



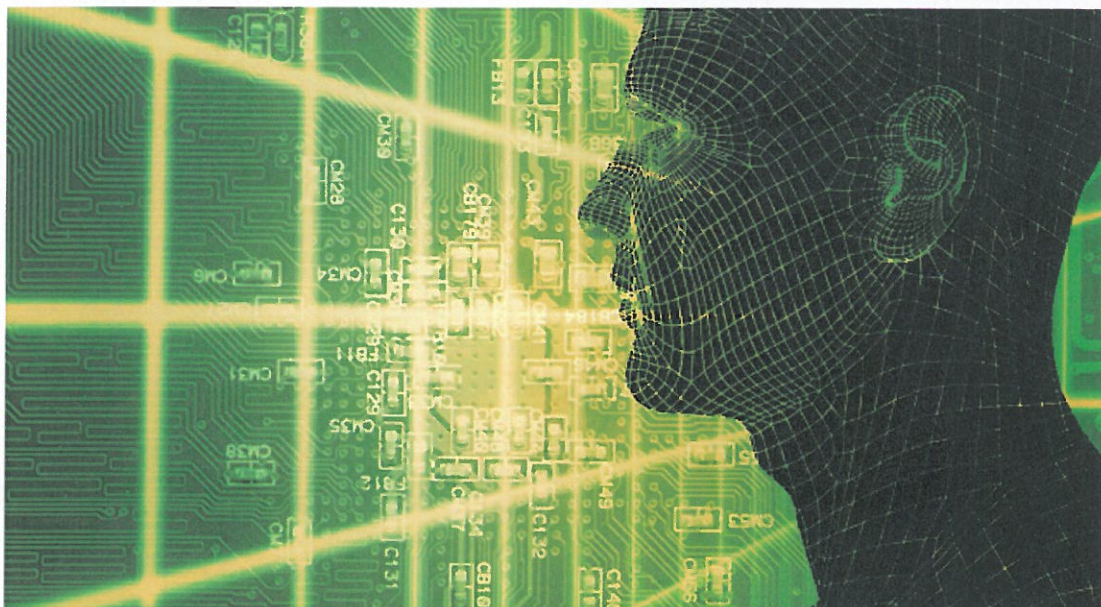
**ΤΕΧΝΟΛΟΓΙΚΟ  
ΕΚΠΑΙΔΕΥΤΙΚΟ  
ΙΔΡΥΜΑ  
ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ**

**ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΑΛΛΑΔΑΣ**

**ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ**

**ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΤΕ.**

**ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ**



**ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ  
ΠΡΟΤΥΠΩΝ ΩΣ ΕΡΓΑΛΕΙΟ ΔΙΑΧΕΙΡΙΣΗΣ  
ΑΝΘΡΩΠΙΝΩΝ ΠΟΡΩΝ**

**ΑΡ.ΠΤΥΧΙΑΚΗΣ : 1633**

**ΜΕΤΣΙΝΗ ΓΑΡΥΦΑΛΙΑ (Α.Μ. 6476)**

**ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΚΑΡΕΛΗΣ ΔΗΜΗΤΡΙΟΣ**

**ΠΑΤΡΑ 2017**

“ ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΤΥΠΩΝ  
ΩΣ ΕΡΓΑΛΕΙΟ ΔΙΑΧΕΙΡΙΣΗΣ ΑΝΘΡΩΠΙΝΩΝ ΠΟΡΩΝ ”

ΜΕΤΣΙΝΗ ΓΑΡΥΦΑΛΙΑ (Α.Μ. 6476)

© 2017 – All rights reserved



## **ΠΡΟΛΟΓΟΣ / ΠΕΡΙΛΗΨΗ**

Σκοπός της Πτυχιακής Εργασίας είναι η πρόταση ενός Συστήματος Βιομετρικής Αναγνώρισης Προτύπων που προσφέρει λύσεις σε επιχειρήσεις, όσον αφορά κάποια σοβαρά ζητήματα διαχείρισης ανθρώπινου δυναμικού, όπως είναι:

- Έγκαιρη προσέλευση στον χώρο εργασίας
- Τήρηση ωραρίων
- Κίνηση σε ζώνες περιορισμένης πρόσβασης
- Προγραμματισμός βαρδιών και αδειών
- Υπέρβαση του χρόνου διαλειμμάτων
- Ασφάλεια στο χώρο εργασίας

Η λύση που προτείνεται αφορά την μελέτη και τοποθέτηση ενός συστήματος, το οποίο διαχειρίζεται μέσω ενός λογισμικού προγράμματος πληροφορίες που προέρχονται από μια βάση δεδομένων σχετικά με την ταυτότητα και το ιστορικό των χρηστών του. Το σύστημα, μεταξύ άλλων, δίνει στο διαχειριστή την δυνατότητα να προσθέσει ή να αφαιρέσει μεγάλο αριθμό χρηστών, να εκχωρήσει ή να ανακαλέσει δικαιώματα και να ορίσει ζώνες προσβασιμότητας και χρόνους κίνησης των χρηστών.

Επιπλέον αναγνωρίζει δακτυλικά αποτυπώματα, κωδικούς πρόσβασης και μαγνητικές κάρτες προκειμένου για την πρόσβαση και κίνηση στον εργασιακό χώρο.

Η βασική μεθοδολογία που εφαρμόστηκε στην Πτυχιακή αυτή συνοψίζεται στα παρακάτω βήματα.

Αρχικά ορίζονται και κατηγοριοποιούνται τα Βιομετρικά Συστήματα Αναγνώρισης Προτύπων. Έπειτα αναλύονται, με την βοήθεια ερευνών, βασικά προβλήματα που αντιμετωπίζουν οι επιχειρήσεις στην Διαχείριση Ανθρώπινων Πόρων. Δίνεται η προτεινόμενη λύση και αναλύεται ο τρόπος εφαρμογής. Δηλαδή, οι λεπτομέρειες εγκατάστασης, τα απαραίτητα περιφερειακά συστήματα, τα συμπληρωματικά προϊόντα και οι οδηγίες χρήσης αυτών. Για την ολοκλήρωση της πρότασης παρουσιάζεται και ο προϋπολογισμός που στηρίζεται σε οικονομικές προσφορές. Μέρος της πρότασης αφορά και το εγχειρίδιο χρήσης του συστήματος, όπως επίσης και την πρόβλεψη πιθανών αδυναμιών-απειλών και αντιμετώπισης αυτών.

Τέλος, παρουσιάζονται τα συνολικά οφέλη προς την επιχείρηση αλλά και προβληματισμοί-ηθικά ζητήματα.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ / ΠΕΡΙΛΗΨΗ .....	I
ΠΕΡΙΕΧΟΜΕΝΑ .....	II
ΕΙΣΑΓΩΓΗ .....	1
ΑΝΑΛΥΣΗ ΘΕΜΑΤΟΣ .....	2
Βιομετρική Ταυτοποίηση (Βιομετρία).....	2
Βιομετρικά Χαρακτηριστικά .....	2
Βιομετρικά Συστήματα.....	4
Χαρακτηριστικά Βιομετρικών Συστημάτων.....	8
Τρόπος Λειτουργίας Βιομετρικών Συστημάτων .....	10
Ιστορική Αναδρομή.....	11
Συστήματα Βιομετρικής Αναγνώρισης .....	14
Φυσικά Χαρακτηριστικά.....	14
Αναγνώριση δακτυλικών αποτυπωμάτων (fingerprint verification).....	14
Βασικές τεχνολογίες των ανιχνευτών αποτυπώματος (fingerprint scanners) .....	16
Βελτίωση Ποιότητας Εικόνας Δακτυλικού Αποτυπώματος .....	17
Αναγνώριση προσώπου (face recognition) .....	19
Ανάλυση ίριδας ματιού (iris recognition) .....	23
Αναγνώριση φωνής (voice recognition) .....	25
Ανάλυση αμφιβληστροειδή (retina analysis).....	26
Ανάλυση γεωμετρίας χεριού (hand geometry analysis).....	27
Ανάλυση DNA (DNA Analysis).....	28
Χαρακτηριστικά Συμπεριφοράς .....	29
Αναγνώριση της υπογραφής (hand-written signature verification) .....	29
Ανάλυση βηματισμού (gait analysis).....	30
Ανάλυση Πληκτρολόγησης (Keystroke analysis).....	32
Εφαρμογή Βιομετρικών Συστημάτων Αναγνώρισης Προτύπων .....	32
Σκανάρισμα – Αναγνώριση Δαχτυλικών Αποτυπωμάτων .....	34
Λίστα Εταιρειών και Ιστοσελίδων, οι οποίες έχουν αναπτύξει την ταυτοποίηση δαχτυλικών αποτυπωμάτων.....	37
Σκανάρισμα – Αναγνώριση Προσώπου.....	37
Σκανάρισμα – Αναγνώριση Τριδας.....	39
Σκανάρισμα – Αναγνώριση Χεριού.....	40
Το πρόγραμμα AFIS (Σύστημα Αναγνώρισης Δαχτυλικών Αποτυπωμάτων χεριού) .....	41
Σκανάρισμα - Αναγνώριση Φωνής.....	42
Ηλεκτρονική υπογραφή.....	43
Διοίκηση Ανθρώπινων Πόρων (ΔΑΠ) .....	44
Εισαγωγή .....	44
Ορισμός.....	44
Διοίκηση Απόδοσης.....	45



Βιομετρικά Συστήματα Αναγνώρισης Προτύπων  
ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

---

<i>Πληροφορικά Συστήματα στη Διοίκηση Ανθρώπινων Πόρων (ΔΑΠ).....</i>	<i>46</i>
<i>Ανάλυση Συστήματος Διοίκησης Ανθρώπινων Πόρων από την πλευρά της Διεύθυνσης &amp; Οργάνωσης Ανθρώπινων Πόρων.....</i>	<i>48</i>
<i>Ανάλυση Συστήματος Διοίκησης Ανθρώπινων Πόρων με την χρήση Βιομετρικού Συστήματος</i>	<i>50</i>
Βασική συνδεσμολογία του Συστήματος.....	54
Υλικά Εγκατάστασης & Απαραίτητες Προδιαγραφές.....	55
<i>Απεικόνιση της εγκατάστασης των μηχανημάτων και χρησιμότητα του καθενός στη συγκεκριμένη θέση. ....</i>	<i>62</i>
Εγγραφή στην πλατφόρμα Διαχείρισης του Λογισμικού. ....	65
Προγραμματισμός Βιομετρικού Συστήματος Αναγνώρισης Δαχτυλικών Αποτυπωμάτων .....	76
Προβλήματα Λειτουργίας και τρόποι Αντιμετώπισης του Συστήματος .....	79
Εκπαίδευση Προσωπικού .....	81
Πλεονεκτήματα & Μειονεκτήματα χρήσης του Βιομετρικού Συστήματος Αναγνώρισης Δαχτυλικών Αποτυπωμάτων .....	82
<i>Πλεονεκτήματα.....</i>	<i>83</i>
<i>Μειονεκτήματα.....</i>	<i>84</i>
Ηθικά Ζητήματα που προκύπτουν με την χρήση των Βιομετρικών Συστημάτων .....	85
<i>Ο ρόλος της Αρχής Προστασίας Δεδομένων.....</i>	<i>86</i>
<b>ΕΠΙΛΟΓΟΣ / ΣΥΜΠΕΡΑΣΜΑ .....</b>	<b>89</b>
<b>ΒΙΒΛΙΟΓΡΑΦΙΑ.....</b>	<b>90</b>
<b>ΠΑΡΑΡΤΗΜΑ.....</b>	<b>93</b>





## **ΕΙΣΑΓΩΓΗ**

Ένα Βιομετρικό Σύστημα είναι στην ουσία ένα Σύστημα Αναγνώρισης Προτύπων που εξακριβώνει την ταυτότητα του ατόμου καθορίζοντας την αυθεντικότητα ενός συγκεκριμένου βιολογικού χαρακτηριστικού.

Πρόκειται για μια εξελισσόμενη μέθοδο που τα τελευταία χρόνια διαδραματίζει πολύ σημαντικό ρόλο στην κοινωνία μας και στην καθημερινότητά των ανθρώπων.

Ο Αλφόνσο Μπέρτιλον, περισσότερο από έναν αιώνα πριν, ήταν ο πρώτος που είχε προτείνει την χρήση των Βιομετρικών Χαρακτηριστικών για την εξιχνίαση εγκλημάτων. Σήμερα, η χρήση τους δεν είναι μόνο για τους σκοπούς της Αστυνομίας και γενικά του εγκληματολογικού χώρου. Τα Βιομετρικά Συστήματα Αναγνώρισης έχουν μπει στην καθημερινότητα των ανθρώπων, των επιχειρήσεών τους αλλά και γενικά των οργανισμών. Για το λόγο αυτό έχουν προσαρμοστεί και προγραμματιστεί ανάλογα με τις ανάγκες και το περιβάλλον στο οποίο θα χρησιμοποιηθούν. Παραδείγματος χάρη, μία επιχείρηση που χρησιμοποιεί ένα Βιομετρικό Σύστημα Αναγνώρισης Δαχτυλικών Αποτυπωμάτων δεν επιτρέπεται να έχει την δυνατότητα περαιτέρω επεξεργασίας των αποτυπωμάτων του προσωπικού της, τα οποία έχει συγκεντρώσει, αλλά μπορεί να τα χρησιμοποιεί για την ταυτοποίηση αυτών και τον έλεγχο τους στον χώρο τον οποίο εργάζονται. Επίσης ο εξοπλισμός και η δυνατότητές του είναι διαφορετικά από αυτά τα οποία μπορεί να χρησιμοποιεί η Αστυνομία για τις εγκληματολογικές της μελέτες και έρευνες.

Τα Βιομετρικά Συστήματα όμως είχαν να αντιμετωπίσουν και κάποιες παραμέτρους, οι οποίες οδήγησαν όλον αυτό τον κλάδο στη στασιμότητα. Οι παράμετροι αυτοί ήταν το αυξημένο κόστος, ο υψηλός βαθμός τεχνογνωσίας που έκανε δύσκολη την εγκατάσταση αλλά και τη χρήση τους, η έλλειψη εμπιστοσύνης για τις πραγματικές δυνατότητες, η αδυναμία των εταιρειών να περάσουν τα σωστά μηνύματα για την προώθησή τους αλλά και να βγάλουν στην αγορά μεγάλο πλήθος προϊόντων, Σημαντικό ρόλο φυσικά έπαιξαν και τα νομικά ζητήματα που τέθηκαν από φορείς που έχουν την ευθύνη προστασίας των ευαίσθητων προσωπικών δεδομένων.

Αν και η χρήση τους πλέον τείνει να αυξάνεται, κανείς δεν μπορεί να ισχυριστεί ότι αποτελεί μια εναλλακτική πρόταση στα συστήματα ελέγχου πρόσβασης που χρησιμοποιούνται για καθημερινές απλές εφαρμογές, τόσο λόγω κόστους όσο και λόγω διάφορων δυσχερειών στη γρήγορη και απρόσκοπτη πρόσβαση του κοινού. Σε σχέση με χώρους όπου απαιτείται μεγάλος βαθμός διαβάθμισης, είναι δύσκολο οποιαδήποτε άλλη μέθοδος να ανταγωνιστεί την ασφάλεια που παρέχουν τα Βιομετρικά Συστήματα.

Αυτό είναι το μεγάλο τους συγκριτικό πλεονέκτημα σήμερα και πάνω σε αυτό θα βασιστούν για την περαιτέρω εξάπλωσή τους και εξέλιξή τους. Όταν δε η εμπορική τους αποδοχή γίνει μεγαλύτερη - με αποτέλεσμα να μειωθεί το κόστος παραγωγής τους και να αυξηθεί παράλληλα η ευχρηστία τους - τότε θα μπορούμε να μιλάμε βάσιμα και για διεύρυνση της χρήσης τους σε πιο απλές και καθημερινές εφαρμογές.

## ΑΝΑΛΥΣΗ ΘΕΜΑΤΟΣ

### Βιομετρική Ταυτοποίηση (Βιομετρία)

Η Βιομετρική Ταυτοποίηση (Βιομετρία) είναι η επιστήμη, η οποία ερευνά τα Βιομετρικά Χαρακτηριστικά και τα βιολογικά στοιχεία (δακτυλικά αποτυπώματα, χαρακτηριστικά του προσώπου, ίριδα του ματιού, ομιλία) των έμβιων όντων και κατά κύριο λόγο του ανθρώπου και μέσω δικών της στατιστικών και μαθηματικών μεθόδων τα αναλύει.

Σκοπός της Βιομετρικής Ταυτοποίησης είναι τα υψηλά επίπεδα ασφάλειας, η διευκόλυνση των ατόμων και η αναίμακτη διαχείριση της ασφάλειας.

Για τους παραπάνω λόγους η Βιομετρική Ταυτοποίηση παρουσιάζει μια εξελικτική πορεία και μέσα από συνεχιζόμενες έρευνες ανακαλύπτει νέες μεθόδους και τεχνικές για την αξιοποίηση των Βιομετρικών Χαρακτηριστικών και της αντιμετώπισης αλλά και αποφυγής προβλημάτων στον τομέα της ασφάλειας.

### Βιομετρικά Χαρακτηριστικά

Τα Βιομετρικά Χαρακτηριστικά ευρέως είναι :

- Η ίριδα του ματιού
- Το πρόσωπο
- Η γεωμετρία του χεριού και των δακτύλων (δακτυλικά αποτυπώματα)
- Η φωνή
- Η υπογραφή και ο γραφικός χαρακτήρας

Ένα χαρακτηριστικό μπορεί να χαρακτηριστεί ως βιομετρικό εφόσον πληρεί τις ακόλουθες παραμέτρους:

- **Καθολικότητα:** κάθε άτομο να διαθέτει το εν λόγω βιομετρικό χαρακτηριστικό.
- **Διακριτικότητα:** το βιομετρικό χαρακτηριστικό είναι διακριτό στο άτομο.
- **Μοναδικότητα:** για οποιαδήποτε δύο άτομα το βιομετρικό αυτό χαρακτηριστικό να είναι διαφορετικό.
- **Μονιμότητα:** το βιομετρικό χαρακτηριστικό να μη μεταβάλλεται με το πέρασμα του χρόνου.
- **Μετρησιμότητα:** το βιομετρικό χαρακτηριστικό να μπορεί να μετρηθεί με κάποια μέθοδο.



**Βιομετρικά Συστήματα Αναγνώρισης Προτύπων  
ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων**

Μια αρχική βαθμολόγηση των παραπάνω Βιομετρικών Χαρακτηριστικών παρουσιάζεται στον πίνακα που ακολουθεί. [01]

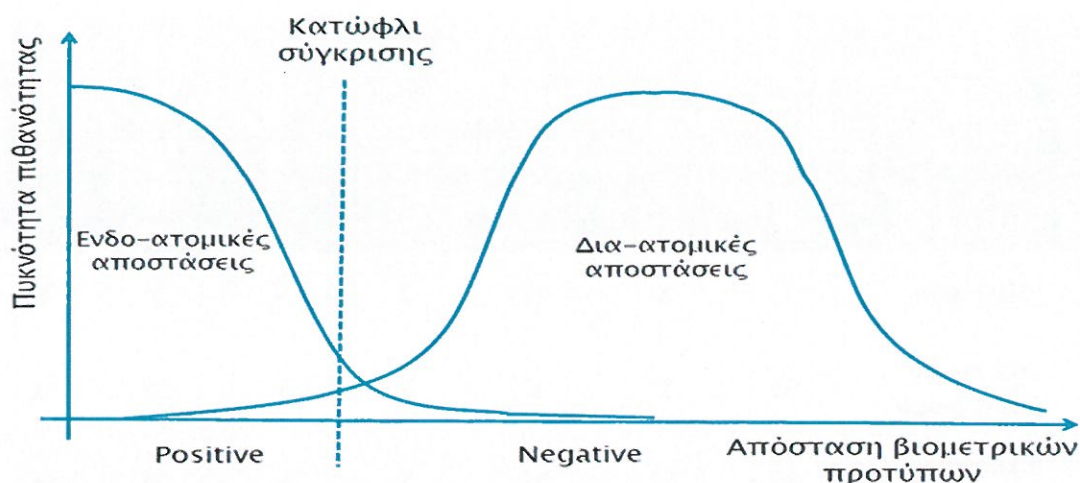
Βιομετρικό	Καθολικότητα	Διακριτικότητα	Μονιμότητα	Συλλεξιμότητα	Απόδοση	Αποδεκτικότητα	Εξασφάλιση
Πρόσωπο	Y	X	M	Y	X	Y	Y
Δακτυλικό αποτύπωμα	M	Y	Y	M	Y	M	M
Γεωμετρία χεριού	M	M	M	Y	M	M	M
Ίριδα	Y	Y	Y	M	Y	X	X
Υπογραφή	X	X	X	Y	X	Y	Y
Φωνή	M	X	X	M	X	Y	Y

**Σύγκριση των πιο συχνά χρησιμοποιούμενων Βιομετρικών Χαρακτηριστικών. Η βαθμολογία έχει τα εξής επίπεδα: X (χαμηλό), M (μεσαίο) και Y (υψηλό).**

Μελετώντας τον Πίνακα παρατηρούμε ότι το δακτυλικό αποτύπωμα ικανοποιεί σε μεγάλο βαθμό όλα τα κριτήρια βαθμολόγησης, ενώ υπερτερεί σε σχέση με τα υπόλοιπα Βιομετρικά Χαρακτηριστικά εφόσον αυτά παρουσιάζουν χαμηλή βαθμολογία σε κάποια κριτήρια. Για το λόγο αυτό, το δακτυλικό αποτύπωμα αποτελεί βασικό χαρακτηριστικό για το διαχωρισμό και την ταυτοποίηση ατόμων.

Τα Βιομετρικά Χαρακτηριστικά – Πρότυπα των ανθρώπων είναι διαφορετικά μεταξύ τους. Έχουν δηλαδή **Δια-ατομική μεταβλητότητα**. Υπάρχουν όμως και περιπτώσεις, στις οποίες τα πρότυπα του ίδιου ατόμου να παρουσιάζουν διαφορές. Τότε έχουμε **Ενδο-ατομική μεταβλητότητα**. Αυτό συμβαίνει για δύο λόγους. Είτε οφείλονται εγγενείς αιτίες, όπως για παράδειγμα η αλλαγή μεγέθους, γήρανση, αύξηση βάρους, τραύματα, υπογραφή μετά από μέθη, βάδισμα κατά την εγκυμοσύνη, παθήσεις αμφιβληστροειδή, κ.α., είτε οφείλονται εξωγενείς αιτίες, όπως για παράδειγμα προβλήματα αισθητήρων & εξοπλισμού, εξωτερικές συνθήκες, κ.α.

Παρακάτω φαίνεται η ταξινόμηση της μεταβλητικότητας των Βιομετρικών Προτύπων.



### **Βιομετρικά Συστήματα**

Τα Βιομετρικά Συστήματα περιλαμβάνουν τέσσερις βασικές υπομονάδες:

✓ **Αισθητήρας:**

Καταγραφή του βιομετρικού (κάμερα, μικρόφωνο, scanner κ.τ.λ.). Παράγει τα πρωτογενή δεδομένα (raw data).

✓ **Εξαγωγή βιομετρικού προτύπου:**

Ποσοτικοποίηση βιομετρικού. Συνήθως δημιουργία ενός διανύσματος μετρήσεων.

✓ **Συγκριτής:**

Συγκρίνει τα βιομετρικά πρότυπα, εγκαθιδρύει ένα είδος ομοιότητας ή απόστασης μεταξύ τους και αποφασίζει για την ταξινόμηση.

✓ **Βάση δεδομένων:**

Χώρος αποθήκευσης γνωστών βιομετρικών προτύπων. Κεντρική ή αποκεντρωμένη (π.χ. σε μαγνητική ταινία που κατέχει ο χρήστης).

Τα Βιομετρικά Συστήματα μπορούν να χωριστούν σε Συστήματα Ταυτοποίησης και Αναγνώρισης.

• Ένα Σύστημα Ταυτοποίησης αποτελείται από μία βάση δεδομένων Βιομετρικών Χαρακτηριστικών και πιστοποιεί την ταυτότητα ενός προσώπου λαμβάνοντας ένα Βιομετρικό του χαρακτηριστικό και συγκρίνοντας το με το ήδη αποθηκευμένο. Το σύστημα αυτό είτε δέχεται είτε απορρίπτει το αίτημα του προσώπου για ταυτοποίηση. Επιπλέον, έχουν αναπτυχθεί συστήματα επικύρωσης που χρησιμοποιούν περισσότερα από ένα βιομετρικά χαρακτηριστικά για την ταυτοποίηση των ατόμων, έτσι ώστε να μεγιστοποιηθεί η ασφάλειά τους.



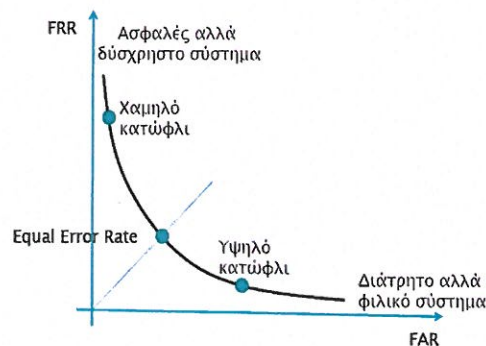
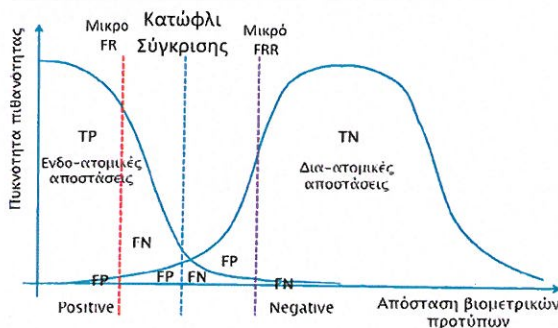
	Αποδοχή	Άρνηση
Νόμιμη προσπάθεια (βιομετρικά ίδιου ατόμου)	True Positive (TP)	False Negative (FN)
Παράνομη προσπάθεια (βιομετρικά διαφορετικών ατόμων)	False Positive (FP)	True Negative (TN)

**False Accept Rate:** Ποσοστό των παράνομων προσπαθειών που γίνονται αποδεκτές.

$$FAR = \frac{FP}{FP + TN}$$

**False Reject Rate:** Ποσοστό των νόμιμων προσπαθειών που απορρίπτονται.

$$FRR = \frac{FN}{TP + FN}$$



- Σε ένα Σύστημα Αναγνώρισης λαμβάνονται ένα ή περισσότερα Βιομετρικά Χαρακτηριστικά ενός ατόμου έτσι ώστε να συγκριθούν με τα ήδη αποθηκευμένα σε μία βάση δεδομένων. Η σύγκριση γίνεται με όλα στοιχεία της συγκεκριμένης βάσης έως ότου βρεθεί (εφόσον υπάρχει) το ήδη αποθηκευμένο Βιομετρικό Χαρακτηριστικό του ατόμου.

Συνεπώς, η διαφορά ανάμεσα στα δύο συστήματα είναι ότι ένα Σύστημα Ταυτοποίησης χρησιμοποιείται για να επιβεβαιώσει την ταυτότητα κάποιου ατόμου, ενώ ένα Σύστημα Αναγνώρισης για την εύρεση της ταυτότητάς του.

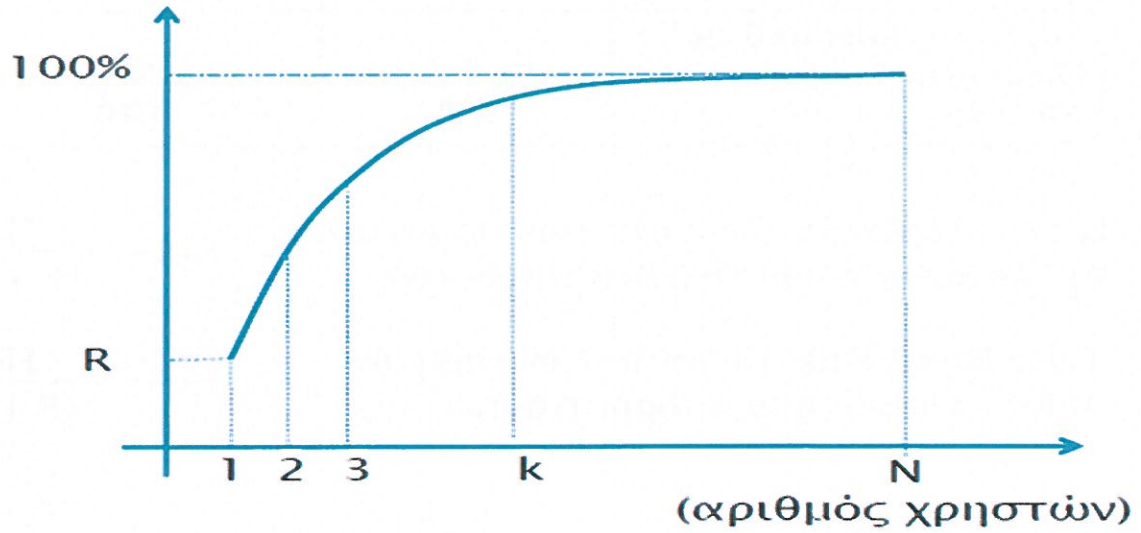
Κάθε τρόπος ή κάθε Σύστημα Αναγνώρισης που επιλέγεται να χρησιμοποιηθεί θα πρέπει να ελέγχεται για το ποσοστό επιτυχίας των αποτελεσμάτων αναγνώρισης που έχει.

Το ποσοστό της ορθής αναγνώρισης (R) μπορεί να επηρεαστεί από τις ελλείψεις πληροφορίες.

Όταν θέλουμε να έχουμε προσέγγιση μίας λίστας χρηστών (watch-list), θέλουμε η ορθή ταυτότητα του χρήστη να βρίσκεται μέσα στις k καλύτερες (top-k) θέσεις που το

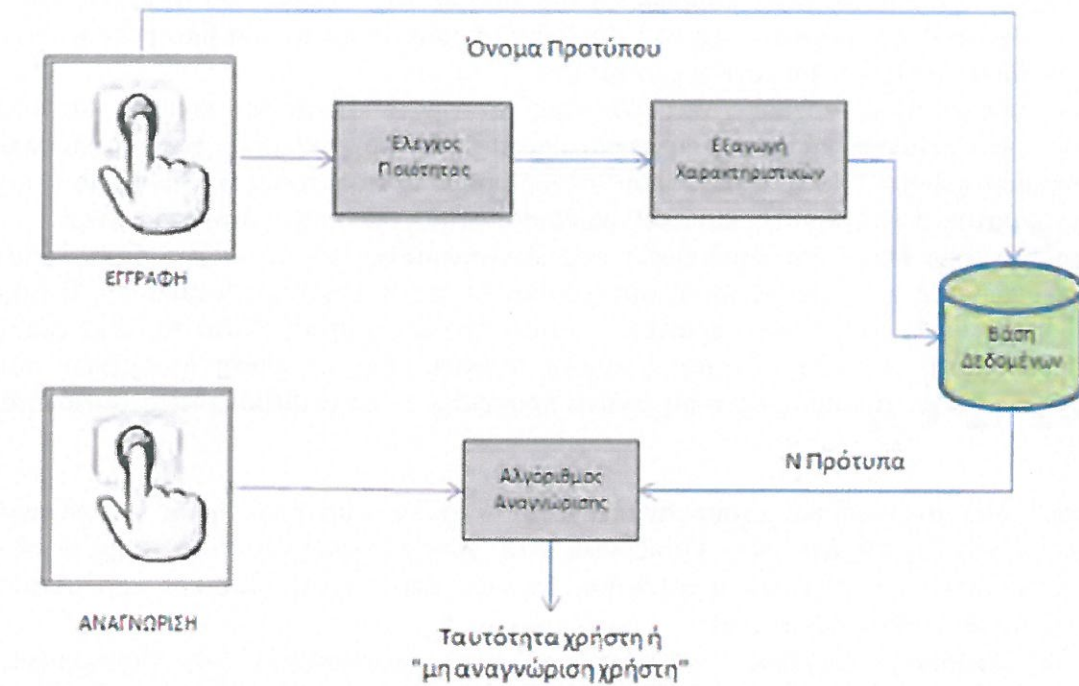
σύστημα επιστρέφει. Το  $k$  πρέπει να επιλέγεται αυθαίρετα από το 1 έως και τον αριθμό των χρηστών και για  $k=1$  το σύστημα να ταυτίζεται με το ποσοστό της ορθής αναγνώρισης ( $R$ ).

Παρακάτω φαίνεται το διάγραμμα ποσοστού ορθής ένταξης της σωστής ταυτότητας στις  $k$ -καλύτερες θέσεις, για κάθε  $k$ .

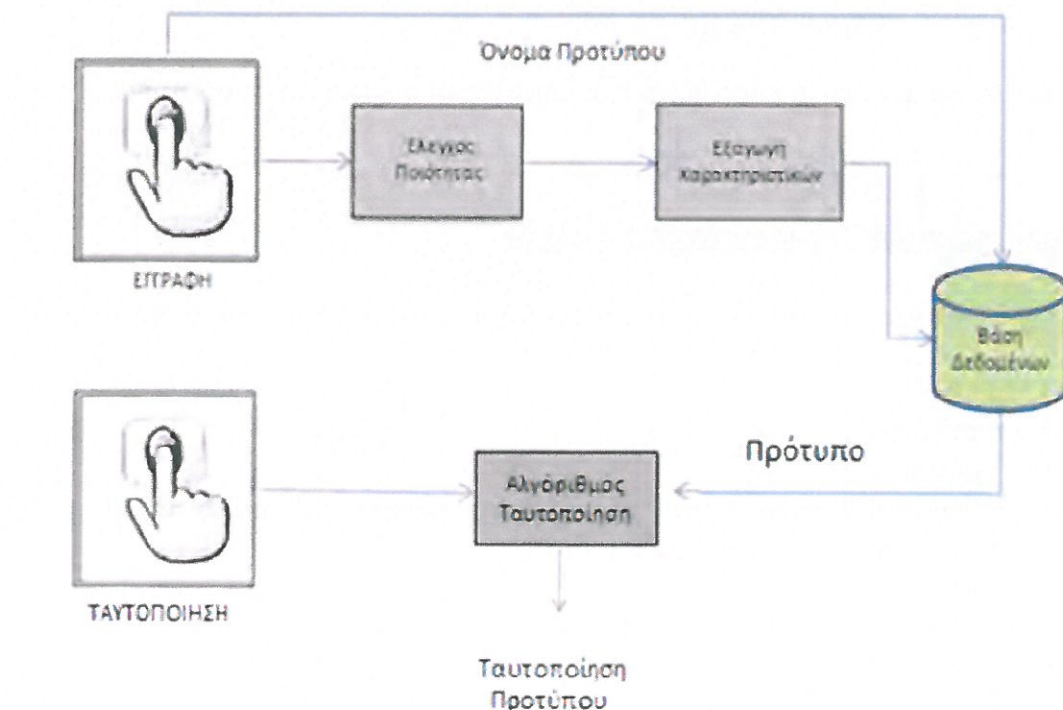


## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

Στα παρακάτω σχήματα παρουσιάζεται ένα τυπικό διάγραμμα για τη διαδικασία (α) Αναγνώρισης και (β) Ταυτοποίησης Δακτυλικών Αποτυπωμάτων.



(α) Διαδικασία εγγραφής & αναγνώρισης δακτυλικού αποτυπώματος



(β) Διαδικασία εγγραφής & ταυτοποίησης δακτυλικού αποτυπώματος



Από το παραπάνω σχήμα είναι φανερό ότι τόσο κατά τη Διαδικασία Αναγνώρισης όσο και κατά τη Διαδικασία Ταυτοποίησης, είναι απαραίτητο να έχει προηγηθεί η διαδικασία εγγραφής της εικόνας-προτύπου του δακτυλικού αποτυπώματος.

Κατά τη διαδικασία αυτή, λαμβάνεται ένα δείγμα της εικόνας του αποτυπώματος (συνήθως από ένα σαρωτή) και στη συνέχεια αποθηκεύεται σε μία βάση δεδομένων σε συνδυασμό με την ταυτότητα του χρήστη.

Πιο συγκεκριμένα, αρχικά γίνεται έλεγχος για την ποιότητα της εικόνας και στη συνέχεια εξάγονται κάποια χαρακτηριστικά της. Τα συγκεκριμένα χαρακτηριστικά χρησιμοποιούνται από τους διάφορους αλγορίθμους ταυτοποίησης ή αναγνώρισης ως βασικά στοιχεία σύγκρισης, και αποθηκεύονται στην αντίστοιχη βάση δεδομένων.

Στη συνέχεια, κατά τη Διαδικασία της Αναγνώρισης (α), η εικόνα δακτυλικού αποτυπώματος προς αναγνώριση συγκρίνεται με τις  $N$  εικόνες-πρότυπα της βάσης δεδομένων έως ότου «αναγνωριστεί» η ταυτότητα του χρήστη. Κατά τη Διαδικασία Ταυτοποίησης (β) λαμβάνεται η εικόνα πρότυπο από τη βάση δεδομένων και συγκρίνεται με την προς εξέταση εικόνα προκειμένου να επιβεβαιωθεί η ταυτότητά του.

Όπως ήδη αναφέρθηκε έχουν αναπτυχθεί σύγχρονα εμπορικά ή/και ερευνητικά Βιομετρικά Συστήματα που βασίζονται στη χρήση συγκεκριμένων Βιομετρικών Χαρακτηριστικών. Για την αξιολόγηση τέτοιων συστημάτων βασικές παράμετροι θεωρούνται οι παρακάτω: [02]

- **Επίδοση:** ακρίβεια και ταχύτητα στην ταυτοποίηση των βιομετρικών χαρακτηριστικών, ικανοποίηση προαπαιτούμενων για την επιτυχή ταυτοποίηση (π.χ. υψηλή ανάλυση εικόνων).
- **Αποδοχή:** κατά πόσο το ευρύ κοινό μπορεί να αποδεχτεί τη συγκεκριμένη μέθοδο ταυτοποίησης ή αναγνώρισης.
- **Ασφάλεια:** κατά πόσο θεωρείται ασφαλές το συγκεκριμένο σύστημα

### Χαρακτηριστικά Βιομετρικών Συστημάτων

Τα κύρια Χαρακτηριστικά Βιομετρικών Συστημάτων που απαιτείται να έχουν είναι:

- η ακρίβεια
- η ταχύτητα
- η αξιοπιστία
- η διαδικασία της αποθήκευσης και των απαιτήσεων της επεξεργασίας
- οι διαδικασίες εγγραφής ενός χρήστη
- η μοναδικότητα
- το ποσοστό αντίστασης σε απάτη
- η αποδοχή τους από το χρήστη.

Παρακάτω αναλύονται κάθε ένα από αυτά τα χαρακτηριστικά.

➤ **Ακρίβεια**

Η ακρίβεια ενός Βιομετρικού Συστήματος ως το πιο κρίσιμο χαρακτηριστικό του, ορίζεται το ποσοστό συχνότητας ορθής αναγνώρισης ενός εξουσιοδοτημένου ατόμου από ένα μη εξουσιοδοτημένο. Δύο μονάδες μέτρησης χρησιμοποιούνται:

α) **το ποσοστό απόρριψης εξουσιοδοτημένων ατόμων** (Σφάλμα τύπου I ή σφάλμα απόρριψης) και

β) **το ποσοστό αποδοχής μη εξουσιοδοτημένων ατόμων** (Σφάλμα τύπου II ή Σφάλμα Αποδοχής). Το σημείο τομής των δύο αυτών μετρήσεων είναι το Ολικό Επίπεδο Σφάλματος (Crossover Error Rate, CER).

Τα δύο παραπάνω χαρακτηριστικά ρυθμίζονται ανάλογα με τις απαιτήσεις ασφάλειας του Βιομετρικού Συστήματος. Σε περιπτώσεις, για παράδειγμα, που είναι απολύτως απαραίτητο να μην υπάρχει πιθανότητα αποδοχής ενός μη εξουσιοδοτημένου ατόμου, το σύστημα θα ρυθμιστεί κοντά στο 0% για τον δείκτη ποσοστού του Σφάλματος Αποδοχής.

➤ **Ταχύτητα**

Η ταχύτητα απόκρισης αποτελεί ακόμη ένα σημαντικό χαρακτηριστικό των Βιομετρικών Συστημάτων. Έρευνες έχουν καταλήξει σε ένα γενικά αποδεκτό χρονικό όριο των πέντε (5) δευτερολέπτων για τη διαδικασία της αναγνώρισης. [03]

➤ **Αξιοπιστία**

Η αξιοπιστία ενός τέτοιου συστήματος ορίζεται ως συνεχής, ακριβής και γρήγορη λειτουργία του, χωρίς να απαιτείται υψηλό ποσοστό συντήρησης ή ελέγχου λειτουργίας.

➤ **Αποθήκευση δεδομένων και Απαιτήσεις επεξεργασίας**

Τα δύο αυτά χαρακτηριστικά στο παρελθόν επηρέαζαν το χρόνο επεξεργασίας ενός χρήστη. Σε ένα σύστημα με ορισμένο χαμηλό επίπεδο αποδοχής σφάλματος, η διαδικασία αναγνώρισης απαιτεί μεγαλύτερο χρόνο καθώς τα δεδομένα που εισάγονται πρέπει να συγκριθούν με όλα τα στοιχεία της βάσης δεδομένων. Η εμφάνιση ταχύτατων επεξεργασιών και η ελάττωση του κόστους σε συσκευές αποθήκευσης δεδομένων, καθιστούν σήμερα τις απαιτήσεις επεξεργασίας των βιομετρικών συσκευών ικανοποιητικές από άποψη λειτουργίας. Το μέσο μέγεθος ενός αρχείου με βιομετρικά στοιχεία κυμαίνεται μεταξύ 256 και 1000 bytes.

➤ **Διαδικασία Καταχώρησης**

Ο συνολικός χρόνος που απαιτείται για την εισαγωγή των στοιχείων ταυτότητας και του βιομετρικού χαρακτηριστικού ενός νέου χρήστη στο σύστημα ονομάζεται



διαδικασία καταχώρησης. Στα σημερινά συστήματα ο χρόνος καταχώρησης δεν αποτελεί πλέον χαρακτηριστικό αξιολόγησης καθώς η πλειοψηφία των συστημάτων εφαρμόζουν το γενικά αποδεκτό χρόνο καταχώρησης των δύο λεπτών ανά άτομο.

➤ **Μοναδικότητα**

Τα βιομετρικά συστήματα που βασίζονται σε μοναδικά χαρακτηριστικά του ανθρώπινου σώματος ενισχύουν την πιθανότητα της ορθής εφαρμογής της αναγνώρισης.

➤ **Παραποίηση στοιχείων**

Με τον όρο αυτό εννοείται τη χρήση ενός αποθηκευμένου αντιγράφου ενός Βιομετρικού Χαρακτηριστικού με σκοπό την επίτευξη μιας μη εξουσιοδοτημένης πρόσβασης στο σύστημα. Τα Βιομετρικά Συστήματα πρέπει να απαιτούν σημαντικό ποσοστό ακριβείας του βιομετρικού χαρακτηριστικού ώστε να μην είναι δυνατό να εισαχθούν ψευδή δεδομένα για την επίτευξη της πρόσβασης.

➤ **Αποδοχή του χρήστη**

Τα Βιομετρικά Συστήματα, λόγω της ιδιομορφίας που παρουσιάζουν ως προς τα εισαγόμενα δεδομένα (π.χ δακτυλικό αποτύπωμα, ίριδα ματιού) προκαλούν κοινωνικές αντιδράσεις. Οι χρήστες συχνά αντιδρούν, νοιώθοντας ότι πρέπει να καταχωρήσουν ένα γνώρισμα (π.χ. διαστάσεις παλάμης) του σώματος τους σε μία βάση δεδομένων του συστήματος κατά τη διαδικασία της εγγραφής τους.

Κυριαρχεί το συναίσθημα ότι παρακολουθούνται από το σύστημα και ότι καταγράφονται οι κινήσεις τους. Επιπλέον, υπάρχει φόβος των μεταδιδόμενων ασθενειών και της πρόκλησης σωματικής βλάβης από το σύστημα (π.χ. η χρήση των κόκκινων φωτεινών ενδείξεων που χρησιμοποιούνται στην ίριδα του ματιού, θυμίζει τις βλαβερές συνέπειες του laser). Παρόλα αυτά, δεν υπάρχουν αναφορές για πρόκληση σωματικών παρενεργειών από τα Βιομετρικά Συστήματα. Για το λόγο αυτό η εκπαίδευση και η ενημέρωση των χρηστών σχετικά με την τεχνολογία αυτή αποτελεί ένα κρίσιμο παράγοντα για την επιτυχή εφαρμογή τους.

### **Τρόπος Λειτουργίας Βιομετρικών Συστημάτων**

Η διαδικασία της βιομετρικής πιστοποίησης και αναγνώρισης ακολουθεί ένα συγκεκριμένο διάγραμμα ροής εργασιών. Οι διεργασίες που συντελούνται είναι οι εξής:

- Ο χρήστης αρχικά εγγράφεται στο βιομετρικό σύστημα παρέχοντας ένα δείγμα από τα βιομετρικά δεδομένα του, το οποίο μετατρέπεται σε προσωρινό αρχείο (template).
- Τα προσωρινά αρχεία (template) αποθηκεύονται στο βιομετρικό σύστημα για να χρησιμοποιηθούν για μελλοντικές συγκρίσεις.
- Κάθε φορά που ο χρήστης πρέπει να υποβληθεί σε πιστοποίηση ή αναγνώριση, προσφέρει τα βιομετρικά του δεδομένα, τα οποία μετατρέπονται

- σε ένα προσωρινό αρχείο (template).
- Το προσωρινό αρχείο (template) που παράχθηκε, συγκρίνεται με ένα ή περισσότερα από τα αποθηκευμένα προσωρινά αρχεία (template).
- Το αποτέλεσμα της σύγκρισης είναι το ποσοστό εμπιστοσύνης για το συγκεκριμένο δείγμα, το οποίο με την σειρά του συγκρίνεται με μια τιμή που έχει οριστεί για τη συγκεκριμένη τεχνολογία, το σύστημα, το χρήστη και τη συναλλαγή.
- Αν το ποσοστό εμπιστοσύνης υπερβαίνει την τιμή, τότε η σύγκριση θεωρείται επιτυχής και ο χρήστης ενημερώνεται.
- Αν το ποσοστό εμπιστοσύνης είναι μικρότερο από την τιμή, τότε η σύγκριση θεωρείται ανεπιτυχής και ο χρήστης ενημερώνεται.

Τα δεδομένα που παρέχει ο χρήστης στο σύστημα είναι μη επεξεργασμένα και δεν μπορούν να χρησιμοποιηθούν αυτούσια για τη διεξαγωγή συγκρίσεων. Πρέπει πρώτα να μετατραπούν σε μια άλλη μορφή, που να μπορεί να αναγνωρίσει και να επεξεργαστεί ο υπολογιστής. Η μορφή αυτή είναι τα προσωρινά αρχεία (template). Το αρχείο αυτό (template) είναι ένα συστατικό στοιχείο βιομετρικής τεχνολογίας, το οποίο παίζει σημαντικό ρόλο στην κατανόηση του τρόπου λειτουργίας των Βιομετρικών Συστημάτων. Πρόκειται για ένα μικρό αρχείο που προκύπτει από τα Βιομετρικά Χαρακτηριστικά του χρήστη. Χάρη στην τεχνολογία των αρχείων (template) τα Βιομετρικά Χαρακτηριστικά των χρηστών δεν χρειάζεται να αποθηκευθούν στο σύστημα.

