Έξυπνες κάρτες

το Α και το Ω της χρήσης τους σε απλές εφαρμογές

του Christian Tavernier

Μετά από μια μάλλον ...διστακτική και γεμάτη επιφυλάξεις πρώτη εμφάνιση, οι έξυπνες κάρτες είναι πλέον ώριμες να αντιμετωπίσουν τις ανάγκες της σημερινής τεχνολογικής κοινωνίας. Αυτό άλλωστε, το αποδεικνύει η χρήση τους στις περισσότερες καθημερινές μας δραστηριότητες. Μια ματιά γύρω μας και θα τις βρούμε σχεδόν παντού: στα κινητά τηλέφωνα, στους αποκωδικοποιητές συνδρομητικών δορυφορικών καναλιών, σε αυτόματα συστήματα πληρωμής κ.λπ. Τι καλύτερο λοιπόν από το να γνωρίζουμε μερικά πράγματα γι' αυτές;

Στο άρθρο αυτό θα αναφερθούμε στη σχεδίαση και στα εσωτερικά κυκλώματα των διαφόρων έξυπνων καρτών. Η συνολική παρουσίαση έχει σαν σκοπό τη γνωριμία με αυτές έτσι ώστε να μπορέσετε να τις αξιοποιήσετε στις δικές σας εφαρμογές. Για να καταφέρετε βέβαια κάτι τέτοιο, θα πρέπει να είστε σε θέση να τις εγγράφετε και να τις διαβάζετε παράγοντας τα κατάλληλα σήματα δεδομένων και χρονισμού. Σε ένα άλλο άρθρο θα μιλήσουμε για τις σχετικές συσκευές προγραμματισμού.

Τυποποιημένος συνδετήρας

Οι κάρτες ημιαγωγού έξυπνες κάρτες υπόκεινται σε ένα αρκετά μεγάλο σύνολο προτύπων ISO αποδεκτών σε όλο τον κόσμο. Από όλα τα πρότυπα αυτά που συναντάμε περισσότερο είναι τα ISO 7816-1 έως και 7816-4, τα οποία ορίζουν επακριβώς τα τεχνικά χαρακτηριστικά των καρτών. Λόγω της περιορισμένης έκτασης του άρθρου, είναι αδύνατον να αναφερθούμε εκτενώς σε αυτά. Αν όμως κάποιοι από τους αναγνώστες μας επιθυμούν να μάθουν περισσότερα, μπορούν να ανατρέξουν στη σχετική εργασία του συγγραφέα [1]. Εμείς θα περιοριστούμε σε μια σύντομη περιγραφή τους ξεκινώντας από την παρουσίαση των εσωτερικών κυκλωμάτων τους. Όπως θα μαντέψατε, κύρια μονάδα τους είναι ένας μικροελεγκτής (σχ. 1).

Για το ποιος θα είναι ο πυρήνας του μικροελεγκτή που κρύβεται κάτω από το πλαστικό κάλυμμα μιας κάρτας ερίζουν πολλές εταιρίες. Η πρόταση της Motorola αφορά σε έναν 68HC05, της Microchip σε έναν PIC16F876, ενώ της Atmel σε έναν AT90S8515. Σε πολλές κάρτες ο μικροελεγκτής συνδέεται άμεσα με μια σειριακή μνήμη EEPROM ή με ένα επεξεργαστή (απο)κρυπτογράφησης απαραίτητο για τις 'προστατευμένες' και 'εμπιστευτικές' εργασίες.

Σε αντίθεση με τις κάρτες τύπου RFID που επικοινωνούν μέσω ηλεκτρομαγνητικών φορέων και για τις οποίες μιλήσαμε αρκετά σε προηγούμενα τεύχη, οι έξυπνες κάρτες 'συνομιλούν' μέσα από καθαρά ωμικές επιχρυσωμένες επαφές τυπωμένες στο κέλυφος του πλαστικοποιημένου σώματός τους. Η διάταξη των επαφών είναι, επίσης, τυποποιημένη και σύμφωνη με το σχ. 2. Τα σήματα που διακινούν θα σας φανούν αυτονόητα εάν προφθάσατε να μελετήσετε το σχ. 1. Ας πούμε όμως δύο λόγια για τις επαφές και τα σήματά τους:

- C1 και C5: Επάνω σε αυτές εφαρμόζεται η τάση τροφοδοσίας (Vcc και GND αντίστοιχα). Μέχρι πρότινος, η τάση αυτή ήταν πάντα +5 V, αλλά οι τεχνολογικές εξελίξεις την έχουν πλέον μειώσει στα +3 V. Σε αυτό άλλωστε συνηγορεί και το ολοένα αυξανόμενο πλήθος των ολοκληρωμένων κυκλωμάτων που δουλεύει με σαφώς χαμηλότερες τάσεις.
- C3: Στην ακίδα αυτή εφαρμόζεται από τη συσκευή διαχείρισης της κάρτας το εξωτερικό σήμα χρονισμού (CLK). Η παρουσία του δικαιολογείται αν σκεφθούμε πως από όλες τις έξυπνες κάρτες απουσιάζει οποιαδήποτε μονάδα ταλάντωσης.
- C2: Δέχεται το εξωτερικό σήμα Αρχικοποίησης (RST) το οποίο επιδρά άμεσα στην ομώνυμη ακίδα του μικρο-

ελεγκτή. Το σήμα ενεργοποιείται σε χαμηλή στάθμη.

- C7: Πρόκειται για την ακίδα μέσω της οποίας διακινούνται όλα τα δεδομένα εισόδου / εξόδου. Η μετάδοση γίνεται με ασύγχρονο σειριακό τρόπο.
- C4 και C8: Σε πολλά έγγραφα και τεχνικά κείμενα ονομάζονται RFU (Reserved for Future Use, Δεσμευμένες για Μελλοντική Χρήση). Το περίεργο είναι πως εδώ και είκοσι περίπου χρόνια που κυκλοφορούν οι έξυπνες κάρτες, κανείς δεν έχει ασχοληθεί με αυτές τις επαφές. Ίσως το μέλλον να είναι ακόμα μακρινό!
- C6: Ήταν απαραίτητη στις πρώτες έξυπνες κάρτες, μιας που μέσω αυτής της επαφής 'περνούσε' η τάση προγραμματισμού των (επαν)εγγράψιμων μνημών εκείνης της εποχής. Σήμερα η τάση αυτή δεν είναι πλέον απαραίτητη και κατά συνέπεια η ακίδα αυτή παραμένει πρακτικά άχρηστη.

