

**ANKARA ÜNİVERSİTESİ**  
**MÜHENDİSLİK FAKÜLTESİ**  
**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**



**X.509 V3 SERTİFİKA ÜRETEN WEB SİTESİ**

**BERAT ERKAN ELÇELİK**  
**18290758**

**18.10.2022**

## ÖZET

Projenin amacı bir kullanıcının kendi X.509 V3 tipinde dijital sertifikasını üretebilmesini, sonrasında istediği formatta indirebilmesini ve diğer formatlar arasında geçiş yapabilmesini sağlayan bir web projesinin gereksinimidir. Bu proje kapsamında geliştirme ortamı olarak Visual Studio 2019 kullanılmıştır. Sertifikaların üretilmesi için System.Security.Cryptography kütüphanesinden yararlanılmıştır. Web sitesi oluşturulması için ise MVC kullanılmıştır. Veri tabanı ile ilişkili olan bu projede Microsoft SQL Server 2018 kullanılmıştır. Entity framework yöntemlerinden CodeFist yapısı kullanılmıştır çünkü kod yazarak oluşturmak diğer yöntemlere göre daha öğretici ve daha kullanımı kolaydır. Birden fazla kullanıcının aynı anda siteye erişimi için ise task yapısı kullanılmıştır. Raporda oluşturulan sayfaların nasıl çalıştığı ve hangi işlevleri yerine getirdiği detaylı bir şekilde açıklanmıştır. Proje verilen sürede tamamlanıp istenen gereksinimler yerine getirilmiştir.





## **1.GİRİŞ**

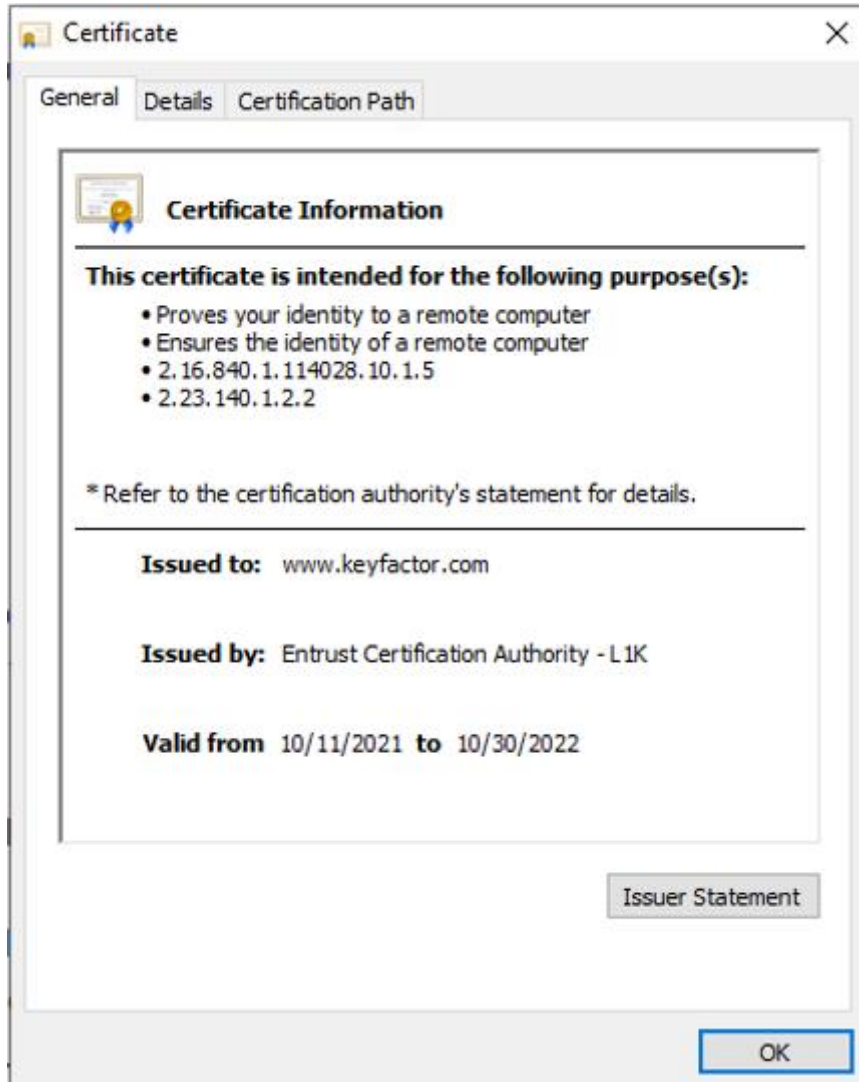
Bu projede web sitelerinin güvenilirliğini kanıtlayan dijital sertifikayı üreten Web uygulaması geliştirilmiştir. Dijital Sertifika siteye giriş yapan kullanıcıya, sitenin kullanıcının ulaşmak istediği adresten yollandığını kanıtlayan belgedir. Dijital Sertifikalar sayesinde kötü amaçlı bilgisayar korsanlarının siteyi değiştirip kullanıcıya iletilmesi engellenmesi sağlanır. Bu projenin asıl amacı; kullanıcıların bir web sitesi sayesinde kendi dijital sertifikalarını kolayca oluşturup, istediği sertifika formatında indirip, sertifika formatları arasında değişim yapabilmelerini sağlamaktır. Bu raporun amacı ise geliştirilen bu projenin amacının, yapılış aşamalarının, kullanımının, işlevinin ve oluşturulurken kullanılan yöntemlerin açıklanmasıdır. Bu raporda aynı zamanda Proje görevlendirmelerinin ne kadarının tamamlandığı ve nelerin geliştirilerek eklendiği bilgisi de verilecektir.

## **2.PROJENİN GEREKSİNİMLERİ**

### **2.1 Dijital Sertifika**

“Dijital sertifika, şifreleme anahtar çiftlerini web siteleri, kişiler veya kuruluşlar gibi varlıklarla ilişkilendirmek için kullanılan bir dosya türüdür. Genel güven gerekliyse, güvenilir Sertifika Yetkilisi (CA) bunları doğrular ve dijital sertifikalar aracılığıyla kriptografik çiftlerle ilişkilendirir.

Bahsedilen anahtar çifti bir ortak anahtar ve bir özel anahtardan oluşur. Ortak anahtar sertifikaya dahil edilirken, özel anahtar güvenli tutulur. Özel anahtarın sahibi daha sonra belgeleri imzalamak için kullanabilir ve ortak anahtar bu imzaların geçerliliğini doğrulamak için kullanılabilir. Üçüncü taraflar, ortak anahtarı yalnızca özel anahtarın sahibinin şifreleyebileceği şifrelenmiş bilgiler göndermek için de kullanabilir.”( Wilson C., 2020)

