Bilgi Yönetimi Dergisi

Cilt: 5 Sayı: 2 Yıl: 2022

https://dergipark.org.tr/tr/pub/by

Hakemli Makaleler
Araştırma Makalesi

Makale Bilgisi

Gönderildiği tarih: 07.05.2022
Kabul tarihi: 09.08.2022
Erken görünüm: 14.12.2022
Yayınlanma tarihi: 30.12.2022

Article Info

Date submitted: 07.05.2022
Date accepted: 09.08.2022
Date early view: 14.12.2022
Date published: 30.12.2022

Anahtar Sözcükler

Güven Çerçevesi, Dijital Kimlik, Elektronik Ticaret

Keywords

Trust Framework, Digital Identity, ElectronicCommerce

DOI Numarası

10.33721/by.1113558

ORCID

0000-0003-1874-4190 (1)
0000-0001-6788-008X (2)

Türkiye'deki e-Ticarete Özgü Blokzincir Tabanlı Dijital Kimlik Güven Çerçevesi Önerisi

Blockchain Based Digital Identity Trust Framework Proposal for e-Commerce in Turkey

Ömer DOĞAN
Gazi Üniversitesi Bilişim Enstitüsü Doktora Öğrencisi,
doganomer@gmail.com

Hacer KARACAN
Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü Öğretim Üyesi,
hkaracan@gazi.edu.tr

Öz

E-ticaret işlemlerinde satıcı firmaların sunduğu ticari kimlik, sertifika, ruhsat, akreditasyon belgesi, kalite belgesi gibi belgelerin doğruluğunun kanıtlanmasındaki zorluklar, e-ticaret ile yapılan alışverişlerde güven sorununa yol açmaktadır. Dijital ortamda sunulan bu belgeler, genellikle kâğıt ortamda alınmış olan fiziksel belgelerin görsellerinden ibaret olduklarından ve bu görsellerin dijital ortamda kolaylıkla taklit edilebilmesi nedeniyle bu belgelerin gerçekliğinden emin olunamamaktadır. Bu nedenle, yetkili kuruluşların kâğıt ortamında muhatabına fiziksel belge sunmalarına ve belgedeki imza, mühür, filigran gibi fiziksel doğrulama yöntemlerine benzer şekilde, dijital ortamda da belgelerin güvenli bir şekilde sunulabilmesini ve gerektiğinde bu belgelerin dijital olarak güvenli bir şekilde doğrulanmasını sağlayan bir yapıya ihtiyaç vardır. Yetkili kuruluşların belgeleri dijital olarak sunabilmesi ve bu belgelerin dijital olarak güvenilir bir şekilde doğrulanabilmesi, bahsedilen güven sorununu büyük ölçüde ortadan kaldıracaktır. Bu çalışma ile literatürde dijital kimlik olarak adlandırılan bu bağlamdaki dijital belgelerin yetkili kuruluşlar tarafından güvenli bir şekilde verilmesi ve alıcılar tarafından doğrulanması için blokzincir tabanlı bir dijital kimlik güven çerçevesi önerisi getirilmektedir. Dijital kimlik güven çerçevesinin teknik gerçekleştirimine yönelik detaylara girilmeden kavramsal seviyede bir model sunulmaktadır. Önerilen dijital kimlik güven çerçevesi, dijital kimliklerin yönetimi ve paylaşımı için uluslararası standartları temel alan ve güven çerçevesi kapsamındaki rolleri ve süreçleri tanımlayan bir kurallar bütünüdür. Güven çerçevesinin tesis edilmesi ve paydaşların güven çerçevesindeki kurallara uymasının sağlanması ile e-ticaret işlemlerinin güvenilirliğinin artacağı öngörülmektedir. Önerilen güven çerçevesinin blokzincir tabanlı olması, güven çerçevesinin teknik olarak güvenli bir alt yapıya sahip olmasını sağlamaktadır.

Abstract

The difficulties in the validation of the records, such as commercial identity, licenses, accreditation certificates, quality certificates and other kinds presented by the sellers cause issue of trust in e-commerce activities. Since the digitally presented records are usually the images of their simply physical counterparts in paper and the images are not tamper-proof, buyers cannot be sure about the validity of these digital records. Therefore, a mechanism is needed in the digital environment that allows organizations to issue digital records and buyers to validate them digitally in a trusted way; similar to how authorized organizations issue paper records with some physical validation means such as signature, seal and watermark.

**Bu makalenin araştırma ve yayın süreci "Araştırma ve Yayın Etiğine" uygun şekilde yürütülmüştür.*

Mentioned issue of trust is expected to be mostly overcome when authorized organizations can digitally issue these records in a trusted way. This study proposes a blockchain based digital identity trust framework at the conceptual level without detailing the technical implementation of the trust framework. Using the proposed trust framework, authorized organizations can issue digital identities and buyers can validate these issued digital identities in a trusted way. Proposed digital identity trust framework is a set of rules which defines the roles and processes in the framework based on international standards for management and sharing of digital identities. It is anticipated that the trust in the e-commerce activities will increase with the establishment of the digital identity trust framework and ensuring that the stakeholders comply with the rules of the trust framework. Having blockchain as part of the technical implementation of the trust framework ensures that it has a secure infrastructure.

1. Giriş

E-ticaret hacmi hem Türkiye'de hem tüm dünyada ivmelenen bir artış göstermektedir. Dünya çapında son beş yılda perakende e-ticaret satışları 107% artış göstermiştir (Statista, 2022). Fakat e-ticaret işlemlerindeki sunulan bilgilerin doğrulanmasıyla ilgili birçok etken, kullanıcıların bu yöntemle yapılan alışverişlerde güven kaygısı yaşamasına sebep olmaktadır. Pek çok çevrim içi işlemde olduğu gibi, e-ticaret işlemlerinde de kullanıcılar karşı tarafın kimliğini bilmemekte veya karşı tarafın beyan ettiği kimlik bilgilerinin doğruluğundan emin olamamaktadır. E-ticaretin bir tarafı olan satıcı firmaların hem ticari kimlikleriyle ilgili hem de sertifika, akreditasyon belgesi, izin belgesi, kalite belgesi gibi diğer belgeleriyle ilgili internet ortamında sundukları bilgiler genellikle fiziksel belgelerin elektronik ortama aktarılmış görüntüsü şeklinde olduğundan doğruluğunun kanıtlanması ve yetkili kuruluş tarafından onaylandığının gösterilmesi çoğu zaman mümkün olamamaktadır. Bu nedenle, satıcı firmaların bu bilgi ve belgeleri dijital olarak yetkili kurumlardan alabildiği, ispat etmesi gerektiğinde dijital olarak sunabildiği ve alıcılara bu bilgi ve belgelerin doğruluğunu kanıtlayabildiği bir sisteme ihtiyaç duyulmaktadır.

Blockchain Türkiye Platformu'nun (BCTR) yayınladığı Dijital Kimlik Raporu'nda kimlik, "kişiye ait biyografik ve biyolojik özellikler de dâhil olmak üzere, bir kişiyi tekil olarak betimleyen özellikler ve karakteristik davranışlar" olarak tanımlanmaktadır (BCTR, 2019). Bu çalışma bağlamında ise kimlik, kişi ile sınırlandırılmamakta ve herhangi bir varlığa ait olabileceği kabul edilmektedir. Uluslararası Telekomünikasyon Birliği'nin (International Telecommunication Union - ITU) "varlıkların bağlam içinde yeterli seviyede ayırt edilmesini sağlayan bir veya daha fazla öznitelik biçimindeki temsili" şeklindeki kimlik tanımı, şirketlerin de kimliklerini kapsayan geniş çerçeveli bir tanımdır (ITU, 2018). Varlığın ayırt edilmesini sağlayan öznitelikler, varlığın çeşidine göre farklılık gösterir. Kişileri ayırt eden öznitelikler kimlik numarası, adı, soyadı, biyometrik verileri, doğum tarihi gibi bilgiler olabilirken şirketleri ayırt eden bilgiler ticari sicil numarası, vergi numarası, MERSİS numarası, unvanı, adresi, kuruluş tarihi, sahip olduğu kanıtlayıcı belgeler gibi bilgiler olabilmektedir. Bu tanımdan yola çıkarak dijital kimlik, varlıkların ayırt edilmesini sağlayan ve özniteliklerden oluşan varlığın özniteliklerileyle birlikte dijital temsili olarak tanımlanabilir. Her tür ortam için geçerli olan kimlik kaydının oluşturulması, kimlik sahibine verilmesi, doğrulanması ve yetkilendirilmesi süreçleri dijital kimlikler için de geçerli olup bu işlemlerin çevrim içi hizmetler kapsamında çevrim içi ortamda gerçekleştirilmesi esastır. Bu çalışma kapsamında dijital kimlikler, e-ticaret firmaları tarafından kullanımları çerçevesinde ele alınmaktadır. Böylece, e-ticaret firmalarının ticari kimlikleri ile diğer bilgi ve belgelerini çevrim içi olarak sunabilmeleri hedeflenmektedir. Bu bilgi ve belgelerin bunları sağlayan yetkili kuruluşların da dâhil olduğu bir yöntemle doğruluk ispatlarının çevrim içi olarak yapılabilmesine yönelik bir öneri sunulmaktadır. Tüm bunlarla birlikte, alıcıların e-ticaret işlemlerini daha güvenle yapmasını sağlayan bir sistem gündeme gelebilir. Fakat alıcıların bu süreçlere güven duyabilmesi için, süreçlerin belli kurallar çerçevesinde şeffaf olarak işletilmesi, süreçlerde yer alan aktörlerin daha önceden tanımlanan kurallara uygun davranması ve teknik alt yapının siber saldırılara ve istismarlara karşı yeterli düzeyde güvenlik sağlaması gerekmektedir. Bu amaçla oluşturulan dijital kimlik güven çerçevesi, dijital kimlik oluşturulması, yönetimi ve kullanılması ile ilgili süreçlerin güvenilirliğini sağlamaya yönelik tanımların, prensiplerin, uyum kıstaslarının, değerlendirme yaklaşımının, standartların ve şartların yer aldığı bir yapıdır (DIACC, Pan-Canadian Trust Framework Glossary, 2020). Bu çalışmada, e-ticaret ekosistemi irdelenerek bu alan özelinde kullanılabilecek bir dijital kimlik güven çerçevesi önerisi sunulmaktadır. Dijital kimlik güven çerçevesinin blokzincir tabanlı, e-ticaret işlemleri kapsamında ve sadece firmaların dijital kimlik kullanımını karşılayan bir

yapıda oluşturulması hedeflenmektedir. Dijital kimlik güven çerçevesinin teknik gerçekleştirimine yönelik detaylara girilmeden kavramsal seviyede bir model sunulmuştur. E-ticaret işlemlerindeki alıcıların dijital kimlik kullanımı bu çalışmanın kapsamı dışındadır.

2. Literatürdeki Çalışmalar

Literatürdeki çalışmalar incelendiğinde, dijital kimlik güven çerçevesi konusunda yapılan çalışmaların önemli bir kısmının ulusal dijital kimlik sistemleri oluşturulması kapsamında olduğu görülmektedir. Bu alanda akademik çalışmalarla birlikte ulusal ve uluslararası kuruluşların araştırmaları ön plana çıkmaktadır. Birleşmiş Milletler (BM) Güney Doğu Asya ülkelerindeki ulusal dijital kimlik stratejilerini incelediği raporunda, ülkelerin dijital kimlik kullanımına geçişi için tavsiyelerde bulunmuştur (BM, 2020). Dünya Bankası (DB), Group of 20 (G20) ülkeleri için finansal kuruluşlar açısından dijital kimliğin rolünü ve finansal kuruluşlardaki uygulamalarını inceleyerek ülkelerin bu konudaki politikaları belirleyen yetkililerine önerilerde bulunmuştur (DB, 2018). AccessNow organizasyonu ise dijital kimlik uygulamalarına insan hakları perspektifinden yaklaşmış ve yetkililere bu çerçevede yönetişim, veri güvenliği, mahremiyet ve siber güvenlik alanlarında politika tavsiyelerinde bulunmuştur (AccessNow, 2018). Dünya Ekonomik Forumu (DEF) dijital kimliğin tedarik zinciri uygulamalarında kullanımı ile ilgili yaptığı bir çalışmada, dijital kimlik güven çerçevesinin temel bileşenlerini içeren bir rehber hazırlamıştır (DEF, 2019). ITU ise ülkelerde dijital kimlik ile ilgili politikaları belirleyen yetkililere rehberlik etmesi amacıyla çok detaylı bir Dijital Kimlik Yol Haritası Rehberi hazırlamıştır (ITU, 2018). Benzer bir amaç ve yaklaşımla DB'nin Gelişim için Kimlik Girişimi (Identification for Development – ID4D) de dijital kimlik uygulama rehberi yayınlamıştır (DB, Practitioner's Guide, 2019). Dijital kimliklerin geniş kitlelere belli prensipler çerçevesinde ulaşmasını amaç edinen ID2020 organizasyonu, yayınladığı manifesto ile bu prensipleri ortaya koymuştur (ID2020, Manifesto, 2018). Ayrıca bu organizasyon, dijital kimlik alanında teknik çözüm sunan şirketlerin ID2020 prensiplerine uygunluğunun sertifikasyonu için teknik gereksinimler paylaşmıştır (ID2020, ID2020 Technical Requirements, 2019).

