ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ
ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ
Π.Σ.Ε. ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΔΙΚΤΥΩΝ Η/Υ
ΕΡΓΑΣΤΗΡΙΟ ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΩΝ ΕΦΑΡΜΟΓΩΝ ΚΑΙ ΜΙΚΡΟΚΥΜΑΤΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Πτυχιακή εργασία

με θέμα

Τεχνολογία και Εφαρμογές

Έξυπνων Καρτών

από τον **Αντώνιο Καπετανάκη**.

Εκπονήθηκε υπό την επίβλεψη του Επίκουρου Καθηγητή Δρ. ***Ιωάννη Βαρδιάμπαση***

στα πλαίσια του "ΕΠΕΑΕΚ ΙΙ – Αρχιμήδης: Ενίσχυση Ερευνητικών Ομάδων στα ΤΕΙ – *Μελέτη- σχεδίαση ευφυών κεραιών με τεχνικές υπολογιστικού ηλεκτρομαγνητισμού και πιλοτική ανάπτυξη- λειτουργία ψηφιακού ραδιοφωνικού σταθμού DAB στα Χανιά (SMART-DAB)"*

Χανιά, Μάρτης 2004

Ευχαριστίες

Θα ήθελα να εκφράσω τις πιο θερμές μου ευχαριστίες στον καθηγητή μου Ιωάννη Βαρδιάμπαση για την πολύτιμη βοήθεια του και τις χρήσιμες υποδείξεις του, που κατέστησαν δυνατή την ολοκλήρωση της παρούσας εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω ιδιαίτερα τους γονείς μου Γεώργιο και Ευτυχία για τη συνεχή ηθική και οικονομική υποστήριξη όλα τα χρόνια των σπουδών μου και τα αδέλφια μου Παύλο και Σοφία.

Αντώνης Καπετανάκης
Χανιά, Μάρτης 2004

Πρόλογος

Σκοπός της παρούσας πτυχιακής εργασίας ήταν η παρουσίαση των έξυπνων καρτών (Smart Card) και των εφαρμογών τους. Στο πρώτο κεφάλαιο γίνεται μια αναφορά στις έξυπνες κάρτες, τα είδη τους και τα τεχνικά χαρακτηριστικά τους,. Στο δεύτερο γίνεται μία λεπτομερής περιγραφή του προτύπου ISO 7816. Τέλος στο τρίτο κεφάλαιο παρουσιάζονται και αναλύονται οι τηλεκάρτες.

Περιεχόμενα

Κεφάλαιο 1ο - Κατηγορίες Καρτών

Κεφάλαιο 2ο - Πρότυπο ISO 7816

Κεφάλαιο 3ο - Τηλεκάρτες

ΚΕΦΑΛΑΙΟ 1

ΚΑΤΗΓΟΡΙΕΣ ΚΑΡΤΩΝ

1.1α Η ιστορία των έξυπνων καρτών

Η χρήση των πλαστικών καρτών ξεκίνησε στις Η.Π.Α στις αρχές της δεκαετίας του 1950. Η χαμηλή τιμή του συνθετικού υλικού του PVC επέτρεψε την παραγωγή εύρωστων και με μεγάλη διάρκεια ζωής καρτών. Αυτές οι κάρτες άρχισαν να είναι περισσότερο βολικές έναντι του χαρτιού που χρησιμοποιώταν μέχρι τότε, το οποίο προφανώς δεν είναι το ίδιο ανθεκτικό, όσο οι πλαστικές κάρτες. Η πρώτη πλαστική κάρτα πληρωμής γενικού σκοπού εκδόθηκε από την Diners Club το 1950 Προοριζόταν για μια συγκεκριμένη, υψηλή, τάξη ανθρώπων και είχε τον χαρακτήρα επικύρωσης της ισχυρής οικονομικής κατάστασης. Η εισαγωγή της Visa και της MasterCard στο πεδίο, οδήγησε στην εξάπλωση της χρησιμοποίησης του πλαστικού χρήματος, αρχικά στις Η.Π.Α, με την Ευρώπη και τον υπόλοιπο κόσμο να ακολουθεί αυτή την τάση λίγα χρόνια αργότερα.

Αρχικά η λειτουργία των καρτών ήταν σχετικά τετριμμένη, καθώς αποτελούσαν φορείς δεδομένων οι οποίοι παρείχαν ασφάλεια ενάντια της πλαστογραφίας. Γενικές πληροφορίες, όπως το όνομα του κατόχου της κάρτας, ήταν τυπωμένες πάνω στην επιφάνεια της, ενώ τα προσωπικά δεδομένα του κατόχου της και ο αριθμός της, ήταν σε ανάγλυφη μορφή. Επιπλέον πολλές κάρτες είχαν ένα πεδίο προκειμένου ο κάτοχος της κάρτας να έχει την δυνατότητα να υπογράφει.Οι κάρτες που μόλις περιγράψαμε ήταν αυτές της πρώτης γενιάς, και παρείχαν προστασία κατά της πλαστογραφίας μέσω μεθόδων που κυρίως ήταν εμφανείς, δηλαδή μέσω του πεδίου της υπογραφής και των εκτυπωμένων πεδίων που περιγράψαμε. Άρα η ασφάλεια του συστήματος είχε να κάνει κυρίως με την ποιότητα του και την ευσυνειδησία του υπαλλήλου που δεχόταν ή όχι, τις κάρτες αυτού του είδους. Αρχικά αυτό δεν ήταν τόσο μεγάλο πρόβλημα, αφού οι κάρτες ήταν λίγες σε αριθμό, ωστόσο καθώς η χρησιμοποίηση των καρτών γινόταν μεγαλύτερη, μεγαλύτερος γινόταν και ο κίνδυνος για κακόβουλη χρήση της κάρτας κάνοντας επιτακτική την ανάγκη ύπαρξης μεθόδων ασφάλειας.

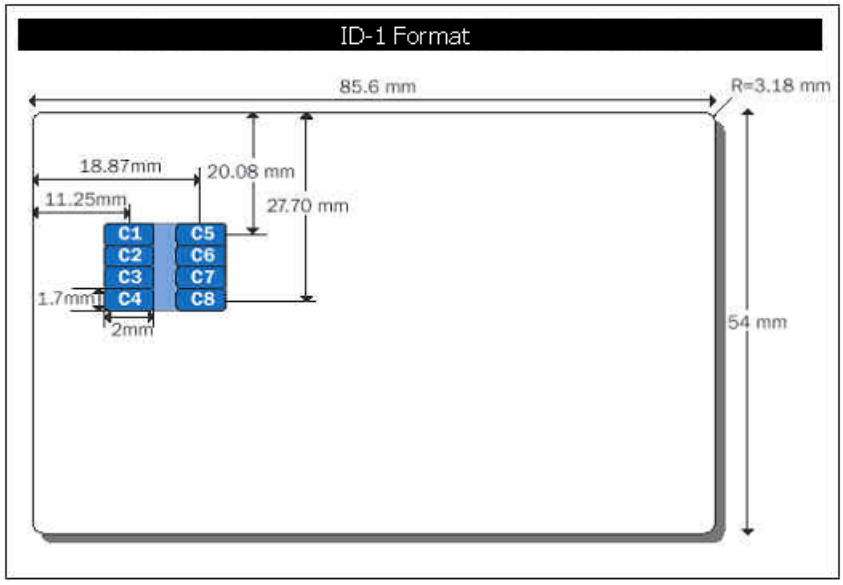
1.1β Τύποι καρτών

Αυτή η ενότητα έχει σαν σκοπό την παρουσίαση διαφόρων τύπων καρτών, που ωστόσο έχουν τα ίδια φυσικά χαρακτηριστικά, όπως την ευλυγισία, την αντίσταση σε διάφορες συνθήκες θερμοκρασίας, και συγκεκριμένες διαστάσεις. ΄Ολοι οι τύποι ανήκουν στο πλαίσιο μιας συγκεκριμένης μορφής την οποία καλούμε [ID-1 format] και είναι ορισμένη από το [ISO standard 7810].

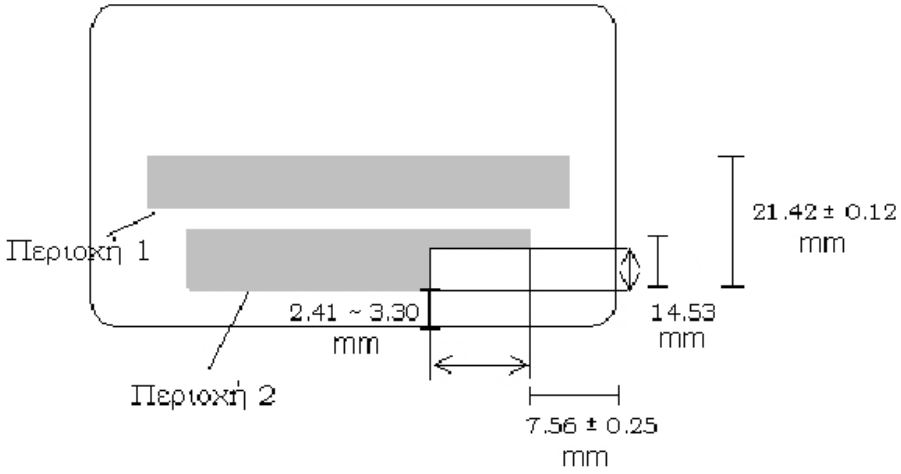
1.1.1 Ανάγλυφες Κάρτες

Η ανάγλυφη μορφή, είναι η παλιότερη τεχνική για την εφαρμογή αναγνωρίσιμων από μηχάνημα στιγμάτων, *Machine-readable markings* για την αναγνώριση της ταυτότητας των καρτών.

Οι ανάγλυφοι χαρακτήρες στην κάρτα μπορούν να μεταφερθούν σε χαρτί χρησιμοποιώντας απλές και οικονομικές συσκευές. Η οπτική ανάγνωση της ανάγλυφης μορφής είναι πολύ απλή και η φύση και η τοπολογία της θέσης των ανάγλυφων χαρακτήρων καθορίζονται από το [ISO standard 7811, Identification Cards - Recording Technique].



Σχήμα 1.1: Η μορφή τουID-1format



Σχήμα 1.2: Οι ανάγλυφες περιοχές σύμφωνα με το ISO 7811-3

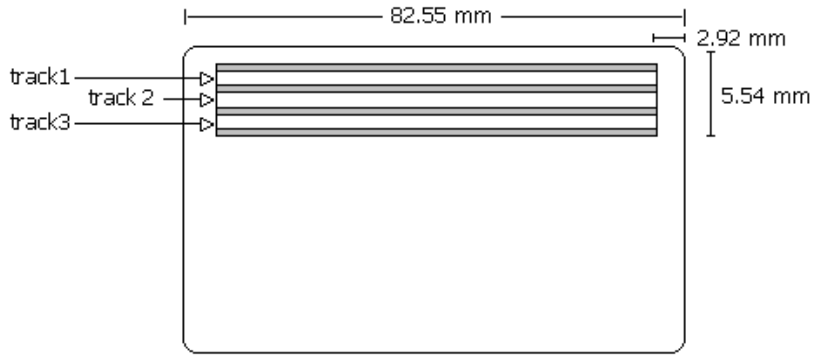
Το [ISO 7811 Part 1] καθορίζει τις απαιτήσεις για τους ανάγλυφους χαρακτήρες, όπως για παράδειγμα την μορφή τους, το μέγεθος τους και διάφορα άλλα χαρακτηριστικά. Το τρίτο τμήμα [ISO 7811 Part 3] ορίζει την ακριβή θέση των χαρακτήρων στην κάρτα, και ορίζει επίσης δύο ξεχωριστές περιοχές. Η πρώτη περιοχή διατηρείται για την τοποθέτηση του Αριθμού Αναγνώρισης της Κάρτας, Identification Card Number το οποίο θα ταυτοποιεί τόσο την κάρτα όσο και τον χρήστη αυτής. Η δεύτερη περιοχή διατηρείται για επιπλέον δεδομένα που αφορούν τον ιδιοκτήτη της κάρτας, όπως για παράδειγμα το όνομα και τη διεύθυνση. Από πρώτη ματιά, η μεταφορά δεδομένων

με αποτύπωση ανάγλυφων χαρακτήρων μπορεί να φαίνεται πρωτόγονη, ωστόσο η απλότητα της την έκανε αποδεκτή ακόμα και σε τεχνολογικά εξελιγμένες χώρες.

1.1.2 Κάρτες με μαγνητική ταινία

Το ουσιαστικό πρόβλημα των ανάγλυφων καρτών είναι ότι δημιουργούν ένα μεγάλο αριθμό από χάρτινες αποδείξεις, οι οποίες είναι δύσκολο να επεξεργαστούν. Μια λύση σε αυτό το θέμα είναι η ψηφιακή κωδικοποίηση των δεδομένων της κάρτας σε μια μαγνητική ταινία η οποία βρίσκεται στο πίσω μέρος της κάρτας. Η μαγνητική ταινία διαβάζεται με το να τη διαπεράσουμε κατά μήκος μιας κεφαλής ανάγνωσης, είτε με μηχανικό, είτε με αυτόματο τρόπο. Η επεξεργασία αυτή δεν απαιτεί την χρήση χαρτιού.

Τα μέρη [ISO 7811 2, 3, 4] καθορίζουν τις ιδιότητες μιας μαγνητικής κάρτας, τις τεχνικές κωδικοποίησης, και την θέση των μαγνητικών ταινιών. Η μαγνητική ταινία μπορεί να περιέχει μέχρι τρεις τομείς, tracks Οι τομείς (1) και (2) είναι καθορισμένοι έτσι ώστε να έχουν μόνο δυνατότητα ανάγνωσης, ενώ ο τομέας (3) έχει και δικαιώματα γραφής. Ακόμα και αν η αποθηκευτική δυνατότητα μιας μαγνητικής ταινίας είναι περίπου 1000 bits, κάτι το οποίο δεν είναι πολύ, είναι ωστόσο υπεραρκετό για την αποθήκευση των στοιχείων που υπάρχουν στις ανάγλυφες κάρτες. Επιπλέον τα δεδομένα μπορούν να γραφούν ή να διαβαστούν στον τρίτο τομέα, όπως για παράδειγμα η τελευταία, πιο πρόσφατη, δοσοληψία που έλαβε χώρα στο τρέχον χρονικό διάστημα της ζωής της κάρτας.



Σχήμα 1.3: Οι περιοχές των μαγνητικών ταινιών σε κάρτα του [ID-1 format]

Το κύριο αρνητικό στοιχείο της τεχνολογίας της μαγνητικής ταινίας είναι ότι τα αποθηκευμένα δεδομένα μπορούν πολύ εύκολα να αλλαχτούν κακοβούλως. Η περίπτωση της πλαστογραφίας μιας ανάγλυφης κάρτας απαιτεί τουλάχιστον ένα σημαντικό ποσοστό επιδεξιότητας, μπορεί όμως εύκολα να γίνει αντιληπτή από ένα έμπειρο και εκπαιδευμένο μάτι. Η αλλαγή των κωδικοποιημένων δεδομένων σε μια μαγνητική ταινία είναι σχετικά εύκολη να γίνει με την χρησιμοποίηση μιας απλής, standard read/write μηχανής, και είναι πολύ δύσκολο στην συνέχεια και αφού η διαδικασία αλλαγής έχει πραγματοποιηθεί, να αποδείξει κάποιος ότι τα δεδομένα δεν είναι τα σωστά. Επιπλέον, οι μαγνητικές κάρτες συχνά χρησιμοποιούνται σε αυτοματοποιημένα

συστήματα στα οποία η οπτική επιθεώρηση είναι αδύνατη, όπως για παράδειγμα στις Αυτόματες Ταμιακές Μηχανές. Ο ενδεχόμενος αντίπαλος ο οποίος έχει λάβει σωστά δεδομένα από την κάρτα, μπορεί εύκολα να χρησιμοποιεί διπλές, duplicated κάρτες σε χωρίς επίβλεψη μηχανές, χωρίς να χρειάζεται να πλαστογραφήσει οπτικά στίγματα ασφαλείας. Οι κατασκευαστές αυτού του είδους καρτών χρησιμοποιούν διάφορα μέσα προκειμένου να μπορούν να προστατεύουν τα δεδομένα που υπάρχουν στην μαγνητική ταινία από την πλαστογραφία. Για παράδειγμα, οι κάρτες German Eurocheck περιέχουν ένα αόρατο και χωρίς την δυνατότητα αλλαγής, unaltered κώδικα στο σώμα της κάρτας, ο οποίος καθιστά αδύνατη την αλλοίωση ή αναπαραγωγή της μαγνητικής ταινίας. Ωστόσο, αυτή όπως και άλλες τεχνικές απαιτούν ένα ειδικό αισθητήρα, *sensor* στο τερματικό της κάρτας, το οποίο αυξάνει αρκετά το κόστος.

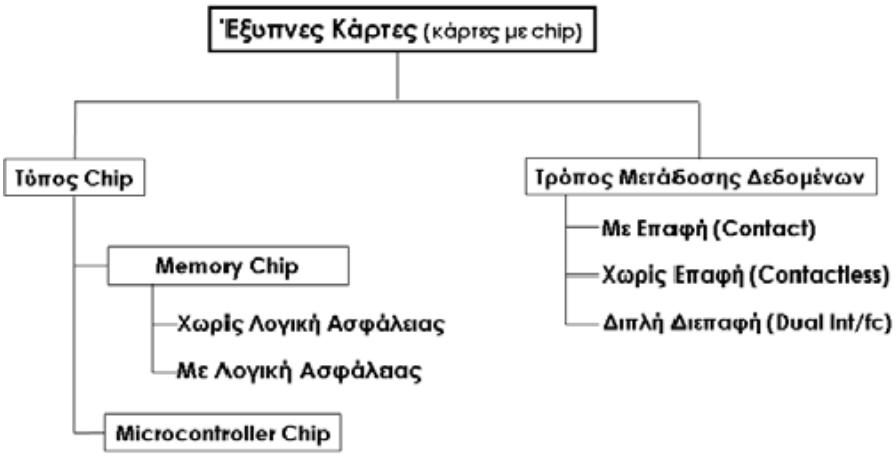
1.1.3 Έξυπνες κάρτες

Οι έξυπνες κάρτες είναι το νεότερο και το πιο εξελιγμένο μέλος της οικογένειας καρτών ταυτοποίησης του [ID-1 format]. Το χαρακτηριστικό τους στοιχείο είναι η ύπαρξη ενός ολοκληρωμένου κυκλώματος πάνω στην κάρτα, το οποίο έχει στοιχεία για μετάδοση, αποθήκευση, και επεξεργασία δεδομένων. Η μετάδοση δεδομένων μπορεί να πραγματοποιηθεί είτε μέσω επαφών που βρίσκονται πάνω στην επιφάνεια της κάρτας, είτε μέσω ηλεκτρομαγνητικού πεδίου, χωρίς την χρήση τέτοιων επαφών. Οι έξυπνες κάρτες προσφέρουν ένα αριθμό πλεονεκτημάτων σε σύγκριση με τις κάρτες μαγνητικής ταινίας. Για παράδειγμα, η μέγιστη αποθηκευτική ικανότητα μιας έξυπνης κάρτας είναι πολλές φορές μεγαλύτερη από αυτή μιας κάρτας με μαγνητική ταινία. Ολοκληρωμένα κυκλώματα με αποθηκευτική ικανότητα πάνω από 32 KBytes μνήμης είναι διαθέσιμα στην αγορά με τάση να αυξάνονται αρκετά με την πάροδο του χρόνου. Μόνο οι οπτικές κάρτες που θα αναφέρουμε στην επόμενη ενότητα έχουν τη δυνατότητα μεγαλύτερης αποθηκευτικής ικανότητας. Ωστόσο, ένας από τους πιο σημαντικούς παράγοντες για τον οποίο οι έξυπνες κάρτες υπερτερούν έναντι όλων των άλλων τύπων καρτών είναι το γεγονός ότι τα αποθηκευμένα δεδομένα μπορούν να προστατεύονται από τη μη εξουσιοδοτημένη πρόσβαση και την πλαστογραφία. Καθώς η πρόσβαση στα δεδομένα λαμβάνει χώρα μόνο από μια σειριακή διεπαφή η οποία ελέγχεται από ένα λειτουργικό σύστημα και λογική ασφάλειας, είναι δυνατόν να εγγραφούν εμπιστευτικά δεδομένα στην κάρτα, έτσι ώστε να μην μπορούν ποτέ να διαβαστούν από τον έξω κόσμο. Αυτά τα εμπιστευτικά δεδοδένα μπορεί κανείς να τα επεξεργαστεί μόνο εσωτερικά από την υπολογιστική μονάδα. Οι λειτουργίες της μνήμης της εγγραφής, ανάγνωσης, και διαγραφής μπορούν να περιοριστούν σε συγκεκριμένους όρους τόσο από την μεριά του υλικού όσο και από την μεριά του λογισμικού. Αυτό επιτρέπει την ανάπτυξη και τον σχεδιασμό πλήθους μηχανισμών ασφάλειας, οι οποίοι μπορούν να προσαρμοστούν στις ειδικές ρυθμίσεις συγκεκριμένων εφαρμογών. Το γεγονός αυτό μαζί με τη δυνατότητα του υπολογισμού κρυπτογραφικών αλγορίθμων επιτρέπει την χρησιμοποίηση των έξυπνων καρτών στη σχεδίαση και ανάπτυξη ασφαλών εφαρμογών οι οποίες μπορούν να εφαρμοστούν σε κάθε περίπτωση. Επιπλέον, τα πλεονεκτήματα των έξυπνων καρτών έχουν να κάνουν με την υψηλό βαθμό αξιοπιστίας που προσφέρουν, και την μεγάλη διάρκεια ζωής που

διαθέτουν σε σύγκριση με αυτή των μαγνητικών καρτών. Οι έξυπνες κάρτες μπορούν να χωριστούν σε δύο σύνολα, ανάλογα με τις διαφορές στη λειτουργία και στην τιμή:

- Κάρτες Μνήμης, *memory cards*
- Κάρτες με μικροεπεξεργαστή, *microprocessor cards*

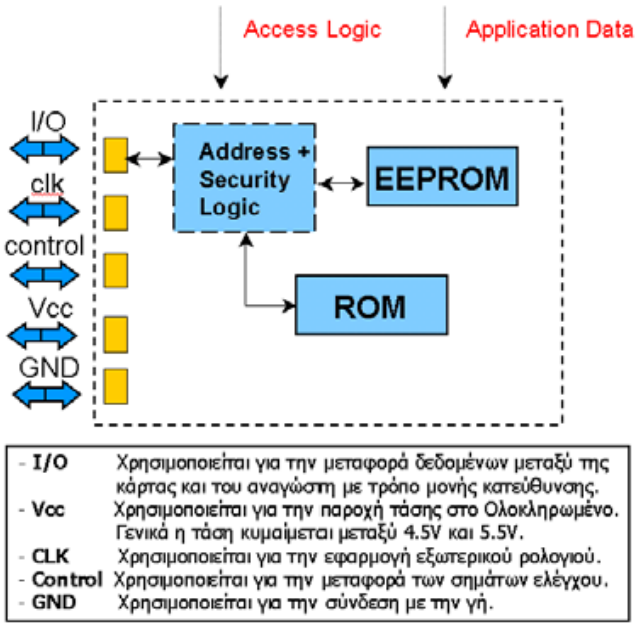
Δίνουμε και έναν πίνακα ταξινόμησης της παραπάνω διάκρισης:



Σχήμα 1.4: Ταξινόμηση έξυπνων καρτών

1.1.4 Κάρτες μνήμης

Το σχήμα που παρουσιάζουμε στη συνέχεια περιγράφει τη δομή του αρχιτεκτονικού διαγράμματος μιας κάρτας μνήμης.



Σχήμα 1.5: Το block διάγραμμα μιας κάρτας μνήμης.

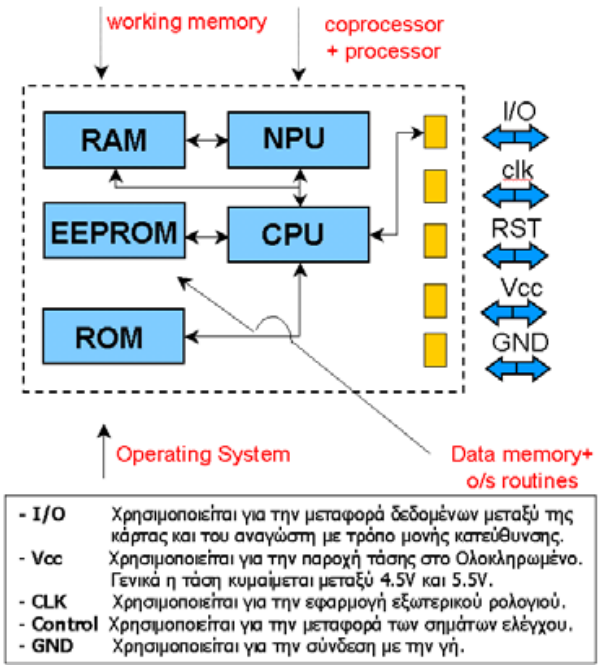
Τα δεδομένα που απαιτούνται για την εφαρμογή, αποθηκεύονται στην μνήμη, η οποία είναι συνήθως η μνήμη EEPROM. Η πρόσβαση στην μνήμη ελέγχεται από μια μονάδα έλεγχου λογικής,

security logic η οποία στην πιο απλή περίπτωση αποτελείται μόνο από προστασία γραφής ή διαγραφής για όλη ή για κάποιες περιοχές της μνήμης. Ωστόσο υπάρχουν και κυκλώματα τα οποία περιέχουν πιο περίπλοκες δομές ασφάλειας, και τα οποία μπορούν να εκτελέσουν απλές κρυπτογραφικές λειτουργίες. Τα δεδομένα μεταφέρονται από και προς την κάρτα μέσω του I/O Iport. Το τρίτο τμήμα [Part 3] του [ISO 7816] πρωτοκόλλου ορίζει έναν ειδικό σύγχρονο τρόπο μεταφοράς ο οποίος επιτρέπει την ανάπτυξη απλών και οικονομικών κυκλωμάτων. Ωστόσο κάποιες κάρτες χρησιμοποιούν το I^2C bus το οποίο χρησιμοποιείται κυρίως σε συνδυασμό με σειριακής πρόσβασης μνήμες. Οι λειτουργίες μιας κάρτας μνήμης είναι βέλτιστες για μια συγκεκριμένη εφαρμογή. Αν και αυτό περιορίζει την ευελιξία, τις καθιστά πιο οικονομικές. Οι κάρτες μνήμης χρησιμοποιούνται κυρίως για προπληρωμένες τηλεφωνικές συνδιαλέξεις, και κάρτες ασφάλειας υγείας.

1.1.5 Κάρτες με μικροεπεξεργαστή

Η καρδιά του κυκλώματος σε μία κάρτα με μικροεπεξεργαστή, όπως φαίνεται και από το όνομα της, είναι ένας επεξεργαστής, ο οποίος περιβάλλεται από τέσσερις επιπλέον λειτουργικές μονάδες οι οποίες είναι:

- ROM. Αυτή η μνήμη περιλαμβάνει το λειτουργικό σύστημα του κυκλώματος, το οποίο γίνεται *burned in* κατά την κατασκευή του κυκλώματος. Το περιεχόμενο της ROM είναι πανομοιότυπο για κάθε κύκλωμα κάθε παραγωγικού κύκλου και δεν μπορεί να αλλάξει κατά τη διάρκεια της ζωής του κυκλώματος.
- EEPROM. Αυτή η μνήμη είναι η διαρκής, *non volatile* μνήμη. Τα δεδομένα και ο κώδικας του προγράμματος μπορεί να γραφούν και να διαβαστούν από αυτή τη μνήμη, κάτω από τον έλεγχο του λειτουργικού συστήματος.
- RAM. Η μνήμη αυτή είναι η μνήμη εργασίας του επεξεργαστή. Είναι *volatile* μνήμη και όλα τα δεδομένα χάνονται όταν χαθεί και η τροφοδοσία του ρεύματος προς το κύκλωμα.
- I/O port. Η σειριακή I/O διεπαφή συνήθως αποτελείται από ένα καταχωρητή, δια μέσω του οποίου τα δεδομένα μεταφέρονται με ένα δυαδικό ψηφίο την φορά.



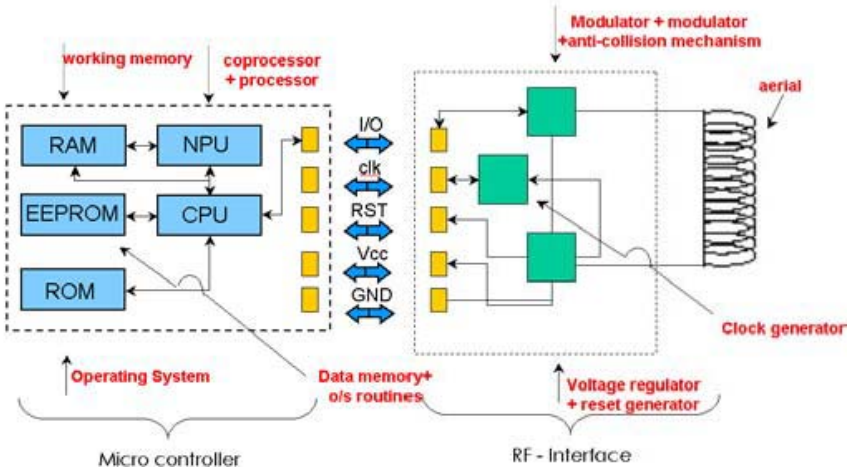
Σχήμα 1.6: Το *block* διάγραμμα μιας κάρτας με μικροεπεξεργαστή.

