



BLOCKCHAIN
T Ü R K İ Y E

DİJİTAL KİMLİK RAPORU

NİSAN 2019



T Ü R K İ Y E B İ L İ Ş İ M V A K F I

DİJİTAL KİMLİK RAPORU

NİSAN 2019

©2019, Blockchain Türkiye Platformu

Tüm hakları saklıdır. Bu eserin tamamı ya da bir bölümü, 4110 sayılı Yasa ile değişik 5846 sayılı FSEK uyarınca, kullanılmazdan önce hak sahibinden 52. Maddeye uygun yazılı izin alınmadıkça, hiçbir şekil ve yöntemle işlenmek, çoğaltılmak, çoğaltılmış nüshaları yayılmak, satılmak, kiralanmak, ödünç verilmek, temsil edilmek, sunulmak, telli/telsiz ya da başka teknik, sayısal ve/veya elektronik yöntemlerle iletilmek suretiyle kullanılamaz.

İşbu Rapor'da yer alan bilgi ve görüşler yazarlarına ait olup yazarların çalıştığı kurumların, TBV'nin ve Blockchain Türkiye Platformu'nun görüşlerini temsil etmemektedir. İşbu Rapor'un içeriği, yazarları tarafından her zaman site üzerinde herhangi bir duyuru yapılmadan değiştirilebilir.

Tasarım ve Grafik Uygulama

TERMINAL MEDYA LTD. ŞTİ.

Maslak Mah. Bilim Sokak No:5 SUN Plaza Kat:13 Sarıyer/İSTANBUL

0(212) 367 4988 ve 0(532)643 6959

Editör

ÖZLEM ÖZKAN

Grafik Uygulama

GÜLİSTAN ŞENOL

Baskı

RUMİ MATBAACILIK

Maltepe Mah. Fazılpaşa Cad. No:8 Topkapı/İSTANBUL

0(212) 612 7172



Finans, Bankacılık ve Sigortacılık

SORUMSUZLUK BEYANI

"Türkiye Bilişim Vakfı altında çalışmakta olan Blockchain Türkiye Platformu'nun "Bankacılık, Finans ve Sigortacılık Çalışma Grubu" tarafından hazırlanan işbu rapor dijital kimlik konusunda farkındalık yaratmak amacıyla hazırlanmış olup, sadece bilgilendirme amaçlıdır, kişi ve kurumları bağlayıcı tavsiye veya görüş niteliği taşımaz. İşbu rapor kamuya açık kaynaklardan yararlanılmış bilgileri içermekte olup, söz konusu bilgilerin güncel ve eksiksiz olduğu taahhüt edilmemektedir. İşbu raporda verilen tüm bilgi ve görüşler zamanla değişkenlik gösterebilir. Bu bağlamda işbu raporun içeriğini okuyan kişilere veya herhangi bir üçüncü kişiye karşı sorumluluğu ve yükümlülüğü bulunmamaktadır."

İÇİNDEKİLER

Sunuş	5
Katkı Sağlayan Kurumlar	6
Önsöz	7
Yönetici Özeti	8
1. Kimlik Nedir?	10
1.1. Kimlik İşlemleri	10
1.2. Kimlik Yaşam Döngüsü	10
2. Kimlik İspatı İle İlgili Zorluklar	11
2.1. Dijital Kimlik Kullanım Alanları ve Ekosistemler	12
3. Ekosistem Paydaşları	13
3.1. Ekosistem Kullanım Senaryoları	14
3.2. Dijital Kimlik Ekosisteminde Yer Alması Önerilen Birleşik Paydaş Listesi	16
4. Dijital Kimlik Sistemlerinin Ana Temel Tasarım Prensipleri	17
4.1. Mahremiyet Odaklı Olması	17
4.2. Güvenlik	17
4.3. Erişebilirlik ve Taşınabilirlik	18
4.4. Kullanıcı Odaklılık	18
4.5. Şeffaflık	18
4.6. Ölçeklenebilirlik	18
4.7. Performans	18
4.8. Kullanılabilirlik	18
4.9. Birlikte Çalışabilirlik	19
4.10. Denetlenebilirlik	19
4.11. Esneklik	19
4.12. Kalıcılık	19
5. Dijital Kimlik Yönetim Modelleri	19
6. Dijital Kimlik Yönetim Çözümlerinin Teknolojik Açıdan Değerlendirilmesi	21
6.1. Merkezi / Dağıtık Teknolojiler	21
7. Dijital Kimlik Yönetimi Çözümlerinde “Blockchain”	22
8. Netleştirilmesi Gereken Kritik Konular	23
8.1. Teknik Model	23
8.2. Yönetişim ve İş Modeli	24
8.3. Standartlar	25
8.4. Hukuki Değerlendirme ve Regülasyon	27
8.5. Güvenlik ve Mahremiyet	28
8.6. İş Akışı ve Hayat Döngüsünün Belirlenmesi	29
9. Yurt Dışı Dijital Kimlik Örnekleri	30
Sonuç	32
Tanımlar Sözlüğü	33
Katkı Sağlayan Kişiler	34
Ekler	38



TÜRKİYE BİLİŞİM VAKFI

Türkiye Bilişim Vakfı, Türkiye'nin bilgi toplumuna dönüşebilmesi için altyapının oluşturulabilmesine katkıda bulunmak ve bilişim sektörünün ekonomideki payının arttırılması için, bilimsel araştırma ve geliştirme etkinliklerinde bulunarak ekonomik ve sosyal çalışmalar yapmak, projeler üretmek ve uygulamalarını sağlamak amacıyla kurulmuştur.

BLOCKCHAIN
TÜRKİYE

Blockchain Türkiye Platformu, Türkiye Bilişim Vakfı (TBV) liderliğinde Türkiye'de sürdürülebilir blokzincir ekosistemi oluşturarak, bu teknoloji ile yeni dönem iş yapış biçimlerinin önündeki zorlukların giderilmesine yönelik bir paylaşım platformu oluşturmak amacıyla kurulmuştur.

SUNUŞ



Faruk Eczacıbaşı

Blockchain Türkiye
Yürütme Kurulu Başkanı
Türkiye Bilişim Vakfı
Yönetim Kurulu Başkanı

Türkiye Bilişim Vakfı'nı Mayıs 1995'te kurduğumuzda, kendine çok basit bir misyon belirlemiştik; bilgi ve iletişim teknolojilerinin ülkenin verimliliğine katkıda bulunmasını sağlamak. Bugün ister Dördüncü Endüstri Devrimi diyelim, ister bilgi toplumu, gerçek şu ki dünya gittikçe hızlanan bir aşamaya girdi ve bizi de yeni bir düşünme biçimine zorluyor.

Blokzincir, bu yeni düşünce kalıbının en devrimsel sonuçları olacak ürünlerinden biri ve bu teknolojinin anlaşılabilmesi, uygulanabilmesi için, deneyimin kazanılması beklenmeli. Her yeni teknolojiye olduğu gibi, blokzincirde de konseptlerle başlayan deneysel süreçlerin pilot aşamalarına, bunların da nihai ürüne dönüşmesi gerekiyor.

Blokzinciri diğer teknolojilerden ayıran en temel özellik ise beraberinde getirdiği sektörler arası konsorsiyumlar, platformlar gibi ortamlarda "birlikte çalışma" ihtiyacı. Yeni bir düşünce kalıbı olarak blokzincir, ekosistemlerin önemini artırırken, teker teker şirketler ve onların ürünlerinden ziyade, bir arada değer yaratmayı başarabilen ekosistemleri ön plana çıkarıyor.

Bu sebepten, Türkiye Bilişim Vakfı olarak 8 Haziran 2018 tarihinde bir adım attık. Blokzincir teknolojisinin Türkiye'de yaygınlaşması, bilinirliği ve kullanımının artırılması, faydalarının araştırılması ve stratejik önceliklerinin saptanması gibi temel hedeflerle, Blockchain Türkiye Platformu'nu (BCTR'yi) hayata geçirdik. Blockchain Türkiye Platformu (BCTR), Türkiye'de sürdürülebilir blokzincir ekosistemi oluşturarak, bu teknoloji ile yeni dönem iş yapış biçimlerinin önündeki zorlukların giderilmesine yönelik bir paylaşım platformu.

Umuyorum ki dünya, buhar makinesinin icadından bu yana alıştığımız "önce üret, sonra sat" iş modelinden, "birlikte üret, sat ve tüket" (Co-create & Prosume) kavramlarına doğru yolculuğa çıkarken, bu platformun ve ürettiği çalışmaların ülkemize bir faydası dokunsun.

KATKI SAĞLAYAN KURUMLAR


BANKALARARASI
KART MERKEZİ
Elektronik Bilgi Güvenliği A.Ş.
FORD OTOSAN
SAĞLAM BANKACILIK
strateji regülasyon politika

ÖNSÖZ



Dilnişin Bayel

Accenture Türkiye
Ülke Direktörü

Hayatımızın bir çok noktasında hizmetlere erişim için kayıt olmak ve kendimizi tanıtmak zorundayız, benzer şekilde firmaların birçoğu da müşterilerinin doğrulanması ve kaydedilmesini takiben işlem yapabiliyorlar.

Ayrıca kimlik kavramı, sadece doğumla verilen bir nüfus kayıt bilgisi olmaktan çok ileriye gitmiş durumda kimlik ve bizi tanımlayan bilgiler zaman içinde genişliyor ve daha çok veri bizi tanımlamak için kullanılabilir hale geliyor. Almak istediğimiz hizmeti sağlayan taraf için anlamlı olan veriler, kurumlar arasında farklılık gösteriyor. Dijital dünyada hizmetlerin özelleştirilmesi için de benzer şekilde daha fazla bilgi kullanılabilir.

Raporda, Dijital Kimlik kavramı ve işletimine ilişkin yaklaşım ile hizmet alan ve verenin arasındaki bu tanıma ve doğrulama akışında Dijital Kimlik modelinin kullanımını anlatmaya çalıştık. Bir sefer kendini sistemde doğrulamış bir kişinin, takip eden işlemlerinin ve hizmet alımlarının bu doğrulanmış bilginin teyid ve tasdiki devam edebilir hale gelmesi önerilmiştir. Kişinin merkezde olduğu, kiminle hangi verisinin paylaşımında inisiyatif ve moderasyon yapabileceği bir kurgu tanımlanmıştır.

Katkıları için tüm BCTR Finans, Bankacılık ve Sigortacılık ekibine teşekkür ederim. Blockchain Türkiye Platformu olarak ekli raporu sizlerle paylaşmaktan büyük mutluluk duyuyoruz.

YÖNETİCİ ÖZETİ

İnsanlar doğdukları andan itibaren kendilerini tekil olarak tanımlayacak kimlik bilgilerine sahip olurlar ve bu bilgilere zaman içerisinde yenilerini eklerler hatta farklı yerlere kayıt oluşturdıkları sırada kendileri için farklı kimlikler yaratırlar. Eski zamanlarda kişilerin kendilerini ispat etmesi görünüşleri ve tanıdıkları vasıtasıyla mümkün olurken ulus devlet yapılarının ve uluslararası sınırların oluşması ile daha resmi araçlara ihtiyaç duyulmuş ve nüfus cüzdanı, ehliyet, pasaport, fatura vb fiziksel dokümanlar ile kim olduklarını ispatlamaya başlamışlardır.

Özellikle son yıllarda kişilerin çok fazla yerde kendilerini tanımlamaları ihtiyacı doğmaya başlamıştır. Bu durum da beraberinde fiziksel doküman paylaşmanın zorluğu ve zaman kaybı, gerekenden fazla bilgi paylaşımı, paylaşılan bilgilerin akıbetinin bilinmemesi, bilgileri açık (sesli ya da yazılı) paylaşmaktan doğan güvenlik zafiyeti gibi zorlukları beraberinde getirmektedir.

Günümüz dünyasında dijitalleşmenin getirdiği imkanlardan azami fayda sağlamak için “dijital kimlik” kavramı ortaya çıkmış olup kişilerin kendi kimlik bilgilerini dijital ortamda farklı kurumlar ile paylaşabilmesi bu sayede kayıt, başvuru gibi süreçlerin tamamını dijital gerçekleştirebilmesi mümkün hale gelmiştir. Hatta bu süreçlerde kişilerin kendi verilerini kaynağını değiştirmeden kendisini kanıtlama amaçlı paylaşması sağlanabilmektedir.

Raporda dijital kimliğin neden önemli olduğu anlatılmış ve örnek kullanım senaryolarından yola çıkılarak böyle bir kimliğin işlemlerini sağlayacak ekosistemin paydaşları belirlenmiştir. Raporda belirtildiği gibi dijital kimliğin hemen tüm sektörlerde kullanım alanı bulunup kamu ve özel paydaşların bir araya gelmesi ile daha büyük etki yaratması mümkün hale gelmektedir.

Raporda sadece gerçek kişilere odaklanılmış olup dijital kimlik konusu genel olarak ele alınmıştır. Dijital kimlik konusunda tüm dünyada farklı çözüm ve alt yapılar gelişmektedir. Raporda dijital kimlik projeleri için önerilen temel prensip ve bileşenlere yer verilmiştir. Ülkemizde dijital kimlik ekosisteminin yaratılmasının getireceği faydalar şu şekilde sıralanmıştır:

- » Mobil cihazlar aracılığı ile kullanıcıların 'kendisi' olduklarını kanıtlayabilmeleri
- » Doğrulan kimlik bilgilerinin tüzel ve gerçek kişilere hızlı, kolay ve güvenli iletimi
- » 'Sadece gerektiği kadar' prensibiyle, kimlik bilgilerinin paylaşım detay ve süresinin kontrolünü kullanıcıya veren artırılmış mahremiyet sağlanması
- » Kullanıcının doğrulanmış bilgilerinin hızlı iletim ve paylaşımıyla zaman kazanımı
- » Merkezi olmayan yapıda veri gizliliği, veri güvenliği ve veri bütünlüğünün birlikte temini

Başarılı dünya örneklerinden, tasarım prensiplerden ve kimlik yönetim modellerinden yola çıkıldığında dijital kimlik hizmetlerini yönetebilmenin en uygun yolunun dağıtık yapılarda işbirlikleri çerçevesinde yapılmasının sürdürülebilir bir dijital kimlik projesi için kaçınılmaz olduğu görülmektedir. Ülkemizde de başka pek çok konuda örnekleri olduğu gibi kolektif bir çalışma örneğinin bu alanda da hayata geçmesini ve daha dijital bir Türkiye'ye ulaşmak en büyük dileğimizdir.

