ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΜΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΚΤΥΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Σχεδίαση και ανάλυση συστήματος για την διαχείριση ταυτότητας με χρήση κρυπτογραφικών βιβλιοθηκών που συνδυάζουν blockchain υποδομή για την προστασία της ιδιωτικότητας του χρήστη

Παγγές Ιωάννης

Επιβλέπων: Επίκουρος Καθηγητής

Λιάγκου Βασιλική

Άρτα, Ιούλιος 2023

Design and analysis of an Identity Management System that utilizes cryptographic libraries that use the blockchain technology for preserving user's privacy

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπουσα καθηγήτρια
   Λιάγκου Βασιλική,
   Επίκουρος Καθηγητής

2. Μέλος επιτροπής
   Στεργίου Ελευθέριος,
   Αναπληρωτής καθηγητής

3. Μέλος επιτροπής
   Στύλιος Χρυσόστομος,
   Καθηγητής

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα μεταπτυχιακή εργασία είναι εκ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Υπογραφή

Παγγές Ιωάννης

ΠΕΡΙΛΗΨΗ

Σήμερα όλες οι ηλεκτρονικές υπηρεσίες που αναπτύσσονται πρέπει να συμμορφώνονται με τους εθνικούς και ευρωπαϊκούς νόμους περί προστασίας δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ).

Στην παρούσα εργασία παρουσιάζεται μια διαδικτυακή πλατφόρμα για μεταπτυχιακές και διδακτορικές εφαρμογές που χρησιμοποιεί ένα εξαιρετικά αποτελεσματικό, κλιμακούμενο και φιλικό προς τον χρήστη σύστημα διαχείρισης ταυτότητας που παρέχει επίσημες εγγυήσεις ασφάλειας και προστασίας της ιδιωτικής ζωής σε όλα τα μέρη.

Η βασική τεχνολογία βασίζεται σε κατανεμημένες τεχνολογίες και σε διαπιστευτήρια με βάση τα χαρακτηριστικά (P-ABC) που διατηρούν την ιδιωτικότητα και αναπτύχθηκαν από τα έργα CyberSec4eu και OLYMPUS. Η άποψή μας είναι ότι τα συστήματα διαχείρισης ταυτοτήτων που μαγεύουν την ιδιωτικότητα προσφέρουν διάφορα οφέλη στις ηλεκτρονικές υπηρεσίες και η υλοποίηση διαφόρων σεναρίων χρήσης θα μειώσει την προσπάθεια ανάπτυξης.

Η προτεινόμενη αναπτυγμένη αρχιτεκτονική του συστήματος διαφυλάττει την ιδιωτικότητα και είναι αρκετά ευέλικτη για την ανάπτυξή του σε πολλούς τομείς εφαρμογών, όπως η ηλεκτρονική υγεία (π.χ. όπου ένας χρήστης μπορεί διαφορετικά μέρη μιας έκθεσης θεραπείας στην ασφαλιστική εταιρεία, τον εργοδότη ή τον οικογενειακό γιατρό του), η ηλεκτρονική διακυβέρνηση (π.χ. επιτυγχάνοντας έτσι την απλοποίηση του χαρτιού με την αντικατάσταση εγγράφων σε χαρτί από αντίστοιχα ηλεκτρονικά έγγραφα, χωρίς να χρειάζεται να εγκαταλείψει την ασφάλεια), ή άλλες, όπως, ενδεικτικά, οι έξυπνες πόλεις, το ηλεκτρονικό εμπόριο ή ο έλεγχος φυσικής πρόσβασης σε περιορισμένους χώρους.

Λέξεις-κλειδιά: συστήματα διαχείρισης ταυτότητας, IdM με διατήρηση της ιδιωτικότητας, διαπιστευτήρια με βάση τα χαρακτηριστικά ιδιωτικότητας, Academic Degree Verification System

ABSTRACT

Today, all electronic services being developed must comply with national and European data protection laws, such as the General Data Protection Regulation (GDPR). In this thesis, we present an online platform for postgraduate and doctoral applications that utilizes an extremely efficient, scalable, and user-friendly identity management system, which provides official guarantees of security and privacy protection in all aspects. The underlying technology is based on distributed technologies and privacy-preserving attribute-based credentials (P-ABC) developed by the CyberSec4eu and OLYMPUS projects. We believe that privacy-preserving identity management systems offer various benefits to electronic services, and implementing different use cases will reduce development efforts.

The proposed architecture of the Academic Degree Verification System, which preserves privacy, is highly flexible for its development in various application domains, such as e-health (e.g., where a user can share different parts of a treatment report with an insurance company, employer, or family doctor), e-governance (e.g., achieving paperless processes by replacing paper documents with electronic ones without compromising security), or others, including smart cities, e-commerce, or physical access control to restricted areas.

Keywords: identity management systems, privacy-preserving IdM, privacy-preserving attribute-based credentials, Academic Degree Verification System

Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΗ

Η επαλήθευση της γνησιότητας των εγγράφων και η προστασία της ιδιωτικότητας είναι δύο κρίσιμα ζητήματα στη σημερινή ψηφιακή εποχή. Από τη μία πλευρά, είναι απαραίτητο να διασφαλιστεί ότι τα έγγραφα είναι αυθεντικά και δεν έχουν πλαστογραφηθεί ή αλλοιωθεί με οποιονδήποτε τρόπο, ιδίως σε ευαίσθητους τομείς όπως η χρηματοδότηση ενός δανείου, η υγειονομική περίθαλψη και τα νομικά έγγραφα. Από την άλλη πλευρά, η προστασία της ιδιωτικότητας είναι εξίσου σημαντική, καθώς οι ευαίσθητες πληροφορίες που περιέχονται στα έγγραφα πρέπει να διατηρούνται ασφαλείς και εμπιστευτικές για την αποφυγή μη εξουσιοδοτημένης πρόσβασης και κακής χρήσης.

Η πρόκληση έγκειται στην εξεύρεση ισορροπίας μεταξύ αυτών των δύο στόχων. Μια λύση είναι η χρήση προηγμένων τεχνολογιών κρυπτογράφησης και ελέγχου ταυτότητας για να διασφαλιστεί ότι τα έγγραφα είναι ασφαλή και αυθεντικά, ενώ ταυτόχρονα προστατεύεται η ιδιωτικότητα μέσω της χρήσης ελέγχων πρόσβασης και άλλων μέτρων διατήρησης . Για παράδειγμα, οι ψηφιακές υπογραφές και η τεχνολογία blockchain μπορούν να χρησιμοποιηθούν για την επαλήθευση της γνησιότητας των εγγράφων, ενώ οι έλεγχοι πρόσβασης και η κρυπτογράφηση μπορούν να χρησιμοποιηθούν για την προστασία της ιδιωτικότητας των ευαίσθητων πληροφοριών.

Επιπλέον στην παρούσα εργασία παρουσιάζουμε ένα σύστημα για την επαλήθευση των ακαδημαϊκών προσόντων των χρηστών. Η εφαρμογή βασίζεται σε ένα σύστημα πολλαπλών υπογραφών, το οποίο καθιστά πολύ δύσκολο να παραποιηθεί ή να πλαστογραφηθεί ένα πιστοποιητικό. Έχουν δημιουργηθεί δύο πιλοτικά σενάρια, ένα για desktop και ένα για κινητές συσκευές.

Συμπερασματικά, η πιστοποίηση της γνησιότητας των εγγράφων και η προστασία της ιδιωτικότητας είναι δύο κρίσιμες προκλήσεις που πρέπει να αντιμετωπιστούν στη σημερινή ψηφιακή εποχή. Με τη χρήση προηγμένων τεχνολογιών και βέλτιστων πρακτικών, είναι δυνατόν να διασφαλιστεί ότι τα έγγραφα είναι αυθεντικά και ασφαλή, ενώ παράλληλα προστατεύεται η ιδιωτικότητα και αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση και κατάχρηση.

Κεφάλαιο 1ο

Ο σκοπός του πρώτου κεφαλαίου είναι να εξετάσει τα ζητήματα απορρήτου των σημερινών συστημάτων διαχείρισης ταυτότητας (IdM). Θα συζητηθούν οι διάφοροι μηχανισμοί ελέγχου ταυτότητας και ασφαλούς πρόσβασης που χρησιμοποιούνται από τα συστήματα IdM, καθώς και οι διάφοροι πάροχοι υπηρεσιών ταυτότητας (IdSPs) που είναι διαθέσιμοι. Θα εξεταστεί επίσης η σημασία της συνδεσιμότητας σε όλους τους τομείς (domain) και η αποκάλυψη ταυτότητας. Τέλος, θα συζητηθούν τα διάφορα τρέχοντα συστήματα IdM και οι προκλήσεις που αντιμετωπίζουν.

Το κεφάλαιο χωρίζεται σε πέντε κύρια τμήματα. Το πρώτο τμήμα παρέχει μια εισαγωγή στο θέμα της διαχείρισης ταυτότητας. Το δεύτερο τμήμα θα εξετάσει τους διάφορους μηχανισμούς ελέγχου ταυτότητας και ασφαλούς πρόσβασης που χρησιμοποιούνται από τα συστήματα IdM. Το τρίτο τμήμα θα συζητήσει τους διάφορους πάροχες υπηρεσιών ταυτότητας (IdSPs) που είναι διαθέσιμοι. Το τέταρτο τμήμα θα εξετάσει τη σημασία της συνδεσιμότητας σε όλους τους τομείς (domain) και την αποκάλυψη ταυτότητας. Το πέμπτο και τελευταίο τμήμα θα συζητήσει τα διάφορα τρέχοντα συστήματα IdM και τις προκλήσεις που αντιμετωπίζουν.

1. Ζητήματα απορρήτου των σημερινών συστημάτων Διαχείρισης Ταυτότητας

Η διαχείριση της ταυτότητας είναι ένα κρίσιμο επιστημονικό ζήτημα που αφορά τη διαχείριση των προσωπικών δεδομένων και την εξασφάλιση ασφαλούς πρόσβασης σε πόρους. Στη σημερινή ψηφιακή εποχή, η διαχείριση ταυτότητας έχει αποκτήσει ολοένα και μεγαλύτερη σημασία, καθώς όλο και περισσότερα προσωπικά δεδομένα συλλέγονται και αποθηκεύονται στο διαδίκτυο.

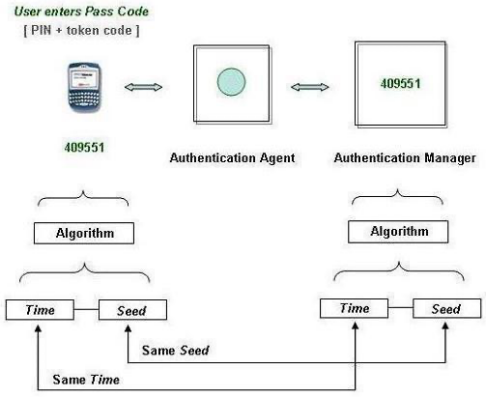
Επιπλέον, η διαχείριση της ταυτότητας είναι σημαντική για την ασφάλεια και την ιδιωτικότητα των ατόμων στην ψηφιακή εποχή. Η ψηφιακή ταυτότητα των ατόμων περιλαμβάνει προσωπικά δεδομένα όπως ονόματα, διευθύνσεις email, κωδικούς πρόσβασης και πληροφορίες πιστωτικών καρτών, και είναι εύθραυστη σε κλοπή από κακόβουλους χρήστες. Έτσι, η διαχείριση της ταυτότητας είναι απαραίτητη για την προστασία των ατόμων από διάφορες μορφές απάτης και κυβερνοεπιθέσεων.

Σε αυτό το κεφάλαιο, θα συζητήσουμε για τα κύρια συστατικά στοιχεία της διαχείρισης ταυτότητας, δηλαδή την ασφάλεια και τα προσωπικά δεδομένα, και θα διερευνήσουμε ορισμένες από τις τεχνολογίες και τις λύσεις που υπάρχουν σε αυτόν τον τομέα.

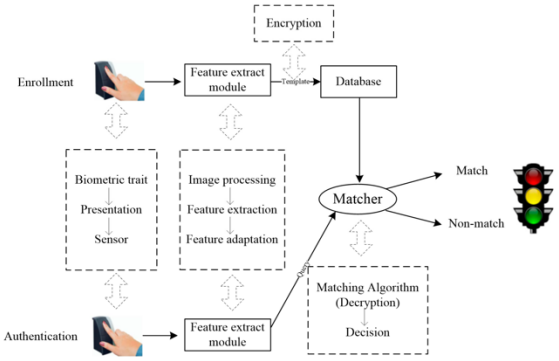
Η ασφάλεια είναι μία από τις σημαντικότερες πτυχές της διαχείρισης ταυτότητας. Περιλαμβάνει την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση, χρήση ή αποκάλυψη. Ακολουθούν ορισμένες από τις τεχνολογίες και τις λύσεις που υπάρχουν σε αυτόν τον τομέα.

1.1 Μηχανισμοί Ελέγχου Ταυτότητας και Ασφαλή Προσβαση

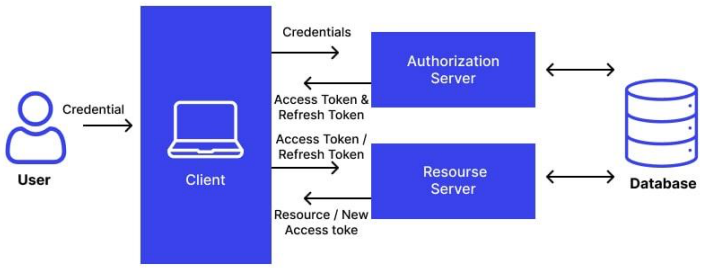
Οι μηχανισμοί ελέγχου ταυτότητας (authentication mechanisms) χρησιμοποιούνται για την επαλήθευση της ταυτότητας ενός ατόμου πριν του χορηγηθεί πρόσβαση σε έναν πόρο. Ορισμένοι από τους χρησιμοποιούμενους μηχανισμούς ελέγχου ταυτότητας περιλαμβάνουν κωδικούς πρόσβασης, έλεγχο ταυτότητας δύο παραγόντων, βιομετρικό έλεγχο ταυτότητας και έλεγχο ταυτότητας με βάση το διαπιστευτήριο (token)[1]



Σχήμα 1: Έλεγχος ταυτότητας δυο παραγόντων



Σχήμα 2: Βιομετρικός έλεγχος ταυτότητας]



Σχήμα 3: Έλεγχος ταυτότητας με βάση το διαπιστευτήριο

Ένα κρίσιμο στοιχείο της διαχείρισης της ταυτότητας είναι τα προσωπικά δεδομένα. Περιλαμβάνει τη συλλογή, αποθήκευση και χρήση προσωπικών δεδομένων, τα οποία μπορεί να περιλαμβάνουν ένα ευρύ φάσμα πληροφοριών, όπως όνομα, διεύθυνση, ημερομηνία γέννησης, αριθμό κοινωνικής ασφάλισης και άλλα.Παρακάτω θα περιγράψουμε ορισμένες από τις τεχνολογίες και τις λύσεις που υπάρχουν σε αυτόν τον τομέα.

Επίσης ο **έλεγχος πρόσβασης** χρησιμοποιείται για τον περιορισμό δηλαδή ποιος μπορεί να έχει πρόσβαση σε ευαίσθητα δεδομένα. Αυτό περιλαμβάνει τον καθορισμό δικαιωμάτων και περιορισμών για να διασφαλιστεί ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση σε συγκεκριμένα δεδομένα ή πόρους.
Οι **πολιτικές απορρήτου(Security Policies)** χρησιμοποιούνται για να ρυθμίζουν τον τρόπο χειρισμού και κοινοποίησης των προσωπικών δεδομένων. Αυτό περιλαμβάνει τον καθορισμό κατευθυντήριων γραμμών και βέλτιστων πρακτικών για το χειρισμό και την κοινή χρήση δεδομένων, καθώς και τον καθορισμό των συνεπειών για τη μη συμμόρφωση.

Τα συστήματα διαχείρισης ταυτότητας και πρόσβασης (Identity and Access Management)[2] έχουν σχεδιαστεί για τη διαχείριση και τον έλεγχο της πρόσβασης σε πληροφορίες και πόρους. Συνήθως περιλαμβάνουν χαρακτηριστικά όπως η πιστοποίηση ταυτότητας, η εξουσιοδότηση και ο έλεγχος.

Ακόμη **τα συστήματα ενιαίας σύνδεσης** (SSO) επιτρέπουν στους χρήστες να πιστοποιούνται μία φορά και στη συνέχεια να έχουν πρόσβαση σε πολλαπλούς πόρους χωρίς να χρειάζεται να εισάγουν εκ νέου τα διαπιστευτήριά τους.

Η ενιαία σύνδεση (SSO)[6] είναι ένα σύστημα που επιτρέπει στους χρήστες να έχουν πρόσβαση σε πολλαπλές ψηφιακές υπηρεσίες με ένα μόνο σύνολο διαπιστευτηρίων σύνδεσης. Με την ενιαία σύνδεση (SSO), οι χρήστες μπορούν να πιστοποιούνται μία φορά και στη συνέχεια να έχουν πρόσβαση σε πολλαπλές υπηρεσίες χωρίς να χρειάζεται να εισάγουν τα διαπιστευτήρια σύνδεσής τους κάθε φορά. Επιπλέον μπορεί να βελτιώσει την ευκολία των χρηστών, ενώ παράλληλα μειώνει τον κίνδυνο προβλημάτων ασφαλείας που σχετίζονται με τους κωδικούς πρόσβασης, όπως οι αδύναμοι κωδικοί πρόσβασης, η επαναχρησιμοποίηση κωδικών πρόσβασης και η κοινή χρήση κωδικών πρόσβασης. Η ενιαία σύνδεση (SSO)[7] υλοποιείται συχνά με τη χρήση πρωτοκόλλων όπως η Security Assertion Markup Language (SAML)[8] ή το OpenID Connect[8], τα οποία επιτρέπουν την ανταλλαγή δεδομένων ελέγχου ταυτότητας και εξουσιοδότησης μεταξύ διαφορετικών εφαρμογών και υπηρεσιών.

Επιπλέον ο **βιομετρικός έλεγχος ταυτότητας** (Biometric Authentication)[3] χρησιμοποιεί φυσικά χαρακτηριστικά όπως δακτυλικά αποτυπώματα, αναγνώριση προσώπου ή σάρωση ίριδας για την πιστοποίηση των χρηστών. Τα βιομετρικά συστήματα ελέγχου ταυτότητας συγκρίνουν φυσικά

χαρακτηριστικά με αποθηκευμένα, επιβεβαιωμένα, αυθεντικά δεδομένα σε μια βάση δεδομένων. Εάν και τα δύο δείγματα των βιομετρικών δεδομένων ταιριάζουν, η αυθεντικοποίηση επιβεβαιώνεται. Συνήθως, η βιομετρική πιστοποίηση χρησιμοποιείται για τη διαχείριση της πρόσβασης σε φυσικούς και ψηφιακούς πόρους, όπως κτίρια, δωμάτια και υπολογιστικές συσκευές.

Ένα σημαντικό στοιχείο της διαχείρισης ταυτότητας είναι η διαχείριση **κωδικού πρόσβασης (Password Management**)[2] , βοηθούν τους χρήστες να δημιουργούν και να διαχειρίζονται ασφαλείς κωδικούς πρόσβασης για τους διάφορους λογαριασμούς τους, μειώνοντας τον κίνδυνο παραβίασης της ασφάλειας που σχετίζεται με τους κωδικούς πρόσβασης.

Ο κωδικός πρόσβασης σύνδεσης είναι μία από τις συνηθέστερες μορφές πιστοποίησης που χρησιμοποιούνται στα συστήματα διαχείρισης ταυτότητας. Περιλαμβάνει την παροχή από τους χρήστες ενός μοναδικού ονόματος χρήστη ή διεύθυνσης ηλεκτρονικού ταχυδρομείου μαζί με έναν κωδικό πρόσβασης για να αποκτήσουν πρόσβαση σε ένα σύστημα ή μια εφαρμογή. Συνήθως ένας συνδυασμός χαρακτήρων, αριθμών και συμβόλων που μόνο ο χρήστης γνωρίζει[4] .

Παρόλο που οι κωδικοί πρόσβασης χρησιμοποιούνται ευρέως, ενέχουν επίσης σημαντικό κίνδυνο για την ασφάλεια. Οι κωδικοί πρόσβασης μπορούν εύκολα να μαντευτούν ή να κλαπούν και πολλοί χρήστες τείνουν να χρησιμοποιούν αδύναμους ή εύκολα μαντεύσιμους κωδικούς πρόσβασης, όπως «password» ή «123456». Αυτό μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα και πόρους, θέτοντας σε κίνδυνο την ασφάλεια του συστήματος διαχείρισης ταυτότητας.

Για τον μετριασμό αυτών των κινδύνων, τα συστήματα διαχείρισης ταυτότητας εφαρμόζουν συνήθως διάφορα μέτρα ασφαλείας για την προστασία των κωδικών πρόσβασης. Αυτά περιλαμβάνουν πολιτικές κωδικών πρόσβασης που επιβάλλουν ισχυρές απαιτήσεις κωδικών πρόσβασης, όπως ελάχιστο μήκος και πολυπλοκότητα, καθώς και απαιτήσεις τακτικής λήξης κωδικών πρόσβασης και ιστορικού κωδικών πρόσβασης. Ορισμένα συστήματα εφαρμόζουν επίσης **έλεγχο ταυτότητας δύο παραγόντων** (2FA) ή έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA), οι οποίοι απαιτούν από τους χρήστες να παρέχουν πρόσθετες μορφές ελέγχου ταυτότητας, όπως δακτυλικό αποτύπωμα ή κωδικό πρόσβασης μιας χρήσης, εκτός από τον κωδικό πρόσβασής τους.

Πέρα από το τυπικό όνομα χρήστη και τον κωδικό πρόσβασης, υπάρχουν και άλλες λύσεις που προσπαθούν να αυξήσουν την ιδιωτικότητα της ασφάλειας, όπως η υποδομή δημόσιου κλειδιού (PKI) , η ενιαία σύνδεση (SSO) και ενισχύουν την ιδιωτικότητα.

Η υποδομή δημόσιου κλειδιού (PKI) και η ενιαία σύνδεση (SSO) είναι δύο τεχνολογίες που χρησιμοποιούνται συνήθως για ασφαλή έλεγχο ταυτότητας και πρόσβασης σε ψηφιακά συστήματα.

Ακόμη η υποδομή δημόσιου κλειδιού (PKI) και η ενιαία σύνδεση (SSO) μπορούν να χρησιμοποιηθούν μαζί για να παρέχουν ένα ασφαλές και απρόσκοπτο σύστημα ελέγχου ταυτότητας και πρόσβασης. Για παράδειγμα, η υποδομή δημόσιου κλειδιού (PKI) μπορεί να χρησιμοποιηθεί για την έκδοση ψηφιακών πιστοποιητικών στους χρήστες, ενώ η ενιαία σύνδεση (SSO) μπορεί να χρησιμοποιηθεί για την παροχή μιας ενιαίας εμπειρίας σύνδεσης σε πολλαπλές εφαρμογές και υπηρεσίες. Αυτό μπορεί να ενισχύσει την ασφάλεια διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε ευαίσθητα δεδομένα ή πόρους, ενώ παράλληλα βελτιώνει την εμπειρία των χρηστών μειώνοντας την ανάγκη για πολλαπλά διαπιστευτήρια σύνδεσης..

Επίσης η υποδομή δημόσιου κλειδιού (PKI)[5] είναι ένα σύστημα που χρησιμοποιεί κρυπτογραφία δημόσιου κλειδιού για την ασφαλή ανταλλαγή πληροφοριών και την επαλήθευση της ταυτότητας ατόμων ή οντοτήτων σε ένα δικτυακό περιβάλλον. Βασίζεται στη χρήση ψηφιακών πιστοποιητικών, τα οποία εκδίδονται από μια αξιόπιστη Αρχή Πιστοποιητικών (ΑΠ) και περιέχουν πληροφορίες σχετικά με την ταυτότητα του κατόχου του πιστοποιητικού, καθώς και ένα δημόσιο κλειδί που μπορεί να χρησιμοποιηθεί για κρυπτογράφηση και ψηφιακές υπογραφές. Όταν ένας χρήστης θέλει να δημιουργήσει μια ασφαλή σύνδεση με ένα άλλο μέρος, μπορεί να παρουσιάσει το ψηφιακό του πιστοποιητικό για να αποδείξει την ταυτότητά του και να δημιουργήσει ένα ασφαλές κανάλι επικοινωνίας. Χρησιμοποιείται ευρέως σε μια ποικιλία εφαρμογών, όπως οι ηλεκτρονικές τραπεζικές συναλλαγές, το ηλεκτρονικό εμπόριο και το ασφαλές ηλεκτρονικό ταχυδρομείο.

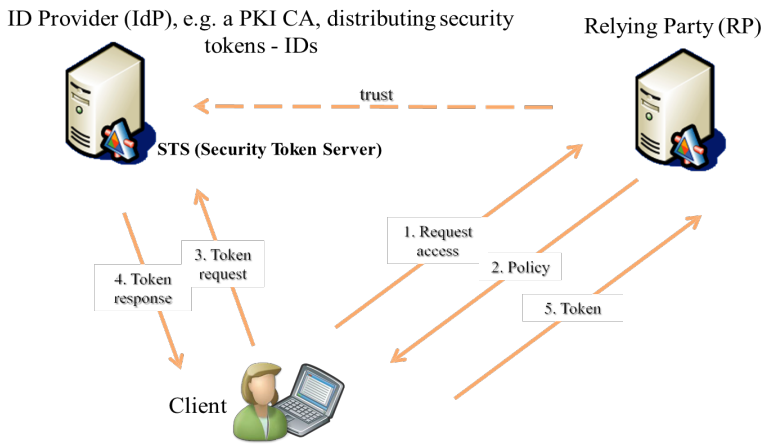
Εν κατακλείδι, η διαχείριση της ταυτότητας αποτελεί κρίσιμο επιστημονικό ζήτημα στην ψηφιακή εποχή. Περιλαμβάνει τη διαχείριση των προσωπικών δεδομένων και την εξασφάλιση ασφαλούς

πρόσβασης σε πόρους. Οι τεχνολογίες και οι λύσεις που συζητήθηκαν σε αυτό το κεφάλαιο μπορούν να βοηθήσουν τους χρήστες, οργανισμούς να διαχειρίζονται και να προστατεύουν καλύτερα τα προσωπικά δεδομένα και να αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση σε πόρους. Ωστόσο, είναι σημαντικό να αναγνωρίσουμε ότι η διαχείριση ταυτότητας είναι μια συνεχής διαδικασία που απαιτεί συνεχή προσοχή και ενημερώσεις για να συμβαδίζει με τις διαρκώς εξελισσόμενες απειλές στο ψηφιακό τοπίο.

Άλλη μια τεχνολογία είναι η **Διαχείριση Ομοσπονδιακής Ταυτότητας (Federated Identity Management)**[10] επιτρέπει στους χρήστες να έχουν πρόσβαση σε πόρους σε διαφορετικούς οργανισμούς ή συστήματα χρησιμοποιώντας ένα ενιαίο σύνολο διαπιστευτηρίων. Με την διαχείριση ομοσπονδιακής ταυτότητας, κάθε οργανισμός διατηρεί το δικό της σύστημα διαχείρισης ταυτότητας, ωστόσο συνδέονται μεταξύ τους μέσω μιας τρίτης υπηρεσίας ,του παρόχου ταυτότητας, που αποθηκεύει τα διαπιστευτήρια και χρησιμεύει ως μηχανισμός εμπιστοσύνης[11].

Μόλις δημιουργηθεί η εμπιστοσύνη, εκτελείται έτσι ώστε όταν οι χρήστες σε διαφορετικές επιχειρήσεις πιστοποιούνται στο σύστημα, και να τους δίνεται αυτόματα πρόσβαση σε όλους τους πόρους που συνδέονται με αυτό, χωρίς να χρειάζεται εκ νέου πιστοποίηση σε αυτούς τους πόρους. Οι χρήστες παρέχουν μόνο διαπιστευτήρια στην υπηρεσία και δεν παρέχουν διαπιστευτήρια στους πόρους που συνδέονται με την υπηρεσία.

Παρόλο που η **Διαχείριση Ομοσπονδιακής Ταυτότητας (FIdM)** δεν είναι μια νέα ιδέα, την τελευταία δεκαετία έχει ωριμάσει σε μια εφικτή επιλογή για τον έλεγχο ταυτότητας μεταξύ των τομέων (cross-domain). Επίσης η ιστορία δείχνει ότι η ευρεία αποδοχή ενός ενιαίου συστήματος Διαχείριση Ομοσπονδιακής Ταυτότητας (FIdM) είναι προβληματική και η επιτυχία έχει επιτευχθεί μόνο σε συγκεκριμένα πλαίσια[12], [13]. Αναγνωρίζοντας τα ελαττώματα των παλαιών συστημάτων, εμφανίστηκαν νέα συστήματα και μόνο ο χρόνος θα δείξει αν είναι επιτυχή ή όχι. Ένας λόγος για τον οποίο τα διάφορα συστήματα απέτυχαν είναι ότι προορίζονταν να χρησιμοποιηθούν σε πολλές εφαρμογές, πράγμα που σημαίνει ότι παρείχαν την αποκάλυψη ταυτότητας για αυθαίρετες υπηρεσίες στο Διαδίκτυο.



Σχήμα 4:Διαχείριση Ομοσπονδιακής Ταυτότητας (FIdM)

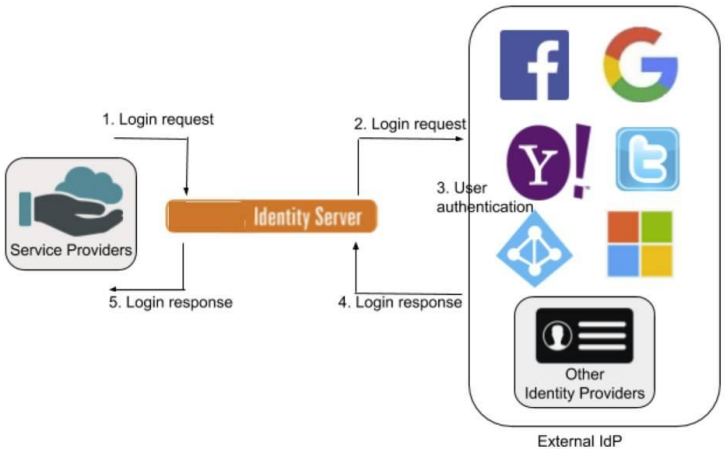
Επιπλέον πολλά από τα προβλήματα που σχετίζονται με τον έλεγχο ταυτότητας στο Διαδίκτυο δεν υπάρχουν όταν οι οργανισμοί-εταίροι συνεργάζονται μεταξύ τους. Η εμπιστοσύνη μεταξύ των οργανισμών είναι αυτονόητη, γιατί ο χρήστης εμπιστεύεται τον οργανισμό για να διαχειριστεί την ταυτότητα του. Στην προκειμένη περίπτωση καθίσταται σαφές στο χρήστη που πρέπει να πιστοποιηθεί και για ποιο λόγο που θα χρησιμοποιηθεί η ταυτότητα του.

Στο επόμενο κεφάλαιο θα συζητήσουμε για την Διαχείριση Ομοσπονδιακής Ταυτότητας (FIdM) που περιλαμβάνει παρόχους υπηρεσίων ταυτότητας (IdSPs), και τρίτα μέρη (Relying Parties).Ένας Πάροχος υπηρεσιών ταυτότητας (IdSP) διαχειρίζεται και επαληθεύει τις ταυτότητες άλλων οντοτήτων και το τρίτο μέρος (Relying Party) βασίζεται σε αναπαραστάσεις ταυτότητας που εκδίδονται από τους Παρόχους υπηρεσιών ταυτότητας (IdSPs).

1.2 Πάροχος υπηρεσιών ταυτότητας (IdSPs) και προκλήσεις

Ο πάροχος υπηρεσιών ταυτότητας (IdSP) είναι ένας τύπος παρόχου υπηρεσιών τρίτου μέρους που προσφέρει υπηρεσίες διαχείρισης ταυτότητας σε άτομα ή οργανισμούς. Οι πάροχοι υπηρεσιών ταυτότητας παρέχουν μια σειρά υπηρεσιών που μπορεί να περιλαμβάνουν επαλήθευση ταυτότητας, πιστοποίηση ταυτότητας και εξουσιοδότηση, καθώς και διαχείριση προφίλ χρήστη και έλεγχο πρόσβασης[14]

Ένα παράδειγμα είναι πιθανόν να έχουμε δει την επιλογή «Εγγραφείτε με το Facebook» κατά την εγγραφή σε μια υπηρεσία, οπότε το Facebook είναι ο πάροχος ταυτότητας. Με τη συγκατάθεση του χρήστη, το Facebook βεβαιώνει στον πάροχο υπηρεσιών ότι έχετε λογαριασμό Facebook και παρέχει τα χαρακτηριστικά που εγκρίνετε στην υπηρεσία για μια εγγραφή, ώστε να μην χρειάζεται να δημιουργήσετε άλλη ταυτότητα για τη νέα υπηρεσία.



Σχήμα 5:Πάροχος υπηρεσιών ταυτότητας (IdSP)

Ένα από τα κύρια πλεονεκτήματα της χρήσης ενός παρόχου υπηρεσιών ταυτότητας(IdSP)[15] είναι ότι μπορεί να απλοποιήσει τη διαδικασία διαχείρισης ταυτοτήτων σε πολλαπλά συστήματα ή πλατφόρμες. Αντί να χρειάζεται να διαχειριζόμαστε τα διαπιστευτήρια των χρηστών και τους ελέγχους πρόσβασης ξεχωριστά για κάθε σύστημα ή πλατφόρμα, ένας πάροχος υπηρεσιών ταυτότητας (IdSP) μπορεί να παρέχει μια λύση διαχείρισης ταυτότητας που μπορεί να χρησιμοποιηθεί σε πολλαπλά συστήματα.

Ένα άλλο πλεονέκτημα της χρήσης ενός παρόχου υπηρεσιών ταυτότητας(IdSP) είναι ότι μπορεί να συμβάλλει στη βελτίωση της ασφάλειας της διαχείρισης ταυτότητας. Οι πάροχοι υπηρεσιών

ταυτότητας(IdSPs) διαθέτουν συνήθως εξειδικευμένη τεχνογνωσία και πόρους που μπορούν να χρησιμοποιηθούν για την εφαρμογή ισχυρών μέτρων ασφαλείας, όπως ο έλεγχος ταυτότητας πολλαπλών παραγόντων, η κρυπτογράφηση και τα συστήματα ανίχνευσης και πρόληψης εισβολών. Αυτό μπορεί να συμβάλλει στη μείωση του κινδύνου παραβίασης της ασφάλειας που σχετίζεται με την ταυτότητα και στην προστασία των ευαίσθητων δεδομένων από μη εξουσιοδοτημένη πρόσβαση.

Μπορούν να χρησιμοποιηθούν από ένα ευρύ φάσμα οργανισμών, συμπεριλαμβανομένων κυβερνητικών υπηρεσιών, παρόχων υγειονομικής περίθαλψης, χρηματοπιστωτικών ιδρυμάτων και επιχειρήσεων ηλεκτρονικού εμπορίου. Ορισμένα παραδείγματα δημοφιλών παροχών υπηρεσιών ταυτότητας(IdSPs) περιλαμβάνουν τις Okta[16], Auth0[17] και Ping Identity[18].

Από την άλλη πλευρά έχουμε και ορισμένα προβλήματα που σχετίζονται με τη Διαχείριση Ομοσπονδιακής Ταυτότητας (FIdM)[19] , είναι ότι ένας πάροχο υπηρεσιών ταυτότητας (IdSP)μπορεί να γίνει μοναδικό σημείο αποτυχίας. Εάν ο πάροχος υπηρεσιών ταυτότητας (IdSP) δεν είναι διαθέσιμος, οι χρήστες ενδέχεται να μην μπορούν να έχουν πρόσβαση σε καμία υπηρεσία και, επιπλέον, δεν είναι δυνατή η πρόσβαση σε τρίτα μέρη (RP) που βασίζονται στον IdSP. Η παροχή εφεδρικών IdSP μπορεί να μειώσει το πρόβλημα.

