

Πανεπιστήμιο Μακεδονίας

Πρόγραμμα Μεταπτυχιακών Σπουδών

Τμήματος Εφαρμοσμένης Πληροφορικής

**Εργασία στο μάθημα της Κρυπτογραφίας**

**Θέμα: Δημιουργία Ασφαλών Κατανεμημένων Εφαρμογών με την Χρήση του Ολοκληρωμένου Πλαισίου «Vanadium»**

Ζήσης Δημήτριος (mai21014)

Μαϊκαντής Θεόδωρος (mai21030)

Υπεύθυνη Καθηγήτρια: Πετρίδου Σοφία

# Περιεχόμενα

[Περίληψη](#_Toc57145660)

[Ευρετήριο Σχημάτων](#_Toc57145662)

[Ευρετήριο Πινάκων](#_Toc57145663)

[1. Εισαγωγή](#_Toc57145664)

[2. Ερευνητικό Υπόβαθρο](#_Toc57145665)

[2.1 Κρυπτογραφία](#_Toc57145666)

[2.2 Αυθεντικοποίηση Machine to Machine (M2M)](#_Toc57145667)

[2.3 Δομή Πελάτη - Διακομιστή](#_Toc57145671)

[2.4 Κλήση Απομακρυσμένης Διαδικασίας](#_Toc57145671)

[3. Vanadium](#_Toc57145670)

[3.1 Μοντέλο Επικοινωνίας](#_Toc57145671)

[3.1.1 Μοντέλο Πελάτη – Διακομιστή στο Vanadium](#_Toc57145673)

[3.1.2 Κλήση Απομακρυσμένης Διαδικασίας στο Vanadium](#_Toc57145673)

[3.2 Μοντέλο Ασφάλειας](#_Toc57145672)

[3.2.1 Γενικά](#_Toc57145673)

[3.2.2 Principals & Blessings](#_Toc57145673)

[3.2.3 Αναθέσεις](#_Toc57145673)

[3.2.4 Περιορισμοί](#_Toc57145673)

[3.2.5 Επαλήθευση των Blessings](#_Toc57145673)

[3.2.6 Εξουσιοδότηση](#_Toc57145674)

[4. Υλοποίηση](#_Toc57145676)

[4.1 Εφαρμογή Ανταλλαγής Άμεσων Μηνυμάτων](#_Toc57145677)

[4.1.1 Κώδικας](#_Toc57145677)

[4.1.1 Εκτέλεση](#_Toc57145677)

[5. Συμπεράσματα](#_Toc57145681)

[Βιβλιογραφία](#_Toc57145682)

[Παραρτήματα](#_Toc57145683)

# Περίληψη

Προκειμένου να υφίσταται η ασφάλεια σε ένα κατανεμημένο σύστημα, είναι άκρως σημαντικό να αξιολογηθεί η αξιοπιστία των συμμετεχόντων οντοτήτων, καθώς η εμπιστοσύνη είναι, γενικότερα, βασική προϋπόθεση για επικοινωνία και συνεργασία. Σε αυτή την εργασία, παρουσιάζουμε ένα ολοκληρωμένο πλαίσιο (framework), το οποίο παρέχει ένα σύνολο εργαλείων, βιβλιοθηκών και υπηρεσιών για την ανάπτυξη ασφαλών κατανεμημένων συστημάτων και εφαρμογών, ονόματι *Vanadium*.

Η διάρθρωση της παρούσας εργασίας εστιάζει στην εξερεύνηση του συγκεκριμένου framework. Το *Vanadium* αποτελεί ένα open-source framework, με το οποίο είναι δυνατή η κατασκευή ασφαλών και κατανεμημένων cross-platform εφαρμογών. Πιο συγκεκριμένα, μελετώνται το *πρωτόκολλο κλήσης απομακρυσμένης διαδικασίας Vanadium* (RPC), το μοντέλο ασφάλειας του *Vanadium*, το οποίο καθορίζει *μηχανισμούς αναγνώρισης* (identification mechanisms), *ελέγχου ταυτότητας* (authentication mechanisms), υποστηρίζοντας, έτσι, μία πλήρως αποκεντρωμένη, λεπτομερή και ελεγχόμενη εξουσιοδότηση όταν επικοινωνούν δύο ή και περισσότερες οντότητες (π.χ. αυτόνομες διεργασίες). Σε ό,τι αφορά τους προαναφερθέντες μηχανισμούς, γίνεται περιγραφή των ιδιοτήτων τους, των υλοποιήσεων που παρέχονται από το *Vanadium Framework* και ορισμένων λεπτομερειών σχεδίασης που σχετίζονται με τα πρωτόκολλα αυτά καθ’ αυτά.

Επιπλέον, εξηγείται εκτενώς η έννοια και η υλοποίηση της ονοματοδοσίας στο framework και ο τρόπος με τον οποίο το σύστημα ονομάτων του *Vanadium* επιτρέπει την ανακάλυψη συσκευών, ανεξάρτητα από τη φυσική τους θέση - με ή χωρίς σύνδεση στο διαδίκτυο. Τέλος, προκειμένου να αναδειχθούν στην πράξη ορισμένες από τις λειτουργίες και δυνατότητες του *Vanadium Framework,* παρέχεται συμπληρωματικά και μία εφαρμογή επίδειξης (σε γλώσσα προγραμματισμού *Go*), η οποία κάνει χρήση των περισσότερων λειτουργιών του framework, και συγκεκριμένα εκείνες που αφορούν την επικοινωνία, την αυθεντικοποίηση, αλλά και την αναγνώριση οντοτήτων.

Συνοψίζοντας, η συμβολή της παρούσας εργασίας εντοπίζεται, κυρίως, στο επίπεδο της μελέτης της δομής και της λειτουργίας του *Vanadium Framework.* Επεκτείνεται, όμως, και στο επίπεδο της προγραμματιστικής υλοποίησης μίας demo εφαρμογής, με την οποία μπορεί να γίνει αντιληπτό το πώς μπορεί κανείς να χρησιμοποιήσει τις δυνατότητες που προσφέρει το *Vanadium Framework* στην πράξη.

# Εισαγωγή

*Υπό κατασκευή…*

# Ερευνητικό Υπόβαθρο

## Κρυπτογραφία

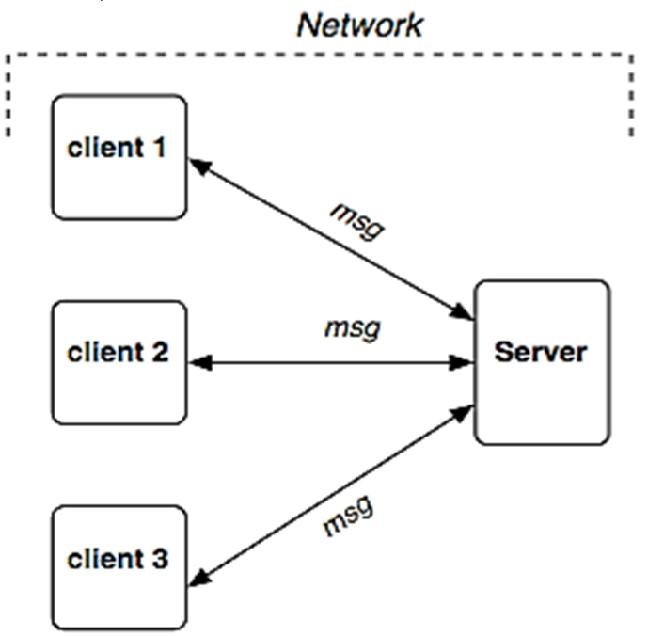
*Υπό κατασκευή…*

## Αυθεντικοποίηση

*Υπό κατασκευή…*

## Δομή Πελάτη – Διακομιστή

Το **μοντέλο πελάτη – διακομιστή** (ή πελάτη – εξυπηρετητή, client – server model) αποτελεί μια υποδομή για κατανεμημένες εφαρμογές, δηλαδή συστήματα στα οποία διάφορες συσκευές συνδέονται μεταξύ τους μέσω ενός δικτύου (ή και του διαδικτύου). Με αυτό τον τρόπο οι πελάτες (υπολογιστής, έξυπνο τηλέφωνο, IoT συσκευή κλπ.), έχουν την δυνατότητα να ζητούν υπηρεσίες από έναν διακομιστή, ο οποίος προσφέρει πληροφορίες ή/και επιπρόσθετη υπολογιστική ισχύ. Το συγκεκριμένο μοντέλο, χρησιμοποιείται από τις περισσότερες (κατανεμημένες) εφαρμογές σήμερα.



**Εικόνα xx**: Μοντέλο Πελάτη – Διακομιστή (Πολλαπλοί Πελάτες, Ένας διακομιστής)

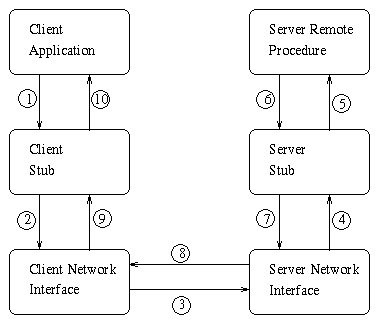
Πηγή: [Architecture of Network and Client-Server model](https://arxiv.org/ftp/arxiv/papers/1307/1307.6665.pdf)

Στην παρούσα εργασία, θα ασχοληθούμε με **μία από τις σημαντικότερες πτυχές του μοντέλου πελάτη – διακομιστή: Την ασφάλεια των δεδομένων που ρέουν σε ένα δίκτυο μέσω μιας κατανεμημένης εφαρμογής**, λόγω των αιτημάτων των πελατών (client requests) και των απαντήσεων του διακομιστή (server replies). Η ανταλλαγή των δεδομένων αυτών, γίνεται μέσω διαφόρων πρωτοκόλλων μεταφοράς (transport protocols), όπως το *TCP* στην περίπτωση του *Vanadium*.