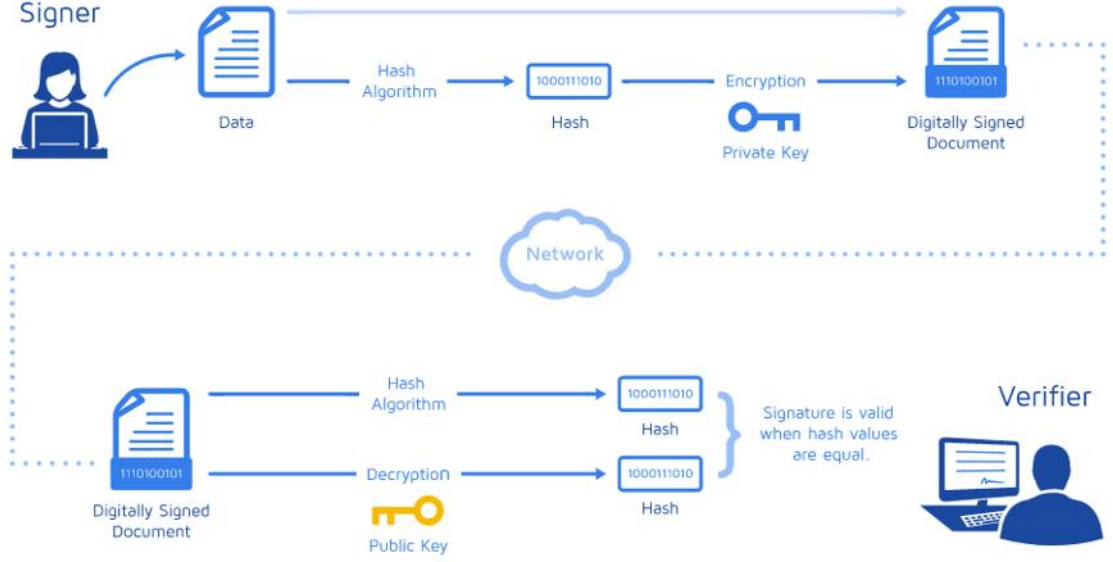


Şekil 1.1. Örnek Dijital sertifika

Dijital sertifikalar bir dijital imza tarafından imzalanması gerekir. Bu sayede güvenilirliklerini kanıtlamış olurlar.

## 2.2 Dijital İmza

“Dijital imza, elektronik ortamda kimlik doğrulama amacıyla kullanılan yasal bir kimlik doğrulama yöntemidir.”( Anonim,2022)



Şekil 2.1. Dijital İmza Adımları

## 2.3 Dijital İmzalar Nasıl Çalışır?

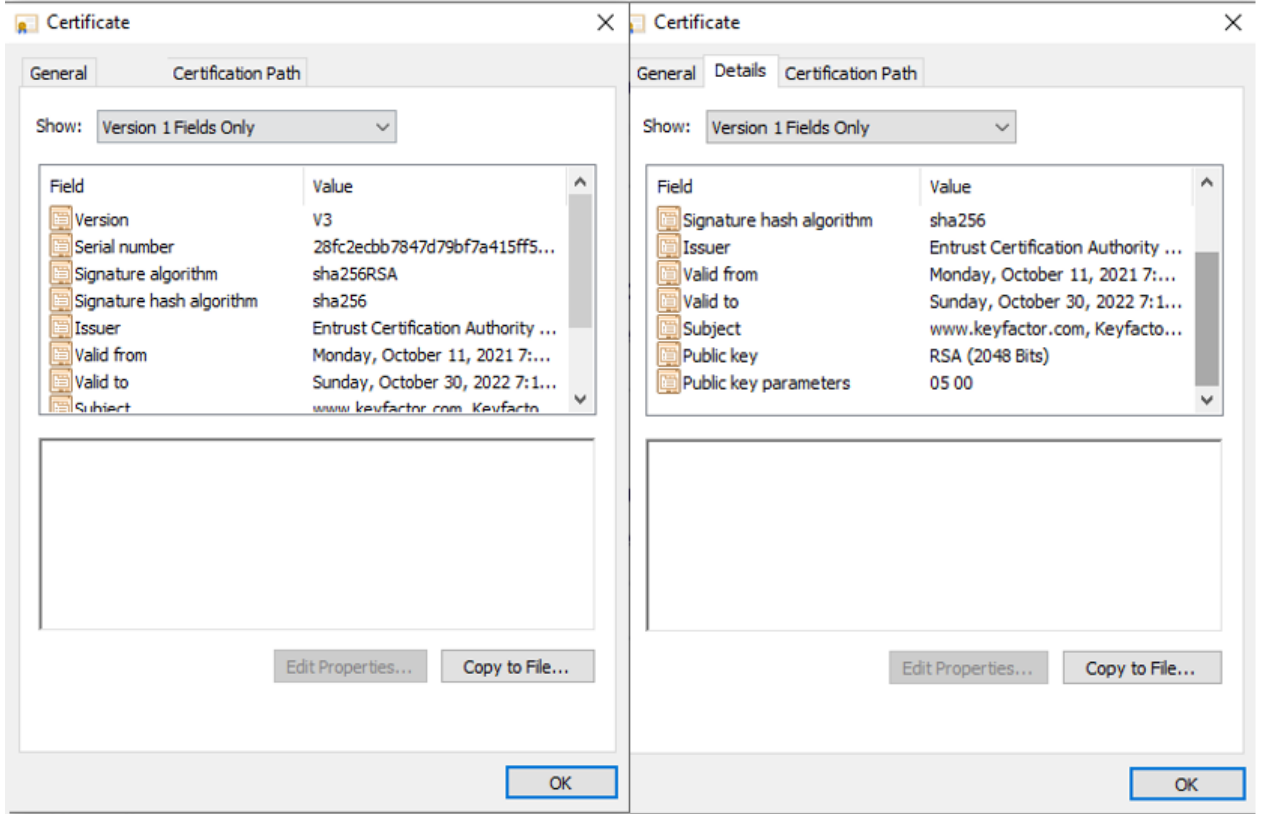
“Dijital imzalar, el yazısı imzalar gibi her imzalayan için benzersizdir Dijital imza çözüm sağlayıcıları PKI adı verilen belirli bir protokolü takip eder. PKI, sağlayıcının anahtar adı verilen iki uzun sayı üretmek için matematiksel bir algoritma kullanmasını gerektirir. Anahtarlardan biri genel, diğeri ise özeldir.

Bir imzalayan bir belgeyi elektronik olarak imzaladığında, imza, imzalayanın özel anahtarı kullanılarak oluşturulur ve bu anahtar her zaman imzalayan tarafından güvenli bir şekilde saklanır. Matematiksel algoritma bir şifre gibi davranarak imzalı belgeyle eşleşen ve hash adı verilen verileri oluşturur ve bu verileri şifreler. Sonuçta ortaya çıkan şifrelenmiş veri dijital imzadır. İmza aynı zamanda belgenin imzalandığı zaman ile de işaretlenir. İmzalandıktan sonra belge değişirse, dijital imza geçersiz kılınır.

Örnek olarak, Jane özel anahtarını kullanarak bir devre mülk satış sözleşmesi imzalar. Alıcı belgeyi teslim alır. Belgeyi alan alıcı Jane'in açık anahtarının bir kopyasını da alır. Açık anahtar imzanın şifresini çözemezse (anahtarların oluşturulduğu şifre aracılığıyla), imza Jane'e ait değil ya da imzalandığından beri değiştirilmiş demektir. Bu durumda imza geçersiz kabul edilir.

İmzanın bütünlüğünü korumak için PKI, anahtarların güvenli bir şekilde oluşturulmasını, yürütülmesini ve kaydedilmesini gerektirir ve genellikle güvenilir bir Sertifika Yetkilisinin (CA) hizmetlerini gerektirir.” ( Anonymous, 2015) Şekil 2.1. bu adımları görsel olarak ifade eder.

