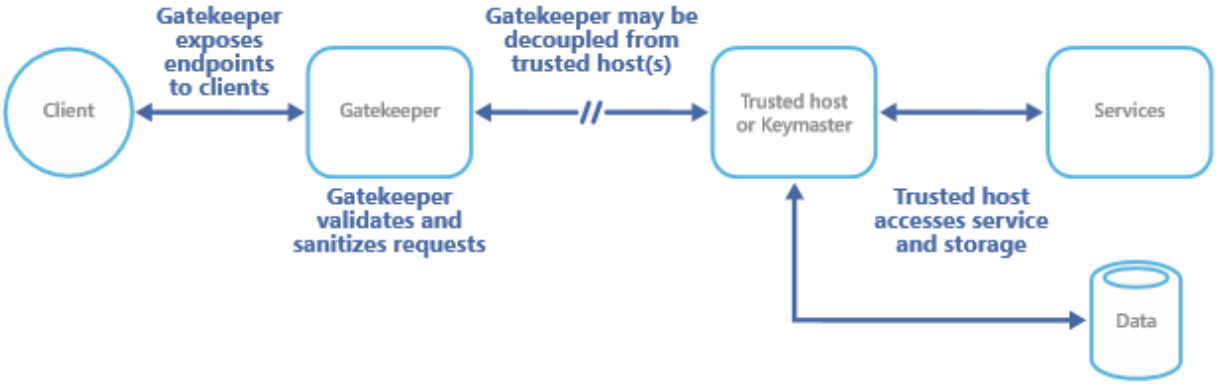
Cloud Design Patterns

Προσφέρουν ανθεκτικότητα, ασφάλεια, επεκτασιμότητα, επίδοση, διαθεσιμότητα σε υπηρεσίες που έχουν υλοποιηθεί χρησιμοποιόντας τα.

Παρουσιάζονται συνδυαστικά τα πρότυπα Gatekeeper και Vallet key.

Αυτό προσέφερε στην εφαρμογή επαυξημένη ασφάλεια και πιθανή επεκτασιμότητα.

Gatekeeper



Gatekeeper

- Λειτουργεί σαν ενδιάμεση υπηρεσία μεταξύ του client και της υπηρεσίας που προσφέρει τα δεδομένα σε αυτον.
- Έτσι ο χρήσης ή πιθανός επιτιθέμενος δεν έχει εύκολη πρόσβαση στα δεδομένα.

Gatekeeper

Το πρότυπο αυτό έχει υλοποιήθεί ως ένα service το οποίο μετά απο κλήση του client κάνει το ίδιο μία κλήση στο backend service που διαχειρίζεται τα δεδομένα, λαμβάνει τα δεδομένα και τελος τα στέλνει στο χρήστη.

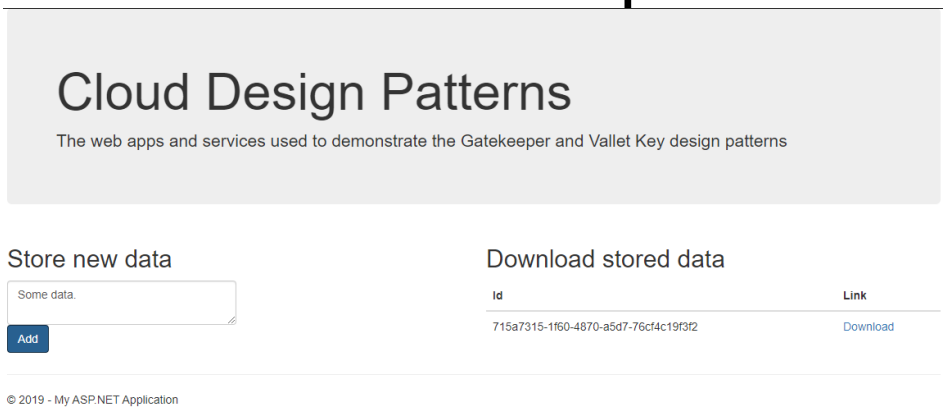
Το service αυτό δεν έχει άμεση πρόσβαση στα δεδομένα ή σε κωδικούς ασφαλείας, έτσι αν ένας επιτιθέμενος πάρει πρόσβαση στο service δεν έχει περαιτέρω δυνατότητα να βλάψει το συνολικό συστημα.

