TAMGA NETWORK

TAMGA NETWORK AKADEMIK ÇALIŞMALAR

Dijital Kimliğin Evrimi

Kullanıcı Adından Kimlik Cüzdanına: Dört Dönem, Dört Güven Modeli

Berke Karataş

Tamga Network

KASIM 2026 · SÜRÜM 1.0

© 2026 Berke Karataş. Bu eser Creative Commons Atıf 4.0 Uluslararası Lisansı (CC BY 4.0) ile yayımlanmıştır: kaynak gösterilerek paylaşılabilir ve uyarlanabilir. https://creativecommons.org/licenses/by/4.0/deed.tr

Özet

İnsanlar binlerce yıl boyunca birbirlerini yüz yüze, bir mühre, bir mektuba ya da bir devletin verdiği kâğıda bakarak tanıdı. İnternet bu düzeni bozdu: karşımızdaki kişiyi görmüyoruz, gönderdiği her şey sınırsız kopyalanabiliyor ve aynı anda milyonlarca kişiyle işlem yapıyoruz. Son altmış yılda bu soruna verilen cevaplar dört büyük dönemde toplanabilir. İlk dönemde her sistem kendi kullanıcı adını ve parolasını tuttu. İkinci dönemde büyük kimlik sağlayıcıları ortaya çıktı ve "Google ile giriş yap" düğmesi hayatımıza girdi. Üçüncü dönemde, kimliği kişinin kendi elinde tutmayı amaçlayan kendi kendine egemen kimlik hareketi doğdu. Dördüncü dönemde ise devletler bu fikirlerin bir kısmını alıp hukuki güvenceyle birleştirdi; Avrupa Birliği'nin 2024'te kabul ettiği eIDAS 2.0 tüzüğü ve Avrupa Dijital Kimlik Cüzdanı bu dönemin en kapsamlı örneğidir.

Bu yazı, hiçbir ön bilgi varsaymadan bu dört dönemi anlatıyor. Her dönem için üç soruyu soruyoruz: kimliği kim veriyor, kim saklıyor ve doğrulama sırasında kim neyi görüyor? Teknik işleyişi de atlamıyoruz: parolaların nasıl saklandığını, "Google ile giriş" sırasında arka planda hangi mesajların gidip geldiğini ve bir dijital imzanın neden taklit edilemediğini adım adım açıklıyoruz. Yazının sonunda dört modeli yan yana koyuyor, bugün hâlâ çözülmemiş soruları tartışıyor ve bu yazı dizisinin sonraki bölümlerine zemin hazırlıyoruz.

Anahtar kelimeler: dijital kimlik · kimlik doğrulama · federasyon · OpenID Connect · kendi kendine egemen kimlik · doğrulanabilir belge · eIDAS 2.0 · EUDI cüzdanı · kimlik güvencesi düzeyi

> ATIF
> Karataş, B. (2026). Dijital Kimliğin Evrimi: Kullanıcı Adından Kimlik Cüzdanına: Dört Dönem, Dört Güven Modeli. Tamga Network Akademik Çalışmalar, A1. https://tamga.network/files/publications/evolution-of-digital-identity-tr.pdf

İçindekiler

1 Giriş: Bir Mühürden Bir Telefona 3
2 Temel Kavramlar: “Kimlik” Derken Neyi Kastediyoruz? 4
2.1 Varlık, kimlik ve öznitelik 5
2.2 Tanımlayıcı 5
2.3 Kimlik bilgisi (belge) 5
2.4 Kimlik doğrulama ve yetkilendirme 5
2.5 Roller: veren, sahip, doğrulayan 6
3 Fiziksel Dünyadan Dijital Dünyaya: Güvenin Üç Dayanağı Neden Çöktü? 7
4 Birinci Dönem: Adalar ve Parolalar 7
4.1 Her şey bir zaman paylaşım sisteminde başladı 7
4.2 Bir parola nasıl saklanır? 8
4.3 Ada modelinin sorunları 9
4.4 Ada döneminin bugünkü mirası 10
5 İkinci Dönem: Federasyon ve “Google ile Giriş Yap” 10
5.1 Fikir: Kimliği bir kez doğrula, her yerde kullan 10
5.2 Kısa bir tarihçe 11
5.3 “Google ile giriş” düğmesine bastığınızda ne olur? 11
5.4 Federasyon neyi çözdü? 13
5.5 Federasyonun bedeli 13
5.6 Bir ara durak: Kimliğin Yedi Yasası 14
6 Üçüncü Dönem: Kendi Kendine Egemen Kimlik 15
6.1 Bir manifestonun doğuşu 15
6.2 Üçgen model: veren, sahip, doğrulayan 16
6.3 Dijital imza: Taklit zorluğunun matematikle kurulması 16
6.4 Merkeziyetsiz tanımlayıcılar ve doğrulanabilir belgeler 17
6.5 Vaatler ve sahada yaşananlar 18
7 Dördüncü Dönem: Devlet Destekli Kimlik Cüzdanları 19
7.1 Neden devletler? 19
7.2 eIDAS: Avrupa’nın ilk adımı 19
7.3 eIDAS 2.0 ve Avrupa Dijital Kimlik Cüzdanı 20
7.4 Cüzdan ekosistemi: kim kimdir? 21
7.5 Teknik mimari ve standartlar 22
7.6 Avrupa dışında 23
8 Kimlik Güvencesi Düzeyleri: Ne Kadar Emin Olmalıyız? 23
9 Dört Modelin Karşılaştırması 24
10 Sınırlar ve Açık Sorular 25
11 Bu Tablonun İçinde Tamga Network 26
12 Sonuç 26
Kaynaklar 26
Okuma listesi: Buradan başlayın 27
Ek A — Sözlük 28

1 Giriş: Bir Mühürden Bir Telefona

Orta Asya bozkırlarında yaşayan Türk boyları, sürülerine ve eşyalarına *tamga* adı verilen işaretler vururdu. Bir atın sağrısındaki tamga, onun hangi boya ait olduğunu, hiçbir söze gerek kalmadan, ilk bakışta anlatırdı. Aynı işaretler kayalara, mezar taşlarına, sikkelere de kazındı. Tamga basit bir çizgiden ibaret görünür ama aslında çok güçlü bir fikri taşır: **bir toplulukta herkesin tanıdığı bir işaret, tanımadığın biri hakkında sana güvenilir bir bilgi verir.** Atın sahibini tanımıyor olabilirsin, ama tamgayı tanıyorsun; tamgaya güvendiğin için de atın kime ait olduğuna güveniyorsun.

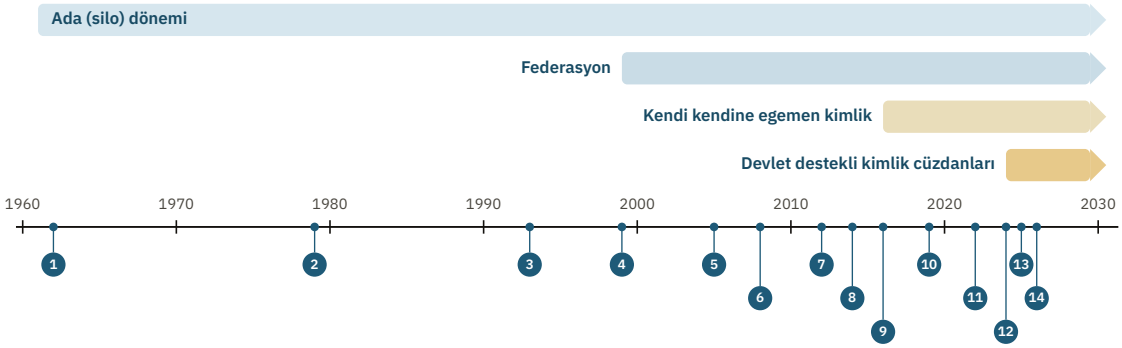
Bu yazının konusu olan dijital kimlik, özünde aynı soruya verilen modern bir cevaptır. Bir web sitesi karşısındaki kişinin gerçekten o kişi olduğunu nasıl bilir? Bir üniversite, başka bir ülkeden gelen diplomanın sahte olmadığını nasıl anlar? Bir banka, hesap açmak isteyen kişinin kimliğini şubeye gelmesini istemeden nasıl doğrular? Ve belki en önemlisi: bütün bunlar yapılırken kişinin gereğinden fazla bilgisi nasıl korunur?

Fiziksel dünyada bu soruların cevapları yüzyıllar içinde oturmuştur. Nüfus cüzdanımızı gösteririz; görevli fotoğrafa ve yüzümüze bakar, kartın sahte olmadığını hologramdan, dokusundan anlar. Diplomamızın aslını ya da noter onaylı suretini veririz. Bir resmî yazının altındaki ıslak imzaya ve mühre bakılır. Bu yöntemlerin hepsi üç şeye dayanır: belgenin **fiziksel olarak taklit edilmesinin zor olması**, işlemin **yüz yüze yapılması** ve belgeyi veren kurumun **herkesçe tanınması**.

Dijital dünyada bu üç dayanak birden çöker. Bir dosya, bir fotoğraf, bir PDF sınırsız kez ve kusursuzca kopyalanabilir; kopyayla aslı arasında hiçbir fark yoktur. İşlemlerin çoğu yüz yüze değildir; karşımızdakini görmeyiz, çoğu zaman karşımızda bir insan bile yoktur, bir sunucu vardır. Ve aynı anda dünyanın her yerinden, birbirini hiç tanımayan milyonlarca kurum ve kişiyle iş yaparız. 1993'te *The New Yorker* dergisinde yayımlanan ünlü bir karikatürde, bilgisayarın başındaki bir köpek yanındaki köpeğe şöyle der: *"İnternette kimse senin köpek olduğunu bilmez."* [1] Otuz yılı aşkın süredir dijital kimlik alanında yapılan çalışmaların neredeyse tamamı, bu karikatürün işaret ettiği sorunu çözme çabası olarak okunabilir.

Bu yazıda bu çabanın hikâyesini dört dönem hâlinde anlatıyoruz (Şekil 1):

1. **Ada (silo) dönemi** — her sistemin kendi kullanıcı hesaplarını ve parolalarını tuttuğu dönem.
2. **Federasyon dönemi** — kimliğin büyük sağlayıcılarda toplandığı, "Google ile giriş yap" döneminin.
3. **Kendi kendine egemen kimlik dönemi** — kimliği kişinin kendi cüzdanına taşımayı amaçlayan hareket.
4. **Devlet destekli kimlik cüzdanları dönemi** — bu fikirlerin hukuki güvenceyle birleştiği, bugün içinde bulunduğumuz dönem.



1. 1962 — CTSS'de bilinen ilk parola hırsızlığı
2. 1979 — Parola özetleme (Morris ve Thompson)
3. 1993 — "İnternette kimse senin köpek olduğunu bilmez"
4. 1999 — Microsoft Passport
5. 2005 — SAML 2.0 · OpenID · Kimliğin Yedi Yasası
6. 2008 — e-Devlet Kapısı
7. 2012 — OAuth 2.0
8. 2014 — OpenID Connect · eIDAS
9. 2016 — Kendi kendine egemen kimlik manifestosu
10. 2019 — WebAuthn (geçiş anahtarları)
11. 2022 — W3C DID 1.0
12. 2024 — eIDAS 2.0
13. 2025 — W3C VC 2.0
14. 2026 — AB'de cüzdan sunma son tarihi

Dönemler birbirinin yerini almaz, üst üste biner.

Şekil 1. Dijital kimliğin dört dönemi (yaklaşık tarihlerle)

Bu dönemleri anlatırken her birinde aynı üç soruyu soracağız; çünkü bir kimlik sistemini anlamanın en kısa yolu bu üç soruya verdiği cevaplara bakmaktır:

- **Kimliği kim veriyor?** Bir bilginin doğru olduğunu kim söylüyor?
- **Kimliği kim saklıyor?** Bilgi nerede duruyor ve kimin kontrolünde?
- **Doğrulama sırasında kim neyi görüyor?** Kişi kendini bir yere tanıttığında, bu işlemden kimlerin haberi oluyor?

Bir uyarıyla başlamak gerekir: Bu dönemler birbirinin yerini almadı. Bugün hâlâ birçok sitede kullanıcı adı ve parolayla giriyoruz, hâlâ "Google ile giriş" düğmesine basıyoruz. Dönemler, bir binanın katları gibi üst üste eklendi. Her yeni kat, bir öncekinin çözemediği bir sorunu çözmeye çalıştı ve çoğu zaman kendi yeni sorunlarını da beraberinde getirdi.

Yazının planı şöyle: Bölüm 2'de dijital kimlikle ilgili temel kavramları, hiçbir ön bilgi varsaymadan tanımlıyoruz. Bölüm 3–7 dört dönemi sırasıyla anlatıyor; Bölüm 6 kendi kendine egemen kimliği, Bölüm 7 ise Avrupa Birliği'nin yeni modelini ele alıyor. Bölüm 8 kimlik güvencesi düzeylerini, Bölüm 9 dört modelin karşılaştırmasını, Bölüm 10 ise hâlâ açık olan soruları tartışıyor. Bölüm 11 bu yazıyı yayımlayan Tamga Network'ün bu tablodaki yerini kısaca anlatıyor. Ek A'da yazıda geçen terimlerin sözlüğü var.

2 Temel Kavramlar: "Kimlik" Derken Neyi Kastediyoruz?

Gündelik dilde "kimlik" denince aklımıza çoğu zaman cüzdanımızdaki kart gelir. Oysa dijital kimlik alanında bu tek kelime, birbirine yakın ama birbirinden farklı birkaç kavramı karşılar. Bu kavramları baştan ayırmak, yazının geri kalanını anlamayı çok kolaylaştırır. Bir örnekle ilerleyelim.

ÖRNEK

Aynur'un hikâyesi

Aynur, Bakü'de lisansını bitirmiş, İstanbul'da yüksek lisans yapmak isteyen bir öğrenci. Başvuru için üniversiteye kimliğini, diplomasını, transkriptini ve dil belgesini sunması gerekiyor. Üniversite ise bu belgelerin gerçek olduğundan, Aynur'a ait olduğundan ve başvuruyu yapanın gerçekten Aynur olduğundan emin olmak istiyor. Bu yazı boyunca Aynur'un başvurusunun, her dönemde nasıl farklı yaşanacağına bakacağız.

2.1 Varlık, kimlik ve öznitelik

Varlık (*entity*), kimliğinden söz ettiğimiz şeydir: bir insan, bir kurum, bir cihaz ya da bir yazılım. Aynur bir varlıktır; üniversite de bir varlıktır.

Öznitelik (*attribute*), bir varlık hakkındaki tek bir bilgi parçasıdır: Aynur'un adı, doğum tarihi, uyruğu, mezun olduğu bölüm, not ortalaması. Özniteliklerin bir kısmı neredeyse hiç değişmez (doğum tarihi), bir kısmı zamanla değişir (adres), bir kısmı ise bir kurumun verdiği bir statüdür (öğrencilik, ehliyet sınıfı).

Kimlik (*identity*), bir varlığa ait özniteliklerin belirli bir bağlamdaki toplamıdır. Bu tanımın en önemli kısmı "belirli bir bağlamdaki" ifadesidir. Aynur'un üniversite için kimliği adı, diploması ve notlarından oluşur; bankası için kimliği adı, kimlik numarası ve geliri; bir sosyal medya sitesi için kimliği ise belki yalnızca bir takma ad ve bir profil fotoğrafıdır. Yani bir insanın tek bir kimliği yoktur; bağlama göre değişen **birçok kısmi kimliği** vardır. İyi tasarlanmış bir kimlik sistemi bu bağlamları birbirinden ayrı tutar; kötü tasarlanmış bir sistem ise hepsini tek bir dosyada birleştirir.