## 2.4 Sertifika Özellikleri



Şekil 3.1. Dijital sertifika ayrıntılarında gösterilen sertifika özellikleri

X.509 Sürüm 3 sertifikaları, X.509 sürüm 1'den beri desteklenen aşağıdaki alanları destekler bu alanlar Şekil 3.1. de görüldüğü üzere Detaylar kısmında gözlenebilir:

Konu: CA'nın sertifikayı verdiği bilgisayarın, kullanıcının, ağ aygıtının veya hizmetin adını sağlar. Konu adı genellikle X.500 veya Hafif Dizin Erişim Protokolü (LDAP) biçimi kullanılarak gösterilir.



Seri Numarası: Bir CA'nın verdiği her sertifika için benzersiz bir tanımlayıcı sağlar.

Veren: Sertifikayı veren CA için ayırt edici bir ad sağlar. Veren adı genellikle bir X.500 veya LDAP biçimi kullanılarak gösterilir.

Geçerlilik Tarihi: Sertifikanın geçerli olacağı tarih ve saati sağlar.

Geçerli Olduğu Tarih: Sertifikanın artık geçerli sayılmayacağı tarih ve saati sağlar. Bir uygulama veya hizmetin sertifikayı değerlendirdiği tarih, sertifikanın geçerli sayılabilmesi için sertifikanın Geçerli Başlangıç ve Geçerli Bitiş alanları arasında olmalıdır.

Ortak Anahtar: Sertifika ile ilişkilendirilmiş anahtar çiftinin ortak anahtarını içerir.

İmza Algoritması: Sertifikayı imzalamak için kullanılan algoritma.

İmza Değeri: Dijital imzayı içeren bit dizesi.

## **2.5 Chain Of Trust**

“Güvenli bir bağlantı üzerinden bir web sitesini ziyaret ettiğinizde, site tarayıcınıza dijital bir sertifika gönderir. İnternet tarayıcınız sertifikayı veren kuruluşu güvenilir Sertifika Yetkilileri (Kök CA) listesiyle karşılaştırır. Bir eşleşme bulunamazsa, istemci tarayıcısı sertifika veren CA sertifikasını güvenilir bir Kök CA'nın imzalayıp imzalamadığını kontrol eder. Tarayıcının zincirleme motoru, güvenilir bir kök bulana kadar veya güven zincirinin sonuna ulaştığında her sertifikayı veren kişiyi doğrulamaya devam eder.

Güven zinciri sertifikasyonu, belirli bir sertifikanın güvenilir bir kaynaktan geldiğini kanıtlamayı amaçlar. Sertifika meşru ise ve istemci tarayıcısının Güven Deposu'ndaki bir Kök CA'ya geri bağlantı veriyorsa, kullanıcı aşağıdaki şekil 1'de gösterildiği gibi arayüz güven göstergelerine dayanarak web sitesinin güvenli olduğunu bilecektir.”( Gaff, T., 2020)

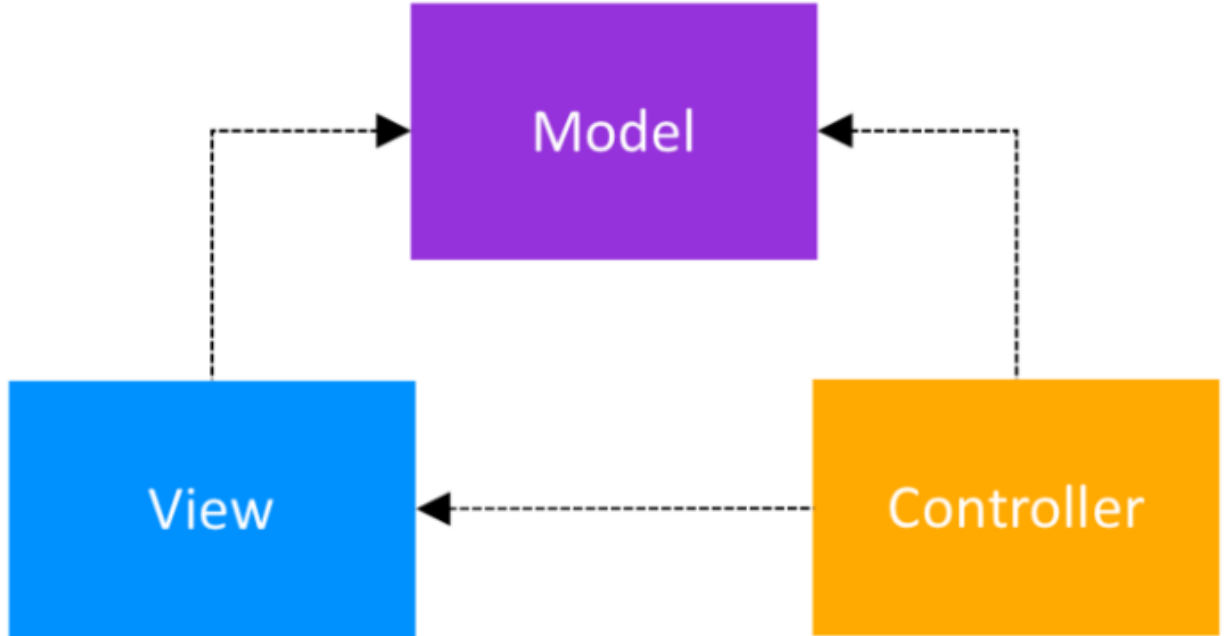
Projede chain of trust yapısı zaman yetersizliği yüzünden kullanılmamıştır.

### 3. PROJE MİMARİSİ

#### 3.1 MVC

“MVC, Yazılım Mühendisliği’nde önemli bir yere sahip architectural patterns (yazılım mimari desenleri)’ın bir parçasıdır. Model, View ve Controller kelimelerinin baş harflerinden oluşan MVC (Model-View-Controller), 1979 yılında Tygve Reeskaug tarafından oluşturulmuş ve yazılım gelişmede birçok projede kullanılmıştır. Son dönemlerde Microsoft’un MVC desenini Asp.Net teknolojisi ile birleştirmesi ile popülaritesi daha da artmıştır.

