

Οργανισμός
Βιομηχανικής
Ιδιοκτησίας (OBI)



(21) Αριθμός αίτησης:

GR 20170100470

(12)

ΔΙΠΛΩΜΑ ΕΥΡΕΣΙΤΕΧΝΙΑΣ (B)

(47) Ημ/νία Δημοσίευσης: **13.08.2018**

(11) Αριθμός Χορήγησης: **1009345**

(22) Ημ/νία Κατάθεσης: **11.10.2017**

(51) Διεθνής Ταξινόμηση (Int. Cl.):

G06F 21/32 (2018.01)

H04M 1/725 (2018.01)

G06K 9/00 (2018.01)

(45) Ημ/νία Δημοσίευσης της Χορήγησης:
31.10.2018 ΕΔΒΙ 8/2018

(71) Αρχικός (οί) Καταθέτης (ες):
MLS ΠΛΗΡΟΦΟΡΙΚΗ Α.Ε.; ΒΕΠΕ Τεχνόπολης, 55535
ΠΥΛΑΙΑ (ΘΕΣΣΑΛΟΝΙΚΗΣ) - GR.

(72) Εφευρέτης (ες):
ΚΑΜΑΤΑΚΗΣ ΙΩΑΝΝΗΣ ΝΙΚΟΛΑΟΥ; , GR. **ΣΤΡΑΤΗΓΑΚΗΣ
ΝΙΚΟΛΑΟΣ ΚΩΝΣΤΑΝΤΙΝΟΥ**; , GR. **ΟΙΚΟΝΟΜΟΥ
ΑΛΕΞΑΝΔΡΟΣ ΣΩΤΗΡΙΟΥ**; , GR.

(73) Δικαιούχος (οί):

MLS ΠΛΗΡΟΦΟΡΙΚΗ Α.Ε.; ΒΕΠΕ Τεχνόπολης, 55535
ΠΥΛΑΙΑ (ΘΕΣΣΑΛΟΝΙΚΗΣ) - GR.

(74) Πληρεξούσιος:

ΖΑΓΛΑΝΙΚΑ ΕΙΡΗΝΗ; Νεοφύτου Βάμβα 9, 10674 ΑΘΗΝΑ
(ΑΤΤΙΚΗΣ).

(54) Τίτλος (Ελληνικά)

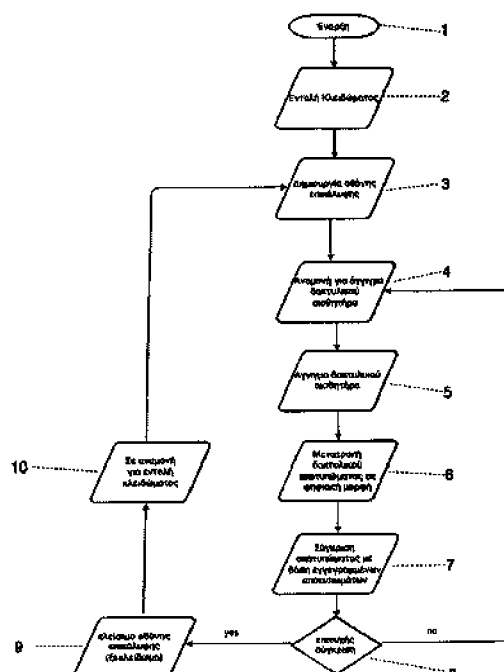
ΜΕΘΟΔΟΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΦΟΡΗΤΕΣ ΣΥΣΚΕΥΕΣ ΜΕ ΑΠΟΚΛΕΙΣΤΙΚΗ ΧΡΗΣΗ ΔΑΚΤΥΛΙΚΟΥ ΑΠΟΤΥΠΩΜΑΤΟΣ

(54) Τίτλος (Αγγλικά)

METHOD FOR PERSONAL DATA PROTECTION IN PORTABLE DEVICES WITH EXCLUSIVE USE OF FINGERPRINTS

(57) Περίληψη

Μέθοδος που επιτρέπει την προστασία και απόκρυψη προσωπικών δεδομένων χρηστών φορητών συσκευών με εγκατεστημένο το λειτουργικό σύστημα Android. Κατά τη μέθοδο αυτή η οθόνη της φορητής συσκευής επικαλύπτεται με μια επιπρόσθετη εικόνα η οποία αποκρύπτει τις εισερχόμενες ειδοποιήσεις του, οι οποίες μπορεί να έχουν πολλαπλές προελεύσεις όπως τα κοινωνικά μέσα δικτύωσης, οι εφαρμογές ηλεκτρονικού ταχυδρομείου, οι τηλεφωνικές κλήσεις, κ.ά. και η οποία (επιπρόσθετη εικόνα) μπορεί να απομακρυνθεί μόνο έπειτα από την εισαγωγή ενός δακτυλικού αποτυπώματος που έχει εξουσιοδοτήσει ο εκάστοτε χρήστης της συσκευής. Παράλληλα, η αποκλειστική χρήση δακτυλικού αποτυπώματος αποτρέπει οποιονδήποτε έχει υποκλέψει κάποιο/α εκ των PIN, συνθηματικού και μοτίβου, που έχει ορίσει ένας χρήστης, από το να αποκτήσει πρόσβαση στις λειτουργίες και κατά επέκταση στα προσωπικά δεδομένα του χρήστη.



