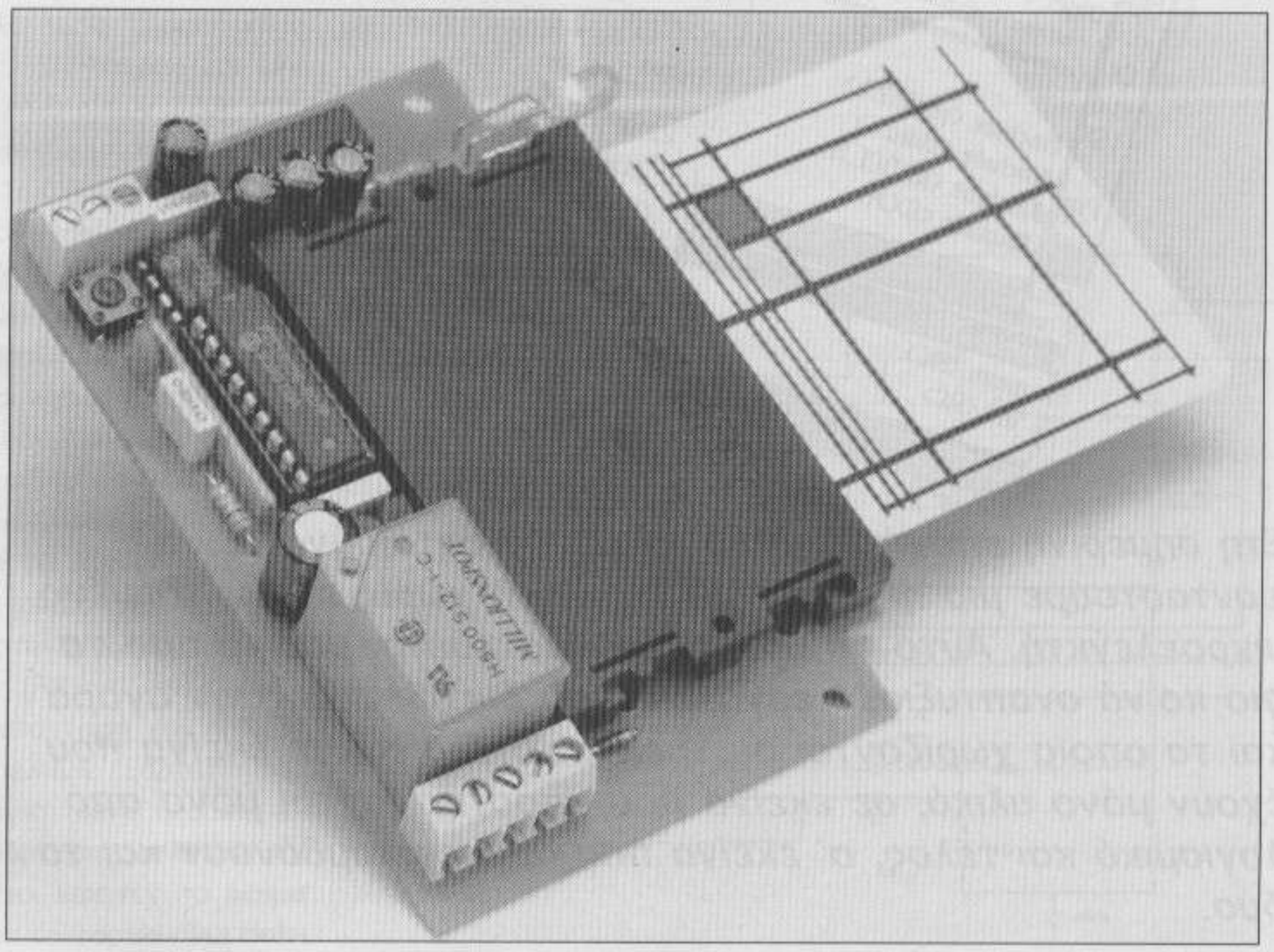
Κωδικοποίηση της πληροφορίας

Προφανώς οι πληροφορίες που περιέχονται στις πιστωτικές ή στις κάρτες των ασφαλιστικών εταιρειών είναι εμπιστευτικές και γι' αυτό τον λόγο πρέπει να προστατεύονται από οποιαδήποτε παράνομη προσπάθεια αντιγραφής ή χρήσης τους. Έτσι χρησιμοποιούνται διάφορες διαδικασίες κωδικοποίησης - απόκρυψης των στοιχείων αυτών, που είναι σύμφωνες με τα παρακάτω πρότυπα:
- DES (Data Encryption Standard). Το πρότυπο αυτό πρωτοπαρουσιάστηκε από την IBM το 1977. Συγκαταλέγεται μεταξύ των πλέον απλών, ασφαλών και ευρέως διαδεδομένων αλγορίθμων.
- FES (Fast data Encryption Standard). Πρόκειται για μια μικρότερων δυνατοτήτων έκδοση του DES που χρησιμοποιεί ακολουθίες - κλειδιά μικρότερου μήκους. Το υπολογιστικό σύστημα που χρησιμοποιεί αυτό τον αλγόριθμο φαίνεται να είναι ταχύτερο, προσφέρει όμως μικρότερη ασφάλεια σ' ότι αφορά την απόκρυψη της χρήσιμης πληροφορίας.
- DSA (Digital Signal Algorithm). Αναπτύχθηκε από την NSA (National Security Agency) με σκοπό την επαλήθευση της αυθεντικότητας της αποθηκευμένης ή διακινούμενης πληροφορίας.
- IDEA (International Data Encryption Algorithm). Πρόκειται για ένα νέο πρότυπο κατοχυρωμένο το 1991.
- RSA Rivest: Μέθοδος κωδικοποίησης - απόκρυψης στοιχείων που είναι ακόμα γνωστή και με το όνομα "Shamir and Antleman public key".

Όταν επιλεχθεί από τον κατασκευαστή της κάρτας αυτός που φαίνεται να είναι ο καλύτερος αλγόριθμος, λαμβάνεται υπόψη και η υπολογιστική ισχύς του μικροελεγκτή που χρησιμοποιείται, προκειμένου να εξασφαλιστεί πως οι χρόνοι εγγραφής / ανάγνωσης της κάρτας δε θα είναι ιδιαίτερα μεγάλοι, χωρίς βέβαια αυτό να αποβαίνει εις βάρος της ασφάλειας της διακινούμενης πληροφορίας.