Οι κάρτες με μικροεπεξεργαστή είναι πολύ ευέλικτες στην χρήση. Στην πιο απλή περίπτωση περιέχουν ένα βελτιστοποιημένο πρόγραμμα για μια εφαρμογή, κι έτσι μπορούν να χρησιμοποιηθούν μόνο για τη δεδομένη εφαρμογή. Ωστόσο, το λειτουργικό σύστημα των σύγχρονων καρτών επιτρέπει την ενσωμάτωση πολλών διαφορετικών εφαρμογών σε μια κάρτα. Στην περίπτωση αυτή η ROM περιέχει μόνο βασικές εντολές του λειτουργικού συστήματος, και το ειδικό τμήμα για την εφαρμογή του προγράμματος φορτώνεται στην EEPROM αφού η κάρτα έχει κατασκευαστεί. Ειδικά βελτιστοποιημένα κυκλώματα με υψηλές δυνατότητες επεξεργασίας και μεγάλη αποθηκευτική ικανότητα έχουν αναπτυχθεί προκειμένου να εκτελούν υψηλής απόδοσης εφαρμογές με ανάγκη για υψηλή ασφάλεια και υπολογισμό περίπλοκων κρυπτογραφικών αλγορίθμων.

1.1.6 Έξυπνες κάρτες χωρίς επαφή

Οι έξυπνες κάρτες με επαφή συμμορφώνονται με τα πρότυπα του [standard ISO 7816 part 1]. Η αξιοπιστία των καρτών αυτών αυξάνεται συνεχώς με την πάροδο των ετών, εξαιτίας της αυξανόμενης εμπειρίας στον χώρο των κατασκευών τέτοιου είδους καρτών. Ένα χαρακτηριστικό παράδειγμα είναι το γεγονός ότι ο ρυθμός βλαβών των καρτών τηλεφωνικών συνδιαλέξεων, έναντι στην αναμενόμενη διάρκεια ζωής τους, που είναι ένας χρόνος, είναι κάτω του 0.1%. Ωστόσο, η επαφή παραμένει ένας από τους βασικότερους λόγους των πιο συχνών αιτιών βλαβών στα ηλεκτρομηχανικά συστήματα, καθώς οι βλάβες προκύπτουν κυρίως από τη φθορά των επαφών. Στα μη σταθερά συστήματα, οι δονήσεις μπορούν να προκαλέσουν σύντομες μη ολοκληρωμένες φορτίσεις, και αφού οι επαφές βρίσκονται στην επιφάνεια της κάρτας και συνδέονται απευθείας στις εισόδους δεδομένων του ολοκληρωμένου κυκλώματος της κάρτας, ο κίνδυνος καταστροφής ή βλάβης του ολοκληρωμένου κυκλώματος λόγω ηλεκτροστατικών αποφορτίσεων -φορτίσεων μερικών χιλιάδων volts είναι πολύ μεγάλος. Αυτά τα προβλήματα τεχνικού είδους αποφεύγονται με την χρησιμοποίηση έξυπνων καρτών χωρίς επαφή. Εκτός των τεχνικών πλεονεκτημάτων που

υπάρχουν, η τεχνολογία των έξυπνων καρτών χωρίς επαφή, προσφέρει τόσο στον κατασκευαστή όσο και στον ιδιοκτήτη της κάρτας πληθώρα νέων ενδεχόμενων εφαρμογών. Για παράδειγμα, οι έξυπνες κάρτες χωρίς επαφή δεν χρειάζεται να εισαχθούν σε τερματικό αναγνώστη, αφού είναι συστήματα που λειτουργούν έως και ένα μέτρο μακριά. Αυτό είναι ένα πολύ σημαντικό πλεονέκτημα σε σύστημα ελέγχου πρόσβασης access control. Έτσι για παράδειγμα μία πόρτα που χρειάζεται να ανοίξει, πλέον μπορεί να ανοίξει χωρίς το άτομο το οποίο επιθυμεί την πρόσβαση να χρειάζεται να βγάλει από την τσέπη του ή το πορτοφόλι του την κάρτα, αφού δεν απαιτείται η εισαγωγή της κάρτας σε κάποιο μηχάνημα ανάγνωσης. Μια άλλη επεκταμένη εφαρμογή για αυτή την τεχνολογία είναι αυτή της τοπικής δημόσιας συγκοινωνίας, κατά την οποία ένας μεγάλος αριθμός ανθρώπων χρειάζεται να αναγνωρισθεί στο μικρότερο δυνατό χρόνο. Ωστόσο,η ασύρματη τεχνολογία έχει πλεονέκτημα ακόμα και στην περίπτωση συστημάτων που απαιτούν την αναγκαστική εισαγωγή της κάρτας στον αναγνώστη, αφού ο τρόπος εισαγωγής δεν παίζει κανένα ρόλο. Αυτό έρχεται σε αντίθεση με τις μαγνητικές κάρτες, ή τις κάρτες με επαφή, οι οποίες πρέπει να εισάγονται με συγκεκριμένο τρόπο στο μηχάνημα του αναγνώστη. Έτσι η ελευθερία που προσφέρουν έναντι στους περιορισμούς που θέτουν οι άλλες μορφές καρτών αυξάνει τη λειτουργικότητα των καρτών χωρίς επαφή και συνεπώς την αποδοχή τους από τους απλούς χρήστες.



Σχήμα 1.7: Το *block* διάγραμμα μιας έξυπνης κάρτας χωρίς επαφή.

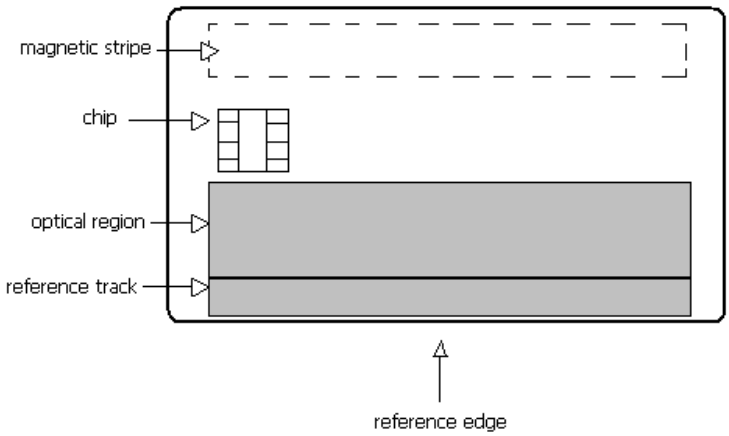
Μια επιπλέον ενδιαφέρουσα παραλλαγή στην χρήση καρτών χωρίς επαφή, σχετίζεται με την χρήση ενός τερματικού επιφάνειας. Σε αυτή την περίπτωση η κάρτα δεν εισάγεται σε κάποια υποδοχή του τερματικού, αλλά απλά εφάπτεται στη μαρκαρισμένη επιφάνεια ενός αναγνώστη. Εκτός της ευκολίας χρήσης, αυτή η λύση είναι ενδιαφέρουσα καθώς έχει την ιδιότητα να αποφεύγει τυχόν βανδαλισμούς, όπως για παράδειγμα την εισαγωγή κόλλας ή άλλων κολλοειδών ουσιών στην υποδοχή του αναγνώστη. ΄Οσον αφορά την εμπορική εκμετάλλευση των καρτών χωρίς επαφή, υπάρχει το πλεονέκτημα ότι κανένα τεχνικό στοιχείο, *technical element* δεν είναι εμφανές στην επιφάνεια της κάρτας, και έτσι ο οπτικός σχεδιασμός τέτοιων καρτών δεν περιορίζεται από μαγνητικές ταινίες ή επιφανειακές επαφές. Μέχρι τη δεδομένη στιγμή οι κάρτες αυτές χρησιμοποιούνται κυρίως για την τοπική συγκοινωνία, όπου λειτουργούν σαν εισιτήρια. Τα

σημερινά συστήματα χρησιμοποιούν κάρτες μιας κύριας λειτουργίας, για την οποία έχουν αναπτυχθεί κυκλώματα με οικονομική λογική. Ωστόσο υπάρχουν σημαντικά δείγματα ότι οι κάρτες με πολυλειτουργικότητα θα γίνουν σύντομα οι αντικαταστάτες των ήδη υπαρχόντων, σχετικά απλών, καρτών.

1.1.7 Οπτικές κάρτες μνήμης

Στις εφαρμογές στις οποίες η αποθηκευτική ικανότητα που απαιτείται είναι μεγαλύτερη από αυτή που μπορούν να προσφέρουν οι έξυπνες κάρτες, έχουμε τη χρησιμοποίηση οπτικών καρτών μνήμης, οι οποίες μπορούν να αποθηκεύσουν ένα μεγάλο ποσό από *megabytes* δεδομένων. Ωστόσο, με την υπάρχουσα τεχνολογία αυτές οι κάρτες μπορούν να εκτελούν εγγραφές μόνο μια φορά και δεν μπορούν να διαγραφούν.

Το [ISO/IEC 11 693-94] καθορίζει τις διαστάσεις και τα φυσικά χαρακτηριστικά των οπτικών καρτών, καθώς και την τεχνική εγγραφής δεδομένων. Ο συνδυασμός της υψηλής αποθηκευτικής ικανότητας των οπτικών καρτών με την ευφυΐα των έξυπνων καρτών έχει ως αποτέλεσμα νέα ενδιαφέροντα χαρακτηριστικά. Για παράδειγμα τα δεδομένα μπορούν να γραφούν κρυπτογραφημένα σε μία οπτική κάρτα, ενώ το ιδιωτικό κλειδί είναι ασφαλώς αποθηκευμένο στην μνήμη του κυκλώματος της κάρτας. Έτσι τα δεδομένα της οπτικής κάρτας είναι προστατευμένα από αναρμόδια πρόσβαση. Παραθέτουμε την μορφή μιας τέτοιας κάρτας, δηλαδή μιας οπτικής έξυπνης κάρτας , στο παρακάτω σχήμα.



Σχήμα 1.8: Μορφή μιας οπτικής έξυπνης κάρτας.

1.2 Ο κύκλος ζωής μιας έξυπνης κάρτας

Όπως ήδη έχουμε αναφέρει κάθε έξυπνη κάρτα περιέχει στο εσωτερικό της ένα λειτουργικό σύστημα, το οποίο μπορεί να περιέχει έναν αριθμό αναγνώρισης ταυτότητας της κάρτας *Identification Card Number,* ο οποίος είναι μοναδικά ορισμένος και τον τοποθετεί ο κατασκευαστής,

ένα σειριακό αριθμό, πληροφορίες για το προφίλ και άλλα. Επίσης, η περιοχή του συστήματος μπορεί να περιέχει διαφορετικά κλειδιά ασφάλειας, όπως το κλειδί του κατασκευαστή, ή το κλειδί της κατασκευής *fabrication key* και το κλειδί της ταυτοποίησης *personalisation key*. Όλες αυτές οι πληροφορίες πρέπει να διατηρηθούν κρυφές και να μην αποκαλυφθούν σε ξένα πρόσωπα. Η παραγωγή μιας ΄Εξυπνης κάρτας χωρίζεται σε διαφορετικά στάδια, τα οποία είναι πέντε στον αριθμό και παρουσιάζονται παρακάτω:

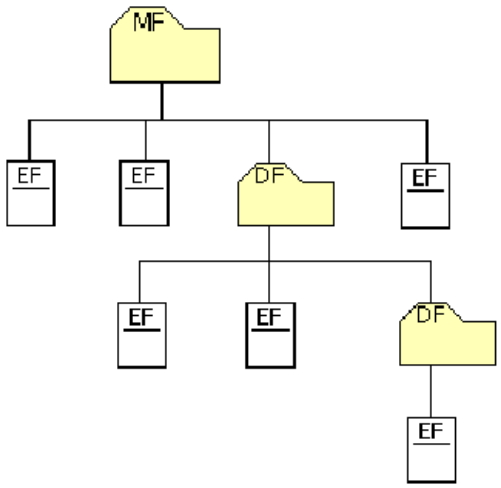
- Φάση Κατασκευής: Αυτή η φάση υλοποιείται από τους κατασκευαστές του κυκλώματος και ελέγχεται κατά τη διάρκεια αυτής της φάσης. ΄Ενα κλειδί κατασκευής *fabrication key* (fk), προστίθεται στο κύκλωμα για να προστατεύσει από πλαστή τροποποίηση μέχρι να συναρμολογηθεί στην πλαστική υποστήριξη της κάρτας. Το fk κάθε κυκλώματος είναι μοναδικό και προέρχεται από ένα κύριο κλειδί κατασκευαστή *master manufacturer key*. Αλλα δεδομένα της συναρμολόγησης θα γραφτούν στο ολοκληρωμένο κύκλωμα στο τέλος αυτής της φάσης.
- Φάση Προ-Προσωποποίησης: Η φάση αυτή υλοποιείται από τους προμηθευτές των καρτών. Κατά τη διάρκεια αυτής της φάσης το κύκλωμα θα επικολληθεί στην πλαστική κάρτα η οποία μπορεί να περιέχει και το σήμα του παροχέα υπηρεσιών. Η σύνδεση μεταξύ του κυκλώματος και του τυπωμένου κυκλώματος θα πραγματοποιηθεί και όλη η μονάδα θα ελεγχθεί. Για επιπλέον ασφάλεια και για την ασφαλή μετάβαση της κάρτας το κλειδί της κατασκευής θα αντικατασταθεί από το κλειδί προσωποποίησης *personalization key*. Μετά από αυτό η ασφάλεια της προσωποποίησης V_{PER} θα γραφεί προκειμένου να εμποδίσει τυχόν μετατροπή του κλειδιού προσωποποίησης. Επιπλέον, η πρόσβαση στην φυσική μνήμη θα γίνει ανενεργή. Η πρόσβαση θα γίνεται μόνο χρησιμοποιώντας διευθυνσιοδότηση λογικής μνήμης, προκειμένου να αποφεύγεται η πρόσβαση στην περιοχή κατασκευής *fabrication area*.
- Φάση Προσωποποίησης: Αυτή η φάση ολοκληρώνεται από τους εκδότες της κάρτας και είναι η φάση κατά την οποία ολοκληρώνεται η δημιουργία των λογικών δομών δεδομένων. Τα περιεχόμενα των αρχείων δεδομένων και των δεδομένων εφαρμογών γράφονται στην κάρτα. Το PIN, και unblocking PIN θα αποθηκευτούν στην κάρτα. Τέλος μια ασφάλεια χρησιμοποίησης V_{UTIL} θα γραφεί προκειμένου να δείξει ότι η κάρτα βρίσκεται στην φάση χρησιμοποίησης, *utilisation phase*.
- Φάση Χρησιμοποίησης: Αυτή είναι η φάση κανονικής λειτουργίας της κάρτας από τον χρήστη. ΄Ολα τα ενεργά μέρη της κάρτας βρίσκονται σε λειτουργία.
- Φάση Απενεργοποίησης: Υπάρχουν δύο τρόποι για να φτάσει μια κάρτα σε αυτό το στάδιο. Ο ένας τρόπος έχει να κάνει με την εφαρμογή η οποία γράφει μια ασφάλεια απενεργοποίησης σε ένα ξεχωριστό αρχείο ή στο Master αρχείο, απενεργοποιώντας έτσι όλες τις δυνατές λειτουργίες της κάρτας. Η μόνη λειτουργία που παραμένει ενεργή είναι αυτή της ανάγνωσης. Ο άλλος τρόπος είναι να τεθεί η κάρτα σε αυτήν την φάση, όταν το σύστημα ελέγχου κλειδώνει αμετάκλητα την πρόσβαση και στη συνέχεια το PIN όσο και το Unblocking PIN μπλοκάρονται έτσι ώστε καμιά λειτουργία να μη μπορεί να εκτελεστεί.

1.3 Λογική δομή και έλεγχος πρόσβασης έξυπνων καρτών

Όταν μια κάρτα διανέμεται σε ένα καταναλωτή από τον παροχέα εφαρμογών, η ασφάλεια της κάρτας ελέγχεται κυρίως από λειτουργικό σύστημα της εφαρμογής. Η κατάσταση φυσικής διευθυνσιοδότησης δεν είναι πλέον διαθέσιμη. Η πρόσβαση στα δεδομένα πρέπει να γίνει μέσω της λογικής δομής αρχείων της κάρτας. Αυτή η ενότητα θα ασχοληθεί με το πως το λειτουργικό σύστημα επιτυγχάνει την προστασία ασφάλειας των δεδομένων που αποθηκεύονται στην κάρτα με το να εξετάζει την λογική δομή αρχείων και το σχετικό έλεγχο πρόσβασης της κάρτας.

1.4 Λογική δομή αρχείων

Γενικά, όσον αφορά την αποθήκευση δεδομένων, μια έξυπνη κάρτα μπορεί να θεωρηθεί σαν ένας σκληρός δίσκος όπου τα αρχεία είναι οργανωμένα σε ιεραρχική δομή μέσω καταλόγων. Όπως με το λειτουργικό σύστημα MS-DOS υπάρχει μόνο ένας κύριος κατάλογος ο οποίος είναι σαν τον root κατάλογο. Κάτω από το root κατάλογο, έχουμε διαφορετικά αρχεία τα οποία αποκαλούμε στοιχειώδη EFs αρχεία και ποικίλους υποκαταλόγους, τους οποίους καλούμε στοιχειώδεις. Η κύρια διαφορά του συστήματος αρχείων της έξυπνης κάρτας και του MS-DOS έγκειται στο ότι τα αφιερωμένα αρχεία της έξυπνης κάρτας μπορούν να περιέχουν δεδομένα. Παρακάτω δίνουμε σχηματικά την μορφή του συστήματος αρχείων της έξυπνης κάρτας.



Σχήμα 1.9: Μορφή του λογικού συστήματος αρχείων μιας έξυπνης κάρτας

Στην ορολογία έξυπνων καρτών, η ρίζα ή το κύριο αρχείο Master File, MF εκτός από το μέρος επικεφαλίδων που περιέχει, περιλαμβάνει και τις επικεφαλίδες όλων των αφιερωμένων αρχείων και στοιχειωδών αρχείων που περιέχουν το κύριο αρχείο στη γονική τους ιεραρχία. Το αφιερωμένο αρχείο DF είναι μια λειτουργική ομαδοποίηση των αρχείων που αποτελείται από τον εαυτό και όλα τα αρχεία που είναι άμεσα παιδιά του. Το στοιχειώδες αρχείο EF αποτελείται απλά από την επικεφαλίδα του και το σώμα που καταχωρεί τα στοιχεία Οι τρόποι με τους οποίους τα δεδομένα ρυθμίζονται μέσα σε ένα αρχείο διαφέρουν, και εξαρτώνται από τα διαφορετικά λειτουργικά συστήματα που χρησιμοποιούνται. Μερικοί από τους τρόπους με τους οποίους τα δεδομένα

μπορούν να διαχειριστούν είναι, απλά μέσω του offset και του μήκους, ενώ άλλα μπορούν να οργανώσουν τα δεδομένα τους σε σταθερά ή μεταβλητά μήκη αρχείων όπως το [Global System Mobile Communication]. Κάθε μια από αυτές τις περιπτώσεις απαιτεί το αρχείο να πρέπει να επιλεχθεί πριν εκτελεστεί οποιαδήποτε άλλη λειτουργία. Οι λογικοί μηχανισμοί πρόσβασης και επιλογής ενεργοποιούνται αφότου διοχετευτεί ρεύμα στην κάρτα ενώ το κύριο αρχείο επιλέγεται αυτόματα. Η λειτουργία επιλογής επιτρέπει τη μετακίνηση γύρω από το δέντρο. Μπορεί να είναι κίνηση πτωτική με την επιλογή ενός από το EF ή DF ή μπορεί να είναι κίνηση προοδευτική με την επιλογή ενός MF ή DF Η οριζόντια μετακίνηση μπορεί να γίνει με την επιλογή ενός EF. Μετά από την επιτυχία της επιλογής, η επικεφαλίδα του αρχείου μπορεί να ανακτηθεί, και η ανάκτηση της θα μπορέσει να μας πληροφορήσει σχετικά με στοιχεία όπως ο αριθμός αναγνώρισης, περιγραφές, τύπους, και το μέγεθος. Ειδικότερα η επικεφαλίδα καταχωρεί τις ιδιότητες του αρχείου που δηλώνουν τους όρους πρόσβασης και την παρούσα κατάσταση. Η πρόσβαση των δεδομένων στο αρχείο εξαρτάται από εάν οι όροι μπορούν να τηρηθούν ή όχι. Εν ολίγοις, η δομή αρχείων του λειτουργικού συστήματος έξυπνων καρτών είναι παρόμοια με άλλα κοινά λειτουργικά συστήματα όπως το MS-DOS και το UNIX Εντούτοις, προκειμένου να παρασχεθεί μεγαλύτερος έλεγχος ασφάλειας, η ιδιότητα κάθε αρχείου ενισχύεται με την προσθήκη όρων πρόσβασης και πεδίων θέσης αρχείων, *status fields* στην επικεφαλίδα αρχείων. Επιπλέον, παρέχεται το κλείδωμα αρχείων, για να αποτραπεί η πρόσβαση στο αρχείο. Αυτοί οι μηχανισμοί και οι αλγόριθμοι ασφάλειας παρέχουν αρκετή προστασία της έξυπνης κάρτας.

ΚΕΦΑΛΑΙΟ 2
ΠΡΟΤΥΠΟ ISO 7816

2.1 Πρότυπα ISO7816-1

Τα πρότυπα ISO7816 είναι χωρισμένα σε 3 διαφορετικά μέρη.

- ISO7816-1 που καθορίζουν τα φυσικά χαρακτηριστικά της κάρτας.
- ISO7816-2 που καθορίζουν τη διάσταση και τη θέση επαφών της κάρτας.
- ISO7816-3 που καθορίζουν τα ηλεκτρικά σήματα και τα πρωτόκολλα μετάδοσης.

Τα πρότυπα ISO7816 καθορίζουν πολλά φυσικά χαρακτηριστικά γνωρίσματα, αλλά εδώ θα περιγράψουμε μόνο τα πιο σημαντικά από αυτά.

- **Υπερβολικό ιώδες φως:**

Οποιαδήποτε προστασία πέρα από το επίπεδο UV φωτός θα είναι ευθύνη του κατασκευαστή.

- **Ακτίνες Χ:**

Έκθεση καθεμίας πλευράς της κάρτας σε μια δόση 0,1 Gy σχετικά με τη μέση-ενέργεια ακτινοβολίας Χ από 70 έως 140 kv (συσσωρευτική δόση ετησίως) δε θα προκαλέσει τη δυσλειτουργία της κάρτας.

- **Σχεδιάγραμμα επιφάνειας των επαφών:**

Η διαφορά στο επίπεδο μεταξύ όλων των επαφών και της παρακείμενης κάρτας, η επιφάνεια θα είναι λιγότερο από 0,1 χιλ.

- ***Mechanical strength* - Μηχανικές καταπονήσεις (της κάρτας και της επαφής):**

Η κάρτα θα αντισταθεί στη ζημία στην επιφάνειά της και οποιαδήποτε συστατικά που περιλαμβάνεται και θα παραμείνει άθικτη κατά τη διάρκεια της κανονικής χρήσης, της αποθήκευσης και του χειρισμού.

Η επιφάνεια (με τις επαφές) δεν πρέπει να καταστραφεί από πίεση που προκαλείται από μία σφαίρα χάλυβα διαμέτρου 1,5 χιλ. στην οποία εφαρμόζεται ένα strenght 1,5 N.

- **Ηλεκτρική αντίσταση:**

Όλες οι αντιστάσεις που μετριούνται μεταξύ των οποιοδήποτε δύο σημείων τον επαφών δεν πρέπει να είναι πάνω από 0,5 Ohm, με οποιαδήποτε τρέχουσα αξία από 50 uA σε 300 mA.

- **Μαγνητικό πεδίο:**

Το τσιπ της κάρτας δεν πρέπει να βλαφθεί από έναν στατικό μαγνητικό πεδίο 79500 A.tr/m

- **Στατικός ηλεκτρισμός:**

Η κάρτα δεν πρέπει να βλαφτεί από μία ηλεκτρική εκκένωση 1500 Volt ενός πυκνωτή 100 pf και μιας αντίστασης 1500 Ohm.

- **Μέγιστη κάμψη καρτών:**

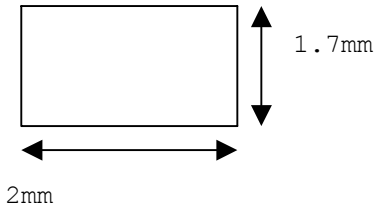
α - μεγάλη πλευρά της κάρτας: παραμόρφωση (f): 2 cm - περιοδικότητα: 30 κάμψεις/min.

β - μικρή πλευρά της κάρτας: παραμόρφωση (f): 1 cm - περιοδικότητα: 30 κάμψεις/min.

Αποδοχή: Η κάρτα πρέπει να λειτουργήσει σωστά και δεν πρέπει να έχει οποιαδήποτε ραγίσματα μετά από τις 1000 κάμψεις.

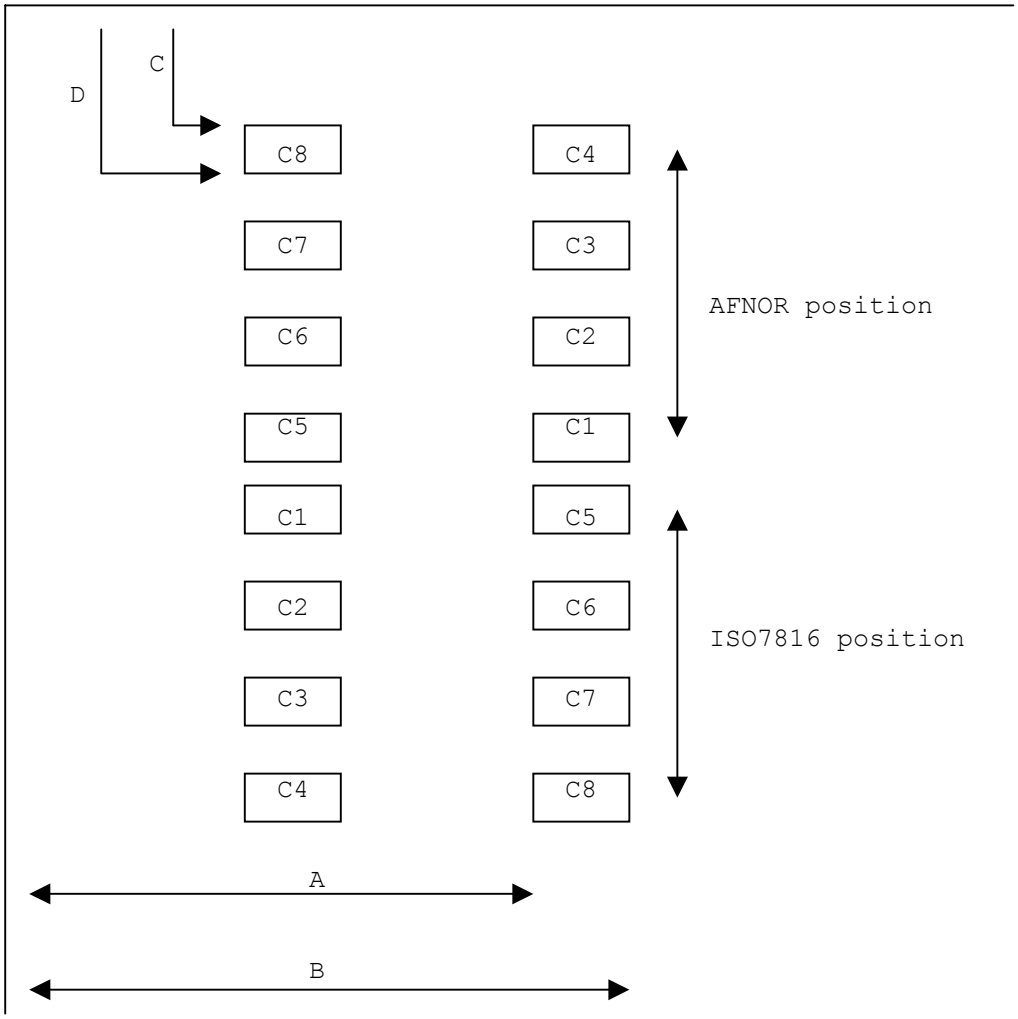
2.2 ISO7816-2 Τυποποίηση

2.2.1 Ελάχιστο μέγεθος επαφών



Σχήμα 2.2.1: Ελάχιστο μέγεθος επαφών

2.2.2 Θέση της επαφής



Σχήμα 2.2.2: Θέση της Επαφής

2.2.3 Προσδιορισμός επαφών

C1: Vcc = 5V	C4: RFU	C7: I/O
C2: Αναστοιχειοθέτηση (Reset)	C5: Gnd	C8: RFU
C3: Ρολόι (Clock)	C6: Vpp	

2.2.4 Θέση επαφών

Όλες οι διαστάσεις είναι σε χιλιοστά.