GR 20170100470 GR 1009345

ΠΕΡΙΓΡΑΦΗ

Μέθοδος προστασίας προσωπικών δεδομένων σε φορητές συσκευές με αποκλειστική χρήση δακτυλικού αποτυπώματος.

5 Τεχνικό πεδίο

Η παρούσα εφεύρεση αναφέρεται σε μια μέθοδο προστασίας προσωπικών δεδομένων σε φορητές συσκευές με εγκατεστημένο το λειτουργικό σύστημα Android, η οποία εξουσιοδοτεί την πρόσβαση στις λειτουργίες και δεδομένα της φορητής συσκευής μόνο σε χρήστες που έχουν εκ των προτέρων καταχωρήσει το δαχτυλικό τους αποτύπωμα στην εν λόγω συσκευή. Σε οποιαδήποτε άλλη περίπτωση τα προσωπικά δεδομένα που εμφανίζονται στην οθόνη της συσκευής αποκρύπτονται, είτε αυτά αφορούν ειδοποιήσεις καινούργιων μηνυμάτων, προερχόμενα από το δίκτυο κινητής τηλεφωνίας ή από άλλες εφαρμογές όπως εφαρμογές κοινωνικής δικτύωσης, είτε αφορούν εισερχόμενες κλήσεις του χρήστη.

Αναφορά της στάθμης προηγούμενης τεχνικής

Οι μέθοδοι προστασίας - κλειδώματος των κινητών τηλεφώνων που εφαρμόζονται σήμερα χωρίζονται στις παρακάτω κατηγορίες: σε αυτές που χρησιμοποιούν PIN, σε αυτές που χρησιμοποιούν μοτίβο, σε αυτές που χρησιμοποιούν συνθηματικό, σε αυτές που χρησιμοποιούν την ταυτοποίηση φωνής, σε αυτές που χρησιμοποιούν αναγνώριση προσώπου και τέλος, σε αυτές που αξιοποιούν το δαχτυλικό αποτύπωμα του χρήστη.

Οι μέθοδοι προστασίας φορητών συσκευών μέσω PIN (Personal Identification Number), μοτίβου, ή συνθηματικού, υστερούν στο ότι κάποιος τρίτος μπορεί να δει, να υποκλέψει τα ανωτέρω και με τον τρόπο αυτό, να μπορέσει να ξεκλειδώσει τη συσκευή. Οι υπόλοιπες, από τις προαναφερθείσες, τρεις μέθοδοι, απαιτούν, πάντα, και μία εφεδρική μέθοδο ξεκλειδώματος της συσκευής, είτε αυτή είναι PIN είτε μοτίβο, υποβαθμίζοντας, ουσιαστικά, την ασφάλεια του συστήματος στην

- 30 ασφάλεια που μπορεί να παρέχει το κλείδωμα με χρήση αποκλειστικά και μόνο PIN ή μοτίβου.

Σύντομη παρουσίαση της εφεύρεσης

- Οι φορητές συσκευές θεωρούνται, πλέον, προέκταση του μυαλού/σκέψεών μας, επομένως θεωρούμε πολύ σημαντικό να υπάρχει πλήρης έλεγχος της ιδιωτικότητας των δεδομένων των χρηστών. Ο σκοπός της εν λόγω μεθόδου είναι να εξασφαλίσει αυτήν την ιδιωτικότητα και πλέον να μην απασχολεί τον χρήστη το ενδεχόμενο του κάποιος να υποκλέψει τα προσωπικά του στοιχεία και δεδομένα. Λόγω της απόλυτης ασφάλειας που παρέχει η εν λόγω μέθοδος, οι χρήστες θα μπορούν να δέχονται μηνύματα, κλήσεις και ειδοποιήσεις γνωρίζοντας πως μόνο εκείνοι θα μπορούν να διαβάσουν το περιεχόμενό τους. Η μέθοδος έχει ως βασικό και μοναδικό κριτήριο λειτουργίας, το δαχτυλικό αποτύπωμα (fingerprint) το οποίο δεν επηρεάζει τη λειτουργία της φορητής συσκευής ή την οποιαδήποτε εμπειρία χρήσης συσκευών με λειτουργικό σύστημα Android που έχει ο χρήστης. Η προτεινόμενη μέθοδος παρέχει την παρακάτω δυνατότητα:
- 45
- Επιτρέπει τη χρήση της συσκευής αποκλειστικά και μόνο με το δαχτυλικό αποτύπωμα, αποκλείοντας όλες τις υπόλοιπες μεθόδους ξεκλειδώματος της φορητής συσκευής.