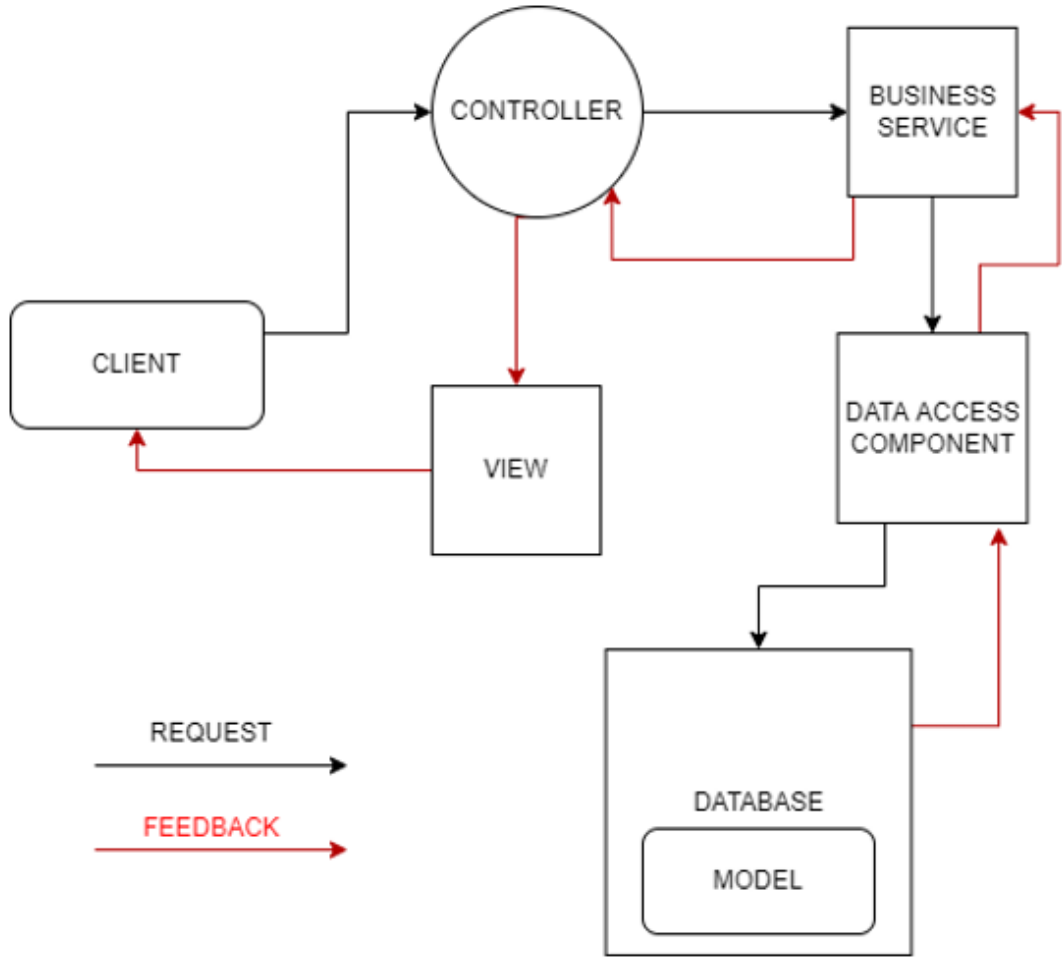
MVC deseni, 3 katmandan oluşmaktadır ve katmanları birbirinden bağımsız (birbirini etkilemeden) olarak çalışmaktadır. Bu sebeple çoğunlukla büyük çaplı projelerde projelerin yönetiminin ve kontrolünün daha rahat sağlanabilmesi için tercih edilmektedir. MVC ile geliştirilen projelerde projenin detaylarına göre birçok kişi eş zamanlı olarak kolaylıkla çalışabilmektedir.” ( Doğan, K., 2019)



Şekil 4.1. MVC yapısı

Projede MVC yapısı kullanılarak bir web sitesi tasarlanmıştır. Fakat programın yeniden kullanılabilirliğini artırmak ve ileriki zamanlar için geliştirme ve okumada kolaylıklar sağlaması için bu 3'lü yapıya ek 2 yapı daha projeye dahil edilmiştir.

### 3.2 Mvc'ye Ek Business Ve Dac Yapısı



Şekil 4.2. Projenin Mimarisi

Şekil 4.2. de görüldüğü üzere MVC'ye ek 2 bölüm daha eklenmiştir. Bunlardan ilki Business Service; Controller'dan gelen isteklerle ilgilenen ve isteklerin veri tabanından getirilmesini bekleyen kısımdır. Projeye eklenme amacı Controller'ı daha sade hale getirmek ve işleri yapan ayrı bir birim oluşturmaktır.

Business Service'ten gelen veri tabanı istekleri doğrudan veri tabanına iletilmez. Bu aşamada mimariye eklenen 2. Kısım devreye giriyor yani Data Access Component. Bu birimde veri tabanı sorguları depolanır ve düzenli bir biçimde tanımlanır. Veri tabanına sorgular yapılır ve gelen cevaplar Business Service'e iletilir.

### **3.3 Entitiy Framework**

Entity framework yapısında 3 adet çok kullanılan yöntem vardır. Bu Projede CodeFirst yapısı kullanılmıştır.”Bu teknik Veritabanı ile Programlama dili arasında bağ kuran bir tekniktir. Projenizde veritabanı işlemlerinizi mümkün merteye Visual Studio tarafında kod yazarak gerçekleştirmenizi sağlayan bir yaklaşımdır. Bu yaklaşım sayesinde veritabanı arayüzü ile yazılımcı arasında ilişki minimize edilmektedir.”( Yıldız, G., 2016) Ve veri tabanı olarak da Microsoft SQL server 2018 kullanılmıştır.

## **4. PROJE GELİŞİMİ**

### **4.1 Şifreleme Algoritması**

Projede kullanıcıların kayıt olması ve siteye giriş yapması beklenmektedir. Bu işlem yapılırken kullanıcıların şifreleri veri tabanında şifrelenmiş yani hash’lenmiş olarak tutulmuştur. Bu şifreleme yapılırken SHA256’dan yararlanılmıştır. “Güvenli hash algoritması anlamına gelen SHA-256 ise Ulusal Standartlar ve Teknoloji Enstitüsü tarafından geliştirilmiştir. Mesaj, dosya ve veri doğrulaması için kullanılan bir şifreleme algoritmasıdır ve SHA-2 hash işlevi ailesinin parçasıdır. Bir veri parçasını güvenli veri dizisine dönüştürmek için 256 bitlik anahtarlar kullanır. Hash değeri adı verilen bu rastgele karakter ve sayı dizisi de 256 bit boyutundadır.”( Dursun, Ö., 2022) Bu tek yönlü bir şifreleme olduğu için şifreler veri tabanından okunamaz. Kullanıcı giriş yaparken denediği şifre hash’lenir ve aynı olup olmadığına göre giriş yetkisi verilir.

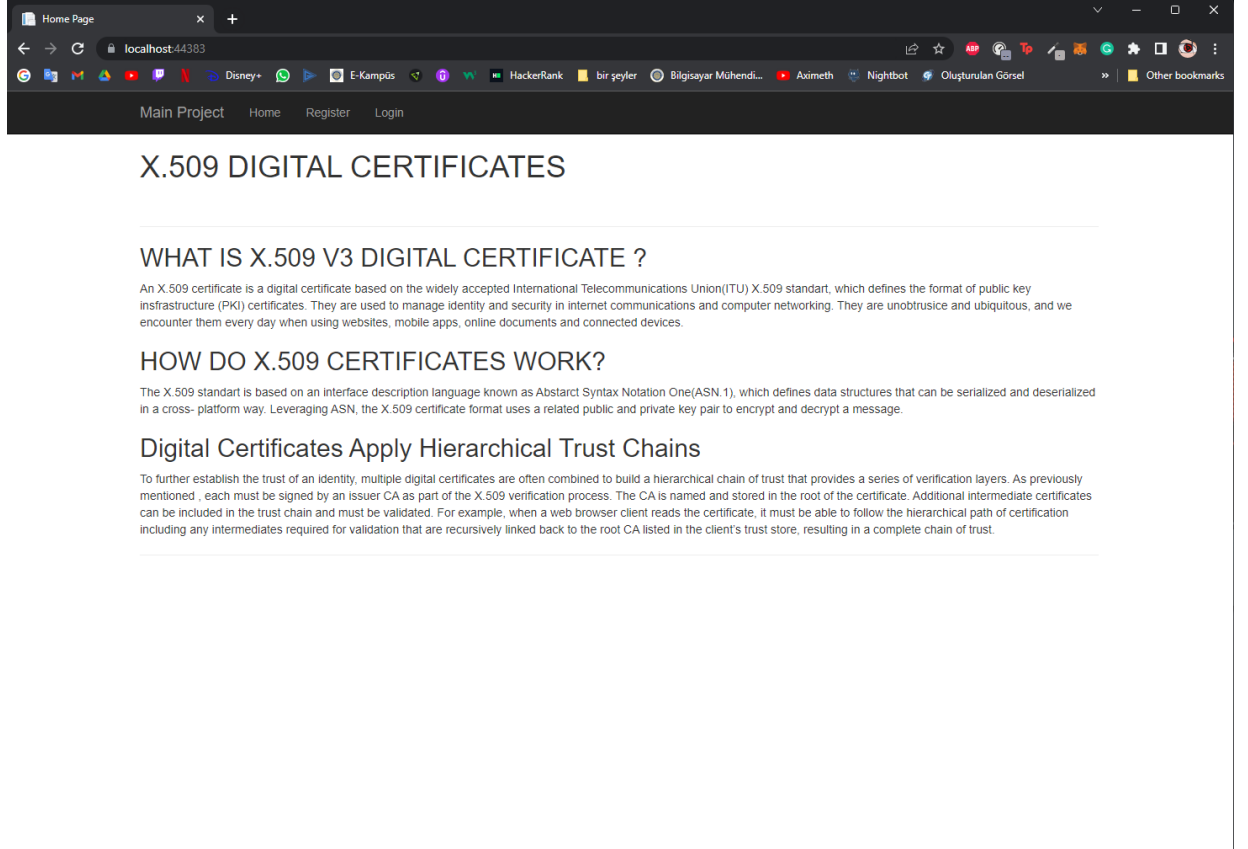
### **4.2 Yetkilendirme Ve Kimlik Doğrulama**