	A	B	C	D
C1	10.25	12.25	19.23	20.93
C2	10.25	12.25	21.77	23.47
C3	10.25	12.25	24.31	26.01
C4	10.25	12.25	26.85	28.55
C5	10.87	19.87	19.23	20.93
C6	10.87	19.87	21.77	23.47
C7	10.87	19.87	24.31	26.01
C8	10.87	19.87	28.85	28.55

ISO7816 Location

	A	B	C	D
C1	17.87	19.87	16.69	18.39
C2	17.87	19.87	14.15	15.85
C3	17.87	19.87	11.61	13.31
C4	17.87	19.87	9.07	10.77
C5	10.25	12.25	16.69	18.39
C6	10.25	12.25	14.15	15.85
C7	10.25	12.25	11.61	13.31
C8	10.25	12.25	9.07	10.77

AFNOR Location

Πίνακας 1: Θέση επαφών σε πρότυπο ISO 7816 και AFNOR

Σημείωση: Η θέση AFNOR είναι μεταβατική κι έχει χρησιμοποιηθεί για λόγους συμβατότητας με τις υπάρχουσες μαγνητικές κάρτες.

2.3 Πρότυπα ISO7816-3

2.3.1 Ηλεκτρική περιγραφή σημάτων

- I/O: Είσοδος ή έξοδος για σειριακά δεδομένα στο ολοκληρωμένο κύκλωμα μέσα στην κάρτα.
- VPP: Τάση Προγραμματισμού (προαιρετική χρήση από την κάρτα).
- Gnd: Γείωση (τάση αναφοράς).
- CLK: Σήμα χρονομέτρησης/συγχρονισμού ή ρολόι/clock (προαιρετική χρήση από την κάρτα).
- RST: Είτε χρησιμοποιείται μόνο του (σήμα αναστοιχειοθέτησης [reset] που παρέχεται από τη συσκευή διεπαφών) ή σε συνδυασμό με ένα εσωτερικό κύκλωμα ελέγχου αναστοιχειοθέτησης [reset] (προαιρετική χρήση από την κάρτα). Εάν η εσωτερική αναστοιχειοθέτηση [reset] εφαρμόζεται, η τάση τροφοδοσίας Vcc της κάρτας είναι υποχρεωτική.
- VCC: Τάση τροφοδοσίας της κάρτας (προαιρετική χρήση από την κάρτα).
  ΣΗΜΕΙΩΣΗ - η χρήση των δύο επαφών που παραμένουν θα καθοριστεί κατάλληλα από τα πρότυπα εφαρμογής.

2.3.2 Τάση και τρέχουσες τιμές

Συντ/μήσεις:

- Vih: Τάση εισόδου υψηλού επιπέδου (high level)
- Vil: Τάση εισόδου χαμηλού επιπέδου (low level)
- Vcc: Τάση παροχής ηλεκτρικού ρεύματος ή τροφοδοσίας σε VCC
- Vpp: Τάση προγραμματισμού σε VPP
- Voh: Τάση εξόδου υψηλού επιπέδου
- Vol: Τάση εξόδου χαμηλού επιπέδου
- TR: Χρόνος ανόδου μεταξύ 10% και 90% του πλάτους σήματος
- TF: Χρόνος πτώσης μεταξύ 90% και 10% του πλάτους σήματος

- Iih: Ρεύμα εισόδου υψηλού επιπέδου
- Iil: Ρεύμα εισόδου χαμηλού επιπέδου
- Icc: Ρεύμα τροφοδοσίας για το VCC
- Ipp: Ρεύμα προγραμματισμού για το VPP
- Ioh: Ρεύμα εξόδου υψηλού επιπέδου
- Iol: Ρεύμα εξόδου χαμηλού επιπέδου
- Cin: Χωρητικότητα εισόδου
- Cout: Χωρητικότητα εξόδου

I/O: Αυτή η επαφή χρησιμοποιείται ως είσοδος (λειτουργία λήψης) ή έξοδος (λειτουργία μετάδοσης) για την ανταλλαγή στοιχείων. Δύο πιθανές καταστάσεις υπάρχουν για το I/O:

- Mark ή υψηλή κατάσταση (κατάσταση Z), εάν η κάρτα και η συσκευή διεπαφών είναι σε κατάσταση λήψης ή εάν η κατάσταση επιβάλλεται από τη συσκευή αποστολής σημάτων.
- Space ή χαμηλή κατάσταση (κατάσταση A), εάν αυτή η κατάσταση επιβάλλεται από τη συσκευή αποστολής σημάτων.

Όταν οι δύο άκρες της γραμμής είναι σε κατάσταση λήψης, η γραμμή θα πρέπει να είναι διατηρημένη σε κατάσταση Z. Όταν οι δύο άκρες είναι σε non-matced μετάδοση, η κατάσταση της γραμμής μπορεί να είναι απροσδιόριστη. Κατά τη διάρκεια των διαδικασιών, η συσκευή διεπαφών και η κάρτα δεν πρέπει να βρίσκονται και οι δύο μαζί σε κατάσταση μετάδοσης.

Symbol	Condition		Minimum	Maximum	Unit
Vih	Either (1)	Iih max = +/- 500uA	2	VCC	V
	Or	Iih max = +/- 50uA	0.7 VCC	VCC (3)	V
Vil	Iil max = 1mA		0	0.8	V
Voh (2)	Either	Iol = max +/- 100uA	2.4	VCC	V
	Or	Iol = max +/- 20uA	3.8	VCC	V
Vol	Iol max = 1mA		0	0.4	V
tr, tf	Cin = 30pF Cout = 30pF			1	us

Πίνακας 2: Ηλεκτρικά χαρακτηριστικά του I/O υπό κανονικούς όρους λειτουργίας.

VPP: Από αυτή την επαφή μπορεί να παρασχεθεί η τάση που απαιτείται για να προγραμματίσουμε ή να σβήσουμε την εσωτερική αμετάβλητη μνήμη. Δύο πιθανές καταστάσεις υπάρχουν για το VPP: κατάσταση αναμονής και ενεργή κατάσταση, όπως καθορίζονται στον πίνακα 2. Η κατάσταση αναμονής

Symbol	Conditions	Minimum	Maximum	Unit
Vpp	Idle State	0.95*Vcc	1.05*Vcc	V
Ipp	(programming non active		20	mA
Vpp	Active State	0.975*P	1.025*P	V
Ipp	(programming the card		I	mA

διατηρείται από τη συσκευή διεπαφών εκτός αν απαιτείται η ενεργός κατάσταση.

Πίνακας 3: Ηλεκτρικά χαρακτηριστικά VPP κάτω από κανονικές συνθήκες λειτουργίας.

Η κάρτα παρέχει στη διεπαφή τις τιμές του P και του I (προκαθορισμένες τιμές: P=5 και I=50). Άνοδος του χρόνου πτώσης: 200 ns μέγιστη. Το ποσοστό αλλαγής του Vpp δεν θα πρέπει να υπερβεί τα 2V/ns. Η μέγιστη Ισχύς Vpp*Ipp δε θα πρέπει να υπερβαίνει το 1.5W όταν υπολογίζεται κατά μέσο όρο για διάρκεια περιόδου 1sec.

CLK: Η πραγματική συχνότητα, που παραδίδεται από τη συσκευή διεπαφών σε CLK, καθορίζεται από το fi, την αρχική συχνότητα κατά τη διάρκεια της απάντησης στην αναστοιχειοθέτηση (answer to reset), ή από το fs, την επόμενη συχνότητα κατά τη διάρκεια της επόμενης μετάδοσης.

Ο κύκλος καθήκοντος για τις ασύγχρονες διαδικασίες είναι μεταξύ 45% και 55% της περιόδου κατά τη διάρκεια της σταθερής λειτουργίας. Προσοχή πρέπει να ληφθεί κατά την αλλαγή συχνότητας (από το fi στο fs) για να εξασφαλίσει ότι κανένας παλμός δεν είναι πιό σύντομος από το 45% η μικρότερης χρονικής περιόδου.

Symbol	Condition		Minimum	Maximum	Unit
Vih	Either (1)	Iih max = +/- 200uA	2.4	VCC (2)	V
	or (1)	Iih max = +/- 20uA	0.7*VCC	VCC (2)	V
	or	Iih max = +/- 10uA	0.7 VCC	VCC (2)	V
Vil	Iil max = +/- 200 uA		0 (2)	0.5	V
tr, tf	Cin = 30pF			9% of the period with a max: 0.5 us	

Πίνακας 4: Ηλεκτρικά χαρακτηριστικά του CLK κάτω από κανονικές συνθήκες λειτουργίας.

RST:

Symbol	Condition		Minimum	Maximum	Unit
Vih	Either (1)	Iih max = +/- 200uA	4	VCC (2)	V
	or	Iih max = +/- 10uA	VCC-0.7	VCC (2)	V
Vil	Iil max = +/- 200 uA		0 (2)	0.6	V

Πίνακας 5: Ηλεκτρικά χαρακτηριστικά του RST κάτω από κανονικές συνθήκες λειτουργίας.

VCC: Αυτή η επαφή χρησιμοποιείται για να παρέχει την τάση τροφοδοσίας Vcc.

Symbol	Minimum	Maximum	Unit
Vcc	4.75	5.25	V
Icc		200	mA

Πίνακας 6: Ηλεκτρικά χαρακτηριστικά του VCC κάτω από κανονικές συνθήκες λειτουργίας.

2.3.3 Διαδικασία Λειτουργίας για τις κάρτες ολοκληρωμένων κυκλωμάτων

Αυτή η διαδικασία λειτουργίας ισχύει για κάθε κάρτα ολοκληρωμένων κυκλωμάτων με επαφές. Η επικοινωνία μεταξύ της συσκευής διεπαφών και της κάρτας θα είναι εφικτή μέσω διαδοχικών διαδικασιών:

- σύνδεση και ενεργοποίηση των επαφών από τη συσκευή διεπαφών.

- αναστοιχειοθέτηση της κάρτας (*Reset*).
- απάντηση στην αναστοιχειοθέτηση από την κάρτα (*Answer to Reset*).
- επόμενη ανταλλαγή πληροφοριών μεταξύ της κάρτας και της συσκευής διεπαφών.
- απενεργοποίηση των επαφών από τη συσκευή διεπαφών.

Οι προηγούμενες διαδικασίες διευκρινίζονται παρακάτω.

ΣΗΜΕΙΩΣΗ: Μία ενεργή κατάσταση στην VPP πρέπει όχι μόνο να παρασχεθεί αλλά και να διατηρηθεί όταν ζητείται από την κάρτα.

Α. Σύνδεση και ενεργοποίηση των επαφών

Τα ηλεκτρικά κυκλώματα δε θα ενεργοποιηθούν έως ότου οι επαφές είναι συνδεδεμένες με τη συσκευή διεπαφών, ώστε να αποφευχθεί η πιθανή ζημία σε οποιοιδήποτε κάρτα που ανταποκρίνεται σε αυτά τα πρότυπα. Η ενεργοποίηση των επαφών από τη συσκευή διεπαφών αποτελείται από διαδοχικές διαδικασίες:

- RST είναι η κατάσταση L
- VCC θα τροφοδοτηθεί με τάση η κάρτα
- Το I/O στη συσκευή διεπαφών θα τεθεί σε κατάσταση λήψης
- VPP θα αυξηθεί στην κατάσταση αναμονής
- CLK θα πρέπει να παρέχεται ένα κατάλληλο και σταθερό ρολόι.

Β. Αναστοιχειοθέτηση της κάρτας (*Reset*)

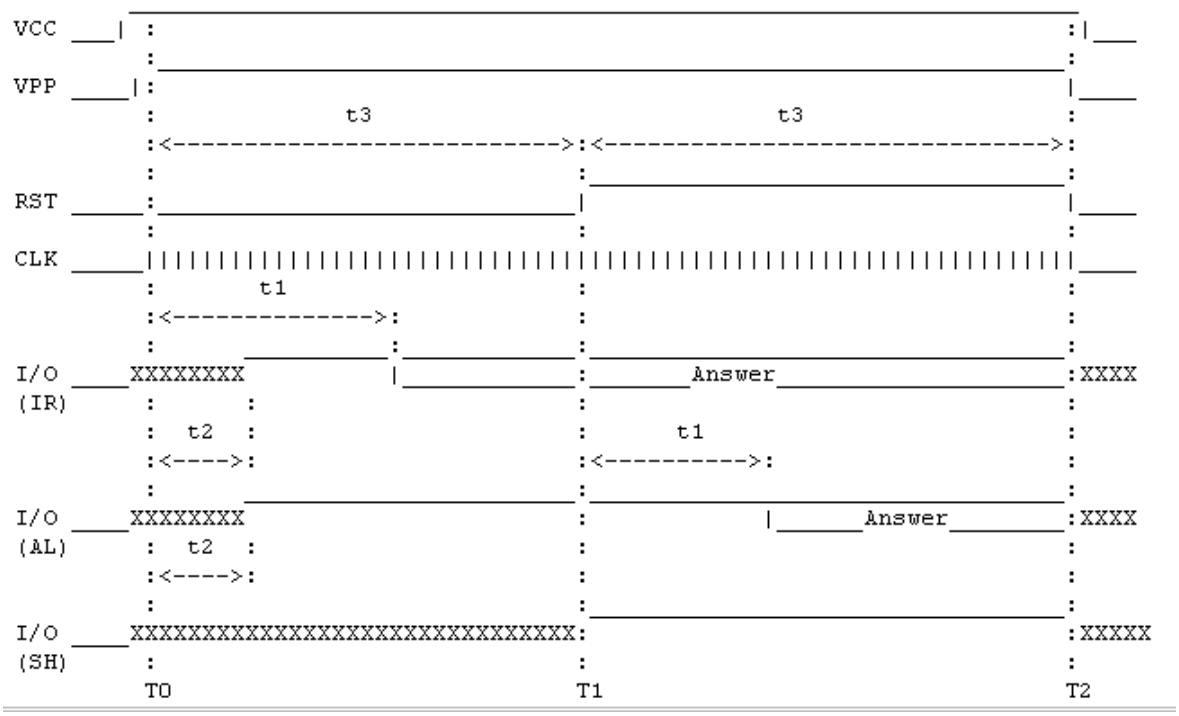
Μια αναστοιχειοθέτηση καρτών (*Reset*) αρχίζει από τη συσκευή διεπαφών, όπου η κάρτα αποκρίνεται με μια απάντηση στην αναστοιχειοθέτηση. Μέχρι το τέλος της ενεργοποίησης των επαφών (Το RST είναι στο L, το VCC τροφοδοτείται και είναι σταθερό, το I/O είναι σε κατάσταση λήψης στη συσκευή διεπαφών, η τάση προγραμματισμού VPP είναι σταθερή σε επίπεδο αναμονής (*idle level*), το CLK που παρέχεται είναι κατάλληλο και σταθερό ρολόι), η απάντηση των καρτών ασύγχρονα είναι έτοιμη για την αναστοιχειοθέτηση.

Το σήμα του ρολογιού εφαρμόζεται στο CLK στο χρόνο T0. Η I/O γραμμή θα τεθεί σε κατάσταση Z μέσα σε 200 κύκλους του ρολογιού του σήματος ρολογιού (t2) που εφαρμόζεται το CLK (χρονικό t2 μετά από T0). Μια εσωτερικά επαναρυθμισμένη κάρτα επαναρυθμίζεται μετά από μερικούς κύκλους του σήματος ρολογιών. Η απάντηση στην αναστοιχειοθέτηση (*answer to reset*) στο I/O θα πρέπει να αρχίσει μεταξύ 400 και 40.000 κύκλων ρολογιών (t1). Μετά από αυτό το σήμα του ρολογιού εφαρμόζεται στο CLK (χρονικό t1 μετά από T0).

Μια κάρτα με μια ενεργό χαμηλή αναστοιχειοθέτηση επαναρρυθμίζεται με τη διατήρηση του RST σε κατάσταση L για τουλάχιστον 40.000 κύκλους ρολογιών (t3) μετά από αυτό το σήμα ρολογιών εφαρμόζονται στο CLK (χρόνος t3 μετά από T0). Κατά συνέπεια εάν καμία απάντηση στην αναστοιχειοθέτηση (*no answer to reset*) αρχίζει με 40.000 κύκλους ρολογιού (t3) με RST σε κατάσταση L, το RST τίθεται σε κατάσταση «Η» (στο χρονικό T1).

Η απάντηση στην αναστοιχειοθέτηση (*answer to reset*) στο I/O θα αρχίσει μεταξύ 400 και 40.000 κύκλων ρολογιών (t1) μετά από την αυξανόμενη άκρη του σήματος σε RST (χρονικό t1 μετά από το T1).

Εάν η απάντηση στην αναστοιχειοθέτηση (*answer to reset*) δεν αρχίζει μέσα σε 40.000 κύκλους ρολογιών (t3) με RST στην κατάσταση «H» (t3 μετά από το T1), το σήμα στο RST θα επανέλθει σε κατάσταση L (στο χρονικό T2) και οι επαφές θα απενεργοποιηθούν από την συσκευή διεπαφών.



Σχήμα 2.3.3.1: Αναστοιχειοθέτηση (*Reset*) της κάρτας

IR: Internal Reset (εσωτερική αναστοιχειοθέτηση) t2 <= 200/fi

AL: Asynchronous Reset (ασύγχρονη αναστοιχειοθέτηση) 400/fi <= t1 <= 40000/fi

SH: Syncronous Reset (σύγχρονη αναστοιχειοθέτηση) 40000/fi <= t3

Με μια κάρτα που απαντά σύγχρονα, η συσκευή διεπαφών θέτει όλες τις γραμμές σε κατάσταση L (δες σχήμα 2). Η VCC τροφοδοτείται, η VPP τίθεται σε κατάσταση αναμονής, το CLK και το RST παραμένει σε κατάσταση L, το I/O τίθεται σε κατάσταση λήψης στη συσκευή διεπαφών, το RST θα διατηρηθεί σε κατάσταση «H» για τουλάχιστον 50 us (t12), πριν επιστρέψει σε κατάσταση L πάλι.

Ο παλμός ρολογιού εφαρμόζεται μετά από ένα διάστημα (t10) από την αυξανόμενη άκρη του σήματος αναστοιχειοθέτησης. Η διάρκεια της κατάστασης «H» του παλμού του ρολογιού μπορεί να έχει οποιαδήποτε αξία μεταξύ 10 us και 50 us, όχι περισσότερο από ένα παλμό ρολογιού κατά τη διάρκεια της αναστοιχειοθέτησης (για high reset) επιτρέπεται. Το χρονικό διάστημα μεταξύ των μειωμένων ακρών σε CLK και RST είναι t11.

Το πρώτο κομμάτι στοιχείων (*data bit*) λαμβάνεται ως απάντηση για να επαναριθμήσει το I/O ενώ το CLK είναι σε κατάσταση L και ισχύει μετά από ένα διάστημα t13 από τη μειωμένη άκρη του RST.

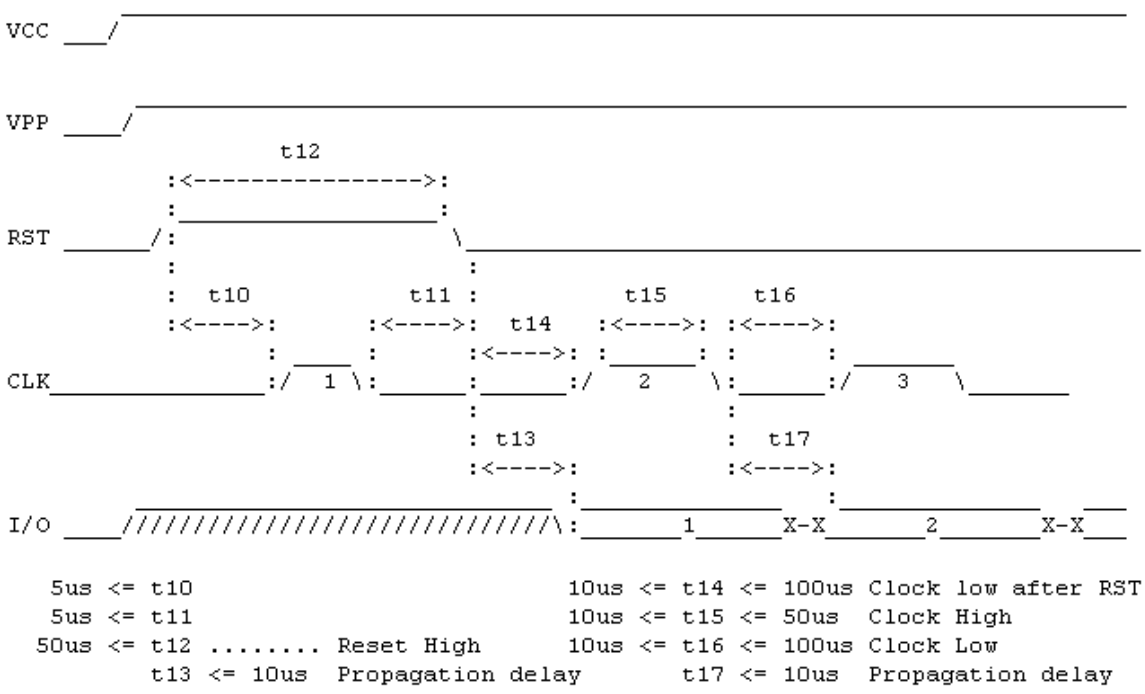
ΣΗΜΕΙΩΣΕΙΣ:

1 - η εσωτερική κατάσταση της κάρτας υποτίθεται ότι δεν καθορίστηκε πριν από την αναστοιχειοθέτηση (reset). Επομένως το σχέδιο της κάρτας πρέπει να αποφύγει μη προβλεπόμενη λειτουργία.

2 - προκειμένου να συνεχιστεί η επικοινωνία με την κάρτα, το RST θα διατηρηθεί σε κατάσταση όπου μια απάντηση εμφανίζεται στο I/O.

3 - η αναστοιχειοθέτηση (*reset*) μιας κάρτας μπορεί να αρχίσει από τη συσκευή διεπαφών οποιαδήποτε στιγμή.

4 - οι συσκευές διεπαφών μπορούν να υποστηρίξουν ένα ή περισσότερο από αυτούς τους τύπους αναστοιχειοθέτησης. Η προτεραιότητα της δοκιμής για τις ασύγχρονες ή σύγχρονες κάρτες είναι μη καθορισμένη σε αυτά τα πρότυπα.



Σχήμα 2.3.3.2: Αναστοιχειοθέτηση (*reset*) της κάρτας όταν αναμένεται μια σύγχρονη απάντηση.

Α. Απενεργοποίηση των επαφών

Όταν η ανταλλαγή πληροφοριών ολοκληρώνεται ή ματαιώνεται (κάρτα που δεν διαβάζεται ή ανιχνεύεται η αφαίρεση των καρτών από συσκευή διεπαφών), οι ηλεκτρικές επαφές πρέπει να απενεργοποιούνται.

Η απενεργοποίηση από τη συσκευή διεπαφών θα αποτελείται από διαδοχικές διαδικασίες:

- Κατάσταση L σε RST
- Κατάσταση L σε CLK
- Vpp ανενεργό
- Κατάσταση «A» στο I/O

- VCC ανενεργό

2.3.4 Απάντηση για αναστοιχειοθέτηση (*answer to reset*)

Δύο τύποι μεταδόσεων εξετάζονται:

Ασύγχρονη μετάδοση: Σε αυτόν τον τύπο μετάδοσης, οι χαρακτήρες διαβιβάζονται στην I/O γραμμή σε έναν ασύγχρονο μισό διπλό τρόπο (*half duplex mode*). Κάθε χαρακτήρας περιλαμβάνει μια οκτάμπιτη ψηφιολέξη (8 bit).

Σύγχρονη μετάδοση: Σε αυτόν τον τύπο μετάδοσης, μία σειρά κομματιών (bits) διαβιβάζεται στην I/O γραμμή σε ένα μισό διπλό τρόπο (half duplex mode) σε συγχρονισμό με το σήμα ρολογιών CLK.

Α. Απάντηση στην αναστοιχειοθέτηση (answer to reset) στην ασύγχρονη μετάδοση

⇒ *Διάρκεια κομματιών (bit)*

Η ονομαστική διάρκεια κομματιών (bit) που χρησιμοποιείται στο I/O ορίζεται ως ένας στοιχειώδης χρόνος μονάδας (*etu – Elementary Time Unit*).

Για τις κάρτες που έχουν εσωτερικό ρολόι, το αρχικό etu είναι το 1/9600 s. Για τις κάρτες που χρησιμοποιούν εξωτερικό ρολόι, υπάρχει μια γραμμική σχέση μεταξύ της στοιχειώδης χρονικής μονάδας που χρησιμοποιούνται στο I/O και η περίοδος που παρέχεται από συσκευή διεπαφών στο CLK. Το αρχικό etu είναι 372/fi s όπου το fi είναι σε Hertz.

Η αρχική συχνότητα fi παρέχεται από τη συσκευή διεπαφών σε CLK κατά τη διάρκεια της απάντησης στην αναστοιχειοθέτηση (*answer to reset*). Προκειμένου να διαβαστεί ο αρχικός χαρακτήρας (TS), όλες οι κάρτες αρχικά επρόκειτο να λειτουργήσουν με το fi σε συχνότητες μεταξύ 1 MHz και 5 MHz.

⇒ *Πλαίσιο χαρακτήρα (frame character) κατά τη διάρκεια της απάντησης στην αναστοιχειοθέτηση (answer to reset)*

Πριν από τη μετάδοση ενός χαρακτήρα, το I/O θα είναι σε κατάσταση Z. Ένας χαρακτήρας αποτελείται από δέκα διαδοχικά bit:

- Το αρχικό bit σε κατάσταση «Α».
- Οκτώ bit των πληροφοριών, που υποδεικνύονται από ba σε bh και τη μεταβίβαση του σε ψηφιολέξη στοιχείων (*data byte*).
- Το δέκατο κομμάτι (bit) bi χρησιμοποιείται για τον έλεγχο ισοτιμίας (*even parity checking*).

Μια ψηφιολέξη στοιχείων (data byte) αποτελείται από 8 bit, b1 έως b8, από το πιο ελάχιστα σημαντικό ψηφίο (lsb, b1) στο σημαντικότερο ψηφίο (msb, b8).

Συνθήκες όπως (κωδικοποίηση επιπέδων, συνδέοντας επίπεδα Z/A σε ψηφία 1 ή 0: και η σημασία κομματιών (bit), συνδέοντας ba...bh σε b1...b8) διευκρινίζεται ο αρχικός χαρακτήρας, κλήση TS, η οποία διαβιβάζεται από την κάρτα σαν απάντηση στην αναστοιχειοθέτηση (*response to reset*).

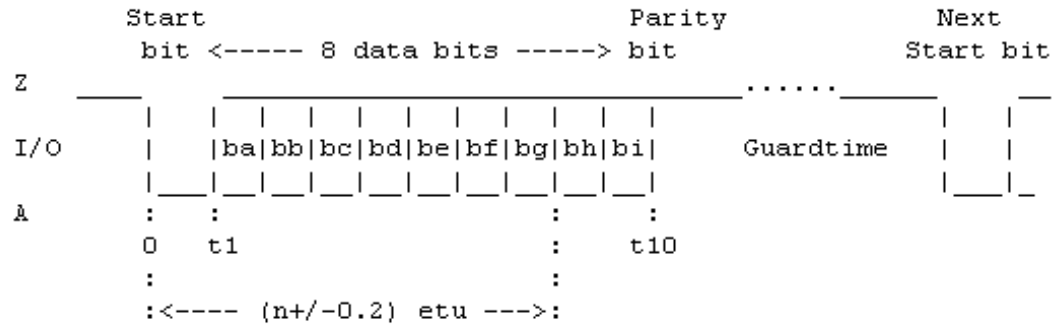
Η ισοτιμία (parity) είναι σωστή όταν ο αριθμός είναι μονός (even) στην ακολουθία από ba στο bi.

Η αναμονή ενός χαρακτήρα, ο χρόνος από την αιχμή του αρχικού bit ως το τελευταίο bit θα είναι ίση με (n+/-0,2) του etu.

Όταν ψάχνουμε την αρχή, τα δείγματα κατά την λήψη στην I/O είναι περιοδικά. Η χρονική προέλευση που είναι ο μέσος όρος μεταξύ της τελευταίας παρατήρησης του επιπέδου Z και της πρώτης παρατήρησης του επιπέδου A, η έναρξη θα ελεγχθεί πριν από 0,7 etu, και κατόπιν το ba λαμβάνεται σε (1,5 +/- 0,2) etu. Η ισοτιμία ελέγχεται συνεχώς.

ΣΗΜΕΙΩΣΗ: Κατά την έναρξη, ο χρόνος δειγματοληψίας θα είναι λιγότερο από 0,2 etu έτσι ώστε όλες οι ζώνες δοκιμής είναι ευδιάκριτες από τις ζώνες μετάβασης.

Η καθυστέρηση μεταξύ δύο συνεχόμενων χαρακτήρων (μεταξύ της έναρξης οδήγησης της αιχμής) είναι τουλάχιστον 12 etu, συμπεριλαμβανομένου ενός etu διάρκειας χαρακτήρα (10+/-0,2) etu συν ένα χρόνο ασφαλείας, η συσκευή διεπαφών και η κάρτα παραμένουν και οι δύο σε κατάσταση λήψης, έτσι ώστε το I/O είναι σε κατάσταση Z.



