İçindekiler

[Z-Anahtar Mobil Uygulama 2](#_Toc125986430)

[Bileşenler 2](#_Toc125986431)

[Z-AnahtarNet API 2](#_Toc125986432)

[Z-Anahtar Backend ve Veritabanı 2](#_Toc125986433)

[BlokZincir Ağı (Hyperledger Indy) 2](#_Toc125986434)

[Akışlar 3](#_Toc125986435)

[Z-Anahtar Uygulamasına Giriş 3](#_Toc125986436)

[Biyometrik Giriş 3](#_Toc125986437)

[QR Kod ile Dijital Kimlik Ekleme 4](#_Toc125986438)

[Kimlik Sağlayıcı (e-Devlet) 4](#_Toc125986439)

[Kimlik Doğrulayıcı (e-Devlet) 4](#_Toc125986440)

[Çipli Kimlik ile Kullanıcıyı Tanıma 4](#_Toc125986441)

[Uygulamayı silme 5](#_Toc125986442)

# Z-Anahtar Mobil Uygulama

Z-Anahtar, e-Devlet üzerinden aldığınız Giriş Kimliğiniz ile e-Devlet platformuna kendinizi kanıtlayabildiğiniz ve güvenli bir şekilde platforma giriş yapmanızı sağlayan blokzincir teknolojisi ile geliştirilmiş dijital kimlik yönetim uygulamasıdır.

Z-Anahtar mimarisinde Z-AnahtarNet API, Z-Anahtar Blokzincir Ağı, Z-Anahtar Backend, Z-Anahtar Mobil Uygulaması bileşenleri bulunmaktadır. Bu bileşenlerle birlikte kullanıcı senaryoları ve süreçleri yapılandırılmıştır.

# Bileşenler

## Z-AnahtarNet API

Z-AnahtarNet API servisi mimaride blokzincir ile Z-Anahtar mobil uygulaması arasında konumlanan blokzincir ile ilgili işlemlerin yapılmasını sağlayan servistir. Kimlik sağlama ve doğrulama işlemlerini yönetir.

## Z-Anahtar Backend ve Veritabanı

Z-Anahtar Backend servisi mobil uygulamanın dijital kimlik dışında kalan işlemleri (ayarlar, versiyon vb) gerçekleştirmek için geliştirilmiştir. Kişisel veri içermez. Kullanıcının uygulamaya giriş yaptığı andan itibaren uygulama üzerinde gördüğü görsel ögeler ve gerçekleştirdiği işlemler uygulamanın backend yapısında gerçekleşir. Kullanıcının uygulama girişinden itibaren karşılaştığı kullanıcı sözleşmeleri, uygulama izinleri, giriş kimliklerinin tutulduğu alanlar, sıkça sorulan sorular ve açıklamalar ile birlikte kullanıcı deneyimi buradan yönetilir.

Veritabanı üzerinde kullanıcının uygulama ile olan etkileşime ait loglamalar, uygulama versiyon bilgileri, ayarlar, kullanıcı sözleşmeleri ve içerikler ile ilgili bilgiler yer alır. Hangi kullanıcının uygulamaya giriş yaptığı ve hangi kullanıcı sözleşmesini kabul ettiği bilgileri loglanır. e-Devlet giriş servisinden dönen kullanıcının uygulamaya giriş yaptığı TC kimlik numarası, telefon numarası ve e-mail bilgisi veritabanı üzerinde tutulması planlanmaktadır. Bu bilgiler kullanıcı sözleşmesi onayı ile birlikte eşleştirilecektir.

## BlokZincir Ağı (Hyperledger Indy)

Z-anahtar uygulaması blokzincir altyapısı olarak Hyperledger Indy'i kullanmaktadır. Hyperledger Indy, merkezi olmayan kimlik için özel olarak oluşturulmuş dağıtık bir defterdir. Indy merkezi olmayan kimliğe odaklanması nedeniyle gizlilik temeli üzerine inşa edilmiştir.

