TAMGA NETWORK

TAMGA NETWORK AKADEMIK ÇALIŞMALAR

Doğrulanabilir Belgeler

Veren, Taşıyan, Doğrulayan: İmzalı Verinin Üç Biçimi ve Belgenin Sahibine Bağlanması

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

Telefonumuzda taşıdığımız belgelerin çoğu, kâğıt belgenin fotoğrafından ya da taranmış bir PDF'inden ibarettir. Böyle bir dosyaya bakan kişi onun gerçek olup olmadığını anlayamaz; anlamak isterse belgeyi veren kuruma sormak zorunda kalır. Doğrulanabilir belge bu durumu değiştirir. Belgeyi veren kurum, içindeki bilgileri bir makinenin okuyabileceği biçimde yazar ve dijital olarak imzalar; kişi belgeyi kendi cüzdanında taşır; belgeyi inceleyen kurum da imzayı kontrol ederek, veren kuruma hiç sormadan, belgenin değiştirilmediğini, kimin verdiğini ve gösteren kişiye ait olduğunu anlar. Bu yazı, dizinin ilk yazısında tanıttığımız veren, sahip ve doğrulayan rollerini bu kez belgenin kendisinden bakarak ele alıyor.

Yazıda önce imzanın neyi kanıtlayıp neyi kanıtlamadığını, sonra doğrulayanın veren kuruma sormak zorunda kaldığı "eve telefon etme" durumunu anlatıyoruz. Ardından bugün yaygın olan üç belge biçimini, W3C Verifiable Credentials Data Model 2.0'ı, IETF'in SD-JWT VC biçimini ve ISO/IEC 18013-5 mobil belge (mdoc) biçimini, örnek veri yapılarıyla yan yana koyuyoruz. Belgenin kopyalanıp başkasınca kullanılmasını önleyen sahip bağlama yöntemini adım adım açıklıyor, son olarak Avrupa Birliği'nin kişi kimlik verisi (PID) ve öznitelik onayları (EAA) için hangi biçimleri seçtiğini ve bu seçimin gerekçelerini tartışıyoruz.

Anahtar kelimeler: doğrulanabilir belge · dijital imza · W3C Verifiable Credentials · SD-JWT VC · ISO/IEC 18013-5 · mdoc · sahip bağlama · eIDAS 2.0 · PID · EAA

ATIF

Karataş, B. (2026). Doğrulanabilir Belgeler: Veren, Taşıyan, Doğrulayan: İmzalı Verinin Üç Biçimi ve Belgenin Sahibine Bağlanması. Tamga Network Akademik Çalışmalar, A2. https://tamga.network/files/publications/verifiable-credentials-tr.pdf

İçindekiler

1 Giriş: Bir Diplomanın Üç Hâli 3
2 Kâğıt Belgeden İmzalı Veriye 4
2.1 Kâğıt belge neden işe yarar? 4
2.2 Telefondaki PDF 4
2.3 İmzalı veri: sayfadan iddialara 5
2.4 İmza neyi kanıtlar, neyi kanıtlamaz? 5
3 Üç Rol ve “Eve Telefon Etme” Sorunu 6
3.1 Veren, sahip, doğrulayan 6
3.2 Doğrulayanın dört sorusu 7
3.3 Eve telefon etme 8
3.4 Doğrulayan da doğrulanır 9
4 Bir Doğrulanabilir Belgenin Anatomisi 10
5 W3C Verifiable Credentials Data Model 11
5.1 Kısa tarihçe 11
5.2 Yapı 11
5.3 Güvenceleme: imza nereye konur? 12
5.4 Sunum 12
5.5 Verenin anahtarı nerede? 12
6 SD-JWT VC: Seçici Açıklamalı JSON Belgesi 13
6.1 JWT’den SD-JWT’ye 13
6.2 Yapı 14
6.3 Sunum 14
7 ISO/IEC 18013-5: Mobil Belge (mdoc) 15
7.1 Mobil ehliyetin doğuşu 15
7.2 Yapı: alan alan imzalanan veri 15
7.3 Yüz yüze ve uzaktan gösterim 16
7.4 Verenin sertifikası nereden gelir? 17
8 Sahip Bağlama: Belge Neden Bir Anahtara Bağlanır? 17
8.1 Kopyalanan belge sorunu 17
8.2 Anahtar bağlama nasıl çalışır? 17
8.3 Anahtar nerede durur? 19
8.4 Başka bağlama yolları 19
9 Biçimlerin Karşılaştırması ve AB’nin Seçimi 20
9.1 Üç biçim yan yana 20
9.2 AB’nin seçimi: PID ve EAA 20
9.3 Bir kurum hangi biçimi seçmeli? 21
10 Sınırlar ve Açık Sorular 22
11 Bu Tablonun İçinde Tamga Network 22
12 Sonuç 23
Kaynaklar 23
Okuma listesi: Buradan başlayın 24
Ek A — Sözlük 24

1 Giriş: Bir Diplomanın Üç Hâli

Aynur'u dizinin ilk yazısından hatırlayan okur, onun Bakü'de lisansını bitirip İstanbul'da yüksek lisans yapmak istediğini bilir. Bu yazıda Aynur'un hikâyesini bir adım ileri taşıyoruz. Başvurusu kabul edildi, İstanbul'a taşındı ve şimdi yarı zamanlı bir iş arıyor. Bir yazılım şirketi onu görüşmeye çağırdı ve görüşmeden önce diplomasının bir kopyasını istedi.

Aynur'un elinde aynı diplomanın üç ayrı hâli var. İlki duvarda asılı duran, mühürlü ve ıslak imzalı kâğıt diploma. İkincisi telefonunun galerisinde duran, bu kâğıdın bir yıl önce çekilmiş fotoğrafı ve onu bir uygulamayla PDF'e çevirdiği dosya. Üçüncüsü ise üniversitesinin mezuniyette telefonundaki cüzdan uygulamasına gönderdiği dijital diploma. Üçü de aynı bilgiyi taşıyor: Aynur'un adı, bölümü, derecesi, mezuniyet tarihi. Ama şirketin insan kaynakları uzmanı açısından bu üç hâl arasında çok büyük bir fark var (Şekil 1).

Kâğıt diplomayı eline alan uzman, mührü, imzayı, kâğıdın dokusunu görebilir, ama İstanbul'da oturup Bakü'deki bir üniversitenin mührünü tanıması beklenemez. PDF'e bakan uzman ise hiçbir şey göremez: bir görüntü düzenleme programıyla on dakikada değiştirilmiş bir dosya ile aslından alınmış bir dosya ekranda aynı görünür. Emin olmak isterse yapabileceği tek şey Bakü'deki üniversiteye e-posta yazıp "Bu kişi gerçekten sizden mezun oldu mu?" diye sormaktır. Üçüncü hâl ise başka bir şeydir. Uzman, şirketin kullandığı yazılım aracılığıyla Aynur'dan diplomasını ister, Aynur telefonundan onaylar ve birkaç saniye içinde yazılım şunu söyler: Bu diploma Bakü'deki üniversite tarafından imzalanmış, imzalandığından beri tek bir harfi değişmemiş, süresi geçmemiş, iptal edilmemiş ve şu anda onu gösteren kişiye ait. Üstelik Bakü'deki üniversite bu işlemden habersiz kalır.

Bu üçüncü hâle **doğrulanabilir belge** (*verifiable credential*) diyoruz. Bu yazının sorusu da şu: Bir belgeyi doğrulanabilir yapan nedir? Bir dosyanın "telefondaki belge" olmasıyla "doğrulanabilir belge" olması arasındaki fark tam olarak nerede başlıyor?

Sorunun cevabı, dizinin ilk yazısında tanıştığımız üç kavramın birleşiminde yatıyor: belgenin içeriğini değiştirilemez kılan **dijital imza**, imzayı atanın kim olduğunu ve buna yetkili olup olmadığını söyleyen **güven altyapısı** ve belgeyi onu taşıyan kişiye bağlayan **sahip bağlama** (*holder binding*). İlki matematikle, ikincisi kurumlarla, üçüncüsü de kişinin elindeki cihazla ilgilidir. Bu yazı ağırlıkla birinci ve üçüncüsünü ele alıyor; güven altyapısı ise dizinin altıncı yazısının konusu.

Yazının planı şöyle. Bölüm 2'de kâğıttan imzalı veriye geçişi ve imzanın sınırlarını anlatıyoruz. Bölüm 3, veren, sahip ve doğrulayan rollerini ve doğrulayanın veren kuruma sormak zorunda kaldığı durumu, yani "eve telefon etme" sorununu ele alıyor. Bölüm 4 her doğrulanabilir belgede bulunan ortak parçaları sıralıyor. Bölüm 5, 6 ve 7 bugünün üç ana belge biçimini, W3C Verifiable Credentials, SD-JWT VC ve ISO mdoc'u sırasıyla anlatıyor. Bölüm 8 sahip bağlamayı, Bölüm 9 da biçimlerin karşılaştırmasını ve Avrupa Birliği'nin seçimini inceliyor. Bölüm 10 açık soruları, Bölüm 11 bu yazıyı yayımlayan Tamga Network'ün bu konudaki yerini anlatıyor. Ek A'da yazıda geçen terimlerin sözlüğü var.



Şekil 1. Bir diplomanın üç hâli ve doğrulayanın her birinde görebildiği

2 Kâğıt Belgeden İmzalı Veriye

2.1 Kâğıt belge neden işe yarar?

Kâğıt bir belgenin değeri, üzerindeki yazıdan çok, o yazının **kimden geldiğini** ve **değiştirilmediğini** gösteren işaretlerden gelir. Bir diplomanın kâğıdındaki filigran, kabartma mühür, hologram ve ıslak imza, belgeyi taklit etmeyi zorlaştırmak için oradadır. Bu işaretler belgeyi inceleyen kişiye iki şey söyler: Bu kâğıt, bu mührü basmaya yetkili bir kurumdan çıkmıştır ve üzerindeki yazı sonradan kazınıp değiştirilmemiştir.

Ama kâğıt belgenin bu iki güvencesi de **inceleyenin bilgisine** dayanır. Bir Türk bankasının memuru, bir Türk nüfus cüzdanının güvenlik özelliklerini tanır; aynı memurun bir Kırgız sürücü belgesinin hologramını tanıması beklenemez. Belgeler sınır geçtikçe güvenleri azalır. Bunun için yüzyıllar içinde bir dizi aracı yapı kuruldu: noter onayı, konsolosluk tasdiki ve sonunda, 1961 Lahey Sözleşmesi ile **apostil**. Apostil, bir belgenin üzerindeki imzanın ve mührün gerçekten o ülkenin yetkili bir makamına ait olduğunu, belgeyi veren ülkenin yetkili bir makamının onaylamasıdır. Yani apostil bir **belge hakkındaki belgedir**: “bu mühür gerçektir” diyen ikinci bir mühür. Aynur’un yüksek lisans başvurusunda haftalarca uğraştığı süreç buydu.

2.2 Telefondaki PDF

Bugün belgelerimizin büyük bir kısmı kâğıttan ekrana taşındı, ama bu taşınmanın önemli bir kısmı yalnızca **görüntünün** taşınmasıdır. Kâğıt diplomanın fotoğrafı, kâğıdın güvenlik özelliklerinin hiçbirini taşımaz: filigran fotoğrafta görünmez, kabartma mühür düz bir lekeye dönüşür, hologramın ışıkla değişen rengi kaybolur. Elde kalan, makinenin değil yalnızca insanın okuyabileceği bir resimdir ve o resim, dizinin ilk yazısında anlattığımız gibi, sınırsız ve izsiz biçimde değiştirilebilir.

Telefondaki belgelerin hepsi bu kadar savunmasız değildir. İki ara biçimi ayırmakta fayda var.

Birincisi **elektronik imzalı PDF**’tir. Bir kurum, ürettiği PDF’i elektronik imza ya da elektronik mühürle imzalayabilir. Böyle bir dosyayı PDF okuyucusunda açtığınızda, okuyucu imzanın geçerli olup olmadığını ve dosyanın imzadan sonra değişip değişmediğini gösterir. Bu, gerçek bir kriptografik güvencedir. Ama bir sınırı vardır: İmza **bütün dosyanın** üzerindedir ve dosyanın içindeki bilgi sayfaya dizilmiş harfler hâlinde durur; bir makinenin tek tek tanıyabileceği alanlara ayrılmamıştır. Bir yazılım bu PDF’ten “mezuniyet tarihi” alanını güvenle okuyamaz; okuduğu şeyin hangi alan olduğunu tahmin

etmek zorundadır. Ayrıca belgeyi göstermek, bütün belgeyi göstermek demektir; içinden yalnız bir satır paylaşılamaz.

İkincisi **doğrulama kodlu belgedir**. Türkiye'de e-Devlet Kapısı üzerinden alınan birçok belgenin altında bir barkod ya da doğrulama kodu bulunur; belgeyi alan kurum bu kodu e-Devlet'in belge doğrulama hizmetine girer ve belgenin aslını sistemden görür. Bu yöntem pratik ve güvenlidir, çünkü doğrulamanın dayanağı belgeyi veren sistemdeki kayıttır; elinizdeki kâğıt yalnızca o kayda ulaşmanın yoludur. Ama tam da bu nedenle, her doğrulama belgeyi veren sisteme yapılan bir sorgudur. Bölüm 3.3'te bu modelin adını koyacağız.