Ένα άλλο πρόβλημα είναι ότι τα διαπιστευτήρια ενός χρήστη χρησιμοποιούνται για την πρόσβαση σε όλες τις υπηρεσίες και αν χαθούν, χάνεται και η πρόσβαση. Για παράδειγμα ο επιτιθέμενος με τα διαπιστευτήρια που έχει υποκλέψει, θα αποκτήσει πρόσβαση σε όλες τις υπηρεσίες. Επομένως, η προστασία των διαπιστευτηρίων είναι ακόμη πιο σημαντική. Ο έλεγχος ταυτότητας μπορεί να βοηθήσει στην προστασία των διαπιστευτηρίων των χρηστών, καθώς τους επιτρέπει να αναγνωρίζουν τους σωστούς παρόχους υπηρεσιών ταυτότητας (IdSPs) και να μην εξαπατώνται ώστε να παρέχουν τα διαπιστευτήριά τους σε έναν ψεύτικο[20].

Η διαλειτουργικότητα μπορεί να αποτελέσει πρόβλημα εάν οι οργανισμοί χρησιμοποιούν χαρακτηριστικά για την δημιουργία ενός παρόχου ταυτότητας (IdSPs)[20] ή χρησιμοποιούν διαφορετικές αρχιτεκτονικές[21].

Κατά την ανάπτυξη όμως ενός συστήματος Διαχείρισης Ομοσπονδιακής Ταυτότητας (FIdM) , είναι σημαντικό να διασφαλιστεί ότι δεν εμποδίζει τη χρηστικότητα και την παραγωγικότητα των χρηστών. Οι χρήστες θα πρέπει να είναι σε θέση να εκτελούν απρόσκοπτα και με ασφάλεια στις

υπηρεσίες τους χωρίς πρόσθετα εμπόδια που εισάγει το σύστημα. Για να επιτευχθεί αυτό, είναι σημαντικό να σχεδιαστεί το σύστημα Διαχείρισης Ομοσπονδιακής Ταυτότητας (FIdM) με γνώμονα τον χρήστη. Αυτό σημαίνει ότι το σύστημα θα πρέπει να είναι διαισθητικό και εύχρηστο, με σαφείς οδηγίες και καθοδήγηση που θα παρέχονται στους χρήστες.

Επιπλέον, το σύστημα Διαχείρισης Ομοσπονδιακής Ταυτότητας (FIdM)[20] θα πρέπει να ενσωματώνεται απρόσκοπτα με τις εφαρμογές και τις υπηρεσίες στις οποίες οι χρήστες χρειάζονται πρόσβαση, έτσι ώστε οι χρήστες να μην χρειάζεται να περνούν από επιπλέον βήματα ή συνδέσεις για να έχουν πρόσβαση στους πόρους τους.

Μια άλλη σημαντική σκέψη είναι να διασφαλιστεί ότι το σύστημα Διαχείρισης Ομοσπονδιακής Ταυτότητας, διατηρεί το απόρρητο και την ασφάλεια των δεδομένων των χρηστών. Οι χρήστες θα πρέπει να έχουν εμπιστοσύνη ότι οι προσωπικές τους πληροφορίες και τα διαπιστευτήριά τους προστατεύονται και ότι έχουν τον έλεγχο του ποιος έχει πρόσβαση στα δεδομένα τους. Δίνοντας προτεραιότητα στη χρηστικότητα, την απρόσκοπτη ενσωμάτωση και την ασφάλεια, ένα σύστημα Διαχείρισης Ομοσπονδιακής Ταυτότητας (FIdM) μπορεί να διευκολύνει επιτυχώς τα καθήκοντα των χρηστών χωρίς να εισάγει περιττά εμπόδια ή να θέτει σε κίνδυνο την ιδιωτικότητα και την ασφάλεια.

Συνολικά, οι πάροχοι υπηρεσιών ταυτότητας(IdSPs) μπορούν να αποτελέσουν ένα πολύτιμο εργαλείο για τους οργανισμούς που επιθυμούν να απλοποιήσουν και να διασφαλίσουν τις διαδικασίες διαχείρισης ταυτότητας. Ωστόσο, είναι σημαντικό για τους οργανισμούς να σταθμίζουν προσεκτικά τα πιθανά οφέλη και τους κινδύνους πριν επιλέξουν έναν πάροχο υπηρεσιών ταυτότητας(IdSPs) και να διασφαλίζουν ότι συνεργάζονται με έναν αξιόπιστο πάροχο με ισχυρό ιστορικό ασφάλειας και συμμόρφωσης.

1.3 Τρέχοντα συστήματα διαχείρισης ταυτότητας (IdM)

Τα τρέχοντα συστήματα διαχείρισης ταυτότητας(IdM) εξακολουθούν να μην πληρούν πραγματικά τις απαιτήσεις ασφαλείας και διαχείρισης απορρήτου, όπως είναι η αποσύνδεση των χρηστών μεταξύ παρόχων υπηρεσιών (SP), η απόκρυψη του παρόχου υπηρεσιών (SP) από τους παρόχους ταυτότητας (IdP) και η επιλεκτική αποκάλυψη προσωπικών δεδομένων.

Από την άποψη αυτή, οι παραδοσιακές προσεγγίσεις Single Sign On (SSO)[3] για συστήματα διαχείρισης ταυτότητας (IdM) που βασίζονται σε εκτεταμένες τεχνολογίες όπως το OAuth[8]ή το

SAML[21], έχουν εισάγει σημαντικά ζητήματα σχετικά με τη διαχείριση των προσωπικών πληροφοριών με αξιόπιστο τρόπο και εξακολουθούν να μην έχουν επιλυθεί. Οι υπηρεσίες ιστού συνήθως επαληθεύουν διευθύνσεις ηλεκτρονικού ταχυδρομείου ή αριθμούς τηλεφώνου χρησιμοποιώντας κωδικούς μιας χρήσης, στην καλύτερη περίπτωση.

Τα συστήματα διαχείρισης ταυτότητας (IdM) αντιμετωπίζουν μια σειρά από προκλήσεις σήμερα. Μερικές από τις πιο σημαντικές προκλήσεις περιλαμβάνουν:

- **Αύξηση της πολυπλοκότητας:** Τα σύγχρονα περιβάλλοντα IT είναι πολύ πιο περίπλοκα από ό,τι στο παρελθόν, γεγονός που καθιστά δύσκολο τον έλεγχο της πρόσβασης σε συστήματα και δεδομένα.
- **Αυξημένος κίνδυνος:** Οι χάκερ γίνονται όλο και πιο έξυπνοι και εξελιγμένοι, γεγονός που καθιστά τα συστήματα IdM ευάλωτα σε επιθέσεις.
- **Απαιτήσεις συμμόρφωσης:** Οι επιχειρήσεις υπόκεινται σε μια σειρά από απαιτήσεις συμμόρφωσης, οι οποίες μπορεί να είναι δύσκολο να εκπληρωθούν χωρίς ένα ισχυρό σύστημα IdM.
- **Κόστος:** Τα συστήματα IdM μπορούν να είναι ακριβά, γεγονός που μπορεί να αποτελέσει εμπόδιο για μικρές και μεσαίες επιχειρήσεις.

Πέρα από αυτές τις προκλήσεις, τα συστήματα διαχείρισης ταυτότητας είναι ζωτικής σημασίας για την ασφάλεια και την προστασία των συστημάτων και των δεδομένων των επιχειρήσεων. Επιπλέον μπορούν να βοηθήσουν στην αποτροπή μη εξουσιοδοτημένων χρηστών από την πρόσβαση σε συστήματα και δεδομένα, και μπορούν επίσης να βοηθήσουν στην αντιμετώπιση επιθέσεων. Τέλος, τα συστήματα IdM μπορούν να βοηθήσουν τις επιχειρήσεις να συμμορφωθούν με τις απαιτήσεις συμμόρφωσης.

1.3.1 Συνδεσιμότητα σε όλους τους τομείς (domain)

Στα σημερινά συστήματα διαχείρισης ταυτότητας, κάθε αξιόπιστος πάροχος μπορεί να αποθηκεύσει όλα τα διαπιστευτήρια που παρουσιάζονται και μπορεί να τα συνδέσει μεταξύ τους. Η συνδεσιμότητα σε διάφορους τομείς αναφέρεται στην ικανότητα διαφορετικών διαδικτυακών υπηρεσιών ή ιστότοπων να συνδέουν τη δραστηριότητα του χρήστη σε πολλαπλούς τομείς ή πλατφόρμες. Αυτό μπορεί να συμβεί όταν οι χρήστες παρέχουν αναγνωρίσιμες πληροφορίες όπως το όνομα, τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή τον αριθμό τηλεφώνου τους σε

διαφορετικές υπηρεσίες ή όταν χρησιμοποιούνται τεχνολογίες παρακολούθησης όπως cookies, διευθύνσεις IP για τη σύνδεση της δραστηριότητας του χρήστη σε διαφορετικούς τομείς[22].

Το απλούστερο παράδειγμα είναι τα πιστοποιητικά X.509[23], όπου τα στοιχεία του πιστοποιητικού, και η υπογραφή του εκδότη λειτουργούν ως ένα είδος ψηφιακού αποτυπώματος, αφήνοντας αναπόφευκτα ένα ψηφιακό ίχνος όπου το άτομο παρουσιάζει το πιστοποιητικό. Με αυτόν τον τρόπο, οι πληροφορίες του χρήστη μπορούν να αποθηκεύονται αυτόματα όπου αφορούν σχετικά με τις συνήθειες, τη συμπεριφορά, τις προτιμήσεις, τα χαρακτηριστικά του.

Η δυνατότητα σύνδεσης μεταξύ τομέων μπορεί να εγείρει σημαντικές ανησυχίες για την προστασία της ιδιωτικότητας των χρηστών, καθώς μπορεί να επιτρέψει τη δημιουργία λεπτομερών προφίλ της διαδικτυακής δραστηριότητας, των προτιμήσεων και της συμπεριφοράς των ατόμων. Αυτά τα προφίλ μπορούν να χρησιμοποιηθούν για στοχευμένη διαφήμιση, κατάρτιση προφίλ ή ακόμη και διακρίσεις. Επιπλέον, η διασύνδεση της δραστηριότητας των χρηστών σε διάφορους τομείς μπορεί να δημιουργήσει πιθανούς κινδύνους για την ασφάλεια, καθώς μπορεί να επιτρέψει σε κακόβουλους φορείς να συλλέγουν και να χρησιμοποιούν ευαίσθητα δεδομένα χρηστών για κακόβουλους σκοπούς.

Άλλες προσεγγίσεις για τη μείωση της δυνατότητας σύνδεσης σε διάφορους τομείς περιλαμβάνουν τη χρήση επεκτάσεων ή εργαλείων του προγράμματος περιήγησης που εμποδίζουν τα cookies παρακολούθησης ή εμποδίζουν τους ιστότοπους να συλλέγουν δεδομένα χρήστη, καθώς και τη χρήση εικονικών ιδιωτικών δικτύων (VPN) ή διακομιστών μεσολάβησης για τη συγκάλυψη της διεύθυνσης IP και της τοποθεσίας ενός χρήστη. Επιπλέον, ορισμένες διαδικτυακές υπηρεσίες ενδέχεται να προσφέρουν ρυθμίσεις απορρήτου ή ελέγχους που επιτρέπουν στους χρήστες να περιορίσουν την ποσότητα των δεδομένων που συλλέγονται και κοινοποιούνται σε άλλες υπηρεσίες.

Από την άλλη πλευρά όμως τα προβλήματα που σχετίζονται με την προστασία της ιδιωτικότητας, την κοινή χρήση τομέων, της ενιαίας σύνδεσης (SSO) και τους παρόχους υπηρεσιών ταυτότητας(IdSPs) αποτελούν κρίσιμες ανησυχίες στο σύγχρονο τεχνολογικό τοπίο.

Η ανησυχία για την προστασία της ιδιωτικότητας προκύπτει λόγω του κινδύνου διαρροής προσωπικών δεδομένων ή πρόσβασης σε αυτά χωρίς τη συγκατάθεση του χρήστη. Αυτό μπορεί να συμβεί όταν τα δεδομένα συλλέγονται ή κοινοποιούνται χωρίς τις κατάλληλες διασφαλίσεις,

όπως η κρυπτογράφηση ή ο έλεγχος πρόσβασης. Επιπλέον, τα δεδομένα προσωπικού χαρακτήρα μπορεί να συλλέγονται για συγκεκριμένο σκοπό αλλά στη συνέχεια να χρησιμοποιούνται για άλλον, χωρίς τη γνώση ή τη συγκατάθεση του ατόμου.[24]

Άλλο ένα πρόβλημα της ιδιωτικότητας που προκύπτει είναι το πρόβλημα της κοινής χρήσης του τομέα(domain) εμφανίζεται όταν πολλοί ιστότοποι ή εφαρμογές μοιράζονται έναν ενιαίο τομέα ή υποτομέα. Αυτό μπορεί να οδηγήσει σε προβλήματα με επιθέσεις cross-site scripting (XSS). Επιπλέον, εάν ένας ιστότοπος στον κοινόχρηστο τομέα παραβιαστεί, μπορεί ενδεχομένως να επηρεάσει την ασφάλεια όλων των άλλων ιστότοπων στον εν λόγω τομέα[25].

Επίσης η ενιαία σύνδεση (SSO) είναι ένας βολικός τρόπος για τους χρήστες να συνδέονται σε πολλές εφαρμογές ή υπηρεσίες με ένα μόνο σύνολο διαπιστευτηρίων. Ωστόσο, η ενιαία σύνδεση (SSO) μπορεί επίσης να παρουσιάζει κινδύνους για την ασφάλεια, καθώς η παραβίαση ενός συστήματος μπορεί δυνητικά να παρέχει σε έναν επιτιθέμενο πρόσβαση σε όλα τα προσωπικά δεδομένα. Αν το σύστημα της ενιαίας σύνδεσης (SSO) δεν έχει ρυθμιστεί ή συντηρηθεί σωστά, μπορεί να είναι ευάλωτο σε επιθέσεις [26].

Οι πάροχοι υπηρεσιών ταυτότητας (IdP) είναι εταιρίες ή οργανισμοί που παρέχουν υπηρεσίες ελέγχου ταυτότητας και εξουσιοδότησης για άλλα συστήματα ή εφαρμογές. Το κυριότερο πρόβλημα που προκύπτει με τους παρόχους ταυτότητας (IdPs) είναι ότι γίνονται κεντρικό σημείο αποτυχίας ή εκτίθενται σε επίθεση, καθώς μια παραβίαση του παρόχου ταυτότητας(IdP) μπορεί δυνητικά να χορηγήσει σε έναν επιτιθέμενο πρόσβαση σε όλα τα συστήματα ή τις εφαρμογές που βασίζονται σε αυτόν.Επίστης οι πάροχοι ταυτότητας ενδέχεται να μην προστατεύουν σωστά τα προσωπικά δεδομένα των χρηστών τους, οδηγώντας ενδεχομένως σε παραβίαση της ιδιωτικότητας[27].

Συνολικά, τα προβλήματα αυτά είναι πολύπλοκα και απαιτούν προσεκτική εξέταση και προσπάθειες μετριασμού για να διασφαλιστεί η ασφάλεια και η προστασία των ευαίσθητων πληροφοριών. Από την άλλη πλευρά η δυνατότητα σύνδεσης μεταξύ τομέων μπορεί να δημιουργήσει σημαντικούς κινδύνους για την ιδιωτικότητα και την ασφάλεια των χρηστών, αλλά υπάρχουν διάφορες τεχνικές και τεχνολογίες που μπορούν να χρησιμοποιηθούν για τη μείωση αυτών των κινδύνων και την προστασία της ιδιωτικότητας των χρηστών. Είναι σημαντικό τα

άτομα και οι οργανισμοί να γνωρίζουν αυτούς τους κινδύνους και να λαμβάνουν μέτρα για την προστασία της ιδιωτικότητας και της ασφάλειάς τους στο διαδίκτυο.

1.3.2 Αποκάλυψη ταυτότητας

Υπάρχουν πολλά σενάρια όπου η χρήση πιστοποιητικών αποκαλύπτει χωρίς λόγο την ταυτότητα των κατόχου της, για παράδειγμα σενάρια όπου μια πλατφόρμα υπηρεσιών χρειάζεται μόνο να επαληθεύσει την ηλικία ενός χρήστη, αλλά όχι την πραγματική του ταυτότητα.

Ένα τυπικό παράδειγμα είναι τα πιστοποιητικά PKI πολιτών, όπου κάθε πολίτης εφοδιάζεται με ένα πιστοποιητικό X.509 [23] ως το ψηφιακό αναγνωριστικό για την ασφαλή πρόσβαση στις διαδικτυακές υπηρεσίες που προσφέρουν οι κυβερνήσεις. Αυτά τα πιστοποιητικά περιέχουν ένα σύνολο χαρακτηριστικών, όπως το ονοματεπώνυμο, την ημερομηνία γέννησης, το φύλο και ο αριθμός ταυτότητας, και αναπόφευκτα όλα θα αποκαλύπτονται στην τρίτη οντότητα κάθε φορά που παρουσιάζεται το πιστοποιητικό. Η αποκάλυψη περισσότερων πληροφοριών από ό,τι είναι απαραίτητο όχι μόνο βλάπτει την ιδιωτικότητα των χρηστών, αλλά αυξάνει και τον κίνδυνο κατάχρησης των πληροφοριών, όπως η κλοπή ταυτότητας, όταν οι πληροφορίες που αποκαλύπτονται πέφτουν σε λάθος χέρια.

1.3.3 Προστασία Ιδιωτικότητας χρήστη

Παρά τις προσπάθειες για την ανάπτυξη συστημάτων διαχείρισης ταυτότητας όπως είναι τα συστήματα χρηστών και η αποθήκευση των κωδικών πρόσβασης είναι ο πιο διαδεδομένος και αποδεκτός τρόπος πιστοποίησης των χρηστών. Από την άποψη αυτή, οι χρήστες δημιουργούν λογαριασμούς σε υπηρεσίες, γεγονός που τους δυσκολεύει να θυμούνται όλα τα διαπιστευτήρια που διαθέτουν. Στο σημείο αυτό οι χρήστες έχουν δύο επιλογές: να χρησιμοποιούν διαχειριστές κωδικών πρόσβασης ή να επαναχρησιμοποιούν τους ίδιους κωδικούς πρόσβασης σε διαφορετικές υπηρεσίες. Στην καλύτερη περίπτωση, οι διαχειριστές κωδικών πρόσβασης χρησιμοποιούνται για την αποθήκευση όλων των δεδομένων σύνδεσής τους σε ένα ενιαίο, ασφαλές δοχείο. Σε περίπτωση που κάποιος καταφέρει να κλέψει ή να αποκτήσει πρόσβαση σε αυτό το δοχείο, ο χρήστης είναι πλήρως εκτεθειμένος. Παρ' όλα αυτά, η πιο διαδεδομένη επιλογή εξακολουθεί να είναι η χρήση του ίδιου κωδικού πρόσβασης χαμηλής ποιότητας (ή μικρού συνόλου κωδικών πρόσβασης), σε πολλές υπηρεσίες, θέτοντας σε κίνδυνο την ηλεκτρονική τους ασφάλεια.

Μέχρι στιγμής, τα καλύτερα διαθέσιμα εν μέρει επιτυχημένα συστήματα είναι λύσεις με απευθείας σύνδεση, όπου οι χρήστες επαναχρησιμοποιούν τους λογαριασμούς τους σε ιστότοπους τρίτων για να συνδεθούν σε μια υπηρεσία. Αυτό είναι βολικό για τους χρήστες, οι οποίοι δεν

χρειάζεται να δημιουργήσουν ξεχωριστούς λογαριασμούς με ξεχωριστούς κωδικούς πρόσβασης και τους παρουσιάζεται μια διεπαφή για την είσοδο σε υπηρεσίες. Ωστόσο, είναι επιζήμιο για την ασφάλεια και την ιδιωτικότητα.

Στην παρούσα εργασία παρουσιάζονται τα ζητήματα προστασίας των προσωπικών δεδομένων των χρηστών στα σημερινά συστήματα διαχείρισης ταυτότητας που οι παροδιακές λύσεις που προαναφέρθηκαν δεν μπορούν να δώσουν λύσεις που εγγυώνται την προστασία της ιδιωτικότητας του χρήστη.

Οι παραδοσιακές λύσεις των συστημάτων διαχείρισης ταυτότητας εισάγουν ένα μόνο σημείο αποτυχίας στο σύστημα, καθώς ο κεντρικός πάροχος ταυτότητας (IdP) εμπλέκεται σε κάθε έλεγχο ταυτότητας σε έναν πάροχο υπηρεσιών. Ο κεντρικός πάροχος ταυτότητας (IdP)είναι σε θέση να πλαστοπροσωπεί τους χρήστες του, εάν ενεργεί με κακόβουλο τρόπο. Μπορεί να λειτουργεί ως «μεγάλος αδερφός» που μπορεί να παρακολουθεί τη συμπεριφορά περιήγησης των χρηστών του και να συνδέει τους λογαριασμούς τους σε διάφορες υπηρεσίες.

Επίσης οι παραδοσιακές υπηρεσίες διαχείρισης ταυτότητας (IdM) βασίζονται στη χρήση κεντρικών παρόχων ταυτότητας (IdP) οι οποίοι, διατηρούν και διαχειρίζονται πληροφορίες σχετικά με την ταυτότητα των χρηστών τους, ενώ παρέχουν υπηρεσίες ελέγχου σε τρίτα μέρη (RP). Οι εν λόγω πάροχοι ταυτότητας (IdPs) επιτρέπουν τη χρήση τεχνολογιών Single Sign-On (SSO), και επιτρέπουν στους χρήστες να εκτελούν τη διαδικασία ελέγχου ταυτότητας μόνο μία φορά. Ωστόσο, σε αυτά τα σενάρια εμφανίζονται ζητήματα συνδεσιμότητας, οι προσωπικές πληροφορίες αποθηκεύονται από διαφορετικούς παρόχους καθιστώντας τους χρήστες ανιχνεύσιμους, για παράδειγμα, συνδέοντας ονόματα χρηστών και μηνύματα ηλεκτρονικού ταχυδρομείου μεταξύ υπηρεσιών ή συγκρίνοντας χαρακτηριστικά που είναι αρκετά συγκεκριμένα.

Το πρωτόκολλο X.509 για παράδειγμα[21], που σε υποδομές δημόσιου κλειδιού (PKI), χρειάζεται μόνο ένα ελάχιστο όριο εμπιστοσύνης για την ανάπτυξή του. Ο χρήστης εμπιστεύεται την αρχή πιστοποίησης (CA), που είναι προσβάσιμη κατά τη στιγμή της έκδοσης, η οποία θα εκδώσει ένα ψηφιακό πιστοποιητικό για ένα σύνολο χαρακτηριστικών του χρήστη. Όταν ένας χρήστης επιθυμεί να πιστοποιηθεί σε μια υπηρεσία μέσω αυτού του συστήματος, η υπηρεσία πρέπει να

βασίζεται στην αρχή πιστοποίησης (CA) ως έγκυρο εκδότη και μόνο ο χρήστης και η υπηρεσία θα συμμετέχουν στη διαδικασία πιστοποίησης.

Τέλος αν και πρόκειται για ένα εύκολο στην υλοποίηση σύστημα, η προσέγγιση αυτή έχει σημαντικές προκλήσεις. Πρώτον, οι πάροχοι υπηρεσιών πρέπει να συμφωνήσουν να χρησιμοποιήσουν αυτό το σύστημα και πρέπει να βασίζονται σε μία ή περισσότερες αρχές πιστοποίησης (CA) ως αξιόπιστες οντότητες. Δεύτερον, οι χρήστες γίνονται ενεργό μέρος της ασφάλειας, καθώς είναι υπεύθυνοι για τη διατήρηση της μνήμης και της ασφάλειας των κωδικών τους (ιδανικά δεν θα πρέπει να υπάρχει αλληλεπίδραση με τον χρήστη, καθώς η εξαγωγή ενός ζεύγους κλειδιών με βάση έναν κωδικό πρόσβασης θα επιτρέψει επιθέσεις εκτός σύνδεσης, δεδομένου μόνο του δημόσιου πιστοποιητικού). Είναι γεγονός ότι οι χρήστες δεν είναι καλοί σε αυτές τις εργασίες και οι περισσότεροι χρήστες χρησιμοποιούν περισσότερες από μία συσκευές, γεγονός που συνεπάγεται ότι τα ιδιωτικά κλειδιά αντιγράφονται σε διάφορες συσκευές. Η αναγκαιότητα για τις τεχνολογίες ενίσχυσης της ιδιωτηκότητας(PET) προκύπτει από το γεγονός ότι η ευρεία χρήση της τεχνολογίας έχει καταστήσει ευκολότερη από ποτέ τη συλλογή, αποθήκευση, ανάλυση και κοινή χρήση προσωπικών δεδομένων. Τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς, συμπεριλαμβανομένης της στοχευμένης διαφήμισης, της επιτήρησης, ακόμη και της κλοπής ταυτότητας. Επιπλέον παρέχουν στα άτομα τα μέσα για να ελέγχουν τον τρόπο με τον οποίο συλλέγονται, χρησιμοποιούνται και κοινοποιούνται τα προσωπικά τους δεδομένα, ενισχύοντας έτσι την ιδιωτικότητα και την ασφάλειά τους.

Κεφάλαιο 2ο

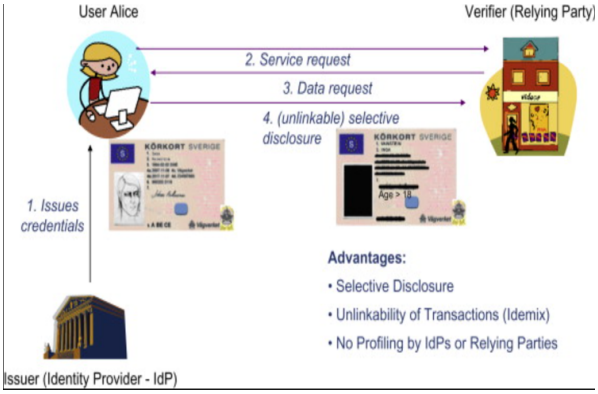
Ο σκοπός του δεύτερου κεφαλαίου είναι να εξετάσει τις τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs), και συγκεκριμένα τα διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου (P-ABC). Τα διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου είναι ένα είδος διαπιστευτηρίου που επιτρέπει στους χρήστες να παρέχουν μόνο τις απαραίτητες πληροφορίες ταυτότητας σε μια υπηρεσία. Αυτό μπορεί να βοηθήσει στη βελτίωση της ιδιωτικότητας των χρηστών, καθώς αποκαλύπτουν περισσότερα δεδομένα από τι χρειάζονται που είναι διαθέσιμα σε τρίτα μέρη.

Το πρώτο κεφάλαιο παρέχει μια εισαγωγή στο θέμα της ιδιωτικότητας. Το δεύτερο τμήμα εξετάζει τις διάφορες τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs), συμπεριλαμβανομένων των P-ABCs. Στο τρίτο τμήμα παρουσιάζονται τα πλεονεκτήματα των P-ABCs. Το τέταρτο τμήμα εξετάζει τις βασικές έννοιες των P-ABCs. Το πέμπτο και τελευταίο τμήμα παρουσιάζει τις προκλήσεις των διαπιστευτηρίων βάσει χαρακτηριστικών απορρήτου.

2.0 Οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (PET)

Το παρών κεφάλαιο αναφέρεται στην παρουσίαση τεχνολογιών για την προστασία της ιδιωτικότητας. Περιλαμβάνει βασικές έννοιες που αφορούν τα διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου.

Οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (PET) είναι τεχνολογίες που ενσωματώνουν θεμελιώδεις αρχές προστασίας δεδομένων ελαχιστοποιώντας τη χρήση προσωπικών δεδομένων, και μεγιστοποιούν την ασφάλεια δεδομένων. Επίσης οι τεχνολογίες αυτές επιτρέπουν στους χρήστες του διαδικτύου να προστατεύουν το απόρρητο των προσωπικών τους στοιχείων (PII)[28], το οποίο συχνά παρέχεται και διαχειρίζεται από υπηρεσίες ή εφαρμογές. Χρησιμοποιούν τεχνικές για την ελαχιστοποίηση της κατοχής προσωπικών δεδομένων από ένα σύστημα πληροφοριών χωρίς να χάνουν την λειτουργικότητά τους.



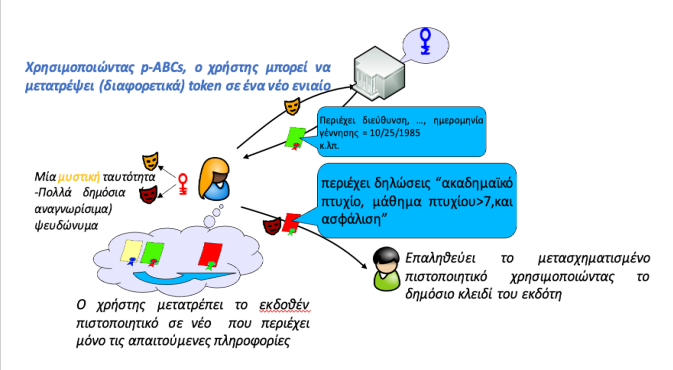
Σχήμα 6:Τεχνολογίες ενίσχυσης της ιδιωτικότητας (PET)

Κύριος στόχος των τεχνολογιών ενίσχυσης ιδιωτικότητας (PET) είναι η προστασία των προσωπικών δεδομένων και η διαβεβαίωση των χρηστών για δύο βασικά σημεία: οι πληροφορίες διατηρούνται εμπιστευτικές και η διαχείριση της προστασίας των δεδομένων αποτελεί προτεραιότητα για τους οργανισμούς που έχουν την ευθύνη για οποιαδήποτε PET[29]. Οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (PET)επιτρέπουν στους χρήστες να προβούν σε μία ή περισσότερες από τις ακόλουθες ενέργειες που σχετίζονται με τα προσωπικά δεδομένα που αποστέλλονται και χρησιμοποιούνται από παρόχους διαδικτυακών υπηρεσιών, εμπόρους ή άλλους χρήστες (ο έλεγχος αυτός είναι γνωστός ως αυτοδιάθεση[30].

Τέλος οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (PET) παρέχουν τη δυνατότητα εξ αποστάσεως ελέγχου της επιβολής αυτών των όρων και προϋποθέσεων στους παρόχους διαδικτυακών υπηρεσιών , επιτρέπουν στους χρήστες να καταγράφουν, να αρχειοθετούν και να αναζητούν προηγούμενες μεταφορές των προσωπικών τους δεδομένων, συμπεριλαμβανομένων των δεδομένων που έχουν μεταφερθεί, πότε σε ποιον και υπό ποιες προϋποθέσεις και να διευκολύνουν τη χρήση τους για επιθεώρηση, διόρθωση και διαγραφή δεδομένων. Τα PET παρέχουν στα άτομα προστασία της ιδιωτικότητας, δηλαδή να κρύψουν την προσωπική τους ταυτότητα. Η διαδικασία περιλαμβάνει την απόκρυψη των προσωπικών πληροφοριών κάποιου και την αντικατάσταση αυτών των πληροφοριών με ψευδο-δεδομένα ή μια ανώνυμη ταυτότητα. Εκτός από τις τεχνολογίες ενίσχυσης της ιδιωτικότητας (PET), παρακάτω θα αναλύσουμε και την τεχνολογία που βασίζεται στα διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου(P-ABC).

2.1 Διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου (Privacy Attribute-based Credentials)

Τα τελευταία χρόνια, έχουν αναπτυχθεί διάφορες τεχνολογίες για τη δημιουργία συστημάτων που ενισχύουν την ιδιωτικότητα, συστήματα διαπιστευτηρίων με βάση τα χαρακτηριστικά (Privacy-ABC) με τρόπο ώστε να μπορούν να είναι αξιόπιστα, όπως τα κανονικά κρυπτογραφικά πιστοποιητικά, ενώ ταυτόχρονα προστατεύουν την ιδιωτικότητα του κατόχου τους. Τα Διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου (Privacy-ABC) εκδίδονται όπως τα συνήθη κρυπτογραφικά πιστοποιητικά (π.χ. πιστοποιητικά X.509) χρησιμοποιώντας ένα ψηφιακό (μυστικό) κλειδί υπογραφής[22].



Σχήμα 7:Διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου(P-ABC)

Τα διαπιστευτήρια με βάση τα χαρακτηριστικά ιδιωτικότητας (P-ABC) είναι ένας τύπος ψηφιακών διαπιστευτηρίων που επιτρέπει στα άτομα να αποκαλύπτουν μόνο τα συγκεκριμένα κομμάτια πληροφοριών που απαιτούνται για μια συγκεκριμένη συναλλαγή ή αλληλεπίδραση, διατηρώντας παράλληλα τα υπόλοιπα προσωπικά τους δεδομένα ιδιωτικά. Έχουν σχεδιαστεί για να ενισχύουν την ιδιωτικότητα και την ασφάλεια στις ψηφιακές συναλλαγές, επιτρέποντας στα άτομα να αποκαλύπτουν επιλεκτικά πληροφορίες χωρίς να αποκαλύπτουν περιττές ή ευαίσθητες πληροφορίες.

Επιπλέον βασίζονται σε μια κρυπτογραφική τεχνική γνωστή ως κρυπτογράφηση βάσει χαρακτηριστικών(Attribute-Based Encryption - ABE)[31], η οποία επιτρέπει την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων βάσει συγκεκριμένων χαρακτηριστικών. Στην περίπτωση των

διαπιστευτηρίων με βάση τα χαρακτηριστικά ιδιωτικότητας (P-ABCs), τα χαρακτηριστικά μπορεί να περιλαμβάνουν όπως η ηλικία, το φύλο ή το επίπεδο εκπαίδευσης και κάθε χαρακτηριστικό συνδέεται με ένα μοναδικό κρυπτογραφικό κλειδί. Όταν ένα άτομο πρέπει να μοιραστεί τις προσωπικές του πληροφορίες, μπορεί να αποκαλύψει επιλεκτικά τα σχετικά χαρακτηριστικά και τα σχετικά κλειδιά, χωρίς να αποκαλύψει καμία πρόσθετη πληροφορία.

Μπορούν να χρησιμοποιηθούν σε διάφορα περιβάλλοντα, όπως η υγειονομική περίθαλψη, τα οικονομικά και το ηλεκτρονικό εμπόριο, και μπορούν να προσφέρουν μια σειρά από οφέλη. Για παράδειγμα, τα διαπιστευτήρια με βάση τα χαρακτηριστικά ιδιωτικότητας (P-ABC) μπορούν να μειώσουν τον κίνδυνο κλοπής ταυτότητας και απάτης, επιτρέποντας στα άτομα να μοιράζονται μόνο τις πληροφορίες που απαιτούνται για μια συγκεκριμένη συναλλαγή, αντί να παρέχουν πλήρη πρόσβαση στα προσωπικά τους δεδομένα. Επίσης, μπορούν να ενισχύσουν την προστασία της ιδιωτικότητας, επιτρέποντας στα άτομα να διατηρούν τα προσωπικά τους δεδομένα ιδιωτικά, παρέχοντας ωστόσο τις απαραίτητες πληροφορίες για μια συναλλαγή.