Projede kullanılan yapılardan bir diğeri ise yetkilendirme ve kimlik doğrulama kısmıdır. Kullanıcılar siteye kayıt olmalı ve giriş yapmalıdır. Bu işlem yapıldıktan sonra kendilerine ait sertifikaları üretebilirler. Bu aşama kimlik doğrulama olarak adlandırılır. Kullanıcı isimleri ve şifreler veri tabanına kaydedilir. Her kullanıcının bir yetki seviyesi vardır. Bu projede kullanıcı ve admin olmak üzere 2 adet yetki mevcuttur. Kullanıcı sadece sertifika oluşturabilir, indirebilir veya uzantı değişimi yapabilir. Admin ise bunlara ek kayıtların tutulduğu sayfaya erişebilir ve kullanıcı listesini görüntüleyebilir.

## 5. TEST İŞLEMİ

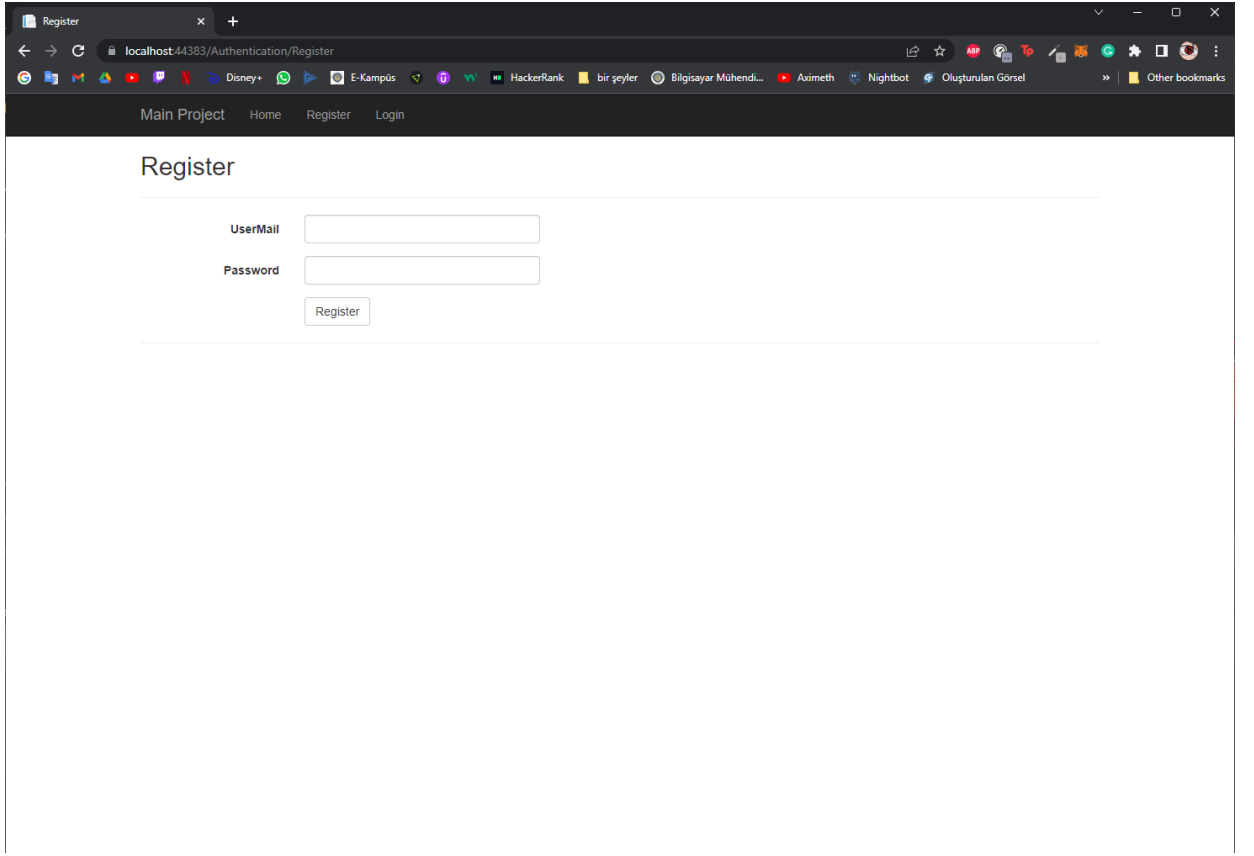
Web sitesi birden fazla kullanıcının aynı anda giriş yapıp aynı anda işlem yapabilmesine olanak sunar. Bunu C#'daki task yapısı ile sağlar. Bunu test etmek için bir client yani müşteri programı yazılmıştır ve aynı anda 100'den fazla istek atılarak sitenin çalışması test edilmiştir.

### 5.1 Web Sitesinin İşlevlerinin Tanıtımı



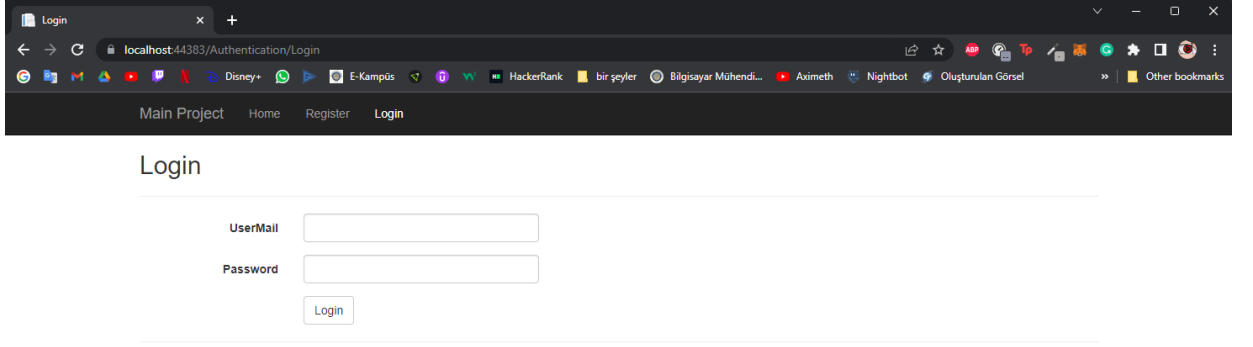
Şekil 5.1. Home sayfası

Şekil 5.1. de görülen home yani anasayfa kısmıdır. Web sitesine giriş yaptığınızda sizi ilk karşılayan sayfa budur ve X509.v3 dijital sertifikası hakkında ön bilgi verilmiştir.