2.3 İmzalı veri: sayfadan iddialara

Elektronik imzalı PDF de imzalıdır; doğrulanabilir belgeye geçişte asıl değişen, **imzanın neyin üzerine atıldığıdır**. Doğrulanabilir belgede veren kurum bir sayfayı imzalamaz, bir **veri yapısını** imzalar. Bu veri yapısı, kişi hakkında yapılan **iddialardan** (*claims*) oluşur. İddia, alan yazınında şöyle tanımlanır: bir özne hakkında söylenen bir şey. "Aynur'un adı Aynur'dur", "Aynur 2001'de doğmuştur", "Aynur Bilgisayar Mühendisliği bölümünden lisans derecesiyle mezun olmuştur" birer iddiadır.

Bu iddialar makinenin okuyabileceği bir biçimde yazılır: her biri bir **ad** ve bir **değerden** oluşur (`derece: "Lisans"`, `mezuniyetTarihi: "2026-06-30"`). Böylece belgeyi alan yazılım, "mezuniyet tarihi" alanını tahmin etmeden, adıyla okur. Bu basit görünen fark üç kapı açar. İlki **otomatik doğrulamadır**: Bir şirketin başvuru sistemi yüzlerce diplomayı insan eli değmeden kontrol edebilir. İkincisi **seçici açıklamadır**: İddialar ayrı ayrı ele alınabildiği için, kişi belgenin tamamını değil yalnızca gereken alanını gösterebilir (dizinin üçüncü yazısının konusu). Üçüncüsü **birlikte çalışabilirliktir**: Alan adları ve anlamları ortak bir sözlükte tanımlanırsa, Bakü'deki bir üniversitenin verdiği diplomayı İstanbul'daki bir şirketin yazılımı da anlar.

TARİHÇE

Kitlesel ölçekte ilk doğrulanabilir belgeler

Doğrulanabilir belge fikri cüzdan uygulamalarından çok daha eskidir ve iki büyük örneği milyarlarca kişinin cebine girmiştir.

Elektronik pasaport. Uluslararası Sivil Havacılık Örgütü'nün (ICAO) makinece okunabilir seyahat belgeleri standardı Doc 9303, pasaportun içine bir çip yerleştirilmesini ve çipteki verilerin (kimlik bilgileri, fotoğraf) pasaportu veren devletin anahtarıyla imzalanmasını tanımlar [14]. Çipte, her veri grubunun özetini içeren ve devletin imzaladığı bir **güvenlik nesnesi** bulunur. Sınır kapısındaki okuyucu, çipten okuduğu verilerin özetini hesaplar, imzalı nesnedeki özetlerle karşılaştırır ve imzayı o devletin sertifikasıyla doğrular. Bu yazıda Bölüm 7'de anlatacağımız mobil belge biçimi, bu tasarımın doğrudan torunudur.

AB Dijital COVID Sertifikası. 2021'de Avrupa Birliği, aşı, test ve iyileşme bilgilerini taşıyan bir sertifikayı Tüzük (AB) 2021/953 ile hayata geçirdi [15]. Sertifika bir QR kodun içine sığdırılmış, CBOR biçiminde kodlanmış ve COSE ile imzalanmış küçük bir veri yapısıydı. Doğrulama uygulamaları, ülkelerin imzalama anahtarlarını önceden indirip saklıyor, QR kodu okuduktan sonra imzayı internete çıkmadan kontrol ediyordu. Avrupa Komisyonu'na göre bu sistemle 2,3 milyardan fazla sertifika verildi; Haziran 2023'te de sistem, küresel bir ağın ilk yapı taşı olarak Dünya Sağlık Örgütü'ne devredildi [16]. Bu, imzalı verinin ve önceden dağıtılmış güven listesinin ölçeklenebildiğinin belki de en güçlü kanıtıdır.

2.4 İmza neyi kanıtlar, neyi kanıtlamaz?

Dijital imzanın matematiğini dizinin ilk yazısında anlattık: Veren, belgenin özetini gizli anahtarıyla imzalar; doğrulayan, özeti yeniden hesaplar ve imzayı verenin açık anahtarıyla kontrol eder. İmza tutuyorsa iki şey kesinleşir. Birincisi **bütünlüktür**: Belge, imzalandığı andan beri tek bir bit bile değişmemiştir. İkincisi **kaynaktır**: İmza, bu açık anahtarın eşi olan gizli anahtarla atılmıştır.

Bu iki güvence çok güçlüdür, ama doğrulanabilir belgeyi tartışırken en sık yapılan hata, imzanın bunlardan fazlasını kanıtladığını sanmaktır. Tablo 1, imzanın tek başına cevap veremediği soruları sıralıyor.

Tablo 1. Dijital imza neyi kanıtlar, neyi kanıtlamaz?

Soru	İmza tek başına cevaplar mı?	Cevap nereden gelir?
Belge imzalandığından beri değişti mi?	evet	özet ve imza doğrulaması
Belge hangi anahtarla imzalandı?	evet	imza doğrulaması
O anahtar kime ait?	hayır	sertifika ya da güven listesi (dizinin 6. yazısı)
O kurum bu tür belgeyi vermeye yetkili mi?	hayır	güven listesi, kurum kaydı
Belge hâlâ geçerli mi, iptal edildi mi?	kısmen (süre)	geçerlilik tarihleri ve durum listesi (dizinin 7. yazısı)
Belgeyi gösteren kişi, belgenin sahibi mi?	hayır	sahip bağlama (Bölüm 8)
İçindeki bilgi doğru mu?	hayır	verenin süreçleri ve sorumluluğu

Son satır özellikle önemli. İmza, verenin bu bilgiyi **söylediğini** kanıtlar; söylediği şeyin **doğru** olduğunu kanıtlamaz. Bir üniversite yanlışlıkla bir öğrencinin bölümünü hatalı yazarsa, imza bu hatalı bilgiyi de aynı titizlikle korur. Doğrulanabilir belgenin güveni, sonuçta onu veren kurumun güvenilirliğinden ve o kurumun bu bilgiyi verirken uyguladığı süreçlerden gelir. Teknoloji bu güveni taşır; onu yaratmaz.

ÖNEMLİ

Bu bölümden akılda kalması gereken

Telefondaki bir belgenin fotoğrafı ya da taranmış PDF'i doğrulanabilir değildir; doğrulamak için belgeyi verene sormak gerekir. Doğrulanabilir belgede veren kurum, makinenin okuyabileceği iddiaları imzalar. İmza belgenin değişmediğini ve hangi anahtarla imzalandığını kanıtlar; anahtarın kime ait olduğunu, belgenin hâlâ geçerli olup olmadığını ve gösterenin sahibi olup olmadığını ise başka mekanizmalar söyler.

3 Üç Rol ve "Eve Telefon Etme" Sorunu

3.1 Veren, sahip, doğrulayan

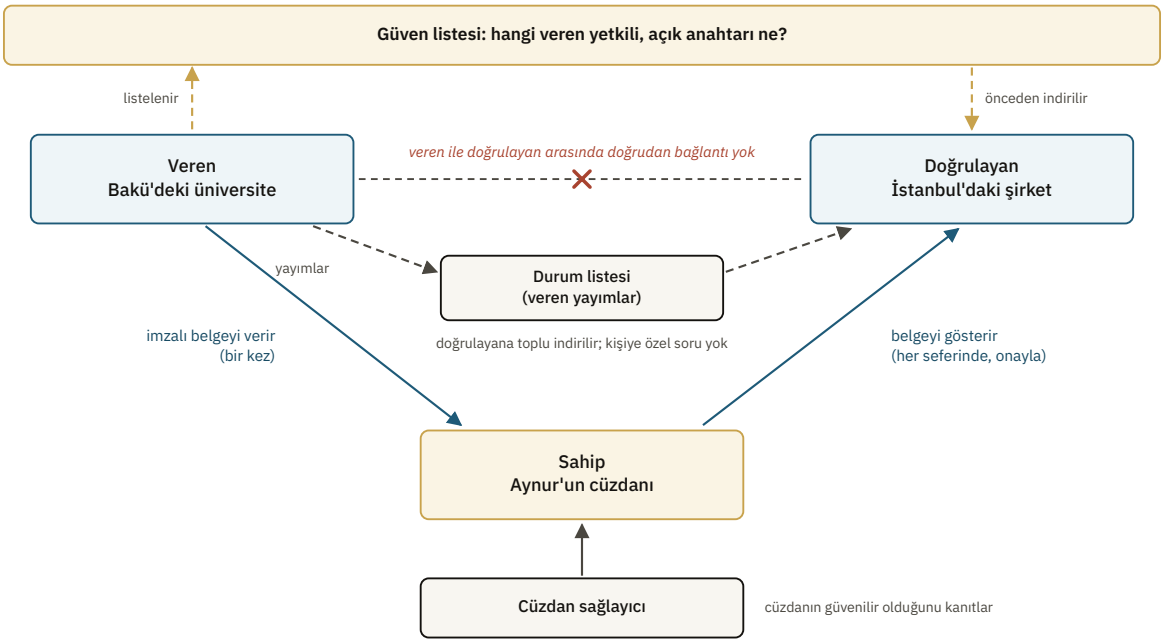
Dizinin ilk yazısında doğrulanabilir belgenin üç rolünü tanıtmıştık. Kısaca hatırlayalım ve bu kez her rolün **ne yaptığını** değil, **neyi bildiğini ve neyi bilmediğini** soralım; çünkü bir belge sisteminin mahremiyeti büyük ölçüde bu bilgi dağılımına bağlıdır.

Veren (*issuer*), belgeyi düzenleyen ve imzalayan kurumdur. Aynur'un diplomasında Bakü'deki üniversite, kimlik bilgisinde Azerbaycan devletinin yetkili kurumu. Veren, belgenin içeriğini bilir, çünkü onu kendisi yazmıştır. Belgeyi kime verdiğini bilir. İyi tasarlanmış bir sistemde ise belgenin **daha sonra kime, ne zaman gösterildiğini** bilmez.

Sahip (*holder*), belgeyi taşıyan ve gösteren taraftır; çoğu zaman belgenin hakkında olduğu kişinin kendisidir. Aynur, belgelerini telefonundaki **cüzdan** uygulamasında saklar. Sahip bütün belgelerini ve onları kime gösterdiğini bilir; cüzdanlar bu bilgiyi kişiye bir işlem geçmişi olarak sunabilir.

Doğrulayan (*verifier*), belgeyi isteyen, inceleyen ve ona dayanarak bir karar veren kurumdur: Aynur'un başvurduğu şirket, bir banka, bir kamu hizmeti. AB'nin hukuki dilinde **güvenen taraf** (*relying party*) olarak da anılır. Doğrulayan yalnızca kendisine gösterilen belgeyi ve belgenin kendisine gösterilen alanlarını bilir.

Gerçek bir sistemde bu üç rolün yanında birkaç **yardımcı rol** daha vardır ve bunlar, belgenin doğrulanmasını mümkün kılar (Şekil 2). **Güven listesi işletmecisi**, hangi verenin hangi belgeyi vermeye yetkili olduğunu ve açık anahtarlarının ne olduğunu söyleyen imzalı listeyi yayımlar. **Durum listesi**, verenin yayımladığı ve belgelerin iptal edilip edilmediğini gösteren bir dosyadır. **Cüzdan sağlayıcı** ise cüzdan uygulamasını geliştiren ve cüzdanın güvenilir olduğunu kanıtlayan kuruluştur. Bu yardımcı rollerin ortak özelliği şudur: Doğrulayan onlardan **toplu bilgi** alır, kişiye özel bir soru sormaz. Güven listesini indiren bir doğrulayan, "Aynur'un diploması gerçek mi?" diye sormaz; "Bakü'deki üniversitenin açık anahtarı nedir?" diye sorar ve bu cevabı binlerce diplomanın doğrulamasında tekrar tekrar kullanır.



Şekil 2. Doğrulanabilir belgenin rolleri: üç ana rol ve yardımcı roller

3.2 Doğrulayanın dört sorusu

Aynur diplomasını şirkete gösterdiğinde, şirketin yazılımı arka planda dört soruya cevap arar. Bu dört soru, hangi belge biçimi kullanılırsa kullanılsın aynıdır ve bir doğrulayıcının bütün işini özetler (Şekil 3).

1. **Belge sağlam mı?** Belgenin imzası, belgede adı geçen verenin açık anahtarıyla doğrulanır. İmza tutmuyorsa belge ya değiştirilmiştir ya da başkası tarafından imzalanmıştır; işlem burada biter.
2. **Veren gerçekten yetkili mi?** İmzayı atan anahtarın, güven listesinde diploma vermeye yetkili bir kuruma ait olup olmadığına bakılır. İmza matematiksel olarak doğru olabilir ama kendine "üniversite" diyen herhangi biri de doğru imza atabilir.
3. **Belge hâlâ geçerli mi?** Belgenin geçerlilik süresi kontrol edilir; verenin yayımladığı durum listesinde belgenin iptal edilip edilmediğine bakılır.
4. **Gösteren, sahibi mi?** Belgeyi gösteren cüzdanın, belgenin bağlandığı anahtarı elinde tuttuğu kanıtlanır. Bu kanıt, belgenin kopyalanıp başkası tarafından gösterilmesini engeller.