### **Ιστορική Αναδρομή**

- **1686:** Ο Marcello Malpighi παρατηρεί τους διαφόρους σχηματισμούς των δακτυλικών αποτυπωμάτων.
- **1788:** Η πρώτη λεπτομερής περιγραφή των δακτυλικών αποτυπωμάτων έγινε από τον Mayer.
- **1809:** Ο Thomas Bewick ξεκίνησε να χρησιμοποιεί τα δακτυλικά του αποτυπώματα ως σφραγίδα του.
- **1823:** Ο Purkinje πρότεινε το πρώτο σχήμα ταξινόμησης των δακτυλικών αποτυπωμάτων.
- **1858:** Πρώτη συστηματική διαδικασία αναγνώρισης ατόμου μέσω του χεριού του.
- **1870:** Ανάπτυξη νέας μεθόδου από τον Bertillon για αναγνώριση ατόμων μέσω ανθρωπομετρικών χαρακτηριστικών.
- **1880:** Ο Henry Fauld βασιζόμενος σε εμπειρικές εκτιμήσεις, αναφέρθηκε στο γεγονός ότι τα δακτυλικά αποτυπώματα κάθε ατόμου είναι διαφορετικά.
- **1885:** Ο Γάλλος γιατρός Alphonse Bertillon προτείνει την ίριδα ως αναγνωριστικό μοναδικότητας.
- **1888:** Ο Galton έκανε μια εκτενή έρευνα σχετικά με τα δακτυλικά αποτυπώματα και είναι ο πρώτος που εισήγαγε τις μικρολεπτομέρειες (minutiae) στη διαδικασία σύγκρισης των αποτυπωμάτων.
- **1892:** Ανάπτυξη ενός νέου συστήματος κατηγοριοποίησης των δακτυλικών αποτυπωμάτων από τον Galton.



- **1896:** Ανάπτυξη νέας μεθόδου κατηγοριοποίησης των δακτυλικών αποτυπωμάτων από τον Henry.
- **1899:** Αναπτύχθηκε από τον Edward Henry το γνωστό «Σύστημα του Henry» για την ταξινόμηση των δακτυλικών αποτυπωμάτων. Σύμφωνα με το «Σύστημα του Henry» τα δακτυλικά αποτυπώματα κατηγοριοποιούνται σύμφωνα με κάποια βασικά τους χαρακτηριστικά. Με τον τρόπο αυτό μειώνεται ο απαιτούμενος χρόνος ταυτοποίησης των αποτυπωμάτων.
- **1903:** Ενσωμάτωση της μεθόδου των δακτυλικών αποτυπωμάτων στις φυλακές της πολιτείας της Νέας Υόρκης. Κατάρρευση της θεωρίας του Bertillon. Το λόγο για την κατάρρευση αυτή αποτελεί η εύρεση διδύμων με ίδια ανθρωπομετρικά χαρακτηριστικά.
- **1924 :** Η βάση του FBI διέθετε περίπου 810K κάρτες αποτυπωμάτων.
- **1936:** Πρόταση από τον οφθαλμολόγο Frank Burch για αναγνώριση ατόμου μέσω του σχεδίου της ίριδας.
- **1949:** Ο Βρετανός οφθαλμίατρος James Duggart παρατηρεί ότι η μοναδικότητα της ίριδας προσομοιάζει αυτή των δακτυλικών αποτυπωμάτων.
- **1960:** Έγιναν οι πρώτες προσπάθειες από το FBI και από την Αστυνομία του Παρισιού, προκειμένου να αναπτυχθούν Αυτόματα Συστήματα Ταυτοποίησης Δακτυλικών Αποτυπωμάτων. Η πρώτη αρχή αποτελεί τη βάση της ταυτοποίησης των αποτυπωμάτων, ενώ η δεύτερη τη βάση του διαχωρισμού των εν λόγω εικόνων σε ομάδες.
- **1960:** Ημι-αυτοματοποίηση της αναγνώρισης προσώπου.
- **1963:** Δημοσίευση μιας έρευνα του Hughes για την αυτοματοποίηση της μεθόδου των δακτυλικών αποτυπωμάτων.
- **1965:** Εκκίνηση ερευνών για αναγνώριση ατόμων μέσω αναγνώρισης της υπογραφής.
- **1969:** Άσκηση πιέσεων από το FBI, ώστε να υιοθετηθεί η μέθοδος της αναγνώρισης των ατόμων μέσω δακτυλικών αποτυπωμάτων, ως μία αυτοματοποιημένη διαδικασία.
- **1970:** Προώθηση της αυτοματοποίησης της διαδικασίας της αναγνώρισης προσώπου. Μοντελοποίηση των συμπεριφορικών χαρακτηριστικών της ομιλίας.
- **1974:** Διάθεση των πρώτων συστημάτων αναγνώρισης ατόμων μέσω της γεωμετρίας του χεριού, για εμπορική χρήση.
- **1975:** Χρηματοδότηση από το FBI για την ανάπτυξη αισθητήρων και για την προώθηση τεχνολογιών για την εξαγωγή των χαρακτηριστικών ενδιαφέροντος των δακτυλικών αποτυπωμάτων.
- **1976:** Ανάπτυξη του πρώτου πρωτότυπου συστήματος για αναγνώριση ομιλίας.
- **1976:** Ιδρύθηκε η Διεθνής Ένωση Αναγνώρισης Προτύπων (IARP).
- **1977:** Κατοχύρωση πατέντας για δυναμική λήψη πληροφορίας από υπογραφή.
- **1978:** Η IARP τέθηκε σε επίσημη ύπαρξη, τον Ιανουάριο του ίδιου έτους.
- **1980:** Η υπολογιστική όραση αναδύθηκε μετά το 1980 ως αποτέλεσμα επέκτασης του πεδίου της πληροφορικής, το οποίο καλείται ψηφιακή επεξεργασία εικόνας σε αλγορίθμους ανάλυσης και κατανόησης εικόνων.
- **1980:** Ίδρυση της ομάδας για την αναγνώριση ομιλίας στο Ινστιτούτο NIST

- (National Institute of Standards and Technology).
- **1985:** Παρουσίαση της ιδέας της μοναδικότητας της ίριδας, από τους οφθαλμολόγους Leonard Flom, Aran Safir.
  - **1986:** Δημοσίευση ενός προτύπου που αφορούσε στην ανταλλαγή δεδομένων ως προς τα δακτυλικά αποτυπώματα.
  - **1987:** Οι οφθαλμίατροι Flom και Safir πατεντάρουν την ιδέα της αναγνώρισης ίριδας.
  - **1988:** Ανάπτυξη του πρώτου ημι-αυτοματοποιημένου μοντέλου για την αναγνώριση ατόμου μέσω του προσώπου. Ανάπτυξη της τεχνικής eigenface στη μέθοδο αναγνώρισης προσώπου (L.Sirovich, M.Kirby).
  - **1991:** Εντοπισμός του προσώπου μέσα σε μία φωτογραφία, γεγονός που καθιστά την αναγνώριση προσώπου εφικτή σε πραγματικό χρόνο (M.A. Turk, A.P. Pentland).
  - **1992:** Ίδρυση της "Βιομετρικής Κοινοπραξίας" στους κόλπους της κυβέρνησης των Ηνωμένων Πολιτειών της Αμερικής.
  - **1993:** Έναρξη ερευνητικών προγραμμάτων για την καθιέρωση ενός προτύπου στο πεδίο της αναγνώρισης της ίριδας.
  - **1994:** Κατοχύρωση της πατέντας για την αναγνώριση ίριδας (Dr. John Daugman).
  - **1995:** Διάθεση εμπορικών προϊόντων για αναγνώριση ίριδας.
  - **1998:** Υιοθέτηση από το FBI της μεθόδου ταυτοποίησης ατόμου μέσω DNA για περιπτώσεις που εμπíπτουν στον τομέα της Εγκληματολογίας.
  - **2000:** Πραγματοποίηση ελέγχου της μεθόδου αναγνώρισης προσώπου σε ευρείας κλίμακας βάσεις δεδομένων.
  - **2001:** Χρήση της μεθόδου αναγνώρισης προσώπου σε αθλητική διοργάνωση ("Super Bow!") στην πόλη Tampa της Florida.
  - **2003:** Έναρξη του επίσημου συντονισμού των βιομετρικών δραστηριοτήτων στη κυβέρνηση των Ηνωμένων Πολιτειών της Αμερικής.  
Ενσωμάτωση των κυανοτυπιών στα ταξιδιωτικά έγγραφα από το διεθνή οργανισμό ICAO (International Civil Aviation Organization).  
Ίδρυση του ευρωπαϊκού οργανισμού EBF (European Biometrics Forum).
  - **2004:** Υιοθέτηση από το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών του συστήματος ABIS (Automated Biometric Identification System).  
Έκδοση Προεδρικής Οδηγίας (από τον πρόεδρο G Bush) για υποχρεωτική χρήση καρτών με σκοπό την ταυτοποίηση ατόμων μέσω βιομετρικών χαρακτηριστικών. Η Προεδρική αυτή απόφαση αφορούσε στα άτομα, τα οποία είχαν πρόσβαση σε κυβερνητικά κτίρια και συστήματα.
  - **2007:** Η βάση του FBI διέθετε πάνω από 200M κάρτες αποτυπωμάτων.



### **Συστήματα Βιομετρικής Αναγνώρισης**

Τα συστήματα βιομετρικής τεχνολογίας διαχωρίζονται σε δύο κατηγορίες:

1. Ανάλογα με τα φυσικά χαρακτηριστικά του ανθρώπου
  - Αναγνώριση δακτυλικών αποτυπωμάτων (fingerprint verification)
  - Αναγνώριση προσώπου (face recognition)
  - Ανάλυση ίριδας ματιού (iris recognition)
  - Αναγνώριση φωνής (voice recognition)
  - Ανάλυση αμφιβληστροειδή (retina analysis)
  - Ανάλυση DNA (DNA analysis)
  - Ανάλυση γεωμετρίας χεριού (hand geometry analysis) [03]
  
2. Ανάλογα με τα στοιχεία συμπεριφοράς του ανθρώπου
  - Αναγνώριση της υπογραφής (hand-written signature verification)
  - Ανάλυση πληκτρολόγησης (keystroke analysis)
  - Ανάλυση βηματισμού (gait analysis)

### **Φυσικά Χαρακτηριστικά**

#### **Αναγνώριση δακτυλικών αποτυπωμάτων (fingerprint verification)**



**ΔΑΚΤΥΛΙΚΟ  
ΑΠΟΤΥΠΩΜΑ**

Ο τύπος και η γεωμετρία των δακτυλικών αποτυπωμάτων είναι διαφορετικός σε κάθε άνθρωπο. Αυτά τα χαρακτηριστικά, δεν μεταβάλλονται με τη γήρανση. Τα πιο χαρακτηριστικά γνωρίσματα είναι οι καμπύλες και οι διαιρέσεις των σπειρών, καθώς και η ολική μορφή του δακτυλικού σπειρώματος.

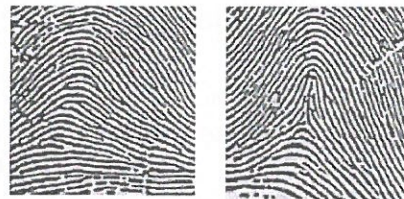
### Κατηγορίες αποτυπωμάτων

Τρεις βασικές κατηγορίες

- Τοξωτά (arch), ~5% των δακτύλων
- Κολποειδή (loop), ~65% των δακτύλων
- Σπειροειδή (whorl), ~30% των δακτύλων



### Τοξωτά (arch)



Plain arch

Tented arch

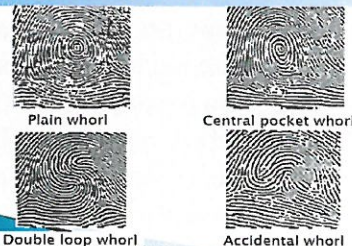
### Κολποειδή (loop)



Radial loop

Ulnar loop

### Σπειροειδή (whorl)



Plain whorl

Central pocket whorl

Double loop whorl

Accidental whorl



Τα συστήματα που χρησιμοποιούνται για την αναγνώριση των δακτυλικών αποτυπωμάτων είναι ιδιαίτερα πολύπλοκα.

Η οπτική ανίχνευση των δακτυλικών αποτυπωμάτων γίνεται από ειδικές κάμερες, οι οποίες είναι σχετικά ογκώδης. Μία ικανοποιητική τεχνική χρησιμοποιεί τις διαφορές των ηλεκτρονικών φορτίων στις σπείρες του δακτύλου ώστε να εντοπίσει τα σημεία του δακτύλου που εφαρμόζουν στο τσιπ.

Τα δεδομένα μετατρέπονται σε γραφική παράσταση και αποθηκεύονται από τη συσκευή.

Οι συσκευές αυτές λέγονται fingerprints scanners και διαθέτουν έναν αισθητήρα, όπου ο χρήστης τοποθετεί το δάκτυλό του για να καταγραφεί το αποτύπωμά του, βάσει του οποίου θα ελέγχεται κάθε ένας που θα προσπαθήσει στο μέλλον να μπει στον υπολογιστή. Το αποτύπωμα αποθηκεύεται σε μία βάση δεδομένων και το ειδικευμένο software που συνοδεύει αυτές τις συσκευές αναλαμβάνει να συγκρίνει τα χαρακτηριστικά του αποτυπώματος του όποιου εκκινεί το σύστημα με τα αποτυπώματα του χρήστη που έχει αποθηκευμένο. Σε περίπτωση μη ταυτοποίησης, ο υπολογιστής κλειδώνει και δεν αφήνει το σύστημα να εκκινήσει. [03]



### Βασικές τεχνολογίες των ανιχνευτών αποτυπώματος (fingerprint scanners)

Δύο είναι οι βασικές τεχνολογίες των fingerprint scanners.

- Η πρώτη προέρχεται απευθείας από τις ψηφιακές φωτογραφικές μηχανές και έχει αρχίσει να εκλείπει. Η συσκευή διαθέτει αισθητήρα CCD και φωτογραφίζει το δάκτυλο του χρήστη.

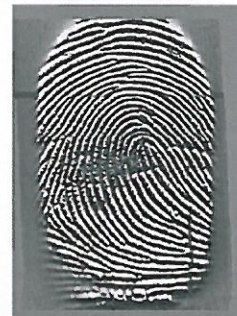
Τα αποτύπωμα αποθηκεύεται με τη μορφή φωτογραφίας. Αυτό σημαίνει ότι η συσκευή μπορεί να παραπλανηθεί από μία υψηλής ανάλυσης φωτογραφία (ακόμη και φωτοτυπία) του δακτύλου του χρήστη, γι' αυτό και δεν προτιμάται αρκετά ως λύση από τους κατασκευαστές.



- Ένας δεύτερος και ευρέως διαδεδομένος- τύπος αισθητήρα, είναι εκείνος που χρησιμοποιεί **πλέγμα κυκλωμάτων ημιαγωγών**.

Πιο συγκεκριμένα, η επιφάνεια του αισθητήρα αποτελείται από χιλιάδες λεπτεπίλεπτους ακροδέκτες (μικρότεροι από το πλάτος των γραμμών του δέρματος).

Οι ακροδέκτες αυτοί μέσω κυκλωμάτων ημιαγωγών φορτίζουν αντίστοιχο αριθμό πυκνωτών. Λόγω του ανάγλυφου της επιφάνειας του χεριού, κάποιοι πυκνωτές φορτίζονται και κάποιοι όχι, καθώς οι γραμμές του δέρματος ακουμπούν μόνο ορισμένους ακροδέκτες μεταδίδοντας το φορτίο του στατικού ηλεκτρισμού, ενώ οι «κοιλάδες» ανάμεσα στις γραμμές που δεν ακουμπούν τους υπόλοιπους ακροδέκτες αφήνουν τους αντίστοιχους πυκνωτές αφόρτιστους. Η διάταξη των φορτισμένων και μη φορτισμένων πυκνωτών αντιστοιχεί με το αποτύπωμα του χεριού. Με αυτόν τον τρόπο η συσκευή δεν εξαπατάται από φωτογραφίες του δάκτυλου του χρήστη, όπως συμβαίνει με τους οπτικούς αισθητήρες. [03]



Οι πρώτοι αλγόριθμοι ήταν αρκετά προβληματικοί, οδηγώντας είτε στην ταυτοποίηση ξένων αποτυπωμάτων, είτε στην απόρριψη του σωστού. Κατάσταση που έδωσε κακό όνομα στις συσκευές αυτές. Τα τελευταία χρόνια όμως η διαδικασία ταυτοποίησης είναι θεαματικά βελτιωμένη και τα σφάλματα ελαχιστοποιήθηκαν.

Συνήθως, προτείνεται το δακτυλικό αποτύπωμα να μην αποθηκεύεται σε κεντρική βάση δεδομένων αλλά σε κάρτα (π.χ έξυπνη κάρτα) ιδιοκτησίας του χρήστη. Η χρήση των παραπάνω συστημάτων είναι ευρεία σε τομείς της ιατρικής, σε κυβερνητικούς φορείς, σε αεροδρόμια, σε χρηματοοικονομικούς οργανισμούς κλπ.

### Βελτίωση Ποιότητας Εικόνας Δακτυλικού Αποτυπώματος

Στην διαδικασία Αναγνώρισης Δακτυλικών αποτυπωμάτων πρέπει να συμπεριλάβουμε και την διαδικασία βελτίωσης της ποιότητας εικόνας, η οποία προϋποθέτει την εφαρμογή τεχνικών που εφαρμόζονται διαδοχικά.

Αρχικά, εξάγεται η περιοχή επεξεργασίας και στη συνέχεια πραγματοποιείται κανονικοποίηση των επιπέδων του γκρι των εικονοστοιχείων που υπάρχουν εντός της περιοχής επεξεργασίας.

Στη συνέχεια, υπολογίζονται το τοπικό πεδίο προσανατολισμού κορυφογραμμών και η τοπική συχνότητα κορυφογραμμών της εικόνας.

Συνοψίζοντας, η διαδικασία για τη βελτίωση της ποιότητας εικόνας δακτυλικού αποτυπώματος περιλαμβάνει τα ακόλουθα βήματα:

- 1) Εξαγωγή Περιοχής Επεξεργασίας
- 2) Κανονικοποίηση
- 3) Υπολογισμός Πεδίου Προσανατολισμού Κορυφογραμμών
- 4) Υπολογισμός Συχνότητας Κορυφογραμμών
- 5) Φιλτράρισμα.

Στο παρακάτω σχήμα φαίνεται ένα διάγραμμα ροής της διαδικασίας βελτίωσης της εικόνας.



#### 1) Εξαγωγή Περιοχής Επεξεργασίας

Η περιοχή επεξεργασίας αποτελείται από όλα τα εικονοστοιχεία της εικόνας εκτός από εκείνα που ανήκουν στο φόντο (background). Ο εντοπισμός των εικονοστοιχείων του φόντου γίνεται με βάση την παρατήρηση ότι η διακύμανση των επιπέδων του γκρι σε μία περιοχή γύρω από αυτά είναι πολύ μικρή.



## 2) Κανονικοποίηση

Ο σκοπός της κανονικοποίησης είναι η μείωση των διακυμάνσεων των επιπέδων του γκρι κατά μήκος των κορυφογραμμών και των κοιλάδων της εικόνας του δακτυλικού

αποτυπώματος.

Έστω  $I$  η εικόνα του δακτυλικού αποτυπώματος,  $I(x,y)$  η τιμή του επιπέδου του γκρι στο σημείο  $(x,y)$ ,  $M$  η μέση τιμή και  $VAR$  η τυπική απόκλιση:

$$M = \frac{1}{N_p} \sum_{(x,y) \in R_p} I(x,y)$$
$$VAR = \frac{1}{N_p - 1} \sum_{(x,y) \in R_p} [I(x,y) - M]^2$$

όπου με  $R_p$  συμβολίζεται η περιοχή επεξεργασίας και  $N_p$  είναι το πλήθος των εικονοστοιχείων που ανήκουν σε αυτήν. Η κανονικοποιημένη εικόνα υπολογίζεται από την εξής σχέση:

$$J(x,y) = \begin{cases} M_0 + \sqrt{\frac{VAR_0 (I(x,y) - M)^2}{VAR}}, & I(i,j) > M \\ M_0 - \sqrt{\frac{VAR_0 (I(x,y) - M)^2}{VAR}}, & I(i,j) \leq M \end{cases}$$

όπου  $M_0$  και  $VAR_0$  είναι η επιθυμητή μέση τιμή και τυπική απόκλιση, αντίστοιχα

## 3) Υπολογισμός Πεδίου Προσανατολισμού Κορυφογραμμών

Ο τοπικός προσανατολισμός μιας κορυφογραμμής δακτυλικού αποτυπώματος σε ένα εικονοστοιχείο  $(x,y)$  είναι η γωνία  $\theta(x,y)$  που σχηματίζει η εφαπτομένη της κορυφογραμμής στο σημείο αυτό με τον οριζόντιο άξονα. Εφόσον οι κορυφογραμμές των δακτυλικών αποτυπωμάτων δεν έχουν κατεύθυνση, η γωνία  $\theta(x,y)$  κυμαίνεται στο εύρος  $[0,\pi]$ .

Έχουν προταθεί αρκετές μέθοδοι για τον υπολογισμό του προσανατολισμού. Οι μέθοδοι αυτές μπορούν σε γενικές γραμμές να διαχωριστούν σε μεθόδους κλίσης (gradient - based), σε μεθόδους σχισμής και προβολής (slit-based) και σε μεθόδους που στηρίζονται στο πεδίο της συχνότητας (frequency-based)

## 4) Υπολογισμός Συχνότητας Κορυφογραμμών

Η τοπική συχνότητα κορυφογραμμής  $F$  σε ένα σημείο  $(x,y)$  είναι ο αριθμός των κορυφογραμμών ανά μονάδα μέτρησης στην κατεύθυνση διανύσματος κάθετου στον τοπικό προσανατολισμό  $\theta(x,y)$ .

Η τοπική συχνότητα κορυφογραμμής, η οποία θα αναφέρεται πλέον ως συχνότητα, μπορεί να διαφέρει όχι μόνο ανάμεσα σε διαφορετικά δακτυλικά αποτυπώματα αλλά και ανάμεσα σε περιοχές της ίδιας εικόνας.

Οι Hong et al, 1998 πρότειναν την εκτίμηση της τιμής της συχνότητας υπολογίζοντας τον μέσο αριθμό των εικονοστοιχείων ανάμεσα σε δύο διαδοχικές κορυφές των επιπέδων του γκρι κατά μήκος της κάθετης κατεύθυνσης στον προσανατολισμό.

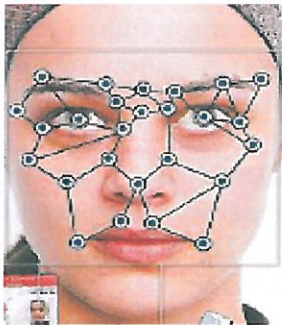
Σε μία περιοχή της εικόνας στην οποία δεν υπάρχουν μικρολεπτομέρειες ούτε σημεία ασυνέχειας, οι τιμές του επιπέδου του γκρι μπορούν να προσεγγιστούν με ένα ημιτονοειδές κύμα κατά μήκος μιας κατεύθυνσης κάθετης στον προσανατολισμό. Στον υπολογισμό της συχνότητας λαμβάνουν μέρος οι τιμές του επιπέδου του γκρι της περιοχής ενδιαφέροντος της εικόνας  $J(x, y)$  και το πεδίο προσανατολισμού  $\theta(x, y)$ .

### 5) Φιλτράρισμα

Εφόσον έχει υπολογιστεί ο προσανατολισμός και η συχνότητα των κορυφογραμμών των εικόνων δακτυλικών αποτυπωμάτων, εφαρμόζονται τεχνικές με σκοπό τη βελτίωση των εικόνων των κορυφογραμμών.

Στη μέθοδο που προτάθηκε από τους Hong et al, εφαρμόζεται ένα φίλτρο Gabor, ενώ σε αυτή που αναπτύχθηκε από τον Hastings το 2007, οι κορυφογραμμές βελτιώνονται με χρήση της προσανατολισμένης διάχυσης.

### Αναγνώριση προσώπου (face recognition)



**Εικόνα  
προσώπου**

Η τεχνική αυτή στηρίζεται στο γεγονός ότι η μοναδικότητα των χαρακτηριστικών γνωρισμάτων του προσώπου (π.χ το μέγεθος της μύτης, το σχήμα των ματιών, το πηγούνι, τα βλέφαρα, το στόμα) υποδεικνύει την ταυτότητα ενός ανθρώπου.

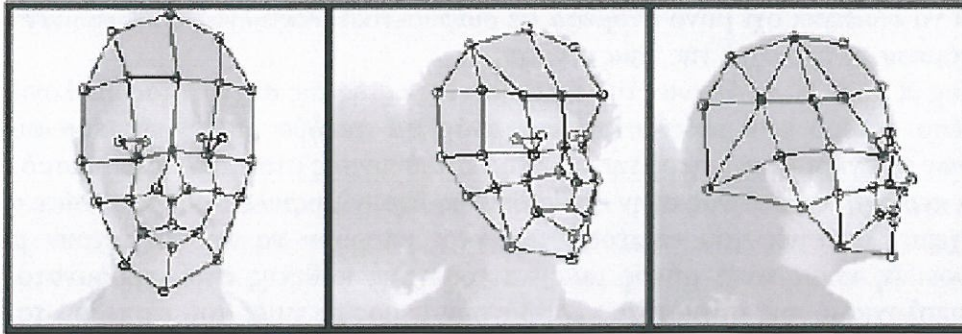
Η εξελισσόμενη, σε αυτό το πεδίο, τεχνολογία είναι ιδιαίτερα ακριβή διότι χρησιμοποιεί μεθοδολογίες νευρολογικών δικτύων. Επιπλέον, απαιτείται η χρήση κάμερας η οποία εξάγει τα χαρακτηριστικά γνωρίσματα του προσώπου και τα αποθηκεύει σε μία μαγνητική κάρτα.

Η διαδικασία αναγνώρισης προσώπου γίνεται μέσω ενός λογισμικού που μεταφράζει τα χαρακτηριστικά του προσώπου, όπως αυτά λαμβάνονται από μια εικόνα ή ένα video, σε ένα μοναδικό σετ ψηφιακών δεδομένων, διαμορφώνοντας έτσι αυτό που θα ονομάζαμε ηλεκτρονικό αποτύπωμα του προσώπου.

Όπως όλες οι βιομετρικές τεχνολογίες, έτσι και αυτή βασίζεται στην ιδιότητα που έχει το ανθρώπινο πρόσωπο να είναι μοναδικό για κάθε άνθρωπο.

Το πρόγραμμα χαρτογραφεί την γεωγραφία του ανθρώπινου κρανίου, διαβάζοντας την σχετική θέση και το μέγεθος των διαφόρων χαρακτηριστικών (μέτωπο, μάτια κ.α.) και τις διαφορές γωνίες και καμπυλότητες που αυτό έχει.





Το αποτύπωμα που σχηματίζεται χρησιμοποιείται τόσο σε συστήματα ταυτοποίησης, όσο και σε συστήματα πιστοποίησης, με συγκρίσεις προσώπων που γίνονται σε πραγματικό χρόνο. Κατά την διαδικασία ταυτοποίησης γίνεται σύγκριση του προσώπου ενός ατόμου με τα πρόσωπα που υπάρχουν σε μια βάση δεδομένων ώστε να καθοριστεί η ταυτότητά του. Η πιστοποίηση χαρακτηρίζεται σαν ένα - προς - ένα ταίριασμα, αφού το πρόσωπο ενός ατόμου συγκρίνεται με ένα μόνο αποθηκευμένο αποτύπωμα με σκοπό να επιβεβαιωθεί η ταυτότητά του.

Η τεχνολογία αναγνώρισης προσώπου είναι μοναδική λόγω της ικανότητάς της για γρήγορη επεξεργασία και ακριβές αποτέλεσμα σε πραγματικό χρόνο, σε βάσεις δεδομένων που περιέχουν εκατομμύρια πρόσωπα. Το λογισμικό μπορεί στιγμιαία να υπολογίσει το αποτύπωμα του προσώπου ενός ατόμου, είτε από ζωντανό video είτε από μια ακίνητη ψηφιακή εικόνα και ύστερα να βρει σε λίγα δευτερόλεπτα, μέσα από μια πολύ μεγάλη βάση δεδομένων, αυτά τα πρόσωπα που μοιάζουν ή αυτό που ταιριάζει ακριβώς. [04]

Οι εφαρμογές που μπορεί να έχει το πρόγραμμα είναι πολλές.

Η χρήση του σαν σύστημα πιστοποίησης βρίσκει εφαρμογή σε όλα τα σημεία που πρέπει να γίνει έλεγχος πρόσβασης. Ένα τέτοιο σημείο είναι τα μηχανήματα ATM των τραπεζών. Μεγάλη χρησιμότητα μπορεί να έχει επίσης και η χρήση του στο Internet και στο ηλεκτρονικό εμπόριο. Όμως η μεγάλη γκάμα των εφαρμογών του βρίσκεται στα συστήματα ασφαλείας.

Η αναγνώριση προσώπου αποτελεί μια βιομετρική τεχνολογία που έχει ένα σημαντικό πλεονέκτημα σε σχέση με τις άλλες. Το σύστημα μπορεί να καταγράψει το αποτύπωμα του προσώπου, με διακριτικό τρόπο, χωρίς το εν λόγω άτομο να το γνωρίζει και χωρίς να έχει την δυνατότητα να το αρνηθεί. Ο συνδυασμός του προγράμματος με ένα δίκτυο από κάμερες και η χρήση μεγάλων βάσεων δεδομένων, μας δίνουν σε όλη την έκταση τις δυνατότητες του συστήματος αυτού. Μπορεί να γίνεται η καταγραφή ενός πλήθους ανθρώπων με συστήματα βίντεο και το πρόγραμμα να εντοπίζει σε πραγματικό χρόνο τα προεπιλεγμένα αυτά άτομα (π.χ. ύποπτοι) που υπάρχουν στη βάση δεδομένων. Εκεί λοιπόν που το πρόγραμμα αυτό εμφανίζει τις μεγάλες του ικανότητες, είναι στις περιπτώσεις παρακολούθησης, ταυτοποίησης και επιτήρησης ανάμεσα σε μεγάλο αριθμό ατόμων. Αυτό το κάνει πολύτιμο σε συστήματα ασφαλείας μεγάλων χώρων.





Έτσι αποτελεί απαραίτητο εργαλείο, στον εντοπισμό υπόπτων ή ανεπιθύμητων προσώπων σε αεροδρόμια, στρατιωτικές βάσεις, κυβερνητικά κτήρια ή άλλους αντίστοιχους χώρους, όπου υπάρχει ανάγκη να γίνεται εντοπισμός υπόπτων, είτε σε μεγάλη απόσταση, είτε ανάμεσα σε μεγάλο πλήθος.

Εκτός αυτών, η τεχνολογία αναγνώρισης προσώπου βρίσκει μεγάλη χρήση στην περίπτωση διαχείρισης καταστάσεων που αφορούν την συγκέντρωση μεγάλου αριθμού ατόμων, όπως θερμοίμαχοι οπαδοί ομάδων ή διαδηλωτές. Έχει ήδη χρησιμοποιηθεί σε γήπεδα της Αμερικής, αλλά και στη καταπολέμηση του χουλιγκανισμού στα ποδοσφαιρικά γήπεδα της Αγγλίας.

Μεγάλες εταιρίες ήδη παρέχουν και νέες λύσεις που συνδυάζουν την τεχνολογία αναγνώρισης προσώπου με άλλες βιομετρικές τεχνολογίες (ίριδα, φωνή, κ.α.) αλλά και με ήδη υπάρχοντα συστήματα ταυτοποίησης που βασίζονται σε κάρτες.

Η τεχνολογία αναγνώρισης προσώπου θα μπορούσε να οδηγήσει στο μέλλον σε ένα κόσμο που δεν θα υπάρχει η ανάγκη για χρήση καρτών, κλειδιών, PIN και υπογραφών, αφού το πρόσωπό μας θα είναι ένα ιδιωτικό, ασφαλές και βολικό password για όλες τις πιθανές χρήσεις.

Στα συστήματα αυτά υπάρχουν αρκετοί περιορισμοί εφαρμογής που σχετίζονται με τη θέση του προσώπου έναντι της κάμερας, το φωτισμό λήψης κλπ.

Επίσης, αντιμετωπίζουν δυσκολίες αναγνώρισης σε περιπτώσεις πρόσκαιρων μεταβολών του προσώπου (π.χ μορφασμοί του προσώπου).

Για την αντιμετώπιση των εκφράσεων χρησιμοποιούνται οι παρακάτω ενέργειες:

- ✓ Η επιφάνεια πρέπει να είναι αμετάβλητη στον φωτισμό, τον προσανατολισμό και την μετατόπιση.

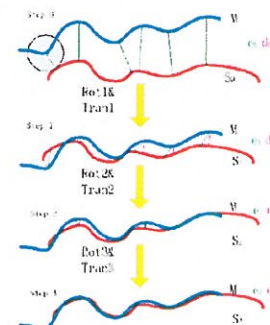
- ✓ Απόρριψη των παραμορφώσιμων περιοχών.

Αυτό μπορεί να γίνει με ευθυγράμμιση επιφανειών με επαναληπτικά βήματα, τα οποία είναι:

- Καθορισμός κοντινότερων σημείων
- Υπολογισμός στροφής και μετατόπισης

- ✓ Ανθεκτικοί τοπικοί περιγραφείς.

- ✓ Μοντέλο ισομετρικής παραμόρφωσης: το δέρμα κάμπτεται, δεν συμπιέζεται, δεν επιμηκώνεται.



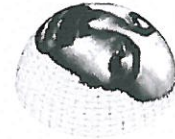


Στις **Ισομετρικές παραμορφώσεις** οι γεωδαισιακές αποστάσεις των σημείων της επιφάνειας παραμένουν σταθερές. Παρακάτω φαίνεται ο υπολογισμός των γεωδαισιακών αποστάσεων και η απεικόνισή τους με MDS σε:

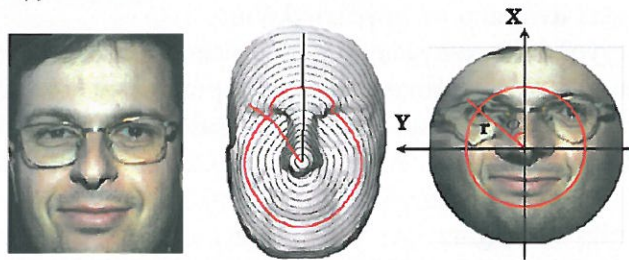
ευκλείδειο χώρο

2 – σφαίρα

3 – σφαίρα



Στην **απεικόνιση των πολικών γεωδαισιακών** συντεταγμένων παρουσιάζεται 'εξαφάνιση' των εκφράσεων.



➤ Έχουμε δύο γραμμικά μοντέλα (PCA)

Σε αυτή την περίπτωση υπάρχει ένα σετ παραμέτρων, το οποίο ελέγχει την ταυτότητα και ένα άλλο την έκφραση. Γίνεται προσαρμογή ενός ελαστικά παραμορφώσιμου μοντέλου στην επιφάνεια του προσώπου. Οι κόμβοι, οι οποίοι δείχνουν τον προσανατολισμό της τοποθέτησης του μοντέλου έχουν ανατομική σημασία και περιγράφονται διανυσματικά (→).



$$v_k^{xp} = \sum_{i=1}^I \sum_{j=1}^J w_{ijk} a_i^x b_j^p$$

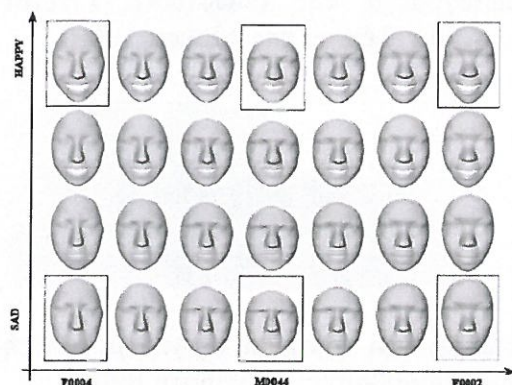
- Για το σχήμα του προσώπου απαιτούνται: ανατομικά σημεία και Προκρούστεια ανάλυση.

$$s = \bar{s} + V_s p_s$$

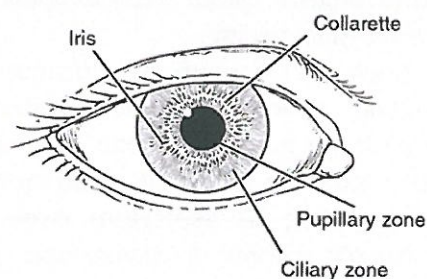
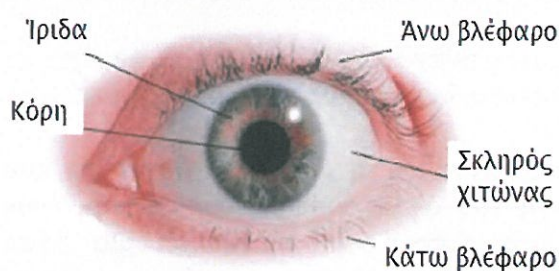
- Για την εμφάνιση ανεξάρτητου σχήματος (warping)

$$A(\bar{s}) = \bar{A}(\bar{s}) + V_{AP}A$$

Αυτά καταλήγουν στην αποσύζευξη της ταυτότητας – έκφρασης.



### Ανάλυση ίριδας ματιού (iris recognition)



Η ίριδα αποτελείται από δύο περιοχές, την Central Pupillary Zone και την Outer Cilliary Zone. Το σύνολό τους λέγεται Collarette.

Η αναγνώριση και ταυτοποίηση της ανθρώπινης ίριδας σύμφωνα πάντα με ειδικούς μελετητές αποτελεί μια μοναδική και απαραβίαστη μέθοδο αναγνώρισης κάποιου ατόμου. Αυτό συμβαίνει γιατί η ίριδα του ματιού ενός ανθρώπου είναι το μοναδικό ανατομικό στοιχείο του, για το οποίο υπάρχει πραγματικά ισχυρή πιθανότητα να μοιάζει με άλλο πάνω στον πλανήτη.

Οι μικρολεπτομέρειες της ίριδας καθορίζονται τυχαία κατά την εμβρυική ανάπτυξη ενός ανθρώπου και είναι διαφορετικές ακόμα και στα δύο μάτια. Το χρώμα αλλάζει – αυξάνεται κατά την παιδική ηλικία και μετά παραμένει σχετικά σταθερή.

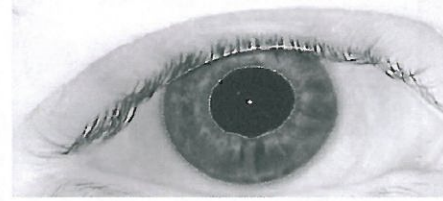
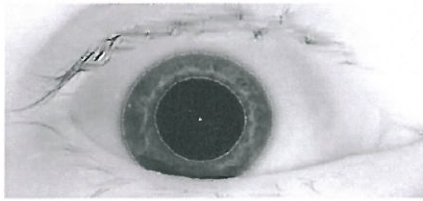
Το όλο σύστημα ονομάζεται Iris Recognition System (IRS) και αναγνωρίζει το κατά πόσο ένας άνθρωπος είναι πραγματικά αυτός που ισχυρίζεται ότι είναι. Το σύστημα



IRS αποτελείται από μια μονάδα οπτικής αναγνώρισης (κάμερα-grabber), μια μονάδα ελέγχου της κάμερας, καθώς και ένα server που διαθέτει μια βάση προσωπικών δεδομένων.

Η διαδικασία οπτικής αναγνώρισης της ίριδας έχει ως εξής:

Όταν το μάτι ενός ανθρώπου πλησιάσει περίπου 5 με 10 εκατοστά από το φακό της οπτικής κάμερας, ο φακός της κάμερας εστιάζει στην περιοχή της ίριδας του. Στη συνέχεια, αφού εστιάζει η κάμερα και έχει μια καθαρή εικόνα της ίριδας, ο μηχανισμός της κάμερας τραβάει μια φωτογραφία της (snapshot). Γίνεται επεξεργασία της εν λόγω φωτογραφίας από τη μονάδα ελέγχου της κάμερας. [04]



Το σχεδιάγραμμα του μοτίβου της ίριδας μετατρέπεται ψηφιακά σε μια μοναδική διάταξη αλγόριθμων, που αποτελεί και τον κωδικό πρόσβασης του χρήστη.[05]

Μόλις ολοκληρωθεί αυτή η διαδικασία, η μονάδα ελέγχου της κάμερας επικοινωνεί με τον κεντρικό server, ο οποίος στη συνέχεια θα ελέγξει τον εν λόγω κωδικό, με την database του. Αν ο χρήστης βρεθεί σαν καταχώρηση στην βάση δεδομένων, τότε η αναγνώριση πραγματοποιείται και επιβεβαιώνεται η ταυτότητα του χρήστη.

Η γενικότερη χρήση του συστήματος IRS, έχει πιστοποιηθεί ως μη επιβλαβής με οποιονδήποτε τρόπο στον ανθρώπινο οργανισμό, σύμφωνα με τα πρότυπα διεθνών οργανισμών υγείας.

Σίγουρα η εφαρμογή ενός τέτοιου συστήματος αναγνώρισης, μπορεί να παρέχει το επίπεδο προστασίας και ασφάλειας προσωπικών δεδομένων που απαιτούν οι επικίνδυνοι καιροί τους οποίους διανύουμε.

Αυτό που θα άξιζε να παρατηρηθεί όμως, είναι και η όλη επικινδυνότητα που ενδεχομένως να περιέχεται στην εφαρμογή του όλου συστήματος. Εφόσον ένας κεντρικός server ή γενικότερα μια μονάδα ελέγχου, θα εμπεριέχει μια βάση δεδομένων γεμάτη από προσωπικά στοιχεία (για παράδειγμα: ταυτότητα χρήστη, αριθμός τραπεζικού λογαριασμού του, διεύθυνσή του κτλ.), υπάρχει η πιθανότητα να διαρρεύσουν στοιχεία σε άτομα ανάξια εμπιστοσύνης. Ενώ δηλαδή δεν υπάρχει πλέον ο κίνδυνος να πλαστογραφηθούν τα στοιχεία μας από κάποιον άλλο, υπάρχει ο κίνδυνος κάποιος τρίτος να “εισβάλλει” στη βάση δεδομένων προσωπικών στοιχείων του συστήματος.

Ας ελπίσουμε τα συστήματα IRS που ετοιμάζονται από διάφορες εταιρείες να διαθέτουν από την πρώτη στιγμή διάθεσής τους υψηλό βαθμό ασφάλειας προσωπικών δεδομένων και να μη χρειαστεί να παρουσιαστεί κάποια διαρροή προσωπικών στοιχείων για να ληφθεί το θέμα της ασφάλειας υπόψη.

Μέθοδοι με τις οποίες μπορεί να γίνει η Αναγνώριση της Ίριδας είναι:

- Η μέθοδος Daugman, κατά την οποία έχουμε φωτισμό Led και χρήση κάμερας, απεικόνιση της ίριδας σε ένα κανονικοποιημένο σύστημα συντεταγμένων, Active



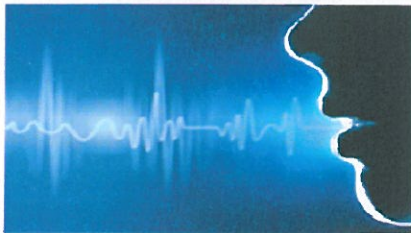
Contours, συνέλιξη με φίλτρα Gabor, κβαντισμό συντελεστών → 256 IrisCode και σύγκριση βάσει απόστασης Hamming.

- Η μέθοδος Wildes, κατά την οποία υπάρχει διάχυτο πολωμένο φως και χρήση κάμερας χαμηλού φωτισμού, Hough Transform, φίλτρα Laplacian of Gaussian και κανονικοποιημένη συσχέτιση.
- Η Τοπική Ισοστάθμιση Ιστογράμματος
- Οι συνδυασμοί PCA, LDA, DLDA, SVM
- Το Linear Prediction Cepstral Coefficients
- Οι Υποζώνες και ημέτρηση αυτοομοιότητας με εκτίμηση της κλασματικής διάστασης (fractal dimension)
- Διαμέριση σε blocks και δημιουργία Local Binary Patterns
- Οι 4 δυαδικές εικόνες από τα 4 MSBs, εφαρμογή connected και υπολογισμός αριθμού Euler.

Χρησιμοποιούνται και εναλλακτικά φίλτρα και μετασχηματιστές όπως:

- Log Gabor Φίλτρα
- Wavelets σε 1 Δ κύκλους γύρω από την κόρη
- Wavelets Packet
- Discrete Cosine Transform
- Hilbert Transform + Αυθεντική Εικόνα

### Αναγνώριση φωνής (voice recognition)



#### Αναγνώριση Φωνής

Τεχνικές που εστιάζονται στον προσδιορισμό της ταυτότητας των ομιλητών στα χαρακτηριστικά των φωνητικών ήχων. Αυτά τα χαρακτηριστικά επηρεάζονται από το μήκος της φωνητικής έκτασης του χρήστη, καθώς επίσης και τη μορφή του στόματος και τις ρινικές κοιλότητες.

Οι μετρήσεις μπορούν να ληφθούν ενώ οι χρήστες εκφράζουν μια οριζόμενη φράση, ή ενώ εκφράζουν οποιοδήποτε συνδυασμό λέξεων ή αριθμών.

Οι μετρήσεις είναι συνήθως επαναλαμβανόμενες

σε διάφορους χρόνους, χτίζοντας έτσι ένα χρήσιμο προφίλ της φωνής. Το σύστημα εξάγει το προφίλ φωνής και το συγκρίνει με προηγούμενως καταγεγραμμένα δείγματα φωνής. Το βασικό προτέρημα αυτής της τεχνολογίας είναι η δυνατότητα για εξ' αποστάσεως πιστοποίηση. Δηλαδή δεν είναι αναγκαίο ο χρήστης να βρίσκεται μπροστά σε κάποιο μηχάνημα ή συσκευή του συστήματος, όπως γίνεται κατά την αναγνώριση δακτυλικού αποτυπώματος ή προσώπου, αλλά μπορεί να βρίσκεται χιλιόμετρα μακριά χρησιμοποιώντας το τηλέφωνό του ή να βρίσκεται στο σπίτι του και να χρησιμοποιήσει ένα κοινό μικρόφωνο.

Η φράση - κλειδί συνήθως πρέπει να είναι διάρκειας ενός έως τριών δευτερολέπτων. Δεν χρειάζεται να περιέχει κανενός είδους μυστικές πληροφορίες ή ειδικές λέξεις. Μερικά τυπικά παραδείγματα τέτοιων φράσεων είναι το ονοματεπώνυμο, η διεύθυνση ή η πόλη του χρήστη.



Ένα πρόβλημα που δημιουργείται συχνά είναι το ότι μαζί με τη φράση-κλειδί περνάνε και θόρυβοι που προκαλούνται άθελα μας, όπως θόρυβος με τα χείλη, θόρυβος αναπνοής, βήχας, άσχετες συλλαβές όπως 'αα' ή 'εε'.