1. KİMLİK NEDİR?

Kimlik, kişiye ait biyografik ve biyolojik özellikler de dahil olmak üzere, bir kişiyi tekil olarak betimleyen özellikler ve karakteristik davranışlardır.

1.1. Kimlik İşlemleri



>> **Kimlik Tanıma:** Bir kişinin kim olduğunu ve/veya olmadığını belirleyen eylemdir



>> **Kimlik Doğrulama:** Bir kimliğin (hizmet alma talebinde bulunan kişinin kimliğinin) yeterli delil ve ispatların beyan edilmesi sonucunda doğrulanmasıdır.

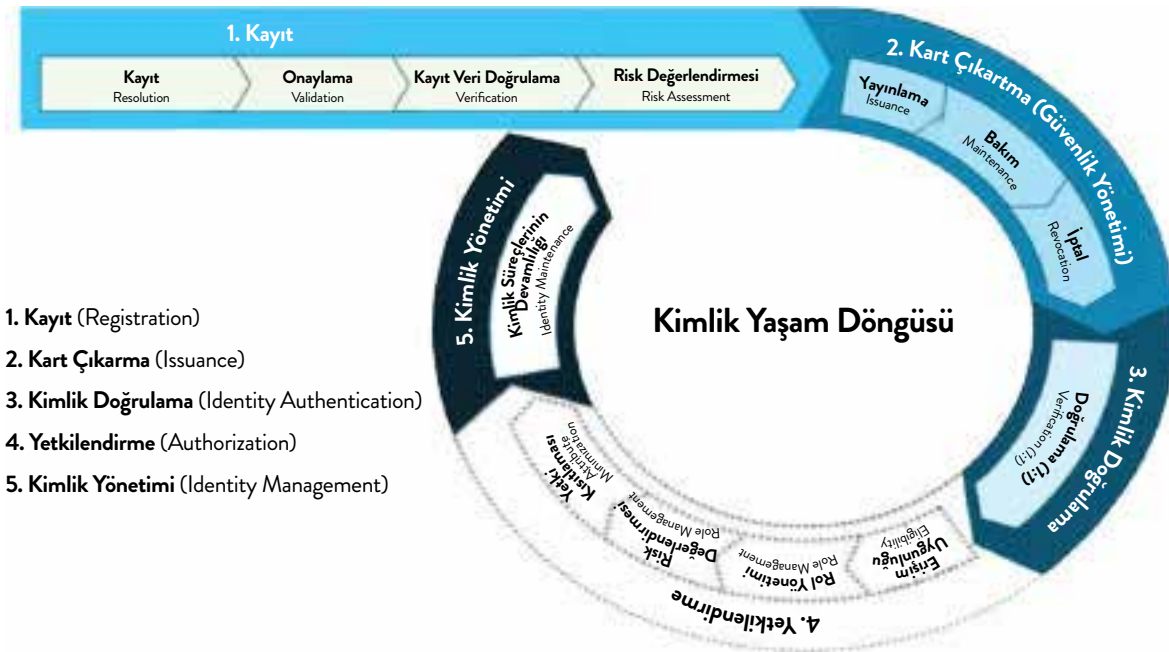


>> **Yetkilendirme:** Kimlik doğrulamadan sonra kişinin belirli kurallar dahilinde belirli süreliğine hizmetlere veya kaynaklara erişimine olanak tanınmasıdır.

1.2. Kimlik Yaşam Döngüsü

Aktif olarak kişinin yaşam süresini, pasif olarak da ölümünden sonraki dönemi kapsayan; kimlik doğrulama süreçlerinde kullanılan kişiye ait öznitelik bilgilerin belirli otoriteler tarafından verilmesi veya atanmasını içeren döngüdür (Şekil 1).^{(1) (2)}

Şekil 1. Kimlik Yaşam Döngüsü⁽¹⁾



1. Kayıt (Registration)

2. Kart Çıkartma (Issuance)

3. Kimlik Doğrulama (Identity Authentication)

4. Yetkilendirme (Authorization)

5. Kimlik Yönetimi (Identity Management)

⁽¹⁾ Technology Landscape for Digital Identification, 2018 - World Bank Group.

⁽²⁾ G20 Digital Identity Onboarding, 2018 - World Bank Group.

Kişiye ait özniteliklerin belirlenmesi ve / veya atanması devlet veya özel kuruluşlar tarafından yapılabilmektedir.

Kimlik yaşam döngüsü, kişiler açısından ilk ve en önemli adım olan ve doğum üzerine gerçekleşen kayıt olma (registration) ile başlar. Sonraki adımlar kişinin zaman içinde kazandığı veya geçerliliğini yitiren öğrenim, evlenme, boşanma, ehliyet, yasal statüler kazanma gibi bilgileri ve öznitelikleri ile güncellenir.



2. KİMLİK İSPATI İLE İLGİLİ ZORLUKLAR

Günlük hayatımızda kurumlara veya bireylere kendimizi doğrulamak için pek çok farklı fiziksel belge ve doküman kullanırız. Örneğin bir banka şubesinde hesap açmak için, mobil operatörden hat almak için veya konaklama yapacağımız otelde kendimizi tanıtmak için kimlik kartlarımız, fatura bilgileri gibi dokümanlar ibraz ederiz. Ülkemizde 2018 senesinde yapılan bir çalışmada⁽¹⁾ kişilerin günlük hayatlarında fiziksel olarak kimlik bilgilerini paylaşmada yaşadıkları temel sorunlar şu şekilde sıralanmıştır:

- » Dokümantasyon, çoklu işlem veya fiziksel eylemin zahmeti ve zaman kaybı
- » İhtiyaç duyulan bilgiye hemen erişememek
- » İhtiyaç duyulandan fazla bilgi paylaşmak
- » Bilgileri açık (sesli ya da yazılı) paylaşmaktan doğan güvenlik zaafiyeti
- » Toplanan bilgilerin akıbetinin ve saklanma süresi/koşullarının bilinmemesi
- » Her yeni servise en baştan kimlik kanıtlama gerekliliği
- » Yönetilmesi ve hatırlanması gereken onlarca dijital kimlik (giriş, şifre) olması
- » Saklanması ve taşınması gereken çok sayıda fiziksel kimlik belgesi olması

Kimliklerin ibraz ve ispatının getirdiği sorunları teknolojinin imkan sağladığı bir imkan olan Dijital Kimlik ile çözmek mümkün görünmektedir.

Dijital Kimlik; kimlik ibraz ve ispatında kullanılabilecek elektronik olarak toplanan, saklanan ve doğrulanabilen, kişiye ait kimlik bilgilerinin tamamı olarak tanımlanmaktadır.^{(2) (3)}

⁽¹⁾ BKM ve Accenture Dijital ID Raporu, 2018

⁽²⁾ World Bank. 2018. Technology Landscape for Digital Identification, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

⁽³⁾ G20 DIGITAL IDENTITY ONBOARDING, 2018. World Bank Group.

Kimlik ibraz ve ispatı için kullanılan çözüme “Dijital Kimlik Servisi” söz konusu servisin çalışmasını sağlayan bileşenlerin tümüne de “Dijital Kimlik Sistemi” denmektedir.

2.1. Dijital Kimlik Kullanım Alanları ve Ekosistemler ^{(1) (2)}

Dijital kimliğin belirtilen faydaları sağlayabileceği, kişilerin günlük hayatında en çok karşılaştığı ve kimlik doğrulamanın ihtiyaç duyulduğu hizmet alanlarına örnekler aşağıdaki gibidir.

Dijital kimliğe uygun kullanım senaryoları oluşturulurken kullanılacak kimlik unsuru veriler ve ekosisteme dahil olması önerilen kamu ve özel sektör paydaşları da belirlenmeye çalışılmıştır.

(*) İlk aşamada, aşağıdaki 12 ekosistem (Tablo 1) ve bu ekosistemlere ilişkin toplam 71 kullanım senaryosu oluşturulmuştur. Ekosistem kavramı ile; belirli bir alanda bulunan gerçek ve tüzel paydaşlar ile bunlar arasındaki etkileşimlerden oluşan yapı kastedilmektedir.

Tablo 1. Dijital Kimlik Kullanılabilecek Ekosistemler

	KAMU HİZMETLERİ		PERAKENDE (MAĞAZA ve ONLINE)
	FİNANSAL HİZMETLER		EV ve BARINMA
	SAĞLIK		MOBİLİTE
	EĞİTİM		KÜLTÜR ve EĞLENCE
	İLETİŞİM		TİCARET
	ULAŞIM ve KONAKLAMA		SİGORTA

⁽¹⁾ <https://www.mckinsey.com/industries/financial-services/our-insights/remaking-the-bank-for-an-ecosystem-world>

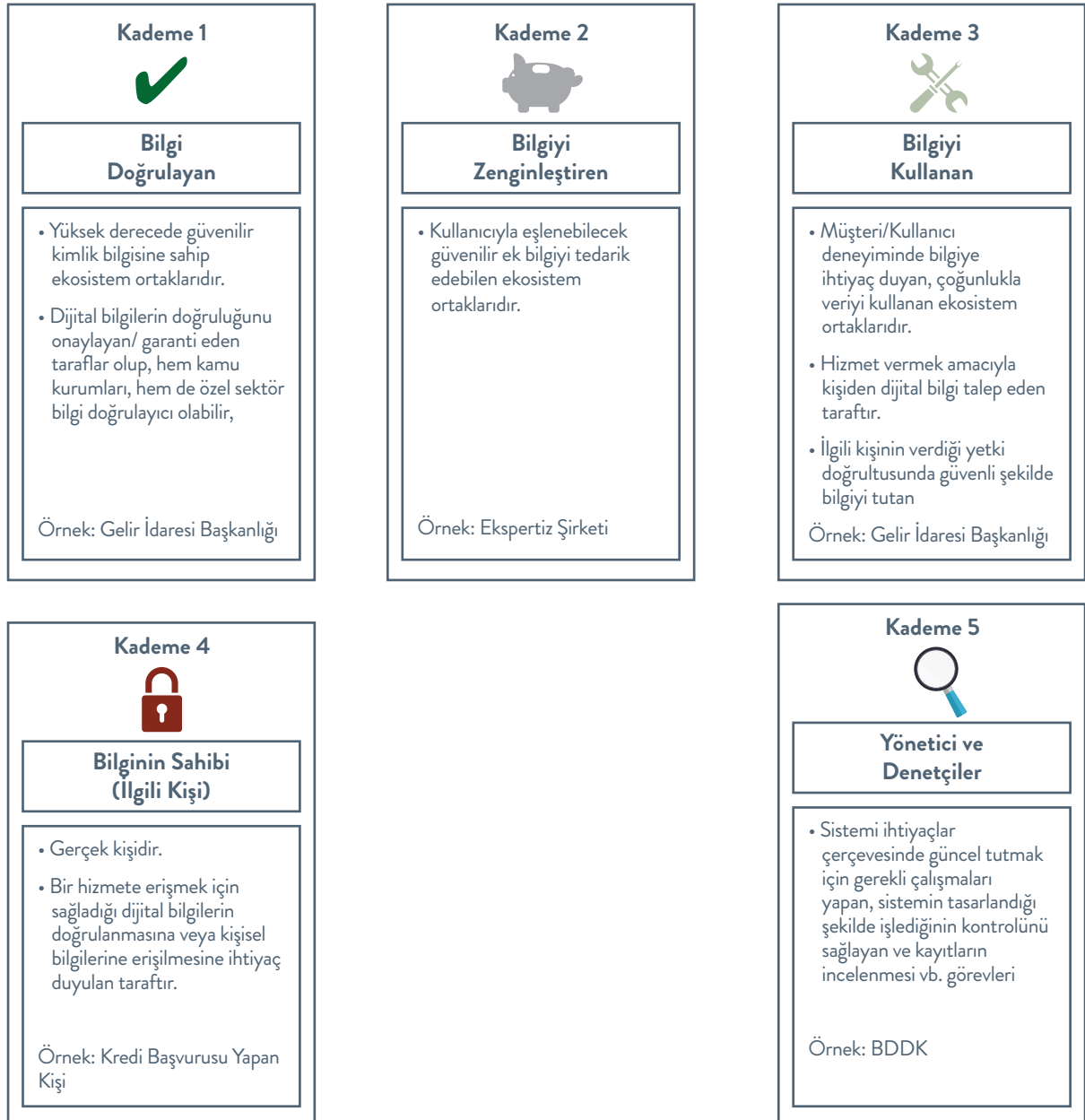
⁽²⁾ Fjord tarafından fasilete edilen ve BKM ile 9 bankanın katılımıyla gerçekleştirilen çalıştay sonrasında oluşturulan Mayıs 2018 tarihli “Dijital Kimlik Çalıştay Raporu

3. EKOSİSTEM PAYDAŞLARI

Kullanım senaryolarından da görülebileceği gibi dijital kimlik denilince çok taraflı bir ekosistemden bahsedilmektedir. Ekosistem içerisinde paydaşlar sahip oldukları, ihtiyaç duydukları bilgi, yetkinlikleri gibi özelliklerine göre farklı kademelerde rol alabilirler. Kademeler arasında geçiş olabileceği gibi bir paydaş aynı anda farklı kademelerde de rol oynayabilir.