## Κλήση Απομακρυσμένης Διαδικασίας

Η Κλήση Απομακρυσμένης Διαδικασίας (*Remote Procedure Call*) αποτελεί μια τεχνική επικοινωνίας μεταξύ διεργασιών που χρησιμοποιείται για εφαρμογές που βασίζονται στο μοντέλο [*πελάτη - διακομιστή*](#_Γενικά).

Ένας πελάτης έχει ένα μήνυμα αίτησης, το οποίο το παραλαμβάνει η εκάστοτε βιβλιοθήκη RPC, το μεταφράζει και το στέλνει στο διακομιστή. Αυτό το αίτημα μπορεί να είναι μια διαδικασία ή μια κλήση διαδικασίας σε έναν απομακρυσμένο διακομιστή (υπολογιστή). Μόλις ο διακομιστής λάβει το αίτημα, στέλνει απάντηση πίσω στον πελάτη. Στην γενική περίπτωση, ο πελάτης συνεχίζει την εκτέλεσή του μόνο μετά την ολοκλήρωση του διακομιστή.



**Εικόνα xx**: Κλήση Απομακρυσμένης Διαδικασίας

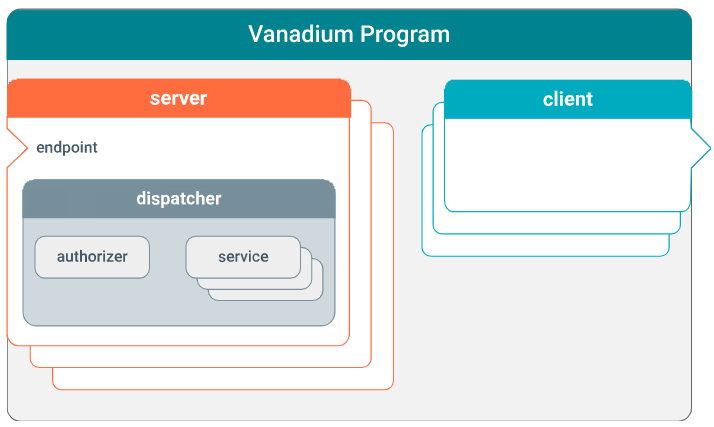
Πηγή: <http://web.mit.edu/6.033/1997/reports/dp1-danlief.html>

Η *εικόνα 4-1-2-1* απεικονίζει τη ροή μιας κλήσης απομακρυσμένης διαδικασίας. Αρχικά, η εφαρμογή πελάτη πραγματοποιεί μια κλήση διαδικασίας, η οποία δε διαφέρει σε κάτι από μια συμβατική κλήση διαδικασίας (τοπική). Η διαδικασία που καλεί ο πελάτης ονομάζεται στέλεχος (stub). Το στέλεχος δημιουργείται από την εκάστοτε βιβλιοθήκη *RPC*. μιας συμβατικής (τοπικής) κλήσης διαδικασίας. Σειριοποιεί τα ορίσματα που του διαβιβάζονται, τα «συσκευάζει» με πρόσθετες πληροφορίες που απαιτούνται από τον διακομιστή και μεταδίδει ολόκληρο το πακέτο (που αποτελείται από τα σεριοποιημένα ορίσματα και τις επιπρόσθετες πληροφορίες) στη διεπαφή του δικτύου πελάτη (Client Network Interface).

## Μοντέλο Επικοινωνίας

### Μοντέλο Πελάτη – Διακομιστή στο Vanadium

Στο *Vanadium*, ένας διακομιστής αποτελείται από ένα τελικό σημείο (endpoint), μια διεύθυνση Vanadium που περιλαμβάνει ένα όνομα κεντρικού υπολογιστή, μια θύρα και έναν διαβιβαστή (dispatcher). Ο διαβιβαστής δρομολογεί κατάλληλα ένα εισερχόμενο αίτημα σε έναν εξουσιοδοτούντα (authorizer) και μια υπηρεσία. Το αίτημα φτάνει στην υπηρεσία **μόνο εάν το εγκρίνει ο εξουσιοδοτών**. Ένας διαβιβαστής έχει στην κατοχή του έναν εξουσιοδοτούντα και μία ή περισσότερες υπηρεσίες. Όλες οι υπηρεσίες περιέχουν **μόνο** τον κώδικα που υλοποιεί την λογική τους, δεν έχουν γνώση της ταυτότητας του εξουσιοδοτούντος που τις προστατεύει.

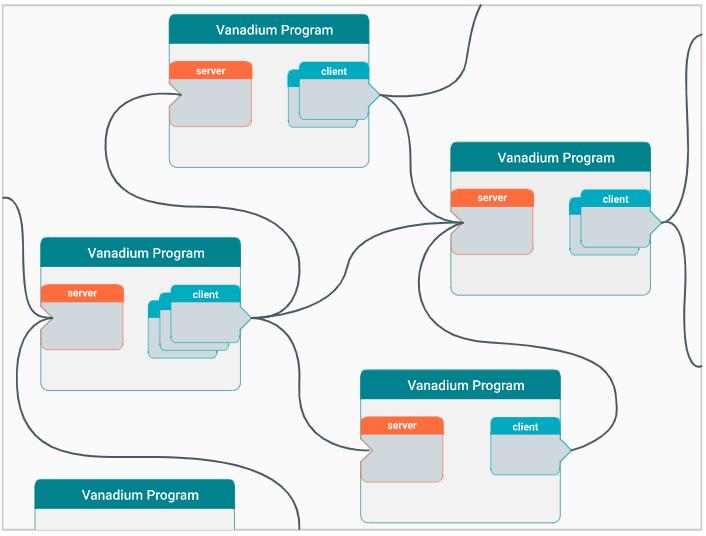


**Εικόνα xx**: Βασική Δομή του Μοντέλου

Πηγή: <https://vanadium.github.io/>

Ένας πελάτης είναι απλώς ένας κώδικας στελέχους (stub code), ο οποίος έχει την δυνατότητα πρόσβασης σε ένα ή περισσότερα τελικά σημεία στο δίκτυο (και κατ’ επέκταση υπηρεσίες) με βάση το όνομα που του έχει δώσει ο διακομιστής (άρα πρέπει να έχει προηγηθεί *ονοματοδοσία*).

Όπως είδαμε στο [*κεφάλαιο 4.1.1*](#_Γενικά), η βασική εκδοχή του μοντέλου πελάτη – διακομιστή συμπεριλαμβάνει έναν διακομιστή και πολλαπλούς πελάτες. Ωστόσο, **μια εφαρμογή *Vanadium* έχει την δυνατότητα να φιλοξενήσει οσουσδήποτε διακομιστές και πελάτες**, δημιουργώντας, έτσι, μία αρκετά πιο πολύπλοκη κατανεμημένη εφαρμογή. Η ιδέα είναι ότι ένα πρόγραμμα θα προσφέρει ορισμένες υπηρεσίες και θα επικοινωνεί με άλλα προγράμματα σε μια προσπάθεια παροχής αυτών των υπηρεσιών.



**Εικόνα xx**: Η περίπτωση δικτύου εφαρμογών

Πηγή: <https://vanadium.github.io/>

### Κλήση Απομακρυσμένης Διαδικασίας στο Vanadium

Όπως έχουμε ήδη αναφέρει, **το *Vanadium* κάνει χρήση του μοντέλου πελάτη – διακομιστή, συνδυάζοντάς το με την τεχνική της Κλήσης Απομακρυσμένης Διαδικασίας**. Σαν δομή, το RPC του ολοκληρωμένου πλαισίου *Vanadium* δε διαφέρει σε κάτι από εκείνη που είδαμε στο *κεφάλαιο 4.1.2*, αφού αποτελεί μια υλοποίηση αυτής με πρόσθετη κρυπτογραφική υποστήριξη.

**Στο *Vanadium RPC***, **υφίσταται συμμετρικός έλεγχος ταυτότητας και κρυπτογραφημένη, αμφίδρομη ανταλλαγή μηνυμάτων**. Η χρήση της υποδομής αυτής είναι **κατάλληλη για εφαρμογές κέντρου δεδομένων μεγάλης κλίμακας** (data centers, clusters), καθώς **και για εφαρμογές μικρότερης κλίμακας**.

Ιδιαίτερο ενδιαφέρον έχουν δύο επιμέρους συστατικά του *Vanadium RPC*, το ***Vanadium Object Marshalling*** (VOM) και το ***Vanadium Definition Language*** (VDL).