Gatekeeper

Αλλες πιθανές χρήσεις:

- Εξισορρόπηση φορτίου (loadbalancing) μεταξύ διαφορετικών υποστάσεων του backend service.
- Κεντρική καταγραφή όλων τών κλήσεων που έρχονται στην υπηρεσία (logging).
- Επαλήθευση (validation) και φιλτράρισμα των κλήσεων.

Gatekeeper



Στο γραφικό περιβάλλον ο χρήστης μπορεί να αποθηκεύσει δεδομένα καθώς και να ανακτήσει δεδομένα που έχουν αποθηκευτεί παρελθοντικά.
Το γραφικό παρέχεται στην παρούσα υλοποίηση από τον ίδιο τον gatekeeper αλλά αυτό αλλάζει εύκολα καθώς η διεπαφή γίνεται με http κλήσεις.
Έτσι θα μπορούσαμε να έχουμε διαφόρων ειδών clients να επικοινωνούν με το κεντρικό gatekeeper service.

Gatekeeper

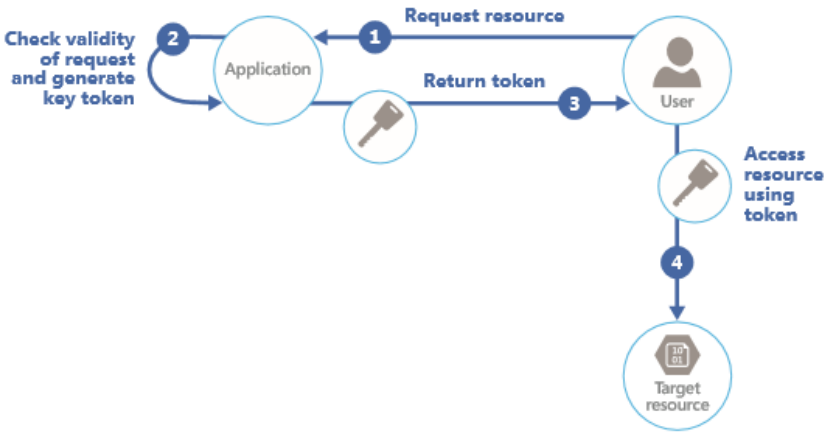
```
0 references
public async Task<string> AddBlob(string text)
{
    var tokenServiceEndpoint = ConfigurationManager.AppSettings["newBlobEndpointUrl"];
    try
    {
        // Get the uri to the data managing service
        var uri = new Uri(tokenServiceEndpoint);
        var request = HttpWebRequest.Create(uri);
        // http request between the services provides a safety layer
        var response = await request.GetResponseAsync();
        var responseString = string.Empty;
        var serializer = new DataContractJsonSerializer(typeof(StorageEntitySas));
        var blobSas = (StorageEntitySas)serializer.ReadObject(response.GetResponseStream());
        // create storage credentials object based on SAS
        var credentials = new StorageCredentials(blobSas.Credentials);
        // using the returned SAS credentials and BLOB Uri create a block blob instance to upload
        var blob = new CloudBlockBlob(blobSas.BlobUri, credentials);
        await blob.UploadTextAsync(text);
        Console.WriteLine("Blob upload successful: {0}", blobSas.Name);
        return blob.Name;
    }
    catch
    {
        throw;
    }
}
0 references
public async Task<string> GetBlob(string id)
{
    var tokenServiceEndpoint = ConfigurationManager.AppSettings["readBlobEndpointUrl"];
    var uri = new Uri(tokenServiceEndpoint+id);
    WebClient webClient = new WebClient();
    var res = webClient.DownloadString(uri);
    return res;
}
```

Εδώ βλέπουμε τους 2 controllers που παρέχει το Gatekeeper service.

Οπως βλέπουμε όλες οι κλήσεις του client καταλήγουν στο gatekeeper έτσι ο client δέν έχει γνώση της τοπολογίας της υπηρεσίας μας.

Request URL: http://localhost:8080/Home/GetBlob/872b982d-6760-436b-9d47-498683ce9964
Request Method: GET
Status Code: 200 OK
Remote Address: 127.0.0.1:8080
Request URL: http://localhost:8080/Home/AddBlob
Request Method: POST
Status Code: 200 OK
Remote Address: 127.0.0.1:8080

Valet Key



Τον ρόλο του User τόσο για το application όσο και για το Target resource παιρνει το gatekeeper service.