Uluslararası kuruluşların rehber ve tavsiye niteliğinde yaptığı çalışmaların yanı sıra bazı ülkelerin de kendi dijital kimlik uygulamalarına yönelik rehberleri ve yayınları bulunmaktadır. Amerika Birleşik Devletleri'nde (ABD) 2018 yılında kurulan Better Identity Coalition, ülkede güvenli bir dijital kimlik altyapısı kurulması için yol haritası hazırlamıştır (The Better Identity Coalition, 2019). ABD'nin yanı sıra Yeni Zelanda da bir dijital kimlik güven çerçevesi oluşturmuş, güven çerçevesinin bileşenlerini ve prensiplerini belirleyerek yayınlamıştır (Yeni Zelanda Hükümeti, 2020). Bununla birlikte, Birleşik Krallık, dijital kimlik uygulamalarına yönelik olarak birçok iyi uygulama rehberleri (Good Practice Guide – GPG) duyurmuştur. Bu rehberler, halka açık çevrim içi hizmetlerin güvenli bir şekilde sağlanması için gereksinimleri (CESG - National Technical Authority for Information Assurance, 2012), çevrim içi servisleri korumak için kimlik doğrulama kullanımını (CESG - National Technical Authority for Information Assurance, 2013) ve bir kişinin kimliğinin ispatı ve doğrulanmasının nasıl yapılması gerektiği bilgilerini (CESG - National Technical Authority for Information Assurance, 2014) içermektedir. Birleşik Krallık'ın iyi uygulama rehberlerinden biri de organizasyonların dijital kimliklerinin olmasına yöneliktir (CESG - National Technical Authority for Information Assurance, 2013). Bu rehber, dijital kimliğin kişiler dışında da uygulanmasına yönelik nadir çalışmalardan biridir. Organizasyonlara dijital kimlik verilmesi ile ilgili çalışma yapan bir diğer ülke de Kanada'dır. Kanada, dijital kimlik güven çerçevesi alanında en detaylı çalışma yapan ve en çok yol kat eden ülkelerden biridir. Kanada'da dijital kimlik konusunda çalışma yapması için kurulan The Digital Identification and Authentication Council of Canada (DIACC), Kanada'ya özgü bir dijital kimlik güven çerçevesi oluşturmuştur (DIACC, Pan-Canadian Trust Framework Model, 2020). Pan-Canadian Trust Framework (PCTF) adı verilen bu güven çerçevesi, hem kişilere hem de organizasyonlara güvenilir bir şekilde dijital kimlik verilebilmesi için gerekli olan süreçleri ve uyulması gereken kıstasları tanımlar. Kimlik kanıtlama, doğrulama, mahremiyetin korunması ve açık rıza konularının nasıl sağlanacağını ayrı bileşenler hâlinde açıklar.

Ülkelerden bağımsız olarak dijital kimlik güven çerçevesini üst seviye bir bakış açısıyla ortaya koyan çalışmalar da bulunmaktadır. Open Identity Exchange adlı topluluk, ilk olarak 2010 yılında açık kimlik güven çerçevesi modelini ortaya koymuştur (Maler, Nadalin, Reed, Rundle ve Thibeau, 2010). Bu modelde dijital kimlik ile ilgili rollerin kimlik sağlayıcı, kullanıcı ve hizmet sağlayıcı olmasının ötesinde politikaları belirleyen yetkililer, açık kimlik güven çerçevesi sağlayıcıları, sertifikasyon için değerlendirme kuruluşları, denetim için denetleme kuruluşları ve anlaşmazlıkları çözmek için ara buluculara yönelik gerekli roller de tanımlanmıştır. Open Identity Exchange topluluğu bunun devamında dijital kimlik ve güven çerçevesi ile ilgili birçok yayın yapmıştır. Topluluk 2020 yılında dijital kimlik güven çerçeveleri ile ilgili bir rehber hazırlayarak güven çerçevelerinin bileşenlerinin nasıl ele alınması gerektiğini ortaya koymuştur (Mothershaw, 2020). Benzer şekilde Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından federe kimlik sistemleri için dijital kimlik güven çerçevesi oluşturulmasına yönelik kapsamlı yayınlar yapılmıştır (Temoshok & Abruzzi, 2018; Grassi, Fenton, Newton, Perlner, & Regenscheid, 2017; Grassi, Garcia, & Fenton, Digital Identity Guidelines, 2017; Grassi, ve diğerleri, 2017; Grassi, Richer, Squire, Fenton, & Nadeau, 2017).

Bu alandaki akademik çalışmalar ağırlıklı olarak blokzincirin kullanıldığı dijital kimlik modellerine yöneliktir. Dijital kimlik kullanımı için güven çerçevesi oluşturulmasına yönelik çalışmalar az sayıdadır. Bu çalışmalardan biri, Lim (2020) tarafından yapılan ve kullanıcı egemen kimlik kullanımı için güven çerçevesi oluşturulması gerektiğini ortaya koyan çalışmadır. Lim güven çerçevesinin oluşturulabilmesi için güven çerçevesinin yönetişimi ve yasal yönleri konusunda mutabakata varılmasının şart olduğunu ortaya koymuştur. Lim bu mutabakatın sağlanabilmesi için Trust Over IP (TOIP) yaklaşımının tüm taraflar tarafından kılavuz olarak alınmasını önermiştir. Goodell ve Aste (2019) dağıtık kayıt defterlerini kullanan merkezi olmayan bir dijital kimlik mimarisi önerisi getirmiştir. Bu öneri ile öncelikle kullanıcıların mahremiyetini korumaya yönelik kısıtları ortaya koymuşlar ve bu kısıtlara uygun olarak dağıtık kayıt defteri teknolojini kullanan teknik bir çözüm önerisi sunmuşlardır. Jamal vd. (2019) ise blokzinciri dijital kimliklerin saklanabileceği ve kimlik doğrulama için kullanılabileceği bir çözüm olarak önermişlerdir. Fakat bu çalışmada dijital kimliklere erişim ile ilgili mahremiyet ihlallerinin nasıl ele alınacağına değinilmemiştir. Dijital kimliklerin blokzincir üzerinde tutulduğu fakat dijital kimliklerin kullanıcı egemen olarak yönetildiği bir başka kimlik yönetim ve erişim kontrolü çalışması da Liao vd. (2022) tarafından yapılmıştır. Liao vd. Ethereum blokzinciri üzerinde bir çözüm önerisi getirerek blokzincir tabanlı kimlik yönetim ve erişim kontrolü yaklaşımını açık bankacılık alanındaki kullanım durumlarına uygulamıştır. Dissanayake vd. (2021) "Trust Pass" adını verdikleri blokzincir tabanlı dijital kimlik platformu ile kimlik kanıtlama ve dijital kimlik alma sürecini yapay sinir ağları kullanarak yüksek doğrulukta doküman ve biyometrik veri doğrulama ile gerçekleştirmeyi hedeflemişlerdir. "Trust Pass" için blokzincir, hassas kullanıcı verilerinin saklandığı bir güvenlik mekanizması olarak kullanılmıştır. Argento vd. (2020) ise farklı kuruluşlar arasında blokzincir üzerinden gerçekleştirilen süreçlere, Avrupa Birliği'nin "electronic identification and trust services for electronic transactions in the internal market" (eIDAS) düzenlemesine uyumlu ulusal dijital kimlik sistemlerinin entegre edilmesini sağlayan bir çözüm önerisi sunmuşlardır. Bu çözüm önerisi, blokzincir üzerinde işlem yapan tarafların kimliklerinin gerçek kimliklerle eşleştirilmesini, işlemlerin inkar edilemezliğini, denetim kayıtlarının tutulmasını ve izlenmesini sağlamıştır. Gada vd. (2021) ise blokzincir tabanlı dijital kimlik yönetim sistemini Ethereum üzerinde bir kitle fonlama sistemi geliştirmek için kullanmıştır.

Blokzincir tabanlı dijital kimlik çözümü ortaya koyan çalışmaların yanı sıra dijital kimlik yönetimi ve doğrulanmasına ilişkin yöntemleri inceleyen çalışmalar da bulunmaktadır. Pöhn ve Hommel (2020) kimlik yönetimi çözümlerinin sağlaması gereken gereksinimleri belirleyerek mevcut çözümlerin eksiklerini ve yeni yaklaşımlara olan ihtiyacı ortaya koymuşlardır. Rasouli vd. (2021) 10 alan uzmanının katıldığı bir araştırma ile dijital kimlik yönetimi için etkili olduğunu tespit ettikleri altı ana unsurun ve 31 alt unsurun önem derecesini incelemişlerdir. Bu araştırmada en etkili ana unsurun stratejik planlama olduğunu ortaya koymuşlardır. Akram ve Sen (2022) ise sıfır bilgi ispatı kullanan blokzincir tabanlı dijital kimlik çözümleri için bankacılık, finans ve sigortacılık sektöründe farklı

vakalar için vaka incelemesi çalışması gerçekleştirmiştir. Lim vd. (2018) 2014 ve 2018 yılları arasında ortaya çıkan blokzincir tabanlı kimlik yönetim ve doğrulama çözümlerini inceleyen bir araştırma yayınlayarak incelenen çözümlerin eksiklerini ve geliştirilmesi gereken yönlerini ortaya koymuşlardır. Liu vd. (2020) ikili haritalama ile dijital kimlik yönetim sistemlerinin ne derece kullanıcı egemen sistemler olduğunu incelemiştir. Liu vd. bu araştırmaları ile blokzincir gibi dağıtık kayıt defteri kullanan dijital kimlik çözümlerinin kullanıcı egemen kimlik modeli için daha umut verici olduğunu ortaya koymuşlardır. Gruner vd. (2018) blokzincir tabanlı dijital kimlik sistemlerinin güven seviyesini nicel olarak ortaya koyan bir güven modeli önermişlerdir. Gruner vd. nicel güven seviyesinden yola çıkarak nitel güvence seviyeleri de tanımlamışlardır.

3. e-Ticaret Dijital Kimlik Güven Çerçevesi

Dijital kimlik güven çerçevesi, geçerli olduğu ekosistemde bulunan aktörlerin birbirleri ile olan ilişkilerinin belli kurallar çerçevesinde gerçekleşmesini temin etmeye yönelik ve katılımcılara güven sağlayan düzenlemelerden oluşur (Mothershaw, 2020). E-ticaret için oluşturulacak dijital kimlik güven çerçevesi işleyişine ilişkin kurallar tüm paydaşlar tarafından açık bir biçimde bilinmeli ve tüm paydaşlar bu kurallara uygun davranmalıdır. Güven çerçevesi dokuz ana başlıktan oluşmaktadır:

1. Güven Çerçevesi Prensipleri
2. Dijital Kimlik Yönetim Modeli
3. Dijital Kimlik Paylaşım Standardı
4. Roller
5. Dijital Kimlik Türleri
6. Kimlik Kanıtlama ve Dijital Kimlik Alma Süreci
7. Dijital Kimlik Sunma ve Doğrulama
8. Güven İşareti
9. Güven Çerçevesi Paydaşları ve Yönetişimi

3.1. Prensipler

Güven çerçevesinin bileşenlerinin detaylı olarak belirlenebilmesi için öncelikle bunlara temel teşkil edecek prensiplerin belirlenmesi gerekmektedir. Literatürde dijital kimlik güven çerçevesi ile ilgili yapılan çalışmaların birçoğunda öncelikle belli prensipler ortaya koyulmuştur. Open Identity Trust Framework (OITF) Model (Maler, Nadalin, Reed, Rundle, & Thibeau, 2010), OIX Guide to Trust Frameworks (Mothershaw, 2020) ve Pan-Canadian Trust Framework Model (DIACC, Pan-Canadian Trust Framework Model, 2020) güven çerçevelerinde yer alan prensipler incelenerek, e-ticaret dijital kimlik güven çerçevesine uygun aşağıdaki prensipler belirlenmiştir.