#### Vanadium Definition Language

**Το *Vanadium Definition Language*** (*VDL*) **αποτελεί μια γλώσσα προδιαγραφών** που χρησιμοποιείται για την περιγραφή της διεπαφής προγραμματισμού εφαρμογών ενός λογισμικού. Αποτελεί μια ειδική υλοποίηση της Γλώσσα περιγραφής διεπαφής (*Interface Definition Language, IDL*) και **επιτρέπει τη διαλειτουργικότητα μεταξύ στοιχείων λογισμικού που εκτελούνται σε διαφορετικά περιβάλλοντα**. Για παράδειγμα, μια εφαρμογή γραμμένη σε Java μπορεί να επιθυμεί να επικοινωνήσει με ένα backend γραμμένο στο Go και βρίσκεται στο cloud. Η χρήση του *VDL*, αν και **δεν είναι απαραίτητη**, συστήνεται.

Η πιο συνήθης χρήση του *VDL*, είναι για τον ορισμό διεπαφών. **Μια διεπαφή (interface) αντιπροσωπεύει ένα σύνολο υπογραφών μεθόδων, χωρίς όμως να συμπεριλαμβάνεται η υλοποίησή τους (το σώμα)**. Οι διεπαφές μπορούν να ενσωματώσουν και άλλες διεπαφές αναφέροντας μόνο το όνομα της προς ενσωμάτωση διεπαφής. Αυτό προσθέτει όλες τις μεθόδους της ενσωματωμένης διεπαφής στο σύνολο των μεθόδων.

Για να αντιληφθούμε καλύτερα την έννοια του *VDL*, ας δούμε το παράδειγμα ορισμού της διεπαφής μιας αριθμομηχανής (calculator):

/\* Κάθε διεπαφή μπορεί να ορίζει τις υπογραφές των μεθόδων \*/

**type** Calculator **interface** {

Add(x, y bignum.Int) (bignum.Int | error)

Sub(x, y bignum.Int) (bignum.Int | error)

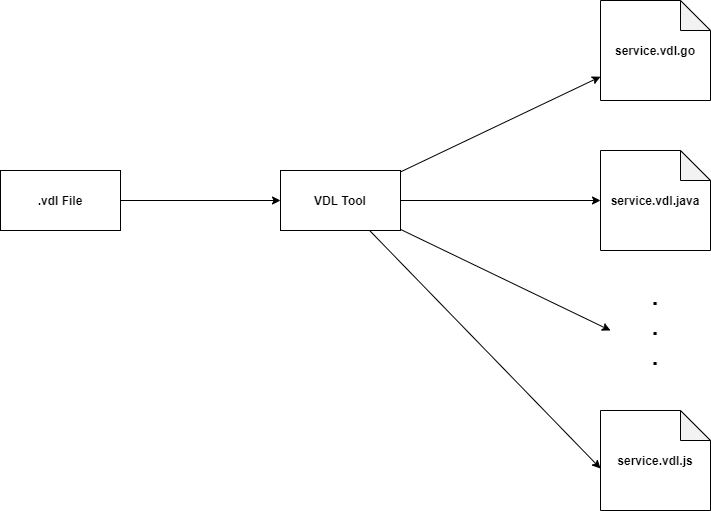
Multi(x, y bignum.Int) (bignum.Int | error)

Div(x, y bignum.Int) (bignum.Int | error)

}

Για να δημιουργήσουμε ένα πρόγραμμα, το οποίο θα κάνει αριθμητικούς υπολογισμούς (στην περίπτωσή μας μόνο για ακεραίους), πρέπει να προσδιορίσουμε τις 4 βασικές αριθμητικές πράξεις ως μεθόδους. Κάθε μέθοδος θα λαμβάνει 2 αριθμούς (ορίσματα μεθόδου) και θα επιστρέφει έναν νέο ακέραιο (bignum.Int, αντίστοιχος του long). Όπως προαναφέραμε, η υλοποίησή τους δεν περιλαμβάνεται.

Τέλος, αφού ολοκληρώσαμε το αρχείο *vdl* που περιέχει την διεπαφή, θα χρησιμοποιήσουμε το *εργαλείο VDL* (*VDL Tool*) για να παράξουμε τον κώδικα στελέχους του πελάτη και του διακομιστή (stub code), στην γλώσσα της επιλογής μας. Ουσιαστικά, το *εργαλείο VDL*, πρόκειται για έναν *μεταγλωττιστή πρωτοκόλλου* (*protocol compiler*), αντίστοιχο με τον *thrift* στο ολοκληρωμένο πλαίσιο *Apache Thrift*, ή τον *proto* στο ολοκληρωμένο πλαίσιο *GRPC*.



**Εικόνα xx**: Λειτουργία Εργαλείου VDL

#### Vanadium Object Marshalling

**Tο *Vanadium Object Marshalling*** (*VOM*) **αποτελεί μηχανισμό κωδικοποίησης** **/** **σειριοποίησης των κλήσεων του *Vanadium* *RPC***. Πρόκειται για μια ειδική υλοποίηση του μηχανισμού που αναφέραμε και στην [*γενικότερη περιγραφή της ιδέας της Κλήσης Απομακρυσμένης Διαδικασίας*](#_Κλήση_Απομακρυσμένης_Διαδικασίας). Το *VOM* σειριοποιεί, ουσιαστικά, κάθε τιμή που υφίσταται σε αρχεία [VDL](#_Vanadium_Definition_Language).

**Το *VOM* είναι μια δυαδική μορφή βασισμένη σε byte**, η οποία αποτελείται από μια ακολουθία μηνυμάτων. Κάθε μήνυμα είναι είτε ορισμός τύπου (type), είτε ορισμός τιμής (value). Προφανώς, οι τύποι καθορίζονται προτού τεκμηριωθούν από τιμές.

Προκειμένου να γίνει περισσότερο κατανοητός ο τρόπος λειτουργίας και αναπαράστασης του *VOM*, μπορούμε να ρίξουμε μια ματιά στο συντακτικό του:

*/\* Το πρώτο byte πάντα είναι ο αριθμός της έκδοσης \*/*

*VOM: version Message\**

*/\* Κάθε μήνυμα θα είναι ορισμός τύπου (TypeMsg) ή ορισμός τιμής (ValueMsg) \*/*

*Message: TypeMsg | ValueMsg*

*/\* Κάθε μήνυμα ξεκινά με την τιμή του typeid, η οποία μπορεί να είναι θετική (+typeid) ή αρνητική (-typeid). Όσα μηνύματα ξεκινούν με θετικό typeid, αποτελούν ορισμό τύπων, ενώ όσα μηνύματα ξεκινούν με θετικό typeid, αποτελούν ορισμό τιμής, σε ήδη ορισμένο τύπο \*/*

*TypeMsg: -typeid MainValue(string)*

*ValueMsg: +typeid MainValue*

##### Κωδικοποίηση

**Η βάση για την κωδικοποίηση *VOM* είναι το var128 (Variable-length quantity)**, ένας μη-προσημασμένος ακέραιος αριθμός μεταβλητού μήκους με μέγιστο μέγεθος 128 bit (δηλ. 16 bytes). Αυτή είναι μια κωδικοποίηση βασισμένη σε byte. Οι τιμές στο εύρος [0, 127] κωδικοποιούνται κατά λέξη σε ένα byte. Μεγαλύτερες τιμές χρησιμοποιούν το πρώτο byte για να κωδικοποιήσουν το μήκος byte της τιμής, με τα επόμενα byte να κωδικοποιούν την τιμή στην ελάχιστη big-endian αναπαράσταση της (το σημαντικότερο byte αποθηκεύεται στην "μικρότερη" θέση μνήμης).

Το πρώτο byte της κωδικοποίησης αποτελεί τον πυρήνα (crux) της κωδικοποίησης. Από τις 256 πιθανές καταστάσεις για το πρώτο byte, 128 καταστάσεις χρησιμοποιούνται για την αναπαράσταση των τιμών [0, 127], και άλλες 16 καταστάσεις χρησιμοποιούνται για να αντιπροσωπεύουν τα μήκη πολλαπλών byte [1, 16]. Αυτό αφήνει 112 καταστάσεις, οι οποίες προορίζονται για καταχωρήσεις ελέγχου.

| **var128 πρώτου byte** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **0x00..0x7F** Τιμή ενός byte | 0 | Τιμή εύρους [0, 127] | | | | | | |
|  |  |  |  |  |  |  |  |  |
| **0x80..0xBF** Control1 (64 καταχωρήσεις) | 1 | 0 | - | - | - | - | - | - |
|  |  |  |  |  |  |  |  |  |
| **0xC0..0xDF** Control2 (32 καταχωρήσεις) | 1 | 1 | 0 | - | - | - | - | - |
|  |  |  |  |  |  |  |  |  |
| **0xE0..0xEF** Control3 (16 καταχωρήσεις) | 1 | 1 | 1 | 0 | - | - | - | - |
|  |  |  |  |  |  |  |  |  |
| **0xF0..0xFF** Μήκος Πολλών byte (FF=1, FE=2, ...) | 1 | 1 | 1 | 1 | Μήκος εύρους [1, 16] | | | |

**Πίνακας xx**: Κωδικοποίηση var-128

Αξίζει να σημειωθεί ότι ενώ έχουν δεσμευτεί 112 καταστάσεις για τις καταχωρήσεις ελέγχου, μόλις 2 χρησιμοποιούνται:

|  |  |  |
| --- | --- | --- |
| **0xE0** | NIL | Αναπαριστά μη-υπάρχουσα τιμή (αντίστοιχο του NULL) |
| **0xE1** | END | Αναπαριστά το τέλος μιας σειράς (αντίστοιχο του EOF) |

**Το *VOM* υποστηρίζει τόσο την σειριοποίηση βασικών τύπων** (int, float, bool κλπ.), όσο **και τύπων ορισμένους από τον χρήστη**. Προφανώς, για τους τύπους ορισμένους από τον χρήστη, υπάρχει η προϋπόθεση ότι και οι δύο πλευρές (πελάτης και διακομιστής) γνωρίζουν τους τύπους αυτούς.