Valet key

- Χρήση “κλειδιού” για περιορισμένη χρονικά πρόσβαση σε έναν πόρο (δεδομένα, ταινίες, υπηρεσίες)
- Επιτρέπει την διασπορά των δεδομένων σε διαφορετικές υπηρεσίες hosting, αυξάνει την επεκτασιμότητα και την επίδοση της εφαρμογής.

Valet Key

Καθώς η μεταφορά δεδομένων δεν γίνεται από-πρός τον application server δέν καταναλώνει περιττούς πόρους.

Έτσι μεγάλος αριθμός χρηστών μπορεί να καλυφθεί από έναν βασικό server.

Έτσι το πρότυπο αυτό προσφέρει οικονομία πόρων στο σύστημα.

Valet key

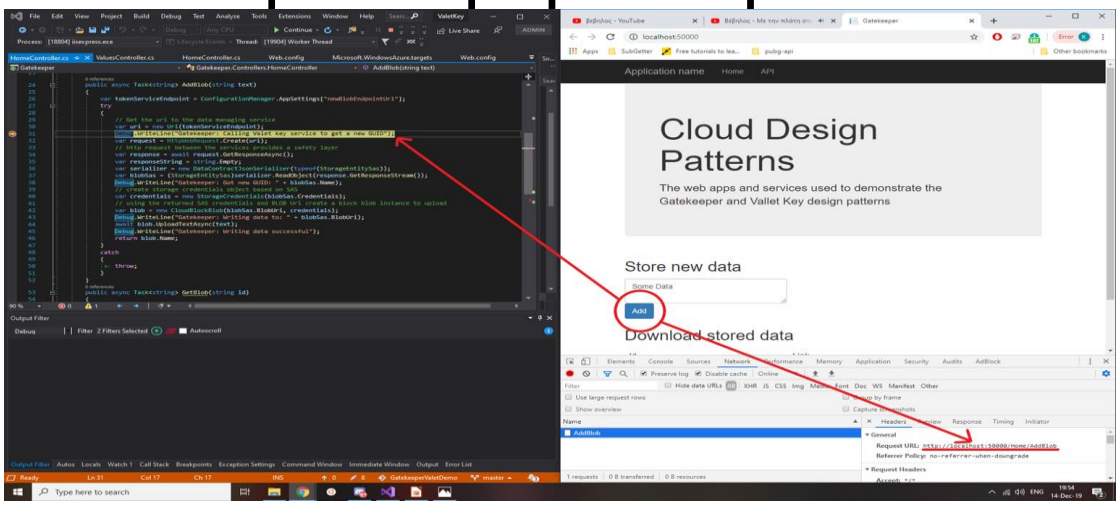
Το service παρέχει tokens με δικαιώματα εγγραφής-ανάγνωσης για 5 λεπτά στο Azure Cloud Storage.

Αυτό παρέχει άμεση σύνδεση client – storage που αυξάνει πολύ την απόδοση χώρις όμως να μειώνει την ασφάλεια καθώς ο χρήστης έχει μόνο το κλειδί για το resource στο οποίο του παραχωρήθηκε άδεια και μόνο για περιορισμένο χρόνο.

