Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης

ψηφιακήελλάδα
Όλα είναι δυνατά
Επιχειρησιακό Πρόγραμμα "Ψηφιακή Σύγκλιση"

ΕΣΠΑ 2007-2013
Ποιότητα ζωής για όλους

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Hellenic Academic Libraries Link
HEAL-LINK
Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών

Υποδομή Πιστοποίησης και Εξουσιοδότησης ΑΑΙ

Shibboleth

Ομοσπονδία HEAL-Link

Ανώτατα Εκπαιδευτικά και Ερευνητικά Ιδρύματα

Παράρτημα - 2

Τεχνικές Προδιαγραφές

&

Προδιαγραφές Ιδιοχαρακτηριστικών

Σχέση Εμπιστοσύνης

Η σχέση εμπιστοσύνης μεταξύ της ομοσπονδίας, των μελών της ομοσπονδίας και των Συνεργατών της ομοσπονδίας βασίζεται σε Τεχνολογία Υποδομής Δημοσίου Κλειδιού X.509 (PKI), που επιτρέπει την αμοιβαία πιστοποίηση. Είναι βασισμένη στη χρήση του SSL/TLS πρωτοκόλλου και ψηφιακών υπογραφών σε έγγραφα XML χρησιμοποιώντας τα κλειδιά που περιέχονται στα πιστοποιητικά X.509, τα οποία προέρχονται από Αρχές Πιστοποίησης (ΑΠ) αναγνωρισμένες από την Ομοσπονδία HEAL-Link.

Όσον αφορά τα μέλη της ομοσπονδίας δεν θα πρέπει να είναι μόνη λύση η χρήση των εμπορικών Αρχών Έκδοσης Πιστοποιητικών. Τα περισσότερα από τα μέλη της ομοσπονδίας έχουν τις δικές τους αρχές έκδοσης πιστοποιητικών στα πλαίσια διαφόρων υπηρεσιών που παρέχουν στα μέλη τους. Αυτές οι αρχές ενεργούν σύμφωνα με τις απαιτήσεις των υπηρεσιών που καθορίζονται από την ακαδημαϊκή κοινότητα. Πέρα από αυτό, υπάρχει μεγάλο κόστος στην ανάκτηση των πιστοποιητικών από μια εμπορική αρχή έκδοσης πιστοποιητικών.

Ως εκ τούτου, η Ομοσπονδία HEAL-Link θα λάβει υπόψη τις πολιτικές των προαναφερόμενων Αρχών Πιστοποίησης και θα τις εντάξει στη λίστα με τις αξιόπιστες αρχές έκδοσης πιστοποιητικών.

Ψηφιακά Πιστοποιητικά

Ομοσπονδία HEAL-Link: Ρόλοι Πιστοποιητικών

Τα πρωτόκολλα και τα προφίλ που χρησιμοποιούνται από την ομοσπονδία κάνουν εκτεταμένη χρήση X.509 πιστοποιητικών που φέρουν τα δημόσια κλειδιά που χρησιμοποιούνται για διάφορους σκοπούς. Τα πιστοποιητικά αυτά μπορεί να κατανεμηθούν σε δύο κύριες κατηγορίες:

- Πιστοποιητικά προγράμματος περιήγησης που είναι ορατά μόνο στον πρόγραμμα περιήγησης του χρήστη. Εδώ μπορούν να χρησιμοποιηθούν Πιστοποιητικά από οποιαδήποτε Αρχή Πιστοποίησης (ΑΠ). Ο βασικός περιορισμός είναι ότι η Αρχή Πιστοποίησης (ΑΠ) θα πρέπει να είναι αποδεκτή ως αξιόπιστη από το πρόγραμμα περιήγησης του χρήστη. Τα πιστοποιητικά προγράμματος περιήγησης είναι:
    - Πιστοποιητικό διακομιστή SSL του IDP του μέλους της Ομοσπονδίας, το οποίο φαίνεται στα προγράμματα περιήγησης (για παράδειγμα, σε μια σελίδα σύνδεσης χρήστη).
    - Πιστοποιητικό διακομιστή SSL του SP του συνεργάτη της Ομοσπονδίας , το οποίο φαίνεται στα προγράμματα περιήγησης (για παράδειγμα, στις πραγματικές σελίδες του site που προστατεύονται από το Shibboleth και σε τελικά σημεία της υπηρεσίας assertion consumer service).
    - Οποιαδήποτε SSL πιστοποιητικά διακομιστή, τα οποία φαίνονται στα προγράμματα περιήγησης κατά τη διαδικασία discovery process (για

παράδειγμα, σε τοπικούς WAYF διακομιστές ή σε δικτυακές πύλες των οργανισμών).