## Μοντέλο Ασφάλειας

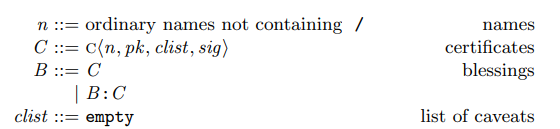
### Γενικά

*Υπό κατασκευή…*

### Principals & Blessings

Στο δίκτυο του Vanadium τα *Principals* αποτελούν τις οντότητες του δικτύου που αλληλοεπιδρούν μεταξύ τους. Τα *Blessings* είναι οι ιδιότητες κάποιας οντότητας, βάση των οποίων κρίνετε η δυνατότητα επικοινωνίας της με κάποια άλλη. Αν θεωρήσουμε σαν οντότητα έναν πάροχο υπηρεσίας, θα μπορούσε ο ίδιος να αδειοδοτήσει έναν τρίτο. Ο σκοπός της αδειοδότησης είναι να δώσει στον τρίτο, την δυνατότητα να καταναλώσει την υπηρεσία του. Πέραν της άμεσης σύνδεσης ενός Blessing ως άδεια επικοινωνίας μεταξύ Principal, χρησιμοποιούνται για την ευκολότερη κατανόησή των αδειών από ανθρώπους. Στην ουσία το *Blessing* είναι η αντιστοίχιση μιας άδειας πρόσβασης με κείμενο. Το κείμενο, είναι μορφής ονόματος ή ιδιότητας ώστε να παρομοιάζει την ανθρώπινη καθημερινότητα. Συμπεράνουμε λοιπόν, πως για κάθε επικοινωνία μεταξύ οντοτήτων μέσα στο δίκτυο Vanadium, είναι προηγουμένως απαραίτητη η αυθεντικοποίηση.

Για τον σκοπό της αυθεντικοποίησης, κάθε οντότητα έχει ένα ζευγάρι δημόσιου και ιδιωτικού κλειδιού. Το ιδιωτικό κλειδί του ζεύγους, ποτέ δεν μεταφέρετε ή διαμοιράζετε μέσω του δικτύου. Κύριο ρόλο στην διαδικασία έχουν τα δημόσια κλειδιά σε συνδυασμό με τις Ιδιότητες (Blessing). Μία οντότητα μπορεί να έχει μία ή περισσότερες Ιδιότητες, βάση των οποίων μπορεί να αποκτά δικαίωμα επικοινωνίας με άλλες οντότητες. Κάθε αίτημα πρόσβασης πρέπει να επιβεβαιωθεί και να εγκριθεί. Κατά την διαδικασία έγκρισης, δεν είναι αναγκαία η παροχή του δημόσιου κλειδιού, εφόσον ο αιτών μπορεί να αποδείξει την κατοχή κατάλληλης ιδιότητας (Blessing). Μία ιδιότητα αποτελείται από ένα σύνολο διαπιστευτηρίων.

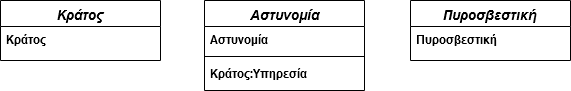


**Εικόνα xx**: Διαπιστευτήρια (Certificates), Ιδιότητες (Blessings) και Περιορισμοί (Caveats) [fosad16]

Στο παραπάνω διάγραμμα βλέπουμε από τι αποτελούνται τα Διαπιστευτήρια (C), οι Ιδιότητες (B) και οι Περιορισμοί (clist). Για τους Περιορισμούς θα γίνει αναφορά αργότερα, οπότε δεν θα εμβαθύνουμε ακόμα. Τα Διαπιστευτήρια αποτελούνται από τέσσερα πεδία, το όνομα (n), το δημόσιο κλειδί (pk), την λίστα των περιορισμών (clist) και την ψηφιακή υπογραφή (sig).

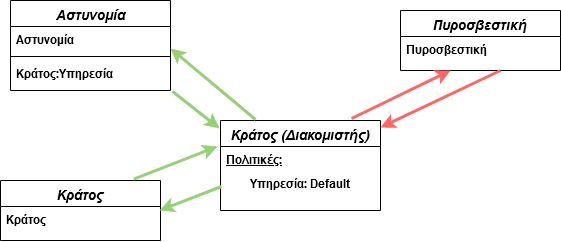
Οι ιδιότητες είναι μια λίστα Διαπιστευτηρίων, όπου κάθε διαπιστευτήριο χρησιμοποιείται για την επαλήθευση ενός κόμβου της Ιδιότητας. Για να γίνει πιο κατανοητό, μία Ιδιότητα είναι της μορφής Πάροχος:Ομάδα1:Ομάδα2:Κατηγορία1… Διαχωρίζοντας την Ιδιότητα στις άνω και κάτω τελείες καταλήγουμε στους κόμβους από τους οποίους αποτελείται. Κάθε κόμβος λοιπόν αντιστοιχίζεται με κάποιο Διαπιστευτήριο, ώστε να μπορεί να επιβεβαιωθεί. Εξαίρεση αποτελεί ο πρώτος κόμβος του Παρόχου, καθώς μπορεί να επιβεβαιωθεί από τα Διαπιστευτήρια του αμέσως επόμενου (στο παράδειγμα μας από τον κόμβο Ομάδα1).

Για την ευκολότερη κατανόηση της χρήσης και αυθεντικοποίησης των Οντοτήτων και Ιδιοτήτων θα υλοποιήσουμε ένα απλό παράδειγμα. Ας υποθέσουμε ότι έχουμε ένα δίκτυο Vanadium με τρεις τρεις οντότητες (*Principals*). Αυτές οι οντότητες είναι το **Κράτος**, η **Αστυνομία** και η **Πυροσβεστική**.



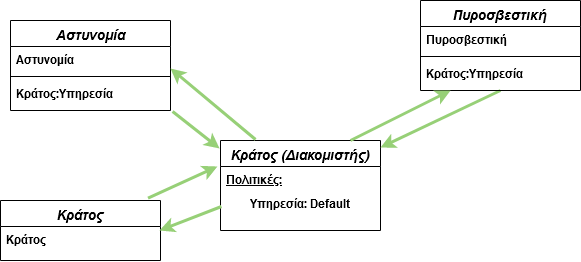
**Εικόνα xx**

Όπως αναφέραμε, στο δίκτυο του Vanadium, κάθε χρήστης είναι εν ’δυνάμει πελάτης και διακομιστής. Στο παράδειγμα μας, η οντότητα Κράτος έχει τον ρόλο του διακομιστή, οπότε οι άλλες οντότητες θα προσπαθήσουν να επικοινωνήσουν με αυτήν. Παρατηρούμε πως κάθε οντότητα έχει κάποιες ιδιότητες (*Blessings*). Η οντότητα Αστυνομία έχει τις ιδιότητες Αστυνομία και Κράτος:Υπηρεσία. Αντίστοιχα, η Πυροσβεστική έχει την ιδιότητα Πυροσβεστική. Μία οντότητα μπορεί να έχει διάφορες ιδιότητες, ανεξάρτητες μεταξύ τους, ώστε να επικοινωνεί ή αποκτά πρόσβαση σε διαφορετικά *Principals*. Για παράδειγμα η Αστυνομία και η Πυροσβεστική θα μπορούσαν να έχουν και την ιδιότητα Ένστολοι:Άμεση\_Δράση, η οποία θα ήταν ανεξάρτητη με την οντότητα του Κράτους. Βάση των προαναφερθέντων ιδιοτήτων, αποφασίζεται η πρόσβαση σε έναν διακομιστή. Ο διακομιστής αποφασίζει ποιος επιτρέπεται να έχει πρόσβαση, βάση των πολιτικών (*policies*) πρόσβασής του.



**Εικόνα xx**

Στην προσομοίωση της *εικόνας xx*, παρατηρούμε πως ο διακομιστής επιτρέπει την επικοινωνία με τις οντότητες του Κράτους και της Αστυνομίας και αρνείται πρόσβαση στην οντότητα της Πυροσβεστικής. Το Κράτος έχει πρόσβαση μιας και πρόκειται για τον εαυτό του, όμως η Αστυνομία αποκτά πρόσβαση διαφορετικά. Βλέπουμε πως η Αστυνομία, αντίθετα με την Πυροσβεστική, έχει την ιδιότητα Κράτος:Υπηρεσία. Επίσης παρατηρούμε πως το Κράτος ως διακομιστής, έχει την πολιτική αυθεντικοποίησης Υπηρεσία. Ως αποτέλεσμα ο διακομιστής επιτρέπει σε οντότητες με ιδιότητα (Blessing) Κράτος:Υπηρεσία να επικοινωνούν μαζί του. Αν το Κράτος προσδώσει την ιδιότητα Κράτος:Υπηρεσία και στην οντότητα της Πυροσβεστικής, τότε θα αποκτήσει και αυτή πρόσβαση.