Συνήθεις ανησυχίες για τα συστήματα Αναγνώρισης φωνής προκαλούν οι απομιμήσεις. Αυτό δεν είναι σημαντικό, γιατί οι συσκευές σκόπιμα εστιάζουν σε διαφορετικά χαρακτηριστικά της ομιλίας, απ' ό,τι οι άνθρωποι. Οι απομιμητές εστιάζονται στα χαρακτηριστικά που ως άνθρωποι ακούν και κάνουν φτωχή δουλειά με τα υπόλοιπα. Ακόμα μια απειλή για τα συστήματα φωνής είναι η κλωνοποίηση της φωνής. Όμως και αυτός ο φόβος είναι μηδαμινός αν υπολογίσει κανείς ότι για να δημιουργηθεί ένας κλώνος φωνής χρειάζονται 10-40 ώρες ομιλίας του αυθεντικού χρήστη και ότι το κόστος πλησιάζει τα 200.000 δολάρια. [04]

### Ανάλυση αμφιβληστροειδή (retina analysis)



### Αμφιβληστροειδής χιτώνας

Μαζί με τη σάρωση ίριδας, η σάρωση αμφιβληστροειδούς είναι ίσως οι πιο ακριβείς και αξιόπιστη βιομετρική τεχνολογία, όμως είναι και μεταξύ των πιο δύσκολων στη χρήση. Η σάρωση αμφιβληστροειδούς είναι ένα από τα παλαιότερα βιομετρικά. Από το 1930 έρευνες έδειξαν ότι η μορφή των αγγείων αίματος στο πίσω μέρος του ανθρώπινου ματιού είναι διαφορετική από άτομο σε άτομο, ακόμα και σε δίδυμα αδέρφια. [04]

Επίσης ο αμφιβληστροειδής παραμένει ίδιος σε όλη τη ζωή του ανθρώπου, με την εξαίρεση ορισμένων τύπων από εκφυλιστικές ασθένειες του ματιού, ή περιπτώσεις σοβαρών τραυμάτων στο κεφάλι. Ο αμφιβληστροειδής χιτώνας του ματιού είναι ένα μικρό νεύρο ( $1/50^{\circ}$  της ίντσας) στο πίσω μέρος του ματιού, είναι το μέρος του ματιού το οποίο αισθάνεται το φως και μεταδίδει παλμούς δια μέσου του οπτικού νεύρου προς τον εγκέφαλο. Τα αιμοφόρα αγγεία που χρησιμοποιούνται για τη βιομετρική αναγνώριση βρίσκονται κατά μήκος του νωτιαίου αμφιβληστροειδούς, το έσχατο από τα τέσσερα επίπεδα του αμφιβληστροειδούς. Οι συσκευές σάρωσης αμφιβληστροειδούς διαβάζουν δια μέσου της κόρης του ματιού, γι' αυτό απαιτείται ο χρήστης να τοποθετήσει το μάτι του εντός μισής ίντσας από τη συσκευή και να μείνει ακίνητος μέχρις ότου η συσκευή ανάγνωσης εξακριβώσει την ταυτότητα του. Ο χρήστης κοιτάει σ' ένα περιστρεφόμενο πράσινο φως. Παίρνονται 350 – 400 σημεία αναφοράς και αποθηκεύονται σ' ένα πεδίο 96 bytes, εξασφαλίζοντας ότι το μέτρημα είναι σωστό, με ένα αμελητέο βαθμό σφάλματος. Σε σύγκριση με το δακτυλικό αποτύπωμα που χρειάζονται 30-70 διακριτά σημεία, γίνεται φανερό το πολύ υψηλό επίπεδο ακρίβειας της τεχνολογίας αυτής.

Στα πλεονεκτήματα αυτής της μεθόδου αναφέρονται τα ακόλουθα :

- Μηδαμινή πιθανότητα να κάποιος χρήστης να διεκδικήσει λάθος ταυτότητα και να γίνει αποδεκτός (μόλις μία πιθανότητα στο ένα εκατομμύριο) [04]
- Σταθερότητα στο βιομετρικό δείγμα

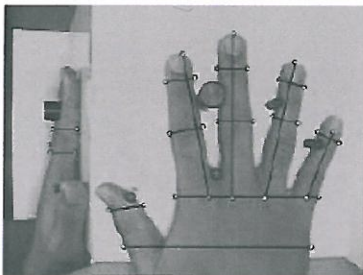


- Ανθεκτική στην απάτη. Θα ήταν πολύ δύσκολο και χρονοβόρο να δημιουργηθεί ένα ψεύτικο δείγμα αμφιβληστροειδούς
- Μικρή ποσότητα δεδομένων (μόλις 96 bytes)

Μερικά μειονεκτήματα είναι τα εξής :

- Δυσκολία στη χρήση
- Διστακτικότητα των χρηστών. Το μάτι και ειδικά το εσωτερικό του ματιού είναι πολύ ευαίσθητο και γι' αυτό πολύ χρήστες είναι διστακτικοί στο να χρησιμοποιήσουν τέτοιες συσκευές
- Στατικός σχεδιασμός. Σε αντίθεση με τις άλλες τεχνολογίες, οι οποίες μπορούν να εκμεταλλευτούν τα πλεονεκτήματα των νέων τεχνολογιών, όπως καλύτερης ποιότητας κάμερες ή αξιοποίηση πυριτίου, ή σάρωση αμφιβληστροειδούς είναι περιορισμένη σε συγκεκριμένους μηχανισμούς σύλληψης του δείγματος και συγκεκριμένα πρωτοκόλλα
- Κόστος. Οι συσκευές σάρωσης αμφιβληστροειδούς κοστίζουν περίπου \$2000-\$2500.

### Ανάλυση γεωμετρίας χεριού (hand geometry analysis)



#### **Γεωμετρία χεριού και δακτύλων**

Είναι μια αυτοματοποιημένη μέτρηση πολλών μεγεθών του χεριού και των δακτύλων. Η τεχνολογία αυτή χρησιμοποιεί το ύψος των δακτύλων, την απόσταση μεταξύ των κλειδώσεων και το σχήμα των αρθρώσεων για να πιστοποιήσει την ταυτότητα του χρήστη. Παρόλο που δεν είναι η πιο ακριβής τεχνολογία, η σάρωση χεριού έχει αποδειχτεί ως η ιδανική λύση για χαμηλού επιπέδου εφαρμογές ασφάλειας. Η μέθοδος απόκτησης του βιομετρικού δείγματος είναι αρκετά απλό. Ο χρήστης τοποθετεί το χέρι του στην ειδική συσκευή ακουμπώντας την παλάμη του σε μία μεταλλική επιφάνεια διαστάσεων 8x10. (Όπως φαίνεται στις παρακάτω εικόνες) Στη συνέχεια ο χρήστης ευθυγραμμίζει το χέρι του σύμφωνα με τα πέντε ειδικά καρφιά, που είναι σχεδιασμένα ώστε να υποδείξουν την κατάλληλη θέση του αντίχειρα, του δείκτη και του μεσαίου. Το σύστημα χρησιμοποιεί μια 32.000 pixel CCD (charged coupled device) ψηφιακή κάμερα, εξάγοντας συμπεράσματα για το μήκος, το πλάτος, το πάχος και την επιφάνεια του χεριού από τις εικόνες των περιγραμμάτων που σχεδιάζονται μέσα στον σαρωτή. Γίνονται πάνω από 90 μετρήσεις και τα χαρακτηριστικά του χεριού αναπαρίστανται σ' ένα πρότυπο 9 bytes. Η σάρωση χεριού ενίοτε παρεξηγείται με τη σάρωση παλάμης που είναι μια εντελώς ξεχωριστή τεχνολογία.



Πλεονεκτήματα της σάρωσης χεριού :

- Ευκολία στη χρήση. Απλή διαδικασία και με κατάλληλη εκπαίδευση μπορούν να μειωθούν και τα λάθη στην τοποθέτηση του χεριού. Με μια μικρή εξαίρεση στα άτομα μεγάλης ηλικίας ή σε άτομα με αρθρικά προβλήματα στα χέρια, που ίσως να μη μπορούν να ανοίξουν τα δάκτυλα και να τοποθετήσουν το χέρι τους στην συσκευή.
- Ανθεκτική στην απάτη.
- Μικρό μέγεθος προτύπου. Μόλις 9 Bytes.
- Αντίληψη του χρήστη. Σε αντίθεση με τη σάρωση προσώπου ή τις τεχνολογίες βασισμένες στο μάτι, οι οποίες μπορεί να συναντούν κάποιες αντιδράσεις, η σάρωση χεριού είναι αποδεκτή από τη συντριπτική πλειοψηφία των χρηστών.

Μειονεκτήματα της σάρωσης χεριού :

- Στατικός σχεδιασμός. Η τεχνολογία της σάρωσης χεριού παραμένει σε μεγάλο βαθμό αμετάβλητη για χρόνια.
- Κόστος. Οι σαρωτές χεριού κοστίζουν περίπου \$1400 - \$2000
- Κακώσεις στο χέρι. Όπως σε όλα τα βιομετρικά φυσικές αλλαγές μπορεί να προκαλέσουν εσφαλμένη απόρριψη των χρηστών.
- Ακρίβεια. Παρόλο που είναι πιο αξιόπιστη από τα βιολογικά βιομετρικά, όπως η φωνή και η υπογραφή, η σάρωση χεριού δεν μπορεί να πραγματοποιήσει αναζητήσεις ένα -προς- πολλά [04]

### Ανάλυση DNA (DNA Analysis)



Το βασικό ερώτημα σ' αυτή την περίπτωση είναι το κατά πόσο το DNA μπορεί να συμπεριληφθεί στις βιομετρικές τεχνολογίες.

Το DNA διαφέρει από τα τυπικά βιομετρικά σε πολλά σημεία :

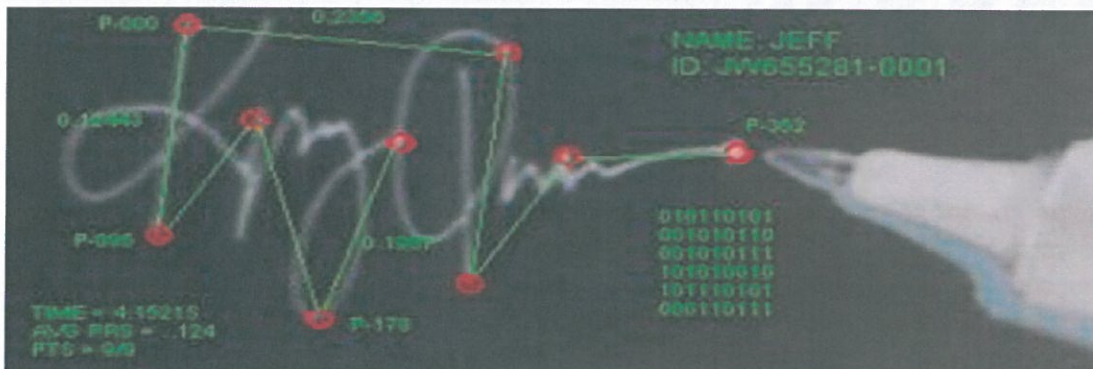
- Το DNA απαιτεί ένα χειροπιαστό φυσικό δείγμα, σε αντίθεση με μια εικόνα, ένα αποτύπωμα, ή μια εγγραφή. [04]
- Το ταίριασμα του DNA δεν γίνεται σε πραγματικό χρόνο και συγχρόνως δεν είναι όλα τα στάδια της σύγκρισης αυτοματοποιημένα.
- Το ταίριασμα του DNA δεν δημιουργεί πρότυπα ή εξαγωγή χαρακτηριστικών, αλλά αντιθέτως αναπαριστά τη σύγκριση με πραγματικά δείγματα.

Ανεξάρτητα από αυτές τις βασικές διαφορές, το DNA είναι ένας τύπος βιομετρικής αφού χρησιμοποιείται ως φυσικό χαρακτηριστικό στην επαλήθευση και τον

προσδιορισμό ενός χρήστη. Το αν το DNA θα βρει χρήση πέρα από την παρούσα χρήση του και σε άλλες εφαρμογές είναι αβέβαιο. Λογικές συζητήσεις πάνω στο πως, πότε και που θα έπρεπε ή δεν θα έπρεπε να χρησιμοποιηθεί, ποιος θα ελέγχει τα δεδομένα, που θα έπρεπε να αποθηκευτούν αυτά, είναι απαραίτητα πριν την χρήση του να επεκτείνονται σε πεδίο ανησυχίας. Οι συνθήκες κάτω από τις οποίες η χρήση, η συλλογή, η αποθήκευση και η διάθεση πρέπει να είναι οροθετημένες και ενισχυμένες. Αυτοί οι προσδιορισμοί θα διαφέρουν από εφαρμογή σε εφαρμογή. Είναι παράλογο η χρήση του DNA σε δημόσιου οφέλους προγράμματα αντιμετώπισει ισοδύναμα με τη χρήση DNA σε μια έρευνα εγκληματία.

### Χαρακτηριστικά Συμπεριφοράς

#### Αναγνώριση της υπογραφής (hand-written signature verification)



Είναι η βιομετρική τεχνολογία, η οποία δεν έχει ευρεία χρήση, όμως ίσως σύντομα βοηθήσει στην αντιμετώπιση της πιστοποίησης επίσημων εγγράφων. Μετρώντας τον τρόπο με τον οποίο ένας χρήστης γράφει το όνομα του, ένα συνθηματικό, ή μια φράση κλειδί, η σάρωση υπογραφής ερευνά τον τρόπο, την ταχύτητα, την πίεση και άλλους παράγοντες οι οποίοι συνδέονται με τη διαδικασία της υπογραφής. Η σάρωση υπογραφής εξασφαλίζει αξιόπιστη αναγνώριση ατόμων, με βάση την υπογραφή τους. Χρησιμοποιεί μετρήσεις του μοναδικού τρόπου με τον οποίο δημιουργείται μια χειρόγραφη υπογραφή, ώστε να επιβεβαιώσει την ταυτότητα του χρήστη.

Σε μεγάλες επιχειρήσεις ή μέσω του internet μια ψηφιακή υπογραφή καθιστά ικανές τις εφαρμογές να παρέχουν αυξημένη μυστικότητα και αξιόπιστη ηλεκτρονική εξουσιοδότηση, σε αντίθεση με ένα συνθηματικό, ένα PIN ή μια keycard, που μπορεί να ξεχαστούν, να χαθούν, ή να κλαπούν. Τα συστήματα αυτά αναλύουν και τα δυναμικά χαρακτηριστικά γνωρίσματα της χειρόγραφης υπογραφής για να ελέγξουν την ταυτότητα του υπογράφοντος.

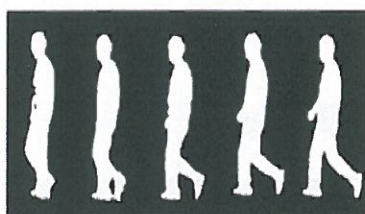
Επειδή κάθε άτομο έχει τον προσωπικό του γραφικό χαρακτήρα, το σύστημα παίρνει τα χαρακτηριστικά του τρόπου γραφής και αναλύουν τη δυναμική του χτυπήματος, της ταχύτητας και της πίεσης. Ενώ με εξάσκηση κάποιος ίσως μπορέσει να αντιγράψει την οπτική εικόνα της υπογραφής κάποιου άλλου, είναι πολύ δύσκολο, έως αδύνατο, να αντιγράψει τον τρόπο με τον οποίο το άτομο αυτό υπογράφει. Ακόμα και αν η υπογραφή είναι τέλεια σχεδιασμένη, η ταχύτητα, η δύναμη και η



πίεση θα διαφέρουν.

Αρκετά συστήματα σάρωσης υπογραφής ενσωματώνουν μια συνάρτηση μάθησης, η οποία μπορεί αυτομάτως να απορροφά και να απεικονίζει κάθε φυσική αλλαγή στην υπογραφή κατά τη διάρκεια του χρόνου. Αυτά τα συστήματα χρησιμοποιούν τις αλλαγές στην πίεση, στη μορφή, στην κατεύθυνση και στην ταχύτητα σε συνάρτηση με το χρόνο. Έτσι τα δεδομένα αναλύονται σε τέσσερις διαστάσεις – x (οριζόντια ταχύτητα), y (κάθετη ταχύτητα), z (πίεση) και t (χρόνος). [04]

### Ανάλυση βηματισμού (gait analysis)



### Βάδισμα

Στην λίστα με τις τεχνολογίες βιομετρικής αναγνώρισης, όπως των δαχτυλικών αποτυπωμάτων, της ίριδας του ματιού και του σχήματος του προσώπου, πρέπει πλέον να προσθέσουμε και την αναγνώριση βηματισμού. Παρόλο που η συγκεκριμένη τεχνολογία βρίσκεται ακόμα στο στάδιο της ανάπτυξης, θεωρείται αρκετά υποσχόμενη και αναμένεται, όταν τελειοποιηθεί, να αποτελέσει ένα ισχυρό όπλο στην προσπάθεια εντοπισμού εγκληματιών. Είναι πλέον διαπιστωμένο ότι κάθε ένας περπατάει με ένα δικό του

μοναδικό τρόπο που ονομάζεται βηματισμός. Ίσως αυτό από πρώτη μάτια να φαίνεται παράξενο, αν όμως ληφθούν υπόψη τα διαφορετικά φυσικά χαρακτηριστικά του κάθε ανθρώπου, συμπερένεται ότι είναι λογικό οι κινήσεις που εκτελεί κάποιος όταν περπατάει να είναι μοναδικές.

Το γεγονός αυτό αξιοποιείται εδώ και κάποιο διάστημα από ερευνητές, προκειμένου να υλοποιήσουν μια πλατφόρμα που θα διακρίνει αυτές τις διαφορές και θα δημιουργεί συγκεκριμένα πρότυπα αποσκοπώντας εντέλει, στην σύγκριση και αναγνώριση της ταυτότητας προσώπων.

Ένα από αυτά είναι και το σύστημα για την αναγνώριση βηματισμού, που ανατέθηκε κυρίως στο Georgia Institute of Technology, ενώ και άλλοι ερευνητές από διάφορα πανεπιστημιακά ιδρύματα ασχολούνται με το συγκεκριμένο θέμα. [04]

Απώτερος σκοπός της έρευνας είναι η δημιουργία προηγμένων συστημάτων επιτήρησης, που θα μπορούν να αναγνωρίσουν και να πιστοποιήσουν ανθρώπινους στόχους από τον τρόπο που περπατάνε σε κρίσιμες περιοχές ασφαλείας, όπως αεροδρόμια ή γύρω από κυβερνητικά κτίρια.

Θέλοντας τώρα να αναλυθεί η τεχνική με την οποία επιτυγχάνεται η αναγνώριση βηματισμού, πρέπει να αναφερθεί ότι οι μέθοδοι που έχουν αναπτυχθεί βασίζονται σε δύο βασικά μοντέλα.

- Το πρώτο μοντέλο χρησιμοποιεί βιντεοκάμερες προκειμένου να συλλαμβάνονται οι εικόνες των ατόμων που περπατάνε.
- Το δεύτερο μοντέλο βασίζεται στην τεχνολογία των Radar.

Στην πρώτη περίπτωση κάμερες και υπολογιστές συνεργάζονται προκειμένου να δημιουργήσουν “υπογραφές βηματισμού” που θα είναι μοναδικές για κάθε άνθρωπο. Όταν ένας άνθρωπος περπατάει, τα μέρη του σώματός του, δηλαδή χέρια, γόνατα,



πόδια, αγκώνες και άλλα, δημιουργούν ένα συγκεκριμένο επαναλαμβανόμενο πρότυπο κίνησης. Έτσι, λοιπόν, βιντεοκάμερες συλλαμβάνουν την δραστηριότητα της κίνησης και μεταφέρουν τα δεδομένα σε ηλεκτρονικό υπολογιστή για περαιτέρω ανάλυση. Ο υπολογιστής επεξεργάζεται τις κινήσεις και σε συνδυασμό με μαθηματικές συναρτήσεις και αλγόριθμους, δημιουργεί την λεγόμενη “υπογραφή βηματισμού”, που είναι ξεχωριστή για τον καθένα και θα αποτελεί εφεξής το στοιχείο αναγνώρισης του. Το συγκεκριμένο μοντέλο επεξεργάζονται ερευνητές από το Ινστιτούτο Τεχνολογίας της Μασαχουσέτης, το πανεπιστήμιο του Southampton.

Οι δοκιμές του προγράμματος πραγματοποιήθηκαν με την συνδρομή εθελοντών που περπάτησαν πάνω σε τεχνητούς διαδρόμους αλλάζοντας κάθε φορά το φόντο. Το ποσοστό ακριβείας στην αντιστοίχιση των προτύπων με το εκάστοτε άτομο που υπόκεινται στον έλεγχο, κυμαίνονταν από 90% μέχρι 95%. Σε πρώτη φάση η επίδοση αυτή θεωρείται αρκετά ενθαρρυντική, πρέπει όμως να λάβουμε υπόψη ότι η έρευνα πραγματοποιήθηκε σε ένα καθαρά πειραματικό περιβάλλον με ιδανικές συνθήκες. Στον «πραγματικό κόσμο» όμως υπεισέρχονται παράγοντες, όπως κίνηση μέσα σε πλήθος, διαφορετικές και δύσκολες συνθήκες φωτισμού, καθώς και μεγάλες αποστάσεις. Όλοι αυτοί οι παράγοντες αποτελούν τις μεγάλες προκλήσεις που καλούνται να αντιμετωπίσουν τα συγκεκριμένα συστήματα.

Οι ψυχολογικές μελέτες δείχνουν ότι οι άνθρωποι έχουν μία μικρή αλλά στατιστικά σημαντική δυνατότητα να αναγνωρίζουν τους βηματισμούς των άλλων. Πρόσφατα, έχει υπάρξει πολύ ενδιαφέρον για το όραμα των μηχανικών συστημάτων που μπορούν να αναπαραγάγουν και να βελτιώσουν επάνω σε αυτά τα συστήματα την ανθρώπινη δυνατότητα για εφαρμογή στο βιομετρικό προσδιορισμό.

Ενώ ο βηματισμός έχει αρκετές πλεονεκτικές ιδιότητες ως βιομετρικό στοιχείο (είναι ήσυχο και μπορεί να γίνει με απλή χρήση οργάνων), υπάρχουν διάφοροι παράγοντες όπως οι μεταβολές λόγω των υποδημάτων, του περιβάλλοντος, της κούρασης, του τραυματισμού, και της μετάβασης του χρόνου.

Οι άνθρωποι συχνά θεωρούν ότι μπορούν να αναγνωρίσουν ένα εξοικειωμένο πρόσωπο από μακριά αναγνωρίζοντας απλά τον τρόπο με τον οποίο περπατάνε. Αυτή η εμπειρία, έχει το προβάδισμα στην ανάπτυξη της αναγνώρισης βηματισμού σαν ένα από του βιομετρικά στοιχεία.

Σαν βιομετρικό σύστημα, ο βηματισμός έχει διάφορες πλεονεκτικές ιδιότητες:

Τη λήψη των εικόνων περιγράφοντας το βηματισμό ενός ατόμου, μπορεί να γίνει εύκολα, με απλή χρήση οργάνων, και δεν απαιτεί τη συνεργασία ή ακόμα και τη ενημέρωση του ατόμου που είναι υπό την επιτήρηση.

Στην πραγματικότητα, φαίνεται ότι υπάρχει η δυνατότητα το άτομο μπορεί να μην γνωρίζει την επιτήρηση και την αναγνώριση που του υποβάλλεται από τις διάφορες βιομετρικές αρχές. [05]



### Ανάλυση Πληκτρολόγησης (Keystroke analysis)



### Πληκτρολόγηση

Όπως υποδηλώνει, αυτή η μέθοδος εξετάζει τον τρόπο με τον οποίο ένα άτομο δακτυλογραφεί ή πιέζει τα πλήκτρα σ' ένα πληκτρολόγιο. Η αυθεντική τεχνολογία προέρχεται από την ιδέα αναγνώρισης ενός αποστολέα σημάτων Morse, χρησιμοποιώντας ένα κλειδί τηλεγραφίας γνωστό ως “ γροθιά του αποστολέα”, δια του οποίου οι χειριστές μπορούσαν να αναγνωρίσουν τους αποστολείς που διαβίβαζαν ένα μήνυμα από το ρυθμό, το μέτρο και τη βραχύτητα του σήματος.

Στις αρχές της δεκαετίας του '80 το Εθνικό Ίδρυμα Επιστημών (National Science Foundation) και το National Institute of Standards στην Αμερική διεξήγαγαν έρευνες για να αποδείξουν ότι ο τρόπος δακτυλογράφησης περιέχει μοναδικά χαρακτηριστικά τα οποία μπορούν να αναγνωριστούν. Αυτή η τεχνολογία αναλύει χαρακτηριστικά όπως η ταχύτητα, η δύναμη, η συχνότητα λάθους, ο συνολικός χρόνος δακτυλογράφησης ενός συγκεκριμένου συνθηματικού και ο χρόνος που μεσολαβεί από το πάτημα ενός συγκεκριμένου πλήκτρου έως το πάτημα ενός άλλου συγκεκριμένου πλήκτρου.

Πλεονεκτήματα της δυναμικής πατήματος πλήκτρου :

- Η επιβεβαίωση βασίζεται στην παραδοχή ότι ο τρόπος δακτυλογραφεί ένα άτομο είναι ξεχωριστός, ειδικά ο ρυθμός του. Ακόμα και αν κάποιος μαντέψει το σωστό συνθηματικό, δεν θα μπορέσει να το δακτυλογραφήσει με τον κατάλληλο ρυθμό.
- Η συσκευή εισόδου μπορεί να είναι το υπάρχον πληκτρολόγιο. Έτσι μειώνεται δραστικά το κόστος.

Μειονεκτήματα αυτής της τεχνολογίας :

- Υπάρχουν πολλές τεχνικές δυσκολίες που κάνουν την συγκεκριμένη τεχνολογία να μην αποδίδει τα αναμενόμενα αποτελέσματα.
- Οι μισές προσπάθειες σε εμπορικές τεχνολογίες έχουν αποτύχει.
- Διαφορές στα πληκτρολόγια, ακόμα και της ίδιας εταιρίας, και στα πρωτόκολλα επικοινωνίας προκαλούν εμπόδια στις εταιρίες ανάπτυξης αυτής της τεχνολογίας.

### Εφαρμογή Βιομετρικών Συστημάτων Αναγνώρισης Προτύπων

Καθώς όλο και περισσότεροι οργανισμοί δίνουν πλέον όλο και μεγαλύτερη έμφαση και προσοχή σε θέματα διαχείρισης κινδύνου (managing risk), οι διάφορες τεχνολογίες που σχετίζονται με τον έλεγχο βιομετρικών δεδομένων θα γνωρίσουν σταθερή ανάπτυξη, λόγω της διαρκώς αναπτυσσόμενης ανάγκης για υψηλότερα επίπεδα ασφάλειας σε δεδομένα και ιδιοκτησίες.

Αντικείμενα μεμονωμένα και με δυνατότητα να μεταφερθούν, μπορούν να

καταγραφούν άμεσα μέσω μιας ακριβούς διαδρομής ελέγχου, έτσι ώστε να περιορίζονται τα φαινόμενα των κλοπών. Συνήθως αυτό επιτυγχάνεται μέσω χειροκίνητων εφαρμογών, απομακρυσμένων συστημάτων διαχείρισης ή ακόμα και έγγραφων λιστών επιλογής. Με την ενσωμάτωση διαδικασιών ασφαλείας, οι αρμόδιοι διαχειριστές μπορούν να γνωρίζουν ανά πάσα στιγμή ποιος είναι σε ποια θέση, και τι ακριβώς κάνει όσο βρίσκεται εκεί.

Τα Βιομετρικά Συστήματα Αναγνώρισης συνήθως χρησιμοποιούνται σε εφαρμογές που σχετίζονται με:

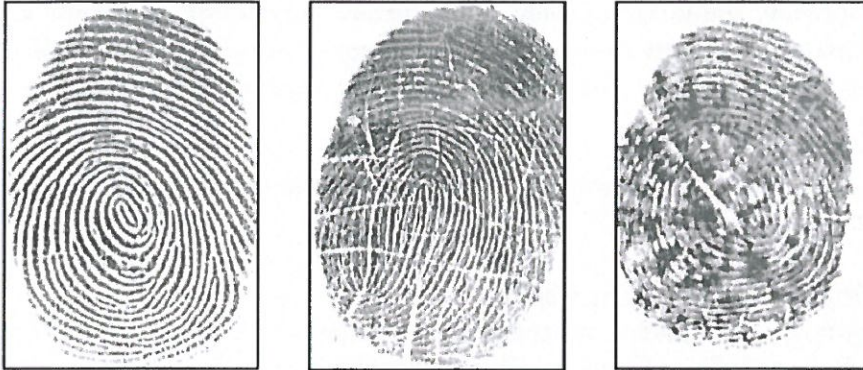
- Έλεγχος πρόσβασης σε φυσικούς χώρους
- Ασφάλεια χρήσης λογισμικών, ταυτοποίηση χρηστών
- Συνοριακό έλεγχο, έκδοση βιομετρικών διαβατηρίων
- Καταγραφή χρόνου εργασίας προσωπικού εταιριών
- Μηχανές αναζήτησης που αναγνωρίζουν αντικείμενα από φωτογραφίες
- Εγκληματολογία για τον εντοπισμό δραστών
- Εφαρμογές διαδικτύου (ηλεκτρονικό εμπόριο, ηλεκτρονική τραπεζική, κ.ά.)
- Αεροδρόμια και οι χώροι επικύρωσης εισιτηρίων και επιβίβασης επιβατών
- Οικονομικές υπηρεσίες
- Εκπαιδευτικές εφαρμογές, στις οποίες χρησιμοποιείται η αναγνώριση ίριδας, π.χ. για δανεισμό βιβλίων ή online εξετάσεις σε σύνδεση με συστήματα ελεγχόμενης εισόδου των σχολικών ιδρυμάτων.

Σε αρκετές περιπτώσεις χρησιμοποιούνται και μικτά βιομετρικά συστήματα. Ένα μικτό βιομετρικό σύστημα ταυτοποίησης (multi-biometrics) συνδυάζει δύο ή περισσότερες βιομετρικές μεθόδους, εκμεταλλευόμενο τα πλεονεκτήματα καθεμίας από αυτές για την επίτευξη ακόμα μεγαλύτερης πιστότητας και αξιοπιστίας. [06]

Παρακάτω αναλύεται η χρήση των Βιομετρικών Συστημάτων στις μέρες μας. Η χρήση τους ποικίλει ανάλογα με τον τομέα στον οποίο χρησιμοποιούνται και την χώρα εφαρμογής τους.



Σκανάρισμα – Αναγνώριση Δαχτυλικών Αποτυπωμάτων



➤ Καναδάς

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) στον έλεγχο εργαζομένων σε Ξενοδοχειακή Μονάδα. Σε ένα πολύ μεγάλο ξενοδοχείο του Καναδά ο Διευθυντής του εγκατέστησε το βιομετρικό σύστημα της Toshiba με το όνομα Experchem, με σκοπό να ελέγχει την επιχείρησή του. Με το πρόγραμμα αυτό οι εργαζόμενοι τοποθετούν ένα ηλεκτρονικό ρολόι σε έναν αναγνώστη και έπειτα ένα δάχτυλό τους σε μια ηλεκτρονική συσκευή αναγνώρισης αποτυπωμάτων και μπορούν να εισέλθουν στην επιχείρηση. Με το σύστημα αυτό οποιαδήποτε παρατυπία μπορεί να αποφευχθεί. Επίσης ο Καναδάς έχει αρχίσει την έρευνα για την τοποθέτηση βιομετρικής τεχνολογίας στα σύνορα μέσω ενός προγράμματος της δημόσιας ασφάλειας και Κοινότητας, με σκοπό την ασφάλεια και τον έλεγχο της μετανάστευσης. [07]

➤ Πουέρτο Ρίκο

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) στον έλεγχο εργαζομένων και πελατών σε Τραπεζικούς Φορείς. Η Τράπεζα Westernbank χρησιμοποιεί τεχνολογία σκαναρίσματος δαχτυλικών αποτυπωμάτων. Η τεχνολογία αυτή είναι προαιρετική για τους πελάτες της και υποχρεωτική για τους υπαλλήλους της. [08]

➤ Μεξικό

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) για την πληρωμή εργαζομένων οικονομικού οργανισμού. Το Grupo Financiero Banorte ένας πρωτοποριακός οικονομικός οργανισμός, χρησιμοποιεί έναν συνδυασμό βιομετρικής τεχνολογίας και smart cards για την πληρωμή των εργαζομένων του, οι οποίοι δεν διαθέτουν τραπεζικό λογαριασμό. Οι εργαζόμενοι αυτοί υποβάλλονται σε έλεγχο δαχτυλικών αποτυπωμάτων και στη συνέχεια χρησιμοποιούν την smart card, η οποία δουλεύει σαν χρεωστική κάρτα και με αυτή παραλαμβάνουν τα χρήματά τους.

➤ Η.Π.Α.

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) στην Υγεία για τήρηση ιστορικού αρχείου και απορρήτου και σε Στρατιωτικές Υπηρεσίες. Το New York



State of Mental Health χρησιμοποιεί τη σκανάρισμα δαχτυλικού αποτυπώματος για καλύτερη τήρηση του ιστορικού αρχείου του και ιατρικού απορρήτου. Επίσης έχουν σχεδιαστεί και τα αμερικάνικα διαβατήρια, τα οποία είναι βασισμένα στα βιομετρικά χαρακτηριστικά. Ακόμα το Υπουργείο Αμύνης κάνει χρήση μιας κάρτας, η οποία έχει διανεμηθεί σε όλο το προσωπικό των Αμερικάνικων Στρατιωτικών Υπηρεσιών και περιέχει τα βιομετρικά τους στοιχεία και φωτογραφία τους, οι οποίες χαράζονται ανάγλυφα με λείζερ. [09]

➤ **Πενσυλβάνια**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) για πίστωση σε εκπαιδευτικά Ιδρύματα. Στο Welsh Valley Middle School οι μαθητές αντί να πληρώνουν το γεύμα τους με μετρητά, μπορούν να χρησιμοποιούν περιφερειακά χρεωστικά μηχανήματα με σκανάρισμα δαχτύλων. Στο τέλος κάθε μήνα αποστέλλεται ο λογαριασμός στους γονείς των μαθητών ή σε προγράμματα δωρεάν σίτισης. Αυτό εξυπηρετεί μια συγκεκριμένη νομοθεσία, η οποία απαγορεύει την αποκάλυψη και διάκριση μαθητών, οι οποίοι σιτίζονται με κυβερνητικά κονδύλια. [10]

➤ **Γκάμπια**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) για έκδοση δελτίων ταυτότητας, αδειών κατοικίας και οδήγησης. Η κυβέρνηση της Γκάμπια χρησιμοποιεί την έκδοση ταυτοτήτων με βιομετρικά στοιχεία, τα οποία αποθηκεύονται σε μια βάση δεδομένων. Μεταξύ των βιομετρικών εγγράφων που εκδίδονται στην Γκάμπια είναι και οι άδειες κατοικίας και οδήγησης.

➤ **Γερμανία**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) για έκδοση διαβατηρίων και ασφάλειας των Ολυμπιακών Αγώνων. Η Γερμανική κυβέρνηση ενέκρινε την εφαρμογή ePass, δηλαδή ένα βιομετρικό διαβατήριο. Τι ePass περιέχει ένα τσιπ με μια ψηφιακή φωτογραφία και ένα δαχτυλικό αποτύπωμα από κάθε χέρι. Επίσης η Γερμανία χρησιμοποιεί την βιομετρική τεχνολογία και στους Ολυμπιακούς Αγώνες για να προστατέψει τους Γερμανούς αθλητές.

➤ **Βραζιλία**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) για έκδοση διαβατηρίων. Τα διαβατήρια αυτά περιλαμβάνουν διάτρηση με λείζερ, UV κρυμμένα σύμβολα, υπογραφή, φωτογραφία και 10 δαχτυλικά αποτυπώματα. Όλα αυτά αποθηκεύονται στο πρόγραμμα ηλεκτρονικών διαβατηρίων ICAO (International Civil Aviation Organisation).

➤ **Ιράκ**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) για έκδοση ταυτοτήτων και ασφάλεια πολιτών. Στο Ιράκ η χρήση βιομετρικών χαρακτηριστικών είναι εκτεταμένη. Σχεδόν όλοι οι πολίτες κατέχουν βιομετρικές ταυτότητες και σε περίπτωση που κάποιος την χάσει, ο προσδιορισμός τους μπορεί να βρεθεί και να ελεγχθεί με την χρησιμοποίηση των μοναδικών βιομετρικών πληροφοριών.



➤ **Ινδία**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) για έκδοση ταυτοτήτων και ασφάλεια πολιτών. Η Ινδία αποσκοπεί στην χρήση των βιομετρικών ταυτοτήτων από όλους τους πολίτες της, οι οποίοι ανέρχονται τους 1.25 δισεκατομμύρια. Εάν το καταφέρει αυτό θα είναι η μεγαλύτερη εφαρμογή βιομετρικών συστημάτων στον κόσμο. Οι ταυτότητες θα αποθηκεύουν τα βιομετρικά χαρακτηριστικά σε μια κεντρική βάση δεδομένων.

➤ **Ηνωμένο Βασίλειο**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) σε σχολεία, ασφάλεια και Εθνικό Σύστημα Υγείας. Σε πολλά σχολεία χρησιμοποιούνται τα δαχτυλικά αποτυπώματα για την διευκόλυνση πληρωμής διδάκτρων και σχολικών γευμάτων. Η χρησιμοποίηση των βιομετρικών χαρακτηριστικών υπολογίζεται να γίνει και σε συστήματα ασφαλείας αλλά και στο Εθνικό Σύστημα Υγείας για την τήρηση ιατρικού ιστορικού αλλά και των φακέλων των ασθενών. [11]

➤ **Ισραήλ**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) για δημιουργία βάσης δεδομένων. Η βάση αυτή θα περιέχει τα δαχτυλικά αποτυπώματα των Ισραηλινών και το περίγραμμα των προσώπων τους.

➤ **Ολλανδία**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) για έκδοση διαβατηρίων. Τα ολλανδικά διαβατήρια περιέχουν τα δαχτυλικά αποτυπώματα και ένα τσιπ με πληροφορίες του κατόχου και τη φωτογραφία του. [12]

➤ **Αυστραλία**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) σε Τραπεζικά Συστήματα. Η Αυστραλία χρησιμοποιεί ένα Πρότυπο ISO βιομετρικών χαρακτηριστικών για την εξακρίβωση της γνησιότητας των καταναλωτών και του προσωπικού στον τομέα των χρηματοπιστωτικών υπηρεσιών με τη χρήση των δαχτυλικών αποτυπωμάτων.

➤ **Ελλάδα**

Εφαρμογή Αναγνώρισης Δαχτυλικών Αποτυπωμάτων (H.R.) σε Βιομετρικά Διαβατήρια. Τα διαβατήρια έχουν ψηφιακή απεικόνιση, σάρωση δαχτυλικών αποτυπωμάτων και βιομετρικών στοιχείων πάνω σε ένα τσιπ RFID. Ο συνδυασμός αυτός των βιομετρικών στοιχείων έχει στόχο να δημιουργήσει ένα ασφαλές περιβάλλον, το οποίο θα προστατεύεται από ψευδή έγγραφα.

## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

Λίστα Εταιρειών και Ιστοσελίδων, οι οποίες έχουν αναπτύξει την ταυτοποίηση δακτυλικών αποτυπωμάτων.

Όνομα Εταιρείας	Ιστοσελίδα
123 ID Inc	<a href="http://www.123id.us">www.123id.us</a>
Antheus Technology Inc	<a href="http://www.antheustechnology.com">www.antheustechnology.com</a>
Avalon Systems Inc	<a href="http://www.avalonsysinc.com">www.avalonsysinc.com</a>
BIO-key International Inc	<a href="http://www.bic-key.com">www.bic-key.com</a>
Biolink Technologies International	<a href="http://www.biolinkusa.com">www.biolinkusa.com</a>
Bioscrypt Inc	<a href="http://www.bioscrypt.com">www.bioscrypt.com</a>
Cogent Systems Inc	<a href="http://www.cogentsystems.com">www.cogentsystems.com</a>
Dermalog Identification Systems GmbH	<a href="http://www.dermalog.de">www.dermalog.de</a>
Golden Finger System	<a href="http://www.ergoldenfinger.com">www.ergoldenfinger.com</a>
Griaule Tecnologia	<a href="http://www.griaule.com">www.griaule.com</a>
Identix Inc	<a href="http://www.identix.com">www.identix.com</a>
Sagem Morpho Inc	<a href="http://www.morpho.com">www.morpho.com</a>
NEC	<a href="http://www.nec.com">www.nec.com</a>
Neurotechnology Ltd	<a href="http://www.neurotechnology.com">www.neurotechnology.com</a>
The Phoenix Group, Inc	<a href="http://www.afix.net">www.afix.net</a>
Motorola	<a href="http://www.motorola.com">www.motorola.com</a>
Raytheon Company	<a href="http://www.raytheon.com">www.raytheon.com</a>
Technomagia Co.Ltd	<a href="http://www.technomagia.co.jp">www.technomagia.co.jp</a>
Ultra-Scan	<a href="http://www.ultra-scan.com">www.ultra-scan.com</a>

Ενδεικτική λίστα εταιρειών και ιστοσελίδων τους που έχουν αναπτύξει συστήματα αυτόματης ταυτοποίησης δακτυλικών αποτυπωμάτων

### Σκανάρισμα – Αναγνώριση Προσώπου



#### ➤ Αγγλία

Εφαρμογή σκαναρίσματος προσώπου από την Αστυνομία για την ασφάλεια χώρων. Στο Newham της Αγγλίας 114 κάμερες CCTV καταγράφουν ότι γίνεται επί 24ώρου σε μια γειτονιά, η οποία θεωρείται επικίνδυνη. Το σύστημα διαθέτει λογισμικό σκαναρίσματος προσώπου της Visionics, το οποίο σκανάρει τα πρόσωπα και τα συγκρίνει με μια λίστα σεσημασμένων κακοποιών. Με αυτό τον τρόπο έχουν καταφέρει μείωση της εγκληματικότητας από 39% σε 21%.

#### ➤ Μεξικό

Εφαρμογή σκαναρίσματος προσώπου για καταγραφή ψηφοφόρων. Η κυβέρνηση με αυτό το πρόγραμμα ήταν σε θέση να αποτρέψει τις πολλαπλές ψήφους από τα ίδια άτομα, τα οποία ήθελαν να ψηφίζουν με πολλά διαφορετικά ονόματα.



➤ **Ατλάντικ Σίτυ, Νιου Τζέρσι, Λας Βέγκας**

Εφαρμογή σκαναρίσματος προσώπου για την ασφάλεια σε καζίνο. Η εταιρεία Biometrica, η οποία ασχολείται με βιομετρικές εφαρμογές έχει εγκαταστήσει συστήματα αναγνώρισης προσώπου σε περισσότερα από 70 καζίνο σε όλο τον κόσμο μεταξύ των οποίων είναι το Taj Mahal. Μάλιστα έχει στην κατοχή της μια βάση δεδομένων με άτομα που είναι επικίνδυνα για τα καζίνο. [13]

➤ **Ιλινόις**

Εφαρμογή σκαναρίσματος προσώπου στην άδεια οδήγησης. Η πολιτεία του Ιλινόις χρησιμοποιεί το σκανάρισμα του προσώπου για την αποφυγή χορήγησης άδειας οδήγησης στο ίδιο άτομο δύο φορές. [14]

➤ **Πενσυλβάνια**

Εφαρμογή σκαναρίσματος προσώπου για την τήρηση της δικαιοσύνης. Αναζητήσεις φωτογραφιών και βίντεο CCTN από τις σκηνές εγκλημάτων, κάνει η Αστυνομία της Πενσυλβάνιας μελετώντας προηγούμενες συλλήψεις. Με αυτό τον τρόπο έχει καταφέρει την επίλυση παλαιών και παγωμένων υποθέσεων. [15]

➤ **Κονέκτικατ**

Εφαρμογή σκαναρίσματος προσώπου από το Facebook. Η εφαρμογή αυτή σαρώνει τις φωτογραφίες που έχει ανεβάσει κάποιος πρόσφατα, συγκρίνει τα πρόσωπα με προηγούμενες αναρτήσεις και στη συνέχεια προσπαθεί να αντιστοιχίσει τα πρόσωπα προτείνοντας ονόματα από τους φίλους του ατόμου που ανέβασε τις φωτογραφίες. Όταν βρεθεί η αντιστοιχία ειδοποιεί το χρήστη για να επικυρώσει τα στοιχεία του ατόμου. [16]

➤ **Φλόριντα**

Εφαρμογή σκαναρίσματος προσώπου για την τήρηση της δικαιοσύνης. Στο Super Bowl η Αστυνομία της Tampa Bay χρησιμοποίησε λογισμικό Viisage για την αναγνώριση προσώπων πιθανών εγκληματιών και τρομοκρατών που συμμετείχαν σε μια τρομοκρατική επίθεση.

➤ **Γερμανία**

Εφαρμογή σκαναρίσματος προσώπου για ασφάλεια πολιτών και αεροδρομίων. Η Γερμανική Αστυνομία χρησιμοποιεί ένα βιομετρικό σύστημα αναγνώρισης προσώπου στους συνοριακούς ελέγχους του διεθνούς αεροδρομίου Frankfurt Rhein-Main. [17]

➤ **Αυστραλία**

Εφαρμογή σκαναρίσματος προσώπου για τελωνεία και ασφάλεια συνόρων. Η τελωνειακή Αστυνομία της Αυστραλίας χρησιμοποιεί ένα σύστημα επεξεργασίας των συνόρων με το όνομα SmartGate, το οποίο συγκρίνει την φωτογραφία του διαβατηρίου με μια βάση δεδομένων για να δει αν είναι ο νόμιμος ιδιοκτήτης. [18]

➤ **Βραζιλία**

Εφαρμογή σκαναρίσματος προσώπου από την Αστυνομία. Οι Αστυνομικοί θα εφοδιαστούν με γυαλιά, τα οποία θα σκανάρουν πρόσωπα και θα αναγνωρίζουν εάν πρόκειται για άτομα που έχουν εμπλακεί σε εγκληματικές ενέργειες. Τα γυαλιά αυτά θα έχουν τη δυνατότητα να σκανάρουν έως και 400 άτομα το δευτερόλεπτο σε απόσταση έως και 45 μέτρα. Συγκρίνοντας τα στοιχεία των ατόμων με μια βάση δεδομένων, όταν θα εντοπίζουν κάποιον ύποπτο, θα ανάβει ένα κόκκινο φως που θα ειδοποιεί τον αστυνομικό. [19]

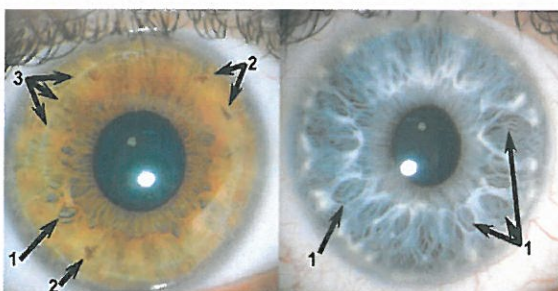
➤ **Ρωσία**

Εφαρμογή σκαναρίσματος προσώπου για Τραπεζικές συναλλαγές. Η μεγαλύτερη τράπεζα της Ρωσίας (Sberbank), έχει εγκαταστήσει στα ATMs ένα πρόγραμμα σκαναρίσματος προσώπου, με το οποίο οι άνθρωποι μπορούν να κάνουν αίτηση για πιστωτική κάρτα. Τα ATMs αυτά έχουν την δυνατότητα σκαναρίσματος του διαβατηρίου, αναγνώριση φωνής, καταγραφής αποτυπωμάτων αλλά μπορούν να τραβήξουν και 3D φωτογραφίες. [20]

➤ **Ελλάδα**

Εφαρμογή σκαναρίσματος προσώπου για Τραπεζικές συναλλαγές. Πλέον οι Ελληνικές Τράπεζες χρησιμοποιούν κατά την είσοδο των πελατών τους την αναγνώριση προσώπου, η οποία γίνεται στα ειδικά κουβούκλια που υπάρχουν στις πόρτες των Τραπεζών. Οι Τράπεζες καταγράφουν τα πρόσωπα των πελατών και τα αποθηκεύουν σε μια βάση δεδομένων.