Hyperledger Indy Blokzinciri’nde herhangi bir kişisel veri tutulmaz, aşağıdaki bilgiler yer almaktadır:

1. Doğrulama anahtarları ve uç noktalarla ilişkili Genel DID’ler
2. Şemalar ve kimlik bilgileri tanımları
3. İptal kayıtları
4. Yetkilendirme politikaları

Decentralized Identity (DID) (Dağıtılmış Tanımlayıcılar) yapısı ile birlikte kişilerin kendi dijital kimliklerini oluşturup kontrol edebildikleri bir model kullanılmaktadır. DID'ler, herhangi bir merkezi otoriteden bağımsız olarak, sahipleri tarafından oluşturulan, benzersiz tanımlayıcılardır. Kullanıcının eklediği giriş kimlikleri, kişinin kendi mobil cihazı üzerinde oluşturulan cüzdanların içerisinde özel anahtarla birlikte şifrelenmiş bir şekilde bulunur. Blokzincirde ise kullanıcıya ait kimlik verileri tutulmaz, kimliğinin kullanıcı tarafından alınıp alınmadığı bilgisi tutulur. Kullanıcının özel anahtarıyla kendi cüzdanında sakladığı bilgiye başka bir yerden erişim mümkün değildir.

Z-Anahtar uygulamasında blokzincir, kullanıcıya bir DID verir; kullanıcı, servisle konuştuğundan emin olabilir. Böylece kişi herhangi bir kimliğini ya da belgesini sağlayıcı kurumdan aldığı zaman sadece mobil cihazında tutmaktadır. Herhangi bir kurum ya da kuruluş kimlik bilgilerini istediği zaman kişiler, kimliklerinde bulunan ve istenilen bilgiyi kendi rızası ile istenilen kadarını paylaşmaktadır. Blokzincir teknolojisine dayanan merkezi olmayan bir sistemin kullanılması, kullanıcılara DID'lerini merkezi otorite ve herhangi bir kurumun ulaşılabilirliği olmadan güvenli bir şekilde kullanma olanağı sağlar.

4 tane blokzincir sunucusu üzerinde çalışmaya başlayacaktır. Hyperledger Indy çerçevesinde sisteme sadece izin verilen sunucular eklenebilmektedir. Genel bir ağ yapısı olarak çalışmasına rağmen yalnızca ağı kullananların yazabileceği özel bir ağ olarak yapılandırılmıştır. Kimlik bilgileri eşler arası bağlantı yoluyla iletilir ve bu bilgiler doğrulanmış şifreleme ile güvence altına alınır.

Uygulama Indy SDK üzerinden kimlikleri oluşturma ve okuma işlemleri yapmaktadır. Kimlik sağlayıcı ve doğrulayıcı kurumları tanımlayan genel anahtar değeri blokzincir ağındaki defterde tutulur. Kimlik sağlayıcı ve doğrulayıcı kurumlar Z-AnahtarNet API servisi aracılığı ile blokzincir üzerinden dijital kimlik yönetimini gerçekleştirir.

# Akışlar

## Z-Anahtar Uygulamasına Giriş

Z-Anahtar uygulamasına e-Devlet Kapısı ile giriş yöntemi ve cihazlarda bulunan biyometrik giriş ile 2 şekilde giriş gerçekleştirilecektir. e-Devlet ile giriş yönteminde yalnız 2FA aktifleştirmiş kullanıcılar sisteme girebilecektir.

Z-Anahtar Backend servisinde e-Devlet Kapısı sonrası tanımlanmış giriş tokenı ile cihazdaki işletim sisteminin (IOS/Android) oluşturduğu genel anahtar kullanılarak ilgili e-Devlet Kapısı hesabı (client id) ve device id ile ilişkilendirilir. Bu sayede device binding sağlanır.

Ayrıca mobil uygulamadaki kimlik cüzdanının güvenliği için giriş sırasında Z-Anahtar mobil uygulamada rastgele bir anahtar değer oluşturulur. Bu anahtar AES (Gelişmiş şifreleme standardı) ile şifrelenerek uygulamaya kaydedilir. Bu anahtar değerin bir parçası backend servisine aktarılır. Böylece mobil uygulamanın anahtar değerini ele geçirebilecek kötü niyetli kişiler backend tarafındaki anahtarı edinemeyeceği için cüzdana erişemez.

## Biyometrik Giriş

Cihazında biyometrik giriş ayarları aktif olan kullanıcılar Z-Anahtar'a biyometrik giriş (Touch ID,Face ID, parmak izi) seçeneği de ekleyebilir. Bu işlemi yapabilmek için öncelikle 2FA (Şifre + OTP) ile giriş yapması zorunludur. Kullanıcı dilerse biyometrik girişi ayarlardan kapatabilir. Kullanıcı biyometrik girişi seçmiş olsa dahi, belli sayıda giriş sonrası tekrar şifre + OTP zorunlu tutulur, böylece güvenlik arttırılır.