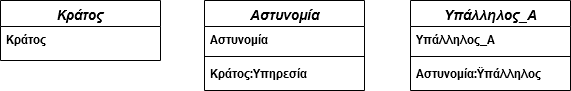


**Εικόνα xx**

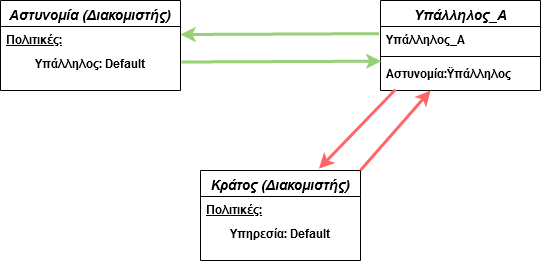
### Αναθέσεις

Στα πλαίσια του Vanadium, μία οντότητα μπορεί να μεταβιβάσει κάποια ιδιότητα της σε μία άλλη, με την διαδικασία της ανάθεσης. Η οντότητα που μεταβιβάζει την ιδιότητα, χρησιμοποιεί ένα νέο όνομα και το προσκολλά στην ήδη υπάρχουσα ιδιότητα.

Για παράδειγμα, ας συνεχίσουμε την δομή που είχαμε προηγουμένως με το Κράτος και την Αστυνομία. Αυτή την φορά όμως θα προσθέσουμε και έναν υπάλληλο που εργάζεται στην υπηρεσία της Αστυνομίας.

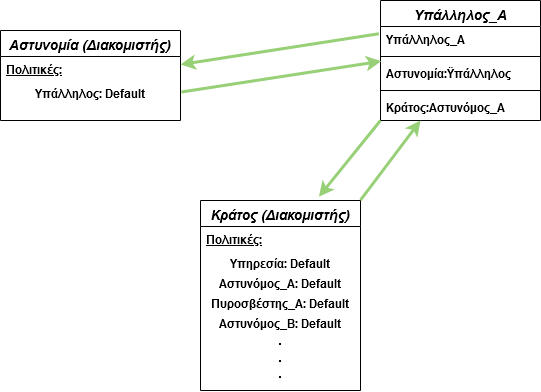


Ο υπάλληλος έχει δύο ιδιότητες, την Υπάλληλος\_Α και την Αστυνομία:Υπάλληλος καθώς εργάζεται στην οντότητα της Αστυνομίας. Στην περίπτωση που η Αστυνομία λειτουργήσει ως διακομιστής, θα περιμένουμε να έχει και την κατάλληλη πολιτική αυθεντικοποίησης ώστε να επιτρέπει στους υπαλλήλους της να έχουν πρόσβαση σε αυτή. Αν θεωρήσουμε ως πελάτη τον Υπάλληλο και ως διακομίστες το Κράτος και την Αστυνομία, έχουμε το παρακάτω αποτέλεσμα.



**Εικόνα xx**

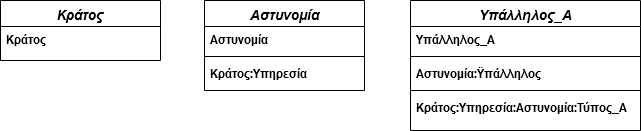
Δεδομένου ότι κάποιος υπάλληλος της Αστυνομίας, πιθανώς να χρειάζεται υπηρεσίες που προσφέρει το κράτος, θα πρέπει να αποκτήσει ιδιότητα (Blessing) ώστε να μπορεί να έχει πρόσβαση. Ο Υπάλληλος\_Α θα μπορούσε να παραλάβει την ιδιότητα κατευθείαν από το Κράτος. Σε αυτήν την περίπτωση το Κράτος θα έπρεπε να δημιουργήσει μια νέα πολιτική αυθεντικοποίησης για τους Υπαλλήλους της Αστυνομίας. Χρησιμοποιώντας αυτή την λογική, η οντότητα Κράτος θα έπρεπε να δίνει Blessing σε κάθε νέο Υπάλληλο. Επίσης το Κράτος θα έπρεπε να δημιουργεί μια νέα πολιτική για κάθε τύπο Υπαλλήλου κάθε Υπηρεσίας.



**Εικόνα xx**

Δεδομένου ότι μία Υπηρεσία μπορεί να έχει διαφορετικούς τύπους Υπαλλήλων, βλέπουμε πως η πολυπλοκότητα και η εξαρτήσεις από μια οντότητα σε μία άλλη αυξάνονται. Επιπρόσθετα οι εξαρτήσεις δεν είναι σωστές, καθώς κάποιος Υπάλληλος εξαρτάτε από το Κράτος και όχι από την Υπηρεσία στην οποία εργάζεται.

Η διαδικασία της ανάθεσης, έρχεται να λύσει αυτό το πρόβλημα. Αντί ο Υπάλληλος να παίρνει ιδιότητα από το Κράτος, του μεταβιβάζεται μία από την υπηρεσία που δουλεύει. (στην προκειμένη περίπτωση η Αστυνομία). Η Αστυνομία επομένως, αναθέτει στον Υπάλληλο την ιδιότητα Κράτος:Υπηρεσία:Αστυνομία:Τύπος\_Α.

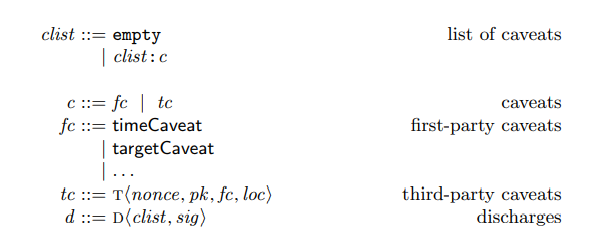


**Εικόνα xx**

Ο υπάλληλος, έχοντας πλέον την νέα του ιδιότητα, μπορεί να επικοινωνήσει με το Κράτος. Δεδομένου ότι το Κράτος έχει φροντίσει να έχει κατάλληλες πολιτικές αυθεντικοποίησης για την οντότητα της Αστυνομίας, θα επιτρέψει στον Υπάλληλο να έχει πρόσβαση.

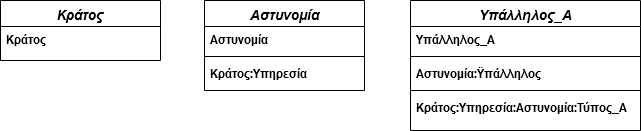
### Περιορισμοί

Με την παροχή της δυνατότητας ανάθεσης δικαιωμάτων σε τρίτους μέσω της μεταφοράς Ιδιότητας, προκύπτει θέμα ασφάλειας. Θα μπορούσε ο Υπάλληλος να έχει πρόσβαση σε όλες της δυνατότητες που δίνει το Κράτος στην Αστυνομία, και θα έπρεπε αυτό να συμβαίνει; Αυτόν τον προβληματισμό έρχονται να επιλύσουν οι Περιορισμοί (*Caveats*). Οι Περιορισμοί δίνονται από ένα *Principal* σε ένα άλλο κατά την διαδικασία της ανάθεσης. Η λειτουργικότητα που προσφέρουν είναι συγκεκριμένη και ο κύριος σκοπός τους είναι η διασφάλιση της σωστή λειτουργίας ενός *Principal* και των εξαρτήσεών του. Οι περιορισμοί μειώνουν τα δικαιώματα της οντότητας στην οποία έχει γίνει η ανάθεση.



**Εικόνα xx**

Όπως παρατηρούμε στην παραπάνω εικόνα, οι περιορισμοί είναι μέρος μίας λίστας. Σε αντίθεση με τα πεδία τιμών που είχαμε δει προηγουμένως, η λίστα των περιορισμών μπορεί να είναι κενή. Σε αυτή την περίπτωση, η οντότητα που κάνει ανάθεση της Ιδιότητας της, μεταφέρει επίσης και όλα τα δικαιώματα που τις έχουν δοθεί.



**Εικόνα** **xx**

Συνεχίζοντας το προηγούμενο παράδειγμα, θεωρούμε πως το *Principal* Αστυνομία, θέλει να περιορίσει τον Υπάλληλο\_Α. Μπορεί να θέσει σαν Περιορισμό (Caveat) ένα ωράριο εργασίας, οπού μετά το πέρας κάποιας ώρας, η ιδιότητα Κράτος:Υπηρεσία:Αστυνομία:Τύπος\_Α που έχει αναθέσει στον Υπάλληλο, παύει να ισχύει. Επίσης μπορεί να περιορίσει την πρόσβαση ενός κατόχου της ιδιότητας, σε συγκεκριμένες λειτουργικότητες του Principal, όπου όταν μία αίτηση στο Κράτος δεν είναι στις επιτρεπτές, να απορρίπτεται.