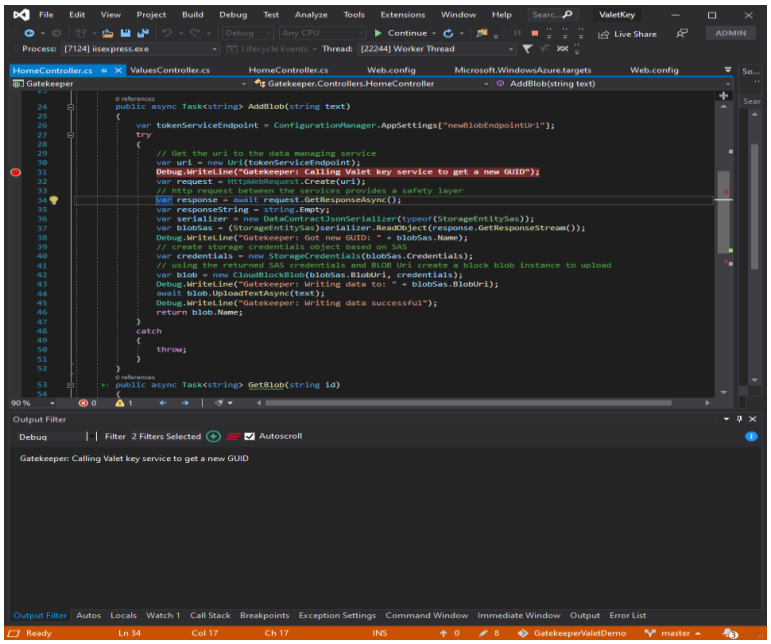
Valet key

Για ακόμα μεγαλύτερη ασφάλεια το service που παρέχει τα κλειδιά θα μπορούσε να βρίσκεται σε διαφορετικό υπολογιστή από τον gatekeeper, αυτό όμως θα δυσκόλευε την παρουσίαση της εργασίας ώς σύνολο.

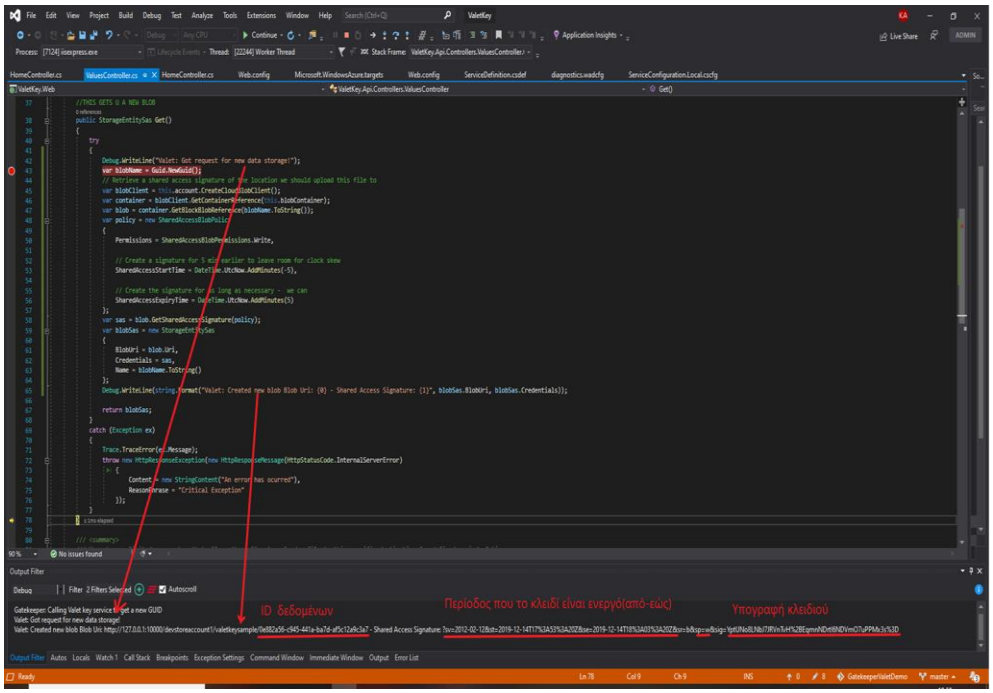
Προσθήκη δεδομένων



Πατώντας το κουμπί μία κλήση γίνεται στο gatekeeper service με τα δεδομένα που θέλει να αποθηκεύσει ο χρήστης.