Επισήμανση των πλεονεκτημάτων της εφεύρεσης

- Κενά ασφάλειας στο λειτουργικό Android επιτρέπουν σε κακόβουλο λογισμικό να υποκλέψει το PIN ή το μοτίβο ή οποιαδήποτε άλλη μέθοδο προστασίας των δεδομένων των χρηστών. Για παράδειγμα πρόσφατα αποδείχτηκε πως μια εφαρμογή η οποία καταγράφει τις μετρήσεις που προέρχονται από τον αισθητήρα επιτάχυνσης και το γυροσκόπιο της συσκευής, είναι σε θέση να αναγνωρίσει τη μοναδική «δόνηση» που δημιουργείται με το πάτημα κάθε αριθμού στην οθόνη εισαγωγής PIN ή συνθηματικού ή στην οθόνη εισαγωγής μοτίβου και στη συνέχεια, χρησιμοποιώντας τεχνικές αναγνώρισης προτύπων, να καταλάβει και να υποκλέψει το PIN, το συνθηματικό ή/και το μοτίβο.
- 55

- Σύμφωνα με την μεθοδολογία υλοποίησης της παρούσας εφεύρεσης, η αποτελεσματική λειτουργία της μεθόδου κλειδώματος βασίζεται στην αποκλειστική χρήση του δακτυλικού αποτυπώματος για το ξεκλείδωμα της
- 60

συσκευής και τις προβολής προσωπικών δεδομένων. Σε υπάρχουσες μεθόδους κλειδώματος, πάντα δίνεται στον χρήστη η εναλλακτική να ξεκλειδώσει το τηλέφωνο του και με μια δεύτερη μέθοδο όπως το PIN ή και το σχηματισμό ενός μοτίβου στην οθόνη. Η εναλλακτική αυτή αποτελεί και την αδυναμία των
 65 υπαρχόντων μεθόδων, όπως προαναφέρθηκε, καθώς κάποιος τρίτος γνωρίζοντας το PIN ή το μοτίβο μπορεί να παρακάμψει το, μέσω δακτυλικού αποτυπώματος, κλείδωμα και να αποκτήσει πρόσβαση στα προσωπικά δεδομένα του κινητού.

Σύντομη περιγραφή των απεικονίσεων των τυχόν σχεδίων

Η εν λόγω μέθοδος δίνει τη δυνατότητα στο χρήστη να αποκρύπτει προσωπικές
 70 πληροφορίες από το περιβάλλον του. Συγκεκριμένα, η βασική λειτουργικότητα σχετίζεται με την πλήρη πρόσβαση στις λειτουργίες μιας συσκευής μόνο έπειτα από εισαγωγή του δακτυλικού αποτυπώματος ενός χρήστη, αποκλείοντας άλλες μεθόδους κλειδώματος, οι οποίες έχουν κριθεί ως μη ασφαλείς τρόποι κλειδώματός της. Επιπρόσθετα, έχει ως βασικό και μοναδικό κριτήριο λειτουργίας, το δακτυλικό
 75 αποτύπωμα (fingerprint) ενώ δεν επηρεάζει τη λειτουργία του τηλεφώνου ή την οποιαδήποτε εμπειρία χρήσης συσκευών με λειτουργικό σύστημα Android που διαθέτει ο χρήστης.

Ένα διάγραμμα ροής που επεξηγεί τον τρόπο λειτουργίας της μεθόδου παρουσιάζεται στο Σχέδιο 1. Σε αυτό το διάγραμμα είναι ξεκάθαρο πως με την
 80 έναρξη (Σχέδιο 1 - σημείο 1) της φορητής συσκευής, είτε από κατάσταση αδράνειας είτε από πλήρως απενεργοποιημένη κατάσταση, εκείνη κλειδώνεται (Σχέδιο 1 - σημείο 2) και δημιουργείται στη συνέχεια η οθόνη κλειδώματος του Android(Σχέδιο 1 - σημ. 3) που αποκρύπτει όλες τις εισερχόμενες ειδοποιήσεις και κλήσεις που φτάνουν στη φορητή συσκευή. Η οθόνη κλειδώματος απομακρύνεται
 85 (Σχέδιο 1 - σημείο 9) μόνο στην περίπτωση που εισαχθεί ένα εξουσιοδοτημένο δακτυλικό αποτύπωμα.

Επιπρόσθετα, στο Σχέδιο 2, απεικονίζεται μια συσκευή, επί της οποίας μπορεί να υλοποιηθεί η εν λόγω μέθοδος, καθώς ενσωματώνει κάποια ελάχιστα βασικά δομικά και λειτουργικά στοιχεία που της το επιτρέπουν. Συγκεκριμένα, η συσκευή
 90 ενσωματώνει αισθητήρα δακτυλικού αποτυπώματος (Σχέδιο 2 - σημείο 3), επεξεργαστή (Σχέδιο 2 - σημείο 2), μνήμη (Σχέδιο 2 - σημείο 1) και μητρική (Σχέδιο 2 - σημείο 4) όπου όλα τα ανωτέρω στοιχεία συνδέονται.

Τέλος, στο Σχέδιο 3, παρουσιάζεται η εγγενής οθόνη κλειδώματος του Android στην οποία μπορούν να εμφανιστούν οποιεσδήποτε πληροφορίες και δεδομένα του χρήστη, όπως ειδοποιήσεις από μηνύματα ή εισερχόμενες κλήσεις.