Η λειτουργία των περιορισμών είναι ιδιαιτέρα χρήσιμη, καθώς μπορεί να χρησιμοποιεί και τεχνικές απομακρυσμένης αδειοδότησης. Σε αυτή την περίπτωση η αρμοδιότητα ελέγχου και επιβεβαίωσης του περιορισμού, δίνεται σε κάποιον τρίτο. Για παράδειγμα η ιδιότητα του Υπάλληλου\_Α θα μπορούσε να είναι ενεργή μόνο όταν ο ίδιος βρίσκετε μέσα στο κτήριο της Αστυνομίας. Για να επιβεβαιωθεί αυτό, θα έπρεπε να υπάρχει ένα σύστημα, με τον ρόλο του τρίτου, που θα παρακολουθεί την τοποθεσία του Υπάλληλου σε σχέση με το κτήριο. Όταν λοιπόν ο Υπάλληλος κάνει μία αίτηση προς το Κράτος, θα πρέπει να πάρει μία επιβεβαίωση (*discharge*) ότι είναι εντός των επιτρεπτών ορίων. Αυτή η επιβεβαίωση μπορεί να έχει περιορισμούς, για να αποφευχθεί η λανθασμένη χρήση της. Για παράδειγμα θα μπορεί να έχει χρονικό περιθώριο εγκυρότητας χρήσης, ή περιορισμένο αριθμό χρήσεων.

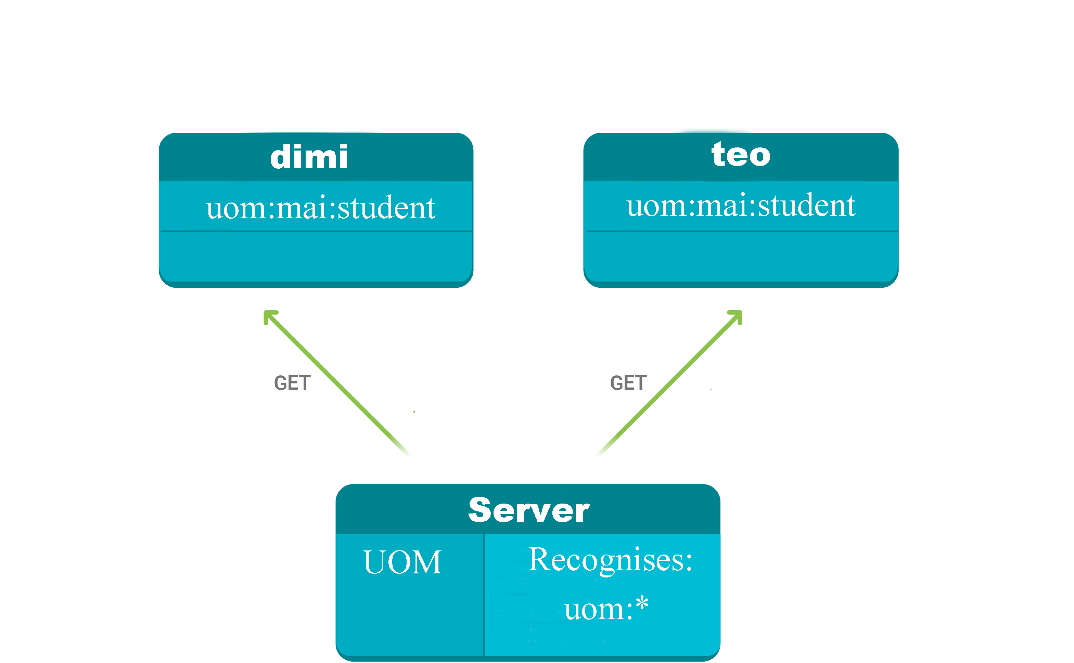
### Επαλήθευση των Blessings

**Ένα *blessing* θεωρείται έγκυρο στο πλαίσιο ενός RPC εάν ισχύουν όλες οι παρακάτω προϋποθέσεις:**

* Το *blessing* είναι κρυπτογραφικά έγκυρο, δηλαδή, κάθε πιστοποιητικό στην αλυσίδα πιστοποιητικών του συγκεκριμένου *blessing* έχει έγκυρη υπογραφή
* Όλοι οι περιορισμοί (*caveats*) που σχετίζονται με το *blessing* είναι έγκυροι στο πλαίσιο του RPC
* Το *blessing* αναγνωρίζεται από τον διακομιστή

Ένα *blessing* αναγνωρίζεται από μια εφαρμογή *Vanadium* εάν και μόνο εάν η εφαρμογή θεωρεί τη ρίζα του *blessing* (blessing root) ως αξιόπιστη για το όνομα του *blessing*. (Ρίζα του *blessing* αποτελεί το δημόσιο κλειδί του πρώτου πιστοποιητικού στην αλυσίδα πιστοποιητικών του *blessing*)

Για παράδειγμα, ένας διακομιστής μπορεί να θεωρήσει τη ρίζα ως έγκυρη σε όλα τα ονόματα των *blessings* που ξεκινούν με το *UOM*. Μια τέτοια εφαρμογή θα αναγνώριζε τότε τo *blessing* *UOM:mai:student* αν έχει τις ρίζες του στο , όπως φαίνεται στην *εικόνα 4-2-5-1.*



**Εικόνα xx**: Παράδειγμα Αναγνώρισης Blessing από τον Διακομιστή

Σε αυτή την περίπτωση, οι 2 πελάτες (*dimi* και *teo*) πραγματοποιούν αίτημα τύπου *GET*. Λόγω του ότι ο διακομιστής (server) αναγνωρίζει όλα τα ονόματα των *blessings* που ξεκινούν με *UOM*, το αίτημά και των δύο πελατών γίνεται δεκτό. Στην περίπτωση του παραδείγματος που παραθέσαμε, ο διακομιστής αναγνωρίζει μόνο αιτήματα τύπου *uom:\**, κάτι το οποίο δεν είναι σε καμία περίπτωση δεσμευτικό. Αντίστοιχα, θα μπορούσε να αναγνωρίζει *blessings* και ξεκινούν με άλλο αλφαριθμητικό, π.χ. *auth:\**.

### Εξουσιοδότηση

Σε μια κλήση απομακρυσμένης διαδικασίας (RPC call), πρέπει να ληφθούν δύο αποφάσεις, μία από κάθε πλευρά, πριν γίνει εξουσιοδότηση:

* **Ο πελάτης εμπιστεύεται τον διακομιστή αρκετά για να καλέσει μία απομακρυσμένη διαδικασία;**
* **Επιτρέπει ο διακομιστής τον πελάτη να καλέσει μια μέθοδο σε ένα αντικείμενο με τα παρεχόμενα ορίσματα;**

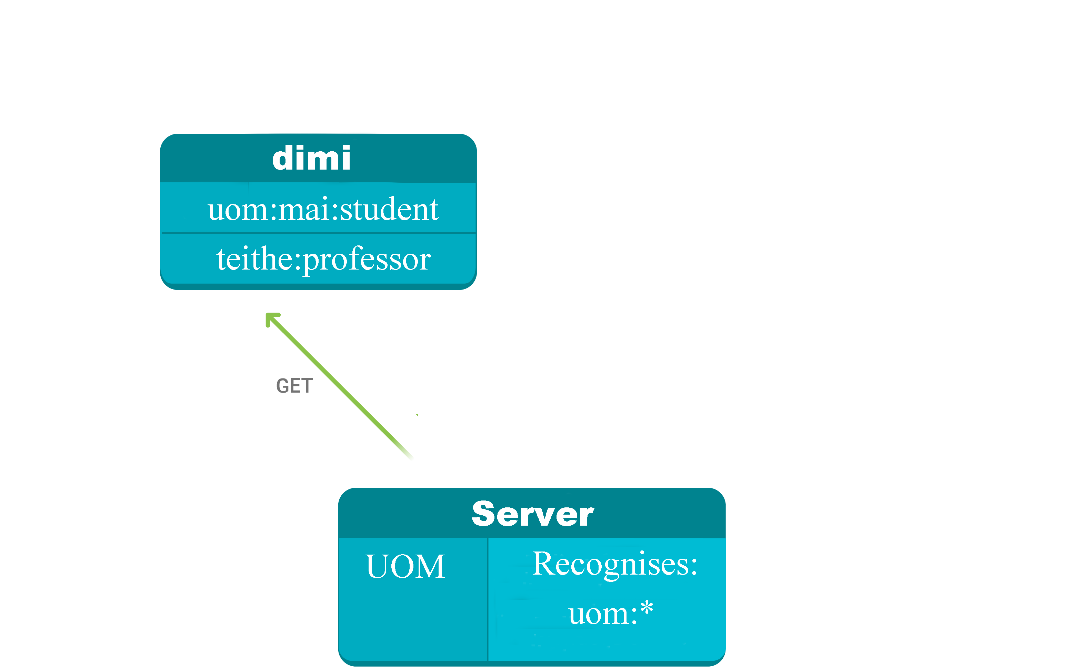
Στο πλαίσιο του *Vanadium*, **η εξουσιοδότηση βασίζεται σε επικυρωμένα ονόματα *blessing***(blessing names) και είναι **αμφίδρομη**.

Αυτό πρακτικά σημαίνει ότι ένας πελάτης θέλει να καλεί μια συγκεκριμένη (απομακρυσμένη) μέθοδο μιας υπηρεσίας, μόνο εάν ο διακομιστής κατέχει ένα *blessing*, το οποίο είναι συγκεκριμένης μορφής (π.χ. *UOM:mai:crypto*). Ομοίως, μια υπηρεσία μπορεί να επιτρέπει σε έναν πελάτη να καλεί μια (απομακρυσμένη) μέθοδο, μόνο εάν ο πελάτης κατέχει ένα *blessing*, το οποίο είναι συγκεκριμένης μορφής (π.χ. *UOM:mai:student*).