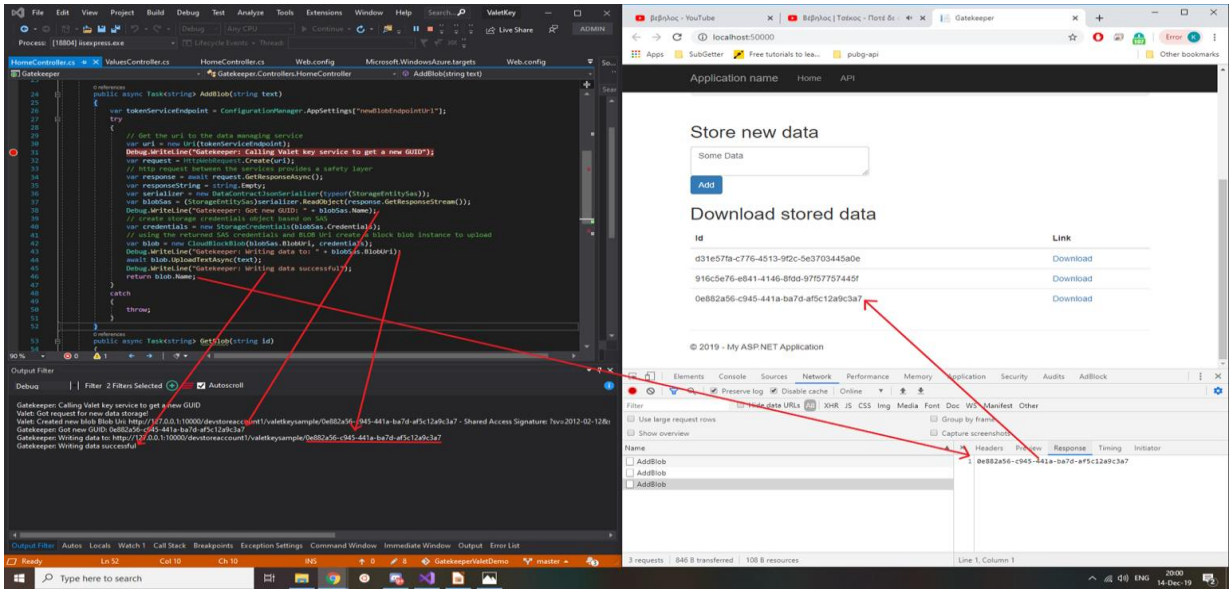


Το gatekeeper service κάνει κλήση στο valet service ώστε να του δωθεί ένα νέο blob στο οποίο να γράψει τα δεδομένα.



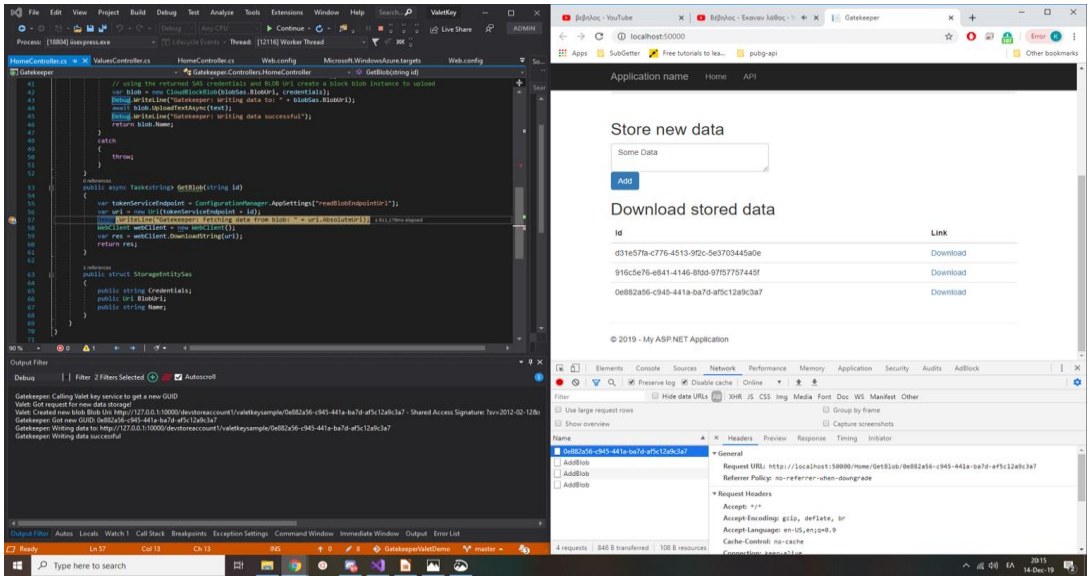
Το Valet service δημιουργεί ένα νέο blob στο azure storage καθώς και ένα κλειδί με διάρκεια ζωής 5 λεπτά και δικαίωμα εγγραφής για το blob.

Έπειτα αποστέλει το blob και το κλειδί στο gatekeeper ώς απάντηση στην κλήση.