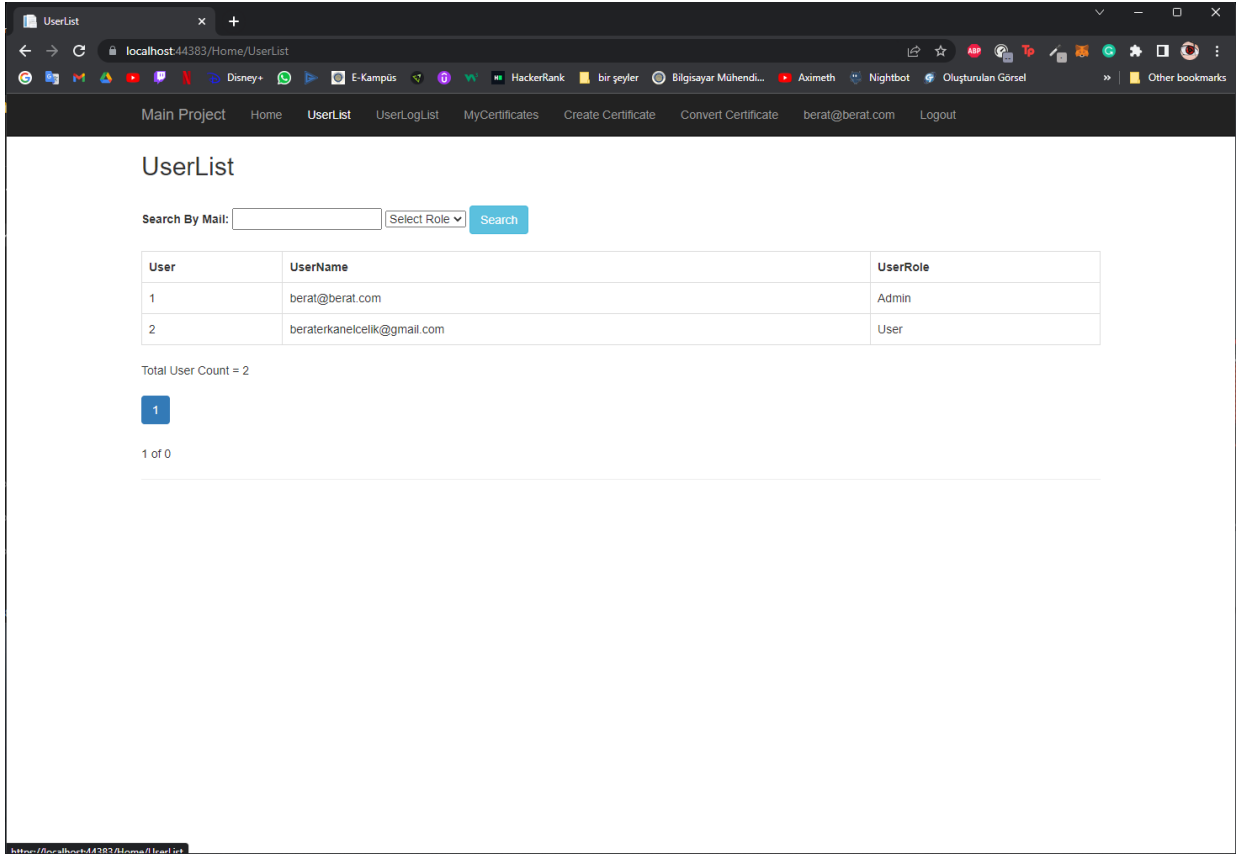
Şekil 5.2. Kayıt olma sayfası

Şekil 5.2. De görüldüğü gibi bu sayfada kullanıcıların mail ve şifre girişi yaparak siteye kayıt olmaları beklenmektedir. Bu aşamada gerekli yanlış girdilerin kontrolleri sağlanmış ve kullanıcı bu usule uygun şekilde uyarılır.



Şekil 5.3. Giriş sayfası

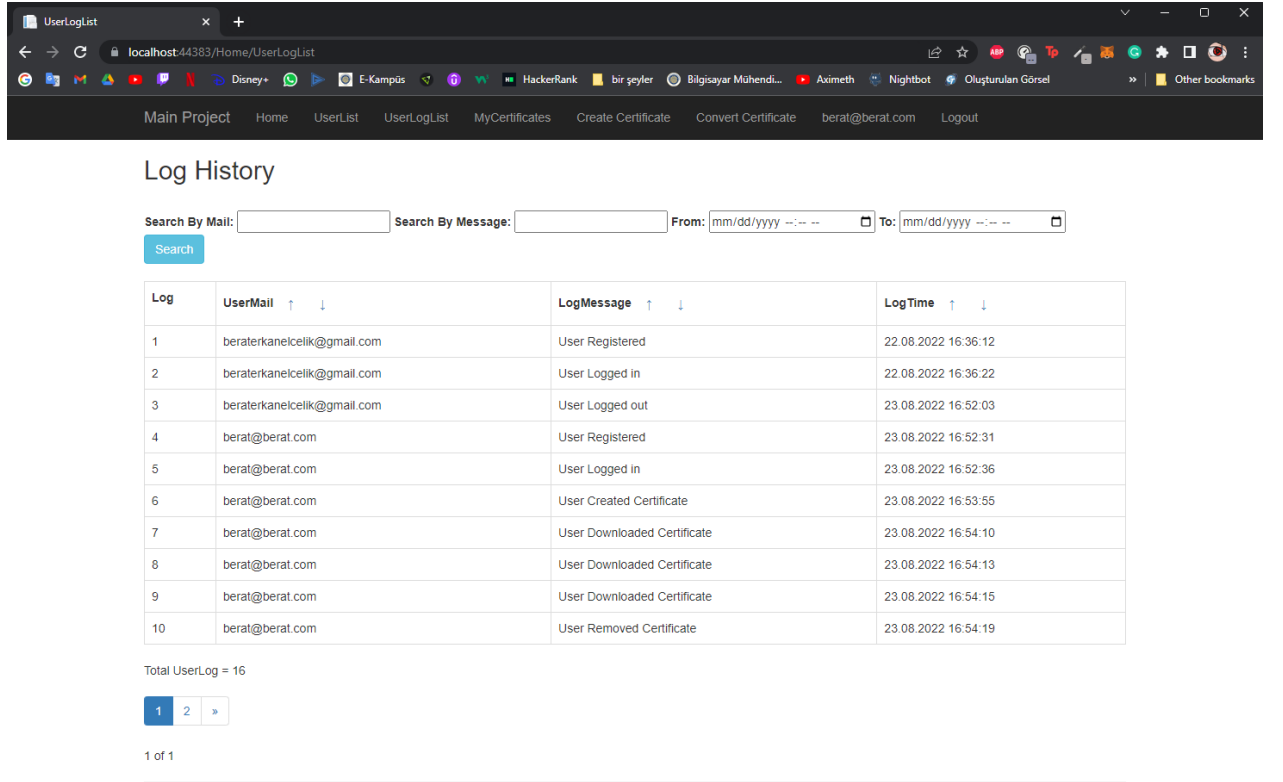
Şekil 5.3. de görüldüğü üzere Bu sayfada kullanıcıların oluşturdukları kimlik ile giriş yapmaları beklenir. Girilen veriler veri tabanındakilerle karşılaştırılarak onay verilir ya da hata ile kullanıcı bilgilendirilir.