Dört soru da evet cevabı alırsa doğrulayan belgedeki iddialara dayanarak kararını verir. Dikkat edilirse bu dört sorunun hiçbiri için verene **o anda** bir soru sorulmuyor. Birinci ve dördüncü soru yalnızca belgeyle ve cüzdanla, ikinci ve üçüncü soru ise önceden indirilmiş, herkese açık listelerle cevaplanıyor.



Hiçbir adımda verene o anda soru sorulmaz.

Şekil 3. Doğrulayanın dört sorusu: her biri nereden cevaplanır?

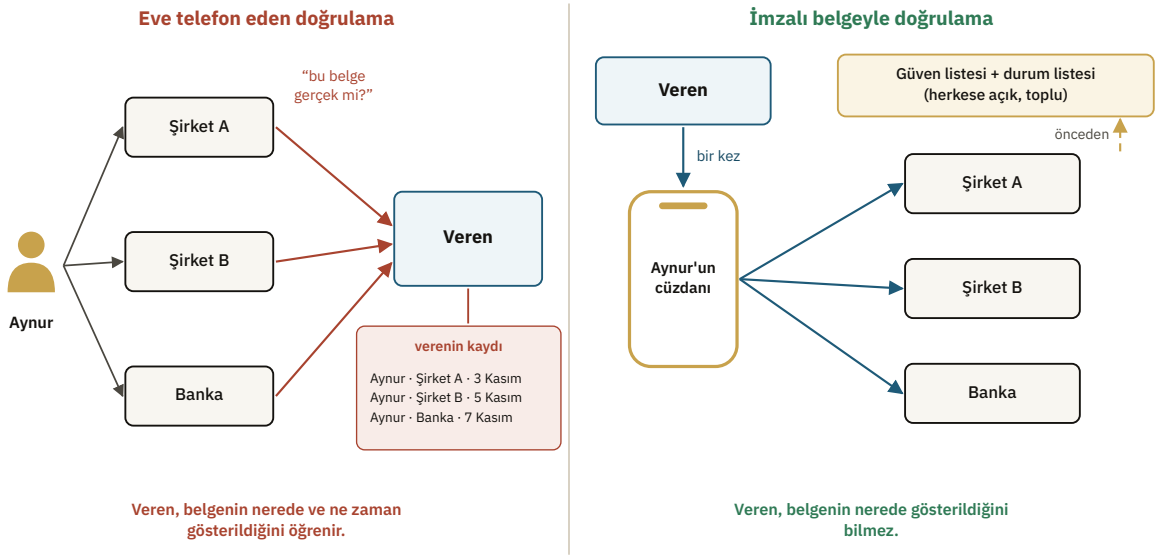
3.3 Eve telefon etme

Şimdi, Bölüm 2.2'de doğrulama kodlu belgelerden söz ederken adını koymayı ertelediğimiz modele dönebiliriz. Doğrulayan bir belgenin gerçek olduğunu anlamak için her seferinde belgeyi verene soruyorsa, alan yazınında bu duruma **eve telefon etme** (*phone home*) denir. Belge, kullanıldığı her yerden "evini", yani kendisini veren kurumu arar.

Eve telefon etmenin birkaç biçimi vardır. En açığı **doğrudan sorgudur**: Doğrulayan, verenin sistemine "şu numaralı belge gerçek mi?" diye sorar. Bölüm 2.2'deki doğrulama kodlu belgeler böyle çalışır. Daha az göze batan biçimi, **çevrimiçi iptal sorgusudur**: Belgenin kendisi imzalı olsa bile, doğrulayan "bu belge iptal edildi mi?" sorusunu verene o belgeye özel olarak sorar. Web'deki sertifikalar için geliştirilen OCSP protokolü bu türden bir sorgudur ve dizinin yedinci yazısında göreceğimiz gibi, mahremiyet açısından aynı sorunu taşır. Üçüncü biçim **sunucudan alma**dır: Kişi belgeyi taşımaz, yalnızca bir erişim anahtarı taşır; doğrulayan bu anahtarla belgenin verisini doğrudan verenin sunucusundan çeker. Bölüm 7'de anlatacağımız mobil ehliyet standardı ISO/IEC 18013-5, cihazdan alma ile birlikte bu "sunucudan alma" (*server retrieval*) yöntemini de tanımlar.

Eve telefon etmenin sakıncası teknik bir kusurdan gelmez; modelin yapısından gelir. Her sorgu, veren kuruma üç bilgi verir: **hangi belge**, **hangi doğrulayana**, **ne zaman** gösterildi. Bir üniversite için bu, mezunlarının hangi şirketlere başvurduğunu görmek demektir. Bir kimlik belgesini veren devlet kurumu içinse, vatandaşın hangi bankaya, hangi siteye, hangi hizmete kimliğini gösterdiğinin eksiksiz bir kaydı demektir. Kurumun bu kaydı kötüye kullanma niyeti olmasa bile kayıt vardır; sızabilir, başka amaçla istenebilir, birleştirilebilir. Dizinin ilk yazısında federasyon için kullandığımız benzetme burada da geçerli: Eve telefon eden bir belge sistemi, verene kişinin dijital hayatının her kapısında bekleyen bir kapıcı rolü verir. Şekil 4 iki modeli yan yana gösteriyor.

Avrupa Birliği bu konuda net bir tutum almıştır. eIDAS 2.0 tüzüğü, cüzdanın teknik çerçevesinin belge verenlerin ya da başka bir tarafın, belge verildikten sonra kişinin işlemlerini izlemesine imkân vermemesini şart koşar [11]. Temmuz 2026'da kabul edilen 2026/1731 sayılı uygulama tüzüğü ise bir adım daha ileri giderek, cüzdanların, belge verenlerin ve AB cüzdanlarından belge isteyen güvenen tarafların ISO/IEC 18013-5'teki sunucudan alma yöntemini **desteklememesini** açıkça yazmıştır [13]. Yani AB'de yüz yüze gösterilen bir mobil belgenin verisi cihazdan alınır; verenin sunucusuna gidilmez.



Şekil 4. Eve telefon eden doğrulama ile imzalı belgeyle doğrulama

ÖRNEK

Aynur'un diploması iki sistemde

Birinci sistemde Aynur'un diploması bir doğrulama kodu taşıyor. Aynur üç şirkete ve bir bankaya başvuruyor; her biri kodu üniversitenin doğrulama sayfasına giriyor. Bir ay sonra Bakü'deki üniversitenin sunucusunda dört kayıt birikmiş durumda: Aynur'un diploması, hangi gün, hangi kurum tarafından doğrulandı. Aynur'un iş aradığını ve hangi sektörlere başvurduğunu, Aynur'un kendisinden başka bilen tek yer üniversitenin sunucusu.

İkinci sistemde diploma imzalı bir belge olarak Aynur'un cüzdanında duruyor. Aynı dört kurum diplomayı doğruluyor; her biri üniversitenin açık anahtarını haftalar önce indirdiği güven listesinden alıyor, iptal durumunu da yine haftada bir indirdiği, binlerce diplomayı birlikte içeren durum listesinden okuyor. Üniversitenin sunucusunda Aynur'a ait tek bir yeni kayıt oluşmuyor.

3.4 Doğrulayan da doğrulanır

Üç rollü modelde gözden kaçan bir soru vardır: Belge isteyen tarafın kim olduğunu kim kontrol ediyor? Kâğıt dünyasında bu soru pek sorulmaz; kimliğinizi bir banka gişesindeki memura uzatırken karşınızdakinin gerçekten bir banka memuru olduğunu çevrenizden anlarsınız. Dijital dünyada ise belge isteyen taraf bir web sayfası, bir QR kod ya da bir okuyucu cihazdır ve onların arkasında kimin durduğunu görmek mümkün değildir. Sahte bir "işe alım" sitesi, kimlik belgesi isteyerek insanların verilerini toplayabilir.

Bu yüzden AB'nin cüzdan mimarisinde doğrulama iki yönlüdür. Cüzdandan belge istemek isteyen kurum, önce kendi ülkesinde **kayıt** olur ve hangi belgeleri, hangi alanları, hangi amaçla isteyeceğini bildirir. Kayıt sonunda iki tür sertifika alır: kim olduğunu kanıtlayan bir **erişim sertifikası** ve neyi istemeye kayıtlı olduğunu söyleyen bir **kayıt sertifikası**. Cüzdan her istekte bu sertifikaları kontrol eder. 2026/1731 sayılı uygulama tüzüğü bu kontrolün ayrıntısını da yazmıştır: Cüzdan, istenen alanları kayıt sertifikasındaki alanlarla karşılaştırır; bir kurum kayıtlı olduğundan fazlasını istiyorsa, cüzdan herhangi bir veri paylaşılmadan önce kişiyi açıkça uyarır ve kişinin ayrıca onay vermesini ister. Sessizlik ya da önceden işaretlenmiş bir kutu onay sayılmaz [13]. Tüzük, cüzdanların kayıt sertifikasını doğrulama yükümlülüğünün 11 Ağustos 2028'den itibaren uygulanacağını da belirtir.

Bu mekanizma doğrulanabilir belgenin kendisinin bir parçası değildir, ama belgenin nasıl kullanıldığını derinden etkiler. Bir belgenin alanlarını tek tek gizleyebilmek, ancak doğrulayanın gereğinden

fazlasını istemesini sınırlayan bir kural varsa anlam kazanır. Dizinin üçüncü yazısında bu konuya seçici açıklama açısından döneceğiz.

4 Bir Doğrulanabilir Belgenin Anatomisi

Bölüm 5, 6 ve 7'de üç farklı belge biçimini inceleyeceğiz. Bu biçimler farklı kurumlarda, farklı ihtiyaçlarla ve farklı teknik geleneklerden doğdu; ilk bakışta da birbirine hiç benzemezler. Ama içlerine bakıldığında hepsinin aynı parçalardan oluştuğu görülür. Bu ortak parçaları önceden tanımak, üç biçimi okumayı çok kolaylaştırır.

İddialar. Belgenin asıl içeriği: ad, doğum tarihi, derece, bölüm. Her biçim iddiaları ad ve değer çiftleri olarak tutar, ama adların nasıl tanımlandığı biçimden biçime değişir.

Veren. Belgeyi kimin verdiğini söyleyen tanımlayıcı. Bu bir web adresi, bir sertifika ya da bir merkeziyetsiz tanımlayıcı (DID) olabilir. Doğrulayan bu tanımlayıcıdan yola çıkarak verenin açık anahtarına ulaşır.

Tür. Belgenin ne tür bir belge olduğu: kimlik bilgisi mi, diploma mı, ehliyet mi? Tür, doğrulayanın hangi iddiaları bekleyeceğini ve onları nasıl yorumlayacağını belirler. Bir türün iddialarının adlarını, değer biçimlerini ve anlamlarını tanımlayan belgeye **şema** denir.

Geçerlilik. Belgenin hangi tarihten itibaren ve hangi tarihe kadar geçerli olduğu. Bu tarih, belgenin hukuki geçerliliğiyle (örneğin ehliyetin son geçerlilik tarihi) aynı olmak zorunda değildir; dijital belge, hukuki belgeden çok daha kısa ömürlü olarak verilip düzenli olarak yenilenebilir.

Durum. Belgenin iptal edilip edilmediğini öğrenmek için bakılacak yer. Genellikle verenin yayımladığı bir durum listesine işaret eden bir adres ve listedeki bir sıra numarasıdır.

Sahip anahtarı. Belgenin bağlandığı açık anahtar. Belgeyi gösteren cüzdan, bu anahtarın gizli eşini elinde tuttuğunu her gösterimde kanıtlar (Bölüm 8).

İmza. Verenin, bütün bu parçaların üzerine attığı dijital imza.

Bu parçalar her biçimde vardır, ama üç konuda biçimler birbirinden ayrılır. Birincisi **kodlama**dır: Veri yapısı metin tabanlı JSON ile mi, yoksa ikili (binary) CBOR ile mi yazılıyor? İkincisi **imzanın nasıl bağlandığı**dır: İmza verinin içine mi yerleştiriliyor, yoksa veri imzalı bir zarfın içine mi konuyor? Üçüncüsü **anlamın nasıl tanımlandığıdır**: Alan adlarının anlamı, internetteki ortak sözlüklere bağlantılarla mı, yoksa belge türüne özel bir tanımla mı belirleniyor?