2.2 Tanımlayıcı

Tanımlayıcı (*identifier*), bir varlığı belirli bir sistem içinde diğerlerinden ayırmaya yarayan değerdir: T.C. kimlik numarası, öğrenci numarası, e-posta adresi, kullanıcı adı. Tanımlayıcı bir özniteliktir ama özel bir özniteliktir; görevi bilgi vermek değil, **ayırt etmektir**.

Tanımlayıcıların önemli bir özelliği **kapsamıdır**. Bir öğrenci numarası yalnızca o üniversite içinde anlamlıdır. Bir T.C. kimlik numarası ise bütün ülke içinde, bütün kurumlarda aynıdır. Kapsamı geniş tanımlayıcılar pratiktir ama bir bedeli vardır: farklı kurumların elindeki kayıtları birleştirmeyi, yani kişinin farklı bağlamlardaki kısmi kimliklerini tek bir profilde toplamayı çok kolaylaştırırlar. Bu konuya, bağlanabilirlik (*linkability*) adı altında, bu dizinin beşinci yazısında ayrıntılı olarak döneceğiz.

2.3 Kimlik bilgisi (belge)

Kimlik bilgisi (*credential*) — bu dizide çoğu zaman kısaca **belge** diyeceğiz — bir kurumun bir varlık hakkında söylediklerini taşıyan, o kurum tarafından onaylanmış bir kayıttır. Nüfus cüzdanı, diploma, ehliyet, pasaport, sağlık raporu fiziksel dünyadaki belgelerdir. Belgenin en önemli özelliği, **onu veren ile onu kullanan arasındaki ayrımdır**: Diplomayı üniversite verir, ama onu iş başvurusunda kullanan mezundur ve onu inceleyen işverendir. Bu üçlü yapıya ileride sık sık döneceğiz.

2.4 Kimlik doğrulama ve yetkilendirme

Kimlik doğrulama (*authentication*), "sen gerçekten iddia ettiğin kişi misin?" sorusunun cevaplanmasıdır. Bir sisteme "ben Aynur'um" dediğinizde, sistemin bunu kontrol etmesi kimlik doğrulamadır.

Yetkilendirme (*authorization*) ise kimlik doğrulandıktan sonra sorulan ikinci sorudur: "Peki, bu kişi bu işi yapmaya yetkili mi?" Aynur'un üniversite sistemine giriş yapması kimlik doğrulamadır; kendi notlarını görüp başkalarınınkini görememesi yetkilendirmedir. Bu iki kavram sık karıştırılır, ama ayrı tutulmaları gerekir; çünkü federasyon döneminde göreceğimiz gibi, birçok teknoloji aslında yetkilendirme için tasarlanmış, sonra kimlik doğrulama için de kullanılmaya başlanmıştır.

Kimlik doğrulama geleneksel olarak üç tür kanıta dayanır; bunlara **doğrulama faktörü** denir:

Tablo 1. Kimlik doğrulama faktörleri.

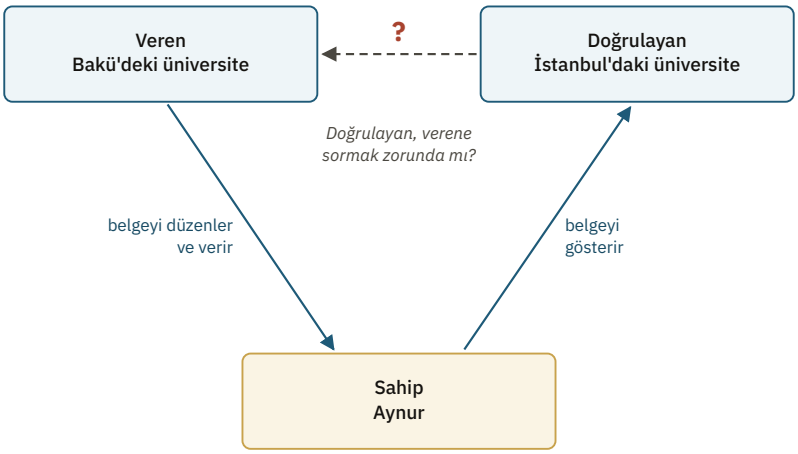
Faktör	Anlamı	Örnekler	Zayıf yanı
Bilinen bir şey	Yalnızca kişinin bildiği bir sır	parola, PIN, güvenlik sorusu	unutulur, tahmin edilir, çalınır, başka sitelerde de kullanılır
Sahip olunan bir şey	Yalnızca kişinin elinde olan bir nesne	telefon, akıllı kart, güvenlik anahtarı	kaybolur, çalınır
Olunan bir şey	Kişinin bedenine ait bir özellik	parmak izi, yüz, iris	değiştirilemez; bir kez sızarsa sonsuza dek sızmış olur

İki ya da daha fazla farklı türden faktörün birlikte kullanılmasına **çok faktörlü kimlik doğrulama** denir. Bankanızın uygulamasına parmak izinizle girmeniz, aslında iki faktördür: parmak iziniz (olunan) ve o parmak izinin yalnızca sizin telefonunuzda açtığı bir anahtar (sahip olunan).

2.5 Roller: veren, sahip, doğrulayan

Bir belgenin hayatında üç rol vardır ve bu üç rol, bu dizinin bütün yazılarında karşımıza çıkacak:

- **Veren** (*issuer*): Belgeyi düzenleyen ve içindeki bilginin doğruluğunu taahhüt eden kurum. Aynur'un diplomasını veren Bakü'deki üniversitesi.
- **Sahip** (*holder*): Belgeyi taşıyan ve gerektiğinde gösteren kişi. Aynur.
- **Doğrulayan** ya da **güvenen taraf** (*verifier, relying party*): Belgeyi inceleyip ona dayanarak bir karar veren kurum. İstanbul'daki üniversite.



Şekil 2. Bir belgenin üç rolü

Şekil 2'deki kesikli çizgi, yazının en önemli sorularından birini temsil ediyor: **Doğrulayan, belgenin gerçek olduğunu anlamak için belgeyi verene sormak zorunda mı?** Fiziksel dünyada çoğu zaman sormaz; diplomaya, mühre, imzaya bakar ve karar verir. Ama şüphelenirse, mezun olunan üniversiteye yazı yazar. Dijital dünyada bu sorunun cevabı, mahremiyet açısından çok büyük bir fark yaratır. Doğrulayan her seferinde verene soruyorsa, veren kurum Aynur'un belgesini **kime, ne zaman** gösterdiğini öğrenir. Bu duruma alan yazında "eve telefon etme" (*phone home*) sorunu denir. Dört dönemi anlatırken bu soruya her seferinde döneceğiz.

3 Fiziksel Dünyadan Dijital Dünyaya: Güvenin Üç Dayanağı Neden Çöktü?

Dijital kimliğin tarihine geçmeden önce, fiziksel dünyadaki düzenin neden bu kadar iyi işlediğini ve dijital dünyaya neden olduğu gibi taşınamadığını biraz daha ayrıntılı düşünmekte fayda var. Çünkü dijital kimlik alanındaki bütün teknolojiler, aslında fiziksel dünyadaki şu üç dayanağın dijital karşılığını kurmaya çalışıyor.

Birinci dayanak: taklit zorluğu. Bir pasaportun sayfalarındaki filigranlar, özel mürekkepler, hologramlar ve gömülü çipler tek bir amaca hizmet eder: belgeyi kopyalamayı, kopyalamanın getireceği kazançtan daha pahalı hâle getirmek. Taklit imkânsız değildir, ama zordur, pahalıdır ve dikkatli bir göz tarafından fark edilebilir. Dijital dünyada ise bir dosyanın kopyası, aslıyla **bit bit aynıdır**. Bir diplomanın taranmış PDF'i, bir fotoğraf düzenleme programıyla dakikalar içinde değiştirilebilir ve değiştirildiğini hiçbir göz fark edemez. Demek ki dijital dünyada taklit zorluğu belgenin fiziksel yapısından gelemez; başka bir yerden, matematikten gelmek zorundadır. Bu matematiğin adı **kriptografi**, onun bu iş için kullandığımız aracının adı da **dijital imza**dır (Bölüm 6.3'te ayrıntılı anlatıyoruz).

İkinci dayanak: yüz yüzelik. Bir banka gişesindeki görevli, size kimliğinizi uzattığınızda iki şeyi aynı anda kontrol eder: kartın gerçek olup olmadığını ve kartın üzerindeki fotoğrafın karşısındaki kişiye ait olup olmadığını. Yani hem belgeyi, hem de belgeyle kişi arasındaki bağı doğrular. İnternette ise bu bağ kopmuştur. Bir web sitesine bir kimlik kartının fotoğrafını yükleyebilirsiniz, ama o kartın sizin olduğunu kanıtlamak çok daha zordur. Dijital kimlik sistemleri bu bağı, belgeyi kişinin elindeki bir cihaza ya da yalnızca onun bildiği bir sırra **bağlayarak** kurar. Bu kavrama dizinin ikinci yazısında "sahip bağlama" (*holder binding*) adıyla ayrıntılı döneceğiz.

Üçüncü dayanak: tanınan veren. Bir nüfus cüzdanının değeri, onu veren devletin tanınmasından gelir. Hangi kurumun hangi belgeyi vermeye yetkili olduğu, toplumda herkesin bildiği ya da kolayca öğrenebileceği bir bilgidir. Dijital dünyada ise ölçek bu bilgiyi bozar: Dünyada on binlerce üniversite, yüz binlerce şirket, milyonlarca web sitesi var. Bir doğrulayan, bir belgenin altındaki dijital imzanın gerçekten "Bakü Devlet Üniversitesi"ne ait olduğunu ve bu üniversitenin gerçekten diploma vermeye yetkili bir kurum olduğunu nasıl bilecek? Bu soru, dijital kimliğin belki de en az konuşulan ama en zor sorusudur: **güvenin kaynağı** sorusu. Dizinin altıncı yazısı tamamen bu soruya ayrılmış durumda.

> ÖNEMLİ
>
> **Bu bölümden akılda kalması gereken**
>
> Fiziksel dünyada güven üç şeye dayanır: belgeyi taklit etmenin zorluğu, işlemin yüz yüze yapılması ve belgeyi verenin herkesçe tanınması. Dijital kimlik sistemlerinin hepsi, bu üç dayanağın dijital karşılığını kurmaya çalışır: taklit zorluğu yerine **dijital imza**, yüz yüzelik yerine **belgenin kişiye ya da cihazına bağlanması**, tanınan veren yerine **güvenilir kurum listeleri**. Dört dönemin her biri bu üç dayanaktan birini ya da birkaçını farklı biçimde kurmuştur.

4 Birinci Dönem: Adalar ve Parolalar

4.1 Her şey bir zaman paylaşım sisteminde başladı

1960'ların başında bilgisayarlar devasa, pahalı ve sayıca çok azdı. Bir üniversitede tek bir bilgisayar olur, araştırmacılar onu sırayla kullanırdı. Massachusetts Teknoloji Enstitüsü'nde (MIT) geliştirilen **CTSS** (*Compatible Time-Sharing System*), birden fazla kişinin aynı bilgisayarı aynı anda, kendi terminallerinden kullanmasını sağlayan ilk sistemlerden biriydi. Ancak bu yeni düzen yeni bir sorun doğurdu: Her kullanıcının kendi dosyaları ve kendisine ayrılmış bir kullanım süresi vardı. Sistem, terminalin başındaki kişinin kim olduğunu bilmek zorundaydı.

Çözüm bugün bize çok tanıdık gelecek kadar basitti: her kullanıcıya bir ad ve bir **parola** verildi. Bilgisayar tarihinin ilk parolalarının 1960'ların başında CTSS'de kullanıldığı kabul edilir [2]. İlginçtir ki bilinen ilk parola hırsızlığı da çok gecikmedi: 1962 baharında bir araştırmacı, kendisine ayrılan süreden fazlasını kullanabilmek için sistemdeki parola dosyasının çıktısını almanın bir yolunu buldu [2]. Yani parola, daha doğduğu ilk yıllarda hem en temel kimlik doğrulama yöntemi hem de en temel güvenlik açığı oldu. Altmış yılı aşkın süredir bu ikili durum değişmedi.

4.2 Bir parola nasıl saklanır?

İlk sistemler parolaları düz metin olarak, yani olduğu gibi bir dosyada saklıyordu. Bu dosyayı ele geçiren herkes bütün parolaları da ele geçirmiş oluyordu. Bu sorunun çözümü, kriptografinin en temel araçlarından birinden geldi: **özet fonksiyonu** (*hash function*).

TEKNİK AYRINTI

Özet fonksiyonu nedir?

Özet fonksiyonu, istediğiniz uzunlukta bir girdiyi alıp sabit uzunlukta bir çıktıya dönüştüren matematiksel bir işlemdir. İyi bir özet fonksiyonunun üç özelliği vardır:

1. **Tek yönlüdür.** Girdiden çıktıyı hesaplamak saniyenin milyonda biri kadar sürer; çıktıdan girdiyi geri bulmak ise pratikte imkânsızdır.
2. **Küçük değişikliğe büyük tepki verir.** Girdideki tek bir harf değişse, çıktı tamamen başka bir şeye dönüşür.
3. **Çakışmaya dayanıklıdır.** Aynı çıktıyı veren iki farklı girdi bulmak pratikte imkânsızdır.

Bugün en yaygın özet fonksiyonlarından biri SHA-256'dır. Örneğin "password" kelimesinin SHA-256 özeti şudur:

TEXT Örnek: "password" kelimesinin SHA-256 özeti

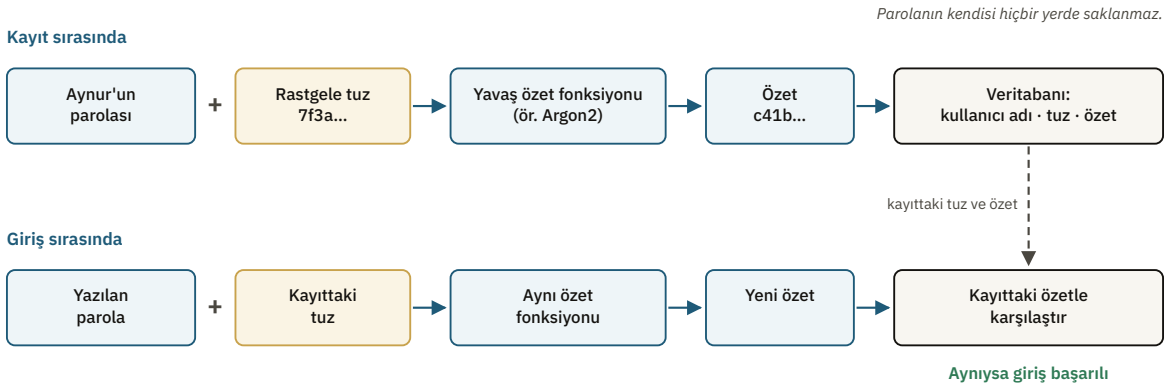
```
password → 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

Bu 64 karakterlik dizi, "password" kelimesinin bir tür parmak izidir. Aynı girdi her zaman aynı parmak izini verir; ama parmak izinden kelimeyi geri hesaplamanın bir yolu yoktur.

Özet fonksiyonu sayesinde sistem parolanın kendisini değil, yalnızca özetini saklayabilir. Aynur giriş yaparken parolasını yazar; sistem bu parolanın özetini hesaplar ve kayıttaki özetle karşılaştırır. İkisi aynıysa parola doğrudur. Dosyayı çalan biri ise yalnızca özetleri ele geçirir; parolaları değil.

Bu fikri sistemli biçimde anlatan ilk çalışmalardan biri, Robert Morris ve Ken Thompson'ın 1979'da yayımladığı "Password Security: A Case History" makalesidir [3]. Makale, Unix işletim sisteminde parolaların nasıl korunduğunu anlatırken bir sorunu daha ortaya koyuyordu: İnsanlar tahmin edilebilir parolalar seçer. Saldırgan parolayı özetten geri hesaplayamasa bile, sık kullanılan bir milyon parolanın özetini önceden hesaplayıp bir tabloya yazabilir. Sonra çaldığı özetleri bu tabloda arar. Yukarıdaki örnekte "password" kelimesinin özetini görür görmez tanıyacaktır, çünkü bu özet her tabloda vardır.

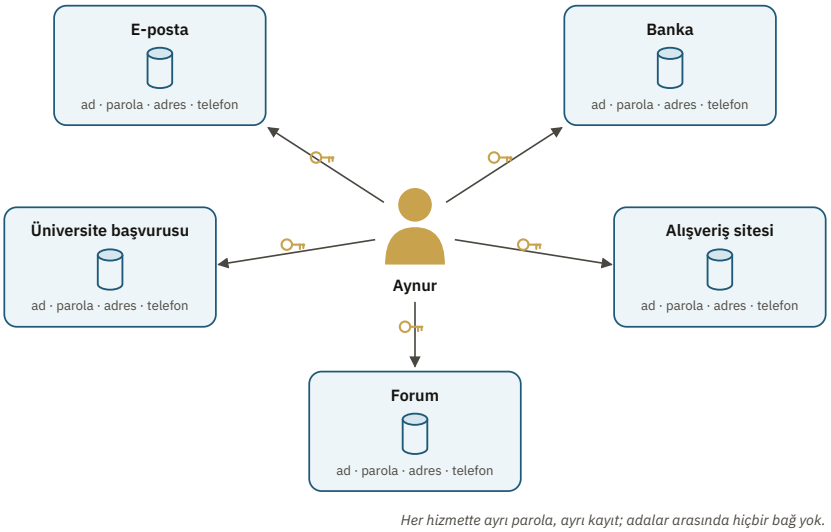
Bunun çözümü **tuz** (*salt*) adı verilen bir yöntemdir: Her kullanıcı için rastgele bir değer üretilir, parola bu değerle birleştirilip öyle özetlenir ve tuz da özetin yanında saklanır. Böylece iki kullanıcı aynı parolayı seçse bile özetleri farklı olur ve önceden hesaplanmış tablolar işe yaramaz hâle gelir. Bugün iyi tasarlanmış sistemler buna bir adım daha ekler ve parolayı özetlerken **bilerek yavaş** çalışan özel fonksiyonlar (bcrypt, scrypt, Argon2 gibi) kullanır. Bir kullanıcının giriş yaparken fark etmeyeceği yüz milisaniyelik bir gecikme, milyarlarca parolayı denemeye çalışan bir saldırganın işini binlerce yıla çıkarabilir.



Şekil 3. Bir parolanın tuzlanıp özetlenerek saklanması ve girişte kontrol edilmesi

4.3 Ada modelinin sorunları

Parolaların güvenli saklanması büyük bir ilerlemeydi. Ama asıl sorun teknik değil yapısaldı ve internetin yaygınlaşmasıyla bütün açıklığıyla ortaya çıktı. Bu dönemde her web sitesi, her uygulama, her kurum **kendi kullanıcı veritabanını** tutar. Bu yüzden bu modele **ada** ya da **silo** modeli denir: her sistem kendi adasında yaşar, diğerlerinden habersizdir (Şekil 4).



Şekil 4. Ada (silo) modeli: her hizmetin kendi kullanıcı kaydı

Bu modelin kullanıcı için ilk sonucu **parola yorgunluğudur**. Ortalama bir internet kullanıcısının onlarca, belki yüzlerce hesabı vardır. Her biri için ayrı, güçlü, akılda kalması imkânsız bir parola seçmek insan doğasına aykırıdır. Sonuç tahmin edilebilir: İnsanlar aynı parolayı birçok yerde kullanır ya da küçük değişikliklerle tekrar eder.

İkinci sonuç, bu davranışın açtığı yeni bir saldırı türüdür: **kimlik bilgisi doldurma** (*credential stuffing*). Bir sitenin veritabanı sızdırıldığında, saldırganlar oradaki e-posta ve parola çiftlerini alır ve otomatik araçlarla başka yüzlerce sitede dener. Aynur'un yıllar önce üye olduğu ve unuttuğu küçük bir forumun veritabanı sızarsa, aynı parolayı kullandığı e-posta hesabı da tehlikeye girer. Yani ada modelinde bir sistemin güvenliği, kullanıcının **en zayıf adasının** güvenliği kadardır.

Üçüncü sonuç, **oltalama**dır (*phishing*). Parola, gerçek siteye girildiğinde de sahte siteye girildiğinde de aynı parola olduğu için, kullanıcıyı gerçeğine çok benzeyen bir sahte sayfaya yönlendirmek parolayı çalmak için yeterlidir. Parola, doğası gereği **kime söylendiğini bilmeyen** bir sırdır.

Dördüncü sonuç, veri birikimidir. Her ada, kendi kayıt formunda kişiden ad, soyad, doğum tarihi, adres, telefon ister. Aynı bilgi onlarca farklı yerde, onlarca farklı güvenlik düzeyiyle saklanır. Kişi, bilgisinin nerede durduğunu çoğu zaman bilmez bile; adresi değiştiğinde hangi kayıtların eskidiğini takip edemez.

Ve beşinci, belki en temel sorun: **Ada modelinde kimse kimseyi doğrulamaz.** Bir siteye "adım Aynur, 1999 doğumluyum" diye kayıt olduğunuzda, site bunun doğru olup olmadığını bilemez. Parola yalnızca "bu hesabı açan kişi ile şimdi giriş yapan kişi aynı kişi" olduğunu kanıtlar; o kişinin gerçekte kim olduğunu değil. Bu yüzden ada modeli, bir bankanın ya da üniversitenin ihtiyaç duyduğu **güvenilir kimlik** sorununu çözmez; yalnızca bir hesabın sürekliliğini sağlar.

> ÖRNEK
>
> **Aynur ada döneminde**
>
> Aynur, İstanbul'daki üniversitenin başvuru sistemine e-posta adresi ve yeni bir parolayla üye olur. Formu doldurur; diplomasının, transkriptinin ve pasaportunun taranmış kopyalarını yükler. Üniversite bu dosyaların gerçek olduğunu anlayamaz; bir taramanın düzenlenip düzenlenmediğini kimse göremez. Bu yüzden Aynur'dan belgelerin noter ve apostil onaylı asıllarını da posta ile göndermesi istenir. Haftalar süren bir süreç başlar. Kimliğin "dijital" olan tek parçası, Aynur'un o sisteme bir daha giriş yapabilmesini sağlayan parolasıdır.

4.4 Ada döneminin bugünkü mirası

Ada modeli hâlâ yaşıyor ve muhtemelen uzun yıllar da yaşayacak. Ama onu güçlendiren iki gelişme anılmaya değer. İlki, bir telefona gönderilen tek kullanımlık kodlar ya da kimlik doğrulama uygulamalarıyla yapılan **iki faktörlü doğrulama**dır. İkincisi ve çok daha köklü olanı ise **geçiş anahtarları**dır (*passkeys*). 2019'da W3C tarafından standartlaştırılan WebAuthn [4], parolanın yerine telefonda ya da bilgisayarda saklanan ve **yalnızca kayıtlı olduğu siteye** cevap veren bir kriptografik anahtar çifti koyar. Geçiş anahtarı, parolanın iki büyük zaafını birden giderir: sunucuda çalınabilecek bir sır saklanmaz ve anahtar sahte bir siteye hiçbir şey vermez, çünkü hangi siteyle konuştuğunu bilir.

Yine de geçiş anahtarları da ada modelinin içindedir: Bir sitenin size güvenli biçimde "bu yine sensin" demesini sağlar, ama "sen gerçekten Aynur'sun ve bu diploma gerçekten senin" demesini sağlamaz. Bu ikinci soruya cevap aramak için kimliği adaların dışına taşımak gerekiyordu.

5 İkinci Dönem: Federasyon ve "Google ile Giriş Yap"

5.1 Fikir: Kimliği bir kez doğrula, her yerde kullan

1990'ların sonunda internet ticarileştikçe ada modelinin sorunları katlandı. Çözüm fikri basitti: Kullanıcının kimliğini her sitenin ayrı ayrı doğrulaması yerine, bu işi bir **kimlik sağlayıcı** (*identity provider*) üstlensin. Kullanıcı yalnızca kimlik sağlayıcıya giriş yapsın; diğer siteler de "bu kullanıcı kim?" sorusunu kimlik sağlayıcıya sorsun. Kimlik doğrulama işini devraldıkları için bu sitelere **güvenen taraf** (*relying party*) denir: kimlik sağlayıcının sözüne güvenirler.

Bu modele **federasyon** (*federated identity*) denir, çünkü birbirinden bağımsız kurumlar ortak kurallar üzerinde anlaşarak bir tür kimlik birliği oluşturur. Fikrin en tanıdık örneği bugün her sitede gördüğümüz "Google ile giriş yap", "Apple ile giriş yap" düğmeleridir. Ama federasyonun ilk ve en güçlü kullanım alanı aslında kurumların içi oldu: Bir şirketin çalışanı sabah bir kez giriş yapar, gün boyunca e-postasına, insan kaynakları sistemine, muhasebe yazılımına ayrı ayrı parola girmeden erişir. Bu deneyime **tek oturum açma** (*single sign-on, SSO*) denir.

5.2 Kısa bir tarihçe

TARİHÇE

Federasyonun yolu: Passport'tan OpenID Connect'e

1999 — Microsoft Passport. Microsoft, kullanıcıların tek bir hesapla Hotmail'e ve ortak sitelere girmesini sağlayan bir hizmet başlattı. Teknik olarak öncüydü ama çok merkezîydi: Bütün kimlik verisi tek bir şirkette toplanıyordu. Diğer şirketler buna güvenmedi; gizlilik ve güvenlik eleştirileri hizmetin geniş çapta benimsenmesini engelledi.

2001 — Liberty Alliance. Microsoft'un tek merkezli modeline karşı, aralarında Sun Microsystems'in de bulunduğu bir grup şirket, birden çok kimlik sağlayıcının birlikte çalışabildiği açık standartlar geliştirmek için bir birlik kurdu.

2005 — SAML 2.0. OASIS standart kuruluşu, Liberty Alliance'ın çalışmalarını da içine alan SAML (*Security Assertion Markup Language*) 2.0 standardını yayımladı [5]. SAML, bugün hâlâ kurumsal tek oturum açmanın ve üniversite kimlik federasyonlarının omurgasıdır.

2005 — OpenID. Kurumsal dünyanın ağır standartlarına karşı, bireysel kullanıcılar için hafif, merkezi-yetsiz bir model: Kişi istediği bir OpenID sağlayıcısı seçer ve web adresini kimliği olarak kullanır. Fikir zarifti, ama kullanıcı deneyimi zordu ve yaygınlaşmadı.

2008 ve sonrası — sosyal giriş. Büyük sosyal ağlar, kendi kullanıcı tabanlarını başka sitelere açtı. "Facebook ile bağlan" gibi düğmeler kısa sürede internetin her yerine yayıldı.

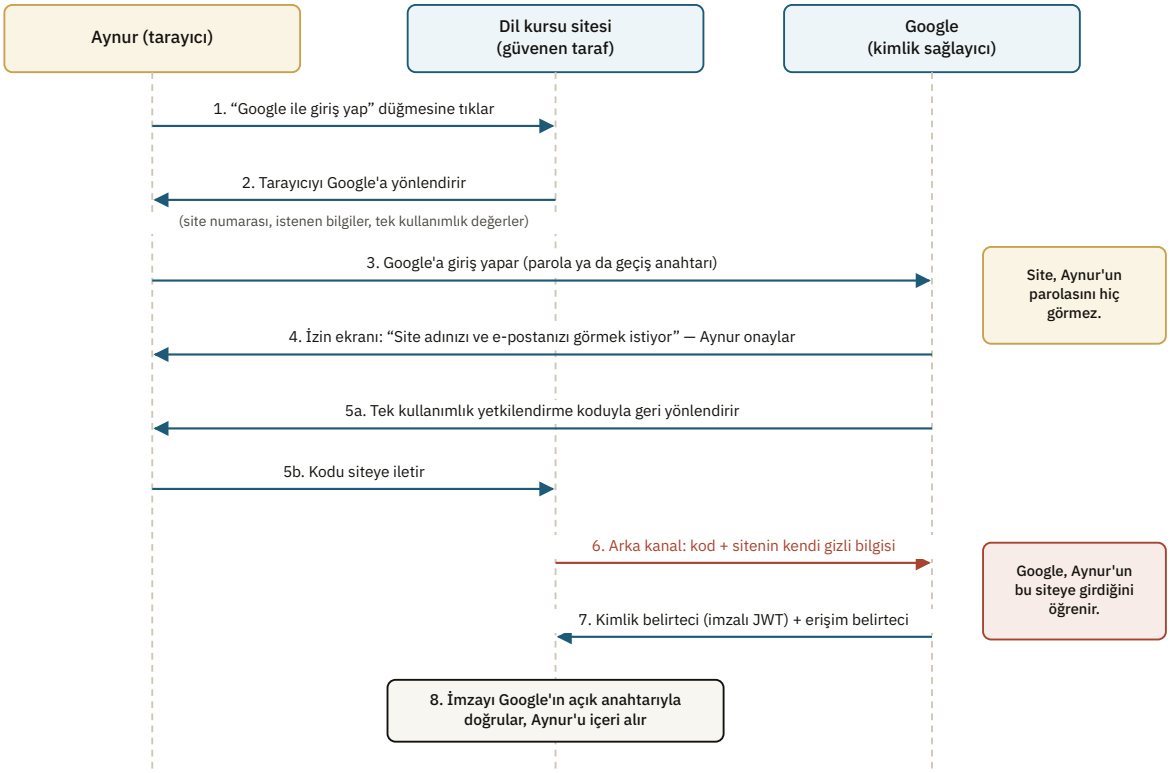
2012 — OAuth 2.0. IETF, bir uygulamanın kullanıcının başka bir hizmetteki verisine, kullanıcının paro-lasını öğrenmeden erişmesine izin veren OAuth 2.0 yetkilendirme çerçevesini yayımladı [6].

2014 — OpenID Connect. OpenID Vakfı, OAuth 2.0'ın üzerine bir kimlik katmanı ekleyerek OpenID Connect'i yayımladı [7]. Bugün "Google ile giriş" düğmesinin arkasındaki teknoloji büyük ölçüde budur.

Bu tarihçedeki en ilginç ders şudur: Teknik olarak en iyi çözüm her zaman kazanmadı. Microsoft Passport ilk denemeydi ama tek bir şirkete güvenmek istenmediği için yaygınlaşamadı. OpenID zarifti ama kullanıcı için anlaşılmazdı. Sonunda kazanan, **milyarlarca kullanıcısı zaten olan** şirketlerin sunduğu basit bir düğme oldu. Dijital kimlikte benimsenmeyi belirleyen çoğu zaman teknoloji değil, **kullanıcının zaten nerede olduğudur**. Bu ders, dördüncü dönemde devletlerin neden işin içine girdiğini anlamak için de önemli.

5.3 "Google ile giriş" düğmesine bastığınızda ne olur?

Federasyonu gerçekten anlamak için, o tanıdık düğmeye bastığınız an ile siteye giriş yapmış olduğu-nuz an arasında geçen yaklaşık iki saniyede neler olduğuna yakından bakalım. Anlatacağımız akış OpenID Connect'in en yaygın biçimi olan "yetkilendirme kodu akışı"dır (Şekil 5). Örnekte Aynur, bir dil kursunun sitesine Google hesabıyla giriş yapıyor.



Şekil 5. OpenID Connect ile giriş: yetkilendirme kodu akışı

Adım adım gidelim:

1–2. Yönlendirme. Aynur düğmeye bastığında dil kursu sitesi, Aynur’un tarayıcısını Google’ın giriş sayfasına yönlendirir. Bu yönlendirmenin adresine birkaç bilgi eklenir: sitenin Google’daki kayıt numarası (*client_id*), sitenin hangi bilgileri istediği (örneğin ad ve e-posta; buna *kapsam*, *scope* denir), işlem bitince Aynur’un hangi adrese geri gönderileceği ve saldırılara karşı koruma için üretilmiş tek kullanımlık rastgele değerler.

3–4. Giriş ve izin. Aynur artık Google’ın sayfasındadır. Google’a daha önce giriş yapmışsa bu adım fark edilmeden geçer; yapmamışsa parolasını ya da geçiş anahtarını kullanır. Sonra Google ona bir izin ekranı gösterir: “Dil kursu sitesi adınızı, e-posta adresinizi ve profil fotoğrafınızı görmek istiyor.” Burada dikkat edilmesi gereken nokta şudur: **Dil kursu sitesi Aynur’un parolasını hiçbir zaman görmez.** Parola yalnızca Google’a girilir. Bu, ada modeline göre büyük bir güvenlik kazancıdır: Dil kursunun veritabanı sızsa bile orada çalınacak bir parola yoktur.

5. Kodla geri dönüş. Aynur onay verince Google, tarayıcıyı dil kursu sitesine geri yönlendirir ve adresin sonuna kısa ömürlü, tek kullanımlık bir **yetkilendirme kodu** ekler. Bu kod tek başına bir işe yaramaz; yalnızca bir sonraki adımda, kısa bir süre içinde, bir kez kullanılabilir.

6–7. Arka kanal. Dil kursu sitesi bu kodu alır ve tarayıcıyı aradan çıkararak doğrudan, sunucudan sunucuya Google’a gönderir. Bunu yaparken kendi kimliğini de kanıtlar (Google’a kayıt olurken aldığı bir gizli bilgiyle ya da bir anahtarla). Google kodu kontrol eder ve karşılığında iki şey verir: bir **erişim belirteci** (*access token*), sitenin daha sonra Aynur adına Google’dan bilgi istemesi için, ve bir **kimlik belirteci** (*ID token*), yani asıl kimlik bilgisi.

8. İmzanın doğrulanması. Kimlik belirteci, JSON Web Token (JWT) adı verilen bir biçimdedir [8] ve Google tarafından dijital olarak imzalanmıştır. Site bu imzayı Google’ın herkese açık olarak yayımladığı anahtarla doğrular. İmza doğruysa, belirtecin içeriğinin gerçekten Google’dan geldiğinden ve yolda değiştirilmediğinden emin olur ve Aynur’u içeri alır.

TEKNİK AYRINTI

Bir kimlik belirtecinin içi

JWT üç parçadan oluşur ve parçalar noktayla ayrılır: **başlık.içerik.imza**. Başlık hangi imza algoritmasının kullanıldığını, içerik asıl bilgiyi, imza ise ilk iki parçanın Google'ın gizli anahtarıyla imzalanmış hâlini taşır. Her parça, internette güvenle taşınabilsin diye Base64URL adlı bir yöntemle metne dönüştürülür; bu yüzden bir JWT ilk bakışta anlamsız bir harf dizisi gibi görünür. İçerik kısmı çözüldüğünde ise şöyle bir şeyle karşılaşırız (değerler örnektir):

JSON Örnek: kimlik belirtecinin (JWT) çözülmüş içerik kısmı