**Σκανάρισμα – Αναγνώριση Ίριδας**



➤ **Η.Π.Α. και Πολιτείες Φλόριντα & Πενσυλβάνια**

Εφαρμογή Αναγνώρισης Ίριδας για την ασφάλεια και αποφυλάκιση των φυλακισμένων. Στις φυλακές της Νέας Υόρκης, της Φλόριντας και της Πενσυλβάνιας χρησιμοποιείται το σκανάρισμα της ίριδας για την αποφυλάκιση των κρατουμένων. Σκοπός είναι η ταυτοποίηση των ατόμων προκειμένου να μην γίνει κάποιο λάθος και αποφυλακιστεί κάποιος λάθος κρατούμενος. Σε κάποια άλλα ιδρύματα χρησιμοποιείται η ίδια τεχνολογία για την ρύθμιση και ταυτοποίηση των επισκεπτών.



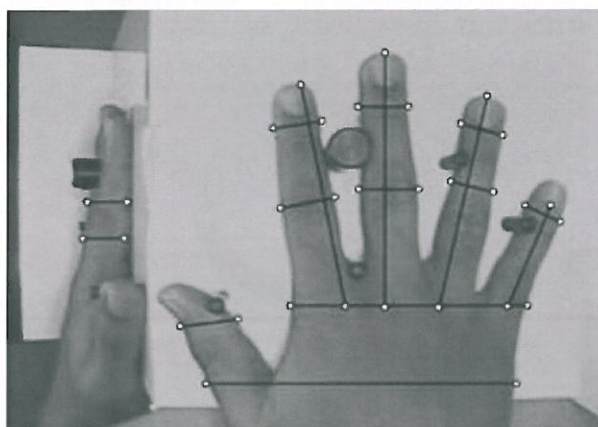
➤ **Αγγλία, Ιαπωνία, Γερμανία**

Εφαρμογή Αναγνώρισης Ίριδας σε δανειοδοτικούς οργανισμούς και τράπεζες. Η τεχνολογία σκαναρίσματος της ίριδας έχει χρησιμοποιηθεί αρκετές φορές σε ATMs τραπεζών. Ένας δανειοληπτικός οργανισμός με το όνομα Nationwide Building Society, το 1997 στην Αγγλία, έδωσε την επιλογή στους πελάτες του να έχουν πρόσβαση στα μηχανήματα ATMs με το σκανάρισμα της ίριδας του και όχι με τα κλασικά Pins. Η ανταπόκριση έφτασε το 94% των πελατών του. Εφαρμογή Αναγνώρισης Ίριδας έχουμε επίσης και σε αεροδρόμια όπως αυτό της Βόρειας Καρολίνας και της Φρανκφούρτης, τα οποία χρησιμοποιούν το σύστημα αυτό στην κίνηση των υπαλλήλων σε ευαίσθητες περιοχές. Το αεροδρόμιο του Λονδίνου χρησιμοποιεί το σύστημα αυτό για την εξυπηρέτηση των συχνών του πελατών, διευκολύνοντάς τους με το να αποφεύγουν τις ουρές αναμονής. Το ίδιο πρόγραμμα υλοποιεί και το αεροδρόμιο του Καναδά. [21]

➤ **Μεξικό**

Εφαρμογή Αναγνώρισης Ίριδας για την έκδοση ταυτότητας. Το Μεξικό χρησιμοποιεί το βιομετρικό σύστημα αναγνώρισης ίριδας για την έκδοση ταυτοτήτων.

**Σκανάρισμα – Αναγνώριση Χεριού**



➤ **Η.Π.Α. και Ισραήλ**

Εφαρμογή Αναγνώρισης Χεριού σε υπηρεσίες μετανάστευσης και αεροδρόμια. Το σύστημα αυτό ελέγχει το σχήμα του χεριού ή των δαχτύλων. Ο χρήστης τοποθετεί το χέρι του επάνω σε μια πλάκα, το ευθυγραμμίζει με πέντε οδηγούς και το σύστημα το φωτογραφίζει εξετάζοντας το τρισδιάστατο σχήμα της παλάμης, το μήκος και πλάτος των δαχτύλων. Η εφαρμογή αυτή χρησιμοποιείται από την Υπηρεσία Μετανάστευσης και Πολιτογράφησης (Immigration Naturalization Service) των ΗΠΑ. Οι συχνοί ταξιδιώτες έχουν αρχειοθετηθεί από την Υπηρεσία και επισπεύδουν τη διέλευσή τους από τον χώρο του τελωνείου. [22]

**Το πρόγραμμα AFIS (Σύστημα Αναγνώρισης Δαχτυλικών Αποτυπωμάτων χεριού)**

Το AFIS αποτελεί την πιο διαδεδομένη εφαρμογή βιομετρικής τεχνολογίας που αναπτύχθηκε προς τα τέλη της δεκαετίας του '70, με σκοπό την αυτοματοποίηση των ερευνών πάνω σε δεκάδες εκατομμύρια αποτυπώματα από μελάνι, που βρίσκονταν στα αρχεία του FBI. Πιο αναλυτικά η τεχνολογία AFIS έχει εφαρμογή στη λήψη αποτυπωμάτων, τόσο από συλληφθέντες υπόπτους για την εξακρίβωση της ταυτότητάς τους, όσο και από αποδέκτες παροχών για την αποφυγή διπλών εγγραφών, αλλά και από επαγγελματίες οικονομικών υπηρεσιών που ελέγχεται το ιστορικό τους. Τέλος χρησιμοποιείται και όταν ανακαλύπτονται αποτυπώματα στον τόπο ενός εγκλήματος. [23]

➤ **Ελλάδα**

Εφαρμογή προγράμματος AFIS στην Ελληνική Αστυνομία (Α.Σ.Α.Δ.Α.). τέθηκε σε λειτουργία στις 16 Ιανουαρίου 1996.

➤ **Δημοκρατία των Φιλιππίνων**

Εφαρμογή προγράμματος AFIS (Σύστημα Αναγνώρισης Δαχτυλικών Αποτυπωμάτων) σε κάρτες Κοινωνικής Ασφάλισης

Οι κάρτες αυτές προσφέρουν λειτουργικότητα 1:1 αλλά και 1:N και έχουν σχεδιαστεί με σκοπό την αποτροπή της απάτης και τη διευκόλυνση της ασφαλούς διανομής δημόσιων αγαθών στους νόμιμους κατόχους. [24]

➤ **Η.Π.Α.**

Εφαρμογή προγράμματος AFIS (Σύστημα Αναγνώρισης Δαχτυλικών Αποτυπωμάτων) για Κοινωνικές Παροχές.

Η εφαρμογή του προγράμματος έγινε με σκοπό την απάλειψη των διπλοεγγεγραμμένων για τις κοινωνικές παροχές και την αποτροπή της απάτης κατά τη λήψη των επιδομάτων οικογενειακής βοήθειας και τη διανομή του συσσιτίου. Άλλες εφαρμογές που χρησιμοποίησαν του πρόγραμμα στις Η.Π.Α. ήταν:

- το Arizona Fingerprint Imaging Program (AFIP)
- το Texas' s Lone Star Image System (LSIS)
- το Automated Fingerprint Image Reporting and Match (AFIRM)
- το New York State' s Public Assistance

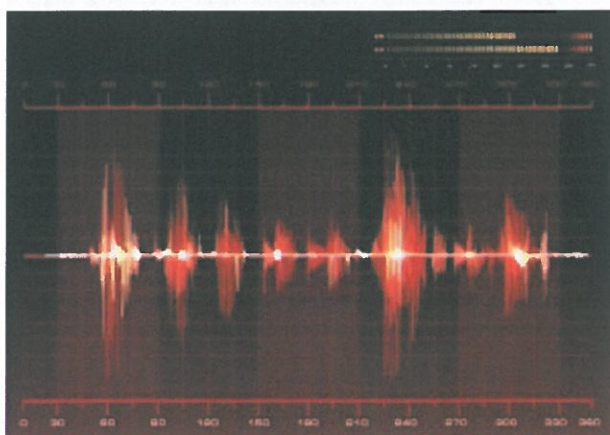
➤ **F.B.I.**

Εφαρμογή του AFIS από τις Αστυνομικές Αρχές του F.B.I. Το F.B.I. μεταβαίνει από τη χρήση του AFIS στη χρήση του AFIT (Advanced Fingerprint Information Technology). Το νέο αυτό πρόγραμμα εκτός από την αναγνώριση δαχτυλικών αποτυπωμάτων έχει και αναγνώριση παλάμης και ίριδας. Το επόμενο βήμα τους είναι το NGI (Next Generation Identification System), το οποίο αυξάνει την ταχύτητα αλλά και την ακρίβεια στην εύρεση πληροφοριών. Αυτό σημαίνει ότι ενώ το AFI είχε



χρόνο εύρεσης των στοιχείων για τις ποινικές υποθέσεις 2 ώρες και για τις αστικές 24 ώρες, το NGI δεν θα ξεπερνά τα 10 για τις ποινικές υποθέσεις και τα 15 λεπτά για τις αστικές.

### **Σκανάρισμα - Αναγνώριση Φωνής**



#### **➤ Νέα Υόρκη**

Εφαρμογή σκαναρίσματος φωνής για σωφρονιστικούς λόγους αλλά και σε χρηματοοικονομικούς οργανισμούς.

Το New York City Department of Corrections (NY DOC) προμηθεύει τους παραβάτες με ένα pager, στον οποίο τους καλεί ανά τακτά χρονικά διαστήματα μετά την ώρα της απαγόρευσης. Το κάθε άτομο πρέπει να τηλεφωνεί από συγκεκριμένο χώρο και σε συγκεκριμένο χρονικό διάστημα την υπηρεσία και έτσι με την αναγνώριση φωνής και κλήσης διαπιστώνεται εάν βρίσκεται στον επιτρεπτό χώρο.

Τέθηκε σε λειτουργία ένα σύστημα αναγνώρισης φωνής, το οποίο επιτρέπει ασφαλείς συναλλαγές μέσω τηλεφώνου. Το σύστημα αυτό αναπτύχθηκε από την Keyware με την βοήθεια της Voxtron, που είναι μια τηλεφωνική εταιρεία. Η Allied Irish Bank χρησιμοποιεί μια τέτοια υπηρεσία τεχνολογίας SpeakerKey της Buytel. [25]

#### **➤ Αυστραλία**

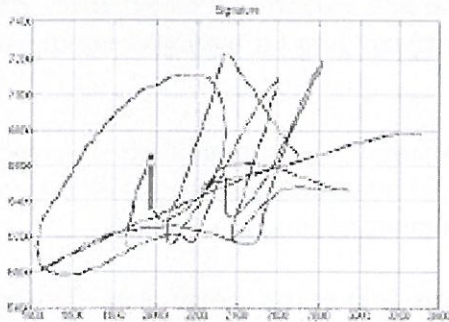
Και στην Αυστραλία στον χρηματοοικονομικό χώρο, γίνεται χρήση του συστήματος αναγνώρισης φωνής, κατά την οποία η Timemac Solutions χάρη σε αυτή την τεχνολογία επιτρέπει την τηλεφωνική διακίνηση μετοχών. Επίσης η National Australia Bank είναι η πρώτη τράπεζα στην Αυστραλία που χρησιμοποιεί τα βιομετρικά χαρακτηριστικά αντί για Pins. Η μέθοδος σκαναρίσματος φωνής είναι διαθέσιμη σε 3,3 εκατομμύρια ιδιώτες πελάτες του τραπεζικού ομίλου.

#### **➤ Ρωσία**

Εφαρμογή σκαναρίσματος φωνής σε χρηματοοικονομικούς οργανισμούς, όπως είναι η μεγαλύτερη τράπεζα της Ρωσίας (Sberbank), η οποία έχει εγκαταστήσει στα ATMs ένα πρόγραμμα αναγνώρισης φωνής, με το οποίο οι άνθρωποι μπορούν να κάνουν αίτηση για πιστωτική κάρτα. Τα ATMs αυτά έχουν την δυνατότητα σκαναρίσματος

του διαβατηρίου, καταγραφής αποτυπωμάτων αλλά μπορούν να τραβήξουν και 3D φωτογραφίες.

### **Ηλεκτρονική υπογραφή**



#### ➤ **Ελλάδα**

Εφαρμογή της ηλεκτρονικής υπογραφής για έκδοση της κάρτας του πολίτη. Η κάρτα αυτή θα αντικαταστήσει την παλιά αστυνομική ταυτότητα και θα είναι βιομετρικού τύπου, δηλαδή θα περιλαμβάνει μικροσίπ, ψηφιακή φωτογραφία, δύο δαχτυλικά αποτυπώματα, ηλεκτρονική υπογραφή και πολλές άλλες προσωπικές πληροφορίες του κατόχου της. [26]

#### ➤ **Η.Π.Α.**

Εφαρμογή ηλεκτρονικής υπογραφής για την έκδοση διαβατηρίων. Τα νέα διαβατήρια των Η.Π.Α. περιλαμβάνουν ένα ενσωματωμένο μικροκύκλωμα, φωτογραφίες των κατόχων τους και ψηφιακή υπογραφή.

#### ➤ **Γερμανία**

Εφαρμογή ηλεκτρονικής υπογραφής για ασφαλή τηλεφωνία μέσω διαδικτύου. Ερευνητές του Πανεπιστημίου Φραουνχόφερ ανέπτυξαν μια ψηφιακή υπογραφή για την διαδικτυακή τηλεφωνία που επιτρέπει την αρχειοθέτηση των τηλεφωνικών κλήσεων με τρόπο νομικά δευμεντικό. Άρα είναι πια δυνατό να κλείνονται συμφωνίες και μέσω τηλεφώνου. [27]



## Διοίκηση Ανθρώπινων Πόρων (ΔΑΠ)

### Εισαγωγή

Κρίνεται σημαντικό να αναφερθεί η έννοια της Διοίκησης Ανθρώπινων Πόρων (ΔΑΠ), καθώς και να εντοπιστούν συχνά ζητήματα που καλείται να διαχειριστεί, στα οποία το Βιομετρικό Σύστημα Αναγνώρισης Προτύπων που θα αναλυθεί παρακάτω μπορεί να συνδράμει τα μέγιστα.

Άλλωστε για να μπορέσει ένας σύγχρονος οργανισμός να παρουσιάσει ανάπτυξη πρέπει να στηριχθεί στην σταθερότητα και την βέλτιστη απόδοση του Ανθρώπινου Δυναμικού του, χωρίς όμως να εξαντλεί του υπόλοιπους πόρους του.

Η φιλοσοφία αυτή αποτυπώνεται καλύτερα στα παρακάτω λόγια των Edward Lawler και Arie De Geus.

*«Για να είσαι ανταγωνιστικός θα πρέπει να διαθέτεις εξειδικευμένο ανθρώπινο δυναμικό. Θα πρέπει να έχεις ένα σχετικά σταθερό εργατικό δυναμικό αφού η "διαρροή" εργαζομένων δρα αρνητικά στον συντονισμό και στην οργάνωση που οδηγούν στην γρήγορη ανταπόκριση και στην υψηλή ποιότητα των αγαθών και των υπηρεσιών».*  
-Edward Lawler

*«Οι εταιρείες πεθαίνουν επειδή τα στελέχη τους εστιάζουν την προσοχή τους στην οικονομική δραστηριότητα της παραγωγής προϊόντος και υπηρεσιών και ξεχνούν πως η αληθινή φύση των οργανισμών τους είναι αυτή της ανθρώπινης κοινότητας».*  
-Arie De Geus

### Ορισμός

Η Διοίκηση Ανθρώπινων Πόρων (ΔΑΠ) ή Διοίκηση Προσωπικού (ΔΠ) περιλαμβάνει την προσέλκυση, επιλογή, ανάπτυξη, αξιοποίηση & προσαρμογή των ανθρώπινων πόρων στον εργασιακό χώρο με σκοπό την αύξηση της εργασιακής τους ικανοποίησης και της αποτελεσματικότητας των επιχειρήσεων.

Η Διοίκηση των Ανθρώπινων Πόρων αποτελεί μια σημαντική επιχειρησιακή λειτουργία, αφού οι άνθρωποι αποτελούν τον πιο σημαντικό και κρίσιμο παράγοντα επιτυχίας κάθε οργανωμένης ανθρώπινης δραστηριότητας. Η λειτουργία αυτή ανατίθεται πλέον σε εξειδικευμένα στελέχη με σχετικές σπουδές και εμπειρίες.

Σχεδόν σε όλες τις μεγάλες επιχειρήσεις (ή τους οργανισμούς) υπάρχει ξεχωριστό τμήμα ή διεύθυνση που έχει την ευθύνη της Διοίκησης των Ανθρώπινων Πόρων. Ο ρόλος του τμήματος ή της Διεύθυνσης είναι να σχεδιάζει τις πολιτικές και τα συστήματα της Διοίκησης Ανθρώπινων Πόρων καθώς και να εκτελεί κάποιες συγκεκριμένες λειτουργίες.

Όμως, σε επιμέρους λειτουργίες, όπως η αξιολόγηση, η εκπαίδευση, οι προσλήψεις, οι προαγωγές συμμετέχουν όλοι οι προϊστάμενοι της επιχείρησης (ή του οργανισμού).

Για παράδειγμα, το Τμήμα Διοίκησης Ανθρώπινων Πόρων σχεδιάζει το σύστημα αξιολόγησης του προσωπικού και υποστηρίζει τη διαδικασία αξιολόγησης, όμως η αξιολόγηση κάθε εργαζόμενου γίνεται κυρίως από τον άμεσο προϊστάμενο με το σύστημα και τη διαδικασία που προβλέπεται.

### **Διοίκηση Απόδοσης**

Ένας σημαντικός παράγοντας που σχετίζεται με τη μακροχρόνια επιτυχία ενός οργανισμού είναι η ικανότητά του να εκτιμά πόσο καλά αποδίδουν οι εργαζόμενοι σε αυτόν και στη συνέχεια να χρησιμοποιεί τις πληροφορίες αυτές για να εξασφαλίσει ότι η εκτέλεση των εργασιών συμφωνεί με τα σύγχρονα πρότυπα και βελτιώνεται με την πάροδο του χρόνου.

Αυτός ο στόχος επιτυγχάνεται με την αξιολόγηση, την εποπτεία, τον συντονισμό και την εκπαίδευση του προσωπικού.

Η παραπάνω προσπάθεια ενισχύεται με την ορθή χρήση συστήματος αμοιβών και παροχών και ολοκληρώνεται με την χρήση των τεχνολογικών μέσων.

Σύμφωνα με τους Kessler και Purcell, τόσο η αξιολόγηση, όσο και η εκπαίδευση εργαζομένων είναι αρκετά πολύπλοκες και ακριβές, από άποψη πόρων, απαιτούν διαδικασίες και συναντούν πολλές δυσκολίες κατά την εφαρμογή τους, ενώ ακόμη και σήμερα, εφαρμόζονται ανεπαρκώς από αρκετές επιχειρήσεις.

Οι κυριότερες λειτουργίες της Διοίκησης Ανθρώπινων Πόρων (ΔΑΠ) είναι οι εξής:

- Προγραμματισμός Ανθρώπινου Δυναμικού
- Προσέλκυση
- Επιλογή
- Αξιολόγηση Εργαζομένων
- Διοίκηση Απόδοσης

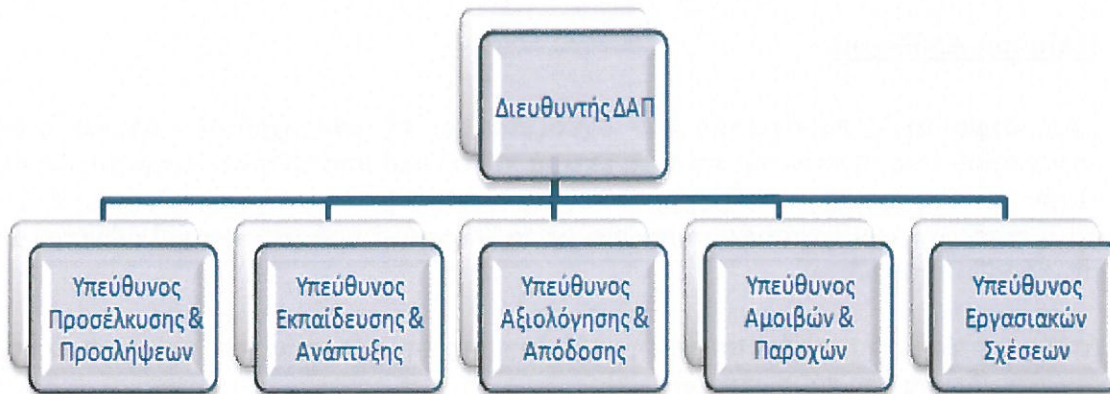
**Στόχοι της Διοίκησης Ανθρώπινων Πόρων (ΔΑΠ)**

- Διαρκής Ανταγωνιστικότητα
- Βελτίωση Ποιότητας και Παραγωγικότητας
- Τήρηση Νομικών και Κοινωνικών Υποχρεώσεων
- Εργασιακή Ικανοποίηση και Ανάπτυξη Προσωπικού
- Επίτευξη Επιχειρησιακών Στόχων
- Διατήρηση αξιοκρατικού περιβάλλοντος



### Οργάνωση της Διοίκησης Ανθρώπινων Πόρων (ΔΑΠ)

#### Δομή Τμήματος Διοίκησης Ανθρώπινων Πόρων (ΔΑΠ) σε Μεγάλη Επιχείρηση



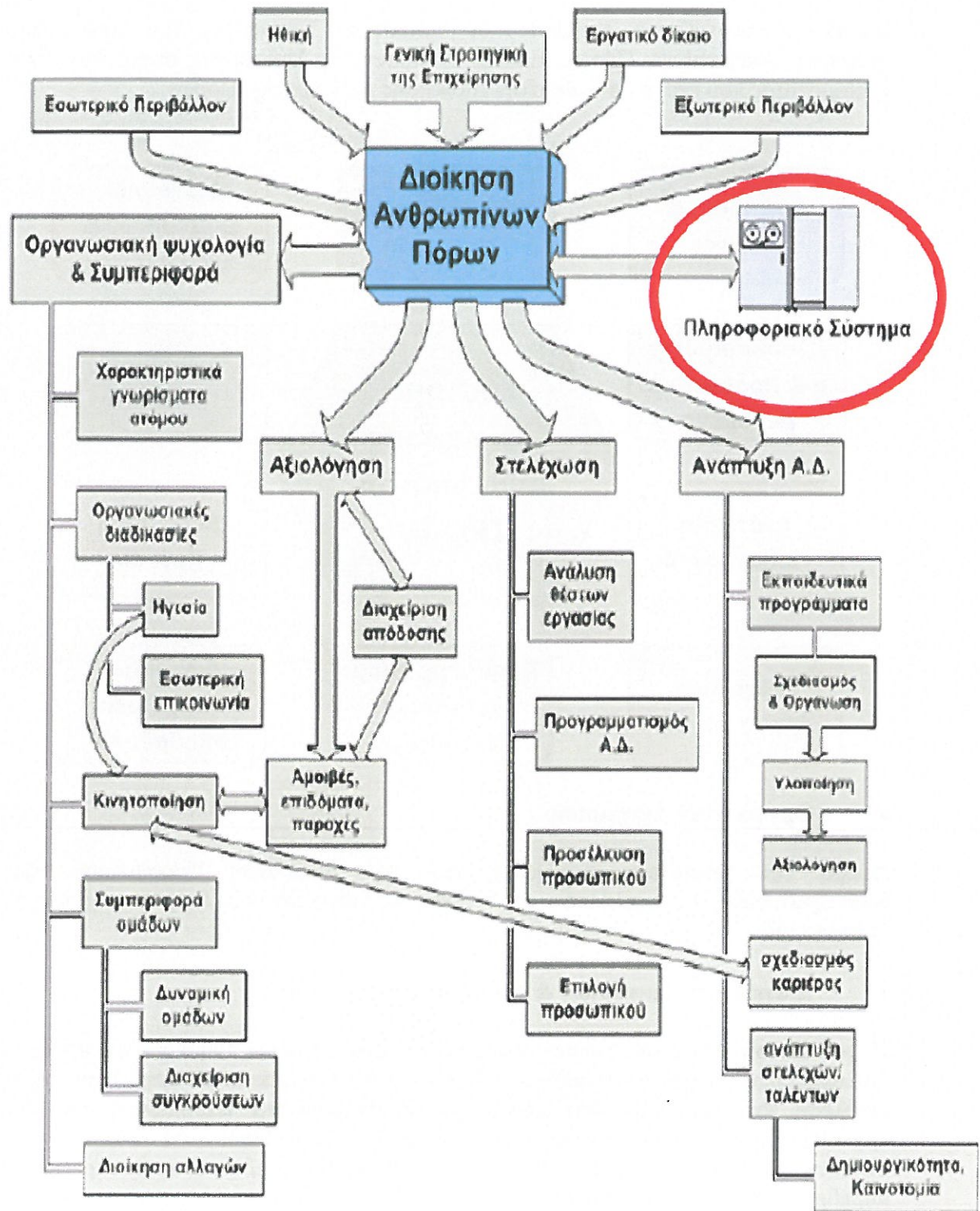
#### Πληροφοριακά Συστήματα στη Διοίκηση Ανθρώπινων Πόρων (ΔΑΠ)

- **Πληροφοριακό Σύστημα (Διοίκησης) Ανθρώπινων Πόρων (Human Resource Information System – HRIS)** ή Σύστημα Διαχείρισης Ανθρώπινου Δυναμικού είναι ένα περιεκτικό σύστημα που συγκροτεί όλες τις λειτουργίες, τις διαδικασίες και τα δεδομένα της Διοίκησης Ανθρώπινων Πόρων και παράγει όλες τις πληροφορίες σχετικές με Ανθρώπινους Πόρους που χρειάζονται όλα τα επίπεδα διοίκησης της επιχείρησης.

Το Πληροφοριακό Σύστημα (Διοίκησης) Ανθρώπινων Πόρων (Human Resource Information System – HRIS) ή Σύστημα Διαχείρισης Ανθρώπινου Δυναμικού μπορεί να συνεργάζεται με επιμέρους συστήματα για την επίτευξη των σκοπών του, όπως συστήματα εποπτείας και ασφάλειας.

#### - Αναγκαιότητα

- Η εκπλήρωση των λειτουργιών της Διοίκησης Ανθρώπινων Πόρων γίνεται αποδοτικότερα και σαφώς ταχύτερα και διευκολύνεται ο συνδυασμός των διαφόρων στοιχείων για τη λήψη αποφάσεων, τα στατιστικά στοιχεία, την αξιολόγηση της απόδοσης και τον έλεγχο ικανοποίησης των στόχων της επιχείρησης.





Ανάλυση Συστήματος Διοίκησης Ανθρώπινων Πόρων από την πλευρά της Διεύθυνσης & Οργάνωσης Ανθρώπινων Πόρων

Παρακάτω συνοψίζονται σχηματικά οι βασικότερες λειτουργίες του Συστήματος Διοίκησης Ανθρώπινων Πόρων. Επίσης αναλύονται οι λειτουργίες αυτές βάσει την χρησιμότητάς που έχει η καθεμία στην Διοίκησης Ανθρώπινων Πόρων.



- **Οργανωτική Διαχείριση**

Αφορά την γενικότερη οργάνωση, από την Διεύθυνση Προσωπικού, των δραστηριοτήτων που εμπλέκεται το Ανθρώπινο Δυναμικό μίας Επιχείρησης ή ενός Οργανισμού.

- **Διαχείριση Σεμιναρίων & Εκδηλώσεων**

Η εκπαίδευση και οι εκδηλώσεις είναι ουσιαστικά εργαλεία ενημέρωσης, προόδου και ανάπτυξης σχέσεων μεταξύ του Ανθρώπινου Δυναμικού. Η οργάνωση και η εκτέλεσή τους παρ'όλα αυτά μπορεί να δυσκολέψει την καθημερινή ροή των εργασιών διότι χρειάζονται χρόνο, τον οποίο πρέπει να διαθέσουν και οι οργανωτές - συντονιστές αλλά και το προσωπικό, το οποίο θα εκπαιδευτεί ή θα πρέπει να παρεβρεθεί σε κάποια εκδήλωση.

- **Διαχείριση Ταξιδιών**

Τα ταξίδια και οι επισκέψεις των στελεχών και του προσωπικού της επιχείρησης μπορεί να έχουν χαρακτήρα εκπαιδευτικό, ενημερωτικό, επαγγελματικό, αναψυχής ή ακόμα και για την αντιμετώπιση κάποιου προβλήματος. Θεωρούνται απαραίτητο εργαλείο για την ανάπτυξη και παραγωγή μιας επιχείρησης.

- **Διαχείριση Χρόνου**

Ίσως το πιο σημαντικό ζήτημα που απασχολεί την διεύθυνση Ανθρώπινου Δυναμικού, μετά την σωστή επιλογή συνεργατών. Ένα ζήτημα μάλιστα με πολλές προεκτάσεις, όπως για παράδειγμα η σωστή κατανομή χρόνου μεταξύ βαρδιών, η αποφυγή σπατάλης χρόνου για διάφορους λόγους, η τήρηση προθεσμιών και πολλές άλλες.

- **Διαχείριση Αποζημίωσης – Μισθοδοσία**

Η διαδικασία υπολογισμού τόσο της μισθοδοσίας όσο και των εργοδοτικών εισφορών αλλά και των αποζημιώσεων μπορεί να γίνει πολύπλοκη καθώς αυξάνεται το πλήθος του Ανθρώπινου Δυναμικού. Λαμβάνονται υπόψιν παράμετροι όπως οι ώρες εργασίας, υπερωρίες, άδειες, δώρα & bonus, απουσίες και πολλά ακόμη που απαιτούν λεπτομερή καταγραφή και άψογη συνεργασία με την οικονομική διεύθυνση. Είναι συχνό φαινόμενο να γίνονται λάθη και παραλείψεις στη μέτρηση και μεταφορά από το ένα τμήμα στο άλλο προκαλώντας δυσλειτουργίες, αδικίες αλλά και πρόστιμα για την επιχείρηση.

- **Προγραμματισμός κόστους Προσωπικού**

Στη Διαχείριση Ανθρώπινου Δυναμικού εμφανίζονται φανερά και κρυφά – έμμεσα κόστη. Φανερό κόστος για παράδειγμα είναι η μισθοδοσία, ενώ κρυφό κόστος είναι οι υπερωρίες που προκύπτουν από κακή διαχείριση του καθημερινού υπολογισμένου χρόνου εργασίας. (π.χ. ένας υπάλληλος που λείπει από την θέση του περισσότερο από το συνηθισμένο γιατί παρατείνει το χρόνο διαλείμματος και έπειτα κάνει υπερωρία προκειμένου να τελειώσει τα εργασιακά του καθήκοντα).

- **Διαχείριση Εργαζομένων**

Η ψυχολογία των εργαζομένων σε μια επιχείρηση καθώς και η διαχείριση των ζητημάτων που αντιμετωπίζουν οι ίδιοι είναι λена εξίσου σοβαρό ζήτημα στη Διαχείριση Ανθρώπινου Δυναμικού. Πολλές φορές, για παράδειγμα, είναι δύσκολο να ενημερώσει η διεύθυνση της επιχείρησης κάποιον εργαζόμενο για ζητήματα όπως αυτά που έχουν αναφερθεί νωρίτερα, χωρίς αυτό να μοιάζει με προσβολή ή με επίπληξη. Η προσπάθεια ελέγχου και εποπτείας συγκρούεται συχνά με την έννοια της παρακίνησης.



- **Ανάπτυξη Προσωπικού**

Το φαινόμενο της έλλειψης προσωπικού σε συγκεκριμένες περιόδους – εποχές είναι κάτι που αντιμετωπίζουν συνήθως οι διευθυντές Ανθρώπινου Δυναμικού την τελευταία στιγμή γιατί δεν έχουν την πολυτέλεια να έχουν άμεσα διαθέσιμο το ιστορικό της παραγωγικής διαδικασίας αλλά και επειδή συχνά οι ενημέρωσή τους είναι ανεπαρκής.

- **Προσβασιμότητα & Προσωπικά Δεδομένα**

Ένα επιπλέον ζήτημα της Διαχείρισης Ανθρώπινου Δυναμικού αποτελεί ο περιορισμός της πρόσβασης σε συγκεκριμένα τμήματα της επιχείρησης καθώς και η διαχείριση προσωπικών δεδομένων από μη εξουσιοδοτημένα άτομα. Όσο μεγαλύτερος ο οργανισμός τόσο πιο δύσκολο να “απομονωθούν” τμήματα της επιχείρησης από μη αρμόδιους υπαλλήλους. Επιπλέον, στα πλαίσια της συναδελφικής αλληλεγγύης μπορεί να επιτρέπεται άτυπα η πρόσβαση σε αντίστοιχους χώρους (λογιστήριο, αρχείο, αποθήκη υλικών κλπ) σε άτομα μη εξουσιοδοτημένα από άτομα εξουσιοδοτημένα.

- **Ασφάλεια & Έλεγχος**

Τελευταίο αλλά εξίσου σημαντικό είναι το σύστημα της ασφάλειας στο χώρο εργασίας, ένα ζήτημα που απασχολεί όλα τα τμήματα ανθρώπινου δυναμικού όλων των επιχειρήσεων. Λέγοντας ασφάλεια νοείται μια μορφή διαχείρισης κινδύνου, που χρησιμοποιείται για να προστατεύσει από τον κίνδυνο. Ιδανικά, η ασφάλεια ορίζεται ως η δίκαιη μεταφορά του κινδύνου πιθανής απώλειας από μια οντότητα σε άλλη, σε αντάλλαγμα μιας λογικής αμοιβής.

Περιπτώσεις όπως κλοπή, διαταραχή της εργασίας, αφαίρεση λογισμικού, δολιοφρορά, έκτακτα περιστατικά, πυρκαγιές, κ.α., μπορούν να αποτελέσουν καταστροφικές απειλές για μια επιχείρηση.

### **Ανάλυση Συστήματος Διοίκησης Ανθρώπινων Πόρων με την χρήση Βιομετρικού Συστήματος**

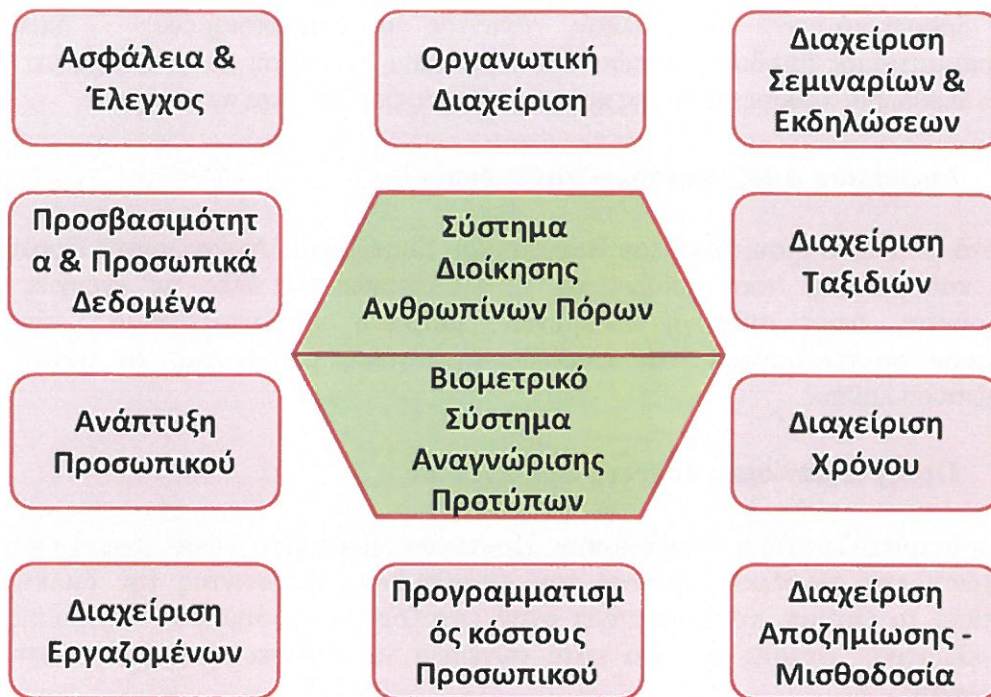
Λαμβάνοντας υπόψη τα ανωτέρω προτείνεται μια εύχρηστη και οικονομικά εφικτή λύση που συνδυάζει την τεχνολογία των βιομετρικών συστημάτων αναγνώρισης με την Διαχείριση των Ανθρώπινων Πόρων.

Πιο συγκεκριμένα η λύση που προτείνεται αφορά την μελέτη και τοποθέτηση ενός συστήματος, το οποίο διαχειρίζεται μέσω ενός λογισμικού προγράμματος, πληροφορίες που προέρχονται από μια βάση δεδομένων σχετικά με την ταυτότητα και το ιστορικό των χρηστών του.

Το σύστημα δίνει στο διαχειριστή την δυνατότητα να προσθέσει ή να αφαιρέσει μεγάλο αριθμό χρηστών, να εκχωρήσει ή να ανακαλέσει δικαιώματα και να ορίσει ζώνες προσβασιμότητας και χρόνους κίνησης των χρηστών.

Επιπλέον προσφέρει μια μεγάλη γκάμα δυνατοτήτων, όπως την έκδοση και τήρηση ιστορικού αλλά και την σύνδεση με άλλα τμήματα της επιχείρησης (π.χ. λογιστήριο).

Παρακάτω συνοψίζονται σχηματικά οι βασικότερες λειτουργίες που θα έχει το Βιομετρικό Σύστημα Αναγνώρισης όσον αφορά την Διοίκηση Ανθρώπινων Πόρων.



- **Οργανωτική Διαχείριση**

Με την χρήση του Βιομετρικού Συστήματος Αναγνώρισης Προτύπων, ενισχύεται το έργο της Οργανωτικής Διαχείρισης, προσφέροντας απαραίτητες αλλά και συνεχείς πληροφορίες μέσα από την βάση δεδομένων του.

- **Διαχείριση Σεμιναρίων & Εκδηλώσεων**

Το Βιομετρικό Σύστημα Αναγνώρισης Προτύπων που προτείνεται, επιλύει ζητήματα όπως η παρακολούθηση απουσιών, η τήρηση έναρξης και λήξης και η προσβασιμότητα επισκεπτών πέραν του σταθερού προσωπικού.

- **Διαχείριση Ταξιδιών**

Η συνδεσιμότητα του Βιομετρικού Συστήματος Αναγνώρισης Προτύπων, ακόμη και μέσω διαδικτύου μπορεί να αποτελέσει την επέκταση του τμήματος Διοίκησης Ανθρώπινου Δυναμικού και εκτός επιχείρησης. Ένα παράδειγμα εφαρμογής είναι ότι ο επιβλέπων – αρχηγός της αποστολής μπορεί με ειδικό κωδικό διαχειριστή να ενημερώνει εξ' αποστάσεως το σύστημα με δεδομένα και παραμέτρους χωρίς να διακόπτεται η συνεχής ροή εργασιών και η παραγωγικότητα.



- **Διαχείριση Χρόνου**

Το Βιομετρικό Σύστημα Αναγνώρισης Προτύπων, αφενός εξοικονομεί χρόνο μέσα από δραστηριότητες που πλέον γίνονται αυτοματοποιημένα, όπως ο προγραμματισμός βαρδιών, αδειών, διαλειμμάτων. Αφετέρου κάνει έλεγχο, με πολύ μικρά περιθώρια λάθους, τήρησης προγραμμάτων, βαρδιών και προθεσμιών.

- **Διαχείριση Αποζημίωσης – Μισθοδοσία**

Σε αυτό το στάδιο η συμβολή του Βιομετρικού Συστήματος Αναγνώρισης Προτύπων είναι καθοριστική, αφού μπορεί να χρησιμοποιηθεί σε όλες τις ενέργειες που απαιτούνται, όπως συλλογή δεδομένων, μέτρηση και υπολογισμός, εξαγωγή σύνθετων αποτελεσμάτων και επαλήθευση αυτών, μειώνοντας το ρίσκο του ανθρώπινου λάθους.

- **Προγραμματισμός κόστους Προσωπικού**

Το Βιομετρικό Σύστημα Αναγνώρισης Προτύπων, μπορεί να δώσει ενημέρωση και εκτύπωση της συνολικής εικόνας του εργαζομένου, βοηθώντας την διοίκηση να εντοπίσει το ζήτημα, να επισημάνει στον εργαζόμενο τη σημασία διόρθωσης της επαγγελματικής στάσης του και κατά συνέπεια να μειώσει τα κρυφά κόστη της επιχείρησης.

- **Διαχείριση Εργαζομένων**

Με την εξαγωγή στατιστικών και την εκτύπωση της εικόνας του εργαζομένου, από το Βιομετρικό Σύστημα Αναγνώρισης Προτύπων, σε διάφορους χρόνους (ημερήσια, εβδομαδιαία, μηνιαία κλπ βάση) ο ίδιος ο εργαζόμενος μπορεί να αξιολογήσει τον εαυτό του επαγγελματικά και να διορθώσει ή βελτιώσει την στάση του. Επιπλέον, η διοίκηση μπορεί να χρησιμοποιήσει το εργαλείο αυτό ως μέσο παρακίνησης και επιβράβευσης των τυπικών και αποδοτικών αποφεύγοντας συγκρούσεις και αρνητικό κλίμα και επιτυγχάνοντας υψηλότερη θετική ψυχολογία στην διαχείριση.

- **Ανάπτυξη Προσωπικού**

Το Βιομετρικό Σύστημα, προσφέρει ιστορικό ετών με συγκριτικά εργαλεία που βοηθούν στη βελτιστοποίηση της πρόβλεψης των αναγκών σε προσωπικό αλλά και την ανάπτυξή του μέσα από την δημιουργία μόνιμων θέσεων που προκύπτουν από την ανάλυση των δεδομένων, π.χ. εντοπίζεται μια θέση όπου συχνά καλύπτεται από πρόσωπα άλλου τμήματος όπως προκύπτει από την αναλυτική αναφορά του συστήματος. Ο διευθυντής προσωπικού με αυτό τον τρόπο μπορεί με τεκμηριωμένα στοιχεία να υποδείξει στην διεύθυνση την ανάγκη και να προτείνει την πρόσληψη νέου προσωπικού.

- **Προσβασιμότητα & Προσωπικά Δεδομένα**

Το Σύστημα, σχεδιάζεται, ρυθμίζεται και προσαρμόζεται στις ανάγκες της επιχείρησης για έλεγχο της προσβασιμότητας. Με την χρήση των βιομετρικών χαρακτηριστικών του προσωπικού, που έχουν προηγουμένως καταχωρηθεί στο λογισμικό του, όχι μόνον απαγορεύει την πρόσβαση σε μη εξουσιοδοτημένα άτομα αλλά εξαλείφει το πρόβλημα "δανεισμού" της κάρτας πρόσβασης. Επίπρόσθετα διατηρεί ιστορικό επισκέψεων που μπορεί να δώσει διαφωτιστικά στοιχεία σε περίπτωση παραβίασης των περιορισμένων ζωνών, πρόκλησης φθοράς κ.α.

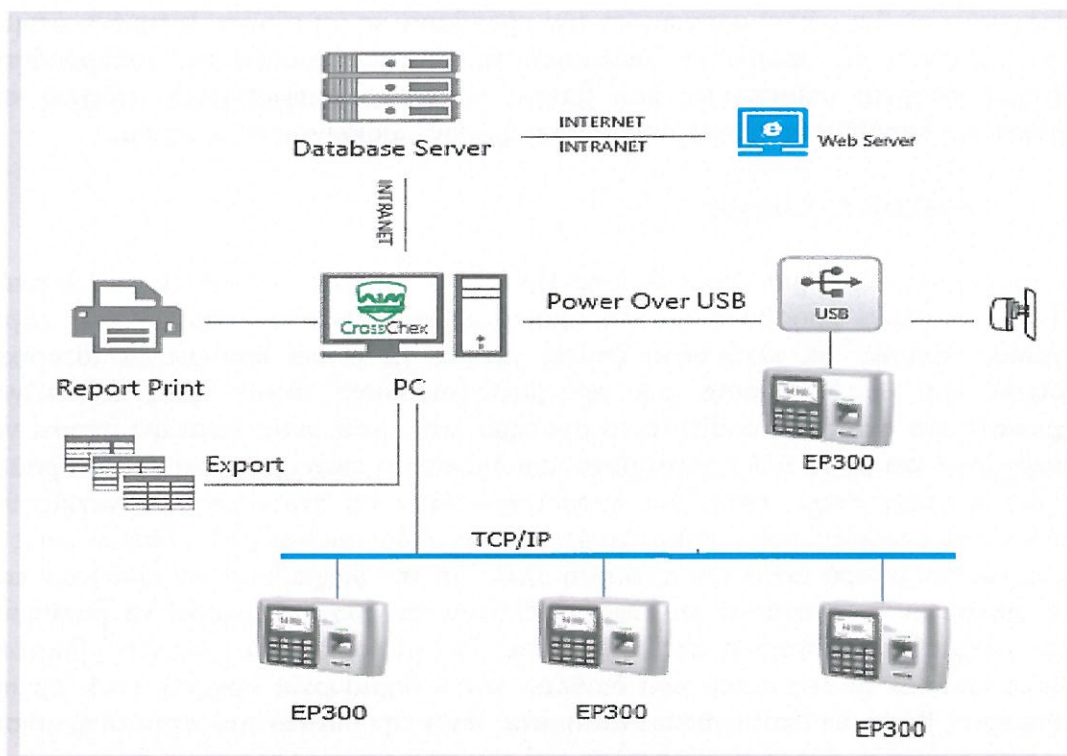
- **Ασφάλεια & Έλεγχος**

Το Βιομετρικό Σύστημα Αναγνώρισης Προτύπων, αρχικά λειτουργεί προληπτικά, αφού εξασφαλίζει πρόσβαση και παραμονή εξουσιοδοτημένων ατόμων στο χώρο εργασίας. Επίσης, σε περίπτωση ζημιάς μπορεί να δώσει απαραίτητα ιστορικά στοιχεία που θα βοηθήσουν μια πραγματογνωμοσύνη. Αυτό όμως που κάνει ξεχωριστό και σχεδόν απαραίτητο το σύστημα που προτείνεται είναι ότι μπορεί να συνεργαστεί και με τα άλλα συστήματα που διαθέτει η επιχείρηση και να συνδράμει σε μια κρίσιμη στιγμή, όπως για παράδειγμα όταν σε περίπτωση πυρκαγιάς θα μπορέσει να υποδείξει που βρισκονται άτομα προς διάσωση στο χώρο. Επειδή όμως η ασφάλεια δεν αφορά μόνο την πρόληψη αλλά και την διαχείριση των κινδύνων και των συνεπειών τους εφόσον και αφού επέλθουν, το σύστημα μπορεί να βοηθήσει στην συνέχιση των εργασιών της επιχείρησης. Πιο συγκεκριμένα η εξαγωγή βάσεων δεδομένων από το λογισμικό που διαθέτει και η δημιουργία αρχείων back up σε καθημερινή βάση, το οποίο γίνεται αυτόματα, δίνει την δυνατότητα στην επιχείρηση να λειτουργήσει σε ένα καινούριο χώρο από την επόμενη κιόλας ημέρα, διατηρώντας τις βάρδιες, τα οικονομικά αρχεία, τους φακέλους του προσωπικού και ότι άλλο κρίνεται απαραίτητο.