**Τα δημόσια κλειδιά των *principal* του πελάτη και του διακομιστή δε θα ληφθούν υπόψη από την στιγμή που υφίσταται *blessing* με ένα έγκυρο όνομα που αντιστοιχεί στην πολιτική εξουσιοδότησης του άλλου άκρου**. Κάθε άκρο επιβεβαιώνει το έγκυρο όνομα του *blessing* του άλλου άκρου, επικυρώνοντας όλους τους περιορισμούς που σχετίζονται με το *blessing* και επαληθεύοντας ότι το συγκεκριμένο *blessing* όντως αναγνωρίζεται.

**Ένα *principal* μπορεί να έχει συλλέξει πολλά *blessings***. Αντί να παρουσιάζει το σύνολο τον *blessings* (όλο τον κατάλογο) κάθε φορά που γίνεται αυθεντικοποίηση, με κόστος διαρροής ευαίσθητων πληροφοριών, **γίνεται επιλεκτική διαμοίραση των *blessings* που βρίσκονται στον κατάλογο, αναλόγως την ταυτότητα του άλλου άκρου**.

Ας δούμε το παράδειγμα της *εικόνας 4-2-6-1*, στο οποίο ο πελάτης *dimi*, έχει, πλέον, και το blessing *teithe:professor* στον κατάλογο των *blessings* του, μαζί με το *blessing* *uom:mai:student*, το οποίο ήδη κατείχε. Με βάση την δομή του *Vanadium*, **o διακομιστής που διαχειρίζεται το Πανεπιστήμιο Μακεδονίας (*UOM*)** **θα είναι σε θέση να διαβάσει μόνο το *blessing* *uom:mai:student* (και όχι το *teithe:professor*)**, όταν ο *dimi* του στείλει κάποιο αίτημα. Οποιοσδήποτε άλλος διακομιστής που επικοινωνεί με τον *dimi* δεν θα γνωρίζει ότι έχει αυτό το *blessing* από τον διακομιστή *UOM.* Κατ’ αντιστοιχία, **κανένας άλλος διακομιστής δε θα είναι σε θέση να γνωρίζει ότι ο *dimi* κατέχει *blessing* από τον διακομιστή *teithe,* εκτός από εκείνους που πρέπει να αυθεντικοποιηθεί με το *blessing teithe:professor***.



**Εικόνα xx**: Παράδειγμα Επιλεκτικής Διαμοίρασης των Blessings

(Ο διακομιστής βλέπει μόνο το uom:mai:student)

# Υλοποίηση

Στο παρόν κεφάλαιο, για λόγους επίδειξης του πλαισίου *Vanadium*,θα παρουσιαστεί μία εφαρμογή γραμμής εντολών ανταλλαγής άμεσων μηνυμάτων (chat app). Με τον τρόπο αυτό, θα γίνει αντιληπτό πώς μπορεί κανείς να χρησιμοποιήσει βασικές λειτουργίες που παρουσιάστηκαν στα προηγούμενα κεφάλαια. Η υλοποίηση είναι διαθέσιμη σε αποθετήριο στο GitHub: <https://github.com/teomaik/MSc_Crypto_ergasia>

## Εφαρμογή Ανταλλαγής Άμεσων Μηνυμάτων

Στην συγκεκριμένη εφαρμογή, για λόγους απλότητας, θεωρούμε ότι τόσο ο διακομιστής, όσο και ο πελάτης στέλνουν ένα μήνυμα τη φορά, δηλαδή η επικοινωνία τους είναι blocking.

### Κώδικας

#### VDL

Προτού αρχίσουμε να παρουσιάζουμε κάποιο κώδικα, θα κάνουμε χρήση του *Vanadium Definition Language*, προκειμένου να δημιουργήσουμε τον «σκελετό» της υπηρεσίας, την οποία πρόκειται να δημιουργήσουμε. Προφανώς, πρακτικά δεν θα είχε νόημα η χρήση του για ένα τόσο μικρό παράδειγμα. Η δημιουργία της διεπαφής της υπηρεσίας γίνεται ως εξής (αρχείο *chat.vdl*):

/\* Το Chat είναι η διεπαφή για την υπηρεσία άμεσων μηνυμάτων \*/

**type** Chat **interface** {

/\* Η SendMessage() στέλνει ένα μήνυμα στον διακομιστή (όρισμα msg τύπου string) και επιστρέφει μία απάντηση τύπου string (reply)

SendMessage(msg **string**) (reply **string** | **error**)

}

Η παραπάνω πληροφορία, αφορά τόσο τον πελάτη, όσο και τον διακομιστή, αφού δίνοντάς την ως είσοδο στο εργαλείο VDL (VDL Tool), παράγει κώδικα (ανάλογα με την γλώσσα της επιλογής μας, επιλέξαμε *Go*), ο οποίος αντιστοιχεί στον κώδικα στελέχους (stub code) του πελάτη και του διακομιστή (αρχείο *chat.vdl.go*, παραλείπεται).

#### Διακομιστής

###### Main

Καθώς πρόκειται για απλουστευμένη εφαρμογή, για την σύνταξη του κώδικα του διακομιστή θα χρειαστούμε 2 συστατικά (με βάση την περιγραφή που κάναμε στο [*κεφάλαιο 4.1*](#_Μοντέλο_Πελάτη_–)):

* Έναν εξουσιοδοτούντα (authorizer)
* Μια υπηρεσία (service) που θα περιέχει τις υλοποιήσεις

ctx, shutdown := v23.Init()

**defer** shutdown()

authorizer := security.DefaultAuthorizer() /\* Παίρνουμε τον απλό εξουσιοδοτούντα \*/

impl := internal.NewImpl() /\* Το αντικείμενο impl περιέχει τις υλοποιήσεις \*/

service := chat.ChatServer(impl) /\* Περνάμε ως παράμετρο στο service τις υλοποιήσεις \*/

ctx, server, err := v23.WithNewServer(ctx, \*name, service, authorizer) /\* Δημιουργία του server με τα 2 απαραίτητα συστατικά \*/

**if** err != **nil** {

log.Panic("Failure creating server: ", err)

}

log.Printf("Listening at: %v\n\n\n", server.Status().Endpoints[**0**])

<-signals.ShutdownOnSignals(ctx)

###### Υλοποίηση

Η υλοποίηση του μοναδικού service της εφαρμογής (ChatService), βρίσκεται στον υποκατάλογο του διακομιστή, internal. Αυτό αποτελεί ένα standard της γλώσσας *Go*, δηλαδή όταν επιθυμούμε να «κρύψουμε» τις υλοποιήσεις, τις τοποθετούμε σε ένα εσωτερικό πακέτο (internal package).

**type** impl **struct** {

}

**func** NewImpl() chat.ChatServerMethods {

**return** &impl{}

}

/\* Η μοναδική διαθέσιμη μέθοδος, αυτή θα καλέσει ο εκάστοτε πελάτης \*/

**func** (f \*impl) SendMessage(\_ \*context.T, \_ rpc.ServerCall, msg **string**) (**string**, **error**) {

log.Printf("%v", msg) /\* Εμφάνισε το μήνυμα στο παράθυρο το διακομιστή \*/

reply := getInput() /\* Μπλόκαρε μέχρι να δεχθείς είσοδο από το πληκτρολόγιο \*/

**return** reply, **nil** /\* Στείλε απάντηση \*/

}

Όπως παρατηρούμε, το *impl* που περάσαμε ως όρισμα στο service (στην [Main](#_Main)) αποτελεί μία κενή δομή. Αυτό συμβαίνει, καθώς στην υλοποίηση που κάναμε δεν έχουμε κάποιου είδους δεδομένα (π.χ. πίνακας με το ιστορικό συνομιλίας). Η υλοποίηση περιέχει μόνο μία μέθοδο: την *SendMessage()* (αγνοούμε την υλοποίηση της βοηθητικής συνάρτησης *get\_input()*).

Σε ό,τι αφορά την μέθοδο αυτή, δέχεται ως μοναδικό όρισμα από τον χρήστη ένα μήνυμα τύπου *string* (τα υπόλοιπα ορίσματα αναλαμβάνει να τα συμπληρώσει η βιβλιοθήκη του *Vanadium RPC* κατά την απομακρυσμένη κλήση).

