Federated Identity Pattern

Πρόβλημα

Οι χρήστες συχνά χρειάζεται να χρησιμοποιήσουν πολλαπλές εφαρμογές διάφορων οργανισμών.

Αναγκάζονται σε ορισμένες περιπτώσεις να έχουν διαφορετικά στοιχεία ταυτοποίησης (credentials) για κάθε μία από αυτές.

Το παραπάνω μπορεί να οδηγήσει σε:

- Προβλήματα εμπειρίας χρήστη (π.χ. δυσκολία απομνημόνευσης διαφορετικών κωδικών)
- Προβλήματα ασφάλειας
- Περιπλοκή διαχείρισης χρηστών

Λύση

Υλοποίηση μηχανισμού επαλήθευσης που χρησιμοποιεί ομοσπονδιακή ταυτότητα, για ανάθεση της επαλήθευσης σε έναν έμπιστο πάροχο ταυτότητας (Trusted IdP).

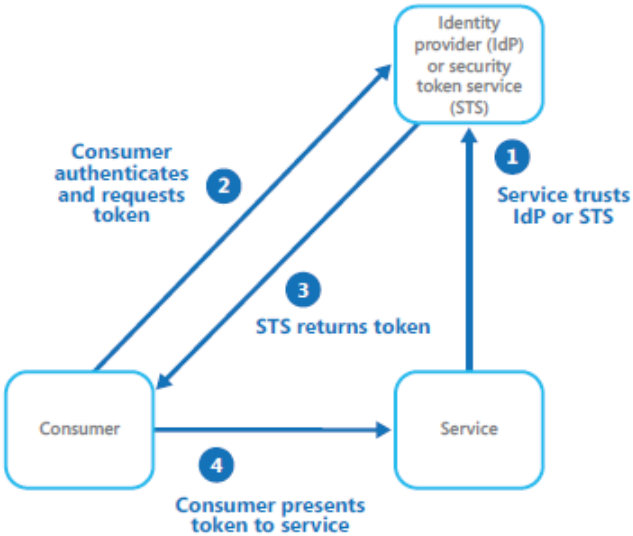
Παραδείγματα έμπιστων παρόχων ταυτότητας είναι:

- Εταιρικοί κατάλογοι
- Τοπικές (on-premises) ομοσπονδιακές υπηρεσίες
- Υπηρεσίες παροχής τεκμηρίων ασφάλειας (security token services - STS) από επιχειρησιακούς συνεργάτες ή Social IdPs (π.χ. Facebook, Google, Microsoft).

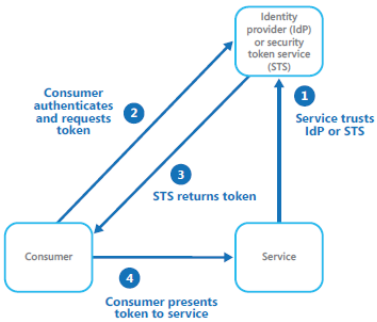
Οι IdPs εκδίδουν τεκμήρια ασφάλειας τα οποία επιβεβαιώνουν πληροφορίες του επαληθευμένου χρήστη (claims).

Claims-based Access Control (1/2)

Η εφαρμογή – πελάτης επικοινωνεί με τον IdP ο οποίος πραγματοποιεί την επαλήθευση των στοιχείων του χρήστη. Εάν αυτή είναι επιτυχημένη, ο IdP επιστρέφει ένα τεκμήριο το οποίο περιέχει τα claims που ταυτοποιούν τον χρήστη στον STS (IdP και STS μπορεί να είναι κοινοί). Ο STS μπορεί σε ορισμένες περιπτώσεις να αλλάξει τα claims του τεκμηρίου. Τέλος, η εφαρμογή – πελάτης μπορεί να προωθήσει το τεκμήριο ως απόδειξη της ταυτότητας του χρήστη.



Claims-based Access Control (2/2)



- Η εφαρμογή βλέπει μόνο τις πληροφορίες ταυτότητας που περιέχονται στο τεκμήριο.
- Η διαχείριση της ταυτότητας και των στοιχείων ταυτοποίησης είναι υπ' ευθύνη του IdP.