Σχήμα 2.3.4.1: Παράθυρο χαρακτήρων (*character frame*)

Κατά τη διάρκεια της απάντησης στην αναστοιχειοθέτηση (answer to reset), η καθυστέρηση μεταξύ της αιχμής έναρξης δύο συνεχόμενων χαρακτήρων από την κάρτα δεν πρέπει να υπερβαίνει τα 9600 etu. Αυτός ο μέγιστος χρόνος ονομάζεται αρχικός χρόνος αναμονής.

⇒ *Ανίχνευση λάθους και επανάληψη χαρακτήρα*

Κατά τη διάρκεια της απάντησης στην αναστοιχειοθέτηση (*answer to reset*), η ακόλουθη επαναληπτική διαδικασία χαρακτήρων εξαρτάται από τον τύπο πρωτοκόλλου. Αυτή η διαδικασία είναι υποχρεωτική για τη χρησιμοποίηση καρτών που χρησιμοποιούν το πρωτόκολλο T=0, είναι προαιρετικό για τη συσκευή διεπαφών και για άλλες κάρτες.

Το I/O (11+/-0,2) etu δοκιμών συσκευών αποστολής σημάτων μετά από την έναρξη αιχμής:

- Εάν το I/O είναι σε κατάσταση Z, έχουμε σωστή λήψη.

- Εάν το I/O είναι σε κατάσταση A, η μετάδοση είναι ανακριβής. Ο ζητούμενος χαρακτήρας θα επαναληφθεί μετά από μια καθυστέρηση τουλάχιστον 2 etu μετά από την ανίχνευση του σήματος λάθους (*signal error*).

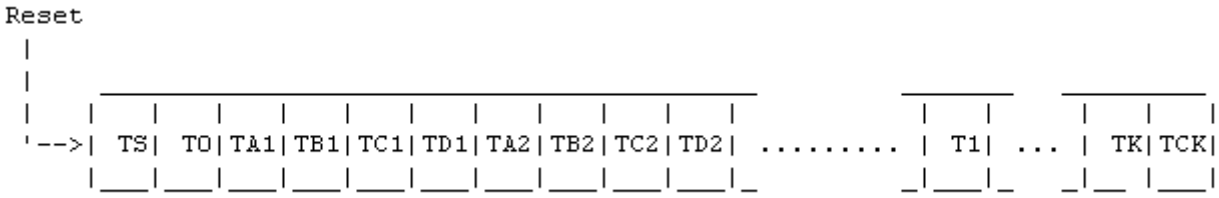
Όταν η ισοτιμία είναι ανακριβής, από (10,5+/-0,2) etu, ο δέκτης διαβιβάζει ένα σήμα λάθους στην κατάσταση A για ελάχιστο χρόνο 1 etu και για μέγιστο χρόνο 2 etu. Ο δέκτης έπειτα θα αναμείνει μια επανάληψη του συζητημένου χαρακτήρα. Εάν καμία επανάληψη χαρακτήρα δεν παρέχεται από την κάρτα:

- Η κάρτα αγνοεί και δεν έχει ζημία από το σήμα λάθους που προέρχεται από τη συσκευή διεπαφών.
- Η συσκευή διεπαφών θα είναι σε θέση να αρχίσει την υποδοχή και ολοκληρώνει την απάντηση για να επαναριθμήσει την ακολουθία απάντησης (answer to reset).

⇒*Δομές και περιεχόμενο*

Μια λειτουργία αναστοιχειοθέτησης οδηγεί στην απάντηση από την κάρτα που αποτελείται από τον αρχικό χαρακτήρα TS που ακολουθείται από 32 χαρακτήρες στην ακόλουθο διαταγή:

- T0 ..... χαρακτήρας σχήματος (υποχρεωτικός)
- TAi, TBi, TCi... χαρακτήρες διεπαφών (προαιρετικοί)
- T1, T2... ,TK ..... ιστορικοί χαρακτήρες (προαιρετικοί)



- TCK..... Χαρακτήρας ελέγχου (υπό όρους)

TS : Αρχικός χαρακτήρας

TO : Χαρακτήρας σχήματος

TAi : Χαρακτήρας διεπαφών [codes FI,DI]

TBi : Χαρακτήρας διεπαφών [codes II,PI1]

TCi : Χαρακτήρας διεπαφών [codes N]

TDi : Χαρακτήρας διεπαφών [codes Yi+1, T]

T1, ... , TK : Ιστορικοί χαρακτήρες (μέγιστοι 15)

TCK : Χαρακτήρας ελέγχου

Σχήμα 2.3.4.2: Γενικές ρυθμίσεις για απάντηση στην αναστοιχειοθέτηση (*answer to reset*)

Οι χαρακτήρες διεπαφών καθορίζουν τις φυσικές παραμέτρους του ολοκληρωμένου κυκλώματος στην κάρτα και τα λογικά χαρακτηριστικά του επόμενου πρωτοκόλλου ανταλλαγής.

Οι ιστορικοί χαρακτήρες δίνουν τις γενικές πληροφορίες, για παράδειγμα των κατασκευαστή των καρτών, το τσιπ που περιέχεται στην κάρτα, το καλυμμένο ROM τσιπ, τη κατάσταση της κάρτας. Οι προδιαγραφές για τους ιστορικούς χαρακτήρες δεν εμπίπτουν στο πεδίο αυτού του μέρους του ISO/IEC7816. Για λόγους σαφήνειας, T0, TAi,……, TCK θα υποδείξουν τις ψηφιολέξεις (bytes) ως χαρακτήρες στους οποίους περιλαμβάνονται.

⇒*Δομή του TS, ο αρχικός χαρακτήρας*

Ο αρχικός χαρακτήρας TS παρέχει μια ακολουθία, συγχρονισμός κομματιών και καθορίζει τις συμβάσεις στις ψηφιολέξεις στοιχείων κώδικα σε όλους τους επόμενους χαρακτήρες. Αυτές οι συμβάσεις αναφέρονται σε ISO1177.

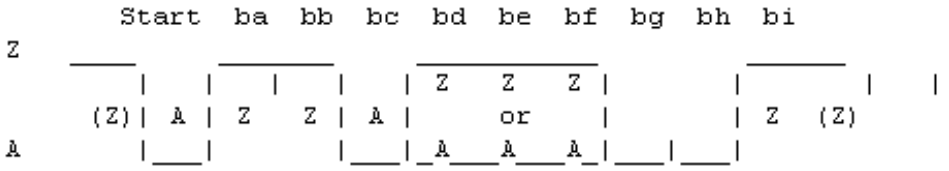
Το I/O είναι αρχικά σε κατάσταση Z. Μια ακολουθία συγχρονισμού κομματιών (Z)AZZA είναι καθορισμένα για το start bit και τα bits ba bb bc.

Τα τελευταία 3 bit bg bh bi θα πρέπει να είναι AAZ για τον έλεγχο της ισότητας.

ΣΗΜΕΙΩΣΗ: Αυτό επιτρέπει στη συσκευή διεπαφών να καθορίσει το etu αρχικά που χρησιμοποιείται από την κάρτα. Μια εναλλακτική μέτρηση του etu είναι το ένα τρίτο της καθυστέρησης μεταξύ των πρώτων δύο μειωμένων ακρών της TS. Οι μηχανισμοί μετάδοσης και λήψης στην κάρτα θα είναι σύμφωνοι με τον εναλλακτικό καθορισμό από το etu.

Οι δύο πιθανές τιμές του TS (δέκα διαδοχικά bits από τα ην έναρξη στο bi και η αντίστοιχη δεκαεξαδική αξία) είναι:

- Αντίστροφη σύμβαση: (Z)ZZAAAAAZ, όπου το επίπεδο λογικής ENA είναι A, το ba είναι b8 (msb πρώτα), ίσος με $3F όταν αποκωδικοποιείται από την αντίστροφη σύμβαση.
- Άμεση σύμβαση: (Z)ZZAZZZAAZ, όπου το επίπεδο λογικής ENA είναι Z, το ba είναι b1 (lsb πρώτα), ίσος με $3B όταν αποκωδικοποιείται από την άμεση σύμβαση.



Σχήμα 2.3.4.3: Ο αρχικός χαρακτήρας TS

⇒ ***Δομή των επόμενων χαρακτήρων στην απάντηση στην αναστοιχειοθέτηση (answer to reset)***

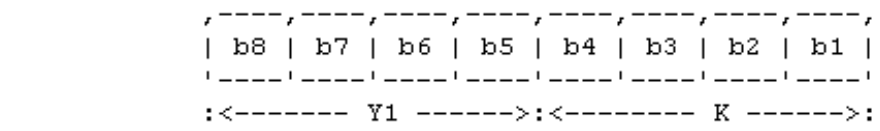
Ο αρχικός χαρακτήρας TS ακολουθείται από έναν μεταβλητό αριθμό επόμενων χαρακτήρων με την ακόλουθη διάταξη: Ο χαρακτήρας σχήματος T0 και προαιρετικά οι χαρακτήρες διεπαφών TAi, TBi, TCi, TDi και οι ιστορικοί χαρακτήρες T1, T2... , TK και υπό όρους, ο χαρακτήρας ελέγχου TCK.

Η παρουσία των χαρακτήρων διεπαφών υποδεικνύεται από έναν χάρτη κομματιών (bit map) τεχνική που εξηγείται παρακάτω. Η παρουσία του χαρακτήρα TCK ελέγχου εξαρτάται από τον τύπο πρωτοκόλλου που ορίζεται παρακάτω.

⇒ *Μορφή χαρακτήρα T0*

Ο T0 χαρακτήρας περιέχει δύο μέρη:

- Η σημαντικότερη μισή ψηφιολέξη (*most significal half byte*) (b5, b6, b7, b8) ονομάζεται Y1 και δείχνει με ένα επίπεδο λογικής ENA την παρουσία επόμενων χαρακτήρων TA1, TB1, TC1, TD1 αντίστοιχα.
- Η λιγότερη σημαντική μισή ψηφιολέξη (*least significal half byte*) (b4 b1) ονομάζεται K και υποδεικνύεται από τους αριθμούς (0 έως 15) των ιστορικών χαρακτήρων.



Y1: δείκτης για την παρουσία των χαρακτήρων διεπαφών

TA1 διαβιβάζεται όταν b5=1, TB1 διαβιβάζεται όταν b6=1

TC1 διαβιβάζεται όταν b7=1, TD1 διαβιβάζεται όταν b8=1

K: αριθμός ιστορικών χαρακτήρων

Σχήμα 2.3.4.4: Πληροφορίες που παρέχονται από το T0

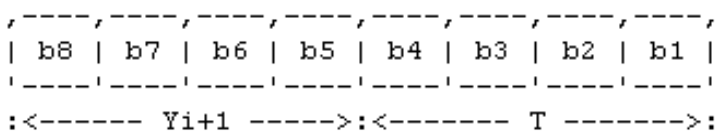
⇒ *Χαρακτήρες διεπαφών TAi, TBi, TCi, TDi*

TAi, TBi, TCi (i=1, 2, 3,...) δείχνει τους παραμέτρους του πρωτοκόλλου.

Το TDi δείχνει τον τύπο του πρωτοκόλλου και την παρουσία επόμενων χαρακτήρων. Κομμάτια (bits) b5, b6, b7, b8 της ψηφιολέξης (bytes) που περιέχει Yi (το T0 περιέχει Y1 το Tdi περιέχει Yi+1) την κατάσταση του χαρακτήρα TAi για b5, χαρακτήρα TBi για b6, ο χαρακτήρας TCi για b7, ο χαρακτήρας TDi για b8 είναι ή δεν είναι (ανάλογα αν το σχετικό κομμάτι είναι 1 ή 0) διαβιβασμένος διαδοχικά με αυτήν την σειρά μετά από τον χαρακτήρα που περιέχει Yi.

Όταν απαιτείται, η συσκευή διεπαφών θα αποδώσει μια προκαθορισμένη αξία πληροφορίας που αντιστοιχεί σε έναν μη διαβιβασθέντα χαρακτήρα διεπαφών.

Όταν το TDi δεν διαβιβάζεται, η προκαθορισμένη αξία Yi+1 είναι μηδενική, ένδειξη ότι κανένας περαιτέρω χαρακτήρας TAi+j, TBi+j, TCi+j, TDi+j διεπαφών δεν θα διαβιβαστεί.



Yi+1: Ο δείκτης για την παρουσία των χαρακτήρων διεπαφών

TAi+1 διαβιβάζεται όταν b5=1

TBi+1 διαβιβάζεται όταν b6=1

TCi+1 διαβιβάζεται όταν b7=1

TDi+1 διαβιβάζεται όταν b8=1

T: Τύπος πρωτοκόλλου για την επόμενη μετάδοση.

Σχήμα 2.3.4.5: Πληροφορίες που παρέχονται από το TDi

⇒ *Ιστορικό χαρακτήρων T1, T2, ... ,TK*

Όταν το K δεν είναι μηδενικό, η απάντηση για να επαναρυθμίσει (*answer to reset*) συνεχίζεται με τη διαβίβαση του K ιστορικού χαρακτήρα T1, T2, ... , TK.

- Έλεγχος χαρακτήρα TCK

Η αξία TCK θα είναι τέτοια που αποκλειστικά όλων των ψηφιολέξεων (bytes) από T0 σε TCK που συμπεριλαμβάνονται είναι μηδενικά. Η απάντηση στην αναστοιχειοθέτηση (*answer to reset*) είναι πλήρες 12 etu μετά από την αιχμή του τελευταίου χαρακτήρα.

- Τύπος πρωτοκόλλου T

Τα τέσσερα πιό λιγότερα σημαντικά κομμάτια (bits) οποιουδήποτε χαρακτήρα διεπαφών TDi δείχνουν το τύπο πρωτοκόλλου T, που διευκρινίζει τους κανόνες που χρησιμοποιούνται για να επεξεργαστεί τα πρωτόκολλα μετάδοσης. Όταν το TDi δεν διαβιβάζεται, το T=0 χρησιμοποιείται.

Το T=0 είναι το ασύγχρονο μισό διπλό (*half duplex*) πρωτόκολλο μετάδοσης χαρακτήρα.

Το T=1 είναι το ασύγχρονο μισό διπλό (*half duplex*)πρωτόκολλο μετάδοσης φραγμών.

Τα T=2 και T=3 είναι διατηρημένο, για τις μελλοντικές πλήρεις διπλές διαδικασίες (*full duplex*).

Το T=4 είναι διατηρημένο για έναν ενισχυμένο ασύγχρονο μισό διπλό χαρακτήρα (half duplex) πρωτόκολλο μετάδοσης.

Τα T=5 και T=13 είναι διατηρημένα για τη μελλοντική χρήση.

Το T=14 είναι διατηρημένο για τα πρωτόκολλα που τυποποιούνται από τον ISO.

Το T=15 είναι διατηρημένο για τη μελλοντική επέκταση.

ΣΗΜΕΙΩΣΗ: Μόνο εάν T=0 είναι υποδειγμένο, το TCK δεν θα σταλεί. Σε όλες τις άλλες περιπτώσεις TCK θα σταλεί.

⇒ *Προδιαγραφές των σφαιρικών ψηφιολέξεων διεπαφών (interface bytes)*

Μεταξύ των ψηφιολέξεων διεπαφών που διαβιβάζονται ενδεχομένως από την κάρτα στην απάντηση η αναστοιχειοθέτηση (answer to reset), αυτό το υποσύνολο καθορίζει μόνο τις σφαιρικές ψηφιολέξεις διεπαφών TA1, TB1, TC1, TD1. Αυτές οι σφαιρικές ψηφιολέξεις διεπαφών μεταβιβάζουν τις πληροφορίες για να καθορίσουν τις παραμέτρους τις οποίες η συσκευή διεπαφών θα λάβει υπόψη.

- Παράμετροι F, D, I, P, N

Αυτό το αρχικό etu χρησιμοποιείται κατά τη διάρκεια της απάντησης (*answer to reset*) για να επαναρυθμίσει την εργασία etu κατά τη διάρκεια της επόμενης μετάδοσης. Το F είναι ο παράγοντας μετατροπής ποσοστού ρολογιού και το D είναι ο παράγοντας ρύθμισης ποσοστού δυαδικών ψηφίων για να καθορίσει το etu εργασίας μέσα στις επόμενες μεταδόσεις.

Για τις κάρτες που περιέχουν εσωτερικό ρολόι: αρχικό etu = 1/9600 s. etu εργασίας = (1/D)*(1/9600) s.

Για τις κάρτες με εξωτερικό ρολόι: αρχικό etu = 372/fi s. etu εργασίας = (1/D)*(F/fs) s.

Η ελάχιστη αξία των fs θα είναι 1MHz.

Η μέγιστη αξία των fs δίνεται από τον πίνακα 2.3.4.6.

I και P καθορίζουν την ενεργή κατάσταση στο VPP.

- Μέγιστο ρεύμα προγραμματισμού: Ipp = 1mA

- Τάση προγραμματισμού: Vpp = P.V

Το N είναι πρόσθετο που ζητείται από την κάρτα. Πρίν λάβει τον επόμενο χαρακτήρα, η κάρτα απαιτεί μια καθυστέρηση τουλάχιστον (12+N) etu από την έναρξη αιχμής του προηγούμενου

χαρακτήρα. Κανένα πρόσθετο δεν χρησιμοποιείται για να στείλει χαρακτήρες από την κάρτα στη συσκευή διεπαφών.

Οι προκαθορισμένες αξίες αυτών των παραμέτρων είναι: F = 372, D = 1, I = 50, P = 5, N = 0.

- Τιμές ακέραιων αριθμών στις σφαιρικές ψηφιολέξεις διεπαφών (*interface bytes*)

Οι σφαιρικές ψηφιολέξεις (bytes) διεπαφών, TA1, TB1, TC1, TB2 κώδικα ακέραιων αριθμών FI, DI II, PI1, N, PI2 που είναι είτε ίσα είτε χρησιμοποιούνται για να υπολογίσουν τις τιμές των παραμέτρων F, D, I, P, N που παρουσιάζονται ανωτέρω.

Ο TA1 κωδικός FI άνω της σημαντικότερης μισής ψηφιολέξης (*most significant half byte*) (b8 b5) και του DI η λιγότερη σημαντική μισή ψηφιολέξη (*least significant half byte*) (b4 b1).

Ο TB1 κωδικός II πέρα από τα κομμάτια (bits) b7 και b6, και PI1 άνω των 5 πιό ελάχιστα σημαντικών κομματιών (*least significant bits*) b5 b1. Το σημαντικότερο κομμάτι (bit) b8 είναι ίσο με 0.

ΣΗΜΕΙΩΣΗ: Η συσκευή διεπαφών μπορεί να αγνοήσει το κομμάτι b8 TB1. Οι TC1 κώδικες N πέρα από τα οκτώ bit (b8 b1).

Οι TB2 κώδικες PI2 πέρα από τα οκτώ bit (b8 b1).

FI	0000	0001	0010	0011	0100	0101	0110	0111
F	Internal clk	372	558	744	1116	1488	1860	RFU
fs (max) MHz	-	5	6	8	12	16	20	-

FI	1000	1001	1010	1011	1100	1101	1110	1111
F	RFU	512	768	1024	1536	2048	RFU	RFU
fs (max) MHz	-	5	7.5	10	15	20	-	-

RFU : Reserved for Future Use

Πίνακας 2.3.4.6: Παράγοντας F μετατροπής ρυθμού ρολογιού (*clock rate*)

DI	0000	0001	0010	0011	0100	0101	0110	0111
D	RFU	1	2	4	8	16	RFU	RFU

DI	1000	1001	1010	1011	1100	1101	1110	1111
D	RFU	RFU	1/2	1/4	1/8	1/16	1/32	1/64

RFU : Reserved for Future Use

Πίνακας 2.3.4.7: Παράγοντας D ποσοστού δυαδικών ψηφίων (bit rate)

- Παράγοντας P τάσης προγραμματισμού

Το PI1 από 5 έως 25 δίνει την αξία του P σε Volt. PI1=0 δείχνει ότι το VPP συνδέεται στην κάρτα που παράγει μια εσωτερική τάση προγραμματισμού από το VCC. Άλλες τιμές PI1 είναι διατηρημένες για τη μελλοντική χρήση.

Όταν το PI2 είναι παρόν, η ένδειξη PI1 πρέπει να αγνοηθεί. Το PI2 από 50 σε 250 δίνει την αξία του P σε 0.1 Volt. Άλλες τιμές PI2 είναι διατηρημένες για μελλοντική χρήση.

II	00	01	10	11
I	25	50	100	RFU

Πίνακας 2.3.4.8: Παράγοντας I για μέγιστο ρεύμα προγραμματισμού

- Πρόσθετος χρόνος N

Το N κωδικοποιεί άμεσα τον πρόσθετο χρόνο, από 0 έως 254 etu. Το N=255 δείχνει ότι η ελάχιστη καθυστέρηση μεταξύ των ακρών έναρξης δύο συνεχόμενων χαρακτήρων μειώνεται κατά 11 etu.

Β. Απάντηση στην αναστοιχειοθέτηση (*answer to reset*) στην σύγχρονη μετάδοση

Συχνότητα παλμών και ποσοστό δυαδικών ψηφίων (bit rate)

Υπάρχει μια γραμμική σχέση μεταξύ του ποσοστού δυαδικών ψηφίων στην I/O γραμμή και τη συχνότητα ρολογιών που παρέχεται από τη συσκευή διεπαφών του CLK.

Οποιαδήποτε συχνότητα παλμού μεταξύ 7kHz και 50kHz μπορεί να επιλεχτεί για την ακολουθία αναστοιχειοθέτησης (*reset sequence*). Μια συχνότητα παλμών 7kHz αντιστοιχεί σε 7kbit/s, για τιμές συχνότητας παλμών πάνω από 50κHz δημιουργεί μία αντίστοιχη ταχύτητα στην μεταφορά δυαδικών ψηφίων που διαβιβάζονται.

Δομή της επικεφαλίδας (header) στην απάντηση της αναστοιχειοθέτησης (answer to reset)

Η λειτουργία της αναστοιχειοθέτησης (*answer to reset*) οδηγεί σε μια απάντηση από την κάρτα που περιέχει μια επικεφαλίδα, που διαβιβάζεται από την κάρτα στη διεπαφή. Η επιγραφή έχει ένα σταθερό μήκος από 32 bit και αρχίζει με δύο υποχρεωτικούς τομείς των 8 bit, H1 και H2.

Η χρονική σειρά της μετάδοσης των κομματιών (bits) πληροφοριών αντιστοιχεί στον προσδιορισμό κομματιών (bit) b1 b32 με το λιγότερο σημαντικό κομμάτι (*least significant bit*) που διαβιβάζεται πρώτα. Η αριθμητική σημασία που αντιστοιχεί σε κάθε κομμάτι (bit) πληροφορίας που εξετάζεται μεμονωμένα είναι αυτή του ψηφίου.

- 0 για μια μονάδα που αντιστοιχεί για να δηλώσει την κατάσταση A (διάστημα).
- 1 για μια μονάδα που αντιστοιχεί σε κατάσταση Z (σύμβολο).

Συγχρονισμός της επικεφαλίδας (header)

Μετά από τη διαδικασία αναστοιχειοθέτησης, οι πληροφορίες εξόδου ελέγχονται από τους παλμούς του ρολογιού. Ο πρώτος παλμός του ρολογιού εφαρμόζεται μεταξύ 10us και 100us (t14) μετά από την μείωση του RST για να διαβάσει τα κομμάτια στοιχείων (*data bits*) από την κάρτα. Η κατάσταση H του παλμού του ρολογιού μπορεί να πάρει τιμές μεταξύ 10us και 50us (t15) και η κατάσταση L μεταξύ 10us και 100us (t16).

Το πρώτο κομμάτι στοιχείων (*data bit*) λαμβάνεται στο I/O ενώ το ρολόι είναι χαμηλό και έχει τιμή τουλάχιστον 10us (t13) μετά από τη μείωση του RST. Τα ακόλουθα κομμάτια στοιχείων (data bits) είναι έγκυρα για χρόνο τουλάχιστον 10us (t17) μετά από την πτώση του CLK. Κάθε κομμάτι στοιχείων (*data bit*) ισχύει μέχρι την επόμενη μείωση του παλμού του ρολογιού CLK.

Τα κομμάτια στοιχείων (*data bits*) μπορούν επομένως να ελεγχθούν με δειγματοληψία στην αυξανόμενη άκρη του ακόλουθου παλμών ρολογιών.

Περιεχόμενο των στοιχείων της επικεφαλίδας (header)

Η επικεφαλίδα επιτρέπει έναν γρήγορο προσδιορισμό της κατάστασης της κάρτα και αν η συσκευή διεπαφών είναι συμβατή. Εάν δεν υπάρχει καμία συμβατότητα, οι επαφές θα είναι ανενεργές.

Ο πρώτος τομέας H1 κωδικοποιεί τον τύπο πρωτοκόλλου. Οι τιμές των κωδίκων και ο αντίστοιχος τύπος πρωτοκόλλου είναι:

Hexadecimal value	protocol type
00 and ff	not to be used
01 to FE	each value is assigned by ISO/IEC JTC1/SC17 to one protocol type

Ο δεύτερος τομέας H2 κωδικοποιεί τους παραμέτρους για τον τύπο του πρωτοκόλλου που κωδικοποιεί τον τομέα H1. Οι τιμές H2 πρόκειται να οριστούν από τον ISO/IEC JTC1/SC17.

2.3.5 Επιλογή τύπων πρωτοκόλλου (PTS)

Εάν μόνο ένας τύπος πρωτοκόλλου FI=D=1 (προκαθορισμένη αξία TA1) και N μικρότερο από 255 είναι υποδειγμένος στην απάντηση στην αναστοιχειοθέτηση (*answer to reset*). Το πρωτόκολλο μετάδοσης συνδεδεμένο με τον τύπο του πρωτοκόλλου μπορεί να αρχίσει αμέσως μετά από μετάδοση της απάντησης στην αναστοιχειοθέτηση (*answer to reset*).

Εάν περισσότεροι από έναν τύπο πρωτοκόλλου ή και TA1 τιμές παραμέτρου εκτός από τις προκαθορισμένες τιμές ή και το N ίσο με 255 είναι υποδειγμένες στην απάντηση στην αναστοιχειοθέτηση (answer to reset), η κάρτα ξέρει σαφώς, μετά που έχει στείλει την απάντηση στην αναστοιχειοθέτηση (answer to reset), ποιο τύπο πρωτοκόλλου και τιμές παραμέτρων μετάδοσης (FI, D, N) θα χρησιμοποιηθεί. Συνεπώς μια επιλογή του τύπου πρωτοκόλλου ή και οι τιμές παραμέτρων μετάδοσης θα διευκρινιστούν.

Εάν η κάρτα είναι σε θέση να επεξεργαστεί περισσότερους από έναν τύπους πρωτοκόλλου και εάν ένας από εκείνους τους τύπους πρωτοκόλλου είναι υποδειγμένοι όπως ο T=0, κατόπιν ο τύπος πρωτοκόλλου T=0 υποδειγμένος για TD1 ως πρώτος πρόσφερε το πρωτόκολλο, και υποτίθεται ότι κανένας PTS δεν εκτελείται.

Εάν μια κάρτα προσφέρει περισσότερα από ένα πρωτόκολλα και εάν οι υποστηρίξεις συσκευών διεπαφών αφορούν μόνο ένα από αυτά τα πρωτόκολλα που δεν είναι T=0 και δεν υποστηρίζει το PTS, η διεπαφή πρέπει να απορρίψει ή να επαναριθμήσει την κάρτα.

2.3.5.a Πρωτόκολλο PTS

Μόνο η συσκευή διεπαφών επιτρέπεται για να αρχίσει μια διαδικασία PTS:

- Η συσκευή διεπαφών στέλνει ένα αίτημα PTS στην κάρτα.
- Εάν η κάρτα λαμβάνει ένα σωστό αίτημα PTS, απαντά με την αποστολή ενός PTS επιβεβαίωσης, εάν εφαρμόζεται ή όχι, ο αρχικός χρόνος αναμονής θα ξεπεραστεί.
- Μετά από την επιτυχή ανταλλαγή του PTS, του αιτήματος PTS και της PTS επιβεβαίωσης, τα στοιχεία θα διαβιβαστούν από τη συσκευή διεπαφών χρησιμοποιώντας τους επιλεγμένους τύπους παραμέτρων ή και μετάδοσης πρωτοκόλλου.
- Εάν η κάρτα λάβει ένα λανθασμένο αίτημα PTS, δεν θα στείλει ένα PTS επιβεβαίωσης.
- Εάν περάσει ο αρχικός χρόνος αναμονής, η συσκευή διεπαφών πρέπει να απορρίπτει την κάρτα.
- Εάν η συσκευή διεπαφών λάβει ένα λανθασμένο PTS επιβεβαιώνει, πρέπει να επαναριθμήσετε ή να απορρίψετε την κάρτα.

Οι παράμετροι για τη μετάδοση του αιτήματος PTS και της PTS επιβεβαίωσης, επιβεβαιώνουν αντίστοιχα εκείνα που χρησιμοποιούνται στην απάντηση στην αναστοιχειοθέτηση για να επαναριθμήσουν το ποσοστό δυαδικών ψηφίων και η σύμβαση που ανιχνεύεται από το TS και που τροποποιείται ενδεχομένως από το TC1.

2.3.5.b Η δομή και το περιεχόμενο του αιτήματος και της επιβεβαίωσης PTS

Το αίτημα και η απάντηση κάθε ένα PTS αποτελούνται από έναν αρχικό χαρακτήρα PTSS, ακολουθούμενο από έναν χαρακτήρα της μορφής PTS0, τρεις προαιρετικούς παραμέτρους χαρακτήρων PTS1 PTS2 PTS3, και έναν χαρακτήρα ελέγχου PCK στην τελευταία ψηφιολέξη (*byte*).