1. Güven çerçevesi, uluslararası standartlara dayanmalı ve başka kimlik sistemleriyle birlikte çalışabilirliği göz önünde bulundurmalıdır.
2. Güven çerçevesi, kimliklerin kanıtlanması ve doğrulanması ile ilgili yöntemlerin güvence seviyelerini belirlemeli ve şeffaf olarak paydaşlarla paylaşmalıdır. Sahip olunan bir dijital kimliğin alınması için kullanılan kimlik kanıtlama yöntemleri güven çerçevesi kullanıcıları tarafından bilinmelidir.
3. Şirketler dijital kimliklerini veya dijital kimliklerinde yer alan bilgileri tamamen veya kısmen paylaşıp paylaşmama hakkına sahip olmalıdır. Şirketler sahip oldukları dijital kimlikler üzerinde tam kontrole sahip olmalıdır.
4. Şirketlerin dijital kimlikler ile paylaştıkları bilgiler sadece paylaşım amacı doğrultusunda kullanılmalı, başka amaçlarla kullanılmamalı ve başkalarıyla paylaşılmamalıdır.
5. Şirketler, sahip oldukları bir dijital kimliği birçok yerde kullanabilmelidir. Dijital kimliklerin kullanımı, e-ticaret işlemlerinin yapıldığı platformlardan bağımsız olmalıdır.
6. Güven çerçevesinde tanımlanan süreçler, dijital kimliklerin ve kimliklerde yer alan verilerin siber güvenlik saldırılarına ve dolandırıcılıklara karşı güvenliğini sağlamaya yönelik yöntemler içermelidir.
7. Güven çerçevesinin kuralları, süreçleri ve yönetişimi şeffaf olmalıdır.

8. Paydaşlar, güven çerçevesi kurallarına uygunluk kontrollerine ve denetimlere açık olmalıdır. Güven çerçevesi, paydaşların kurallara uyduğuna dair değerlendirme sonuçlarını gösterecek işaretlere yer vermelidir.
9. Şirketler, farklı kimlik sağlayıcılardan alınmış aynı amacı karşılayan birden fazla dijital kimliğe sahip olabilmelidir.

3.2. Dijital Kimlik Yönetim Modeli

Dijital kimlik yönetimi, merkezi, federe ve dağıtık olmak üzere üç farklı yönetim modelinde gerçekleştirilebilir (DEF, 2018).

- Merkezi kimlik yönetim modelinde dijital kimlik verileri tek bir merkezi kuruluşta saklanır ve o kuruluş tarafından yönetilir. Örneğin Türkiye'de tüm vatandaşların kimlik verileri Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünde (NVİGM) saklanır ve NVİGM tarafından yönetilir. NVİGM, e-devlet sistemi üzerinden hizmet sağlayan başka kuruluşların hizmetlerine erişmek için kimlik doğrulama hizmeti sağlar. Bu gibi merkezi sistemler çok büyük bir kitlenin kimlik verilerini sakladığından, siber saldırılar için çekici hedefler hâline gelmektedir. Ayrıca kimlik verilerinin yönetiminde ve paylaşılmasında kimlik sahibi kullanıcının kontrolü az olduğundan mahremiyet ve veri kontrolü konusunda zayıftır.
- Federe kimlik yönetim modelinde ise, birden fazla merkezi kuruluş belli yöntemlerle aralarında güven tesis ederek birbirlerinin kimlik yönetimlerine dayalı çalışırlar. Örneğin Avrupa Birliği'nde yer alan devletler "electronic identification and trust services for electronic transactions in the internal market" (eIDAS) adı verilen bir düzenlemeyle, ülkelerin kendi milli kimlik sistemleriyle yapılan kimlik doğrulamalarının diğer Avrupa Birliği ülkelerinde de geçerli olması sağlanmaktadır (Avrupa Birliği, 2014). Federe kimlik yönetim modelinde de kimlik sahibi kullanıcının veriler üzerindeki kontrolü azdır. Ayrıca kimlik yönetimi yapan kuruluşlar arasında güven ilişkilerinin kurulması, standartların ve yöntemlerin belirlenerek oturtulması genellikle zor ve zaman alıcı faaliyetlerdir.
- Dağıtık (Kullanıcı egemen) kimlik yönetim modelinde dijital kimlik verileri kimlik sahibi kullanıcının sahip olduğu dijital cihazlar üzerinde yer alan dijital kimlik cüzdanlarında saklanır. Geleneksel kimlik sağlayıcı kuruluşlar tarafından sağlanan dijital kimlikler bu cüzdanlarda saklanarak yönetimi ve paylaşılması kimlik sahibi tarafından gerçekleştirilir.

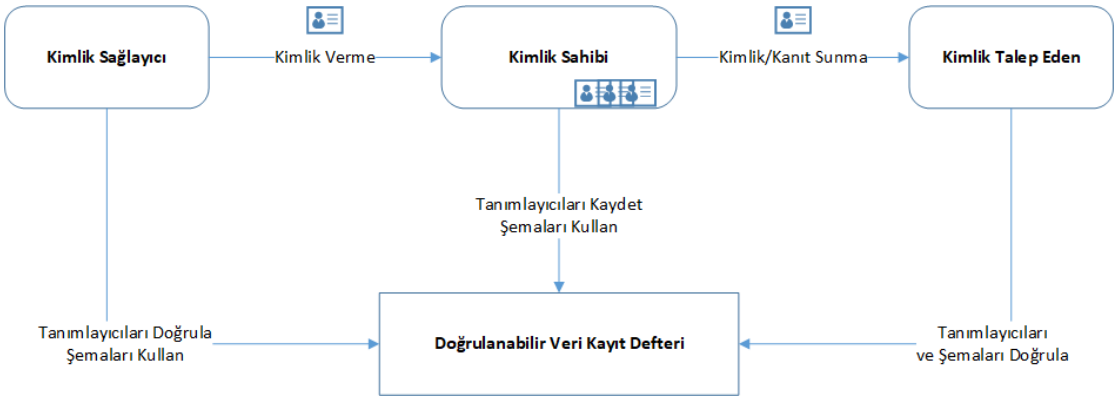
E-ticaret dijital kimlik güven çerçevesi prensipleri dikkate alındığında, en uygun kimlik yönetim modelinin dağıtık model olduğu değerlendirilmektedir. Şirketlerin dijital kimlikleri üzerinde tam kontrole sahip olmaları ile ilgili prensibi sağlayan model, dağıtık kimlik yönetimidir. Bu nedenle çalışmada önerilen e-ticaret dijital kimlik güven çerçevesinin yönetim modeli, dağıtık (kullanıcı egemen) kimlik yönetim modeli olarak belirlenmiştir.

3.3. Dijital Kimlik Paylaşım Standardı

E-ticaret dijital kimlik güven çerçevesi prensiplerinden ilki, uluslararası standartları kullanması ve diğer kimlik sistemleriyle birlikte çalışabilirliği bu yolla desteklemesidir. Bu prensibe uygun olarak güven çerçevesi kapsamındaki dijital kimlikler için dijital kimliklerin çevrim içi ortamda saklanması ve paylaşılması ile ilgili olarak World Wide Web Consortium (W3C) tarafından yayınlanan "Doğrulanabilir Kimlik Veri Modeli" (Verifiable Credentials Data Model) kullanılmaktadır (W3C, 2019). Bu standart, kimliklerin çevrim içi ortamda kriptografik olarak güvenli, mahremiyete önem veren ve başka sistemler tarafından doğrulanabilen bir yöntemle ifade edilmesini sağlar. Temel olarak aşağıda gösterilen "Güven Üçgeni" mekanizmasına dayanır.

Şekil 1

Doğrulanabilir Kimlik Rolleri ve Veri Akışı (W3C, 2019)



Doğrulanabilir Kimlik Veri Modelinde kimlik sağlayıcı rolü ile kimlik talep eden rolü arasında doğrudan bir bağımlılık bulunmaz. Kimlik sağlayıcı kimlik sahibine dijital kimlik verirken o dijital kimliğin kime kanıt olarak sunulacağı ile ilgilenmez. Kimlik sahibi herhangi bir kimlik sağlayıcıdan aldığı dijital kimliği istediği kimlik talep edene kanıt olarak sunabilir. Doğrulanabilir Kimlik Veri Modelindeki bu esneklik ile güven çerçevesi prensiplerinden Prensip 5 gerçekleştirilmiş olur.

Önerilen e-ticaret dijital kimlik güven çerçevesinde, bu standardın ortaya koyduğu Doğrulanabilir Veri Kayıt Defteri olarak blokzincir kullanılmaktadır. Blokzincir, dijital kimlik ekosisteminde yer alan aktörlerin erişebildiği güvenilir bir dağıtık kayıt defteri olarak kullanılır (W3C, 2019). Bu defterde dijital kimlikleri doğrulamak için gerekli olan açık anahtarlar ve dijital kimliklerin geçerliliğini kanıtlayan bazı kriptografik bilgiler yer alır. Dijital kimlikler ise kimlik sahibine ait cihazlar üzerindeki dijital cüzdan yazılımlarında tutulur. Blokzincir, yapısı gereği sadece yazmaya izin veren, daha sonradan değiştirilemeyen ve dağıtık olarak tutulan kayıtlardan oluşur. Bu nedenle blokzincirdeki verilerin sadece izin verilen kullanıcılar tarafından yazıldığı ve daha sonra değiştirilmediği garanti edilmiş olur. Böylelikle güven çerçevesi prensiplerinden Prensip 6 gerçekleştirilmiş olur.

3.4. Roller

Temel bir kimlik kullanımı senaryosunun merkezinde kimlik sahibi yer alır. İlk adım olarak yetkili bir kimlik sağlayıcı kuruluş tarafından kimlik sahibine kimlik verilir. Kimlik sahibi, kim olduğunu veya nelere ehil olduğunu ispat etmek istediğinde, kimlik kanıtını talep eden kişi veya kuruluşlara sahip olduğu kimliği ibraz ederek kanıt sunmuş olur. Kimlik kanıtını talep eden ise, ibraz edilen kimliğin o kimliği vermeye yetkili bir kuruluş tarafından verildiğine ve kimliğin geçerli olduğuna karar verdiğinde, kimlik ibrazına sebep olan işlemi gerçekleştirir.

E-ticaret dijital kimlik güven çerçevesi kapsamında da temel kimlik kullanımında yer alan rollerin özelleşmiş biçimleri bulunmaktadır:

- **Müşteriler:** E-ticaret işleminde mal veya hizmeti satın alan kullanıcılardır. Müşteri, e-ticaret dijital kimlik güven çerçevesinde Kimlik Kanıtı Talep Eden rolüne sahiptir. E-ticaret firmalarının müşterilere kimlik ispatlarını sunmaları ve müşterilerin sunulan kimlik ispatlarını blokzincir üzerinden doğrulamaları için, kullanıcının bilgisayarlarında veya mobil cihazlarında e-ticaret dijital kimlik doğrulamasını yapabilecek bir uygulama bulunması gerekmektedir.
- **E-ticaret Firmaları:** E-ticaret işleminde mal veya hizmeti müşteriye sunan e-ticaret firmasıdır. E-ticaret firması, e-ticaret dijital kimlik güven çerçevesinde Kimlik Sahibi rolüne sahiptir. Dijital Kimlik Sağlayıcılardan e-ticaret firmasına verilmiş olan dijital kimliklere ait ispat bilgisini, ispatı talep eden müşterilere göndererek blokzincir üzerinden doğrulanmasını sağlar.
- **Üretici Firmalar:** E-ticaret işleminde e-ticaret firması tarafından sunulan mal veya hizmeti üreten firmalardır. E-ticaret firması tarafından satılan ürünün asıl üreticisi olan Üretici Firmalar, e-ticaret dijital kimlik güven çerçevesinde Kimlik Sahibi rolüne sahiptir. Üretici Firmaların Dijital Kimlik

Sağlayıcılardan aldıkları dijital kimlikler, satışını yapan e-ticaret firmasından bağımsız olarak ürüne veya üretici firmaya verilen kimliklerdir.

- **Dijital Kimlik Sağlayıcılar:** E-ticaret ve üretici firmalara dijital kimlik vermeye yetkili kuruluşlardır. E-ticaret firmalarına temel ticari kimlik sağlayabilecek olan T.C. Ticaret Bakanlığı, ticaret odaları, vergi daireleri gibi kuruluşların yanı sıra firmalara sertifika, akreditasyon belgesi, izin belgesi, kalite belgesi gibi diğer kanıtlayıcı belgeleri sunan kuruluşlar da e-ticaret dijital kimlik güven çerçevesinde Kimlik Sağlayıcı rolüne sahiptir.