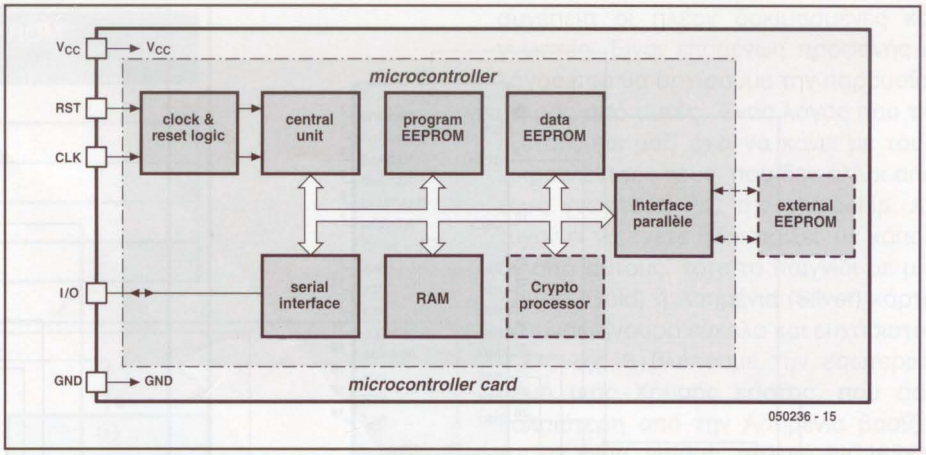
Για άλλη μια φορά ο περιορισμένος χώρος του περιοδικού μας εμποδίζει να αναφερθούμε στο πρωτόκολλο επικοινωνίας των έξυπνων καρτών με την συσκευή διαχείρισης τους. Αν παρόλα αυτά οι αναγνώστες μας, ζητήσουν να μάθουν περισσότερα υποσχόμαστε να δημοσιεύσουμε όλα τα απαραίτητα στοιχεία στο δικτυακό μας τόπο.

Οι κάρτες της αγοράς

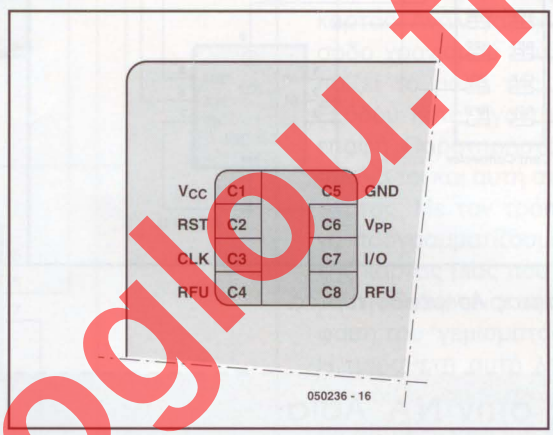
Σήμερα διατίθενται στην αγορά πολλές κάρτες οι οποίες στερούνται (δυστυχώς) επαρκούς τεκμηρίωσης. Η απουσία στοιχείων μας ξενίζει κατ' αρχήν, αλλά μάλλον την δικαιολογούμε εκ των υστέρων αν λάβουμε υπόψη μας ότι πολλές απο αυτές χρησιμοποιούνται σε συστήματα που προέχει η ασφάλεια. Για το λόγο αυτό και για να βοηθήσουμε αυτούς που "σπάνε" τους κωδικούς για όχι και τόσο καθαρούς λόγους. Παρ' όλα αυτά στο Internet μπορούμε να βρούμε όλες τις πληροφορίες για τις περισσότερες κάρτες. Σημειώνουμε πάντως, πως για αρκετές από τις κάρτες που κυκλοφορούν σήμερα στην αγορά, οι κατασκευαστές τους διαθέτουν άφθονα στοιχεία, έτσι ώστε να μπορέσετε να τις χρησιμοποιήσετε στις δικές σας εφαρμογές.

Η Χρυσή και η Ασημένια κάρτα

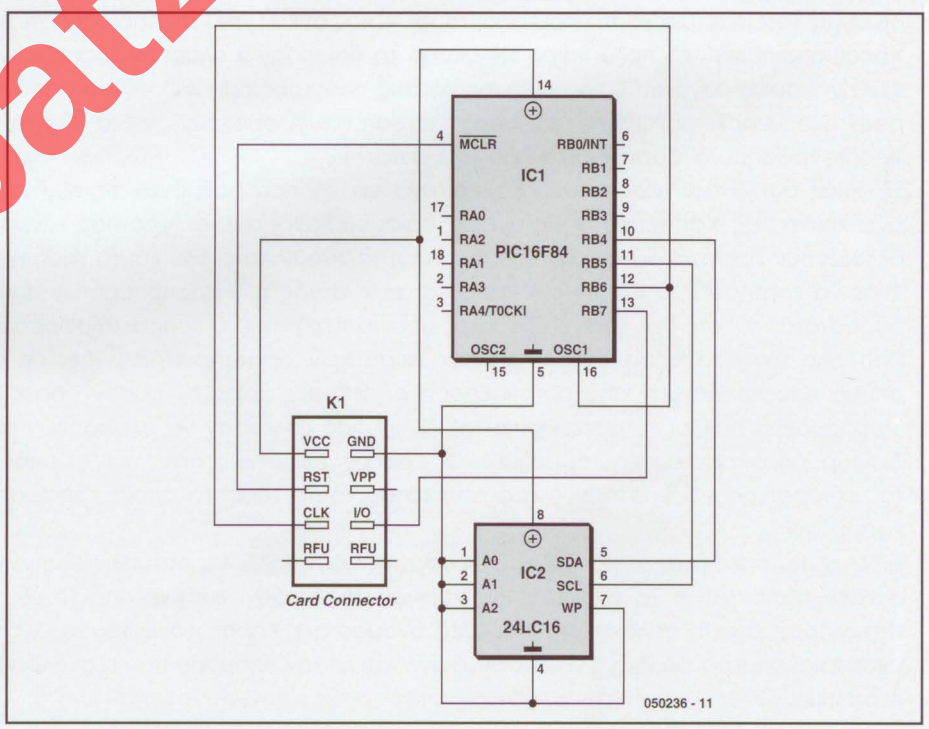
Από ιστορική άποψη οι παραπάνω κάρτες είναι οι παλαιότερες και κατά