Το PTSS προσδιορίζει το αίτημα PTS ή τα PTS επιβεβαιώνουν και κωδικοποιούνται FF. Το PTS0 υποδεικνύεται από τα κομμάτια (*bits*) b5, b6, b7 καθορισμένα σε 1 στη συνέχεια στέλνονται προαιρετικοί χαρακτήρες PTS1, PTS2, PTS3 αντίστοιχα. Κωδικοποιούνται Αυτό από τα λιγότερα σημαντικά στοιχεία (*least significant bits*) b4 έως b1 στο επιλεγμένο πρωτόκολλο τύπου T όπως κωδικοποιείται στις ψηφιολέξεις (bytes) του TD. Το σημαντικότερο κομμάτι (*most significant bit*) b8 (προεπιλογή b8=0) είναι διατηρημένο για μελλοντική χρήση.

Το PTS1 κωδικοποιεί τις παραμέτρους των τιμών του FI και το D όπως κωδικοποιείται στο TA1. Η συσκευή διεπαφών μπορεί να στείλει PTS1 προκειμένου να δηλώσουν την επιλογή του FI ή και της τιμής D στην κάρτα. Εάν PTS1 δε στέλνεται, τα FI=1 και D=1 θεωρούνται ως προεπιλογές.

Η κάρτα έτσι και αλλιώς βεβαιώνει την λήψη των τιμών FI και D με την αντήχηση PTS1 είτε στέλνεται PTS1 δείχνοντας τη χρήση των προκαθορισμένων αξιών.

Το PTS2 δείχνει την υποστήριξη N=255, όταν το κομμάτι (*bit*) b1 τίθεται σε κατάσταση 1. Το κομμάτι (*bit*) b1 καθορισμένο σε 0 είναι η προεπιλογή και δείχνει ότι η περίοδος 11 etu δεν χρησιμοποιείται. Εάν το κομμάτι (bit) b2 τίθεται 1, η κάρτα θα χρησιμοποιήσει ένα πρόσθετο χρόνο 12 etu για την εκπομπή των χαρακτήρων στη συσκευή διεπαφών. Το κομμάτι (*bit*) b2 καθορισμένο σε 0 είναι προκαθορισμένο και δείχνει ότι κανένας πρόσθετος χρόνος δεν απαιτείται. Το κομμάτι (bit) b3 b8 είναι διατηρημένο για μελλοντική χρήση.

Εάν το PTS2 στέλνεται από τη συσκευή διεπαφών και δεν αντηχείται από την κάρτα, η συσκευή διεπαφών πρέπει να απορρίψει ή να επαναριθμήσει την κάρτα.

Η κωδικοποίηση και η χρήση του PTS3 δεν καθορίζεται. Η αξία PCK θα είναι τέτοια ώστε για όλους τους χαρακτήρες από PTSS σε PCK που συμπεριλαμβάνονται να είναι μηδενικός.

2.3.6 Τύπος πρωτοκόλλου T=0, πρωτόκολλο ασύγχρονης μισής αμφίδρομης μετάδοσης χαρακτήρα (*asynchronous half duplex character transmission*)

Αυτή η πρόταση καθορίζει τη δομή και την επεξεργασία των εντολών που αρχίζουν από την συσκευή διασύνδεσης για τον έλεγχο μετάδοσης και για το συγκεκριμένο έλεγχο καρτών μέσα σε ένα ασύγχρονο μισό διπλό πρωτόκολλο μετάδοσης χαρακτήρα (*asynchronous half duplex character transmission*).

Αυτό το πρωτόκολλο χρησιμοποιεί τις παραμέτρους που υποδεικνύονται από την απάντηση για την αναστοιχειοθέτηση (*answer to reset*), εκτός αν τροποποιήσουμε την επιλογή των τύπων πρωτοκόλλου.

2.3.6.a Συγκεκριμένοι παράμετροι διεπαφών: ο χρόνος αναμονής εργασίας

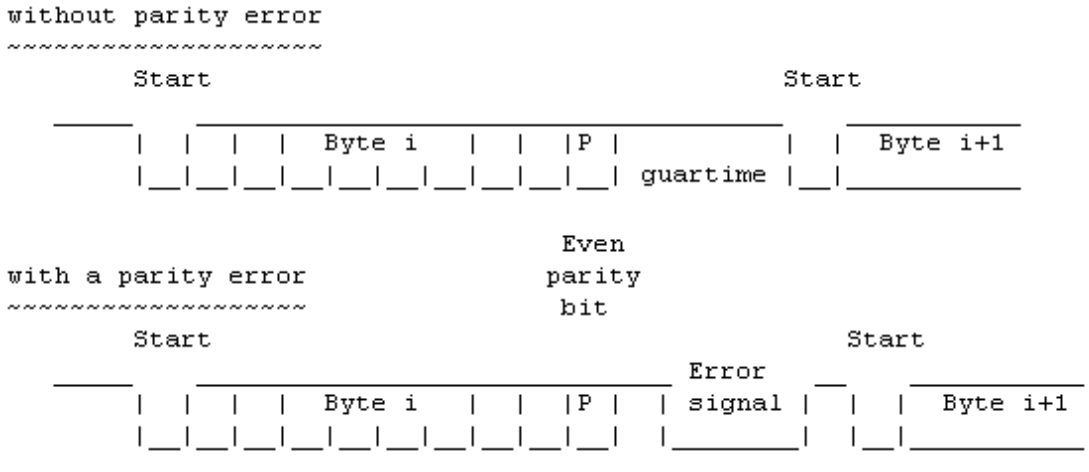
Σε μια απάντηση στην αναστοιχειοθέτηση, ο χαρακτήρας διεπαφών TC2 κωδικοποιεί την αξία ακέραιων αριθμών WI των οκτώ bit b8 έως b1. Όταν δεν εμφανίζεται κανένα TC2 στην απάντηση στην αναστοιχειοθέτηση (*answer to reset*), η προκαθορισμένη αξία των WI είναι 10.

Το διάστημα μεταξύ της αιχμής έναρξης οποιουδήποτε χαρακτήρα που στέλνεται από την κάρτα από την αιχμή έναρξης του προηγούμενου χαρακτήρα (που στέλνεται είτε από την κάρτα είτε από τη συσκευή διεπαφών) δεν υπερβαίνει το 960*OWI etu εργασίας. Αυτή η μέγιστη καθυστέρηση ονομάζεται χρόνος αναμονής εργασίας.

2.3.6.b Δομή και επεξεργασία των εντολών

Μια εντολή αρχίζει πάντα από τη συσκευή διεπαφών. Λέει στην κάρτα τι να κάνει σε μια επικεφαλίδα (*header*) 5-ψηφιολέξεων (5-byte), και να επιτρέψει μια μεταφορά των ψηφιολέξεων στοιχείων (*data byt*e) κάτω από τον έλεγχο των ψηφιολέξεων διαδικασίας που στέλνονται από την κάρτα.

Υποτίθεται ότι η κάρτα και η συσκευή διεπαφών ξέρουν εκ τον προτέρων την κατεύθυνση των στοιχείων, προκειμένου να ξεχωρίσουν μεταξύ των οδηγιών για εισερχόμενη μεταφορά στοιχείων (όπου τα στοιχεία εισάγονται στην κάρτα κατά τη διάρκεια της εκτέλεσης) και οδηγίες για τις εξερχόμενες μεταφορές στοιχείων (όπου τα στοιχεία αφήνουν την κάρτα κατά τη διάρκεια της



Αν

εκτέλεσης).

Σχήμα 2.3.4.9: Διάγραμμα μετάδοσης byte χωρίς ισοτιμία λάθους (*parity error*) και με ισοτιμία λάθους (*parity error*).

Εντολή επιγραφής στέλνεται από τη συσκευή διεπαφών

Η συσκευή διεπαφών διαβιβάζει μια επιγραφή άνω των πέντε διαδοχικών ψηφιολέξεων (*bytes*) οριζόμενο CLA, INS, A1, A2, L.

- CLA είναι μια κατηγορία οδηγίας. Η τιμή FF είναι κατοχυρωμένη για το PTS

- Το INS είναι ένας κώδικας οδηγίας στην κατηγορία οδηγίας. Η οδηγία του κώδικα ισχύει μόνο εάν το λιγότερο σημαντικό κομμάτι (*least significant bit*) είναι 0, και η πιο σημαντική μισή ψηφιολέξη (*most significant half byte*) δεν είναι ούτε 6 ούτε 9.

- P1, P2 είναι μια αναφορά (π.χ. μια διεύθυνση) ολοκληρώνοντας τον κώδικα οδηγίας

- P3 κωδικοποιεί τον αριθμό n ψηφιολέξεων στοιχείων (*data bytes*) (D1... , Dn) τα οποία πρόκειται να διαβιβασθούν κατά τη διάρκεια της εντολής. Η κατεύθυνση της μετακίνησης αυτών των στοιχείων είναι μια λειτουργία της οδηγίας. Σε μια εξερχόμενη εντολή μεταφοράς στοιχείων, το P3=0 εισάγει μια μεταφορά 256 στοιχείων ψηφιολέξεων από την κάρτα. Σε μία εισερχόμενη εντολή μεταφοράς στοιχείων, το P3=0 δεν εισάγει καμία μεταφορά των στοιχείων. Όλες οι υπόλοιπες δυνατότητες κωδικοποίησης για την επιγραφή διευκρινίζονται παρακάτω.

Μετά από τη μετάδοση τέτοιας επικεφαλίδας 5 ψηφιολέξεων, η συσκευή διεπαφών περιμένει την ψηφιολέξη διαδικασίας.

Διαδικασίες ψηφιολέξεων (bytes) που στέλνονται από την κάρτα

Η τιμή των ψηφιολέξεων θα δείξει τη δράση που ζητείται από την συσκευή διεπαφών. Υπάρχουν τρεις τύποι διαδικασιών ψηφιολέξεων:

- ACK: (Τα επτά σημαντικότερα κομμάτια σε μια ψηφιολέξη είναι όλα ίσα ή συμπληρωματικά με εκείνα στην ψηφιολέξη INS, εκτός από τις τιμές 6x και 9x). Ο έλεγχος της συσκευής διεπαφών της κατάστασης VPP και τα στοιχεία ανταλλαγών είναι ανάλογα με τιμές του ACK.

- NULL: (= $60) Αυτή η ψηφιολέξη (byte) στέλνεται από την κάρτα για να ξαναξεκινήσει το χρόνο απασχόλησης,

- SW1 (= $6x ή $9x, αναμένει $60) Η συσκευή διεπαφών διατηρεί ή θέτει VPP σε κατάσταση αναμονής και περιμένει μια SW2 ψηφιολέξη να ολοκληρώσει την εντολή. Οποιαδήποτε μετάβαση της κατάστασης VPP (ενεργού/αναμονής) πρέπει να εμφανιστεί μέσα σε συγκεκριμένο χρόνο από την διαδικασία ψηφιολέξης ή στην χρονική περίοδο της αναμονής της εργασίας.

Σε κάθε διαδικασία ψηφιολέξης, η κάρτα μπορεί να συνεχίσει με την εντολή από ένα ACK ή NULL ψηφιολέξη, ή παρουσιάζει την απόδειξη με το να γίνει αδιάφορη, ή ολοκληρώνει μια ακολουθία SW1-SW2.

Byte	Value	Result
	INS	VPP is idle. All remaining data bytes are transferred subsequently.
	INS+1	VPP is active. All remaining data bytes are transferred subsequently.
ACK	___	
	INS	VPP is idle. Next data byte is transferred subsequently.
	_____	
	INS+1	VPP is active. Newt data byte is transferred subsequently.
NULL	$60	No futher action on VPP. The interface device waits for a new procedure byte
SW1	SW1	VPP is idle. The interface device waits for a SW2 byte

Σχήμα 2.3.4.10: Διαδικασίες ψηφιολέξεων *(bytes*) που στέλνονται από την κάρτα

Ψηφιολέξεις Επιβεβαίωσης (Acknoledge bytes)

Οι ψηφιολέξεις ACK χρησιμοποιούνται για να ελέγξουν τη κατάσταση του Vpp και τη μεταφορά των στοιχείων.

- Κατά αποκλειστικότητα η ψηφιολέξη ACK με INS ψηφιολέξη δίνει $00 ή $$00, η συσκευή διεπαφών διατηρεί ή θέτει το VPP ενεργό.
- Κατά αποκλειστικότητα η ψηφιολέξη ACK με INS ψηφιολέξη δίνει $01 ή $$00, η συσκευή διεπαφών διατηρεί ή θέτει το VPP ενεργό.
- Όταν τα επτά σημαντικότερα κομμάτια στην ψηφιολέξη ACK έχουν την ίδια αξία όπως εκείνα στην ψηφιολέξη INS, όλες οι υπόλοιπες ψηφιολέξεις στοιχείων (Di…, Dn) εάν κάποιες παραμένουν, μεταφέρονται στη συνέχεια.
- Όταν τα επτά σημαντικότερα κομμάτια στην ψηφιολέξη ACK είναι συμπληρωματικά σε εκείνα στην ψηφιολέξη INS, μόνο η επόμενη ψηφιολέξη στοιχείων (Di), εάν κάποιο παραμένει, μεταφέρεται.

Μετά από αυτές τις ενέργειες, η συσκευή διεπαφών περιμένει μια νέα διαδικασία.

Μηδενική ψηφιολέξη - *Null Byte* (= $60)

Αυτή η ψηφιολέξη στέλνεται από την κάρτα για να επαναρυθμίσει το χρόνο εργασίας και να περιμένει μια επόμενη ψηφιολέξη διαδικασίας.

Ψηφιολέξεις θέσης (SW1=$6x ή $9x, αναμένουν $60 SW2 οποιαδήποτε αξία).

Η ακολουθία SW1-SW2 δίνει τη θέση καρτών στο τέλος της εντολής. Το κανονικό τελείωμα υποδεικνύεται από SW1-SW2 = $90-$00.

Όταν η σημαντικότερη μισή ψηφιολέξη SW1 είναι $6, η έννοια SW1 είναι ανεξάρτητη της εφαρμογής. Οι ακόλουθες πέντε τιμές διευκρινίζονται:

$6E η κάρτα δεν υποστηρίζει την κατηγορία οδηγίας.

$6D ο κώδικας οδηγίας δεν είναι προγραμματισμένος ή είναι άκυρος.

$6B η αναφορά είναι ανακριβής.

$67 το μήκος είναι ανακριβές.

$6F κανένας ακριβής διαγνωστικός έλεγχος δεν δίνεται.

Άλλες τιμές διατηρούνται για τη μελλοντική χρήση από ISO7816.

Όταν SW1 δεν είναι ούτε $6E ούτε $6D, η κάρτα υποστηρίζει την οδηγία.

Αυτό το μέρος ISO7816 δεν ερμηνεύει το $9X SW1 της ψηφιολέξης, ούτε το SW2 ψηφιολέξης. Η έννοιά τους αφορά την ίδια την εφαρμογή.

Ψηφιολέξεις διαδικασίας (Procedure bytes) που στέλνονται από την κάρτα

Η αξία των ψηφιολέξεων διαδικασίας θα δείξει τη δράση που ζητείται κοντά η συσκευή διεπαφών. Τρεις τύποι ψηφιολέξεων διαδικασίας διευκρινίζονται:

- ACK: (Τα επτά σημαντικότερα κομμάτια σε μια ψηφιολέξη ACK είναι όλος ο ίσος ή συμπληρωματικός σε εκείνοι στην ψηφιολέξη INS, εκτός από τις τιμές 6x και 9x). Το κράτος ελέγχου VPP συσκευών διεπαφών και τα στοιχεία ανταλλαγών ανάλογα με τιμές ACK.
- NULL: (= $60) αυτή η ψηφιολέξη στέλνεται από την κάρτα για να ξαναξεκινήσει το χρόνο απασχόλησης, τέλος για να προσδοκήσει μια επόμενη ψηφιολέξη διαδικασίας. Δεν ζητά κατόπιν η δράση ούτε σε VPP ούτε στα στοιχεία.
- SW1 (= $6x ή $9x, αναμένει $60) Η συσκευή διεπαφών διατηρεί ή θέτει VPP σε μη απασχόλησης και περιμένει μια SW2 ψηφιολέξη να ολοκληρώσει την εντολή. Οποιαδήποτε μετάβαση του κράτους VPP (ενεργού/μη απασχόλησης) πρέπει να εμφανιστεί μέσα στο *guardtime* από την ψηφιολέξη διαδικασίας, ή περιμένοντας χρονική υπερχείλιση της εργασίας. Σε κάθε byte διαδικασίας, η κάρτα μπορεί να συνεχίσει με την εντολή από ένα ACK ή Η ΜΗΔΕΝΙΚΗ byte, ή ολοκληρώνει κοντά μια ακολουθία Sw1-Sw2 τελών.

Συμπλήρωμα:

SW1 SW2 έννοια

62,81 Τα επιστρεφόμενα στοιχεία μπορούν να αλλοιωθούν.

62,82 Το τέλος του αρχείου έχει επιτευχθεί πριν από το τέλος της ανάγνωσης.

62,84 Το επιλεγμένο αρχείο δεν ισχύει.

65,01 Αποτυχία μνήμης. Έχουν υπάρξει προβλήματα εγγραφής ή ανάγνωσης του EEPROM.

Άλλα προβλήματα υλικού μπορούν επίσης να προκαλέσουν αυτό το λάθος.

68,00 Η λειτουργία αιτήματος δεν υποστηρίζεται από την κάρτα.

6A 00 ψηφιολέξεις P1 ή και P2 είναι ανακριβείς.

6A 80 οι παράμετροι στον τομέα στοιχείων είναι ανακριβή.

6A 82 αρχείο που δεν βρίσκεται.

6A 83 αρχείο που δεν βρίσκεται.

6A 84 υπάρχει ανεπαρκές διάστημα μνήμης στο στοιχείο ή το αρχείο.

6A 87 Η P3 αξία δεν είναι σύμφωνη με τις P1 και P2 τιμές.

6A 88 παραπεμφθέντα στοιχεία που δεν βρίσκονται.

6C XX ανακριβές P3 μήκος.

ΚΕΦΑΛΑΙΟ 3

ΤΗΛΕΚΑΡΤΕΣ

3.1 Εισαγωγή

Από τα μέσα της δεκαετίας του '80 έχει εμφανιστεί μια νέα γενεά καρτών (έξυπνες κάρτες ή κάρτες τσιπ) που έχουν αντικαταστήσει τις περισσότερες μαγνητικές κάρτες, που είχαν εφαρμογή, ειδικότερα σε ηλεκτρονικές πληρωμές και επίσης τις πιστωτικές κάρτες. Αυτές οι κάρτες είναι πολύ ασφαλέστερες από τις μαγνητικές κάρτες και υπάρχει μία πληθώρα εφαρμογών. Οι πιο απλές, είναι οι απλές κάρτες μνήμης, όπως αυτή που χρησιμοποιείται ως τηλεκάρτα. (Γενικά όλο το περιεχόμενο μνήμης είναι αναγνώσιμο, και υπάρχει και μία περιοχή, η περιοχή του κατασκευαστή της κάρτας, που δεν μπορούμε να γράψουμε).

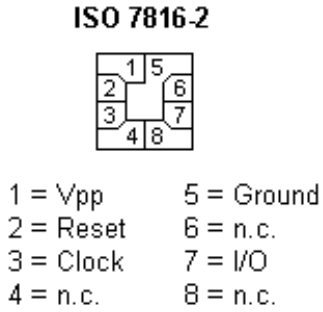
Σχετικά με τις τηλεκάρτες, ακόμα κι αν αυτές οι κάρτες είναι οι λιγότερο ασφαλείς, όλα τα στοιχεία μέσα στην κάρτα είναι αναγνώσιμα, δεδομένου ότι δεν υπάρχουν προσωπικά στοιχεία μέσα, οι κάρτες είναι πολύ ασφαλείς για την πληρωμή τηλεπικοινωνιών στο δημόσιο θάλαμο.

Τι ακριβώς είναι μία τηλεκάρτα; Στην πραγματικότητα είναι ένα 128 bit EEPROM ($1^{ης}$ γενιάς τηλεκάρτες) ή 256 bit EEPROM ($2^{ης}$ γενιάς τηλεκάρτες) με μία σειριακή έξοδο και μερικούς άλλους ακροδέκτες εξόδου.

Αυτό βέβαια δεν σημαίνει ότι μπορούμε να προγραμματίσουμε και τα 256 bit. Πριν περάσουμε σε αυτό βέβαια καλό θα ήταν να δούμε λίγο τον τρόπο πρόσβασης στις περιοχές μνήμης της τηλεκάρτας. Το ISO/AFNOR chip της τηλεκάρτας αποτελείται από 8 διαφορετικές διεπαφές οι οποίες είναι εμφανείς. Οι πιο βασικές από αυτές είναι η I/O(7), η VCC=+5V(1), η RESET (2) και η CLOCK (3). Η διαφορά μεταξύ ISO και AFNOR chip είναι στο *Pin-Out* και μόνο τα υπόλοιπα παραμένουν τα ίδια. Προκειμένου να προσπελάσουμε την θέση n στην μνήμη της τηλεκάρτας θα πρέπει να δώσουμε n σήματα (παλμούς) στο Clock εάν βρισκόμαστε στην θέση 0 ή n-m σήματα (παλμούς) στο Clock εάν βρισκόμαστε στην θέση m με mn τότε ή θα πρέπει να δώσουμε έναν παλμό στο Reset και μετά n σήματα στο Clock ή 256-m+n σήματα (το Clock λειτουργεί κυκλικά 256+1=0 θέση). Στην πραγματικότητα όμως ο ακροδέκτης 4 (Reset) δεν λειτουργεί, οπότε θα πρέπει πάντα να χρησιμοποιούμε το κυκλικό μοντέλο. Με αυτόν τον τρόπο μπορούμε και αναφερόμαστε στις θέσεις μνήμης της τηλεκάρτας. Πιο αναλυτικά:

Στο Chip υπάρχει PROM χωρητικότητας 256 bit. Εάν ο μετρητής βρίσκεται στην θέση n τότε μπορούμε να διαβάζουμε και να γράφουμε στην θέση n. Για να πάει κάποιος στην επόμενη διεύθυνση πρέπει να δώσει παλμό στο Clock του μετρητή. Τότε θα πάει στην θέση n+1. Υπάρχει και είσοδος Reset η οποία βάζει τον μετρητή στο 0. Ο μετρητής είναι κυκλικό μοντέλο. Δηλαδή εάν εμείς βρισκόμαστε στην θέση 20 , και θέλουμε να πάμε στην θέση 18 τότε υπάρχουν δυο τρόποι: Ο

πρώτος είναι να κάνουμε Reset και να δώσουμε 18 παλμούς στο Clock, και δεύτερος είναι να δώσουμε απλώς 254 παλμούς.



Σχήμα 3.1: Επαφή της τηλεκάρτας

3.2 Περιεχόμενα και περιοχές μνήμης

Το PROM από τον κατασκευαστή του έχει σε όλες τις θέσεις μνήμης του 0. Με τον προγραμματισμό του αλλάζουμε συγκεκριμένα bit από 0 σε 1. Μετά από αυτήν την αλλαγή δε μπορούμε να ξαναγράψουμε στο chip διότι είναι μιας χρήσης (μπορεί να προγραμματιστεί δηλαδή μια μόνο φορά). Οι τηλεκάρτες έχουν τα πρώτα 96bit σε μια περιοχή στην οποία δεν μπορούμε να γράψουμε (έχει κατασκευαστεί στο εργοστάσιο παραγωγής και έχει προστασία που περιλαμβάνει το λιώσιμο της εσωτερικής ασφάλειας). Σε αυτήν την περιοχή υπάρχουν πληροφορίες σχετικά με τον τύπο της κάρτας, το εργοστάσιο παραγωγής, το serial number της καθώς επίσης και την ημερομηνία λήξης της τηλεκάρτας. Η περιοχή από 96-105 ή 246-255 είναι μια περιοχή που περιέχει μόνο μονάδες (1) και αυτό έχει γίνει από τον κατασκευαστή για να ελέγχεται η ποιότητα της τηλεκάρτας. Οι υπόλοιπες περιοχές περιέχουν τις μονάδες της τηλεκάρτας. Αναλυτικότερα:

Το PROM μετά την παρασκευή του έχει 0 (μηδενικά) σε όλες τις θέσης της μνήμης από το 96 Bit μέχρι το 255 Bit, εμείς μπορούμε να αλλάξουμε το 0 σε 1 στις θέσεις μνήμης από 97 bit έως 256 bit, όμως ποτέ δεν θα μπορέσουμε να γράψουμε 0 αντί για 1 στις θέσεις μνήμης από 0 bit έως 95 bit γιατί είναι χώρος μνήμης *Read Only*. Οι τηλεκάρτες έχουνε μια περιοχή 96 bit στην οποία δεν μπορούμε να γράψουμε, αυτή η περιοχή είναι τα πρώτα 96 bit της PROM. Στην θέση αυτή υπάρχουν πληροφορίες για το εργοστάσιο παραγωγής του chip, το τύπο της κάρτας, το σειριακό αριθμό, και ημερομηνία λήξης της τηλεκαρτας. Υπάρχει μια περιοχή ακόμα στην οποία υπάρχουν άσσοι (1), αυτό έχει γίνει κατά την δοκιμή της ποιότητας της κάρτας στο εργοστάσιο και καταλαμβάνουν διευθύνσεις από 96 - 105 ή 246 - 255. Όπως καταλαβαίνουμε, όταν βάζουμε την τηλεκάρτα στην συσκευή το πρώτο πράγμα που γίνεται είναι: διαβάζει την προστατευόμενη περιοχή και συλλέγει πληροφορίες για την τηλεκάρτα, δηλαδή το εργοστάσιο παραγωγής όπως και την αξία της τηλεκάρτας. Εάν αυτή η τηλεκάρτα είναι ακόμη μέσα στα όρια χρήσης τότε προχωράει παρακάτω. διαβάζοντας μέχρι που είναι γραμμένη και πόσο χρόνος ομιλίας έμεινε. Κατά την ομιλία μας στο

τηλέφωνο το μηχάνημα γράφει στην θέση μνήμης του PROM της μονάδες (δηλαδή τα 1) και παράλληλα επαληθεύει την εγγραφή. Έτσι η διαδικασία συνεχίζεται μέχρι να γίνουν όλα τα μηδενικά μονάδες (0 ---> 1) στην θέση μνήμης της PROM από 96 bit έως 255 bit, οπότε έτσι τελειώνουν οι μονάδες στην κάρτα.

000:	**11011000**	**00101010**	**11111111**	**11001010**
032:	**00101110**	**11101000**	**01001100**	**11000000**
064:	**00000000**	**00000000**	**00000011**	**00000111**
096:	**00001111**	**1111111**1	**11111111**	**11111111**
128:	**11111111**	**11111111**	**11111111**	**11111111**
160:	**11111111**	**11111111**	**11111111**	**11111111**
192:	**11111111**	**11111111**	**11111111**	**11111111**
224:	**11111111**	**11111111**	**11111111**	**11111111**
256:	**11111111**	**11111111**	**11111111**	**11111111**
288:	**11111111**	**11111111**	**11111111**	**11111111**
320:	**10101010**	**00100100**	**11011011**	**11101111**
352:	**00010000**	**10011010**	**00101000**	**01111010**
384:	**11111111**	**11111111**	**11111111**	**11111111**
416:	**11111111**	**11111111**	**11111111**	**11111111**
448:	**11111111**	**11111111**	**11111111**	**11111111**
480:	**11111111**	**11111111**	**11111111**	**11111111**

= Τομέας Προσδιορισμού (*Identification Area*)

= Περιοχή Μετρητή (*Counter Area*)

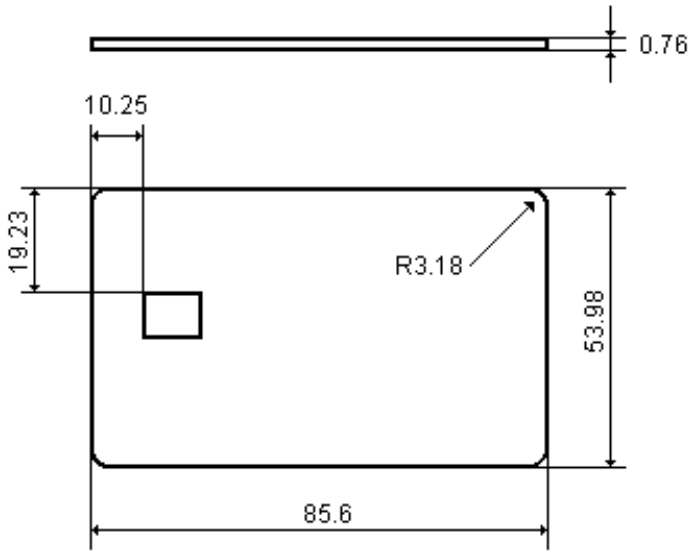
= Bit που ενεργοποιεί την ακολουθία πρόκληση/απάντηση (*Bit to activate Challenge/Response sequence*)

= Περιοχή στοιχείων 1 & 2 (*User Data Area 1 and 2*)

Σχήμα 3.2: Περιεχόμενα μνήμης

3.3 Γεωμετρική προδιαγραφή

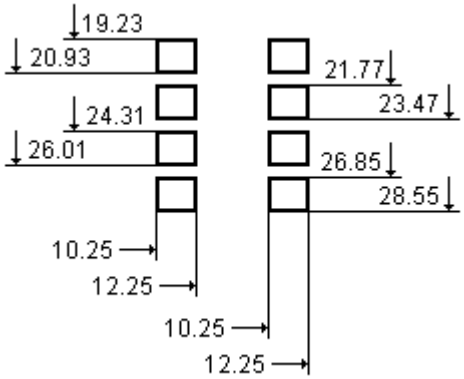
Μέγεθος της κάρτας σύμφωνα με τον ISO 7816 (όλες οι διαστάσεις σε mm)



Σχήμα 3.3.1: Μέγεθος της κάρτας σύμφωνα με τον ISO 7816

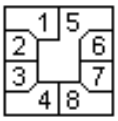
Η ακριβής θέση των επαφών chip:

(Όλες οι διαστάσεις μετρώνται σε mm, από την κορυφή ή από την αριστερή πλευράς της κάρτας. Κάθε επαφή πρέπει να έχει ένα ελάχιστο μέγεθος από 2 έως 1,7 mm. Φυσικά οι επαφές μπορούν να είναι μεγαλύτερες αλλά πρέπει να απομονωθούν κατάλληλα.)