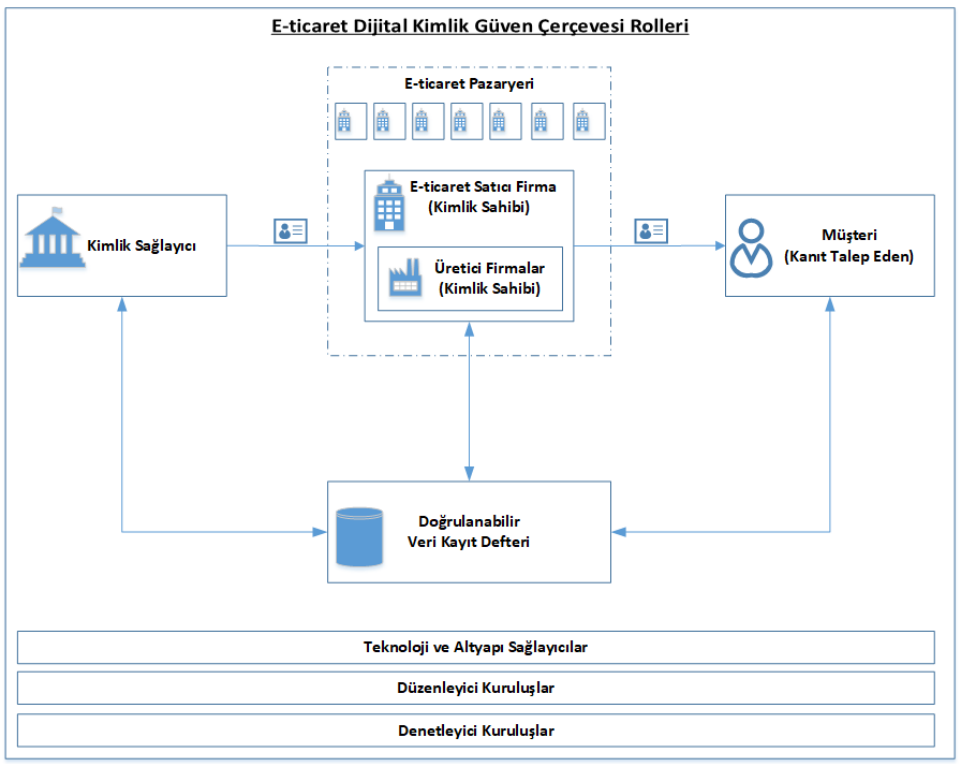
Temel rollerin yanı sıra, e-ticaret dijital kimlik güven çerçevesini destekleyici başka roller de bulunmaktadır:

- **Teknoloji ve Altyapı Sağlayıcılar:** Dijital kimlik işlemleri için gerekli teknoloji ve altyapıları sağlayan roldür. Dijital kimlikleri saklamak için dijital cüzdan sağlayıcıları, aktörler arası dijital kimlik ve kanıt aktarımı için altyapı sağlayıcıları gibi aktörler bu rolü temsil ederler.
- **E-ticaret Pazaryerleri:** E-ticaret firmalarının mal ve hizmetlerini sunabilmeleri ve satış işlemlerini gerçekleştirebilmeleri için çevrim içi platform sağlayan, e-ticaret firmalarına dijital mağaza hizmeti sunan roldür.
- **Düzenleyici Kuruluşlar:** E-ticaret dijital kimlik güven çerçevesi kapsamındaki rolleri ve işlemleri etkileyebilecek her türlü yasal düzenlemeyi yapan ulusal veya uluslararası kuruluşlardır.
- **Denetleyici Kuruluşlar:** Güven çerçevesi paydaşlarının güven çerçevesi kurallarına uygun davrandığını denetleyen ve Güven İşareti vermeye yetkili kuruluşlardır.

Aşağıdaki şekil, e-ticaret dijital kimlik güven çerçevesinde yer alan rolleri ve bu roller arasındaki temel kimlik akışını göstermektedir.

Şekil 2

e-ticaret Dijital Kimlik Güven Çerçevesi Rolleri



3.5. Dijital Kimlik Türleri

E-ticaret dijital kimlik güven çerçevesi kapsamında e-ticaret firmalarına verilebilecek iki farklı dijital kimlik türü bulunmaktadır. Bunlardan biri, bundan sonra temel dijital kimlik olarak ifade edilecek olan

e-ticaret firmasının kuruluşuna ve var olmasına ilişkin temel bilgilerin yer aldığı dijital kimliktir. Diğeri ise, e-ticaret firmasının ticari faaliyetlerine ilişkin izinleri, sertifikaları, akreditasyonları veya yetkinlikleri gibi özelliklerini gösteren ve bundan sonra bağlamsal dijital kimlikler olarak ifade edilecek olan kimliklerdir. Bağlamsal kimliklerin alınabilmesi için öncelikle en az bir temel kimliğin alınması gerekmektedir. E-ticaret firmaları, bağlamsal kimlik sağlayıcılarına öncelikle temek kimliklerini ispat olarak sunarlar ve temel kimliğin doğrulanması şartıyla bağlamsal kimliklerini alabilirler.

3.5.1.Temel Dijital Kimlikler

E-ticaret firmalarının alabileceği temel dijital kimlik türleri aşağıdaki tabloda verilmiştir.

Tablo 1

Temel Dijital Kimlikler

Dijital Kimlik Türü	Kimlik Sağlayıcı Kuruluş
Ticari Sicil Kimliği	Ticaret Bakanlığı Ticaret Odaları
Vergi Kimliği	Maliye Bakanlığı Vergi Daireleri
Esnaf/Sanatkâr Sicil Kimliği	Ticaret Bakanlığı Esnaf ve Sanatkâr Odaları

Bu temel kimlikler bir firmanın yasal olarak var olduğunu kanıtlayan türde kimlikler olup ayırt edici bir numara ile birlikte en az firmanın unvanı ve adresi bilgilerini içerir. Temel dijital kimliklerin farklı kimlik sağlayıcı kuruluşlardan alınsa bile ayırt edici olabilmesi için ortak bir ayırt edici numara belirlenmelidir. Her bir temel kimlik türüne has ayırt edici numaralar incelendiğinde, ortak ayırt edici bilginin Vergi Kimlik Numarası olduğu görülmektedir. Bununla birlikte, tüm temel kimliklerde olması gereken ortak alanlar da belirlenerek asgari dijital temel kimlik bilgileri bulunmalıdır. E-ticaret dijital kimlik güven çerçevesinin dijital kimlik paylaşım standardı "Doğrulanabilir Kimlikler" (Verifiable Credentials) olarak belirlenmiştir. Bu standarda uygun olarak asgari dijital temel kimliğin aşağıdaki şekilde olabileceği değerlendirilmektedir.


```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.ticaret.gov.tr/digital-identity/schemas/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
       ],
    "type": ["VerifiableCredential", "TemelKimlik"],
    "issuer": "...",
    "issuanceDate": "...",
    "expirationDate": "...",
    "credentialSubject": {
          "id": "..."
          "kimlik": {
                    "turu": "TemelKimlik",
                    "unvan": "...",
                    "vergiKimlikNo": "..."
                    "vergiDairesi": "...",
                    "kurulusTarihi": "...",
                    "adres": "...",
                    "sehir": "..."
                  }
    },
    "proof": {
```

```
        "type": "Ed25519Signature2020",
        "created": "…",
        "verificationMethod": "…",
        "proofPurpose": "…",
        "proofValue": "…",
    }
}
```

Yukarıda gösterilen asgari temel dijital kimlikte yer alan bilgilere ek olarak, her temel kimlik sağlayıcının ekleme yaparak kimliği zenginleştirebileceği başka alanlar bulunmaktadır. Doğrulanabilir Kimlikler standardının genişleyebilir özelliği kullanılarak asgari temel dijital kimliği esas alan başka temel kimlikler tanımlanabilmektedir. Örneğin Ticaret Bakanlığı ve Ticaret Odaları tarafından verilebilecek olan Ticari Sicil Kimliği, asgari temel dijital kimliği esas alan yeni bir temel dijital kimlik olarak tanımlanabilir. Bu amaçla, sadece asgari temel kimlikte olmayan alanların yer aldığı yeni bir JSON-LD bağlamı oluşturularak yayınlanmalıdır. Ticaret Bakanlığı'nın aşağıdaki JSON-LD bağlamını https://www.ticaret.gov.tr/digital-identity/contexts/ticarisicil.jsonld gibi bir adreste yayınladığını varsayalım.

Ticaret Bakanlığı'nın asgari temel dijital kimliği genişleterek oluşturduğu yeni bir temel dijital kimlik olan Ticari Sicil Kimliği, asgari kimliğe yeni bağlam bilgisi eklenerek aşağıdaki şekilde tanımlanabilir.

```
{
  "@context": {
    "mersisNo": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#mersisNo",
    "firmaTuru": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#firmaTuru",
    "sicilMudurlugu": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#sicilMudurlugu",
    "firmaDurumu": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#firmaDurumu",
    "sicilNo": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#sicilNo",
    "eTebligatAdresi": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#eTebligatAdresi",
  }
}
```

```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.ticaret.gov.tr/digital-identity/schemas/v1",
      "https://www.ticaret.gov.tr/digital-identity/contexts/ticarisicil.jsonld"
      ],
    "type": ["VerifiableCredential", "TemelKimlik", "TicariSicilKimligi"],
    "issuer": "...",
    "issuanceDate": "...",
    "expirationDate": "...",
    "credentialSubject": {
        "id": "..."
        "kimlik": {
            "turu": "TemelKimlik",
            "unvan": "...",
            "vergiKimlikNo": "..."
            "vergiDairesi": "...",
            "kurulusTarihi": "...",
            "adres": "...",
            "sehir": "...",
            "mersisNo": "...",
            "firmaTuru": "...",
            "sicilMudurlugu": "...",
            "firmaDurumu": "...",
            "sicilNo": "...",
            "eTebligatAdresi": "..."
        }
     },
    "proof": {
```

```
            "type": "Ed25519Signature2020",
            "created": "…",
            "verificationMethod": "…",
            "proofPurpose": "…",
            "proofValue": "…",
        }
}
```


Benzer şekilde, Vergi Kimliği ve Esnaf/Sanatkâr Sicil Kimliği de asgari temel dijital kimliğin uygun şekilde genişletilmesiyle oluşturulabilir.

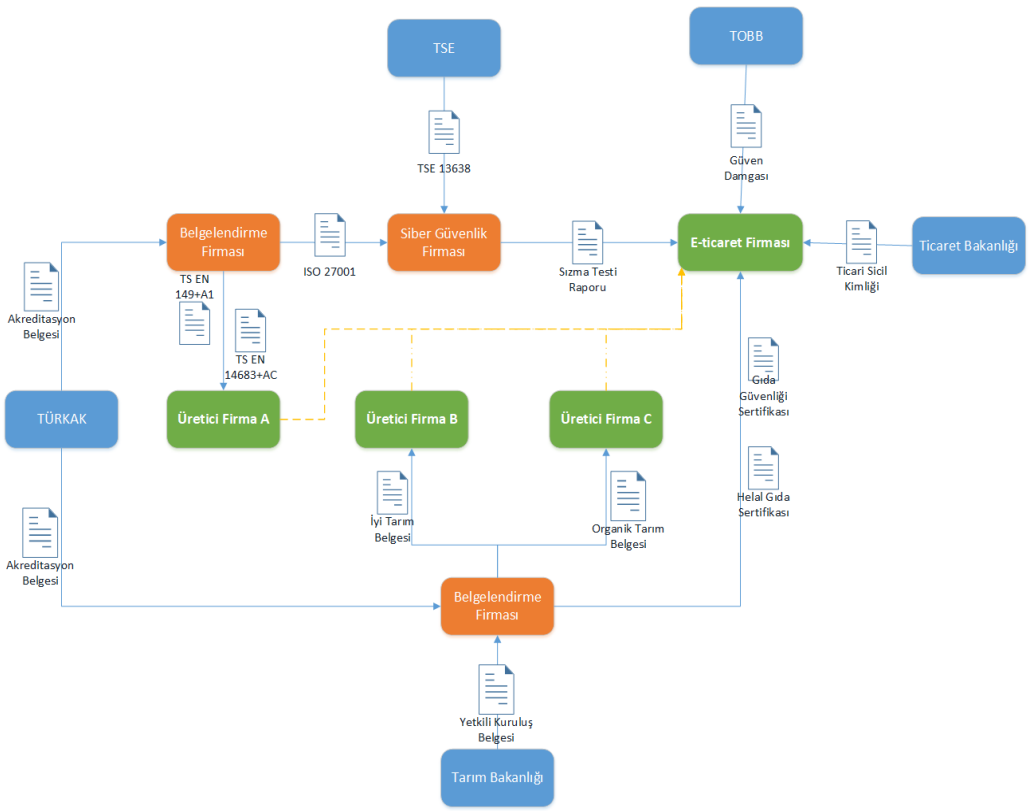
Bir kimlik sahibinin temel kimlik olarak hem Ticaret Bakanlığından Ticari Sicil Kimliği hem de Maliye Bakanlığından Vergi Kimliği alması mümkündür. Kimlik sahibi, her iki temel kimliği de kanıt talep edenlere temel dijital kimlik ispatı olarak sunabilir. Kimlik sahibinin farklı kimlik sağlayıcılardan alınan aynı amacı karşılayan kimliklere sahip olabilmesi ve bunlardan istediğini kanıt talep edenlere kanıt olarak sunabilmesi ile güven çerçevesi prensiplerinden Prensip 9 gerçekleştirilmiş olur.

3.5.2.Bağlamsal Dijital Kimlikler

Bağlamsal dijital kimlikler, temel dijital kimliğini almış e-ticaret firmalarının, üretici firmaların ve ekosistemde yer alan diğer firmaların alabileceği, firmaların sektörlerine ve satışını yaptığı ürün çeşitlerine göre çok farklılık gösterebilen kimliklerdir. Türkiye'deki e-ticaret ekosisteminde yer alan tüm firmaların alabileceği tüm bağlamsal dijital kimliklerin tam listesini oluşturmak ve güncelliğini korumak mümkün olmadığından, bu bölümde örnek bir senaryo üzerinden bağlamsal dijital kimlikler verilmiştir. Aşağıdaki akış şeması, farklı üretici firmaların sağlık ve tarım ürünlerinin satışını yapan örnek bir e-ticaret firmasının, müşterilerin doğrulayabilmesi için satış platformu üzerinde sunabileceği dijital kimliklerin akışı ve bağımlılıklarını göstermektedir.

Şekil 3

e-ticaret İşlemlerine İlişkin Örnek Bağlamsal Dijital Kimlikler



Akışta gösterilen örnek belge gereksinimleri, Türkiye'deki mevcut yasal düzenlemelere göre gerekli olan belgelerdir. E-ticaret dijital kimlik güven çerçevesinin amacı, aynı yasal çerçeveye uygun olarak gerekli olan belgelerin dijital kimliklerle temsil edilmesini ve çevrim içi ortamda güvenli bir şekilde doğrulanabilmesini sağlamaktır.

Güven Damgası, sektöründen bağımsız olarak her e-ticaret firmasının alması beklenen ve sadece Türkiye Odalar ve Borsalar Birliğinin vermeye yetkili olduğu bir belgedir. Güven Damgası, bir e-ticaret firmasının 06/06/2017 tarihinde yayınlanan tebliğde öngörülen asgari güvenlik ve hizmet kalitesi standartlarına uyduğunu gösteren bir elektronik işarettir (Elektronik Ticarette Güven Damgası Hakkında Tebliğ, 2017). Bir e-ticaret firmasının Güven Damgası alabilmesi için, öncelikle Ticaret Bakanlığından Ticari Sicil Kimliğini alması gerekir. Ayrıca bu firmanın Türk Standartları Enstitüsü (TSE) tarafından Onaylı Sızma Testi Firması olarak yetkilendirilmiş ve TSE 13638 belgesi verilmiş olan bir Siber Güvenlik Firmasına sızma testi yaptırarak Sızma Testi Raporu alması gerekir. Siber Güvenlik Firması ise TSE'den bu belgeyi alabilmek için, öncelikle yetkili bir belgelendirme kuruluşundan ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgesi edinmeye hak kazanmalıdır. Belgelendirme kuruluşu da ISO 27001 belgesini verebilmek için TÜRKAK'a akredite olmalıdır.

Organik Tarım ve İyi Tarım belgeleri, Tarım Bakanlığı tarafından yetkilendirilmiş Belgelendirme Kuruluşları tarafından, tarım ürünleri üreticilerinin denetimleri sonrasında verilen belgelerdir. Benzer şekilde, TÜRKAK'tan akredite edilmiş Belgelendirme Kuruluşları tarafından, N95 ve Cerrahi maske üreticilerinin CE Belgesi için uyumlu olması gereken TS EN 149+A1 ve TS EN 14683+AC standartlarına uyumluluk testleri yapılabilmektedir. Ayrıca, yine TÜRKAK'tan akredite edilmiş Belgelendirme Kuruluşları tarafından Gıda Güvenliği Sertifikası ve Helal Gıda Sertifikası verilebilmektedir.

Şekil *3*'te gösterilen örnek bağlamsal dijital kimlikler için dijital kimlik türü, kimliği alan ve kimlik sağlayıcı **Tablo *2***'de verilmiştir.

Tablo 2

e-ticaret İşlemlerine İlişkin Örnek Bağlamsal Dijital Kimlikler

Dijital Kimlik Türü	Kimliği Alan	Kimlik Sağlayıcı
Güven Damgası	E-ticaret Firması	Türkiye Odalar ve Borsalar Birliği
Sızma Testi Raporu	E-ticaret Firması	Siber Güvenlik Firması
TSE 13638 - Sızma testi yapan personel ve firmalar için şartlar	Siber Güvenlik Firması	TSE
ISO 27001 - Bilgi Güvenliği Yönetim Sistemi	Siber Güvenlik Firması	Belgelendirme Kuruluşu
TÜRKAK Akreditasyon Belgesi	Belgelendirme Kuruluşu	TÜRKAK
Tarım Bakanlığı Yetkili Kuruluş Belgesi	Belgelendirme Kuruluşu	Tarım Bakanlığı
Organik Tarım Sertifikası	Üretici Firma	Belgelendirme Kuruluşu
İyi Tarım Uygulamaları Sertifikası	Üretici Firma	Belgelendirme Kuruluşu
TS EN 149+A1 - Parçacıklara karşı koruma amaçlı filtreli yarım maskeler - Özellikler, deneyler ve işaretleme	Üretici Firma	Belgelendirme Kuruluşu
TS EN 14683+AC - Tıbbi yüz maskeleri – Gereklilikler ve deney yöntemleri	Üretici Firma	Belgelendirme Kuruluşu

ISO 22000 - Gıda Güvenliği Yönetim Sistemi	E-ticaret Firması/ Üretici Firma	Belgelendirme Kuruluşu
TS OIC/SMIIC 1: 2011 Helal Gıda Genel Kılavuzu Standardı	E-ticaret Firması/ Üretici Firma	Belgelendirme Kuruluşu

Bağlamsal dijital kimlikler de güven çerçevesinin dijital kimlik paylaşım standardı olan Doğrulanabilir Kimlikler standardına uygun olarak JSON biçiminde gösterilebilir. Örneğin Güven Damgası dijital kimliğinde yer alan bilgiler dikkate alındığında aşağıdaki gibi bir gösterimin uygun olacağı değerlendirilmektedir.

```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.tobb.org.tr/digital-identity/schemas/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
       ],
    "type": ["VerifiableCredential", "BaglamsalKimlik", "GuvenDamgasi"],
    "issuer": "...",
    "issuanceDate": "...",
    "expirationDate": "...",
    "credentialSubject": {
          "id": "...",
          "kimlik": {
                    "turu": " GuvenDamgasi",
                    "unvan": "...",
                    "sektor": "..."
                    "mersisNo": "...",
                    "guvenDamgasiSicilNo": "...",
                }
    },
    "proof": {
          "type": "Ed25519Signature2020",
          "created": "…",
          "verificationMethod": "…",
          "proofPurpose": "…",
          "proofValue": "…",
    }
}
```

3.6 Kimlik Kanıtlama ve Dijital Kimlik Alma

Kimlik kanıtlama ve dijital kimlik alma süreci, potansiyel dijital kimlik sahibinin yetkili kimlik sağlayıcıya kendini ve/veya sahip olduğu yetkiyi ispatlayarak dijital kimliğini alması sürecidir. Firmalar için kimlik kanıtlama ve dijital kimlik alma sürecinde, hem başvuruyu yapan firma yetkilisinin doğrulanması hem de firmanın bilgilerinin doğrulanması yer almaktadır. Bu süreçte dijital kimliği sağlayan kuruluşun kimlik kanıtlama ve dijital kimlik sağlama sürecinde uyguladığı yöntemlere göre farklı güvence seviyeleri ortaya çıkmaktadır. Kimlik sağlayıcı kuruluşun ilgili kimlik için sorumlu yetkili kuruluş olup olmaması da güvence seviyesini etkilemektedir. Bir kimlik türü için sorumlu yetkili kuruluş, ilgili mevzuat ile o kimlik veya kimlikteki bilgilerin kayıt altına alınması ve idame edilmesi için yetkilendirilmiş kuruluştur. Örneğin, bir firmanın ticari sicilinin kayıt ve idamesi ilgili mevzuat gereği bağlı olduğu ticaret odasının sorumluluğunda olduğundan, ticaret odası ticari sicil kimliği için sorumlu yetkili kuruluş olarak kabul edilir. Bir firmanın temel dijital kimliği olarak verilebilecek ticari sicil kimliği, ilgili ticaret odası yerine banka tarafından da sağlanabilir. Fakat dijital kimliğin ticaret odası tarafından sağlanmış olması güvence seviyesinin daha yüksek olmasını sağlayacaktır. Bu çalışma kapsamında e-ticaret dijital kimlik güven çerçevesi için yüksek güvence seviyesi sağlayacak bir kimlik kanıtlama yöntemi belirlenmiştir. Bu yöntem, e-ticaret firması yetkilisinin Elektronik Kimlik Doğrulama Sistemi (EKDS) ile belirlenmesini ve kimlik sağlayıcı kuruluşun sorumlu yetkili kuruluş olmasını gerektirmektedir. Güven çerçevesinin kimlik kanıtlama

için kullanılacak güvence seviyesinin belirlenmesiyle güven çerçevesi prensiplerinden Prensip 2 gerçekleştirilmiş olur. EKDS, T.C. Kimlik Kartının elektronik uygulamalarda kullanımını sağlayacak altyapı olarak TÜBİTAK BİLGEM tarafından geliştirilmiştir. EKDS ile yapılan doğrulamada (UEKAE, 2015):

- Kimlik kartının NVİGM tarafından verildiğini,
- Hizmet alan kişinin kimlik kartının sahibi olduğunu ve hizmet verilen yerde bulunduğu,
- Kimlik doğrulama işleminin ne zaman, nerede ve niçin gerçekleştirildiğini garanti eder.

EKDS ile kimlik doğrulamayı düzenleyen Yönetmelik 22/10/2020 tarihinde yayınlanmıştır (Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliği, 2020). Bu Yönetmelik'te kullanılan güvenlik mekanizmalarına ve kart okuyucu tiplerine göre belirlenmiş 11 farklı kimlik doğrulama yöntemi (Y1-Y11) tanımlanmıştır. Bu yöntemler özet olarak EKDS web sitesinde de sunulmuştur (UEKAE, 2015).

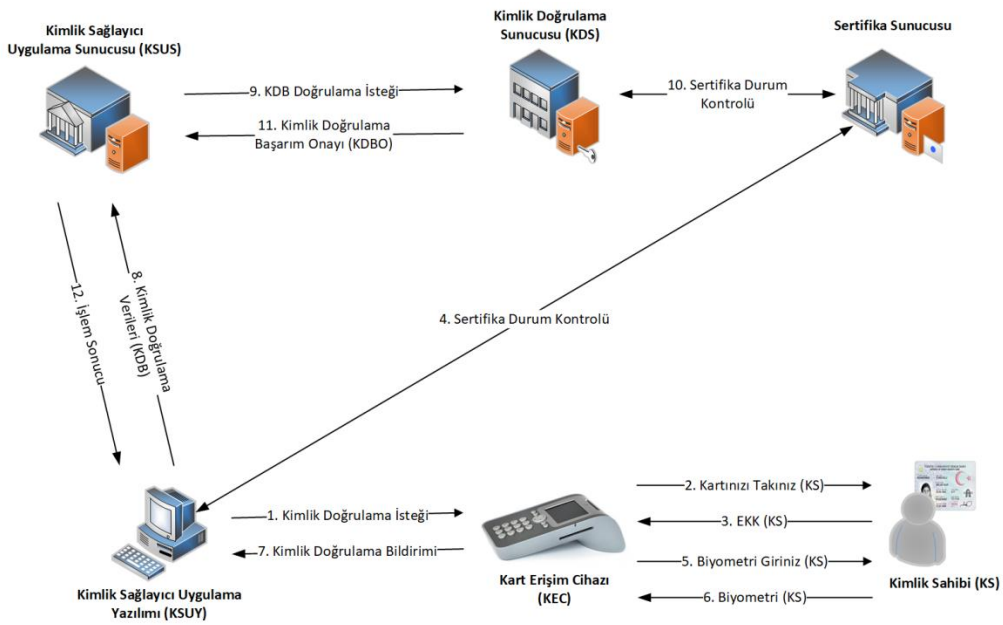
Bu çalışma kapsamında önerilen güven çerçevesinde kabul edilen kimlik kanıtlama yöntemi, EKDS kimlik doğrulama yöntemlerinden en güvenlisi olan ve aşağıdaki güvenlik mekanizmalarının hepsini zorunlu kılan Y11 yöntemidir:

- Güvenli mesajlaşma (Kart okuyucu ile kartın birbirini doğrulaması)
- Kimlik doğrulama sertifikasını doğrulama
- PIN ile kart sahibini doğrulama
- Biyometri ile kart sahibini doğrulama
- Fotoğrafla kart sahibini doğrulama

EKDS ile kimlik doğrulama süreci, bahsedilen kimlik doğrulama yöntemlerinin yanı sıra, kullanılan Kart Erişim Cihazı (KEC) türüne, Kimlik Doğrulama Politika Sunucusu (KDPS) kullanılıp kullanılmayacağına ve kimlik tespiti yapan kişinin kimlik kartının doğrulama sürecine katılıp katılmayacağına göre farklı süreçlerle yapılmaktadır. Bu süreçler TSE'nin yayınladığı EKDS ile ilgili standartlarda tanımlanmaktadır (TSE, 2017). Her bir süreci burada değerlendirmek mümkün olmayacağından, Y11 kimlik doğrulama yöntemini destekleyebilecek en basit süreç seçilerek aşağıda gösterilmiştir. Bu süreç, güvenli mesajlaşma sağlayan, kimlik ve biyometri doğrulama özelliği olan Universal Serial Bus (USB) arabirim kullanan bir KEC cihazı ile gerçekleştirilen, KDPS kullanmayan ve kimlik tespiti yapan kişinin kimlik kartının sürece katılmadığı bir süreçtir.