Πρόσθετα Χαρακτηριστικά

Υπενθύμιση: η επαλήθευση χρήστη αποτελεί μοναδικό σημείο αποτυχίας (Single Point of Failure – SPOF).

Οι μηχανισμοί επαλήθευσης μπορεί να διαθέτουν τρόπους για ρύθμιση του επιπέδου πρόσβασης με βάση claims ρόλου στο τεκμήριο επαλήθευσης (Role-Based Access Control – RBAC).

Η επαλήθευση με claims χρησιμοποιώντας Social IdPs (π.χ. Facebook, Microsoft) συνήθως παρέχει μόνο διεύθυνση ηλεκτρονικού ταχυδρομείου ή σε κάποιες περιπτώσεις μόνο ένα μοναδικό αναγνωριστικό.

Αν υπάρχει παραπάνω από ένας IdP για το STS πρέπει να ανιχνευθεί ο πάροχος στον οποίο θα ανακατευθυνθεί (Home Realm Discovery).

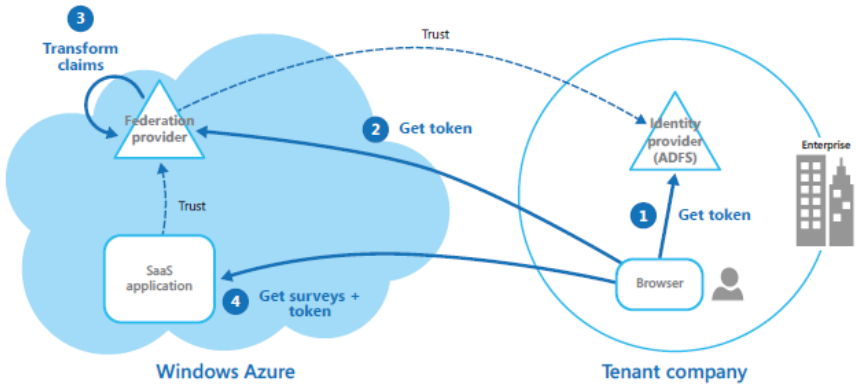
Περιπτώσεις Χρήσης

- Κοινός λογαριασμός για όλες τις υπηρεσίες του οργανισμού (Single Sign On – SSO).
- Για ταυτοποίηση εργαζομένων αλλά και επιχειρησιακών συνεργατών, οι οποίοι ίσως δεν διαθέτουν λογαριασμό στον εταιρικό κατάλογο.
- Ταυτοποίηση χρηστών εφαρμογών λογισμικού ως υπηρεσία (Software as a Service – SaaS).

Περιπτώσεις Πιθανής Αποφυγής Χρήσης

- Όλοι οι χρήστες της εφαρμογής μπορούν να ταυτοποιηθούν από έναν IdP μόνο.
- Η εφαρμογή είχε αρχικά αναπτυχθεί χρησιμοποιώντας έναν διαφορετικό μηχανισμό επαλήθευσης στοιχείων χρηστών.

Παράδειγμα



Βήμα 1: Οι ένοικοι επαληθεύονται από τον IdP τους, ο οποίος επιστρέφει ένα τεκμήριο επαλήθευσης.

Βήμα 2: Το πρόγραμμα - πελάτης προωθεί αυτό το τεκμήριο στον ομοσπονδιακό πάροχο της SaaS εφαρμογής, ο οποίος εμπιστεύεται τα τεκμήρια του IdP, ώστε να λάβει τεκμήριο έγκυρο για αυτόν.

Βήμα 3 (προαιρετικό): Αλλαγή των πληροφοριών του τεκμηρίου από τον ομοσπονδιακό πάροχο ώστε να τα αναγνωρίζει η SaaS εφαρμογή.

Βήμα 4: Η SaaS εφαρμογή εμπιστεύεται τα τεκμήρια που εκδίδει ο ομοσπονδιακός πάροχος της και χρησιμοποιώντας τις πληροφορίες (claims) από το τεκμήριο εφαρμόζει πιθανούς κανόνες που καθορίζουν το επίπεδο πρόσβασης.

Πηγές

Cloud Design Patterns, Prescriptive Architecture Guidance For Cloud Applications, Microsoft (εικόνες και πληροφορίες από το κεφάλαιο “Federated Identity Pattern”.