Bir önceki bölümde belirlenen kullanım senaryoları için farklı kademelerde 5 paydaş rolü tanımlanmış olup, ilk 3 kademedeki paydaşlar kullanım senaryosu bazında önerilmiştir. Daha önce de belirtildiği gibi paydaşların birden fazla kademeye ilişkin görevleri bulunabilir.

5 kademeli paydaş rolleri şu şekilde olup örnek bir kullanım senaryosu olarak «Konut Kredisi Başvurusu Yapmak» sürecine ilişkin paydaş örnekleri de belirtilmiştir:



3.1. Ekosistem Kullanım Senaryoları

12 ekosisteme ilişkin kullanım senaryoları ve paydaşları aşağıda yer alan Tablo 2 ve Tablo 3’de listelenmiş olup bu senaryolara ilişkin detay bilgilere ise EK-1’de yer verilmiştir. Ekosistemler arası geçişkenlik nedeniyle bir senaryo birden fazla ekosistem altında değerlendirilebilecek olsa da Mükerrerlik yaratmamak ve daha fazla senaryoya yer vermek adına aşağıdaki tablolarda yer alan senaryolar birden fazla ekosistem ile ilişkili olsa dahi sadece bir ekosistem ile eşleştirilerek belirtilmiştir.”

Tablo 2. Örnek Kullanım Senaryoları

	KAMU HİZMETLERİ	• Ehliyet Başvurusu • Adli İşlemler / Dava Açma • İkametgah Belgesi Alınması • Doğum Belgesi Alınması • Tapu Devri • Evlilik Cüzdanı Alınması • Sporcu Lisansı Alınması • E-Devlet Sistemine Giriş • Vekalet İşlemleri • İşe Alım / Staj Başvurusu • Vergi ve Ceza Ödemeleri
	FİNANSAL HİZMETLER	• Bireysel Hesap Açılması • Gerçek Kişi Tacire Hesap Açılması • Online/Mobil Bankacılık Müşterisi Olmak • Müşterisi Olunan Bankaya Kredi Ürün Başvurusu Yapmak (kredi, kredi kartı vb.) • Dijital Çek Kullanılması • Sim Kart Değişikliğinin Bildirilmesi • Bankadaki Kişisel ve Teyitli Bilgilerin Paylaşılması • Yatırım Ürünleri Alım Satımı • Kripto Varlık Alım Satımı • Banka Dışı Finansal Kurumlarda İşlem Yapılabilmesi
	SAĞLIK	• Elektronik Reçete Oluşturulması • Sağlık Raporu Alınması • İş Görmelik Belgesi Alınması • Sağlık Kuruluşlarında Muayene Olmak • Eczaneden İlaç Alınması • Laboratuvar Tahlilleri • Provizyon Alınması • Hastane Ziyareti • Mülteciler için Dijital Kimlik ile Sağlık Bilgilerine Ulaşılması / Sağlık Hizmeti Verilmesi • Göçmenler için Dijital Kimlik ile Sağlık Bilgilerine Ulaşılması / Sağlık Hizmeti Alınması
	EĞİTİM	• Diploma Alınması • Transkript (Not Durum Belgesi) Alınması • Okul kaydı (Zorunlu Eğitim Dönemi) • Öğrencinin başka bir eğitim kurumuna nakli • Yurt Kaydı • ÖSYM Sınavına Girecek Adayların Fiziksel Özelliklerini Doğrulamak Amacıyla Biyometrik Yöntemlerle Kimlik Doğrulaması • Mülteciler için Dijital Kimlik ile Eğitim Bilgilerine Ulaşılması • Göçmenler için Dijital Kimlik ile Eğitim Bilgilerine Ulaşılması • KYK Başvurusu

	İLETİŞİM	• Abonelik İşlemleri (tesis, taşıma, iptal vb.) • Mobil İmza Alınması
	ULAŞIM KONAKLAMA	• Otel Rezervasyonu ve Check-In İşlemi • Yolculuk Bileti Satın Almak ve Havalimanında Check-In İşlemi • Araba, Drone, Bisiklet vb. Ürünlerin Kiralanması • Vize Başvurusunda Bulunmak
	PERAKENDE (MAĞAZA / ONLINE)	• İnternette / Mağazadan Alışveriş Yapılması • Sadakat Programı Uygulamaları (kişinin hak kullanımı veya işlemini kartına işletmesi vb.) • Uluslararası Ticarete Karşılıklı Kredibilite Sorgulaması (finansal bilgilerin teyidi) • Satışı Kısıtlı Olan Ürünlerin Satışı (ör: silah, alkol vb.) • Captcha Kullanımı
	EV / BARINMA	• Zorunlu Deprem Sigortası • Ev Kiralama • Kurum Üyelikleri (elektrik, su vb.) • Taşınma ve Renovasyon
	MOBİLİTE	• Zorunlu Trafik Sigortası • Uber, Taksi ve Scotty gibi Şehir İçi Ulaşım Platformları • Başkası Adına Kargo / Paket Teslim Alınması • Paylaşımlı Araç Hizmetleri (ör: otomobil, servis) • Araç Bakım ve Muayene
	KÜLTÜR EĞLENCE ve FİZİKSEL MEKAN GİRİŞLERİ	• Etkinlikler İçin Bilet / Sadakat Kartı Alınması • Etkinliklerde Yaş Kontrolü • Şans Oyunları • Bina/Plaza Girişleri • Spor Salonu vb. Toplu Alanlara Fiziksel Giriş-Çıkış • Emanet alma (Ör: müze/tercüme kulaklıkları)
	TİCARET	• Motorlu Taşıt Satışı • Gümrük Müşavirliği İşlemleri • Mal Alım Satımlarda Smart Kontrat • Şirket Açmak / İş Kurmak • Kıymetli Maden Satışı
	SİGORTA	• Sigorta Başvurusu⁽¹⁾ • Sigorta Hasar Talebi

⁽¹⁾ Sigorta ekosistemi altında genel sigorta başvurusu belirtilmiş olup Zorunlu Deprem ve Trafik Sigortası kullanım senaryolarına sırasıyla «Ev / Barınma» ve «Mobilité» ekosistemleri altında yer verilmiştir

3.2. Dijital Kimlik Ekosisteminde Yer Alması Önerilen Birleşik Paydaş Listesi

Tablo 3. Paydaş Listesi

KAMU PAYDAŞLARI	ÖZEL SEKTÖR PAYDAŞLARI
• Bankalar • Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) • Sosyal Güvenlik Kurumu (SGK) • Hastaneler • Nüfus ve Vatandaşlık İşleri • Milli Eğitim Bakanlığı • Eğitim Kurumları / Okullar • Gelir İdaresi Başkanlığı • E-Devlet • Emniyet Genel Müdürlüğü • Adalet Bakanlığı • Ticaret Bakanlığı • Sağlık Bakanlığı • Tapu ve Kadastro Genel Müdürlüğü • Belediyeler • Gençlik ve Spor Bakanlığı • Noterler • Elektrik / Su / Doğalgaz Abonelik ve Dağıtım Şirketleri • Mali Suçları Araştırma Kurulu (MASAK) • Türkiye Odalar ve Borsalar Birliği • Merkezi Nüfus İdare Sistemi (MERNİS) • Türkiye Cumhuriyet Merkez Bankası (TCMB) • Konsolosluklar • Sermaye Piyasası Kurulu (SPK) • Kimlik Paylaşım Sistemi (KPS) • Yükseköğretim Kurulu • Yurtkur • Ölçme, Seçme ve Yerleştirme Merkezi (ÖSYM) • Afet ve Acil Durum Yönetimi Başkanlığı • Müzeler • Doğal Afet Sigortaları Kurumu (DASK)	• Bankalar • Hastaneler, Sağlık Kuruluşları ve Doktorlar • Sigorta Şirketleri • Eczaneler • Yatırım / Portföy Şirketleri • Aracı Kurumlar • Faktoring / Leasing / Tüketici Finansmanı / Ödeme Şirketleri • Sürücü Kursları • Emlakçılar • Oteller / Turizm Şirketleri • Sosyal Yardım Kuruluşları • Spor Kuruluşları, Kulüpleri • Spor Müسابakaları Düzenleyen Kuruluşlar • Eğitim Kurumları / Okullar • Elektrik / Su / Doğalgaz Abonelik ve Dağıtım Şirketleri • Ekspertiz Şirketleri • Otomotiv Şirketleri / Bayileri • Kredi Kayıt Bürosu (KKB) • Takasbank • Bankalararası Kart Merkezi (BKM) • Borsa İstanbul • GSM, Telekomünikasyon, İnternet Hizmeti Firmaları • Bilet Satan Ulaşım / Konaklama, Turizm Şirketleri • Araç Kiralama Platformları / Şirketleri • Kargo Şirketleri • Araç Muayene, Bakım & Onarım Servisleri • Renovasyon Hizmeti Veren Şirketler ve Pazaryerleri • Müzeler • Etkinlik Bileti Satan Platformlar / Şirketler • Kuyumcular • Meslek Odaları

4. DİJİTAL KİMLİK SERVİSLERİNİN ANA TASARIM PRENSİPLERİ

Dijital kimlik doğrulama servislerinin tasarımında 12 temel prensibin dikkate alınması önerilmektedir.

4.1. Mahremiyet Odaklı Olması

- » Kimlik bilgilerinin paylaşım detay ve süresinin kontrolü kullanıcıya ait olmalıdır.
- » Kişiye ait dijital kimlik bilgilerine kişi haricinde, Kanun tarafından açıkça yetkilendirilen kişiler haricinde, kimsenin erişim yetkisi olmamalıdır.
- » Bir kimlik bilgisinin herhangi bir alt kümesi, bilginin tümüne erişim yetkisi olanlar dahil tüm erişim sağlayanlardan gizlenebilmelidir.
- » Dijital kimlik sahibi, hukuki zorunluluk durumları haricinde, kimlik bilgilerini erişime kapalı tutabilmelidir.
- » Dijital kimlik sahibi, istediği kurum/kuruluş ile bilgilerini paylaşabilmeli ve/veya süreli veya süresiz olarak erişime açabilmelidir. Süreli veya süresiz paylaşım durumlarında, bilgilerin paylaşıldığı kurumun, bilgileri kendi sisteminde kalıcı olarak depolamayacağı garanti altına alınmalıdır.
- » Kimlik bilgisi sadece ilgili işlem için kullanılmalı, aynı kişinin daha önce elde edilmiş olan farklı kimlik bilgilerinin birbirleriyle ilişkilendirilemeyecek şekilde işlenmesini sağlayacak tedbirler alınmalıdır.
- » Kimlik bilgisinin yanlışlıkla veya gereksiz yere ifşa edilmesine karşı koruma önlemleri olmalıdır.
- » Kimlik bilgileri, bir işlemin gerçekleştirilme amacıyla bağlantılı, orantılı ve ölçülü bir şekilde talep edilmeli ve işlenmelidir.
- » Kimlik bilgilerine erişim talepleri kapsamında, ihtiyacı karşılayacak (minimum) miktarda kimlik verisinin paylaşılması garanti altına alınmalıdır/sağlanmalıdır.
- » Başta 6698 sayılı Kişisel Verilerin Korunması Kanunu ile ikincil düzenlemeleri ve Kişisel Verileri Koruma Kurumu'nun rehberleri ile Kurulu'nun ilke kararlarına ve diğer ilgili ulusal ve uluslararası yasal düzenlemelere uyumlu olmalıdır.

4.2. Güvenlik

- » İlgili kurumlar tarafından doğrulanmış verilerin kullanılması esastır. Ancak bilgiyi talep eden kurum doğrulanmış veri aramıyorsa kişi doğrulanmamış verisini de paylaşabilir
- » Siber saldırılara karşı dayanıklı olmalıdır. Sisteme saldırı durumlarının gözlemlenebileceği yetenekleri içerisinde barındırmalıdır. Kimlik yönetim sistemleri için siber saldırıya derhal müdahale edilebilecek güvenlik sistemi/ekipleri oluşturulmalıdır.
- » Dijital kimlik sisteminin paydaşı olmak isteyen kurum ve kuruluşların, sisteme güvenli dahil olması ile ilgili adımları tanımlayan standartlar hazırlanmalıdır.

» Dijital kimlik sistemi, kimlik bilgilerinin izinsiz okunmasını, değiştirilmesini, silinmesini ve çalınmasını önleyecek şekilde işlemelidir. Tanımlanmış yetki seviyesine uygun ölçüde değişiklik yapılması garanti edilmelidir.

4.3. Erişebilirlik ve Taşınabilirlik

- » Cihazdan ve işletim sisteminden bağımsız olmalıdır.
- » Yaygın olmalı, geniş kitleler tarafından ulaşılabilirlik.
- » Dijital kimlik verileri merkezi bir sistemde veya cihaz üzerinde tutulmamalı ancak mobil ortamdan kullanıcı tarafından erişilerek doğrulama talebi yapan kuruma süreli/süresiz kullanım hakkı verilmelidir
- » Uluslararası ve yerel standartlara uygun olmalıdır.
- » Taşınabilir ve coğrafi konumdan bağımsız bir şekilde erişilebilir olmalıdır.

4.4. Kullanıcı Odaklılık

- » Hizmet veya Kimlik Sağlayıcı merkezli değil, kullanıcı (kimlik sahibi) merkezli olmalıdır.
- » Kullanıcı kendi kimlik bilgilerinin paylaşım detaylarını yönetebilmelidir
- » Kullanıcı kimlik doğrulama için ekosistemde arzu ettiği servis sağlayıcıları kullanabilmelidir
- » Dijital kimlik sahibi, kimlik bilgilerini, istediği kurum/kuruluş ile paylaşabilmelidir. Bu bilgileri, kalıcı veya kısıtlı bir süre için kullanıma/erişime açıp kapatabilmelidir.

4.5. Şeffaflık

- » Paylaşılan bilgilerin kullanım amaç ve süreleri kullanıcı tarafından bilinir ve yönetilebilir olmalıdır.

4.6. Ölçeklenebilirlik

- » Sistemdeki ekosistem paydaşların ve işlemlerin sayısı arttıkça sistem performansı etkilenmemelidir.

4.7. Performans

- » Erişim hızı ve servis standartlarının ekosistem paydaşlarının işleyişini olumsuz etkilemeyecek şekilde olmalıdır.
- » Sistem, gereksinimleri ve standartları sürekli uyarlayacak ve sistem performansını izleyecek bir yönetim yapısına sahip olmalıdır.

4.8. Kullanılabilirlik

- » Basit ve anlaşılabilir olmalıdır.
- » Kullanıcıyı minimum şekilde müdahale etmek zorunda bırakmalıdır.

4.9. Birlikte Çalışabilirlik

- » Uluslararası standartlara uyumlu olmalıdır, yurt dışı ekosistem paydaşları ile gerektiğinde iş birliği yapabilmelidir
- » Kimlikler, kimlik yönetimi ile ilgili sistemler arasında kullanılabilir olmalıdır.
- » Farklı kurumların sisteme kolay entegre olabilmesi için uygun altyapıya sahip olmalıdır

4.10. Denetlenebilirlik

- » İşlem izinleri ispatlanabilir olmalıdır.
- » Bilgiler işlem kaydı olmadan değiştirilemez olmalıdır.
- » İşlem kayıtları güvenli tutulmalıdır ve denetlenebilir olmalıdır.

4.11. Esneklik

- » Teknoloji geliştikçe sistemin de güncellenme ihtiyacı olabilir. Sistemin güncellenmesine yönelik prosedürler belirlenmiş olmalıdır.

4.12. Kalıcılık

- » Sosyal, ekonomik, politik (ör: savaş), doğal koşullardan (ör: afet) etkilenmeyecek şekilde tasarlanmalı ve kalıcı olmalıdır

5. DİJİTAL KİMLİK YÖNETİM MODELLERİ

Dijital kimliğin yönetilebileceği dört farklı servis mimarisi bulunmaktadır.

- » **Merkezi:** Veri sahipliğinin ve kontrolünün tek bir merkezde olduğu, ekosistemdeki tüm paydaşların veriyi merkezi bir veritabanına beslediği ve aynı veritabanından kullandığı model.
- » **Federe:** Veri sahipliği ve kontrolünün ekosistemdeki belirli paydaşların yetkinliğinde olduğu, nihai kontrolün ise yine merkezi bir otorite tarafından sağlandığı model.
- » **Dağıtık:** Veri sahipliği ve kontrolünün kullanıcı inisiyatifinde olduğu, ekosistemdeki paydaşların kullanıcı izni ve onayı ile veriyi kullandığı ve birbirleriyle paylaştığı model.

Merkezi



Federe



Dağıtık



Kullanıcı-
Egemen



» **Kullanıcı Egemen:** Veri sahipliği ve kontrolünün tamamen kullanıcıda olduğu, ekosistemdeki paydaşların kullanıcıya dair hiçbir veriye sahip olmadığı model.

Diğer modellerin, gelecekte kullanım dışı kalabileceği değerlendirilmiştir.

Tüm kullanıcı bilgilerinin tek merkezde (ya da federe kurguyla tek merkezle ilgili olarak) toplanmasının 3.bölümde yer alan Tasarım Presiplerinden gerek mahremiyet, gerek şeffaflık prensipleriyle çeliştiği görülmektedir. Diğer yandan bilgi üretildiği yerde üretildiği amaca uygun iş ve hukuki kurallar doğrultusunda saklanır. Örneğin sağlık bilgisini sağlık kurumu, eğitim bilgisini eğitim kurumu, finansal bilgiyi finans kurumu saklar. Kullanım senaryolarında görüleceği üzere bir kimliğin özniteliklerinin oluştuğu ve kullanıldığı bir çok alan vardır.

Tasarım prensipleri ile uyumlu ve dünyada da genel trend olarak Dağıtık ve Kullanıcı Egemen çözümlerin tercih edilmesi nedeniyle raporda bunlar ele alınmıştır.

Ademi Merkezi (Dağıtık)

«Benim doğrulanabilir
bir kimliğim var»

Kullanıcı Egemen

«Ben kimim
diyorsam oyum»

VERİ SAHİPLİĞİ

- Kimlik bilgilerinin kontrolü, tamamen kullanıcının kendisindedir
- Ekosistemdeki paydaşlar kullanıcı izni ve onayı ile kimlik bilgisini / kişisel veriyi kullanır ve paylaşır
- Kimlik bilgileri parça parça farklı ekosistem paydaşlarında bulunur, hiçbir paydaş verinin tamamına sahip değildir
- Kullanıcının açık rızası ve birlikte çalışabilirlik (interoperability) özellikleri öne çıkar
- Kimlik bilgisi ilk oluşturulduğu yerde saklanır, kullanıcı talebiyle doğrulanır; ancak el değiştirmez

- Kimlik bilgilerinin kontrolü, tamamen kullanıcının kendisindedir
- Ekosistemdeki paydaşlar kullanıcıya dair hiçbir veriye sahip değildir
- Kullanıcı, kimlik ve şahsi verilerinin tek hakimi ve kullanımı hususunda tek yetkili mercidir
- Kullanıcının açık rızası esastır. Kimliğin sahibi kullanıcıdır. Kullanıcının kendisi kimlik yaratma ve iptal etme hakkına sahiptir.

KİMLİK

- Kullanıcı kendi kimliğini farklı hizmet sağlayıcıları üzerinde oluşturup tutabilir
- Kullanıcı kimlik bilgilerini dilediği kişi veya kurumlar ile paylaşabilir
- Bu model, merkezi kimlik modelinin, kimlik bilgilerinin kimlerle ve nasıl paylaşılacağı konusunda kullanıcının rızasının dikkate alındığı, tek elden kontrol edilen, birlikte çalışabilir kimliklerin olduğu modele dönüşmüş halidir. Kullanıcının kimlik verilerini oluşturduğu ve depoladığı sistemlere bağımlılığı bulunmaktadır

- Kimliğin taşınabilirliği esastır. Herhangi bir hizmet sağlayıcıya ve veri deposuna bağımlılık yoktur
- Kullanıcı kendi kimliğinin sağlayıcısı olabilir
- Kullanıcının kendisi veya başka bir yayımcı tarafından, bu kullanıcı hakkında, birden çok sayıda doğrulanabilir kimlik iddiası/önermesi (verifiable claim) hazırlanabilir
- Her hizmet sağlayıcı, hangi yayımcı tarafından hazırlanmış kimliklere güvенеceğine kendisi karar verir

6. DİJİTAL KİMLİK YÖNETİMİ ÇÖZÜMLERİNİN TEKNOLOJİK AÇIDAN DEĞERLENDİRİLMESİ

6.1. Merkezi / Dağıtık Teknolojiler

Dijital kimlik hizmetlerin, yaygın, kesintisiz ve yüksek doğrulukta sürdürülmesi amaçları için kişisel veri (kimlik bilgisi) yönetim modeli çok önemlidir. Bilginin merkezi ya da dağıtık tutulmasının aşağıdaki tabloda belirtildiği gibi avantaj ve dezavantajları vardır.

Merkezi olarak tutulan bilgilerin güncelliğini sağlamak daha kolay olsa da bu bilgilerin değiştirilmeye karşı güvenliği sağlanmalıdır. Beklenmedik durum ve saldırı altında, merkezi sistemlerin erişilebilirliğinin sağlanması da zordur.

Bilginin dağıtık yerlerde tutulması ise verinin güncelliği ile ilgili sorunları yanında getirecektir. Buna karşın dağıtık noktalardaki verinin yetkisiz değiştirilmesi çok daha zordur.

Kişisel verilerin dağıtık noktalarda tutulması, verilere erişilebilirliği de kolaylaştırmaktadır. Bununla birlikte, çok noktada tutulan kişisel verinin açığa çıkmasını engellemek daha zordur.

Tablo 4. **Merkezi ve Ademi Merkezi (Dağıtık) Sistemlerin Karşılaştırması**

	Merkezi Teknolojiler	Ademi Merkezi (Dağıtık) Teknolojiler
Avantajlar	- Yönetilmeleri daha kolaydır - Kişisel verilerin açığa çıkmasını önleme mekanizmalarını gerçekleştirmek daha kolaydır	- Bilgilerin dağıtık olarak tutulması yetkisiz değiştirme riskini azaltır - Bilgi farklı noktalardan edinilebileceği için erişilebilirliği sağlamak daha kolaydır
Dezavantajlar	- Barındırdıkları bilgilerin yetkisiz değiştirilme riskine karşı daha yüksek koruma gerektirir - Zayıf Bileşen (single point of failure) olmamaları için erişilebilir durumda tutulmaları daha maliyetlidir - İçeriden gelen tehditlere karşı koruma da gerekir	- Bilginin dağıtık noktalardaki tutarlılığını ve güncelliğini sağlamak için ek mekanizmalar gerekir - Kişisel verilerin açığa çıkmasını engellemek daha zordur

7. DİJİTAL KİMLİK YÖNETİMİ ÇÖZÜMLERİNDE «BLOCKCHAIN»

Blokzincir, dağıtık defter teknolojisinin (distributed ledger technology) bir gerçekleştirme yöntemidir. Kayıtlar/işlemler bir uzlaşma mekanizması yardımıyla dağıtık olarak birçok noktada tutulur. Böylelikle tüm kayıtlar, yüksek güvenlik gerektiren merkezi veri tabanlarında tutulmak yerine dağıtık noktalarda tutulur. Kullanılan kriptografik mekanizmalar sayesinde işlem kayıtlarının tutulduğu veri blokları zincir şeklinde birbirine bağlanır. Böylelikle, işlemler geri dönülemez ve değiştirilemez şekilde dağıtık noktalarda kayıt altına alınır.

Dağıtık sistemler ve veri tabanları uzun zamandır kullanılmaktadır.

Blokzincirin getirdiği en önemli yenilik ve değer, blokzincirde tutulan verilerin doğruluğuna olan güvendir.

Blokzincir teknolojisinin getirdiği avantajlar göz önünde bulundurulduğunda güvenli dijital kimlik yönetim sistemlerinin geliştirilmesinde yapıtaşı olarak kullanılabileceği görülmektedir.

Dünyada ve ülkemizde kişisel verileri korumasına verilen önem gittikçe artmaktadır. İlgili yönetmelikler ve kanunlar gereğince kişi ile ilişkilendirilen verilerin toplanmasında kişinin açık rızasını almak gerekmektedir. Ayrıca kişinin istemesi durumunda, kişisel bilgilerinin silinmesi de gerekmektedir. Bu nedenlerden dolayı blokzincir, kişisel bilgilerin kendilerinin değil fakat doğruluk ve erişim kanıtlarının tutulması amacı ile kullanılabileceği görülmektedir.

Verilerin yetkisiz olarak açığa çıkmasını önlemek için de kişisel verilerin bir kısmının blokzincir üzerinde tutulması, diğer kısımlarının blokzincir dışındaki sistemlerde tutulması ve/veya blokzincir üzerinde, verilerin ispatları, özetleri, şifreli hallerinin tutulması gibi stratejiler kullanılabilir.

Diğer yandan, blokzincir teknolojileri gelişim aşamasındadır. Ölçeklenebilir, güvenli uzlaşma mekanizmalarının geliştirilmesi, blokzincirin kullanılabilirliği açısından önem arz etmektedir. Uluslararası kabul görececek bir standart çözüm üzerinde çalışılması halinde yurtdışında da geçerli olabilecek bir sistem inşa edilebilmesi mümkündür.

8. NETLEŞTİRİLMESİ GEREKEN KRİTİK KONULAR

Dijital kimlik sisteminin kullanılabilir olması ve yaygınlaşabilmesi açısından aşağıdaki öncelikli konuların netleştirilmesi gerekmektedir. Bu konular 6 ana başlıkta gruplandırılarak detaylandırılmış olup kritik hususlar, çözüm bulunması gereken konular ve öneriler ileride değerlendirilmesi amacıyla belirtilmiştir. Söz konusu öneriler rehber niteliğinde olup yapılması gerekenlerin tamamını kapsamamaktadır.

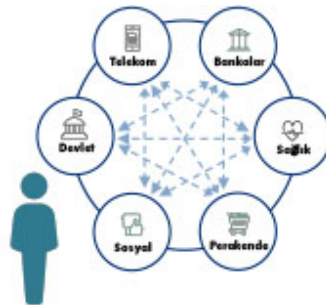
- 1. Teknik Model:** Temel prensiplere uygun yönetim modeli seçimi
- 2. İş Modeli:** Tüm paydaşları kapsayıcı ve koruyucu iş modeli oluşturulması
- 3. Standartlar:** Sistemin standartlara uygun olması
- 4. Hukuki Değerlendirme ve Regülasyon:** İlgili mevzuatlara uygun olması
- 5. Güvenlik ve Mahremiyet:** Tasarım aşamasından itibaren güvenlik ve mahremiyetin dikkate alınması
- 6. İş Akışı ve Hayat Döngüsünün Belirlenmesi:** Sistemin kolay kullanımı açısından sade ve anlaşılır olması

8.1. Teknik Model⁽¹⁾

Kimlik doğrulama sistemlerinin yönetim modelleri, Merkezi, Federe, Ademi Merkezi (Dağıtık) ve Kullanıcı-Egemen sistemler olarak çeşitlilik göstermektedir. Dünyada, mahremiyet odaklı dijital kimlik sistemlerinin kullanıcı egemen sistemlere doğru gittiği görülmektedir. Ulaşılmak istenen temel tasarım prensipleri çerçevesinde geliştirilecek dijital kimlik platformunda hedeflenecek mimari modele karar verilmelidir.

Bu model belirlenirken merkezi ve dağıtık sistemlerin Tablo 4’de belirtilen avantaj ve dezavantajlarının da dikkate alınması gereklidir. Belirlenecek model, sistemdeki kayıtların nerede tutulacağı, nasıl tutulacağı ve nasıl paylaşılacağını da etkileyecektir.

Günümüz sistemlerinin, hızlı değişen ihtiyaçlara cevap verebilmesi için çevik olması gereklidir. Bu kapsamda, sistemdeki gerekli güncellenmelerin hızlıca hayata geçirilebilmesi bir zorunluluktur. Söz konusu ihtiyaçların, teknik ve idari açıdan ele alınarak uygulamaya konması sağlayacak bir mekanizma kurgulaması gerekmektedir.



⁽¹⁾ World Bank. 2018. Technology Landscape for Digital Identification, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

8.2. Yönetişim ve İş Modeli⁽¹⁾

Çok paydaşlı, etkin ve verimli çalışan bir dijital kimlik sisteminin kurulması, farklı sektörlerden paydaşların bir araya gelmesini gerektirir. Bu paydaşların yatırım şekli ve miktarı, işletim kuralları, teknik standartlar gibi konularda hangi karar mekanizmalarını nasıl işleteceklerini de belirlemeleri gerekecektir. Böyle bir sistemi kurmak ve işler kılmak yatırım da gerektirir. Bu yatırımı yapmaya niyetli kurumlar belirlenmeli, yönetim yapısı oluşturulmalı ve ticari bir teşebbüs ortaya çıkmalıdır. Bu teşebbüsün kalıcılığını ve işleyecek olan dijital kimlik hizmetinin güvenilirliğini sağlayacak kalitede veri işlenmesi için servis paydaşlarına ticari gelir imkanı sunmalıdır.

Yönetişim ve iş modelini kurgularken aşağıdaki prensiplerin dikkate alınmasının gerektiği düşünülmektedir.

- 1.** Kurumların, hizmet verdiği her süreç için dijital kimlik sisteminden güncel bilgi almasını sağlayacak bir yapıya ihtiyaç olacaktır.
- 2.** Kurumlarca verilecek her hizmet için talep edilebilecek bilgi ihtiyacını sınırlayan asgari bilgi envanteri, kurum ve kuruluşlara ilgili bilgileri doğrulama konusunda yetkilendirme mekanizması ve güncel bilgilerin hangi kurumlardan sağlanacağı konusunda ilgili bir envanter tutulması faydalı olacaktır.
- 3.** Dijital kimlik kapsamında bireysel kullanıcıların paylaşmak istedikleri bilgileri bir panelden yönetmesi sağlanmalıdır. Ayrıca, kullanıcıların paylaşmak istemediği bilgilere yetkisiz erişimlerin engellenmesi sağlanmalıdır.
- 4.** Sistemin işletilmesi ve bütün paydaşların fayda sağlaması amacıyla bir gelir modeli belirlenmesine ihtiyaç bulunmaktadır. Bu amaçla, bilgiyi onaylayan kurum ve kuruluşlar ile veri sahibi olmayan ancak sistemi işleten kurum(lar) ücret talep edebilirler. Modelin belirlenmesi için fizibilite çalışması yapılması faydalı olacaktır.
- 5.** Gelişen ihtiyaçlar karşısında sistemde gerekli olabilecek değişikliklere karar verme yetkisine sahip bir yönetim şeklinin belirlenmesi gerekmektedir.

⁽¹⁾ World Bank. 2016. Digital identity : towards shared principles for public and private sector cooperation. Washington, D.C. : World Bank Group.

8.3. Standartlar

Geliştirilecek sistemin uluslararası ölçekte birlikte çalışabilir olması önemlidir. Bu amaçla, ulusal ve uluslararası standartlara uyumlu olmak gerekmektedir. Örneğin, AB'nin eIDAS⁽¹⁾ e-imza ve kimlik doğrulama standartları dikkate alınmalıdır.

Geliştirilecek dijital kimlik sisteminde aşağıdaki konuların ele alınması gerekmektedir.

Kategori	Konu	Detay Sorular
Açık Anahtar Altyapısı (PKI)	Kullanılacak PKI alt yapısı belirlenmelidir.	1. Merkezi PKI⁽²⁾ / Merkezi Olmayan PKI⁽³⁾ 2. Sertifika otoritesinin kim(ler) olacağı, nasıl yetkilendirileceği 3. Zaman-Damgası sağlanması⁽²⁾⁽⁴⁾ 4. Onaylayıcı/Doğrulamayı kurumlara sınırlı amaçlar için belge verme (imza atma) yetkisi sağlanması 5. Özel anahtarların güvenliğinin sağlanması
	Dijital kimliğin niteliği ve formatı belirlenmelidir.	1. Her ilişki türü için ayrı tekil belirleyici (Unique Identifier) 2. Her bir ilişki türü için ayrı tekil belirleyiciler (DID)⁽⁵⁾ (Sadece kişi ve “yetkili kurumlar” tekil belirleyicilerin kime ait olduğunu belirleyebilir, ilişkilendirebilir) 3. Belirleyicilerden dijital bilgi sahibinin (açık anahtar vb.) çözülme mekanizması 4. Bilgilerin güncellenmesi 5. İptal mekanizmaları
Dijital Bilgi / Belge	Dijital bilgi/belgelerin (doğrulanabilir bilgi) onaylanma ve doğrulanma mekanizmaları belirlenmelidir. ^{(6) (7)}	1. Merkez Yöntemleri: • Sadece yayınlayıcı/doğrulamayı kurumlar oluşturabilir 2. Ademi Merkezi (Dağıtık) Yöntemler: • Bilgi sahibi kendi oluşturabilir (assertion) • Yayınlayıcı/Doğrulamayı kurumdan onay alınır (attestation) 3. Dijital bilgi üzerindeki imza veya blokzincir üzerindeki verilerle doğrulanır. Gerektiğinde güvenilir kurumdan doğrulama istenir (validation) 4. Merkezi ve ademi merkezi (dağıtık) yöntemlerin birlikte kullanımı
	Dijital bilgi/belgeleri edinme ve doğrulamada yetkili servisleri tanıma/bulma mekanizması belirlenmelidir.	1. Servis kataloğu (Naming & Discovery) 2. Yetkilendirme mekanizmaları
	Dijital kimlik ve bilgi/belgelerin sahibinin kim olacağı belirlenmelidir.	1. Bilgi/belgeler kişiye aittir 2. Bilgi/belgeler yetkili devlet kurumlarına aittir 3. Bilgi/belgeler onaylayıcısı olan güvenilir kurumlara aittir 4. Bilgi/belgeler hizmet sağlayıcılara aittir
	Dijital bilgi/belgelerin geçerlilik süresi olmalıdır.	1. Değişmez bilgi/belgeler (Doğum belgesi, diploma vb.) • Süreli veya süresiz verilebilir • Gerektiğinde iptal edilebilir olmalı 2. Değişebilir bilgi/belgeler • Geçerlilik süresi tanımlanmalı • Geçerlilik süresi sona ermeden iptal edilebilmeli
	Dijital belgeler gerektiğinde öznede ki kişilerle ilişkilendirilebilmelidir	1. İlişkilendirmeyi sadece belge sahibi kişi yapabilir 2. İlişkilendirmeyi yetkili kurumlar yapabilir

Kategori	Konu	Detay Sorular
Dijital Bilgi / Belge	Dijital bilgi/belgeleri güvenli saklama mekanizmaları belirlenmelidir	1. Kişinin sahip olduğu cihazlardan çıkmayacak bilgi/belgeler (özel anahtar vb.) 2. Kişinin hizmet aldığı kurumlarda saklanan bilgi/belgeler 3. Blokzincir üzerinde saklanacak bilgi/belgeler 4. Bilgi/belgeleri yayınlayan/doğrulayan kurumlarda saklanan bilgi/belgeler
	Dijital bilgi/belgeleri edinme yöntemleri belirlenmelidir	1. Açık rıza yönetimi 2. Bilgi/belgelerin nereden alınacağı 3. Hangi bilgi/belgelere ihtiyaç olduğu 4. Ne kadar süreyle bu bilginin kullanılabileceği 5. Süreci kimin başlatacağı • Kişi tarafından başlatılabilir • Hizmet sağlayıcı tarafından başlatılabilir • Yetkili kurumlar tarafından başlatılabilir
	Dijital bilgi/belgelerin partiler arasında iletim yöntemi belirlenmelidir	1. Dijital bilgilerin sahibinden hizmet sağlayıcıya aktarımı 2. Onaylayıcı/doğrulayıcı üzerinden bilgi aktarımı 3. Block zincir üzerine yazılacak işlem bilgileri ile bilgi paylaşımı
	Dijital bilgi/belgelerin doğrulanması yöntemi belirlenmelidir	1. Hizmet sağlayıcı blokzincirdeki verileri kullanarak doğrulama yapabilir • Doğrulanabilir bilgiler geçerli olduğu sürece birden çok kullanılabilir 2. Yayınlayan kurumlar aracılığı ile doğrulama yapabilir • Her doğrulama için yayınlayıcı kurum ile iletişim gereklidir
Kayıt Olma	Sisteme kayıt olma noktaları belirlenmelidir.	1. Devlet kurumları 2. PTT 3. Bankalar 4. Operatörler vb.
	Sisteme giriş yapma noktaları belirlenmelidir.	1. Değişmez bilgi/belgeler (Doğum belgesi, diploma vb.) • Süreli veya süresiz verilebilir • Gerekğinde iptal edilebilir olmalı 2. Değişebilir bilgi/belgeler • Geçerlilik süresi tanımlanmalı • Geçerlilik süresi sona ermeden iptal edilebilmeli
	Dijital belgeler gerektiğinde öznedeki kişilerle ilişkilendirilebilmelidir	Giriş noktası ve yöntemine göre verilecek hizmetler sınırlandırılabilir 1. e-Devlet kapsı (parola, kimlik kartı, dijital imza, mobil imza) 2. Bankalar (İnternet bankacılığı) vb.
Block Zincir Modeli⁽¹⁾	Blokzincir modeli belirlenmelidir	1. Açık / Özel 2. İzimli / İzinsiz
Diğer	Doküman içerisinde DİJİTAL KİMLİK SİSTEMİ TEMEL TASARIM PRENSİPLERİ bölümünde yer alan prensiplerin sağlanması	

⁽¹⁾ eIDAS Regulation (EU) No 910/2014⁽²⁾ Public Key Infrastructure For Financial Services: <https://www.iso.org/standard/63134.html>⁽³⁾ Decentralized Key Management and DPKI: <https://bit.ly/2RCavx5> <https://bit.ly/1TEd4bB>⁽⁴⁾ Time Stamping on Blockchain: <https://chainpoint.org/>⁽⁵⁾ W3C DID Specifications: <https://w3c-ccg.github.io/did-spec/>⁽⁶⁾ W3C Verifiable Claims WG: <https://www.w3.org/2017/vc/WG/>⁽⁷⁾ W3C Verifiable Credentials Data Model 1.0: <https://w3c.github.io/vc-data-model/>⁽⁸⁾ NIST-IR 8202: Blockchain Technology Overview, <https://doi.org/10.6028/NIST.IR.8202>

8.4. Hukuki Değerlendirme ve Regülasyon

Gelişen ve değişen dünyada dijitalleşme süreçlerinin ivme kazanması ile birlikte bu hususta hukuk dünyasının da gelişmelere cevap verme mecburiyeti doğmaktadır. Yaşam ile birlikte evrilen sosyal bir dal olan hukuk, dijitalleşme ile oluşan ihtiyaçlara yetismeye çalışmaktadır. Başka bir ifade ile gelişmelerin beraberinde getirdiği ve öngörülen yeni sorunlar kapsamında mevcut hukuki düzenlemelerin geliştirilmesi ve değiştirilmesi beklenmektedir. Zira mevcut hukuki düzenlemeler, bugünün gereksinim ve yaşam modeli uyarınca insan odaklıdır, hukuki düzenlemelerin konu ettiği sorunlarda içinde insanı, insan eylemini, insan ve fiil icraatını barındırır. Oysaki dijitalleşme bunu tam tersini öngörmektedir. Dijitalleşme sürecinde düzenlemelerin temel aldığı insan faktörü yerine nesnelere, nesnelerin birbiriyle iletişimine, entegrasyonuna, yapay zekâya, yazılım ve donanımlarla kontrol edilen robotlara, insan gücüne dayalı olmaksızın çalışan akıllı fabrikalara bırakmaktadır. Hukuk sistemlerinde dijitalleşme süreçlerini takiben birçok konuda değişiklikler yapılıyor ve konu üzerinde mevzuat çalışmaları yapılmaktadır.

Dünyada dijitalleşme eğilimlerinin odak noktasını “veri” kavramı oluşturmaktadır. Bu verilerin kullanımı, işlenmesi süreçlerinde hukukun koruma çatısı altında olması gerekmekte olup aynı zamanda oluşturulacak veri tabanlı dijitalleşme alanı olan “dijital kimlik” kavramının düzenlenmesi gerekliliği ortaya çıkmıştır.

8.4.1. Dijital Kimlik Mevzuatının Yapılandırılması

Dünyadaki örneklerle ve Türkiye’deki gelişmelere bakıldığında Dijital Kimlik mevzuatının aşağıdaki gibi bir hiyerarşik yapıya sahip olduğu görülmektedir:

Yasama organı tarafından oluşturulan ve tüm kimlik sistemleri ile devlet tarafından tanımlanan yetkilere istinaden kimlik yönetim sistemi paydaşlarına uygulanan genel kanunlardır.

Bu kanunların düzenlediği ana konular kimlik sistemlerine ilişkin değildir. Ancak konuları itibarıyla sıklıkla kimlik yönetimi ve kimlik sistemlerini düzenleyen mekanizmaları barındırırlar ve kimlik işlemleriyle ilgili yetki ve kuralları belirlerler.

2018 yılı dijital kimlik sistemlerinin yaygınlaşması ve gelişmesi açısından birçok örneğe sahne oldu. Bu örneklerin önde gelenleri dijital ehliyet, mobil kimlik uygulamaları ve dijital pasaportları.

Dijital kimliğin en önemli düzenlemelerinden biri elektronik imzaya ilişkindir.

Ülkemizde, henüz dijital kimliğe ilişkin özel bir düzenleme bulunmuyor olsa da dijital kimliğe ilişkin temeller 23 Temmuz 2004 tarihinde yürürlüğe giren 5070 sayılı Elektronik İmza Kanunu (“E-İmza Kanunu”) ile atılmıştır. E-İmza Kanunu aynı zamanda güvenli elektronik imza ile elektronik imza arasındaki ayrıma ve zaman damgası, elektronik veri, elektronik sertifika gibi kavramların tanımları ile düzenlemelerine de yer vermektedir. E-İmza Kanunu’nun akabinde mobil elektronik imza konusunun da hukuki alt yapısı Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile oluşturulmuştur. Ülkemizde dijital kimlik sistemine uygulanabilecek genel ve kimlik özelinde yasal düzenlemeler arasında 4721 sayılı Türk

Medeni Kanunu, 5490 sayılı Nüfus Hizmetleri Kanunu, 5682 sayılı Pasaport Kanunu, 5901 sayılı Türk Vatandaşlığı Kanunu bulunmaktadır.

Bu düzenlemelerin yanı sıra, bir kimlik sisteminin çerçevesini oluşturan önemli bir dayanak noktası kişisel verilerin korunması ve gizliliğidir. Ülkemizde kişisel verilerin korunması 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil düzenlemeleri kapsamında düzenlenmektedir.

Dijital kimlik yönetim sistemlerinin doğası gereği bir riski vardır: Gözetleme için bir araç olarak kullanılabilirler. Kimlik yönetimi kaçınılmaz olarak, kullanıcının bulunduğu yeri, ne zaman bulunduğunu, kullandığı bilgi türünü, kimliğin kaç kez kullanıldığı vb. bilgileri edinebilir. Bu sorunlar, doğrudan kullanıcının gizlilik alanına etki eder. Tamamen dijital bir ekonomi geliştirmek istiyorsak, ülkelerin kimlik kayıt süreçlerinde toplanan kişisel özniteliklerin toplanması, depolanması ve paylaşılmasının güvenli ve uygun olduğunu garanti eden güçlü veri koruma yasaları oluşturması gerekmektedir.

8.5. Güvenlik ve Mahremiyet

Son yıllarda kişisel verilerin bilgisayar korsanlarınca çalındığını daha sık duymaya başladık. Bunun bir nedeni, internetin hayatımızın birçok alanına girmesiyle birlikte e-devlet, e-belediye, e-bankacılık, e-perakendecilik gibi internet üzerinden sağlanan hizmetlerin sayısının artmasıdır. Diğer bir neden olarak ise bu hizmetlerde yeterince güvenlik önlemi alınmaması gösterilebilir. Fakat kişisel verinin giderek daha büyük oranda açığa çıkmasının asıl nedeni hizmetleri/sistemleri tasarlarken mahremiyet odaklı düşünülmemesidir. Bu nedenle ISO 27001 gibi genel bilgi güvenliği standartları olmasına rağmen mahremiyet odaklı ISO 27018⁽²⁾ ve ISO 29100⁽³⁾ standartları yayınlanma ihtiyacı doğmuştur.

Dijital kimlik sistemleri, büyük miktarda veriyi depolamayı, işlemeyi ve paylaşmayı teknik olarak mümkün kılar. Bu kapsamda, eğitim, sağlık, finans, yer ve zaman gibi birçok kişisel veri işlenecektir. Bilgisayar korsanları için cazip birçok verinin işlendiği bu sistemler veri ihlallerine yatkın olmamalı, hizmetlerin durmasına sebep olabilecek zayıf bileşen haline gelmemelidir. Bu bağlamda mahremiyet, gizlilik, bütünlük, erişilebilirlik dörtlemesi ve siber güvenlik konuları dijital kimlik uygulamalarında göz önünde bulundurulması gereken temel konulardır. Kullanıcı verileri ve kişisel verileri de içeren kullanıcı gizliliği, mevcut yasalar (GDPR⁽¹⁾ ve KVKK⁽²⁾) ile uyumlu olarak korunmalıdır.

Günümüzde siber saldırılar hızlı bir şekilde artmaya devam etmektedir. Saldırganlar fikri mülkiyet hakları, kişisel veri, sağlık kayıtları, finansal veri gibi değerli verileri çalmayı hedeflerken gelişmiş fidye yazılımları kullanarak veri erişiminden para kazanma veya hizmet engelleme saldırılarıyla işletmeleri kesintiye uğratmak gibi yüksek kazançlı stratejilere başvurmaktadır.⁽³⁾ Bu saldırılar sonucunda bilgilerin yetkisiz kişilerin eline geçmesine ek olarak hizmetler kesintiye uğrarken, hem

⁽¹⁾ The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (EIDAS).

⁽²⁾ ISO Standard: Code of Practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

⁽³⁾ ISO Standard: Information technology, security techniques, privacy framework

vatandaş hem de işletmeler zarar görmektedir. Bu sebeple, dijital kimlik sistemi kurgulanırken mevcut tehditler ve riskler dikkatli bir şekilde belirlenmeli, siber saldırının etkisini en aza indireyecek stratejiler ve teknik önlemler alınmalıdır.

Blokzincir teknolojisinin doğası gereği merkezi bir kırılma noktası yoktur. Bu nedenle, kesintisiz hizmet verme potansiyelini artırmaktadır. Bu özellik aynı zamanda hizmet kesintilerine neden olan saldırılarının etkisini de büyük ölçüde azaltmaktadır.

Blokzincir, uzlaşmayı temel alarak çalıştığı için olası sahtekârlık faaliyetlerinin önlenmesini sağlar. Blokzincire yazılan veriler kullanılan kriptografik mekanizmalar nedeniyle değiştirilememektedir. Bu da blokzincirdeki verilere olan güveni artırmaktadır. Blokzincir teknolojisi, dijital kimlik sistemlerinde siber savunmanın geliştirilmesine büyük katkıda bulunabilir. Bununla birlikte, kullanıcı taraflarında (istemci/wallet uygulamalarının çalıştığı) siber riskler aynen devam etmektedir.

8.6. İş Akışı ve Hayat Döngüsünün Belirlenmesi

Dijital kimlik sistemi iş akışı ve hayat döngüsü oluşturulurken Bölüm 3'te önerilen Ana Tasarım Prensipleri göz önünde bulundurulmalıdır. Bu kapsamda yanıtlanması gereken sorulardan bazıları aşağıda belirtilmiştir.

- » Dijital kimliğin bir parçası olarak değişmesi daha zor olan biyometrik unsurlar kullanılmalı mı? (Cep telefonunda veya güvenlik aracında tutulan anahtarlara erişim vb. amaçlar için)
- » GSM numarası
 - Dijital kimliğin bir parçası olmalı mı?
 - Zorunlu tutulmalı mı?
- » Müşterini Tanı (KYC: Know Your Customer)'nin bir banka tarafından yapıldığı durumlarda;
- » Müşterisi olmadan başka bankalardan hizmet alınabilir mi?
 - Başka bankanın fiyatından döviz alım-satım işlemi yapılması vb. uygulamalarda kullanılabilir mi?
 - Diğer uygulanabilir işlemler belirlenebilir (Her ürün/hizmet için teknik açıdan mümkün olmayabilir).
- » Kişilerin dijital kimlik bilgilerini yönettiği sisteme erişime ilişkin bilgilerin unutulması, kullanılmaz hale gelmesi veya yetkisiz kişilerin eline geçmesi gibi durumların yaşam döngüsü ve anahtar yönetimi kapsamında ele alınması gerekmektedir.
 - Sisteme yeniden giriş nasıl olacak?
 - Yedekleme ve geri kazanma mekanizmalarının hem basit ve hızlı olması hem de sahtekarlıklara yol açmaması sağlanabilir mi?
- » Yedeklenen verinin sahipliği, korunması ve değiştirilebilirliği kişisel verileri riski atmadan adreslenebilir mi?
- » Müşteri tanıma sürecini (KYC) geçip sisteme hileli olarak girmiş bir kimliğin dağılmasının engellenmesi konusunda önlemlerin alınması

9. YURT DIŞI DİJİTAL KİMLİK ÖRNEKLERİ

Yakın gelecekte tüm sektörlerdeki iş yapış biçimini değiştireceği öngörülen trend teknolojilerden Blockzincir, barındırdığı potansiyel nedeniyle pek çok farklı kullanım alanına ait örneğe sahiptir.

Ticari işlemlerin kurallarını otomatik bir şekilde kontrol edilebileceği akıllı sözleşmeler, bir varlığın mülkiyetini parçalara bölerek dijital tokenlaştırma, üretim bileşenleri ve süreçlerini blockzincir ile depolayarak tedarik süreçlerini iyileştirmek, IoT platformlarında güvenliği Blockzincir sistemi ile sağlamak ve daha pek çok kullanım alanı bunlardan sadece birkaçını oluşturmaktadır.

Dijital dünyanın temel ihtiyaç noktalarından olan kimlik kavramı ve bu kavramdan yola çıkılarak örnekler geliştirilen “Dijital Kimlik” kullanım senaryosu da blok zincir alt yapısının en önemli kullanım alanlarındanıdır.



uPort, New York, ABD

http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

- 3 ana bileşenden oluşmaktadır: Akıllı sözleşmeler, geliştirici kütüphaneleri ve mobil uygulama.
- Kimlikler, kendi kendine egemen yani içerik sahibinin tamamen sahip olduğu ve kontrol ettiği, oluşturma veya onaylama için merkezi üçüncü taraflara güvenmediği yapıdadır
- Kimlikler, Blockzincir etkileşimine sahip olduklarından kripto para birimleri veya diğer tokenize edilmiş varlıklar gibi dijital taşıyıcı varlıkları da kontrol edebilir
- Ethereum'a dayalı bir dijital kimlik sistemi

Verified.Me, Toronto, Canada ⁽⁴⁾

<https://verified.me/>

- SecureKey Technologies Inc. tarafından geliştirilmiş Blockzincir tabanlı dijital kimlik platformu
- Kimlik bilgilerinin güvenli ve çevrimiçi olarak sahipleri tarafından doğrulanmasını ve telefonda çevrimiçi olarak istenilen hizmetlere ya da ürünlere ulaşılmasını hedefler
- Ekosistemindeki ortakları arasında Desjardins, National Bank ve Kanada'daki Big Five bankaları bulunmaktadır
- Hyperledger'e dayalı bir dijital kimlik sistemi

CIVIC, San Francisco, ABD

<https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf>

- Kişilerin kimlik bilgilerinin kullanımını kontrol etmelerine izin veren platform, kişisel bilgi aktarımını güvence altına almak ve korumak için blockzincir kimlik doğrulama teknolojisini kullanır
- Mobil cihazlardaki blok zinciri ve biyometri ile merkezi olmayan mimarisi sayesinde, authentication çözümlerini kullanarak şifresiz yetkilendirmeyi hedefler
- Platformun road map'inde uluslararası KYC doğrulamaları için altyapı oluşturma bulunmaktadır
- Ethereum'a dayalı bir dijital kimlik sistemi

AADHAAR. Hindistan ⁽¹⁾

<https://uidai.gov.in/>

- Vatandaşlarının biyometrik (iris ve parmak izleri) ve demografik verilerini barındıran, yasal bir otorite olan UIDAI tarafından yönetilen biyometrik kimlik platformu
- Dijital kimlik bilgileri Aadhaar Numarası (Ulusal Kimlik Numarası) kullanılarak Blockzincir mimarisinde depolanır
- Kullanıcılar tarafından yapılan her işlem anahtarları ve her işlem sonrasında üretilen özel anahtarlar imha edilir
- Özel (Private) Blockzincir'e dayalı bir dijital kimlik sistemi

IDHub, Beijing, Çin

http://www.idhub.network/IDHub_whitepaper_v0.5.0_en.pdf

- Akıllı sözleşmelerle merkezi olmayan blok zinciri ve gizlilik korumasından faydalanır, kullanıcılara kimlik egemenliği kazandırmaktadır
- Tasarım ilkeleri egemenlik, güvenlik ve gizlilik
- Blok zinciri mimarisinin ve NaCl gibi şifreleme kitaplığının değişmezliği ile kullanıcı kimlik bilgilerinin güvenliği ve gizliliği Kademlia gibi dağıtık depolama ile sağlanmaktadır
- Özel (Private) Blockzincir'e dayalı bir dijital kimlik sistemi

ID2020, Uluslararası ⁽²⁾

<https://id2020.org/>

- Dijital kimlikle yaşamı iyileştirmeye kendini adanmış küresel bir kamu-özel ortaklığıdır
- İttifak, kullanıcının sahip olduğu ve kontrol ettiği güvenli bir dijital kimlik için teknik standartları belirlemek üzere çok uluslu, kar amacı güden ve kar amacı gütmeyen kurumları ve hükümetleri bir araya getirmektedir. Aynı zamanda korunmasız topluluklara dijital kimlik sağlayan pilot projeleri finanse etmektedir
- Ethereum'a dayalı bir dijital kimlik sistemi

Sovrin, Uluslararası ⁽³⁾

<https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf>

- Analog kimliklerin dijital kimliklere dönüştürülebilmesi için tasarlanmış yeni bir standarttır
- İnsanlara, kuruluşlara ve kendi yaşamları boyu doğrulanabilir dijital kimlik bilgilerini toplama ve taşıma özgürlüğü sağlanması hedeflenmektedir
- "Self-sovereign" kavramı ile bireysel kimlik sahibinin istediği zaman ağ üzerindeki kimlik bilgilerine erişip kullanabilmesi amaçlanmaktadır
- Açık ve izine dayalı bir dijital kimlik sistemi

⁽¹⁾ https://www.emudhra.com/case-studies/Whitepaper_Blockchain.pdf

<https://www.mygov.in/frontendgeneral/pdf/white-paper-mobile-as-digital-identity-v0-2.pdf>

⁽²⁾ https://static1.squarespace.com/static/578015396a4963f7d4413498/t/5b4f6273575d1feb288ae0a5/1531929204374/ID2020%2BAlliance%2BDoc_UPDATED.pdf

⁽³⁾ <https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf>

⁽⁴⁾ <https://2m6dv3zi6nj31h9a91s1wdk-wpengine.netdna-ssl.com/wp-content/uploads/2018/05/Case-Study-government-of-canada.pdf>

<https://securekey.com/digital-id-ecosystem/>

SONUÇ

Çok hızlı teknolojik değişimin yaşandığı çağımızda, dijital kimlik, kişi ve kurumlar için önemli değer yaratma fırsatı sunmaktadır. McKinsey¹ raporuna göre dijital kimlik ile yeni müşteri kazanım süreçlerinde %90'a varan maliyet avantajı sağlanacağını ve daha fazla kişinin finansal sisteme dahil olabilmesi mümkün hale geliyor.