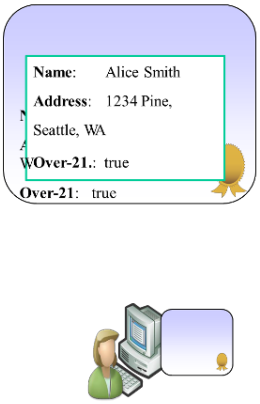
Συνοπτικά, τα διαπιστευτήρια με βάση τα χαρακτηριστικά ιδιωτικότητας (P-ABC) είναι μια πολλά υποσχόμενη τεχνολογία για την ενίσχυση της ιδιωτικότητας και της ασφάλειας στις ψηφιακές συναλλαγές. Επιτρέποντας στα άτομα να αποκαλύπτουν επιλεκτικά μόνο τις απαραίτητες πληροφορίες για μια συναλλαγή, μπορούν να μειώσουν τον κίνδυνο κλοπής ταυτότητας και απάτης, προστατεύοντας παράλληλα τα προσωπικά δεδομένα των ατόμων. Ωστόσο, η υιοθέτηση και η εφαρμογή των διαπιστευτηρίων με βάση τα χαρακτηριστικά ιδιωτικότητας (PABCs) θα απαιτήσει σημαντικό συντονισμό και αλλαγές στις υποδομές, ενώ ενδέχεται να υπάρξουν δυνητικοί κίνδυνοι για την ασφάλεια και την προστασία της ιδιωτικότητας που συνδέονται με τη χρήση κρυπτογραφικών κλειδιών.

Από την άλλη όμως πλευρά στη βιβλιογραφία υπάρχουν μερικές προτάσεις για τον τρόπο υλοποίησης ενός συστήματος Privacy-ABC. Αξιοσημείωτη είναι κυρίως η εμφάνιση δύο τεχνολογιών, του Identity Mixer[13] της IBM και το U-Prove[32] της Microsoft. Ειδικότερα, τα χρηματοδοτούμενα από την ΕΕ έργα PRIME[2] και PrimeLife[29] έδειξαν ότι η σύγχρονη έρευνα πρωτοτύπων των συστημάτων Privacy-ABC που μπορούν πράγματι να αντιμετωπίσουν τις προκλήσεις της ιδιωτικότητας της ταυτότητας συστημάτων διαχείρισης.

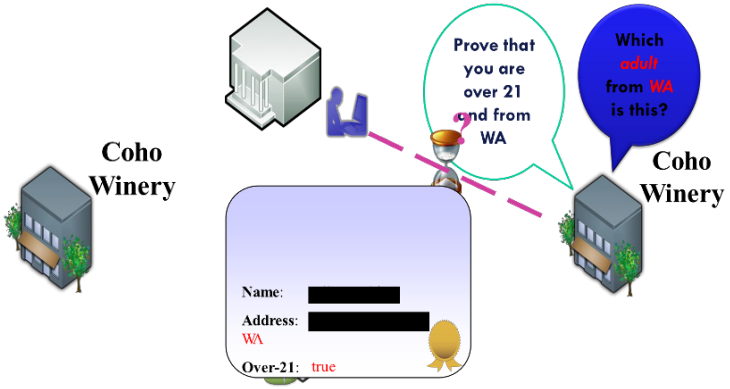
2.2 Τι προσφέρουν τα Διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου (Privacy Attribute-based Credentials)

Στο παρών κεφάλαιο θα παρουσιάσουμε τι μπορούν να προσφέρουν τα διαπιστευτήρια βάση χαρακτηριστικών απορρήτου (P-ABC)[33].

Ελάχιστη αποκάλυψη (Minimal Disclosure): Τα διαπιστευτήρια βάση χαρακτηριστικών απορρήτου (P-ABC)επιτρέπουν στους χρήστες να αντλούν αυθεντικά και επαληθεύσιμα διαπιστευτήρια που περιέχουν μόνο τις απαιτούμενες πληροφορίες, αποφεύγοντας έτσι την αποκάλυψη όλων των χαρακτηριστικών στα διαπιστευτήρια. Για παράδειγμα, οι πολίτες μιας χώρας μπορούν να αποκτήσουν ένα διαπιστευτήριο ταυτότητας από το κυβέρνηση και να χρησιμοποιήσουν αυτό το διαπιστευτήριο για να συμμετάσχουν σε μια διαδικτυακή δημοσκόπηση της περιοχής διαμονής τους αποκαλύπτοντας μόνο το χαρακτηριστικό ταχυδρομικό κώδικα της διεύθυνσής τους. Επιπλέον, είναι ακόμη δυνατό να γίνει απόδειξη της κατοχής ενός συγκεκριμένου τύπου διαπιστευτηρίων χωρίς να αποκαλύπτεται κανένα από τα πιστοποιημένα χαρακτηριστικά. Ως παράδειγμα, ένας φοιτητής του Πανεπιστημίου των Ιωαννίνων θα μπορούσε να έχει δωρεάν πρόσβαση σε έναν διαδικτυακό κινηματογράφο παρέχοντας μια απόδειξη ότι κατέχει έγκυρο «Φοιτητικό διαπιστευτήριο το πανεπιστήμιο».



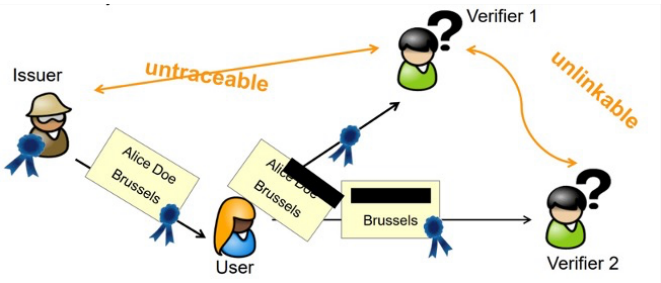
Σχήμα 8:Παράδειγμα ελάχιστης αποκάλυψης



Σχήμα 9:Πλήρες παράδειγμα ελάχιστης αποκάλυψης

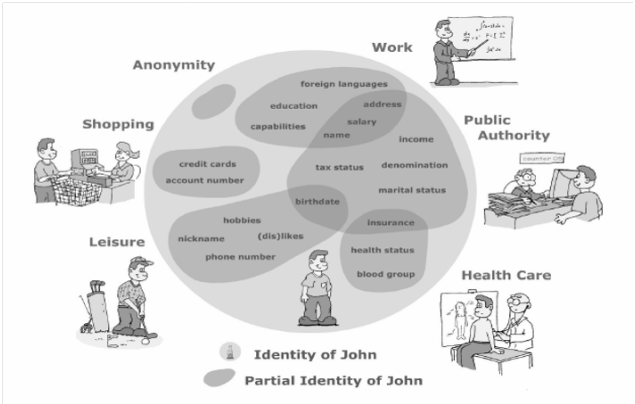
Μη συνδεσιμότητα(Unlinkability): Ένα άλλο βασικό χαρακτηριστικό των διαπιστευτηρίων βάση χαρακτηριστικών απορρήτου (P-ABC)είναι η μη συνδεσιμότητα, η οποία εμφανίζεται σε δύο διαφορετικούς τύπους, η μη συνδεσιμότητα με την έκδοσή τους και η μη συνδεσιμότητα σε διαφορετικές παρουσιάσεις. Η πρώτη υποδηλώνει ότι η έκδοση και η χρήση ενός διαπιστευτηρίου

δεν μπορούν να συσχετιστούν παρά μόνο λόγω των αποκαλυπτόμενων χαρακτηριστικών. Επομένως, εάν ο χρήστης δεν αποκαλύπτει καμία αναγνωρίσιμη πληροφορία, ο εκδότης διαπιστευτηρίων και ο πάροχος υπηρεσιών (ελεγκτής) δεν μπορούν να μάθουν περισσότερα για τον χρήστη, ακόμη και αν συνεννοηθούν. Ομοίως, στην τελευταία περίπτωση, δεν θα ήταν δυνατόν να συσχετιστούν διαφορετικές συναλλαγές του ίδιου χρήστη όταν οι πληροφορίες που αποκαλύπτονται δεν παρέχουν καμία δυνατότητα σύνδεσης.



Σχήμα 9:Μη συνδεσιμότητα

Partial Identities and identifiers(Μερικές ταυτότητες και αναγνωριστικά): Η έννοια των ψευδωνύμων στα διαπιστευτήρια βάση χαρακτηριστικών απορρήτου (P-ABC) διευκολύνει την καθιέρωση διαφορετικών προφίλ και τη θέσπιση ορίων μεταξύ διαφορετικών δραστηριοτήτων ενός ατόμου στο πλαίσιο ή σε διαφορετικά πλαίσια, και συνεπώς επιτυγχάνει ένα ελεγχόμενο επίπεδο συνδεσιμότητας. Τα ψευδώνυμα είναι παρόμοια με τα δημόσια κλειδιά και προέρχονται από τα μυστικά κλειδιά των χρηστών. Ωστόσο, σε αντίθεση με τα δημόσια κλειδιά των οποίων υπάρχει μόνο ένα για κάθε μυστικό κλειδί, οι χρήστες μπορούν να δημιουργήσουν απεριόριστο αριθμό μη συνδέσιμων ψευδονύμων για ένα μόνο μυστικό κλειδί.



Σχήμα 10:Partial Identities and identifiers(Μερικές ταυτότητες και αναγνωριστικά)

2.3 Βασικές έννοιες Διαπιστευτηρίων βάσει χαρακτηριστικών απορρήτου

Οι κύριες οντότητες είναι οι χρήστες(users), οι εκδότες(issuers) και οι επαληθευτές(verifiers), ενώ προαιρετικές οντότητες είναι οι επιθεωρητές(inspectors) και οι αρχές ανάκλησης(revocation authorities):

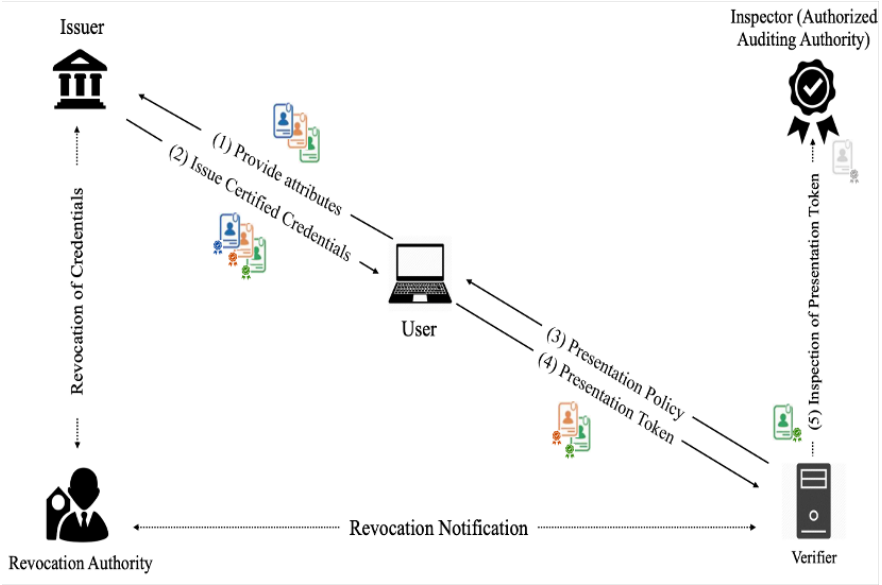
Ο χρήστης(user) συλλέγει διαπιστευτήρια από διάφορους εκδότες και ελέγχει ποιες πληροφορίες από ποια διαπιστευτήρια παρουσιάζονται σε ποιους επαληθευτές.

Ο εκδότης(issuer) εκδίδει διαπιστευτήρια στους χρήστες, και εγγυάται έτσι για την ορθότητα των των πληροφοριών που περιέχονται στο διαπιστευτήριο σε σχέση με τον χρήστη στον οποίο εκδίδεται το διαπιστευτήριο. Κάθε εκδότης παράγει ένα μυστικό κλειδί έκδοσης και δημοσιεύει το παραμέτρους του εκδότη που περιλαμβάνουν το αντίστοιχο δημόσιο κλειδί επαλήθευσης.

Ο επαληθευτής(verifier) προστατεύει την πρόσβαση σε έναν πόρο ή μια υπηρεσία που προσφέρει, επιβάλλοντας περιορισμούς στα διαπιστευτήρια που πρέπει να κατέχουν οι χρήστες και στις πληροφορίες από τα διαπιστευτήρια που πρέπει να παρουσιάζουν οι χρήστες για να έχουν πρόσβαση στην υπηρεσία.

Η αρχή ανάκλησης (προαιρετικά)(revocation authority) είναι υπεύθυνη για την ανάκληση των εκδοθέντων διαπιστευτηρίων, έτσι ώστε αυτά τα διαπιστευτήρια να μην μπορούν πλέον να χρησιμοποιηθούν για τη δημιουργία ενός διακριτικού παρουσίασης.

Ο επιθεωρητής (προαιρετικό)(inspector) είναι μια έμπιστη αρχή που μπορεί να αποανωνυμοποιήσει τα διακριτικά παρουσίασης υπό συγκεκριμένες συνθήκες.



Σχήμα 11:Βασικές έννοιες Διαπιστευτηρίων βάσει χαρακτηριστικών απορρήτου

Ένα διαπιστευτήριο περιέχει ζεύγη χαρακτηριστικών-τιμών, πιστοποιημένα από τον εκδότη. Ένας χρήστης μπορεί να δημιουργήσει ένα διακριτικό παρουσίασης που περιέχει ένα υποσύνολο των πιστοποιημένων χαρακτηριστικών. Κατά την παραλαβή ενός διακριτικού παρουσίασης από έναν χρήστη, ένας επαληθευτής ελέγχει αν το διακριτικό παρουσίασης είναι έγκυρο σε σχέση με τα δημόσια κλειδιά των σχετικών εκδοτών. Εάν η επαλήθευση είναι επιτυχής, ο επαληθευτής μπορεί να είναι βέβαιος ότι οι αντίστοιχοι εκδότες εγγυώνται για τα χαρακτηριστικά. που περιέχονται στα διακριτικά παρουσίασης (presentation token).

Μια ασφαλής υλοποίηση ενός συστήματος Privacy-ABC πρέπει να εγγυάται τα εξής:

1) οι χρήστες μπορούν να δημιουργήσουν ένα έγκυρο διαπιστευτήριο(token) μόνο εάν όντως τους έχει εκδοθεί το αντίστοιχο διαπιστευτήριο, και

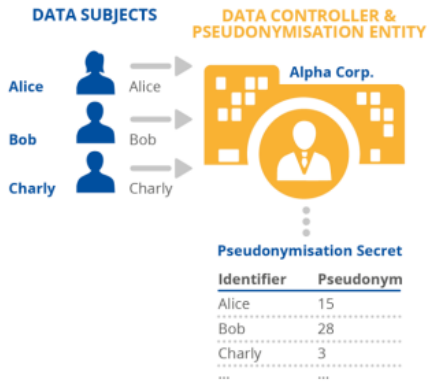
2) τα διακριτικά παρουσίασης(presentation token) δεν αποκαλύπτουν καμία περαιτέρω πληροφορία για τους χρήστες εκτός από τα χαρακτηριστικά που περιέχονται σε αυτά.

Το σημείο (2) περιλαμβάνει τη μη συνδεσιμότητα και τη μη ανιχνευσιμότητα των διαπιστευτηρίων (tokens). Η μη συνδεσιμότητα σημαίνει ότι τα διαφορετικά διακριτικά που προέρχονται από το ίδια διαπιστευτήρια δεν μπορούν να συνδεθούν μεταξύ τους. Η μη ανιχνευσιμότητα καλύπτει τη διαδικασία έκδοσης και απαιτεί ότι ο εκδότης δεν μπορεί να συνδέσει ένα διαπιστευτήριο (token) με μια συγκεκριμένη συνεδρία του χρήστη. Και οι δύο

ιδιότητες μόνο ισχύουν σε σχέση με την αναγνωρισιμότητα λόγω των αποκαλυπτόμενων χαρακτηριστικών.

2.4 Ψευδώνυμα (Pseudonyms)

Στην παραδοσιακή κρυπτογραφία δημόσιου κλειδιού, οι χρήστες δημιουργούν ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού που μπορεί να χρησιμοποιηθεί για την πιστοποίηση της ταυτότητας των χρηστών. Σε ένα σύστημα Privacy-ABC, ωστόσο, οι χρήστες μπορούν να δημιουργήσουν όσα δημόσια κλειδιά επιθυμούν από ένα δημιουργημένο μυστικό κλειδί. Αυτά τα δημόσια κλειδιά ονομάζονται ψευδώνυμα. Τα ψευδώνυμα είναι κρυπτογραφικά ασύνδετα, πράγμα που σημαίνει ότι αν δοθούν δύο διαφορετικά ψευδώνυμα, δεν μπορεί κανείς να πει αν δημιουργήθηκαν από το ίδιο ή από διαφορετικά μυστικά κλειδιά[34].



Σχήμα 12:Παράδειγμα Ψευδώνυμου[35]

Με τη δημιουργία διαφορετικών ψευδωνύμων οι χρήστες μπορούν να είναι γνωστοί με διαφορετικά μη συνδεόμενα ψευδώνυμα σε διαφορετικούς ιστότοπους, αλλά να χρησιμοποιούν το ίδιο μυστικό κλειδί για να πιστοποιούνται σε όλους αυτούς.

Επιπλέον ένα μυστικό κλειδί μπορεί να δημιουργηθεί από ένα κομμάτι αξιόπιστου υλικού (π.χ. έξυπνη κάρτα) που αποθηκεύει το κλειδί και το χρησιμοποιεί σε υπολογισμούς (π.χ. για τη δημιουργία ψευδωνύμων), αλλά ποτέ δεν αποκαλύπτει το κλειδί. Το κλειδί είναι έτσι συνδεδεμένο με το υλικό, έτσι ώστε το υλικό πρέπει να είναι παρόν για να χρησιμοποιηθεί το κλειδί.

Υπάρχουν καταστάσεις όπου η δυνατότητα να δημιουργηθούν πολλά μη συνδεόμενα ψευδώνυμα είναι ανεπιθύμητη. Για παράδειγμα σε μια διαδικτυακή δημοσκόπηση, οι χρήστες δεν θα πρέπει να μπορούν να ψηφίζουν εισάγοντας πολλαπλές ψήφους με διαφορετικά ψευδώνυμα. Σε τέτοιες περιπτώσεις, ο επαληθευτής μπορεί να ζητήσει ένα ειδικό ψευδώνυμο που ονομάζεται αποκλειστικό πεδίο εφαρμογής ψευδώνυμο, το οποίο είναι μοναδικό για τον χρήστη.

2.5 Διαπιστευτήρια και δέσμευση κλειδιών (Credentials and Key Binding)

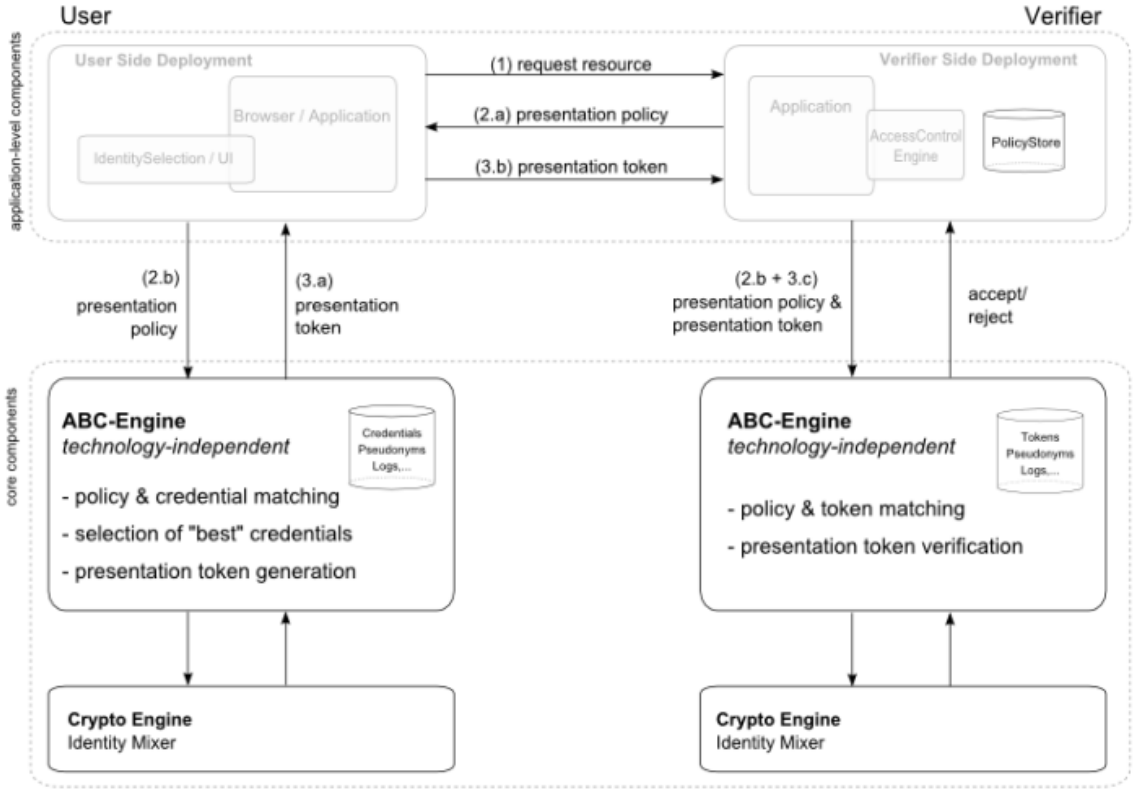
Ένα διαπιστευτήριο περιλαμβάνει τα χαρακτηριστικά του χρήστη που αποδίδονται σε αυτόν από τον εκδότη. Ένα χαρακτηριστικό περιγράφεται από τον τύπο του χαρακτηριστικού που καθορίζει τη σημασιολογία του χαρακτηριστικού (π.χ. όνομα) και την τιμή του χαρακτηριστικού που καθορίζει το περιεχόμενό του (π.χ. "John"). Με την έκδοση ενός διαπιστευτηρίου, ο εκδότης εγγυάται για την ορθότητα των περιεχόμενων χαρακτηριστικών σε σχέση με τον χρήστη[49].

Προαιρετικά, ένα διαπιστευτήριο συνδέεται με το μυστικό του κλειδί του χρήστη, δηλαδή δεν μπορεί να χρησιμοποιηθεί χωρίς το μυστικό κλειδί. Αυτό το ονομάζουμε δέσμευση κλειδιού. Είναι κάπως ανάλογο με τα παραδοσιακά πιστοποιητικά δημοσίου κλειδιού, όπου το πιστοποιητικό περιέχει την υπογραφή της CA στο δημόσιο κλειδί του χρήστη, αλλά σε αντίθεση με τα παραδοσιακά πιστοποιητικά δημοσίου κλειδιού, ένα Privacy-ABC[36] δεν συνδέεται με ένα μοναδικό δημόσιο κλειδί, συνδέεται μόνο με ένα μοναδικό μυστικό κλειδί του χρήστη. Ένας χρήστης μπορεί να αντλήσει ψευδώνυμα από αυτό το μυστικό κλειδί και (προαιρετικά) να δείξει ότι αυτά προέρχονται από το ίδιο μυστικό κλειδί που διέπει το πιστοποιητικό. Όπως και τα ψευδώνυμα, τα διαπιστευτήρια μπορούν επίσης να συνδεθούν με μια αξιόπιστη φυσική συσκευή, όπως μια έξυπνη κάρτα.

2.6 Παρουσίαση διαπιστευτηρίου (Presentation token)

Ο χρήστης σε μια τυπική αλληλεπίδρασης ζητάει πρώτα πρόσβαση σε έναν προστατευόμενο πόρο, οπότε ο επαληθευτής αποστέλλει μια πολιτική παρουσίασης που περιγράφει ποια διαπιστευτήρια πρέπει να παρουσιάσει ο χρήστης και ποιες πληροφορίες από αυτά τα διαπιστευτήρια πρέπει να αποκαλυφθούν για να αποκτήσει πρόσβαση. Στη συνέχεια, η μηχανή ABC του χρήστη ελέγχει αν διαθέτει τα απαραίτητα διαπιστευτήρια, και αν ναι, παράγει ένα διακριτικά παρουσίασης (presentation token) που περιέχει τα κατάλληλα κρυπτογραφικά αποδεικτικά στοιχεία[22].

Μετά τη λήψη του διακριτικά παρουσίασης (presentation token), ο επαληθευτής ελέγχει ότι τα κρυπτογραφικά αποδεικτικά στοιχεία είναι έγκυρα για το παρουσιαζόμενο διακριτικό και ελέγχει ότι το εν λόγω διακριτικό αν ικανοποιεί την πολιτική παρουσίασης. Εάν και οι δύο έλεγχοι είναι επιτυχείς, τότε χορηγεί πρόσβαση στον πόρο. Η αλληλουχία μιας αλληλεπίδρασης διακριτικά παρουσίασης απεικονίζεται στο Σχήμα 13 παρακάτω.



Σχήμα 13:Presentation[22]

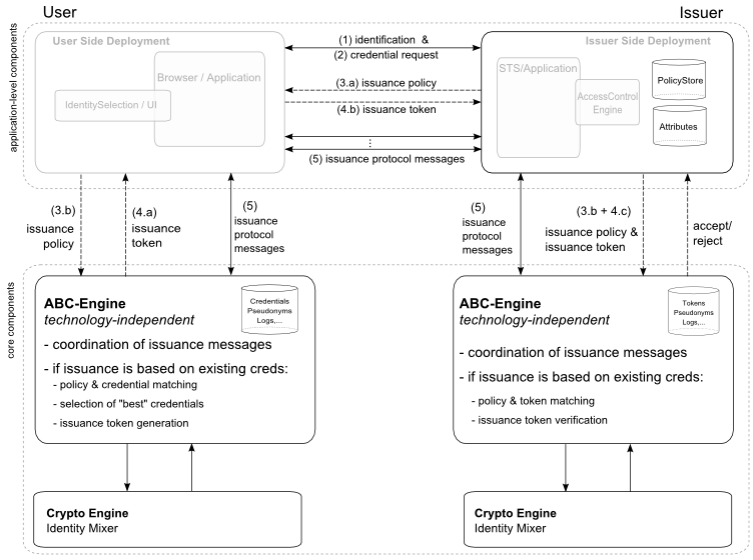
Τα διακριτικά παρουσίασης(presentation token) αποκαλύπτουν μόνο τα χαρακτηριστικά που ζητούνται ρητά από την πολιτική παρουσίασης - όλα τα άλλα χαρακτηριστικά στα διαπιστευτήρια παραμένουν κρυφά. Επιπλέον, τα διακριτικά παρουσίασης(presentation token) είναι κρυπτογραφικά μη συνδεόμενα και μη ανιχνεύσιμα (δεν υπάρχει συνεννόηση εκδοτών και επαληθευτών). Μπορεί να πει αν δύο διακριτικά παρουσίασης παράγονται από τον ίδιο ή από διαφορετικούς χρήστες, ή να συσχετίσει ένα διακριτικό παρουσίασης (presentation token) με την έκδοση του.

Αντί να ζητήσει και να αποκαλύψει πλήρη τιμές των χαρακτηριστικών, οι πολιτικές παρουσίασης(presentation policy) και τα διαπιστευτήρια (tokens) μπορούν να ζητούν και να αποκαλύπτουν κατηγορήματα πάνω σε ένα χαρακτηριστικό. Για παράδειγμα ένα διακριτικό μπορεί να αποκαλύψει ότι το όνομα στην πιστωτική κάρτα του χρήστη ταιριάζει με εκείνο στην άδεια οδήγησης, χωρίς να αποκαλύπτει το όνομα, ή ένα σύμβολο θα μπορούσε να αποκαλύψει ότι η ημερομηνία γέννησης του χρήστη είναι πριν από την 1η Ιανουαρίου 1994, χωρίς να αποκαλύψει την ακριβή ημερομηνία γέννησής της.

Όταν η πολιτική παρουσίασης(presentation policy) απαιτεί διαπιστευτήρια συνδεδεμένα με κλειδί, το παράγωγο διακριτικό παρουσίασης περιέχει πάντα μια έμμεση απόδειξη της γνώσης του υποκείμενου μυστικού κλειδιού. Με αυτόν τον τρόπο ο επαληθευτής μπορεί να είναι βέβαιος ότι ο νόμιμος κάτοχος του διαπιστευτηρίου συμμετείχε στη δημιουργία του διακριτικού παρουσίασης. Όταν το μυστικό κλειδί του χρήστη είναι κλειδί συσκευής, δηλαδή ένα κλειδί που φυλάσσεται σε μια αξιόπιστη συσκευή και δεν μπορεί να εξαχθεί από τη συσκευή, τότε η απόδειξη της του κλειδιού πραγματοποιείται στη συσκευή και περιλαμβάνεται στη δημιουργία του διακριτικού παρουσίασης. Κατά συνέπεια, για διαπιστευτήρια που είναι συνδεδεμένα με κλειδί σε μια φυσική συσκευή είναι αδύνατο να δημιουργηθεί ένα διακριτικό παρουσίαση(Presentation token) χωρίς τη συσκευή.

2.7 Έκδοση(Issuance)

Στην απλούστερη περίπτωση, ο εκδότης γνωρίζει όλες τις τιμές των χαρακτηριστικών που πρόκειται να εκδοθούν. Η έκδοση διαπιστευτηρίων είναι ένα διαδραστικό πρωτόκολλο πολλαπλών γύρων μεταξύ του εκδότη και του χρήστη, στο τέλος του οποίου ο χρήστης αποκτά ένα νέο διαπιστευτήριο. Πριν από την έκδοση, ο εκδότης μπορεί να έχει λάβει και επαληθεύσει όλες τις τιμές των χαρακτηριστικών μέσω μιας διαδικασίας εκτός ζώνης[22]. Η αλληλουχία μιας αλληλεπίδρασης έκδοσης διαπιστευτηρίων απεικονίζεται στο σχήμα 14 παρακάτω.



Σχήμα 14:Issuance

Τα ABCs υποστηρίζουν επίσης προηγμένα χαρακτηριστικά έκδοσης, στα οποία τα χαρακτηριστικά «μεταφέρονται» τυφλά από τα υπάρχοντα διαπιστευτήρια, χωρίς ο εκδότης να γνωρίζει τις τιμές τους. Παρομοίως, ο εκδότης μπορεί να εκδώσει τυφλά τις τιμές των χαρακτηριστικών που ο ίδιος ο χρήστης έχει δηλώσει (δηλαδή, που δεν έχουν πιστοποιηθεί από ένα υπάρχον διαπιστευτήριο), να μεταφέρει το μυστικό κλειδί με το οποίο δεσμεύεται ένα διαπιστευτήριο ή να εκχωρήσει μια ομοιόμορφη τυχαία τιμή σε ένα χαρακτηριστικό, έτσι ώστε ο εκδότης να μην μπορεί να τη δει και ο χρήστης να μην μπορεί να τη στρεβλώσει.

Η προηγμένη έκδοση είναι ένα διαδραστικό πρωτόκολλο μεταξύ του χρήστη και του εκδότη. Σε πρώτη φάση, ο εκδότης παρέχει στον χρήστη μια πολιτική έκδοσης που αποτελείται από μια πολιτική παρουσίασης που καθορίζει ποια ψευδώνυμα ή/και υφιστάμενα διαπιστευτήρια πρέπει να παρουσιάσει ο χρήστης και από ένα πρότυπο διαπιστευτηρίων που καθορίζει ποια

χαρακτηριστικά ή μυστικά κλειδιά του νεοεκδιδόμενου διαπιστευτηρίου που θα δημιουργηθούν τυχαία ή θα μεταφερθούν από διαπιστευτήρια ή ψευδώνυμα στην πολιτική παρουσίασης. Σε απάντηση, ο χρήστης αποστέλλει ένα διακριτικό έκδοσης που περιέχει ένα διακριτικό παρουσίασης που ικανοποιεί την πολιτική έκδοσης, στη συνέχεια εκτελείται το πρωτόκολλο κρυπτογραφικής έκδοσης.

Κεφάλαιο 3ο

Το παρών κεφάλαιο έχει ως σκοπό να παρουσιάσει την κρυπτοβιβλιοθήκη OLYMPUS, η οποία παρέχει κρυπτογραφικές τεχνικές και υιοθετεί τεχνολογίες ενίσχυσης της ιδιωτικότητας με κατανεμημένο τρόπο με τη χρήση blockchain. Επίσης η κρυπτοβιβλιοθήκη OLYMPUS μπορεί να χρησιμοποιηθεί για την ανάπτυξη εφαρμογών που βελτιώνουν την ιδιωτικότητα των χρηστών, όπως η ηλεκτρονική ταυτότητα, η πρόσβαση σε πόρους και η επαλήθευση ταυτότητας.

Το πρώτο τμήμα παρέχει μια εισαγωγή στο θέμα της ιδιωτικότητας. Επίσης το δεύτερο τμήμα παρουσιάζει την κρυπτοβιβλιοθήκη OLYMPUS, συμπεριλαμβανομένης της αρχιτεκτονικής της και των λειτουργιών της. Το τρίτο τμήμα αποτελείται από τις σχεδιαστικές επιλογές των διαπιστευτηρίων βάσει χαρακτηριστικών απορρήτου (P-ABC) παρόχων ταυτότητας (IdPS) που χρησιμοποιούνται από την κρυπτοβιβλιοθήκη OLYMPUS. Το τέταρτο τμήμα περιγράφει τις κύριες αρχιτεκτονικές διαδικασίες για την εφαρμογή της διαχείρισης χρηστών για την πιστοποίηση ακαδημαϊκών τίτλων χρησιμοποιώντας την κρυπτοβιβλιοθήκη OLYMPUS. Το πέμπτο και τελευταίο τμήμα παρουσιάζει τα πλεονεκτήματα και τις προκλήσεις της χρήσης της κρυπτοβιβλιοθήκης OLYMPUS.

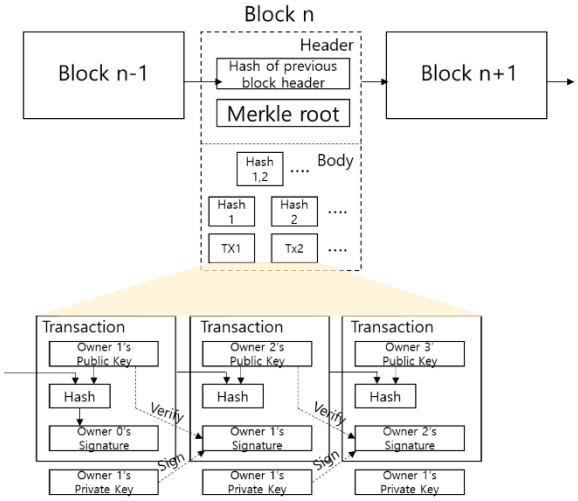
3.0 Τεχνολογίες για την προστασία ιδιωτικότητας και blockchain υποδομή

Στο παρόν κεφάλαιο θα παρουσιάσουμε την κρυπτοβιβλιοθήκη που παρέχει κρυπτογραφικές τεχνικές και υιοθετεί τεχνολογίες ενίσχυσης της ιδιωτικότητας με κατανεμημένο τρόπο με την χρήση Blockchain(αλυσίδα μπλοκ)[37].

Η αλυσίδα μπλοκ(blockchain) είναι μια αποκεντρωμένη, ψηφιακή τεχνολογία που επιτρέπει την ασφαλή αποθήκευση και μεταφορά πληροφοριών, και δεδομένων. Μια αλυσίδα μπλοκ αποτελείται από ένα μπλοκ (block), όπου κάθε μπλοκ(block) περιέχει ένα σύνολο συναλλαγών ή δεδομένων που επαληθεύονται από ένα δίκτυο κόμβων πριν προστεθούν στην αλυσίδα.

Ένα μπλοκ(block) συνήθως αποτελείται από την τιμή κατακερματισμού του προηγούμενου μπλοκ, την υπογραφή του συνεισφέροντος, ένα ωφέλιμο φορτίο και τη χρονική σήμανση. Η τιμή κατακερματισμού του προηγούμενου μπλοκ καθιστά την αλυσίδα μπλοκ αμετάβλητη (Σχήμα 15). Επομένως, σε αντίθεση με τις υπάρχουσες βάσεις δεδομένων, μπορεί να προσθέσει μόνο

συναλλαγές, τα δεδομένα δεν μπορούν να τροποποιηθούν ή να διαγραφούν. Επομένως, είναι εξαιρετικά δύσκολο να παραποιηθούν τα δεδομένα.