Şekil 5.4. Kullanıcı listesi sayfası

Şekil 5.4. 'ten itibaren admin girişi yapılmış şekilde sayfalar tanıtılacaktır. Kullanıcının sahip olduğu sayfalar kullanıcı listesi sayfası ve kullanıcı kayıtları sayfasının dışında kalanlardır. Şekil 5.4. te kullanıcı listesi sayfası görülmektedir. Bu sayfada tüm kayıtlı kullanıcılar ve rolleri admine gösterilir. Admin eğer isterse mevcut arama ve sıralama özelliklerini kullanarak istediği kullanıcıyı kontrol edebilir.





Log	UserMail	LogMessage	LogTime
1	beraterkanekelik@gmail.com	User Registered	22.08.2022 16:36:12
2	beraterkanekelik@gmail.com	User Logged in	22.08.2022 16:36:22
3	beraterkanekelik@gmail.com	User Logged out	23.08.2022 16:52:03
4	berat@berat.com	User Registered	23.08.2022 16:52:31
5	berat@berat.com	User Logged in	23.08.2022 16:52:36
6	berat@berat.com	User Created Certificate	23.08.2022 16:53:55
7	berat@berat.com	User Downloaded Certificate	23.08.2022 16:54:10
8	berat@berat.com	User Downloaded Certificate	23.08.2022 16:54:13
9	berat@berat.com	User Downloaded Certificate	23.08.2022 16:54:15
10	berat@berat.com	User Removed Certificate	23.08.2022 16:54:19

Total UserLog = 16

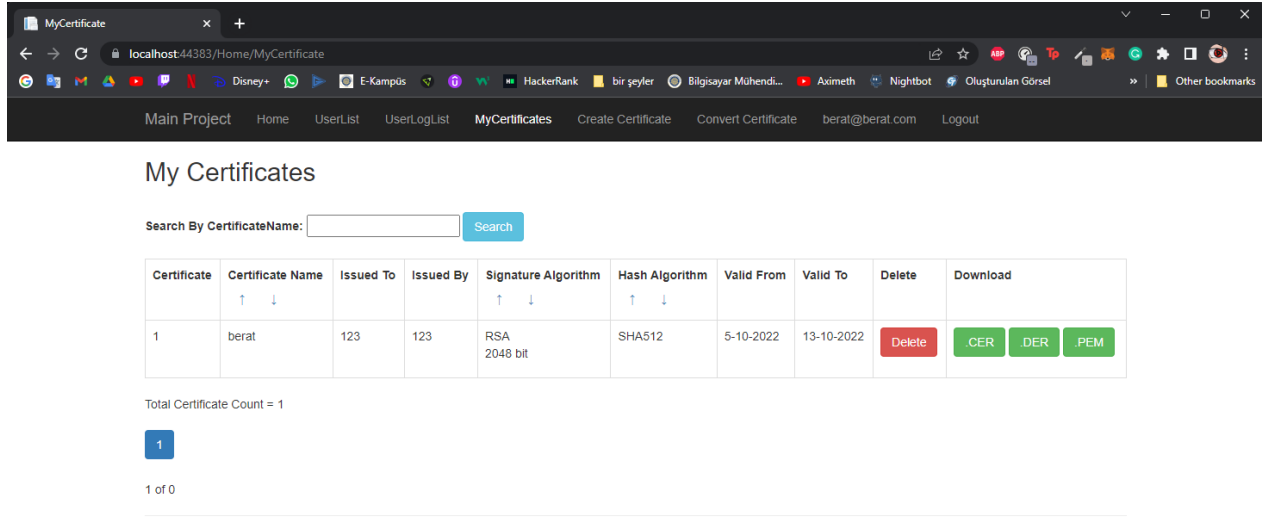
1 2 »

1 of 1

www.beraterkanekelik.com

## Şekil 5.5. Kullanıcı Kayıtları Sayfası

Şekil 5.5. te görüldüğü üzere kullanıcıların yaptığı tüm işlemler örneğin: giriş,çıkış,sertifika oluşturma vs. zaman da dahil olmak üzere kayıt altına alınır ve admine gösterilir. Admin eğer isterse sayfanın üst kısmında bulunan butonlar ve aramalar sayesinde istediği kayıtlara ulaşabilir.



Şekil 5.6 Oluşturulan Sertifikaların görüntülediği sayfa

Şekil 5.6 'da görüldüğü üzere oluşturulan sertifikalar burada görüntülenir ve eğer kullanıcı isterse silebilir, istediği sertifikayı araştırıp bulabilir veya istediği formatta indirebilir.

Create Certificate

CertificateName

IssuerName

HashAlgorithm

SignatureAlgorithm

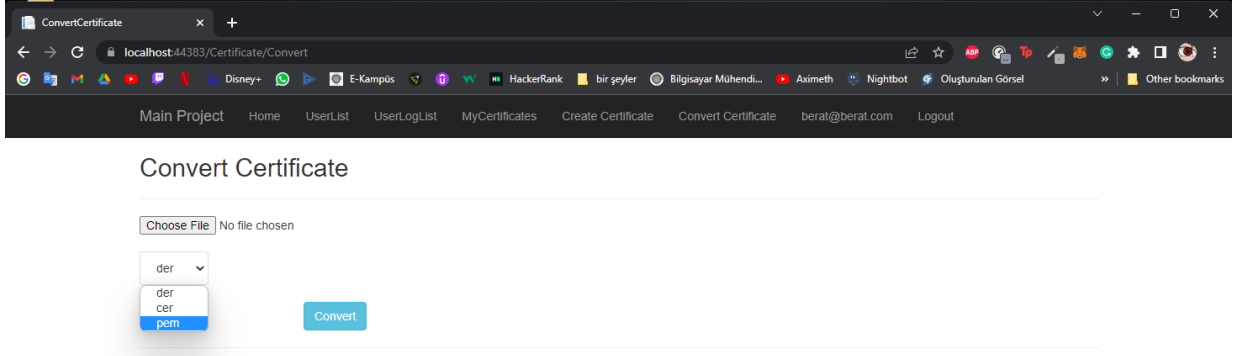
SignatureBit

ValidFrom

ValidTo

Şekil 5.7. Sertifika Oluşturma sayfası

Şekil 5.7. de sertifikaların oluşturulduğu sayfa verilmiştir. Bu aşamada sertifikanın özellikleri girilerek istenen sertifika oluşturulur ve veri tabanına bu özellikler kayıt edilir. Hata oluşturan girişler kontrol edilerek kullanıcı uyarılır.



Şekil 5.8. Sertifika formatının değiştirildiği sayfa

Şekil 5.8. de Sertifika formatının değiştirildiği sayfa görüntülenmektedir. Kullanıcı formatının değiştirilmesini istediği sertifikayı bilgisayarından seçerek sayfaya yükler ve formatı seçtikten sonra sayfadan indirebilir.

Ve son olarak çıkış butonu tüm resimlerde görüldüğü üzere çıkış yapmayı sağlar ve Kullanıcıyı Şekil 5.1. deki görüntüye ulaştırır.