Dijital kimliklerin; kişisel olması ve kimlik sahibi tarafından yönetilmesi, her yerden her zaman ulaşılabilir olması, kalıcı olması ve herkesi kapsaması özellikleri öne çıkmaktadır.

Başarılı dünya örneklerinden, tasarım prensiplerden ve kimlik yönetim modellerinden yola çıkıldığında dijital kimlik hizmetlerini yönetebilmenin en uygun yolunun dağıtık yapılarda işbirlikleri çerçevesinde yapılmasının sürdürülebilir bir dijital kimlik projesi için kaçınılmaz olduğu görülmektedir. Ülkemizde de başka pek çok konuda örnekleri olduğu gibi kolektif bir çalışma örneğinin bu alanda da hayata geçmesini ve daha dijital bir Türkiye'ye ulaşmak en büyük dileğimizdir.

⁽¹⁾ MGI Digital Identification

TANIMLAR SÖZLÜĞÜ

- » **Ekosistem:** Belirli bir alanda bulunan gerçek ve tüzel paydaşlar ile bunlar arasındaki etkileşimlerden oluşan yapıdır.
- » **Kullanım Senaryosu:** Dijital kimliğin, ilgili paydaşlar ile bu paydaşlar arasındaki ilişkiyi de gösterecek şekilde, ekosistem içerisindeki kullanım alanıdır.
- » **Issuer:** Bilgiyi oluşturan kişidir.
- » **Açık Anahtar Altyapısı:** Dijital imza amacı ile kullanılan anahtarların yaşam döngüsü boyunca yönetimini (anahtar düzenleme, iptal etme vb.) sağlayan altyapıdır. Merkezi, hiyerarşik ya da ademi merkezi (dağıtık) olarak modellenebilir. (İng. PKI: Public Key Infrastructure)
- » **Anahtar Yönetimi:** Sistemdeki tüm anahtarların yönetimini sağlayan mekanizmalardır. Merkezi veya ademi merkezi (dağıtık) olarak modellenebilir. (İng. Key Management)
- » **Zaman Damgası:** Dijital verinin belirli bir tarihten önce var olduğunu kanıtlayan veridir. Sertifika otoritesi tarafından veya blokzincir kullanarak sağlanabilir. (İng. Time Stamp)
- » **Tekil Belirleyici:** Sistemdeki kişilerin tekil olarak ayırmaya yarar, örnek olarak, T.C. Kimlik numarası verilebilir. Bu amaçla açık anahtarlar veya özeti kullanılabilir. (İng. Unique Identifier)
- » **Doğrulanabilir Bilgi/Belge:** W3C Verifiable Claims çalışma grubu tarafından hazırlanmaktadır. Kişi hakkındaki bilgi vermeye yetkili kurum kuruluş tarafından onaylanan, kriptografik olarak güçlü güvenlik sağlayan, mahremiyeti koruyabilen ve makine tarafından doğrulanabilen veri kümesidir. (İng. Verifiable Claims/Credentials)
- » **NFC (Near-field Communication):** Birkaç santimetre uzaklıktaki iki cihaz arasında küçük miktarda veri transferi gerçekleştirebilmeyi sağlayan bir teknolojidir.
- » **W3C:** World Wide Web Consortium
- » **KVKK:** 6698 Sayılı Kişisel Verilerin Korunması Kanunu
- » **GDPR:** European Union General Data Protection Regulation

KATKI SAĞLAYAN KİŞİLER

Demet Memiş

Accenture

Mehmet Albayrak

Murat Bitirici

Akbank

Mustafa Saraç

Albaraka Türk Katılım Bankası

İsmail Özeren

Anadolu Sigorta

Emek Akbak

Avivasa

Celal Cündoğlu

Özge Çelik

BKM

Emel Özgümüş

Deloitte

Şahika Mut

Can Orhun

E-güven

Ufuk Özkan

Elif Ülger Göktaş

Ford Otomotiv Sanayi AŞ

Itır Ürünay Aydoğan

Efe Kaşoğlu

Arda Çolak

Garanti Bankası

Fırat Dürüst

Tolga Gümüş

Halim Memiş

Boğaç Devrimci

İş Bankası

Erman Taylan

Koç Finans

Gökhan Murtezaoglu

Koç Sistem

Merve Can Kuş

Hasan Özkul

Kuveyt Türk

Seda Akdemir

Ferhat Dilman

Duygu Ateş

Microsoft

Av. Dr. Çiğdem Ayözger Öngün

Av. Begüm Ertürk

SRP-Legal Hukuk Bürosu

Darço Akkaranfil

İbrahim Kara

Umut Esen

Didem Gökçe Güçkıran

Softtech

Av. Çağhan Tansel
TANSEL Danışmanlık & Hukuk

Erdal Çokol
TEB

Gürcan Erim
Turkcell

Fatih Birinci
Dr. Oktay Adalier
Taner Dursun
Gökhan Abbasoğlu
Mustafa Selvi
TÜBİTAK BİLGEM

İbrahim Niyazi Ülgür,
Mehmet Kıvılcım Keleş
Şükrü Çakmak
Arge ve İnovasyon Müdürlüğü - Vakıfbank

Esat Belhan
Umut Keçecioğlu
Yapı Kredi Bankası

KAMU HİZMETLERİ EKOSİSTEMİ KULLANIM SENARYOLARI

Sıra	Kullanım Senaryosu Tanımı	Kullanım Senaryosu			Faydalar
		Kullanımda Olmayan Bilgiler	Bilgi / Doğrulanan Faydalar	Bilgi / Zenginleşen Faydalar	Bilgi / Kullanılan Faydalar
1	Emlak Başvurusu	* TCNO * Doğum Tarihi * Eğitim Durumu * Sağlık Raporu * Statü Kurum Tanımlama Bilgisi * Harç Makbuzu * Dilekçe Örneği Emlak Sınıfı * Davacı / Davalı TCNO * Adres * Yanılama Harcı Ödemesi * Davaya Konu Dilekçe * TCNO * Doğum Tarihi * Doğum Sınıfı * Cinsiyet * Boy ve Kilo * Anne Adı * Akı ve Salko İçin TCNO, İsim, Soyad * Gayrimenkulün Adres Bilgisi, Patna no, Ada no, Parsel no, Yüz ölçümü, Sığır binaları, İşlem tarihi	* Paszeler * Statü Kurum * Nüfus ve Vatandaşlık İşleri (NVI) * Paszeler * MİE Eğitim Bilançosu (MEB) * NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
2	Araç İşlemleri / Davacı Açma	* TCNO * Doğum Tarihi * Doğum Sınıfı * Cinsiyet * Boy ve Kilo * Anne Adı * Akı ve Salko İçin TCNO, İsim, Soyad * Gayrimenkulün Adres Bilgisi, Patna no, Ada no, Parsel no, Yüz ölçümü, Sığır binaları, İşlem tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
3	İkametgah Bilgisi / Alınması	* TCNO * Doğum Tarihi * Doğum Sınıfı * Cinsiyet * Boy ve Kilo * Anne Adı * Akı ve Salko İçin TCNO, İsim, Soyad * Gayrimenkulün Adres Bilgisi, Patna no, Ada no, Parsel no, Yüz ölçümü, Sığır binaları, İşlem tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
4	Doğum Bilgisi Alınması	* TCNO * Doğum Tarihi * Doğum Sınıfı * Cinsiyet * Boy ve Kilo * Anne Adı * Akı ve Salko İçin TCNO, İsim, Soyad * Gayrimenkulün Adres Bilgisi, Patna no, Ada no, Parsel no, Yüz ölçümü, Sığır binaları, İşlem tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
5	Tapu Davası	* TCNO, İsim, Soyad * Emlak Tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
6	EmlakÇözüm Alınması	* TCNO, İsim, Soyad * Emlak Tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
7	Sporcu Lisans Alınması	* TCNO, İsim, Soyad * Doğum Tarihi * Doğum Sınıfı * Cinsiyet * Boy ve Kilo * Anne Adı * Akı ve Salko İçin TCNO, İsim, Soyad * Gayrimenkulün Adres Bilgisi, Patna no, Ada no, Parsel no, Yüz ölçümü, Sığır binaları, İşlem tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
8	E-Devlet Sistemine Giriş	* TCNO * Doğum Tarihi * Doğum Sınıfı * Cinsiyet * Boy ve Kilo * Anne Adı * Akı ve Salko İçin TCNO, İsim, Soyad * Gayrimenkulün Adres Bilgisi, Patna no, Ada no, Parsel no, Yüz ölçümü, Sığır binaları, İşlem tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
9	Vatandaş İşlemleri	* TCNO * Doğum Tarihi * Doğum Sınıfı * Cinsiyet * Boy ve Kilo * Anne Adı * Akı ve Salko İçin TCNO, İsim, Soyad * Gayrimenkulün Adres Bilgisi, Patna no, Ada no, Parsel no, Yüz ölçümü, Sığır binaları, İşlem tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
10	İşlem Alın / Sığır Başvurusu	* TCNO * Doğum Tarihi * Doğum Sınıfı * Cinsiyet * Boy ve Kilo * Anne Adı * Akı ve Salko İçin TCNO, İsim, Soyad * Gayrimenkulün Adres Bilgisi, Patna no, Ada no, Parsel no, Yüz ölçümü, Sığır binaları, İşlem tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI
11	Yeni ve Cezalı Ödemeleri	* TCNO * Doğum Tarihi * Doğum Sınıfı * Cinsiyet * Boy ve Kilo * Anne Adı * Akı ve Salko İçin TCNO, İsim, Soyad * Gayrimenkulün Adres Bilgisi, Patna no, Ada no, Parsel no, Yüz ölçümü, Sığır binaları, İşlem tarihi	* NVI * Paszeler * Gıda Kurumu (GİB) * E-Devlet * NVI * Paszeler * Sağlık Bakanlığı	* Emlak Genel Müdürlüğü (EOM) * NVI	* NVI

[illegible][illegible]

SAĞLIK EKOSİSTEMİ KULLANIM SENARYOLARI

Sıra	Kullanım Senaryosu Tanımı		Paydaşlar	
	Kullanım Senaryosu Tanımı	Kullanılacak Dijital Kimlik Bilgileri	Bilgiyi Doğrulayan Paydaşlar	Bilgiyi Zenginleştirilen Paydaşlar
1	Elektronik Raporla Olupunulması	*TCKN, İsim, Soyadı	*Doktorlar	*Doktorlar
		*İlaç Adı ve Adıd	*Hastaneler ve Sağlık Kuruluşları	*Hastaneler ve Sağlık Kuruluşları
		*Kullanım Bilgisi		*Eczaneler
		*Raporla Düzeltiyen Doktor ve Sağlık Kuruluşu Bilgileri (doktor no, kurum adı vb.)		*Sağlık Bakanlığı
2	Sağlık Raporu Alınması	*Olupunulma Tarihi		
		*TCKN, İsim, Soyadı	*Doktorlar / Sağlık Hizmetleri	*Doktorlar
		*Sağlık Durumu Bilgisi	*Hastaneler ve Sağlık Kuruluşları	*Hastaneler ve Sağlık Kuruluşları
		*Düzeltiyen Doktor veya Hekim Verilme Tarihi		*Eczaneler ve Sağlık Kuruluşları
3	İlgilenecek Bilgileri Alınması			
		*TCKN, İsim, Soyadı	*Doktorlar / Sağlık Hizmetleri	*Hastaneler ve Sağlık Kuruluşları
		*Sağlık Durumu Bilgisi	*Hastaneler ve Sağlık Kuruluşları	*Hastaneler ve Sağlık Kuruluşları
		*Düzeltiyen Doktor veya Hekim Verilme Tarihi		*Eczaneler ve Sağlık Kuruluşları
4	Sağlık Kuruluşlarında Müeyyene Olmak	*İlaç Başlama Tarihi		
		*TCKN	*SGK	*Hastaneler, Sağlık Kuruluşları ve Doktorlar
		*İlaç Başlama Tarihi	*SGK	*Hastaneler, Sağlık Kuruluşları ve Doktorlar
		*Sağlık Durumu Bilgisi	*SGK	*Eczaneler
5	Eczanelerden İlaç Alınması	*Hastane Geçmiş		
		*TCKN	*SGK	*Eczaneler
		*Sağlık Durumu Bilgisi	*SGK	*SGK
		*İlaç Adı ve Adıd	*Hastaneler, Sağlık Kuruluşları ve Doktorlar	
6	Laboratuvar Talepleri	*Klinik Karar veya Diğ. Karar Numarası		
		*TCKN	*SGK	*Laboratuvarlar
		*Sağlık Durumu Bilgisi	*SGK	
		*Raporla / Talebi Talebi	*SGK	
7	Provizyon Alınması			
		*Sağlık Durumu Bilgisi	*SGK	*Hastaneler, Sağlık Kuruluşları ve Doktorlar
		*Hastane / Doktor Bilgileri	*SGK	*Hastaneler, Sağlık Kuruluşları ve Doktorlar
		*Teşhis / Tanı Bilgileri		
8	Hastane Ziyareti	*TCKN		
		*Alacaklar / Yatırım Bilgisi	*KPS	*Hastaneler, Sağlık Kuruluşları ve Doktorlar
		*TCKN, İsim, Soyadı		
		*Alacaklar / Yatırım Bilgisi		
9	Materyaller için Dijital Kimlik ile Sağlık Bilgi Verilmesi / Sağlık Hizmeti Verilmesi	*TCKN, İsim, Soyadı		
		*Sağlık Bilgileri	*Materyallerin gelip gideni için kurumu	
		*Sağlık Bilgileri		
		*Sağlık Bilgileri		
10	Doktorlar için Dijital Kimlik ile Sağlık Bilgi Verilmesi / Sağlık Hizmeti Alınması	*TCKN, İsim, Soyadı		
		*Sağlık Bilgileri	*Materyallerin gelip gideni için kurumu	
		*Sağlık Bilgileri		
		*Sağlık Bilgileri		

EĞİTİM EKOSİSTEMİ KULLANIM SENARYOLARI

Sıra	Kullanım Senaryosu		Paydaşlar	
	Kullanım Senaryosu Tanımı	Kullanılacak Dijital Kimlik Bilgileri	Diğer Doğrulayan Paydaşlar	Diğer Zenginleştirici Paydaşlar
1	Diploma Alınması	* TOKN, İm, Soyadı * Okul * Diploma No.lu	* MEB * Yükseköğretim Kurulu (YÖK)	* Şirketler * Kamu Kurumları * Meslek Odaları * Okullar
2	Transcript Alınması	* TOKN, İm, Soyadı * Okul * Öğretim Yılı ve Dönemi * Dersler	* MEB * Yükseköğretim Kurulu (YÖK) * Okullar	* Şirketler * Kamu Kurumları * Meslek Odaları * Okullar
3	Okul veya (Zorunlu Eğitim Dönemi)	* İkametgah Bilgileri * Nüfus Bilgileri * Kimlik Bilgileri * Fotoğraf * Veli Kimlik Bilgileri	* Nüfus İl Müdürlüğü * E-Devlet Veri Tabanı	* Okul * MEB
4	Öğrencinin beşer bir eğitim kurumuna maddi	* İkametgah Bilgileri * Nüfus Bilgileri * Kimlik Bilgileri * Fotoğraf * Öğrencinin 18 yaş altı olması halinde Veli Kimlik Bilgileri	* Nüfus İl Müdürlüğü * E-Devlet Veri Tabanı	* Okul * MEB
5	Yurt Kaydı	* Sağlık Bilgileri * Aile Hekimliği Durumu Bilgi Bilgi * Fotoğraf * Veli ve öğrenciye ait İkametgah Bilgileri	* SGK * Resmi Sağlık Kurumları * Banka	* Öğrenci Yurdu
6	Öğrencinin girişimci olarak Adaylığını Fiksal Olarak Doğrulamak Amaçlı	* TOKN, İm, Soyadı * Biyometrik Fotoğraf	* Mülkiyet * OSYM Başvurusu	* Okullar * OSYM
7	Mülteciler için Dijital Kimlik ile Eğitim Bilgilerine Ulaşımları	* TOKN, İm, Soyadı * Okul * Transcription Bilgileri	* Mültecilerin geçiştiği devlet yurt kurumu	* Şirketler * Kamu Kurumları * Meslek Odaları * Okullar * OSYM
8	Göçmenler için Dijital Kimlik ile Eğitim Bilgilerine Ulaşımları	* TOKN, İm, Soyadı * Okul * Transcription Bilgileri	* Mültecilerin geçiştiği devlet yurt kurumu	* Şirketler * Kamu Kurumları * Meslek Odaları * Okullar * OSYM
9	KYK Başvurusu	* TOKN, İm, Soyadı * Okul	* OSYM Başvurusu	* Yurtlar

İLETİŞİM ve ULAŞIM/KONAKLAMA EKOSİSTEMİ KULLANIM SENARYOLARI

Ekosistem	Sıra	Kullanıcı Senaryosu		Paydaşlar		
		Kullanıcı Senaryosu Tanımı	Kullanıcının Dijital Kimlik Bilgileri	Bilgiyi Doğrulayan Paydaşlar	Bilgiyi Zenginleştirilen Paydaşlar	Bilgiyi Kullanan Paydaşlar
İletişim	1	Akronik İşlemler (Araba, bilet, iptal vb.)	* TOKN * Adres, İletişim Bilgileri	* Bankalar	* GSM Operatörleri * İnternet Sağlayıcıları * TV Uydusistemleri	* GSM Operatörleri * İnternet Sağlayıcıları * TV Uydusistemleri
	2	Mobil İnce Alınması	* TOKN, İsim, Soyadı * Doğum Yeri, Doğum Tarihi * GSM Numarası	* Bankalar * GSM Operatörleri	* Mobil İnce Sağlayıcıları (ör. E-Global)	* GSM Operatörleri
Ulaştırma & Konaklama	Sıra	Kullanıcı Senaryosu		Paydaşlar		
		Kullanıcı Senaryosu Tanımı		Kullanıcının Dijital Kimlik Bilgileri		
	1	Çoel Rezervasyonu ve Check-in İşlemi	* TOKN	* Bilgiyi Doğrulayan Paydaşlar * Bankalar * İPOS	* Çoel Rezervasyonu Yapılan Aracı Turizm Platformları / Şirketleri * Sipariş Şirketleri	* Çoel ve Turizm Şirketleri * Turizm Bakanlığı * Emniyet Genel Müdürlüğü * Hırsyolu / Otobüs / Tren İşleten Firmalar * Aracı Turizm Şirketleri * Emniyet Genel Müdürlüğü
	2	Yolculuk Bilgi Satın Alınak ve Hırsyalarında Check-in İşlemi	* TOKN	* Bankalar * İPOS	* Yolculuk Bilgi Satın Alınan Platformlar / Şirketler * Sipariş Şirketleri	
	3	Araba, Drone, Bilet vb. Ürünlerin Kiralaması	* TOKN * Eriyet Bilgileri	* Bankalar * İPOS * KCB (kredi skoru takip edilmesi durumunda) * Bankalar * E-Devlet * Kamu ve Çoel Sektör Kurumları * Ulaştırma ve Konaklama Hizmeti Veren Platformlar	* Sipariş Şirketleri	* Aracı Kiralamaya Platformları / Şirketler
	4	Mıza Başvurusunda Bulunmak	* TOKN			* Kurumca Kurum

PERAKENDE EKOSİSTEMİ KULLANIM SENARYOLARI

Sıra	Kullanım Senaryosu		Paydaşlar		
	Kullanım Senaryosu Tanımı	Kullanılacak Dijital Hesap Bilgileri	Bilgi Doğrulama Paydaşlar	Bilgi Zenginleştirme Paydaşlar	Bilgiyi Kullanan Paydaşlar
1	İnternette / Mağazadan Alışveriş Yapılması	* Ad, Soyadı * İletişim Bilgisi (adres, telefon e-mail) * Kredi Kartı / Debit Kart / Banka Hesabı Bilgisi * Ad, Soyadı	* Bankalar * Ödeme Kurumları * KPS * Bankalar	* E-Ticaret Şirketleri * Kargo Şirketleri	* E-Ticaret Şirketleri * Kargo Şirketleri
2	Sadıklat Programı Uygulanması (Meyin hak kullanım veya işlemi gerçekleştirilmesi vb.)	* GSM Numarası	* Ödeme Kurumları * KPS	* Sadıklat Programı Çan Firmalar	* Bankalar * Sadıklat Programı Çan Firmalar
3	Ulaştırması / Ticareti Karşılıklı Kredilike Sorulması:(finansal bilgileri beyan)	* Uzun Vergi Numarası * İletişim Bilgileri * Sicil & Faaliyet Bilgileri * Mali Bilgiler * Firma Ratingi	* Bankalar * Öd. Tirore Bankleri * KPS	* Bankalar * Öd. Tirore Bankleri	* İhtiyaçlar * İhtiyaçlar
4	Satış Karşı Öden Ücretin Satışı (ör. sığın, akıllı vb.)	* TOKN, Doğum Tarihi	* Bankalar * KPS		* İgi Ücretleri Satan Firmalar * İnternette Hizmet Sağlayan Firmalar
5	Capdata Kullanımı				

EV VE BARINMA EKOSİSTEMİ KULLANIM SENARYOLARI

Kullanım Senaryosu		Paydaşlar			
Sıra	Kullanım Senaryosu Tanımı	Kullanılacak Dijital Kimlik Bilgileri	Bilgiyi Doğrultan Paydaşlar	Bilgiyi Doğrultan Paydaşlar	Bilgiyi Kullanarak Fayda Sahipleri
1	Zorunlu Deprem Sigortası Yapılması	* TC Kimlik No Bilgisi	* Barındıran * Sigorta Şirketi		* Barındıran * Sigorta Şirketi
		* Gayrimenkul bilgileri			
		* Sigorta bağlanacağı tarih, Sigorta bedeli bilgisi			
		* Sigorta şirketi			
		* Sigorta numarası			
2	Evi Kiralama	* TC Kimlik No, Ad, Soyad, kimlik bilgisi, İmza Bilgisi (Mühür ve Mühür Bilgisi)	* Barındıran		* Elektronik(Dijital) Ağac Akıllılık ve Dağılım Şirketleri
		* Tapu Bilgileri			
		* Banka Hesap Bilgileri			
		* Kira ve Depozito Tutarı			
		* Kiralama Süresi			
3	Kurum Üyelik (istatistik, su vs.)	* Demirbaş Üstleri	* Barındıran		* Elektronik(Dijital) Ağac Akıllılık ve Dağılım Şirketleri
		* Kiralama Mühür Bilgisi			
		* TC Kimlik No			
		* Mühür Bilgisi			
		* Mühür Bilgisi			
4	Tapınma ve Raporlama	* İletişim ve Yeri Kimlik Adresi	* Barındıran		* Elektronik(Dijital) Ağac Akıllılık ve Dağılım Şirketleri
		* Tapınma Tarihi			

KÜLTÜR / EĞLENCE ve TİCARET EKOSİSTEMİ KULLANIM SENARYOLARI

Ekolasyon	Sıra	Kullanım Senaryosu Tanımı	Kullanım Senaryosu Tanımı	Paydaşlar	Paydaşlar	Paydaşlar
Kültür & Eğlence	1	Kullanım Senaryosu Tanımı	Kullanım Senaryosu Tanımı	Elgiz Doğruyazın Paydaşlar	Elgiz Zenginleşimin Paydaşlar	Elgiz / Kullanan Paydaşlar
	2	Elgiz Alınması	Elgiz Alınması			Paydaşlar
	3	Elgiz Alınması	Elgiz Alınması			Paydaşlar
Ticaret	1	Mağazanın Tazminatı	Mağazanın Tazminatı	Elgiz Doğruyazın Paydaşlar	Elgiz Zenginleşimin Paydaşlar	Elgiz / Kullanan Paydaşlar
	2	Mağazanın Tazminatı	Mağazanın Tazminatı			Paydaşlar
	3	Mağazanın Tazminatı	Mağazanın Tazminatı			Paydaşlar
	4	Mağazanın Tazminatı	Mağazanın Tazminatı			Paydaşlar
	5	Mağazanın Tazminatı	Mağazanın Tazminatı			Paydaşlar

SİGORTA EKOSİSTEMİ KULLANIM SENARYOLARI

Sıra	Kullanım Senaryosu		Paydaşlar		
	Kullanım Senaryosu Tanımı	Kullanılacak Dijital Kimlik Bilgileri	Büyük Doğrudan Paydaşlar	Büyük Zenginleştirici Paydaşlar	Büyük Kullanım Paydaşlar
1	Sigorta Bayıruunu Yapmak	* TC-KN	* Barhalar * Sigorta Şirketleri * DASK		* Sigorta Şirketleri * DASK
2	Sigorta Hizmet Talebinde Bulunmak	* Trafik Sigortası İçin Kaza Tespit * Tutarı, Sigorta Poliçesi, Sınır * Belgesi, Aray Ruhu ve Tespit Bilgileri	* Barhalar * Sigorta Şirketleri * DASK		* Emniyet Genel Müdürlüğü (EGM) * Hükümet ve Sağlık Kuruluşları * Sigorta Şirketleri * DASK * Aray Servisi



BLOCKCHAIN

T Ü R K İ Y E



T Ü R K İ Y E B İ L İ Ŗ İ M V A K F I