> TEKNİK AYRINTI
>
> **JSON, CBOR ve Base64URL**
>
> **JSON** (*JavaScript Object Notation*), verinin ad–değer çiftleri hâlinde, insanın da okuyabileceği metin olarak yazıldığı bir biçimdir: `{"ad": "Aynur", "derece": "Lisans"}`. Web'in ortak dilidir; hemen her programlama dili onu okuyabilir.
>
> **CBOR** (*Concise Binary Object Representation*), JSON'a benzer bir veri modelini ikili, yani bayt bayt yazılan bir biçimde kodlar [9]. Aynı veri CBOR'da genellikle daha az yer kaplar ve çok kısıtlı cihazlarda bile hızla işlenir. Bedeli, insanın doğrudan okuyamamasıdır; CBOR verisini incelemek için onu "teşhis gösterimi" (*diagnostic notation*) denen, JSON'a benzeyen bir metne çeviren araçlar kullanılır. Bu yazıdaki CBOR örnekleri bu gösterimle yazılmıştır.
>
> **Base64URL**, ikili veriyi yalnızca harf, rakam, tire ve alt çizgiden oluşan bir metne çeviren bir kodlamadır. İmzalar ve özetler ikili değerlerdir; onları bir web adresinin ya da JSON metninin içinde güvenle taşıyabilmek için bu kodlamadan geçirilir. Bir JWT'nin ilk bakışta anlamsız bir harf dizisi gibi görünmesinin nedeni budur.

İmzanın bağlanma biçimi için iki ad kullanılır. **Zarflayan imza** (*enveloping*): Veri bir zarfın içine konur, imza zarfın tamamının üzerine atılır; doğrulayan önce zarfı açar. JWT ve COSE böyle çalışır. **Gömülü imza** (*embedded*): İmza, verinin içinde ayrı bir alan olarak durur; doğrulayan imza alanını çıkarıp kalan veriyi standart bir yöntemle düzenler ve imzayı onun üzerinde kontrol eder.

5 W3C Verifiable Credentials Data Model

5.1 Kısa tarihçe

"Doğrulanabilir belge" ifadesini bir standart adına dönüştüren kurum, web'in temel standartlarını belirleyen W3C'dir (*World Wide Web Consortium*). W3C'nin Verifiable Credentials Data Model (doğrulanabilir belge veri modeli) standardının ilk sürümü Kasım 2019'da W3C önerisi (*Recommendation*) olarak yayımlandı [2]. Mart 2022'de küçük düzeltmeler içeren 1.1 sürümü geldi. Kapsamlı bir yenilemeyle hazırlanan 2.0 sürümü ise 15 Mayıs 2025'te, onu güvenceye alan iki tamamlayıcı standartla birlikte yayımlandı [1, 20].

Bu standart, dizinin ilk yazısında anlattığımız kendi kendine egemen kimlik hareketinin içinden doğdu ve o hareketin iki temel fikrini taşır: belgenin kişinin elinde bir nesne olması ve belgenin anlamının web üzerinde paylaşılan ortak sözlüklerle tanımlanması. W3C modeli bir **veri modelidir** yani belgenin hangi parçalardan oluştuğunu ve bu parçaların ne anlama geldiğini tanımlar, ama belgenin nasıl imzalanacağını tek bir yönteme bağlamaz.

5.2 Yapı

Aynur'un diplomasının W3C VC 2.0 biçiminde nasıl görünebileceğine bakalım.

TEKNİK AYRINTI

Bir W3C VC 2.0 diploması

Aşağıdaki örnek, standardın zorunlu ve yaygın alanlarını gösteriyor. Değerler örnektir; `DiplomaBelgesi` türü ve onun alanları standardın parçası sayılmaz; örnek bir eğitim sözlüğünden gelir.

JSON Örnek: W3C VC 2.0 biçiminde bir diploma

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://egitim.example/sozluk/v1"
  ],
  "type": ["VerifiableCredential", "DiplomaBelgesi"],
  "issuer": "https://universite.example.az",
  "validFrom": "2026-06-30T00:00:00Z",
  "credentialSubject": {
    "id": "did:jwk:eyJrdHkiOiJFQyIsImNydiI6IlAtMjU2Ii…",
    "ad": "Aynur",
    "derece": "Lisans",
    "bolum": "Bilgisayar Mühendisliği",
    "mezuniyetTarihi": "2026-06-30"
  },
  "credentialStatus": {
    "type": "BitstringStatusListEntry",
    "statusPurpose": "revocation",
    "statusListIndex": "94567",
    "statusListCredential": "https://universite.example.az/durum/3"
  }
}
```

- `@context` : Belgedeki adların hangi sözlüklere göre yorumlanacağı. İlk öğe her zaman standardın kendi sözlüğüdür; sonrakiler belge türüne özel sözlüklerdir.
- `type` : Belgenin türü. `VerifiableCredential` zorunludur; yanına belgenin özel türü eklenir.
- `issuer` : Veren. Bir web adresi ya da DID olabilir.
- `validFrom` ve isteğe bağlı `validUntil` : Geçerlilik aralığı.

- `credentialSubject`: Belgenin kim hakkında olduğu ve iddiaları. İçindeki `id`, özneyi tanımlar; burada Aynur'un cüzdanındaki bir anahtardan türetilmiş bir DID kullanıldı.
- `credentialStatus`: İptal durumunun nereden öğrenileceği.

Bu belge henüz **imzasız**dır. Standarda göre onu doğrulanabilir yapan, Bölüm 5.3'te anlatılan güvenceleme yöntemlerinden biridir.

`@context` alanı W3C modelinin en ayırt edici özelliğidir ve biraz açıklamayı hak eder. W3C modeli, JSON-LD (*JSON for Linked Data*) adı verilen bir yönteme dayanır. Bu yöntemde belgedeki her alan adı, aslında internette tanımlı bir kavramın kısaltmasıdır. Örneğin `derece` alanı, örnek eğitim sözlüğünde "bir yükseköğretim kurumunun verdiği akademik unvan" diye tanımlanmış bir kavrama karşılık gelir. Böylece iki farklı kurum, farklı dillerde farklı adlar kullansa bile aynı kavrama işaret edebilir. Bu, özellikle eğitim gibi, binlerce kurumun ortak bir anlam üzerinde anlaşmak zorunda olduğu alanlar için güçlü bir özelliktir. Avrupa Birliği'nin eğitim belgeleri için geliştirdiği Avrupa Öğrenme Modeli ve büyük ölçekli pilotlardan biri olan DC4EU'nun eğitim çalışmaları da bu yüzden W3C modelini esas almıştır.

Aynı özelliğin bir bedeli de vardır. JSON-LD ile yazılmış bir belgeyi tam olarak yorumlamak ve gömülü imzayla doğrulamak, belgenin standart bir biçime getirilmesini (*canonicalization*) ve sözlüklerin çözülmesini gerektirir. Bu işlemler karmaşıktır, hata yapmaya açıktır ve sözlüklerin internetten çekilmesi gerekiyorsa doğrulamayı ağ bağlantısına ve sözlüğü yayımlayan sunucuya bağımlı kılar. Uygulamada doğrulayıcılar bu sözlükleri önceden yükleyip saklar.

5.3 Güvenceleme: imza nereye konur?

W3C VC 2.0, belgeyi imzalamanın iki ailesini tanır [1, 20].

Gömülü kanıt (*embedded proof*) yönteminde imza, belgenin içine `proof` adlı bir alan olarak eklenir. W3C'nin "Verifiable Credential Data Integrity" standardı bu yöntemi tanımlar ve imzanın hangi algoritmayla, hangi düzenleme yöntemiyle üretileceğini **şifre takımı** (*cryptosuite*) adı verilen paketlerle belirler. Örneğin eliptik eğri imzalarını kullanan takımlar ve dizinin üçüncü yazısında anlatacağımız BBS imzalarını kullanan bir takım bu ailededir.

Zarflayan kanıt (*enveloping proof*) yönteminde ise belge olduğu gibi bir zarfın içine konur ve zarf imzalanır. W3C'nin "Securing Verifiable Credentials using JOSE and COSE" standardı, belgeyi bir JWT'nin, bir SD-JWT'nin ya da bir COSE yapısının içine koymayı tanımlar. Bu yöntemde JSON-LD düzenlemesine gerek kalmaz; imza, belgenin baytları üzerindedir.

Bu ikilik, W3C modelinin hem esnekliği hem de karmaşıklığıdır. "W3C VC destekliyorum" diyen iki sistemin birbiriyle konuşabilmesi için, aynı veri modelinin yanında aynı güvenceleme yöntemini ve aynı şifre takımını da seçmiş olmaları gerekir.

5.4 Sunum

W3C modeli bir belgenin doğrulayana nasıl gösterildiğini de tanımlar. Sahip, bir ya da birkaç belgeyi **doğrulanabilir sunum** (*verifiable presentation*) adı verilen bir yapıya koyar ve bu sunumu kendi anahtarıyla imzalar. Sunumun içinde, doğrulayanın gönderdiği tek kullanımlık bir değer (*challenge* ya da *nonce*) ve sunumun hangi doğrulayan için hazırlandığı da bulunur. Böylece doğrulayan iki şeyi birlikte kontrol eder: içerideki belgelerin veren tarafından imzalandığını ve sunumu hazırlayanın, belgelerin bağlandığı anahtarı elinde tuttuğunu. Bu, Bölüm 8'de anlatacağımız sahip bağlamanın W3C modelindeki karşılığıdır.

5.5 Verenin anahtarı nerede?

W3C modelinde `issuer` alanı bir web adresi ya da bir DID olabilir. Doğrulayan, verenin açık anahtarını bu tanımlayıcıdan yola çıkarak bulur. DID kullanılıyorsa tanımlayıcı "çözülür" ve ortaya çıkan DID

belgesinden anahtar okunur; dizinin ilk yazısında anlattığımız gibi, bu belgenin nerede durduğu DID yöntemine göre değişir. Örneğin `did:web` yönteminde DID belgesi, verenin kendi alan adındaki bir web sunucusunda yayımlanır.

Bu esneklik bir soruyu da beraberinde getirir. Doğrulayan anahtarı her doğrulamada verenin sunucusundan çekiyorsa, Bölüm 3.3'teki eve telefon etme sorunu farklı bir kapıdan geri döner: Veren, belgesinin doğrulandığını tam olarak bilmese de, anahtarının ne zaman, hangi adresten istendiğini görebilir. Bu yüzden iyi tasarlanmış sistemlerde doğrulayıcılar anahtarları önbellekte tutar ya da güven listesi gibi toplu kaynaklardan alır. Tanımlayıcının bir DID olması, "bu DID gerçekten Bakü'deki üniversitenin mi?" sorusunu da tek başına cevaplamaz; bu soru, hangi biçim kullanılırsa kullanılsın, bir güven altyapısına gider.

> ÖRNEK
>
> **Aynur'un diploması W3C modelinde**
>
> Aynur'un üniversitesi, ulusal eğitim belgeleri ağının ortak sözlüğünü kullanarak diplomayı W3C VC 2.0 biçiminde verir ve SD-JWT ile zarflar. İstanbul'daki şirketin başvuru sistemi aynı sözlüğü tanıdığı için `derece` alanının bir lisans derecesini, `bolum` alanının da bir öğretim programını gösterdiğini anlar ve diplomayı adayın profilindeki uygun kutulara kendiliğinden yerleştirir. Aynı diploma bir Avrupa üniversitesinin yüksek lisans başvuru sistemine gösterildiğinde de, o sistem aynı sözlüğü kullandığı sürece bir çeviriye gerek kalmaz. W3C modelinin eğitim dünyasında güçlü olmasının nedeni, belgeden çok bu ortak sözlüklerdir.

6 SD-JWT VC: Seçici Açıklamalı JSON Belgesi

6.1 JWT'den SD-JWT'ye

Dizinin ilk yazısında "Google ile giriş" düğmesinin arkasında dönen kimlik belirtecini, yani JSON Web Token'ı (JWT) [7] incelemiştik. JWT basit ve yaygın bir yapıdır: bir başlık, bir içerik ve bir imza, aralarında noktalarla. Web'deki neredeyse her sistem JWT üretip doğrulayabilir. Doğrulanabilir belge için JWT'yi kullanmak bu yüzden cazip bir fikirdi.

Ama JWT'nin belge olarak kullanılmasının önünde bir engel vardı. Bir JWT'nin imzası içeriğin tamamını kapsar; içerikten tek bir alanı çıkarırsanız imza bozulur. Federasyonda bu bir sorun değildi, çünkü kimlik sağlayıcı her giriş için o siteye özel, yalnız gereken alanları içeren yeni bir belirteç üretiyordu. Ama kişinin elinde duran ve yıllarca farklı yerlere gösterilecek bir belge için bu kabul edilemez: Aynur ehliyetini yalnızca yaşını kanıtlamak için gösterdiğinde, adresini de göstermek zorunda kalmamalıdır.

IETF'in OAuth çalışma grubu bu sorunu çözmek için **SD-JWT** (*Selective Disclosure for JWTs*, seçici açıklamalı JWT) adlı bir yöntem geliştirdi. Fikir şudur: Veren, gizlenebilecek her alan için yalnızca o alanın **tuzlanmış bir özetini** imzalar. Alanların kendileri imzanın dışında, ayrı parçalar olarak kişiye verilir. Kişi bir doğrulayana yalnızca göstermek istediği alanların parçalarını verir; doğrulayan bu parçaların özetini hesaplar ve imzalı listede bulur. Yöntemin bütün ayrıntısı, adım adım hesaplarıyla birlikte, dizinin üçüncü yazısının konusu. SD-JWT, Kasım 2025'te IETF'in RFC 9901 numaralı standardı olarak yayımlandı [3].

SD-JWT genel bir yöntemdir: Herhangi bir JWT'yi seçici açıklamalı hâle getirir. **SD-JWT VC** ise bu yöntemi doğrulanabilir belgeler için kullanmanın kurallarını koyan ayrı bir IETF belgesidir [4]: Belgenin türü nasıl belirtilir, veren nasıl tanımlanır, sahibin anahtarı nereye yazılır, hangi alanlar her zaman açık kalmak zorundadır. Bu yazının yazıldığı Kasım 2026 itibarıyla SD-JWT VC, IETF'te yayın öncesi son inceleme aşamasındadır (6 Kasım 2026 tarihli 26. taslak).

6.2 Yapı

Bir SD-JWT VC'nin içeriğine, Avrupa Birliği'nin kişi kimlik verisi (PID) için tanımladığı alan adlarıyla bakalım.

TEKNİK AYRINTI

Bir SD-JWT VC kimlik belgesinin imzalı içeriği

Verenin imzaladığı JWT iki parçadan oluşur. Önce hangi algoritmayla imzalandığını söyleyen başlık gelir:

JSON Örnek: JWT başlığı