```json
{
  "iss": "https://accounts.google.com",
  "sub": "110169484474386276334",
  "aud": "dil-kursu-sitesi-istemci-numarasi",
  "iat": 1793606400,
  "exp": 1793610000,
  "nonce": "n-0S6_WzA2Mj",
  "email": "aynur@example.com",
  "email_verified": true,
  "name": "Aynur …"
}
```

- `iss` (*issuer*): belirteci kim verdi — Google.
- `sub` (*subject*): Google'ın bu kullanıcıya verdiği kalıcı tanımlayıcı.
- `aud` (*audience*): belirteç kimin için üretildi — yalnızca bu site kabul etmeli.
- `iat` ve `exp`: ne zaman üretildi, ne zaman geçersiz olacak (saniye cinsinden zaman damgası). Belirteç birkaç dakika ya da bir saat geçerlidir.
- `nonce`: sitenin 2. adımda ürettiği tek kullanımlık değer; aynı belirtecin tekrar kullanılmasını engeller.

Dikkat edin: Bu belirteç Google'ın imzasını taşıyan, **doğrulanabilir** bir kayıttır. Ama ömrü kısadır ve yalnızca tek bir site için üretilmiştir. Aynur onu alıp başka bir yerde kullanamaz. Federasyonda kimlik bilgisi kişinin **elinden geçer** ama kişi onu **tutmaz** her giriş için kimlik sağlayıcı yeni bir belirteç üretir.

5.4 Federasyon neyi çözdü?

Federasyon, ada modelinin en ağır sorunlarının birçoğunu çözdü. Kullanıcı tek bir güçlü hesabı korur; onlarca parolayla uğraşmaz. Küçük siteler parola saklama sorumluluğundan kurtulur; büyük kimlik sağlayıcılar ise güvenliğe çok daha fazla yatırım yapabilir, şüpheli girişleri tespit edebilir, çok faktörlü doğrulamayı yaygınlaştırabilir. Kurumsal dünyada bir çalışan işten ayrıldığında tek bir hesabı kapatmak, onun bütün sistemlere erişimini kesmeye yeter. Üniversiteler arasında kurulan federasyonlar sayesinde bir araştırmacı başka bir ülkedeki üniversitenin kütüphanesine kendi kurumunun hesabıyla girebilir.

Daha da önemlisi, federasyon **doğrulanmış özniteliklerin** taşınmasının da yolunu açtı. Bir kimlik sağlayıcı yalnızca "bu kişi şu hesabın sahibi" demekle kalmaz, "bu kişinin e-postası doğrulanmış", "bu kişi şu üniversitenin öğrencisi" gibi bilgileri de imzalı olarak iletebilir. Devletler de bu modeli benimsedi: Türkiye'de 2008'de hizmete giren **e-Devlet Kapısı**, özünde bir devlet kimlik sağlayıcısıdır; vatandaş e-Devlet şifresi, e-imza ya da mobil imza ile bir kez giriş yapar ve yüzlerce kamu hizmetine erişir. Estonya'nın kimlik kartı ve ona bağlı dijital hizmetler, Hindistan'ın Aadhaar sistemi gibi ulusal kimlik altyapıları da, farklı mimarilerle de olsa, merkezî bir kimlik sağlayıcının sorulara cevap verdiği modeller üzerine kuruludur.

5.5 Federasyonun bedeli

Federasyon kullanıcıya kolaylık getirdi, ama bu kolaylığın görünmeyen bir bedeli vardı. Bu bedeli görmek için, Bölüm 2'deki üç soruyu tekrar soralım.

Kimliği kim veriyor? Kimlik sağlayıcı. **Kimliği kim saklıyor?** Yine kimlik sağlayıcı. **Doğrulama sırasında kim neyi görüyor?** İşte burada sorun başlıyor. Şekil 5'teki 6. ve 7. adımlara dikkat edin:

Aynur her giriş yaptığında, dil kursu sitesi Google'a doğrudan bağlanır. Yani **Google, Aynur'un hangi siteye, hangi gün, hangi saatte girdiğini öğrenir**. Bu, Bölüm 2'de söz ettiğimiz "eve telefon etme" sorununun ta kendisidir. Federasyonda kimlik sağlayıcı, kullanıcının dijital hayatının **her kapısında bekleyen bir kapıcı** gibidir. Aynur'un hangi sitelere üye olduğunu, ne sıklıkla girdiğini, hangi saatlerde aktif olduğunu bilen tek bir kurum vardır.

Bu bilginin değeri büyüktür. Sosyal giriş düğmelerinin bu kadar hızlı yayılmasının nedenlerinden biri de budur: Düğmeyi sunan şirket, karşılığında kullanıcının internetteki dolaşımına dair zengin bir veri elde eder. Bu verinin nasıl kullanılabileceğine dair belki de en çarpıcı örnek, 2018'de kamuoyuna yansıyan Cambridge Analytica olayıdır. Facebook'un kendi açıklamasına göre, bir kişilik testi uygulaması aracılığıyla yaklaşık 87 milyon kişinin verisi bu kişilerin bilgisi olmadan bir siyasi danışmanlık şirketinin eline geçmişti [9]. Olay doğrudan bir giriş protokolü açığı değildi; ama bir platforma "bu uygulamaya izin ver" diye tıklamanın, kişinin sandığından çok daha fazla veriyi açabileceğini herkese gösterdi.

İkinci bedel **bağımlılık**tır. Kimliğiniz kimlik sağlayıcının elindedir ve sizin değil, onun kurallarına tabidir. Hesabınız bir gün herhangi bir nedenle (yanlış bir otomatik tespit, kural ihlali iddiası, şirketin bir ülkeden çekilmesi) kapatılırsa, o hesapla girdiğiniz bütün sitelere erişiminizi de bir anda kaybedebilirsiniz. Federasyon, ada modelindeki onlarca kırılgan kilidi, **tek bir büyük kilitle** değiştirmiştir. O kilidin anahtarı ise sizde değildir.

Üçüncü bedel **güvenin sınırlılığıdır**. Bir sosyal ağın "bu kişinin e-postası doğrulanmış" demesi, bir alışveriş sitesi için yeterli olabilir; ama bir bankanın ya da bir üniversitenin ihtiyaç duyduğu güvence bu değildir. Sosyal kimlik sağlayıcıları genellikle kişinin gerçek kimliğini doğrulamaz; doğrulasalar bile bunu hukuki bir sorumluluk altında yapmazlar. Devlet kimlik sağlayıcıları ise yüksek güvence sunar, ama genellikle **yalnızca kendi ülkelerinde** ve çoğunlukla yalnızca kamu hizmetleri için. Aynur'un Azerbaycan'daki devlet kimliğini İstanbul'daki bir üniversite doğrudan kullanamaz.

ÖRNEK

Aynur federasyon döneminde

Aynur bu kez üniversitenin başvuru sistemine Google hesabıyla girer; yeni bir parola oluşturması gerekmez. Ama üniversite Google'dan yalnızca adını ve e-postasını öğrenir. Diploması, transkripti, pasaportu konusunda hiçbir şey değişmemiştir; yine taranmış kopyalar, yine noter ve apostil onaylı asıllar, yine haftalar. Bakü'deki üniversitesi kendi öğrencileri için bir kimlik sağlayıcı işletiyor olsa bile, İstanbul'daki üniversite o federasyonun üyesi değildir; üye olsa bile, Aynur'un her başvurusunda Bakü'deki üniversite bundan haberdar olacaktır.

ÖNEMLİ

Bu bölümden akılda kalması gereken

Federasyon kimlik doğrulamayı kolaylaştırdı ve parolaları daha güvenli hâle getirdi. Ama kimliği kişinin elinden alıp büyük bir sağlayıcıya teslim etti; o sağlayıcı da her girişte kişinin nereye gittiğini görmeye başladı. Federasyonda kimlik bilgisi bir **nesne** değil, bir **hizmettir**: Kişi onu taşımaz, her seferinde sağlayıcıdan yeniden ister.

5.6 Bir ara durak: Kimliğin Yedi Yasası

Federasyonun yükseldiği yıllarda, bu modelin sınırlarını en açık biçimde dile getirenlerden biri bir Microsoft mühendisiydi. Kim Cameron, 2005'te yayımladığı **"Kimliğin Yasaları"** (*The Laws of Identity*) adlı yazısında, kalıcı ve yaygın bir internet kimlik sisteminin uyması gereken yedi ilkeyi sıraladı [10]. Bu ilkeler bugün okunduğunda şaşırtıcı derecede güncel görünür; çünkü sonraki yirmi yılda tartışılan neredeyse bütün konuları önceden işaret eder:

Tablo 2. Kim Cameron'ın yedi yasası (2005) ve bugünkü karşılıkları.

#	Yasa	Anlamı	Bugün nerede karşımıza çıkıyor
1	Kullanıcı kontrolü ve onayı	Kişi, bilgisinin paylaşılmasına bilerek izin vermeli	cüzdanlarda her paylaşım öncesi onay ekranı
2	Kısıtlı kullanım için asgari açıklama	Bir iş için gerekenden fazla bilgi açılmamalı	seçici açıklama (dizinin 3. yazısı)
3	Haklı taraflar	Bilgi yalnızca işlemde meşru yeri olan taraflara gitmeli	"eve telefon etme" sorununun reddi
4	Yönlendirilmiş kimlik	Herkese açık tanımlayıcılar ile kişiye özel tanımlayıcılar ayrılmalı	siteye özel takma adlar (dizinin 5. yazısı)
5	İşletmecilerin ve teknolojilerin çoğulculuğu	Tek bir sağlayıcı ya da teknoloji olmamalı	birden çok cüzdan, birden çok belge biçimi
6	İnsanla bütünleşme	Kullanıcı sistemin bir parçası olarak tasarlanmalı	cüzdan arayüzü tasarımı
7	Bağlamlar arası tutarlı deneyim	Kişi farklı bağlamlarda neyi paylaştığını aynı biçimde görebilmeli	ortak cüzdan deneyimi kuralları

Cameron'ın ilkeleri, Microsoft'un 2006'da tanıttığı *CardSpace* adlı bir ürüne dönüştü. CardSpace, kimlikleri bilgisayarda "kartlar" olarak saklıyor, kullanıcıya bir siteye hangi kartı göstereceğini seçtiriyordu; bugünkü kimlik cüzdanlarının şaşırtıcı derecede erken bir öncüsüydü. Ancak web siteleri onu benimsemedi ve Microsoft Şubat 2011'de ürünün yeni sürümünü çıkarmayacağını açıkladı. CardSpace'in başarısızlığı, federasyon tarihindeki dersi bir kez daha doğruladı: Doğru fikir, doğru zamanda ve doğru benimseme koşullarıyla buluşmadıkça yayılmaz. Bu fikirlerin geri dönmesi için on yıl daha geçmesi gerekecekti.

6 Üçüncü Dönem: Kendi Kendine Egemen Kimlik

6.1 Bir manifestonun doğuşu

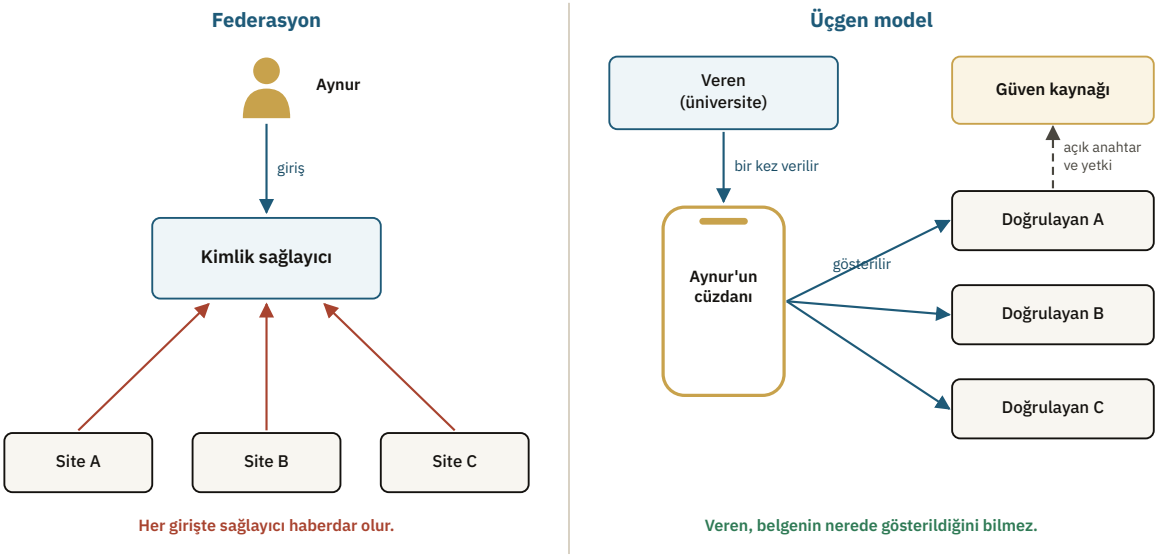
2016 Nisan'ında Christopher Allen adlı bir teknoloji uzmanı, "Kendi Kendine Egemen Kimliğe Giden Yol" (*The Path to Self-Sovereign Identity*) başlıklı bir yazı yayımladı [11]. Allen, internet kimliğinin tarihini dört aşamaya ayırıyordu: merkezî kimlik (bizim ada dönemimiz), federe kimlik, kullanıcı merkezli kimlik (Cameron'ın fikirleri ve OpenID gibi girişimler) ve son olarak henüz kurulmamış olan **kendi kendine egemen kimlik** (*self-sovereign identity*, kısaca SSI). Ona göre ilk üç aşamanın ortak sorunu, kimliğin her zaman **bir başkasının sisteminde** yaşamasıydı. Kişi kimliğini bir kurumdan kiralıyordu; o kurum istediği an onu geri alabilirdi.

SSI'ın temel iddiası şuydu: **Kimlik kişiye ait olmalı.** Kişi kimlik bilgilerini kendi denetimindeki bir yazılımda, bir **dijital cüzdanda** tutmalı; kime, ne zaman, ne kadarını göstereceğine kendisi karar vermeli; bir doğrulayan, belgenin gerçek olduğunu anlamak için veren kuruma sormak zorunda kalmamalı. Allen bu fikri on ilkeyle somutlaştırdı: varlık, kontrol, erişim, şeffaflık, kalıcılık, taşınabilirlik, birlikte çalışabilirlik, onay, asgarileştirme ve koruma.

Bu fikirler boşlukta doğmadı. Aynı yıllarda blokzincir teknolojisi büyük bir ilgi görüyordu ve SSI hareketinin önemli bir kısmı, kimlik sisteminin "güven kaynağını" tek bir kurum yerine merkeziyetsiz bir deftere taşıma fikriyle birleşti. Bu birleşme hem hareketin enerjisinin hem de, aşağıda göreceğimiz gibi, sorunlarının önemli bir kaynağı oldu.

6.2 Üçgen model: veren, sahip, doğrulayan

SSI'ın getirdiği asıl yenilik, Bölüm 2.5'te tanımladığımız üç rolü dijital dünyada **gerçekten ayırmak** oldu. Federasyonda kimlik sağlayıcı hem veren hem de her doğrulamanın aracısıydı. SSI'da ise bu iki iş birbirinden kopar (Şekil 6):



Şekil 6. Kendi kendine egemen kimlikte üçgen model ve federasyonla farkı

1. **Veren**, bir kez belge düzenler ve onu dijital olarak imzalar. Örneğin Aynur'un üniversitesi, Aynur'un diplomasını dijital bir belge olarak üretir, imzalar ve Aynur'un cüzdanına gönderir.
2. **Sahip**, yani Aynur, bu belgeyi kendi cüzdanında saklar. Belge artık bir hizmet değil, Aynur'un elindeki bir **nesnedir** tıpkı fiziksel diploma gibi.
3. **Doğrulayan**, belgeyi Aynur'dan alır ve veren kuruma sormadan, yalnızca imzayı kontrol ederek gerçek olup olmadığını anlar.

Bu modelde veren kurum, Aynur'un diplomasını **kime gösterdiğini bilmez**. Federasyondaki "her kapıda bekleyen kapıcı" ortadan kalkmıştır. Fiziksel diploma ile aynı mahremiyet düzeyine, ama dijitalin hızı ve sahteciliğe karşı dayanıklılığıyla ulaşılmıştır. Bu, SSI hareketinin kalıcı katkısıdır ve dördüncü dönemin sistemleri de bu modeli aynen benimsemiştir.

6.3 Dijital imza: Taklit zorluğunun matematikle kurulması

Bölüm 3'te, dijital dünyada taklit zorluğunun belgenin fiziksel yapısından gelemeyeceğini, matematikten gelmesi gerektiğini söylemiştik. Üçgen modelin tamamı bu matematiğe dayandığı için, onu biraz açmakta fayda var.

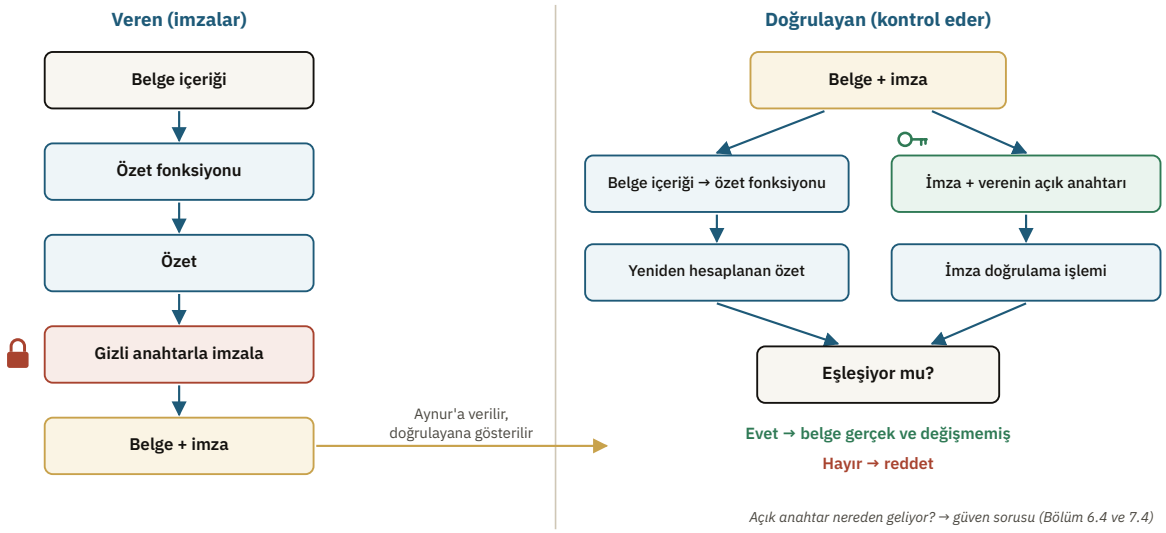
Dijital imza, **açık anahtarlı kriptografi** (*public-key cryptography*) adı verilen bir yönteme dayanır. Bu yöntemde her taraf, birbirine matematiksel olarak bağlı iki anahtardan oluşan bir **anahtar çifti** üretir:

- **Gizli anahtar** (*private key*): Yalnızca sahibinde kalır, hiç kimseyle paylaşılmaz.
- **Açık anahtar** (*public key*): Herkesle paylaşılabilir, hatta herkesin bilmesi gerekir.

Bu iki anahtarın ilişkisi bir **mühür ve onun kaydı** gibi düşünülebilir. Gizli anahtar mühürdür: Yalnızca sahibi onunla mühür basabilir. Açık anahtar ise o mührün herkesin elinde bulunan bir örneğidir: Herkes, bir belgedeki mühür izini bu örnekle karşılaştırıp mührün gerçek olup olmadığını anlayabilir; ama örneğe bakarak yeni bir mühür basamaz.

Matematiksel olarak süreç şöyle işler:

1. **İmzalama.** Veren kurum önce belgenin içeriğinin özetini (Bölüm 4.2'deki gibi) çıkarır. Sonra bu özeti kendi gizli anahtarıyla bir matematiksel işlemden geçirir. Ortaya çıkan değer **imzadır**. İmza belgeye eklenir.
2. **Doğrulama.** Doğrulayan, belgenin içeriğinin özetini kendisi yeniden hesaplar. Sonra imzayı, verenin açık anahtarıyla bir başka matematiksel işlemden geçirir. Bu işlem "bu imza, bu özet için, bu açık anahtarın eşi olan gizli anahtarla mı üretilmiş?" sorusuna evet ya da hayır cevabı verir.



Şekil 7. Dijital imzanın üretilmesi ve doğrulanması

Bu yöntemin iki gücü vardır. Birincisi, belgedeki tek bir harf bile değiştirilirse özet değişir ve imza artık tutmaz; yani belge **değiştirilemez**. İkincisi, imzayı yalnızca gizli anahtarın sahibi üretebilir; açık anahtarı bilmek, imza üretmeye yetmez. Yani belge **taklit edilemez**. Bugün yaygın kullanılan imza algoritmaları (örneğin eliptik eğrilere dayanan ECDSA), bu taklidi en güçlü bilgisayarlar için bile pratikte imkânsız kılacak biçimde tasarlanmıştır. (Kuantum bilgisayarların bu tabloyu nasıl değiştirebileceği dizinin son yazısının konusu.)

Dikkat edilirse bu, Bölüm 5.3'te gördüğümüz kimlik belirtecindeki imzayla aynı mekanizmadır. Fark, imzanın **neyin üzerine** ve **ne kadar süreliğine** atıldığıdır. Federasyonda Google, bir saatlik ömrü olan ve tek bir siteye özel bir belirteci imzalıyordu. Üçgen modelde ise veren kurum, yıllarca geçerli olabilecek ve kişinin istediği yere götürebileceği bir belgeyi imzalar.

6.4 Merkeziyetsiz tanımlayıcılar ve doğrulanabilir belgeler

SSI hareketi bu fikirleri standartlaştırmak için iki temel yapı geliştirdi. Her ikisi de, web'in temel standartlarını belirleyen W3C (*World Wide Web Consortium*) bünyesinde yayımlandı.

Merkeziyetsiz tanımlayıcı (*Decentralized Identifier, DID*) [12], bir kişinin ya da kurumun, herhangi bir merkezî kayıt kurumuna (örneğin bir alan adı kayıt şirketine ya da bir devlet dairesine) bağlı olmadan kendi başına oluşturabildiği bir tanımlayıcıdır. Bir DID şuna benzer:

TEXT Örnek: bir merkeziyetsiz tanımlayıcı (DID)