Σχήμα 3.3.2: Η ακριβής θέση των επαφών chip.

3.4 Ηλεκτρικές προδιαγραφές



1 = Vpp	5 = Ground
2 = Reset	6 = n.c.
3 = Clock	7 = I/O
4 = n.c.	8 = n.c.

Vpp: Τάση τροφοδοσίας του chip, +5V

Reset: Αναστοιχειοθέτηση - επαναρίθμηση της κάρτας,

Clock: Ρολόι, εισαγωγή παλμών

Ground: Γείωση, 0V

I/O: Είσοδος/Εξοδος

n.c.: not connected, Δεν χρησιμοποιείται

Σχήμα 3.4: Ακροδέκτες της κάρτας

3.5 Το πρωτόκολλο

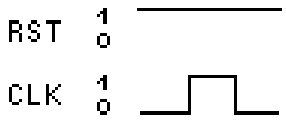
Η επικοινωνία με το τσιπ γίνεται άνω των 3 καλωδίων: RST, CLK και I/O .

Τα καλώδια RST και CLK ονομάζονται καλώδια ελέγχου. Το I/O καλώδιο απεικονίζει την κατάσταση του κυττάρου μνήμης του EPROM, το οποίο δείχνει ο μετρητής διευθύνσεων (*address counter*). Ο μετρητής διευθύνσεων θα μπορούσε μόνο να αυξηθεί ή να μειωθεί σε 0. Επειδή πρέπει

να είναι αδύνατη η επαναφόρτιση μίας τηλεκάρτας, μπορείτε μόνο να σβήσετε τα κομμάτια (*bits)* στην αντίθετη περιοχή (*counter area*). Εδώ είναι οι 4 εντολές:

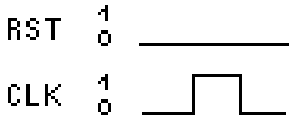
- **Θέστε τον μετρητή διευθύνσεων (*address counter*) σε κατάσταση 0**

Αύξηση της άκρης του CLK ενώ το RST είναι 1.



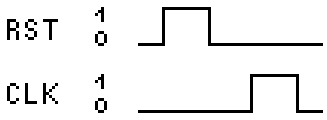
- **Αύξηση μετρητή διευθύνσεων**

Αύξηση της άκρης CLK ενώ το RST είναι 0.



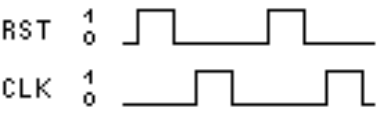
- **"Write" Γράψε ένα bit (θέστε 0)**

παλμός στο RST ενώ το CKL είναι 0, ακολουθούμενος από παλμό στο CLK ενώ το RST είναι 0. Ο μετρητής διευθύνσεων (*address counter*) δεν αλλάζει. Το "write" είναι δυνατό μόνο σε ορισμένες θέσεις.



- **"Write" Γράψε ένα bit με *carry* (*WriteCarry*)**

Εάν επαναλαμβάνετε την ακολουθία "write" δύο φορές στο ίδιο bit, το οποίο πρέπει να είναι το τελευταίο bit ενός οκτάμπιτου μετρητή (8-bit counter), αυτό το bit σβήνεται και στον επόμενο χαμηλότερο μετρητή γεμίζει με 11111111 (FFh). Παραδείγματος χάριν εάν εκτελέσουμε αυτήν την εντολή στο bit στην διεύθυνση 88, όλα τα bit από 96 έως 113 θα τεθούν 1. Με άλλα λόγια, αλλάξατε μια 8-μονάδα σε 81-μονάδες.



3.6 Χάρτης Μνήμης

3.6.1 Ελληνική τηλεκάρτα 128 bits (1ης γενιάς)

Byte (Bit)	Hexa				
0-3 (0..31)	$10	$2B	$FF	$7B	--> Greece (Gemplus)
	$92	$3B	$FF	$7B	--> Greece (G+D)
	$94	$3B	$FF	$7B	--> Greece (G+D)
	$98	$35	$1D	$7B	--> Greece (Solaic)
	$E8	$2B	$FF	$7B	--> Greece (Gemplus - 512 bits ???)
4-7 (32..63)	$..	$..	$..	$..	--> Serial Number (see below)
8..11 (64..95)	c512	c64	c8	c1	--> 4 stage octal counter
12 (96..103)	$..				
13 (104..111)	$..				
14 (112..119)	$..				
15 (120..127)	$..				

Σχήμα 3.6.1: Χάρτης μνήμης τηλεκάρτας 128 bits (1ης γενιάς)

ΣΗΜΕΙΩΣΗ: Για την Ελλάδα ο μετρητής είναι δύο φορές η αξία μονάδων της κάρτας (200 bit για μια 100u κάρτα).

Αύξων αριθμός (serial number) = b(63..32) που εμφανίζεται στο δεκαδικό.

Οι αύξοντες αριθμοί για Solaic φαίνονται να αρχίζουν από "11", Gemplus από "21", και Schlumberger από "31". Ένας νέος κατασκευαστής εμφανίζεται με την αρχή αυξόντων αριθμών από "41".

3.6.2 Ελληνική τηλεκάρτα 512 bits (2ης γενιάς)

Byte (Bit)	Hexa				
0..2 (0..23)	$93	$AB	$FF	$7B	--> Greece (Gemplus)
	$E8	$20	$FF	$7B	--> Greece (Schlumberger)
	$E9	$22	$80	$7B	--> Greece (Unknown manufacturer)
	$E9	$30	$FF	$7B	--> Greece (Schlumberger)
4..7 (32..63)	ss	ss	ss	ss	--> Serial Number
8..11 (64..95)	c512	c64	c8	c1	--> 4 stage octal counter
12..15 (96..127)	$FF	$FF	$FF	$FF	
16..63 (128..511)	$FF	. . +	. . +	. . +	$FF +

Σχήμα 3.6.2: Χάρτης μνήμης τηλεκάρτας 512 bits (2ης γενιάς)

Αύξων αριθμός (*serial number*) = b(63..32) που εμφανίζεται στο δεκαδικό.

Οι αύξοντες αριθμοί για Solaic φαίνονται να αρχίζουν από "11", Gemplus από "21", και Schlumberger από "31". Ένας νέος κατασκευαστής εμφανίζεται με την αρχή αυξόντων αριθμών από "41".

3.6.3 Χάρτης μνήμης για τις τηλεκάρτες από άλλες χώρες

```
Byte (Bit)      Hexa

                +-----+                                  95
0 (0..7)        |     |  --> Check Sum Byte = $D8 - Sum b(i)
                +-----+                                  i=8
1 (8..15)       | $83 |  --> Telecard
                | $80 |  --> Other Applications (See below)
                | $9A |  --> PIAF card [TBC]
                | $C0 |  --> AVANT card [TBC]
                +-----+-----+
2-3 (16..31)    | $1x | $xx |  --> Units+2 (0x1152 : exemple for a 150u card).
                + - - - - - +
                | $10 | $00 |  --> In case of special Argentine telecard
                | $3D | $13 |  -->  80u (Morocco)
                | $DB | $B5 |  -->  40u (Morocco)
                +-----+-----+

                ARGENTINA
                +-----+-----+-----+-----+
4..7 (32..63)   | $Ta | $bc | $de | $fg | T = Manufacturer (4 Gemplus, 0 Schlumberger)
                |     |     |     |     | S.N. = a*64 + b*32 + c*16 + d*8 + e*4 + f*2 + g
                +-----+-----+-----+-----+
8..9  (64..79)  |     |     | --> Don't Know
                +-----+-----+




                HUNGARY
                +-----+-----+-----+-----+
4..7 (32..63)   | $Ta | $B  | $C  | $D  | T = Manufacturer (4 Gemplus, C ODS)
                |     |     |     |     | S.N. = a*2^21 + B*2^17 + C*2^9 + D
                +-----+-----+-----+-----+
8..9  (64..79)  |     |     | --> Unit value : $0103 for 120u;  $010A for 50u
                +-----+-----+

                PORTUGAL
                +-----+-----+-----+-----+
4..7 (32..63)   | $00 | $A  | $B  | $C  | Portugal : S.N. = A*2^17 + B*2^9 + C
                +-----+-----+-----+-----+
8..9  (64..79)  |     |     | --> Certificate
                +-----+-----+

                OTHERS
                +-----+
4 (32..39)      | $Tx | --> T = Manufacturer 0 --> Schlumberger
                |     | -->                  1 --> Solaic [TBC]
                |     | -->                  3 --> Gemplus [TBC] (finnish cards)
                |     | -->                  4 --> Gemplus
                +-----+----+----+----+----+
5..9  (40..79)  |     |    |    |    |    | --> Serial Number
                +-----+----+----+----+----+
```

```
                +-----+-----+
10-11(80..95)   | $10 | $16 | --> French Polynesia
                |     | $78 | --> DisneyLand Paris (see note #1)
                | $11 | $15 | --> Djibouti
                |     | $1C | --> Senegal (Sonatel)
                |     | $1D | --> French Cinecarte [TBC]
                |     | $1E | --> Sweden
                |     | $28 | --> Argentina (Telefonica de Argentina)
                |     | $30 | --> Norway (Telenor).
                |     | $31 | --> New Caledonia
                |     | $32 | --> Cameroon
                |     | $33 | --> Andorra
                |     | $36 | --> Central African Republic (Socatel)
                |     | $39 | --> Luxembourg
                |     | $3C | --> Ireland
                |     | $3D | --> Gambia
                |     | $3F | --> Guinean Equatorial Republic (Getesa)
                |     | $47 | --> Portugal
                |     | $54 | --> Malta
                |     | $55 | --> Czech Republic / Yougoslavia
                |     | $58 | --> Comores
                |     | $5C | --> Argentina (Telecom Argentina)
                |     | $5D | --> Burkina Faso
                |     | $5E | --> Mali
                |     | $5F | --> Gabon
                |     | $65 | --> Finland
                |     | $6A | --> Madagascar (Telecom Malagasy S.A.)
                |     | $72 | --> Togo (OPT Togo)
                |     | $86 | --> Slovakia
                |     | $9E | --> Cuba (Etecsa)

                |     | $B7 | --> Morocco (Special Operator)
                |     | $BC | --> Israel (Bezeq)
                |     | $BE | --> Guinea (Sotelgui)
                |     | $C3 | --> Emirates (Etisalat)
                |     | $D5 | --> Poland
                |     | $E0 | --> Hungary
                |     | $E1 | --> Cameroon (CamTel)
                |     | $E2 | --> Morocco (Ave Phone)
                | $1E | $5C | --> Argentina (Special Cards)
                +-----+-----+
12 (96..103)    |     | --> The units area: each time a unit
     .          |     |     is used, then a bit is set to "1";
     .          |     |
     .          |     |     The first two units are fused in
     .          |     |     factory as test.
     .          |     |
     .          |     |     In some countries 5 extra units are burned when the
     .          |     |     card is empty (credit seems to be -5 units).
     .          |     |
     .          |     |     Hungary: Each bit set to 1 in this area is a unit used.
     .          |     |     ~~~~~~~  10u are used in factory when the cards is new.
31 (248..255)   |     |
                +-----+
```

Σχήμα 3.6.3: Χάρτης μνήμης τηλεκάρτας από άλλες χώρες

Σημείωση # 1: Για την DisneyLand του Παρισιού η περιοχή μονάδων του είναι b(128..239), B(30), όταν τίθεται $FF χαρακτηρίζει μια κενή κάρτα.

3.6.4 Χάρτης μνήμης για τις κάρτες από τη Γαλλία και του Μονακό

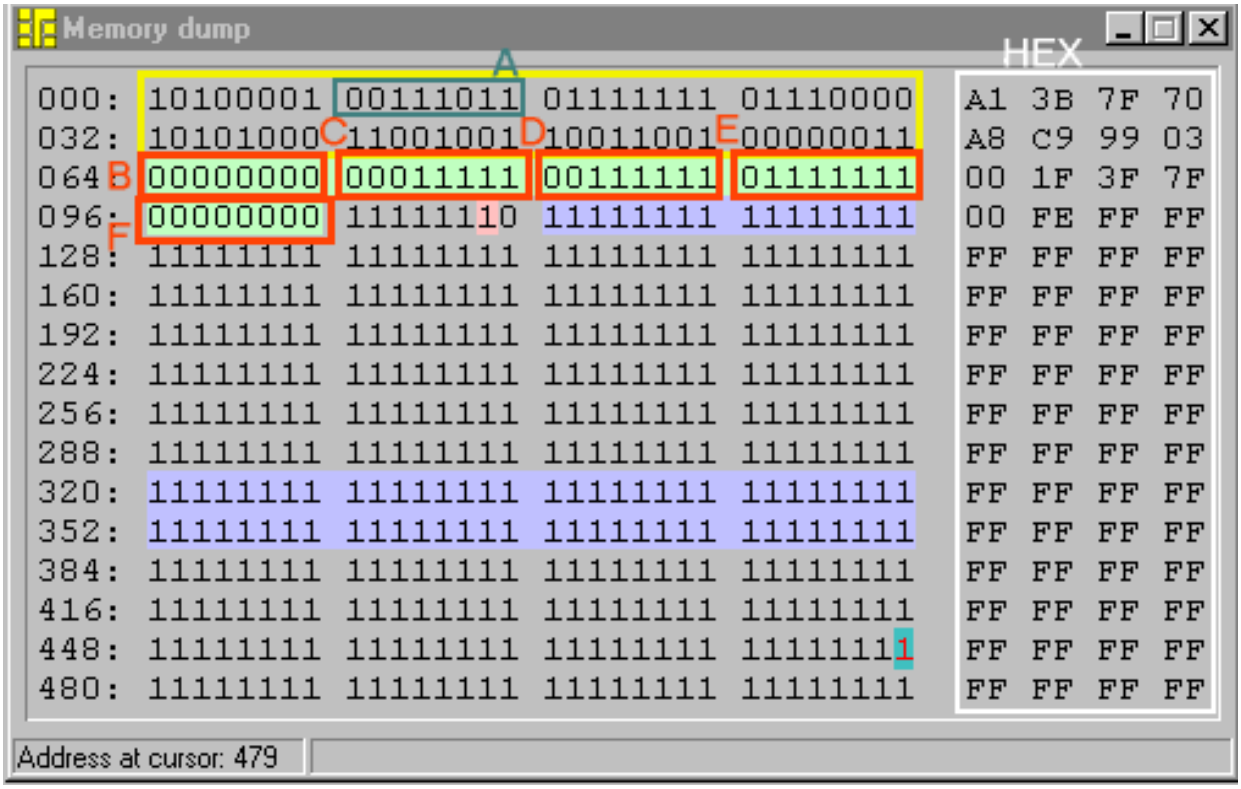
Byte (Bit)	Hexa		
0 (0..7)		-->	Checksum for bytes 1, 2, 3 (*)
1 (8..15)	$0s	-->	French telecard Serial Number (1st byte)
	$80	-->	St Marten
2 (16..23)		-->	Serial Number (2nd byte)
3 (24..31)		-->	Serial Number (3rd byte)
4 (32..39)		-->	checksum for bytes 5, 6, 7 (*)
5 (40..47)		-->	Serial Number (4th byte)
6 (48..55)		-->	Serial Number (5th byte)
7 (56..63)		-->	? [TBD]
	$FF	-->	St Marten
8 (64..71)		-->	checksum for byte 9, 10, 11 (*)
9 (72..79)		-->	? [TBD]
	$FF	-->	St Marten
10 (80..87)	$10	-->	France and Monaco
	$14	-->	St Marten
11 (88..95)	$13	-->	120 units
	$07	-->	60 units (St Marten)
	$06	-->	50 units
	$05	-->	40 units
	$04	-->	25 units
	$02	-->	5 units
12 (96..103)		-->	The unit area: each time a unit is used then a bit is set to "1"; The 1st 10 units are fused in factory for test (15 units for 25u and 5u cards).
.			
.			
.			
.			
30 (240..247)			
31 (248..255)	$FF	-->	$FF is set when all the units are used.

Σχήμα 3.6.4 Χάρτης μνήμης για τις κάρτες από τη Γαλλία και του Μονακό

(*) Το checksum υπολογίζεται από την ακόλουθη έκφραση:

max		min=32*(j-1)+8
$E3 - 4 * Sum b(i)	where	max=32*j-1
i=min		and j is the checksum number (1, 2 or 3)

3.6.5 Ανάλυση του περιεχομένου <u>γεμάτης</u> ελληνικής τηλεκάρτας με το πρόγραμμα SmartLab.



= Identification Area

= Counter Area

= Bit to activate Challenge/Response sequence

= User Data Area 1 and 2

A --> Country Code = Greece

B --> 4096 Units

C --> 512 Units

D --> 64 Units

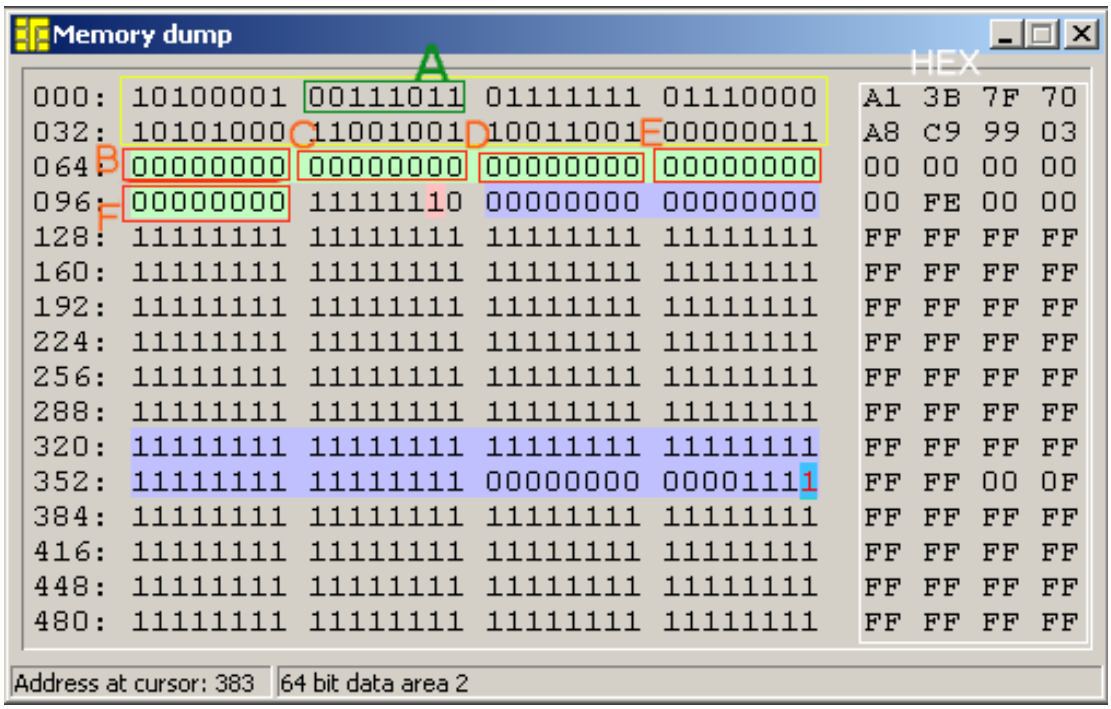
E --> 8 Units

F --> 1 Units

Στην Δεξιά στήλη υπάρχει ο ίδιος πίνακας σε δεκαεξαδική μορφή

Μονάδες στην κάρτα: 0*4096 + 5*512 + 6*64 + 7*8 + 0*1 = 12800 + 384 + 56 = 13240 Μονάδες

3.6.6 Ανάλυση του περιεχομένου <u>άδειας</u> ελληνικής τηλεκάρτας με το πρόγραμμα SmartLab



= Identification Area

= Counter Area

= Bit to activate Challenge/Response sequence

= User Data Area 1 and 2

A --> Country Code = Greece

B --> 4096 Units

C --> 512 Units

D --> 64 Units

E --> 8 Units

F --> 1 Units

Στη δεξιά στήλη υπάρχει ο ίδιος πίνακας σε δεκαεξαδική μορφή.

3.7 Ανάλυση της Τηλεκάρτας

3.7.1 Header – Επικεφαλίδα ή Επιγραφή:

Η επικεφαλίδα αποτελείται από 40 bits, τα οποία είναι ελεύθερα και προγραμματίσημα από τον κατασκευαστή καρτών. Συνήθως αυτή η περιοχή περιέχει την ημερομηνία έκδοσης και το *serial number*. Σημειώστε ότι (= 4 bit) η σύσταση από τα κομμάτια 36 - 63 πρέπει να αντανακληθεί για να διαβάσει την ημερομηνία και το *serial number* .

Παράδειγμα: Ψηφιολέξη (byte) 4 = 00100001b, ψηφιολέξη (byte) 5 = 00110101b

Είναι μια κάρτα με μια ονομαστική αξία 10. - (0010b). Το έτος έκδοσης είναι το 1998 (0001b που αντανακλάται = 1000b = 8d). Ο μήνας του ζητήματος είναι Δεκέμβριος (0011b που αντανακλάται = 1100b = 12d). Το ψηφίο 9 του αύξοντος αριθμού είναι "A" (0101b που αντανακλάται = 1010b = 10d = Ah).

3.7.2 Counter Area - Περιοχή του μετρητή

Αυτή η περιοχή περιέχει τις υπόλοιπες μονάδες στην κάρτα. Η αρχική αξία της είναι προγραμματισμένη στην κατασκευή του τσιπ. Η περιοχή του μετρητή διαιρείται σε 5 οκτάμπιτους μετρητές (*8-bit counters*). Ο αριθμός των κομματιών (*bits*) θέτονται σε κατάσταση 1 πολλαπλασιάζονται με το αντίστοιχο σθένος. Οι μετρητές έχουν σθένος 1, 8, 64, 512 και 4096.

	Byte 9	Byte 10	Byte 11	Byte 12	Byte 13
Δυαδική Αξία	0000 0000	0000 0111	0000 1111	0111 1111	0111 1111
Αριθμό των bits που θέτονται	0	3	4	7	7
Σθένος ενός bit	8^4=4096	8^3=512	8^2=64	8^1=8	8^0=1
Αξία	0*4096=0	3*512=1536	4*64=256	7*8=56	7*1=7
Συνολική αξία	1855				

Πίνακας 3.7.2: Μια τηλεκάρτα με 18,55 sFr, αντιστοιχεί σε 1855 μονάδες

3.7.3 Οκταδικός μετρητής

Η περιοχή του μετρητή (*counter area*) αποθηκεύει τις μονάδες της κάρτας. Η αρχική αξία της διευκρινίζεται από τον εκδότη των καρτών και τίθεται κατά τη διάρκεια της κατασκευής.

Η περιοχή του μετρητή (*counter area*), διαιρείται σε μετρητή 5 σταδίων, ή μετρητή 4 σταδίων. Ανάλογα με το chip:

- Γράψτε ένα bit και θέστε το για "1" για να αλλάξετε την αξία του θέστε το σε 0" (οικογένεια Eurochip).
- Γράψτε ένα bit και θέστε το για "0" για να αλλάξετε την αξία του θέστε το σε "1" (οικογένεια T2G).

Η οκταδική αξία κάθε σταδίου καθορίζεται από τον αριθμό των bits που έχουν τεθεί σε "1" (Eurochip και Γαλλικό T2G από τη France Telecom) ή "0" (Γαλλική T2G). Αυτή η αξία πρέπει να σταθμιστεί από τον συντελεστή 8^n (όπου το "n" είναι μεταξύ [4..0] ή [3..0]).

Byte8 (c4096)	Byte9 (c512)	Byte10 (c64)	Byte11 (c8)	Byte12 (c1)
00000111	00111111	01111111	00000001	00000011
(3)octal	(6)octal	(7)octal	(1)octal	(2)octal

Value = 3*8^4 + 6*8^3 + 7*8^2 + 1*8^1 + 2*8^0
= 3*4096 + 6*512 + 7*64 + 1*8 + 2*1

TOTAL = 15818 Units

Πίνακας 3.7.3.1: Οκταδικός μετρητής 5 καταστάσεων με 15818 μονάδες για Eurochip or French T2G from France Telecom.

Byte8 (c4096)	Byte9 (c512)	Byte10 (c64)	Byte11 (c8)	Byte12 (c1)
11111000	11000000	10000000	11111110	11111100
(3)octal	(6)octal	(7)octal	(1)octal	(2)octal

Value = 3*8^4 + 6*8^3 + 7*8^2 + 1*8^1 + 2*8^0
= 3*4096 + 6*512 + 7*64 + 1*8 + 2*1

TOTAL = 15818 Units

Πίνακας 3.7.3.2: Οκταδικός μετρητής 5 καταστάσεων με 15818 μονάδες, για French T2G.

Δύο τύποι καρτών υπάρχουν:

- Κάρτες που μετρούν τις υπόλοιπες μονάδες (κυρίως Eurochips και Γαλλικές T2G)
- Κάρτες που μετρούν τις χρησιμοποιημένες μονάδες (κυρίως Γαλλικές T2G από France Telecom).

Για τις κάρτες που μετρούν τις χρησιμοποιημένες μονάδες πρέπει να ξέρετε την αξία της κάρτας (για να υπολογίσει την υπόλοιπη αξία της κάρτας). Πρέπει να γνωρίσετε τον αριθμό των μονάδων που "καίγεται" στο εργοστάσιο (προκειμένου να εξεταστεί η κάρτα).

Για παράδειγμα: Για 120 μονάδες της Γαλλικής τηλεκάρτας από τη France Telecom 9 μονάδες καίγονται στο εργοστάσιο, έτσι μια πλήρως χρησιμοποιημένη κάρτα μετρά 129 μονάδες.

```
          b64 ..................................... b103
          ---------------------------------------------------
          00000111 - 00111111 - 01111111 - 00000000 - 00000011
-1                                                      ^     WRITE(b102)
          00000111 - 00111111 - 01111111 - 00000000 - 00000001
-1                                                       ^    WRITE(b103)
          00000111 - 00111111 - 01111111 - 00000000 - 00000000
-1                             ^         ^          ^
          00000111 - 00111111 - 00111111 - 11111111 - 00000000 + WRITECARRY(b81)
          00000111 - 00111111 - 00111111 - 01111111 - 11111111 + WRITECARRY(b88)
          00000111 - 00111111 - 00111111 - 01111111 - 01111111 + WRITE(b96)
-1
          00000111 - 00111111 - 00111111 - 01111111 - 00111111 + WRITE(b97)
-1
          00000111 - 00111111 - 00111111 - 01111111 - 00011111 + WRITE(b98)

          Etc ....
```

Πίνακας 3.7.3.3: Πίνακας WRITE και WRITECARRY (Eurochip).

Ας σημειωθεί ότι μπορείτε μόνο να μειώσετε το μετρητή και δε μπορείτε να γράψετε στο μετρητή μια αξία μεγαλύτερη από την παλαιά αξία.

Στην πραγματικότητα οι περισσότερες από τις μονάδες καρτών δεν αντιπροσωπεύουν τις τηλεφωνικές μονάδες, αλλά το κόστος τον μονάδων, για παράδειγμα στις γερμανικές κάρτες κάθε τηλεφωνική μονάδα αντιπροσωπεύει 30 πένες.

3.7.4 Αύξων αριθμός - *serial number*

Ο μοναδικός αριθμός που ορίζεται σε ένα τσιπ, αυτός ο αριθμός είναι προγραμματισμένος στο chip από τον κατασκευαστή, δεν μπορείτε να τον αλλάξετε. Μερικές κάρτες δεν έχουν αύξοντα αριθμό. Ένα αντίγραφο του αύξοντος αριθμού είναι μερικές φορές τυπωμένος στην ίδια στην κάρτα.

3.7.5 *Checksum*

Checksums χρησιμοποιούνται προκειμένου να ελεγχθεί εάν η επιγραφή μιας κάρτας (header) δεν έχει αλλαχθεί. Μια ψηφιολέξη της επιγραφής(header) υπολογίζεται χρησιμοποιώντας έναν απλό τύπο (δηλ.: αν θέσω ένα μπιτ στη θέση "1" στις ψηφιολέξεις (bytes) 1 ..2 ..3 αφαιρώ 4 στην αξία 227, πρέπει να λάβετε την συνολική αξία της κάρτας στην ψηφιολέξη 0.