```
{ "alg": "ES256", "typ": "dc+sd-jwt", "x5c": ["MIIC…"] }
```

Sonra asıl bilgiyi taşıyan içerik (değerler örnektir; özetler kısaltıldı):

JSON Örnek: imzalı içerik (PID alanları gizli, yalnızca özetleri var)

```
{
  "iss": "https://pid.example.az",
  "vct": "urn:eudi:pid:1",
  "iat": 1793606400,
  "nbf": 1793606400,
  "exp": 1801382400,
  "_sd_alg": "sha-256",
  "_sd": [
    "022jpYd1uSsyCIWiJRDeYYaF0nCKxp75v0fgum7ZZ9E",
    "OeH1--ehivaXNs5kBlsDPpD3JeQEu-XXHiRevIUdnac",
    "PjFFF-Lc218Ug-IP53G9NMRRb_2c_r2WraLn4mip1pY",
    "pTFbYDVDTkHXcfRPACRNCEd9pDAV3n56yJjuO6vYn-8",
    "…"
  ],
  "cnf": { "jwk": { "kty": "EC", "crv": "P-256", "x": "RyZ4…", "y": "rM9h…" } },
  "status": { "status_list": { "idx": 41207, "uri": "https://pid.example.az/durum/12" } }
}
```

- Başlıktaki `typ` değeri `dc+sd-jwt`, bu yapının bir SD-JWT VC olduğunu söyler ("dc", *digital credential* kısaltması). `x5c`, verenin sertifikasını taşır; doğrulayan bu sertifikayı güven listesine bağlar.
- `vct` (*verifiable credential type*): Belgenin türü. AB, kişi kimlik verisinin temel türünü `urn:eudi:pid:1` olarak belirlemiştir [13].
- `iat`, `nbf`, `exp`: Belgenin verildiği an, geçerli olmaya başladığı an ve geçerliliğinin bittiği an (saniye cinsinden zaman damgaları).
- `_sd`: Gizlenebilir alanların tuzlanmış özetleri. Ad, soyad, doğum tarihi ve uyruk burada **açık olarak yazmaz** yalnızca özetleri vardır. Listede gerçek alanlardan fazla özet bulunabilir; bunlar alan sayısını gizlemek için eklenen sahte özetlerdir.
- `cnf` (*confirmation*): Belgenin bağlandığı sahip anahtarı [8]. Bölüm 8'de bu alana döneceğiz.
- `status`: Durum listesinin adresi ve bu belgenin listedeki sırası (dizinin yedinci yazısı).

Alanların kendileri, imzalı içeriğin dışında, **açıklama** (*disclosure*) adı verilen küçük parçalar olarak cüzdana verilir. Örneğin doğum tarihinin açıklaması, `["eI8ZWm9QnKPpNPeNenHdhQ", "birthdate", "2001-03-14"]` dizisinin Base64URL ile kodlanmış hâlidir; dizinin ilk öğesi rastgele bir tuzdur.

SD-JWT VC'nin bir özelliği dikkat çekicidir: Belgenin anlamını tanımlamak için JSON-LD gibi ayrı bir mekanizmaya başvurmaz. Alan adları ya JWT dünyasında zaten kayıtlı olan ortak adlardır (`given_name`, `family_name`, `birthdate`) ya da belge türüne özel tanımlanır. `vct` değeri bir web adresi olarak yazılırsa, o adreste türün açıklaması, şeması ve cüzdanda nasıl gösterileceğine dair bilgiler (*type metadata*) yayımlanabilir. Doğrulayıcı için bu yapı sadedir: Belgeyi anlamak için bir JSON okuyucusu ve bir JWT kütüphanesi yeterlidir.

6.3 Sunum

SD-JWT VC'nin sunumu, birbirine tilde (`~`) işaretiyle eklenmiş parçalardan oluşan tek bir metindir:

TEXT Biçim: SD-JWT VC sunumunun parçaları

```
<verenin imzaladığı JWT>~<açıklama 1>~<açıklama 2>~…~<sahip bağlama JWT'si>
```

Aynur doğum tarihini ve uyruğunu göstermek istiyorsa, verenin imzaladığı JWT'nin arkasına yalnız bu iki alanın açıklamalarını ekler; adı ve soyadı göstermek istemiyorsa onların açıklamalarını eklemez. En sona da, doğrulayanın gönderdiği tek kullanımlık değeri kendi anahtarıyla imzaladığı küçük bir JWT ekler. Bu son parça, belgenin sahibine bağlı olduğunun kanıtıdır ve Bölüm 8'de ayrıntılı anlatılıyor.

ÖNEMLİ

SD-JWT VC'yi akılda tutmanın kısa yolu

SD-JWT VC, web'in en tanıdık imzalı veri yapısı olan JWT'ye iki şey ekler: alanların tek tek gizlenebilmesi ve belgenin sahibinin anahtarına bağlanması. JSON bilen her yazılımcının kısa sürede okuyabileceği kadar sadedir; bu sadelik, onu AB cüzdanının çevrimiçi kullanımda ana biçimlerinden biri yapmıştır.

7 ISO/IEC 18013-5: Mobil Belge (mdoc)

7.1 Mobil ehliyetin doğuşu

Üçüncü biçim, ne web dünyasından ne de kendi kendine egemen kimlik hareketinden doğdu. Kökeni, ehliyet ve pasaport gibi devletin verdiği kimlik belgelerini standartlaştıran ISO/IEC'nin ortak komitesindeki çalışmalardır. Bu komite, plastik sürücü belgesinin ISO 18013 adlı standart ailesini zaten yönetiyordu. Akıllı telefonların yaygınlaşmasıyla aynı ailenin beşinci parçası olarak **mobil sürücü belgesi** (*mobile driving licence, mDL*) tanımlandı. ISO/IEC 18013-5 standardı Eylül 2021'de yayımlandı [5]. Ekim 2024'te yayımlanan ISO/IEC TS 18013-7 ise aynı belgenin internet üzerinden, yani uzaktan gösterilmesini tanımladı [6].

Standardın adında ehliyet geçse de tanımladığı veri yapısı yalnız ehliyete özgü değildir. Bu yapıya genel olarak **mobil belge** (*mobile document*, kısaca **mdoc**) denir ve herhangi bir belge türünü taşıyabilir. Avrupa Birliği, kişi kimlik verisinin mdoc biçimini `eu.europa.ec.eudi.pid.1` belge türüyle tanımlamıştır [13]. Amerika Birleşik Devletleri'nde birçok eyalet, mobil ehliyetlerini bu standarda göre vermeye başlamıştır.

mdoc'un tasarımında iki öncelik öne çıkar. Birincisi **yüz yüze kullanımdır**: Bir polis memurunun yol kenarında, bir market kasiyerinin kasada, bir havalimanı görevlisinin kontrol noktasında, çoğu zaman internet bağlantısı olmadan, telefondan belgeyi okuyabilmesi. İkincisi **kısıtlı cihazlarda verimliliktir**: Veri küçük olmalı ve Bluetooth ya da NFC gibi yavaş kanallarda hızla aktarılabilmelidir. Bu iki öncelik, metin tabanlı JSON yerine ikili CBOR kodlamasını ve JWT yerine COSE imzalarını (*CBOR Object Signing and Encryption*) [10] seçmeyi doğal kılmıştır.

7.2 Yapı: alan alan imzalanan veri

mdoc'un iç yapısı, Bölüm 2.3'teki tarihçe kutusunda anlattığımız elektronik pasaportun güvenlik nesnesine çok benzer. Veren, her veri alanını ayrı bir küçük paket olarak hazırlar. Her paketin içinde alanın adı, değeri, bir sıra numarası ve rastgele bir değer (tuz) bulunur. Veren bu paketlerin her birinin özetini hesaplar ve bütün özetleri tek bir yapıda toplar. Bu yapıya **mobil güvenlik nesnesi** (*Mobile Security Object, MSO*) denir. Veren yalnızca MSO'yu imzalar; alanların kendileri imzanın dışında durur.

TEKNİK AYRINTI

mdoc'un iç yapısı (CBOR teşhis gösterimiyle)

Her alan, `IssuerSignedItem` adlı bir pakete konur. Paketin kendisi CBOR olarak kodlanır ve 24 numaralı CBOR etiketiyle ("içinde kodlanmış CBOR var") sarılır. Değerler örnektir:

TEXT Örnek: doğum tarihi alanının paketi (IssuerSignedItem)

```
24(<< {
  "digestID": 3,
  "random": h'8D1F0C7A…C2A9',
  "elementIdentifier": "birth_date",
  "elementValue": 1004("2001-03-14")
} >>)
```

Veren bu paketin baytlarının SHA-256 özetini alır ve MSO'ya yazar. MSO'nun kendisi şöyle bir yapıdır:

TEXT Örnek: veren kurumun imzaladığı MSO