```
did:example:123456789abcdefghi
```

İlk kısım (`did`) bunun bir DID olduğunu, ikinci kısım (`example`) hangi **yöntemle** çözüleceğini, üçüncü kısım ise o yöntem içindeki benzersiz tanımlayıcıyı gösterir. Bir DID "çözüldüğünde", yani sorgulandığında, ortaya bir **DID belgesi** çıkar. Bu belgenin en önemli içeriği, o tanımlayıcının sahibine ait **açık anahtarlardır**. Yani DID, Bölüm 6.3'teki "açık anahtar nereden geliyor?" sorusuna SSI'ın verdiği cevaptır: Verenin DID'ini çöz, açık anahtarını oradan al, imzayı onunla doğrula. Farklı DID yöntemleri

bu belgeyi farklı yerlerde tutar: bir blokzincirde, bir web sunucusunda ya da yalnızca tanımlayıcının kendisinin içinde.

Doğrulanabilir belge (*Verifiable Credential, VC*) [13] ise üçgen modeldeki belgenin standart biçimidir. İlk sürümü 2019'da, ikinci sürümü 2025'te W3C önerisi olarak yayımlanmıştır. Basitleştirilmiş bir örnek, Aynur'un diplomasının nasıl göründüğü hakkında fikir verebilir:

JSON Örnek: basitleştirilmiş bir W3C doğrulanabilir belge (diploma)