Μπορείτε να χρησιμοποιήσετε αυτά τα checksums (και άλλα bits στην περιοχή του header) για να ελέγξετε εάν μια κάρτα είναι γνήσια.

3.7.6 Πιστοποίηση - *certificate*

Η πιστοποίηση χρησιμοποιείται στης 2ης γενιάς τηλεκάρτες για να ελέγξουν εάν μια κάρτα είναι πλαστή. Τα πιστοποιητικά έχουν μήκος 16 ή 32 και υπολογίζονται χρησιμοποιώντας μια λειτουργία (κάθε χειριστής έχει την δική του), ένα μυστικό κλειδί (ο χειριστής το καθορίζει αυτό) και η αξία των κομματιών περιλαμβάνονται στην επιγραφή (header) της κάρτας.

Επειδή η λειτουργία και το κλειδί κρατιούνται μυστικά, δεν μπορούμε να υπολογίσουμε ένα πιστοποιητικό, ούτε μπορούμε να ελέγξουμε εάν η κάρτα είναι ενός δεδομένου τύπου.

Προκειμένου να αποφύγουμε τους χάκερ που κάνουν crypto-ανάλυση στα πιστοποιητικά που χρησιμοποιεί ένας μεγάλος αριθμός καρτών, αυτό το πιστοποιητικό μπορεί να σβηστή όταν η κάρτα είναι κενή. Η εγγραφή σε αυτήν την περιοχή μπορεί να ακυρώσει την κάρτα.

3.7.7 Μετρητής-(counter)/ Μονάδα-(Unit)

Αυτή η περιοχή περιέχει τον αριθμό μονάδων που παραμένουν (ή έχουν χρησιμοποιηθεί) στην κάρτα. Σχεδιάζεται έτσι ώστε δεν μπορούμε να αυξήσουμε την αξία της κάρτας. Το πώς γίνεται αυτή η εργασία, (αποκωδικοποίηση και γράψιμο) εξαρτάται από τον τύπο της κάρτας.

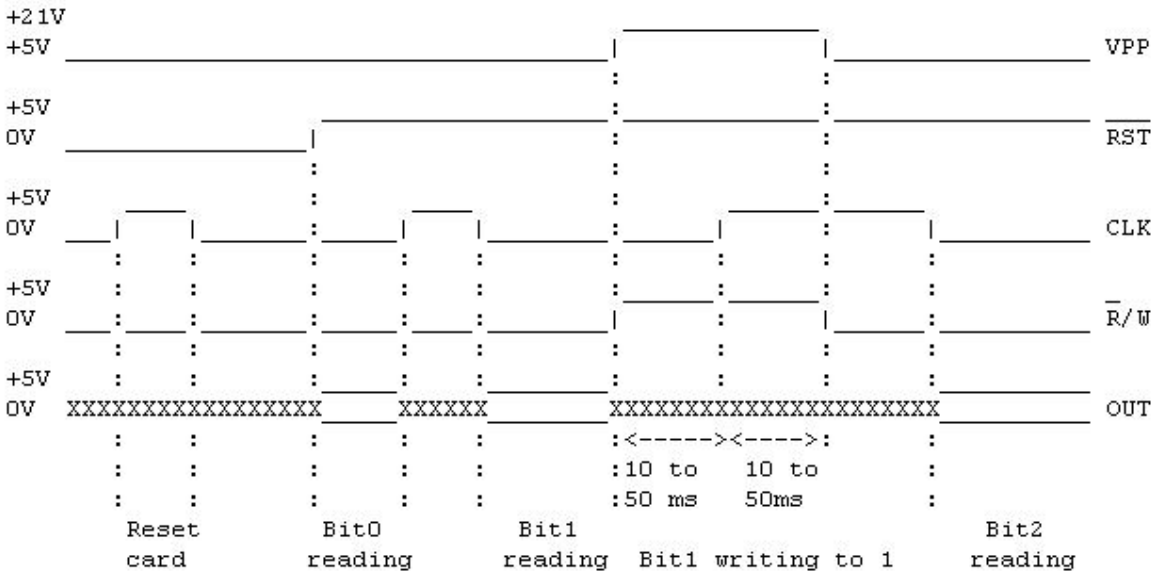
3.7.8 Anti-tearing

Οι Anti-tearing σημαίες (επίσης γνωστές ως pull-out σημαίες) χρησιμοποιούνται για να εξασφαλίσουν στον κάτοχο της κάρτας ότι δεν θα χάσει μονάδες (χρήματα) εάν αφαιρέσει την κάρτα κατά τη διάρκεια μιας λειτουργίας. Οι Anti-tearing_σημαίες γράφονται όταν γράφει και ο μετρητής (counter), σβήνονται όταν ολοκληρώνεται η λειτουργία. Εάν η κάρτα αφαιρεθεί κατά τη διάρκεια της λειτουργίας της, χρησιμοποιείται η Anti-tearing διαδικασία, για να αποκαταστήσει την περιοχή του μετρητή (counter area) την επόμενη φορά που θα χρησιμοποιηθεί η κάρτα.

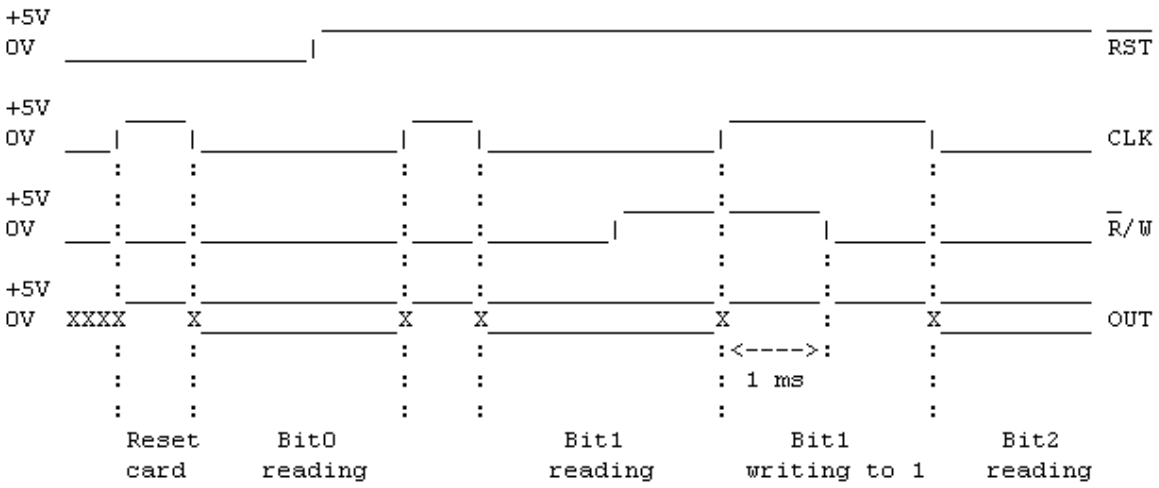
3.7.9 Επικύρωση - *Authentification*

Η επικύρωση χρησιμοποιείται στης 2ης γενιάς τηλεκάρτες ο αναγνώστης στέλνει μια τυχαία ακολουθία αποκαλούμενη "πρόκληση" ή “challenge”, αυτή η πρόκληση χρησιμοποιείται από την κάρτα για να υπολογίσει την απάντηση που θα στείλει πίσω στον αναγνώστη. Εάν η απάντηση είναι σωστή ο αναγνώστης μπορεί να υποθέσει ότι η κάρτα είναι "έγκυρη".

3.8 Χρονικά Διαγράμματα



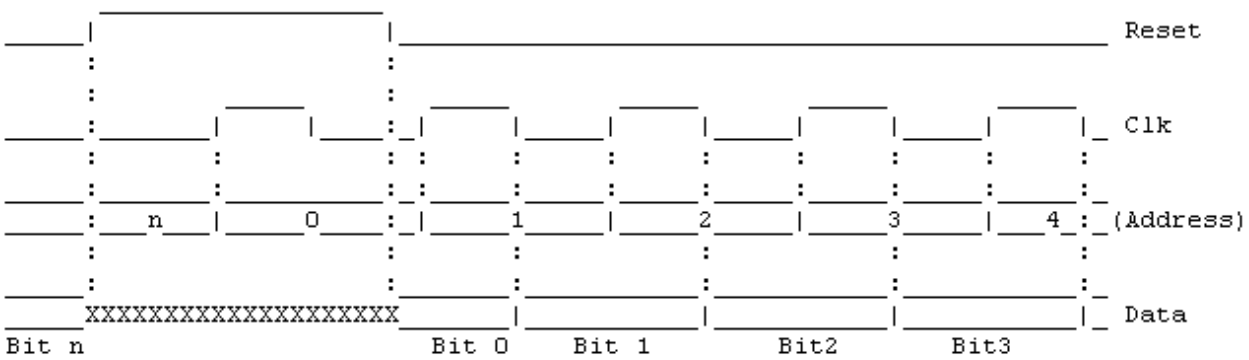
Σχήμα 3.8.1 Κάρτες από Schlumberger, Solaic, Gemplus



Σχήμα 3.8.2 Κάρτες από G+D (Ισπανικές κάρτες που χαρακτηρίζονται από το 5^{o} byte (ψηφιολέξη) = $30).

Reset

Ο μετρητής διευθύνσεων επαναρρυθμίζεται σε 0 όταν αυξάνεται η γραμμή CLK ρολογιών ενώ η γραμμή R ελέγχου είναι υψηλή (σημειώστε ότι ο μετρητής διευθύνσεων δεν μπορεί να επαναρρυθμιστεί όταν είναι στη σειρά 0 έως 7).



Σχήμα 3.8.3 Εντολή Reset

Ο μετρητής διευθύνσεων αυξάνεται κατά 1 με κάθε παλμό του ρολογιού CLK, εφ' όσον η γραμμή ελέγχου R παραμένει χαμηλή. Τα στοιχεία που φυλάσσονται μέσα σε κάθε εξετασμένο κομμάτι είναι η παραγωγή στην I/O επαφή κάθε φορά που μετράει το CLK. Είναι αδύνατον να μειώσουμε τον μετρητή διευθύνσεων, επομένως πρέπει να εξετάσουμε το προηγούμενο κομμάτι (bit). Ο μετρητής διευθύνσεων πρέπει να επαναρρυθμιστεί, για να ζητήσει την αξία.

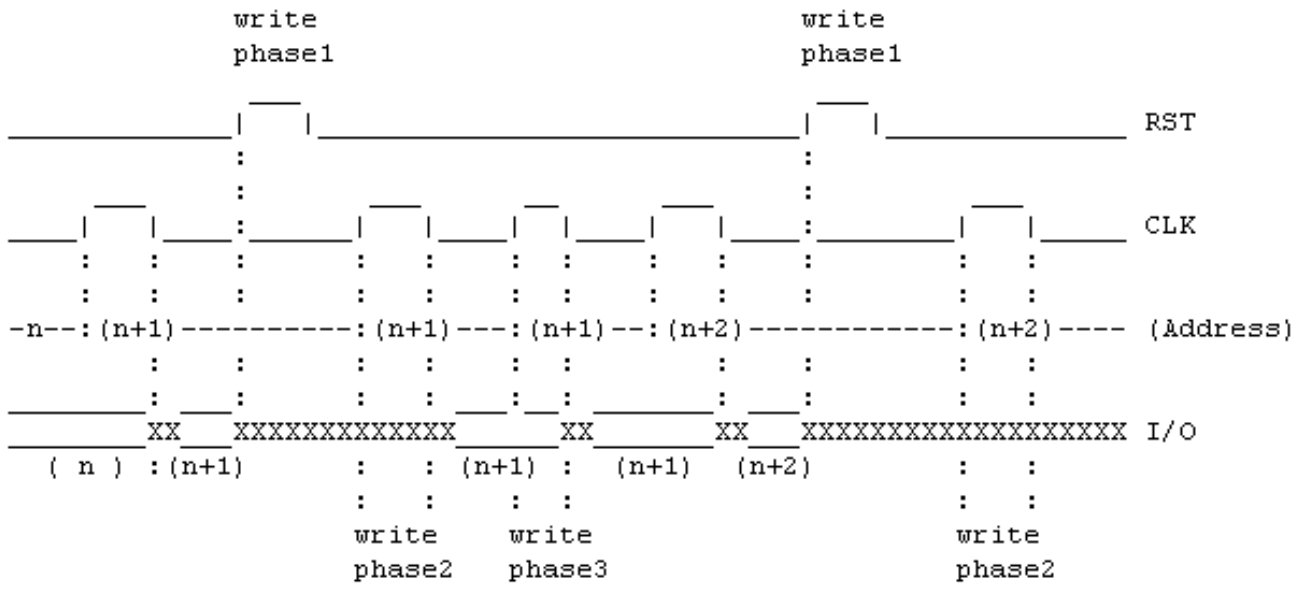
Λειτουργία Εγγραφής (write operation):

Όλα τα άγραφα κομμάτια (bits) στη διεύθυνση 64-103 μπορούν να γραφτούν (θέστε "0"). Όταν ένα bit είναι άγραφο, τίθεται σε κατάσταση "1". Το εξετασμένο κομμάτι (addressed bit) μπορεί να γραφτεί από την ακόλουθη διαδικασία:

1. Το RST αυξάνεται ενώ το CLK είναι χαμηλό, για να θέσω εκτός λειτουργίας τον μετρητή διευθύνσεων (address counter) αυξάνω για ΔΥΟ παλμούς του ρολογιού (όχι ένα παλμό ρολογιού, όπως αναφέρεται σε άλλα κείμενα).
2. Το CLK αυξάνεται για ένα ελάχιστο χρόνο (10ms) για να γράψει στο εξετασμένο κομμάτι. (addressed bit).
3. Το CLK αυξάνεται πάλι για ένα ελάχιστο χρόνο (1ms) για να τελειώσει την λειτουργία εγγραφής.

Όταν η λειτουργία εγγραφής τελειώσει και ο CLK πέσει, ο μετρητής διευθύνσεων (*address counter*) ξεκλειδώνεται, και το περιεχόμενο του γραπτού κελιού (*written cell*), που είναι τώρα “0”, είναι η έξοδος της I/O επαφής.

Ο επόμενος παλμός του CLK θα αυξήσει τη διεύθυνση κατά ένα, κατόπιν η ακολουθία της εγγραφής μπορεί να επαναληφθεί για να γράψετε το επόμενο κομμάτι (bit).



Σχήμα 3.8.4: Λειτουργία Εγγραφής (*write operation*)

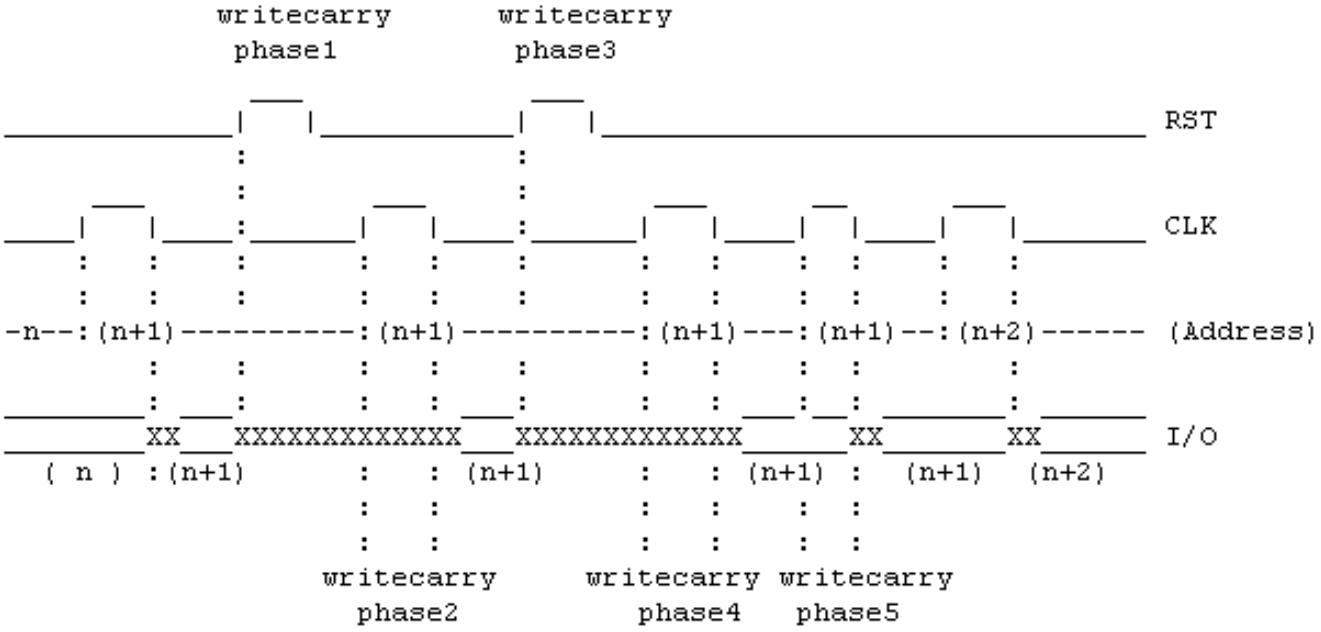
Λειτουργία *WriteCarry*

Η ακολουθία WriteCarry χρησιμοποιείτε για να γράψει το διευθυνσιοδοτημένο κομμάτι (*addressed bit*) και να σβήσει το επόμενο στάδιο του μετρητή (θέστε όλα τα κομμάτια (bits) σε κατάσταση "1") ταυτόχρονα.. Δεν είναι δυνατό να σβηστεί το επόμενο στάδιο του μετρητή εάν το διευθυνσιοδοτημένο κομμάτι (addressed bit) είναι ήδη γραμμένο (θέστε το σε "0").

Η ακολουθία WriteCarry είναι η ακόλουθη:

1. Το RST αυξάνεται ενώ το CLK είναι χαμηλό, για να θέσουμε εκτός λειτουργίας την αύξηση του μετρητή διευθύνσεων (addressed counter).
2. Το CLK αυξάνεται για ένα ελάχιστο χρόνο (10ms) για να γράψει στο εξετασμένο κομμάτι (*addressed bit*).

3. Το RST αυξάνεται πάλι ενώ το CLK είναι χαμηλό για να θέσει εκτός λειτουργίας την αύξηση διευθύνσεων για τους επόμενους δύο παλμούς του ρολογιού.



4. Το CLK αυξάνει για ένα ελάχιστο χρόνο (10ms) για να σβήσει το επόμενο στάδιο του μετρητή.

Σχήμα 3.8.5: Λειτουργία *WriteCarry*

Όλα τα κομμάτια (bits) στο επόμενο στάδιο του μετρητή έχουν τεθεί σε κατάσταση "1".

5. Το CLK αυξάνει πάλι για ένα ελάχιστο χρόνο (1ms) για να λήξη την *writecarry* λειτουργία.

Initial state of credits counter	b64 ..... b103 00000111 - 00111111 - 01111111 - 00000000 - 00000011
Counter decrease by 1	Action: Write operation on bit 102 Result: 00000111 - 00111111 - 01111111 - 00000000 - 00000001
Counter decrease by 1	Action: Write operation on bit 103 Result: 00000111 - 00111111 - 01111111 - 00000000 - 00000000
Counter decrease by 1	Action: WriteCarry operation on bit 81 Result: 00000111 - 00111111 - 00111111 - 11111111 - 00000000 Action: WriteCarry operation on bit 88 Result: 00000111 - 00111111 - 00111111 - 01111111 - 11111111 Action: Write operation on bit 96 Result: 00000111 - 00111111 - 00111111 - 01111111 - 01111111
Counter decrease by 1	Action: Write operation on bit 97 Result: 00000111 - 00111111 - 00111111 - 01111111 - 00111111
Counter decrease by 1	Action: Write operation on bit 98 Result: 00000111 - 00111111 - 00111111 - 01111111 - 00011111

Σχήμα 3.8.7: Παράδειγμα της ακολουθίας Write και WriteCarry.

3.9 Ηλεκτρικά χαρακτηριστικά

Γενικά Χαρακτηριστικά

	Σύμβολο	Ελάχιστη	Μέγιστη	Μονάδες
Τάση Τροφοδοσίας	Vcc	-0.3	6	V
Τάση Εισόδου	Vss	-0.3	6	V
Θερμοκρασία Λειτουργίας	Tstg	-20	+55	^{o}C
Ισχύς Απωλειών	Pd	-	50	mW

Πίνακας 3.9.1: Γενικά χαρακτηριστικά

DC Χαρακτηριστικά

	Σύμβολο	Ελάχιστη	Μέγιστη	Μονάδες
Ρεύμα Τροφοδοσίας	Icc	-	5	MA
Τάση Εισόδου (low) (χαμηλή)	Vl	0	0.8	V
Τάση Εισόδου (high) (υψηλή)	Vh	3.5	Vcc	V
Ρεύμα Εισόδου R	Ih	-	100	uA
Ρεύμα Εισόδου Clk	Il	-	100	uA
Ρεύμα Εξόδου (χαμηλό) (Vol=0.5V)	Iol	-	10	uA
Ρεύμα Εξόδου (χαμηλό) (Voh=5V)	Ioh	-	0.5	mA

Πίνακας 3.9.2: DC Χαρακτηριστικά

AC Χαρακτηριστικά

	Σύμβολο	Ελάχιστη	Μέγιστη	Μονάδες
Διάρκεια Παλμού R αναστοιχειοθέτηση διευθύνσεων (reset address)	tr	50	-	us
Διάρκεια Παλμού R Εγγραφής (write)	ts	10	-	us
Υψηλή Στάθμη ρολογιού (High level Clk)	th	8	-	us
Χαμηλή Στάθμη ρολογιού (Low level Clk)	tl	12	-	us

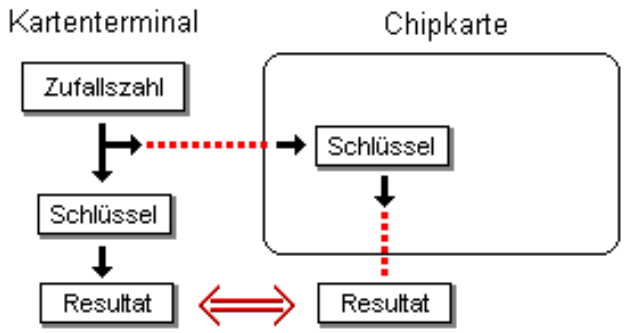
Εγγραφή Παραθύρου (Write window)	Twrite	10	-	us
Σβήσιμο Παραθύρου (Erase window)	Terase	10	-	us
	tv1	5	-	us
	tv2	3.5	-	us
	tv3	3.5	-	us
	tv4	3.5	-	us
	tv5	3.5	-	us
	tv6	5	-	us
	tv7	5	-	us

Πίνακας 3.9.3: AC Χαρακτηριστικά

3.10 Χαρακτηριστικά του Chip (2ης γενιάς τηλεκάρτες)

3.10.1 Ασφάλεια

Φυσικά μία τηλεκάρτα έχει διάφορα χαρακτηριστικά γνωρίσματα ασφάλειας για να αποτρέψει την κατάχρηση. Παραδείγματος χάριν μια απλή λογική αποτρέπει το μετρητή από την αύξηση. Η αυθεντικότητα της κάρτας εξετάζεται με ένα πρωτόκολλο πρόκλησης/απάντησης (*challenge/ response protocol*). Τα βήματα αυτής της διαδικασίας είναι τα εξής :



Σχήμα 3.10.1: Διαδικασία πιστοποίησης αυθεντικότητας της κάρτας

1. Το τερματικό (τηλέφωνο) υπολογίζει έναν τυχαίο αριθμό τον στέλνει στην κάρτα.
2. Το τερματικό και η κάρτα και οι δύο κάνουν έναν μυστικό υπολογισμό χρησιμοποιώντας αυτόν τον τυχαίο αριθμό.

3. Η κάρτα στέλνει το αποτέλεσμα εκείνου του υπολογισμού πίσω στο τερματικό.

4. Το τερματικό συγκρίνει το αποτέλεσμα από την κάρτα με το αποτέλεσμά του.

Μόνο εάν και τα δύο αποτελέσματα είναι τα ίδια, το τερματικό ξέρει ότι μιλά σε μια "πραγματική" κάρτα.

3.10.2 SLE4436

Το SLE4436 είναι ένα τσιπ για τις σύγχρονες τηλεκάρτες που κατασκευάζεται από τη SIEMENS. Χρησιμοποιείται σε όλο τον κόσμο στα σύγχρονα συστήματα τηλεκαρτών. Τα κυριότερα σημεία του τσιπ είναι τα ακόλουθα:

*** 221 bit EEPROM and 16 bit maskprogrammable ROM.**

Τα πρώτα 64 bit είναι ο **"τομέας προσδιορισμού" (*Identification Area*)** που θα μπορούσε να κωδικοποιηθεί από τον κατασκευαστή καρτών. Μετά από αυτήν την περιοχή τα 40 bit είναι η **"περιοχή του μετρητή" (*Counter Area*).** Επιπλέον υπάρχει μία περιοχή 16 bit, είναι η **"περιοχή στοιχείων χρηστών 1" (*User Data Area 1*)** από τη διεύθυνση 112 έως 127 bit σε αυτήν την σειρά θα μπορούσαν να διαγραφούν. Δυστυχώς η λειτουργία αυτών των κομματιών στις τηλεκάρτες είναι άγνωστη. Μία δεύτερη περιοχή 64 bit **"περιοχή στοιχείων χρηστών 2" (*User Data Area 2*)** βρίσκεται από τη διεύθυνση 320 έως 383. (Εάν δεν υπάρχει κανένα δεύτερο κλειδί επικύρωσης χρησιμοποιούμενο, δείτε επίσης το datasheet του chip).

*** Counter with up to 33352 count units fully compatible with SLE 4406**.

Περιέχει ένα μετρητή (counter) με πάνω από 33352 μονάδες μέτρησης πλήρης συμβατό με το chip SLE 4406. Όπως αναφέρεται ανωτέρω από τη διεύθυνση 64 έως 103. Περισσότερα στο κεφάλαιο 1.

*** High security authentication unit**

Η "Μονάδα επικύρωσης υψηλής ασφάλειας" (High security authentication Unit) **είναι αρμόδια για το πρωτόκολλο πρόκλησης/απάντησης (challenge/response) που περιγράφεται στην προηγούμενη παράγραφο. Το SLE4436 χρειάζεται ένα κλειδί 48-κομματιών (48-bit key) για να παραγάγει μια δεκαεξάμπιτη απάντηση (16-bit response).** Το "μυστικό κλειδί" (Secret Key) **και η τρέχουσα** "Αξία του μετρητή" (Counter Value) **χρησιμοποιείται επίσης σε αυτόν τον υπολογισμό. Παρακάτω θα περιγράφει πώς να στείλει μια πρόκληση στο τσιπ και να διαβάσει την απάντηση (challenge/response).**

*** Transport Code protection for delivery**

Η **"Προστασία Κώδικα Μεταφορών κατά την παράδοση" (Transport Code protection for delivery)** χρησιμοποιείται για να αποτρέψει τους ανθρώπους από το κλέψιμο τσιπ στην διαδρομή τους από το τσιπ - στην κάρτα-κατασκευαστή. Τα τσιπ θα μπορούσαν μόνο να ξεκλειδωθούν με έναν ειδικό κώδικα..

*** Chip layout of security relevant areas protected against physical / electrical signal analysis**

Με το **"σχεδιάγραμμα τσιπ των σχετικών ζωνών ασφάλειας προστατευόμενων από τη φυσική/ηλεκτρική ανάλυση σημάτων"** δεν είναι δυνατό (ή τουλάχιστον μη εύκολο) να εξεταστούν τα μέρη του τσιπ από ένα ηλεκτρονικό μικροσκόπιο ακτινών.

000:	11011000	00101010	11111111	11001010
032:	00101110	11101000	01001100	11000000
064:	00000000	00000000	00000011	00000111
096:	00001111	11111111	11111111	11111111
128:	11111111	11111111	11111111	11111111
160:	11111111	11111111	11111111	11111111
192:	11111111	11111111	11111111	11111111
224:	11111111	11111111	11111111	11111111
256:	11111111	11111111	11111111	11111111
288:	11111111	11111111	11111111	11111111
320:	10101010	00100100	11011011	11101111
352:	00010000	10011010	00101000	01111010
384:	11111111	11111111	11111111	11111111
416:	11111111	11111111	11111111	11111111
448:	11111111	11111111	11111111	11111111
480:	11111111	11111111	11111111	11111111

= Identification Area

= Counter Area

= Bit to activate Challenge/Response sequence

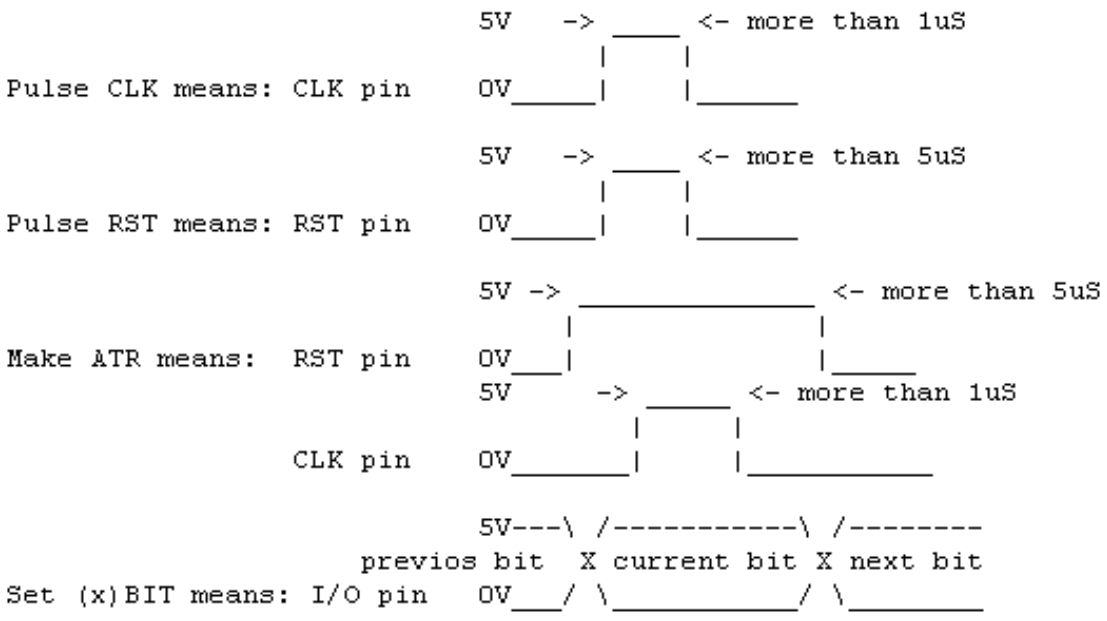
= User Data Area 1 and 2

Σχήμα 3.10.2 Μια επισκόπηση της χρήσης μνήμης σε ένα SLE4436 σε μία ελβετική τηλεκάρτα.