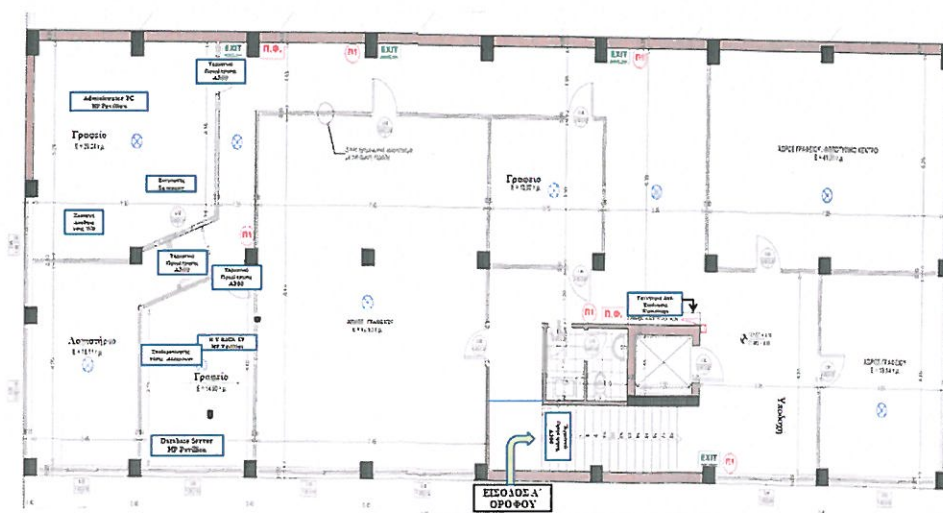
**Βασική συνδεσμολογία του Συστήματος**

Παρακάτω φαίνονται τα κύρια μέσα που θα χρησιμοποιηθούν για την εφαρμογή του Βιομετρικού Συστήματος Αναγνώρισης.



Πριν την εγκατάσταση όμως του Βιομετρικού Συστήματος θα πρέπει να προηγηθεί ο σχεδιασμός σύμφωνα με την κάτοψη της επιχείρησης όπου θα υποδεικνύονται τα σημεία πρόσβασης άρα και εγκατάστασης των συσκευών καθώς και η συνδεσιμότητα με τα απαραίτητα περιφερειακά.

Η κάτοψη της επιχείρησης για την τοποθέτηση του συστήματος θα έχει ως εξής:



**Υλικά Εγκατάστασης & Απαραίτητες Προδιαγραφές**

Για να λειτουργήσει το σύστημα θα χρειαστεί ένας κεντρικός υπολογιστής που θα αντλεί τα δεδομένα των υπαλλήλων από τη βάση δεδομένων. Οι συσκευές αναγνώρισης, που επίσης συνδέονται με τον κεντρικό υπολογιστή, τοποθετούνται στα σημεία πρόσβασης και σκανάρουν τα δαχτυλικά αποτυπώματα των χρηστών, τα οποία τα ταυτοποιούν με τα στοιχεία της βάσης και δίνεται η έγκριση ή η απόρριψη εισόδου. Ο διαχειριστής μπορεί να εκτυπώσει τις αναφορές ή να τις εξάγει σε ψηφιακή μορφή.

Για την λειτουργία, την εγκατάσταση και την τοποθέτηση του Συστήματος αυτού, απαιτούνται διάφορες συσκευές (όπως θα αναλυθούν παρακάτω), ορθή σύνδεση αυτών και προγραμματισμός.

Έγινε έρευνα αγοράς και επιλέχθηκαν συγκεκριμένα προϊόντα με γνώμονα την ποιότητα κατασκευής, την ευελιξία τους, την παροχή service και εγγύησης, την ευχρηστία, τον συνδυασμό διαφορετικών βιομετρικών χαρακτηριστικών και άλλων δεδομένων και την εφικτή τιμή.

Τα προϊόντα αυτά είναι:

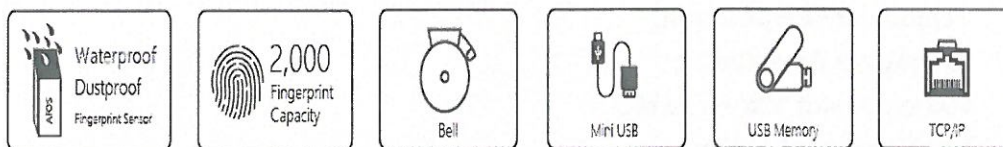
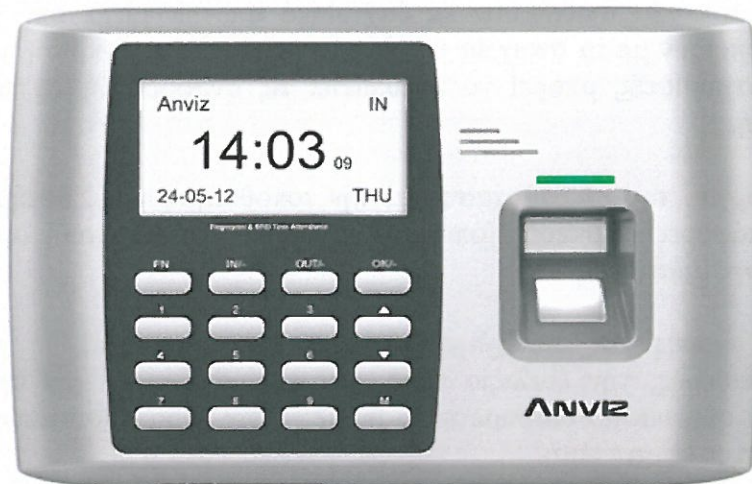
- Τερματικά Ωρομέτρησης
- Λογισμικό Διαχείρισης
- Ηλεκτρονικοί Υπολογιστές
- Σταθεροποιητής τάσης
- Εφεδρική Γεννήτρια
- Εκτυπωτής
- Συσκευές Αποθήκευσης

Παρακάτω θα αναλύσουμε την χρησιμότητα, τα χαρακτηριστικά των υλικών - εξοπλισμού εγκατάστασης και το κόστος αγορά τους.



➤ Τερματικά Ωρομέτρησης

Επιλέχθηκε μετά από έρευνα αγοράς το Βιομετρικό Σύστημα Αναγνώρισης Αποτυπωμάτων A300 της εταιρείας Anviz.



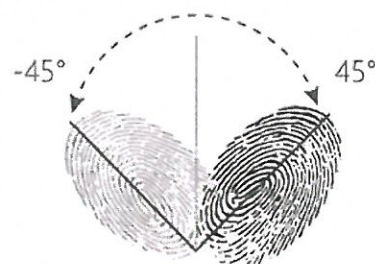
Οι λόγοι επιλογής είναι η σχέση τιμής και ποιότητας, η σύγχρονη τεχνολογία που εφαρμόζει, η πληθώρα επιλογών που προσφέρει καθώς και η συμβατότητά του με το λογισμικό πρόγραμμα.

Πιο συγκεκριμένα ο αισθητήρας δακτυλικών αποτυπωμάτων είναι αδιάβροχος, με προστασία από την σκόνη και τα γρατζουνίσματα. Το A300 προσφέρει μια ιδανική λύση διαχείρισης ανθρώπινου δυναμικού και ελέγχου πρόσβασης. Απόλυτος έλεγχος κινήσεων (είσοδος, έξοδος, διαλείμματα) εργαζομένων με χρήση του δακτυλικού αποτυπώματος ή με RFID κάρτας. Το κόστος του κυμαίνεται στα 200,00€ ανά τεμάχιο. Θα χρειαστεί η τοποθέτηση τεσσάρων τερματικών ωρομέτρησης άρα το κόστος θα διαμορφωθεί στα 800,00€.

Τα στοιχεία που καταχωρούνται στο σύστημα, μπορούν να αντληθούν ανά πάσα στιγμή από το λογισμικό που θα χρησιμοποιηθεί (όπως θα αναλυθεί παρακάτω).

Επιπλέον το A300 χρησιμοποιεί ένα κορυφαίο κρυπτογραφημένο αλγόριθμο δακτυλικών αποτυπωμάτων (BioNANO).

Ο αλγόριθμος της Anviz που καλείται BioNANO αυξάνει την γωνία αναγνώρισης Αποτυπώματος από  $\pm 15^{\circ}$  που ήταν προηγουμένως σε  $\pm 45^{\circ}$ .

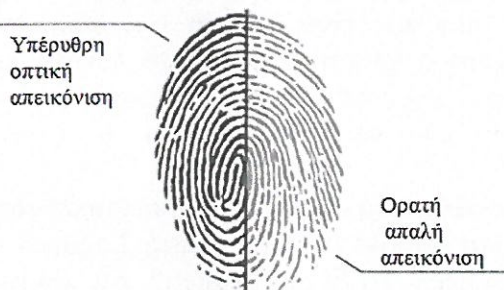


## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

Πρόκειται για αναβάθμιση της τάξεως του 300% σε σχέση με το προηγούμενο προϊόν.

Επίσης διπλασιάστηκε η ταχύτητα αναγνώρισης.

1. Αισθητήρας αποτυπωμάτων Οπτικού Κρυστάλλου  
σειράς ANVIZ AFOS



2. Θεραπεύει τις σπασμένες γραμμές της εικόνας  
(βάση αλγορίθμου ANVIZ)



3. Εξυπνη αναβάθμιση παλέτας αποτυπωμάτων



### ➤ Λογισμικό Διαχείρισης



Easy to Operate



Simple to Install



Expansion and Integration



Enhanced Security



Types of Reports



Auto Upgrade

Το λογισμικό που χρησιμοποιείται είναι το CrossChex. Τα στοιχεία που καταχωρούνται στα τερματικά ωρομέτρησης, μπορούν να αντληθούν ανά πάσα στιγμή από το λογισμικό ωρομέτρησης CrossChex, το οποίο μπορεί να βρίσκεται εγκατεστημένο σε ένα κεντρικό υπολογιστή ή περισσότερους. Το λογισμικό φροντίζει για την καταγραφή του προσωπικού, την σωστή μεταφορά των δεδομένων και την καταχώρηση τους στο αρχείο κινήσεων. Η ανάγνωση των στοιχείων από τα τερματικά ωρομέτρησης γίνεται αυτόματα σε χρόνους που καθορίζονται από τον διαχειριστή του συστήματος. Τα πάντα μπορούν εύκολα να αποκτηθούν. Η Anviz



δίνει την δυνατότητα της δωρεάν εγκατάστασης του λογισμικού αυτού σε οποιονδήποτε ηλεκτρονικό υπολογιστή επιθυμεί ο χρήστης.

➤ **Ηλεκτρονικοί Υπολογιστές**

Θα χρειαστούν στο σύνολο τρεις ηλεκτρονικοί υπολογιστές με κοινά τεχνικά χαρακτηριστικά. Επειδή οι απαιτήσεις του προγράμματος δεν είναι πολύ υψηλές δεν χρειάζεται να επιλεγούν ακραίες κατηγορίες μηχανημάτων. Σε κάθε περίπτωση στην αγορά υπάρχει πλήθος επιλογών. Η λύση που προτείνεται είναι μία αξιόπιστη εταιρεία με καλή εγγύηση, σχετικά μέσο κόστος χρήσης και όσο το δυνατό πιο σύγχρονα χαρακτηριστικά (μνήμη, επεξεργαστής, χωρητικότητα) έτσι ώστε να είναι δυνατή η αναβάθμιση των υπολογιστών και να καθυστερήσει ο χρόνος αντικατάστασής τους.

Το σετ του υπολογιστή που προτείνεται αποτελείται από οθόνη 18,5'' (κατασκευαστή LG & μοντέλο 19M38A-B), πληκτρολόγιο και ποντίκι (κατασκευαστή Logitech & μοντέλο Wireless Combo MK220 και Logitech B170 αντίστοιχα) και φυσικά τερματικό (κατασκευαστή HP Pavillion & μοντέλο 510-P153ng).

Συνολικά το κόστος ανά υπολογιστή ανέρχεται στα 583,90€ (75,90€ η οθόνη, 18,90€ το πληκτρολόγιο, 9,10€ το ποντίκι και 480,00€ το τερματικό).

Τα βασικά χαρακτηριστικά των υπολογιστών είναι τα εξής:

**Κατασκευαστής:** Intel

**Οικογένεια:** Core i5

**Μοντέλο:** 6400T

**Συχνότητα:** 2,2 GHz

**Μνήμη RAM:** Μέγεθος 8 GB, Τύπος DDR4

**Σκληρός Δίσκος:** Τύπος HDD, Χωρητικότητα 1000 GB

**Κάρτα Γραφικών:** Intel, Μοντέλο HD Graphics 530

**Λειτουργικό:** No OS



✓ **Υπολογιστής αποθήκευσης δεδομένων (Database Server)**

Ο υπολογιστής αυτός θα χρησιμοποιηθεί αποκλειστικά για τη βάση δεδομένων των προσωπικών στοιχείων των υπαλλήλων. (π.χ. ονοματεπώνυμο, αποτύπωμα, κ.α.). Είναι σημαντικό να είναι ξεχωριστός από τον κεντρικό υπολογιστή διαχείρισης καθώς τα προσωπικά δεδομένα των υπαλλήλων δεν μπορούν βάση νομοθεσίας να εκτίθενται σε κίνδυνο επεξεργασίας από τρίτα πρόσωπα. Ουσιαστικά μετά την καταχώρηση των δεδομένων στον Database Server κανείς δεν έχει δυνατότητα επεξεργασίας, αντιγραφής, παραποίησης ή αλλαγής και βρίσκονται σε ασφαλές περιβάλλον. Μόνο το λογισμικό διαχείρισης CrossChex "συμβουλευτείται" τα δεδομένα χωρίς όμως να τα επεξεργάζεται.

- ✓ Κεντρικός υπολογιστής διαχείρισης συστήματος (Administrator PC)

Πρόκειται για τον υπολογιστή που αποτελεί το συνδετικό κρίκο όλου του συστήματος. Σε αυτόν εγκαθίσταται το λογισμικό διαχείρισης CrossChex που ελέγχει τη λειτουργία των βιομετρικών τερματικών ωρομέτρησης. Επίσης συνδέεται με τον Database Server για την ταυτοποίηση των στοιχείων. Τέλος, συνδέεται με τον υπόλοιπο υποστηρικτικό εξοπλισμό (π.χ. εκτυπωτή, UPS, κ.λ.π.). Τον έλεγχο και την εποπτεία του κεντρικού υπολογιστή έχει μόνο ο υπεύθυνος διαχειριστής του προγράμματος, ο οποίος μπορεί με τη σειρά του να εξουσιοδοτήσει κάποιον υπάλληλο για την καταχώρηση και αλλαγή δεδομένων όπως είναι οι βάρδιες. Μπορεί να συνδεθεί και με άλλα τμήματα της επιχείρησης, όπως το λογιστήριο, μέσω Ethernet ή Internet για τη μεταφορά αυτών των δεδομένων και την εξοικονόμηση του χρόνου και την αποφυγή λαθών.

- ✓ Εφεδρικός υπολογιστής διαχείρισης συστήματος (Back up Administrator PC)

Λειτουργεί παράλληλα με τον κεντρικό υπολογιστή διαχείρισης συστήματος ως καθρεπτικός υπολογιστής. Τα δεδομένα αποθηκεύονται σε πραγματικό χρόνο (real time) έτσι ώστε σε βλάβη του κεντρικού υπολογιστή να χρησιμοποιείται χωρίς καμία καθυστέρηση. Για λόγους ασφάλειας τοποθετείται σε άλλο χώρο από τον κεντρικό Η/Υ και έχει ακριβώς τις ίδιες τεχνικές προδιαγραφές με αυτόν, τόσο σε hardware όσο και σε software.

#### ➤ Σταθεροποιητής τάσης

Για την αδιάκοπη λειτουργία του συστήματος και την προστασία από συχνές διακοπές ρεύματος επιλέχθηκε να τοποθετηθούν τρεις σταθεροποιητές τάσεως, ένας δίπλα σε κάθε υπολογιστή. Μετά από έρευνα αγοράς προτείνεται το προϊόν Ups της εταιρείας *Accupower* με κωδικό μοντέλου **ISY 1200VA**. Τόσο η τιμή του (109,99€) όσο και τα τεχνικά χαρακτηριστικά του (αναφέρονται παρακάτω) το καθιστούν μια λογική λύση. Σε περίπτωση διακοπής ρεύματος εξασφαλίζει 30 με 40 λεπτά λειτουργίας.

<b>Μέγιστη Ισχύς (VA)</b>	1200VA
<b>Τύπος Λειτουργίας</b>	Line Interactive
<b>Αυτονομία Μπαταρίας</b>	30-40MIN (250W PC + MONITOR 15")
<b>Συνδέσεις</b>	3x Schuko, USB
<b>Εγγύηση</b>	2 έτη





➤ Εφεδρική Γεννήτρια

Προαιρετικά προτείνεται η χρήση μια γεννήτρια αυτόματης εκκίνησης σε διακοπή ρεύματος προκειμένου να συνεχίσει η λειτουργία του Βιομετρικού Συστήματος Αναγνώρισης ακόμη και μετά τα 30 λεπτά που προσφέρει το UPS. Αφενός αυξάνεται το κόστος της πρότασης κατά 1200,00€ αφετέρου όμως με την προσθήκη αυτή δημιουργείται ένα ολοκληρωμένο σύστημα με αυτονομία και υψηλή ασφάλεια. Το προϊόν που προτείνεται (κατασκευαστής Kumatsugen, μοντέλο GP 8000), αν και δεν αποτελεί την φθηνότερη επιλογή, έχει μηδαμινά κόστη συντήρησης και πολύ καλές κριτικές.

Ακολουθούν αναλυτικότερα τα χαρακτηριστικά της γεννήτριας.

**AVR**



Τεχνικά Χαρακτηριστικά

Μέγιστη απόδοση: 6 KVA

Τάση: 400/230 V

Ισχύς: 10.5 Hp

Κυβισμός: 418 cc

Κινητήρας: 4 χρονος αερόψυκτος

Καύσιμο: Diesel

Χωρητικότητα: 12.5 Lt

Χρόνος λειτουργίας: 6.5 h

Διαστάσεις: 79x52x74 cm

Βάρος: 113 kg

- Αυτόματη εκκίνηση σε διακοπή ρεύματος
- Σύστημα αυτόματης παύσης λειτουργίας όταν δεν υπάρχει λάδι στον κινητήρα OIL ALERT SYSTEM
- Εξάτμιση χαμηλού θορύβου
- Βολτόμετρο για παρακολούθηση της παραγόμενης ισχύος
- Διακόπτης ασφαλείας διακοπής κυκλώματος CFCI
- Μεγάλο ντεπόζιτο για αυτονομία
- Διαθέτει μίζα και συμπεριλαμβάνεται η μπαταρία
- 6,5 ώρες συνεχούς λειτουργίας με ένα ντεπόζιτο και κατανάλωση υπό πλήρες φορτίο
- Ιδανική για βιομηχανική χρήση, υψηλές απαιτήσεις και εφαρμογές
- Ρουλεμάν ακριβείας
- Ζεύγη χωρίς ψύκτρες που δεν χρειάζονται συντήρηση
- Λαστιχένιοι απορροφητήρες κραδασμών

➤ **Εκτύπωσης**

Για την εκτύπωση των αναφορών και ότι άλλο χρειαστεί μπορεί να χρησιμοποιηθεί υφιστάμενος εξοπλισμός της επιχείρησης. Παρ' όλα αυτά και για λόγους εμπιστευτικότητας και ασφάλειας προτείνεται η εγκατάσταση εκτυπωτή δίπλα στον κεντρικό υπολογιστή διαχείρισης ή σε χώρο που θα έχει πρόσβαση μόνο ο διαχειριστής του συστήματος. Καθώς δεν χρειάζονται ιδιαίτερες προδιαγραφές και με γνώμονα την χαμηλότερη τιμή συντήρησης συνίσταται ο ασπρόμαυρος εκτυπωτής της εταιρείας Samsung μοντέλο SL-M2825ND τεχνολογίας laser, με κόστος 125,00€, δυνατότητα διπλής όψης και ταχύτητα εκτύπωσης 28 σελίδες/λεπτό, ο οποίος αρκεί για την χρήση που προορίζεται. Είναι σημαντικό για την μεγιστοποίηση της ασφάλειας να προτιμηθεί προϊόν εκτύπωσης και όχι πολυμηχάνημα που προσφέρει την δυνατότητα φωτοτύπησης.

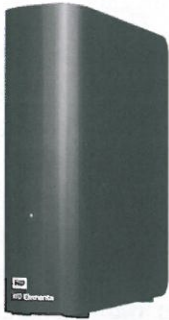


➤ **Συσκευές Αποθήκευσης**

Για τη δημιουργία εφεδρικού αρχείου Back up έχει χρησιμοποιηθεί ο Εφεδρικός υπολογιστής διαχείρισης συστήματος (Back up Administrator PC) που λειτουργεί καθρεπτικά στον κεντρικό υπολογιστή. Παρ' όλα αυτά πρέπει να προβλεφθεί η καθημερινή αρχειοθέτηση σε εφεδρικό εξωτερικό δίσκο που προστατεύει το εγχείρημα σε μεγάλο βαθμό αν τα κεντρικά γραφεία υποστούν μεγάλη ζημιά, κλοπή ή καταστροφή. Ο εξωτερικός δίσκος πρέπει να βρίσκεται στα χέρια του διαχειριστή, σε ασφαλές μέρος εκτός εταιρείας και να έχει μεγάλη χωρητικότητα και υψηλή ποιότητα υλικών. Για το λόγο αυτό προτείνεται ο εξωτερικός σκληρός δίσκος του κατασκευαστή Western Digital, μοντέλο Elements Desktop 4TB. Εκτός από τις μικρές διαστάσεις, τον τεράστιο αποθηκευτικό χώρο, με χωρητικότητα 4TB και την σύνδεση USB 3.0, παρέχεται με ειδική εργοστασιακή εγγύηση επιστροφής και αντικατάστασης από την μητρική εταιρεία. Η τιμή αγοράς είναι 169,90€.



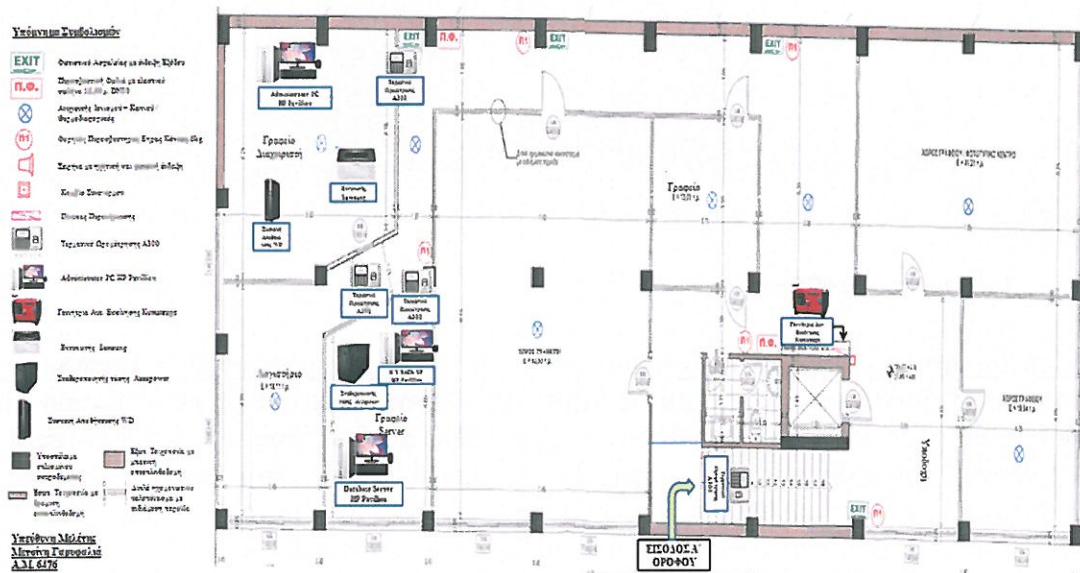
## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων



- Χωρητικότητα:4 TB
- Μέγεθος Δίσκου:3.5"
- Σύνδεση:USB 3.0

### Απεικόνιση της εγκατάστασης των μηχανημάτων και χρησιμότητα του καθενός στη συγκεκριμένη θέση.

Αφού επιλέχθηκαν ο κατάλληλος εξοπλισμός και τα μηχανήματα έχει φτάσει το στάδιο απεικόνισής τους στο χώρο της επιχείρησης.  
Η τελική μορφή της κάτοψης της επιχείρησης μετά την τοποθέτηση του συστήματος και του εξοπλισμού του θα έχει ως εξής:



(Δείτε την κάτοψη και σε μεγαλύτερη κλίμακα στο παράρτημα της Πτυχιακής Εργασίας.)

Τα μηχανήματα ωρομέτρησης τοποθετήθηκαν στην είσοδο τεσσάρων χώρων - γραφείων. Το κάθε ένα από αυτά έχει την δική του σημασία και χρήση. Τα υπόλοιπα μηχανήματα που αποτελούν τον εξοπλισμό για την λειτουργία όλου του Συστήματος Αναγνώρισης κατανεμήθηκαν στους χώρους της επιχείρησης αφού πρώτα έγινε έρευνα των χώρων, των αναγκών τους και της ασφάλειά τους.

✓ **Υπολογιστής αποθήκευσης δεδομένων (Database Server)**

Η χρήση του υπολογιστή αυτού είναι αποκλειστικά για τη βάση δεδομένων των προσωπικών στοιχείων των υπαλλήλων. Αυτόν τον υπολογιστή δεν μπορεί να τον χρησιμοποιήσει κανένας άλλος εκτός από τον διαχειριστή του Συστήματος, ο οποίος έχει την συγκεκριμένη εξουσιοδότηση. Για τον λόγο αυτό αναφέρεται και παρακάτω η τοποθετηθείσα στην είσοδο του γραφείου server ενός Μηχανήματος Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων, το οποίο θα αποτρέπει την είσοδο σε άτομα χωρίς την εξουσιοδότηση αυτή.

✓ **Κεντρικός υπολογιστής διαχείρισης συστήματος (Administrator PC)**

Ο συνδετικός κρίκος όλου του Συστήματος είναι ο Administrator PC. Ο υπολογιστής αυτός θα ελέγχει όλη την λειτουργία του Συστήματος Αναγνώρισης καθώς σε αυτόν είναι εγκατεστημένο και το λογισμικό διαχείρισης CrossChex. Θα βρίσκεται στο γραφείο του διαχειριστή όπου και θα χρησιμοποιεί τον Data server για την ταυτοποίηση των στοιχείων. Η είσοδος του γραφείου του διαχειριστή θα ελέγχεται και αυτή από ένα Μηχάνημα Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων.

✓ **Εφεδρικός υπολογιστής διαχείρισης συστήματος (Back up Administrator PC)**

Ο υπολογιστής αυτός θα βρίσκεται στον ίδιο χώρο με τον Database Server με σκοπό την απευθείας αποθήκευση των στοιχείων και των αρχείων που καταχωρούνται στον Database Server. Θα είναι σε θέση να αντικαταστήσει τον Database Server σε περίπτωση βλάβης.

✓ **Μηχάνημα Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων Κεντρικής Εισόδου/Εξόδου**

Η τοποθέτηση ενός Μηχανήματος Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων στην κεντρική είσοδο/έξοδο της επιχείρησης, που βρίσκεται στον πρώτο (Α΄) όροφο του κτιρίου, δίνει την δυνατότητα στην επιχείρηση να ελέγχει της είσοδο/έξοδο του προσωπικού και να περιορίζει, όταν το κρίνει απαραίτητο, την είσοδο σε μη εξουσιοδοτημένα άτομα.

✓ **Μηχάνημα Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων Εισόδου/Εξόδου Λογιστηρίου**

Η τοποθέτηση ενός Μηχανήματος Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων στην είσοδο του λογιστηρίου της επιχείρησης γίνεται με σκοπό να πραγματοποιείται έλεγχος των ατόμων που θέλουν να εισέλθουν στο λογιστήριο, να καταμετράται η ώρα παραμονής τους σε αυτό (π.χ. εάν είναι υπάλληλοι του λογιστηρίου να πιστώνονται οι ώρες της βάρδιάς τους ή αν είναι επισκέπτες να φαίνεται ο χρόνος παραμονής τους στο χώρο αυτό) και σε περίπτωση που κάποιο άτομο δεν έχει την άδεια εισόδου σε αυτό το χώρο να μην μπορεί να εισέλθει.



✓ **Μηχάνημα Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων Εισόδου/Εξόδου χώρου Administrator PC**

Η τοποθέτηση ενός Μηχανήματος Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων στην είσοδο του χώρου του Administrator PC της επιχείρησης γίνεται προκειμένου να μην μπορούν να εισέλθουν άτομα χωρίς την επιτρεπτή εξουσιοδότηση και κατ' επέκταση ο Administrator PC να μην είναι εκτεθειμένος σε κινδύνους παραβίασης, υποκλοπής ή παραποίησης αρχείων. Είναι ένας χώρος που λίγα άτομα της επιχείρησης έχουν εξουσιοδότηση εισόδου.

✓ **Μηχάνημα Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων Εισόδου/Εξόδου χώρου Database Server & Back up Server**

Η τοποθέτηση ενός Μηχανήματος Ωρομέτρησης και Αναγνώρισης Δαχτυλικών Αποτυπωμάτων στην είσοδο του χώρου των Database Server & Back up Server γίνεται για να περιορίζεται η άδεια εισόδου μόνο στα άτομα που έχουν αυτή την εξουσιοδότηση, όπως ακριβώς συμβαίνει και στην είσοδο του Administrator PC.

✓ **Γεννήτρια Αυτόματης Εκκίνησης**

Τοποθετείται μια γεννήτρια αυτόματης εκκίνησης δίπλα στον ηλεκτρολογικό πίνακα με σκοπό εάν γίνει κάποια διακοπή ρεύματος να ξεκινήσει απευθείας έτσι ώστε να μην υπάρξει κάποιο πρόβλημα στην ομαλή λειτουργία του Βιομετρικού Συστήματος Αναγνώρισης, των υπολογιστών που το στηρίζουν και γενικά όλου του εξοπλισμού του. Με αυτό τον τρόπο αποφεύγεται οποιαδήποτε καθυστέρηση του προσωπικού κατά την είσοδο ή έξοδό τους και επίσης η καταγραφή και παρακολούθηση των βαρδιών, των διαλειμμάτων, κ.α. είναι συνεχείς χωρίς κάποια διακοπή με αποτέλεσμα να υπάρχουν λάθη.

✓ **Σταθεροποιητής Τάσης**

Τοποθετείται ένας Σταθεροποιητής Τάσης στον χώρο που βρίσκεται ο Database Server & Back up Server με σκοπό να αποφευχθεί οποιοδήποτε πρόβλημα στην λειτουργία των υπολογιστών και κατεπέκταση όλου του Συστήματος κατά την εμφάνιση μιας πτώσης τάσης

✓ **Συσκευές Αποθήκευσης**

Θα τοποθετηθούν στο χώρο του Administrator PC αλλά θα λειτουργούν ως ένα ακόμη Back up για τον Database Server. Η δημιουργία περισσότερων αντιγράφων καθιστά πιο ασφαλή την χρήση τους γιατί σε περίπτωση μιας μεγάλης ζημιάς (π.χ. πυρκαγιάς) θα υπάρχουν ακόμη τα αρχεία και η λειτουργία της επιχείρησης θα μπορεί να συνεχιστεί χωρίς απώλειες. Οι συσκευές αυτές τοποθετούνται στον χώρο του Administrator PC όπου αν και μακριά από τον Database Server & τον Back up Server, υπάρχει και εκεί αυστηρός έλεγχος εισόδου και εξόδου, άρα μειώνονται κατά πολύ οι πιθανότητες υποκλοπής.

✓ **Εκτυπωτής**

Τοποθετείται στο χώρο του Administrator PC με σκοπό την εκτύπωση των καταστάσεων του προσωπικού. Η εκτύπωση σε αυτό το χώρο είναι ελεγχόμενη και έτσι δεν μπορεί ούτε εδώ να παρουσιαστούν τυχόν υποκλοπές.

**Εγγραφή στην πλατφόρμα Διαχείρισης του Λογισμικού.**

Μετά την εγκατάσταση και τοποθέτηση του παραπάνω εξοπλισμού, πρέπει να γίνει η εγγραφή από τον διαχειριστή του Βιομετρικού Συστήματος Αναγνώρισης, στην πλατφόρμα διαχείρισης του λογισμικού, συμπληρώνοντας τα παρακάτω στοιχεία και παραμέτρους και ακολουθώντας τα αναφερόμενα βήματα με σκοπό να επιτραπεί η ηλεκτρονική αποθήκευση του λογισμικού CrossChex.

➤ **Βήμα 1ο : Εγγραφή – Register**

Αρχικά πρέπει να συμπληρωθεί η καρτέλα του παρακάτω πίνακα για την εγγραφή στο σύστημα. Τα απαραίτητα στοιχεία είναι: σύνδεσμος επικοινωνίας, εταιρεία, χώρα και e-mail.

Software Guide

Register Database Department Staff Attendance Scheduling Device

Registrar Information \* Mandatory Field

\*Contact  Tel

\*Company  Website

\*Country  Address

\*Email

1.This is a free software, so please register at first in order to ensure a better service  
2.Our register information will be encrypted so it is safe to use.  
3.This is just used for technical service support provided by us.  
4.The information will be saved in localand it will be registered automatically when network connect.

Back Next Step



➤ **Βήμα 2ο : Βάση Δεδομένων – Database**

Σε αυτό το βήμα δηλώνεται στο πρόγραμμα τον υπερσύνδεσμο με την πηγή των δεδομένων. Υπάρχει η δυνατότητα δημιουργίας αρχείου Excel ή μπορεί να οριστεί ένας SQL Server. Προτείνεται το Excel καθώς είναι πιο εύκολο να συσχετιστεί με στοιχεία από άλλα τμήματα της επιχείρησης που δουλεύουν κυρίως το Microsoft Office.

Software Guide

Register Database Department Staff Attendance Scheduling Device

ACCESS

Access File: C:\Program Files (x86)\Anviz\CrossChex Standard\DB\CrossChex. View

SQL SERVER

Server IP: [ ]

User Name: sa

Password: [ ]

Database Name:  Select Database  Creat New Database

Database Mode: [ ] Start New

Back Next Step

➤ **Βήμα 3ο : Τμήμα – Department**

Σε αυτό τη βήμα μπορεί να κατηγοριοποιηθεί το προσωπικό σε ένα ή περισσότερα τμήματα. Αυτό θα βοηθήσει στον ευκολότερο προγραμματισμό κατά τη διαχείριση του προγράμματος. Η κατηγοριοποίηση δεν είναι οριστική, αφού ένα τμήμα μπορεί να προστεθεί, να τροποποιηθεί ή και να διαγραφεί ανά πάσα στιγμή από τον διαχειριστή του συστήματος. Σε περίπτωση διαγραφής του τμήματος το προσωπικό που είναι κάτω από αυτό μεταφέρεται στα κεντρικά.

The screenshot shows a software interface titled "Software Guide" with a progress bar at the top. The progress bar has seven steps: Register, Database, Department (highlighted), Staff, Attendance, Scheduling, and Device. Below the progress bar is the "Department List" management screen. It features a list box containing "TEI PATRAS". To the right of the list box are buttons for "Add", "Modify", "Del", "Save", and "Cancel". Below the list box, there are two input fields: "Selected Department:" with "TEI PATRAS" entered, and "New Department:" which is empty. At the bottom of the screen are "Back" and "Next Step" buttons. Two instructions are listed below the input fields: "1. When adding a new dept, it cannot repeat with the existing one" and "2. When deleting a dept, all staff under it will be transferred to head office".



➤ **Βήμα 4ο : Προσωπικό – Staff**

Σε αυτό το βήμα μπορούν να προστεθούν παράμετροι και πληροφορίες στο εισερχόμενο αρχείο προσωπικού. Με την ολοκλήρωσή του δημιουργείται μια Standard πλατφόρμα προσωπικού σύμφωνα με την δομή του συστήματος. Σε περίπτωση που δεν είναι απαραίτητο να προστεθεί κάποιο δεδομένο επιλέγεται η δημιουργία της Standard καρτέλας με τα ήδη υπάρχοντα στοιχεία.

Software Guide

Register Database Department **Staff** Attendance Scheduling Device

1. Please click the first button to get standard staff template
2. Please fill staff information in standard staff template
3. Click the second button and choose the finished staff information and then upload it to software
4. If you don't need to fill staff information now, you can click 'next step' and then add this in software

1. Get standard staff template

2. Upload finished staff information

Back Next Step

➤ **Βήμα 5ο : Παρουσία – Attendance**

Στο βήμα αυτό γίνεται η απαραίτητη παραμετροποίηση όσον αφορά τον χρόνο και τις μονάδες μέτρησης αυτού για να μπορέσει αργότερα το σύστημα να μοιράζει σε βάρδιες, εργάσιμες και αργίες το προσωπικό. Συμπληρώνονται δυο καρτέλες. Στη πρώτη καρτέλα ο διαχειριστής του προγράμματος θα πρέπει σε συνεργασία με το τμήμα προσωπικού να έχει προσχεδιάσει τους χρόνους εργασίας για όλο το προσωπικό. Έτσι θα μπορεί να συμπληρώσει στοιχεία όπως:

- α) Πόσα διαθέσιμα λεπτά συνιστούν μια εργάσιμη ημέρα (π.χ. 480 λεπτά για ένα οκτάωρο)
- β) Ποιά είναι η μικρότερη δυνατή εργάσιμη ώρα (π.χ. 10 λεπτά)
- γ) Ποιό είναι το μεγαλύτερο διάστημα εργασίας σε μια ημέρα (π.χ. 720 λεπτά δηλαδή οκτάωρο με επιπλέον τέσσερις ώρες υπερωρία)
- δ) Σε πόσα λεπτά θεωρείται καθυστέρηση προσέλευσης και σε πόσα καθυστέρηση αποχώρησης
- ε) Αν θα μετρούν στην συνολική ώρα και τα διαλείμματα ή όχι
- στ) Από ποιιά ώρα και μετά η εργασία καταλογίζεται ως υπερωρία
- ζ) Κατηγορίες υπερωρίας (π.χ. καθημερινές, σαββατοκύριακα, αργίες)
- η) Πόσες ημέρες καλύπτει μια βάρδια (π.χ. 09:00 με 17:00 είναι μια βάρδια σε μια ημέρα ενώ 22:00 με 06:00 είναι μια βάρδια σε δύο ημέρες)
- θ) Ποιές ημέρες της εβδομάδας είναι εργάσιμες

The screenshot shows a software configuration window titled 'Software Guide' with a navigation bar at the top containing 'Register', 'Database', 'Department', 'Staff', 'Attendance', 'Scheduling', and 'Device'. The 'Attendance' tab is active. The main area is divided into 'Stat. Rule' and 'Stat. Items' sections. Under 'Stat. Rule', there are several settings: 'A workday count as' (480 Minute), 'The shortest working time' (10 Minute), 'The longest working time' (720 Minute), and checkboxes for 'Not clock in count as late', 'Not clock out count as early', 'deduct the 'On duty X minutes earlier'', and 'deduct the 'Off duty X minutes later''. Under 'Stat. Items', there are 'Overtime Calculation' settings (Normal: 1, Weekend: 2, Festival: 3) and 'Weekend' checkboxes for Monday through Sunday, with Saturday and Sunday checked. At the bottom, there are 'Back' and 'Next Step' buttons.



## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

Στη δεύτερη καρτέλα στο βήμα παρουσία δηλώνονται παράμετροι όπως κατηγορίες απουσίας – παρουσίας (π.χ. κανονική εργασία, κανονική άδεια, αναρρωτική άδεια, αδικαιολόγητη απουσία, υπερωρία, υπερωρία άνευ αποδοχών, αποστολή – απόσπαση, κλπ).

Software Guide

Register Database Department Staff **Attendance** Scheduling Device

Stat. Rule Stat. Items

Stat. Items:

- Normal
- Late
- Early
- Business Leave
- Leave
- Absence
- Stay away
- Overtime
- Free Overtime

Stat. Rule

Device Set

Device: Day

Minimum: 0,5

Indicating Symbol

Indicating Symbol: /

Round-off control

- Round down
- Round up
- Round off
- Round at total
- Accumulate by times

Back Next Step

➤ **Βήμα 6ο : Προγραμματισμός – Scheduling**

Σε αυτό το βήμα ο διαχειριστής συμπληρώνει τρεις επιπλέον καρτέλες. Η πρώτη καρτέλα αφορά τη ρύθμιση του χρονοδιαγράμματος της επιχείρησης (π.χ. ώρα έναρξης και ώρα κλεισίματος). Μπορεί να προσθέσει πλήθος χρονοδιαγραμμάτων ανάλογα με τις ανάγκες του οργανισμού. Κάθε χρονοδιάγραμμα ονοματίζεται και ενεργοποιείται είτε χειροκίνητα είτε αυτόματα από το πρόγραμμα ανάλογα με την επιθυμία του διαχειριστή.

The screenshot displays the 'Scheduling' module of a software application. At the top, a 'Software Guide' bar contains a progress indicator with seven steps: Register, Database, Department, Staff, Attendance, Scheduling (highlighted), and Device. Below this, three tabs are visible: 'Timetable Setting', 'Shift Setting', and 'User Scheduling'. The 'Timetable Setting' tab is active, showing a 'Timetable List' table with one entry: 'Timetable N On Duty Time Off Duty Time'. To the right, the 'Timetable Information' form includes fields for 'Timetable Name', 'On Duty Time', 'Off Duty Time', 'Begin Clock-In Time', 'End Clock-In Time', 'Begin Clock-Out Time', 'End Clock-Out Time', 'Late error allowance' (5 Minutes), 'Early error allowance' (5 Minutes), 'Count As Workday' (1), and 'Total Work Time' (480 Minutes). Checkboxes for 'Must C-In', 'Must C-Out', 'Free Time', and 'OT Time' are present. 'Back' and 'Next Step' buttons are at the bottom.



## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

Η δεύτερη καρτέλα αφορά τη ρύθμιση των βάρδιών. Με την ίδια λογική όπως και στην πρώτη καρτέλα προσθαφαιρούνται βάρδιες αφού ονοματιστούν και ρυθμίζονται σε σταθερό ή κυλιόμενο ωράριο. Ρυθμίζεται επίσης ο κύκλος της βάρδιας (π.χ. εβδομαδιαίως).

Software Guide

Register Database Department Staff Attendance Scheduling Device

Timetable Setting Shift Setting User Scheduling

Shift List:

Shift Name

Shift Information

Shift Name  Cycles 1  Cycle Device Week

Add Del Modify  As Default Class

	Time1	Time2	Time3	Time4
Sunday				
Monday				
Tuesday				
Wednesday				
Thursday				
Friday				
Saturday				

Back Next Step

## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

Η τρίτη καρτέλα αφορά το μοίρασμα του προσωπικού στις βάρδιες που έχουν δημιουργηθεί προηγουμένως. Από τη βάση δεδομένων αντλούνται τα στοιχεία του προσωπικού και ουσιαστικά δημιουργούνται νέοι χρήστες με ορισμένες εξουσίες (π.χ. είσοδο/έξοδο μόνο). Ένας χρήστης μπορεί να αλλάξει θέση σε κάποιες βάρδιες αν αυτό χρειαστεί.

Software Guide

Register Database Department Staff Attendance Scheduling Device

Timetable Setting Shift Setting User Scheduling

User No. User Name Search Select All Intelligent sched

User ID	Name	Dept.	Shift	User Number
---------	------	-------	-------	-------------

Normal scheduling

Shift Name Add

Beginning 2012-01-01 Delete

Ending 2012-12-31 Clear

Shift Name	Beginning	Ending
------------	-----------	--------

Back Next Step



➤ **Βήμα 7ο : Συσκευή – Device**

Στο τελευταίο βήμα συνδέονται τα δεδομένα της διαχείρισης με τις συσκευές. Αρχικά γίνεται η αναζήτηση των διαθέσιμων συσκευών και έπειτα δηλώνεται ανά συσκευή το όνομά της και από ποιο αρχείο αντλεί δεδομένα ταυτοποίησης. Μπορούν όλες οι συσκευές να έχουν ακριβώς την ίδια ρύθμιση ή ανάλογα με την επιθυμία προσβασιμότητας να ρυθμιστούν όλες διαφορετικά. Με αυτόν τον τρόπο προσθαφαιρούνται εύκολα συσκευές.

Software Guide

Register Database Department Staff Attendance Scheduling Device

Search Device Setting Device Add Device

Search Setting Add

No	Device type	Device ID	Serial number	IP	Mask	Gate	MAC
----	-------------	-----------	---------------	----	------	------	-----

Back Next Step

## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

Software Guide

Register Database Department Staff Attendance Scheduling Device

Search Device Setting Device Add Device

Select Device in the Search Device Tab

Setting information

Device ID

IP

Mask

Gate

ServerIP

Port

Mode

Authentication information

User name

Password

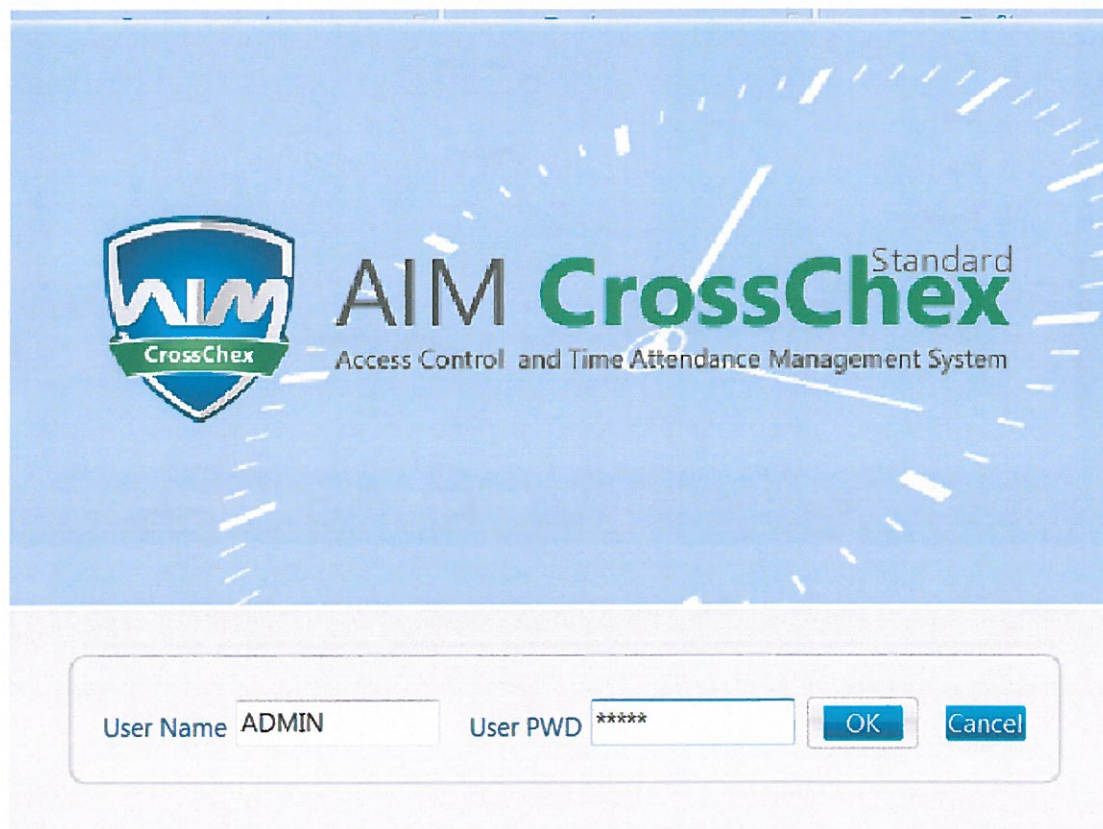
Setting

Back Next Step



➤ **Βήμα 8ο : Δημιουργία Κωδικού Διαχειριστή**

Στο βήμα αυτό δηλώνεται ο ατομικός και εμπιστευτικός κωδικός του διαχειριστή του συστήματος. Δεν μπορούν να υπάρξουν περισσότεροι από έναν κωδικοί για λόγους ασφαλείας.