```json
{
  "@context": ["https://www.w3.org/ns/credentials/v2"],
  "type": ["VerifiableCredential", "DiplomaBelgesi"],
  "issuer": "did:example:baku-universitesi",
  "validFrom": "2026-06-30T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:aynur-cuzdan-anahtari",
    "ad": "Aynur …",
    "derece": "Lisans",
    "bolum": "Bilgisayar Mühendisliği",
    "mezuniyetTarihi": "2026-06-30"
  },
  "proof": { "…": "verenin dijital imzası" }
}
```

Bu yapıda `issuer` belgeyi kimin verdiğini, `credentialSubject` belgenin kim hakkında olduğunu ve ne söylediğini, `proof` ise verenin imzasını gösterir. `credentialSubject` içindeki `id` alanı önemlidir: Belgeyi Aynur'un cüzdanındaki bir anahtara **bağlar**. Aynur belgeyi gösterirken bu anahtarla da bir imza atar ve böylece belgenin yalnızca doğru olmadığını, aynı zamanda **onun** olduğunu da kanıtlar. Bölüm 3'te yüz yüzeliğin dijital karşılığı olarak söz ettiğimiz "belgenin kişiye bağlanması" budur.

ÖRNEK

Aynur üçgen modelde

Aynur'un Bakü'deki üniversitesi, mezuniyetinde diplomasını imzalı bir dijital belge olarak Aynur'un cüzdanına gönderir. İstanbul'daki üniversitenin başvuru sayfası bir QR kod gösterir; Aynur telefonuyla okutur, cüzdanı "Bu üniversite diplomanızı görmek istiyor" der, Aynur onaylar. Birkaç saniye içinde İstanbul'daki üniversite belgenin imzasını kontrol eder: belge değiştirilmemiş, Bakü'deki üniversite tarafından imzalanmış ve Aynur'a ait. Bakü'deki üniversite bu işlemden hiç haberdar olmaz. Noter yok, posta yok, haftalar yok.

Ama bir soru açıkta kaldı: İstanbul'daki üniversite, `did:example:baku-universitesi` tanımlayıcısının gerçekten o üniversiteye ait olduğunu ve o üniversitenin gerçekten diploma vermeye yetkili bir yükseköğretim kurumu olduğunu nereden biliyor?

6.5 Vaatler ve sahada yaşananlar

SSI fikri 2016'dan sonra büyük bir heyecan yarattı. Yüzlerce girişim kuruldu, birçok hükümet ve uluslararası kuruluş pilot projeler başlattı, blokzincir tabanlı kimlik ağları kuruldu. Ancak aradan geçen yıllarda, bu projelerin çok azı pilot aşamasını geçip milyonlarca insanın gündelik hayatına girebildi. Bunun nedenlerini anlamak, dördüncü dönemi anlamak için zorunludur.

Birinci neden: güven sorusu çözülmemişti. Aynur örneğinin sonunda açıkta kalan soru, SSI'ın en zayıf noktasıydı. Teknoloji, bir belgenin belirli bir DID tarafından imzalandığını kusursuzca kanıtlıyordu. Ama o DID'in arkasında kimin durduğunu ve o kimsenin gerçekten yetkili olup olmadığını kanıtlamıyordu. Herkes kendi DID'ini oluşturabildiğine göre, herkes kendine "Bakü Devlet Üniversitesi" adını verebilirdi. Bu sorunun çözümü için "güven çerçeveleri" (*trust frameworks*) ve "yönetişim kuralları" geliştirildi; ama her projenin kendi çerçevesi vardı ve bu çerçeveler birbirini tanımıyordu. Yani teknolojik olarak merkeziyetsiz olan sistem, güven açısından yeni adalara bölündü.

İkinci neden: blokzincir ve kişisel veri. İlk SSI sistemlerinin birçoğu tanımlayıcıları, anahtarları ve bazen belgelerin iptal bilgilerini bir blokzincire yazıyordu. Blokzincirin değişmezliği, burada bir avantaj

değil, bir sorun hâline geldi: Avrupa'nın Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'nin Kişisel Verilerin Korunması Kanunu (KVKK), kişiye verisinin silinmesini isteme hakkı tanır. Değişmez bir deftere yazılmış kişisel veri ise silinemez. Kişiye ait tanımlayıcılar bile, bir kez zincire yazıldığında, o kişinin farklı işlemlerini birbirine bağlamak için kullanılabilir. Bu yüzden zamanla, kişiye ait hiçbir şeyin zincire yazılmaması gerektiği konusunda geniş bir uzlaşma oluştu; ama bu uzlaşma, zincirin kimlik sistemindeki rolünü de tartışmaya açtı. (Bu konuya dizinin on ikinci yazısında ayrıntılı döneceğiz.)

Üçüncü neden: anahtar kaybı. Kimliği kişinin kendi elinde tutmanın kaçınılmaz bir sonucu vardır: Kişi anahtarını kaybederse, kimliğini de kaybeder. Federasyonda parolanızı unuttuğunuzda "şifremi unuttum" bağlantısına tıklarsınız; kimlik sağlayıcı sizi başka yollarla tanır ve hesabınızı geri verir. Saf bir SSI modelinde ise böyle bir merci yoktur. Telefonu kaybolan, çalınan ya da bozulan biri, içindeki bütün belgeleri kaybedebilir. Bunun için sosyal kurtarma, yedekleme gibi çözümler önerildi; ama her biri ya kullanıcı deneyimini zorlaştırıyor ya da sistemi yeniden bir tür merkeze bağımlı hâle getiriyordu.

Dördüncü neden: tavuk ve yumurta. Bir cüzdanın değeri, içine belge verecek kurumların ve o belgeleri kabul edecek doğrulayanların sayısına bağlıdır. Kurumlar, kimse cüzdan kullanmadığı için belge vermek istemedi; kullanıcılar, cüzdanda işe yarar bir belge olmadığı için cüzdan indirmedi; doğrulayanlar ise ikisinin de olmadığı bir sisteme yatırım yapmadı. Federasyon tarihinden çıkardığımız ders burada da geçerliydi: Benimseme, teknolojinin zarafetinden değil, **kullanıcının zaten bulunduğu yerden** gelir.

Beşinci neden: hukuki karşılığın yokluğu. Bir dijital diplomanın imzası matematiksel olarak doğru olabilir. Ama bir işverenin, bir bankanın ya da bir devlet dairesinin bu belgeye dayanarak karar vermesi için, o belgenin **hukuken** de geçerli olması gerekir. SSI projelerinin büyük çoğunluğu bu hukuki çerçeveden yoksundu.

> ÖNEMLİ
>
> **Bu bölümden akılda kalması gereken**
>
> Kendi kendine egemen kimlik hareketi, dijital kimliğe kalıcı iki şey kazandırdı: **üçgen model** (verenin, belgenin nerede gösterildiğini bilmemesi) ve **kişinin elindeki cüzdan** fikri. Ama "kime güveneceğiz?" sorusunu, anahtar kaybını ve hukuki geçerliliği çözemedi. Teknoloji hazırdı; eksik olan, ölçek, yönetişim ve hukuktu.

7 Dördüncü Dönem: Devlet Destekli Kimlik Cüzdanları

7.1 Neden devletler?

SSI'ın çözemediği üç sorun (güvenin kaynağı, anahtar kaybı ve hukuki geçerlilik), aslında devletlerin yüzyıllardır çözmekte olduğu sorunlardır. Kimin üniversite olduğunu, kimin diploma vermeye yetkili olduğunu belirleyen devlettir. Kimliğini kaybeden vatandaşa yenisini veren devlettir. Bir belgenin hukuki geçerliliğini tanımlayan da devlettir. Üstelik devletler, bir sistemi milyonlarca kişiye ulaştırabilecek tek aktörlerdendir.

Ancak devletlerin dijital kimlik alanına girişi yeni değildi. Bölüm 5.4'te gördüğümüz gibi, birçok ülke ulusal kimlik sağlayıcıları kurmuştu. Asıl yenilik, devletlerin bu sefer **federasyon modeli yerine üçgen modeli** benimsemesi oldu. Bu dönüşümün en kapsamlı ve en iyi belgelenmiş örneği Avrupa Birliği'dir.

7.2 eIDAS: Avrupa'nın ilk adımı

Avrupa Birliği'nin dijital kimlik alanındaki ilk büyük düzenlemesi, 2014'te kabul edilen **eIDAS Tüzüğü**dür (Tüzük (AB) No 910/2014) [14]. Adı, *electronic IDentification, Authentication and trust Services*, yani elektronik kimlik, kimlik doğrulama ve güven hizmetleri ifadesinden gelir. Tüzük iki ana konuyu düzenledi.

Birincisi **elektronik kimlik**: Bir üye devlet, kendi vatandaşlarına verdiği elektronik kimlik sistemini AB'ye bildirirse, diğer üye devletlerin kamu hizmetleri bu kimliği tanımak zorunda kalıyordu. Bu zorunluluk 29 Eylül 2018'de başladı. Örneğin bir Alman vatandaşı, kendi ülkesinin elektronik kimliğiyle bir İtalyan kamu hizmetine giriş yapabilecekti. Bunu sağlamak için her ülke bir "eIDAS düğümü" kurdu; düğümler birbirine bağlanarak ülkeler arası bir federasyon oluşturdu.

İkincisi **güven hizmetleri**: elektronik imzalar, elektronik mühürler, zaman damgaları, web sitesi sertifikaları ve bunları sunan kuruluşların denetimi. eIDAS, belirli koşulları sağlayan **nitelikli elektronik imzanın** el yazısıyla atılan imzayla hukuken eşdeğer olduğunu bütün AB'de geçerli kıldı. Ayrıca her üye devletin, kendi ülkesindeki denetlenmiş güven hizmeti sağlayıcılarını imzalı bir **güven listesinde** (*trusted list*) yayımlamasını ve AB'nin bütün bu listelerin listesini tutmasını şart koştu. Bu "listelerin listesi" mimarisi, Bölüm 6.5'te SSI'ın çözemediğini söylediğimiz "kime güveneceğiz?" sorusuna Avrupa'nın verdiği cevabın temelidir ve dördüncü dönemin bütün yapısını taşır (dizinin altıncı yazısı).

eIDAS'ın elektronik kimlik ayağı ise beklenen etkiyi yaratmadı. Bildirilen sistemler yalnızca kamu hizmetleri için zorunluydu; özel sektör bunları pek kullanmadı. Sistem tamamen federasyon mantığıyla kuruluydu ve Bölüm 5.5'teki bütün sınırlamaları taşıyordu: Kişi bir belge taşımıyor, her seferinde kendi ülkesinin kimlik sağlayıcısına yönlendiriliyordu. Yalnızca temel kimlik bilgileri (ad, soyad, doğum tarihi, kişisel tanımlayıcı) taşınabiliyordu; diploma, ehliyet, meslek belgesi gibi bilgiler kapsam dışındaydı. Ve birçok AB vatandaşı bu sistemin varlığından haberdar bile değildi.

7.3 eIDAS 2.0 ve Avrupa Dijital Kimlik Cüzdanı

eIDAS'ın sınırları ve SSI hareketinin fikirleri, 2021'de Avrupa Komisyonu'nun yeni bir öneri sunmasına yol açtı. Uzun müzakerelerin ardından **Tüzük (AB) 2024/1183**, yaygın adıyla **eIDAS 2.0**, 11 Nisan 2024'te kabul edildi ve 20 Mayıs 2024'te yürürlüğe girdi [15]. Tüzük, eski eIDAS'ı yürürlükten kaldırmadı; onu değiştirerek genişletti. Ama getirdiği değişikliğin özü, Avrupa'nın dijital kimlik modelini **federasyondan üçgen modele** taşımasıydı.

Tüzüğün merkezinde **Avrupa Dijital Kimlik Cüzdanı** (*European Digital Identity Wallet*, kısaca EUDI cüzdanı) vardır. Tüzüğe göre her üye devlet, vatandaşlarına ve yerleşiklerine en az bir cüzdan sunmak zorundadır; bu cüzdan, uygulama düzenlemelerinin yürürlüğe girmesinden itibaren yirmi dört ay içinde, yani 24 Aralık 2026'ya kadar, kullanıma hazır olmalıdır. Cüzdanı devlet kendisi geliştirebilir ya da devletin yetkilendirdiği ya da tanıdığı bir kuruluş sağlayabilir.

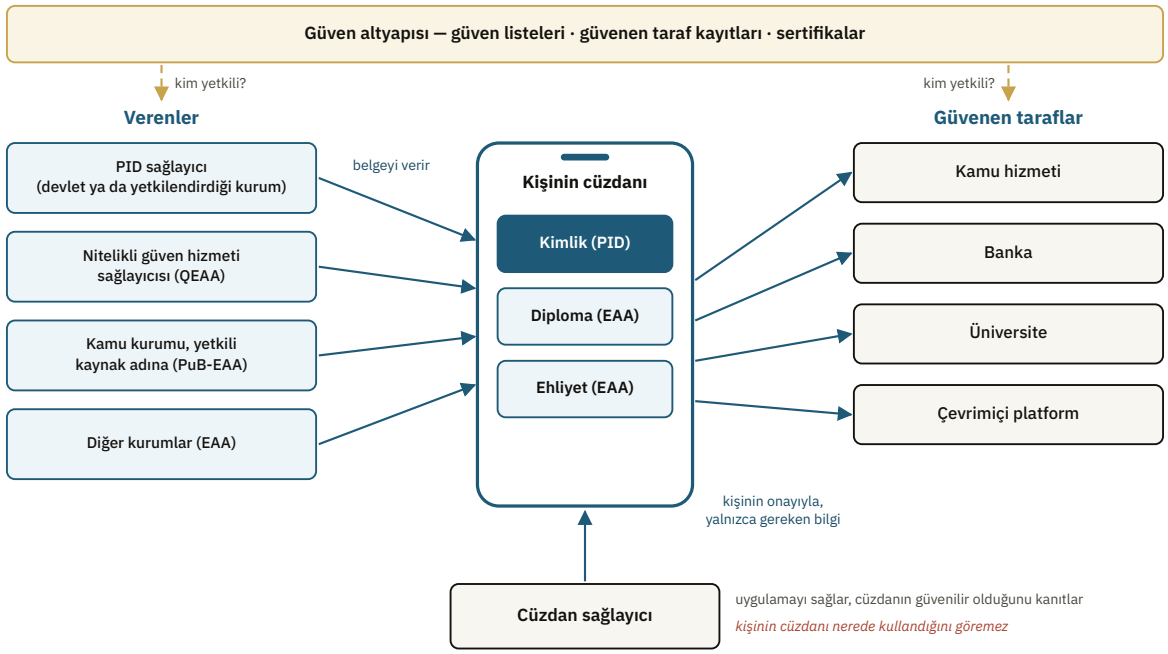
Tüzüğün getirdiği temel ilkeleri şöyle özetleyebiliriz:

- **Gönüllülük ve ücretsizlik.** Cüzdan kullanmak zorunlu değildir; kullanmayan kişi hiçbir hizmetten dışlanamaz. Cüzdan, gerçek kişiler için ücretsizdir.
- **Kişinin kontrolü.** Hangi bilginin kime gösterileceğine kişi karar verir. Cüzdan, kişinin bilgisini kimlerle paylaştığını gösteren bir panel (*dashboard*) sunar ve kişinin bir doğrulayanın verisini silmesini istemesini, kötüye kullanımı veri koruma otoritesine bildirmesini kolaylaştırır.
- **Seçici açıklama.** Kişi bir belgenin tamamını değil, yalnızca gereken kısmını gösterebilir; örneğin bütün kimlik kartını değil, yalnızca "18 yaşından büyüktür" bilgisini.
- **İzlenmeme.** Cüzdan sağlayıcısı, kişinin cüzdanını nerede ve nasıl kullandığı hakkında bilgi toplayamaz. Veren kurum da belgenin nerede gösterildiğini öğrenmez. Yani üçgen modelin mahremiyet vaadi hukuki bir yükümlülüğe dönüşür.
- **Kayıtlı doğrulayanlar.** Cüzdandan bilgi istemek isteyen kurumlar (güvenen taraflar) önce kendi ülkelerinde kayıt olmak ve hangi bilgileri, hangi amaçla isteyeceklerini bildirmek zorundadır. Cüzdan, bir kurumun kayıtlı olduğundan fazlasını istemesi durumunda kişiyi uyarabilir.
- **Zorunlu kabul.** Kamu hizmetlerinin yanı sıra, belirli bir geçiş süresinin ardından, yasal olarak güçlü kimlik doğrulama yapması gereken özel sektör kuruluşları (örneğin bankalar) ve çok büyük çevrimiçi platformlar da kullanıcı isterse cüzdanı kabul etmek zorundadır. Bu, SSI döneminin "tavuk ve yumurta" sorununa hukuki bir cevaptır.

- **Sertifikasyon ve açık kaynak.** Cüzdanlar bağımsız kuruluşlarca sertifikalandırılır; cüzdan uygulamasının kaynak kodu, belirli güvenlik istisnaları dışında açık kaynak lisansıyla yayımlanır.

7.4 Cüzdan ekosistemi: kim kimdir?

eIDAS 2.0, Bölüm 2.5'teki üç rolü korur ama her birini hukuki olarak tanımlanmış aktörlere dönüştürür ve bunlara birkaç yeni rol ekler (Şekil 8).



Şekil 8. Avrupa Dijital Kimlik Cüzdanı ekosistemi (sadeleştirilmiş)

Kişi kimlik verisi (*Person Identification Data*, **PID**), cüzdanın temelini oluşturan kimlik bilgisidir: ad, soyad, doğum tarihi, uyruk gibi. PID'i yalnızca devlet ya da devletin yetkilendirdiği bir kuruluş verebilir. Cüzdan kurulduğunda ilk yüklenen belge budur ve diğer belgelerin kişiye ait olduğunu kanıtlamanın dayanağı olur. Bu, SSI'ın çözemediği **hukuki geçerlilik** sorununu çözer: PID, bir devletin imzasını taşıyan ve AB genelinde tanınan bir kimlik bilgisidir.

Öznitelik onayları (*Electronic Attestations of Attributes*, **EAA**), PID dışındaki bütün belgelerdir: diplomalar, ehliyetler, meslek belgeleri, üyelik kartları, sağlık bilgileri. Tüzük bunları güvence düzeyine göre üç türe ayırır: nitelikli güven hizmeti sağlayıcılarının verdiği **nitelikli** onaylar (QEAA), yetkili bir kamu kaynağı adına bir kamu kurumunun verdiği onaylar (PuB-EAA) ve diğer kurumların verdiği onaylar (EAA). Nitelikli bir onay, tıpkı nitelikli elektronik imza gibi, bütün AB'de kâğıt üzerindeki karşılığıyla aynı hukuki etkiye sahiptir.