Πλήρης περιγραφή της εφεύρεσης με τη λεπτομερειακή ανάπτυξη ενός ή περισσότερων τρόπων πραγματοποίησης της εφεύρεσης

Η μέθοδος που αποτελεί το αντικείμενο της παρούσας εφευρέσεως συνίσταται από μία σειρά φάσεων που επιτρέπουν στο χρήστη να προστατεύσει τα ευαίσθητα προσωπικά δεδομένα του. Αυτή η μέθοδος θα περιγραφεί σε σχέση με τις εργασίες που επιθυμεί να εκτελέσει ο χρήστης στη φορητή συσκευή του. Πρέπει να τονιστεί πως για να λειτουργήσει η προτεινόμενη μέθοδος πρέπει απαραίτητως η συσκευή να ενσωματώνει έναν λειτουργικό αισθητήρα δαχτυλικού αποτυπώματος και επιπλέον ο χρήστης να έχει ήδη εισάγει τα εξουσιοδοτημένα δαχτυλικά αποτυπώματα όλων των ατόμων που θέλει να έχουν πρόσβαση στα δεδομένα του.

Η προτεινόμενη μέθοδος προστασίας δεδομένων επιτρέπει την απομάκρυνση της οθόνης κλειδώματος, όπως αυτή παρουσιάζεται ενδεικτικά στο Σχέδιο 3 μόνο όταν το δαχτυλικό αποτύπωμα ταιριάζει με κάποιο από αυτά που βρίσκονται αποθηκευμένα στη συγκεκριμένη συσκευή. Με αυτό τον τρόπο εξαλείφεται η αδυναμία των υπάρχοντων κλειδωμάτων καθώς δεν έχει εφεδρικό τρόπο ξεκλειδώματος αλλά και δε μπορεί να υποκλαπεί όπως το PIN ή το μοτίβο.

Για να πραγματοποιηθεί η εν λόγω εφεύρεση οφείλει αρχικώς ο χρήστης να προαποθηκεύσει τα δαχτυλικά αποτυπώματα των ατόμων στα οποία επιθυμεί να παρέχεται πρόσβαση στα δυνητικώς ευαίσθητα δεδομένα του στην ίδια τη συσκευή μέσω της ενσωματωμένης λειτουργίας αποθήκευσης που προσφέρει το ίδιο το λειτουργικό σύστημα Android.

Τα δαχτυλικά αποτυπώματα αυτά μετατρέπονται σε ψηφιακή μορφή (ουσιαστικά πρόκειται για μια ψηφιακή εικόνα) από το ίδιο το σύστημα, η οποία (εικόνα) καταχωρείται και χρησιμεύει ως πρότυπο για τον έλεγχο της ταυτότητας του χρήστη. Η αποθήκευση και επεξεργασία που σχετίζεται με τα δαχτυλικά αποτυπώματα πραγματοποιείται σε ένα περιβάλλον αξιόπιστης εκτέλεσης σε επίπεδο υλισμικού της συσκευής ούτως ώστε να παρέχεται ένα υψηλότερο επίπεδο ασφάλειας και να μην υπάρχει δυνατότητα υποκλοπής τους. Πρακτικά, η μέθοδος

125 βασίζεται στο τρίπτυχο χρήστης, αισθητήρας δαχτυλικού αποτυπώματος της συσκευής και το βασιζόμενο σε υλισμικό περιβάλλον αξιόπιστης εκτέλεσης της συσκευής όπου γίνεται η αποθήκευση, η επεξεργασία και η ταυτοποίηση των δαχτυλικών αποτυπωμάτων.

Καθώς ο χρήστης λαμβάνει μια ειδοποίηση ή κλήση στη φορητή συσκευή του, 130 μπορεί να την ξεκλειδώσει μόνο αν εισάγει το δαχτυλικό του αποτύπωμα στον αισθητήρα της συσκευής (Σχέδιο 1 - σημείο 4, Σχέδιο 1 - σημείο 5), το οποίο και συγκρίνεται με τα ήδη αποθηκευμένα αποτυπώματα (Σχέδιο 1 - σημείο 6, Σχέδιο 1 - σημείο 7). Σε περίπτωση ταυτοποίησής του με ένα από αυτά, ο χρήστης αποκτά πρόσβαση στα προσωπικά του δεδομένα (Σχέδιο 1 - σημείο 7, Σχέδιο 1 - σημείο 8, 135 Σχέδιο 1 - σημείο 9, Σχέδιο 1 - σημείο 10) ενώ σε αντίθετη περίπτωση πρέπει να δοκιμάσει και πάλι έως ότου προκύψει μια επιτυχημένη ταυτοποίηση (Σχέδιο 1 - σημείο 8, Σχέδιο 1 - σημείο 4).

Περιγραφή τουλάχιστον ενός τρόπου εφαρμογής της εφεύρεσης, με αναφορά στα σχέδια

140 Η παρούσα μέθοδος μπορεί να κατανοηθεί πλήρως από την ακόλουθη αναλυτική περιγραφή ενός παραδείγματος που βασίζεται στο σχέδιο της εφεύρεσης, όπου γίνονται αναφορές στις ακόλουθες συνημμένες Εικόνες.

- Σχέδιο 1 είναι τα βήματα της μεθόδου που ακολουθούνται κατά το κλείδωμα της συσκευής.
- 145 - Σχέδιο 2 αποτελεί μια ενδεικτική απεικόνιση συσκευής που ενσωματώνει τα απαραίτητα δομικά στοιχεία ώστε να υποστηρίξει την υλοποίηση της εν λόγω μεθόδου.
- Σχέδιο 3 εμφανίζεται η εγγενής οθόνη κλειδώματος του Android.
- Σχέδιο 4 είναι η αρχική οθόνη μιας μη προστατευμένης συσκευής 150 όπου εμφανίζεται η κλασική οθόνη κλειδώματος που εμφανίζεται εγγενώς στο λειτουργικό σύστημα Android. Στο Σχέδιο 1 – σημείο 2 εμφανίζεται πληροφορία σχετική με μηνύματα ή κλήσεις που έχει λάβει ο χρήστης καθώς αυτή δεν προστατεύεται.

155 Όπως έχει προαναφερθεί, για να λειτουργήσει η προτεινόμενη μέθοδος θεωρούμε πως ο χρήστης έχει ήδη προαποθηκεύσει τα δαχτυλικά αποτυπώματα των ατόμων στα οποία επιτρέπεται η πρόσβαση στα δεδομένα της φορητής συσκευής.

Παράδειγμα Α.

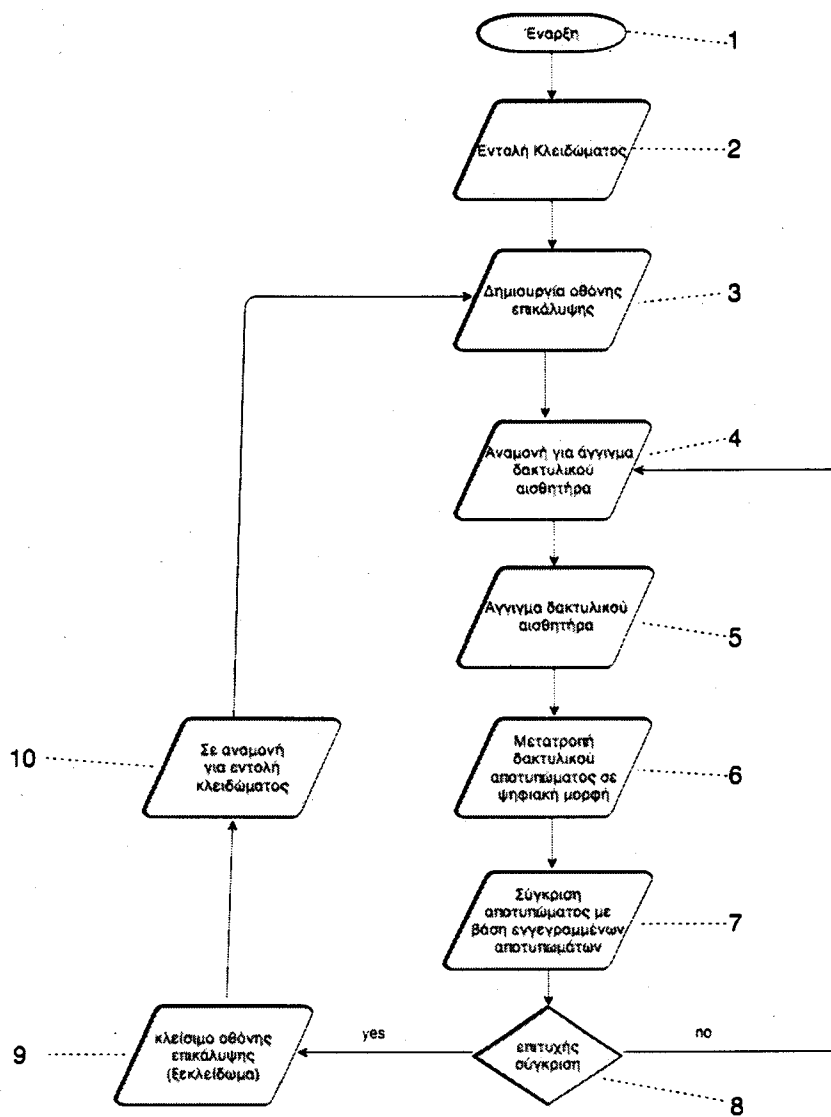
160 Στην περίπτωση που ένας χρήστης θελήσει να δει τα αρχεία που έχει αποθηκεύσει
στο κινητό του, ή τα emails που έχει δεχτεί ή να εκκινήσει μια από τις
εγκατεστημένες εφαρμογές στη φορητή συσκευή του, τότε σε περίπτωση που
εκείνη είναι απροστάτευτη μπορεί να το κάνει χρησιμοποιώντας απλώς τη
λειτουργία ξεκλειδώματος του λειτουργικού συστήματος Android όπως εκείνη
συνήθως εμφανίζεται στο Σχέδιο 4 - σημείο 3. Ακόμη και αν έχει ασφαλίσει τη
165 συσκευή του με κάποια μέθοδο κλειδώματος από αυτές που έχουν προαναφερθεί
(π.χ. PIN, μοτίβο), είναι αρκετά εύκολο για κάποιον να υποκλέψει τον εκάστοτε
κωδικό ή/και μοτίβο και να αποκτήσει πρόσβαση στη συσκευή.

Αντιθέτως, σε μια προστατευμένη συσκευή, ο χρήστης μπορεί να αποκτήσει
πρόσβαση μόνο χρησιμοποιώντας το προ-εγκεκριμένο δαχτυλικό του αποτύπωμα.
170 Συγκεκριμένα, όπως ακριβώς τον ενημερώνει η προτεινόμενη μέθοδος μέσω του
ενημερωτικού μηνύματος που εμφανίζεται στο Σχέδιο 3.

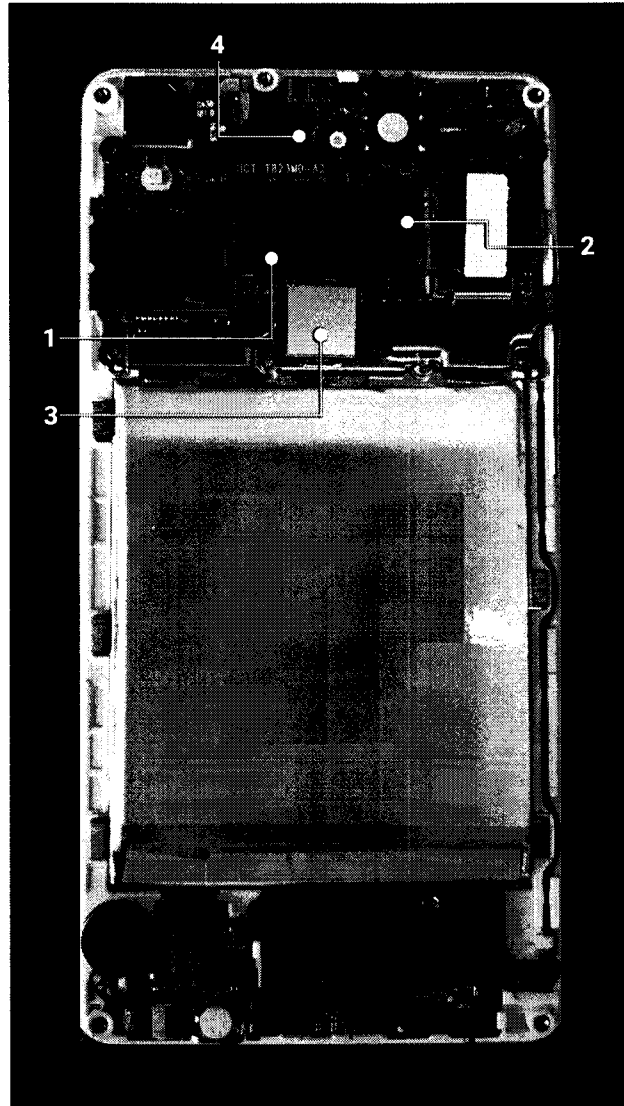
Αξιώσεις

- 5 1. Μέθοδος προστασίας προσωπικών δεδομένων σε φορητές συσκευές με λειτουργικό σύστημα Android που επιτρέπει σε ένα χρήστη να εισέλθει στα δεδομένα της συσκευής μόνο μέσω της αποκλειστικής χρήσης δαχτυλικού αποτυπώματος και της αλληλεπίδρασης του με τον ενσωματωμένο αισθητήρα δαχτυλικού αποτυπώματος, επιτρέποντας την αναβάθμιση του
- 10 επιπέδου ασφάλειας της οργανικής μεθόδου κλειδώματος του λειτουργικού συστήματος της φορητής συσκευής. Χαρακτηρίζεται από τον αποκλεισμό της δυνατότητας παράκαμψης του δαχτυλικού αποτυπώματος μέσω χρήσης οποιουδήποτε άλλου εναλλακτικού τρόπου προστασίας (π.χ. μοτίβο, αλφαριθμητικός κωδικός, κ.τ.λ.) καθώς επίσης και από την ανάγκη
- 15 προαποθήκευσης των δαχτυλικών αποτυπωμάτων του χρήστη, ως αναγκαίο βήμα, ώστε να μπορέσει να λειτουργήσει σύμφωνα με τα βήματα που έχουν περιγραφεί (Σχέδιο 1). Συγκεκριμένα, εφόσον έχει προηγηθεί η προαποθήκευση των δαχτυλικών αποτυπωμάτων, ακολουθεί η εντολή κλειδώματος του χρήστη (Σχέδιο 1 - σημείο 2) και η δημιουργία της
- 20 εγγενούς οθόνης επικάλυψης του Android (Σχέδιο 1 - σημείο 3) που αποκρύπτει τυχόν προσωπικά δεδομένα που εμφανίζονται στην οθόνη της φορητής συσκευής. Στη συνέχεια η συσκευή μπαίνει σε μια κατάσταση αναμονής για άγγιγμα του δαχτυλικού αισθητήρα (Σχέδιο 1 - σημείο 4), το οποίο όταν πραγματοποιηθεί (Σχέδιο 1 - σημείο 5) έχει ως αποτέλεσμα το
- 25 λειτουργικό σύστημα Android να μετατρέψει το εισαγόμενο δαχτυλικό αποτύπωμα σε ψηφιακή μορφή (Σχέδιο 1 - σημείο 6) ώστε να μπορέσει εν τέλει να το συγκρίνει με τα προαποθηκευμένα δαχτυλικά αποτυπώματα (Σχέδιο 1 - σημείο 7). Αν η σύγκριση του εισερχόμενου αποτυπώματος με τη βάση προεγγεγραμμένων αποτυπωμάτων αποδειχτεί επιτυχής τότε
- 30 απομακρύνεται η οθόνη επικάλυψης που δημιουργήθηκε από το λειτουργικό σύστημα Android (Σχέδιο 1 - σημείο 8, Σχέδιο 1 - σημείο 9) και η φορητή συσκευή πλέον έχει ξεκλειδωθεί. Σε αντίθετη περίπτωση, αν η σύγκριση αποδειχτεί ανεπιτυχής τότε το κινητό επιστρέφει στην κατάσταση αναμονής καινούργιου δαχτυλικού αποτυπώματος (Σχέδιο 1 -
- 35 σημείο 8, Σχέδιο 1 - σημείο 4).

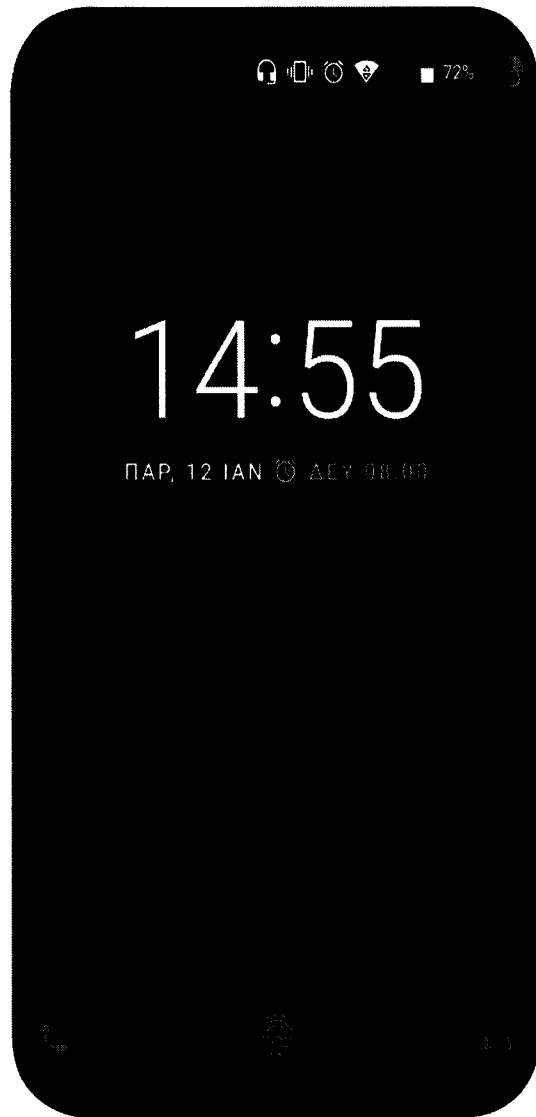
2. Μέθοδος, σύμφωνα με την αξίωση 1, χαρακτηριζόμενη από το γεγονός πως δεν επιτρέπει την εμφάνιση ειδοποιήσεων στην οθόνη μιας φορητής συσκευής χωρίς την εξουσιοδότηση του χρήστη μέσω ενός εκ των καταχωρημένων δαχτυλικών αποτυπωμάτων.
- 40 3. Μέθοδος, σύμφωνα με την αξίωση 1, χαρακτηριζόμενη από το γεγονός πως δεν επιτρέπει την εμφάνιση εισερχόμενων κλήσεων στην οθόνη μιας φορητής συσκευής χωρίς την εξουσιοδότηση του χρήστη μέσω ενός εκ των καταχωρημένων δαχτυλικών αποτυπωμάτων.
- 45 4. Μέθοδος, σύμφωνα με την αξίωση 1, χαρακτηριζόμενη από το γεγονός πως δεν επηρεάζει, κατά τα άλλα, τη λειτουργία μιας φορητής συσκευής και σέβεται τις ήδη καταχωρημένες προτιμήσεις του χρήστη, όπως τους επιλεγμένους ήχους ειδοποίησης και κλήσεις.
- 50 5. Μέθοδος σύμφωνα με την αξίωση 1, χαρακτηριζόμενη από το γεγονός πως συνεχίζει να μεταφέρει στο χρήστη όλες τις απαραίτητες πληροφορίες που σχετίζονται με τη λειτουργία της συσκευής του όπως τη στάθμη της μπαταρίας, της στάθμης του σήματος και της κατάστασης της συνδεσιμότητας (Σχέδιο 4 - σημείο 1).
- 55 6. Συσκευή για την υλοποίηση της προτεινόμενης μεθόδου, η οποία πρέπει απαραίτητως να ενσωματώνει βασικά στοιχεία για την υλοποίηση της εν λόγω μεθόδου και συγκεκριμένα έναν αισθητήρα ανίχνευσης δαχτυλικού αποτυπώματος (Σχέδιο 2 - σημείο 3), έναν επεξεργαστή (Σχέδιο 2 - σημείο 2), μία μνήμη (Σχέδιο 2 - σημείο 1) και μια μητρική (Σχέδιο 2 - σημείο 4) όπου όλα τα ανωτέρω στοιχεία συνδέονται.



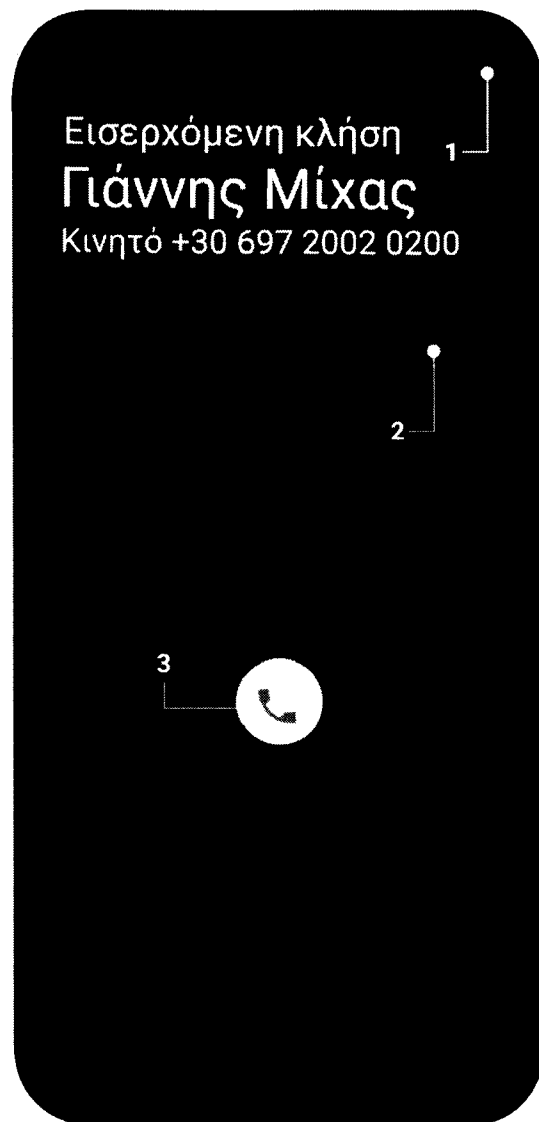
Σχέδιο 1



Σχέδιο 2



Σχέδιο 3



Σχέδιο 4



ΟΡΓΑΝΙΣΜΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ
(Ο.Β.Ι.)

ΕΚΘΕΣΗ ΕΡΕΥΝΑΣ

Αριθμός αίτησης
20170100470

ΕΓΓΡΑΦΑ ΘΕΩΡΟΥΜΕΝΑ ΩΣ ΣΧΕΤΙΚΑ			
Κατηγορία	Σχετικό έγγραφο με επισήμανση, όπου χρειάζεται, των σχετικών παραγράφων	Σχετικό με αξίωση	Διεθν. Ταξινόμηση Int. Cl. 01/01/2018(AL)
EX	WO2018044504 A1 / (QUALCOMM INC) 08.03.2018 *Ολόκληρο το έγγραφο*	1-6	
X	US2009083847 A1 / (FADELL & AL) 26.03.2009 *Περιγραφή: [0029]-[0034],[0039],[0059]-[0062], [0079],[0092]-[0094] Σχήματα: 1,6,15*	1-6	G06F 21/32 G06K 9/00 H04M 1/725
X	EP3185163 A1 / (HUAWEI TECH CO LTD) 28.06.2017 *Ολόκληρο το έγγραφο*	1-6	
OX	GRXP2018058 / (TechManiacsGR) 30.04.2014 *video https://www.youtube.com/watch?v=AAx6eBcAcgs "MLS iQTalk Fingerprint Hands on Review"	1-6	
OX	GRXP2018059 / (DigitalLifeMag) 08.05.2014 *video https://www.youtube.com/watch?v=8lcB50nGf7c "MLS iQTalk Fingerprint hands-on review"	1-6	Τεχνικά πεδία που ερευνήθηκαν
X	US2015033231 A1 / (YE XIN TECHNOLOGY CONSULTING CO LTD) 29.01.2015 *Ολόκληρο το έγγραφο*	6	G06F G06K H04M
Τα αναφερόμενα έγγραφα έχουν σταλεί στον πληρεξούσιο Δικηγόρο			
Ημερομηνία περάτωσης της έρευνας : 08/05/2018			
ΚΑΤΗΓΟΡΙΑ ΔΗΛΟΥΜΕΝΩΝ ΕΓΓΡΑΦΩΝ			
X: ιδιαίτερα σχετικό αν ληφθεί μεμονωμένα Y: ιδιαίτερα σχετικό αν συνδυαστεί με άλλο έγγραφο της ίδιας κατηγορίας A: τεχνολογικό υπόβαθρο O: μη έγγραφη αποκάλυψη P: ενδιάμεσο έγγραφο			
T: βασική θεωρία ή αρχή στην οποία βασίζεται η εφεύρεση E: προγενέστερο δίπλωμα ευρεσιτεχνίας, το οποίο δημοσιεύτηκε την ημερομηνία κατάθεσης ή μετά από αυτήν D: έγγραφο αναφερόμενο στην αίτηση L: έγγραφο αναφερόμενο για άλλους λόγους Δ: μέλος της ίδιας οικογένειας ευρεσιτεχνιών, αντίστοιχο έγγραφο			