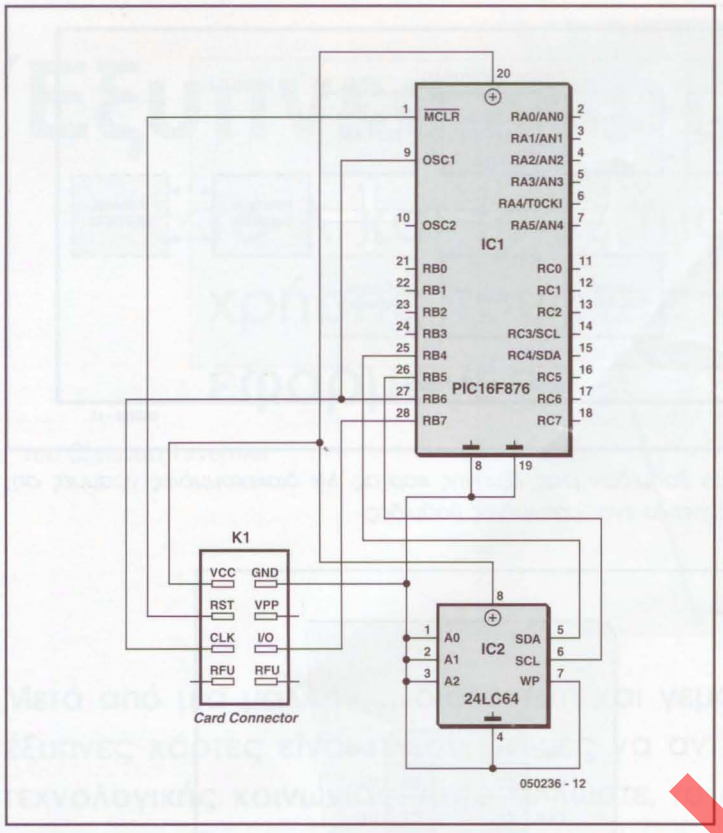
Σχ. 1. Το διάγραμμα βαθμίδων μιας έξυπνης κάρτας. Με διακεκομμένες γραμμές σημειώνονται οι προαιρετικά ενσωματωμένες βαθμίδες.



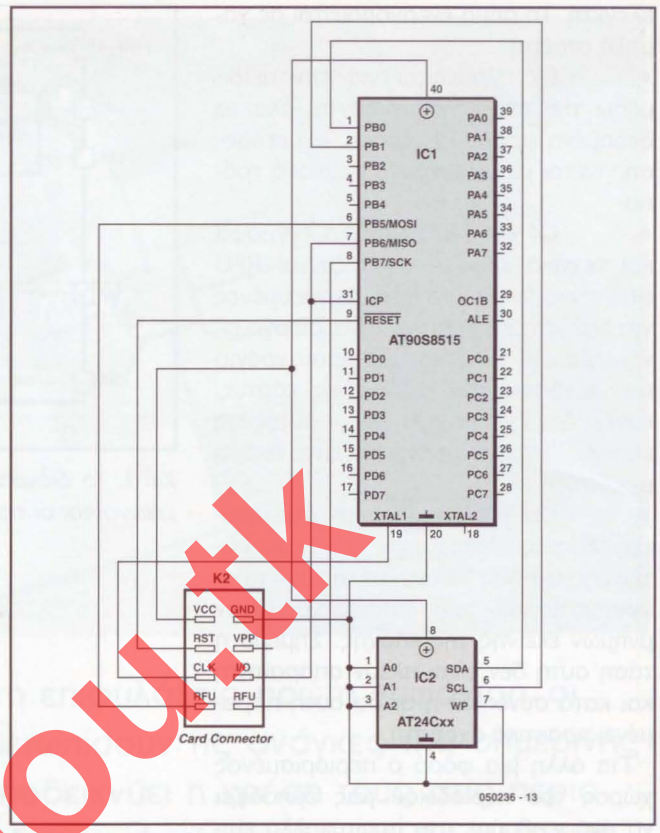
Σχ. 2. Ονομασίες επαφών και σημάτων μιας έξυπνης κάρτας.



Σχ. 3. Το κύκλωμα μιας Χρυσής κάρτας.



Σχ. 4. Το κύκλωμα μιας Ασημένιας κάρτας.



Σχ. 5. Το κύκλωμα μιας κάρτας Fun (ή Purple).

Οι κάρτες στην N.A. Ασία

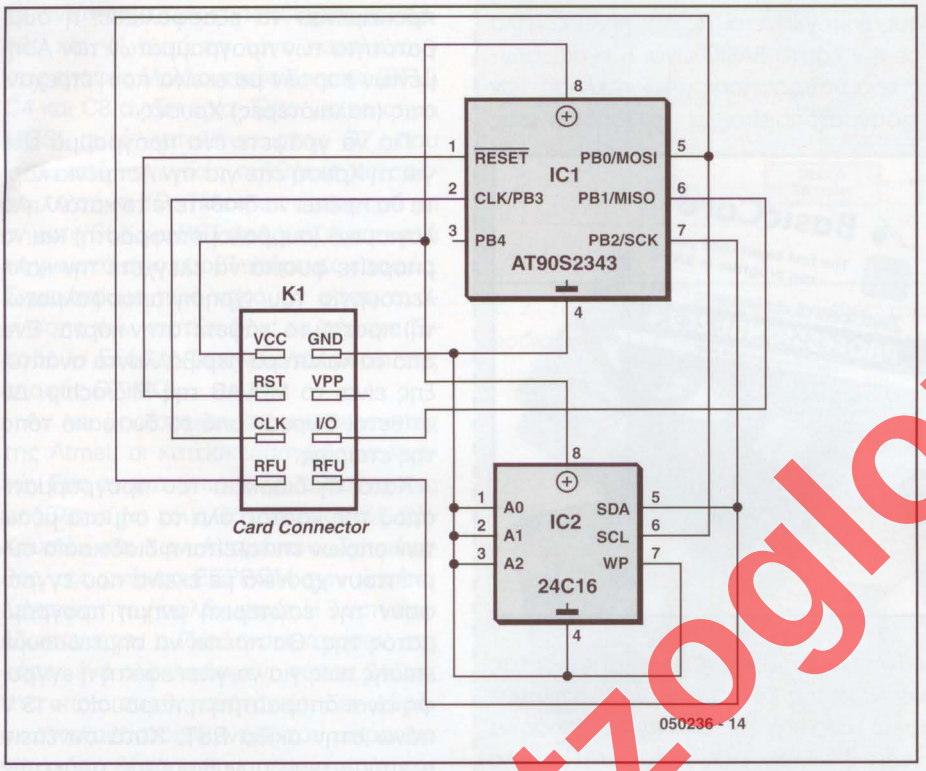
Λόγω της χρήσης τους που εντοπίζεται κυρίως στην προστασία 'ευαίσθητων' πληροφοριών, οι έξυπνες κάρτες βρίσκονται πάντα στο στόχαστρο των πειρατών και των χάκερ. Αντιπροσωπευτικό παράδειγμα τέτοιων 'πρωτοβουλιών' αποτέλεσε η περιώνυμη YesCard, μια κάρτα που απαντούσε καταφατικά ('yes') σε οποιοδήποτε ερώτημα της έδετε ο Αναγνώστης καρτών. Χρησιμοποιήθηκε για πολύ καιρό με σκοπό τη δημιουργία πλαστών τραπεζικών καρτών πρόσβασης στα διάφορα ATM. Δεν είναι όμως μόνο αυτό το είδος της κάρτας που χρησιμοποιήθηκε για παράνομους σκοπούς. Στο Διαδίκτυο κυκλοφορούν ακόμα αρκετοί κώδικες που από τη στιγμή που 'φορεθούν' σε μια έξυπνη κάρτα είναι σε θέση να 'σπάσουν' πολλά 'κρυπτογραφημένα' δορυφορικά προγράμματα.