## 6. SONUÇ

Bu projenin ana amacı kullanıcıların kendi X.509 v3 tipinde dijital sertifika üretmelerini, dönüştürmelerini ve istedikleri formatta indirebilmelerini sağlamak olarak belirlenmiştir. Bu amaç doğrultusunda kullanıcıların bu işlemleri yapabilmesi için bir web sitesi tasarlanmıştır. Bu web sitesi aracılığıyla kullanıcılar kayıt yapabilir, istedikleri sertifika bilgilerini gerekli sekmeden giriş yaparak oluşturabilir ve sertifikalarını sekmesine giderek istedikleri sertifikayı bulduktan sonra üç farklı formatta indirebilirler. Daha sonrasında sertifika formatları arasında geçiş yapmak isterlerse sertifika format değiştirmeleri için de format değiştirme bölümü de bunlara ek olarak eklenmiştir. Bu projede verilen işlev görevleri yerine getirilmiştir. Bu web sitesinde kullanıcıların kendi ürettiği dijital sertifikaları görüntüleyebiliş istedikleri formatta indirebilmeleri kullanıcılara büyük ölçüde kolaylık sağlamaktadır. Üretilen web sitesi sayesinde kullanıcıların yaklaşık beş dakika içerisinde kendi sertifikalarını üretmeleri sağlanmıştır. Günümüzde bunu yapabilecek bir site mevcut değildir ve yazılım bilgisi olmayan fakat kendi sitelerinin güvenliğini kanıtlamak isteyen müşteriler bu sertifikaları üretmekte zorluk çekecektir. Bu yüzden bu site onlara hem kolaylık hem de pratiklik sağlamıştır. Site, zaman yetersizliğinden dolayı yayınlanamamıştır ve görünüşüne pek vakit ayırılamamıştır. İleriki aşamada projenin görünüm kısmına da önem verilerek kullanıcılara daha verimli deneyimler kazandırılabilir. Bunlara ek olarak çok önemli bir sistem olan chain of trust(güven zinciri) yapısı kullanıcıların deneyimine sunulabilir.

## 7. KAYNAKÇA

- Yıldız, G., 2016. Entity Framework İle Code First Yaklaşımı – Yazılım Mimarileri ve Tasarım Desenleri Üzerine [WWW Document]. Entity Framework İle Code First Yaklaşımı – Yazılım Mimarileri ve Tasarım Desenleri Üzerine. URL [https://www.gencayyildiz.com/blog/entity-framework-ile-code-first-yaklasimi/#:~:text=Code%20First%20Nedir%3F,yaz%C4%B1l%C4%B1mc%C4%B1%20aras%C4%B1nda%20ili%C5%9Fki%20minimize%20edilmekt edir. \(Erişim Tarihi:10.18.22\).](https://www.gencayyildiz.com/blog/entity-framework-ile-code-first-yaklasimi/#:~:text=Code%20First%20Nedir%3F,yaz%C4%B1l%C4%B1mc%C4%B1%20aras%C4%B1nda%20ili%C5%9Fki%20minimize%20edilmekt edir. (Erişim Tarihi:10.18.22).)
- Doğan, K., 2019. MVC Nedir? MVC Yaşam Döngüsü (Life Cycle) [WWW Document]. Medium. URL [https://medium.com/@kdrandogan/mvc-nedir-mvc-ya%C5%9Fam-d%C3%B6ng%C3%BCs%C3%BC-life-cycle-8e124f24650c \(Erişim Tarihi:10.18.22\).](https://medium.com/@kdrandogan/mvc-nedir-mvc-ya%C5%9Fam-d%C3%B6ng%C3%BCs%C3%BC-life-cycle-8e124f24650c (Erişim Tarihi:10.18.22).)
- Gaff, T., 2020. What is the Certificate Chain of Trust? &ndash; Keyfactor [WWW Document]. Keyfactor. URL [https://www.keyfactor.com/blog/certificate-chain-of-trust/ \(Erişim Tarihi:10.18.22\).](https://www.keyfactor.com/blog/certificate-chain-of-trust/ (Erişim Tarihi:10.18.22).)
- Anonim, n.d. DİJİTAL İMZA NEDİR? [WWW Document]. DİJİTAL İMZA NEDİR? URL [https://www.beyaz.net/tr/guvenlik/makaleler/dijital\\_imza\\_nedir.html \(Erişim Tarihi:10.18.22\).](https://www.beyaz.net/tr/guvenlik/makaleler/dijital_imza_nedir.html (Erişim Tarihi:10.18.22).)
- Dursun, Ö., 2022. Hash nedir? SHA-256 algoritması [WWW Document]. Teknoloji Haberleri - ShiftDelete.Net. URL [https://shiftdelete.net/hash-nedir-sha-256-algoritmasi \(Erişim Tarihi:10.18.22\).](https://shiftdelete.net/hash-nedir-sha-256-algoritmasi (Erişim Tarihi:10.18.22).)
- Wilson, C., 2020. Dijital Sertifika nedir? [WWW Document]. SSL.com. URL [https://www.ssl.com/tr/faqs/dijital-sertifika-nedir/ \(Erişim Tarihi: 10.18.22\).](https://www.ssl.com/tr/faqs/dijital-sertifika-nedir/ (Erişim Tarihi: 10.18.22).)
- Anonymous, 2015. What is a Digital Signature & How Do I Create One? [WWW Document]. DocuSign. URL [https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq \(Erişim Tarihi: 10.18.22\).](https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq (Erişim Tarihi: 10.18.22).)
- Yıldız, G., 2019. C# Repository Design Pattern(Repository Tasarım Deseni) – Yazılım Mimarileri ve Tasarım Desenleri Üzerine [WWW Document]. C# Repository Design Pattern(Repository Tasarım Deseni) – Yazılım Mimarileri ve Tasarım Desenleri Üzerine. URL [https://www.gencayyildiz.com/blog/c-repository-design-patternrepository-tasarim-deseni/ \(Erişim Tarihi: 6.22\).](https://www.gencayyildiz.com/blog/c-repository-design-patternrepository-tasarim-deseni/ (Erişim Tarihi: 6.22).)
- Singh, J., 2018. Unit of Work in Repository Pattern [WWW Document]. Unit of Work in Repository Pattern. URL [https://www.c-sharpcorner.com/UploadFile/b1df45/unit-of-work-in-repository-pattern/ \(Erişim Tarihi: 6.22\).](https://www.c-sharpcorner.com/UploadFile/b1df45/unit-of-work-in-repository-pattern/ (Erişim Tarihi: 6.22).)

- Anderson, R., 2022. ASP.NET Core yetkilendirmeye giriş | Microsoft Learn [WWW Document]. ASP.NET Core yetkilendirmeye giriş | Microsoft Learn. URL <https://learn.microsoft.com/tr-tr/aspnet/core/security/authorization/introduction?view=aspnetcore-6.0> (Erişim Tarihi: 6.22).
- Gillis, A.S., 2020. What is REST API (RESTful API)? [WWW Document]. SearchAppArchitecture. URL <https://www.techtarget.com/searchapparchitecture/definition/RESTful-API> (Erişim Tarihi: 6.22).
- Stallings, W., 2011. Cryptography and Network Security: Principles and Practice. Prentice Hall, Harlow, England (Erişim Tarihi: 6.22).
- Housley, R., Ford, W., Polk, W., Solo, D., n.d. RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile [WWW Document]. RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. URL <https://www.rfc-editor.org/rfc/rfc2459#appendix-A> (Erişim Tarihi: 6.22).