- Τα πιστοποιητικά trust fabric είναι ορατά μόνο στο λογισμικό των IDP και SP αντίστοιχα και όχι στο πρόγραμμα περιήγησης του χρήστη (browser). Μόνο συγκεκριμένα προϊόντα πιστοποιητικών είναι αποδεκτά για το σκοπό αυτό. Τα πιστοποιητικά trust fabric είναι:
    - Το πιστοποιητικό για την υπογραφή εγγράφων XML με ζεύγος κλειδιών του IDP για υπηρεσίες SAML.
    - Το πιστοποιητικό για SSL διακομιστή με ζεύγος κλειδιού του IDP για υπηρεσίες SAML.
    - Το πιστοποιητικό για SSL ζεύγος κλειδιού του πελάτη του SP για υπηρεσίες SAML.
    - Το πιστοποιητικό για την υπογραφή εγγράφων XML με ζεύγος κλειδιών του SP για υπηρεσίες SAML.

Η εγκατάσταση του λογισμικού είναι απλούστατη όταν είναι δυνατόν να επιλεγεί το ίδιο πιστοποιητικό για χρήση σε όλους τους ρόλους για μια δεδομένη οντότητα. Στην περίπτωση αυτή, τα πιστοποιητικά του προγράμματος περιήγησης και τα πιστοποιητικά trust fabric συνδυάζονται.

Προδιαγραφές Ιδιοχαρακτηριστικών

Η προδιαγραφή ιδιοχαρακτηριστικών στην υποδομή AAI είναι πολύ σημαντική για την ανταλλαγή δεδομένων μεταξύ της Ομοσπονδίας HEAL-Link και συμμετεχόντων σε αυτήν. Αυτό το έγγραφο θέτει τα πρότυπα ιδιοχαρακτηριστικά μεταξύ όλων των συμμετεχόντων οργανισμών. Η μορφοποίηση του ορισμού του ιδιοχαρακτηριστικού είναι κοντά στην σύνταξη LDAP. Η προδιαγραφή αυτή ξεκίνησε με ένα βασικό σύνολο των ιδιοχαρακτηριστικών και βασίζεται στο έργο του [Internet2] για την προδιαγραφή [eduPerson]. Το σύνολο των ιδιοχαρακτηριστικών θα μπορούσε να επεκταθεί περαιτέρω σε μελλοντικές εκδόσεις, ανάλογα με τις απαιτήσεις σε ιδιοχαρακτηριστικά των Ιδιοκτητών των πόρων και τις δυνατότητες των πάροχων των ιδιοχαρακτηριστικών (Οργανισμοί Προέλευσης) να τα προμηθεύσουν.

Το πιο σημαντικό καθήκον των διαχειριστών των Οργανισμών Προέλευσης και των Ιδιοκτητών των Πόρων, όσον αφορά τα ιδιοχαρακτηριστικά, είναι ο σεβασμός της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων. Οι χρήστες αντιλαμβάνονται πολλά από τα ιδιοχαρακτηριστικά που ορίζονται στο παρόν έγγραφο ως πολύ ευαίσθητες πληροφορίες. Όλοι οι άνθρωποι που έρχονται σε επαφή με αυτά τα ιδιοχαρακτηριστικά πρέπει να σέβονται πλήρως το απόρρητο του χρήστη, τους σχετικούς νόμους προστασίας προσωπικών δεδομένων και τους κανονισμούς που ορίζουν πώς να ασχοληθεί κάποιος με τα προσωπικά δεδομένα.

