ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ **ΝΟΜΟΣ ΑΤΤΙΚΗΣ** **ΔΗΜΟΣ ΓΑΛΑΤΣΙΟΥ** **Δ/νση Οικονομικών Υπηρεσιών** **Τμήμα Προγραμματισμού Οργάνωσης & Πληροφορικής**	Γαλάτσι, 28/6/2019

ΜΕΛΕΤΗ ΓΙΑ ΤΗ ΔΗΜΙΟΥΡΓΙΑ ΕΦΑΡΜΟΓΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΧΡΗΣΤΩΝ (AUTHSERVER)

ΠΕΡΙΕΧΟΜΕΝΑ:

ΤΕΧΝΙΚΗ ΕΚΘΕΣΗ

Ο Δήμος Γαλατσίου, στα πλαίσια της συντήρησης του πληροφοριακού συστήματος του και για την διασφάλιση της εύρυθμης, απρόσκοπτης, αποτελεσματικής και ασφαλούς λειτουργίας του, κρίνει αναγκαίο να δημιουργήσει εφαρμογή ταυτοποίησης χρηστών, που έχει σαν στόχο τη διευκόλυνση και απλοποίηση της παροχής νέων υπηρεσιών σε ταυτοποιημένους χρήστες.

Η παρούσα μελέτη αφορά ανάθεση υπηρεσιών σύμφωνα με τις διατάξεις

- του Ν. 3463/2006 «Δημοτικός και Κοινοτικός Κώδικας»,
- του Ν. 4412/2016 «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών(προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)»,
- του Ν. 4555/2018 «Μεταρρύθμιση του θεσμικού πλαισίου της Τοπικής Αυτοδιοίκησης - Εμβάθυνση της Δημοκρατίας – Ενίσχυση της Συμμετοχής – Βελτίωση της οικονομικής και αναπτυξιακής λειτουργίας των Ο.Τ.Α.»,

όπως αυτές αναδιατυπώθηκαν κατά περίπτωση και διατηρήθηκαν σε ισχύ, καθώς και λοιπών διατάξεων που ορίζονται στην σχετική Πρόσκληση ενδιαφέροντος.

Ο Συντάξας

Γκιουζέλης Ιωάννης

προϊστάμενος Τμήματος

Προγραμματισμού, Οργάνωσης & Πληροφορικής

ΘΕΩΡΗΘΗΚΕ

Η προϊσταμένη

Δ/νσης Οικονομικών Υπηρεσιών

Πρίντζου Ελένη

ΤΕΧΝΙΚΗ ΠΕΡΙΓΡΑΦΗ

Στη συνέχεια ακολουθεί η περιγραφή της εφαρμογής (συστήματος) ταυτοποίησης χρηστών που πρέπει να υλοποιήσει ο ανάδοχος.

Εισαγωγή

Η εφαρμογή ταυτοποίησης χρηστών έχει σαν στόχο τη διευκόλυνση και απλοποίηση της παροχής νέων υπηρεσιών σε ταυτοποιημένους χρήστες. Με την εφαρμογή αυτή θα υπάρχει διαβαθμισμένη πιστοποίηση ανάλογα με το αίτημα του κάθε χρήστη για παροχή υπηρεσίας.

Η νέα διαδικασία ταυτοποίησης θα αποτελεί πρότυπο αυθεντικοποίησης και για οποιαδήποτε άλλη εφαρμογή δημιουργήσει ο Δήμος στο μέλλον. Παράλληλα, θα δημιουργηθεί μια υποδομή που μπορεί να επιλύσει προβλήματα στην εσωτερική διαχείριση χρηστών στο Δήμο, με δεδομένο ότι στην υποδομή του συστήματος αυθεντικοποίησης θα αποτυπώνεται η δομή και η ιεραρχία του Δήμου, μέσω ενός υποσυστήματος καταλόγου (LDAP), το οποίο θα αποτελεί το πρότυπο για την διαχείριση των χρηστών σε πληροφοριακά συστήματα του.