## QR Kod ile Dijital Kimlik Ekleme

Z-Anahtar'a kimlik sağlayıcı olarak entegre olan kurumun sistemine (başlangıçta yalnız e-Devlet olacak) güvenli giriş yaparak, burada oluşturulan QR kodu Z-Anahtar “QR Okuyucu” menüsünden okutan kullanıcı, Z-Anahtar'a dijital kimliğini ekleyebilir. Dijital kimlik oluşturulurken, kişinin Z-Anahtarı’ndan telefon, TCKN gibi bilgileri paylaşması istenerek bu bilgi ile kimlik vericinin sistemindeki veri karşılaştırılır. Bu sayede kimliğin doğru kişiye verildiği garanti edilir. Bu işlem herhangi bir belge / kimlik almak için bir kuruma gittiğimizde karşımızdaki kişinin kimliğimizi kontrol etmesi ile benzerdir. Kimliği veren kurum, kendi sistemine giriş yapan kullanıcıya daha önceden verdiği bir kimlik varsa onu geçersiz yapar. Böylece kimliğin tekil kalması sağlanır. Yani bir kimlik en çok 1 cihazda yer alabilir. Bu durum da yeni tip bir kimlik, pasaport çıkarttığımızda eskisinin imha edilmesi süreci ile eşleştirilebilir. Kimlik tiplerine göre buradaki güvenlik seviyesi düşürülebilir veya arttırılabilir.

### Kimlik Sağlayıcı (e-Devlet)

e-Devlet’e giriş yaptıktan sonra uygun bir sayfasında kimlik sahibine özel QR kod gösterilir. Kullanıcı Z-Anahtar üzerinden bu QR kodu okutur ve kişinin dijital kimliği Z-Anahtar’a eklenir. Kurum kendi tercihi doğrultusunda güvenlik katmanı olarak QR kod okutulduktan sonra kimliğin gerçek sahibini doğrulamak amaçlı diğer ekli kimliklerinden kanıt isteyebilir. Kullanıcı bu kanıtı kurum ile paylaşmayı onaylarsa dijital kimlik eklenir. Örneğin, e-Devlet sitesine girildikten sonra sitenin içerisinde kullanıcının dijital giriş kimliğinin oluşturulduğu bir ekran içerisinde kullanıcıya özel QR kod paylaşılır. Kullanıcı bu kodu okutarak Z-Anahtar içerisine e-Devlet Giriş Kimliği'ni eklemiş olur.

### Kimlik Doğrulayıcı (e-Devlet)

Kurumun tercihine göre konumlanan kimlik doğrulama adımına gelindiğinde QR kod gösterimi yapılır. QR okuyucu ile doğrulanmak istenen dijital kimlik bilgileri kullanıcı onayına sunulur. İzin verildiği takdirde kimlik bilgileri kurum ile paylaşılır. Örneğin, e-Devlet Giriş Kimliği almış olan kullanıcı e-Devlet sitesine girmek istediğinde Z-Anahtar ile giriş yapma seçeneğini seçtikten sonra site üzerinde paylaşılan QR kodu Z-Anahtar üzerinde okutur. Daha önceden almış olduğu e-Devlet Giriş Kimliği bu kullanıcının kim olduğunu kanıtlayarak siteye girmesine izin verir.

## Çipli Kimlik ile Kullanıcıyı Tanıma

Kullanıcı “Kimliklerim” ekranındaki yönlendirmeleri takip ederek çipli T.C Kimlik aracılığı ile kendini Z-Anahtar'a tanıtabilir. Kimlik bilgileri NFC ile çipten okunduğu için bu akış sadece NFC (Yakın Mesafe İletişimi) destekleyen cihazlarda gerçekleşmektedir. Burada OCR teknoloji ile kimlik üzerindeki alanlar okunur, NFC teknoloji ile çip üzerinden kimlik bilgileri alınır. Cihazın kamerasından kullanıcı kimlik üzerinde bulunan fotoğrafı karşılaştırılır. Pasif ve aktif canlılık kontrolü ile kimlik sahibi doğrulanır. Kontroller cihaz içerisinde gerçekleşir. Biyometrik veri doğrulama sürecinde veriler sunucuya kaydedilmez, herhangi bir veritabanında tutulmaz.

## Uygulamayı silme

Z-Anahtar uygulamasını cihazından kaldıran kullanıcının tüm dijital kimlik verileri de silinmiş olur. Tek seferde tüm kimlikleri siler gibi dijital kimlik silme aksiyonları gerçekleşir. Ek olarak, kimliklerini aldığı kurumlar ile oluşturulan bağlantı bilgileri de silinir. Uygulamayı tekrar kurduğunda ilgili kimlik sağlayıcı kurumlardan tek tek dijital kimliklerini yeniden alması gerekir.