**Προγραμματισμός Βιομετρικού Συστήματος Αναγνώρισης Δαχτυλικών Αποτυπωμάτων**

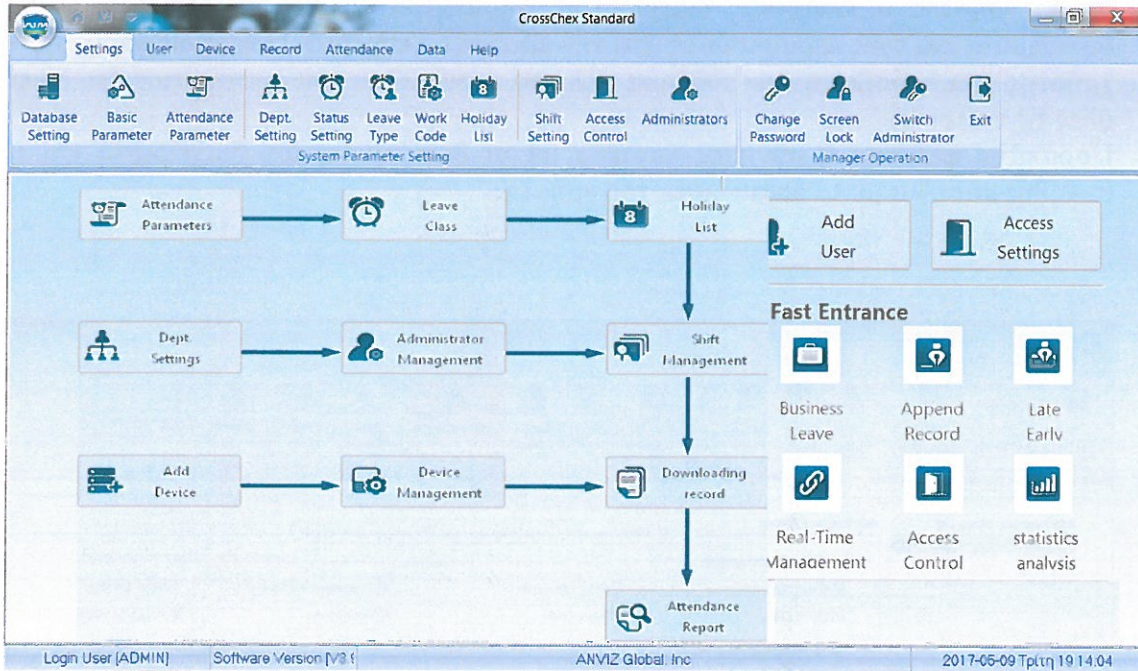
Ολοκληρώνοντας και την εγγραφή στην παραπάνω πλατφόρμα του λογισμικού CrossChex, σειρά έχει ο προγραμματισμός του Βιομετρικού Συστήματος, ο οποίος θα πραγματοποιηθεί από τον Administrator PC ακολουθώντας τις οδηγίες όπως φαίνονται και στο manual. Αφού όλα τα παραπάνω βήματα ολοκληρωθούν θα μπορεί να λειτουργεί ο υπολογισμός των αναφορών. Οι αναφορές μπορούν να υπολογίσουν τον χρόνο παρουσίας όλων των υπαλλήλων μαζί ή ενός μεμονωμένου υπαλλήλου από ένα συγκεκριμένο τμήμα και για μια συγκεκριμένη χρονική περίοδο. Στην καρτέλα "παρουσία" πρέπει ο διαχειριστής να επιλέξει την αρχή και το τέλος της ημερομηνίας που τον ενδιαφέρει. Στη συνέχεια επιλέγοντας την στατιστική ανάλυση ( statistical analysis) το σύστημα θα υπολογίσει αυτόματα τα δεδομένα και θα ελέγξει την ορθότητα των αρχείων (π.χ. μερικές φορές υπάρχουν λανθασμένα αρχεία που δημιουργούνται κατά τη χρήση όπως όταν ένας υπάλληλος περνάει δύο φορές το



## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

αποτύπωμά του από τον αισθητήρα σε πολύ μικρό χρονικό διάστημα με αποτέλεσμα ένα από τα δυο αρχεία να θεωρείται λανθασμένο). Εάν εντοπιστεί κάποιος λάθος στον υπολογισμό του συστήματος ο διαχειριστής μπορεί να διορθώσει χειροκίνητα το αρχείο ώστε να εξασφαλίσει την ορθότητα των αποτελεσμάτων. Μετά την πρώτη φορά όλες οι παραπάνω δραστηριότητες μπορούν να ρυθμιστούν από το διαχειριστή από την κεντρική σελίδα του προγράμματος.

Η κεντρική σελίδα του προγράμματος είναι η εξής:



Όπως φαίνεται και από την παραπάνω απεικόνιση του προγράμματος υπάρχει πλήθος επιλογών και εντολών για την διευκόλυνση του διαχειριστή, όπως η πρόσθεση νέου χρήστη, ο ορισμός κωδικών πρόσβασης και πολλά άλλα. Αυτό που έχει όμως πολύ ενδιαφέρον είναι το διάγραμμα διαδικασιών του προγράμματος που εμφανίζεται στο κέντρο της σελίδας. Έχει σχεδιαστεί έτσι ώστε να θυμίζει ανά πάσα στιγμή στον διαχειριστή την σειρά που πρέπει να ακολουθήσει χωρίς να χρειάζεται να ανατρέχει συνεχώς στο manual.

Στο διάγραμμα διαδικασιών εμφανίζονται:

- οι Παράμετροι Παρουσίας (Attendance Parameters)
- το Ωράριο Αποχώρησης (Leave Class)
- η Λίστα Αργιών – διακοπών (Holiday List)
- οι Ρυθμίσεις Τμημάτων (Department Settings)
- η Οργάνωση του Διαχειριστή (Administrator Management)
- η Διαχείριση Βαρδιών (Shift Management)
- η Πρόσθεση Συσκευών (Add Device)
- η Διαχείριση Συσκευών (Device Management)

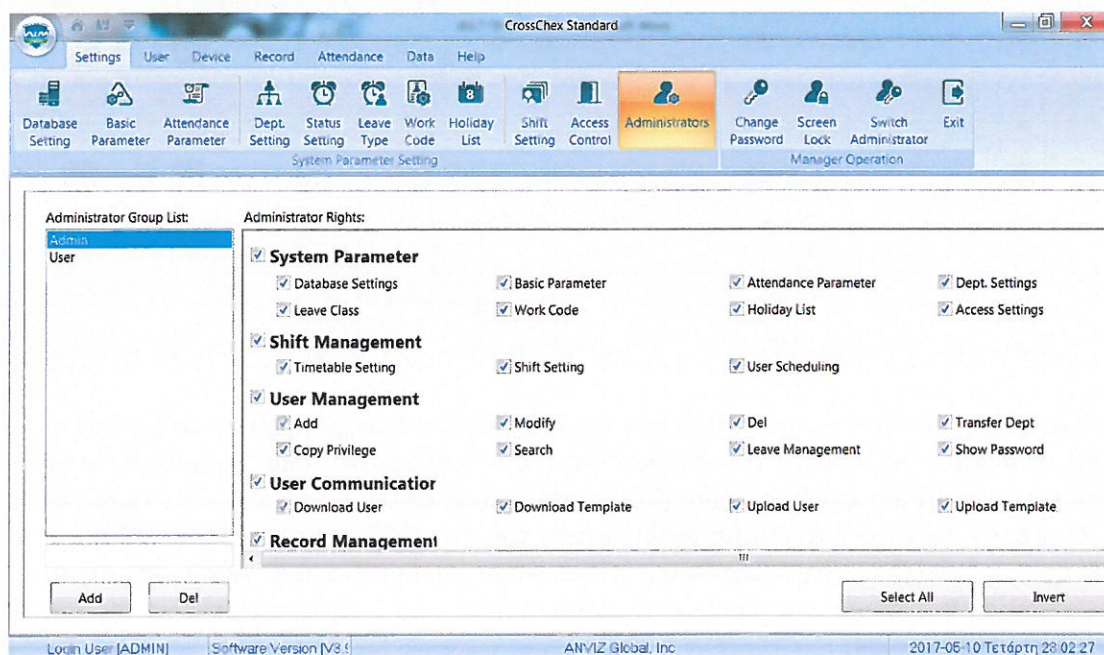


## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων

- το Κατέβασμα Αρχείων (Downloading Record)
- η Αναφορά Παρουσίας (Attendance Report)

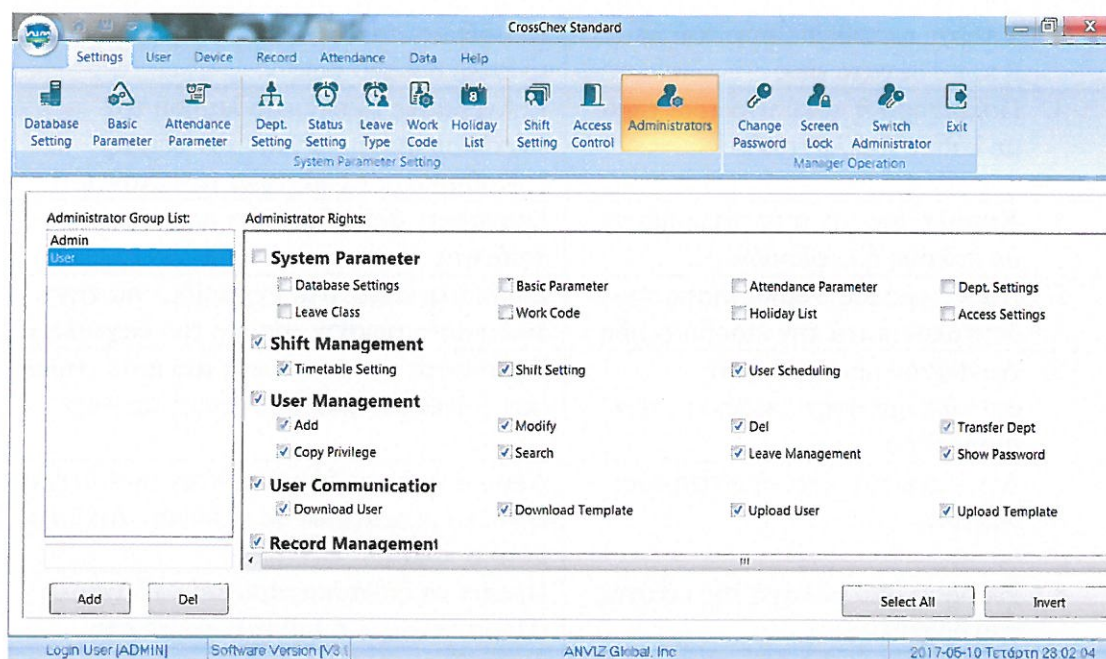
Ουσιαστικά η κεντρική σελίδα του προγράμματος περιέχει όλα τα βήματα που έγιναν για την έναρξη του προγράμματος χωρίς απαραίτητα να ακολουθείται η ίδια σειρά. Μπορεί να διατηρηθεί η αρχική καταχώρηση των στοιχείων, η οποία πραγματοποιήθηκε κατά την εγκατάσταση του λογισμικού ή να αλλάξουν κάποιες παράμετροι και στοιχεία. Σε περίπτωση που δημιουργηθεί δεύτερος διαχειριστής ή απλός χρήστης ο κεντρικός διαχειριστής δημιουργεί το προφίλ επιλέγοντας τα δικαιώματα και τους περιορισμούς από την παρακάτω καρτέλα. Ο νέος διαχειριστής – χρήστης έχει πρόσβαση στο σύστημα αλλά το περιβάλλον του συστήματος δεν δίνει όλες τις επιλογές.

Παρακάτω φαίνεται η συνήθης καρτέλα με τα δικαιώματα του διαχειριστή και η συνήθης καρτέλα με τα δικαιώματα του χρήστη.



**Καρτέλα με τα δικαιώματα του διαχειριστή**

## Βιομετρικά Συστήματα Αναγνώρισης Προτύπων ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων



**Καρτέλα με τα δικαιώματα του χρήστη**

### Προβλήματα Λειτουργίας και τρόποι Αντιμετώπισης του Συστήματος

Όταν το πρόγραμμα εγκατασταθεί επιτυχώς και προγραμματιστεί το λογισμικό και κατ' επέκταση λειτουργήσουν τα τερματικά ωρομέτρησης, το σύστημα είναι έτοιμο για την καταχώρηση των στοιχείων των υπαλλήλων.

Στην διάρκεια εφαρμομογής του συστήματος μπορεί να υπάρξουν και κάποιες δυσλειτουργίες όσον αφορά την χρήση του, όπως για παράδειγμα όταν το δαχτυλικό αποτύπωμα έχει καταχωρηθεί αλλά συχνά στην ταυτοποίηση εμφανίζεται η ένδειξη "ΑΠΟΤΥΧΙΑ", τότε υπάρχουν κάποιες παράμετροι που πρέπει να ελεγχθούν για να βρεθεί που οφείλεται η ένδειξη αυτή και πως μπορεί να αντιμετωπιστεί.

Παρακάτω φαίνονται κάποιες περιπτώσεις δυσλειτουργίας και τις παραμέτρους που πρέπει να ελεγχθούν προκειμένου να αντιμετωπιστούν.

- Το δαχτυλικό αποτύπωμα έχει καταχωρηθεί αλλά συχνά στην ταυτοποίηση εμφανίζεται "ΑΠΟΤΥΧΙΑ".

ΑΙΤΙΑ	ΛΥΣΗ
1. Το αποτύπωμα δεν σκαναρίστηκε σωστά	Πρέπει να ξανασκαναριστεί το δάχτυλο (Παρακαλούμε συμβουλευτείτε στο εγχειρίδιο την σωστή πίεση του δαχτύλου)



**Βιομετρικά Συστήματα Αναγνώρισης Προτύπων  
ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων**

2. Υπήρχε απευθείας φως του ήλιου ή πολύ δυνατό φως	Αποφύγετε το απευθείας φως του ήλιου ή το πολύ δυνατό φως
3. Πολύ ξηρό ή πολύ υγρό δάχτυλο με λάδι ή καλλυντικά	1, Ανεβάστε το επίπεδο λαδιού του δαχτύλου ακουμπώντας τον δείκτη. 2, Καθαρίστε τα δάχτυλα με πετσέτα
4. Χαμηλή ποιότητα αποτυπώματος με κάλους ή ξεφλούδισμα	Σκανάρετε άλλα δάχτυλα με καλύτερη ποιότητα
5. Λάθος τρόπος τοποθέτησης του δαχτύλου κατά την είσοδο/έξοδο	Συμβουλευτείτε στο εγχειρίδιο για την διαδικασία σωστής πίεσης του δαχτύλου
6. Λανθάνον προηγούμενο αποτύπωμα στην επιφάνεια του αισθητήρα	Καθαρίστε την επιφάνεια του αισθητήρα (προτείνονται απορροφητικές ταινίες)
7. Δεν ασκείται αρκετή πίεση στο δάχτυλο	Ακουμπήστε το δάχτυλο στον αισθητήρα ώστε να μοιράζεται σε όλον και ασκήστε μέτρια πίεση
8. Επιρροή από αλλαγή της εικόνας του δαχτύλου	Πρέπει να ξανασκαναριστεί το δάχτυλο (Παρακαλούμε συμβουλευτείτε στο εγχειρίδιο την σωστή πίεση του δαχτύλου)

- Δεν βρέθηκαν αρχεία σχετικά με την χρονομέτρηση εισόδου/εξόδου του προσωπικού.

<b>ΑΙΤΙΑ</b>	<b>ΛΥΣΗ</b>
1. Η μονάδα ενέργειας έμεινε καιρό κλειστή (ο χρόνος επιστρέφει αυτόματα στο μηδέν)	Συγχρονίστε τον χρόνο
2. Το αρχείο δεν έχει κατέβει	Παρακαλούμε κατεβάστε το αρχείο από την συσκευή
3. Η χωρητικότητα έχει εξαντληθεί	Καθαρίζετε τα αρχεία με τον καιρό

- Η συσκευή δεν συνδέεται με τον υπολογιστή.

<b>ΑΙΤΙΑ</b>	<b>ΛΥΣΗ</b>
1. Ο τρόπος επικοινωνίας δεν έχει οριστεί σωστά	Επιλέξτε την σωστή μέθοδο επικοινωνίας
2. Το καλώδιο δεν εφαρμόζει σωστά ή έχει βλάβη	Τοποθετείστε το καλώδιο σωστά ή αντικαταστήστε το
3. Δεν δύναται να συνδεθεί με το COM (λάθος αριθμός COM)	Εισάγετε τον σωστό αριθμό COM (διεύθυνση)

**Βιομετρικά Συστήματα Αναγνώρισης Προτύπων  
ως Εργαλείο Διαχείρισης Ανθρώπινων Πόρων**

---

4. Δεν δύναται να συνδεθεί με το TCP/IP (λάθος ρυθμιστής)	Συμβουλευτείτε το εγχειρίδιο σχετικά με την σύνδεση του τερματικού ωρομέτρησης
---	--

- Η ώρα των τερματικών λειτουργεί άψογα αλλά το σκάνερ αποτυπωμάτων είναι κλειστό. Οι υπάλληλοι δεν μπορούν να εγγραφούν.

ΑΙΤΙΑ	ΛΥΣΗ
1. Η μονάδα βρίσκεται σε διαδικασία ύπνου (αναμονή ή αδρανοποίηση)	Πατήστε οποιοδήποτε κουμπί για να ενεργοποιηθεί
2. Η συσκευή βρίσκεται σε σύνδεση επικοινωνίας ή υπάρχει διακοπή στην διαδρομή	1, Βγείτε από το σύστημα πατώντας έξοδο συστήματος. Αν κλείσει απότομα η συσκευή θα επανέρχεται στη συλλογή αποτυπωμάτων κάθε 1 λεπτό 2, Διώξτε το εμπόδιο της διαδρομής
3. Η χωρητικότητα έχει εξαντληθεί	Καθαρίζετε τα αρχεία με τον καιρό

- Δεν χρησιμοποιούμε το ID και το αποτύπωμα ως μέθοδο αναγνώρισης.

ΑΙΤΙΑ	ΛΥΣΗ
1. Λάθος καταχώρηση ID	Καταχωρήστε το σωστό ID
2. Ο χρήστης δεν έχει δικαίωμα χρήσης 1:1 μεθόδου αναγνώρισης	Ρυθμίστε την μέθοδο αναγνώρισης 1:1 για αυτό το χρήστη

- Η μονάδα δίνει σήμα (BEEP) αυτόματα όταν κανείς δεν εισέρχεται/εξέρχεται.

ΑΙΤΙΑ	ΛΥΣΗ
3. Υπάρχει απευθείας φως του ήλιου ή πολύ δυνατό φως	Αποφύγετε το απευθείας φως του ήλιου ή το πολύ δυνατό φως
4. Λανθάνον προηγούμενο αποτύπωμα στην επιφάνεια του αισθητήρα	Καθαρίστε την επιφάνεια του αισθητήρα (προτείνονται απορροφητικές ταινίες)

### Εκπαίδευση Προσωπικού

Για την αποτελεσματικότερη χρήση του συστήματος αναγνώρισης θα πρέπει το προσωπικό της επιχείρησης αλλά και τα στελέχη της να εκπαιδευτούν πάνω στην σωστή διαχείριση του συστήματος.

Αρχικά ο υπεύθυνος του συστήματος, που ουσιαστικά παίζει και τον ρόλο του διαχειριστή, θα πρέπει να εκπαιδευτεί σε όλο το φάσμα των εφαρμογών και των



δυνατοτήτων που παρέχει το σύστημα. Φυσικά θα πρέπει να έχει άριστη γνώση του εγχειριδίου το οποίο πρέπει να συμβουλευέται σε συχνή βάση.

Επίσης οι αρχικές ρυθμίσεις, ο προγραμματισμός και η εγκατάσταση του συστήματος θα πρέπει να γίνουν από την ομάδα εγκατάστασης και τον ηλεκτρολόγο μηχανικό που θα έχει κάνει την χωροταξική και ηλεκτρολογική μελέτη, παρουσία όμως πάντα του υπεύθυνου διαχείρισης του συστήματος στην επιχείρηση.

Το υπόλοιπο προσωπικό θα λάβει δευτερεύουσα εκπαίδευση, με πληροφορίες που θα περιορίζονται στα απαραίτητα για την ορθή λειτουργία του συστήματος. Κάθε εργαζόμενος στην επιχείρηση θα πρέπει να λάβει τους προσωπικούς του κωδικούς και να δώσει το αποτύπωμά του για να ταυτιστεί με τα στοιχεία του. Επίσης στην εκπαίδευσή του θα περιλαμβάνονται και οι υποδείξεις για την ορθή λειτουργία του συστήματος χωρίς να υπάρχουν επιπλοκές ή τυχόν καθυστερήσεις και ένα οργανωμένο πλαίσιο του χρόνου αλλά και του χώρου στο οποίο θα εργάζονται και θα μπορούν να κινούνται οι υπάλληλοι.

Στόχος της εκπαίδευσης αλλά και της χρήσης του προγράμματος είναι ο κάθε υπάλληλος να μπορεί (ανάλογα με το πρωτόκολλο πρόσβασης στο σύστημα) να τσεκάρει των εαυτό του, να διορθώνει τα κενά και να επιδεικνύει την δέουσα επιμέλεια, γεγονός που δυνητικά ενισχύει την απόδοση της επιχείρησης και ανακουφίζει το βάρος που επωμίζονται οι επιμελείς εργαζόμενοι από τους αμελείς συναδέλφους τους αλλά και η ίδια η επιχείρηση από το σύνολο των εργαζομένων της.

Η εκπαίδευση θα έχει μεγαλύτερο αποτέλεσμα όταν εκτός από την βασική εκπαίδευση πραγματοποιούνται, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, σενάρια προσομοίωσης πραγματικών περιπτώσεων, προβλημάτων ή καθημερινών διαδικασιών και λειτουργιών.

Τέλος, η εκπαίδευση δεν αφορά μόνο στην είσοδο και έξοδο από το χώρο εργασίας αλλά και στην καθημερινή χρήση και συμπεριφορά στον χώρο από τους εργαζομένους και από τα στελέχη.

### **Πλεονεκτήματα & Μειονεκτήματα χρήσης του Βιομετρικού Συστήματος Αναγνώρισης Δαχτυλικών Αποτυπωμάτων**

Η αναγνώριση δαχτυλικών αποτυπωμάτων χρησιμοποιεί τα διακριτά χαρακτηριστικά του δαχτυλικού αποτυπώματος με σκοπό την αναγνώριση και ταυτοποίηση των ατόμων.

Η επιφάνεια στη οποία τοποθετείται το δάχτυλο προκειμένου να γίνει το σκανάρισμα λέγεται platen ή scanner. Ένα platen μπορεί να είναι φτιαγμένο από γυαλί, πλαστικό, σιλικόνη, κ.α. υλικά. Ένα platen είναι μέρος του module. Ένα module αποτελεί τον βασικό πυρήνα μιας περιφερειακής ή ανεξάρτητης συσκευής σκαναρίσματος δαχτυλικών αποτυπωμάτων. Τα σύγχρονα module έχουν τη δυνατότητα να εκτελούν όλες τις λειτουργίες του συστήματος, δηλαδή την απόκτηση και επεξεργασία εικόνας, τη δημιουργία και προσωρινή αποθήκευση των αρχείων της εικόνας (template), την αποστολή αυτών των εικόνων και το ταίριασμά τους με την βάση δεδομένων και την θετική ή αρνητική ταυτοποίηση της εικόνας.

Άρα η βιομετρική ταυτοποίηση των δαχτυλικών αποτυπωμάτων έχει πέντε στάδια υλοποίησης.

- την απόκτηση της εικόνας,
- την επεξεργασία της εικόνας,
- τον εντοπισμό των διακριτών χαρακτηριστικών,
- την δημιουργία του αρχείου (templates),
- το ταίριασμα του αρχείου (templates).

Το παραπάνω βιομετρικό σύστημα αναγνώρισης έχει τα πλεονεκτήματα και τα μειονεκτήματά του.

### **Πλεονεκτήματα**

#### **➤ Αυξημένη αξιοπιστία και ακρίβεια**

Η ανάλυση και ταξινόμηση των δαχτυλικών αποτυπωμάτων έχει ξεκινήσει εδώ και χρόνια. Η εφαρμογή της αναγνώρισης δαχτυλικών αποτυπωμάτων είναι πολύ διαδεδομένη και μέχρι στιγμής κανένα άλλο σύστημα αναγνώρισης δεν μπορεί να φτάσει τα μηδενικά ποσοστά λάθους που έχει η αναγνώριση δαχτυλικών αποτυπωμάτων με λήψη ενός ή δύο δειγμάτων.

#### **➤ Δυνατότητα χρησιμοποίησης σε διαφορετικά περιβάλλοντα**

Χάρη στο μέγεθος που έχουν αποκτήσει πλέον οι συσκευές σκαναρίσματος δαχτυλικών αποτυπωμάτων είναι πολύ εύκολο να τοποθετηθούν ή ακόμα και να μεταφερθούν σε οποιοδήποτε περιβάλλον και μέρος χρειαστεί. Δεν επηρεάζονται από τις κλιματικές ή περιβαλλοντολογικές συνθήκες (π.χ. φωτισμό, κρύο, ζέστη). Σήμερα κάποιος μπορεί να βρει πληθώρα επιλογών και προτάσεων σχετικά με τον εξοπλισμό σκαναρίσματος αποτυπωμάτων, τα οποία μπορεί να τα προσαρμόσει στις ανάγκες του.

#### **➤ Χρήση εργονομικών συσκευών**

Η τοποθέτηση του δαχτύλου στη συσκευή σκαναρίσματος είναι μια πολύ απλή κίνηση, η οποία δεν χρειάζεται κάποια συγκεκριμένη εκπαίδευση, σε σχέση με τη χρήση κάποιων άλλων βιομετρικών συσκευών. Έτσι η χρήση της μπορεί να γίνει με μια πολύ απλή καθοδήγηση είτε από τις εργοστασιακές πληροφορίες, είτε από κάποιο υπεύθυνο.

#### **➤ Δυνατότητα εγγραφής με πολλά δάχτυλα**

Το σύστημα δίνει την δυνατότητα στο χρήστη να χρησιμοποιήσει και τα 10 δάχτυλα ως τρόπο κλειδώματος και ξεκλειδώματος, αν και αυτό είναι κάτι το οποίο δεν συνηθίζεται αλλά δίνει το πλεονέκτημα της ασφάλειας. Εάν κάποιος χρησιμοποιήσει δύο από τα δάχτυλά του ως κωδικό, τότε κάνει την περίπτωση της κλοπής ή της παραβίασης πολύ δύσκολη, έως ακατόρθωτη. Επίσης υπάρχει και η δυνατότητα



χρήσης ξεχωριστού δαχτύλου για ξεχωριστή ενέργεια. Επιπλέον το σύστημα μπορεί να ζητήσει και την επίδειξη των δαχτύλων με μπερδεμένη σειρά.

➤ **Τεχνολογία που δεν θεωρείται ενοχλητική**

Οι χρήστες σκαναρίσματος των δαχτυλικών αποτυπωμάτων στην πλειοψηφία δεν θεωρούν την εφαρμογή ενοχλητικά ή απειλητική. Αυτό οφείλεται στο ότι η εγγραφή και η αποθήκευση των στοιχείων του χρήστη είναι απλή, εύκολη και γρήγορη.

➤ **Τεχνολογία που έχει ως βάση αμετάβλητα χαρακτηριστικά του ανθρώπου**

Τα αποτυπώματα του ανθρώπου είναι μοναδικά στο κάθε άτομο και δεν μεταβάλλονται κατά την διάρκεια της ζωής του. Επίσης η απώλεια ή η αύξηση βάρους δεν μπορούν να μεταβάλλουν τα δαχτυλικά αποτυπώματα καθιστώντας τα μια από τις πιο αξιόπιστες βιομετρικές εφαρμογές αναγνώρισης.

### **Μειονεκτήματα**

➤ **Αδυναμία εγγραφής κάποιων χρηστών**

Υπάρχει ένα ποσοστό χρηστών, το οποίο δεν μπορεί ή δεν επιθυμεί να εγγραφεί στα περισσότερα συστήματα σκαναρίσματος δαχτυλικών αποτυπωμάτων. Το ποσοστό αυτό αν και είναι πολύ μικρό δημιουργεί κάποια λειτουργικά προβλήματα. Ένα από αυτά είναι ότι η επιχείρηση που χρησιμοποιεί κάποιο από αυτά τα βιομετρικά συστήματα μπορεί να έχει διπλοεγγραφές αυτών των χρηστών.

➤ **Μακροπρόθεσμη μείωση απόδοσης**

Αν και τα δαχτυλικά αποτυπώματα είναι από τα αμετάβλητα χαρακτηριστικά του ανθρώπου που δεν αλλάζουν κατά την πορεία της ζωής του, η καθημερινότητα μπορεί να τους προκαλέσει κάποιες φθορές, οι οποίες πιθανόν να επηρεάσουν την αποδοτικότητα του βιομετρικού συστήματος. Τα άτομα που η εργασία τους είναι περισσότερο χειρονακτική, μπορεί να παρουσιάσουν λάθη στο σύστημα. Αυτό μπορεί να αποφευχθεί ενημερώνοντας τα στοιχεία του συστήματος κατά τακτά χρονικά διαστήματα ή χρησιμοποιώντας περισσότερα από ένα δαχτυλικά αποτυπώματα.

➤ **Συσχετισμός με εφαρμογές της σήμανσης**

Η διαδικασία αναγνώρισης δαχτυλικών αποτυπωμάτων δημιουργεί σε πολύ κόσμο μια συσχέτιση του τρόπου εφαρμογής της, με αυτόν της λήψης και αναγνώρισης δαχτυλικών αποτυπωμάτων που κάνει η σήμανση για εγκληματικούς λόγους. Αυτό δημιουργεί ένα συναίσθημα ανασφάλειας και αβεβαιότητας και οι χρήστες είναι δύσπιστοι στο να δώσουν τα δαχτυλικά τους αποτυπώματα. Παρ' ότι η λήψη των δαχτυλικών αποτυπωμάτων από τα βιομετρικά αυτά συστήματα δεν είναι για επεξεργασία ή αποθήκευση, πολύς κόσμος δεν το γνωρίζει και δεν θεωρεί αυτή την διαδικασία σωστή.

➤ **Ανάγκη για εξειδικευμένες συσκευές**

Για να χρησιμοποιηθεί ένα σύστημα σκαναρίσματος και αναγνώρισης δαχτυλικών αποτυπωμάτων απαιτείται η εγκατάσταση εξειδικευμένων συσκευών. Αυτό απαιτείται γιατί το σκανάρισμα των αποτυπωμάτων δεν μπορεί να στηριχθεί σε συσκευές που ήδη υπάρχουν σε έναν οργανισμό ή μια επιχείρηση, όπως γίνεται για παράδειγμα στην αναγνώριση φωνής όπου μπορούν να κάποια μικρόφωνα ή και τα τηλέφωνα. Οι συσκευές που χρησιμοποιούνται στο σκανάρισμα δαχτύλων διαφέρουν σε κάθε εφαρμογή.

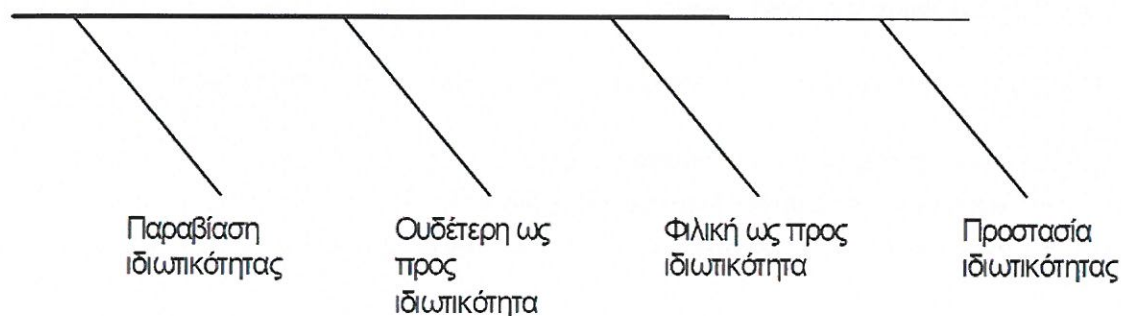
**Ηθικά Ζητήματα που προκύπτουν με την χρήση των Βιομετρικών Συστημάτων**

Από την πρώτη στιγμή που η χρήση των Βιομετρικών Συστημάτων Αναγνώρισης έκαναν την εμφάνισή τους αλλά μέχρι και σήμερα που έχουν ενταχθεί στην καθημερινότητα των ανθρώπων στο έπακρον, δεν παύουν να δημιουργούν και ένα αίσθημα ανασφάλειας και παραβίασης. Πολλοί είναι αυτοί που εκφράζουν την ανησυχία τους για την παραβίαση της ιδιωτικότητας που γίνεται μέσω της ψηφιοποίησης των φυσικών χαρακτηριστικών και την αποθήκευση αυτών σε βάσεις δεδομένων. Άλλοι πάλι υποστηρίζουν ότι η χρήση των Βιομετρικών Συστημάτων προστατεύει τους ανθρώπους από τις εγκληματικές ενέργειες και τις κακόβουλες πράξεις. Τα Βιομετρικά Συστήματα βέβαια δεν είναι αλάνθαστα, πράγμα που σημαίνει ότι μπορεί η ιδιωτικότητα όλους αυτών που τα χρησιμοποιεί, από μια λάθος ενέργεια ή από μια κίνηση παραβίασης να βρεθεί εκτεθειμένη. Ωστόσο μετά από την αντιμετώπιση και την πρόληψη πληθώρας εγκληματικών και τρομοκρατικών ενεργειών η στάση των ανθρώπων φαίνεται να αλλάζει και λίγοι να είναι αυτοί που υποστηρίζουν την αρνητική σχέση των Βιομετρικών Συστημάτων και της ιδιωτικοποίησης.

Η χρήση των Βιομετρικών Συστημάτων μπορεί ανάλογα με τον τομέα, το περιβάλλον και το λόγο για τον οποίο χρησιμοποιούνται, να παραβιάσει και να εισχωρήσει στην ιδιωτικότητα των χρηστών τους, να είναι φιλική στην ιδιωτικότητα, ουδέτερη ή ακόμη και να προστατεύει την ιδιωτικότητα.

**Αρνητική σχέση**

**Θετική σχέση**



Το χειρότερο σενάριο είναι στην περίπτωση που η χρήση των Βιομετρικών Συστημάτων παραβιάσει την ιδιωτικότητα των χρηστών. Αυτό μπορεί να συμβεί χωρίς την έγκριση του χρήστη. Μπορεί να προκύψει από διαρροές από άλλες πηγές ή ακόμα εάν δεν υπάρχουν περιορισμοί μπορεί να χρησιμοποιηθεί για λόγους όπως



είναι ο εντοπισμός ή η κατάργηση της ανωνυμίας κάποιου χρήστη. Για να επιτευχθεί αυτό μπορούν να αξιοποιηθούν συστήματα, τα οποία ενώ η χρήση τους δεν προορίζονταν για τέτοιες ενέργειες δίνουν και αυτή την δυνατότητα.

Υπάρχει όμως και η ουδέτερη χρήση των βιομετρικών συστημάτων απέναντι στην ιδιωτικότητα. Αυτή η περίπτωση προκύπτει όταν δεν υπάρχει καμία προστασία και διασφάλιση σε τυχόν παραβιάσεις ή ακόμα και υποκλοπές.

Από την άλλη δε υπάρχει και η θετική σχέση των βιομετρικών συστημάτων με την ιδιωτικότητα. Σε αυτή την περίπτωση τα βιομετρικά συστήματα μπορούν να είναι φιλικά ή και να προστατεύουν την ιδιωτικότητα από διάφορες επικίνδυνες παραμέτρους.

### **Ο ρόλος της Αρχής Προστασίας Δεδομένων**

Για την προστασία και ιδιωτικότητα των ανθρώπων δημιουργήθηκε η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η οποία είναι συνταγματικά κατοχυρωμένη ως ανεξάρτητη Αρχή. Η ΑΠΔΠΧ ιδρύθηκε με το νόμο 2472/1997, ο οποίος ενσωματώνει στο ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία 95/46/ΕΚ. Η Οδηγία αυτή θέτει κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες της Ευρωπαϊκής Ένωσης.

Στόχος της Αρχής είναι η προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής του ατόμου στην Ελλάδα, σύμφωνα με τις διατάξεις των Ν.2472/1997 και 3471/2006.

Πρωταρχικός σκοπός της Αρχής είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που διαπιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα (χρηματοπιστωτικά, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ, κ.ο.κ.).

Επίσης, σκοπός της Αρχής είναι η υποστήριξη και καθοδήγηση των υπεύθυνων εφαρμογής των Βιομετρικών Συστημάτων στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο, λαμβάνοντας υπόψη τις νέες ανάγκες υπηρεσιών της ελληνικής κοινωνίας, καθώς και την διεύθυνση των σύγχρονων ψηφιακών επικοινωνιών και δικτύων. Ως εκ τούτου, η Αρχή στρέφει ιδιαίτερα την προσοχή της μεταξύ άλλων στην παρατήρηση και αντιμετώπιση ζητημάτων που προκύπτουν με την εξέλιξη των νέων τεχνολογιών και εφαρμογών.

Οι αρμοδιότητες της Αρχής μπορούν να ομαδοποιηθούν σε τρεις τομείς:

- Διοικητικές-Ελεγκτικές αρμοδιότητες
- Κανονιστικές-Συμβουλευτικές αρμοδιότητες
- Αρμοδιότητες Δημοσιοποίησης-Απολογισμού Συνεργασιών

Παρακάτω παραθέτονται αναλυτικά οι αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.



➤ **Διοικητικές-Ελεγκτικές αρμοδιότητες**

✓ Αρχείο γνωστοποιήσεων - Έκδοση αδειών

Οι υπεύθυνοι εφαρμογής των Βιομετρικών Συστημάτων υποχρεούνται να υποβάλλουν γνωστοποίηση προς την Αρχή όσον αφορά στη σύσταση και λειτουργία αρχείου, λαμβάνοντας υπόψη τις εξαιρέσεις που αναφέρονται στον Ν. 2472/1997. Βάσει των ανωτέρω γνωστοποιήσεων και στις περιπτώσεις που αυτό απαιτείται από τον Ν. 2472/1997, η Αρχή εκδίδει άδειες για τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα, για τη διαβίβαση δεδομένων σε χώρες εκτός Ε.Ε. ή/και για τη διασύνδεση δεδομένων. Οι άδειες χορηγούνται με συγκεκριμένους όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του δικαιώματος της ιδιωτικής ζωής των υποκειμένων ή τρίτων, ενώ η Αρχή απευθύνει υποδείξεις και συστάσεις σχετικά με το απόρρητο και την ασφάλεια της επεξεργασίας.

✓ Διενέργεια διοικητικών ελέγχων

Η Αρχή ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους σε αρχεία, τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Οι έλεγχοι διενεργούνται από εντεταλμένους υπαλλήλους του Τμήματος των Ελεγκτών, οι οποίοι συνοδεύονται σε περιπτώσεις που κρίνονται σημαντικές από μέλη της Αρχής. Οι διενεργούντες τον έλεγχο, ως ειδικοί ανακριτικοί υπάλληλοι, έχουν δικαίωμα πρόσβασης σε κάθε αρχείο χωρίς να μπορεί να τους αντιταχθεί κανενός είδους απόρρητο.

Κατά τον έλεγχο εξετάζεται καταρχήν η εναρμόνισή του ελεγχόμενου με τις απαιτήσεις των Ν.2472/97, 3471/2006 (γνωστοποίηση, ενημέρωση, λοιπές υποχρεώσεις κατά περίπτωση, αποδεικτικά στοιχεία). Στη συνέχεια πραγματοποιείται έλεγχος του πληροφοριακού του συστήματος, όπου σύμφωνα με τα άρθρα 6 και 10 του ν. 2472/1997, εξετάζονται τα βασικά χαρακτηριστικά του συστήματος, η φύση των δεδομένων, καθώς και το επίπεδο ασφαλείας που εξασφαλίζουν τα οργανωτικά και τεχνικά μέτρα που έχει λάβει ο υπεύθυνος επεξεργασίας για την προστασία των δεδομένων. Η ολοκλήρωση του ελέγχου οδηγεί στην σύνταξη πορίσματος το οποίο υποβάλλεται στην ολομέλεια της Αρχής

Η Αρχή ασκεί επίσης ανεξάρτητο έλεγχο στο εθνικό τμήμα του Συστήματος Πληροφοριών Σένγκεν, σύμφωνα με το άρθρο 114 παράγραφος 1 της Σύμβασης Εφαρμογής της Συμφωνίας Σένγκεν (ν. 2514/1997 ΦΕΚ 140 Α'), ασκεί τις αρμοδιότητες της εθνικής εποπτικής αρχής που προβλέπεται στο άρθρο 23 της Σύμβασης ΕΥΡΩΠΟΛ (ν. 2605/1998 ΦΕΚ 88 Α'), και τις αρμοδιότητες της εθνικής εποπτικής αρχής που προβλέπεται στο άρθρο 17 της Σύμβασης για τη χρήση της πληροφορικής στον τελωνειακό τομέα (ν. 2706/1999 ΦΕΚ 77 Α'), καθώς και τις αρμοδιότητες εποπτείας που προκύπτουν από οποιαδήποτε άλλη διεθνή συμφωνία.

✓ Εξέταση προσφυγών-καταγγελιών-ερωτημάτων

Η ΑΠΔΠΧ εξετάζει παράπονα και ερωτήματα σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων όταν αυτά θίγονται από την επεξεργασία δεδομένων και εκδίδει σχετικές Αποφάσεις. Επίσης, επιβάλλει στους υπεύθυνους επεξεργασίας ή στους τυχόν εκπροσώπους τους διοικητικές κυρώσεις, για παράβαση των υποχρεώσεών τους που απορρέουν από τον νόμο 2472/97 και από



κάθε άλλη ρύθμιση που αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Τέλος, η Αρχή μπορεί να καταγγέλλει τις παραβάσεις των διατάξεων του νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.

➤ **Κανονιστικές-Συμβουλευτικές αρμοδιότητες**

Η Αρχή εκδίδει Οδηγίες προς τον σκοπό ενιαίας εφαρμογής των ρυθμίσεων που αφορούν στην προστασία του ατόμου από την χρήση δεδομένων προσωπικού χαρακτήρα, καθώς και Κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων.

Επίσης, απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους εφαρμογής ή τους τυχόν εκπροσώπους τους και δίδει κατά την κρίση της δημοσιότητα σε αυτές, και υποστηρίζει τα επαγγελματικά σωματεία και λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία στην κατάρτιση κωδίκων δεοντολογίας σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα.

Τέλος, η Αρχή γνωμοδοτεί για κάθε ρύθμιση που αφορά στην επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

➤ **Αρμοδιότητες Δημοσιοποίησης-Απολογισμού Συνεργασιών**

Οι κύριοι επικοινωνιακοί στόχοι της ΑΠΔΠΧ αφορούν την ενημέρωση και την ευαισθητοποίηση των υποκειμένων των δεδομένων καθώς και των υπεύθυνων επεξεργασίας ως προς τα δικαιώματα και τις υποχρεώσεις τους. Προς τούτο η Αρχή:

1. Συντάσσει κάθε χρόνο έκθεση για την εκτέλεση της αποστολής της κατά το προηγούμενο ημερολογιακό έτος.
2. Ανακοινώνει στη Βουλή παραβάσεις των ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
3. Συνεργάζεται με αντίστοιχες αρχές άλλων κρατών μελών της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της.

[28]

**Επίλογος / Συμπέρασμα**

Μετά από την παραπάνω μελέτη και έρευνα, που πραγματοποιήθηκε στα πλαίσια της Πτυχιακής Εργασίας, προτείνεται μια ολοκληρωμένη λύση στην επιχείρηση, για την διαχείριση νευραλγικών αναγκών της Διοίκησης Ανθρώπινων Πόρων, μέσω της Τεχνολογίας των Βιομετρικών Συστημάτων. Μια λύση που δεν θα ήταν εφικτή χωρίς τη συμβολή ενός Ηλεκτρολόγου Μηχανικού.

Το θετικό της πρότασης που έχει αναλυθεί είναι ότι αφορά ένα Σύστημα με πληθώρα επιλογών, δυνατότητα αναβάθμισης και προσαρμογή σε οποιοδήποτε περιβάλλον χρειαστεί, ανάλογα με τις απαιτήσεις της επιχείρησης. Ένα Σύστημα, το οποίο έχει μια συνεχή ανάπτυξη και μπορεί να συμβαδίσει με τις εξελίξεις της τεχνολογίας.

Εάν κάθε επιχείρηση πραγματοποιούσε την τοποθέτηση – εγκατάσταση ενός τέτοιου Βιομετρικού Συστήματος Αναγνώρισης θα ήταν σε θέση να εξοικονομήσει πολύτιμο χρόνο από το προσωπικό και τα στελέχη της Διοίκησης Ανθρώπινων Πόρων αλλά και από το προσωπικό και τα στελέχη Ασφάλειας που κατέχει.

Θα είχε μια πιο αποτελεσματική οργάνωση που θα σήμαινε ταυτόχρονη αύξηση της παραγωγής διότι, για παράδειγμα δεν θα χρειαζόταν να επιβαρύνει το προσωπικό της με πολύωρες συζητήσεις και συμπληρώσεις εγγράφων σχετικά με τις ώρες εργασίας που έχουν συμπληρωθεί αλλά και τις υπερωρίες που χρειάστηκαν να γίνουν απρογραμματίστα. Επίσης θα αποφεύγονταν τυχόν λάθη ή παραλείψεις, τα οποία θα οδηγούσαν στη δυσαρέσκεια του προσωπικού. Ακόμα θα είχε αντιμετωπιστεί και κάθε τυχόν κίνδυνος, όπως για παράδειγμα το να μπει κάποιος μη εξουσιοδοτημένος επισκέπτης στους χώρους της επιχείρησης.

Άρα, η χρήση των Βιομετρικών Συστημάτων Αναγνώρισης Προτύπων και ιδιαίτερα η Αναγνώριση των Δαχτυλικών Αποτυπωμάτων που εξετάζονται στην Πτυχιακή Εργασία, είναι σε θέση να καλύψει τις ανάγκες ή και τα προβλήματα μιας επιχείρησης που την ‘κρατούν πίσω’ όσον αφορά θέματα παραγωγής, ανάπτυξης, επέκτασης και ευχαρίστησης του προσωπικού.

Η τοποθέτηση – εγκατάσταση του Συστήματος αυτού κρίνεται πλέον αναγκαία στις μέρες μας καθώς οι απαιτήσεις όλο και αυξάνονται.



**BIBΛΙΟΓΡΑΦΙΑ**

[01]Maltoni D., Maio D., Jain A.K. and Prabhakar S., “Handbook of Fingerprint Recognition Second Edition,” Springer-Verlang London Limited, 2009.

[02]S. C. Dass, A. K. Jain and X. Lu, “Face Detection and Synthesis Using Markov Random Field Models” Proc International Conference on Pattern Recognition, Quebec City, August 11-15-2002.