3.10.3 SLE5536

Το SLE5536 έχει πολλά κοινά σημεία με το SLE4436. Έχει τις ίδιες λειτουργίες και επιπλέον προσφέρει τη δυνατότητα να κρυπτογραφηθεί η επικοινωνία χρησιμοποιώντας φραγμό αλυσιδωτής επικοινωνίας (c*ypher-block-chaining*). Αυτό το τσιπ είναι επίσης γνωστό ως "Eurochip II".

Πώς να διαβάζεται η απάντηση από τα τσιπ SLE4436 και SLE 5533 Eurochip.



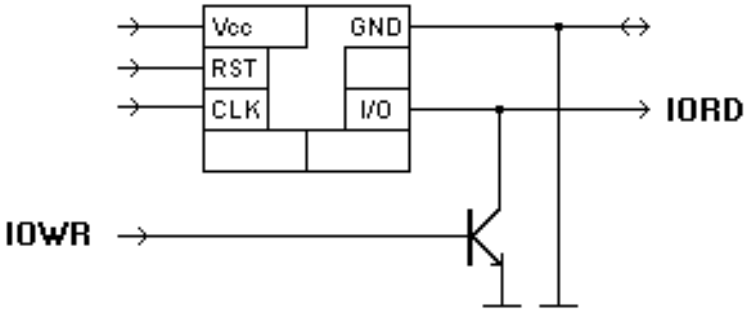
Σχήμα 4.3.1: Ακολουθία παλμών για ανάγνωση της απάντησης από τα τσιπ SLE4436 και SLE 5533.

Ο αλγόριθμος για την απάντηση:

1. κάνει τον ATR (Answer to Reset)
2. παλμός του CLK 110 φορές (έτσι ώστε στην I/O επαφή είναι 6 μπιτ (από 0 έως 7) (από την ψηφιολέξη 13 (byte 13) (από 0 έως 15))
3. παλμός RST
4. παλμός CLK
5. αναμονή 10 uS
6. σφυγμός CLK 177 φορές
7. θέτουν (first)BIT από την πρόκληση
8. παλμός CLK
9. επαναλαμβάνεται το βήμα 7 και 8 με (2^o, 3^o, …48^o) κομμάτι-bit από την πρόκληση, η οποία είναι 6 τυχαία bytes που εκδίδονται από το SAM (*Security Application Module* - ενότητα εφαρμογής ασφάλειας). Όταν στέλνεται το τελευταίο 48^o κομμάτι-bit προχωρά στο βήμα 10
10. παλμός CLK (ρολογιού) 160 φορές
11. διάβασε την I/O επαφή (αυτή τη στιγμή έχετε το πρώτο (ή κάθε επόμενο) κομμάτι-bit από την απάντηση της κάρτας στην I/O επαφή)
12. επανέλαβε τα βήματα 10 και 11 μέχρι το τελευταίο 16^o κομμάτι-bit να διαβάζεται, εάν συνεχίζετε τους παλμούς του ρολογιού, η κάρτα αποκαθίσταται..

3.10.4 Πρόκληση/απάντηση (Challenge/Response)

Στην παράγραφο αυτή περιγράφεται λεπτομερώς ο τρόπος με τον οποίο μια πρόκληση στέλνεται σε ένα SLE4436 και ο τρόπος με τον οποίο η απάντηση διαβάζεται. Για αυτό πρέπει να έχουμε μια διεπαφή που να οδηγεί τη γραμμή I/O του chip αμφίδρομα. Ακολουθεί ένα παράδειγμα τέτοιας διεπαφής:



Βλέπουμε ότι τώρα 2 γραμμές I/O είναι απαραίτητες. Μία για ανάγνωση (IORD) όπως πριν, και μία για γράψιμο (IOWR). Με αυτή τη γραμμή η επαφή IO του τσιπ μπορεί να γειωθεί στο έδαφος.
Για να ενεργοποιήσουμε το πρωτόκολλο *challenge/Response*, προχωράμε στα παρακάτω βήματα:

1. Επαναρίθμησε την κάρτα (reset card) (ακολουθία αναστοιχειοθέτησης-RESET sequence)
2. Παλμός CLK (ρολογιού), 110 φορές (έως ότου είστε στην θέση-κομμάτι 110, (bit position 110))

3. Ακολουθία –Εγγραφής (write-sequence) στο κομμάτι 110 (bit 110), (παλμός στο RST και CLK)
4. Παλμός στο CLK (ρολόι) 177 φορές
5. καθορισμένο κομμάτι (1), (set bit "1") της πρόκλησης (σε IOWR)
6. Παλμός CLK (ρολόι) μία φορά
7. Επανέλαβε βήματα 5 και 6 για τα κομμάτια 2 - 48 της πρόκλησης (bits 2 - 48 of the challenge)
8. Παλμός CLK (ρολόι) 160 φορές
9. Διαβάστε (1) το μπιτ στην απάντηση (από IORD)
10. Επανέλαβε βήματα 8 και 9 για τα κομμάτια 2 - 16 της απάντησης (bits 2 - 16 of the response).

Είναι σημαντικό ο παλμός του CLK (ρολογιού) να έχει ακριβώς τα σωστά χρονικά διαστήματα, διαφορετικά το τσιπ παρουσιάζει λανθασμένη απάντηση. Όπως μπορείτε να δείτε, το τσιπ χρειάζεται 160 παλμούς του CLK (ρολογιού) για να παράγει ένα μπιτ της απάντησης (*bit of response*). Η απάντηση εξαρτάται από τον **"τομέα προσδιορισμού" (*Identification Area*)**, την **"τρέχουσα αντίθετη αξία" (*current counter value*)** και την **"περιοχή στοιχείων χρηστών 1" (*User Data Area 1*)** αλλά ΟΧΙ από τη **"περιοχή στοιχείων χρηστών 2" (*User Data Area 2*)**. Επομένως δύο κάρτες με τις ίδιες τιμές σε αυτές τις περιοχές παράγουν την ίδια απάντηση για την ίδια πρόκληση!

3.10.5 Υποκλοπή Επικοινωνίας Τηλεκάρτας με το Καρτοτηλέφωνο

Με το κατάλληλο λογισμικό (SCALA 1.4) μπορούμε να παρέμβουμε μεταξύ του τηλεφώνου και της τηλεκάρτας και να το συνδέσουμε με έναν υπολογιστή Έτσι είναι εύκολα δυνατό να καταγραφεί η επικοινωνία μεταξύ μίας πραγματικής τηλεκάρτας και ενός τηλεφώνου.

3.10.6 Πιθανά "κενά" ασφάλειας

Με την εισαγωγή των έξυπνων καρτών και την χρησιμοποίηση του τσιπ SLE4436, πολύ δύσκολα μπορούμε να εξαπατήσουμε τις επιχειρήσεις τηλεφωνίας. Εντούτοις το σύστημα δεν είναι 100% εξασφαλισμένο. (όπως κανένα σύστημα δεν είναι). Το μόνο πρόβλημα είναι ο αλγόριθμος που χρησιμοποιείται για τον υπολογισμό της απάντησης. Εάν αυτός έσπαζε, μία τηλεκάρτα θα μπορούσε εύκολα να μιμηθεί με την βοήθεια ενός μικροελεγκτή.

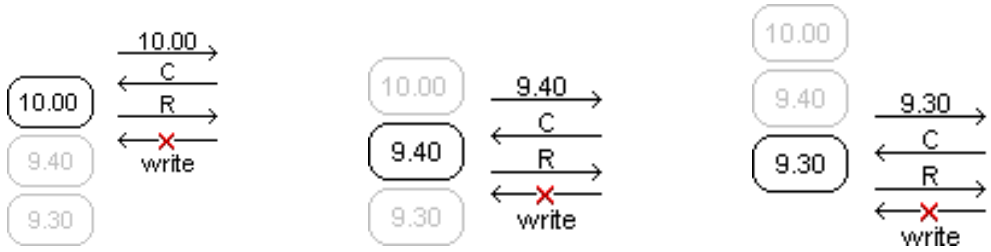
Αλλά το σύστημα έχει (ή είχε) μια αδυναμία: Για λόγους προστασίας των προσωπικών στοιχείων, μερικές φορές δεν αποθηκεύονται όλα τα ψηφία του serial number στο τσιπ. Εάν το τελευταίο ψηφίο λείπει, υπάρχουν 100 απολύτως ίδιες κάρτες. Όπως αναφέρεται τέτοιες κάρτες παράγουν την ίδια απάντηση για την ίδια πρόκληση. Σύμφωνα με αυτό το γεγονός και χρησιμοποιώντας (το ελάχιστο 2) τέτοιες ίδιες κάρτες, η πρώτη κάρτα θα αποθήκευε ολόκληρο το ποσό των μονάδων, η δεύτερη κάρτα ένα ποσό από τις μονάδες που μειώθηκαν , η τρίτη κάρτα ένα ποσό από μερικές πρόσθετες μονάδες και τα λοιπά. Η διαδικασία έχει ως εξής :

1. Η πρώτη κάρτα συνδέεται με το τηλέφωνο

2. Το τηλέφωνο διαβάζει τις διαθέσιμες μονάδες, στέλνει μια πρόκληση και ελέγχει την απάντηση
3. Ένας αριθμός σχηματίζεται
4. Το τηλέφωνο δοκιμάζει να μειώσει τις μονάδες, αλλά αυτή η εντολή φιλτράρεται και δεν περνά στην κάρτα!
5. Η δεύτερη κάρτα συνδέεται με το τηλέφωνο (τίποτα δεν έχει γραφτεί στην πρώτη κάρτα!)
6. Το τηλέφωνο διαβάζει τις διαθέσιμες μονάδες στη δοκιμή εάν ήταν επιτυχής, μια νέα πρόκληση στέλνεται και η απάντηση ελέγχετε
7. Μετά από μια στιγμή (της ομιλίας...) το τηλέφωνο δοκιμάζει να μειώσει λίγο περισσότερες μονάδες από την κάρτα. Πάλι αυτήν την εντολή φιλτράρεται και δεν περνούν στην κάρτα!
8. Η τρίτη κάρτα συνδέεται με το τηλέφωνο (τίποτα δεν έχει γραφτεί στη δεύτερη κάρτα!)

Τώρα συνεχίστε το βήμα **6** όσο θέλετε, και δεδομένου ότι πήρατε τις πρόσθετες κάρτες ...

Βήμα 1,2,3,4 Βήμα 5,6 Βήμα 7,8

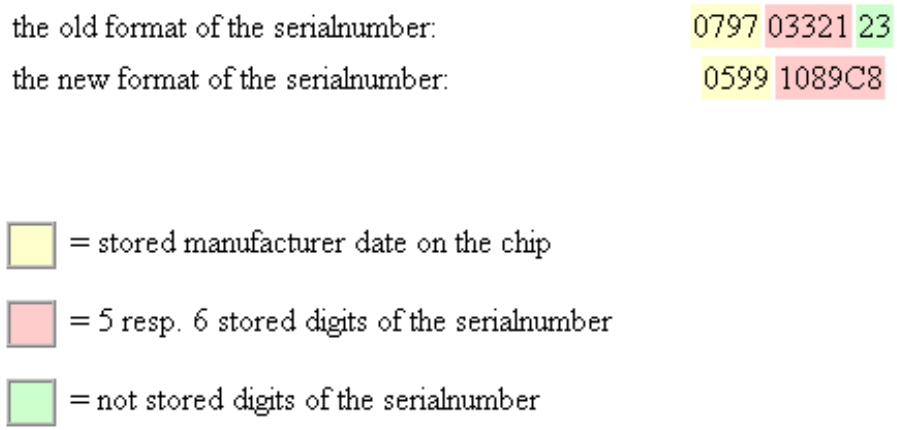


Η μόνη προϋπόθεση είναι ότι ξέρετε πόσες μονάδες θα αφαιρεθούν από την κάρτα σε κάθε βήμα. Αλλά συνήθως αυτό είναι γνωστό, παραδείγματος χάριν στην Ελβετία: -60 για την κλήση και έπειτα -10 με κάθε λεπτό.

Γιατί αυτή η θεωρία δεν λειτουργεί πάντα

Σε όλες τις νεώτερες τηλεκάρτες ο πλήρης σειριακός αριθμός αποθηκεύεται στο τσιπ. Συνεπώς δεν μπορούν να βρεθούν δύο όμοιες κάρτες. Κάθε κάρτα μπορεί τώρα να προσδιοριστεί.

Όπως μπορείτε να δείτε, το νέο *serial number* είναι ένα ψηφίο λιγότερο από το παλαιό, αλλά τώρα επίσης τα ψηφία δεκαεξαδικού (AF) επιτρέπονται. Το πρόσθετο αποθηκευμένο ψηφίο αποθηκεύεται

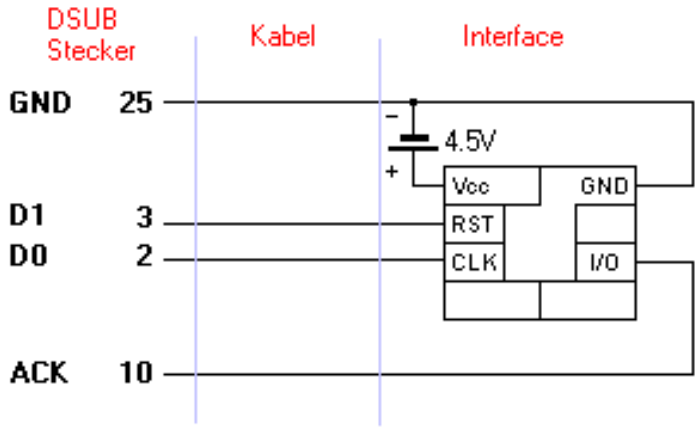


στα κομμάτια 17-20.

3.10.7 Κατασκευάζοντας ένα απλό αναγνώστη καρτών

Μπορείτε να ξοδέψετε πολλά χρήματα για τους αναγνώστες *chipcard*. Αλλά οι κάρτες ασύγχρονης επικοινωνίας όπως οι τηλεκάρτες μπορούν εύκολα να συνδεθούν με μια συσκευή αναγνώστη καρτών στην παράλληλη θύρα του υπολογιστή. Πρώτα χρειάζεστε μια συσκευή επαφής. Κατόπιν χρειάζεστε ένα καλώδιο με τουλάχιστον 4 καλώδια, και ένα κονέκτορα (D-SUB 25pin) παράλληλης θύρας 25 επαφών για να τον συνδέσετε με τον υπολογιστή σας. Για την παροχή ηλεκτρικού ρεύματος, μια μπαταρία 4.5V είναι κατάλληλη.

Το κύκλωμα θα έμοιαζε με αυτό:



Σχήμα 3.10.7 Απλός αναγνώστης καρτών

3.10.8 Γράφοντας ένα απλό λογισμικό

Με την παράλληλη θύρα μπορούμε να έχουμε εύκολα πρόσβαση σε περιβάλλον DOS. Κάτω από περιβάλλον windows NT/2000 αυτό δεν είναι άμεσα δυνατό. Έτσι τα ακόλουθα παραδείγματα βασίζονται στο σύστημα DOS ή των WINDOWS. Η γλώσσα προγραμματισμού είναι η Turbo-PASCAL, η οποία είναι ακόμα μια καλή γλώσσα για τους αρχαρίους.

Οι παράλληλες θύρες έχουν 8 γραμμές στοιχείων (*data lines*) που μπορούν να προσεγγιστούν άμεσα ως έξοδοι (*outputs*). Επιπλέον υπάρχουν 5 γραμμές εισόδου και 4 αμφίδρομες γραμμές που μπορείτε να χρησιμοποιήσετε.

Η διεύθυνση της παράλληλης θύρας είναι είτε η 378h (LPT1) είτε η 278h (LPT2). Για να γράψει τα στοιχεία (*write data*) στις 8 γραμμές παραγωγής (*output lines*), αυτό που πρέπει να κάνετε είναι να γράψετε ένα databit στη διεύθυνση της παράλληλης θύρας. Στο ακόλουθο παράδειγμα υποθέτουμε την 378h ως διεύθυνση της παράλληλης θύρας..

```
Port[$378] := $FF;   { set all lines to 1 }
```

Ο κατάλογος θέσης, και ως εκ τούτου οι γραμμές εισαγωγής προσεγγίζεται πέρα από την διεύθυνση της παράλληλης θύρας 379h αντίστοιχα 279h:

```
b := Port[$378+1];   { read inputs and store them in b }
```

Από το πρωτόκολλο που περιγράψαμε στο 1.2 και το υλικό που περιγράφεται στο 1.3, εδώ έχουμε μια μικρή βιβλιοθήκη λειτουργίας:

```
const
  LPT = $378;
  RST =
```

```
  CLK =
  IO  =
{--- set the address to 0 ---}
procedure Reset_Card;
begin
  Port[LPT] := 0;
  Port[LPT] := RST;
  delay(5);
  Port[LPT] := RST or CLK;
  delay(5);
  Port[LPT] := RST;
  delay(5);
  Port[LPT] := 0;
end;

{--- read bit at current address ---}
function Read_Bit: byte;
begin
  if (Port[LPT+1] and IO) > 0 then Read_Bit := 1
    else Read_Bit := 0;
end;

{--- increment address by 1 ---}
procedure Clock;
begin
  Port[LPT] := CLK;
  delay(10);
  Port[LPT] := 0;
end;

{--- set (write) bit at current address to 0 ---}
procedure Write_Bit;
begin
  Port[LPT] := RST;
  delay(5);
  Port[LPT] := 0;
  Clock;
end;
```

3.10.9 Κατασκευαστές chip

Υπάρχουν αρκετές εταιρίες που κατασκευάζουν τσιπ για τηλεκάρτες. Ο ΟΤΕ προμηθεύεται τις τηλεκάρτες του από τέσσερις από αυτές: *Gemplus*, *Orga*, *Solaic*, *Schlumberger*. Παρακάτω βλέπουμε τα λογότυπα των εταιριών. Η κωδικοποίηση των κατασκευαστών για την Ελλάδα, που περιλαμβάνονται στον αριθμό ελέγχου είναι: Πρώτο Ψηφίο: 0 GPT, 1 Solaic, 2 Gemplus, 3 Schlumberger, 4 Orga. Μερικές φορές, οι κατασκευαστές μπορούν να χρησιμοποιήσουν το σύστημα του αριθμού ελέγχου τους: **Gemplus**, "GEM" + διαδοχικός αριθμός και **GPT**, 0 έως 3 ψηφία (θέτετε το προσδιοριστικό) + ένας κώδικας γραμμάτων που προσδιορίζει το χειριστή + διαδοχικό αριθμό.

F.N.M.T. (Spanish Royal Mint)

Gemplus www.gemplus.com/

Gieseke & Devriendt

ODS, Oldenburg Data System

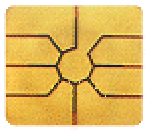
Orga www.orga.com/

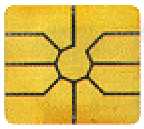
Schlumberger www.slb.com/ or www.smartcards.net/

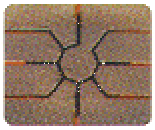
Solaic www.winforms.phil.tu-bs.de/winforms/company/solaic/solaic.html

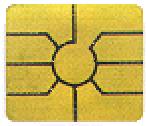
Uniqua www.uniqa.at/

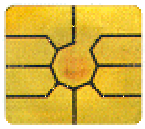
Gemplus Chip Modules

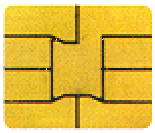

23

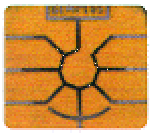

24

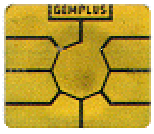

25


26


27


28

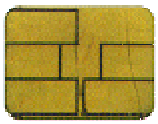

29

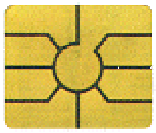

30

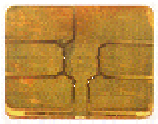
Σημείωση 1: Θα δείτε ότι το GEM1 (23) φαίνεται παρόμοιο με το SO2, αλλά η ενότητα αυξάνεται ελαφρώς στη μέση.

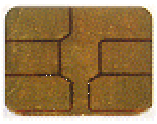
Σημείωση 2: GEM1 (23) και GEM2 (24) είναι διαφορετικά. Στο GEM1, οι κάτω-αριστερά προς πάνω δεξιά διαγώνιες αντισταθμίζονται, ενώ το GEM2 δεν είναι το ίδιο. Και οι δύο τύποι τσιπ μπορούν να βρεθούν στην ίδια σειρά καρτών. Μια περαιτέρω ταξινόμηση αυτών των καρτών είναι η γωνία των διαγωνίων, οι οποίες μπορούν να είναι 90 ή 75 μοίρες. Δείτε το παρακάτω γραφικό:

Orga / Uniqa Chip Modules


52

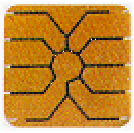

53

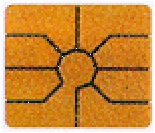

54

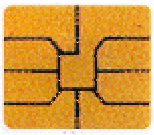

55

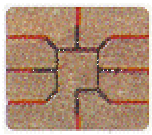
Σημείωση: Η Uniqa έχει αγοράσει την Orga.

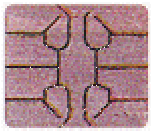
Solaic Chip Modules

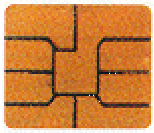

78


79


80

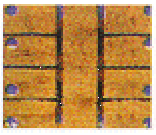

81

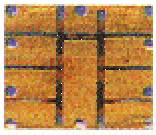

82

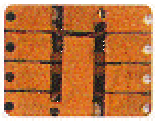

83

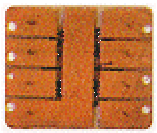

84

Schlumberger Chip Modules


59

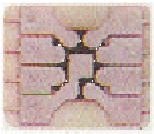

60

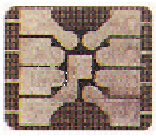

61

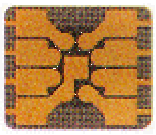

62

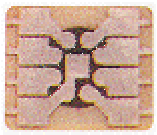

63

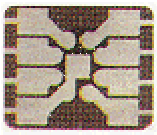

64

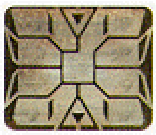

65

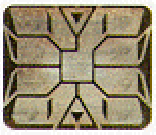

66

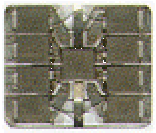

67

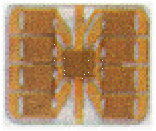

68


69


70

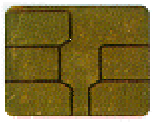

71

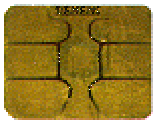

72

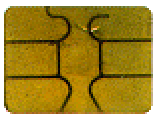

73

GEC Plessey Telecommunications (GPT) Chip Modules


37


38


39


40

Σημείωση: Οι απεικονίσεις 37 & 38 φαίνονται παρόμοιες αλλά οι κεντρικές περιοχές έχουν διαφορετικά μεγέθη. Όλες είναι της Siemens.

Επίλογος

Τι να περιμένουμε στο μέλλον από τις έξυπνες κάρτες; Η απάντηση ήδη υπάρχει, είναι η εμφάνιση των έξυπνων καρτών που προγραμματίζονται.

Ίσως το πιό επαναστατικό γεγονός στην ιστορία των έξυπνων καρτών τα τελευταία 25 χρόνια είναι η πρόσφατη εμφάνιση των προγραμματίσιμων έξυπνων καρτών.

Το περιεχόμενο της μνήμης έχει προγραμματιστεί από τον κατασκευαστή και είναι μόνο για ανάγνωση, οι προγραμματίσιμες έξυπνες κάρτες αφήνουν πρόσθετα, τον εκτελέσιμο κώδικα στην έξυπνη κάρτα, την διάρκεια ζωής της κάρτας. Η αρχική προοριζόμενη χρήση των προγραμματίσιμων έξυπνων καρτών είναι να δημιουργηθούν πολύ οι έξυπνες κάρτες εφαρμογής στις οποίες οι εφαρμογές μπορούν να προστεθούν και να διαγραφούν.

Υπάρχουν διάφορες προγραμματίσιμες έξυπνες κάρτες στην αγορά. Μερικές μπορούν να είναι προγραμματισμένες στις υψηλού επιπέδου γλώσσες, μερικές μπορούν να προγραμματιστούν σε εικονική ή Συμβολική γλώσσα (*Assembly*) (γλώσσα του τσιπ).

Η *Basic* κάρτα από Zeitcontrol (www.zeitcontrol.com) μπορεί να προγραμματιστεί σε γλώσσα προγραμματισμού Basic. Η Zeitcontrol έχει κάνει μια άριστη εργασία πάνω στην ενσωμάτωση ανάπτυξης του προγράμματος για την έξυπνη κάρτα με την ανάπτυξη προγράμματος για τον οικοδεσπότη ή το τερματικό που θα χρησιμοποιούν.

Η έξυπνη κάρτα MULTOS (www.multos.com) είναι μια έξυπνη κάρτα που καθορίζεται κοντά MAOSCO, ένα υποπροϊόν MONDEX και της MasterCard. Η κάρτα MULTOS μπορεί να είναι προγραμματισμένh σε γλώσσα C αλλα και σε MEL (εκτελέσιμη γλώσσα MAOS), το οποίο είναι Συμβολική γλώσσα (*Assembly*) για την εικονική μηχανή στην κάρτα.

Η εταιρία Keycorp (www.keycorp.com.au) εμπορεύεται μια έξυπνη κάρτα αποκαλούμενη OSSCA (Λειτουργικό σύστημα για τις εφαρμογές έξυπνων καρτών-Operating System for Smart Card Application) που μπορείτε να προγραμματίσετε σε Forth γλώσσα.

Διάφοροι κατασκευαστές καρτών έχουν αναγγείλει τις κάρτες που μπορούν να είναι προγραμματισμένες σε Java αλλά μόνο η Schlumberger (www.cyberflex.austin.et.slb.com) διαθέτει τέτοιες κάρτες στην αγορά. Η Gemplus (www.gemplus.com) έχει διαθέσιμες τριανταδυάμπιτες πειραματικές κάρτες που τρέχουν την Java.

Η Syprus (www.spyrus.com) και η Datakey (www.datakey.com) προσπαθούν να κατασκευάσουν κάρτες που θα επιτρέπουν την πρόσθεση προγραμμάτων που γράφονται σε assembly. Το λειτουργικό σύστημα στην κάρτα Spyrus ονομάζεται SPYCOS και η λειτουργία του συστήματος στη βασική κάρτα στοιχείων ονομάζεται DKCCOS.

Το λειτουργικό σύστημα HOST από την Oberthur (www.oberthurkirk.com) είναι επίσης γνωστό ότι υποστηρίζει την φόρτωση των εγγενών εφαρμογών κώδικα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] W. Rankl and W. Effing, "***Smart Card Handbook"***, John Wiley & Sons; 2nd edition, 2000.

[2] Timothy M. Jurgensen, Scott B. Guthery, Bertrand du Castel, Scott Guthery, and Tim Jurgensen, "***Smart Cards: The Developer's Toolkit",*** Prentice Hall PTR, 2002.

[3] Mike Hendry, "***Smart Card Security and Applications",*** Artech House, 2nd edition, 2001.

[4] Yahya Haghiri and Thomas Tarantino, "***Smart Card Manufacturing: A Practical Guide",*** John Wiley & Sons, 2002.

Links στο Internet

http://www.iso.org

http://www.infineon.com

http://www.maxking.co.uk

http://www.smartcardbasics.com/

http://www.cix.co.uk/~dlc/chipsf.html

http://www.compinfo-center.com/tpsmrt-t.htm

http://gsho.thur.de/phonecard/index_main_e.htm

http://www.gae.ucm.es/~padilla/extrawork/smart.html

http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx

http://www.jacquinot.com/smartcards/smartcard_standard_ISO7816.htm