Şekil 4

EKDS Kimlik Doğrulama Örnek Süreci (TSE, 2017)



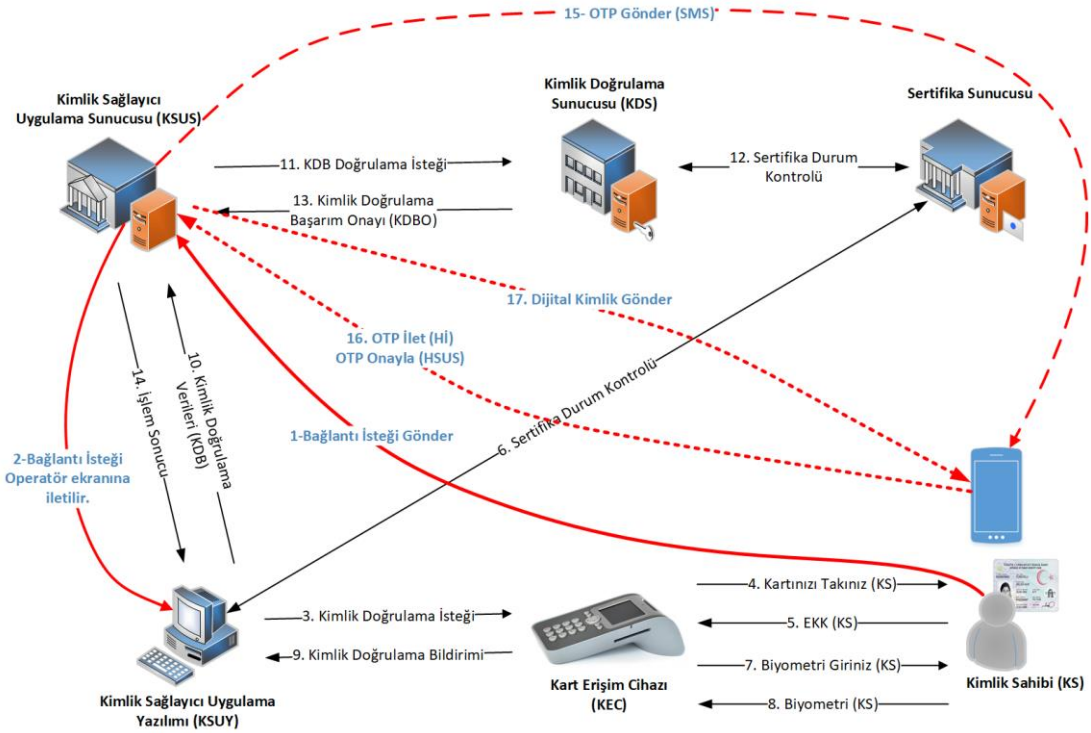
Yukarıda gösterilen EKDS ile kimlik doğrulama sürecindeki Kimlik Sahibi, e-ticaret dijital kimlik güven çerçevesi kapsamında e-ticaret firma yetkiline karşılık gelmektedir. Bu süreç;

- Kimlik Sahibinin sunduğu kimlik belgesinin NVİGM tarafından verilmiş olan geçerli bir kimlik olduğunu (KEC ile kimlik kartı doğrulama)
- Kimlik belgesinin Kimlik Sahibine ait olduğunu (Biyometri doğrulama)
- Kimlik Sahibinin hizmet verilen yerde bulunduğunu (KEC ile kimlik kartı doğrulama ve Biyometri doğrulama) garanti eder.

Bu süreç sonunda dijital kimlik sağlayıcı kuruluş, e-ticaret şirketi yetkilisinin kimliğini doğrulamış olur. Bundan sonraki işlem, e-ticaret şirketi için talep edilen dijital kimliğe ilişkin bilgi ve belgelerin kontrol edilerek doğrulanması sonrasında dijital kimliğin şirket yetkilisine verilmesi işlemidir. EKDS doğrulaması ile dijital kimlik alma süreci aşağıda gösterilmiştir.

Şekil 5

EKDS Doğrulaması ile Dijital Kimlik Alma



3.6. Dijital Kimlik Sunma ve Doğrulama

E-ticaret işlemlerindeki müşterilerin talep etmesi durumunda dijital kimlik sahibi olan e-ticaret firmalarının ve üretici firmaların kendi dijital kimliklerini sunabilmesi ve geçerliliğini ispatlayabilmesi gerekir. E-ticaret dijital kimlik güven çerçevesinin kimlik yönetim modeli olarak kullanıcı egemen kimlik belirlendiğinden, e-ticaret firmaları ve üretici firmalar dijital kimliklerini kendileri saklıyor ve yönetiyor olmalıdır. Bu firmalar, dijital kimliklerini saklamak ve gerektiğinde sunmak için bir dijital cüzdana sahip olmalıdır. Dijital cüzdanlar, elektronik olarak imzalanmış olan doğrulanabilir kimlikleri saklayabilen yapılardır (Nitin & Jenkins, 2020).

E-ticaret dijital kimlik güven çerçevesinin dijital kimlik paylaşım standardı "Doğrulanabilir Kimlikler" (Verifiable Credentials) olarak belirlenmiştir. Buna göre dijital kimliklerin doğrulanması için kimlik ispatı olarak sunulan veriyi doğrulayacak tarafın doğrulanabilir veri kayıt defteri olarak kullanılan blokzincire erişimi olmalı ve oradan alacağı imza bilgileri ile dijital kimliği doğrulayabilmelidir. Doğrulanabilir Kimlikler Veri Modeli, kimlik sağlayıcıdan kimlik sahibinin aldığı dijital kimlik ile

kimlik sahibinin kanıt talep edene sunduğu kanıtı ayırmaktadır. Kimlik sahibinin kanıt talep edene sunduğu dijital veri Doğrulanabilir İbraz (Verifiable Presentation) olarak tanımlanmıştır. Doğrulanabilir İbraz, bir veya birden fazla Doğrulanabilir Kimlikten kimlik sahibinin istediği bilgileri seçerek paketleyebildiği bir yapıdır. Örneğin kimlik sahibi ticari sicil kimliğinden sadece unvan ve kurulusTarihi bilgileri ile güven damgası kimliğinden guvenDamgasiSicilNo bilgisini seçerek yeni bir Doğrulanabilir İbraz oluşturup kanıt talep edene sunabilir. Bu şekilde oluşturulan bir Doğrulanabilir İbraz JSON biçiminde aşağıdaki şekilde gösterilebilir.


```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.ticaret.gov.tr/digital-identity/schemas/v1",
      "https://www.tobb.org.tr/digital-identity/schemas/v1"
   ],
   "type": "VerifiablePresentation",
   "verifiableCredential": [
   {
      "@context": [
         "https://www.w3.org/2018/credentials/v1",
         "https://www.ticaret.gov.tr/digital-identity/schemas/v1"
      ],
      "type": ["VerifiableCredential", "TemelKimlik", "TicariSicilKimligi"],
      "credentialSchema": {
         "id": "...",
         "type": "..."
       },
   "issuer": "...",
   "credentialSubject": {
      "unvan": "...",
      "kurulusTarihi": "..."
      },
   "proof": {
      "type": "AnonCredDerivedCredentialv1",
      "primaryProof": "...",
      "nonRevocationProof": "..."
      }
   },
   {
      "@context": [
         "https://www.w3.org/2018/credentials/v1",
         "https://www.tobb.org.tr/digital-identity/schemas/v1"
      ],
      "type": ["VerifiableCredential", "BaglamsalKimlik", "GuvenDamgasi"],
      "credentialSchema": {
         "id": "...",
         "type": "..."
      },
      "issuer": "...",
      "credentialSubject": {
         "guvenDamgasiSicilNo": "..."
      },
   "proof": {
      "type": "AnonCredDerivedCredentialv1",
      "primaryProof": "...",
      "nonRevocationProof": "..."
      }
 }],
   "proof": {
      "type": "AnonCredPresentationProofv1",
      "proofValue": "..."
   }
}
```

Kimlik sahibinin bir veya birden fazla doğrulanabilir kimlikten istediği alanları birleştirerek doğrulanabilir ibraz oluşturabilmesi ve sadece istediği bilgileri ifşa etmesi ile güven çerçevesi prensiplerinden Prensip 3 gerçekleştirilmiş olur. Doğrulanabilir ibraz yapısı, kimlik sahibinin dijital kimlikleri üzerinde tam kontrole sahip olmasını sağlar.

Sunulan kimlik ispatını alabilmek, saklayabilmek, blokzincire erişebilmek ve sonunda kimlik ispatı verisini doğrulayabilmek için dijital kimliklere özel dijital cüzdan yazılımlarının kullanılması gerekir. E-ticarette firmaların dijital kimliklerini kimlik talep eden rolündeki müşteriler doğrulamak isteyecektir. Dijital kimlik cüzdan yazılımına sahip müşteriler, e-ticaret firmasının çevrim içi olarak sunacağı dijital kimlik ispatlarını doğrulayabileceklerdir. Dijital kimlik doğrulama işleminin etkin kullanılabilirliğini artırmak için e-ticaret firmalarının kare kod gibi mobil cihazlardaki dijital cüzdan yazılımlarından kolayca erişilebilen yöntemler kullanmaları önerilmektedir.

3.7. Güven İşareti

Güven İşareti, e-ticaret firmalarının e-ticaret dijital kimlik güven çerçevesine uyumlu olarak faaliyette bulunulduğunu gösteren bir işarettir. E-ticaret firmasının güven çerçevesi kapsamındaki kurallara uyma taahhüdü ve güven çerçevesi yönetişimi kapsamında belirlenecek yetkili kuruluşların düzenli denetimleri yoluyla e-ticaret firmasının Güven İşareti taşımasına izin verilir. Bu kurallara uymayan e-ticaret firmaları Güven İşareti taşıma hakkını elde edemezler. Bir e-ticaret firmasının Güven İşareti taşıması, diğer paydaşların e-ticaret firmasına duyacağı güveni artıran bir unsur olacaktır. Güven işareti, e-ticaret firmasının güven çerçevesi kapsamındaki kurallara uygun davrandığının denetlendiğini göstermektedir. Böylelikle güven çerçevesi prensiplerinden Prensip 8 gerçekleştirilmiş olur.

Türkiye'de Güven İşaretine benzer bir uygulama Güven Damgası adıyla yer almaktadır. Fakat Güven Damgası, e-ticaret sitesinin sadece belli güvenlik ve hizmet kuralları çerçevesinde faaliyette bulunduğunu göstermektedir. 06/06/2017 tarihinde yayınlanan tebliğ (Elektronik Ticarette Güven Damgası Hakkında Tebliğ, 2017) ile düzenlenen Güven Damgası, "asgari güvenlik ve hizmet kalitesi standardının" varlığına işarettir (TOBB, 2018). Türkiye'de Güven Damgası vermeye yetkili tek kuruluş Türkiye Odalar ve Borsalar Birliğidir. Güven Damgasının görseli aşağıdaki gibidir.

Şekil 6

Güven Damgası

Güven İşareti ise, e-ticaret firmasının sunduğu dijital kimliklerle ilgili olarak güven çerçevesi kapsamında belirlenen kurallara uyduğunu gösterecektir. Dolayısıyla TOBB tarafından verilen Güven Damgası, e-ticaret dijital kimlik güven çerçevesine dâhil edilebilecek bir dijital kimlik türü olabilir. Bu durumda dijital kimlik Güven İşareti, Güven Damgasının TOBB tarafından güven çerçevesi kurallarına uygun olarak, belli bir güvence seviyesinde verildiğini ve Güven Damgasının dijital kimlik olarak doğrulanabilmesini sağlayan mekanizmaların varlığını ifade eder.