Σχήμα 15: Blockchain(αλυσίδα μπλοκ)

Επίσης η εισαγωγή δεδομένων είναι μη αναστρέψιμη δεδομένου του υπολογισμού κατακερματισμού εντός του μπλοκ. Δεύτερον, τα περιεχόμενα του προηγούμενου μπλοκ σχηματίζουν μια αλυσίδα με τα περιεχόμενα του επόμενου μπλοκ. Αυτό αποφεύγει το πιθανό πρόβλημα ενός σημείου αποτυχίας των κεντρικών δομών. Οι αλυσίδες μπλοκ χωρίζονται σε δημόσιες αλυσίδες μπλοκ στις οποίες μπορεί να συμμετάσχει ο καθένας και σε επιτρεπόμενες αλυσίδες μπλοκ που δέχονται μόνο εξουσιοδοτημένα μέλη. Ένα επιτρεπόμενο blockchain περιέχει ένα μέλος που προσδιορίζει εξουσιοδοτημένους χρήστες ή ομάδες.

Η κρυπτοβιβλιοθήκη που χρησιμοποιεί blockchain (αλυσίδα μπλοκ) είναι η OLYMPUS[38] είναι μια νέα πρόταση για τη διαχείριση της ταυτότητας με κατανεμημένη τεχνικές, με σκοπό να επιλύσει τα προβλήματα που παρουσιάστηκαν σε προηγούμενες λύσεις για την διαχείριση ταυτότητας. Η προσέγγιση αυτή επινοεί μια λύση που διατηρεί την ιδιωτικότητα ως λύση διαχείρισης ταυτότητας που εξελίσσεται από τα συστήματα ταυτότητας και εξαλείφει τον πάροχο ταυτότητας (IdP) ως το μοναδικό σημείο αποτυχίας. Εισάγει την έννοια της διαχείρισης ταυτότητας με λήθη[39]. Αυτή η προσέγγιση κατανέμει τη χωρητικότητα του παραδοσιακού παρόχου ταυτότητας σε πολλαπλούς παρόχους ταυτότητας. Κανένας διακομιστής , δεν μπορεί να υποδυθεί τους χρήστες του, να παρακολουθήσει τη διαδικτυακή τους συμπεριφορά, να συνδέσει τις εικονικές τους ταυτότητες σε διάφορες υπηρεσίες, ή να ανακτήσει τους κωδικούς πρόσβασης.

Επιπλέον η κρυπτοβιβλιοθήκη OLYMPUS[38] εστιάζει στην ευχρηστία, διαθέτοντας ένα πλαίσιο που με ελάχιστες απαιτήσεις στις συσκευές των χρηστών και δεν βασίζεται σε ασφαλή διαπιστευτήρια (token). Επίσης, σέβεται την ιδιωτικότητα των χρηστών, επιβάλλοντας τη μη δυνατότητα σύνδεσης των πιστοποιήσεων και την ελάχιστη αποκάλυψη δεδομένων που αφορούν τόσο τους παρόχους υπηρεσιών όσο και τους παρόχους ταυτότητας.

Τέλος στην παρούσα ενότητα παρουσιάζεται η τρέχουσα κατάσταση της τεχνολογίας όσον αφορά τα παραδοσιακά συστήματα διαχείρισης ταυτότητας (IdM) και παρουσιάζονται λύσεις που βασίζονται στην αλυσίδα μπλοκ (blockchain). Περιγράφουμε μια νέα πρόταση που βασίζεται στη διαχείριση ταυτότητας που βασίζεται στην κρυπτοβιβλιοθήκη OLYMPUS[9], [40] σε συνδυασμό με τεχνολογίες DLT (distributed ledger technologies).

3.2 Παρουσίαση πρωτοκόλλου /κρυπτοβιβλιοθήκης OLYMPUS

Για την υλοποίηση επιλέξαμε να δημιουργήσουμε μια διαδικτυακή εφαρμογή που εκμεταλλεύεται την κρυποτοβιβλιοθήκη OLYMPUS[38] για να προσφέρει έλεγχο ταυτότητας με διατήρηση της ιδιωτικότητας με βάση τα διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου(P-ABC).

Η κύρια ιδέα της κρυπτοβιβλιοθήκης OLYMPUS είναι η έννοια ενός κατανεμημένου εικονικού παρόχου ταυτότητας (IdP) (vIdP), που αντικαθιστά την παραδοσιακή έννοια του παρόχου ταυτότητας (IdP). Σε έναν παραδοσιακό πάροχο ταυτότητας (IdP) δίνεται ένα όνομα χρήστη και ένας κωδικός πρόσβασης (ή παρόμοιος τύπος διαπιστευτηρίων) και παράγει ένα διαπιστευτήριο πρόσβασης. Το διακριτικό πρόσβασης μπορεί στη συνέχεια να χρησιμοποιηθεί από τρίτους, δηλαδή από παρόχους υπηρεσιών, για να επαληθεύσουν την ταυτότητα του χρήστη.

Στην κρυπτοβιβλιοθήκη OLYMPUS[38], ο παραδοσιακός πάροχος ταυτότητας (IdP) αντικαθίσταται από έναν εικονικό πάροχο ταυτότητας vIdP (που αποτελείται από δύο ή περισσότερους μερικούς IdPs OLYMPUS (pIdP)). Διανέμοντας τις λειτουργίες του παρόχου ταυτότητας (IdP) στον εικονικό πάροχο ταυτότητας vIdP, η κρυπτοβιβλιοθήκη OLYMPUS προσφέρει κατανεμημένη επαλήθευση κωδικού πρόσβασης (όπου ένας μόνο IdP δεν μαθαίνει ποτέ τον κωδικό πρόσβασης του χρήστη) και κατανεμημένες υπογραφές (όπου όλοι οι IdP πρέπει να συνεργάζονται, προκειμένου να παράγουν ένα έγκυρο διακριτικό πρόσβασης).

Αυτά τα χαρακτηριστικά αναγκάζουν έναν επιτιθέμενο να θέσει σε κίνδυνο όλους τους παρόχουσ ταυτότητας (IdPs) να ρυθμίσουν τον εικονικό πάροχο ταυτότητας vIdP, προκειμένου να υποδυθεί

τους χρήστες ή να μάθει τους κωδικούς τους, βελτιώνοντας την ασφάλεια σε σύγκριση με έναν παραδοσιακό πάροχο ταυτότητας (IdP).

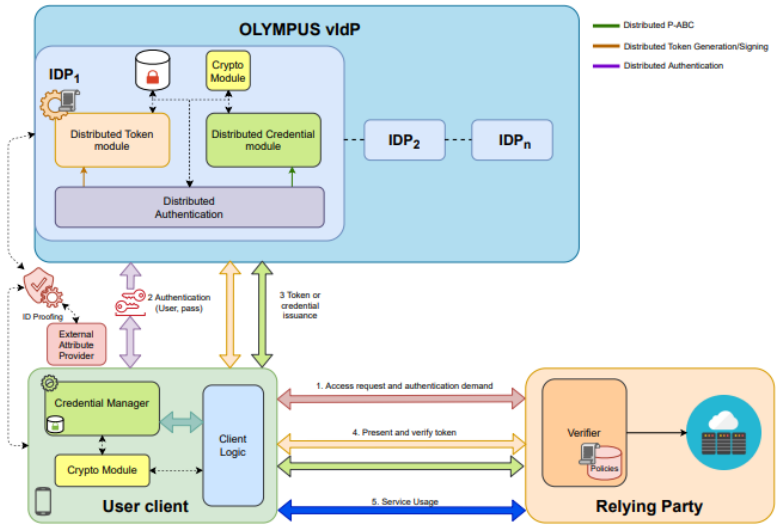
Συμπερασματικά αυτά τα νέα χαρακτηριστικά αυξάνουν την πολυπλοκότητα της ταυτότητας. Όπως θα δούμε και στην επόμενη ενότητα στόχος της κρυπτοβιβλιοθήκης είναι να διασφαλίσει τη συμβατότητα με τις υπάρχουσες τεχνολογίες των παραδοσιακών συστημάτων διαχείρισης ταυτότητας (IdM), όπως το OpenID Connect[9] και το SAML[21], τα κατανεμημένα πρωτόκολλα για την επαλήθευση κωδικού πρόσβασης και τις υπογραφές, απαιτούν μια ειδική εφαρμογή πελάτη και όχι την εγγενή υποστήριξη του προγράμματος περιήγησης.

3.3 Αρχιτεκτονική της κρυπτοβιβλιοθήκης OLYMPUS

Το σύστημα διαχείρισης ταυτότητας OLYMPUS(Σχήμα 5) περιλαμβάνει τρία κύρια μέρη : την εικονική ταυτότητα παρόχου (vIdP), το πελάτη-χρήστη και το τρίτο μέρος (RP)[38].

Virtual IdP: Είναι ένα σύνολο οντοτήτων (μερικοί IdPs) που συνεργάζονται για την εκτέλεση το ρόλο του παρόχου ταυτότητας. Κάθε ταυτότητα παρόχου (IdP) έχει τρεις ενότητες για την κύρια λειτουργία:

- Distributed authentication: διαχείριση λογαριασμών και σύνδεση χρηστών μέσω επαλήθευση κωδικού πρόσβασης (και ενδεχομένως έλεγχο ταυτότητας πολλαπλών παραγόντων). Ένα βασικό στοιχείο στη διαδικασία εγγραφής, κατά την οποία τα χαρακτηριστικά από αξιόπιστους εξωτερικούς παρόχους χαρακτηριστικών συνδέονται με το λογαριασμό.



Σχήμα 16: Αρχιτεκτονική Olympus[38]

- Distributed credential module: Δημιουργεί διαπιστευτήρια για το κατανεμημένο σχήμα p-ABC. Κάθε μονάδα δημιουργείται ανεξάρτητα από κάθε μερικό IdP (δηλ. δεν απαιτείται επικοινωνία ή ρητή συνεργασία κατά τη διάρκεια της διαδικασίας).
- Distributed token module: Δημιουργεί διαπιστευτήρια (υπογραφή τύπου RSA), τα οποία αποτελούν μέρος της "online" προσέγγισης του OLYMPUS.

User client: Παρέχει κοινές λειτουργίες ταυτότητας (εγγραφή, πιστοποίηση ταυτότητας, διαχείριση χαρακτηριστικών). Είναι υπεύθυνο για τις κρυπτογραφικές λειτουργίες και την ασφαλή διαχείριση των διαπιστευτηρίων.

Relying party: Δέχεται διαπιστευτήρια του OLYMPUS (p-ABC) για έλεγχο ταυτότητας χρήστη προκειμένου να εκτελεί έλεγχο πρόσβασης βάσει χαρακτηριστικών. Το τρίτο μέρος θα ορίζει και θα κοινοποιεί τις πολιτικές που πρέπει να πληρούνται για τη χορήγηση πρόσβασης (π.χ., να είναι κανείς άνω των 18 ετών ή να αποκαλύπτει το όνομα του χρήστη).

3.3 Διεργασίες για την υποστήριξη της ανώνυμης πρόσβασης

Στην παρούσα ενότητα περιγράφονται οι σχεδιαστικές επιλογές που χρειάζονται για την υλοποίηση του πιλοτικού προγράμματος. Αρχικά με την χρήση της κρυπτοβιβλιοθήκης OLYMPUS[38] τροποποιήσαμε τον πελάτη(Client) που συνεργαζόταν με την κλάση PestoIdPRESTConnection IdP και τον μετατρέψαμε σε PabcIdPRESTConnection IdP με αυτόν τον τρόπο καταφέραμε να τροποποιήσουμε και να λειτουργήσουμε τον Διαχειριστή Πιστοποιητικών έτσι ώστε να μπορεί να αποθηκεύει τα διαπιστευτήρια στον Πελάτη (Client). Κατά την εγγραφή των φοιτητών από τη γραμματεία του τμήματος, λαμβάνουν έναν κωδικό μιας χρήσης (OTP) για να μπορέσουν να συνδεθούν στο σύστημα.

Επιπλέον, στις φόρμες αίτησης για το μεταπτυχιακό ή διδακτορικό πρόγραμμα σπουδών κατά τη διάρκεια της αίτησης, στο στάδιο της εκτέλεσης, η αίτηση ανακατευθύνεται και αποστέλλεται ένα διακριτικό επαλήθευσης (verification token) από τον διακομιστή. Μετά την ανακατεύθυνση, η εφαρμογή αιτήσεων λαμβάνει ένα σύμβολο επαλήθευσης, ότι το διαπιστευτήριο που έχει μεταφορτωθεί έχει επαληθευτεί επιτυχώς από την πλευρά του πελάτη(client).

Για να λειτουργήσει ορθά η εφαρμογή ακολουθήσαμε τις μεθόδους που απευθύνονται για τη ρύθμιση pABC IdP και προορίζονται για κλήση από τον αντίστοιχο πελάτη.

- Perform OPRF (Username, Nonce, Cryptographic value, Token, TokenType):Εκτελεί μια λειτουργία OPRF σε μια κρυπτογραφική τιμή που βασίζεται σε έναν μη πραγματικό κωδικό (κατασκευασμένο με χρήση του κωδικού πρόσβασης του χρήστη). Εάν ένας λογαριασμός για έναν χρήστη με το δεδομένο όνομα χρήστη υπάρχει ήδη, τότε επικυρώνεται επίσης το προαιρετικό Token του TokenType πριν από την εκτέλεση της λειτουργίας OPRF. Ο χρήστης θα χρησιμοποιήσει την έξοδο για την (εκ νέου) δημιουργία ενός ζεύγους δημόσιου/ιδιωτικού κλειδιού υπογραφής.
- Finish Registration (Username, Cookie, Public Key, Signature, Nonce, idProof): Ολοκληρώνει την εγγραφή ενός λογαριασμού χρήστη αποθηκεύοντας ένα δημόσιο κλειδί που σχετίζεται με το όνομα χρήστη και προσθέτοντας χαρακτηριστικά στο προαιρετικό idProof (εφόσον μπορούν να επαληθευτούν). Ωστόσο, η υπογραφή στο nonce, το idProof και το Username πρέπει πρώτα να επαληθευτεί με το δημόσιο κλειδί. Επιπλέον, πρέπει επίσης να επαληθευτεί ότι το Cookie είναι έγκυρο (δηλαδή έχει ξεκινήσει η φάση εγγραφής

του χρήστη). Το δημόσιο κλειδί θα συσχετιστεί με το όνομα χρήστη και θα χρησιμοποιηθεί για την επαλήθευση μελλοντικών προσπαθειών ελέγχου ταυτότητας.

- AddAttributes (Username, Cookie, Nonce, Signature, idProof): Πιστοποιεί έναν ήδη υπάρχοντα χρήστη με βάση το όνομα χρήστη, ένα cookie συνεδρίας και μια υπογραφή στο όνομα χρήστη, το Nonce και το idProof. Εάν ο έλεγχος ταυτότητας πετύχει, τότε τα χαρακτηριστικά στο idProof προστίθενται στο λογαριασμό του χρήστη, με την προϋπόθεση ότι αυτά τα χαρακτηριστικά μπορούν να επαληθευτούν.
- DeleteAttributes (Username, Cookie, Nonce, Signature, Attributes): Ελέγχει την αυθεντικότητα ενός ήδη υπάρχοντος χρήστη με βάση το όνομα χρήστη, ένα cookie συνεδρίας και μια υπογραφή στο όνομα χρήστη, το Nonce και τα χαρακτηριστικά. Στη συνέχεια, διαγράφει τα Attributes που έχουν καθοριστεί από το λογαριασμό του χρήστη.
- DeleteAccount (Username, Cookie, Nonce, Signature):Ελέγχει την αυθεντικότητα ενός ήδη υπάρχοντος χρήστη με βάση το όνομα χρήστη, ένα cookie συνεδρίας και μια υπογραφή στο όνομα χρήστη, Nonce και διαγράφει εντελώς το λογαριασμό του χρήστη.
- ChangePassword (Username, NewSignature, OldSignature, New Public Key, Cookie, Nonce): Πιστοποιεί έναν ήδη υπάρχοντα χρήστη με βάση το όνομα χρήστη, ένα cookie συνεδρίας και δύο υπογραφές (NewSignature και OldSignature) για το όνομα χρήστη, το Nonce και το νέο δημόσιο κλειδί. Εάν ο έλεγχος είναι επιτυχής, συσχετίζει το Νέο Δημόσιο Κλειδί με το Όνομα Χρήστη.
- RefreshCookie (Cookie): Επικυρώνει ότι το cookie είναι ακόμα έγκυρο και επιστρέφει ένα νέο cookie με ανανεωμένο χρόνο ισχύος.
- Authenticate (Username, Cookie, Nonce, Signature, Policy): Ελέγχει την αυθεντικότητα ενός ήδη υπάρχοντος χρήστη με βάση το όνομα χρήστη, ένα cookie συνεδρίας και μια υπογραφή στο όνομα χρήστη, το Nonce και την πολιτική. Η υπογραφή επαληθεύεται με το δημόσιο κλειδί που σχετίζεται με το όνομα χρήστη. Εάν ο έλεγχος ταυτότητας είναι επιτυχής, τότε κατασκευάζεται και επιστρέφεται στον χρήστη ένα διακριτικό με βάση τα αποθηκευμένα χαρακτηριστικά του χρήστη σύμφωνα με την παρεχόμενη πολιτική. Δηλαδή, η πολιτική καθορίζει ποια χαρακτηριστικά του χρήστη περιλαμβάνονται στο διακριτικό (εάν υπάρχουν).

Τέλος εκτός από τις παραπάνω μεθόδους, ο PABC IdP παρέχει επιπλέον μεθόδους που περιγράφονται παρακάτω , οι οποίες μας βοήθησαν για την υλοποίηση του προγράμματος.

- Get dp-ABC Public Parameters:Επιστρέφει τις συγκεκριμένες παραμέτρους dp-ABC των διακομιστών.
- GetCredential (Username, Cookie, Nonce, Signature):Ελέγχει την αυθεντικότητα ενός ήδη υπάρχοντος χρήστη με βάση το όνομα χρήστη, ένα cookie συνεδρίας και μια υπογραφή στο όνομα χρήστη, το Nonce και την πολιτική. Η υπογραφή επαληθεύεται με το δημόσιο κλειδί που σχετίζεται με το όνομα χρήστη. Εάν ο έλεγχος ταυτότητας επιτύχει, τότε κατασκευάζεται και επιστρέφεται στον χρήστη ένα διαπιστευτήριο με βάση όλα τα χαρακτηριστικά του χρήστη.

3.4 Κύριες αρχιτεκτονικές διαδικασίες για την εφαρμογή διαχείρισης χρηστών για την Πιστοποίηση ακαδημαϊκών τίτλων

Το σύστημα μας Academic Degree Verification System περιλαμβάνει κατα κύριο λόγο τρεις φάσεις. Η φάση εγγραφής , η φάση παραγωγής(generation phase), κατά την οποία ένας εγγεγραμμένος χρήστης μπορεί να λάβει διακριτικά ή διαπιστευτήρια και τη φάση επαλήθευσης.

α) Η φάση εγγραφής

Επιτρέπει στο χρήστη να δημιουργήσει έναν νέο λογαριασμό χρήστη στον κατανεμημένο πάροχο ταυτότητας (vIdP).Ο λογαριασμός δημιουργείται για ένα όνομα χρήστη και προστατεύεται με έναν κωδικό πρόσβασης pwd. Η εγγραφή είναι μια διαδραστική φάση μεταξύ του και όλων των παρόχων ταυτότητας που συνθέτουν τον vIdP. Η εγγραφή πραγματοποιείται με τη χρήση ενός ονόματος χρήστη, ενός κωδικού πρόσβασης και προαιρετικά ενός συνόλου χαρακτηριστικών. Αυτά τα χαρακτηριστικά θα πρέπει να τα έχει λάβει ο χρήστης από έναν εξωτερικό πάροχο χαρακτηριστικών , ώστε ο vIdP να μπορεί να επαληθεύσει την εγκυρότητά τους πριν τα αποδεχθεί και τα αποθηκεύσει. Στο τέλος του πρωτοκόλλου εγγραφής ο χρήστης λαμβάνει ένα μήνυμα επιβεβαίωσης που υποδεικνύει την επιτυχή ολοκλήρωση της δημιουργίας λογαριασμού.

β) Η φάση παραγωγής(generation phase)

Η φάση δημιουργίας στο σύστημά μας αρχίζει όταν ένας χρήστης θέλει να κάνει χρήση της υπηρεσίας που προσφέρεται από το τρίτο μέρος (βήματα 1 και 2 του σχήματος 16). Η διαδικασία αυτή εκτελείται εκτός του πλαισίου της κρυπτοβιβλιοθήκης OLYMPUS. Ο κύριος στόχος της φάσης δημιουργίας είναι η κατανεμημένη παραγωγή/παρουσίαση της πιστοποίησης.

Η διαδικασία ελέγχου ταυτότητας αρχίζει όταν ο χρήστης πληκτρολογεί το όνομα χρήστη (user) και τον κωδικό πρόσβασης (pwd) στον vIdP (βήμα 3 του σχήματος 5). Μετά τον επιτυχή έλεγχο ταυτότητας προς τους παρόχους ταυτότητας, υπάρχει το κατανεμημένο P-ABC (Distributed Privacy-Attribute Based Credentials) είναι ένα κρυπτογραφικό πρωτόκολλο και ένα πλαίσιο που συνδυάζει κρυπτογράφηση βασισμένη σε χαρακτηριστικά και τεχνολογίες ενίσχυσης της ιδιωτικότητας για να επιτρέπει ασφαλή και διατηρητική της ιδιωτικότητας.

Επιπλόν στο σύστημα ο χρήστης παίρνει ένα διαπιστευτήριο P-ABC που έχει δημιουργηθεί με κατανεμημένο τρόπο (βήματα 4β, 5β και 6β). Τώρα ο χρήστης είναι σε θέση να χρησιμοποιήσει μια υπηρεσία που απαιτεί μια πολιτική πρόσβασης αντλώντας ο ίδιος ένα διακριτικό πρόσβασης με βάση το διαπιστευτήριο που έλαβε προηγουμένως (βήματα 7b και 8b). Τέλος ο χρήστης μπορεί να κρατήσει το διαπιστευτήριο με ασφάλεια στο σύστημα του, ο χρήστης μπορεί να δημιουργήσει το διακριτικό πρόσβασης χωρίς να επικοινωνήσει με τον vIdP (έτσι, μεταβαίνει απευθείας από το βήμα 2 στο βήμα 7b).

γ)Φάση επαλήθευσης

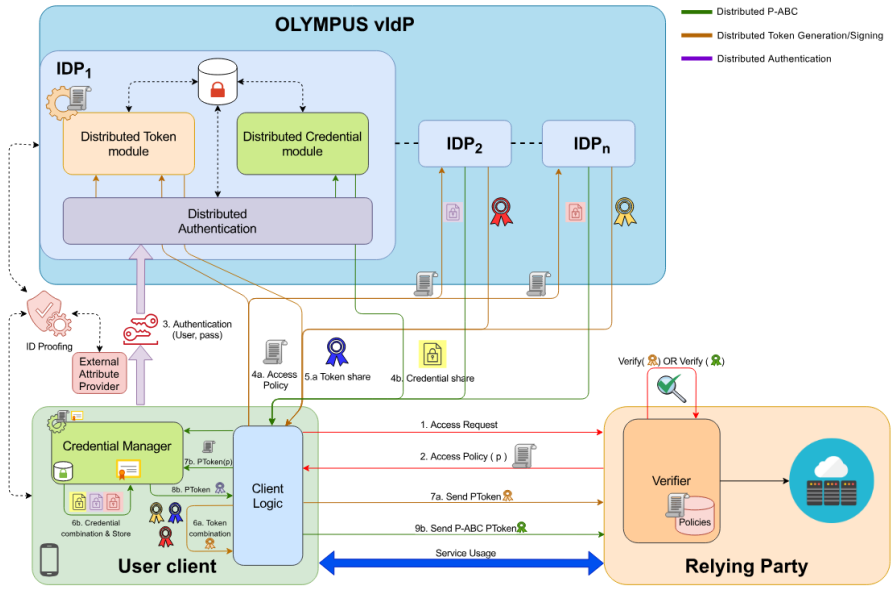
Είναι υπεύθυνη για την επαλήθευση της εγκυρότητας των υποβαλλόμενων διακριτικών πρόσβασης (συμπεριλαμβανομένου του ελέγχου των υπογραφών) και για το αν τα εν λόγω διακριτικά είναι κατάλληλα για μια δεδομένη πολιτική πρόσβασης. Ο επαληθευτής μπορεί να εφαρμόσει τα κατανεμημένα p-ABC που προέρχονται από τα διαπιστευτήρια του χρήστη.

Στην συνέχεια θα περιγραφούν οι σχεδιαστικές επιλογές διαπιστευτηρίων βάσει χαρακτηριστικών απορρήτου(P-ABC) παρόχων ταυτότητας (IdPS) για την εφαρμογή διαχείρισης χρηστών για την πιστοποίηση ακαδημαϊκών πιστοποιητικών

3.5 Βασικά συστήματα για την υποστηριξη της εφαρμογή διαχείρισης χρηστών για την πιστοποίηση ακαδημαϊκών τίτλων

Το σχήμα dP-ABC[38] (distributed partial attribute-based credential), το οποίο είναι ένα κρυπτογραφικό πρωτόκολλο που επιτρέπει τη διανομή των διαπιστευτηρίων των χρηστών μεταξύ πολλαπλών παρόχων ταυτότητας (IdPs), διατηρώντας παράλληλα το απόρρητο και την ασφάλεια.

Κάθε IdP δημιουργεί ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού και υπογράφει τα χαρακτηριστικά του χρήστη χρησιμοποιώντας το ιδιωτικό του κλειδί, με αποτέλεσμα ένα μερικό διαπιστευτήριο που περιέχει μόνο ένα υποσύνολο των χαρακτηριστικών του χρήστη. Ο χρήστης συνδυάζει τα διαπιστευτήρια από όλους τους IdPs σε ένα τελικό επαληθεύσιμο διαπιστευτήριο χρησιμοποιώντας το δημόσιο κλειδί του vIdP. Αυτό το σύστημα βασίζεται στην έννοια των διαπιστευτηρίων βάσει χαρακτηριστικών, όπου η πρόσβαση σε έναν πόρο χορηγείται με βάση την ικανοποίηση ορισμένων πολιτικών που βασίζονται σε χαρακτηριστικά. Συνολικά, το σχήμα απεικονίζει τη διαδικασία διανομής και συνδυασμού μερικών διαπιστευτηρίων από πολλούς IdPs για τη δημιουργία ενός τελικού επαληθεύσιμου διαπιστευτηρίου για πρόσβαση σε πόρους (Σχήμα 16).



Σχήμα 16:Σχήμα OLYMPUS[38]

Στο πλαίσιο της υλοποίησης της εφαρμογής για την πιστοποίηση των ακαδημαϊκών τίτλων σχεδιάστηκαν και υλοποιήθηκαν οι παρακάτω μέθοδοι για να μπορέσει η εφαρμογή να εκδόσει πιστοποιητικά για ακαδημαϊκούς τίτλους, οι οποίοι να μπορούν να πιστοποιηθούν από την εφαρμογή κατάθεσης υποψηφιότητας για μεταπτυχιακό.

1) SignIdentityProof

Το Academic Degree verification system είναι ένα σύστημα που εκδίδει και πιστοποιεί τους τιτλους (7,3,1). Στο σύστημα δημιουργήσαμε μια κλάση "SignIdentityProof" που επεκτείνει μια κλάση με το όνομα "SignIdentityProof" και εφαρμόσαμε την υπογραφή με χαρακτηριστικά(attributes).

Επιπλέον η κλάση έχει δύο μεταβλητές instance: α)υπογραφή (signature), η οποία είναι μια συμβολοσειρά που αναπαριστά την ψηφιακή υπογραφή, και β)data, η οποία είναι ένα αντικείμενο της κλάσης UniAttributes που αναπαριστά διάφορα χαρακτηριστικά που σχετίζονται με τα πανεπιστημιακά στοιχεία.

α) Η υπογραφή είναι μια μεταβλητή String που περιέχει την ψηφιακή υπογραφή που σχετίζεται με τα πανεπιστημιακά στοιχεία. Η ψηφιακή υπογραφή είναι μια κρυπτογραφική τεχνική που χρησιμοποιείται για την επαλήθευση της αυθεντικότητας και της ακεραιότητας ενός ψηφιακού εγγράφου ή μηνύματος. Σε αυτό το πλαίσιο, χρησιμοποιείται για να επαληθεύσει ότι το πτυχίο που σχετίζεται με το αντικείμενο UniAttributes είναι αυθεντικό.

β) Το data(δεδομένα) είναι ένα αντικείμενο της κλάσης UniAttributes που περιέχει διάφορα χαρακτηριστικά που σχετίζονται με τα πανεπιστημιακά στοιχεία. Η κλάση UniAttributes περιέχει πιθανώς μεταβλητές περίπτωσης που αποθηκεύουν το όνομα του κατόχου του πτυχίου, την ημερομηνία γέννησης, το όνομα του πανεπιστημίου, το πτυχίο που απονεμήθηκε και τον αριθμό μητρώου φοιτητή. Το αντικείμενο δεδομένων χρησιμοποιείται για την αναπαράσταση αυτών των πληροφοριών με δομημένο τρόπο, ώστε να είναι εύκολα προσβάσιμες και να χρησιμοποιούνται από άλλα μέρη του προγράμματος.

Ο εικονικός πάροχος ταυτότητας (vIdP)(4a,5) σχηματίζεται με την άθροιση των δημόσιων κλειδιών όλων των μερικών παρόχων ταυτότητας (IdPs), χρησιμοποιώντας ένα ασφαλές πρωτόκολλο υπολογισμού πολλαπλών μερών. Αυτό διασφαλίζει ότι το ιδιωτικό κλειδί του

εικονικού παρόχου ταυτότητας (vIdP) δεν αποκαλύπτεται ποτέ σε κανέναν, ενώ του επιτρέπει να επαληθεύει την αυθεντικότητα των διαπιστευτηρίων που παρέχονται από τον χρήστη(4b).

Ο χρήστης θα δημιουργήσει ένα επαληθεύσιμο διαπιστευτήριο(6a,6b), μπορεί να έχει ευαίσθητα προσωπικά δεδομένα τα οποία δεν θέλει να μοιραστεί απευθείας με τρίτους. Αντ' αυτού, ο χρήστης μπορεί να δημιουργήσει συγκεκριμένα τμήματα αυτών των δεδομένων που είναι κρυπτογραφημένα ή προστατεύονται με άλλο τρόπο(7b,8b) και στη συνέχεια να τα διανείμει σε έναν εικονικό πάροχο ταυτότητας (vIdP)(4b) ή άλλες οντότητες που συμμετέχουν στη διαδικασία δημιουργίας διαπιστευτηρίων.

Επιπλέον ο εικονικός πάροχος ταυτότητας (vIdP) μπορεί στη συνέχεια να χρησιμοποιήσει ένα συγκεντρωτικό δημόσιο κλειδί για να συνδυάσει αυτά τα δεδομένα και να δημιουργήσει ένα τελικό επαληθεύσιμο διαπιστευτήριο που μπορεί να παρουσιαστεί από τον χρήστη για να αποδείξει την ταυτότητά του ή άλλα χαρακτηριστικά. Η προσέγγιση αυτή επιτρέπει μια κατανεμημένη και ελαχιστοποιημένη σε επίπεδο εμπιστοσύνης διαδικασία για τη δημιουργία διαπιστευτηρίων, όπου καμία μεμονωμένη οντότητα δεν έχει πρόσβαση σε όλα τα προσωπικά δεδομένα του χρήστη.

Επίσης η κλάση περιέχει τρεις κατασκευαστές(constructors):α)έναν προεπιλεγμένο κατασκευαστή(empty constructor) που δεν δέχεται ορίσματα, β)έναν κατασκευαστή που δέχεται ένα JSONObject ως όρισμα και αρχικοποιεί τις μεταβλητές, γ)και έναν κατασκευαστή που δέχεται την υπογραφή. Οι παραπάνω κατασκευαστές δημιουργούνε ένα διαπιστευτήριο(token).

1. public SignIdentityProof() {}: Πρόκειται για έναν κατασκευαστή χωρίς όρισμα που δημιουργεί μια νέα περίπτωση της κλάσης SignIdentityProof χωρίς να έχει εκχωρηθεί καμία τιμή στις μεταβλητές instance signature και data. Αυτός ο κατασκευαστής μπορεί να είναι χρήσιμος σε σενάρια όπου πρέπει να δημιουργήσουμε μια περίπτωση της κλάσης χωρίς να καθορίσουμε οποιεσδήποτε αρχικές τιμές.
2. public SignIdentityProof(JSONObject json): Αυτός ο κατασκευαστής δημιουργεί μια νέα περίπτωση της κλάσης SignIdentityProof χρησιμοποιώντας την παράμετρο JSONObject. Αρχικά ανακτά την τιμή της υπογραφής από το αντικείμενο JSON και την αναθέτει στη μεταβλητή περίπτωσης signature. Στη συνέχεια προσπαθεί να αναλύσει το αντικείμενο δεδομένων από το JSON και να δημιουργήσει ένα νέο αντικείμενο UniAttributes με τα περιεχόμενά του. Εάν αυτή η διαδικασία αποτύχει, εκτυπώνει το ίχνος στοίβας της εξαίρεσης(stack trace of the exception). Αυτός ο κατασκευαστής είναι χρήσιμος γιατί έχουμε αντικείμενο JSON που περιέχει πληροφορίες υπογραφής και δεδομένων που πρέπει να δημιουργήσουμε μια περίπτωση SignIdentityProof από αυτό.
3. public SignIdentityProof(String signature, UniAttributes data): Αυτός ο κατασκευαστής (constructor) δημιουργεί μια νέα περίπτωση της κλάσης SignIdentityProof με μια υπογραφή και το αντικείμενο UniAttributes ως παραμέτρους. Αναθέτει την υπογραφή στη μεταβλητή περίπτωσης signature και το αντικείμενο UniAttributes στη μεταβλητή περίπτωσης data. Ο constructor(κατασκευαστής) είναι χρήσιμος όταν έχουμε ήδη την υπογραφή και το αντικείμενο UniAttributes και πρέπει να δημιουργήσομε μια νέα περίπτωση SignIdentityProof από αυτά.

2) Uniatrributes

Υλοποιήθηκε η κλάση "UniAttributes" ώστε να ενσωματωθεί μια απόδειξη ταυτότητας που έχει υπογραφεί από την κλάση "SignIdentityProof" περιέχει χαρακτηριστικά στοιχεία όπως είναι το όνομα του φοιτητή, η ημερομηνία γέννησης, το πτυχίο, και τον αριθμό μητρώου. Ακόμη χρησιμεύει ως αποδεικτικό στοιχείο της ταυτότητας του προσώπου και μπορεί να χρησιμοποιηθεί για την επαλήθευση της ταυτότητάς του όταν απαιτείται. Παρέχει τη διαβεβαίωση στους άλλους ότι οι πληροφορίες που παρουσιάζονται είναι γνήσιες και έχουν επιβεβαιωθεί από το ίδιο το άτομο μέσω της υπογραφής του.

Χρησιμοποιήθηκε η μέθοδος "toString" που επιστρέφει μια αναπαράσταση συμβολοσειράς του αντικειμένου(object) εννοούμε τις τρέχουσες τιμές των μεταβλητών (πεδίων) του αντικειμένου. Με άλλα λόγια, η τρέχουσα κατάσταση ενός αντικειμένου αναφέρεται στις τιμές των χαρακτηριστικών του σε μια συγκεκριμένη χρονική στιγμή.Στην περίπτωση της κλάσης UniAttributes, η κατάσταση του αντικειμένου καθορίζεται από τις τιμές των πεδίων του, όπως name, dateOfBirth, university, awardeddegree και studentid. Επιπλέον χρησιμοποιείται η μέθοδος "toJson" που χρησιμοποιεί την κλάση ObjectMapper για τη μετατροπή του αντικειμένου(object) σε συμβολοσειρά JSON για να μπορεσει να περιεχει την απόδειξη ταυτοτητας.

Επιστρέφει το αλφαριθμητικό "Attributes{}" ακολουθούμενο από ένα χαρακτήρα νέας γραμμής (\n) και ένα χαρακτήρα tab (\t) για λόγους μορφοποίησης. Στη συνέχεια, προσθέτουμε το πεδίο name στη συμβολοσειρά, ακολουθούμενο από ένα κόμμα και άλλη μια νέα γραμμή/tab για μορφοποίηση. Στη συνέχεια κανουμε προσάρτηση το πεδίο dateOfBirth, ακολουθούμενο επίσης από ένα κόμμα και άλλη μια νέα γραμμή/ταμπέλα.Η ίδια διαδικασία επαναλαμβάνεται για τα πεδία university, awardeddegree και studentid, το καθένα ακολουθούμενο από ένα κόμμα και έναν νέο χαρακτήρα γραμμής/tab. Συνολικά, η μέθοδος toString() παράγει ένα όμορφα διαμορφωμένο αλφαριθμητικό που παραθέτει όλα τα πεδία του αντικειμένου και τις τρέχουσες τιμές τους.

Διαθέτει δυο κατασκευαστές (constructors): α) έναν προεπιλεγμένο κατασκευαστή(empty constructor) που δεν δέχεται ορίσματα και β)και ένα που δέχεται παραμέτρους για τα χαρακτηριστικά σε συνδυασμό με την κλάση “SignIdentityProof” αναπαριστά ένα αντικείμενο απόδειξης ταυτότητας που περιλαμβάνει μια υπογραφή και συναφή χαρακτηριστικά. Επεκτείνει την κλάση IdentityProof και περιλαμβάνει ένα πεδίο υπογραφής και ένα πεδίο δεδομένων τύπου

Uniattributes. Η κλάση Uniattributes αναπαριστά χαρακτηριστικά που σχετίζονται με την πανεπιστημιακή ταυτότητα.

Ο πρώτος contructor (κατασκευαστής) είναι ένας προεπιλεγμένος κατασκευαστής που δεν δέχεται ορίσματα. Χρησιμοποιείται για τη δημιουργία μιας περίπτωσης της κλάσης "UniAttributes" με προεπιλεγμένες τιμές για όλες τις μεταβλητές περίπτωσης. Καλείται όταν δημιουργείται ένα αντικείμενο της κλάσης "UniAttributes" χρησιμοποιώντας τη λέξη κλειδί "new" χωρίς να μεταβιβάζονται ορίσματα. Σε αυτόν τον κατασκευαστή, όλες οι μεταβλητές παραδείγματος αρχικοποιούνται στις προεπιλεγμένες τιμές τους, οι οποίες είναι null για τις μεταβλητές συμβολοσειράς και 0 για τις αριθμητικές μεταβλητές.

Τέλος ο δεύτερος constructor (κατασκευαστής) είναι ένας παραμετροποιημένος κατασκευαστής που δέχεται πέντε ορίσματα: "name", "dateOfBirth", "university", "awardeddegree" και "studentid". Χρησιμοποιείται για τη δημιουργία μιας περίπτωσης της κλάσης "UniAttributes" με τις καθορισμένες τιμές για όλες τις μεταβλητές περίπτωσης. Αυτός ο κατασκευαστής καλείται όταν δημιουργείται ένα αντικείμενο της κλάσης "UniAttributes" χρησιμοποιώντας τη λέξη κλειδί "new"(JSONParser parser = new JSONParser();)και περνώντας τις τιμές για όλες τις μεταβλητές στιγμής ως ορίσματα. Σε αυτόν τον κατασκευαστή, οι μεταβλητές περίπτωσης αρχικοποιούνται με τις τιμές των αντίστοιχων ορίων που μεταβιβάζονται στον κατασκευαστή.

3) SignIdentityProver

Η κλάση SignIdentityProof, υλοποιεί τη διεπαφή IdentityProver και αναπαριστά ένα αντικείμενο απόδειξης ταυτότητας που περιέχει μια υπογραφή και τα σχετικά χαρακτηριστικά (Uniattributes). Η κλάση SignIdentityProver είναι υπεύθυνη για την επαλήθευση της εγκυρότητας μιας απόδειξης ταυτότητας και την προσθήκη των σχετικών χαρακτηριστικών στο προφίλ ενός χρήστη που περιέχονται στο « Storage» για ένα δεδομένο όνομα χρήστη(6b).

Η κλάση διαθέτει έναν κατασκευαστή(constructor) που δέχεται ως παράμετρο ένα αντικείμενο Storage. Το αντικείμενο Storage χρησιμοποιείται για την αποθήκευση χαρακτηριστικών που σχετίζονται με τα στοιχεία του χρήστη. Ο constructor (κατασκευαστής) αρχικοποιεί το πεδίο αποθήκευσης, το οποίο είναι μια μεταβλητή της κλάσης, με το παρεχόμενο αντικείμενο Storage. Το αντικείμενο Storage χρησιμοποιείται σε όλη την κλάση για την αποθήκευση και ανάκτηση χαρακτηριστικών που σχετίζονται με ένα όνομα χρήστη(6b).

Επιπλέον η μέθοδος isValid δέχεται ως παραμέτρους το idProof και το username σχετίζεται με το όνομα χρήστη. Το idProof είναι μια συμβολοσειρά JSON που περιέχει τα δεδομένα απόδειξης ταυτότητας που πρέπει να επαληθευτούν. Σε αυτή την υλοποίηση, η συμβολοσειρά idProof αναλύεται σε ένα αντικείμενο JSON και στη συνέχεια μεταβιβάζεται για την επαλήθευση της υπογραφής της απόδειξης. Εάν η υπογραφή είναι έγκυρη, η μέθοδος επιστρέφει true τιμή, διαφορετικά επιστρέφει false τιμή.

Η παράμετρος username είναι μια συμβολοσειρά που προσδιορίζει τον χρήστη του οποίου η ταυτότητα επαληθεύεται. Αυτή η παράμετρος χρησιμοποιείται για την ανάκτηση των χαρακτηριστικών που σχετίζονται με τον χρήστη από το αντικείμενο Storage. Εάν η επαλήθευση του idProof είναι επιτυχής, η μέθοδος επιστρέφει true και τα σχετικά χαρακτηριστικά αποθηκεύονται στο αντικείμενο Storage για μελλοντική χρήση.

Συνολικά, η μέθοδος isValid είναι υπεύθυνη για την επαλήθευση της ταυτότητας ενός χρήστη με βάση το παρεχόμενο idProof και την αποθήκευση των σχετικών χαρακτηριστικών τους στο αντικείμενο Storage.

Η μέθοδος addAttributes δέχεται ως παραμέτρους τα στοιχεία proof και username. Το proof είναι μια συμβολοσειρά JSON που περιέχει τα δεδομένα απόδειξης ταυτότητας. Αυτή η μέθοδος αναλύει την παράμετρο proof σε ένα αντικείμενο SignIdentityProof, εξάγει τα χαρακτηριστικά από το αντικείμενο SignIdentityProof και τα αποθηκεύει.Το αντικείμενο SignIdentityProof περιέχει τα χαρακτηριστικά που σχετίζονται με την απόδειξη ταυτότητας.

Επίσης η παράμετρος username είναι μια συμβολοσειρά που προσδιορίζει τον χρήστη του οποίου η ταυτότητα επαληθεύεται. Αυτή η παράμετρος χρησιμοποιείται για την αποθήκευση των χαρακτηριστικών που σχετίζονται με τον χρήστη στο αντικείμενο Storage. Τα χαρακτηριστικά αποθηκεύονται σε ένα αντικείμενο Map, όπου το κλειδί είναι μια συμβολοσειρά που αντιπροσωπεύει το όνομα του χαρακτηριστικού και η τιμή είναι ένα αντικείμενο Attribute που περιέχει την τιμή του χαρακτηριστικού.Στη μέθοδο addAttributes καλείται η μέθοδος getProof

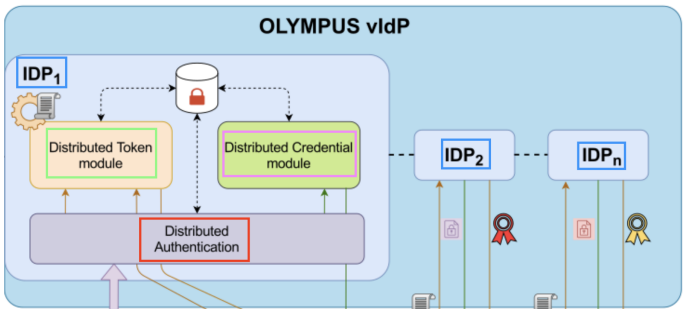
Η μέθοδος getProof λαμβάνει την απόδειξη ως παράμετρο και επιστρέφει ένα αντικείμενο SignIdentityProof αναλύοντας την παράμετρο της απόδειξης χρησιμοποιώντας την κλάση ObjectMapper για να αποκαταστήσει τη συμβολοσειρά JSON σε ένα αντικείμενο SignIdentityProof. Η βιβλιοθήκη χρησιμοποιείται για την αφαίρεση των δεδομένων JSON σε

αντικείμενα Java. Ο ObjectMapper διαβάζει τη συμβολοσειρά απόδειξης και την αντιστοιχίζει στο αντικείμενο SignIdentityProof με βάση τον ορισμό της κλάσης. Εάν η συμβολοσειρά απόδειξης μπορεί να αναλυθεί επιτυχώς σε ένα αντικείμενο SignIdentityProof, η μέθοδος επιστρέφει το αντικείμενο SignIdentityProof. Διαφορετικά, επιστρέφει τιμή null. Αυτή η μέθοδος χρησιμοποιείται στη μέθοδο addAttributes για την εξαγωγή των χαρακτηριστικών που σχετίζονται με την απόδειξη ταυτότητας και την αποθήκευσή τους στο αντικείμενο Storage για μελλοντική χρήση.

4) Vidp(Εικονικός Πάροχος Ταυτότητας)

Στο σύστημα τροποποιήσαμε τους εικονικούς παρόχους ταυτότητας (vIdP) που χρησιμοποιεί ο διακομιστής(Σχήμα). Ο διακομιστής χρησιμοποιεί το πρωτόκολλο P-ABC (Privacy-ABC) και επικοινωνεί με άλλους διακομιστές χρησιμοποιώντας REST (Representational State Transfer) API(Σχήμα 7).

Καθένας από τους VIdPs διαθέτει τρεις ειδικές ενότητες: μία για τον έλεγχο ταυτότητας(μπλέ) και δύο για την έκδοση: Είναι υπεύθυνη για τον έλεγχο του παρεχόμενου ονόματος χρήστη και του κωδικού πρόσβασης με βάση πρωτόκολλα διανομής κλειδιών. Η κατανεμημένη πιστοποίηση ταυτότητας(Distributed Authenticaton)(κόκκινα) συνεργάζεται με τις υπόλοιπες μονάδες ελέγχου ταυτότητας(πράσινο,μωβ) και μόλις ελεγχθεί η εγκυρότητα, ο χρήστης πιστοποιείται στον vIdP(βήμα 3).



Σχήμα 17:Σχήμα OLYMPUS vIdP

Επιπλέον δημιουργεί έναν πάροχο ταυτότητας (IdP) με βάση το Pesto χρησιμοποιώντας το σχήμα P-ABC. Ο πάροχος ταυτότηρας (IdP) είναι υπεύθυνος για την έκδοση και την επαλήθευση των διαπιστευτηρίων για τους χρήστες. Ο κώδικας χρησιμοποιεί μια βάση δεδομένων στη μνήμη για την αποθήκευση των δεδομένων των χρηστών, έναν δοκιμαστικό ελεγκτή ταυτότητας που

αποθηκεύει μια αντιστοίχιση κλειδιού-τιμής των χαρακτηριστικών και μια μονάδα κρυπτογράφησης διακομιστή βασισμένη σε λογισμικό για κρυπτογραφικές λειτουργίες.

Επιπλέον η κύρια μέθοδος διαβάζει το αρχείο διαμόρφωσης είτε από το όρισμα της γραμμής εντολών είτε από τη μεταβλητή περιβάλλοντος CONFIG_FILE. Στη συνέχεια δημιουργεί ένα αντικείμενο PABCIdPImpl (Privacy-ABC Identity Provider Implementation), το οποίο είναι υπεύθυνο για τον χειρισμό των αιτήσεων του πρωτοκόλλου PABC από τους πελάτες. Το αντικείμενο PABCIdPImpl αρχικοποιείται με μια λίστα αντικειμένων IdentityProver, ένα αντικείμενο PestoDatabase, ένα αντικείμενο ServerCryptoModule και άλλες απαραίτητες παραμέτρους.

Στη συνέχεια, το αντικείμενο PABCIdPImpl μεταβιβάζεται σε ένα αντικείμενο RESTIdPServer, το οποίο εκκινεί έναν διακομιστή REST API στην καθορισμένη θύρα. Το αντικείμενο RESTIdPServer είναι υπεύθυνο για τον χειρισμό των αιτήσεων REST API και την προώθησή τους στο αντικείμενο PABCIdPImpl για επεξεργασία.

Το αρχείο ρυθμίσεων περιέχει πληροφορίες σχετικά με την ταυτότητα του διακομιστή, την αποθήκη κλειδιών, την αποθήκη εμπιστοσύνης, τα cookies εξουσιοδότησης και άλλες παραμέτρους που είναι απαραίτητες για τη ρύθμιση του αντικειμένου PABCIdPImpl και του αντικειμένου RESTIdPServer.

5) User Client

Στο σύστημα Academic Degree Verification System, ο πελάτης-χρήστης συμμετέχει στη διαδικασία ελέγχου ταυτότητας, αποστέλλοντας το όνομα χρήστη και τον κωδικό πρόσβασης στον vIdP(βήμα 3), ο χρήστης προστατεύεται μέσω των αρχών της ελάχιστης αποκάλυψης και της έκδοσης κατανεμημένου κρυπτογραφικού υλικού. Η προσέγγιση αυτή παρέχει στον χρήστη συνδεσιμότητα και του επιτρέπει να ανακαλύπτει την ταυτότητα.

Αυτό του επιτρέπει να βρίσκει με ασφάλεια τους εγγεγραμμένους εικονικούς παρόχους ταυτότητας (vIdPs) και τους παρόχους ταυτότητας (IdPs) πριν καν εγγραφεί στην πλατφόρμα. Ομοίως, μπορεί να βρει τους νομίμως εγγεγραμμένους παρόχους υπηρεσιών μαζί με τα δεδομένα που θα χρειαστούν. Αυτό φέρνει τον χρήστη σε πλεονεκτική θέση, καθώς μπορεί να αρχίσει να λαμβάνει αποφάσεις χωρίς να θέτει σε κίνδυνο το απόρρητο ή την ασφάλειά του.

Ο κώδικας του User Client ορίζει μια μέθοδο createUserClient() η οποία επιστρέφει μια περίπτωση του UserClient. Η μέθοδος ξεκινά με τη διάσπαση ενός string servers με κόμμα και την αποθήκευση του προκύπτοντος πίνακα στο serverArray. Στη συνέχεια δημιουργεί μια κενή λίστα idps τύπου PabcIdPRESTConnection.

Η μέθοδος ξεκινά με τη μεταβλητή servers και είναι μια συμβολοσειρά που περιέχει μία ή περισσότερες διευθύνσεις διακομιστών χωρισμένες με κόμμα. Η μέθοδος createUserClient() ξεκινά με το διαχωρισμό αυτού του αλφαριθμητικού σε έναν πίνακα αλφαριθμητικών χρησιμοποιώντας τη μέθοδο split(), περνώντας το χαρακτήρα κόμμα ως διαχωριστικό. Ο προκύπτων πίνακας διευθύνσεων διακομιστών αποθηκεύεται στη συνέχεια σε μια νέα μεταβλητή που ονομάζεται serverArray.

Στη συνέχεια, δημιουργείται μια κενή λίστα τύπου PabcIdPRESTConnection και αποθηκεύεται στη μεταβλητή idps. Αυτή η λίστα θα χρησιμοποιηθεί για την αποθήκευση περιπτώσεων αντικειμένων PabcIdPRESTConnection που θα δημιουργηθούν στον επόμενο βρόχο.

Στη συνέχεια, η μέθοδος θέτει ορισμένες ιδιότητες του συστήματος που σχετίζονται με το SSL truststore συγκεκριμένα, η ιδιότητα javax.net.ssl.trustStore καθορίζει τη διαδρομή προς ένα αρχείο που περιέχει αξιόπιστα πιστοποιητικά και η ιδιότητα javax.net.ssl.trustStorePassword καθορίζει τον κωδικό πρόσβασης στο truststore. Επιπλέον πραγματοποιεί βρόχους σε κάθε διακομιστή στο serverArray για να δημιουργήσει ένα αντικείμενο PabcIdPRESTConnection με τη διεύθυνση του διακομιστή, ένα κενό αλφαριθμητικό, έναν δείκτη i και ένα χρονικό όριο 100000 χιλιοστών του δευτερολέπτου. Κάθε αντικείμενο PabcIdPRESTConnection προστίθεται στη λίστα idps.

Δημιουργεί έναν χάρτη publicKeys τύπου Map<Integer, MSverfKey> και τον συμπληρώνει με τα δημόσια κλειδιά από κάθε αντικείμενο PabcIdPRESTConnection στη λίστα idps. Επιπλέον ανακτά τις δημόσιες παραμέτρους του πρώτου αντικειμένου PabcIdPRESTConnection στη λίστα idps και δημιουργεί ένα αντικείμενο PSCredentialManagement με αυτό, τον χάρτη publicKeys και έναν seed.

Ακόμη δημιουργεί ένα αντικείμενο SoftwareClientCryptoModule με ένα αντικείμενο Random και το modulus του δημόσιου κλειδιού του πρώτου αντικειμένου PabcIdPRESTConnection στη λίστα idps. Κατασκευάζεται ένα αντικείμενο PabcClient με τη λίστα idps, το αντικείμενο

credentialManagement και το αντικείμενο cryptoModule. Δημιουργεί επίσης ένα αντικείμενο PSPABCVerifier και το ρυθμίζει με τη λίστα idps και τον seed.

Τέλος η περίπτωση credentialManagement δημιουργείται χρησιμοποιώντας την κλάση PSCredentialManagement, η οποία είναι μια υλοποίηση της διεπαφής CredentialManagement. Η κλάση PSCredentialManagement χρησιμοποιείται για τη διαχείριση των διαπιστευτηρίων με τρόπο που διατηρεί την ιδιωτικότητα χρησιμοποιώντας το σύστημα διαπιστευτηρίων P-ABC (Privacy-ABC).

Ο κατασκευαστής (constructor) της κλάσης PSCredentialManagement λαμβάνει δύο παραμέτρους: μια boolean τιμή που υποδεικνύει αν θα χρησιμοποιηθεί ένα offline ή online πρωτόκολλο για την έκδοση διαπιστευτηρίων και μια υλοποίηση της διεπαφής CredentialStorage που χρησιμοποιείται για την αποθήκευση των διαπιστευτηρίων του χρήστη.

Στη συνέχεια καλείται η μέθοδος setup() της PSCredentialManagement με τις παραμέτρους publicParam, publicKeys και seed. Αυτή η μέθοδος αρχικοποιεί το σύστημα διαχείρισης διαπιστευτηρίων με τη δημιουργία ενός εκδότη P-ABC και την έκδοση ενός νέου συνόλου διαπιστευτηρίων για τον χρήστη. Η παράμετρος publicParam είναι οι δημόσιες παράμετροι του συστήματος διαπιστευτηρίων P-ABC, ενώ η παράμετρος publicKeys είναι ένας χάρτης των κοινών δημόσιων κλειδιών του IdP (όπως εξηγήθηκε προηγουμένως). Η παράμετρος seed είναι ένας κρυπτογραφικός σπόρος που χρησιμοποιείται για τη δημιουργία του ιδιωτικού κλειδιού του χρήστη.

Συνοπτικά, η περίπτωση credentialManagement αναπαριστά ένα σύστημα διαχείρισης διαπιστευτηρίων με διατήρηση της ιδιωτικότητας που βασίζεται στο σχήμα P-ABC και χρησιμοποιείται για τη διαχείριση και την έκδοση διαπιστευτηρίων χρηστών με ασφαλή και διατηρώντας την ιδιωτικότητα.

Επιπλέον Δημιουργήθηκε η μέθοδος storage() δημιουργεί ένα νέο αντικείμενο Storage, το οποίο είναι μια κλάση που αντιπροσωπεύει την αποθήκευση των διαπιστευτηρίων ενός χρήστη. Στη συνέχεια, δημιουργείτε ένα Map από String keys και Attribute values, το οποίο αντιπροσωπεύει τα χαρακτηριστικά ενός διαπιστευτηρίου που θέλει να αποθηκεύσει ο χρήστης. Στη συνέχεια, συμπληρώνετε το Map με τέσσερα χαρακτηριστικά: "name", "university", "awardeddegree" και

"studentid". Κάθε χαρακτηριστικό αντιπροσωπεύεται από ένα νέο αντικείμενο Attribute και συσχετίζεται με το αντίστοιχο κλειδί του στο Map.

Τέλος καλείται μέθοδος storeCredential() του αντικειμένου Storage, περνώντας το διαπιστευτήριο που πρόκειται να αποθηκευτεί. Αφού αποθηκευτεί το διαπιστευτήριο, καλείται η μέθοδος checkCredential() του αντικειμένου Storage. Αυτή η μέθοδος ελέγχει αν το αποθηκευμένο διαπιστευτήριο μπορεί να ανακτηθεί και αν είναι έγκυρο.

6) Τρίτο μέρος(Relying Party)

Το τρίτος μέρος προστατεύει την πρόσβαση σε μια σειρά πόρων ή υπηρεσιών. Ο κύριος σκοπός του είναι να παράγει τις πολιτικές πρόσβασης που θα πρέπει να ικανοποιεί ο χρήστης για να έχει πρόσβαση στην υπηρεσία(βήμα 1,2). Ο χρήστης θα πρέπει να συμφωνήσει με την πολιτική και να δώσει τη συγκατάθεσή του για την αποκάλυψη των χαρακτηριστικών(βήμα 2).

Το τρίτο μέρος αναλαμβάνει το ρόλο του επαληθευτή(Verifier), οπότε πρέπει να επικυρώσει τα υπογεγραμμένα διακριτικά πρόσβασης που παρουσιάζει ο χρήστης(βήμα 7a, 9a).Η διαδικασία αυτή περιλαμβάνει δύο βασικά στοιχεία: α)τον επαληθευτή(Verifier) και β)την πολιτική(Policy).

Για τον επαληθευτή(Verifier), η μόνη σύνδεση που απαιτείται να δημιουργηθεί με τον εικονικό πάροχο (vIdP) πραγματοποιείται στη φάση εγκατάστασης, για την απόκτηση των απαραίτητων πληροφοριών (δημόσιο κλειδί, παράμετροι pabc κ.λπ.) που θα χρησιμοποιηθούν κατά την επαλήθευση. Η ίδια η διαδικασία επαλήθευσης εκτελείται μέσα στην εφαρμογή του επαληθευτή, χρησιμοποιώντας το κατάλληλο στοιχείο επαλήθευσης, οπότε δεν απαιτείται επικοινωνία με τον εικονικό πάροχο (vIdP) για τη διαδικασία αυτή.

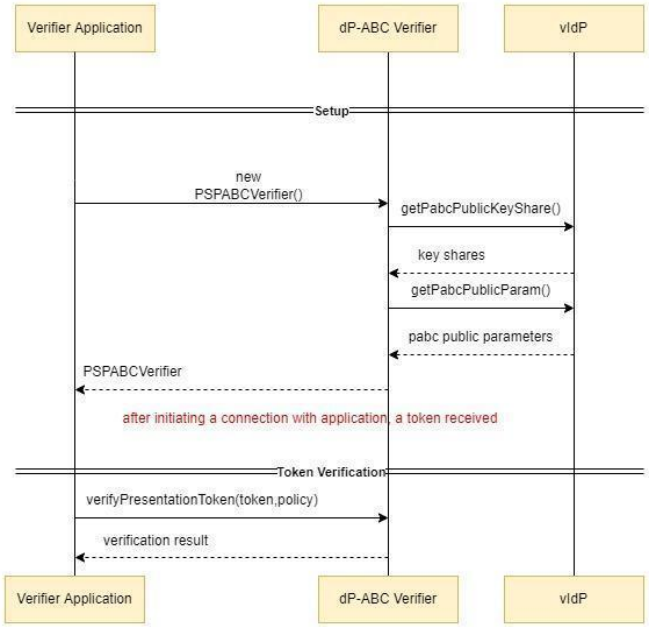
Η επικοινωνία με τον vIdP γίνεται απευθείας από την εφαρμογή επαλήθευσης, η οποία στη συνέχεια μεταβιβάζει το δημόσιο κλειδί που έλαβε στο στοιχείο επαλήθευσης, προκειμένου να ολοκληρωθεί η διαδικασία εγκατάστασης.

Η εφαρμογή επαλήθευσης εκκινεί τη συνιστώσα dP-ABC Verifier, η οποία ζητά το δημόσιο κλειδί P-ABC και τις δημόσιες παραμέτρους από τον vIdP κατά τη φάση εγκατάστασης. Για τη φάση επαλήθευσης, η εφαρμογή επαλήθευσης αποστέλλει το διακριτικό ελέγχου ταυτότητας απευθείας στον dP-ABC Verifier (Σχήμα 8). Αυτά τα στοιχεία χειρίζονται τη διαδικασία επαλήθευσης και διαβιβάζουν το αποτέλεσμα πίσω στην εφαρμογή επαλήθευσης.

Επιπλέον ο επαληθευτής (Verifier) είναι υπεύθυνος για την επαλήθευση της εγκυρότητας των υποβαλλόμενων διακριτικών πρόσβασης (συμπεριλαμβανομένου του ελέγχου των υπογραφών) και για το αν τα εν λόγω διακριτικά είναι κατάλληλα για μια δεδομένη πολιτική πρόσβασης.

Δημιουργεί πρώτα μια λίστα αντικειμένων PabcIdPRESTConnection, καθένα από τα οποία αντιπροσωπεύει μια σύνδεση με έναν διαφορετικό πάροχο ταυτότητας (IdP). Ο αριθμός των παρόχων ταυτότητας (IdPs) και οι αντίστοιχες θύρες τους καθορίζονται από τις μεταβλητές serverCount και ports, αντίστοιχα. Κάθε σύνδεση IdP αρχικοποιείται με ένα cookie διαχειριστή και μια τιμή χρονικού ορίου.

Στη συνέχεια, δημιουργείται ένα αντικείμενο PSPABCVerifier και ρυθμίζεται ώστε να χρησιμοποιεί τους παρόχους υπηρεσιών (IdPs), που καθορίζονται από τη λίστα των αντικειμένων PabcIdPRESTConnection και και επαληθεύει ότι ένα τυχαιοποιημένο διαπιστευτήριο είναι έγκυρο. Στον επαληθευτή δίνεται επίσης μια τιμή που χρησιμοποιείται για τη δημιουργία κλειδιών για το σχήμα P-ABC.



Σχήμα 18: Verifier Application

Μια πολύ σημαντική διεπαφή που χρησιμοποιείται κατά τη διαδικασία επαλήθευσης είναι η σύνδεση μεταξύ του Academic Degrees Verification System και του επαληθευτή(Verifier). Προκειμένου να γίνει η επαλήθευση, ο επαληθευτής(Verifier) πρέπει να δημιουργήσει μια

σύνδεση με το Academic Degrees Verification System που περιέχει τα απαραίτητα δεδομένα. Όταν επιτευχθεί αυτό, οι δύο συσκευές είναι έτοιμες να ανταλλάξουν δεδομένα. Στη εφαρμογή ο επαληθευτής(Verifier) πρέπει να στείλει την πολιτική(policy) στον κάτοχο, οπότε αυτός θα την προωθήσει στον εικονικό πάροχο (vIdP) και θα ζητήσει ένα διαπιστευτήριο (token) που συμμορφώνεται με τους κανόνες της εν λόγω πολιτικής .

Η πολιτική(policy) Περιέχει ένα σύνολο πολιτικών, οι οποίες μπορεί να περιγράφονται μέσω JSON ή XML, που ορίζονται για μια συγκεκριμένη υπηρεσία ή υπηρεσίες. Δηλαδή, συγκεκριμένα χαρακτηριστικά του χρήστη, τη μορφή τους και τα χαρακτηριστικά που θα ζητηθούν. Η αλληλεπίδραση μεταξύ των εφαρμογών φαίνεται στο ακόλουθο Σχήμα (Σχήμα 9).

Σχήμα 19: Διασύνδεση του συστήματος Academic Degree Verification System και της εφαρμογής επαλήθευσης (Verifier)

3.5.1 Εφαρμογή Πιστοποίησης Ακαδημαϊκών Τίτλων με Χρήση Blockchain και Προστασία Προσωπικών Δεδομένων

Το Academic Degree Verification System είναι ένα σύστημα για την επαλήθευση των ακαδημαϊκών προσόντων των χρηστών. Η εφαρμογή βασίζεται σε ένα σύστημα πολλαπλών υπογραφών, το οποίο καθιστά πολύ δύσκολο να παραποιηθεί ή να πλαστογραφηθεί ένα πιστοποιητικό. Έχουν δημιουργηθεί δύο πιλοτικά σενάρια, ένα για desktop και ένα για κινητές συσκευές.

α) Πιλοτικό σενάριο για desktop

Ο χρήστης εισάγει τα στοιχεία του πτυχίου του στην εφαρμογή, η οποία στη συνέχεια επαληθεύει τα στοιχεία αυτά με τα στοιχεία που είναι αποθηκευμένα στη βάση δεδομένων τις . Εάν τα στοιχεία επαληθευτούν, η εφαρμογή εκδίδει ένα πιστοποιητικό για το πτυχίο του χρήστη.

β) Πιλοτικό σενάριο για κινητές συσκευές

Ο χρήστης εγκαθιστά την εφαρμογή στη κινητή συσκευή του και στη συνέχεια εισάγει τα στοιχεία του στην εφαρμογή. Η εφαρμογή επαληθεύει τα στοιχεία αυτά με τα στοιχεία που είναι αποθηκευμένα στη βάση δεδομένων της εφαρμογής. Εάν τα στοιχεία επαληθευτούν, η εφαρμογή εκδίδει ένα πιστοποιητικό για το πτυχίο του χρήστη, το πιστοποιητικό αυτό μπορεί να αποθηκευτεί στη συσκευή του χρήστη.

Και τα δύο πιλοτικά σενάρια έχουν σχεδιαστεί για να διευκολύνουν τους χρήστες να επαληθεύσουν τα ακαδημαϊκά τους προσόντα , και παρουσιάζονται αναλυτικά στο Κεφάλαιο 4 (για desktop) και στο Κεφάλαιο 5(για mobile)

3.6 Βασική Ροή Εφαρμογής

Η Εφαρμογή ξεκινάει

- ✓ Event 1

Ο ενδιαφερόμενος φοιτητής επισκέπτεται τη γραμματεία του πανεπιστημίου με τη ταυτότητα του για να δηλώσει το ενδιαφέρον για το σύστημα ψηφιακής πιστοποίησης. Οι πληροφορίες εισάγονται στο σύστημα επαλήθευσης Academic Degree Verification System και ο χρήστης λαμβάνει έναν κωδικό μιας χρήσης (OTP) που μπορεί να χρησιμοποιηθεί για την ενεργοποίηση του λογαριασμού του.

- ✓ Event 2

Ο φοιτητής επισκέπτεται την διαδικτυακή εφαρμογή Academic Degree Verification System και συνδέεται χρησιμοποιώντας τον OTP για να οριστικοποιήσει την εγγραφή του.

- ✓ Event 3

Ο χρήστης καλείται να αλλάξει τον OTP της σε έναν ασφαλή κωδικό πρόσβασης για περαιτέρω χρήση.

- ✓ Event 4

Για αυξημένη ασφάλεια, ο χρήστης επιλέγει έναν κωδικό πρόσβασης ο οποίος απαιτείται για την πρόσβαση σε οποιαδήποτε τοπικά αποθηκευμένη πληροφορία, όπως το μυστικό κλειδί χρήστη

που δημιουργήθηκε προηγουμένως. Το υλικό του μυστικού κλειδιού του χρήστη παράγεται και αποθηκεύεται.

- ✓ Event 5

Ο χρήστης πιστοποιείται από την διαδικτυακή εφαρμογή και ανακατευθύνεται στην πύλη αιτήσεων.

- ✓ Event 6

Ο χρήστης προσθέτει τις πληροφορίες και τα δεδομένα της αίτησής του, όπως, π.χ., αίτηση διδακτορικών σπουδών και βιογραφικό σημείωμα

Η πύλη υποβολής αιτήσεων προσφέρει τη δυνατότητα προσθήκης ακαδημαϊκών πτυχίων. Ως εκ τούτου, ο χρήστης προσδιορίζει το πανεπιστήμιο έκδοσης και τον τύπο του πτυχίου. Χρησιμοποιώντας τα αποθηκευμένα διαπιστευτήριά της, η εφαρμογή υπολογίζει στη συνέχεια μια κρυπτογραφική απόδειξη ότι ο χρήστης είναι πράγματι κάτοχος του συγκεκριμένου πτυχίου και τη μεταφορτώνει στον διακομιστή, μπορεί να αρκούν διαφορετικές πληροφορίες για την αίτηση (π.χ. μπορεί να μην απαιτείται η ημερομηνία έκδοσης ή ορισμένοι βαθμοί).

Η πύλη υποβολής αιτήσεων επαληθεύει το ληφθέν διακριτικό παρουσίασης και προσθέτει το πτυχίο του χρήστη, εάν ο έλεγχος ήταν θετικός- σε αντίθετη περίπτωση, το δηλωθέν στοιχείο δεν γίνεται δεκτό.

- ✓ Τέλος της περίπτωσης χρήσης

Κεφάλαιο 4ο

Ο σκοπός αυτού του κεφαλαίου είναι να παρουσιάσει την εφαρμογή διαχείρισης χρηστών για την πιστοποίηση ακαδημαϊκών τίτλων με βάση την τεχνολογία blockchain, η οποία διασφαλίζει την προστασία των προσωπικών δεδομένων των χρηστών. Η εφαρμογή αποτελείται από τη διαδικτυακή πλατφόρμα όπου οι χρήστες θα μπορούν να υποβάλουν αιτήσεις για την πιστοποίηση των ακαδημαϊκών τους τίτλων. Η πλατφόρμα βασίζεται στην τεχνολογία blockchain, η οποία θα διασφαλίζει την ασφάλεια και την εμπιστευτικότητα των δεδομένων των χρηστών.

Το παρών κεφάλαιο χωρίζεται σε πέντε κύρια τμήματα, το πρώτο τμήμα παρέχει μια εισαγωγή στο θέμα της διαχείρισης ταυτότητας και της πιστοποίησης ακαδημαϊκών τίτλων. Το δεύτερο τμήμα παρουσιάζει την αρχιτεκτονική της εφαρμογής, συμπεριλαμβανομένης της χρήσης της τεχνολογίας blockchain. Το τρίτο τμήμα αποτελείται από τα πλεονεκτήματα της χρήσης της τεχνολογίας blockchain για την εφαρμογή αυτή. Στο τέταρτο τμήμα παρουσιάζεται η αρχιτεκτονική του πιλοτικού προγράμματος που πραγματοποιήθηκε. Το πέμπτο και τελευταίο τμήμα είναι τα συμπεράσματα και οι προοπτικές της εφαρμογής αυτής.

4.0 Εφαρμογή διαχείρισης χρηστών για την πιστοποίηση ακαδημαϊκών τίτλων

Οι προηγμένες τεχνικές κρυπτογράφησης που χρησιμοποιεί η βιβλιοθήκη OLYMPUS[38] επιτρέπουν τη μετάβαση από ένα κεντρικοποιημένο σε ένα κατανεμημένο μοντέλο παρόχου ταυτότητας (IdP). Οι εργασίες κατανέμονται μεταξύ των IdPs που λειτουργούν συλλογικά ως εικονικό πάροχος ταυτότητας (Virtual Identity Provider (vIdP)). Μόνο με την παραβίαση όλων των παρόχων ταυτότητας (IdPs) θα ήταν δυνατόν να παραβιαστεί η ακεραιότητα του συστήματος. Η κρυπτοβιβλιοθήκη παρέχει κατανεμημένο έλεγχο ταυτότητας χρήστη και κωδικού πρόσβασης για να λειτουργεί με τη χρήση του διαδικτύου. Σε αυτή την περίπτωση η κρυπτοβιβλιοθήκη συμπεριφέρεται σαν ένα σύστημα P-ABC, όπου ο χρήστης μπορεί να αποκτήσει ένα

διαπιστευτήριο για να αντλήσει διαπιστευτήρια πρόσβασης αργότερα χωρίς να χρησιμοποιήσει τον πάροχο ταυτότητας και πάλι.

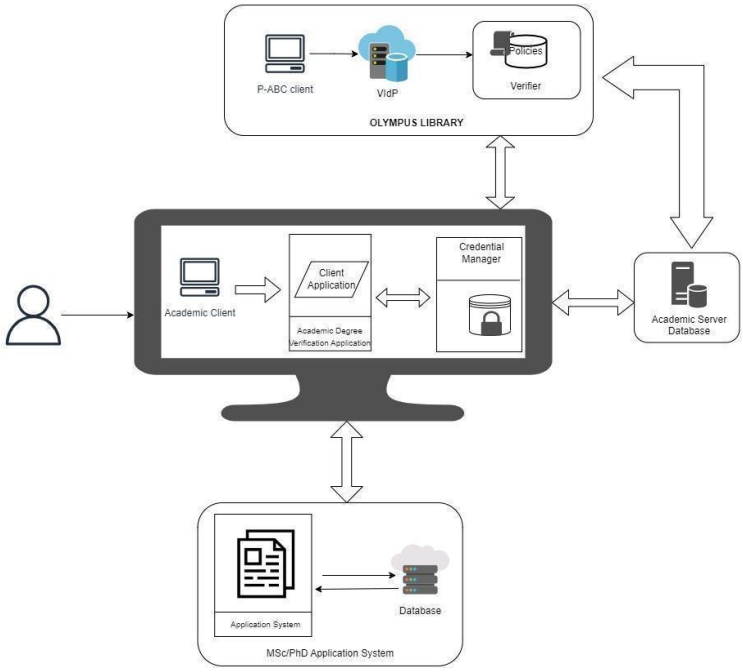
Για το σενάριο μας (Academic Degree Verification System) θα περιγράψουμε τα στάδια που αφορούν για την υλοποίηση του πιλοτικού προγράμματος που βασίζεται στα διαπιστευτήρια P-ABC όπου χρησιμοποιείται ένα σύστημα πολλαπλών υπογραφών. Κάθε πάροχος ταυτότητας (IdP) υπογράφει τα χαρακτηριστικά χρήστη (με το κλειδί του που δημιουργείται ανεξάρτητα), δημιουργώντας ένα κοινόχρηστο στοιχείο διαπιστευτηρίων του οποίου η λειτουργικότητα είναι ισοδύναμη με ένα διαπιστευτήριο που εκδίδεται από ένα μόνο πάροχο ταυτότητας (IdP).

Τέλος θα περιγράψουμε την αρχιτεκτονική συστήματος και στη δεύτερη φάση την εγκατάσταση της εφαρμογής και πώς τα διαπιστευτήρια (δηλαδή οι εγγραφή των φοιτητών, η πιστοποίηση κ.α) λαμβάνονται. Θα παρουσιάσουμε επίσης τα βήματα που πρέπει να ακολουθήσει ένας φοιτητής για να εγγραφεί, να πιστοποιήσει τα διαπιστευτήρια, να δημιουργήσει και να υποβάλει αίτηση για την απόκτηση μεταπτυχιακού ή διδακτορικού τίτλου σπουδών.

4.1 Διεπαφές

Η εφαρμογή του συστήματος Academic Degree Verification System τόσο για το φοιτητή και τόσο για τον επαληθευτή(Verifier) πρέπει να επικοινωνούν με τον εικονικό πάροχο ταυτότητας (vIdP). Από την πλευρά του φοιτητή, είναι απαραίτητο να δημιουργηθεί ένας λογαριασμός στον εικονικό πάροχο ταυτότητας (vIdP), ο οποίος περιλαμβάνει τις προσωπικές πληροφορίες του φοιτητή, οι οποίες θα είναι διαθέσιμες για επαλήθευση.

Επιπλέον, υπάρχει ανάγκη να δημιουργηθεί ένα διαπιστευτήριο (token), το οποίο θα δημιουργηθεί κατά τον έλεγχο ταυτότητας. Αυτό είναι δυνατό με τη χρήση του πελάτη P-ABC, το οποίο μπορεί να αποθηκεύσει τα διαπιστευτήρια που λαμβάνονται από τον εικονικό πάροχο ταυτότητας (vIdP) κατά την εγγραφή και να τα χρησιμοποιεί αργότερα για τη δημιουργία διαπιστευτηρίων για συγκεκριμένες πολιτικές. Από την πλευρά του επαληθευτή (Verifier), η μόνη σύνδεση που πρέπει να δημιουργηθεί με τον εικονικό πάροχο ταυτότητας (vIdP), είναι κατά τη διαδικασία ρύθμισης για να μπορέσει να χρησιμοποιηθεί (σχήμα 20).



Σχήμα 20:Διεπαφή για τοAcademic Degree Verification System

4.2.1 Academic Degree Verification System Issuance

Για το πιλοτικό σενάριο, η εφαρμογή Academic Degree Verification System συνδέεται με τους τρεις παρόχους ταυτότητας (IdPs) μέσω των διεπαφών πελάτη P-ABC[40], ενώ η εφαρμογή επαλήθευσης χρησιμοποιεί τη διεπαφή επαλήθευσης για να συνδεθεί με τον εικονικό πάροχο ταυτότητας (vIdP). Αυτές οι δύο διεπαφές παρέχουν όλες τις απαιτούμενες λειτουργίες και είναι σε θέση να εκτελέσουν την εγγραφή φοιτητών, την έκδοση διαπιστευτηρίων και την επαλήθευση τους.

4.2.2 Academic Degree Verification System

Για το διαδικτυακό σενάριο, υλοποιήθηκαν δύο διαδικτυακές εφαρμογές σύμφωνα με την κρυπτοβιβλιοθήκη OLYMPUS, το Academic Degree Verification System και ο Verifier. Υλοποιήθηκαν με τέτοιο τρόπο ώστε όταν η εφαρμογή ξεκινάει, να εκκινεί την εφαρμογή Verifier όταν αποστέλλεται το διαπιστευτήριο.

Με την διαδικτυακή εφαρμογή Academic Degree Verification System, όλοι οι φοιτητές που έχουν αποφοιτήσει ή κατέχουν έγκυρο τίτλο από το πανεπιστήμιο μπορούν να εγγραφούν στην διαδικτυακή εφαρμογή Academic Degree Verification System , η διαδικτυακή εφαρμογή πρέπει να είναι σε σύνδεση με το διαδίκτυο κατά τη διάρκεια της εγγραφής.

Επίστης όταν ένας φοιτητής έχει αποφοιτήσει ή έχει αποκτήσει έναν ακαδημαϊκό τίτλο, τότε η γραμματεία του τμήματος εισάγει τα στοιχεία των φοιτητών στη βάση δεδομένων μας και δημιουργεί έναν κωδικό πρόσβασης μίας χρήσης (OTP) για την εγγραφή. Ο υπάλληλος της γραμματείας μπορεί να έχει πρόσβαση στην διαδικτυακή εφαρμογή Academic Degree Verification System μέσω κωδικού πρόσβασης και να συμπληρώσει τα στοιχεία του φοιτητή και να αποθηκεύσει στη βάση δεδομένων μας. Επίσης, μπορεί να διαμορφώσει και να αποθηκεύσει το κωδικό πρόσβασης μιας χρήσης(OTP) για κάθε φοιτητή για τη διαδικασία εγγραφής .

Οι φοιτητές ολοκληρώνουν τη φάση επαλήθευσης με επιτυχία, μπορούν να έχουν πρόσβαση μέσω του κωδικού μια χρήσης. Ο εγγεγραμμένος φοιτητής μπορεί να συνδεθεί και να αλλάξει τον κωδικό πρόσβασής. Μετά την επιτυχή αλλαγή του κωδικού πρόσβασης είναι σε θέση να συνδεθεί και να δει τις προσωπικές πληροφορίες, εμφανίζεται μια ειδοποίηση στη διεπαφή χρήστη- το

σύστημα που παρέχει μια συνοπτική πολιτική απορρήτου για τον χρήστη και μπορεί να δει τις προσωπικές του πληροφορίες.

Επιπλέον, εάν ο φοιτητής έχει εγγραφεί επιτυχώς, μπορεί να εκδοθεί διαπιστευτήριο P-ABC για τον ακαδημαϊκό του τίτλο, αποκτώντας πρόσβαση στην εφαρμογή χρησιμοποιώντας τον κωδικό πρόσβασής του. Μπορεί να ζητήσει να λάβει τα διαπιστευτήριά του P-ABC από το εικονικό πάροχο ταυτότητας (vIdP). Ο φοιτητής που κατέχει έναν τίτλο μεταπτυχιακού επιπέδου, μπορεί να εκδώσει διαπιστευτήριο p-ABC και εμφανίζεται μια ειδοποίηση στον χρήστη, το σύστημα παρέχει μια ειδοποίηση για τον χρήστη όπου μπορεί να δει τα διαπιστευτήρια που εκδόθηκαν (Εικόνα).

Ο φοιτητής έχει ολοκληρώσει επιτυχώς το τα δύο προαναφερθέντα βήματα, μπορεί να προχωρήσει στην υποβολή της αίτησής του, σε ένα πρόγραμμα MSc ή PhD. Ο φοιτητής συμπληρώνει την αίτηση στην εφαρμογή υποβολής αιτήσεων και ανεβάζει ανώνυμο βιογραφικό σημείωμα. Εάν ο φοιτητής διαθέτει έγκυρα διαπιστευτήρια για ένα μεταπτυχιακό τίτλο σπουδών από το Πανεπιστήμιο Ιωαννίνων και μπορεί να χρησιμοποιήσει τα διαπιστευτήριά της P-ABC για να επαληθεύσει.

Ο φοιτητής ανακατευθύνεται στην Academic Degree Verification System και συνδέεται για να επαληθεύσει τον τίτλο. Η διαδικτυακή εφαρμογή υποστηρίζει επίσης τη διαγραφή του τίτλου σπουδών με τη χρήση drag and drop. Η επιλογή αυτή δίνεται επειδή ο φοιτητής μπορεί να αποφασίσει να το διαγράψει και να μην συνεχίσει στην εφαρμογή. Από την άλλη πλευρά, εάν αποφασίσει να συνεχίσει και το διαπιστευτήριο που ανέβασε έχει επαληθευτεί επιτυχώς από το Πανεπιστήμιο, τότε ένα διαπιστευτήριο (token) για την υποστηριζόμενη πολιτική θα δημιουργηθεί και θα προωθηθεί στον Επαληθευτή (verifier).

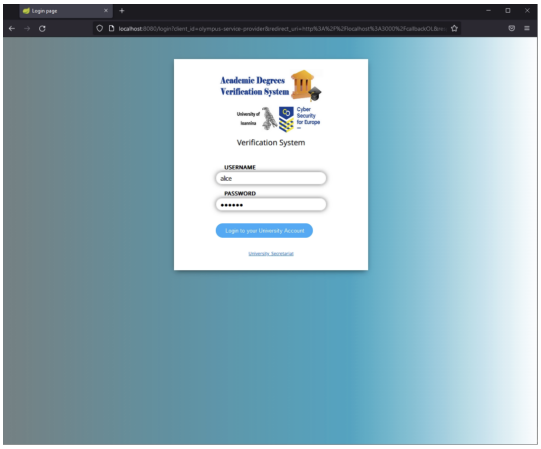
Τέλος, ο φοιτητής επιστρέφει στη φόρμα και μπορεί να προχωρήσει στην υποβολή της αίτησης διδακτορικής του διατριβής και μπορεί να επανεξετάσει την υποβολή.Στην οθόνη θα εμφανιστούν τα επαληθευμένα στοιχεία του τίτλου που κατέχει και μια ειδοποίηση επιτυχούς υποβολής. Στο τέλος, ο φοιτητής μπορεί να συνδεθεί και να δει τις υποβολές (MSc, PhD) και μπορεί να διαγράψει ή να τις αναθεωρήσει.

4.3 Εγκατάσταση συστήματος

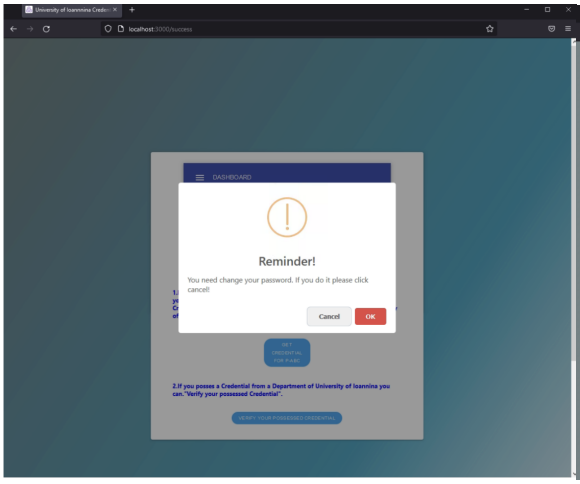
Η παρούσα ενότητα περιγράφει τη διαδικασία για τη δημιουργία της πιλοτικής διαδικτυακής εφαρμογής. Η φάση εγκατάστασης αποτελείται από τα παρακάτω βήματα. Το Academic Degree Verification System πρέπει να έχει ενεργή σύνδεση στο διαδίκτυο κατά τη φάση της εγγραφής. Όταν ένας φοιτητής έχει αποφοιτήσει ή έχει κατέχει έναν ακαδημαϊκό τίτλο, τότε η γραμματεία του τμήματος εισάγει τα στοιχεία των φοιτητών στη βάση δεδομένων μας και δημιουργεί κωδικό μια χρήσης (One Time Password) για την εγγραφή (Εικόνα 1).

Εικόνα 1:Διαδικασία εγγραφής

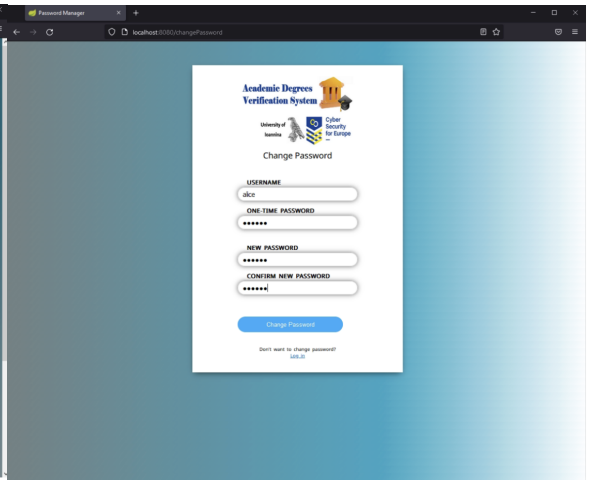
Το επόμενο βήμα για διαδικασία εγγραφής πραγματοποιείται από τον φοιτητή. Κάθε φοιτητής πρέπει να επισκεφθεί τη γραμματεία του τμήματος για να λάβει τον κωδικό μια χρήσης (OTP). Ο φοιτητής πρέπει να επιδείξει τη φοιτητική του ταυτότητα για να επαληθευτεί από τον υπάλληλο της γραμματείας. Αρχικά, ο φοιτητής πρέπει να χρησιμοποιήσει τον κωδικό μια χρήσης (OTP) που έλαβε από την γραμματεία του τμήματος προκειμένου να συνδεθεί στο Academic Degree Verification System (Εικόνα 2). Ο εγγεγραμμένος φοιτητής μπορεί να συνδεθεί και να αλλάξει τον κωδικό πρόσβασής(Εικόνα 3,4).Επιπλέον, ο η εγγραφή θεωρείται επιτυχής όταν ο φοιτητής μπορεί να εκδοθεί ένα διαπιστευτήριο P-ABC για τον ακαδημαϊκό του τίτλο (Εικόνα 5).



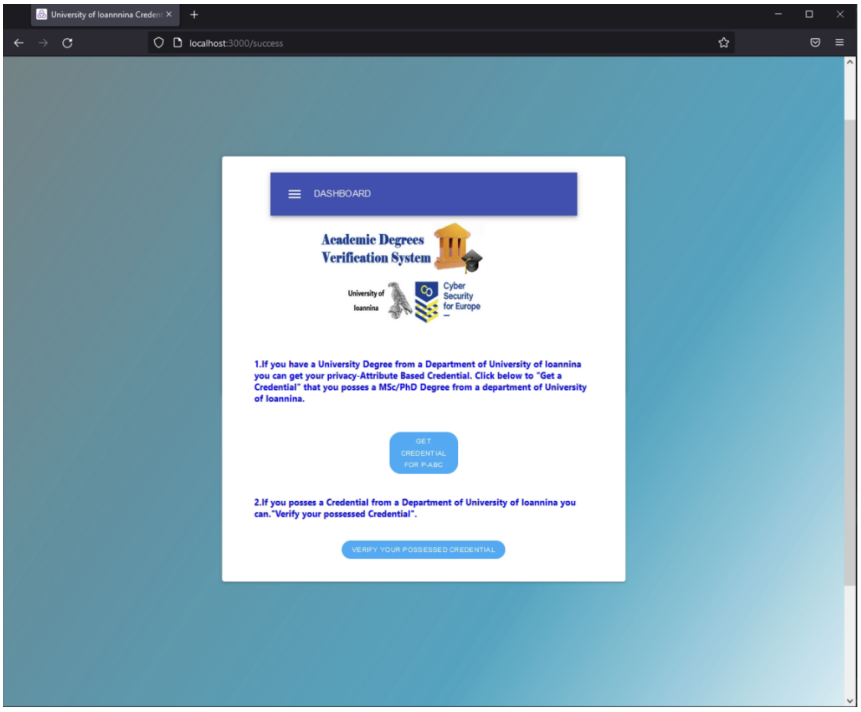
Εικόνα 2:Πρόσβαση μέσω OTP



Εικόνα 3:Υπενθύμιση για αλλαγή κωδικού



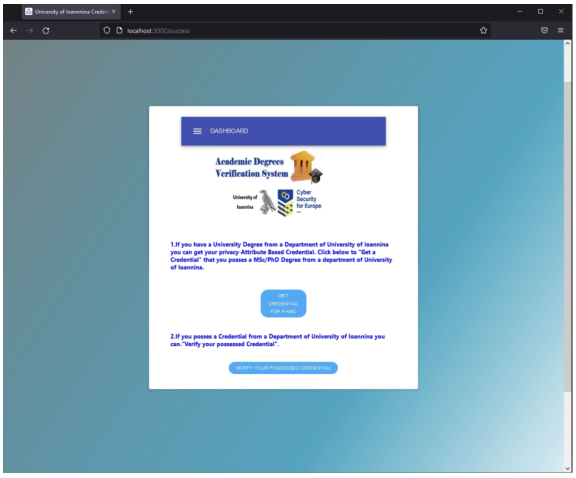
Εικόνα 4:Αλλαγή κωδικού



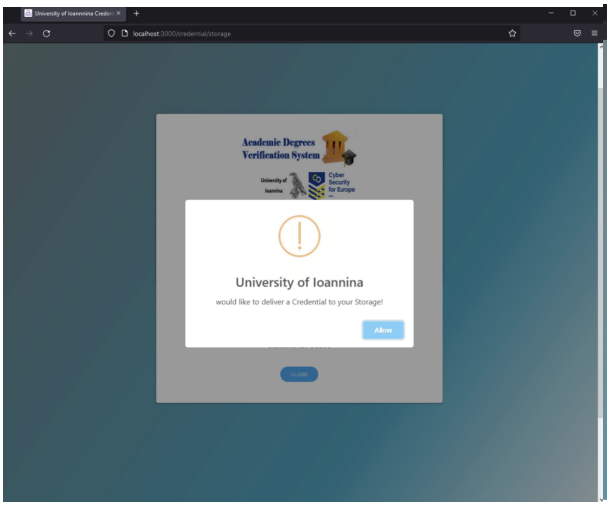
Εικόνα 5:Πρόσβαση στο περιβάλλον εφαρμογής

4.4 Απόκτηση πανεπιστημιακού διαπιστευτηρίου

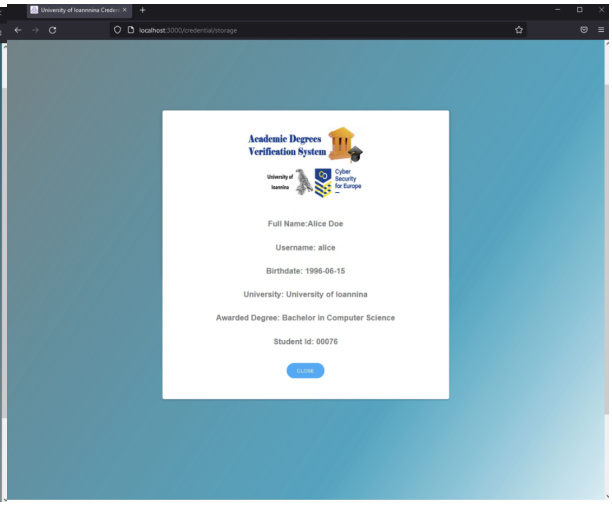
Για να αποκτήσει τα διαπιστευτήρια του Πανεπιστημίου, ο φοιτητής πρέπει να έχει εγγραφεί επιτυχώς στην πλατφόρμα και να έχει πρόσβαση στην εφαρμογή χρησιμοποιώντας τον κωδικό πρόσβασης. Επίσης για να συλλέξει ένα πανεπιστημιακό, διαπιστευτήριο ο φοιτητής μπορεί να αιτηθεί τα διαπιστευτήριά του κάνοντας κλικ στην καρτέλα “Get-Credential” (Εικόνα 6). Εάν ο φοιτητής κατέχει μεταπτυχιακό τίτλο σπουδών, μπορεί να εκδοθεί πιστοποιητικό P-ABC, και εμφανίζεται ειδοποίηση στη διεπαφή χρήστη(Εικόνα 7) όπου μπορεί να δει το διαπιστευτήριο που εκδόθηκε (Εικόνα 8).



Εικόνα 6:Απόκτηση πιστοποιητικού p-ABC



Εικόνα 7:Ειδοποίηση διεπαφής



Εικόνα 8:Αποθηκευμένα διαπιστευτήρια

4.4.1 Βασική Ροή Εφαρμογής

- ✓ Event 1

Ο φοιτητής μπορεί να αποκτήσει διαπιστευτήρια από την πλατφόρμα κάνοντας κλικ στην καρτέλα "Get-Credential". Στη συνέχεια, θα πρέπει να εισάγει τα στοιχεία του πτυχίου τους συμπεριλαμβανομένου του ονόματος του πανεπιστημίου, του τίτλου σπουδών και της ημερομηνίας αποφοίτησης. Εάν ο φοιτητής κατέχει μεταπτυχιακό τίτλο σπουδών, εκδίδεται ένα πιστοποιητικό P-ABC.

- ✓ Event 2

Μετά την έκδοση του πιστοποιητικού, εμφανίζεται μια ειδοποίηση στη διεπαφή χρήστη που ενημερώνει τον φοιτητή ότι το πιστοποιητικό εκδόθηκε. Ο φοιτητής μπορεί να κάνει κλικ στην ειδοποίηση για να προβάλλει το πιστοποιητικό.

- ✓ Event 3

Ο φοιτητής μπορεί να δει το πιστοποιητικό που εκδόθηκε στην καρτέλα "Credentials". Η καρτέλα "Credentials" περιέχει μια λίστα με όλα τα πιστοποιητικά που έχουν εκδοθεί για τον φοιτητή. Ο φοιτητής μπορεί να κάνει κλικ σε ένα πιστοποιητικό για να το προβάλλει.

- ✓ Τέλος της περίπτωσης χρήσης

4.5 Υλοποίηση διαδικτυακής πλατφόρμας για την κατάθεση αιτήσεων χρησιμοποιώντας την εφαρμογή διαχείρισης ταυτότητας

Η εφαρμογή μας για την επαλήθευση του πτυχίου χρησιμοποιεί μια ηλεκτρονική πλατφόρμα υποβολής αιτήσεων (για μεταπτυχιακό ή διδακτορικό πρόγραμμα) για πανεπιστήμια (και εκπαιδευτικά ιδρύματα γενικότερα) που διασφαλίζει την ιδιωτικότητα, ενώ, παράλληλα εγγυάται ότι συμμετέχουν μόνο οι φοιτητές, απαιτώντας τους να αποκαλύπτουν μόνο πληροφορίες που αποδεικνύουν αυτή την επιλεξιμότητα και τίποτα άλλο.

Ο σχεδιασμός ενός τέτοιου συστήματος πρέπει να πληροί τις παραδοσιακές απαιτήσεις ασφάλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, αλλά πρέπει να λάβει υπόψη δύο πρόσθετες απαιτήσεις διαφάνειας που βασίζονται στην ιδιωτικότητα και την παρεμβατικότητα.

Διαφάνεια: Η ικανοποίηση αυτής της απαίτησης συνεπάγεται τη σαφή και κατανοητή δήλωση των εμπλεκόμενων ρυθμιστικών μέτρων, όπως νόμοι, συμβάσεις ή πολιτικές προστασίας της ιδιωτικότητας, καθώς και την περιγραφή των χρησιμοποιούμενων τεχνολογιών, των οργανωτικών διαδικασιών και των αντίστοιχων αρμοδιοτήτων, μεταξύ άλλων.

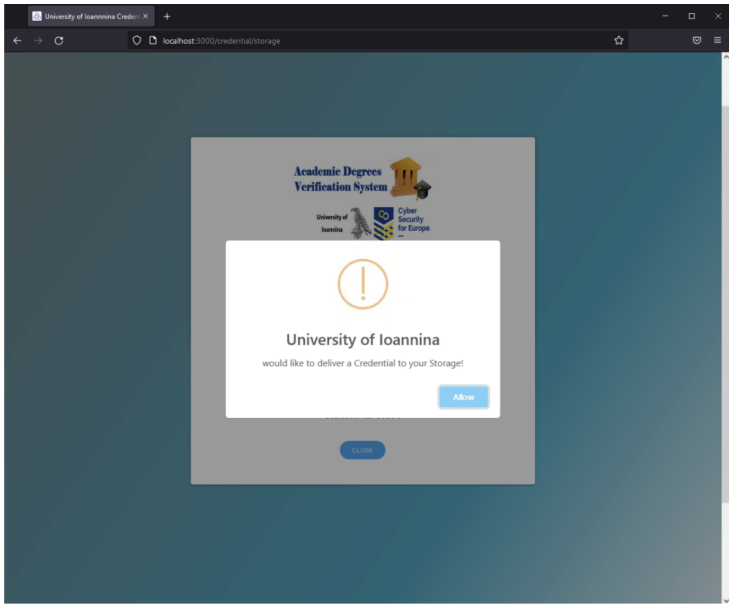
Όλα τα εμπλεκόμενα μέρη που εμπλέκονται σε οποιαδήποτε δραστηριότητα επεξεργασίας δεδομένων με κρίσιμη σημασία για την προστασία της ιδιωτικότητας θα πρέπει να συμφωνούν σαφώς και να κατανοούν τους νομικούς, τεχνικούς και οργανωτικούς όρους. Ιδανικά, όλα τα ενδιαφερόμενα μέρη (π.χ. ο υπεύθυνος επεξεργασίας δεδομένων, ο εκτελών την επεξεργασία δεδομένων και τα υποκείμενα των δεδομένων) θα πρέπει να κατανοούν τους κινδύνους και να διαθέτουν επαρκείς πληροφορίες σχετικά με τα πιθανά αντίμετρα για τους κανονισμούς προστασίας της ιδιωτικότητας, καθώς και για τη χρήση και τους περιορισμούς τους.

Οι διαδικασίες και οι μηχανισμοί για την παροχή αυτών των πληροφοριών θα πρέπει να παρέχονται πριν από την επεξεργασία των δεδομένων (εκ των προτέρων διαφάνεια), η οποία είναι, ιδίως, απαραίτητη εάν ζητείται η συγκατάθεση των υποκειμένων των δεδομένων ή εάν οι υπεύθυνοι επεξεργασίας δεδομένων θέλουν να αποφασίσουν για τη χρήση ενός συγκεκριμένου συστήματος.

Επιπλέον για την παροχή αυτών των πληροφοριών διακρίνονται συνήθως σε εκ των προτέρων διαφάνεια (πριν από τη συλλογή των δεδομένων) και εκ των υστέρων διαφάνεια (μετά τη συλλογή των δεδομένων και κατά τη διάρκεια της επεξεργασίας). Όσον αφορά την εκ των προτέρων διαφάνεια, το σύστημα επαλήθευσης ακαδημαϊκών πτυχίων βελτιώθηκε με την παροχή των ακόλουθων χαρακτηριστικών:

Ειδοποίηση απορρήτου: Η βασική διεπαφή που χρησιμοποιείται για τη διαχείριση των διαπιστευτηρίων περιλαμβάνει μια συνοπτική πολιτική απορρήτου που γνωστοποιεί και διαχειρίζεται τα δεδομένα του χρήστη.

Αυτή η ειδοποίηση επιβεβαιώνει τη διαχείριση του διαπιστευτηρίου (Εικόνα 9). Οι εν λόγω ειδοποιήσεις παρέχουν επίσης πληροφορίες σχετικά με τα δικαιώματα των υποκειμένων των δεδομένων και τα μέτρα ασφαλείας που λαμβάνονται για να διασφαλιστεί η ασφάλεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Στο περιβάλλον της εφαρμογής, οι χρήστες θεωρείται ότι διαβάζουν τα μηνύματα, τα κατανοούν και δίνουν τη συγκατάθεσή τους μετά από ενημέρωση, σύμφωνα με την οποία ενημερώνονται και αναμένεται να ενεργούν προς το συμφέρον τους.

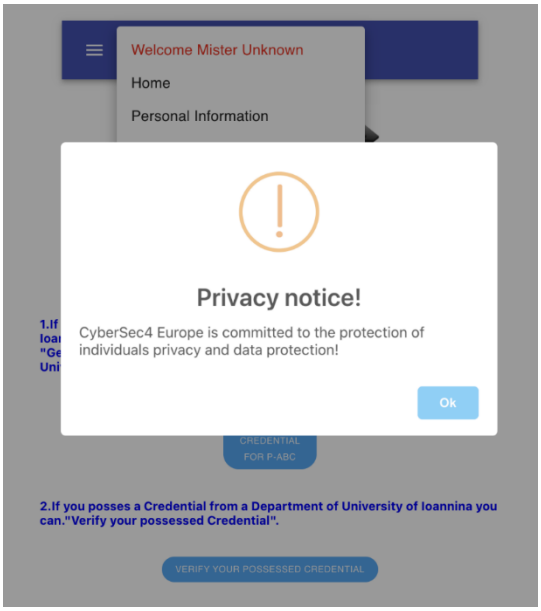


Εικόνα 9:Ζητώντας τη συγκατάθεση του χρήστη

Συναίνεση μετά από ενημέρωση: Μόλις συνδεθεί επιτυχώς στο σύστημα, ο χρήστης μπορεί να δει τις προσωπικές πληροφορίες που έχει μοιραστεί. Το σύστημα είναι επίσης ρυθμισμένο ώστε να αλληλεπιδρά με τον χρήστη σε κάθε βήμα της εφαρμογής.

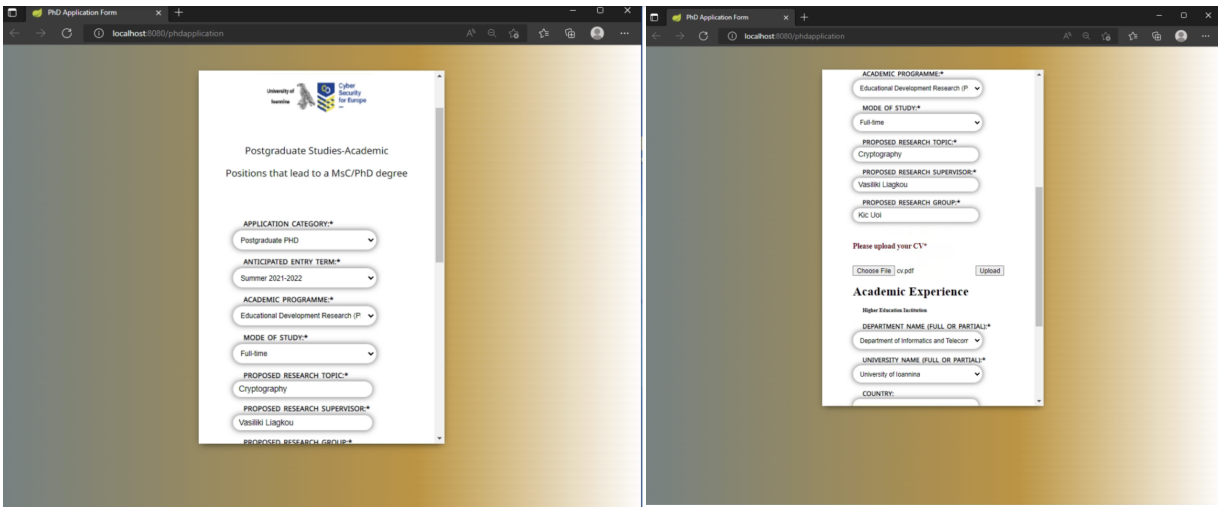
Επιπλέον, κατά την είσοδο στο σύστημα, ο χρήστης ακολουθεί μια διαδικασία επικοινωνίας με το σύστημα όπου αποκαλύπτει τις προσωπικές του πληροφορίες στην οντότητα, άλλοτε ρητά και άλλοτε σιωπηρά δίνοντας τη συγκατάθεσή του για τη χρήση τους για έναν ή περισσότερους σκοπούς. Η συγκατάθεση αποτελεί βασική αρχή των περισσότερων νόμων περί προστασίας δεδομένων/ιδιωτικότητας. Ο επακόλουθος έλεγχος της αποθήκευσης, της χρήσης και της περαιτέρω αποκάλυψης αυτών των πληροφοριών βασίζεται στην έννοια της εμπιστοσύνης ότι η συγκατάθεση θα γίνει σεβαστή. Με βάση μια κατανοητή ειδοποίηση απορρήτου, οι χρήστες παρέχουν συγκατάθεση μετά από ενημέρωση.

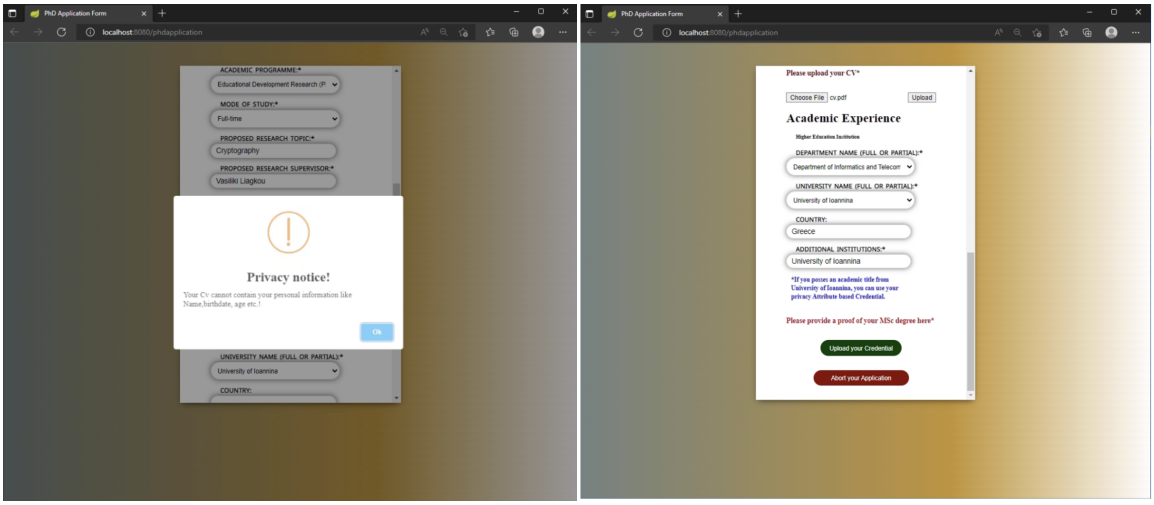
Η διεπαφή συγκατάθεσης μετά από ενημέρωση επιτρέπει στους χρήστες να κατανοήσουν την έκταση της συλλογής και επεξεργασίας δεδομένων, τα εμπλεκόμενα μέρη, τους σκοπούς της επεξεργασίας και την πιθανή κοινή χρήση δεδομένων. Οι χρήστες θα πρέπει επίσης να μπορούν να επιλέγουν επιλεκτικά τους σκοπούς για τους οποίους συμφωνούν/διαφωνούν μέσω μιας σαφούς καταφατικής απάντησης. Η συγκατάθεση αυτή καταχωρίζεται στη συνέχεια στο σύστημα με τη χρήση μηχανισμού διαχείρισης της συγκατάθεσης, ο οποίος θα επιτρέπει αργότερα την άσκηση δικαιωμάτων παρεμβατικότητας (Εικόνα 10).



Εικόνα 10:Ειδοποίηση απορρήτου

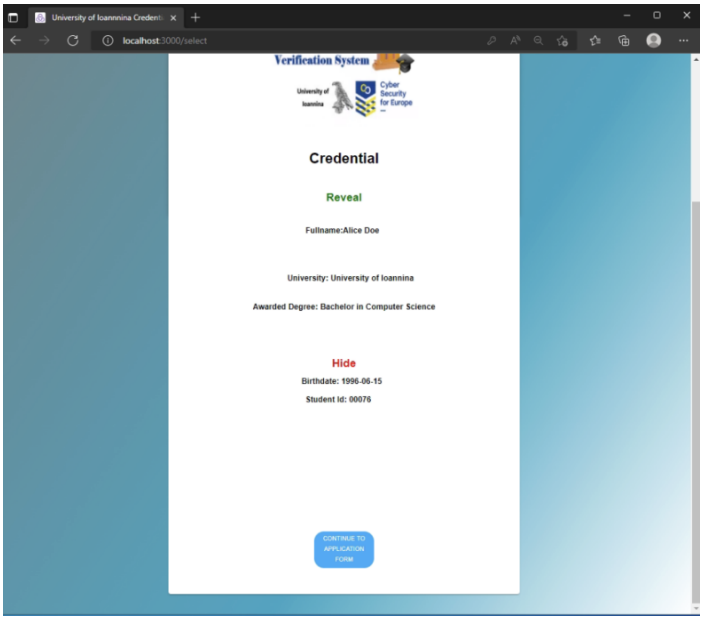
Ειδοποιήσεις και υποδείξεις απορρήτου: Μετά την ολοκλήρωση της εισαγωγής δεδομένων για την αίτηση MSc/ PhD, οι διεπαφές παρέχουν ειδοποιήσεις για την προστασία της ιδιωτικότητας, όπως κατά την εισαγωγή του βιογραφικού σημειώματος- για παράδειγμα, δεν πρέπει να περιέχει καμία προσωπική πληροφορία(Εικόνα 11).





Εικόνα 11:Αίτηση MSc/PhD

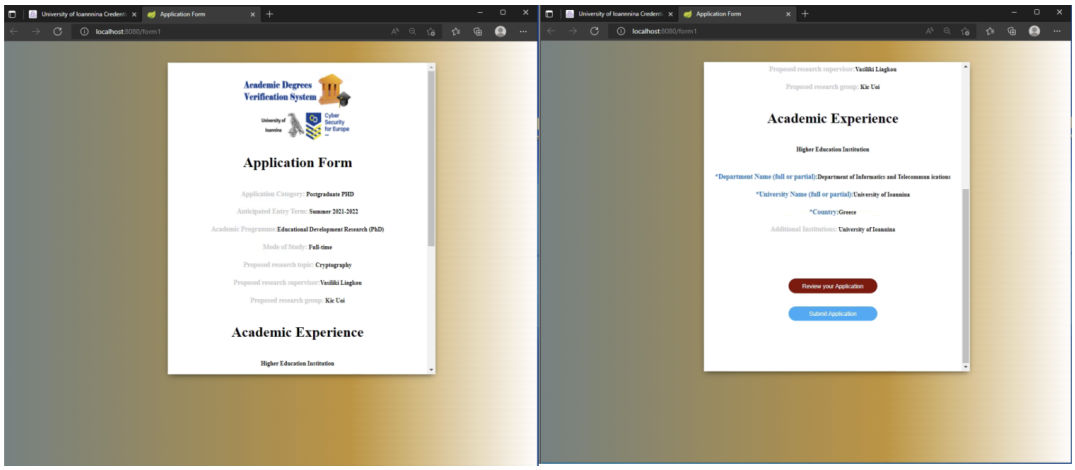
Ο χρήστης μπορεί να αποκαλύψει ή να αποκρύψει τις πληροφορίες που θέλει να μοιραστεί με το σύστημα. Παρέχεται ένα σύνολο ειδοποιήσεων απορρήτου για να βοηθηθούν οι χρήστες να κατανοήσουν τα βασικά οφέλη των συστημάτων, όπως οι ιδιότητες του p-ABCs (εικόνα 12).



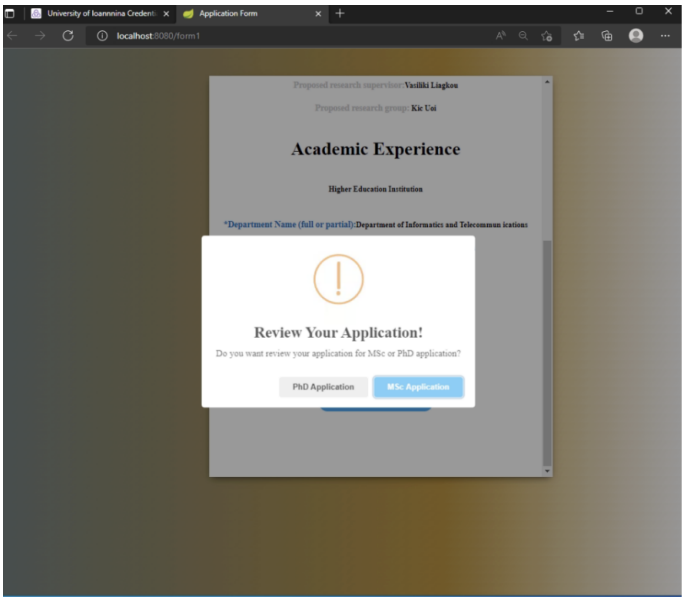
Εικόνα 12:Μενού Drag and Drop για την αποκάλυψη δεδομένων

Επανεξέταση της διεπαφής πριν από την υποβολή: Μετά την ολοκλήρωση της εισαγωγής δεδομένων, ο χρήστης μπορεί να κάνει προεπισκόπηση των δεδομένων(Εικόνα 13). Κατά την προεπισκόπηση των δεδομένων, μπορεί να επιλέξει ποια δεδομένα θέλει να κοινοποιηθούν και ποια δεδομένα θέλει να είναι ιδιωτικά- δίνεται η δυνατότητα στους χρήστες να επανεξετάσουν το

αίτημά τους και να κάνουν διορθώσεις. Ειδικότερα για αυτή την περίπτωση χρήσης σχετικά με την αίτηση εργασίας και το P-ABC, η διεπαφή θα ήταν χρήσιμη για τους χρήστες ώστε να μπορούν να επανεξετάζουν τα δεδομένα που κοινοποιούνται καθώς και τα δεδομένα που δεν κοινοποιούνται (δηλ. για να κατανοήσουν καλύτερα την επιλεκτική κοινοποίηση των χαρακτηριστικών), πριν από την υποβολή της αίτησης εργασίας οι χρήστες μπορούν να την επανεξετάσουν(Εικόνα 14).

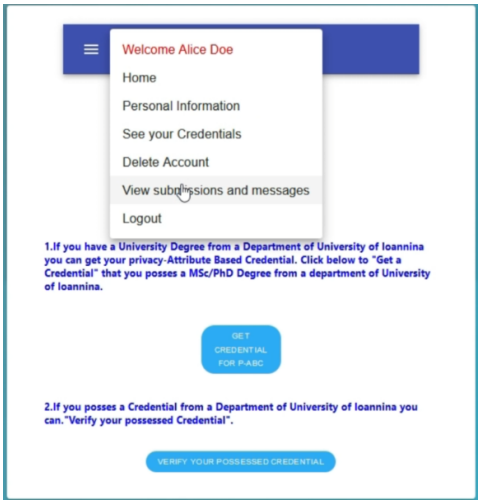


Εικόνα 13:Προεπισκόπηση δεδομένων

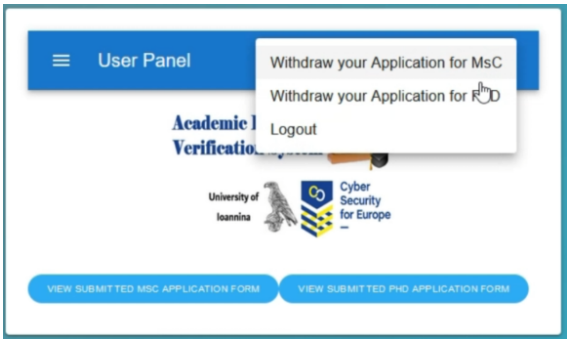


Εικόνα 14:Επανεξέταση αίτησης

Πρόσβαση στα δεδομένα: Οι χρήστες μπορούν να απεικονίσουν όλα τα δεδομένα που συλλέγονται και τα αιτήματα εργασίας που υποβάλλονται στο σύστημα. Το σύστημα επιτρέπει τους χρήστες να βλέπουν τις αιτήσεις που έχουν κάνει και το σύστημα τους επιτρέπει να διαγράφουν τις αιτήσεις τους(Εικόνα 15). Ο χρήστης στην διαδικτυακή εφαρμογή μπορεί να την επεξεργαστεί τις αιτήσεις του για να κάνει διορθώσεις ή να τις διακόψει(Εικόνα 16).



Εικόνα 15:Πρόσβαση στις αιτήσεις



Εικόνα 16:Διόρθωση ή διακοπή αιτήσεων

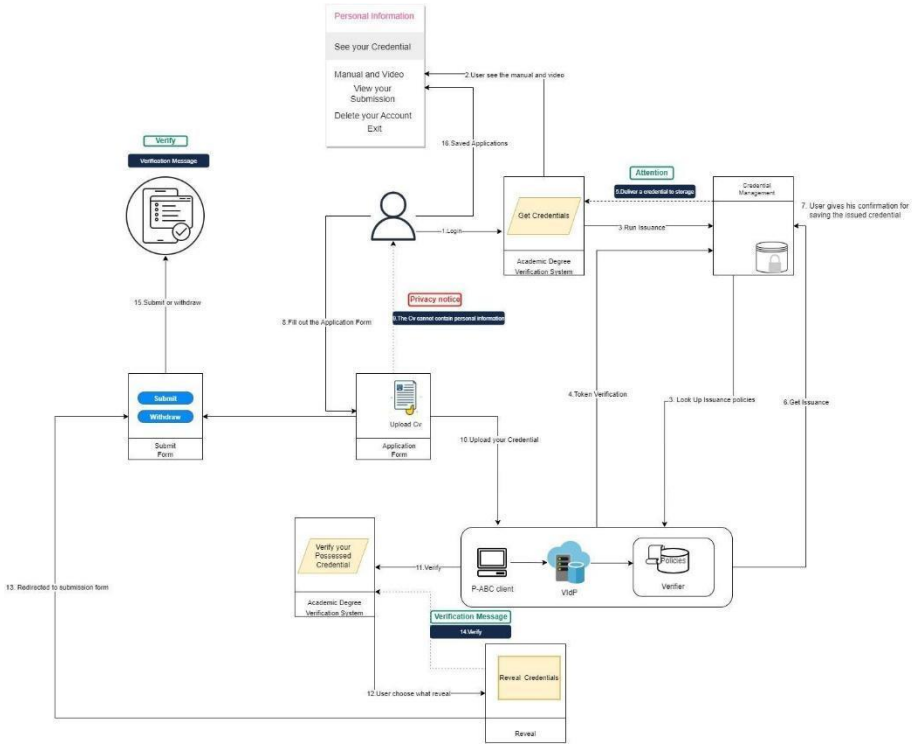
Παρεμβατικότητα: Η δυνατότητα παρέμβασης αναφέρεται στη δυνατότητα των υποκειμένων των δεδομένων να παρεμβαίνουν στα δεδομένα που έχουν συλλεχθεί ή υποβάλλονται σε επεξεργασία. Περιλαμβάνει διάφορες λειτουργίες για τη διόρθωση, την ενημέρωση, τη διαγραφή και την εναντίωση στην επεξεργασία, δίνοντας υποκείμενα των δεδομένων περισσότερο έλεγχο των δεδομένων τους. Όσον αφορά την παρεμβατικότητα, η εφαρμογή μας παρέχει:

Διόρθωση και διαγραφή δεδομένων: Ο ΓΚΠΔ(GPDR) ορίζει ότι τα δεδομένα μπορούν να ζητήσουν τη διόρθωση των προσωπικών τους δεδομένων εάν υπάρχουν σφάλματα και να διαγραφούν τα δεδομένα μόλις αυτά παύουν να υφίστανται. Επιπλέον, το σύστημα παρέχει διεπαφές που επιτρέπουν στους χρήστες να έχουν πρόσβαση και να τροποποιούν τις πληροφορίες τους και τις εφαρμογές εργασίας τους. (Εικόνα 17).

Εικόνα 17:Προβολή αποθηκευμένων διαπιστευτηρίων

4.6 Περιγραφή υψηλού επιπέδου του πιλοτικού προγράμματος: Αρχιτεκτονική του συστήματος

Η αρχιτεκτονική του συστήματος βασίζεται σε διάφορα στοιχεία που έχουν διαφορετικές λειτουργίες και ρόλους. Θα περιγράψουμε τις ιδιότητές τους και την αλληλεπίδρασή τους στο πλαίσιο του πιλοτικού προγράμματος. Η εφαρμογή είναι μια διαδικτυακή εφαρμογή της οποίας οι χρήστες είναι οι φοιτητές και η γραμματεία είναι η γραμματεία του πανεπιστημίου. Επιπλέον, στο παρών σύστημα που αναπτύξαμε(Σχήμα 21), ο πάροχος εικονικής ταυτότητας(vIdP) χωρίζεται σε τρεις ενότητες μία για τον έλεγχο ταυτότητας και δύο για την έκδοση (αίτηση για μεταπτυχιακό και διδακτορικό).



Σχήμα 21:Αρχιτεκτονική Συστήματος

Η ενότητα ελέγχου ταυτότητας(Authentication module) είναι κυρίως υπεύθυνη για την επαλήθευση του ονόματος χρήστη και του κωδικού πρόσβασης. Συνεργάζεται επίσης με το άλλες ενότητες ελέγχου ταυτότητας, και μόλις επικυρωθεί, ο χρήστης πιστοποιείται στον εικονικό πάροχο ταυτότητας (vIdP). Η φάση έκδοσης περιέχει πληροφορίες σχετικά με τη χρήση των

διαπιστευτηρίων P-ABC[33]. Από την άλλη πλευρά, στο P-ABC η διαχείριση διαπιστευτηρίων είναι υπεύθυνη για τη διαχείριση των διαπιστευτηρίων, κάθε πάροχος ταυτότητας (IdP) παράγει ένα διαπιστευτήριο και δεν σχετίζεται με κανενός είδους πολιτική πρόσβασης. Ο συνδυασμός όλων έχει ως αποτέλεσμα ένα πλήρες διαπιστευτήριο χρήστη που μπορεί να επαναχρησιμοποιηθεί για την απόκτηση κρυπτογραφικών αποδείξεων που μπορούν να παρουσιαστούν σε ένα μέρος που βασίζεται για πρόσβαση σε προστατευόμενους πόρους και υπηρεσίες.

Κεφάλαιο 5ο

5.0 Εφαρμογή κινητής συσκευής διαχείρισης χρηστών για την πιστοποίηση ακαδημαϊκών τίτλων διασφαλίζοντας την προστασία των προσωπικών δεδομένων των χρηστών.

Οι παραδοσιακές τεχνολογίες διαχείρισης ταυτότητας, όπως οι SAML[12], OpenID[13], OAuth[13], παρέχουν λύσεις ασφάλειας και ιδιωτικότητας σε διαδικτυακά σενάρια[41]. Τα συστήματα ανώνυμων διαπιστευτηρίων (Anonymous Credential Systems)[20], όπως το Idemix[20], επιτρέπουν την ελάχιστη αποκάλυψη προσωπικών χαρακτηριστικών, επιτρέποντας την προστασία της ιδιωτικότητας μέσω χαρακτηριστικών σχεδιασμού στο σύστημα διαχείρισης ταυτότητας.

Τα συστήματα ανώνυμων διαπιστευτηρίων βασίζονται σε χαρακτηριστικά και σε λειτουργίες κρυπτογραφίας, όπως οι κρυπτοποδείξεις μηδενικής γνώσης (ZKP), για να παρέχουν ψευδωνυμία, ανωνυμία και ελάχιστη αποκάλυψη χαρακτηριστικών με ποικίλα κατηγορήματα. Επιπλέον τα συγκεκριμένα συστήματα παρέχουν μεγάλες δυνατότητες και εφαρμογές και όπως έχουμε παρατηρήσει οδεύουν σε καινοτόμα υπολογιστικά σενάρια όπως έχουμε περιγράψει σε αλυσίδες μπλοκ(blockchain) για την καλύτερη διαχείριση της ταυτότητας, και λειτουργούν σε διαδικτυακές εφαρμογές για την αντιμετώπιση της ιδιωτικότητας.

Επιπλέον τα παραπάνω συστήματα επιτρέπουν ανώνυμες αλλά αυθεντικοποιημένες συναλλαγές μεταξύ χρηστών και παρόχων υπηρεσιών. Ως εκ τούτου, αντιπροσωπεύουν μια ισχυρή τεχνική για την προστασία της ιδιωτικότητας των χρηστών κατά τη διενέργεια συναλλαγών στο Διαδίκτυο.

Τέλος στην παρούσα ενότητα περιγράφουμε το σχεδιασμό και την υλοποίηση ενός συστήματος πιστοποίησης εγγράφων διασφαλίζοντας την ιδιωτικότητα του χρήστη σε κινητές συσκευές βασίζεται σε νέα πρωτόκολλα υψηλού επιπέδου και διεπαφές που επιτρέπουν την εύκολη ενσωμάτωση σε συστήματα ελέγχου πρόσβασης.

5.1 Σύστημα πιστοποίησης εγγράφων διασφαλίζοντας την ιδιωτικότητα του χρήστη σε κινητές συσκευές

Το σύστημα πιστοποίησης εγγράφων θα επιτρέψει σε μια υποδομή ταυτότητας να ικανοποιήσει την ανάγκη για ισχυρή αυθεντικοποίηση με διατήρηση της ιδιωτικότητας με μια κατανεμημένη και κλιμακούμενη πλατφόρμα για τη διαχείριση αυτόνομων ταυτοτήτων με διατήρηση της ιδιωτικότητας.

Επίσης η πλατφόρμα θα επιτρέπει στους χρήστες να συλλέγουν και να διαχειρίζονται χαρακτηριστικά από παρόχους υπηρεσιών ταυτότητας, να πιστοποιούνται στους παρόχους υπηρεσιών, να παρέχουν τη συγκατάθεσή τους και να ελέγχουν τη χρήση των προσωπικών δεδομένων και να διατηρούν την ιδιωτικότητας τους.

Η εφαρμογή που βασίζεται σε κινητές συσκευές είναι ένα παράδειγμα ασφαλούς και αξιόπιστης ανταλλαγής πιστοποιητικών τριτοβάθμιας εκπαίδευσης μεταξύ οργανισμών, όπως εκπαιδευτικά ιδρύματα, πανεπιστήμια, κρατικές υπηρεσίες, οργανισμούς του ιδιωτικού τομέα, καθώς και με ιδιώτες. Θα επιτρέψει στους αποφοίτους τριτοβάθμιας εκπαίδευσης να ανταλλάσσουν έγγραφα και να αποδεικνύουν την εξειδίκευσή τους κατά τη διάρκεια ενός σταδίου προεπιλογής.

Επιπλέον η επαλήθευση των πιστοποιητικών εκπαίδευσης θα κρατήσει τις πληροφορίες των αποφοίτων ιδιωτικές μέχρι να χρειαστούν αργότερα, όπως για παράδειγμα για την πρόσληψη σε κάποια εργασία. Οι απόφοιτοι θα μπορούν να αποδεικνύουν τις ικανότητές τους καθώς και άλλα προσόντα, αποκρύπτοντας πληροφορίες που δεν είναι σχετικές με την περίπτωση, γεγονός που αποτελεί παράδειγμα εφαρμογής της αρχής της διασφάλισης των δεδομένων, όπως απαιτείται από το ΓΚΠΠΔ[42].

Επιπροσθέτως θα παράσχει υποστήριξη και θα δώσει τη δυνατότητα στους τελικούς χρήστες και τους οργανισμούς να ελέγχουν την ιδιωτικότητά τους και να αυξάνουν την εμπιστοσύνη τους στις υπηρεσίες του Διαδικτύου.

Όπως αναφέρθηκε προηγουμένως, καθώς και στους κύριους στόχους του συστήματος διαχείρισης ταυτότητας με διατήρηση της ιδιωτικότητας προορίζεται να αυξήσει την αξιοπιστία και την ιδιωτικότητα της διαχείρισης ταυτότητας. Ιδιαίτερη έμφαση δίνεται στην ακεραιότητα και την προστασία της ιδιωτικότητας των συστημάτων πιστοποίησης πανεπιστημιακών πτυχίων.

5.2 Περιγραφή εφαρμογής

Η εφαρμογή αποτελείται από δύο μέρη(Academic Degree Verification System, Wallet) και έχει δημιουργηθεί για κινητές συσκευές και περιγράφει όλα τα βήματα και τις αλληλεπιδράσεις που απαιτούνται για την ένταξη ενός χρήστη σε ένα σύστημα διαχείρισης ταυτότητας με διατήρηση της ιδιωτικότητας. Για λόγους διασφάλισης της ταυτότητας η εφαρμογή κινητού μπορεί να περιλαμβάνει διαδικασίες εκτός σύνδεσης (φυσικές), όπως η επίσκεψη στο γραφείο μιας αρχής, ή διαδικτυακά βήματα με την αξιοποίηση υφιστάμενων συστημάτων, όπως οι ηλεκτρονικές ταυτότητες. Κατά τη διάρκεια της εγγραφής, παράγεται το απαραίτητο (κύριο) υλικό κλειδιού για έναν χρήστη και καθίσταται προσβάσιμο στον χρήστη, π.χ. όπως μια έξυπνη κάρτα, ή μέσω εφαρμογής κινητού.

Συγκεκριμένα, η εφαρμογή περιγράφει, αυτή η περίπτωση χρήσης περιλαμβάνει όλα τα βήματα που απαιτούνται για την εγγραφή ενός πτυχιούχου στο σύστημα και στο σύστημα πιστοποίησης πτυχίου. Το σύστημα πιστοποίησης πτυχίων έχει αποθηκεύσει τους τίτλους σπουδών και τις επαγγελματικές πιστοποιήσεις. Ο απόφοιτος ακολουθεί τις οδηγίες της εφαρμογής προκειμένου να θεωρηθεί εγγεγραμμένος χρήστης.

5.2.1 Actors

Οι ακόλουθοι actors συμμετέχουν ενεργά στην εφαρμογή. Παρακάτω ανακεφαλαιώνουμε εν συντομία το ρόλο του κάθε actor.

Αρχικά στοιχεία:

Users (Χρήστες). Οι χρήστες επιθυμούν να λαμβάνουν διαπιστευτήρια από τους εκδότες και αργότερα να παρουσιάζουν (τμήματα) αυτών των χαρακτηριστικών στους παρόχους υπηρεσιών με τρόπο που να διατηρεί την ιδιωτικότητα. Συγκεκριμένα, στην εφαρμογή μας, οι απόφοιτοι λαμβάνουν πιστοποιητικά σχετικά με τα πτυχία, και μπορούν αργότερα να αποκαλύψουν επιλεκτικά αυτές τις πληροφορίες, π.χ. όταν υποβάλλουν αίτηση για μια θέση εργασίας, στις τοπικές αρχές κ.λπ.

Service providers / Verifiers. Οι φορείς θέλουν να λάβουν αποδεδειγμένα αυθεντικές πληροφορίες για έναν χρήστη, ώστε να του χορηγήσουν πρόσβαση σε μια συγκεκριμένη

υπηρεσία. Πρέπει επίσης να είναι σε θέση να ορίσουν μια (ελάχιστη) πολιτική που πρέπει να πληροί ένας χρήστης προκειμένου να του χορηγηθεί πρόσβαση. Στο πλαίσιο της περίπτωσης χρήσης μας, οι εκπαιδευτικοί οργανισμοί πρέπει να είναι σε θέση να λαμβάνουν επαληθεύσιμους ισχυρισμούς σχετικά με τα βραβεία των υποψηφίων προκειμένου να τους αποδεχτούν για μια θέση εργασίας.

IdM platform providers. Οι πάροχοι αυτοί φιλοξενούν και συντηρούν την κεντρική υποδομή που απαιτείται για ένα σύστημα διαχείρισης ταυτότητας. Ανάλογα με τη συγκεκριμένη περίπτωση του συστήματος, η αποκλειστική τους ευθύνη μπορεί να είναι η παροχή ορισμένων παραμέτρων του συστήματος, αλλά μπορεί επίσης να ενεργούν ως μεσολαβητής για τα μηνύματα που ανταλλάσσονται μεταξύ των διαφόρων φορέων, ή ακόμη και να αναλαμβάνουν σημαντικά τμήματα του υπολογισμού για να επιτύχουν μια λύση από την πλευρά του χρήστη.

Δευτερεύοντα στοιχεία:

Academic Degree verification system. Αυτό το σύστημα πραγματοποιεί έλεγχο πρόσβασης παρουσιάζοντας μια πολιτική στους αποφοίτους. Μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο σύστημα επαλήθευσης πτυχίου. Δυνητικοί χρήστες αυτής της εφαρμογής είναι το προσωπικό του Πανεπιστημίου.

Ορισμένες προϋποθέσεις του συστήματος είναι οι παρακάτω:

Ένας εγγεγραμμένος φοιτητής επιθυμεί να ενταχθεί στο σύστημα. Η ταυτότητα του χρήστη έχει ήδη επαληθευτεί από το πανεπιστήμιο και οι πληροφορίες αυτές έχουν γίνει προσβάσιμες στο σύστημα επαλήθευσης πτυχίου.

Το σύστημα έχει ήδη αρχικοποιηθεί εκ των προτέρων, δηλαδή έχει ήδη δημιουργηθεί και ρυθμιστεί το βασικό υλικό των εκδοτών (π.χ. πανεπιστήμιο) κ.λπ.

Wallet Application: Η εφαρμογή Academic Degree Verification System λαμβάνει το URL που είναι κωδικοποιημένο και το μεταβιβάζει στο Wallet Application. Μόλις ολοκληρωθεί, το Wallet ζητά απευθείας από τον Verifier επαλήθευση της πολιτικής(policy).

Ο Verifier απαντά στο Wallet με την πολιτική παρουσίασης(policy presentation) και το Wallet θα ζητήσει από τον χρήστη να λάβει επιβεβαίωση (ή όχι) σχετικά με τις πληροφορίες που απαιτούνται. Όταν ο χρήστης επιβεβαιώσει, το Wallet δημιουργεί μια πολιτική που πληροί τις

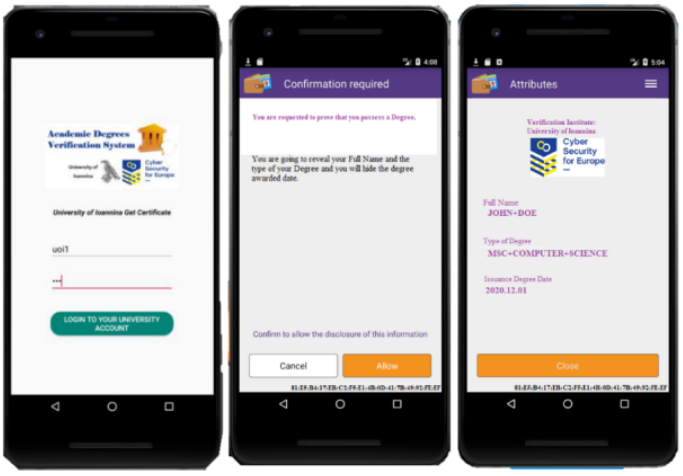
πληροφορίες που ζητήθηκαν από τον verifier και του αποστέλλει μήνυμα. Τέλος, ο verifier επαληθεύει την πολιτική και ανακοινώνει το αποτέλεσμα στην οθόνη της κινητής συσκευής.

5.3 Υλοποίηση Εφαρμογής

Η εφαρμογή αποτελείται από δύο μέρη(Academic Degree Verification System, Wallet) και έχει δημιουργηθεί για κινητές συσκευές και περιγράφει όλα τα βήματα και τις αλληλεπιδράσεις που απαιτούνται για την ένταξη ενός χρήστη σε ένα σύστημα διαχείρισης ταυτότητας με διατήρηση της ιδιωτικότητας.

Στην εφαρμογή Academic Degree Verification System ο χρήστης επιθυμεί να πιστοποιηθεί ότι είναι φοιτητής στο Service Provider και ξεκινάει την διαδικασία απόδειξης της πολιτικής. Στην εφαρμογή θέσαμε ως πολιτικές ότι είναι ο χρήστης κατέχει πτυχίο και ότι ήταν φοιτητής του τμήματος.

Τέλος η εφαρμογή λαμβάνει το URL και το μεταβιβάζει στο Wallet για να δημιουργήσει μια νέα απόδειξη με το URL της συνεδρίας. Μόλις ολοκληρωθεί η απόδειξη, το Wallet ζητά απευθείας από τον Verifier ότι η πολιτική παρουσίασης είναι έγκυρη. Ο Verifier απαντά στο Wallet με την πολιτική παρουσίασης και το πορτοφόλι θα ζητήσει από τον χρήστη να λάβει επιβεβαίωση (ή όχι) σχετικά με τις πληροφορίες που απαιτούνται. Όταν ο χρήστης επιβεβαιώσει, το Wallet παράγει μια απόδειξη που πληροί την απαιτούμενες πληροφορίες από το Wallet (Εικόνα 18).

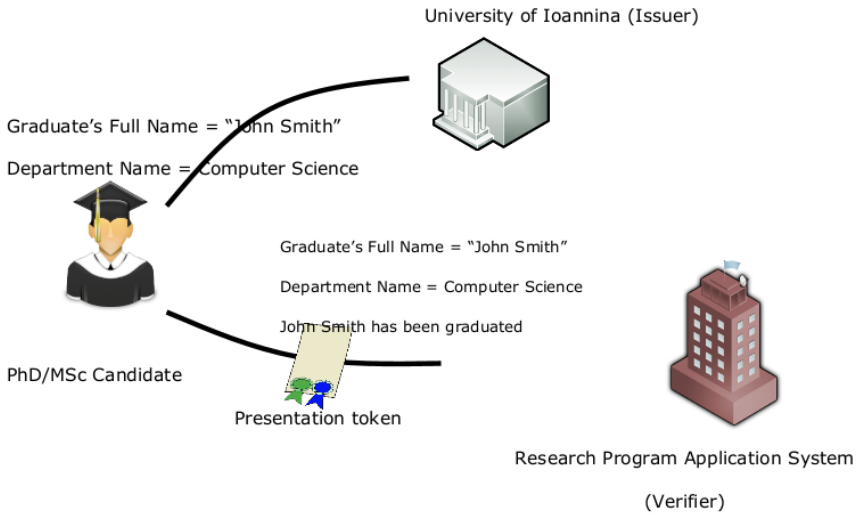


Εικόνα 18: Υλοποίηση Εφαρμογής σε κινητή συσκευή

5.3.1 Εγκατάσταση συστήματος

α) Περιγραφή Σεναρίου

Οι απόφοιτοι του Πανεπιστημίου Ιωαννίνων θα μπορούν να υποβάλλουν ανώνυμα αίτηση για ένα μεταπτυχιακό ερευνητικό πρόγραμμα, εξασφαλίζοντας παράλληλα ότι κατέχουν ένα Ακαδημαϊκό Πτυχίο(Εικόνα 19).



Εικόνα 19: Σενάριο

β) Academic Degree Verification System

Ένας χρήστης μπορεί να υποβάλει αίτηση για ένα πρόγραμμα PhD/MSc:

χρησιμοποιώντας τα διαπιστευτήριά του με τεχνολογίες ABC για να αποδείξει ορισμένα γεγονότα για τον ίδιο, π.χ.: εάν παρακολούθησε συγκεκριμένα μαθήματα, αν αποφοίτησε από το τμήμα του, εάν κατέχει πτυχίο.

γ) Υποβολή αίτησης για πρόγραμμα PhD/MSc

Ένας απόφοιτος θα χρησιμοποιήσει δύο εφαρμογές

- Wallet Application
- Academic Degree Verification System

Χρησιμοποιώντας τα διαπιστευτήρια που είναι αποθηκευμένα στο Wallet Application ο χρήστης μπορεί να, ανώνυμα, να υποβάλει αίτηση για μεταπτυχιακό τίτλο σπουδών αφού αποδείξει ότι έχει ένα ακαδημαϊκό πτυχίο.

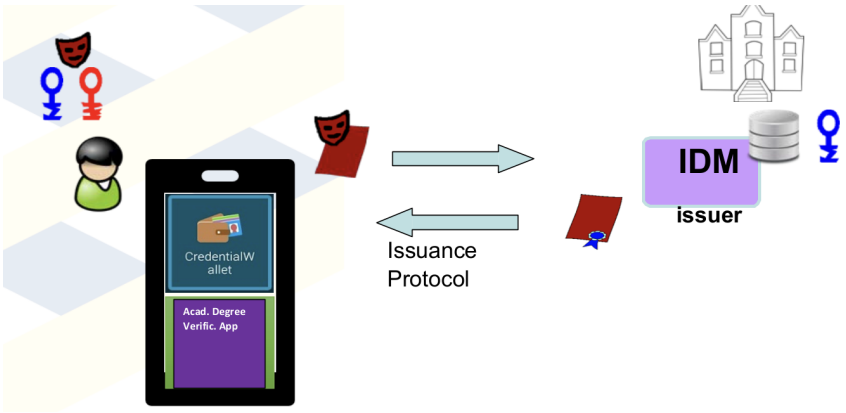
δ)Λήψη διαπιστευτηρίων από το IDM Σύστημα

Ο χρήστης χρησιμοποιεί την εφαρμογή Academic Degree Verification System για τη δημιουργία ενός διαπιστευτηρίου χρησιμοποιώντας το login/pwd του και το αρχικό δημόσιο κλειδί που περιέχει "γνωστά" χαρακτηριστικά τα οποία το σύστημα IDM επαληθεύει με τη βάση δεδομένων του (Εικόνα 20).

Τα "γνωστά" χαρακτηριστικά είναι:

- Πλήρες όνομα
- Όνομα τμήματος
- Ημερομηνία αποφοίτησης
- Ημερομηνία γέννησης κ.λπ.

Ο φοιτητής είναι ο αποδέκτης του πιστοποιητικού και τα διαπιστευτήρια αποθηκεύονται στην εφαρμογή Wallet(Σχήμα).