#### Πελάτης

Ο κώδικας του πελάτη αποτελείται από μόνο ένα αρχείο (το main.go) και είναι παρόμοιος με τον κύριο κώδικα του διακομιστή:

**var** (

serverName = flag.String("serverName", "/127.0.0.1:2507", "Name of the server to connect to") /\* Κάθε φορά προσδιορίζουμε την διεύθυνση IP και την πόρτα του διακομιστή \*/

)

**func** main() {

ctx, shutdown := v23.Init()

**defer** shutdown()

client := chat.ChatClient(\*serverName) /\* Δημιουργία Client \*/

ctx, cancel := context.WithTimeout(ctx, time.Minute)

**defer** cancel()

**for** **true** { /\* Μέχρι ο πελάτης να αποσυνδεθεί (CTRL+C), δέξου είσοδο \*/

**var** msg **string** = getInput()

value, \_ := client.SendMessage(ctx, msg) /\* Η απομακρυσμένη κλήση μεθόδου, μπλοκάρει μέχρι να δεχθεί πίσω απάντηση (value) \*/

log.Printf("%v", value) /\* Εμφάνιση απάντησης \*/

}

}

Η λογική της ροής του κώδικα είναι αρκετά απλή:

* Δημιουργούμε έναν πελάτη τύπου *ChatClient*, συνδεόμαστε σε έναν διακομιστή, του οποίου τα στοιχεία τα έχουμε προκαθορίσει (πριν την εκτέλεση)
* Εφόσον βρεθεί ο διακομιστής και γίνει επιτυχής σύνδεση, μπορούμε να στέλνουμε μηνύματα στον διακομιστή, περιμένοντας να δεχθούμε σε κάθε μήνυμα μια απάντηση από τον διακομιστή (αφού κάναμε την παραδοχή της blocking επικοινωνίας). (\*)

*(\*): Προκειμένου να στέλνουμε μηνύματα στον διακομιστή, δεν αρκεί μόνο να γίνει επιτυχής σύνδεση, αλλά και να μας αναγνωρίσει ο εξουσιοδοτών (authorizer) του διακομιστή, την οποία επιθυμούμε να χρησιμοποιήσουμε (το chat service). Επειδή ο διακομιστής, όπως υλοποιήθηκε, χρησιμοποιεί τον προεπιλεγμένο εξουσιοδοτούντα (Default Authorizer), χρειάζεται να διαθέτουμε blessing από τον διακομιστή, προκειμένου να είναι σε θέση να μας αναγνωρίσει ο εξουσιοδοτών.*

### Εκτέλεση

Για να εκτελέσουμε χωρίς προβλήματα τις παρακάτω εντολές, θα πρέπει να βρισκόμαστε στον υποκατάλογο *chat*, που προηγείται τόσο αυτόν του διακομιστή, όσο και αυτόν του πελάτη. Επίσης, η κλωνοποίηση του αποθετηρίου πρέπει να γίνει στο κεντρικό κατάλογο του χρήστη (/home/<user>).

#### Διακομιστής

Καταρχάς, χρειάζεται να δημιουργήσουμε ένα principal για τον διακομιστή (άπαξ το κάνουμε αυτό), με την ακόλουθη εντολή:

*go run v.io/x/ref/cmd/principal create --with-passphrase=false --overwrite ~/MSc\_Crypto\_ergasia/vanadium-demo/chat/server/cred/dimi dimi*

Από την στιγμή που τρέξουμε αυτή την εντολή, **έχουμε δημιουργήσει**, ουσιαστικά, **ένα ζεύγος κλειδιών (δημόσιου, ιδιωτικού)**, το οποίο **είναι άρρηκτα συνδεδεμένο με το όνομα (χρήστη) *dimi***. Πάνω σε αυτό το *principal*, μπορούμε να συνδέσουμε και διάφορα *blessings*. Όλα τα αρχεία που αφορούν *principals* και *blessings* αποθηκεύονται στον υποκατάλογο cred.

Εμείς θα δημιουργήσουμε ένα μόνο *blessing* της μορφής *friend:<name>*, το οποίο θα αφορά το όνομα/χρήστη *teo*. Αυτό μπορούμε να το πετύχουμε με την ακόλουθη εντολή:

go run v.io/x/ref/cmd/principal bless \

--v23.credentials ~/MSc\_Crypto\_ergasia/vanadium-demo/chat/server/cred/dimi \

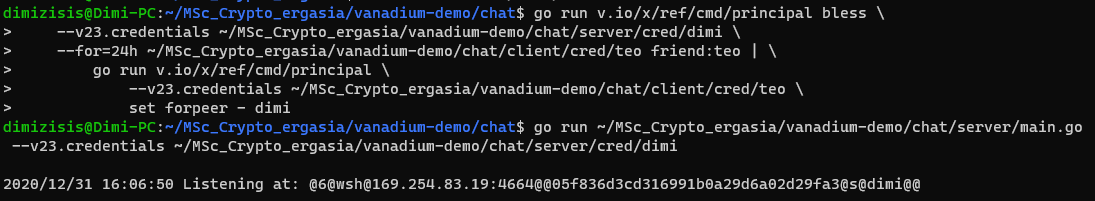
--for=24h ~/MSc\_Crypto\_ergasia/vanadium-demo/chat/client/cred/teo friend:teo

Επομένως, έχουμε δημιουργήσει ένα *blessing* για τον χρήστη *teo*, το οποίο θα είναι **σε ισχύ για 24 ώρες**.

Πλέον, είμαστε σε θέση να τρέξουμε τον διακομιστή μας, ώστε να ακούει σε μια συγκεκριμένη διεύθυνση IP και θύρα:

go run ~/MSc\_Crypto\_ergasia/vanadium-demo/chat/server/main.go --v23.credentials ~/MSc\_Crypto\_ergasia/vanadium-demo/chat/server/cred/dimi

Μετά την εκτέλεση των εντολών αυτών, θα πρέπει ο διακομιστής να είναι σε θέση να δεχτεί αιτήματα:



**Εικόνα xx**: Στιγμιότυπο Οθόνης Γραμμής Εντολών Διακομιστή

#### Πελάτης

Για τον πελάτη η διαδικασία είναι ακόμα απλούστερη, αφού χρειάζεται μόνο να δημιουργήσουμε το *principal* (ζεύγους δημόσιου-ιδιωτικού κλειδιού), το οποίο θα είναι «δεμένο» με το όνομα *teo*. Αυτό το πετυχαίνουμε με την ακόλουθη εντολή:

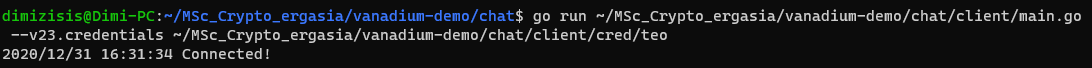
go run v.io/x/ref/cmd/principal \

--v23.credentials ~/MSc\_Crypto\_ergasia/vanadium-demo/chat/client/cred/teo

Τέλος, για να εκκινήσουμε τον πελάτη, τρέχουμε την εντολή:

go run ~/MSc\_Crypto\_ergasia/vanadium-demo/chat/client/main.go --v23.credentials ~/MSc\_Crypto\_ergasia/vanadium-demo/chat/client/cred/teo

Και η γραμμή εντολών του πελάτη θα πρέπει να εμφανίσει το μήνυμα επιτυχής σύνδεσης:

****

**Εικόνα xx**: Στιγμιότυπο Οθόνης Γραμμής Εντολών Πελάτη

Πλέον, μπορούμε να στέλνουμε (blocking) μηνύματα ανάμεσα σε πελάτη και διακομιστή.

# Συμπεράσματα

*Υπό κατασκευή…*

# Βιβλιογραφία

Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2017, 9). Authentication Protocols for Internet of Things: A Comprehensive Survey. *Security and Communication Networks, 2017*. doi:10.1155/2017/6562953

Hummen, R., Ziegeldorf, J. H., Shafagh, H., Raza, S., & Wehrle, K. (2013). Towards Viable Certificate-Based Authentication for the Internet of Things. *Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy* (σσ. 37–42). New York, NY, USA: Association for Computing Machinery. doi:10.1145/2463183.2463193

Kim, H., & Lee, E. A. (2017). Authentication and Authorization for the Internet of Things. *IT Professional, 19*, 27-33. doi:10.1109/MITP.2017.3680960

Lee, J., Lin, W., & Huang, Y. (2014). A lightweight authentication protocol for Internet of Things. *2014 International Symposium on Next-Generation Electronics (ISNE)*, (σσ. 1-2). doi:10.1109/ISNE.2014.6839375

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013, 3 10). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber Security and Mobility, 1*, 309–348.

Ramos, J. H., Jara, A., Marín, L., & Gómez-Skarmeta, A. F. (2013). Distributed Capability-based Access Control for the Internet of Things. *J. Internet Serv. Inf. Secur., 3*, 1-16.

Taly, A., & Shankar, A. (2016). Distributed Authorization in Vanadium. Στο A. Aldini, J. Lopez, & F. Martinelli (Επιμ.), *Foundations of Security Analysis and Design VIII: FOSAD 2014/2015/2016 Tutorial Lectures* (σσ. 139–162). Cham: Springer International Publishing. doi:10.1007/978-3-319-43005-8\_4

Wu, D. J., Taly, A., Shankar, A., & Boneh, D. (2016). Privacy, Discovery, and Authentication for the Internet of Things. Στο I. Askoxylakis, S. Ioannidis, S. Katsikas, & C. Meadows (Επιμ.), *Computer Security – ESORICS 2016* (σσ. 301–319). Cham: Springer International Publishing.

Taly, A., Practical Distributed Authorization, Two day course at the 2016 International School on Foundations of Security Analysis and Design, Bertinoro, Italy (Aug. 29 - Sep. 2)

Zhang, Hai. (2013). Architecture of Network and Client-Server model.

[Vanadium Official WebSite](https://vanadium.github.io/)

[Προσπελάστηκε 29/11/2020]