Βασικό στοιχείο της νέας κατάστασης, που θα επιφέρει η δημιουργία και η λειτουργία ενός τέτοιου συστήματος ταυτοποίησης, είναι και η μετακύλιση της διαδικασίας ταυτοποίησης σε «έμπιστες» τρίτες πηγές. Οι πηγές αυτές παρέχουν στοιχεία αυθεντικοποίησης για τις εφαρμογές (username/password) και οι ίδιες έχουν προχωρήσει στην ταυτοποίηση του χρήστη. Χαρακτηριστικό παράδειγμα αυτής της περίπτωσης αποτελεί η εφαρμογή του TAXISnet, όπου οι Δ.Ο.Υ. της χώρας έχουν ταυτοποιήσει όλους τους χρήστες του συστήματός τους με φυσικό τρόπο και εγγυώνται την αντιστοιχία στοιχείων χρήστη με φυσικό ή νομικό πρόσωπο. Η διαδικασία αυτή αποτελεί μια ισχυρή μορφή ταυτοποίησης, η οποία μπορεί να δώσει τη δυνατότητα παροχής ισχυρά προσωποποιημένων πληροφοριών προς το Δήμο αντίστοιχη με αυτή της Γ.Γ.Π.Σ. (όπως π.χ. δημοτική ενημερότητα, κατάσταση οφειλών, ρύθμιση οφειλών κ.α.).

Βασικά χαρακτηριστικά

Τα βασικά χαρακτηριστικά του συστήματος θα είναι:

- **οι Χρήστες του συστήματος**: Ως χρήστες του συστήματος θεωρούνται Φυσικά Πρόσωπα (πολίτες), Νομικά Πρόσωπα (φορείς), Υπάλληλοι του Δήμου, Διαχειριστές και τρίτες εφαρμογές του Δήμου
- **η Διαβαθμισμένη Πρόσβαση**: Όπως προκύπτει από τα παραπάνω είναι αναγκαίο το σύστημα αυτό να προσφέρει διαχείριση διαβαθμισμένης πρόσβασης στην πληροφορία, σύμφωνα με τους ρόλους των Χρηστών, αλλά και με εξαιρέσεις που μπορεί να προκύψουν
- **η Ενιαία πρόσβαση Χρηστών**: Η προτεινόμενη λύση θα υποστηρίζει ενιαία πρόσβαση (single sign-on) σε σύγχρονες διαδικτυακές εφαρμογές και APIs μέσω των διαδεδομένων πρωτοκόλλων αυθεντικοποίησης OpenID Connect και oAuth2. Και τα δύο πρωτόκολλα επιτρέπουν σε εφαρμογές να αιτηθούν πρόσβαση (Access Tokens) από μια κεντρική υπηρεσία (Security Token Service) και να επικοινωνήσουν μέσω APIs
- **η Πρόσβαση τρίτων εφαρμογών:** Επίσης, θα υπάρχει συνδυαστικός τρόπος επικοινωνίας μέσω της αυθεντικοποίησης μιας τρίτης εφαρμογής και της αυθεντικοποίησης ενός χρήστη με Όνομα χρήστη και Κωδικό.

Δομικά στοιχεία λειτουργίας

Τα δομικά στοιχεία λειτουργίας του συστήματος θα είναι:

- ο κεντρικός εξυπηρετητής πιστοποίησης χρηστών που πρέπει να έχει τη δυνατότητα να χρησιμοποιεί ως βάση χρηστών την υπηρεσία καταλόγου του Δήμου (LDAP)
- η ομάδα των εφαρμογών που έχουν το ρόλο πελάτη (client) και είναι συνδεδεμένες με την υπηρεσία Ενιαίας Πρόσβασης Χρηστών μέσω ενός καθορισμένου πρωτοκόλλου επικοινωνίας.
- το σύστημα Ενιαίας Πρόσβασης που θα ταυτοποιεί και θα πιστοποιεί Χρήστες στις υποστηριζόμενες από αυτό εφαρμογές και υπηρεσίες.
- η ροή των διεργασιών που απαιτείται για τη σύνδεση ενός χρήστη σε εφαρμογή ή υπηρεσία υποστηριζόμενη από το σύστημα ενιαίας πρόσβασης.

Εγγραφή χρηστών (πολιτών ή φορέων) στην χρήση ηλεκτρονικών υπηρεσιών

Η εγγραφή των πολιτών ή φορέων (νομικών και φυσικών προσώπων) στις ηλεκτρονικές υπηρεσίες που θα παρέχει ο Δήμος θα διενεργείται με διάφορους τρόπους, ανάλογα με τους περιορισμούς και τις ανάγκες που ορίζει η εκάστοτε υπηρεσία. Οι υπηρεσίες που θα παρέχονται διακρίνονται στα εξής διαβαθμισμένα επίπεδα:

- **Επίπεδο 1**: ανώνυμη πρόσβαση η οποία μπορεί να επιτευχθεί μέσω της τεχνολογίας blockchain. Αυτός είναι ο ελάχιστός δυνατός τρόπος αυθεντικοποίησης, ικανός όμως να ελέγξει τη μοναδικότητα των χρηστών, που μπορεί να χρησιμοποιηθεί π.χ. στο σύστημα ανώνυμης ηλεκτρονικής ψηφοφορίας
- **Επίπεδο 2**: μέσω της τεχνολογίας oAuth2 για αυθεντικοποίηση μπορεί να γίνει χρήση των κοινωνικών δικτύων, όπως Facebook και Google.
- **Επίπεδο 3**: μέσω της τεχνολογίας oAuth2 και την υπηρεσία που παρέχει η Γ.Γ.Π.Σ. για αυθεντικοποίηση μέσω TAXISnet. Αυτός ο τρόπος χρησιμοποιείται σε περιπτώσεις που είναι αναγκαίο ο χρήστης να ταυτοποιηθεί μέσω του Α.Φ.Μ. του. Οι περιπτώσεις αυτές αφορούν π.χ. την προβολή ιστορικού και την είσπραξη βεβαιωμένων οφειλών.

Εγγραφή χρηστών (υπαλλήλων) του Δήμου

Η αυθεντικοποίηση χρηστών δεν θα περιλαμβάνει μόνο την ταυτοποίηση πολιτών ή φορέων (νομικών και φυσικών προσώπων), αλλά και την ταυτοποίηση των υπαλλήλων του Δήμου. Απαιτείται να υπάρχει συγχρονισμός μεταξύ του LDAP του Δήμου και του ενιαίου συστήματος αυθεντικοποίησης χρηστών. Όταν δημιουργείται ή απενεργοποιείται ένας χρήστης στο LDAP του Δήμου, η Ενιαία πρόσβαση Χρηστών θα ενημερώνεται με αυτοματοποιημένο τρόπο και ο διαχειριστής του Δήμου θα πρέπει σε δεύτερη φάση να ορίζει τα δικαιώματα για την πρόσβαση του χρήστη στις εφαρμογές.

Ένταξη τρίτου συστήματος (Πιστοποίηση τρίτων συστημάτων)

Το σύστημα ταυτοποίησης θα αναλαμβάνει και την εγκαθίδρυση «σχέσης εμπιστοσύνης» με τρίτες εφαρμογές και διαδικτυακές υπηρεσίες έχοντας τις κατάλληλες πιστοποιήσεις, ηλεκτρονικές υπογραφές, πρωτόκολλα ασφαλούς διασύνδεσης και μετάδοσης δεδομένων. Κάθε τρίτο σύστημα και κάθε web API που επιθυμεί πρόσβαση θα πρέπει να είναι εγγεγραμμένο σε συγκεκριμένο μητρώο πρόσβασης. Τα τρίτα συστήματα θα αιτούνται Access

tokens από την υπηρεσία Security token service που παρέχει η Ενιαία πρόσβαση Χρηστών και στη συνέχεια θα τους χορηγείται πρόσβαση.

Ροή διεργασιών του συστήματος

Η ροή διεργασιών του συστήματος θα έχει ως εξής :

- Αίτηση σύνδεσης του χρήστη σε προστατευόμενη από το σύστημα ενιαίας πρόσβασης χρηστών διαδικτυακή εφαρμογή
- Ανακατεύθυνση του χρήστη στο σημείο του συστήματος ενιαίας πρόσβασης χρηστών για εισαγωγή των διαπιστευτηρίων του
- Επικοινωνία του συστήματος ενιαίας πρόσβασης χρηστών με την υπηρεσία καταλόγου για επιβεβαίωση των εισαχθέντων διαπιστευτηρίων
- Αποστολή αποτελέσματος ελέγχου ταυτότητας στο σύστημα ενιαίας πρόσβασης
- Στην περίπτωση που ο έλεγχος ταυτότητας επιστρέψει θετικό αποτέλεσμα θα ενεργοποιείται μοναδικό Session και θα γίνεται επιστροφή του χρήστη στην προστατευόμενη εφαρμογή ως συνδεδεμένος χρήστης
- Αίτηση ανάκτησης των ιδιοτήτων (LDAP Attributes) του πιστοποιημένου χρήση από το σύστημα ενιαίας πρόσβασης
- Επιστροφή των εγκεκριμένων από το σύστημα ενιαίας πρόσβασης ιδιοτήτων του συγκεκριμένου χρήστη στην εφαρμογή για περαιτέρω εκμετάλλευση