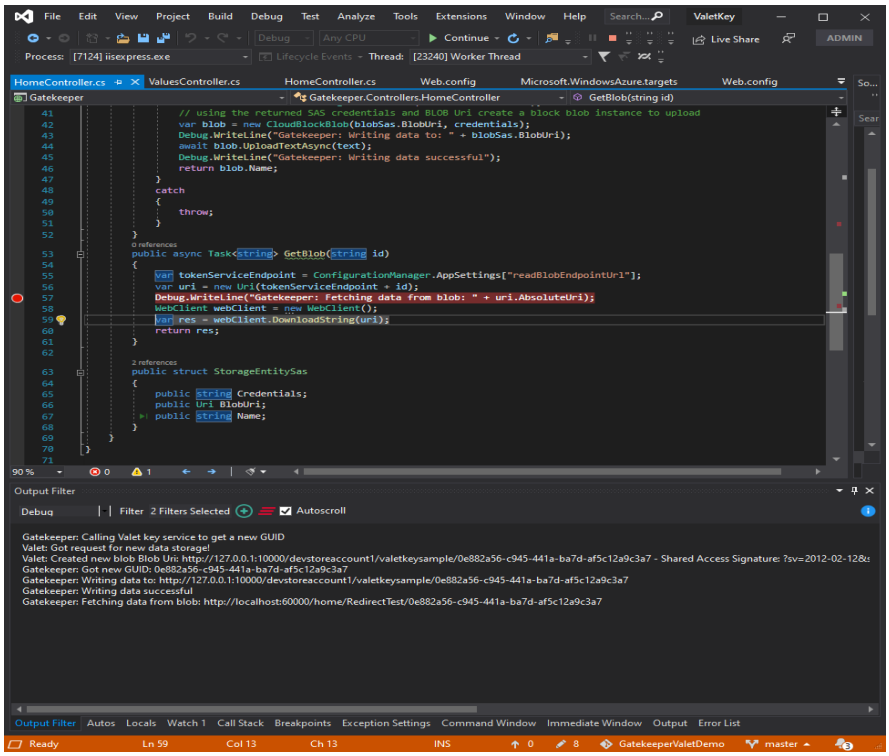


Το gatekeeper αφού πάρει το κλειδί για το blob γράφει σε αυτό τα δεδομένα και επιστρέφει το id του blob στον client.
Ο client μόλις λάβει το id σαν απάντηση, το προσθέτει στον πίνακα με τα κλειδιά που έχει δημιουργήσει.