Εξ αιτίας αυτών των περιστατικών πολλοί είναι εκείνοι που φοβούνται τις έξυπνες κάρτας πιστεύοντας πως η χρήση τους είναι επισφαλής. Κάτι τέτοιο όμως είναι εξ ορισμού λανθασμένο. Αυτό που κάνουν οι πειρατές είναι να επεμβαίνουν και να αλλοιώνουν προγράμματα τα οποία δεν προστατεύουν καλά τον εαυτό τους ή προγράμματα τα οποία κανείς δεν φρόντισε να κρατήσει μυστικά. Αν ο ίδιος ο κατασκευαστής των προγραμμάτων που εισάγονται μέσα στις κάρτες τα 'αφήνει' απροστάτευτα, τότε δεν φταίνε οι κάρτες που τα περιεχόμενά τους κυκλοφορούν ανεμπόδιστα στο Διαδίκτυο!

Παρ' όλο τον παράνομο χαρακτήρα των 'πειρατικών' δραστηριοτήτων, δεν θα πρέπει να αγνοήσουμε και μερικά θετικά σημεία που προέκυψαν από αυτόν. Επειδή οι πειρατές χρειαζόντουσαν άδειες κάρτες για να 'βολέψουν' τις δικές τους ...εφαρμογές, πολλοί κατασκευαστές της N.A. Ασίας έσπευσαν να σχεδιάσουν αρκετούς τύπους καρτών βασισμένους σε διάφορους μικροελεγκτές και μνήμες. Οι Χρυσές, Ασημένιες όπως και οι υπόλοιπες ...έγχρωμες κάρτες δεν είναι τίποτα περισσότερο και τίποτα λιγότερα από τα προϊόντα τους, τα οποία χρησιμοποιούμε σήμερα στις δικές μας (νόμιμες) εφαρμογές.

Η N.A. Ασία αποδείχθηκε για άλλη μια φορά το λίκνο πολλών προτύπων έξυπνων καρτών, που όλες τους κυκλοφόρησαν σχεδόν ταυτόχρονα. Τα ονόματα των καρτών προέκυψαν, κυρίως, από τα εξωτερικά χαρακτηριστικά των πρώτων αντιτύπων τους. Έτσι, η παλαιότερη από όλες ονομάστηκε Χρυσή λόγω του χρώματος της, όνομα (και χρώμα) που διατηρεί ακόμα και σήμερα. Το ίδιο άλλωστε συμβαίνει και με την Ασημένια που εξακολουθεί να πουλιέται σε ένα ασημένιο πλαστικό περίβλημα.

Πίνακας 1 Τύπος κάρτας	Μνήμη EEPROM
Fun (standard)	24C64
Fun 2	24C64
Fun 4	24C256
Fun 5	24C512
Fun 6	24C1024



Σχ. 6. Το κύκλωμα μιας κάρτας Jupiter (Ροζ).

συνέπεια οι πλέον δοκιμασμένες και γνωστές. Είναι επομένως προφανής ο λόγος που θα αρχίσουμε την παρουσίαση μας από αυτές. Ένας λόγος που τις εξετάζουμε μαζί έχει να κάνει με τους μικροελεγκτές τους, που δεν άλλοι από τους γνωστούς PIC της Microchip. Αν τυχαίνει να έχετε ήδη 'παίξει' με κάποιον από αυτούς, τότε το παιγνίδι με μια Χρυσή (Gold) ή Ασημένια (Silver) κάρτα θα είναι σίγουρα εύκολο και ευχάριστο.

Στο σχ. 3 βλέπουμε την εσωτερική δομή μιας Χρυσής κάρτας, που σαν παλαιότερη από την Ασημένια βασίζεται σε έναν, επίσης, παλαιό PIC16F84. Η συνδεσμολογία του είναι προφανής: Η ακίδα αρχικοποίησής του συνδέεται στην ομώνυμη επίχρυση επαφή της κάρτας. Ανάλογα ισχύουν και για την είσοδο χρονισμού του, ενώ η ακίδα RB7 παίζει το ρόλο της ακίδας Εισόδου / Εξόδου καταλήγοντας στην αντίστοιχη επαφή. Παρατηρήστε ακόμα, ότι η RB6 συνδέεται και αυτή στην επαφή CLK της κάρτας. Με τον τρόπο αυτό μπορούμε να προγραμματίζουμε το μικροελεγκτή της κάρτας μιας που η ακίδα αυτή μαζί με την Reset είναι απαραίτητες κατά την φάση του 'γεμίσματός' της μνήμης του. Η πρόσθετη αυτή λειτουργία δεν μας εμποδίζει, φυσικά, να χρησιμοποιούμε τις επαφές CLK και I/O με τον προβλεπόμενο τυποποιημένο τρόπο.

Επειδή η μνήμη EEPROM του PIC16F84 ήταν πολύ μικρή, γρήγορα συμπεριλήφθηκε στη Χρυσή Κάρτα και ένα

Κάρτες με μικροελεγκτή ή με μνήμη;

Ο γενικός όρος 'κάρτα ημιαγωγού' (chipcard) καλύπτει δύο μεγάλες κατηγορίες καρτών. Προς αποφυγήν παρεξηγήσεων σπεύδουμε να ρίξουμε φως στις οποιεσδήποτε παρανοήσεις. Οι κάρτες ημιαγωγού χωρίζονται σε δύο μεγάλες κατηγορίες: στις 'κάρτες μνήμης' (memory card) που όπως προδίδει το όνομά τους περιέχουν μόνο μνήμες και στις 'έξυπνες κάρτες' (smart card) που εξασφαλίζουν ισχυρή επεξεργαστική ικανότητα βασισμένες σε μικροελεγκτές. Οι διαφορές ανάμεσα στις δύο παραλλαγές τους είναι μεγάλες και γι' αυτό το λόγο θα πρέπει να είμαστε πάντα προσεκτικοί στις επιλογές μας.