```
{
  "version": "1.0",
  "digestAlgorithm": "SHA-256",
  "docType": "eu.europa.ec.eudi.pid.1",
  "valueDigests": {
    "eu.europa.ec.eudi.pid.1": {
      0: h'75167333…', 1: h'67E539D6…', 2: h'3394372D…', 3: h'2E35AD3C…'
    }
  },
  "deviceKeyInfo": { "deviceKey": { 1: 2, -1: 1, -2: h'…', -3: h'…' } },
  "validityInfo": {
    "signed": 0("2026-11-02T09:00:00Z"),
    "validFrom": 0("2026-11-02T09:00:00Z"),
    "validUntil": 0("2027-02-02T09:00:00Z")
  }
}
```

- `docType` belgenin türünü, `valueDigests` içindeki ad alanı (*namespace*) alanların hangi sözlüğe ait olduğunu söyler. Ulusal ek alanlar ayrı bir ad alanında tutulabilir.
- `valueDigests` , sıra numarası ile özet arasındaki eşlemedir. 3 numaralı özet, yukarıdaki doğum tarihi paketinin özetidir.
- `deviceKeyInfo` , belgenin bağlandığı cihaz anahtarıdır; COSE anahtar biçiminde yazılır (1: 2 eliptik eğri anahtarı, −1: 1 P-256 eğrisi, −2 ve −3 açık anahtarın koordinatları).
- `validityInfo` , belgenin imzalandığı anı ve geçerlilik aralığını verir.

MSO da CBOR olarak kodlanır ve bir **COSE_Sign1** yapısının içine konup verenin anahtarıyla imzalanır. COSE_Sign1'in başlığında verenin sertifikası (`x5chain`) taşınır. Mobil ehliyette bu sertifika, ehliyeti veren makamın kök sertifikasına bağlanır.

Doğrulayan bir alanı aldığında, o alanın paketinin özetini hesaplar ve imzalı MSO'daki listede aynı sıra numarasının karşısındaki özetle karşılaştırır. Eşleşiyorsa alan, verenin imzaladığı alandır. Gösterilmeyen alanların yalnızca özetleri MSO'da kalır; bu özetlerden alanların değeri geri hesaplanamaz, çünkü her paketin içinde tahmin edilemeyen bir tuz vardır.

Bu yapının ilginç bir sonucu var: mdoc'ta seçici açıklama sonradan eklenmiş bir özellik sayılmaz, doğrudan tasarımdan gelir. Her alan baştan ayrı paketlenmiştir; bir alanı göstermek, yalnızca o paketi göndermek demektir. SD-JWT'deki tuzlu özet fikri ile mdoc'taki MSO fikri aynı aileden gelir ve dizinin üçüncü yazısında ikisini yan yana inceleyeceğiz.

7.3 Yüz yüze ve uzaktan gösterim

mdoc'un gösterimi, belgenin yapısından daha karmaşıktır, çünkü standart iki cihazın birbirini hiç tanımadan, çoğu zaman internet olmadan güvenli bir bağlantı kurmasını tanımlar. Kabaca şöyle işler: Aynur'un telefonu bir QR kod gösterir ya da NFC ile okuyucuya dokundurulur; bu ilk temasta iki cihaz geçici anahtarlar değiş tokuş eder ve bir şifreli oturum kurar. Okuyucu bu oturum üzerinden hangi alanları istediğini bildirir ve gerekirse kendi kimliğini de kanıtlar. Aynur'un telefonu ona isteği gösterir,

Aynur onaylar, telefon yalnızca istenen alanların paketlerini, imzalı MSO'yu ve bu oturuma özel bir sahip imzasını gönderir. Bütün bu konuşmanın ayrıntıları dizinin dokuzuncu yazısının konusu.

Uzaktan gösterimde ise, yani Aynur bir web sitesine belgesini gösterdiğinde, aynı yapı OpenID4VP protokolü ya da tarayıcıların yeni Digital Credentials arayüzü üzerinden taşınır. Veri yapısı değişmez; değişen, iki tarafın birbirine nasıl ulaştığıdır.

> ÖRNEK
>
> **Aynur ehliyetini gösteriyor**
>
> Aynur, İstanbul'da bir araç kiralama ofisinde. Görevli tezgâhtaki okuyucuyu gösteriyor; Aynur telefonunu okuyucuya yaklaştırıyor. Telefonun ekranında "Bu okuyucu ehliyet sınıfınızı, ehliyetin geçerlilik tarihini, adınızı ve fotoğrafınızı istiyor" yazıyor. Adresini ve doğum yerini istemiyor; zaten istese bile Aynur onları ayrı ayrı reddedebilir. Aynur onaylıyor. Okuyucu imzalı MSO'yu ehliyeti veren makamın sertifikasıyla doğruluyor, gelen dört alanın özetini MSO'daki özetlerle karşılaştırıyor ve telefonun bu oturum için attığı imzayı, MSO'daki cihaz anahtarıyla kontrol ediyor. Ofisin internet bağlantısı o sırada kesik olsa bile bütün bu işlem tamamlanabiliyor.

7.4 Verenin sertifikası nereden gelir?

mdoc'ta doğrulayanın verenin açık anahtarına ulaşma yolu, web'deki sertifika düzenine benzer ama daha kapalıdır. Her veren makamın bir **kök sertifikası** vardır; mobil ehliyet dünyasında buna verenin kök sertifika otoritesi denir. Bu kök, günlük imza işlerinde kullanılmaz; yalnızca belge imzalayan sertifikaları onaylar. Belgeleri imzalayan anahtar ise kısa ömürlü bir **belge imzalayan sertifikası** taşır ve bu sertifika her mdoc'un imzasının yanında gönderilir. Doğrulayan, belge imzalayan sertifikanın güvendiği bir köke zincirlendiğini kontrol eder.

Bu düzenin bir sonucu, doğrulayanın hangi köklere güveneceğini önceden bilmesi gerektiğidir. Elektronik pasaportta bu iş için ICAO'nun ülkelerin sertifikalarını topladığı ortak bir dizin vardır. Mobil ehliyette Amerika'daki eyaletlerin kök sertifikaları için benzer bir ortak liste işletilir. AB cüzdanında ise bu rolü, üye devletlerin ve Komisyon'un yayımladığı güven listeleri üstlenir. Bu, Tablo 1'deki "o anahtar kime ait?" sorusunun mdoc dünyasındaki cevabıdır ve hangi biçim kullanılırsa kullanılsın, güvenin sonunda bir listeye, o listenin de bir kuruma dayandığını gösterir. Güven listelerinin yapısı ve yönetimi dizinin altıncı yazısında ayrıntılı ele alınıyor.

8 Sahip Bağlama: Belge Neden Bir Anahtara Bağlanır?

8.1 Kopyalanan belge sorunu

Bölüm 2'deki imza tartışmasında bir noktayı açıkta bırakmıştık. Dijital imza bir belgenin değiştirilmediğini kanıtlar; ama dijital bir belgenin **kopyalanmasını** engellemez. Aynur'un diploması bir dosyaysa, o dosyanın bir kopyası da aynı imzayı taşır ve aynı ölçüde "geçerlidir". Aynur'un telefonuna sızan biri, ya da Aynur'un belgeyi gösterdiği kötü niyetli bir doğrulayan, belgeyi kopyalayıp başka bir yerde Aynur'muş gibi gösterebilir.

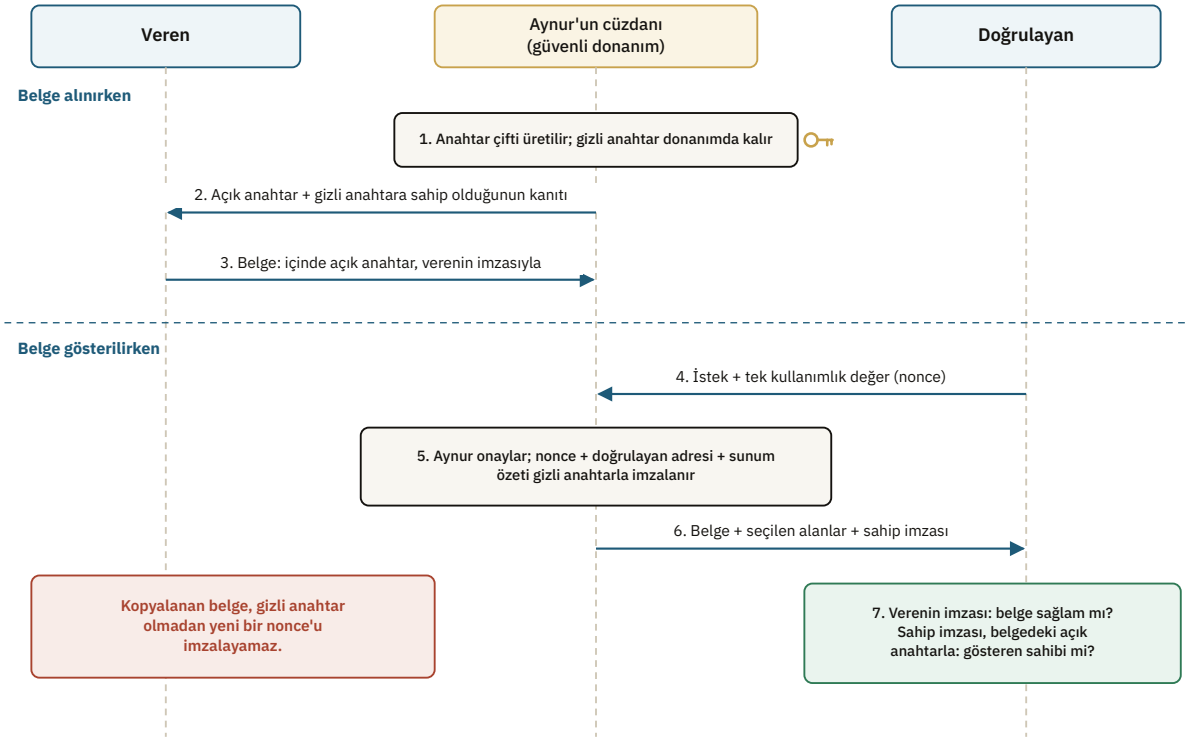
Fiziksel dünyada bu sorunun çözümü belgenin üzerindeki fotoğraftır. Bir banka memuru kimlik kartının gerçek olduğunu hologramdan, kartın size ait olduğunu fotoğraftan anlar. Dijital dünyada bunun karşılığı **sahip bağlama**dır (*holder binding*): Belge, yalnızca sahibinin elinde olan bir şeye bağlanır ve her gösterimde o şeyin elde olduğu kanıtlanır.

8.2 Anahtar bağlama nasıl çalışır?

En yaygın sahip bağlama yöntemi, belgenin bir **anahtar çiftine** bağlanmasıdır. Akış şöyledir (Şekil 5):

1. **Belge alınırken.** Aynur'un cüzdanı, telefonunun güvenli donanımında yeni bir anahtar çifti üretir. Gizli anahtar donanımdan hiç çıkmaz. Cüzdan açık anahtarı verene gönderir ve gizli anahtarı elinde tuttuğunu, verenin gönderdiği bir değeri imzalayarak kanıtlar.
2. **Belge imzalanırken.** Veren, bu açık anahtarı belgenin içine yazar ve belgeyi öyle imzalar. SD-JWT VC'de bu, `cnf` alanıdır; mdoc'ta MSO'daki `deviceKeyInfo` alanı; W3C modelinde genellikle `credentialSubject.id` alanındaki tanımlayıcı.
3. **Belge gösterilirken.** Doğrulayan, isteğiyle birlikte tek kullanımlık, tahmin edilemeyen bir değer gönderir (*nonce*). Cüzdan, bu değeri ve doğrulayanın kimliğini içeren küçük bir yapıyı gizli anahtarıyla imzalar ve belgeyle birlikte gönderir.
4. **Doğrulanırken.** Doğrulayan, belgenin içindeki açık anahtarla bu imzayı kontrol eder. İmza tutuyorsa, belgeyi gösteren taraf, belgenin bağlandığı gizli anahtarı **şu anda** elinde tutuyordur.

Tek kullanımlık değerin önemi büyüktür. Eğer doğrulayan her seferinde yeni bir değer göndermeseydi, Aynur'un bir kez gösterdiği bir sunumu kaydeden kötü niyetli bir doğrulayan, aynı sunumu başka bir yerde **tekrar oynatabilirdi** (*replay*). Sunumun içinde doğrulayanın kimliğinin bulunması da benzer bir saldırıyı engeller: Bir doğrulayan için hazırlanmış bir sunum, başka bir doğrulayana götürülürse reddedilir.



Şekil 5. Sahip bağlama: belge bir anahtara bağlanır, her gösterimde o anahtarın elde olduğu kanıtlanır

TEKNİK AYRINTI

SD-JWT VC'de sahip bağlama JWT'si

SD-JWT VC sunumunun son parçası, cüzdanın imzaladığı küçük bir JWT'dir (*Key Binding JWT*). Başlığındaki `typ` değeri `kb+jwt`'dir. İçeriği dört alandan oluşur (değerler örnektir):

JSON Örnek: sahip bağlama JWT'sinin içeriği