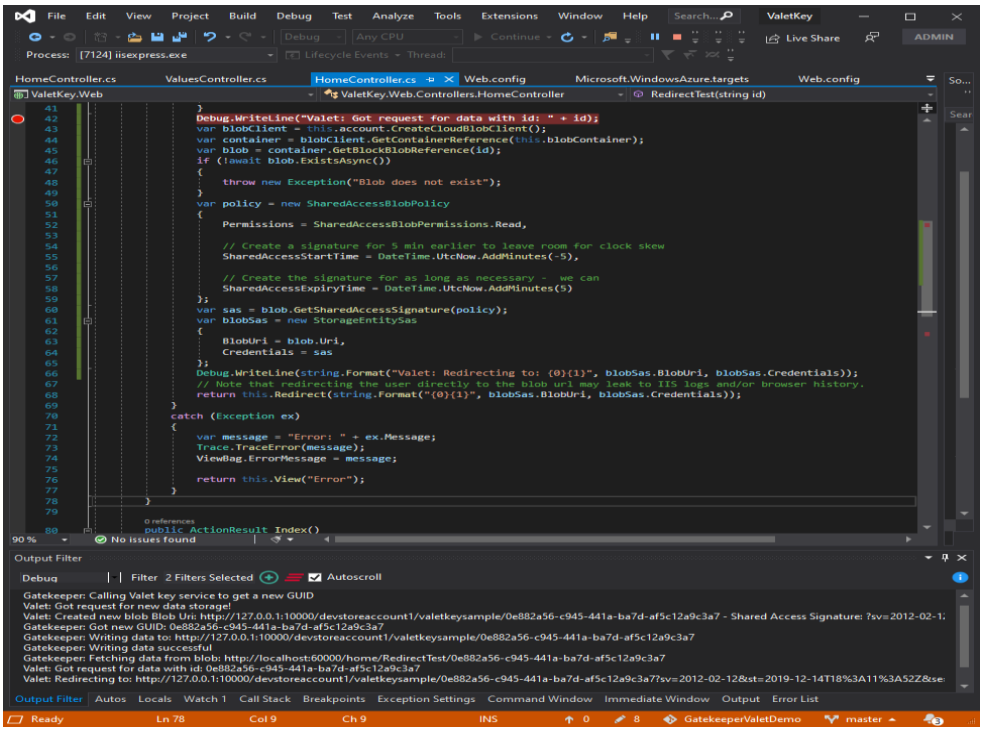
Λήψη Δεδομένων



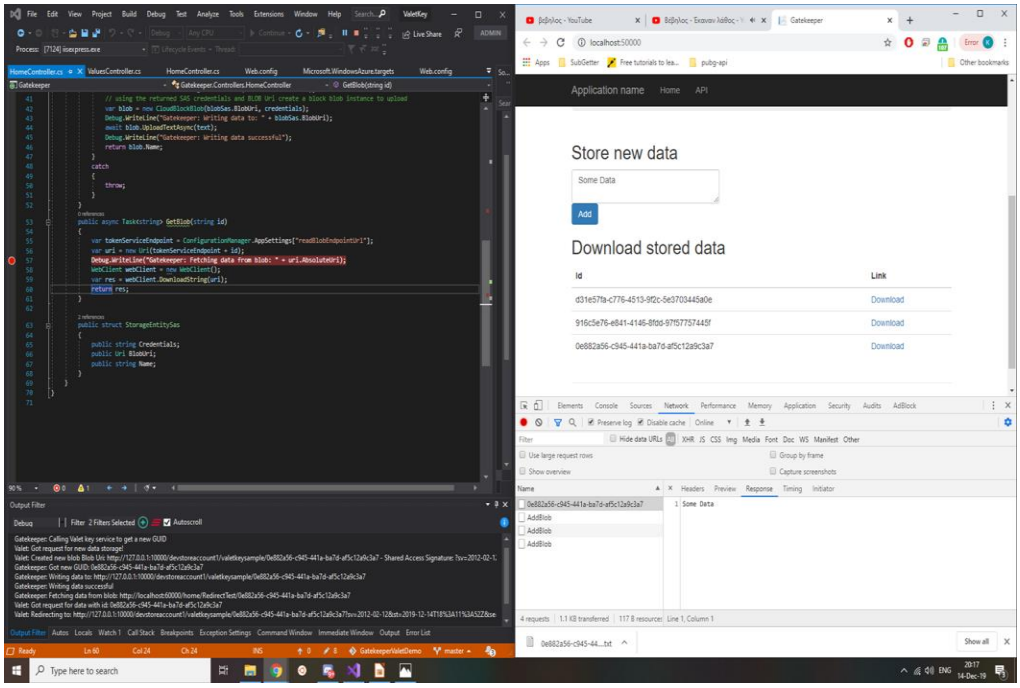
Κάνοντας click στο Download μία κλήση γίνεται από τον client στο gatekeeper service.



Το gatekeeper service κάνει μία κλήση προς το valet key service ζητώντας το uri και ένα κλειδί για το blob που ζήτησε ο χρήστης.



Το valet service όταν δεχτεί την κλήση δημιουργεί ένα κλειδί για το blob με 5 λεπτά διάρκεια ζωής και δικαίωμα ανάγνωσης μόνο.
Έπειτα κάνει redirect την κλήση στο azure storage χρησιμοποιόντας το κλειδί που έφτιαξε.



Με το redirect το gatekeeper αποκτά τα δεδομένα που ζητήθηκαν τα οποία επιστρέφει ώς απάντηση στον client.

Ο client τέλος δημιουργεί ένα νέο αρχείο για τον χρήστη που περιέχει τα δεδομένα που ζήτησε.

Παρατηρούμε τα εξής:

- Ο client έχει πρόσβαση μόνο στο gatekeeper
- Το gatekeeper έχει πρόσβαση στο valet και στο azure storage. Αλλά δεν μπορεί να δημιουργήσει κλειδία για να γράψει ή να διαβάσει δεδομένα
- Το valet key service είναι το μόνο που έχει credentials ώστε να δημιουργεί κλειδιά στο azure storage και ελέγχει στα κλειδιά τη διάρκεια ζώης καθώς και τα δικαιώματα.

ΠΡΟΗΓΜΕΝΟ ΛΟΓΙΣΜΙΚΟ ΥΠΗΡΕΣΙΩΝ ΙΣΤΟΥ

Κωνσταντίνος Αρώνης
ΑΜ: 18002