Οι προπληρωμένες κάρτες μνήμης που χρησιμοποιούνται στα τηλέφωνα, στα καταστήματα με πλυντήρια / στεγνωτήρια ρούχων και στα συστήματα πρόσβασης γενικότερα, φιλοξενούν στο εσωτερικό τους μια ακολουθία αριθμών φυλαγμένη μέσα σε μια EEPROM. Είναι προφανές πως τα περιεχόμενα μιας τέτοιας κάρτας είναι δυνατόν να διαβαστούν, διαγραφούν ή να επανεγγραφούν περισσότερο ή λιγότερο εύκολα σύμφωνα πάντα με το επίπεδο προστασίας που υποστηρίζει η κάρτα. Το απλούστερο που μπορεί να γίνει προκειμένου να εξασφαλιστεί το απόρρητο των περιεχομένων τους είναι η κρυπτογράφησης τους σύμφωνα με κάποιους προκαθορισμένους κανόνες.

Προτού αγοράσετε μια κάρτα με δυνατότητες κρυπτογράφησης και αναζητήσετε στοιχεία για τη λειτουργία της, θα πρέπει να υπογράψετε μια συμφωνία με τον κατασκευαστή σύμφωνα με την οποία θα κρατήσετε μυστικά όλα τα στοιχεία που θα σας δοθούν (συμφωνία Non Disclosure Agreement, NDA).

Στο παρόν άρθρο θα αποφύγουμε να ασχοληθούμε με τις κάρτες μνήμης λόγω των περιορισμένων εφαρμογών τους. Θα εστιάσουμε το ενδιαφέρον μας στις έξυπνες κάρτες που αποτελούν σήμερα το βασικό 'συστατικό' των τραπεζικών συναλλαγών μας, των κινητών τηλεφώνων μας ή των δορυφορικών δεκτών μας. Οι κάρτες αυτές είναι αναντίρρητα πολύ πιο χρήσιμες σε έναν ηλεκτρονικό μιας που με τη βοήθεια τους μπορεί να αναπτύξει οποιαδήποτε εφαρμογή προϋποθέτει ασφαλή πρόσβαση σε εμπιστευτικά δεδομένα. Τα πράγματα γίνονται ακόμα πιο εύκολα αν σκεφθούμε πως οι κάρτες αυτές πουλιούνται απρογραμμάτιστες έτοιμες για χρήση.

Κάρτα Basic, μια σαφώς διαφορετική κάρτα

Η κάρτα αυτή, που κατασκευάζεται αποκλειστικά και μόνο από τη μικρή Γερμανική εταιρία ZeitControl, ανήκει στην κατηγορία καρτών με ενσωματωμένο λειτουργικό σύστημα. Όπως υπαινίσσεται το όνομά της προγραμματίζεται με τη βοήθεια εντολών γλώσσας BASIC. Οι εντολές που αντιλαμβάνεται, είναι ίδιες με αυτές της παλιάς καταξιωμένης BASIC που 'έτρεχαν' οι παλαιότεροι PC, μόνο που έχουν τροποποιηθεί ελαφρά ώστε να ανταποκρίνονται στις ιδιόμορφες απαιτήσεις των εφαρμογών που 'χωρούν' σε μια έξυπνη κάρτα. Κάτω από αυτές τις προϋποθέσεις ο προγραμματισμός τους επιτυγχάνεται με ένα πολύ εύκολο και βολικό τρόπο. Το πλέον ενδιαφέρον με την κάρτα BASIC είναι η ενσωμάτωση βιβλιοθηκών εξοπλισμένων με κώδικες κρυπτογράφησης, ενώ η κλήση των γνωστών αλγορίθμων DES και 3DES με πραγματοποιείται με τη βοήθεια μιας μοναδικής εντολής.

Μέχρι τη στιγμή που γράφονται αυτές οι γραμμές διατίθενται στην αγορά δεκαπέντε διαφορετικές παραλλαγές της κάρτας BASIC που διαφέρουν μεταξύ τους στη χωρητικότητα της μνήμης και στις δυνατότητες κρυπτογράφησης. Για την ανάπτυξη εφαρμογών με μια τέτοια κάρτα θα χρειαστείτε ένα ειδικό περιβάλλον ανάπτυξης, γεγονός που απορρέει από την εξειδικευμένη γλώσσα προγραμματισμού της. Το περιβάλλον αυτό διατίθεται δωρεάν από το κατασκευαστή της κάρτας (κάντε μια σύντομη επίσκεψη στο δικτυακό τόπο της ZeitControl). Σημειώνουμε πως το περιβάλλον αυτό εργάζεται εξ ίσου καλά και μέσα από τα Windows αλλά και κάτω από τον έλεγχο του παλιού □ καλού DOS. Ανάμεσα σε όλα τα άλλα διαθέτει ένα προσομοιωτή κάρτας και ένα προσομοιωτή αναγνώστη. Χρησιμοποιώντας τους μπορείτε να είστε βέβαιοι για την καλή λειτουργία της εφαρμογής σας προτού ακόμα επιχειρήσετε να την υλοποιήσετε στον πάγκο του εργαστηρίου σας.

Η παρουσία του ενσωματωμένου λειτουργικού συστήματος μας επιτρέπει να την προγραμματίσουμε με οποιαδήποτε συσκευή προγραμματισμού υποστηρίζεται από το περιβάλλον ανάπτυξης. Για τους χρήστες των συνηθισμένων υπολογιστών με Windows αποδεικνύεται μια πολύ εύκολη εργασία μιας που αρκεί

πρόσθετο ολοκληρωμένο κύκλωμα ικανό να παρακάμπτει αυτό το πρόβλημα. Το εξάρτημα αυτό δεν ήταν άλλο από μια σειριακή EEPROM τύπου 24LC16 (ή συμβατή με αυτήν) που επικοινωνούσε με τον μικροελεγκτή μέσω σημάτων διαύλου I²C. Τα τελευταία αναδεικνυόντουσαν από τις ακίδες RB4 και RB5 κάτω από τον έλεγχο του κατάλληλου λογισμικού (ο PIC16F84 δεν διαθέτει ενσωματωμένη μονάδα I²C). Εννοείται πως αν η δική σας εφαρμογή αρκείται στις λιγοστές θέσεις της EEPROM που φιλοξενούνται στο εσωτερικό του ίδιου του μικροελεγκτή, τότε μπορείτε να 'παραλείψετε' τον κώδικα υποστήριξη του παραπάνω διαύλου.