3.8. Güven Çerçevesi Paydaşları ve Yönetişimi

Önerilen blokzincir tabanlı dijital kimlik sisteminde iki ana katman yer almaktadır:

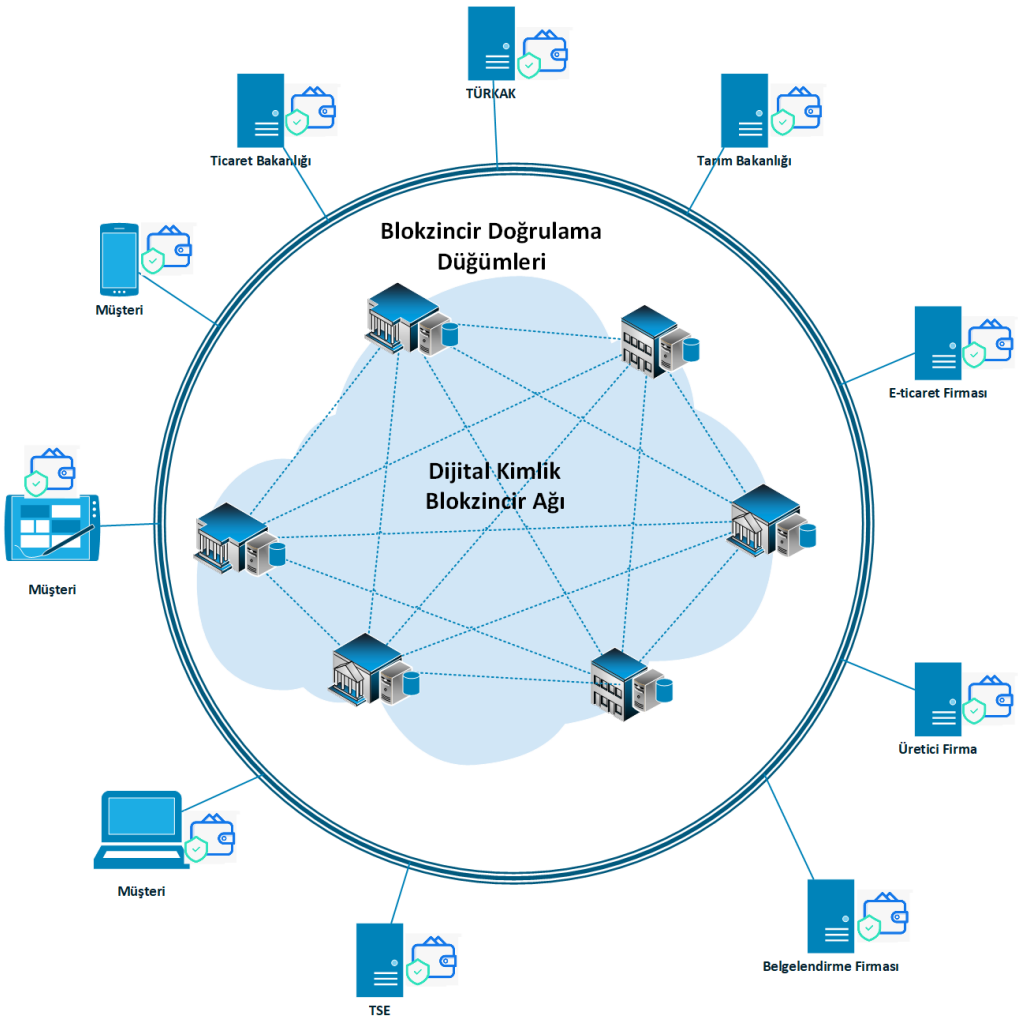
1. Dijital Kimlik Blokzincir Ağı
2. Dijital Cüzdan Sahibi İstemciler

Aşağıdaki şekilde ilk katmanda görüldüğü üzere, birden fazla blokzincir doğrulama düğümü bir araya gelerek Dijital Kimlik Blokzincir Ağını oluştururlar. Blokzincirde tutulan verilerin güvenilirliği ve tutarlılığı, bu düğümlerin hepsinde tutulan ve değiştirilemez olan blokzincir kayıt defterleri aracılığıyla sağlanır. Düğümleri oluşturan paydaşların dijital kimlik sağlayıcı kuruluşlar, dijital kimlik sahipleri veya kanıt talep eden kullanıcılar olması gibi bir zorunluluk yoktur. Düğümler dijital kimlik veren veya alan kuruluşlardan tamamen farklı kuruluşlar tarafından oluşturulabilir. E-ticaret Dijital Kimlik Güven Çerçevesinde belirlenmiş olan Dağıtık Kimlik Yönetim Modeli nedeniyle Blokzincir Ağında dijital kimlikler tutulmaz. Blokzincir Ağında dijital kimlikleri doğrulamak için gerekli olan açık anahtarlar ve dijital kimliklerin geçerliliğini kanıtlayan bazı kriptografik bilgiler yer alır. Bu bilgilere kimlik sağlayıcı kuruluşların, kimlik sahiplerinin ve kanıt talep eden kullanıcıların erişmesi gerektiğinden blokzincirde tutulan verileri okumak için izin alınması gerekmez. Diğer taraftan, kimlik sağlayıcı kuruluşların açık anahtar gibi bilgilerini blokzincire yazmaları gerektiğinden bu kuruluşların sisteme dahil olabilmeleri izne tabidir. Bu nedenle önerilen dijital kimlik güven çerçevesinde yer alacak blokzincir "Kısmen İzin Gerektirmeyen Blockzincir Ağı" olmalıdır (Usta & Doğantekin, 2019).

Dijital Kimlik Blokzincir Ağının dışındaki katmanda ise, bu ağ ile güvenli bir şekilde haberleşen ve dijital kimlikleri saklamak için dijital cüzdanları olan istemciler yer alır. Güven çerçevesinde yer alan dijital kimlik sağlayıcı kuruluşlar, dijital kimlik sahibi firmalar ve dijital kimlik kanıtı talep eden müşteriler bu katmanı oluştururlar.

Şekil 7

Blokzincir Tabanlı Dijital Kimlik Mimarisi



Dijital cüzdan sahibi istemciler, blokzincir ağı ile haberleşen, ağa veri yazan ve ağdan veri okuyan kullanıcı katmanını oluştururlar. Kullanıcı katmanı, güven çerçevesinde yer alan kimlik sağlayıcı, kimlik sahibi ve kanıt talep eden rollerine sahip kullanıcılardan oluşur. Bu kullanıcılar, blokzincir ağının yapısından ve paydaşlarından bağımsız olarak zaman içinde artabilir veya azalabilirler. Blokzincir ağı ise, sistemin teknolojik omurgasını oluşturan, istemci sayısına göre belli miktarda yükü karşılayabilmesi gereken ve sistemin sağlıklı işlemesi için idame edilmesi gereken katmanıdır. Bu nedenle, blokzincir ağını oluşturan paydaşların bu ağın kurulması ve idame edilmesi için kaynak ayırması ve yatırım yapması gerekmektedir.

Dijital kimlik blokzincir ağını oluşturan paydaşlar, dijital kimlik güven çerçevesinin yönetişimi için de ana unsurlar olacaktır. Bu paydaşlardan oluşturulacak bir koordinasyon kurulu, dijital kimlik blokzincir ağının nasıl yönetileceği, ağa yeni üyelerin katılma koşulları, dijital kimlik güven çerçevesine ilişkin kuralların nasıl belirleneceği gibi hususlarda karar verici organizasyon olarak görev yapacaktır. Bu ağı oluşturan paydaşların e-ticaret ekosisteminde farklı rollerle yer alan, yeterli paydaş çeşitliliğini sağlayacak kuruluşlar olmasına özen gösterilmelidir. E-ticaretin ana düzenleyici kuruluşlarından olan Ticaret Bakanlığı, e-ticarette yetkili kuruluşlardan olan TOBB, belge sağlayıcı ana kuruluşlardan olan TSE ve TÜRKAK, belgelendirme kuruluşlarından temsilci kuruluşlar, e-ticaret pazaryerleri ve satıcı firmalarından temsilci kuruluşlar, e-ticaret dernekleri gibi paydaşların bu ağda nihai olarak yer alması hedeflenmelidir. E-ticaret ekosisteminde farklı rolleri temsil eden kuruluşların yer alması, e-ticaret dijital kimlik güven çerçevesinin tüm taraflarının temsil edilmesini ve görüşlerinin dikkate alınmasını mümkün kılacaktır. Güven çerçevesinin yönetişiminin farklı rollerdeki paydaşlardan ortak oluşturulmuş bir kurul tarafından sağlanması, güven çerçevesinin kurallarının ve süreçlerinin de şeffaf bir şekilde ilgili tüm paydaşlara açık olmasını sağlayacaktır. Bu şeffaflık ile güven çerçevesi prensiplerinden Prensip 7 gerçekleştirilmiş olur.

E-ticaret dijital kimlik güven çerçevesi koordinasyon kurulu, blokzincir ağının idame edilmesi için gerekli kaynakları sağlayacağından hem ağa katılacak üyelerin katılma koşullarını hem de bu ağdan hizmet alacak istemci kuruluşların hizmet alma koşullarını düzenleme yetkisine sahip olacaktır. Bu düzenlemeler kapsamında en az aşağıdaki hususların yer alması önerilmektedir:

- Blokzincir ağına katılacak üyelerin katılım için izlemesi gereken yol ve yöntemler,
- Blokzincir ağına katılacak üyelerin sağlaması gereken kaynaklar ve hizmet seviyesi taahhütleri,
- Blokzincir ağından hizmet alacak olan dijital kimlik sağlayıcı yetkili kuruluşların yetkili kuruluş olduklarının doğrulanması için izlenmesi gereken adımlar,
- Dijital kimlik sağlayıcı yetkili kuruluşların uyması gereken şartlar,
- Blokzincir ağından hizmet alacak olan istemcilerden özellikle ağa veri yazacak olan dijital kimlik sağlayıcı kuruluşlara sunulan bu hizmetin ücretlendirilmesi,
- Aynı amaca yönelik farklı yetkili kuruluşlar tarafından verilen dijital kimliklerin ortaklanması amacıyla asgari dijital kimlik yapısının oluşturulması.

Güven çerçevesinde yer alan kuruluşların yanı sıra kanıt talep eden rolündeki e-ticaret müşterileri de güven çerçevesinin kurallarına uymalıdırlar. E-ticaret firmalarından kanıt talep eden müşteriler, firmalara ilişkin doğrulanabilir ibraz yoluyla aldıkları bilgileri sadece dijital cüzdan aracılığıyla doğrulayarak firmaların güvenilirliği hakkında fikir edinebilmek için kullanmalıdırlar. Firmalara ilişkin bilgileri başka bir amaçla kullanmamalıdır. Güven çerçevesi hizmetlerinden faydalanacak olan müşterilerin öncelikle güven çerçevesi kurallarını kabul ettiklerine dair elektronik rıza alınmalıdır. Böylelikle güven çerçevesi prensiplerinden Prensip 4 gerçekleştirilmiş olur.

4. Tartışma ve Sonuç

Bu çalışma ile e-ticaret işlemlerinde güveni artırmak amacıyla, e-ticarete özgü bir dijital kimlik güven çerçevesi önerisi getirilmiştir. Dijital kimlik güven çerçevesine ilişkin yapılmış olan literatürdeki çalışmalar daha çok dijital kimliklerin ülke çapında vatandaşlar tarafından kullanımına ve kamu kurumları tarafından sağlanan hizmetlerin çevrim içi olarak dijital kimlik alt yapısı üzerinden sunulmasına odaklanmıştır. Bu çalışma ile önerilen dijital kimlik güven çerçevesi ise e-ticaret işlemlerinde alıcıların güvenle işlem yapabilmesini ve satıcı ve üretici firmalara güven duymalarını sağlama amacına uygun olarak tasarlanmıştır. Araştırmalarımızda dijital kimlik güven çerçevesinin e-

ticaret işlemlerinde, bu çalışmadaki bağlamda kullanımına yönelik Türkiye'de ve yurt dışında bir çalışmaya rastlanmamıştır. Bu çalışmada önerilen dijital kimlik güven çerçevesi, e-ticaret ekosisteminin paydaşlarını içine alan, güven çerçevesinin prensiplerini, yönetim modelini, standartlarını, kurallarını, işleyişini ve yönetişimini tartışmak yolunda atılan mütevazi bir adım olarak değerlendirilebilir.