[03]Σ . Κατσίκας- Δ. Γκρίτζαλης- Στ. Γκρίτζαλης ‘Ασφάλεια Πληροφοριακών Συστημάτων’ , Εκδόσεις Νέων Τεχνολογιών, 2004

[04]Δρ. Ελευθέριος Μπόβιος ‘Σημειώσεις Εφαρμοσμένης Ασφάλειας Πληροφοριακών Συστημάτων’ Τμήμα Πληροφορικής Σ.Τ.Ε.Φ. ΑΤΕΙ Θεσσαλονίκης, 2004

[05][www.techlife.gr/computing](http://www.techlife.gr/computing)

[06][http://www.dpa.gr/APDPXPortlets/images/menu\\_2ndlined2.jpg](http://www.dpa.gr/APDPXPortlets/images/menu_2ndlined2.jpg)

[07][http://www.businessweek.com/technology/content/jun2003/tc2030620\\_3373\\_19.htm](http://www.businessweek.com/technology/content/jun2003/tc2030620_3373_19.htm)

[08]<http://www.bankersonline.com/articles/bhv012/bhv09n12a2.html>

[09]<http://www.privacy.org/pi/>

[10]<http://www.inbiometrics.com/biometriclibrary.htm>

[11]<http://www.biometricsolutions.com/>

[12]<http://www.biometricgroup.com/>

[13][http://www.angelfire.com/nt/selcukgun/en/tran\\_2.htm](http://www.angelfire.com/nt/selcukgun/en/tran_2.htm)

[14]A. K. Jain and S. Pankanti, “Biometrics Systems Anatomy of Performance”, IEICE Trans Fundamentals Vo L.E00, No 1 January 2001

[15]<http://www.channelinsider.com/c/a/Security/Are-Enterprises-Ready-for-Biometrics-as-a-Security-Solution>

[16][http://www.findbiometrics.com/Pages/iris\\_retinal.html](http://www.findbiometrics.com/Pages/iris_retinal.html)

[17]<http://www.channelinsider.com/c/a/Security/Are-Enterprises-Ready-for-Biometrics-as-a-Security-Solution>

[18]Gail R. Light, “ Security vs Liberty: weighing the options” MSU Today, June20, 2002.

[19]“Coming Soon: ATMs That Recognize Your Eyes”, The Christian Science Monitor, 2 December 1997

[20]“Coming Soon: ATMs That Recognize Your Eyes”, The Christian Science Monitor, 2 December 1997

[21][http://www.findbiometrics.com/Pages/iris\\_retinal.html](http://www.findbiometrics.com/Pages/iris_retinal.html)

[22]J. Gonzalez-Rodriguez, J. Fierrez-Aguilar, J. Ortega-Garcia, and J.J. Lucena-Molina, “Biometric Identification in Forensic Cases According to the Bayesian Approach”, 28 May 2002

[23][http://en.wikipedia.org/wiki/Automated\\_fingerprint\\_identification](http://en.wikipedia.org/wiki/Automated_fingerprint_identification)



[24] A. K. Jain S. Prabhakar, and A. Ross, “Biometrics-Based Web Access”.

[25] <http://www.emory.edu/BUSINESS/et/biometric/Biometrics.htm>

[26] <http://www.eett.gr/opencms/opencms/EETT/FAQS/DigitalSignatures/>

[27] [http://www.businessweek.com/technology/content/jun2003/tc2030620\\_3373\\_19.htm](http://www.businessweek.com/technology/content/jun2003/tc2030620_3373_19.htm)

[28] [http://www.dpa.gr/portal/page?\\_pageid=33,123437&\\_dad=portal&\\_schema=PORTAL](http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL)

**ΠΑΡΑΡΤΗΜΑ**

1. Χαρακτηριστικά & Λεπτομέρειες Μηχανήματος Ωρομέτρησης (566260\_Anviz-A300-Catalogue)
2. Manual Συστήματος Αναγνώρισης Δαχτυλικών Αποτυπωμάτων A300 της Anviz (535909\_User\_Manual\_V1.5\_EN)
3. Γρήγορος Οδηγός Σύνδεσης Συστήματος Anviz (96891\_A\_Series\_EN\_Quick\_Guide)
4. Κάτοψη Επιχείρησης σε μεγάλη κλίμακα
5. Πιστοποιητικά Εταιρείας Anviz & Συστήματος Αναγνώρισης και Ωρομέτρησης Anviz A300





1.

*Χαρακτηριστικά*

*&*

*Λεπτομέρειες Μηχανήματος  
Ωρομέτρησης*

*(566260\_Anviz-A300-Catalogue)*





# A 300

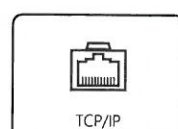
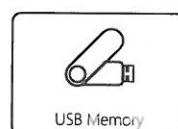
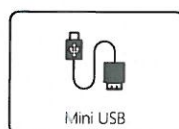
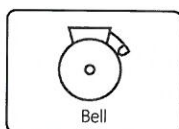
Fingerprint & RFID Time Attendance

EMII



## Exquisite Time Attendance Solution

A300 employs Anviz's industry-leading fingerprint algorithm BioNANO. With a waterproof, dustproof and scratchproof fingerprint sensor, A300 offers a perfect time-attendance solution. Whenever you need to get the employee in and out records, everything can be easily acquired through a USB cable- no driver needed, just a USB pen drive or TCP/IP network.







## BioNANO - The core algorithm

BioNano is applied in all Anviz biometric-based products used for identification.

### BioNANO

#### Core Algorithm

Fingerprint - Facial - Iris

- Independent research and development
- Suitable for both wet and dry fingers
- Automatically heals the broken lines in fingerprint images
- Extraction of features in worn fingerprints
- Fingerprint template auto update

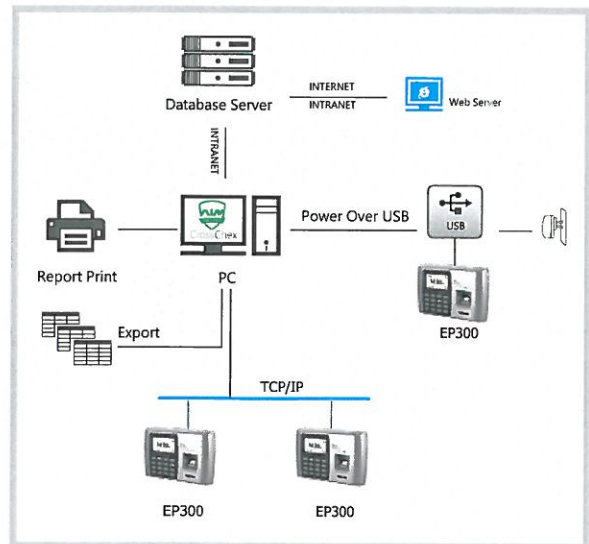
## Technical Specifications

Item	Description
Processor	32-bit ARM MCU
Algorithm	BioNANO
Sensor	AFOS
Scan Area	22mm*18mm
Resolution	500 DPI
LCD	128*64 White LCD
Fingerprint Capacity	2,000
Card Capacity	2,000(Optional)
Log Capacity	50,000
Identification Mode	FP, Card, ID+FP, ID+PW, PW+Card, FP+Card
Identification Time	<0.5 Sec
FRR	0.001%
FAR	0.00001%
Communication Interface	TCP/IP, Mini USB, USB Memory, Optional RS232
Relay Out	Yes(For schedule bell)
Card Reader Module	125KHZ EM RFID
Fingerprint Image Display	Yes
Self-defined Status	8 different customizable
Dimensions(WxHxD)	200 x 140 x 38mm(7.87x5.51x1.5")
Temperature	-30°C ~60°C
Certificate	CE, FCC, RoHS
Soft	Anviz Crosschex Standard

## Features

- ▶ 2,000 Fingerprints, 50,000 Records
- ▶ TCP/IP, Mini USB & USB Memory, Optional RS232
- ▶ Relay Output
- ▶ Power Over USB or DC 5V
- ▶ 8 Customizable T&A States, 6-digit Work Code
- ▶ FP, Card ID+FP, ID+PW, PW+Card, FP+Card, FP+PW
- ▶ Optional EM/Mifare Card

## Network Access Control System



## CrossChex

Time Attendance and Access Control Management System



**Employee**  
Unify Employee management



**Shift**  
Manual and intelligent shift schedule



**Device**  
Quick Add, Easy Setting



**Export**  
Flexible and Practical Report output



Easy to Operate



Simple to Install



Enhanced Security



Types of Reports

For more information, visit [www.anviz.com](http://www.anviz.com), or email us [sales@anviz.com](mailto:sales@anviz.com).

2016© Anviz Global. All Rights Reserved. Due to the consistent improving of the product, this specification and appearance is subject to change without notice.





2.

*Manual*

*Συστήματος Αναγνώρισης  
Δαχτυλικών Αποτυπωμάτων*

*A300 της Anviz*

*(535909\_User\_Manual\_V1.5\_EN)*







# User Manual

**(V1.5)**

Models: D100/D200/Aseries/EPseries/  
TC550/OC500/T60/VF30/VP30/TC530



## PREFACE

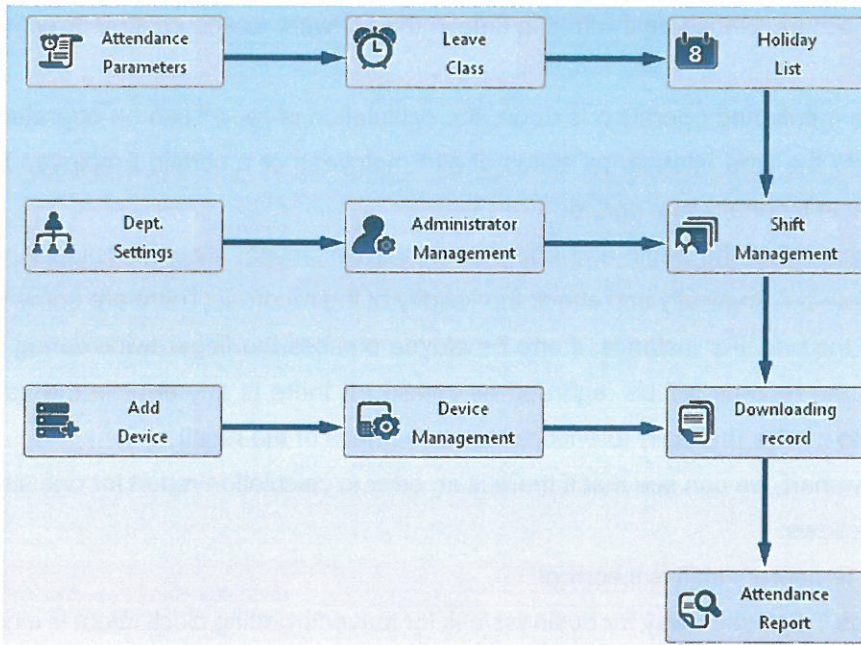
Honorable customers:

Thank you for choosing products from Anviz Technology Co.,Ltd. Our products contain world cutting edge technologies like Fingerprint/Iris/card Recognition and other biometric recognitions, Surveillance, Computer Communication, as well as Microelectronics. With the combination of three technologies: Electronics, Optics, and Computer Communication; Anviz Technology Co.,Ltd. is fast becoming the first choice for standalone time & attendance products for enterprises with its strong functions and veracity. Please read the user manual carefully before installation. You will have a general understanding of product functions and basic knowledge of installation, debugging, maintenance, application and management to better use this product.

Our product adopts the latest fingerprint and RFID recognition technology. It will bring enterprises the unparalleled reliability and convenience. In which users will get many benefits from using our products.


## Software Operation Flowchart

This software includes: Attendance parameter, Department settings, Administrator management, Device management, Leave class, Holiday List and Attendance report etc. Then how to use this system in a right way? It is far from enough to understand only the function of each module but to know the connections between them and the system operation flowchart. Thus, a correct report can be generated. Software operation flowchart can be described in brief as follows:



1. When the software is run for the first time, please set parameters including department name, time attendance rule, statistic rule for early, late and overtime, leave class etc. When the setting is completed, it is usually not needed to be modified unless the management rules of this company changes.
2. Normally there are many departments in one company and all departments need to be entered manually unlike the directly import of Employee. Department setting should be completed before Employee maintenance.
3. When the software is used for the first time, please make an MS Excel file (\*.xls) for company



Employee in accordance with certain format. For the format, please refer to  so that all Employee can be imported to the system at one time. Employee can be added, deleted, modified and transferred to new department during future use.

4. First add the proper scheduling (from on-duty time to off-duty time) according to the company rule and then set shifts.



5. After the shift setting is completed, it will work until shift is allocated to Employee. Each Employee can only have one shift. Please note the starting date of the shift. After the allocation of the shift, the arranged working date and time can be seen clearly for each Employee.
6. Attendance records are stored in the time attendance unit. Please download the records from the unit before report calculation. In addition, staff information and fingerprint templates can be uploaded and downloaded between the unit and the computer.
7. There is always staff away for business, asking for leave and forgetting clock happening in a company. Once it occurs, please deal with it in time in the software to ensure the correctness of the statistic report.
8. After all the above mentioned operation is done, the calculation of report can be operated. The report can calculate the time attendance status of all Employees or a certain Employee from a certain department in a certain time period.

In [Attendance], first please select the begin and end date of the Employee, click 'Statistical Analysis' and the system will calculate automatically and check the validity of the records. (There are some invalid records during the use of the unit. For instance, if one Employee presses the finger twice during a very short time period, one of the records will be regarded as invalid.) If there is any error in the software calculation, admin can also modify manually to ensure the correctness of the result.

**Note:** From the above flowchart, we can see that if there is an error in calculation report for one staff, the possible reasons are as follows:

- Employee shift or temporary shift is incorrect.
- Exceptions such as Employee away for business/ask for leave/forgetting clock in/out is incorrect.
- Checking and calculation of transaction records is incorrect.

## CONTENTS

1.	Notice For User .....	2
1.1	Security Considerations .....	2
1.2	Illustration for Pressing Fingerprint ★ .....	2
2.	Operation Guide .....	5
2.1	Menu List ★ .....	5
2.2	Button Instruction .....	6
2.3	Time Attendance Status .....	6
2.4	User .....	6
2.4.1	User Enroll .....	6
2.4.2	User Deletion .....	9
2.4.3	Verify Mode .....	9
2.4.4	Group Setup ★ .....	10
2.4.5	Admin Setup .....	11
2.4.6	Admin Clear .....	12
2.5	Setup .....	13
2.5.1	System Setup .....	14
2.5.2	Log Setup .....	27
2.5.3	Re-Verify Time .....	28
2.5.4	Hardware Test .....	28
2.6	USB Flash ★ .....	30
2.6.1	New Log Backup .....	30
2.6.2	All Log Backup .....	30
2.6.3	User Backup .....	30
2.7	System Info ★ .....	31
2.8	T&A Status Setting .....	32
2.9	Shut Down .....	32
3.	FAQ .....	34
3.1	Fingerprint has enrolled but often gets failure in identification. ....	34
3.2	No records found though staff have clocked in/out. ....	34
3.3	The machine cannot connect with PC. ....	34
3.4	Clock's time works fine, but FP scanner is off, Employee cannot attendance ....	35
3.5	We do not use the ID + fingerprint mode to verified. ....	35
3.6	The unit beeps automatically when no one punches in/out. ....	35

**Note:** ★ This mark represents the special model function which differs from the different devices, so it may be determined by the actual function of the device.



## **Chapter1. Notice For User**

It's a comprehensive manual. Some specific functions are subject to actual device.

Models:D100/D200/Aseries/EPseries/TC550  
/OC500/T60 /VF30/VP30/TC530.



# 1. Notice For User

## 1.1 Security Considerations

Please read carefully before using the manual:

1. Please read it carefully first of all;
2. Don't install the terminal under direct light, humid, dusty or sooty environment;
3. Don't install the terminal near the magnetic field;
4. Don't install the terminal near the calefaction device;
5. Don't sprinkle the liquid (water, drink, chemistry) on the terminal;
6. Always keep the surface of the terminal clean;
7. Clear the terminal by towel when there is water on the surface;
8. Don't break the terminal;
9. Don't press two keys at the same time;
10. Don't take down, repair or change the terminal without authorization;
11. Don't allow children to touch the terminal;
12. This terminal is only used for fingerprint verification, don't use it for other purposes;
13. If in doubt, please contact the local distributor;

## 1.2 Illustration for Pressing Fingerprint ★

**Correct method:**



Place the center of the finger on the center of scanner window.

**Wrong method:**



Too less valid area   Too left   Too right   Defluxion   Too down



**Note:**

1. It is better for each user to register two finger prints in case of one finger can't work.
2. Place finger flatly and the center of the finger is on the center of scanner window and press a little hard on scanner so it can scan as large finger area as possible to extract enough minutia.
3. Keep the angle and direction of finger the same each time placing on scanner.
4. If your finger has sweat or water, please make it dry first and then register.
5. If your finger is too dry, make it a little wet or touch the forehead to increase oily of the finger, press a little hard on scanner. (The dry finger can cause the finger image not clear .)
6. Avoiding the callus , peeling or injury of the finger to ensure the register and identification successful.
7. You'd better register the thumb first , then index finger or middle finger to increase the precision.

## **Chapter2.** Operation Guide

This chapter is mainly about appearance illustration and relevant system settings such as how to add and delete users etc.





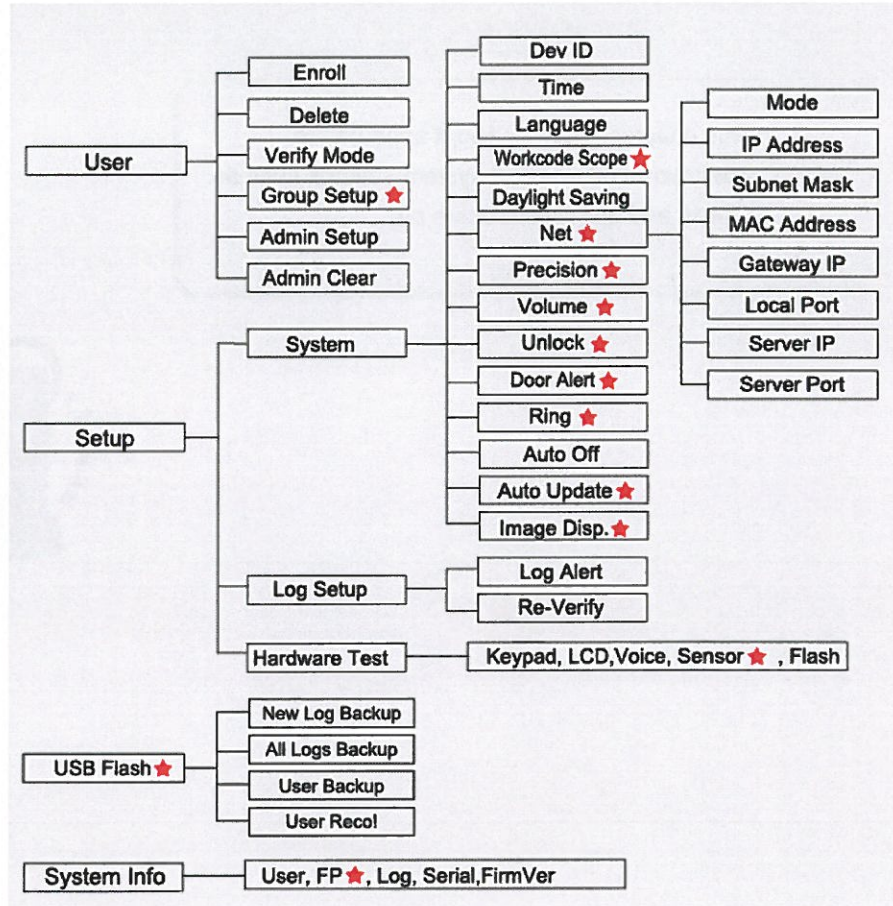
## 2. Operation Guide

### 2.1 Menu List★

Press [M] key to enter system management menu.

(This requires the administrator authorization if there is admin registered in the system.)

Menu List:



Note: ★ mark for special model function.

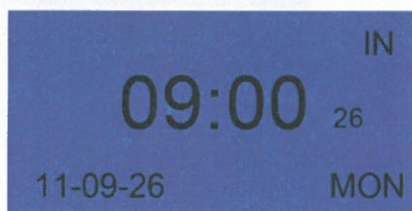
## 2.2 Button Instruction

Button	Function	Button	Function
[Fn]	Work Code	[M]	Menu
[OK]	Confirm	[C]	Delete / Exit
[☉]	Power	[1-9]	Number
[<IN] [OUT>] [▲][▼]	Status/Navigate Key		

**Note:** [C] also is work code function for T60 device.★

## 2.3 Time Attendance Status

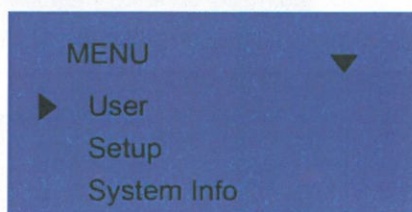
Standby status we can run: time attendance, status setting, entering management mode and power off operation.



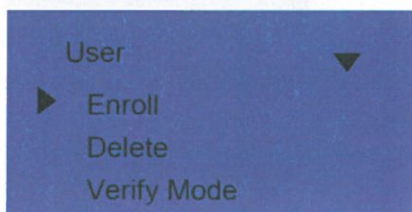
## 2.4 User

Employee info management includes user registration, user deletion; verify mode, group setting, manager setup and deletion.

Press [M] to enter system management mode. Select [User] option with [<IN] or [OUT>] key.



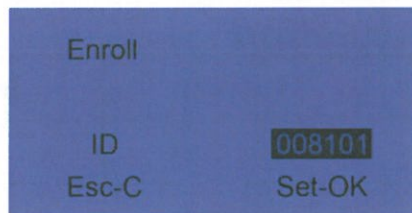
Press [OK] button to enter the sub-menu.



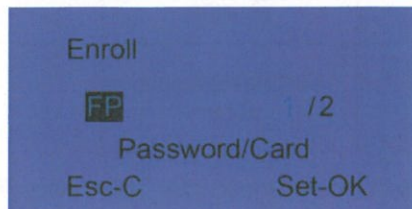
### 2.4.1 User Enroll

Select [Enroll] option and press [OK] to enter user registration interface. Input user ID, i.e. 8101





Press [OK] to continue.

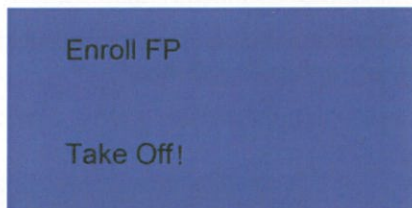


**Fingerprint registration:★**

Press [◀ IN] or [OUT ▶] key to select 1 or 2, 1 is to register the 1st FP, 2 is for 2nd FP.  
Press [OK] to continue.



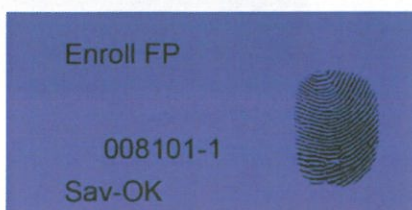
Place the finger on sensor scanner. Please follow the screen prompts to register the fingerprint.



Remove finger, the system will prompt.



Place the same finger on sensor scanner again. After scanning successfully, the system will prompt as follow:

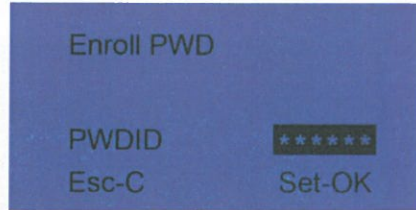


Press [OK] to save fingerprint. Press [C] back to user registration interface.

The 2nd finger registration as the same steps as above.

**Password registration:**

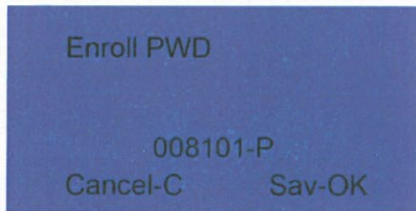
Press [◀ IN] or [OUT▶] key to [Password] option. Press [OK] to continue.



Please Input 1-6 digits as password. Press [OK] to confirm and input same password again. The system will prompt:



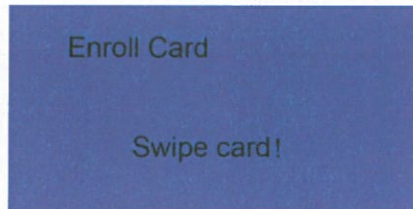
Press [OK] to save interface.



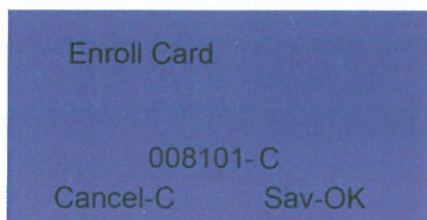
Press [OK] to save password. Press [C] to cancel and exit back to user registration interface.

**Card registration:**

Press [◀ IN] or [OUT▶] key to [Card] option. Press [OK] to continue.



Swipe the ID card on card reader area. The terminal will get card number and enter save interface.



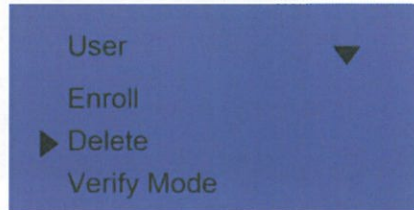
Press [OK] to save, press [C] to cancel and exit back to user registration interface.



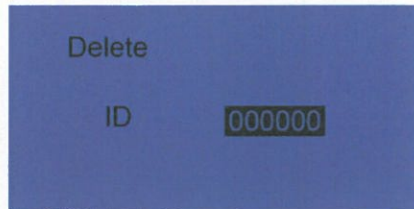
### 2.4.2 User Deletion

When there are employees leaving, we need to delete these employees to free more memory space.

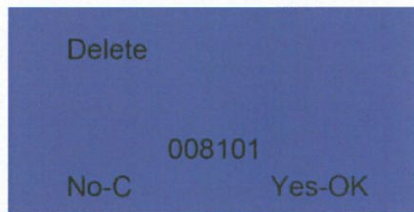
In [User] menu, press [◀ IN] or [OUT ▶] to select [Delete] option.



Press [OK] key to enter user deletion interface.



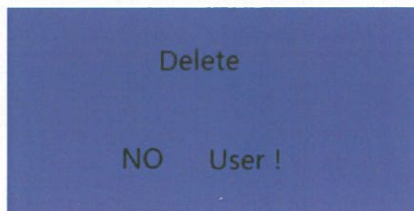
Input employee ID to delete. Press [OK] enter delete confirm interface.



Press [OK] to confirm delete. Press [C] to cancel.

**Note:** Employee deletion will delete all information of the employee and can't be resumed. Please take caution!

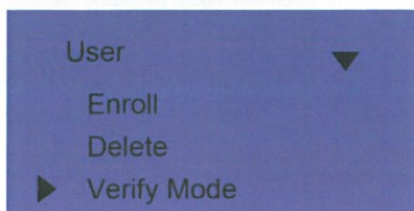
When machine do not have this employee ID, the system will prompt as follow:



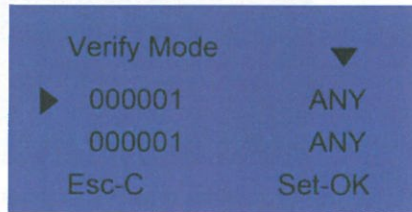
### 2.4.3 Verify Mode

Setting verify mode of the employee, there are four modes: SEPT, RF+PW, PW+FP, and RF+FP.

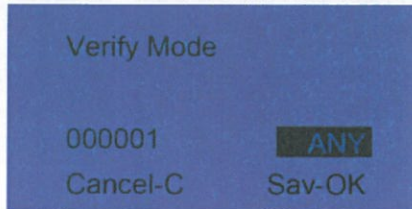
In [User] menu, press [◀ IN] or [OUT ▶] key to select [Verify Mode] option:



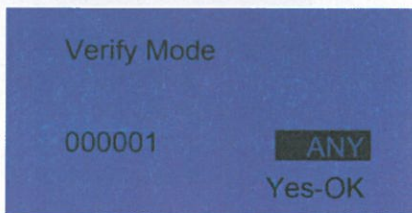
Press [OK] key to enter setting interface:



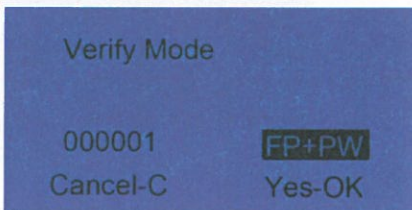
Press [◀ IN] or [OUT▶] key to select employee's ID or press [OK] to input user ID:



After input user ID, press [OK] to enter setting interface.



Setting employee's verify mode through [◀ IN] or [OUT▶] key, then press [OK] key to confirm and enter save interface:

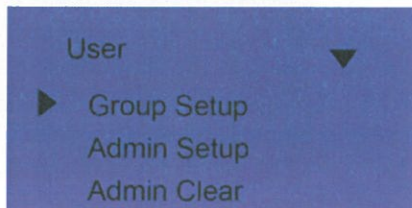


Then press [OK] key to save; Press [C] key to cancel this operation.

#### 2.4.4 Group Setup★

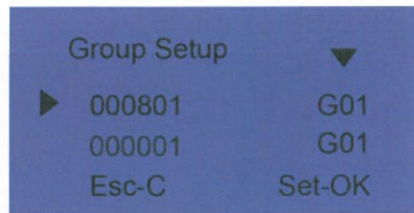
Group is based on time zones. One group can set max 4 time zone. There are supply 16 groups. Normally, system will default group 0 as normal close, group 1 as normal open.

In [User] menu, press [◀ IN] or [OUT▶] key to select [Group Setup] option.

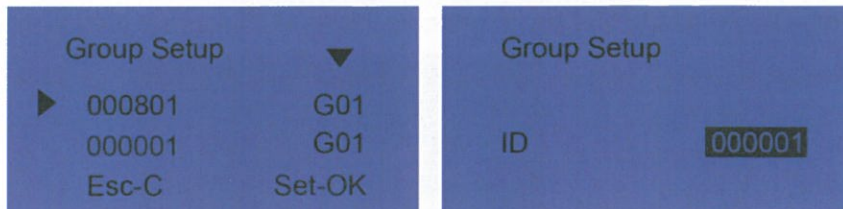


Press [OK] key to enter group setup interface.

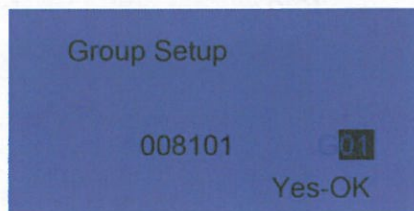




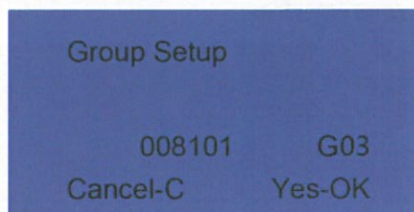
Press [◀ IN] or [OUT▶] key to select user ID or press [OK] to input user ID manually.



After input user ID, press [OK] to enter group interface.



Group number can be input through [◀ IN] or [OUT▶] key or number key. (Max group number is 16 ). Press [OK] key to confirm and enter save interface.

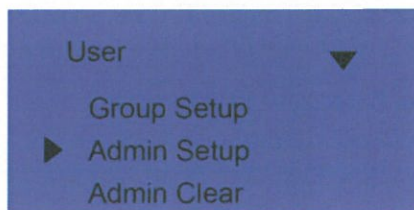


Then press [OK] key to save employee' group settings. Press [C] key to cancel this operation as well.

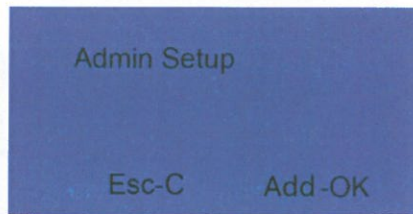
### 2.4.5 Admin Setup

To prevent illegal operation, we need to set device admin to enter menu.

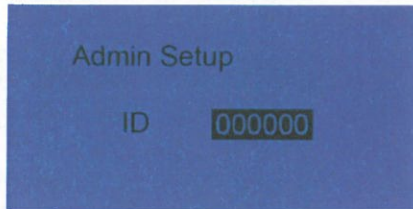
In [User] menu, press [◀ IN] or [OUT▶] key to select [Admin Setup] option:



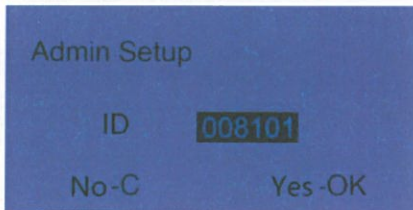
Press [OK] key to enter [Admin Setup] interface.



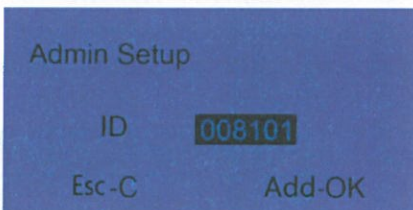
Press [OK] to start adding admin.



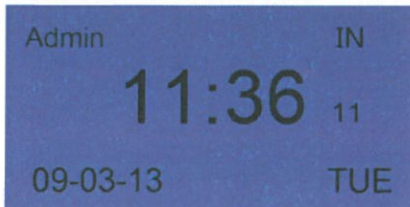
Input the user ID i.e. 8101. Press [OK] key to enter admin setup save interface.



Press [OK] key again to confirm saving. After adding completed, exit to admin setup interface.

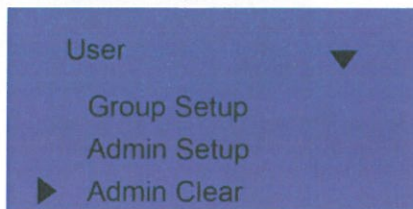


You can press [OK] key to continuously add other admin, and press [C] to exit as well. After adding admin, it needs the verification of the administrator's fingerprint to enter Menu. The interface is as following:



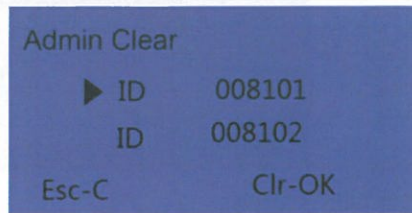
#### 2.4.6 Admin Clear

Select [Admin Clear] option in [User] menu.

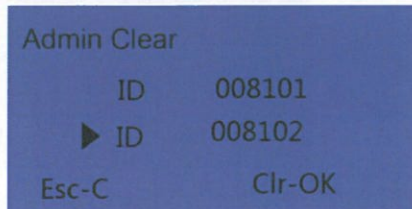




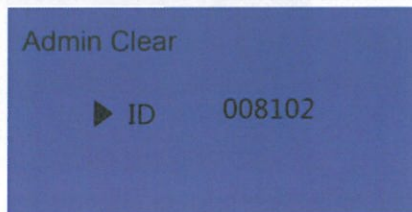
Press [OK] to enter admin clear interface.



Press [◀ IN] or [OUT▶] key to choose the admin ID to be deleted, i.e. 8102:

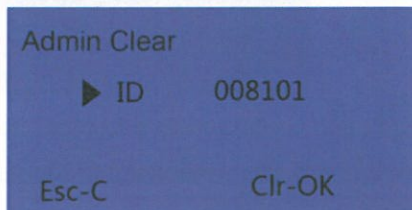


Press [OK] key to confirm the admin ID.



**Note:** in admin clear interface, you can press [OK] key to input admin ID and delete it manually.

Press [OK] key again and confirm to delete manager 8102. Then exit to manager clear interface.

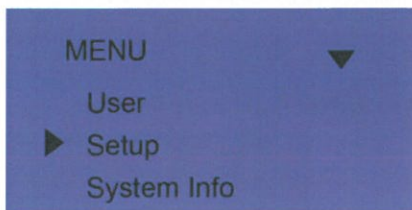


Press [OK] key to delete manager continuously. Press [C] key to exit manager clear interface as well.

## 2.5 Setup

[Setup] menu mainly includes [system], [log setup] and [Hardware Test].

Enter management menu, press [◀ IN] or [OUT▶] key to select [Setup] option.

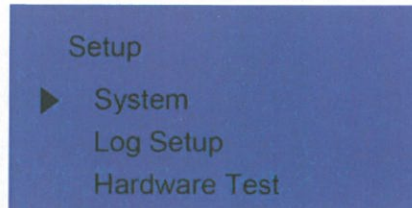


Press [OK] key to enter [Setup] sub-menu. Press [◀ IN] or [OUT▶] key to shift menu.

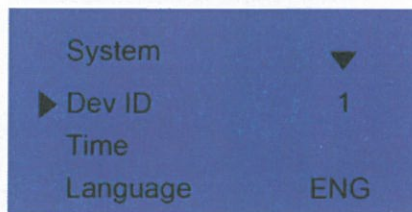
## 2.5.1 System Setup

### 2.5.1.1 Device ID

In [Setup] menu, press [◀ IN] or [OUT ▶] key to enter [System] setup option.



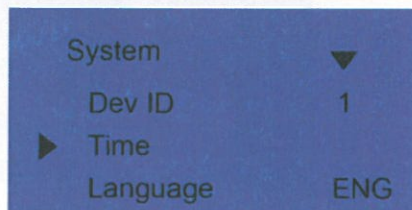
Press [OK] key to enter system setting sub-menu.



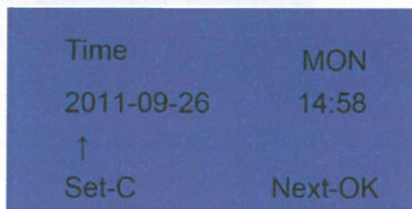
**Note:** Device ID range is 0-99999999, and default is 1. (Device ID must enter as same as in the communication software), When the device as "0", must use the lasted 8 digit of the serial number to communication with software.

### 2.5.1.2 Time

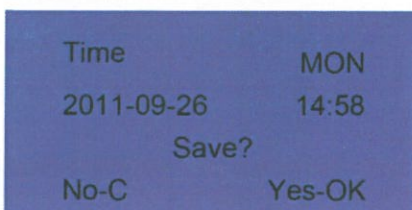
Press [◀ IN] or [OUT ▶] key to select [Time] option,



Press [OK] key to enter time setting interface.



You can press the [OK] key to move the cursor to shift the year, month, day. And use number and [◀ IN] or [OUT ▶] key adjust the time. After setting completed, press [C] key and enter system time save interface.

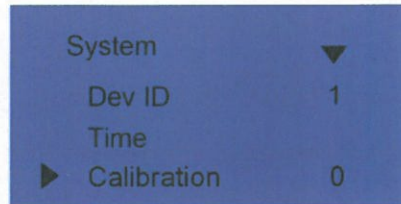




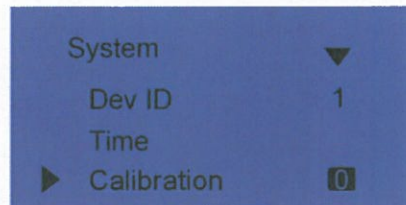
Press [OK] key to save system time. Press [C] key to cancel and exit to upper menu.

### 2.5.1.3 Calibration★

In [System], press [◀ IN] or [OUT▶] key to select [Calibration] option.



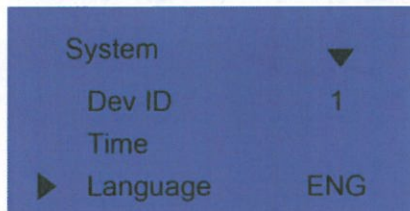
Press [OK] key to enter the time setting (Time unit: second).



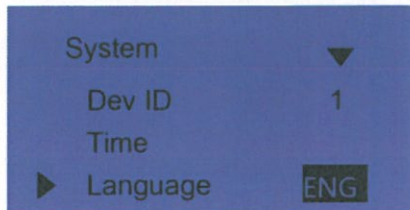
You can press [◀ IN] or [OUT▶] key to get the calibration time you need. And press [OK] to confirm. Then you can continue to do other function settings.

### 2.5.1.4 Language

In [System], press [◀ IN] or [OUT▶] key to select [Language] option.

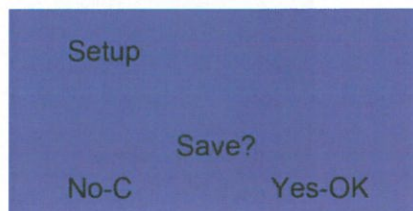


Press [OK] key to enter language setting interface.



You can press [◀ IN] or [OUT▶] key to switchover the language. And press [OK] to confirm.

Then you can continue to do other function settings. And press [C] key to enter setting save interface.

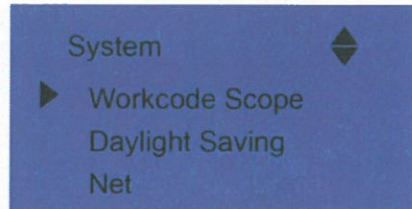


Press [OK] key to save system setting. Press [C] to cancel and exit to upper menu.

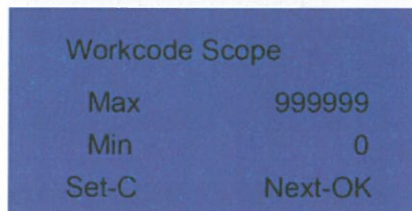
### 2.5.1.5 Work Code Scope★

Work code is a code for different work. Use for device supply a parameter to label an attendance record as which kind of the work. It is easy for count attendance time for different work. The scope of the work code is: 0-999999. It is an invalid when over this scope.

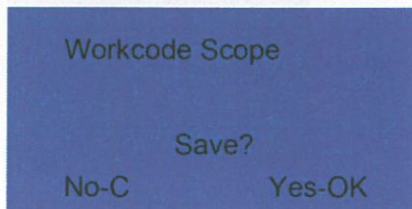
In [System], press [◀ IN] or [OUT ▶] key to select [Work code scope] option.



Press [OK] key to enter work code scope interface.



When you finish setting, press [C] key enter save interface.

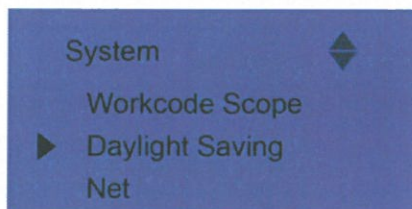


Press [OK] to confirm and save.

### 2.5.1.6 Daylight Saving

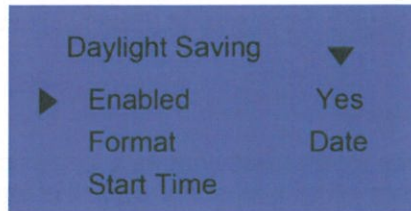
Automatically switch daylight saving time base on week or date.

In [System], press [◀ IN] or [OUT ▶] key to select [Daylight Saving] option.

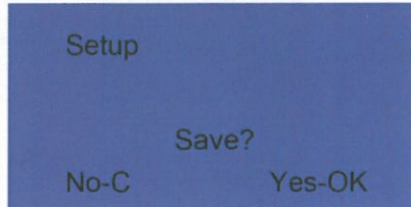


Press [OK] key to enter Daylight Saving interface:





When you enable “Daylight Saving” function you need select week or date format first. Then you need set the time point for “Daylight Saving” start time and end time. And press [C] key enter save interface.

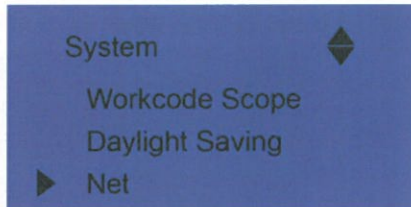


Press [OK] to Confirm and save.

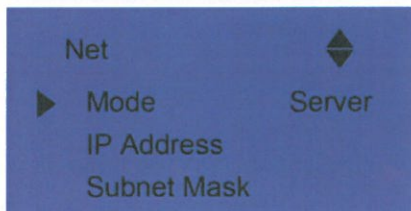
### 2.5.1.7 Net ★

Network setting main includes [IP Address], [Subnet Mask], [MAC Address] and [Gateway IP] settings.

In [System], press [◀ IN] or [OUT ▶] key to select [Net] option.



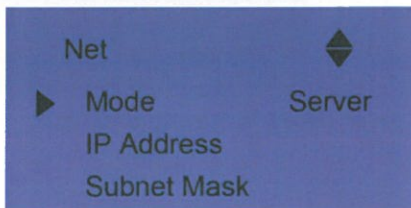
Press [OK] key to enter net parameter interface.



#### Mode:

There are two modes for networking.

Press [◀ IN] or [OUT ▶] key to select [Server] or [Client].

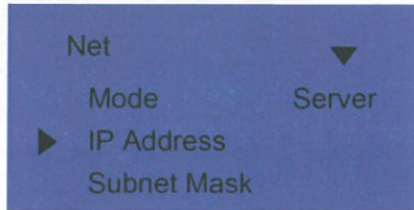


Server: Normal net mode;

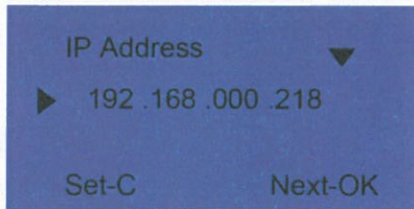
Client: Only communication with the PC which has server IP.

**IP Address**

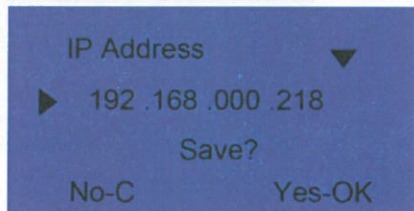
Press [◀ IN] or [OUT ▶] key to select [IP address] option:



Press [OK] key to enter IP address setting interface:



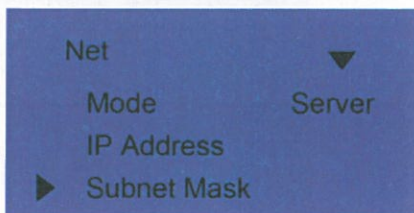
Press [◀ IN] or [OUT ▶] key or number key to input IP address. Press [OK] key to shift between the 4 segments. After set is completed, press [C] key to enter IP address save interface.



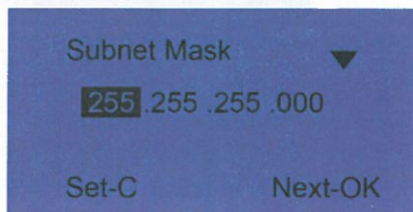
Press [OK] key to save the modification. Press [C] key to cancel.

**Subnet Mask**

Press [◀ IN] or [OUT ▶] key to select [Subnet mask] option.

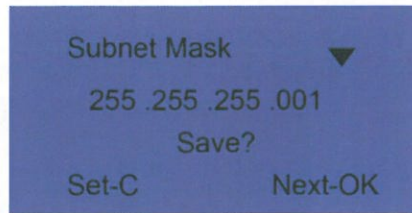


Press [OK] key to enter subnet mask setting interface.



Press [◀ IN] or [OUT ▶] key or number key to input subnet mask. Press [OK] key to shift between the 4 segments. After set is completed, press [C] key to enter subnet mask save interface.

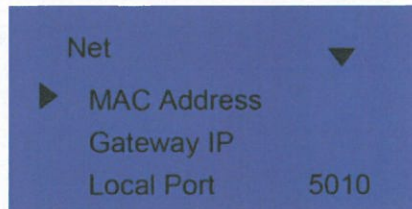




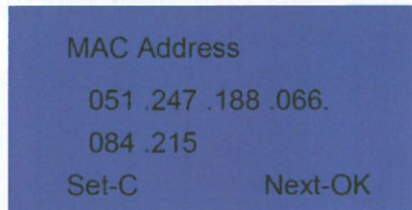
Press [OK] key to save the modification. Press [C] key to cancel.