Το κύκλωμα της Ασημένιας κάρτας (βλ. σχ. 4) είναι το ίδιο απλό με εκείνο της Χρυσής, μόνο που ο μικροελεγκτής έχει αντικατασταθεί με έναν PIC16F876. Το ίδιο έχει γίνει και με τη μνήμη, που έχει δώσει τη θέση της σε μια μεγαλύτερη τύπου 24LC64. θα συμφωνήσουμε όλοι πως αυτές οι βελτιώσεις δεν ήταν και τόσο ουσιαστικές, αλλά μάλλον απαραίτητες αν σκεφθούμε πως η κάρτα αυτή σχεδιάστηκε από 'πειρατές' για καθαρά 'πειρατική' χρήση ('σπάσιμο' τηλεοπτικών προγραμμάτων). Η μνήμη EEPROM εξακολουθεί να συνδέεται στις ακίδες RB4 και RB5 του μικροελεγκτή, γεγονός που κάνει απαραίτητη την παρουσία λογισμικού υποστήριξης I2C. Το τελευταίο θα μπορούσε να παραλειφθεί αν η μνήμη κατέληγε στις ακίδες RB3 και RB4 στις οποίες καταλήγουν οι έξοδοι της ενσωματωμένης στον PIC16F876 μονάδας I²C. Προτιμήθηκε όμως αυτή η μάλλον 'παλιομοδίτικη' συνδεσμολογία προκειμένου να εξασφαλισθεί η συμβατότητα των προγραμμάτων των Ασημένιων καρτών με εκείνα που 'έτρεχαν' στις (παλαιότερες) Χρυσές.

Για να γράψετε ένα πρόγραμμα είτε για τη Χρυσή είτε για την Ασημένια κάρτα θα πρέπει να διαθέτετε το κατάλληλο λογισμικό (συμβολομεταφραστή) και να μπορείτε φυσικά να ελέγχετε την καλή λειτουργία του (χρήση αποσφαλματωτή) προτού το 'κάψετε' στην κάρτα. Ένα από τα καλύτερα περιβάλλοντα ανάπτυξης είναι το MPLAB της Microchip. Διατίθεται δωρεάν από το δικτυακό τόπο της εταιρίας.

Κατά τη διάρκεια του προγραμματισμού της κάρτας όλα τα σήματα μέσω των οποίων επιτελείται η διαδικασία συμπίπτουν χρονικά με εκείνα που εγγράφουν την εσωτερική μνήμη προγράμματός της. Θα πρέπει να σημειώσουμε επίσης πως για να γίνει εφικτή η εγγραφή είναι απαραίτητη η παρουσία +13 V πάνω στην ακίδα RST. Κατά συνέπεια η χρήση μιας συνηθισμένης συσκευής ανάγνωσης (Αναγνώστη) Χρυσών και Ασημένιων καρτών για την εγγραφή τους είναι, κατ' αρχήν, αδύνατη. Παρ' όλα αυτά θα σας δείξουμε το πως μπορείτε να παρακάμψετε αυτό το πρόβλημα κάνοντας μερικές απλές προσθήκες / τροποποιήσεις.

Οι κάρτες Fun, Purple Pink και Jupiter

Την ίδια περίπου εποχή με εκείνη που εμφανίστηκαν οι Χρυσές και Ασημένιες κάρτες, πολλοί άλλοι κατασκευαστές διέθεσαν στην αγορά τις δικές τους σειρές καρτών που βασιζόντουσαν σε άλλους μικροελεγκτές. Αν και οι περισσότερες από αυτές δεν είχαν τόσο μεγάλη εμπορική επιτυχία, κατασκευάστηκαν σε μεγάλες ποσότητες με αποτέλεσμα να καθιερωθούν και να κυκλοφορούν ακόμα και σήμερα.

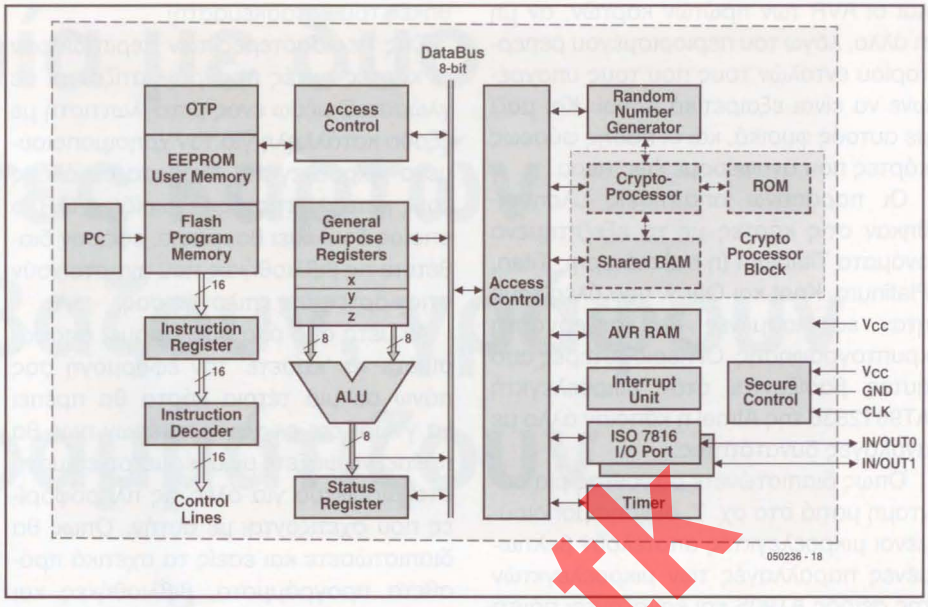
Οι κάρτες Fun, που αρχικά είχαν ονομαστεί Μωβ (Purple) λόγω του χρώματός τους, βασίζονται σε ένα μικροελεγκτή τύπου AT90S8515 της Atmel (σχ.

5). Σε ότι αφορά τη διασύνδεσή τους, χρησιμοποιούν την ίδια μορφή και διάταξη επαφών με τις προηγούμενες επιδεικνύοντας όμως μερικές διαφορές. Η αιτία των διαφοροποιήσεων εντοπίζεται στον τρόπο εγγραφής / ανάγνωσης των μνημών των μικροελεγκτών της σειράς AT90S που βασίζεται στα σήματα SCK, MISO και MOSI του διαύλου SPI. Τα δύο πρώτα είναι τελείως ασύμβατα με τα αντίστοιχα των τυποποιημένων καρτών και γι' αυτό το λόγο καταλήγουν στις επαφές Μελλοντικής Χρήσης (RFU) C4 και C8 αντίστοιχα. Όσο για το σήμα MOSI αυτό καταλήγει στην C7, που κάτω από κανονικές συνθήκες μεταφέρει το σήμα I/O. Τέλος σε ότι αφορά τα σήματα CLK και RST εφαρμόζονται κατά τα γνωστά στις προβλεπόμενες επαφές. Σημειώνουμε πως κατά τη φάση ανάγνωσης των καρτών Fun, τα σήματα Εισόδου / Εξόδου διακινούνται μέσω της επαφής C7 (I/O).

Αν και βασίστηκαν σε μικροελεγκτές της Atmel, οι κατασκευαστές των καρτών Fun αντιμετώπισαν και αυτοί το ίδιο πρόβλημα με τους κατασκευαστές των Χρυσών και των Ασημένιων. Το μέγεθος της μνήμης EEPROM των μικροελεγκτών ήταν πολύ μικρό. Η λύση που έδωσαν ήταν η ίδια: ενσωμάτωσαν στη κάρτα ένα ολοκληρωμένο τύπου 24Cxx, στο οποίο αποθηκευόταν ότι δεν χώραγε στην αντίστοιχη μνήμη του μικροελεγκτή. Στη θέση του xx μπορείτε να φαντασθείτε κάποιον από τους αριθμούς 64, 256, 512 ή 1024 που υποδηλώνουν άμεσα τη χωρητικότητά της. Ο Πίνακα 1 αντιστοιχίζει τους τύπους των καρτών Fun σύμφωνα με την χωρητικότητα της μνήμης τους. Απουσία οποιουδήποτε αριθμού υποδηλώνει μνήμη 64 Kbit ή, συνηθέστερα, 8 Kbyte.

Οι κάρτες Jupiter ή Ροζ (Pink) λόγω του χρώματος των πρώτων αντιτύπων τους βασίζονται και αυτές σε ένα μικροελεγκτή της Atmel με λιγότερες όμως δυνατότητες από εκείνον της Fun. Όπως θα παρατηρήσατε ήδη στο σχ. 6, ενσωματώνουν τον AT90S2343 ο οποίος συνοδεύεται πάντα από μια σειριακή μνήμη EEPROM 24C16. Ο τρόπος σύνδεσης των παραπάνω εξαρτημάτων με τις επαφές της κάρτας είναι ίδιος με εκείνον της κάρτας Fun, αφού ο AT90S2343 προσπελαύνεται με τον ίδιο τρόπο που προσπελαύνεται και ο AT90S8515.

Οι κάρτες Jupiter χρησιμοποιήθηκαν κατά το παρελθόν με μεγάλη επιτυχία για το 'σπάσιμο' κωδικοποιημένων τηλε-



Σχ. 7. Το διάγραμμα βαθμίδων ενός μικροελεγκτή της σειράς AT90Sxxxx της Atmel εφοδιασμένου με επεξεργαστή κρυπτογράφησης.

Οι παλιές κάρτες ημιαγωγού (αριστερά) ήταν συμβατές με το πρότυπο AFNOR. Σήμερα οι ίδιες κάρτες (δεξιά) είναι σύμφωνες με τα παγκοσμίως αποδεκτά πρότυπα ISO.

οπτικών προγραμμάτων, αλλά στις ημέρες μας έχουν σαφώς ξεπεραστεί από άλλες με περισσότερες δυνατότητες. Για το λόγο αυτό καλό είναι να αποφύγετε να τη χρησιμοποιήσετε σε εφαρμογές που σκοπεύετε να ξεκινήσετε στο άμεσο μέλλον.

Όπως και για τις Χρυσές και Ασημένιες κάρτες, έτσι και για τις Fun και Jupiter ο προγραμματισμός τους απαιτεί τη γνώση της συμβολικής γλώσσας του χρησιμοποιούμενου μικροελεγκτή. Το καλύτερο περιβάλλον γι' αυτήν τη δουλειά είναι το AVR Studio της κατασκευάστριας Atmel το οποίο μπορείτε να 'κατεβάσετε' δωρεάν από το δικτυακό τόπο της.

Η εγγραφή του προγράμματος στο μικροελεγκτή απαιτεί τη χρήση ειδικής συσκευής, μιας που οι περισσότεροι Αναγνώστες καρτών δεν ...ασχολούνται καθόλου με τις επαφές C4 και C8. Θα σας δείξουμε όμως πώς να τροποποιήσετε μια τέτοια συσκευή έτσι ώστε με λιγοστά εξαρτήματα να καταφέρει να εγγράψει τη μνήμη του μικροελεγκτή. Η τροποποιημένη συσκευή θα είναι σε θέση να γράφει τόσο την κάρτα Fun όσο και τη λιγότερο συνηθισμένη Jupiter.

Κάρτες Titanium, Knot και Opos

Στην προσπάθεια τους να εμποδίσουν την πειρατεία των προϊόντων τους, οι παροχείς συνδρομητικών προγραμμάτων ζήτησαν από τους κατασκευαστές καρτών να διαθέσουν στην αγορά καινούργιες κάρτες με αυξημένες δυνατότητες προστασίας. Από τη στιγμή όμως που οι αλγόριθμοι κρυπτογράφησης / αποκρυπτογράφησης απαιτούσαν αυξημένη υπολογιστική ισχύ ήταν προφανές πως έπρεπε να εγκαταλειφθούν οι PIC

και οι AVR των πρώτων καρτών, αν μη τι άλλο, λόγω του περιορισμένου ρεπερτορίου εντολών τους που τους υποχρέωνε να είναι εξαιρετικά αργοί. Και μαζί με αυτούς φυσικά, και οι πάσης φύσεως κάρτες που αναφέραμε έως τώρα.

Οι παραπάνω απαιτήσεις υλοποιήθηκαν στις κάρτες με τα εξεζητημένα ονόματα Titanium (η παλαιότερη), Titan, Platinum, Knot και Opos, που όλες τους ήταν εφοδιασμένες με επεξεργαστή κρυπτογράφησης. Οι περισσότερες από αυτές βασίζονται στον μικροελεγκτή AT9012836 της Atmel ή κάποιον άλλο με ανάλογες δυνατότητες.

Όπως διαπιστώνετε ρίχνοντας μια σύντομη ματιά στο σχ. 7, οι χρησιμοποιούμενοι μικροελεγκτές αποτελούν βελτιωμένες παραλλαγές των μικροελεγκτών της σειράς AT90S και εργάζονται πάντα συνοδευόμενοι από ένα περισσότερο ή λιγότερο ισχυρό επεξεργαστή κρυπτογράφησης. Ο συνδυασμός των δύο παραπάνω επιμέρους μονάδων επιτρέπει τη γρήγορη εκτέλεση των πολύπλοκων πράξεων που απαιτούν οι αλγόριθμοι κρυπτογράφησης DES, 3DES, RSA κλπ που χρησιμοποιούνται σήμερα από την πλειονότητα των παροχέων κρυπτογραφημένων υπηρεσιών. Κάτω από αυτές τις προϋποθέσεις ο μικροελεγκτής αρκεί να δίνει μια εντολή στον επεξεργαστή κρυπτογράφησης και να περιμένει απλώς να πάρει το αποτέλεσμα από αυτόν, αφήνοντας για τον εαυτό του την εκτέλεση μόνο των απλών εντολών. Δυστυχώς δεν μπορούμε να παραθέσουμε περισσότερα στοιχεία γι' αυτούς τους μικροελεγκτές μιας που τα τεχνικά εγχειρίδια τους 'αποκρύπτονται' από τις εταιρίες κατασκευής τους ή, ορθότερα, διατίθενται μόνο εφόσον συμφωνήσουμε να μην τα φανερώσουμε σε τρίτους (Non Disclosure Agreement, NDA).

Το ίδιο ισχύει και για τον προγραμματισμό τους σε γλώσσα χαμηλού επιπέδου (συμβολική). Θα πρέπει και γι' αυτό να έχετε αποδεχθεί τους όρους της παραπάνω συμφωνίας. Για την παράκαμψη αυτού του προβλήματος όλες οι έξυπνες κάρτες που βασίζονται σε συνδυασμό μικροελεγκτή / επεξεργαστή κρυπτογράφησης υποστηρίζουν ένα εξειδικευμένο ανοικτό λειτουργικό σύστημα (OS), του οποίου το όνομα, οι εκδόσεις όπως και οι υποστηριζόμενες συναρτήσεις διαφοροποιούνται σύμφωνα με τον τύπο της κάρτας, την προέλευσή της και ...από το πόσο σύγχρονο είναι το υλικό που έχει ξεμείνει στις αποθήκες του κατασκευαστή!

Στις περισσότερες των περιπτώσεων οι κάρτες αυτές προγραμματίζονται σε γλώσσα C μέσω ενός μεταγλωττιστή με έξοδο κατάλληλη για τον χρησιμοποιούμενο μικροελεγκτή. Ανάμεσα σε όλους τους μεταγλωττιστές ξεχωρίζει ο IAR, ο οποίος δουλεύει θαυμάσια, εφόσον διαθέτετε τις βιβλιοθήκες που αντιστοιχούν στις κάρτες της επιλογής σας.

Αν μετά από όλα όσα είπαμε, αποφασίσετε να 'κτίσετε' την εφαρμογή σας πάνω σε μια τέτοια κάρτα θα πρέπει να γνωρίζετε εκ των προτέρων πως θα πρέπει να ψάξετε με υπέρμετρη επιμονή στο Διαδίκτυο για όλες τις πληροφορίες που σχετίζονται με αυτήν. Όπως θα διαπιστώσετε και εσείς τα σχετικά πρόσθετα προγράμματα, βιβλιοθήκες και εγχειρίδια φιλοξενούνται σε δικτυακούς τόπους που βρίσκονται στα όρια της νομιμότητας ή, ενδεχομένως, τα έχουν ξεπεράσει.

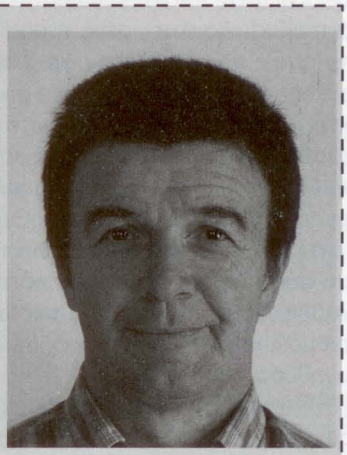
Τελειώνοντας θα πρέπει να σημειώσουμε πως οι παραπάνω κάρτες προγραμματίζονται πολύ εύκολα με τη βοήθεια ενός απλού Αναγνώστη, αρκεί βέβαια να είναι συμβατές με το πρότυπο Phoenix. Στο σχετικό άρθρο που φιλοξενείται στο ίδιο τεύχος θα δείξουμε πως μπορείτε να τις 'κάψετε' με το δικό σας πρόγραμμα.

Τελικά...

Σε αντίθεση με τις πρώτες έξυπνες κάρτες που δεν είχαν κανενός είδους προστασία και προοριζόντουσαν για γενική χρήση, όλες οι καινούργιες έχουν σχεδιαστεί με γνώμονα τη διασφάλιση και την προστασία κωδικοποιημένων υπηρεσιών. Ανεξάρτητα όμως από αυτό, μπορείτε να βρείτε κάρτες, σε όσες μεγάλες ποσότητες θέλετε, που είναι ικανές να εξυπηρετήσουν τις ανάγκες της δικής σας εφαρμογής.

(050236-1)

Λίγα λόγια για το συγγραφέα



Ο Christian Tavernier έχει σπουδάσει ηλεκτρονικά και θεωρείται σαν ένας από τους καλύτερους στο χώρο των ηλεκτρονικών, της πληροφορικής και της επιστήμης των τηλεπικοινωνιών.
Έχει γράψει επίσης πολλά βιβλία και άρθρα σε διάφορα περιοδικά με κύριο αντικείμενο τα ηλεκτρονικά και τις εφαρμογές πληροφορικής. Στους τομείς αυτούς, άλλωστε, εργάζεται εδώ και 25 χρόνια.
www.tavernier-c.com
contact@tavernier-c.com www.microchip.com

Microchip (MPLAB download):
www.microchip.com
Atmel (AVR Studio download):
www.atmel.com
ZeitControl (developer of the Basic Card):
www.zeitcontrol.de
ZeitControl (Basic Card):
www.basiccard.com
Author's general website:
www.tavernier-c.com
Author's website dedicated to chipcards only: