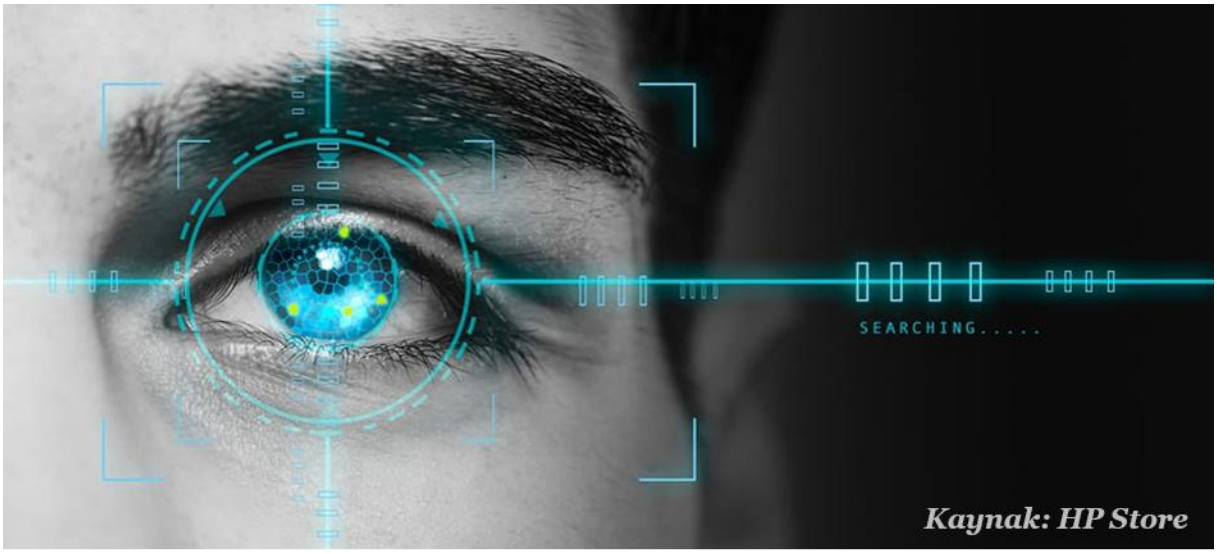
Elektronik Kimlik Trendleri

Kimlik hırsızları genellikle şifre, kimlik numarası, kredi kartı numarası veya sosyal güvenlik numarası gibi kişisel bilgileri ele geçirir ve bunları kurbanın adına sahtekârlık yapmak için kullanırlar. Bu hassas bilgiler, kredi başvurusu, çevrimiçi alışveriş veya kurbanın tıbbi ve finansal verilerine erişmek gibi çeşitli yasa dışı amaçlar için kullanılabilir.

Avrupa Komisyonu - Deloitte, Eylül 2018

Çeviren: Ercan Caner, Sun Savunma Net, 28 Temmuz 2021



Giriş

Elektronik kimlik (eID – Electronic Identification) alanı; güvenlik, veri gizliliği ve kolaylığa yönelik geniş çaplı küresel değişimler nedeniyle hızlı bir şekilde değişmekte, fiziksel ve sayısal dünyalar arasındaki hatlar ise giderek bulanıklaşmaktadır. Biyometri gibi uzun süredir kullanılan kimlik belirleme teknolojileri, sayısal kimliğe yönelik geleneksel yaklaşımları altüst etmek üzere yeni ortaya çıkan teknolojilerle birleşmektedir. Teknoloji alanındaki bu gelişme ve değişimler, hükümetlerin vatandaşlarına kimlik verme şeklini de derinden etkileyecektir.

Elektronik kimlik veya eID denildiğinde, çevrim içi hizmetlere erişmek veya çevrimiçi işlemler yapmak maksadıyla kişi veya kuruluşlar için bir kimlik kanıtı sağlayan sayısal bir çözümden bahsedilmektedir.

Bu makalenin amacı; eID'yi etkileyen mevcut teknolojilerin hâlihazır durumunun genel bir çerçevesini ortaya koymak ve kısa ile uzun vadede elektronik tanımlamanın geleceğini şekillendirecek olan temel trendleri kısaca özetlemektir. Devletler tarafından verilen eID'lerin, özel sayısal kimlik[i] çözümleriyle karşılaştırıldıklarında uygulanabilir olmalarını sağlamak ve kullanılabilirlik ile güvenlik açılarından da

vatandaşların ihtiyaçlarına uygun olarak kalmalarını sağlamak maksadıyla politika belirleyicilerin eID alanında beklenen gelişimi anlamaları çok önemlidir.

Her ne kadar bir kişinin kimliğini kanıtlamak için kullanılan biyometri, akıllı kartlar[ii] ve mobil uygulamalar gibi araçları etkileyen temel teknolojileri ya da belirli bir program kapsamında verilen kimliklere güven duyulmasını sağlayan blok zinciri[iii] teknolojileri belirlenebilse de bu teknolojiler birbirlerinden bağımsız olarak değil, bir bütün olarak analiz edilmelidirler. Bu nedenle bu makale; eID gelişimi üzerinde etkileri olan çok daha geniş toplumsal, ekonomik, politik ve teknolojik faktörleri de incelemektedir.

Biyometrik Kimlik Doğrulamada İris Tabakası ve parmak İzi Uygulamaları

İşte bu nedenle; teknolojik uygulamaların yükseliş ve düşüşü ile hızlı değişimi ile karakterize edilen bu ortamda, politika belirleyicilere çok önemli ve oynaması gerçekten zor bir görev düşmektedir. Politika belirleyiciler bu teknolojilerin gelişmesi için doğru ortamı oluştururken, işletmeler ve vatandaşların da bu teknolojilere erişmesi ve faydalanmasını sağlamaları ve onları riskler ile oluşabilecek zararlara karşı korumaları gerekmektedir. Bu makale, 2018 yılı başlarında kimlik ve erişim yönetimi, siber risk danışmanlığı, sistem mimarisi, hizmet tasarımı ve iş stratejisinin yanı sıra politika ile düzenleyici meseleler konularında, alanlarında uzman kişilerle yapılan bir çalıştaya dayanmaktadır.[iv]

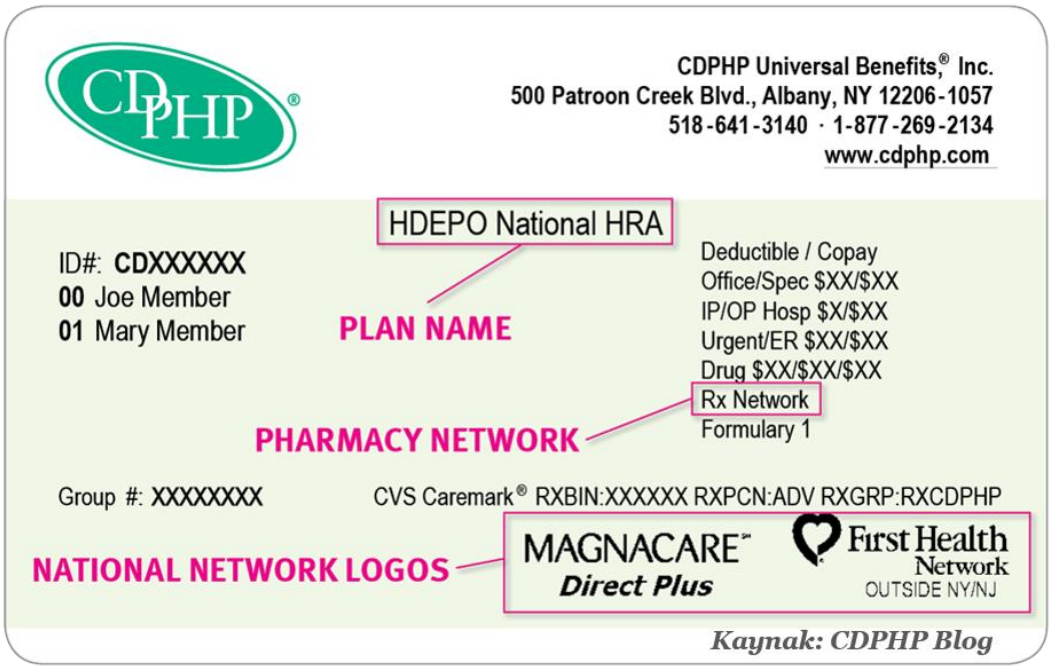
Elektronik Tanımlamanın Yükselişi

Kısa Geçmiş

Kişilerin tanımlanması ihtiyacı, insanların ilk kez karmaşık sosyal etkileşimler geliştirmeye ve birbirleriyle ticaret yapmaya başladıkları toplumların kökenine kadar uzanabilir. Uzun bir süre boyunca kimlik doğrulaması; kişilerin fiziksel, statü ve güç sembolleri (örneğin: elbiseler, aksesuarlar, dövmeler) veya üye olarak seçilmesi

(örneğin güvenilen biri tarafından tanıtılması) dâhil olmak üzere resmi olmayan yöntemlerle gerçekleştirilmiştir.

İnsan toplumu tarihinde ülkeler tarafından resmi kimlik belge/kanıtlarının verilmesi oldukça yeni bir olgudur. Kimlik belgelerinin yaygın olarak kullanımı tam manasıyla, devlet otoritesini güçlendirmek, göçleri çok daha iyi kontrol etmek ve dolandırıcılıkla mücadele etmek maksatlarıyla II. Dünya Savaşı sonrasında başlamıştır. 20'nci yüzyılın ikinci yarısında refah devleti kavramının gelişmesi ve ekonominin hükümetler tarafından artan şekilde düzenlenmesi bu eğilimi giderek güçlendirmiştir.



Kaynak: CDPHP Blog

Başlangıçta kâğıt tabanlı olan sistem, bilgi toplumunun yükselişine paralel olarak giderek sayısal hale getirilmiştir. Sosyal güvenlik, vergi, sağlık vb. gibi farklı hükümet veri tabanlarıyla eşleştirmek maksadıyla vatandaşlara tanımlayıcılar/kimlik numaraları verilmiştir. Bu yaklaşım her ne kadar işlevselliğini korusa da örneğin sağlık sigorta kartı gibi kendine özgü kimliklerin verilmesi; ülkeler ve vatandaşları açısından artan karmaşıklığa neden olan çok sayıda paralel kimlik tanıma sistemlerinin ortaya çıkmasına neden olmuştur.[v]

Hükümetler tarafından kamu hizmetlerine erişim için uygulamaya sokulan çevrimiçi sistemler de potansiyel dolandırıcılara karşı zayıf bir güvenlik sağlayan statik şifrelere dayanmaktadır.

Son yirmi yılda vatandaşların, ödemeler, e-ticaret[vi], veri değiş tokuşu gibi günlük işlemlerini desteklemek için internet kullanımında büyük bir patlama görülmüş ve bu nedenle de vatandaşların "sayısal yaşamları" giderek daha da önem kazanmıştır.

Bununla birlikte çevrimiçi ortamın herkese açık olması dolandırıcılık ve kimlik hırsızlığı risklerini de önemli ölçüde artırmıştır. Bu nedenlerden ötürü de hem kamu hem de özel sektörde birbirleriyle etkileşim halindeki insanlar için güven ve teminat gereksinimi çok önemli hale gelmiştir.

İşte bu nedenle bazı hükümetler, kâğıt esaslı kimlik kartlarını, vatandaşlara sayısal dünyada kimliklerini kanıtlama imkânı sağlayan elektronik kimlik ilave etme kararı almıştır. Akıllı kart tabanlı eID'ler, genellikle çeşitli diğer kimlik kartı belgelerinin yerini alarak ve farklı kamu hizmetlerine bağlı çeşitli tanımlayıcıları birleştirerek birçok yerde uygulamaya girmiş ve elektronik kimlikler devlet veri tabanlarında bulunan bütün kişisel bilgilerin kilidini açmanın anahtarı olmuştur.

Son yıllarda, başta mobil kimlik çözümleri olmak üzere, vatandaşların sayısal kimliklerini içeren farklı araçlar kullanılmaya başlanmıştır. Bu çeşitlilik, sayısal kimliklerin artan kullanımına bağlı olarak sadece daha fazla kullanıcı dostu çözümlere duyulan ihtiyaca değil, aynı zamanda giderek artan ROCA şifreleme güvenlik açığı gibi siber tehditlere de bir yanıt olmuştur.[vii]

Günümüzde Elektronik Tanımlama Teknolojisinin Durumu

Günümüzde eID teknolojisi hızlı hareket eden ve karmaşık bir görüntü sunmaktadır. Sayısal Tanımlama için Teknoloji Alanı[viii] hakkında yazılan yakın tarihli bir raporda, Dünya Bankası (World Bank) tanımlama ve doğrulama maksatlı kullanılan teknolojileri üç ana kategoride gruplandırmıştır:

- Kimlik bilgileriyle bağlantılı teknolojiler: biyometri, kartlar, mobil ve destekleyici teknolojiler;
- Kimlik Doğrulama ve güvenli yazılım çatıları bağlantılı teknolojiler;
- Analitik bağlantılı teknolojiler (özellikle risk değerlendirmeleri için).

Kimlik Bilgisi Teknolojileri

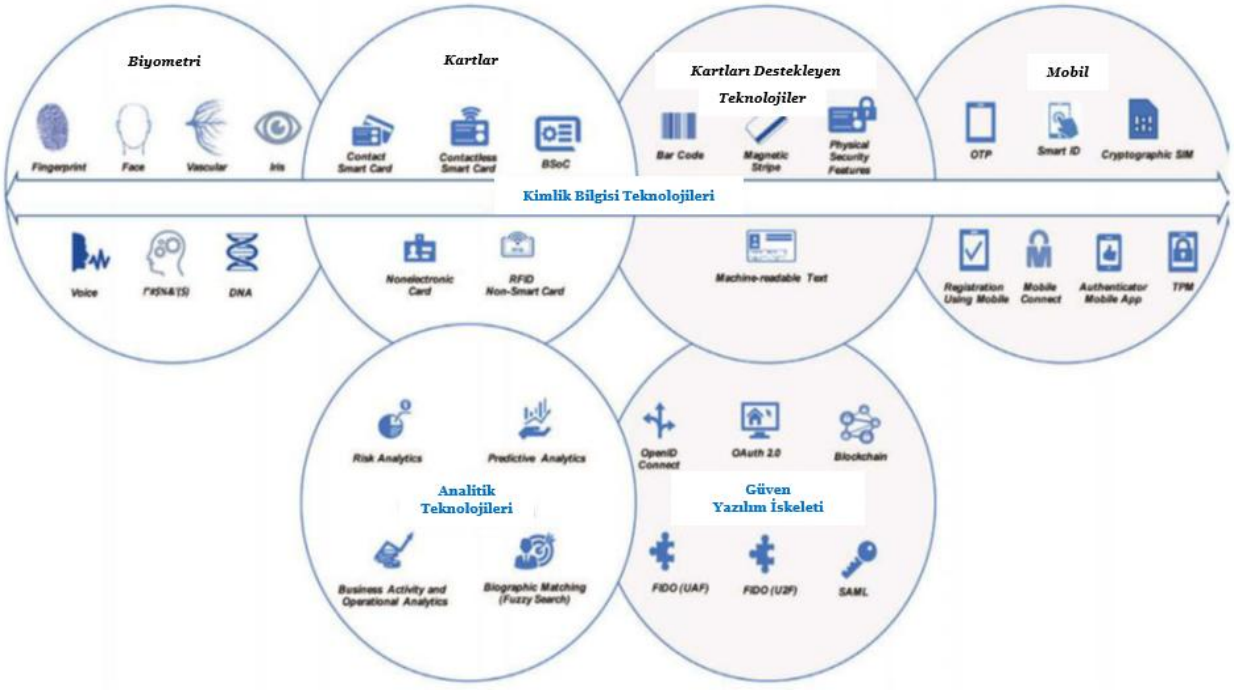
Biyometri

Biyometrik tanıma bir kişinin kendisine özel fizyolojik ve davranışsal özelliklerini, onları tanımlamak ve doğrulamak maksadıyla kullanır. Fizyolojik nitelikler parmak izlerini, iris paternlerini ve yüz özelliklerini içermektedir. Davranışsal niteliklere; yürüyüş, imza, tuş vuruş paternleri ve fare kullanımı örnek olarak gösterilebilir.

Kartlar

Belirli bir kişinin kimlik özelliklerini saklayan kartlar, çeşitli formatlarda bulunur ve özel veri giriş cihazları veya kart okuyucular tarafından okunabilirler. Bu kartlar, temel demografik bilgileri sunan elektronik olmayan kartlardan, kart okuyuculara

takılmak üzere tasarlanmış yongalı ve temassız akıllı kartlara kadar çeşitlilik gösterirler.



Tanımlama ve Doğrulama Teknolojileri, Kaynak: World Bank

Kartlar için destekleyici teknolojiler

Kartlar için destekleyici teknolojiler genellikle kartların okunmalarını veya güvenliklerini sağlayan teknolojilerdir. Barkodlar, manyetik şeritler, fiziksel güvenlik özellikleri ya da makine tarafından okunabilen metinler içerirler.

Kartlar İçin Destekleyici Teknolojiler: Barkodlar, manyetik şerit ve makine tarafından okunabilen metin.

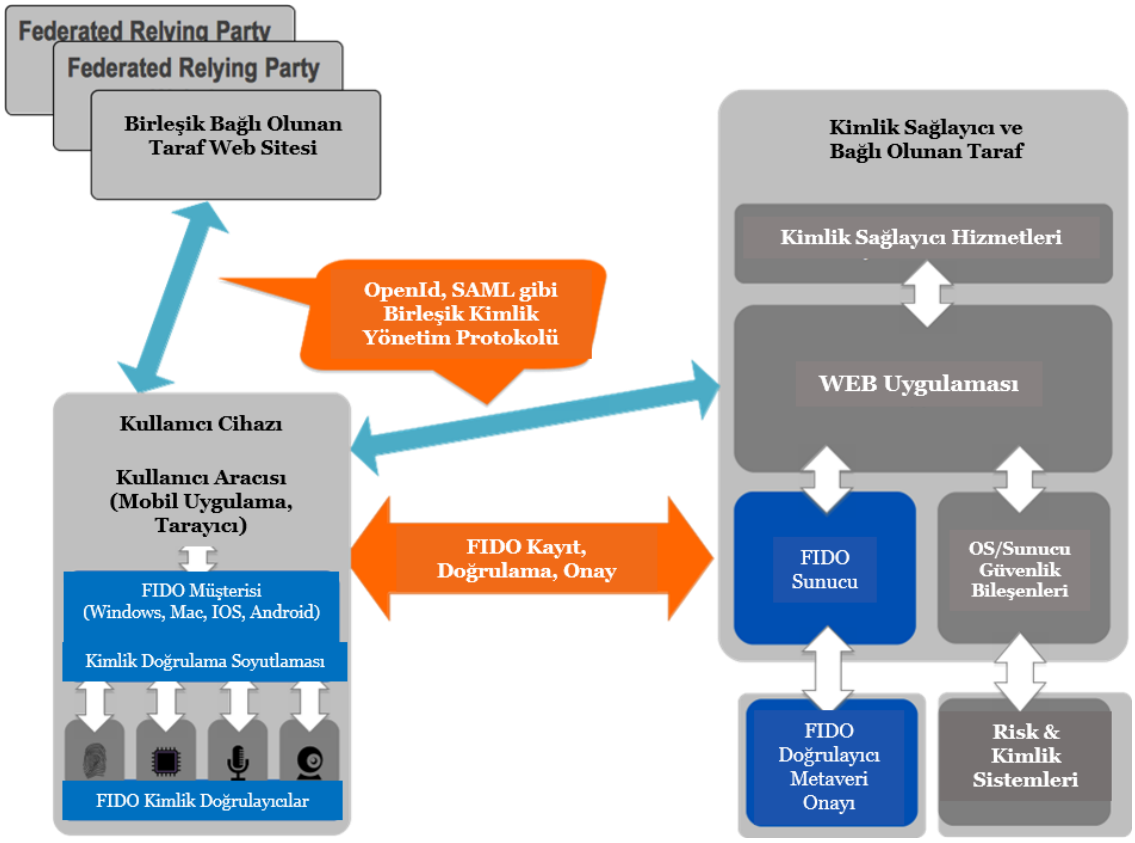
Mobile ID

Kimlik tanımlamayla ilgili mobil teknolojiler, bir bireyin kimliğini kaydetmek, doğrulamak ve teyit etmek için kullanılan telefon ve tablet tabanlı donanım ve yazılım çözümlerinden oluşmaktadır.[ix]

Kimlik Doğrulama ve Güvenli Yazılım Çatıları (framework)

Güvenli yazılım çatıları[x], kimlik ve hizmet sağlayıcılara; güvenilir kimlik bilgilerinin sağlanmasına ve bireylerin kimliklerinin tanınan güvence seviyelerinde doğrulanmasına izin veren üzerinde anlaşabilecekleri bir dizi yasal, ticari ve teknik kurallar sağlamaktadır. Bunlar, güvenli kimliklerinin birçok organizasyon tarafından ve bu organizasyonlar arasında iletildiği birleşik kimlik düzenlerinin ana temelidir.

FIDO UAF & U2F (Fast IDentity Online Universal Authentication Framework & Universal Second Factor – Çevrimiçi Hızlı Kimlik Doğrulama Üniversal Kimlik Doğrulama Yazılım Çatısı & Üniversal İkinci Faktör), SAML[xi] (Security Assertion Markup Language – Güvenlik Onaylama Biçimlendirme Dili), OpenID Connect ve OAuth 2.0 dâhil olmak üzere birçok iyi yapılandırılmış yazılım çatısı bulunmaktadır.



Kaynak: FIDO Alliance

İlave olarak blok zinciri (blockchain) gibi, bireyleri kendi merkezi olmayan kimliklerinin (Decentralised Identity) kontrolüne sokan güvenli yazılım çatıları oluşturma potansiyeline sahip dağıtık defter teknolojileri (DLT – Distributed Ledger Technology)[xii] de ortaya çıkmaktadır.

Analitikler

Analitik teknolojileri, verilerde anlamlı iç görüler bulmak maksadıyla bir dizi veri kaynağında matematiksel ve istatiksel modelleme tekniklerini kullanır. Kimlik tanımlama dünyasında analitik teknolojileri; paternlerin çevrimiçi olarak işlem

yapma ve etkileşime girme biçimlerini analiz ederek, bir birey için kapsamlı bir kimlik oluşturmada için kullanılabilir.

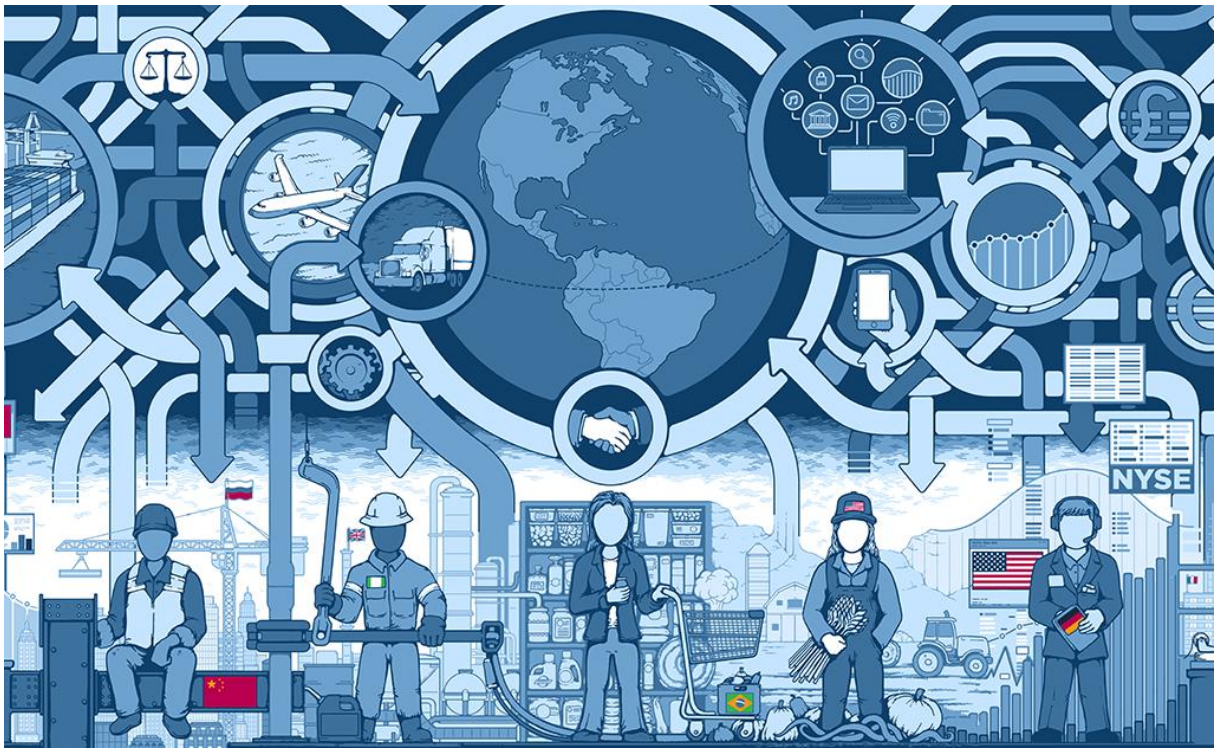
ELEKTRONİK KİMLİK EVRİMİNİ TETİKLEYEN FAKTÖRLER

Mevcut elektronik tanımlama (eID) ile ilgili teknolojilere kısa bir bakıştan sonra dikkatimizi bu teknolojiler ve genel eID piyasasının gelecekte nasıl evrimleşeceğine çevirebiliriz. Bunun için de bu gelişimde etkisi olan daha kapsamlı; toplumsal, ekonomik, siyasi ve teknolojik faktörlerin incelenmesi gerekmektedir.

Toplumsal

Küreselleşme ve Bağlantılı Toplum

Kentleri, bölgeleri ve ülkeleri ekonomik, teknolojik ve sosyal olarak birbirlerine bağlayan halen sürmekte olan küreselleşme süreci, insanların serbest dolaşımını ve iş dünyasının benzersiz ölçüde uluslararası hale gelmesini teşvik etmektedir.



Kaynak: Peterson Institute for International Economics

Sayısal çağın başlamasıyla birlikte küreselleşmenin hızı önemli ölçüde ivme kazanmıştır. Artık, mobil ağların hızındaki süratli artışların olanaklı kıldığı, günlük hayatımızda kullandığımız sayısız cihazla sürekli olarak birbirine bağlanan ve giderek daha fazla "network – ağ" haline gelen bir dünyada yaşıyoruz.

Mobil cihaz kullanımının yükselişi çok derin olmuştur ve kullanıcılar toplam medya süresinin %69'unu akıllı telefonlarda geçirmektedirler.[xiii] İnsanlar, işletmeler ve

giderek artan oranda da makinelerin sınırların ötesinde, her yerde ve her an işlem yaptığı bir dünyada, sayısal ve mobil kimlik ihtiyacı geçmişte hiç bu kadar büyük olmamıştır. Bu durum; 2017 yılı dördüncü çeyreğinde mobil kullanıcıların %76'sının mobil operatörler tarafından sağlanan kimlik hizmetlerini kullanmak istedikleri örneği göz önüne alındığında, kullanıcıların tercihlerinin mobil kimlik çözümlerine kaymasında görülmektedir.[xiv]

Sorunsuz deneyimlere olan talep artışı

Vatandaşların beklentileri, çevrimiçi hizmetlerin hızı ve kullanılabilirliğini yükselten teknolojiye paralel olarak artmıştır. Günümüzde kullanıcılar, 7/24 ve tek bir butona basılarak erişilebilen kesintisiz ve çok kanallı hizmetlerin beklentisi içindedirler. Süratli ve çok kanallı işlem yapabilme beklentisi, daha önce de bahsedildiği gibi mobil tabanlı kimlik çözümlerinin yükselişini tetiklemiştir.

Bunun da ötesinde son birkaç yılda, tüketicilerin %86'dan fazlasının formatın güvenliği ve uygunluğu konusunda şüpheleri olduğu, kullanıcı adı ve şifre tabanlı kimlik çözümlerinin dışında, kullanıcı tercihlerinde çarpıcı bir değişim yaşanmıştır.[xv]

Parolalar kolayca unutulabilmekte bu da kullanıcılarda önemli hayal kırıklıklarına neden olabilmektedir. Çağrı merkezlerine yapılan destek taleplerinin %30'a kadarı parola sıfırlama talepleridir.[xvi] İşte bu nedenle kullanıcılar birden fazla kimlik bilgilerini yönetmek yerine birden çok uygulama için tek bir sayısal kimliği kullanmayı tercih etmektedirler. Organizasyonların, mobil cihazlarda parola kullanımı yerine, fiziksel veya davranışsal biyometriye yatırım yapmalarının nedeni de budur.

Biyometrinin, fiziksel ve davranışsal olmak üzere iki ana tipi bulunmaktadır. Fiziksel tanımlama yöntemleri arasında; yüz şekli ve geometrisi, parmak izleri, kafatası şekli ve yapısı, retina, iris, avuç içi/el/parmak geometrisi, yüz ve el termografisi, avuç içi/parmak damar deseni ve DNA bulunmaktadır. Davranışsal tanımlama yöntemleri

arasında ise imza tanımlaması, tuş dinamikleri, konuşma tanıma ve yürüme biçimi gibi yöntemler bulunmaktadır.

Kişisel verilerin hükümetler ve işletmeler tarafından kullanımına yönelik artan endişeler

Kullanıcılar çevrimiçi işlem yaparken genellikle verilerinin ne ölçüde toplanılıp kullanıldığının farkında olmamaktadır. Bu nedenle sayısal kimlikleri üzerinde tam bir kontrole sahip değildirler. Amerikalı bilgisayar uzmanı, eski CIA (Central Intelligence Agency - Merkezi İstihbarat Teşkilatı) ve NSA (National Security Agency - Ulusal Güvenlik Dairesi) çalışanı Snowden ifşaatları ve Cambridge Analytica (firma 50 milyondan fazla Facebook profilinden alınan kişisel verileri, kişiselleştirilmiş siyasi reklamlarla ABD'li seçmenleri hedef almak için izinsiz kullanmıştır)[xvii] gibi siyasi skandalların ardından kamuoyu, hükümet ve organizasyonel verilerine erişim ve bunların kendi rızaları dışında kullanılabileceği ve manipüle edilebileceği konusunda çok daha bilinçli hale gelmiştir.

Bütün dünyada büyük yankı uyandıran Cambridge Analytica skandalında 50 milyon Facebook profilinin kişisel bilgileri rızaları olmadan ele geçirilmiş olabilir. Edward Snowden'in gizli Pentagon belgelerini sızdırması ise, bazıları tarafından ABD tarihinin en büyük ve önemli sızıntısı olarak nitelendirilmektedir. Snowden'e göre onu belgeleri sızdırmaya iten tek neden; halkı onlar adına ne yapıldığı ve onlara karşı neler yapıldığı konusunda bilgilendirmektir. Kaynaklar: ABC News (sol) ve VİKİPEDİ

Snowden'in ifşaatları ve Cambridge Analytica skandalları, halkın elektronik kimlik projeleri gibi hükümet faaliyetlerine olan güvenini azaltmış ve insanların kişisel verilerinin güvenliğine çok daha fazla önem vermesine neden olmuştur.

Ekonomik

Giderek kalabalıklaşan ve parçalanan sayısal kimlik pazarı

Hem ulusal düzeyde (örneğin devlet tarafından verilen eID'ler veya ulusal ölçekte kullanılan özel sektör çözümleri) hem de işlevsel düzeyde (örneğin hizmetlerine erişebilmeleri için müşterilerine kimlik bilgilerini veren özel sektör aktörleri) küresel olarak sunulan elektronik kimlik çözümleri sayısında önemli bir artış olmuştur. Bu

durum, birçok durumda pazardaki rekabeti artırmakta ve kimlik çözümlerinin vatandaşlar için çok daha ucuz, erişilebilir ve kullanımı kolay hale getirmektedir.

Bununla birlikte, ülkeler arasında ve ülke içinde teknoloji ve teknolojik olgunluk seviyeleri açısından önemli bir çeşitlilik ortaya çıkması parçalanma riski ve çözümler arasında birlikte çalışabilirlik eksikliğinin yanı sıra, ölçek verimliliğinden yararlanma fırsatını kaybetme riskini artırmaktadır.[xviii] Bu parçalanma, kullanıcının sistemler arasında birden çok kimlik bilgilerini yönetmesini de gerektirebileceğinden kullanıcı deneyimini de etkilemektedir.

Tallinn Deklarasyonu[xix] ve Geleceğin Hükümeti: varsayılan olarak birlikte çalışabilir ve sayısal (The Tallinn Declaration and Government of the Future: interoperable and digital by default') başlıklı yazıdan alıntıdır. Kaynak: OpenForum Europe

Kamu ve özel sektör arasında artan bağımlılık

Hükümetler ve özel sektör kuruluşları, kimlik doğrulaması için güvenli sistemleri kullanabilme konusunda ortak bir faydaya sahiptirler. Tarihsel olarak, güvenilir tanımlama araçlarının sağlanması hükümetlerin etki alanındadır, ancak bu durum, kamu ve özel sektör çözümleri arasında genellikle önemli örtüşmelerin olduğu bir noktaya evirilmiştir. Çoğu durumlarda özel kuruluşlar, müşterilerin kimliğini doğrulamak veya kendi ilave kimlik çözümlerini oluşturmak maksadıyla devlet tarafından verilen kimlik bilgilerine (örneğin ulusal kimlik numaralarına) güvenmektedirler. Öte yandan, kamu idareleri, devlet tarafından yönetilen programları desteklemek veya devlet hizmetlerine doğrudan erişim sağlamak

maksadıyla giderek özel sektör kimlik sağlayıcılarına yönelmektedirler. Ortaya çıkan bu karşılıklı bağımlılık, taraflar arasında başarılı olmak için yeni açıklık ve güven seviyeleri gerektiren yeni çalışma ve işbirliği modellerini zorunlu kılmaktadır.[xx]

Politik

Avrupa Birliği öncelikleri olarak kullanıcı odaklılık, birlikte çalışabilirlik ve veri gizliliği

Son zamanlarda uygulamaya giren üst düzey Avrupa Birliği mevzuatları, çevrimiçi işlemler yapan vatandaşların ihtiyaçlarının giderek daha fazla karşılanması ve sayısal kimliklerinin kötü maksatlı olarak kullanılmasını önlemeye çalışmaktadır. AB'nin konuya yaklaşımı bunun yanı sıra, ülkeler arasında ve içinde, diğer uygulamalarla etkileşimde olmayan sistemlerin (siloed systems) çoğalarak yayılması nedeniyle ortaya çıkan engelleri de ortadan kaldırmaya çalışmaktadır (yukarıda ele alındığı gibi parçalanma trendine karşı koyma girişimi). Ekim 2017 tarihli Tallinn Deklarasyonu ve AB 2016-2020 e-Devlet Eylem Planı, önümüzdeki beş yıl boyunca e-Devlet uygulamalarının geliştirilmesi için ortak hedefleri belirlemiştir.

Her ikisi de TOOP (The Once Only Principle – Tek Seferlik İlke)[xxi], tamamen sayısal (digital-by-default), açıklık ve şeffaflık ile tamamen birlikte çalışabilirlik dâhil olmak üzere, kamu hizmetlerinin tasarım ve sunulmasında uygulanacak olan bir dizi temel kullanıcı odaklı prensipleri öne çıkarmaktadır.

Eylül 2018'de yürürlüğe giren eIDAS[xxii] (Electronic Identification, Authentication & Trust Services - Elektronik Kimlik Belirleme ve Güven Hizmetleri) Yönetmeliği'nin elektronik kimlikle ilgili bölümü; işletmeler, vatandaşlar ve kamu otoriteleri arasında güvenli ve sorunsuz elektronik etkileşimler sağlamak maksadıyla öngörülebilir bir

düzenleme ortamı oluşturmaktadır. Ana hedeflerinden bir tanesi; insanlar ve işletmelerin diğer AB ülkelerindeki çevrimiçi kamu hizmetlerine erişebilmelerini sağlamak için kendi ulusal eID'lerini kullanabilmelerini sağlamak ve Avrupa'da karşılıklı olarak birlikte çalışabilen bir eID ağ düzeni oluşturmaktır.

Nisan 2018'den beri yürürlükte olan Genel Veri Koruma Yönetmeliği (GDPR – General Data Protection Regulation)[xxiii], Avrupa Birliği ve Avrupa Ekonomik Alanı vatandaşları ve sakinlerine, Avrupa sınırları içinde iş yapan bütün işletmelerden gelen kişisel verilerin kullanılması ve işlenmesine yönelik gereksinimleri belirleyerek, kişisel verileri üzerinde bir kontrol sağlamayı amaçlamaktadır. Verilen örnekler, Avrupa'da elektronik kimliğin evrimleşerek daha kullanıcı dostu, mobil ve yeniden kullanılabilir çözümlere doğru yönlendirmeli ve vatandaşların kendi verileri üzerinde daha fazla kontrol sahibi olma yönündeki beklentilerine ivme kazandırmalıdır.

Teknolojik

Artan siber güvenlik[xxiv] riskleri

Giderek artan karşılıklı bağlantı, küreselleşme ve siber suçların ticarileşmesi, veri ihlalleri de dâhil olmak üzere siber olayların sıklık ve şiddetini artırmaktadır.[xxv] 2021 yılına kadar, siber suçların vereceği zararın maliyetinin yıllık 6 trilyon dolara ulaşacağı tahmin edilmektedir.[xxvi] Dolandırıcılık yapmak için kullanılabilecek sosyal güvenlik numarası gibi geçerli verilerin yeni, hayali bir kimlik oluşturmak maksadıyla sahte bilgilerle birleştirildiği "Sentetik Kimlik" siber suç[xxvii] alanında özellikle hızla büyüyen bir siber suç örneğidir.

2016 yılında kredi kartı dolandırıcılığından kaynaklanan bütün kayıpların %80'inin arkasında sentetik kimlik olduğu tahmin edilmektedir.[xxviii] Görüldüğü gibi giderek artan siber tehdide tepki olarak Avrupa Birliği'nde verilerin korunması mevzuatı, veri

ihlalleri için önemli para cezalarıyla, giderek daha da sertleşmekte ve yaygınlaşmaktadır. Artan siber risk ve daha da önemlisi vatandaşların bu riske yönelik farkındalığının yükselmesi de daha güvenli kimlik çözümlerine olan talebi artırmaktadır.

Üstel teknolojinin yükselişi

Yeni teknolojiler, sürekli artan bir oranda devamlı olarak gelişmekte ve kimlik yönetim çözümlerinin imkân ve kabiliyetleri ile yönünde değişikliklere yol açmaktadır. Örnekler aşağıdadır:

- Muazzam miktarda bilginin merkezi olarak toplanmasını, sınıflandırılmasını ve depolanmasını sağlayan bulut bilişim ve veri işleme motorları.
- Her bir kullanıcı için tek bir sayısal kimliği, merkezi olmayan, güvenilir ve değiştirilemez bir şekilde depolayarak kimlik yönetiminde geleneksel yaklaşımı altüst etme potansiyeline sahip dağıtılmış defter teknolojisi. Bu teknoloji sayesinde kimlik nitelikleri kullanıcı tarafından, kendi isteğine bağlı olarak birden fazla veri tabanında paylaşılabilir.
- Sayısal kimlik için geçmişte var olmayan senaryolar oluşturabilen Nesnelerin İnterneti (IoT – Internet of Things).[xxix] 2025 yılına kadar geçecek sürede, küresel olarak kurulan bazı cihazların sayısı, üç kat artarak 23 milyardan 75 milyara çıkacaktır.[xxx] Bu hızlı artış, cihazları giderek daha fazla kimlik hırsızlığı ve manipülasyona karşı hassa bırakacağından etkili IoT kimlik ve güvenlik çözümlerine olan talep artacaktır.
- İşlemlerin geçerliliğini belirlemek maksadıyla karmaşık paternler ve yapılandırılmamış veri kaynakları arasındaki ilişkilerden yararlanarak sayısal kimliklerin otomatik olarak izlenmesine giderek daha fazla imkân sağlayacak olan yapay zekâ. Algoritmalar, bir yönetimsel veri tabanındaki varlıklarına dayalı olarak verilen statik kimlik bilgileri yerine, kişilerin bir devlet veri

tabanındaki eylemler ve işlemlerine dayanan sayısal ayak izlerini bir kimlik kanıtı olarak kullanılmasına imkân sağlayacaktır. Nesnelerin İnterneti aynı zamanda makine kimliği kavramını da devreye sokacaktır.

- Sahte bilgileri yaymak, sonuçları çarpıtmak ve kötü amaçlı yazılımları yaymak için kullanılan sahte sayısal kimliklerin (örneğin botlar) yükselişi için uygun bir platform haline gelen sosyal medya.

ELEKTRONİK KİMLİK TRENDLERİ

Yukarıda anlatılanların ışığında, elektronik kimlik tanımlamada (eID) geleceğe yönelik birkaç net trend ortaya çıkmıştır.

Önce Mobil

Mobil cihazların kullanımı hızla artmaktadır ve 2017 yılında gerçekleştirilen web sitesi ziyaretlerinin %63'ü mobil cihazlar üzerinden yapılması ile geleneksel masaüstü kullanım cihazlarını geride bırakmıştır.[xxxi] Artan mobil cihaz kullanımıyla birlikte mobil işlemlerin sayısı da giderek artmaktadır.

Örneğin, dünya genelinde mobil ödeme teknolojileri pazarının 2016 ve 2024 yılları arasında %20,5'lik yıllık bileşik büyüme oranında (CAGR – Compound Annual Growth Rate) artması beklenmektedir.[xxxii] Mobil işlemleri gerçekleştirme isteği, kullanıcıların belirli bir yerde olmasına veya ilave donanım taşımalarına bağlı olmayan, güvenli mobil tabanlı kimlik tanımlamalarına yönelik artan bir ihtiyacı da beraberinde getirmiştir.

Mobil kimlik, sayısal kimlik sistemlerinin uygulanmasında giderek daha fazla tercih edilen bir seçenek haline gelmektedir. Avrupa'da mobil tabanlı sistemler hâlihazırda;

Avusturya, Belçika, Estonya, Finlandiya, Almanya, İzlanda, Letonya, Litvanya, Norveç ve İsveç gibi ülkelerde kullanılmaktadır.[xxxiii]

Farklı türde mobil kimlik çözümleri de ortaya çıkmaktadır. Örneğin Smart ID, kullanıcıların sayısal kimlik kartları ve sertifikalarını kullanarak cihazlarını kaydedebilecekleri bir uygulamadır. Kullanıcılar, bir kez kayıt olduktan sonra, çeşitli hizmetlere erişim için cihazlarda kimliklerini doğrulamak için uygulamayı kullanabilirler.[xxxiv] Estonya, Letonya ve Litvanya'da bir milyondan fazla Smart ID kullanıcısı bulunmaktadır.

Başka bir örnek de; kartı bir kullanıcı tanımlama aracına dönüştürmek için kriptografik algoritmalar kullanan SIM (Subscriber Identification Module – Abone Kimlik Modülü) kart[xxxv] tabanlı çözümlerdir. Bu tür çözümler şu anda Estonya, Finlandiya ve Moldavya gibi ülkelerde kullanılmaktadır.

Dünyanın dört bir yanından mobil operatörler tarafından yürütülen bir girişim olan Mobile Connect[xxxvi], kullanıcıları doğrudan kendi mobil telefonlarına bağlayan bir dizi mobil tabanlı kimlik hizmeti sağlamaktadır. Mobile Connect uygulaması; tanımlayıcı olarak bir kişinin mobil telefon numarasını ve kimlik doğrulama cihazı olarak da mobil telefonu kullanarak, çeşitli web siteleri ve uygulamalara kayıt olma ve oturum açma ile çevrimiçi işlemlerin yetkilendirmesini desteklemektedir. [xxxvii] Mobile Connect uygulaması şu anda dünyada 30 ülkede kullanılmaktadır ve eIDAS ile uyumluluğu da kanıtlanmış durumdadır.[xxxviii]

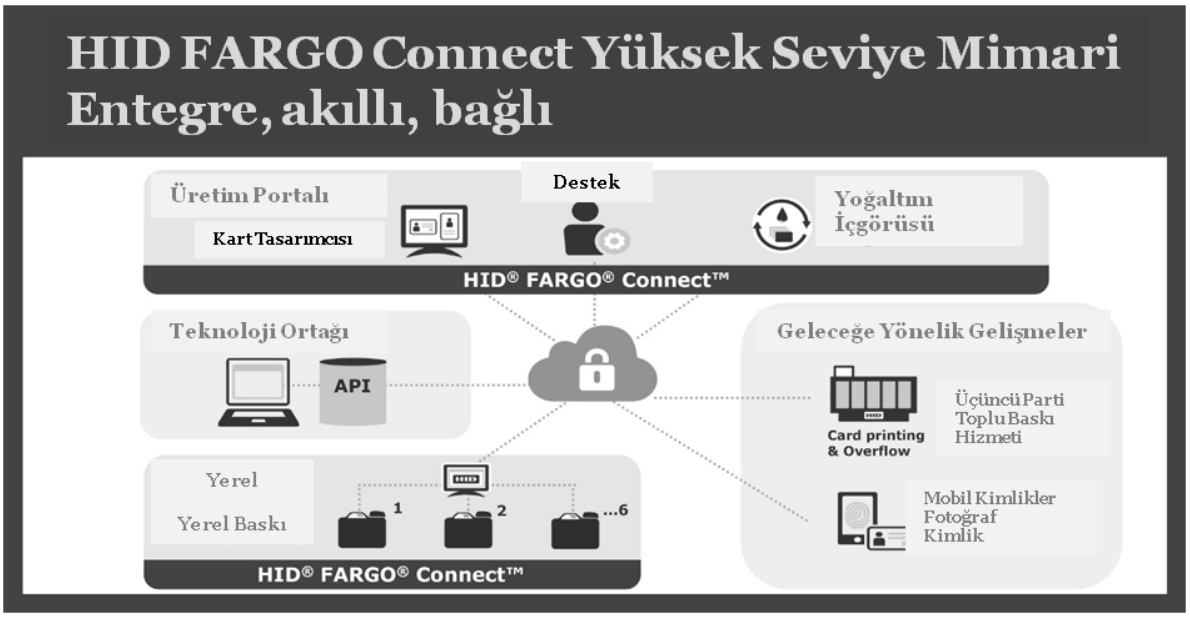
Bilgisayar korsanları giderek çok daha donanımlı hale geldiğinden ve veri depolama cihazlarına kolaylıkla sızabildiklerinden; kimlik hırsızlığı ve hileli işlemler çok hızlı bir şekilde artmaktadır. Bir zamanlar insan tanımlamanın en güçlü yöntemlerinden bir tanesi olarak kabul edilen parmak izleri dahi bugün kopyanabilir ve biyometrik kimlik doğrulamasını maharetle alt edebilmek için kullanılabilir hale gelmiştir. Statik biyometrik veriler aslında parolalar kadar taklit, yanıltma ve sahte kimliğe bürünmeye karşı savunmasız olabilirler.

Bu gibi çözümler kolaylık ve güvenlik sağlamaktadır ve toplum içinde mobil cihazlara erişim derinleştikçe de ivme kazanmaya devam edeceklerdir. Mevcut trend, mobil telefonu numarasının hem tanımlayıcı hem de kimlik doğrulayıcı olarak kullanılması nedeniyle kullanıcıları giderek daha fazla kimlik hırsızlığı riskine sokan SMS tabanlı kimlik doğrulama sisteminden uzaklaşma yönündedir.[xxxix]

Coğrafi konum ve kullanıcıların işlem geçmişleri gibi faktörlere dayanan dinamik kimlik doğrulama tekniklerini, kullanarak mobil cihazların sağladığı bütün fırsatlardan yararlanan mobil uygulamaları yakın gelecekte görmeye başlayacağız (makalenin ilerleyen bölümlerinde daha ayrıntılı olarak incelenecektir).

Biyometri: Çoklu mod ve biyometri: Çoklu ve davranışsal moda geçiş

Biyometrik kimlik doğrulama yöntemleri tipik olarak bir kişinin, örneğin parmak izi, retina, iris, damar, ses ve yüz gibi fiziksel bir özelliğini süzer ve zaman içinde geçmişteki bir noktada alınan referans verileriyle karşılaştırır. Karşılaştırma sonrası olasılıksal skor bireyin olması gereken kişi olup olmadığını belirler. Biyometrik kimlik doğrulama, kullanılabilecek çeşitli yerleşik sensörlere (parmak izi tarayıcıları, kameralar, yüz tanıma sistemleri vb. gibi) olan ihtiyaç nedeniyle genellikle cihaz tabanlıdırlar.



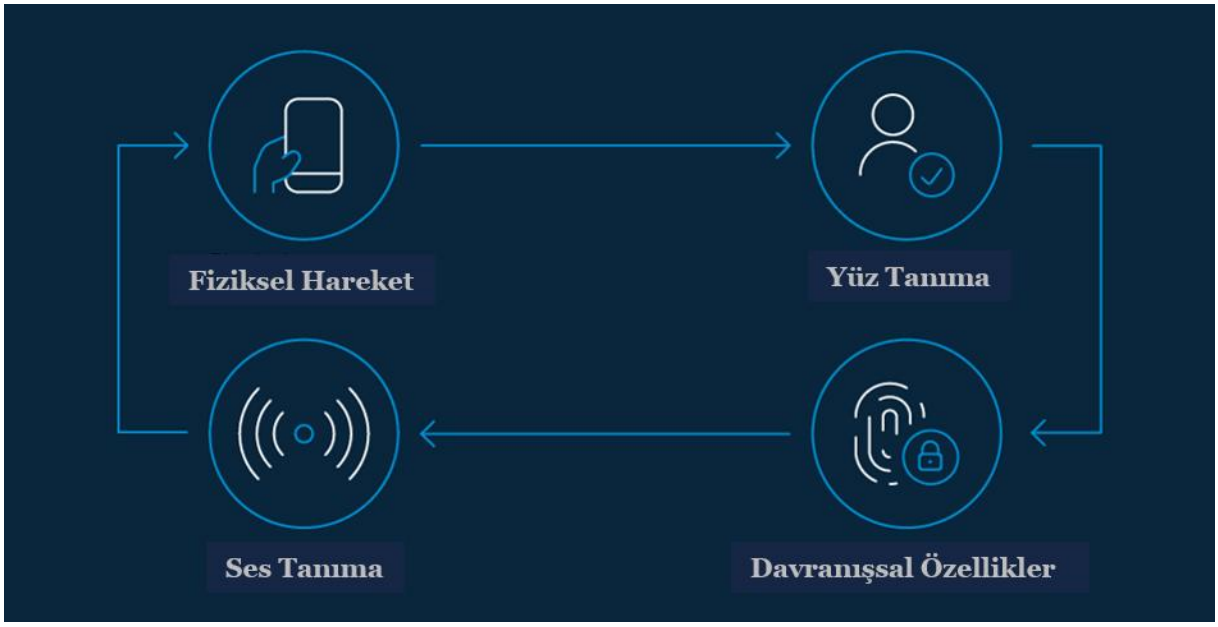
Higgins Corporation tarafından geliştirilen Bulut Tabanlı Kimlik Kartı Oluşturma Sistemi. Kaynak: higgins3.com

Aslında biyometrik teknoloji yeni olmasa da mobil cihaz kullanımı ve sensör donanımlı akıllı telefon[xl] sayısındaki büyük artış (2018 yılında bir milyardan fazla parmak izi sensör donanımlı telefon piyasaya sürülmüştür[xli]), son yıllarda biyometrik kimlik doğrulamanın yükselişini desteklemiştir. Acuity firması, 2022 yılına kadar 1,37

trilyon işlemin biyometrik olarak doğrulanması maksadıyla 5,6 milyar mobil cihazın kullanılacağını tahmin etmektedir.[xlii]

Tek bir modaliteyi değerlendiren biyometrik teknoloji, kullanıcı açısından yönetilmesi zor olan parolalara olan bağımlılığı azaltarak kimlik doğrulama sürecinde kullanıcı deneyimlerini iyileştirebilir. Biyometri bunun yanı sıra, bulut tabanlı bir kimlik sistemine erişebilmek için de kullanılabildiğinden, kimlik doğrulama araçlarının kaydileştirilmesinde kullanım senaryolarını da destekleyebilir.[xliii]

Bilinenler, sahip olunanlar ve kimlik bilgilerini bir araya getiren, çok faktörlü kimlik doğrulamanın bir bileşeni olarak biyometri, iyi bir güvenlik seviyesi sağlayabilmektedir. Bununla birlikte, biyometrik teknolojinin saldırıya maruz kalması (hack) veya ele geçirilmesinin hâlâ birçok yolu bulunmaktadır. Örneğin, biyometrik tanıma başarısız olduğunda, varsayılan (default) işleyiş mekanizması genellikle bir parola gereksinimine geri döndüğünden, bütün parola tabanlı kimlik tanımlama uygulamalarının aynı güvenlik açıklarına sahiptir.



Buna karşılık, iris, parmak izi ve yüz modalitelerinin bir kombinasyonunu kullanan çok modlu biyometrik sistemler; doğruluk, güvenlik ve uygunluğun bir kombinasyonunu sağlayan gelecek vaat eden çözümlerdir. Oldukça ilgi çeken bir başka umut verici alan da davranışsal biyometridir.

Davranışsal biyometri, perde arkasında çalışan ve parmağınızın ekrana uyguladığı basınç, yazma hızınız, cihazı tuttuğunuz açı ve mevcut teknolojiden yararlanan diğer birçok parametre gibi kullandığınız cihazlar ile tam olarak nasıl etkileşim kurduğunuzu analiz eder.[xliv] Bütün bu davranışların birleşimi, kullanıcıya, aldıkları erişim düzeyini belirleyen bir güven skoru sağlamaktadır.

Davranışsal biyometri, kullanıcı deneyimine müdahale etmez ve tek seferlik değil, işlem boyunca sürekli kimlik doğrulama sağladığından saldırıya maruz kalması zordur. Bu nedenlerden dolayı, küresel davranışsal biyometrik pazarının 2020 yılına kadar %17'lik bir yıllık bileşik büyüme oranına (CAGR) sahip olacağı ve davranışsal biyometrinin giderek yaygınlaşacağı öngörülmektedir.[xlv]

Gerçek zamanlı ve sürekli doğrulamayı mümkün kılan analitikler

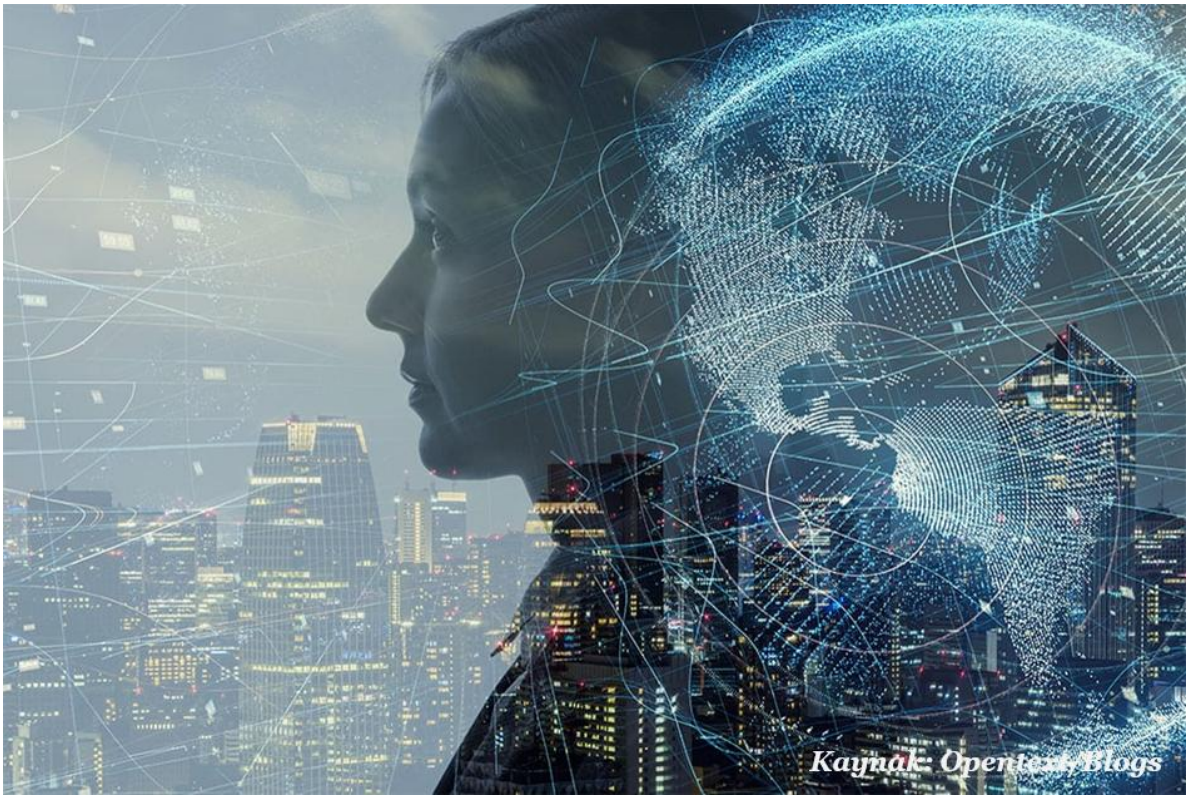
Önceki bölümde görüldüğü gibi, bir kullanıcının bir cihazla etkileşim biçiminin sürekli olarak değerlendirilmesi yoluyla, belirli bir noktada kimlik doğrulama yerine sürekli kimlik doğrulamaya doğru bir geçiş yaşanmaktadır. Bununla birlikte, analitik, yapay zekâ (Artificial Intelligence) ve Nesnelerin İnterneti'nin (IoT) bir araya gelmesi sürekli kimlik doğrulama ilkesini, izole tek bir cihazın kullanılmasının çok ötelerine genişletmektedir.

Günlük yaşamı boyunca her insan kendisine özgü ve benzersiz bir davranış paterni oluşturur ve farklı cihazlar ve kimlik doğrulama araçları kullanarak çeşitli web sitelerinde oturum açar. Kişiler bu cihazlar ve uygulamalarla benzersiz şekillerde etkileşime girerler. İnsanların sıklıkla ziyaret ettikleri yerler veya kullandıkları rotalar gibi belirli seyahat paternleri vardır. Zaman içinde, kullanıcı davranışları analitiği bütün bu benzersiz paternlerini; kullanıcı ile belirli cihazlar, konumlar ve kimlik

bilgileri arasındaki ilişkilerin son derece güvenilir bir resmini sunan, tamamen kullanıcıya özel benzersiz bir sayısal profile dönüştürebilir.[xlvi]

Bütün bu izler, bir bireyin benzersiz sayısal ayak izini oluşturur. Bu, esas olarak, bir kullanıcının günlük işlemleri sırasında yüksek derecede doğruluk ve güvenlikle sorunsuz ve sürekli olarak doğrulanabildiği anlamına gelmektedir. Birden fazla başarısız oturum açma girişimleri veya davranışsal anormallikler gibi potansiyel tehditler otomatik olarak algılanabilir ve hızlı bir şekilde kontrol altına alınarak engellenebilir. Gizliliği korumak maksadıyla hassas veriler, kişisel olarak tanımlanabilir bilgiye (PII – Personally Identifiable Information) dönüştürülemeyen hassas karşılıkları ile değiştirilen bir süreç aracılığıyla anonim hale getirilebilir.

Hiç şüphesiz yapay zekâ (Artificial Intelligence)[xlvii] ve makine öğrenimi (Machine Learning)[xlviii] bu gibi teknolojilerde önemli bir rol oynamaktadır. Tanımlama araçları için kullanıcı davranışlarının analitiğine dayanan sistemler; bir kişinin davranışı, alışkanlıkları ve hatta fiziksel özellikleri zaman içinde örneğin yaşlanma veya hastalık gibi nedenlerle değiştikçe, bunları otomatik olarak öğrenebilmeli ve uyumlandırabilmelidir.



Yapay Zekâ

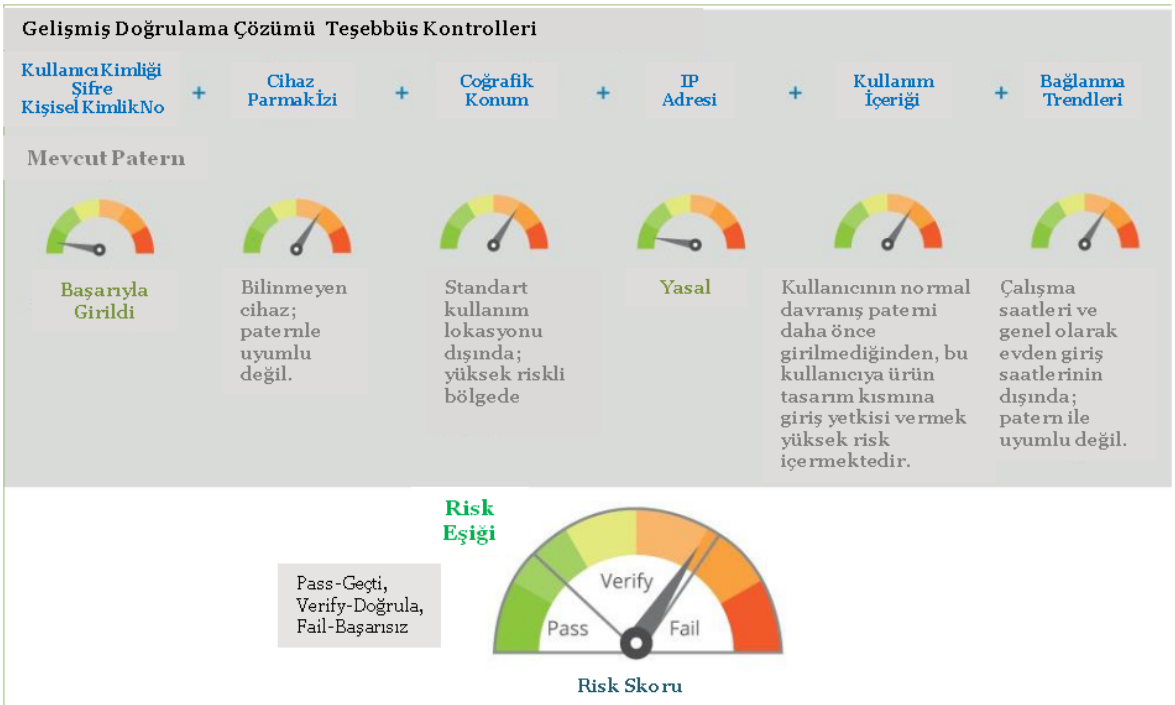
Yapay zekâ ana akım ve kolay ulaşılabilir ticari bir teknoloji geldiğinden, hem işletmeler hem de kötü niyetli kişiler yapay zekânın bu özelliklerinden faydalanmak

istemektedirler. Özellikle siber güvenlik uzmanlarının, gelecekte dünyanın birçok yapay zekâ destekli saldırıları göreceğine dair tahminleri bulunmaktadır.

Yapay zekânın bu özellikleri, döngüde insan geri bildirimi olmaksızın bu türden saldırılara karşı etkin yaklaşımlar oluşturabilen ve uygulayabilen otonom ajanlar kullanan çok daha karmaşık siber savunma sistemlerinin geliştirilmesini zorunlu kılmaktadır.

Makine Öğrenimi Kullanarak Anormallik Algılama

Anormallik Tespit Sistemleri[xlix] (ADS – Anomaly Detection Systems), bir veri kümesinde beklenen normal davranışa uymayan paternleri ortaya çıkarmak için tasarlanmıştır. Anormallik algılama problemlerinin çoğu; etiketlenmiş normal davranış örneklerini içeren bir veri kümesinin, sinir ağları (Neural Networks)[l] veya destek vektör makineleri gibi denetimli veya yarı denetimli makine öğrenim modellerini eğitmekte kullanıldığı, makine öğreniminde tipik bir sınıflandırma görevi olarak formüle edilebilir. Denetimsiz öğrenme, anormallik tespitinde kullanılabilse de denetimli veya yarı denetimli öğrenme ile karşılaştırıldığında performansının düşük olduğu gösterilmiştir.



Risk-tabanlı kullanıcı doğrulama. Kaynak: Deloitte University Press DUPress.com

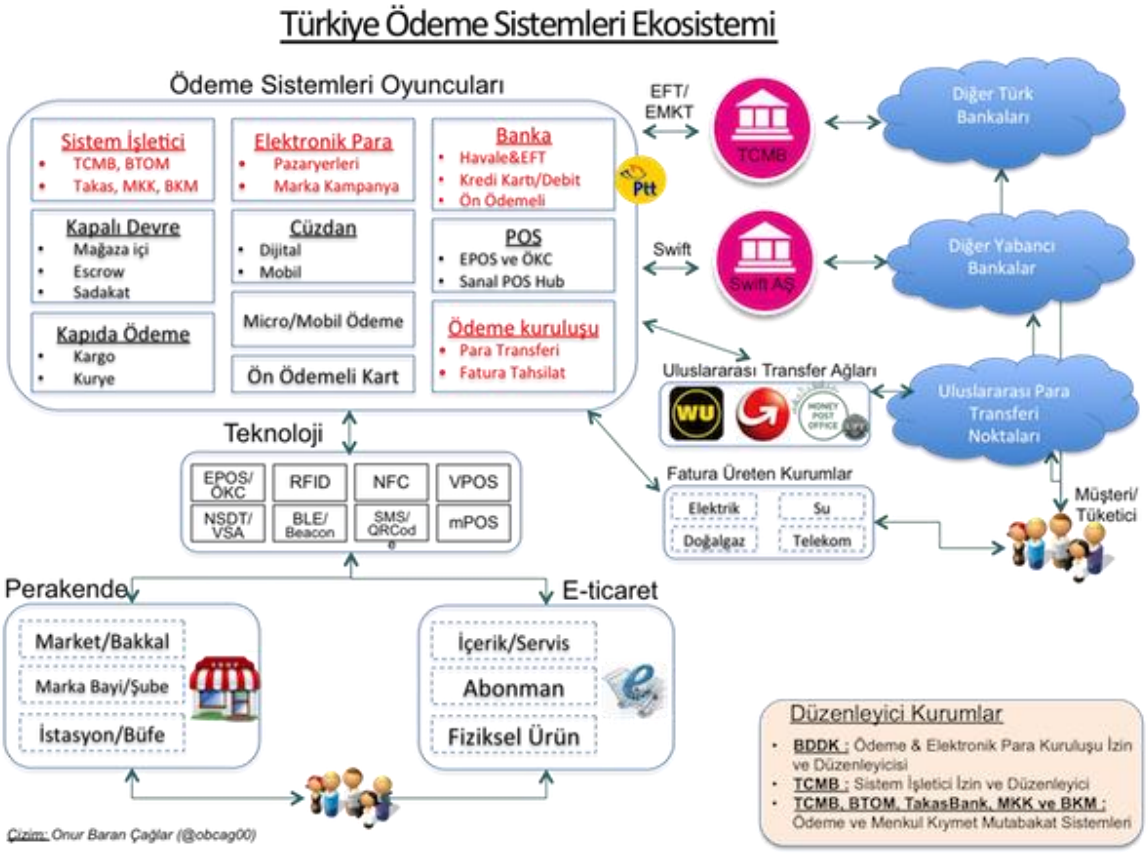
Siber savunma gibi alanlarda, saldırganların algılama sistemleri tarafından tespit edilmekten kaçınmak maksadıyla sürekli evrim geçirmeleri nedeniyle saldırı senaryolarını devamlı değiştirmeleri, anormallik tespit sistemlerinin bir öğrenme sistemine sahip olmalarını zorunlu kılmaktadır. Bu ancak, prensip olarak, sürekli denetlenen bir sinyalin sisteme geri beslendiği ve modelin, kavram değişimlerini veri kümesine dâhil etmek için son verilere verilen daha fazla ağırlıkla sürekli olarak eğitildiği çevrimiçi makine öğrenmesi kullanılarak başarılabilir.

Google tarafından geliştirilen Abacus projesi, bir bireyin akıllı telefonu tarafından toplanan; yazma paternleri, mevcut konum, hız ve ses paternleri gibi veri noktalarının çeşitliliğinden yararlanarak, sürekli bir güven skoru oluşturmak maksadıyla bu teknolojisinin nasıl çalışabileceğine güzel bir örnektir.

Sadece risklerin daha yüksek olduğu değerlendirildiğinde, sistem parola gibi ilave gereksinimler talep etmektedir. Bu çözümün, parmak izlerinden on kat ve günümüzde telefonların kilidini açmak için yaygın olarak kullanılan geleneksel dört basamaklı PIN kodlarından yüz kat daha güvenli olduğu kabul edilmektedir.[li]

Fiziksel ve sayısal dünyalar arasındaki bulanık çizgiler

Küresel olarak birbirlerine bağlı cihazların sayısındaki çok büyük artış (2025 yılına kadar sadece yoğunluk nedeniyle artacak olan büyümenin 75 milyar olması öngörülmektedir[lii]) kimlik ve erişim yönetim (IAM – Identification & Access Management)[liii] sistemleri üzerinde önemli bir baskı oluşturmaya başlamıştır.



2015 yılı başlarında, Garner tarafından geliştirilen kimlik ve erişim yönetimi ekibinde AR-GE Başkan Yardımcısı olan Ant Allan, geleneksel kimlik doğrulama sistemlerimin, IoT (Nesnelerin İnterneti) cihazlarından ziyade büyük oranda yalnızca insanlara odaklanması nedeniyle; IAM sistemlerinin birbirine bağlı cihazların çoğalmasına uyum sağlamayacağı konusunda bir uyarıda bulunmuştur.[liv]

Gelişen bu durum, IoT bünyesindeki cihazları güvenlik olaylarına karşı çok açık bir hale getirmiştir. Örneğin; 2014 yılında, yönlendiriciler, televizyonlar ve buzdolapları dâhil internete bağlı ev aletlerine yönelik dünyanın dört bir yanındaki işletmeler ve bireylere yönelik küresel bir saldırıda, 750,000'den fazla kötü amaçlı elektronik posta gönderilmiştir.[lv] Kişisel verilerin kamuya sızdırılması veya siber suçlular tarafından ele geçirilmesi durumunda, işletmeler ve hükümetlerin önemli mali, itibari ve yasal sonuçlarla karşı karşıya kalmaları kaçınılmazdır.[lvi]

İşletmeler ve hükümetler bu nedenle IoT genişleyip yaygınlaştıkça ortaya çıkan güvenlik açıklarını kapatmak için birbirleriyle yarışarak kimlik pazarının gelişmesine yön vermektedirler.

Küresel kimlik yönetiminde, artık sadece kullanıcılara odaklanma yerine, işlem ekosistemindeki bütün veri tabanı oluşumlarına dikkat edilmesi gerekliliği anlaşıldığında, kimlik yönetim yaklaşımı büyük ölçüde değişecektir. Geleneksel olarak kimlik ve erişim yönetimi (IAM) sistemlerinde olduğu gibi bir uygulamaya, hizmete veya cihaza bağlı bir kişinin kimliğini yönetmek artık yeterli değildir, günümüzde farklı cihazlar, uygulamalar ve hizmetler arasındaki ilişkiler de çok önemli hale gelmiştir.

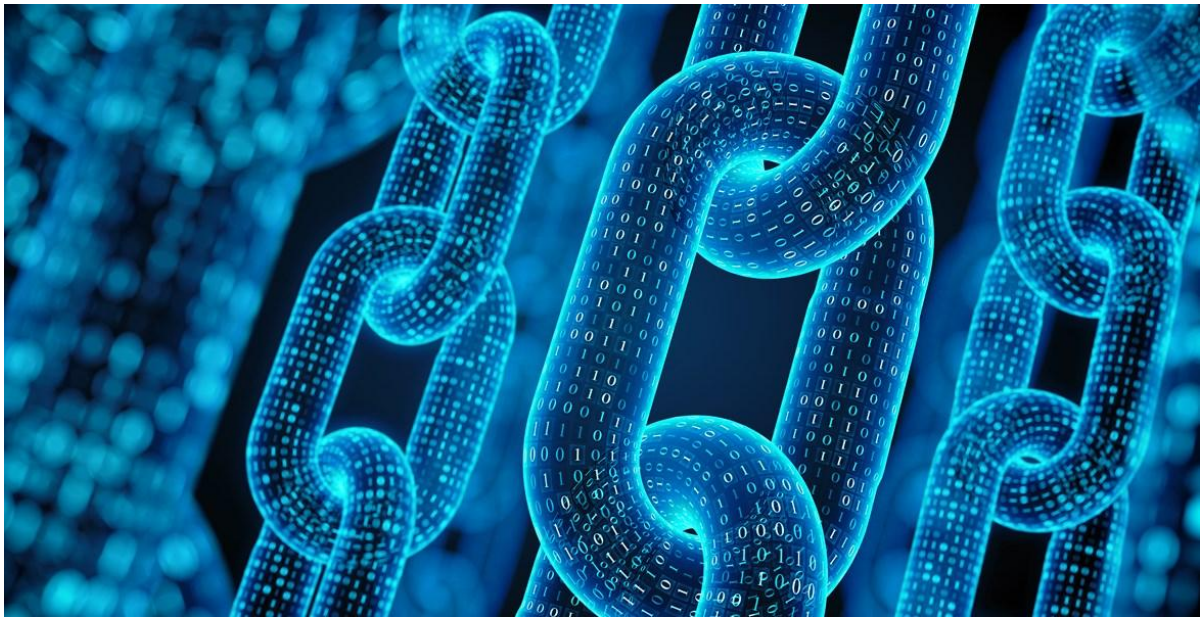
Kaynak: The Channel Pro Network

Nesnelerin Kimliği (IDoT – Identity of Things) bütün veri tabanı oluşumlarının aynı etkileşim çerçevesine sahip oldukları açık fakat güvenli bir ekosistemdir. Bu nedenle sayısal kimlik platformları, Nesnelerin İnterneti ekosisteminin bütün yelpazesinde güvenli ve güvenilir ilişkiler kurabilmek için giderek gelişmektedir. Bu, yukarıda incelenen sürekli kimlik doğrulama kavramıyla ilgilidir.

Bu yeni paradigmada başarılı olabilmek için IAM sistemleri; IP adresi, konum, oturum açma süresi ve diğer bağlamsal ipuçlarına dayalı olarak kullanıcılar için uyarlanabilir risk profilleri oluşturmak üzere içerik bilinçli olmalıdırlar.

Vatandaş-kontrollü veri

Veri gizliliği konusundaki artan endişeler ve "çöken bir sistem" algıları ile kamçılanan dünyanın dört bir yanındaki vatandaşlar, kendi verileri üzerinde daha fazla kontrole talep etmektedir. Büyük şirketler, devasa miktarda vatandaş verisini depolamakta ve kâr sağlamakta, ancak vatandaşların kimlik hırsızlığı riskine sokan veri ihlaller meydana geldiğinde yeterince sorumlu tutulmamaktadırlar. Bu algı sadece özel sektöre karşı değil, devletlere karşı da vardır.



"Blockchain Hayatımızı Değiştirecek" başlıklı yazıdan alıntıdır. Kaynak: STM Teknolojik Düşünce Merkezi

GDRP (General Data Protection Regulation – Genel Veri Koruma Yönetmeliği) gibi mevzuatlar; vatandaşlara işletmelerin verilerine erişim ve bu verilerin saklanmasını sınırlama hakkı vererek ve veri koruması alanında işletmeleri daha fazla sorumlu hale getirerek bu endişelerin bazılarını gidermeye yönelik bir girişimdir.

Kullanıcıların web sitelerinde kimlik doğrulaması yapmak maksadıyla Facebook, Linkedin, Twitter, Google+ vb. gibi sosyal kimliklerini kullanmalarına olanak sağlayan BYOI (Bring Your Own Identity – Kendi Kimliğini Getir) konsepti kullanıcılara verileri üzerinde daha fazla "sahiplik" sağlayan bir yaklaşımdır.

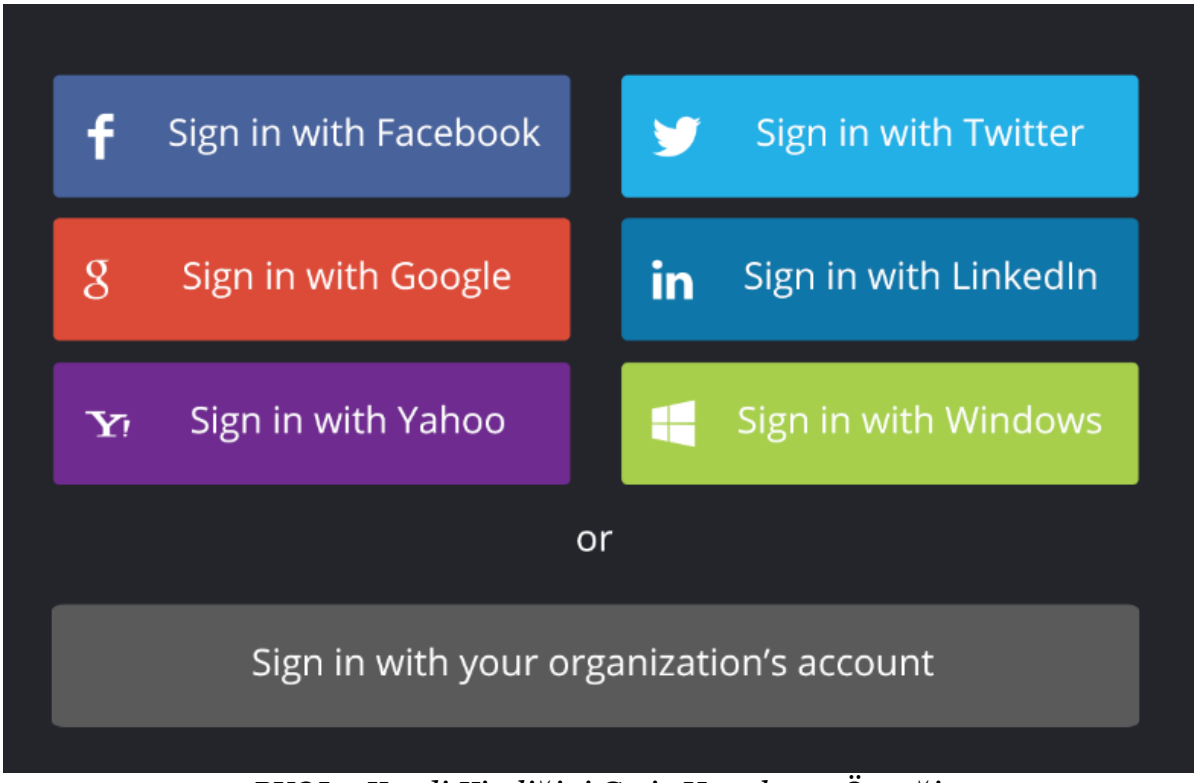
Ancak aslında BYOI, daha iyi UX (User Experience – Kullanıcı Deneyimi) arzusu ve işletmelerin idari maliyetlerinde azalma ile güdülenmektedir ve bazı çarpıcı veri gizliliği riskleri (örneğin, tek bir hata noktası 'SPOF - Single Point of Failure" olarak kimlik sağlayıcısı, kullanıcıların profilinin çıkarılması vb.) bulunmaktadır.

Tek Bir Hata Noktası, bir sistemin başarısız olması durumunda tüm sistemin çalışmasını durduracak bir parçasıdır. Bir iş pratiği, yazılım uygulaması veya başka

bir endüstriyel sistem olsun, SPOF'lar yüksek kullanılabilirlik veya güvenilirlik hedefine sahip herhangi bir sistemde istenmeyen bir durumdur. Yüksek düzeyde erişilebilir bir sistem, son kullanıcısı için kesintileri en aza indirebilmeli ve her türlü arıza durumunu hızlı bir şekilde atlatabilmelidir.

BYOI Konsepti

Çevrimiçi hizmetlere erişmek maksadıyla birden fazla sayısal kimliği yönetmek insanlar için önemli bir yük haline gelmiş durumdadır. Web sitelerinde gezinirken kullanıcılardan genellikle erişmek istedikleri her hizmet için bir sayısal kimlik oluşturmaları talep edilmekte, bu da kullanıcıları birden fazla hesap/token/parolayı yönetmeye zorlamaktadır. Bu durum kullanıcıları çeşitli risklere maruz bırakmaktadır ve bu sayısal kimliklerin çoğu birlikte çalışabilir nitelikte olmadığından ve işletmelerin sayısallaşması nedeniyle sayıları da sürekli arttığından bu modelin uzun vadede sürdürülebilir olmadığı açıktır. İnsanlar birçok alanda (domain) yeniden kullanabilecekleri, güvenli ve kolay bir şekilde sayısal kimlik oluşturabilmeyi istemektedirler. Benzer şekilde, ekonominin sayısallaşmasıyla birlikte, özel işletmeler de işlerini web'e taşımakta ve kullanıcıları güvenli bir şekilde tanımlamanın yollarını aramaktadır. Bu taleplere bir yanıt; kullanıcıların kendileri veya üçüncü bir tarafça yönetilen ve hizmetin dışında olan sayısal kimliği seçmesine ve kullanmasına olanak tanıyan bir sayısal kimlik yaklaşımı olan Kendi Kimliğini Getir (BYOI) konsepti tarafından sunulmaktadır.



BYOI – Kendi Kimliğini Getir Uygulama Örneği

Diğer teknolojik gelişmeler, gerçek vatandaş kontrolü ve yüksek güvenlik sağlayarak kimlik yönetimi hakkındaki düşünceleri değiştirme potansiyeline sahiptir. Başta blok

zinciri (blockchain) olmak üzere dağıtılmış defter teknolojileri (DLT – Distributed Ledger Technology) bunlara iyi bir örnektir.

Devlet örneği kullanıldığında, örneğin sosyal güvenlik numaraları gibi geleneksel vatandaş verileri merkezi bir veri tabanında depolanmaktadır. Bu durum, tek bir ihlal çok sayıda insanı etkileyebileceğinden ciddi bir güvenlik açığı oluşturmaktadır.

Dağıtılmış Defter Teknolojisi. Kaynak: LPEA

Öte yandan, dağıtılmış bir defter, bilgileri büyük bir ağdaki her bir katılımcı (node) tarafından bağımsız olarak depolayıp güncelleyerek merkezi olmayan bir hale getirmektedir.[lvii] Defterde yapılan her güncellemenin geçmişi, bütünlüğü ve doğruluğu herkes tarafından teyit edilebilmekte, ancak içeriği de şifrelenebilmektedir (giderek artan bir şekilde sıfır bilgi ispatı kullanılarak, bir işlemim gerçek amacını ifşa etmeden geçerli olduğunu gösterebilen ya da diğer hassas ayrıntılar[lviii]).

Sıfır Bilgi İspatı

Sıfır Bilgi İspatı (Zero Knowledge Proof), iki taraf arasında şifre veya işlemle ilgili herhangi bir bilgi kullanılmadan veri paylaşımına olanak sağlayan sayısal protokoldür. En temel biçimde sıfır bilgi gizliliği, (yaygın olarak ZKP diye adlandırılır) şifreler veya diğer hassas veriler kullanılmadan sayısal doğrulama sürecinin gerçekleştirilebileceği bir protokol olarak düşünülebilir. Gönderen veya alıcı tarafından hiçbir bilginin gizliliği asla ihlal edilmez. Bu güvenlik sistemi, üçüncü partiyle paylaşmadan veri iletişimini mümkün kılmaktadır.

Sıfır Bilgi İspatı ve Waldo Nerede Örneği

"Waldo Nerede?" adlı çocuk kitaplarında okuyucudan; çeşitli şeyler yapan insanların bulunduğu bir şekilde, gözlük takan, üzerinde kırmızı-beyaz bir kazak ve balıkçı şapkası olan Waldo'yu bulması istenmektedir. Yazar ispat eden, okur da doğrulayan olarak kabul edildiğinde; yazar elinde Waldo'nun kolayca bulunmasını sağlayan bir algoritma olduğunu iddia etmekte ve bunu sadece bir ücret karşılığı vereceğini ifade etmektedir. Okur ise algoritmayı istemekte ancak işe yaradığını görmeden ve teyit etmeden para ödemek istememektedir. Yani birçok işlemde olduğu gibi iki taraf işbirliği yapmak istemekte, ancak birbirlerine tam olarak güvenmemektedir.

Yazar elinde çalışan bir algoritma olduğunu ispatlamak için aşağıdaki şekilde ortadaki resmi yere koyar ve okuyucuya gözlerini kapamasını söyledikten sonra, üzerinde küçük bir oyuk olan ve resimden daha büyük siyah renkli bir karton ile resmi kapatır. Siyah karton üzerindeki küçük oyuk okuyucunun sadece Waldo'yu görmesini sağlamakta, ancak Waldo'nun resim içindeki yeri ve bulmacanın siyah karton altında nerede olduğu konusunda ona herhangi bir ayrıntı vermemektedir. Okuyucu tekrar gözlerini kapadıktan sonra siyah karton resim üzerinden alınır. Yazar okuyucuya; resim içindeki Waldo'nun tam yerini, onu nasıl bu kadar süratle bulabildiğini veya resim hakkında başka hiçbir söylemeksizin, Waldo'yu süratle bulabileceğini ispatlamıştır.

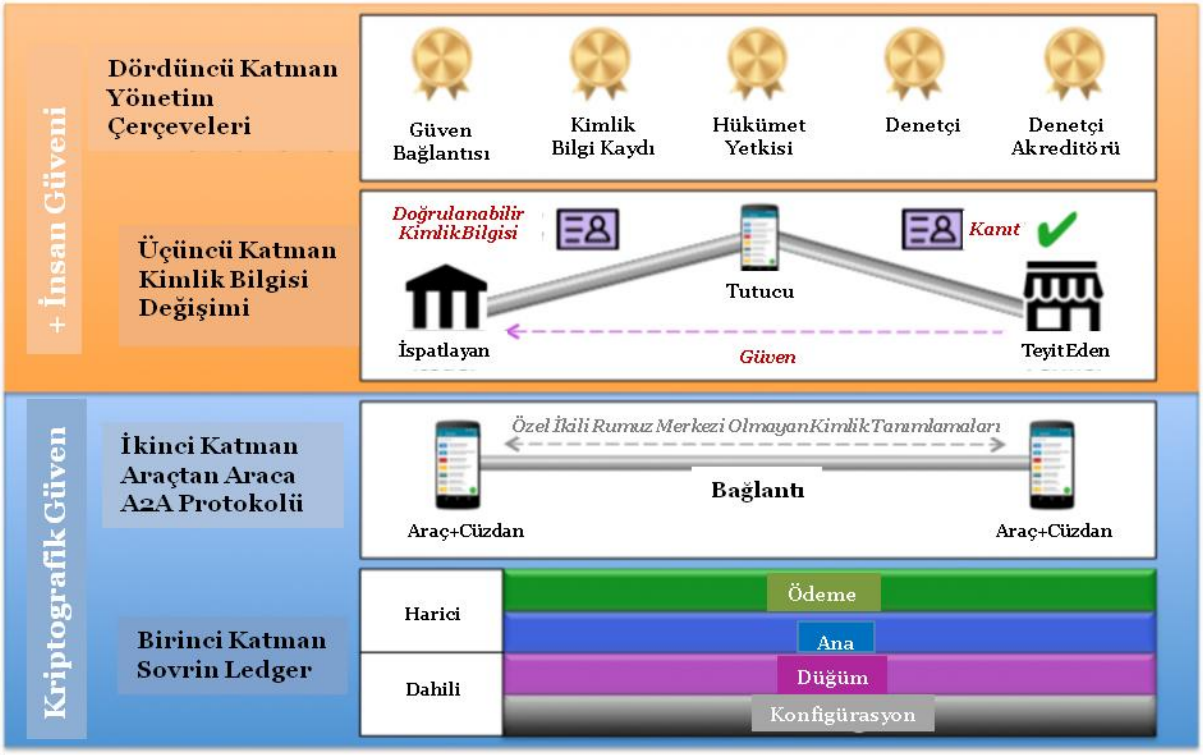
Sıfır Bilgi İspatı - Waldo Nerede Örneği

Belirli verileri hacklemek, milyarlarca defter arasındaki her bir defter girişinin bulunmasını ve daha sonra da zaman ve bilgi işlem açılarından büyük bir maliyetle ayrı ayrı "kırılmasını" gerektirmektedir, bu da veri tabanının bir bütün olarak çok güvenli olmasını sağlamaktadır.[lix]

Bu teknolojinin merkezi olmayan ve güvenli doğası, onu kimlik yönetimi açısından çok ilginç kılmaktadır ve birçok işletme hâlihazırda dağıtılmış defter tabanlı sistemlerin uygulanması üzerinde çalışmalarını sürdürmektedir. Temel kullanım durumu, bir kullanıcı olarak, ağda bulunan; belgeler, biyometri, sağlık verileri, akademik sertifikalar vb. gibi bütün verilerin daima güvenli olan onaylı kopyalarına sahip olunmasıdır.

Akıllı defterler kullanılarak, belirli veriler görmesi gerekenlerle paylaşılabilir, gerektiğinde erişimler iptal edilebilir ve başka bir tarafın verileri diğerlerine iletip iletmeyeceği kontrol edilebilir. Önemli olan husus kullanıcının kendi kimliği üzerinde yegâne mülkiyet ve kontrole sahip olmasıdır.

UPort, Jolocom, Evernym, Sovrin ve Riddle & Code dâhil olmak üzere birden fazla yeni şirket, bireyler ve makineler için bu tür "özerk kimlik" sistemleri üzerinde çalışmakta ve uygulamaktadır. Özerk kimlik (SSI – Self-Sovereign Identity), bireylere sayısal kimliklerinin kontrolünü veren sayısal kimlik uygulamalarına yönelik bir yaklaşımdır.



Sovrin Yığını, Sovrin Foundation ve küresel SSI (Özerk Kimlik) toplumu tarafından geliştirilmiştir ve 2019 yılı başlarında piyasaya sürülmüştür. Açık-kaynak Sovrin Yönetişim Çerçevesi'nin bir parçası olarak düzenlenmiştir. Sovrin Yığını, alt iki tabakanın makine-makine arası ihtiyaç duyulan kriptografik güveni ve üst iki tabakanın da iş, yasal ve sosyal etkileşimler için insan güvenini sağladığı SSI altyapısının, dört katmanlı bir yığın olarak ilk kavramsallaştırılmasıdır. Kaynak: sovrin

Temel olarak dağıtılmış defter/özer kimlik sistemleriyle, potansiyel bir gelecek senaryosunda; kimlik ekosisteminin farklı aktörlerinin (örneğin hükümetler) rol ve değer dağılımının yeniden şekillendiği görülebilir. Veri yönetiminde (kâr açısından) işletme/hükümetten bireysel kullanıcılara doğru bir güç kayması olduğu görülebilir. Verilerinin yegâne sahibi olan bireyler, çevrimiçi işlemler yaparken verilerini kelimenin tam anlamıyla "satıp satmamayı" kendileri seçebilirler.

Dağıtık Defter Teknolojisinin Faydaları

- Gerçek zamanlı işlem yerleştirme ve otomasyonu: akıllı sözleşmeler, örneğin işlemler veya otomatik ödemelerin doğrulanmasını otomatik hale getirebilir;
- Dağıtılmış verilerin şeffaflığı ve arabulucu sistemlerden arındırılması: bu, tek bir gerçek kaynağın olmasıyla uzlaşma çalışma miktarını önemli ölçüde azaltır;
- Noter işlevi: blok zincir, belgelerin doğrulanmasını ve kayıtların izlenebilirliğini garanti edebilir.

Değişen kimlik ekosistemi

Kimlik sağlama ekosistemi, yeni iş modelleri ve aktörlerin ortaya çıkmasıyla birlikte temel değişimlerden geçmektedir. Bu genişleme, büyük ölçüde, hem kendi müşterilerine hem de diğer kuruluşlara giderek daha fazla kimlik çözümleri veya hizmetleri sağlayan özel sektör kuruluşlarının müdahalesi sayesinde olmaktadır.

Geleneksel olarak kimlik ekosisteminde açıkça tanımlanmış roller bulunmaktadır. Hükümetler vatandaşlara kimlik bilgileri sağlamışlar ve bu belgeler daha sonra sınırlı sayıda da olsa insanların kimliklerini fiziksel olarak kanıtlamasında kullanılmıştır. Kredi ofisleri gibi kuruluşlar, potansiyel müşterilerle ilgili temel özellikleri toplama ve başkalarına satma konusunda uzmanlaşmışlardır.

Günümüzde her ne kadar bu roller sürüyor olsalar da, kamu ve özel sektörler arasında kullanıcı tanımlamasını gerektiren veya bundan faydalanabilecek çevrimiçi hizmetlerin yaygınlaşması pazarı genişletmiş ve değiştirmiştir.

Bankalar artık kimlik çözümlerinin araştırılması ve geliştirilmesi için yılda toplamda bir milyar dolardan fazla para harcamakta, bu da onları, ulusal hükümetler ve polis teşkilatlarının dahi önünde, dünyanın önde gelen yatırımcıları yapmaktadır.[lx]

Bankalar, telekom operatörleri ve postaneler dâhil olmak üzere, daha önce kimlik doğrulaması yapan ve düzenleyici nedenlerle kimlik bilgilerini toplayan aktörler, günümüzde bu hizmeti doğrulanmış kimliklerle çalışmak zorunda olan diğer işletmelere satmaktadırlar. İtalya'da SPID[lxi], İsveç'te BankID[lxii], Birleşik Krallık'ta GOV. UK Verify[lxiii] ve Belçika'da Itsme[lxiv] dâhil olmak üzere, özel sektör kimlik sağlayıcılarından oluşan bir federasyona dayalı, hükümetin yönlendirmesi altında veya hükümetten bağımsız çeşitli elektronik kimlik düzenlemeleri ortaya çıkmıştır.

İtalya, İsveç, Birleşik Krallık ve Belçika'da Kimlik Sağlayıcıları

Facebook ve Google tarafından kullanıcıların hizmetine sunulan BYOI (Bring Your Own Identity) çözümleri, kullanıcılara farklı hizmetlerde kimlik doğrulaması yapabilmeleri için sosyal profillerden faydalanma imkânı tanımaktadır. Mevcut çözümler, kullanıcıların gerçek kimlikleriyle ilgili daha düşük bir güven düzeyine sahip olsalar da, temel web siteleri ve hizmetlerine erişimde giderek çok daha popüler hale gelmişlerdir.

Kullanıcıların sosyal ağları ve gruplaşmanın gücü, bir bireyin kimliğini kanıtlamada gerçekten faydalıdır, ancak bireysel olarak kullanılamaz. Sonuç olarak, sosyal ağ faaliyetleri, daha önce de ifade edildiği gibi, insanların sayısal ayak izlerine dayanan daha dinamik kimlik risk analiz yaklaşım ve çözümlerine katkıda bulunabilirler.

Tek bir kimlik bilgisiyle (SSO - Single Sign-On) çok sayıda uygulamaya erişim sağlayan VERIMI gibi platformlar da günümüzde kullanıcıların hizmetine sunulmuş durumdadır. Almanya çıkışlı ve 10 uluslararası kuruluş (Allianz, Daimler, Deutsche Bank, Deutsche Telecom ve Lufthansa dâhil) ile ortak olan VERIMI, ortak kuruluşların sağladığı hizmetler ve ürünler ile birlikte kullanılabilen güvenli bir kimlik (pasaport, kimlik kartı veya ehliyet gibi resmi belgelerden elde edilen) sağlamayı hedeflemektedir.

Platform son derece güvenilirdir, bütün kimlik doğrulama seviyelerini desteklemektedir ve kullanıcıların kendi verileri üzerinde tam bir kontrol sahibi olmalarını sağlamaktadır. Örneğin, kullanıcılar hangi kişisel verilerini hangi ortaklar ile paylaşmak istediklerine kendileri karar verebilmekte ve onay verdikten sonra da herhangi bir zamanda iptal edebilmektedirler.[lxv]

VERIMI, GDPR (General Data Protection Regulation – Genel Veri Koruma Yönetmeliği) gibi yasal yükümlülüklerini yerine getirirken, hem güvenlik hem de kullanım kolaylığı taleplerine yanıt veren yeni kimlik çözümlerine güzel bir örnektir.

Özel sektör katılımının artmasına rağmen, hükümetlerin vatandaşların kişisel verilerinin yeterli şekilde korunmasını sağlamak ve biyometrik verileri işleyen kamu ve özel sektör kuruluşlarının hesap verebilirliğini sağlaması büyük önem arz etmeye devam etmektedir.

Devlet buna ilave olarak, bireyler hakkında toplanan farklı veri noktalarının artan bir şekilde birbirlerine bağlanmalarının bir sonucu olarak, bireysel profil oluşturma ve izlemelere karşı da önlemler almalıdır.

Kimliğin sağlanması konusunda, hükümetler ve özel kimlik sağlayıcılar arasında, kesinlikle daha fazla işbirliği yapılmasına ihtiyaç bulunmaktadır. Hükümetler tarafından oluşturulan elektronik kimlik tanımlama (eID) düzenleri kanıtlanmış ve iyi tesis edilmiş kimlik doğrulama prosedürlerine dayalı olarak genellikle yüksek seviyede güvene ihtiyaç duyabilirler.

Devlet tarafından verilen elektronik kimlikler bu nedenle diğer kuruluşlar tarafından sağlanan kimlikleri "doğrulamak" ve "teyit etmek" maksatlı kullanılabilir. Bu yaklaşım, özellikle eIDAS (Elektronik Kimlik belirleme ve Güven Hizmetleri) yönetmeliği kapsamında tanınan elektronik kimlikler için AB Üye Devletleri tarafından halen araştırılmakta olan olasılıklardan bir tanesidir.[lxvi]

ELEKTRONİK KİMLİK EVRİMİNİN UYGULAMALARI

Kısa ve orta vadede senaryolar

Gözlemlenen trendlere ve oyun alanındaki daha güçlere bakıldığında, önümüzdeki yıllarda aşağıda belirtilen gelişmelerin gerçekleşmesi beklenmektedir:

2 Yıl İçinde:

- ✓ Küresel akıllı telefon kullanıcılarının sayısı 6 milyarı (tahmini küresel nüfusun %80'i) aşacaktır.[lxvii] Önce-Mobil platformlar ve çözümlere yönelik talep çok büyük olacaktır.
- ✓ Yeni üretilen bütün akıllı telefonlar biyometrik özellikli olacak ve biyometrik cihaz sayısı 4,8 milyara ulaşacaktır.[lxviii]
- ✓ 50 milyar bağlı cihaz piyasada dolaşımda olacaktır. Bu büyüme, IAM (Identity & Access Management – Kimlik & Erişim Yönetim) sistemlerinin, Nesnelerin İnterneti'ni (IoT) etkin bir şekilde güvence altına alma yeteneğini geride bırakmaya devam edecektir.
- ✓ Çok uluslu şirketleri kapsayan daha fazla veri ihlali, daha güvenli kimlik yönetimine olan talebi daha da yükseltmeye hizmet edecektir. Güvenli Veri Koruma Yönetmeliği'nin (GDPR) etkileri giderek daha fazla hissedilecek ve kullanıcı verilerinin yanlış kullanımı nedeniyle büyük işletmelere karşı birçok yüksek ceza vakası açılacaktır.

- ✓ Parmak izi tanıma en popüler biyometrik yöntemi olmaya devam edecek, ancak yüz tanıma, davranışsal ve çok modlu biyometriye olan ilgi artacaktır. Davranışsal biyometri ve analitik tabanlı sürekli kimlik doğrulama çözümleri sunan sağlayıcıların sayısı artmaya devam edecektir.
- ✓ Mobil kimlik çözümleri, güvenlik ve kullanım kolaylığının bir karışımını sunan birkaç yerleşik şirketin ortaya çıkmasıyla gelişmiş ülkelerde önemli bir ivme kazanacaktır.
- ✓ Neredeyse bütün gelişmiş ülkeler, ulusal seviyede onaylanmış bir elektronik kimlik tanıma sistemine sahip olacak, ancak edinme oranları ülkeler arasında tutarsızlıklar gösterecektir.
- ✓ Kamu/özel sektör işbirliği artacak, ancak ülkeler arasında tutarsızlıkla olmaya devam edecektir. Bazı ülkelerde, hem kamu hem de özel hizmetler için benzer çözümler sunan özel sektör kimlik sağlayıcıları ve özel sektör hizmetleriyle kullanım için mevcut ulusal elektronik kimlik sistemleri ile kamu ve özel sektör liderliğindeki çözümler arasında önemli bir örtüşme görülecektir. Diğer ülkelerde, kamu hizmetleri için kimlik yönetimi, özel sektörün bağımsız olarak gelişmesiyle sıkı bir şekilde hükümet kontrolü altında olacaktır.
- ✓ Elektronik Kimlik Belirleme ve Güven Hizmetleri Yönetmeliği kapsamında EIDAS Ağına dâhil edilen kimlik sistemlerinin sayısı bütün AB ve Avrupa Ekonomik Alanını kapsama seviyesine yaklaşacaktır. Ağ içinde kullanım için bazı özel sektör çözümleri, kendi başlarına ya da onaylı bir sistemin türevi olabilecektir.

5 Yıl İçinde

- ✓ Gelişmiş ülkelerde yetişkinlerin %90'ı akıllı telefon kullanacaklar[lxix] ve akıllı telefonların %80'i yapay zekâ kabiliyetli olacaktır.[lxx] 5G[lxxi] abone sayısı 5 milyara ulaşacaktır.[lxxii]
- ✓ Mobil biyometri, 2018 yılının 17 kat daha fazlası olarak yıllık mağaza içi ve uzaktan mobil ödemelerde 2 trilyon dolarlık bir değere ulaşacaktır.[lxxiii]
- ✓ Kullanıcılar, en azından bir dizi özel ve kamu hizmetleri için son derece güvenli ve yeniden kullanılabilir, sorunsuz mobil tabanlı kimlik çözümlerini bekler hale gelecektir. Ayrıca, hangi bilgilerin, ne zaman ve kiminle paylaşılacağını seçerek, kimlik özellikleri üzerinde giderek daha fazla kontrole sahip olmak isteyeceklerdir.
- ✓ Çok yönlü ve gelişmiş kimlik çözümleri çoktan beridir mevcuttur. Daha önce dağınık ve parçalanmış durumda olan kimlik piyasası, sektörler arasında

analitik ve davranış esaslı kimlik yönetimi sağlayan büyük, ana akım aktörlerle birlikte birçok ülkede bir araya gelerek güçlerini birleştirmeye başlamıştır.

- ✓ Blok zinciri kimlik yönetim piyasası, bankacılık ve finansal hizmetler başta olmak üzere, 2018 yılından beri iki ikiye katlanmış durumdadır.[lxxiv] Bununla birlikte büyüme, ortak düzenleyici standartların eksikliği ve halen belirsizliğini koruyan düzenleyici ortam nedeniyle sınırlı seviyede kalacaktır.

- ✓ Kimlik sağlama konusunda başarılı olan kamu/özel ortaklıkları daha da yayınlaşacaktır. Birleşmiş özel sektör aktörleri tarafından desteklenen hükümet kontrolündeki kimlik sistemleri sektörler arası hizmetlere erişim maksadıyla kullanılacaktır. Alternatif olarak, hükümetler tarafından uygun bulunan ve onaylanan özel sektör kimlik yönetim sistemleri nüfusun çok geniş kesimlerine hizmet sağlayacaktır. Hükümetlerin rolü giderek kimlik sağlayıcıdan tüketiciye ya da onaylayana dönüşecektir.

- ✓ Bütün Avrupa Birliği ve Avrupa Ekonomik Topluluğu ülkelerinde, Elektronik Kimlik Belirleme ve Güven Hizmetleri Düzenlemesi (eIDAS) Ağı'na çok sayıda kamu ve özel sektör liderliğinde olan kimlik sistemleri katkıda bulunacaktır.

10 Yıl İçinde

Bu kadar zaman sonraki gelişmeleri doğru olarak tahmin etmek zor olabilir, ancak en azından aşağıda sıralanan gelişmeler beklenebilir:

- ✓ Neredeyse dünyanın dört bir yanında küresel akıllı telefon kullanımı yaygınlaşacaktır.
- ✓ Küresel olarak elektronik kimlik kullanım oranı çok yükselecektir.
- ✓ Yüksek hızlı internet yaygınlaşacak ve ucuzlayacaktır.

- ✓ Fiziksel ve sayısal yaşamın eksiksiz bir şekilde birleşimi gerçekleşecek ve kullanıcılar sürekli doğrulanan ve yeni nesil cihazlar aracılığı ile her zaman ve her yerde güvenli işlemler yapacaktır.

- ✓ Her bir kullanıcının kendi kontrolünde olan ve hizmetlerin çoğu için yeniden kullanabilecekleri bir sayısal kimlikleri bulunmaktadır. Blok zincir tabanlı veya diğer Özerk Kimlikler ana kullanım şeklidirler.

- ✓ Kimlik doğrulama hiçbir zaman daha güvenli ve sofistike olmasa da siber tehditler, muhtemelen yapay zekânın kötüye kullanımı yoluyla eşit derecede sofistike bir hale gelecektir. Her zaman olduğu gibi, güvenlik ve veri gizliliği devamlı sıkıştıran ve baskı uygulayan bir endişe kaynağı olacaktır. Kuantum teknolojisinin gelişmesi nedeniyle yaygın kriptografik güvenli öğelere yönelik tehditler önem kazanacaktır.

- ✓ Kimlik yönetimi küresel bağlamda karşılıklı çalışabilir hale gelecektir.

- ✓ Devletin kimlik sağlama ve yönetimiyle ilgili rolü büyük ölçüde değişmiş olacak, belki de doğası gereği devlet tamamen düzenleyici rolüne doğru kayacaktır.

Avrupa Komisyonu[lxxv]'nun dikkate alması gereken hususlar

Avrupa Komisyonu, meydana gelecek değişikliklerde önemli ancak çok zor bir rol üstlenmek zorunda kalacaktır. Avrupa Komisyonu, daha güvenli ve kullanıcı dostu çözümler getireceğinden, üye devletleri elektronik tanımlamada rekabet ve yeniliğe teşvik etmelidir.

Avrupa Komisyonu bunun yanı sıra üye devletlerin hükümetin potansiyel olarak değişen rolüne ve yeni iş modellerine hazırlanmalarına da yardımcı olmalıdır. Aşağıda, üzerinde daha fazla araştırma yapılması gereken bazı önemli hususlar sıralanmıştır.

AB Aşı Pasaportu. Kaynak: Frank Hoermann/SVEN SIMON/Picture Alliance

Ulusal hükümetler ile özel sektör arasındaki işbirliğine katkı sağlamak

Ulusal düzeyde elektronik kimlikler, kamu ve özel sektör arasındaki aktif işbirliğinden önemli ölçüde fayda sağlayacaktır. Kamu ve özel sektör arasındaki işbirliği birkaç şekilde gerçekleşebilir:

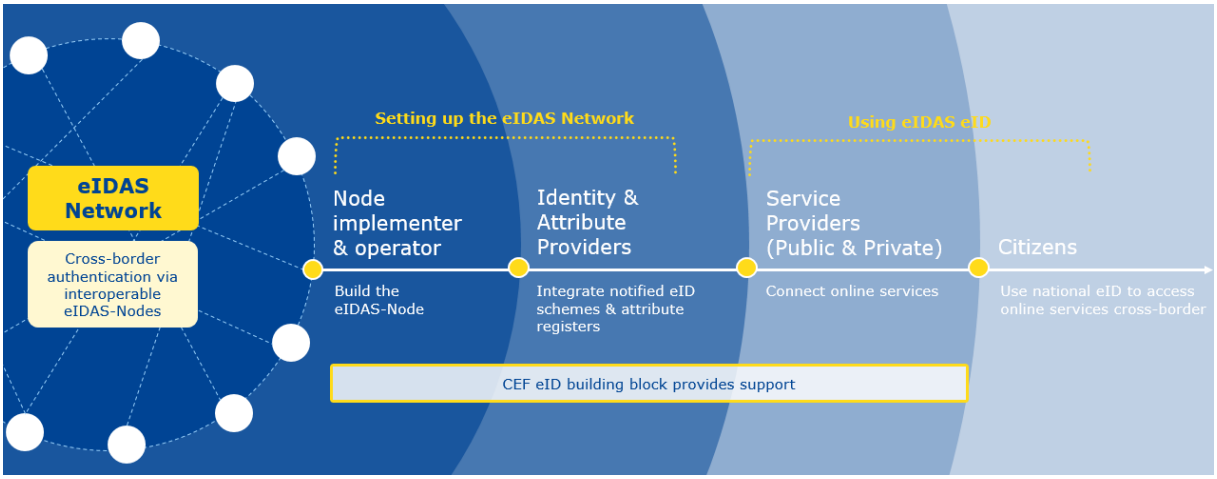
- ➢ Ulusal bir elektronik kimlik (eID) sistemine katkıda bulunan devlet tarafından yönetilen birleşmiş özel kimlik sağlayıcıları.
- ➢ Hükümet tarafından uygun görülen ya da tanınan özel bir elektronik tanımlama sistemi.

- Daha yüksek bir güvenlik düzeyini başarmak maksadıyla türettikleri kimlikleri doğrulamak için hükümet elektronik tanımlama sistemini kullanan özel kimlik çözümleri.
- Hem kamu hem de özel çevrimiçi hizmetlere erişmek maksadıyla yukarıda belirtilen yaklaşımlardan bir tanesini izleyen elektronik tanımlama sistemi.

Kamu/özel sektör ortaklıkları, hükümetlerin en son yeniliklerden faydalanmasına, yeni işler yaratırken özel sektör tarafından sunulanların güvenliğini güçlendirmeye yardımcı olmasına ve vatandaşların bütün hizmetler için her yerde ve güvenli bir çözüme erişmesine olanak tanıyacaktır. Bununla birlikte, böyle bir ortaklık oluşturmak, ortaklığın türü ve kapsamının ve ayrıca iş modelinin dikkatli bir şekilde değerlendirilmesini gerektirmektedir.[lxxvi]

Avrupa Komisyonu konuyla ilgili olarak Üye Devletler arasında diyaloğa aktif bir şekilde katkı sağlayabilir ve başarılı uygulamaları örneklerine katkı sağlayabilir.

EIDAS Ağının özel sektöre açık ve uyumlu kalmasının sağlanması



Elektronik Tanımlama Yönetmeliği, ulusal eID sistemlerinin Avrupa dâhilinde karşılıklı çalışabilirliğini sağlamayı başarmayı hedeflemektedir ve bu, günümüzün giderek birbiriyle daha bağlantılı ve sınırların kalktığı bir dünyada gerçekten önemli ve değerli bir hedeftir. Bununla birlikte eIDAS Ağının yararlı olabilmesi için yukarıda da ifade edildiği gibi giderek artan bir şekilde ulusal düzeyde mevcut kamu/özel ortaklıklarından faydalanması gerekmektedir.

Bu, ulusal hükümetlerin, onları ağa katılmaya teşvik etmek ve desteklemek için özel sektör kimlik ve hizmet sağlayıcılarla birlikte çalışması gerektiği anlamına gelmektedir. Bu maksatla farkındalığı artırmanın yanı sıra, ulusal düzeyde Avrupa Komisyonu tarafından desteklenmesi gereken önemli ilk adımlar aşağıdadır:

- eIDAS'ın özel sektör tarafından erişimine açılması kararının verilmesi.

- Özel sektörün katılımının sağlanması için ticari bir modelin tasarlanması.
- Özel sektör katılımı için bir sorumluluk modelinin belirlenmesi.

Avrupa Komisyonu bunlara ilave olarak eIDAS elektronik tanımlamanın özel sektör ihtiyaçlarına yararlı olmasını da sağlamalıdır. Örneğin, sadece temel kullanıcı bilgileri sağlayan bir eIDAS minimum veri kümesi, bir özel sektör hizmet sağlayıcısının gerektireceği bütün sektörel kimlik özelliklerini sağlamayabilir.

Değişen bir dünya için düzenlemeler

Dünya, vatandaşların kendi verileri üzerinde daha fazla kontrole sahip olması (belki de nihayetinde gerçekten özerk tanımlama) yönünde ilerlerken, aynı zamanda yaşamın artan sayıda yönlerini izlemek için çeşitli analitiklerin ortaya çıktığına da tanıklık etmektedir. Bu izleme, kimliklerimizi (örneğin davranışsal biyometri) güvende tutmaya hizmet edecek, ancak aynı zamanda, özellikle gelecekte güçlü özel sektör kurumlarının baskın kimlik sağlayıcıları olarak ortaya çıkmaları durumunda "büyük birader" düşüncesini de gündeme getirecektir.

Avrupa Komisyonu kısa vadede mevcut düzenlemenin "vatandaş kontrolü" ruhuna uygun hale getirilmesini sağlamalıdır. Örneğin Genel Veri Koruma Yönetmeliği (GDPR-General Data Protection Regulation), vatandaşları sorumlu tutmayı amaçlarken, eIDAS Yönetmeliği ise doğası gereği vatandaş merkezli (örnek vermek

gerekirse, kullanıcı nitelikleri eIDAS beyanında varsayılan olarak seçilmektedir) değildir.

eIDAS tarafından sağlanan hizmetlerin evrimi, örneğin sıfır-bilgi taleplerini destekleyebilir, gerçek niteliklerin paylaşılması yerine Evet/Hayır soruları (örneğin, kullanıcının gerçek doğum tarihini paylaşmak yerine 18 yaşından büyük olduğuna dair kanıt sağlamak) yanıtlanabilir.

Avrupa Komisyonu uzun vadede ise blok zincir tabanlı kimlik yönetimini düzenleyen ve sayısal kimliklerin çeşitli kuruluşlar tarafından kötü maksatlı kullanılmasını engelleyen çok önemli bir rolü üstlenmelidir.

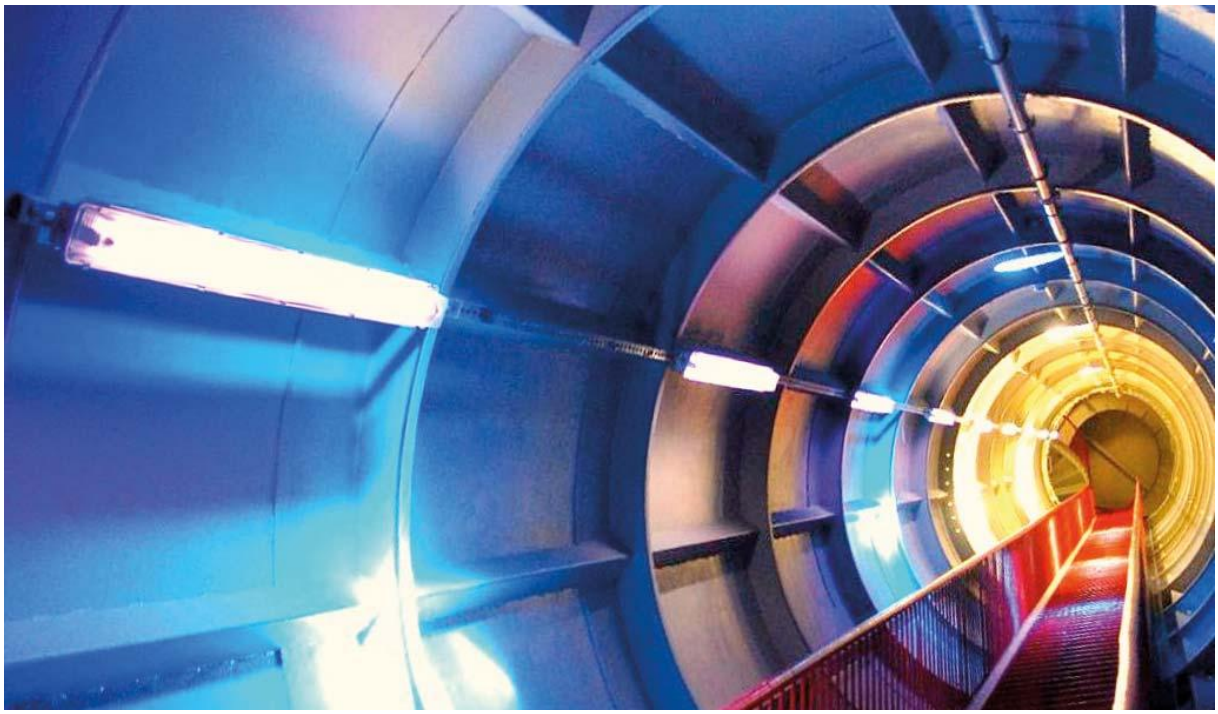
SONUÇ

Bu makale, mevcut elektronik tanımlama ortamının üst düzey bir resmini sağlamanın yanı sıra, evrimini karakterize eden temel trendlere de genel bir bakış sunmayı amaçlamaktadır. Makalede ayrıca, bu trendleri şekillendiren daha geniş bağlamsal güçlerin bir özeti ve bu trendlerin toplum ve özellikle Avrupa Komisyonu açısından ne gibi etkileri olabileceğine dair görüşler de sunulmaktadır.

Dünya giderek daha da küreselleşirken ve birbirine çok daha fazla bağlantılı hale gelirken, anında ve kullanışlı çevrimiçi işlemlere olan talep hiç bu kadar yüksek olmamıştır. Bunun yanı sıra benzeri görülmeyen bir siber risk çağına da girmekteyiz ve kişisel verilerin korunması da artık çok ön plandadır. Güvenlik ve kullanıcı deneyiminin bu iki ayağı, elektronik tanımlama teknolojisindeki yeniliklere yön vermektedir.

Piyasada ortaya çıkan elektronik tanımlama çözümlerinde; mobil, biyometri, yapay zekâ (AI-Artificial Intelligence), nesnelerin interneti (IoT-Internet of Things) ve analitiğin kesiştiklerini görmekteyiz. Ayrıca, blok zinciri gibi teknolojiler, kamu ve özel sektör arasındaki yeni ilişkilerle zaten yeniden şekillendirilmiş olan bir

ekosistem olan eID ekosistemini tamamen bozabilecek yeni bir güven çerçevesi oluşturmaya çalışmaktadırlar.



Kaynak: Keesing Platform

Bu değişikliklerin, önümüzdeki beş yıl ve sonrasında toplum üzerinde derin bir etkisi olacaktır. Avrupa Komisyonu, ileriye dönük olarak, hem elektronik tanımlamada rekabet ve yeniliğin destekleyicisi olmalı, hem de kimlik verilerinin kötü maksatlı kullanılmasına karşı bir koruma görevi üstlenmelidir.

Bu makalede belirtilen bilgi ve görüşler yazarlara aittir ve Avrupa Komisyonu'nun resmi görüşlerini yansıtmamaktadır. Avrupa Komisyonu, bu çalışmada yer alan verilerin doğruluğunu garanti etmemektedir. Ne Avrupa Komisyonu ne de Avrupa Komisyonu adına hareket eden herhangi bir kişi, bu makalede yer alan bilgilerin kullanımından sorumlu tutulamaz.

***Çevirenin Notları**: Avrupa Komisyonu için Deloitte tarafından yapılan 'Trends in electronic identification" başlıklı çalışma aslına sadık kalınarak çevrilmiş, anlaşılmayı kolaylaştırmak maksadıyla çeşitli kaynaklardan alıntılar çeviren tarafından son not olarak eklenmiştir.*

SON NOTLAR

---

[i] ***Sayısal Kimlik****: Sayısal kimlik, kullanıcıların farklı dijital ortamlarda kim olduklarını ispatlamaya yarayan kimlik bilgilerinin bir uzantısı olarak tanımlanabilir.* https://circlelove.co/dijital-kimlik-nedir/

[ii] ***Akıllı Kartlar****: Akıllı kartlar, kredi kartı boyutlarında içerisinde işlemci, RAM ve ROM belleği bulunan gömülü bir mikroçipe sahip donanımlardır. Üzerinde manyetik şerit, barkod, temassız radyo frekans vericileri gibi farklı teknolojileri bulundurabilir. Günümüzde giriş kontrolü, elektronik ticaret, kimlik doğrulama, kişisel gizlilik gerektiren birçok uygulamada çok yaygın olarak kullanılmaya başlanmıştır. Recep Selami Özbey, Akıllı Kart Teknolojileri, TÜBİTAK UEKAE Gebze, KOCAELİ.*

https://kamusm.bilgem.tubitak.gov.tr/dosyalar/makaleler/Akilli%20Kart%20Teknolojileri.pdf

[iii] ***Blok Zinciri:*** Blockchain *bir iş ağındaki işlemlerin kaydedilmesi ve varlıkların takip edilmesi sürecini kolaylaştıran, paylaşılan ve üzerinde değişiklik yapılamayan bir büyük defterdir.* Varlıklar *somut (ev, araba, nakit, toprak) veya soyut (fikri mülkiyet, patent, telif hakları, marka) olabilir. Değerli hemen hemen her şey bir blockchain ağında izlenebilir ve üzerinde işlem yapılabilir, bu da riski azaltır ve işe dâhil olan tüm maliyetlerin düşürülmesini sağlar.*
https://www.ibm.com/tr-tr/topics/what-is-blockchain

[iv] *Bu çalıştay 30 Ocak 2018 tarihinde Belçika'nın Brussels kentinde Deloitte Gateway Building'de; AB Kamu Hizmetleri Politikaları biriminden Benoit Vandresse ve Marie Eichholtzer, Deloitte Digital'den Nils Mc Grath, Saki Kourtidis ve Rory Aston James, Risk Danışmanı Yasemin Doğan, Cyber Risk'ten Joran Frik, Cristof Fleurus ve Jan Vanhaecht ile TS&A'dan Frédéric Berger ve Benoit Vermoortel katılımlarıyla gerçekleştirilmiştir.*

[v] *USAID, Identity in the digital age - Sayısal çağda kimlik: infrastructure for inclusive development – kapsamlı gelişme için altyapı, Eylül 2017,*
https://www.usaid.gov/digital-development/digital-id/report

[vi] ***E-Ticaret:*** *Elektronik ticaret ya da kısaca e-ticaret, 1995 yılından sonra İnternet kullanımının artmasıyla ortaya çıkan, ticaretin elektronik ortamda yapılması kavramıdır. Mal ve hizmetlerin üretim, tanıtım, satış, sigorta, dağıtım ve ödeme işlemlerinin bilgisayar ağları üzerinden yapılmasıdır. Elektronik ticaret, ticari işlemlerden biri veya tamamının elektronik ortamda gerçekleştirilmesi yoluyla reklam ve pazar araştırması, sipariş ve ödeme, teslimat olmak üzere üç aşamadan oluşmaktadır. Elektronik ticaret, tüm dünyada ticaretin serbestleştirilmesi eğilimi ile birlikte, 2000'li yıllardan sonra yaşanan ve bilgi iletişimini kolaylaştıran teknolojik gelişmelerin bir parçası olarak ortaya çıkmıştır. Geleneksel pazarlama yöntemlerine, İnternet olanaklarını da ekleyen kuruluşlar, sadece belirli bir kitleye satış yapabilmenin ötesine geçip, üretkenliği ve yaratıcılığı arttıran küresel e-ticaret bağlantıları kurma şansını elde edebilmeye başlamıştır. Eskiden birçok*

şirket televizyon, gazete, radyo gibi araçları kullanarak potansiyel müşterilerine ulaşmaya uğraşırken, bugün bunlara İnternet üzerinden reklamcılık da eklenmiştir. *https://tr.wikipedia.org/wiki/Elektronik_ticaret*

[vii] ***ROCA (Return Of Coppersmith Attack) Güvenlik Açığı**: Çek Cumhuriyeti Masaryk Üniversitesi'ndeki Kriptografi ve Güvenlik Araştırma Merkezi'nden Slovak ve Çek güvenlik araştırmacıları tarafından Infineon Technologies tarafından geliştirilen bir kod kütüphanesinin içerdiği bir hata nedeniyle RSA (Rivest-Shamir-Adleman adlı bilim insanları tarafından geliştirilen asimetrik şifreleme algoritmasıdır. Anahtar dağıtımının yanı sıra şifreleme ve şifre çözme işlemlerini de gerçekleştiren, güvenilirliği çok büyük tam sayılarla işlem yapmanın zorluğuna dayanan bir şifreleme tekniğidir) anahtar üretiminin uygulanmasında keşfedilen güvenlik açığıdır. Güvenlik açığından etkilenen şifreleme anahtarları, donanım yongaları, kimlik doğrulama belirteçleri (token), yazılım paketleri, elektronik belgeler, TLS/HTTPS (Transport Layer Security – Taşıma Katmanı Güvenliği/Hypertext Transfer Protocol Secure – Güvenli Köprü Metin Aktarım Protokolü) anahtarları ve PGP (Pretty Good Privacy) gibi birçok teknolojiyi güvence altına almak için kullanılmaktadır. Infineon Technologies'in akıllı kartları, güvenlik belirteçleri ve 2012 yılından beri üretilen güvenli donanım yongaları etkilenen kod kitaplığını kullanmaktadır. Bu güvenlik açığından yararlanmak isteyen bir saldırgan pratik bir zaman diliminde asal çarpanlara ayırma yöntemini kullanarak genel anahtardan bir özel anahtar türetebilmektedir. Lostar GÜVENLİ GÜNLER sitesinden alıntıdır.*
https://www.internetsociety.org/blog/2017/11/roca-encryption-vulnerability/

[viii]*Technology Landscape for Digital Identification, World Bank Group, 2018,* *http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf*

[ix] *World Bank Group, Technology Lanscape for Digital Identification.*

http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf

[x] ***Güvenli Yazılım Çatısı**: Bilgisayar programlamada yazılım iskeleti, yazılım çerçevesi ya da yazılım çatısı (İngilizce software framework), standart (çok kullanılan) fonksiyonların hazır olarak sunulduğu ancak programcı tarafından bu fonksiyonlardan arzu edilen kısımların ek kodlarla istenildiği şekilde güncellenebildiği sistemlerdir.* *https://tr.wikipedia.org/wiki/Yaz%C4%B1l%C4%B1m_iskeleti*

[xi] ***Güvenlik Onayı Biçimlendirme Dili (SAML)**, güvenli web alanlarının, kullanıcı kimlik doğrulaması ve kullanıcı yetkilendirme verilerinin alışverişini yapmasına olanak tanıyan bir standarttır. Çevrimiçi bir hizmet sağlayıcı SAML'yi kullanarak, güvenli içeriğe erişmeye çalışan kullanıcıların kimlik doğrulamasının yapılması için ayrı bir çevrimiçi kimlik sağlayıcıya başvurabilir.*
https://support.google.com/cloudidentity/answer/6262987?hl=tr

[xii] ***Dağıtılmış Defter Teknolojisi**: Dağıtılmış defter teknolojisi (distributed ledger technology; "DLT"), ekonomi, toplum ve endüstride organizasyon ve*

işbirliğini değiştirme potansiyeline sahip bilgi teknolojileri alanında en umut verici yeniliklerden biridir. Dağıtılmış defter teknolojileri, değer yaratma ve yakalama için yeni imkânlar yaratarak, klasik hale gelen ticari işlem kavramlarını yeniden oluşturmaktadır. DLT; verilerin, bir ağ üzerinde bulunan birden fazla alanda erişilebilir, güncellenebilir, doğrulanabilir olmasına imkân sağlayan, merkeziyetsiz, teknolojik altyapıdır. Bir tür konsensüs mekanizması olarak tanımlanır. Merkeziyetsiz yapılarda herhangi bir otorite söz konusu olmadığı için verilerin fikir birliği içerisinde saklanması, erişilmesi, güncellenmesi ve doğrulanması gerekir.

Dağıtılmış defter teknolojisi , Bitcoin ve blok zinciri teknolojisinden önce de var olan bir kavramdır. 1992 yılında Bayer, Haber ve Stornetta kriptografik hash işlevlerini ve Merkle ağaçlarını kullanarak dağıtılmış sistemlerde dijital verilere verimli ve güvenli bir şekilde zaman damgası eklemek için kriptografik olarak bağlantılı veri blokları zinciri fikrini ortaya atmıştır. Bununla birlikte, bu gelişmeler, kripto para birimleri ve daha genel olarak blok zinciri teknolojilerinin aksine çok daha az ilgi görmüştür. Daha sonrasında kripto para birimleri ve blok zincirine duyulan ilgi, DLT sistem türlerinin ve uygulamalarının hızlı bir şekilde gelişmesine neden olmuştur.
https://tr.wikipedia.org/wiki/Da%C4%9F%C4%B1t%C4%B1lm%C4%B1%C5%9F_defter_teknolojisi

[xiii] *2019 yılına kadar mobil reklamcılığın bütün ABD sayısal reklam harcamalarının %72'sini oluşturacağı tahmin edilmektedir.* *https://www.impactbnd.com/blog/mobile-marketing-statistics*

[xiv] *Sayısal kimlik pazarı kesinlikle finansal hizmetler endüstrisi tarafından desteklenmeye devam edecektir. Tüketici güvenine böylesine bağlı olan bir sektörde işlemlerin ve hesaba erişimin devam etmekte olan sayısallaşması kimlik yönetimine çok daha fazla yatırım yapılmasını teşvik etmektedir.*

https://www.gsma.com/identity/digital-identity-expect-2018

[xv] *2017 yılı sayısal kimlik açısından çok önemli bir yıl olmuştur. Kullanıcıların %86'dan fazlasının güvenlik açısından kuşku duydukları kullanıcı adı ve şifre uygulamasına olan ilgi azalmış ve dünyanın dört bir yanındaki mobil ağ operatörleri alternatif çözümler üzerinde işbirliği yapma kararı almıştır.*
https://www.gsma.com/identity/digital-identity-expect-2018

[xvi] *BBVA, Digital Identity: current state of affairs.*https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf

[xvii] *Christopher Wylie'nin ileri sürdüğüne göre Cambridge Analytica veri analiz firması; 50 milyon Facebook kullanıcısının kişisel bilgilerini izinleri olmaksızın kullanarak, psikolojik profillerine dayanan siyasi reklamlarla ABD'li seçmenleri hedefleyen bir algoritma oluşturmuştur.*
https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far

[xviii] *GSMA, Regulatory and policy trends impacting Digital Identity and the role of mobile Considerations for emerging markets October 2016.*
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/10/Regulatory-and-policy-trends-impacting-Digital-Identity-and-the-role-of-mobile.pdf

[xix] *04 Ekim 2017 tarihinde Estonya/Tallinn'de e-Governance Academy (EGA) tarafından gerçekleştirilen ve siber alan ile e-demokrasinin güvenliği ile ilgili konuların tartışıldığı, alan uzmanları ve politika yapıcıların katılımı ile iyi uygulama örneklerine ait sunumların yapıldığı ve mevcut uygulamalar odağında fikir alışverişinin sağlandığı e-Partnership Conference etkinliğidir.*

[xx] *World Bank, Julia Clark, Kyla Reid, STÉPHANIE DE LABRIOLLE, Public-private cooperation to build digital identity systems, 26 Temmuz 2016.*

http://blogs.worldbank.org/ic4d/public-private-cooperation-build-digital-identity-systems

[xxi] ***TOOP Projesi:*** *Tek Seferlik İlke Projesi, Avrupa Komisyon'u tarafından, 20 üye ülkeden 50 kuruluşu içine alan ve Ocak 2017'de başlatılan bir projedir. TOOP Projesinin ana hedefi sınırlar ötesinde de Tek Seferlik İlke uygulamasının işlediğini göstermektir. TOOP, işle ilgili bilgilerin veya belgelerin kamu idareleri arasında daha iyi alınıp verilmesini ve hem iş hem de kamu çevrelerinde iş yükünü azaltmayı hedeflemektedir.* *https://toop.eu/info*

[xxii] ***eIDAS****: eIDAS düzenlemesi kişiler ve şirketler için çevrimiçi alışveriş, kamu ve mali hizmetleri "güven" unsurunun sağlandığı çevrimiçi yasal bir ortam sağlamaktadır. Elektronik imza, mühür, zaman damgası, hizmet sunumu, kimlik doğrulama gibi elektronik tanımlama ve güven servislerinin oluşturduğu tek bir kural kümesi ile çevrimiçi güven, güvenlik ve kolaylığı sağlamakta ve geliştirmektedir. Kısaca; eIDAS ile kişiler veya şirketler, kendi ülkelerinde veya AB ülkesinde iş yaparken kendilerine ait "ulusal e-kimliklerini (eID)" kullanabileceklerdir. eIDAS bürokrasiyi azaltmakta, süreçleri daha az maliyetli gerçekleştirmekte, kişi ve şirketlerin hayatını daha kolay hale getirmektedir.* *http://www.egovturkey.com/eidas-hakkinda-25092018*

[xxiii] ***GDPR****: Genel Veri Koruma Yönetmeliği (GDPR - General Data Protection Regulation) Avrupa genelinde AB vatandaşlarının kişisel verilerini korumaya yönelik oluşturulmuş yönetmeliktir. 25 Mayıs 2018 tarihinden itibaren Avrupa Birliği'ne üye ülkelerde yürütmeye giren GDPR, Avrupa Birliği'ne üye ülkelerde büyük kurum ve kuruluşlarda var olan kişisel verilerin yönetmelikte belirtilen kurallar çerçevesinde güvenliğini sağlamayı konu edinmektedir. GDPR Avrupa birliği sınırları içerisindeki vatandaşlarının kişisel verilerini barındıran bütün işletmeleri kapsar. Şirketin konumu Avrupa birliği sınırları içerisinde bulunmasa dahi bu vatandaşların verilerini topladığı için yönetmelikten sorumlu tutulmaktadır. Hiçbir kişisel veri, yönetmelikte belirtildiği şekilde yapılmadığı veya*

ilgili kişiden (kişisel veri sahibinden) açık bir onay almadığı sürece işlenemez. İlgili kişi bu izni istediği zaman iptal etme hakkına sahip olmaktadır. GDPR geçmişte saklanmış verileri de kapsamaktadır. Genel Veri Koruma Tüzüğü GDPR maddelerine uyum sağlamayan işletmeleri ciddi ceza ve yaptırımlar beklemektedir. https://www.beyaz.net/tr/guvenlik/makaleler/gdpr_nedir.html

[xxiv] ***Siber Güvenlik:*** *Siber güvenlik, bilgisayar sistemlerinin, ağların ve verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini siber saldırılara veya yetkisiz erişime karşı korumaya yardımcı olan toplu yöntemler, teknolojiler ve işlemler olarak tanımlanabilir. Siber güvenliğin temel amacı, tüm kurumsal varlıkları hem iç hem de dış tehditlerden korumaktır.* https://fordefence.com/siber-guvenlik-nedir/

[xxv] *Allianz, A Guide to Cyber Risk, Eylül 2015.* https://www.agcs.allianz.com/insights/white-papers-and-case-studies/cyber-risk-guide/

[xxvi] *CSO, Josh Fruhlinger, Top cybersecurity facts, figures and statistics, 09 Mart 2020.* https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

[xxvii] ***Sentetik Kimlik Hırsızlığı****: Sentetik kimlik hırsızlığı, bir suçlunun yeni bir kimlik oluşturmak için gerçek ve sahte bilgileri birleştirdiği bir dolandırıcılık türüdür. Bu dolandırıcılıkta kullanılan gerçek bilgiler genellikle çalınır. Bu bilgiler sahte hesaplar açmak ve hileli satın alımlar yapmak için kullanılır. Sentetik kimlik hırsızlığı, suçlunun sahte kimliğe dayanarak kredi açan kredi kartı şirketleri dahil alacaklılardan para çalmasına olanak tanır.* https://tr.nesrakonk.ru/synthetic-identity-theft/

[xxviii] *LexisNexis Risk Solutions.* https://www.digitalidentityguide.com/synthetic-id/

[xxix] ***Nesnelerin İnterneti:*** *Nesnelerin interneti kavramı ya da diğer adıyla IoT, birbiri ile ilişkisi olan bilgi işlem cihazları, dijital makineler, mekanik nesneler ya da benzersiz tanımlayıcılarla sağlanan, insana gerek duymadan ağ üstünden veri aktarımı yapabilen sistemlerin tamamını açıklamaktadır. Her geçen gün artan bir biçimde, farklı endüstrilerde bulunan kuruluşlar çok daha verimli çalışabilmek, müşterilerine çok daha iyi bir hizmet sunabilmek, iş değerini artırabilmek, müşterilerini iyi anlayabilmek ve karar verme sürecini geliştirebilmek için IoT teknolojisinden yararlanmaktadır. Internet of Things yani IoT, ilk kez Kevin Ashton tarafından 1991 senesinde ortaya atılmış bir kavramdır. Nesnelerin internetine örnek vermek gerekirse; koldaki bir akıllı saatin gidilen mesafeyi, atılan adımları ve tüm aktiviteler süresince kalp atışını algılanmasından bahsedilebilir. Sensörler yardımıyla gerçekleşen bu algılama ile verilen bir istemci aracılığıyla analiz edilerek hayatın düzenlenmesine katkıda bulunulmaktadır. Bu iki cihaz arasında*

sağlanan iletişim, nesnelerin interneti kavramını oluşturan temel özellik olmaktadır.
https://www.isbank.com.tr/blog/nesnelerin-interneti-nedir

[xxx] *https://www.newgenapps.com/blog/iot-statistics-internet-of-things-future-research-data*

[xxxi] *https://www.stonetemple.com/mobile-vs-desktop-usage-study/*

[xxxii] *Mağazada mobil ödeme hacminin 2020 yılına kadar 503 milyar dolara ulaşması beklenmektedir. Yine 2020 yılına kadar mağazada mobil ödeme yapanların sayısının da 150 milyona ulaşması beklenmektedir. Bu rakam, 2020 yılındaki nüfusun yaklaşık %56'sına karşılık gelmektedir.*
https://home.bluesnap.com/snap-center/blog/22-mind-blowing-mobile-payment-statistics/

[xxxiii] *Technology Landscape for Digital Identification, World Bank Group, 2018,*
http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf

[xxxiv] *Kişisel tanımlama uygulaması Smart-ID ücretsizdir ve sınırsız olarak kullanılabilir. Smart-ID uygulaması Android ve iOS akıllı cihazlara indirilebilir. Diğer cihazlardan da elektronik hizmetlere erişim maksadıyla kullanılabilir.*
https://www.smart-id.com/

[xxxv] *SIM Kartlar GSM operatörleri tarafından müşterilerine sunulan ve içerisinde adres defteri barındırmakta olan bir mikroçiptir. Bu mikroçipler yardımıyla tanımlanan numara kullanabilir, GSM operatörünün sunduğu arama yapma, SMS, sesli mesaj ve internet gibi tüm servislerden faydalanabilinir. SIM kartların en büyük avantajlarından bir tanesi de içerisinde özel bir rehber barındırma kapasitesine sahip olmasıdır. Bu rehber sayesinde telefon değişikliklerinde SIM kart içindeki numaralar kolayca yeni rehbere taşınabilir ve böylece numara kaybı olmadan tüm kişiler kolayca aktarılabilir.* *https://wmaraci.com/nedir/sim*

[xxxvi] *Mobile Connect, mobil kullanıcılara hassas verileri paylaşma ve işlemleri güvenle yapma imkânı sağlayan basit ve güvenli bir uygulamadır. Doğrulama, yetkilendirme ve kimlik tanımlamasını küresel olarak ve maliyet-etkin bir şekilde gerçekleştirmeyi sağlar Dünyanın dört bir yanında 70 operatör tarafından kullanılmaktadır.* *https://www.gsma.com/identity/mobile-connect*

[xxxvii] *Technology Landscape for Digital Identification, World Bank Group, 2018,*
http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf

[xxxviii] *Mobile Connect for Cross-Border Digital Services Lessons Learned from the eIDAS Pilot, 2018*
https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-FINAL-web.pdf

[xxxix] *Lily Hay Newman, Phone Numbers Were Never Meant as ID. Now We're All At Risk Services increasingly rely on your phone number to know who you are—and that's increasingly a problem, 25 Ağustos 2018.*https://www.wired.com/story/phone-numbers-indentification-authentication/

[xl] ***Akıllı Telefon:*** *İş yerlerinde, sokakta, evde ve daha birçok yerde her anımızın vazgeçilmez bir parçası olan akıllı telefonlar, telefon görüşmesi ve mesajın yanı sıra çok sayıda fonksiyonu bir arada bulunduran ürünlerdir. Bu ürünlerin kullanım alanlarına göre çok sayıda işlevi vardır. Akıllı telefonların öne çıkan işlevleri arasında amatör ve profesyonel olarak resim ve videolar çekmek, İnternet uygulamaları ve oyunları çalıştırmak, elektronik postaların takibi, çevrimiçi etkinliklere katılmak, sosyal medya ile iletişim, kitap okumak vb. gibi işlevler öne çıkmaktadır.* https://teknoseyir.com/blog/akilli-telefon-nedir-ne-ise-yarar

[xli] *Counterpoint's Components Tracker tarafından yapılan araştırmaya göre; bütün sensörler dikkate alındığında 2017 yılında akıllı telefonlar üzerindeki sensör sayısı 6 milyardır ve bu rakamın 2020 yılında 10 milyarı geçeceği tahmin edilmektedir.* https://www.counterpointresearch.com/sensors-smartphones-top-10-billion-unit-shipments-2020/

[xlii] *Acuity'nin tahminine göre; 2022 yılına kadar 5.6 milyar mobil cihaz, 1.37 trilyon işlemin doğruluğunu biyometrik olarak doğrulamak maksadıyla kullanılacaktır.* https://findbiometrics.com/shift-cloud-based-biometrics-acuity-409204/

[xliii] https://www.acuity-mi.com/hdfsjosg/euyotjtub/Taming_The_Authentication_Beast.pdf

[xliv] *Info Security Magazin.* https://www.infosecurity-magazine.com/opinions/password-takes-last-breath/

[xlv] *Global Behavioral Biometric Market 2016-2020.*

https://www.technavio.com/report/global-it-security-behavioral-biometric-market

[xlvi] *Support Well-informed Identity and Trust Decisions Across the Customer Continuum.* https://www.digitalidentityguide.com/what-is-a-digital-identity/

[xlvii] ***Yapay Zekâ****: En basit ifadeyle yapay zekâ (AI), görevleri yerine getirmek için insan zekâsını taklit eden ve topladıkları bilgilere göre yinelemeli olarak kendilerini iyileştirebilen sistemler veya makineler anlamına gelir. Yapay Zekâ, herhangi bir özel biçim veya işlevden ziyade süper güçlendirilmiş düşünce ve veri analizi yeteneği ve süreciyle ilgilidir. Yapay zekâ üst seviye işleve sahip insan benzeri robotların dünyayı ele geçirmesine ilişkin görüntüler sunsa da, yapay zekânın amacı insanların yerini almak değildir. Amaç insan yeteneklerini belirgin şekilde geliştirmek ve bunlara katkıda bulunmaktır.* https://www.oracle.com/tr/artificial-intelligence/what-is-ai/

[xlviii] ***Makine Öğrenimi**: Makine öğrenmesi esas olarak 1959 yılında bilgisayar biliminin yapay zekâda sayısal öğrenme ve model tanıma çalışmalarından geliştirilmiş bir alt dalıdır. Makine öğrenmesi yapısal işlev olarak öğrenebilen ve veriler üzerinden tahmin yapabilen algoritmaların çalışma ve inşalarını araştıran bir sistemdir. Bu tür algoritmalar statik program talimatlarını harfiyen takip etmek yerine örnek girişlerden veri tabanlı tahminleri ve kararları gerçekleştirebilmek amacıyla bir model inşa ederek çalışırlar.*
https://www.endustri40.com/makine-ogrenimi-nedir/

[xlix] *Anormallik tespiti (anomaly detection) yaklaşımı, temel olarak sistemde meydana gelen anormal olayları, normal olaylardan ayırt etme mantığı ile çalışmaktadır. Bir bilgi güvenliği sistemi içerisinde yer alan STS için anormallik, normal aktivitelerden herhangi bir 56 sapma durumuna karşılık gelir. Sistemin normal davranışı, uzun süren bir analiz sonucunda elde edilebilir. Sistemdeki kullanıcı veya kullanıcı gruplarının davranış profillerinin ortaya çıkartılması anormallik tespiti için en temel iştir. Normal davranış profili belirlendikten sonra, farklılık gösteren davranışlar saldırı olarak tespit edilir. Anormallik tespitinde saldırıların doğru tespit edilmesi, normal davranış profilinin ne kadar doğru belirlendiğiyle orantılıdır. Güven, E., N., "Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 2007'den aktaran Muhammet Baykara, Doktora Tezi, Şubat 2016.*
https://openaccess.firat.edu.tr/xmlui/bitstream/handle/11508/20773/424189.pdf?sequence=1&isAllowed=y

[l] ***Sinir Ağları:** Neural Networks (sinir ağları) adı verilen yapay zekâ öğrenme modelidir, insan beyninin çalışma şeklini taklit ederek, bir veri kümesindeki temel ilişkileri tanımaya çalışan bir dizi algoritmadan oluşmaktadır. Katmanlar şeklinde kurulmuş bir yapıdır. Çok katmanlı olabileceği gibi tek katmanlı da olma ihtimali vardır. Tek katmanlı Neural Networkler fazla karmaşık olmayan sorunların çözülmesi için kullanılmaktadır. İlk katman giriş ve son katman çıkış olarak adlandırılır. Orta kısım gizili katmanlar olarak adlandırılmaktadır. Her katmanda belirli bir sayıda nöron bulunmaktadır ve bu nöronlar sinapslar ile bağlantılıdır. Sinapslar bağlı oldukları nörondaki bilginin ne kadar önemli olduğunu belirtmek için katsayılara sahiptirler. Google Bu alanda sektöründe lider konumda bulunan ve 2014 yılında satın almış olduğu DeepMind şirketi ile çalışmaktadır.*
https://www.dopinger.com/tr/blog/neural-networks/

[li] *Tom Maxwell, Smart Lock Passwords is cool, but Google Project Abacus puts us closer to a password-free world, 29 Mayıs 2015.*

https://9to5google.com/2015/05/29/smart-lock-passwords-is-cool-but-google-project-abacus-wants-to-eliminate-password-authentication/

[lii] *https://www.newgenapps.com/blog/iot-statistics-internet-of-things-future-research-data*

[liii] ***Kimlik ve Erişim Yönetimi****: Kimlik ve Erişim Yönetimi (IAM), kullanıcı kimliklerini ve erişim izinlerini güvenli bir şekilde başlatmak, depolamak ve yönetmek için geliştirilen bir sistemdir. IAM, kullanıcıların söyledikleri kişiler olduklarını doğrular (authentication); kullanma izinlerine sahip oldukları uygulamalara ve kaynaklara erişebilmelerine olanak tanır (authorization). Kimlik ve Erişim Yönetimi (IAM) temel olarak doğru kullanıcılara doğru erişimin verilmesini sağlar. İyi kurgulanan bir IAM uygulamasında; bir IT çalışanın şirketin mali kayıtlarına erişimi olmadığını, ancak şirketin muhasebe sorumlusunun bu erişime sahip olabileceğini düşünürsek doğru yetkilerin doğru kişilere verilmesini sağlayan bir yönetim sistemi olduğunu söyleyebiliriz. Ancak, kötü kurgulanan bir IAM uygulamasında; bir çalışanın hangi bilgilere ve uygulamalara erişiminin olduğu net olarak bilinmez ise bu şirketler için çok can sıkıcı durumlara yol açabilir.* https://monosign.com/tr/blog/identity-access-management-kimlik-ve-erisim-yonetimi-nedir

[liv] *Gartner, Gartner Says Managing Identities and Access Will Be Critical to the Success of the Internet of Things,* https://www.gartner.com/newsroom/id/2985717

[lv] *Nesnelerin İnterneti milyarlarca yeni kullanıcı, bulut hizmetleri ve bağlı çevrimiçi cihazların ortaya çıkmasına neden olmuştur. Eski kimlik sistemleri sayısal ilişkileri bu kadar büyük ölçekte yönetmek için tasarlanmadığından, yeni IoT girişimlerini kötü niyetli saldırılara karşı savunmasız bırakmıştır.*
https://www.secureidnews.com/news-item/how-identity-can-fix-the-iot/

[lvi] How identity can fix the IoT, *The possibilities to lead organizations and governments towards a successful digital transformation. Daniel Raski, 17 Şubat 2016.* https://www.secureidnews.com/news-item/how-identity-can-fix-the-iot/#

[lvii] *Coin Desk, What is distributed ledger? Nolan Bauerle, 09 Mart 2017.*
https://www.coindesk.com/information/what-is-a-distributed-ledger/

[lviii] *Sıfır bilgi kanıtları blok zincir kullanıcıları için gizliliği ve güvenliği büyük oranda artırma potansiyelleri nedeniyle son zamanlarda finans çevrelerinde heyecan yaratmaktadır. Oysa kriptograflar yıllardır sıfır bilgi/etkileşimli kanıtlar üzerinde çalıştığından bu kavram yeni değildir.* https://venturebeat.com/2017/12/16/what-zero-knowledge-proofs-will-do-for-blockchain/

[lix] *Sosyal güvenlik numaraları veya kredi raporlarını saklamak için kullanılanlar gibi merkezi bir veri tabanıyla ilgili sorun, bir kez ele geçirildiğinde, bir hırsızın orada depolanan tüm bilgileri kopyalama yeteneğine sahip olmasıdır.*
https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data

[lx] *GDPR, Avrupa Birliği vatandaşlarına kişisel verileri üzerinde daha fazla hak vermek ve onlara bu verilerin nasıl toplandığı, saklandığı ve aktarıldığı üzerinde daha fazla kontrol sağlamak için tasarlanmış en son önlemdir – gizlilik ihlallerine*

ve siber saldırılara karşı korunma sorumluluğu yakında bireysel şirketlere yüklenecektir. https://www.gsma.com/identity/digital-identity-expect-2018

[lxi] *Registro della federazione SPID.* https://registry.spid.gov.it/identity-providers

[lxii] *BankID, sayısal ortamlarda kendinizi tanımlamanın yaygın bir yoludur. Farklı aktörlerle şifreli hesaplar oluşturmak zorunda değilsiniz ve bunun yerine herkes için aynı güvenli çözümü kullanabilirsiniz. Bu tıpkı sayısal olarak kimliğinizi göstermek gibidir.* https://www.bankid.com/en/om-bankid/detta-ar-bankid

[lxiii] *GOV.UK Verify, çevrimiçi olduğunuzu kanıtlamanın güvenli bir yoludur. Vergi belgelerini doldurmak veya ehliyetinizdeki bilgileri kontrol etmek gibi devlet hizmetlerine erişmeyi güvenli, hızlı ve kolay hale getirir. GOV.UK Verify'ı kullandığınızda, kimliğinizi şahsen kanıtlamanıza veya postayla bir şeyin gelmesini beklemenize gerek yoktur.* https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

[lxiv] ***The itsme® Identity Application****: Belçika'da ilk kez 2017 yılında piyasaya sürülen uygulama Belçika vatandaşlarına kimliklerini kanıtlama imkânı sağlamaktadır. Piyasaya sürülmesinin ardından geçen dört yıllık sürede kullanıcı sayısı üç milyonu aşmıştır. Çalışan Belçika vatandaşlarının %40'nın "Itsme" hesabı bulunmakta ve her gün 3.500 yeni kullanıcı devreye girmektedir.* https://www.itsme.be/en/

[lxv] *Ödeme kartları. Hepsi aynı şekle sahip olsa da, çok farklı olabilirler. Bazıları çekici tasarımlara sahiptir. Diğerleri premium kullanıcılara verilir ve metalden yapıldıkları için öne çıkar. Ve diğerleri hala oldukça standartır. Yine de tüketiciler ve finans kurumları tarafından akıllı kartlara yönelik talepler son yıllarda çarpıcı bir şekilde artmıştır. Bugün beklentiler, çevrimdışı kullanıldığında hassas bilgileri korumaya yönelik önlemlerden, ihraççılar için uygun maliyetli pazarlama araçlarını desteklemeye kadar uzanmaktadır.* https://www.gi-de.com/en/au/g-d-group/press/press-releases/detail/press-detail/the-green-button-is-online-verimi-is-gradually-launching-its-id-and-data-platform/

[lxvi] https://ec.europa.eu/cefdigital/wiki/x/Yg3NAg

[lxvii] *Yeni mobil tabanlı cihazların ortaya çıkmasına rağmen ve tabletler gibi yeni kategorilerin piyasaya sürülmesine rağmen akıllı telefonlar mobil alanda en önde gitmektedir. 2020 yılına kadar bütün mobil veri trafiğinin %80'i akıllı telefonlar üzerinden yapılacağı tahmin edilmektedir.*

https://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/

[lxviii] *Acuity Market Intelligence tahminlerine göre biyometri özellikli akıllı telefonlar, tabletler ve giyilebilir mobil cihazlara olan artan talep nedeniyle 2020 yılına kadar piyasada yaklaşık 4,8 milyar biyometrik cihaz olması beklenmektedir.*

http://www.biometricupdate.com/201412/4-8-billion-biometric-devices-predicted-by-2020

[lxix] *The future of the smartphone: the era of invisible innovation.*

https://www2.deloitte.com/content/dam/Deloitte/au/Documents/technology-media-telecommunications/deloitte-au-tmt-predictions-smartphones-010218.pdf

[lxx] *Strategy Analytics: On Device Artificial Intelligence Already Powers One Third of Smartphones.*
https://www.businesswire.com/news/home/20180716005617/en/Strategy-Analytics-Device-Artificial-Intelligence-Powers-Smartphones

[lxxi] ***5G Teknolojisi**: 5G, günümüz 4G LTE ağlarının önemli bir evrimi olan 5. nesil mobil ağı olarak tanımlanmaktadır. Son yıllarda ortaya çıkan büyük veri ve nesnelerin interneti kavramlarının bir gereği olarak geliştirilmekte olan 5G teknolojisi, çok daha hızlı bir internet bağlantısını mümkün kılmaktadır. Birbirine bağlanan milyarlarca cihazın duyduğu hızlı internet ihtiyacını karşılayacak olan 5G, en uzun filmleri bile birkaç saniyede indirmeye olanak sağlamaktadır. Bağlantılarda meydana gelen kopukluğun da bu teknoloji ile asgariye inmesi beklenmektedir. Ayrıca geniş kapsama alanı, 5G'nin en önemli özellikleri arasında yer almaktadır. Hâlihazırda satışı başlayan 5G uyumlu telefonlar ile birlikte çalışacak olan bu teknolojinin başlangıçta 4G ağlarıyla birlikte çalışması, daha sonraki sürümlerinde ise kapsamının genişletilerek tamamen bağımsız ağlar aracılığıyla çalışması tasarlanmaktadır. Temel çalışma prensibi, diğer ağlardaki gibi radyo dalgaları ile veri dağıtımı olan 5G, 4G'nin kullandığı LTE yerine OFDM denilen yeni bir şifreleme kullanacaktır.* https://www.wissenakademie.com/blog/5g-teknolojisi-nedir

[lxxii] *Ericsson Mobility Report Haziran 2018.*
https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf

[lxxiii] *Parmak izi biyometrileri süratle akıllı telefonlarda ortak özellik olma yolunda dev adımlarla ilerlemektedir. Parmak izi sensörleri içeren akıllı telefon model sayısı hızla artmaktadır. 2014 yılında %3 olan parmak izi sensörü olan akıllı telefon oranı 2017 yılında %65'e yükselmiştir ve günümüzde de bu oran %80'dir.*
https://www.mobilemarketer.com/news/study-mobile-biometrics-market-to-surge-17x-by-2023/528892/

[lxxiv] *Blockchain Identity Management Market, 2023 by Provider, Organization Size, Vertical and Region - ResearchAndMarkets.com*
https://www.businesswire.com/news/home/20180608005738/en/Blockchain-Identity-Management-Market-2023-Provider-Organization

[lxxv] ***Avrupa Komisyonu:** Avrupa Komisyonu, yasama sürecini başlatan, ayrıca Birliğin yürütme organı olarak AB müktesebatını, bütçeyi ve programları*

uygulamaktan ve idari denetimden sorumlu kurumdur. Avrupa Komisyonu, her bir üye devletten bir kişinin yer aldığı, 5 yıl için seçilen 27 üyeden oluşur. Bu kişilere "komiser" adı verilir. Her komiser bir veya daha fazla AB politikasının yürütülmesinden sorumludur. Komisyon adeta bir Bakanlar Kurulu gibi faaliyet gösterir. Komisyon'da komiserlerin yanı sıra, Avrupa Birliği görevlilerinden oluşan 25.000 kişilik bir idari teşkilat da mevcuttur.
https://www.ab.gov.tr/avrupa-komisyonu_45629.html

[lxxvi] *Dünya Bankası Temmuz 2014'de herkese erişim ve hizmet sağlamayı hedefleyen 21. Yüzyıl çözümlerini kullanarak gelişmeyi desteklemek maksadıyla Identification for Development (ID4D) (Gelişme için Kimlik) projesini başlatmıştır.*

http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf