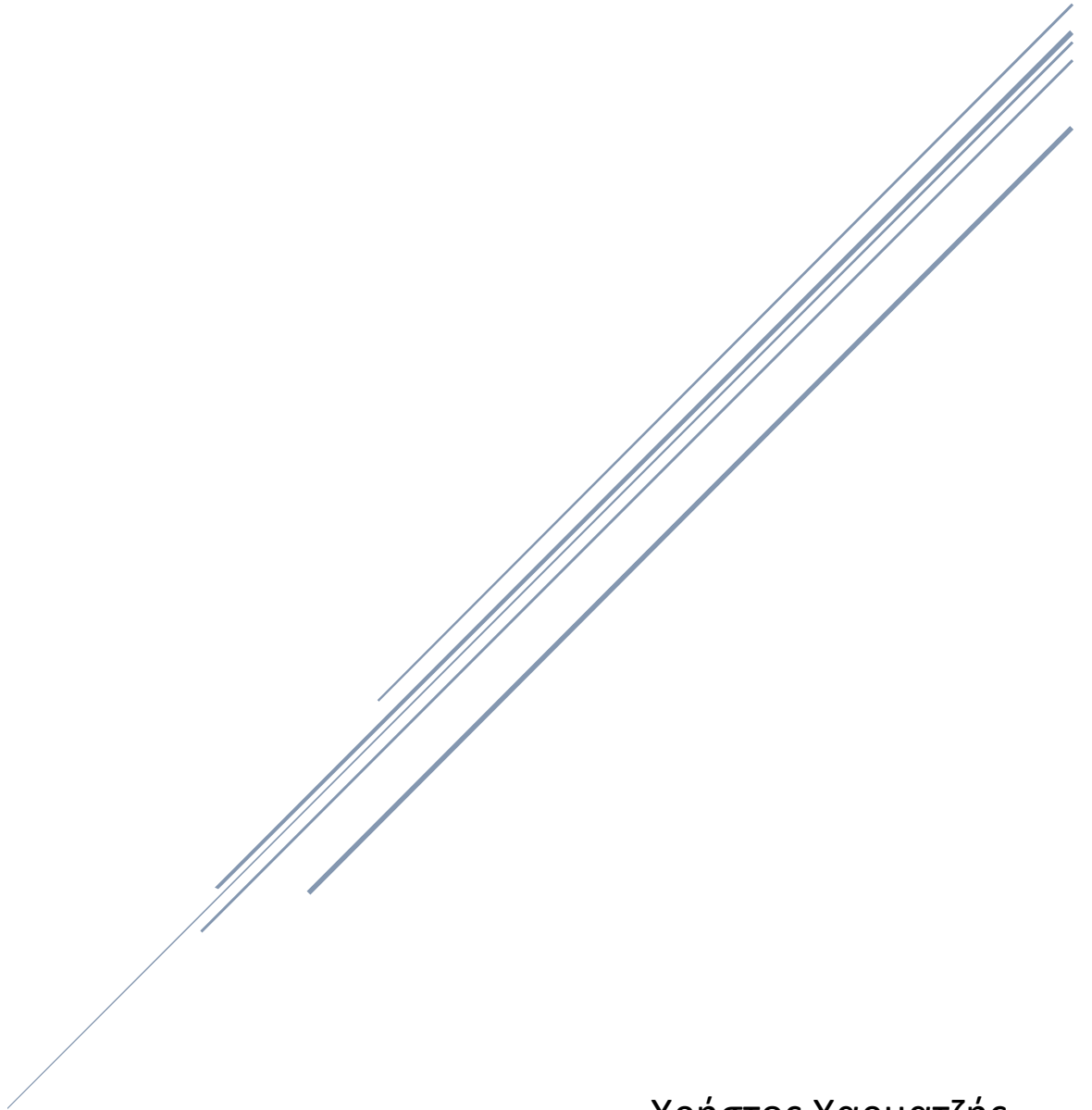


IT4GOV

IT4GOV.IdentityServer



Χρήστος Χαρματζής
29/02/2016

ΓΕΝΙΚΑ

ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΟΥ

Το αντικείμενο του έργου είναι η δημιουργία μίας υπηρεσίας ταυτοποίησης πολιτών, όπου θα ταυτοποιεί τους πολίτες για τα προσωπικά τους στοιχεία και τους διάφορους κωδικούς αριθμούς όπως το ΑΦΜ, ΑΜΚΑ, ΑΤ κλπ. Το συγκεκριμένο πληροφοριακό σύστημα μπορεί, να αποτελέσει βάση, για την πλήρη υποστήριξη των δημόσιων υπηρεσιών στην ανάγκη ταυτοποίησης των πολιτών που αιτούνται κάποια ενέργεια από το Δημόσιο.

Το όνομα της υπηρεσίας για τον διαγωνισμό IT4GOV ονομάζεται IT4GOV.IdentityServer και προσφέρει ακριβώς αυτήν την δυνατότητα ταυτοποίησης.

Το εν λόγω πληροφοριακό σύστημα θα προσφέρει την δυνατότητα εγγραφής των πολιτών, της ταυτοποίησης των εγγεγραμμένων πολιτών και της επεξεργασίας των στοιχείων τους ώστε να είναι ενημερωμένα.

ΥΦΙΣΤΑΜΕΝΗ ΚΑΤΑΣΤΑΣΗ

Στην παρούσα κατάσταση κάθε φορέας ή δημόσια υπηρεσία έχει αναπτύξει το δικό της σύστημα καταχώρισης δεδομένων πολιτών με αποτέλεσμα είτε μερικά στοιχεία να είναι ελλιπή, να καθυστερούν να ενημερωθούν ή να μην ενημερώνονται. Παράδειγμα, όταν ένας πολίτης αλλάξει διεύθυνση κατοικίας θα πρέπει να επισκεφτεί όλες τις υπηρεσίες, όπου στέλνουν κάποια ενημέρωση στο σπίτι του, όπως εφορία, ΔΕΗ, ΕΥΔΑΠ, δήμος κλπ.

Επίσης, όταν ένας πολίτης επισκέπτεται έναν φορέα ή δημόσια υπηρεσία θα πρέπει πρώτα να ερωτηθεί για τον ειδικό κωδικό μητρώου της αντίστοιχης υπηρεσίας πχ. Εφορία => ΑΦΜ, ΙΚΑ => Αριθμός μητρώου ΙΚΑ ή ΑΜΚΑ. Έπειτα, να ταυτοποιηθεί, σε πολλές των περιπτώσεων με την επίδειξη της αστυνομικής του ταυτότητας, από τον υπάλληλο. Τέλος, μπορεί ο πολίτης να ερωτηθεί επιπλέον για κάποια άλλα προσωπικά δεδομένα όπου δεν υπάρχουν στην βάση δεδομένων της υπηρεσίας και είναι απαραίτητα για την ολοκλήρωση της αίτησης από τον υπάλληλο.

ΣΤΟΧΟΙ

Στόχοι της υπηρεσίας IT4GOV.IdentityServer είναι να διευκολύνει τους πολίτες:

1. με τις διάφορες δημόσιες υπηρεσίες όπου χρειάζεται να ταυτοποιηθεί προτού προχωρήσει σε οποιαδήποτε ενέργεια αίτησης,
2. ώστε να μην χρειάζεται να θυμούνται τους διάφορους κωδικούς αριθμούς όπως ΑΦΜ, ΑΜΚΑ, ΑΤ κλπ.

Στόχοι της υπηρεσίας IT4GOV.IdentityServer είναι οι δημόσιες υπηρεσίες:

1. να έχουν μία κεντρική υπηρεσία δεδομένων για τα βασικά δεδομένα των πολιτών
2. να διευκολύνονται στην ταυτοποίηση των πολιτών για πιο ασφαλείς και άμεσες ενέργειες με τους πολίτες,
3. να μειωθεί η πιθανότητα λάθους των προσωπικών δεδομένων του εξυπηρετούμενου πολίτη,

4. να μην παρέχονται πληροφορίες του πολίτη στην υπηρεσία, οι οποίες δεν χρειάζονται για την διεκπεραίωση της αίτησης από την υπηρεσία,
5. να μην χρειάζονται από τις δημόσιες υπηρεσίες περεταίρω γραφειοκρατία για την ενημέρωση των στοιχείων των πολιτών,
6. να μην χρειάζονται περαιτέρω εργατώρες για την συντήρηση δεδομένων για τα προσωπικά στοιχεία των πολιτών στις διάφορες δημόσιες υπηρεσίες.

ΑΝΑΜΕΝΟΜΕΝΑ ΟΦΕΛΗ

Τα τελευταία έτη, με την ραγδαία ανάπτυξη της τεχνολογίας και των κινητών τηλεφώνων, καθιστώντας το διαδίκτυο το πιο αξιοποιήσιμο εργαλείο στην ανάπτυξη ενός κράτους, η αξιοποίηση της υπηρεσίας IT4GOV.IdentityServer θα δώσει στο δημόσιο την κατάλληλη ώθηση στην:

- μείωση της γραφειοκρατίας
- στον εκσυγχρονισμό των υποδομών της
- στην ομογενοποίηση υπηρεσιών ταυτοποίησης που χρησιμοποιούνται ευρύτατα
- στην ενοποίηση των δεδομένων για την πιο αξιόπιστη χρήση τους
- στην μελλοντική ενοικίαση της υπηρεσίας στον ιδιωτικό τομέα όπου χρειάζονται υπηρεσίες ταυτοποίησης πολιτών. Π.χ. τράπεζες, ιδιωτικά θεραπευτικά κέντρα, ΕΥΔΑΠ, ΔΕΗ, ΟΤΕ, καταστήματα εταιριών κινητής τηλεφωνίας, γραφεία κτηματογράφησης κα.

ΛΕΙΤΟΥΡΓΙΚΕΣ ΚΑΙ ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

Το IT4GOV.IdentityServer θα προσφέρει στους πολίτες και στους εμπλεκόμενους φορείς (οργανισμοί, άλλες δημόσιες υπηρεσίες), υψηλής ποιότητας και ευχρηστίας υπηρεσίες, προσαρμοσμένες κάθε φορά στις απαιτήσεις των χρηστών της υπηρεσίας. Οι εφαρμογές που έχουν ήδη αναπτυχθεί στους διάφορους φορείς θα αλληλεπιδρούν μέσω διαδικτυακών υπηρεσιών (web services) με το IT4GOV.IdentityServer στο επίπεδο των απαιτούμενων πληροφοριών σε σχέση με την ταυτοποίηση του πολίτη.

Η υπηρεσία IT4GOV.IdentityServer είναι μία web υπηρεσία ταυτοποίησης χρηστών. Η ταυτοποίηση πραγματοποιείται χρησιμοποιώντας ένα workflow **two-factor authentication** ([Wikipedia](#)) με πρώτο βήμα ταυτοποίησης το **όνομα χρήστη** και τον **κωδικό** του και δεύτερο βήμα ταυτοποίησης ένας κωδικός με SMS στο **κινητό του τηλεφώνου**. Η υπηρεσία IT4GOV.IdentityServer είναι μία υπηρεσία όπου χρησιμοποιεί ως στάνταρτ το **OpenID Connect** ([Wikipedia](#)), όπου είναι ένα επίπεδο ταυτοποίησης το οποίο είναι πάνω από το επίπεδο ταυτοποίησης **OAuth 2.0** ([Wikipedia](#)).

ΥΠΗΡΕΣΙΑ ΕΓΓΡΑΦΗΣ ΠΟΛΙΤΗ

Με την ανάπτυξη της τεχνολογίας, οι τελευταίες συσκευές smart phones παρέχουν την δυνατότητα ταυτοποίησης των χρηστών τους.

Δηλαδή η συσκευή smart phone αναγνωρίζει τον χρήστη είτε από το δακτυλικό αποτύπωμα (λίστα με τις συσκευές smart phones που παρέχουν την δυνατότητα [αυτή](#)), είτε από την αναγνώριση προσώπου και ίριδας “Windows Hello” ([σύνδεσμος](#)). Οπότε, πια η smart phone συσκευή για να ξεκλειδώσει χρειάζεται τα βιομετρικά στοιχεία του χρήστη του. Αυτό καθιστά την συσκευή να είναι

ασφαλής από κακόβουλους χρήστες όπου προσπαθούν να έχουν πρόσβαση στην συσκευή και να κλέψουν προσωπικά δεδομένα από την συσκευή.

Επίσης, κάθε πελάτης οποιασδήποτε εταιρίας κινητής τηλεφωνίας, όπου έχει αγοράσει κάποιον αριθμό κινητού τηλεφώνου έχει καταγραφεί και ταυτοποιηθεί, σύμφωνα με Ν. 3783/2009 "Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις" (ΦΕΚ 136/Α/7-8-09), ([ΕΕΤΤ](#)).

Ο συνδυασμός τον παραπάνω μας οδηγεί στο συμπέρασμα ότι ένας πολίτης, οποίος κατέχει μία τέτοια συσκευή, θα μπορεί να ταυτοποιηθεί από το κινητό του.

Το IT4GOV.IdentityServer είναι μία υπηρεσία η οποία, οι πολίτες που:

1. έχουν στην κυριότητα τους μία τέτοια συσκευή,
2. θα την έχουνε ρυθμίσει καταλλήλως ώστε να ξεκλειδώνει με τα βιομετρικά χαρακτηριστικά,
3. θα έχουν ταυτοποιηθεί ως χρήστες από τις εταιρίες κινητής τηλεφωνίας, σύμφωνα με τον ισχύοντα νόμο
4. και θα επιθυμούν να ταυτοποιούνται με βάση το κινητό τους

θα μπορούν να εγγράφονται σε αυτήν την υπηρεσία.

Τα στοιχεία που θα εισάγει ο πολίτης στην υπηρεσία θα είναι:

1. Όνομα χρήστη και κωδικός
2. Ονοματεπώνυμο, πατρώνυμο, ημερομηνία γέννησης
3. Διεύθυνση
4. Email, αριθμός κινητού
5. ΑΦΜ
6. ΑΜΚΑ
7. Αριθμός ταυτότητας
8. Φωτογραφία πολίτη

ΥΠΗΡΕΣΙΑ ΤΑΥΤΟΠΟΙΗΣΗΣ ΠΟΛΙΤΗ

Από την στιγμή που ο εγγεγραμμένος χρήστης έχει ταυτοποιηθεί από τον μηχανισμό IT4GOV.IdentityServer, θα μπορεί να πραγματοποιήσει συναλλαγές με τους φορείς χωρίς να επιδείξει ΑΤ και να παρέχουν μόνο τα κατάλληλα στοιχεία (ΑΜΚΑ, ΑΦΜ, αριθμός μητρώου ΙΚΑ κλπ.).

Παρακάτω, περιγράφεται ένα απλό παράδειγμα χρήσης του IT4GOV.IdentityServer:

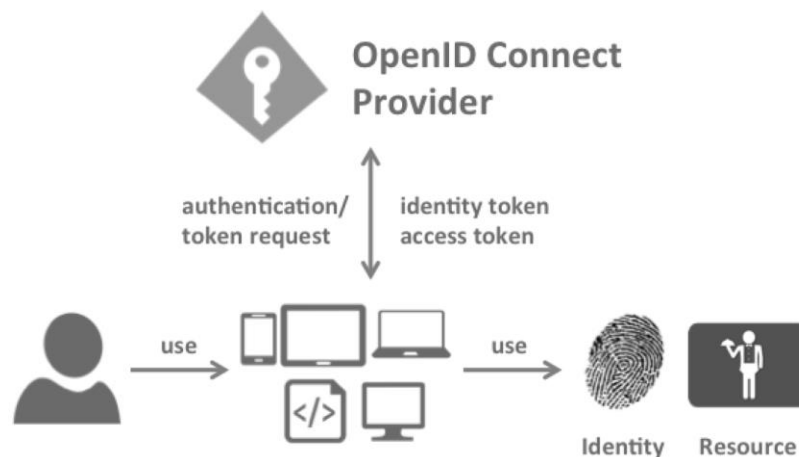
1. Ο υπάλληλος θα ρωτάει τον πολίτη, εάν επιθυμεί να ταυτοποιηθεί μέσω της υπηρεσίας IT4GOV.IdentityServer.
2. Στην περίπτωση που ο πολίτης θα εγκρίνει την παραπάνω ενέργεια, ο υπάλληλος θα εμφανίσει σε μία συσκευή αφής την φόρμα, όπου θα πρέπει να συμπληρώσει ο πολίτης για να ταυτοποιηθεί.
3. Ο πολίτης θα εισάγει σε αυτήν την φόρμα το username και το password.

4. Ο IT4GOV.IdentityServer από την στιγμή που θα ταυτοποιεί τον χρήστη θα μεταφέρεται σε μία δεύτερη φόρμα όπου θα του ζητείται να εισάγει το 6ψήφιο κωδικό που του έχει αποσταλεί στο κινητό του σε μορφή SMS.
5. Ο πολίτης θα εισάγει 6ψήφιο κωδικό στην φόρμα (two-factor authentication).
6. Θα ταυτοποιείται ο 6ψήφιος κωδικός από τον IT4GOV.IdentityServer και σε περίπτωση επιτυχίας θα εμφανίζεται μία φόρμα όπου ο πολίτης θα μπορεί να επιλέγει τα προσωπικά του δεδομένα θα χρειάζονται από την εφαρμογή του υπαλλήλου.
7. Τα στοιχεία τα οποία θα είναι απαραίτητα θα έχουν ένα θαυμαστικό δίπλα από το αντίστοιχο στοιχείο και τα στοιχεία που θα είναι προαιρετικά δεν θα έχουν θαυμαστικό.
8. Με την αποδοχή της τελευταίας φόρμας θα εισάγονται αυτόματα στην φόρμα του υπαλλήλου τα προσωπικά δεδομένα που θα έχει επιλέξει ο πολίτης.

ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΠΡΟΤΕΙΝΟΜΕΝΗΣ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΟΣ

Σύμφωνα με το παρακάτω σχήμα ο IT4GOV.IdentityServer όπου είναι ο OpenID Connect Provider παρέχει υπηρεσίες ταυτοποίησης με tokens. Ο χρήστης μέσω των διαφόρων clients χρησιμοποιεί την υπηρεσία ταυτοποίησης και έχει πρόσβαση στα δεδομένα του προφίλ του.



ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΛΟΓΙΣΜΙΚΑ

Το project έχει αναπτυχθεί με το **ASP.NET Core** (<https://github.com/aspnet/Home>) όπου είναι μία καινούργια πλατφόρμα open source και cross platform που αναπτύσσεται από την Microsoft, για την δημιουργία web-project.

Επίσης, το project IT4GOV.IdentityServer χρησιμοποιεί το IdentityServer4 ([σύνδεσμος](#)) όπου είναι το framework που έχει αναπτυχθεί με βάση τις προδιαγραφές του OpenID Connect ([σύνδεσμος](#)) και του OAuth 2.0 ([σύνδεσμος](#)).

ΚΑΤΑΛΛΗΛΟΛΗΤΑ ΛΟΓΙΣΜΙΚΩΝ

Ο λόγος που έχει αναπτυχθεί σε ASP.NET Core είναι γιατί:

- είναι μία καινούργια web τεχνολογία με όλα τα καινούργια τεχνολογικά χαρακτηριστικά ακολουθώντας τις βέλτιστες πρακτικές σε έργα πληροφορικής,
- υποστηρίζεται από μία μεγάλη εταιρία software την Microsoft,
- είναι open source και cross platform και μπορεί να εγκατασταθεί σε λειτουργικά συστήματα Windows, Linux, Mac OS X
- τέλος έχει μία εντυπωσιακή απόδοση, με παραπάνω από 1 εκατομμύριο requests/sec σε plain text with HTTP Pipelining (<https://github.com/aspnet/benchmarks>).

ΆΔΕΙΕΣ ΧΡΗΣΗΣ

Η άδεια χρήσης του ASP.NET Core είναι η Apache License, Version 2.0, January 2004 ([σύνδεσμος](#)).

Η άδεια χρήσης του IdentityServer4 είναι η Apache License, Version 2.0, January 2004 ([σύνδεσμος](#))

ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

Το πρωτόκολλο OpenID Connect και το OAuth 2.0 μπορεί να συνδεθεί με οποιαδήποτε εφαρμογή είτε αυτή είναι server side, είτε είναι client side, είτε είναι Desktop app, native app, ή web app. Η client ανάπτυξη διασύνδεσης με την υπηρεσία IT4GOV.IdentityServer παρέχει ένα ευρύ φάσμα τεχνολογιών και γλωσσών προγραμματισμού (Java, PHP, Python, Node.JS, JavaScript κλπ.)

ΩΡΙΜΟΤΗΤΑ

Η ιδέα της ταυτοποίησης των χρηστών είναι μία ιδέα η οποία βρίσκει όλο και πιο πολύ εφαρμογή σε enterprise πληροφοριακά συστήματα με εκατομμύρια χρήστες. Χαρακτηριστικά αναφέρεται πως μεγάλες εταιρίες έχουν υιοθετήσει αυτό το σύστημα όπως η Google, η Microsoft, το Facebook, το Tweeter, το LinkedIn κα.

Η υπηρεσία IT4GOV.IdentityServer σε περίπτωση που επιλεγεί μπορεί να αναπτυχθεί περαιτέρω για τις ανάγκες ταυτοποίησης πολιτών με αγορά πιστοποιητικών για https συνδέσεων, σύμβαση με εταιρία παροχής αποστολής SMS, φιλοξενία σε cloud περιβάλλον για τις αυξανόμενες ανάγκες τις υπηρεσίας από χρήστες, την δημιουργία σχεσιακής βάσης δεδομένων, κατάλληλου σχήματος και σύνδεσης με την εφαρμογή κα.