Güvenen taraflar (*relying parties*), cüzdandan bilgi isteyen bankalar, üniversiteler, kamu hizmetleri ve platformlardır. Kayıt olur, bir sertifika alırlar ve cüzdana her başvuruda bu sertifikayı gösterirler; böylece cüzdan da onların kim olduğunu doğrulayabilir. Yani doğrulama **iki yönlüdür**: Doğrulayan belgeyi doğrularken, cüzdan da doğrulayanı doğrular.

Cüzdan sağlayıcı, cüzdan uygulamasını geliştiren ve işleten kuruluştur. Cüzdanın, belge veren kurumlara "ben sertifikalı, güvenilir bir cüzdanım ve anahtarlarım güvenli donanımda saklanıyor" diyebilmesini sağlayan bir kanıt üretir. Bu kanıt SSI'daki anahtar kaybı sorununa da bir çerçeve getirir: Telefon kaybolduğunda kişi yeni bir cüzdan kurar, PID'ini yeniden alır ve belgelerini yeniden yükler; kayıp telefondaki cüzdan ise uzaktan geçersiz kılınabilir.

Ve hepsinin üstünde **güven altyapısı** durur: Hangi kurumun PID verebileceğini, hangi kurumun nitelikli onay verebileceğini, hangi cüzdanların sertifikalı olduğunu ve hangi güvenen tarafların kayıtlı olduğunu söyleyen imzalı listeler. Bölüm 6.5'te SSI'ın "kime güveneceğiz?" sorusunu çözemediğini söylemiştik. eIDAS 2.0'ın cevabı, 2014'ten beri işleyen güven listesi mimarisini bu yeni rollere genişletmektir. Doğrulayan, verenin açık anahtarını bir blokzincirden ya da bir DID'den değil, bir devletin imzaladığı ve AB'nin listeler listesinde yer alan bir güven listesinden öğrenir.

7.5 Teknik mimari ve standartlar

Tüzük ilkeleri ve rolleri belirler; ama bir Fransız cüzdanının bir Alman bankasıyla, bir İspanyol üniversitesinin bir Polonyalı öğrencinin cüzdanıyla konuşabilmesi için ortak teknik kurallar gerekir. Bu kurallar, Avrupa Komisyonu'nun çağrısıyla üye devletlerin uzmanlarınca hazırlanan **Mimari ve Başvuru Çerçevesi** (*Architecture and Reference Framework*, **ARF**) [16] ve 2024'ün sonundan itibaren yayımlanan bir dizi **uygulama tüzüğü** ile belirlenir. ARF, herkese açık olarak geliştirilen ve düzenli olarak güncellenen yaşayan bir belgedir.

ARF, tek bir teknolojiye bağlanmak yerine, olgunlaşmış uluslararası standartlardan oluşan bir set seçmiştir. Bunların ayrıntıları dizinin ilerleyen yazılarının konusudur; burada yalnızca genel bir harita vermekle yetiniyoruz:

Tablo 3. EUDI cüzdanının dayandığı başlıca standartlar.

Katman	Standart	Ne işe yarar	Dizide ayrıntısı
Belge biçimi	**SD-JWT VC** (IETF) — seçici açıklamalı JSON Web Token [17]	Bölüm 5.3'teki JWT'nin, alanların tek tek gizlenebildiği bir türü	2. ve 3. yazı
Belge biçimi	**mdoc** — ISO/IEC 18013-5 [18]	Mobil ehliyet için geliştirilmiş, yüz yüze kullanıma uygun, ikili (CBOR) biçim	2. ve 9. yazı
Belge verme	**OpenID4VCI** (OpenID Vakfı)	Bir kurumun cüzdana belge vermesi için protokol	8. yazı
Belge gösterme	**OpenID4VP** (OpenID Vakfı)	Bir doğrulayanın cüzdandan belge istemesi için protokol	8. yazı
Yüz yüze gösterme	**ISO/IEC 18013-5**	QR, NFC ve Bluetooth ile internetsiz gösterim	9. yazı
İptal	**Token Status List** (IETF)	Belgenin iptal edilip edilmediğini, verene sormadan öğrenmek	7. yazı
Güven	**ETSI güven listeleri** (TS 119 612, TS 119 602)	Hangi kurumun hangi rolde yetkili olduğunu söyleyen imzalı listeler	6. yazı

Bu tablonun dikkat çekici yanı, SSI'ın iki temel yapısıyla (DID ve W3C VC) ilişkisidir. ARF, belge biçimi olarak ağırlıklı olarak SD-JWT VC ve mdoc'u benimsemiş, güven kaynağı olarak da DID yerine güven listelerini seçmiştir. Bunun gerekçesi, bu standartların olgunluğu, seçici açıklamayı doğal olarak desteklemeleri ve mevcut kamu anahtarı altyapısıyla uyumlarıdır. Yine de W3C VC modeli, özellikle eğitim alanında, AB'nin büyük ölçekli pilot projelerinde kullanılmaya ve tartışılmaya devam etmektedir. Yani dördüncü dönem, üçüncü dönemin **fikirlerini** benimsemiş, ama **araçlarının** bir kısmını başka araçlarla değiştirmiştir.

AB, bu mimariyi sahada denemek için 2023'te dört **büyük ölçekli pilot** projeyi başlattı. Yüzlerce kamu kurumu, şirket ve üniversitenin katıldığı bu pilotlar; mobil ehliyet, banka hesabı açma, diploma doğrulama, seyahat, sağlık reçetesi ve sosyal güvenlik belgeleri gibi senaryoları gerçek ortamlarda sınadı. Bu dizide yer yer bu pilotlardan çıkan derslere değineceğiz.

ÖRNEK

Aynur dördüncü dönemde

Bu dönemin sistemi tam kurulduğunda Aynur'un deneyimi şöyle olabilir: Aynur, devletinin tanıdığı bir cüzdanı telefonuna kurar ve kimlik bilgisini (PID) çipli kimlik kartını telefona okutarak ya da bir devlet hizmeti aracılığıyla alır. Mezun olduğunda üniversitesi diplomasını cüzdanına gönderir. İstanbul'daki üniversite, Aynur'dan diplomasını ve yalnızca adını, doğum tarihini ve uyruğunu ister; Aynur'un cüzdanı, isteği gönderen üniversitenin kayıtlı bir kurum olduğunu ve bu bilgileri istemeye yetkili olduğunu kontrol eder ve Aynur'a gösterir. Aynur onaylar. İstanbul'daki üniversite, diplomanın imzasını Azerbaycan'ın güven listesinde yer alan Bakü'deki üniversitenin anahtarıyla doğrular. Bakü'deki üniversite işlemden habersiz kalır. Bütün süreç bir dakikadan kısa sürer.

Bu senaryonun önünde, Avrupa Birliği dışındaki ülkeler için, hâlâ çözülmesi gereken önemli bir soru var: Azerbaycan ya da Türkiye'nin güven listesi AB'nin listeler listesinde değil. Bu soruya Bölüm 10'da döneceğiz.

7.6 Avrupa dışında

Dördüncü dönem yalnızca Avrupa'ya ait değil. Mobil ehliyet standardı ISO/IEC 18013-5, Amerika Birleşik Devletleri'nde birçok eyalette telefon cüzdanlarında kullanılmaya başlandı. Dünyanın birçok ülkesi de kendi dijital kimlik cüzdanlarını geliştiriyor ya da mevcut ulusal kimlik sistemlerine cüzdan katmanı ekliyor. Bu ülkelerin bir kısmı kendi yollarını izlerken, giderek artan bir kısmı AB'nin mimarisini ve standartlarını referans alıyor; çünkü bu mimari açık, belgelenmiş ve uluslararası standartlara dayanıyor. Bu, AB dışındaki ülkeler için de önemli bir fırsat yaratıyor: Aynı standartları kullanan sistemler, ileride birbirini tanıyabilecek sistemlerdir.

8 Kimlik Güvencesi Düzeyleri: Ne Kadar Emin Olmalıyız?

Dört dönemi karşılaştırmadan önce, dijital kimlik sistemlerini değerlendirmek için kullanılan önemli bir kavramı tanıtmamız gerekiyor. Her işlem aynı düzeyde güven gerektirmez. Bir haber sitesine yorum yazmak için bir e-posta adresi yeterlidir; bir banka hesabı açmak için kimliğin resmî belgelerle doğrulanmış olması gerekir; tapu devri için ise çok daha fazlası.

Bu farkı sistematik biçimde ifade etmek için **kimlik güvencesi düzeyleri** (*levels of assurance*, LoA) kullanılır. eIDAS, elektronik kimlik sistemleri için üç düzey tanımlar [14, 19]:

Tablo 4. eIDAS'ta kimlik güvencesi düzeyleri.

Düzey	Amacı	Kimlik nasıl doğrulanmış olmalı	Örnek kullanım
Düşük (*low*)	Kimlik iddiasına sınırlı güven	kişinin beyanı ya da basit bir doğrulama	bir hizmete üyelik, düşük riskli işlemler
Önemli (*substantial*)	Kimlik iddiasına önemli düzeyde güven	resmî bir belgeyle doğrulama; en az iki faktörlü giriş	çoğu kamu hizmeti, birçok bankacılık işlemi
Yüksek (*high*)	Kimlik iddiasına en yüksek güven; sahteciliği önlemeye yönelik	yüz yüze ya da eşdeğer güvenlikte doğrulama; kopyalanamaz donanımla korunan anahtarlar	nitelikli imza, PID, yüksek riskli kamu işlemleri

Bu düzeyler iki farklı şeyi birlikte ölçer: **Kişinin kimliği ilk başta ne kadar sağlam doğrulandı?** (örneğin yüz yüze mi, yalnızca beyanla mı) ve **kişi her girişte ne kadar sağlam tanınıyor?** (örneğin yalnızca parolayla mı, güvenli donanımda saklanan bir anahtarla mı). Amerika Birleşik Devletleri'nde NIST'in dijital kimlik kılavuzu SP 800-63 [20] bu iki boyutu ayrı ayrı ölçer: kimlik kanıtlama düzeyi (IAL), kimlik doğrulama düzeyi (AAL) ve federasyon düzeyi (FAL).

Güvence düzeyleri, dört dönemi karşılaştırmak için de kullanışlı bir mercektir. Ada modeli genellikle düşük düzeyde kalır; çünkü kimse kimseyi doğrulamaz. Sosyal federasyon da çoğunlukla düşük

düzeydedir. Devlet kimlik sağlayıcıları önemli ya da yüksek düzeye ulaşabilir, ama genellikle yalnızca kendi ülkelerinde. Saf SSI sistemleri, belgenin içeriği kadar güvenilirdir; ama "belgeyi veren kim?" sorusu çözülmediği için güvence düzeyi tanımlanamaz. EUDI cüzdanının PID'i ise tüzük gereği **yüksek** düzeyde olmak zorundadır; bu, dördüncü dönemin en belirgin farklarından biridir.

9 Dört Modelin Karşılaştırması

Artık dört dönemi yan yana koyabiliriz. Tablo 5, yazının başında sorduğumuz üç soruyu ve birkaç ek ölçütü bir araya getiriyor.

Tablo 5. Dört dijital kimlik modelinin karşılaştırması.

Ölçüt	Ada (silo)	Federasyon	Kendi kendine egemen kimlik	Devlet destekli cüzdan (EUDI)
Kimliği kim veriyor?	her hizmet kendisi (çoğu zaman kişinin beyanı)	kimlik sağlayıcı	herhangi bir veren	yetkilendirilmiş, listelenmiş verenler
Kimliği kim saklıyor?	her hizmet ayrı ayrı	kimlik sağlayıcı	kişi, cüzdanında	kişi, cüzdanında
Doğrulamada veren haberdar olur mu?	— (veren yok)	**evet**, her girişte	hayır	hayır (hukuki yükümlülük)
Belge bir nesne mi, hizmet mi?	hesap	hizmet	nesne	nesne
Güvenin kaynağı	yok	kimlik sağlayıcının itibarı	DID / blokzincir / güven çerçevesi	devletlerin imzaladığı güven listeleri
Seçici açıklama	yok	sınırlı (izin ekranında kapsam)	var	var (zorunlu)
Hukuki geçerlilik	yok	sınırlı	çoğunlukla yok	var (nitelikli onaylar ve PID)
Anahtar ya da hesap kaybı	parola sıfırlama	sağlayıcı kurtarır	çözülmemiş	PID'i yeniden alıp belgeleri yeniden yükleme
Güvence düzeyi	düşük	düşük – yüksek	belirsiz	yüksek (PID)
Ölçek ve benimseme	evrensel	çok yüksek	düşük	hukuken zorunlu kabul ile yükseliyor
Başlıca risk	sızıntılar, parola tekrarı	izlenme, bağımlılık	güven belirsizliği, anahtar kaybı	aşırı kimlik isteme, platform bağımlılığı (Bölüm 10)

Tabloyu okurken dikkat edilmesi gereken birkaç nokta var.

Birincisi, dönemler arasındaki geçiş **doğrusal bir ilerleme** değildir. Her model bir şeyi kazanırken başka bir şeyi kaybetmiştir. Federasyon kolaylık kazandırdı ama mahremiyet kaybettirdi. SSI mahremiyeti ve kişinin kontrolünü geri getirdi ama güven ve hukuki geçerlilikte zayıf kaldı. Devlet destekli cüzdanlar bu dengeyi kurmaya çalışıyor; ama Bölüm 10'da göreceğimiz gibi, bu da kendi risklerini taşıyor.

İkincisi, modeller birbirinin yerini almaz, **birbirini tamamlar**. EUDI cüzdanının yaygınlaştığı bir dünyada da bir habere yorum yazmak için kullanıcı adı ve parola (ya da geçiş anahtarı) kullanmaya devam edeceğiz; çünkü orada yüksek güvenceye ihtiyaç yoktur ve kimliğimizi göstermek istemeyiz. Şirket içi sistemlere hâlâ federasyonla gireceğiz. Hatta cüzdanın kendisi bir kimlik sağlayıcıyla birlikte de kullanılabilir: Bir site, cüzdandaki PID ile kişiyi bir kez doğrulayıp ona kendi hesabını açabilir. Doğru soru "hangi model en iyi?" değil, **"bu iş için hangi model yeterli ve hangisi gereğinden fazla?"** sorusudur.

Üçüncüsü, tablodaki "doğrulamada veren haberdar olur mu?" satırı, dijital kimliğin mahremiyet tarihinin özeti gibidir. Ada modelinde verenin olmaması bir eksiklikti; federasyonda verenin her şeyi görmesi bir tehlike; üçgen modelde verenin hiçbir şey görmemesi ise bir tasarım hedefi. Dördüncü dönemde bu hedef, bir teknoloji tercihi olmaktan çıkıp **hukuki bir yükümlülüğe** dönüşmüştür.

10 Sınırlar ve Açık Sorular

Dördüncü dönem, dijital kimlik tarihinin en kapsamlı girişimi. Ama hiçbir teknoloji ya da düzenleme bütün sorunları çözmez; bazı sorunları ise yenilerini doğurarak çözer. Bu bölümde, bu yazı dizisi boyunca tekrar tekrar döneceğimiz açık soruları sıralıyoruz.

Aşırı kimlik isteme. Kimlik göstermek zahmetli olduğu sürece, kurumlar ondan gerçekten gerekmedikçe kaçınır. Ama cüzdandan kimlik bilgisi istemek tek bir dokunuşa indiğinde, gerekmediği hâlde kimlik isteme eğilimi artabilir. Daha önce anonim kullanılan hizmetler, "nasılsa kolay" diye kimlik istemeye başlayabilir. Tüzük, güvenen tarafların kayıt olmasını ve isteyebilecekleri bilgileri önceden bildirmesini şart koşarak bu riski sınırlamaya çalışıyor. Ama bir kurumun bir bilgiyi **isteme hakkının** olup olmadığına kimin, nasıl karar vereceği, uygulamada en zor sorulardan biri olmaya devam edecek.

Bağlanabilirlik. Üçgen model, verenin belgenin nerede gösterildiğini öğrenmesini engeller. Ama aynı belgeyi gören iki farklı doğrulayan, bir araya gelip notlarını karşılaştırırsa, aynı imzayı ya da aynı anahtarı tanıyarak aynı kişiyle iş yaptıklarını anlayabilir. Bu soruna karşı tek kullanımlık belge kopyaları, siteye özel takma adlar ve sıfır bilgi ispatları gibi çözümler var; ama her birinin bir bedeli var. Dizinin dördüncü ve beşinci yazıları bu konuya ayrılmış durumda.