```json
{
  "iat": 1794470400,
  "aud": "https://insankaynaklari.example",
  "nonce": "XZOUco1u_gEPknxS78sWWg",
  "sd_hash": "XqVtZy8NJutyLDb_vMSsQUKhNZIwrg7W6IQCwhClvlg"
}
```

- `aud` : Sunumun hangi doğrulayan için hazırlandığı.
- `nonce` : Doğrulayanın bu işlem için gönderdiği tek kullanımlık değer.
- `sd_hash` : Sunumun geri kalanının, yani verenin JWT'si ile Aynur'un seçtiği açıklamaların özeti. Bu alan sayesinde sahip imzası, **hangi alanların** gösterildiğini de kapsar; yolda biri bir açıklamayı ekleyip çıkaramaz.

Doğrulayan bu JWT'nin imzasını, verenin imzaladığı içerikteki `cnf` anahtarıyla kontrol eder [3, 4]. mdoc'ta aynı işi `DeviceAuth` adlı yapı görür: Cüzdan, iki cihazın kurduğu oturuma özgü bir veriyi (*SessionTranscript*) MSO'daki cihaz anahtarıyla imzalar. Fikir aynıdır; yalnızca kodlama farklıdır.

8.3 Anahtar nerede durur?

Sahip bağlama, gizli anahtarın gerçekten kopyalanamaz olmasına dayanır. Anahtar telefonun sıradan belleğinde bir dosya olarak dursaydı, telefona sızan bir zararlı yazılım onu belgeyle birlikte kopyalayabilir ve bağlama anlamını yitirirdi. Bu yüzden yüksek güvence gerektiren belgelerde anahtar, telefonun **güvenli donanımında** üretilir ve orada kalır. Bu donanım, anahtarı dışarı vermeden onunla imza atabilen, ayrı bir küçük işlemcidir; imza için kullanıcıdan PIN ya da biyometrik doğrulama isteyebilir. AB cüzdanında belge veren kurum, anahtarın gerçekten böyle bir donanımda saklandığını, cüzdan sağlayıcının imzaladığı bir **anahtar kanıtı** ile öğrenir. Güvenli donanımın türleri, uzaktan güvenli donanım ve cüzdan kanıtları dizinin onuncu yazısında anlatılıyor.

Her belgenin bir cihaza bağlanması gerekmez. Bazı belgeler doğası gereği kişiye değil bir nesneye ya da bir duruma aittir (örneğin bir bilet ya da bir ürün sertifikası); bazılarında ise bağlama başka bir belge üzerinden kurulur. AB'nin 2026/1731 sayılı uygulama tüzüğü de "cihaza bağlı olmayan" öznitelik onaylarının varlığını kabul eder ve bunlar için anahtar kanıtı kullanılmamasını öngörür [13]. Ama kişi kimlik verisi ve kişiye özgü önemli belgeler için cihaz bağlama esastır.

8.4 Başka bağlama yolları

Anahtar bağlamanın yanında iki yöntem daha anılmaya değer. **Biyometrik bağlama**da belgenin içinde kişinin fotoğrafı bulunur; yüz yüze gösterimde görevli, tıpkı kâğıt kimlikte olduğu gibi fotoğrafla kişiyi karşılaştırır. Mobil ehliyet bu yöntemi anahtar bağlamayla birlikte kullanır. AB de kişi kimlik verisinde fotoğrafı bir alan olarak tanımlamış, fotoğrafın paylaşılmasını ise kişinin ayrıca ve açıkça onay vermesine bağlamıştır [13]. **İddia tabanlı bağlama**da ise bir belge, başka bir belgedeki bir iddiaya bağlanır: Örneğin bir diploma, Aynur'un kimlik belgesindeki ad, soyad ve doğum tarihiyle eşleşmesi beklenen alanlar taşır ve doğrulayan ikisini birlikte ister. Bu yöntem kolaydır ama her iki belgenin de gösterilmesini, dolayısıyla daha fazla veri paylaşılmasını gerektirir.

ÖNEMLİ

Bu bölümden akılda kalması gereken

İmza belgenin değişmediğini kanıtlar ama kopyalanmasını engellemez. Sahip bağlama, belgeyi kişinin cihazındaki bir gizli anahtara bağlar ve her gösterimde, doğrulayanın gönderdiği tek kullanımlık bir değeri o anahtarla imzalatır. Kopyalanan belge, anahtar olmadan yeni bir değeri imzalayamaz. Bağlamanın gücü, anahtarın gerçekten kopyalanamaz bir donanımda durmasına bağlıdır.

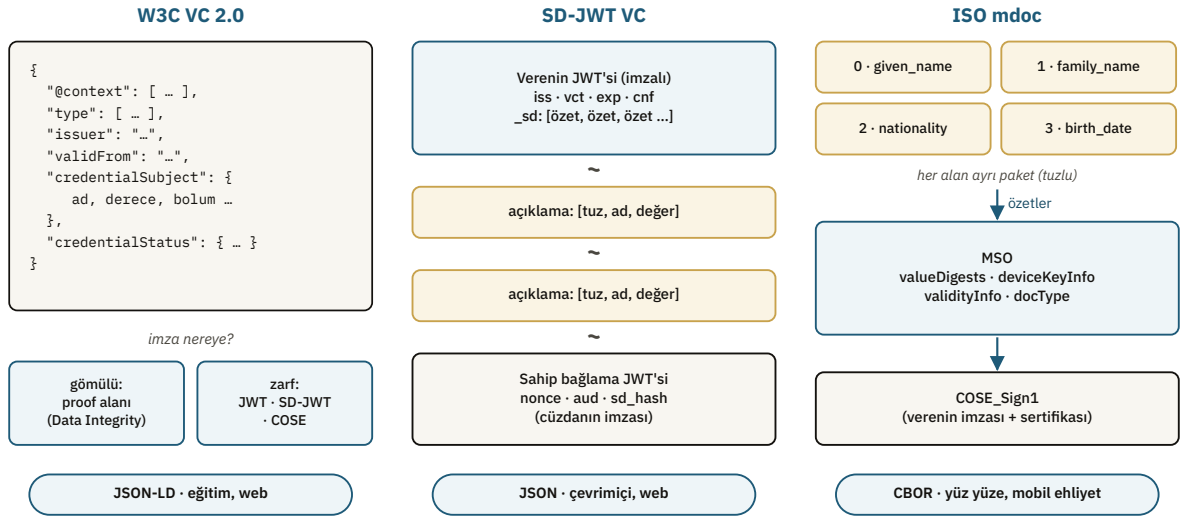
9 Biçimlerin Karşılaştırması ve AB'nin Seçimi

9.1 Üç biçim yan yana

Üç biçimi tanıdıktan sonra onları yan yana koyabiliriz (Şekil 6 ve Tablo 2). Karşılaştırmayı okurken bir noktayı akılda tutmak gerekir: Bu biçimler farklı ihtiyaçlar için ortaya çıktı ve aynı cüzdan çoğu zaman birden fazlasını birlikte destekler.

Tablo 2. Üç doğrulanabilir belge biçiminin karşılaştırması.

Ölçüt	W3C VC 2.0	SD-JWT VC	ISO mdoc (18013-5)
Yayımlayan	W3C	IETF	ISO/IEC
Durum (Kasım 2026)	W3C önerisi (Mayıs 2025)	RFC 9901 + SD-JWT VC son taslak aşamasında	uluslararası standart (2021); uzaktan gösterim TS 18013-7 (ilk baskı 2024, ikinci baskı 2025)
Kodlama	JSON-LD (JSON)	JSON	CBOR (ikili)
İmza	gömülü (Data Integrity) ya da zarflayan (JOSE/COSE)	zarflayan (JWS)	zarflayan (COSE_Sign1)
Anlamın tanımı	internetteki ortak sözlükler (`@context`)	tür tanımlayıcısı (`vct`) ve tür bilgisi	belge türü (`docType`) ve ad alanları
Seçici açıklama	güvenceleme yöntemine bağlı (SD-JWT ya da BBS ile)	yerleşik (tuzlu özetler)	yerleşik (MSO özetleri)
Sahip bağlama	sunumun imzalanması	`cnf` + sahip bağlama JWT'si	`deviceKeyInfo` + `DeviceAuth`
Yüz yüze kullanım	tanımlı değil	tanımlı değil	yerleşik (QR, NFC, BLE)
Güçlü yanı	anlamsal zenginlik, eğitim ekosistemi	sadelik, web araçlarıyla uyum	çevrimdışı ve kısıtlı cihazlarda verimlilik
Zayıf yanı	seçeneklerin çokluğu, düzenleme karmaşıklığı	yüz yüze profil yok	ikili biçim, standart metni ücretli



Şekil 6. Üç belge biçiminin iç yapısı yan yana

9.2 AB'nin seçimi: PID ve EAA

Avrupa Birliği'nin cüzdan mimarisinde iki tür belge vardır ve dizinin ilk yazısında ikisini de tanıtmıştık. **Kişi kimlik verisi** (*Person Identification Data*, PID), devletin ya da devletin yetkilendirdiği kurumun verdiği temel kimlik bilgisidir. **Öznitelik onayları** (*Electronic Attestations of Attributes*, EAA) ise diploma, ehliyet, meslek belgesi gibi diğer bütün belgelerdir.

PID için AB'nin tercihi açıktır: Kişi kimlik verisi **hem SD-JWT VC hem de ISO mdoc** biçiminde verilir. 2026/1731 sayılı uygulama tüzüğü, PID'in bu iki biçimde nasıl kodlanacağını alan alan tanımlar: SD-JWT VC'de tür `urn:eudi:pid:1`, mdoc'ta belge türü `eu.europa.ec.eudi.pid.1`'dir; doğum tarihi SD-JWT VC'de `birthdate`, mdoc'ta `birth_date` adıyla taşınır [13]. Tüzük ayrıca her PID alanının **tek tek seçici açıklanabilir** olmasını şart koşar. Bu çift biçim tercihinin gerekçesi basittir: mdoc yüz yüze gösterimde, SD-JWT VC ise web üzerindeki çevrimiçi gösterimde güçlüdür ve bir kimlik belgesi her iki ortamda da kullanılacaktır.

Öznitelik onayları için tüzük, ETSI'nin öznitelik onayı profillerini tanımlayan TS 119 472-1 standardını esas alır [13, 19]. Bu standart SD-JWT VC ve mdoc profillerinin yanında W3C modeli için de bir profil tanımlar. Tüzüğün gerekçe bölümü W3C modeline ayrıca değinir: W3C modeli özellikle eğitim alanında referans biçim olarak kullanıldığından, bu biçim için yeni profiller hazır olduğunda AB cüzdanlarının onu da desteklemesi gerektiğini belirtir [13]. Yani eğitim dünyasının W3C modeline yaptığı yatırım boşa gitmemektedir; ama AB cüzdanının bugünkü zorunlu çekirdeği SD-JWT VC ve mdoc üzerine kuruludur.

Belgeyi cüzdana vermek ve cüzdandan istemek için kullanılan protokoller de bu biçimleri taşıyacak şekilde tasarlanmıştır. OpenID Vakfı'nın belge gösterme protokolü OpenID4VP 1.0 (Temmuz 2025), SD-JWT VC için `dc+sd-jwt`, mdoc için `mso_mdoc`, W3C modeli için de ayrı biçim tanımlayıcıları içerir [17]; belge verme protokolü OpenID4VCI 1.0 (Eylül 2025) de aynı biçimleri destekler [18]. Bu protokoller dizinin sekizinci yazısının konusu.

> ÖRNEK
>
> **Aynur'un kimliği iki biçimde**
>
> Bu sistem Azerbaycan'da kurulmuş olsaydı, Aynur'un cüzdanına kimlik bilgisi iki kez yüklenirdi: bir kez SD-JWT VC, bir kez mdoc olarak. Aynur bir bankanın web sitesinde hesap açarken cüzdan SD-JWT VC kopyasını kullanır; bir otelde resepsiyondaki okuyucuya telefonunu yaklaştırdığında mdoc kopyasını. Aynur bu ayrımı hiç görmez; cüzdan, istek hangi biçimdeyse o biçimdeki kopyayı seçer. İki kopyanın içeriği aynıdır, imzaları ve anahtarları farklıdır.

9.3 Bir kurum hangi biçimi seçmeli?

Belge vermeye hazırlanan bir kurumun sorusu genellikle "hangi biçim en iyisi?" olur. Bu yazının vardığı yer, sorunun böyle sorulmaması gerektiğidir. Doğru soru, belgenin **nerede ve kime** gösterileceğidir. Tablo 3, sık karşılaşılan durumlar için pratik bir başlangıç noktası veriyor; kesin kurallar değil, eğilimlerdir.

Tablo 3. Kullanım durumuna göre biçim eğilimleri.

Kullanım durumu	Öne çıkan biçim	Gerekçe
Kimlik bilgisi (PID), AB uyumlu cüzdan	SD-JWT VC ve mdoc birlikte	AB tüzüğünün zorunlu kıldığı iki kodlama
Kasada, kapıda, yol kenarında gösterim	mdoc	yakın alan iletişimi standartta tanımlı; internet gerekmez
Web sitesinde çevrimiçi gösterim	SD-JWT VC (ya da mdoc)	web araçlarıyla uyum; tarayıcı arayüzü ikisini de taşıyabilir
Diploma, transkript, mikro yeterlilik	W3C VC ve SD-JWT VC	eğitim ekosisteminin ortak sözlükleri W3C modeline dayanıyor; AB cüzdanı için SD-JWT VC profili
Kısa ömürlü bilet, giriş kartı	SD-JWT VC ya da mdoc	küçük, hızlı doğrulanan, cihaza bağlı olmayabilir
Sınır ötesi, çok sayıda veren	profil üzerinde anlaşmaya bağlı	biçimden çok şema ve güven listesi uyumu belirleyici

Tablonun son satırı, bu yazının belki de en pratik dersidir. Bir belgenin sınırı geçip geçemeyeceğini çoğu zaman biçim değil, biçimin içindeki alanların ortak bir anlamda kullanılıp kullanılmadığı ve imzayı atan kurumun karşı tarafın güvendiği bir listede yer alıp almadığı belirler. İki ülke aynı biçimi kullanıp birbirinin belgesini anlamayabilir; farklı biçimler kullanıp, ortak bir profil ve güven listesi üzerinde anlaştıkları için birbirini rahatça doğrulayabilir.

10 Sınırlar ve Açık Sorular

Biçim çokluğu. Üç biçim, her birinin içinde de birden fazla seçenek (özellikle W3C modelinin güvenceleme yöntemleri) bulunması, cüzdanlara, verenlere ve doğrulayıcılara ciddi bir uygulama yükü getirir. Bir doğrulayıcının "doğrulanabilir belge kabul ediyorum" demesi yetmez; hangi biçimi, hangi profili, hangi imza algoritmasını kabul ettiğini söylemesi gerekir. ETSI'nin ve OpenID Vakfı'nın profilleri bu seçenekleri daraltmaya çalışıyor; ama biçimler arasındaki çeviri her zaman kayıpsız değildir.

Anlam uyumu. İki kurum aynı biçimi kullansa bile, "derece" ya da "mezuniyet tarihi" gibi alanları aynı anlamda kullanmıyorsa belgeler birbirini anlamaz. Doğrulanabilir belgelerin gerçekten sınır ötesi işlemesi için biçimden çok **şemalar** ve **sözlükler** üzerinde anlaşmak gerekir. Bu, teknik olmaktan çok yönetişimle ilgili ve yavaş ilerleyen bir iştir.

İmza, bağlanabilirliği de taşır. Bu yazıda anlatılan üç biçimin hepsinde verenin imzası, belge her gösterildiğinde aynıdır. Aynur aynı belgeyi iki farklı doğrulayana gösterirse, iki doğrulayan ellerindeki imzaları karşılaştırarak aynı kişiyle iş yaptıklarını anlayabilir. Seçici açıklama bu sorunu çözmez; dizinin üçüncü yazısı nedenini, beşinci yazısı ise çözüm yollarını anlatıyor.