Εφαρμογές

Οι κάρτες που προορίζονται για χρήση σε τηλεφωνικούς θαλάμους αποτελούν αναντίρρητα την πιο κοινή μορφή κάρτας με ολοκληρωμένο που κυκλοφορεί σήμερα στην αγορά. Διατίθενται σε δύο παραλλαγές: σ' αυτές που χρεώνουν άμεσα τον τραπεζικό λογαριασμό του κατόχου τους κάθε φορά που ο τελευταίος πραγματοποιεί μια συνδιάλεξη και σ' εκείνες που με την αγορά τους εξασφαλίζετε την πραγματοποίηση συνδιαλέξεων έχοντας σαν περιορισμό ένα προκαθορισμένο αριθμό μονάδων, για παράδειγμα 10 ή 50. Οι δεύτερες αν και δεν είναι προσωπικές, χαρακτηρίζονται από ένα μοναδικό αριθμό σειράς που τις κάνει ιδανικές στις περιπτώσεις εκείνες που θέλετε π.χ. να εξασφαλίσετε την πρόσβαση ορισμένων μόνο προσώπων σ' ένα φυλασσόμενο χώρο. Έτσι αντί να τις πετάξετε μόλις αυτές πάψουν να έχουν "μονάδες", μπορείτε να διαβάσετε τους αριθμούς σειράς τους και να προγραμματίσετε τον μικροελεγκτή που ελέγχει τις κλειδαριές του κτιρίου, έτσι ώστε να επιτρέπει την πρόσβαση μόνο σε εκείνους που θα εισάγουν στη σχισμή της συσκευής ανάγνωσης μια από τις επιλεγμένες κάρτες. Μια περισσότερο πολύπλοκη εφαρμογή θα μπορούσε, αξιοποιώντας πάλι τους αριθμούς σειράς μερικών καρτών, να καταχωρεί τις ώρες εισόδου / εξόδου του κάθε υπαλλήλου, υπολογίζοντας έτσι τον συνολικό χρόνο εργασίας του.
Για περισσότερα στοιχεία:
Amphenol, chip card product information, C702-X, C703, C704, C705, C707, C708
OKI, smart card product information.
ISO 177, DIN 66003, ISO 7810, ISO 7811/1, ISO 7811/2, ISO 7811/3, ISO 7811/4, ISO 7811/5, ISO 7816-1, ISO 7816-2, ISO 7816-3, ISO 7816.
A.N.S.I Date Encryption Algorithm 1, DES X3.92-1991



Σχήμα 7: Μια απλή και οικονομική συσκευή ανάγνωσης.