Όταν η περιγραφείσα διαδικασία έχει επιτυχώς ολοκληρωθεί, τότε η αυτοματοποιημένη σύνδεση του χρήστη σε συνεργαζόμενες διαδικτυακές υπηρεσίες/υποσυστήματα θα ενεργοποιείται. Η αυτοματοποιημένη σύνδεση του χρήστη στις υπηρεσίες θα τερματίζεται όταν λήξει το προαναφερθέν Session, το οποίο συμβαίνει όταν περάσει ένα μεγάλο χρονικό διάστημα ή όταν ο χρήστης επιλέξει να «κλείσει» την εφαρμογή ή τον φυλλομετρητή του (web browser).

Λειτουργικές Μονάδες της Ενιαίας πρόσβασης Χρηστών

Για την υλοποίηση των παραπάνω, το σύστημα ενιαίας πρόσβασης χρηστών θα αποτελείται από τις ακόλουθες λειτουργικές μονάδες:

- Γραφικές διεπαφές εισόδου εγγεγραμμένων χρηστών και εγγραφής νέου χρήστη
- Βάση δεδομένων συστήματος, με ικανότητα καταγραφής όλων των απαραίτητων δεδομένων χρηστών και παροχή αποτύπωσης δομής και ιεραρχίας του Δήμου
- Μονάδα διασύνδεσης με το TAXISnet και πιθανές άλλες «έμπιστες» μονάδες ταυτοποίησης
- Μονάδα διασύνδεσης εσωτερικών υπηρεσιών του Δήμου
- Μονάδα διασφάλισης της εμπιστευτικότητας και ασφάλειας των δεδομένων των εγγεγραμμένων χρηστών
- Μονάδα ελέγχου διαβάθμισης επιπέδου ταυτοποίησης και παρεχόμενων δικαιωμάτων χρήστη

Χρονοδιάγραμμα υλοποίησης

Η δημιουργία της εφαρμογής ταυτοποίησης χρηστών, όπως περιγράφηκε παραπάνω, πρέπει να ολοκληρωθεί και να παραδοθεί από τον ανάδοχο μέσα σε διάστημα 2 μηνών από την υπογραφή της σύμβασης.

Ο Συντάξας

Γκιουζέλης Ιωάννης

προϊστάμενος Τμήματος

Προγραμματισμού, Οργάνωσης & Πληροφορικής

ΘΕΩΡΗΘΗΚΕ

Η προϊσταμένη

Δ/νσης Οικονομικών Υπηρεσιών

ρίντζου Ελένη

ΕΝΔΕΙΚΤΙΚΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ

Το μέγιστο συνολικό κόστος της ανωτέρω ανάθεσης υπηρεσιών για τη δημιουργία της εφαρμογής ταυτοποίησης χρηστών για τον Δήμο Γαλατσίου, προϋπολογίζεται σε € 2.480, συμπεριλαμβανομένου Φ.Π.Α. 24%. Οι προσφορές για την παροχή των υπηρεσιών αυτών δεν πρέπει να υπερβαίνουν (ως συνολικό κόστος) το ποσό των € 2.480, συμπεριλαμβανομένου Φ.Π.Α. 24%.

Αναλυτικότερα η δαπάνη έχει ως εξής:

ΠΕΡΙΓΡΑΦΗ ΑΝΤΙΚΕΙΜΕΝΟΥ	ΚΟΣΤΟΣ	Φ.Π.Α. 24%	ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ
Δημιουργία εφαρμογής ταυτοποίησης χρηστών (Authserver) για τον Δήμο Γαλατσίου	€ 2000	€ 480	€ 2480

Η σχετική πίστωση λαμβάνεται από τον προϋπολογισμό του Δήμου Γαλατσίου για το οικονομικό έτος 2019 και θα βαρύνει τον Κ.Α. 10.6266.0001, με προϋπολογισθείσα μέγιστη συνολική δαπάνη €2.480, συμπεριλαμβανομένου Φ.Π.Α. 24%.

Ο Συντάξας

Γκιουζέλης Ιωάννης

προϊστάμενος Τμήματος

Προγραμματισμού, Οργάνωσης & Πληροφορικής

ΘΕΩΡΗΘΗΚΕ

Η προϊσταμένη

Δ/νσης Οικονομικών Υπηρεσιών

Ιρίντζου Ελένη

ΣΥΓΓΡΑΦΗ ΥΠΟΧΡΕΩΣΕΩΝ

ΑΡΘΡΟ 1°

ΑΝΤΙΚΕΙΜΕΝΟ ΤΗΣ ΑΝΑΘΕΣΗΣ ΥΠΗΡΕΣΙΩΝ

Δημιουργία εφαρμογής ταυτοποίησης χρηστών (Authserver) για τον Δήμο Γαλατσίου.

ΑΡΘΡΟ 2°

ΙΣΧΥΟΥΣΕΣ ΔΙΑΤΑΞΕΙΣ

Η ανάθεση των υπηρεσιών θα γίνει σύμφωνα με τις διατάξεις που αναγράφονται στην Τεχνική Έκθεση, την Πρόσκληση ενδιαφέροντος και την Σύμβαση.

ΑΡΘΡΟ 3°

ΣΥΜΒΑΤΙΚΑ ΣΤΟΙΧΕΙΑ

Τα συμβατικά στοιχεία της ανάθεσης υπηρεσιών είναι:

1) η Πρόσκληση ενδιαφέροντος
2) η Τεχνική Έκθεση
3) η Τεχνική Περιγραφή
4) ο Ενδεικτικός Προϋπολογισμός
5) η Συγγραφή Υποχρεώσεων
6) η Προσφορά του Αναδόχου

ΑΡΘΡΟ 4°

ΠΡΟΣΦΟΡΕΣ

Η προσφορά του αναδόχου θα αποτελεί αναπόσπαστο μέρος της σχετικής σύμβασης. Από την προσφορά του αναδόχου θα πρέπει να προκύπτει σαφώς ότι οι προσφερόμενες υπηρεσίες συμφωνούν πλήρως με τα στοιχεία της παρούσας μελέτης.

ΑΡΘΡΟ 5°

ΣΥΜΒΑΣΗ

Ο ανάδοχος των υπηρεσιών, μετά την έγκριση του αποτελέσματος κατακύρωσης της ανάθεσης των υπηρεσιών, είναι υποχρεωμένος να έρθει σε επικοινωνία με το τμήμα Προμηθειών και Αποθήκης της Διεύθυνσης Οικονομικών Υπηρεσιών του Δήμου Γαλατσίου για την υπογραφή της σύμβασης ανάθεσης των υπηρεσιών. Με την υπογραφή της σύμβασης τα οριζόμενα στα συμβατικά στοιχεία της ανάθεσης των υπηρεσιών θα είναι δεσμευτικά για τον ανάδοχο.

ΑΡΘΡΟ 6°

ΠΡΟΣΩΠΙΚΟ ΚΑΙ ΕΥΘΥΝΗ ΤΟΥ ΑΝΑΔΟΧΟΥ

Το προσωπικό του αναδόχου που θα απασχοληθεί στην παροχή των υπηρεσιών θα πρέπει, με ευθύνη του αναδόχου, να έχει εξειδίκευση και εμπειρία στην παροχή των υπηρεσιών αυτών. Ο ανάδοχος επίσης υποχρεούται να συμμορφώνεται πλήρως προς τους ισχύοντες νόμους, συλλογικές συμβάσεις εργασίας, κοινωνικές ασφαλίσεις κλπ.

ΑΡΘΡΟ 7°

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ο ανάδοχος υποχρεούται να τηρεί τις διατάξεις περί προστασίας προσωπικών δεδομένων και να παράσχει τις υπηρεσίες του σε πλήρη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) με αριθμ. 679/2016. Υποχρεούται επίσης να μην χρησιμοποιήσει δεδομένα του Δήμου, στα οποία πιθανόν να έχει πρόσβαση κατά την παροχή των υπηρεσιών του, για κανέναν άλλο λόγο πλην της παροχής των υπηρεσιών του.

ΑΡΘΡΟ 8°

ΕΠΙΛΥΣΗ ΔΙΑΦΟΡΩΝ

Οι διαφορές που πιθανόν να εμφανισθούν κατά την εφαρμογή της σύμβασης, επιλύονται σύμφωνα με τις ισχύουσες διατάξεις. Σε περίπτωση δικαστικής εμπλοκής αρμόδια είναι τα δικαστήρια της Αθήνας.

Ο Συντάξας

Γκιουζέλης Ιωάννης

προϊστάμενος Τμήματος

Προγραμματισμού, Οργάνωσης & Πληροφορικής

ΘΕΩΡΗΘΗΚΕ

Η προϊσταμένη

Δ/νσης Οικονομικών Υπηρεσιών

Πρίντζου Ελένη