**MAC Address**

Press [◀ IN] or [OUT ▶] key to select [MAC address] option.



Press [OK] key to enter MAC address setting interface.

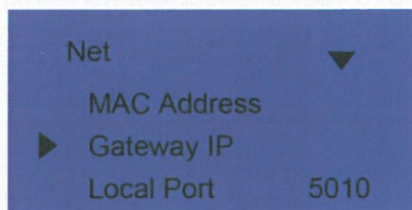


Please do not change the MAC address for device.

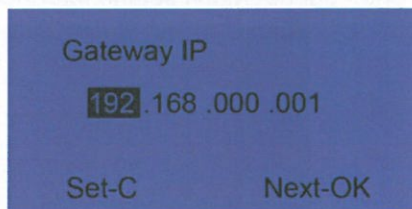
Press [OK] key to save the modification. Press [C] key to cancel.

**Gateway IP**

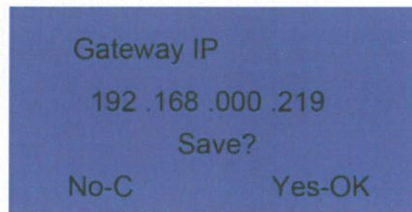
Press [◀ IN] or [OUT ▶] key to select [Gateway IP] option.



Press [OK] key to enter gateway IP setting interface.



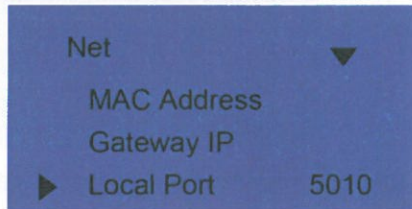
Press [◀ IN] or [OUT ▶] key or number key to input gateway IP. Press [OK] key to shift between the 4 segments. After set is completed, press [C] key to enter gateway IP save interface.



Press [OK] key to save the modification. Press [C] key to cancel.

Local Port:

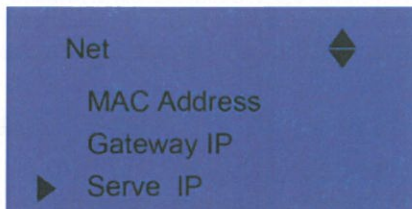
Press [◀ IN] or [OUT ▶] to select [Local Port] option:



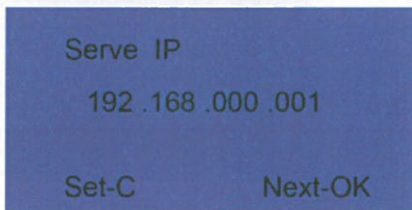
Press [◀ IN] or [OUT ▶] key or number key to input port. After set is completed, press [C] key to enter save interface.

**Server IP address**

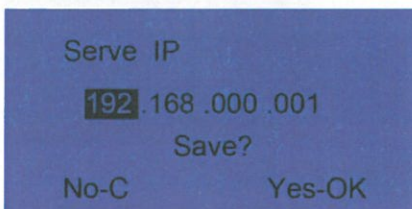
Press [◀ IN]、 [OUT ▶]to select[Server IP]option:



Press [OK] key to enter Server IP setting interface.



Press [◀ IN] or [OUT ▶] key or number key to input server IP. After set is completed, press [C] key to enter save interface.

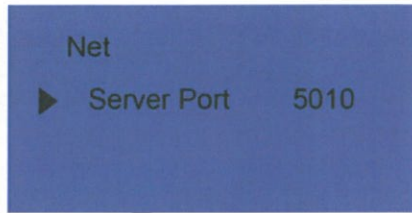


Press [OK] key to save the modification. Press [C] key to cancel.

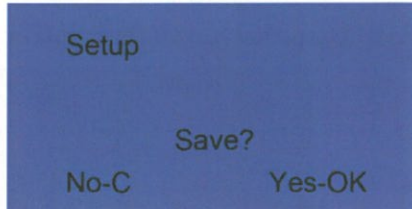
**Server port**

Press [◀ IN]、 [OUT ▶]to select [Server port] option:





Press [◀ IN] or [OUT▶] key or number key to input server port. After set is completed, press [C] key to enter save interface.



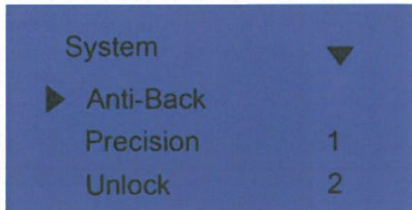
Press [OK] key to save the modification. Press [C] key to cancel.

### 2.5.1.8 Anti-Back ★

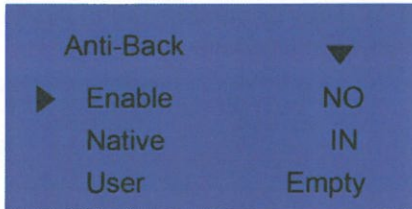
The anti-back feature is designed to prevent misuse of the access control system. The anti-back feature is most commonly used at parking gates and employee entrance doors, where there is both an “in” reader at the entry gate and an “out” reader at the exit gate. The anti-back feature requires that for every use of a card at the “in” reader, there be a corresponding use at the “out” reader before the card can be used at the “in” reader again.

Standalone access control (T60, VF/VP30 etc.) must work with T5s to realize anti-back function.

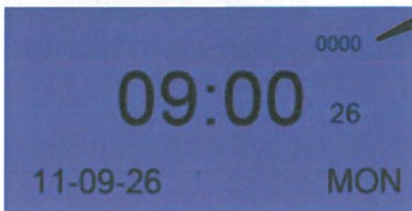
Via [◀ IN] or [OUT▶] select [Anti-Back] option:



Press [OK] to confirm enter “Anti Pass Back” menu.



Enable: Enable or Disable anti-back function.



Stranded

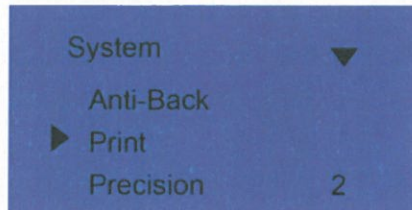
Native: Setting device always as “In” or “Out” states.

Empty User: Clear all the stranded user records which have been accessed in.

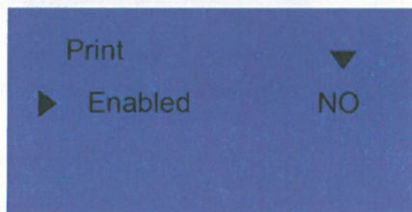
Press [◀ IN] or [OUT▶] key to setting the anti-back function and press[OK]to confirm, then press[C]save and exit.

### 2.5.1.9 Print ★

Via [◀ IN] or [OUT▶] select [Print] option:



Press [OK] to confirm:



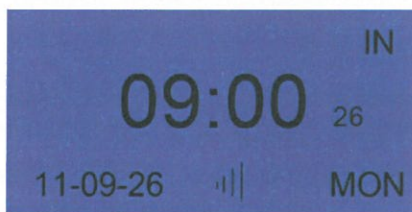
Set up if enabled print function, and then press [C] key to set to be saved.

Printer Settings:

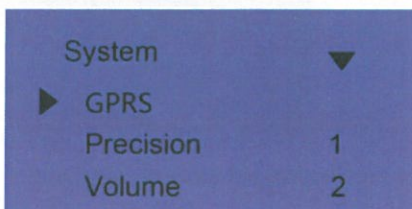
<b>Com Port</b>	Communication or Print function
<b>Baud Rate</b>	Baud Rate:19200 for print function
	Baud Rate:57600 for communication function
<b>Output Code</b>	Font coding for Print

### 2.5.1.10 GPRS★

Insert the standard SIM card. The device will search the GPRS signal.

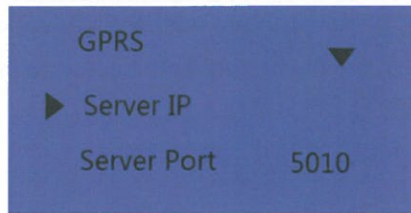


Via [◀ IN] or [OUT▶] select [GPRS] option:



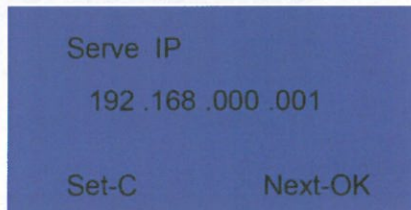


In the GPRS option there are two options:



Server IP: The server IP is the Public IP address (it is from ISP). It is the PC Server IP that the T60/TC530 device will connected with.

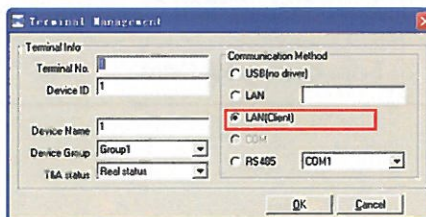
Press 'OK' to enter IP setting interface. And input public IP address.



Server Port: The port is the software communication port. The device will send the attendance data and get commands via this port to attendance software. (The default port is 5010)



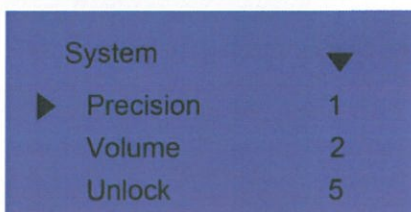
The next step need set the software. In the Prjcomm.exe software interface, Please add a terminal first. Please notice you just select 'LAN(Client)' mode for device GPRS communication.



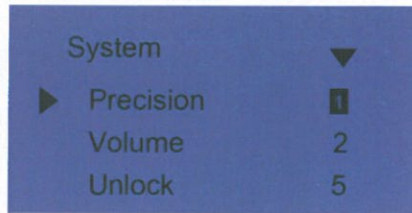
### 2.5.1.11 Matching Precision ★

There are three fingerprint matching precision levels (0, 1, and 2). 0 is lower precision (Basic). 1 is standard precision (Good). 2 is high precision (Excellent).

Press [◀IN] or [OUT▶] key to select [Precision] option.



Press [OK] key to enter precision setting interface.

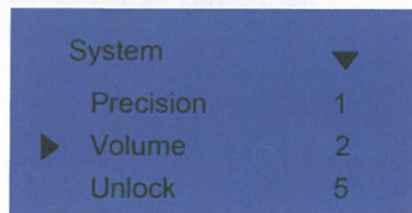


Press [◀ IN] or [OUT▶] key or number key to adjust the precision. Press [OK] key to confirm. Then press [C] to save the setting.

### 2.5.1.12 Volume ★

There are five levels for device's volume, 0-mute, MAX-5

In [System] setup, press [◀ IN] or [OUT▶] key to select [volume] option

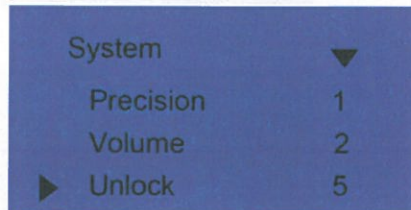


Press [OK] key to enter volume setting interface, Press [◀ IN] or [OUT▶] key set the volume. Press [OK] key to confirm. Then press [C] to save the setting.

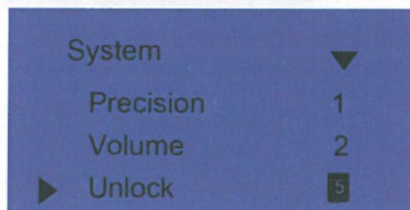
### 2.5.1.13 Unlock ★

Lock delay is the time range since lock open to close after user access granted. 'No' means no delay and the max delay time is 15 seconds.

Press [◀ IN] or [OUT▶] key to select [Unlock] option,



Press [OK] key to enter delay time setting interface,



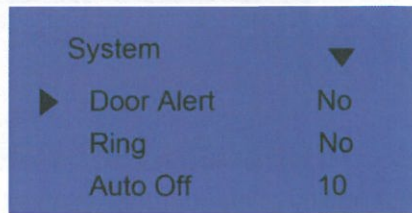
Press [◀ IN] or [OUT▶] key or number key to input delay time. Press [OK] key to confirm. Then press [C] to save the setting.

### 2.5.1.14 Door Alert ★

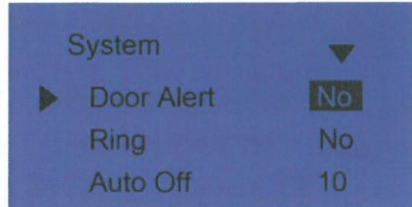
Door alert use for monitor lock whether door was closed after user access. If lock does not close the device will alarm out. The delay time for door alert is 1-99 sec and "No" means disable the door alert function.



Press [◀ IN] or [OUT ▶] key to select [Door Alert] option,



Press [OK] key to enter door alert setting interface,

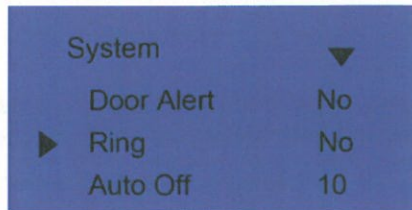


Press [◀ IN] or [OUT ▶] key or number key to input door alert value. Press [OK] key to confirm. Then press [C] to save the setting.

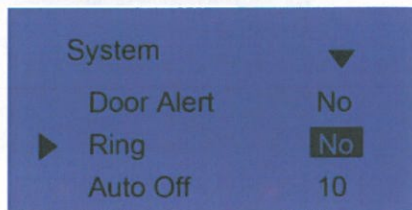
### 2.5.1.15 Ring ★

Ring is the time range for ring delay. "No"- no delay with ring, the max is 15 sec.

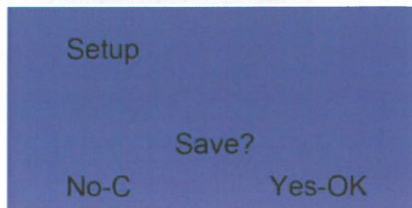
Press [◀ IN] or [OUT ▶] key and shift to [Ring] option,



Press [OK] key to enter Ring setting interface,



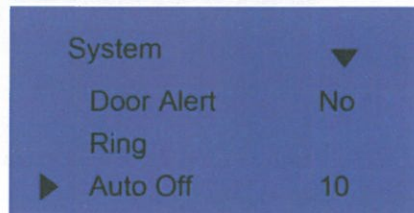
Press [◀ IN] or [OUT ▶] key or number key to input delay time value. Press [OK] key to confirm. Then press [C] to save the setting and press [OK] to be saved.



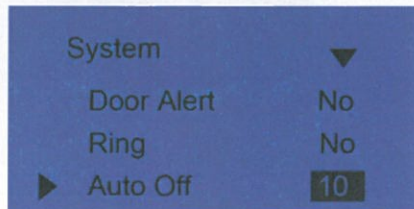
### 2.5.1.16 Auto Off

Auto off is the time period from the last operation on device to coming into dormancy status. Time range is 1-250 minutes. 'No' is no dormancy forever.

Press [◀ IN] or [OUT ▶] key to select [Auto off] option.



Press [OK] key to enter auto off setting interface,

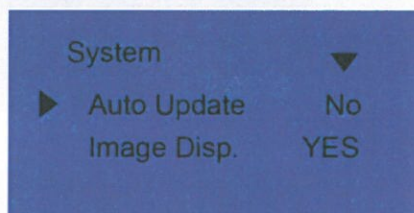


Press [◀ IN] or [OUT ▶] key or number key to input dormancy time. Press [OK] key to confirm. Then press [C] to save the setting.

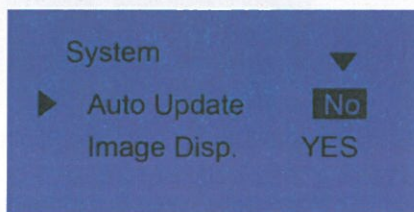
### 2.5.1.17 Auto Update ★

Update the fingerprint template intelligently: During fingerprint sensor identification process, the sensor replaces the lowest-quality data with new, higher-quality data that it acquired in the matching process. This enables the sensor to maintain high quality data at all times, saving the user from repeated authentication attempts.

Press [◀ IN] or [OUT ▶] key and shift to [Auto Update] option:



Press [OK] key to enter auto off setting interface:



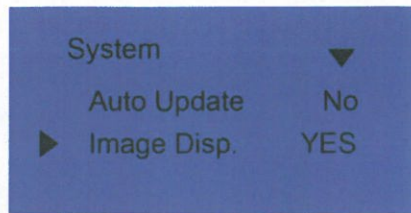
Press [◀ IN] or [OUT ▶] key to choose 'Yes' or 'No', and then press [OK] key to confirm. Then press [C] to save the setting.

### 2.5.1.18 Image Display ★

Whether display the fingerprint image on the LCD after user access granted.

In [System] setup, press [◀ IN] or [OUT ▶] key to select [Image Disp.] option,





Press [OK] key to enter setting interface:

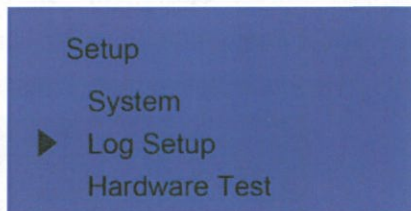


Press [◀ IN] or [OUT▶] key to choose 'Yes' or 'No', and then press [OK] key to confirm. Then press [C] to save the setting.

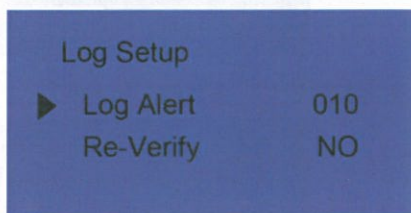
## 2.5.2 Log Setup

Log warning number has the highest limit of 5000. When the available records memory is less than the "Glog Wrn", system will prompt corresponding operation.

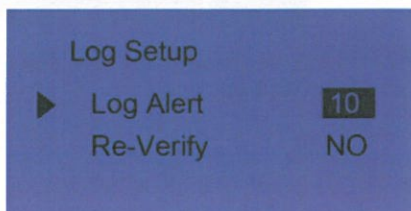
Press [◀ IN] or [OUT▶] key to select [Log Setup] option.



Press [OK] key to enter sub-menu,



Press [◀ IN] or [OUT▶] key to select [Log Alert] option. Press [OK] key to enter log alert setting interface.

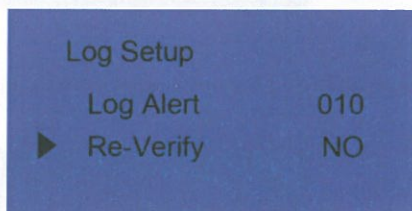


Press [◀ IN] or [OUT▶] key or number key to input log warning number. Press [OK] key to confirm. Then press [C] to save the setting.

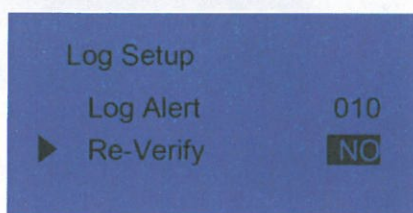
### 2.5.3 Re-Verify Time

The Re-verify time is the time interval in which you make continuous records with the same finger (1-250 minutes), and then the device will only save the first record. If the re-verify value is "NO", it means that you every record saved in the device.

In [Log Setup] menu, press [◀ IN] or [OUT ▶] key to select [Re-Verify] option,



Press [OK] key to enter re-verify setting interface,



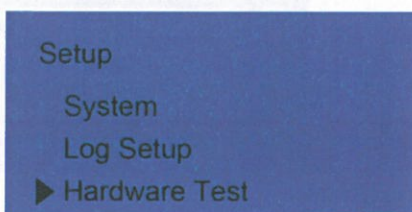
Press [◀ IN] or [OUT ▶] key or number keypad to input time. Press [OK] key to confirm. Then press [C] to save the setting.

Prompt: If the same finger is identified continuously in re-verify time period, only the first record will be saved in device memory.

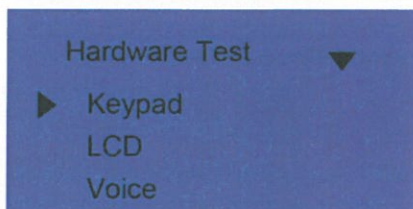
### 2.5.4 Hardware Test

Test the functions of machine keys, LCD, voice, scanner and Flash.

Select [Hardware test] option in [Setup] menu:



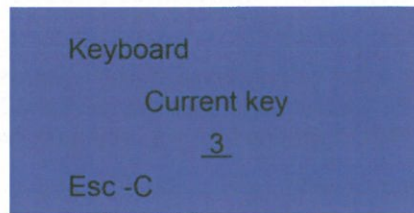
Press [OK] to enter setting interface as following:



Press [◀ IN] or [OUT ▶] key to choose testing option and press [OK] key to start.

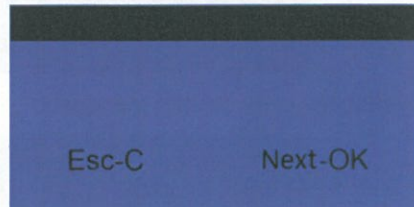
Keyboard: press [◀ IN] or [OUT ▶] key to select [Keyboard] option, and press [OK] to enter keyboard testing interface. Then press any key to start keys testing (i.e. press key 3, if interface shows current key as 3, it indicates the key 3 works.)





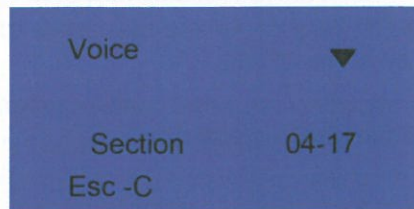
Press "C" exit the test

LCD: Press [◀ IN] or [OUT▶] key to select [LCD] option, and press [OK] to enter LCD testing interface.

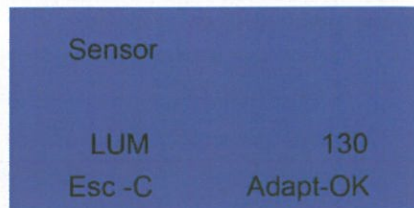


Press "C" exit the test

Voice: Press [◀ IN] or [OUT▶] key to select [Voice] option, and press [OK] to enter voice testing interface. ★



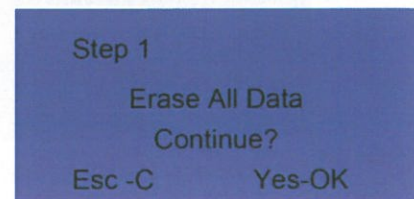
Sensor: Press [◀ IN] or [OUT▶] key to select [Sensor] option, and press [OK] to enter sensor testing interface. ★

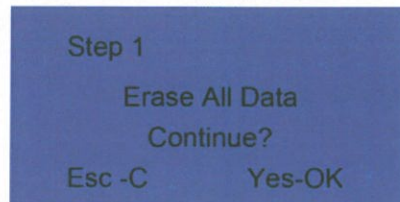


Press "C" exit the test

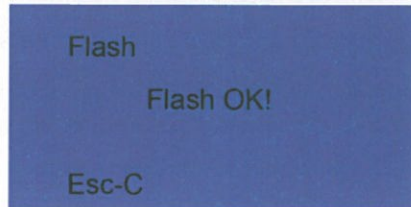
Flash: Press [◀ IN] or [OUT▶] key to select [Flash] option, and press [OK] to enter flash testing interface.

Two steps: 1. Erase all data; 2. Check





After checking completed, the interface will show the checking result,



After each test are finished, press [C] key to exit.

## 2.6 USB Flash ★

Put U flash driver into terminal USB port and press [M] to management menu. Select [USB Flash] Press [OK] enter sub menu.

### 2.6.1 New Log Backup

Download the new records into U flash driver.

Press [◀ IN] or [OUT ▶] key to select [New Log Backup] option, press [OK] key to download the new attendance record.



After back successful, Press [C] key exit to upper menu.

The new record file stores in the BAK.KQ file which under G:\00000001 directory.

[G]: The driver letter of the USB flash driver; [00000001]: is the terminal device ID.

### 2.6.2 All Log Backup

Download all the records into U flash driver. All attendance files store in the BAK.KQ file which under G:\00000001 directory.

**Note:** Please copy the backup record files to another direction of the local PC, Otherwise running [All Log Backup] will instead backup files.

### 2.6.3 User Backup

Download user information and fingerprint template to USB flash driver, the backup file store in BAK.YG and BAK.ZW file under G:\00000001 directory.



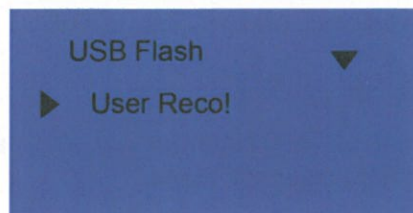
Recover the user information back to the terminal from USB flash driver.

There are two methods for recover the data:

Copy BAK.YG and BAK.ZW files to root direction of the USB flash driver, and put USB flash driver into terminal USB port to recover the records;

Through USB flash driver management software export employee information to root direction of the USB flash driver, will generate BAK.YG and BAK.ZW two files. then put USB flash driver into terminal USB port to recover the records.

Press [◀ IN] or [OUT▶] key to select [User Record] option, press [OK] key to recover the user records.

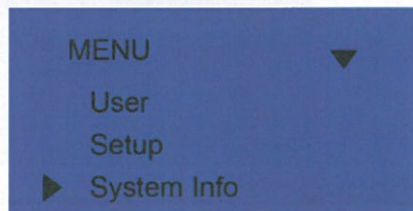


After recover, Press [C] key exit and back to upper menu.

## 2.7 System Info ★

System info shows the current usage status of device, such as user quantity, fingerprint quantity, records quantity and the firmware version etc.

In management mode, press [◀ IN] or [OUT▶] key and shift to [System Info] option,



Press [OK] key to enter system info interface, and check info of correct operated device.

★



User: Registered user number in device

FP: registered fingerprints number. Select it and press [OK] key and you can check the password and card number .★

Log: The number of the attendance record stored in the device.

Serial: The unique identifier of the device and cannot be modified.

FirmVer: the firmware version of program which write in EROM or EPROM (Programmable read only memory). So called firmware is firm program saved in integrated circuit firmly, responsible for controlling and dealing with integrated circuit.

After checking completed, click [C] to exit.

## 2.8 T&A Status Setting

Press [◀ IN] or [OUT ▶] key to shift attendance status. System default statuses are IN, OUT.



## 2.9 Shut Down

In time attendance status, keep pressing [OK] key until interface shows as following,



Then device will shut down.

Notice: If external power is connected, you can press [OK] key to power on device.



## **Chapter3. FAQ**

Frequently asked questions and answers



## 6 FQA

### 6.1 Fingerprint has enrolled but often gets failure in identification.

Reason	Solution
1. The fingerprint was not captured properly.	Enroll the finger again. Please refer to illustration of pressing finger.
2. Direct sun light or too bright light.	Avoid direct sun light or other bright light.
3. Too dry finger, too wet finger with oil or cosmetics.	1, Touch the forehead to increase oily level of the finger. 2, Clean fingers with towel.
4. Low fingerprint quality with callus or peeling.	Enroll other fingers with better quality.
5. Wrong way in placing fingers when punching in/out.	Please refer to illustration of pressing finger.
6. Latent fingerprint on the surface of sensor.	Clean sensor surface (Adhesive tapes recommended).
7. Not enough finger pressure.	Place the finger evenly on the sensor with moderate pressure.
8. Influence by fingerprint image change.	Enroll fingerprint again. Please refer to illustration of pressing finger.

### 6.2 No records found though staff have clocked in/out.

Reason	Solution
1. Unit power break for a long time (time turn to zero as default).	Synchronize the time.
2. The record hasn't been downloaded.	Please download the record from the device.
3. The capacity has been fully occupied.	Please clear the records in time.

### 6.3 The machine cannot connect with PC.

Reason	Solution
1. Communication method not set	Select the correct communication



correctly.	method.
2. Cable not plugged firmly or cable hardware problem.	Plug the cable firmly or change another cable.
3. Not able to connect COM (wrong COM No).	Please enter the right COM No.
4. Not able to connect TCP/IP (wrong setting).	Refer to the manual for connecting Time Attendance terminal.

#### 6.4 Clock's time works fine, but FP scanner is off, Employee cannot attendance

Reason	Solution
1. Unit in dormancy status.	Press any key to activate.
2. The device is on communication or the route has been interfered.	1. Please exit the system by clicking [Exit system].If quit abnormally, the device will resume collecting fingerprint every 1 minute. 2. Eliminate the interference of the route.
3. The capacity has been fully occupied.	Please clear the records in time.

#### 6.5 We do not use the ID + fingerprint mode to verified.

Reason	Solution
1. Wrong ID entered.	Enter the right ID.
2. This user has no right to use 1:1 identification method.	Set 1:1 identification method for this user.

#### 6.6 The unit beeps automatically when no one punches in/out.

Reason	Solution
1. Direct sun light or too bright light.	Avoid direct sun light or other bright light.
2. Latent fingerprint on the surface of sensor.	Clean sensor surface (adhesive tapes recommended).

**Note:** Should you have any other problems, please kindly email us the log files in zip or rar (The log files are in Log directory in the installation directory of the software)!

### 3.

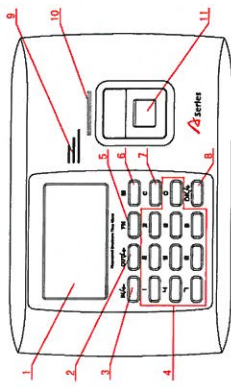
## *Γρήγορος Οδηγός Σύνδεσης Συστήματος Αννιζ*

*(96891\_A\_\_Series\_EN\_Quick\_Guide)*





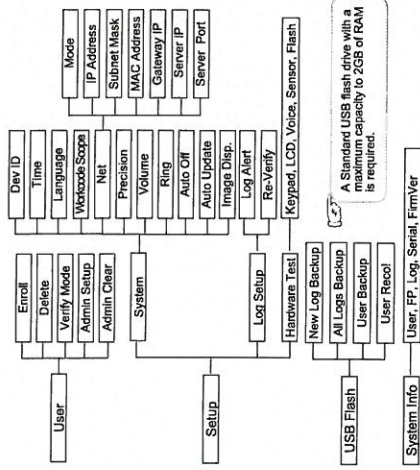
## Product Appearance



- 1. LCD
- 2. State Key (Clock Out) Page Down
- 3. State Key (Clock In) Page Up
- 4. 0-9 Num. Key
- 5. FN key
- 6. Menu Key
- 7. Delete/Exit key
- 8. Confirm/Power Key
- 9. Loudspeaker
- 10. LED
- 11. Fingerprint Sensor

## Menu List

Press [OK] about 3 seconds to turn on the terminal, press [M] key to enter the management menu. Menu list:

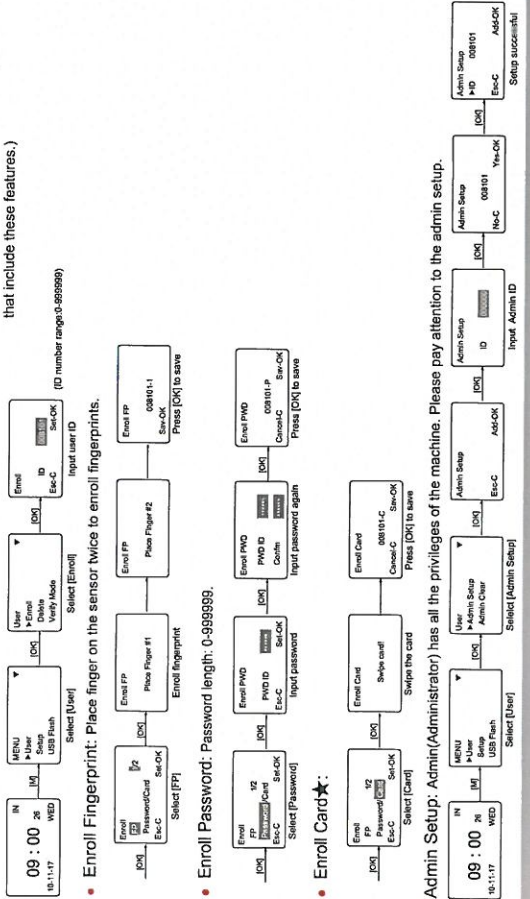


## Illustration for placing finger

- Correct method:**
  - Place finger flat on the sensor surface.
  - Sliding, rolling or moving finger during the enrollment process.
- Incorrect method:**
  - Do not remove finger during the enrollment process.
  - Using the tip of your finger.

## Operation Guide

**Enroll User:** Each user can register two fingerprints, one password and one RFID card. (Functions marked with a Star are for specific models that include these features.)



## Other Setup

**Verify Mode:** M-[Setup]-[OK]-[Verify Mode]-[OK]-[OK]-[Input employee ID]-[OK]-[OK]-[OK]  
 Use [IN]-[OUT]-[ ] to select ANYRF-PF-PW-FP-M-FP-FP-PW-ID-FP-[OK]-[OK]

Item	Explanation
Any	Fingerprint only, Card only or ID+Password only
RF+FP	It requires both Card and Fingerprint verification together
PW+FP	It requires both Password and Fingerprint verification together
RF+PW	It requires both Card and Password verification together
ID+FP	Enter the user ID first, then verify the fingerprint
Factory default setting	Any

**Dev ID:** M-[Setup]-[OK]-[System]-[OK]-[Dev ID]-[OK]-[Input the device's ID]-[OK]-[OK]

Item	Explanation
1-99999999	Device ID of the unit which is required in software communication
Factory default setting	1

**Language:** M-[Setup]-[OK]-[System]-[OK]-[Language]-[OK]-[ ]  
 Use [IN]-[OUT]-[ ] to select ENGRFCHGERM-[OK]-[OK]-[OK]

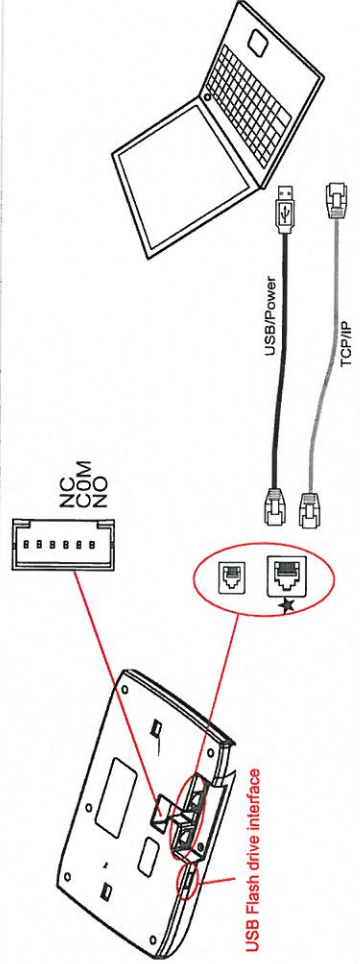
Item	Explanation
Language	Contains 11 languages: ENG(English), FRCH(French), GERM(German), SPAN(Spanish), PTG(Portuguese), ITA(Italian), BUI(Bulgarian), SLAK(Slovak), HUNG(Hungarian), SLVN(Slovenian), TURK(Turkish)
Factory default setting	Related Language

**WorkCode:** M-[Setup]-[OK]-[System]-[OK]-[WorkCode Scope]-[OK]-[ ]  
 Input Max-[OK]-[Input Min]-[OK]-[OK]-[OK]

Item	Explanation
0-999999	Valid scope for the WorkCode
Factory default setting	Max: 999999 Min: 0

**Tips:** WorkCode indicates the work type, easily distinguishes which attendance record is related to which work type.

## Wiring Diagram



**Ring:** Use the function in the software.

Item	Explanation
1-15	The duration of the audible alarm to notify employees of events. (Lunch, break, Off Duty)
No	Electric bell under closed state
Factory default setting	5

**Net:** M-[Setup]-[OK]-[System]-[OK]-[Net]-[OK]-[ ] to select ModemIP AddressSubnet Mask  
 MAC AddressGateway IP-Server IP-Server Port-[OK]-[Modify parameters]-[OK]-[OK]

Item	Explanation
Mode	TCP/IP Server mode: Common network mode TCP/IP Client mode: Only communicate with the PC which has static IP
IP Address	Set terminal IP address when communication of TCP/IP. IP address must be a static IP address
Subnet Mask	Subnet Mask of the LAN
MAC Address	Unique Physical address of the network module. This setting can not be modified.
Gateway IP	Default Gateway of the LAN
Server IP	The IP address of the Server Machine which is in Client Mode TCP/IP
Server Port	It's the Software Port number used when the read is configured for TCP/IP communication
Factory default setting	5010

**Precision, Volume, Auto off, Auto Update, Image Disp., Log Alert, Re-Verify**

Item	Explanation
Precision	Set terminal fingerprint matching precision. 0-[Normal], 1-[Good], 2-[Exact].
Volume	Set the terminal voice volume. 0-[mute], 5-[Max].
Auto off	Set the time duration for an idle clock to go into sleep mode. No-[Not Off], 20min-[Max Time].
Auto Update	Auto update means the previous lower quality fingerprint template will be automatically replaced by the new higher quality one during fingerprint verification.
Image Disp.	Choose to display the fingerprint image on the screen during the verification process. [Yes]- show fingerprint image, [No]- not show fingerprint image
Log Alert	The terminal will alarm when the memory capacity is less than the [Log Alert] value [No]-Not alarm, Max. value 5,000.
Re-Verify	The duration of time in which the terminal will ignore repeated attempts for authentication. [No]- Disable the function; Max. value is 250 min.





4.

*Κάτοψη Επιχείρησης  
σε μεγάλη κλίμακα*





**Υπόμνημα Συμβολισμών**



Φορητό Αποσπασίμο σε ελάττωξη Επίπεδο



Προβλεπόμενη Θύρα σε κλειστά επίπεδα 1.5.00.4. DNN20



Ανεγερτής Ισχύος - Κεντρικό/ Οριζ. Αεριστήρας



Φορητός Προβλεπόμενος Σημάς Κέντρου Δίχτυ



Σημάς σε στήριξη και οριζωνιά σήμαξη



Κερίλο Σημασίαν



Πίνακας Διαχειρίσεως



Τελετηράς Επεξεργασίας Α100



Administer PC HP Pavilion



Υποστήρικτη Αντ. Εκτύπωσης Συμβατότητας



Εκτυπωτής Συμβατός



Επιχρυσωμένη Κάρτα Αποθήκευσης



Συνολική Αποθήκευσης WD



Υποστήρικτη σε κεντρικό/ οριζωνιά σήμαξη



Εκτυπώτρια σε κεντρικό/ οριζωνιά σήμαξη



Εκτυπώτρια σε κεντρικό/ οριζωνιά σήμαξη



Εκτυπώτρια σε κεντρικό/ οριζωνιά σήμαξη



Εκτυπώτρια σε κεντρικό/ οριζωνιά σήμαξη

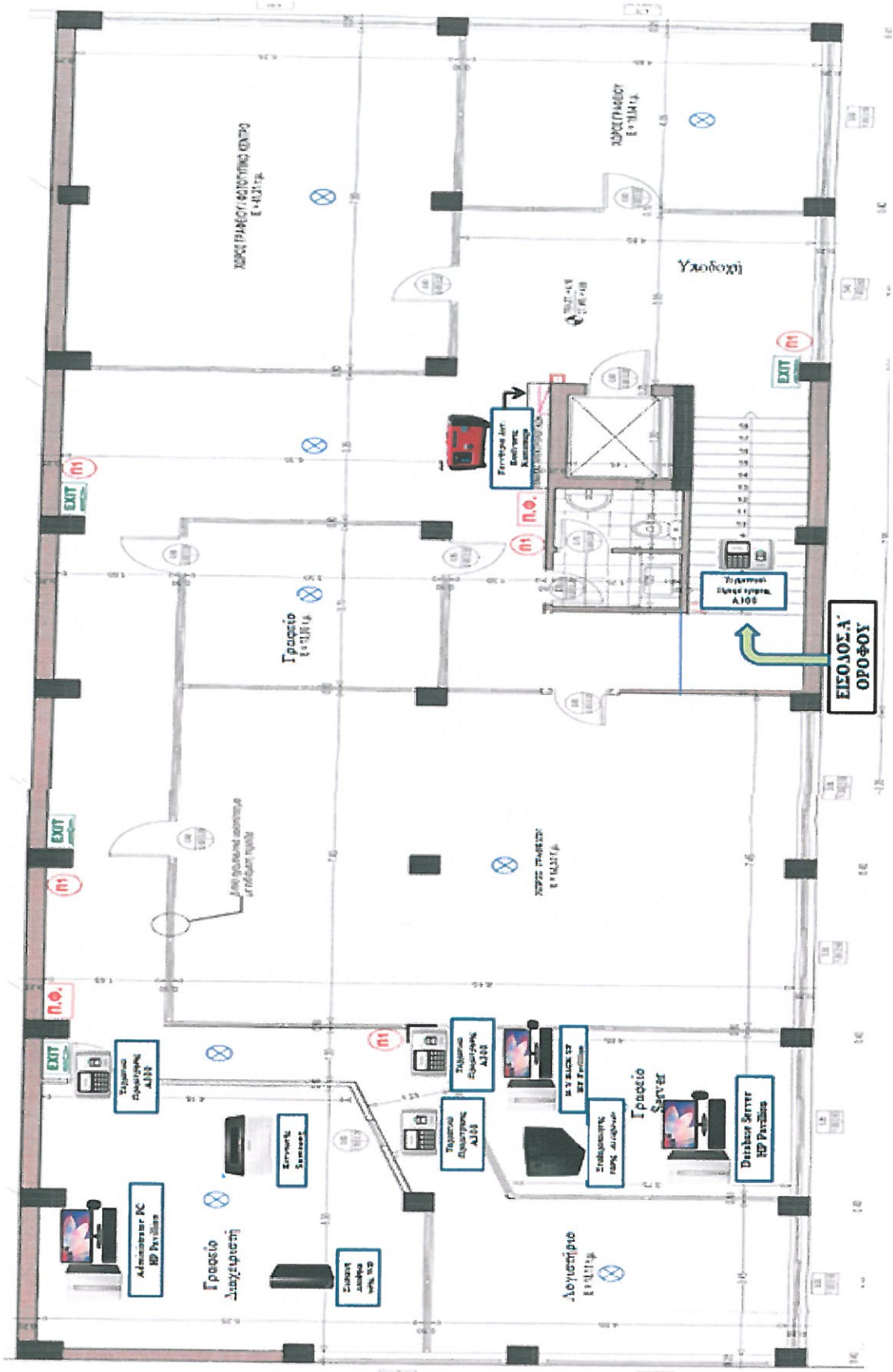


Εκτυπώτρια σε κεντρικό/ οριζωνιά σήμαξη



Εκτυπώτρια σε κεντρικό/ οριζωνιά σήμαξη

**Υπεύθυν Μελέτης**  
**Μερίνα Γεροπούλη**  
**A.M. 6476**







5.

*Πιστοποιητικά Εταιρείας Αννιζ*

*&*

*Συστήματος Αναγνώρισης και  
Ωρομέτρησης Αννιζ A300*





# Certificate of Conformity

Registration No.: T1861387 01, T1861387 02

Applicant : Shanghai Anviz Technology Co.Ltd

Address : 2th Floor,4289Jindu Road,Shanghai China

Product : Fingerprint & RFID Time Attendance

Model No. : A300

Trade Name : **ANVIZ**

The submitted products have been tested by us with the listed standards and found in compliance with the following European Directives:

## The R&TTE Directive 1999/5/EC

EN 300 330-1 V 1.7.1:2010

EN 300 330-2 V 1.5.1:2010

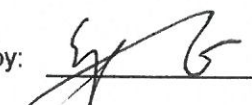
The tests were performed in normal operation mode, the test results apply only to the particular sample tested and to the specific tests carried out. This certificate applies specifically to the sample investigated in our test reference number only.

The CE markings as shown below can be affixed on the product after preparation of necessary technical documentation.

Other relevant Directives have to be observed.



Certified by:

  
July 26, 2016



Shenzhen Alpha Product Testing Co., Ltd.  
Building B, East Area of Nanchang Second Industrial Zone,  
Gushu 2<sup>nd</sup> Road, Bao'an District, Shenzhen 518126, P. R. China  
Website: <http://www.a-lab.cn> Email: [service@a-lab.cn](mailto:service@a-lab.cn)

**0001365**





# DECLARATION of Conformity

Registration No.: CSTE140320196



**Applicant** : Shanghai Anviz Technology Co., Ltd  
**Address** : 5th Floor, 4299 Jindu Road, Shanghai China  
**Product** : Fingerprint Time Attendance  
**Model No.** : A series

The submitted products have been tested by us with the listed standards and found in compliance with the following European Directives:

**The EMC Directive 2004/108/EC**

EN 55022:2010  
EN 55024:2010  
EN 61000-3-2:2006+A1:2009+A2:2009  
EN 61000-3-3:2013

The tests were performed in normal operation mode. The test results apply only to the particular sample tested and to the specific tests carried out. This certificate applies specifically to the sample investigated in our test reference number only.

The CE markings as shown below can be affixed on the product after preparation of necessary technical documentation.

Other relevant Directives have to be observed.



Certified By:

A handwritten signature in black ink, appearing to be 'Zhang', written over a horizontal line.

Manager

March 26, 2014



Shenzhen Certification Technology Service Co., Ltd.  
2<sup>F</sup>, Building B, East Area of Nanchang Second Industrial Zone,  
Gushu 2<sup>nd</sup> Road, Bao'an District, Shenzhen 518126, P.R. China

Website: <http://www.ceszz.com>

Email: [service@ceszz.com](mailto:service@ceszz.com)





# VERIFICATION

of Conformity

Registration No.: CST-FV140320041



We Shenzhen Certification Technology Service Co., Ltd. here declare that the product referred below:

**Applicant** : Shanghai Anviz Technology Co., Ltd

**Address** : 5th Floor, 4299 Jindu Road, Shanghai China

**Product** : Fingerprint Time Attendance

**Model No.** : A series

was tested to conform to the applicable FCC Rules and Regulations:

**FCC Rules and Regulations Part 15 Subpart B Class B**

The method of testing was in accordance to the most accurate measurement standards possible, and that all necessary steps have been enforced to assure that all production units of the same equipment will continue to comply with the Federal Communications Commission's requirements.



Certified By:

  
Manager

March 25, 2014



Shenzhen Certification Technology Service Co., Ltd.  
2F, Building B, East Area of Nanchang Second Industrial Zone,  
Gushu 2<sup>nd</sup> Road, Bao'an District, Shenzhen 518126, P.R. China  
Website: <http://www.cessz.com> Email: [services@cessz.com](mailto:services@cessz.com)





# DECLARATION

of Conformity

Registration No.: CSTR140320212



**Applicant** : Shanghai Anviz Technology Co., Ltd  
**Address** : 5th Floor, 4299 Jindu Road, Shanghai China  
**Product** : Fingerprint Time Attendance  
**Model No.** : A series

The verification of RoHS Compliance has been granted to the applicant based on the review of test report on the sample of the above-mentioned product in accordance with the relevant provisions of EU RoHS Directive 2011/65/EU.


The results in this report are applicable only to the devices tested and/or test reports verified. This report shall not be re-produced except in full without the written approval of the undersigned. This report is valid only accompanied with the RoHS report verified and identified by the undersigned.

The CE mark as shown below can be used under the responsibility of the manufacturer, after completion of an EU Declaration of Conformity and compliances with all relevant EU Directives.

*(This certificate is only valid without the test report: CSTR140320212)*



Certified By:

  
\_\_\_\_\_  
Manager  
March 31, 2014



Shenzhen Certification Technology Service Co., Ltd.  
2F, Building B, East Area of Nanchang Second Industrial Zone,  
Gushu 2<sup>nd</sup> Road, Bao'an District, Shenzhen 518126, P.R. China  
Website: <http://www.cesst.com> Email: [service@cesst.com](mailto:service@cesst.com)