Dijital uçurum. Cüzdan, akıllı telefonu olan, onu kullanabilen ve güvenli bir telefona erişimi olan insanlar için tasarlanmıştır. Yaşlılar, engelliler, yoksullar ve dijital okuryazarlığı düşük olanlar için cüzdan bir kolaylık değil bir engel olabilir. Tüzüğün gönüllülük ve ayrımcılık yasağı ilkeleri bu riski kabul ediyor; ama bir hizmetin cüzdan kullanmayana gerçekten eşit kalitede sunulup sunulmadığı, uygulamada izlenmesi gereken bir soru.

Platform bağımlılığı. Cüzdanlar akıllı telefonlarda çalışır ve dünyadaki akıllı telefonların neredeyse tamamı iki şirketin işletim sistemini kullanır. Cüzdanın güvenliği büyük ölçüde bu işletim sistemlerinin güvenli donanımına ve cihaz doğrulama hizmetlerine dayanır. Federasyon döneminde kimliğin büyük şirketlere teslim edilmesinden kaçınmak için kurulan bir sistemin, başka bir katmanda yine aynı şirketlere bağımlı hâle gelmesi, üzerinde düşünülmesi gereken bir paradokstur.

Devlet gücü. Devlet destekli bir cüzdan, devletin kimliği tanımlama gücünü dijital dünyaya taşır. Hukuk devletinin güçlü olduğu yerlerde bu bir güvencedir; zayıf olduğu yerlerde ise bir gözetim aracına dönüşme riski taşır. Tüzüğün, cüzdan sağlayıcının kişinin işlemlerini görememesi ve açık kaynak zorunluluğu gibi ilkeleri bu riske karşı önemli teknik güvencelerdir. Ama teknik güvencelerin ancak onları koruyan bir hukuk düzeni içinde anlamlı olduğu unutulmamalıdır.

Sınır ötesi tanıma ve AB dışındaki ülkeler. eIDAS 2.0, AB içinde 27 ülkenin cüzdanlarının birbirini tanımasını sağlıyor. Peki ya AB dışındaki ülkeler? Tüzük, üçüncü ülkelerin güven hizmetlerinin ve kimlik sistemlerinin belirli koşullar altında tanınabilmesi için yollar öngörüyor; ama bu yollar uzun, karmaşık ve siyasi müzakereler gerektiren süreçler. Aynur'un örneğindeki gibi Azerbaycan'dan Türkiye'ye, Kazakistan'dan Özbekistan'a uzanan bir öğrenci, işçi ya da girişimci hareketliliği için ortak bir güven altyapısı henüz yok. Türk dünyası ülkelerinin her birinin kendi güçlü e-devlet ve kimlik sistemleri var; ama bu sistemlerin birbirini tanıması ve AB ile uyumlu biçimde konuşabilmesi, ayrı bir çabayı gerektiriyor. Dizinin on üçüncü yazısı bu konuya ayrılacak.

Hızla değişen standartlar. Tablo 3'teki standartların bir kısmı hâlâ geliştirilme aşamasında. Bir cüzdanın ya da bir doğrulama sisteminin bugün yaptığı tasarım tercihleri, birkaç yıl içinde yenilenen

standartlar karşısında güncellenmek zorunda kalabilir. Bu, erken benimseyenler için hem bir maliyet hem de standartların gelişimine katkıda bulunma fırsatıdır.

11 Bu Tablonun İçinde Tamga Network

Bu yazı dizisi, Tamga Network tarafından yayımlanıyor. Okurun, yazarların hangi bakış açısından yazdığını bilmesi için bu konumu kısaca açıklamak doğru olur.

Tamga Network, Türkiye ve Türk dünyası için kâr amacı gütmeyen bir dijital güven ağı olarak tasarlanmıştır. Bu yazıda anlatılan dördüncü dönemin modelini, yani Avrupa Birliği'nin eIDAS 2.0 ve EUDI mimarisini, Avrupa Birliği üyesi olmayan ülkeler için uygulanabilir kılmayı hedefler. Ağ, Bölüm 7.4'te anlatılan rollerden belge veren kurumların ve cüzdanların kimler olduğunu söyleyen **imzalı güven listelerini** yayımlar ve bu ekosistemin kurallarını açık bir çerçeve belgesi olarak tanımlar. Kurumlar kişinin cüzdanına belge verir; kişi yalnızca istenen alanları paylaşır; doğrulayan da belgeyi, veren kuruma sormadan saniyeler içinde doğrular. Güven listelerinde hiçbir kişisel veri yer almaz. Ağ kendisi bir cüzdan işletmez; cüzdanları, belge veren kurumları ve doğrulayanları listeler.

Yani Tamga Network, bu yazının Bölüm 10'da açık bıraktığı son sorulardan biri olan **AB dışındaki ülkeler arasında ortak bir güven altyapısı** sorusuna, AB'nin kendi standartlarıyla uyumlu bir cevap üretmeye çalışan bir girişimdir. Adını da, yazının başında anlattığımız, bir toplulukta herkesin tanıdığı ve tanımadığın biri hakkında güvenilir bilgi veren işaretten alır.

12 Sonuç

Altmış yılı aşkın bir sürede dijital kimlik, bir zaman paylaşım bilgisayarındaki parola dosyasından, devletlerin imzasını taşıyan ve kişinin cebinde duran cüzdanlara uzanan uzun bir yol yürüdü. Bu yolun her durağı, bir öncekinin sorununu çözmeye çalıştı.

Ada döneminde her sistem kendi adasında yaşadı; kullanıcılar onlarca parolanın yükünü taşıdı ve kimse kimseyi gerçekten doğrulayamadı. Federasyon bu yükü büyük kimlik sağlayıcılarına devretti; ama karşılığında, kişinin dijital hayatının her kapısında bekleyen bir kapıcı yarattı. Kendi kendine egemen kimlik hareketi, belgeyi kişinin eline geri verdi ve verenin, belgenin nerede gösterildiğini öğrenmediği üçgen modeli kurdu; ama "kime güveneceğiz?" sorusunu cevapsız bıraktı. Dördüncü dönemde devletler, üçgen modeli kendi güven listeleri ve hukuki güvenceleriyle birleştirerek bu soruya bir cevap verdi.

Bu hikâyeden çıkarılabilecek belki en önemli ders şudur: Dijital kimlik, temelde bir teknoloji sorunu değil, bir **güven** sorunudur. Teknoloji, bir belgenin değiştirilmediğini ve kimin imzaladığını kusursuzca kanıtlayabilir. Ama o imzayı atanın kim olduğuna, o kişinin o belgeyi vermeye yetkili olup olmadığına ve belgeyi gören kurumun o bilgiyi istemeye hakkı olup olmadığına teknoloji tek başına karar veremez. Bu kararlar, bir toplumun ortak kurallarına, kurumlarına ve hukukuna dayanır. Bozkırdaki tamganın gücü de çizginin kendisinden değil, o çizgiyi herkesin tanımasından geliyordu.

Bu yazı dizisinin sonraki bölümlerinde, burada genel hatlarıyla tanıttığımız kavramların her birine yakından bakacağız: doğrulanabilir belgelerin iç yapısına, seçici açıklamanın matematiğine, sıfır bilgi ispatlarına, bağlanamazlığa, güven listelerine, iptal mekanizmalarına, belge verme ve gösterme protokollerine ve bütün bunların Türk dünyası için ne anlama geldiğine.

Kaynaklar

[1] Steiner, P. (1993). "On the Internet, nobody knows you're a dog." *The New Yorker*, 5 Temmuz 1993.

[2] McMillan, R. (2012). “The World’s First Computer Password? It Was Useless Too.” *Wired*, 27 Ocak 2012.
[3] Morris, R. ve Thompson, K. (1979). “Password Security: A Case History.” *Communications of the ACM*, 22(11), 594–597.
[4] W3C (2019). *Web Authentication: An API for accessing Public Key Credentials, Level 1.* W3C Recommendation, Mart 2019.
[5] OASIS (2005). *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, Mart 2005.
[6] Hardt, D. (Ed.) (2012). *The OAuth 2.0 Authorization Framework.* IETF RFC 6749.
[7] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B. ve Mortimore, C. (2014). *OpenID Connect Core 1.0.* OpenID Foundation, 25 Şubat 2014.
[8] Jones, M., Bradley, J. ve Sakimura, N. (2015). *JSON Web Token (JWT).* IETF RFC 7519.
[9] Schroepfer, M. (2018). “An Update on Our Plans to Restrict Data Access on Facebook.” Meta Newsroom, 4 Nisan 2018.
[10] Cameron, K. (2005). *The Laws of Identity.* Microsoft Corporation, Mayıs 2005.
[11] Allen, C. (2016). “The Path to Self-Sovereign Identity.” *Life With Alacrity*, 25 Nisan 2016.
[12] W3C (2022). *Decentralized Identifiers (DIDs) v1.0.* W3C Recommendation, 19 Temmuz 2022.
[13] W3C (2025). *Verifiable Credentials Data Model v2.0.* W3C Recommendation, 15 Mayıs 2025.
[14] Avrupa Parlamentosu ve Konseyi (2014). *İç pazarda elektronik işlemler için elektronik kimlik ve güven hizmetlerine ilişkin 910/2014 sayılı Tüzük (AB) (eIDAS).* Avrupa Birliği Resmî Gazetesi, L 257, 28 Ağustos 2014.
[15] Avrupa Parlamentosu ve Konseyi (2024). *Avrupa Dijital Kimlik Çerçevesinin oluşturulması bakımından 910/2014 sayılı Tüzüğü değiştiren 2024/1183 sayılı Tüzük (AB).* Avrupa Birliği Resmî Gazetesi, 30 Nisan 2024.
[16] Avrupa Komisyonu ve eIDAS Uzman Grubu. *European Digital Identity Wallet — Architecture and Reference Framework (ARF).* github.com/eu-digital-identity-wallet (yaşayan belge; okunan sürüm yazının yayın tarihindeki son sürümdür).
[17] Fett, D., Yasuda, K. ve Campbell, B. (2025). *Selective Disclosure for JSON Web Tokens.* IETF RFC 9901, Kasım 2025. Ayrıca: *SD-JWT-based Verifiable Credentials (SD-JWT VC)*, IETF OAuth Çalışma Grubu taslağı.
[18] ISO/IEC (2021). *ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application.*
[19] Avrupa Komisyonu (2015). *Elektronik kimlik araçlarının güvence düzeylerine ilişkin teknik şartları ve prosedürleri belirleyen 2015/1502 sayılı Uygulama Tüzüğü (AB).*
[20] Grassi, P. A., Garcia, M. E. ve Fenton, J. L. (2017). *Digital Identity Guidelines.* NIST Special Publication 800-63-3, Haziran 2017. (Dördüncü revizyonu SP 800-63-4, Temmuz 2025.)

Okuma listesi: Buradan başlayın

Konuya yeni başlayan bir okur için, bu yazıdan sonra okunabilecek beş kaynak:

1. **Kim Cameron, *The Laws of Identity* (2005).** Kısa, sade ve yirmi yıl sonra hâlâ geçerli. Dijital kimlikte “doğru” sorusunun ne olduğunu anlamak için en iyi başlangıç.
2. **Christopher Allen, *The Path to Self-Sovereign Identity* (2016).** SSI hareketinin manifestosu; bu yazıdaki dönemlendirmenin de kaynaklarından biri.
3. **W3C, *Verifiable Credentials Data Model v2.0* — giriş bölümleri.** Standardın ilk bölümleri, üçgen modeli ve temel kavramları örneklerle anlatıyor; teknik ayrıntılara girmeden okunabilir.
4. **Tüzük (AB) 2024/1183’ün gerekçe bölümleri (*recitals*).** Tüzüğün başındaki gerekçeler, maddelerden çok daha okunaklıdır ve AB’nin cüzdanla neyi amaçladığını kendi ağzından anlatır.
5. **EUDI ARF’nin “Introduction” ve “Ecosystem” bölümleri.** Bölüm 7.4’teki rollerin resmî tanımları ve aralarındaki ilişkiler.

Ek A — Sözlük

Bu yazıda geçen terimler, yazıdaki anlamlarıyla. Teknik terimlerin İngilizce karşılıkları, başka kaynaklarda aranabilmeleri için parantez içinde verilmiştir.

Tablo A.1. Terimler sözlüğü.

Terim	İngilizce	Anlamı
Açık anahtar	public key	Bir anahtar çiftinin herkesle paylaşılan yarısı; imzaları doğrulamaya yarar
Açık anahtarlı kriptografi	public-key cryptography	Gizli ve açık anahtardan oluşan çiftlerle imza ve şifreleme yapan yöntem
Ada (silo) modeli	siloed identity	Her hizmetin kendi kullanıcı kaydını tuttuğu model
ARF	Architecture and Reference Framework	AB dijital kimlik cüzdanının teknik mimari ve başvuru çerçevesi
Belge, kimlik bilgisi	credential	Bir kurumun bir kişi hakkında söylediklerini taşıyan, onaylanmış kayıt
Doğrulanabilir belge	verifiable credential (VC)	Veren tarafından dijital olarak imzalanmış, doğrulanabilir belge
Doğrulayan, güvenen taraf	verifier, relying party	Belgeyi inceleyip ona dayanarak karar veren kurum
EAA / QEAA / PuB-EAA	(qualified / public body) electronic attestation of attributes	PID dışındaki öznitelik onayları ve güvence türleri
Federasyon	federated identity	Kimlik doğrulamanın bir kimlik sağlayıcıya devredildiği model
Geçiş anahtarı	passkey	Parolanın yerine geçen, yalnızca kayıtlı olduğu siteye cevap veren kriptografik anahtar
Gizli anahtar	private key	Bir anahtar çiftinin yalnızca sahibinde kalan yarısı; imza üretmeye yarar
Güven listesi	trusted list	Hangi kurumun hangi rolde yetkili olduğunu söyleyen, imzalı resmî liste
Kendi kendine egemen kimlik	self-sovereign identity (SSI)	Kimliğin kişinin kendi cüzdanında tutulduğu model
Kimlik	identity	Bir varlığa ait özniteliklerin belirli bir bağlamdaki toplamı
Kimlik belirteci	ID token	OpenID Connect'te kimlik sağlayıcının imzaladığı, kısa ömürlü kimlik kaydı
Kimlik doğrulama	authentication	"İddia ettiğin kişi misin?" sorusunun cevaplanması
Kimlik güvencesi düzeyi	level of assurance (LoA)	Bir kimlik iddiasına ne kadar güvenilebileceğinin ölçüsü
Kimlik sağlayıcı	identity provider (IdP)	Federasyonda kullanıcıların kimliğini doğrulayan kurum
Merkeziyetsiz tanımlayıcı	decentralized identifier (DID)	Merkezî bir kayıt kurumuna bağlı olmadan oluşturulan tanımlayıcı
Oltalama	phishing	Kullanıcıyı sahte bir sayfaya yönlendirip bilgisini çalma
Öznitelik	attribute	Bir varlık hakkındaki tek bir bilgi parçası
Özet fonksiyonu	hash function	Girdiden sabit uzunlukta, geri döndürülemez bir parmak izi üreten işlem
PID	person identification data	Devletin ya da yetkilendirdiği kurumun verdiği temel kişi kimlik bilgisi
Sahip	holder	Belgeyi taşıyan ve gösteren kişi
Seçici açıklama	selective disclosure	Bir belgenin yalnızca gereken kısmını gösterebilme
Tanımlayıcı	identifier	Bir varlığı belirli bir sistem içinde diğerlerinden ayıran değer

Terim	İngilizce	Anlamı
Tek oturum açma	single sign-on (SSO)	Bir kez giriş yapıp birçok sisteme erişebilme
Tuz	salt	Parolayla birleştirilip özetlenen, kullanıcıya özel rastgele değer
Veren	issuer	Belgeyi düzenleyen ve içeriğini taahhüt eden kurum
Yetkilendirme	authorization	“Bu kişi bu işi yapmaya yetkili mi?” sorusunun cevaplanması