Tazelik ve iptal. Doğrulayanın verene sormaması mahremiyet kazancıdır, ama bir bedeli vardır: Belge iptal edildiğinde doğrulayan bunu ancak durum listesinin bir sonraki güncellemesiyle öğrenir. Çevrimdışı doğrulamada bu gecikme daha da uzayabilir. Kısa ömürlü belgeler ve sık yenileme bir çözümdür ama cüzdan ile veren arasında daha sık iletişim gerektirir. Bu dengenin ayrıntısı dizinin yedinci yazısında.

Anahtar kaybı. Sahip bağlama, kişinin telefonunu kaybettiğinde belgelerinin de kullanılamaz hâle gelmesi demektir. AB modelinde çözüm, kişinin yeni bir cüzdan kurup belgelerini yeniden almasıdır; bu da verenlerin yeniden belge verme süreçlerini kolay ve hızlı tutmasını gerektirir.

Gerçek dünyayla köprü. Doğrulanabilir belge, onu kabul eden doğrulayan kadar değerlidir. Bugün iş başvurularının, kira sözleşmelerinin ve kamu işlemlerinin büyük kısmı hâlâ PDF ve fotokopi ile yürüyor. Kâğıttan dijitale geçiş dönemi uzun sürecek; bu süre boyunca kurumların hem eski hem yeni yolu kabul etmesi gerekecek ve cüzdanı olmayan kişiler dışlanmamalı.

11 Bu Tablonun İçinde Tamga Network

Bu yazıyı yayımlayan Tamga Network, Türkiye ve Türk dünyası için AB'nin eIDAS 2.0 ve EUDI profilleri üzerine kurulan, kâr amacı gütmeyen bir dijital güven ağıdır. Bu yazıda anlatılan üç rol ağın da temel modelidir: Kurumlar kişinin cüzdanına belge verir, kişi yalnızca istenen alanları paylaşır, doğrulayan da belgeyi veren kuruma sormadan saniyeler içinde doğrular.

Biçim tarafında ağ, AB'nin PID ve EAA için seçtiği iki biçimi esas alır: SD-JWT VC ve ISO/IEC 18013-5 mdoc. Ağın açık kaynak paketleri bu iki biçimde belge üretmeyi, seçici açıklamayı, sahip bağlamayı ve doğrulamayı gerçekleştirir. Doğrulayanın "veren yetkili mi?" sorusunu cevapladığı yer ise ağın yayımladığı imzalı güven listeleridir; bu listelerde hiçbir kişisel veri yer almaz. Ağ kendisi bir cüzdan işletmez; cüzdanları, belge veren kurumları ve doğrulayanları listeler.

12 Sonuç

Aynur'un diplomasının üç hâline döndüğümüzde, aralarındaki farkın kâğıt ile ekran arasında değil, **kimin neyi kanıtlayabildiği** arasında olduğunu görüyoruz. Kâğıt diploma, onu inceleyenin mührü tanımasına dayanır. Taranmış PDF hiçbir şey kanıtlamaz ve doğrulayanı verene sormaya mecbur bırakır. Doğrulanabilir belge ise doğrulayana, verene sormadan, dört soruya cevap verir: Belge değişmedi mi, kim imzaladı, hâlâ geçerli mi, gösteren sahibi mi?

Bu dört sorunun cevapları farklı yerlerden gelir. İlki imzadan, ikincisi güven listesinden, üçüncüsü geçerlilik tarihleri ve durum listesinden, dördüncüsü sahip bağlamadan. Bir doğrulanabilir belge sistemini değerlendirirken bu dört kaynağın her birinin sağlam olup olmadığına ve hiçbirinin doğrulayanı verene sormaya zorlayıp zorlamadığına bakmak gerekir.

Biçimler meselesi ise ilk bakışta göründüğünden daha az bölücüdür. W3C modeli, SD-JWT VC ve mdoc aynı parçaları farklı dillerde yazar: iddialar, veren, tür, geçerlilik, durum, sahip anahtarı ve imza. Avrupa Birliği'nin kişi kimlik verisi için iki biçimi birlikte seçmesi de bunun kabulüdür: Web için JSON, kasa ve kapı için CBOR. Asıl zor olan, bu biçimlerin içine yazılacak anlam üzerinde ve imzayı atanların kim olduğu üzerinde anlaşmaktır.

Dizinin bir sonraki yazısında, bu yazıda birkaç kez ertelediğimiz bir soruya yakından bakacağız: Aynur belgesinin yalnızca bir alanını gösterdiğinde, geri kalan alanlar matematiksel olarak nasıl gizli kalıyor ve bu gizlilik nerede yetersiz kalıyor?

Kaynaklar

[1] Sporny, M., Thibodeau Jr, T., Herman, I., Cohen, G. ve Jones, M. B. (Ed.) (2025). *Verifiable Credentials Data Model v2.0.* W3C Recommendation, 15 Mayıs 2025.

[2] W3C (2019). *Verifiable Credentials Data Model 1.0.* W3C Recommendation, 19 Kasım 2019.

[3] Fett, D., Yasuda, K. ve Campbell, B. (2025). *Selective Disclosure for JSON Web Tokens.* IETF RFC 9901, Kasım 2025.

[4] Terbu, O., Fett, D. ve Campbell, B. (2026). *SD-JWT-based Verifiable Digital Credentials (SD-JWT VC).* IETF Internet-Draft draft-ietf-oauth-sd-jwt-vc (çalışma sürüyor; erişim tarihindeki son taslak: –26; erişim 11 Kasım 2026).

[5] ISO/IEC (2021). *ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application.* Eylül 2021.

[6] ISO/IEC (2025). *ISO/IEC TS 18013-7:2025 Personal identification — ISO-compliant driving licence — Part 7: Mobile driving licence (mDL) add-on functions.* İkinci baskı, Mayıs 2025 (ilk baskı Ekim 2024).

[7] Jones, M., Bradley, J. ve Sakimura, N. (2015). *JSON Web Token (JWT).* IETF RFC 7519, Mayıs 2015.

[8] Jones, M., Bradley, J. ve Tschofenig, H. (2016). *Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs).* IETF RFC 7800, Nisan 2016.

[9] Bormann, C. ve Hoffman, P. (2020). *Concise Binary Object Representation (CBOR).* IETF RFC 8949, Aralık 2020.

[10] Schaad, J. (2022). *CBOR Object Signing and Encryption (COSE): Structures and Process.* IETF RFC 9052, Ağustos 2022.

[11] 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.

[12] Avrupa Komisyonu (2024). *Avrupa Dijital Kimlik Cüzdanlarına verilen kişi kimlik verisi ve öznitelik onaylarına ilişkin kuralları belirleyen 2024/2977 sayılı Uygulama Tüzüğü (AB).* 28 Kasım 2024.

[13] Avrupa Komisyonu (2026). *2024/2977, 2024/2979, 2024/2980 ve 2024/2982 sayılı Uygulama Tüzüklerini uygulanacak standartlar ve şartnameler bakımından değiştiren 2026/1731 sayılı Uygulama Tüzüğü (AB).* 15 Temmuz 2026; Avrupa Birliği Resmî Gazetesi, 22 Temmuz 2026.
[14] ICAO (2021). *Doc 9303: Machine Readable Travel Documents.* Sekizinci baskı, Uluslararası Sivil Havacılık Örgütü.
[15] Avrupa Parlamentosu ve Konseyi (2021). *COVID-19 salgını sırasında serbest dolaşımı kolaylaştırmak için birlikte çalışabilir aşı, test ve iyileşme sertifikalarının (AB Dijital COVID Sertifikası) verilmesi, doğrulanması ve kabulüne ilişkin çerçeve hakkında 2021/953 sayılı Tüzük (AB).* 14 Haziran 2021.
[16] Avrupa Komisyonu. "EU Digital COVID Certificate" (bilgi sayfası, commission.europa.eu) ve "The European Commission and WHO launch landmark digital health initiative to strengthen global health security." Basın açıklaması IP/23/3043, 5 Haziran 2023.
[17] Terbu, O., Lodderstedt, T., Yasuda, K., Fett, D. ve Heenan, J. (2025). *OpenID for Verifiable Presentations 1.0.* OpenID Foundation, 9 Temmuz 2025.
[18] Lodderstedt, T., Yasuda, K., Looker, T. ve Bastian, P. (2025). *OpenID for Verifiable Credential Issuance 1.0.* OpenID Foundation, 16 Eylül 2025.
[19] ETSI (2026). *ETSI TS 119 472-1 V1.2.1: Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 1: General requirements.* Şubat 2026.
[20] W3C (2025). *Securing Verifiable Credentials using JOSE and COSE* ve *Verifiable Credential Data Integrity 1.0.* W3C Recommendation, 15 Mayıs 2025.

Okuma listesi: Buradan başlayın

1. **W3C, *Verifiable Credentials Data Model v2.0*, Bölüm 1 ve 3.** Giriş ve temel kavramlar bölümleri, üç rolü ve belgenin parçalarını çizimlerle anlatıyor; teknik ayrıntıya girmeden okunabilir.
2. **IETF, RFC 9901 (SD-JWT), Bölüm 1 ve 4.** Yöntemin amacı ve veren tarafındaki adımlar, kısa örneklerle anlatılıyor.
3. **AB Dijital COVID Sertifikası teknik şartnameleri (eHealth Network).** Kitlesel ölçekte çalışmış bir imzalı belge ve güven listesi sisteminin nasıl kurulduğunu görmek için kısa ve öğretici bir örnek.
4. **2026/1731 sayılı Uygulama Tüzüğü'nün eki, Bölüm 4.** AB kişi kimlik verisinin SD-JWT VC ve mdoc'ta alan alan nasıl kodlandığı; iki biçimi aynı veri üzerinde karşılaştırmanın en somut yolu.
5. **OpenID for Verifiable Presentations 1.0, Ek B.** Farklı belge biçimlerinin aynı protokolde nasıl taşındığını gösteren biçim tanımları.

Ek A — Sözlük

Bu yazıda geçen terimler, yazıdaki anlamlarıyla. İngilizce karşılıklar, başka kaynaklarda aranabilmeleri için verilmiştir.

Tablo A.1. Terimler sözlüğü.

Terim	İngilizce	Anlamı
Açıklama	disclosure	SD-JWT'de gizlenebilir bir alanın tuz, ad ve değerden oluşan, imzanın dışında taşınan parçası
Apostil	apostille	Bir belgedeki imza ve mührün yetkili bir makama ait olduğunu onaylayan uluslararası tasdik
Base64URL	base64url	İkili veriyi web adreslerinde güvenle taşınabilen metne çeviren kodlama

Terim	İngilizce	Anlamı
CBOR	Concise Binary Object Representation	JSON'a benzer veri modelini ikili olarak kodlayan biçim
COSE	CBOR Object Signing and Encryption	CBOR verisini imzalamak ve şifrelemek için yapılar
Doğrulanabilir belge	verifiable credential	Veren tarafından imzalanmış, makinenin okuyabileceği iddialardan oluşan belge
Doğrulanabilir sunum	verifiable presentation	Sahibin bir ya da birkaç belgeyi doğrulayana göstermek için hazırladığı imzalı yapı
Durum listesi	status list	Verenin yayımladığı, belgelerin iptal edilip edilmediğini gösteren liste
EAA	electronic attestation of attributes	PID dışındaki öznitelik onayları (diploma, ehliyet vb.)
Eve telefon etme	phone home	Doğrulayanın her doğrulamada belgeyi verene sorması
Gömülü kanıt	embedded proof	İmzanın verinin içinde ayrı bir alan olarak durduğu yöntem
İddia	claim	Bir özne hakkında söylenen tek bir bilgi; ad ve değerden oluşur
JSON-LD	JSON for Linked Data	Alan adlarını internetteki ortak sözlüklere bağlayan JSON yöntemi
JWT	JSON Web Token	Başlık, içerik ve imzadan oluşan imzalı JSON yapısı
mdoc	mobile document	ISO/IEC 18013-5'te tanımlı, CBOR tabanlı mobil belge biçimi
mDL	mobile driving licence	Mobil sürücü belgesi
MSO	mobile security object	mdoc'ta alan özetlerini, cihaz anahtarını ve geçerliliği taşıyan imzalı nesne
Nonce	nonce	Doğrulayanın her işlem için ürettiği tek kullanımlık, tahmin edilemeyen değer
PID	person identification data	Devletin ya da yetkilendirdiği kurumun verdiği temel kişi kimlik verisi
Sahip bağlama	holder binding	Belgenin sahibinin elindeki bir anahtara bağlanması ve bunun her gösterimde kanıtlanması
SD-JWT VC	SD-JWT-based verifiable digital credential	Seçici açıklamalı JWT tabanlı doğrulanabilir belge biçimi
Seçici açıklama	selective disclosure	Belgenin yalnızca gereken alanlarını gösterebilme
Şema	schema	Bir belge türünün alanlarını, değer biçimlerini ve anlamlarını tanımlayan belge
Şifre takımı	cryptosuite	Data Integrity'de imza algoritmasını ve düzenleme yöntemini birlikte belirleyen paket
Tekrar oynatma	replay	Daha önce kaydedilmiş bir sunumun başka bir zamanda ya da yerde yeniden kullanılması
Zarflayan kanıt	enveloping proof	Verinin imzalı bir zarfın içine konduğu yöntem