Bu çalışmada önerilen dijital kimlik güven çerçevesi modeli, çalışmada belirtilen prensipler üzerine inşa edilmiştir. Bu prensiplerden biri, kuruluşların dijital kimliklerinde yer alan bilgileri tamamen veya kısmen paylaşıp paylaşmama hakkına sahip olmalarıdır. Bu nedenle güven çerçevesinin dijital kimlik yönetim modeli dağıtık veya diğer bir ifadeyle kullanıcı egemen kimlik yönetim modeli belirlenmiştir. Bu kimlik yönetim modeliyle kuruluşların temel ve bağlamsal dijital kimlikleri kendilerinde saklanmakta ve kimliklerde yer alan bilgilerin ne kadarını nasıl paylaşabilecekleri konusunda tam kontrole sahip olmaları sağlanmaktadır. Kuruluşun bir belgesinin varlığını ispat edebilmesi için o belgenin tamamını paylaşma zorunluluğu bulunmamaktadır. Bu sayede belgede yer alan ve kişisel veri kapsamına girebilecek verilerin ifşasının önüne geçilebilmektedir. Bu nedenle, önerilen dijital kimlik güven çerçevesi modelinin Kişisel Verileri Koruma Kanunu (KVKK) ile çelişen bir yönü bulunmamaktadır.

Bu çalışmada önerilen dijital kimlik güven çerçevesi amacı bakımından, Türkiye'de uygulamada olan Güven Damgası ile benzerlik göstermektedir. Güven Damgası da e-ticaret ekosisteminde faaliyet gösteren firmalara müşteriler tarafından duyulan güvenin artırılmasını amaçlayan bir uygulamadır. Güven Damgası uygulaması, firmaların sadece mevzuatta öngörülen asgari güvenlik ve hizmet kalitesi standartlarına sahip olduğuna yönelik bir işaret iken bu çalışmada önerilen dijital kimlik güven çerçevesi ise güven konusunu çok daha geniş bir perspektiften ele almaktadır. E-ticaret firmalarının ve üreticilerin sahip oldukları kuruluş kimliği, sertifika, yetki belgesi, akreditasyon, uygunluk belgesi, güven damgası gibi tüm belgelerin geçerli olduğunu ve yetkili kuruluşlar tarafından verildiğini ispatlayan blokzincir tabanlı dijital kimliklerin kullanımına ilişkin bir model sunulmaktadır. Bu güven çerçevesine katılan ve kurallarına uygun hareket eden kuruluşlara da Güven Damgasına benzer şekilde Dijital Kimlik Güven Çerçevesi Güven İşareti verilmesi önerilmektedir. Bu Güven İşareti, kuruluşun güven çerçevesine uygun davrandığını ve sunduğu dijital kimliklerin güven çerçevesi işleyişine uygun olarak doğrulandığını göstermektedir.

Dijital kimlik güven çerçevesi model olarak bütünsel bir yaklaşım gösterse de uygulanabilmesi için bazı ön şartlar bulunmaktadır. Bunların başında, güven çerçevesinin işletilmesine olanak sağlayacak yasal düzenlemelerin çıkarılması gelmektedir. Blokzincir tabanlı dijital kimlik alt yapısı teknolojik olarak yüksek seviyede güvenilirlik sağlamaktadır. Bu yöntemle sağlanan dijital kimliklerin yasal olarak geçerli sayılabilmesi için mevzuatta gerekli düzenlemelerin yapılması zorunluluğu vardır. 2004 yılında çıkarılan 5070 sayılı Elektronik İmza Kanunu ve bu kapsamdaki düzenlemeler ile elektronik imzanın yasal olarak kabul edilmesi sağlanmıştır. Bu Kanun mevcut hâliyle elektronik sertifika hizmet sağlayıcılarından alınan sertifikalara ve zaman damgasına dayalı olduğundan bu modelde önerilen dijital kimliklerin yasal olarak kabul edilmesi için yeterli değildir. Ayrıca, önerilen model birçok kamu kurumunun bu güven çerçevesi içerisinde dijital kimlik sağlayıcı rolüyle yer almasını öngörmektedir. Kamu kurumlarının bu hizmetleri sunmaları için de gerekli düzenlemelerin yapılmasına ihtiyaç duyulmaktadır. Güven Damgasında denetleyici ve belge sağlayıcı kuruluş olarak TOBB'un yetkilendirilmesine benzer olarak, dijital kimlik güven çerçevesinde yer alacak denetleyici ve Güven İşareti sağlayıcı kuruluşlar da belirlenmeli ve yetkilendirilmelidirler.

Önerilen dijital kimlik güven çerçevesi Türkiye'ye ve e-ticaret ekosistemine özgü olarak şekillendirilmiş olsa da hem yurt dışında hem de farklı sektörlerde uygulanabilecek bir çok yönü bulunmaktadır. Güven çerçevesinin prensipleri, dijital kimlik yönetim modeli, dijital kimlik paylaşım standardı, dijital kimlik sunma ve doğrulama ile güven işareti küçük uyarlamalarla istenilen sektöre ve ülkeye uygun hale getirilebilir. Bu çalışmada önerilen güven çerçevesinin kimlik kanıtlama ve dijital kimlik alma yöntemi EKDS'ye dayalı olduğundan Türkiye'ye özgü bir yöntemdir. Farklı ülkelerde uygulanması için o ülkeye özgü kimlik kanıtlama yöntemlerinin kullanılması gerekecektir. Önerilen güven çerçevesinde yer alan paydaşlar ise e-ticaret ekosisteminde yer alan paydaşlar olup farklı sektörler için uygun paydaşların belirlenmesi gerekmektedir.

Bu çalışmada önerilen Türkiye'deki e-ticarete özgü dijital kimlik güven çerçevesi, e-ticarette güvenin artırılmasına yönelik olarak öngörülebilen yönleriyle bütünsel bir güven çerçevesi modeli ortaya koymaya çalışmaktadır. Dijital kimlik güven çerçevesinin teknik gerçekleştirimine yönelik detaylara girilmeden kavramsal seviyede bir model sunulmuştur. Fakat model için gereken yasal düzenlemeler, kamu kurumlarının bu modele uyum sağlamasında yaşanabilecek zorluklar ve modelin e-ticaret ekosistemindeki birçok paydaşın birlikte çalışmasını içermesi gibi yönleri, modelin hayata geçirilmesinin önündeki zorluklar olarak değerlendirilebilir. Diğer taraftan günümüz dijital dönüşüm çağındaki yeniliklere kamu ve özel sektör kuruluşlarının daha hızlı uyum sağlama reflekslerinin gelişmesi; elektronik imza, e-ticaret ve uzaktan kimlik tespiti gibi konularda hali hazırda yasal düzenlemelerin bulunması, bu zorlukların aşılması için umut vericidir. Bu çalışmanın söz konusu zorluklar hakkında yapılacak tartışmalara katkı sunması temenni edilmektedir.

Etik Standartlar ile Uyumluluk

Çıkar Çatışması: Yazarlar herhangi bir çıkar çatışmasının olmadığını beyan eder.

Etik Kurul İzni: Bu çalışma için etik kurul iznine gerek yoktur.

Yazar Katkı Beyanı: Yazarlar eşit oranda katkı sağladığı beyan etmektedir.

Finansal Destek: Yoktur.

Kaynakça

AccessNow. (2018). *National Digital Identity Programmes: What's Next?* Access Now.

Akram, M., & Sen, A. (2022). A case study Evaluation of Blockchain for digital identity verification and management in BFSI using Zero-Knowledge Proof. *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, (s. 1295-1299).

Argento, L., Buccafurri, F., Furfaro, A., Graziano, S., Guzzo, A., Lax, G., . . . Saccà, D. (2020). ID-Service: A Blockchain-Based Platform to Support Digital-Identity-Aware Service Accountability. *Applied Sciences.*

BCTR. (2019). *Dijital Kimlik Raporu.* Blockchain Türkiye Platformu.

BM. (2020). Digital Identity for Trade and Development: TrainForTrade case studies in South-East Asia. *TrainForTrade Programme of the United Nations Conference on Trade and Development (UNCTAD.* Birleşmiş Milletler.

CESG. (2012). *GPG 43: Requirements for Secure Delivery of Online Public Services.* CESG - National Technical Authority for Information Assurance.

CESG. (2013). *GPG 44: Using authenticators to protect an online service.* CESG - National Technical Authority for Information Assurance.

CESG. (2013). *GPG 46: Organisation Identity.* CESG - National Technical Authority for Information Assurance.

CESG. (2014). *GPG 45: How to prove and verify someone's identity.* CESG - National Technical Authority for Information Assurance.

DIACC. (2020). *Pan-Canadian Trust Framework Glossary.* The Digital Identification and Authentication Council of Canada.

DIACC. (2020). *Pan-Canadian Trust Framework Model.* The Digital Identification and Authentication Council of Canada.

Dissanayake, K., Somarathne, P., Fernando, U., Pathmasiri, D., Liyanapathirana, C., & Rupasinghe, D. L. (2021). "Trust Pass" - Blockchain-Based Trusted Digital Identity Platform Towards Digital Transformation. *2021 2nd International Informatics and Software Engineering Conference (IISEC)*, (s. 1-6).

European Union. (2014, 08 28). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union*.

Gada, S., Dhuri, A., Jain, D., Bansod, S., & Toradmalle, D. (2021). Blockchain-Based Crowdfunding: A Trust Building Model. *2021 International Conference on Artificial Intelligence and Machine Vision (AIMV).*

Goodell, G., & Aste, T. (2019). Decentralized Digital Identity Architecture. *Front. Blockchain, 2-17*.

Gruner, A., Muhle, A., Gayvoronskaya, T., & Meinel, C. (2018). A Quantifiable Trust Model for Blockchain-Based Identity Management. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1475–1482.

ID2020. (2018). Manifesto. https://id2020.org/manifesto.

ID2020. (2019, 01). ID2020 Technical Requirements. ID2020.

ITU. (2018). *Digital Identity Roadmap Guide.* The International Telecommunication Union.

Jamal, A., Helmi, R. A., Syahirah, A. S., & Fatima, M.-A. (2019). Blockchain-Based Identity Verification System. *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*, (s. 253-257).

Liao, C.-H., Guan, X.-Q., Cheng, J.-H., & Yuan, S.-M. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. *Future Generation Computer Systems*, 450-466.

Lim, J. (2020). Self-Sovereign Identity: The Harmonising Of Digital Identity Solutions Through Distributed Ledger Technology. *Australian National University Journal of Law and Technology*.

Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L., Ang, T. F., & Ismail, R. (2018). Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. *International Journal on Advanced Science, Engineering and Information Technology*.

Liu, J., Hodges, A., Clay, L., & Monarch, J. (2020). An analysis of digital identity management systems - a two-mapping view. *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, (s. 92-96).

Maler, E., Nadalin, A., Reed, D., Rundle, M., & Thibeau, D. (2010). *Open Identity Trust Framework (OITF) Model.* Open Identity Exchange.

Mothershaw, N. (2020). *OIX Guide to Trust Frameworks.* Open Identity Exchange.

Nitin, N., & Jenkins, P. (2020). *Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology*. 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), (s. 90-95)

NZ Digital government. (2020, 07). *Digital Identity Trust Framework | NZ Digital government*. https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/digital-identity-trust-framework/

Pöhn, D., & Hommel, W. (2020). An overview of limitations and approaches in identity management. *Proceedings of the 15th International Conference on Availability, Reliability and Security.*

Rasouli, H., Valmohammadi, C., Azad, N., & Esfeden, G. A. (2021). Proposing a digital identity management framework: A mixed-method approach. *Concurrency and Computation: Practice and Experience*.

Resmi Gazete. (2017, 06 06). Elektronik Ticarette Güven Damgası Hakkında Tebliğ.

Resmi Gazete. (2020, 10 22). Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliği.

Resmi Gazete. (2021, 04 01). Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik.

Statista. *Global retail e-commerce market size 2014-2023*. https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Temoshok, D., & Abruzzi, C. (2018). *Developing Trust Frameworks to Support Identity Federations.* National Institute of Standards and Technology.

The Better Identity Coalition. (2019). *Better Identity in America: A Blueprint for Policymakers.*

TOBB. (2018). Güven Damgası. https://www.guvendamgasi.org.tr/

TSE. (2017, 04 24). Elektronik kimlik doğrulama sistemi - Bölüm 1: Genel bakış.

UEKAE. (2015). *Elektronik Kimlik Doğrulama Sistemi*. EKDS. https://www.ekds.gov.tr/ekds/elektronik-kimlik-dogrulama-sistemi

UEKAE. (2015). *Kimlik Doğrulama Yöntemleri*. https://www.ekds.gov.tr/ekds/kimlik-dogrulama-yontemleri

Usta, A., & Doğantekin, S. (2019). *Blockchain 101*. Bankalararası Kart Merkezi.

W3C. (2019, 11 19). *Verifiable Credentials Data Model 1.0*. https://www.w3.org/TR/vc-data-model/

WBG. (2018). *G20 Digital Identity Onboarding.* The World Bank Group.

WBG. (2019). *Practitioner's Guide.* The World Bank Group.

WEF. (2018). *Identity in a Digital World.* World Economic Forum.

WEF. (2019). *Digital Identity.* World Economic Forum.