Η αποκάλυψη των τιμών των ιδιοχαρακτηριστικών μπορεί να επιφέρει κίνδυνο ασφάλειας. Ως παράδειγμα μπορεί να αναφερθεί το "uid", το μοναδικό αναγνωριστικό το

οποίο θα μπορούσε να παράσχει πολύτιμες πληροφορίες σε κάποιον κακόβουλο τρίτο. Η σημασιολογία του προορίζεται στο να είναι αναγνωριστικό του χρήστη για έλεγχο ταυτότητας (γνωστός και ως σύνδεση), ενδεχομένως και στον Οργανισμό Προέλευσης. Επομένως, είναι κρίσιμες οι αποφάσεις για την ασφάλεια και οι διαχειριστές του Οργανισμού Προέλευσης θα πρέπει να αναλογιστούν προσεκτικά την απόφαση να απελευθερώσουν το ιδιοχαρακτηριστικό UID σε όλους τους πόρους, ακόμη και εντός του οργανισμού τους. Αντίθετα, οι διαχειριστές των Ιδιοκτητών των Πόρων δεν θα πρέπει να απαιτούν την ιδιότητα uid εκτός αν έχουν διμερή συμφωνία με τους διαχειριστές του Οργανισμού Προέλευσης (στην περίπτωσή μας με την Ομοσπονδία HEAL-Link). Σημειώστε ότι το Shibboleth δεν έχει σχεδιαστεί για να απελευθερώνει τα στοιχεία που χρησιμοποιούνται για την πιστοποίηση στον Οργανισμό Προέλευσης (π.χ. Κωδικός χρήστη). Εφόσον οι πληροφορίες διανέμονται σε τρίτους, ο κίνδυνος της ασφάλειας πρέπει να εξεταστεί προσεκτικά.

Οργανισμοί Προέλευσης και Ιδιοχαρακτηριστικά

Οι Οργανισμοί Προέλευσης συγκεντρώνουν και να διατηρούν τις πληροφορίες, οι οποίες θα πρέπει να διατίθεται μέσω των ιδιοχαρακτηριστικών. Είναι αποθηκευμένες σε έναν κατάλογο χρηστών, ο οποίος μπορεί να υλοποιηθεί με τη χρήση ενός καταλόγου συμβατού με LDAP (π.χ. OpenLDAP ή Active Directory) ή μια βάση δεδομένων SQL. Ο Οργανισμός Προέλευσης είναι υπεύθυνος για την **ορθή διαχείριση ταυτότητας και τα επικαιροποιημένα προσωπικά δεδομένα**. Επιπλέον, είναι επίσης υπεύθυνος για την ορθή διαμόρφωση της Πολιτικής (Shibboleth Attribute Release Policy ARP) που καθορίζει τα ιδιοχαρακτηριστικά που μπορούν να απελευθερωθούν σε ποιους πόρους με στόχο την προστασία της ιδιωτικότητας των χρηστών του. Κάθε οργανισμός που συμμετέχει στην Ομοσπονδία HEAL-Link πρέπει να έχει υλοποιήσει και να έχει διαθέσιμα τουλάχιστον τα υποχρεωτικά ιδιοχαρακτηριστικά όπως αυτά ορίζονται στο παρόν έγγραφο.

Ιδιοκτήτες Πόρων και Ιδιοχαρακτηριστικά

Το σύνολο των ιδιοχαρακτηριστικών που απαιτούνται από κάποιον Πόρο εξαρτάται από την υπηρεσία που προσφέρει στους χρήστες του. Το σύνολο μπορεί να είναι ελάχιστο για ανώνυμες υπηρεσίες και αρκετά μεγάλο για εξατομικευμένες υπηρεσίες με κοκκώδη(granular) εξουσιοδότηση. Ένα πράγμα που πρέπει να ακολουθηθεί είναι το εξής: σύμφωνα με τις αρχές προστασίας προσωπικών δεδομένων θα πρέπει να επεξεργαστούν, όσο το δυνατόν λιγότερα δεδομένα προσωπικού χαρακτήρα!

Επιπλέον, ο Ιδιοκτήτης των Πόρων πρέπει να εξετάσει προσεκτικά ποια πληροφορία να αποθηκεύσει κατά τη διάρκεια συνεδριών των χρηστών. Όσο λιγότερες πληροφορίες αποθηκεύονται, σε περίπτωση οποιουδήποτε συμβάντος πιθανής κακής χρήσης θα έχει το μικρότερο αντίκτυπο. Γι 'αυτό είναι καθήκον του Ιδιοκτήτη των Πόρων να καθορίσει ποια ιδιοχαρακτηριστικά είναι αυτά που **πραγματικά απαιτούνται** για την προσφορά την υπηρεσίας και **όποια επιπλέον επιθυμητά ιδιοχαρακτηριστικά** θα μπορούσαν να του

επιτρέψουν την προσφορά προαιρετικών προηγμένων υπηρεσιών. Κατά τον καθορισμό των απαιτήσεων των ιδιοχαρακτηριστικών τους, οι Ιδιοκτήτες των Πόρων πρέπει πάντα να ελέγχουν εάν το ιδιοχαρακτηριστικό αυτό είναι ενσωματωμένο και προσφέρεται από την Ομοσπονδία HEAL-Link. Εάν ένας Πόρος απαιτεί ένα ιδιοχαρακτηριστικό που δεν έχει ενσωματωθεί (ακόμη) στην στον Οργανισμό Προέλευσης των υποψήφιων χρηστών του, οι χρήστες δεν θα μπορούν να έχουν πρόσβαση στον Πόρο. Συνεπώς, στην περίπτωση της επικαιροποίησης στα απαιτούμενα ιδιοχαρακτηριστικά τους, οι Ιδιοκτήτες των Πόρων θα πρέπει να ειδοποιούν την Ομοσπονδία HEAL-Link σε εύθετο χρόνο, προκειμένου να γίνουν οι κατάλληλες ενέργειες για την εφαρμογή του νέου ιδιοχαρακτηριστικού.

Οι ελάχιστες απαιτήσεις για τους χρήστες της Ομοσπονδίας HEAL-Link σε ιδιοχαρακτηριστικά περιγράφονται παρακάτω.

Υποχρεωτικά Ιδιοχαρακτηριστικά για τους Συμμετέχοντες της Ομοσπονδίας HEAL-Link
(Mandatory Attributes for HEAL-Link Federation Participants)

Entitlement (eduPersonEntitlement)

- Description
    - URI (either URL or URN) that indicates a set of rights to specific resources.
    - A simple example would be a URI for a contract with a licensed resource provider. When a principal's home institutional directory is allowed to assert such entitlements, the business rules that evaluate a person's attributes to determine eligibility are evaluated there. The target resource provider does not learn characteristics of the person beyond their entitlement. The trust between the two parties must be established out of band. One check would be for the target resource provider to maintain a list of subscribing institutions. Assertions of entitlement from institutions not on this list would not be honored.
    - This attribute is suitable when a home organization knows to which resources a certain set of their students, staff etc. should have access to. The home organization knows their users and can therefore add a specific entitlement value to the entries of entitled users.
- Permissible values
    - *urn:mace:dir:entitlement:shared:common-lib-terms*
- Typical usage
    - authorization
- Origin
    - [eduPerson]
- OID

    - 1.3.6.1.4.1.5923.1.1.1.7
- LDAP syntax
    - Directory String

Προαιρετικά Ιδιοχαρακτηριστικά για τους Συμμετέχοντες της Ομοσπονδίας HEAL-Link
(Optional Attributes for HEAL-Link Federation)

TargetedID (eduPersonTargetedID)

- Description
    - A unique identifier for a person, mainly for inter-institutional user identification on personalized services.
- Semantics
    - <unique-local-ID> (local part)
    - It is an ID uniquely allocated by the home organization for a user that has been authenticated according to the local authentication policy. It has to be unique. It MAY NOT be reassigned, also if the former user left the home organization.
    - A home organization has to be able to identify the person matching that <unique-local-ID>.
    - TargetedID should not be exposed to end users; especially require a user to provide it manually.
- Typical usage
    - Personalization, authorization
- Origin
    - [eduperson]
- OID
    - 1.3.6.1.4.1.5923.1.1.1.10
- LDAP Syntax
    - Directory String
- Notes
    - It MUST NOT exceed 256 characters in length.

Η σύνταξη του παρόντος εγγράφου βασίστηκε στα παρακάτω έγγραφα:

- **JISC (UK federated access management)**
- **SWITCHaai (Authentication and Authorization Infrastructure AAI Federation, Switzerland).**