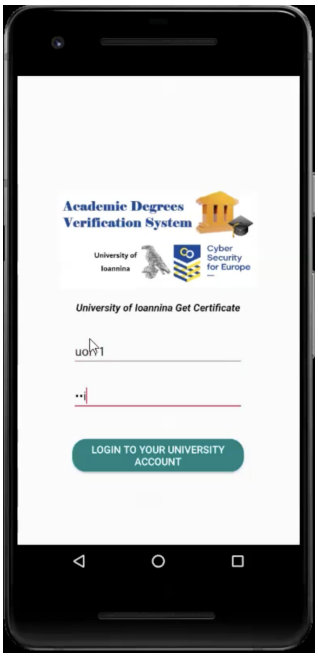


Εικόνα 20: Λήψη διαπιστευτηρίων από το IDM Σύστημα

ε) Παρουσίαση συστήματος

Βήμα 1: Είσοδος

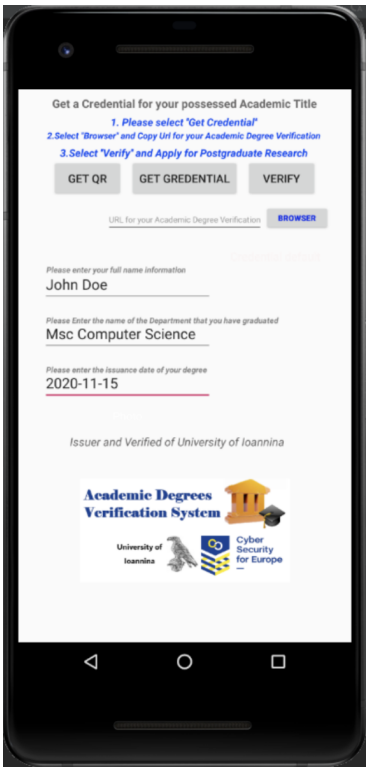
Ο φοιτητης ανοίγει στο κινητό την εφαρμογή Academic Degree Verification System και εισάγει τα διαπιστευτήρια (όνομα χρήστη, κωδικός πρόσβασης). Επιλέξτε “Login to your University Account” για να επαληθεύσει τα διαπιστευτήρια του(Εικόνα 21).



Εικόνα 21: Εισαγωγή στην εφαρμογή

Βήμα 2: Get Credential

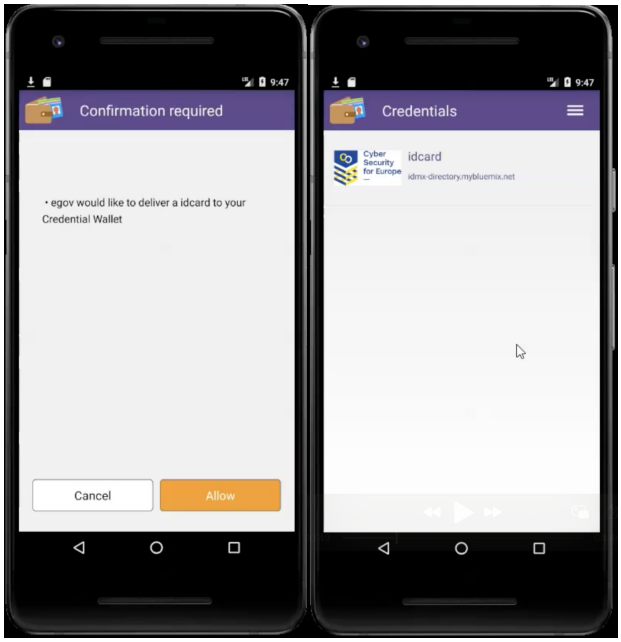
Ο φοιτητής εισάγει το "Ονοματεπώνυμο, Τμήμα, Όνομα, Ημερομηνία έκδοσης" και επιλέγει "Get Credential"(Εικόνα 22).



Εικόνα 22: Περιβάλλον εφαρμογής

Βήμα 3: Αποθήκευση Διαπιστευτηρίου

- Μια σελίδα επιβεβαίωσης θα εμφανιστεί
- Ο χρήστης επιλέγει “Allow”
- Μετά από αυτό θα δει το αποθηκευμένο διαπιστευτήριο στο Wallet App(Εικόνα 23)



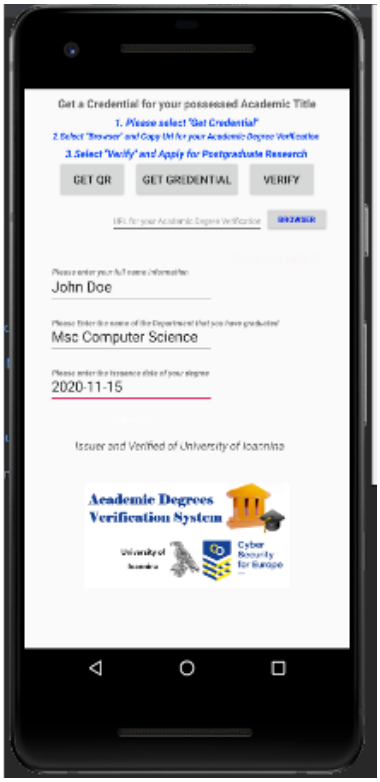
Εικόνα 23: Wallet App

Βήμα 4: Επαλήθευση του διαπιστευτηρίου

- Ο χρήστης ανοίγει το πρόγραμμα περιήγησης και αποκτά πρόσβαση στην διεύθυνση Url (http//:192.168.3.65:3011/show)
- Αντιγράφει τη διεύθυνση Url επαλήθευσης (Εικόνα 24).
- Κάνει επικόλληση την διεύθυνση Url για το Academic Degree Verification" (Επαλήθευση ακαδημαϊκού πτυχίου)(Εικόνα 25)
- Επιλέγει το κουμπί " Verify "(Εικόνα 26)

Εικόνα 24: Επαλήθευση διεύθυνσης

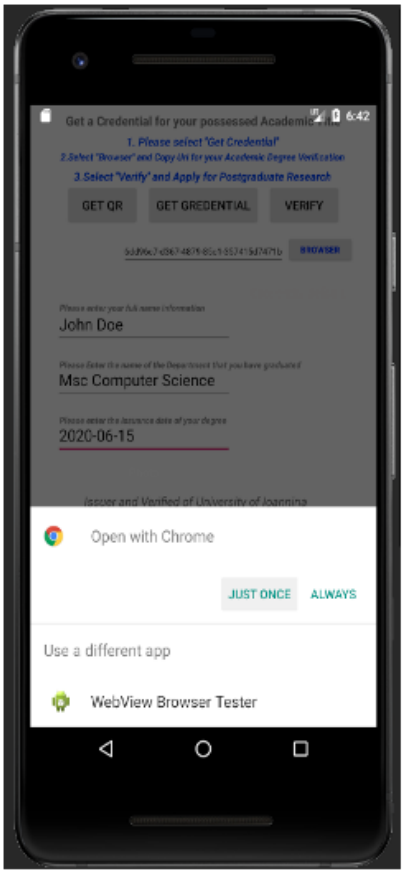
Εικόνα 25: Επαληθευμένο διαπιστευτήριο



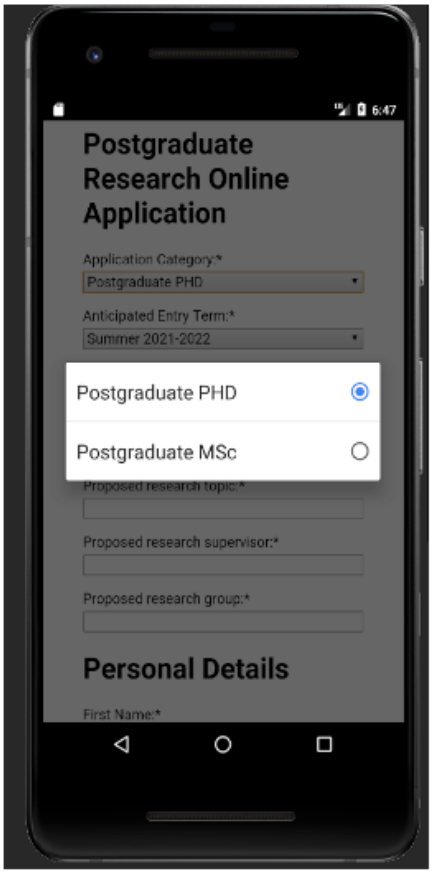
Εικόνα:26 Διαπιστευτήριο

Βήμα 5: Υποβολλή αίτησης για Μεταπτυχιακή/Διδακτορική έρευνα

Αφού ο χρήστης λάβει επιτυχημένο μήνυμα επαλήθευσης μπορείτε να προχωρήσει στην υποβολή της ηλεκτρονικής φόρμα αίτησης (Εικόνα 27, 28, 29).



Εικόνα 27: Άνοιγμα εφαρμογής

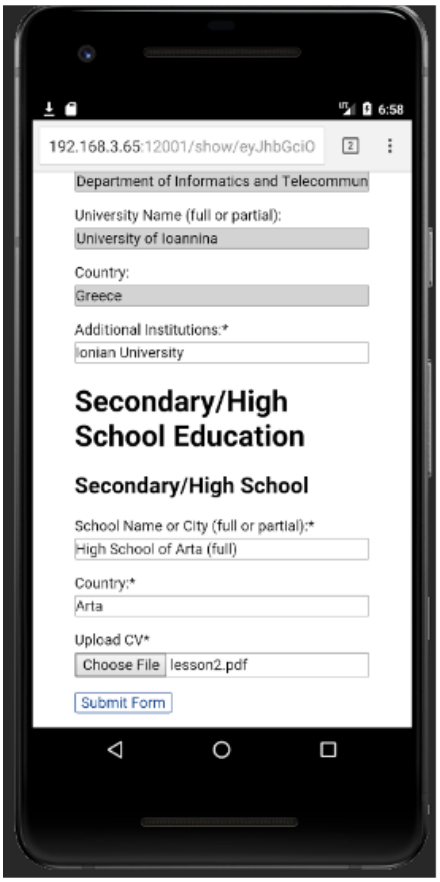


Εικόνα 28:Επιλογή Μεταπτυχιακού/Διδακτορικού

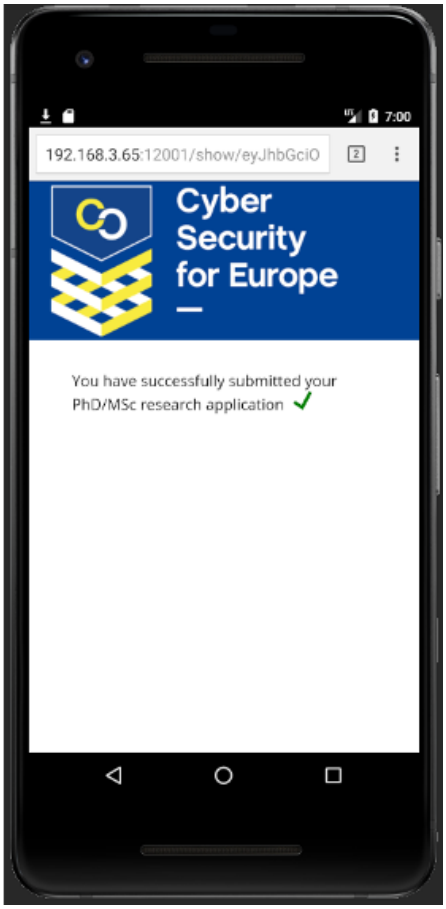
Εικόνα 29: Διαπιστευτήριο

Βήμα 6: Υποβολή την αίτηση

- Ο χρήστης συμπληρώνει τη φόρμα και ανεβάζει το βιογραφικό σημείωμα και επιλέγει "Submit Form"(Εικόνα 30).
- Θα λάβει επιβεβαίωση μήνυμα αφού έχει υποβάλει την ηλεκτρονική φόρμα(Εικόνα 31)
- Κάθε φοιτητής μπορεί να υποβάλει αίτηση μόνο μία φορά



Εικόνα 30: Ολοκλήρωση φόρμας



Εικόνα 31: Υποβολή φόρμας

5.3.2 Βασική Ροή Εφαρμογής

Η Εφαρμογή ξεκινάει

- ✓ Event 1

Ο ενδιαφερόμενος φοιτητής επισκέπτεται τη γραμματεία του πανεπιστημίου για να δηλώσει το ενδιαφέρον για το σύστημα ψηφιακής πιστοποίησης. Οι πληροφορίες εισάγονται στο σύστημα επαλήθευσης Academic Degree Verification Systems και ο χρήστης λαμβάνει έναν κωδικό μιας χρήσης (OTP) που μπορεί να χρησιμοποιηθεί για την ενεργοποίηση του λογαριασμού του.

- ✓ Event 2

Ο φοιτητής επισκέπτεται την εφαρμογή κινητού Academic Degree Verification System και συνδέεται χρησιμοποιώντας τον OTP για να οριστικοποιήσει την εγγραφή του.

- ✓ Event 3

Ο χρήστης καλείται να αλλάξει τον OTP της σε έναν ασφαλή κωδικό πρόσβασης για περαιτέρω χρήση.

- ✓ Event 4

Για αυξημένη ασφάλεια, ο χρήστης επιλέγει έναν κωδικό πρόσβασης ο οποίος απαιτείται για την πρόσβαση σε οποιαδήποτε τοπικά αποθηκευμένη πληροφορία, όπως το μυστικό κλειδί χρήστη που δημιουργήθηκε προηγουμένως.Το υλικό του μυστικού κλειδιού του χρήστη παράγεται τοπικά και αποθηκεύεται στη συσκευή του χρήστη.

- ✓ Event 5

Ο χρήστης προσθέτει τις πληροφορίες και τα δεδομένα της αίτησής του, όπως, π.χ., αίτηση διδακτορικών σπουδών και βιογραφικό σημείωμα.

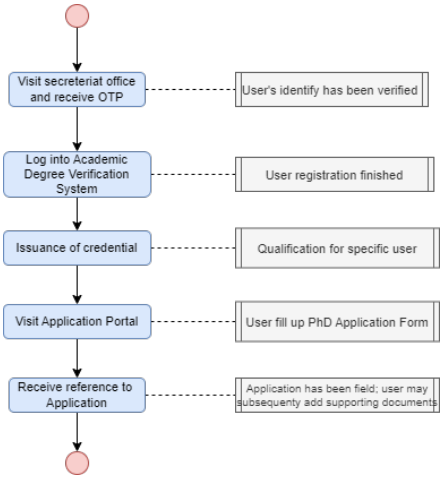
Η πύλη υποβολής αιτήσεων προσφέρει τη δυνατότητα προσθήκης ακαδημαϊκών πτυχίων. Ως εκ τούτου, ο χρήστης προσδιορίζει το πανεπιστήμιο έκδοσης και τον τύπο του πτυχίου. Χρησιμοποιώντας τα τοπικά αποθηκευμένα διαπιστευτήριά της, η εφαρμογή υπολογίζει στη συνέχεια μια κρυπτογραφική απόδειξη ότι ο χρήστης είναι πράγματι κάτοχος του συγκεκριμένου

πτυχίου και τη μεταφορτώνει στον διακομιστή, μπορεί να αρκούν διαφορετικές πληροφορίες για την αίτηση (π.χ. μπορεί να μην απαιτείται η ημερομηνία έκδοσης ή ορισμένοι βαθμοί).

Η πύλη υποβολής αιτήσεων επαληθεύει το ληφθέν διακριτικό παρουσίασης και προσθέτει το πτυχίο του χρήστη, εάν ο έλεγχος ήταν θετικός- σε αντίθετη περίπτωση, το δηλωθέν στοιχείο δεν γίνεται δεκτό.

- ✓ Τέλος της περίπτωσης χρήσης

Η παραπάνω ροή απεικονίζεται επίσης με το ακόλουθο σχήμα (Σχήμα 21)



Σχήμα 21:Βασική Ροή

5.4 Επίδειξη εφαρμογής

Στην Ελλάδα παρατηρείτε αύξηση των περιπτώσεων όπου πλαστά πανεπιστημιακά πτυχία και διπλώματα πωλούνται στο Διαδίκτυο χωρίς να απαιτείται από τον αγοραστή να κάνει οτιδήποτε άλλο εκτός από την καταβολή αμοιβής- ειδικότερα, δεν απαιτούνταν ακαδημαϊκός τίτλος σπουδών.

Προκειμένου να αμβλυνθούν τέτοιου είδους πλαστά πανεπιστημιακά πτυχία, η εφαρμογή στοχεύει στην παροχή μιας κρυπτογραφικά ασφαλής εναλλακτικής λύσης , που βασίζεται στην πιστοποίηση πανεπιστημιακών πτυχίων, επιτυχών μαθημάτων. Οι φοιτητές μπορούν να τα χρησιμοποιήσουν αργότερα τα κρυπτογραφικά διαπιστευτήρια (tokens) και να τα παρουσιάσουν σε μελλοντικούς εργοδότες, και σε άλλα πανεπιστήμια (π.χ. κατά τη διάρκεια προγραμμάτων ανταλλαγής), δημόσιες αρχές κ.λπ. με τρόπο που να παρέχει υψηλές εγγυήσεις αυθεντικότητας στον παραλήπτη, ενώ παράλληλα να σέβεται την ιδιωτικότητα του χρήστη.

Δηλαδή, το μέρος που βασίζεται θα έχει κρυπτογραφικές εγγυήσεις ότι οι πληροφορίες που δόθηκαν ήταν αυθεντικές και όντως πιστοποιημένες από ένα διαπιστευμένο πανεπιστήμιο- από την άλλη πλευρά, ο χρήστης θα έχει τον πλήρη έλεγχο του ποιες πληροφορίες αποκαλύπτονται σε ποιον. Για παράδειγμα, για ορισμένα σενάρια μπορεί να μην είναι απαραίτητο να αποκαλυφθούν όλες οι πληροφορίες (π.χ. όταν αποδεικνύεται η κατοχή ενός πτυχίου σε μια αρχή, μπορεί να μην είναι απαραίτητο να αποκαλυφθεί ο συνολικός βαθμός).

5.4.1 Περιπτώσεις χρήσης

Κατά τη διάρκεια της πρώτης φάσης του συστήματος, θα παρουσιαστούν οι ακόλουθες περιπτώσεις χρήσης.

Εγγραφή(Registration):Αυτή η περίπτωση χρήσης περιγράφει όλα τα βήματα και τις αλληλεπιδράσεις που απαιτούνται για την ένταξη ενός χρήστη σε ένα σύστημα διαχείρισης ταυτότητας με διατήρηση της ιδιωτικότητας. Για λόγους διασφάλισης της ταυτότητας η εφαρμογή μπορεί να περιλαμβάνει διαδικασίες εκτός σύνδεσης (φυσικές), όπως η επίσκεψη στο γραφείο μιας αρχής, ή διαδικτυακά βήματα με την αξιοποίηση υφιστάμενων συστημάτων. Κατά τη διάρκεια της εγγραφής, παράγεται το απαραίτητο (κύριο) υλικό κλειδί για έναν χρήστη και καθίσταται προσβάσιμο στον χρήστη. Συγκεκριμένα, η εφαρμογή περιλαμβάνει όλα τα βήματα που απαιτούνται για την εγγραφή ενός πτυχιούχου στο σύστημα επίδειξης και στο σύστημα πιστοποίησης πτυχίου. Το σύστημα πιστοποίησης πτυχίων έχει αποθηκεύσει τους ανεβασμένους τίτλους σπουδών και τις επαγγελματικές πιστοποιήσεις.

Έκδοση(Issuance): Για να αποκτήσει ένα πιστοποιητικό, ο χρήστης συμμετέχει σε μια συνεδρία έκδοσης με έναν εκδότη πιστοποιητικών, ο οποίος μπορεί να είναι, π.χ., μια δημόσια αρχή, ένα πανεπιστήμιο ή ένας πάροχος υπηρεσιών. Σε μια τέτοια αλληλεπίδραση, ο χρήστης συνήθως πιστοποιείται έναντι του εκδότη και τα δύο μέρη διαπραγματεύονται τα συγκεκριμένα χαρακτηριστικά που πρέπει να πιστοποιηθούν για τον χρήστη (π.χ. ηλικία, ημερομηνία γέννησης, τόπος κατοικίας, εθνικότητα, ημερομηνία λήξης, ακαδημαϊκοί τίτλοι σπουδών κ.λπ.).

Στο τέλος της αλληλεπίδρασης, ο χρήστης λαμβάνει ένα ψηφιακό πιστοποιητικό (ή αλλιώς διαπιστευτήριο) που πιστοποιεί αυτά τα χαρακτηριστικά. Ειδικότερα στο πλαίσιο της περίπτωσης χρήσης του Academic Degree Verification System, το βήμα αυτό απαιτείται για να λάβει ένας απόφοιτος διαπιστευτήριο από το σύστημα πιστοποίησης πτυχίου. Τα χαρακτηριστικά πιστοποιούν ότι διαθέτει έναν τίτλο σπουδών. Ο απόφοιτος αποκτά πρόσβαση στο Academic Degree Verification System προκειμένου να ζητήσει πιστοποιηθεί ότι διαθέτει ένα ακαδημαϊκό πτυχίο/τίτλο/πιστοποιητικό.

Παρουσίαση (Presentation): Ένας χρήστης μπορεί να αποδείξει ότι είναι κάτοχος ενός διαπιστευτηρίου που πιστοποιεί ορισμένα προσωπικά χαρακτηριστικά σε έναν πάροχο υπηρεσιών (ή αλλιώς το μέρος που βασίζεται) συμμετέχοντας σε ένα πρωτόκολλο παρουσίασης. Σε αυτό το

πρωτόκολλο, τα δύο μέρη συμφωνούν για το ποια χαρακτηριστικά πρέπει να αποκαλύψει ο χρήστης. Στο τέλος της αλληλεπίδρασης ο πάροχος υπηρεσιών λαμβάνει αυτά τα χαρακτηριστικά με υψηλές εγγυήσεις αυθεντικότητας, ενώ ο χρήστης έχει την εγγύηση ότι δεν αποκαλύφθηκε καμία άλλη πληροφορία στον πάροχο υπηρεσιών. Συγκεκριμένα, η εφαρμογή εκτελείται όταν ένας φοιτητής χρειάζεται να δημιουργήσει μια επαληθεύσιμη απόδειξη ότι κατέχει έναν συγκεκριμένο τίτλο ή ότι παρακολούθησε συγκεκριμένα μαθήματα.

Κεφάλαιο 6ο

6.0 Συμπεράσματα /Μελλοντική Εργασία

Παρουσιάστηκε μια προηγμένη αρχιτεκτονική διαχείρισης ταυτότητας που εστιάζει στην αυθεντικοποίηση και τη διαχείριση των πρόσβασης με τη χρήση κρυπτογραφίας. Έγινε ανάλυση για τη διαχείριση διαπιστευτηρίων p-ABC, η οποία αποτελεί μια αποτελεσματική λύση για προβλήματα σύνδεσης και αποσύνδεσης.

Επιπλέον δημιουργήθηκαν δύο εφαρμογές για Mobile και Desktop όπου εξετάστηκε πώς η αρχιτεκτονική OLYMPUS μπορεί να ενισχύσει την ιδιωτικότητα και την ασφάλεια σε αυτά τα σενάρια. Η αρχιτεκτονική OLYMPUS προσφέρει βασικές δυνατότητες που απαιτούνται για την ανάπτυξη λύσεων διαχείρισης ταυτότητας με πραγματική διαφύλαξη της ιδιωτικότητας. Αυτές οι δυνατότητες περιλαμβάνουν τη μη συνδεσιμότητα τόσο στους Παρόχους Υπηρεσιών (Service Providers) όσο και στους Παρόχους Ταυτότητας (Identity Providers), την ανωνυμία από τους Παρόχους Ταυτότητας και την επιλεκτική και ελάχιστη αποκάλυψη προσωπικών πληροφοριών.

Στο πλαίσιο μελλοντικής εργασίας, σχεδιάζουμε να εφαρμόσουμε την προσέγγιση p-ABC που αναπτύχθηκε στο OLYMPUS, προκειμένου να αντιμετωπίσουμε τις προκλήσεις που συναντάμε στη διαχείριση της ταυτότητας με διατήρηση της ιδιωτικότητας. Αυτή η προσέγγιση μας επιτρέπει να αναπτύξουμε αποδοτικές και αξιόπιστες κρυπτο-αποδείξεις για την τεχνολογία του blockchain, εξασφαλίζοντας ταυτόχρονα τη διατήρηση της ιδιωτικότητας των χρηστών.

Επιπλέον, θα επικεντρωθούμε στη βελτιστοποίηση και αλλαγή των δομών της κρυπτοβιβλιοθήκης του OLYMPUS, προκειμένου να επιτύχουμε βελτιωμένη απόδοση στο σύστημά μας. Αυτή η βελτιστοποίηση μπορεί να περιλαμβάνει την αναβάθμιση των αλγορίθμων κρυπτογράφησης, τη βελτίωση της διαχείρισης κλειδιών ή την εφαρμογή πιο αποτελεσματικών μεθόδων κρυπτογραφικής απόδειξης.

Ο συνδυασμός της προσέγγισης p-ABC με την βελτιστοποίηση των δομών της κρυπτοβιβλιοθήκης του OLYMPUS θα μας επιτρέψει να δημιουργήσουμε ένα πιο ισχυρό και αποδοτικό σύστημα διαχείρισης ταυτότητας με προστασία της ιδιωτικότητας. Αυτό θα επιφέρει θετικές επιπτώσεις σε διάφορους τομείς όπως η ασφάλεια των δεδομένων, η προστασία των προσωπικών πληροφοριών και η αποδοτικότητα των διαδικασιών διαχείρισης ταυτότητας.

Βιβλιογραφία

[1] I. Sene, A. A. Ciss, and O. Niang, "I2PA: An Efficient ABC for IoT," *Cryptogr. 2019 Vol 3 Page 16*, vol. 3, no. 2, p. 16, Jun. 2019, doi: 10.3390/CRYPTOGRAPHY3020016.

[2] D. Rountree, "What Is Federated Identity?," in *Federated Identity Primer*, Elsevier, 2013, pp. 13–36. doi: 10.1016/B978-0-12-407189-6.00002-9.

[3] IBM, "What is identity and access management (IAM)?," *IBM*, [Online]. Available: https://www.ibm.com/topics/identity-access-management

[4] R. Shay *et al.*, "Can long passwords be secure and usable?," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Apr. 2014, pp. 2927–2936. doi: 10.1145/2556288.2557377.

[5] C. Adams, S. Lloyd, and C. Adams, "Understanding PKI : concepts, standards, and deployment considerations," p. 322, 2003.

[6] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," *Proc. Second ACM Workshop Digit. Identity Manag. DIM 2006 Co-Located 13th ACM Conf. Comput. Commun. Secur. CCS06*, pp. 11–16, 2006, doi: 10.1145/1179529.1179532.

[7] P. Voigt and A. von dem Bussche, "The EU General Data Protection Regulation (GDPR) : a practical guide," p. 383.

[8] Dick Hardt, "The OAuth 2.0 Authorization Framework," *IETF*, Jan. 2020, [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-oauth-v2/31/

[9] N. Sakimura *et al.*, "Final: OpenID Connect Discovery 1.0 incorporating errata set 1," *OpenID*, Nov. 2014, [Online]. Available: https://openid.net/specs/openid-connect-discovery-1_0.html

[10] J. Camenisch and B. Pfitzmann, "Federated Identity Management," in *Security, Privacy, and Trust in Modern Data Management*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 213–238. doi: 10.1007/978-3-540-69861-6_15.

[11] Carl Wikblom, "Federated identity management AD FS for single sign-on and federated identity management," 2012.

[12] Kim Cameron, "THE LAWS OF IDENTITY – Kim Cameron's Identity Weblog," *Microsoft*, May 2005, [Online]. Available: https://www.identityblog.com/?p=352

[13] S. Landau and T. Moore, "Economic Tussles in Federated Identity Management," May 2011.

[14] IBM, "Identity provider and service provider roles - IBM Documentation," *IBM*, Mar. 2021, [Online]. Available: https://www.ibm.com/docs/no/tfim/6.2.2.7?topic=configuring-identity-provider-service-provider-roles

[15] R. Weingärtner and C. M. Westphall, "Enhancing Privacy on Identity Providers".

[16] Okta, "Identity", [Online]. Available: https://www.okta.com/

[17] Auth0, "Auth0: Secure access for everyone. But not just anyone.", [Online]. Available: https://auth0.com/

[18] Ping Identity, "Identity Security for the Digital Enterprise", [Online]. Available: https://www.pingidentity.com/en.html

[19] S. S. Y. Shim, G. Bhalla, and V. Pendyala, "Federated identity management," *Computer*, vol. 38, no. 12, pp. 120–122, Dec. 2005, doi: 10.1109/MC.2005.408.

[20] W. Hommel and H. Reiser, "Federated Identity Management in Business-to-Business Outsourcing," 2005.

[21] M. Ates, C. Gravier, J. Lardon, J. Fayolle, and B. Sauviac, "Interoperability between heterogeneous federation architectures: Illustration with SAML and WS-federation," *Proc.* -

Int. Conf. Signal Image Technol. Internet Based Syst. SITIS 2007, pp. 1063–1070, 2007, doi: 10.1109/SITIS.2007.148.
[22] P. Bichsel *et al.*, "D2.2-Architecture for Attribute-based Credential Technologies-Final Version," 2014.
[23] D. W. Chadwick, A. Otenko, and E. Ball, "Role-based access control with X.509 attribute certificates," *IEEE Internet Comput.*, vol. 7, no. 2, pp. 62–69, 2003, doi: 10.1109/MIC.2003.1189190.
[24] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information".
[25] N. Nikiforakis *et al.*, "You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions", [Online]. Available: www.google.com/jsapi
[26] M. Papathanasaki, L. Maglaras, and N. Ayres, "Modern Authentication Methods: A Comprehensive Survey," *AI Comput. Sci. Robot. Technol.*, vol. 2022, pp. 1–24, Jun. 2022, doi: 10.5772/ACRT.08.
[27] Bill Kleyman, "The importance of identity federation in the cloud | TechTarget", [Online]. Available: https://www.techtarget.com/searchcloudcomputing/tip/The-importance-of-identity-federation-in-the-cloud
[28] P. Consortium, "Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents," 2003.
[29] PRIME, "PRIME - Privacy and Identity Management for Europe — Portal for the PRIME Project," *Prime*, 2016, [Online]. Available: https://web.archive.org/web/20161026044309/https://www.prime-project.eu/
[30] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements," *Requir. Eng.*, vol. 16, no. 1, pp. 3–32, Mar. 2011, doi: 10.1007/S00766-010-0115-7.
[31] S. Hohenberger and B. Waters, "Online/Offline Attribute-Based Encryption," 2014, pp. 293–310. doi: 10.1007/978-3-642-54631-0_17.
[32] C. Paquin and G. Zaverucha, "U-Prove Cryptographic Specification V1.1," 2013, [Online]. Available: http://www.microsoft.com/openspecifications/en/us/programs/osp/default.aspx.
[33] F. Bieker, M. Hansen, G. L. Mikkelsen, and H. Obersteller, "ABC4Trust Workshop on Core Features of Privacy-ABCs, Practical Use, and Legal Issues," 2015, pp. 253–266. doi: 10.1007/978-3-319-18621-4_17.
[34] S. Brands, L. Demuynck, and B. D. Decker, "A practical system for globally revoking the unlinkable pseudonyms of unknown users," *Lect. Notes Comput. Sci. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma.*, vol. 4586 LNCS, pp. 400–415, 2007, doi: 10.1007/978-3-540-73458-1_29/COVER.
[35] Meiko Jensen (Kiel University), Cedric Lauradoux (INRIA), and Konstantinos Limniotis (HDPA), "Pseudonymisation techniques and best practices," *Eur. Union Agency Cybersecurity*, Dec. 2009, [Online]. Available: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices
[36] P. Bichsel *et al.*, "An Architecture for Privacy-ABCs," in *Attribute-based Credentials for Trust*, Cham: Springer International Publishing, 2015, pp. 11–78. doi: 10.1007/978-3-319-14439-9_2.
[37] S. Y. Lim *et al.*, "Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 4–2, p. 1735, Sep. 2018, doi: 10.18517/ijaseit.8.4-2.6838.

[38] R. T. Moreno *et al.*, "The OLYMPUS Architecture—Oblivious Identity Management for Private User-Friendly Services," *Sens. 2020 Vol 20 Page 945*, vol. 20, no. 3, p. 945, Feb. 2020, doi: 10.3390/S20030945.
[39] D. Fett, R. Küsters, and G. Schmitz, "A Comprehensive Formal Security Analysis of OAuth 2.0," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, Oct. 2016, pp. 1204–1215. doi: 10.1145/2976749.2978385.
[40] K. Rannenberg, J. Camenisch, and A. Sabouri, "Attribute-based credentials for trust: Identity in the information society," *Attrib.-Based Credentials Trust Identity Inf. Soc.*, pp. 1–391, Jan. 2015, doi: 10.1007/978-3-319-14439-9/COVER.
[41] Y. Yu *et al.*, "Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 4, pp. 767–778, Apr. 2017, doi: 10.1109/TIFS.2016.2615853.
[42] Νομική Βιβλιοθήκη, "Άρθρο 5 - Γενικός Κανονισμός για την Προστασία Δεδομένων - Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα | Νομοθεσία | Lawspot," *Νομική Βιβλιοθήκη*, May 2018, [Online]. Available: https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-5-genikos-kanonismos-gia-tin-prostasia-dedomenon-arhes

7.0 Παράρτημα

Λεξιλόγιο Ορών

Identity management (IdM) = Σύστημα διαχείρισης ταυτότητας

Identity service providers(IdSP) = Πάροχος υπηρεσιών ταυτότητας

Domain = Τομέας

Authentication mechanism = Μηχανισμός ελέγχου ταυτότητας

Token = Διαπιστευτήριο

Access control = Ελεγχος πρόσβασης

Security Policies = Πολιτικές απορρήτου

Single sign-on (SSO) = Συστήματα ενιαίας σύνδεσης

Biometric Authentication = Βιομετρικός έλεγχος ταυτότητας

Password Management = Διαχείριση κωδικού πρόσβασης

One Time Password = Κωδικός πρόσβασης μίας χρήσης

Two Factor Authentication (2FA) = Έλεγχος ταυτότητας δύο παραγόντων

Multi-factor authentication (MFA) = Έλεγχος ταυτότητας πολλαπλών παραγόντων

Public key infrastructure (PKI) = Υποδομή δημόσιου κλειδιού

Security Assertion Markup Language (SAML) = Γλώσσα σήμανσης ισχυρισμών ασφαλείας (SAML)

Federated Identity Management(FIdM) = Διαχείριση Ομοσπονδιακής Ταυτότητας

Relying Party = Τρίτο Μέρος

Attributes = Χαρακτηριστικά

Virtual private network (VPN) = Εικονικά Ιδιωτικά Δίκτυα

IP address = Διεύθυνση Διαδικτυακού Πρωτοκόλλου

Service Provider (SP) = Πάροχος υπηρεσιών

Certificate Authority(CA) = Αρχή πιστοποίησης

Privacy-enhancing technologies (PET) = Τεχνολογίες ενίσχυσης της ιδιωτηκότητας

Privacy Attribute-based Credentials (P-ABC) = Διαπιστευτήρια βάσει χαρακτηριστικών απορρήτου

Minimal Disclosure = Ελάχιστη αποκάλυψη

Unlinkability = Μη συνδεσιμότητα

Partial Identities and identifiers = Μερικές ταυτότητες και αναγνωριστικά

User = Χρήστης

Issuer = Εκδότης

Revocation authority = Αρχή ανάκλησης

Inspector = Επιθεωρητής

Pseudonyms = Ψευδώνυμα

Credentials and Key Binding = Διαπιστευτήρια και δέσμευση κλειδιών

Presentation token = Παρουσίαση διαπιστευτηρίου

Blockchain = Αλυσίδα μπλοκ

Distributed ledger technologies (DLT) = Τεχνολογία Κατανεμημένου κώδικα (DLT)

Identity provider (IdP) = Πάροχος ταυτότητας

Virtual Identity provider (vIdP) = Εικονικός Πάροχος Ταυτότητας

Distributed authentication = Κατανεμημένος έλεγχος ταυτότητας

Distributed credential module = Κατανεμημένη μονάδα διαπιστευτηρίων

Distributed token module = Κατενεμημένη μονάδα διαπιστευτηρίων

Signature = Υπογραφή

Constructors = Κατασκευαστής

Empty constructor = Προεπιλεγμένος κατασκευαστής

Registration = Εγγραφή

Issuance = Έκδοση

Presentation = Παρουσίαση

JSON (JavaScript Object Notation) = Συμβολισμός αντικειμένου JavaScript

ZKP (Zero-knowledge proof) = Απόδειξη μηδενικής γνώσης ή πρωτόκολλο μηδενικής γνώσης